Panda Endpoint Protection

Guía de administración de Panda Endpoint Protection

Autor: Panda Security

Versión: 9.30.00

Fecha: 08/05/2024

panda

pandasecurity.com

Aviso legal.

Marcas registradas.

Información de contacto.

Oficinas centrales:

Panda Security

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 España.

https://www.pandasecurity.com/spain/about/contact/

Acerca de la Guía de administración de Panda Endpoint Protection

Para obtener la versión más reciente de la documentación en formato PDF consulta la dirección web:

https://www.pandasecurity.com/rfiles/enterprise/solutions/endpointprotection/latest/ENDPOINTPROTECTIONoAP-guia-ES.pdf

Para consultar un tema específico, accede a la ayuda web del producto disponible en:

https://www.pandasecurity.com/enterprise/downloads/docs/product/help/endpointprotection/latest/es/index.htm

Información sobre las novedades de la versión

Para conocer las novedades de la ultima versión de Panda Endpoint Protection consulta la siguiente URL:

https://info.pandasecurity.com/aether/?product=EP&lang=es

Soporte técnico

Panda Security ofrece un soporte técnico global cuyo objetivo principal es responder a cuestiones especificas sobre el funcionamiento de sus productos. El equipo de soporte técnico también genera documentación sobre detalles técnicos del producto, que ofrece a través de su portal eKnowledge Base.

Para acceder a información específica del producto consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/endpoint-protection-aether.htm

Para acceder al portal eKnowledge Base consulta la siguiente URL:

https://www.pandasecurity.com/spain/support/#enterprise

Encuesta sobre la Guía de administración de Panda Endpoint Protection

Evalúa esta Guía de administración y envíanos sugerencias y peticiones para próximas versiones de la documentación en:

https://es.surveymonkey.com/r/feedbackEPGuideES

Tabla de contenidos

Capítulo 1

Prólogo

La Guía de administración contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto Panda Endpoint Protection.

Contenido del capítulo

¿A quién está dirigida esta Guía de administración?

Esta documentación está dirigida a administradores de red que necesitan gestionar la seguridad de los equipos informáticos de su empresa, determinar los problemas de seguridad detectados y establecer planes de respuesta y prevención que mitiguen las amenazas encontradas.

¿Qué es Panda Endpoint Protection?

Panda Endpoint Protection es un servicio gestionado que protege los equipos de la red sin la intervención activa y constante del administrador. Adicionalmente, provee información muy detallada del parque informático y del estado de la seguridad, gracias a la nueva plataforma Aether, desarrollada por Panda Security.

Panda Endpoint Protection está dividido en dos áreas funcionales bien diferenciadas:

- Panda Endpoint Protection
- Plataforma Aether

Panda Endpoint Protection

Es el producto que implementa todas las características orientadas a garantizar la seguridad de los puestos de usuario y servidores, sin requerir la intervención del administrador de la red.

Plataforma Aether

Aether es el ecosistema orientado a la gran cuenta y MSPs donde se ejecuta Panda Endpoint Protection: una plataforma eficiente, extensible y escalable para gestionar de forma centralizada las soluciones de seguridad de Panda Security. Aether presenta la información generada por Panda Endpoint Protection sobre los procesos, los programas ejecutados por los usuarios y los dispositivos instalados en la empresa, todo ello en tiempo real, de forma ordenada y con un alto nivel de detalle.

Iconos

En esta Guía de administración se utilizan los siguientes iconos:

Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consulta en otra sección de la Guía de administración.

Capítulo 2

Información básica de Panda Endpoint Protection

Panda Endpoint Protection es una solución completa de seguridad para puestos de usuario y servidores, formada por múltiples tecnologías que ofrecen a los clientes un completo servicio de protección contra el malware, sin necesidad de instalar, gestionar o mantener nuevos recursos hardware en la infraestructura de la organización.

Contenido del capítulo

Beneficios de Panda Endpoint Protection

Panda Endpoint Protection es una solución de seguridad basada en múltiples tecnologías de protección, que permiten sustituir el producto de antivirus *on premise* o *standalone* utilizado en la organización por un completo servicio cloud gestionado desde la nube.

Es un software de seguridad muy ligero que se instala en los equipos de la red protegiéndolos de forma centralizada e ininterrumpida, y con una única consola de administración web alojada en la nube, accesible en cualquier momento y lugar.

Con Panda Endpoint Protection la protección se gestiona cómoda y fácilmente de forma centralizada desde una única consola Web, sin necesidad de instalar en la organización nueva infraestructura para el control del servicio, manteniendo de esta manera un TCO bajo.

Al tratarse de un producto multiplataforma, alojado en la nube y compatible con Windows, macOS, Linux, Android y con entornos virtuales y VDI, tanto persistentes como no persistentes, es suficiente una única herramienta para cubrir la seguridad de todos los equipos de la empresa.

Características de Panda Endpoint Protection

Panda Endpoint Protection es un producto que gestiona la seguridad de todos los equipos de la red, sin impacto negativo en el rendimiento de los dispositivos y al menor coste de propiedad posible. Entre sus principales beneficios se encuentran:

Producto muy ligero

Todas las operaciones se ejecutan en la nube: el impacto en el rendimiento del equipo es prácticamente nulo.

- **Ligero en consumo de memoria**: con un menor tamaño de 'los ficheros de firmas gracias al acceso en tiempo real a la inteligencia colectiva, que permite mover la base de datos de malware del equipo de usuario a la nube.
- **Ligero en consumo de red**: reducción al mínimo del volumen de descargas.
- **Fichero de firmas compartidas entre equipos**: se descarga una vez y se comparte entre los equipos dentro de la red.
- **Ligero en consumo de procesador**: la inteligencia de detección se traslada a la nube con lo que se requieren menos recursos de procesador en los equipos protegidos.

Seguridad Multiplataforma

Cubre todos los vectores de infección en equipos Windows, Linux, macOS y Android.

- **Seguridad en todos los vectores de ataque**: navegación, correo, sistema de ficheros y control de los dispositivos conectados al PC.
- **Seguridad contra amenazas desconocidas**: mediante tecnologías heurísticas y análisis contextuales.
- **Seguridad en todas las plataformas:** Windows, Linux, macOS, Android y motores virtuales (Wmware, Virtual PC, MS Hyper-V, Citrix). También gestiona de forma transparente las licencias asignadas a equipos pertenecientes a infraestructuras VDI, tanto persistentes como no persistentes.

Fácil de Manejar

- Gestión sencilla, sin mantenimientos ni necesidad de infraestructuras en la red del cliente.
- **Fácil de mantener**: no requiere infraestructura específica para alojar la solución; el departamento de IT podrá dedicarse a tareas más productivas.
- **Fácil de proteger a usuarios remotos**: cada equipo protegido con Panda Endpoint Protection se comunica con la nube; los usuarios desplazados y delegaciones remotas se protegen de forma natural, sin instalaciones ni configuraciones VPN particulares.
- **Fácil de desplegar**: múltiples métodos de despliegue y con desinstaladores automáticos de antivirus de la competencia, que facilitan una rápida migración desde soluciones de terceros.
- **Curva de aprendizaje muy suave**: interface web de gestión intuitivo y sencillo, con las opciones más utilizadas a un solo clic.

Características de la plataforma Aether

Aether es la nueva plataforma de gestión, comunicación y tratamiento de la información desarrollada por Panda Security, que agrupa y centraliza los servicios comunes a todos sus productos.

La plataforma Aether gestiona las comunicaciones con los agentes desplegados en los equipos protegidos de los clientes, y presenta en la consola de administración, de forma ordenada y comprensible, toda la información recogida por Panda Endpoint Protection para su posterior análisis por parte del administrador de la red.

Este diseño modular de la solución evita la instalación de nuevos agentes o productos en los equipos del cliente por cada módulo adicional contratado. Todos los productos de Panda Security que funcionan sobre la plataforma Aether comparten un mismo agente en el equipo del usuario y una misma consola web de administración, facilitando su gestión y minimizando los recursos de los equipos.

Principales beneficios de Aether

A continuación, se presentan los principales servicios ofrecidos por Aether para todos los productos de Panda Security que sean compatibles con la plataforma:

Plataforma de gestión Cloud

Aether es una plataforma que reside en la nube, incorporando importantes ventajas de cara a su manejo, funcionalidad y accesibilidad:

No requiere servidores de gestión que alojen la consola de administración en las instalaciones del cliente: al funcionar desde la nube, es directamente accesible por todos los equipos suscritos al

servicio, desde cualquier lugar y en cualquier momento, sin importar si están dentro de la oficina o desplazados.

El administrador de la red puede acceder a la consola de administración desde cualquier momento y en cualquier lugar, simplemente con un navegador compatible desde un equipo portátil, un equipo de sobremesa o incluso un dispositivo móvil como una tablet o un smartphone.

Es una plataforma ofrecida en régimen de alta disponibilidad, operativa el 99'99% del tiempo. El administrador de la red queda liberado de diseñar y desplegar costosos sistemas en redundancia para alojar las herramientas de gestión.

Comunicación con la plataforma en tiempo real

El envío de configuraciones y tareas programadas desde y hacia los equipos de la red se realiza en tiempo real, en el momento en que el administrador aplica la nueva configuración a los dispositivos seleccionados. El administrador puede ajustar los parámetros de la seguridad de forma casi instantánea para solucionar posibles brechas de seguridad o adaptar el servicio de seguridad al constante cambio de la infraestructura informática de las empresas.

Multi producto y Multiplataforma

La integración de los productos de Panda Security en una misma plataforma ofrece las siguientes ventajas al administrador:

- **Minimiza la curva de aprendizaje**: todos los productos comparten una misma consola, de esta forma se minimiza el tiempo que el administrador requiere para aprender el manejo de una nueva herramienta, redundando en menores costes de TCO.
- **Único despliegue para múltiples productos**: solo es necesario un único programa instalado en cada equipo para ofrecer la funcionalidad de todos los productos compatibles con Aether Platform. De esta forma se minimizan los recursos utilizados en los equipos de los usuarios en comparación con la utilización de productos independientes.
- **Mayores sinergias entre productos**: todos los productos reportan en una misma consola: el administrador dispone de un único panel de control donde observa toda la información generada, minimizando el tiempo y el esfuerzo invertido en mantener varios repositorios de información independientes y en consolidar la información generada en fuentes distribuidas.
- **Compatible con múltiples plataformas**: no es necesario contratar distintos productos para cubrir todo el espectro de dispositivos de la compañía: Aether Platform funciona para Windows, Linux, macOS y Android, además de entornos virtuales y VDI tanto persistentes como no persistentes.

Configuraciones flexibles y granulares

El nuevo modelo de configuración permite acelerar la gestión de los equipos mediante la reutilización de configuraciones, haciendo uso de mecanismos específicos como la herencia y la

asignación de configuraciones a equipos individuales. El administrador de la red podrá asignar configuraciones mucho más específicas y con menor esfuerzo.

Información completa y a medida

Aether Platform implementa mecanismos que permiten configurar la cantidad de datos mostrados a lo largo de una amplia selección de informes, según las necesidades del administrador o del consumidor final de la información.

La información se completa además con datos sobre los equipos, hardware y software instalado, así como un registro de cambios, que ayudarán al administrador a valorar el estado de la seguridad del parque informático administrado.

Arquitectura de Aether

La arquitectura de Aether está diseñada de forma escalable para ofrecer un servicio flexible y eficiente. La información se envía y se recibe en tiempo real desde / hacia múltiples fuentes y destinos de forma simultánea. Los orígenes y destinos pueden ser equipos vinculados al servicio, consumidores externos de información como sistemas SIEM o servidores de correo, instancias web para las peticiones de cambios de configuración y presentación de información de los administradores de red, entre otros.

Además, Aether implementa un backed y una capa de almacenamiento que utiliza una amplia variedad de tecnologías que le permite manipular los múltiples tipos de datos de forma ágil.

Estructura lógica de la plataforma Aether muestra un diagrama a alto nivel de Aether Platform.

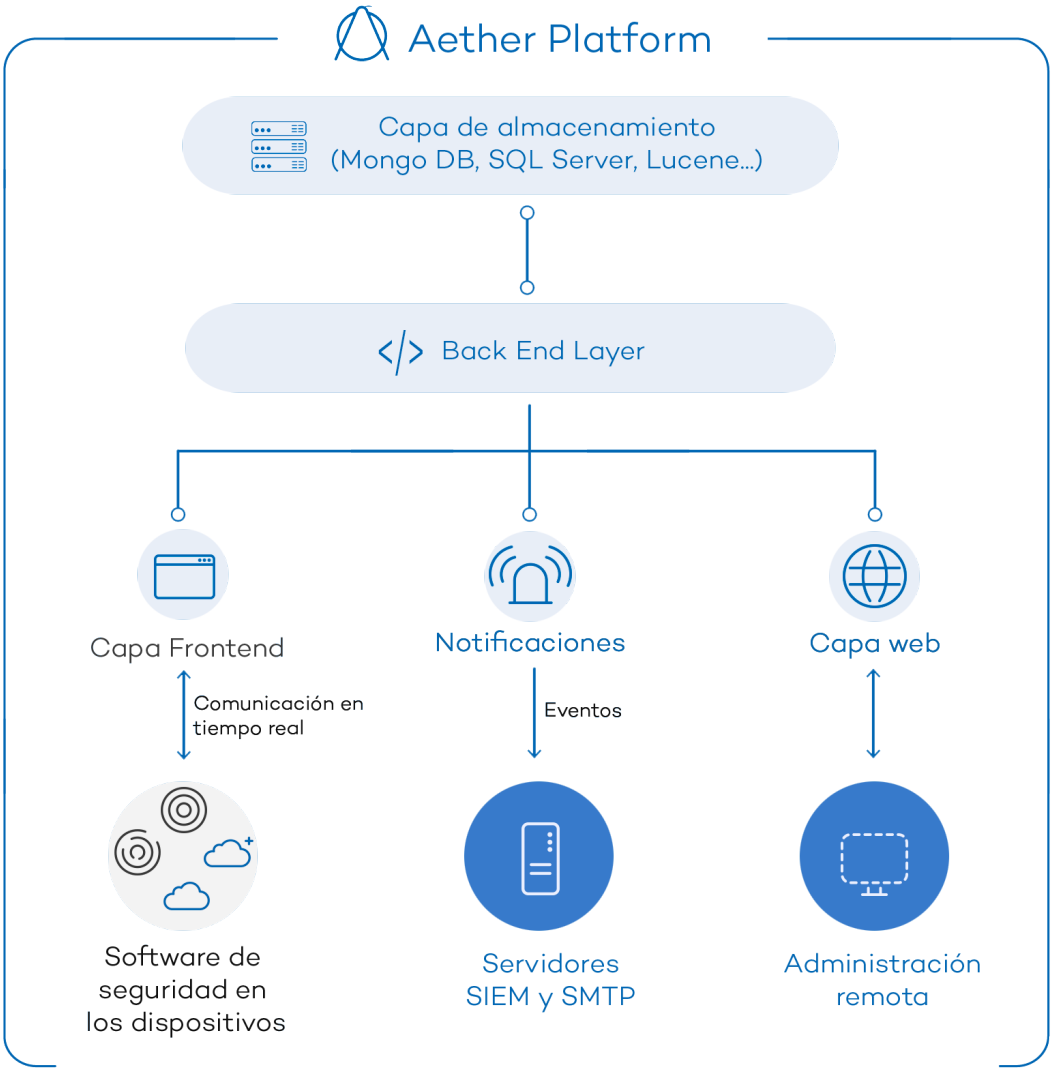


Figura 2.1: Estructura lógica de la plataforma Aether

Aether en los equipos de usuario

Los equipos de la red protegidos con Panda Endpoint Protection llevan instalado un software, formado por dos módulos independientes pero relacionados, que aportan toda la funcionalidad de protección y gestión:

- **Módulo Agente de comunicaciones Panda (agente Panda)**: es el encargado de servir de puente entre el módulo de protección y la nube, gestionando las comunicaciones, eventos y configuraciones de seguridad implementadas por el administrador desde la consola de administración.
- **Módulo Protección Panda Endpoint Protection**: es el encargado de proteger de forma efectiva el equipo del usuario. Para ello se sirve del agente de comunicaciones para recibir las configuraciones y emite estadísticas y datos de las detecciones y elementos analizado.

Agente de comunicaciones en tiempo real Panda

El agente Panda se encarga de las comunicaciones entre los equipos administrados y el servidor de Panda Endpoint Protection, y de establecer un diálogo entre los equipos que pertenecen a una misma red del cliente.

Este módulo también gestiona los procesos de la solución de seguridad y recoge los cambios de configuración que el administrador haya realizado a través de la consola Web, aplicándolos sobre el módulo de protección.

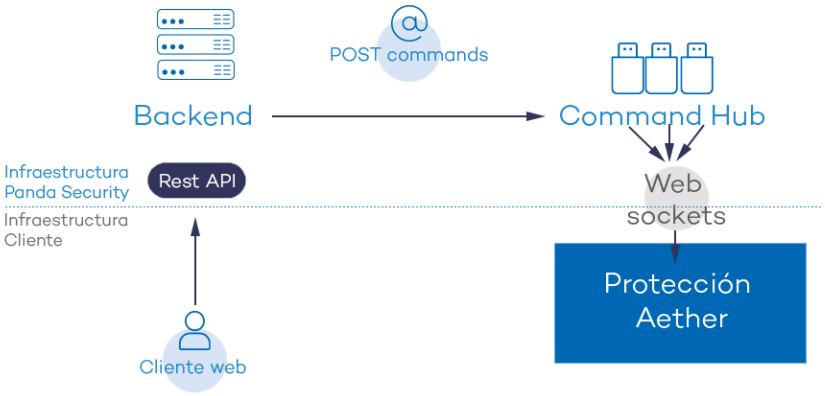


Figura 2.2: Recorrido de los comandos introducidos con la consola de administración

La comunicación entre los dispositivos y el Command Hub se implementa mediante conexiones websockets persistentes y en tiempo real, estableciendo una conexión por cada uno de los equipos para el envío y recepción de datos. Para evitar que dispositivos intermedios provoquen el cierre de las conexiones, se genera un flujo de keepalives constante.

Las configuraciones establecidas por el administrador de la red mediante la consola de administración Panda Endpoint Protection se envían mediante una API REST al backend; éste las reenvía al Command hub generando un comando POST, el cual finalmente ejecuta un push de la información a todos los dispositivos suscritos. Con un buen funcionamiento de las líneas de comunicación, los equipos recibirán la configuración en tiempo real.

Componentes principales

Panda Endpoint Protection es un servicio de seguridad cloud que mueve el almacenamiento de la inteligencia de seguridad y gran parte de las tareas de análisis a la infraestructura IT desplegada en los CDPs de Panda Security. De esta manera se consigue un software de seguridad muy ligero, con un bajo consumo de recursos y simplificando al máximo los requisitos necesarios para su puesta en marcha en las organizaciones.

Esquema general Panda Endpoint Protection representa el esquema general de Panda Endpoint Protection y los componentes que lo forman:

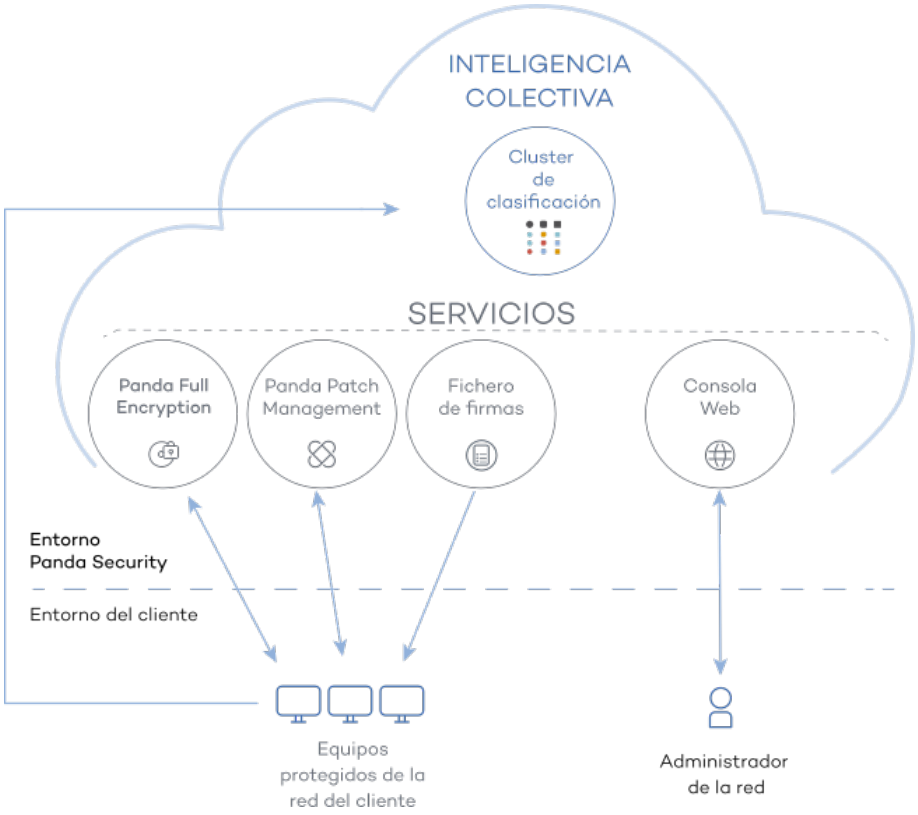


Figura 2.3: Esquema general Panda Endpoint Protection

- **Servidores de inteligencia colectiva**: dan soporte a la recogida y clasificación de muestras y evidencias enviadas por los clientes de Panda Security. Adicionalmente publican una base de datos accesible en tiempo real con todas las amenazas detectadas.
- **Servidores de descargas del fichero de firmas**: publican el fichero de firmas descargable por los productos de Panda Security.
- **Servicio Panda Data Control (opcional)**: servicio de visibilidad, inventario y supervisión de la información personal que almacenan los ficheros PII.
- **Servicio Evaluación de vulnerabilidades**: localización de software con vulnerabilidades e información sobre parches disponibles.
- **Servicio Panda Patch Management (opcional)**: parcheo de sistemas operativos Windows y aplicaciones de terceros.
- **Servicio Panda Full Encryption (opcional)**: cifra los dispositivos de almacenamiento interno de los equipos Windows para minimizar la exposición de datos en caso de perdida o robo, o al desechar dispositivos de almacenamiento sin borrar completamente su contenido.
- **Consola web**: servidor de la consola de administración.
- Equipos protegidos mediante el software Panda Endpoint Protection instalado.
- Equipo del administrador de red que accede a la consola Web.

Servidores de inteligencia colectiva

Los servidores que soportan la inteligencia se encargan de clasificar y procesar de forma automática toda la información que la comunidad de usuarios proporciona sobre las detecciones producidas en sus equipos. Estos servidores pertenecen a la infraestructura de Panda Security desplegada en la nube; la protección Panda Endpoint Protection instalada en los equipos realiza consultas a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos.

Servidores de ficheros de firmas

Son los recursos en la nube que Panda Security pone a disposición de los usuarios para poder descargar los ficheros de firmas, necesarios para completar las tareas de detección de Panda Endpoint Protection. Dado que los ficheros de firmas pueden alcanzar un tamaño considerable y que su descarga es como mínimo diaria, los servidores de ficheros de firmas también controlan la versión ya instalada en el equipo del cliente para calcular las diferencias con respecto a la versión publicada y enviar unicamente los datos necesarios, minimizando así los costes de ancho de banda del cliente relativos a la actualización de la solución de antivirus instalada en el parque.

Servidor Web de la consola de administración

La consola Web es compatible con los navegadores más comunes y es accesible desde cualquier lugar y en cualquier momento con cualquier dispositivo que tenga instalado un navegador compatible.

*Para verificar si tu navegador es compatible con el servicio consulta **Acceso a la consola web** en la página **637**.*

La consola Web es "responsive", de modo que se puede utilizar sin problemas desde móviles y tablets.

Equipos protegidos con Panda Endpoint Protection

Panda Endpoint Protection requiere de la instalación de un componente software en todas las máquinas del parque informático susceptibles de sufrir problemas de seguridad. Este componente está formado por dos módulos: el agente de comunicaciones Panda y el módulo de la protección Panda Endpoint Protection.

Panda Endpoint Protection se instala sin problemas en máquinas con otras soluciones de seguridad de la competencia.

El módulo de la protección contiene las tecnologías encargadas de proteger los equipos del cliente. Panda Endpoint Protection reúne en un mismo producto todos los recursos necesarios para detectar el malware, al tiempo que incorpora herramientas de resolución, para desinfectar los equipos comprometidos.

Servicios Panda Endpoint Protection

Panda Security ofrece otros servicios, algunos de carácter opcional, que integran la solución con la infraestructura IT del cliente, y obtener de forma directa la inteligencia de seguridad generada en los laboratorios de Panda Security.

Servicio Panda Patch Management (opcional)

Este servicio reduce la superficie de ataque de los puestos de usuario y servidores Windows actualizando el software vulnerable (sistemas operativos y aplicaciones de terceros) con los parches publicados por los proveedores correspondientes.

Además, permite localizar los programas que han entrado en EoL (End Of Life) considerados peligrosos por no tener mantenimiento de su proveedor original y ser el blanco de los hackers que aprovechan las vulnerabilidades conocidas y sin corregir. El administrador puede localizar con facilidad todos los programas en EoL y planificar una sustitución controlada de los mismos.

En caso de incompatibilidades o mal funcionamiento de las aplicaciones parcheadas, Panda Patch Management permite ejecutar un Rollback / desinstalación de los parches que lo permitan o excluirlos previamente para evitar su instalación.

Servicio Evaluación de vulnerabilidades

Este servicio gratuito realiza una búsqueda en los equipos para detectar software instalado que tenga vulnerabilidades. Con el fin de evitar que el malware aproveche estas brechas de seguridad para dañar e infectar los equipos y servidores, informa de la existencia de parches disponibles que eviten el impacto de las vulnerabilidades.

Para instalar de forma centralizada los parches disponibles es necesario obtener una licencia de Panda Patch Management.

Servicio Panda Full Encryption (opcional)

El cifrado de la información contenida en los dispositivos de almacenamiento interno de los equipos es un recurso fundamental a la hora de proteger los datos que contienen en caso de robo o pérdida y cuando la empresa recicla dispositivos de almacenamiento sin borrar completamente. Panda Endpoint Protection utiliza la tecnología BitLocker (Windows) Y FileVault (macOS) para cifrar el contenido de los discos duros a nivel de sector y gestiona de forma centralizada las claves de recuperación en caso de pérdida o cambio de configuración de hardware.

El módulo Panda Full Encryption permite utilizar el modulo de plataforma segura TPM si está disponible, y ofrece varias configuraciones de autenticación para añadir flexibilidad a la protección de los datos contenidos en el equipo.

Perfil de usuario del producto

Aunque Panda Endpoint Protection es un servicio gestionado que ofrece seguridad sin intervención del administrador de la red, también provee información muy detallada y comprensible sobre la actividad de los procesos ejecutados por los usuarios en toda la infraestructura de IT de la empresa. Esta información puede ser utilizada por el administrador para precisar el impacto de problemas de seguridad y adaptar sus protocolos, evitando así la repetición de situaciones similares en el futuro.

Dispositivos e idiomas soportados

*Para una descripción detallada de las plataformas y requisitos consulta **Funcionalidades del producto y requisitos** en la página **619** para más información.*

Compatibilidad con sistemas operativos

- Windows Workstation
- Windows Server
- Sistemas virtuales y VDI persistentes y no persistentes
- macOS
- Linux
- Tablets y móviles Android

Compatibilidad con navegadores web

La consola de administración es compatible con las últimas versiones de los navegadores mostrados a continuación:

- Chrome
- Microsoft Edge
- Firefox
- Opera

Idiomas soportados en la consola web

- Español
- Inglés
- Sueco
- Francés
- Italiano
- Alemán
- Portugués
- Húngaro
- Ruso
- Japonés
- Finlandés (solo consola local)

Capítulo 3

La consola de administración

Panda Endpoint Protection utiliza las últimas tecnologías de desarrollo web para ofrecer una consola de administración alojada en la nube que permite interactuar de manera cómoda y ágil con el servicio de seguridad. Sus principales características son:

- **Adaptable**: diseño "responsive" que se adapta al tamaño del dispositivo empleado para administrar el servicio.
- **Amigable**: interface desarrollado con tecnología Ajax que evita las recargas de páginas completas.
- **Flexible**: interface adaptable que almacena los ajustes realizados para posteriores accesos.
- **Homogénea**: patrones de usabilidad bien definidos para minimizar la curva de aprendizaje del administrador.
- **Interoperable**: datos exportables en formato `csv` con campos extendidos para su posterior consulta.

Contenido del capítulo

Beneficios de la consola web

La consola Web es la herramienta principal del administrador para la gestión de la seguridad. Al tratarse de un servicio Web, hereda una serie de características que influirán de manera positiva en la forma de trabajo del departamento de IT.

Única herramienta para la gestión completa de la seguridad

El administrador podrá distribuir de forma centralizada el paquete de instalación Panda Endpoint Protection en los equipos de la red, establecer las configuraciones de seguridad, monitorizar el estado de la protección de los equipos y disponer de herramientas de resolución en caso de incidentes de seguridad. Toda la funcionalidad se ofrece desde una única consola Web, favoreciendo la integración de las distintas herramientas y minimizando la complejidad de utilizar varios productos de distintos proveedores.

Gestión centralizada de la seguridad para oficinas remotas y usuarios desplazados

La consola Web está alojada en la nube, por lo que no son necesarias configuraciones de VPN ni redirecciones de puertos en los routers corporativos para su acceso desde el exterior de la oficina. Tampoco son necesarias inversiones en infraestructuras IT, tales como servidores, licencias de sistemas operativos o bases de datos, ni es necesaria una gestión del mantenimiento / garantía para asegurar el funcionamiento del servicio.

Gestión de la seguridad desde cualquier lugar y en cualquier momento

La consola Web es de tipo "responsive / adaptable" con lo que se ajusta al tamaño del dispositivo utilizado por el administrador. De esta manera se puede gestionar la seguridad desde cualquier lugar y en cualquier momento, mediante un smartphone, un notebook o un PC de escritorio.

Acceso a la consola web y requisitos

Requisitos para acceder a la consola web

- Credenciales válidas (cuenta de usuario y contraseña) y un segundo factor de autenticación (opcional). Consulta **Acceso, control y supervisión de la consola de administración** en la página **53**.
- Última versión de un navegador web certificado:

  - Google Chrome
  - Microsoft Edge
  - Firefox
  - Opera
- Conexión a Internet y comunicación por el puerto 443.

Acceso la consola web

Si tu proveedor de seguridad es Panda Security:

- Abre un navegador compatible y accede a la URL **https://www.pandacloudsecurity.com/PandaLogin/**
- Escribe las credenciales de tu cuenta de usuario.
- Si tu cuenta de usuario tiene acceso a varias cuentas de cliente distintas, se abrirá la ventana **Selecciona la cuenta**. Elige el cliente que tiene asociada la consola a la que deseas acceder.
- Se abrirá la consola de Panda Endpoint Protection mostrando el panel de control **Seguridad**.

Si tu proveedor de seguridad es WatchGuard, para acceder a la consola Web de Panda Endpoint Protection:

- Accede a la URL **https://www.watchguard.com/** y haz clic en el botón **Log in** situado en la esquina superior derecha de la pantalla.
- Escribe tus credenciales de WatchGuard. Se mostrará la ventana **Support Center**.
- Haz clic en el menú superior **MY WATCHGUARD**. Se abrirá un menú desplegable.
- Haz clic en la opción **Manage Panda Products**. Se abrirá la ventana Panda Cloud con todos los servicios contratados.
- Haz clic en el panel asociado a Panda Endpoint Protection. Se abrirá la consola de administración mostrando el panel de control **Seguridad**.

Estructura general de la consola web

La consola web cuenta con recursos que facilitan una experiencia de gestión homogénea y coherente para administrar la seguridad de la red.

El objetivo de la consola web es entregar al administrador una herramienta sencilla, pero a la vez flexible y potente, que le permita comenzar a gestionar la seguridad de la red de forma productiva en el menor período de tiempo posible.

A continuación, se incluye una descripción de los elementos de la consola y su modo de uso.

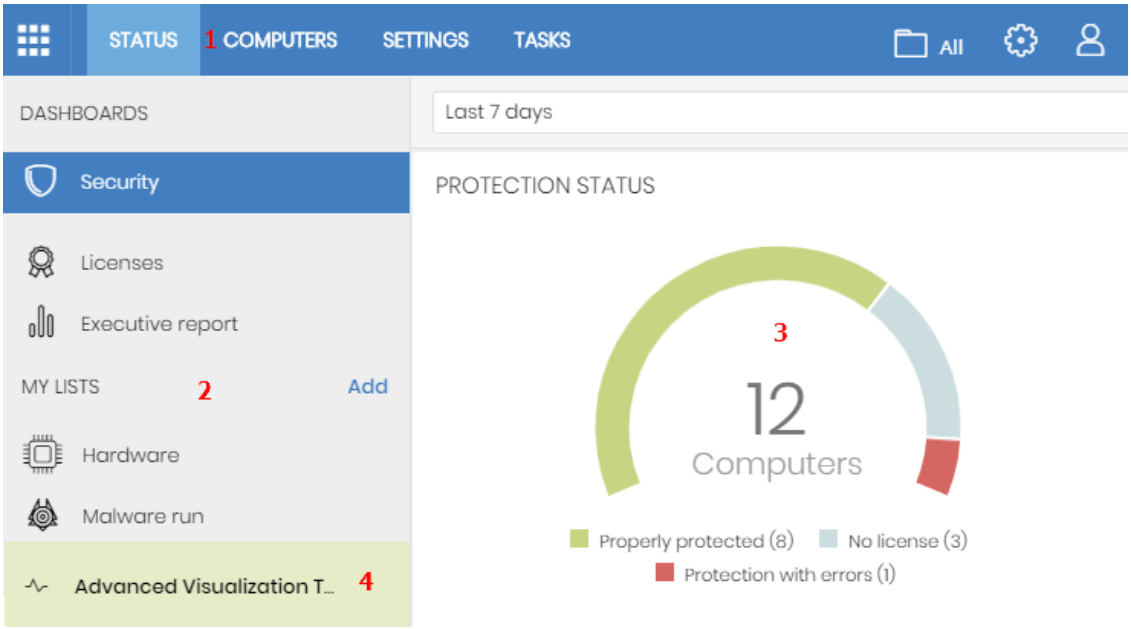


Figura 3.1: Vista general de la consola de administración Panda Endpoint Protection

Menú superior (1)

La consola distribuye toda su funcionalidad en varias zonas accesibles desde el menú superior:

- Botón Panda Cloud
- Estado
- Equipos
- Configuración
- Tareas
- Filtro por grupo
- Notificaciones web
- Configuración general
- Cuenta de usuario

Botón Panda Cloud

Haz clic en el botón situado en el lateral izquierdo del menú superior para elegir el producto de seguridad contratado y gestionarlo o modificar la configuración de tu cuenta de usuario.

Menú superior Estado

Muestra el panel de control de la consola desde la cual el administrador tiene acceso de un vistazo a toda la información de seguridad, ya sea de forma gráfica mediante widgets como por los

listados situados en el menú lateral. Consulta **Esquema general de la zona Estado** para más información.

Menú superior Equipos

Ofrece las herramientas básicas para definir la estructura de los equipos de la red que mejor se ajuste a la configuración de seguridad diseñada para el parque informático. Elegir una correcta estructura de dispositivos es fundamental a la hora de asignar configuraciones de seguridad. Consulta **La zona equipos** en la página **210** para más información.

Menú superior Configuración

Permite al administrador de la red definir el comportamiento de Panda Endpoint Protection en los equipos de usurario y servidores donde se encuentra instalado. La asignación de la configuración se establece de forma global para todos los equipos de la red, o únicamente para algunos equipos concretos mediante plantillas, dependiendo del tipo de configuración a establecer. Estas plantillas de configuración se pueden asignar a uno o más equipos de la red que tengan requerimientos de seguridad similares, permitiendo minimizar el tiempo del administrador dedicado a gestionar la seguridad de su red de equipos.

*Consulta **Gestión de configuraciones** en la página **279** para obtener información detallada sobre cómo crear una configuración en Panda Endpoint Protection.*

Menú superior Tareas

Permite la gestión de tareas de seguridad programadas para su ejecución en los intervalos de tiempo designados por el administrador. Consulta **Tareas** en la página **603**.

Icono Filtro por grupo

Limita la información generada mostrada en la consola por los equipos que pertenezcan al grupo o grupos elegidos. Consulta **Filtrar resultados por grupos** en la página **226** para más información.

Icono Notificaciones web

Al hacer clic en el icono se muestra un desplegable con las comunicaciones de carácter general que Panda Security pone en conocimiento para todos los usuarios de la consola, y ordenadas según su importancia:

- Paradas programadas de mantenimiento
- Avisos de vulnerabilidades críticas
- Consejos de seguridad

- Mensajes para iniciar el proceso de actualización de la consola. Consulta **Actualización de la consola de administración** en la página **206**.

Cada comunicación tiene asociada un nivel de prioridad:

- Importante
- Aviso
- Informativa

El número del icono indica la cantidad de notificaciones web nuevas (que quedan por leer).

Para eliminar una notificación web, haz clic en su icono de aspa asociado. Las notificaciones así eliminadas no se volverán a mostrar, y el icono ajustará su número al total de notificaciones web que se muestran.

Icono Configuración General

Muestra un menú desplegable que permite el acceso a la documentación del producto, cambio de idioma de la consola y otras herramientas.

Entrada	Descripción
Ayuda online	Acceso a las ayudas web del producto.
Guía de administración de Panda Endpoint Protection	Acceso a la Guía de administración del producto Panda Endpoint Protection.
Soporte técnico	Carga la dirección web correspondiente al soporte técnico de Panda Endpoint Protection.
Buzón de sugerencias	Lanza la herramienta de correo local instalada en equipo para enviar un mensaje de correo al departamento de soporte técnico de Panda Security.
Acuerdo de licencia	Muestra el EULA (End User License Agreement).
Acuerdo sobre tratamiento de datos	Muestra el acuerdo de protección de datos de la plataforma según la normativa europea.
Novedades de Panda	Enlace a la página web de soporte que muestra los cambios y

Entrada	Descripción
Endpoint Protection	nuevas funcionalidades incluidas en la versión.
Idioma	Permite seleccionar el idioma en que se mostrará la consola de administración.
Acerca de…	Muestra la versión de los diferentes elementos de Panda Endpoint Protection. • **Versión**: versión del producto. • **Versión de la protección**: versión interna del módulo de protección instalado en los equipos. • **Versión del agente**: versión interna del módulo de comunicaciones instalado en los equipos.

Tabla 3.1: Menú Configuración general

Icono Cuenta de usuario

Muestra un menú desplegable con las siguientes entradas de configuración:

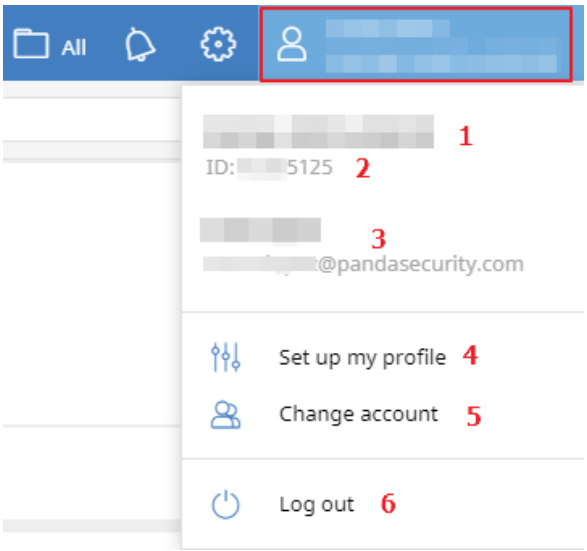


Figura 3.2: Menú desplegable Cuenta de usuario

Entrada	Descripción
Nombre del cliente (1)	Nombre y apellidos de la cuenta de usuario con la que se ha accedido a la consola.

Entrada	Descripción
Id de cliente (2)	El identificador de cliente es un número que Panda asigna a la cuenta de cliente para identificarlo. El departamento de Soporte de Panda Security puede requerirlo en sus comunicaciones con el cliente.
Dirección de correo (3)	Dirección de correo utilizada para acceder a la consola de administración.
Configurar mi perfil (4)	Modifica la información de la cuenta de usuario. Consulta **Cambiar los datos personales de una cuenta de usuario** en la página **60**.
Cambiar de cuenta (5)	Muestra las cuentas de cliente accesibles desde la cuenta de usuario que inició la sesión, y permite seleccionar una cuenta de cliente diferente para operar con la consola asociada al producto.
Cerrar sesión (6)	Termina la sesión en la consola.

Tabla 3.2: Menú Cuenta de usuario

Menú lateral (2)

Muestra las diferentes subzonas dentro de la zona seleccionada, actuando como un selector de segundo nivel con respecto al menú superior.

El menú lateral varía en función de la zona presentada, adaptándose al tipo de información que se muestra.

Para maximizar el espacio de visualización del panel central reduce el tamaño del menú lateral haciendo clic en la barra de separación del panel. Si se reduce por debajo del tamaño de los nombres de las opciones, el menú lateral se contraerá completamente. Para volver expandirlo a su tamaño original haz clic en el icono .

Panel central (3)

Recoge toda la información relevante de la zona y subzona elegidas por el administrador. **Vista general de la consola de administración Panda Endpoint Protection** muestra la zona **Estado** subzona **Seguridad**, formada por los widgets que permiten interpretar la información de seguridad recogida. Para obtener más detalle acerca de los widgets consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.

Elementos básicos de la consola web

Menú de pestañas superior

En las zonas de la consola más complejas se muestra un selector de tercer nivel en forma de pestañas que mantiene la información ordenada por categorías.

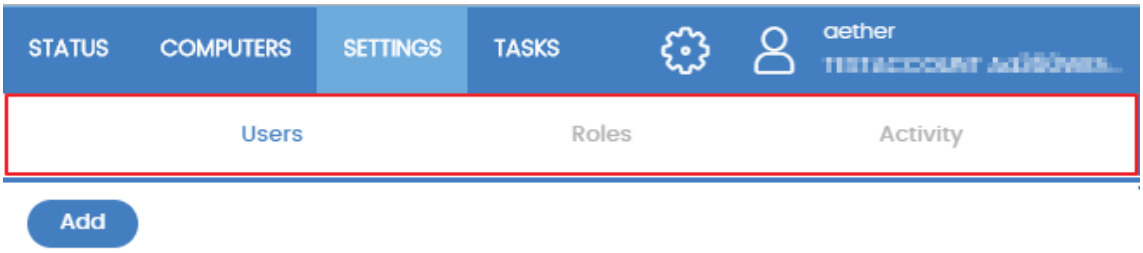


Figura 3.3: Menú de pestaña

Barra de acciones

Figura 3.4: Barra de acciones

Para facilitar la navegación de la consola y el acceso a algunas operaciones comunes sobre los puestos de usuario y servidores administrados, se incorpora una barra de acciones en la parte superior de la pantalla. El número de botones mostrados se adapta al tamaño de la ventana. Los botones que quedan fuera se añaden al icono ▪▪▪ situado a la derecha de la barra de acciones.

En la esquina derecha de la barra de acciones se muestra el número total de equipos seleccionados. Haz clic en el icono del aspa para deshacer la selección.

Herramientas de filtrado y búsqueda

Las herramientas de filtrado y búsqueda muestran los subconjuntos de información de interés para el administrador. Algunas herramientas de filtrado son generales y aplican a toda la zona de la consola mostrada, como por ejemplo en el menú superior **Estado** o menú superior **Equipos**.

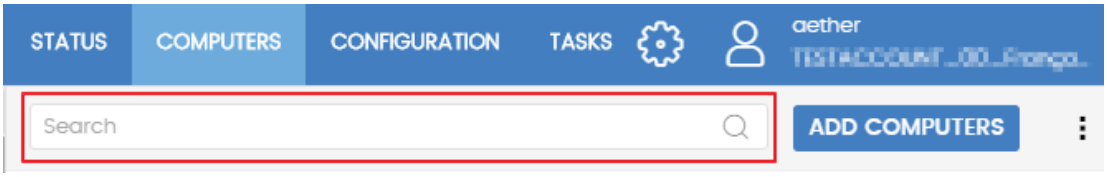


Figura 3.5: Herramienta de búsqueda

Parte de las herramientas de filtrado se ocultan por defecto bajo el desplegable **Filtros**, y permiten definir búsquedas por categorías, rangos y otros parámetros dependientes del tipo de información mostrada.

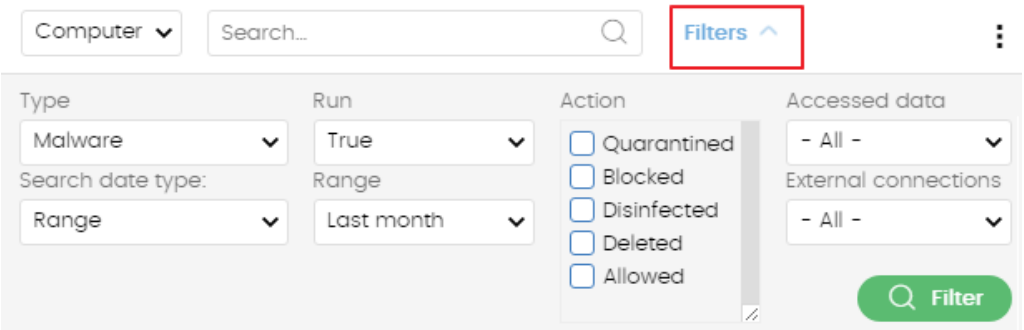


Figura 3.6: Sistema de filtrado de información en listados

Elementos de configuración

La consola web Panda Endpoint Protection utiliza controles estándar para introducir configuraciones, como son:

- Botones. **(1)**
- Links. **(2)**
- Casillas de activación y desactivación. **(3)**
- Desplegables de selección. **(4)**
- Combos de selección. **(5)**
- Cuadros de texto. **(6)**

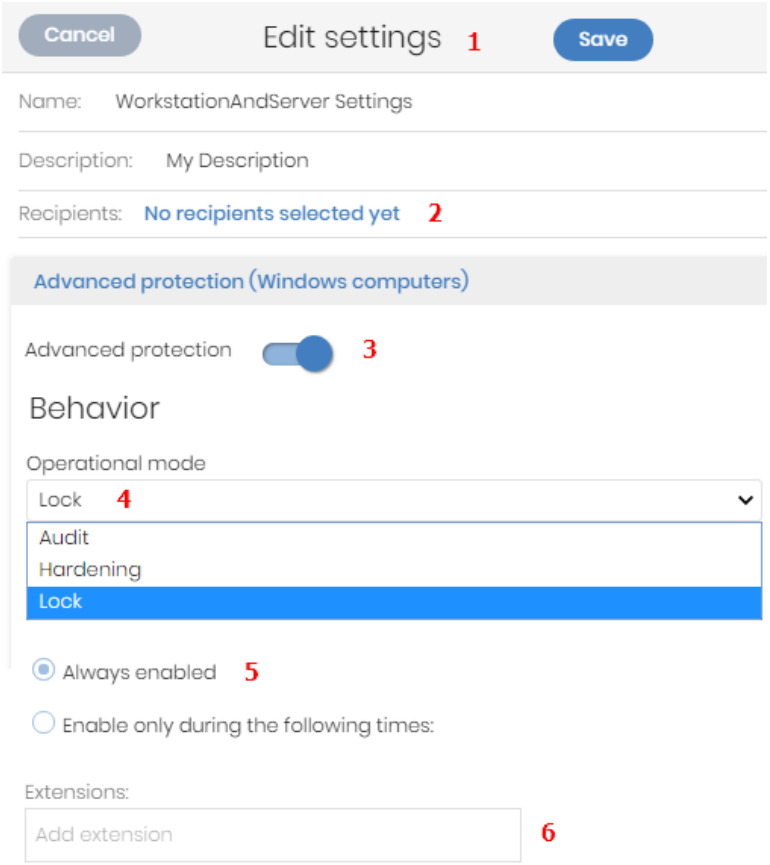


Figura 3.7: Controles para el manejo de la consola de administración

Botón de ordenación

En algunos listados de elementos, como por ejemplo en la zona **Tareas** (menú superior **Tareas**) o en la zona **Configuración** (menú superior **Configuración**) se muestra el botón en la esquina superior derecha o en algunos casos en la esquina inferior derecha. Este botón permite establecer el criterio de ordenación del listado:

- **Ordenado por fecha de creación** los elementos se ordenan según su fecha de incorporación al listado.
- **Ordenado por nombre** los elementos se ordenan por su nombre.
- **Ascendente**
- **Descendente**

Menús de contexto

Son menús desplegables que se muestran al hacer clic en el icono , con opciones que afectan al ámbito al que pertenecen según su posición.

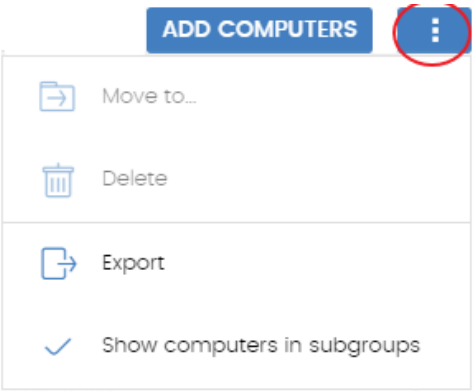


Figura 3.8: Menús de contexto

Copiar, pegar y borrar contenidos

Al pasar el puntero del ratón por las cajas de texto que admiten múltiples valores separados por espacios, se muestran dos botones flotantes para copiar y borrar su contenido.

- **Botón de copiar (1)**: copia al portapapeles el contenido de los elementos que contiene la caja de texto separando cada uno de ellos con un retorno de carro. La consola muestra un mensaje cuando la operación se completa.
- **Botón de borrar (2)**: limpia el contenido de la caja de texto.

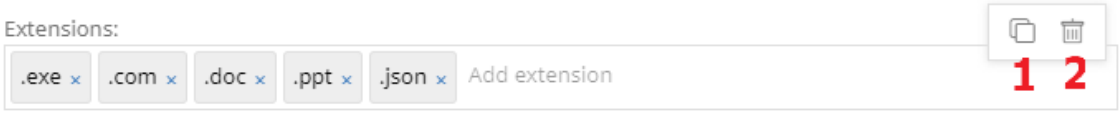


Figura 3.9: Botones Copiar y Borrar

- Al pulsar Control+v sobre una caja de texto se vuelca el contenido del portapapeles, siempre que éste contenga lineas de texto separadas por retornos de carro.

Esquema general de la zona Estado

El menú **Estado** reúne las principales herramientas de visibilidad, y está distribuido en varias secciones:

Acceso al panel de control (1)

El acceso al panel de control se realiza mediante el menú superior **Estado**. Desde aquí se acceden a los diferentes widgets, así como a los listados.

Los widgets o paneles gráficos representan aspectos concretos del parque de equipos gestionado, dejando a los listados la entrega de datos más detallados.

Selector del intervalo de tiempo (2)

El panel de control muestra la información relevante en el intervalo de tiempo fijado por el administrador mediante la herramienta situada en la parte superior de la ventana **Estado**. Los

intervalos disponibles son:

- Últimas 24 h.
- Últimos 7 días.
- Último mes.
- Último año.

No todos los paneles soportan el filtrado de datos por el último año. Los paneles que no soporten este intervalo de tiempo mostrarán una leyenda en la parte superior indicándolo.

Selector de panel (3)

- **Seguridad**: estado de la seguridad del parque informático. Para más información sobre los widgets incluidos consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.
- **Patch Management**: actualización del sistema operativo y del software instalado en los equipos. Para más información sobre los widgets incluidos consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.
- **Panda Full Encryption**: estado del cifrado de los dispositivos de almacenamiento internos en los equipos. Para más información sobre los widgets incluidos consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.
- **Licencias**: estado de las licencias de Panda Endpoint Protection asignadas a los equipos de la red. Consulta **Licencias** en la página **185** para obtener más información acerca de la gestión de licencias.
- **Informes programados**: consulta **Envío programado de informes y listados** en la página **577** para obtener más información acerca de la configuración y generación de informes.

Mis listados (4)

Son tablas de datos con la información presentada en los paneles. Esta información se presenta con gran nivel de detalle e implementa herramientas de búsqueda y distribución que ayudan a localizar los datos requeridos.

Paneles informativos / Widgets (5)

Está formado por widgets o paneles informativos centrados en un único aspecto de la seguridad de la red.

Los paneles se generan en tiempo real y son interactivos: pasando el ratón por encima de los elementos se muestran tooltips con información extendida.

Todas las gráficas incluyen una leyenda que permite determinar el significado de cada serie representada, e incorporan zonas activas que al ser seleccionadas abren distintos listados asociados al widget con filtros predefinidos.

Panda Endpoint Protection utiliza varios tipos de gráficas para mostrar la información de la forma más conveniente según el tipo de dato representado:

- Gráficos de tarta.
- Histogramas.
- Gráficas de líneas.

Gestión de listados

Panda Endpoint Protection estructura la información recogida en dos niveles: un primer nivel que representa de forma gráfica los datos mediante paneles o widgets y un segundo nivel más detallado, donde la información se representa mediante listados compuestos por tablas. La mayor parte de los paneles tienen un listado asociado para que el administrador pueda acceder de forma rápida a un resumen gráfico de la información y después profundizar mediante los listados en caso de requerir mayor nivel de detalle.

Panda Endpoint Protection soporta el envío programado de listados por correo electrónico. De esta forma, el administrador no necesita acceder a la consola Web para conocer el detalle de los eventos que se producen en la red. Además, esta funcionalidad facilita la compartición de información entre departamentos y permite habilitar la construcción de un repositorio externo con el histórico de todos los eventos que se han producido, mas allá de los límites de la consola Web. Con este repositorio, el equipo directivo podrá realizar un seguimiento de la información generada libre de interferencias de terceros.

Plantillas, configuraciones y vistas

Un listado es la suma de dos elementos: una plantilla y una configuración de un filtro.

Una plantilla representa una fuente de datos sobre un apartado específico tratado por Panda Endpoint Protection.

Un filtro es una configuración específica de las herramientas de filtrado asociadas a cada plantilla.

Un filtro aplicado sobre una plantilla da como resultado una "vista de listado", también llamado simplemente "listado". El administrador puede crear y almacenar nuevos listados modificando los filtros asociados a una plantilla para su consulta posterior. De esta forma se evita reconfigurar los filtros de las plantillas más frecuentemente utilizadas, lo que lleva a un ahorro del tiempo de administración.

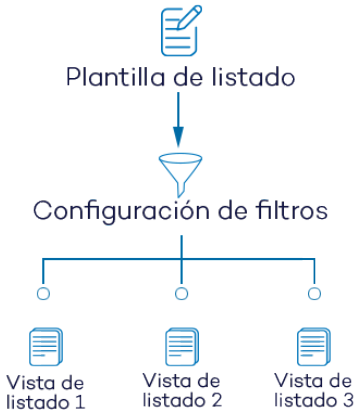


Figura 3.10: Generación de tres listados a partir de una misma plantilla / fuente de datos

Plantillas de listado

En el menú superior **Estado**, panel lateral **Mis listados** se encuentra el enlace **Añadir** que muestra una ventana con las plantillas disponibles agrupadas por su tipo:

Grupo	Listado	Descripción
General	Licencias	Muestra en detalle el estado de las licencias de los equipos de la red. Consulta **Listados del módulo Licencias** en la página **192** para más información.
	Equipos no administrados descubiertos	Muestra los equipos Windows de la red que no tienen el software Panda Endpoint Protection instalado. Consulta **Listado Equipos no administrados descubiertos** en la página **118** para más información.
	Equipos con nombre duplicado	Muestra los equipos con el mismo nombre y pertenecen al mismo dominio. Consulta **Equipos con nombre duplicado** en la página **247** para más información
	Software	Muestra el software instalado en los equipos del parque informático. Consulta **Software** en la página **244** para más información.

Grupo	Listado	Descripción
	Hardware	Muestra el hardware instalado en los equipos del parque informático. Consulta **Hardware** en la página **241** para más información.
Seguridad	Estado de protección de los equipos	Muestra en detalle el estado del módulo de la protección instalada en los equipos. Consulta **Estado de protección de los equipos** en la página **479** para más información.
	Amenazas detectadas por el antivirus	Ofrece información consolidada y completa de todas las detecciones realizadas en todas las plataformas soportadas y desde todos los vectores de infección analizados. Consulta **Amenazas detectadas por el antivirus** en la página **486** para más información.
	Intentos de intrusión bloqueados	Muestra los ataques de red bloqueados por el cortafuegos del equipo. Consulta **Intentos de intrusión bloqueados** en la página **497** para más información.
	Dispositivos bloqueados	Muestra en detalle todos los equipos de la red que tienen establecida alguna limitación en el acceso a sus periféricos. Consulta **Dispositivos bloqueados** en la página **492** para más información.
	Conexiones bloqueadas	Muestra las conexiones que fueron bloqueadas por el cortafuegos local. Consulta **Intentos de intrusión bloqueados** en la página **497** para más información.
Patch Management	Estado de gestión de parches	Muestra en detalle todos los equipos de la red compatibles con Panda Patch Management Consulta **Estado de gestión de parches** en la página **390** para más información.

Grupo	Listado	Descripción
	Parches disponibles	Muestra el detalle de todos los parches sin instalar en los equipos de la red y publicados por Panda Security. Consulta **Parches disponibles** en la página **378** para más información.
	Historial de instalaciones	Muestra los parches que Panda Endpoint Protection intentó instalar y los equipos que los recibieron en un intervalo determinado. Consulta **Historial de instalaciones** en la página **412** para más información.
	Programas "End of Life"	Muestra la información relativa al "end of life" de los programas instalados en los equipos de la red, agrupados según el plazo restante. Consulta **Programas "End of Life"** en la página **420** para más información.
	Parches excluidos	Muestra los pares equipo - parche que son excluidos de su instalación. Consulta **Parches excluidos** en la página **423** para más información.
Protección de datos	Estado del cifrado	Muestra toda la información referente a los equipos de la red compatibles con la funcionalidad de cifrado. Consulta **Estado del cifrado** en la página **458**para más información.

Tabla 3.3: Listado de plantillas disponibles en Panda Endpoint Protection

Adicionalmente, existen otras plantillas accesibles directamente desde el menú de contexto de ciertos listados o desde algunos widgets del panel de control. Consulta el capítulo correspondiente al widget en cuestión.

Secciones de los listados

Los listados incorporan un conjunto de herramientas comunes que facilitan su interpretación. A continuación se muestran las partes principales de un listado de ejemplo.

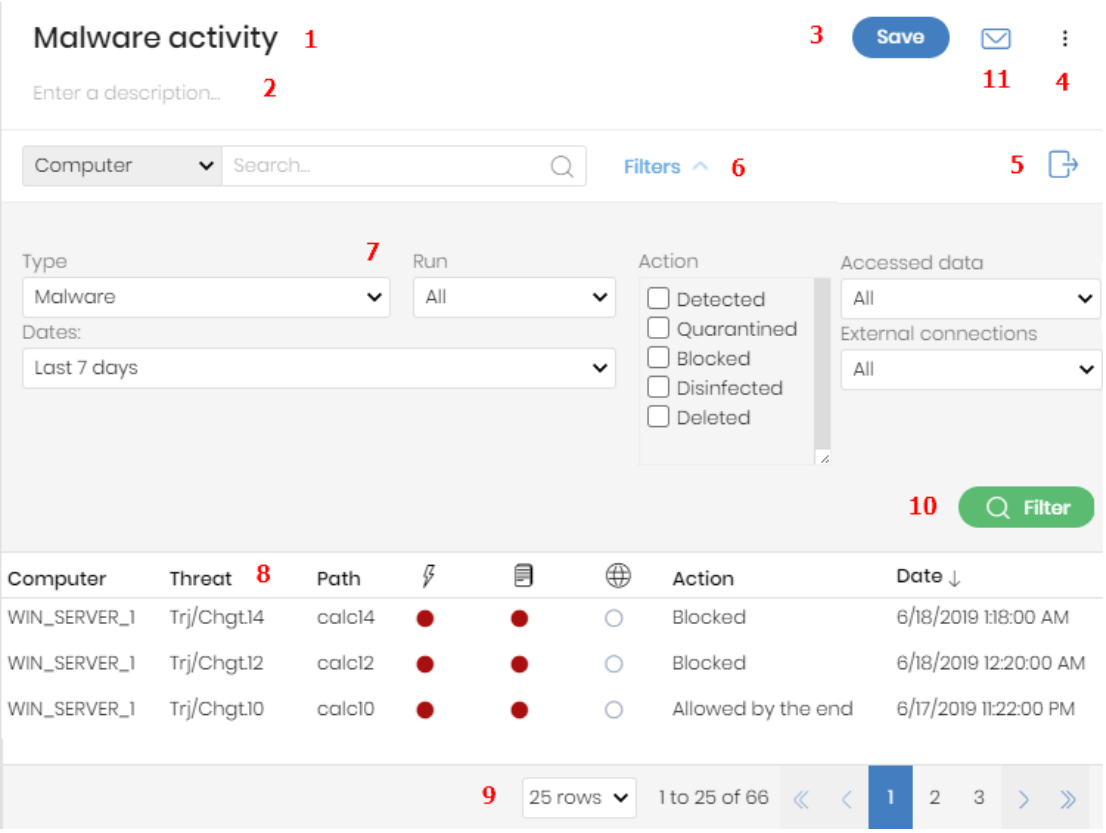


Figura 3.11: Elementos de las pantallas de listados

- **Nombre del listado (1)**: identifica el tipo de datos que se muestran en el listado.
- **Descripción (2)**: caja de texto libre donde el administrador puede indicar el objetivo del listado.
- **Salvar (3)**: botón que salva la vista actual y crea un nuevo listado en el árbol Mis listados
- **Menú de contexto (4)**: menú desplegable con las operaciones disponibles sobre el listado (copiar y eliminar. Consulta **Operaciones con listados** para más información.
- **Menú de contexto (5)**: menú desplegable con las opciones de exportación del listado.
- **Enlace de herramientas de filtrado y búsqueda (6)**: al hacer clic se despliega un panel con las herramientas de filtrado. Una vez configuradas haz clic en el botón **Filtrar (10)**.
- **Bloque de controles de filtrado y búsqueda (7)**: filtra los datos mostrados en el listado.
- **Criterio de ordenación (8)**: al hacer clic en el nombre de las columnas el listado se ordena tomando como referente esa columna. Haz clic varias veces en el nombre de la columna para cambiar el sentido de la ordenación (ascendente o descendente). El sentido de ordenación se muestra mediante una fecha ascendente ↑ o descendente ↓. Si accedes a la consola de administración desde un dispositivo móvil de menor tamaño, haz clic en el icono  situado en la esquina inferior derecha para desplegar un menú con el nombre

de las columnas.

- **Paginación (9)**: en el pie de la página se incluyen una serie de controles para navegar la información mostrada.

Icono	Descripción
25 rows	Selector del número de filas mostradas por página.
1 to 25 of 67	Intervalo de registros mostrados del total disponible.
«	Retroceso a la primera página.
‹	Retroceso a la página anterior a la actual.
1 2 3	Acceso directo por número de páginas.
›	Avance a la siguiente página.
»	Avance a la última página.

Tabla 3.4: Herramientas de paginación

- **Envío programado del listado (11)**: Panda Endpoint Protection permite el envío de correos electrónicos con el contenido del listado, adjuntando una exportación de los datos en formato csv. Consulta **Envío programado de informes y listados** en la página **577** para obtener más información.

Operaciones con listados

En el menú superior **Estado**, panel lateral **Mis listados** se muestran todos los listados que el administrador a creado previamente y los listados que Panda Endpoint Protection incorpora por defecto. Consulta **Listados incluidos por defecto**para más información.

Crear un listado personalizado

Hay varias formas de añadir un nuevo listado personalizado / vista:

- **Desde el panel lateral Mis listados**
    - Al hacer clic sobre el link **Añadir** del panel **Mis listados** se muestra una ventana con un desplegable que contiene las plantillas disponibles.

- Elige una plantilla, configura las herramientas de filtrado, modifica el nombre y la descripción y pulsa el botón **Guardar (3)**.

- **Desde un panel del dashboard**
  - Haz clic en un widget en el panel de control para abrir su plantilla asociada.
  - Haz clic en el menú de contexto **(4)** y selecciona **Copiar**. Se creará un nuevo listado.
  - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.

- **Desde un listado ya creado**
  - Haz una copia de un listado ya generado mediante el menú contextual **(4)** y haz clic en **Copiar**. Se generará un nuevo listado con el nombre "copia de...".
  - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.

- **Desde el menú de contexto del panel Mis listados**
  - Haz clic en el menú de contexto asociado al listado a copiar.
  - Haz clic en **Hacer una copia**. Se creará una nueva vista de la plantilla con el nombre "copia de...".

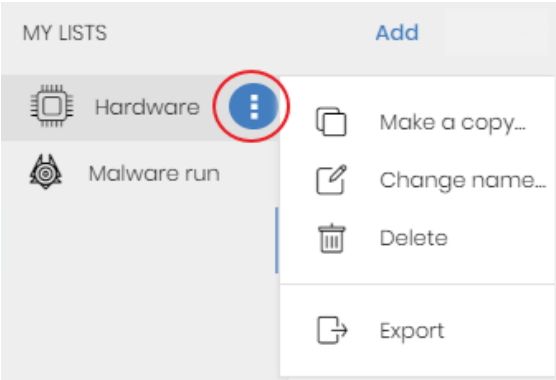


Figura 3.12: Menú de contexto de los listados accesibles desde el Panel de listados

Borrar un listado

Puedes borrar un listado de varias maneras:

- **Desde el panel Mis listados**
  - Haz clic el menú de contexto asociado al nombre del listado en el panel **Mis Listados**.
  - Haz clic en el icono .

- **Desde el propio listado**
  - Haz clic en el menú de contexto **(4)**.
  - Haz clic en el icono del menú desplegable.

Copiar un listado

Puedes copiar un listado de varias maneras:

- Desde el panel **Mis listados:**
  - Haz clic en el menú de contexto asociado al nombre del listado en el panel **Mis listados**.
  - Haz clic en el icono .
- **Desde el propio listado:**
  - Haz clic en el menú de contexto **(4)**.
  - Haz clic en el icono del menú desplegado.

Exportar un listado

Exporta un listado en formato csv para ampliar la información que se muestra en los listados de la consola Web. Los campos del fichero exportado están documentados en el capitulo correspondiente de esta Guía de administración. Puedes exportar un listado de varias maneras:

- Desde el panel **Mis listados**:
  - Si el listado no soporta la exportación del detalle haz clic en el icono . Se descargará un fichero .csv con los datos del listado.
  - Si el listado sí soporta la exportación del detalle haz clic en el icono **(5)**. Se mostrará un menú desplegable.
  - Haz clic en **Exportar**. Se descargará un fichero .csv con los datos del listado.
- **Desde el propio listado:**
  - Haz clic en el menú de contexto **(4)**.
  - Haz clic en el icono **Exportar** del menú desplegado. Se descargará un fichero .csv con los datos del listado.

Según el módulo o funcionalidad de que se trate, algunos listados pueden ofrecer un nivel mayor de detalle en los datos del fichero exportado.

Exportar los detalles de un listado

Exporta los detalles de un listado para ampliar la información mostrada en la exportación csv. Los campos del fichero exportado están documentados en el capitulo correspondiente de esta Guía de administración. Puedes exportar un listado de varias maneras:

- **Desde el panel :**
  - Haz clic en el icono **(5)**. Se mostrará un menú desplegable.
  - Haz clic en **Exportación detallada**. Se descargará un fichero .csv con el detalle del listado.
- **Desde el propio listado:**
  - Haz clic en el menú de contexto **(4)**. Se mostrará un menú desplegable.
  - Haz clic en el icono **Exportación detallada** del menú desplegado. Se descargará un fichero .csv con el detalle del listado.

Según el módulo o funcionalidad de que se trate, algunos listados pueden ofrecer un nivel mayor de detalle en el fichero exportado.

Personalizar un listado

- Asigna un nuevo nombre al listado **(1)**. Por defecto la consola forma un nuevo nombre para el listado añadiendo la cadena "Nuevo" al tipo de listado o "Copia" si el listado es la copia de uno anterior.
- Asigna una descripción **(2)**: este paso es opcional.
- Haz clic en el enlace **Filtros (6)** para desplegar las herramientas de búsqueda y filtrado.
- Haz clic en **Filtrar (10)** para aplicar el filtro configurado con el objetivo de comprobar si el filtrado configurado se ajusta a las necesidades. En el cuerpo del listado se mostrará la búsqueda resultado.
- Haz clic en el botón **Guardar (3)**. El listado se añadirá en el panel de la izquierda bajo **Mis listados**, y será accesible a partir de ese momento haciendo clic en su nombre.

Programar el envío de un listado

- **Desde el menú de contexto del panel Listados**:
  - Haz clic en el menú de contexto del listado que quieres enviar y elige la opción **Programar envío**.

- Se mostrará una ventana con la información necesaria para enviar de forma automática la información.

- **Desde el propio listado:**
  - Haz clic en el icono **(11)**. Se mostrará una ventana con la información necesaria para enviar de forma automática la información.

*Consulta **Envío programado de informes y listados** en la página **577** para obtener más información*

Acciones sobre equipos en los listados

En algunos listados se incorporan casillas de selección por cada equipo. Al marcar uno o más equipos, se muestra la barra de acciones en la parte superior de la ventana, para facilitar la administración de los puestos de usuario y servidores seleccionados. Consulta **Barra de acciones (8)** en la página **277**.

En cada página de los listados se muestra información sobre 25 equipos. Para operar sobre todos los equipos de una página, selecciona la casilla situada en la esquina superior izquierda del listado **(1)**:

En el caso de los listados **Equipos** y **Equipos no administrados descubiertos**, una vez seleccionada la casilla se puede operar sobre todos los equipos de todas las páginas del listado **(2)**.

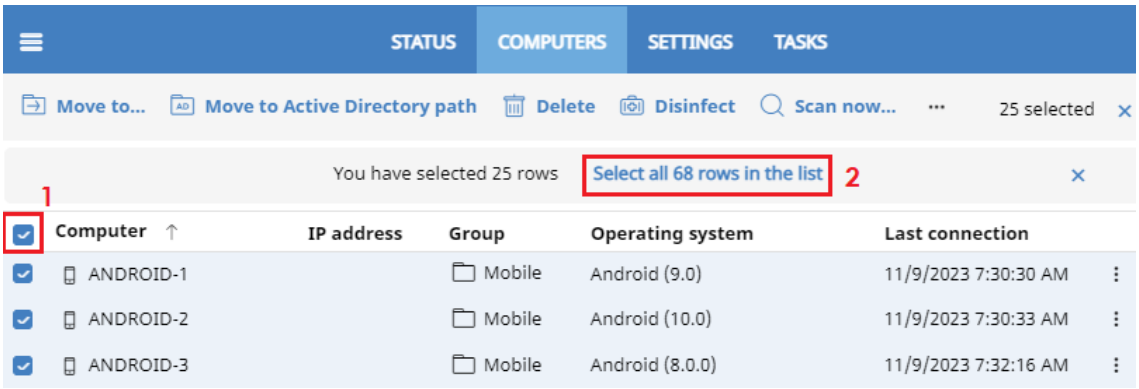


Figura 3.13: Selección de equipos en los listados

Listados incluidos por defecto

La consola de administración incluye varios listados pre generados:

- Estaciones y portátiles desprotegidos.
- Servidores desprotegidos.
- Hardware
- Software

Estaciones y portátiles desprotegidos

Localiza todos los equipos de escritorio y portátiles, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Equipos en proceso de instalación del software Panda Endpoint Protection o con error en la instalación.
- Equipos con la protección desactivada o en estado de error.
- Equipos sin licencia asignada o con licencia caducada.
- Consulta **Estado de protección de los equipos** en la página **479** para más información.

Servidores desprotegidos

Localiza todos los equipos de tipo servidor, sin importar el sistema operativo instalado, considerados vulnerables a las amenazas debido a un problema en el funcionamiento de la protección:

- Servidores en proceso de instalación del software Panda Endpoint Protection o con error en la instalación.
- Servidores con la protección desactivada o en estado de error.
- Servidores sin licencia asignada o con licencia caducada. Consulta **Estado de protección de los equipos** en la página **479** para más información.

Software

Muestra una relación de los programas instalados en el parque informático. Consulta **Software** en la página **244** para más información.

Hardware

Muestra una relación de los componentes hardware instalados en el parque informático. Consulta **Hardware** en la página **241** para más información.

Capítulo 4

Acceso, control y supervisión de la consola de administración

Panda Endpoint Protection implementa varios recursos diseñados para limitar, controlar y supervisar el acceso a su consola web de gestión, y las acciones que el administrador de la red tiene permitido ejecutar en ésta:

- Cuenta de usuario.
- Roles asignados a las cuentas de usuario.
- Registro de la actividad de las cuentas de usuario.

Contenido del capítulo

Conceptos generales

Cuenta de usuario

Es un recurso formado por un conjunto de datos que Panda Endpoint Protection utiliza para permitir el acceso de los administradores a la consola web, y establecer las acciones que éstos podrán realizar sobre los equipos de los usuarios.

Las cuentas de usuario son utilizadas únicamente por los administradores de IT que acceden a la consola web de Panda Endpoint Protection. Cada administrador puede tener una o más cuentas de usuario asignadas.

Las principales características de las cuentas de usuario son:

- Son cuentas gestionadas por el propio administrador, que puede crear o borrar cuentas nuevas, cambiar su contraseña, añadir o quitar permisos o activar la verificación en dos pasos.
- Una cuenta de usuario permite acceder a todos los productos contratados con Panda Security a través de Panda Cloud
- Una cuenta de usuario puede tener acceso a distintos clientes. El administrador podrá elegir el producto al que desea acceder en Panda Cloud, y después seleccionar la consola a la que desee acceder en la ventana **Selecciona cuenta**.

Panda Cloud

Es el portal que centraliza el acceso a todos los productos del portfolio de Panda Security. Una cuenta de usuario creada en un producto de Panda Security da acceso a este portal, desde donde el administrador puede acceder a la distintas consolas de los productos contratados.

Para más información, consulta ***https://documents.managedprotection.pandasecurity.com/Help/PandaCloud/es-es/#t=001.htm***.

Cuenta de cliente

Es un recurso formado por datos confidenciales asociados a un cliente que tiene contratado algún producto con Panda Security. La dirección fiscal, el nombre completo, NIF y otros datos forman parte de la cuenta de cliente.

Gestión de cuentas de usuario

Una cuenta de usuario está formada por varias piezas de información que se generan en el momento de su creación:

- **Login de la cuenta**: identifica al usuario que accede a la consola.
- **Contraseña de la cuenta**: permite o impide el acceso a la consola de administración.
- **Rol asignado**: establece los equipos sobre los cuales la cuenta tiene capacidad de administración, y las acciones que puede ejecutar sobre ellos.

Diferencias entre clientes WatchGuard y Panda Security

Los clientes de Panda Security y los de WatchGuard siguen procedimientos distintos para crear o modificar sus cuentas de usuario. Los clientes de Panda Security gestionan las cuentas de usuario directamente desde la consola de Panda Endpoint Protection, mientras que los clientes de WatchGuard acceden a sus productos contratados y crean sus cuentas de usuario desde WatchGuard Portal.

Crear la primera cuenta de usuario para clientes de Panda Security

El procedimiento para crear la primera cuenta de usuario es distinto al utilizado para crear cuentas posteriores. La primera cuenta de usuario siempre tendrá asignado el rol Control total, que permite al administrador realizar cualquier operación en la consola. Esta cuenta no se puede borrar ni modificar.

Recibe el mensaje de correo de bienvenida

- Al adquirir Panda Endpoint Protection recibirás un mensaje de correo electrónico procedente de Panda Security.
- Haz clic en el enlace **Haz clic aquí** del mensaje para acceder a la web desde donde podrás crear la primera cuenta de usuario.

Completa el formulario Crea tu cuenta Panda

- Escribe tu dirección de email y haz clic en el botón **Crear**. Recibirás un nuevo mensaje de correo electrónico en la dirección especificada en el formulario para activar la cuenta creada.

Activa la cuenta de usuario

- Haz clic en el botón de activación del mensaje recibido para confirmar la dirección proporcionada al crear la cuenta de usuario. Si el botón no funciona, copia en el navegador el enlace que se muestra en el mensaje. Se abrirá la ventana **Panda Cuenta**.
- Escribe la contraseña de la cuenta de usuario creada. Se requieren al menos 8 caracteres, de los cuales al menos uno debe ser numérico y otro debe ser una letra.
- Elige el país y haz clic en el botón **Activar cuenta**. Se mostrará la ventana **Un segundo y terminamos**.
- Escribe tu nombre y apellidos, tu fecha de nacimiento, número de teléfono y dirección y haz clic en el botón **Guardar**, o salta este paso haciendo clic en el botón **Ahora no**. Se mostrará el acuerdo de licencia de Panda Cloud.
- Haz clic en el botón **Aceptar y continuar**. Se abrirá la ventana Panda Cloud, desde donde podrás acceder a todos los servicios contratados con Panda Security.

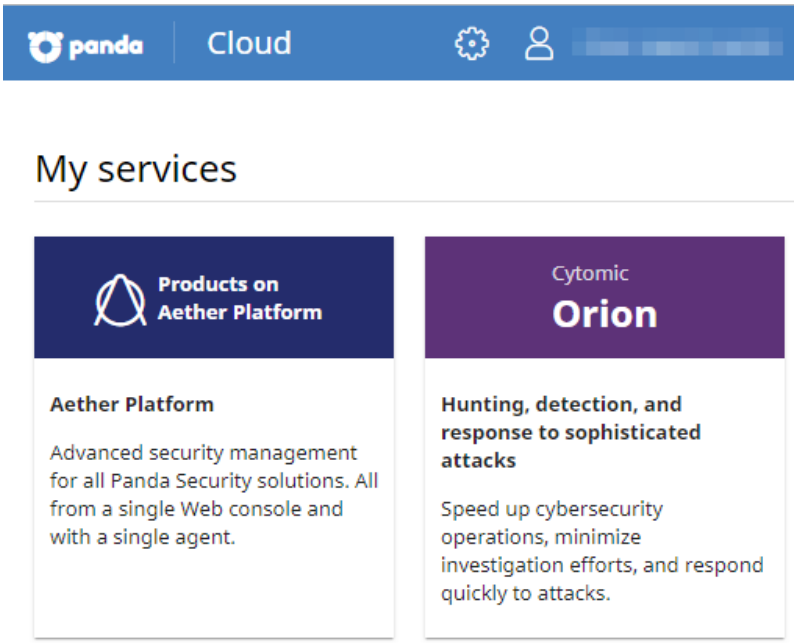


Figura 4.1: Ventana Panda Cloud

- Para acceder a la consola de Panda Endpoint Protection, haz clic en el panel Panda Endpoint Protection que encontrarás en **Mis servicios**. La primera vez que accedas se abrirá un asistente para aceptar los acuerdos de licencia y confidencialidad:

- Haz clic en el botón **Aceptar y continuar** de la ventana **Acuerdo de licencia**.
- Haz clic en el botón **Ir al acuerdo sobre tratamiento de datos** de la ventana **Acuerdo sobre tratamiento de datos**.
- Haz clic en el botón **Aceptar** de la ventana **Data Processing Agreement**. Se abrirá la consola Panda Endpoint Protection.

Crear la primera cuenta de usuario para clientes de WatchGuard

Los usuarios que pertenecen al proveedor de seguridad WatchGuard y todavía no tienen ningún producto contratado con Panda Security, crean una cuenta de cliente y una cuenta de usuario en Panda Security al activar por primera vez una licencia comercial de Panda Endpoint Protection.

Si ya tenías un producto Panda Endpoint Protection contratado y quieres acceder a la consola desde WatchGuard, consulta ***Acceder a la consola de Panda Endpoint Protection desde WatchGuard Portal con una cuenta ya existente***.

- Accede a WatchGuard Portal en **https://www.watchguard.com/** con la cuenta de usuario que accederá a la consola de Panda Endpoint Protection.
- Haz clic en la opción **Activate products** del menú superior **MY WATCHGUARD**. Se mostrará la ventana **Activate products**.
- Escribe la clave de licencia del producto Panda Security y haz clic en el botón **Continue**.
- Haz clic en **I need a Panda account**. Se mostrará una ventana con el identificador de la cuenta de cliente creada y su nombre. Guarda esta información para más adelante.
- Haz clic en **Submit** y **Continue**. Se mostrará el **Centro de Soporte de WatchGuard**.
- Si la página web lo solicita, escribe de nuevo la clave de licencia del producto Panda Security. Se mostrará el asistente **Activar producto.**
- Para aceptar las condiciones de uso de la licencia, haz clic en el botón **Siguiente**.
- En el desplegable **Select a license** selecciona la opción **New license** y haz clic en el botón **Next**.
- Introduce un nombre descriptivo que te permita identificar el producto en la web de WatchGuard y haz clic en el botón **Next**.
- Selecciona la casilla **I accept the enduser license agreement** y haz clic en **Next**. Se mostrará la página **Activación Completada** y las licencias se añadirán al mantenimiento correspondiente en Panda Endpoint Protection.

Una vez que el proceso ha terminado, la cuenta de usuario de WatchGuard podrá acceder a la consola Panda Endpoint Protection. Consulta **Acceso la consola web** en la página **31**.

Crear cuentas de usuario sucesivas desde la consola de Panda Endpoint Protection

Una vez creada la primera cuenta de usuario, el administrador tendrá acceso a la consola de administración de Panda Endpoint Protection, desde donde se pueden crear el resto de cuenta de usuario que necesite.

- Comprueba que el usuario tiene asignado el permiso **Gestionar usuarios y roles**. Consulta **Descripción de los permisos implementados**.
- En el menú superior **Configuración** haz clic en el menú lateral **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará el listado de usuarios creados en la consola de administración.
- Haz clic en el botón **Añadir**. Se abrirá la ventana **Añadir usuario**.
- Escribe la cuenta de correo del usuario de la consola en el campo **Email de acceso** y la descripción si es necesaria.
- Indica el rol que tendrá asignada la cuenta de usuario. Consulta **Descripción de los permisos implementados**.
- Haz clic en el botón **Guardar**. Panda Endpoint Protection enviará un correo a la cuenta de correo indicada para que el usuario pueda generar una contraseña de acceso y aceptar los términos de la licencia y el tratamiento de sus datos.

Crear cuentas de usuario sucesivas en Panda Endpoint Protection desde WatchGuard Portal

Las cuentas de usuario que pertenecen al proveedor de seguridad WatchGuard tienen la posibilidad de acceder a la consola de Panda Endpoint Protection directamente desde WatchGuard Portal. El administrador puede crear un usuario en la consola de Panda Endpoint Protection por cada cuenta creada en WatchGuard Portal mediante WatchGuard AccountMapper.

Las cuentas de usuario que pertenecen a un mismo cliente WatchGuard crearán siempre cuentas de usuario en un mismo cliente Panda Security. Esto implica que no será posible acceder a varias consolas de Panda Endpoint Protection alojadas en distintas cuentas de cliente de Panda Security desde las cuentas de usuario de WatchGuard que pertenecen a un mismo cliente.

Antes de iniciar este procedimiento, comprueba que has cerrado la sesión en WatchGuard Portal y en la consola de Panda Endpoint Protection, así como el navegador web.

- Abre el navegador, accede a **https://accountmapper.watchguard.com** y haz clic en **I have a WatchGuard account and need a Panda Account**. Se abrirá la ventana **Create new account with Panda**.
- Haz clic en el botón **Continue** para confirmar la creación de la cuenta de usuario en Panda Endpoint Protection. Se mostrará la ventana **Proporcione los siguientes detalles**.
- Escribe la cuenta de usuario WatchGuard que accederá a la consola de Panda Endpoint Protection y su contraseña, y haz clic en el botón **Continuar**. Se abrirá la ventana **Inicia sesión para acceder a Panda Cloud**.
- Escribe el usuario y contraseña del primer usuario de Panda Endpoint Protection y haz clic en el botón **Iniciar sesión**.
- Haz clic en el botón **Continue**. En la consola de Panda Endpoint Protection se habrá creado automáticamente un nuevo usuario con el prefijo "generated", y se vinculará con el usuario de WatchGuard utilizado para completar el procedimiento.

Una vez que el proceso ha terminado, la cuenta de usuario de WatchGuard podrá acceder a la consola Panda Endpoint Protection. Consulta **Acceso la consola web** en la página **31**.

Acceder a la consola de Panda Endpoint Protection desde WatchGuard Portal con una cuenta ya existente

Si ya existe una cuenta de usuario creada en Panda Endpoint Protection y se quiere utilizar para acceder a la consola desde WatchGuard Portal, es necesario ejecutar un proceso que consiste en vincular una cuenta de usuario de WatchGuard con la cuenta de usuario de Panda Endpoint Protection que accederá a la consola. Solo es necesario ejecutar el procedimiento de vinculación una vez; cuando éste haya terminado, el administrador podrá acceder a la consola de Panda Endpoint Protection con la cuenta de su elección desde WatchGuard Portal.

Antes de iniciar este procedimiento, comprueba que has cerrado la sesión en WatchGuard Portal y en la consola de Panda Endpoint Protection, así como el navegador web.

- Accede a la web **https://accountmapper.watchguard.com** y haz clic en **I have both WatchGuard and Panda accounts**. Se abrirá la ventana **Map your existing accounts?**

advirtiendo de que esta opción solo funciona si las cuentas de usuario de WatchGuard y de Panda están ya creadas y no están vinculadas.

- Haz clic en el botón **Continue**. Se mostrará la pantalla de inicio de sesión en WatchGuard.
- Introduce los datos de la cuenta de usuario WatchGuard que quieres vincular y haz clic en el botón **Continuar**. Se abrirá la ventana **Inicia sesión con tu cuenta Panda**.
- Introduce los datos de la cuenta de usuario de Panda Endpoint Protection que quieres vincular y haz clic en el botón **Iniciar sesión**. Se mostrará una ventana indicando si el proceso de vinculación terminó con éxito o, si no ha sido así, la razón del error.
- Haz clic en el botón **Continue**. Una vez que el proceso ha terminado, la cuenta de usuario de WatchGuard podrá acceder a la consola Panda Endpoint Protection. Consulta **Acceso la consola web** en la página **31**.

Cambiar los datos personales de una cuenta de usuario

- Haz clic en el icono situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**. El procedimiento varía dependiendo de si el administrador entró a la consola desde Panda Cloud o desde WatchGuard Portal.

Panda Cloud

- Se abrirá la ventana **Panda cuenta**.
- Haz clic en el panel izquierdo **Información personal** y escribe en el formulario los datos personales de la cuenta.
- Haz clic en el botón **Guardar**. Los cambios se almacenarán en el servidor de Panda Security.

WatchGuard Portal

- Se abrirá la ventana **User Information**.
- Haz clic en el botón **Edit** situado en la zona inferior de la pantalla y escribe en el formulario los datos personales de la cuenta.
- Haz clic en el botón **Save**. Los datos se almacenarán en el servidor de WatchGuard.

Cambiar la dirección de correo o la contraseña de una cuenta de usuario

- Haz clic en el icono situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.

- Haz clic en **Configurar mi perfil**. El procedimiento varía dependiendo de si el administrador entró a la consola desde Panda Cloud o desde WatchGuard Portal.

Panda Cloud

- Se abrirá la ventana **Panda cuenta**.
- Haz clic en el panel izquierdo **Inicio de sesión** y en los enlaces **Cambiar dirección de email** o **Cambiar contraseña**. Se abrirá una ventana para validar la información antigua e introducir la nueva.
- Haz clic en el botón **Cambiar**.

WatchGuard Portal

- Se abrirá la ventana **User Information**.
- Haz clic en el botón **Edit** asociado al campo **EMAIL** o en el enlace **Change Password** para cambiar los datos.

Borrar o bloquear cuentas de usuarios en la consola de Panda Endpoint Protection

Al borrar una cuenta de usuario de Panda Endpoint Protection vinculada a una cuenta de WatchGuard, solo se elimina la cuenta de Panda Endpoint Protection.

- Comprueba que el usuario tiene asignado el permiso **Gestionar usuarios y roles**. Consulta **Descripción de los permisos implementados**.
- En el menú superior **Configuración** haz clic en el menú lateral **Usuarios.**
- Haz clic en la pestaña **Usuarios**. Se mostrará el listado de usuarios creados en la consola de administración.
- Haz clic en el icono asociado a la cuenta de usuario que quieres borrar.
- Para desactivar temporalmente el acceso de la cuenta a la consola web, haz clic en una cuenta de usuario y desplaza el control deslizante **Bloquear este usuario**. De esta manera, esa cuenta tendrá denegado el acceso a la consola de administración, y si ya está conectada será expulsada de forma inmediata. También dejará de recibir alertas por correo en las direcciones de correo especificadas en su configuración.

Activar la verificación en dos pasos

Panda Endpoint Protection es compatible con el estándar 2FA (Two Factor Authentication), que añade una capa de seguridad adicional a la establecida en el esquema básico "usuario - contraseña". De esta manera, cuando el administrador de la red accede a la consola web, se

introduce un elemento nuevo en el sistema de autenticación básico: un código que solo posee el propietario de la cuenta. Este código es aleatorio y solo puede generase en un dispositivo concreto, normalmente el teléfono móvil o tablet personal del administrador de Panda Endpoint Protection.

Requisitos para activar 2FA

- Acceso a un teléfono móvil o tablet personal con cámara de fotos integrada.
- Descarga la aplicación gratuita WatchGuard AuthPoint (o una aplicación equivalente) en:
  - **iOS**: https://apps.apple.com/app/watchguard-authpoint/id1335115425
  - **Android** : https://play.google.com/store/apps/details?id=com.watchguard.authpoint

Activar 2FA

- Haz clic en el icono situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**. El procedimiento varía dependiendo de si el administrador entró a la consola desde Panda Cloud o desde WatchGuard Portal.

Panda Cloud

- Se abrirá la ventana **Panda cuenta**.
- Haz clic en el panel izquierdo **Inicio de sesión** y en el enlace **Activar** de la sección **Verificación en dos pasos**. Se abrirá la ventana **Sincronización con la app de autenticación**.
- Si es la primera vez que utilizas la aplicación WatchGuard AuthPoint en tu dispositivo móvil, pulsa el botón **Activar**. Si ya la has utilizado anteriormente, pulsa en el icono del QR situado en la esquina superior derecha. Se abrirá la cámara de fotos del dispositivo móvil.

Figura 4.2: Escaneo del código QR con WatchGuard Authpoint

- Enfoca con la cámara el código QR que se muestra en la consola de Panda Endpoint Protection. Se añadirá una nueva entrada en WatchGuard AuthPoint y se empezarán a generar tokens cada 30 segundos.
- Escribe el código generado por WatchGuard AuthPoint en la consola de Panda Endpoint Protection para enlazar el dispositivo con la cuenta de usuario, y haz clic en el botón

Verificar. Se abrirá una ventana con el mensaje **Se ha activado la verificación en dos pasos**.

- Haz clic en el botón **Aceptar**.

WatchGuard Portal

- Se abrirá la ventana **User Information**.
- Haz clic en el botón **Edit** asociado al campo **MULTI-FACTOR AUTHENTICATION**. Se mostrará la ventana **Manage Multi-Factor Authentication**.
- Haz clic en el botón **Enable MFA**. Se abrirá la ventana **Are you sure you want to enable MFA?**.
- Haz clic en el botón **Continue**. Se enviará un email a la dirección de correo del usuario para generar el token.
- Abre el correo y haz clic en el botón **START ACTIVATION**. Se abrirá la ventana **Bienvenido a AuthPoint**.
- Si es la primera vez que utilizas la aplicación WatchGuard AuthPoint en tu dispositivo móvil, pulsa el botón **Activar**. Si ya la has utilizado anteriormente, pulsa en el icono del QR situado en la esquina superior derecha. Se abrirá la cámara de fotos del dispositivo móvil.

Figura 4.3: Escaneo del código QR con WatchGuard AuthPoint

- Enfoca con la cámara el código QR que se muestra en la consola de Panda Endpoint Protection. Se añadirá una nueva entrada en WatchGuard AuthPoint.

Acceder a la consola Web mediante una cuenta con 2FA activado desde Panda Cloud

- Accede a **https://www.pandacloudsecurity.com/PandaLogin/** escribe el usuario y la contraseña y haz clic en el botón **Iniciar sesión**.
- Introduce el código de verificación generado por WatchGuard AuthPoint en tu dispositivo móvil y haz clic en el botón **Verificar**. Se abrirá la ventana **Panda Cloud**.

Acceder a la consola Web mediante una cuenta con 2FA activado desde WatchGuard Portal

- Accede a **https://www.watchguard.com/**, escribe el usuario y la contraseña y haz clic en el botón **Continuar**. Se abrirá la ventana **Elige un método de autenticación**.

- Haz clic en el botón **Enviar Push**. En la aplicación WatchGuard AuthPoint se abrirá la ventana **Estas intentando iniciar la sesión?**.
- Haz clic en el botón **Aprobar** para completar el proceso de acceso a WatchGuard Portal. Se mostrará la ventana **Support Center**.
- Haz clic en el menú superior **MY WATCHGUARD**. Se abrirá un menú desplegable.
- Haz clic en la opción **Manage Panda Products**. Se abrirá la ventana Panda Cloud con todos los servicios contratados.

Forzar la activación de 2FA a todos los usuarios de la consola

Es necesario que la cuenta de usuario que forzará el uso de 2FA tenga el permiso **Gestionar usuarios y roles** y visibilidad completa sobre el parque informático. Consulta **Gestión de roles y permisos**

- En el menú superior **Configuración** haz clic en la pestaña **Seguridad**.
- Activa la opción **Exigir tener activada la verificación en dos pasos para acceder a esta cuenta**.
- Si la cuenta de usuario que activa la funcionalidad 2FA para todos los usuarios de la consola no tiene activada la verificación en dos pasos para su propia cuenta, se mostrará una ventana de aviso que le permitirá acceder a la **Cuenta Panda** para activarlo. Consulta **Activar 2FA**.

Listado de usuarios

Permisos requeridos

Todos los usuarios de la consola pueden ver el listado de usuarios.

Acceso al listado

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará un listado con todas las cuentas de usuario creadas en Panda Endpoint Protection con la información mostrada a continuación:

Campo	Descripción
Nombre de la cuenta	Nombre de la cuenta de usuario.
Rol	Rol asignado a la cuenta de usuario.
Cuenta de correo	Cuenta de correo asignada al usuario.

Campo	Descripción
Candado	Indica si la cuenta tiene activada la funcionalidad de 2FA (Verificación en dos pasos / factores, Two Factor Authentication).
Estado	Indica si la cuenta de usuario esta activada o bloqueada.

Tabla 4.1: Campos del listado de usuarios

Organizar y buscar en el listado de usuarios: haz clic en el icono para organizar el listado de usuarios de manera ascendente / descendente, por nombre o por fecha creación. Para buscar un usuario, escribe el texto en el cuadro de búsqueda y haz clic en el icono .

Campos mostrados en fichero exportado

Campo	Definición	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del perfil de usuario.	Cadena de caracteres
Email de acceso	Email con el que se ha accedido a la consola.	Cadena de caracteres
Rol	Rol asignado al usuario.	Cadena de caracteres
Descripción	Descripción añadida al perfil de usuario.	Cadena de caracteres
Verificación en dos pasos	Indica si la cuenta tiene activada o desactivada la verificación en dos pasos.	Booleano
Bloqueado	Indica si la cuenta de usuario esta activada o bloqueada.	Booleano

Tabla 4.2: Campos de fichero exportado Listado de usuarios

Herramientas de filtrado

Campo	Comentario	Valores
Buscar usuario	Busca por el nombre y la cuenta de correo del usuario. Permite búsquedas parciales de cadenas.	Cadena de caracteres
Bloqueados	Filtra las cuentas de usuario bloqueadas del listado.	• Todos • Si • No
Verificación en dos pasos	Filtra las cuentas de usuario que tienen activado el sistema de verificación en dos pasos.	• Todos • Activado • Desactivado

Tabla 4.3: Campos de filtrado para el listado Estado de Data Control

Herramientas de ordenación

Para mostrar los criterios de ordenación disponibles, haz clic en el icono .

Gestión de roles y permisos

Conceptos básicos

Roles

Un rol es una configuración específica de permisos que se aplica a una o más cuentas de usuario. Una cuenta de usuario estará autorizada a ver o modificar determinados recursos de la consola, dependiendo de rol que tenga asignado.

Una cuenta de usuario solo puede tener un único rol asignado, aunque un mismo rol puede estar asignado a una o más cuentas de usuario.

Un rol está formado por los siguientes elementos:

- **Nombre del rol**: designado en el momento de la creación del rol, su objetivo es meramente identificativo.
- **Visibilidad**: restringe el acceso a determinados equipos de la red.
- **Juego de permisos**: determina las acciones concretas que las cuentas de usuario pueden ejecutar sobre los equipos que pertenecen a los grupos definidos con accesibles.

Roles predefinidos

Una licencia de Panda Endpoint Protection siempre incluye dos roles predefinidos. Estos roles no se pueden editar ni borrar y cualquier cuenta de usuario puede pertenecer a estos roles previa asignación en la consola Web:

El rol Control total

La primera cuenta de usuario que se crea siempre tiene el rol Control total asignado, y permite ejecutar todas las acciones disponibles en la consola sobre todos los equipos integrados en Panda Endpoint Protection.

El rol Solo lectura

Este rol permite el acceso a todas las secciones de la consola, pero no permite crear, modificar o borrar configuraciones, tareas, etc, por lo que permite una visión total del entorno pero sin ninguna modificación. Está especialmente indicado para aquellos administradores de red encargados de la vigilancia del parque informático,pero que no poseen los permisos suficientes para realizar modificaciones, como por ejemplo editar configuraciones o lanzar análisis bajo demanda.

Permiso

Un permiso regula el acceso a una sección concreta de la consola de administración. Existen varios permisos que establecen el acceso a otros tantos aspectos de la consola de Panda Endpoint Protection. Una configuración particular de todos los permisos disponibles forma un rol, que puede ser asignado a una o más cuentas de usuario.

Visibilidad

Cada cuenta de usuario puede configurar la seguridad de un subconjunto de equipos determinado por su visibilidad, de entre todos los equipos integrados en la consola de Panda Endpoint Protection.

Crear un rol

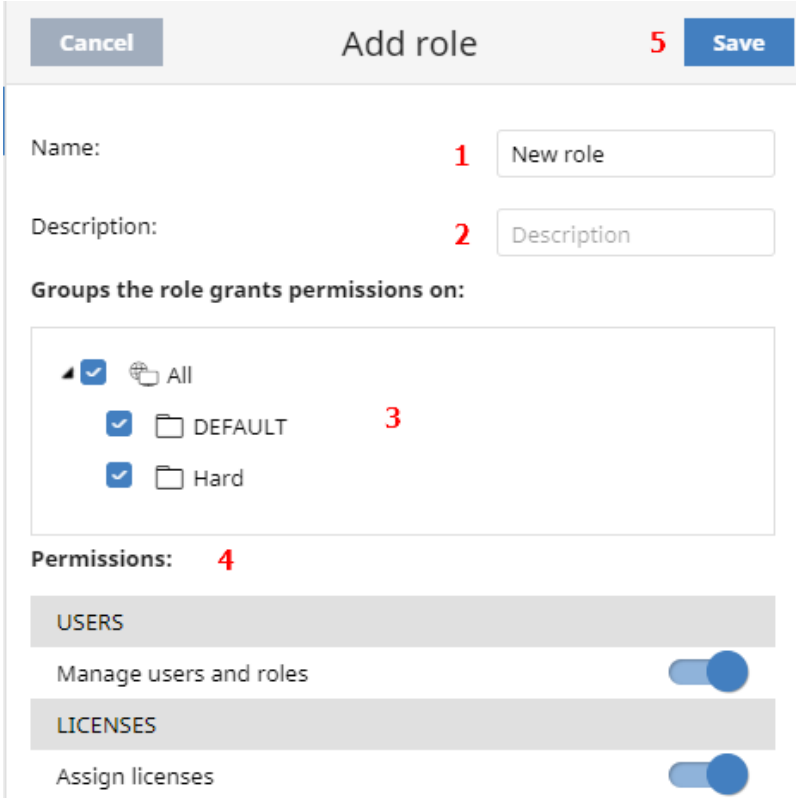


Figura 4.4: Ventana Panda Cloud

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.** Se abrirá una ventana con el listado de usuarios creados.
- Haz clic en la pestaña **Roles** y en el botón **Añadir**. Se abrirá la ventana **Añadir rol**.
- Escribe el nombre del rol **(1)** y una descripción opcional **(2)**.
- Indica la visibilidad del rol **(3)**.
- Activa o desactiva los permisos **(4)**.
- Haz clic en el botón **Guardar (5)**.

Limitaciones en la creación de usuarios y roles

Para evitar una situación de escalado de permisos, los usuarios con el permiso **Gestionar usuarios y roles** activo tienen las siguientes limitaciones a la hora de crear roles o asignarlos a otros usuarios ya creados:

- Una cuenta de usuario solo puede crear roles nuevos con los mismos permisos o menos de los que tiene asignada.
- Una cuenta de usuario sólo puede editar los permisos que tenga activos en los roles ya existentes. El resto permanecerán desactivados.

- Una cuenta de usuario no puede asignar un rol a un usuario si ese rol tiene más permisos asignados que la cuenta de usuario.
- Una cuenta de usuario no puede copiar un rol si ese rol tiene más permisos asignados que la cuenta de usuario.

Borrar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.**
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic sobre el icono de un rol para borrarlo. Si al borrar un rol éste ya tiene cuentas de usuario asignadas, se cancela el proceso de borrado.

Copiar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.**
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic sobre el icono de un rol para copiarlo. Se abrirá la ventana **Copiar rol** con la configuración del rol copiado.
- Modifica la configuración del rol copiado y haz clic en el botón **Guardar**.

Modificar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic en el rol a editar. Se abrirá la ventana **Editar rol**.
- Modifica la configuración del rol y haz clic en el botón **Guardar**.

Descripción de los permisos implementados

Gestionar usuarios y roles

- **Al activar**: el usuario de la cuenta puede crear, borrar y editar cuentas de usuario y roles.
- **Al desactivar**: el usuario de la cuenta deja de poder crear, borrar y editar cuentas de usuario y roles. Se permite ver el listado de usuarios dados de alta y los detalles de las cuentas, pero no el listado de roles creados.

Asignar licencias

- **Al activar**: el usuario de la cuenta puede asignar y retirar licencias de los equipos gestionados.
- **Al desactivar**: el usuario de la cuenta no puede asignar y retirar licencias, pero puede ver si los equipos tienen licencias asignadas.

Modificar el árbol de equipos

- **Al activar**: el usuario de la cuenta tiene pleno acceso al árbol de grupos y puede crear y eliminar grupos, y mover equipos a grupos ya creados.
- **Al activar con conflicto de permisos**:debido a los mecanismos de herencia que se aplican en el árbol de equipos, cualquier modificación en la estructura del mismo puede implicar un cambio de asignación de configuración para los dispositivos. Por ejemplo, en los casos en los que el administrador no tiene permisos para asignar configuraciones, y mueve un equipo de un grupo a otro, la consola web mostrará una advertencia indicando que debido al movimiento de equipos efectuado y a los mecanismos de herencia que se aplican la asignación de configuraciones de los equipos que se han movido podría cambiar (aunque el administrador no tenga permisos para asignar configuraciones). Consulta el apartado **Asignación manual y automática de configuraciones** en la página **287**.
- **Al desactivar**: el usuario de la cuenta puede visualizar el árbol de carpetas y las configuraciones asignadas a cada grupo, pero no puede crear nuevos grupos ni mover equipos.

Añadir, descubrir y eliminar equipos

- **Al activar**: el usuario de la cuenta puede distribuir el instalador entre los equipos de la red e integrarlos en la consola, eliminarlos y configurar toda la funcionalidad relativa al descubrimiento de puestos no gestionados: asignar y retirar el rol de descubridor a los equipos, editar las opciones de descubrimiento, lanzar descubrimientos inmediatos e instalar el agente de Panda de forma remota desde los listados de equipos descubiertos.
- **Al desactivar**: el usuario de la cuenta no puede descargar el instalador, ni por lo tanto distribuirlo entre los equipos de la red. Tampoco puede eliminar equipos previamente integrados ni gestionar la funcionalidad relativa al descubrimiento de equipos no gestionados.

Modificar configuración de red (proxys y caché)

- **Al activar**: el usuario de la cuenta puede crear nuevas configuraciones de tipo **Configuración de red**, editar o borrar las existentes y asignarlas a los equipos integrados en la consola.

- **Al desactivar**: el usuario de la cuenta deja de poder crear nuevas configuraciones de tipo **Configuración de red**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.

Configurar ajustes por equipo (actualizaciones, contraseñas, etc.)

- **Al activar**: el usuario de la cuenta puede crear nuevas configuraciones de tipo **Ajustes por equipo**, editar y borrar las ya creadas y asignar a los equipos integrados en la consola.
- **Al desactivar**: el usuario de la cuenta deja de poder crear nuevas configuraciones de tipo **Ajustes por equipo**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.

Reiniciar y reparar equipos

- **Al activar**: el usuario de la cuenta puede reiniciar equipos desde los listados de equipos en estaciones y servidores. También puede iniciar la reinstalación remota del software Panda Endpoint Protection en equipos Windows.
- **Al desactivar**: el usuario de la cuenta deja de poder reiniciar equipos y de reinstalar remotamente el software Panda Endpoint Protection.

Configurar seguridad para estaciones y servidores

- **Al activar**: el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de seguridad para estaciones y servidores.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de seguridad para estaciones y servidores**.

Ver configuraciones de seguridad para estaciones y servidores

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar la seguridad para estaciones y servidores.

- **Al activar**: el usuario de la cuenta puede únicamente visualizar las configuraciones de seguridad creadas, así como ver la configuración de un equipo o de un grupo.
- **Al desactivar**: el usuario de la cuenta deja de poder ver las configuraciones de seguridad creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Configurar seguridad para dispositivos móviles

- **Al activar**: el usuario de la cuenta puede crear, editar, borrar y asignar configuraciones de dispositivos móviles.
- **Al desactivar**: el usuario de la cuenta deja de poder crear, editar, borrar y asignar configuraciones de dispositivos móviles.

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de seguridad para dispositivos móviles**, explicado a continuación.

Ver configuraciones de seguridad para dispositivos móviles

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar la seguridad para dispositivos móviles.

- **Al activar**: el usuario de la cuenta únicamente puede visualizar las configuraciones de dispositivos móviles creadas, así como ver la configuración de un dispositivo o grupo de dispositivos móviles.
- **Al desactivar**: el usuario de la cuenta deja de poder ver las configuraciones de dispositivos móviles creadas, y tampoco podrá acceder a las configuraciones asignadas de cada dispositivo móvil.

Utilizar la protección antirrobo para dispositivos móviles (localizar, borrar, bloquear, etc).

- **Al activar**: el usuario de la cuenta puede visualizar el mapa de geolocalización y operar con el panel de acciones que permite enviar tareas antirrobo a los dispositivos móviles.
- **Al desactivar**: el usuario de la cuenta no puede visualizar el mapa de geolocalización ni operar con el panel de acciones que permite enviar tareas antirrobo a los dispositivos móviles.

Visualizar detecciones y amenazas

- **Al activar**: el usuario de la cuenta puede acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado,** y crear nuevos listados con filtros personalizados.
- **Al desactivar**: el usuario de la cuenta no puede visualizar ni acceder a los paneles y listados de la sección **Seguridad** en el menú superior **Estado,** ni crear nuevos listados con filtros personalizados.

El acceso a la funcionalidad relativa a la exclusión y desbloqueo de amenazas y elementos desconocidos se establece mediante el permiso Excluir temporalmente amenazas Malware, PUP y Bloqueados

Lanzar análisis y desinfectar

- **Al activar**: el usuario de la cuenta puede crear editar, modificar y borrar tareas de tipo análisis y desinfección.
- **Al desactivar**: el usuario de la cuenta no puede crear, editar, modificar ni borrar las tareas ya creadas de tipo análisis. Únicamente podrá listar las tareas y visualizar su configuración.

Excluir temporalmente amenazas Malware y PUPs

- **Al activar**: el usuario de la cuenta puede no volver a detectar y dejar de permitir malware y PUPs.
- **Al desactivar**: el usuario de la cuenta no puede crear excepciones o modificar las ya existentes sobre el malware y PUPs.

*Es necesario activar **Visualizar detecciones y amenazas** para poder ejercer completamente **Excluir temporalmente amenazas Malware y PUPs**.*

Configurar gestión de parches

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de gestión de parches para equipos Windows, macOS y Linux.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de gestión de parches para equipos Windows, macOS y Linux.

Al desactivar este permiso se mostrará el permiso **Visualizar configuraciones de gestión de parches**.

Visualizar configuraciones de gestión de parches

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar gestión de parches.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de gestión de parches creadas, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones Gestión de parches creadas, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Instalar / desinstalar y excluir parches

- **Al activar**: el usuario de la cuenta podrá crear tareas de parcheo, desinstalación y exclusión de parches, así como acceder a los listados **Parches disponibles**, **Programas "End of life"**, **Historial de instalaciones** y **Parches excluidos**.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear tareas de parcheo, desinstalación y exclusión de parches.

Visualizar parches disponibles

Este permiso solo es accesible cuando se ha deshabilitado el permiso Instalar / desinstalar y excluir parches

- **Al activar**: el usuario de la cuenta podrá acceder a los listados **Estado de gestión de parches**, **Parches disponibles**, **Programas "End of life"** e **Historial de instalaciones**.
- **Al desactivar**: el usuario de la cuenta dejará de poder acceder a los listados **Parches disponibles**, **Programas "End of life"** e **Historial de instalaciones**.

Configurar Evaluación de vulnerabilidades

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de evaluación de vulnerabilidades para equipos Windows, macOS y Linux.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de evaluación de vulnerabilidades para equipos Windows, macOS y Linux.

Al desactivar este permiso se mostrará el permiso **Visualizar configuraciones de evaluación de vulnerabilidades.**

Visualizar configuraciones de evaluación de vulnerabilidades

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar evaluación de vulnerabilidades.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de evaluación de vulnerabilidades creadas, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones de evaluación de vulnerabilidades, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Visualizar parches disponibles

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar gestión de parches.

- **Al activar**: el usuario de la cuenta podrá acceder a los listados **Estado de la evaluación de vulnerabilidades**, **Parches disponibles por equipos** y **Programas "End of life"**.
- **Al desactivar**: el usuario de la cuenta dejará de poder acceder a los listados **Estado de la evaluación de vulnerabilidades**, **Parches disponibles por equipos** y **Programas "End of life"**.

Configurar cifrado de equipos

- **Al activar**: el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de cifrado.
- **Al desactivar**: el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de cifrado.

Ver configuraciones de cifrado de equipos

Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar cifrado de equipos.

- **Al activar**: el usuario de la cuenta podrá únicamente visualizar las configuraciones de cifrado de equipos, así como ver la configuración asignadas a un equipo o a un grupo.
- **Al desactivar**: el usuario de la cuenta dejará de poder ver las configuraciones de cifrado creadas, y tampoco podrá acceder a las configuraciones asignadas a cada equipo.

Acceder a las claves de recuperación de unidades cifradas

- **Al activar**: el usuario de la cuenta podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados y administrados por Panda Endpoint Protection.
- **Al desactiva**: el usuario de la cuenta no podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados.

