seguridad **en la nube**

GUÍA DE ADMINISTRACIÓN

panda

euskaltel

Contenidos

1. Presentación

¿Qué es Endpoint Protection?
Tecnologías de protección
Información y consultas
Requisitos y URL necesarias

1.1 ¿Qué es Endpoint Protection?

Endpoint Protection es una solución completa de seguridad concebida para que puedas proteger tu red informática y gestionar la seguridad de manera sencilla y en modo on line. La protección que proporciona neutraliza spyware, troyanos, virus y cualquier otra amenaza dirigida contra tus equipos.

Sus principales características son:

- Máxima protección para PCs, portátiles, servidores y dispositivos Android.
- Fácil de instalar, gestionar y mantener a través de su consola Web.
- Gestión y organización basada en perfiles de protección y grupos de equipos.

El centro de gestión de Endpoint Protection es la consola Web, desde donde podráss:

1. Configurar la protección -ya sea para Windows, Linux, OS X o Android- distribuirla e instalarla en los equipos.
2. Monitorizar el estado de la protección en los equipos.
3. Extraer informes sobre el estado de la seguridad y las amenazas detectadas.
4. Gestionar las detecciones realizadas y saber en todo momento qué se ha detectado, cuándo y en qué equipo.
5. Configurar la cuarentena de elementos sospechosos.

1.1.1 La protección

De acuerdo con las necesidades de protección de tus equipos, podrás crear perfiles y determinar cuál será el comportamiento de las diferentes protecciones para el perfil que estás creando. A continuación, podrás asignar dicho perfil a los grupos de equipos que quieres proteger.

La protección para servidores Exchange, la protección de control de accesos a páginas Web y la protección antirrobo para dispositivos Android solo podrás activarlas si has adquirido licencias de Endpoint Protection Plus.

Configuración de la protección

Puedes configurar la protección instalada en los equipos antes o después de la instalación. **En el caso de esta guía, se ha optado por explicar el proceso de configuración como paso previo a la instalación de la protección en los equipos**. En cualquier caso, es recomendable que dediques un tiempo a analizar en profundidad cuáles son las necesidades de protección de tu red.

Estas necesidades pueden variar de unos equipos a otros o también pueden ser las mismas para todos ellos. En consecuencia, podrás necesitar crear perfiles nuevos o te bastará con la configuración por defecto que Endpoint Protection proporciona.

1.1.2 La instalación

Recomendaciones previas a la instalación

Antes de instalar la protección, te invitamos a consultar las recomendaciones previas a la instalación, donde encontrarás información importante sobre cuestiones que tienen que ver con el proceso de instalación y desinstalación.

Requisitos de los equipos

Tampoco olvides consultar los requisitos que los diferentes equipos y dispositivos han de reunir para poder instalar la protección en ellos y configurarla para aprovechar al máximo todo lo que Endpoint Protection te ofrece.

Esperamos que todas las indicaciones que encontrarás a lo largo de esta guía te resulten útiles.

1.2 Tecnologías de protección

1.2.1 Tecnología Anti-Exploit

Panda Security ha desarrollado una nueva tecnología, denominada Anti-Exploit, que refuerza sus soluciones de seguridad de manera muy importante y que posibilita detectar virus que ninguna otra compañía de seguridad está detectando.

La tecnología Anti-Exploit detecta y neutraliza el malware que explota vulnerabilidades de día cero (Java, Adobe , MS Office ..) como Blackhole o redkit antes de que infecte el ordenador. La clave es utilizar las tecnologías heurísticas con gran capacidad de detección. Para ello, la nueva protección Anti-Exploit de Endpoint Protection analiza el comportamiento de los exploits en lugar de su morfología.

Endpoint Protection utiliza múltiples sensores para enviar información a la Inteligencia Colectiva sobre el comportamiento de archivos sospechosos que intentan explotar vulnerabilidades de día 0 para infectar equipos informáticos. Esta información permite actualizar constantemente las tecnologías proactivas incluidas en los productos de Panda Security mediante actualizaciones en caliente en la nube.

En definitiva, Endpoint Protection detecta y neutraliza este tipo de malware antes de que se haya identificado y antes incluso de que se haya creado, protegiendo a los usuarios frente a nuevas variantes de malware.

1.2.2 Seguridad desde la nube & Inteligencia Colectiva

¿Qué es "la nube"?

La computación en la nube (*Cloud computing*) es una 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.

Endpoint Protection se sirve de la nube conectándose a los servidores de Inteligencia Colectiva y así proteger su PC desde el primer momento, aumentando la capacidad de detección y evitando penalizar

el rendimiento del equipo. Ahora todo el conocimiento está en la nube y, gracias a Endpoint Protection, tú puedes beneficiarte de ello.

¿Qué es la Inteligencia Colectiva?

La Inteligencia Colectiva es una plataforma de seguridad que ofrece un alto nivel de protección en tiempo real, aumentando exponencialmente la capacidad de detección de Endpoint Protection.

¿Cómo es la detección con la Inteligencia Colectiva?

La Inteligencia Colectiva consta de servidores que clasifican y procesan de forma automática toda la información que la comunidad de usuarios proporciona sobre las detecciones que se han producido en sus equipos. Endpoint Protection realiza consultas a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos de los equipos.

Cuando un nuevo ejemplar de malware es detectado en el equipo de un miembro de la comunidad de usuarios, Endpoint Protection se encarga de enviar la información necesaria a los servidores de Inteligencia Colectiva alojados en la nube, de forma totalmente automática y anónima. La información es procesada por dichos servidores, entregando una solución no sólo al usuario afectado, sino también al resto de usuarios de la comunidad, en tiempo real. De ahí el nombre de Inteligencia Colectiva.

Sin lugar a dudas, en el contexto actual de crecimiento continuo del malware, la Inteligencia Colectiva y los servicios alojados y servidos desde la nube vienen a complementar a las actualizaciones tradicionales para afrontar con éxito y anticipación la enorme cantidad de amenazas que surgen en la actualidad.

1.3 Información y consultas

1.3.1 Información, consultas y servicios

Junto a los productos, Panda Security pone a tu disposición ayudas y documentación con las que podrás ampliar información, resolver dudas, acceder a las últimas actualizaciones y beneficiarte de otros servicios. Además, podrás estar al tanto de la actualidad y las novedades sobre seguridad informática. Visita la Web de Panda Security y accede a toda la información que necesitas.

1.3.2 Enlaces de interés

- Página principal: http://www.pandasecurity.com/spain.

Toda la información de Panda Security a tu disposición.

- Documentación: http://www.pandasecurity.com/spain/enterprise/downloads/docs/product

Encontrarás la documentación actualizada de los productos y otras publicaciones de interés.

- Soporte técnico: http://www.pandasecurity.com/spain/enterprise/support

Resuelve tus dudas sobre infecciones, virus, productos y servicios de Panda Security a cualquier hora del día y cualquier día del año, con información y ayuda continua y completamente actualizada.

- Soporte técnico de Endpoint Protection

http://www.pandasecurity.com/spain/enterprise/support/cloud-office-protection.htm

- Soporte técnico de Endpoint Protection Plus
http://www.pandasecurity.com/spain/enterprise/support/cloud-office-protection-advanced.htm

- Software de evaluación: http://www.pandasecurity.com/spain/enterprise/downloads/evaluation/

Panda Security te proporciona software de evaluación para que pruebes gratuitamente el producto que desees.

- Productos: http://www.pandasecurity.com/spain/enterprise/solutions/

Consulta las características de todos los productos de Panda Security. También puedes adquirirlos y probarlos sin compromiso.

1.3.3 Servicios de Endpoint Protection

Además de esta guía en la que encontrarás la información que necesitas para sacar el máximo rendimiento a tu protección, Panda Security te proporciona otros servicios. Son valores añadidos al producto que has adquirido y que te permitirán contar, desde el primer momento, con el asesoramiento y la última tecnología que, en materia de seguridad, Panda Security aplica a sus productos.

Los servicios que ofrece Endpoint Protection son:

- Actualizaciones diarias del archivo de identificadores.
http://www.pandasecurity.com/spain/enterprise/downloads/clients

-Soporte técnico especializado tanto telefónico como vía e-mail.
http://www.pandasecurity.com/spain/enterprise/support/

- Actualización general de Endpoint Protection: nuevas características, mejoras en su capacidad de detección, etc.

- Documentación: Acceso a la Guía avanzada de administración.
http://documents.managedprotection.pandasecurity.com/AdvancedGuide/es-es/index.htm

1.3.4 Otros servicios

Desde la consola Web de Endpoint Protection, puedes acceder a otros servicios que te permitirán enviar sugerencias y contactar con el soporte técnico de Panda Security. Haz clic en **Otros servicios**.

1.3.5 Soporte técnico

Desde la ventana **Otros servicios,** podrás enviar sugerencias a Panda Security y acceder al área de soporte técnico, donde encontrarás las respuestas a las dudas que puedas tener sobre Endpoint Protection y todo el resto de información y utilidades que Panda Security pone a tu disposición.

1.3.6 Solución de problemas

En la página de soporte técnico encontrarás un **listado con los códigos de error más comunes** de Endpoint Protection e información actualizada sobre todos ellos.

Accede a la siguiente dirección:

http://www.pandasecurity.com/spain/enterprise/support/card?id=50032

1.3.7 Buzón de sugerencias

Con tus comentarios y sugerencias podremos continuar mejorando Endpoint Protection y adaptándolo a tus necesidades. Por favor, no dudes en ponerte en contacto con nosotros.

1.4 Iconos

En esta guía aparecen los siguientes iconos:


Información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.


Sugerencias y recomendaciones.


Consejo importante de cara a un uso correcto de las opciones de Endpoint Protection.

1.5 Requisitos y URLs necesarias

Endpoint Protection ha sido concebido como la solución óptima para proteger tu red informática, pero para poder extraer todo su potencial y disfrutar al máximo de sus funcionalidades, los equipos que intervienen en el proceso de acceso, instalación, configuración y despliegue de la protección han de reunir una serie de requisitos.

1.5.1 Requisitos de instalación en sistemas Windows .

Requisitos para acceder a la Consola de Administración:

Navegador:

- Internet Explorer
- Mozilla Firefox
- Google Chrome

Red:

- Conexión a Internet: directa o a través de una red local.
- Conexión HTTPS (puerto 443).

Requisitos mínimos del equipo desde el que se realiza el despliegue:

- Sistema operativo: Windows 8.1 (PCOP 6.70.20), Windows 8 (PCOP 6.20.10), Windows 7 (32 y 64 bits), Windows Vista (32 y 64 bits), Windows XP Professional (32 y 64 bits), Windows 2000 Professional, Windows Server 2000, Windows Server 2003 (32 y 64 bits), Windows Server 2008 (32 y 64 bits), Windows Server 2008 R2, Windows Home Server, Windows Server 2012 y Windows Server 2012 R2 (PCOP 6.70.20).
- Memoria: 64 MB
- Disco duro: 20 MB
- Procesador: Pentium II 300 MHz o equivalente
- Windows Installer 2.0 (aunque se recomienda Windows Installer 3.0 si se quiere poder desinstalar de forma remota)
- Navegador: Internet Explorer 6.0 o superior

Otros:

- Tener acceso al recurso Admin$ de los equipos en los que se va a distribuir la protección.
- Disponer de un usuario con derechos de administrador sobre los equipos en los que se va a distribuir la protección.

Requisitos mínimos de los equipos a los que se distribuye la protección:

- Procesador: Pentium 300 Mhz. o equivalente
- Disco duro: 256 MB
- Espacio para la instalación: 500 MB
- Navegador: Internet Explorer 6.0 o superior
- Otros: En equipos con sistema operativo anterior a Windows XP SP2 o Windows 2003 Server SP1:
- Windows Installer 2.0 (aunque se recomienda Windows Installer 3.0 si se quiere poder desinstalar de forma remota)
- Deshabilitar el firewall de Windows o bien configurar la excepción Compartir archivos e impresoras (Inicio, Configuración,Panel de Control, Conexiones de red, Conexión de área local, (botón derecho) Propiedades, pestaña General).
- Tener desactivado el uso compartido simple de archivos (en Windows XP, Herramientas, Opciones de carpeta, Ver, Utilizar uso compartido simple de archivos).

Estaciones:

- Sistemas operativos: Windows 8.1 (PCOP 6.70.20), Windows 8 (PCOP 6.20.10), Windows 7 (32 y 64-bit), Windows Vista (32 y 64-bit), Windows XP (32 y 64-bit) y Windows 2000 Professional.
- Memoria RAM: Para la protección Antivirus: 64 MB y para la protección Firewall: 128 MB

Servidores:

- Sistemas operativos: Windows 2000 Server, Windows Home Server, Windows Server 2003 (32 y 64 bits), Windows Server 2008 (32 y 64 bits)*, Windows Server 2008 R2*, Windows Server 2012 (PCOP 6.20.10) y Windows Server 2012 R2 (PCOP 6.70.20).
- Memoria RAM: 256 MB

Otras aplicaciones compatibles:

- VMWare ESX 3.x,4.x, 5,x
- VMWare Workstation 6.0, 6.5, 7.x, 8.x y 9.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008 R2 y 2012 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer y XenApp 5.x y 6.x

Para distribuir desde la herramienta de distribución a máquinas con Windows server 2008 R2, se debe activar la opción de "Activar la gestión remota del servidor desde otro ordenador". Esta opción, está desactivada por defecto, y es necesario que esté activada y permitida por el firewall. Para activar esta opción, se deben seguir las instrucciones de Microsoft especificadas en el siguiente artículo: http://support.microsoft.com/kb/976839

Requisitos mínimos de los equipos a los que se distribuye la protección de Servidores Exchange (solo en Endpoint Protection Plus)

Los requisitos de hardware para instalar la protección de Servidores Exchange son los que marca el propio Exchange Server:

Exchange 2003:

http://technet.microsoft.com/es-es/library/cc164322(v=exchg.65).aspx

Exchange 2007:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.80).aspx

Exchange 2010:

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.141).aspx

Exchange 2013

http://technet.microsoft.com/es-es/library/aa996719(v=exchg.150).aspx

Versiones que protege la protección para Servidores Exchange incluida en Endpoint Protection Plus:

- Microsoft Exchange Server 2003 Standard (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2003 Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2003 included in Windows SBS 2003
- Microsoft Exchange Server 2007 Standard (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 Enterprise (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 included in Windows SBS 2008
- Microsoft Exchange Server 2010 Standard (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 included in Windows SBS 2011
- Microsoft Exchange Server 2013 Standard
- Microsoft Exchange Server 2013 Enterprise

Roles en los que se instala la protección Servidores Exchange en Exchange 2007 y Exchange 2010:

- Mailbox
- Hub Transport
- Edge Transport

Roles en los que se instala la protección Servidores Exchange en Exchange 2013:

- Mailbox

Sistemas operativos soportados:

Exchange 2003: Windows Server 2003 32bits SP1+ y Windows Server 2003 R2 32bits

Exchange 2007: Windows Server 2003 64bits SP1+, Windows Server 2003 R2 64bits, Windows 2008 64bits y Windows 2008 R2

Exchange 2010: Windows 2008 64bits y Windows 2008 R2

Exchange 2013: Windows 2012

No se soporta la instalación del Firewall en Servidores Windows Server 2008 con balanceo NLB en versiones 5.X.

Para más información, consulte el siguiente artículo sobre cómo evitar la pérdida de comunicación en un cluster de Windows Server 2008 con Network Load Balancing (NLB) e instalar la protección:

http://www.pandasecurity.com/spain/support/card?id=50048&idIdioma=1

Tenga en cuenta que si desea que sus equipos se comuniquen con los servidores de la Inteligencia Colectiva, es necesario que tengan conexión a Internet. Si tienen acceso y éste se realiza a través de un proxy, recuerde que ha de configurarlo adecuadamente.

Para ello, introduzca los datos necesarios en la sección Configuración general del perfil.

1.6 Requisitos de instalación en sistemas Linux

1.6.1 Distribuciones soportadas

Endpoint Protection se ha certificado en las siguientes versiones de Sistemas Operativos:

- Ubuntu (32/64 bits) versión 12 o superior
- Red Hat Enterprise (64 bits) versión 6.0 o superior
- Debian Squeeze (32/64 bits)
- OpenSuse (32/64 bits) versión 12 o superior
- Suse Enterprise Server de 64 bits versión 11SP2 o superior
- CentOS 6.x o superior

1.6.2 Prerrequisitos

Para que el producto funcione correctamente el sistema debe cumplir los siguientes requisitos:

- Debe estar instalada la utilidad lsb_release (en RedHat y Debian).
- Esta utilidad se utiliza para determinar la distribución de Linux en que se está ejecutando el instalador.
- En Debian se debe descargar e instalar el paquete: ***lsb-release_3.2-23.2squeeze1_all.deb***
- En RedHat se debe descargar e instalar el paquete: ***redhat-lsb.i686***

1.6.3 Dependencias de la protección PavSL (todas las distribuciones).

La protección PavSL necesita de la instalación de las siguientes librerías para su correcto funcionamiento:

- libsoup-2.4.so.1 (HTTP client/server library for GNOME)
- libgthread-2.0
- libmcrypt.so.4 (MCrypt - encryption functions)
- libz.so.1 (zlib compression and decompression library)

Comprobar que en el directorio /opt/PCOPAgent/PCOPScheduler/pavsl-bin/ se encuentran todas las dependencias de la "PavSL":

- # ldd libPskcomms.so

En caso de SUSE/OpenSUSE de x64, si hay problemas, aplicar la siguiente solución alternativa o workaround:

- Instalar (si no lo está) libsoup-2_4-1-32bit. Por ejemplo:

  # zypper install libsoup-2_4-1-32bit

- Instalar (si no lo está) libgthread-2_0-0-32bit. Por ejemplo:

  # zypper install libgthread-2_0-0-32bit

- Desinstalar libmcrypt y mcrypt:

  # zypper rm libmcrypt

  # zypper rm mcrypt

- Instalar "libmcrypt-2.5.8-109.1.2.i586.rpm". Descargar e instalar si no lo está ya.

En caso de Ubuntu x64 se deben ejecutar los siguientes comandos para instalar las dependencias necesarias para el correcto funcionamiento del servicio:

- sudo dpkg --add-architecture i386
- sudo apt-get update
- sudo apt-get install libglib2.0-0:i386
- sudo apt-get install libsoup2.4-1:i386
- sudo apt-get install libmcrypt4:i386
- sudo apt-get install libgssapi-krb5-2:i386

1.6.4 AT/CRON se encuentran correctamente instalados y habilitados (en todas las distribuciones)

Verifique que los servicios de AT y CRON se encuentran correctamente instalados y activados en los servicios del sistema.

Workaround para el "ATD" (En SUSE y OpenSUSE)

Las acciones para solucionar que el "atd" no arranque de forma automática en openSUSE son las siguientes:

Alterar el fichero: /etc/sysconfig/atd

ATD_BATCH_INTERVAL = "60"

ATD_LOADAVG = "0.8"

Alterar el fichero /lib/systemd/system/atd.service para transformarlo en:

cat /lib/systemd/system/atd.service

[Unit]

Description=Execution Queue Daemon

After=syslog.target

[Service]

Type=forking

EnvironmentFile=-/etc/sysconfig/atd

ExecStart=/usr/sbin/atd -b ${ATD_BATCH_INTERVAL} -l ${ATD_LOADAVG}

[Install]

WantedBy=multi-user.target

Recargar el demonio, arrancarlo y comprobar el status:

- # chkconfig --add atd
- # systemctl --system daemon-reload
- # systemctl enable atd.service
- # systemctl start atd.service
- # systemctl status atd.service

atd.service - Execution Queue Daemon

Loaded: loaded (/lib/systemd/system/atd.service; disabled)

Active: active (running) since Fri, 05 Oct 2012 12:14:52 -0500; 1s ago

Process: 20851 ExecStart=/usr/sbin/atd -b ${ATD_BATCH_INTERVAL} -l ${ATD_LOADAVG} (code=exited, status=0/SUCCESS)

Main PID: 20852 (atd)

CGroup: name=systemd:/system/atd.service

|_ 20852 /usr/sbin/atd -b 60 -l 0.8

Reiniciar la máquina para que a partir de ese momento lo tenga en cuenta cada vez que arranca:

reboot

Una vez reiniciada, verificar el estado del servicio:

systemctl status atd.service

Para ejecutar el script de configuración del proxy es necesario que esté disponible el comando whiptail. En SUSE este comando se encuentra en el paquete newt. Para instalarlo se debe utilizar el siguiente comando:

zipper install newt

1.7 Requisitos de instalación en sistemas OS X

Endpoint Protection for OS X necesita que el equipo donde se instale cuente con los siguientes requisitos de sistema para instalarse y funcionar correctamente:

Sistemas operativos

Endpoint Protection soporta los siguientes sistemas OS X:

- MAC OS X 10.6 Snow leopard (Procesador Intel Core 2 Duo o superior)
- MAC OS X 10.7 Lion
- MAC OS X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- Mac OS X 10.10 Yosemite

Hardware

- Procesador: Intel® Core 2 Duo
- Disco duro: 1.5 GB espacio libre en disco
- Navegador: Internet Explorer: 5.5 o superior, Firefox y Chrome

Otros

Debe concederse acceso a las siguientes direcciones:

- mp-agents-inst.pandasecurity.com
- mp-agents-sync.pandasecurity.com
- mp-agents-async.pandasecurity.com
- proinfo.pandasoftware.com
- http://www.netupdate2.intego.com
- https://www.netupdate2.intego.com
- http://www.integodownload.com
- http://www.intego.com

1.8 Requisitos de los dispositivos Android

Se soportan todas las versiones iguales o superiores a 2.3 (Gingerbread).

Es recomendable que antes de instalar la protección te asegures de que dispones de una aplicación de escaneo de códigos QR instalada en el dispositivo.

1.9 URL's necesarias

Para acceder a los servidores de Endpoint Protection y poder descargar las actualizaciones, es necesario que al menos uno de los equipos de la subred tenga acceso a una serie de páginas Web:

Consola

https://www.pandacloudsecurity.com/

https://managedprotection.pandasecurity.com/

https://pandasecurity.logtrust.com

Updates y upgrades

http://acs.pandasoftware.com/member/installers/

http://acs.pandasoftware.com/member/uninstallers/

http://enterprise.updates.pandasoftware.com/pcop/pavsig/

http://enterprise.updates.pandasoftware.com/pcop/nano

http://enterprise.updates.pandasoftware.com/pcop/sigfiles/sigs

http://acs.pandasoftware.com/free/

http://acs.pandasoftware.com/sigfiles

http://acs.pandasoftware.com/pcop/uacat

http://enterprise.updates.pandasoftware.com/pcop/uacat/

http://enterprise.updates.pandasoftware.com/updates_ent/

https://pcopsupport.pandasecurity.com

http://pcoplinux.updates.pandasecurity.com/updates/nanoupdate.phtml (en sistemas Linux)

http://pcoplinux.downloads.pandasecurity.com/nano/pavsignano/nano_1/ (en sistemas Linux)

http://www.intego.com (OS X systems)

http://www.integodownload.com (OS X systems)

http://www.netupdate2.intego.com (OS X systems)

https://www.netupdate2.intego.com (OS X systems)

Megacuarentena

http://hercules.pandasoftware.com/getqesi.aspx

http://hercules.pandasoftware.com/getqesd.aspx

Comunicaciones con el servidor

https://mp-agents-inst.pandasecurity.com

http://mp-agents-inst.pandasecurity.com/Agents/Service.svc

https://mp-agents-inst.pandasecurity.com/AgentsSecure/Service.svc

http://mp-agents-sync.pandasecurity.com/Agents/Service.svc

https://mp-agents-sync.pandasecurity.com/AgentsSecure/Service.svc

http://mp-agents-async.pandasecurity.com/Agents/Service.svc

https://agentscomp.pandasecurity.com/AgentsSecure/Service.svc

mp-agents-inst.pandasecurity.com (OS X systems)

mp-agents-sync.pandasecurity.com (OS X systems)

mp-agents-async.pandasecurity.com (OS X systems)

https://pac100pacprodpcop.table.core.windows.net

https://storage.accesscontrol.pandasecurity.com

https://prws.pandasecurity.com

https://rpuws.pandasecurity.com/frws (v7.10)

https://pcopsupport.pandasecurity.com

Comunicaciones con los servidores de Inteligencia Colectiva

http://cache.pandasoftware.com

http://cache2.pandasecurity.com

https://rpkws.pandasecurity.com/kdws/files

http://proinfo.pandasoftware.com (OS X systems)

http://proinfo.pandasoftware.com/connectiontest.html

Si el acceso a esta URL falla, el producto intentará establecer la conexión con http://www.iana.org.

https://ims.pandasecurity.com/ProySRF

http://statistics.pandasoftware.com

https://euws.pandasecurity.com

https://rpuws.pandasecurity.com

https://rpkws.pandasecurity.com/kdws/sigs

Android

https://dmp.devicesmc.pandasecurity.com

https://rpuws.pandasecurity.com

https://rpkws.pandasecurity.com/kdws/sigs

http://iext.pandasecurity.com/ProyIEXT/ServletIExt

Instalación de agente de Panda Cloud Systems Management desde PCOP (desde v6.70)

https://sm.pandasecurity.com/csm/profile/downloadAgent/

Tráfico entrante y saliente (Antispam y URL Filtering en PCOPA)

http://*.pand.ctmail.com

http://download.ctmail.com

Es necesario que habilite los puertos (intranet del cliente) TCP 18226 y UDP 21226 para el correcto funcionamiento de la tecnología P2P y centralización de conexiones con el servidor a través de un equipo.

2. Creación de Cuentas Panda

¿Qué es la Cuenta Panda?

¿Cómo puedes crear tu Cuenta Panda?

¿Cómo puedes activar tu Cuenta Panda?

2.1 ¿Qué es la Cuenta Panda?

Cuando adquieres Endpoint Protection recibirás un mensaje de correo electrónico procedente de Panda Security. Al hacer clic en el vínculo que contiene el mensaje, accederás a la Web desde la que podrá crear tu Cuenta Panda.

A continuación deberás activar tu Cuenta Panda, utilizando para ello el vínculo que te será enviado en otro mensaje de correo electrónico.

Finalmente accederás a Panda Cloud, donde encontrarás el icono de acceso directo a la consola Web de Endpoint Protection.

De esta forma se incrementa el nivel de seguridad con respecto a las contraseñas de acceso, ya que en lugar de recibirlas por correo electrónico, es el administrador quien crea y activa su Cuenta Panda, la llave que le permitirá el acceso a la consola Web de Endpoint Protection.

Gracias a Panda Cloud podrás gestionar de forma rápida y sencilla las diferentes soluciones cloud que tienes contratadas y, si lo necesitas, acceder a información sobre otras soluciones de Panda Security que, sin duda, cubrirán todas las necesidades que en materia de seguridad y protección tiene tu red informática.

2.2 ¿Cómo puedes crear una Cuenta Panda?

Tras adquirir las licencias correspondientes recibirás un mensaje de correo electrónico. Es el momento de crear la Cuenta Panda. Para ello:

1. Abre el mensaje y haz clic en el vínculo que aparece.
2. Accederás a la página desde la que podrás crear la Cuenta Panda.
3. Introduce tu dirección de email y haz clic en **Crear**.

Utiliza el desplegable situado en la esquina inferior derecha si deseas que la página se muestre en otro idioma. También puedes acceder al acuerdo de licencia y la política de privacidad haciendo clic en el vínculo correspondiente.

A continuación recibirás un mensaje de correo electrónico en la dirección que has especificado al crear la Cuenta Panda. Utilizando ese mensaje podrás activar la cuenta.

2.3 ¿Cómo puedes activar tu Cuenta Panda?

Una vez creada la **Cuenta Panda** es necesario activarla. Para ello hay que utilizar el mensaje de correo electrónico que has recibido en la bandeja de entrada de la dirección mail que se utilizó para crear la Cuenta Panda.

1. Ve a la bandeja de entrada y localiza el mensaje.

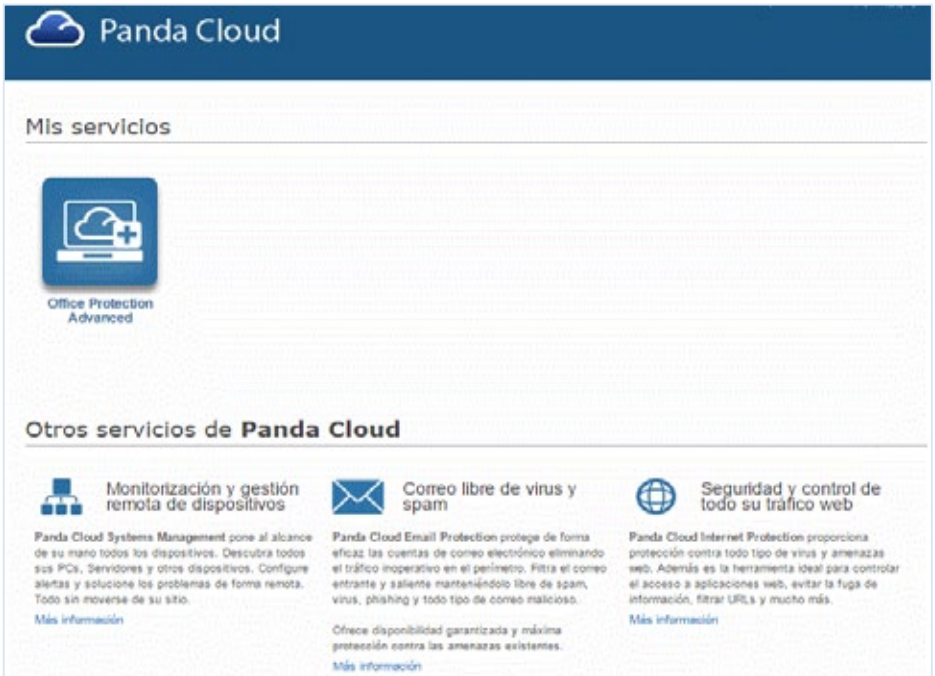
2. A continuación, haz clic en el botón de activación. Al hacerlo, se confirmará como válida la dirección proporcionada al crear la Cuenta Panda. En caso de que el botón no funcione, copia en el navegador el enlace que se muestra en el mensaje.

3. La primera vez que se acceda a la Cuenta Panda se solicitará una confirmación de contraseña. Después, haz clic en el botón **Activar cuenta**.

4. Introduce los datos necesarios y haz clic en Guardar datos. Si prefieres facilitar los datos en otra ocasión, utiliza la opción **Ahora no**.

5. Acepte el acuerdo de licencias y haz clic en **Aceptar**.

Has finalizado con éxito el proceso de activación de la Cuenta Panda. Ahora te encontrarás en la página principal de Panda Cloud. Desde aquí ya puedes acceder a la consola Web de Endpoint Protection. Para ello, utiliza el icono de acceso directo que encontrarás en **Mis servicios**.



3. Acceso a la consola Web

Acceso a la consola Web

Preferencias

3.1 Acceso a la consola Web

Cuando accedas a la consola, se mostrará la ventana Estado. Mediante unos contadores te indicará cuál es el estado de la protección y sus licencias.

Si aún no has instalado la protección en ninguno de tus equipos, se mostrará una invitación para que lo hagas e indicaciones para que sepas desde dónde lo puedes realizar.

3.1.1 Otras opciones disponibles desde la consola Web

Salir de la consola

Mediante la opción **Salir**, puedes cerrar la sesión.

Selección de idioma

También puedes seleccionar el idioma en el que deseass visualizar la consola Web, utilizando el desplegable **Idioma** situado junto al idioma activo.

Crear usuarios

Para crear nuevos usuarios y asignarles permisos de acceso y privilegios de gestión de la consola Web, haz clic en **Usuarios**.

Establecer preferencias

Para establecer la configuración general de tu consola Web, haz clic en Preferencias.

Acceder a más información

Si deseas acceder a la ayuda de Endpoint Protection y conocer las últimas novedades o consultar la Guía Avanzada de Administración, selecciona la opción correspondiente en el menú desplegable **Ayuda**.

Utiliza también este menú si lo que deseas es acceder al Acuerdo de Licencia, enviar sugerencias o acceder a soporte técnico.

Acerca de...

Este menú muestra información sobre:

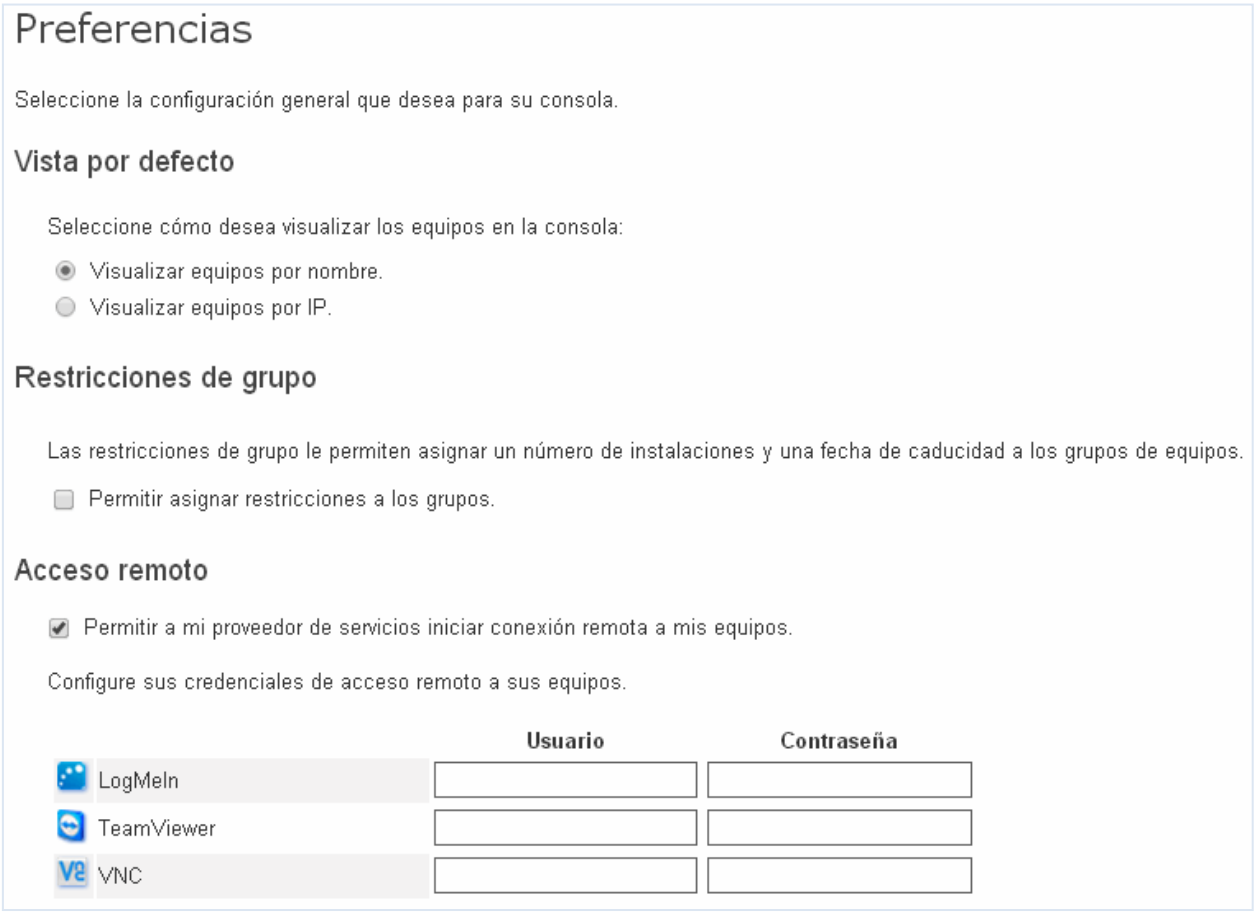
- La versión de la consola Web.
- La última versión de Endpoint Protection instalada en el parque informático.
- La última versión del agente instalada en el parque informático.
- Si tienes varios equipos y en cada uno de ellos hay instalada una versión diferente de la protección, el menú **Acerca de** mostrará la versión más reciente de todas ellas.
- Si no has instalado la protección en ningún equipo, se muestra la última versión disponible de la protección, es decir, la que será instalada en los equipos.

3.2 Preferencias

Desde esta ventana, puedes establecer configuraciones generales que afectarán a tu consola Web.

3.2.1 Vista por defecto

Elige la manera en que se mostrarán los equipos: por nombre o por IP. Marca la opción deseada.



3.2.2 Restricciones de grupo

Selecciona esta opción si deseas limitar el número de instalaciones y la fecha de caducidad de los grupos. Para ello, marca la casilla correspondiente.

3.2.3 Acceso remoto

Utiliza esta sección para introducir las credenciales con las que accederás a los equipos a través de las diferentes herramientas de acceso remoto.

Estas credenciales serán propias de cada usuario, es decir, usuarios diferentes de la consola de administración podrán incluir credenciales diferentes de acceso a los equipos.

Si deseas eliminar el acceso remoto a tus equipos a tu proveedor de servicio, desmarca la opción **Permitir a mi proveedor de servicios iniciar conexión remota a mis equipos**.

Acceso remoto desde la consola de Partner Center

En el caso de que el acceso a la consola se produzca desde una consola de Partner Center

(http://www.pandasecurity.com/spain/enterprise/solutions/cloud-partner-center/), las credenciales que introduzca el usuario que acceda por primera vez, serán las mismas que utilizarán otros usuarios de la consola de Partner Center que intenten acceder con posterioridad.

Cada usuario que acceda desde la consola de Partner Center tendrá la posibilidad de cambiar las credenciales, pero dicho cambio afectará al resto de usuarios.

3.2.4 Gestión automática de archivos sospechosos

Utiliza esta opción si deseas que los archivos sospechosos sean enviados al laboratorio para su estudio. De esta forma, en caso de infección se podrá proporcionar una respuesta en el menor tiempo posible y acelerar la distribución de la protección adecuada.

3.2.5 Gestión de cuentas

Si eres un usuario con permisos de control total, podrás acceder a las funcionalidades de gestión de cuentas:

- Unificar cuentas
- Delegar la gestión de la seguridad en un partner

4. La ventana Estado

Estado de la protección

Estado de las licencias

Visualización de las licencias

4.1 Estado de la protección

La ventana **Estado** es la primera que se muestra una vez que se accede a la consola. En ella se detalla información sobre el estado de la protección y sus licencias, utilizando para ello unos contadores.

Si tú aun no has instalado la protección en ninguno de tus equipos, se te mostrará la ventana **Equipos** con un mensaje invitando a que lo hagas y las indicaciones necesarias para ello.

4.1.1 Notificaciones

Esta sección se mostrará cuando existan cuestiones que pueden ser de tu interés, tales como la existencia de versiones nuevas del producto o avisos sobre incidencias técnicas, mensajes informativos acerca del estado de tus licencias o cuestiones críticas que requieran especialmente tu atención.

4.1.2 Acceso a nueva versión del producto

En el caso de existir una nueva versión del producto, podrás ver un resumen de las principales novedades utilizando el link **Ver novedades de la version XXX**.

Para actualizar el producto, haz clic en el botón **Cambiar a la nueva versión** y acepta el mensaje de confirmación. Una vez fuera de la consola, se te solicitará que introduzcas de nuevo la contraseña y el Login Email. Acto seguido accederás a la consola Web de la nueva versión de Endpoint Protection.

4.1.3 Estado de la protección

Podrás ver cuál es el estado de la protección instalada en tus equipos así como qué protecciones muestran algún error o falta de actualización del motor de la protección o del archivo de identificadores (incluye los equipos que tienen desactivada la actualización automática de la protección). También se te indicará si hay algún equipo pendiente de reinicio.

Protecciones instaladas

Si haces clic en el número de equipos con protección instalada, accederás al listado de equipos protegidos.

Protecciones desactualizadas

Si haces clic en el número que representa protecciones desactualizadas (ya sean de motor de la protección, de fichero de firmas o pendientes de reinicio), accederás al listado de equipos protegidos correspondiente.

Equipos excluidos

Si haces clic en el número de equipos excluidos, podrás ver un listado de los equipos a los que no se les está aplicando protección.

Equipos sin conexión

Si haces clic en alguno de los números que se muestran bajo el epígrafe **Sin conexión**, accederás al listado de equipos protegidos que no se han conectado con los servidores de Endpoint Protection en los últimos 30 días, 7 días o 72 horas.

Equipos sin protección

Si haces clic sobre el número de equipos, accederás al listado de equipos desprotegidos.

> ***Solo podrás ver la información correspondiente a los equipos sobre los que tengas permiso. Consulta el apartado*** Tipos de permisos.

4.2 Estado de las licencias

Aquí puedes ver cuál es el número de licencias de Endpoint Protection que posees para los diferentes sistemas operativos, cuáles están en uso y cuáles están a punto de caducar y en qué fecha lo harán.

Al contrario de lo que sucede con los contadores del estado de la protección, el número de licencias contratadas que se muestra es el total, independientemente de los permisos del usuario.

Próxima caducidad

Si haces clic en el número de licencias, accederás a la ventana **Listado de licencias** desde donde podrás añadir más licencias para equipos Windows/Linux.

La caducidad de las licencias supone que tus equipos dejan de estar protegidos, por lo que es recomendable que adquieras más licencias. Para ello, contacta con tu distribuidor o comercial habitual.

Licencias contratadas

Si haces clic en el número de licencias, accederás al detalle de las mismas en la ventana **Listado de licencias**.

Licencias usadas

Si haces clic en el número de licencias, accederás al listado de equipos protegidos.

Equipos sin licencia

Los equipos sin licencia son aquellos a los que no se les está aplicando la protección debido a que no se dispone de licencias suficientes para protegerlos o a que son equipos que forman parte de un grupo sujeto a algún tipo de restricción que no se les está aplicando.

> ***Solo podrás ver los equipos sin licencia que formen parte de grupos sobre los que tengas permiso. Consulta el apartado Tipos de permisos.***

El color de las licencias contratadas, usadas y sin usar varía en función de que se estén utilizando más licencias de las contratadas y licencias de gracia (se mostrará en tonalidad rojo-gris) o se estén utilizando todas las licencias contratadas y además haya equipos sin licencia (color rojo).

Ejemplo:

Si estás utilizando más licencias de las contratadas y licencias de gracia: 

Si estás utilizando todas las licencias contratadas y además hay equipos sin licencia: 

4.3 Visualización de las licencias

En la sección **Licencias** de la ventana **Estado** se muestra el número de licencias que has contratado y cuál es su periodo de validez.

4.3.1 Listado de licencias

Para acceder al listado de licencias, haz clic en el número que indica las licencias contratadas. Si haces clic en el número de licencias usadas, accederás al listado de equipos protegidos.

Datos que se muestran en el listado de licencias:

Los datos se muestran en cuatro columnas: **Contratadas** (número total de licencias contratadas), **Tipo** (tipo de licencias), **Caducidad** y **Unidades.**

Las protecciones se representan mediante un sistema de iconos, cuyo significado podrás ver si sitúas el cursor sobre la **Leyenda**.

Los datos corresponden a las licencias para equipos con sistema operativo Windows/Linux/Android así como a las contratadas para la protección de equipos-servidores MAC. En este último caso, se especifica mediante el texto "(OS X)" en la columna **Tipo**.

A medida que las diferentes licencias vayan caducando, desaparecerán del listado.

4.3.2 ¿Cómo se gestionan las licencias caducadas o a punto de caducar?

Windows/Linux/Android

Si un mantenimiento caducara en menos de 30 días y, una vez caducado, el número de licencias consumidas superara al número de licencias contratadas que restan por consumir, podrás utilizar la opción de anulación de licencias. Para ello, haz clic en el vínculo **Gestionar la anulación de licencias** y accederás a la ventana **Seleccionar licencias a liberar**.

OS X

Si alguno de los mantenimientos de OS X está a punto de caducar ello supone que alguno de los equipos afectados pase a estar en la lista de equipos sin licencia.

Cuando la caducidad esté cerca se te mostrará una notificación y a continuación podrás gestionar la anulación de licencias. Para ello, haz clic en **Gestionar la anulación de licencias**.

4.3.3 ¿Cómo se pueden anular licencias y mover equipos a la lista de equipos sin licencia?

Windows/Linux/Android

Si eres un usuario con permiso de control total, puede anular licencias de los equipos que usted seleccione. Si opta por esta opción, los equipos afectados por la anulación de su licencia dejarán de estar protegidos y pasarán automáticamente a la lista de equipos sin licencia.

OS X

Una vez que has seleccionado **Gestionar la anulación de licencias**, puedes seleccionar los equipos OS X cuyas licencias se anularán.

Los equipos afectados por la anulación de su licencia dejarán de estar protegidos y pasarán automáticamente a la lista de equipos sin licencia.

Si deseas más información acerca del control y la gestión de licencias, consulta el apartado **Gestión de licencias**.

Cada cliente sólo puede disponer de licencias de un tipo: Endpoint Protection o Endpoint Protection Plus, que pueden ser utilizables tanto para equipos Windows/Linux/Android como para OS X.

5. Amenazas detectadas

Amenazas detectadas y su origen

Mensajes filtrados

Accesos a páginas Web

Detalle de detecciones

Análisis programados

5.1 Amenazas detectadas y origen de las amenazas

Los resultados de las detecciones realizadas se muestran en los paneles **Amenazas detectadas** y **Origen de las detecciones**, en la ventana **Estado**.

Los paneles muestran cuál es el estado de la protección que has instalado en los equipos, en función del tipo y el origen de las detecciones.

5.1.1 Detecciones en equipos con sistema operativo Linux

1. En el gráfico de detecciones por tipo, las detecciones de Linux se añaden en la categoría apropiada. En caso de no poder identificar la categoría, se añadirán al contador **Otros**.

2. En el gráfico de detecciones por origen, las detecciones de Linux se suman al contador de **Sistema archivos.**

5.1.2 Detecciones en equipos con OS X

1. En el gráfico de amenazas detectadas las detecciones de OS X se añaden en la categoría **Virus**.

2. En el gráfico de origen de las detecciones, las detecciones de OS X se suman al contador de **Sistema archivos**.

Para conocer qué detecciones se han encontrado durante un periodo de tiempo determinado, selecciona una opción dentro de la lista desplegable **Periodo.**

5.1.3 Detecciones en dispositivos con Android

En función de su origen, las amenazas se mostrarán dentro del contador de sistema de archivos, en el gráfico de origen de las amenazas.

En cuanto al gráfico de amenazas detectadas, seguirán el mismo patrón de clasificación que para los equipos Windows, tal y como se explica a continuación.

5.1.4 Detecciones en equipos Windows

Amenazas detectadas

Se mostrarán las detecciones de cada tipo de amenaza encontradas. Además, se mostrarán también datos sobre el número de bloqueos de intentos de intrusión, de dispositivos, de operaciones peligrosas y de *tracking cookies*.

En el caso de las URL, las consideradas como malware se incluyen en la categoría **Otros**, y las consideradas como phishing o fraude en la categoría **phishing**.

Origen de las amenazas

Informa sobre el origen de las detecciones.

Se incluirán las detecciones reportadas por:

- Sistema de archivos
- Correo
- Web (detección de páginas Web correspondientes a malware y/o phishing)
- Firewall
- Control de dispositivos (bloqueos de llaves USB, lectores de CD/DVD, dispositivos de imágenes y Bluetooth o accesos denegados a dichos dispositivos)
- Exchange Server (detecciones realizadas en servidores Exchange)

Si deseas ver la lista de análisis programados, haz clic en el vínculo **Análisis programados**.

Para obtener más información sobre las detecciones, haz clic en el vínculo **Detalle de detecciones**.

El listado de detecciones mostrará el detalle de las detecciones correspondientes a los últimos 7 días.

5.2 Mensajes filtrados

En el gráfico **Mensajes filtrados** se muestra la cantidad de mensajes de correo que han sido bloqueados por contener archivos adjuntos considerados sospechosos. Esta protección se aplica a los servidores Exchange.

Previamente, habrás tenido que configurar en la ventana **Filtrado de contenidos** las extensiones que deseas bloquear y autorizar (en el caso de dobles extensiones).

Para saber más, consulta el apartado Filtrado de contenidos para servidores Exchange.

5.3 Accesos a páginas Web

5.3.1 Accesos a páginas Web

Si dispones de licencias de Endpoint Protection Plus, habrás podido configurar el control de acceso a páginas Web en el apartado de configuración de los diferentes perfiles de protección.

De acuerdo con la configuración realizada, en esta ventana **Estado** podrás ver los porcentajes de acceso a páginas Web que se han producido y obtener detalles sobre ello.

Si no dispones de licencias pero quieres probar o comprar Endpoint Protection Plus, contacta con tu distribuidor o comercial habitual.

5.3.2 Resultados del control de accesos a páginas Web

Si dispones de licencias de Endpoint Protection Plus podrás ver en este panel la información correspondiente a las páginas Web a las que se ha accedido desde los diferentes equipos de tu red.

Como puedes observar, la información se presenta en forma de gráfico coloreado con los colores asignados a las diferentes categorías. Cada porción del gráfico detalla el porcentaje de accesos a la categoría en cuestión.

La configuración de estas categorías la habrás realizado previamente en la configuración del control de acceso a páginas Web.

1. Si haces clic en el gráfico, éste se ampliará.
2. Si utilizas el link **Ver detalle de accesos a páginas Web** situado en la parte inferior del panel, accederás a la ventana **Accesos a páginas Web**.

En la ventana **Accesos a páginas Web**, en primer lugar selecciona si desea que se te muestren los datos correspondientes a los últimos siete días, últimas 24 horas o último mes. Haz clic en **Aplicar**.

La información resultante se muestra en cuatro paneles:

- Top 10 de **Categorías más accedidas**
- Top 10 de **Equipos que más acceden**
- Top 10 de **Categorías más bloqueadas**
- Top 10 de **Equipos con más accesos bloqueados**

Si lo que deseas es ver el listado completo de categorías accedidas y bloqueadas o el de equipos con accesos a páginas Web, utiliza el link **Ver listado completo**.

Equipos que más acceden/con más accesos bloqueados

Si haces clic en el nombre de un equipo, se mostrarán todos los accesos que desde el equipo seleccionado se han permitido o denegado a las diferentes categorías.

Categorías más accedidas/bloqueadas

Si haces clic en el nombre de una categoría, se mostrarán los accesos que se han permitido o denegado a páginas Web de esa categoría para todos los equipos.

Puedes exportar los resultados utilizando la opción **Exportar a excel o .csv**.

5.4 Detalle de detecciones

5.4.1 Detalle de detecciones

Mediante la monitorización de detecciones, puedes realizar búsquedas en tu red informática para saber cuándo han sido amenazados los equipos, qué tipo de amenaza ha sido detectada, y qué acción ha sido puesta en marcha para bloquear el ataque.

Para acceder al detalle de detecciones, haz clic en el vínculo **Detalle de detecciones**, en la ventana **Estado**.

Utiliza el desplegable para seleccionar el criterio en base al cual quieres realizar la búsqueda:

- **Amenazas detectadas**. Al seleccionar esta opción, se mostrará el listado de todas las categorías de malware y el número total de veces que se ha detectado cada una de ellas en el periodo de tiempo seleccionado.
- **Equipos con más amenazas**. Al seleccionar esta opción, se muestran todos los equipos ordenados de mayor a menor número de detecciones.
- **Malware más detectado**. Al seleccionar esta opción, se muestra el malware más detectado en tus equipos.

En todos los casos, puedes utilizar el desplegable situado en la zona superior derecha de la ventana para que la información que se muestre en los resultados de búsqueda sea la correspondiente a las últimas 24 horas, los últimos 7 días o el último mes.

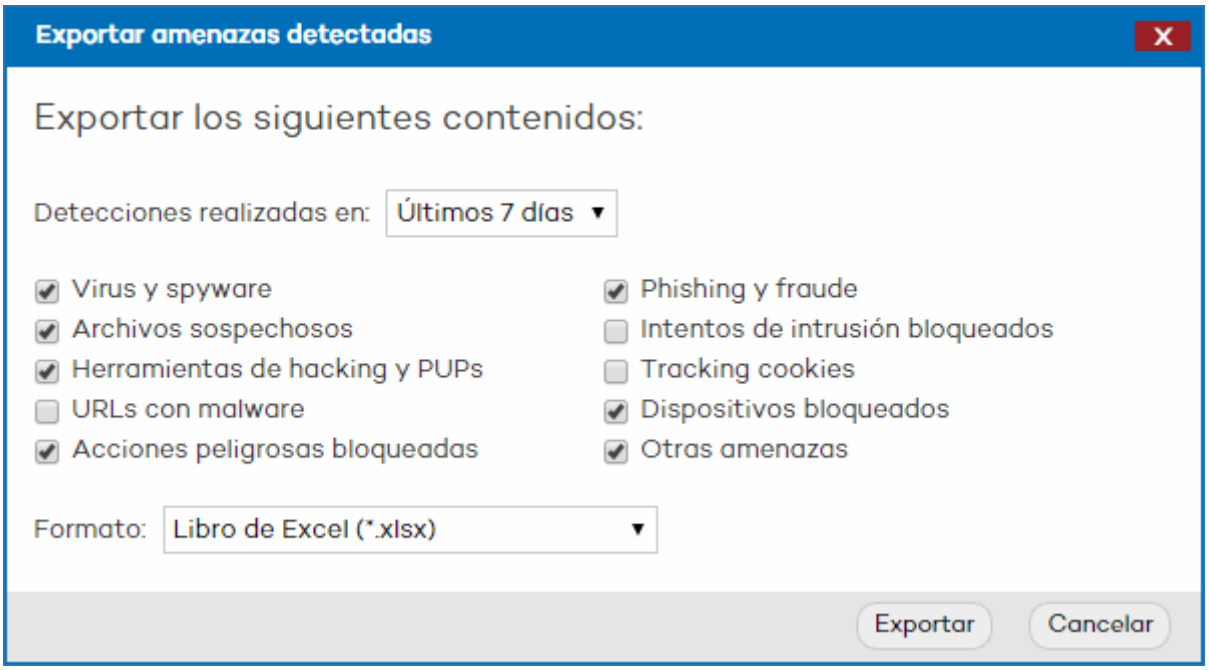
Detalle de detecciones en equipos Linux/OS X/Android

En el caso de equipos con sistema operativo Linux, OS X o dispositivos Android, los valores que se muestran en los detalles de la detección son los mismos que se muestran para la protección permanente de los equipos con sistema operativo Windows.

Exportar el listado

La lista de detecciones obtenida se puede exportar, bien en formato excel o en CSV. Para ello, haz clic en el botón **Exportar** situado en la zona superior de la ventana.

Una vez en la ventana **Exportar amenazas detectadas**, selecciona el intervalo que deseas que se refleje en el listado (últimas 24 horas, últimos 7 días, último mes) y marca la casilla correspondiente a las amenazas que deseas incluir.



Ambos formatos -excel y .csv- incluyen una cabecera que especifica la fecha y hora en que se ha emitido el archivo, un resumen de los criterios de búsqueda utilizados, y el detalle del listado, incluyendo la dirección IP origen de la infección o infecciones detectadas.

En las exportaciones, se mostrará la ruta completa del grupo (*Todos\grupo1\grupo2*)

5.4.2 Resultado de la búsqueda de amenazas detectadas

Haz clic en el icono ⊕ situado junto al nombre de la amenaza cuyos resultados deseas ver.

Las amenazas sobre las que puedes hacer búsquedas son:

- Virus y spyware
- Archivos sospechosos
- Herramientas de hacking y PUPs (programas potencialmente no deseados)
- URLs con malware
- Acciones peligrosas bloqueadas
- Phishing y fraude
- Intentos de intrusión bloqueados
- Tracking cookies
- Dispositivos bloqueados
- Otras amenazas

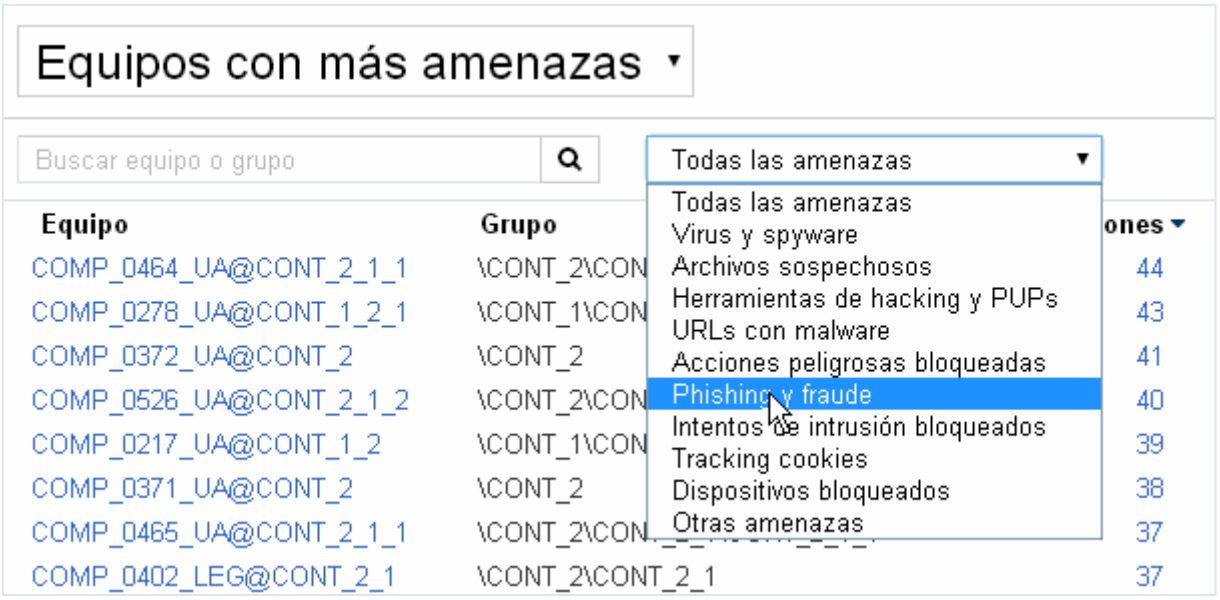
En el listado resultante, podrás ver información detallada sobre qué amenazas ha sido detectadas y en qué equipos, la acción que la protección ha llevado a cabo para bloquearlas (desinfección, envío a cuarentena,...) y la fecha de detección.

También se mostrará información sobre el lugar en el que ha sido detectada la amenaza (en el sistema de archivos, en el correo, en Exchange Server,...)

En el caso de los dispositivos bloqueados, puedes filtrar en el desplegable para seleccionar el dispositivo.

5.4.3 Resultado de la búsqueda de equipos con más amenazas

Utiliza el desplegable para seleccionar la amenaza sobre la que quieres realizar la búsqueda.



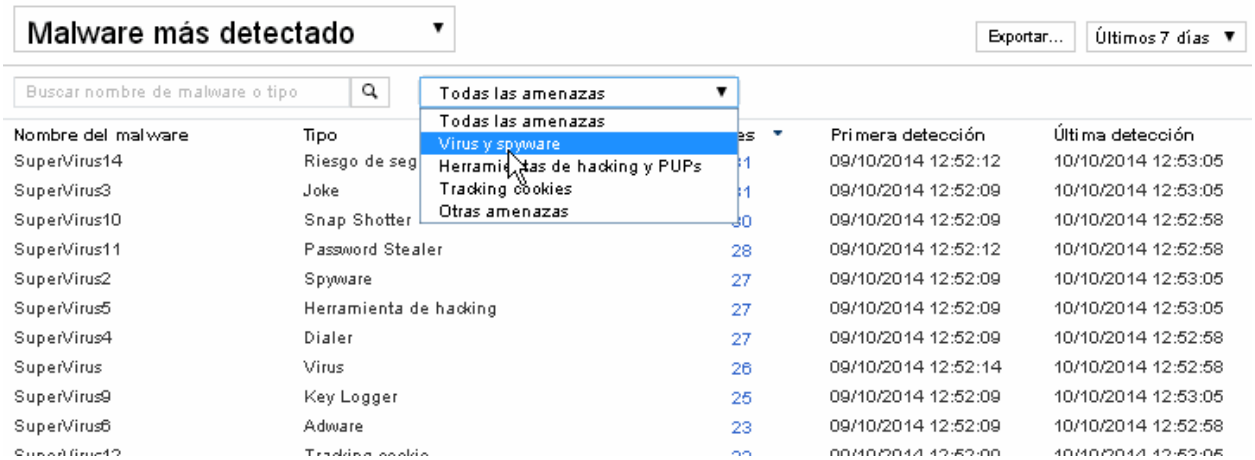
En el listado que aparece se mostrarán los equipos en los que se ha detectado la amenaza seleccionada, el grupo al que pertenecen los equipos, el número de detecciones y la fecha de la primera y última detección.

Detalle de las diferentes detecciones

Haz clic en el número de detecciones, y después en el icono ⊕ situado junto al nombre de la amenaza. Podrás ver en qué equipos ha sido detectada, la acción que la protección ha llevado a cabo para bloquearlas (desinfección, envío a cuarentena,...) y la fecha de detección.

5.4.4 Resultado de la búsqueda del malware más detectado

Utiliza el desplegable para seleccionar el malware sobre el que quieres realizar la búsqueda:



- Todas las amenazas
- Virus y spyware
- Herramientas de hacking y PUPs
- Tracking cookies
- Otras amenazas

En el listado que aparece, se mostrará el nombre y tipo del malware más detectado, el número de detecciones y la fecha de la primera y última detección.

Nombre del malware	Tipo	Detecciones	Primera detección	Última detección
SuperVirus14	Riesgo de seguridad	31	09/10/2014 12:52:12	10/10/2014 12:53:05
SuperVirus11	Password Stealer	28	09/10/2014 12:52:12	10/10/2014 12:52:58
SuperVirus2	Spyware	27	09/10/2014 12:52:09	10/10/2014 12:53:05
SuperVirus	Virus	26	09/10/2014 12:52:14	10/10/2014 12:52:58
SuperVirus6	Adware	23	09/10/2014 12:52:09	10/10/2014 12:52:58
SuperVirus8	Troyano	21	09/10/2014 12:52:09	10/10/2014 12:52:58
Super7Virus	Gusano	18	09/10/2014 12:52:12	10/10/2014 12:53:05
VirusDeRed_Spyware	Virus de red	15	09/10/2014 12:52:09	10/10/2014 12:52:58

Filas 20 1 - 8 de 8

En algunos casos podrá acceder a la información que Panda Security ofrece en su página Web sobre determinadas amenazas. Para ello, haz clic en el nombre de la amenaza detectada.

Las detecciones reportadas por los análisis en background de la protección Exchange (Exchange 2007 / Exchange 2010), se muestran en el detalle de detección como "Notificado por: Análisis inteligente de buzones".

En los servidores Exchange 2003 no se puede diferenciar que se ha detectado en background y aparecen igual que las detecciones de buzones ("Notificado por: Protección Exchange Server ").

5.5 Análisis programados

5.5.1 Ver la lista de análisis programados

Si deseas ver la lista de análisis programados, en la ventana **Estado** haz clic en el vínculo Análisis programados, situado en la zona inferior de la ventana.

En la ventana **Análisis programados** puedes ver en todo momento qué tareas de análisis programados se han creado para los diferentes perfiles de configuración y acceder a los resultados de dichas tareas.

La información se estructura en cuatro columnas:

- **Nombre**. Muestra el nombre de la tarea de análisis programado. Si haces clic sobre el nombre de la tarea, podrás acceder a la ventana de resultados del análisis programado.

- **Perfil.** Indica el perfil de configuración al que pertenece el análisis programado.
- **Periodicidad**. Detalla el tipo de análisis (periódico, inmediato, programado).
- **Estado tarea**. En esta columna se utilizan una serie de iconos para indicar el estado de la tarea de análisis. Puedes ver la lista de iconos situando el cursor sobre la opción **Leyenda.**

5.5.2 Resultados de las tareas de análisis programados

En esta ventana se muestra un listado de los equipos que se encuentran involucrados en tareas de análisis, salvo que la tarea se encuentre en situación de *En espera*.

Si se trata de un análisis de tipo periódico, podrás elegir entre las opciones **Ver resultados del último análisis** o **Ver resultados de análisis anteriores**.

Los datos se muestran en seis columnas:

- **Equipo.** Indica cuál es el equipo involucrado en la tarea. Este equipo aparecerá con su nombre o con su dirección IP, según lo que hayas configurado en las preferencias.
- **Grupo.** El grupo al que pertenece el equipo.
- **Estado.** En esta columna se utilizan una serie de iconos para indicar el estado del equipo involucrado en la tarea. Puedes ver la lista de iconos situando el cursor sobre la opción **Leyenda**.
- **Detecciones.** Se muestra el número de detecciones realizadas durante la tarea. Haz clic sobre el número y accederás al listado de detecciones.
- **Fecha de comienzo.** Indica la fecha y hora de comienzo de la tarea.
- **Fecha de fin.** Indica la fecha y hora de finalización de la tarea.

Si deseas consultar la configuración de los análisis programados para el perfil de protección al que pertenece el equipo, haz clic en el vínculo **Ver configuración**.

Equipos con sistema operativo Linux

En los equipos con sistema operativo Linux, la protección permite hacer análisis bajo demanda y programados. A la hora de seleccionar los elementos a analizar, el comportamiento de la protección es el siguiente:

- **Todo el PC.** Analizará todo el equipo.
- **Discos duros.** Analizará todos los discos duros.

- **Correo.** No analizará nada dado que en Linux no se analizan carpetas de correo.
- **Otros elementos.** Permite seleccionar rutas en formato Linux.

Ejemplo: /root/documents

Para saber más acerca de los análisis programados, consulta la sección Opciones avanzadas de análisis.

Dispositivos Android

En los dispositivos Android, se pueden programar análisis de tres tipos: inmediato, programado y periódico.

Para saber más sobre estos análisis, consulta el capítulo **Configuración de la protección para dispositivos Android**.

6. Gestión de licencias

Alertas relacionadas con las licencias

Liberar licencias

Añadir licencias mediante código de activación

6.1 Alertas relacionadas con las licencias

Puedes adquirir licencias de Endpoint Protection para Windows/Linux/Android o de Endpoint Protection para OS X. De acuerdo con tus necesidades, podrás instalar las protecciones en los equipos, desinstalarlas, eliminar equipos de la lista de equipos protegidos, añadir equipos a dicha lista, etc.

La utilización que hagas de tus licencias tiene su reflejo en el número de licencias disponibles.

Las licencias para Endpoint Protection para Windows/Linux/Android pueden ser utilizadas indistintamente en equipos con sistema operativo Windows, Linux o Android.

Si deseas proteger tus equipos y servidores OS X, deberás adquirir licencias específicas para ello, ya que son independientes de las que se adquieren para equipos con sistema operativo Linux/Windows/Android.

6.1.1 Actualización del número de licencias

Si tú:

- **Instalas la protección en un equipo** ▶ Del total de licencias disponibles se restará una licencia de Endpoint Protection para Windows/Linux/Android o de Endpoint Protection para OS X, en función del sistema operativo en el que instales la protección.
- **Eliminas un equipo de la lista de equipos protegidos** ▶ Al total de licencias disponibles se sumará una licencia de Endpoint Protection para Windows/Linux/Android o de Endpoint Protection para OS X, en función del sistema operativo del equipo eliminado.
- **Disminuyes en X unidades el número de licencias contratadas** ▶ En la ventana Equipos se mostrarán como equipos sin licencia tantos equipos Windows/Linux/Android u OS X como licencias del sistema operativo en cuestión hayan disminuido.

6.1.2 Alerta por fecha de caducidad de licencias contratadas

En el área de notificaciones aparecerán diferentes avisos en función de la proximidad de la fecha de caducidad (menos de 60 días); también si se ha superado dicha fecha o si las caducidades dejarían menos licencias disponibles de las usadas actualmente.

Estas notificaciones son independientes en función del sistema operativo que tengan los equipos afectados por la caducidad de la licencia, es decir, se mostrarán por una parte las notificaciones de caducidad de licencias Endpoint Protection para Windows/Linux/Android, y, por otra, de las de Endpoint Protection para OS X.

En ambos casos podrás renovar la licencia poniéndote en contacto con tu distribuidor habitual o comercial. Endpoint Protection te lo recordará mediante un mensaje en la ventana **Estado**. Una vez concluido el plazo de 60 días, dispondrás de otros 15 días *de gracia* para realizar la renovación. Superado este tiempo, la renovación no será posible.

6.1.3 Equipos excluidos

Si excluyes un equipo, éste pasará a formar parte de la lista de equipos excluidos en la ventana Equipos y no se mostrará información ni alertas referentes a ellos en ningún otro lugar de la consola.

6.1.4 Equipos sin licencia

Si intentas instalar en un equipo la protección cuando se ha superado el número de instalaciones permitidas o cuando la licencia ha caducado, el equipo se incluirá en la lista de equipos sin licencia de la ventana **Equipos**.

La inclusión automática en esta lista también se produce al superar las restricciones impuestas a un grupo, restricciones que puedes habilitar en la ventana **Preferencias** y configurar en **Configuración** / **Editar grupo**.

La inclusión de un equipo en la lista de equipos sin licencia implica que dicho equipo no se actualiza y que la información procedente de él no es tenida en cuenta a ningún efecto de las estadísticas, informes y análisis realizados por Endpoint Protection. Sin embargo, la licencia del equipo no se sumará al total de licencias consumidas sino que se restará del mismo.

Consulta el apartado Monitorización de los equipos.

6.2 Liberar licencias

Si dispones de varios mantenimientos -ya sean de Windows, Linux, Android u OS X- y esté próxima alguna fecha de caducidad Endpoint Protection te lo indicará mediante un un aviso en el área de notificaciones de la ventana Estado.

En el aviso se indicará la fecha de caducidad de licencias más próxima en el tiempo, el número de licencias que es necesario anular y la advertencia de, que una vez transcurrida la fecha de caducidad, los equipos afectados por la anulación se enviarán automáticamente a la lista de equipos sin licencia.

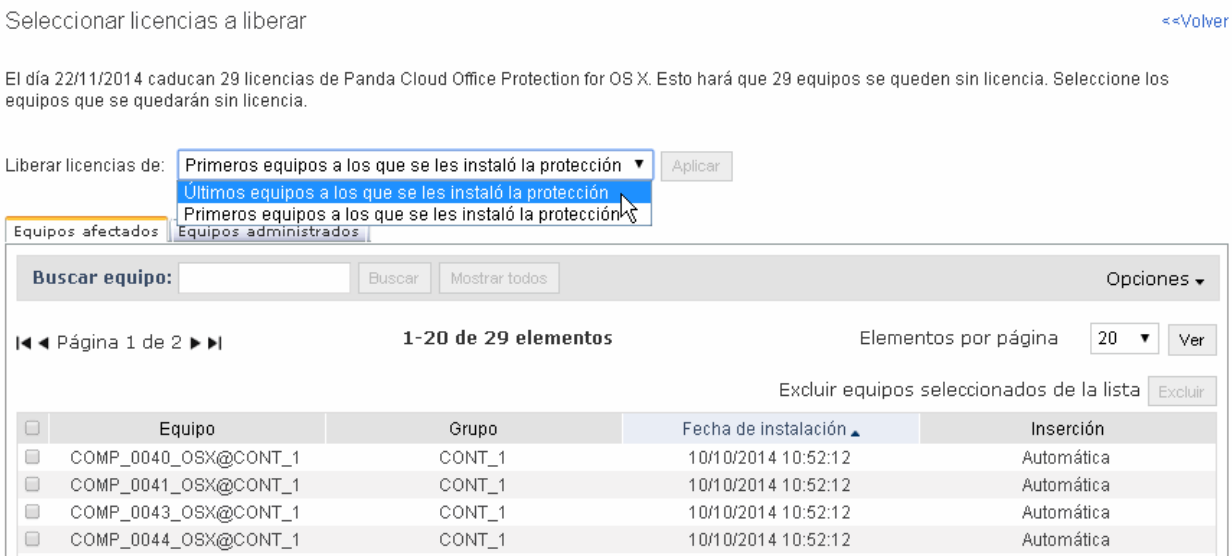
Mediante la liberación de licencias, podrás elegir qué equipos quedarán desprotegidos a partir de la fecha de caducidad que se muestra en el aviso.

Selección de las licencias

1. Haz clic en el vínculo **Seleccionar licencias a liberar** que aparece en el aviso.

2. En el desplegable **Liberar licencias de** selecciona los equipos que se quedarán sin licencia. Para ello, puedes elegir entre anular el número de licencias que necesitas de entre los primeros equipos a los que se instaló la protección o de entre los últimos.

3. Haz clic en el botón **Aplicar**. Se mostrarán en el listado tantos equipos como licencias sea necesario liberar.



6.2.1 Equipos afectados y equipos administrados

En la ventana **Seleccionar** licencias a liberar, los equipos se muestran en dos pestañas: equipos afectados y equipos administrados.

Equipos afectados

Esta es la pestaña por defecto, en la que se muestra la lista de equipos cuyas licencias se anularán y que, por tanto, dejarán de estar administrados.

En caso de que las licencias que vayan a caducar sean de Endpoint Protection para Windows/Linux, sólo se mostrarán equipos con este sistema operativo. Si las licencias próximas a caducar fueran de Endpoint Protection para OS X, se mostraran los equipos con dicho sistema operativo.

Esta pestaña distribuye la información en cuatro columnas: **Equipo**, **Grupo**, **Fecha de instalación** e **Inserción**. Esta última columna mostrará el término **Automático** si el equipo proviene de la selección que has hecho en el desplegable **Anular licencias de**, o **Manual** si el equipo proviene de la pestaña **Equipos administrados**.

Para excluir un equipo de la lista de equipos cuyas licencias serán anuladas, marca la casilla correspondiente y haz clic en **Excluir**.

Mediante el desplegable **Opciones**, puedes refinar la búsqueda de equipos, especificando periodos de tiempo en los que se instaló protección en los equipos y obtener así listados diversos.

Equipos administrados

Esta pestaña muestra los equipos que administras. Si deseas añadir alguno de ellos a la lista de equipos afectados, marca la casilla correspondiente, haz clic en **Agregar** y el equipo pasará a la lista de equipos afectados, donde mostrará en la columna **Inserción** el término **Manual**.

En caso de que las licencias que vayan a caducar sean de Endpoint Protection para Windows/Linux, sólo se mostrarán equipos con este sistema operativo. Si las licencias próximas a caducar fueran de Endpoint Protection para OS X, se mostraran los equipos con dicho sistema operativo.

Finalmente, cuando haya transcurrido la fecha de caducidad, desde la lista de equipos afectados se enviarán a la lista de equipos sin licencia tantos equipos como licencias haya sido necesario anular.

6.3 Añadir licencias mediante código de activación

Mediante esta funcionalidad, será tú quien decida cuándo ampliar tus licencias de Endpoint Protection para Windows/Linux/Android.

Desde tu consola Web podrás activar el servicio de manera sencilla y rápida, utilizando el código de activación que te proporcionó Panda Security o tu distribuidor en el momento de la compra.

Sigue los siguientes pasos:

1. En la ventana **Estado** haga clic sobre el número de licencias contratadas**.** Se mostrará la ventana **Listado de licencias**.

2. Haz clic en el vínculo **Añadir más licencias**.
3. Introduce el código de activación.
4. Haz clic en **Aceptar**.

El proceso de añadir licencias no es inmediato, por lo que puede que transcurra un tiempo hasta que las licencias añadidas se muestren en la sección Licencias de la ventana Estado.

En caso de error, consulta el apartado Errores posibles al añadir licencias.

6.3.1 Errores posibles al añadir licencias para equipos Windows/Linux/Android

Al introducir el código de activación, pueden aparecer los siguientes errores:

- *El código de activación introducido no es válido / no existe*. Asegúrate de haber introducido correctamente todos los dígitos.
- *El código de activación introducido ya está en uso*. Se trata de un código de activación que ya ha sido usado. En este caso, ponte en contacto con tu distribuidor o comercial habitual para poder adquirir un código nuevo.
- *No se puede realizar la operación*. Es posible que las características de los servicios/licencias que has contratado no permitan la utilización de la funcionalidad de ampliación de licencias.

  Este error también se reportará cuando un cliente de Endpoint Protection intente añadir licencias introduciendo un código de activación de Endpoint Protection Plus en la consola cliente y viceversa.

6.3.2 Otros errores

Una vez introducido con éxito el código de activación, puede darse el siguiente error:

- *No se ha podido dar de alta la solicitud*. Este error tiene lugar cuando el proceso falla por un motivo desconocido. Por favor, vuelve a intentarlo y si no consigues realizar la activación, contacta con el soporte técnico de Panda Security.

7. Gestión de cuentas

Introducción

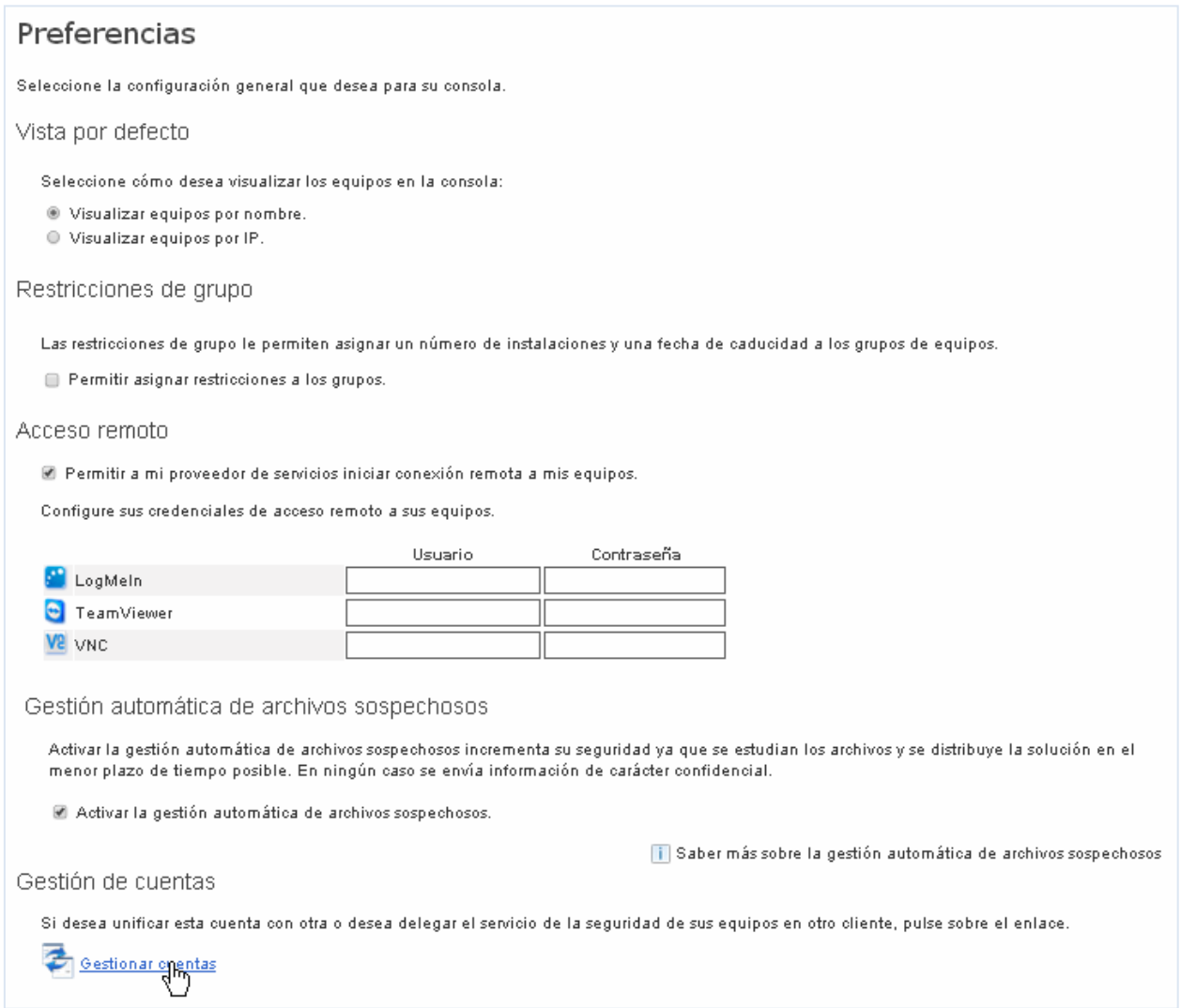
Delegar la gestión de una cuenta

Unificar cuentas

7.1 Introducción a la gestión de cuentas

Si eres un usuario con permisos de control total, puedes acceder a las funcionalidades de gestión de cuentas que Endpoint Protection pone a tu disposición: delegar la gestión de una cuenta y unificar cuentas.

Ambas opciones están accesibles en la ventana **Gestión de cuentas.** Puedes acceder a ella desde la ventana **Preferencias** > Haz clic en el vínculo **Gestionar cuentas.**



7.1.1 Delegar la gestión de una cuenta

Al utilizar esta opción, podrás permitir que la seguridad de tus equipos sea gestionada por un proveedor de servicio (partner) o bien podrás modificar el proveedor al que deseas encomendar la gestión de tu seguridad.

Para ver más información sobre esta opción, consulta el apartado Delegar la gestión de una cuenta.

7.1.2 Unificar cuentas

Cuando existen varias cuentas de cliente, se pueden unificar en una y posibilitar así la gestión centralizada de la seguridad de los equipos.

Para ver más información sobre esta opción, consulta el apartado Unificar cuentas.

7.2 Delegar la gestión de una cuenta

7.2.1 Delegar la gestión de una cuenta

Si deseas delegar la gestión de la seguridad de tus equipos en un proveedor de servicio o cambiar el proveedor que gestione tu seguridad, puedes hacerlo mediante la funcionalidad **Delegar servicio**. El proveedor en quien delegues tendrá acceso a tu consola.

Para delegar la gestión de tu cuenta en un partner, necesitarás el identificador de Panda Security de dicho partner.

Sigue los siguientes pasos:

1. Haz clic en **Gestionar cuentas** de la ventana **Preferencias**. Se mostrará la ventana **Gestión de cuentas**.

2. En el apartado **Delegar seguridad a su proveedor de servicio** introduce el identificador del proveedor que gestionará la seguridad de los equipos.

Para confirmar que deseas proceder a la delegación, haz clic en **Delegar**.

El proceso de delegación de gestión no es inmediato, por lo que puede que transcurra un tiempo hasta que tus datos sean accesibles para el proveedor especificado.

En caso de error, consulta el apartado Errores posibles al delegar la gestión de una cuenta.

7.2.2 Errores posibles al delegar la gestión de una cuenta

Al tratar de activar la funcionalidad de delegación del servicio, pueden aparecer los siguientes errores:

- *El identificador introducido no es válido*. Por favor, revísalo e introdúcelo de nuevo. Por favor, asegúrate de haber introducido correctamente todos los dígitos del identificador del partner.

- *No dispone de licencias para realizar esta operación*. Contacta con tu distribuidor o comercial habitual para renovarlas. Si tus licencias han caducado, no podrás acceder a la funcionalidad de delegación de servicio. Por favor, contacta con tu distribuidor o comercial habitual para renovar tus licencias.

- *No puede realizar esta operación*. Consulta con tu distribuidor o comercial habitual. Es posible que las características de los servicios/licencias que contrataste no permitan la utilización de la funcionalidad de delegación de servicio. Por favor, consulta a tu distribuidor o comercial habitual.

7.2.3 Otros errores

- *Ha ocurrido un error y no se ha podido dar de alta la solicitud*. Por favor, inténtalo de nuevo. Este error tiene lugar cuando el proceso falla por un motivo desconocido. Por favor, vuelve a intentarlo y si no consigues realizar la activación del servicio, contacta con el soporte técnico de Panda Security.

7.3 Unificar cuentas

7.3.1 ¿Qué es la unificación de cuentas?

Si posees varias cuentas de cliente y deseas unificarlas para gestionarlas de manera centralizada, puedes hacerlo mediante la unificación de cuentas. De esta forma, podrás gestionar todas tus cuentas desde una sola consola Web.

> ⚠ ***Antes de proceder a la unificación de cuentas, es importante comprender cuáles son las consecuencias de ello. Por favor, consulta el apartado*** ***Consecuencias de la unificación de cuentas******.***

¿Cuándo NO es posible unificar cuentas?

1. Cuando los clientes están utilizando versiones diferentes de la protección.

2. Cuando los clientes disponen de productos distintos:

    - No es posible unificar cuentas cuando el cliente de la cuenta origen dispone de licencias de Systems Management.

    - No se pueden unificar cuentas si uno de los clientes tiene licencias de Endpoint Protection y el otro tiene licencias de Endpoint Protection Plus.

3. Cuando las cuentas que se desean unificar pertenecen a clientes que dependen de partners diferentes.

7.3.2 ¿Cómo se realiza la unificación de cuentas?

Básicamente el proceso consiste en traspasar los datos de una cuenta-origen (cuenta A) a una cuenta-destino (cuenta B). Esta cuenta-destino ha de encontrarse activa.

Para unificar las cuentas:

1. Accede a la consola Web de la cuenta-origen (cuenta A), la que será dada de baja.

2. Haz clic en **Gestionar cuentas** en la ventana **Preferencias**. Se mostrará la ventana **Gestión de cuentas**.

3. Selecciona **Unificar**.

4. Introduce el Login Email de un usuario que disponga de permiso de control total sobre la cuenta a la que desea traspasar los datos y el número de cliente (identificador) que le fue enviado en el mensaje de bienvenida.

Si estás seguro de que deseas unificar las cuentas, haz clic en **Unificar**.

> ***El proceso de traspaso de datos no es inmediato, por lo que puede que transcurra un tiempo hasta que puedas comprobarlo en la consola Web de tu cuenta B.***

En caso de error, consulta el apartado Errores posibles en el proceso de unificación de cuentas.

7.3.3 ¿Qué información se traslada al unificar cuentas?

La unificación de cuentas implica el traslado de información sobre los equipos gestionados desde la cuenta A

1. **Todos los mantenimientos activos y no caducados**, es decir, la información sobre las licencias activas, sus fechas de inicio y caducidad, tipo de licencia, etc.

2. **Perfiles de configuración.** Todos los perfiles de configuración de las protecciones de la cuenta-origen. En el caso de que en la cuenta-destino exista un perfil con el mismo nombre (por ejemplo, *Perfil Comercial*), el perfil procedente de la cuenta-origen será "renombrado" mediante un sufijo numérico (*Perfil Comercial-1*).

> ***El perfil por defecto -perfil Default- de la cuenta-origen se traspasará a la cuenta-destino, pero será considerado como un perfil más y perderá la marca de perfil por defecto.***

3. **Grupos de equipos.** Todos los grupos de equipos. En el caso de grupos de igual nombre, el funcionamiento será similar al aplicado para los perfiles en el punto anterior.

> ***El grupo por defecto -grupo Default- de la cuenta-origen se traspasará a la cuenta-destino, pero será considerado como un grupo más y perderá la marca de grupo por defecto.***

4. **Información de las protecciones** activas y de las correspondientes a equipos excluidos o sin licencia.

5. **Informes y estadísticas** de detección.

6. **Todos los elementos en cuarentena**, incluyendo los elementos excluidos de cuarentena y los restaurados.

7. Los **usuarios** de la consola Web (con sus correspondientes permisos), excepto el usuario por defecto *-Default-*.

7.3.4 Consecuencias de la unificación de cuentas

Antes de proceder a la unificación de cuentas, es **MUY IMPORTANTE** que tengas en cuenta las consecuencias que ello conlleva:

1. Los **servicios asociados** a la cuenta A **dejarán de estar activos** y la cuenta será eliminada. Obviamente, el acceso a la consola Web de la cuenta A será denegado.

2. En la consola Web de la cuenta B, se mostrarán los datos e informaciones sobre los equipos gestionados desde la cuenta A. Para comprobarlo, tan sólo tienes que acceder a la consola Web de la cuenta B.

3. Se producirá la **reasignación automática** de las protecciones instaladas en los equipos gestionados desde la cuenta A, pasando a ser gestionados desde la cuenta B. **No será necesario reinstalar las protecciones**.

El proceso de traspaso de datos no es inmediato, por lo que puede que transcurra un tiempo hasta que puedas comprobarlo en la consola Web de su cuenta B.

En caso de error, consulta el apartado Errores posibles en el proceso de unificación de cuentas.

7.3.5 Errores posibles en el proceso de unificación de cuentas

Al tratar de acceder al formulario **Gestión de cuentas**, pueden producirse los siguientes errores:

- *El Login Email y/o identificador (número de cliente) no son correctos.* Por favor, asegúrate de haber introducido correctamente todos los caracteres.
- *No se puede realizar la operación*. Es posible que las características de los servicios/licencias que has contratado no permitan la utilización de la funcionalidad de unificación de cuentas. Por favor, consulta con tu distribuidor o comercial habitual.
- *No dispone de licencias para realizar esta operación*. Si tus licencias han caducado, no podrás acceder a la funcionalidad de unificación de cuentas. Por favor, contacta con tu distribuidor o comercial habitual para renovar tus licencias.
- *La cuenta especificada tiene una fusión en curso*. En el caso de que la cuenta B (cuenta-destino) que has especificado esté inmersa en otro proceso de unificación, será necesario aguardar a que dicho proceso termine para poder comenzar el tuyo.
- *La cuenta con la que ha iniciado sesión supera el número permitido de equipos*. El proceso de unificación de cuentas sólo es posible si la cuenta A (cuenta-origen) tiene menos de 10.000 equipos asociados.
- *Las cuentas implicadas en la unificación pertenecen a versiones diferentes de* Endpoint Protection. Para que la unificación de las cuentas A y B se lleve a cabo de manera correcta, es necesario que ambas pertenezcan a la misma versión de Endpoint Protection. Es improbable que las cuentas pertenezcan a diferentes versiones, salvo en situaciones de actualización de versión.
- *No se ha podido dar de alta la solicitud*. Cuando haya fallado el proceso por un motivo desconocido, por favor, vuelve a intentarlo y si no consigues realizar la unificación de cuentas, contacta con el soporte técnico de Panda Security.

8. Creación y gestión de usuarios

Crear usuarios

Modificar los datos del usuario

8.1 Crear usuarios

Si la opción por defecto no se ajusta a las necesidades de protección de tu red informática, puedes optar por crear nuevos usuarios y asignarles diferentes tipos de permisos, en función de lo que desees que gestione cada usuario.