Registro de la actividad de las cuentas de usuario

Panda Endpoint Protection registra todas las acciones efectuadas por los administradores de red en la consola web de gestión para determinar quién realizó un cambio, en que momento y sobre qué objeto.

Para acceder a la sección de actividad haz clic en el menú superior **Configuración** y después en la pestaña **Actividad**.

Registro de sesiones

La sección de sesiones lista todos los accesos a la consola de administración, los exporta a formato csv y filtra la información.

Campos mostrados en el listado de sesiones

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se produce el acceso.	Fecha
Usuario	Cuenta de usuario que accede.	Cadena de caracteres
Actividad	Acción que ejecuta la cuenta.	• Iniciar sesión • Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso.	Cadena de caracteres

Tabla 4.4: Campos del listado sesiones

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se produce el acceso	Fecha
Usuario	Cuenta de usuario que accede.	Cadena de caracteres
Actividad	Acción que ejecuta la cuenta	• Iniciar sesión • Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso.	Cadena de caracteres

Tabla 4.5: Campos del fichero exportado sesiones

Herramienta de búsqueda

Campo	Descripción	Valores
Desde	Establece el limite inferior del intervalo de búsqueda.	Fecha
Hasta	Establece el limite superior del intervalo de búsqueda.	Fecha
Usuarios	Nombre del usuario.	Listado de cuentas de usuario creados en la consola de administración.

Tabla 4.6: Campos de filtrado para el listado de sesiones

Registro de acciones de usuario

La sección de **Acciones de usuario** lista todas las acciones ejecutadas por las cuentas de usuario, exporta las acciones a formato csv y filtra la información.

Campos mostrados en el listado de acciones

Campo	Descripción	Valores
Fecha	Fecha y hora en la que ha producido la acción.	Fecha
Usuario	Cuenta de usuario que ejecutó la	Cadena de caracteres.

Campo	Descripción	Valores
	acción.	
Acción	Tipo de operación ejecutada.	Consulta la tabla **Tipos de elementos y acciones**.
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **Tipos de elementos y acciones**.
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **Tipos de elementos y acciones**.

Tabla 4.7: Campos del Registro de acciones

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido la acción.	Fecha
Usuario	Cuenta de usuario que ejecutó la acción.	Cadena de caracteres
Acciones	Tipo de operación realizada.	Consulta la tabla **Tipos de elementos y acciones**.
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **Tipos de elementos y acciones**.
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla **Tipos de elementos y acciones**.

Tabla 4.8: Campos del fichero exportado Registro de acciones

Herramienta de búsqueda

Campo	Descripción	Valores
Desde	Establece el límite inferior del intervalo de búsqueda.	Fecha

Campo	Descripción	Valores
Hasta	Establece el límite superior del intervalo de búsqueda.	Fecha
Usuarios	Nombre del usuario encontrado.	Listado de cuentas de usuario creados en la consola de administración.

Tabla 4.9: Campos de filtrado para el Registro de acciones

Tipos de elementos y acciones

Tipo de elemento	Acción	Elemento
Acuerdo de licencia	Aceptar	Número de versión del EULA aceptado.
Amenaza	Permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
	Dejar de permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
Búsqueda de información	Lanzar	Nombre de la búsqueda sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la búsqueda sobre la que el usuario realizó la acción.
	Cancelar	Nombre de la búsqueda sobre la que el usuario realizó la acción.
Cuenta	Actualizar consola	De Versión origen a Versión destino.
	Cancelar actualización de consola	De Versión origen a Versión destino.
Certificado push de Apple	Cargar	Nombre del certificado importado en la consola
Configuración -	Crear	Nombre de la configuración sobre la

Tipo de elemento	Acción	Elemento
'Configuración de red'		que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Ajustes por equipo'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Estaciones y servidores'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Dispositivos Android'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - Dispositivos iOS	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la

Tipo de elemento	Acción	Elemento
		que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Patch Management'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Panda Full Encryption'	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - Evaluación de vulnerabilidades	Crear	Nombre de la configuración sobre la que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre la que el usuario realizó la acción.
Configuración - 'Criterios para red de confianza'	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
Dispositivo	Editar nombre	Nombre de la configuración sobre la que el usuario realizó la acción.
Envío programado	Crear	Nombre del envío programado

Tipo de elemento	Acción	Elemento
		sobre el que el usuario realizó la acción.
	Editar	Nombre del envío programado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del envío programado sobre el que el usuario realizó la acción.
Equipo	Eliminar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar nombre	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Cambiar Grupo	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Heredar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'dispositivos Android'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'dispositivos Android'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desasignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reiniciar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Bloquear	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Borrar datos	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Foto al ladrón	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Alarma remota	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Localizar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Designar Proxy Panda	Nombre del equipo sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Revocar Proxy Panda	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar descubrimiento	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Descubrir ahora	Nombre del equipo sobre el que el usuario realizó la acción.
	Mover a su ruta de Active Directory	Nombre del equipo sobre el que el usuario realizó la acción.
	Desinstalar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar agente	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar protección	Nombre del dispositivo sobre el que el usuario realizó la acción
Equipo no administrado	Ocultar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Visibilizar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Instalar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
Filtro	Crear	Nombre del filtro sobre el que el usuario realizó la acción.
	Editar	Nombre del filtro sobre el que el usuario realizó la acción.
	Eliminar	Nombre del filtro sobre el que el usuario realizó la acción.
Grupo	Crear	Nombre del grupo sobre el que el usuario realizó la acción.
	Editar	Nombre del grupo sobre el que el usuario realizó la acción.
	Eliminar	Nombre del grupo sobre el que el usuario realizó la acción.
	Cambiar Grupo-Padre	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de Proxy e idioma	Nombre del grupo sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Heredar configuración de Proxy e idioma	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Sincronizar grupo	Nombre del grupo sobre el que el usuario realizó la acción.
	Mover equipos a su ruta de Active Directory	Nombre del grupo sobre el que el usuario realizó la acción.
Informes avanzados	Acceder	
Listado	Crear	Nombre del listado sobre el que el usuario realizó la acción.
	Editar	Nombre del listado sobre el que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Eliminar	Nombre del listado sobre el que el usuario realizó la acción.
Control de acceso a redes	Editar	Nombre de la configuración sobre la que el usuario realizó la acción.
Parche	Excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Descargado manualmente"	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Requiere descarga manual"	Nombre del parche sobre el que el usuario realizó la acción.
Preferencia ante reclasificación de amenaza	Editar	
Preferencia para envío emails	Editar	
Preferencia para eliminación automática de equipos	Editar	
Preferencia para entornos VDI	Editar	

Tipo de elemento	Acción	Elemento
Preferencia para evaluación de riesgos	Editar	
Preferencia para MDR	Editar	
Preferencia de acceso de equipo de Panda Security S.L.	Editar	
Preferencia de acceso del distribuidor	Editar	
Preferencia para envío emails distribuidor	Editar	
Preferencia de verificación en dos pasos	Editar	
Rol	Crear	Nombre del rol sobre el que el usuario realizó la acción.
	Editar	Nombre del rol sobre el que el usuario realizó la acción.
	Eliminar	Nombre del rol sobre el que el usuario realizó la acción.
Tarea - Análisis de seguridad	Crear	Nombre de la tarea sobre la que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
	Publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
Tarea - Instalación de parches	Crear	Nombre de la tarea sobre la que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
Usuario	Crear	Nombre del usuario sobre la que el usuario realizó la acción.
	Editar	Nombre del usuario sobre la que el usuario realizó la acción.
	Eliminar	Nombre del usuario sobre la que el usuario realizó la acción.
	Bloquear	Nombre del usuario sobre la que el usuario realizó la acción.
	Desbloquear	Nombre del usuario sobre la que el usuario realizó la acción.

Tipo de elemento	Acción	Elemento
Tarea - Desinstalación de parches	Crear	Nombre de la tarea sobre la que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre la que el usuario realizó la acción.
	Crear y publicar	Nombre de la tarea sobre la que el usuario realizó la acción.

Tabla 4.10: Tipos de elemento y acciones

Eventos del sistema

Lista los eventos que se producen en Panda Endpoint Protection y que no tienen una cuenta de usuario como origen, sino que son desencadenados por el propio sistema como respuesta las situaciones mostradas en**Tipos de elementos y acciones**.

Campos mostrados en el listado de eventos del sistema

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Panda Endpoint Protection.	Consulta **Tipos de elementos y acciones**.
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta **Tipos de elementos y acciones**.
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta **Tipos de elementos y acciones**.

Tabla 4.11: Campos del listado Eventos del sistema

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Panda Endpoint Protection.	Consulta Tipos de elementos y acciones.
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta Tipos de elementos y acciones.
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta Tipos de elementos y acciones.

Tabla 4.12: Campos del listado Eventos del sistema

Herramienta de búsqueda

Campo	Descripción	Valores
Desde	Establece el límite inferior del intervalo de búsqueda.	Fecha
Hasta	Establece el límite superior del intervalo de búsqueda.	Fecha

Tabla 4.13: Campos del listado Eventos del sistema

Tipos de elementos y acciones

Tipo de elemento	Acción	Elemento
Equipo no-persistente	Eliminar automáticamente	Nombre del equipo sobre el que se realizó la acción.
Equipo	Registrar en servidor por primera vez.	Nombre del equipo sobre el que se realizó la acción.
	Registrar en servidor tras eliminación de equipo.	Nombre del equipo sobre el que se realizó la acción.
	Registrar en servidor tras reinstalación de agente.	Nombre del equipo sobre el que se realizó la acción.

Tipo de elemento	Acción	Elemento
	Desinstalar el agente	Nombre del equipo sobre el que se realizó la acción.
	Desinstalar el agente y eliminar automáticamente	Nombre del equipo sobre el que se realizó la acción.
	Eliminar automáticamente	Nombre del equipo sobre el que se realizó la acción.
Envío programado	Desactivar automáticamente	Nombre del envío programado sobre el que se realizó la acción.

Tabla 4.14: Tipos de elementos y acciones

Capítulo 5

Instalación del software cliente

La instalación del software de seguridad comprende un conjunto de procesos que tienen como objetivo integrar en los dispositivos de los clientes los componentes software necesarios para protegerlos de las amenazas informáticas. En lineas generales, se compone de las etapas siguientes:

- **Despliegue**: crea el paquete de instalación con los componentes que forman la solución de seguridad y lo envía a cada uno de los dispositivos de los usuarios de la red.
- **Instalación**: descomprime el paquete de instalación e integra en el sistema operativo del dispositivo los ficheros que forman el software de seguridad.
- **Configuración** : el software de seguridad instalado en el dispositivo recibe las configuraciones necesarias para protegerlo desde el momento de su instalación, sin necesidad de acciones por parte del usuario.
- **Integración en la consola**: la consola de Panda Endpoint Protection muestra el dispositivo y el administrador puede ejecutar acciones sobre el mismo.

Contenido del capítulo

Instalación en sistemas Windows

Visión general del despliegue de la protección

El proceso de instalación en equipos Windows comprende varios pasos, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger:

- Localizar los equipos desprotegidos en la red.
- Satisfacer los requisitos mínimos.
- Desinstalar productos de la competencia y reinicio de equipos.
- Establecer la configuración por defecto de los equipos.
- Establecer el procedimiento de despliegue.
- Comprobar que el software de seguridad se instaló correctamente.

Localizar los equipos desprotegidos en la red

- Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Panda Endpoint Protection. En redes de tamaño grande, es posible acelerar esta tarea mediante las funcionalidades de descubrimiento (consulta **Visualizar equipos descubiertos**).
- Comprueba que el número de licencias libres contratadas es suficiente (consulta **Licencias** en la página **185**).

Panda Endpoint Protection permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Satisfacer los requisitos mínimos

Para conocer los requisitos mínimos consulta **Requisitos de instalación**.

Desinstalar productos de la competencia y reinicio de equipos

*Para crear una configuración de seguridad, consulta **Configuración de la seguridad en estaciones y servidores** en la página **319**. Para asignar una configuración a los equipos de la red, consulta **Asignación manual y automática de configuraciones** en la página **287**.*

Los servicios de protección de Panda Endpoint Protection funcionan sin reiniciar el equipo en el caso de no tener un antivirus previamente instalado.

Algunas versiones anteriores de Citrix pueden requerir un reinicio del equipo o producir pequeños microcortes en las conexiones.

Para instalar Panda Endpoint Protection en un equipo con una solución de seguridad de terceros, elige entre instalarlo sin retirar la protección anterior, o desinstalarla y funcionar exclusivamente con Panda Endpoint Protection. Asigna una configuración de **Estaciones y servidores** con la opción **Desinstalar otros productos de seguridad** ajustada según tus necesidades (consulta **Desinstalar otros productos de seguridad** en la página **322**). Coincidiendo con la búsqueda de actualizaciones, Panda Endpoint Protection comprueba una vez al día la configuración establecida. Para obtener un listado de los productos de seguridad de terceros que Panda Endpoint Protection desinstala de forma automática, consulta el recurso web **https://www.pandasecurity.com/es/support/card?id=50021**.

Para completar la desinstalación del antivirus de terceros, es posible que se requiera un reinicio el equipo.

En función del tipo de versión de Panda Endpoint Protection que quieras instalar, el comportamiento por defecto varía tal y como se muestra a continuación.

Versiones Trials

No se desinstalarán por defecto las soluciones de seguridad de terceros para evaluar Panda Endpoint Protection.

Versiones comerciales

Por defecto, Panda Endpoint Protection no se instala en un equipo que ya dispone de otra solución ajena a Panda Security. Si está disponible un desinstalador del producto, el antivirus de terceros se eliminará del equipo y se lanzará la instalación de Panda Endpoint Protection. En caso contrario, la instalación se detiene.

El comportamiento por defecto es configurable tanto en versiones trial como en versiones comerciales asignando una configuración de **Estaciones y servidores** donde esté deshabilitada la opción **Desinstalar otros productos de seguridad**.

Productos de protección antivirus de Panda Security

Si el equipo está protegido previamente con Panda Endpoint Protection, Panda Endpoint Protection Plus o Panda Fusion, se desinstalará automáticamente el agente de comunicaciones

para instalar el agente Panda y, posteriormente, el sistema comprobará si es necesaria una actualización de la protección. En caso de serlo, se requerirá un reinicio del equipo.

Probabilidad de reinicio al cambiar de producto de protección resume el comportamiento del equipo para completar la instalación de Panda Endpoint Protection.

Producto Anterior	Panda Endpo-int Protection	Reinicio
Ninguno	Trial o comercial	NO
Panda Endpoint Protection Legacy, Panda Endpoint Protection Plus Legacy	Comercial	PROBABLE (solo si requiere actualización de la protección)
Antivirus de terceros	Trial	NO (por defecto los dos productos conviven)
Antivirus de terceros	Comercial	POSIBLE (se puede requerir un reinicio para completar la desinstalación del producto de terceros)
Sistemas Citrix	Trial o comercial	POSIBLE (en versiones anteriores)

Tabla 5.1: Probabilidad de reinicio al cambiar de producto de protección

Establecer la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Panda Endpoint Protection establece las configuraciones por defecto asignadas al grupo **Todos**. En el proceso de despliegue, es posible cambiar el grupo al que pertenecerá el equipo para asignarle otras configuraciones. Consulta **Gestión de configuraciones** en la página **279**.

Una vez instalado el software en el equipo, Panda Endpoint Protection aplica las configuraciones establecidas en el grupo al que pertenece el equipo. Posteriormente, si la configuración de red del grupo seleccionado difiere de la indicada al generar el instalador, se genera una asignación manual. De esta forma, la configuración de red seleccionada en la instalación prevalece por encima de la asignada en el árbol de grupos. Consulta **Generar el paquete de instalación y despliegue manual**.

Establecer el procedimiento de despliegue

Dependiendo del número total de equipos Windows a proteger, los puestos y servidores con un agente Panda ya instalado y la arquitectura de red de la empresa, es preferible utilizar un procedimiento u otro de los disponibles:

- Despliegue manual. Consulta **Generar el paquete de instalación y despliegue manual**.
- Herramienta de despliegue centralizado. Consulta **Instalar mediante generación de imágenes gold**.
- Despliegue remoto desde la consola de administración. Consulta **Descubrimiento de equipos e instalación remota del software cliente** .
- Despliegue mediante generación de imágenes gold. Consulta **Instalar mediante generación de imágenes gold**.

Comprobar que el software de protección se instaló correctamente

- Selecciona el menú superior **Equipos** y localiza el equipo instalado. Para obtener más información sobre buscar equipos consulta **Gestión de equipos y dispositivos** en la página **209**.
- Haz clic en el equipo en el que has instalado el software de seguridad. Se abrirá la ventana de detalles del equipo.
- Haz clic en la pestaña **Detalles**. Se mostrará toda la información recogida del equipo y el estado de la instalación.
- En la sección **Seguridad** comprueba el estado de los distintos módulos:
    - **Instalando...**: el proceso de instalación no se ha completado o ha terminado en error. Espera unos minutos.
    - **Activado / desactivado:** transcurridos unos minutos, si la instalación terminó correctamente se mostrará el estado de los módulos de protección.

Detectar y solucionar fallos de instalación

Si transcurridos unos minutos la sección **Seguridad** desaparece del detalle del equipo, esto indica que el software de seguridad no se instaló correctamente. Comprueba los siguientes puntos:

- Si la instalación se realizó de forma manual comprueba que en el equipo del usuario no se muestran mensajes de error.
- Comprueba si el equipo se muestra en los listados. Consulta **Comprobar el despliegue**.
- Comprueba en el equipo del usuario el visor de sucesos. Consulta **Comprobar el despliegue**
- Consulta que el equipo del usuario cumple con los requisitos indicados en **Requisitos de instalación** y actualiza la versión del producto o la versión del sistema operativo. Consulta **Actualización del producto** en la página **201**.

Requisitos de instalación

Para una descripción completa de los requisitos por plataforma consulta ***Funcionalidades del producto y requisitos*** *en la página* ***619****.*

Requisitos por plataforma

Windows

- **Estaciones de trabajo**: Windows XP SP3, Windows Vista, Windows 7, Windows 8, Windows 10 y Windows 11.
- **Servidores**: Windows 2003 SP2, Windows 2008, Windows Server Core 2008, Windows Small Business Server 2011, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022.
- **Versiones con procesador ARM**: Windows 10 Home y Pro. Windows 11 Home y Pro.
- **Espacio para la instalación**: 650 Mbytes.
- **Certificados raíz actualizados** para utilizar el módulo Panda Patch Management y las comunicaciones en tiempo real con la consola de administración. Consulta **Actualizar los certificados raíz** en la página **627**.
- **Compatibilidad con SHA-256**: para poder actualizar el software de seguridad a la última versión disponible, es necesario que el equipo del usuario o servidor sea compatible con las firmas de drivers SHA-256 . Para obtener más información sobre los sistemas operativos afectados y cómo actualizarlos, consulta **Compatibilidad con firma de drivers SHA-256** en la página **628**. Para localizar los equipos que no admiten el firmado de drivers SHA-256, consulta **Equipos no compatibles con firma de drivers SHA-256** en la página **220**.

IoT y Windows Embedded Industry

Compatible con Windows XP Embedded y superiores.

Los sistemas embedded pueden instalarse de forma personalizada, por lo que el funcionamiento de Panda Endpoint Protection y de algunos de sus módulos en dichos sistemas puede variar según la instalación. Para comprobarlo, instala Panda Endpoint Protection y verifica que las diferentes protecciones funcionan correctamente.

Requisitos de red

En su funcionamiento normal, Panda Endpoint Protection accede a varios recursos alojados en Internet. De forma general, se requiere acceso a los puertos 80 y 443. Para un listado completo de

las URLs que se acceden desde los equipos con el software Panda Endpoint Protection instalado, consulta **Acceso a URLs del servicio** en la página **637**.

Otros requisitos

Actualizar los certificados raíz

Para que el producto funcione correctamente deben mantenerse actualizados los certificados raíz instalados en los equipos protegidos. Si los certificados raíz no se actualizan, algunas funcionalidades del producto podrían dejar de funcionar. Consulta **Actualizar los certificados raíz** en la página **627**.

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, es muy recomendable que el reloj de los equipos protegidos con Panda Endpoint Protection esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP. Consulta **Sincronización horaria de los equipos (NTP)** en la página **627**.

Generar el paquete de instalación y despliegue manual

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se abriráuna ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono Windows, tanto para equipos con procesador x86 como ARM. Se abrirá la ventana **Windows**.

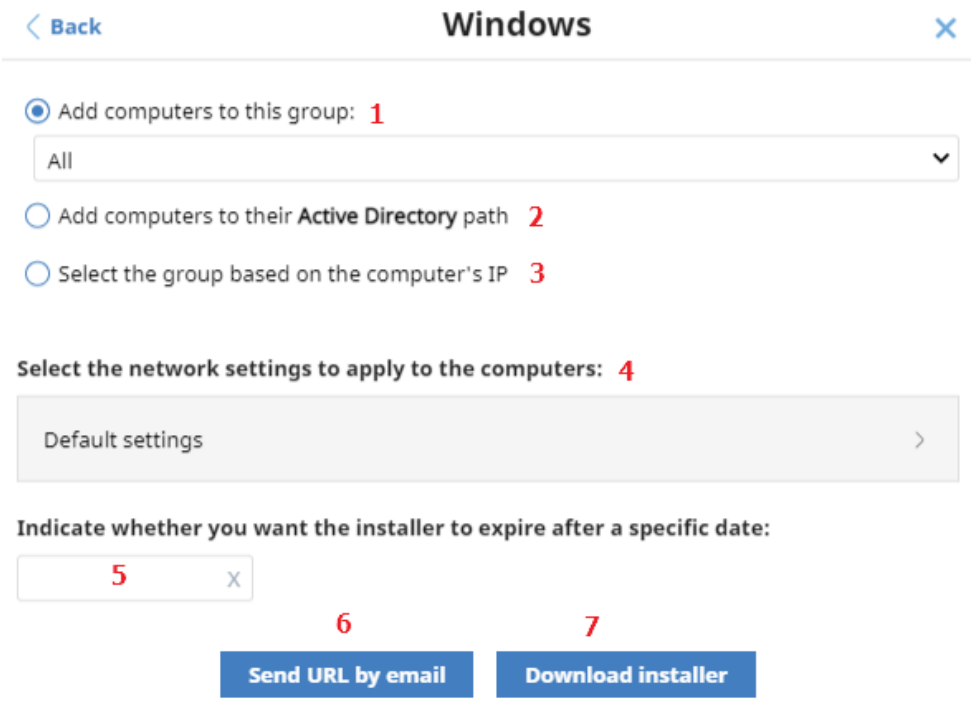


Figura 5.1: Configuración del paquete de descarga

- Selecciona el grupo donde se integrará el equipo en el árbol de carpetas (para más información sobre los diferentes tipos de grupos y sus particularidades, consulta **Tipos de grupos** en la página **221**:
    - Para integrar el equipo en un grupo nativo, haz clic en **Añadir los equipos al siguiente grupo (1)** y selecciona el destino en el árbol de carpetas mostrado.
    - Para integrar el equipo en un grupo Directorio Activo, haz clic en **Añadir los equipos en su ruta de Directorio Activo (2)**.

> *Las políticas de seguridad asignadas a un equipo dependen del grupo al que pertenece. Si has elegido **Añadir los equipos en su ruta de Directorio Activo** y el administrador del directorio activo de la empresa mueve el equipo de una unidad organizativa a otra, este cambio se replicará en la consola de Panda Endpoint Protection como un cambio de grupo. Por esta razón, las políticas de seguridad asignadas a ese equipo también podrían cambiar sin ser advertido por el administrador de la consola Web.*

    - Para integrar el equipo en un grupo u otro en función de su dirección IP, haz clic en la opción **Seleccionar el grupo en función de la IP del equipo (3)** y elige el grupo a partir del cual se buscará un destino que coincida con la IP del equipo. Consulta **Integración de equipos según su dirección IP**.

- Para establecer una configuración de red alternativa al grupo donde se integrará el equipo, haz clic en **Selecciona la configuración de red para los equipos (4)** y elige una configuración de red en el desplegable: inicialmente, todas las configuraciones que se aplican al equipo en el momento de la integración son las que están asignadas al grupo de la consola al que pertenecerá. Sin embargo, para prevenir fallos de conectividad y evitar que el equipo quede inaccesible desde la consola de administración por una configuración de red no apropiada, es posible establecer una configuración de red alternativa. Para más información sobre crear configuraciones de red consulta **Configuración remota del agente** en la página **299**.
    - **Grupos nativos y grupos IP**: el desplegable **Selecciona la configuración de red para los equipos (4)** muestra la configuración de red asignada al grupo elegido en **Añadir los equipos al siguiente grupo (1).**
    - **Grupos Active Directory**: el desplegable **Selecciona la configuración de red para los equipos (4)** muestra la configuración de red asignada al grupo de Active Directory seleccionado en el árbol de grupos. Si no estaba seleccionado ningún grupo de directorio activo antes de hacer clic en el botón **Añadir equipo**, será necesario establecer una configuración de red.

- Para evitar que el instalador pueda utilizarse más allá de una fecha determinada, haz clic en la caja de texto **Indica si quieres que el instalador no se pueda utilizar a partir de una fecha** y selecciona la fecha en el calendario.
- Para enviar el instalador al usuario por correo electrónico:
    - Haz clic en el botón **Enviar URL por email (6)**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador con un mensaje ya generado que contiene la URL de descarga.
    - Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.
    - El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo para iniciar la descarga del instalador.
- Para descargar el paquete de instalación y compartirlo con los usuarios de la red, haz clic en el botón **Descargar instalador (7)**.

Instalación del paquete descargado

- Haz doble clic en el paquete y sigue el asistente de instalación. Durante todo el proceso se muestra una ventana que indica el progreso de la tarea.
- Si el número de licencias libres no es suficiente para asignar una al equipo en proceso de instalación, se mostrará un aviso en pantalla. Independientemente de este hecho, el equipo se integrará en la consola de administración pero no estará protegido hasta que no haya licencias disponibles.

Una vez instalado el agente, éste realiza una serie de comprobaciones automáticas:

- **Integración del agente en Aether**: el agente envía la información del equipo a la nube de Panda para integrarlo en la plataforma.
- **Descarga del instalador del módulo de la protección**: el agente descarga e instala el módulo de protección.
- **Descarga del fichero de firmas**: el agente descarga el fichero de firmas con el malware conocido.
- **Descarga de configuraciones** : se descargan y aplican las configuraciones predeterminadas y creadas por el administrador.
- **Comprobar la conectividad con la nube de Panda**: en caso de error se reporta su tipo a los siguientes lugares:
    - **En la consola de instalación del agente**: se muestra un mensaje de error y las URLs que fallan. Haz clic en el botón **Reintentar** para realizar una nueva verificación.
    - **En el visor de sucesos de Windows (Eventlog)**: se muestra un mensaje de error y las

URLs que fallan.

- **En la consola web**: se muestra un mensaje de error y las URLs que fallan.

Integración de equipos según su dirección IP

Panda Endpoint Protection permite asignar rangos de direcciones IPs e IPs individuales a grupos. Los equipos con una IP que pertenezca al rango del grupo, se moverán automáticamente a éste en el momento de su instalación. Consulta **Crear y organizar grupos** en la página **222**.

El objetivo de esta funcionalidad consiste en ahorrar tiempo al administrador organizando de forma automática los equipos recién integrados en el producto. Cuando un equipo nuevo se integra en Panda Endpoint Protection se siguen los pasos mostrados a continuación:

- Si la opción elegida en la integración es **Seleccionar el grupo en función de la IP del equipo**, Panda Endpoint Protection ejecutará una búsqueda en profundidad para recuperar las IPs asociadas al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos** y las de todos sus hijos.
- Si se encuentra una única IP coincidente con el equipo, éste se moverá al grupo pertinente.
- Si hay varios grupos de IPs que coinciden con la IP del equipo, se tomará siempre el grupo de mayor profundidad. Si existen varios grupos que coinciden con la IP con un mismo nivel de profundidad se elegirá el último de ellos.
- Si no existe ninguna coincidencia, el equipo se moverá al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos**, y si este grupo no existe en el momento de la integración, el equipo se moverá al grupo **Todos**.

Una vez movido el equipo al grupo correspondiente, el equipo no se volverá a mover automáticamente al cambiar su IP, ni tampoco se reorganizarán los equipos ya integrados al cambiar las IPs asignadas a los grupos de IPs.

Instalar con herramientas centralizadas

En redes de tamaño medio o grande es conveniente instalar el software cliente para equipos Windows de forma centralizada con la ayuda de herramientas de terceros.

Línea de comandos del paquete de instalación

Para automatizar la instalación e integración del software de seguridad en la consola de administración se implementan los parámetros siguientes de línea de comandos:

- **`GROUPPATH="grupo1\grupo2"`**: ruta dentro del árbol de grupos y sin indicar el nodo raíz **Todos** donde se integrará el equipo. Si el grupo no existe, el equipo se integra en el nodo raíz **Todos**.
- **`PRX_SERVER`**: dirección IP o nombre del servidor proxy corporativo.
- **`PRX_PORT`**: puerto del servidor proxy corporativo.

- **PRX_USER**: usuario del servidor proxy corporativo.
- **PRX_PASS**: contraseña del servidor proxy corporativo.

A continuación, se muestra un ejemplo de instalación con parámetros:

```
Msiexec /i "PandaAetherAgent.msi" GROUPPATH="Madrid\Contabilidad"
PRX_SERVER="ProxyCorporative" PRX_PORT="3128" PRX_USER="admin" PRX_
PASS="panda"
```

Para realizar la instalación de modo silencioso, añade el parametro `/qn`:

```
Msiexec /i "PandaAetherAgent.msi" /qn
GROUPPATH="Madrid\Contabilidad" PRX_SERVER="ProxyCorporative" PRX_
PORT="3128" PRX_USER="admin" PRX_PASS="panda"
```

Despliegue desde Panda Systems Management

Para los clientes de Panda Systems Management, el despliegue de Panda Endpoint Protection está completamente automatizado a través de los componentes:

- Panda Endpoint Protection on Aether Installer for Windows
- Panda Endpoint Protection Installer on Aether for macOS
- Panda Endpoint Protection Installer on Aether for Linux

Los tres componentes son gratuitos para todos los usuarios de Panda Systems Management y están disponibles en la Comstore.

Características y requisitos del componente

Los componentes no tienen ningún requisito más allá de los indicados para Panda Systems Management y Panda Endpoint Protection.

El tamaño del componente es:

- Panda Endpoint Protection on Aether Installer for Windows: 1.5 Mbytes
- Panda Endpoint Protection Installer on Aether for macOS: 3 Kbytes
- Panda Endpoint Protection Installer on Aether for Linux: 3 Kbytes

Una vez desplegado y ejecutado, el componente descargará el instalador Panda Endpoint Protection. Dependiendo de la versión, el tamaño varía entre 6 y 8 Mbytes por cada equipo a instalar.

Despliegue con Microsoft Active Directory

Limitaciones de Microsoft Active Directory al desplegar el software de seguridad

- El método de despliegue con Microsoft Active Directory instala el software de seguridad en un equipo por primera vez. No se soporta la actualización del software de seguridad ya instalado.
- El equipo donde se define la GPO (Group Policy Object) no puede tener instalado el software de seguridad. En caso contrario, el proceso mostrará el error "The process of adding failed. The deployment information could not be retrieved from the package. Make sure that the package is correct".

Pasos para preparar una GPO (Group Policy Object) de instalación

1. Descarga el paquete Panda Endpoint Protection y comparte el instalador en la red.
    - Coloca el instalador Panda Endpoint Protection en una carpeta compartida que sea accesible por todos los equipos que vayan a recibir el software.
2. Crea una nueva UO (Unidad Organizativa) de nombre "Despliegue Aether".
    - Abre la `mmc` y agrega el snap-in Administrador de políticas de grupo.
    - Con el botón de la derecha en el nodo del dominio, haz clic en **Nuevo** y **Unidad Organizativa** para crear una unidad organizativa de nombre "Despliegue Aether".
    - Haz clic con el botón de la derecha del ratón en la unidad organizativa recién creada y selecciona en el menú **Bloquear herencia**.

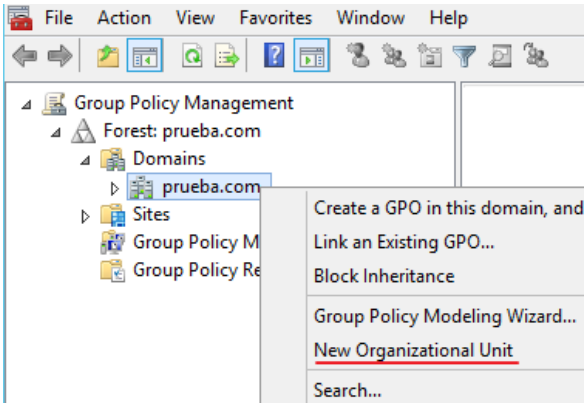


Figura 5.2: Nueva unidad organizativa

3. Crea una nueva GPO con el paquete de instalación

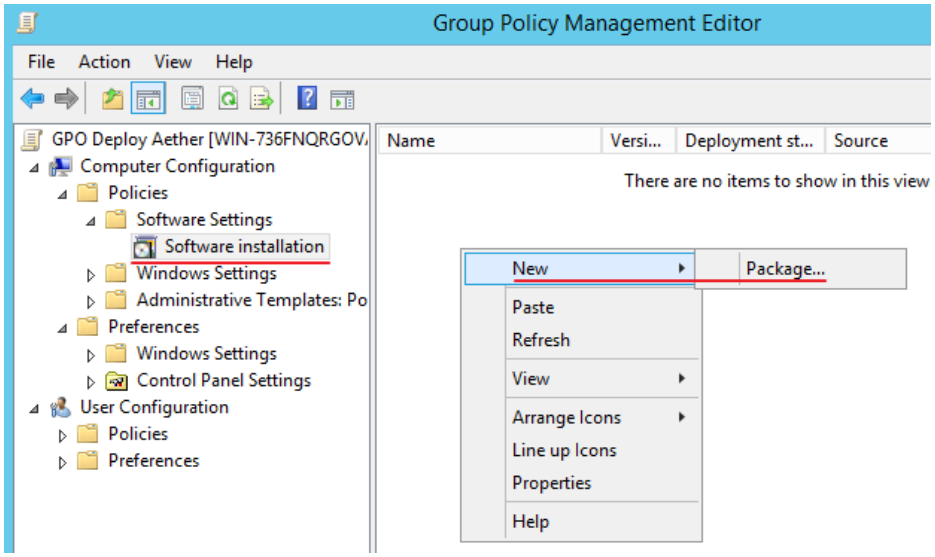


Figura 5.3: Nuevo paquete de instalación

- Haz clic con el botón de la derecha del ratón en la Unidad Organizativa recién creada y selecciona **Crear una GPO** de nombre "GPO Despliegue Aether".
- Edita la GPO recién creada y añade el paquete de instalación que contiene el software Panda Endpoint Protection en la rama **Configuración del equipo, Políticas, Configuración de software, Instalación del software**.
    - Con el botón de la derecha en el panel de la derecha, haz clic en **Nuevo**, **Paquete**.
    - Añade el fichero de instalación `.msi` de Panda Endpoint Protection.

4. Edita las propiedades del paquete

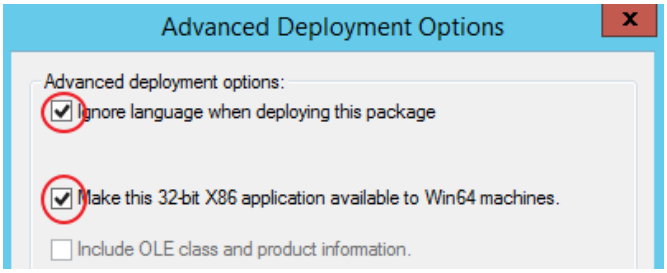


Figura 5.4: Configuración del despliegue

- Haz clic con el botón derecho sobre el paquete agregado y selecciona **Propiedades**, pestaña **Despliegue** y **Avanzado**. Selecciona las casillas que evitan las comprobaciones de idioma y de plataforma entre el sistema operativo de destino y el definido en el instalador.
- Añade a la OU "Despliegue Aether" todos los equipos de la red que recibirán el agente.

Instalar mediante generación de imágenes gold

Sigue los pasos exactos que se muestran en este apartado para generar y desplegar imágenes Windows con Panda Endpoint Protection instalado. De no seguir el procedimiento tal y como se indica, las capacidades de gestión y de protección de tu producto de seguridad se verán reducidas.

En redes grandes formadas por muchos equipos homogéneos, el procedimiento de instalación del sistema operativo y del software que lo acompaña puede automatizarse generando una imagen gold (también conocida como imagen "master", "base", "maqueta" o imagen "plataforma"). Posteriormente, esta imagen se distribuye a todos los equipos de la red, lo que evita gran parte del proceso manual de instalación desde cero.

Para generar una imagen gold, es necesario instalar en un equipo de la red el sistema operativo ya actualizado junto a todo el software que el usuario vaya a necesitar, incluyendo las herramientas de seguridad. Una vez listo el equipo, es necesario utilizar un software de virtualización para "sellar" o "cerrar" la instalación y distribuirla en los equipos de la red. Para obtener información especifica de tu solución de virtualización, consulta la documentación de tu proveedor.

Plataformas de virtualización compatibles

- VMware Workstation
- VMware Server
- VMware ESX
- VMware ESXi
- Citrix XenDesktop
- XenApp
- XenServer
- MS Virtual Desktop
- MS Virtual Servers

Conceptos básicos y herramientas necesarias

Identificador de los equipos VDI

Panda Endpoint Protection genera un identificador único en el proceso de instalación, que se utiliza internamente para referenciar a cada equipo en la consola de administración.

Si Panda Endpoint Protection se instala una única vez en la imagen gold que posteriormente se copiará en los equipos de la red pero no se instala de forma individual en cada uno de los equipos, todos los equipos clonados heredarán el mismo identificador.

Compartir un mismo identificador en varios equipos tiene las siguientes consecuencias negativas:

- Se reducen las capacidades de gestión: la consola de administración solo muestra un equipo, generalmente el primero que se integró en ella. El resto de equipos clonados no serán accesibles desde la consola de Panda Endpoint Protection.
- Se reducen las capacidades de protección del software de seguridad.

Para evitar compartir un mismo identificador en varios equipos, es necesario seguir un protocolo de preparación de la imagen muy estricto que tiene como fin generar una imagen gold sin identificador. Este protocolo incluye:

- Borrar el identificador de la imagen gold
- Desactivar el servicio de protección

Borrar el identificador de la imagen gold

Descarga la herramienta gratuita `Endpoint Agent Tool` en la página web de soporte de Panda Securityen la siguiente URL (contraseña `panda`):

https://www.pandasecurity.com/resources/tools/endpointagenttool.zip

Desactivar el servicio de protección

Muchas soluciones de virtualización inician de forma transparente la imagen gold recién creada como parte del proceso de preparación y despliegue. Esto provoca que Panda Endpoint Protection se inicie, y al detectar que su identificador fue borrado, genera un identificador nuevo, e invalida a imagen generada. Para evitar este escenario, es necesario desactivar el servicio de protección antes de cerrar la imagen gold y programar su lanzamiento mediante métodos alternativos en el inicio de los equipos clonados.

Hay varias formas para ejecutar este paso; la más popular y tratada en este apartado es mediante una GPO si el equipo pertenece a un dominio Windows. Si éste no es el caso, existen otras soluciones alternativas:

- Las soluciones de virtualización pueden incorporar este tipo de herramientas, como por ejemplo Horizon en VMWare.
- RMMs como Panda Systems Management.
- Herramientas como PDQ Deploy, PSExec de Sysinternals, PowerShell de Microsoft, o scripts que utilicen WMI, entre muchos otros.

Activar y desactivar la actualización de Panda Endpoint Protection

En entornos no persistentes donde el sistema de almacenamiento de los equipos clonados se borra cada cierto tiempo, es importante evitar la actualización del software de protección. Esta tarea se delega en el mantenimiento de la imagen gold, para evitar el consumo de red generado por los equipos clonados y un excesivo uso de la CPU en el sistema anfitrión.

Para seguir los procedimientos que permiten generar con éxito una imagen gold, es necesario asignar configuraciones que activan y/o desactivan la actualización de Panda Endpoint Protection en el equipo a clonar:

- Para activar o desactivar la actualización del agente, consulta **Actualización del agente de comunicaciones** en la página **204**.
- Para activar o desactivar la actualización de la protección, consulta **Actualización del motor de protección** en la página **202**.
- Para asignar configuraciones a equipos, consulta **Gestión de configuraciones** en la página **279**.
- Para obtener más información acerca de los grupos en Panda Endpoint Protection, consulta **Árbol de grupos** en la página **220**.

Ya que en algunos escenarios es necesario alternar entre un juego de configuraciones y otro, se recomienda crear dos grupos en la consola de administración: uno con las configuraciones asignadas que activan las actualizaciones de Panda Endpoint Protection y otro con las configuraciones que las desactivan. De esta forma, para activar o desactivar las actualizaciones solo será necesario mover el equipo que contiene la imagen gold de un grupo a otro en la consola.

Adicionalmente, siempre que se hable de un cambio de configuración en la consola de Panda Endpoint Protection, es recomendable seguir el procedimiento mostrado a continuación para asegurarse de que el cambio de configuración se recibe en el equipo utilizado para generar la imagen gold:

- Mover el equipo al grupo adecuado para que herede las configuraciones.
- En el área de notificaciones de la barra de tarea de Windows, haz clic con el botón derecho del ratón sobre el icono de Panda Endpoint Protection. Se mostrará un menú desplegable.
- Selecciona **Sincronizar**. Esto forzará la descarga en el equipo de las configuraciones de seguridad pendientes de recibir desde el servidor.

Crear y desplegar una imagen gold en entornos VDI persistentes

Pasos a ejecutar en el equipo que genera la imagen gold

- Instala el sistema operativo actualizado y los programas que necesitarán los usuarios.
- Comprueba que hay conexión a Internet y que la MAC de la tarjeta de red es estática.
- Instala Panda Endpoint Protection según los pasos mostrados en **Generar el paquete de instalación y despliegue manual** **en un grupo con las actualizaciones activadas**.
- Ejecuta la herramienta `Endpoint Agent Tool`, selecciona las opciones **Detections**, **Counters** y **Check commands**, y haz clic en el botón **Send**.

- **Comprueba que la casilla de selección Is a gold image NO está marcada.**
- Si el equipo está protegido por AntiTamper, escribe la contraseña en **AntiTamper password**; si no, deja este campo en blanco.
- Haz clic en el botón **Prepare image**.
- **Deshabilita el servicio Panda Endpoint Agent**.
- Apaga el equipo y genera la imagen con el software de administración de entornos virtuales que utilices.

Pasos a ejecutar para activar el servicio de protección

Este procedimiento activa el servicio Panda Endpoint Agent en los equipos clonados mediante una GPO:

- Dentro de la configuración de la GPO, navega la ruta **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **System Services**, **Panda Endpoint Agent**.
- El servicio aparecerá como **Deshabilitado**. Cámbialo a **Automático**.

Para conocer más detalles sobre las GPOs, consulta la URL ***https://www.microsoft.com/es-ES/download/details.aspx?id=21895*** .

Crear, desplegar y mantener una imagen gold para entornos VDI no persistentes

Pasos a ejecutar en el equipo que genera la imagen gold

- Instala el sistema operativo actualizado y los programas que necesitarán los usuarios.
- Comprueba que el equipo tiene conexión a Internet .
- Instala Panda Endpoint Protection según los pasos mostrados en **Generar el paquete de instalación y despliegue manual** **en un grupo con las actualizaciones desactivadas**.
- **Mueve el equipo a un grupo con las actualizaciones activadas**.
- Si la persistencia de los equipos clonados será inferior a una semana, es recomendable, aunque no estrictamente necesario, precargar las cachés de Panda Endpoint Protection. Sigue uno de estos dos métodos:
    - En la herramienta `Endpoint Agent Tool` haz clic en el botón **Start cache scan** y espera a que el proceso termine.

      o
    - Haz clic con el botón derecho del ratón en el icono de Panda Endpoint Protection en la barra de notificaciones de Windows.

  - Haz clic en **Antivirus**.
  - Haz clic en el botón **Analizar ahora** y espera a que el proceso termine.

- Ejecuta la herramienta `Endpoint Agent Tool`, selecciona las opciones **Detections**, **Counters** y **Check commands**, y haz clic en **Send**.
- **Comprueba que la casilla de selección Is a gold image SÍ está marcada.**
- Si el equipo está protegido por AntiTamper, escribe la contraseña en **AntiTamper password**; si no, deja este campo en blanco.
- Haz clic en el botón **Prepare image**.
- **Deshabilita el servicio Panda Endpoint Agent**.
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.

Pasos a ejecutar en la consola de administración de Panda Endpoint Protection

- Haz clic en el menú superior **Configuración** y en el panel lateral **Entornos VDI** .
- Define el máximo número de equipos VDI no persistentes que estarán activos simultáneamente.

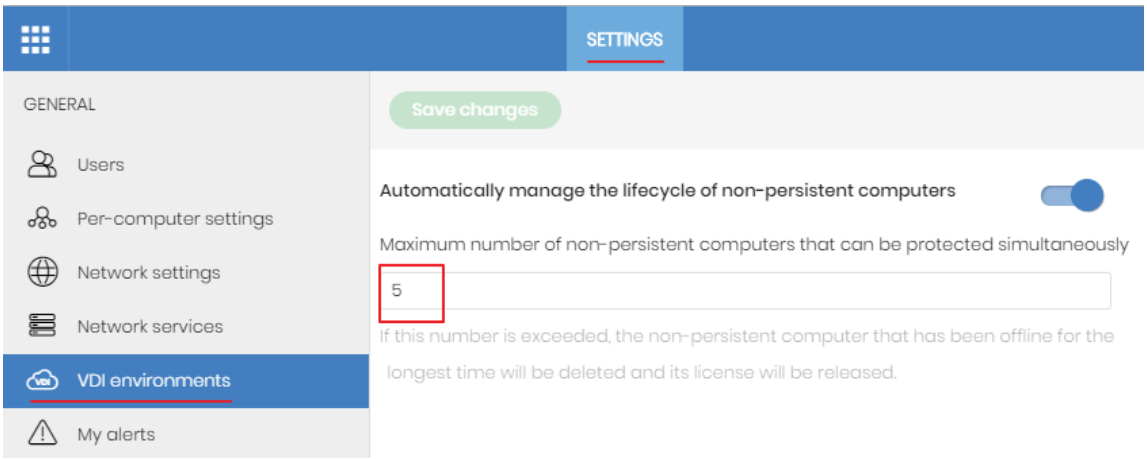


Figura 5.5: Configuración del numero de licencias asignadas a equipos VDI no persistentes

Pasos para activar el servicio de protección

Este procedimiento activa el servicio Panda Endpoint Agent en los equipos clonados mediante una GPO:

- Dentro de la configuración de la GPO, navega la ruta **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **System Services**, **Panda Endpoint Agent**.
- El servicio aparecerá como **Deshabilitado**. Cámbialo a **Automático**.

Ppara conocer más detalles sobre las GPO, consulta la URL
https://www.microsoft.com/es-ES/download/details.aspx?id=21895

Mantener la imagen gold en entornos VDI no persistentes

Dado que los equipos VDI tienen asignada una configuración de actualización deshabilitada, para que reciban la última versión de la protección y del fichero de firmas, es necesario actualizar la imagen gold de forma manual por lo menos una vez al mes. Para ello, accede al equipo que tiene instalada la imagen gold y sigue los pasos mostrados a continuación:

- Comprueba que el equipo tiene conexión a Internet.
- **Mueve el equipo a un grupo con las actualizaciones activadas.**
- Las actualizaciones se hacen en segundo plano, por lo que es necesario esperar varios minutos para completar el proceso. Si hay una versión nueva de la protección, se solicitará el reinicio del equipo. En este caso, tras el reinicio se recomienda volver a forzar una sincronización para asegurar que Panda Endpoint Protection está totalmente actualizado y con la configuración correcta.
- Precarga las cachés de Panda Endpoint Protection. Sigue uno de estos dos métodos:
    - En la herramienta `Endpoint Agent Tool` haz clic en el botón **Start cache scan** y espera a que el proceso termine.

      o
    - Haz clic con el botón derecho del ratón en el icono de Panda Endpoint Protection en la barra de notificaciones de Windows.
    - Haz clic en **Antivirus**.
    - Haz clic en el botón **Analizar ahora** y espera a que el proceso termine.
- En la herramienta `Endpoint Agent Tool` selecciona las opciones **Detections**, **Counters** y **Check commands**, y haz clic en **Send.**
- **Comprueba que la casilla de selección Is a gold image SI está marcada**.
- Si el equipo está protegido por AntiTamper, escribe la contraseña en **AntiTamper password**; de lo contrario, deja este campo en blanco.
- Haz clic en el botón **Prepare image**.
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.
- Sustituye en el entorno VDI la imagen anterior por la nueva obtenida.
- Repite este proceso de mantenimiento una vez al mes por lo menos.

Comprobar que el proceso de clonación es correcto

No existe una fórmula única para comprobar que los equipos clonados son correctos en todos los escenarios posibles, pero a continuación se ofrece una lista de comprobación mínima.

Mostrar los equipos VDI persistentes y no persistentes

Un síntoma de no haber seguido correctamente el procedimiento de generación de imágenes gold, es la aparición de un número de equipos VDI en la consola de administración de Panda Endpoint Protection menor que el realmente instalado en el parque informático. En este caso, las capacidades de gestión y de protección de tu producto de seguridad se verán severamente reducidas.

Para obtener un listado de los equipos VDI no persistentes, sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Entornos DVI** haz clic en el enlace **Mostrar los equipos no persistentes**.
- Se mostrará el listado de equipos con el filtro **Equipos no persistentes** configurado.

Para obtener un listado de los equipos VDI persistentes, sigue los pasos mostrados a continuación:

- En el menú superior **Equipos**, haz clic en el icono de carpeta en el panel lateral. Se mostrará el árbol de grupos.
- Haz clic en el nodo raíz **Todos**. En el panel derecho se mostrarán todos los equipos integrados en la consola de Panda Endpoint Protection.
- Comprueba que todos los equipos persistentes están incluidos en el listado.

Comprobar el estado de las actualizaciones de Panda Endpoint Protection en los equipos clonados

- En el menú superior **Equipos**, haz clic en el icono de carpeta en el panel lateral. Se mostrará el árbol de grupos.
- Localiza en el panel de la derecha los equipos persistentes y no persistentes.
- Por cada equipo clonado haz clic en su nombre. Se abrirá una ventana con el detalle.
- Haz clic en la pestaña **Configuración**. Se mostrarán las configuraciones aplicadas en el equipo.
- Comprueba que las configuraciones **Ajustes por equipo** y **Seguridad para estaciones y servidores** tienen los valores correctos:
    - Para equipos persistentes las actualizaciones deben estar activadas.
    - Para equipos no persistentes las actualizaciones deben estar desactivadas.

Descubrimiento de equipos e instalación remota del software cliente

Los productos basados en Aether Platform incorporan las herramientas necesarias para localizar los puestos de usuario y servidores Windows sin proteger, e iniciar una instalación remota y desatendida del software de seguridad desde la consola de administración.

Para instalar la el software de protección de forma remota en un equipo mediante la consola de administración, es necesario seguir los pasos mostrados a continuación:

- Asignar el rol de descubridor a uno o más equipos de la red. Consulta **Asignar el rol de descubridor a un equipo**.
- Comprobar que los equipos de la red cumplen con los requisitos mínimos. Consulta **Requisitos de red y sistema operativo**.
- Iniciar la instalación remota del software de seguridad. Consulta **Instalación remota del software cliente**.

El descubrimiento de equipos se efectúa a través de un equipo con el rol de descubridor asignado. Todos los equipos que cumplan los requisitos se mostrarán en el listado **Equipos no administrados descubiertos**, independientemente de si el sistema operativo o el tipo de dispositivo admite la instalación de Panda Endpoint Protection.

El primer equipo Windows que se integre en Panda Endpoint Protection, tendrá asignado el rol descubridor de forma automática.

El equipo descubridor puede utilizar al mismo tiempo uno o los dos sistemas de descubrimiento existentes: descubrimiento mediante escaneo de red o descubrimiento mediante directorio activo. Consulta **Utilizar la red para descubrir equiposUtilizar el Directorio activo para descubrir equipos** y **Asignar el rol de descubridor a un equipo**.

Asignar el rol de descubridor a un equipo

- Comprueba que el equipo descubridor tiene instalado Panda Endpoint Protection.
- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y pestaña **Descubrimiento**.
- Haz clic en el botón **Añadir equipo descubridor** y selecciona en el listado los equipos que lanzarán procesos de descubrimiento en la red.

Una vez asignado el rol de descubridor a un equipo, éste se mostrará en la lista de equipos descubridores (menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**). Para cada equipo descubridor se muestra la siguiente información:

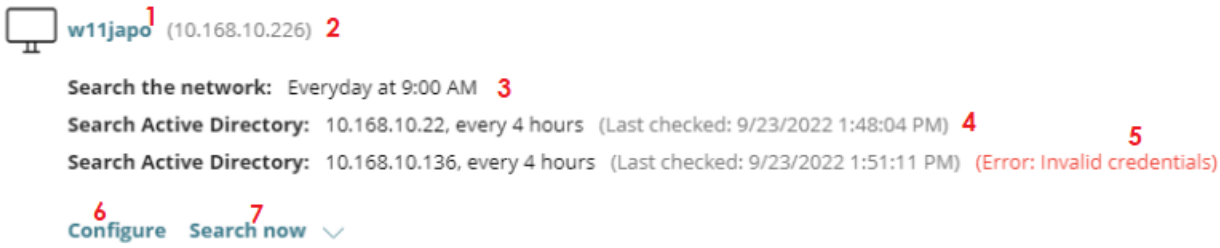


Figura 5.6: Información del equipo descubridor

Campo	Descripción
Nombre del equipo (1)	Nombre del equipo descubridor.
Dirección IP (2)	Dirección IP del equipo descubridor.
Configuración de las tareas de descubrimiento (3)	Descripción de la configuración de las tareas automáticas definidas en el equipo descubridor.
Última comprobación (4)	Fecha y hora de la última vez que se lanzó la tarea de descubrimiento.
Códigos de error (5)	• "El equipo está apagado o sin conexión": el equipo descubridor no es accesible por el servidor de Panda Endpoint Protection. • Error: credenciales incorrectas. • Error: servidor de directorio activo no encontrado. • Error (<código de error>): si se trata de un error desconocido.
Configurar (6)	Establece el alcance y tipo de descubrimiento (automático o manual). Si es automático, la tarea de descubrimiento se ejecutará una vez al día. Consulta **Asignar el rol de descubridor a un equipo**.
Buscar ahora (7)	Lanza la tarea de búsqueda de forma manual. Consulta **Lanzar las tareas de descubrimiento manualmente**.

Tabla 5.2: Campos del detalle de un equipo con el rol descubridor asignado

Utilizar la red para descubrir equipos

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, selecciona el equipo descubridor que quieres configurar y haz clic en el enlace **Configurar**. Se abrirá la ventana **Configurar descubrimiento en <nombre de equipo>**
- Para activar el descubrimiento, desplaza el control deslizante en la sección **Descubrir equipos de la red**.
- En la sección **Limitar alcance del descubrimiento** selecciona un criterio:
  - **Buscar en toda la red**: el equipo descubridor utiliza la máscara configurada en la interface para efectuar un barrido completo de la subred a la que pertenece. La búsqueda se realiza solo sobre rangos de IPs privadas.
  - **Buscar solo en los siguientes rangos de direcciones IPs**: define varios rangos de búsqueda en la red separados por comas. Separa el inicio y el final del rango mediante el carácter guion '-'. Solo se admite especificar rangos de IPs privadas.
  - **Buscar sólo equipos de los siguientes dominios**: la búsqueda queda limitada a los dominios Windows indicados separados por comas.

Todas las configuraciones de alcance de descubrimiento están limitadas al segmento de red donde está conectado el equipo descubridor. Para buscar dispositivos en todos los segmentos de red, asigna el rol de descubridor a por lo menos un equipo en cada segmento de red.

Utilizar el Directorio activo para descubrir equipos

El equipo descubridor se conecta al Directorio Activo de la empresa para buscar los equipos de la red. Cada equipo descubridor puede conectarse a más de un servidor para lanzar las consultas en los directorios, siendo el máximo 3 servidores.

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, selecciona el equipo descubridor cuyo alcance quieres configurar y haz clic en el enlace **Configurar**. Se abrirá la ventana **Configurar descubrimiento**.
- Para activar el descubrimiento, desplaza el control deslizante en la sección **Descubrir equipos en el directorio activo**.
- Haz clic en el enlace **Añadir servidor de directorio activo.** Se abrirá la ventana **Añadir servidor de Directorio Activo.**
- En la ventana que se muestra, escribe el nombre o dirección IP del servidor (campo obligatorio) en el que quieres hacer la búsqueda, y las credenciales si fueran necesarias (pueden ser datos opcionales).

- Para finalizar la configuración, haz clic en el botón **Guardar**. El equipo descubridor preguntará al directorio activo por los equipos de la red cada 4 horas.

Programar las tareas de descubrimiento

Las tareas de descubrimiento de equipos se pueden lanzar de forma programada cada cierto tiempo por los equipos descubridores.

Descubrimiento de red

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
- En el desplegable **Ejecutar automáticamente** elige **Todos los días**.
- Elige la hora a la que se ejecutará la tarea.
- Si quieres que la tarea se rija por la hora local del equipo en lugar de por la del servidor de Panda Endpoint Protection, selecciona la casilla **Hora local del dispositivo**.
- Haz clic en **Guardar**. El equipo descubridor mostrará en su descripción la programación configurada.

Descubrimiento mediante Directorio activo

- En el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**, selecciona el equipo que quieres configurar y haz clic en el enlace **Configurar**. Se abrirá la ventana **Configurar descubrimiento**.
- Haz clic en el directorio activo a configurar. Se abrirá la ventana **Editar servidor de Directorio Activo**.
- En el desplegable **Periodicidad**, selecciona cada cuántas horas se lanzarán las búsquedas.

Lanzar las tareas de descubrimiento manualmente

Para lanzar una tarea de descubrimiento manual, es necesario que el equipo descubridor esté en funcionamiento y tenga conexión con el servidor de Panda Endpoint Protection.

- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Descubrimiento**.
- Haz clic en el enlace **Comprobar ahora** del equipo descubridor de tu elección. Si el equipo descubridor solo tiene un método de descubrimiento configurado, se mostrará el mensaje **Búsqueda de equipos no administrados en curso** y se lanzará la tarea de descubrimiento en segundo plano.
- Si el equipo descubridor tiene configurados varios métodos de descubrimiento, se mostrará un menú de contexto al hacer clic en el enlace **Comprobar ahora**:
    - **Buscar en todos los sitios**: el equipo descubridor realizará un escaneo de la red y de todos los servidores con directorio activo que se hayan configurado.

- **Buscar en la red**: el equipo descubridor realizará un escaneo de red.
- **Buscar en <nombre_servidor>**: el equipo descubridor buscará solo en el servidor seleccionado.

Visualizar equipos descubiertos

Los equipos descubiertos mediante el escaneo de red o mediante directorio activo se muestran en el listado **Equipos no administrados descubiertos**.

> *Para mas información sobre los métodos de descubrimiento de equipos, consulta* ***Utilizar la red para descubrir equipos*** *y* ***Utilizar el Directorio activo para descubrir equipos***

Existen dos formas de acceder al listado de **Equipos no administrados descubiertos**:

- **Widget Estado de protección**: desde el menú superior **Estado** accede al panel de control de Panda Endpoint Protection donde se encuentra el widget **Estado de la protección**. En su parte inferior se mostrará el enlace **Se han descubierto x equipos que no están siendo administrados desde Panda Endpoint Protection**. Haz clic en el enlace para abrir el listado **Equipos no administrados descubiertos**.
- Accede a la sección **Mis listados** desde el panel lateral y haz clic en el enlace **Añadir**. Selecciona en el desplegable el listado **Equipos no administrados descubiertos.**

Listado Equipos no administrados descubiertos

Este listado contiene los equipos descubiertos en la red del cliente que no tienen instalado Panda Endpoint Protection o que, habiéndose instalado correctamente, su funcionamiento no es el adecuado.

Campo	Descripción	Valores
Equipo	Nombre del equipo descubierto.	Cadena de caracteres
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	• — **No administrado**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • **Instalando**: el proceso de instalación se ha iniciado. • **Error instalando**: mensaje con el tipo de error

Campo	Descripción	Valores
		producido en la instalación. Para una relación de mensajes de error y la explicación de cada uno de ellos, consulta **Sección alertas de equipo (2)** en la página **255** . Si el error es de origen desconocido, se mostrará su código de error asociado.
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Ruta de directorio activo	Ruta del directorio activo donde el equipo ha sido descubierto por última vez.	Cadena de caracteres
Último descubridor	Nombre del dispositivo que descubrió más recientemente el puesto de trabajo o servidor.	Cadena de caracteres
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 5.3: Campos del listado de equipos no administrados descubiertos

Cuando el campo **Estado** muestra **Error instalando** y es un error de origen conocido, se añade una cadena de texto que lo describe. Para obtener un listado de los errores de instalación reportados por Panda Endpoint Protection, consulta **Sección alertas de equipo (2)** en la página **255** .

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del equipo descubierto.	Cadena de caracteres
IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección MAC	Dirección física del equipo.	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Directorio activo	Ruta del directorio activo donde el equipo ha sido descubierto por última vez.	Cadena de caracteres
Primera vez visto	Fecha en la que el equipo fue descubierto por primera vez.	Cadena de caracteres
Primera vez visto por	Nombre del equipo	Cadena de caracteres

Campo	Descripción	Valores
	descubridor que vio por primera vez al equipo de usuario.	
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Última vez visto por	Nombre del equipo descubridor que vio por última vez al equipo de usuario.	Cadena de caracteres
Descripción	Descripción del equipo descubierto.	Cadena de caracteres
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	• **No administrado**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • **Instalando**: el proceso de instalación se ha iniciado. • **Error instalando:** mensaje con el tipo de error producido en la instalación. Para una relación de mensajes de error y la explicación de cada uno de ellos, consulta **Sección alertas de equipo (2)** en la página **255**.
Error	Descripción del error encontrado.	Para más información, consulta **Sección alertas de equipo (2)** en la página **255**.

Campo	Descripción	Valores
Fecha error instalación	Fecha y hora en la que se produjo el error.	Fecha

Tabla 5.4: Campos del fichero exportado del listado de equipos no administrados descubiertos

Herramienta de búsqueda

Campo	Descripción	Valores
Buscar	Búsqueda por el nombre del equipo, IP, fabricante de la tarjeta de red o equipo descubridor.	Cadena de caracteres
Estado	Estado de la instalación de Panda Endpoint Protection.	• **No administrado**: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • **Instalando**: el proceso de instalación se ha iniciado. • **Error instalando**: mensaje con el tipo de error producido en la instalación.
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	• Últimas 24 horas • Últimos 7 días • Último mes

Campo	Descripción	Valores
Método de descubri-miento	Método empleado para descubrir al equipo	• Todos • Escaneo de red. Consulta **Descubrimiento de equipos e instalación remota del software cliente** • Directorio activo. Consulta **Descubrimiento de equipos e instalación remota del software cliente**

Tabla 5.5: Campos de filtrado para el listado de equipos no administrados descubiertos

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo.

Detalle de los equipos descubiertos

En el listado de **Equipos no administrados descubiertos**, haz clic en un equipo descubierto para ver su ventana de detalle dividida en tres secciones:

- **Alertas de equipo (1)**: muestra potenciales problemas asociados a la instalación del equipo.
- **Detalles del equipo (2)**: muestra un resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Último descubridor (3):** muestra los equipos descubridores que vieron el equipo no administrado.

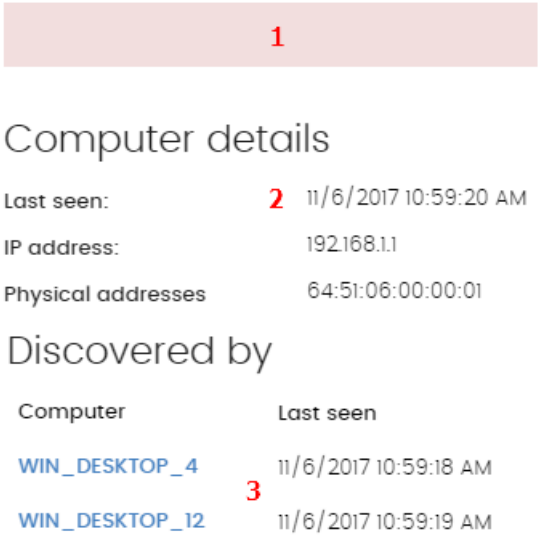


Figura 5.7: Distribución de la información en un equipo descubierto

Alertas de equipo (1)

Estado	Tipo	Resolución
Error instalando el agente de Panda	Indica el motivo del error en la instalación del agente.	
	Credenciales incorrectas	Lanza de nuevo la instalación con unas credenciales que tengan suficientes privilegios para realizar la instalación.
	No es posible conectar con el equipo	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible descargar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible copiar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible instalar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible registrar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.

Estado	Tipo	Resolución
Error instalando la protección de Panda Endpoint Protection	Indica el motivo del error en la instalación de la protección.	
	No hay suficiente espacio libre en el disco para realizar la instalación	Para ver los requisitos de espacio necesarios para instalar Panda Endpoint Protection, consulta **Requisitos hardware** en la página **626**.
	El servicio de Windows Installer no está operativo	Comprueba que el servicio Windows Installer se esté ejecutando. Detiene y pone en marcha el servicio.
	El usuario canceló la desinstalación de la protección de otro fabricante	Acepta la desinstalación del antivirus de terceros.
	Hay otra instalación en curso	Espera a que finalice la instalación previa.
	Error desinstalando automáticamente protecciones de otros fabricantes	Para ver una lista de fabricantes con desinstalador compatible con Panda Security, consulta **Desinstaladores compatibles**.
	Desinstalador no disponible para protección de otro fabricante	Contacta con el departamento de soporte para pedir un desinstalador.
Instalando agente de Panda	Una vez terminado el proceso de instalación, el equipo dejará de aparecer en el listado de Equipos no administrados descubiertos.	
Equipo no administrado	El equipo no tiene el agente Panda instalado. Comprueba que se trata de un equipo compatible con Panda Endpoint Protection y que cumple con los requisitos indicados en **Funcionalidades del producto y requisitos** en la página **619**.	

Tabla 5.6: Campos del listado Equipos protegidos

Detalles del equipo (2)

Campo	Descripción
Nombre del equipo	Nombre del equipo descubierto.
Descripción	Permite asignar una descripción al equipo, aunque no esté administrado todavía.
Primera vez visto	Fecha y hora de la primera vez que el equipo fue descubierto.
Última vez visto	Fecha y hora de la ultima vez que el equipo fue descubierto.
Ruta de directorio activo	En el caso de ser un equipo no administrado descubierto mediante directorio activo, indica la ruta en la que fue descubierto.
Dirección IP	Dirección IP de la tarjeta de red del equipo descubierto.
Direcciones físicas (MAC)	Dirección física de la tarjeta de red del equipo descubierto.
Dominio	Dominio Windows al que pertenece el equipo.
Fabricante NIC	Fabricante de la tarjeta de red instalada en el equipo.

Tabla 5.7: Detalles de los equipos descubiertos

Último descubridor (3)

Campo	Descripción
Equipo	Nombre del equipo descubridor que vio al equipo no administrado.
Última vez visto	Fecha y hora de la última vez que el equipo fue visto por el equipo descubridor.
Método de descubrimiento	Indica si el equipo fue descubierto mediante directorio activo o a través del escaneo de red.

Tabla 5.8: Último descubridor

Borrar y ocultar equipos

Borrar equipos

Panda Endpoint Protection no elimina de la lista **Equipos no administrados descubiertos** los equipos que una vez fueron detectados pero ya no están accesibles por haberse retirado (avería, robo o cualquier otra razón).

Para eliminar de forma manual estos equipos nunca más accesibles, sigue los pasos mostrados a continuación:

- En **Equipos no administrados descubiertos** haz clic en **Descubiertos** u **Ocultos** en la parte superior derecha del listado.
- Selecciona las casillas correspondientes de los equipos a borrar.
    - Para borrar varios equipos, haz clic en el menú de contexto general y en **Eliminar**.
    - Para borrar un único equipo, haz clic en el menú de contexto del equipo y en **Eliminar**.

Un equipo que se elimina de la consola sin desinstalar el software Panda Endpoint Protection, y sin retirarse físicamente de la red, volverá a aparecer en la siguiente tarea de descubrimiento. Borra únicamente los equipos que nunca más vayan a ser accesibles.

Equipos ocultos

Para evitar generar listados muy extensos de equipos no administrados descubiertos que incluyan dispositivos sin interés para la instalación de Panda Endpoint Protection, es posible ocultarlos de forma selectiva:

- En **Equipos no administrados descubiertos** haz clic en **Descubiertos** en la parte superior derecha del listado.
- Selecciona las casillas correspondientes de los equipos a ocultar.
- Para ocultar varios equipos, haz clic en el menú de contexto general y en **Ocultar y no volver a descubrir**.
- Para ocultar un único equipo, haz clic en el menú de contexto del equipo y en **Ocultar y no volver a descubrir**.

Instalación remota del software cliente

El administrador de la red puede instalar de forma remota el software de seguridad en los equipos sin proteger descubiertos. Para ello, es necesario disponer de un equipo descubridor configurado que pueda establecer una conexión con el equipo a instalar.

La instalación remota es compatible con plataformas Windows.

Requisitos de red y sistema operativo

Para poder instalar Panda Endpoint Protection de forma remota, es necesario que los equipos cumplan con los requisitos indicados a continuación:

- Abrir los puertos UDP 21226 y 137 para el proceso `System`.
- Abrir el puerto TCP 445 para el proceso `System`.
- Habilitar el protocolo NetBIOS sobre TCP.
- Permitir las resoluciones DNS.
- Acceso al recurso de administración `Admin$`. En las ediciones "Home" de Windows es necesario habilitar este recurso de forma explícita.
- Credenciales de administrador de dominio o de la cuenta de administrador local generada por defecto en la instalación del sistema operativo.
- Activar la Administración remota.

*Para cumplir con estos requisitos de forma rápida sin necesidad de añadir reglas de forma manual en el firewall de Windows, selecciona **Activar la detección de redes** y **Activar el uso compartido de archivos e impresoras** en Centro de redes y recursos compartidos, Configuración de uso compartido avanzado.*

- Adicionalmente, para que un equipo de la red con Panda Endpoint Protection instalado pueda descubrir a otros equipos es necesario que:
    - No estén ocultos por el administrador.
    - No estén siendo ya administrados por Panda Endpoint Protection sobre Aether Platform.
    - Se encuentren en el mismo segmento de subred al que pertenece el equipo descubridor.

Instalación remota desde el listado de Equipos no administrados descubiertos

- Accede al listado de **Equipos no administrados descubiertos**.
    - Desde el panel lateral **Mis listados**, **Añadir**, selecciona el listado **Equipos no administrados descubiertos**.

  - Desde el menú superior **Estado** en el widget **Estado de la protección**, haz clic en el enlace **Se han descubierto x equipos que no están siendo administrados desde Panda Endpoint Protection**.
  - Desde el menú superior **Equipos** haz clic en **Añadir equipos** y selecciona **Descubrimiento e instalación remota**. Se mostrará una ventana con un asistente. Haz clic en el enlace **Ver equipos no administrados descubiertos**.

- En el listado de **Equipos no administrados descubiertos**, haz clic en **Descubiertos u Ocultos** dependiendo del estado del dispositivo.
- Selecciona las casillas correspondientes a los equipos a instalar.
  - Para instalar varios equipos, haz clic en el menú de contexto general y en **Instalar agente de Panda**.
  - Para instalar un único equipo, haz clic en el menú de contexto del equipo y en **Instalar agente de Panda**.
- Configura la instalación según los pasos descritos en **Generar el paquete de instalación y despliegue manual**.
- Escribe una o varias credenciales de instalación. Es necesario utilizar una cuenta de administración local del equipo o del dominio al que pertenece para completar la instalación con éxito.

Instalación remota desde la pantalla de detalles de equipo

Al hacer clic en un equipo descubierto se mostrará su detalle y en la parte superior el botón **Instalar agente de Panda**. Sigue los pasos descritos en **Generar el paquete de instalación y despliegue manual**.

Diferencias en la instalación según el método de descubrimiento utilizado

El procedimiento para instalar la protección en los equipos seleccionados varía en función del método por el que fueron descubiertos.

Instalar la protección en equipos descubiertos mediante escaneo de red

Cuando un equipo descubre a otro mediante escaneo de red, siempre tiene conexión con éste, de forma que no requiere ninguna configuración adicional con respecto a lo descrito en **Generar el paquete de instalación y despliegue manual**.

- **Si todos los equipos han sido descubiertos por el mismo equipo descubridor**: el equipo descubridor lanzará la instalación sobre todos los equipos descubiertos.
- **Si NO todos los equipos han sido descubiertos por el mismo equipo descubridor**: cada equipo descubridor lanzará la instalación sobre los equipos que hayan sido descubiertos por él.

Instalar la protección en equipos descubiertos mediante directorio activo

Cuando un equipo descubre a otro mediante la búsqueda en directorio activo, no significa necesariamente que tenga conexión con él. En este caso, para hacer una instalación remota del software de seguridad, es imprescindible seleccionar el equipo descubridor que se conectará con él para realizar la instalación.

- Si todos los equipos seleccionados han sido descubiertos solo mediante directorio activo: el administrador deberá seleccionar los equipos instaladores, que lanzarán la instalación sobre los equipos seleccionados.
- Si entre los equipos seleccionados hay alguno o algunos que han sido descubiertos mediante ambos métodos, el administrador deberá seleccionar el equipo descubridor, que lanzará la instalación solo sobre aquellos equipos seleccionados que hayan sido descubiertos exclusivamente mediante directorio activo. Para el resto de equipos la instalación se llevará a cabo de la forma habitual, según lo indicado en **Generar el paquete de instalación y despliegue manual**.

Errores posibles en la instalación

Si el equipo instalador no logra conectarse correctamente al equipo descubierto, se mostrarán los errores de instalación:

- En el listado de equipos no administrados descubiertos: **Error instalando. No es posible conectar con el equipo.** Consulta **Visualizar equipos descubiertos**
- En la ventana **Información de equipo** en la página **251**: **Error instalando el agente de Panda. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota**. Consulta **Descubrimiento de equipos e instalación remota del software cliente** .

Instalación en sistemas Linux

Visión general del despliegue de la protección

El proceso de instalación en equipos Linux comprende varios pasos, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger:

- Localizar los equipos desprotegidos en la red
- Satisfacer los requisitos mínimos
- Desinstalar productos de la competencia y reiniciar equipos
- Establecer la configuración por defecto de los equipos
- Establecer el método de instalación en los equipos
- Comprobar que el software de seguridad se instaló correctamente.

Localizar los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Panda Endpoint Protection, y comprueba que el número de licencias libres contratadas es suficiente. Consulta **Licencias** en la página **185**.

Panda Endpoint Protection permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Satisfacer los requisitos mínimos

Para conocer los requisitos mínimos, consulta **Requisitos de instalación**.

Desinstalar productos de la competencia

Se recomienda desinstalar el antivirus y el software de seguridad de terceras compañías antes de iniciar la instalación de Panda Endpoint Protection.

Establecer la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Panda Endpoint Protection establece las configuraciones por defecto asignadas al grupo **Todos**. En el proceso de despliegue, es posible cambiar el grupo al que pertenecerá el equipo para asignarle otras configuraciones. Consulta **Gestión de configuraciones** en la página **279**.

Comprobar que el software de protección se instaló correctamente

- Selecciona el menú superior **Equipos** y localiza el equipo instalado. Para obtener más información sobre buscar equipos consulta **Gestión de equipos y dispositivos** en la página **209**.
- Haz clic en el equipo en el que has instalado el software de seguridad. Se abrirá la ventana de detalles del equipo.
- Haz clic en la pestaña **Detalles**. Se mostrará toda la información recogida del equipo y el estado de la instalación.
- En la sección **Seguridad** comprueba el estado de los distintos módulos:
    - **Instalando...**: el proceso de instalación no se ha completado o ha terminado en error. Espera unos minutos.
    - **Activado / desactivado:** transcurridos unos minutos, si la instalación terminó correctamente se mostrará el estado de los módulos de protección.

Detectar y solucionar fallos de instalación

Si transcurridos unos minutos la sección **Seguridad** desaparece del detalle del equipo, esto indica que el software de seguridad no se instaló correctamente. Comprueba los siguientes puntos:

- Si el equipo tiene instalada una interface gráfica comprueba si se muestran mensajes de error.
- Comprueba si el equipo se muestra en los listados. Consulta **Comprobar el despliegue**.
- Consulta que el equipo del usuario cumple con los requisitos indicados en **Requisitos de instalación** y actualiza la versión del producto o la versión del sistema operativo. Consulta **Actualización del producto** en la página **201**.

Requisitos de instalación

Para una descripción completa de los requisitos por plataforma, consulta ***Funcionalidades del producto y requisitos*** *en la página* ***619****.*

- **Sistemas operativos 64 bits**: Ubuntu 14.04 LTS y superiores, Fedora 23 y superiores, Debian 8 y superiores, RedHat 6.0 y superiores, CentOS 6.0 y superiores, LinuxMint 18 y superiores, SuSE Linux Enterprise 11.2 y superiores, Oracle Linux 6 y superiores. No requiere sistema de ventanas instalado. Para gestionar el software de seguridad, utiliza la herramienta /usr/local/protection-agent/bin/pa_cmd desde la linea de comandos.
- **Sistemas operativos 32 bits**: RedHat 6.0 a 6.10 y CentOS 6.0 a 6.10.

Para comprobar las versiones del kernel de Linux soportadas en cada distribución, consulta la web de soporte en ***https://www.pandasecurity.com/spain/support/card?id=700009*** *.*

- **Espacio para la instalación**: 500 Mbytes.
- **Puertos**: se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento de la detección web de malware. En equipos sin entorno gráfico, la detección web está deshabilitada.

Para instalar Panda Endpoint Protection en plataformas Linux, es recomendable que el equipo tenga conexión a Internet durante todo el proceso. El script de instalación conectará con los repositorios apropiados dependiendo del sistema (rpm o deb), y se descargarán todos los paquetes necesarios para finalizar la instalación con éxito. Para instalar Panda Endpoint Protection en plataformas Linux aisladas de la red, consulta el apartado **Instalación en plataformas Linux sin conexión a Internet (sin dependencias)**.

Requisitos de red

En su funcionamiento normal, Panda Endpoint Protection accede a varios recursos alojados en Internet. De forma general se requiere acceso a los puertos 80 y 443. Para un listado completo de las URLs a las que se accede desde los equipos con el software Panda Endpoint Protection instalado, consulta **Acceso a URLs del servicio** en la página **637**.

Otros requisitos

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, es muy recomendable que el reloj de los equipos protegidos con Panda Endpoint Protection esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP. Consulta **Sincronización horaria de los equipos (NTP)** en la página **627**.

Acceso al repositorio de la distribución

El proceso de instalación del software de protección tiene como requisito acceder al repositorio donde están almacenados los paquetes de la instalación, siendo el proveedor de la distribución el encargado de mantener al menos un repositorio por cada versión publicada. En muchos casos, al entrar en EOL una versión, el proveedor da de baja el repositorio, con lo que la instalación del software de seguridad fallará. En estos casos se recomienda:

- Utilizar un repositorio local si existe.
- Utilizar la instalación sin dependencias. Consulta **Instalación en plataformas Linux sin conexión a Internet (sin dependencias)**.

Generar el paquete de instalación y despliegue manual

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **Linux**. Se mostrará la ventana **Linux**.

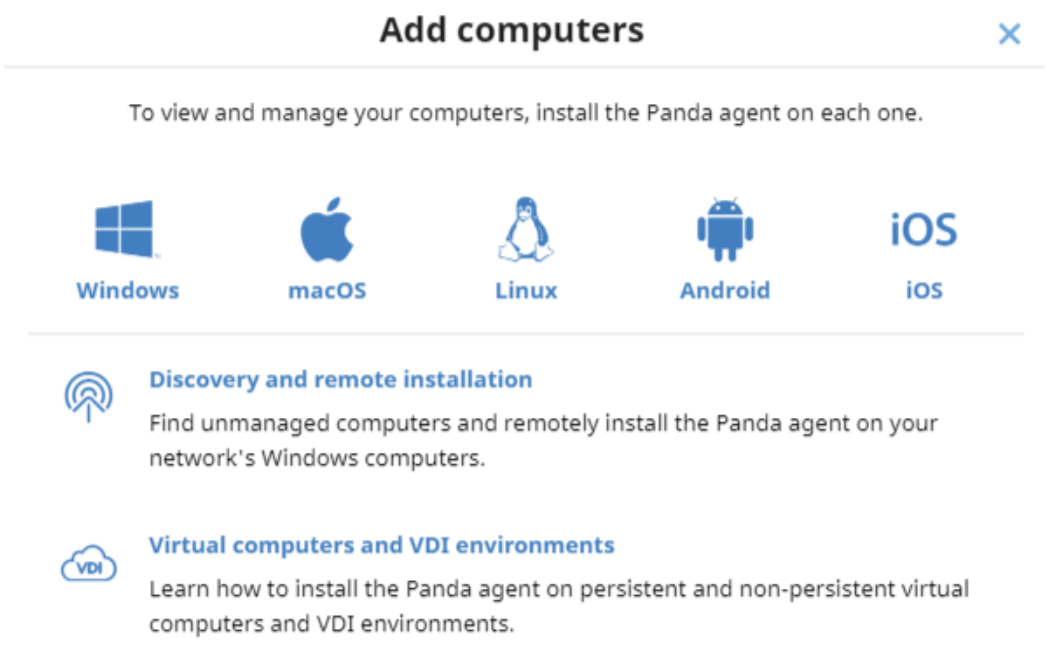


Figura 5.8: Ventana de selección de plataforma compatible con ,Panda Endpoint Protection

- Para elegir el grupo en el que se integrarán los equipos, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Para integrar el equipo en un grupo Directorio Activo, haz clic en **Añadir los equipos en su ruta de Directorio Activo.**

> *Las políticas de seguridad asignadas a un equipo dependen del grupo al que pertenece. Si has elegido **Añadir los equipos en su ruta de Directorio Activo** y el administrador del directorio activo de la empresa mueve el equipo de una unidad organizativa a otra, este cambio se replicará en la consola de Panda Endpoint Protection como un cambio de grupo. Por esta razón, las políticas de seguridad asignadas a ese equipo también podrían cambiar sin ser advertido por el administrador de la consola Web.*

- Para establecer una configuración de red alternativa al grupo donde se integrará el equipo, haz clic en **Selecciona la configuración de red para los equipos** y elige una configuración de red en el desplegable. Inicialmente, todas las configuraciones que se aplican al equipo en el momento de la integración son las que están asignadas al grupo de la consola al que pertenecerá. Sin embargo, para prevenir fallos de conectividad y evitar que el equipo quede inaccesible desde la consola de administración por una configuración de red no apropiada, es posible establecer una configuración de red alternativa. Para más información sobre cómo crear configuraciones de red, consulta

Configuración remota del agente en la página **299**.

- Para enviar el instalador al usuario por correo electrónico:
  - Haz clic en el botón **Enviar URL por email**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador, con un mensaje pregenerado que contiene la URL de descarga.
  - Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.
  - El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo para iniciar la descarga del instalador.
- Para descargar el paquete de instalación y compartirlo con los usuarios de la red, haz clic en el botón **Descargar instalador**.

Instalación en plataformas Linux

Dependiendo de las características del equipo destino, el agente puede instalarse de varias maneras:

- Instalación en plataformas Linux con conexión a Internet
- Instalación en plataformas Linux con Secure Boot
- Instalación en plataformas Linux sin conexión a Internet (sin dependecias)

Instalación en plataformas Linux con conexión a Internet

Instalar el producto en el equipo de usuario requiere permisos de administrador y que el paquete descargado tenga permisos de ejecución. Al ejecutar el programa de instalación, éste localizará en el equipo del usuario todas las librerías que necesita. Las librerías que no consiga encontrar las descargará de Internet de forma automática.

- Abre una terminal en la carpeta donde reside el paquete descargado y ejecuta los comandos siguientes.

```
$ sudo chmod +x "/Ruta descarga/Panda Endpoint Agent.run"
$ sudo "/RutaDescarga/Panda Endpoint Agent.run"
```

- En equipos bastionados utiliza el comando `--target ./install/` para generar una carpeta temporal en la ubicación del script.

```
$ sudo "/RutaDescarga/Panda Endpoint Agent.run" --target ./install/
```

- Si utilizas un servidor proxy para acceder a Internet, añade el parámetro `--proxy`. Si quieres indicar una lista de proxies, utiliza el parámetro `--proxy=<proxy-list>` . El script de instalación utilizará el primer proxy de la lista y, en caso de error, recorrerá la lista de

proxys especificada hasta encontrar uno que funcione correctamente.

`<proxy-list>` es una lista de servidores proxy separadas por comas indicando el usuario y el protocolo con la sintaxis:

```
<http|https>://<user1>:<pass1>@<host1>:<port1>
```

Por ejemplo, para instalar un agente Linux que utilizará dos proxies:

```
$ sudo "/RutaDescarga/Panda Endpoint Agent.run" -- --
proxy=http://user1:pass1@192.168.0.1:3128,
http://user2:pass2@192.168.0.2:3128
```

- Para comprobar que el proceso `AgentSvc` se está ejecutando, utiliza el comando siguiente:

```
$ ps ax | grep AgentSvc
```

- Para comprobar que se han creado los directorios de instalación:

```
/usr/local/management-agent/*
```

Instalación en plataformas Linux con Secure Boot

Algunas distribuciones Linux detectan si el equipo tiene la funcionalidad de Secure Boot activada, que deshabilita el software de protección que no esté debidamente firmado. La presencia de Secure Boot puede ser detectada tanto en el momento de la instalación del software de protección como más adelante, si la distribución originalmente no daba soporte a esta funcionalidad, pero posteriormente se añade en alguna actualización. En ambos casos, se muestra un error en la consola y el software de protección no funcionará. Para habilitar el software de protección en este caso, es necesario seguir el procedimiento y cumplir con los requisitos mostrados a continuación.

Requisitos de la distribución

- **Sistemas DKMS (Dynamic Kernel Module Support)**: paquetes `mokutil` y `openssl` instalados.
- **Oracle Linux 7.x/8.x y kernel UEKR6**: repositorio `ol7_optional_latest` activado y los paquetes `openssl, keyutils, mokutil, pesign, kernel-uek-devel-$(uname -r)` instalados.

Habilitar el software de protección en equipos con Secure Boot activado

Para habilitar el software de protección es necesario seguir el procedimiento mostrado a continuación directamente en el equipo, ya que es necesario interactuar con su sistema de

arranque:

- Comprueba el estado de Secure Boot:

```
$ mokutil --sb-state
```

Si Secure Boot está activado en el equipo se muestra el mensaje `Secure Boot enabled`.

- Verifica que el driver de la protección no está cargado:

```
$ lsmod | grep prot
```

- Importa las claves de la protección:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

*Los ficheros del agente y de la protección tienen el formato **protection-agent-03.01.00.0001-1.5.0_741_g8e14e52**. El nombre varía en función de la versión y del driver.*

Se muestra un mensaje de aviso sobre las implicaciones del uso de Secure Boot.

- Presiona C para registrar el certificado usado para firmar los módulos.
- Genera una contraseña de ocho caracteres.
- Reinicia el equipo y completa el proceso de registro:
    - Presiona cualquier tecla para iniciar el proceso de registro (esta pantalla tiene un tiempo limitado, por lo que si no se presiona ninguna tecla dentro del tiempo definido, habrá que reiniciar el proceso de registro).
    - En el menú, selecciona la opción **Enroll MOK**. Se abrirá un nuevo menú que muestra el número de KEYS que se van a registrar.
    - Selecciona la opción **View key**para revisar que las KEYS son las correspondientes a la protección de Panda Security, y selecciona la opción **Continue** para seguir con el proceso de registro.
    - Cuando aparezca la opción **Enroll the key**, selecciona **Yes**.
    - Escribe la contraseña generada en el paso 3 y reinicia el equipo con la opción **REBOOT**.
    - Comprueba que el driver está cargado:

```
$ lsmod | grep prot
```

Oracle Linux 7.x/8.x con Kernel UEKR6

Una vez terminado el procedimiento general, si la distribución instalada en el equipo es Oracle Linux 7.x/8.x con kernel UEKR6, sigue estos pasos adicionales:

- Vuelve a ejecutar el comando:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

Se añadirá el certificado con el que se firmaron los módulos a la lista de certificados confiables del kernel. Se firmará el kernel modificado y se añadirá a la lista de kernels de GRUB.

- Reinicia el equipo. El módulo estará cargado y arrancado.
- Para comprobar que el certificado se ha añadido correctamente ejecuta el comando:

```
$ sudo /usr/src/protection-agent-<version>/scripts/sb_import_key.sh
```

Se obtiene como resultado:

```
The signer´s common name is UA-MOK Driver Signing
 Image /boot/vmlinuz-<kernel-version>-panda-secure-boot already
signed
 Kernel module succesfully loaded
```

Instalación en plataformas Linux sin conexión a Internet (sin dependencias)

Los servidores o equipos de usuario sin acceso a Internet (ni directo ni a través de un proxy Panda Security o corporativo) pueden completar la instalación del software de seguridad utilizando las librerías incluidas en el propio paquete de distribución de Panda Endpoint Protection. Este método de instalación solo es recomendable en los casos en los que realmente el equipo esté aislado de Internet, ya que si se detectan fallos de seguridad en librerías de terceros incluidas en el paquete de instalación, éstas no serán actualizadas de forma automática.

El instalador sin dependencias es compatible con las siguientes distribuciones:

- Redhat 6, 7, 8.
- CentOS 6, 7, 8.
- SuSE Linux Enterprise 11.2 a 15.2.
- Oracle Linux 6, 7 y 8.

El instalador completo es compatible con las siguientes versiones de agente y protección Linux:

- Protección 3.00.00.0050 y posteriores
- Agente 1.10.06.0050 y posteriores

Si se utiliza la instalación sin dependencias en una distribución no compatible, la instalación dará un error. Este método de instalación solo es posible sobre equipos sin versiones anteriores del software de seguridad. En caso contrario, se mantiene la configuración previa del repositorio.

Para instalar el agente Panda Endpoint Protection abre una terminal en la carpeta donde reside el paquete descargado y ejecuta:

```
$ sudo chmod +x "/Ruta descarga/Panda Endpoint Agent.run"
$ sudo "/DownloadPath/Panda Endpoint Agent.run" -- --no-deps
```

Instalación en sistemas macOS

Visión general del despliegue de la protección

El proceso de instalación en equipos macOS comprende varios pasos, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger :

- Localizar los equipos desprotegidos en la red
- Satisfacer los requisitos mínimos
- Desinstalar productos de la competencia
- Establecer la configuración por defecto de los equipos
- Comprobar que el software de seguridad se instaló correctamente.

Localizar los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Panda Endpoint Protection y comprueba que el número de licencias libres contratadas es suficiente. Consulta **Licencias** en la página **185**.

Panda Endpoint Protection permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Satisfacer los requisitos mínimos

Para conocer los requisitos mínimos consulta **Requisitos de instalación**.

Desinstalar productos de la competencia

Se recomienda desinstalar el antivirus y el software de seguridad de terceras compañías antes de iniciar la instalación de Panda Endpoint Protection.

Establecer la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Panda Endpoint Protection establece las configuraciones por defecto asignadas al grupo **Todos**. En el proceso de despliegue, es posible cambiar el grupo al que pertenecerá el equipo para asignarle otras configuraciones. Consulta **Gestión de configuraciones** en la página **279**.

Comprobar que el software de protección se instaló correctamente

- Selecciona el menú superior **Equipos** y localiza el equipo instalado. Para obtener más información sobre buscar equipos consulta **Gestión de equipos y dispositivos** en la página **209**.
- Haz clic en el equipo en el que has instalado el software de seguridad. Se abrirá la ventana de detalles del equipo.
- Haz clic en la pestaña **Detalles**. Se mostrará toda la información recogida del equipo y el estado de la instalación.
- En la sección **Seguridad** comprueba el estado de los distintos módulos:
    - **Instalando...**: el proceso de instalación no se ha completado o ha terminado en error. Si el proceso terminó en error, el estado no cambiará hasta que se resuelva el problema de instalación.
    - **Activado / desactivado:** transcurridos unos minutos, si la instalación terminó correctamente se mostrará el estado de los módulos de protección.

Detectar y solucionar fallos de instalación

Si transcurridos unos minutos la sección **Seguridad** desaparece del detalle del equipo, esto indica que el software de seguridad no se instaló correctamente. Comprueba los siguientes puntos:

- Comprueba en el equipo del usuario si se muestran mensajes de error.
- Comprueba si el equipo se muestra en los listados. Consulta **Comprobar el despliegue**.
- Consulta que el equipo del usuario cumple con los requisitos indicados en **Requisitos de instalación** y actualiza la versión del producto o la versión del sistema operativo. Consulta **Actualización del producto** en la página **201**.

Requisitos de instalación

Para una descripción completa de los requisitos por plataforma consulta ***Funcionalidades del producto y requisitos*** *en la página* **619**.

- **Sistemas operativos**: macOS 10.10 Yosemite y superiores.
- **Espacio para la instalación**: 400 Mbytes.

Requisitos de red

En su funcionamiento normal Panda Endpoint Protection accede a varios recursos alojados en Internet. De forma general, se requiere acceso a los puertos 80 y 443. Para un listado completo de las URLs a las que se accede desde los equipos con el software Panda Endpoint Protection instalado, consulta **Acceso a la consola web** en la página **637**. Para poder activar el producto es necesario disponer de acceso a ciertos rangos de direcciones IP. Para más información, consulta**Requisitos de plataformas macOS** en la página **629**

Otros requisitos

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, es muy recomendable que el reloj de los equipos protegidos con Panda Endpoint Protection esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP. Consulta **Sincronización horaria de los equipos (NTP)** en la página **627**.

Permisos necesarios

Para el correcto funcionamiento de la protección, es necesario:

- Activar extensiones de red.
- Activar extensiones de sistema.
- Activar el acceso total al disco.
- Activar la ejecución en segundo plano.

Para más información, consulta **Requisitos de plataformas macOS** en la página **629**.

Despliegue manual del agente macOS

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se mostrará una ventana con

las plataformas compatibles con Panda Endpoint Protection.

- Haz clic en el icono **macOS**. Se mostrará la ventana **macOS**.

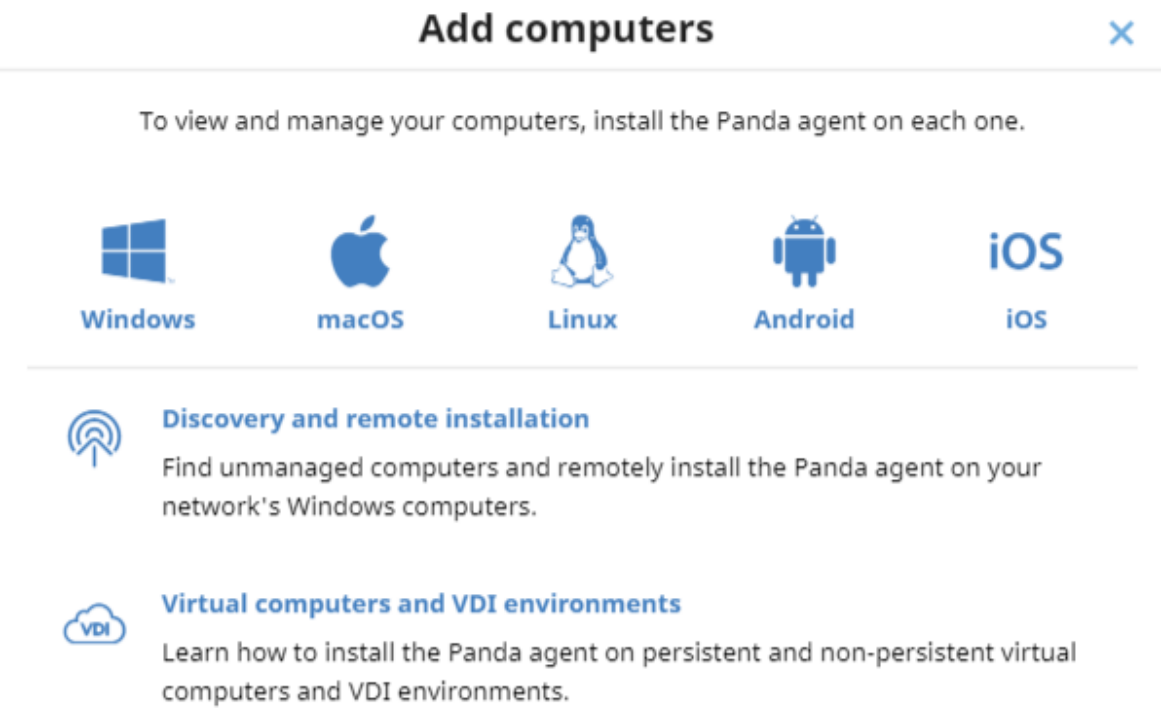


Figura 5.9: Ventana de selección de plataforma compatible con Panda Endpoint Protection

- Para elegir el grupo en el que se integrarán los dispositivos, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Para establecer una configuración de red alternativa al grupo donde se integrará el equipo, haz clic en **Selecciona la configuración de red para los equipos** y elige una configuración de red en el desplegable. Inicialmente, todas las configuraciones que se aplican al equipo en el momento de la integración son las que están asignadas al grupo de la consola al que pertenecerá. Sin embargo, para prevenir fallos de conectividad y evitar que el equipo quede inaccesible desde la consola de administración por una configuración de red no apropiada, es posible establecer una configuración de red alternativa. Para más información sobre cómo crear configuraciones de red, consulta **Configuración remota del agente** en la página **299**.

  Para enviar el instalador al usuario por correo electrónico:

  - Haz clic en el botón **Enviar URL por email**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador con un mensaje ya generado que contiene la URL de descarga.
  - Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.

- El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo para iniciar la descarga del instalador.

- Para descargar el paquete de instalación y compartirlo con los usuarios de la red haz clic en el botón **Descargar instalador (7)**.

Instalación del paquete descargado

- Haz doble clic en el archivo `.dmg` y ejecuta el contenedor `.pkg`. Durante el proceso de instalación se mostrará una ventana con el progreso de la tarea. Independientemente de si existen licencias libres disponibles, el equipo se integrará en el servicio. Si no hay licencias disponibles el equipo no estará protegido.

- Una vez completado, el producto comprobará que tiene la última versión del fichero de firmas y del motor de protección. Si no es así, iniciará una actualización automática.

- Para verificar la instalación del agente, ejecuta el siguiente comando que comprobará si el proceso AgenSvc se está ejecutando:

```
$ ps ax | grep Agent Svc
```

- También puedes comprobar que se han creado los siguientes directorios de instalación:

```
/Applications/Management-Agent.app/
/Library/Application Support/Management Agent/
```

Para instalar el agente del producto en dispositivos con macOS Catalina, es necesario asignar permisos específicos. Para más información, consulta la web ***https://www.pandasecurity.com/es/support/card?id=700079*** .

Instalación en sistemas Android

Visión general del despliegue de la protección

El proceso de instalación en dispositivos Android comprende varios pasos, dependiendo de si están o no gestionados por un MDM / EMM.

MDM (Movile Device Management) / EMM (Enterprise Mobility Management) es un tipo de solución software que monitoriza y administra dispositivos móviles, sin importar el operador de telefonía o el proveedor de servicios elegidos. Las soluciones MDM/ EMM permiten instalar remotamente aplicaciones en los dispositivos gestionados, localizarlos y rastrearlos, sincronizar sus

archivos, y reportar datos de forma remota y centralizada. Este tipo de aplicaciones son frecuentes en empresas que gestionan un gran número de dispositivos.

Para desplegar e instalar con éxito el software de protección, es necesario planificar los siguientes puntos :

- Localizar los dispositivos desprotegidos en la red.
- Satisfacer los requisitos mínimos. Consulta **Requisitos de instalación**.
- Desinstalar productos de la competencia antes de iniciar la instalación de Panda Endpoint Protection.
- Establecer la configuración por defecto de los dispositivos. Consulta **Establecer la configuración por defecto de los equipos**.
- Establecer el procedimiento de despliegue en función de la pertenencia o no de los dispositivos a un MDM / EMM. Consulta **Establecer el procedimiento de despliegue**.

Localizar los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Panda Endpoint Protection, y comprueba que el número de licencias libres contratadas es suficiente. Consulta **Licencias** en la página **185**.

Panda Endpoint Protection permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Establecer la configuración por defecto de los equipos

Para proteger a los equipos de la red desde el primer momento, Panda Endpoint Protection establece configuraciones por defecto asignadas al grupo **Todos**. Sin embargo, en el proceso del despliegue, es posible cambiar el grupo al que pertenecerá el dispositivo para asignarle otras configuraciones. Para crear y asignar nuevas configuraciones, consulta **Gestión de configuraciones** en la página **279**.

Establecer el procedimiento de despliegue

Dependiendo de la integración de los dispositivos en una solución MDM / EMM o no, y de su tipo, se soportan los siguientes tipos de despliegue:

- Despliegue manual sin pertenencia a un MDM / EMM. Consulta **Despliegue e instalación manual del agente Android**.

- Despliegue a través de un MDM / EMM de terceros. Consulta **Despliegue del agente Android desde un MDM/EMM**.

Requisitos de instalación

Dispositivos compatibles

- **Sistemas operativos**: Android 5.0 y superiores.
- **Espacio para la instalación**: 10 Mbytes (dependiendo del modelo de dispositivo se requerirá espacio adicional).

Requisitos de red

Para que las notificaciones push funcionen correctamente desde la red de la empresa, es necesario abrir los puertos 5228, 5229 y 5230 a todo el bloque de IPs ASN 15169 correspondientes a Google.

Permisos requeridos en el dispositivo

Para que todas las características de Panda Endpoint Protection funcionen correctamente en el teléfono móvil, el usuario debe aceptar todos los permisos que la aplicación le solicite. Para obtener un listado completo de los permisos requeridos, consulta **Permisos requeridos en el dispositivo** en la página **634**.

Despliegue e instalación manual del agente Android

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **Android**. Se mostrará la ventana **Android**.

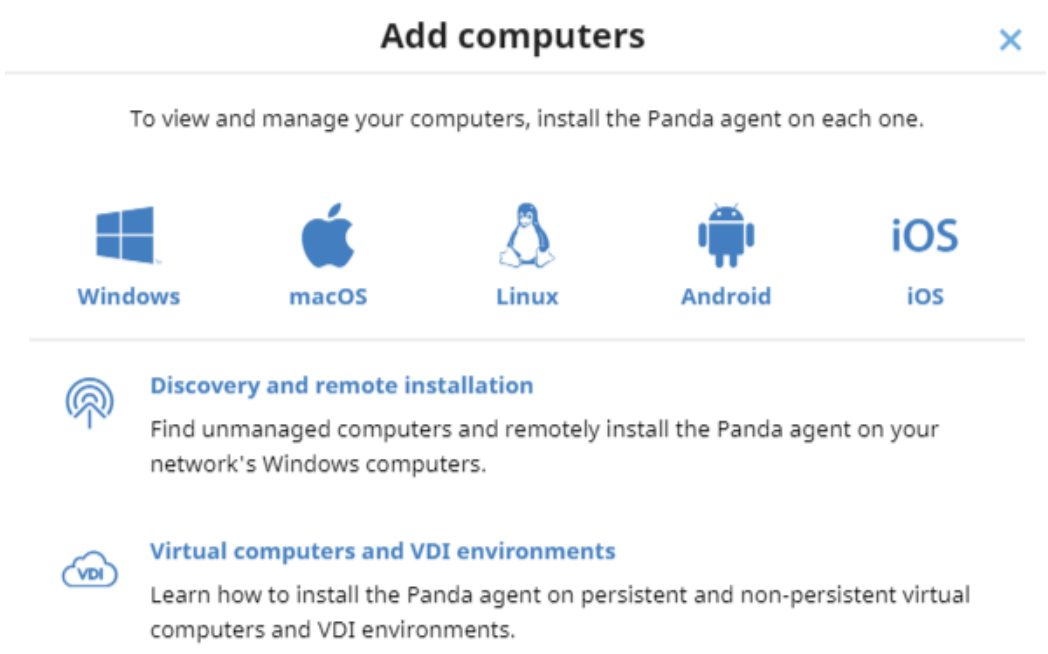


Figura 5.10: Ventana de selección de plataforma compatible con Panda Endpoint Protection

- Para elegir el grupo en el que se integrarán los dispositivos Android, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Para instalar el agente Android en el dispositivo mediante el código QR:
    - Escanea con la cámara del dispositivo el código que se muestra en la ventana. Se mostrará la tienda Google Play con la aplicación **Protection - Panda Aether**.
    - Haz clic en el botón **Instalar**. La aplicación se descargará e instalará de forma automática.
- Para descargar el instalador en el dispositivo directamente desde la Google play.
    - Haz clic en el icono **Acceso a Google Play** desde el propio dispositivo a instalar. Se mostrará la aplicación Google Play con la aplicación **Protection - Panda Aether**.
    - Haz clic en el botón **Instalar**. La aplicación se descargará e instalará de forma automática.
- Para enviar el instalador al usuario por correo electrónico:
    - Haz clic en el botón **Enviar URL por email**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador con un mensaje pregenerado que contiene la URL de descarga.
    - Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.
    - El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo a instalar. Se mostrará la Google Play con la aplicación **Protection - Panda Aether**.

  - El usuario debe hacer clic en el botón **Instalar**. La aplicación se descargará e instalará de forma automática.

- Al iniciarse por primera vez la aplicación en el dispositivo móvil, se mostrará la ventana **Seleccionar alias**.
- Escribe el nombre que se mostrará en la consola Panda Endpoint Protection para representar el dispositivo, y presiona el botón **Continuar**. Se mostrará una serie de mensajes indicando el estado de la instalación y una ventana donde se pide al usuario aceptar una serie de permisos. Si el usuario no acepta estos permisos, la aplicación no funcionará correctamente. Consulta **Permisos requeridos en el dispositivo** en la página **634**.
- Tanto si se aceptan los permisos como si no, la instalación de la aplicación en el dispositivo móvil habrá terminado y se mostrará en la consola de administración de Panda Endpoint Protection.

Despliegue del agente Android desde un MDM/EMM

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **Android**. Se mostrará la ventana **Android**.
- Haz clic en el enlace **Enviar URL por email**. Se abrirá el programa de correo instalado por defecto con un mensaje pregenerado. Anota el enlace para utilizarlo como URL de integración en tu solución MDM/EMM.
- En el MDM/EMM, importa la aplicación **Watchguard Mobile Security** obtenida en la tienda de aplicaciones Play Store.
- En el MDM/EMM añade como parámetros de la aplicación importada en el paso anterior:
  - **Use automatic name**: parámetro de tipo booleano. Si tiene establecido el valor **True** se asignará de forma automática un nombre basado en el patrón "Modelo de dispositivo;identificador único".
  - **Device name**: nombre que se asignará al dispositivo si el parámetro **Use automatic name** tiene asignado el valor **False**. El administrador puede utilizar comodines y otros caracteres especiales atendiendo a las especificaciones del MDM/EMM, para generar nombres diferentes a cada dispositivo.
  - **Integration URL**: URL de integración mostrada en la consola de Panda Endpoint Protection.
- Al iniciarse por primera vez la aplicación en el dispositivo móvil, se mostrará la ventana **Seleccionar alias**.
- Si el parámetro **Use automatic name** está establecido a **False** y **Device name** no se ha definido, la aplicación pedirá el nombre con el que se representará el dispositivo en la

consola Panda Endpoint Protection.

- Pulsa el botón **Continuar**. Se mostrará una serie de mensajes relativos al estado de la instalación y una ventana donde se pide al usuario aceptar una serie de permisos. Si el usuario no acepta estos permisos, la aplicación no funcionará correctamente. Consulta **Permisos requeridos en el dispositivo** en la página **634**.
- Tanto si se aceptan los permisos como si no, la instalación de la aplicación en el dispositivo móvil habrá terminado y se mostrará en la consola de administración de Panda Endpoint Protection.

Instalación en sistemas iOS

Visión general del despliegue de la protección

El proceso de instalación en dispositivos iOS comprende varios pasos, dependiendo de si existe o no una solución MDM (Mobile Device Management) implementada en la empresa:

- Localizar los dispositivos desprotegidos en la red.
- Satisfacer los requisitos mínimos. Consulta **Requisitos de instalación**.
- Desinstalar productos de la competencia antes de iniciar la instalación de Panda Endpoint Protection.
- Establecer la configuración por defecto de los dispositivos. Consulta **Establecer el procedimiento de despliegue**.
- Establecer el procedimiento de despliegue en función de la pertenencia o no de los dispositivos a un MDM. Consulta **Establecer el procedimiento de despliegue**.

Localizar los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Panda Endpoint Protection, y comprueba que el número de licencias libres contratadas es suficiente. Consulta **Licencias** en la página **185**.

Panda Endpoint Protection permite la instalación del software sin tener contratadas licencias suficientes. Estos equipos serán visibles en la consola de administración y mostrarán el software instalado, hardware y otras características, pero no estarán protegidos frente al malware.

Establecer la configuración por defecto de los equipos

Para proteger a los equipos de la red desde el primer momento, Panda Endpoint Protection establece configuraciones por defecto asignadas al grupo **Todos**. Sin embargo, en el proceso del

despliegue, es posible cambiar el grupo al que pertenecerá el dispositivo para asignarle otras configuraciones. Para crear y asignar nuevas configuraciones, consulta **Gestión de configuraciones** en la página **279**.

Establecer el procedimiento de despliegue

El procedimiento de despliegue del agente iOS varía en función de si el dispositivo será gestionado por un MDM, o si se trata de un dispositivo supervisado.

- Despliegue manual sin pertenencia a un MDM. Consulta **Despliegue e instalación en dispositivos sin integración en MDM**.
- Despliegue a través del MDM de Panda. Consulta **Despliegue e instalación en dispositivos integrados en el MDM de Panda**.
- Despliegue a través de un MDM de terceros. Consulta **Despliegue e instalación en dispositivos integrados en un MDM de terceros**.
- Despliegue en dispositivos supervisados con Panda MDM. Consulta **Establecer el modo supervisado e integrar el dispositivo en Panda MDM**.
- Despliegue en dispositivos supervisados con MDM de terceros. Consulta **Establecer el modo supervisado y distribuir el agente iOS desde un MDM de terceros**.

Para obtener más información sobre los posibles escenarios en Panda Endpoint Protection, consulta **Conceptos básicos**.

Si el dispositivo será gestionado por el MDM de Panda, consulta **Gestionar el ID de Apple y los certificados digitales**.

Conceptos básicos

MDM (Mobile Device Management)

Es un tipo de solución software que monitoriza y administra dispositivos móviles, sin importar el operador de telefonía o el proveedor de servicios elegidos. La mayoría de las soluciones MDM permiten instalar remotamente aplicaciones en dispositivos iOS, localizar y rastrearlos, sincronizar sus archivos, y reportar datos de forma remota y centralizada. Este tipo de aplicaciones son frecuentes en empresas que gestionan un gran número de dispositivos.

Administración de dispositivos iOS con soluciones MDM

Un dispositivo iOS solo puede ser administrado remotamente por un MDM en un momento determinado. La pertenencia del dispositivo a un MDM se establece en el proceso de integración, al final del cual se envía desde el MDM un perfil de configuración al dispositivo, que el usuario instala en el terminal.

PandaMDM

Dado que las capacidades de administración remota de un dispositivo iOS son muy inferiores si el dispositivo no está integrado en un MDM, Panda Endpoint Protection incorpora de forma transparente su propio MDM en la consola de administración. Como cada dispositivo iOS solo puede gestionarse desde un único MDM, es importante tomar la decisión correcta sobre qué MDM gestionará los dispositivos de la empresa a la hora de decidir el tipo de integración a implementar en Panda Endpoint Protection.

> *Si tus dispositivos iOS ya están integrados en un MDM de terceros y decides integrarlos en el MDM de Panda, perderás las capacidades de gestión centralizada ofrecidas por tu MDM y el acceso a todo el software que hayas distribuido a través de él. Consulta* ***Tipos de integraciones disponibles en Panda Endpoint Protection****.*

Tipos de integraciones soportadas en Panda Endpoint Protection

Dependiendo del tipo de integración, Panda Endpoint Protection pone a disposición del administrador un juego más o menos amplio de funcionalidades desde su consola.

Tipo de integración	Funcionalidades disponibles en la consola Panda Endpoint Protection
Instalación con integración en MDM Panda (recomendada si no utilizabas un MDM previamente)	• Inventario de hardware • Inventario de software • Protección web * • Filtrado web * • Geolocalización • Alarma remota • Borrar datos • Bloquear
Instalación con integración en MDM de terceras compañías (recomendada si ya utilizas un MDM)	• Inventario de hardware • Protección web * • Filtrado web * • Geolocalización • Alarma remota
Instalación sin integración en MDM	• Inventario de hardware

Tipo de integración	Funcionalidades disponibles en la consola Panda Endpoint Protection
	• Geolocalización • Alarma remota

Tabla 5.9: Tipos de integraciones disponibles en Panda Endpoint Protection

* Para filtrar el tráfico web es necesario que el dispositivo iOS esté en modo supervisado.

Requisitos de integración con Panda MDM

Para integrar un dispositivo iOS en la consola de administración de Panda Endpoint Protection y utilizar el MDM de Panda es necesario:

- **Una cuenta de usuario de Apple (ID de Apple)**: requerida para poder generar e importar el certificado en la consola de administración. Puedes utilizar una cuenta ya existente o crear una nueva.
- **Un certificado digital emitido por Apple**: necesario para que los dispositivos iOS a gestionar se comuniquen con los servidores de Apple de forma segura. El certificado digital tiene una validez de 1 año, transcurrido el cual caducará. Registra todos los dispositivos iOS de tu empresa con el mismo certificado digital.

Para obtener mas información consulta **Gestionar el ID de Apple y los certificados digitales**.

Requisitos de instalación

Versiones de iOS compatibles

- iOS 13 / iPadOS 13
- iOS 14 / iPadOS 14
- iOS 15 / iPadOS 15

Requisitos hardware

Se requiere un mínimo de 12 megabytes de espacio en la memoria interna del dispositivo.

Requisitos de red

La aplicación instalada en el dispositivo móvil utiliza el servicio de notificaciones push de Apple (APNs, Apple Push Notification Service) para comunicarse con Panda Endpoint Protection. En condiciones normales, si el dispositivo está conectado a la red de telefonía por 2G/3G/4G y superiores no es necesario cumplir ningún requisito de red específico. Para otros escenarios, consulta **Requisitos de plataformas iOS** en la página **634**.

Permisos requeridos en el dispositivo

Para que todas las características de Panda Endpoint Protection funcionen correctamente en el teléfono móvil, el usuario debe aceptar todos los permisos que la aplicación le solicite. Para obtener un listado completo de los permisos requeridos, consulta **Permisos requeridos en el dispositivo** en la página **635**.

Despliegue e instalación del agente iOS

Despliegue e instalación en dispositivos sin integración en MDM

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos** situado en la parte superior derecha de la pantalla. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.

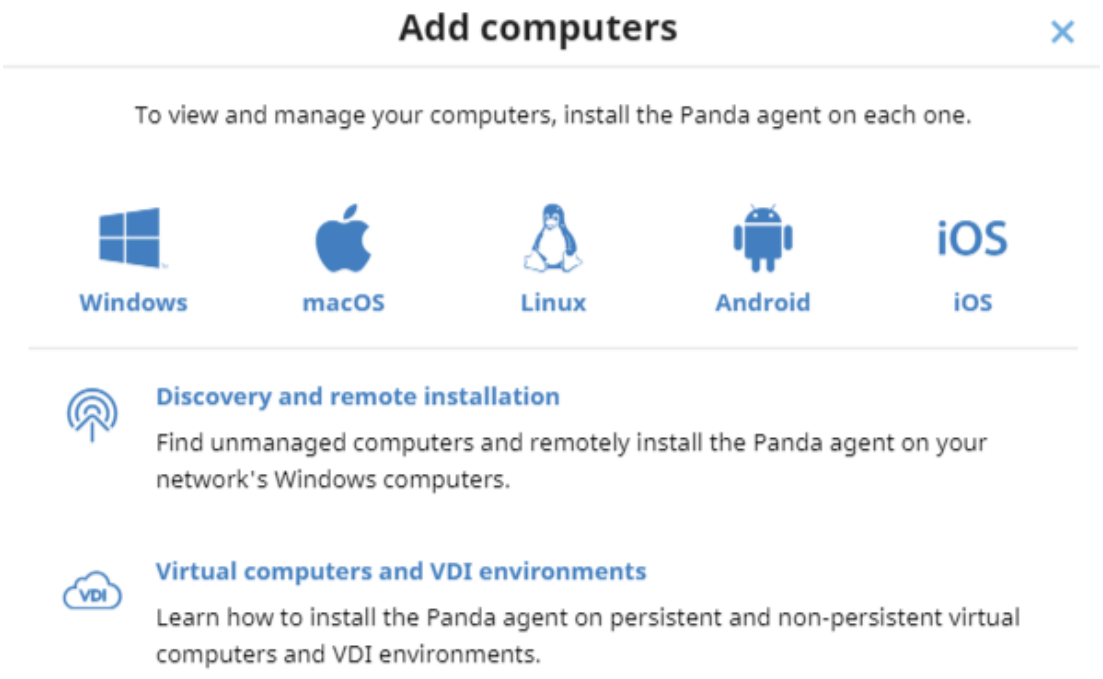


Figura 5.11: Ventana de selección de plataforma compatible con Panda Endpoint Protection

- Haz clic en el icono **iOS**. Se mostrará la ventana **iOS**.
- Haz clic en el enlace **Instalación sin MDM**. Se mostrará la ventana **iOS**.
- Para elegir el grupo en el que se integrarán los dispositivos iOS, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Para instalar el agente iOS en el dispositivo mediante el código QR:
    - Escanea con la cámara del dispositivo el código que se muestra en la ventana. Se mostrará la tienda Apple Store con la aplicación **WatchGuard Mobile Security**.

    - Haz clic en el botón **Instalar**. La aplicación se descargará e instalará de forma automática.

- Para descargar el instalador en el dispositivo directamente desde la Apple Store.
    - Haz clic en el icono **Acceso al Apple Store** desde el propio dispositivo a instalar. Se mostrará la aplicación Apple Store con la aplicación **WatchGuard Mobile Security**.
    - Pulsa el botón **Instalar**. La aplicación se descargará e instalará de forma automática.
- Para enviar el instalador al usuario por correo electrónico:
    - Haz clic en el botón **Enviar URL por email**. Se mostrará la aplicación de correo instalada por defecto en el equipo del administrador con un mensaje pregenerado que contiene la URL de descarga.
    - Añade al mensaje los destinatarios de correo y haz clic en el botón **Enviar**.
    - El usuario que reciba el correo deberá hacer clic en la URL desde el dispositivo a instalar. Se mostrará la Apple Store con la aplicación **WatchGuard Mobile Security**.
    - El usuario debe hacer clic en el botón **Instalar**. La aplicación se descargará e instalará de forma automática.
- En el dispositivo iOS, al iniciarse por primera vez la aplicación, se mostrará la ventana de bienvenida y nos mostrará el dialogo **"Watchguard Mobile Security" quiere enviarte notificaciones**. Pulsa el botón **Permitir**.
- Si la aplicación **WatchGuard Mobile Security**fue instalada buscándola de forma manual en la Apple Store, es necesario integrarla manualmente en Panda Endpoint Protection:
    - Pulsa el botón **Use QR Code**. Se mostrará la ventana **"Watchguard Mobile Security" quiere acceder a la cámara**.
    - Pulsa el botón **Permitir** y apunta la cámara del teléfono móvil al código QR mostrado en la consola de Panda Endpoint Protection. En el teléfono móvil se mostrará el mensaje **Descargando configuración**.
- Cuando la configuración se termina de descargar, se muestra la ventana **"Watchguard Mobile Security" quiere buscar dispositivos en tu red local y conectarse a ellos**. Pulsa el botón **Ok**. Se mostrará la ventana **Introduce el alias**.
- Introduce el nombre que se mostrará en la consola Panda Endpoint Protection para representar el dispositivo, y pulsa el botón **Continua**. Se mostrará una serie de mensajes de estado de la instalación y la ventana **"Watchguard Mobile Security" quiere filtrar contenido de la red**.
- Pulsa el botón **Permitir**. Se mostrará la ventana **Introduce el código del iPhone**.
- Escribe la contraseña del dispositivo. Se mostrará la ventana **Correcto** y la instalación habrá finalizado.

Despliegue e instalación en dispositivos integrados en el MDM de Panda

- Comprueba que tienes un certificado Apple válido y cargado en la consola de administración de Panda Endpoint Protection. Para generar un certificado, consulta **Crear e importar el certificado digital en la consola Panda Endpoint Protection**. Si tu certificado está a punto de caducar, consulta **Renovar el certificado de Apple**.
- Comprueba que los dispositivos iOS de la empresa no tienen un perfil MDM de terceras compañías previamente instalado. Si es así, borra el perfil de los dispositivos. Para conocer las implicaciones de borrar un perfil MDM de terceras compañías, consulta **Administración de dispositivos iOS con soluciones MDM** y **Tipos de integraciones soportadas en Panda Endpoint Protection**.
- En el menú superior **Equipos** de la consola de administración de Panda Endpoint Protection, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **iOS**. Se mostrará la ventana **iOS** con información del certificado previamente cargado.

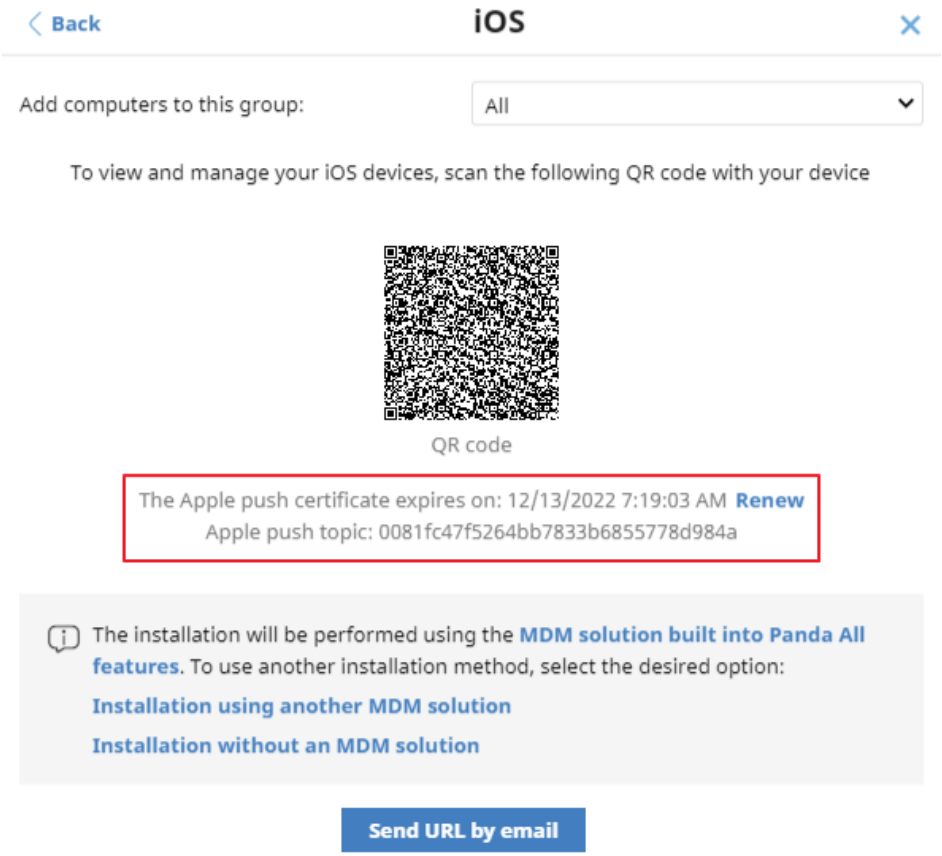


Figura 5.12: Ventana con el certificado digital de Apple ya cargado

- Para elegir el grupo en el que se integrarán los dispositivos iOS, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Elige el método para enviar el perfil de instalación al dispositivo iOS:
    - Para enviar el perfil de instalación mediante el código QR, escanea con la cámara del dispositivo el código. Se mostrará una ventana con el mensaje **Este sitio esta intentando descargar un perfil de configuración. ¿Quieres permitirlo?**.
    - Para enviar por correo el enlace de descarga del perfil de instalación al usuario, haz clic en el botón **Enviar URL por email**. Al pulsar en dispositivo del usuario el enlace se mostrará una ventana con el mensaje **Este sitio web esta intentando descargar un perfil de configuración. Quieres permitirlo?**.
- Pulsa **Permitir**. Una vez descargado el perfil en el dispositivo iOS, se mostrará la ventana **Perfil descargado**.
- Pulsa en la aplicación **Ajustes** del dispositivo iOS. Se mostrará la ventana **Ajustes**.
- Pulsa la opción **General**. Se mostrará la ventana **General**.
- Pulsa en la opción **VPN y gestión de dispositivos**. Se mostrará el perfil descargado **Watchguard MDM Service**.
- Pulsa en la entrada **Watchguard MDM Service**. Se mostrará la ventana **Instalar perfil** con información de seguridad del fichero descargado.
- Pulsa en el enlace **Instalar** situado en la parte superior derecha de la pantalla. Se pedirá la contraseña del teléfono.
- Introduce la contraseña. Se mostrará la ventana **Aviso** indicando que el dispositivo pasará a ser gestionado remotamente.
- Pulsa en el enlace **Instalar** situado en la parte superior derecha de la pantalla. Se mostrará la ventana **Gestión remota**.
- Pulsa en **Confiar**. El perfil se instalará y al cabo de unos minutos se mostrará una notificación en el dispositivo para descargar e instalar el agente Panda Endpoint Protection de forma automática.
- Pulsa el botón **Instalar** en la notificación. La aplicación se descargará e instalará en el dispositivo.
- Una vez descargada e instalada la aplicación, pulsa sobre ella para ejecutarla por primera vez. Se mostrará la ventana **"Watchguard Mobile Security" quiere enviarte notificaciones**.
- Pulsa el botón **Permitir**. El dispositivo comenzará a integrarse en la consola de Panda Endpoint Protection y se mostrará la ventana **Introduce el código del iPhone**.
- Escribe la contraseña del dispositivo. Se mostrará la ventana **Correcto** y la configuración habrá finalizado.

Despliegue e instalación en dispositivos integrados en un MDM de terceros

Los procedimientos referidos al software MDM mostrados en este apartado varían dependiendo del proveedor utilizado. Consulta la ayuda del producto para obtener más información.

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **iOS**. Se mostrará la ventana **iOS**.
- Haz clic en el enlace **Instalación mediante otro MDM**. Se mostrará la ventana **iOS - Otro MDM** con la información que el MDM necesitará para integrar el dispositivo.

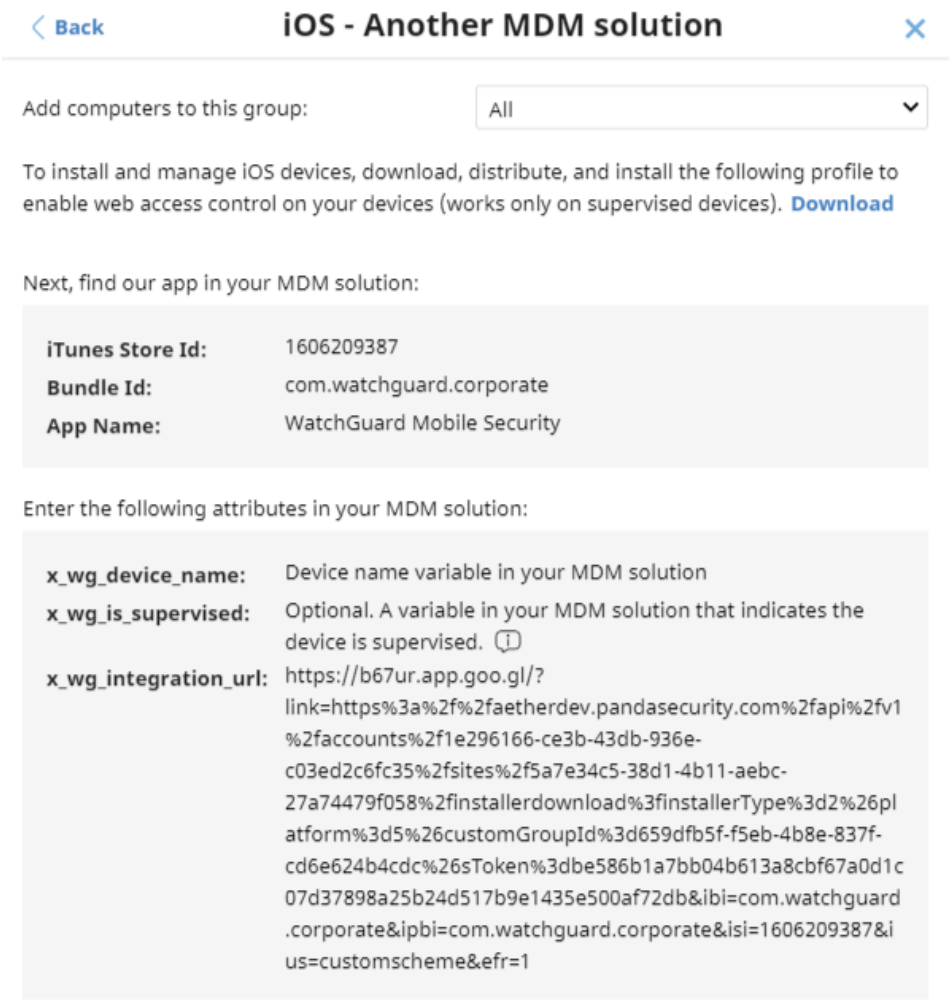


Figura 5.13: Ventana con los parámetros de integración para el MDM de terceros

- En el MDM de terceros, importa la aplicación **Watchguard Mobile Security** directamente desde la Apple Store. Utiliza para ello los campos **iTunes Store Id**, **Bundle Id** o **App Name** de la figura **Ventana con los parámetros de integración para el MDM de terceros** o las funcionalidades de búsqueda integradas en el propio MDM.
- Asocia y define los parámetros **x_wg_device_name**y **x_wg_integration_url** en la aplicación **Watchguard Mobile Security** importada en el repositorio del MDM de terceros. La información contenida en estos parámetros se enviará junto a la aplicación **Watchguard Mobile Security** cuando el administrador la empuje a los dispositivos administrados con el MDM:
    - **x_wg_device_name**: contiene el nombre del dispositivo que se mostrará en la consola Panda Endpoint Protection. Introduce en el parámetro **x_wg_device_name** la variable utilizada por el MDM que representa el nombre del dispositivo que recibirá la aplicación **Watchguard Mobile Security**.
    - **x_wg_integration_url**: contiene la URL que apunta a la información que necesita **Watchguard Mobile Security** para integrarse en el grupo elegido por el administrador de Panda Endpoint Protection. Copia el contenido de **x_wg_integration_url** mostrado en la consola de Panda Endpoint Protection en el parámetro definido en el MDM.

Cada MDM utiliza nombres de variables y sintaxis diferentes, consulta la documentación de tu producto para obtener esta información.

*Utiliza una variable en el parámetro x_wg_device_name. Si en vez de la variable que representa al nombre del dispositivo introduces un nombre de dispositivo directamente, todos los terminales móviles que reciban **Watchguard Mobile Security** se mostrarán en la consola de Panda Endpoint Protection con el mismo nombre.*

- Empuja la aplicación Watchguard Mobile Security desde el MDM a los dispositivos que deseas proteger. Al cabo de unos minutos se mostrará una notificación en el dispositivo para descargar e instalar el agente Panda Endpoint Protection de forma automática.
- Pulsa el botón **Instalar** en la notificación. La aplicación se descargará e instalará en el dispositivo.
- Una vez descargada e instalada la aplicación, pulsa sobre ella para ejecutarla por primera vez. Se mostrará la ventana **"Watchguard Mobile Security" quiere enviarte notificaciones**.
- Pulsa el botón **Permitir**. El dispositivo comenzará a integrarse en la consola de Panda Endpoint Protection y se mostrará la ventana **Introduce el código del iPhone**.

- Escribe la contraseña del dispositivo. Se mostrará la ventana **Correcto** y la configuración habrá finalizado.

Despliegue e instalación en dispositivos supervisados

Es necesario configurar los dispositivos iOS en modo supervisado para poder utilizar las capacidades de filtrado de URLs de Panda Endpoint Protection.

> *Activar el modo supervisado implica restaurar los valores de fábrica del dispositivo iOS. Todos los datos, programas y configuraciones almacenadas en el teléfono móvil se perderán. Restaurar a valores de fábrica nuevamente eliminará el modo supervisado del dispositivo.*

Conceptos

Modo supervisado

Es un modo de ejecución para dispositivos iOS utilizados en entornos corporativos, y que dota al administrador de una mayor flexibilidad en la configuración de aplicaciones y en la gestión del propio dispositivo. En el modo supervisado, el administrador puede aplicar en el primer inicio del dispositivo y antes de su activación, perfiles de configuración para aplicaciones y recursos del teléfono móvil , así como programar la instalación de aplicaciones o imponer restricciones a su uso. Para establecer un dispositivo iOS en modo supervisado es necesario conectarlo a un equipo con sistema operativo macOS mediante un cable USB.

Apple configurator 2

Es la aplicación que se ejecuta en el equipo macOS y permite establecer el modo supervisado en el dispositivo iOS.

Finder

Es el explorador de archivos nativo de macOS. Se utiliza para realizar la copia de seguridad completa del dispositivo iOS y su posterior restauración.

iCloud

Servicio de almacenamiento en la nube. Mediante el appleID, el usuario puede acceder online a sus documentos, fotografías, calendarios y otros recursos sin necesidad de almacenarlos en el dispositivo móvil.

Proyecto

Es el contenedor que almacena el conjunto de aplicaciones que se quieren enviar al dispositivo para configurarlo. Además, en el proyecto se establece la pertenencia o no del dispositivo a un MDM, y se permite activar o desactivar parte del asistente de configuración que se le muestra al usuario la primera vez que enciende el dispositivo.

Requisitos

- Equipo con macOS 10.15.6 o posterior.
- Aplicación Apple Configurator 2. Descárgala gratuitamente en **https://apps.apple.com/es/app/apple-configurator-2/id1037126344?mt=12**
- Cable USB para conectar el dispositivo iOS al equipo macOS.
- Para activar las capacidades de filtrado web en dispositivos iOS supervisados e integrados con un MDM de terceros, es necesario que éste permita importar perfiles externos. Comprueba si tu MDM soporta esta funcionalidad antes de iniciar el procedimiento descrito en este apartado.
- **Opcional**: aplicación Finder para hacer una copia de seguridad en caso de ser necesario y restaurarla. Consulta **Procedimiento para no perder datos del dispositivo iOS al activar el modo supervisado**.

Establecer el modo supervisado e integrar el dispositivo en Panda MDM

El proceso para activar el modo supervisado se ejecuta de forma independiente al proceso de integración con Panda MDM.

Al activar el modo supervisado, todos los datos y aplicaciones contenidos en el dispositivo iOS se borran. Para hacer una copia de seguridad previa y restaurar los datos una vez terminado el procedimiento, consulta **Procedimiento para no perder datos del dispositivo iOS al activar el modo supervisado**.

Para comprobar que el dispositivo iOS está en modo supervisado, consulta **Comprobar que el dispositivo está supervisado**.

Crear el proyecto

- En el equipo macOS abre la aplicación Apple configurator 2 y haz clic en el menú superior **Archivo** y **Nuevo proyecto**. Se mostrará la ventana **Todos los proyectos** con los proyectos creados, y el nuevo seleccionado de forma automática.
- Escribe el nombre del nuevo proyecto y pulsa Enter.

Obtener la URL de integración de Panda Endpoint Protection MDM

- Comprueba que tienes un certificado Apple válido y cargado en la consola de administración de Panda Endpoint Protection. Para generar un certificado, consulta **Crear e importar el certificado digital en la consola Panda Endpoint Protection**. Si tu certificado está a punto de caducar, consulta **Renovar el certificado de Apple**.
- Comprueba que los dispositivos iOS de la empresa no tienen un perfil MDM de terceras compañías previamente instalado. Si es así, borra el perfil de los dispositivos. Para conocer las implicaciones de borrar un perfil MDM de terceras compañías, consulta **Administración**

de dispositivos iOS con soluciones MDM y Tipos de integraciones soportadas en Panda Endpoint Protection.

- En el menú superior **Equipos** de la consola de administración de Panda Endpoint Protection, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **iOS**. Se mostrará la ventana **iOS** con información del certificado previamente cargado.

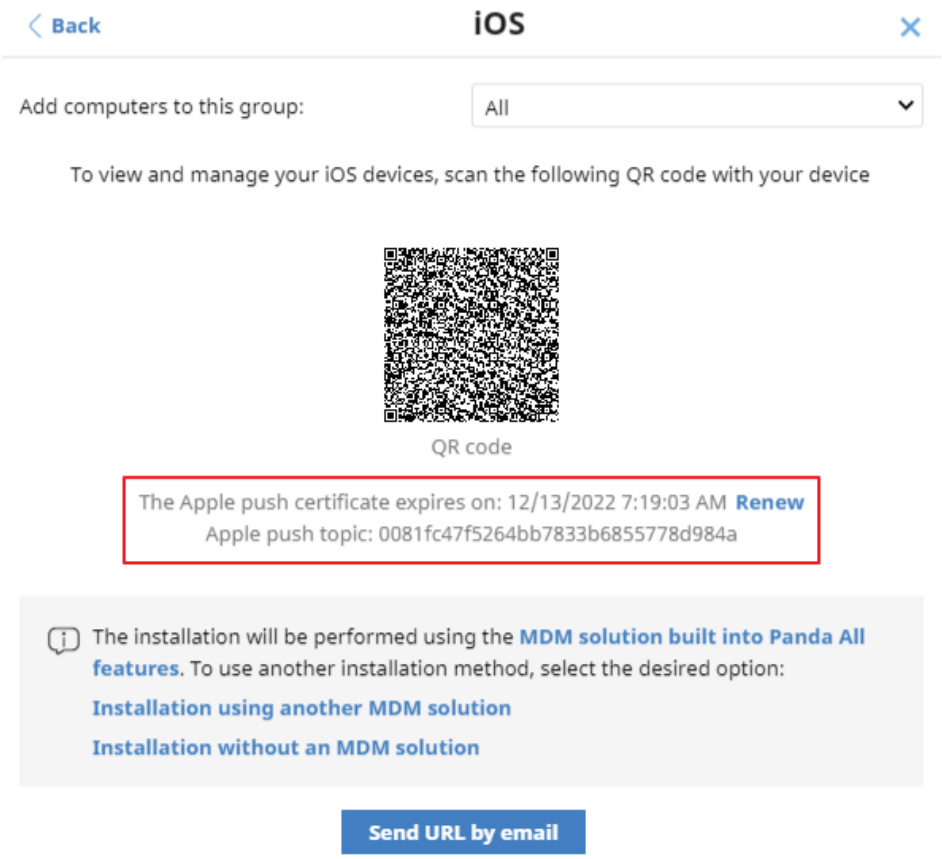


Figura 5.14: Ventana con el certificado digital de Apple ya cargado

- Para elegir el grupo en el que se integrarán los dispositivos iOS, haz clic en el desplegable **Añadir los equipos al siguiente grupo**.
- Haz clic en el botón **Enviar URL por email**. Se abrirá el programa de correo instalado en el equipo.
- Escribe la dirección de correo del usuario que utilizará el dispositivo iOS a integrar y haz clic en **Enviar**.

Preparar el dispositivo

- En la aplicación Apple configurator 2, selecciona el proyecto creado y haz clic en el botón **Preparar** de la barra superior. Se abrirá la ventana **Preparar dispositivos**.

- En **Preparar con** selecciona **Configuración manual**, **Supervisar dispositivos** y **Permitir a los dispositivos enlazarse con otros ordenadores**, y haz clic en el botón **Siguiente**. Se mostrará la ventana **Inscríbelos en un servidor MDM**.
- En **Servidor** selecciona **No inscribir en MDM** y haz clic en el botón **Siguiente**. Se mostrará la ventana **Inicia sesión en Apple School Manager o en Apple Business Manager**.
- Haz clic en el botón **Omitir**. Se mostrará la ventana **Asígnaselos a una organización**.
- Escribe la información de tu empresa y haz clic en el botón **Siguiente**.
- Haz clic en la opción **Crear una identidad de supervisión nueva** y haz clic en el botón **Siguiente**. Se mostrará la ventana **Configura el asistente de iOS**.
- Selecciona los pasos del asistente de configuración que se mostrarán al usuario la primera vez que encienda el dispositivo iOS y haz clic en el botón **Preparar**. Se mostrará una ventana pidiendo las credenciales del administrador del equipo macOS.
- Haz clic en el botón **Actualizar configuración**. Se abrirá una ventana emergente con el estado de la configuración.
- Una vez terminado el procedimiento, el proyecto estará creado y listo para aplicar a todos los dispositivos iOS necesarios.

Aplicar el proyecto al dispositivo iOS

Es requisito indispensable desactivar la opción Find my iPhone para integrar correctamente un dispositivo iOS supervisado en un MDM.

- Desactiva **Buscar mi iPhone** en el dispositivo iOS del usuario:
  - Pulsa **Ajustes**.
  - Pulsa en el nombre del usuario y en **Buscar mi**.
  - Pulsa **Buscar mi iPhone** y luego pulsa para desactivar esta opción.
  - Escribe la contraseña del ID de Apple.
  - Pulsa **Desactivar**.
- Conecta el dispositivo iOS al equipo macOS por USB con la aplicación Apple Configurator 2 abierta. Se mostrará el mensaje **Confiar en este ordenador?** en el dispositivos móvil.
- Pulsa **Confiar** en el dispositivo móvil.
- En la aplicación Apple Configurator 2 haz clic en el botón **Todos los dispositivos** de la barra superior. Se mostrará el dispositivo conectado.
- Haz clic con el botón derecho del ratón sobre el dispositivo. Se mostrará un menú desplegable.

- Haz clic en **Aplicar** y selecciona el proyecto creado. Se mostrará una ventana emergente para confirmar la configuración del dispositivo.
- Si pulsas en **Aplicar** se ejecutarán las siguientes acciones en el dispositivo iOS:
    - Se restablecerá a su configuración original de fábrica.
    - Se borrarán todos los datos y aplicaciones previamente almacenadas.
    - Se activará el modo supervisado.

Comprobar que el dispositivo está supervisado

- Haz clic en el botón **Supervisado** de la barra superior. Apple Configurator 2 mostrará el nuevo dispositivo supervisado.
- Pulsa **Ajustes** en el dispositivo iOS. En la parte superior izquierda, debajo del nombre del teléfono móvil, se mostrará "Este iPhone está supervisado y gestionado por (Nombre de la compañía)."

Integrar el dispositivo supervisado en Panda MDM

- Configura la aplicación de correo en el dispositivo iOS supervisado y descarga el mensaje que contiene la URL de integración con el MDM enviado previamente desde la consola de Panda Endpoint Protection.
- Al pulsar en el enlace se mostrará una ventana con el mensaje **Este sitio web esta intentando descargar un perfil de configuración. Quieres permitirlo?**.
- Pulsa **Permitir**. Una vez descargado el perfil en el dispositivo iOS, se mostrará la ventana **Perfil descargado**.
- Pulsa en la aplicación **Ajustes** del dispositivo iOS. Se mostrará la ventana **Ajustes**.
- Pulsa la opción **General**. Se mostrará la ventana **General**.
- Pulsa en la opción **VPN y gestión de dispositivos**. Se mostrará el perfil descargado **Watchguard MDM Service**.
- Pulsa en la entrada **Watchguard MDM Service**. Se mostrará la ventana **Instalar perfil** con información de seguridad del fichero descargado.
- Pulsa en el enlace **Instalar** situado en la parte superior derecha de la pantalla. Se pedirá la contraseña del teléfono.
- Introduce la contraseña. Se mostrará la ventana **Aviso** indicando que el dispositivo pasará a ser gestionado remotamente.
- Pulsa en el enlace **Instalar** situado en la parte superior derecha de la pantalla. Se mostrará la ventana **Gestión remota**.
- Pulsa en **Confiar**. El perfil se instalará y al cabo de unos minutos se descargará e instalará el agente Panda Endpoint Protection de forma automática.

- Una vez descargada e instalada la aplicación, pulsa sobre ella para ejecutarla por primera vez. Se mostrará la ventana **"Watchguard Mobile Security" quiere enviarte notificaciones**.
- Pulsa el botón **Permitir**. El dispositivo comenzará a integrarse en la consola de Panda Endpoint Protection y la configuración habrá finalizado.

Establecer el modo supervisado y distribuir el agente iOS desde un MDM de terceros

Las distintas soluciones MDM disponibles en el mercado soportan diferentes métodos para establecer el modo supervisado en los dispositivos iOS. Consulta la documentación de tu MDM para establecer el modo supervisado de los dispositivos iOS integrados.

Para establecer Watchguard Mobile Security como la aplicación encargada del filtrado web en el dispositivo iOS, es necesario que el MDM utilizado permita importar perfiles de configuración externos. Comprueba si tu MDM soporta esta funcionalidad antes de iniciar el procedimiento descrito en este apartado.

Distribuir la aplicación Watchguard Mobile Security usando un MDM de terceros

Los procedimientos referidos al software MDM mostrados en este apartado varían dependiendo del proveedor utilizado. Consulta la ayuda del producto para obtener más información.

- En el menú superior **Equipos** de la consola de administración, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **iOS**. Se mostrará la ventana **iOS**.
- Haz clic en el enlace **Instalación mediante otro MDM**. Se mostrará la ventana **iOS - Otro MDM** con la información que el MDM necesitará para integrar el dispositivo.

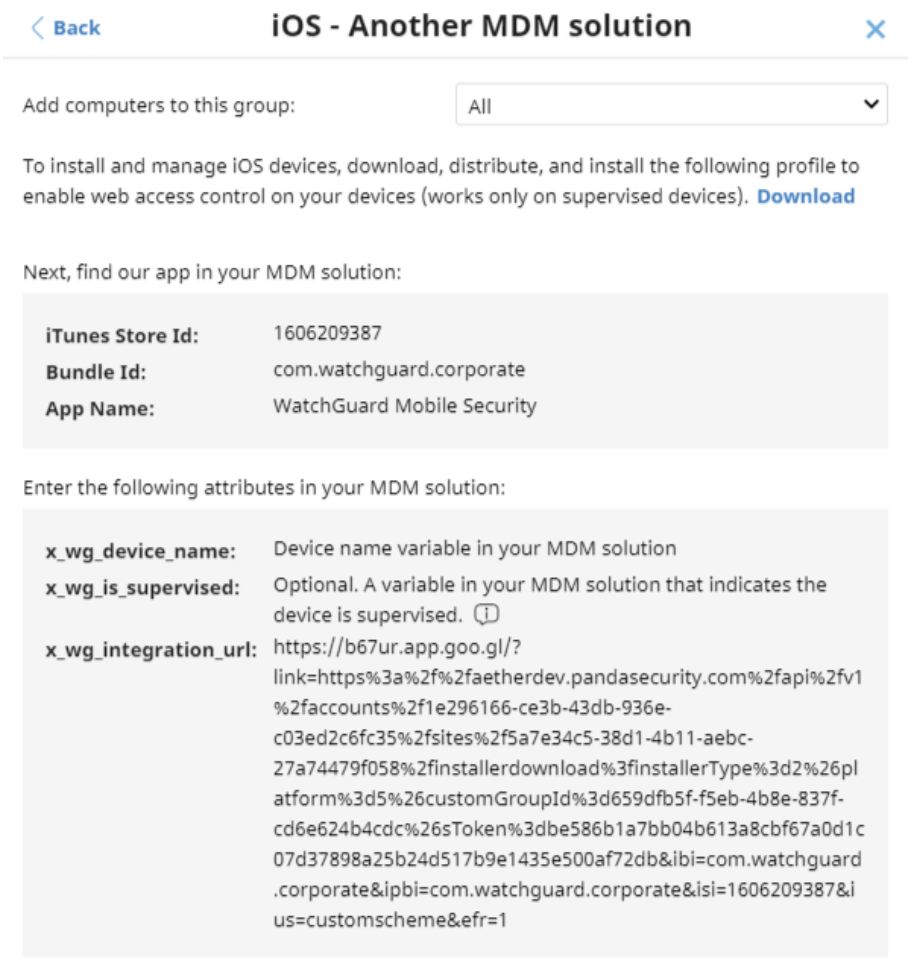


Figura 5.15: Ventana con los parámetros de integración para el MDM de terceros

- Haz clic en el enlace **Descargar** para obtener el perfil que establecerá a **Watchguard Mobile Security** como la aplicación configurada para filtrar el tráfico web en el dispositivo iOS. Se descargará en el equipo del administrador un fichero xml con extensión .mobileconfig.
- Importa el fichero .mobileconfig en el MDM de terceros y empújalo a los dispositivos iOS que requieren activar el filtrado de URLs.
- En el MDM de terceros, importa la aplicación **Watchguard Mobile Security** directamente desde la Apple Store. Utiliza para ello los campos **iTunes Store Id**, **Bundle Id** o **App Name** de la figura **Ventana con los parámetros de integración para el MDM de terceros** o las funcionalidades de búsqueda integradas en el propio MDM.
- Asocia y define los parámetros **x_wg_device_name**, **x_wg_integration_url** y **x_wg_supervised** en la aplicación **Watchguard Mobile Security** importada en el repositorio del MDM de terceros. La información contenida en estos parámetros se enviará junto a la aplicación **Watchguard Mobile Security** cuando el administrador la empuje a los dispositivos administrados con el MDM:

- **x_wg_device_name**: contiene el nombre del dispositivo que se mostrará en la consola Panda Endpoint Protection. Introduce en el parámetro **x_wg_device_name** la variable utilizada por el MDM que representa el nombre del dispositivo que recibirá la aplicación **Watchguard Mobile Security**.
- **x_wg_integration_url**: contiene la URL que apunta a la información que necesita **Watchguard Mobile Security** para integrarse en el grupo elegido por el administrador de Panda Endpoint Protection. Copia el contenido de **x_wg_integration_url** mostrado en la consola de Panda Endpoint Protection en el parámetro definido en el MDM.
- **x_wg_is_supervised**: le indica a **Watchguard Mobile Security** si el dispositivo donde se instalará está supervisado o no. Si tu producto MDM tiene una variable que permite establecer el contenido de este parámetro de forma dinámica añádelo. En caso contrario, no añadas este parámetro. **Watchguard Mobile Security** intentará determinar por su cuenta si se está ejecutando en un dispositivo administrado o no.

Cada MDM utiliza nombres de variables y sintaxis diferentes, consulta la documentación de tu producto para obtener esta información.

Utiliza variables en los parámetros x_wg_device_name y x_wg_is_supervised. Si, por ejemplo, en vez de la variable que representa al nombre del dispositivo introduces un nombre de dispositivo directamente, todos los terminales móviles que reciban Watchguard Mobile Security se mostrarán en la consola de Panda Endpoint Protection con el mismo nombre.

- Empuja la aplicación **Watchguard Mobile Security** desde el MDM a los dispositivos que deseas proteger. Al cabo de unos minutos la aplicación se instalará de forma silenciosa.
- Una vez instalada la aplicación, pulsa sobre ella para ejecutarla por primera vez. Se mostrará la ventana **"Watchguard Mobile Security" quiere enviarte notificaciones**.
- Pulsa el botón **Permitir**. El dispositivo comenzará a integrarse en la consola de Panda Endpoint Protection y la configuración habrá finalizado.

Procedimiento para no perder datos del dispositivo iOS al activar el modo supervisado

El procedimiento mostrado a continuación para hacer una copia de seguridad y su posterior restauración, no está soportado oficialmente por Apple. Por esta razón, se recomienda ejecutarlo previamente en un entorno de pruebas antes de utilizarlo con los teléfonos móviles de la empresa.

Establecer la necesidad de realizar una copia de seguridad manual

El proceso de activación del modo supervisado de un dispositivo iOS devuelve su medio de almacenamiento interno a su estado de fábrica, lo que supone perder todas las aplicaciones y los datos almacenados en él por el usuario. Para evitar esta situación, es necesario utilizar un método de copia de seguridad y recuperación, que varía dependiendo del tipo de datos almacenados y del software de copias utilizado:

- **iCloud**: si el usuario utiliza el almacenamiento en la nube de Apple, es muy posible que no sea necesario realizar ninguna copia de seguridad manual; en este caso, sus documentos, fotos y otros elementos no se almacenan en el dispositivo móvil sino que lo harán en la nube de forma automática. Una vez que el dispositivo esté formateado y en modo supervisado, el usuario deberá utilizar el mismo ID de Apple para volver a tener acceso a toda su información.

Para comprobar si iCloud almacena en la nube todos los tipos de datos que quieres conservar después de activar el modo supervisado, consulta ***https://support.apple.com/es-es/HT207428****. Si iCloud no almacena todos los tipos de datos que quieres conservar, utiliza la aplicación Finder tal y como se explica en este procedimiento.*

- **Finder**: si el usuario no utiliza iCloud, o quiere conservar aplicaciones o tipos de datos no soportados por la nube de Apple, es necesario realizar una copia de seguridad manual del dispositivo móvil siguiendo un protocolo muy específico. Esto es necesario debido a que Finder almacena también el estado del dispositivo en la copia de seguridad, con lo que al restaurar los datos también se restauraría el estado previo no supervisado del dispositivo.

Finder no almacena la configuración de todas las aplicaciones existentes en la Apple Store. Comprueba previamente si las aplicaciones instaladas en el dispositivo del usuario requerirán o no de una configuración manual posterior al proceso de restauración.

Requisitos para realizar una copia de seguridad con Finder

- Equipo macOS con la versión Catalina o superior y la aplicación Finder.
- iPhone del usuario a supervisar.
- iPhone auxiliar con la misma versión del sistema operativo que el iPhone del usuario.
- Cable de tipo lightning y USB.

Procedimiento para realizar una copia de seguridad

Copia de seguridad del iPhone del usuario

- En el teléfono móvil del usuario desactiva **Buscar mi iPhone**:
    - Pulsa **Ajustes**.
    - Pulsa en el nombre del usuario y en **Buscar mi**.
    - Pulsa **Buscar mi iPhone** y luego pulsa para desactivar esta opción.
    - Escribe la contraseña del ID de Apple.
    - Pulsa **Desactivar**.
- Abre la aplicación **Finder** y conecta el iPhone del usuario al equipo macOS.
- Si te pide el código del dispositivo o que confirmes que confías en el equipo Mac, sigue los pasos que aparecen en pantalla.
- En el panel de la izquierda del Finder haz clic en el iPhone del usuario.
- En la pestaña **General** haz clic en **Guarda en este Mac una copia de seguridad de todos los datos del iPhone**.
- Haz clic en el botón **Realizar copia de seguridad ahora**.
- Cuando haya terminado, anota la hora exacta a la que se realizó la copia de seguridad.

Restaurar la copia de seguridad del iPhone del usuario en el iPhone auxiliar

- Desactiva **Buscar mi iPhone** en el teléfono móvil auxiliar:
    - Pulsa **Ajustes**.
    - Pulsa en el nombre del móvil y en **Buscar mi**.
    - Pulsa **Buscar mi iPhone** y luego pulsa para desactivar esta opción.

    - Escribe la contraseña del ID de Apple.
    - Pulsa **Desactivar**.
- Desconecta el iPhone del usuario y conecta el iPhone auxiliar al equipo Mac.
- Si te pide el código del dispositivo o que confirmes que confías en el equipo Mac, sigue los pasos que aparecen en pantalla.
- En el panel de la izquierda del Finder haz clic en el iPhone auxiliar.
- En la pestaña **General** haz clic en **Restaurar copia de seguridad**.
- Elige la copia de seguridad previamente realizada teniendo en cuenta la fecha y hora anotada.

Copia de seguridad del iPhone auxiliar

- Comprueba que **Buscar mi iPhone** en el teléfono móvil auxiliar continua desactivado, si no es así:
    - Pulsa **Ajustes**.
    - Pulsa en el nombre del teléfono y en **Buscar mi**.
    - Pulsa **Buscar mi iPhone** y luego pulsa para desactivar esta opción.
    - Escribe la contraseña del ID de Apple.
    - Pulsa **Desactivar**.
- En el panel de la izquierda del Finder haz clic en el iPhone auxiliar.
- En la pestaña **General** haz clic en **Guarda en este Mac una copia de seguridad de todos los datos del iPhone**.
- Haz clic en el botón **Realizar copia de seguridad ahora**.
- Cuando haya terminado, anota la hora exacta a la que se realizó la copia de seguridad.

Restaurar la copia de seguridad del iPhone auxiliar en el iPhone del usuario

- Comprueba que **Buscar mi iPhone** en el teléfono móvil del usuario continua desactivado, si no es así:
    - Pulsa **Ajustes**.
    - Pulsa en el nombre del usuario y en **Buscar mi**.
    - Pulsa **Buscar mi iPhone** y luego pulsa para desactivar esta opción.
    - Escribe la contraseña del ID de Apple.
    - Pulsa **Desactivar**.
- Desconecta el iPhone auxiliar y conecta el iPhone del usuario al equipo Mac.

- Si te pide el código del dispositivo o que confirmes que confías en el equipo Mac, sigue los pasos que aparecen en pantalla.
- En el panel de la izquierda del Finder haz clic en el iPhone del usuario.
- En la pestaña **General** haz clic en **Restaurar copia de seguridad**.
- Elige la copia de seguridad previamente realizada teniendo en cuenta la fecha y hora anotada.
- Cuando termine el proceso, el iPhone del usuario mostrará la pantalla **Hola**. **En este punto es imprescindible no manipular el teléfono móvil e iniciar el proceso para activar el modo de supervisión**. Consulta **Establecer el modo supervisado e integrar el dispositivo en Panda MDM**.

Gestionar el ID de Apple y los certificados digitales

Crear un ID de Apple

- Accede con un navegador compatible al sitio **https://appleid.apple.com/account**. Se mostrará la ventana **Create Your Apple ID**.
- Rellena el formulario indicando la cuenta de correo y el número de teléfono del dispositivo que verificará la petición del certificado (normalmente es el dispositivo asignado al administrador de Panda Endpoint Protection), y haz clic en el botón **Continue**. Recibirás un correo en el buzón indicado en el formulario, con un código de verificación.
- Escribe en el formulario el código de verificación y haz clic en el botón **Continuar**. Recibirás un nuevo código por SMS en el teléfono móvil indicado en el formulario.
- Escribe el código SMS y haz clic en **Continuar**. El proceso habrá terminado y se mostrará el panel de control asociado a la cuenta creada. En este panel de control puedes gestionar la cuenta y ver todos los certificados generados hasta el momento.

Crear e importar el certificado digital en la consola Panda Endpoint Protection

Para integrar dispositivos iOS en Panda Endpoint Protection utilizando el MDM de Panda es necesario generar un certificado digital que asegure la confidencialidad de las comunicaciones con los servidores de Apple:

- En el menú superior **Equipos**, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **iOS**. Si no se ha importado previamente un certificado, se mostrará una ventana con el procedimiento para crear un certificado válido.

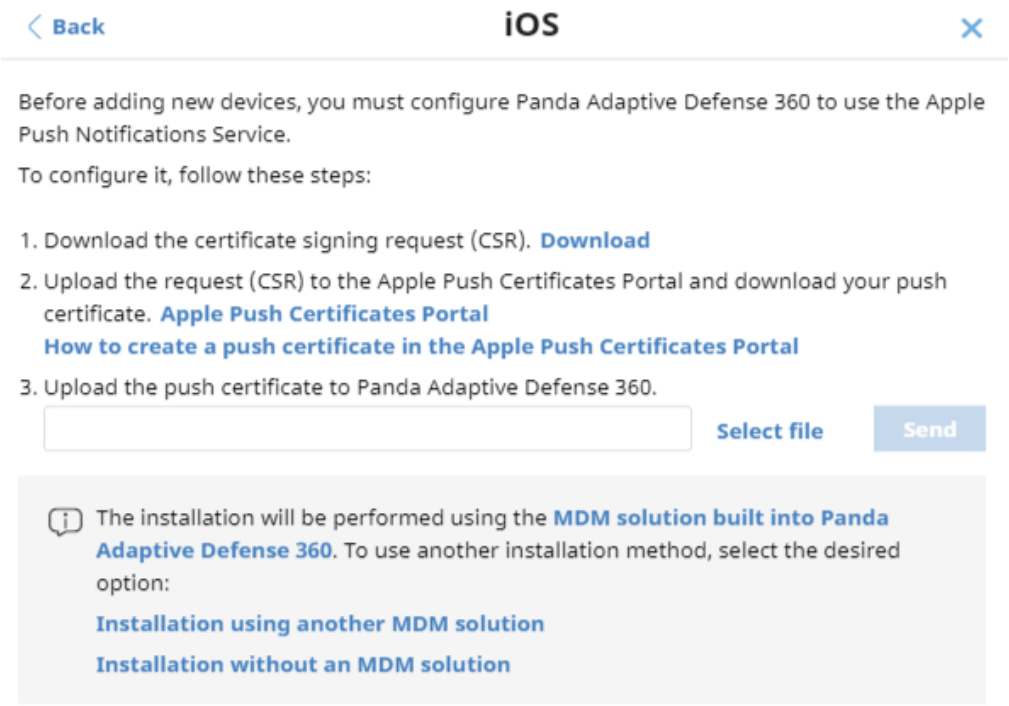


Figura 5.16: Ventana con el procedimiento para crear e importar un certificado digital de Apple

- Haz clic en el enlace **Descargar**. Se descará el fichero `apple_push.csr` que contiene la petición de certificado firmada y codificada en base64.
- Haz clic en el enlace **Apple Push Certificates Portal**. Si has iniciado la sesión previamente, se abrirá un navegador web con la página para gestionar los certificados digitales de Apple. Si no, escribe tus credenciales del ID de Apple. Consulta **Crear un ID de Apple**.
- Haz clic en el icono **Create certificate**. Se mostrará la pantalla **Terms of Use**.
- Haz clic en la casilla de verificación **I have read and agree to these terms and conditions** y haz clic en el botón **Accept**. Se mostrará la ventana **Create a New Push Certificate**.
- Haz clic en el botón **Seleccionar archivo**, elige el archivo `apple_push.csr` descargado previamente de la consola de administración de Panda Endpoint Protection y haz clic en el botón **Upload**. Se mostrará la ventana **Confirmation** con información del certificado generado y recibirás un correo informativo.
- Haz clic en el botón **Download**. Se descargará el fichero `MDM_ Panda Security, S.L._ Certificate.pem` que contiene el certificado digital.
- En la consola de administración de Panda Endpoint Protection haz clic en el enlace **Seleccionar archivo** y elige el fichero `MDM_ Panda Security, S.L._Certificate.pem` descargado del portal de Apple. Se mostrará la ventana **iOS** indicando la fecha de caducidad del certificado importado y su identificador.

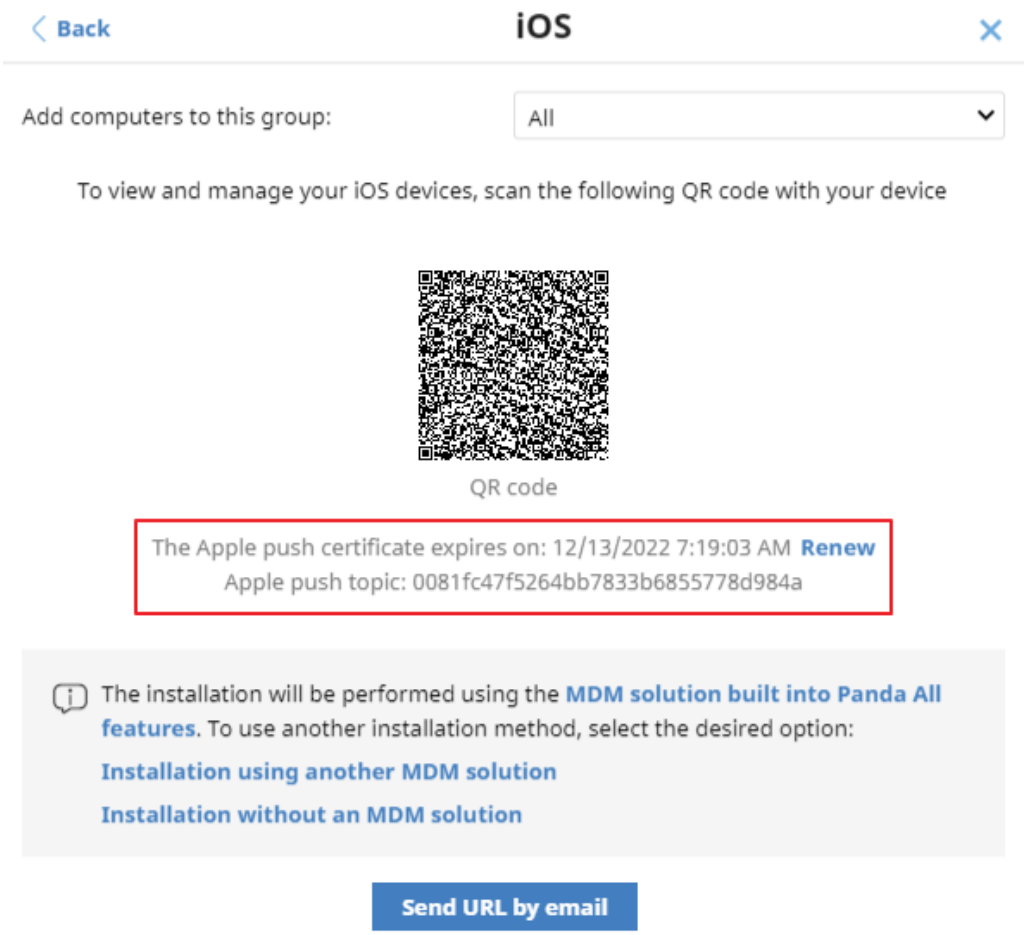


Figura 5.17: Ventana con la información del certificado digital cargado

Renovar el certificado de Apple

Los certificados generados por Apple tienen un periodo de validez de 1 año, transcurrido el cual caducan.

> *Recuerda renovar el certificado con margen suficiente antes de su vencimiento. Si el certificado caduca, dejarás de poder gestionar los dispositivos desde la consola de Panda Endpoint Protection y deberás volver a generar un certificado y a integrar de nuevo todos los dispositivos iOS de tu empresa.*

- Accede a **https://identity.apple.com/pushcert/** con las credenciales de ID Apple (consulta **Crear un ID de Apple**). Se mostrará la ventana **Certificates for Third-Party Servers**.

Figura 5.18: Ventana de selección de plataforma compatible con Panda Endpoint Protection

- Haz clic en el botón **Renew** asociado al certificado en uso. Se mostrará la ventana **Renew Push Certificate.**
- Haz clic en el botón **Seleccionar Archivo** y elige el fichero `apple_push.csr`. Si ya no tienes el fichero disponible puedes crear uno nuevo. Consulta **Crear e importar el certificado digital en la consola Panda Endpoint Protection**.
- Haz clic en el botón **Upload**. Se mostrará la ventana **Confirmation**.
- Haz clic en el botón **Download**. Se descargará el certificado actualizado.
- En el menú superior **Equipos** de la consola de administración de Panda Endpoint Protection, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **iOS**. Se mostrará una ventana con la información del certificado previamente cargado.
- Haz clic en **Renovar**. Se mostrará la ventana **iOS** con información de la fecha de caducidad del certificado y su identificador (Apple Push Topic).
- Haz clic en el enlace **Seleccionar archivo** y elige el fichero `apple_push.csr` que utilizaste al crear el certificado por primera vez. Si ya no tienes acceso a este fichero, puedes descargarte otro desde la consola de administración de Panda Endpoint Protection. Consulta **Crear e importar el certificado digital en la consola Panda Endpoint Protection**.
- Haz clic en el botón **Enviar**. Se mostrará la ventana **iOS** con la información de la fecha de caducidad del certificado actualizada.

Comprobar la fecha de caducidad del certificado

- En el menú superior **Equipos**, haz clic en el botón **Añadir equipos**. Se mostrará una ventana con las plataformas compatibles con Panda Endpoint Protection.
- Haz clic en el icono **iOS**. Si se ha importado previamente un certificado, se mostrarán sus datos.
- Si el certificado ha caducado se mostrará un mensaje de advertencia.

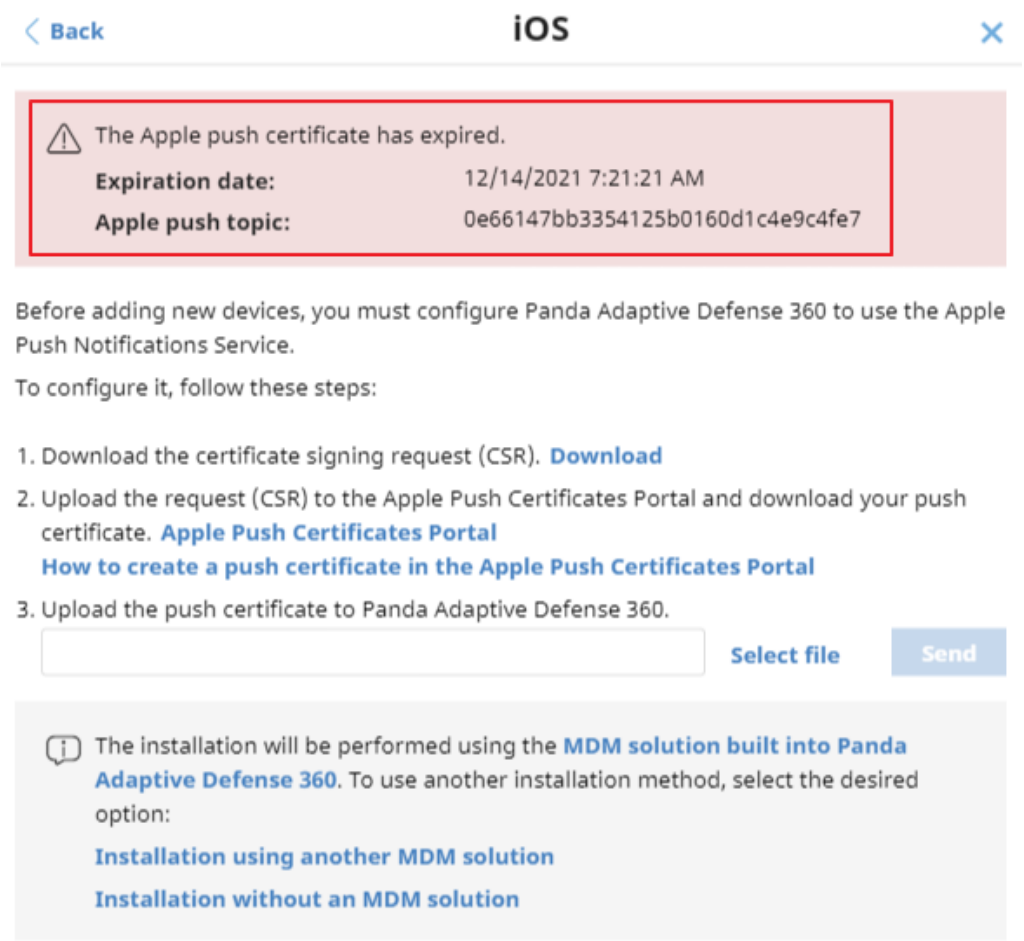


Figura 5.19: Ventana con la información del certificado digital caducado

Comprobar el despliegue

El administrador de la red dispone de tres formas complementarias para determinar el resultado del despliegue del software Panda Endpoint Protection en la red gestionada:

- Mediante el widget **Estado de protección**. Consulta Estado de protección en la página 470.
- Mediante el listado **Estado de la seguridad de los equipos**. Consulta Estado de protección de los equipos en la página 479.
- Mediante el registro **Aplicación** del visor de sucesos en los equipos Windows.

Visor de sucesos Windows

El registro **Aplicación** del visor de sucesos recoge información extendida sobre el resultado de la instalación del agente en el equipo del usuario y sobre su funcionamiento una vez instalado. A continuación se muestra una tabla con la información suministrada por Panda Endpoint Protection en cada campo del visor de sucesos.

Mensaje	Nivel	Categoría	Id
The device %deviceId% was unregistered	Advertencia	Registro (1)	101
The device %deviceId% was registered	Información	Registro (1)	101
A new SiteId %SiteId% was set	Advertencia	Registro (1)	102
Error %error%: Cannot change SiteId	Error	Registro (1)	102
Error %error%: Calling %method%	Error	Registro (1)	103
Error %code%: Registering device, %description%	Error	Registro (1)	103
Installation success of %fullPath% with parameters %parameters%	Información	Instalación (2)	201
A reboot is required after installing %fullPath% with parameters %parameters%	Advertencia	Instalación (2)	201
Error %error%: executing %fullPath% with parameters %parameters%	Error	Instalación (2)	201
Message: %Module% installer error with next data: (optional) Extended code: %code% (optional) Extended subcode: %subCode% (optional) Error description: %description% (optional) The generic uninstaller should be launched (optional) Detected AV: Name = %name%, Version = %version%	Error	Instalación (2)	202
Uninstallation success of product with code %productCode% and parameters %parameters%	Información	Desinstalación (4)	401
A reboot is required after uninstalling	Advertencia	Desinstalación (4)	401

Mensaje	Nivel	Categoría	Id
product with code %productCode% and parameters %parameters%			
Error %error%: Uninstalling product with code %productCode% and parameters %parameters%	Error	Desinstalación (4)	401
Uninstallation of product with code %productCode% and command line %commandLine% was executed	Información	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Desinstalación (4)	401
Error %error%: Uninstalling product with code %productCode% and command line %commandLine%	Error	Desinstalación (4)	401
Generic uninstaller executed: %commandLine%	Información	Desinstalación (4)	402
Error %error%: executed generic uninstaller %commandLine%	Error	Desinstalación (4)	402
Configuration success of product with code %productCode% and command line %commandLine%	Información	Reparación (3)	301
A reboot is required after configuring product with code %productCode% and command line %commandLine%	Advertencia	Reparación (3)	301
Error %error%: Configuring product with code %productCode% and command line %commandLine%	Error	Reparación (3)	301

Tabla 5.10: Códigos de resultado del proceso de instalación del agente en el visor de sucesos

Eliminación automática de equipos

Esta funcionalidad libera la licencia del software de seguridad de los equipos protegidos y los elimina de la consola. Los equipos a liberar han de cumplir ciertas condiciones, que se establecen mediante un filtro específico, que es necesario crear antes de activar la funcionalidad. Una vez creado el filtro, se aplicará de forma periódica.

Permisos necesarios

La eliminación automática de equipos es visible para todos los usuarios de la consola web, pero para poder configurar y modificar esta funcionalidad, el usuario ha de tener visibilidad total sobre todos los equipos y el permiso **Añadir, descubrir y eliminar equipos**.

Para más información, consulta **Descripción de los permisos implementados** en la página **69**

Consecuencias de la eliminación

La eliminación de equipos tiene lugar una vez al día, entre las 01:00 y las 03:00 UTC.

Al eliminar un equipo:

- El equipo y toda su información desaparecerán de la consola web.
- El equipo quedará desprotegido.
- Si el equipo está cifrado, permanecerá cifrado pero no se podrán obtener las claves de recuperación.

Es recomendable apagar el equipo tras su eliminación, ya que de lo contrario volverá a aparecer en la consola web en el momento en que se conecte de nuevo a los servidores de Aether.

La información generada por un equipo protegido no se elimina definitivamente de los servidores de Panda Endpoint Protection: cuando se reasigna una licencia al equipo y se restablece su conexión con Aether, toda su información aparecerá de nuevo en la consola web. No obstante, si al día siguiente el filtro no se ha desactivado, el equipo volverá a eliminarse.

Crear un filtro para eliminar equipos

Toda la información sobre los diferentes elementos disponibles para configurar un filtro está disponible en **Configurar filtros** en la página **216**.

Ten en cuenta que al tratarse de una funcionalidad de eliminación de equipos, es recomendable que el nombre del filtro sea fácilmente identificable.

Para filtrar de manera que la búsqueda proporcione como resultado los equipos no conectados al servidor de Aether, utiliza los siguientes parámetros:

- **Categoría**: Equipo
- **Propiedad**: Última conexión
- **Operador:**
    - Está entre (para buscar los equipos no conectados entre fechas concretas).
    - Antes de (para buscar los equipos no conectados antes de una fecha concreta).
    - Después de (para buscar los equipos no conectados a partir de una fecha concreta).

Activar la funcionalidad

- Haz clic en el menú superior **Configuración**, panel lateral **Mantenimiento de equipos**.
- Desplaza el control deslizante **Activar la eliminación automática de equipos**.
- En el desplegable, selecciona el filtro que quieres aplicar.
- Haz clic en el botón **Guardar cambios**.

El filtro no puede ser modificado ni eliminado durante su ejecución.

Programar el envío periódico de los equipos a eliminar

El administrador puede programar el envío automático de un informe periódico con el listado de equipos que van a ser eliminados. Consulta **Acceso al envío de informes y listados** en la página **580**

Desinstalar el software

Puedes desinstalar el software Panda Endpoint Protection de forma manual desde el panel de control del sistema operativo, o de forma remota desde el menú superior **Equipos** o desde los listados **Estado de la protección de los equipos** y **Licencias**.

Desinstalación manual

El propio usuario podrá ejecutar una desinstalación manual siempre y cuando el administrador de la protección no haya establecido una contraseña de desinstalación al configurar el perfil de la protección para su PC. Si lo ha hecho, se necesitará autorización o disponer de las credenciales necesarias para poder desinstalar la protección.

Para establecer o eliminar la password de desinstalación del agente, consulta ***Protección del agente mediante contraseña*** *en la página* ***314****.*

La instalación de Panda Endpoint Protection incluye varios programas independientes, según sea la plataforma de destino:

- **Equipos Windows y macOS**: agente y protección.
- **Equipos Linux**: agente, protección y módulo del kernel.
- **Dispositivos Android**: protección.
- **Dispositivos iOS**: protección y perfil MDM si está administrado.

Para desinstalar completamente Panda Endpoint Protection es necesario quitar todos los módulos. Si se desinstala únicamente el módulo de la protección, transcurrido un tiempo el agente la reinstalará de forma automática.

Windows 8 o superior

- Panel de Control > Programas > Desinstalar un programa.
- También puedes desinstalar tecleando, en el menú Metro: "desinstalar un programa".

Windows Vista, Windows 7, Windows Server 2003 y superiores

- Panel de Control > Programas y características > Desinstalar o cambiar un programa.

Windows XP

- Panel de Control > Agregar o quitar programas.

Desinstalar mediante la herramienta de desinstalación

En el caso de Windows, durante el proceso de desinstalación normal puede ocurrir que algunos archivos o librerías no se eliminen completamente, provocando ciertos mensajes de error. En estos casos, será necesario utilizar la herramienta que Panda Security pone a tu disposición para completar la desinstalación tanto del agente como de la protección.

Este proceso de desinstalación puede durar unos minutos. Una vez finalizado el proceso, reinicia el equipo.

Sigue los pasos que se indican a continuación:

- Descarga y descomprime el archivo **dg_aether.zip** (contraseña "panda").
- Ejecuta el archivo de desinstalación del agente `DG_AETHER.exe` y reinicia el equipo.
- Ejecuta el archivo de desinstalación de la protección `DG_PANDAPROT8_XX.exe` y reinicia el equipo.

macOS

- Abre el menú de comandos desde: Finder > Aplicaciones > Utilidades > Terminal
- Para desinstalar la protección ejecuta el comando `sudo sh /Applications/Endpoint-Protection.app/Contents/uninstall.sh`
- Para desinstalar el agente ejecuta el comando `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`

Dispositivos Android

- Accede a Configuración de Android > Seguridad > Administradores de dispositivos.
- Desactiva la casilla correspondiente a Panda Endpoint Protection. A continuación, Desactivar > Aceptar.
- De nuevo en la pantalla de Configuración de Android selecciona Aplicaciones instaladas. Haz clic en Panda Endpoint Protection > Desinstalar > Aceptar.

Dispositivos iOS sin integración con MDM

- Mantén pulsada la aplicación Watchguard Mobile Security en la pantalla de inicio. Los aplicaciones empezarán a moverse y se mostrará el icono "-" sobre cada una de ellas.
- Pulsa el icono "-" en la esquina superior izquierda de la aplicación Watchguard Mobile Security. Se abrirá la ventana **¿Eliminar Watchguard Mobile Security?**.
- Pulsa **Eliminar app**. Se abrirá la ventana **¿Quieres eliminar Watchguard Mobile Security**?
- Pulsa **Eliminar**. La aplicación se habrá desinstalado del teléfono móvil.

Dispositivos iOS integrados en Panda MDM

- En la pantalla de inicio pulsa en **Ajustes**. Se abrirá la ventana **Ajustes**.
- En el panel lateral pulsa **General**. Se abrirá la ventana **General**.

- Pulsa en la opción **VPN y gestión de dispositivos**. Se mostrará el perfil descargado **Watchguard MDM Service**.
- Pulsa el botón **Eliminar gestión**. Se abrirá la ventana **Eliminar gestión**.
- Pulsa el botón **Eliminar**. El perfil de gestión se eliminará y acto seguido también lo hará la aplicación Watchguard Mobile Security.

Dispositivos iOS integrados en un MDM de terceros

A diferencia de la integración con Panda MDM, se recomienda desinstalar la aplicación Watchguard Mobile Security mediante el MDM de terceros utilizado para la gestión. Si eliminas el perfil del teléfono móvil de forma manual, todo el software que se haya instalado a través del MDM también se perderá, y además ya no será posible gestionar el dispositivo de forma centralizada desde el MDM.

Linux

En Linux se utiliza el entorno gráfico para gestionar paquetes incluidos en la distribución.

- **Fedora**: Actividades > Software > Instalado
- **Ubuntu**: Software de Ubuntu > Instaladas

Se recomienda utilizar la línea de comandos como root para desinstalar el producto. Abre una linea de comandos e introduce:

```
$ /usr/local/management-agent/repositories/pa/install --remove
(desinstala la protección)
$ /usr/local/management-agent/repositories/ma/install --remove
(desinstala el agente y los repositorios)
```

Resultado de la desinstalación manual

Al desinstalar el software Panda Endpoint Protection (agente Panda y Protección) el equipo desaparecerá completamente de la consola de administración. Todos los contadores, entradas en informes e información de la actividad del equipo y de sus procesos se borrarán.

Si, posteriormente, el mismo equipo vuelve a ser integrado en la consola de administración mediante la reinstalación del software Panda Endpoint Protection, se recuperará toda la información previamente eliminada.

Desinstalación remota

Para desinstalar de forma remota un equipo Windows protegido con Panda Endpoint Protection :

- En el menú superior **Equipos**, o en los listados **Licencias** y **Estado de la protección de equipos** marca los equipos a desinstalar con las casillas de selección.
- En la barra de acciones haz clic en el botón **Eliminar**. Se mostrará una ventana de confirmación.
- En la ventana de confirmación haz clic en la casilla **Desinstalar el agente de Panda de los equipos seleccionados** para retirar por completo el software Panda Endpoint Protection.

La desinstalación remota solo es compatible con plataformas Windows. En plataformas Linux y macOS únicamente se retirará el equipo de la consola junto a todos los contadores, si bien en el próximo descubrimiento de la red el equipo será reincorporado a la consola, junto a toda su información.

Reinstalación remota

Para resolver algunos situaciones donde el software Panda Endpoint Protection presenta un mal funcionamiento, se permite su reinstalación remota desde la consola de administración, tanto para equipos de usuario como para servidores.

La reinstalación del software se realiza por separado para el agente y para el módulo de la protección.

Requisitos de la funcionalidad de reinstalación remota

- Equipo de usuario o servidor con sistema operativo Windows instalado.
- Un equipo con el rol de descubridor asignado en el mismo segmento de red que el equipo a reinstalar y que comunique con la nube de Panda Security.
- Credenciales de una cuenta de administrador local o de dominio.

Acceso a la funcionalidad

Desde los listados mostrados a continuación accesibles en el menú superior **Estado**, haciendo clic en el enlace **Añadir** del panel lateral:

- **Estado de protección de los equipos** en la página **479**.
- **Estado de gestión de parches** en la página **390**.
- **Estado del cifrado** en la página **458**.
- **Listados del módulo Licencias** en la página **192**.
- **Hardware** en la página **241**.

La funcionalidad también es accesible desde el listado de **Equipos** en el menú superior **Equipos**, haciendo clic en una rama del árbol de carpetas o filtros situado en el panel lateral.

> *Las opciones **Reinstalar la protección (requiere reinicio)** y **reinstalar agente** solo se mostrarán en equipos compatibles con esta funcionalidad.*

Descubrimiento de equipos a reinstalar

Utiliza el listado **Equipos no administrados descubiertos** para localizar los dispositivos en los que es necesario realizar la reinstalación. Consulta **Visualizar equipos descubiertos**.

Reinstalación en un equipo

- Localiza en el listado el equipo a reinstalar.
- En el menú de contexto asociado al equipo selecciona la opción **Reinstalar la protección (requiere reinicio)** o **Reinstalar el agente**. Se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta **Ventana de selección Reinstalar la protección** y **Ventana de selección Reinstalar el agente**.

Reinstalación en varios equipos

- Selecciona con las casillas de selección en el listado los equipos que reinstalarán su protección o agente.
- En la barra de herramientas selecciona la opción **Reinstalar la protección (requiere reinicio)** o **Reinstalar el agente**. Se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta **Ventana de selección Reinstalar la protección** y **Ventana de selección Reinstalar el agente**.

Ventana de selección Reinstalar la protección

Al configurar la reinstalación de la protección, se abre una ventana flotante con dos opciones:

- **Reinstalar la protección inmediatamente (requiere reinicio)**: el reinicio se producirá en el plazo de 1 minuto. Si el equipo de destino no está accesible en ese momento por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Panda Endpoint Protection durante 1 hora.
- **Ofrecer un margen de tiempo antes de forzar la reinstalación**: el reinicio se producirá en el plazo configurado por el administrador. Si el equipo de destino no está accesible por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Panda Endpoint Protection durante 7 días.

En el momento en que el administrador inicia la reinstalación de la protección, el usuario del equipo recibe un mensaje emergente dándole la posibilidad de reiniciar el equipo en ese momento o esperar a que finalice el tiempo definido por el administrador. Una vez que ha expirado el plazo, la protección se desinstalará y el equipo se reiniciará de forma automática para reinstalar la protección.

Si la desinstalación de la protección presenta algún tipo de problema, Panda Endpoint Protection iniciará de forma transparente para el usuario un desinstalador genérico que tratará de desinstalar nuevamente la protección y limpiar cualquier rastro en el equipo. Para ello es posible que se requiera un reinicio adicional.

Ventana de selección Reinstalar el agente

Al configurar la reinstalación del agente, se muestra una ventana flotante que solicita la información siguiente:

Seleccionar el equipo con el rol de descubridor desde el cual se reinstalará el agente:

- Asegúrate de que el equipo descubridor se encuentra en el mismo segmento de red que el equipo a reinstalar.
- Si el equipo descubridor está apagado, la petición se mantendrá en espera hasta que sea visible de nuevo. Las peticiones se mantienen en espera por un intervalo de 1 hora, transcurrido el cual se descartan.

Credenciales para reinstalar los equipos: escribe una o varias credenciales de instalación. Utiliza una cuenta de administración local del equipo o del dominio al que pertenece para completar la reinstalación con éxito.

Una vez introducida la información, el equipo con el rol de descubridor seguirá los pasos mostrados a continuación:

- Conectará con el equipo a reinstalar.
- Desinstalará el agente instalado en el equipo a reinstalar.
- Descargará un nuevo agente preconfigurado con el cliente, grupo y la configuración de red asignada al equipo, lo copiará y lo ejecutará remotamente en el equipo a reinstalar.
- Si hay algún problema en el transcurso de la operación, se lanzará el desinstalador genérico y, si es necesario, se mostrará al usuario un mensaje con una cuenta atrás para el reinicio del equipo automático y un botón para reiniciar de forma manual e inmediata.

Códigos de error

Para obtener un listado de los mensajes de error y las acciones recomendadas para corregirlos, consulta **Errores en el proceso de reinstalación del software de protección** en la página **259**.

Capítulo 6

Licencias

Para proteger los equipos de la red de las amenazas es necesario contratar licencias de Panda Endpoint Protection en un número igual al número de puestos de usuario y servidores a proteger. Una licencia de Panda Endpoint Protection solo se puede asignar a un único dispositivo en un momento concreto.

A continuación se detalla el proceso de gestión de licencias de Panda Endpoint Protection: su asignación a los equipos de la red, liberación y comprobación de su estado.

Contenido del capítulo

Definiciones y conceptos clave

Para interpretar correctamente la información y las gráficas suministradas por Panda Endpoint Protection que reflejan el estado de las licencias del producto es necesario conocer los términos mostrados en este apartado.

Para contratar y/o renovar licencias consulta con tu partner asignado.

Mantenimientos

Las licencias contratadas por el cliente se agrupan en mantenimientos. Un mantenimiento es un conjunto de licencias con características comunes:

- **Tipo de Producto**: Panda Endpoint Protection, Panda Full Encryption, Panda Patch Management, .
- **Licencias contratadas**: número de licencias que pertenecen al mantenimiento.
- **Tipo de licencias**: NFR, Trial, Comercial, Suscripción.
- **Caducidad**: Fecha en la que las todas las licencias del mantenimiento caducan y los equipos dejarán de estar protegidos.

Estado de los equipos

Desde el punto de vista de las licencias, Panda Endpoint Protection distingue tres estados en los equipos de la red:

- **Equipos con licencia**: equipos con una licencia válida en uso asignada.
- **Equipos sin licencia**: equipos que no tienen una licencia en uso, pero que son candidatos a tenerla.
- **Excluidos**: equipos que no compiten por la obtención de una licencia. Estos equipos no están ni estarán protegidos por Panda Endpoint Protection aunque haya licencias sin asignar disponibles. Los equipos excluidos se seguirán mostrando en la consola y podrás utilizar algunas funcionalidades de gestión. Para excluir un equipo es necesario liberar su licencia de forma manual.

Es necesario distinguir entre el número de equipos sin licencia asignada (candidatos a tenerla en caso de existir licencias sin asignar) y el número de equipos excluidos (sin posibilidad de tener una licencia asignada, aunque haya licencias disponibles).

Estado de las licencias y grupos

Las licencias contratadas pueden tener dos estados:

- **Asignada**: licencia usada por un equipo de la red.
- **Sin asignar**: licencia que no está siendo usada por ningún equipo de la red.

Las licencias se agrupan por su estado en dos grupos:

- **Grupo de licencias usadas**: formado por todas las licencias asignadas a equipos.
- **Grupo de licencias sin usar**: formado por las licencias sin asignar.

Tipos de licencias

- **Licencias comerciales**: son las licencias estándar de Panda Endpoint Protection. Un equipo con una licencia comercial asignada tiene acceso a toda la funcionalidad del producto licenciado.
- **Licencias de prueba (Trial)**: son licencias gratuitas de prueba, válidas por un periodo limitado de 30 días. Un equipo con una licencia de prueba asignada tiene acceso completo a la funcionalidad del producto.
- **Licencias NFR**: licencias Not For Resale, destinadas a personal interno y partners de Panda Security. No está permitida su venta ni uso por personal o partners ajenos a Panda Security.
- **Licencias de tipo suscripción**: son licencias que no tienen fecha de caducidad. El servicio es de tipo "pago por uso".

Asignar licencias

Puedes asignar licencias de forma manual o automática.

*Consulta **Gestión de equipos y dispositivos** en la página **209** para obtener más información acerca de la herramienta de búsqueda y del árbol de carpetas y árbol de filtros.*

Asignación automática

Al instalar el software Panda Endpoint Protection en un equipo de la red, y siempre que existan licencias sin utilizar, el sistema le asignará de forma automática una licencia libre.

Asignación manual

Sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a asignar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar la ventana de detalle.
- En la pestaña **Detalles**, **Licencias** se mostrará el estado **Sin licencias**. Haz clic en el icono y se asignará de forma automática una licencia libre.

Liberar licencias

Liberar una licencia es un proceso equivalente a la asignación de licencias.

Liberación automática

- Al desinstalar el software Panda Endpoint Protection de un equipo de la red, el sistema recupera de forma automática una licencia y la devuelve al grupo de licencias sin usar.
- Al caducar un mantenimiento se liberan automáticamente licencias de los equipos siguiendo la lógica de licencias caducadas explicadas en Lógica de liberación de licencias caducadas.

Liberación manual

La liberación manual de una licencia asignada previamente a un equipo lo convierte en un equipo excluido. Aunque existan licencias libres, estas no son asignadas al equipo de forma automática.

Para liberar manualmente una licencia de Panda Endpoint Protection de un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a liberar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar su información.
- En la pestaña **Detalles**, **Licencias** se mostrará el estado del equipo. Haz clic en el icono para liberar la licencia y devolverla al grupo de licencias sin utilizar.

Procesos asociados a la asignación de licencias

Caso I: Equipos con licencia asignada y equipos excluidos

Por defecto, a cada nuevo equipo integrado en la plataforma Aether se le asigna una licencia de producto Panda Endpoint Protection de forma automática, pasando a tomar el estado de **Equipo con licencia asignada**. Este proceso se repite hasta que el grupo de licencias sin usar número quede reducido a 0.

Al retirar una licencia de un equipo de forma manual, éste toma el estado de **Equipo excluido**. A partir de ese momento el equipo no competirá por la asignación de una licencia de forma automática, en el caso de existir licencias sin usar.

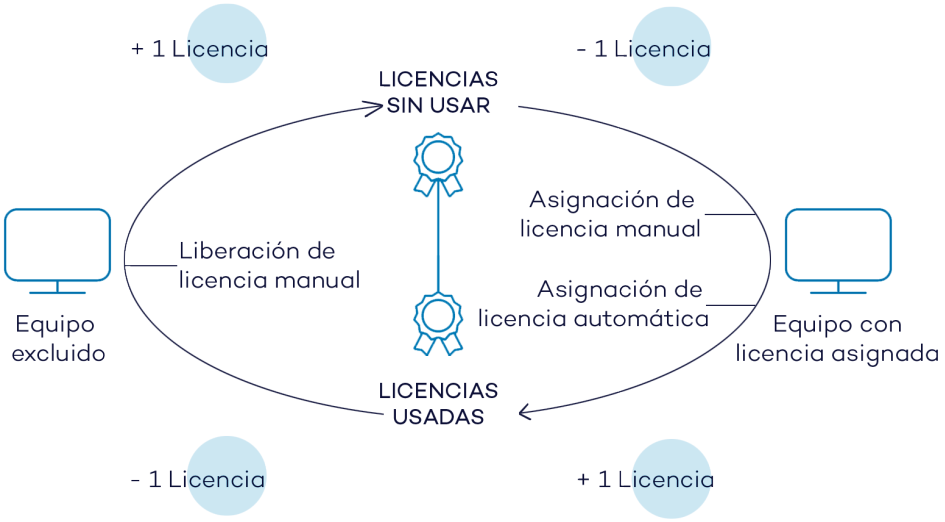


Figura 6.1: Modificación de los grupos de licencias en equipos con licencia asignada y excluidos

Caso II: Equipos sin licencia asignada

En el momento en que nuevos equipos se incorporan a la plataforma Aether y el grupo de licencias sin usar está a 0, los equipos pasarán al estado **Equipos sin licencia**. Cuando estén disponibles nuevas licencias, estos equipos tomarán una licencia de forma automática.

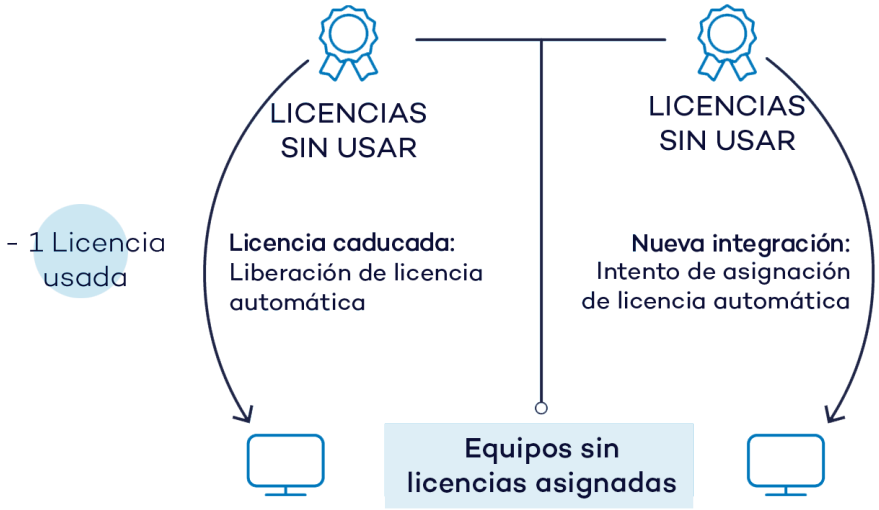


Figura 6.2: Equipos sin licencia asignada por caducar su mantenimiento y estar vacío el grupo de licencias sin usar

De la misma forma, en el momento en que una licencia asignada caduque, un equipo de la red pasará al estado **Sin licencia asignada**, siguiendo la lógica de licencias caducadas explicadas en **Lógica de liberación de licencias caducadas**.

Paneles / widgets del módulo licencias

Acceso al panel de control

Para acceder haz clic en el menú superior **Estado**, panel lateral **Licencias**.

Permisos requeridos

No se necesitan permisos adicionales para acceder a los widgets asociados al panel de licencias.

Para visualizar el detalle de las licencias contratadas haz clic en el menú superior **Estado** y después en el menú lateral **Licencias**. Se mostrará una ventana con dos gráficas (widgets): **Licencias contratadas** y **Caducidad de licencias**.

Licencias

El panel representa cómo se distribuyen las licencias del producto contratado.

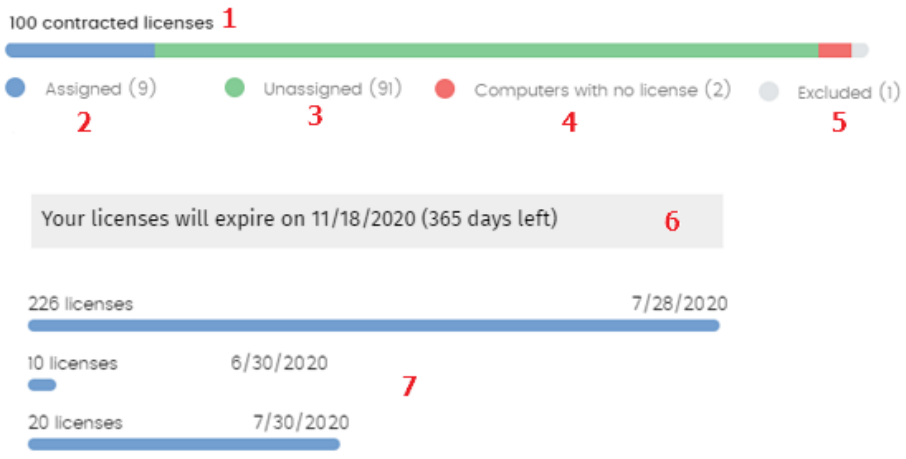


Figura 6.3: Panel de licencias mostrando tres mantenimientos

Significado de las series

Zona activa	Descripción
Número de licencias contratadas totales (1)	Número máximo de equipos que se pueden proteger, en el caso de que todas las licencias contratadas sean asignadas.
Número de licencias asignadas (2)	Número de equipos protegidos con una licencia asignada.
Número de licencias sin asignar (3)	Número de licencias contratadas pero que no se han asignado a ningún equipo y por lo tanto están sin utilizar.
Número de equipos sin licencia (4)	Equipos no protegidos por no disponer de licencias suficientes. El sistema les asignará licencia de forma automática si se adquieren nuevas licencias.
Número de equipos excluidos (5)	Equipos sin licencia asignada que no son candidatos a tenerla.
Caducidad de las licencias (6)	Si existe un único mantenimiento contratado, todas las licencias caducaran a la vez, en la fecha indicada.

Zona activa	Descripción
Caducidad por mantenimiento (7)	Si un mismo producto ha sido contratado varias veces a lo largo del tiempo se mostrará una gráfica de barras horizontales con las licencias asociadas a cada contrato / mantenimiento y su fecha de caducidad independiente.

Tabla 6.1: Descripción de las series de Licencias

Filtros preestablecidos desde el panel

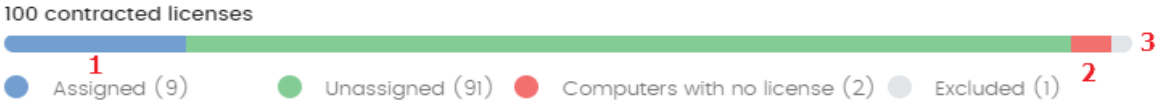


Figura 6.4: Zonas activas del panel licencias contratadas

Se muestra el listado **Licencias** con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

Campo para filtrar	Valor
(1) Estado de licencia	Asignada
(2) Estado de licencia	Sin licencia
(3) Estado de licencia	Excluido

Tabla 6.2: Filtros del listado de licencias

Listados del módulo Licencias

Acceso al listado

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Licencias** y en el widget.

ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona el listado **Licencias** de la sección **General** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

El acceso al listado **Licencias** no requiere permisos adicionales para el administrador.

Licencias

Muestra en detalle el estado de las licencias de los equipos de la red e incorpora filtros que ayudan a localizar los puestos de trabajo o dispositivos móviles en función de su estado.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Licencia asignada • Equipo sin licencia • Equipo excluido
Última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security.	Fecha.

Tabla 6.3: Campos del listado Licencias

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el producto.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Servidor • Dispositivo móvil

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android
Directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o esta virtualizado.	Booleano
Versión del agente	Versión interna del componente agente que forma parte del software de cliente Panda Endpoint Protection.	Cadena de caracteres
Versión de la protección	Versión interna del componente protección que forma parte del software de cliente Panda Endpoint Protection.	Cadena de caracteres
Fecha de arranque del sistema	Fecha en la que el equipo se inició por última vez.	Fecha
Fecha instalación	Fecha en la que el software Panda Endpoint Protection se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security.	Fecha
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • No asignada • Excluido

Campo	Descripción	Valores
Grupo	Carpeta dentro del árbol de carpetas de Panda Security a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres

Tabla 6.4: Campos del fichero exportado Licencias

Herramienta de filtrado

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	• Todos • Hace menos de 24 horas • Hace menos

Campo	Descripción	Valores
		de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • Sin licencia • Excluido

Tabla 6.5: Campos de filtrado para el listado Licencias

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta **Información de equipo** en la página **251** para obtener más información.

Licencias caducadas

Excepto los mantenimientos de tipo suscripción, todos los demás tienen asignada una fecha de caducidad, pasada la cual los equipos de la red dejarán de están protegidos.

Comportamiento de los productos basados en Aether al caducar sus licencias

La caducidad de los productos basados en Aether, tiene un impacto importante en los equipos afectados ya que:

- Se desactivan todas las protecciones configuradas en los equipos.
- Los equipos pierden el acceso a las actualizaciones del fichero de firmas y a las bases de conocimiento de la inteligencia colectiva.

- Las tareas programadas dejan de funcionar, y, por tanto, ya no es posible realizar análisis programados ni instalaciones de parches para actualizar programas vulnerables.

Por tanto, los equipos pasan a estar en una situación grave de vulnerabilidad y muy expuestos a posibles filtraciones de datos e infecciones de diferente grado de peligrosidad, desde PUPs, a ransomware o incluso amenazas avanzadas con diferentes objetivos (ATPs).

7 días de gracia

Para evitar esta situación, Panda ofrece un periodo de siete días de gracia durante el que se garantiza la protección total a los equipos afectados mientras se lleva a cabo la renovación de las licencias.

El periodo de 7 días de gracia no es aplicable a Panda Fusion (Panda Endpoint Protection Plus sobre Aether + Panda Systems Management), que no tiene período de gracia.

Comportamiento cuando caduca uno de los mantenimientos contratados

En los casos en los que el cliente tiene contratados varios mantenimientos con fechas de finalización distintas, los equipos con licencias asignadas no pertenecen a un mantenimiento concreto; en su lugar, todas las licencias de todos los mantenimientos se suman en un único grupo de licencias disponibles, que posteriormente se reparten entre los equipos de la red.

En el momento en que un mantenimiento caduca, Panda Endpoint Protection determina el número de licencias asignadas a ese mantenimiento. Acto seguido, se ordenan los equipos de la red con licencia asignada utilizando como criterio de ordenación el campo **Última conexión**, que contiene la fecha en la que el equipo se conectó por última vez a la nube de Panda Security.

Los equipos candidatos a retirar su licencia de protección son aquellos no vistos en el periodo de tiempo más alejado. Así, se establece un sistema de prioridades donde la mayor probabilidad de retirar una licencia corresponde a los equipos que no han sido utilizados recientemente.

Seleccionar qué equipos serán los que primero se queden sin licencia

Aether permite seleccionar previamente los equipos a los que se retirará la licencia antes de que ésta caduque.

Para ello, puedes:

- Eliminar equipos desde la consola. En las herramientas de gestión del listado de equipos, encontrarás la opción para eliminar un equipo. Consulta **Herramientas de gestión** en la página **239**.

- Desactivar la licencia de los equipos que no quieras proteger, pero que sí quieras seguir gestionando desde la consola. Para más información, consulta **Liberación manual**

> *Ten en cuenta que si no desinstalas el agente de los equipos eliminados, el equipo se integrará automáticamente de nuevo en la consola y volverá a consumir una licencia cuando el agente contacte con el servidor Panda Endpoint Protection.*

Comportamiento de Panda Endpoint Protection tras caducar todas las licencias

Desde que las licencias caducan y durante el período de gracia de 7 días (días X al X+7):

- Se dispondrá de acceso a la consola
- Las protecciones continuarán actualizadas y funcionando al 100%.

Tras el período de gracia (X+8) y durante 83 días más (días X+8 al X+90) los datos del mantenimiento se mantienen pero los equipos estarán desprotegidos. Durante este período:

- No se dispondrá de acceso a la consola
- Todas las protecciones estarán desactivadas

Renovar antes de 90 días tras caducar las licencias

Si la renovación tiene lugar antes de cumplir 90 días tras la caducidad de las licencias:

- Los equipos volverán a activar las protecciones y a actualizarse en un tiempo máximo de 4 horas desde que se renuevan las licencias, siempre y cuando el equipo se conecte a Internet.

Renovar tras más de 90 días desde la caducidad de las licencias

Transcurridos 90 días desde que caducan las licencias (desde X+90), el agente y las protecciones se desinstalarán automáticamente, y los datos del mantenimiento se eliminarán de las bases de datos de Panda Security.

Para renovar, será necesario comenzar el proceso de instalación y configuración desde cero, es decir:

- Crear los usuarios
- Reinstalar el agente y las protecciones
- Crear de nuevo las configuraciones

Mensajes de caducidad próxima y vencida

A los 30 días de vencer el mantenimiento, el panel **Licencias** contratadas mostrará un mensaje con los días que quedan para finalizar el mantenimiento y el número de licencias que se verán afectadas.

Adicionalmente, se mostrará un mensaje por cada mantenimiento caducado, indicando el número de licencias que ya no son funcionales en el plazo de los 30 últimos días.

Si todos los productos y mantenimientos están caducados se denegará el acceso a la consola de administración.

Licencias de prueba sobre licencias comerciales

En el caso de tener contratadas licencias comerciales de Panda Endpoint Protection, Panda Endpoint Protection Plus o Fusion sobre la plataforma Aether y obtener una trial de Panda Endpoint Protection, se producirán una serie de ajustes, tanto en la consola de administración como en el software instalado en los equipos de la red:

- Se crea un mantenimiento nuevo de tipo trial, con la duración contratada para la prueba y un número de licencias igual a la suma de las licencias disponibles previamente y las licencias contratadas para la trial.
- Los mantenimientos comerciales se desactivan temporalmente mientras dure el periodo de trial, pero el ciclo de caducidad y renovación se mantiene intacto.
- Se habilita la funcionalidad asociada al producto en pruebas sin necesidad de actualizar los equipos de la red.
- Panda Endpoint Protection se activa por defecto en todos los equipos con el modo de protección Audit. En caso de no querer activar Panda Endpoint Protection en todos los puestos o de querer establecer un modo de protección distinto, establece la configuración oportuna.

*Consulta **Asignación manual y automática de configuraciones** en la página **287** para obtener información acerca de asignar perfiles de configuración a los equipos de la red.*

- Una vez terminado el periodo de prueba, el mantenimiento creado para la trial se elimina y el mantenimiento comercial se reactiva. Los equipos de la red sufrirán un "downgrade"

automático, manteniendo las configuraciones previas.

Buscar equipos según su estado de licencia

Panda Endpoint Protection incluye la categoría **Licencia** para crear filtros que ayuden a localizar los equipos de la red que tengan un determinado estado de licencia.

*Consulta **Crear y organizar filtros** en la página **214** para obtener más información acerca de cómo crear un filtro en Panda Endpoint Protection.*

A continuación, se muestran las propiedades de la categoría **Licencias** para crear filtros que generen listados de equipos con información relevante sobre licencias.

Categoría	Propiedad	Valor	Descripción
Licencia	Estado	Establece filtros según el estado de la licencia.	
		Asignada	Lista los equipos con una licencia Panda Endpoint Protection asignada.
		Sin asignar	Lista los equipos que no tiene una licencia Panda Endpoint Protection asignada.
		Desasignada manualmente	El administrador de la red liberó la licencia Panda Endpoint Protection previamente asignada al equipo.
		Desasignada automáticamente	El sistema liberó al equipo la licencia Panda Endpoint Protection asignada previamente.

Tabla 6.6: Campos del listado Equipos protegidos

Capítulo 7

Actualización del producto

Panda Endpoint Protection es un servicio cloud gestionado, y por lo tanto el administrador de la red no necesita ejecutar tareas de mantenimiento en la infraestructura de back-end que lo soporta. Sin embargo, sí es necesaria la actualización del software cliente instalado en los equipos de la red, así como iniciar la actualización de la consola de administración, si así lo desea.

Contenido del capítulo

Módulos actualizables en el software cliente

Los elementos instalados en el equipo del usuario son:

- Agente de comunicaciones Aether Platform.
- Motor de la protección Panda Endpoint Protection.
- Archivo de identificadores / fichero de firmas.

Dependiendo de la plataforma a actualizar, el procedimiento y las posibilidades de configuración varían tal y como se indica en **Formas de actualización según el componente del software cliente**.

Módulo	Plataforma			
	Windows	macOS	Linux	Android
Agente Panda	Bajo demanda			
Protección Panda Endpoint Protection	Configurable	Configurable	Configurable	No
Archivo de identificadores	Habilitar / Deshabilitar	Habilitar / Deshabilitar	Habilitar / Deshabilitar	No

Tabla 7.1: Formas de actualización según el componente del software cliente

- **Bajo demanda**: el administrador puede iniciar la actualización una vez que esté disponible, o retrasarla hasta el momento que considere oportuno.
- **Configurable**: el administrador podrá definir en la consola web ventanas de actualización recurrentes y en el futuro, siendo posible además desactivar la actualización.
- **Habilitar / Deshabilitar** : El administrador puede desactivar la actualización. Si la actualización está activada ésta se producirá automáticamente cuando esté disponible.
- **No**: El administrador no puede influir en el proceso de actualización. Las actualizaciones se efectuarán cuando estén disponibles y no es posible deshabilitarlas.

Actualización del motor de protección

Para configurar la actualización del motor de protección crea y asigna un perfil de configuración de tipo **Ajustes por equipo**, accesible desde el menú superior **Configuración**, en el panel de la izquierda de la consola de administración.

Limitación de la descarga de actualizaciones del motor a través de equipos caché y Proxy Panda

La descarga de las actualizaciones del motor de protección puede realizarse directamente desde Internet o también a través de un equipo caché o Proxy Panda. Consulta **Configuración de las descargas mediante equipos caché** en la página **307** y **Configuración de listas de acceso a través de proxy** en la página **305**.

Según el sistema operativo instalado en el equipo, pueden existir ciertas limitaciones a la hora de utilizar un método de descarga u otro:

- **Equipos con sistema operativo Windows o macOS**: pueden descargar instaladores a través de equipos caché, proxy e Internet.
- **Equipos con sistema operativo Linux**: al utilizar el gestor de paquetes propio de la distribución para hacer las descargas, no pueden descargar instaladores a través de equipos caché ni proxy de Panda Endpoint Protection.

Los equipos caché almacenan los instaladores hasta que dejan de ser válidos, momento en el que se eliminarán.

Actualizaciones

Para habilitar la actualización automática del módulo de protección Panda Endpoint Protection haz clic en el botón de activación **Actualizar automáticamente Panda Endpoint Protection en los dispositivos**. Esta acción habilitará el resto de configuraciones de la página. Si esta opción esta deshabilitada, el módulo de protección no se actualizará nunca.

Se desaconseja totalmente deshabilitar la actualización del motor de protección. Los equipos con la protección sin actualizar serán más vulnerables en el medio plazo frente a las amenazas avanzadas y el malware.

Aplicar actualizaciones en rangos de horas

Indica los siguientes parámetros para que los equipos apliquen las actualizaciones disponibles dentro de un rango de horas concreto:

- Hora de inicio
- Hora de fin

Para aplicar las actualizaciones en cualquier momento haz clic en la casilla de selección **A cualquier hora**.

Aplicar actualizaciones en fechas determinadas

Utiliza el desplegable para indicar las fechas en las que se aplicará la actualización:

- **En cualquier fecha**: las actualizaciones se aplicarán el día que estén disponibles. Esta opción no limita la actualización de Panda Endpoint Protection a fechas concretas.
- **Los siguientes días de la semana**: utiliza las casillas de selección para establecer los días de la semana en los que Panda Endpoint Protection se actualizará. La actualización se producirá el primer día de la semana que coincida con la selección del administrador en caso de haber una actualización disponible.

- **Los siguientes días del mes**: utiliza los desplegables para establecer un rango de días hábiles dentro del mes en los que Panda Endpoint Protection se actualizará. La actualización se producirá el primer día del mes que coincida con los seleccionados por el administrador en caso de haber una actualización disponible.
- **Los siguientes días**: utiliza los desplegables para establecer un rango de días hábiles dentro del calendario en los que Panda Endpoint Protection se actualizará. Los rangos definidos en esta opción se establecen de forma absoluta para casos en que el administrador quiera establecer rangos que no se repiten en el tiempo. De esta forma, se permite definir rangos de fechas concretas de actualización, pasadas las cuales dejan de tener efecto. Este método requiere redefinir los rangos de actualización de forma constante una vez hayan vencido.

Reinicio de equipos

Panda Endpoint Protection permite definir la lógica de reinicios en caso de que sea necesario, mediante el desplegable situado al final de la pantalla de configuración:

- **No reiniciar automáticamente**: se mostrará al usuario una ventana en intervalos de tiempo cada vez más cortos, aconsejando el reinicio de la máquina para aplicar la actualización.
- **Reiniciar automáticamente sólo las estaciones de trabajo**.
- **Reiniciar automáticamente sólo los servidores**.
- **Reiniciar automáticamente tanto estaciones de trabajo como servidores**.

Actualización del agente de comunicaciones

La actualización del agente Panda se ejecuta bajo demanda. Panda Endpoint Protection incluirá una notificación en la consola de administración indicando la existencia de una nueva versión del agente, y el administrador podrá lanzar la actualización cuando lo desee.

La actualización del agente Panda no requiere reinicio del equipo del usuario y suele implicar cambios y mejoras en la consola de administración que facilitan la gestión de la seguridad.

Limitación de la descarga de actualizaciones del agente de comunicaciones a través de equipos caché y Proxy Panda

La descarga de las actualizaciones del agente de comunicaciones puede realizarse directamente desde Internet o también a través de un equipo caché o Proxy Panda. Consulta **Configuración de las descargas mediante equipos caché** en la página **307** y **Configuración de listas de acceso a través de proxy** en la página **305**.

Según el sistema operativo instalado en el equipo, pueden existir ciertas limitaciones a la hora de utilizar un método de descarga u otro:

- **Equipos con sistema operativo Windows o macOS**: pueden descargar instaladores a través de equipos caché, proxy e Internet.
- **Equipos con sistema operativo Linux**: al utilizar el gestor de paquetes propio de la distribución para hacer las descargas no pueden descargar instaladores a través de equipos caché ni Proxy Panda .

Los equipos caché almacenan los instaladores hasta que dejan de ser válidos, momento en el que se eliminarán.

Actualizaciones del conocimiento

La configuración de la actualización del fichero de firmas en Panda Endpoint Protection se realiza en el perfil de configuración de seguridad asignado al equipo, según sea su tipo.

Descarga del conocimiento a través de equipos caché y Proxy Panda

Los sistemas operativos Windows, Linux y macOS pueden descargar el conocimiento directamente desde Internet, así como desde equipos con el rol de Proxy Panda o caché asignado.

Los equipos caché almacenan los ficheros de firmas hasta que dejan de ser válidos, momento en el que se eliminarán.

Dispositivos Windows, Linux y macOS

La configuración se realiza en los perfiles de tipo **Estaciones y Servidores**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

En la pestaña **General** las opciones disponibles son:

- **Actualizaciones automáticas de conocimiento**: habilita o deshabilita la descarga del fichero de firmas. Si se deshabilita el fichero de firmas nunca será actualizado.

Se desaconseja totalmente deshabilitar la actualización del conocimiento. Los equipos con la protección sin actualizar serán más vulnerables en el corto plazo frente a las amenazas avanzadas y el malware.

- **Realizar un análisis en segundo plano cada vez que se actualice el conocimiento**: lanza de forma automática un análisis cada vez que un fichero de firmas se descarga en el equipo. El análisis tendrá prioridad mínima para no interferir en el trabajo del usuario.

Dispositivos Android

La configuración se realiza en los perfiles **Dispositivos móviles**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

Panda Endpoint Protection permite limitar las actualizaciones del software de forma que no consuman datos de conexiones móviles sujetas a tarificación.

Haz clic en el botón de **Activación** para restringir las actualizaciones a aquellos momentos en que el smartphone o tablet tenga conexión wifi disponible.

Actualización de la consola de administración

El administrador de la red puede indicar el momento en el que iniciar el proceso para actualizar la versión de la consola en los servidores de Panda Security. En caso contrario, Panda Security actualizará de forma automática la consola de administración a la última versión disponible.

Para realizar este proceso, es necesario que la cuenta de usuario que accede a la consola web tenga asignado el rol de Control total. Consulta **El rol Control total** en la página **67**.

Consideraciones previas para actualizar la versión de la consola

Aunque se trata de un proceso que se produce íntegramente en los servidores de Panda Security, el cambio de versión de la consola puede acarrear la disponibilidad de nuevas versiones del software de seguridad instalado en los equipos del cliente. Esto puede generar un consumo de tráfico y la necesidad de reiniciar los equipos en algunos casos. Para mitigar el consumo de tráfico en las actualizaciones, consulta **Configuración de las descargas mediante equipos caché** en la página **307**.

La actualización de la consola es transparente para el administrador y no verá interrumpido su funcionamiento. Cuando el proceso se completa, la consola se cierra automáticamente. Al iniciar de nuevo la sesión, el administrador accederá a la consola actualizada.

Iniciar la actualización de la consola de administración

- Haz clic en icono **Notificaciones web** situado en la parte derecha del menú superior. Se desplegarán las notificaciones pendientes de leer.
- Si hay una actualización de la consola disponible, se muestra el mensaje **Nueva versión de la consola de Administración** con el enlace **Nuevas características y mejoras**, la versión de la consola a la que se actualizará, y el botón **Actualizar la consola ahora**. Este tipo de notificación no se puede eliminar ya que no tiene el icono asociado. Consulta **Icono Notificaciones web** en la página **33**.

*El botón **Actualizar la consola ahora** solo se muestra si la cuenta de usuario utilizada para acceder a la consola de administración tiene asignado el rol Control total. En caso de no tener el nivel de permisos requeridos, este botón no se mostrará.*

- Al hacer clic en el botón, la petición de actualización entra en la cola del servidor para ser procesada. El tiempo de permanencia máximo de la petición en la cola del servidor son 10 minutos.
- Una vez procesada la petición, se inicia el proceso de actualización y la notificación muestra el texto **Actualización en curso**. Si alguna cuenta de usuario inicia la sesión en la consola será expulsada, y mientras dure el proceso de actualización no será posible iniciar sesión en la consola de administración.
- Al cabo de un tiempo que depende del número de equipos administrados y de los datos almacenados en la consola, se finalizará el proceso de actualización a la nueva versión.

Cancelar la actualización

- Una vez iniciado el proceso de actualización, haz clic en el icono **Notificaciones web** situado en la parte derecha del menú superior. Se desplegarán las notificaciones pendientes de leer.
- Si hay una actualización de la consola en la cola de peticiones pero que todavía no se ha iniciado, se muestra el mensaje **Nueva versión de la consola de Administración** con el enlace **Nuevas características y mejoras** y el botón **Cancelar la actualización**.
- Para eliminar de la cola la petición de actualización, haz clic en el botón **Cancelar la actualización**. El botón desparecerá y se mostrará nuevamente el botón **Actualizar la consola ahora**.

Capítulo 8

Gestión de equipos y dispositivos

La consola web muestra los dispositivos administrados de forma ordenada y flexible, aplicando distintas estrategias que permiten localizarlos rápidamente para facilitar su gestión.

Para que un equipo de la red sea gestionable por Panda Endpoint Protection se requiere como mínimo de la instalación del agente Panda en el equipo. Los equipos sin licencia pero con el agente Panda instalado, aparecerán en la consola de administración, aunque su protección estará desactualizada y no podrán ejecutar tareas, análisis ni otras acciones vinculadas con el servicio de protección.

Contenido del capítulo

La zona equipos

La zona **Equipos** es el área de la consola web donde se gestionan los dispositivos integrados en Panda Endpoint Protection.

Para acceder a la ventana de administración de equipos, haz clic en el menú superior **Equipos**. Se mostrarán dos zonas diferenciados: el panel lateral con el **Árbol de equipos (1)** y el panel central con el **Listado de equipos (2)**. Ambos paneles trabajan de forma conjunta: al seleccionar una rama del árbol de equipos, el listado de equipos se actualiza con todos sus equipos asignados.