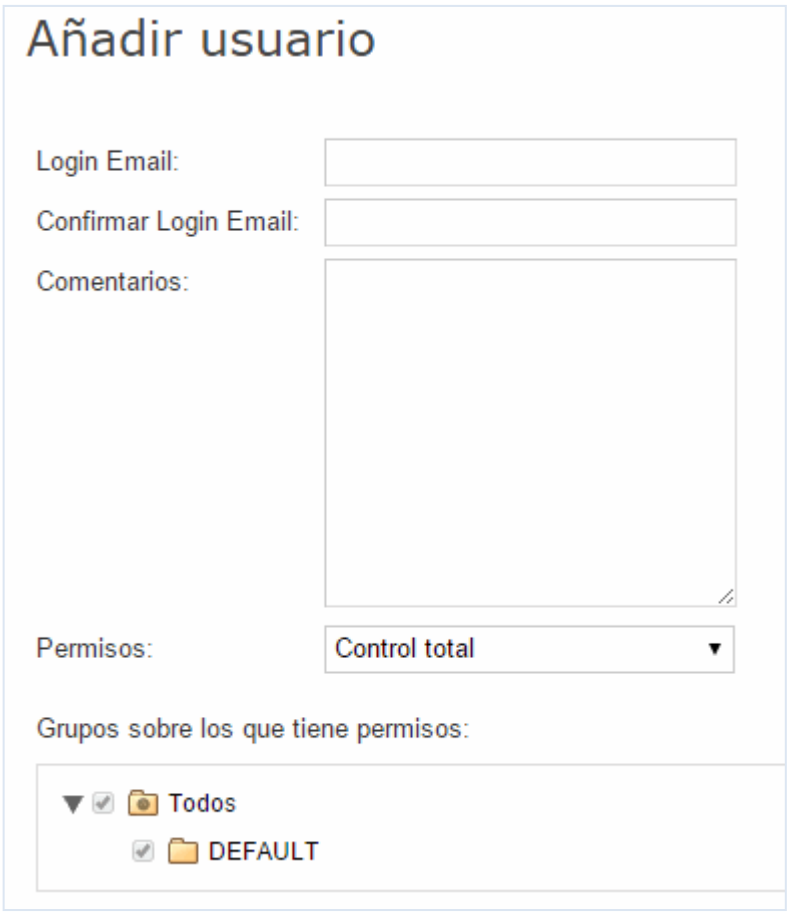
En la ventana principal de la consola Web, haz clic en **Usuarios**.

La ventana **Usuarios** distribuye la información en tres columnas: **Login Email**, **Nombre** y **Permisos**. A medida que vayas creando usuarios, éstos aparecerán en el listado, junto al tipo de permisos que les hayas otorgado.

Para crear un usuario:

1. En la ventana Usuarios, haz clic en **Añadir usuario.**

2. Introduce el Login **Email** y confírmalo.



3. Puedes añadir información adicional si lo deseas, utilizando para ello la caja de texto **Comentarios**.

4. Selecciona el permiso que deseas asignar al usuario. Por favor, para más información consulta el apartado Tipos de permisos.

5. En **Grupos,** selecciona el grupo/subgrupo o grupos/subgrupos sobre los que el usuario administrador y de monitorización podrá actuar, de acuerdo con el permiso que le hayas asignado. El usuario con permiso de control total podrá actuar sobre todos los grupos.

6. Haz clic en **Añadir**. A continuación se mostrará un mensaje informándote del envío de un correo electrónico a la dirección que has especificado al crear el usuario.

7. Una vez creado el usuario, se mostrará en el listado de la ventana **Usuarios**.

8.2 Modificar los datos del usuario

En la ventana Usuarios, si haces clic en la dirección de correo electrónico del usuario, accederás a la ventana de edición de datos.

En esta ventana podrás modificar los comentarios, el permiso y el grupo al que pertenece el usuario pero no el Login Email ni el nombre de usuario.

En el caso del usuario por defecto, solo se podrá modificar el campo Comentarios.

Si creas un usuario administrador con permiso sobre un grupo (es decir, un usuario con permiso sobre el grupo y todos sus subgrupos) y después añades un nuevo subgrupo, el usuario tendrá permiso automáticamente sobre dicho subgrupo.

Si creas un usuario administrador con permiso sobre algunos de los subgrupos de un grupo, y después se añade un nuevo subgrupo, el usuario NO tendrá permiso automáticamente sobre dicho subgrupo.

8.2.1 Modificar el nombre del usuario

Si lo que deseas es cambiar el nombre de un usuario, es necesario acceder a la consola Panda Cloud con las credenciales de ese usuario y hacer clic en el nombre del usuario. A continuación, selecciona **Modificar cuenta.**

Esta opción de modificar cuenta en la consola de Panda Cloud solo estará disponible siempre y cuando hayas activado su Cuenta Panda con anterioridad.

Accederás a la ventana de gestión de su Cuenta Panda, donde podrás modificar los datos del usuario y cambiar su contraseña si lo deseas. A continuación, haz clic en **Actualizar**.

Automáticamente, ambas consolas Web (Panda Cloud y Endpoint Protection) mostrarán el nuevo nombre del usuario.

8.2.2 Borrar un usuario

Si deseas eliminar un usuario, puedes hacerlo desde la ventana **Usuarios**.

Selecciona en el listado el usuario que deseas borrar, marca la casilla correspondiente que está situada junto al Login Email del usuario y, a continuación, haz clic en el botón **Borrar**.

9. Creación y gestión de grupos

Crear grupos

Mover equipos a un grupo

Integrar un equipo en un grupo durante la instalación

Añadir o eliminar grupos

9.1 Creación de grupos

Endpoint Protection te permite reunir en un grupo una serie de equipos y aplicar a todo el grupo el mismo perfil de protección.

9.1.1 Tipos de grupo

Grupo manual

Estos grupos se caracterizan porque los equipos que los forman han sido integrados en el grupo en el momento de la instalación de la protección en ellos o, una vez instalada la protección, los equipos han sido asignados al grupo utilizando la opción **Mover** disponible en la ventana **Equipos**.

Consulta el apartado de esta guía titulado Mover equipos a un grupo.

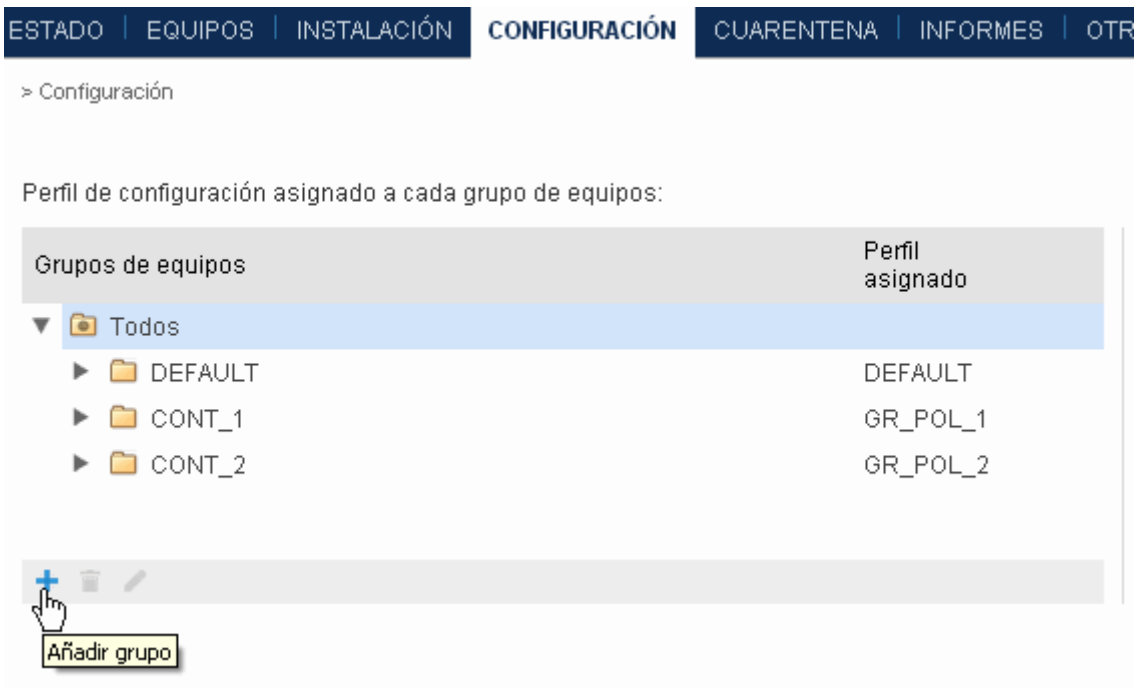
Grupo automático por direcciones IP

Los equipos que se mueven a este grupo se integrarán automáticamente en los subgrupos que indique el administrador en función de sus direcciones IP.

> ***Por favor, ten en cuenta que una vez creado el grupo no podrás cambiar el tipo de grupo que le has asignado.***

9.1.2 Crear un grupo manual

1. Haz clic en la pestaña **Configuración**.
2. A continuación haz clic en el icono 



3. Introduce el nombre del grupo y selecciona el perfil de protección que deseas asignar al grupo añadido. Recuerda que no es posible crear grupos cuyo nombre coincida con el de otro grupo del mismo nivel.

4. Tipo de grupo: selecciona **Manual**.

5. Haz clic en **Añadir**. El grupo creado se añadirá en el árbol de grupos en la ventana **Configuración** y también estará visible en el árbol de grupos de la ventana **Equipos**.

Para editar el grupo, selecciónalo y haz clic en el icono  . Podrás asignar el perfil que desees al grupo que acabas de crear.

9.1.3 Crear un grupo automático por direcciones IP

La creación de grupos automáticos por direcciones IP solo es posible cuando las restricciones de grupo de la ventana Preferencias están desactivadas.

1. El proceso de creación para estos grupos es el mismo que para los manuales pero seleccionando **Automático por direcciones IP** en **Tipo de grupo**.

2. Haz clic en **Añadir**. A continuación se mostrará la ventana de edición de grupo automático por IP. Desde esta ventana podrás configurar las reglas automáticas para el grupo que acabas de crear.

A la hora de establecer las reglas automáticas para el grupo, puedes importarlas si las tienes almacenadas en un archivo .csv o puedes configurarlas manualmente.

Importación desde el archivo .csv

1. Haz clic en **Importar.**

2. Introduce el nombre del archivo o búscalo mediante el botón **Seleccionar**.

3. Haz clic en **Aceptar**. Automáticamente se creará la estructura correspondiente en función de las direcciones IP asignadas a los equipos.

Formato del archivo .csv que se desea importar

El archivo .csv debe mostrar los datos de la forma siguiente:

En cada línea se podrán mostrar de una a tres cadenas de datos separadas por tabulador, en el siguiente orden:

1. **Ruta del grupo** a crear (desde el origen de la importación), por ejemplo: \Justicia, palacio\sala1

2. **Rango de IP**, con dos posibilidades: IP-IP o IP-máscara (este campo es opcional)

3. **Perfil** (este campo es opcional)

En el caso de no especificar rango de IP pero sí perfil, habrá que utilizar **doble tabulador** entre los dos campos visibles (ruta del grupo y perfil):

\PalacioJusticia PJusticia

Otros ejemplos:

\Hospital\Urgencias\Ambu1 10.10.10.10-10.10.10.19

\Hospital\Urgencias

\Hospital\Urgencias\Ambu2 10.10.10.20-10.10.10.29 PAmbulancia

\Hospital\AmbulatorioAreilza 10.10.20.10/22 PerfilAmbulatorio

\Justicia, Palacio\Segunda Instacia 10.10.50.10/12 Justicia 2

Si al importar grupos mediante un archivo .csv la información de alguna de las líneas del fichero no es correcta, se mostrará un error especificando la línea y cadena cuyo formato no es válido. En caso de error en al menos una de las líneas ningún grupo del archivo .csv será importado.

Una vez se hayan importado satisfactoriamente grupos mediante un archivo .csv dentro de un grupo automático por IP, ya no será posible volver a repetir esta acción para ese mismo grupo.

Configuración manual de las reglas del grupo

1. Haz clic en el icono  .
2. Selecciona el perfil que deseas asignar al grupo.
3. Introduce las direcciones IP o rangos de IP correspondientes de los equipos.
4. Haz clic en **Aceptar**.

9.2 Mover equipos a un grupo

Un equipo o grupo de equipos siempre se puede mover a cualquier grupo, ya sea éste manual o automático por direcciones IP.

En la ventana de detalles de equipo podrás ver información sobre la IP del equipo, el grupo al que fue asignado el equipo al instalar la protección y el grupo al que ha sido movido posteriormente.

Para mover equipos a un grupo:

1. En la ventana **Equipos**, dentro de la pestaña **Protegidos**, selecciona en el listado el/los equipos que deseas asignar.
2. Haz clic en el botón **Mover**.
3. En la ventana **Mover equipos** selecciona el grupo/subgrupo en el que deseass incluir el/los equipos.
4. Haz clic en el botón **Mover**.

La asignación de equipos no es posible realizarla si tu permiso es de monitorización. Para el resto de permisos, visita el apartado Tipos de permisos de esta guía.

En caso de intentar mover equipos a un grupo que haya alcanzado su número máximo de instalaciones, recibirás un mensaje advirtiendo de la imposibilidad de realizar la acción.

9.3 Integrar un equipo en un grupo durante la instalación

Al iniciar el proceso de instalación de la protección en un equipo mediante la descarga del instalador, hay que seleccionar el grupo en el que se integrará el equipo una vez terminada la instalación.

Los grupos pueden ser manuales o automáticos por direcciones IP y dentro de ellos se pueden crear subgrupos. En el caso de los grupos/subgrupos automáticos, los equipos han de cumplir con unas reglas en función de sus direcciones IP. Estas reglas se configuran al crear el grupo/subgrupo.

Si, con posterioridad, se descarga el instalador de la protección para otro equipo ajeno a estos grupos e indicamos que el equipo debe integrarse en alguno de ellos, la integración del equipo en el grupo/subgrupo seleccionado será diferente si se trata de un grupo manual o automático por direcciones IP.

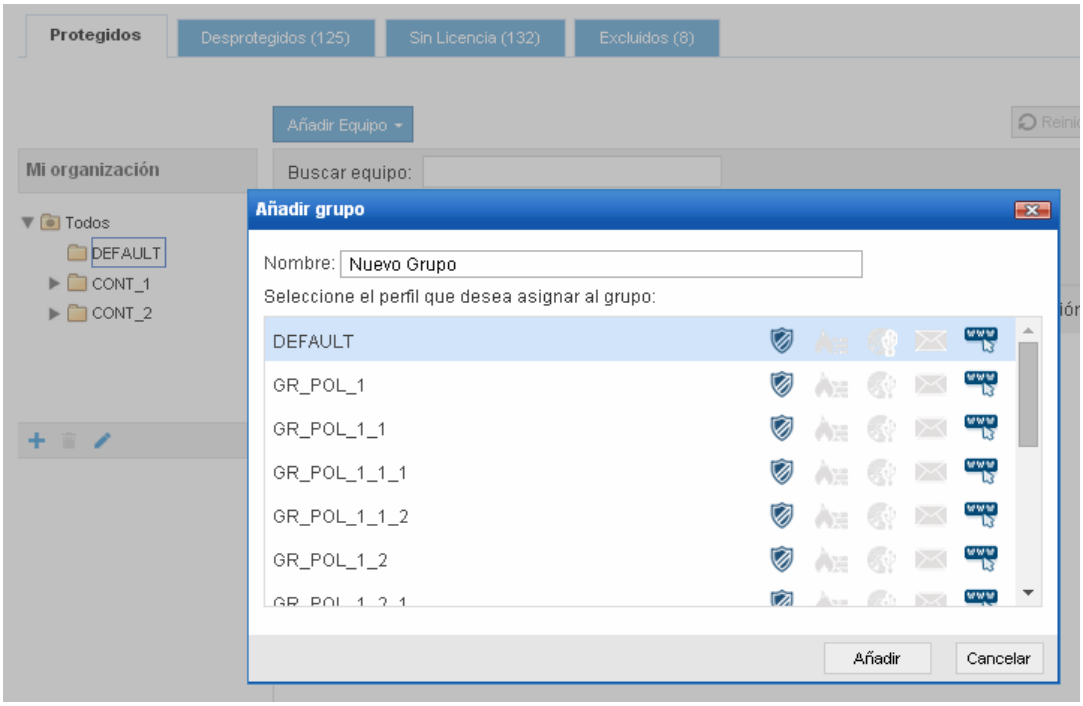
En el caso de los equipos manuales no hay impedimento alguno. Sin embargo, si el equipo se quiere integrar en un subgrupo automático por direcciones IP, el equipo debe cumplir con las reglas especificadas para el subgrupo automático en cuestión.

Si el equipo no encaja en el subgrupo pero sí en alguno de sus grupos padre, el equipo se moverá al grupo padre cuyas reglas sí cumple y las comenzará a aplicar automáticamente.

9.4 Añadir o eliminar grupos

9.4.1 Añadir grupos manuales

Para añadir un grupo a otro ya existente:



1. En la ventana **Equipos** selecciona en el árbol **Mi organización** el grupo *padre* al que añadirás el nuevo.
2. A continuación haz clic en el icono ✚.
3. Introduce el nombre del grupo que has creado y selecciona el perfil de protección que deseas asignar al grupo añadido (por defecto estará seleccionado el perfil del *padre* del grupo).
4. Haz clic en **Añadir**. El grupo creado se añadirá en el árbol como subgrupo o *hijo* del grupo *padre* qe había seleccionado en el paso 1.

Ten en cuenta que el número máximo de grupos que puedes añadir es 6.

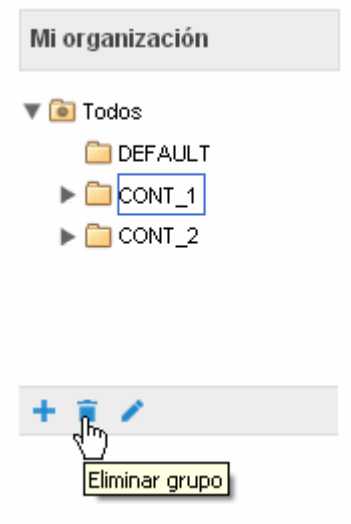
Recuerda que no es posible crear un grupo cuyo nombre sea el mismo que el de otro grupo del mismo nivel.

9.4.2 Añadir grupos automáticos por direcciones IP

1. En la ventana **Configuración**, selecciona el grupo padre al que añadirás el nuevo.
2. A continuación, haz clic en el icono .
3. Haz clic en el botón **Editar grupo**.
4. Haz clic en el icono ✚ y selecciona nombre, perfil y rangos de IP. Haz clic en **Añadir**.

9.4.3 Eliminar un grupo

Para eliminar un grupo, selecciónalo en el árbol y a continuación haz clic en el icono .

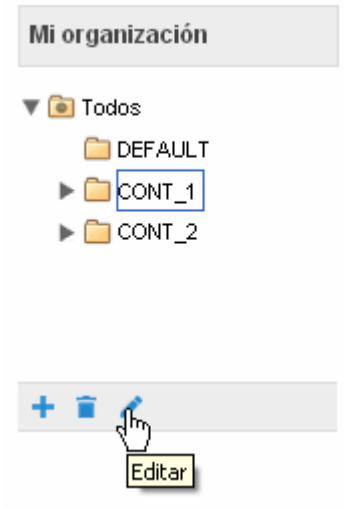


A la hora de eliminar un grupo, es importante que tengas en cuenta que no es posible eliminarlo si contiene grupos o subgrupos. Por ello, antes de eliminar un grupo es necesario que procedas a mover los equipos que lo integran, es decir, tienes que asignarlos a otro grupo/subgrupo.

Una vez realizada la asignación, entonces sí podrás eliminar el grupo/subgrupo en cuestión.

9.4.4 Editar un grupo manual

Para editar un grupo manual selecciónalo en el árbol y haz clic en el icono .



A continuación, podrás editar el nombre del grupo y asignarle el perfil de la protección que desees, elegido de entre la lista de perfiles que se te mostrarán.

En el caso de que el grupo posea subgrupos, podrás aplicar a todos ellos el perfil seleccionado. Para ello, marca la casilla correspondiente y haz clic en **Aceptar**.

Desde la pantalla **Configuración** también es posible acceder a las opciones de crear, eliminar y editar grupo.

9.4.5 Editar un grupo automático por direcciones IP

1. Para editar un grupo automático selecciónalo en el árbol y haz clic en el icono  .

2. A continuación, haz clic en el botón **Editar grupo**.

3. En la ventana **Editar grupo automático por direcciones IP** haz clic en el icono  .

4. A continuación podrás editar el nombre del grupo y asignarle el perfil de la protección que desees. También podrás añadir, modificar o eliminar las direcciones IP.

10. Tipos de permisos

10.1 Tipos de permisos

En Endpoint Protection se han establecido tres tipos de permisos. En función del permiso que se asigne a un usuario, éste podrá realizar mayor o menor número de acciones que afectarán o bien a todos o a algunos equipos y grupos.

Las acciones que el usuario podrá llevar a cabo afectan a diferentes aspectos de configuración básica y avanzada de la protección, y van desde la creación y modificación de sus propias credenciales de usuario y la configuración y asignación de perfiles a grupos y equipos, hasta la generación y obtención de diferentes tipos de informes, entre otros.

Los permisos existentes son:

- Permiso de control total
- Permiso de administrador
- Permiso de monitorización

Selecciona el tipo de permiso cuyas especificaciones desees consultar. Te resultarán de utilidad para asignar funciones a los diferentes integrantes de tus equipos de trabajo y obtener el máximo rendimiento de todas las funcionalidades que Endpoint Protection ha preparado para tu seguridad.

10.2 Permiso de control total

Gestión de usuarios

El usuario puede:

1. Ver todos los usuarios creados en el sistema.
2. Eliminar usuarios.

Gestión de grupos y equipos

El usuario puede:

1. Crear y eliminar grupos/subgrupos.
    - El permiso de control total sobre un grupo es extensible a todos sus subgrupos.
    - En el caso de que se creen nuevos subgrupos sobre un grupo para el que esté autorizado un usuario con control total, dicho usuario tendrá automáticamente permiso sobre el nuevo subgrupo creado.
2. Gestionar la configuración de los perfiles de protección de todos los grupos.
3. Asignar equipos a todos los grupos/subgrupos.
4. Mover equipos de un grupo/subgrupo a otro.

5. Editar el campo **Comentarios** en la pantalla Detalle de equipos.
6. Acceso remoto a cualquier equipo.

Gestión de perfiles e informes

El usuario puede:

1. Copiar perfiles y ver todas las copias realizadas de todos los perfiles.
2. Configurar análisis programados de rutas específicas para cualquier perfil.
3. Visualizar informes (informes inmediatos, no programados), de cualquier grupo.
4. Crear tareas de envío de informes programados sobre cualquier grupo
5. Visualizar todas las tareas de envío de informes.

Búsqueda de equipos desprotegidos

El usuario puede:

1. Configurar tareas de búsqueda de equipos desprotegidos.
2. Visualizar y/o eliminar cualquiera de las tareas creadas.

Desinstalación de la protección

El usuario puede:

1. Configurar tareas de desinstalación de protecciones.
2. Visualizar y/o eliminar cualquiera de todas las tareas creadas.

Gestión de licencias y cuentas

El usuario puede:

1. Utilizar la opción de Ampliar licencias mediante código de activación.
2. Utilizar la opción de Unificar cuentas.
3. Delegar la gestión de su cuenta en un partner.

10.3 Permiso de administrador

Las acciones que el usuario con permiso de administrador puede llevar a cabo y que tienen que ver con gestión de usuarios, equipos, grupos, configuración y desinstalación de la protección, sólo son aplicables a equipos o grupos sobre los que el usuario administrador tenga permiso o que hayan sido creados por él.

Gestión de usuarios

El usuario puede:

1. Modificar sus propias credenciales.
2. Crear usuarios.

Búsqueda de equipos desprotegidos

El usuario puede:

1. Crear tareas de búsqueda para que equipos de los grupos sobre los que se tienen permisos realicen la búsqueda.
2. Visualizar y/o eliminar cualquiera de las tareas de búsqueda de equipos creadas, pero sólo desde equipos pertenecientes a grupos sobre los que tenga permiso.

Gestión de grupos y equipos

El usuario puede:

1. Crear grupos/subgrupos, ya sean manuales o automáticos por dirección IP, y gestionar la configuración de los perfiles de los grupos sobre los que tiene permiso. Su permiso es efectivo sobre todos los grupos existentes hasta el grupo *hijo* seleccionado, es decir, el usuario administrador no podrá tener acceso a un grupo *hijo* sin tenerlo también al grupo *padre*.
2. Eliminar los grupos sobre los que tiene permisos. Sólo se podrán eliminar grupos que no tengan equipos, por lo que antes de eliminar un grupo/subgrupo es necesario asignar o mover sus equipos a otro grupo/subgrupo. Una vez "vaciado" el grupo/subgrupo se podrá proceder a la eliminación.
3. Editar el campo **Comentarios** de los equipos sobre los que tenga permisos, en la pantalla Detalle de equipos.
4. Acceso remoto a aquellos equipos que pertenezcan a grupos/subgrupos sobre los que tenga permiso.

Desinstalación de protecciones

El usuario puede:

1. Configurar tareas de desinstalación de protecciones en equipos o grupos sobre los que tenga permiso.

2. Visualizar y/o eliminar tareas de desinstalación, pero sólo en equipos pertenecientes a grupos sobre los que tenga permiso.

Gestión de perfiles e informes

El usuario puede:

1. Crear perfiles nuevos y visualizarlos.

2. Crear copias de perfiles sobre los que tiene permiso y visualizarlos.

3. Configurar análisis programados de rutas específicas para perfiles sobre los que tenga permiso o hayan sido creados por él.

4. Visualizar informes (informes inmediatos, no programados) que incluyan grupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos que aparezcan en el informe.

5. Crear tareas de envío de informes programados sobre grupos sobre los que tenga permisos

6. Visualizar las tareas de envío de informes que incluyan grupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos que aparezcan en el informe. En caso contrario no podrá visualizar la tarea de envío de informes.

10.4 Permiso de monitorización

El usuario puede:

1. Modificar sus propias credenciales.

2. Ver y monitorizar la protección de los grupos/subgrupos que se le asignen.

    - El permiso de monitorización sobre un grupo es extensible a todos sus subgrupos.

    - En el caso de que se creen nuevos subgrupos sobre un grupo para el que esté autorizado un usuario con permiso de monitorización, éste tendrá automáticamente permiso sobre el nuevo subgrupo creado.

3. Visualizar los perfiles asignados a grupos/subgrupos sobre los que tenga permiso.

4. Visualizar las tareas de búsqueda de equipos protegidos realizadas desde equipos pertenecientes a grupos/subgrupos sobre los que tenga permiso.

5. Visualizar las tareas de desinstalación de los grupos/subgrupos sobre los que tiene permiso.

6. Visualizar informes (informes inmediatos) de grupos/subgrupos sobre los que tenga permisos.

7. Visualizar las tareas de envío de informes que incluyan grupos/subgrupos a los que tenga permiso, siempre y cuando el permiso sea extensible a todos los grupos/subgrupos que aparezcan en el informe. En caso contrario no podrá visualizar la tarea de envío de informes.

11. Configurar la protección

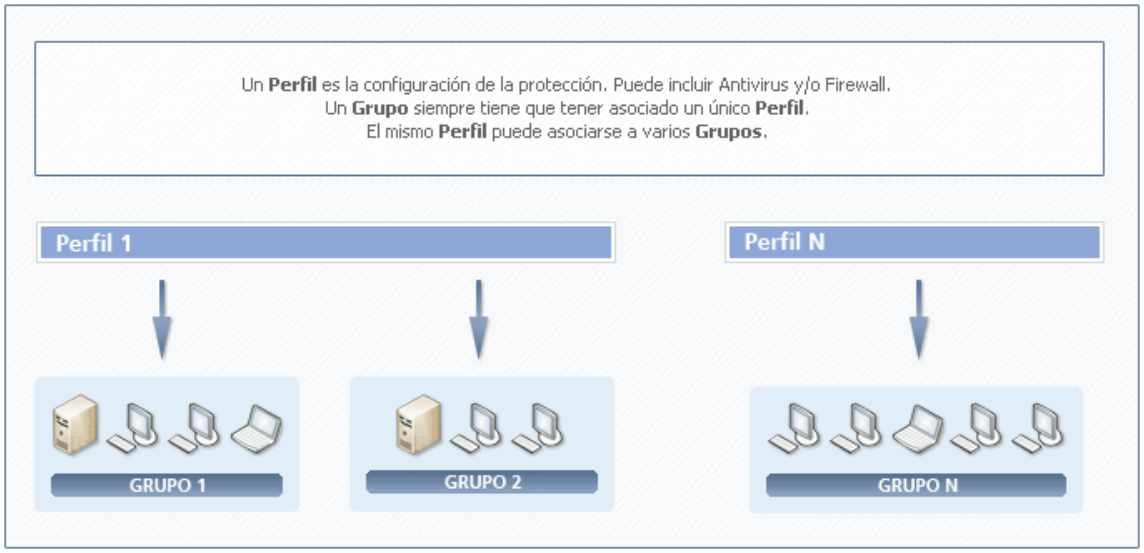
11.1 Introducción

La protección que Endpoint Protection proporciona está pensada para ser instalada y distribuida en la red informática de tu empresa. En consecuencia, la protección a instalar variará en función del tipo de equipos a proteger y de las diferentes necesidades que tengas en cuanto a seguridad.

Endpoint Protection ofrece una protección multiplataforma que te permitirá proteger tus equipos y servidores Windows , Linux Android y OS X.

Puedes configurar la protección antes o después de la instalación. **En el caso de esta guía, se ha optado por explicar el proceso de configuración como paso previo a la instalación de la protección en los equipos**. Para ello debes crear un perfil y después asignarlo al grupo o grupos a los que deseass aplicarlo.

> ***IMPORTANTE:*** ***A lo largo de esta guía se describe el proceso de configuración de las diferentes protecciones partiendo de la creación desde cero de un perfil (Configuración / Perfiles / Añadir perfil /...).***
> ***No obstante, la configuración de las protecciones de los perfiles puede modificarse en cualquier momento, por lo que para perfiles ya existentes los pasos a seguir serán (Configuración / Perfiles / Nombre del perfil / y a continuación realizar las modificaciones en la ventana Edición de perfil)***



A la hora de asignar perfiles a los grupos creados, las opciones son varias: un mismo perfil se puede aplicar a varios grupos, cada grupo puede tener un perfil diferente o se puede dar el caso de que sólo se necesiten un único perfil y un único grupo.

Al crear un perfil configurarás el comportamiento que la protección tendrá para ese perfil específico, esto es, determinarás qué tipo de análisis se realizarán y sobre qué elementos, y cada cuánto tiempo se actualizará la protección.

Antes de acceder a la opción **Instalación**, si lo deseas puedes crear los perfiles que necesites y configurar cuál será el comportamiento de la protección en cada perfil. A continuación se

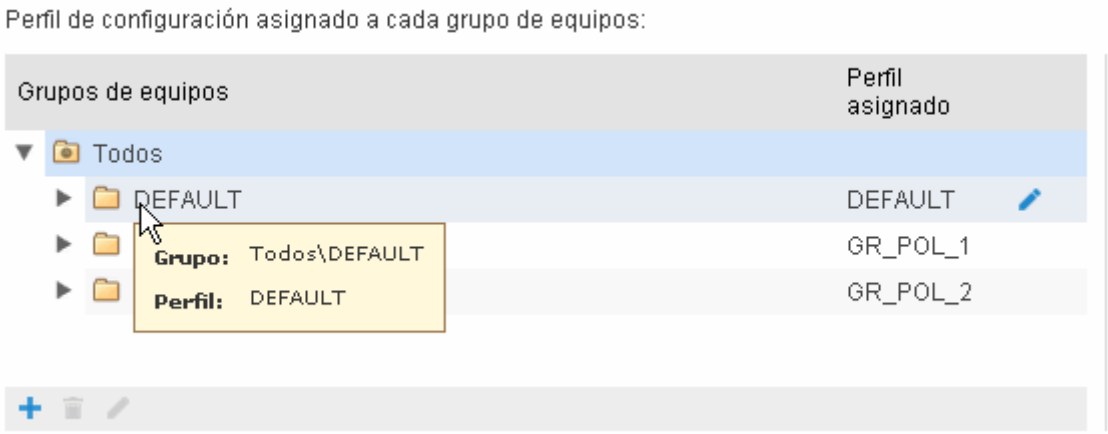
crearán los grupos de equipos necesarios, asignándoles el perfil que se desee, con lo que dicho perfil se aplicará a todos los equipos que formen parte del grupo.

También puedes proteger tus equipos con la configuración por defecto proporcionada por Panda Security.

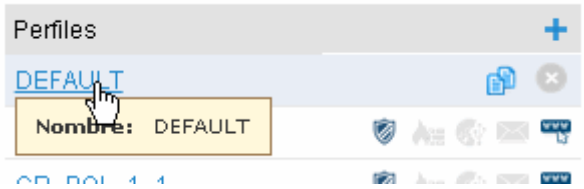
11.2 Perfil Default

En la ventana **Configuración** se muestran los perfiles existentes y el detalle de las protecciones activadas en cada uno de esos perfiles. Para ello, se utiliza un sencillo sistema de iconos que indican la existencia en el equipo de unas u otras protecciones. Estos iconos están disponibles si sitúas el cursor sobre la leyenda:

Además también se detalla el perfil asignado a cada uno de los grupos.



La primera vez que accedas a esta ventana se mostrará el perfil por defecto ***–Default***- e información sobre las protecciones que tiene asociadas.



Ten en cuenta que:

1. Las siguientes protecciones están desactivadas por defecto:
    - La protección de correo electrónico.
    - El control de dispositivos.
    - La protección para Exchange Servers (sólo disponible para clientes que dispongan de licencias de Endpoint Protection Plus).
    - La protección de control de acceso a páginas Web (sólo disponible para clientes que dispongan de licencias de Endpoint Protection Plus).
    - La protección antirrobo para los dispositivos Android (sólo disponible para clientes que dispongan de licencias de Endpoint Protection Plus).
2. La protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010 y 2013.

Modificar el perfil Default

Si en algún momento quieres modificar la configuración de este perfil, haz clic sobre el nombre del perfil. Accederás a la ventana **Editar perfil**. Realiza las modificaciones que desees y haz clic en **Aceptar**.

Restaurar la configuración original del perfil Default

Si posteriormente deseas restaurar la configuración original del perfil, hazlo mediante la opción **Restaurar configuración por defecto** de la ventana **Editar perfil**.

11.3 Visión general

La ventana **Configuración** te permite tener una visión global acerca de qué perfiles de protección tienes configurados, a qué grupos están asignados esos perfiles y qué restricciones tienen dichos grupos. En definitiva, lo que verás será el resumen de la configuración de las diferentes protecciones.

La ventana **Configuración** se estructura en dos listas. En la zona derecha se muestra una lista con todos los perfiles disponibles y en la zona izquierda aparecen los grupos de equipos y el perfil que cada uno de ellos tiene asignado.

11.4

11.5 Perfiles disponibles

11.5.1 Crear un perfil nuevo

Al hacer clic en el símbolo + situado en la lista de perfiles de esta ventana **Configuración**, accederás a la ventana **Editar perfil** desde la que podrás iniciar la configuración de las diferentes protecciones para el perfil.

En la lista de perfiles se utiliza un sencillo sistema de iconos para mostrar, junto al nombre de cada perfil, las protecciones que dicho perfil tiene configuradas.

El significado de cada icono está disponible en la leyenda:

11.5.2 Copiar un perfil

Mediante los iconos  podrás copiar y/o eliminar el perfil. Estos iconos se muestran al desplazar el puntero sobre el nombre del perfil. Para más información, consulta el apartado Copiar un perfil.

11.5.3 Editar perfil

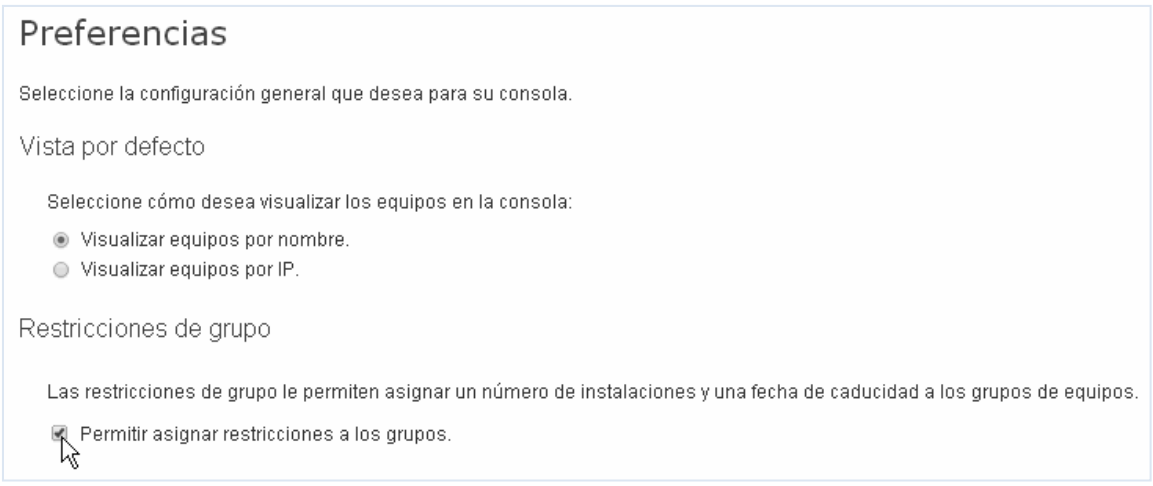
Al pinchar sobre el nombre del perfil, se accederá a la pantalla de edición del perfil, desde donde podrás modificar la configuración del mismo.

11.6 Grupos y perfiles asignados

La información se estructura en cuatro columnas:

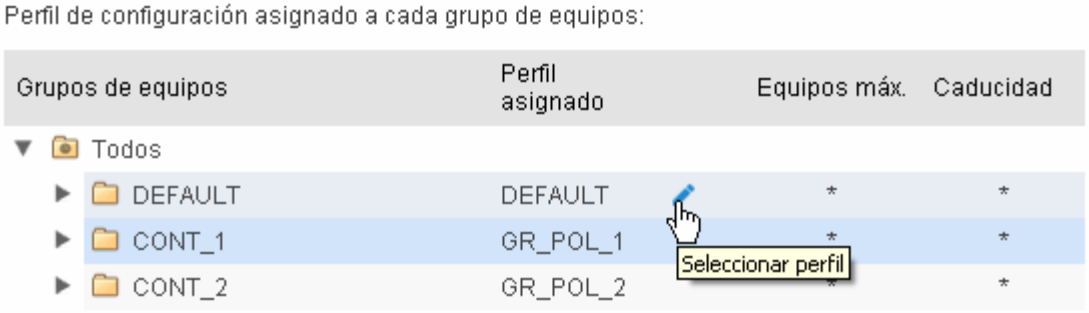
- Grupos de equipos
- Perfil asignado
- Número máximo de instalaciones
- Caducidad

Las dos últimas sólo serán visibles siempre y cuando hayas seleccionado la opción **Permitir asignar restricciones a los grupos** en la ventana Preferencias.

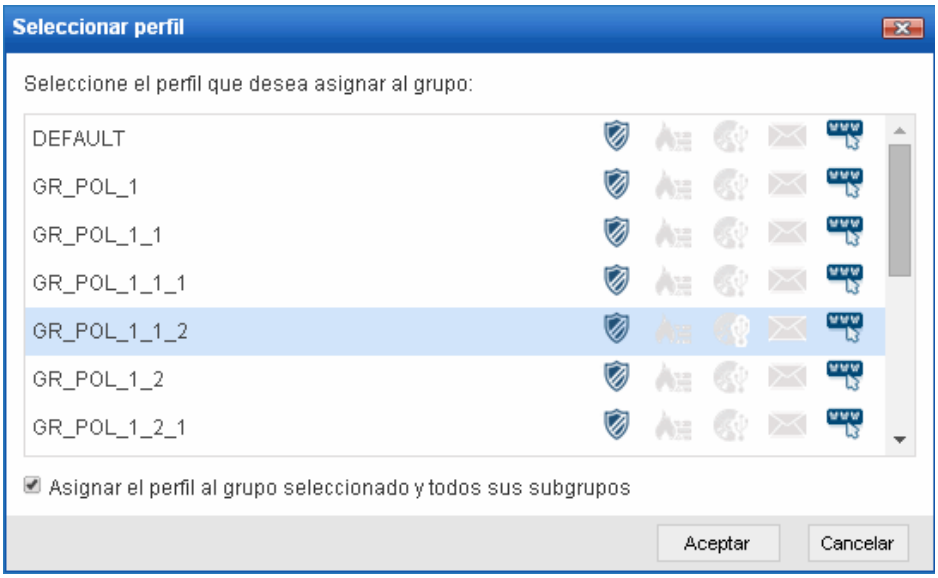


11.6.1 Modificar el perfil asignado a un grupo

Como norma general, para modificar desde esta ventana **Configuración** el perfil asignado a un grupo, haz clic en el icono de edición situado junto al nombre de perfil.



A continuación, en la ventana **Seleccionar perfil**, selecciona de entre la lista el nuevo perfil que deseas asignar y haz clic en **Aceptar**. Si deseas que el perfil elegido sea aplicado también a los subgrupos "hijos" del grupo seleccionado, marca la casilla correspondiente.



12. Crear y configurar un perfil

Crear un perfil

Copiar un perfil

Configuración general del perfil

12.1 Crear un perfil

Si necesitas crear perfiles nuevos, a medida que los crees se mostrarán en la ventana de **Configuración** junto al perfil ***Default*** ya existente, acompañados de información sobre las protecciones que incluyen.

Después podrás modificar en cualquier momento la configuración de un perfil haciendo clic sobre su nombre y accediendo a la ventana **Editar perfil**.

Si se intenta asignar a un perfil un nombre ya utilizado para otro, se mostrará un mensaje de error.

12.1.1 Permisos necesarios

Si no puedes visualizar el perfil que ya existe con dicho nombre es porque seguramente no disponga de permiso para ello. Para más información, consulta el apartado Tipos de permisos.

Para crear el perfil haz click en el icono de **Añadir perfil** (**+**) existente en la página de **Configuración** y accederás a la ventana **Editar perfil**. Desde aquí podrás configurar el perfil nuevo.

12.1.2 Configuración del perfil

La configuración de un perfil se estructura en las siguientes secciones: General, Windows/Linux, OS X y Android.

- Dentro de la opción de Windows y Linux podrás configurar: antivirus, firewall, control de dispositivos, protección para servidores Exchange y control de accesos a páginas Web (estas dos últimas protecciones sólo las podrás configurar si dispones de licencias de Endpoint Protection Plus).

- Dentro de la opción de OS X podrás configurar la protección antivirus.

- En el caso de los dispositivos Android, podrás configurar la protección permanente antivirus y la protección antirrobo (en este caso, sólo si posees licencias de Endpoint Protection Plus o Fusion).

Todo el proceso de configuración del perfil se describe con detalle a lo largo de las siguientes secciones:

Configuración general del perfil

Configuración de Windows/Linux

- Configuración de la protección antivirus
- Configuración de la protección firewall
- Configuración del control de dispositivos
- Configuración de la protección para servidores Exchange
- Configuración de la protección de control de acceso a páginas Web

Configuración OS X

- Configurar la protección para equipos y servidores MAC

Configuración para Android

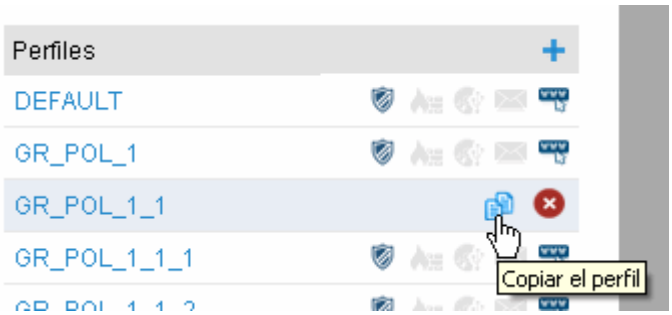
- Configuración de la protección antivirus para dispositivos Android
- Configuración de la protección antirrobo para dispositivos Android

12.2 Copiar un perfil

Endpoint Protection te ofrece la posibilidad de realizar copias de perfiles existentes. Esto resulta útil cuando preveas que la configuración básica de un perfil que ya has creado es susceptible de ser aplicada a otros equipos.

De esta manera, en lugar de crear dicha configuración básica cada vez, podrás copiar el perfil para después personalizarlo y adaptarlo a las circunstancias concretas de protección que necesites.

En la pantalla de configuración, posiciona el cursor sobre los iconos que muestran las protecciones activas del perfil que deseas copiar y haz clic en el icono .



Una vez copiado el perfil, éste se mostrará en la lista bajo el perfil original con el mismo nombre que tiene el perfil original, añadiendo el texto *(copia)* al final.

En el caso del perfil Default, es posible hacer una copia de él, pero el perfil copiado no tendrá la condición de perfil por defecto ni será asignado automáticamente a ningún equipo. El perfil Default original será siendo el predeterminado.