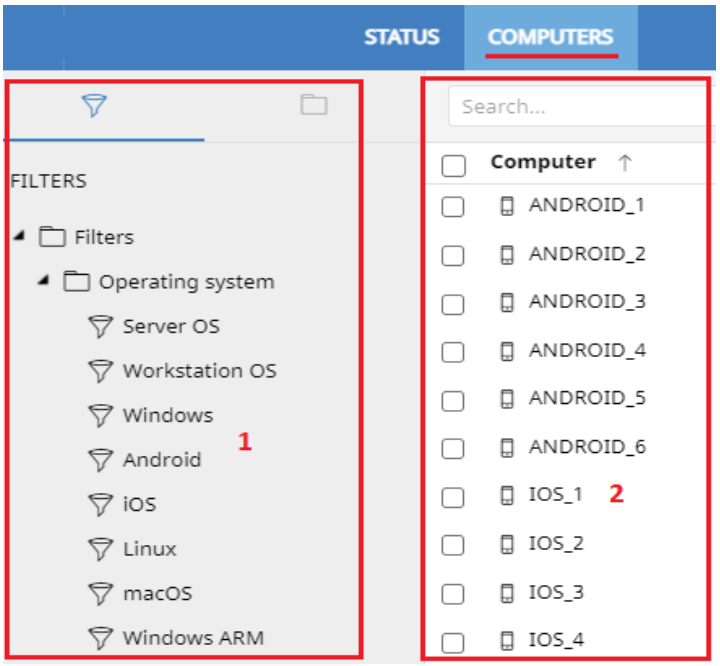


Figura 8.1: Vista general de los paneles en la zona Equipos

Mostrar equipos en subgrupos

Para ampliar o limitar el listado de los equipos activa o desactiva la opción **Mostrar equipos de los subgrupos** disponible en el menú de contexto general.

- Si la opción está activada, al seleccionar una rama del árbol se mostrarán todos los equipos que pertenecen a ella y a todas las ramas de orden inferior.
- Si la opción esta desactivada, al seleccionar una rama del árbol se mostrarán únicamente todos los equipos que pertenecen a ella.

El panel Árbol de equipos

Panda Endpoint Protection representa la estructura de equipos mediante el **Árbol de equipos (1)**, que presenta dos vistas o árboles independientes **(2)**:

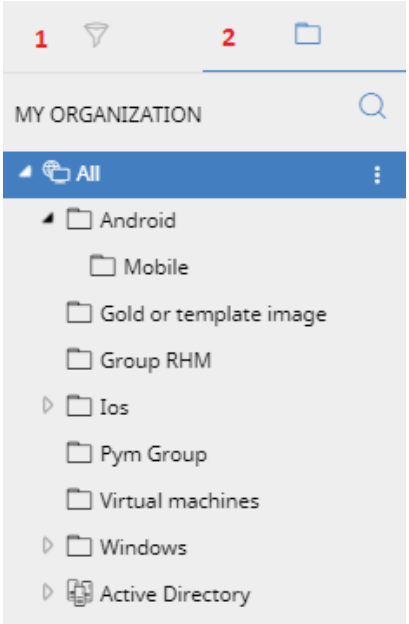


Figura 8.2: El panel Árbol de equipos

- **Árbol de filtros (1)**: gestiona los equipos de la red mediante agrupaciones dinámicas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma automática.
- **Árbol de grupos (2)**: gestiona los equipos de la red mediante agrupaciones estáticas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma manual.

Los dos árboles muestran el parque de dispositivos del cliente de distintas formas, con el objeto de favorecer la ejecución de tareas de diferentes tipos, tales como:

- Localizar los equipos que cumplan con características determinadas, relativas al hardware, software o a la seguridad.

- Asignar perfiles de configuración de seguridad de forma rápida.
- Ejecutar acciones de resolución sobre grupos de equipos.

Para localizar equipos desprotegidos o de características determinadas relativas a la seguridad o al estado de la protección consulta ***Visibilidad del malware y del parque informático*** *en la página* ***469****. Para asignar perfiles de configuración de seguridad consulta* ***Asignación manual y automática de configuraciones*** *en la página* ***287****. Para ejecutar tareas de resolución de problemas consulta* ***Herramientas de resolución*** *en la página* ***589****.*

Al pasar el puntero del ratón por las ramas del árbol de filtros y de grupos se muestra el icono de menú de contexto. Haz clic para desplegar un menú emergente con todas las operaciones disponibles sobre la rama del árbol seleccionada.

Árbol de filtros

Es una de las dos vistas del Árbol de equipos, y permite agrupar de forma dinámica los equipos en la red mediante reglas y condiciones que describen características de los dispositivos. Estas reglas se pueden combinar mediante operaciones lógicas para producir expresiones complejas.

Para acceder al Árbol de filtros haz clic en el icono del filtro desde el panel de la izquierda. Al hacer clic en los diferentes elementos del árbol, el panel de la derecha se actualiza, presentando todos los equipos que cumplen con los criterios establecidos en el filtro seleccionado.

Definición de filtro

Son agrupaciones dinámicas de equipos. La pertenencia de un equipo a un filtro se determina de forma automática cuando el equipo en cuestión cumple con las condiciones de pertenencia al filtro que haya configurado el administrador.

Un equipo puede pertenecer a más de un filtro.

Un filtro está constituido por un conjunto de reglas o condiciones que los equipos tendrán que satisfacer para pertenecer a aquél. En la medida en que el equipo cumpla con las características descritas formará parte del filtro; de la misma forma, cuando un equipo cambie su estado y no cumpla los criterios de pertenencia, automáticamente dejará de formar parte de la agrupación descrita por el filtro.

Los filtros se pueden ordenar de forma manual agrupándolos en carpetas, con el criterio que el administrador considere oportuno.

Filtros predefinidos

Panda Endpoint Protection incorpora filtros de uso muy común que el administrador puede utilizar desde el primer momento para ordenar y localizar equipos en la red. Los filtros predeterminados se pueden modificar o borrar.

No es posible recuperar un filtro predeterminado que haya sido borrado.

Nombre	Grupo	Descripción
SO de servidores	Sistema operativo	Lista los equipos con un sistema operativo de tipo Servidor instalado.
SO de estaciones	Sistema operativo	Lista los equipos con un Sistema operativo de tipo estación de trabajo.
Windows	Sistema operativo	Lista todos los equipos con sistema operativo Windows instalado.
Android	Sistema operativo	Lista todos los dispositivos con sistema operativo Android instalado.
iOS	Sistema operativo	Lista todos los dispositivos con sistema operativo iOS instalado.
Linux	Sistema operativo	Lista todos los equipos con sistema operativo Linux instalado.
macOS	Sistema operativo	Lista todos los equipos con sistema operativo macOS instalado.
Windows ARM	Sistema operativo	Lista todos los equipos con sistema operativo Windows y microprocesador ARM.
Estaciones y servidores	Tipo de sistema	Lista los equipos físicos de sobremesa o servidores.

Nombre	Grupo	Descripción
Portátiles	Tipo de sistema	Lista los equipos físicos portátiles.
Móviles y tablets	Tipo de sistema	Lista los dispositivos de tipo smartphone y tablet.
Virtuales	Tipo de sistema	Lista los equipos virtualizados.
< 2GB de memoria	Hardware	Lista los equipos con una memoria menor que 2 GByte
Java	Software	Lista todos los equipos que tiene instalado el SDK JRE Java.
Adobe Acrobat Reader	Software	Lista todos los equipos que tiene instalado el software Acrobat Reader.
Adobe Flash Player	Software	Lista todos los equipos que tiene instalado el plugin de reproducción Flash.
Google Chrome	Software	Lista todos los equipos que tiene instalado el navegador Chrome.
Mozilla Firefox	Software	Lista todos los equipos que tiene instalado el navegador Firefox.
Servidores Exchange	Software	Lista los equipos que tienen instalado el servidor de correo Microsoft Exchange Server.

Tabla 8.1: Listado de filtros predefinidos

Crear y organizar filtros

Para crear y organizar filtros haz clic en el icono de menú de contexto de las ramas del árbol de filtros. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Crear carpetas

- Haz clic en el menú de contexto de la rama donde quieres crear la carpeta y haz clic en **Añadir carpeta**.
- Introduce el nombre de la carpeta y haz clic en **Aceptar**.

Una carpeta no puede depender de un filtro. Si seleccionas un filtro antes de crear la carpeta, ésta se creará al mismo nivel que el filtro, compartiendo su carpeta padre.

Crear filtros

Para crear un filtro es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto de la carpeta en el árbol donde será creado el filtro.
    - Si deseas crear una estructura jerárquica de filtros, crea carpetas contenedoras y mueve los filtros dentro de ellas. Una carpeta puede contender otras carpetas con filtros.
- Haz clic en **Añadir filtro**.
- Introduce el nombre del filtro. No es necesario que sea un nombre único. El resto de la configuración se detalla en **Configurar filtros**.

Borrar filtros y carpetas

Para borrar un filtro o una carpeta haz clic en el menú de contexto de la rama a borrar y elige la opción **Eliminar**. La rama se borrará junto a todos sus descendientes.

No se permite borrar el nodo raíz Filtros.

Mover y copiar filtros y carpetas

- Haz clic en el menú de contexto de la rama a copiar o mover.
- Haz clic en **Mover** o **Hacer una copia**. Se mostrará una ventana emergente con el árbol de filtros de destino.
- Selecciona la carpeta de destino y pulsa **Aceptar**.

No es posible copiar carpetas de filtros. Únicamente se permite la copia de filtros.

Renombrar filtros y carpetas

- Haz clic en el menú de contexto de la rama a renombrar.
- Haz clic en **Renombrar**.
- Introduce el nuevo nombre.

No es posible renombrar la carpeta raíz. Para renombrar un filtro es necesario editarlo.

Buscar filtros

En infraestructuras IT muy grandes, el árbol de filtros puede contener un gran número de elementos, lo que dificulta la localización de un determinado filtro.

Para localizar un filtro, sigue los siguientes pasos:

- Haz clic en el icono situado en la parte superior del árbol de filtros. Se mostrará una caja de texto debajo.
- Escribe las letras que forman parte del nombre del filtro que quieres buscar. Se mostrarán los filtros que comiencen, terminen o contengan la cadena de caracteres indicada.
- Una vez realizada la búsqueda, selecciona el filtro de tu interés y haz clic en el icono . Se volverá a mostrar el árbol de filtros completo pero conservando la selección sobre el filtro que has buscado.

Configurar filtros

Haz clic en el menú de contexto del filtro y elige la entrada **Editar filtro** del menú. Se mostrará la ventana de configuración de filtros.

Un filtro está formado por una o más reglas, relacionados entre sí mediante operadores lógicos Y / O. Un equipo formará parte de un filtro si cumple con los valores especificados en las reglas del filtro.

El esquema general de un filtro se compone de cuatro bloques:

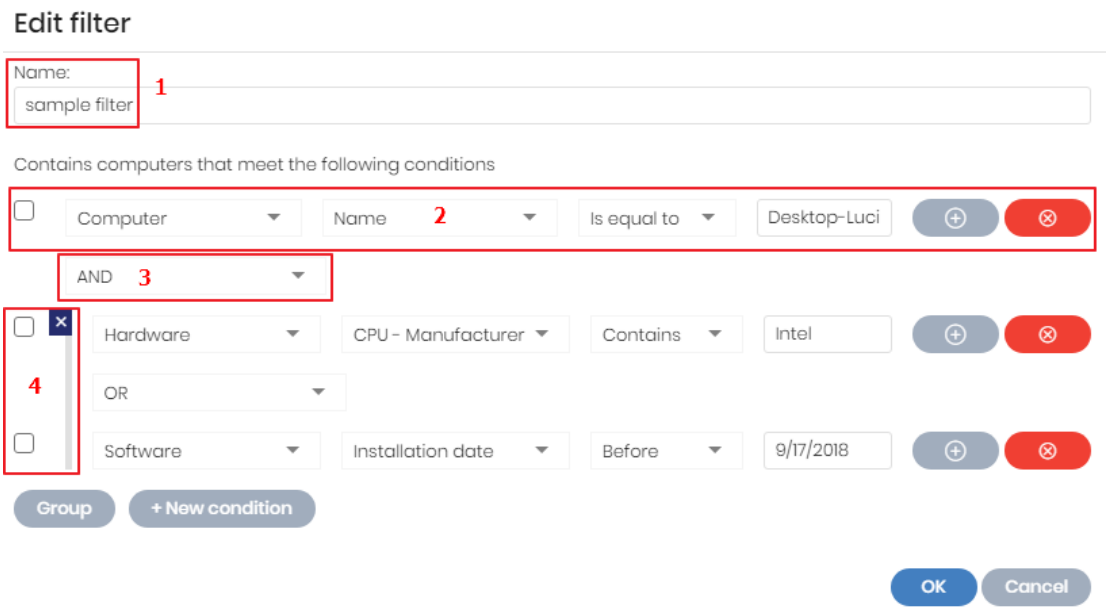


Figura 8.3: Vista general de configuración de un filtro

- **Nombre del filtro (1)**: identifica al filtro.
- **Reglas de filtrado (2)**: construye condiciones indivisibles de pertenencia al filtro. Una regla de filtrado únicamente comprueba una característica concreta de los equipos de la red.
- **Operadores lógicos (3)**: combina dos reglas de filtrado mediante los operadores lógicos Y o O.
- **Agrupaciones (4)**: varían el orden de evaluación de las reglas de filtrado configuradas y relacionadas mediante operadores lógicos.

Reglas de filtrado

Una regla de filtrado se compone de los elementos mostrados a continuación:

- **Categoría**: agrupa las propiedades en secciones para facilitar su localización.
- **Propiedad**: característica del equipo que se evaluará para determinar su pertenencia al filtro.
- **Operador**: establece el modo de comparación del contenido de la propiedad del equipo con el valor de referencia que establezca el administrador para el filtro.
- **Valor**: contenido de la propiedad. Dependiendo del tipo de propiedad el campo valor cambiará para ajustarse a entradas de tipo fecha, literales etc.

Para añadir reglas de filtrado a un filtro haz clic en el icono y para borrarlas en el icono .

Operadores lógicos

Para combinar dos reglas en un mismo filtro se utilizan los operadores lógicos Y y O. Al añadir una segunda regla y sucesivas a un filtro se mostrará de forma automática un desplegable con los

operadores lógicos disponibles, que se aplicarán a las reglas adyacentes.

Agrupaciones de reglas de filtrado

Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores que relacionan las reglas de filtrado introducidas.

Para encerrar dos o más reglas en un paréntesis crea una agrupación marcando con las casillas de selección las reglas que formarán parte del grupo y haz clic en el botón **Agrupación**. Se mostrará una línea delgada que abarcará las reglas de filtrado que forman parte de la agrupación.

Mediante el uso de paréntesis se definen agrupaciones de varios niveles para poder anidar grupos de operandos en una expresión lógica.

Casos de uso comunes

A continuación se indican, a modo de ejemplo, algunos casos de uso de filtros muy utilizados por los administradores de redes:

Equipos Windows según el procesador instalado (x86, x64, ARM64)

Lista los equipos que tienen instalado el sistema operativo Windows y su microprocesador pertenece a la familia ARM.

Este filtro se compone de dos condiciones unidas mediante el operador Y:

- **Condición 1:**
  - **Categoría**: Equipo
  - **Propiedad**: Plataforma
  - **Condición**: Es igual a
  - **Valor**: Windows
- **Condición 2:**
  - **Categoría**: Equipo
  - **Propiedad**: Arquitectura
  - **Condición**: Es igual a
  - **Valor**: {nombre de la arquitectura: ARM64, x86, x64}

Equipos sin parches instalados

Lista los equipos que no tienen un determinado parche instalado. Para obtener más información sobre Panda Patch Management ,consulta **Panda Patch Management (Actualización de programas vulnerables)** en la página **345**.

- **Categoría**: Programas
- **Propiedad**: Nombre del software
- **Condición**: No contiene
- **Valor**: {Nombre del parche}

Equipos sin conectar con la nube de Panda Security en X días

Lista los equipos que no conectaron con la nube de Panda Security en el intervalo configurado:

- **Categoría**: Equipo
- **Propiedad**: Última conexión
- **Condición**: Antes de
- **Valor**: {Fecha en formato dd/mm/aa}

Equipos que no conectan con los servicios de inteligencia de seguridad de Panda Security

Localiza todos los equipos que muestran problemas de conexión con la nube de Panda Security:

- **Categoría**: Seguridad
- **Propiedad**: Conexión para inteligencia colectiva
- **Condición**: Es igual a
- **Valor**: Con problemas
- **Regla**:
    - **Categoría**: Seguridad
    - **Propiedad**: Conexión para inteligencia colectiva
    - **Condición**: Es igual a
    - **Valor**: Con problemas

Integración con otras herramientas de gestión

Muestra los equipos que coinciden con alguno de los nombres de equipo especificados en un listado obtenido por una herramienta de terceros. Cada línea del listado deberá terminar con un retorno de carro y será considerada como un nombre de equipo.

- **Categoría**: Equipo
- **Propiedad**: Nombre
- **Condición**: En
- **Valor**: listado de nombres de equipo

Equipos no compatibles con firma de drivers SHA-256

- **Categoría**: Equipo
- **Propiedad**: Soporta drivers con firma SHA-256
- **Condición**: Es igual a
- **Valor**: Falso

Equipos con IP pública

Busca los equipos que accedieron a Internet a través de un dispositivo (router / proxy / extremo VPN) con la IP indicada.

- **Categoría**: Equipo
- **Propiedad**: Dirección IP pública
- **Condición**: Es igual a (Para buscar los equipos que acceden a Internet a través de un dispositivo que tiene una IP concreta)

Equipos descubiertos en directorio activo

Busca los equipos administrados y no administrados que han sido descubiertos mediante el método de descubrimiento en directorios activos.

- **Categoría**: Equipo
- **Propiedad**: Última vez visto en directorio activo
- **Condición**: Está entre (para buscar los equipos descubiertos entre fechas concretas)

Árbol de grupos

El árbol de grupos reúne de forma estática los equipos en la red en las agrupaciones definidas por el administrador.

Para acceder al árbol de grupos:

- Haz clic en el icono de carpeta en el panel lateral.
- Al hacer clic en las diferentes ramas del árbol, el panel de la derecha se actualiza, presentando todos los equipos que contienen el grupo seleccionado y sus subgrupos.

Definición de grupo

Es un contenedor de equipos asignados de forma manual por el administrador. El árbol de grupos admite crear una estructura de n niveles compuesta por grupos, subgrupos y equipos.

El máximo nivel de profundidad del árbol es 10.

Tipos de grupos

Tipo de grupo	Descripción
Grupo raíz	Grupo padre del que cuelgan el resto de carpetas.
Grupos nativos	Grupos estándar de Panda Endpoint Protection que soportan todas las operaciones (movimiento, renombrado, borrado etc.) Pueden contener otros grupos nativos y equipos.
Grupos IP	Grupo nativo con IPs o rangos de IPs asociados para acelerar la integración de nuevos equipos en el servicio de seguridad.
Grupos Directorio Activo	Replican la estructura del Directorio Activo instalado en la empresa, por esta razón tienen limitadas algunas operaciones. Pueden contener otros grupos de Directorio Activo y equipos.
Grupo raíz del directorio activo	Abarca todos los dominios del Directorio Activo configurados en la red de la organización. Contiene grupos de dominio Directorio Activo.
Grupo de dominio Active Directory	Ramas del Directorio Activo que representan dominios. Contienen otros grupos de dominio Directorio Activo, grupos Directorio Activo y equipos.

Tabla 8.2: Tipos de grupos en Panda Endpoint Protection

El tamaño de la organización, lo homogéneos que sean los equipos gestionados y la presencia o no de un servidor de Directorio Activo en la red de la empresa determinará la estructura del árbol de grupos. La estructura de grupos podrá variar desde un árbol plano de un único nivel para los casos más sencillos, hasta una estructura compleja con varios niveles, para redes grandes formadas por equipos muy heterogéneos.

En un momento determinado un equipo solo puede pertenecer a un grupo, a diferencia de los filtros donde un equipo puede pertenecer a varios simultáneamente.

Grupos de Directorio Activo

Para las organizaciones que tienen instalado un servidor de Directorio Activo en la red, Panda Endpoint Protection puede obtener de forma automática la estructura configurada y replicarla en el árbol de grupos: los agentes Panda reportan a la consola Web el grupo del Directorio Activo al que pertenecen y, conforme se despliegan los agentes en los equipos, el árbol se completará con las distintas unidades organizativas. De esta manera, bajo la rama se presentará una distribución de los equipos familiar para el administrador, con el objeto de acelerar la localización de dispositivos y su gestión.

Para mantener la coherencia entre el Directorio activo de la empresa y el árbol representado en la consola de administración, los grupos de directorio activo no son modificables desde la consola de Panda Endpoint Protection: únicamente cambiarán cuando lo haga la estructura de Directorio Activo de la empresa. Los cambios se replicarán en la consola Web de Panda Endpoint Protection transcurrido un máximo de una hora.

Si el administrador de la red mueve en la consola de Panda Endpoint Protection un equipo que reside en un grupo de tipo Directorio Activo a un grupo nativo o al grupo raíz se romperá la sincronización con el Directorio Activo de la empresa. Cualquier cambio de grupo en el Directorio Activo de la empresa que afecte a ese equipo no se replicará en la consola de Panda Endpoint Protection.

Para restablecer la sincronización de un equipo y así continuar replicando la estructura original del Directorio Activo de la empresa en la consola de Panda Endpoint Protection consulta **Restaurar la pertenencia de varios equipos a su grupo Active Directory**.

Crear y organizar grupos

Para acceder a las operaciones disponibles sobre grupos haz clic en el icono de menú de contexto de las ramas del árbol de grupos. Se mostrará un menú emergente con las opciones permitidas para esa rama en particular.

Crear grupos

- Selecciona el menú de contexto del grupo padre del cual dependerá el grupo a crear, y haz clic en **Añadir grupo**.
- Introduce el nombre del grupo en la caja de texto **Nombre** y haz clic en el botón **Añadir**.

No es posible crear grupos de Directorio Activo en el árbol de grupos. Solo se replicarán los grupos y unidades organizativas creadas en el servidor de Directorio Activo de la empresa.

Si deseas que los equipos sobre los cuales se va a instalar un agente Panda Endpoint Protection se muevan a un determinado grupo según su IP sigue los pasos mostrados a continuación:

- Haz clic en el enlace **Añadir reglas de asignación automática por IPs**, se mostrará una caja de texto donde añadir las IPs de los equipos que serán movidos al grupo.
- Especifica IPs individuales separadas por comas o rangos de IPs separados por un guion.

El movimiento del equipo se efectuará únicamente en el momento de la instalación del agente Panda Endpoint Protection. Si posteriormente el equipo cambia de IP éste permanecerá en el grupo asignado inicialmente.

Borrar grupos

Selecciona el menú de contexto del grupo a borrar. Si el grupo contiene subgrupos o equipos asignados, la consola de administración mostrará un error.

No se permite borrar el nodo raíz Todos.

Para borrar los grupos vacíos de tipo Directorio Activo que cuelgan de uno dado, haz clic en el menú de contexto del grupo y selecciona **Eliminar grupos vacíos**.

Mover grupos

- Selecciona el menú de contexto del grupo a mover.
- Haz clic en **Mover**. Se mostrará una ventana emergente con el árbol de grupos de destino.
- Selecciona el grupo de destino y pulsa **Aceptar**.

No se permite el movimiento del nodo raíz Todos ni de grupos Directorio Activo.

Renombrar grupos

- Selecciona el menú de contexto del grupo a renombrar.
- Haz clic en **Cambiar nombre**.

- Introduce el nuevo nombre.

No es posible renombrar el grupo raíz Todos ni grupos Directorio Activo.

Importar reglas de asignación por IPs en grupos ya creados

Para añadir direcciones IP a un grupo nativo ya creado sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo nativo que no sea el grupo Todos y haz clic en la opción **Importar reglas de asignación por IPs**. Se mostrará una ventana para poder arrastrar un fichero con las direcciones IP.
- El fichero deberá contener una o más lineas de texto con el formato mostrado a continuación:
    - Para direcciones IP independientes añadir una linea por cada una de ellas a asignar:
        - `.\Grupo\Grupo\Grupo (tabulación) IP`
    - Para rangos de IPs, añadir una linea por cada rango a asignar:
        - `.\Grupo\Grupo\Grupo (tabulación) ExtremoInferiorIP-ExtremoSuperiorIP`
    - Todos las rutas indicadas son interpretadas por Panda Endpoint Protection como relativas a la rama del árbol seleccionada.
    - Si los grupos indicados en el fichero no existieran, Panda Endpoint Protection los creará y asignará la direcciones IP indicadas.
- Haz clic en **Importar**. Las IPs se asignarán a los grupos indicados en el fichero y el árbol de grupos actualizará sus iconos para mostrar el cambio de tipo de grupo.

Las direcciones IP previamente asignadas a un grupo IP se borrarán al importar un fichero con nuevos pares grupo - IP.

Una vez terminado el procedimiento, todos los equipos nuevos que se integren en Panda Endpoint Protection se moverán al grupo indicado según su dirección IP.

Exportar reglas de asignación por IPs

Para exportar un fichero con las reglas de grupos IP ya asignadas sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo IP, y haz clic en la opción **Exportar reglas de asignación por IPs**. Se descargará un fichero .csv con las reglas de asignación de IPs

establecidas en el grupo IP y en todos sus descendientes.

- El formato del fichero .csv es el indicado en el punto **Importar reglas de asignación por IPs en grupos ya creados**.

Mover equipos entre grupos

Para mover uno o varios equipos a un grupo, el administrador puede seguir varias estrategias:

Mover conjuntos de equipos a grupos

- Selecciona el grupo **Todos** para listar todos los equipos administrados o utiliza la herramienta de búsqueda para localizar los equipos a mover.
- Selecciona con las casillas los equipos en el panel de listado de equipos.
- Haz clic en el icono ⋮ situado a la derecha de la barra de búsqueda. Se mostrará un menú desplegable con la opción **Mover a**. Haz clic para mostrar el árbol de grupos destino.
- Selecciona el grupo destino del árbol de grupos mostrado.

Mover un único equipo a un grupo

Para asignar un único equipo a un grupo se pueden seguir varias estrategias:

- Seguir el método mostrado más arriba para asignar conjuntos de equipos a grupos, pero seleccionando un único equipo.
- Seleccionar con la casilla el equipo dentro del panel de listado de equipos que quieras asignar y haz clic en el icono de menú ⋮ situado en la parte derecha de la fila de ese equipo.
- Desde la ventana de detalles del propio equipo a mover:
    - Dentro en el panel de listado de equipos haz clic en el equipo que quieras mover para mostrar la ventana de detalles.
    - Localiza el campo **Grupo** y haz clic en el botón **Cambiar**. Se mostrará una ventana con el árbol de grupos de destino.
    - Selecciona el grupo destino y haz clic en **Aceptar**.

Mover equipos desde grupos Active Directory

Un equipo que reside en un grupo Directorio Activo está sincronizado con el Directorio Activo de la empresa y por tanto no es posible mover lo a otro grupo de tipo Directorio Activo desde la consola de Panda Endpoint Protection. En este caso será necesario mover el equipo en el Directorio Activo de la empresa y esperar como máximo 1 hora hasta que la consola Panda Endpoint Protection se sincronice. Sin embargo, un equipo que reside en un grupo de tipo Directorio Activo sí puede moverse a un grupo nativo.

Al mover un equipo desde un grupo de tipo Directorio Activo a un grupo nativo se dejarán de sincronizar los cambios del grupo de origen. Consulta ***Grupos de Directorio Activo*** *para más información.*

Mover equipos hacia grupos Active Directory

No es posible mover un equipo desde un grupo nativo a un grupo Directorio Activo específico. El único movimiento que se permite es mover el equipo al grupo de tipo Directorio Activo en el que reside dentro del servidor de Directorio Activo de la empresa. Para ello haz clic en el menú de contexto del equipo y selecciona **Mover a su ruta de Active Directory**.

Restaurar la pertenencia de varios equipos a su grupo Active Directory

Para restablecer la pertenencia de equipos a su grupo Directorio Activo original haz clic en el menú de contexto de un grupo de Directorio Activo y selecciona la opción **Recuperar los equipos de esta rama de Active Directory**. Todos los equipos que pertenecen a ese grupo en el Directorio Activo de la empresa y que el administrador movió a otros grupos dentro de la consola Panda Endpoint Protection serán devueltos a su grupo original.

Filtrar resultados por grupos

La función de filtrar resultados por grupos muestra en la consola únicamente la información generada por los equipos de la red que pertenecen a los grupos elegidos por el administrador. Es una forma rápida de establecer un filtro que afecta de forma transversal a toda la consola (listados, paneles de control y configuraciones) y que ayuda a resaltar los datos de interés para el administrador.

Configurar el filtro de resultados por grupos

Para configurar el filtrado de resultados por grupos sigue los pasos mostrados a continuación:

- Haz clic en el botón del menú superior. Se desplegará una ventana con el árbol de grupos.
- Selecciona los grupos que se mostrarán de entre el árbol de equipos y pulsa en el botón **Aceptar**.

La consola mostrará únicamente la información generada de los equipos que pertenecen a los grupos seleccionados.

Filtrar equipos no afecta a la visibilidad de tareas, ni al envío de alertas por email, ni al envío programado de informes ejecutivos.

Filtrar grupos

En infraestructuras IT muy grandes, el árbol de grupos puede contener un gran número de nodos distribuidos en muchos niveles, dificultando la localización de un determinado grupo. Para filtrar el

árbol de grupos y mostrar únicamente aquellos que coincidan con el patrón de caracteres introducido:

- Haz clic en el icono situado en la parte superior del árbol de grupos. Se mostrará una caja de texto debajo.
- Introduce las letras que forman parte del nombre del grupo a buscar. Se mostrarán los grupos que comiencen, terminen o contengan la cadena de caracteres indicada.
- Una vez realizada la búsqueda, selecciona el grupo de tu interés y haz clic en el icono para volver a mostrar el árbol de grupos completo, pero conservando la selección del grupo.

Listados disponibles para gestionar equipos

Listado de equipos

Acceso al listado

- Haz clic en el menú superior **Equipos**. En el panel lateral izquierdo se mostrará el árbol de equipos o de carpetas, y en el panel lateral derecho un listado con todos los equipos administrados en la red.
- Haz clic en un elemento del árbol de grupos o de filtros en el panel lateral izquierdo. El panel derecho se refrescará con el contenido del elemento seleccionado.

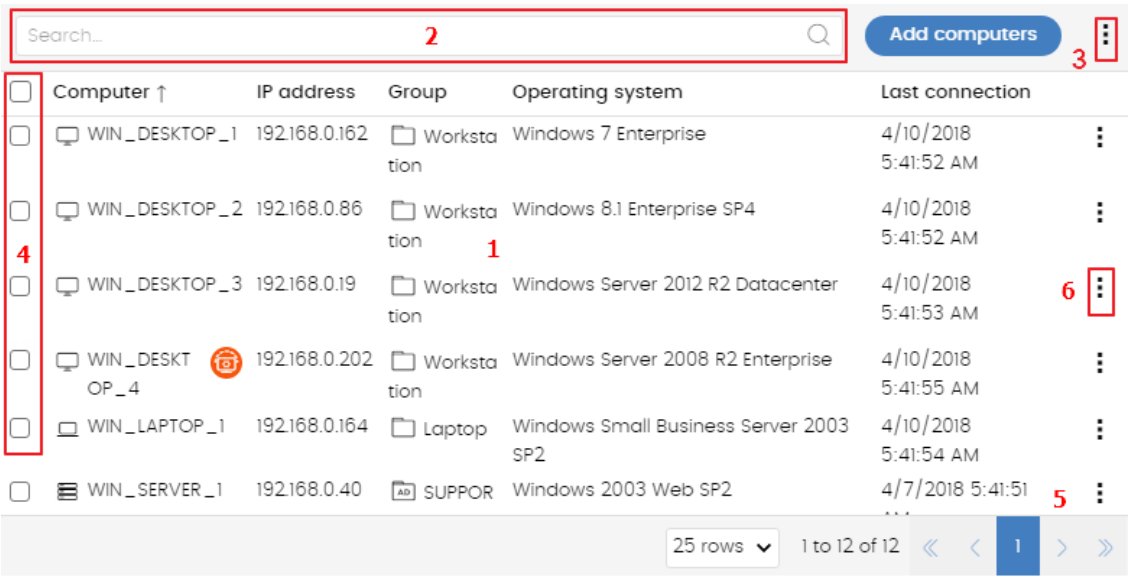


Figura 8.4: El panel Listado de equipos

Permisos requeridos

El acceso al panel **Listado de equipos** no requiere permisos adicionales para el administrador.

Equipos

El listado de equipos muestra los puestos de usuario y servidores correspondientes al grupo o filtro seleccionado en el árbol de equipos. Además, incluye herramientas que permiten gestionar uno o varios equipos simultáneamente.

A continuación, se muestra un esquema del panel listado de equipos:

- **(1)** Listado de equipos que pertenecen a la rama del árbol seleccionada.
- **(2)**Herramienta de búsqueda: localiza equipos por su nombre, descripción, dirección IP o último usuario registrado, admitiendo coincidencias parciales sin tener en cuenta mayúsculas y minúsculas.
- **(3)** Menú de contexto general: aplica una misma acción a varios equipos.
- **(4)** Casillas de selección de equipos.
- **(5)** Sistema de paginación en la parte inferior del panel.
- **(6)** Menú de contexto del equipo.

El listado de equipos es configurable para poder adaptar la información mostrada a las necesidades del administrador.

Para añadir o quitar columnas, haz clic en el menú de contexto situado en la parte superior derecha y elige la opción **Añadir o eliminar columnas**. Se mostrarán las columnas disponibles y el enlace **Columnas por defecto** para restaurar la configuración del listado a sus valores iniciales.

Utiliza el menú de contexto para exportar el listado de equipos. La exportación puede incluir todos los datos del listado de equipos (consulta **Campos mostrados en el fichero exportado**) o una versión reducida (consulta**Campos mostrados en el fichero reducido exportado**), muy útil cuando se trata de una gran número de equipos.

- Haz clic en el icono para desplegar las opciones de listados.
- Haz clic en el icono correspondiente al tipo de listado para generar las exportaciones o las exportaciones reducidas del listado de los equipos.

Por cada equipo se incluye la información mostrada a continuación:

Campo	Descripción	Valores
Equipo	Nombre del equipo y su tipo.	Cadena de caracteres: • Puesto de trabajo o servidor • Equipo portátil

Campo	Descripción	Valores
		• Dispositivo móvil (smart-phone o tablet Android)
Estado del equipo	Reinstalación del agente: • Reinstalando agente. • Error en la reinstalación del agente Reinstalación de la protección: • Reinstalando la protección • Error en la reinstalación de la protección. • Pendiente de reinicio.	Icono
Dirección IP	Dirección IP principal del equipo.	Dirección IP
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo y su tipo.	Cadena de caracteres: • Grupo • Grupo IP • Dominio AD o raíz del Directorio Activo • Unidad Organizativa • Raíz del árbol de grupos

Campo	Descripción	Valores
Ruta del directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Nombre y versión del sistema operativo instalado en el equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security.	Fecha

Tabla 8.3: Campos del Listado de equipos

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Lista separada por comas de todas las direcciones IP de las tarjetas instaladas en el equipo.	Cadena de caracteres
Dirección IP pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta la red del cliente con Internet.	Dirección IP
Direcciones físicas (MAC)	Lista separada por comas de todas las direcciones físicas de las tarjetas instaladas en el equipo.	Cadena de caracteres

Campo	Descripción	Valores
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Fecha arranque del sistema	Fecha en la que se inicio el equipo por última vez.	Fecha
Fecha de instalación	Fecha en la que el Software Panda Endpoint Protection se instaló con éxito en el equipo.	Fecha
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado.	Booleano
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o, por el contrario, se regenera a su estado original.	Booleano

Campo	Descripción	Valores
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección.	Fecha
Licencias	Producto licenciado en el equipo.	Panda Endpoint Protection
Configuración de red	Nombre de la configuración de red que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de red.	Cadena de caracteres
Seguridad para estaciones y servidores	Nombre de la configuración de seguridad que afecta al puesto de trabajo o servidor.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
Seguridad para dispositivos Android	Nombre de la configuración de seguridad que afecta al dispositivo móvil.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
Seguridad para dispositivos iOS	Nombre de la configuración de seguridad que afecta al dispositivo móvil.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
Ajustes por equipo	Nombre de la configuración de ajustes que afecta al equipo.	Cadena de caracteres
Configuración	Nombre de la carpeta donde fue asignada	Cadena de caracteres

Campo	Descripción	Valores
heredada de	la configuración de ajustes.	
Data Control	Nombre de la configuración de seguimiento de información personal (Panda Data Control) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguimiento de información personal.	Cadena de caracteres
Gestión de parches	Nombre de la configuración de parcheo (Panda Patch Management) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de parcheo.	Cadena de caracteres
Cifrado	Nombre de la configuración de cifrado (Panda Full Encryption) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de cifrado.	Cadena de caracteres
Bloqueo de programas	Nombre de la configuración de programas bloqueados por el administrador que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de bloqueo de programas.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Último usuario logueado	Nombres de las cuentas de usuario separados por coma que mantienen una sesión interactiva abierta en equipos Windows.	Cadena de caracteres
Acción solicitada	Petición pendiente de ejecutar o en	• Reinicio

Campo	Descripción	Valores
	ejecución.	• Reinstalación de protección • Reinstalación de agente
Error en la acción solicitada	Tipo de error reportado en la acción solicitada.	• Credenciales incorrectas • Equipo descubridor no disponible • No es posible conectar con el equipo • Sistema operativo no soportado • No es posible descargar el instalador del agente • No es posible copiar el instalador del agente • No es posible desinstalar el agente • No es posible instalar el agente • No es posible registrar el agente • Requiere intervención del usuario
Último proxy utilizado	Método de acceso empleado por Panda Endpoint Protection en su ultima conexión con la nube de Panda Security. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su	Cadena de caracteres

Campo	Descripción	Valores
	valor correcto.	
Shadow Copies	Indica el estado de la funcionalidad: • Activo • Desactivado • **Error 2010**: No se ha podido habilitar el servicio de Shadow copies. • **Error 2011**: Se ha producido un error al crear el último Shadow copy.	Enumeración
Última copia realizada	Fecha y hora en la que se realizó la última copia.	Fecha

Tabla 8.4: Campos del fichero exportado Listado de equipos

Campos mostrados en el fichero reducido exportado

Al seleccionar **Exportación reducida**se genera un fichero con la siguiente información:

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	• Estación • Portátil • Servidor
Dirección IP	Lista separada por comas de todas las direcciones IP de las tarjetas instaladas en el equipo.	Cadena de caracteres
Dirección IP Pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta la red del cliente con Internet.	Dirección IP
Direcciones físicas (MAC)	Lista separada por comas de todas las direcciones físicas de las tarjetas instaladas en el equipo.	Cadena de caracteres

Campo	Descripción	Valores
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Directorio Activo	Ruta dentro del árbol de Directorio Activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Última vez visto en directorio activo	Fecha en la que el equipo fue visto por última vez en el Directorio Activo.	
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Fecha de arranque del sistema	Fecha en la que se inicio el equipo por última vez.	Cadena de caracteres
Fecha de instalación	Fecha en la que el SoftwarePanda Endpoint Protection se instaló con éxito en el equipo.	Fecha
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado.	Booleano
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de	Booleano

Campo	Descripción	Valores
	almacenamiento que perdura entre reinicios o, por el contrario, se regenera a su estado original.	
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección.	Fecha
Licencias	Producto licenciado en el equipo.	Panda Endpoint Protection
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Último usuario logueado	Nombres de las cuentas de usuario separados por coma que mantienen una sesión interactiva abierta en equipos Windows.	Cadena de caracteres
Acción solicitada	Petición pendiente de ejecutar o en ejecución.	• Reinicio • Reinstalación de protección • Reinstalación de agente
Error en acción solicitada	Tipo de error reportado en la acción solicitada.	• Credenciales incorrectas • Equipo descubridor no disponible • No es posible conectar con el equipo • Sistema operativo no soportado • No es posible descargar el

Campo	Descripción	Valores
		instalador del agente • No es posible copiar el instalador del agente • No es posible registrar el agente • Requiere intervención del usuario
Último proxy utilizado por agente	Método de acceso empleado por Panda Endpoint Protection en su ultima conexión con la nube dePanda Security. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.	Cadena de caracteres
Shadow Copies	Indica el estado de la funcionalidad: • **Activo** • **Desactivado** • **Error 2010**: No se ha podido habilitar el servicio de Shadow Copies • **Error 2011**: Se ha producido un error al crear el último Shadow Copies	Enumeración
Última copia realizada	Fecha y hora en la que se realizo la última copia.	Fecha

Tabla 8.5: Campos del fichero exportado reducido Listado de equipos

Herramientas de filtrado

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres.

Tabla 8.6: Filtros disponibles en el listado Equipos

Herramientas de gestión

Las herramientas de gestión están disponibles en:

- Al seleccionar uno o más equipos con las casillas de selección **(4)**, la herramienta de búsqueda **(2)** se oculta y en su lugar se muestra la barra de acciones **(7)**.

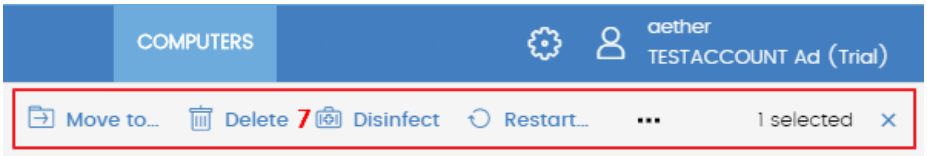


Figura 8.5: Barra de acciones solapando a la herramienta de búsqueda

  Al seleccionar la casilla de selección situada a la altura de la cabecera de la tabla **(4)**, se marcarán todos los equipos de la página actual del listado y se mostrará el mensaje **Seleccionar las xx filas del listado**, que permite marcar todos los equipos del listado independientemente de la paginación.

- Al hacer clic en el menú de contexto **(6)** asociado a un equipo o dispositivo móvil.

Acción	Descripción
Mover a	Muestra una ventana con el árbol de grupos. Elige un grupo como destino de los equipos seleccionados. Los equipos heredarán las configuraciones asignadas al grupo de destino. Para más información, consulta **Crear y gestionar configuraciones** en la página **285**.
Mover a su ruta de directorio activo	Mueve los equipos seleccionados al grupo que se corresponde con la unidad organizativa del directorio activo de la empresa.
Eliminar	Borra el equipo de la consola y desinstala el software de cliente Panda Endpoint Protection. Para más información, consulta **Desinstalar el software** en la página **178**.
Analizar ahora	Para una introducción a las tareas de análisis, consulta **Análisis y desinfección bajo demanda de equipos** en la página **591**. Para una

Acción	Descripción
	descripción completa, consulta **Tareas** en la página **603**.
Programar análisis	Para una introducción a las tareas de análisis, consulta **Análisis y desinfección bajo demanda de equipos** en la página **591**. Para una descripción completa, consulta **Tareas** en la página **603**.
Reiniciar	Reinicia el equipo. Par más información, consulta **Reiniciar equipos** en la página **599**.
Visualizar parches disponibles	Abre el listado **Parches disponibles** filtrado por el equipo seleccionado. Consulta **Parches disponibles** en la página **396**.
Programar instalación de parches	Para obtener información sobre cómo instalar parches en equipos Windows, consulta **Panda Patch Management(Actualización de programas vulnerables)** en la página **345**.
Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Para más información, consulta **Reinstalación remota** en la página **182**.
Reinstalar agente	Reinstala el agente en caso de mal funcionamiento. Para más información, consulta **Reinstalación remota** en la página **182**.
Seleccionados	Anula la selección actual de equipos.
Notificar un problema	Envía un informe al departamento de soporte de Panda Security para diagnosticar problemas en el equipo.

Tabla 8.7: Herramientas para gestionar equipos

El panel Mis listados

Acceso al panel Mis listados

- Haz clic en el menú superior **Estado** y en el menú lateral **Mis listados**. Se mostrará una ventana con todos los listados disponibles.

- Selecciona en el grupo **General** el listado **Hardware**, **Software** o **Equipos con nombre duplicado**.

Para obtener información sobre los tipos de listados y como operar con ellos, consulta ***Gestión de listados*** *en la página* ***42****.*

Consulta el capítulo correspondiente al grupo al que pertenece cada listado para obtener información acerca de sus campos y de las herramientas de filtrado y búsqueda que implementan.

Permisos requeridos

El acceso al panel **Mis listados** no requiere permisos adicionales para el administrador.

Hardware

Contiene los componentes hardware instalados en cada equipo del parque informático. Un mismo componente hardware se mostrará de forma independiente cada vez que sea detectado en un equipo.

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo que contiene el componente hardware.	Cadena de caracteres: • Puesto de trabajo o servidor. • Equipo portátil. • Dispositivo móvil (smart-phone o tablet Android).
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
CPU	Marca y modelo del microprocesador instalado en	Cadena de

Campo	Descripción	Valores
	el equipo. Se indica el número de núcleos / cores instalados entre paréntesis.	caracteres
Memoria	Cantidad total de memoria RAM instalada.	Cadena de caracteres
Capacidad de disco	Suma de la capacidad de todos los discos duros internos conectados al equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	Fecha
Menú de contexto	Herramientas de gestión. Para más información, consulta **Herramientas de gestión**.	

Tabla 8.8: Campos del Listado de hardware

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección IP pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta la red del cliente con Internet.	Cadena de caracteres

Campo	Descripción	Valores
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Sistema	Nombre del modelo hardware del equipo.	Cadena de caracteres
CPU-X	Marca, modelo y características de la CPU numerada X.	Cadena de caracteres
CPU-X Número de núcleos	Número de núcleos o cores de la CPU numerada X.	Numérico
CPU-X Número de procesadores lógicos	Número de núcleos lógicos mostrados al sistema operativo por el sistema de HyperThreading / SMT (Simultaneous MultiThreading).	Numérico
Memoria	Suma de todos los bancos de memoria RAM instalados en el equipo.	Cadena de caracteres

Campo	Descripción	Valores
Disco-X Capacidad	Espacio total del medio de almacenamiento interno numerado X.	Cadena de caracteres
Disco-X Particiones	Numero de particiones reportadas al sistema operativo del medio de almacenamiento interno numerado X.	Numérico
Versión de especificación del TPM	Versiones de las APIs compatibles con el chip TPM.	Cadena de caracteres
BIOS - número de serie	Número de serie de la BIOS del equipo.	Cadena de caracteres

Tabla 8.9: Campos del fichero exportado Hardware

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Marca del sistema operativo.	• Windows • Android

Tabla 8.10: Filtros disponibles en el Listado de hardware

Software

Contiene todos los programas instalados en los equipos de la red. Por cada paquete se indica el número de equipos que lo tienen instalado e información sobre la versión y su fabricante.

Al hacer clic en un paquete de software, se abrirá el listado **Equipos** filtrado por el paquete seleccionado, para mostrar los equipos que lo tienen instalado.

Campo	Descripción	Valores
Nombre	Nombre del paquete software encontrado en el	Cadena de

Campo	Descripción	Valores
	parque.	caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 8.11: Campos del Listado de software

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 8.12: Campos del Listado de software

Campos mostrados en el excel de detalle

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Equipo que contiene el paquete encontrado.	Numérico
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Fecha de instalación	Fecha en la que se instaló el software.	Fecha
Tamaño	Tamaño del software instalado.	Numérico
Versión	Versión interna del paquete software.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 8.13: Campos del listado exportado de detalle

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Marca del sistema operativo.	• Windows • Linux • macOS • Android

Tabla 8.14: Filtros disponibles en el Listado de software

Ventana listado de equipos

Al hacer clic en una de las filas del listado se mostrará el listado de equipos filtrado por el paquete de software seleccionado. Para obtener más información, consulta **Equipos**.

Equipos con nombre duplicado

Muestra los equipos detectados en la red con el mismo nombre y que pertenecen al mismo dominio. De cada grupo de equipos duplicados Panda Endpoint Protection considerará correcto el equipo con la fecha de conexión a la nube de Panda Security más reciente, y el resto como erróneos. El equipo considerado correcto se excluirá del listado para que el administrador seleccione y elimine el resto de equipos de una vez.

Para eliminar los equipos duplicados selecciónalos mediante las casillas de selección y la opción **Eliminar** del menú de herramientas. Se mostrará una ventana preguntando si quieres desinstalar el agente Panda Endpoint Protection o no.

*Borrar equipos del listado **Equipos con nombre duplicado** sin desinstalar el agente Panda Endpoint Protection únicamente los borra de la consola de Panda Endpoint Protection. Un equipo así eliminado volverá a aparecer en la consola de Panda Endpoint Protection al ponerse en contacto con la nube. Ante un borrado masivo de equipos sin tener la seguridad de cuales están realmente duplicados se recomienda no desinstalar previamente el agente de ningún equipo y comprobar qué equipos reaparecen en la consola.*

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo	Cadena de caracteres: • Puesto de equipo o servidor • Equipo portátil. • Dispositivo móvil (smart-phone o tablet Android).
Dirección IP	Dirección principal del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel del parche aplicado.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	Fecha

Tabla 8.15: Campos del Listado de Equipos con nombre duplicado

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de

Campo	Descripción	Valores
		caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de instalación	Fecha en la que el Software Panda Endpoint Protection se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Directorio Activo	Ruta completa del equipo en el Directorio Activo de la empresa.	Cadena de caracteres

Campo	Descripción	Valores
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres
Fecha arranque del sistema	Fecha en la que se inició el equipo por última vez.	Fecha

Tabla 8.16: Campos del fichero exportado Equipos con nombre duplicado

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Marca del sistema operativo.	• Todos • Windows • Linux • macOS • Android
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días

Campo	Descripción	Valores
		• Hace más de 7 días • Hace más de 30 días

Tabla 8.17: Filtros disponibles en el listado Equipos con nombre duplicado

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Para obtener más información, consulta **Información de equipo** .

Información de equipo

Al seleccionar un dispositivo en el panel de listado de equipos se muestra una ventana con el detalle de la información del hardware y software instalado, así como de la configuración de seguridad asignada.

La ventana de detalle del equipo se divide en varias secciones:

Figura 8.6: Vista general de la información de equipo

- **General (1)**: información que ayuda a identificar el equipo.
- **Alertas de equipo (2)**: mensajes con problemas potenciales asociados al equipo.
- **Detalles (3)**: resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Detecciones (4)**: estado de la seguridad del equipo.

- **Hardware (5)**: hardware instalado en el equipo, componentes y periféricos conectados, su consumo y uso.
- **Software (6)**: paquetes de software instalados en el equipo, su versión y un registro de cambios.
- **Configuración (7)**: configuraciones de seguridad y otras asignadas al equipo.
- **Barra de herramientas (8)**: agrupa las operaciones disponibles para aplicar sobre el equipo administrado.
- **Iconos ocultos (9)**: si la ventana no es lo suficientemente grande, parte de las herramientas se ocultan agrupadas.
- **Riesgo del equipo (10):** gráfica de distribución que muestra el nivel de riesgo global del equipo y los riesgos detectados en él. Consulta **Listados del módulo Evaluación de riesgos** en la página **509**.

Sección general (1)

Contiene la siguiente información para todos los tipos de dispositivo:

Campo	Descripción
Equipo	Nombre del equipo e icono de estado del equipo.
Dirección IP	Dirección IP del equipo.
Último usuario logueado	Nombre del último usuario logueado en el equipo.
Descripción	Información del equipo asignada por el administrador.
Grupo	Carpeta del árbol de grupos a la que pertenece el equipo.
Ruta del directorio activo	Ruta completa del equipo en el Directorio Activo de la empresa.
Dominio	Dominio al que pertenece el equipo.
Sistema operativo	Versión completa del sistema operativo instalado en el equipo.
Última conexión	Fecha de la última conexión del software de cliente con la nube de Panda Endpoint Protection

Campo	Descripción
Riesgo del equipo	Gráfica de distribución que muestra el nivel de riesgo global del equipo y los riesgos detectados en él. Consulta **Listados del módulo Evaluación de riesgos** en la página **509**.

Tabla 8.18: Campos de la sección general de la información del equipo

Sección general en dispositivos móviles

En los dispositivos móviles la sección general **(1)** y la sección de alertas de equipo **(2)** se sustituyen por el panel de antirrobo, que le permite al administrador lanzar acciones remotas sobre los dispositivos gestionados.

*En el caso de los dispositivos iOS, las acciones que se pueden llevar a cabo varían dependiendo de si el dispositivo móvil está integrado en un MDM o no. Consulta **Instalación en sistemas iOS** en la página **149**.*

*Consulta **Antirrobo** en la página **341** para activar la funcionalidad antirrobo en los dispositivos móviles y la configuración del modo privado.*

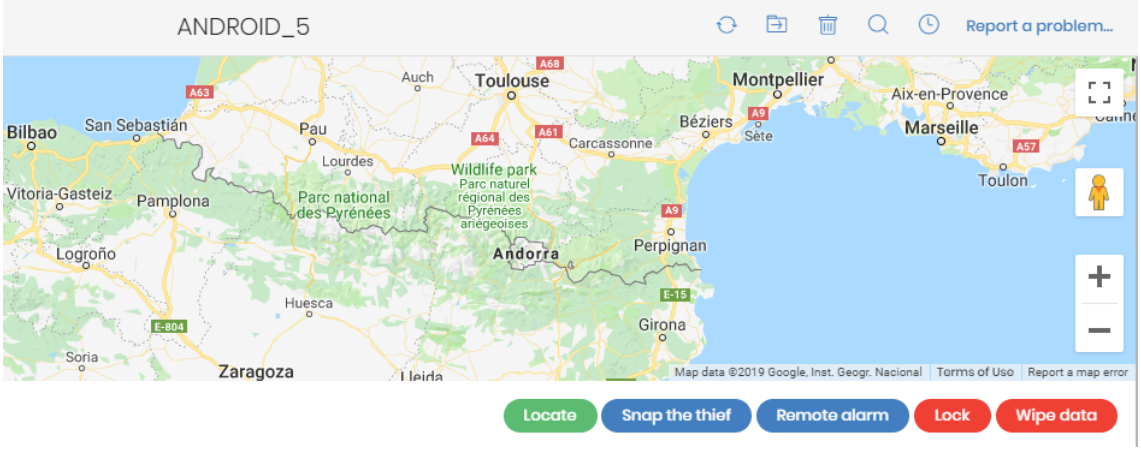


Figura 8.7: Panel de antirrobo mostrado en dispositivos móviles

Las acciones disponibles son:

Acción	Descripción
Localizar	• **Modo privado activado**: la consola muestra una ventana donde se solicita al administrador el número que el usuario del dispositivo tecleó al activar el

Acción	Descripción
	modo privado. Si el número es correcto el servidor Panda Endpoint Protection solicita al dispositivo sus coordenadas y el mapa de la consola se actualiza con la nueva posición. • **Modo privado desactivado**: el servidor Panda Endpoint Protection solicita directamente al dispositivo sus coordenadas y el mapa de la consola se actualiza con la nueva posición.
Foto al ladrón	Esta opción no está disponible para dispositivos iOS. Muestra una ventana donde el administrador puede introducir la dirección de correo a la que se enviará la fotografía y permite elegir el momento en el que se realizará: • **Ahora**: el agente Panda Endpoint Protection enviará la fotografía a la cuenta de correo indicada en el momento de recibir la petición. • **Al tocar la pantalla**: el agente Panda Endpoint Protection enviará la fotografía a la cuenta de correo indicada en el momento en que el usuario o el ladrón toquen la pantalla del terminal.
Alarma remota	Muestra una ventana donde el administrador podrá introducir un mensaje para el usuario y un número de contacto. Una vez enviada la petición el mensaje se mostrará en el dispositivo del usuario junto a la reproducción de un sonido al máximo volumen, aunque el dispositivo esté bloqueado. Haz clic en la casilla de selección **No reproducir ningún sonido** si unicamente quieres mostrar el mensaje.
Bloquear	Bloquea el teléfono móvil para impedir su uso en caso de pérdida o robo, y establece en el dispositivo el PIN introducido en la consola del administrador para desbloquearlo. Aunque la consola del administrador siempre pide el PIN de desbloqueo al activar esta funcionalidad, el comportamiento es diferente en función de la versión de Android o iOS que utiliza el dispositivo. **Android**: • **Versión inferior a 7**: se establece el PIN solicitado al administrador para desbloquear el dispositivo. • **Versión entre 7 y 10**: solo se establece el PIN solicitado al administrador para desbloquear el dispositivo si el usuario no tiene establecido un PIN previamente. Si el usuario tiene un PIN establecido, se utilizará éste para

Acción	Descripción
	desbloquear el dispositivo, independientemente del PIN que introduzca el administrador en la consola. • **Versión igual y superior a 11**: si el usuario tiene un PIN establecido, se utilizará para desbloquear el dispositivo, independientemente del PIN que introduzca el administrador en la consola. Si no tiene un PIN establecido se apaga la pantalla del dispositivo y no se establece ningún PIN de desbloqueo. **iOS**: • **Versión 13 o superior**: si el usuario tiene un PIN establecido, se utilizará para desbloquear el dispositivo, independientemente del PIN que introduzca el administrador en la consola. Si no tiene un PIN establecido se apaga la pantalla del dispositivo y no se establece ningún PIN de desbloqueo.
Borrar datos	El dispositivo se formatea y se devuelve a su estado original, destruyendo todos los datos y aplicaciones que contenía.

Tabla 8.19: Acciones soportadas por el módulo antirrobo para dispositivos móviles

Sección alertas de equipo (2)

Las alertas describen los problemas encontrados en los equipos de la red en lo que respecta al funcionamiento de Panda Endpoint Protection y su motivo, así como indicaciones para solucionarlos.

En ocasiones las alertas **(1)** van acompañadas de códigos **(2)**.

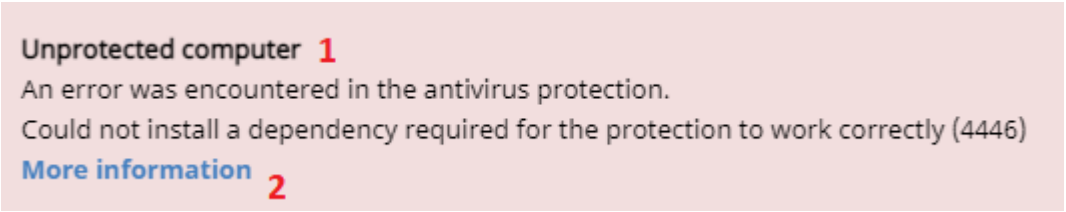


Figura 8.8: Alerta de Equipo desprotegido y código asociado

Cada código se relaciona con un error que puede aparecer durante o después de la instalación de la protección en los equipos. Para acceder a toda la información sobre los diferentes códigos, consulta **https://www.pandasecurity.com/es/support/card?id=700031**

A continuación, se muestra un resumen de los tipos de alertas generadas y las acciones recomendadas para su resolución.

Licencias

Alerta	Descripción	Referencia
Equipo sin licencia	No hay licencias libres para asignar al equipo. Retira una licencia asignada o adquiere más licencias de Panda Endpoint Protection.	Para más información, consulta **Liberar licencias** en la página **188**.
	Hay licencias libres pero no se han asignado a este equipo.	Para más información, consulta **Asignar licencias** en la página **187**.

Tabla 8.20: Alertas relacionadas con la asignación de licencias

Errores en el proceso de instalación del software de protección

Los errores ocurridos durante el proceso de instalación del software de protección se reflejan mediante un código de error, su código extendido de error asociado y un subcódigo extendido de error, si están disponibles. Para más información, consulta ***Campos mostrados en fichero exportado*** *en la página* ***481****.*

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha producido un error instalando la protección en el equipo. En el caso de errores de origen conocido se mostrará una descripción de la causa que lo motiva. Si el origen es desconocido, se mostrará el código de error asociado.	Para más información, consulta **Funcionalidades del producto y requisitos** en la página **619**.

Alerta	Descripción	Referencia
	El equipo requiere un reinicio para completar la instalación debido a una desinstalación previa.	Para más información, consulta **Reiniciar equipos** en la página **599** .
	El agente no cuenta con los permisos necesarios en equipos macOS.	Para más información, consulta **Requisitos de plataformas macOS** en la página **629**.
	Error al instalar en macOS 13 Ventura. El usuario debe permitir EndpointProtectionService en Login Items	Para más información, consulta **Requisitos de plataformas macOS** en la página **629**.
	El Kernel del equipo Linux no es compatible.	Para más información consulta **https://www.pandasecurity.com/en/support/card?id=700031**.
	Versión del Unbreakable Enterprise Kernel (UEK) no es compatible.	Para más información consulta **https://www.pandasecurity.com/en/support/card?id=700031**.
Error instalando Data Control	Se ha producido un error instalando Panda Data Control en el equipo.	Para más información, consulta **Requisitos de Panda Data Control**.
Error instalando la protección y Data Control	Se ha producido un error instalando la protección y el módulo en el equipo.	Para más información, consulta **Funcionalidades del producto y requisitos** en la página **619** y **Requisitos de Panda Data Control**.
Error instalando el	Se ha producido un error instalando el	Para más información, consulta**Comprobar que Panda Patch Management funciona**

Alerta	Descripción	Referencia
gestor de parches	módulo de gestión de parches.	correctamente en la página 350.
Error instalando el módulo de cifrado	Se ha producido un error instalando el módulo de cifrado.	Para más información, consulta Requisitos mínimos de Panda Full Encryption en la página 439 .
Error instalando el agente de Panda	Credenciales incorrectas.	Para más información, consulta Equipos sin conexión en la página 473.
	El equipo descubridor no está disponible.	Para más información, consulta el widget Paneles/Widgets del módulo de seguridad en la página 470 y Asignar el rol de descubridor a un equipo en la página 114.
	No es posible conectar con el equipo destinatario del paquete de instalación por estar apagado o no cumplir con los requisitos de hardware y de red.	Para más información, consulta el widget Paneles/Widgets del módulo de seguridad en la página 470 y Funcionalidades del producto y requisitos en la página 619.
	El sistema operativo del equipo no está soportado.	Para más información, consulta Funcionalidades del producto y requisitos en la página 619.
	No es posible descargar el instalador del agente por un fallo de red.	Para más información, consulta Funcionalidades del producto y requisitos en la página 619.
	No es posible copiar el instalador del agente en el equipo por falta de espacio.	Para más información, consulta Funcionalidades del producto y requisitos en la página 619.

Alerta	Descripción	Referencia
	No es posible instalar el agente por no cumplirse los requisitos de instalación remota o el equipo está apagado.	Para más información, consulta el widget **Equipos sin conexión** en la página **473** y **Funcionalidades del producto y requisitos** en la página **619**.
	No es posible registrar el agente.	Para más información, consulta el widget **Equipos sin conexión** en la página **473** y **Funcionalidades del producto y requisitos** en la página **619**.
Error comunicando con servidores.	El equipo no puede conectar con alguno de los servidores de la nube de Panda.	Para más información, consulta **Funcionalidades del producto y requisitos** en la página **619**.

Tabla 8.21: Alertas relacionadas con la instalación del software Panda Endpoint Protection

Errores en el proceso de reinstalación del software de protección

*Los errores ocurridos durante el proceso de instalación del software de protección se reflejan mediante un código de error, su código extendido de error asociado y un subcódigo extendido de error, si están disponibles. Para más información, consulta **Campos del fichero exportado Estado de protección de los equipos** en la página **1**.*

Alerta	Descripción	Referencia
Pendiente de reinstalación de la protección	El administrador solicitó la reinstalación de la protección de este equipo pero todavía no se ha realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	Consulta el widget **Equipos sin conexión** en la página **473** y **Requisitos de la funcionalidad de reinstalación remota** en la página **182**.
Pendiente de reinstalación del	El administrador solicitó la reinstalación del agente en este equipo pero todavía no se ha	Consulta el widget **Equipos sin conexión** en

Alerta	Descripción	Referencia
agente	realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	la página 473 y Requisitos de la funcionalidad de reinstalación remota en la página 182.
Error instalando el agente de Panda	Credenciales incorrectas.	Consulta el widget Equipos sin conexión en la página 473.
	Equipo descubridor no disponible.	Consulta el widget Equipos sin conexión en la página 473.
	No es posible conectar con el equipo por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 473 y Requisitos de la funcionalidad de reinstalación remota en la página 182.
	Sistema operativo no soportado por no cumplir con los requisitos de instalación remota.	Consulta Requisitos de la funcionalidad de reinstalación remota en la página 182.
	No es posible descargar el instalador del agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 473 y Requisitos de la funcionalidad de reinstalación remota en la página 182.
	No es posible copiar el instalador del agente por no estar encendido o no cumplir los requisitos de instalación remota.	Consulta el widget Equipos sin conexión en la página 473 y Requisitos de la

Alerta	Descripción	Referencia
		funcionalidad de reinstalación remota en la página **182**.
	No es posible desinstalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget **Equipos sin conexión** en la página **473** y **Requisitos de la funcionalidad de reinstalación remota** en la página **182**.
	No es posible instalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget **Equipos sin conexión** en la página **473** y**Requisitos de la funcionalidad de reinstalación remota** en la página **182**
	No es posible registrar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget **Equipos sin conexión** en la página **473** y **Requisitos de la funcionalidad de reinstalación remota** en la página **182**
	Requiere intervención del usuario.	Consulta el widget **Equipos sin conexión** en la página **473** y **Requisitos de la funcionalidad de reinstalación remota** en la página **182**

Tabla 8.22: Alertas relacionadas con la reinstalación del agente Panda Endpoint Protection

Errores de funcionamiento del software Panda Endpoint Protection

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha detectado un error en la protección antivirus. Reinicia el equipo para solucionar el problema.	Consulta Reiniciar equipos en la página 599
Error cifrando el equipo	No se puede cifrar el equipo por un error.	Consulta Reiniciar equipos en la página 599

Tabla 8.23: Alertas relacionadas con el mal funcionamiento del software Panda Endpoint Protection

Acción pendiente del usuario o del administrador

Alerta	Descripción	Referencia
Cifrado pendiente de acción del usuario	Para completar el proceso de cifrado es necesario que el usuario reinicie el equipo o introduzca las credenciales de cifrado.	Consulta Proceso de cifrado y descifrado en Windows en la página 441 y Proceso de cifrado y descifrado en macOS
Pendiente de reinicio	El administrador ha solicitado el reinicio de este equipo pero todavía no se ha completado por falta de conexión o por no haberse cumplido el plazo para ejecutar un inicio forzoso.	Consulta el widget Equipos sin conexión en la página 473
Reinstalando la protección	El administrador ha solicitado la reinstalación de la protección en este equipo y todavía no se ha completado por estar el equipo apagado, sin conexión, sin completar el plazo configurado antes del reinicio o por estar el proceso en curso.	Consulta Reinstalación remota en la página 182
Equipo desprotegido	La protección antivirus está desactivada. Activa la protección.	Consulta Asignación manual y automática de configuraciones en la página 287, Crear y

Alerta	Descripción	Referencia
		gestionar configuraciones en la página **285** y **Antivirus** en la página **324**
Equipo sin conexión desde hace X días	Es posible que el equipo esté apagado o no se cumplan los requisitos de acceso a la red.	Consulta **Funcionalidades del producto y requisitos** en la página **619**.
Protección desactualizada	La protección necesita que el usuario local reinicie manualmente el equipo para completar la instalación*.	* solo reproducible en las versiones Windows Home y Starter.
Problemas de conexión con los equipos de Panda Security	El equipo no se puede conectar correctamente con los servidores donde se almacena la inteligencia de seguridad.	Consulta **Funcionalidades del producto y requisitos** en la página **619**.
El administrador ha cambiado el estado de las protecciones desde la consola local	El administrador cambió la configuración de la protección desde el propio agente instalado en el equipo del usuario o servidor. De esta forma, la configuración actual no coincide con la establecida desde la consola web.	
No es posible actualizar la protección de este equipo a la última versión.	Las nuevas versiones de la protección requieren que el sistema operativo reconozca los drivers firmados con el formato SHA-256. Este equipo no soporta dicho formato de firma, y por lo tanto no es posible actualizar la protección instalada en él a la última versión.	Consulta **Compatibilidad con firma de drivers SHA-256** en la página **628**.

Tabla 8.24: Alertas relacionadas con la falta de acción del usuario o administrador de la red

Equipo desactualizado

Alerta	Descripción	Referencia
Protección desactualizada	La protección requiere que el equipo se reinicie para terminar la actualización.	Para más información, consulta **Reiniciar equipos** en la página **599**
	Se ha producido un error intentando actualizar la protección. Comprueba que se cumplen los requisitos de hardware y de red.	Consulta **Funcionalidades del producto y requisitos** en la página **619** y el espacio disponible en disco en **Sección Hardware (5)**.
	Las actualizaciones están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta **Actualización del motor de protección** en la página **202**.
Conocimiento sobre malware y otras amenazas desactualizado	Las actualizaciones de conocimiento están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta **Actualizaciones del conocimiento** en la página **205**.

Tabla 8.25: Alertas relacionadas con el software Panda Endpoint Protection desactualizado

Alertas de dispositivos móviles

Alerta	Descripción	Referencia
El dispositivo iOS ha sido manipulado	El dispositivo ha sido manipulado (Jailbreak) para permitir la instalación de aplicaciones sin certificar, y puede estar expuesto a fuga de datos privados o a la desinstalación del software de seguridad.	Contacta con el usuario.
Dispositivos iOS o Android con falta de	El usuario del dispositivo ha denegado algún permiso a Panda Endpoint Protection, lo	Consulta **Requisitos de plataformas iOS**

Alerta	Descripción	Referencia
permisos	que limita su funcionamiento.	en la página 634 y Requisitos de plataformas Android en la página 633.

Tabla 8.26: Alertas de dispositivos móviles

Sección Detalles (3)

La información se divide en los siguientes apartados:

- **Equipo**: información de la configuración del dispositivo ofrecida por el agente Panda.
- **Seguridad**: estado de las protecciones de Panda Endpoint Protection.
- **Protección de datos** (sólo Windows): estado de los módulos que protegen el contenido de los datos almacenados en el equipo.

Equipo

Campo	Descripción
Riesgo	Para los dispositivos Android, se muestra la gráfica de distribución que muestra el nivel de riesgo global del equipo y los riesgos detectados en él. Consulta Listados del módulo Evaluación de riesgos en la página 509.
Nombre	Nombre del equipo.
Descripción	Texto descriptivo asignado por el administrador.
Direcciones IP	Listado con todas las direcciones IP (principal y alias).
Dirección IP pública	Dirección IP del último dispositivo (router / proxy / extremo VPN) que conecta a la red del cliente con Internet.
Direcciones físicas (MAC)	Dirección física de las tarjetas de red instaladas.
Dominio	Dominio Windows al que pertenece el equipo. Vacío si no pertenece a un dominio.

Campo	Descripción
Ruta de directorio activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.
Grupo	Grupo dentro del árbol de grupos al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón **Cambiar**.
Sistema operativo	Sistema operativo instalado en el equipo.
Máquina virtual	Indica si el equipo es físico o esta virtualizado.
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o por el contrario se regenera a su estado original.
Licencias	Licencias de productos de Panda Security instalados en el equipo. Consulta **Licencias** en la página **185** para más información.
Versión del agente	Versión interna del agente Panda instalado en el equipo.
Fecha de arranque del sistema	Fecha en la que se inició el equipo por ultima vez.
Fecha de instalación	Fecha en la que se instaló el sistema operativo del equipo por última vez.
Último proxy utilizado	Método de acceso empleado por Panda Endpoint Protection en su ultima conexión con la nube de Panda Security. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.
Última conexión del agente con la infraestructura Panda Security	Fecha de la última conexión del software de cliente con la nube de Panda Security. Como mínimo el agente de comunicaciones contactará cada 4 horas.
Último chequeo de la configuración	Fecha en la que Panda Endpoint Protection comprobó por última vez la configuración en la nube de Panda Security en busca de cambios.
Shadow Copies	Indica el estado de la funcionalidad;

Campo	Descripción
	• Activado • Desactivado • Código de error
Última copia realizada	Indica la fecha y hora de la última copia realizada.
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.
Control remoto	Indica el estado de la funcionalidad: • **Activado** • **Desactivado** • **Error instalando**: el módulo de control remoto reportó un error en el proceso de instalación. • **Sin licencia**: el software de seguridad no tiene una licencia de Panda Endpoint Protection asignada. • **Sin información**: el agente todavía no ha enviado información del estado del módulo al servidor.

Tabla 8.27: Campos de la sección detalles del equipo

Seguridad

En esta sección se indican el estado (Activado, Desactivado, Error) de las distintas tecnologías de Panda Endpoint Protection que protegen al equipo del malware.

Campo	Descripción
Antivirus de archivos	Protección del sistema de ficheros.
Antirrobo	Acciones para mitigar la exposición de datos ante robos de dispositivos móviles. En el caso de los dispositivos iOS, si no han sido instalados mediante un MDM esta funcionalidad no estará disponible. Consulta **Instalación en sistemas iOS** en la página **149**.

Campo	Descripción
Antivirus de correo	Protección de los protocolos empleados en el envío y recepción de correos electrónicos.
Antivirus para navegación web	Protección frente al malware descargado de páginas web con el navegador instalado en el equipo. En el caso de los dispositivos iOS, si no han sido instalados mediante un MDM esta funcionalidad no estará disponible. Consulta **Instalación en sistemas iOS** en la página **149**.
Firewall	Protección frente a tráfico de red generado por aplicaciones.
Control de dispositivos	Protección frente a la infección mediante dispositivos externos de almacenamiento o que permiten conectar el equipo a Internet sin pasar por la infraestructura de comunicaciones de la organización (módems).
Gestión de parches	Instalación de parches y actualizaciones de sistemas operativos Windows, macOS, Linux y aplicaciones de terceros. Detección del estado del parcheo de los equipos y desinstalación de los parches problemáticos.
Instalación de parches	Indica si se ha bloqueado la instalación de parches en el equipo, o si se trata de un equipo de prueba para la instalación de parches. Para más información, consulta **Funcionalidades de Panda Patch Management**
Fecha de la última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se publicaron nuevos parches.
Versión de la protección	Versión interna del módulo de la protección instalado en el equipo.
Versión de actualización del conocimiento	Fecha de la última descarga del fichero de firmas en el equipo.
Cifrado de discos duros (solo equipos Mac)	Estado del módulo de cifrado: • **No disponible**: el equipo no es compatible con Panda Full Encryption. • **Sin información**: el equipo todavía no ha enviado información del módulo de cifrado.

Campo	Descripción
	• **Activado**: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • **Desactivado**: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • **Error instalando**: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • **Sin licencia**: el equipo no tiene una licencia de Panda Endpoint Protection asignada. **Obtener la clave de recuperación**: muestra una ventana con el identificador de la clave de recuperación asociada al equipo y la propia clave. Consulta **Proceso para obtener la clave de recuperación** en la página **447** para más información. Estado del proceso de cifrado: • **Desconocido**: alguna unidad no tiene un estado conocido. • **Discos no cifrados**: el inicio del proceso de cifrado en el equipo está pendiente de que el usuario introduzca la contraseña con permisos de administrador. • **Discos cifrados**: todas las unidades compatibles con la tecnología de cifrado están cifradas. • **Cifrando**: al menos una unidad del equipo está siendo cifrada. • **Descifrando**: al menos una unidad del equipo está siendo descifrada. • **Cifrado por el usuario**: todos los medios de almacenamiento se encuentran cifrados por el usuario. • **Cifrado por el usuario (parcialmente)**: algunos de los medios de almacenamiento se encuentran cifrados por el usuario.
Método de autenticación (equipos Mac)	• **Contraseña:** el método de autenticación aplicado es la contraseña solicitada en el inicio del equipo.
Conexión con servidores de	Estado de la conexión del equipo con los servidores de Panda Security. En caso de errores se incluyen los enlaces a las páginas de ayuda que

Campo	Descripción
conocimiento	recopilan los requisitos de obligado cumplimiento.

Tabla 8.28: Campos de la sección detalles de la seguridad

Protección de datos (Windows)

En esta sección se indica el estado de los módulos que protegen los datos almacenados en el equipo.

Campo	Descripción
Cifrado de discos duros	Estado del módulo de cifrado: • **No disponible**: el equipo no es compatible con Panda Full Encryption. • **Sin información**: el equipo todavía no ha enviado información del módulo de cifrado. • **Activado**: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • **Desactivado**: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • **Error**: la configuración establecida por el administrador no permite aplicar un método de autenticación soportado por Panda Full Encryption en la versión del sistema operativo instalada en el equipo. • **Error instalando**: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • **Sin licencia**: el equipo no tiene una licencia de Panda Endpoint Protection asignada. **Obtener la clave de recuperación**: muestra una ventana con los identificadores de los medios de almacenamiento cifrados del equipo. Al hacer clic en cualquier de ellos se muestra la clave de recuperación. Consulta **Proceso para obtener la clave de recuperación** en la página **447** para más información.
Estado del proceso	• **Desconocido**: alguna unidad no tiene un estado conocido.

Campo	Descripción
de cifrado:	• **Discos no cifrados**: alguna de las unidades compatibles con la tecnología de cifrado no esta cifrada ni en proceso de cifrado. • **Discos cifrados**: todas las unidades compatibles con la tecnología de cifrado están cifradas. • **Cifrando**: al menos una unidad del equipo está siendo cifrada. • **Descifrando**: al menos una unidad del equipo está siendo descifrada. • **Cifrado por el usuario**: todos los medios de almacenamiento se encuentran cifrados por el usuario. • **Cifrado por el usuario (parcialmente)**: algunos de los medios de almacenamiento se encuentran cifrados por el usuario.
Método de autenticación	• **Desconocido**: método de autenticación no compatible con los soportados por Panda Patch Management. • **Procesador de seguridad (TPM).** • **Procesador de seguridad (TPM) + Contraseña.** • **Contraseña:** método de autenticación por PIN, PIN extendido o passphrase. • **USB** método de autenticación por llave USB. • **Sin cifrar**: ninguna de las unidades compatibles con la tecnología de cifrado está cifrada ni en proceso de cifrado.
Fecha de cifrado	Fecha del proceso de cifrado completado más antigua dentro de la primera vez que se cifró de forma total el equipo.
Cifrado de unidades de almacenamiento extraíbles	Estado del módulo de cifrado: • **No disponible**: el equipo no es compatible con Panda Full Encryption. • **Sin información**: el equipo todavía no ha enviado información del módulo de cifrado. • **Activado**: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • **Desactivado**: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y

Campo	Descripción
	no se han producido errores. • **Error**: la configuración establecida por el administrador no permite aplicar un método de autenticación soportado por Panda Full Encryption en la versión del sistema operativo instalada en el equipo. • **Error instalando**: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • **Sin licencia**: el equipo no tiene una licencia de Panda Endpoint Protection asignada. **Ver dispositivos cifrados de este equipo:** muestra una ventana con los identificadores de los medios de almacenamiento externos cifrados del equipo. Al hacer clic en cualquier de ellos se muestra la clave de recuperación. Consulta **Proceso para obtener la clave de recuperación** en la página **447** para más información.

Tabla 8.29: Campos de la sección Protección de datos

Sección Detecciones (4) en Windows, Linux y macOS

Muestra los contadores asociados a la seguridad y al nivel de parcheo del equipo mediante los siguientes widgets:

Panel de Control	Descripción
Amenazas detectadas por el antivirus	Consulta **Amenazas detectadas por el antivirus** en la página **475**.
Parches disponibles	Consulta **Parches disponibles** en la página **378**.
Evolución de los parches disponibles	Consulta **Evolución de los parches disponibles** en la página **375**.
Programas "End of life"	Consulta **Programas "End of life"** en la página **373**.

Tabla 8.30: Listado de widgets disponibles en la sección Detecciones

Sección Detecciones (4) en Android e iOS

Muestra los contadores asociados a la seguridad del dispositivo mediante los siguientes widgets:

Panel de Control	Descripción
Amenazas detectadas por el antivirus	Consulta Amenazas detectadas por el antivirus en la página 475.

Tabla 8.31: Listado de widgets disponibles en la sección Detecciones

Sección Hardware (5)

Contiene información sobre los recursos hardware instalados en el equipo:

Campo	Descripción	Valores
CPU	Información del microprocesador instalado en el equipo y serie temporal con el consumo de CPU en diferentes periodos e intervalos según la selección del desplegable.	• Intervalos de 5 minutos para la última hora. • Intervalos de 10 minutos para las 3 últimas horas. • Intervalos de 40 minutos para las últimas 24 horas.
Memoria	Información sobre las características de los chips de memoria instalados y serie temporal con el consumo de memoria en diferentes períodos e intervalos según la selección del desplegable.	• Intervalos de 5 minutos para la última hora. • Intervalos de 10 minutos para las 3 últimas horas. • Intervalos de 40 minutos para las últimas 24 horas.
Disco	Información sobre las características del sistema de almacenamiento masivo y un gráfico de tarta con el porcentaje de espacio libre y ocupado en el momento de la consulta.	• ID de dispositivo • Tamaño • Tipo • Particiones

Campo	Descripción	Valores
		• Revisión de firmware • Número de serie • Nombre
BIOS	Información sobre la versión de la BIOS instalada en el equipo.	• Versión • Fecha de fabricación • Número de serie • Nombre • Fabricante
TPM	Información del chip de seguridad integrado en la placa base del equipo. Para poder ser utilizado por Panda Endpoint Protection el TPM debe de estar activado, habilitado y ser propietario.	• **Versión del fabricante**: versión interna del chip. • **Versión de especificación**: versiones de las APIs compatibles. • Versión • Fabricante • **Activado**: el TPM está preparado para recibir comandos. Se utiliza en sistemas con varios TPMs. • **Habilitado**: el TPM esta preparado para funcionar ya que ha sido activado desde la BIOS. • **Propietario**: el sistema operativo puede interactuar con el TPM.

Tabla 8.32: Campos de la sección hardware de la información del equipo

Sección Software (6)

Contiene información del software instalado en el equipo, de las actualizaciones del sistema operativo Windows y un histórico de sus movimientos.

Herramienta de búsqueda

Introduce el nombre o editor en la caja de texto **Buscar** y presiona la tecla Enter para efectuar una búsqueda. A continuación se muestra la información del software encontrado:

Campo	Descripción
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha de instalación	Fecha en la que se instaló el programa por última vez. En los dispositivos iOS integrados en MDM, indica la fecha en la que la app instalada fue localizada por primera vez en el dispositivo. Consulta **Despliegue e instalación del agente iOS** en la página **153**. Esta información no está disponible para los dispositivos iOS que no están integrados en MDM. Los dispositivos integrados en el MDM de Panda envían al servidor un informe diario de las apps de terceros que tienen instaladas.
Tamaño	Tamaño del programa instalado.
Versión	Versión interna del programa instalado.

Tabla 8.33: Campos de la sección software de la información del equipo

- Para limitar la búsqueda selecciona en el desplegable el tipo de software que se mostrará:
  - Solo programas
  - Solo actualizaciones
  - Todo el software

Instalaciones y desinstalaciones

- Haz clic en el link **Instalaciones y desinstalaciones** para mostrar un histórico de los cambios efectuados en el equipo:

Campo	Descripción
Evento	• Software desinstalado en el equipo. • Software instalado en el equipo.
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha	Fecha en la que se instaló o desinstaló el programa.
Versión	Versión interna del programa instalado.

Tabla 8.34: Campos de la sección Instalaciones y desinstalaciones

Sección Configuración (7)

Muestra toda la información relevante de la asignación de configuraciones al equipo, y permite su gestión y modificación:

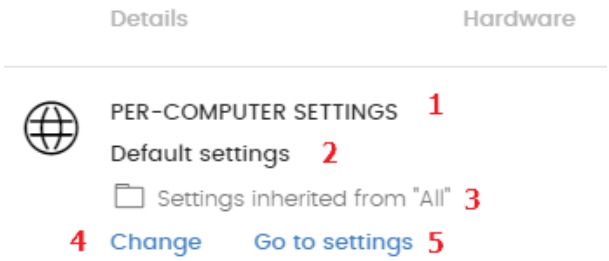


Figura 8.9: Ejemplo de asignación heredada y manual

- **(1) Nombre de la categoría de la configuración**: indica el tipo de configuración. Consulta Introducción a las clases de configuraciones en la página 282para conocer los distintos tipos de configuraciones disponibles en Panda Endpoint Protection.
- **(2) Nombre de la configuración asignada**.
- **(3) Método de asignación de la configuración**: directamente al equipo o heredada de un grupo superior.
- **(4) Botón para cambiar la asignación de la configuración**.
- **(5) Botón para editar el contenido de la configuración**.

*Consulta **Crear y gestionar configuraciones** en la página **285** para crear, editar y modificar perfiles de configuración.*

Barra de acciones (8)

Recurso que agrupa múltiples operaciones disponibles para aplicar sobre los equipo administrados:

Acción	Descripción
Mover a	Mueve el equipo a un grupo estándar.
Mover a su ruta de Active Directory	Mueve el equipo a su grupo Directorio Activo original.
Eliminar	Libera la licencia de Panda Endpoint Protection y elimina el equipo de la consola Web.
Analizar ahora	Programa una tarea de análisis de ejecución inmediata. Consulta **Análisis y desinfección bajo demanda de equipos** en la página **591** para más información.
Programar análisis	Programa una tarea de análisis. Consulta **Análisis y desinfección bajo demanda de equipos** en la página **591** para más información.
Programar instalación de parches	Crea una tarea que instalará los parches publicados y no aplicados en el equipo. Consulta **Descargar e instalar parches** en la página **352**para más información.
Reiniciar	Reinicia el equipo de forma inmediata. Consulta **Reiniciar equipos** en la página **599** para más información.
Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Consulta **Reinstalación remota** en la página **182** para obtener más información.
Notificar un problema	Abre un ticket de mantenimiento con el departamento técnico de Panda Security. Consulta **Notificar un problema** en la página **600** para

Acción	Descripción
	más información.

Tabla 8.35: Acciones disponibles en la ventana de información del equipo

Iconos ocultos (9)

Dependiendo del tamaño de la ventana y del número de iconos a mostrar, parte de ellos pueden quedar ocultos bajo el icono ... Haz clic para desplegar el menú con los iconos restantes.

Capítulo 9

Gestión de configuraciones

Las configuraciones, también llamadas "perfiles de configuración" o simplemente "perfiles", ofrecen a los administradores un modo rápido de establecer los parámetros de seguridad y conectividad gestionados por Panda Endpoint Protection en los equipos que administran.

Contenido del capítulo

Estrategias para crear la estructura de configuraciones

El administrador de la red creará tantos perfiles como variaciones de configuraciones sean necesarias para gestionar la seguridad de la red. Se genera una nueva configuración por cada grupo de equipos con necesidades de protección similares:

- Equipos de usuario utilizados por personas con distintos niveles de conocimientos en informática requieren configuraciones más o menos estrictas frente a la ejecución de software, acceso a Internet o a dispositivos externos.
- Usuarios que desempeñan diferentes tareas tienen diferentes usos y necesidades, y por tanto requerirán de configuraciones que permitan el acceso a diferentes recursos.
- Usuarios que manejan información confidencial o delicada para la empresa requieren un nivel de protección superior frente a amenazas e intentos de robo de la propiedad intelectual de la compañía.
- Equipos en distintas delegaciones requieren configuraciones distintas que les permitan conectarse a Internet utilizando diferentes infraestructuras de comunicaciones.
- Servidores críticos para el funcionamiento de la empresa requieren configuraciones de seguridad específicas.

Visión general para asignar configuraciones a equipos

La asignación de configuraciones a los equipos de la red es un proceso de cuatro pasos:

1. Crear los grupos que reúnan equipos del mismo tipo o con idénticos requisitos de conectividad y seguridad.
2. Asignar los equipos de la red a su grupo correspondiente.
3. Asignar los distintos tipos de configuraciones a los grupos creados.
4. Difundir las configuraciones a todos los equipos de la red.

Todas estas operaciones se realizan desde el árbol de grupos, accesible desde el menú superior **Equipos**. El árbol de grupos es la herramienta principal para asignar configuraciones de forma rápida y sobre conjuntos amplios de equipos.

Por lo tanto, la estrategia principal del administrador consiste en reunir todos los equipos similares en un mismo grupo y crear tantos grupos como conjuntos diferentes de equipos existan en la red que gestiona.

*Para obtener más información sobre el manejo del árbol de grupos y asignación de equipos a grupos consulta **El panel Árbol de equipos** en la página **211**.*

Difusión inmediata de la configuración

Una vez que una configuración es asignada a un grupo, esa configuración se aplicará a los equipos del grupo de forma inmediata y automática, siguiendo las reglas de la herencia mostradas en **Asignación indirecta de configuraciones: las dos reglas de la herencia**. La configuración así establecida se aplica a los equipos sin retardos, en cuestión de unos pocos segundos.

*Para desactivar la difusión inmediata de la configuración consulta **Configuración de la comunicación en tiempo real** en la página **309**.*

Árbol multinivel

En empresas de tamaño mediano y grande, la variedad de configuraciones puede ser muy alta. Para facilitar la gestión de parques informáticos grandes, Panda Endpoint Protection permite generar árboles de grupos de varios niveles para que el administrador pueda gestionar los equipos de la red con la suficiente flexibilidad.

Herencia

En redes de tamaño amplio es muy probable que el administrador quiera reutilizar configuraciones ya establecidas en grupos de orden superior dentro del árbol de grupos. El mecanismo de herencia permite asignar una configuración sobre un grupo y, de forma automática, sobre todos los grupos que dependen de éste, ahorrando tiempo de gestión.

Configuraciones manuales

Para evitar la propagación de configuraciones en todos los niveles inferiores de una rama del árbol, o asignar una configuración distinta a la recibida mediante la herencia sobre un determinado equipo dentro de una rama, es posible asignar de forma manual configuraciones a equipos individuales o a grupos.

Configuración por defecto

Inicialmente todos los equipos en el árbol de grupos heredan la configuración establecida en el nodo raíz **Todos**. Este nodo tiene asignadas las configuraciones por defecto creadas en Panda Endpoint Protection para proteger a los equipos desde el primer momento, incluso antes de que el administrador haya accedido a la consola para establecer una configuración de seguridad.

Introducción a las clases de configuraciones

Panda Endpoint Protection distribuye la configuración a aplicar en los equipos administrados a lo largo de varias clases de perfiles, cada una de las cuales cubre un área concreta de la seguridad.

A continuación se muestra una introducción a cada una de las clases soportadas en Panda Endpoint Protection:

Panda Endpoint Protection permite configurar los siguientes aspectos del servicio:

Configuración	Descripción
Usuarios	Gestiona las cuentas que podrán acceder a la consola de administración, así como las acciones permitidas dentro de ella (roles) y su actividad. Para más información, consulta **Acceso, control y supervisión de la consola de administración** en la página **53**.
Ajustes por equipo	Define las plantillas de configuración donde se indica cada cuánto se actualizará el software de seguridad Panda Endpoint Protection instalado en los equipos de usuario y servidores. También establece la configuración global frente a manipulaciones externas y desinstalaciones no autorizadas. Para más información, consulta **Configuración remota del agente** en la página **299**.
Configuración de red	Define plantillas de configuración que establecen el idioma del software Panda Endpoint Protection instalado en los equipos de usuario y servidores, y el tipo de conexión que se utilizará para conectar con la nube de Panda Security. Para más información, consulta **Configuración remota del agente** en la página **299**.
Servicios de red	Define el comportamiento del software Panda Endpoint Protection en lo referente a la comunicación con los equipos vecinos de la red del cliente: • **Proxy**: define de forma global los equipos que realizarán tareas de proxy para facilitar el acceso a la nube de equipos con Panda Endpoint Protection instalado y asilados de la red. Para más información, consulta **Rol de Proxy Panda** en la página **300**. • **Caché**: define de forma global los repositorios de ficheros de firmas, parches de seguridad y componentes utilizados para actualizar el software Panda Endpoint Protection instalado en los equipos de la red. Para más información, consulta **Rol de caché** en la página **302**. • **Descubrimiento**: define de forma global los equipos de la red

Configuración	Descripción
	encargados de rastrear la aparición de dispositivos sin proteger. Para más información, consulta **Rol de descubridor** en la página **304**.
Entornos DVI	Define el número de equipos alojados en infraestructuras de virtualización no persistentes para facilitar la asignación de licencias.
Mis Alertas	Establece el tipo de alertas que el administrador recibirá en su buzón de correo. Para más información, consulta **Alertas** en la página **569**.
Estaciones y servidores	Define plantillas de configuración que establecen el comportamiento de Panda Endpoint Protection para proteger a los equipos de la red frente a las amenazas y el malware. Para más información, consulta **Configuración de la seguridad en estaciones y servidores** en la página **319**.
Dispositivos moviles	Define plantillas de configuración que establecen el comportamiento de Panda Endpoint Protection para proteger a los tablets y teléfonos móviles frente a las amenazas y el malware y al robo de estos dispositivos. Para más información, consulta **Configuración de seguridad para dispositivos móviles** en la página **339**
Gestión de parches	Define las plantillas de configuración que establecen el comportamiento del descubrimiento de nuevos parches de seguridad publicados por los proveedores de software y del sistema operativo Windows. Para más información, consulta **Panda Patch Management (Actualización de programas vulnerables)** en la página **345**.
Cifrado	Define las plantillas de configuración que permiten cifrar el contenido de los dispositivos de almacenamiento interno. Para más información, consulta **Panda Full Encryption(Cifrado de dispositivos)** en la página **433**.

Tabla 9.1: Descripción de las configuraciones disponibles en Panda Endpoint Protection

Perfiles de configuración modulares vs monolíticos

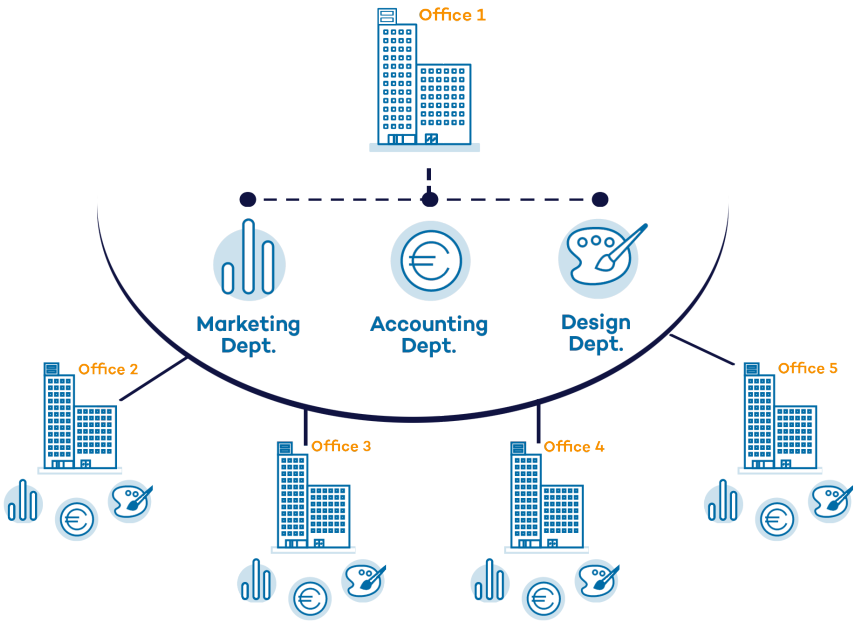
Con el soporte de las distintas clases de perfiles, Panda Endpoint Protection adopta un enfoque modular para crear y distribuir las configuraciones a aplicar en los equipos administrados. El objetivo de utilizar perfiles modulares y no un único perfil de configuración monolítico que abarque toda la configuración es el de reducir el número de perfiles distintos que el administrador tendría

que manejar en la consola y así minimizar el tiempo de gestión. El enfoque modular permite generar configuraciones más pequeñas y ligeras, frente a perfiles monolíticos que fomentan la aparición de muchos perfiles de configuración muy largos y redundantes, con muy pocas diferencias entre sí.

Caso práctico: Creación de configuraciones para varias delegaciones

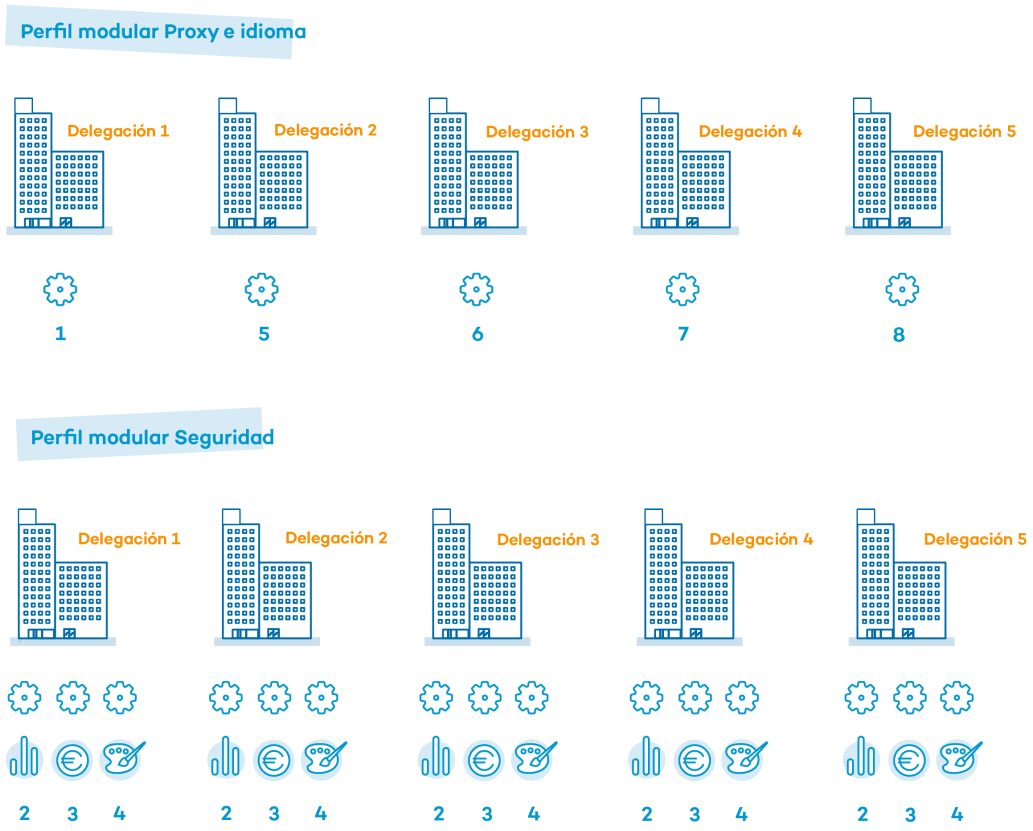
En este caso práctico tenemos una empresa con 5 delegaciones, cada una de ellas tiene una infraestructura de comunicaciones distinta y por tanto una configuración de proxy diferente. Además, dentro de cada delegación se requieren 3 configuraciones de seguridad diferentes, una para el departamento de diseño, otro para el departamento de contabilidad y otra para el departamento de marketing.

Network of a company formed by several offices:



Con un perfil monolítico son necesarios 15 perfiles de configuración distintos (5 oficinas x 3 clases de configuración en cada oficina = 15) para dar servicio a todos los departamentos de todas las delegaciones de la empresa.

Como Panda Endpoint Protection separa la configuración de proxy de la de seguridad, el número de perfiles a crear se reduce (5 perfiles de proxy + 3 perfiles de departamento = 8) ya que los perfiles de seguridad por departamento de una delegación se pueden reutilizar y combinar con los perfiles de proxy en otras delegaciones.



Crear y gestionar configuraciones

Haz clic en el menú superior Configuración para crear, copiar y borrar configuraciones. En el panel de la izquierda se encuentran las entradas correspondientes a las clases de configuraciones

posibles (1). En el panel de la derecha se muestran los perfiles de configuración ya creados (2) de la clase seleccionada y los botones para añadir (3), copiar (4) y eliminar perfiles (5). Utiliza la barra de búsqueda (6) para localizar los perfiles ya creados de forma rápida.

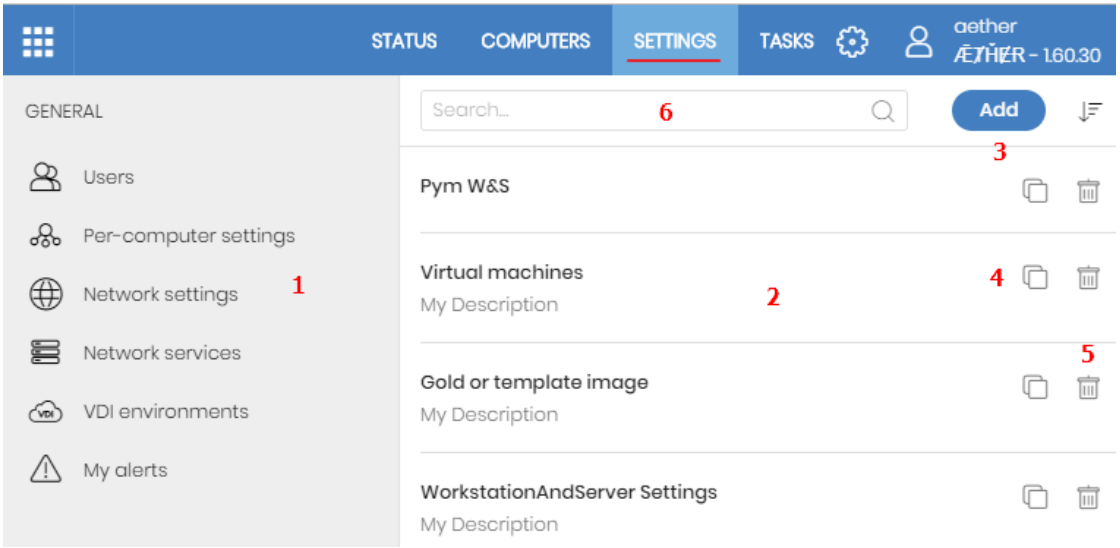


Figura 9.1: Pantalla para crear y gestionar configuraciones

Las configuraciones creadas desde Panda Partner Center, se muestran con la etiqueta en verde Panda Partner Center. Al posicionarse sobre ella se muestra el mensaje: "Esta configuración está gestionada desde Panda Partner Center". Las configuraciones creadas desde Panda Partner Center son de sólo lectura, y únicamente permiten cambiar los destinatarios. Para más información, consulta la sección Configuraciones para productos basados en Panda, en el manual de ***Panda Partner Center****.*

Crear configuraciones

Haz clic sobre el botón **Añadir** para mostrar la ventana de creación de configuraciones. Todos los perfiles tienen un nombre principal y una descripción que se muestran en los listados de configuraciones.

Ordenar configuraciones

Haz clic en el icono **(7)** para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Copiar, borrar y editar configuraciones

- Para copiar y borrar un perfil de configuración utiliza los iconos **(4)** y **(5)**. Si el perfil ha sido asignado a uno o más equipos se impedirá su borrado hasta que sea liberado.
- Haz clic en el perfil de configuración para editarlo.

Antes de modificar un perfil comprueba que la nueva configuración sea correcta ya que, si el perfil ya está asignado a equipos de la red, esta nueva configuración se propagará y aplicará de forma automática y sin retardos.

Asignación manual y automática de configuraciones

Una vez creados los perfiles de configuración, éstos pueden ser asignados a los equipos de la red siguiendo dos estrategias diferentes:

- Mediante asignación manual (asignación directa).
- Mediante asignación automática a través de la herencia (asignación indirecta).

Ambas estrategias son complementarias y es muy recomendable que el administrador comprenda las ventajas y limitaciones de cada mecanismo para poder definir una estructura de equipos lo más simple y flexible posible, con el objetivo de minimizar las tareas de mantenimiento diarias.

Asignación directa / manual de configuraciones

Consiste en establecer de forma directa los perfiles de configuración a equipos o grupos. De esta manera es el administrador el que, de forma manual, asigna una configuración a un grupo o equipo.

Una vez creados los perfiles de configuración, estos se asignan de tres maneras posibles:

- Desde el menú superior **Equipos**, en el árbol de grupos mostrado en el panel de la izquierda.
- Desde el detalle del equipo en el panel de listado de equipos, accesible desde el menú superior **Equipos**.
- Desde el propio perfil de configuración creado o editado.

Para obtener más información sobre el árbol de grupos consulta ***Árbol de grupos*** *en la página* ***220***

Desde el árbol de grupos

Para asignar un perfil de configuración a un conjunto de equipos que pertenecen a un grupo:

- Haz clic en el menú superior **Equipos** y selecciona el árbol de grupos en el panel izquierdo.
- Haz clic en el menú contextual en la rama apropiada del árbol de grupos.
- Haz clic en el menú emergente **Configuraciones**, se mostrará una ventana con el nombre de los perfiles ya asignados al grupo seleccionado, separados por su clase, y el tipo de asignación:
- **Manual / Asignación directa**: mediante la leyenda **Asignada directamente a este grupo**.
- **Heredada / Asignación indirecta**: mediante la leyenda **Configuración heredada de** y el nombre del grupo del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.

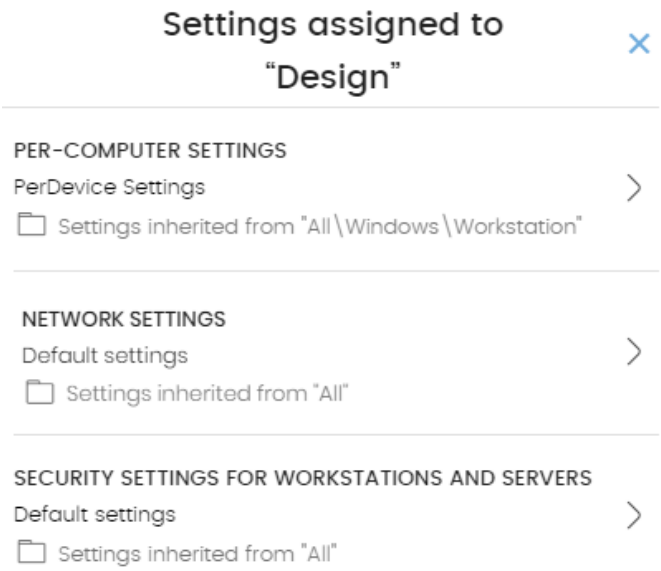


Figura 9.2: Ejemplo de asignación heredada y manual

Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al grupo. La configuración se propagará de forma inmediata a todos los equipos miembros del grupo y sus descendientes.

Desde el panel listado de equipos

Para asignar un perfil de configuración a un equipo concreto:

- En el menú superior **Equipos** haz clic en el grupo o filtro donde reside el equipo a asignar la configuración. Haz clic sobre el equipo en la lista de equipos mostrada en el panel derecho para ver la pantalla detalles de equipo.
- Haz clic en la pestaña **Configuración**. Se mostrarán los perfiles asignados al equipo separados por su clase, y el tipo de asignación:
    - **Manual / Asignación directa**: mediante la leyenda **Asignada directamente a este grupo**.
    - **Heredada / Asignación indirecta**: mediante la leyenda **Configuración heredada de** y el nombre del grupo del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.
- Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al equipo. La configuración se aplicará de forma inmediata.

Desde el propio perfil de configuración

La forma más rápida de asignar una configuración a varios equipos que pertenecen a grupos distintos es a través del propio perfil de configuración.

Para asignar equipos o grupos de equipos a un perfil de configuración:

- En el menú superior **Configuración**, panel lateral, haz clic en la clase de perfil que quieres asignar.
- Selecciona la configuración a asignar y haz clic en el botón **Destinatarios**. Se mostrará una ventana dividida en dos secciones: **Grupos de equipos y Equipos adicionales**.
- Haz clic en los botones para añadir equipos individuales o grupos de equipos al perfil de configuración.
- Haz clic en el botón **Atrás**. El perfil quedará asignado a los equipos seleccionados y la nueva configuración se aplicará de forma inmediata.

Al retirar un equipo de la lista de equipos asignados a una configuración, el equipo volverá a heredar las configuraciones asignadas al grupo al que pertenece. La consola de administración resaltará este hecho mostrando una ventana de advertencia antes de aplicar los cambios.

Asignación indirecta de configuraciones: las dos reglas de la herencia

La asignación indirecta de configuraciones se realiza a través del mecanismo de la herencia. Esta funcionalidad permite propagar de forma automática un mismo perfil de configuración a todos los

equipos subordinados del nodo sobre el cual se asignó la configuración.

Las reglas que rigen la interacción entre los dos tipos de asignaciones (manuales / directas y automática / herencia) se muestran por orden de prioridad:

Regla de la herencia automática

Un grupo o equipo hereda de forma automática las configuraciones del grupo del cual depende (grupo padre o de orden superior).

La asignación de configuración es manual sobre el grupo padre y todos sus descendientes (equipos y otros grupos con equipos en su interior) reciben la configuración de forma automática.

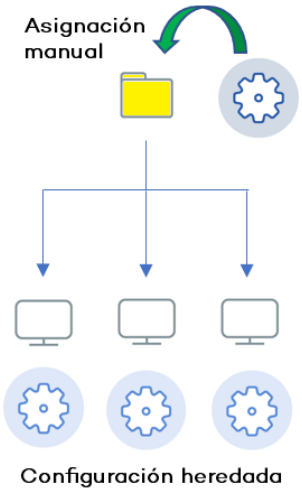


Figura 9.3: Herencia / asignación indirecta

Regla de la prioridad manual

Una configuración manual prevalece sobre una configuración heredada.

Los equipos reciben las configuraciones heredadas por defecto pero si se establece una configuración manual sobre un grupo o equipo, todos sus descendientes recibirán la configuración manual, y no la configuración heredada de orden superior.

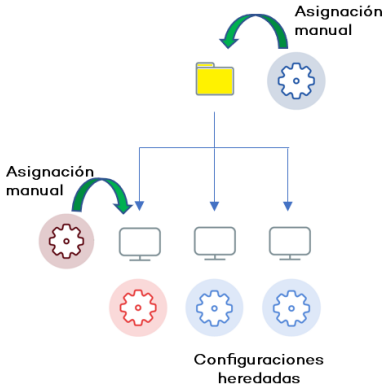


Figura 9.4: Prevalencia de configuración manual sobre heredada

Límites de la herencia

La configuración asignada a un grupo (manual o heredada) se propaga a todos los elementos de la rama del árbol hasta que se encuentra una asignación manual.

Este nodo y todos sus descendientes reciben la configuración manual asignada, y no la establecida en el nodo de orden superior.

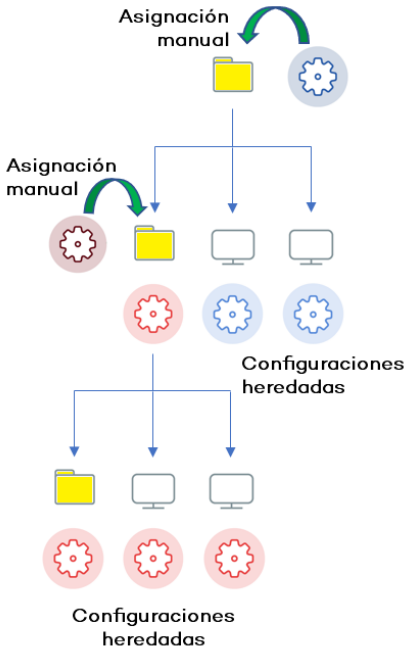


Figura 9.5: Limite de la herencia

Sobre-escritura de configuraciones

La regla de la prioridad manual indica que las configuraciones manuales prevalecen sobre las configuraciones heredadas en un escenario típico donde primero se establece la configuración sobre el nodo de orden superior para que todos sus descendientes la hereden, y posteriormente se asignan de forma manual aquellas configuraciones especiales sobre ciertos nodos de orden inferior.

Sin embargo, es frecuente que una vez establecidas las configuraciones heredadas y manuales, haya un cambio de configuración en un nodo de orden superior. Se distinguen dos casos:

- **No hay configuraciones manuales en los nodos descendientes**: el nodo padre recibe una nueva configuración que se propaga a todos sus nodos descendientes.
- **Sí hay configuraciones manuales en algún nodo descendiente**: el nodo padre recibe una configuración que intenta propagar a todos los nodos descendientes, pero el sistema de herencia no permite asignar una configuración de forma automática sobre un nodo que recibió anteriormente una configuración manual.

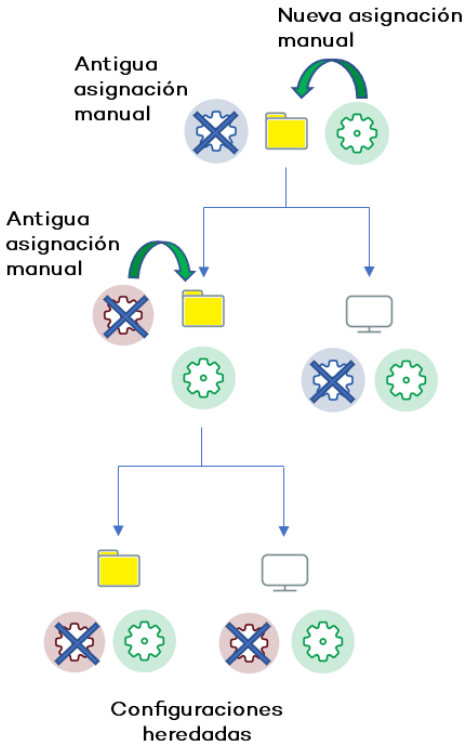


Figura 9.6: Sobre escritura de configuraciones manuales

De esta manera, cuando el sistema detecta un cambio de configuración que tenga que propagar a los nodos subordinados, y alguno de estos tenga una configuración manual (sin importar el nivel en el que se encuentre) se presentará la pantalla de selección, preguntando al administrador sobre el comportamiento a seguir: **Hacer que todos hereden esta configuración** o **Mantener todas las configuraciones**.

Hacer que todos hereden esta configuración

¡Utiliza esta opción con mucho cuidado, esta acción no tiene vuelta atrás! Todas las configuraciones manuales que dependan del nodo padre se perderán y se aplicará la configuración heredada de forma inmediata en los equipos. El comportamiento de Panda Endpoint Protection podrá cambiar en muchos equipos de la red

La nueva asignación directa se propaga mediante la herencia a todo el árbol por completo, sobrescribiendo la asignación directa anterior y llegando hasta los nodos hijos de último nivel.

Mantener todas las configuraciones

La nueva configuración solo se propaga a aquellos nodos subordinados que no tengan configuraciones manuales establecidas.

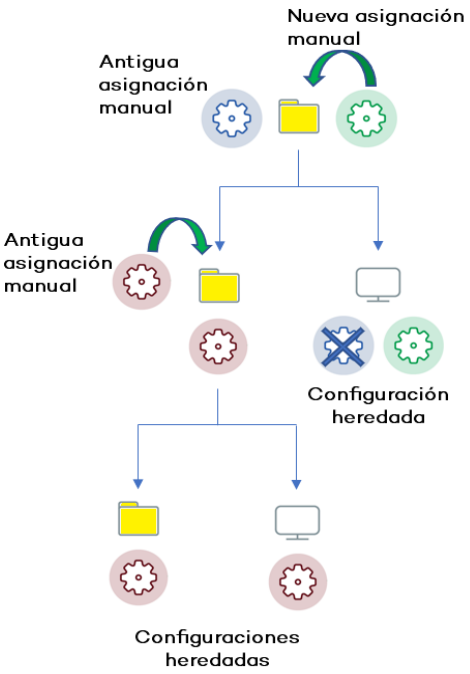


Figura 9.7: Mantener las configuraciones manuales

Si eliges la opción de mantener las configuraciones establecidas de forma manual, la propagación de la nueva configuración heredada se detiene en el primer nodo configurado manualmente.

Eliminar asignaciones manuales y restaurar la herencia

Para eliminar una asignación manual aplicada sobre una carpeta y volver a heredar la configuración de la rama padre:

- En el menú superior **Equipos** haz clic en el grupo que tiene la asignación manual a eliminar, dentro del árbol de grupos situados en el panel izquierdo.
- Haz clic en el icono del menú contextual de la rama apropiada. Se mostrará una ventana emergente con las configuraciones asignadas. Elige el perfil que esté asignado de forma manual y quieres eliminar.
- Se desplegará un listado con todos los perfiles disponibles para realizar una nueva asignación manual, y al final de la lista se mostrará el botón **Heredar del grupo padre** junto con información de la configuración que se heredaría, y el grupo del cual se heredará.

Movimiento de grupos y equipos

Al mover un equipo o grupo de equipos a otra rama del árbol con una configuración aplicada, el comportamiento de Panda Endpoint Protection con respecto a las configuraciones que tomará el equipo o grupo movido varia en función de si se trata de grupos completos o equipos individuales.

Movimiento de equipos individuales

Se respetan las configuraciones manuales establecidas sobre los equipos movidos, y se sobrescriben de forma automática las configuraciones heredadas con las configuraciones establecidas en el nuevo grupo padre.

Movimiento de grupos

Se muestra una ventana con la pregunta **¿Quieres que las configuraciones asignadas a este grupo mediante herencia, sean sustituidas por las del nuevo grupo padre?**

- En el caso de contestar **SI**, el procedimiento será el mismo que en el movimiento de equipos: las configuraciones manuales se respetan y las heredadas se sobrescriben con las configuraciones establecidas en el grupo padre.
- En el caso de contestar **NO** , las configuraciones manuales se respetan pero las configuraciones heredadas originales del grupo movido prevalece, pasando de esta forma a ser configuraciones manuales.

Excepciones a la herencia indirecta

A los equipos que se integran en la consola Web dentro de un grupo de tipo nativo, Panda Endpoint Protection les asigna la configuración de red del grupo de destino mediante el mecanismo estándar de asignación indirecta / herencia. Sin embargo, si un equipo se integra en la consola Web dentro de un grupo de tipo IP o de tipo directorio activo, la asignación de la configuración de red se produce de forma manual. Este cambio en la forma de asignar la configuración de red repercute a su vez en un cambio de comportamiento al mover posteriormente ese equipo de un grupo a otro: ya no heredará de forma indirecta la configuración de red asignada al grupo de destino, sino que conservará la suya propia.

Este comportamiento particular de la herencia, se debe a que en empresas de tamaño medio y grande, el departamento que administra la seguridad puede no ser el mismo que el que administra el directorio activo de la empresa. Por esta razón, un cambio de grupo efectuado por el departamento técnico que mantiene el directorio activo puede desembocar de forma inadvertida en un cambio de configuración de red dentro de la consola de Panda Endpoint Protection. Esta situación podría dejar sin conectividad al agente de protección instalado en el equipo y, por lo tanto, en una menor protección. Al asignar de forma manual la configuración de red, se impiden cambios de configuración cuando el equipo cambia de grupo en la consola de Panda Endpoint Protection, debido a un cambio de grupo del directorio activo de la empresa.

Configuraciones recibidas desde el partner

Los partners son empresas u organizaciones que tienen como objetivo aprovisionar y gestionar de forma remota las soluciones de seguridad en sus clientes.

Pueden ser de dos tipos:

- Distribuidores que asignan productos a sus clientes y los gestionan de forma remota.
- Compañías que delegan la gestión del servicio de seguridad en cada departamento, pero que además quieren controlar de forma centralizada el cumplimiento de las directrices de protección comunes a toda la empresa.

Para gestionar el software de seguridad de forma remota, los partners envían configuraciones a sus clientes. Estas configuraciones se muestran en la consola de administración con la etiqueta Panda Partner Center .

Características de las configuraciones enviadas por el partner

Las configuraciones enviadas por los partners no son modificables ni se pueden borrar desde la consola de administración. Si el partner autoriza su edición, el administrador podrá modificar ciertos aspectos de la configuración. Para obtener más información consulta **Exclusiones establecidas por el partner** en la página **323** y **Software autorizado establecido por el partner**.

Requisitos

Para recibir las configuraciones enviadas por el partner sigue los pasos mostrados a continuación.

- En el menú superior **Configuración (1)**, selecciona **Usuarios (2)** en el panel lateral izquierdo.
- En la pestaña superior **Usuarios**, activa la opción **Permitir a mi distribuidor acceder a mi consola (3)**.

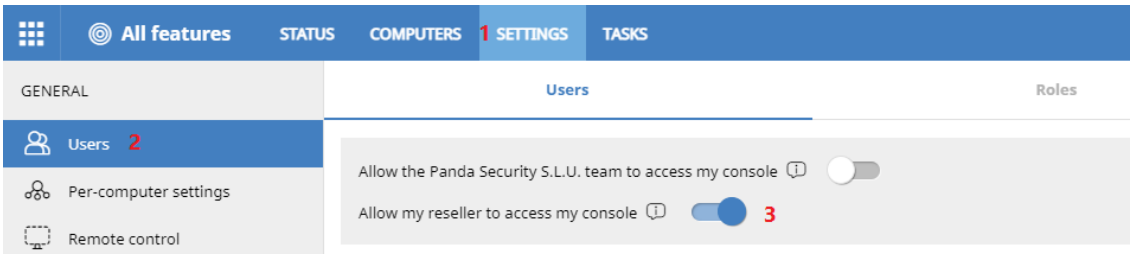


Figura 9.8: Opción Permitir a mi distribuidor acceder a mi consola

Visualizar las configuraciones asignadas

La consola de administración implementa hasta cuatro formas de mostrar los perfiles de configuración asignados a un grupo o equipo:

- En el árbol de grupos.
- En la pantalla de definición de la configuración.
- En la pestaña **Configuración** del equipo.
- En el listado de equipos exportado.

Mostrar las configuraciones en el árbol de grupos

- Haz clic en el menú superior **Equipos** y en la pestaña situada en la parte superior del panel lateral para mostrar el árbol de grupos.
- Selecciona el menú de contexto de la rama elegida y haz clic en el menú emergente **Configuraciones** para mostrar una ventana con las configuraciones asignadas a la carpeta.

A continuación, se indica la información mostrada en cada entrada:

- **Tipo de configuración**: indica la clase a la que pertenece la configuración mostrada.
- **Nombre de la configuración**: nombre asignado por el administrador en la creación de la configuración.
- **Tipo de herencia aplicada**:
  - **Configuración heredada de…:** la configuración fue asignada a la carpeta padre indicada, y los equipos que pertenecen a la rama actual la heredan.
  - **Asignada directamente a este grupo**: → la configuración de los equipos es la que el administrador asignó de forma manual a la carpeta.

Mostrar las configuraciones en la definición de la configuración

Haz clic en el menú superior **Configuraciones** y selecciona el tipo de configuración en el menú lateral.

Selecciona una configuración en el listado de configuraciones.

Si la configuración esta asignada a uno o más equipos o grupos, se mostrará el botón **Ver equipos**.

Haz clic en el botón **Ver equipos**. Se mostrará la zona **Equipos** con un único listado formado por todos los equipos que tienen la configuración asignada, tanto si se asignó de forma individual o mediante grupos de equipos. En la parte superior de la ventana se mostrará el criterio de filtrado establecido.

Mostrar las configuraciones en la pestaña configuración del equipo

En el menú superior **Equipos**, selecciona un equipo del panel de la derecha para mostrar la ventana de detalle. En la pestaña **Configuración** se listan los perfiles asignados al equipo.

Mostrar las configuraciones en el listado de equipos exportado

Desde el árbol de equipos (árbol de grupos o árbol de filtros) haz clic en el menú contextual y elige la opción **Exportar**.

*Consulta **Campos mostrados en el fichero exportado** en la página **230**para más información.*

Capítulo 10

Configuración remota del agente

El administrador puede cambiar desde la consola web el funcionamiento de varios aspectos del agente Panda instalado en los equipos de la red:

- El papel o rol que el equipo representa para el resto de puestos y servidores protegidos.
- Las protecciones frente al tampering o manipulación indebida del software cliente Panda Endpoint Protection por parte de amenazas avanzadas y APTs.
- La visibilidad del agente en el equipo de usuario o servidor y su idioma.
- La configuración de las comunicaciones de los equipos con la nube de Panda Security.
- La aplicación de una capa extra de seguridad en las conexiones VPN entre los equipos y las redes corporativas.

Contenido del capítulo

Configuración de los roles del agente Panda

El agente Panda instalado en los equipos Windows de la red puede adoptar tres roles diferentes:

- Proxy
- Descubridor
- Caché

Para asignar un rol a un equipo con el agente Panda ya instalado haz clic en el menú superior **Configuración** y en el panel lateral **Servicios de red**. Se mostrarán cuatro pestañas: Proxy de Panda Endpoint Protection, **Caché**, **Descubrimiento** y **Control de acceso a redes**.

Solo los equipos con sistema operativo Windows instalado pueden adquirir el rol de Proxy, Descubridor o Caché.

Rol de Proxy Panda

Para acceder a la nube de Panda, el software de seguridad instalado en los equipos requiere de acceso a Internet. En los casos de equipos aislados, se permite el acceso a través del proxy corporativo de la organización. Si no existe este recurso, Panda Endpoint Protection permite designar a uno o a varios equipos con el rol de proxy Panda.

Los equipos con el rol de proxy Panda asignado escuchan peticiones de los equipos y las redirigen a la nube de Panda por una conexión válida.

Solo se recomienda utilizar equipos con el rol de proxy Panda asignado en los casos de equipos aislados que además no tengan acceso a ningún proxy corporativo.

Un equipo con el rol de proxy Panda asignado puede dar servicio a un número de dispositivos muy variable, que depende de los recursos hardware instalados. Como norma general, se establece que un equipo puede dar servicio como máximo a 100 equipos.

Limitaciones de los equipos con el rol de Proxy Panda asignado

Por motivos de seguridad, cuando Panda Endpoint Protection tiene asignado el rol de Proxy Panda, únicamente puede establecer conexiones con la nube de Panda. Por esta razón, existen varias limitaciones al tipo de descargas que el software de seguridad puede realizar si tiene configurado el acceso a Internet a través de un nodo Proxy Panda:

- **Windows y macOS**:
  - El software de seguridad no puede descargar parches de Panda Patch Management pero sí puede reportar los parches pendientes de instalación. Consulta **Descargar e instalar parches** en la página **352**.
- **Linux**:
  - El software de seguridad no puede descargar parches de Panda Patch Management pero sí puede reportar los parches pendientes de instalación. Consulta **Descargar e instalar parches** en la página **352**.
  - El software de seguridad no puede descargar la protección para instalarla o actualizarla. Consulta **Actualización del motor de protección** en la página **202**.

Estas limitaciones no aplican al proxy corporativo de la empresa.

Requisitos para asignar el rol de proxy Panda a un equipo

- Panda Endpoint Protection instalado en un equipo con sistema operativo Windows.
- Soporte para el formato de ficheros 8+3. Consulta el artículo de la MSDN **https://docs.microsoft.com/en- us/previous- versions/windows/it- pro/windows- server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN** para habilitar esta funcionalidad.
- Puerto TCP 3128 sin usar por otras aplicaciones.
- Configuración del cortafuegos del equipo que permita el tráfico entrante y saliente por el puerto 3128.
- Resolver el nombre del equipo con el rol de proxy asignado desde el equipo que lo utiliza.

Asignar el rol de proxy Panda a un equipo

- Haz clic en el menú superior **Configuración,** panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.
- Haz clic en el botón **Añadir servidor proxy**. Se mostrará una ventana con todos los equipos administrados por Panda Endpoint Protection que cumplen los requisitos para ejercer de

proxy en la red.

- Utiliza la caja de búsqueda para localizar el equipo y haz clic sobre el mismo para agregarlo al listado de equipos con el rol de proxy asignado.

Retirar el rol de proxy Panda a un equipo

- Haz clic en el menú superior **Configuración,** panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.
- Haz clic en el icono del equipo que quieres retirar el rol de proxy.

Para configurar el uso de un equipo con el rol de proxy asignado consulta ***Configuración de listas de acceso a través de proxy***.

Rol de caché

Panda Endpoint Protection permite asignar el rol de caché a uno o más puestos de la red. Estos equipos descargan y almacenan de forma automática todos los ficheros que necesitan otros puestos con Panda Endpoint Protection instalado. Esto produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Limitaciones de los equipos con el rol de caché asignado

Por motivos de seguridad, cuando Panda Endpoint Protection tiene asignado el rol de caché, únicamente puede establecer conexiones con la nube de Panda. Por esta razón, hay ciertas restricciones en cuanto al tipo de descargas que el software de seguridad puede llevar a cabo cuando se configuran para realizarse a través de un nodo caché:

- Los equipos Linux no pueden descargar parches de actualización de Panda Patch Management. Consulta **Descargar e instalar parches** en la página **352**.
- Los equipos Linux no pueden descargar paquetes del software de seguridad para instalarlo o actualizarlo. Consulta **Actualización del motor de protección** en la página **202**.

Elementos cacheados

Un equipo con el rol de caché asignado puede cachear los elementos siguientes durante un periodo de tiempo variable dependiendo de su tipo:

- **Archivo de identificadores**: hasta que dejan de ser válidos.
- **Paquetes de instalación**: hasta que dejan de ser válidos.
- **Parches de actualización para** Panda Patch Management: 30 días.

Dimensionamiento de un equipo caché

El dimensionamiento de un equipo con el rol de caché asignado depende completamente del número de conexiones simultáneas en los picos de carga y del tipo de tráfico que gestione (descargas de ficheros de firmas, instaladores etc.). Como aproximación, un equipo con el rol de caché asignado puede servir en torno a 1000 equipos de forma simultánea.

Asignar el rol de caché a un equipo

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- Haz clic en el botón **Añadir equipo caché**.
- Utiliza la herramienta de búsqueda situada en la parte superior de la ventana para localizar equipos candidatos a asignar el rol de caché.
- Selecciona un equipo de la lista y pulsa **Aceptar**.

A partir de ese momento, el equipo seleccionado adoptará el rol de caché y comenzará la descarga de todos los archivos necesarios, manteniendo sincronizado su repositorio de forma automática. El resto de los puestos de la subred contactarán con el equipo caché para la descarga de actualizaciones.

Retirar el rol de caché a un equipo

Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red**, pestaña **Caché.**

Haz clic en el icono del equipo al que quieres retirar el rol caché.

Establecer la unidad de almacenamiento

Es posible configurar el agente Panda Endpoint Protection para almacenar los elementos a cachear en un volumen / unidad concreta del equipo, aunque la ruta de la carpeta dentro del volumen es fija. Para configurar esta característica sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- En un equipo con el rol de caché asignado y que ya haya reportado a la nube su estado haz clic en el enlace **Cambiar**. Se mostrará una ventana con las unidades locales disponibles.
- Por cada unidad se muestra el nombre del volumen, la unidad asignada, el espacio ocupado y el espacio libre.

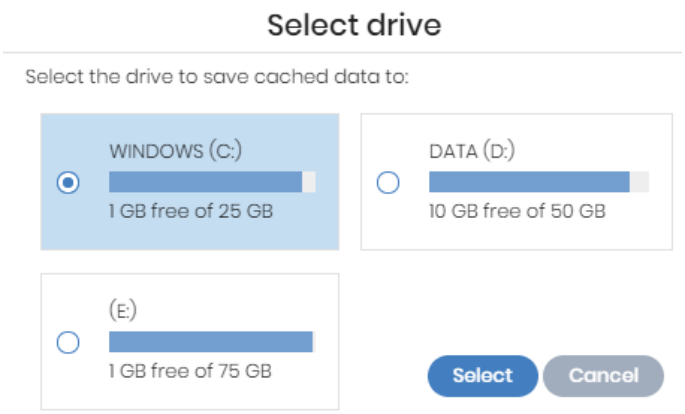


Figura 10.1: Ventana de selección de volumen en un equipo con el rol de caché asignado

- Para ver los porcentajes de espacio ocupado y libre pasa el ratón por encima de las barras y se mostrará una etiqueta con la información.
- Indica con el selector la unidad con 1 Gigabyte libre o más que almacenará los elementos cacheados, y haz clic en el botón **Seleccionar**. Panda Endpoint Protection comenzará a copiar los elementos ya cacheados y, una vez completado el proceso, los borrará de su ubicación original.

*Solo es posible seleccionar la unidad donde se almacenarán los elementos a cachear en los equipos que hayan reportado su estado al servidor Panda Endpoint Protection. Si no se cumple esta condición, se tomará por defecto la unidad que almacena los ficheros de instalación de Panda Endpoint Protection. Una vez reportado, se mostrará el enlace **Cambiar** en el equipo con el rol de cache asignado y se podrá modificar la unidad de almacenamiento. Un equipo puede tardar en reportar su estado varios minutos.*

Si no hay espacio suficiente o se produce algún error de escritura al cambiar la unidad de almacenamiento, se mostrará un mensaje debajo del equipo con el rol de caché asignado, indicando la fuente del problema.

Rol de descubridor

En el menú superior **Configuración**, panel lateral **Servicios de red**, la pestaña **Descubrimiento** está directamente relacionada con el procedimiento de instalación y despliegue de Panda Endpoint Protection en la red del cliente.

*Consulta **Visualizar equipos descubiertos** en la página **118** para obtener más información acerca del proceso de descubrimiento e instalación de Panda Endpoint Protection.*

Configuración de listas de acceso a través de proxy

Panda Endpoint Protection permite asignar a los equipos de la red uno o más métodos de conexión con el exterior, en función de los recursos existentes en la infraestructura IT de la compañía.

Los métodos de conexión se organizan a través de dos listas independientes:

- **Lista de acceso**: contiene los métodos de conexión configurados por el administrador.
- **Lista de fallback**: lista no modificable de métodos de conexión incluidos por defecto en Panda Endpoint Protection.

Si existen métodos de conexión repetidos entre ambas listas, se retirarán automáticamente de la lista de fallback.

Lista de acceso

Es la lista de métodos de acceso configurable por el administrador. Se recorre de forma ordenada cuando el agente necesita conectar con la nube de Panda Security. Una vez seleccionado un método de acceso, éste no cambia hasta que queda inaccesible, momento en el cual Panda Endpoint Protection recorrerá la lista desde el inicio hasta encontrar un nuevo método de acceso válido. Si llega al final de la lista sin encontrarlo se buscará en la lista de fallback. Consulta **Lista de fallback** .

Los tipos de conexión admitidos en la lista de acceso son:

Tipo de proxy	Descripción
No usar proxy	Acceso directo a Internet. Los equipos acceden de forma directa a la nube de Panda Security para descargar las actualizaciones y enviar los reportes de estado del equipo. En este caso, el software Panda Endpoint Protection utilizará la configuración del equipo para comunicarse con Internet.
Proxy corporativo	Acceso a Internet vía proxy instalado en la red de la organización. • **Dirección**: dirección IP del servidor de proxy.

Tipo de proxy	Descripción
	• **Puerto**: puerto del servidor de proxy. • **El proxy requiere autenticación**: habilitar si el proxy requiere información de usuario y contraseña. • **Usuario**: cuenta de un usuario del proxy que permita su uso. • **Contraseña**: contraseña de la cuenta de usuario.
Descubrimiento automático de proxy a través de Web Proxy Autodiscovery Protocol (WPAD)	Pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración. Alternativamente se puede indicar directamente el recurso HTTP o HTTPS donde se encuentra el archivo PAC de configuración. En equipos Linux no está disponible este tipo de configuración y será ignorada. Panda Security no se recomienda su uso para este sistema operativo.
Proxy Panda	Acceso a la nube de Panda Security a través de un equipo de la red con el rol de proxy Panda asignado. Una lista de acceso puede tener varios proxys Panda definidos. Para conocer las limitaciones de acceso de un proxy Panda y cómo asignar este rol a un equipo de la red consulta Rol de Proxy Panda.

Tabla 10.1: Tipos de acceso a la red soportados por Panda Endpoint Protection

Configurar una lista de acceso

Para configurar una lista de acceso crea una configuración de tipo **Configuración de red**:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** haz clic en el icono . Se mostrará una ventana con los tipos de conexión disponibles.
- Selecciona un tipo de conexión (Tipos de acceso a la red soportados por Panda Endpoint Protection) y haz clic en el botón **Aceptar**. El tipo de conexión se añadirá a la lista.
- Para modificar el orden de los métodos de conexión selecciona un elemento haciendo clic en la casilla de selección y utiliza las fechas y para subirlo o bajarlo.
- Para borrar un método de conexión haz clic en el icono .

- Para modificar un método de conexión selecciónalo con las casillas de selección y haz clic en el icono . Se mostrará una ventana donde editar la configuración del método.

Lista de fallback

Cuando el agente no puede conectar con la plataforma Aether y ya ha probado todos los métodos de conexión indicados en la lista de acceso configurada, recorrerá la lista de fallback. Esta lista de métodos de acceso no es configurable por el administrador y se recorre de forma ordenada. Una vez que el agente Panda ha encontrado un método de conexión válido, éste no se cambiará hasta que quede inaccesible, momento en el cual se volverá a recorrer la lista de acceso configurada por el administrador desde su inicio. Si ninguno de los métodos de acceso indicados en la lista de acceso o de fallback es válido, el agente devolverá un error de comunicaciones.

La lista de fallback es fija y contiene los métodos de acceso siguientes (no todos están disponibles en todas las plataformas):

- **Internet Explorer**: Panda Endpoint Protection intenta recuperar la configuración de proxy de Internet Explorer suplantando a la cuenta de usuario que inició sesión en el equipo. Solo disponible en sistemas operativos Windows.
    - Este método de acceso no se puede utilizar si la configuración de las credenciales para el uso del proxy está definida de forma explícita .
    - Si la configuración de proxy de Internet Explorer utiliza PAC (Proxy Auto-Config), solo se obtendrá la URL del archivo de configuración si el protocolo de acceso al recurso es HTTP o HTTPs.
- **Proxy por defecto**: Panda Endpoint Protection lee la configuración del proxy configurada por defecto en el sistema operativo.
- **WPAD**: Panda Endpoint Protection pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración. En equipos Linux no está disponible este tipo de configuración.
- **Conexión directa**: Panda Endpoint Protection intenta conectarse directamente a la nube de Panda Security.

Configuración de las descargas mediante equipos caché

La utilización de un equipo con el rol de caché puede establecerse de dos maneras:

- **Método automático**: el equipo que inicia la descarga utiliza los equipos con el rol de caché descubiertos en la red y que cumplan con los requisitos indicados en **Requisitos para usar un equipo con el rol de caché asignado**. Si se encuentran varios equipos caché se

balancearán las descargas para no sobrecargar a un único equipo caché.

- **Método manual**: el administrador establece de forma manual el equipo de la red con el rol de caché que será utilizado para descargar datos de la nube de Panda Security. El comportamiento de un equipo cache asignado de forma manual tiene las siguientes diferencias con respecto al modo automático:
    - Si un equipo tiene varios equipos cache asignados de forma manual, no se repartirán las descargas.
    - Si el primer equipo caché no está accesible, se recorrerá la lista hasta encontrar un equipo que funcione. Si no se encuentra ningún equipo se intentará la salida directa a Internet.

Requisitos para usar un equipo con el rol de caché asignado

Modo automático

- El equipo con el rol de cache asignado y el equipo que descarga elementos de éste deben estar en la misma subred. Si un equipo caché tiene varias tarjetas de red, podrá servir de repositorio en cada uno de los segmentos a los que esté conectado.

> *Se recomienda asignar un equipo como rol caché en cada segmento de la red de la compañía.*

- El resto de equipos descubrirán de forma automática la presencia de un equipo caché y redirigirán hacia él sus peticiones de actualización.
- Se requiere asignar una licencia de protección al equipo caché para su funcionamiento.
- Configura el cortafuegos para permitir el tráfico SSDP (uPnP) entrante y saliente en los puertos
    - 21226 UDP
    - 18226 TCP

Modo manual

- No es necesario que el equipo con el rol de cache asignado y el equipo que descarga elementos estén en la misma subred.
- Se requiere asignar una licencia de protección al equipo caché para su funcionamiento.
- Configura el cortafuegos para permitir el tráfico entrante y saliente en los puertos

- 21226 UDP y TCP
- 18226 TCP

Descubrimiento de equipos caché

En el momento de la asignación del rol al equipo, éste lanzará un broadcast hacia los segmentos de red a los que pertenecen sus interfaces. Los puestos de trabajo y servidores con el método automático de asignación recibirán la publicación del servicio y, en el caso de que en un mismo segmento haya más de un equipo caché designado, los equipos se conectarán al más adecuado en función de los recursos libres que posea.

Adicionalmente, cada cierto tiempo los equipos de la red con el método automático de asignación configurado preguntarán si existe algún equipo con el rol de caché asignado.

Configuración del método de asignación de equipos caché

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y elige una configuración.
- En la sección **Caché** elige una opción:
  - **Utilizar automáticamente los equipos caché vistos en la red**: los equipos que reciben esta configuración buscarán de forma automática los equipos caché de su segmento de red.
  - **Utilizar los siguientes equipos caché (por orden de preferencia)**: haz clic en el icono ⊕ para añadir equipos con el rol de caché asignado y configurar una lista de ellos.

    Los equipos que reciban esta configuración conectarán con los equipos caché indicados en la lista para realizar las descargas.

Configuración de la comunicación en tiempo real

Panda Endpoint Protection se comunica en tiempo real con la plataforma Aether para recuperar las configuraciones establecidas en la consola sobre los equipos protegidos, transcurriendo unos pocos segundos desde que el administrador asigna una configuración a un equipo hasta que éste la aplica.

Las comunicaciones en tiempo real entre los equipos protegidos y el servidor Panda Endpoint Protection requieren el mantenimiento de una conexión abierta por cada puesto de forma permanente. Desactiva las comunicaciones en tiempo real cuando el número de conexiones abiertas afecte al rendimiento del proxy instalado en la red, o cuando el impacto en el consumo de ancho de banda sea elevado al cambiar simultáneamente las configuraciones de un gran número de equipos.

Requisitos para comunicación en tiempo real

- Las comunicaciones en tiempo real son compatibles con todos los sistemas operativos soportados por Aether excepto Windows XP y Windows 2003.
- Si el equipo accede a Internet mediante un proxy corporativo, se requiere que las conexiones https no sean manipuladas. Muchos proxys utilizan técnicas Man in the Middle para analizar las conexiones https o funcionar como proxys caché. En estos casos la comunicación en tiempo real no funcionará.

Deshabilitar las comunicaciones en tiempo real

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** despliega la sección **Opciones avanzadas** y desactiva la casilla **Activar la comunicación en tiempo real.**

Al deshabilitar las comunicaciones en tiempo real, los equipos se comunicarán con el servidor Panda Endpoint Protection cada 15 minutos.

Configuración del idioma del agente

Para asignar el idioma del agente Panda a uno o varios equipos es necesario crear una configuración de tipo **Configuración de red**:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección idioma elige el idioma de entre los disponibles:
    - Alemán
    - Español
    - Finlandés
    - Francés
    - Húngaro
    - Inglés
    - Italiano
    - Japonés
    - Portugués
    - Ruso
    - Sueco

Si se produce un cambio de idioma y la consola local de Panda Endpoint Protection estaba abierta se pedirá un reinicio de la consola local. Este procedimiento no afecta a la seguridad del equipo.

Configuración de la visibilidad del agente

Para las empresas donde el servicio de seguridad sea 100% administrado por el departamento de IT no es necesario que el icono del agente Panda Endpoint Protection sea visible en el área de notificaciones de los equipos de la red. Para ocultar o mostrar el icono sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Preferencias** y activa o desactiva la opción **Mostrar icono en la bandeja del sistema.**

Control de acceso a redes

Control de acceso a redes aporta una capa extra de seguridad cuando los equipos de usuario se conectan a la red corporativa, ya sea remotamente a través de VPN o localmente a través de Wi-Fi.

El equipo de usuario que intenta conectarse a la red corporativa a través de VPN o de Wi-Fi, ha de cumplir una serie de condiciones para que se le permita acceder. Si no las cumple, el acceso se denegará.

El agente Panda instalado en el equipo es el encargado de reunir y enviar la información necesaria para que el dispositivo que validará el acceso (Firebox -en el caso de VPN- o Access Point -para Wi-Fi-) pueda realizar las comprobaciones necesarias.

Mecanismo de validación y generación de UUIDs

Un UUID (Universally Unique IDentifier) es una cadena de caracteres que identifica de forma única a un dispositivo.

El mecanismo utilizado en el dispositivo (FireBox o Access Point) para validar las conexiones VPN o Wi-Fi es un UUID + contraseña. Esto implica tener configurado el mismo par UUID - contraseña en el dispositivo y en la consola de Panda Endpoint Protection.

Si no tienes previamente configurado un UUID en tu dispositivo, será necesario generar uno nuevo. Al ser un formato abierto, existen muchos generadores de UUIDs gratuitos, como por ejemplo **https://www.uuidgenerator.net/**

Utiliza una contraseña lo suficientemente larga que incluya caracteres especiales, números y mayúsculas.

Para más información sobre Firebox y su configuración de conexiones VPN, consulta ***https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/Fireware/services/tdr/tdr_host_sensor_enforcement_configure.html***

Requisitos

Para que el equipo de usuario pueda conectarse a la red corporativa, tiene que cumplir los siguientes requisitos:

- Tener una protección instalada, activa y debidamente configurada en el equipo del usuario.
- Tener un UUID y una clave de autenticación válidos y configurados tanto en el dispositivo que comprueba la conexión como en la consola de Panda Endpoint Protection.
- **Sistema operativo instalado en el equipo**:
  - Windows 8.1 o superior.
  - MacOS High Sierra 10.13 o superiores.
- **Puertos abiertos en el equipo**: el agente Panda requiere el puerto 33000 para comunicarse con el dispositivo que valida la conexión.
- **Una configuración de protección válida**: protección antivirus Panda Endpoint Protection activada y en ejecución.

Control de acceso a redes no es compatible con el sistema operativo Linux.

Comprobación de los requisitos

Cuando el equipo trata de conectarse a la red corporativa, el dispositivo que valida la conexión lleva a cabo las siguientes acciones:

- Solicita información sobre el estado de la protección instalada en el equipo de usuario.
- Comprueba que la UUID de la cuenta y la clave de autenticación son válidas.
- Confirma que el sistema operativo del equipo de usuario es válido, comparándolo con los que tiene configurados.

Si todas las comprobaciones son positivas, el dispositivo permitirá el acceso del equipo a la red corporativa; en caso contrario, no lo permitirá.

De forma predeterminada, los equipos tienen activada la exigencia de cumplimiento de los requisitos de seguridad para conectarse a la red corporativa.

Acceso a la configuración de Control de acceso a redes

- Selecciona el menú lateral **Servicios de red**.
- En el menú de pestañas superior, haz clic en **Control de acceso a redes**.
- Para activar la protección, mueve el control deslizante.
- Escribe el UUID de la cuenta y la clave de autenticación.
- Haz clic en el botón **Guardar cambios**.

Configuración de contraseña y anti-tampering

Anti-tamper

Muchas amenazas avanzadas incorporan técnicas para desactivar el software de seguridad de los equipos. La protección Anti-tamper evita la modificación no autorizada del funcionamiento de la protección impidiendo que el software se detenga, pause o se desinstale mediante el establecimiento de una contraseña.

Para evitar estos problemas, la protección Anti-tamper de Panda Endpoint Protection funciona de la siguiente manera:

- La configuración de **Ajustes de equipo** creada por defecto incluye una contraseña pre calculada única para cada cliente. Esta contraseña no se puede cambiar ya que las configuraciones por defecto son de solo lectura.
- En las configuraciones de **Ajustes por equipo** generadas por el usuario la opción de anti-tamper puede ser desactivada o activada, dependiendo de las medidas de seguridad que se quieran aplicar.

Las contraseñas creadas para las configuraciones de seguridad deben tener entre 6 y 15 caracteres.

Habilitar / Inhabilitar anti-tamper

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existen o selecciona **Añadir** para crear una nueva.

- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**:
    - **Activar protección anti-tamper**: impide que los usuarios o ciertos tipos de malware puedan detener las protecciones. Requiere el establecimiento de una contraseña ya que es posible que el administrador o el equipo de soporte necesiten detener temporalmente desde la consola local las protecciones para diagnosticar problemas. Mediante el botón de la derecha se puede activar o desactivar esta funcionalidad de las configuraciones creadas.

*Al desactivar la opción de seguridad **Activar protección anti-tamper** o **Solicitar contraseña para desinstalar la protección de los equipos** aparecerá un aviso de seguridad cuando se guarde la configuración. No es recomendable desactivar estas opciones de seguridad.*

Protección del agente mediante contraseña

Para evitar que el usuario modifique las características de protección o desinstale completamente el software Panda Endpoint Protection, el administrador puede establecer una contraseña local que cubra ambos casos.

Asignar una contraseña local

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**:
    - **Solicitar contraseña para desinstalar Aether desde los equipos**: evita que el usuario desinstale el software Panda Endpoint Protection protegiéndolo con una contraseña.
    - **Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos**: permite administrar las capacidades de seguridad del equipo desde la consola local. Requiere el establecimiento de una contraseña.

Si un equipo pierde la licencia asignada, de manera manual o por caducidad o cancelación, las protecciones anti-tampering y las protección por contraseña contra las desinstalación quedarán desactivadas.

Activar verificación en dos pasos (2FA)

Establece un doble factor de autenticación sobre el agente instalado en los dispositivos para evitar manipulaciones no autorizadas por parte de terceros.

Puedes generar un único segundo factor de autenticación para toda la cuenta, o varios, dependiendo del número de administradores que operan la consola. De este modo podrás compartir un mismo factor de autenticación en algunas configuraciones de **Ajustes por equipo**, o asignar un doble factor de autenticación independiente para cada configuración de **Ajustes por equipo**.

Para asignar un doble factor de autenticación para toda la cuenta (todas configuraciones de **Ajustes por equipo** comparten el mismo código QR):

- Desde el menú superior **Configuración**, haz clic en **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**
- Activa con el botón **Activar verificación en dos pasos (2FA)**.
- Selecciona **Utilizar un código QR compartido en toda la cuenta**.
- Haz clic en **Mostrar código QR**. Se mostrará el código QR generado para todas las configuraciones de **Ajustes por equipo** de la cuenta.
- Sincroniza el código QR de la cuenta con la aplicación **Watchguard Authpoint** o una equivalente.
- Haz clic en el botón **Cerrar**.
- Haz clic en el botón **Guardar**.

Para asignar un doble factor de autenticación para una configuración de **Ajustes por equipo** particular:

- Desde el menú superior **Configuración**, haz clic en **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**.
- Activa con el botón **Activar verificación en dos pasos (2FA)**.
- Selecciona **Generar un código QR para esta configuración**.
- Haz clic en el botón **GENERAR CÓDIGO**.
- Escribe una contraseña de 6 a 20 caracteres utilizando códigos alfanuméricos. Esta contraseña está vinculada al código QR que genera la consola y puede ser reutilizada en otras configuraciones de **Ajustes por equipo**.
- Haz clic en **GENERAR CÓDIGO**.

- Haz clic en el botón **Cerrar**.
- Haz clic en el botón **Guardar**.

Para asignar un doble factor de autenticación para algunas configuraciones de **Ajustes por equipo**:

- Desde el menú superior **Configuración**, haz clic en **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**.
- Activa con el botón **Activar verificación en dos pasos (2FA)**.
- Selecciona **Generar un código QR para esta configuración**.
- Haz clic en el botón **GENERAR CÓDIGO**.
- Escribe una contraseña que ya has utilizado en otras configuraciones de **Ajustes por equipo**. Se generará el mismo código QR.
- Haz clic en **GENERAR CÓDIGO**.
- Haz clic en el botón **Cerrar**.
- Haz clic en el botón **Guardar**.

Activar la protección cuando el equipo arranca en modo seguro con funciones de red

Algunos tipos de malware están diseñados para forzar el reinicio de equipos Windows en modo seguro con funciones de red activadas. En este modo de inicio, el antivirus está desactivado y los equipos son vulnerables.

Puedes configurar Panda Endpoint Protection para que proteja a los equipos cuando arrancan en modo seguro con funciones de red, de manera que todas las protecciones que tienen configuradas se mantengan activas y funcionando con normalidad.

Para proteger los equipos Windows que inician en modo seguro con acceso a la red, sigue estos pasos:

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**.
- En **Activar protección cuando los equipos Windows arrancan en Modo Seguro**, sitúa el cursor deslizante en la posición **ON**.

Configuración de Shadow Copies

Shadow Copies es una tecnología implementada en sistemas operativos Windows que permite realizar copias de seguridad transparentes de los ficheros almacenados en el equipo del usuario.

A través de la consola de Panda Endpoint Protection, el administrador puede interactuar con el servicio Shadow Copies de los equipos de la red de forma remota y centralizada, y utilizarlo como herramienta de resolución frente ataques de tipo ransomware.

Características de Shadow Copies en Panda Endpoint Protection

Panda Endpoint Protection completa al servicio Shadow Copies de Windows con características adicionales que permiten proteger los datos del usuario frente a las amenazas:

- Configura y gestiona un repositorio de copias (snapshot) independiente de los que haya creado el usuario.
- Protege al servicio y al snapshot frente a modificaciones realizadas por amenazas o por el mismo usuario. De esta manera, se impide la detención del servicio o el borrado de las copias de seguridad ya realizadas por Panda Endpoint Protection.
- Permite configurar el porcentaje de espacio del disco duro dedicado a la copia de seguridad (por defecto utiliza un 10% del espacio del dispositivo).
- Realiza una copia de los ficheros cada 24 horas. La primera copia se produce en el momento en el que el administrador activa la funcionalidad (por defecto se entrega desactivada).
- Guarda hasta un total de 7 copias de cada fichero, dependiendo del espacio libre asignado al repositorio. Si el espacio no es suficiente, se elimina la copia más antigua para dar cabida a la más reciente.

Requisitos

- Sistema operativo:
    - Windows Vista y superiores.
    - Windows 2003 Server y superiores.
- Espacio en disco suficiente para realizar las copias.
- Medio de almacenamiento identificado por el sistema operativo como fijo (discos duros internos y conectados por usb) y con formato NTFS.

Acceso a la funcionalidad de Shadow Copies

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Ajustes por equipo**. Se mostrará el listado de configuraciones.

- Haz clic sobre una configuración o crea una nueva.
- En el apartado **Shadow Copies** mueve el control deslizante para activar la funcionalidad, y establece el porcentaje máximo del disco que ocuparán las copias en los discos de los equipos.

Aunque Panda Endpoint Protection utiliza un snapshot independiente de los creados por el usuario o el administrador de la red, todos ellos comparten la misma configuración. Además, el porcentaje máximo del disco establecido en la consola de administración tiene prioridad frente a otras configuraciones establecidas por el administrador de la red.

Buscar los equipos con Shadow Copies activado mediante filtros

- Haz clic en el menú superior **Equipos**
- Haz clic en el icono del panel lateral. Se mostrará el árbol de filtros.
- Haz clic en el icono de cualquier carpeta del árbol de filtros. Se desplegará el menú de contexto.
- Haz clic en **Añadir Filtro**. Se abrirá la ventana **Añadir filtro**.
- Configura el filtro con los valores siguientes:
  - **Categoría**: Equipo
  - **Propiedad**: Shadow Copies
  - **Operador**: Es igual a
  - **Valor**: Activado

*Para más información, consulta **Configurar filtros** en la página **216***

Capítulo 11

Configuración de la seguridad en estaciones y servidores

Panda Endpoint Protection ofrece todas las funcionalidades de protección incluidas en el producto mediante las configuraciones de seguridad para estaciones y servidores. El administrador de la red podrá proteger los activos de la empresa frente a amenazas informáticas de muy diversa índole, asignando configuraciones de seguridad a los equipos de la red.

A continuación se explican todos los parámetros incluidos en la configuración de seguridad para estaciones y servidores. También se indican algunas recomendaciones prácticas para asegurar los puestos de trabajo de la red y minimizar los inconvenientes ocasionados al usuario.

Para obtener información adicional sobre los distintos apartados del módulo Estaciones y servidores consulta las referencias siguientes:

***Crear y gestionar configuraciones** en la página **285**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.*

***Acceso, control y supervisión de la consola de administración** en la página **53**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.*

Contenido del capítulo

Acceso a la configuración y permisos necesarios

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Estaciones y servidores**.

Permisos requeridos

Permiso	Tipo de acceso
Configurar seguridad para estaciones y servidores	Crear, modificar, borrar, copiar o asignar las configuraciones de Estaciones y servidores.
Ver configuraciones de seguridad para estaciones y servidores	Visualizar las configuraciones de Estaciones y servidores.

Tabla 11.1: Permisos requeridos para acceder a la configuración Estaciones y servidores

Introducción a la configuración de la seguridad

Las configuraciones de seguridad para estaciones y servidores se dividen en varios apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con la información asociada. A continuación, se muestran las diferentes secciones con una breve explicación.

Sección	Descripción
General	Establece el comportamiento de las actualizaciones, desinstalaciones de los antivirus de otros fabricantes y los ficheros excluidos en el equipo del usuario o servidor protegido que no se analizarán.
Antivirus	Establece el comportamiento de la protección antimalware tradicional frente a virus y amenazas.

Sección	Descripción
Firewall (Dispositivos Windows)	Establece el comportamiento del cortafuegos y del IDS que protege al equipo de los ataques de red.
Control de dispositivos (Dispositivos Windows)	Determina el acceso del usuario a los periféricos conectados al equipo.

Tabla 11.2: Descripción de los módulos disponibles en Panda Endpoint Protection

No todas las funcionalidades se encuentran disponibles en todas las plataformas soportadas. A continuación se muestra un resumen de las funcionalidades de seguridad incluidas en Panda Endpoint Protection por plataforma compatible:

Funcionalidad	Windows	macOS	Linux	Windows Exchange (1)
Antivirus (1)	X	X	X	X
Cortafuegos & IDS	X			
Protección Email	X			
Protección Web	X	X		
Control de dispositivos	X			

Tabla 11.3: Funcionalidades de seguridad por plataforma

(1) El filtrado de correo para servidores Microsoft Exchange solo está disponible para clientes que contrataron Panda Endpoint Protection en la versión 3.72.00 y anteriores.

Configuración General

La configuración general establece el comportamiento de Panda Endpoint Protection relativo a las actualizaciones, desinstalación de programas de la competencia y exclusiones de ficheros y carpetas que no se analizarán.

Alertas en los equipos

Campo	Descripción
Mostrar alertas de malware, firewall y control de dispositivos	Introduce un mensaje descriptivo para informar al usuario del motivo de la alerta. El agente Panda Endpoint Protection mostrará una ventana desplegable con el contenido del mensaje
Mostrar alertas cada vez que el control de acceso a páginas web bloquee una página	Muestra una ventana emergente en el equipo del usuario o servidor cada vez que Panda Endpoint Protection bloquea el acceso a una página web. En los equipos Windows, es posible desactivarlo para que no se muestre el mensaje.

Tabla 11.4: Campos Alertas en los equipos

Actualizaciones

*Consulta **Actualización del producto** en la página **201** para obtener información acerca de los procedimientos necesarios para actualizar el agente, la protección y el fichero de firmas de software cliente instalado en el equipo del usuario.*

Desinstalar otros productos de seguridad

*Consulta **Visión general del despliegue de la protección** en la página **95** para establecer el comportamiento de la instalación de la protección en el caso de que otro producto de seguridad esté instalado previamente en el equipo del usuario.*

*Consulta **Des instaladores soportados** para obtener un listado de todos los productos de la competencia que Panda Endpoint Protection desinstala automáticamente del equipo del usuario.*

Archivos y rutas excluidas del análisis

Configura los elementos del equipo que no serán, borrados o desinfectados en busca de malware.

Esta configuración desactiva la protección antivirus. Debido a que el uso de esta configuración genera potenciales agujeros de seguridad, Panda recomienda limitar su uso, quedando éste restringido a evitar problemas del rendimiento.

Exclusiones establecidas por el partner

Por defecto los administradores no pueden modificar o eliminar las configuraciones de **Estaciones y servidores** enviadas por el partner. Sin embargo, el partner puede establecer configuraciones como editables, que se mostrarán marcadas con la etiqueta **Exclusiones Editables**. En este caso los administradores podrán añadir exclusiones pero no borrar o modificar la lista de exclusiones definida por el partner.

Si el partner cambia el estado de las configuraciones enviadas de editable a no editable, las exclusiones añadidas por el usuario se ocultarán y dejarán de aplicarse, de modo que solo se aplicarían las enviadas por el partner. Si el partner vuelve a establecer como editable, las exclusiones añadidas por el administrador se restaurarán y volverán a aplicarse.

Excluir los siguientes archivos en disco

Indica los ficheros en el disco de los equipos protegidos que no serán borrados o desinfectados por Panda Endpoint Protection.

Campo	Descripción
Extensiones	Extensiones de ficheros que no serán analizadas.
Carpetas	Carpetas cuyo contenido no será analizado. Se pueden utilizar variables de sistema para excluir carpetas del análisis. No se pueden excluir carpetas utilizando variables creadas por el propio usuario.
Archivos	Ficheros que no serán analizados. Se permite el uso de los caracteres comodín '*' y '?'. Si no se especifica la ruta a un fichero, éste se excluirá en todas las carpetas donde se encuentre. En caso de especificar la ruta, solo se excluirá del análisis el fichero de esa carpeta. No se admite el uso de comodines al especificar la ruta completa de un fichero.
Exclusiones	Al hacer clic en el botón **Añadir**, se cargan de forma automática las

Campo	Descripción
recomendadas para Exchange	exclusiones recomendadas por Microsoft para optimizar el rendimiento del producto en servidores Exchange.

Tabla 11.5: Ficheros en disco que no serán analizados por Panda Endpoint Protection

Excluir los siguientes archivos adjuntos de correo

Especifica la lista de extensiones de ficheros que no son analizados en caso de encontrarse como adjuntos en mensajes de correo.

Antivirus

Esta sección configura el comportamiento general del motor de antivirus basado en ficheros de firmas.

Campo	Descripción
Protección de archivos	Activa o desactiva la protección antivirus que afecta al sistema de ficheros.
Protección de correo	Activa o desactiva la protección antivirus que afecta al cliente de correo instalado en el equipo del usuario. Panda Endpoint Protection detectará las amenazas recibidas por el protocolo POP3 y sus variantes cifradas.
Protección web	Activa o desactiva la protección antivirus que afecta al cliente web instalado en el equipo del usuario. Panda Endpoint Protection detectará las amenazas recibidas por el protocolo HTTP y sus variantes cifradas.

Tabla 11.6: Módulos de protección antivirus disponibles en Panda Endpoint Protection

La acción que ejecuta Panda Endpoint Protection ante un fichero de tipo malware o sospechoso se define en los laboratorios de Panda Security:

- **Ficheros conocidos como malware desinfectable**: sustituir el fichero original por una copia desinfectada.
- **Ficheros conocidos como malware no desinfectable**: se guarda una copia de seguridad y el fichero original se elimina.

Amenazas a detectar

Configura el tipo de amenazas que Panda Endpoint Protection busca y elimina en el sistema de archivos, cliente de correo y web instalados en el equipo del usuario.

Campo	Descripción
Detectar virus	Ficheros que contienen patrones identificados por el fichero de firmas como peligrosos.
Detectar herramientas de hacking y PUPs	Programas no deseados (programas que contienen publicidad intrusiva, barras de navegación etc.) y herramientas utilizadas por los hackers para ganar acceso a los sistemas.
Bloquear acciones maliciosas	Activa tecnologías heurísticas y de análisis contextual para supervisar localmente el comportamiento de los procesos y buscar actividades sospechosas.
Detectar Phishing	Ataques basados en el engaño por web y correo.
No detectar amenazas en las siguientes direcciones y dominios	Lista blanca de direcciones y dominios que no se analizarán en busca de ataques por phishing. Se compara a nivel de sub cadenas y sin tener en cuenta las mayúsculas y minúsculas por lo que para incluir una dirección en la lista blanca es suficiente con indicar una parte de la misma.
Crear Decoy Files para ayudar a la detección de ransomware	Crea en el equipo del usuario ficheros de control que son permanentemente monitorizados porPanda Endpoint Protection. En caso de detectarse cambios, se clasifica identifica al proceso que lo originó como ransomware y se finaliza para evitar el cifrado masivo del sistema de ficheros.

Tabla 11.7: Tipos de malware detectados por la protección antivirus de Panda Endpoint Protection

Tipos de archivos

Indica los tipos de archivos que Panda Endpoint Protection analiza:

Campo	Descripción
Analizar comprimidos en disco	Descomprime los ficheros empaquetados y analiza su contenido en busca de malware.
Analizar comprimidos en mensajes de correo	Descomprime los ficheros adjuntos que viajan en los correos electrónicos y analiza su contenido en busca de malware.

Campo	Descripción
Analizar todos los archivos independientemente de su extensión cuando son creados o modificados (No recomendado)	Por cuestiones de rendimiento no se recomienda analizar todos los ficheros ya que técnicamente muchos tipos de ficheros de datos no pueden presentar amenazas a la seguridad del equipo.

Tabla 11.8: Tipos de archivos analizados por la protección antivirus de Panda Endpoint Protection

Firewall (Equipos Windows)

Panda Endpoint Protection supervisa las comunicaciones que recibe o envía cada equipo de la red, bloqueando aquellas que cumplan con las reglas definidas por el administrador. Este módulo es compatible tanto con IPv4 como con IPv6, e incluye varias herramientas para filtrar el tráfico de red:

- **Protección mediante reglas de sistema**: describen características de las comunicaciones establecidas por el equipo (puertos, IPs, protocolos etc.), con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas configuradas.
- **Protección de programas**: permite o deniega la comunicación a determinados programas instalados en el equipo de usuario.
- **Sistema de detección de intrusos**: detecta y rechaza patrones de tráfico mal formado que afectan a la seguridad o al rendimiento del equipo protegido.

Modo de funcionamiento

Se accede mediante el control **La configuración firewall la establece el usuario de cada equipo:**

- **Activado (firewall en modo usuario o auto administrado)**: el propio usuario podrá configurar desde la consola local el firewall de su equipo.
- **Desactivado (firewall en modo administrador)**: el administrador configura el cortafuegos de los equipos a través de perfiles de configuración.

Tipo de red

Los equipos de usuario portátiles pueden conectarse a redes con un grado de seguridad muy diverso según se trate de accesos públicos, como la red wifi de un cibercafé, o de redes gestionadas o de acceso limitado, como la red de una empresa. Para ajustar el comportamiento por defecto del cortafuegos, el administrador de la red puede seleccionar de forma manual el tipo de red al que se conectan usualmente los equipos del perfil configurado, o puede dejar a Panda Endpoint Protection. la elección de la red mas apropiada.

Tipo de red	Descripción
Red pública	Redes que se encuentran en cibercafés, aeropuertos, etc. Implica establecer limitaciones en el nivel de visibilidad de los equipos protegidos y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios. Las reglas de Panda Security pueden activarse o no al criterio del administrador.
Red de confianza	Redes que se encuentran en oficinas y domicilios. El equipo es perfectamente visible para el resto de usuarios de la red, y viceversa. Las reglas de Panda Security no se aplican, de forma que no hay limitaciones para compartir archivos, recursos y directorios.
Detectar automáticamente	El tipo de red (red pública o red de confianza) se selecciona de forma automática en función de una serie de criterios que el equipo del usuario debe de cumplir. Haz clic en el enlace **Configurar reglas para determinar cuándo un equipo está conectado a una red de confianza**.

Tabla 11.9: Tipos de red compatibles con el cortafuegos

El comportamiento de Panda Endpoint Protection según la red seleccionada se traduce en un mayor o menor número de reglas añadidas de forma automática. Estas reglas se pueden ver en Reglas de programa y Reglas de conexión como "reglas de Panda".

El tipo de red es un concepto aplicable a cada interface de red del equipo de forma independiente. Es posible que equipos con varias interfaces de red tengan distintos tipos de red asignados y por lo tanto las reglas del cortafuegos serán diferentes para cada interface de red.

Configurar criterios para determinar el tipo de red

Panda Endpoint Protection permite añadir uno o más criterios que el equipo protegido por el cortafuegos deberá de cumplir para seleccionar de forma automática la configuración **Red de confianza**. Si ninguna de estas condiciones se cumplen el tipo de red establecido en el interface de red será **Red pública**.

Un criterio es una regla que determina si una interface de red del equipo se considera que está conectado a una red de confianza. Esta asociación se realiza mediante la resolución de un dominio definido previamente en un servidor DNS interno de la empresa: si el equipo es capaz de conectar con el servidor DNS de la empresa y resolver el dominio configurado querrá decir que

está conectado a la red de la empresa, y por lo tanto el cortafuegos puede asumir que el equipo se encuentra en una red de confianza.

A continuación se muestra un ejemplo de configuración completo:

- En este ejemplo se utilizará "`miempresa.com`" como la zona principal del cliente que quiere que sus equipos detecten de forma automática si están conectados a la red corporativa.
- Añade el registro de tipo A "`criteriocortafuegos`" en la zona "`miempresa.com`" del servidor DNS interno de la red, sin especificar dirección IP ya que no tendrá ninguna utilidad.
- Según esta configuración, "`criteriocortafuegos.miempresa.com`" será el dominio que Panda Endpoint Protection intentará resolver para comprobar que se encuentra dentro de la red corporativa.
- Reinicia el servidor DNS para cargar la nueva configuración si fuera necesario, y comprueba que " `criteriocortafuegos.miempresa.com` " se resuelve correctamente desde todos los segmentos de la red interna con las herramientas `nslookup`, `dig` o `host`.
- En la consola de Panda Endpoint Protection haz clic en el enlace **Configurar reglas para determinar cuándo un equipo está conectado a una red de confianza**. Se mostrará una ventana con los siguientes campos a completar:
    - **Nombre del criterio**: indica un nombre descriptivo de la regla a configurar. Por ejemplo "`micriterioDNS`".
    - **Servidor DNS**: indica la dirección IP del servidor DNS de la red interna de la empresa que recibirá la petición de resolución.
    - **Dominio**: indica la petición que el equipo enviará al servidor DNS para su resolución. Introduce "`criteriocortafuegos.miempresa.com`".
- Haz clic en el botón **Aceptar**, en el botón **Guardar** y nuevamente en el botón **Guardar**.
- Una vez configurado y aplicado el criterio el equipo intentará resolver el dominio "`criteriocortafuegos.miempresa.com`" en el servidor DNS especificado cada vez que se produzca un evento en la interface de red (conexión desconexión, cambio de IP etc.). Si la resolución DNS es correcta se asignará a la interface de red que se utilizó la configuración asignada a la red de confianza.

Reglas de programa

En esta sección se configuran los programas del usuario que comunican con la red y los que tienen bloqueado el envío y recepción de datos.

Para desarrollar una correcta estrategia de protección sigue los pasos mostrados a continuación, en el orden indicado:

1. **Establecer la acción por defecto**.

Acción	Descripción
Permitir	Estrategia permisiva basada en aceptar por defecto las conexiones de todos los programas cuyo comportamiento no ha sido definido explícitamente mediante una regla en el paso 3. Este es el modo configurado por defecto y considerado el más básico.
Denegar	Estrategia restrictiva basada en denegar por defecto las conexiones de los programas cuyo comportamiento no ha sido definido explícitamente mediante una regla en el paso 3. Este es el modo avanzado de funcionamiento ya que requiere añadir reglas para todos los programas que los usuarios utilizan de forma habitual; de otro modo las comunicaciones de esos programas son denegadas, afectando probablemente a su buen funcionamiento.

Tabla 11.10: Tipos de acción por defecto en el cortafuegos para los programas instalados en el equipo del usuario

2. **Activar o desactivar las reglas de Panda Security**.

Solo se aplican en caso de que el equipo esté conectado a una red pública.

3. **Añadir reglas para definir el comportamiento específico de una aplicación**.

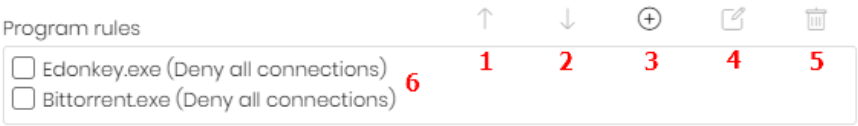


Figura 11.1: Controles de edición de reglas de red

Los controles situados a la derecha permiten subir **(1)**, bajar **(2)**, añadir **(3)**, editar **(4)** y borrar **(5)** reglas de programas. Las casillas de selección **(6)** determinan sobre qué reglas se realizarán las acciones.

Al crear una regla es necesario indicar los siguientes campos:

- **Descripción**: descripción de la regla.
- **Programa**: selecciona el programa cuyo comportamiento en red se va a controlar.
- **Conexiones permitidas para este programa**: define las características del tráfico que se controlará:

Campo	Descripción
Permitir	El programa se podrá conectar a la red (Internet y redes locales) y también

Campo	Descripción
conexiones entrantes y salientes	se permitirá que otros se conecten a él. Existen ciertos tipos de programas que requieren este tipo de permisos para funcionar correctamente: programas de intercambio de archivos, aplicaciones de chat, navegadores de Internet, etc.
Permitir conexiones salientes	El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.
Permitir conexiones entrantes	El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos para establecer nuevas conexiones.
Denegar todas las conexiones	El programa no podrá acceder a la red.

Tabla 11.11: Modos de comunicación de los programas permitidos

- **Permisos avanzados**: define las características exactas del tráfico que es aceptado o denegado.

Campo	Descripción
Acción	Establece la acción que ejecutará Panda Endpoint Protection si la regla coincide con el tráfico examinado. • **Permitir**: permite el tráfico. • **Denegar**: bloquea el tráfico. Hace un `Drop` de la conexión.
Sentido	Establece la dirección del tráfico para protocolos orientados a conexión, como TCP. • **Salientes**: tráfico con origen el equipo de usuario y destino otro equipo de la red. • **Entrantes**: tráfico con destino el equipo de usuario y origen otro equipo de la red.
Zona	La regla solo se aplica si la zona indicada coincide con la zona configurada en Tipo de red. Las reglas que tengan en campo **Zona** a **Todos** se aplican siempre sin tener en cuenta la zona configurada en el perfil de protección.

Campo	Descripción
Protocolo	Especifica el protocolo de nivel 3 del tráfico generado: • Todos • TCP • UDP
IP	• **Todos**: no tiene en cuenta los campos IP de origen y destino de la conexión. • **Personalizado**: define la IP de origen o destino del tráfico a controlar. Especifica más de una IP separadas por ',' o utiliza el carácter '-' para establecer rangos de IPs. Selecciona en el desplegable si las direcciones IP son IPv4 o IPv6. No es posible mezclar tipos de direcciones IP en una misma regla. • **Puertos**: selecciona el puerto de la comunicación. Elige **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.

Tabla 11.12: Modos avanzados de comunicación de los programas permitidos

Reglas de conexión

Son reglas tradicionales de filtrado de tráfico TCP/IP. Panda Endpoint Protection extrae el valor de ciertos campos de las cabeceras de cada paquete que reciben o envían los equipos protegidos, y explora el listado de reglas introducido por el administrador. Si alguna regla coincide con el tráfico examinado se ejecuta la acción asociada.

Las reglas de conexiones afectan a todo el sistema, independientemente del proceso que las gestione, y son prioritarias con respecto a las reglas por programa, configuradas anteriormente.

Para desarrollar una correcta estrategia de protección frente a tráfico no deseado o peligroso sigue los pasos mostrados a continuación, en el orden que se indica:

1. **Establecer la acción por defecto del cortafuegos, situada en Reglas para programas**.

Acción	Descripción
Permitir	Estrategia permisiva basada en aceptar por defecto las conexiones cuyo comportamiento no ha sido definido mediante reglas en el paso 3. Este es el modo básico de configuración: todas las conexiones no descritas mediante reglas son automáticamente aceptadas.
Denegar	Estrategia restrictiva basada en denegar por defecto las conexiones cuyo

Acción	Descripción
	comportamiento no ha sido definido mediante reglas en el paso 3. Este es el modo avanzado de funcionamiento: todas las conexiones no descritas mediante reglas son automáticamente denegadas.

Tabla 11.13: Tipos de acción por defecto en el cortafuegos para las conexiones gestionadas en el equipo del usuario

2. **Activar o desactivar las reglas de Panda Security.**

Solo se aplican en caso de que el equipo esté conectado a una red pública.

3. **Añadir reglas que describan conexiones de forma específica junto a una acción asociada.**

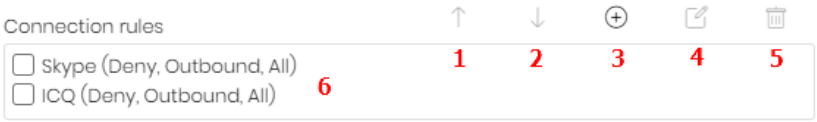


Figura 11.2: Controles de edición de reglas de red

Los controles situados a la derecha permiten subir **(1)**, bajar **(2)**, añadir **(3)**, editar **(4)** y borrar **(5)** reglas de conexión. Las casillas de selección **(6)** determinan sobre qué reglas se aplican las acciones.

El orden de las reglas en la lista es importante: su aplicación se evalúa en orden descendente y, por lo tanto, al desplazar una regla hacia arriba o abajo en la lista, se modificará su prioridad.

A continuación, se describen los campos que forman una regla de sistema:

Campo	Descripción
Nombre de regla	Asigna un nombre único a la regla.
Descripción	Descripción del tipo de tráfico filtrado por la regla.
Sentido	Establece la dirección del tráfico para protocolos orientados a conexión, como TCP. • **Salientes**: tráfico saliente. • **Entrantes**: tráfico entrante.
Zona	La regla solo se aplica si la zona indicada coincide con la zona configurada en **Tipo de red**. Las reglas que tengan en campo **Zona** a **Todos** se aplican siempre sin tener en cuenta la zona configurada en el perfil de

Campo	Descripción
	protección.

Protocolo	Especifica el protocolo del tráfico. Según la elección se mostrarán unos controles u otros para identificarlo de forma precisa:
	• **TCP, UPD, TCP/UDP:** describe reglas TCP y / o UDP incluyendo puertos locales y remotos.
	  • **Puertos locales**: puerto de la conexión utilizado en el equipo del usuario. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
	  • **Puertos remotos**: puerto de la conexión utilizado en el equipo remoto. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
	• **Servicios ICMP**: crea reglas que describen mensajes ICMP, indicando su tipo y subtipo.
	• **Servicios ICMPv6**: crea reglas que describen mensajes ICMP sobre IPv6, indicando su tipo y subtipo.
	• **Tipos IP**: crea reglas para el protocolo IP y otros protocolos se orden superior.

Direcciones IP	Direcciones IP de origen o destino del tráfico. Especifica varias direcciones IP separadas por coma o mediante rangos con guión. Selecciona en el desplegable si las direcciones IP son IPv4 o IPv6. No es posible mezclar tipos de direcciones IP en una misma regla.
Direcciones MAC	Direcciones MAC de origen o destino del tráfico.

Tabla 11.14: Campos de las reglas de conexión

Las direcciones MAC de origen y destino se reescriben en las cabeceras del paquete de datos cada vez que el tráfico atraviesa un proxy, enrutador etc. Los paquetes llegarán al destino con la MAC del último dispositivo que manipuló el tráfico.

Bloquear intrusiones

El módulo IDS permite detectar y rechazar tráfico mal formado y especialmente preparado para impactar en el rendimiento o la seguridad del equipo a proteger. Este tipo de tráfico puede provocar un mal funcionamiento de los programas del usuario que lo reciben, resultando en problemas de seguridad y permitiendo la ejecución de aplicaciones de forma remota por parte del hacker, extracción y robo de información etc.

A continuación, se detallan los tipos de tráfico mal formado soportados y una explicación de cada uno de ellos:

Campo	Descripción
IP explicit path	Rechaza los paquetes IP que tengan la opción de "explicit route". Son paquetes IP que no se encaminan en función de su dirección IP de destino, en su lugar la información de encaminamiento es fijada de ante mano.
Land Attack	Comprueba intentos de denegación de servicios mediante bucles infinitos de pila TCP/IP al detectar paquetes con direcciones origen y destino iguales.
SYN flood	Controla los el numero de inicios de conexiones TCP por segundo para no comprometer los recursos del equipo atacado. Pasado cierto limite las conexiones se rechazan.
TCP Port Scan	Detecta conexiones simultáneas a varios puertos del equipo protegido en un tiempo determinado y filtra tanto la petición de apertura como la respuesta al equipo sospechoso, para que el origen del tráfico de escaneo no obtenga información del estado de los puertos.
TCP Flags Check	Detecta paquetes TCP con combinaciones de flags inválidas. Actúa como complemento a las defensas de "Port Scanning" al detener ataques de este tipo, tales como "SYN & FIN" y "NULL FLAGS" y los de "OS identification" ya que muchas de estas pruebas se basan en respuesta a paquetes TCP inválidos.
Header lengths	• **IP**: rechaza los paquetes entrantes con un tamaño de cabecera IP que se salga de los límites establecidos. • **TCP**: rechaza los paquetes entrantes con un tamaño de cabecera TCP que se salga de los límites establecidos. • **Fragmentation control**: comprueba el estado de los fragmentos de los paquetes a reensamblar, protegiendo al equipo de ataques por consumo excesivo de memoria en ausencia de fragmentos, del redireccionado de

Campo	Descripción
	ICMP disfrazado de UDP y del escaneo de equipos.
UDP Flood	Rechaza los paquetes UDP que llegan a un determinado puerto si superan un limite en un periodo establecido.
UDP Port Scan	Protección contra escaneo de puertos UDP.
Smart WINS	Rechaza las respuestas WINS que no se corresponden con peticiones que el equipo ha solicitado.
Smart DNS	Rechaza las respuestas DNS que no se corresponden con peticiones que el equipo ha solicitado.
Smart DHCP	Rechaza las respuestas DHCP que no se corresponden con peticiones que el equipo ha solicitado.
ICMP Attack	• **SmallPMTU**: detecta valores inválidos en el tamaño de los paquetes ICMP para generar una denegación de servicio o ralentizar el tráfico saliente. • **SMURF**: rechaza las respuestas ICMP no solicitadas si estás superan un limite en un intervalo. Este tipo de ataque envía grandes cantidades de tráfico ICMP (echo request) a la dirección de broadcast de la red con la dirección de origen cambiada (spoofing) apuntando a la dirección de la víctima. La mayoría de los equipos de la red responderán a la víctima, multiplicando el tráfico por cada equipo de la subred. • **Drop unsolicited ICMP replies**: rechaza todas las respuestas ICMP no solicitadas o que han expirado por el timeout establecido.
ICMP Filter echo request	Rechaza las peticiones de Echo request.
Smart ARP	Rechaza las respuestas ARP que no se corresponden con peticiones que el equipo protegido ha solicitado para evitar escenarios de tipo ARP caché poison.

Campo	Descripción
OS Detection	Falsea datos para engañar a los detectores de sistemas operativos y así evitar posteriores ataques dirigidos a aprovechar las vulnerabilidades asociadas al sistema operativo detectado. Esta defensa se complementa con la de "TCP Flags Check".

Tabla 11.15: Tipos de tráfico mal formado soportados

No bloquear intrusiones desde las siguientes IPs:

Permite excluir determinadas direcciones IP y/o rangos de IPs de las detecciones realizadas por el firewall.

Control de dispositivos (Equipos Windows)

Dispositivos de uso común como llaves USB, unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles son una vía de infección muy común para los equipos de la red.

Control de dispositivos define el comportamiento del equipo protegido al conectar u operar con un dispositivo extraíble o de almacenamiento masivo. Para ello, hay que seleccionar el dispositivo o dispositivos autorizados y asignar un nivel de utilización.

Activar el control de dispositivos

- Marca la casilla **Activar control de dispositivos.**
- Elige en el desplegable correspondiente el nivel de autorización a aplicar para el tipo de dispositivo a limitar su uso.
    - En el caso de las llaves USB y las unidades CD/DVD elige entre **Bloquear**, **Permitir lectura** o **Permitir lectura y escritura**.
    - Para Bluetooth, dispositivos de imágenes, módems USB y teléfono móviles las opciones son **Permitir y Bloquear**.

Dispositivos permitidos

Gestiona mediante una lista blanca aquellos dispositivos individuales que sí están permitidos cuando toda su familia esté bloqueada:

- Haz clic en icono ⊕ de **Equipos permitidos** para mostrar un listado con todos los dispositivos conectados a los equipos del parque informático.

- Elige aquellos que quieras excluir del bloqueo general previamente configurado.
- Borra con el botón exclusiones ya creadas.

Exportar e importar listas de dispositivos permitidos

Despliega las opciones de **Exportar** e **Importar** del menú de contexto ⋮.

Obtener el identificador único del dispositivo

Para gestionar dispositivos sin esperar a que el usuario los conecte a su equipo o para poder excluirlos de forma manual, es necesario obtener el identificador de estos dispositivos:

- En el Administrador de dispositivos de Windows selecciona el dispositivo del que se va a obtener el identificador. Haz clic con el botón derecho del ratón sobre el nombre del dispositivo y accede a **Propiedades**.
- Accede a la pestaña **Detalles**.
- En el desplegable **Propiedad** selecciona **Ruta de acceso a la instancia del dispositivo**. En el campo **Valor**, se encuentra el identificador único del dispositivo.

En el supuesto de que no se muestre ningún valor Ruta de acceso a instancia del dispositivo, no será posible obtener el identificador del dispositivo. En este caso puedes utilizar como identificador el correspondiente al hardware del dispositivo:

- En el desplegable **Propiedad**, selecciona **Identificador de hardware** y se mostrará el identificador correspondiente.

Este identificador no identifica de forma única a cada dispositivo, sino que representa a todos los dispositivos de la misma gama.

Apunta todos los identificadores de dispositivo en un fichero de texto según se indica en **Exportar e importar listas de dispositivos permitidos**.

Cambio de nombre de los dispositivos

El nombre asignado por Panda Endpoint Protection a los dispositivo del equipo puede llevar en ocasiones a confusión, o a impedir al administrador identificarlos correctamente. Para solucionar este problema es posible asignar nombres personalizados a los dispositivos:

- En la sección **Dispositivos permitidos** selecciona el dispositivo a cambiar de nombre.
- Haz clic en el icono . Se mostrará una ventana donde introducir el nuevo nombre del dispositivo.

- Haz clic en el botón **Aceptar**. La lista **Dispositivos permitidos** se actualizará con el nuevo nombre.

Capítulo 12

Configuración de seguridad para dispositivos móviles

Panda Endpoint Protection centraliza en el menú superior **Configuración** toda la configuración de los parámetros de seguridad para smartphones y tablets. Haz clic en el menú lateral **Dispositivos móviles** para mostrar un listado con todas las configuraciones de seguridad ya creadas o para crear nuevas.

A continuación se muestran todos los parámetros incluidos en la configuración de seguridad y antirrobo para dispositivos moviles, y se indican algunas recomendaciones prácticas para asegurar móviles y tablets y reducir los inconvenientes en su manejo al usuario.

*Para obtener información adicional sobre los distintos apartados del módulo **Dispositivos móviles**, consulta las referencias siguientes:*

***Crear y gestionar configuraciones** en la página **285**: información para crear, modificar, borrar o asignar configuraciones a los equipos de la red.*

***Acceso, control y supervisión de la consola de administración** en la página **53**: gestión de cuentas de usuario y asignación de permisos.*

Contenido del capítulo

Configuración de Dispositivos Android

Acceso a la configuración

- Selecciona el menú superior **Configuración**.
- Selecciona el menú lateral **Dispositivos moviles**.
- En el menú de pestañas **Dispositivos Android**, haz clic en el botón **Añadir**. Se abrirá la ventana de configuración de dispositivos Android.

Permisos requeridos

Permiso	Tipo de acceso
Configurar seguridad para dispositivos móviles	Crear, modificar, borrar, copiar o asignar las configuraciones de dispositivos móviles.
Ver configuraciones de seguridad para dispositivos moviles	Visualizar las configuraciones de dispositivos móviles.
Utilizar la protección antirrobo para dispositivos móviles	Enviar acciones a los dispositivos móviles para evitar la filtración de datos, localizarlos en caso de pérdida o robo y bloquearlos.

Tabla 12.1: Permisos requeridos para acceder a la configuración Dispositivos Android

Actualización

Establece el tipo de conexión que utilizará el dispositivo para descargar las actualizaciones de la nube de Panda Security.

La configuración de las actualizaciones se describe en ***Actualización del producto*** *en la página* ***201****.*

Antivirus

La protección antivirus para dispositivos móviles Android, analiza bajo demanda o de forma permanente tanto el dispositivo como las tarjetas de memoria SD conectadas a él. También protege frente a la instalación en el dispositivo de aplicaciones de origen desconocido que puedan contener malware y PUPs.

Para activar la protección antivirus y el análisis de aplicaciones de origen desconocido, utiliza los controles deslizantes.

Exclusiones

Excluye del análisis las aplicaciones instaladas. Escribe los nombres de los paquetes a excluir separados por el carácter ",".

Para localizar el nombre del paquete correspondiente a una aplicación instalada, búscala en Google Play. En la URL de su ficha se mostrará el parámetro `'?id='`, que contiene la cadena que identifica de forma única a la aplicación.

Antirrobo

La configuración antirrobo permite enviar acciones a los dispositivos móviles Android para evitar la filtración de los datos que contienen, o favorecer su localización en caso de pérdida o robo del terminal.

Acceder a la protección antirrobo

- Selecciona el menú superior **Configuración** y el menú lateral **Dispositivos móviles**.
- En el menú de pestañas superior, selecciona **Dispositivos Android**. Se mostrará un listado de configuraciones ya creadas.
- Para crear una configuración nueva, haz clic en el botón **Añadir**. Se abrirá la ventana **Añadir configuración**.
- Para modificar una configuración existente, haz clic en la configuración. Se abrirá la ventana **Añadir configuración**.
- Haz clic en la sección **Antirrobo** y activa o desactiva la funcionalidad con el control deslizante.
- Haz clic en el botón **Guardar**.

Para obtener información sobre las acciones antirrobo disponibles en Panda Endpoint Protection, consulta ***Sección general en dispositivos móviles*** *en la página* ***253****.*

Configurar la protección antirrobo

Campo	Descripción
Informar de la localización del dispositivo	El dispositivo envía sus coordenadas GPS al servidor Panda Endpoint Protection. Para activarlo o desactivarlo, utiliza el control deslizante.

Campo	Descripción
Sacar foto al tercer intento de desbloqueo y enviarla por email	Si el usuario del dispositivo falla tres veces consecutivas al desbloquearlo, se tomará una fotografía y se enviará por correo electrónico a las direcciones de correo separadas por coma introducidas en la caja de texto. Para activarlo o desactivarlo, utiliza el control deslizante.
Privacidad	Permite al usuario activar el modo privado, lo que impide el registro de las coordenadas GPS y su posterior envío al servidor Panda Endpoint Protection. Para activarlo o desactivarlo, utiliza el control deslizante.

Tabla 12.2: Funcionalidades antirrobo de dispositivos Android

Configuración de dispositivos iOS

Acceso a la configuración

- Selecciona el menú superior **Configuración.**
- Selecciona el menú lateral **Dispositivos móviles.**
- En el menú de pestañas **Dispositivos iOS**, haz clic en el botón **Añadir**. Se abrirá la ventana de configuración de dispositivos iOS.

Permisos requeridos

Permiso	Tipo de acceso
Configurar seguridad para dispositivos móviles	Crear, modificar, borrar, copiar o asignar las configuraciones de dispositivos iOS
Ver configuraciones de seguridad para dispositivos móviles	Visualizar las configuraciones de dispositivos iOS
Utilizar la protección antirrobo para dispositivos móviles	Enviar acciones a los dispositivos para evitar la filtración de datos, localizarlos en caso de pérdida o robo, y bloquearlos.

Tabla 12.3: Permisos requeridos para acceder a la configuración Dispositivos iOS

Antivirus para navegadores web

La protección antivirus para dispositivos iOS, analiza las URLs a las que se conecta el dispositivo para evitar la instalación en él de aplicaciones que contengan malware o phishing.

Para activar la detección de URLs de malware y phishing, utiliza los controles deslizantes.

Esta funcionalidad no está disponible para dispositivos iOS no integrados en un MDM. Consulta ***Instalación en sistemas iOS*** *en la página* ***149****.*

Exclusiones

Es posible excluir del análisis determinadas URLs y dominios. Utiliza la caja de texto para escribir las URL y dominios que quieres excluir.

Antirrobo

La configuración antirrobo permite enviar acciones a los dispositivos iOS para evitar la filtración de los datos que contienen o favorecer su localización en caso de pérdida o robo del terminal.

Acceder a la protección antirrobo

- Selecciona el menú superior **Configuración** y el menú lateral **Dispositivos móviles**.
- En el menú de pestañas superior, selecciona **Dispositivos iOS**. Se mostrará un listado de configuraciones ya creadas.
- Para crear una configuración nueva, haz clic en el botón **Añadir**. Se abrirá la ventana **Añadir configuración**.
- Para modificar una configuración existente, haz clic en la configuración. Se abrirá la ventana **Añadir configuración**.
- Haz clic en la sección **Antirrobo** y activa o desactiva la funcionalidad con el control deslizante.
- Haz clic en el botón **Guardar**.

Consulta ***Sección general en dispositivos móviles*** *en la página* ***253*** *para obtener información sobre las acciones antirrobo disponibles en Panda Endpoint Protection.*

Configurar la protección antirrobo

Campo	Descripción
Comportamiento	El dispositivo envía sus coordenadas GPS al servidor Panda Endpoint Protection Para activarlo o desactivarlo, utiliza el control deslizante.
Privacidad	Permite al usuario activar el modo privado, lo que impide el registro de las coordenadas GPS y su posterior envío al servidor Panda Endpoint Protection. Para activarlo o desactivarlo, utiliza el control deslizante.

Tabla 12.4: Funcionalidades antirrobo de dispositivos iOS

Capítulo 13

Panda Patch Management (Actualización de programas vulnerables)

Panda Patch Management es un módulo integrado en la plataforma Aether que localiza los equipos de la red que contienen software con vulnerabilidades conocidas, y los actualiza de forma automática y centralizada. De esta forma minimiza la superficie de ataque, evitando que el malware aproveche fallos del software instalado en los equipos de los usuarios y servidores para infectarlos.

Panda Patch Management es compatible con sistemas operativos Windows, macOS y Linux y detecta aplicaciones de terceros pendientes de actualizar o en EoL (End of Life), así como los parches y actualizaciones publicados por Microsoft para todos sus productos (sistemas operativos, bases de datos, suites ofimáticas, etc.).

Para más información sobre los proveedores y aplicaciones incluidas en Patch Management, consulta ***https://info.pandasecurity.com/patchmanagementapp/?type=windows***

Para obtener información adicional sobre los distintos apartados del módulo Panda Patch Management consulta las referencias siguientes:

***Crear y gestionar configuraciones** en la página **285**: información sobre cómo crear, modificar, borrar o asignar configuraciones a los equipos de la red.*

***Acceso, control y supervisión de la consola de administración** en la página **53**: gestión de cuentas de usuario y asignación de permisos.*

***Gestión de listados** en la página **42**: información sobre cómo gestionar listados.*

Contenido del capítulo

Funcionalidades de Panda Patch Management

Toda la funcionalidad de Panda Patch Management se concentra en los puntos de la consola de administración mostrados a continuación:

- **Configuración del descubrimiento de parches a aplicar**: a través del perfil de configuración **Gestión de parches**, accesible desde el panel lateral en el menú superior **Configuración.** Consulta **Configuración del descubrimiento de parches sin aplicar** para más información.
- **Configuración de las exclusiones de parches**: desde el listado **Parches disponibles**. Consulta **Excluir parches en todos o en algunos equipos**para más información.
- **Visibilidad del estado de actualización del parque IT**: mediante widgets en un panel de control independiente, accesible desde el menú superior **Estado**, panel lateral **Patch Management**. Consulta **Estado de gestión de parches** para más información.
- **Listados de parches pendientes de aplicar**: desde los listados **Estado de gestión de parches**, **Parches disponibles** y **Programas "End of Life"** accesibles desde el menú superior **Estado**, panel lateral **Mis listados, Añadir**. Consulta **Listados del módulo Panda Patch Management** para más información.

- **Histórico de parches instalados**: desde el listado **Historial de instalaciones**, accesible desde el menú superior **Estado**, panel lateral **Mis listados, Añadir**. Consulta **Historial de instalaciones** para más información.
- **Parcheo de equipos**: desde el menú superior **Tareas** y creando una tarea programada de tipo **Instalar parches**. También se pueden parchear los equipos desde los menús de contexto del árbol de grupos en el menú superior **Equipos,** de los listados y desde **Detalle de equipo**. Consulta **Descargar e instalar parches** para más información.
- **Excluir equipos de las tareas de instalación de parches**. Es posible excluir equipos o grupos de equipos a la hora de ejecutar tareas de instalación de parches. La exclusión de equipos de las tareas de instalación de parches es una funcionalidad dirigida a los partners que utilizan Panda Partner Center y que gestionan a varios clientes con una única consola de administración Panda Partner Center.

  Para más información, consulta el capítulo **Configuraciones para los productos de seguridad** de la **guía de administración de Panda Partner Center**.
- **Parcheo de equipos de prueba**: al configurar Patch Management es posible designar equipos de prueba en los que instalar parches y comprobar los resultados de la instalación antes de aplicar los parches al resto de equipos de la red. Para designar equipos de pruebas:
  - Crea una configuración de Panda Patch Management, selecciona la opción **Designar como equipos de prueba e instalar parches** en el desplegable **Instalación de parches** y asígnala a los equipos de prueba. Para más información consulta **Instalación de parches**.
  - Crea una tarea de Panda Patch Management y activa el selector **Ejecutar la tarea sólo en equipos de prueba**. Para más información consulta **Configuración de una tarea de instalación de parches**.
- **Desinstalación de parches**: elige una de las opciones siguientes:
  - Desde el widget **Últimas tareas de instalación de parches**, haz clic en el link **Ver historial de instalaciones**. Consulta **Últimas tareas de instalación de parches** para más información.
  - Desde el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado **Historial de instalaciones**. Consulta **Historial de instalaciones** para más información.
  - Desde en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en **Ver parches instalados**.
- Al hacer clic en el parche se muestra su información asociada y el botón **Desinstalar** si es compatible con su desinstalación. Consulta **Desinstalar un parche ya instalado** para más información.

Requisitos mínimos de Panda Patch Management

Versiones de sistemas operativos Windows compatibles

Estaciones

- Windows 7 (32 y 64 bits)
- Windows 8 (32 y 64 bits)
- Windows 8.1 (32 y 64 bits)
- Windows 10 (32 y 64 bits)
- Windows 11 (64 bits)

Servidores

- Windows 2008 (32 y 64 bits) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 y 2016
- Windows Server 2022

Comportamiento en equipos Windows no compatibles

Para equipos no compatibles con Panda Patch Management, el comportamiento será el siguiente:

- No se instalará en ellos Panda Patch Management
- Los equipos conservarán las configuraciones y tareas de Panda Patch Management que tenían asignadas, pero no les serán aplicadas.
- En el listado **Parches disponibles** no se incluirá información sobre estos equipos ni el estado de los parches instalados.
- Los equipos no computarán a los efectos de licencias consumidas de Panda Patch Management
- En el historial de instalaciones, las instalaciones anteriores de Panda Patch Management se mostrarán como **No disponible**.

Versiones de sistemas operativos macOS compatibles

- macOS 10.15 Catalina
- macOS 11 Big Sur

- macOS 12 Monterey
- macOS Ventura.
- macOS Sonoma

Instalación de parches de sistema operativo en equipos macOS con arquitectura Apple

Para instalar parches de sistema operativo en estos equipos, se solicitará al usuario sus credenciales, con un límite de tres intentos. Una vez instalado el parche, el equipo se reiniciará automáticamente.

Si en la tarea de instalación existen otros parches que no necesitan credenciales, su instalación se llevará a cabo con normalidad. Consulta **Instalación de parches de sistema operativo en equipos macOS** .

Versiones de sistemas operativos Linux compatibles

Distribuciones de 64 bits compatibles:

- **Red Hat**: 7.0, 8.0
- **CentOS**: 7.0
- **SuSE Linux Enterprise**: 12, 15.

- **Red Hat**: Versión 7.0 y superiores; 8.0 y superiores.
- **CentOS**: Versión 7.0 y superiores.
- **SuSE Linux Enterprise**: Versión 12.0 y superiores; 15.0 y superiores.

Para una correcta instalación de los parches, es necesario que la configuración del repositorio del equipo no haya sido modificada y apunte a los servidores del proveedor de la distribución.

URLs necesarias

- **https://content.ivanti.com**
- **https://application.ivanti.com**
- **https://stlicense.ivanti.com**
- **https://help.ivanti.com**
- **https://license.shavlik.com**

Flujo general de trabajo

Panda Patch Management es una herramienta integral que gestiona el parcheo y actualización de los sistemas operativos y programas instalados en los equipos de la red. Para conseguir reducir de forma eficiente la superficie de ataque de los equipos, es necesario seguir los pasos mostrados a continuación:

- Comprobar que Panda Patch Management funciona correctamente en los equipos instalados.
- Comprobar que los parches publicados están instalados.
- Instalar los parches seleccionados.
- Desinstalación (Rollback) de los parches que muestran un mal funcionamiento.
- Excluir parches en todos o en algunos equipos.
- Comprobar que los programas instalados en los equipos no han entrado en EoL.
- Comprobar puntualmente el histórico de instalaciones de parches y actualizaciones.
- Comprobar puntualmente el estado del parcheo de equipos con incidencias.

Comprobar que Panda Patch Management funciona correctamente

Sigue los pasos mostrados a continuación:

- Comprueba que los equipos de la red tienen una licencia asignada de Panda Patch Management y que el módulo está instalado y en funcionamiento. Utiliza el widget **Estado de gestión de parches**
- Comprueba que los equipos con una licencia de Panda Patch Management asignada se comunican con la nube de Panda Security. Utiliza el widget **Tiempo desde la última comprobación**
- Comprueba que los equipos donde se instalarán los parches tienen el servicio Windows Update en ejecución con las actualizaciones automáticas desactivadas.

*Activa la configuración **Desactivar Windows Update en los equipos** en el perfil de configuración de Gestión de parches para que Panda Endpoint Protection pueda gestionar correctamente el servicio. Para más información, consulta **Configuración general**.*

*En el caso de Windows 10 y posteriores, el sistema operativo permite posponer las actualizaciones de parches de calidad pero no desactivarlas, por lo que estas actualizaciones se lanzarán transcurridos 30 días aunque la configuración **Desactivar Windows Update en los equipos** esté activada.*

Comprobar que los parches publicados están instalados

Los parches y actualizaciones se publican de forma constante según los proveedores del software instalado en la red detectan vulnerabilidades y las corrigen. Estos parches tienen asociada una criticidad y un tipo.

- Para obtener una visión general de los parches pendientes de instalar según su tipo y criticidad utiliza el widget **Criticidad de los parches**
- Para ver los parches pendientes de instalación en un equipo o grupo de equipos:
    - En el árbol de equipos (menú superior **Equipos**, pestaña **Carpeta** en el panel lateral) haz clic en el menú de contexto de un grupo y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el grupo.

  ó

    - En el panel de equipos (menú superior **Equipos**, panel derecho) haz clic en el menú de contexto de un equipo y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.
- Para obtener una visión global detallada de los parches pendientes de instalar:
    - En el menú superior **Estado** haz clic en el panel lateral **Mis listados, Añadir** y selecciona el listado **Parches disponibles**.
    - Utiliza la herramienta de filtrado para acotar la búsqueda.
- Para buscar los equipos que no tienen instalado un parche concreto:
    - En el menú superior **Estado** haz clic en el panel lateral **Mis listados**,**Añadir** y selecciona el listado **Parches disponibles**.
    - Utiliza la herramienta de filtrado para acotar la búsqueda.
    - Haz clic en el menú de contexto del equipo – parche a buscar y selecciona el menú **Visualizar equipos** con el parche disponible para su instalación.

Descargar e instalar parches

Para instalar los parches y actualizaciones, Panda Patch Management utiliza la infraestructura de tareas implementada en Panda Endpoint Protection.

Requisitos de funcionamiento

La instalación de parches publicados por Microsoft utiliza el servicio Windows Update en el equipo del usuario o servidor. Sin embargo, para no solapar la actividad de Panda Patch Management con la del servicio Windows Updates, es recomendable que la configuración de éste se establezca de forma que no tenga actividad en el equipo. Consulta **Configuración general**

Permisos necesarios

La cuenta de usuario utilizada para acceder a la consola web tiene que tener asignado el permiso **Instalar, desinstalar y excluir parches** a su rol. Para obtener más información sobre el sistema de permisos consulta **Gestión de roles y permisos** en la página **66**.

Descarga de parches y ahorro de ancho de banda

Antes de la instalación de un parche, es necesaria su descarga desde los servidores del proveedor de software. Esta descarga se produce de forma transparente e independiente en cada equipo cuando se lanza la tarea de instalación. Para minimizar el ancho de banda consumido se puede aprovechar la infraestructura de equipos caché instalada en la red del cliente.

Limitación de la descarga de parches a través de equipos caché y proxy

La descarga de los parches puede realizarse directamente desde Internet o también a través de un equipo caché o proxy de Panda Endpoint Protection. Consulta **Configuración de las descargas mediante equipos caché** en la página **307** y **Configuración de listas de acceso a través de proxy** en la página **305**.

Según el sistema operativo instalado en el equipo, hay limitaciones a la hora de utilizar un método de descarga u otro;

- **Equipos con sistema operativo Windows o macOS**: pueden descargar parches a través de equipos caché e Internet. No pueden descargar parches a través de proxy de Panda Endpoint Protection
- **Equipos con sistema operativo Linux**: utilizan el gestor de paquetes propio de la distribución para hacer la descarga de los parches desde Internet. No pueden descargar parches a través de equipos caché ni proxy de Panda Endpoint Protection.

Los equipos caché almacenan los parches durante un periodo máximo de 30 días, transcurrido el cual se eliminarán. Si un equipo solicita a un equipo caché la descarga de un parche y éste no lo tiene en su repositorio, el equipo solicitante dará un tiempo al equipo caché para que lo descargue. Este tiempo depende del tamaño del parche a descargar. Si no es posible la descarga, el equipo solicitante la iniciará de forma directa.

Una vez aplicados los parches en los equipos, éstos se borrarán del medio de almacenamiento donde residen.

Tipos de tareas de instalación parches

- **Inmediatas (opción Instalar)**: instala el parche en el momento sin necesidad de completar toda la configuración de la tarea, pero no reinicia el equipo del usuario, aunque sea requisito para completar la instalación. Las tareas inmediatas inician la descarga de los parches necesarios en el momento en que éstas se crean, de forma que puede darse un alto consumo de ancho de banda si afectan a muchos equipos, o el volumen de la descarga es alto.
- **Programadas (programar instalación)**: permite configurar todos los parámetros de la actualización de parches. Si varias tareas coinciden en el mismo momento de inicio se introduce un retardo aleatorio de hasta un máximo de 2 minutos para evitar el solapamiento de descargas y minimizar el consumo de ancho de banda.

Interrupción de las tareas de instalación de parches

Las tareas de instalación de parches pueden cancelarse si el proceso de instalación en el equipo no se ha iniciado todavía. Si la instalación ya ha comenzado no se podrá cancelar la tarea, ya que podría causar errores en los equipos.

Envío de parches según el sistema operativo del equipo

Aunque el administrador establezca como destinatario un equipo incompatible con el tipo de parche a instalar, el equipo solo recibirá los parches correspondientes a su sistema operativo.

Instalación de parches de sistema operativo en equipos macOS

Algunos parches de sistema operativo para equipos macOS fuerzan el reinicio del equipo para finalizar su instalación, independientemente de las opciones de reinicio seleccionadas en la configuración de las tareas de instalación de parches.

Estos parches incorporan soluciones, arreglos y mejoras del sistema operativo instalado, pero no suponen la actualización total del mismo a una versión mayor superior. Se distinguen porque incluyen el texto *SoftwareUpdate* en su nombre, visible en la ventana **Parche detectado** y en el listado **Parches disponibles**.

Mensajes de advertencia

Dado que la instalación de estos parches conlleva un reinicio automático imprescindible, el usuario y el administrador son advertidos de ello en los siguientes supuestos:

- Si el administrador selecciona alguno de estos parches en el listado de parches disponibles para crear una tarea rápida o una tarea programada, se mostrará un mensaje de advertencia. Si lo acepta, se lanzará la instalación (tarea rápida) o se accederá a la configuración de la tarea (tarea programada). Consulta **Desde el listado Parches**

disponibles.

- Si el administrador al configurar la tarea selecciona **macOS** en **Instalar parches de los siguientes productos**se mostrará un mensaje advirtiendo del reinicio y preguntando si quiere incluir estos parches en la tarea. Por defecto, esta opción está desactivada. Consulta **Configuración de una tarea de instalación de parches**.
- En los equipos destinatarios de la tarea, se le mostrará al usuario un mensaje advirtiendo de que la instalación está en curso y que implica reinicio.

Instalación en equipos macOS con arquitectura Apple

En el caso de los equipos macOS con arquitectura Apple, para instalar parches de sistema operativo es necesario escribir las credenciales de *Volume Owner*.

- **Si las credenciales son correctas**: en la columna **Instalación** del listado **Parches disponibles** se mostrará **Pendiente de reinicio**. Cuando se complete la instalación del parche, el equipo se reiniciará automáticamente y el parche desaparecerá del listado.
- **Si el usuario cancela la instalación**: el equipo se mostrará junto a un código de error en la ventana de resultado de la tarea. Consulta **Resultados de una tarea** en la página **614**

Si la tarea de instalación para equipos macOS con arquitectura Apple incluye otros parches para cuya instalación no son necesarias credenciales, su instalación se llevará a cabo con normalidad.

Instalación en equipos macOS con arquitectura Intel

En este caso no es necesario escribir credenciales. En el equipo destinatario de la tarea se mostrará un mensaje advirtiendo de que la instalación del parche está en curso y de que cuando finalice se reiniciará el equipo.

Dado que no es posible posponer el reinicio automático, es muy recomendable salvar y cerrar los archivos que se están utilizando.

Acceso a la instalación de parches en la consola

Desde el listado Parches disponibles

- Selecciona el menú superior **Estado**.
- En la sección **Mis listados** del panel lateral, haz clic en **Añadir** y selecciona el listado **Parches disponibles**
- Utiliza las herramientas de filtrado para acotar la búsqueda.

- Selecciona las casillas de los equipos – parches a instalar.
- Para crear una tarea rápida, haz clic en **Instalar** en la barra superior de herramientas. Para crear una tarea programada, haz clic en **Programar instalación**. Para configurar una tarea programada consulta **Configuración de una tarea de instalación de parches**.

*Si entre los parches elegidos para su instalación hay alguno de tipo sistema operativo para macOS que requiera reinicio automático, se mostrará un mensaje advirtiendo de ello. Consulta **Instalación de parches de sistema operativo en equipos macOS***

Desde el listado Parches disponibles por equipo

- Selecciona el menú superior **Estado**.
- En la sección **Mis listados** del panel lateral, haz clic en **Añadir** y selecciona el listado **Parches disponibles por equiposParches disponibles**
- Utiliza las herramientas de filtrado para acotar la búsqueda.
- Haz clic en el menú contextual asociado al parche. Se mostrará el listado **Parches disponibles**. Consulta **Desde el listado Parches disponibles**.

Desde el árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpetas** del árbol de equipos situado en el panel izquierdo.
- Para instalar parches en un grupo de equipos haz clic en el menú de contexto del grupo y selecciona **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles**. Consulta **Desde el listado Parches disponibles**.
- Para programar la instalación de parches en un grupo de equipos haz clic en el menú de contexto del grupo y selecciona **Programar instalación de parches**. Se creará una nueva tarea de instalación de parches. Para configurarla consulta **Configuración de una tarea de instalación de parches**.

Desde el listado del árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpetas** del árbol de equipos situado en el panel izquierdo.
- Selecciona el grupo de equipos y haz clic en las casillas de selección del listado de equipos.
- Para instalar parches, si has seleccionado un solo equipo haz clic en el menú de contexto asociado al equipo y selecciona **Visualizar parches disponibles**. Si has seleccionado varios, haz clic en **Visualizar parches disponibles**en la barra superior de herramientas. Se mostrará el listado **Parches disponibles**. Consulta **Desde el listado Parches disponibles**.

- Para programar la instalación de grupos de parches, si has seleccionado un solo equipo haz clic en el menú de contexto asociado al equipo y selecciona **Programar instalación de parches**. Si has seleccionado varios, haz clic en **Programar instalación de parches** en la barra superior de herramientas. Se creará una nueva tarea de instalación de parches. Para configurarla consulta **Configuración de una tarea de instalación de parches**.

Desde el menú superior Tareas

En el menú superior selecciona **Tareas**, haz clic en **Añadir tarea** y selecciona **Instalar parches**.

Configuración de una tarea de instalación de parches

- Escribe la información general de la tarea en los campos **Nombre** y **Descripción**.
- Si la tarea no tiene destinatarios activados, haz clic en el enlace **Destinatarios** (**No se ha asignado a ningún equipo**) para abrir una ventana nueva donde seleccionar los equipos que recibirán la tarea configurada.

> *Para acceder a la ventana de selección de equipos, es necesario guardar previamente la tarea. Si la tarea no ha sido guardada, se mostrará una ventana de advertencia.*

- Si quieres enviar la tarea de instalación de parches solo a los equipos de prueba que has designado en la red, desplaza el cursor deslizante **Ejecutar la tarea solo en equipos de prueba**. El rol de equipo de prueba se asigna en la configuración de Panda Patch Management asignada al equipo. Consulta **Funcionalidades de Panda Patch Management**.
- Selecciona el tipo de equipos que recibirán la tarea: **Estación**, **Portátil** o **Servidor**.
- Haz clic en el botón para agregar equipos individuales o grupos de equipos, y en el botón para eliminarlos.
- En la ventana **Editar tarea**, haz clic en el botón **Ver equipos** para verificar los equipos que recibirán la tarea.
- Indica la programación horaria de la tarea. Se establece mediante dos parámetros:

- **Empieza**: marca el inicio de la tarea.

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o cuando se encuentre disponible dentro del margen definido en el desplegable **Equipo apagado**.
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Panda Endpoint Protection.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea en función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • **No ejecutar**: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido o no es accesible. • **Dar un margen de**: define un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • **Ejecutar cuando se encienda**: no establece ningún intervalo de tiempo sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 13.1: Comportamiento del inicio de la tarea si el equipo no está disponible

- **Frecuencia**: establece un intervalo de repetición cada día, semana, mes o año tomando como referencia la fecha indicada en el campo **Empieza**:

Valor	Descripción
Ejecución única	La tarea se ejecuta de forma puntual a la hora indicada en el campo **Empieza**.

Valor	Descripción
Diaria	La tarea se ejecuta todos los días a la hora indicada en el campo **Empieza**.
Semanal	Haz clic en las casillas de selección para establecer la ejecución de la tarea en los días de la semana elegidos, a la hora indicada en el campo **Empieza**.
Mensual	Elige una de las opciones: • Ejecutar la tarea un día concreto de cada mes. Si se eligen los días 29, 30 o 31 y el mes no tiene esos días, la tarea se ejecuta el último día del mes. • Ejecutar la tarea el primer, segundo, tercer, cuarto o ultima día de la semana de cada mes.

Tabla 13.2: Configuración de la frecuencia de la tarea

- En **Parches de seguridad** indica el nivel de criticidad de los parches a instalar.
- En **Instalar parches de los siguiente productos**, el árbol de productos aparece ordenado por sistemas operativos. Cada sistema operativo contiene los parches disponibles para él. Indica qué productos recibirán parches utilizando las casillas de selección en el árbol de productos.

> *Si entre los parches elegidos para su instalación hay alguno de tipo sistema operativo para macOS que requiera reinicio automático, se mostrará un mensaje para que selecciones si deseas incluir este tipo de parches en la tarea. Consulta* ***Instalación de parches de sistema operativo en equipos macOS***

Dado que el árbol de productos es un recurso vivo que cambia a lo largo del tiempo, ten en cuenta las siguientes reglas al seleccionar los elementos del árbol:

- Al seleccionar un nodo se marcarán todos sus nodos hijos y sus descendientes. Por ejemplo, al seleccionar Adobe se seleccionarán todos los nodos que quedan por debajo de este nodo.
- Si seleccionas un nodo y posteriormente Panda Patch Management agrega de forma automática un nuevo nodo hijo en la rama seleccionada, este nodo también quedará seleccionado de forma automática. Por ejemplo, si seleccionas el nodo Adobe se seleccionarán todos sus nodos hijos, y si posteriormente dentro de Adobe

Panda Patch Management agrega un nuevo nodo (un nuevo programa o familia de programas), éste quedará seleccionado de forma automática. Por el contrario, si se seleccionan manualmente algunos nodos hijo individuales de Adobe y Panda Patch Management añade un nuevo nodo hijo, éste no se seleccionará de forma automática.

- Los programas a parchear se evalúan en el momento en que se ejecuta la tarea, no en el momento de su creación o configuración. Esto implica que si Panda Patch Management agrega una nueva entrada en el árbol después de que el administrador haya configurado una tarea de parcheo, y esta entrada es seleccionada de forma automática según la regla del punto anterior, se instalarán los parches asociados a ese nuevo programa en el momento en que se ejecute la tarea.

- Establece las opciones de reinicio en el caso de que sea un requisito reiniciar el puesto de trabajo o servidor para completar la instalación del parche:

  - **No reiniciar automáticamente**: al terminar la tarea de instalación de parches se le muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora** y **Recordar más tarde**. En caso de elegir ésta última, se volverá a mostrar a las 24 horas siguientes.

    A los equipos con sistema operativo Linux sin entorno gráfico, se les enviará un mensaje informando de la necesidad de reiniciar para completar la instalación del parche.

  - **Reiniciar automáticamente solo las estaciones de trabajo**: elige el intervalo en el que se reiniciarán los equipos de tipo estación de trabajo. Al cumplirse el tiempo establecido, el agente mostrará al usuario del equipo una ventana de aviso con el botón **Reiniciar ahora** y una cuenta atrás indicando el tiempo restante para el reinicio.

    A los equipos con sistema operativo Linux sin entorno gráfico, se les enviará un mensaje concretando el tiempo restante para el reinicio.

    Conforme el momento de reinicio se vaya acercando, el usuario dejará de poder cerrar la ventana de aviso. Cada 30 minutos, la pantalla se mostrará en primer plano para recordarle al usuario la necesidad del reinicio. Cuando la cuenta atrás se haya completado, el equipo se reiniciará automáticamente.

- **Reiniciar automáticamente solo los servidores**: el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica solo a equipos de tipo servidor.
- **Reiniciar automáticamente tanto las estaciones de trabajo como los servidores**: el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica tanto a estaciones de trabajo como a servidores.

- Haz clic en **Guardar**. La tarea aparecerá en el listado de tareas configuradas, pero mostrará la etiqueta **Sin publicar**, indicando que no está activa.
- Haz clic en el enlace **Publicar** para introducir la tarea en el programador de Panda Endpoint Protection, encargado de marcar el momento en que se lanzan las tareas según su configuración.

Cuando dos o más tareas de instalación de parches que requieren reinicio se solapan en el tiempo, Panda Endpoint Protection sigue la estrategia de reiniciar el equipo cuando así lo indique la tarea que tenga establecido el intervalo de reinicio más cercano en el tiempo. De esta forma se evita posponer el reinicio del equipo indefinidamente si se encadenan sucesivas tareas de instalación de parches.

Conversión automática de la frecuencia de ejecución e intervalo de reinicio

Las versiones anteriores de Panda Endpoint Protection que no soporten la característica de determinar el intervalo de reinicio, lo establecen de forma automática en 4 horas.

Si alguno de los equipos del parque informático tiene instalada una versión anterior del software de seguridad, es posible que no sea capaz de interpretar correctamente las configuraciones de frecuencia establecidas por el administrador en la consola web. En este caso, cada equipo establecerá las siguientes correspondencias para la configuración de la frecuencia en las tareas a ejecutar:

- **Tareas diarias**: sin cambios.
- **Tareas semanales**: se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 7 días.
- **Tareas mensuales**: se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 30 días.

Descargar los parches de forma manual

En algunos casos Panda Patch Management no puede obtener una URL de descarga para iniciar la instalación del parche de forma automática. El motivo de este escenario es diverso:

- El parche puede ser de pago, o no ser un parche público y requerir el registro previo del usuario, entre otras razones.
- Los parches protegidos por EULAs no pueden ser descargados y redistribuidos por Panda Security

En estos casos Panda Patch Managementmostrará un enlace que el administrador podrá tomar como referencia para localizar la descarga del parche. Si el enlace no resulta de utilidad será necesario contactar con el proveedor del software a parchear. Para obtener más información consulta **https://www.pandasecurity.com/es/support/card?id=700111.**

Panda Patch Management implementa un mecanismo mediante el cual integra estas descargas manuales en la consola web para que el administrador pueda añadir los parches descargados manualmente.

Los sistemas operativos Linux y macOS no so compatibles con el procedimiento de descarga manual de parches.

Para añadir un parche de forma manual al repositorio es necesario disponer la URL de descarga del parche proporcionada por el proveedor del producto a actualizar. Una vez tengas la URL sigue los pasos mostrados a continuación:

- Identifica los parches que requieren una descarga manual.
- Obtén la URL de descarga del proveedor.
- Integra el parche descargado en el repositorio de parches.
- Habilita el parche descargado para su instalación.
- Opcional: deshabilita un parche ya habilitado para su instalación

Identifica los parches que requieren una descarga manual

- Desde el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una lista con todos los listados disponibles.
- Elige el listado **Parches disponibles** y configura los siguientes filtros:
    - **Instalación**: Requiere descarga manual.
    - **Mostrar parches no descargables**: Si.
- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches reportados por Panda Patch Management como necesarios para actualizar los equipos de la red y que no son descargables de forma automática.

Obtén la URL de descarga

- Con el listado de parches no descargables que se indica en **Identifica los parches que requieren una descarga manual** haz clic en un parche concreto. Se mostrarán los detalles del parche.
- Haz clic en el campo **URL de descarga** para iniciar la descarga del parche y guarda el nombre del fichero que aparece en el campo **Nombre del archivo**.

Integra el parche descargado en el repositorio de parches

- Localiza en la red un equipo con Panda Endpoint Protection instalado y el rol de caché asignado y copia el fichero descargado en la ruta siguiente:

```
c:\Programdata\Panda Security\Panda Aether
Agent\Repository\ManuallyDeploy.
```

Si la unidad de almacenamiento del equipo ha cambiado a otra diferente de la establecida por defecto en el proceso de instalación del software Panda Endpoint Protection, accede a la siguiente ruta:
`x:\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy`
Siendo x la unidad donde reside el repositorio del equipo. Consulta ***Establecer la unidad de almacenamiento*** *en la página* ***303*** *para mas información.*

- Si la carpeta **ManuallyDeploy** no existe, créala con permisos de administrador para lectura y escritura.
- Si es necesario, renombra el parche recién copiado con el nombre obtenido en el campo **Nombre de archivo** indicado en **Obtén la URL de descarga**.

Habilita el parche descargado para su instalación

- Una vez copiado el parche en el repositorio vuelve al listado **Parches disponibles** y haz clic en el menú de contexto asociado al parche descargado manualmente.
- Elige la opción **Marcar como descargado manualmente** del menú desplegable. A partir de este momento el parche pasará del estado previo **Requiere descarga manual** al estado **Pendiente (descargado manualmente)** para todos los equipos que requieran su instalación. Una vez en estado **Pendiente (descargado manualmente)** se habilitarán todas las opciones necesarias en el menú de contexto del parche para poder instalarse de la

misma forma que un parche descargado automáticamente. Consulta **Descargar e instalar parches** para más información.