La copia de perfil será posible en función del tipo de permiso del que dispongas. Para más información, consulta el apartado Tipos de permisos.

12.3 Configuración general del perfil

Aquí da comienzo la configuración de opciones de tipo general para el perfil de protección que has creado. Por ello, es importante tener claro no solo qué tipo de perfil deseas configurar sino cuáles son los equipos en los que lo instalarás.

Esta configuración afectará tanto a los equipos Windows/Linux/Android como a los equipos OS X.

Para acceder a la configuración general del perfil, haz clic en el menú **Configuración/Añadir nuevo perfil**.

12.3.1 Pestaña Información

Al seleccionar la opción de **Añadir perfil** podrás dar un nombre al perfil que estás creando y añadir una descripción adicional que le sirva para identificar el perfil y seleccionar el idioma en el que se instalará la protección.

La configuración del idioma por defecto de la protección sólo afectará a los equipos Windows, ya que la protección de Endpoint Protection para OS X se instala siempre en inglés. En el caso de los dispositivos Android, la protección se instalará en el idioma del dispositivo y, en su defecto, en inglés.

12.3.2 Pestaña Proxy

Configura la conexión a Internet de los equipos. Establece cuál es la conexión a Internet del equipo, si ésta se realiza a través de proxy y si se requiere una autenticación para ello.

En el caso de los equipos con sistema operativo Linux, esta configuración de la conexión a Internet es necesario hacerla desde el equipo mediante la línea de comandos.

12.3.3 Pestaña Aplica a

Cuando asignes el perfil que estás creando a algún grupo o grupos, éstos aparecerán listados aquí.

13. Antes de instalar

Recomendaciones previas a la instalación

Instalación según sistema operativo

Instalación rápida

Casos de instalación

13.1 Recomendaciones previas a la instalación

13.1.1 Requisitos que deben cumplir los diferentes equipos

Independientemente del modo de instalación que vayas a utilizar, es recomendable consultar los requisitos que los diferentes equipos afectados por la instalación deben reunir. Consulta el apartado Requisitos.

13.1.2 Existencia de otras protecciones instaladas en los equipos

Protección ajena a Panda Security

Si vas a instalar Endpoint Protection en un equipo en el que ya se encuentra instalada alguna otra solución de seguridad ajena a Panda Security, puedes elegir entre instalarlo sin desinstalar la otra protección, de tal manera que ambas soluciones de seguridad convivan en el mismo equipo o, por el contrario, desinstalar la otra solución de seguridad y funcionar exclusivamente con Endpoint Protection.

En función del tipo de versión de Endpoint Protection que desees instalar, el comportamiento por defecto varía.

- **Versiones Trials:** En versiones de evaluación, por defecto Endpoint Protection se instalará en un equipo que ya dispone de otra solución ajena a Panda Security.
- **Versiones comerciales:** En este caso, por defecto Endpoint Protection no se instalará en un equipo que ya dispone de otra solución ajena a Panda Security. Si Endpoint Protection dispone del desinstalador de dicho producto, lo desinstalará y a continuación se lanzará la instalación de Endpoint Protection. En caso contrario, se detendrá la instalación.

Este comportamiento por defecto es configurable tanto en versiones trials como en versiones comerciales. Puedes modificarlo desde la ventana de **Configuración / (pulsar sobre el perfil a editar) / Windows y Linux / Opciones Avanzadas**. Además, tanto en la ventana **Equipos** como en la de **Instalación** se te indicará en todo momento cuál es la opción de instalación que tienes configurada.

Este aviso será visible solo en el caso de que tengas la misma configuración de instalación definida para todos tus perfiles.

Protección de Panda Security

Si la otra solución de seguridad ya existente es alguna de las de Panda Security, sí será necesario desinstalarla antes de instalar Endpoint Protection en el equipo.

Lista de desinstaladores

nsultar una lista de los antivirus que Endpoint Pro
automáticamente. Si la solución que tienes que desinstalar no está en la lista, tendrás que desinstalarla manualmente.

13.1.3 Desinstalación manual

En Windows 8 o superior:

Panel de Control > Programas > Desinstalar un programa.

También puedes realizar la desinstalación tecleando, en el menú Metro: "desinstalar un programa".

En Windows Vista, Windows 7, Windows Server 2003, 2008 y 2012:

Panel de Control > Programas y características > Desinstalar o cambiar.

En Windows XP:

Panel de Control > Agregar o quitar programas.

En OS X:

Finder > Aplicaciones > Arrastra el icono de la aplicación que deseas desinstalar a la papelera.

En dispositivos Android:

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

13.1.4 Configuración de exclusiones en la protección de archivos para servidores con Exchange Server

Con el fin de que no se produzcan interferencias entre Endpoint Protection y Exchange, en servidores en los que se va a instalar o ya se ha instalado Endpoint Protection es necesario excluir una serie de carpetas del análisis de la protección de archivos.

Para más información, acude al centro de soporte técnico (http://www.pandasecurity.com/spain/enterprise/support/).

Si dispones de licencias de Endpoint Protection las exclusiones ya se habrán realizado por defecto.

13.2 Instalación según sistema operativo

En función del sistema operativo de los equipos en los que se va a instalar la protección, el proceso de instalación se podrá llevar a cabo de diferentes maneras.

Método de instalación	Sistema operativo			
	Windows	Linux	OS X	Android
Descarga del instalador	SÍ	SÍ	SÍ	SÍ*
Generar URL de instalación	SÍ	SÍ	SÍ	SÍ
Herramienta de distribución	SÍ	NO	NO	NO

* Sólo si la descarga se realiza desde un dispositivo Android. En cualquier otro sistema, se mostrará un código QR y un botón de acceso a la página de Endpoint Protection en Google Play, desde donde se iniciará el proceso de instalación y vinculación del dispositivo con Endpoint Protection.

En la práctica esto supone que:

- **Si dispones de licencias de Endpoint Protection tanto para OS X como para Windows/Linux/Android,** tendrás disponibles las dos maneras de instalación comentadas y además también podrás utilizar la herramienta de distribución para distribuir la protección para Windows.
- **Si solo dispones de licencias de Endpoint Protection para OS X**, no tendrás disponibles las opciones de descarga para Windows/Linux/Android.

  Encontrarás toda la información en el capítulo Instalar la protección.

13.3 Instalación rápida

Si acabas de adquirir el producto y aún no has instalado la protección en ningún equipo, al acceder a la consola se mostrará la pantalla de **Equipos**.

En esta pantalla podrás ver un mensaje informando sobre el estado (cliente sin equipos instalados), y se te invitará a realizar instalaciones.

Para ello, podrás:

- **Instalar en este equipo ahora**. Al pinchar en esta opción, se descargará el instalador para Windows en el equipo en el que te encuentras.
- **Enviar url por correo**.

Además también dispondrás de las siguientes opciones:

- Descargar el instalador para el sistema operativo correspondiente.
- Descargar la herramienta de distribución (solo para equipos Windows).

Una vez que se haya realizado la instalación, los equipos se mostrarán en el listado de equipos protegidos de la ventana **Equipos**.

drás de ningún grupo, y, por lo tanto, todas las instala
sobre el grupo por defecto (*Default*); es decir, con la configuración por defecto establecida por Panda Security.

Si además del grupo *Default* has creado otros grupos, todos ellos se mostrarán en el árbol de niveles de grupos llamado **Mi organización**, situado en la parte izquierda de la ventana.

13.3.1 Añadir equipo

Si ya dispones de equipos instalados, los podrás ver en la pantalla de **Equipos.** Además, en esta pantalla se te ofrece la opción de añadir nuevos equipos de forma sencilla.

Al seleccionar esta opción se mostrarán las mismas opciones que se muestran a los clientes que no disponen de equipos instalados:

- Instalar en este equipo ahora.
- Enviar url por correo.
- Descargar el instalador para el sistema operativo correspondiente.
- Descargar la herramienta de distribución (solo para equipos Windows).

13.4 Casos de instalación

13.4.1 Instalación en equipos sin protección previa instalada

1. Accede a la consola Web e introduce tu Login Email y contraseña.
2. Crea un perfil nuevo (o utiliza el perfil por defecto, según tus necesidades).
3. En función de las licencias que poseas, configura el comportamiento de las diferentes protecciones:
    - Protección antivirus
    - Protección firewall
    - Control de dispositivos
    - Servidores Exchange (Si dispones de licencias de Endpoint Protection Plus)
    - Control de accesos a páginas Web (Si dispones de licencias de Endpoint Protection Plus)
    - Protección para OS X
    - Protección antivirus para dispositivos Android
    - Protección antirrobo para dispositivos Android (Si dispones de licencias de Endpoint Protection Plus o Fusion).
4. Cree un grupo (opcional).

:a para ello el modo de instalación que mejor se adap
necesidades y a las características de tu red informática.

13.4.2 Instalación en equipos con protección previa instalada

El proceso de instalación es similar al caso anterior, pero **es muy importante** que antes de instalar la protección de Endpoint Protection establezcas en la configuración si prefieres:

- que se instale la protección junto a las otras soluciones de seguridad que ya tuvieras en el equipo
- que se desinstalen otras protecciones antes de instalar Endpoint Protection.

Consulta las **Recomendaciones previas a la instalación**.

En la mayoría de los casos de instalación de la protección y desinstalación de protecciones previas, el número de reinicios que el proceso exige es de 1, y nunca será superior a 2.

14. Instalar la protección

Instalación en equipos Windows/Linux

Instalación en equipos OS X

Instalación en dispositivos Android

14.1 Instalar en equipos Windows/Linux

14.1.1 Instalar la protección mediante el instalador

Por favor, ten en cuenta que, si bien en general este método de instalación es muy parecido para todos los sistemas operativos (Windows, Linux, OS X, Android), es recomendable que consultes el apartado de instalación correspondiente a cada uno de ellos, con el fin de conocer a fondo las peculiaridades del proceso de instalación.

- Instalación en equipos Linux.
- Instalación en equipos OS X.
- Instalación en dispositivos Android.

Tanto en Linux como en Windows el instalador es el mismo para plataformas de 32 y de 64 bits. Te recomendamos que antes de descargar el instalador consultes los requisitos que los equipos y dispositivos deben cumplir.

14.1.2 Descarga del instalador

En primer lugar, selecciona el sistema operativo para el que vas a descargar el instalador.

Si dispones de más de un grupo, deberás seleccionar el grupo en el que se integrarán los equipos a los que instalarás la protección. Si, por el contrario, dispones de un solo grupo (el grupo por defecto o *Default*), no se mostrará la ventana de selección de grupos, y la instalación se realizará en el grupo por defecto.

1. Haz clic en **Descargar**
2. En el cuadro de diálogo de descarga de archivo selecciona **Guardar**, y una vez la descarga haya finalizado, ejecuta el archivo desde el directorio en el que lo hayas guardado. El asistente te guiará a lo largo del proceso de instalación.
3. Distribuye la protección al resto de equipos de la red. Para ello puedes utilizar tus propias herramientas o bien instalarlo manualmente.

Generar URL de instalación

Utiliza esta opción si lo que deseas es lanzar la instalación desde cada equipo.

1. Selecciona el grupo en el que deseass que se integren los equipos (por defecto está seleccionado el grupo por defecto).

2. Copia la URL de instalación para el sistema operativo que necesites, y después accede a ella desde cada uno de los equipos a los que tengas acceso y a los que desees instalar la protección.

Envío del enlace por correo electrónico

1. Selecciona el grupo en el que deseass que se integren los equipos (por defecto está seleccionado el grupo por defecto) y haz clic en **Enviar por correo**.

2. Automáticamente, los usuarios recibirán un correo electrónico con el enlace de descarga correspondiente a su sistema operativo. Al hacer clic en el enlace, se iniciará la descarga del instalador.

3. El asistente te guiará a lo largo del proceso de instalación.

14.2 Instalar la protección mediante la herramienta de distribución remota

Este método de instalación sólo es válido para equipos con sistema operativo Windows.

14.2.1 Descarga de la herramienta de distribución

Es importante que antes de descargar la herramienta de distribución, compruebes los requisitos que debe reunir el equipo. Los encontrarás en el capítulo 1.

La herramienta de distribución te permite instalar y desinstalar la protección de forma centralizada en los equipos de la red con sistema operativo Windows, evitando así la intervención manual de los usuarios a lo largo del proceso.

Recuerda que, en el caso de que desees desinstalar la protección, se te solicitará que introduzcas la contraseña que estableciste para el perfil de configuración correspondiente.

1. En **Instalación,** haz clic en **Descargar herramienta de distribución remota**.

2. En el cuadro de diálogo de descarga de archivo selecciona **Guardar**, y cuando la descarga haya finalizado, ejecuta el archivo desde el directorio en el que lo hayas guardado. El asistente te guiará a lo largo del proceso de instalación.

Una vez instalada la herramienta de distribución de Endpoint Protection, es necesario abrirla para poder desplegar la protección en los equipos. A continuación se mostrará la ventana principal desde la que podrás instalar y desinstalar las protecciones.

Instalación de la protección

A la hora de seleccionar los equipos en los que instalar la protección, la herramienta de distribución te permite hacerlo en base a dos criterios: por dominios, o por IP/nombre de equipo.

Por dominios

1. Haz clic en **Instalar protecciones**.

2. Haz clic en **Por dominios**.

3. Especifica el grupo en el que deseass agrupar los equipos (opcional).

4. Localiza en el árbol los equipos a los que deseass distribuir la protección, y marca la casilla correspondiente.

Opcionalmente, puedes indicar un nombre de usuario y contraseña con privilegios de administrador en los equipos seleccionados.

Es aconsejable utilizar una contraseña de administrador de dominio. De este modo, no tendrás que indicar el nombre de usuario y la contraseña de cada equipo.

Por IPs o nombre de equipo

1. Haz clic en **Por IPs o nombre de equipo**.

2. Especifica el grupo en el que deseas agrupar los equipos (opcional).

3. Indique los equipos a los que deseas distribuir la protección.

   Puedes introducir los nombres de los equipos, sus direcciones IP o rangos de IP, separando estos datos con comas.

   Haz clic en **Añadir** para sumarlos a la lista, y en **Eliminar** para suprimirlos.

- *Ejemplo de IP individual: 127.0.0.1*

- *Ejemplo de nombre de equipo: EQUIPO03*
- *Ejemplo de rango de IP: 192.0.17.5-192.0.17.145*

Opcionalmente, puedes indicar un nombre de usuario y contraseña con privilegios de administrador en los equipos seleccionados.

Es aconsejable utilizar una contraseña de administrador de dominio. De este modo, no tendrás que indicar el nombre de usuario y la contraseña de cada equipo.

Para obtener información más detallada sobre la tarea, activa el **Log de eventos** (menú **Ver**)

Instalación mediante otras herramientas

Si utilizas habitualmente herramientas de distribución de archivos propias, puedes utilizarlas para distribuir la protección.

14.3 Instalar en equipos OS X

14.3.1 Requisitos que deben cumplir los equipos

Antes de instalar la protección, es muy importante que tengas en cuenta los requisitos que deben reunir los diferentes equipos. Los encontrarás en el capítulo 1. También puedes acceder a la dirección:

http://www.pandasecurity.com/spain/enterprise/support/card?id=50076

14.3.2 Modos de instalación

En los equipos cuyo sistema operativo es OS X la instalación puede realizarse de dos maneras:

1. Mediante el instalador.
2. Generando una URL de instalación y lanzando la instalación posteriormente desde los equipos.

Para saber más sobre la instalación en equipos MAC, consulta el apartado Instalacion en equipos OS X.

14.4 Instalación en equipos con OS X

14.4.1 Descarga del instalador

Este sistema de instalación es similar al descrito para los equipos Windows y Linux.

1. En la ventana **Instalación** selecciona la opción de descargar el instalador para OS X.
2. Selecciona el grupo en el que deseas que se integren los equipos (por defecto, se integrarán en el grupo llamado Default).

3. En el cuadro de diálogo de descarga de archivo selecciona **Guardar**, y una vez la descarga haya finalizado, ejecuta el archivo desde el directorio en el que lo hayas guardado. El asistente te guiará a lo largo del proceso de instalación.

4. Distribuye la protección al resto de equipos de la red. Para ello puedes utilizar tus propias herramientas o bien instalarlo manualmente.

14.4.2 Generar URL de instalación

Utiliza esta opción si lo que deseas es lanzar la instalación desde cada equipo.

1. Selecciona el grupo en el que deseas que se integren los equipos (por defecto está seleccionado el grupo por defecto).

2. Copia la URL de instalación para MAC, y después accede a ella desde cada uno de los equipos a los que tengas acceso y a los que desees instalar la protección.

Envío del enlace por correo electrónico

1. Selecciona el grupo en el que deseas que se integren los equipos (por defecto está seleccionado el grupo por defecto) y haz clic en **Enviar por correo**.

2. Automáticamente, los usuarios recibirán un correo electrónico con el enlace de descarga (recibirán la URL de instalación que has generado anteriormente). Al hacer clic en ella se iniciará la instalación.

3. El asistente te guiará a lo largo del proceso de instalación.

Una vez instalada la protección en los equipos, podrás configurarla. Consulta el apartado Configuración de la proteccion para equipos con OS X.

Información detallada sobre la instalación en equipos OS X

Una vez distribuido el instalador a los equipos OS X, la instalación en local de la protección de EndPoint Protection para OS X es muy sencilla, gracias a su asistente.

Ten en cuenta que la protección de EndPoint Protection para OS X se instalará siempre en inglés.

Sigue estos pasos para instalar la protección en un equipo OS X:

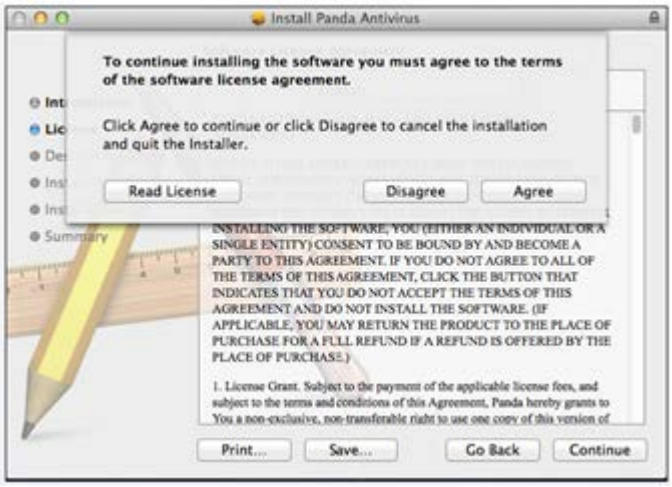
1. Ejecuta el instalador del programa.

2. El asistente muestra una ventana de bienvenida notificando el inicio de la instalación de EndPoint Protection para OS X.

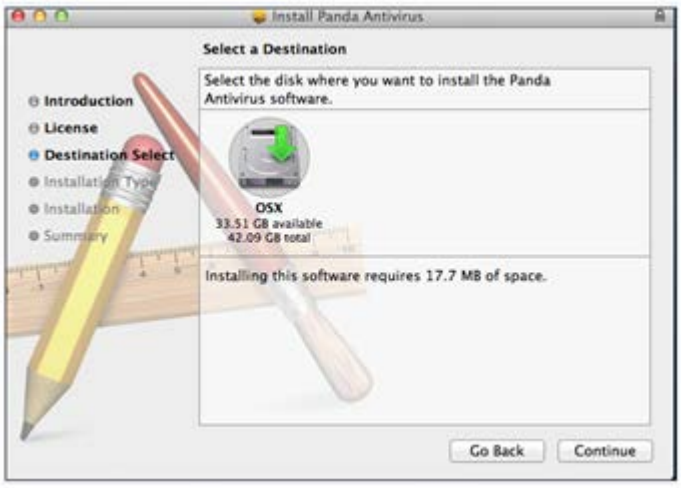
3. Haz clic en **Continuar**.

4. Haz clic en **Read License** si deseas leer el acuerdo de licencia.

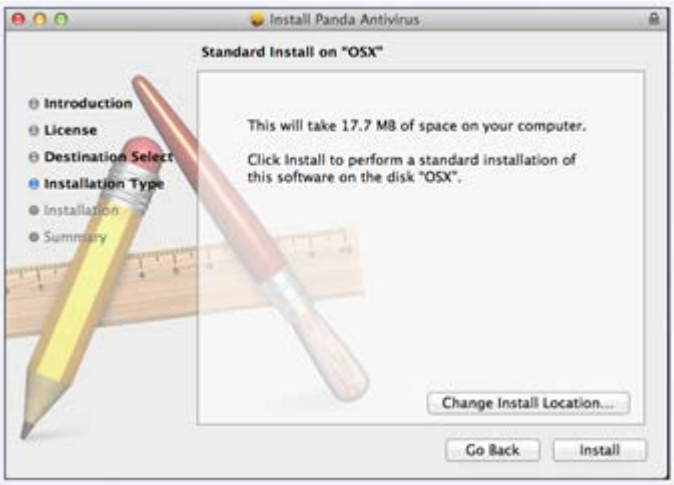
5. Si estás de acuerdo, haz clic en **Agree** y a continuación **Continue** para proseguir con la instalación.



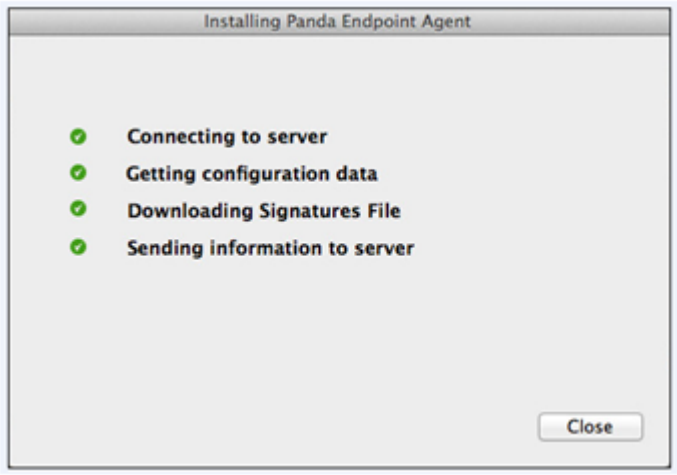
6. Selecciona la unidad de disco en la que deseas realizar la instalación de la protección y haz clic en **Continue**.



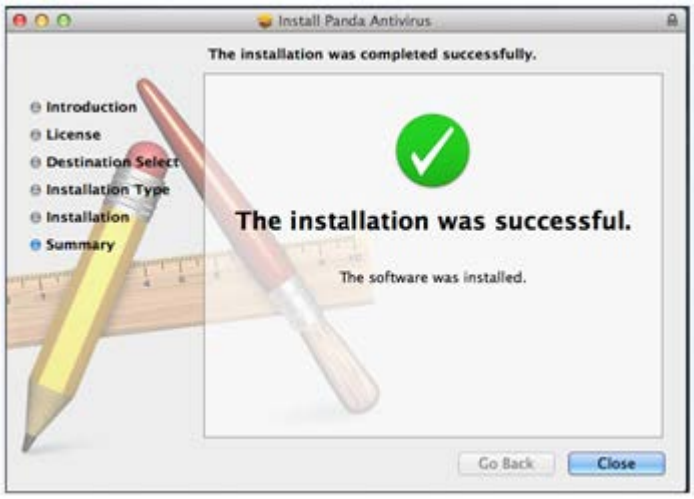
7. Si deseas modificar la ruta de instalación de la protección - por defecto en /Applications y /Library/Intego – haz clic en **Change Install Location**… y selecciona otra ruta.



8. Haz clic en **Pulse Install** para que comience el proceso de instalación.



9. Cuando concluya la copia de archivos, el sistema mostrará en pantalla el resultado de la instalación.



10. Haz clic en **Close** para finalizar.

14.5 Instalar en dispositivos Android

14.5.1 Introducción

La instalación de Endpoint Protection en dispositivos Android tiene la particularidad de que, una vez instalada, es necesario realizar una labor adicional para vincular el dispositivo Android con el grupo de equipos en el que se integrará en la consola Web de Endpoint Protection.

De esta forma, la consola Web detectará la existencia del dispositivo y lo reconocerá como tal dentro del listado de equipos protegidos.

14.5.2 Modos de instalación

En los dispositivos Android es posible realizar la instalación de dos maneras:

Desde la consola Web de Endpoint Protection

La instalación se realizará descargando el instalador correspondiente al sistema operativo Android.

Desde el dispositivo

1. Accediendo a la página Web de Endpoint Protection en Google Play.
2. Por medio de la URL de instalación que recibirás en un correo electrónico. En el mismo mensaje se incluye también la URL necesaria para realizar el proceso de vinculación dispositivo-consola Web que se ha mencionado anteriormente.

14.5.3 Instalación desde la consola Web

Descarga del instalador

En la ventana **Instalación** de la consola Web, selecciona la opción de descarga del instalador para Android. A continuación, se mostrará información sobre el proceso de instalación:

1. **Instalación mediante código QR.** Requiere que el usuario del dispositivo disponga de acceso a la consola Web de Endpoint Protection. Además, es necesario que tenga instalada en su dispositivo una aplicación para el escaneo de códigos QR.

2. **Instalación a través de Google Play.** No es necesario disponer del dispositivo que se quiere proteger en el momento de realizar la instalación, pero sí de las credenciales de la cuenta de Google asociada a dicho dispositivo.

En ambos casos se mostrará la página de Endpoint Protection en Google Play desde la que podrás realizar la instalación.

Vinculación del dispositivo con la consola Web

Una vez realizada la instalación, es el momento de integrar el dispositivo en el grupo que desee. Para ello:

1. Abre la protección que acabas de instalar en el dispositivo.

2. Aparecerá la pantalla que te indicará que vas a iniciar el proceso para añadir el dispositivo al listado de equipos y dispositivos gestionados desde la consola Web de Endpoint Protection.

3. Haz clic en el botón **Usar QR**. Aparecerá otra pantalla indicándote que debes acceder a la consola Web de Endpoint Protection para poder escanear el código QR.

4. Ya en la consola, en la ventana **Instalación**, haz clic en el botón correspondiente a la descarga del instalador para Android.

5. Selecciona el grupo en el que deseas integrar el dispositivo y escanea el código QR.

6. Introduce el nombre con el que quieres que se muestre el dispositivo en la consola Web de Endpoint Protection, haz clic en **Continuar** y activa los permisos necesarios para poder activar el antirrobo.

Ya ha finalizado el proceso de instalación e integración. El dispositivo se mostrará en el listado de la ventana **Equipos**, dentro del grupo que has seleccionado anteriormente.

14.5.4 Instalación desde el dispositivo

Instalación desde la página Web de Endpoint Protection

En la ventana **Instalación** de la consola Web, selecciona la opción de descarga del instalador para Android. A continuación, se mostrará información sobre el proceso de instalación:

1. Selecciona la opción para instalar desde Google Play. Se mostrará la página correspondiente a Endpoint Protection.

2. Haz clic en **Instalar**.

3. Una vez instalada, abre la aplicación y, de nuevo en la consola Web de Endpoint Protection, selecciona el grupo en el que deseas instalar la protección.

4. Haz clic en **Añadir este dispositivo al grupo**. A continuación se iniciará el proceso de vinculación.

5. Introduce el nombre con el que quieres que se muestre el dispositivo en la consola Web de Endpoint Protection.

6. Haz clic en **Continuar** y activa los permisos necesarios para poder activar la protección antirrobo (sólo disponible si posees licencias de Endpoint Protection Plus o Fusion).

Envío de la URL por correo electrónico

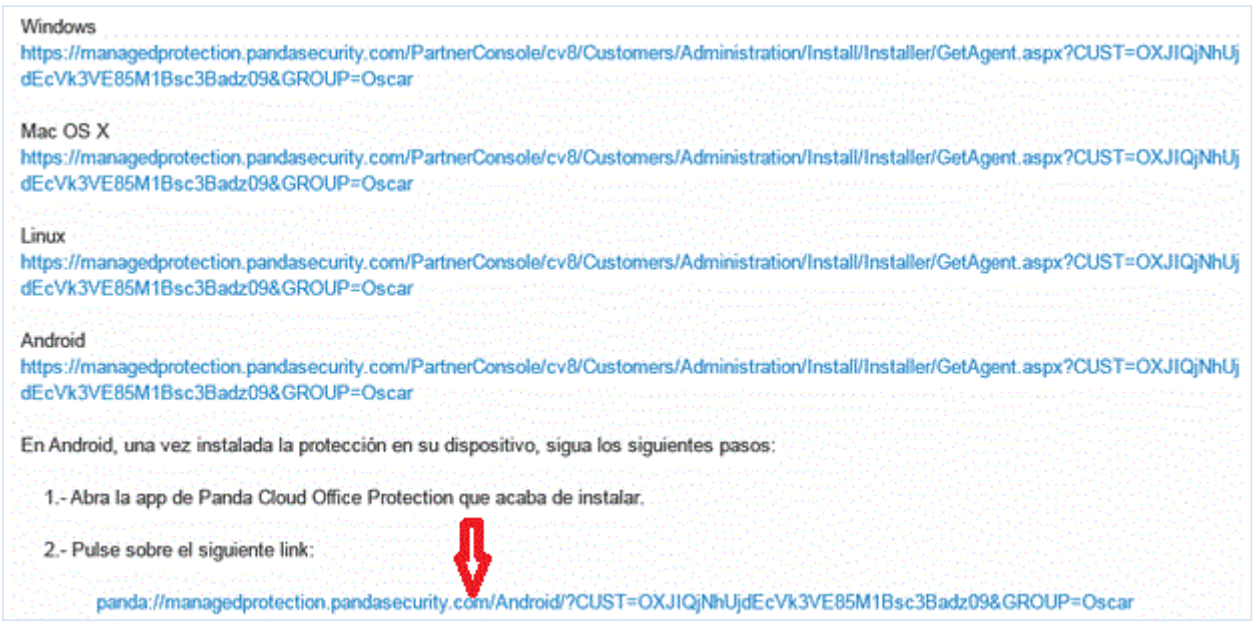
En este caso, la instalación se realiza desde el dispositivo Android, mediante una URL de instalación que se envía por correo electrónico.

1. En la consola Web de Endpoint Protection, selecciona el grupo en el que deseas integrar el dispositivo (por defecto está seleccionado el grupo por defecto) y haz clic en **Enviar por correo**.

2. Automáticamente, los usuarios recibirán un correo electrónico que contiene dos URL. La primera de ellas es la de instalación. Al hacer clic en ella, se accede a la página de Endpoint Protection de Google Play desde donde podrás realizar la instalación.

Vinculación del dispositivo y activación de la protección antirrobo

Una vez instalada la protección, es necesario abrir desde el dispositivo y a continuación hacer clic en la segunda URL que contiene el correo recibido anteriormente.


Windows
https://managedprotection.pandasecurity.com/PartnerConsole/cv8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST=OXJIQjNhUjdEcVk3VE85M1Bsc3Badz09&GROUP=Oscar

Mac OS X
https://managedprotection.pandasecurity.com/PartnerConsole/cv8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST=OXJIQjNhUjdEcVk3VE85M1Bsc3Badz09&GROUP=Oscar

Linux
https://managedprotection.pandasecurity.com/PartnerConsole/cv8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST=OXJIQjNhUjdEcVk3VE85M1Bsc3Badz09&GROUP=Oscar

Android
https://managedprotection.pandasecurity.com/PartnerConsole/cv8/Customers/Administration/Install/Installer/GetAgent.aspx?CUST=OXJIQjNhUjdEcVk3VE85M1Bsc3Badz09&GROUP=Oscar

En Android, una vez instalada la protección en su dispositivo, sigua los siguientes pasos:

1.- Abra la app de Panda Cloud Office Protection que acaba de instalar.

2.- Pulse sobre el siguiente link:

panda://managedprotection.pandasecurity.com/Android/?CUST=OXJIQjNhUjdEcVk3VE85M1Bsc3Badz09&GROUP=Oscar

Introduce el nombre con el que quieres identificar al dispositivo en la consola Web, haz clic en **Continuar** y activa los permisos necesarios para poder activar el antirrobo.

Para poder utilizar la protección antirrobo, es necesario disponer de licencias de Endpoint Protection Plus o Fusion. En caso de no disponer de estas licencias, acude a tu distribuidor habitual.

Ya ha finalizado el proceso de instalación e integración del dispositivo. El dispositivo se mostrará en el listado de la ventana **Equipos**, dentro del grupo que has seleccionado anteriormente.

15. Configurar la protección para equipos Windows/Linux

Configuración general del perfil

Configuración de la protección antivirus

Configuración de la protección firewall

Configuración del control de dispositivos

Configuración de la protección para servidores Exchange

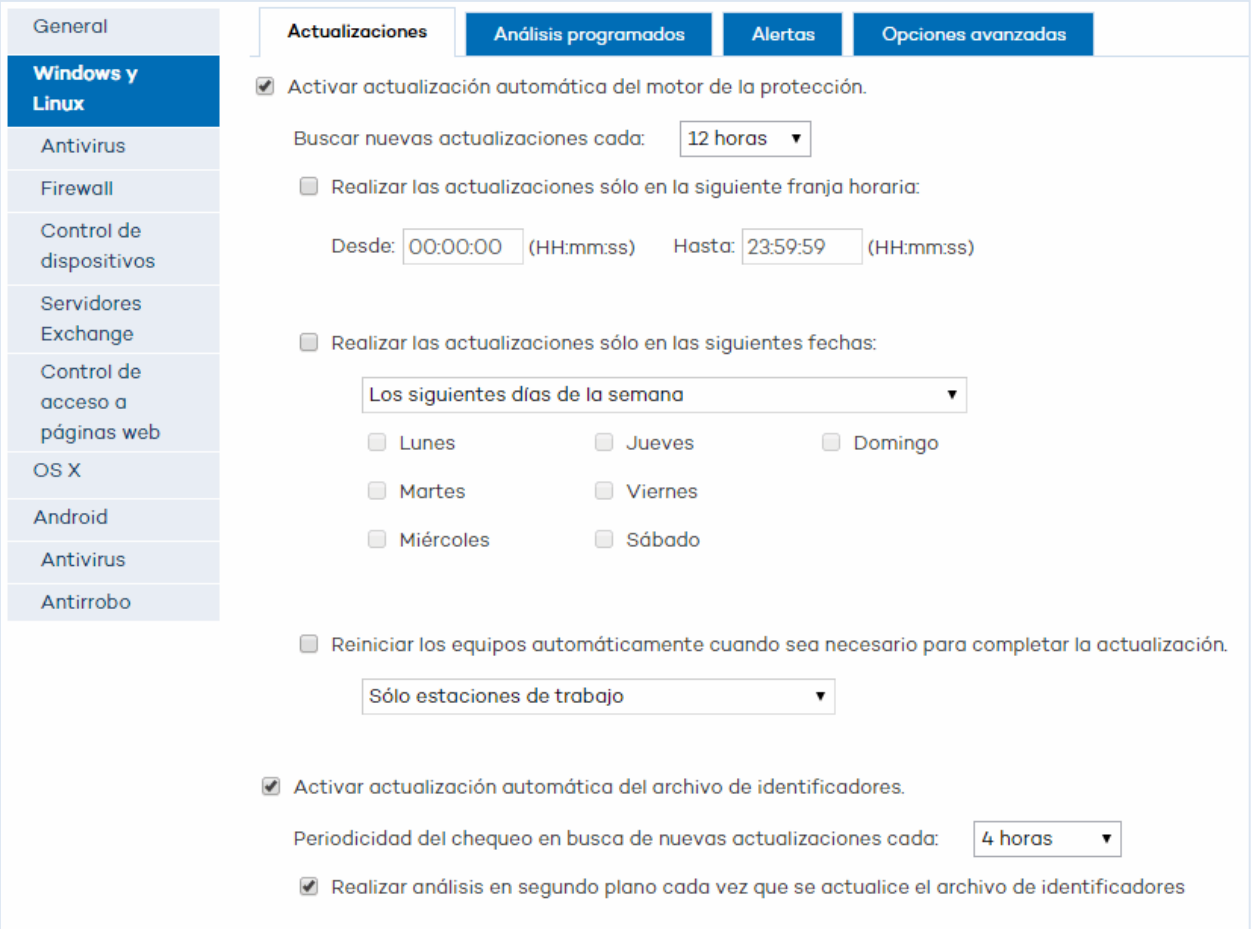
Configuración del control de acceso a páginas Web

15.1 Configuración general del perfil para Windows/Linux

15.1.1 Configuración de las actualizaciones

Para acceder a la configuración, haz clic en el menú **Configuración > Añadir nuevo perfil > Windows y Linux > Actualizaciones**.

Puedes utilizar las opciones que encontrarás en esta pestaña para realizar la configuración automática de la actualización tanto del motor de la protección como del archivo de identificadores.



Actualización automática del motor de la protección

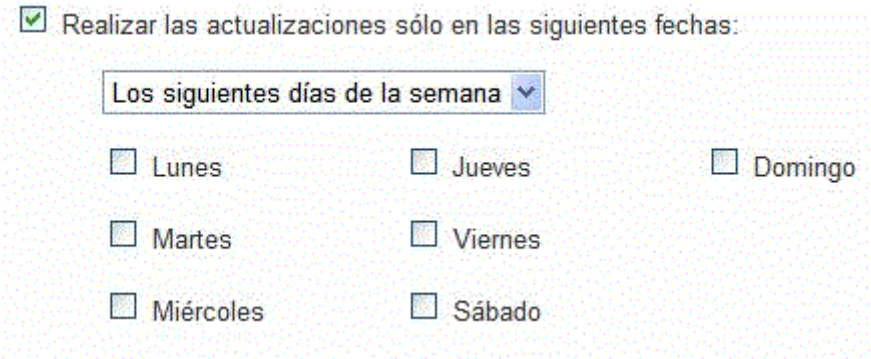
Equipos Windows

1. En primer lugar, marca la casilla de activación de las actualizaciones.

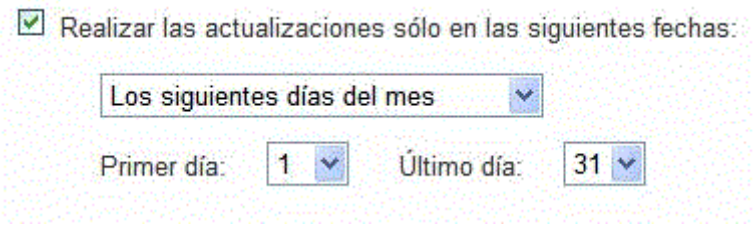
2. Utiliza el desplegable para establecer cada cuánto tiempo deseas que se busquen nuevas actualizaciones.

3. Si lo deseas, podrás establecer la fecha en la que tendrán lugar las actualizaciones automáticas y la franja horaria. Se permite seleccionar:

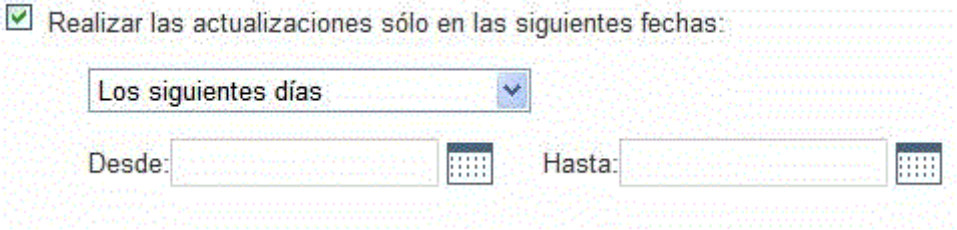
El día o los días de la semana en los que se quiere realizar la actualización.



El intervalo de días del mes en los que se realizará la actualización.



El intervalo de fechas en los que se realizará la actualización.



4. Y, para terminar, marca la casilla si deseas permitir que los equipos afectados por las actualizaciones -estaciones de trabajo, servidores o ambos- se reinicien cuando el proceso termine.

5. Haz clic en **Aceptar**.

Es recomendable que reinicies el equipo tan pronto como se muestre un mensaje en este sentido, aunque es posible que no sea necesario hacerlo hasta pasados varios días después de la actualización.

Equipos Linux

En el caso de los equipos con sistema operativo Linux no es posible realizar una actualización automática, por lo que cuando exista una nueva versión de la protección ésta deberá instalarse de nuevo en los equipos.

Cuando transcurran 7 días desde que exista una versión de la protección superior a la que los equipos tienen instalada, los equipos con sistema operativo Linux aparecerán como "desactualizados" en la ventana **Estado**, momento en el que el administrador podrá proceder a instalar la versión superior en los equipos.

Actualización automática del archivo de identificadores

Equipos Windows

1. Marca la casilla para activar la actualización automática.
2. Selecciona en el desplegable la periodicidad con la que deseas que se realice la búsqueda de actualizaciones.
3. Haz clic en **Aceptar**.

Equipos Linux

En el caso de los equipos con sistema operativo Linux, no es posible configurar la periodicidad de la actualización automática del archivo de identificadores.

Se hará siempre cada 4 horas.

15.1.2 Configuración de análisis programados

Equipos con sistema operativo Windows/Linux

Para acceder a la configuración, haz clic en el menú **Configuración > Añadir nuevo perfil > Windows y Linux > Análisis programados**.

Utiliza las opciones que se muestran en la pestaña **Análisis programados** para crear tareas de análisis, periódicas, puntuales o inmediatas y determinar si afectarán a todo el PC o a determinados elementos del mismo.

También puedes optar por programar análisis exclusivos de los discos duros o especificar las rutas concretas en las que se encuentran las carpetas o archivos que desees analizar.

A medida que vayas creando tareas de análisis, éstas se irán añadiendo en el listado principal de la pestaña **Análisis programados** de la ventana **Editar perfil**, desde donde podrás editarlas o eliminarlas.

Pasos a seguir para la configuración de los análisis

En primer lugar, haz clic en el botón **Nuevo** para acceder a la ventana **Edición de perfil – Nueva tarea de análisis**.

Sigue los siguientes pasos:

1. **Nombre:** indica el nombre con el que quieres identificar el análisis que vas a programar.

2. **Tipo de análisis:** selecciona el tipo de análisis que vas a crear: inmediato , programado o periódico.

   Análisis inmediato

   Una vez configurado el análisis, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de Endpoint Protection y se constate que se ha producido alguna modificación en la configuración de la protección.

   Análisis programado

   El análisis tendrá lugar en la hora y fecha que tú determines en **Fecha de comienzo** y **Hora de comienzo**.

   Análisis periódico

   Determina **Fecha y hora de comienzo** y selecciona en el desplegable **Repetición** la periodicidad que deseas adjudicar al análisis.

3. **Analizar**: selecciona la opción que deseas:

   - Todo el PC

   - Discos duros

   - Otros elementos: Utiliza esta opción para analizar elementos concretos almacenados (archivos, carpetas,...). Tendrás que introducir la ruta en la que se encuentra el elemento a analizar. El formato de la ruta ha de empezar por \\equipo, \\IP o (letra de unidad):\ Ejemplos:

   * *equipo**carpeta*

   * *c:\carpeta1\carpeta2*

   El número máximo de rutas a analizar que podrás introducir por cada perfil es 10. En función del permiso que poseas, podrás establecer rutas específicas de análisis. Para más información, consulta el apartado Tipos de permisos (capítulo 10).

En Linux se deben seleccionar rutas en formato Linux. *Ejemplo: /root/documents*

4. **Fecha de comienzo**: indica la fecha de realización del análisis.

5. **Hora de comienzo:** especifica la hora del análisis, teniendo en cuenta si la hora es la marcada por el equipo (local) o por el servidor de Endpoint Protection.

6. **Repetición**: en el caso de que el análisis sea del tipo periódico, especifica aquí la periodicidad del mismo (diaria, semanal o mensual).

15.1.3 Opciones avanzadas de análisis

A esta ventana se accede a través del vínculo **Opciones avanzadas** de la pantalla **Edición de perfil - nueva tarea de análisis**.

Aquí podrás configurar aspectos complementarios de los análisis programados con anterioridad.

Sigue los siguientes pasos:

1. Haz clic en el vínculo **Opciones avanzadas**. Se mostrará la ventana **Opciones avanzadas de análisis**.

2. Si deseas activar el análisis de archivos comprimidos, marca la casilla correspondiente.

3. Selecciona el software malintencionado que deseas analizar.

4. Puedes analizar todo por defecto o excluir del análisis determinadas extensiones, carpetas o archivos. En este caso utiliza los botones **Añadir, Vaciar** y **Eliminar** para conformar la lista de exclusiones.

Equipos con sistema operativo Linux

En la configuración avanzada de los análisis nuevos que se creen, no todas las opciones están disponibles en Linux.

Estas son las opciones avanzadas de análisis soportadas en Linux:

- Analizar archivos comprimidos.
- Analizar virus (siempre está activa).
- Analizar sospechosos.

El análisis de herramientas de hacking y programas potencialmente no deseados (PUPs) estará siempre activo; sin embargo, las exclusiones no.

Por favor, ten en cuenta que en Linux no hay protección en tiempo real. El método para proteger los equipos pasa por la realización de análisis bajo demanda o la programación de análisis periódicos.

15.1.4 Configuración de alertas

Para acceder a la configuración, haz clic en el menú **Configuración > Añadir nuevo perfil > Windows y Linux > Alertas**.