Panda Patch Management no comprueba que un parche en estado Pendiente (descargado manualmente) realmente exista en algún equipo con el rol de caché asignado. De igual manera, tampoco comprueba que todos los equipos de la red que deberían recibir el parche tienen asignado un equipo caché con el parche copiado en su repositorio. Es responsabilidad del administrador asegurarse de que los equipos caché que se utilizarán en la descarga de parches tienen en la carpeta ManuallyDeploy los parches necesarios descargables de forma manual.

Deshabilita un parche para su instalación

Para retirar del repositorio un parche previamente integrado sigue los pasos mostrados a continuación:

- En el listado **Parches disponibles** configura un filtro de las siguientes características:
  - **Instalación**: Pendiente (descargado manualmente).
  - **Mostrar parches no descargables**: Si.
- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches descargados de forma manual y habilitados para su instalación.
- Haz clic en el menú de contexto asociado al parche habilitado para su instalación y elige la opción **Marcar como "Requiere descarga manual"** . A partir de este momento el parche dejará de pertenecer al repositorio de parche instalables y perderá las opciones de su menú de contexto.

Desinstalar los parches defectuosos

En alguna ocasión puede suceder que los parches publicados por los proveedores del software no funcionen correctamente. Aunque se recomienda seleccionar un reducido grupo de equipos de prueba previo al despliegue en toda la red, Panda Patch Management también soporta la desinstalación de parches (Rollback).

La desinstalación de parches no es compatible con Linux y macOS.

Requisitos para desinstalar un parche instalado

- El rol del administrador tiene el permiso **Instalar / desinstalar** parche habilitado. Consulta **Instalar / desinstalar y excluir parches** en la página **74** para obtener más información.
- La instalación del parche a desinstalar finalizó completamente.
- El parche se puede desinstalar. No todos los parches soportan esta funcionalidad.

Desinstalar un parche ya instalado

- Accede a la pantalla de desinstalación del parche:
  - En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona **Historial de instalaciones**.
  - Accede al listado de parches instalados en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en el link **Ver parches instalados**, situado en la parte superior derecha de la ventana de la tarea.
  - Accede al widget **Últimas tareas de instalación de parches** el menú superior **Estado**, menú lateral **Patch Management** y haz clic en el link **Historial de instalaciones**.
- Selecciona de la lista el parche a desinstalar.
- Si el parche se puede desinstalar, se mostrará el botón **Desinstalar el parche**. Haz clic en el botón para mostrar la ventana de selección de equipos:
  - Selecciona **Desinstalar en todos los equipos** para eliminar el parche de todos los equipos de la red.
  - Selecciona **Desinstalar solo en…** para eliminar el parche del equipo indicado.
- Panda Patch Management creará una tarea de ejecución inmediata que desinstalará el parche.
- Si el parche requiere el reinicio del equipo de usuario para completar su desinstalación, se esperará a que el usuario lo reinicie de forma manual.

*Un parche desinstalado volverá a mostrarse en los listados de parches disponibles a no ser que haya sido excluido. Si has configurado una tarea programada de instalación de parches y el parche no ha sido excluido, éste se volverá a instalar en su próxima ejecución. Si el parche ha sido retirado por el proveedor, no se volverá a mostrar ni a instalar. Consulta **Excluir parches en todos o en algunos equipos**para más información.*

Comprobar el resultado de las tareas de instalación / desinstalación de parches

Para consultar las tareas de instalación / desinstalación, haz clic en el menú superior **Tareas** se puede consultar aquellas que han instalado o desinstalado parches en los equipos. Ambas ofrecen la posibilidad de Ver resultados para ver en detalle sobre qué equipos se ha realizado cada una de las acciones y qué parches se han instalado/desinstalado. Consulta **Resultados tarea de instalación / desinstalación de parches** y **Ver parches instalados / desinstalados** para más información.

Excluir parches en todos o en algunos equipos

Para evitar la instalación de los parches que han tenido un mal funcionamiento o que cambian de forma importante las características del programa que los recibe, el administrador de la red puede excluirlos a discreción. Para ello sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Estado** y en el panel lateral **Añadir** en la zona **Mis listados**. Elige el listado **Parches disponibles**. Este listado muestra una linea por cada par equipo - parche disponible. Un parche disponible es aquel que no ha sido instalado en algún equipo de la red o que ha sido desinstalado.
- Para excluir un único parche haz clic en el menú de contexto asociado al parche y elige la opción **Excluir**. Se mostrará una ventana emergente para seleccionar el tipo de exclusión.
    - **Excluir solo para el equipo X**: excluye el parche elegido en el equipo indicado en el listado.
    - **Excluir para todos los equipos**: el parche elegido se excluirá de todos los equipos de la red.
- Para excluir varios parches y/o un único parche de varios equipos selecciónalos con las casillas de selección, haz clic en la barra de acciones y elige la opción **Excluir**. Se mostrará una ventana emergente para seleccionar el tipo de exclusión:
    - **Excluir solo para los equipos seleccionados**: excluye los parches elegidos en los equipos indicados en el listado.
    - **Excluir para todos los equipos**: los parches elegidos se excluirán de todos los equipos de la red.

Los parches excluidos hacen referencia a una versión concreta del parche, de forma que si se excluye un determinado parche y posteriormente el proveedor del software publica otro posterior, éste último no se excluirá automáticamente.

Comprobar que los programas no han entrado en EoL

Los programas que han entrado en EoL no reciben ningún tipo de actualización por parte de los proveedores de software, de forma que se recomienda sustituirlos por alternativas equivalentes o por versiones más avanzadas.

Para localizar los programas actualmente en EOL o que entrarán en EOL en breve:

- Haz clic en el menú superior **Estado**, panel lateral **Patch Management**:
- En el widget **Programas "End of life"**se muestra la información dividida en tres series:
    - **Actualmente en EOL** : programas instalados en la red que ya no reciben actualizaciones de sus respectivos proveedores.
    - **Actualmente o en 1 año en EOL**: programas instalados en la red que ya están en EOL o que entrarán en EOL en el plazo de un año.
    - **Con fecha EOL conocida**: programas instalados en la red que tienen fecha EOL conocida.

Para localizar todos los programas con información de EOL conocida:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir.**
- Selecciona el **Programas "End of Life"**

El listado contiene una entrada por cada par equipo – programa en EoL.

Comprobar el histórico de instalaciones de parches y actualizaciones

Para determinar si un parche concreto está instalado en los equipos de la red:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir.**
- Selecciona **Historial de instalaciones**.

El listado contiene una entrada por cada par equipo – parche instalado, junto con información sobre su nombre, versión, programa o sistema operativo al que afecta y criticidad / tipo del parche.

Al hacer clic en el menú de contexto de un equipo se muestran las opciones que permiten:

- Ver tareas asociadas a la instalación o desinstalación del parche.
- Ver todos los parches instalados en el equipo.
- Ver todos los equipos que tienen instalados el parche elegido.

Comprobar el nivel de parcheo de los equipos con incidencias

Panda Patch Management relaciona los equipos que tienen incidencias detectadas con su nivel de parcheo, deforma que es posible determinar si un equipo infectado o con amenazas detectadas tiene o no aplicados todos los parches que se han publicado.

Para comprobar si un equipo con una incidencia detectada tiene parches pendientes de instalación:

- En el menú superior **Estado**, widget **Amenazas detectadas por el antivirus** haz clic en una amenaza - equipo. Se mostrará la información de la amenaza detectada en el equipo.
- En la sección **Equipo afectado** haz clic en el botón **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.
- Selecciona todos los parches disponibles para este equipo y haz clic en la barra de acciones **Instalar** para crear una tarea inmediata que parcheará el equipo.

*Debido a que este proceso puede implicar descargas de parches desde los servidores del proveedor del software a parchear, y por lo tanto retrasar su aplicación en el tiempo, se recomienda aislar el equipo de la red si el equipo ha sido infectado y muestra tráfico de red en su ciclo de vida. De esta forma se minimiza el riesgo de propagación de la infección en la red del cliente mientras el proceso de parcheo se completa. Consulta **Análisis forense** para obtener más información acerca del ciclo de vida del malware y **Aislar uno o varios equipos de la red de la organización** para más información.*

Configuración del descubrimiento de parches sin aplicar

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Gestión de parches**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Gestión de parches	Crear, modificar, borrar, copiar o asignar las configuraciones de Gestión de parches.

Permiso	Tipo de acceso
Ver configuraciones de parches	Visualizar las configuraciones de Gestión de parches.

Tabla 13.3: Permisos requeridos para acceder a la configuración Gestión de parches

Configuración general

- Escribe el nombre y la descripción para la configuración.
- Para que Panda Patch Management gestione las actualizaciones de forma exclusiva y sin interferencias con la configuración local de Windows Update, haz clic en **Desactivar Windows Update en los equipos**.

> *En el caso de Windows 10 y posteriores, el sistema operativo permite posponer las actualizaciones de parches de calidad pero no desactivarlas, por lo que estas actualizaciones se lanzarán transcurridos 30 días aunque la configuración* ***Desactivar Windows Update en los equipos*** *esté activada.*

- Haz clic en el botón **Guardar**.
- En la lista de configuraciones, haz clic en la configuración que has creado. Se mostrara la ventana **Editar configuración**. Para seleccionar los equipos a los que se asignará la configuración, haz clic en el enlace **Destinatarios (No se ha asignado a ningún equipo)**.
- Para agregar equipos individuales, utiliza . Para eliminarlos, haz clic en .
- En la ventana **Editar configuración**, haz clic en el selector **Buscar parches automáticamente** para activar la búsqueda de parches. Si el selector no está activado los parches pendientes de instalación no se mostrarán en los listados, aunque las tareas de instalación de parches podrán aplicarlos de forma independiente.

Instalación de parches

Al configurar Patch Management se pueden seleccionar diferentes opciones de instalación de parches, que se aplicarán a los equipos y grupos de equipos destinatarios:

- **Instalar parches** los parches se instalarán en los equipos y grupos de equipos destinatarios.
- **Designar como equipos de prueba e instalar parches**: los equipos o grupos destinatarios serán identificados como equipos de prueba para la instalación de parches. Para más

información, consulta **Funcionalidades de Panda Patch Management**

- **No instalar parches**: los parches no se instalarán en los equipos o grupos de equipos destinatarios. Esta opción es aplicable a proveedores de servicios que tengan contratado Panda Patch Management. Para más información, consulta el capítulo **Configuraciones para los productos de seguridad** de la Guía de administraciónde Panda Partner Center.

Frecuencia de la búsqueda

Buscar parches con la siguiente frecuencia establece cada cuanto tiempo Panda Patch Management consulta los parches instalados en los equipos y los compara con las bases de datos de parches disponibles.

Criticidad de los parches

Establece la criticidad de los parches que Panda Patch Management busca en las bases de datos de parches disponibles.

En el caso de los equipos y dispositivos con sistema operativo macOS o Linux, no se aplican parches de tipo Windows Service Pack.

La criticidad de cada parche está establecida por cada proveedor del software afectado por la vulnerabilidad. Este criterio de clasificación no es uniforme y se recomienda comprobar previamente la descripción del parche para aquellos que no estén clasificados como "críticos", con el objetivo de evitar su instalación si no se padecen los síntomas descritos.

*Las criticidades relacionadas con parches de resolución de bugs y mejoras para macOS y Linux, se incluyen dentro de la categoría **Otros parches (no de seguridad)**.*

Paneles/widgets en Panda Patch Management

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **Panda Patch Management**.

Permisos requeridos

Permisos	Acceso al widget
Sin permisos	• Estado de gestión de parches • Tiempo desde la última comprobación

Permisos	Acceso al widget
Instalar, desinstalar y excluir parches	• Programas "End Of Life" • Parches disponibles • Últimas tareas de instalación de parches
Visualizar parches disponibles	• Programas "End Of Life" • Parches disponibles • Últimas tareas de instalación de parches

Tabla 13.4: Permisos requeridos para los widgets de Gestión de parches

Estado de gestión de parches

Muestra los equipos donde Panda Patch Management está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. El estado del módulo se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

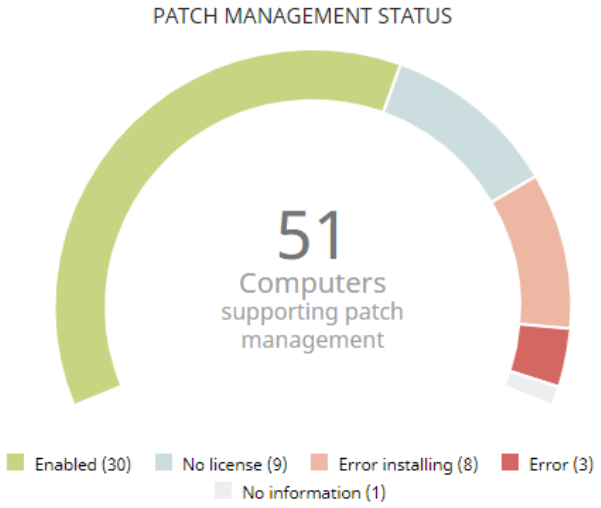


Figura 13.1: Panel de Estado de gestión de parches

Significado de las series

Serie	Descripción
Activado	Indica el porcentaje de equipos en los que Panda Patch Management se instaló sin errores, su ejecución no presenta problemas y la configuración asignada permite buscar parches automáticamente.

Serie	Descripción
Desactivado	Indica el porcentaje de equipos en los que Panda Patch Management se instaló sin errores, su ejecución no presenta problemas y la configuración asignada no permite buscar parches automáticamente.
Sin licencia	Equipos compatibles con Panda Patch Management pero sin licencia de Panda Endpoint Protection asignada.
Error instalando	Indica los equipos donde el módulo no se pudo instalar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con el agente sin actualizar.
Error	El módulo Panda Patch Management no responde a las peticiones del servidor y su configuración difiere de la establecida en la consola web.
Parte central	Refleja el número de total de equipos compatibles con el módulo Panda Patch Management.
Pendiente de reinicio	Indica el número de equipos que están pendientes de reinicio para completar la instalación o desinstalación de parches.

Tabla 13.5: Descripción de la serie Estado de gestión de parches

Filtros preestablecidos desde el panel

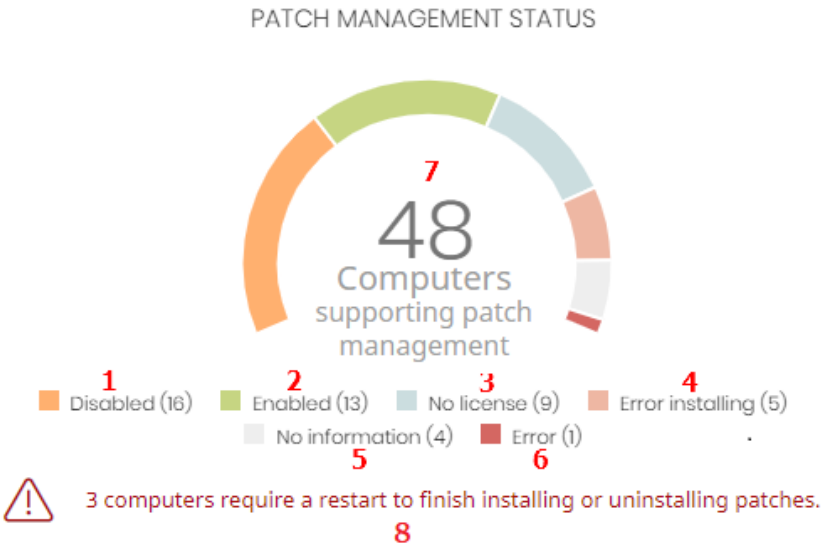


Figura 13.2: Zonas activas del panel Estado de gestión de parches

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado de gestión de parches** se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de gestión de parches = Desactivado.
(2)	Estado de gestión de parches = Activado.
(3)	Estado de gestión de parches = Sin licencia. El equipo no tiene asignada licencia de Panda Endpoint Protection.
(4)	Estado de gestión de parches = Error instalando.
(5)	Estado de gestión de parches = Sin información.
(6)	Estado de gestión de parches = Error.
(7)	Sin filtro.
(8)	Estado de gestión de parches = Pendiente de reinicio.

Tabla 13.6: Definición de filtros del listado Estado de gestión de parches

Tiempo desde la última comprobación

Muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo para comprobar su estado de parcheo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

Figura 13.3: Panel Tiempo desde la última comprobación

Significado de las series

Serie	Descripción
72 horas	Número de equipos que no comprobaron su estado de parcheo en

Serie	Descripción
	las últimas 72 horas.
7 días	Número de equipos que no comprobaron su estado de parcheo en las últimas 7 días.
30 días	Número de equipos que no comprobaron su estado de parcheo en los últimas 30 días.

Tabla 13.7: Descripción de la serie Tiempo desde la última comprobación

Filtros preestablecidos desde el panel

Figura 13.4: Zonas activas del panel Tiempo desde la ultima comprobación

Al hacer clic en las zonas indicadas en **Zonas activas del panel Tiempo desde la ultima comprobación** se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 3 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(2)	Última conexión = Hace más de 7 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(3)	Última conexión = Hace más de 30 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.

Tabla 13.8: Definición de filtros del listado Estado de gestión de parches

Programas "End of life"

Muestra la información relativa al "end of life" de los programas instalados en los equipos de la red, agrupados según el plazo restante.

Figura 13.5: Panel Programas "End of life"

Significado de las series

Serie	Descripción
Actualmente en EOL	Programas instalados en el parque informático que ya entraron en EOL.
Actualmente o en 1 año en EOL	Programas instalados en el parque informático que ya han entrado en EOL o entrarán dentro de un año.
Con fecha EOL conocida	Programas instalados en el parque informático cuya fecha de EOL es conocida.

Tabla 13.9: Descripción de la serie Programas "End of life"

Filtros preestablecidos desde el panel

Figura 13.6: Zonas activas del panel Programas "End of life"

Al hacer clic en las zonas indicadas en **Zonas activas del panel Programas "End of life"** se abre el listado **Programas "End Of Life'** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Actualmente en EOL.
(2)	Actualmente o en 1 año en EOL.

Zona activa	Filtro
(3)	Con fecha EOL conocida.

Tabla 13.10: Definición de filtros del listado Programas "End Of Life'

Últimas tareas de instalación de parches

*Consulta **Gestionar tareas** en la página **611** para obtener más información sobre como modificar una tarea ya creada.*

Muestra un listado de las últimas tareas de instalación de parches y actualizaciones creadas. Este widget está formado por varios enlaces que permiten gestionar las tareas de instalación de parches:

Figura 13.7: Panel de Últimas tareas de instalación de parches

- Haz clic en una tarea para editar su configuración.
- Haz clic en el enlace **Ver todas** para acceder directamente al menú superior **Tareas** donde se muestran todas las tareas creadas.
- Haz clic en el enlace **Ver historial de instalaciones** para acceder al listado **Historial de instalaciones** con todas las tareas de instalación de parches terminadas con éxito o con error.
- Haz clic en el menú de contexto asociado a una tarea para mostrar una lista desplegable con las opciones siguientes:
    - **Cancelar**: interrumpe la tarea antes de iniciar el proceso de instalación de parches en el equipo.
    - **Ver resultados**: muestra los resultados de la tarea.

Evolución de los parches disponibles

Muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad.

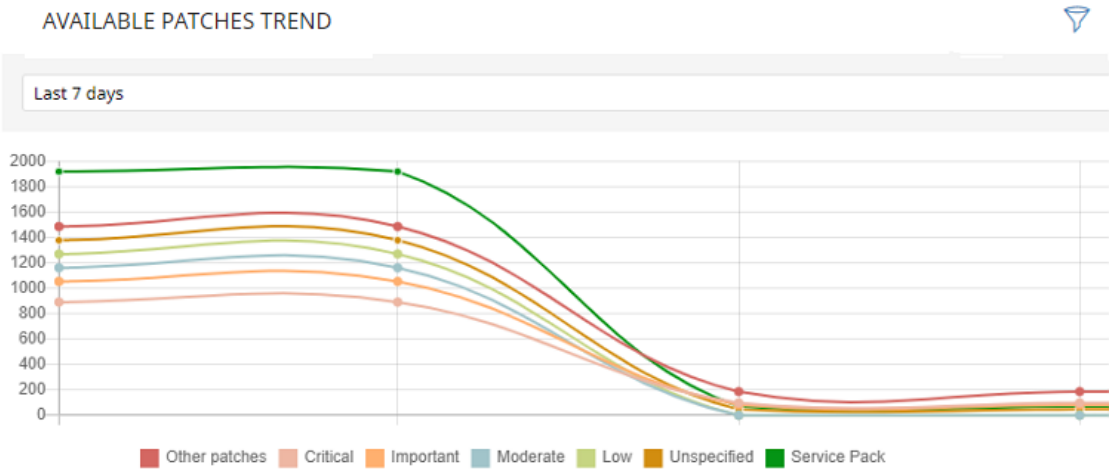


Figura 13.8: Gráfico de Evolución de parches disponibles

Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad – No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía. No aplicable a equipos con sistema operativo Linux o macOS.

Tabla 13.11: Descripción de la serie Parches disponibles

Al situar el cursor del ratón sobre uno de los nodos se muestra un tooltip con la siguiente información:

- Fecha
- Tipo
- Número de parches

Filtros preestablecidos desde el panel

Haz clic sobre los elementos de la leyenda debajo de la gráfica para acceder al listado **Parches disponibles** con el filtro correspondiente al tipo seleccionado. Haz clic sobre la gráfica, para acceder al listado completo de **Parches disponibles** sin aplicar ningún filtro.

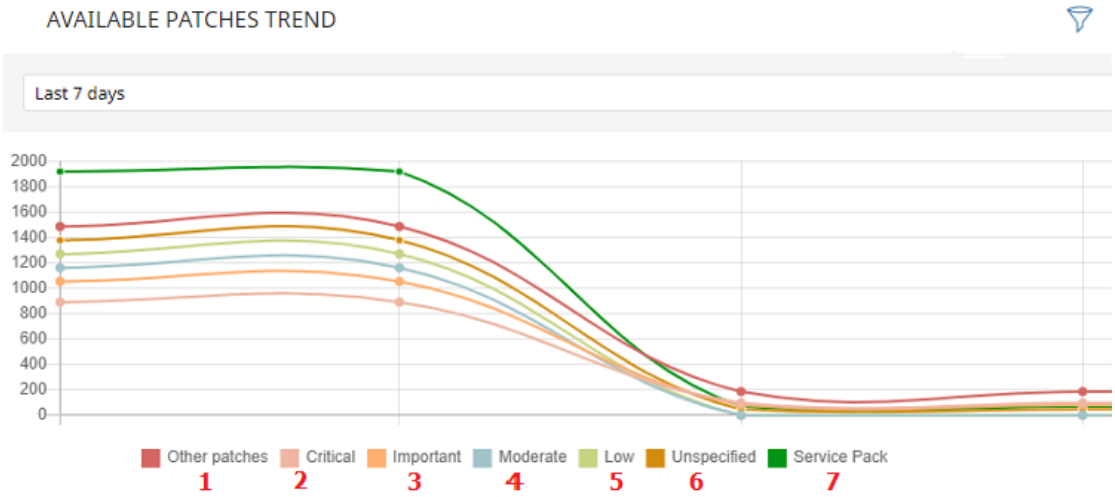


Figura 13.9: Series mostradas en el gráfico Evolución de parches disponibles

Zona activa	Filtro
(1)	Criticidad = Otros parches (no de seguridad).
(2)	Criticidad = Critica (de seguridad).
(3)	Criticidad = Importante (de seguridad).
(4)	Criticidad = Moderada (de seguridad).
(5)	Criticidad = Baja (de seguridad).
(6)	Criticidad=No clasificado (de seguridad)
(9)	Criticidad = Service Pack.

Tabla 13.12: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Al hacer clic en el icono se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

Filtro	Definición
Tipo de equipo	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.
Parches de sistema operativo	Parches disponibles para sistemas operativos.
Parches de aplicaciones	Parches disponibles para las aplicaciones . Para ver el listado completo de aplicaciones soportadas por Panda Patch Management, consulta https://info.pandasecurity.com/patchmanagementapp/. Para obtener más información acerca de cómo seleccionar las aplicaciones a parchear consulta Configuración de una tarea de instalación de parches.

Tabla 13.13: Filtros disponibles para el widget Evolución de parches disponibles

Parches disponibles

Muestra un recuento de parejas parche - equipo sin aplicar, distribuido por la categoría del parche. Cada parche no aplicado se contabiliza tantas veces como equipos no lo tengan instalado.

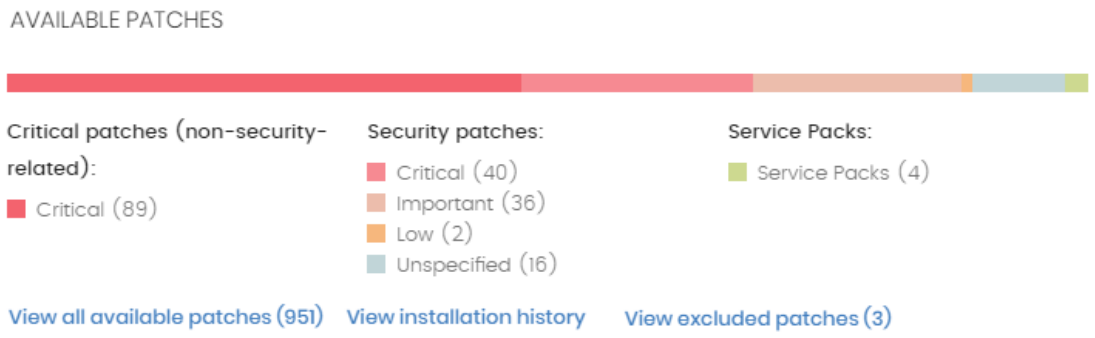


Figura 13.10: Panel Parches disponibles

Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad – No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía.
Ver todos los parches disponibles	Número de parches de cualquier importancia relativos o no a la seguridad del sistema y que no han sido aplicados todavía.
Ver parches excluidos	Número de parches excluidos de su instalación.

Tabla 13.14: Descripción de la serie Parches disponibles

Filtros preestablecidos desde el panel

Figura 13.11: Zonas activas del panel Parches disponibles

Al hacer clic en las zonas indicadas en **Descripción de la serie Parches disponibles** se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Parches disponibles	Criticidad = Critica (de seguridad).
(2)	Parches disponibles	Criticidad = Importante (de seguridad).
(3)	Parches disponibles	Criticidad = Baja (de seguridad).
(4)	Parches disponibles	Criticidad = No clasificado (de seguridad).
(5)	Parches disponibles	Criticidad = Otros parches (no de seguridad).
(6)	Parches disponibles	Criticidad = Service Pack.
(7)	Parches disponibles	Sin filtros.
(8)	Historial de instalaciones	Sin filtros.
(9)	Parches excluidos	Sin filtros.

Tabla 13.15: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Al hacer clic en el icono se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

Filtro	Definición
Tipo de equipo	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.
Parches de sistema operativo	Parches disponibles para sistemas operativos.
Parches de aplicaciones	Parches disponibles para las aplicaciones . Para ver el listado completo de aplicaciones soportadas por Panda Patch Management, consulta **https://info.pandasecurity.com/patchmanagementapp/**. Para obtener más información acerca de cómo seleccionar las aplicaciones a parchear consulta **Configuración de una tarea de instalación de parches**.

Tabla 13.16: Filtros disponibles para el widget Evolución de parches disponibles

Parches disponibles en más equipos

Muestra el número de equipos afectados por cada parche disponible en estado **Pendiente** o **Pendiente de reinicio** .

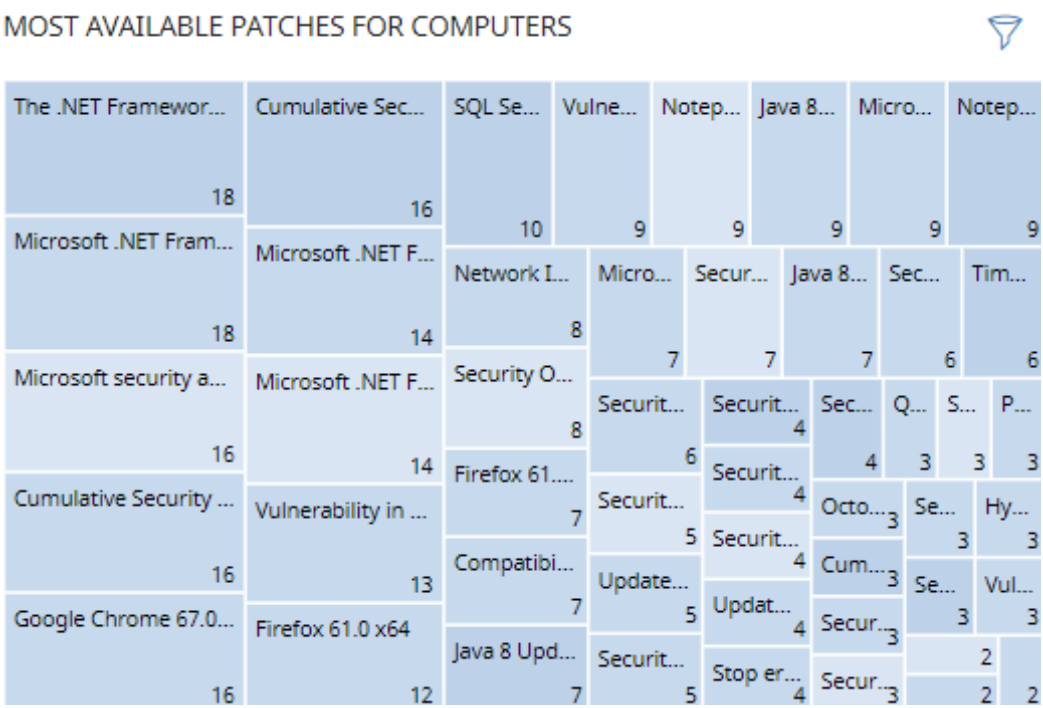


Figura 13.12: Panel Parches disponibles en más equipos

Significado de las series

Serie	Descripción
Nombre	Nombre del parche disponible.
Número	Número de equipos con el parche disponible en estado **Pendiente** o **Pendiente de reinicio**.
Enlace Ver todos los parches disponibles	Acceso al listado completo de parches disponibles por equipos.

Tabla 13.17: Descripción de las series de Parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra un tooltip con la siguiente información:

- Nombre del parche.
- Número de equipos que tienen disponible el parche.
- Programa (o familia del sistema operativo).
- Criticidad.
- Fecha de publicación
- Número CVE (Common Vulnerabilities and Exposures).

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles**.

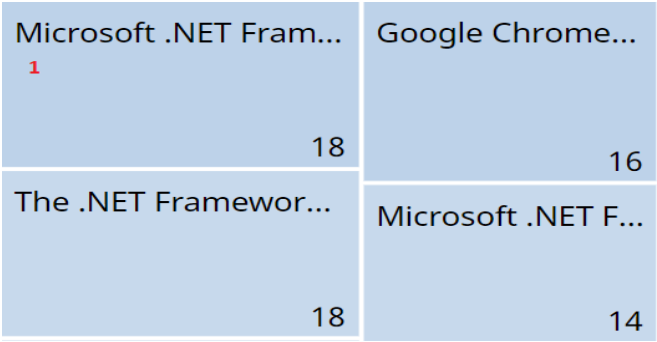


Figura 13.13: Zonas activas del panel Parches disponibles en más equipos

Zona activa	Filtro
(1)	Parche = Nombre del parche seleccionado

Tabla 13.18: Definición de filtros del listado Parches disponibles en más equipos

Filtros disponibles sobre el widget

Haz clic en el icono para mostrar los filtros disponibles que se aplican sobre la información mostrada en el propio widget:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows

Filtro	Descripción	Valores
		• Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones • Parches de sistema operativo

Tabla 13.19: Filtros del panel Parches disponibles en más equipos

Equipos con más parches disponibles

Muestra los equipos de la red que tienen más parches disponibles para instalar, y su número.

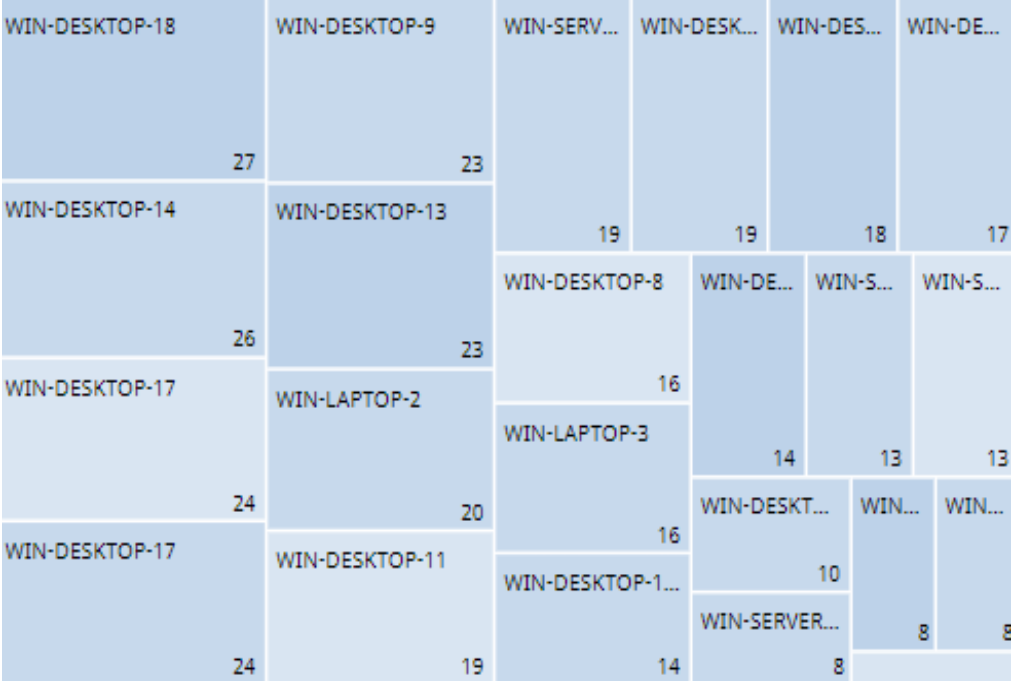


Figura 13.14: Panel Equipos con más parches disponibles

Significado de las series

Serie	Descripción
Nombre	Nombre del equipo con más parches disponibles.
Número	Número de parches disponibles en el equipo.

Tabla 13.20: Descripción de las series del panel Parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra una etiqueta con la siguiente información:

- Nombre del equipo.
- Número de parches tiene disponible el equipo.

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles**.

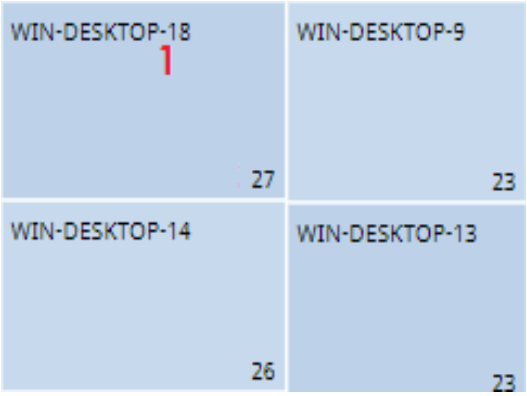


Figura 13.15: Zonas activas del panel Equipos con más parches disponibles

Zona activa	Filtro
(1)	Equipo = Nombre del equipo seleccionado

Tabla 13.21: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Haz clic en el icono para mostrar los filtros disponibles:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Filtro	Descripción	Valores
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones. • Parches de sistema operativo.

Tabla 13.22: Definición de filtros del panel Equipos con más parches disponibles

Programas con más parches disponibles

Muestra los programas que tienen más parches disponibles para instalar, y su número.

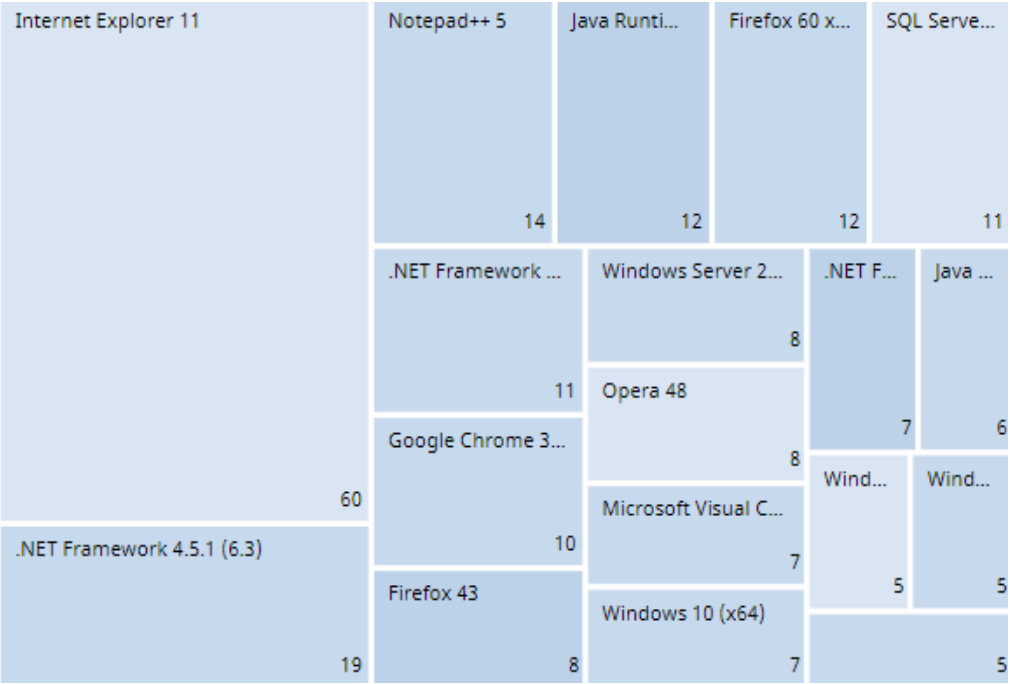


Figura 13.16: Panel Programas con más parches disponibles

Significado de las series

Serie	Descripción
Nombre	Nombre del programa.
Número	Número de parches del programa disponibles.

Tabla 13.23: Descripción de las series del panel Programas con más parches disponibles

Al situar el cursor del ratón sobre un cuadro, se muestra una etiqueta con la siguiente información:

- Nombre del programa.
- Número de parches disponibles del programa.

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles**.

Figura 13.17: Zonas activas del panel Programas con más parches disponibles

Zona activa	Filtro
(1)	Programa = Nombre del programa seleccionado

Tabla 13.24: Definición de filtros del listado Parches disponibles

Filtros disponibles sobre el widget

Haz clic en el icono para mostrar los filtros disponibles:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad)

Filtro	Descripción	Valores
		• Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones. • Parches de sistema operativo.

Tabla 13.25: Definición de filtros del panel Programas con más parches disponibles

Listados del módulo Panda Patch Management

Acceso a los listados

El acceso a los listados se podrá hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Patch Management** y en el widget relacionado.

  ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se abrirá una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Gestión de parches** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Los listados de instalación o desinstalación de parches se pueden consultar desde el widget **Historial de instalaciones**, haciendo clic en **Ver historial de instalaciones**.

Los listados **Resultados tarea de instalación / desinstalación de parches** y **Ver parches instalados / desinstalados** se pueden consultar desde el menú superior **Tareas**, haciendo clic en **Ver resultados** en una tarea de instalación o desinstalación.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	• Estado de gestión de parches
Instalar, desinstalar y excluir parches	Acceso a los listados y a los menús de contexto para instalar y desinstalar parches: • Parches disponibles • Historial de instalaciones • Programas "End Of Life" • Parches excluidos • Resultados tarea de instalación / desinstalación de parches • Ver parches instalados / desinstalados

Permisos	Acceso a listados
Visualizar parches disponibles	Acceso de solo lectura a los listados: • Parches disponibles • Historial de instalaciones • Programas "End Of Life" • Parches Exclusivos • Resultados tarea de instalación / desinstalación de parches • Ver parches instalados / desinstalados • Evolución de los parches disponibles • Parches disponibles en más equipos • Equipos con más parches disponibles • Programas con más parches disponibles

Tabla 13.26: Permisos requeridos para los listados de Gestión de parches

Estado de gestión de parches

Este listado muestra en detalle todos los equipos de la red compatibles con Panda Patch Management, incorporando filtros que permiten localizar aquellos puestos de trabajo y servidores que no estén recibiendo el servicio por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Estado del equipo	Reinstalación del agente: • Reinstalando agente. • Error en la reinstalación del agente Reinstalación de la protección: • Reinstalando la protección. • Error en la reinstalación de la protección. • Pendiente de reinicio. Estado de aislamiento del equipo:	Icono

Campo	Comentario	Valores
	• Equipo en proceso de entrar en aislamiento. • Equipo aislado. • Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP: • Equipo en modo contención de ataque RDP. • Finalizando modo de contención: de ataque RDP. Instalación de parches • No instalar parches. • Designar como equipos de prueba e instalar parches.	
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Gestión de parches	Estado del módulo.	• Activado • Desactivado • Error instalando (motivo del error) • Sin licencia • — Sin información • Error

Campo	Comentario	Valores
Última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	Fecha

Tabla 13.27: Campos del listado Estado de gestión de parches

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Instalación de parches	Opción de instalación de parches aplicada al equipo:	Enumeración

Campo	Comentario	Valores
	• Instalar parches: el equipo tiene Patch Management activado. Los parches se instalarán en el equipo. • Equipo de prueba: el equipo tiene Patch Management activado y ha sido designado "equipo de prueba" para la instalación de parches. • No instalar parches: el equipo tiene Patch Management desactivado. Los parches no se instalarán en el equipo.	
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el módulo Panda Patch Management se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Booleano
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Estado de gestión de parches	Estado del módulo.	• Activado • Desactivado

Campo	Comentario	Valores
		• Error instalando • Sin licencia • Sin información • Error
Requiere reinicio	El equipo no se ha reiniciado para completar la instalación o desinstalación de uno o más parches descargados.	Booleano
Fecha de la última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Panda Patch Management y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	• Error en la descarga • Error en la ejecución

Tabla 13.28: Campos del fichero exportado Estado de gestión de parches

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor

Campo	Comentario	Valores
Última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	• Todos • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha
Pendiente de reinicio para completar la instalación o desinstalación de parches	El equipo no se ha reiniciado para completar la instalación o desinstalación de uno o más parches.	Booleano
Instalación de parches	Opciones de instalación de parches.	• Instalación de parches activada • Equipo de prueba para la instalación de parches • Instalación de parches desactivada

Campo	Comentario	Valores
Estado de gestión de parches	Estado del módulo.	• Activado • Desactivado • Error • Error instalando • Sin licencia • Sin información

Tabla 13.29: Campos de filtrado para el listado Estado de gestión de parches

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se abrirá la ventana de detalle del equipo. Consulta Información de equipo en la página 251 para obtener más información.

Parches disponibles

Muestra el detalle de los parches disponibles y la información sobre los parches que están en proceso de instalación. Cada línea del listado refleja un par parche – equipo de la red.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado y opción de instalación de parches asignada al equipo en la configuración de Panda Patch Management: • No instalar parches. • Designar como equipos de prueba e instalar parches.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información	Cadena de

Campo	Comentario	Valores
	adicional (fecha de publicación, número de la Knowledge base etc.).	caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Indica el estado de la instalación del parche: • **Pendiente**: el parche está disponible para el equipo y no ha completado su instalación. • **Requiere descarga manual**: el parche requiere que el administrador descargue de forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta **Descargar los parches de forma manual** para más información. • **Pendiente (descargado manualmente)**: el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta **Descargar los parches de forma manual**para más información. • **Pendiente de reinicio:** el parche ha sido instalado pero el equipo no ha sido reiniciado. Algunos parches pueden no aplicarse hasta realizar este	Enumeración

Campo	Comentario	Valores
	proceso.	
Menú de contexto	Despliega un menú de acciones: • **Instalar**: crea una tarea inmediata de instalación del parche en el equipo elegido. • **Programar instalación**: crea una tarea configurable de instalación del parche elegido. • **Excluir**: permite elegir de qué equipo se quiere excluir el parche. • **Visualizar parches disponibles del equipo**: filtra el listado por el equipo elegido para mostrar todos los parches disponibles que aun no se han instalado. • **Visualizar equipos con el parche disponible**: muestra todos los equipos que tienen disponible el parche elegido para su aplicación.	Enumeración

Tabla 13.30: Campos del listado Parches disponibles

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede incluir todos los datos del listado de parches disponibles o una versión más reducida que muestra los datos correspondientes a la evolución de los parches disponibles durante los últimos 7 días, último mes o el último año.

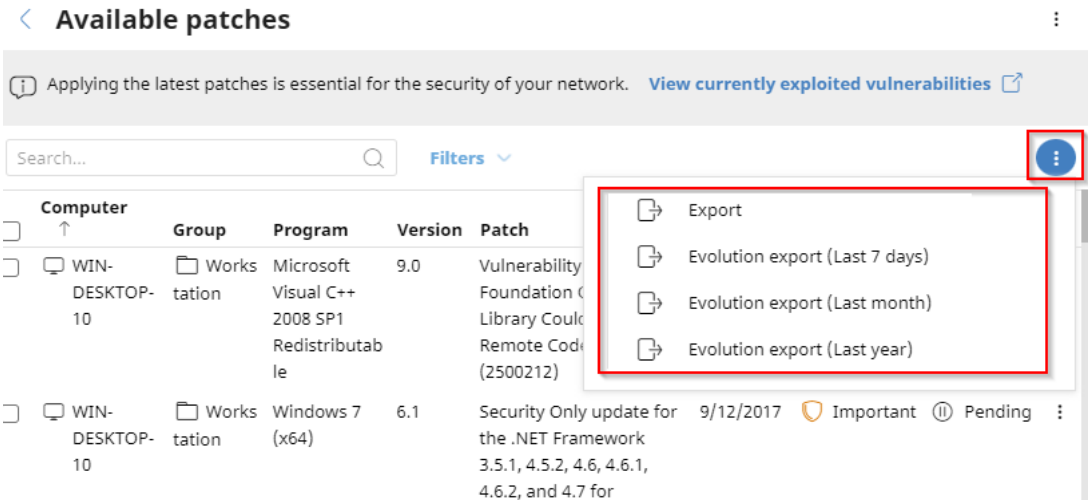


Figura 13.18: Menú de contexto para exportaciónlosTP

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Instalación de parches	Opción de instalación de parches aplicada al equipo.	• Instalación de parches activada • Equipo de prueba para la instalación de parches

Campo	Comentario	Valores
		• Instalación de parches desactivada
Vendor	Compañía creadora del programa desactualizado.	Cadena de caracteres
Familia de producto	Nombre de producto con parches pendientes de aplicar o reiniciar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado.	Numérico
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad)

Campo	Comentario	Valores
		• Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Es descargable	Indica si el parche está disponible para su descarga o requiere un contrato adicional con el proveedor del software para acceder a aquel.	Booleano
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Estado	Indica el estado de la instalación del parche: • **Pendiente**: el parche está disponible para el equipo y no ha completado su instalación. • **Pendiente (descargado manualmente)**: el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta **Descargar los parches de forma manual** para más información. • **Requiere descarga manual**: el parche requiere que el administrador descargue de	Enumeración

Campo	Comentario	Valores
	forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta **Descargar los parches de forma manual** para más información.	
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres
URL de descarga	Recurso HTTP en la infraestructura del proveedor del software para descargar el parche.	Cadena de caracteres

Tabla 13.31: Campos del fichero exportado Parches disponibles

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Publicación del parche	Fecha en la que el parche se publica y está disponible para su descarga.	• Todos • Hace menos de 7 días • Hace menos de 14 días • Hace menos de un mes • Hace menos de dos meses • Hace más de 7 días • Hace más de 14 días • Hace más de un mes

Campo	Comentario	Valores
		• Hace más de dos meses
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Tipo de parche	Clase de parche disponible.	• Parches de aplicaciones • Parches de sistema operativo
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Programa, familia o vendor	La búsqueda se aplicará al programa, familia de productos o compañía seleccionada.	Cadena de caracteres
Instalación de parches	Opción de instalación de parches.	• Instalación de parches activada • Equipo de prueba para la instalación de parches

Campo	Comentario	Valores
		• Instalación de parches desactivada
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Muestra los parches que se encuentran en proceso de instalación filtrándolos por la etapa en la que se encuentran.	• Pendiente • Requiere descarga manual • Pendiente (descargado manualmente) • Pendiente de reinicio
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Panda Patch Management debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 13.32: Campos de filtrado para el listado Parches disponibles

Ventana Parche detectado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche detectado**, en la que se muestra información detallada sobre el parche. Los datos pueden variar según el sistema operativo instalado en los equipos.

Esta ventana puede tener el siguiente contenido:

- Información sobre el parche disponible, así como el botón **Instalar el parche**.
- Información sobre el parche en proceso de instalación. El texto **Pendiente de reinicio** aparecerá junto al botón **Instalar el parche**.

Haz clic en el botón **Instalar el parche**. Aparecerá una ventana emergente en la que podrás seleccionar los destinatarios de la tarea de instalación del parche:

- **Instalar solo en el equipo actual**: La tarea se realiza en el equipo seleccionado en la lista.
- **Instalar en todos los equipos del filtro seleccionado**: Selecciona un filtro del árbol de filtros mostrado. El parche se instala en todos los equipos del filtro seleccionado.
- **Instalar en todos los equipos**: El parche se instala en todos los equipos de la red.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base, etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres
Familia	Nombre de producto con parches pendientes de aplicar o reiniciar. No disponible para parches de macOS o Linux.	Cadena de caracteres
Vendor	Compañía creadora del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad)

Campo	Comentario	Valores
		• Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Estado de la instalación	Estado de la instalación del parche o actualización.	• Pendiente • Requiere descarga manual • Pendiente (descargado manualmente) • Pendiente de reinicio
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico

Campo	Comentario	Valores
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera. No disponible para parches de macOS o Linux.	Cadena de caracteres
URL de la descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres
Descripción	Información sobre el impacto que la vulnerabilidad podría tener en los equipos. No disponible para parches de macOS o Linux.	Cadena de caracteres

Tabla 13.33: Campos de la ventana Parche detectado

Parches disponibles por equipos

Este listado muestra los parches disponibles y el número de equipos donde el parche está disponible para su instalación.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de

Campo	Comentario	Valores
		seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Equipos	Número de equipos en los que está disponible el parche.	Numérico
Menú de contexto	**Visualizar equipos con el parche disponible**: muestra todos los equipos que tienen disponible el parche elegido para su aplicación.	

Tabla 13.34: Campos del listado Parches disponibles por equipos

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede incluir todos los datos del listado de parches disponibles o una versión más reducida que muestra los datos correspondientes a la evolución de los parches disponibles durante los últimos 7 días, último mes o el último año.

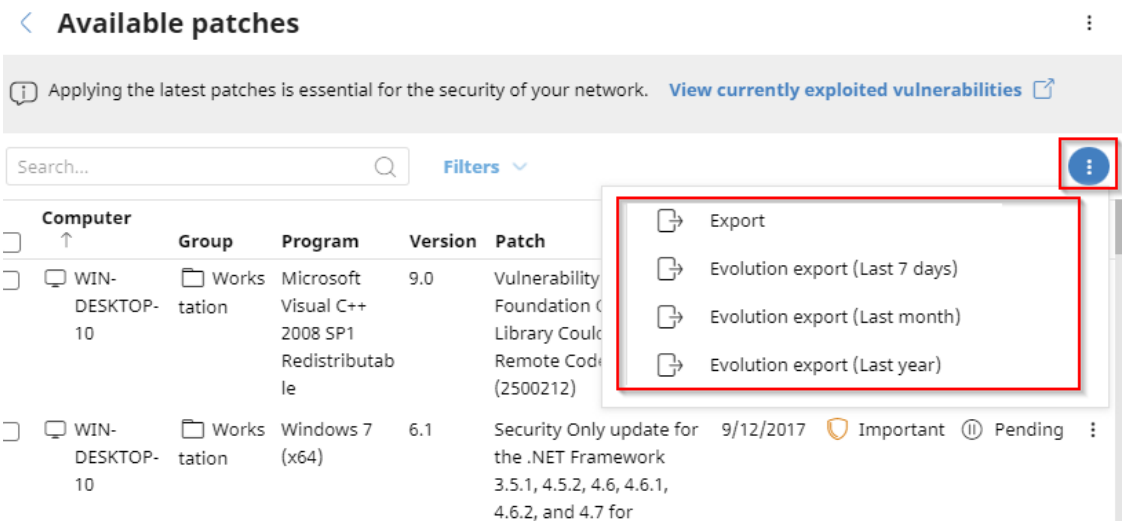


Figura 13.19: Menú de contexto para exportación

Campo	Comentario	Valores
Vendor	Compañía creadora del programa desactualizado.	Cadena de caracteres
Familia de producto	Nombre de producto con parches pendientes de aplicar o reiniciar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado.	Numérico
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad)

Campo	Comentario	Valores
		• Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Equipos	Número de equipos en los que está disponible el parche	Numérico
Plataforma	Sistema operativo instalado en el equipo.	• Windows • macOS • Linux

Tabla 13.35: Campos del fichero exportado Parches disponibles por equipos

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux

Campo	Comentario	Valores
		• macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Tipo de parche	Clase de parche disponible.	• Parches de aplicaciones • Parches de sistema operativo
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Selecciona versión de programa, familia o vendor	La búsqueda se aplicará al programa, familia de productos o compañía seleccionada.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de

Campo	Comentario	Valores
		seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Panda Patch Management debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 13.36: Campos de filtrado para el listado Parches disponibles por equipos

Ventana Parche detectado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche detectado**, en la que se muestra información detallada sobre el parche. Consulta Ventana Parche detectado.

Historial de instalaciones

Muestra las operaciones que Panda Patch Management ha ejecutado a lo largo del tiempo en los equipos de la red.

Campo	Comentario	Valores
Fecha	Fecha en la que se registró la operación.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa o versión del sistema operativo.	Cadena de caracteres
Versión	Versión del programa o sistema	Cadena de caracteres

Campo	Comentario	Valores
	operativo.	
Parche	Nombre del parche.	Cadena de caracteres
Criticidad	Importancia del parche.	• Otros parches • Crítica • Importante • Moderada • Baja • No clasificado • Service Pack
Instalación	Estado de la operación registrada.	• Instalado • Requiere reinicio • El parche ya no es requerido • Desinstalado (requiere reinicio) • Error
Menú de contexto ⋮	Muestra un desplegable con opciones.	• **Ver tarea**: muestra la configuración de la tarea asociada a la operación registrada. • **Visualizar parches instalados del equipo**: filtra el listado por el equipo elegido para mostrar todos los parches instalados en él. • **Visualizar equipos con el parche instalado**: muestra todos los equipos que tienen instalado el parche elegido.

Tabla 13.37: Campos del listado Historial de instalaciones

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede ser detallada e incluir todos los datos del listado de historial de instalaciones de parches, o una versión más reducida. En

ambos casos, se muestran los datos correspondientes a la instalación de parches durante el tiempo seleccionado.

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Fecha	Fecha de la operación registrada.	Fecha
Programa	Nombre del programa o versión del sistema operativo.	Cadena de caracteres
Versión	Versión del programa o sistema operativo.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de

Campo	Comentario	Valores
		caracteres
Criticidad	Importancia del parche.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Instalación	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Error de instalación	El módulo de Panda Patch Management no se instaló correctamente.	• **Imposible realizar la descarga**:

Campo	Comentario	Valores
		instalador no disponible • **Imposible realizar la descarga**: fichero corrupto • **Espacio insuficiente en disco** • Error en la instalación • Error en la descarga
URL de descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Código de resultado	Código resultado de la operación. Consulta la documentación del proveedor para interpretar el código de resultado.	Numérico
Nombre de la tarea	Nombre de la tarea asociada a la instalación del parche en el equipo. Visible solo al utilizar la opción de exportación detallada.	Cadena de caracteres
Fecha de lanzamiento de la tarea	Fecha para la que se programa la ejecución de la tarea de Panda Patch Management asociada al equipo. Visible solo al utilizar la opción de exportación detallada.	Fecha
Fecha de inicio de la tarea	Fecha de comienzo de ejecución de la tarea de Panda Patch Management asociada al equipo. Visible solo al utilizar la opción de exportación detallada.	Fecha

Campo	Comentario	Valores
Fecha de finalización de la tarea	Fecha en que finaliza la ejecución de la tarea de Panda Patch Management asociada al equipo. Visible solo al utilizar la opción de exportación detallada.	Fecha

Tabla 13.38: Campos del fichero exportado Historial de instalaciones

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fechas	Período en el que se aplican las instalaciones de parches.	• Últimas 24 horas • Últimos 7 días • Último mes • Rango personalizado
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad)

Campo	Comentario	Valores
		• Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Estado de la operación registrada.	• Instalado • Requiere reinicio • El parche ya no es requerido • Desinstalado (requiere reinicio) • Error • Error en la descarga • Error en la instalación
Programa	Nombre del programa o versión del sistema operativo.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres
Intentos de instalación	Muestra todos los intentos fallidos de instalación de un parche en el equipo, o solo el último intento.	• Mostrar sólo el último intento • Mostrar todos los intentos
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociada al parche.	Cadena de caracteres

Tabla 13.39: Campos de filtrado para el listado Historial de instalaciones

Ventana Parche instalado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche instalado** con información detallada de la operación registrada. Los datos pueden variar según el sistema operativo instalado en los equipos.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociada al parche.	Cadena de caracteres
Equipo	Nombre del equipo.	Cadena de caracteres
Fecha de instalación	Fecha en la que el parche se registró la operación.	Fecha
Resultado	Estado de la operación registrada.	• Instalado

Campo	Comentario	Valores
		• Requiere reinicio • Error • El parche ya no es requerido • Desinstalado • Error en la instalación • Error en la descarga
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones especiales y problemas solucionados.	Cadena de caracteres

Tabla 13.40: Campos de la ventana Parche instalado

Programas "End of Life"

Muestra los programas que ya no tienen soporte por parte de sus proveedores y que por tanto son un objetivo especialmente vulnerable para el malware y las amenazas.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software en EoL.	Cadena de caracteres

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha (en rojo si el equipo entró en EOL)

Tabla 13.41: Campos del listado Programas EoL

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres

Campo	Comentario	Valores
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EoL	Fecha en la que el programa entró en EoL.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 13.42: Campos del fichero exportado Programas EoL

Herramienta de filtrado

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS

Campo	Comentario	Valores
Fecha de "End Of Life"	Fecha en la que el programa entrará en EOL.	• Todos • Actualmente en "End of life" • Actualmente o en 1 año en "End Of Life"

Tabla 13.43: Campos de filtrado para el listado Programas EoL

Ventana Detalles del programa

Al hacer clic en uno de los programas del listado se accede a la ventana de **Detalles del programa**:

Campo	Comentario	Valores
Programa	Nombre del programa o versión del sistema operativo que recibió el parche.	Cadena de caracteres
Familia	Bundle, suit o grupo de programas al que pertenece el software.	Cadena de caracteres
Editor/Empresa	Empresa que diseñó o publicó el programa.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha

Tabla 13.44: Campos de la ventana Detalles del programa

Parches excluidos

Este listado muestra los parches que el administrador ha marcado como excluidos para evitar su instalación en los equipos de la red. Se muestra una linea por cada par parche - equipo excluido, excepto en el caso de exclusiones para todos los equipos de la red, que se mostrarán en una única linea.

Campo	Comentario	Valores
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía:	Cadena de caracteres

Campo	Comentario	Valores
	Si el parche se ha excluido para un único equipo se incluye el nombre del equipo. Si el parche se ha excluido para todos los equipos de la cuenta se incluye el literal "(Todos)".	
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres

Campo	Comentario	Valores
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 13.45: Campos del listado Parches excluidos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía: Si el parche se ha excluido para un único equipo, indica el nombre del equipo. Si el parche se ha excluido para todos los equipos de la cuenta, indica el literal "(Todos)".	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción del equipo asignada por el administrador de la red.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres

Campo	Comentario	Valores
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la	Tamaño del parche en formato comprimido. La	Numérico

Campo	Comentario	Valores
descarga (KB)	aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 13.46: Campos del fichero exportado Parches excluidos

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con un parche excluido.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Panda Patch Management debido a requisitos adicionales del proveedor	Booleano

Campo	Comentario	Valores
	(aceptación de EULA, introducción de credenciales, captchas etc.).	
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Tabla 13.47: Campos de filtrado para el listado Parches excluidos

Ventana Parche excluido

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche excluido** con información detallada del parche marcado para no instalarse en los equipos de la red. Los datos pueden variar según el sistema operativo instalado en los equipos.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres

Campo	Comentario	Valores
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha y hora en que excluido el parche.	Numérico
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones	Cadena de caracteres

Campo	Comentario	Valores
	especiales y problemas solucionados.	

Tabla 13.48: Campos de la ventana Parche excluido

Resultados tarea de instalación / desinstalación de parches

Este listado muestra los resultados de tareas de instalación o desinstalación de parches en los equipos de la red.

Campo	Descripción	Valores
Equipo	Nombre del equipo en el que se realizó la instalación / desinstalación del parche.	Cadena de caracteres
Grupo	Grupo de Panda Endpoint Protection al que pertenece el equipo.	Cadena de caracteres
Estado	Estado de la tarea.	• Pendiente • En curso • Finalizada • Con error • Cancelada (no se pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Parches instalados / desinstalados	Número de parches instalados / desinstalados.	Cadena de caracteres.
Fecha de comienzo	Fecha en la que se inicio la instalación.	Fecha
Fecha de fin	Fecha en la que se finalizo la instalación.	Fecha

Tabla 13.49: Campos de resultados de tarea de instalación / desinstalación

Herramientas de filtrado

Campo	Descripción	Valores
Estado	Estado de la tarea de instalación / desinstalación.	• Pendiente • En curso • Finalizada • Con error • Cancelada (no se pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Parches aplicados / desinstalados	Equipos en los que se han instalado / desinstalado parches.	• Todos • Sin parches instalados / desinstalados • Con parches instalados / desinstalados

Tabla 13.50: Filtros disponibles en listado Resultados tarea de instalación / desinstalación de parches

Ver parches instalados / desinstalados

Muestra los parches instalados en los equipos y otra información adicional.

Campo	Descripción	Valores
Equipo	Nombre del equipos en el que se realizó la instalación / desinstalación.	Cadena de caracteres
Grupo	Grupo de Panda Endpoint Protection al que pertenece el equipo.	Cadena de caracteres
Programa	Programa que recibe el parche.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres

Campo	Descripción	Valores
Parche	Parche instalado / desinstalado.	Cadena de caracteres
Criticidad	Relevancia del parche instalado / desinstalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Resultado	Indica si el proceso se ha completado correctamente o ha sucedido algún error.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Fecha	Fecha de ejecución del proceso.	Fecha

Tabla 13.51: Campos de resultado de instalación / desinstalación de parches

Capítulo 14

Panda Full Encryption (Cifrado de dispositivos)

Panda Full Encryption es un módulo integrado en la plataforma Aether que cifra el contenido de los medios de almacenamiento conectados a los equipos administrados por Panda Endpoint Protection. Su objetivo es minimizar la exposición de la información de las empresas, tanto en casos de pérdida o robo de los equipos como al descartar sistemas de almacenamiento en uso sin borrar previamente su contenido.

Panda Full Encryption es compatible con ciertas versiones de sistemas operativos Windows 7 en adelante y con determinadas versiones de macOS (consulta **Versiones compatibles del sistema operativo Windows**) y permite controlar el estado del cifrado de los equipos de la red, gestionando de forma centralizada sus claves de recuperación. Además, aprovecha recursos hardware como los chips TPM, ofreciendo una gran flexibilidad a la hora de elegir el sistema de autenticación más adecuado en cada caso.

Para obtener información adicional sobre los distintos apartados del módulo Panda Full Encryption consulta las referencias siguientes:

***Crear y gestionar configuraciones** en la página **285**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.*

***Acceso, control y supervisión de la consola de administración** en la página **53**: gestión de cuentas de usuario y asignación de permisos.*

***Gestión de listados** en la página **42**: información sobre como gestionar listados.*

Contenido del capítulo

Introducción a los conceptos de cifrado

Panda Full Encryption utiliza las herramientas integradas en los sistemas operativos Windows y macOS para gestionar el cifrado en los equipos de la red gestionados con Panda Endpoint Protection.

Para una correcta comprensión de los procesos involucrados en el cifrado y descifrado de la información, es necesario presentar algunos conceptos relativos a la tecnología de cifrado utilizada.

TPM

TPM (Trusted Platform Module, módulo de plataforma segura) es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación.

Ademas, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

La versión mínima de TPM soportada por Panda Full Encryption es la 1.2. y Panda Security recomienda su uso en combinación con otros sistemas de autenticación soportados. En algunos escenarios es posible que el TPM esté deshabilitado en la BIOS del equipo y sea necesario su activación manual.

Tipos de autenticación soportados

Contraseña de inicio de sesión

En el sistema operativo macOS no se dispone de métodos de autenticación independientes, por lo que se utiliza siempre la contraseña de inicio de sesión, compatible con todas las versiones de

macOS soportadas por Panda Full Encryption.

PIN

El PIN (Personal Identification Number, número de identificación personal) es una secuencia de números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible. Compatible con todas las versiones de Windows soportadas.

PIN extendido

Si el hardware es compatible, Panda Full Encryption utilizará un PIN extendido o PIN mejorado compuesto por letras y números para incrementar la complejidad de la contraseña.

Debido a que el PIN Extendido se pide en el proceso de inicio del equipo previo a la carga del sistema operativo, las limitaciones de la BIOS pueden restringir la entrada de teclado a la tabla ASCII de 7 bits.

Adicionalmente, los teclados que utilizan una distribución distinta a la dispuesta en el mapa de caracteres EN- US, tales como teclados QWERTZ o AZERTY, pueden provocar el fallo en la introducción del PIN Extendido. Por esta razón, Panda Full Encryption controla que los caracteres introducidos por el usuario pertenecen al mapa EN-US antes de establecer el PIN Extendido en el proceso de cifrado del equipo.

Compatible con todas las versiones de Windows soportadas.

Passphrase

Una passphrase es una contraseña de mayor longitud formada por caracteres alfanuméricos equivalente al PIN Extendido.

Panda Full Encryption establece las siguientes prioridades al solicitar un tipo u otro de contraseña al usuario:

- Passphrase: siempre que el equipo tenga un TPM instalado.
- PIN extendido: si el sistema operativo y el hardware del equipo lo soportan.
- PIN: si todas las demás opciones no son válidas.

Compatible con equipos Windows 8 y posteriores sin TPM.

Llave USB

Permite almacenar la clave de acceso en un dispositivo USB formateado con NTFS, FAT o FAT32. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

Compatible con equipos Windows 7 sin TPM.

Algunos PCs antiguos no son capaces de acceder a las unidades USB en el proceso de arranque, comprueba que los equipos de tu organización tienen acceso a las unidades USB desde la BIOS.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Panda Full Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo.

Panda Full Encryption únicamente almacena las claves de recuperación de los equipos que gestiona. La consola de administración no mostrará las claves de recuperación de los equipos cifrados por el usuario y no gestionados por Panda Security.

La clave de recuperación se solicita en los escenarios mostrados a continuación:

- Cuando se introduce errónea y repetidamente el PIN o la passphrase en el proceso de inicio del equipo.
- Cuando un equipo protegido con TPM detecta un cambio en la secuencia de arranque (disco duro protegido por TPM y conectado en otro equipo).
- Cuando se ha cambiado la placa base del equipo y por lo tanto el TPM.
- Al desactivar, deshabilitar o borrar el contenido del TPM.
- Al cambiar los valores de configuración de arranque del equipo.
- Al cambiar el proceso de arranque del equipo:
    - Actualización de la BIOS.
    - Actualización del firmware.
    - Actualización de la UEFI.
    - Modificación del sector de arranque.
    - Modificación del registro maestro de arranque (master boot record).
    - Modificación del gestor de arranque (boot manager).
    - Cambio del firmware implementado en ciertos componentes que forman parte del proceso de arranque del equipo (tarjetas de vídeo, controladores de discos, etc.) conocido como Option ROM.

- Cambio de otros componentes que intervienen en las fases iniciales del arranque del sistema.

BitLocker

Es el software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo. Panda Full Encryption instala BitLocker automáticamente en aquellas versiones de servidor que no lo incluyan pero sean compatibles.

FileVault

Es el software integrado en el sistema operativo macOS, que permite cifrar de forma automática todos los archivos que se almacenan en el disco duro o memoria SSD del ordenador.

Partición de sistema

En el sistema operativo Windows, es una zona pequeña del disco duro que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio. Panda Full Encryption crea automáticamente esta partición de sistema si no existiera previamente.

Algoritmo de cifrado

El algoritmo de cifrado para Windows elegido en Panda Full Encryption es el AES-256 aunque los equipos con volúmenes cifrados por el usuario que utilicen otro algoritmo de cifrado también son compatibles.

En macOS, el único algoritmo disponible es el AES-XTS.

Visión general del servicio de Panda Full Encryption

El proceso general de cifrado abarca varios apartados que el administrador deberá conocer para gestionar correctamente los recursos de la red susceptibles de contener información delicada o comprometedora en caso de robo, pérdida o descarte del volumen sin borrar:

- **Cumplimiento de los requisitos mínimos de hardware y software:** consulta **Requisitos mínimos de Panda Full Encryption** para ver las limitaciones y particularidades del cifrado en cada plataforma compatible.
- **Estado previo del cifrado en el equipo del usuario**: dependiendo de si BitLocker o FileVault estaba siendo usado previamente en el equipo del usuario, el proceso de integración en Panda Full Encryption puede variar ligeramente.
- **Asignación de configuraciones de cifrado**: establece el estado (cifrado o no cifrado) de los equipos de la red y el o los métodos de autenticación.

- **Interacción del proceso de cifrado con el usuario del equipo:** el proceso de cifrado inicial requiere de la colaboración del usuario para completarse de forma correcta. Consulta **Cifrado de volúmenes sin cifrado previo** para más información.
- **Visualización del estado de cifrado del parque informático**: mediante los widgets / paneles incluidos en el menú superior **Estado**, panel lateral **Panda Full Encryption**. Consulta **Paneles / widgets del módulo Panda Full Encryption**para una descripción completa de los widgets incluidos en Panda Full Encryption. También se soportan filtros para localizar equipos en los listados según su estado. Consulta **Filtros disponibles** para más información.
- **Restricción de los permisos de cifrado a los administradores de la seguridad**: el sistema de roles mostrado en **Descripción de los permisos implementados** en la página **69** abarca la funcionalidad de cifrado y visualización del estado de los equipos de la red.
- **Obtención de la clave de recuperación**: en los casos en que el usuario haya olvidado la contraseña, el PIN / passpharse o el TPM haya detectado una situación anómala el administrador de la red podrá obtener de forma centralizada la clave de recuperación y enviársela al usuario. Consulta **Proceso para obtener la clave de recuperación** para más información.

Características generales de Panda Full Encryption

Tipos de autenticación soportados

Dependiendo de la existencia o no de TPM y de la versión del sistema operativo, Panda Full Encryption admite distintas combinaciones de métodos de autenticación, mostrados a continuación de forma ordenada según la recomendación de Panda Security:

Windows

- **TPM + PIN**: compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS y el establecimiento de un PIN.
- **Solo TPM**: compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS excepto en Windows 10, donde se habilita de forma automática.
- **Dispositivo USB**: requiere una llave USB y un equipo que pueda acceder a dispositivos USBs en el arranque. Necesario en equipos Windows 7 sin TPM.
- **Passprhase**: solo disponible en equipos Windows 8 y posteriores sin TPM.

macOS

No se utiliza un método de autenticación independiente sino la contraseña de inicio de sesión, compatible con todas las versiones del sistema operativo soportadas por Panda Full Encryption. Consulta **Versiones compatibles del sistema operativo Windows**

Panda Full Encryption utiliza por defecto un método de autenticación que incluye el uso de TPM si se encuentra disponible. Si se elige una combinación de autenticación no incluida en el listado anterior, la consola de administración mostrará una ventana de advertencia indicando que el equipo permanecerá sin cifrar.

Tipo de dispositivos de almacenamiento compatibles

Panda Full Encryption cifra todos los dispositivos internos de almacenamiento masivo:

Windows y macOS

- Unidades de almacenamiento fijas del equipo (sistema y datos).

Windows

- Discos duros virtuales (VHD) pero unicamente el espacio utilizado independientemente de lo indicado en la consola de administración.
- Discos duros extraibles.
- Llaves USB.

No se cifrarán:

- Discos duros internos dinámicos.
- Particiones de tamaño muy reducido.
- Otros dispositivos de almacenamiento externo.

Requisitos mínimos de Panda Full Encryption

Los requisitos mínimos se dividen en:

- Versiones y familias compatibles del sistema operativo Windows.
- Versiones compatibles del sistema operativo macOS.
- Requisitos de hardware para equipos Windows.

Versiones compatibles del sistema operativo Windows

- Windows 7 (Ultimate, Enterprise)
- Windows 8/8.1 (Pro, Enterprise)
- Windows 10 (Pro, Enterprise, Education)
- Windows 11 (Pro, Enterprise, Education)
- Windows Server 2008 R2 y superiores (incluyendo a las ediciones Server Core)

Versiones compatibles del sistema operativo macOS

- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma

Requisitos de hardware para equipos Windows

- TPM 1.2 y superiores si se utiliza este método de autenticación.
- Llave USB y equipo compatible con la lectura de dispositivos USB desde la BIOS en sistemas Windows 7 sin TPM.

En el caso del sistema operativo macOS, no hay requisitos de hardware específicos.

Gestión de equipos según su estado de cifrado previo

Administración de equipos por Panda Full Encryption

Para que un equipo de la red se considere gestionado por Panda Full Encryption es necesario que se cumplan las condiciones siguientes:

- El equipo cumple con los requisitos mínimos descritos en **Requisitos mínimos de Panda Full Encryption**
- El equipo ha recibido al menos una vez una configuración desde la consola de administración que establezca el cifrado de los volúmenes y éste se ha completado con éxito.

Los equipos que previamente tenían cifrado alguno de sus volúmenes y no han recibido una configuración que cifre sus unidades no serán gestionados por Panda Full Encryption y por lo tanto el administrador no tendrá acceso a la clave de recuperación ni al estado del equipo.

Por el contrario, los equipos que han recibido una configuración que cifre sus unidades, independientemente de su estado anterior (cifrado o no) serán administrados por Panda Full Encryption.

Desinstalación del agente Panda Endpoint Protection

Independientemente de si el equipo estaba siendo administrado por Panda Full Encryption o no, si los dispositivos de almacenamiento estaban cifrados, al desinstalar Panda Endpoint Protection se dejaran tal y como están. No obstante, se perderá el acceso centralizado a la clave de recuperación.

Si posteriormente el equipo se reintegra en Panda Endpoint Protection se mostrará la última clave de recuperación almacenada.

Proceso de cifrado y descifrado en Windows

Cifrado de volúmenes sin cifrado previo

El proceso de cifrado se inicia cuando el agente Panda Endpoint Protection instalado en el equipo de usuario se descarga una configuración de tipo Cifrado. En ese momento se le mostrará al usuario una ventana informativa que le guiará en todo el proceso.

El número de pasos total varía dependiendo del tipo de autenticación elegida por el administrador y del estado previo del equipo. Si cualquiera de los pasos termina en un error, el agente lo reportará a la consola de administración y el proceso se detendrá.

No se permitirá el cifrado de equipos desde una sesión de escritorio remoto ya que es necesario el reinicio del equipo y la introducción de una clave antes de la carga del sistema operativo, operaciones que no son posibles con un sistema de escritorio remoto estándar.
El proceso de cifrado se iniciará cuando la instalación o desinstalación en curso de parches gestionados por el módulo Panda Full Encryption haya finalizado.

A continuación se muestra el proceso completo de cifrado y se indica si se muestra feedback al usuario del equipo y si es necesario el reinicio de la máquina:

Paso	Proceso en el equipo	Interacción con el usuario
1	El agente recibe una configuración del módulo de cifrado que pide cifrar el contenido de los dispositivos de almacenamiento instalados.	Ninguno
2	Si el equipo es de tipo servidor y no tiene las herramientas de BitLocker instaladas éstas se descargan y se instalan.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la instalación de BitLocker

Paso	Proceso en el equipo	Interacción con el usuario
		o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. **Requiere reinicio**.
3	Si el equipo no estaba cifrado previamente se crea la partición de sistema.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la creación de la partición de sistema o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. **Requiere reinicio**.
4	Si existe una directiva de grupo definida previamente por el administrador de la red que colisione con las establecidas por Panda Full Encryption se mostrará un error y el proceso terminará. Las directivas de grupo configuradas por Panda Full Encryption son: En el Editor de Directivas de grupo local, navega la ruta siguiente: Directiva equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Cifrado de unidad BitLocker > Unidades del sistema operativo. Marca a Sin definir las políticas de grupo indicadas para evitar este error.	Si el administrador no ha definido directivas de grupo globales que entren en colisión con las directivas locales definidas por Panda Full Encryption no se mostrará ningún mensaje.
5	Preparación del TPM si existe y si el método de autenticación elegido involucra a éste componente y no estaba habilitado previamente desde la BIOS.	Requiere confirmar un reinicio para que el usuario pueda entrar en la BIOS del equipo y habilitar el TPM. En sistemas operativos Windows 10 no

Paso	Proceso en el equipo	Interacción con el usuario
		es necesario modificar la BIOS pero se requiere el reinicio igualmente. El reinicio del paso 3, en caso de haberlo, se juntará con el actual.
6	Preparación del dispositivo USB si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir un dispositivo USB para almacenar la contraseña de inicio de equipo.
7	Almacenamiento del PIN si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir el PIN. Si se utilizan caracteres alfanuméricos y el hardware no es compatible se mostrará el error "-2144272180". En este caso introduce un PIN numérico.
8	Almacenamiento de la passphrase si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir la passphrase.
9	Se genera la clave de recuperación y se envía a la nube de Panda Security. Una vez que la clave se ha recibido, el proceso continúa en el equipo del usuario.	Ninguno.
10	Comprobación de que el hardware del equipo es compatible con la tecnología de cifrado, e inicio del cifrado.	Se requiere confirmar un reinicio para hacer el chequeo del hardware utilizado en los distintos métodos de autenticación elegidos. Requiere reinicio.
11	Cifrado de volúmenes.	Comienza el proceso de cifrado en segundo plano sin ocasionar molestias al usuario del equipo. La duración depende del volumen de datos a cifrar. Una duración media del tiempo de cifrado se sitúa en torno a las 2-3 horas.

Paso	Proceso en el equipo	Interacción con el usuario
		El usuario puede utilizar y apagar el equipo normalmente. El proceso de cifrado se reanudará en el siguiente encendido del equipo.
12	El proceso de cifrado se completa de forma silenciosa y a partir de ese momento el proceso de cifrado y descifrado es transparente para el usuario.	Dependiendo del método de autenticación elegido el usuario puede necesitar introducir una llave USB, un PIN, una passphrase o nada en el inicio del equipo.

Tabla 14.1: Pasos para el cifrado de volúmenes sin cifrar previamente

Cifrado de volúmenes ya cifrados previamente

En el caso de que algún volumen del equipo ya estuviera cifrado, Panda Full Encryption modifica algunos parámetros para habilitar su gestión centralizada. A continuación se indican las acciones realizadas:

- Si el método de autenticación elegido por el usuario no coincide con el especificado en la configuración, éste se cambiará, solicitándole al usuario las claves o recursos hardware necesarios. Si no es posible asignar un método de autenticación compatible con la plataforma y con la configuración especificada por el administrador, el equipo quedará cifrado por el usuario y no será gestionado por Panda Full Encryption.
- Si el algoritmo de cifrado utilizado no está soportado (distinto de AES-256) se dejará sin cambios para evitar el descifrado y cifrado completo el volumen pero el equipo será administrador por Panda Full Encryption.
- Si existen tanto volúmenes cifrados como sin cifrar, se cifrarán todos los volúmenes aplicando el mismo método de autenticación.
- Si el método de autenticación elegido previamente involucra la introducción de una contraseña y es compatible con los métodos soportados por Panda Full Encryption, se volverá a pedir la contraseña al usuario para unificar el método de autenticación en todos los volúmenes.
- Si el usuario eligió una configuración de cifrado distinta a la establecida por el administrador (cifrado unicamente de los sectores ocupados frente al cifrado completo del volumen) el volumen se dejará sin cambios para minimizar el proceso de cifrado.
- Al final de todo el proceso el dispositivo pasa a ser gestionado por Panda Full Encryption y se genera la clave de recuperación para su posterior envío a la nube de Panda Security.

Cifrado de nuevos volúmenes

Si una vez completado el proceso de cifrado el usuario del equipo crea un nuevo volumen, Panda Full Encryption lo cifrará inmediatamente respetando la configuración asignada por el administrador de la red.

Descifrado de volúmenes

Se distinguen tres casos:

- Si Panda Full Encryption cifra un equipo, a partir de ese momento el administrador podrá asignar una configuración para descifrarlo.
- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Panda Full Encryption y se le asigna una configuración de cifrado se considerará cifrado por Panda Full Encryption y se podrá descifrar asignando una configuración desde la consola de administración.
- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Panda Full Encryption y nunca se le ha asignado una configuración de cifrado no se considerará cifrado por Panda Full Encryption y no se podrá descifrar asignando una configuración desde la consola de administración.

Modificación local de la configuración de BitLocker

El usuario del equipo tiene acceso a la configuración local de BitLocker desde las herramientas de Windows pero los cambios que efectúe serán revertidos de forma inmediata a la configuración establecida por el administrador de la red a través de la consola de administración. El comportamiento de Panda Full Encryption ante un cambio de esta naturaleza se muestra a continuación:

- **Desactivar el desbloqueo automático de una unidad**: se revierte a la configuración de bloqueo automático.
- **Quitar la contraseña de un volumen**: se pedirá la nueva contraseña.
- **Descifrar un volumen previamente cifrado por Panda Full Encryption** : se cifrará automáticamente el volumen.
- **Cifrar una unidad descifrada**: si la configuración de Panda Full Encryption implica descifrar las unidades la acción del usuario prevalece y no se descifrará la unidad.

Cifrado y descifrado de discos duros externos y llaves USB

Como el usuario del equipo puede conectar y desconectar medios de almacenamiento externos en cualquier momento, el comportamiento de Panda Full Encryption para este tipo de dispositivos difiere en los puntos siguientes:

- Si el equipo del usuario o servidor no dispone de BitLocker, el agente no descargará los paquetes necesarios, y por lo tanto el dispositivo no se cifrará ni mostrará ningún aviso al usuario.

- Si el equipo dispone de BitLocker, solo se mostrará un mensaje emergente al usuario ofreciendo la posibilidad de cifrarlo en las siguientes situaciones:
    - Cada vez que conecte un dispositivo de almacenamiento USB sin cifrar.
    - Si hay un dispositivo conectado en el equipo y sin cifrar cuando el administrador activa la configuración desde la consola web.
- El mensaje de cifrado se mostrará al usuario durante 5 minutos, transcurridos los cuales dejará de ser visible. Tanto si el usuario acepta el cifrado como si no, el dispositivo podrá ser utilizado de forma normal, a no ser que se haya establecido previamente una configuración que impida el uso de estos dispositivos sin cifrar. Consulta **Escritura en unidades de almacenamiento extraíbles** para más información.
- Cifrar en un dispositivo USB no requiere crear una partición de sistema.
- Si el dispositivo de almacenamiento externo ya está cifrado por otra solución distinta de Panda Full Encryption, al conectarlo al equipo no se mostrará el mensaje de cifrado y se podrá usar con normalidad. Panda Full Encryption no enviará las claves de recuperación a la consola web.
- No se permitirá la escritura en dispositivos USB si está establecida la configuración **Escritura en unidades de almacenamiento extraibles** de Panda Data Control y el dispositivo no ha sido cifrado con BitLocker o con Panda Full Encryption. Consulta **Escritura en unidades de almacenamiento extraíbles** para más información.
- Para descifrar un dispositivo cifrado por Panda Full Encryption el usuario puede utilizar BitLocker de forma manual.
- Solo se cifra el espacio utilizado.
- Todas la particiones del dispositivo se cifran con la misma clave.

Retirar un dispositivo USB cuando el proceso de cifrado no se ha completado puede corromper todo su contenido.

Comportamiento de Panda Full Encryption ante errores

- **Errores en el test de hardware**: el test de hardware se ejecuta cada vez que se inicia el equipo hasta que sea superado, momento en el que el equipo comenzará el cifrado automáticamente.
- **Error al crear la partición de sistema**: muchos errores al crear la partición de sistema son subsanables por el propio usuario del equipo (por ejemplo la falta de espacio).

Periódicamente Panda Full Encryption intentará crear la partición de forma automática.

- **Negativa a activar el chip TPM por parte del usuario**: el equipo mostrará un mensaje en cada proceso de inicio pidiéndole al usuario la activación del chip TPM. Hasta que esta condición no sea resuelta el proceso de cifrado no comenzará.

Proceso para obtener la clave de recuperación

La introduccion de la clave de recuperación es necesaria en los siguientes escenarios:

- **Windows**: cuando el usuario haya perdido el PIN / passphrase / dispositivo USB, o el chip TPM haya detectado un cambio en la cadena de inicio del equipo.
- **macOS**: cuando el usuario haya perdido la contraseña de inicio de sesión o se detecte un cambio en la cadena de inicio del equipo.

Panda Full Encryption almacena todas las claves de recuperación de los equipos de la red cuyo cifrado gestiona, por lo que el administrador puede obtener la clave desde la consola web. Para ello, el administrador necesita los siguientes datos según el sistema operativo instalado en el equipo:

- **Windows**: es necesario el identificador de volumen cifrado (*Recovery Key ID*), que es una cadena de 40 dígitos asociado a cada volumen de datos cifrado.
- **macOS**: es necesario el identificador de la clave de recuperación asociada al equipo. Este identificador es único para todo el equipo e independiente del número de unidades de almacenamiento de que disponga.

Permisos requeridos

Permiso	Tipo de acceso
Acceder a las claves de recuperación de unidades cifradas	Buscar y obtener la clave de recuperación de una unidad cifrada.

Tabla 14.2: Permisos requeridos para obtener la clave de recuperación

Obtener el identificador de volumen cifrado (Windows)

Cuando el usuario no recuerda la contraseña de inicio del equipo o del USB cifrado al que desea acceder, el sistema le mostrará una ventana de aviso:

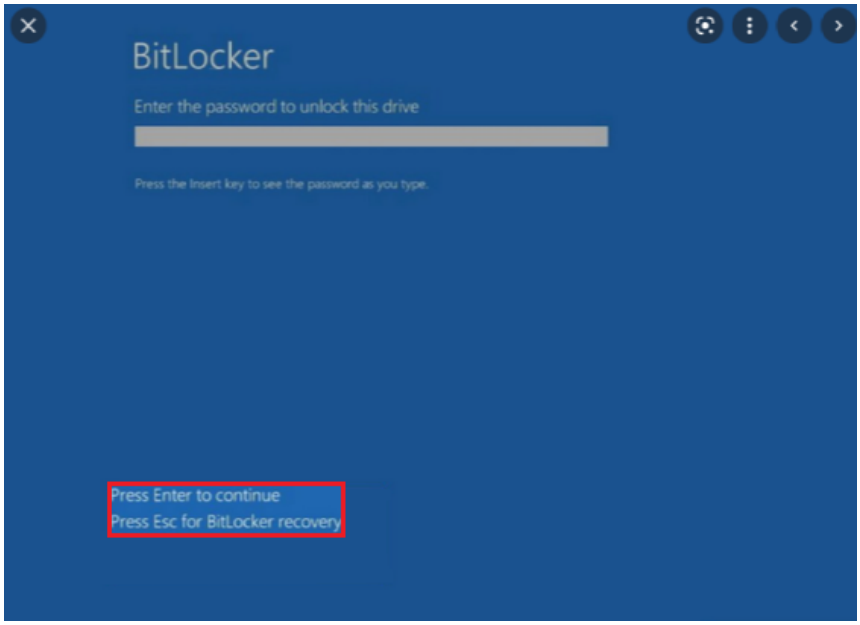


Figura 14.1: Acceso al identificador de volumen cifrado
Figura 14.2:

Al presionar la tecla **Esc**, el usuario accede a la ventana donde se muestra el identificador de volumen cifrado:

Figura 14.3: Identificador de volumen cifrado

Cuando se trata de particiones de disco cifradas, la ventana que se muestra al usuario cuando intenta acceder a la partición es diferente, y en ella solo están visibles los primeros 8 dígitos del identificador de volumen cifrado:

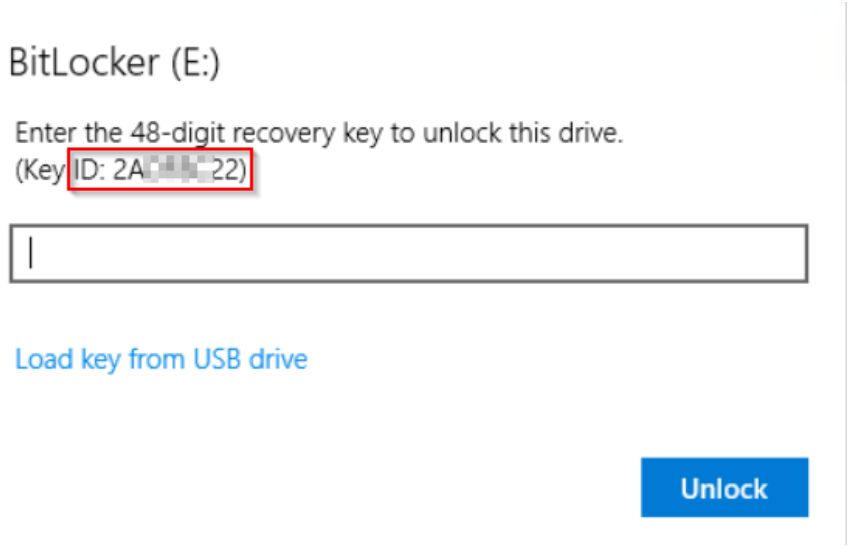


Figura 14.4: Identificador de partición de disco cifrada

Para más información sobre cifrado de volúmenes en los equipos, consulta el apartado ***Proceso de cifrado y descifrado en Windows***.

Obtener el identificador de la clave de recuperación asociada al equipo (macOS)

Al intentar acceder al equipo cifrado, en la pantalla de login se muestra un mensaje que contiene el identificador de la clave de recuperación asociada al equipo, y recomienda contactar con el administrador de la configuración del cifrado.

Obtener la clave de recuperación

- En el menú superior **Equipos** haz clic en el equipo cuya clave quieres recuperar.
- En la pestaña **Detalles**, sección **Protección de datos**, haz clic en el enlace **Obtener la clave de recuperación** (en el caso de cifrado de unidades de almacenamiento extraíbles, utiliza el enlace **Ver dispositivos cifrados en este equipo**).

  Se abrirá una ventana con los identificadores de volumen cifrados almacenados por Aether.
- Haz clic en un identificador. Se abrirá una ventana con la clave de recuperación.
- Copia la clave y envíasela al usuario.

Buscar la clave de recuperación

Si el usuario tiene visibilidad sobre todos los equipos de la cuenta, en los resultados de la búsqueda también se incluirán identificadores de volumen correspondientes a equipos que hayan sido eliminados.

Buscar la clave de recuperación desde el widget Equipos cifrados

- Haz clic en el enlace **Búsqueda de clave de recuperación**.
- Escribe el identificador de volumen cifrado proporcionado por el usuario. Se mostrará la clave de recuperación que el usuario podrá utilizar para acceder al equipo.
- En el caso de los identificadores de volumen cifrado para particiones de disco, escribe los 8 primeros dígitos. Se mostrará la clave de recuperación que el usuario podrá utilizar para acceder a la partición de disco bloqueada.

> *Puede darse el caso de que los 8 dígitos iniciales sean los mismos para más de una clave de recuperación, en cuyo caso se mostrarán todas ellas en los resultados de la búsqueda.*

Buscar la clave de recuperación desde el detalle del equipo

- En el menú superior **Equipos** haz clic en el equipo cuyas claves quieres recuperar.
- En la pestaña **Detalles**, sección **Protección de datos**, haz clic en el enlace **Obtener la clave de recuperación** (en el caso de cifrado de unidades de almacenamiento extraíbles, utiliza el enlace **Ver dispositivos cifrados en este equipo**).

  Se abrirá una ventana con los identificadores de volumen cifrados almacenados por Aether.
- Haz clic en el enlace **Buscar otra clave** e introduce el identificador de volumen cifrado.

Paneles / widgets del módulo Panda Full Encryption

Acceso al panel de control

Para acceder haz clic en el menú superior **Estado**, panel lateral Panda Full Encryption.

Permisos requeridos

No se necesitan permisos adicionales para acceder a los widgets asociados a **Panda Full Encryption**.

Estado del cifrado

Muestra el total de equipos compatibles con Panda Full Encryption así como su estado con respecto a la tecnología de cifrado.

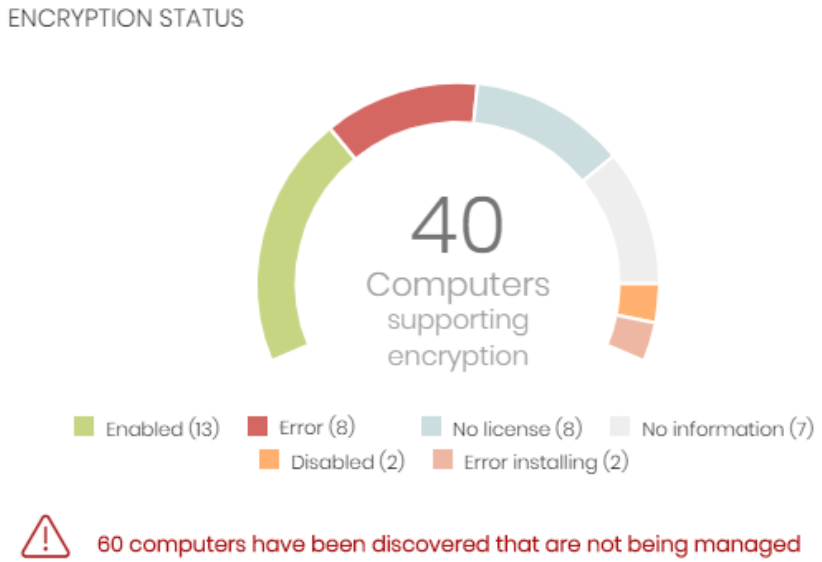


Figura 14.5: Panel de Estado del cifrado

Significado de las series

Serie	Descripción
Activado	Equipos con Panda Full Encryption instalado, con una configuración que indica cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Desactivado	Equipos con Panda Full Encryption instalado, con una configuración que indica no cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Error	No se ha podido realizar la acción que el administrador ha indicado en la configuración de cifrado o descifrado.
Error instalando	No se ha podido descargar e instalar BitLocker si fue necesario.
Sin licencia	Equipo compatible con Panda Full Encryption pero sin licencia de Panda Endpoint Protection asignada.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con un agente sin actualizar.

Tabla 14.3: Descripción de la serie Estado del cifrado

Filtros preestablecidos desde el panel

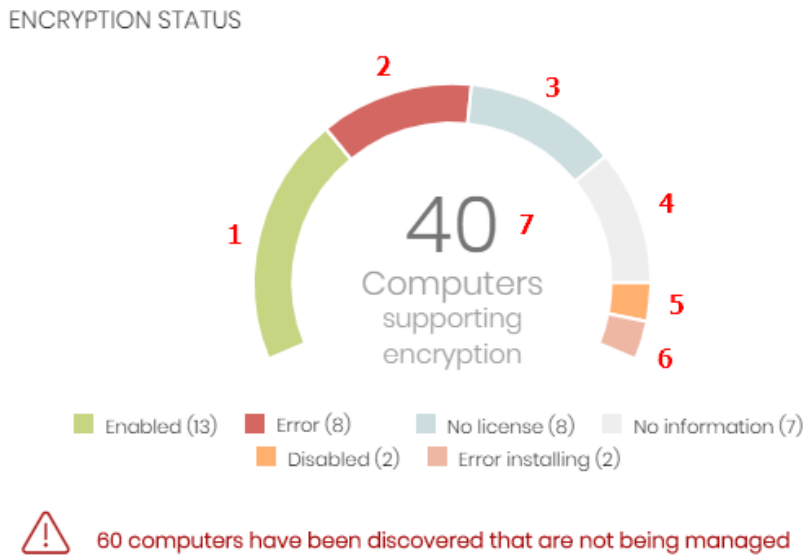


Figura 14.6: Zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado del cifrado** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado del cifrado = Activado.
(2)	Estado del cifrado = Error.
(3)	Estado del cifrado = Sin licencia. El equipo no tiene asignada licencia de Panda Endpoint Protection.
(4)	Estado del cifrado = Sin información.
(5)	Estado del cifrado = Desactivado.
(6)	Estado del cifrado = Error instalando.
(7)	Sin filtros.

Tabla 14.4: Definición de filtros del listado Estado del cifrado

Equipos compatibles con cifrado

Muestra los equipos compatibles y no compatibles con la tecnología de filtrado agrupados en series según su tipo.

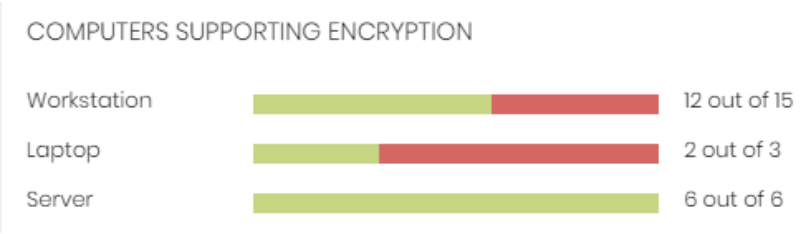


Figura 14.7: Panel de Equipos compatibles con cifrado

Significado de las series

Serie	Descripción
Estación - verde	Dispositivos de tipo estación compatibles con cifrado.
Estación - rojo	Dispositivos de tipo estación no compatibles con cifrado.
Portátil - verde	Dispositivos de tipo portátil compatibles con cifrado.
Portátil - rojo	Dispositivos de tipo portátil no compatibles con cifrado.
Servidor - verde	Dispositivos de tipo servidor compatibles con cifrado.
Servidor - rojo	Dispositivos de tipo servidor no compatibles con cifrado.

Tabla 14.5: Descripción de la serie Equipos compatibles con cifrado

Filtros preestablecidos desde el panel

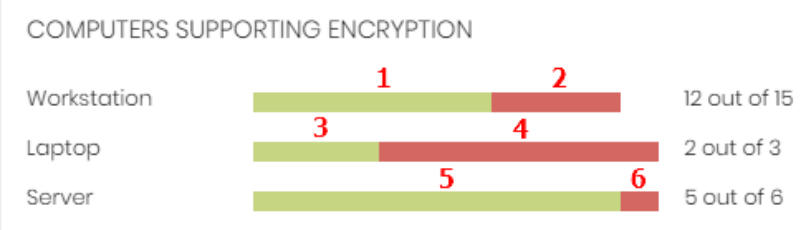


Figura 14.8: Zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado del cifrado** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Tipo de equipo = Estación.
(2)	Listado de equipos con filtro **No compatibles con cifrado.**

Zona activa	Filtro
(3)	Tipo de equipo = Portátil.
(4)	Listado de equipos con filtro **No compatibles con cifrado.**
(5)	Tipo de equipo = Servidor.
(6)	Listado de equipos con filtro **No compatibles con cifrado.**

Tabla 14.6: Definición de filtros del listado Estado del cifrado

Equipos cifrados

Muestra el estado del proceso de cifrado en los equipos de la red compatibles con Panda Full Encryption.

Para saber más sobre el proceso de búsqueda de claves de recuperación, consulta el apartado ***Proceso para obtener la clave de recuperación****.*

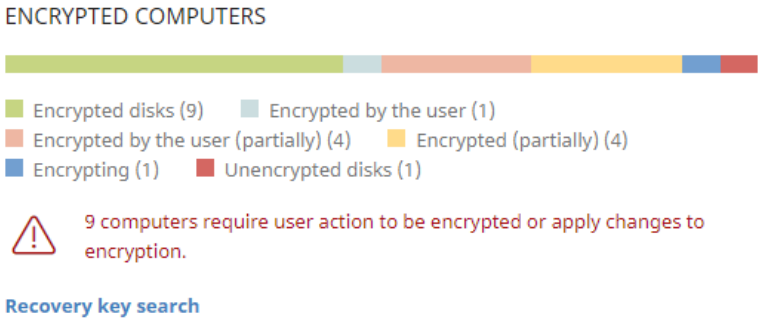


Figura 14.9: Panel Equipos cifrados

Significado de las series

Serie	Descripción
Desconocido	Medios de almacenamiento cifrados con un método de autenticación no soportado por Panda Full Encryption.
Discos no cifrados	Ninguno de los medios de almacenamiento del equipo están cifrados ni por el usuario ni por Panda Full Encryption.
Discos cifrados	Todos los medios de almacenamiento del equipo están cifrados por

Serie	Descripción
	Panda Full Encryption.
Cifrando	Al menos un medio de almacenamiento del equipo está en proceso de cifrado.
Descifrando	Al menos un medio de almacenamiento del equipo está en proceso de descifrado.
Cifrado por el usuario	Todos los medios de almacenamiento se encuentran cifrados pero alguno de ellos o todos fueron cifrados por el usuario.
Cifrado por el usuario (parcialmente)	Alguno de los medios de almacenamiento se encuentran cifrados por el usuario y el resto permanece sin cifrar o está cifrado por Panda Full Encryption.
Cifrado (parcialmente)	Al menos uno de los medios de almacenamiento del equipo está cifrado por Panda Full Encryption pero el resto permanece sin cifrar.

Tabla 14.7: Descripción de la serie Equipos cifrados

Filtros preestablecidos desde el panel

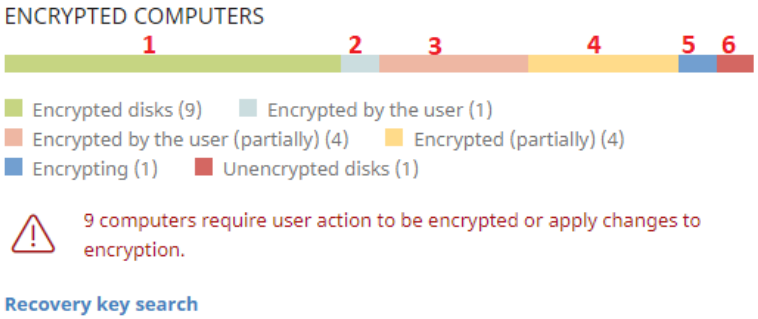


Figura 14.10: Zonas activas del panel Equipos Cifrados

Al hacer clic en las zonas indicadas en **Zonas activas del panel Equipos Cifrados** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Cifrado de discos = Discos cifrados.
(2)	Cifrado de discos = Cifrado por el usuario.

Zona activa	Filtro
(3)	Cifrado de discos = Cifrado por el usuario (parcialmente).
(4)	Cifrado de discos = Cifrado (parcialmente).
(5)	Cifrado de discos = Cifrando.
(6)	Cifrado de discos = Discos no cifrados.
(7)	Cifrado de discos = Descifrando.
(8)	Cifrado de discos = Desconocido.

Tabla 14.8: Definición de filtros del listado Estado del cifrado

Métodos de autenticación aplicados

Muestra los equipos con el cifrado configurado en la red, agrupados por el tipo de autenticación elegido. Consulta los tipos de autenticación compatibles en **Características generales de Panda Full Encryption**.

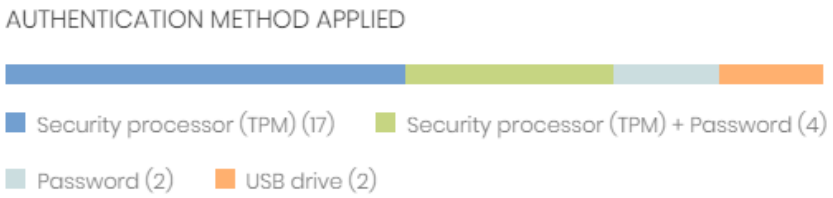


Figura 14.11: Panel Métodos de autenticación

Significado de las series

Serie	Descripción
Desconocido	El método de autenticación elegido por el usuario del equipo no está soportado por Panda Full Encryption.
Procesador de seguridad (TPM)	El método de autenticación utilizado es TPM.
Procesador de seguridad (TPM) + Contraseña	El método de autenticación utilizado es TPM y PIN o passphrase solicitado en el inicio del equipo.
Contraseña	• **Equipos Windows**: el método de autenticación elegido es PIN

Serie	Descripción
	o passphrase solicitado en el inicio del equipo. • **Equipos Mac**: el método de autenticación aplicado es la contraseña solicitada en el inicio del equipo.
USB	El método de autenticación elegido es dispositivo USB conectado en el arranque del equipo.
Sin cifrar	Ninguno de los dispositivos de almacenamiento del equipo está cifrado.

Tabla 14.9: Descripción de la serie Métodos de autenticación aplicado

Filtros preestablecidos desde el panel

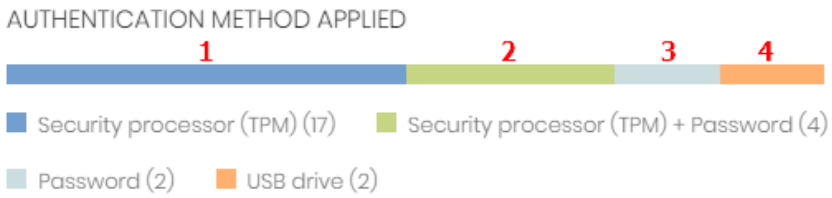


Figura 14.12: Zonas activas del panel Métodos de autenticación aplicado

Al hacer clic en las zonas indicadas en **Zonas activas del panel Métodos de autenticación aplicado** se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Método de autenticación = Procesador de seguridad (TPM)
(2)	Método de autenticación= Procesador de seguridad (TPM) + Contraseña
(3)	Método de autenticación = Contraseña
(4)	Método de autenticación = USB
(5)	Método de autenticación = Desconocido
(6)	Método de autenticación = Sin cifrar

Tabla 14.10: Definición de filtros del listado

Listados en Panda Full Encryption

Acceso a los listados

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Panda Full Encryption** y en el widget relacionado.

  ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Protección de datos** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

El acceso al listado **Estado del cifrado** no requiere permisos adicionales para el administrador.

Estado del cifrado

Este listado muestra todos los equipos de la red gestionados por Panda Endpoint Protection y compatibles con Panda Full Encryption. Incorpora filtros relativos al módulo para controlar el estado del cifrado en el parque informático.

Campo	Comentario	Valores
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Estado del equipo	Reinstalación del agente: • Reinstalando agente. • Error en la reinstalación del agente. Reinstalación de la protección: • Reinstalando la protección. • Error en la reinstalación de la protección. • Pendiente de reinicio. Estado de aislamiento del equipo: • Equipo en proceso de entrar en aislamiento.	Icono

Campo	Comentario	Valores
	• Equipo aislado. • Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP: • Equipo en modo contención de ataque RDP. • Finalizando modo de contención de ataque RDP.	
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo y versión instalada en el equipo de usuario o servidor.	Cadena de caracteres
Cifrado de discos duros	Estado del módulo Panda Full Encryption.	• Sin información • Activado • Desactivado • Error • Error instalando • Sin licencia
Estado de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario • Cifrado por el usuario (parcialmente) • Cifrado

Campo	Comentario	Valores
		(parcialmente)
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Sin cifrar
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha

Tabla 14.11: Campos del listado Estado de cifrado

Para visualizar los datos del listado gráficamente accede al widget ***Equipos cifrados***

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de

Campo	Comentario	Valores
		caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres¡
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Panda.	Cadena de caracteres
Fecha de instalación	Fecha en la que el software Panda Endpoint Protection se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión		Fecha
Plataforma	Sistema operativo instalado en el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	El módulo de la protección instalado en el equipo es la última versión publicada.	Booleano
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Booleano
Fecha de la ultima actualización	Fecha de la descarga del fichero de firmas.	Fecha

Campo	Comentario	Valores
Cifrado de discos duros	Estado del módulo Panda Full Encryption.	• Sin información • Activado • Desactivado • Error • Error instalando • Sin licencia
Estados de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario • Cifrado (parcialmente) • Cifrado por el usuario (parcialmente)
Acciones de cifrado pendientes del usuario	El usuario tiene pendiente introducir información o reiniciar el equipo para completar el proceso de cifrado de los volúmenes.	Booleano
Métodos de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB

Campo	Comentario	Valores
		• Sin cifrar
Fecha de cifrado	Fecha del volumen más antiguo cifrado dentro de la primera que vez se consideró al equipo como completamente cifrado (se cifraron todos sus volúmenes compatibles).	Fecha
Versión de especificación del TPM	Versión de las especificaciones TPM soportadas por el chip incluido en el equipo.	Cadena de caracteres
Fecha error instalación cifrado	Fecha del último error de instalación reportado.	Fecha
Error instalación cifrado	Se ha producido un error al instalar el módulo Panda Full Encryption en el equipo.	Cadena de caracteres
Fecha error cifrado	Última fecha en la que se reportó un error de cifrado en el equipo.	
Error cifrado	El proceso de cifrado devolvió un error.	Cadena de caracteres

Tabla 14.12: Campos del fichero exportado

Herramienta de filtrado

Campo	Comentario	Valores
Fecha de cifrado desde	Límite inferior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Fecha de cifrado hasta	Límite superior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows

Campo	Comentario	Valores
		• macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Estado de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario • Cifrado (parcialmente) • Cifrado por el usuario (parcialmente)
Cifrado de discos duros	Estado del módulo Panda Full Encryption.	• Sin información • Activado • Desactivado • Error • Error Instalando • Sin licencia
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña

Campo	Comentario	Valores
		• Contraseña • USB • Ninguno
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	Fecha
Acciones de cifrado pendientes del usuario	Indica si el proceso de cifrado está a la espera de acciones por parte del usuario.	• Todos • Si • No

Tabla 14.13: Campos de filtrado para el listado

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta Información de equipo en la página 251 para obtener más información.

Configuración del cifrado

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Cifrado**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Configurar cifrado de equipos.	Crear, modificar, borrar, copiar o asignar las configuraciones de Cifrado.
Ver configuraciones de cifrado de equipos	Visualizar las configuraciones de Cifrado.

Tabla 14.14: Permisos requeridos para acceder a la configuración de Cifrado

Opciones de configuración de Panda Full Encryption

Cifrar todos los discos duros de los equipos

Indica si los dispositivos de almacenamiento interno del equipo serán cifrados o no. Dependiendo del estado anterior del equipo, el comportamiento de Panda Full Encryption será diferente:

- Si el equipo está cifrado por Panda Full Encryption y se deshabilita **Cifrar todos los discos duros de los equipos**, se descifrarán todos los volúmenes cifrados.
- Si el equipo está cifrado pero no por Panda Full Encryption y se deshabilita **Cifrar todos los discos duros de los equipos** los volúmenes no sufren ningún cambio.
- Si el equipo está cifrado pero no por Panda Full Encryption y se habilita **Cifrar todos los discos duros de los equipos** se adecuará la configuración interna de cifrado para que coincida con los métodos soportados en Panda Full Encryption evitando volver a cifrar el volumen. Consulta **Cifrado de volúmenes ya cifrados previamente** para más información.

  Si se trata de un equipo con sistema operativo macOS, se generará una clave de recuperación nueva. Consulta **Proceso de cifrado y descifrado para macOS**
- Si el equipo no está cifrado y se habilita **Cifrar todos los discos duros de los equipos** se cifrarán todos los volúmenes. Consulta **Proceso de cifrado y descifrado en Windows** y **Proceso de cifrado y descifrado para macOS**.

Solicitar una contraseña para acceder al equipo (Windows)

Habilita la autenticación por contraseña en el arranque del equipo. Dependiendo de la plataforma y de la existencia de hardware TPM se permitirá el uso de dos tipos de contraseña:

- **Equipos con TPM**: se pedirá una contraseña de tipo PIN.
- **Equipos sin TPM**: se pedirá una contraseña de tipo passphrase.

Si estableces esta configuración a No y el equipo no tiene acceso a un procesador de seguridad TPM compatible, sus medios de almacenamiento no se cifrarán.

No cifrar los equipos que requieren un USB para autenticarse (Windows)

Para evitar la utilización de dispositivos USB soportados por Panda Full Encryption en la autenticación, el administrador puede deshabilitar su uso.

Solo los equipos Windows 7 sin TPM están en posición de utilizar el método de autenticación por USB. Si el administrador deshabilita el uso de USBs, estos equipos no serán cifrados.

Cifrar sólo el espacio utilizado (Windows)

El administrador puede minimizar el tiempo de cifrado empleado restringiendo la protección a los sectores del disco duro que están siendo utilizados. Los sectores liberados tras borrar un fichero continuarán cifrados pero el espacio libre previo al cifrado del disco duro permanecerá sin cifrar, siendo accesible por terceros mediante herramientas de recuperación de ficheros borrados.

Ofrecer cifrado de unidades de almacenamiento extraíbles (Windows)

Muestra al usuario una ventana con la posibilidad de cifrar los medios de almacenamiento masivo externos y llaves USB cuando los conecta al equipo. Consulta **Cifrado y descifrado de discos duros externos y llaves USB** para obtener más información acerca del comportamiento y los requisitos de esta configuración.

Filtros disponibles

Para localizar los equipos de la red que coincidan con alguno de los estados de cifrado definidos en Panda Full Encryption utiliza los recursos del árbol de filtros mostrados en **Árbol de filtros** en la página **212** con los campos mostrados a continuación:

- Cifrado:
    - Acciones de cifrado pendientes del usuario.
    - Cifrado de discos.
    - Fecha de cifrado.
    - Método de autenticación.
    - Tiene acciones pendientes de cifrado del usuario.
- Configuración:
    - Cifrado.
- Equipo:
    - Tiene TPM.
- Hardware:
    - TPM - Activado.
    - TPM - Fabricante.
    - TPM - Propietario.
    - TPM - Versión.
    - TPM - Versión de especificación.
- Módulos:
    - Cifrado.

Capítulo 15

Visibilidad del malware y del parque informático

Panda Endpoint Protection ofrece al administrador tres grandes grupos de herramientas para visualizar el estado de la seguridad y del parque informático que gestiona:

- El panel de control, con información actualizada en tiempo real.
- Listados personalizables de incidencias, malware detectado y dispositivos gestionados junto a su estado.
- Informes con información del estado del parque informático, recogida y consolidada a lo largo del tiempo.

*Los informes consolidados se tratan en **Envío programado de informes y listados** en la página **577** para más información.*

Las herramientas de visualización y monitorización determinan en tiempo real el estado de la seguridad de la red y el impacto de las brechas de seguridad que se puedan producir para facilitar la adopción de las medidas de seguridad apropiadas.

Contenido del capítulo

Paneles/Widgets del módulo de seguridad

Panda Endpoint Protection muestra mediante widgets el estado de la seguridad del parque informático, o de un equipo concreto:

- **Parque informático**: haz clic en el menú superior **Estado** y en el menú lateral **Seguridad** .Se mostrarán los contadores relativos a la seguridad de los equipos visibles para el administrador. Consulta **Gestión de roles y permisos** en la página **66** para establecer los grupos de equipos que serán visibles para la cuenta que accede a la consola de administración, e **Icono Filtro por grupo** en la página **33** para restringir la visibilidad de los grupos ya establecida en el rol.
- **Equipo**: haz clic en el menú superior **Equipos**, elige un equipo de la red y haz clic en la pestaña **Detecciones**. Se mostrarán los contadores relativos a la seguridad del equipo seleccionado. Consulta **Sección Detecciones (4) en Windows, Linux y macOS** en la página **272**.

A continuación, se detallan los distintos widgets implementados en el dashboard de Panda Endpoint Protection, las distintas áreas y zonas activas incorporadas y los tooltips y su significado.

Estado de protección

Muestra los equipos donde Panda Endpoint Protection funciona correctamente y aquellos con errores y problemas en la instalación o en la ejecución del módulo de protección. El estado de los equipos es representado mediante un círculo con distintos colores y contadores asociados.

En la parte inferior del widget se indica el número de equipos que se encuentran en modo auditoría, si los hubiera. Para más información, consulta **Modo auditoría**

> *La suma de los porcentajes de las diferentes series puede resultar más de un 100% debido a que los estados no son mutuamente excluyentes, y un mismo equipo puede encontrarse en varias series a la vez.*

El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

> *Los dispositivos iOS se suman al total de equipos y dispositivos de la parte central del widget, pero sus datos no se incluyen, dado que en el caso de iOS no se dispone de protección avanzada ni antivirus. Para más información, consulta **Configuración de dispositivos iOS** en la página **342***

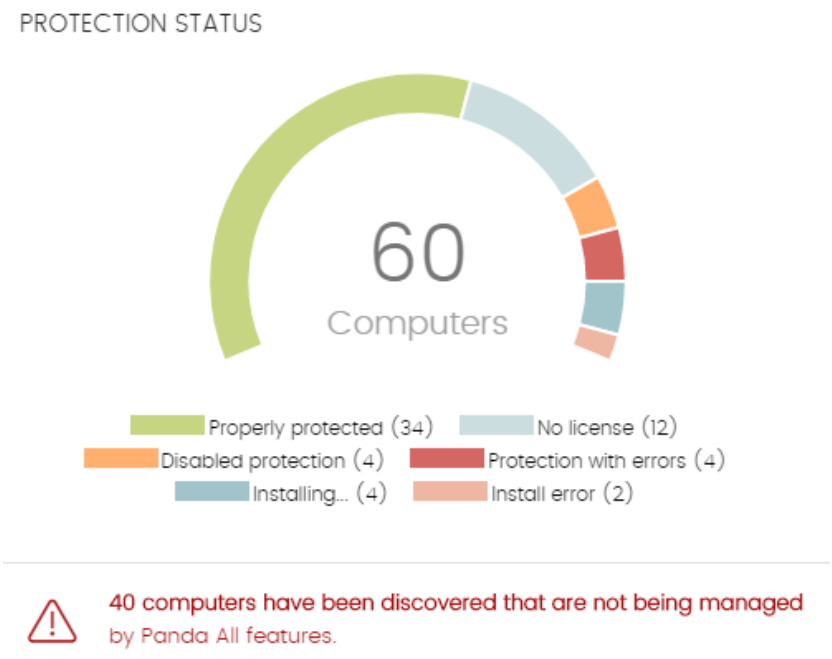


Figura 15.1: Panel de Estado de protección

Descripción de las series

Serie	Descripción
Correctamente protegido	Porcentaje de equipos en los que Panda Endpoint Protection se instaló sin errores y su ejecución no presenta problemas.
Instalando...	Porcentaje de equipos en los que Panda Endpoint Protection se encuentra en proceso de instalación.
Sin licencia	Equipos sin protección por la falta de suficientes licencias, o por no haberse asignado una licencia disponible.
Protección desactivada	Equipos sin activar la protección antivirus.
Protección con error	Equipos con Panda Endpoint Protection instalado cuyo módulo de protección no responde a las peticiones desde los servidores de Panda Security.
Error instalando	Equipos cuya instalación no se pudo completar.

Serie	Descripción
Parte central	Equipos con un agente Panda instalado.

Tabla 15.1: Descripción de la serie Equipos desprotegidos

Filtros preestablecidos desde el panel

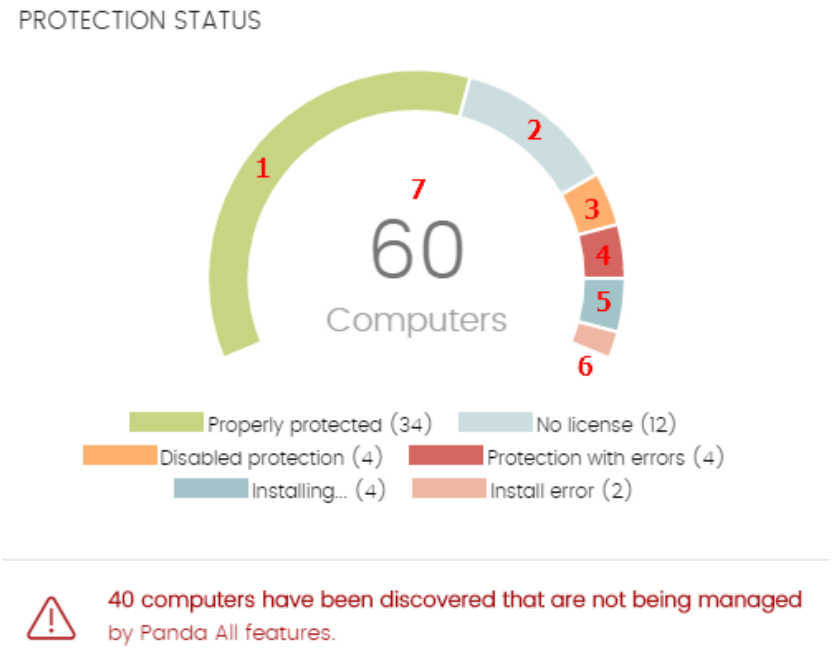


Figura 15.2: Zonas activas del panel Estado de protección

Haz clic en las zonas indicadas en **Zonas activas del panel Estado de protección** para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de protección = Correctamente protegido.
(2)	Estado de protección = Instalando…
(3)	Estado de protección = Protección desactivada.
(4)	Estado de protección = Protección con error.
(5)	Estado de protección = Sin licencia.
(6)	Estado de protección = Error instalando.

Zona activa	Filtro
(7)	Sin filtro.

Tabla 15.2: Definición de filtros del listado Estado de protección de los equipos

Equipos sin conexión

Muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

Figura 15.3: Panel Equipos sin conexión

Descripción de las series

Serie	Descripción
72 horas	Número de equipos que no enviaron su estado en las últimas 72 horas.
7 días	Número de equipos que no enviaron su estado en las últimas 7 días.
30 días	Número de equipos que no enviaron su estado en las últimas 30 días.

Tabla 15.3: Descripción de la serie Equipos sin conexión

Filtros preestablecidos desde el panel

Figura 15.4: Zonas activas del panel Equipos sin conexión

Haz clic en las zonas indicadas en **Zonas activas del panel Equipos sin conexión** para abrir el listado **Equipos sin conexión** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 72 horas.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 15.4: Definición de los filtros del listado Equipos sin conexión

Protección desactualizada

Muestra los equipos cuya última versión del fichero de firmas instalada difiere en más de 3 días del fichero publicado por Panda Security. También muestra los equipos cuya versión del motor de protección difiere en más de 7 días del publicado por Panda Security. Por lo tanto, estos equipos pueden ser vulnerables frente a los ataques de amenazas.

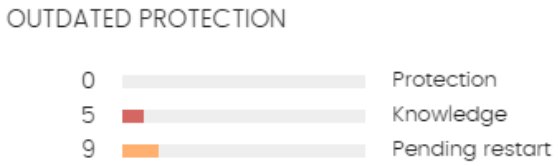


Figura 15.5: Panel Protección desactualizada

Descripción de las series

El panel muestra el porcentaje y el número de equipos vulnerables por estar desactualizados, divididos en tres conceptos:

Serie	Descripción
Protección	Desde hace 7 días el equipo tiene un motor de protección instalado anterior a la última versión publicada por Panda Security.
Conocimiento	Desde hace 3 días el equipo no se actualiza con el fichero de firmas publicado.
Pendiente de reinicio	El equipo requiere un reinicio para completar la actualización.

Tabla 15.5: Descripción de la serie Protección desactualizada

Filtros preestablecidos desde el panel

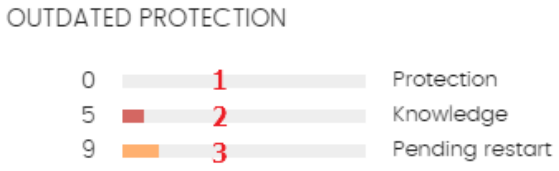


Figura 15.6: Zonas activas del panel Protección desactualizada

Haz clic en las zonas indicadas en **Zonas activas del panel Protección desactualizada**para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = No.
(2)	Conocimiento = No.
(3)	Protección actualizada = Pendiente de reinicio.

Tabla 15.6: Definición de los filtros del listado Equipos con protección desactualizada

Amenazas detectadas por el antivirus

Consolida todos los intentos de intrusión que Panda Endpoint Protection gestionó en el periodo de tiempo establecido.

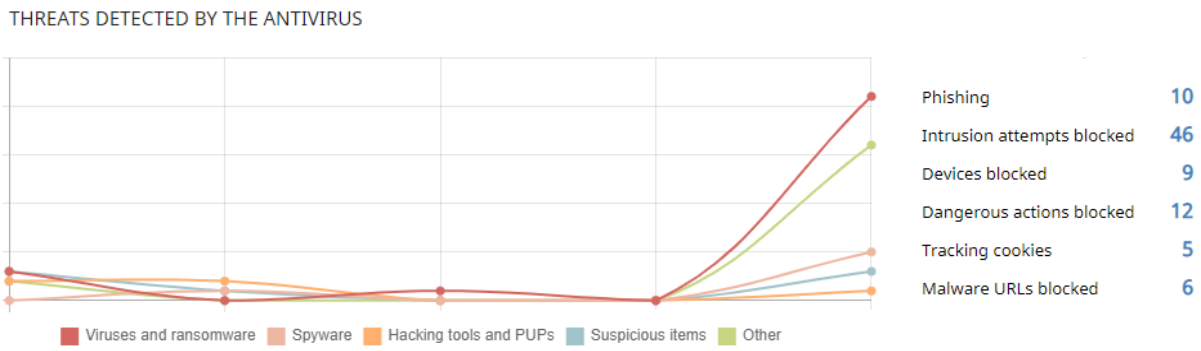


Figura 15.7: Panel Amenazas detectadas por el antivirus

Los datos reflejados abarcan todos los vectores de infección y todas las plataformas soportadas, de manera que el administrador pueda disponer de información concreta (volumen, tipo, forma de ataque) relativa a la llegada de malware a la red, durante el intervalo de tiempo determinado.

Descripción de las series

Este panel está formado por dos secciones: un gráfico de líneas y un listado resumen.

El diagrama de líneas representa las detecciones encontradas en el parque informático a lo largo del tiempo separadas por tipo de malware:

Serie	Descripción
Virus y Ransomware	Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.
Herramientas de hacking y PUPs	Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.
Sospechosos	Fichero con una alta probabilidad de ser malware tras ser analizado por las tecnologías heurísticas. Este tipo de tecnologías solo se utilizan en los análisis bajo demanda, efectuados desde tareas programadas. En este tipo de análisis, el fichero investigado no se ejecuta, y por tanto el software de seguridad dispone de mucha menos cantidad de información para evaluar su comportamiento, con lo que la fiabilidad de la clasificación es menor. Para compensar esta menor fiabilidad del análisis estático, se utilizan las tecnologías heurísticas.
Phishing	Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.
Otros	Hoax, Worms, Troyanos y otros tipos de virus.

Tabla 15.7: Descripción de la serie Amenazas detectadas por el antivirus

El listado de la derecha muestra los eventos relevantes que requieren una supervisión por parte del administrador en busca de síntomas o situaciones potenciales de peligro.

Serie	Descripción
Acciones peligrosas bloqueadas	Detecciones realizadas por análisis del comportamiento local.
Intentos de intrusión	Detección de tráfico de red mal formado cuyo objetivo es provocar un error de ejecución en algún componente del equipo que origine un

Serie	Descripción
bloqueados	comportamiento indeseado en el sistema.
Dispositivos bloqueados	Intento de uso por parte del usuario del equipo de un dispositivo restringido según la configuración establecida por el administrador de la red en el módulo Control de dispositivos.
Tracking cookies	Cookies detectadas para registrar la navegación de los usuarios.
URL con malware bloqueadas	Direcciones Web que apuntaban a páginas con malware.

Tabla 15.8: Descripción de la serie Amenazas detectadas por el antivirus

Filtros preestablecidos desde el panel

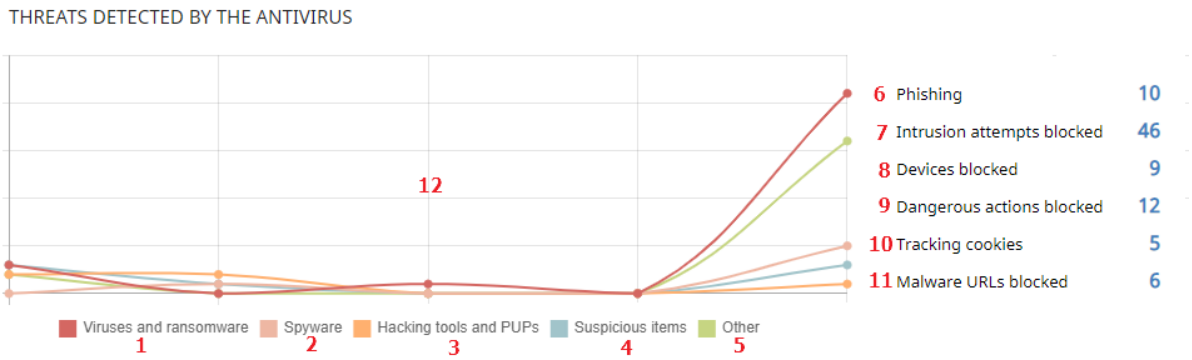


Figura 15.8: Zonas activas del panel Amenazas detectadas por el antivirus

Haz clic en las zonas indicadas en **Zonas activas del panel Amenazas detectadas por el antivirus** para abrir el listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Amenazas detectadas por el antivirus	Tipo de amenaza = Virus y Ransomware
(2)	Amenazas detectadas por el antivirus	Tipo de amenaza = Spyware.
(3)	Amenazas detectadas por el antivirus	Tipo de amenaza = Herramientas de hacking y PUPs.

Zona activa	Listado	Filtro
(4)	Amenazas detectadas por el antivirus	Tipo de amenaza = Sospechosos.
(5)	Amenazas detectadas por el antivirus	Tipo de amenaza = Otros.
(6)	Amenazas detectadas por el antivirus	Tipo de amenaza = Phishing.
(7)	Intentos de intrusión bloqueados	Sin filtro.
(8)	Dispositivos bloqueados	Sin filtro.
(9)	Amenazas detectadas por el antivirus	Tipo de amenaza = Acciones peligrosas bloqueadas.
(10)	Amenazas detectadas por el antivirus	Tipo de amenaza = Tracking cookies.
(11)	Amenazas detectadas por el antivirus	Tipo de amenaza = URLs con malware.
(12)	Amenazas detectadas por el antivirus	Sin filtro.

Tabla 15.9: Definición de los filtros del listado Amenazas detectadas por el antivirus

Listados del módulo de seguridad

Los listados de seguridad muestran la información de la actividad relativa a la protección de los equipos de la red recogida por Panda Endpoint Protection, y cuentan con un grado de detalle muy alto al contener la información en bruto utilizada para generar los widgets.

Para acceder a los listados de seguridad elige uno de los dos procedimientos mostrados a continuación:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad** y en widget para abrir su listado asociado. Dependiendo del lugar donde se haga clic dentro del widget se aplicará un filtro

distinto asociado al listado.

o

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana donde se muestran todos los listados disponibles en Panda Endpoint Protection.
- Haz clic en un listado de la sección **Seguridad**. Se mostrara el listado apropiado sin filtros establecidos.

Al hacer clic en una entrada del listado se mostrará la ventana de detalle, que se ajustará al tipo de información mostrada.

Estado de protección de los equipos

Muestra en detalle todos los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles que no estén protegidos por alguno de los conceptos mostrados en el panel asociado.

Para garantizar el buen funcionamiento de la protección, los equipos de la red deben comunicarse con la nube de Panda Security. Consulta el listado de URLs accesibles desde los equipos en **Acceso a URLs del servicio** en la página **637**.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Estado del equipo	Reinstalación del agente: • Reinstalando agente. • Error en la reinstalación del agente. Reinstalación de la protección: • Reinstalando la protección. • Error en la reinstalación de la protección. • Pendiente de reinicio. Modo Contención de ataque RDP: • Equipo en modo contención de	Icono

Campo	Descripción	Valores
	ataque RDP. • Finalizando modo de contención de ataque RDP.	
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres • Grupo Todos • Grupo nativo • Grupo Directorio activo
Antivirus	Estado de la protección antivirus	• Instalando • Error. Si es conocido se mostrará su origen, si es desconocido se mostrará el código de error • Activado • Desactivado • Sin licencia
Protección actualizada	El módulo de la protección instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se muestra la versión de la protección instalada.	• Actualizado • No actualizado (7 días sin actualizar desde la publicación) • Pendiente de reinicio.
Conocimiento	El fichero de firmas descargado en el equipo coincide con la última versión publicada o no.	• Actualizado • No actualizado (3

Campo	Descripción	Valores
	Al pasar el puntero del ratón por encima del campo se muestra la fecha de actualización de la versión descargada.	días sin actualizar desde la publicación)
Conexión con conocimiento	Indica si el equipo es capaz de comunicarse con la nube de Aetherpara enviar los eventos monitorizados y descargar la inteligencia de seguridad.	• Conexión correcta • Uno o varios servicios no son accesibles • Información no disponible
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	Fecha

Tabla 15.10: Campos del listado Estado de protección de los equipos

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres

Campo	Descripción	Valores
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Panda.	Cadena de caracteres
Fecha instalación	Fecha en la que el Software Panda Endpoint Protection se instaló con éxito en el equipo.	Fecha
Fecha de la última actualización	Fecha de la última actualización del agente.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	El módulo de la protección instalado en el equipo es la última versión publicada.	Binario
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Binario
Fecha de última	Fecha de la descarga del fichero de	Fecha

Campo	Descripción	Valores
actualización	firmas.	
Antivirus de archivos Antivirus para navegación web FirewallControl de dispositivos Antirrobo	Estado de la protección asociada.	• **No instalado** • **Error**: si es conocido se mostrará su origen, si es desconocido se mostrará el código de error • **Activado** • **Desactivado** • **Sin licencia**
Fecha de error	Se produjo un error en la instalación de Panda Endpoint Protection en la fecha y hora indicadas.	Fecha
Error instalación	Descripción del error producido en la instalación de Panda Endpoint Protection en el equipo.	Cadena de caracteres
Código error instalación	Muestra código que permite detallar el error producido durante la instalación.	Los códigos se muestran separados por ";": • Código de error • Código extendido error • Subcódigo extendido error
Otros productos de seguridad	Nombre del antivirus de terceros fabricantes encontrado en el equipo en el momento de la instalación de Panda Endpoint Protection.	Cadena de caracteres

Campo	Descripción	Valores
Conexión para inteligencia colectiva	Muestra el estado de la conexión del equipo con los servidores que almacenan los ficheros de firmas y la inteligencia de seguridad.	• Correcta • Con problemas

Tabla 15.11: Campos del fichero exportado Estado de protección de los equipos

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Endpoint Protection a la nube de Panda Security.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Protección actualizada	La protección instalada coincide con la última versión publicada o no.	• Todos • Si • No

Campo	Descripción	Valores
		• Pendiente de reinicio
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android
Conocimiento actualizado	Indica si el fichero de firmas encontrado en el equipo es o no el último publicado.	Binario
Conexión con servidores de conocimiento	Indica si el equipo es capaz de comunicarse con la nube de Aetherpara enviar los eventos monitorizados y descargar la inteligencia de seguridad.	• **Todos** • **Correcta** • **Con problemas**: uno o varios servicios no son accesibles
Estado de protección	Estado del módulo de protección instalado en el equipo.	• Instalando... • Correctamente protegido • Protección con error • Protección desactivada • Sin licencia • Error instalando
Modo "Contención de ataque RDP"	Estado del modo de Contención de ataque RDP.	• Todos • No • Si

Tabla 15.12: Campos de filtrado para el listado Estado de protección de los equipos

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Para obtener más información, consulta **Información de equipo** en la página **251**.

Amenazas detectadas por el antivirus

El listado de detecciones ofrece información consolidada y completa de todas las detecciones realizadas en todas las plataformas soportadas y desde todos los vectores de infección analizados, utilizados por los hackers para intentar infectar equipos en la red.

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que perte-nece el equipo.	Cadena de caracteres • Grupo Todos • Grupo nativo • Grupo Directorio activo
Tipo de amenaza	Clase de la amenaza detectada.	• Virus y ransomware • Spyware • Herramientas de hacking y PUPs • Phising • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware • Otros.

Campo	Descripción	Valores
Ruta	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Acción	Acción desencadenada por Panda Endpoint Protection.	• Borrado • Desinfectado • Movido a cuarentena • Bloqueado • Proceso terminado • Permitido (modo auditoría)
Fecha	Fecha de la detección.	Fecha

Tabla 15.13: Campos del listado Amenazas detectadas por el antivirus

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Nombre malware	Nombre de la amenaza detectada.	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza detectada.	• Virus y ransomware

Campo	Descripción	Valores
		• Spyware • Herramientas de hacking y PUPs • Phising • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware • Otros
Tipo de malware	Subclase de la amenaza detectada.	Cadena de caracteres
Acción	Acción desencadenada por Panda Endpoint Protection.	• Movido a cuarentena • Borrado • Bloqueado • Proceso terminado • Permitido (modo auditoría)
Detectado por	Motor que detectó la amenaza.	• Control de dispositivos • Protección de ficheros • Firewall • Protección de correo • Análisis bajo demanda

Campo	Descripción	Valores
		• Protección Web
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Excluido	La amenaza ha sido excluida del análisis por el administrador para permitir su ejecución.	Binario
Fecha	Fecha de la detección.	Fecha
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo donde se realizó la detección.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador de la red.	Cadena de caracteres

Tabla 15.14: Campos del fichero exportado Amenazas detectadas por el antivirus

Herramienta de filtrado

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Fechas	**Rango**: establece un intervalo de fechas desde el día presente hacia el pasado. **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil

Campo	Descripción	Valores
		• Dispositivo móvil • Servidor
Tipo de Amenazas	Clase de amenaza.	• Virus y ransomware • Spyware • Herramientas de hacking y PUPs • Phising • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware • Otros

Tabla 15.15: Campos de filtrado para el listado Amenazas detectadas por el antivirus

Ventana de detalle

Muestra información detallada del virus detectado.

Campo	Descripción	Valores
Amenaza	Nombre de la amenaza.	Cadena de caracteres
Acción	Acción que ejecutó Panda Endpoint Protection. Consulta **Restaurar elementos de cuarentena** en la página **568**.	• Movido a cuarentena • Borrado • Bloqueado • Proceso terminado • Permitido (modo auditoría)

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se realizó la detección. Incluye un enlace a la ventana Detalles del equipo	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.	Cadena de caracteres
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Nombre	Nombre de la amenaza.	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza.	Cadena de caracteres
Tipo de malware	Clase de malware.	• Virus y ransomware • Spyware • Herramientas de hacking y PUPs • Phishing • Sospechosos • Acciones peligrosas bloqueadas • Tracking cookies • URLs con malware

Campo	Descripción	Valores
		• Otros.
Detectado por	Módulo que realizó la detección.	
Fecha	Fecha de la detección.	Fecha

Tabla 15.16: Detalle del listado de Amenazas detectadas por el antivirus

Dispositivos bloqueados

Este listado muestra en detalle todos los equipos de la red que tienen limitado el acceso a alguno de los periféricos conectados.

Campo	Descripción	Valores
Equipo	Nombre del equipo desprotegido.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	• Cadena de caracteres • > Grupo Todos • Grupo nativo • Grupo Directorio activo
Nombre	Nombre que el administrador asigna de forma manual al dispositivo para facilitar su identificación.	Cadena de caracteres
Tipo	Familia del dispositivo afectado por la configuración de seguridad.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth

Campo	Descripción	Valores
		• Módems • Dispositivos móviles
Acción	Tipo de acción efectuada sobre el dispositivo.	• Bloquear • Permitir Lectura • Permitir Lectura y escritura
Fecha	Fecha en la se aplicó la acción.	Fecha

Tabla 15.17: Campos del listado Dispositivos bloqueados

Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Nombre original	Nombre del periférico conectado al equipo y afectado por la configuración de seguridad.	Cadena de caracteres
Nombre	Nombre asignado al dispositivo por el administrador.	Cadena de caracteres
Tipo	Clase de dispositivo.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes

Campo	Descripción	Valores
		• Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Id. de instancia	Identificador del dispositivo afectado.	Cadena de caracteres
Número de detecciones	Número de veces que se detectó una operación no permitida sobre el dispositivo.	Numérico
Acción	Tipo de acción efectuada sobre el dispositivo.	• Bloquear • Permitir Lectura • Permitir Lectura y escritura
Detectado por	Módulo que detectó la operación no permitida.	Control de dispositivos
Fecha	Fecha en la se detectó la operación no permitida.	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 15.18: Campos del fichero exportado Dispositivos bloqueados

Herramienta de filtrado

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fechas	• **Rango**: establece un intervalo de fechas desde el día presente hacia el pasado. • **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Tipo de dispositivo	Familia del dispositivo afectado por la configuración de seguridad.	• Unidades de almacenamiento extraibles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Nombre	Nombre del dispositivo.	Cadena de caracteres

Tabla 15.19: Campos de filtrado para el listado Dispositivos bloqueados

Ventana de detalle

Muestra información detallada del dispositivo bloqueado.

Campo	Descripción	Valores
Dispositivo	Nombre del dispositivo bloqueado.	Cadena de caracteres
Acción	Acción que ejecutó Panda Endpoint	• Movido a

Campo	Descripción	Valores
	Protection.	cuarentena • Borrado • Bloqueado • Proceso terminado
Equipo	Nombre del equipo donde se realizó el bloqueo del dispositivo.	Cadena de caracteres
Tipo de equipo	Clase del equipo.	• Estación • Portátil • Servidor • Dispositivo móvil
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Nombre original	Nombre del dispositivo bloqueado.	Cadena de caracteres
Nombre	Nombre asignado por el administrador al dispositivo. Se puede modificar al hacer clic en el icono .	Cadena de caracteres
Tipo de dispositivo	Categoría del dispositivo.	• Unidades de almacenamiento extraibles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Id. de instancia	Identificador del dispositivo afectado.	Cadena de caracteres

Campo	Descripción	Valores
Bloqueado por	Módulo que realizó la detección.	Control de dispositivos
Número de detecciones	Número de bloqueos detectados.	Numérico
Fecha	Fecha de la detección.	Fecha

Tabla 15.20: Detalle del listado Dispositivos bloqueados

Intentos de intrusión bloqueados

Este listado muestra los ataques de red recibidos por los equipos y bloqueados por el módulo de cortafuegos.

Campo	Descripción	Valores
Equipo	Nombre del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP	Dirección IP del interface red principal del equipo que recibió el ataque de red.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Tipo de intrusión	Indica el tipo de intrusión detectado. Para obtener más información acerca de cada uno de los ataques enumerados, consulta **Bloquear intrusiones** en la página **334**.	• Todos los intentos de intrusión • ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit

Campo	Descripción	Valores
		pathLand attack • Smart DNS • ICMP filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Fecha	Fecha y hora en la que Panda Endpoint Protection registró el ataque en el equipo.	Fecha

Tabla 15.21: Campos del listado Intentos de intrusión bloqueados

Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	Cadena de caracteres
Equipo	Nombre del equipo que recibió el ataque de red.	Cadena de caracteres
Tipo de intrusión	Indica el tipo de intrusión detectado. Para obtener más información acerca de cada uno de los ataques enumerados, consulta Bloquear intrusiones en la página 334 .	• ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit path • Land attack

Campo	Descripción	Valores
		• Smart DNS • ICM filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Dirección IP local	Dirección IP del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP remota	Dirección IP del equipo que inició el ataque de red.	Cadena de caracteres
MAC remota	Dirección física del equipo que inició el ataque de red, siempre que se encuentre en el mismo segmento de red que el equipo que recibió el ataque.	Cadena de caracteres
Puerto Local	Si el ataque es TCP o UDP indica el puerto donde se recibió el intento de intrusión.	Numérico
Puerto remoto	Si el ataque es TCP o UDP indica el puerto desde donde se envió el intento de intrusión.	Numérico
Número de detecciones	Número de intentos de intrusión del mismo tipo recibidos.	Numérico
Acción	Acción ejecutada por el cortafuegos según su configuración. Consulta **Firewall (Equipos Windows)** en la página **326** para más información.	Bloquear

Campo	Descripción	Valores
Detectado por	Motor de detección que realizó la detección del ataque de red.	Firewall
Fecha	Fecha en la que se registró el ataque de red.	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP del interface red principal del equipo que recibió el ataque de red.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 15.22: Campos del fichero exportado Intentos de intrusión bloqueados

Herramienta de filtrado

Campo	Descripción	Valores
Fechas	• **Rango**: establece un intervalo de fechas desde el día presente hacia el pasado. • **Rango personalizado**: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Tipo de intrusión	Indica el tipo de intrusión detectado. Para obtener más información acerca de cada uno de los ataques enumerados, consulta **Bloquear intrusiones** en la página **334**.	• Todos los intentos de intrusión • ICMP attack • UDP port scan • Header

Campo	Descripción	Valores
		lengths • UDP flood • TCP flags check • Smart WINS • IP explicit pathLand attack • Smart DNS • ICMP filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor

Tabla 15.23: Campos de filtrado para el listado Intentos de intrusión bloqueados

Ventana de detalle

Muestra información detallada del ataque de red detectado.

Campo	Descripción	Valores
Tipo de intrusión	Indica el tipo de intrusión detectado. Para obtener más información acerca de cada uno de los ataques enumerados, consulta **Bloquear intrusiones** en la página **334**.	• ICMP attack • UDP port scan • Header lengths

Campo	Descripción	Valores
		• UDP flood • TCP flags check • Smart WINS • IP explicit path • Land attack • Smart DNS • ICM filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Acción	Acción que ejecutó Panda Endpoint Protection.	Bloqueado
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección IP local	Dirección IP del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP remota	Dirección IP del equipo que inició el ataque de red.	Cadena de caracteres

Campo	Descripción	Valores
MAC remota	Dirección física del equipo que inició el ataque de red, siempre que se encuentre en el mismo segmento de red que el equipo que recibió el ataque.	Cadena de caracteres
Puerto local	Si el ataque es TCP o UDP indica el puerto donde se recibió el intento de intrusión.	Numérico
Puerto remoto	Si el ataque es TCP o UDP indica el puerto desde donde se envió el intento de intrusión.	Numérico
Detectado por	Módulo que realizó la detección.	Firewall
Número de detecciones	Número de veces que se repitió de forma sucesiva el mismo tipo de ataque entre los mismos equipos origen y destino.	Numérico
Fecha	Fecha de la detección.	Fecha

Tabla 15.24: Detalle del listado de Intentos de intrusión bloqueados

Capítulo 16

Evaluación de riesgos

La funcionalidad de evaluación de riesgos permite al administrador de la consola web monitorizar el estado global del riesgo de seguridad de los equipos que gestiona.

Panda Endpoint Protection monitoriza y evalúa de forma individual cada configuración y cada módulo de seguridad instalado en los equipos de la red. Cada característica evaluada se compara con una configuración o estado ideal definido por Panda Security. Cuando la configuración ideal y la encontrada en el equipo del usuario difieren, se le asigna un nivel de riesgo a esa característica en concreto.

Al configurar la funcionalidad de evaluación de riesgos, el administrador puede elegir qué aspectos de la seguridad desea monitorizar en el equipo y cuáles no. En el caso de que la funcionalidad evaluada difiera de la configuración ideal, Panda Security establece un nivel de riesgo particular (Medio, Alto o Critico), aunque el administrador puede cambiarlo en función de sus prioridades.

Una vez evaluado el funcionamiento del software de seguridad del usuario desde todos los ángulos posibles, Panda Endpoint Protection calcula un nivel de riesgo global aplicable para todo el equipo, que será el del mayor nivel de riesgo asignado a las distintas configuraciones y características evaluadas.

No todas las características a evaluar son aplicables a todos los sistemas operativos instalados en la red. Panda Security añadirá nuevas comprobaciones con cada versión futura del producto para mejorar progresivamente la evaluación de riesgos.

Para obtener información adicional sobre los distintos recursos de la evaluación de riesgos, consulta las referencias siguientes:

Acceso, control y supervisión de la consola de administración *en la página* ***53****información sobre cómo gestionar cuentas de usuario y asignar permisos.*

Gestión de listados *en la página* ***42****: información sobre cómo gestionar listados.*

Contenido del capítulo

Configuración de la evaluación de riesgos

Permisos requeridos

La evaluación de riesgos es visible para todos los usuarios de la consola web, pero para su configuración es necesario disponer del rol control total. Para más información, consulta **Gestión de roles y permisos** en la página **66**. La configuración de la evaluación de riesgos se aplica por igual a todos los equipos del parque informático.

Acceso a la configuración

Haz clic en el menú superior **Configuración**, menú lateral **Riesgos**. Se abrirá la ventana **Riesgos**. La información se distribuye en dos zonas principales: la lista de riesgos y los desplegables para asignar los niveles de riesgo correspondientes.

Lista de riesgos

La mayoría de los riesgos tienen que ver con las diferentes configuraciones implementadas por Panda Endpoint Protection. Otros riesgos están relacionados con la información sobre el estado de la protección que los equipos envían a los servidores de Panda Security.

Los riesgos disponibles para su evaluación varían en función del sistema operativo instalado en los equipos.

Riesgo	Comentario
Sin protección	El equipo presenta errores en la instalación de la protección o no dispone de licencia. Consulta **Estado de protección** en la página **470**
Protección desactualizada	La versión del motor de la protección instalada en el equipo no está actualizada. El equipo es vulnerable frente a las amenazas. Consulta **Sección Detalles (3)** en la página **265**.
Conocimiento desactualizado (más de 30 días)	La versión del fichero de firmas instalada en el equipo no está actualizada, por lo que el equipo es vulnerable frente a las amenazas. Consulta **Protección desactualizada** en la página **474**.

Riesgo	Comentario
Sin conectividad con servidores de conocimiento	Las comunicaciones entre el equipo y los servidores de Aether no están funcionando correctamente. El equipo no está debidamente protegido. Consulta **Funcionalidades del producto y requisitos** en la página **619** para comprobar que el equipo cumple los requisitos de conexión necesarios.
Sin protección ante desinstalación	El equipo no está protegido con contraseña para evitar la desinstalación o modificación de la protección. Consulta **Protección del agente mediante contraseña** en la página **314**.
Protección antitamper desactivada	El funcionamiento de la protección podría ser modificado y manipulado. Consulta **Configuración de contraseña y anti-tampering** en la página **313**.
Antivirus (de archivos) desactivado	El antivirus está desactivado. Consulta **Antivirus** en la página **324**y **Antivirus para navegadores web** en la página **343**(Android).
Antiphishing desactivado	El equipo no está protegido contra ataques basados en el engaño por web y correo. Consulta **Amenazas a detectar** en la página **324**.
Antivirus para navegación web desactivado	El equipo no está protegido frente a las amenazas procedentes de determinadas páginas web y URLs. Consulta **Antivirus** en la página **324** y **Antivirus para navegadores web** en la página **343**
Exclusiones de carpetas, archivos o extensiones	Hay extensiones, archivos o carpetas que no están siendo analizados en busca de malware. Consulta **Archivos y rutas excluidas del análisis** en la página **322** y **Software autorizado y exclusiones de elementos**.
Parches críticos pendientes de instalación	El equipo tiene instalado Patch Management y notifica la existencia de parches críticos pendientes de instalar. Esta notificación puede producirse de forma inmediata o una vez transcurrido un determinado número de días desde la publicación de los parches. Por defecto el número de días es 30, pero el administrador puede modificarlo al activar este riesgo para su evaluación. Consulta **Configuración del descubrimiento de parches sin aplicar** en la página **367**.

Tabla 16.1: Lista de riesgos

Funcionamiento de la evaluación de riesgos

De forma predeterminada, Panda Security asigna un nivel de riesgo específico a cada riesgo detectado en el equipo. Este nivel de riesgo asignado por defecto se muestra al acceder por vez primera a la ventana **Configuración**, **Riesgos**. El administrador puede cambiar el nivel de riesgo asignado por defecto y seleccionar el que desee, en función de sus necesidades.

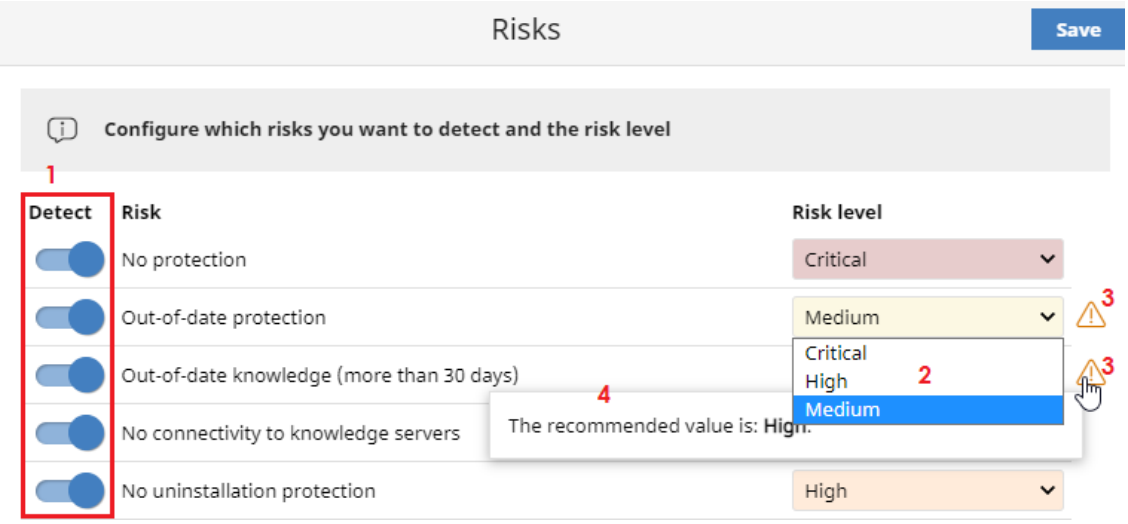


Figura 16.1: Configurar la evaluación de riesgos

Para configurar la evaluación de riesgos:

- En la lista de riesgos **(1)**, activa los que quieres detectar. Para ello, utiliza los controles deslizantes.
- Utiliza el desplegable **Nivel de riesgo (2)**, para asignar a cada riesgo su nivel : **Crítico**, **Alto**, **Medio**.

  Si el nivel de riesgo que has seleccionado no coincide con el recomendado por Panda Security, se mostrará el icono ⚠ **(3)**. Al situar el cursor sobre el icono se mostrará el mensaje **(4)** recordando cuál es el nivel de riesgo recomendado por Panda Security.
- Haz clic en el botón **Guardar**.

> *La actualización de riesgos es asíncrona, es decir, puede transcurrir un pequeño margen de tiempo entre la aplicación de la configuración de riesgos y la aparición de los datos en los listados y widgets.*

Monitorización de la evaluación de riesgos

Los resultados de la evaluación de riesgos se reflejan en los widgets y listados correspondientes. Para más información, consulta **Listados del módulo Evaluación de riesgos** y **Paneles/widgets del módulo Evaluación de riesgos**.

Modificación y recálculo de los valores recomendados

Panda Security puede modificar los niveles de riesgo recomendados para los diferentes riesgos, pero este cambio no tendrá efecto inmediato sobre los riesgos seleccionados por el administrador, salvo si actualiza a una nueva versión de Panda Endpoint Protection, en cuyo caso:

- Los riesgos cuyo nivel de riesgo no haya sido modificado por el usuario, se actualizarán automáticamente con el nuevo valor por defecto recomendado por Panda Security.
- Panda Endpoint Protection calculará otra vez el riesgo de todos los equipos y la configuración por defecto mostrará los nuevos niveles de riesgo recomendados.

Cálculo del nivel de riesgo global asignado a cada equipo

La evaluación del nivel de riesgo asignado a cada equipo se produce en dos momentos:

- Para todo el parque informático, con cada actualización de la versión de Panda Endpoint Protection.
- Para un equipo concreto, cuando suceden determinadas circunstancias, como por ejemplo asignar configuraciones al equipo, mover los equipos o dispositivos de un grupo a otro, registrar nuevos dispositivos o equipos y, en algunos casos, modificar su asignación de licencias.

  El nivel de riesgo global del equipo coincide con el nivel mayor alcanzado en la evaluación de los riesgos.

  Por ejemplo:

  - En el equipo hay 5 riesgos activos, de los cuáles 1 es de nivel **Alto** y los otros 4 de nivel **Medio**. El nivel de riesgo global del equipo será **Alto**.
  - En el equipo hay 5 riesgos, 4 activos (1 de nivel **Alto**, 3 de nivel **Medio**) y 1 riesgo inactivo de nivel **Crítico**. El nivel de riesgo global del equipo será **Alto**.

Listados del módulo Evaluación de riesgos

Acceso a los listados

Accede a los listados de evaluación de riesgos siguiendo dos rutas:

- Haz clic en el menú superior **Estado.**
- Haz clic en el menú lateral **Riesgos** y en el widget relacionado.

  o

- Haz clic en el menú superior **Estado**.
- En el panel lateral, haz clic en el enlace **Añadir** situado junto a **Mis listados**. Se mostrará la ventana **Añadir listado** con los listados disponibles.

- En la sección **General**, selecciona qué listado de riesgos deseas utilizar: **Riesgos por equipo** o **Riesgos detectados**. Se abrirá la plantilla del listado y podrás modificarla y guardarla. Después, el listado se añadirá a la sección **Mis listados** del panel lateral.

Listado Riesgos por equipo

Este listado ofrece información sobre los riesgos detectados en el equipo o dispositivo y el nivel de los mismos.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Grupo al que pertenece el equipo.	Cadena de caracteres
Última conexión	Fecha y hora del último envío del estado del equipo a la nube de Panda Security.	Fecha/hora
Nivel de riesgo	Nivel de riesgo del equipo o dispositivo. Coincide con el nivel de riesgo mayor detectado en los riesgos activados durante la evaluación.	• **Sin riesgo**: ninguno de los riesgos ha sido evaluado como crítico, alto o medio. • **Crítico**: al menos uno de los riesgos ha sido evaluado como crítico. • **Alto**: el nivel mayor de riesgo detectado durante la evaluación ha sido alto. • **Medio**: el nivel mayor de riesgo detectado durante la evaluación ha sido medio.
Riesgos del equipo	Gráfica de distribución de los riesgos detectados en el equipo o dispositivo durante la evaluación de riesgos.	• **Rojo**: número de riesgos críticos. • **Naranja**: número de riesgos altos. • **Amarillo** : número de riesgos medios. • **Verde**: número de riesgos sin impacto en la seguridad.

Campo	Comentario	Valores
		• **Gris claro**: número de riesgos no compatibles con el sistema operativo del equipo o dispositivo. • **Gris oscuro**: número de riesgos no evaluados por no haber sido activados por el administrador.

Tabla 16.2: Campos del listado Riesgos por equipo

Al hacer clic en una de las filas del listado, se mostrará la ventana de detalle del equipo. Consulta **Información de equipo** en la página **251** y **Sección Detalles (3)** en la página **265**

Campos mostrados en fichero exportado

La información del listado se puede exportar en formato .CSV. Para ello, haz clic en el icono . En el fichero exportado se muestran los datos siguientes:

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Fecha de última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security.	Fecha

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android • iOS
Nivel de riesgo	Nivel de riesgo global del equipo o dispositivo.	• Sin riesgo • Medio • Alto • Crítico
Riesgos críticos	Número de riesgos críticos por equipo.	Numérico
Riesgos altos	Número de riesgos altos por equipo.	Numérico
Riesgos medios	Número de riesgos medios por equipo.	Numérico
Sin riesgo	Número de riesgos sin impacto en la seguridad por equipo.	Numérico
Riesgos no aplican	Número de riesgos no aplicables al equipo según el sistema operativo instalado.	Numérico
Riesgos sin evaluar	Número de riesgos por equipo no activados por el administrador para su evaluación.	Numérico

Tabla 16.3: Campos del fichero exportado Riesgos por equipo

Herramienta de filtrado

Para acceder a la herramienta de filtrado, haz clic en el enlace **Filtros**, situado junto a la caja de búsqueda de la ventana **Riesgos por equipo**. Los campos de filtrado son los siguientes:

Campo	Comentario	Valores
Buscar equipo	Filtra los equipos según su nombre.	Cadena de caracteres

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Dispositivo móvil • Servidor
Última conexión	Fecha del último envío de riesgos por equipo a la nube de Panda Security.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android • iOS
Riesgo detectado	Riesgo que ha sido activado por el administrador para su evaluación.	• Todos • Sin protección • Protección desactualizada • Conocimiento desactualizado (más de 30 días) • Sin conectividad con servidores de conocimiento • Sin protección ante desinstalación

Campo	Comentario	Valores
		• Protección antitamper desactivada • Antivirus (de archivos) desactivado • Antiphishing desactivado • Antivirus para navegación web desactivado • Exclusiones de carpetas, archivos o extensiones • Parches críticos pendientes de instalación
Nivel de riesgo	Nivel de riesgo asignado	• Critico • Alto • Medio • Sin riesgo

Tabla 16.4: Campos de filtrado para el listado Riesgos por equipo

Listado Riesgos

El listado **Riesgos** muestra los riesgos activados por el administrador para su evaluación y el número de equipos afectados según el nivel de cada riesgo. Al hacer clic sobre una de las líneas del listado, accederás al listado **Riesgos por equipo**.

El listado **Riesgos** muestra los datos siguientes:

Campo	Comentario	Valores
Riesgo	Nombre del riesgo.	Cadena de caracteres
Equipos	Número de equipos en los que ha sido detectado el riesgo.	Numérico
Nivel de riesgo	Nivel de riesgo asignado.	• Crítico • Alto • Medio

Campo	Comentario	Valores
		• Riesgo de los indicadores de ataque (consulta **Configuración de la evaluación de riesgos**).
Riesgo por equipos	Gráfica de distribución que indica el número de equipos en los que el riesgo ha sido detectado y con determinado nivel de riesgo asignado (Crítico, Alto, Medio) o sin riesgo (seleccionados por el administrador pero no detectados).	• **Rojo**: número de equipos en los que el riesgo ha sido detectado con nivel Crítico asignado. • **Naranja**: número de equipos en los que el riesgo ha sido detectado con nivel Alto asignado. • **Amarillo**: número de equipos en los que el riesgo ha sido detectado con nivel Medio asignado. • **Gris claro**: número de equipos en los que el riesgo no ha sido evaluado por no ser compatible con el sistema operativo. • **Gris oscuro**: numero de equipos en los que el riesgo no ha sido evaluado por no haber sido activado para su evaluación por el administrador.

Tabla 16.5: Campos del listado Riesgos

Campos del fichero exportado

La información del listado se puede exportar en formato .CSV. Para ello, haz clic en el icono .

En el fichero exportado se muestran los datos siguientes:

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Riesgo	Nombre del riesgo activado por el administrador para su evaluación.	Cadena de caracteres
Nivel de riesgo	Nivel de riesgo asignado.	• Crítico • Alto • Medio
Equipos con riesgo detectado	Número de equipos en los que se ha detectado el riesgo.	Numérico
Crítico	Número de equipos de la cuenta con nivel de riesgo Crítico.	Numérico
Alto	Número de equipos de la cuenta con nivel de riesgo Alto.	Numérico
Medio	Número de equipos de la cuenta con nivel de riesgo Medio.	Numérico
Equipos sin riesgo	Número de equipos en los que no se ha detectado el riesgo.	Numérico
Equipos a los que no aplica	Número de equipos en los que no se evalúa el riesgo por ser incompatible con el sistema operativo instalado.	Numérico
Equipos con riesgo no evaluado	Número de equipos en los que el riesgo no ha sido activado para su detección.	Numérico

Tabla 16.6: Campos del fichero exportado Riesgos

Herramienta de filtrado

Para acceder a la herramienta de filtrado, haz clic en el enlace **Filtros**, situado junto a la caja de búsqueda de la ventana **Riesgos**. Los campos de filtrado son los siguientes:

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android • iOS

Tabla 16.7: Campos de filtrado para el listado Riesgos

Para programar el envío periódico de los listados de riesgos, consulta ***Envío programado de informes y listados*** *en la página* ***577***

Paneles/widgets del módulo Evaluación de riesgos

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, menú lateral **Riesgos**.

Riesgo de la compañía

Indica el número de equipos sobre los que el usuario tiene visibilidad y cuáles de ellos se encuentran en alguno de los niveles de riesgo establecidos. El estado de los equipos se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

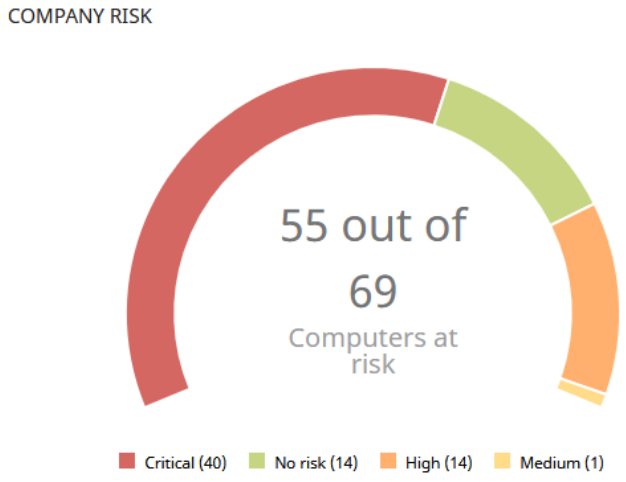


Figura 16.2: Panel Riesgo de la compañía

Significado de las series

Serie	Descripción
Crítico	Número de equipos que se encuentran en nivel de riesgo crítico.
Alto	Número de equipos que se encuentran en nivel de riesgo alto.
Medio	Numero de equipos que se encuentran en nivel de riesgo medio.
Sin riesgo	Número de equipos que no están en situación de riesgo.
Parte central	Suma de todos los equipos que se encuentran en algún nivel de riesgo.

Tabla 16.8: Descripción de la serie Riesgo de la compañía

Filtros preestablecidos desde el panel

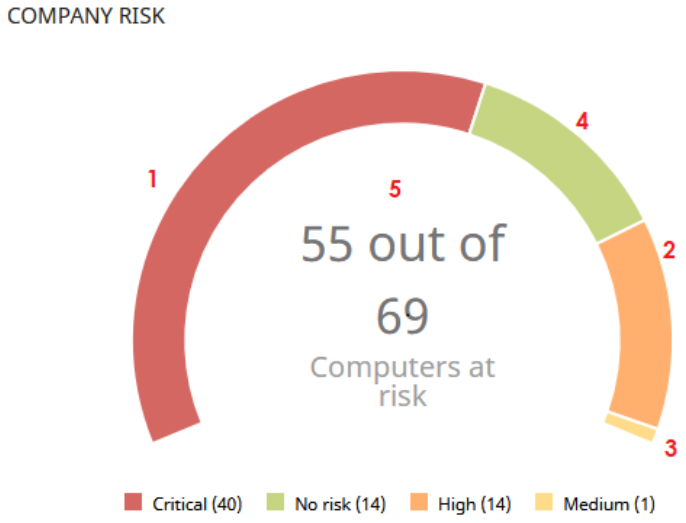


Figura 16.3: Zonas activas del panel Riesgo de la compañía

Al hacer clic en las zonas indicadas en **Zonas activas del panel Riesgo de la compañía** se abre el listado **Riesgos por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Riesgo = Alto
(2)	Riesgo = Crítico
(3)	Riesgo = Sin riesgo
(4)	Riesgo = Medio
(5)	Sin filtros

Tabla 16.9: Zonas activas del panel Riesgo de la compañía

Evolución del riesgo

Indica cómo cambia a lo largo del tiempo el número de equipos que están en un determinado nivel de riesgo.

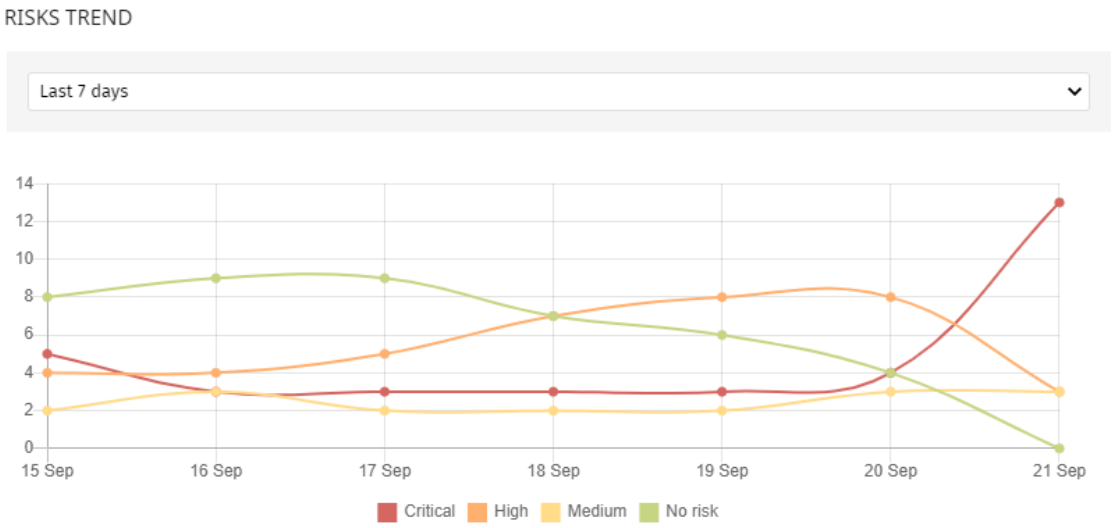


Figura 16.4: Gráfico de Evolución de riesgos

Significado de las series

Serie	Descripción
Riesgo crítico	Evolución del número de equipos en riesgo crítico.
Riesgo alto	Evolución del número de equipos en riesgo alto.
Riesgo medio	Evolución del número de equipos en riesgo medio.
Sin riesgo	Evolución del número de equipos sin riesgo.

Tabla 16.10: Descripción de la serie Evolución del riesgo

Al situar el cursor del ratón sobre uno de los nodos se muestra una etiqueta con la siguiente información:

- Fecha
- Nivel de riesgo
- Número de equipos

Filtros preestablecidos desde el panel

Haz clic sobre los elementos de la leyenda debajo de la gráfica para acceder al listado **Riesgos por equipo** con el filtro correspondiente al tipo seleccionado. Para acceder al listado completo de **Riesgos por equipo** sin aplicar ningún filtro, haz clic sobre cualquier espacio en blanco de la gráfica.

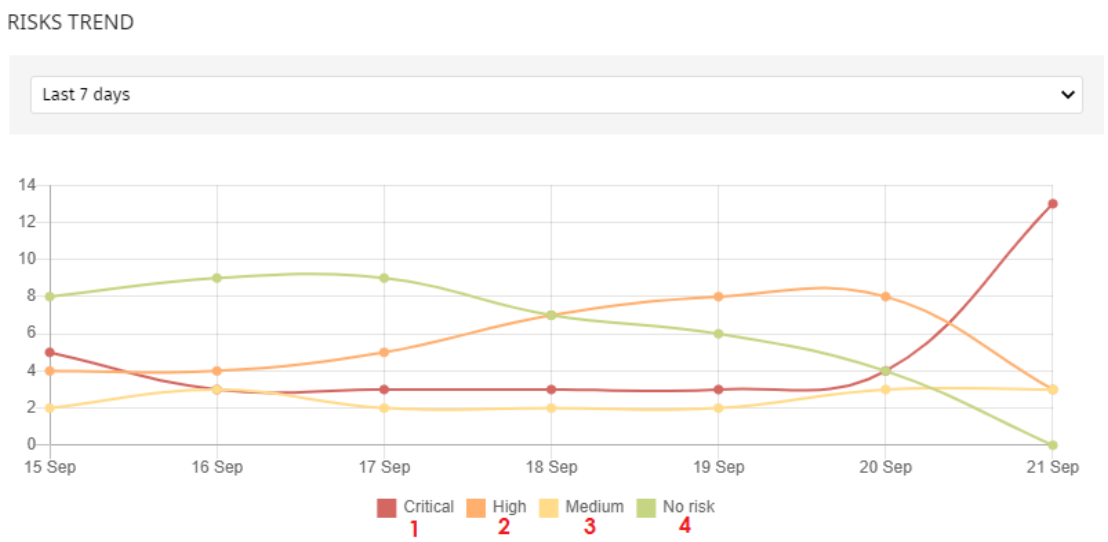


Figura 16.5: Series mostradas en el gráfico Evolución del riesgo

Zona activa	Filtro
(1)	Riesgo= Crítico
(2)	Riesgo= Alto
(3)	Riesgo= Medio
(4)	Sin riesgos

Tabla 16.11: Zonas activas del panel Evolución del riesgo

Riesgos detectados

Muestra una lista de los riesgos que más se han detectado en los equipos.

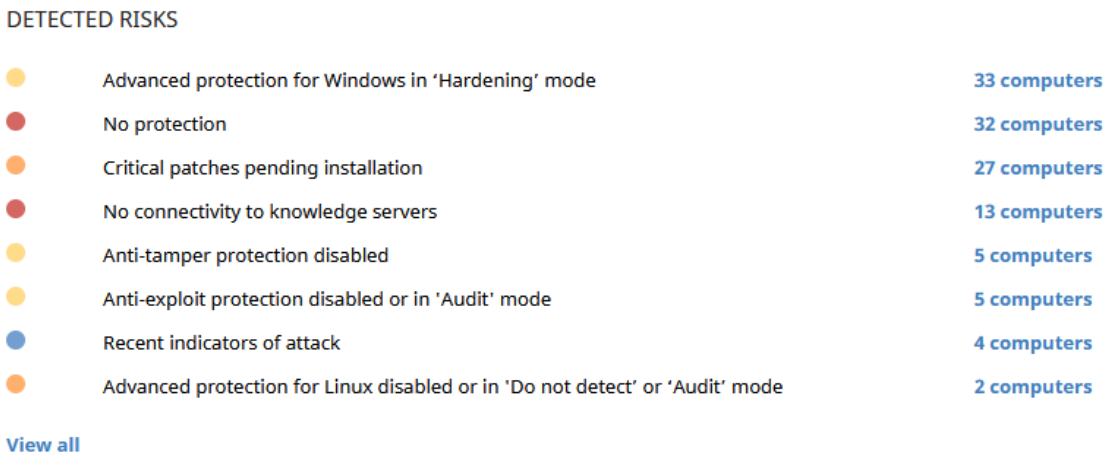


Figura 16.6: Panel Riesgos detectados

Significado de las series

Serie	Descripción
Icono	Nivel del riesgo definido por el administrador. • **Rojo**: Crítico • **Naranja**: Alto • **Amarillo**: Medio • **Azul**: Personalizado
Nombre	Nombre del riesgo.
Número	Número de equipos en los que se ha detectado el riesgo.
Ver todos	Enlace al listado completo de riesgos detectados.

Tabla 16.12: Descripción de las series del panel Riesgos detectados

Filtros establecidos desde el panel

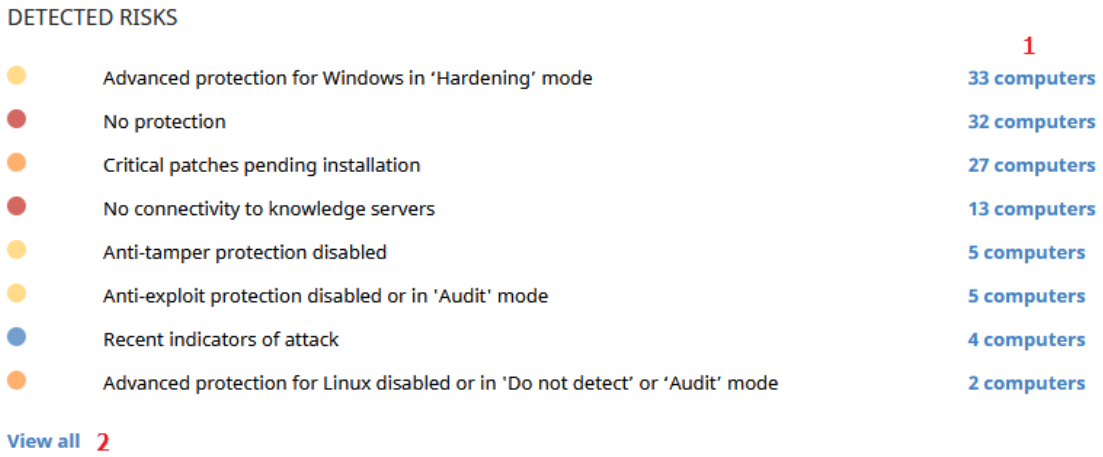


Figura 16.7: Series mostradas en el panel Riesgos detectados

Al hacer clic en las zonas indicadas, se muestran listados con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(3)	Riesgos por equipo	Riesgo detectado = Riesgo seleccionado en el widget

Zona activa	Listado	Filtro
(4)	Riesgos	Sin filtros

Tabla 16.13: Zonas activas del panel Riesgos detectados

Equipos en riesgo (Top 10)

Muestra una lista de los diez equipos con el nivel de riesgo global más elevado.

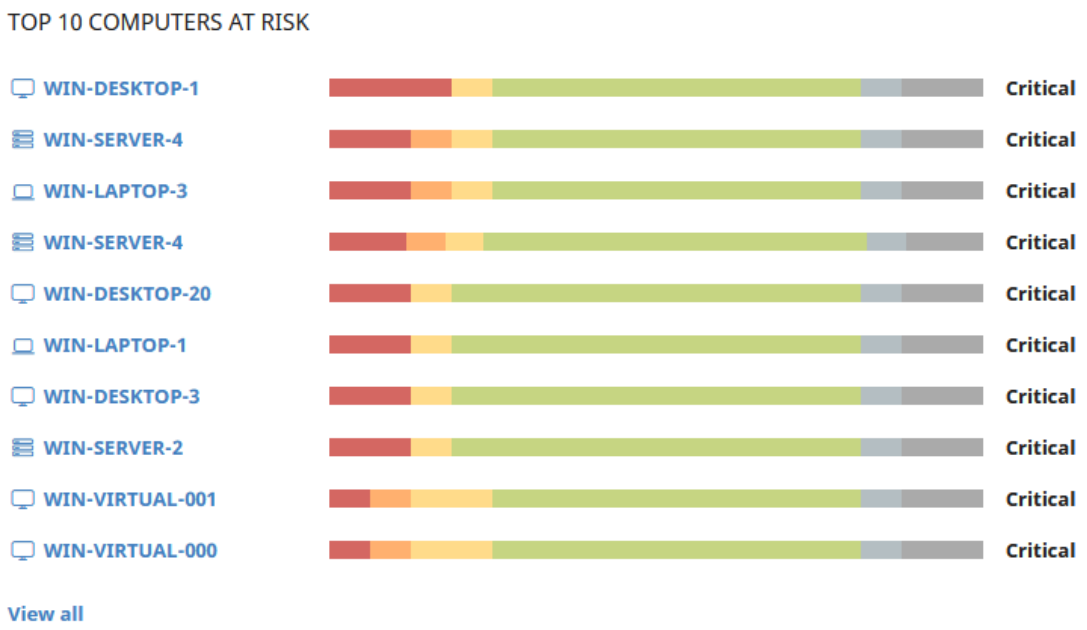


Figura 16.8: Panel Equipos en riesgo (Top 10)

El nivel de riesgo global del equipo coincide con el del riesgo de mayor nivel detectado en el equipo. Para obtener más información consulta ***Cálculo del nivel de riesgo global asignado a cada equipo***

Significado de las series

Serie	Descripción
Nombre	Nombre y tipo del equipo o dispositivo.
Barra de colores	Gráfica de distribución de riesgos del equipo.
Nivel de riesgo	Nivel de riesgo global asignado al equipo.

Serie	Descripción
Enlace Ver Todos	Acceso al listado completo de riesgos por equipo.

Tabla 16.14: Descripción de las series del panel Equipos en riesgo (Top 10)

Filtros establecidos desde el panel

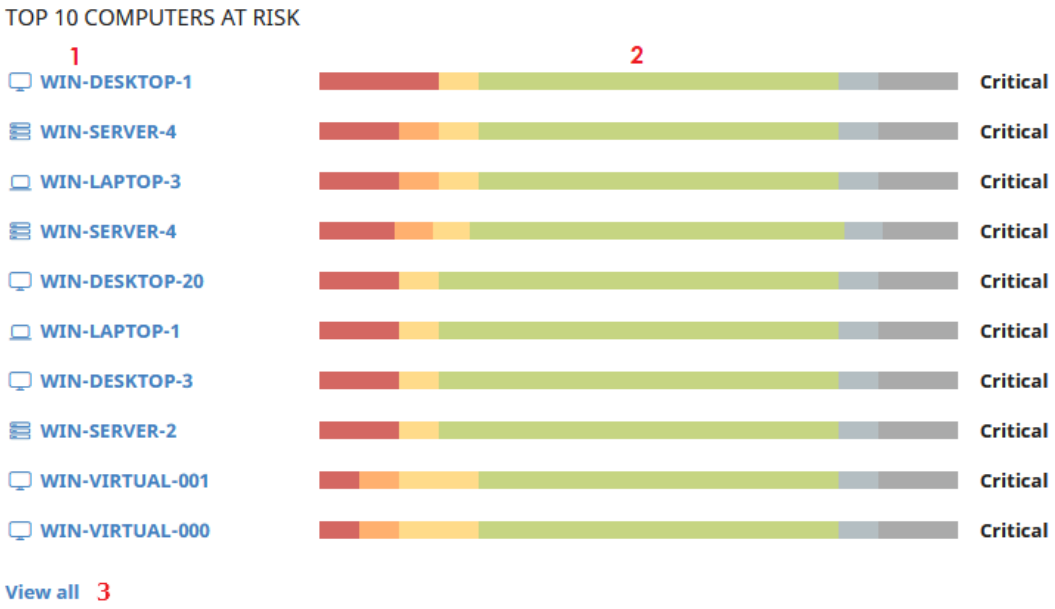


Figura 16.9: Zonas activas del panel Equipos en riesgo (Top 10)

Al hacer clic en las zonas indicadas, se muestran listados con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Detalle del equipo	
(2)	Riesgos	Equipo seleccionado en el widget.
(3)	Riesgos por equipo	Sin filtros

Tabla 16.15: Zonas activas del panel Equipos en riesgo (Top 10)

La información sobre el estado de los riesgos en el equipo está disponible también en la ventana **Detalles del equipo**. Para más información, consulta **Información de equipo** en la página **251**

Capítulo 17

Evaluación de vulnerabilidades

El módulo Evaluación de vulnerabilidades integrado en la plataforma Aether localiza los equipos de la red que contienen software con vulnerabilidades conocidas, e informa sobre la disponibilidad de parches para evitar su impacto en los equipos.

Evaluación de vulnerabilidades es compatible con sistemas operativos Windows macOS y Linux, y detecta aplicaciones de terceros pendientes de actualizar o en EoL (End of Life), así como los parches y actualizaciones publicados por Microsoft para todos sus productos (sistemas operativos, bases de datos, suites ofimáticas, etc.).

Evaluación de vulnerabilidades no instala las parches detectados en los equipos gestionados. El administrador de la red puede instalar los parches necesarios por su cuenta o adquirir el módulo Patch Management para instalar los parches de forma centralizada y desde la misma consola de Panda Endpoint Protection.

Para obtener información adicional sobre los distintos apartados del módulo Evaluación de vulnerabilidades, consulta las referencias siguientes:

Crear y gestionar configuraciones *en la página* ***285****: información sobre cómo crear, modificar, borrar o asignar configuraciones a los equipos de la red.*

Acceso, control y supervisión de la consola de administración *en la página* ***53****: gestión de cuentas de usuario y asignación de permisos.*

Gestión de listados *en la página* ***42****: información sobre cómo gestionar listados.*

Contenido del capítulo

Requisitos de la evaluación de vulnerabilidades

Versiones de sistemas operativos Windows compatibles

Estaciones

- Windows 7 (32 y 64 bits)
- Windows 8 (32 y 64 bits)
- Windows 8.1 (32 y 64 bits)
- Windows 10 (32 y 64 bits)
- Windows 11 (64 bits)

Servidores

- Windows 2008 (32 y 64 bits) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 y 2016
- Windows Server 2022

Comportamiento en equipos Windows no compatibles con Evaluación de vulnerabilidades

- No se instalará el módulo en los equipos.
- Los equipos conservarán las configuraciones de evaluación de vulnerabilidades que tenían asignadas, pero no les serán aplicadas.
- En el listado **Parches disponibles por equipos** no se incluirá información sobre estos equipos.

Versiones de sistemas operativos macOS compatibles

- macOS 10.15 Catalina
- macOS 11 Big Sur

- macOS 12 Monterey
- macOS Ventura.
- macOS Sonoma

Versiones de sistemas operativos Linux compatibles

Distribuciones de 64 bits soportadas:

- **Red Hat**: 7.0, 8.0
- **CentOS**: 7.0
- **SuSE Linux Enterprise**: 12, 15.

<MODIFICADO>

Configuración de Evaluación de vulnerabilidades

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Evaluación de vulnerabilidades**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Configurar evaluación de vulnerabilidades	Crear, modificar, borrar, copiar o asignar las configuraciones de Evaluación de vulnerabilidades.
Visualizar parches disponibles	Visualizar las configuraciones de Evaluación de vulnerabilidades.

Tabla 17.1: Permisos requeridos para acceder a la configuración de Evaluación de vulnerabilidades

Configuración general

Haz clic en el selector **Buscar parches automáticamente** para activar la búsqueda de parches. Si el selector no está activado, los parches pendientes de instalación no se mostrarán en los listados.

El administrador de la red puede decidir entre instalar los parches de forma manual o utilizar herramientas de terceros para ello. Sin embargo, al adquirir el módulo Panda Patch Management podrá llevar a cabo la instalación de los parches de forma centralizada y automática, y desde la misma consola de Panda Endpoint Protection.

Frecuencia de la búsqueda

Buscar parches con la siguiente frecuencia establece cada cuanto tiempo consulta la evaluación de vulnerabilidades los parches instalados en los equipos y los compara con las bases de datos de parches disponibles.

Criticidad de los parches

Establece la criticidad de los parches que Evaluación de vulnerabilidades busca en las bases de datos de parches disponibles.

En el caso de los equipos y dispositivos con sistema operativo macOS o Linux, no se aplican parches de tipo Windows Service Pack.

La criticidad de cada parche está establecida por cada proveedor del software afectado por la vulnerabilidad. Este criterio de clasificación no es uniforme y se recomienda comprobar previamente la descripción del parche para aquellos que no estén clasificados como "críticos", con el objetivo de evitar su instalación si no se padecen los síntomas descritos.

*Las criticidades relacionadas con parches de resolución de bugs y mejoras para macOS y Linux, se incluyen dentro de la categoría **Otros parches (no de seguridad)**.*

Paneles/widgets de Evaluación de vulnerabilidades

Descubre Patch Management

Panda Patch Management es un módulo integrado en la plataforma Aether que localiza los equipos de la red que contienen software con vulnerabilidades conocidas, y los actualiza de forma automática y centralizada.

Para acceder a más información sobre Panda Patch Management, haz clic en los enlaces **Ver vídeo** o **Más información**.

Para cerrar el panel informativo o para que no se muestre de nuevo, haz clic en el icono ✕.

Acceso al panel de control

Para acceder al panel de control, haz clic en el menú superior **Estado**, panel lateral **Evaluación de vulnerabilidades**

Permisos requeridos

Permisos	Acceso al widget
Sin permisos	• Estado de evaluación de vulnerabilidades • Tiempo desde la última comprobación
Visualizar parches disponibles	• Programas "End Of Life" • Parches disponibles • Evolución de los parches disponibles • Parches disponibles en más equipos • Programas con más parches disponibles

Tabla 17.2: Permisos requeridos para los widgets de Evaluación de vulnerabilidades

Estado de la evaluación de vulnerabilidades

Muestra los equipos donde la evaluación de vulnerabilidades está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. El estado del módulo se representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

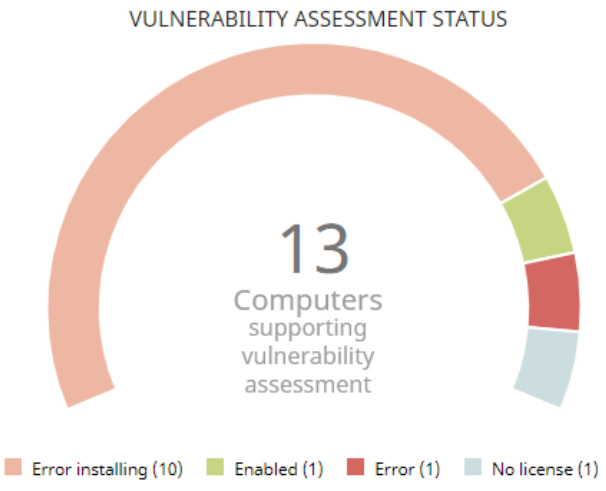


Figura 17.1: Panel de Estado de evaluación de vulnerabilidades

Significado de las series

Serie	Descripción
Activado	Indica el porcentaje de equipos en los que el módulo de evaluación de vulnerabilidades se instaló sin errores, su ejecución no presenta problemas

Serie	Descripción
	y la configuración asignada permite buscar parches automáticamente.
Desactivado	Indica el porcentaje de equipos en los que el módulo de evaluación de vulnerabilidades se instaló sin errores, su ejecución no presenta problemas y la configuración asignada no permite buscar parches automáticamente.
Sin licencia	Equipos sin servicio de evaluación de vulnerabilidades, debido a que no se poseen licencias suficientes de Panda Endpoint Protection o no se les ha asignado una licencia disponible.
Error instalando	Indica los equipos donde el módulo no se pudo instalar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con el agente sin actualizar.
Error	El módulo de evaluación de vulnerabilidades no responde a las peticiones del servidor y su configuración difiere de la establecida en la consola web.
Parte central	Refleja el número de total de equipos compatibles con la evaluación de vulnerabilidades.

Tabla 17.3: Descripción de la serie Estado de evaluación de vulnerabilidades

Filtros preestablecidos desde el panel

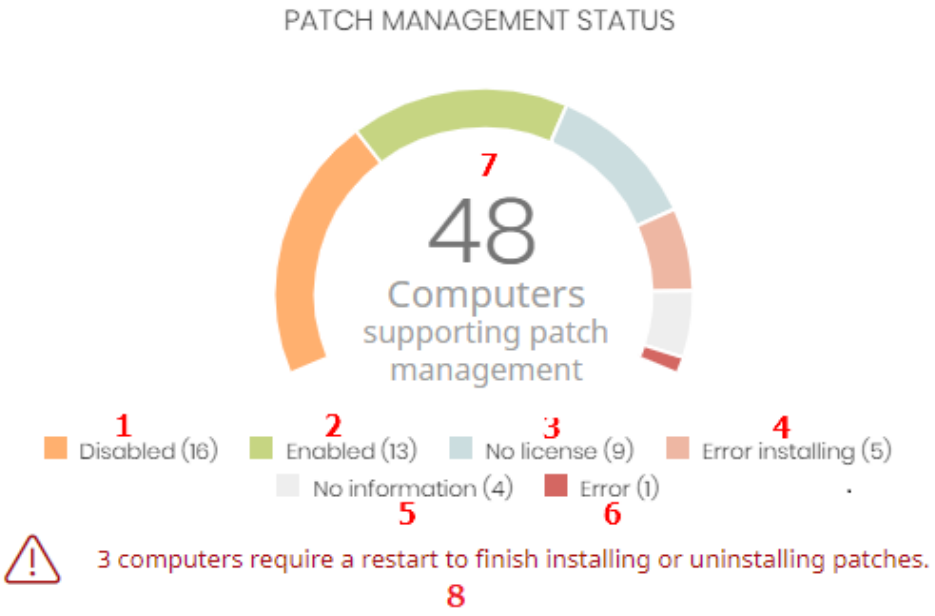


Figura 17.2: Zonas activas del panel Estado de evaluación de vulnerabilidades

Al hacer clic en las zonas indicadas en **Zonas activas del panel Estado de evaluación de vulnerabilidades** se abre el listado **Estado de la evaluación de vulnerabilidades** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de evaluación de vulnerabilidades = Desactivado.
(2)	Estado de evaluación de vulnerabilidades = Activado.
(3)	Estado de evaluación de vulnerabilidades = Sin licencia.
(4)	Estado de evaluación de vulnerabilidades = Error instalando.
(5)	Estado de evaluación de vulnerabilidades = Sin información.
(6)	Estado de evaluación de vulnerabilidades = Error.
(7)	Sin filtro.

Tabla 17.4: Definición de filtros del listado Estado de evaluación de vulnerabilidades

Tiempo desde la última comprobación

Muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo para comprobar su estado de parcheo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

Figura 17.3: Panel Tiempo desde la última comprobación

Significado de las series

Serie	Descripción
72 horas	Número de equipos que no comprobaron su estado de parcheo en las últimas 72 horas.
7 días	Número de equipos que no comprobaron su estado de parcheo en las últimas 7 días.
30 días	Número de equipos que no comprobaron su estado de parcheo en los últimas 30 días.

Tabla 17.5: Descripción de la serie Tiempo desde la última comprobación

Filtros preestablecidos desde el panel

Figura 17.4: Zonas activas del panel Tiempo desde la última comprobación

Al hacer clic en las zonas indicadas en **Zonas activas del panel Tiempo desde la última comprobación** se abre el listado **Estado de la evaluación de vulnerabilidades** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 3 días y Estado de vulnerabilidades = Activado o Desactivado o Sin información o Error.
(2)	Última conexión = Hace más de 7 días y Estado de vulnerabilidades = Activado o Desactivado o Sin información o Error.
(3)	Última conexión = Hace más de 30 días y Estado de vulnerabilidades = Activado o Desactivado o Sin información o Error.

Tabla 17.6: Definición de filtros del listado Estado de la evaluación de vulnerabilidades

Programas "End of life"

Muestra la información relativa al "end of life" de los programas instalados en los equipos de la red, agrupados según el plazo restante.

Figura 17.5: Panel Programas "End of life"

Significado de las series

Serie	Descripción
Actualmente en EOL	Programas instalados en el parque informático que ya entraron en EOL.
Actualmente o en 1 año en EOL	Programas instalados en el parque informático que ya han entrado en EOL o entrarán dentro de un año.
Con fecha EOL conocida	Programas instalados en el parque informático cuya fecha de EOL es conocida.

Tabla 17.7: Descripción de la serie Programas "End of life"

Filtros preestablecidos desde el panel

Figura 17.6: Zonas activas del panel Programas "End of life"

Al hacer clic en las zonas indicadas en **Zonas activas del panel Programas "End of life"** se abre el listado **Programas "End Of Life'** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Fecha de End Of Life = Actualmente en "End Of Life".
(2)	Fecha de End Of Life = Actualmente o en 1 año en "End Of Life".
(3)	Fecha de End Of Life = Todos.

Tabla 17.8: Definición de filtros del listado Programas "End Of Life'

Parches disponibles

Muestra un recuento de parches disponibles, distribuido por la categoría del parche. Cada parche no aplicado se contabiliza tantas veces como equipos no lo tengan instalado.

Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de	Número de parches sin determinar su importancia relativos a la

Serie	Descripción
seguridad – No clasificados	seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía. No aplicable a equipos con sistema operativo Linux o macOS.

Tabla 17.9: Descripción de la serie Parches disponibles

Filtros preestablecidos desde el panel

Al hacer clic en las zonas indicadas en **Paneles/widgets de Evaluación de vulnerabilidades** se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Criticidad = Critica (de seguridad).
(2)	Criticidad = Importante (de seguridad).
(3)	Criticidad = Baja (de seguridad).
(4)	Criticidad = No clasificado (de seguridad).
(5)	Criticidad = Otros parches (no de seguridad).
(6)	Criticidad = Service Pack.
(7)	Sin filtros.

Tabla 17.10: Definición de filtros del listado Parches disponibles por equipos

Filtros disponibles sobre el widget

Al hacer clic en el icono se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

Filtro	Definición
Tipo de equipo	• Estación • Portátil • Servidor
Plataforma	• Todos • Windows • Linux • macOS
Tipo de parche	• Parches de sistema operativo: parches disponibles para sistemas operativos Windows, Linux y macOS. • Parches de aplicaciones: parches disponibles para las aplicaciones.

Tabla 17.11: Filtros disponibles para el widget Evolución de Parches disponibles

Evolución de los parches disponibles

Muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad.

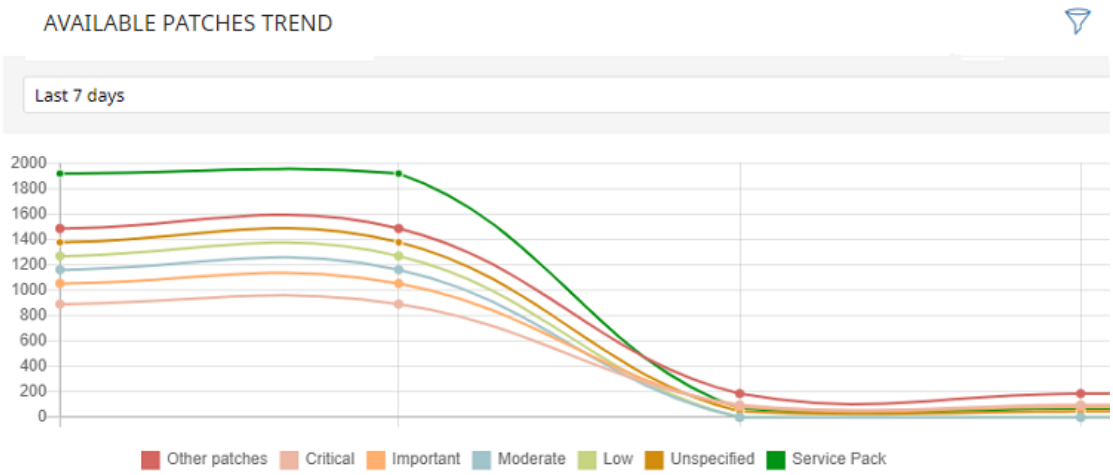


Figura 17.7: Gráfico de Evolución de los parches disponibles

Significado de las series

Serie	Descripción
Parches de seguridad	Número de parches clasificados como de importancia crítica

Serie	Descripción
- Críticos	relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad – No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía. No aplicable a sistemas operativos macOS y Linux.

Tabla 17.12: Descripción de la serie Evolución de los parches disponibles

Al situar el cursor del ratón sobre uno de los nodos se muestra un tooltip con la siguiente información:

- Fecha
- Tipo
- Número de parches

Filtros preestablecidos desde el panel

Haz clic sobre los elementos de la leyenda debajo de la gráfica para acceder al listado **Parches disponibles por equipos** con el filtro correspondiente al tipo seleccionado. Haz clic sobre la gráfica, para acceder al listado completo de **Parches disponibles por equipos** sin aplicar ningún filtro.

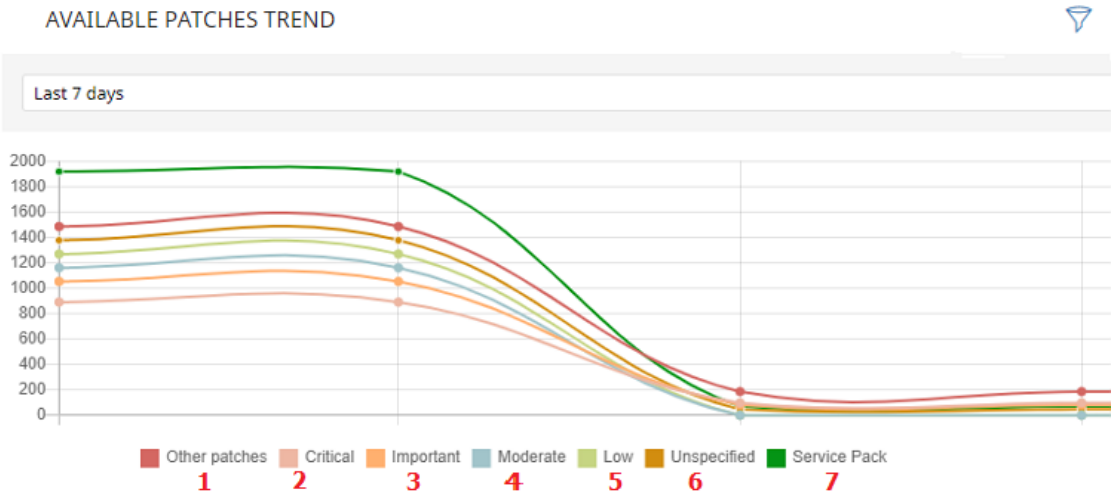


Figura 17.8: Series mostradas en el gráfico Evolución de los parches disponibles

Zona activa	Filtro
(1)	Criticidad = Otros parches (no de seguridad).
(2)	Criticidad = Critica (de seguridad).
(3)	Criticidad = Importante (de seguridad).
(4)	Criticidad = Moderada (de seguridad).
(5)	Criticidad = Baja (de seguridad).
(6)	Criticidad=No clasificado (de seguridad)
(9)	Criticidad = Service Pack.

Tabla 17.13: Definición de filtros del listado Parches disponibles por equipos

Filtros disponibles sobre el widget

Al hacer clic en el icono se muestran los filtros disponibles, que se aplican sobre la información mostrada en el propio widget:

Filtro	Definición
Tipo de equipo	• Estación • Portátil • Servidor

Filtro	Definición
Plataforma	• Todos • Windows • Linux • macOS
Tipo de parche	• Parches de sistema operativo: parches disponibles para sistemas operativos Windows, Linux y macOS. • Parches de aplicaciones: parches disponibles para las aplicaciones.

Tabla 17.14: Filtros disponibles para el widget Evolución de los parches disponibles

Parches disponibles en más equipos

Muestra el número de equipos afectados por cada parche disponible en estado **Pendiente**.

Significado de las series

Serie	Descripción
Nombre	Nombre del parche disponible.
Número	Número de equipos con el parche disponible en estado **Pendiente**.
Enlace Ver todos los parches disponibles	Acceso al listado completo de parches disponibles por equipos.

Tabla 17.15: Descripción de las series de Parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra un tooltip con la siguiente información:

- Nombre del parche.
- Número de equipos que tienen disponible el parche.
- Programa (o familia del sistema operativo).
- Criticidad.
- Fecha de publicación
- Número CVE (Common Vulnerabilities and Exposures).

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles por equipos**, filtrado por el parche seleccionado.

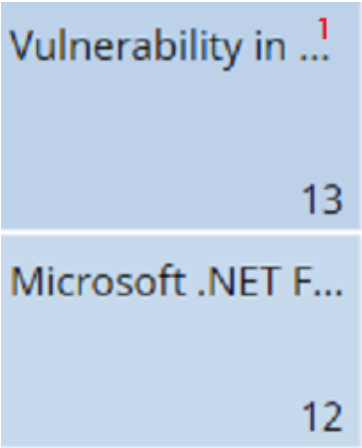


Figura 17.9: Zonas activas del panel Parches disponibles en más equipos

Zona activa	Filtro
(1)	Parche = Nombre del parche seleccionado

Tabla 17.16: Definición de filtros del listado Parches disponibles en más equipos

Filtros disponibles sobre el widget

Haz clic en el icono para mostrar los filtros disponibles que se aplican sobre la información mostrada en el propio widget:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	• Estación

Filtro	Descripción	Valores
		• Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones • Parches de sistema operativo

Tabla 17.17: Filtros del panel Parches disponibles en más equipos

Programas con más parches disponibles

Muestra los programas con más parches disponibles para instalar, y su número.

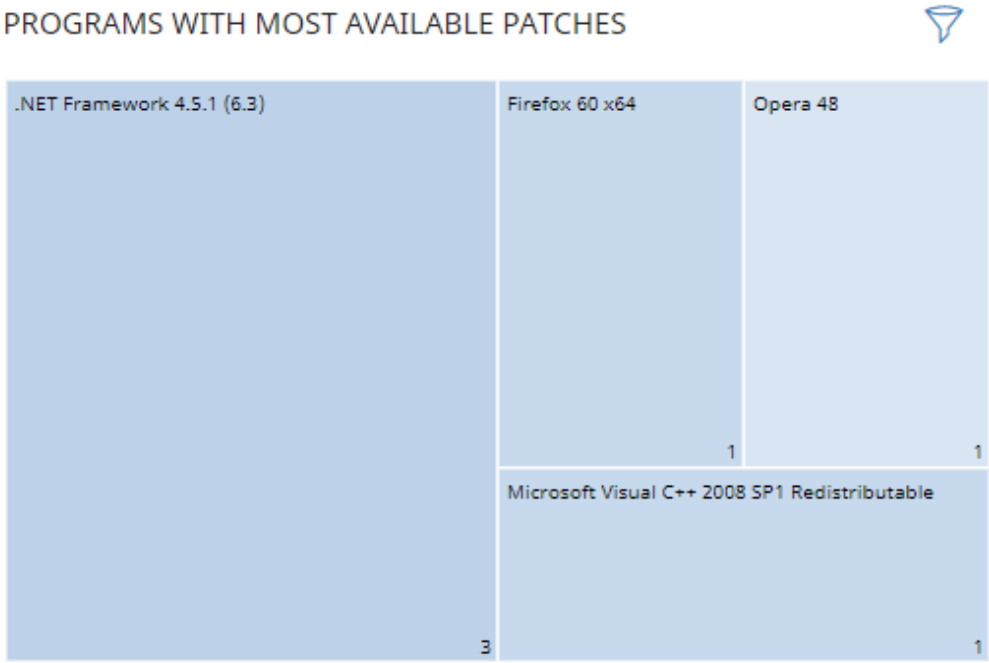


Figura 17.10: Panel Programas con más parches disponibles

Significado de las series

Serie	Descripción
Nombre	Nombre del programa con más parches disponibles.
Número	Número de parches disponibles para el programa.

Tabla 17.18: Descripción de las series del panel Programas con más parches disponibles en más equipos

Al situar el cursor del ratón sobre un cuadro, se muestra una etiqueta con la siguiente información:

- Nombre del programa.
- Número de parches disponibles para el programa.

Filtros preestablecidos desde el panel

Al hacer clic en cualquiera de los cuadros del panel, se abre el listado **Parches disponibles por equipos**.

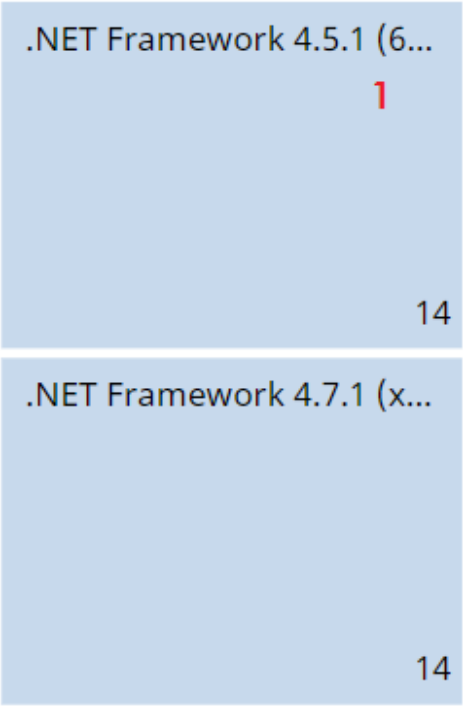


Figura 17.11: Zonas activas del panel Programas con más parches disponibles

Zona activa	Filtro
(1)	Equipo= Nombre del programa seleccionado

Tabla 17.19: Definición de filtros del listado Programas con más parches disponibles

Filtros disponibles sobre el widget

Haz clic en el icono para mostrar los filtros disponibles:

Filtro	Descripción	Valores
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Tipo de equipo	Clase de dispositivo al que se aplica el parche.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de parche	Tipo de software al que se aplicará el parche.	• Parches de aplicaciones. • Parches de sistema operativo.

Tabla 17.20: Definición de filtros del panel Programas con más parches disponibles

Listados del módulo Evaluación de vulnerabilidades

Acceso a los listados

El acceso a los listados se podrá hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Evaluación de vulnerabilidades** y en el widget relacionado.

  ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se abrirá una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Evaluación de vulnerabilidades** para ver su plantilla asociada. Modifica la plantilla y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	• Estado de evaluación de vulnerabilidades
Visualizar parches disponibles	Acceso de solo lectura a los listados: • Estado de la evaluación de vulnerabilidades • Parches disponibles por equipos • Programas "End Of Life"

Tabla 17.21: Permisos requeridos para los listados de Evaluación de vulnerabilidades

Estado de la evaluación de vulnerabilidades

Este listado muestra en detalle todos los equipos de la red compatibles con la evaluación de vulnerabilidades, e incorpora filtros que permiten localizar aquellos puestos de trabajo y servidores que no estén recibiendo el servicio por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Estado del equipo	Reinstalación del agente: • Reinstalando agente.	Icono

Campo	Comentario	Valores
	• Error en la reinstalación del agente Reinstalación de la protección: • Reinstalando la protección. • Error en la reinstalación de la protección. • Pendiente de reinicio. Estado de aislamiento del equipo: • Equipo en proceso de entrar en aislamiento. • Equipo aislado. • Equipo en proceso de salir del aislamiento. Modo Contención de ataque RDP: • Equipo en modo contención de ataque RDP. • Finalizando modo de contención: de ataque RDP.	
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Evaluación de vulnerabilidades	Estado del módulo.	• Activado • Desactivado • Error instalando (motivo del error) • Sin licencia

Campo	Comentario	Valores
		• — Sin información • Error
Última comprobación	Fecha en la que la evaluación de vulnerabilidades consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Última conexión	Fecha del último envío del estado de la evaluación de vulnerabilidades a la nube de Panda Security.	Fecha

Tabla 17.22: Campos del listado Estado de la evaluación de vulnerabilidades

*Para visualizar los datos del listado gráficamente accede al widget **Estado de la evaluación de vulnerabilidades***

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo	Cadena de caracteres

Campo	Comentario	Valores
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el módulo se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Booleano
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Estado de la evaluación de vulnerabilidades	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información

Campo	Comentario	Valores
		• Error
Fecha de la última comprobación	Fecha en la que la evaluación de vulnerabilidades consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Fecha error instalación	Fecha en la que se intentó la instalación del módulo y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	• Error en la descarga • Error en la ejecución
Error de la evaluación de vulnerabilidades	Error en la búsqueda de parches disponibles.	Numérico

Tabla 17.23: Campos del fichero exportado Estado de la evaluación de vulnerabilidades

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Última comprobación	Fecha en la que la evaluación de vulnerabilidades consultó a la nube para comprobar si se han publicado nuevos parches.	• Todos • Hace más de 3 días

Campo	Comentario	Valores
		• Hace más de 7 días • Hace más de 30 días
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha
Estado de la evaluación de vulnerabilidades	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información • Error

Tabla 17.24: Campos de filtrado para el listado Estado de la evaluación de vulnerabilidades

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se abrirá la ventana de detalle del equipo. Consulta **Información de equipo** en la página **251** para obtener más información.

Parches disponibles por equipos

Muestra el detalle de los parches disponibles y la información sobre los parches que están en proceso de instalación.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Fecha de	Fecha en la que el parche se liberó para su descarga	Fecha

Campo	Comentario	Valores
publicación	y aplicación.	
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Equipos	Número de equipos en los que está disponible el parche.	Numérico

Tabla 17.25: Campos del listado Parches disponibles por equipos

Para visualizar los datos del listado gráficamente accede al widget ***Parches disponibles*** *en la página* ***378***

Campos mostrados en fichero exportado

Utiliza el menú de contexto para exportar los datos. La exportación puede incluir todos los datos del listado de parches disponibles o una versión más reducida que muestra los datos correspondientes a la evolución de los parches disponibles durante los últimos 7 días, último mes o el último año.

Campo	Comentario	Valores
Vendor	Compañía creadora del programa desactualizado.	Cadena de caracteres

Campo	Comentario	Valores
Familia de producto	Nombre de producto con parches pendientes de aplicar o reiniciar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado.	Numérico
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades	Cadena de caracteres

Campo	Comentario	Valores
	corregidas por el parche y sus requisitos si los hubiera.	
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Equipos	Número de equipos en los que está disponible el parche.	Numérico
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS

Tabla 17.26: Campos del fichero exportado Parches disponibles por equipos

Herramienta de filtrado

Campo	Comentario	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Tipo de parche	Clase de parche disponible.	• Parches de aplicaciones • Parches de sistema operativo
Buscar equipo	Nombre del equipo.	Cadena de caracteres

Campo	Comentario	Valores
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Selecciona versión de programa, familia o vendor	La búsqueda se aplicará al programa, familia de productos o compañía seleccionada.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Mostrar parches no descargables	Indica los parches que no son descargables directamente debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 17.27: Campos de filtrado para el listado Parches disponibles por equipos

Ventana Parche detectado

Al hacer clic en una de las filas del listado se abrirá la ventana **Parche detectado**, en la que se muestra información detallada sobre el parche. Los datos pueden variar según el sistema operativo instalado en los equipos.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base, etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo con parches pendientes de aplicar.	Cadena de caracteres
Versión de programa	Número de versión del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres
Familia	Nombre de producto con parches pendientes de aplicar o reiniciar. No disponible para parches de macOS o Linux.	Cadena de caracteres
Vendor	Compañía creadora del programa desactualizado. No disponible para parches de macOS o Linux.	Cadena de caracteres
Criticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Campo	Comentario	Valores
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera. No disponible para parches de macOS o Linux.	Cadena de caracteres
Descripción	Información sobre el impacto que la vulnerabilidad podría tener en los equipos. No disponible para parches de macOS o Linux.	Cadena de caracteres

Tabla 17.28: Campos de la ventana Parche detectado

Programas "End of Life"

Muestra los programas que ya no tienen soporte por parte de sus proveedores y que por tanto son un objetivo especialmente vulnerable para el malware y las amenazas.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software en EoL.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha (en rojo si el equipo entró en

Campo	Comentario	Valores
		EOL)

Tabla 17.29: Campos del listado Programas EoL

Para visualizar los datos del listado gráficamente accede al widget ***Programas "End of life"*** *en la página* ***373***

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres

Campo	Comentario	Valores
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EoL	Fecha en la que el programa entró en EoL.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 17.30: Campos del fichero exportado Programas EoL

Herramienta de filtrado

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS
Fecha de "End Of Life"	Fecha en la que el programa entrará en EOL.	• Todos • Actualmente en "End of life" • Actualmente o en "End of life" en 1 año

Tabla 17.31: Campos de filtrado para el listado Programas EoL

Ventana Detalles del programa

Al hacer clic en uno de los programas del listado se accede a la ventana de **Detalles del programa**:

Campo	Comentario	Valores
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Familia	Bundle, suit o grupo de programas al que pertenece el software.	Cadena de caracteres
Editor/Empresa	Empresa que diseñó o publicó el programa.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha

Tabla 17.32: Campos de la ventana Detalles del programa

Capítulo 18

Gestión de amenazas, elementos en clasificación y cuarentena

Panda Endpoint Protection incorpora la capacidad de equilibrar la eficacia del servicio de seguridad con el impacto que perciben los usuarios protegidos en su actividad diaria. Este equilibro se consigue a través de herramientas que permiten gestionar la detección de las amenazas encontradas.

Contenido del capítulo

Introducción a las herramientas de gestión de amenazas

El administrador de la red puede variar el comportamiento de Panda Endpoint Protection con respecto a las amenazas encontradas mediante las herramientas siguientes:

- Permitir / dejar de permitir la ejecución de programas clasificados como virus.
- No volver a detectar / detectar programas clasificados como virus.

- Gestionar el backup / cuarentena.

No volver a detectar / detectar programas clasificados como virus

El administrador puede permitir la ejecución del software que implemente algunas funcionalidades valoradas por los usuarios pero que ha sido clasificado como una amenaza. Este es el caso, por ejemplo, de PUPs, programas generalmente en forma de barras de navegador, que ofrecen capacidades de búsqueda al tiempo que recolectan información privada del usuario o confidencial de la empresa con objetivos publicitarios. Para más información consulta **Permitir y volver a impedir la ejecución de elementos**.

Gestionar el backup / cuarentena

El administrador puede recuperar los elementos considerados como amenazas que han sido eliminados de los equipos de los usuarios.

Permitir y volver a impedir la ejecución de elementos

Restaurar / no volver a detectar programas clasificados como virus

Si los usuarios requieren cierta funcionalidad incluida en un programa que ha sido clasificado por el fichero de firmas como una amenaza, y el administrador considera que el peligro para la integridad del parque IT administrador es bajo, puede permitir su ejecución:

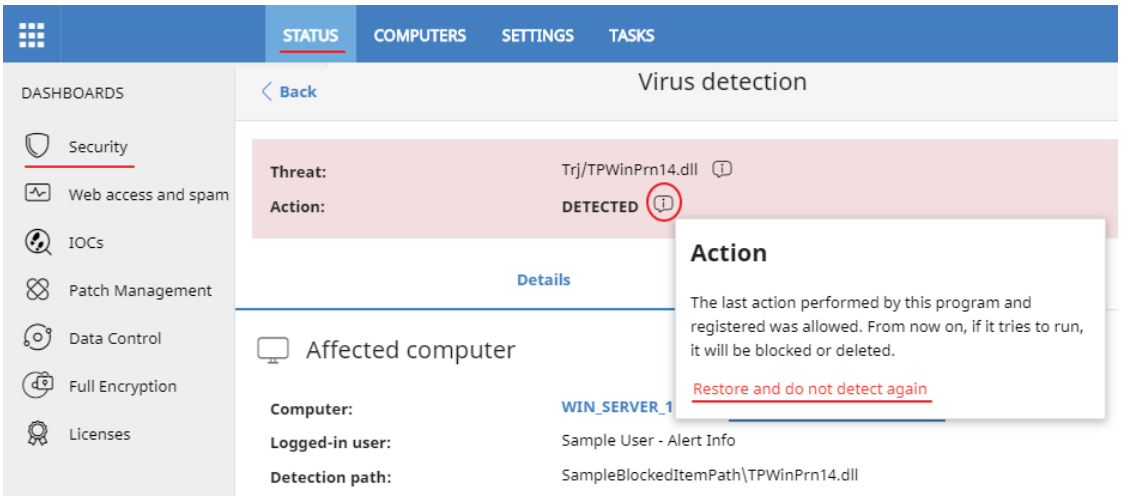


Figura 18.1: Restaurar y no volver a detectar una amenaza

Para restaurar desde la cuarentena / backup un programa borrado y no volver a detectarlo:

- Selecciona el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Amenazas detectadas por el antivirus** y selecciona el elemento que quieres permitir su ejecución.

- Haz clic en el icono del campo **Acción**. Se mostrará un ventana explicando la acción tomada por Panda Endpoint Protection.
- Haz clic en el enlace **Restaurar y no volver a detectar**. Panda Endpoint Protection ejecutará las siguientes acciones:
    - El elemento se copia desde la cuarentena / backup a su ubicación original en los equipos del parque informático.
    - El elemento podrá ser ejecutado y no generará detecciones.
    - El programa se incorpora al listado **Programas permitidos por el administrador**.

Dejar de permitir la ejecución de elementos previamente permitidos

Para volver a bloquear un elemento previamente permitido por el administrador:

- Selecciona en el menú superior **Estado**, panel lateral **Seguridad**.
- Dentro del panel **Elementos detectados permitidos por el administrador** haz clic en el tipo de elemento a dejar de permitir: **malware**, **PUP**, **exploit**, **en clasificación** o **ataques de red**.
- Dentro del panel **Programas permitidos por el administrador** haz clic en el tipo de elemento a dejar de permitir: **malware**, **PUP**, **en clasificación** o **exploits**.
- En el listado **Programas permitidos por el administrador** haz clic en el icono situado a la derecha del elemento cuya ejecución quieres dejar de permitir.

Al hacer clic en el icono asociado al elemento, Panda Endpoint Protection ejecuta las acciones siguientes:

- El elemento se retira del listado **Programas permitidos por el administrador.**
- Se añade una entrada al listado **Historial de programas permitidos por el administrador**indicando como **Acción** el valor **Exclusión eliminada por el usuario**.
- El elemento volverá aparecer en el listado **Amenazas detectadas por el antivirus.**
- El elemento volverá a generar incidentes.

Listado de amenazas permitidas

El administrador dispone de varios paneles y listados para obtener información sobre los programas que inicialmente fueron bloqueados por Panda Endpoint Protection y cuya ejecución ha sido permitida:

- El panel **Programas permitidos por el administrador**.
- El listado **Programas permitidos por el administrador**.
- El listado **Historial de programas permitidos por el administrador**.

Programas permitidos por el administrador

Muestra los programas que Panda Endpoint Protection inicialmente almacenó en cuarentena, pero cuya ejecución fue permitida por el administrador con posterioridad. Estos elementos fueron considerados como una amenaza al ser detectados mediante el fichero de firmas.

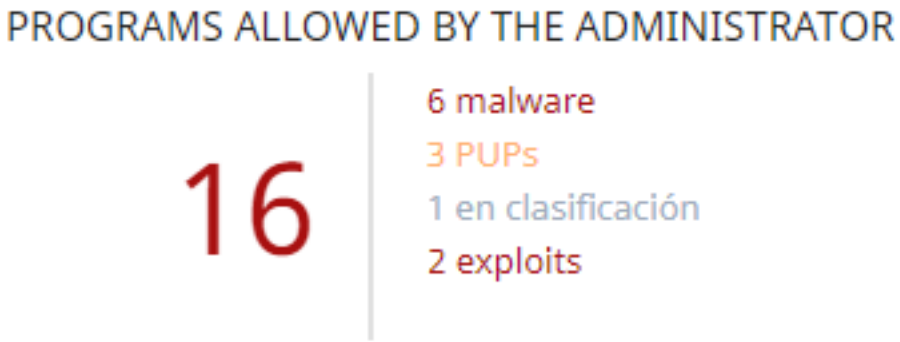


Figura 18.2: Panel Programas permitidos por el administrador

Descripción de las series

El panel representa el número total de elementos que el administrador excluyó del bloqueo, desagregados por su tipo:

- Malware
- PUP
- En clasificación
- Exploit

Filtros preestablecidos desde el panel

Figura 18.3: Zonas activas del panel Programa permitidos por el administrador

Haz clic en las zonas indicadas en **Zonas activas del panel Programa permitidos por el administrador** para abrir el listado **Listado Programas permitidos por el administrador** con los filtros preestablecidos mostrados a continuación:.

Zona activa	Filtro
(1)	Sin filtros.
(2)	Clasificación = malware.
(3)	Clasificación = PUP.
(4)	Clasificación = En clasificación (bloqueados y sospechosos).
(5)	Clasificación = Exploit.

Tabla 18.1: Definición de los filtros del listado Programas permitidos por el administrador

Listado Programas permitidos por el administrador

Muestra todos los elementos considerados amenazas que el administrador ha permitido.

Campo	Descripción	Valores
Clasificación	Tipo de la amenaza a la que se permite la ejecución.	• Malware • PUP • Goodware
Amenaza	Nombre del elemento cuya ejecución se permite.	Cadena de caracteres
Detalles	Nombre del fichero que contiene la amenaza.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Nombre de usuario	Cuenta de usuario de la consola que añadió la exclusión del elemento.	Cadena de caracteres
Permitido el	Fecha en la que se produjo el evento.	Fecha
Borrar	Elimina la exclusión del elemento.	