Aquí podrás configurar las alertas que se mostrarán cuando se detecte malware en los equipos, intentos de intrusión o dispositivos no permitidos y si estas alertas serán de tipo local, por correo, o de las dos maneras.

La diferencia entre ambas está en que la alerta local se mostrará en el equipo o equipos en los que se produjeron las detecciones, mientras que si optas por activar la alerta por correo, cada equipo en el que se produce la detección enviará una alerta en forma de mensaje de correo electrónico a la cuenta o cuentas habilitadas. Para ello:

1. En primer lugar, activa la casilla **Enviar alerta por correo.**
2. Cumplimenta el campo **Asunto del mensaje**.
3. Introduce la dirección de correo y especifica el servidor SMTP que se utilizará para enviar las alertas. En el caso de que el servidor requiera autenticación, introduce el usuario y la contraseña necesarios.
4. Haz clic en **Aceptar**.

15.1.5 Configuración de opciones avanzadas

Para acceder a la configuración:

1. Haz clic en el menú **Configuración.**
2. Haz clic en el perfil que deseas configurar.
3. En la columna de la izquierda haz clic en **Windows y Linux.**
4. Haz clic en **Opciones avanzadas.**

Aquí puedes especificar aspectos que tienen que ver con la instalación de la protección en los equipos, así como con la conexión de éstos a Internet y a los servidores de Endpoint Protection. También podrás configurar opciones relacionadas con la cuarentena de los archivos sospechosos.

Instalación

Especifica en qué directorio quieres instalar la protección. Endpoint Protection muestra por defecto una ruta que puedes modificar.

Desde aquí podrás especificar si deseas que Endpoint Protection desinstale los productos de la competencia instalados en el equipo, o si por el contrario, quieres que ambos productos convivan.

Si deseas conocer cuál es el comportamiento por defecto establecido para las diferentes versiones de la protección (versión trial o versión comercial) consulta el capítulo 13.

Instalación en equipos Linux

En el caso de los equipos con sistema operativo Linux, la instalación se realiza en un directorio por defecto que no puede ser modificado.

Conexión con la Inteligencia Colectiva

El administrador podrá desactivar los análisis con la inteligencia Colectiva. Es recomendable mantener activa esta opción si deseas disfrutar de toda la protección que la Inteligencia Colectiva proporciona.

La conexión en equipos Linux

En el caso de los equipos con sistema operativo Linux, no es posible desactivar la conexión con la Inteligencia Colectiva, por lo que siempre que los equipos estén conectados a Internet la protección instalada en ellos se alimentará de la Inteligencia Colectiva.

Opciones de conexión con el servidor

Determina cada cuánto tiempo deseas que el equipo envíe información a los servidores de Endpoint Protection acerca del estado de la protección instalada.

Modifica, si así lo deseas, el número de horas que la aplicación muestra por defecto, pero siempre en un intervalo entre 12 y 24.

También puedes especificar el equipo a través del cual deseas que se centralicen las conexiones con el servidor de Endpoint Protection.

Para ello, marca la casilla y haz clic en el botón **Seleccionar**. En la pantalla **Selección de equipo** elige el equipo o búscalo mediante el botón **Buscar**. A continuación Haz clic en **Aceptar**.

Requisitos del equipo que se utilizará para realizar las conexiones con el servidor:

Conexión a internet.

1. Mínimo de 128 MB de RAM.
2. Deberá ser un equipo protegido (equipo perteneciente al listado de equipos protegidos) y además deberá disponer de una versión de agente 5.04 o superior.
3. No puede ser un equipo sin licencia o excluido.
4. No deberá llevar más de 72 horas sin conectarse con el servidor.

Opciones de cuarentena

Los archivos que se encuentran en situación de cuarentena son analizados hasta determinar si suponen una amenaza o no.

En caso de no ser una amenaza, puedes optar por restaurarlos, utilizando para ello la opción **Restaurar** de la ventana **Cuarentena** e indicando la ruta del directorio en el que se restaurarán.

Contraseña de administración

Esta opción no está disponible para equipos con sistema operativo Linux u OS X.

La contraseña de administración te permite realizar tareas de desinstalación y configuración de la protección local en modo administrador. Es decir, con la misma contraseña podrás desinstalar Endpoint Protection de los equipos en los que lo has instalado o permitir que sea el usuario de dichos equipos quien active o desactive las protecciones desde la consola local de Endpoint Protection. No se trata de opciones excluyentes, por lo que puedes optar por seleccionar ambas a la vez si así lo deseas.

Consulta el apartado modo administrador.

El modo administrador

El modo administrador resulta muy útil porque mediante él puedes realizar las modificaciones que desees en la protección instalada en los equipos y hacerlo desde esos mismos equipos.

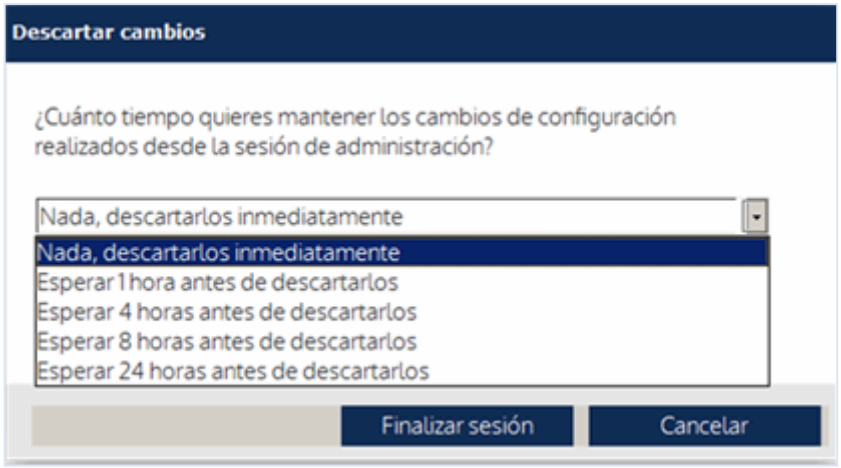
Al ser conocedor de la contraseña de administración, podrás acceder en cualquier momento y desde cualquiera de los equipos al panel del administrador sin necesidad de trasladarte hasta el lugar en el que se ubica el equipo desde el que te conectas a la consola Web.

Bastará con que hagas clic en el vínculo **Panel del administrador** e introduzcas la contraseña de administración.

Evidentemente, si alguno de los usuarios de estos equipos conoce la contraseña de administración, también podrá realizar modificaciones en las configuraciones y activar o desactivar las protecciones antivirus y firewall.

15.2 Modificar el estado de las protecciones

Una vez que has introducido la contraseña, se muestra el panel del administrador con información sobre el estado de las protecciones instaladas en el equipo. Aquí podrás activar o desactivar las protecciones.



Vigencia de los cambios realizados

Cualquier cambio que el administrador realice en las configuraciones será de carácter temporal. Al cerrar la sesión de administrador, tendrá que indicar durante cuánto tiempo quiere que estén vigentes los cambios. Los cambios también serán descartados si transcurren 6 horas sin realizar cambios en esta pantalla.

Durante el periodo de tiempo indicado por el administrador, la protección despreciará las solicitudes de modificación que le sean solicitadas por los servidores de Endpoint Protection. Una vez finalizado el periodo de vigencia de las modificaciones establecido por el administrador, se volverán a tener en cuenta los requerimientos procedentes de los servidores de Endpoint Protection de acuerdo con la configuración del perfil de la protección para el equipo.

15.3 Configuración de la protección antivirus

15.3.1 Pestañas Archivo, Correo y Web

Para acceder a la configuración, haz clic en el menú **Configuración** > **Añadir perfil** > **Antivirus**.

Mediante las pestañas **Archivos, Correo y Web** puedes configurar el comportamiento general de la protección permanente antivirus para el perfil que estás creando.

Pestaña Archivos

Aquí puedes configurar el comportamiento básico de la protección antivirus en lo que a la protección de archivos se refiere.

Selecciona la casilla **Activar protección permanente de archivos**.

1. A continuación, marca la casilla correspondiente si deseas que la protección de archivos incluya a los archivos comprimidos.

2. Selecciona los tipos de malware que deseas que sean detectados por la protección.

> ***La detección de virus se encontrará activa siempre que la protección de archivos lo esté.***

A continuación, selecciona si deseas que se bloqueen acciones maliciosas y la detección de archivos sospechosos en función de su comportamiento.

La protección permanente no se aplica a los equipos con sistema operativo Linux.

Si deseas profundizar en esta configuración, haz clic en **Opciones avanzadas**. Accederás a la ventana **Opciones avanzadas Antivirus - Protección de Archivos**.

Pestaña Correo

En esta ventana puedes configurar cuál va a ser el comportamiento de la protección antivirus del perfil que estás creando, en lo que a correo electrónico se refiere.

Si deseas profundizar en la configuración de dicho comportamiento, haz clic en **Opciones avanzadas**. Accederás a la ventana **Opciones avanzadas Antivirus - Protección de Correo**

1. Activa la protección permanente de correo y la de archivos comprimidos si deseas que la protección se aplique también a este tipo de archivos.

2. Selecciona el tipo de malware que deseas detectar. Marca la casilla correspondiente.

Haz clic en **Aceptar**.

Pestaña Web

Desde aquí puedes configurar el funcionamiento de la protección para la navegación Web. De esta manera evitarás verte afectado por malware o phishing procedente de páginas Web.

Esta protección va desactivada por defecto. Para activarla, Sigue los siguientes pasos:

1. Marca la casilla para activar la protección permanente para navegación Web.

2. Si deseas activar la detección de phishing en las páginas Web, marca la casilla correspondiente.

La detección de virus se encuentra activada por defecto.

En el panel **Detecciones por tipo** de la ventana **Estado** se contabilizarán las detecciones realizadas en URLs con phishing dentro de la categoría **Phishing**, y las de URLs con malware dentro de la categoría **Otros**.

Estas detecciones también se muestran en:

- El informe de detección.

- En los informes.

Las detecciones de URL con Phishing se contabilizan como Phishing y las de URL con malware se contabilizan dentro de la categoría **Otros**. Cualquier phishing o malware detectado por esta protección, será bloqueado.

Las detecciones de malware y phishing reportadas por la protección de navegación Web no se contabilizan como categorías bloqueadas.

15.3.2 Análisis locales

Una vez instalada la protección en los equipos, puedes acceder a las diferentes opciones de análisis mediante el menú contextual de windows o desde el menú contextual de la propia protección.

Análisis contextual sobre un elemento seleccionado

Selecciona una carpeta, unidad, archivo o cualquier otro elemento analizable y haz clic sobre él con el botón derecho. A continuación, aparecerá el menú contextual de windows, donde podrás seleccionar la opción **Analizar con Endpoint Protection**.

Inmediatamente se lanza el análisis del elemento. Este análisis puede ser detenido y reanudado con posterioridad. Cuando finaliza, muestra el resultado del análisis y te da la posibilidad de imprimir o exportar el informe y guardarlo en la ubicación que desees.

Análisis locales desde Endpoint Protection

- Análisis optimizado

Al seleccionar esta opción, Endpoint Protection examinará las carpetas del PC donde suele ocultarse el malware, para poder detectar y eliminar las amenazas en el menor tiempo posible.

- Otros análisis

Al hacer clic en esta opción dispondrás de las siguientes dos opciones:

- Analizar todo mi PC

Esta opción analizará de forma exhaustiva todos los elementos de tu PC: todas las unidades de disco, la memoria, etc. La duración de este análisis dependerá de la cantidad de datos almacenados en tu PC, así como de las características de tu equipo.

- Analizar otros elementos...

Esta opción es la más adecuada cuando sólo quieres analizar algún archivo concreto, alguna carpeta, etc. Es decir, te permite analizar sólo aquello que te interesa en un momento concreto, sin tener que realizar un análisis completo del PC. Una vez seleccionada esta opción, localiza las carpetas o archivos que desees analizar y haz clic en **Comenzar**.

Nota importante: Asegúrate de que tu PC está conectado a Internet antes de comenzar el análisis para garantizar la máxima capacidad de detección.

Aparte de estos análisis, que puedes realizar cuando desees, Endpoint Protection te protege también de forma permanente analizando todos los archivos que abres o ejecutas en cada momento, y neutralizando las posibles amenazas.

15.3.3 Opciones avanzadas antivirus - protección de archivos

En esta ventana puedes configurar con detalle la protección antivirus que deseas para un perfil, en lo que a la protección de archivos se refiere.

Accederás a esta ventana desde **Antivirus** > pestaña **Archivos** > **Opciones avanzadas.**

Analizar todos los archivos cuando se crean o modifican

Puedes hacerlo en base a un criterio general para todo tipo de archivos. Esto quiere decir que todos los archivos serán analizados en el momento en que se crean o modifican.

Aunque esta opción no supone en sí un aumento de la protección -de hecho, disminuye el rendimiento- lo que sí propicia es rapidez, entendida ésta como la inmediatez que supone analizar los archivos en el mismo momento en que son creados o modificados.

La alternativa es analizar solo aquéllos archivos con determinado tipo de extensión. Para ello, podrás excluir del análisis las extensiones, carpetas o archivos que indiques.

Exclusiones

En cada uno de los casos, utiliza los botones **Añadir**, **Eliminar** y **Vaciar** para conformar la lista de elementos (extensiones, carpetas, archivos) a excluir de los análisis.

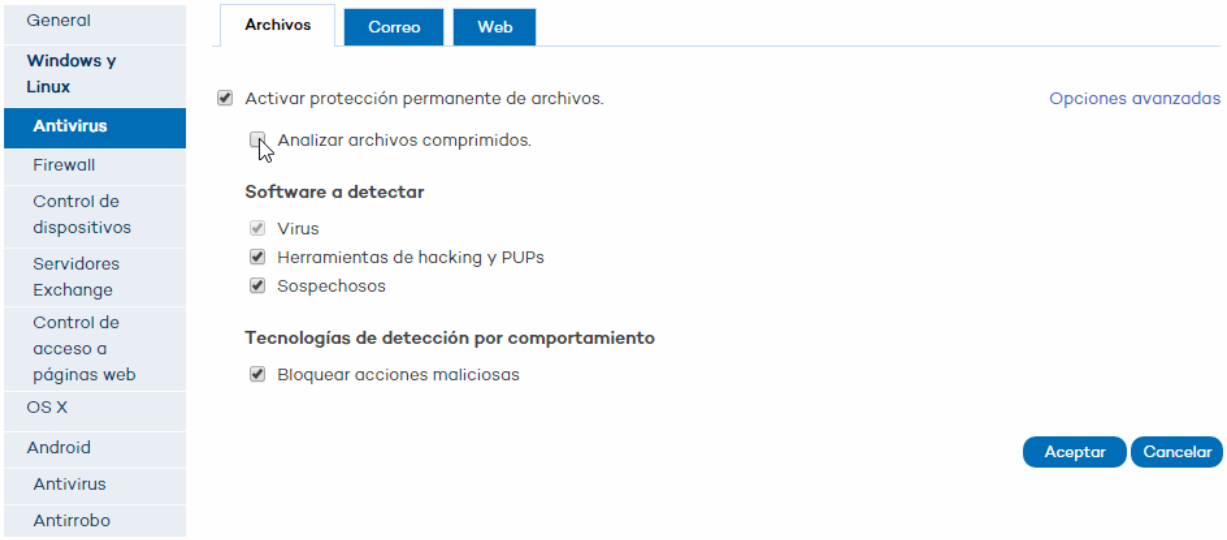
Cuando hayas finalizado, haz clic en **Aceptar** para guardar los cambios.

15.3.4 Opciones avanzadas antivirus - protección de correo

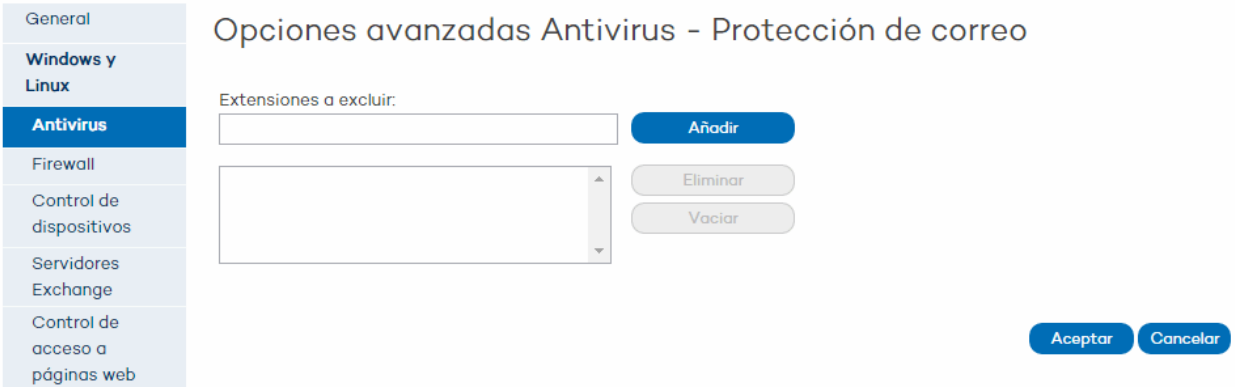
Endpoint Protection te ofrece la posibilidad de activar la protección de correo (esta protección está desactivada por defecto). Esta protección te ayudará a mantener un nivel óptimo de seguridad en tus equipos informáticos, protegiéndolos de las amenazas que puedan llegar a través de sistemas de correo electrónico.

1. Haz clic en **Antivirus** > pestaña **Correo.**
2. Marca la casilla **Activar protección permanente de correo**

3. Marca la casilla correspondiente si deseas que el análisis de correo incluya a los archivos comprimidos. Selecciona también el tipo de malware que deseas detectar.



4. Haz clic en el vínculo **Opciones avanzadas**. Se mostrará la ventana **Opciones avanzadas antivirus-Protección de correo**.



Endpoint Protection te permite elaborar una lista de extensiones sobre las que no se realizará análisis. Utiliza para ello los botones **Añadir**, **Eliminar** y **Vaciar**.

Cuando hayas finalizado, haz clic en **Aceptar** para guardar los cambios.

15.4 Configuración de la protección firewall

15.4.1 Introducción

Para acceder a la configuración, haz clic en el menú **Configuración** > **Perfiles** > **Añadir perfil** > **Firewall**.

Lo primero que debes hacer a la hora de configurar la protección del firewall es decidir si los usuarios pertenecientes al grupo al que se aplique este perfil configurarán el firewall desde sus equipos (firewall en modo usuario) o si serás tú, como administrador, quien se encargue de ello (firewall en modo administrador).

Firewall en modo usuario

Seleccione la opción que permite que la configuración del firewall la establezca el usuario de cada equipo.

En este caso consulta la sección Firewall en modo usuario

Firewall en modo administrador

Si, por el contrario, prefieres que la configuración se realice desde la consola Web, serás tú, como administrador, quien establezca las limitaciones, bloqueos, permisos, en definitiva, la configuración del firewall que se aplicará a los equipos que elijas.

Si optas por este método de administración centralizada del firewall desde la consola Web, mantén la opción por defecto **Aplicar la siguiente configuración al firewall.**

También tendrás que establecer si la configuración de la protección firewall se aplicará a servidores y/o estaciones Windows. Utiliza para ello las casillas correspondientes.

A continuación podrás realizar todo el proceso de configuración a través de las opciones que encontrarás en las pestañas General, Programas, Prevención de intrusiones y Sistema.

15.4.2 Firewall en modo usuario

El usuario podrá acceder a la configuración del firewall siempre y cuando haya sido autorizado para ello por el administrador de Endpoint Protection, tal y como se ha comentado en el apartado Introducción a la configuración del firewall.

Mediante la configuración del firewall, el usuario no sólo filtra las conexiones que entran y salen del ordenador cuando éste se conecta a Internet, sino que también interviene en las conexiones establecidas entre su equipo y otros equipos de la red con los que puede intercambiar archivos y compartir carpetas e impresoras, entre otras cosas.

Cada vez que un programa intente conectarse a Internet desde el equipo del usuario (conexiones salientes), o cuando se produzca un intento de conexión desde el exterior al PC del usuario (conexiones entrantes), Endpoint Protection preguntará al usuario si desea autorizar dicha conexión. Para ello utilizará un sistema de avisos mediante los que se podrán autorizar o no las conexiones y configurar aspectos relativos a las mismas.

Si deseas denegar o autorizar permanentemente la conexión en cuestión, puedes hacerlo seleccionando la opción correspondiente en el aviso que se mostrará.

En el caso de las conexiones salientes, si marcas la opción Activar asignación automática de permisos, Endpoint Protection no preguntará si autoriza las conexiones y las realizará de manera automática.

De este modo, a medida que el usuario asigne permisos y concrete la configuración, obtendrá un control total de las conexiones que se establezcan desde su ordenador a la red local e Internet, y viceversa.

Encontrarás toda la información sobre la configuración del firewall en:

- Conexión de programas a la Red
- Prevención de intrusiones
- Reglas de sistema

Desinstalación de Endpoint Protection

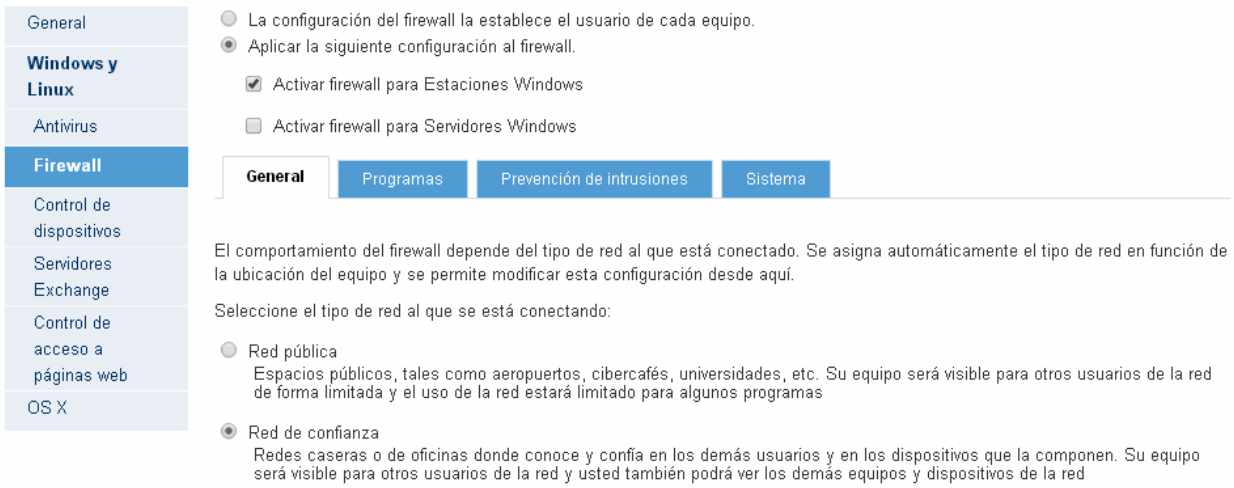
Al estar configurado el firewall en modo usuario, la desinstalación se podrá llevar a cabo desde el panel de control de Windows.

Si, por el contrario, el firewall está configurado en modo administrador, para desinstalar será necesario contar con la contraseña necesaria.

15.4.3 Firewall en modo administrador

Activar el firewall en modo administrador

1. Para acceder a la configuración, haz clic en el menú **Configuración**
2. Haz clic en el icono de **Añadir perfil (+)** y haz clic en **Firewall**, en la columna de la parte izquierda de la ventana.
3. Selecciona la casilla **Aplicar la siguiente configuración al firewall.**
4. Selecciona si deseas aplicar la configuración del firewall a estaciones y/o servidores Windows.
5. Marca la casilla correspondiente al tipo de red al que se conectará. La configuración será más restrictiva si se trata de una ubicación pública y más flexible si la ubicación es de confianza.



Red pública

Una red de este tipo es propia de cyberlocales, aeropuertos, etc. Conlleva limitación de su nivel de visibilidad y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Red de confianza

Este tipo de red generalmente es de oficina o casera. El equipo es perfectamente visible para el resto de equipos de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

Haz clic en **Aceptar**.

En la ventana principal, también se mostrará el vínculo **Panel del administrador**. Al hacer clic en él, el usuario habrá de introducir la contraseña de administración necesaria para activar o desactivar las protecciones, realizar modificaciones en sus configuraciones, etc.

Conexión de programas a la Red

Haz clic en el menú **Configuración** > **Perfiles** > **Añadir perfil** > **Firewall** > **Programas**.

1. Activa las reglas de Panda. Se trata de unas reglas predefinidas para las aplicaciones más comunes, y que te pueden facilitar las tareas de configuración. Pueden ser modificadas, pero no eliminadas.
2. Añade programas y asígnales permisos de comunicación. Para ello, haz clic en **Añadir**.
3. Modifica o elimina los programas añadidos, mediante los botones **Configurar** y **Eliminar**.
4. Decide si quieres permitir o denegar el acceso a comunicaciones para los que no exista una regla determinada. Utiliza para ello la lista desplegable **Acción**

Los permisos pueden ser:

- Permitir entrantes y salientes

El programa se podrá conectar a la red (Internet y redes locales) y también permitirá que otros programas o usuarios se conecten con 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 salientes

El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.

- Permitir entrantes

El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos de salida.

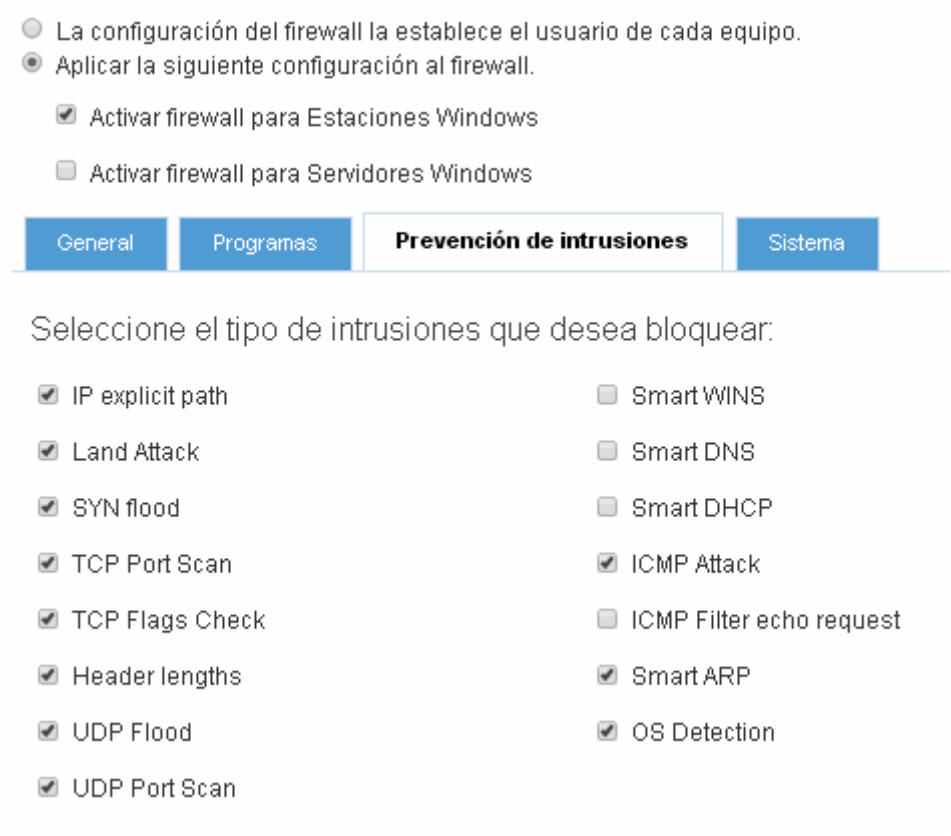
- No permitir ninguna conexión

El programa no podrá acceder a la red.

Prevención de intrusiones

Haz clic en el menú **Configuración > Añadir perfil > Firewall** > **Prevención de intrusiones.**

Aquí podrás configurar cuál será el comportamiento de la protección firewall en cada perfil en lo que a prevención de intrusiones se refiere.



Selecciona las casillas correspondientes y haz clic en **Aceptar**.

Reglas de sistema

Haz clic en el menú **Configuración** > **Perfiles** > **Añadir perfil** > **Firewall** > **Sistema**.

- ¿Qué son las reglas de sistema?

Mediante las reglas de sistema puedes establecer reglas de conexión que afectarán a todo el sistema, y que son prioritarias con respecto a las reglas configuradas anteriormente para la conexión de los programas a la red.

A medida que vayas creando reglas de sistema, éstas aparecerán en el listado. El orden de las reglas en la lista no es aleatorio, es decir, su aplicación va en orden descendente, por lo que al desplazar una regla hacia arriba o abajo modificarás la prioridad en su aplicación.

- Creación de reglas de sistema

Activa las reglas de sistema. Se trata de unas reglas predefinidas que te pueden facilitar las tareas de configuración.

Para añadir reglas de sistema haz clic en el botón **Añadir**. Accederás a la ventana **Edición de perfil-nueva regla de sistema**, donde podrás seleccionar la acción que deseas denegar o permitir al sistema, elegir cuál será la dirección de la comunicación para dicha acción, y la red que se utilizará.

También puedes determinar el protocolo, puerto, y los PCs a los que se aplicará la regla, especificando su dirección IP, su dirección MAC o ambas.

Para modificar o eliminar alguna de las reglas y permisos establecidos, utiliza los botones **Configuración** y **Eliminar**.

15.5 Configuración del control de dispositivos

15.5.1 Introducción

Dispositivos de uso común como las llaves USB, las unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles pueden constituir también una vía de infección para los equipos cuya seguridad deseas preservar.

La opción de configuración del control de dispositivos te permite determinar cuál será el comportamiento de este tipo de protección para el perfil que estás creando. Para ello, seleccionarás el dispositivo o dispositivos que deseas autorizar y les asignarás un nivel de utilización.

Notificaciones

Según cómo sea la configuración para los dispositivos, se mostrará un aviso advirtiendo de ello.

- Dispositivos no permitidos

Cuando la protección detecte que se ha conectado al equipo un dispositivo cuyo uso no esté permitido por el perfil de seguridad aplicado a dicho equipo, se mostrará un aviso al respecto advirtiendo al usuario de que no tiene permiso para acceder a dicho dispositivo.

- Dispositivos con permiso de solo lectura

El dispositivo conectado se mostrará con normalidad en el directorio Mi PC del equipo. Al hacer doble clic sobre la unidad, se mostrará un aviso advirtiendo de que el usuario no tiene permiso para escribir en el dispositivo.

Para activar el control de dispositivos

1. Haz clic en el menú **Configuración** y selecciona un perfil de la lista de perfiles situados en la parte derecha de la ventana, bajo **Perfiles.**

2. En la ventana **Editar perfil**, selecciona **Control de dispositivos.**

3. Marca la casilla **Activar el control de dispositivos**.

4. A continuación, puede elegir en el desplegable correspondiente el nivel de autorización que deseas aplicar al dispositivo que te interesa configurar.

   En el caso de las llaves USB y las unidades CD/DVD, puedes elegir entre **Bloquear**, **Permitir lectura** o **Permitir lectura y escritura.**

   Para Bluetooth, dispositivos de imágenes, modems USB y teléfono móviles las opciones son **Permitir** y **Bloquear**.

   Haz clic en **Aceptar** para guardar la configuración del control de dispositivos.

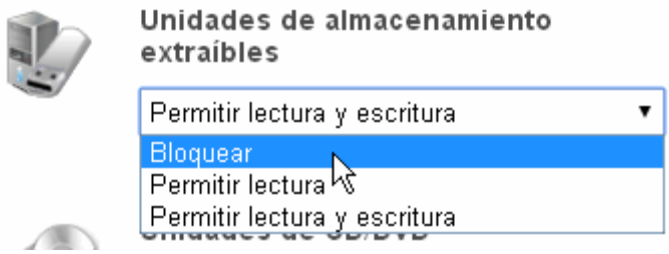
15.5.2 Elaborar una lista de dispositivos permitidos

Se puede dar el caso de que no autorices el uso de determinado tipo de dispositivos y que, sin embargo, necesites autorizar el uso de un dispositivo en particular de ese tipo en concreto.

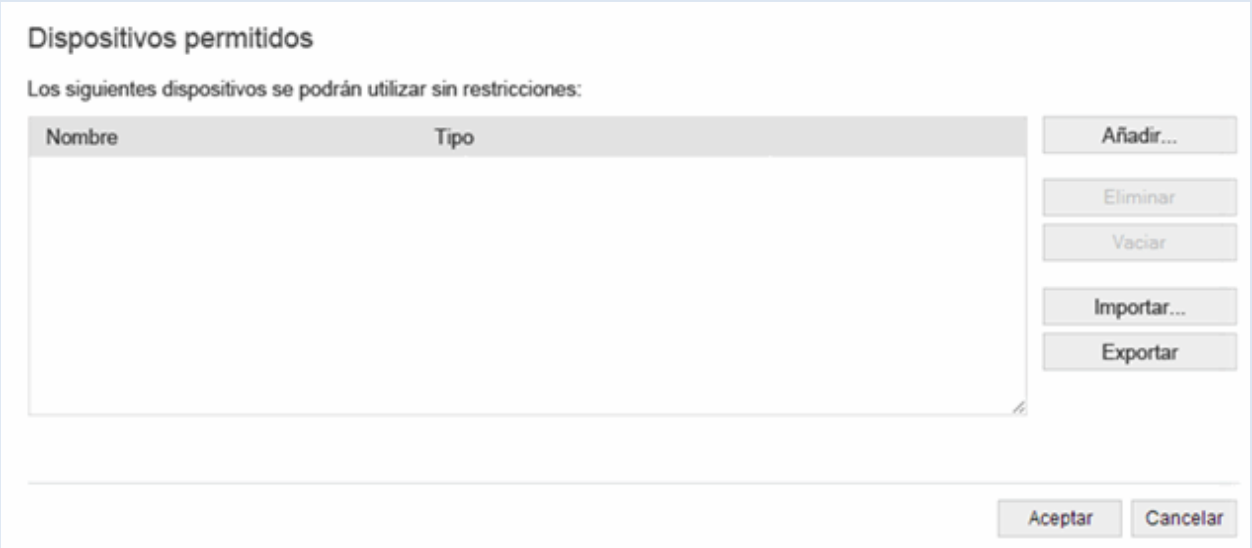
Puedes solventar esta situación elaborando una "lista blanca", es decir, una lista de dispositivos cuyo uso permitirás aunque sobre el papel pertenezcan a grupos de dispositivos que hayas marcado como no autorizados.

También podrás autorizar que un dispositivo sea excluido del bloqueo una vez detectado.

Por ejemplo, supongamos que deseas autorizar la utilización de una llave USB y tienes configurado el control de dispositivos de manera que bloquee este tipo de dispositivos:



Puedes hacerlo en el apartado **Dispositivos permitidos**



1. Haz clic en **Añadir**.
2. En la lista de dispositivos que aparece, selecciona el que deseas autorizar y haz clic en **Aceptar**.

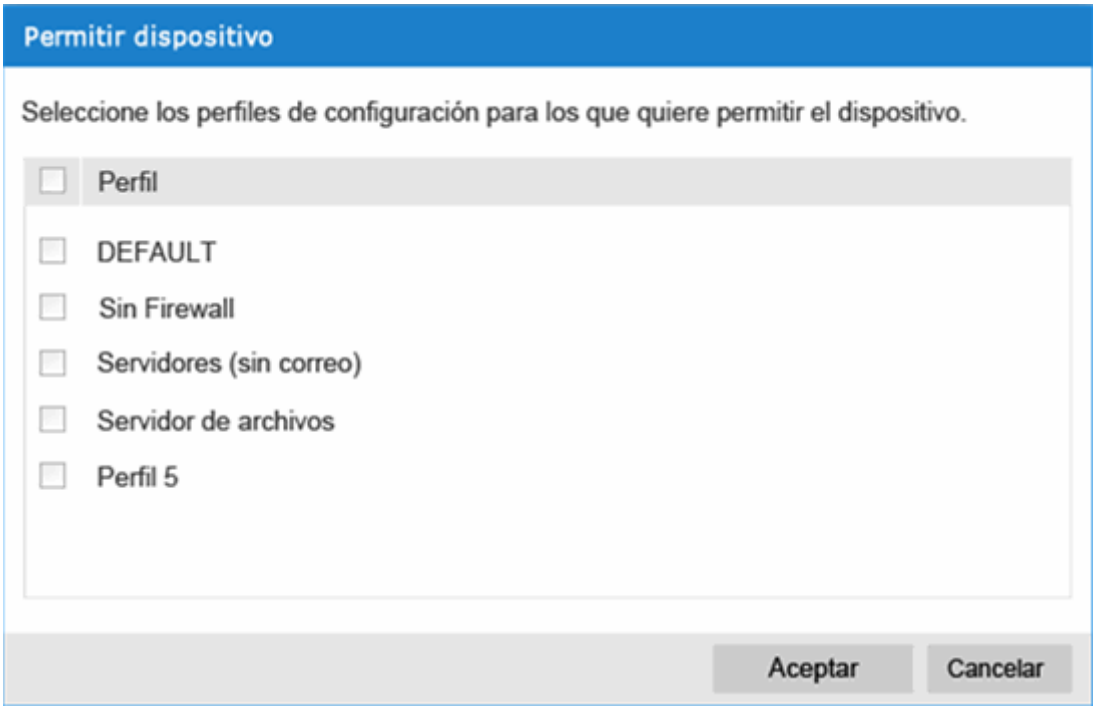
Una vez que hayas configurado la lista de dispositivos que deseas autorizar, puedes importarla o exportarla a formato .txt. Utiliza los botones correspondientes para vaciar el listado o eliminar alguno de los dispositivos de la lista.

15.5.3 Autorizar un dispositivo una vez detectado

Cada vez que un dispositivo no autorizado intenta conectarse al equipo, Endpoint Protection toma nota de ello y lo refleja en el detalle de detecciones.

Este listado de detecciones está disponible desde la ventana **Estado** > **Origen de las detecciones** > **Detalle de detecciones** > **Amenazas detectadas** > **Dispositivos bloqueados**.

Dentro del detalle de la detección encontrarás el botón **Permitir este dispositivo.** Si haces clic en dicho botón podrás seleccionar a qué perfiles de la protección afectará la autorización del dispositivo, es decir, el dispositivo se incluirá en la lista de dispositivos permitidos para los perfiles seleccionados.



Haz clic en **Aceptar** para guardar los cambios.

15.6 Configuración de la protección para servidores Exchange

15.6.1 Introducción

Si dispones de las licencias correspondientes, desde tu consola Web podrás activar la protección para servidores Exchange y aplicarla a cualquier servidor Exchange que esté administrando.

> ***Esta protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010 y 2013.***

La protección para servidores Exchange está compuesta por las unidades **Antivirus**, **Anti-spam** y **Filtrado de contenidos**.

Antivirus

Analiza en busca de virus, herramientas de hacking y programas potencialmente no deseados sospechosos, con destino a buzones situados en el servidor Exchange, así como el acceso a sus buzones y carpetas públicas.

Para saber más sobre esta protección, consulta Antivirus para la protección de servidores Exchange.

Anti-spam

Esta unidad se encarga de detectar y detener el spam.

Para saber más sobre esta protección, consulta Protección anti-spam para servidores Exchange.

Filtrado de contenidos

Mediante esta protección podrás establecer filtros para los mensajes de correo electrónico en función de cuál sea la extensión de los archivos adjuntos.

Para saber más sobre esta protección, consulta Filtrado de contenidos para servidores Exchange.

15.6.2 Monitorización de la protección para servidores Exchange

Al igual que sucede con el resto de protecciones que ofrece Endpoint Protection Plus, el estado de la protección para servidores Exchange se mostrará en la ventana Equipos, además de en los diferentes informes que Endpoint Protection Plus proporciona.

Las detecciones reportadas por la protección para servidores Exchange serán visibles en:

- La ventana Estado, dentro de la sección **Origen de las detecciones**, junto al resto de detecciones aportadas por las diferentes protecciones integradas en Endpoint Protection Plus.
- El listado de detecciones.
- Los informes de detección, informe ejecutivo e informe ejecutivo extendido.

15.6.3 Protección antivirus para servidores Exchange

Protección de buzones

Para acceder a la configuración de la protección Antivirus para servidores Exchange, haz clic en el menú **Configuración** > **Perfiles** > **Añadir perfil** > **Servidores Exchange** > pestaña **Antivirus**.

Aquí puedes configurar el comportamiento básico de la protección Antivirus en lo que a protección de buzones de correo electrónico se refiere.

1. Activa la casilla de verificación **Activar protección de buzones**.

   Al activar la protección de buzones, podrás mantener libres de software malintencionado los correos electrónicos almacenados en los buzones de correo administrados por tu servidor Exchange. De esta manera aumentará tu seguridad y evitarás el robo de datos y la pérdida de información.

2. En la sección **Software malintencionado a detectar** marca los elementos que deseas detectar.

   En las versiones anteriores a Microsoft Exchange 2013, existe una API de detección de virus que ofrece las funciones para el análisis de la protección de buzones.

En Exchange 2013 para interceptar el tráfico entre buzones se ha desarrollado un nuevo interceptador que recoge el tráfico entre buzones por SMTP (protocolo para la transferencia simple de correo electrónico).

- Modelo de actuación de la protección Antivirus de Buzones

En buzones se actuará sobre el elemento concreto que se ha detectado como malware o sospechoso, no sobre el mensaje completo (por ejemplo, si se detecta malware en un fichero adjunto, se actúa sobre el propio fichero adjunto).

La actuación se realiza de la siguiente forma:

1. Se realiza sobre el fichero en concreto la acción por defecto de la plataforma, determinada por el laboratorio: Desinfectar, Borrar, Mover a cuarentena...

2. Se notifica al usuario introduciendo un security_alert.txt.

3. Cuando se restaure de cuarentena, el correo se restaura al buzón de los destinatarios. Si se produce algún problema en esta restauración, se restaura directamente a la carpeta Lost&Found, dejando un fichero con el nombre del elemento insertado en cuarentena.

- Modelo de actuación de la protección Antivirus de buzones en Exchange 2013

La actuación en la protección de buzones de Exchange 2013 será equivalente a la actuación existente en la protección de transporte. La actuación será:

1. En caso de detectar malware o sospechosos los correos completos irán siempre a cuarentena.

2. Estos mensajes se mantienen en cuarentena un tiempo máximo:

Clasificación	Tiempo	Acción transcurrido el tiempo
Malware	7 días	Borrar
Sospechoso	14 días	Restaurar

3. Cuando un mensaje se mueve a cuarentena, se envía una notificación a los destinatarios del correo con el asunto original, avisando de que el correo ha sido bloqueado y de que contacte con su administrador si desea recuperar el mensaje.

4. Cuando se restaure de cuarentena, el correo se restaura al buzón de los destinatarios. Si se produce algún problema en esta restauración, se restaura directamente a la carpeta Lost&Found, dejando un fichero con nombre del asunto del mensaje. Este fichero contiene el mensaje completo.

Protección de transporte

Para acceder a la configuración de la protección antivirus para servidores Exchange, haz clic en el menú **Configuración** > **Perfiles** > **Añadir perfil** > **Servidores Exchange** > pestaña **Antivirus**.

Ahora puedes configurar el comportamiento básico de la protección Antivirus en lo que a protección de transporte se refiere.

1. Activa la casilla de verificación **Activar protección de transporte**.

   Al activar la protección de transporte asegurarás que los correos electrónicos que circulen a través de tus servidores Exchange lo hagan con total seguridad y libres de virus y malware.

2. En la sección **Software malintencionado a detectar** marca los elementos que deseas detectar.

- Modelo de actuación de la protección Antivirus de Transporte

En la protección de transporte se actúa sobre el correo completo de la siguiente forma:

1. En caso de detectar malware o sospechosos se mueven los correos completos a cuarentena, independientemente de la acción que se debe realizar. Estos mensajes se mantienen en cuarentena el tiempo establecido por Panda Security.

2. Cuando un mensaje se mueve a cuarentena, se envía una notificación a los destinatarios del correo con el asunto original avisando de que el correo ha sido movido a cuarentena y que contacte con su administrador si desea recuperar el mensaje

3. Cuando se restaure de cuarentena, el correo se restaura al buzón de los destinatarios. Si se produce algún problema en esta restauración, se restaura directamente a la carpeta Lost&Found, dejando un fichero con nombre del asunto del mensaje. Este fichero contiene el mensaje completo.

Análisis inteligente de buzones

Si eliges activar esta opción, la protección aprovechará los momentos de menor actividad de sus servidores Exchange para analizar en profundidad todos los correos electrónicos que almacenan.

Además de realizar el análisis en la franja horaria que menor impacto pueda tener en el normal funcionamiento de los servidores, solo serán analizados aquellos correos electrónicos que no lo hayan sido con anterioridad y que contengan archivos adjuntos.

Al desactivar la protección de buzones se deshabilita el análisis inteligente de buzones.

- Modelo de actuación en las detecciones reportadas por los análisis en Background

La actuación en la protección de background es igual a la de buzones.

Los análisis en background no están disponibles para Exchange 2013.

15.6.4 Protección anti-spam para servidores Exchange

La eliminación del correo basura -spam- de los servidores Exchange es una labor que requiere de mucho tiempo de dedicación. El spam no solo supone un gran peligro de estafa, sino que además es una enorme pérdida de tiempo que no tienes por qué soportar.