Tabla 18.2: Campos del listado Programas permitidos por el administrador

Campos incluidos en fichero exportado

Campo	Descripción	Valores
Detalles	Nombre del fichero que contiene la amenaza.	Cadena de caracteres
Tipo actual	Clasificación en el momento actual de la amenaza cuya ejecución se permitió.	• Malware • PUP • Goodware
Tipo original	Clasificación de la amenaza cuya ejecución se permitió en el momento en que se detectó por primera vez.	• Malware • PUP • Goodware
Amenaza	Nombre del elemento cuya ejecución se permite.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Nombre de usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido.	Cadena de caracteres
Permitido el	Fecha en la que se registró el evento.	Fecha

Tabla 18.3: Campos del fichero exportado Elementos detectados permitidos por el administrador

Herramienta de filtrado

Campo	Descripción	Valores
Buscar	• **Detalles**: detalles de la amenaza. • **Amenaza**: nombre de la amenaza detectada. • **Nombre de usuario**: cuenta de usuario de la consola que añadió la exclusión del elemento. • **Hash**: cadena resumen de identificación del archivo.	Enumeración

Tabla 18.4: Campos de filtrado para el listado Elementos detectados permitidos por el administrador

Listado Historial de programas permitidos por el administrador

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a las amenazas cuya ejecución permitió el administrador. El listado muestra el ciclo de estados completo de un fichero, desde que entra en el listado de **Programas permitidos por el administrador** hasta que lo abandona, pasando por todos los cambios de estado intermedios que Panda Endpoint Protection o el administrador provoque.

Este listado no tiene un panel asociado, y es accesible únicamente mediante el botón **Historial**, situado en la esquina superior derecha del listado **Programas permitidos por el administrador**.

Campo	Descripción	Valores
Clasificación	Tipo de la amenaza cuya ejecución se permitió.	• Malware • PUP • Goodware
Amenaza	Nombre del elemento cuya ejecución se permite.	Cadena de caracteres
Detalles	Nombre del fichero que contiene la amenaza.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido. • **Exclusión eliminada por el usuario**: el administrador permitió introducir de nuevo el elemento en la cuarentena. • **Exclusión añadida por el usuario**: el administrador permitió extraer el elemento de la cuarentena.	Enumeración
Nombre de usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido.	Cadena de caracteres
Permitido el	Fecha en la que se registró el evento.	Fecha

Tabla 18.5: Campos del listado Historial de elementos permitidos por el administrador

Campos incluidos en fichero exportado

Campo	Descripción	Valores
Detalles	Nombre del fichero que contiene la amenaza.	Cadena de caracteres
Tipo actual	Clasificación en el momento actual de la amenaza cuya ejecución se permitió.	• Malware • PUP
Tipo original	Clasificación de la amenaza cuya ejecución se permitió en el momento en que se detectó por primera vez.	• Malware • PUP
Amenaza	Nombre del malware o PUP cuya ejecución se permite.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido. • **Exclusión eliminada por el usuario**: el administrador permitió introducir de nuevo el elemento en la cuarentena. • **Exclusión añadida por el usuario**: el administrador permitió extraer el elemento de la cuarentena.	Enumeración
Nombre de usuario	Cuenta de usuario de la consola que añadió la exclusión del elemento.	Cadena de caracteres
Permitido el	Fecha en la que se produjo el evento.	Fecha

Tabla 18.6: Campos del fichero exportado Historial de Programas permitidos por el administrador

Herramienta de filtrado

Campo	Descripción	Valores
Buscar	• **Detalles**: detalles de la amenaza. • **Usuario**: cuenta de usuario de la consola que añadió la exclusión del elemento.	Enumeración

Campo	Descripción	Valores
	• **Hash**: cadena resumen de identificación del archivo.	
Acción	Acción aplicada sobre el elemento permitido. • **Exclusión eliminada por el usuario**: el administrador permitió bloquear de nuevo el elemento. • **Exclusión eliminada por reclasificación**: Panda Endpoint Protection aplica la acción asociada a la categoría obtenida de la reclasificación. • **Exclusión añadida por el usuario**: el administrador permitió ejecutar el elemento. • **Exclusión mantenida por reclasificación**: Panda Endpoint Protection no bloqueó el elemento al reclasificarlo.	Enumeración

Tabla 18.7: Campos de filtrado para el listado Historial de Programas permitidos por el administrador

Gestión de la zona de backup / cuarentena

La cuarentena en Panda Endpoint Protection es el área de backup donde se copian los elementos clasificados como amenaza que han sido eliminados.

La cuarentena se almacena en el propio equipo del usuario, en el directorio `Quarantine` dentro de la carpeta donde se instaló el software. Se trata de un área cifrada e inaccesible al resto de procesos del equipo, de manera que no es posible el acceso ni la ejecución de los programas allí contenidos de forma directa, si no es a través de la consola Web.

La cuarentena es compatible con las plataformas Windows, macOS y Linux.

El departamento de Panda Labs en Panda Security establece la acción a ejecutar en función de la clasificación y tipo de elemento detectado. De esta forma, se pueden producir las situaciones siguientes:

- **Elementos maliciosos no desinfectables**: se mantienen en cuarentena permanentemente.
- **Elementos maliciosos desinfectables**: el malware de tipo virus se desinfecta y el fichero se restaura a su ubicación original, manteniendo una copia en backup durante 30 días.

- **Elementos no maliciosos restaurados**: si se clasificó de forma errónea un elemento que es goodware (falso positivo), se restaura desde la cuarentena a su ubicación original, manteniendo una copia en backup durante 7 días.
- **Elementos sospechosos**: se almacenan en la cuarentena durante 30 días. Si finalmente resultan ser goodware, se restauran automáticamente.

Panda Endpoint Protection no borra ningún fichero del equipo del usuario. Todos los elementos eliminados son enviados al área de backup.

Visualizar los elementos en cuarentena

Para obtener un listado de los elementos introducidos en la cuarentena:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Amenazas detectadas por el antivirus**.
- En los filtros del listado haz clic en las casillas de selección **Movido a cuarentena** y **Eliminado** del campo **Acción** y haz clic en el botón **Filtrar**.

Restaurar elementos de cuarentena

- Haz clic en el menú superior **Estado** y en el panel lateral **Seguridad**.
- Haz clic en el panel **Amenazas detectadas por el antivirus**.
- En el listado, selecciona la amenaza cuyo campo **Acción** muestre **Movido a Cuarentena** o **desinfectado**.
- Haz clic en el icono del campo **Acción**. Se mostrará una ventana que explica el motivo del movimiento del elemento a cuarentena.
- Haz clic en el enlace **Restaurar y no volver a detectar**. El elemento se moverá a su ubicación original. Se restaurarán también los permisos, propietario, entradas del registro referidas al fichero y otra información.

Capítulo 19

Alertas

El sistema de alertas es un recurso utilizado por Panda Endpoint Protection para comunicar de forma rápida al administrador situaciones que afectan al buen funcionamiento del servicio de seguridad.

En conjunto, las alertas informan al administrador de las situaciones mostradas a continuación:

- Detección de malware.
- Detección de ataques de red.
- Intento de uso de dispositivos externos no autorizados
- Reclasificación de elementos desconocidos, malware o PUP.
- Cambios en el estado de las licencias.
- Errores de instalación y desprotegidos.

Contenido del capítulo

Alertas por correo

Son mensajes generados por Panda Endpoint Protection cuando se producen determinados eventos y enviados a las cuentas de correo configuradas como destinatarios, generalmente mantenidas por los administradores de la red.

Acceso a la configuración de alertas

Desde el menú superior **Configuración**, en el panel de la izquierda **Mis alertas** se accede al menú de **Alertas** por correo en el que se establecen las opciones de las alertas por correo.

Configuración de alertas

La configuración de las alertas se divide en tres partes:

- **Enviar alertas en los siguientes casos**: selecciona que eventos generan una alerta. Consulta Tipos de alertas para más información.
- **Enviar alertas a la siguiente dirección**: introduce las direcciones de correo que recibirán la alerta.
- **Enviar las alertas en el siguiente idioma**: elige el idioma del mensaje de alerta entre los soportados por la consola:
    - Alemán
    - Español
    - Francés
    - Inglés
    - Italiano
    - Japonés
    - Magiar
    - Portugués
    - Sueco

Nivel de acceso del administrador y envío de alertas

Las alertas se definen de forma independiente por cada usuario de la consola. El contenido de una alerta queda limitado por la visibilidad de los equipos administrados que tiene asignado el rol de la cuenta de usuario.

Tipos de alertas

Tipo	Frecuencia	Condición	Información contenida
Detecciones de malware (solo protección en tiempo real)	Máximo 2 mensajes por equipo – malware – día.	• Por cada malware detectado en tiempo real en el equipo. • Solo en equipos Windows.	• Primer o segundo mensaje. • Nombre del programa malicioso. • Nombre del equipo. • Grupo. • Fecha y hora UTC.

Tipo	Frecuencia	Condición	Información contenida
			• Ruta del programa malicioso. • Hash. • Tabla de acciones de programa. • Listado de equipos donde fue previamente visto el malware.
URLs con malware bloqueadas	Cada 15 minutos	• Cuando se producen detecciones de URL que apuntan a malware.	• Número de URL que apuntan a malware detectadas en el intervalo de tiempo. • Número de equipos afectados.
Detecciones de phishing	Cada 15 minutos	• Cuando se produzcan detecciones de phishing.	• Número de ataques de phishing detectadas en el intervalo de tiempo. • Número de equipos afectados.
Intentos de intrusión bloqueados	Cada 15 minutos	• Cuando se producen intentos de intrusión bloqueados por el módulo IDS. • Compatible con equipos Windows.	• Número de intentos de intrusión bloqueados en el intervalo de tiempo.

Tipo	Frecuencia	Condición	Información contenida
			• Número de equipos afectados.
Dispositivos bloqueados	Cada 15 minutos	• Se producen accesos por parte del usuario a dispositivos y periféricos bloqueados por el administrador. • Compatible con equipos Windows, Linux, macOS y Android.	• Número de accesos bloqueados a dispositivos. • Número de equipos afectados.
Equipos con error en la protección	Cada vez que se detecte el hecho relevante	• Por cada equipo desprotegido de la red. • Equipos con la protección en estado de error o fallo en la instalación de la protección	• Nombre del equipo. • Grupo. • Descripción. • Sistema operativo. • Dirección IP. • Ruta del directorio activo. • Dominio. • Fecha y hora UTC. • **Motivo de la desprotección**: Protección con error o Error instalando.
Equipos sin licencia	Cada vez que se detecte el hecho relevante	Por cada equipo que intenta licenciarse, pero no lo consigue por falta de licencias libres.	• Nombre del equipo. • Descripción. • Sistema operativo • Dirección IP

Tipo	Frecuencia	Condición	Información contenida
			• Grupo • Ruta del directorio activo • Dominio. • Fecha y hora UTC. • Motivo de la desprotección: equipo sin licencia.
Errores durante la instalación	Cada vez que se detecte el hecho relevante	• Por cada uno de los equipos de la red, cada vez que se crea una nueva situación que derive en el cambio de estado **(1)** de protegido a desprotegido. • Si en un mismo momento se detectan varios motivos que derivan en el cambio de estado en un mismo equipo, solo se genera una alerta con todos los motivos.	• Nombre del equipo. • Estado de la protección. • Razón del cambio del estado de la protección.

Tipo	Frecuencia	Condición	Información contenida
Equipos no administrados descubiertos	Cada vez que se detecte el hecho relevante	• Cada vez que un equipo descubridor termina un descubrimiento. • El descubrimiento ha encontrado equipos no vistos anteriormente en la red.	• Nombre del equipo descubridor. • Número de equipos descubiertos. • Enlace al listado de los equipos descubiertos en la consola.

Tabla 19.1: Tabla de alertas

Cambios de estado (1)

Las razones de cambio de estado que generan una alerta son:

- **Protección con error**: sólo se contempla el estado de las protecciones antivirus.
- **Error instalando**: se enviará alerta cuando se haya producido un error en la instalación que requiera de la intervención del usuario (e.g., no hay espacio en disco), y no ante errores transitorios que podrían solucionarse autónomamente tras varios reintentos.
- **Sin licencia**: cuando el equipo no ha recibido una licencia tras registrarse, por no haber libres en ese momento.

Las razones de cambio de estado que no generan una alerta son:

- **Sin licencia**: cuando el administrador ha quitado la licencia al dispositivo o cuando Panda Endpoint Protection haya retirado la licencia automáticamente al equipo por haberse reducido el número de licencias contratadas.
- **Instalando**: por no resultar útil recibir una alerta cada vez que se instala un equipo.
- **Protección desactivada**: este estado es consecuencia de un cambio de configuración voluntario.
- **Protección desactualizada**: no implica necesariamente que el equipo este desprotegido, pese a estar desactualizado.
- **Pendiente de reinicio**: no implica necesariamente que el equipo este desprotegido.
- **Desactualizado el conocimiento**: no implica necesariamente que el equipo este desprotegido.

Dejar de recibir alertas por correo

Si el destinatario de las alertas por correo quiere dejar de recibirlas pero no tiene acceso a la consola de Panda Endpoint Protection o no tiene permisos suficientes para modificar la configuración, puede darse de baja del servicio si sigue los pasos mostrados a continuación:

- Haz clic en el enlace del pie de mensaje **"Si no deseas recibir más mensajes de este tipo, pincha aquí."**. Se mostrará una ventana pidiendo la dirección de correo del usuario. El enlace tiene una caducidad de 15 días.
- Si se ha introducido una dirección de correo que pertenece a alguna configuración de Panda Endpoint Protection se envía un correo al usuario para confirmar la baja de notificaciones para esa cuenta.
- Haz clic en el enlace del nuevo correo para retirar la cuenta de correo de todas la configuraciones en las que aparezca. El enlace tiene una caducidad de 24 horas.

Capítulo 20

Envío programado de informes y listados

Panda Endpoint Protection envía por correo electrónico toda la información de seguridad que se produce en los equipos que protege. Este método de entrega facilita la compartición de información entre los distintos departamentos de la empresa, así como permite guardar un histórico de todos los eventos producidos por la plataforma, más allá de los límites de capacidad de la consola Web. De esta forma, es posible realizar un seguimiento completo del estado de la seguridad sin necesidad de que el administrador tenga que acudir a la consola web, ahorrando tiempo de gestión.

El envío automático de informes por correo electrónico permite entregar a las personas interesadas toda la información de los eventos de seguridad generados, sin dejar espacio a manipulaciones para poder evaluar de forma precisa el estado de la seguridad de la red.

Contenido del capítulo

Características de los informes

Según el intervalo de tiempo abarcado

Dependiendo del momento en el que se produce la información incluida en el informe se distinguen dos tipos:

- **Informes consolidados**: reúnen en un solo documento toda la información generada en un intervalo de fechas.
- **Informes instantáneos**: contienen información que refleja el estado de la seguridad de la red en un momento concreto.

Según la forma de envío

Panda Endpoint Protection genera y envía informes de forma automática según la configuración establecida en el programador de tareas o de forma manual bajo demanda.

Con el envío de informes automáticos, los destinatarios obtendrán de forma automática y sin necesidad de acudir a la consola Web la información producida en el parque de equipos gestionado.

Según el formato de salida

Dependiendo del tipo de informe Panda Endpoint Protection entrega informes en formato pdf y /o csv.

Según su contenido

Dependiendo del tipo de informe su contenido será configurable, permitiendo abarcar más o menos módulos soportados por Panda Endpoint Protection o estableciendo filtros para limitar la información a equipos que cumplan con determinadas características.

Tipos de informes

Panda Endpoint Protection permite generar 3 tipos de documentos, cada uno de ellos con sus características asociadas:

- Vistas de listados
- Informes ejecutivos
- Listados de dispositivos

A continuación se resumen las características de cada tipo de informe:

Tipo	Intervalo	Envío	Contenido	Salida
Vistas de	Instantáneo	Automático	Configurable	csv

Tipo	Intervalo	Envío	Contenido	Salida
listados			mediante búsquedas	
Informes ejecutivos	Consolidado	Automático y bajo demanda	Configurable por categorías y por grupos	pdf,csv, excel, word
Listados de dispositivos	Instantáneo	Automático	Configurable mediante filtros	csv

Tabla 20.1: Resumen de tipos de informes y sus características

Requisitos para generar informes

Los usuarios con el rol de solo lectura podrán previsualizar los informes ejecutivos pero no podrán programar el envío de nuevos informes.

A continuación se detallan las tareas previas que el administrador deberá realizar antes de poder utilizar la funcionalidad de envío de informes y listados programados.

Vistas de listados

El administrador deberá de crear previamente una vista y configurar las herramientas de búsqueda hasta que el listado muestre la información que considere relevante. Una vez hecho esto podrá crear un informe programado. Consulta **Crear un listado personalizado** en la página **47** para obtener información de cómo crear vistas de listados con búsquedas asociadas.

Informes ejecutivos

No es necesaria la ejecución de ninguna tarea previa: su contenido se determina en el momento de configurar el informe programado.

Listado de dispositivos filtrado

El administrador deberá crear un filtro o utilizar uno de los filtros ya creados en Panda Endpoint Protection. Consulta **Árbol de filtros** en la página **212** para obtener más información acerca del manejo y configuración de los filtros.

Acceso al envío de informes y listados

Desde la sección Informes programados

Para acceder al listado de tareas que envían informes y listados haz clic en el menú superior **Estado**, panel lateral **Informes programados**. Se mostrará una pantalla con las herramientas necesarias para buscar tareas de envío ya creadas, editarlas, borrarlas o crear nuevas.

Desde una vista de listado

Las vistas de listados se almacenan en el panel lateral izquierda del menú superior **Estado**, y cada una de ellas puede enviarse de forma programada siguiendo los pasos mostrados a continuación:

- **Desde el menú de contexto**: haz clic en el menú de contexto de la vista de listado y en la opción **Programar informe**. Se mostrará la ventana de información requerida explicada en **Configuración de los informes y listados**.
- **Desde la propia vista del listado**: haz clic en el icono situado en la esquina superior derecha de la ventana. Se mostrará la ventana de información requerida explicada en **Configuración de los informes y listados**.

Al completarse la creación del informe programado se mostrará un mensaje emergente en la esquina superior derecha de la pantalla indicado la generación de una nueva tarea de envío.

Desde un filtro

- En el menú superior **Equipos** haz clic en la pestaña para mostrar el árbol de filtros.
- Al hacer clic en un filtro, el listado de dispositivos se actualizará para mostrar los dispositivos cuyos atributos satisfagan las condiciones impuestas por el filtro seleccionado.
- Haz clic en el icono del menú de contexto asociado al filtro y selecciona la opción **Programar Informe**. Se mostrará la ventana de información requerida explicada en **Configuración de los informes y listados**.

Al completarse la creación del informe programado se mostrará un mensaje emergente en la esquina superior o inferior derecha de la pantalla indicado la generación de una nueva tarea de envío y un enlace para ver el listado de informes programados. Consulta **Configuración de los informes y listados**.

Gestión de informes

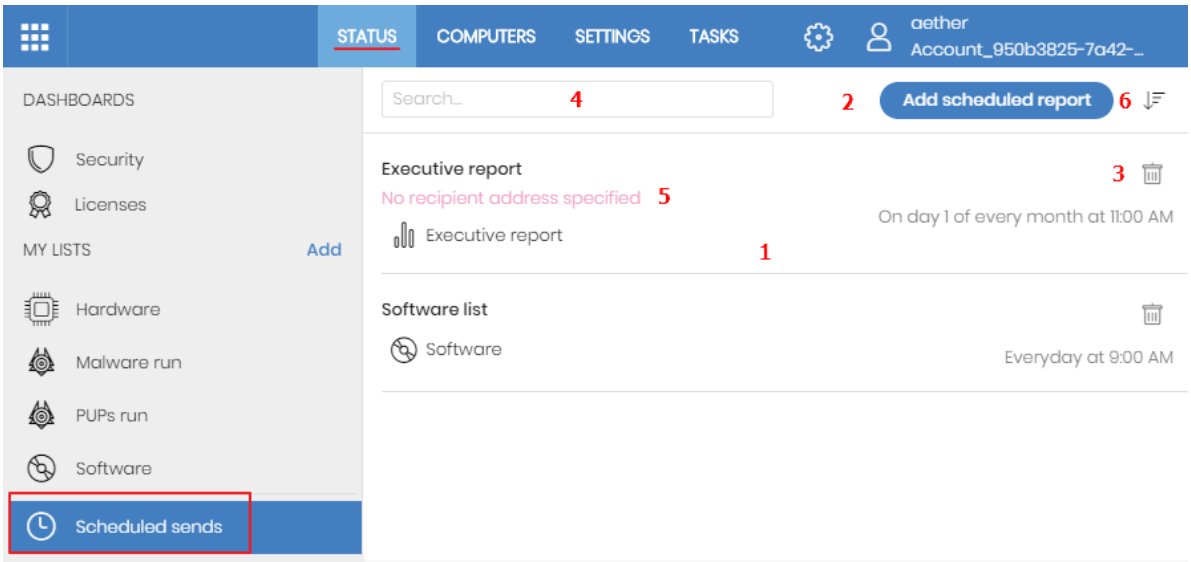


Figura 20.1: Ventana para gestionar los informes programados

Para crear, borrar, editar y listar informes programados haz clic en el menú superior **Estado** y en el menú lateral **Informes programados**.

Listado de Informes programados

En el panel de la derecha se muestran los informes programados ya creados).

Todas las tareas de envío incluye un nombre y debajo una serie de mensajes que indican si faltan datos por indicar en la configuración del informe programado **(5)**.

Crear Informes programados

Haz clic sobre el botón **Añadir Informe programado (2)** para mostrar la ventana de configuración.

Consulta **Configuración de los informes y listados** para obtener información sobre los datos que el administrador debe aportar al crear un informe programado.

Ordenar Informes programados

Haz clic en el icono **(6)** para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Borrar y editar Informes programados

Para borrar y editar un informe programado sigue los pasos mostrados a continuación:

- Para borrar un informe programado utiliza el icono (**3**).
- Haz clic en el nombre del informe programado para editarlo.

Una vista de listado o listado filtrado que tenga configurado un informe programado no podrá borrarse hasta que el informe programado sea eliminado.
Los listados enviados por un informe programado se corresponden a una vista de listado o a un listado filtrado concretos. Si éstos son modificados, el informe programado se actualizará con la nueva configuración.

Configuración de los informes y listados

Campo	Descripción
Nombre	Nombre de la entrada que se mostrará en el listado de informes programados.
Enviar automáticamente	Frecuencia de envío del informe o listado: • **Todos los días**: el envío se producirá todos los días a la hora seleccionada. • **Todas la semanas**: el envío se producirá todos las semanas a la hora y día de la semana seleccionados. • **Todos los meses**: el envío se producirá todos los meses en el día del mes y hora seleccionados.
Tipo de informe	Tipo de informe que se enviará: • Informe ejecutivo • Listado • Filtro El contenido del informe varía según su tipo. Para más información, consulta **Contenido de los informes y listados**.
Previsualizar informe	Este enlace solo se muestra cuando el tipo de informe elegido es Informe ejecutivo. Al hacer clic, se abrirá una nueva pestaña en el navegador con el contenido del informe para previsualizarlo. De esta manera es posible configurar el informe, descargarlo o imprimirlo mediante la barra de herramientas superior.

Campo	Descripción
	Para los listados y filtros el formato elegido es csv, por lo que la opción de previsualizar no está disponible.
Fechas	Intervalo de tiempo que abarca el informe. Esta configuración de fechas solo está disponible para los informes ejecutivos. • Último mes • Últimos 7 días • Últimas 24 horas En el caso de los listados y filtros el informe obtenido es de tipo instantáneo, por lo que la información que muestra es la correspondiente al estado de la seguridad en el momento en que se genera el informe. Para más información, consulta **Características de los informes**.
Equipos	De qué equipos se extraen datos para generar el informe ejecutivo: • **Todos los equipos**. • **Los grupos seleccionado**s: muestra el árbol de grupos para seleccionar de forma individual los grupos mediante las casillas de selección. Este campo solo está disponible cuando el tipo de informa es Informe ejecutivo.
Para	Direcciones de correo separadas por comas que recibirán el informe.
CC	Direcciones de correo en copia separadas por comas que recibirán el informe.
CCO	Direcciones de correo en copia oculta separadas por comas que recibirán el informe.
Asunto	Frase resumen que describe el correo.
Formato	• **Para vistas de listado**: adjunta un fichero en formato csv al correo. • **Para informes ejecutivos**: adjunta al correo electrónico el informe en formato .PDF, Excel o Word.

Campo	Descripción
Idioma	Idioma en el que se envía el informe.
Contenido	Tipo de información que incluye el informe: • **Tabla de contenidos**: índice de los distintos apartados dentro del informe. • **Estado de licencias**: muestra la información de las licencias contratadas, consumidas y su fecha de caducidad. Consulta Licencias en la página 185 para más información. • **Estado de seguridad**: funcionamiento del software Panda Endpoint Protection en los equipos de la red donde ha sido instalado. • **Detecciones**: muestra las amenazas detectadas en la red. • **Riesgos**: muestra el estado global del riesgo de seguridad asignado a los equipos. Consulta Paneles/widgets del módulo Evaluación de riesgos en la página 517 • **Gestión de parches**: muestra el estado del parcheo de los equipos. Consulta Paneles/widgets en Panda Patch Management en la página 369 para más información. • **Estado de la evaluación de vulnerabilidades**: muestra los equipos de la red que contienen software con vulnerabilidades conocidas, e informa sobre la disponibilidad de parches para evitar su impacto en los equipos. Visible solo si el cliente no tiene contratado Patch Management Para más información, consulta Paneles/widgets de Evaluación de vulnerabilidades en la página 528 • **Cifrado**: muestra el estado del cifrado en los equipos de la red. Consulta Paneles / widgets del módulo Panda Full Encryption en la página 450 para más información. Consulta Contenido de los informes y listados.

Tabla 20.2: Información para generar informes bajo demanda

Contenido de los informes y listados

Listados

El contenido de los listados enviados equivale a la opción **Exportar** o **Exportación detallada** de una vista de listado. Si la vista de listado soporta exportación detallada, al configurar el envío se muestran dos opciones:

- **Informe resumido**: se corresponde con la opción **Exportar** del listado.
- **Informe completo**: se corresponde con la opción **Exportación detallada** del listado.

Los listados que admiten exportación detallada son:

- Inventario de Software
- Historial de instalaciones de parches

Consulta **Gestión de listados** en la página **42** para obtener información sobre los tipos de listados disponibles en Panda Endpoint Protection y su contenido.

El listado incluirá información de los equipos visibles por la cuenta de usuario que modificó por última vez el informe programado. Por esta razón, un listado modificado por una cuenta con menor visibilidad que la cuenta que lo creó inicialmente contendrá información de un número de equipos menor que la que mostró en el momento de su creación.

Listados de dispositivos

El contenido del informe enviado se corresponde con la exportación simple del listado de dispositivos filtrados por un criterio. Consulta **Equipos** en la página **228** para obtener información sobre el contenido del fichero csv enviado y **Árbol de filtros** en la página **212** para obtener información acerca del manejo y configuración de los filtros.

Informe ejecutivo

Dependiendo de la configuración establecida en el campo **Contenido**, el informe ejecutivo contendrá los datos mostrados a continuación:

Información general

- **Creado el**: fecha de generación del informe.
- **Periodo**: intervalo de tiempo que abarca el informe.

- **Información incluida**: equipos de la red incluidos en el informe.

Tabla de contenidos

Índice con enlaces a las distintas secciones incluidas en el informe ejecutivo.

Estado de las licencias

- **Licencias contratadas**: número de licencias adquiridas por el cliente.
- **Licencias consumidas**: número de licencias asignadas a los equipos de la red.
- **Fecha de caducidad**: fecha en la que caduca el mantenimiento.

Consulta **Licencias** en la página **185**.

Estado de seguridad

Funcionamiento del módulo de protección en los equipos de la red donde ha sido instalado.

- **Estado de protección**: consulta **Estado de protección** en la página **470**.
- **Equipos conectados**: consulta **Equipos sin conexión** en la página **473**.
- **Protecciones actualizado**: consulta **Protección desactualizada** en la página **474**.
- **Conocimiento actualizado**: consulta **Protección desactualizada** en la página **474**.

Detecciones

Amenazas detectadas en la red.

- **Clasificación de todos los programas ejecutados y analizados**: consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.
- **Equipos con más detecciones (top 10)**: los 10 equipos con mayor número de detecciones realizadas por el módulo de antivirus el en el intervalo configurado:
    - **Equipo**: nombre del equipo.
    - **Grupo**: grupo al que pertenece el equipo.
    - **Detecciones**: número de detecciones en el intervalo configurado.
    - **Primera detección**: fecha de la primera detección.
    - **Última detección**: fecha de la última detección.
- **Actividad del malware**: consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.
- **Actividad de PUPs:** consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.
- **Actividad de exploits**: consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.

- **Protección contra ataques de red**: consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.
- **Últimas detecciones de malware**: consulta **Detección del malware**.
- **Últimas detecciones de PUPs**: consulta **Detección del malware**.
- **Últimas detecciones de exploits**: consulta **Detección exploit**.
- **Últimas detecciones de ataques de red**: consulta **Listados del módulo de seguridad** en la página **478**
- **Amenazas detectadas por el antivirus**: consulta **Amenazas detectadas por el antivirus** en la página **475**.
- **Filtrado de contenidos en Exchange servers**: consulta **Paneles/Widgets del módulo de seguridad** en la página **470**.

Riesgos

Estado global del riesgo de seguridad asignado a los equipos. Consulta **Paneles/widgets del módulo Evaluación de riesgos** en la página **517**

- **Riesgo de la compañía**: número de equipos que se encuentran en alguno de los niveles de riesgo establecidos.
- **Evolución del riesgo**: evolución del número de equipos que se encuentran en algún nivel de riesgo a lo largo de un periodo de tiempo determinado.
- **Riesgos detectados**: lista de los riesgos que más veces se han detectado en los equipos.
- **Equipos en riesgo (Top 10)**: lista de los 10 equipos con el nivel de riesgo global más elevado.

Gestión de parches

Estado del parcheo de los equipos.

- **Estado de gestión de parches**: consulta **Estado de gestión de parches** en la página **370**.
- **Equipos con más parches disponibles (top 10)**: listado de los 10 equipos de la red que tiene más parches disponibles sin instalar agrupados por su tipo: parches de seguridad, parches no de seguridad y Service Packs. Consulta **Equipos con más parches disponibles** en la página **384**.
- **Parches más críticos (top 10)**: listado de los 10 parches más críticos ordenado por el número de equipos afectados.
- **Evolución de los parches disponibles:** muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad. Consulta **Evolución de los parches disponibles** en la página **375**.

Evaluación de vulnerabilidades

- **Estado de la evaluación de vulnerabilidades**: muestra los equipos donde la evaluación de vulnerabilidades está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. Consulta **Estado de la evaluación de vulnerabilidades** en la página **529**.

  Tiempo desde la última comprobación: muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo para comprobar su estado de parcheo. Consulta **Tiempo desde la última comprobación** en la página **532**.

- **Parches más críticos (top 10)**: listado de los 10 parches más críticos ordenado por el número de equipos afectados.
- **Programas con más parches disponibles (top 10)** listado de los 10 programas con más parches disponibles para su instalación.
- **Evolución de los parches disponibles:** muestra la evolución de los parches pendientes de instalar en los equipos de la red según su criticidad. Consulta **Evolución de los parches disponibles** en la página **536**.

Cifrado

Estado del cifrado de los equipos. Incluye los widgets y listados mostrados a continuación:

- **Estado del cifrado**: consulta **Estado del cifrado** en la página **451**.
- **Equipos compatibles con cifrado**: consulta **Equipos compatibles con cifrado** en la página **452**.
- **Equipos cifrados**: consulta **Equipos cifrados** en la página **454**.
- **Método de autenticación aplicado**: consulta **Métodos de autenticación aplicados** en la página **456**.
- **Últimos equipos cifrados**: listado de los 10 equipos que han sido cifrados recientemente por Panda Full Encryption, ordenados por 'Fecha de cifrado'. Cada linea del listado contiene el nombre del equipo, grupo al que pertenece, sistema operativo instalado, método de autenticación configurado y fecha de cifrado.

Capítulo 21

Herramientas de resolución

Panda Endpoint Protection cuenta con varias herramientas de resolución que permiten al administrador solucionar los problemas encontrados en las fases de Protección, Detección y Monitorización del ciclo de protección adaptativa. Algunas de estas herramientas son automáticas y no necesitan que el administrador intervenga, otras sin embargo requieren la ejecución de acciones concretas a través de la consola Web.

Contenido del capítulo

Herramientas de resolución disponibles en Panda Endpoint Protection muestra las herramientas disponibles por plataforma y sus características.

Herramienta de resolución	Plataforma	Tipo	Acción
Análisis y desinfección automático de equipos	Windows, macOS, Linux, Android	Automático	Detecta y desinfecta el malware cuando se registra un movimiento en el sistema de ficheros (copia, movimiento, ejecución) o en un vector de infección soportado.

Herramienta de resolución	Plataforma	Tipo	Acción
Análisis y desinfección bajo demanda de equipos	Windows, macOS, Linux, Android	Automático (Programado) / Manual	Detecta y desinfecta el malware en el sistema de ficheros cuando lo requiera el administrador: en franjas horarias concretas o cuando cree la tarea de resolución.
Reinicio bajo demanda	Windows	Manual	Fuerza un reinicio del equipo para aplicar actualizaciones, completar desinfecciones manuales y corregir errores detectados en la protección.

Tabla 21.1: Herramientas de resolución disponibles en Panda Endpoint Protection

Análisis y desinfección automática de equipos

Los módulos de protección Panda Endpoint Protection detecta y desinfecta de forma automática las amenazas encontradas en los equipos protegidos y recibidas en los siguientes vectores de infección:

*La desinfección automática no requiere de la intervención del administrador, si bien es necesario que esté seleccionada la casilla **Protección de archivos** en la configuración de seguridad asignada al equipo. Consulta **Configuración de la seguridad en estaciones y servidores** en la página **319** para más información sobre las configuraciones disponibles en el módulo antivirus de Panda Endpoint Protection.*

- **Web**: malware que se recibe mediante una descarga producida por el navegador web.
- **Correo**: malware que se recibe como adjunto de un correo en el cliente instalado en el equipo.
- **Sistema de ficheros**: cuando se ejecuta, se mueve o se copia un fichero que contiene una amenaza conocida o desconocida y reside en el sistema de almacenamiento del equipo.
- **Red**: intentos de intrusión recibidos por la red y bloqueados por el cortafuegos.

Ante la detección de una amenaza conocida, Panda Endpoint Protection desinfecta de forma automática los elementos afectados siempre y cuando exista un método de desinfección conocido. En su defecto, el elemento se moverá a cuarentena.

Análisis y desinfección bajo demanda de equipos

Para analizar y desinfectar los equipos de usuario bajo demanda, Panda Endpoint Protection utiliza la infraestructura de tareas.

Permisos necesarios

La cuenta de usuario utilizada para acceder a la consola web tiene que tener asignado el permiso **Lanzar análisis y desinfectar** a su rol. Para obtener más información sobre el sistema de permisos consulta **Gestión de roles y permisos** en la página **66**.

Tipos de tareas de análisis bajo demanda

Inmediatas (opción Analizar ahora)

Tarea de inicio inmediato que analiza y desinfecta el sistema de ficheros local (no analiza las unidades de red).

Panda Endpoint Protection crea una tarea con las características siguientes:

- **Tiempo de ejecución máxima de la tarea**: sin límite.
- **Inicio de la tarea**:
    - Si el equipo esta encendido, la tarea se inicia en el momento de su lanzamiento.
    - Si el equipo está apagado, la tarea retrasa su ejecución hasta los siguientes 7 días.
- Los elementos del equipo analizado en busca de malware son los siguientes:
    - **Todo el ordenador**:
        - Memoria.
        - Sistema de arranque.
        - Cookies.
        - Dispositivos de almacenamiento interno. Sistema de ficheros completo, todas las extensiones.
        - Dispositivos de almacenamiento conectados físicamente al equipo (discos USB y otros). Sistema de ficheros completo, todas las extensiones.
    - **Áreas críticas**:

    - Memoria.
    - Sistema de arranque.
    - Cookies.
    - %windir%\system32, %windir%\SysWow64. Todas las extensiones.
- La acción predeterminada del proceso de análisis es:
    - **Para ficheros desinfectables**: se reemplazan los ficheros desinfectados por una versión desinfectada.
    - **Para ficheros no desinfectables**: se eliminan y se realiza una copia de seguridad en la cuarentena.

Programadas (opción Análisis programado)

Crea una tarea sin configurar. Para más información acerca de cómo configurar una tarea de análisis consulta **Configuración de una tarea de análisis**.

Acceso a las tareas de análisis y desinfección bajo demanda

Desde el Árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpetas** del árbol de equipos situado en el panel izquierdo.
- Para lanzar un análisis inmediato sobre un grupo de equipos haz clic en el menú de contexto del grupo y selecciona **Analizar ahora**. Se mostrará la ventana **Selecciona el tipo de análisis**.
- Selecciona el tipo de análisis: **Todo el ordenador** o **Áreas criticas (Recomendado)** y haz clic en el botón **Aceptar**. Se mostrará el mensaje **Nueva tarea de análisis creada** y la tarea se añadirá a la lista de tareas en la sección **Tareas**.
- Para programar una tarea de análisis en un grupo de equipos haz clic en el menú de contexto del grupo y selecciona **Programar análisis**. Se creará una nueva tarea de análisis. Para configurarla consulta **Configuración de una tarea de análisis**.

Desde el listado del árbol de equipos

- Selecciona el menú superior **Equipos** y haz clic en la pestaña **Carpetas** del árbol de equipos situado en el panel izquierdo.
- Selecciona el grupo de equipos y haz clic en las casillas de selección del listado de equipos.
- Para lanzar un análisis inmediato, si has seleccionado un solo equipo haz clic en el menú de contexto asociado al equipo y selecciona **Analizar ahora**. Si has seleccionado varios, haz clic en **Analizar ahora** en la barra superior de herramientas. Se mostrará la ventana **Selecciona el tipo de análisis**.

- Selecciona el tipo de análisis: **Todo el ordenador** o **Áreas criticas (Recomendado)** y haz clic en el botón **Aceptar**. Se mostrará el mensaje **Nueva tarea de análisis creada** y la tarea se añadirá a la lista de tareas en la sección **Tareas**.
- Para programar una tarea de análisis, si has seleccionado un solo equipo haz clic en el menú de contexto asociado al equipo y selecciona **Programar análisis**. Si has seleccionado varios, haz clic en **Programar análisis** en la barra superior de herramientas. Se creará una nueva tarea de análisis. Para configurarla consulta **Configuración de una tarea de análisis**.

Configuración de una tarea de análisis

- Escribe la información general de la tarea en los campos **Nombre** y **Descripción**.
- Si la tarea no tiene destinatarios activados haz clic en el enlace **Destinatarios** (**No se ha asignado a ningún equipo**) para abrir una ventana nueva donde seleccionar los equipos que recibirán la tarea configurada.

> *Para acceder a la ventana de selección de equipos es necesario guardar previamente la tarea. Si la tarea no ha sido guardada se mostrará una ventana de advertencia.*

- Selecciona el tipo de equipos que recibirán la tarea: **Estación**, **Portátil** o **Servidor**.
- Haz clic en el botón para agregar equipos individuales o grupos de equipos, y en el botón para eliminarlos.
- Haz clic en el botón **Ver equipos** para verificar los equipos que recibirán la tarea.
- Indica la programación horaria de la tarea. Se establece mediante tres parámetros:

- **Empieza**: marca el inicio de la tarea.

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o cuando se encuentre disponible dentro del margen definido en el desplegable **Equipo apagado**.
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Panda Endpoint Protection.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea en función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • **No ejecutar**: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido o no es accesible. • **Dar un margen de**: define un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • **Ejecutar cuando se encienda**: no establece ningún intervalo de tiempo sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 21.2: Comportamiento del inicio de la tarea si el equipo no está disponible

- **Tiempo máximo de ejecución**: indica el tiempo máximo que la tarea puede tardar en completarse, transcurrido el cual se cancelará con error si no ha terminado.

- **Opciones de análisis**:

Valor	Descripción
Tipo de análisis	• **Todo el ordenador**: análisis profundo del equipo incluyendo a

Valor	Descripción
	todos los dispositivos de almacenamiento conectados. • **Áreas críticas**: análisis rápido del equipo que incluye: • `%WinDir%\system32` • `%WinDir%\SysWow64` • Memoria • Sistema de arranque • Cookies • **Elementos específicos**: indica las rutas de los dispositivos de almacenamiento masivo que se analizarán. Se admite el uso de variables de entorno. Se analizará la ruta indicada y todas las carpetas y ficheros que cuelguen de ella.
Detectar virus	Detecta los programas que se introducen en los ordenadores y producen efectos nocivos. Esta opción está siempre activada.
Detectar herramientas de hacking y PUPs	Detecta los programas utilizados por los hackers para causar perjuicios a los usuarios de un ordenador y los programas potencialmente no deseados.
Detectar archivos sospechosos	En los análisis programados, el software de seguridad analiza los programas instaladas en el equipo del usuario de forma estática, sin ejecutarlos, con lo que se reducen las posibilidades de detectar ciertos tipos de amenazas. Para mejorar el ratio de detección en este tipo de análisis, Panda Endpoint Protection puede utilizar algoritmos heurísticos. Únicamente si un programa es detectado mediante la protección heurística, el software de seguridad lo tratará como un programa sospechoso.
Analizar archivos comprimidos	Descomprime y analiza los archivos empaquetados.
Excluir del análisis los siguientes archivos	• **No analizar los archivos excluidos para las protecciones permanentes**: los archivos que el administrador ha marcado para permitir su ejecución no serán analizados, junto a los archivos ya excluidos de forma global en la consola.

Valor	Descripción
	• **Extensiones**: introduce las extensiones de los archivos que no se analizarán separados por comas. • **Archivos**: introduce el nombre de los archivos que no se analizarán separados por comas. • **Directorios**: introduce el nombre de las carpetas que no se analizarán separados por comas.

Tabla 21.3: Opciones de análisis

Listados generados por tareas de análisis

Las tareas de análisis generan listados con los resultados.

Acceso a los listados

Para acceder a estos listados sigue los pasos a continuación:

- Desde el menú superior **Tareas**, haz clic en la **Ver resultados** en la tarea de análisis para acceder al listado **Resultados de tarea**.
- En el listado de **Resultados de Tarea**, selecciona **Ver Detecciones** para acceder al listado.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	Listado **Resultados de la tarea de análisis**.
Ver detecciones y amenazas	Acceso a los listados **Ver Detecciones** dentro de la tarea.

Tabla 21.4: Permisos requeridos para los listados de tareas de análisis

Listado Resultados tarea de análisis

Este listado muestra las detecciones de malware realizada sobre los equipos de la red:

Campo	Descripción	Valores
Equipo	Nombre del equipo analizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que	Cadena de caracteres

Campo	Descripción	Valores
	pertenece el equipo.	
Detecciones	Número de elementos encontrados en el equipo.	Cadena de caracteres
Estado	Estado de la tarea de análisis en el equipo.	• Todos los estados • Pendiente • En curso • Finalizado • Con error • Cancelada (no pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Fecha de comienzo	Fecha en la que comenzó el análisis del equipo.	Fecha
Fecha de fin	Fecha en la que finalizó el análisis del equipo.	Fecha

Tabla 21.5: Campos del listado de Resultado de tarea de análisis

Herramientas de filtrado

Campo	Comentario	Valores
Estado	Según el estado de la tarea	• Todos los estados • Pendiente • En curso • Finalizado • Con error • Cancelada (no pudo iniciar a la hora programada)

Campo	Comentario	Valores
		• Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Detecciones	Equipos con detecciones de malware o sin ellas	• Todos • Con detecciones • Sin detecciones

Tabla 21.6: Filtros Resultado de tareas de análisis

Listado Ver detecciones

Este listado muestra el detalle de cada una de las detecciones de malware encontradas por la tarea de análisis.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Tipo de amenaza	Función del archivo detectado.	• Virus y ransomware • Spyware • Tracking Cookies • Herramientas de hacking y PUPs • Pishing • Acciones peligrosas bloqueadas • URLs con malware

Campo	Descripción	Valores
		• Otros
Ruta	Ubicación de la amenaza en los equipos.	Cadena de caracteres
Acción	Acción realizada en el equipo.	• Borrado • Desinfectado • En cuarentena • Bloqueado • Proceso terminado
Fecha	Fecha en la que se realizó la acción.	Fecha

Tabla 21.7: Campos del listado Ver detecciones

Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Para obtener más información, consulta **Información de equipo** en la página **251**.

Reiniciar equipos

Para mantener los equipos actualizados a la última versión de la protección, o si se detecta algún error en la protección, el administrador puede reiniciar los equipos involucrados desde la consola web:

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la derecha.
    - **Para reiniciar un único equipo**: selecciona el menú de contexto del equipo en el listado de equipos.
    - **Para reiniciar varios equipos**: mediante las casillas de selección, marca los equipos que quieres reiniciar y haz clic en el icono de la barra de acciones.

Para los equipos que estén apagados Panda Endpoint Protection guardará la orden de reinicio hasta 7 días, momento en el cual si el equipo no se ha iniciado se desechará.

Notificar un problema

En algunas ocasiones es posible que el software Panda Endpoint Protection instalado en los equipos de la red presente un mal funcionamiento. Algunos de los síntomas pueden ser:

- Fallos en el reporte del estado del equipo.
- Fallos en la descarga de conocimiento o de las actualizaciones del motor.
- Motor de protección en estado de error.

Si Panda Endpoint Protection presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Panda Security a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior Equipos, selecciona el equipo que presente errores y haz clic en el menú de contexto. Se desplegará un menú con la opción Indícanos el problema.

Si Panda Endpoint Protection presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Panda Security a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior **Equipos**, selecciona el equipo que presente errores y haz clic en el menú de contexto ⋮. Se desplegará un menú con la opción **Notificar un problema**.

Permitir el acceso externo a la consola Web

Para aquellos problemas que el administrador de la red no pueda resolver, existe la posibilidad de habilitar el acceso a la consola únicamente para equipo de soporte de Panda Security:

- Haz clic en el menú superior **Configuración**, panel lateral **Usuarios**.
- En la pestaña **usuarios** haz clic en el control **Permitir al equipo de Panda Security S.L acceder a mi consola**.

Eliminar el ransomware y recuperar el estado anterior

Las amenazas de tipo ransomware cifran el contenido de los ficheros en los equipos de usuario y servidores, y piden un rescate a la empresa para obtener la clave de recuperación que permite

acceder nuevamente a la información cifrada. Este tipo de amenaza es sumamente peligrosa por su potencial impacto en el funcionamiento del negocio. Panda Endpoint Protection implementa varias funcionalidades que ayudan tanto en la fase de detección del ataque como en su resolución.

Sigue los pasos mostrados a continuación si detectas un ataque de tipo ransomware:

> *Dado que Shadow Copies realiza una copia de seguridad diaria de los ficheros y mantiene un máximo de 7 copias, es importante recuperar los archivos encriptados antes del período de 7 días. Si no es así, todas las copias almacenadas estarían cifradas.*

- Desconecta de la red los equipos afectados para evitar la propagación de la amenaza.
- Comprueba que el software de protección está funcionando en todos los equipos:
  - Para ver el estado de la protección, consulta el widget **Estado de protección** en la página **470**.
  - Reinstala el software de seguridad de aquellos que muestran el estado **Error**.
  - Descubre los equipos sin software de seguridad instalado. Si necesitas más información para configurar esta funcionalidad, consulta **Visualizar equipos descubiertos** en la página **118**.
- Configura la protección Antivirus de archivos, Antivirus de correo y Antivirus para navegación web para todos los tipos de amenazas. Si necesitas más información para configurar esta funcionalidad, consulta **Antivirus** en la página **324**.
- Configura la protección anti tamper y establece una contraseña para evitar la desinstalación del software de protección. Si necesitas más información para configurar esta funcionalidad, consulta **Configuración de contraseña y anti-tampering** en la página **313**.
- Comprueba que la funcionalidad Shadow Copies está configurada entre el 10 y el 20% para evitar el borrado de copias por falta de espacio. Si necesitas más información para configurar esta funcionalidad, consulta **Configuración de Shadow Copies** en la página **317**.
- Para eliminar el ransomware sigue los pasos mostrados a continuación:
  - Instala como mínimo los parches que corrigen las vulnerabilidades criticas detectadas. Consulta **Panda Patch Management (Actualización de programas vulnerables)** en la página **345**.
  - Lanza una tarea de análisis bajo demanda. Consulta **Análisis y desinfección bajo demanda de equipos**.

    - Reinicia los equipos afectados para cerrar cualquier conexión remota en curso. Si necesitas más información para configurar esta funcionalidad, consulta **Reiniciar equipos**.
    - Si tras el reinicio continúa la actividad del ransomware, contacta con el departamento de soporte de Panda Security.
- Restaura los archivos cifrados en cada equipo con Shadow copies o con el procedimiento de recuperación de datos implantado en tu empresa.
- Restaura las configuraciones de seguridad modificadas al comienzo de este procedimiento a sus valores habituales.

Capítulo 22

Tareas

Una tarea es un recurso implementado en Panda Endpoint Protection que permite establecer dos características a la ejecución de un proceso: la repetición y el aplazamiento de su inicio.

- **Repetición**: configura la tarea para su ejecución de forma puntual o repetida a lo largo del tiempo.
- **Aplazamiento**: configura la tarea para ser ejecutada en el momento en que se define (tarea inmediata), o aplazada en el tiempo (tarea programada).

Contenido del capítulo

Introducción al sistema de tareas

Accesibilidad del sistema de tareas

Dependiendo de la necesidad o no de configurar todos los parámetros de una tarea, ésta se puede crear desde varios lugares dentro de la consola:

- Menú superior **Tareas**
- Árbol de equipos en el menú superior **Equipos**
- Listados asociados a los distintos módulos soportados.

El árbol de equipos y los listados permiten programar y lanzar tareas de forma ágil, sin necesidad de pasar por todo el proceso de configuración y publicación descrito en **Secuencia completa para lanzar una tarea**, perdiendo algo de flexibilidad en su definición.

Secuencia completa para lanzar una tarea

El recurso principal para crear una tarea se encuentra en la zona **Tareas**, accesible dese el menú superior de la consola. En esta ventana se definen las tareas desde cero, controlando todos los aspectos del proceso.

El proceso para lanzar una tarea consta de tres pasos:

- **Crear y configurar la tarea**: establece los equipos afectados, las características de la tarea, el momento en que será lanzada, el número de veces que se ejecutará y su comportamiento en caso de error. La configuración de una tarea depende de su tipo. Para obtener información sobre cómo crear y configurar una tarea consulta **Tipos de procesos ejecutados por una tarea**
- **Publicar la tarea**: las tareas creadas se introducen en el programador de procesos de Panda Endpoint Protection para lanzarse en el momento marcado por su configuración.
- **Ejecutar la tarea**: el programador lanza el proceso en los equipos cuando se alcanzan las condiciones especificadas en la definición de la tarea.

Tipos de procesos ejecutados por una tarea

Panda Endpoint Protection ejecuta como tarea los procesos siguientes:

- Análisis y desinfección de ficheros. Consulta **Análisis y desinfección bajo demanda de equipos** en la página **591** para más información.
- Instalación de parches y actualizaciones del sistema operativo y de los programas instalados en el equipo. Consulta **Descargar e instalar parches** en la página **352**para más información.

Permisos asociados a la gestión de tareas

*Para obtener más información sobre el sistema de permisos implementado en Panda Endpoint Protection consulta **Descripción de los permisos implementados** en la página **69**.*

Para crear, editar, eliminar o visualizar tareas es necesario utilizar una cuenta de usuario que tenga asignado el permiso apropiado a su rol. Dependiendo del tipo de tarea, los permisos necesarios son:

- **Lanzar análisis y desinfectar** : para crear borrar y modificar tareas de tipo Análisis programado.
- **Instalar, desinstalar y excluir parches**: para crear borrar y modificar tareas de tipo Instalar parches.
- **Visualizar detecciones** : para visualizar los resultados de las tareas de tipo Análisis programado.

Crear tareas desde la zona Tareas

- Haz clic el menú superior **Tareas**. Se mostrará un listado con todas las tareas y su estado.
- Haz clic en el botón **Añadir tarea** y elige el tipo de tarea en el desplegable: se mostrará una ventana con los datos de la tarea, distribuidos en varias zonas:
    - **Información general (1)**: nombre de la tarea y descripción.
    - **Destinatarios (2)**: equipos que recibirán la tarea.
    - **Programación (3)**: configuración del momento en que se lanzará la tarea.
    - **Configuración (4)**: establece las acciones a ejecutar por la tarea. Esta sección varía según el tipo de tarea y se detalla en la documentación asociada al módulo relacionado.

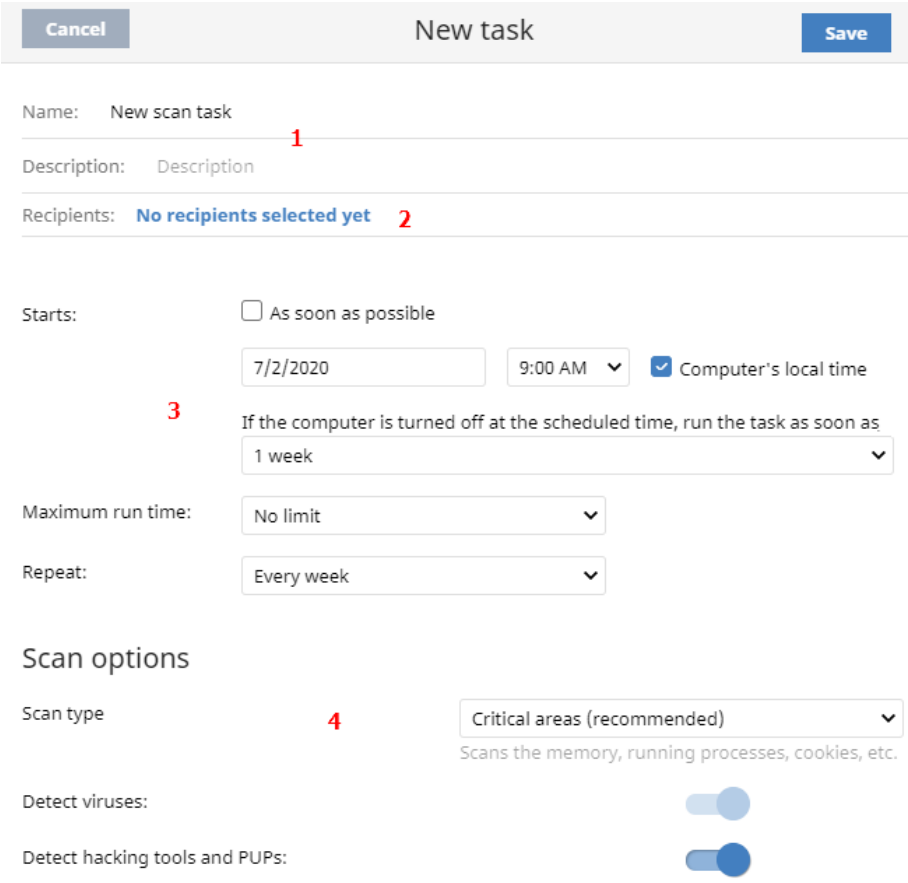


Figura 22.1: Vista general de la ventana Nueva tarea para una tarea de tipo análisis

Destinatarios de la tarea (2)

Para acceder a la ventana de selección de equipos, es necesario guardar previamente la tarea. Si la tarea no ha sido guardada, se mostrará una ventana de advertencia.

- Haz clic en el enlace **Destinatarios** (**No se ha asignado a ningún equipo**) para abrir una ventana nueva donde seleccionar los equipos que recibirán la tarea configurada.
- Selecciona el tipo de equipos que recibirán la tarea: **Estación**, **Portátil**, **Servidor** o **Dispositivo móvil**. El tipo de equipo que puede recibir la tarea variará dependiendo de la tarea que se va a ejecutar.
- Haz clic en el botón para agregar equipos individuales o grupos de equipos, y en el botón para eliminarlos.

*Si se trata de una tarea de instalación de parches y quieres que se envíe solo a equipos de prueba, desplaza el cursor deslizante **Ejecutar la tarea solo en equipos de prueba**. Esta opción solo es aplicable a proveedores de servicios que tengan contratado Panda Partner Center. Para más información, consulta* ***Funcionalidades de Panda Patch Management** en la página **346***

- En la ventana **Editar tarea**, haz clic en el botón **Ver equipos** para verificar los equipos que recibirán la tarea.

Programación horaria y repetición de la tarea

Se establece mediante tres parámetros:

- **Empieza**: marca el inicio de la tarea.

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o cuando se encuentre disponible dentro del margen definido en el desplegable **Equipo apagado**.
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Panda Endpoint Protection.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea en función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • **No ejecutar**: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido o no es accesible. • **Dar un margen de**: define un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • **Ejecutar cuando se encienda**: no establece ningún intervalo de tiempo sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 22.1: Comportamiento del inicio de la tarea si el equipo no está disponible

- **Tiempo máximo de ejecución**: indica el tiempo máximo que la tarea puede tardar en completarse, transcurrido el cual se cancelará con error si no ha terminado.

Valor	Descripción
Sin límite	La duración de la ejecución de la tarea no está definida, pudiéndose extender hasta el infinito.
1, 2, 8 o 24 horas	La duración de la ejecución de la tarea está acotada. Transcurrido el tiempo indicado, la tarea se cancela con error si no ha terminado.

Tabla 22.2: Configuración de la duración de la tarea

- **Frecuencia**: establece un intervalo de repetición cada día, semana, mes o año tomando como referencia la fecha indicada en el campo **Empieza**:

Valor	Descripción
Ejecución única	La tarea se ejecuta de forma puntual a la hora indicada en el campo **Empieza**.
Diaria	La tarea se ejecuta todos los días a la hora indicada en el campo **Empieza**.
Semanal	Haz clic en las casillas de selección para establecer la ejecución de la tarea en los días de la semana elegidos, a la hora indicada en el campo **Empieza**.
Mensual	Elige una de las opciones: • Ejecutar la tarea un día concreto de cada mes. Si se eligen los días 29, 30 o 31 y el mes no tiene esos días, la tarea se ejecuta el último día del mes. • Ejecutar la tarea el primer, segundo, tercer, cuarto o ultima día de la semana de cada mes.

Tabla 22.3: Configuración de la frecuencia de la tarea

Conversión automática de la frecuencia de ejecución

Si alguno de los equipos del parque informático tiene instalada una versión anterior del software de seguridad, es posible que no sea capaz de interpretar correctamente las configuraciones de frecuencia establecidas por el administrador en la consola web. En este caso, cada equipo establecerá las siguientes correspondencias para la configuración de la frecuencia en las tareas a ejecutar:

- **Tareas diarias**: sin cambios.
- **Tareas semanales**: se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 7 días.
- **Tareas mensuales**: se omiten los días elegidos por el administrador. La primera ejecución se realiza en la fecha indicada en **Empieza** y, a partir de este punto, se ejecutará nuevamente cada 30 días.

Publicar tareas

Una vez creada y configurada, la tarea aparecerá en el listado de tareas configuradas, pero mostrará la etiqueta **Sin publicar**, indicando que no está activa.

Haz clic en el enlace **Publicar** para introducir la tarea en el programador de Panda Endpoint Protection, encargado de marcar el momento en que se lanzan las tareas según su configuración.

Listado de tareas

Haz clic en el menú superior **Tareas** para listar tareas creadas, su tipo, estado y otra información relevante.

Campo	Comentario	Valores
Icono	Tipo de la tarea	• Tarea de tipo instalación o desinstalación de parches • Tarea de tipo análisis bajo demanda • Tarea de tipo desinfección
Nombre	Nombre de la tarea creada	Cadena de caracteres
Programación	Cuando se ejecuta la tarea.	Cadena de caracteres
Estado	• **Sin destinatarios**:la tarea no se ejecutará	Cadena de

Campo	Comentario	Valores
	porque no tiene destinatarios asignados. Asigna uno o más equipos a la tarea. • **Sin publicar**: la tarea no se ejecutará porque no ha entrado en la cola del programador. Publica la tarea para que el programador de procesos planifique su ejecución. • **En curso**: la tarea se está ejecutando. • **Cancelada**: la tarea fue cancelada de forma manual. No implica que todos los procesos en ejecución en los diferentes equipos se hayan detenido. • **Finalizada**: todos los equipos terminaron la ejecución de la tarea asignada, independientemente de que haya finalizado con éxito o con error. Este estado solo se da en las tareas de ejecución puntual o única.	caracteres

Tabla 22.4: Campos del listado Tareas creadas

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de tarea	Clase de la tarea	• Todos • Análisis • Desinfección • Instalación de parches • Desinstalación de parches
Buscar tarea	Nombre de la tarea	Cadena de caracteres
Programación	Frecuencia de la repetición de la tarea	• Todos • Inmediata • Una vez • Programada

Campo	Comentario	Valores
Estado	Estado de la tarea	• Todos • Sin destinatarios • Sin publicar • En curso • Cancelada • Finalizada
Ordenar listado	Criterio de ordenación de las tareas creadas.	• Ordenar por fecha de creación • Ordenar por nombre • Ascendente • Descendente

Tabla 22.5: Campos de filtrado para el listado Tareas creadas

Gestionar tareas

Haz clic en el menú superior **Tareas** para borrar, copiar, cancelar o visualizar los resultados de las tareas creadas.

Modificar tareas publicadas

Haz clic en el nombre de la tarea creada para mostrar su ventana de configuración, donde es posible modificar algunos de sus parámetros.

Las tareas publicadas solo admiten cambio de nombre y de descripción. Para modificar otros parámetros de una tarea publicada, es necesario copiarla previamente.

Cancelar tareas publicadas

Haz clic en las casillas de selección de las tareas a cancelar y en el icono **Cancelar** de la barra de herramientas. Las tareas se cancelarán, aunque no se borrarán de la ventana de tareas para poder acceder a sus resultados. Únicamente se pueden cancelar las tareas en estado **En curso**.

Borrar tareas

Las tareas ejecutadas no se eliminan automáticamente, para ello es necesario hacer clic en las casillas de selección y después en el icono en la barra de herramientas. Una tarea publicada solo se puede borrar si previamente es cancelada.

Al borrar una tarea se borrarán también sus resultados.

Copiar tareas

Copiar una tarea implica replicar toda su configuración. Con el objeto de reutilizar tareas para asignarlas a distintos grupos de equipos, la copia de los destinatarios de la tarea original es opcional.

- Haz clic en el menú superior **Tareas** y en el icono de la tarea que quieres copiar. Se mostrará un menú para seleccionar el tipo de copia.

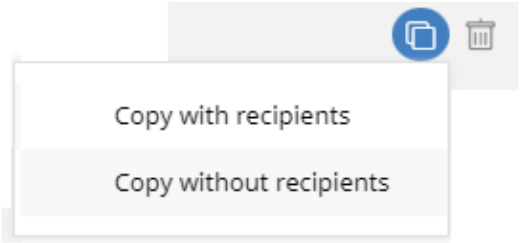


Figura 22.2: Ventana del icono Copiar tarea

- Si has seleccionado **Copia sin destinatarios**, se abrirá la ventana **Copiar tarea**.
    - Para asignar destinatarios haz clic en el enlace **No se ha asignado a ningún equipo**. Se mostrará la ventana **Destinatarios**.
    - Selecciona los destinatarios de la tarea y haz clic en el botón **Guardar** situado en la esquina superior derecha de la ventana.

*Si se trata de una tarea de instalación de parches y quieres que se envíe solo a equipos de prueba, desplaza el cursor deslizante **Ejecutar la tarea solo en equipos de prueba**. Esta opción solo es aplicable a proveedores de servicios que tengan contratado Panda Partner Center. Para más información, consulta* ***Funcionalidades de Panda Patch Management*** *en la página* ***346***

Si has seleccionado **Copia con destinatarios**, se abrirá la ventana **Copiar tarea** con los destinatarios de la tarea original.

Exportar tareas

Haz clic en el icono para exportar un listado de las tareas creadas. El archivo csv. se guardará en la carpeta que elija el usuario.

En el archivo descargado se muestran los campos:

Campo	Definición
Nombre de la tarea	Nombre de la tarea
Tipo de la tarea	Tipo de tarea: • Búsqueda de IOCs • Desinstalación de parches • Instalación de parches • Análisis
Programación	Frecuencia de ejecución de la tarea: • Inmediata • Una vez • Programada
Estado	Estado en el que se encuentra la tarea: • Sin destinatarios • Sin publicar • En curso • Cancelada • Finalizada
Grupo destinatario	Grupo destinatario de la tarea.
Estación	• **Sí**: la tarea se asignará a los equipos de tipo Estación del grupo destinatario. • **No**: la tarea no se asignará a los equipos de tipo

Campo	Definición
	Estación del grupo destinatario.
Portátil	• **Sí**: la tarea se asignará a los equipos de tipo Portátil del grupo destinatario. • **No**: la tarea no se asignará a los equipos de tipo Portátil del grupo destinatario.
Servidor	• **Sí**: la tarea se asignará a los equipos de tipo Servidor del grupo destinatario. • **No**: la tarea no se asignará a los equipos de tipo Servidor del grupo destinatario.
Dispositivo móvil	• **Sí**: la tarea se asignará a los dispositivos móviles del grupo destinatario. • **No**: la tarea no se asignará a los dispositivos móviles del grupo destinatario.
Equipo destinatario	Equipo destinatario de la tarea.
Grupo del equipo destinatario	Tipo de equipo destinatario de la tarea: • Estación • Portátil • Servidor • Dispositivo móvil

Tabla 22.6: Listado de exportación de tareas

Resultados de una tarea

Al hacer clic en el enlace **Ver resultados** de una tarea publicada se mostrarán los resultados obtenidos hasta ese momento y una herramienta de filtrado que permite localizar equipos específicos que recibieron la tarea.

Algunos de los campos incluidos en el listado de resultados son específicos de cada tarea. Estos campos se incluyen en la documentación del módulo correspondiente. A continuación se muestran los campos comunes a todos los listados de resultados.

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se registró un evento de ejecución de tarea.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Endpoint Protection a la que pertenece el equipo.	Cadena de caracteres
Estado	Estado del proceso asignado por la tarea para su ejecución en el equipo: • **Pendiente**: la tarea no ha iniciado la ejecución de su siguiente repetición por estar programada para un momento posterior. • **En curso**: la tarea se está ejecutando en el equipo. • **Finalizada**: la tarea terminó con éxito. • **Con error**: la tarea terminó con error. • **Cancelada (no se pudo iniciar a la hora programada)**:la tarea estaba programada para iniciar su ejecución pero en ese momento el equipo estaba apagado o en un estado que impedía su ejecución. • **Cancelada**: el proceso fue cancelado en el equipo. • **Cancelando**: la tarea se canceló pero el equipo todavía no ha completado la orden de cancelar el proceso. • **Cancelada (tiempo máximo superado)**: la tarea se canceló automáticamente al expirar el tiempo máximo establecido para su ejecución.	Cadena de caracteres
Fecha de comienzo	Fecha de inicio de la tarea.	Fecha
Fecha fin	Fecha de finalización de la tarea.	Fecha

Tabla 22.7: Campos comunes en el resultado de una tarea

Herramienta de filtrado de tareas

Campo	Descripción	Valores
Fecha	Desplegable con las fechas en las que la tarea pasó a estado activo según su programación configurada. Una tarea activa puede iniciarse en el momento o esperar a que el equipo esté disponible. Esta fecha se indica en la columna fecha.	Fecha
Estado	• **Pendiente**: la tarea todavía no se ha iniciado por no haber alcanzado la ventana de ejecución configurada. • **En progreso**: la tarea se está ejecutando en este momento. • **Con éxito**: la tarea terminó con éxito. • **Con error**: la tarea terminó con error. • **Cancelada (no se pudo iniciar a la hora programada)**: el equipo no estaba disponible en el momento del inicio de la tarea o en el intervalo definido. • **Cancelada:** la tarea fue cancelada de forma manual. • **Cancelada (tiempo máximo expirado)**: la tarea duró más tiempo que el indicado en la configuración de la tarea y se canceló.	Enumeración

Tabla 22.8: Filtros de búsqueda en los resultados de una tarea

Ajuste automático de los destinatarios de una tarea

Si el administrador establece un grupo de equipos como destinatario de una tarea, el conjunto final de equipos sobre los que se ejecutará puede variar debido a que los grupos son entidades dinámicas que varían a lo largo del tiempo.

De esta manera, una tarea definida en el momento T1 y asignada a un grupo tendrá como destinatarios los equipos que forman el grupo seleccionado, pero en el momento de ejecución posterior T2, los miembros de ese grupo pueden haber cambiado.

A la hora de resolver qué equipos pertenecen al grupo asignado a la tarea, se distinguen tres casos según su tipo:

- Tareas inmediatas.
- Tareas programadas de ejecución puntual o única.
- Tareas programadas de ejecución repetida.

Tareas inmediatas

Estas tareas se crean, se publican y se lanzan de forma atómica e inmediata una única vez. El grupo destinatario se evalúa en el momento en que el administrador crea la tarea. Los equipos afectados aparecerán en estado **Pendiente** en la tarea.

Añadir equipos al grupo destinatario

No se permite añadir nuevos equipos. Aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea.

Quitar equipos del grupo destinatario

Sí se pueden retirar equipos del grupo destinatario. Para cancelar la tarea mueve los equipos a otro grupo.

Tareas programadas de ejecución única

Estas tareas admiten dos estados con respecto a la posibilidad de cambiar a los integrantes del grupo de equipos destinatario:

Tareas cuya ejecución comenzó hace menos de 24 horas

En las primeras 24 horas de la ejecución, el administrador puede añadir o retirar equipos a los grupos destinatarios. Se marca un plazo de 24 horas para abarcar todos los husos horarios en aquellas multinacionales con presencia en varios países.

Tareas cuya ejecución comenzó hace más de 24 horas

Una vez cumplido el plazo de 24 horas no será posible añadir nuevos equipos y, aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea. Para cancelar las tareas en curso sobre equipos muévelos fuera del grupo destinatario.

Tareas programadas de ejecución repetida

Estas tareas permiten agregar o eliminar equipos destinatarios en cualquier momento hasta su cancelación o finalización.

Las tareas programadas de ejecución repetida no muestran los equipos destinatarios en estado **Pendiente** de forma automática, sino que éstos se irán mostrando de forma progresiva a medida que la plataforma Aether reciba información del estado de la tarea de cada equipo.

Capítulo 23

Funcionalidades del producto y requisitos

Contenido del capítulo

Funcionalidades por plataforma

General

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Consola web	X	X	X	X	X
Dashboards	X	X	X	X	X
Organización de los	X	X	X	X	X

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
equipos por filtros					
Organización de los equipos en grupos	X	X	X	X	X
Idiomas disponibles en el software de protección	11	11	11	16	10

Tabla 23.1: Funcionalidades generales

Listados e informes

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Frecuencia de envío al servidor de la actividad del malware y PUPs	1 min	10 min	10 min	Tras fin análisis	N/A
Frecuencia de envío de otras detecciones	15 min	15 min	15 min	Tras fin análisis	15 min
Listado de detecciones	X	X	X	X	X
Informe ejecutivo	X	X	X	X	X
Informe ejecutivo programado	X	X	X	X	X

Tabla 23.2: Funcionalidades de listados e informes

Protecciones

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Anti-tamper	X				
Anti-Phishing	X		X		X
Protección permanente AV en tiempo real	X	X	X	X	
Detecciones contextuales	X	X			
Evaluación de riesgos	X	X	X	X	X
Shadow Copies	X				
Decoy Files	X				
Firewall	X				
Control de dispositivos	X				
Antirrobo				X	X

Tabla 23.3: Funcionalidades de protección

Información de hardware y software

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Información y listado de hardware	X	X	X	X	X
Información y	X	X	X	X	X

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
listado de software					
Registro de cambios de software	X	X	X	X	X
Información de los parches instalados del sistema operativo	X				
Evaluación de vulnerabilidades	X	X	X		

Tabla 23.4: Funcionalidades de información de hardware y software

Configuraciones

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Seguridad para estaciones y servidores	X	X	X	N/A	N/A
Contraseña para desinstalar la protección y tomar acciones en local	X				
Control de acceso a redes VPN	X		X		
Control de acceso a redes WiFi	X		X		
Asignar listas de	X	X	X	N/A	N/A

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
proxies					
Actuar como Proxy Panda	X			N/A	N/A
Acceder a la red través de proxy	X	X	X	N/A	N/A
Actuar como caché de descargas	X			N/A	N/A
Utilizar caché de descargas	X			N/A	N/A
Descubrir equipos desprotegidos	X				
Alertas por correo ante infecciones	X	X	X	X	N/A
Alertas por correo ante equipos desprotegidos	X	X	X	X	N/A

Tabla 23.5: Funcionalidades de configuración

Acciones remotas desde Consola Web

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Acciones en tiempo real	X	X	X	X	X
Análisis bajo demanda	X	X	X	X	N/A

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Análisis programados	X	X	X	X	N/A
Instalación remota del agente de Panda	X				
Posibilidad de reinstalar agente de protección	X				
Reiniciar equipo	X	X	X		
Reportar una incidencia (PSInfo)	X			X	X
Notificar un problema	X	X	X	X	X

Tabla 23.6: Acciones remotas disponibles

Actualizaciones del software de seguridad

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
Actualizaciones de firmas	X	X	X	X	NA
Actualizaciones de la protección	X	X	X	X	NA
Programar la actualización de la protección	X	X	X	Google Play	App Store

Tabla 23.7: Funcionalidades de actualización del software de seguridad

Módulos disponibles

Características disponibles	Windows (Intel & ARM)	Linux	macOS (Intel & ARM)	Android	iOS
	X	X	X		
Patch Management	X	X	X		
Panda Full Encryption	X	X	X		

Tabla 23.8: Módulos disponibles

(*) Disponible solo en microprocesadores Intel y parcialmente en Windows (ARM)

Requisitos de plataformas Windows

Sistemas operativos soportados

Estaciones de trabajo con microprocesador x86 y x64

- Windows XP SP3 (32 bits)
- Windows Vista (32 y 64-bit)
- Windows 7 (32 y 64-bit)
- Windows 8 (32 y 64-bit)
- Windows 8.1 (32 y 64-bit)
- Windows 10 (32 y 64-bit)
- Windows 11 (64 bits)

Equipos con microprocesador ARM

- Windows 10 Pro
- Windows 10 Home
- Windows 11 Pro
- Windows 11 Home

Servidores con microprocesador x86 y x64

- Windows 2003 (32, 64-bit y R2) SP2
- Windows 2008 (32 y 64-bit) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016 y 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 y 2019
- Windows Server 2022

IoT y Windows Embedded Industry

- Windows XP Embedded
- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64 bits)
- Windows Embedded Standard 2009, 7, 7 (64 bits), 8, 8 (64 bits),
- Windows Embedded Pro 8, 8 (64 bits)
- Windows Embedded Industry 8, 8 (64 bits), 8.1, 8.1 (64 bits)
- Windows IoT Core 10, 10 (64 bits)
- Windows IoT Enterprise 10, 10 (64 bits)
- Windows Server IoT 2019

Los sistemas embedded pueden instalarse de forma personalizada, por lo que el funcionamiento de Panda Endpoint Protection y de algunos de sus módulos en dichos sistemas podría variar según la instalación. Para comprobarlo, instala Panda Endpoint Protection y verifica que las diferentes protecciones funcionan correctamente.

Requisitos hardware

- **Procesador**: CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM**: 1 Gbyte
- **Espacio libre en el disco duro para la instalación**: 650 Mbytes

Otros requisitos

Actualizar los certificados raíz

Para que el producto funcione correctamente, deben mantenerse actualizados los certificados raíz instalados en cada equipo protegido. Además, se requiere que los equipos puedan acceder a las siguientes URLs:

http://*.globalsign.com

http://*.digicert.com

http://*.sectigo.com

Los equipos Windows actualizan automáticamente los certificados raíz a través de Windows Update. No obstante, pueden darse problemas si las actualizaciones no han sido debidamente instaladas.

Si los certificados raíz no se actualizan, funcionalidades como la comunicación en tiempo real de los agentes con la consola de administración y el módulo Patch Management podrían dejar de funcionar.

Para identificar y actualizar los certificados raíz, utiliza la herramienta que encontrarás en ***https://www.pandasecurity.com/resources/tools/wescertcheck.zip***

Sincronización horaria de los equipos (NTP)

Aunque no es un requisito indispensable, si es muy recomendable que el reloj de los equipos protegidos con Panda Endpoint Protection esté sincronizado. La mayoría de las veces, la sincronización se establece mediante el uso de un servidor NTP.

Si la sincronización no es correcta, la seguridad del equipo puede verse afectada de diferentes maneras:

- Inestabilidad en las comunicaciones entre el equipo y los servidores dePanda Security.
- Fallo en las comprobaciones de certificados, que serán válidos o estarán caducados en función de la fecha del equipo y no de la real.
- Fechas erróneas en las alertas generadas por las diferentes protecciones, que mostrarán como fecha y hora de detección la del equipo, y no la real.
- En el detalle de las tareas de análisis o de instalación de parches se mostrarán fechas no reales.
- La caducidad del instalador no se respetará.
- Algunas acciones programadas, como el reinicio del equipo y la recepción de notificaciones de problemas, podrían no ejecutarse correctamente.

Compatibilidad con firma de drivers SHA-256

Para mantener el software de seguridad actualizado a la última versión publicada por Panda Security, es necesario que el equipo del usuario o servidor sea compatible con la firma de drivers SHA-256. Algunas versiones del sistema operativo Windows no incorporan de fábrica esta funcionalidad y requieren ser actualizadas:

Plataforma Windows	Actualizaciones necesarias	URL
Vistax86 / Vistax64	SP2 + KB4474419	Enlace a KB4474419 Enlace a SP2
Server 2008x86 / Server 2008x64	SP2 + KB4474419	Enlace a KB4474419 Enlace a SP2
W7x86 / W7x64	SP1 + KB4474419	Enlace a KB4474419 Enlace a SP1
2008R2x64	KB4474419	Enlace a KB4474419

Tabla 23.9: Actualizaciones requeridas para compatibilidad con SHA-256

Los equipos no compatibles con la firma de drivers SHA-256 no actualizarán el software de protección más allá de la versión 9.00.00, y tampoco se mostrarán en el widget **Protección desactualizada** en la página **474** como candidatos a actualizarse. Estos equipos se muestran con la alerta **No es posible actualizar la protección de este equipo a la última versión** . Para obtener más información sobre las alertas de equipo y cómo visualizarlas consulta **Información de equipo** en la página **251**.

Para localizar los equipos no compatibles con el firmado de drivers SHA-256 crea un filtro en el árbol de filtros con los parámetros mostrados en **Equipos no compatibles con firma de drivers SHA-256** en la página **220**. Para obtener más información acerca del árbol de filtros consulta **Árbol de filtros** en la página **212**.

Panda Security recomienda actualizar todos los equipos de la red para mantenerlos protegidos con la última versión del software de protección disponible en todo momento.

Cuando el administrador instala los parches indicados, se descargará de forma automática la última versión del software de protección disponible en un plazo máximo de 4 horas, si bien requerirá un reinicio para completar la actualización.

Requisitos de plataformas macOS

Sistemas operativos soportados

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey
- macOS 13 Ventura
- macOS 14 Sonoma

Requisitos hardware

- **Procesador**: Intel® Core 2 Duo
- **Memoria RAM**: 2 Gbyte
- **Espacio libre en el disco duro para la instalación**: 400 Mbytes
- **Puertos**: se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento de la detección web de malware.

Direcciones IP necesarias para activar el producto

En el proceso de instalación del software de protección, el cortafuegos corporativo debe permitir el tráfico a los siguientes rangos de direcciones IP:

- 17.248.128.0/18
- 17.250.64.0/18
- 17.248.192.0/19

Permisos necesarios

Para el correcto funcionamiento de la protección, es imprescindible que el software de seguridad cuente con los permisos necesarios en el equipo del usuario. Para ello, es necesario activar los siguientes permisos:

- Extensiones de red
- Extensiones de sistema

- Acceso total al disco
- Ejecución en segundo plano.

Según la versión de sistema operativo, los pasos a seguir son diferentes.

Instrucciones para macOS Catalina o superior

Para habilitar el permiso Extensiones del Kernel / Sistema:

- Abre el agente Panda Endpoint Protection en el equipo del usuario y haz clic en el botón **Abrir preferencias de seguridad**.
- Haz clic en el icono del candado, situado en la esquina inferior izquierda de la ventana. Se abrirá la ventana **Seguridad y privacidad**.
- Escribe las credenciales del administrador y haz clic en el botón **Desbloquear**.
- Haz clic en el botón **Permitir**. Las extensiones se han habilitado.

Para activar el permiso Acceso total al disco:

- Abre el agentePanda Endpoint Protection en el equipo del usuario y haz clic en el botón **Abrir preferencias de acceso a disco**.
- Haz clic en el icono del candado, situado en la esquina inferior izquierda de la ventana. Se abrirá la ventana **Seguridad y privacidad**.
- Escribe las credenciales del administrador y haz clic en el botón **Desbloquear**.
- Selecciona la casilla correspondiente a **Protection Agent.**
- Haz clic en el botón **Salir y abrir**. El acceso al disco se ha activado.

Instrucciones para macOS Mojave 10.14 o inferior

Al iniciarse Panda Endpoint Protection, el sistema operativo podría bloquear las extensiones de kernel necesarias para el correcto funcionamiento de la protección.

Esto se debe a que estas versiones de macOS contienen una característica de seguridad que requiere la aprobación del usuario antes de cargar nuevas extensiones de kernel de terceros.

Para mas información, consulta
https://developer.apple.com/library/archive/technotes/tn2459/_index.html#//apple_ref/doc/uid/DTS40017658

Cuando esto sucede, se mostrarán dos mensajes:

- Mensaje de bloqueo de extensiones de sistema.
- Mensaje advirtiendo de que el equipo está desprotegido.

Para resolverlo, sigue los siguientes pasos:

- En el mensaje de bloqueo de extensiones de kernel, haz clic en **OK**. También puedes hacer clic en el botón **Abrir preferencias del sistema** del mensaje de equipo en estado desprotegido. Se abrirá la ventana **Preferencias del sistema**.
- Haz clic en **Seguridad y privacidad**.
- Para desbloquear, haz clic en el icono del candado, situado en la esquina inferior izquierda de la ventana.
- En la ventana **Seguridad y privacidad**, haz clic en el botón **Permitir**. Las extensiones se han habilitado.

Instrucciones para macOS Ventura 13

La protección puede detenerse en los equipos al no permitirsela ejecución en segundo plano del agente. Por ello, es necesario asegurarse de que los equipos cuenten con el permiso de **Ejecución en segundo plano** activo.

Requisitos de plataformas Linux

Panda Endpoint Protection se instala tanto en estaciones de trabajo como en servidores Linux. Si no está presente un entorno gráfico en el momento de la instalación las protecciones URL filter y Web filter quedarán deshabilitadas. En equipos sin entorno gráfico utiliza la herramienta `/usr/local/protection-agent/pa_cmd` para controlar la protección.

Distribuciones de 64 bits soportadas

- **Ubuntu**: 14.04 LTS, 14.10, 15.04, 15.10, 16.04 LTS, 16.10, 17.04, 17.10, 18,04 LTS, 18.10, 19.04, 19.10, 20.04 LTS, 20.10, 21.04, 21.10, 22.04 LTS, 22.10 y 23.04.
- **Fedora**: 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37 y 38.
- **Debian**: 8, 9, 10, 11 y 12.
- **RedHat**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1 y 9.2.
- **CentOS**: 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3, 8.4, y 8.5.
- **CentOS Stream**: 8, 9.
- **Rocky Linux**: 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1 y 9.2.
- **Alma Linux**: 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1 y 9.2.
- **LinuxMint**: 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2, 19.3, 20, 20.1,20.2, 20.3, 21 y 21.1.
- **SuSE Linux Enterprise**: 11 SP2, 11 SP3, 11 SP4, 12, 12 SP1, 12 SP2, 12 SP3, 12 SP4, 12 SP5,15, 15 SP1, 15 SP2, 15 SP3 , 15 SP4 y 15 SP5.

- **Oracle Linux:** 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9,8.0, 8 , 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1 y 9.2.

Distribuciones de 32 bits soportadas

- RedHat 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10
- CentOS 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10

Versiones del kernel soportadas.

Para más información sobre las distribuciones y kernels soportados en Linux consulta: **https://www.pandasecurity.com/es/support/card?id=700009#show2**.

Panda Endpoint Protection no es compatible con versiones especiales o modificadas del kernel de Linux.

Gestores de ficheros soportados

- Nautilus
- Pcmanfm
- Dolphin

Requisitos hardware

- **Procesador**: CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM**: 1.5 Gbytes
- **Espacio libre en el disco duro para la instalación**: 500 Mbytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento de la detección web de malware.

Dependencias del paquete de instalación

El agente Linux utiliza el gestor de paquetes de la distribución para descargar todas las dependencias que no estén satisfechas. De forma general, los paquetes necesarios son:

- **Libcurl**: para distribuciones basadas en Debian consulta **Librerías libcurl**
- **OpennSSL**
- **Gcc y las utilidades de compilación**: make y makeconfig solo en Fedora.

El proceso de instalación en Fedora incluye la compilación de los módulos necesarios para el buen funcionamiento del agentePanda Endpoint Protection.

Para mostrar las dependencias del agente ejecuta los comandos mostrados a continuación en una terminal según la distribución de destino:

- Para distribuciones basadas en Debian: `dpkg --info paquete.deb`
- Para distribuciones basadas en Fedora: `rpm --qRp paquete.rpm`

Librerías libcurl

El módulo de la protección requiere la instalación de las librerías `libcurl3` o `libcurl4` de 32 bits. Si tienes ya instalada una de estas librerías para 64 bits comprueba que el gestor de paquetes descarga la misma librería (`libcurl3` o `libcurl4`) con la misma versión pero para la arquitectura 32 bits. De no ser así Panda Endpoint Protection no se ejecutará correctamente el equipo y será necesario instalar la librería apropiada de forma manual.

Por ejemplo, si en tu equipo tienes instalada la librería `libcurl3 x.y.z` para 64 bits, el gestor de paquetes deberá descargar la librería `libcurl3 x.y.z` para 32 bits y no la `libcurl4 x.y.z` para 32 bits.

Requisitos de plataformas Android

Sistemas operativos soportados

- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0
- Pie 9.0
- Android 10
- Android 11
- Android 12

Requisitos hardware

Se requiere un mínimo de 10 megabytes de espacio en la memoria interna del dispositivo. Dependiendo del modelo, es posible que el espacio requerido sea superior.

Requisitos de red

Para que las notificaciones push funcionen correctamente desde la red de la empresa, es necesario abrir los puertos 5228, 5229 y 5230 a todo el bloque de IPs ASN 15169 correspondientes a Google.

Permisos requeridos en el dispositivo

Para utilizar todas las características de Panda Endpoint Protection es necesario que el usuario acepte los permisos siguientes:

- Acceso a la cámara
- Leer el estado del teléfono
- Realizar llamadas
- Obtener ubicación
- Servicios de ubicación
- Mostrar encima de otras apps
- Actuar como administrador del dispositivo
- Acceso al almacenamiento externo
- Obtener ubicación en segundo plano

En dispositivos con Android 12 se requieren también los siguientes permisos:

- Deshabilitar hibernación de aplicaciones
- Ignorar optimizaciones de batería

En dispositivos con Android 13 se requieren también los siguientes permisos:

- Permitir mostrar notificaciones

Requisitos de plataformas iOS

Sistemas operativos soportados

- iOS 13 / iPadOS 13
- iOS 14 / iPadOS 14
- iOS 15 / iPadOS 15
- iOS 16/iPadOS 15

Requisitos de red

La aplicación instalada en el dispositivo móvil utiliza el servicio de notificaciones push de Apple (APNs, Apple Push Notification Service) para comunicarse con Panda Endpoint Protection. En condiciones normales, si el dispositivo está conectado a la red de telefonía por 2G/3G/4G y superiores no es necesario cumplir ningún requisito de red específico.

Si el dispositivo está conectado a la red mediante Wi-Fi, punto de acceso (AP) o cualquier otro método alternativo, es necesario que pueda conectarse a servidores específicos por los puertos mostrados a continuación:

- Puerto TCP 5223 para comunicarse con APNs.
- Puerto TCP 443 o 2197 para enviar notificaciones a APNs.

Los servidores que conforman el servicio APNs usan balanceo de carga, por lo que el dispositivo no se conectará siempre a las mismas IPs. Si es posible, permite en el firewall las conexiones con todo el rango 17.0.0.0/8 asignado a Apple. Si no es posible, permite la conexión a los siguientes rangos de IPs:

IPv4

- 17.249.0.0/16
- 17.252.0.0/16
- 17.57.144.0/22
- 17.188.128.0/18
- 17.188.20.0/23

IPv6

- 2620:149:a44::/48
- 2403:300:a42::/48
- 2403:300:a51::/48
- 2a01:b740:a42::/48

Para más información consulta ***https://support.apple.com/en-us/HT203609***

Permisos requeridos en el dispositivo

Para utilizar todas las características de Panda Endpoint Protection es necesario que el usuario acepte los permisos siguientes:

- Obtener ubicación
- Servicios de ubicación
- Obtener ubicación en segundo plano
- Filtrar contenido de red
- Receive push notifications

- Send Notificacions
- Permitir refresco en background

Puertos locales

Para poder implementar ciertas funciones, el software de seguridad instalado en los equipos de la red utiliza los puertos de escucha mostrados a continuación:

Windows

- **TCP 18226**: equipos con el rol caché en todas las interfaces de red. Consulta **Rol de caché** en la página **302**.
- **TCP 21226**: equipos con el rol de caché para recoger peticiones de ficheros a enviar en todas las interfaces de red. Consulta **Rol de caché** en la página **302**.
- **TCP 3128**: equipos con el rol de proxy en todas las interfaces de red. Consulta **Rol de Proxy Panda** en la página **300**.
- **UDP 21226**: equipos con el rol de descubridor en todas las interfaces de red. Consulta **Rol de descubridor** en la página **304**.
- **TCP 33000**: equipos que inician una conexión VPN con Firebox en todas las interfaces de red. Consulta **Control de acceso a redes** en la página **311**.
- **UDP 35621**: módulo de protección en la interfaz localhost.

Linux

- **UDP 21226**: equipos con el rol de descubridor en todas las interfaces de red. Consulta **Rol de descubridor** en la página **304**.
- **TCP 4575**: módulo de protección en la interfaz localhost.
- **TCP 8310**: módulo de protección en la interfaz localhost.
- **TCP 5560**: comunicación interna de procesos en la interfaz localhost.

macOS

- **UDP 21226**: equipos con el rol de descubridor en todas las interfaces de red. Consulta **Rol de descubridor** en la página **304**.
- **TCP 33000**: equipos que inician una conexión VPN con Firebox en todas las interfaces de red. Consulta **Control de acceso a redes** en la página **311**.
- **TCP 4575**: módulo de protección en la interfaz localhost.
- **TCP 8310**: módulo de protección en la interfaz localhost.
- **TCP 5560**: comunicación interna de procesos en la interfaz localhost.

Acceso a la consola web

La consola de administración es accesible con la última versión de los navegadores compatibles mostrados a continuación:

- Chrome
- Microsoft Edge
- Firefox
- Opera

Acceso a URLs del servicio

Para el correcto funcionamiento de Panda Endpoint Protection es necesario que las URL mostradas a continuación sean accesibles desde los equipos protegidos de la red.

Nombre de producto	URLs

Panda Endpoint Protection	• https://*.pandasecurity.com
	  • Descarga de instaladores, desinstalador genérico y políticas.
	  • Comunicaciones de agente (registro, configuración, tareas, acciones, estados comunicación en tiempo real).
	  • Comunicaciones de protección con Inteligencia colectiva.
	  • Descarga de ficheros de firmas en Android.
	• http://*.pandasecurity.com
	  • Descarga de ficheros de firmas (salvo Android).
	• https://*.windows.net
	Urls para el envío de ficheros desconocidos:
	• cmg-fusmb.pandasecurity.com
	• cmp-fusmb.pandasecurity.com
	• cpg-fusmb.pandasecurity.com
	• cpp-fusmb.pandasecurity.com
	• cppi-fusmb.pandasecurity.com
	• cppl-fusmb.pandasecurity.com
	• cppe-fusmb.pandasecurity.com
	• rpuws.pandasecurity.com

Nombre de producto	URLs
Certificados raiz	• http://*.globalsign.com • http://*.digicert.com • http://*.sectigo.com
Panda Patch Management	• https://content.ivanti.com • https://application.ivanti.com • https://stlicense.ivanti.com • https://help.ivanti.com • https://license.shavlik.com
Testeo de la actividad	Para versiones de protección Windows superiores a 8.00.16 • http://proinfo.pandasoftware.com/connectiontest.html Para el test de conectividad. • http://*.pandasoftware.com
Protección contra ataques de red	• https://cpg-nap.pandasecurity.com/nap/buffer • https://cpp-nap.pandasecurity.com/nap/buffer

Tabla 23.10: URLs de acceso al servicio

Puertos

- Port 80 (HTTP)
- Port 443 (HTTPS, websocket)
- Puerto 8080 (aceso desde Orion)

Descarga de parches y actualizaciones (Panda Patch Management)

Consulta la página de soporte **https://www.pandasecurity.com/spain/support/card?id=700044** para obtener un listado completo de las urls accesibles desde los equipos de la red que recibirán los parches o desde los equipos con rol de caché .

Glosario

1

100% Attestation Service

Servicio de Panda Endpoint Protection incluido en la licencia básica que clasifica el 100% de los procesos ejecutados en los equipos de usuario y servidores para emitir una valoración sin ambigüedades (goodware o malware, sin sospechosos).

A

Adaptador de red

Hardware que permite la comunicación entre diferentes equipos conectados a través de una red de datos. Un equipo puede tener más de un adaptador de red instalado y es identificado en el sistema mediante un número de identificación único.

Adware

Programa que una vez instalado o mientras se está instalando, ejecuta, muestra o descarga automáticamente publicidad en el equipo.

Agente Panda Security

Uno de los dos módulos del software de cliente Panda Endpoint Protection . Se encarga de las comunicaciones entre los equipos de la red y los servidores en la nube de Panda, además de gestionar los procesos locales.

Alerta

Ver Incidencia.

Análisis heurístico

Análisis estático formado por un conjunto de técnicas que inspeccionan de forma estática los ficheros potencialmente peligrosos. Este tipo de análisis se realiza en base a cientos de características que ayudan a determinar la probabilidad de que el fichero pueda llevar a cabo acciones maliciosas o dañinas cuando se ejecute en el equipo del usuario.

Anti-tamper

Conjunto de tecnologías que evitan la manipulación de los procesos de Panda Endpoint Protection por parte de amenazas avanzadas y APT que buscan sortear las capacidades de protección de la herramienta de seguridad instalada.

Antirrobo

Conjunto de tecnologías incorporadas en que facilitan la localización de los dispositivos móviles extraviados y minimizan la exposición de los datos que contienen en caso de robo.

Antivirus

Módulo de protección basado en tecnologías tradicionales (fichero de firmas, análisis heurístico, análisis contextual etc.), que detecta y elimina virus informáticos y otras amenazas.

Árbol de carpetas

Estructura jerárquica formada por agrupaciones estáticas, utilizada para organizar el parque de equipos y facilitar la asignación de configuraciones.

Árbol de filtros

Colección de filtros agrupados en carpetas que facilitan la organización del parque de equipos y la asignación de configuraciones.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

ARP (Address Resolution Protocol)

Protocolo utilizado para resolver direcciones del nivel de red a direcciones del nivel de enlace. En redes IP traduce las direcciones IP a direcciones físicas MAC.

Asignación automática de configuraciones

Ver Herencia.

Asignación indirecta de configuraciones

Ver Herencia.

Asignación manual de configuraciones

Asignación de una configuración a un grupo de forma directa, en contraposición al establecimiento de configuraciones automático o indirecto, que utiliza el recurso de la herencia para fijar configuraciones sin intervención del administrador.

ASLR (Address Space Layout Randomization)

Técnica implementada por el sistema operativo para mitigar los efectos de ataques de tipo exploit basados en desbordamiento de buffer. Mediante ASLR el sistema operativo introduce aleatoriedad a la hora de asignar direcciones de memoria para reservar espacio destinado a la pila, el heap y las librerías cargadas por los procesos.

De esta forma, se dificulta la utilización ilegítima de llamadas a funciones del sistema por desconocer la dirección física de memoria donde residen.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

Conjunto de recursos desarrollados por la empresa Mitre Corp. para describir y categorizar los comportamientos peligrosos de los ciberdelincuentes, basados en observaciones a lo largo de todo el mundo. ATT&CK es una lista ordenada de comportamientos conocidos de los atacantes, separados en tácticas y técnicas, y que se expresan a través de una matriz. Ya que esta lista es una representación completa de los comportamientos que los hackers reproducen cuando se infiltran en las redes de las empresas, es un recurso útil para desarrollar mecanismos tanto defensivos como preventivos y resolutivos por parte de las organizaciones. Consulta Mitre corp..

B

Backup

Área de almacenamiento de ficheros maliciosos no desinfectables, así como de spyware y herramientas de hacking detectadas. Todos los programas eliminados del sistema por ser clasificados como amenazas se copian de forma temporal en el área de backup / cuarentena durante un periodo de entre 7 y 30 días según su tipo.

BitLocker

Software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo y utilizado por Panda Full Encryption.

Broadcast

Transmisión de paquetes en redes de datos a todos los nodos de la subred: un paquete de datos llegará a todos los equipos dentro de la misma subred sin necesidad de enviarlo de forma individual a cada nodo. Los paquetes de broadcast no atraviesan encaminadores y utilizan un direccionamiento distinto para diferenciarlos de los paquetes unicast.

C

Caché (rol)

Equipos que descargan y almacenan de forma automática todos los ficheros necesarios para que otros equipos con Panda Endpoint Protection instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Ciclo de vida del malware

Detalle de todas las acciones desencadenadas por un programa malicioso, desde que fue visto por primera vez en un equipo del

cliente hasta su clasificación como malware y posterior desinfección.

CKC (Cyber Kill Chain)

La empresa Lockheed-Martin describió en 2011 un marco o modelo para defender las redes informáticas, en el que se afirmaba que los ciberataques ocurren en fases y cada una de ellas puede ser interrumpida a través de controles establecidos. Desde entonces, la Cyber Kill Chain ha sido adoptada por organizaciones de seguridad de datos para definir las fases de los ciberataques. Estas fases abarcan desde el reconocimiento remoto de los activos del objetivo hasta la exfiltración de datos.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Panda Full Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación de 48 dígitos. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo. Cada volumen cifrado tendrá su propia clave de recuperación independiente.

Configuración

Ver Perfil de configuración.

Consola Web

Herramienta de gestión del servicio de seguridad avanzada Panda Endpoint Protection, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador puede desplegar el software

de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección. También permite utilizar herramientas de análisis forense que establecen el alcance de los problemas de seguridad.

Control de dispositivos

Módulo que define el comportamiento del equipo protegido al conectar dispositivos extraíbles o de almacenamiento masivo, para minimizar la superficie de exposición del equipo.

Cuarentena

Ver Backup.

Cuenta de usuario

Ver Usuario (consola).

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

D

DEP

Característica de los sistemas operativos que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.

Desbordamiento de buffer

Fallo en la gestión de los buffers de entrada de un proceso. En estos casos, si el volumen de datos recibido es mayor que el tamaño del buffer reservado, los datos sobrantes no se descartan, sino que se escriben en zonas de memoria adyacentes al buffer. Estas zonas de memoria pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.

Descubridor (rol)

Equipos capaces descubrir puestos de usuario y servidores no administrados para iniciar una instalación remota del agente Panda Endpoint Protection.

Desinfectable

Fichero infectado por malware del cual se conoce el algoritmo necesario para poder revertirlo a su estado original.

DHCP

Servicio que asigna direcciones IP a los nuevos equipos conectados a la red.

Dialer

Programa que marca un número de tarificación adicional (NTA), utilizando para ello el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

Directorio Activo

Implementación propietaria de servicios LDAP (Lightweight Directory Access Protocol, Protocolo Ligero/Simplificado de Acceso a Directorios) para máquinas Microsoft Windows. Permite el acceso a un servicio de directorio para buscar información diversa en entornos de red.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio (PDC) o Directorio Activo (AD).

E

Entidad

Predicado o complemento incluido en las tablas de acciones del módulo análisis forense.

Entidad (Data Control)

Conjunto de datos que tomados como una unidad adquieren un significado propio.

EoL (End Of Life)

Término utilizado para indicar el final del ciclo de vida de un producto. A partir de la fecha indicada el producto ya no recibirá actualizaciones ni parches que corrijan sus defectos, convirtiéndose en un objetivo claro para los hackers.

Equipos sin licencia

Equipos cuya licencia ha caducado o no ha sido posible asignar una licencia válida por haberse superado el número máximo permitido de instalaciones de la protección. Estos equipos no están protegidos, pero son visibles en la consola web de administración.

Excluido (programa)

Son programas inicialmente bloqueados por haber sido clasificados como malware o PUP, pero que el administrador de la red permite su ejecución de forma selectiva y temporal excluyéndolos del análisis.

F

Filtro

Contenedor de equipos de tipo dinámico que agrupa de forma automática aquellos elementos que cumplen con todas las condiciones definidas por el administrador. Los filtros simplifican la asignación de configuraciones de seguridad y facilitan la administración de los equipos del parque informático.

Firewall

También conocido como cortafuegos, es una tecnología que bloquea el tráfico de red que coincide con patrones definidos por el administrador mediante reglas. De esta manera se limita o impide la comunicación de ciertas aplicaciones que se ejecutan en los equipos, restringiéndose la superficie de exposición del equipo.

FQDN (Fully Qualified Domain Name)

Es un nombre de dominio que especifica la localización de forma precisa y sin ambiguedades dentro del árbol de jerarquía del sistema de nombres DNS. El FQDN especifica todos los niveles del dominio incluyendo el nivel superior y la zona raiz (root).

Fragmentación

En redes de transmisión de datos, cuando la MTU del protocolo subyacente es menor que el tamaño del paquete a transmitir, los encaminadores dividen el paquete en piezas más pequeñas (fragmentos) que se encaminan de forma independiente y se ensamblan en el destino en el orden apropiado.

G

Geolocalizar

Posicionar en un mapa un dispositivo en función de sus coordenadas.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grupo

Contenedor de tipo estático que agrupa a uno o más equipos de la red. La pertenencia de un equipo a un grupo se establece de forma manual. Los grupos se utilizan para simplificar la asignación de configuraciones de seguridad y para facilitar la administración de los equipos del parque informático.

Grupo de trabajo

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios residen en cada uno de los equipos de forma independiente.

H

Heap Spraying

Head Spray es una técnica utilizada para facilitar la explotación de vulnerabilidades por parte de un proceso malicioso independiente. Debido a la constante mejora de los sistemas operativos, la explotación de vulnerabilidades se ha convertido es un proceso muy aleatorio. Debido a que el comienzo de la región de memoria heap de un proceso es predecible, y las posteriores reservas de espacio son secuenciales, Head Spray aporta predictibilidad a los ataques, sobrescribiendo porciones de la región de memoria heap del proceso objetivo. Estas porciones de memoria serán referenciadas más adelante por un proceso malicioso para ejecutar el ataque. Esta técnica es muy empleada para explotar vulnerabilidades de navegadores y sus plugins correspondientes.

Herencia

Método de asignación automática de configuraciones sobre todos los grupos descendientes de un grupo padre, ahorrando tiempo de gestión. También llamado Asignación automática de configuraciones o Asignación indirecta de configuraciones.

Herramienta de hacking

Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

I

ICMP (Internet Control Message Protocol)

Protocolo de control y notificación de errores utilizado por el protocolo IP en Internet.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

Incidencia

Mensaje relativo a la protección avanzada de Panda Endpoint Protection, susceptible de requerir la intervención del administrador. Las incidencias se reciben mediante la consola de administración y el correo electrónico (alertas), y el usuario del

equipo protegido mediante mensajes generados por el agente que se visualizan en el escritorio de su dispositivo.

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

J

Joke

Broma con el objetivo de hacer pensar a los usuarios que han sido afectados por un virus.

L

Llave USB

Dispositivo utilizado en equipos con volúmenes cifrados que permite almacenar la clave en una memoria portátil. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

M

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña

un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

Malware freezer

Comportamiento del backup / cuarentena cuyo objetivo es evitar la pérdida de datos por falsos positivos. Todos los ficheros clasificados como malware o sospechosos son enviados a la zona de backup / cuarentena, evitando su borrado completo en previsión de un fallo en la clasificación que derive en pérdida de datos.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

MTU (Maximun transmission unit)

Tamaño máximo del paquete que el protocolo subyacente puede transportar.

MyTerm

N

Nube (Cloud Computing)

Tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

O

OU (Organizational Unit)

Forma jerárquica de clasificar y agrupar objetos almacenados en directorios.

P

Parche

Pequeños programas publicados por los proveedores de software que modifican sus programas corrigiendo fallos y añadiendo nuevas funcionalidades.

Partición de sistema

Zona del disco duro que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio en los equipos con activado.

Partner

Empresa que ofrece productos y servicios de Panda.

Passphrase

También llamado Enhanced PIN (PIN mejorado) o PIN extendido, es una contraseña equivalente al PIN pero que permite añadir caracteres alfanuméricos. Se aceptan letras en mayúscula y minúscula, números, espacios en blanco y símbolos.

PDC (Primary Domain Controller)

Es un rol adoptado por servidores en redes Microsoft de tipo Dominio, que gestiona de forma centralizada la asignación y validación de las credenciales de los usuarios para el acceso a los

recursos de red. En la actualidad el Directorio Activo cumple esta función.

Perfil de configuración

Un perfil es una configuración específica de la protección o de otro aspecto del equipo administrado. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que lo forman.

Phishing

Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

PIN (Personal Identification Number, número de identificación personal)

Secuencia de números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible.

Programas potencialmente no deseados (PUP)

Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.

Protección (módulo)

Una de las dos partes que componen el software que se instala en los equipos. Contiene las tecnologías encargadas de proteger el parque informático y las herramientas de resolución para

desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Software que hace de intermediario de las comunicaciones establecidas entre dos equipos, un cliente situado en una red interna (por ejemplo, una intranet) y un servidor en una extranet o en internet.

Proxy (rol)

Equipo que hace la funciona de pasarela, conectando a otros puestos de usuario y servidores sin salida directa a Internet con la nube de Panda Endpoint Protection.

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

Q

QR (Quick Response), código

Representación gráfica en forma de matriz de puntos que almacena de forma compacta información.

R

Red de confianza

Redes desplegadas en locales privados, tales como oficinas y domicilios. Los equipos conectados son generalmente visibles por sus vecinos y no es necesario establecer limitaciones al compartir archivos, recursos y directorios.

Red pública

Redes desplegadas en locales abiertos al público como cafeterías, aeropuertos, etc. Debido a su naturaleza publica se recomienda establecer límites en el nivel de visibilidad de los equipos que se conectan a este tipo de redes ellas, y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para visualizarlas.

RIR (Regional Internet Registry)

Organización que supervisa la asignación y el registro de direcciones IP y de sistemas autónomos (AS, Autonomous System) dentro de una región particular del mundo.

Rol

Configuración específica de permisos que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los suyos propios). Este tipo de software es utilizado para esconder evidencias y utilidades en sistemas previamente comprometidos.

S

Servicio Advanced Visualization Tool

Servicio avanzado de explotación del conocimiento generado en tiempo real por los productos y . Facilita el descubrimiento de amenazas desconocidas, ataques dirigidos y APTs, representando los datos de actividad de los procesos ejecutados por los usuarios y poniendo el énfasis en los eventos relacionados con la seguridad y la extracción de información.

Servicio Data Control

Modulo compatible con que descubre ficheros PII en la red de la empresa y monitoriza su acceso para cumplir con las regulaciones de almacenamiento de datos vigentes, tales como la GDRP.

Servicio Panda Full Encryption

Módulo compatible con que cifra el contenido de los dispositivos de almacenamiento interno del equipo. Su objetivo es minimizar la exposición de los datos de la empresa ante la pérdida o robo, o en caso de sustitución y retirada de los dispositivos de almacenamiento sin formatear.

Servicio Patch Management

Módulo compatible con Panda Endpoint Protection que parchea y actualizar los programas instalados en los equipos de usuario y

servidores para eliminar las vulnerabilidades producidas por fallos de programación, minimizando así su superficie de ataque.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

Software cliente Panda Endpoint Protection

Programa que se instala en los equipos a proteger. Se compone de dos módulos: el agente Panda y la protección.

Sospechoso

Programa con alta probabilidad de ser considerado malware y clasificado por el análisis heurístico. Este tipo de tecnología solo se utiliza en los análisis programados o bajo demanda lanzados desde el módulo de tareas, y nunca en el análisis en tiempo real. La razón de su uso es la menor capacidad detección de las tareas programadas ya que el código de los programas se analiza de forma estática, sin llegar a ejecutar el programa. Consulta Análisis heurístico.

Spyware

Programa que acompaña a otro y se instala automáticamente en un ordenador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal y utilizarla posteriormente.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

SYN

Bandera (flag) en el campo TOS (Type Of Service) de los paquetes TCP que los identifican como paquetes de inicio de conexión.

T

Táctica

En terminología ATT&CK, las tácticas representan el motivo u objetivo final de una técnica. Es el objetivo táctico del adversario: la razón para realizar una acción. Consulta ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

Tarea

Conjunto de acciones programadas para ejecutarse con una frecuencia y en un intervalo de tiempo configurables.

TCO (Total Cost of Ownership, Coste total de Propiedad)

Estimación financiera que mide los costes directos e indirectos de un producto o sistema

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

Técnica

En terminología ATT&CK, las técnicas representan la forma o la estrategia un adversario logra un objetivo táctico. Es decir, el "cómo". Por ejemplo, un adversario, para lograr el objetivo de acceder a algunas credenciales (táctica) realiza un volcado de

las mismas (técnica). Consulta ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0.

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

TPM (Trusted Platform Module, módulo de plataforma segura)

Es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación. Ademas, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

Troyanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad de los datos del usuario.

U

UDP (User Datagram Protocol)

Protocolo del nivel de transporte dentro de la pila de protocolos de Internet, no confiable y no orientado a la conexión para el envío y recepción de paquetes IP.

Usuario (consola)

Recurso formado por un conjunto de información que Panda Endpoint Protection utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Personal de la empresa que utiliza equipos informáticos para desarrollar su trabajo.

V

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

VDI (Virtual Desktop Infrastructure)

Solución de virtualización de escritorio que consiste en alojar máquinas virtuales en un centro de datos al cual los usuarios acceden desde un terminal remoto con el objetivo de centralizar y simplificar la gestión y reducir los costes de mantenimiento. Se distinguen dos grupos de entornos VDI: Persistente: el espacio de almacenamiento asignado a cada usuario se respeta entre reinicios, incluyendo el software instalado, datos y actualizaciones del sistema operativo. No persistente: el espacio de almacenamiento asignado a cada usuario se elimina cuando la

instancia VDI se reinicia, restaurándose a su estado inicial y deshaciendo todos los cambios efectuados.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de su infección. Durante este periodo de tiempo el malware puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia.

Virus

Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

W

Widget (Panel)

Panel que contiene un gráfico configurable y que representa un aspecto concreto de la seguridad de la red del cliente. El conjunto

de widgets forma el dasboard o panel de control de Panda Endpoint Protection.