Para solucionar esta situación, puedes utilizar la protección anti-spam para servidores Exchange que te ofrece Endpoint Protection Plus. Así, conseguirás optimizar tu tiempo de trabajo y aumentar la seguridad de tus servidores Exchange.

Para activar o desactivar esta protección, utiliza la casilla de verificación **Detectar spam**.

Acción para mensajes de spam

Las acciones a llevar a cabo son:

- Dejar pasar el mensaje. Se añadirá la etiqueta *Spam* al Asunto de los mensajes. Esta será la opción configurada por defecto.
- Mover el mensaje a... Será necesario especificar la dirección de correo electrónico a la que se moverá el mensaje, con la etiqueta *Spam* añadida en el *Asunto*.
- Borrar el mensaje
- Marcar con SCL (*Spam Confidence Level*).

  SCL -*Spam Confidence Level*- es una escala de valores comprendidos entre el 0 y el 9 que se aplican a los mensajes de correo electrónico susceptibles de ser spam. Para ello se analizan su cabecera, asunto y contenido.

  El valor 9 se asigna a los mensajes que con total probabilidad son spam. El 0 es el valor que se aplica a los mensajes que no son spam.

  Este valor SCL se puede utilizar para marcar los mensajes que posteriormente serán tratados en función de un umbral configurable en Active Directory: la protección adjudica al mensaje el valor SCL correspondiente y le permite pasar.

  A continuación será el administrador, en función del umbral determinado en el Active Directory, quien seleccione la acción que finalmente se realizará con el mensaje.

Direcciones y dominios permitidos y denegados

Utilizando los botones **Añadir**, **Eliminar** y **Vaciar**, puedes configurar listas de direcciones y dominios cuyos mensajes no serán analizados por la protección anti-spam (*lista blanca*) o, por el contrario, otra lista de dominios y direcciones cuyos mensajes serán interceptados por la protección y eliminados (*lista negra*).

A la hora de configurar las listas es importante tener en cuenta lo siguiente:

1. Si un dominio se encuentra en la lista negra y una dirección perteneciente a dicho dominio se encuentra en la lista blanca, se permitirá dicha dirección, pero no el resto de direcciones del dominio.

2. Si un dominio se encuentra en la lista blanca y una dirección perteneciente a dicho dominio se encuentra en la lista negra, dicha dirección no será aceptada, pero sí el resto de direcciones de dicho dominio.

3. Si un dominio (por ejemplo: domain.com) se encuentra en la lista negra y un subdominio de este (ej: mail1.domain.com) se encuentra en la lista blanca, se permitirán direcciones de dicho subdominio, pero no el resto de direcciones del dominio o de otros subdominios diferentes.

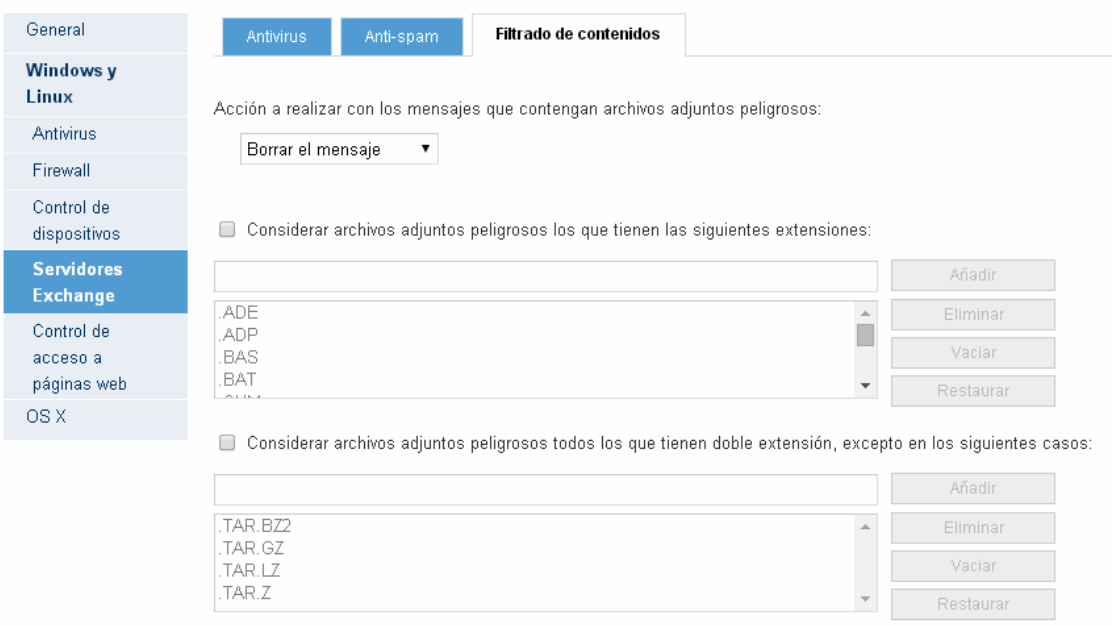
4. Si un dominio se encuentra en la lista blanca también se considerarán incluidos en la lista blanca todos sus subdominios.

15.6.5 Filtrado de contenidos para servidores Exchange

El filtrado de contenidos te permite filtrar los mensajes de correo electrónico en función de cuál sea la extensión de los archivos adjuntos incluidos en ellos.

Una vez establecida la lista de mensajes susceptibles de albergar adjuntos sospechosos, podrás indicar qué acción deseas que la protección realice con dichos mensajes.

También se puede aplicar el filtrado de contenidos a mensajes que incluyan adjuntos con dobles extensiones.



Archivos considerados peligrosos

Marca la casilla si deseas considerar como peligrosos los archivos adjuntos con alguna extensión determinada. Una vez marcada la casilla, utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de extensiones que deseas bloquear.

Archivos con doble extensión considerados peligrosos

El filtrado de contenidos impedirá la entrada de todos los mensajes de correo electrónico con adjuntos de doble extensión, excepto aquellos cuyos adjuntos tengan las extensiones que tú selecciones. Utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de dobles extensiones que sí permitirás.

Acción a realizar

Selecciona si deseas que los mensajes se borren o si prefieres desviarlos a otra dirección de correo electrónico. Esto puede resultarte útil para analizar a posteriori, con calma, los adjuntos recibidos y modificar si así lo deseas la lista de extensiones seleccionadas como peligrosas.

Haz clic en **Aceptar** y a partir de este momento sus servidores Exchange estarán a salvo de los archivos con adjuntos peligrosos.

15.7 Configuración del control de acceso a páginas Web

15.7.1 Configuración del control de acceso a páginas Web

Para acceder a la configuración, haz clic en el menú **Configuración** > **Perfiles** > **Añadir perfil** y selecciona **Control de acceso a páginas Web.**

Podrás activar esta protección de forma independiente para estaciones y servidores.

Si eres un cliente que acaba de adquirir la versión más reciente del producto, esta opción estará activada por defecto en estaciones. Sin embargo, estará desactivada por defecto en servidores.

Si tu versión del producto no es la más reciente, deberás activar esta funcionalidad en la consola Web. Para ello, deberás activar la casilla **Activar monitor de accesos a páginas Web**.

Con esta protección podrás restringir el acceso a determinadas categorías Web y configurar URLs a las que autorizarás o restringirás el acceso. Esto contribuirá a la optimización del ancho de banda de tu red y a la productividad de tu negocio.

Denegar el acceso a páginas Web

Las páginas Web se agrupan por categorías. Tan solo tendrás que seleccionar las categorías a las que deseas denegar el acceso, y podrás modificar las categorías seleccionadas siempre que lo desees.

1. Accede a **Configuración** y haz clic en el perfil para el que deseas configurar el acceso a páginas Web.

2. En la columna de la izquierda, haz clic en **Control de acceso a páginas Web**.

3. Marca la casilla correspondiente para activar el control de acceso a páginas Web para estaciones Windows, servidores Windows o ambos.

4. Selecciona las categorías a las que quieres denegar el acceso.

Cuando desde el equipo se intente acceder a una página Web que pertenece a una categoría de las anteriores, se mostrará un aviso al respecto. Recuerda que puedes configurar la aparición o no de estos avisos. Consulta el apartado Configuración de alertas.

Denegar el acceso a páginas de categoría desconocida

En el caso de páginas no categorizadas, puedes optar por denegar el acceso también. Para ello no tienes más que activar la casilla correspondiente.

Es importante que tengas en cuenta que en el caso de Intranets o Webs de tipo interno que se conectan a través de los puertos 80 u 8080, puede suceder que se clasifiquen como pertenecientes a una categoría desconocida y, por tanto, se deniegue el acceso a ellas con el consiguiente perjuicio para los usuarios.

Por eso es conveniente que analices a fondo cual es la situación de estas conexiones antes de activar esta opción, aunque siempre puedes optar por mantener activada la denegación de acceso a páginas de categoría desconocida y "rescatar" las páginas Web que necesitas mediante su inclusión en la lista de direcciones y dominios permitidos.

- Modificación de las categorías permitidas/denegadas y actualización en los equipos

Cuando se modifiquen las categorías a las que se desea restringir o permitir el acceso, transcurrirá un **plazo máximo de 4 horas** hasta que los equipos recojan la nueva configuración.

Durante este intervalo de tiempo, el comportamiento del control de acceso a páginas Web será el anterior a la modificación.

No obstante, si fuera necesario forzar la actualización, siempre puedes hacerlo desde cada uno de los equipos en los que está instalada la protección. Para ello, haz clic en el icono de la protección situado en la barra de tareas, junto al reloj de Windows, y a continuación selecciona la opción **Actualizar**.

- Lista de direcciones y dominios permitidos o denegados

Por otra parte, también podrás especificar listas de páginas Web a las que siempre se permitirá o denegará el acceso. Es lo que se denomina lista blanca (acceso permitido) o lista negra (acceso denegado).

Podrás modificar ambas listas en cualquier momento en función de tus necesidades.

1. Introduce en la caja de texto la URL del dominio o dirección.
2. Haz clic en **Añadir**.
3. Utiliza los botones **Eliminar** y **Vaciar** para modificar la lista en función de tus necesidades.
4. Finalmente, haz clic en **Aceptar** para guardar la configuración.

Una vez finalizada la configuración, en la ventana **Estado** podrás ver un resumen de los accesos realizados a páginas Web así como detalle de los mismos.

- Base de datos de URLs accedidas desde los equipos

Cada uno de los equipos recopila en una base de datos información sobre las URL a las que se ha accedido desde él.

Esta base de datos solo se puede consultar en local, es decir, desde el propio equipo, durante un plazo de 30 días.

Los datos almacenados en la base de datos son:

1. Identificador del usuario.
2. Protocolo (http o https).
3. Dominio.
4. URL
5. Categorías devueltas por Commtouch.
6. Acción (Permitir/denegar).
7. Fecha de acceso.
8. Contador acumulado de accesos por categoría y dominio.

15.7.2 Configurar horarios del control de accesos a páginas Web

Restringir el acceso a páginas Web puede resultar muy útil a la hora de optimizar el horario de trabajo. Además te permitirá sacar el máximo provecho de tu ancho de banda, lo que repercute también notablemente en la marcha de tu actividad empresarial.

El control de acceso a páginas Web es aplicable de forma independiente tanto a estaciones de trabajo como a servidores. Una vez que hayas seleccionado el tipo de equipo de que se trata, la configuración es similar para ambos casos.

Para poder utilizar la configuración de horarios es necesario disponer de licencias de Endpoint Protection Plus. En caso de no disponer de licencias, acude a tu distribuidor habitual.

Con la configuración de horarios podrás restringir el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorizarlo en el horario no laborable o en el fin de semana.

Para acceder a la configuración de horarios, haz clic en **Configuración** / **Control de accesos a páginas Web**.

El control de acceso a páginas Web está desactivado por defecto. A la hora de activarlo, puedes seleccionar entre:

- Disponer del control de acceso a páginas Web siempre activado.

- Seleccionar las horas en las que quieres que el control horario esté activado. Para activarlo sólo en un horario determinado, marca la casilla correspondiente y utiliza la cuadrícula para señalar las horas en las que se activará. También puedes activarlo para días enteros.

Haz clic en **Aceptar** para que se guarden los cambios.

> ***Ten en cuenta que se usará la hora local de cada equipo, no la hora del servidor.***

16. Configurar la protección para equipos OS X

Introducción

Características de la protección para OS X

Configuración de la protección para equipos con OS X

16.1 Introducción

La protección específica Endpoint Protection para OS X se caracteriza porque sus licencias son independientes de las que puedas poseer para equipos con sistema operativo Windows/Linux/Android.

Por lo tanto, es posible adquirir tantas licencias trial/release de Endpoint Protection para OS como se desee, independientemente del número y tipo (trial /release) de licencias de Endpoint Protection para Windows/Linux/Android que se tengan contratadas. Como es lógico, también se pueden adquirir únicamente licencias trial/release de Endpoint Protection para OS X.

Además, la configuración de los equipos con OS X se realiza de forma independiente, es decir, solo será necesario configurar en dichos equipos las funcionalidades que les correspondan.

16.2 Características de la protección para OS X

La protección para OS X reúne una serie de características propias que la diferencian de la protección para equipos con sistema operativo Windows/Linux. Son las siguientes:

Configuración de las actualizaciones en equipos con sistema operativo OS X

En el caso de los equipos con sistema operativo OS X, no es posible configurar la periodicidad de la actualización automática del archivo de identificadores, por lo que se realizará cada hora.

Transcurridas 48 horas desde que exista una versión del archivo de identificadores superior a la que los equipos tienen instalada, los equipos se mostrarán como desactualizados en la ventana **Estado**.

- Frecuencias de las actualizaciones de la protección para equipos con OS X

Las frecuencias con que se realizan las actualizaciones de la protección para los equipos con sistema operativo OS X, es la siguiente:

- Actualización del fichero de firmas ==> Cada hora
- Cambios en la configuración de la protección ==> Cada 4 horas
- Actualización de la información de detecciones ==> Cada 6 horas
- Actualización de la información del estado de los equipos ==> Cada 12 horas

Actualización automática del motor de la protección

En el caso de los equipos con sistema operativo OS X no es posible realizar una actualización automática, por lo que cuando exista una nueva versión de la protección usted deberá descargarla e instalarla en los equipos.

Transcurridas 72 horas desde que exista una versión de la protección superior a la que los equipos tienen instalada, los equipos se mostrarán como desactualizados en la ventana Estado.

Durante la instalación se procederá a desinstalar la versión anterior y a instalar la nueva.

Configuración de análisis programados en equipos con sistema operativo OS X

Los análisis programados no aplican a estos equipos. La protección disponible para equipos con sistema operativo OS X afecta únicamente a la protección permanente antivirus para archivos.

Instalación de la protección para OS X

La instalación de la protección para OS X puede realizarse de dos maneras: descargando el instalador o generando una URL de instalación.

Consulta el apartado Instalación en equipos con OS X, donde encontrarás toda la información al respecto.

16.3 Configuración de la protección para equipos con OS X

La protección de Endpoint Protection para OS X afecta únicamente a la protección permanente antivirus para archivos. En el caso del resto de configuraciones, consulta el apartado Características específicas de la protección para OS X.

La protección permanente antivirus está activada por defecto. Si deseas cambiar esta configuración, Sigue los siguientes pasos:

1. En la ventana principal de la consola de Endpoint Protection haz clic en el menú **Configuración**.
2. Haz clic en el nombre del perfil para el que deseas configurar la protección antivirus.
3. En la columna de la izquierda, haz clic en la opción **Antivirus** que se muestra bajo OS X.

Por defecto, esta protección estará activada. Para desactivarla, deberás desmarcar la casilla **Activar la protección permanente de archivos**.

Una vez instalada la protección en los equipos, dispondrás de una consola local en cada uno de ellos desde donde podrás realizar las siguientes acciones:

1. Seleccionar el dispositivo que desea analizar.
2. Lanzar un análisis completo del equipo.
3. Lanzar un análisis rápido.
4. Ver las detecciones.
5. Visualizar el listado de archivos sospechosos (archivos en cuarentena).
6. Visualizar la fecha del fichero de firmas.
7. Planificar un análisis en tiempo real.
8. Planificar un análisis rápido o completo.

17. Configurar la protección para dispositivos Android

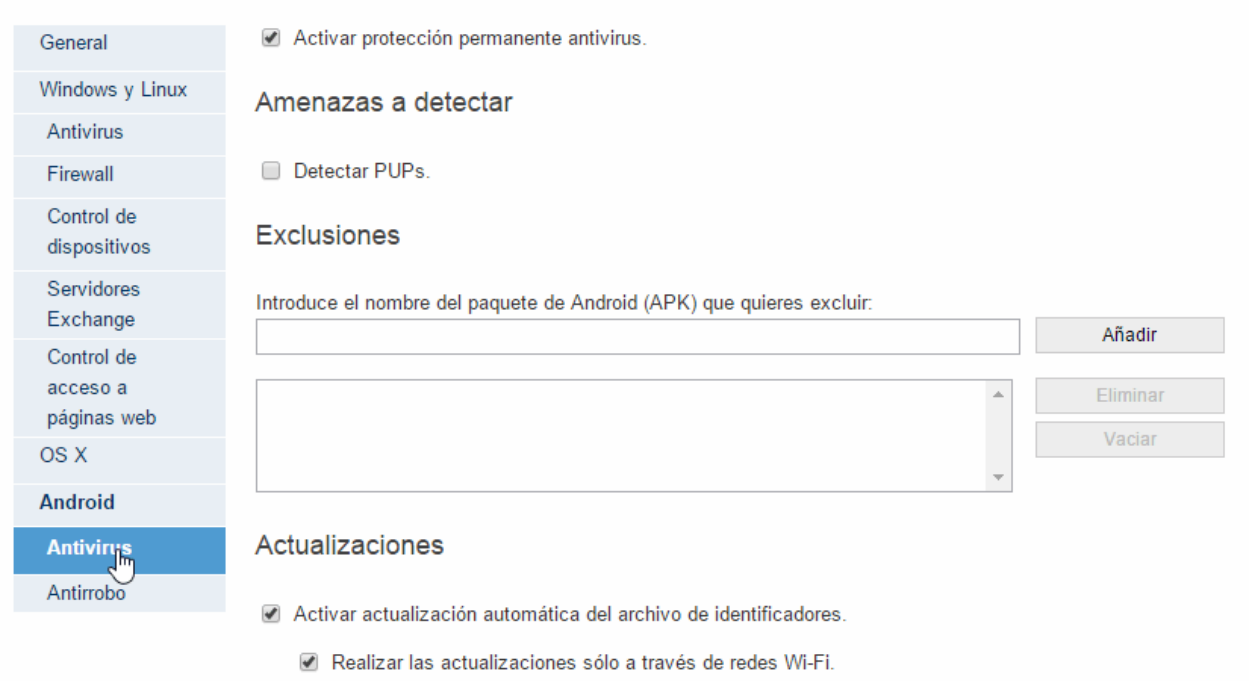
Configurar la protección antivirus

Configurar la protección antirrobo

17.1 Configurar la protección antivirus

En la ventana **Configuración,** haz clic en el perfil para el que quieres configurar la protección antivirus para dispositivos Android.

A continuación, haz clic en la opción **Antivirus**, situada bajo **Android**:



17.1.1 Activar la protección

1. Marca la casilla para activar la protección antivirus.
2. Marca la casilla para que la protección antivirus detecte los programas potencialmente no deseados (PUP).

17.1.2 Exclusiones

La protección para Android permite realizar exclusiones de cualquiera de las aplicaciones instaladas, en su totalidad. Para ello, sigue los siguientes pasos:

1. Introduce el nombre del paquete de Android (apk) que deseas excluir de los análisis y haz clic en **Añadir**.
2. Utiliza los botones **Eliminar** y **Vaciar** si necesitas limpiar o modificar la lista de exclusiones.

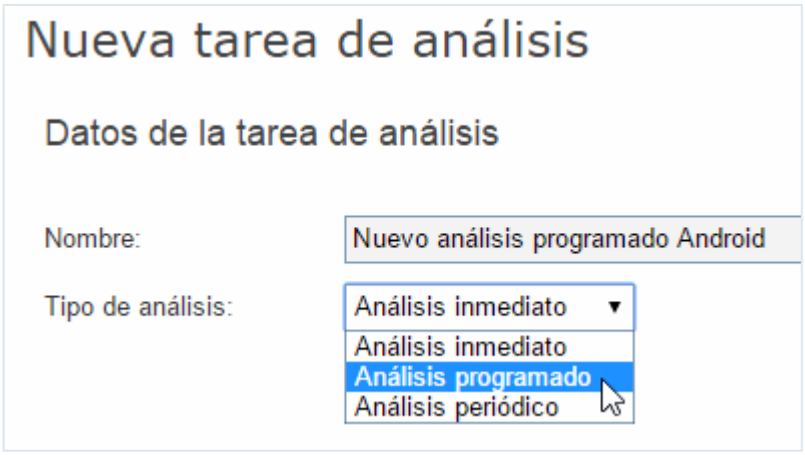
17.1.3 Actualizaciones

Puedes realizar las actualizaciones del archivo de identificadores de forma automática. Además, también puedes elegir si deseas que estas actualizaciones se realicen exclusivamente por medio de redes Wi-Fi.

17.1.4 Análisis programados

1. Para programar un análisis, haz clic en el botón **Nuevo**.

2. Utiliza las opciones que se muestran en la ventana **Nueva tarea de análisis** para crear tareas de análisis, que podrán ser inmediatos, programados o periódicos.



A medida que vayas creando tareas de análisis, éstas se mostrarán en el listado de análisis programados del perfil para el que estás configurando la protección antivirus. Desde allí podrás editarlas o eliminarlas.

Características de cada tipo de análisis programado

- Análisis inmediato

Una vez configurado el análisis, éste tendrá lugar en el momento en que se produzca la conexión del equipo con el servidor de Endpoint Protection.

- Análisis programado

El análisis tendrá lugar en la hora y fecha que determines. Para ello, es necesario que la configuración de la programación se realice con la antelación suficiente. En caso de no disponer de conexión con el servidor de Endpoint Protection en la fecha y hora programadas, el análisis se realizará en el momento en que se establezca la conexión.

- Análisis periódico

El análisis tendrá lugar en la hora y fecha que tú determines y se repetirá con la periodicidad que selecciones.

Al igual que sucede con el análisis programado, es recomendable realizar la programación del análisis con antelación suficiente para garantizar la existencia de conexión con el servidor de Endpoint Protection. En caso contrario, el análisis se realizará en el momento en que se establezca la conexión.

17.2 Configurar la protección antirrobo

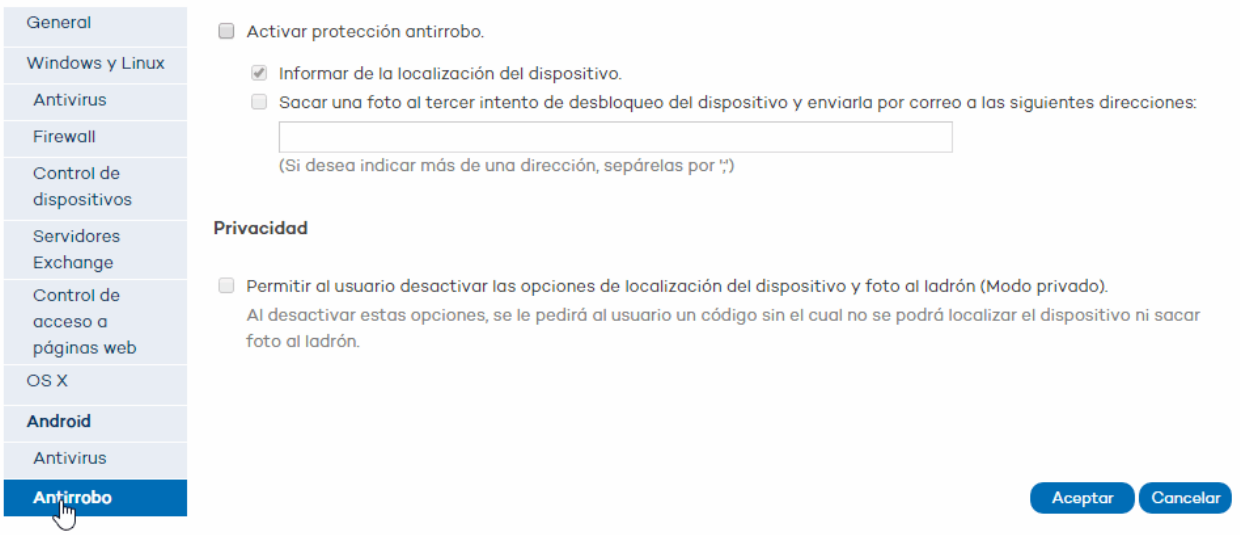
Importante: para poder utilizar la protección antirrobo, es necesario disponer de licencias de Endpoint Protection Plus o Fusion. En caso de no disponer de estas licencias, acude a su distribuidor habitual.

La protección antirrobo de Endpoint Protection te permitirá controlar en todo momento tus dispositivos Android y determinar cuál será su comportamiento en el caso de que te los roben.

Al configurar esta protección desde la consola Web, podrás localizar los dispositivos, borrarlos, bloquearlos, sacar una fotografía al ladrón y enviarla por correo electrónico a una dirección concreta.

17.2.1 Activar la protección antirrobo

1. En la ventana principal de la consola de Endpoint Protection haz clic en el menú **Configuración**.
2. Haz clic en el nombre del perfil para el que deseas configurar la protección antirrobo.
3. En la columna de la izquierda, haz clic en la opción **Antirrobo** que se muestra bajo **Android**.



4. Activa la protección antirrobo.
5. Si deseas que se te informe sobre la localización del dispositivo automáticamente, marca la casilla correspondiente. Esto facilita la localización del dispositivo incluso en el caso de que se agote la batería.
6. Si deseas recibir un correo electrónico cuando se detecte actividad en un dispositivo robado, marca la casilla correspondiente. A continuación, introduce la dirección o direcciones de correo electrónico a las que se enviará la fotografía. Separa las direcciones utilizando punto y coma (;).

   Si además de la opción de envío de foto del ladrón, has seleccionado previamente la de localización del dispositivo, junto con la foto del ladrón recibirás el mapa detallando la localización del dispositivo.

Una vez realizada esta configuración, desde la ventana Detalles de equipo podrás ver en todo momento dónde se encuentra el dispositivo, bloquearlo mediante una clave y modificar la dirección de correo electrónico para recibir la fotografía.

17.2.2 Privacidad (Modo privado)

Si quieres, como administrador puedes conceder permiso al usuario de un dispositivo determinado para que lo utilice en modo privado. Esto permitirá al usuario desactivar las opciones automáticas de localización del dispositivo y de foto al ladrón, utilizando para ello una contraseña.

Tanto la localización del dispositivo como la foto al ladrón bajo demanda seguirán siendo opciones disponibles siempre y cuando se disponga de la contraseña que el usuario ha introducido

Para activar de nuevo la localización y la foto al ladrón automática, será imprescindible desactivar el modo privado.

18. Acceso remoto a los equipos

Visualizar equipos con acceso remoto

Comportamiento de las herramientas de acceso remoto

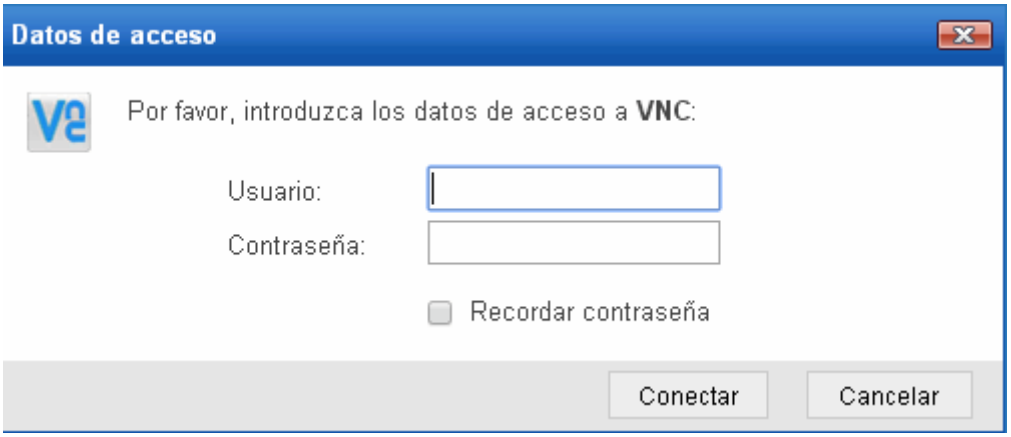
18.1 Visualizar equipos con acceso remoto

La funcionalidad de acceso remoto a los equipos resulta muy útil cuando deseaS acceder a los equipos de tu red desde tu consola de administración sin necesidad de trasladarte.

> ***IMPORTANTE: El control remoto de los equipos solo es posible para los equipos con sistema operativo Windows.***

Endpoint Protection te permite acceder a los equipos utilizando alguna de las herramientas de acceso remoto siguientes: TeamViewer, RealVNC, UltraVNC, TightVNC, LogmeIn.

En la ventana **Equipos** se mostrarán mediante un icono los equipos que tienen instalada alguna de estas herramientas de acceso remoto. Si solo es una, haciendo clic sobre el icono podrás acceder a la herramienta y, una vez introducidas las credenciales correspondientes, acceder al equipo.



Puedes introducir las credenciales desde la propia ventana **Equipos** o desde la de Preferencias.

Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrás elegir cuál de ellas deseas utilizar para acceder al equipo.

En el apartado Comportamiento de las herramientas de acceso remoto encontrarás información sobre cada una de las herramientas.

> ***En el caso de que el equipo tenga más de una herramienta VNC instalada, solo se podrá acceder a través de una de ellas, siendo la prioridad de acceso la siguiente: 1-RealVNC, 2-UltraVNC, 3-TightVNC.***

Dependiendo de si posees permiso de control total o de administrador, podrás utilizar el acceso remoto para acceder a más o menos equipos. Si tu permiso es de monitorización, no podrás acceder a ninguno y el icono de la columna **Acceso remoto** aparecerá deshabilitado.

18.1.1 Cómo obtener acceso remoto

Acceso desde la ventana Equipos

La primera vez que accedes a la ventana **Equipos** se mostrará un aviso indicándote que tus equipos no disponen de acceso remoto instalado. Si deseas instalarlo, utiliza el vínculo que se te mostrará en el aviso.

Acceso desde la ventana Detalles de equipo

Desde la ventana **Detalles de equipo** también podrás utilizar el acceso remoto, siempre y cuando el equipo seleccionado tenga alguna de las herramientas de acceso remoto instalada. Si es así, haz clic en el icono de la herramienta de acceso remoto que desees usar para ello.

Para poder tener acceso remoto, deberás instalar en tus maquinas una de las soluciones de control remoto soportadas: TightVNC, UltraVNC, RealVNC , TeamViewer, LogMeIn.

En el caso de las herramientas VNC se seguirá la misma prioridad comentada anteriormente para el caso de que el equipo tenga instaladas más de una de estas herramientas.

18.2 Comportamiento de las herramientas de acceso remoto

18.2.1 Herramientas VNC

Estas herramientas sólo se podrán utilizar para acceder a equipos que estén en la misma red local que la del cliente.

Dependiendo de la configuración de autenticación de las herramientas, es posible que se pueda acceder a ellas sin necesidad de incluir credenciales de acceso remoto en la consola, o, por el contrario, tenga que configurar únicamente el password de acceso remoto o tanto el usuario como la password para poder conectar remotamente.

Para que al administrador pueda acceder a sus equipos a través de estas herramientas, debe permitir la ejecucion del applet de Java en su propio equipo, en caso contrario, el acceso a los equipos, no funcionará correctamente.

18.2.2 TeamViewer

Esta herramienta se podrá utilizar para acceder a equipos que se encuentren fuera de la red local del cliente.

Para acceder a los equipos a través de TeamViewer solo será obligatorio introducir la password de los equipos, el campo “usuario” puede dejarse en blanco.

La password que hay que incluir para acceder a un equipo a través de TeamViewer es la password de TeamViewer del equipo o la password configurada para el acceso no presencial, y no la password de la cuenta de cliente de TeamViewer.

Es recomendable disponer de la misma password de TeamViewer en todos los equipos, ya que cada usuario de la consola de Endpoint Protection sólo puede incluir una password para el acceso remoto a sus equipos a través de TeamViewer.

El equipo del administrador (equipos a través del cual se accede a la consola), deberá disponer de TeamViewer instalado (no es suficiente disponer de TeamViewer en modo ejecutor en dicho equipo).

18.2.3 LogMeIn

Esta herramienta se podrá utilizar para acceder a equipos que se encuentren fuera de la red local del cliente.

Para acceder a los equipos a través de LogMein, será necesario incluir el usuario y la password de la cuenta de LogMein.

19. Monitorización de los equipos

19.1 Introducción

Desde la consola Web puedes ver cuál es el estado de los equipos. En el caso de equipos a los que se ha distribuido la protección, puedes monitorizar en todo momento el estado de la misma. Para ello, en la ventana **Equipos** se muestran las siguientes listas:

- Lista de equipos protegidos.
- Lista de equipos desprotegidos.
- Lista de equipos sin licencia.
- Lista de equipos excluidos.

Cada lista ofrece una visión general del estado de la protección en los equipos que la integran, pero además también permiten conocer al detalle si la protección se ha instalado correctamente, si se ha producido algún error durante el proceso de instalación, si se encuentra a la espera de reinicio y cuál es su nivel de actualización, por ejemplo.

En la parte izquierda de la pantalla encontrarás el árbol de grupos por el que podrás desplazarte a través de los diferentes niveles y ver los equipos que contiene cada grupo.

Para acceder a las listas de equipos protegidos y desprotegidos, haz clic en la pestaña **Equipos**. En la ventana que se muestra, encontrarás las siguientes pestañas: **Protegidos, Desprotegidos, Sin licencia** y **Excluidos.**

Selecciona la pestaña correspondiente. Podrás realizar búsquedas de equipos y exportar la lista a formato excel o csv. Como norma general, al hacer clic sobre el nombre de un equipo accederás a la ventana de detalle del equipo.

19.2 Detalles de equipo

Si deseas acceder a los detalles de un equipo concreto, haz clic en dicho equipo. A continuación se mostrará la ventana **Detalles de equipo,** con información sobre el estado del equipo, independientemente de que esté protegido o no.

La información que se muestra es la misma para todos los equipos -Windows, Linux u OS X- excepto en el caso de los datos sobre el dominio, que no estarán visibles para equipos con OS X.

En el caso de los dispositivos Android, la ventana de detalles de equipo te proporcionará información específica que puedes consultar en el apartado Detalles de equipo dispositivos Android.

Utiliza el campo **Comentario** si deseas añadir información adicional que te pueda ayudar a identificar el equipo. Si eres un usuario con permiso de monitorización, no podrás modificar este campo. Para más información, consulta el apartado Tipos de permisos.

19.2.1 Desinfectar el equipo

Si deseas desinfectar el equipo, utiliza para ello la herramienta de desinfección Panda Cloud Cleaner. Para ello, haz clic en el botón **Desinfectar equipo**.

A continuación se te mostrará la configuración por defecto establecida para la desinfección. Como administrador, podrás seleccionar opciones de desinfección adicionales a las establecidas.

Selecciona también si la desinfección se realizará de manera visible o silenciosa. Consulta el apartado Desinfectar equipos.

19.2.2 Notificar problemas en el equipo

Utiliza esta opción si deseas notificar algún problema del equipo. En el formulario que se mostrará, podrás introducir una breve descripción del problema y enviarlo a personal cualificado que analizará el problema y se pondrá en contacto contigo para solucionarlo. Para ello, es necesario que introduzcas una dirección de correo electrónico.

19.2.3 Reiniciar equipos

Mediante esta opción, podrás reiniciar los equipos que, por cualquier motivo, figuren en el listado de equipos protegidos como pendientes de reinicio. Consulta el apartado Reiniciar equipos.

19.2.4 Eliminar y excluir equipos

Si deseas eliminar equipos que no se han conectado con el servidor desde hace tiempo, utilice la opción **Eliminar de la base de datos**. Los datos del equipo dejarán de ser utilizables y por tanto tampoco podrás controlarlo.

Si lo que deseas es excluir equipos de la base de datos, hazlo mediante la opción **Excluir**. Los equipos excluidos se mostrarán en la lista de equipos excluidos de la ventana **Equipos**. Podrás deshacer la exclusión en cualquier momento. Consulta el apartado Eliminar y excluir equipos desprotegidos.

19.3 Detalles de equipo (dispositivos Android)

En el caso de los dispositivos Android, en la ventana **Detalles de equipo** se muestran los datos del dispositivo y el estado de las protecciones antivirus y antirrobo, según la configuración que hayas realizado.

Si la protección antirrobo está activada en el dispositivo, se mostrará un mapa con la localización del dispositivo y las opciones correspondientes de la protección antirrobo: borrar, bloquear el dispositivo, realizar fotografía al ladrón y localizar el dispositivo.

Si alguna de las protecciones muestra un estado de error, haz clic en el vínculo **¿Cómo solucionar errores?** y accederás a instrucciones de soporte técnico que te resultarán útiles para resolver el problema.

19.3.1 Borrar dispositivo

Utiliza el botón **Borrar** para eliminar la información que se muestra del dispositivo y restaurar la configuración de fábrica.

19.3.2 Bloquear dispositivo

Utiliza el botón **Bloquear dispositivo** para introducir la clave de cuatro dígitos necesaria para realizar el bloqueo.

19.3.3 Foto al ladrón

Al solicitar esta acción, cuando se detecte actividad en el dispositivo robado se sacará automáticamente una fotografía al autor de la sustracción. Introduce en la casilla de texto la dirección de correo electrónico a la que se enviará la fotografía. Puedes introducir varias direcciones, separadas por punto y coma (;).

Por defecto, se mostrarán las direcciones de correo que se hayan introducido al realizar la configuración de la protección antirrobo para el perfil correspondiente.

19.3.4 Modo privado

Si el administrador ha concedido permiso al usuario del dispositivo para que lo utilice en modo privado, y el usuario lo ha activado mediante una contraseña, las opciones automáticas de localizar el dispositivo o de sacar foto al ladrón no funcionarán.

La activación manual o bajo demanda de la localización y la foto al ladrón no podrán utilizarse, salvo que el usuario proporcione la clave que introdujo para establecer el modo privado.

19.3.5 Lista de tareas

El dispositivo Android mostrará el registro de tareas con información sobre las tareas que se han configurado desde la consola Web para que sean ejecutadas en el dispositivo. Consulta el apartado **Lista de tareas**.

19.4 Lista de tareas (dispositivos Android)

Las tareas de alertas de robo, borrado y localización del dispositivo Android que se solicitan desde la consola Web para que se ejecuten en el dispositivo, se muestran en el registro de tareas de la ventana Detalles de equipo**.**

Registro de Tareas

Hora	Acción	Resultado	Estado tarea
27/03/2015 13:49:55	Localizar dispositivo	Pendiente...	
27/03/2015 13:33:10	Alertas de robo	Pendiente...	
26/03/2015 18:37:16	Borrar	Ejecutada	
26/03/2015 18:11:03	Localizar dispositivo	Ejecutada	
26/03/2015 14:37:53	Alertas de robo	Recibida	
26/03/2015 13:44:50	Alertas de robo	Ejecutada	

El registro muestra una tarea por estado. Por ejemplo, si, como se muestra en la imagen, existen tres tareas de alertas de robo, se mostrará una de ellas Ejecutada, otra como Recibida y otra como Pendiente. En la medida en que la primera tarea finalice y desaparezca del listado, la que se encuentra como Recibida pasará a Ejecutada y la que está como Pendiente pasará a Recibida.

19.4.1 Estado de las tareas

Pendiente

Las tareas se encontrarán en estado pendiente durante el intervalo de tiempo que va desde la configuración de la tarea en la consola Web hasta su recepción en el dispositivo. Hay que tener en cuenta que puede darse el caso de que el dispositivo se encuentre apagado o sin acceso a red, tiempo éste durante el que la tarea figurará como pendiente.

Recibida

En este caso, el dispositivo ha recibido la solicitud de realización de una tarea pero aun no la ha ejecutado o está en plena ejecución, y, por tanto, no ha finalizado. Por ejemplo, cuando se trata de una tarea de localización del dispositivo, la tarea se mostrará como recibida hasta que la localización sea efectiva.

En el caso de la tarea de foto al ladrón, la tarea también se mostrará como recibida en tanto en cuanto no se ejecute el acto de sacar la fotografía. Esto es debido a que desde que se envía la solicitud de tarea transcurre el tiempo que el ladrón tarda en activar el dispositivo, es decir, en tocar la pantalla.

Ejecutada

La tarea se mostrará como ejecutada una vez que el dispositivo informe de la finalización de la misma (ya sea correctamente o con error).

19.5 Visualizar equipos con acceso remoto

Tanto en la pestaña de **Equipos protegidos** como en la de **Equipos desprotegidos**, se indican los equipos en los que se ha instalado previamente alguna herramienta de control remoto, de tal manera que, en

función de los permisos que posees, puedes utilizar dicha herramienta para acceder a ellos desde tu consola de administración.

> ***No se podrá acceder remotamente a los equipos desprotegidos que se encuentren en estado "descubierto" o "desinstalado".***

Si el equipo tiene varias herramientas de acceso remoto instaladas y sitúas el cursor sobre el icono que aparece en la columna **Acceso remoto**, podrás ver con detalle qué herramientas de acceso remoto hay instaladas en el equipo. Haz clic sobre el icono para acceder al equipo.

Si el equipo dispone de varias herramientas de VNC instaladas, (RealVNC, UltraVNC,TightVNC), sólo podrás acceder remotamente a través de una de ellas, siguiendo la siguiente prioridad:

- RealVNC
- UltraVNC
- TightVNC

Si deseas conocer cómo es el proceso de instalación de las herramientas de acceso remoto en los equipos, haz clic en el vínculo que encontrarás dentro del recuadro informativo de color azul.

Para más información, visita el apartado Acceso remoto a los equipos.

20. Acciones sobre equipos protegidos

Añadir y buscar equipos protegidos

Mover y eliminar equipos

Reiniciar equipos

Desinfectar equipos

Solucionar errores en la protección

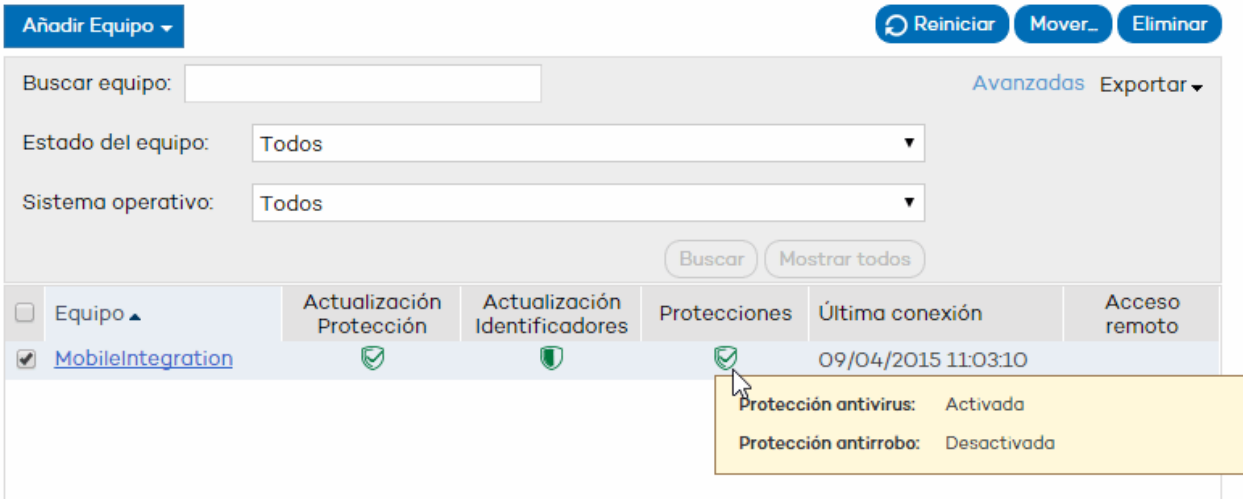
Solucionar errores de actualización del fichero de firmas

20.1 Añadir y buscar equipos protegidos

La lista de equipos protegidos que se muestra en la ventana **Equipos** te permite conocer el estado en el que se encuentra la protección instalada en los equipos de tu red informática.

Por favor, recuerda que:

- **Equipos Linux.** Los equipos Linux protegidos disponen únicamente de análisis bajo demanda y programados.
- **Equipos OS X.** Los equipos con OS X protegidos disponen únicamente de protección permanente de archivos. Para saber más sobre esta protección, consulta el apartado Configuración de la protección para equipos OS X.
- **Dispositivos Android.** Estos dispositivos disponen de protección permanente antivirus y protección antirrobo (solo disponible si posees licencias de Endpoint Protection Plus).



Selecciona en el árbol de grupos el grupo o subgrupo que quieres explorar.

Si seleccionas **Todos** se mostrarán todos los equipos, independientemente del grupo/subgrupo en el que esté el equipo.

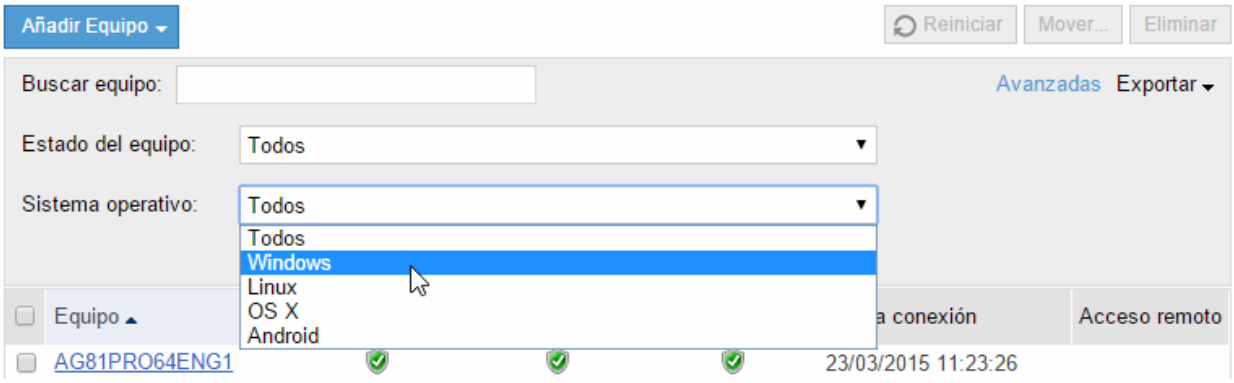
> ***Según los permisos de que dispongas, podrás ver más o menos equipos. Consulta el apartado Tipos de permisos.***

20.1.1 Añadir equipos

Si deseas añadir un equipo, haz clic en **Añadir**. A continuación consulta el apartado Instalación según sistema operativo para conocer cómo puedes instalar la protección en el equipo, según el sistema operativo del que se trate.

20.1.2 Búsqueda de equipos

Puedes elegir que se le muestren todos los equipos protegidos, utilizando para ello el botón **Mostrar todos**, o puedes utilizar el desplegable **Avanzadas** y activar el filtro que te permitirá buscar equipos en función del estado en el que se encuentra la protección instalada en ellos o el sistema operativo:



En el caso de los equipos con OS X, al disponer únicamente de la protección para archivos, se muestra si está activa, con error o desactivada.

En el caso de los equipos Linux, se muestra el icono de estado correcto en la columna **Protecciones**.

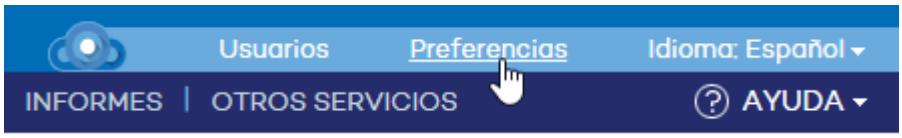
Esta herramienta de búsqueda también es muy útil para conocer qué equipos no disponen de la versión actualizada del archivo de identificadores o disponer de un listado de los que, por alguna razón, no se han conectado con el servidor de Endpoint Protection en las últimas 72 horas.

Selecciona el estado que te interesa en el desplegable **Estado del equipo**, y haz clic en **Buscar.**

La información resultante de la búsqueda se presenta en las siguientes columnas:

- La columna **Equipo** muestra el listado de los equipos protegidos, denominándolos por su nombre o por su IP. Si hay diferentes equipos con igual nombre y dirección IP, se mostrarán como equipos diferenciados en la consola Web siempre y cuando tanto su dirección MAC como su identificador del agente de administración sean diferentes.

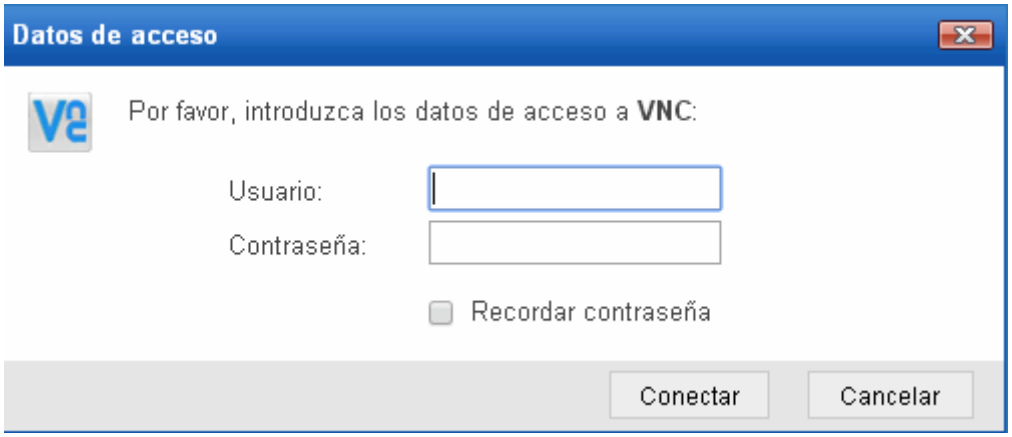
  Si deseas cambiar el modo en el que se nombran, puedes hacerlo en la ventana Preferencias, a la que se accede desde el vínculo situado en la cabecera de la consola Web



- Las columnas **Actualización Protección**, **Actualización Identificadores**, y **Protecciones** utilizan una serie de iconos para indicar el estado de actualización de las protecciones y la situación general de la protección en sí. Sitúe el cursor sobre el icono para visualizar la información.

- En **Última conexión** podrás ver la fecha y hora exactas de la última conexión del equipo con el servidor de actualizaciones.

- **Acceso remoto.** Si esta columna muestra un icono, indica que el equipo tiene instalada alguna herramienta de acceso remoto. Si solo es una, haciendo clic sobre el icono podrás acceder a la herramienta y, una vez introducidas las credenciales correspondientes, acceder al equipo:



Ten en cuenta que el acceso remoto solo está disponible para equipos con Windows.

Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrás elegir cuál de ellas deseas utilizar para acceder al equipo:

Si sitúas el cursor sobre el nombre de un equipo, se mostrará una etiqueta amarilla con la siguiente información:

1. Nombre y dirección IP del equipo.
2. Ruta completa del grupo al que pertenece el equipo.
3. Sistema operativo que tiene instalado el equipo.
4. Fecha de instalación de la protección.
5. Comentario asociado al equipo.
6. Otros datos de interés.

20.2 Mover y eliminar equipos protegidos

20.2.1 Mover equipos de un grupo a otro

Podrás seleccionar uno o N equipos y desplazarlos de un grupo/subgrupo a otro. Si el grupo tiene asignadas restricciones y se ha alcanzado el número máximo de instalaciones establecidas, al intentar mover un equipo a dicho grupo/subgrupo obtendrás un mensaje de error.

Para mover equipos marca las casillas correspondientes a los equipos que deseas mover y haz clic en el botón **Mover**. A continuación, selecciona el grupo/subgrupo al que deseas moverlos y haz clic en **Mover**.

Los usuarios con permiso de monitorización no podrán realizar esta acción.

20.2.2 Eliminar equipos

Podrás seleccionar uno o N equipos y eliminarlos todos a la vez. Esto te resultará muy útil cuando, por ejemplo, necesites eliminar de forma masiva N equipos que no se hayan conectado con el servidor desde una fecha determinada.

Para eliminar equipos marca las casillas correspondientes a los equipos que deseas eliminar y haz clic en el botón **Eliminar**. A continuación, acepta el mensaje de confirmación. Una vez eliminados los equipos, la información sobre ellos dejará de estar disponible.

Los usuarios con permiso de monitorización no podrán realizar esta acción.

20.3 Reiniciar equipos

Si posees permiso de administrador, puedes actuar remotamente desde la consola Web y reiniciar los equipos que figuren en el listado de equipos protegidos.

Para ello, en la ventana **Equipos** > **Protegidos** marca la casilla correspondiente al equipo o equipos que deseas reiniciar y haz clic en el botón **Reiniciar**.

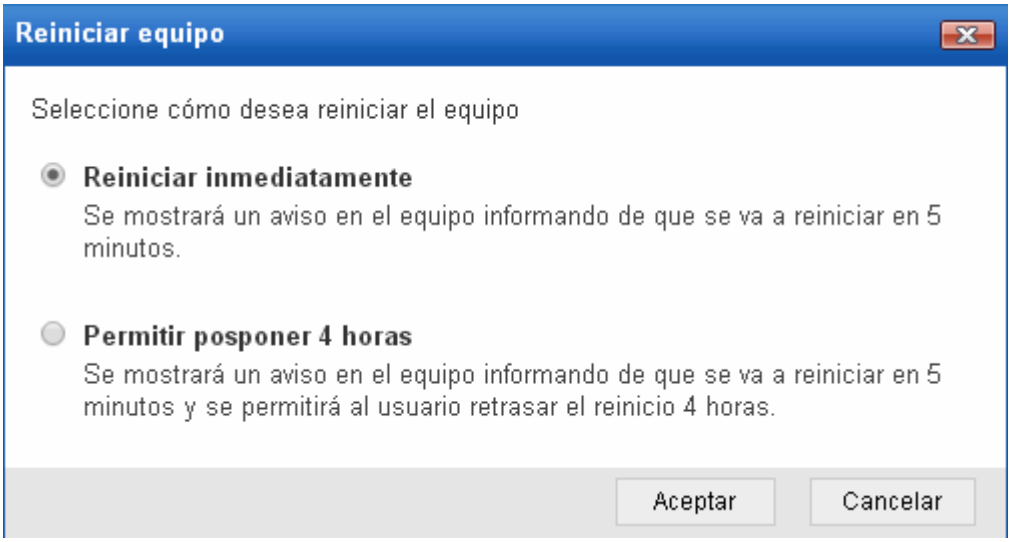
Si haces clic en el nombre del equipo, se mostrará la ventana **Detalles de equipo** desde la que también podrás ordenar el reinicio del equipo utilizando para ello el botón **Reiniciar**.

En el caso de los equipos con sistema operativo Linux/OS X/Android, no es posible ejecutar el reinicio de forma remota. Esta funcionalidad solo está disponible para equipos con sistema operativo Windows.

20.3.1 Reinicio inmediato

Si seleccionas la opción de reiniciar de forma inmediata, en cuanto el equipo seleccionado reciba la nueva configuración (15 minutos como máximo desde el cambio de configuración en consola), se le mostrará al usuario un aviso indicándole que el equipo se va a reiniciar.

El usuario no podrá cancelar el reinicio configurado por ti desde la consola Web.



20.3.2 Reinicio pospuesto

Si, por el contrario, configuras el reinicio como pospuesto, en el mensaje que se le envíe al usuario del equipo seleccionado se le preguntará si desea reiniciar de forma inmediata o posponer el reinicio 4 horas.

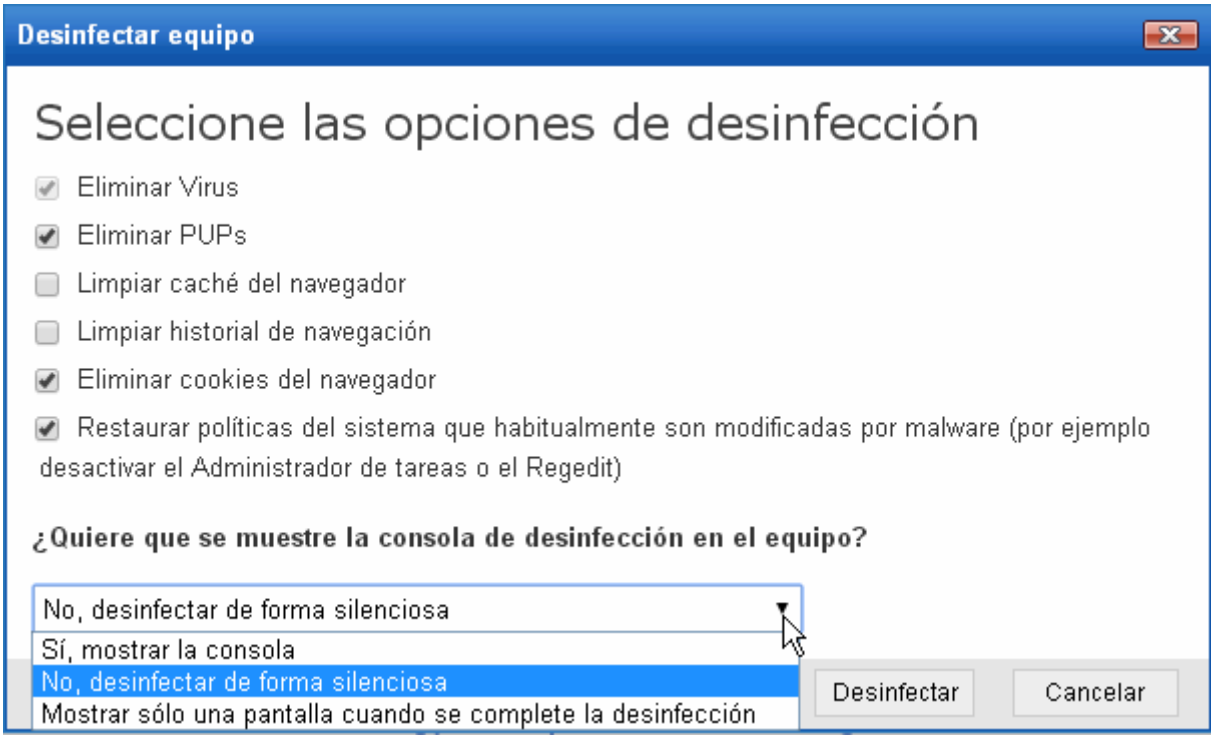
20.4 Desinfectar equipos

Si posees permiso de administrador, podrás desinfectar equipos de manera remota desde la consola Web, utilizando Panda Cloud Cleaner.

Esta opción de desinfección remota puede resultar de gran utilidad ya que no tendrás que trasladarte físicamente hasta el equipo que deseas desinfectar, con lo que ganarás en comodidad, tiempo y dinero sin que la efectividad de la protección se vea afectada.

La opción desde la que desinfectar los equipos se encuentra disponible en la ventana Detalles de equipo.

Una vez que hayas hecho clic en el botón **Desinfectar equipo**, podrás seleccionar las opciones de desinfección y decidir si la desinfección será visible o silenciosa:



20.4.1 Desinfección visible

En el equipo a desinfectar se mostrará la consola de desinfección, con información sobre el progreso de la desinfección y datos adicionales.

20.4.2 Desinfección silenciosa

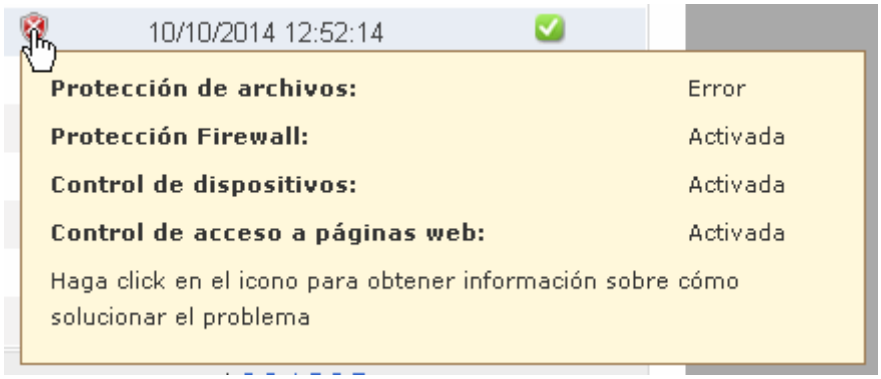
Todo el proceso de desinfección se realizará de forma no visible para el usuario del equipo. Solo se le mostrará un mensaje avisando de la existencia de una tarea de desinfección que se prolongará durante unos minutos e instrucciones sobre cómo acceder al resultado de la tarea de desinfección una vez que el proceso de desinfección concluya.

Si dispones de licencias de Cleaner Monitor o de Fusion, también podrás acceder a los resultados de desinfección desde el icono de acceso Cleaner Monitor en tu consola de Panda Cloud.

20.5 Solucionar errores en la protección

Si dispones de equipos que muestran algún error en la protección instalada, ahora puedes solucionarlo de manera sencilla y rápida.

Para ello, haz clic en el icono de error que muestra el equipo en la columna **Protecciones**, de la pestaña **Equipos protegidos**. A continuación accederás a una ayuda detallada.

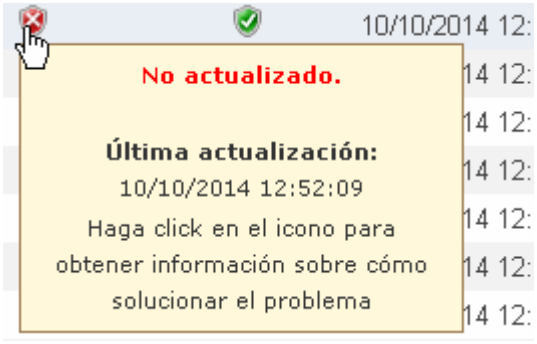


También podrás acceder a esta ayuda desde la sección **Protecciones** en la ventana Detalles de equipo.

20.6 Solucionar errores de actualización del fichero de firmas

Si dispones de equipos que muestran algún error en la actualización del fichero de firmas, ahora puedes solucionarlo de manera sencilla y rápida.

Para ello, haz clic en el icono de error que muestra el equipo en la columna **Actualización identificadores** de la pestaña **Equipos protegidos**. A continuación accederás a una ayuda detallada.



También podrás acceder a esta ayuda desde la sección **Protecciones** en la ventana Detalles de equipo.

21. Acciones sobre equipos desprotegidos

Introducción

Eliminar y excluir equipos desprotegidos

Establecer tareas de búsqueda de equipos desprotegidos

21.1 Introducción

En la ventana **Equipos** se muestra la lista de equipos desprotegidos.

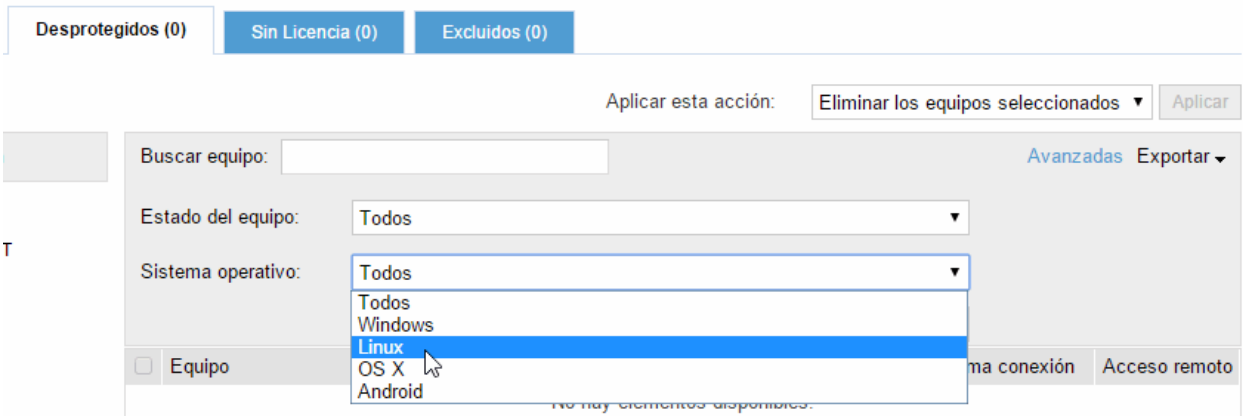
Un equipo puede figurar como desprotegido cuando está en proceso de instalación/desinstalación de la protección, cuando al instalar/desinstalar se ha producido algún error o cuando el equipo ha sido descubierto mediante una búsqueda.

En la parte izquierda de la pantalla encontrarás el árbol de grupos por el que podrá desplazarse a través de los diferentes niveles y ver los equipos que contiene cada grupo.

21.1.1 Búsqueda de equipos

A la hora de buscar los equipos desprotegidos, puedes introducir en la caja de texto **Buscar equipo** el nombre del equipo que deseas localizar y hacer clic en el botón **Buscar**.

Haz clic en el **Estado del equipo** y podrás filtrar la búsqueda según varios criterios:



Selecciona el estado que te interesa y haz clic en **Buscar.**

La información resultante de la búsqueda se presenta en cinco columnas:

- La columna **Equipo** muestra el listado de los equipos analizados, denominándolos por su nombre o por su IP. En el supuesto de que el nombre del equipo no se conozca, se mostrará la cadena *Desconocido*.

- La columna **Estado** muestra cuál es la situación de la protección. Para ello utiliza una serie de iconos. Haz clic en **Leyenda** para poder verlos.

- En la columna **Detalles** se especifica el motivo por el cual el equipo se encuentra en determinado estado. Por ejemplo, si muestra el estado *Error instalando*, en **Detalle** se puede mostrar el código del error producido. Si, por el contrario, la columna **Estado** muestra *Sin protección*, **Detalle** mostrará la explicación *Protección desinstalada*.

- **Última conexión**. Muestra la fecha y hora en que tuvo lugar la última conexión con el equipo.

- **Acceso remoto.** Si esta columna muestra un icono, indica que el equipo tiene instalada alguna herramienta de acceso remoto. Si solo es una, haciendo clic sobre el icono podrás acceder a la herramienta y, una vez introducidas las credenciales correspondientes, al equipo.

Si el equipo tiene instaladas varias herramientas de acceso remoto, al situar el cursor sobre el icono se mostrarán dichas herramientas y podrás elegir cuál de ellas deseas utilizar para acceder al equipo.

Los equipos con OS X figurarán como desprotegidos cuando hayan sido descubiertos a través de una búsqueda lanzada desde la consola.

21.2 Eliminar y excluir equipos desprotegidos

21.2.1 Eliminar equipos

Podrás seleccionar uno o varios equipos y eliminarlos todos a la vez. Esto te resultará muy útil cuando, por ejemplo, necesites eliminar de forma masiva varios equipos que no se hayan conectado con el servidor desde una fecha determinada.

Para eliminar equipos, marca las casillas correspondientes a los equipos que deseas eliminar y haz clic en el botón **Eliminar**. A continuación, acepta el mensaje de confirmación. Una vez eliminados los equipos, la información sobre ellos dejará de estar disponible.

Los usuarios con permiso de monitorización no podrán realizar esta acción.

21.2.2 Excluir equipos

Al excluir equipos, éstos pasarán a mostrarse en la pestaña **Excluidos** de la ventana **Equipos** y no se mostrará información ni alertas referentes a ellos en ningún otro lugar de la consola.

Ten en cuenta que la exclusión puede deshacerse en cualquier momento.

21.3 Establecer tareas de búsqueda de equipos desprotegidos

Con el fin de facilitar y mejorar la labor del administrador a la hora de monitorizar la protección instalada en los equipos, Endpoint Protection permite establecer tareas de búsqueda y detección de equipos desprotegidos.

Esta labor de búsqueda se puede realizar incluso cuando el administrador no se encuentra dentro de la red que se quiere monitorizar, es decir, el administrador puede, desde una ubicación remota, ver en todo momento en su consola información actualizada tanto de equipos protegidos como desprotegidos.

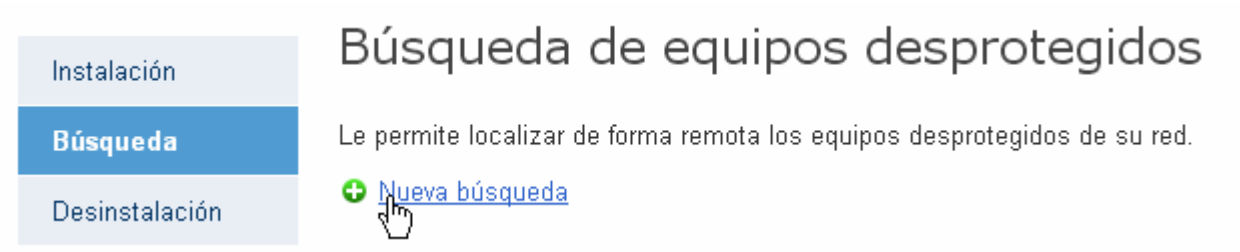
La búsqueda de equipos desprotegidos no está disponible desde equipos con sistema operativo Linux ni OS X.

Si necesitas o deseas ejecutar de forma simultánea búsquedas de equipos desprotegidos y tareas de desinstalación remota de las protecciones, consulta el apartado Compatibilidad de tareas de gestión remota.

21.3.1 Crear tarea de búsqueda de equipos desprotegidos

En la ventana principal de la consola Web, haz clic en **Instalación**. A continuación, en el menú de la izquierda selecciona la opción **Búsqueda**. Accederás a la pantalla **Búsqueda de equipos desprotegidos**.

Para crear una tarea de búsqueda, haz clic en **Nueva búsqueda**.



A continuación, en la pantalla **Edición de búsqueda** podrás concretar qué equipo será el encargado de realizar la búsqueda. Para ello, utiliza el botón **Seleccionar.**

El alcance de la búsqueda se definirá en función de que decidas realizarla en la subred del equipo encargado de llevar a cabo la búsqueda, en rangos de direcciones IP determinados, o en dominios concretos.

- Requisitos del equipo que realiza la búsqueda

Para poder llevar a cabo la tarea de búsqueda, el equipo encargado de ello tiene que reunir una serie de requisitos.

1. Ha de disponer de conexión a Internet y haberse conectado durante las últimas 72 horas con el servidor de Endpoint Protection, además de estar debidamente protegido con la versión 5.05 o posterior de Endpoint Protection.

2. Debe estar operativo y no podrá ser un equipo excluido ni sin licencia. Tampoco podrá estar realizando tareas de desinstalación remota.

Es importante que compruebes que el equipo no tiene configurada una tarea de desinstalación remota. Para más información, consulta el apartado Compatibilidad entre tareas de gestión remota.

3. Debe ser un equipo con sistema operativo Windows.

21.3.2 Visualización de las búsquedas

Las búsquedas creadas aparecerán listadas en la pantalla **Búsqueda de equipos desprotegidos**, desde donde podrás también eliminar las tareas si así lo deseas, utilizando para ello el botón **Eliminar.**

> ***Las tareas en estado Iniciando o En curso no se pueden eliminar.***

En esta pantalla la información se organiza en las siguientes columnas:

- **Nombre**: muestra el nombre que se ha dado a la búsqueda cuando se ha creado.
- **Estado**: indica mediante iconos el estado en que se encuentra la tarea de búsqueda. Haz clic en **Leyenda** para poder verlos.
- **Descubiertos**: detalla el número de equipos desprotegidos encontrados.
- **Fecha creación**: fecha en que se creó la tarea de búsqueda.
- **Creado por**: usuario que creó la tarea de búsqueda.

Según el permiso del que dispongas podrás crear, visualizar o eliminar tareas de búsqueda de equipos desprotegidos. Para más información, consulta el apartado Tipos de permisos.

21.3.3 Resultado de las búsquedas

Al hacer clic en el nombre de una búsqueda de las que aparecen en la pantalla **Búsqueda de equipos desprotegidos,** accederás a la pantalla **Resultado de la búsqueda**. Aquí se mostrarán los equipos desprotegidos que se han descubierto tras ejecutar la tarea de búsqueda correspondiente.

Además del nombre de la búsqueda, sus fechas de inicio y fin y el estado, esta pantalla también proporcionará información cuando durante la ejecución de la búsqueda se haya producido algún error.

> ***En el caso de que la tarea esté en estado En espera, la fecha de inicio mostrará un guión (-). Lo mismo sucederá con la fecha de fin si la tarea no ha finalizado.***

Si deseas consultar la configuración de la tarea de búsqueda, utiliza el vínculo **Ver configuración**.

22. Cuarentena

La cuarentena

Búsqueda de elementos en cuarentena

Archivos excluidos del análisis

22.1 Cuarentena

Endpoint Protection almacena en situación de cuarentena aquellos contenidos sospechosos de ser maliciosos o no desinfectables, así como el spyware y herramientas de hacking detectadas.

Una vez que los elementos sospechosos han sido enviados para su análisis, se pueden producir tres situaciones:

- Si se comprueba que **los elementos son maliciosos**, son desinfectados y posteriormente restaurados a su ubicación original, siempre y cuando exista desinfección para ello.
- Si se comprueba que **los elementos son maliciosos y no existe manera de desinfectarlos**, son eliminados.
- Si se comprueba que **no se trata de elementos perjudiciales**, son restaurados directamente a su ubicación.

22.1.1 La cuarentena en equipos Linux

En los equipos Linux, ni los elementos sospechosos ni el malware detectado se envían a cuarentena.

El malware detectado será desinfectado o eliminado y sobre los sospechosos se informa, peo no se realiza ninguna acción.

22.1.2 La cuarentena en equipos OS X

Estos equipos sólo disponen de cuarentena local. Una vez que los archivos son enviados a cuarentena, podrás optar por aplicar sobre ellos alguna de las opciones disponibles (marcar como no sospechosos, reparar o eliminar).

22.1.3 La cuarentena en equipos Windows

En la ventana principal de la consola Web, haz clic en **Cuarentena** para abrir la ventana del mismo nombre. La ventana se estructura en dos secciones: una zona de búsqueda y otra para mostrar el listado de elementos resultantes de dicha búsqueda.

22.2 Búsqueda de elementos en cuarentena

En la zona de búsqueda puedes filtrar los elementos que deseas visualizar en función de estas características:

- Motivo. Selecciona en la lista desplegable **Motivo** el tipo de archivos que deseas buscar. Los archivos se clasifican en función de la razón o motivo por la que fueron puestos en cuarentena.

  Por defecto, se muestran los elementos que se han enviado a cuarentena por ser considerados sospechosos.

- Grupo. Una vez seleccionado el tipo de archivos que deseas buscar, indica el grupo o subgrupo de equipos en que deseas centrar la búsqueda.

- Fecha

    1. Selecciona el periodo de tiempo que deseas.

    2. Haz clic en **Buscar**.

Si deseas restaurar algún elemento, marca la casilla correspondiente, haz clic en **Restaurar** y responde afirmativamente al mensaje de confirmación. A continuación, el elemento desaparecerá del listado de búsqueda y podrás encontrarlo en la pestaña **Archivos excluidos del análisis**.

Si lo que quieres es eliminar alguno de los elementos encontrados, selecciona la casilla correspondiente, haz clic en **Eliminar** y responde afirmativamente al mensaje de confirmación.

22.2.1 Listado de elementos en cuarentena

En el caso de que existan varios elementos que contengan el mismo tipo de malware, al restaurar o eliminar uno de ellos se restaurarán o eliminarán todos.

Si sitúas el cursor sobre cualquiera de los elementos del listado de búsqueda, aparece una etiqueta amarilla con información sobre dicho elemento.

La columna **Equipo** muestra el nombre del equipo o su IP, en función de lo que selecciones en la opción **Vista por defecto**, en **Preferencias**.

En la columna **Grupo** se detalla el nombre del grupo al que pertenece el equipo. La ruta completa del grupo sólo se muestra en el tooltip y en las exportaciones a Excel y a CSV.

Gracias a la tecnología Anti-Exploit, Endpoint Protection realiza una copia de todos los elementos que envía a cuarentena. En caso de error o de envío a cuarentena de un elemento que no debe ser tratado como tal, Endpoint Protection es capaz de restaurar el archivo en la ruta original.

22.3 Archivos excluidos del análisis

Cuando seleccionas un elemento en la ventana Cuarentena y optas por restaurarlo, el elemento en cuestión desaparece de **Archivos en cuarentena** y pasa a figurar como archivo excluido del análisis (**Cuarentena** > **Archivos excluidos del análisis)**.

De igual manera que has decidido excluir elementos de la cuarentena, puedes también devolverlos a dicha situación. Para ello, marca la casilla del elemento que deseas devolver y haz clic en **Deshacer exclusión**. A continuación acepta el mensaje de confirmación.

El elemento seleccionado desaparecerá del listado de exclusiones, y volverá a aparecer en el listado de archivos en cuarentena cuando sea detectado de nuevo.

23. Informes

Informe ejecutivo

Informe de estado

Informe de detección

Generar informes

Visualizar informes

23.1 Ejecutivo

Información que incluye:

- Resumen del estado de las protecciones instaladas y las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes.
- Listas *top* 10 de equipos con malware detectado y ataques bloqueados, respectivamente.
- Listas *top* 10 de equipos con dispositivos bloqueados.
- Información sobre el estado de las licencias contratadas.
- Detalle del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).

Si dispones de licencias de Endpoint Protection Plus, en el informe se mostrará la cifra de spam detectado así como las listas *top* 10 de:

- Categorías más accedidas.
- Equipos que más acceden.
- Equipos que han accedido a categorías prohibidas y a los cuales se les han bloqueado el acceso a URLs.

23.1.1 Equipos con sistema operativo Linux

En el caso del informe ejecutivo, para los equipos con sistema operativo Linux se indica si tienen los ficheros de firmas actualizados y si la protección está actualizada o no.

23.1.2 Equipos OS X

En el caso de los equipos con OS X, el informe muestra información sobre el estado de la licencias, de las protecciones, información sobre las detecciones, etc.

23.1.3 Dispositivos Android

El informe muestra información sobre el estado de las licencias y de la protección instalada en los dispositivos Android (recuerda que para disponer de la protección antirrobo es necesario poseer licencias de Endpoint Protection Plus).

23.2 De estado

Información que incluye:

- Proporciona una visión general del estado de las protecciones y sus actualizaciones en el momento de solicitar el informe, sin hacer distinción con respecto a los equipos MAC.
- Detalle del número de equipos que se encuentran en proceso de instalación de la protección en el momento de generar el informe (se incluyen los equipos con error en la instalación).

23.2.1 Equipos con sistema operativo Linux

En el informe de estado se indica si los equipos con sistema operativo Linux tienen los ficheros de firmas actualizados y si la protección está actualizada o no.

Además se muestra el estado de las protecciones. Dado que en los equipos con Linux no hay protecciones permanentes sino que se dispone de la protección a través de análisis bajo demanda y programados, el estado de la protección deberá ser correcto y se mostrará el icono verde siempre y cuando se haya instalado correctamente la protección.

23.2.2 Equipos OS X

El estado de la protección instalada en los equipos OS X está incluido dentro de la información resumen para todos los equipos. Es decir, no se hace distinción en función del sistema operativo.

Sin embargo, en la información de detalle de los equipos, el informe sí especifica si se trata de un equipo OS X.

23.3 De detección

Información que incluye:

- Ofrece la evolución de las detecciones realizadas en las últimas 24 horas, últimos 7 días, o último mes.
- Detalla el equipo, grupo, tipo de detección, número de veces (ocurrencia) de la detección, acción realizada y la fecha en que se produjo la detección.

23.3.1 Equipos con sistema operativo Linux

En el informe de detección en los equipos con sistema operativo Linux se muestran las detecciones realizadas por los análisis bajo demanda o programados.

23.3.2 Equipos OS X

El informe incluye las detecciones reportadas por la protección para OS X, tanto en el gráfico como en la información de detalle de los equipos.

23.3.3 Dispositivos Android

El informe incluye las detecciones reportadas por la protección para dispositivos Android, tanto en el gráfico como en la información de detalle de los equipos.

23.4 Generar informes

Con Endpoint Protection puedes obtener informes sobre el estado de la seguridad en tu red informática y las detecciones realizadas en un determinado periodo de tiempo. Además, también puedes seleccionar

el contenido que aparecerá en el informe, si quieres que la información sea detallada y si deseas acompañarla de gráficos. Todo ello de manera rápida y sencilla.

En la ventana principal de la consola Web, haz clic en **Informes**. Se abrirá la ventana **Informes**, que se estructura en dos secciones: en una de ellas podrás seleccionar cuál será el contenido y el alcance del informe y en la otra programar el envío del informe por correo.

23.4.1 Contenido del informe

1. En primer lugar, selecciona el tipo de informe que deseas generar.
2. Selecciona el intervalo que deseas que refleje el informe (últimas 24 horas, últimos 7 días, o último mes).

Según el tipo de informe de que se trate, podrás seleccionar que se muestren diferentes informaciones.

23.4.2 Alcance del informe

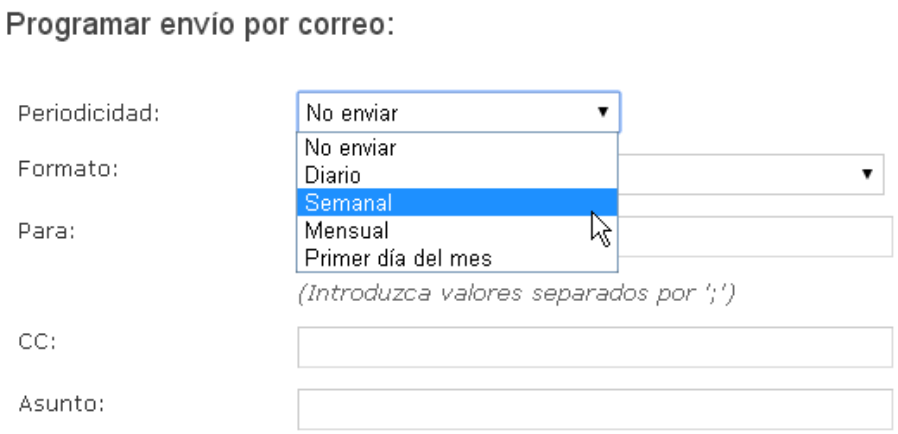
1. En el árbol situado bajo **Alcance del informe**, selecciona el grupo/subgrupo o grupos/subgrupos que se incluirán en el informe.
2. Marca la casilla **Todos** si necesitas seleccionar todos los grupos existentes.

Si no necesitas programar el envío del informe, haz clic en **Generar informe**. El informe se generará al momento y aparecerá en la lista de informes de la parte izquierda de la pantalla.

23.4.3 Programar envío por correo

Si lo necesitas, puedes programar el envío por correo del informe a los usuarios que tú decidas y utilizando determinados formatos.

Las opciones de frecuencia con la que podrás programar los informes son: mensual, semanal, diaria o de primer día del mes.



Podrás programar hasta 27 tareas de envío de informes. Una vez alcanzado dicho valor necesitarás eliminar alguna de ellas para crear más.

Para poder programar tareas de envío de informes es necesario contar con el permiso necesario. Por favor, consulta la sección Tipos de permisos.

Si, por el contrario, no necesitas programar el envío de sus informes, el número de informes que podrás guardar es ilimitado. Podrás acceder de nuevo a un informe haciendo clic en el nombre del mismo en la lista que aparecerá en la parte izquierda de la ventana **Informes**.

Para finalizar con la generación del informe y la configuración de su envío programado, haz clic en **Guardar**. El informe aparecerá en la lista de informes de la parte izquierda de la pantalla, y se enviará en la fecha establecida.

23.5 Visualizar informes

Una vez generado el informe, utilizando los controles de navegación podrás desplazarte por sus páginas, realizar búsquedas en él y exportarlo en un formato diferente.

1. Para exportar el informe, haz clic en el icono  y selecciona en la lista desplegable el formato que desea.

Para poder exportar los informes en Internet Explorer hay que tener desmarcada la casilla No guardar las páginas cifradas en el disco en el apartado Seguridad de la pestaña Opciones avanzadas (Herramientas > Opciones de Internet).

2. Haz click en  para actualizar la vista del informe.

3. Si deseas imprimir el informe, previamente has de exportarlo. Una vez exportado, puedes imprimirlo desde el archivo descargado.

La primera vez que desees imprimir un informe (solo disponible en Internet Explorer) se solicitará la instalación de un control ActiveX de SQLServer.

24.Desinstalación

Tipos de desinstalación

Desinstalación local

Desinstalación centralizada

Desinstalación remota

24.1 Tipos de desinstalación

La desinstalación de las protecciones puede realizarse de diferentes maneras.

Desinstalación local

Si deseas realizar la desinstalación de manera local, tendrás que hacerlo desde cada uno de los equipos, desde la opción correspondiente del panel de control del sistema operativo 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, necesitarás autorización o disponer de las credenciales necesarias para poder desinstalar la protección.

Desinstalación centralizada

Esta desinstalación solo está disponible para equipos con Windows.

La desinstalación de la protección de forma centralizada en varios equipos a la vez se realiza mediante la herramienta de distribución. Esta herramienta se descarga y ejecuta en el equipo desde el que lanzarás el proceso de desinstalación que afectará a los equipos seleccionados.

Desinstalación remota

Esta desinstalación solo está disponible para equipos con Windows.

El método de desinstalación remota se utiliza para desinstalar la protección desde una consola Web situada en una ubicación diferente a la de los equipos afectados. Para ello, se configuran tareas de desinstalación y se especifica cuáles serán los equipos afectados.

> ⚠ ***En caso de ser necesario, tanto en el método de desinstalación local como en el centralizado se le requerirá que introduzca la contraseña que estableciste en su día para el perfil de configuración de la protección correspondiente. La desinstalación protegida con contraseña no es aplicable a equipos con sistema operativo Linux ni OS X.***

24.2 Desinstalación local

La desinstalación de Endpoint Protection se realiza de forma manual desde el panel de control del sistema operativo, 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, necesitarás autorización o disponer de las credenciales necesarias para poder desinstalar la protección.

24.2.1 Desinstalación manual de Endpoint Protection

En Windows 8 o superior:

Panel de Control > Programas > Desinstalar un programa.

También puedes realizar la desinstalación tecleando, en el menú Metro: "desinstalar un programa".

En Windows Vista, Windows 7, Windows Server 2003, 2008 y 2012:

Panel de Control > Programas y características > Desinstalar o cambiar.

En Windows XP:

Panel de Control > Agregar o quitar programas.

En OS X:

Finder > Aplicaciones > Arrastra el icono de la aplicación que deseas desinstalar a la papelera.

En dispositivos Android:

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

24.3 Desinstalación centralizada

Esta desinstalación solo está disponible para equipos con Windows.

En la ventana principal de la consola Web, haz clic en **Instalación** y, a continuación, en la opción **Desinstalación** del menú situado a la izquierda de la ventana. Selecciona **Desinstalación centralizada.** Accederás a la pantalla **Desinstalación centralizada.**

IMPORTANTE: antes de descargar e instalar la herramienta de distribución, consulta los requisitos que debe reunir el equipo desde el que se realizará el despliegue.

24.3.1.1 Descarga e instalación de la herramienta de distribución

1. En la ventana principal de la consola Web, haz clic en **Instalación** y, a continuación, en la opción **Desinstalación** del menú situado a la izquierda de la ventana. Selecciona **Desinstalación centralizada (herramienta de distribución)**.
2. En el cuadro de diálogo de descarga de archivo, selecciona **Guardar**, y cuando la descarga haya finalizado ejecuta el archivo desde el directorio en el que lo hayas guardado. El asistente te guiará a lo largo del proceso de instalación.

Una vez instalada la herramienta de distribución, es necesario abrirla para poder desinstalar la protección de los equipos. Se mostrará la ventana principal desde la que podrás desinstalar las protecciones.

24.3.2 Desinstalación por dominios

1. Abre la herramienta de distribución.
2. En la ventana principal, haz clic en **Desinstalar**.
3. Localiza en el árbol los equipos a los que deseas desinstalar la protección, y marca la casilla correspondiente.
4. Si fuera necesario, se te solicitará que introduzcas la contraseña que estableciste para el perfil de configuración correspondiente.
5. Indica el nombre de usuario y contraseña con privilegios de administrador si en su momento lo estableciste para los equipos seleccionados.

Si deseas que durante el proceso de desinstalación se eliminen los elementos en cuarentena y que al finalizar dicho proceso los equipos se reinicien, marca la casilla correspondiente.

24.3.3 Desinstalación por IP o nombre de equipos

1. Abre la herramienta de distribución.
2. En la ventana principal de la herramienta de distribución, haz clic en **Desinstalar**.
3. Indica los equipos a los que deseas desinstalar la protección. Puedes introducir los nombres de los equipos, sus direcciones IP o rangos de IP, separando estos datos con comas.
4. Si fuera necesario, se te solicitará que introduzcas la contraseña que estableciste para el perfil de configuración correspondiente.
5. Indica el nombre de usuario y contraseña con privilegios de administrador si en su momento lo estableciste para los equipos seleccionados.

Si deseas que durante el proceso de desinstalación se eliminen los elementos en cuarentena, y que al finalizar dicho proceso los equipos se reinicien, marca la casilla correspondiente.

24.4 Desinstalación remota

24.4.1 Creación de tareas de desinstalación remota

Esta desinstalación solo está disponible para equipos con Windows.

Con la desinstalación remota es posible desinstalar la protección desde la consola Web de forma sencilla y eficaz. No será necesario que te desplaces hasta el lugar donde se encuentran

los equipos. Este tipo de desinstalación supone, por tanto, un abaratamiento en costes y desplazamientos.

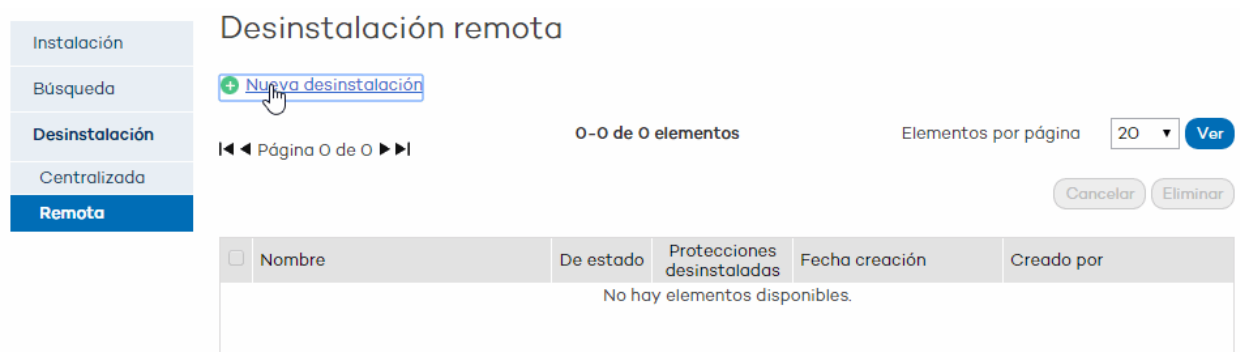
> ***Esta opción no está disponible para equipos con sistema operativo Linux***

El proceso se inicia con la creación y configuración de tareas de desinstalación. Para ello, el administrador seleccionará el grupo y los equipos del grupo a los que afectará la desinstalación, y, finalmente, podrá comprobar cuáles han sido los resultados del proceso de desinstalación y acceder a detalles sobre cada uno de ellos.

24.4.2 Pasos para crear una tarea de desinstalación remota

1. En la ventana principal de la consola Web, haz clic en **Instalación** y, a continuación, en la opción **Desinstalación** del menú situado a la izquierda de la ventana.

2. Selecciona **Desinstalación remota.** Accederás a la pantalla **Desinstalación remota.**



> ***Para establecer tareas de desinstalación el usuario debe poseer permiso de control total o administrador. Para más información, consulta el apartado*** Tipos de permisos.

3. Para establecer una tarea de desinstalación, haz clic en **Nueva desinstalación**.

   A continuación, en la pantalla **Edición de desinstalación** podrás nombrar la tarea y seleccionar el grupo en el que están los equipos cuya protección quieres desinstalar. Los grupos mostrados serán aquellos sobre los que tengas permisos.

> ***Si seleccionas la opción Reiniciar los equipos al finalizar la desinstalación, recuerda que es importante guardar toda la información que se esté utilizando en dichos equipos.***

4. Si el grupo seleccionado tiene aplicado un perfil de configuración que incluye una contraseña de desinstalación, introdúcela en la caja de texto **Contraseña**.

5. Selecciona los equipos en el listado de equipos que se muestran en la pestaña **Equipos disponibles**, y haz clic en **Agregar**. Al seleccionarlos, se mostrarán en la pestaña **Equipos seleccionados**.

Para ver el desarrollo de la desinstalación remota y sus resultados, acude de nuevo a la pantalla **Desinstalación remota**.

24.4.3 Visualización y resultado de la desinstalación remota

- Visualización de las desinstalaciones

Las tareas de desinstalación aparecerán listadas en la pantalla **Desinstalación remota**, desde donde podrás también eliminarlas si así lo deseas, utilizando para ello el botón **Eliminar**.

En esta pantalla la información se organiza en las siguientes columnas:

- **Nombre**: muestra el nombre que se ha dado a la tarea de desinstalación cuando se ha creado.
- **Estado**: indica mediante iconos el estado en que se encuentra la tarea de desinstalación.
- **Protecciones desinstaladas**: detalla el número de protecciones desinstaladas.
- **Fecha creación**: fecha en que se creó la tarea de desinstalación.
- **Creado por**: usuario que creó la tarea de desinstalación.

Según el permiso del que dispongas, podrás crear, visualizar o eliminar tareas de desinstalación de protecciones. Para más información, consulta el apartado Tipos de permisos.

Si deseas ver los detalles de alguna de las desinstalaciones, haz clic sobre el nombre de la desinstalación y accederás a la pantalla Resultado de la desinstalación.

24.4.4 Resultado de la desinstalación remota

Al hacer clic en el nombre de una desinstalación de las que aparecen en la pantalla **Desinstalación remota,** accederás a la pantalla **Resultado de la desinstalación**.

Además del nombre y las fechas de comienzo y final de la desinstalación, esta pantalla también proporcionará información sobre los equipos afectados por la desinstalación y el estado en el que ésta se encuentra.

En el caso de que la tarea esté en estado En espera, la fecha de inicio mostrará un guión (-). Lo mismo sucederá con la fecha de fin si la tarea no ha finalizado.

Si deseas consultar la configuración de la tarea de desinstalación, utiliza el vínculo **Ver configuración**.

24.4.5 Incompatibilidad entre tareas de búsqueda de equipos desprotegidos y desinstalación remota

Si un equipo está involucrado en una tarea de desinstalación (*En espera*, *Iniciando*, o *En curso*), **no es posible** crear otra tarea de desinstalación sobre él ni seleccionarlo como equipo desde el que lanzar búsquedas de equipos desprotegidos.

Si un equipo está ejecutando una tarea de descubrimiento de equipos desprotegidos, **no es posible** crear una tarea de desinstalación sobre él**.**

25. Conceptos clave

Adaptador de red

El adaptador de red permite la comunicación entre los diferentes aparatos conectados entre sí y también permite compartir recursos entre dos o más equipos. Tienen 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

El agente se encarga de las comunicaciones entre los equipos administrados y los servidores de Endpoint Protection, además de la gestión de los procesos locales.

Análisis heurístico genético

El análisis heurístico genético analiza los elementos sospechosos del software malintencionado en base a unos "genes digitales", representados por unos pocos cientos de características de cada archivo analizado.

Así se determina el potencial que el software detectado tiene para llevar a cabo acciones maliciosas o dañinas cuando se ejecuta en un ordenador, y ello permite su clasificación como virus, spyware, troyano, gusano, etc.

Antivirus

Programas cuya función es detectar y eliminar virus informáticos y otras amenazas.

Archivo de identificadores

Es el fichero que permite a los antivirus detectar las amenazas. También es conocido con el nombre de fichero de firmas.

Broadcast

Area lógica en una red de equipos en la que cualquiera de ellos puede transmitir directamente a otro equipo en el dominio broadcast sin precisar ningún dispositivo de encaminamiento.

Consola Web

Mediante la consola Web puedes configurar la protección, distribuir a todos los equipos de tu red y gestionarla. Desde la consola puedes conocer en todo el momento el estado de la protección instalada en tu parque informático y extraer e imprimir los informes que necesites sobre ello.

Cuarentena

La cuarentena es la situación en la que se almacenan contenidos sospechosos de ser maliciosos o no desinfectables, así como el spyware y herramientas de hacking detectadas.

Dialer

Se trata de un 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 a una interfaz 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. Es individual, cada dispositivo tiene su propia identificación MAC determinada.

Equipos excluidos

Son aquellos equipos seleccionados por el usuario a los que no se les aplicará la protección. En calidad de excluidos, la consola Web no muestra ninguna información ni alerta sobre ellos. Ten en cuenta que la exclusión puede deshacerse en cualquier momento.

Equipos sin licencia

Son aquellos equipos cuya licencia ha caducado o en los que ha superado el número máximo permitido de instalaciones de la protección. Estos equipos abandonan la lista de equipos sin licencia en el momento en que el usuario adquiere nuevas licencias.

Firewall

También conocido como cortafuegos. Es una barrera o protección que permite a un sistema salvaguardar la información al acceder a otras redes como, por ejemplo, Internet.

Funcionalidad Peer To Peer (P2P)

La red Peer to Peer (P2P) es una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores respecto de los demás nodos de la red. Es una forma legal de compartir archivos de forma similar a como se hace en el correo electrónico o mensajería instantánea, sólo que de una forma más eficiente.

En el caso de Endpoint Protection, la funcionalidad Peer To Peer reduce además el consumo de ancho de banda de la conexión a Internet, dando prioridad a que los equipos que ya han actualizado un archivo desde Internet lo compartan con otros que también necesitan actualizarlo. Así se evitan los accesos masivos a Internet y los consiguientes colapsos.

Funcionalidad Proxy

Esta funcionalidad permite el funcionamiento de Endpoint Protection en equipos sin acceso a Internet, realizándose los accesos a través de otro agente instalado en un equipo de su misma subred.

Grupo

En Endpoint Protection, un grupo es un conjunto de equipos informáticos a los que se aplica el mismo perfil de configuración de la protección. En Endpoint Protection existe un grupo inicial o

grupo por defecto -*Default*- en el que se pueden incluir todos los ordenadores a proteger. También se pueden crear grupos nuevos.

Herramienta de distribución

Una vez descargada de Internet al PC administrador e instalada en éste, la herramienta de distribución permite instalar y desinstalar a distancia las protecciones en los equipos seleccionados. En Endpoint Protection, la herramienta de distribución solo se puede utilizar para desplegar la protección en equipos con sistema operativo Windows.

Herramienta de hacking

Programa que puede ser utilizado por un hacker 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.

Identificador del agente de administración

Número único o GUID (*Globally Unique IDentifier*) que identifica a cada agente de administración de Endpoint Protection.

Joke

No es un virus, sino bromas de mal gusto que tienen por objeto hacer pensar a los usuarios que han sido afectados por un virus.

Malware

Es un 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 tiene como objetivo infiltrarse en dañar un ordenador sin el conocimiento de su dueño y con finalidades muy diversas.

Nodo

Un nodo es un punto de intersección o unión de varios elementos que confluyen en el mismo lugar. Aplicado a las redes informáticas, cada uno de los equipos de la red es un nodo y, si la red es Internet, cada servidor constituye también un nodo.

Nube

La computación en la nube (Cloud Computing) es una 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.

Perfil

Un perfil es una configuración específica de la protección. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que forman parte de dicho grupo o grupos.

Phishing

Intento de conseguir información confidencial de un usuario de forma fraudulenta. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

Proceso local

Los procesos locales son los encargados de realizar tareas necesarias para la correcta implantación y administración de la protección en los equipos.

Programas potencialmente no deseados

Son programas que se instalan en el equipo aprovechando la instalación de otro programa que es el que realmente se desea instalar.

Al finalizar la instalación del programa se muestran mensajes al usuario para que acepte la instalación de otros "programas" (PUPs) que aparentemente "forman parte" del que se quiere instalar y se presentan como necesarios para una correcta instalación. Al aceptar, se abre la puerta del equipo del usuario a estos programas potencialmente no deseados.

Protocolo

Sistema utilizado para la interconexión entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Un servidor proxy actúa como un intermediario entre una red interna (por ejemplo, una intranet) y una conexión externa a Internet. De esta forma, se puede compartir una conexión para recibir ficheros desde servidores Web.

Puerto

Punto de acceso a un ordenador o medio a través del cual tienen lugar las transferencias de información (entradas / salidas) del ordenador con el exterior y viceversa (vía TCP-IP).

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los propios normalmente). Este tipo de software no es malicioso en sí mismo, pero es utilizado por los piratas informáticos para esconder evidencias y utilidades en los sistemas previamente comprometidos. Existen ejemplares de malware que emplean rootkits con la finalidad de ocultar su presencia en el sistema en el que se instalan.

Servidor Exchange

Es un servidor de correo de la compañía Microsoft. El servidor Exchange almacena los correos electrónicos entrantes y/o salientes y gestiona la distribución de los mismos en las bandejas de entrada configuradas para ello. Para conectarse al servidor y descargar el correo electrónico que haya llegado a su bandeja, los usuarios han de tener instalado en su equipo un agente de correo electrónico.

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.

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.

Topología de red

Cadena de comunicación que los nodos que conforman una red usan para comunicarse.

Troyanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario.

Red pública

Una red de este tipo es propia de cyberlocales, aeropuertos, etc. Conlleva limitación de su nivel de visibilidad y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Red de confianza

Este tipo de red generalmente es de oficina o casera. El equipo es perfectamente visible para el resto de equipos de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

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.

Virus

Programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

26. Apéndice 1

Operaciones por línea de comandos (Windows)

26.1 Introducción

Las operaciones básicas que se van a poder realizar son:

- Instalación remota
- Verificación remota de la instalación de la protección
- Desinstalación
- Actualización de los ficheros de firmas
- Actualización de políticas o configuraciones
- Obtención de la fecha de última actualización del fichero de firmas
- Obtención de la información del estado del antivirus y del firewall

26.2

26.3 Paso previo. Descarga del paquete de Instalación

Antes de lanzar la instalación, es necesario obtener el paquete de Instalación de Endpoint Protection: WaAgent.msi. Este paquete de instalación podrá estar ubicado en el repositorio de las soluciones SaaS de Remote Desktop Management para el cliente concreto sobre el que se esté realizando la instalación.

26.3.1 Opciones en la descarga del paquete de instalación

El paquete de instalación utilizado puede ser uno genérico o uno específico para el cliente y para el cliente y perfil de seguridad.

Según la opción seleccionada, la línea de comando utilizada deberá complementarse con parámetros específicos o no. Las Opciones de descarga son:

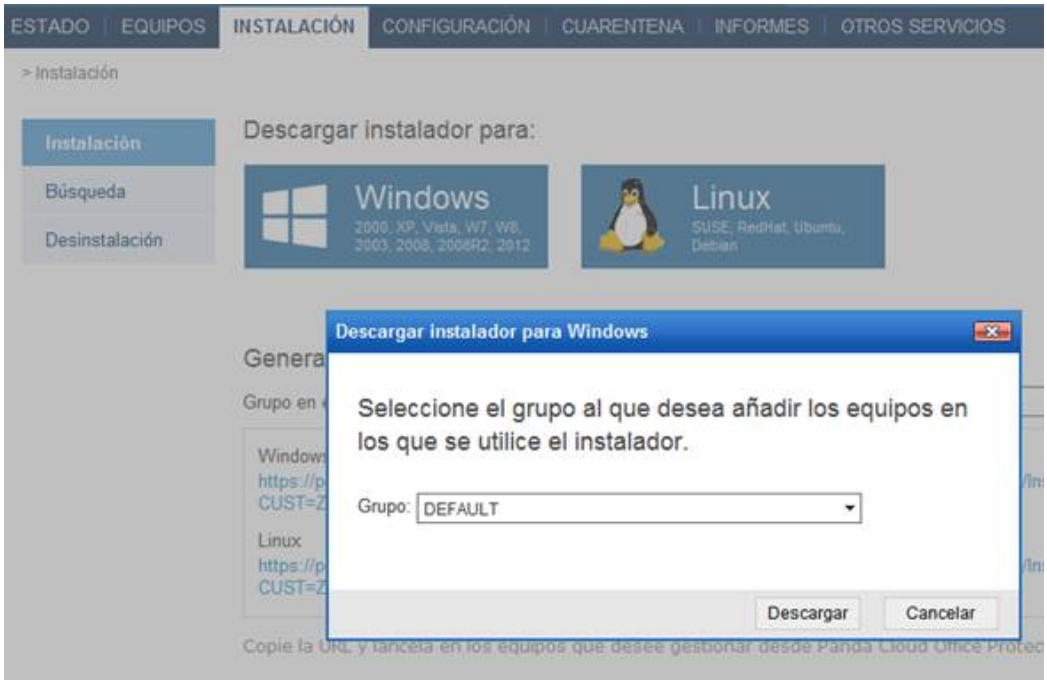
1. Descargar el paquete desde una cuenta cualquiera de cliente y para el perfil DEFAULT. Posteriormente en la instalación se podrá pasar como parámetro el Identificador del cliente y el correspondiente al grupo con un perfil de seguridad para ese cliente. De esta forma estaremos indicando a qué cliente pertenece la protección instalada y a que perfil de seguridad y grupo.
2. Descargar para cada cliente su propio paquete de instalación. En este caso, no es necesario indicar el identificador del cliente.
3. Descargar para cada cliente y por cada grupo con su perfil de seguridad, su propio paquete de instalación. En este caso, no es necesario indicar ni el identificador del cliente ni el grupo al que pertenece el equipo.

26.3.2 Pasos para la descarga del paquete de instalación (WaAgent.msi)

1. Accedemos a la cuenta de cliente específica a través de la consola Panda Cloud. (https://www.pandacloudsecurity.com/)

2. Hacemos clic en el icono correspondiente a Endpoint Protection para acceder a la consola.

3. Accedemos a la sección de **Instalación**. A continuación, descargaremos el paquete de instalación de este cliente para el grupo Default, que pertenece al perfil de seguridad default, es decir, antivirus activado.



4. Descargamos el paquete de instalación y lo guardamos en local.

26.4 Pasos de Instalación

26.4.1 Paso 1.

Descargar el paquete de instalación en los equipos que deseamos proteger.

26.4.2 Paso 2.

Ejecutar la sentencia de instalación en el directorio donde se ha descargado el paquete de instalación.

msiexec /i "WaAgent.msi" /qn <GROUP> <GUID> <ALLOWREBOOT>

Los parámetros opcionales son:

<GROUP> El grupo y, por tanto, el perfil de seguridad del equipo dentro del parque del cliente.

El msi ya tendrá un valor asignado en la descarga, este valor se puede sobrescribir indicando el parámetro GROUP.

<GUID> Identificador del cliente al que pertenece el equipo donde se está realizando la instalación.

El msi ya tendrá un valor asignado en la descarga, este valor se puede sobrescribir indicando el parámetro GUID.

El GUID se obtiene en la sección de **Instalación** de la consola Web, como parámetro CUST en el acceso directo al paquete de instalación:

<ALLOWREBOOT> Permitirá indicar si el instalador de la protección puede o no reiniciar el equipo, si fuera necesario, una vez haya finalizado.

ALLOWREBOOT=TRUE ==> permite el reinicio

ALLOWREBOOT=FALSE No permite el reinicio

Ejemplos

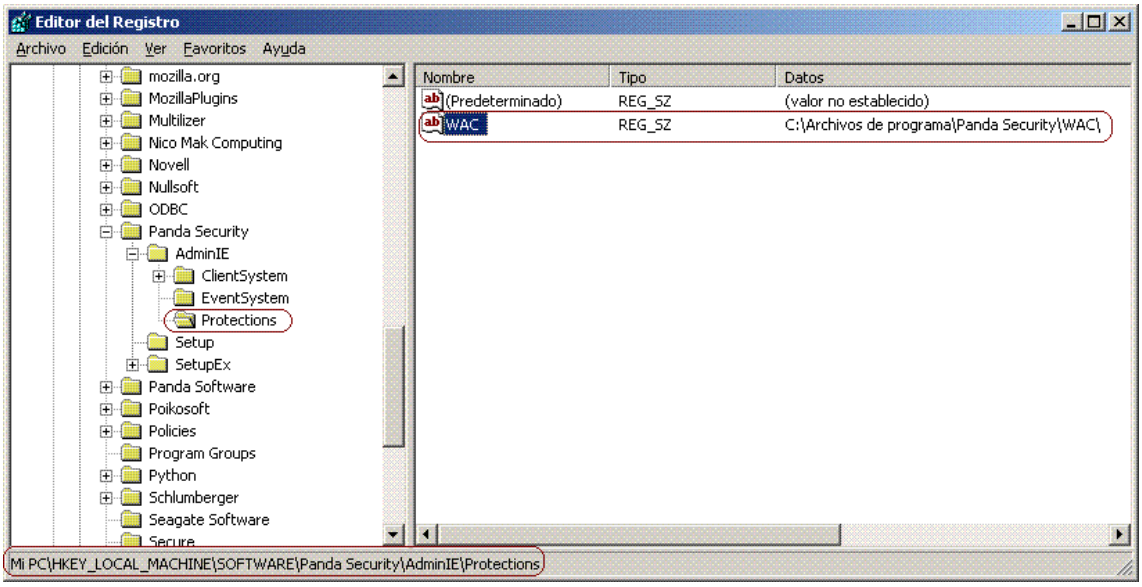
msiexec /i " WaAgent.msi" GROUP=GROUP_ONLYAV GUID={81729831} /qn

msiexec /i " WaAgent.msi" GROUP=DEFAULT ALLOWREBOOT=TRUE /qn

26.5 Verificación de la instalación de la protección

La comprobación de que en el equipo se encuentra instalada la protección de Endpoint Protection, se realiza mediante consultar de la entrada del registro.

HKLM\Software\Panda Security\AdminIE\Protections



26.5.1 Pasos para la verificación

Paso 1

Comprobar la existencia de la entrada.

HKLM\Software\Panda Security\AdminIE\Protections

Si existe, ir a paso 2. Si no existe, entonces la protección no está instalada.

Paso 2

Obtener el valor de WAC.

Los datos asociados a este valor representan la ubicación de la instalación de la protección.

Si existe y no es vacío, entonces la protección está instalada.

Si no existe o es vacío, entonces la protección no está instalada.

26.6 Desinstalar Endpoint Protection

Para desinstalar Endpoint Protection de un equipo, se debe desinstalar primero el agente y luego la protección.

26.6.1 Pasos para la desinstalación

Paso 1.

El comando de desinstalación del agente se obtiene mediante consulta al registro del valor UnPath de la clave

HKLM\SOFTWARE\Panda Security\SetupEx\AdminIE.

Paso 2.

Ejecución de la desinstalación del agente de forma silenciosa:

<valor de UnPath de HKLM\SOFTWARE\Panda Security\ SetupEx\AdminIE > /qn PASS=<Contraseña>

Sólo será necesario utilizar el parámetro PASS en caso de haber configurado una contraseña de desinstalación en el perfil.

Paso 3.

El comando de desinstalación de la protección se obtiene mediante consulta al registro del valor UnPath de la clave HKLM\SOFTWARE\Panda Software\Setup.

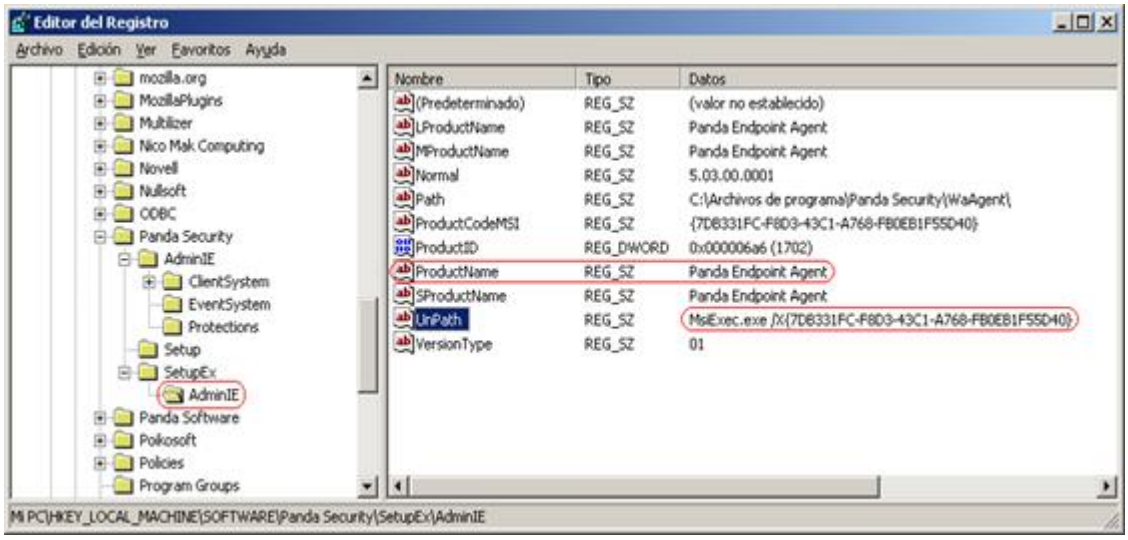
Paso 4.

Ejecución de la desinstalación de la protección de forma silenciosa:

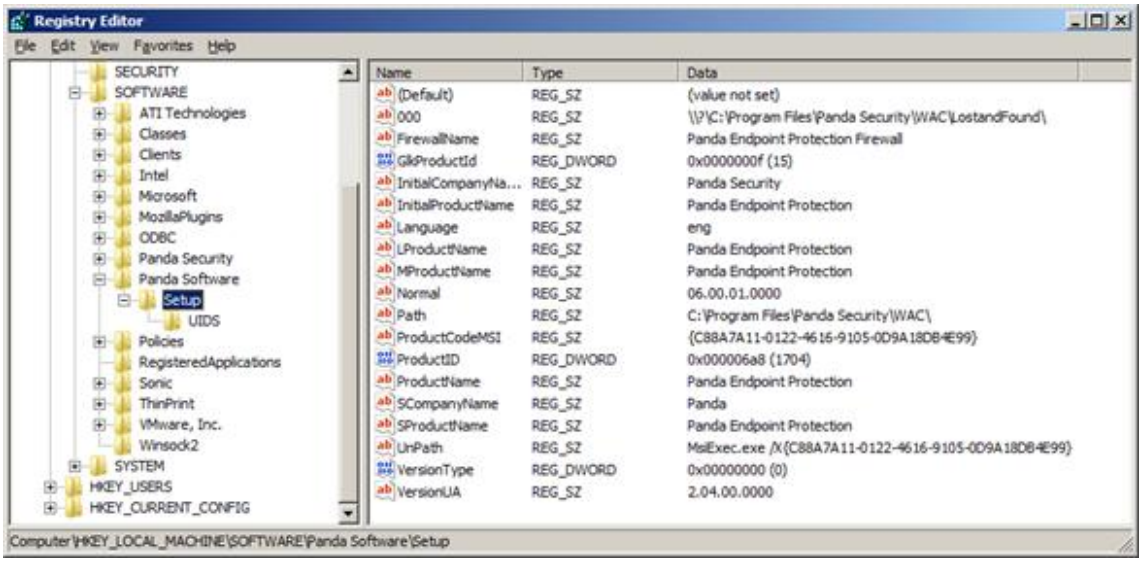
<valor de UnPath de HKLM\SOFTWARE\Panda Software\Setup> > /qn PASS=<Contraseña>

Sólo será necesario utilizar el parámetro PASS en caso de haber configurado una contraseña de desinstalación en el perfil.

Ejemplo



MsiExec.exe /X{7DB331FC-F8D3-43C1-A768-FB0EB1F55D40} /qn



MsiExec.exe /X{C88AtAA-0122-4616-9105-0D9A18D84E99} /qn

26.7 Actualización del fichero de firmas

La actualización del fichero de firmas se realiza mediante el proceso local `WalUpd`.

26.7.1 Pasos para la actualización de los ficheros de firmas

Actualización de políticas o configuraciones

Si se realiza algún cambio en el perfil de seguridad del grupo al que pertenece el equipo protegido, esta actualización se propagará al puesto, cuando este realice una consulta al servidor. Sin embargo, es posible forzar la actualización de la configuración mediante el proceso local WalConf.

26.7.2 Pasos para la actualización de la configuración

CD %ProgramFiles %\Panda Security\WaAgent\WasLpMng

WAPLPMNG.exe WALCONF -force

CD %ProgramFiles %\Panda Security\WaAgent\ WasLpMng

WAPLPMNG walscan –T:<FILENAME> -P:WAC –A:START

Obtención de la fecha de última actualización del fichero de firmas

La determinación de si la protección se encuentra actualizada con los últimos ficheros de firmas, se elabora en el backend de Endpoint Protection.

El agente envía al servidor su última fecha de actualización y ésta se contrasta con la fecha de los últimos ficheros de firmas publicados.

En esta sección se explica el método para obtener la última fecha de actualización de los ficheros de firmas en el equipo.

Es importante tener presente que esta información, junto con otra sobre el estado real de la protección, se actualiza continuamente en el equipo en un fichero denominado WALTEST.DAT.

Este fichero tiene formato de fichero XML, por lo que puede tratarse como tal para analizar sintácticamente su contenido en busca de la información que nos interese.

En la sección <PavsigDate> encontramos la información relativa a la fecha del último catálogo de fichero de firmas utilizado para actualizar.

Necesitamos, por tanto, recuperar este fichero y realizar un tratamiento de su contenido en búsqueda del tag <PavsigDate>

26.7.3 Pasos para obtener la fecha de los ficheros de firmas

Paso 0

Previamente a la obtención de la información, se recomienda lanzar la actualización de los ficheros de. Posteriormente será necesario actualizar la información del fichero waltest.dat lanzando el proceso local waltest.

CD %ProgramFiles %\Panda Security\WaAgent\WasLpMng

WAPLPMNG.exe WALUPD –force

WAPLPMNG waltest –force

(Update the file WALTEST.DAT)

Paso 1

Nos situamos en el directorio del proceso local Waltest y recuperamos el fichero waltest.dat.

CD &ProgramFiles %\Panda Security\WaAgent\WalTest

(find the file: WALTEST.DAT)

Paso 2

Buscamos el tag "<PavSigDate>". Para ello, podemos utilizar un programa que nos permita analizar sintácticamente ficheros XML. Necesitaremos renombrar el fichero waltest.dat a XML, o

bien podremos utilizar el comando de DOS FindString que nos permite buscar cadenas en ficheros.

A continuación se explica cómo hacerlo mediante el comando FindString:

FindStr "<PavSigDate>" waltest.dat

(find tag <PavSigDate>)

Obtendremos una información similar a la siguiente:

<PavSigDate>2012-03-23 12:25:43</PavSigDate>

En este ejemplo, la fecha del último catálogo utilizado para actualizar es "2012-03-23 12:25:43".

Obtención de la información del estado de la protección

Esta información se actualiza continuamente en el fichero denominado WALTEST.DAT. Se localiza junto a otra relativa al estado real de la protección.

Como ya se ha indicado en el punto anterior, este fichero tiene formato de fichero XML, por lo que puede tratarse como tal para analizar sintácticamente su contenido en busca de la información que nos interese.

En la sección <AVSTATUSINFO> encontramos la información relativa al estado de cada una de las protecciones del antivirus. Cada sección <JOBID> hace referencia a cada protección y la información disponible es:

<IsInstalled> Protección instalada

<IsStarted> Esta ejecutándose.

<IsActivated> Esta activada desde configuración

Los valores y significados de los JobIDs son:

JobID	Significado
2	Protección de archivos (file resident)
4	Protección de correo (mail resident)
64	Protección firewall
256	Control de dispositivos
512	Protección de transporte en servidores Exchange.

1024	Protección de buzones en servidores Exchange.
2048	Protección anti-spam en servidores Exchange.
4096	Monitorización de URLs.
8192	Protección antimalware en navegación web.

26.7.4 Pasos para obtener información del estado de la protección

Paso 0

Previamente, aunque no sea necesario, se recomienda lanzar la actualización del fichero waltest.dat, ejecutando para ello, el proceso local WalTest.

CD %Program Files %\Panda Security\WaAgent\WasLpMng

WAPLPMNG waltest –force

(Update the file WALTEST.DAT)

CD %ProgramFiles %\Panda Security\WaAgent\WalTest

Paso 1

Nos situamos en el directorio del proceso local Waltest y recuperamos el fichero waltest.dat.

CD %Program Files %\Panda Security\WaAgent\WalTest

(find the file: WALTEST.DAT)

Paso 2

Obtenemos la información que buscamos.

FindStr "<JobID> <IsInstalled> <IsStarted> <IsActivated> " waltest.dat

(find info in the file WALTEST.DAT)

Obtendremos una información similar a la siguiente:

<AVStatusInfo><JobStatusInfo><JobInfo><JobID>2</JobID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>4</JobID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>64</JobID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>256</JobID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

</JobStatus></JobStatusInfo>

En este ejemplo vemos lo siguiente:

Residente de ficheros (JobID = 2): Instalado, ejecutándose y activo.

Residente de correo (JobID = 4): Instalado, ejecutándose y activo.

Firewall (JobID = 64): Instalado, ejecutándose y activo.

Device Control (JobID = 256): Instalado, ejecutándose y activo.

Formato WALTEST.DAT. <AVSTATUSINFO>

<AVProducts><AVProduct><AVID><AVName>WAC</AVName>

<AVVersion>6.00.12.0000</AVVersion>

</AVID><PendingUpgrade>false</PendingUpgrade>

<PavSigDate>2012-03-23 12:25:43</PavSigDate>

<MUID>69c87ea1-90d4-463d-999a-89302d311e26</MUID>

<AVStatusInfo><JobStatusInfo><JobInfo><JobID>2</JobID>

<UnitID>1</UnitID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

<IsStatusCoherence>true</IsStatusCoherence>

<ReqConform>0</ReqConform>

</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>4</JobID>

<UnitID>1</UnitID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

<IsStatusCoherence>true</IsStatusCoherence>

<ReqConform>0</ReqConform>

</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>64</JobID>

<UnitID>2</UnitID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

<IsStatusCoherence>true</IsStatusCoherence>

<ReqConform>0</ReqConform>

</JobStatus></JobStatusInfo><JobStatusInfo><JobInfo><JobID>256</JobID>

<UnitID>8</UnitID>

</JobInfo><JobStatus><IsInstalled>true</IsInstalled>

<IsStarted>true</IsStarted>

<IsActivated>true</IsActivated>

<IsStatusCoherence>true</IsStatusCoherence>

<ReqConform>0</ReqConform>

</JobStatus></JobStatusInfo></AVStatusInfo></AVProduct></AVProducts></TestRepor>

27. Apéndice 2

Proceso de despliegue de la protección (Windows)

27.1 Introducción

Antes de entrar al detalle de los archivos, claves de registro, directorios y carpetas que se crean al desplegar la protección en los equipos, se ofrece información acerca del agente de administración, la funcionalidad P2P o rumor, la funcionalidad proxy y tiempos de instalación de la protección.

Todos ellos son aspectos a tener en cuenta para conocer con más detalle el proceso de despliegue.

27.2 El agente de administración

El agente es el encargado de las comunicaciones entre los equipos administrados y los servidores de Endpoint Protection. Se encarga de "hablar" con los agentes de los diferentes equipos de su mismo grupo y de las descargas de programas de instalación desde Internet.

Al ejecutar el instalador del agente, se lanza el proceso de instalación de Endpoint Protection. A lo largo de este proceso de instalación se realizarán diferentes tareas, como la descarga de las configuraciones, la instalación de las protecciones, la actualización del archivo de identificadores, etc.

Como elemento fundamental en el diálogo entre los diferentes equipos, el agente es imprescindible para la puesta en práctica de la funcionalidad P2P, que se describe en el siguiente apartado.

27.3 Funcionalidad Peer to Peer o de rumor

La funcionalidad Peer to Peer, también conocida como "rumor", consiste en una funcionalidad de tipo P2P que reduce el consumo de ancho de banda de la conexión a Internet.

Para ello, otorga prioridad a que los equipos que ya han actualizado un archivo desde Internet lo compartan con otros que también necesitan actualizarlo. De esta forma, se evitan los accesos masivos a Internet y los consiguientes colapsos.

La funcionalidad P2P es de gran utilidad en el despliegue de Endpoint Protection a la hora de descargarse el programa de instalación. Cuando uno de los equipos ha descargado de Internet el programa de instalación, los otros tienen conocimiento de ello por medio de sus respectivos agentes de comunicación, que han sido activados y han puesto en marcha el proceso de instalación de Endpoint Protection.

Estos agentes de comunicación, en lugar de acceder a Internet acuden al equipo que posee el programa de instalación, lo cogen directamente de él y a continuación lanzan la instalación en su equipo correspondiente.

Pero esta funcionalidad P2P es muy útil también en el caso de actualizaciones del motor de la protección y del archivo de identificadores, y se implementa en los dos procesos locales que necesitan descargar ficheros de Internet: WalUpd y WalUpg.

La activación se hace en los ficheros de configuración de estos procesos:

WALUPD.ini

[GENERAL]

UPDATE_FROM_LOCAL_NETWORK=1

WALUPG.ini

[GENERAL]

UPGRADE_FROM_LOCAL_NETWORK=1

La funcionalidad P2P funciona de forma independiente en cada uno de estos procesos locales, pudiendo estar activa únicamente en uno de ellos.

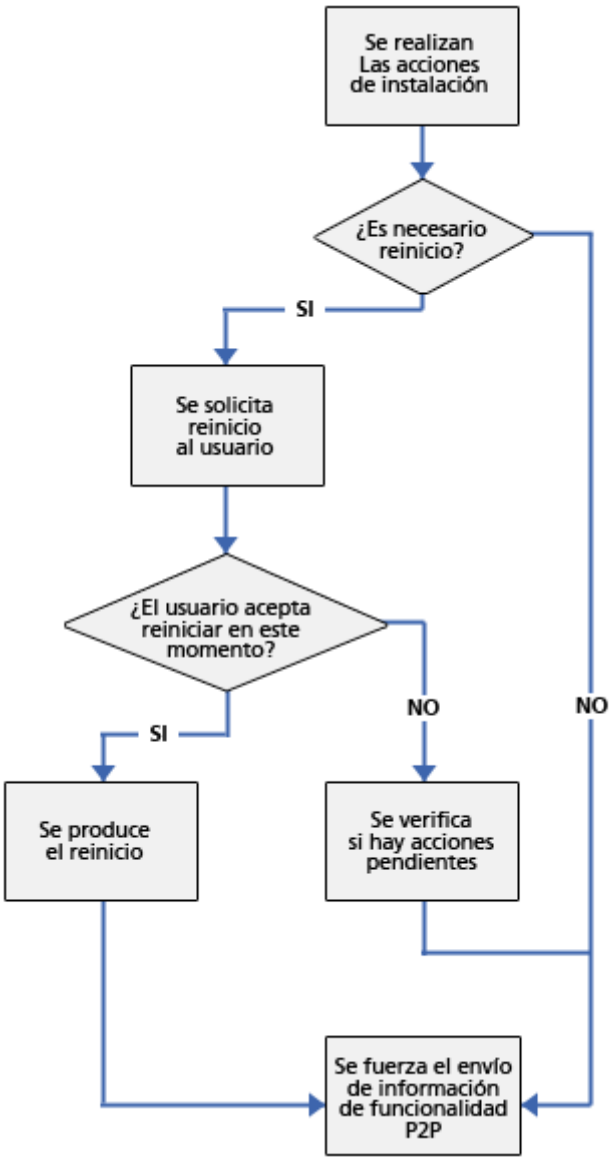
27.3.1 Bases del funcionamiento de la funcionalidad P2P

Cuando un equipo termina de actualizar los ficheros de firmas o alguna protección -o el propio agente- lo comunica vía broadcast al resto de equipos de la red.

En cuanto al envío de la información en WALUpg, puede ser necesario reiniciar el equipo después de la instalación/actualización de las protecciones.

Si el usuario opta por no reiniciar el equipo inmediatamente sino más tarde, la información de la funcionalidad P2P se enviará de forma inmediata en lugar de esperar al reinicio.

El funcionamiento se muestra en el siguiente diagrama:



1. Los equipos que reciben el mensaje guardarán la información que han recibido para utilizarla cuando la necesiten.
2. Si un equipo necesita algún fichero, antes de intentar descargarlo de Internet comprobará si puede obtenerlo de otro equipo. Si es así, enviará un mensaje al equipo que lo tiene disponible para solicitárselo. El fichero se recibirá de forma asíncrona y se esperará un tiempo máximo a recibirlo antes de reintentar.
3. El equipo poseedor del fichero recibirá un mensaje de solicitud y como respuesta enviará un mensaje con el fichero.
4. El equipo que solicitó el fichero lo recibirá y podrá proseguir con la actualización o upgrade.

Para que un equipo pueda facilitar ficheros a otros a través de la funcionalidad P2P debe tener al menos 128 MB de RAM.

27.3.2 Proxy dinámico

El agente de comunicación guarda una lista con información sobre los equipos de la red cuyos agentes son capaces de enviar mensajes a Internet. Estos agentes se denominan proxys.

> ***Para poder actuar como proxy para otros agentes, un equipo debe cumplir los siguientes requisitos: disponer de conexión directa a Internet y, al menos,de 128 MB de RAM. Además, el equipo no puede estar en lista negra y debe haber concluido completamente la secuencia de instalación***

Cuando la lista de proxys está vacía o ninguno de los agentes que están en ella responde (Disponibilidad = 0), el agente envía un mensaje por broadcast a la subred preguntando ¿quién es Proxy? para que estos le respondan y pueda mandar mensajes a Internet a través de ellos.

Mientras realiza la espera por datos de la lista de proxys válidos, el módulo del Proxy no atenderá peticiones de otros mensajes.

La lista de proxys tendrá un valor asociado para cada uno de ellos con el número de intentos que se permiten fallar en la comunicación con otro agente antes de invalidar ese agente como proxy.

Por defecto el número de veces será 3, y cuando este valor alcance 0 se entenderá que ese agente no es válido como proxy. Si en algún momento todos los proxys de la lista son inválidos, se entiende que la lista es no válida en su conjunto y se comenzará la búsqueda de proxys, lanzando un mensaje "¿quién es proxy?".

¿qué sucede si un equipo proxy no dispone de conexión a Internet?

Puede ocurrir que el mensaje se envíe correctamente a un proxy de la lista pero que éste, al intentar mandar el mensaje a Internet, descubra que ya no tiene conexión.

En ese caso, el agente remoto repetirá la secuencia aquí descrita reenviando el mensaje a un proxy de su lista, pero además enviará por TCP al agente del que le llegó el mensaje otro de tipo "Yo no soy Proxy", para indicarle que lo borre de su lista porque ya no tiene conexión a Internet.

Este proceso se repetirá hasta que el mensaje se envíe correctamente a Internet o hasta que pase por un número máximo de proxy sin conseguir enviarse, en cuyo caso se perderá.

Se puede configurar el número de proxys por los que puede pasar un mensaje. Por defecto sólo se enviará a 1, y si falla el envío desde ése se perderá el mensaje.

Dentro del mensaje se guarda la lista de proxys por los que ha pasado, de modo que no se envíe dos veces al mismo proxy sin conexión a Internet.

27.3.3 Proxy estático

Si deseamos que todos los accesos a Internet se hagan a través de un equipo concreto decidido por el administrador (proxy estático), en lugar de por equipos determinados de forma

dinámica, el agente de comunicaciones permite especificar qué equipo deseamos que actué como proxy.

El equipo que actué como proxy estático debe cumplir los siguientes requisitos:

1. Debe tener un agente instalado versión 6.0 o superior.
2. Debe tener acceso directo a Internet.
3. Disponer de al menos 128 MB de memoria.
4. Debe haber comunicado con el servidor en las últimas 72 horas.
5. Además, el equipo no puede estar en lista negra y debe haber concluido completamente la secuencia de instalación.

Si en algún momento el equipo que se estableció para que actuara como proxy estático dejara de cumplir alguno de los requisitos necesarios para ejercer como tal, se desactivará en la consola la configuración del proxy estático. A continuación desaparecerá el nombre del equipo que estaba configurado y se mostrará un mensaje indicando cuál de los requisitos se incumple.

También es posible seleccionar otro equipo para que realice las funciones de proxy estático. Si un equipo deja de ser proxy estático por haber sido incluido en la lista negra, una vez que deje de pertenecer a dicha lista, si se desea que actúe de proxy estático será necesario configurarlo de nuevo para que transiten por él todas las comunicaciones con el servidor.

Cuando el agente tenga que realizar un acceso a Internet, en primer lugar intentará comunicarse utilizando el proxy estático.

Si la comunicación con el proxy estático no es posible, se intentará llevar a cabo el acceso a internet siguiendo la secuencia de comunicaciones habitual:

1. Si tiene una configuración válida almacenada, intentará la comunicación utilizando dicha configuración.
2. En caso contrario, intentará comunicarse mediante conexión directa a Internet.
3. Si tampoco consigue la conexión directa, lo intentará a través de otro equipo proxy dinámico, cuyo funcionamiento se ha detallado en el apartado anterior.

Cuando el equipo que está actuando como proxy recibe una petición de acceso a Internet, intentará realizar la conexión de forma directa. Si la conexión se realiza con éxito enviará la respuesta obtenida al agente que solicitó la conexión.

La configuración del proxy estático se realiza en el apartado **Opciones de conexión con el servidor** de la pestaña **Opciones avanzadas** del menú **Windows y Linux** .

27.4 Despliegue de Panda Endpoint Agent

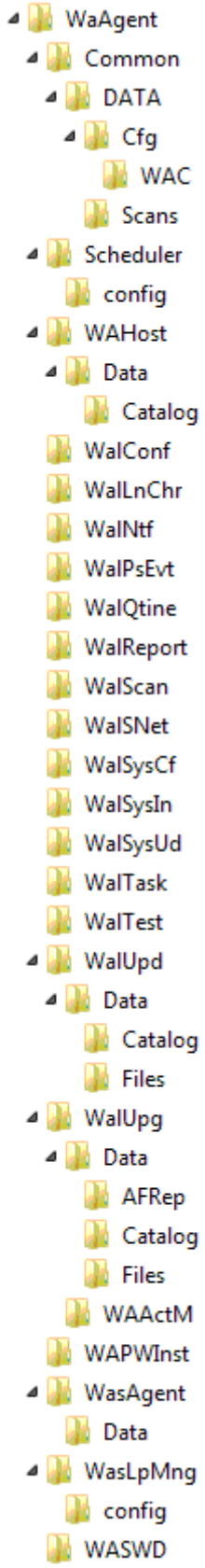
Módulos principales de la arquitectura

Panda Endpoint Agent está formado por cuatro componentes principales:

1. Agente de administración.
2. Procesos Locales.
3. Watchdog.
4. Planificador de tareas (scheduler).

27.4.1 Árbol de carpetas y entradas de registro de Panda Endpoint Agent

En el diagrama siguiente AdminIEClientPath es la ruta raíz donde se han instalado los módulos.



WaAgent– carpeta raíz de instalación de Panda Endpoint Agent.

Common – carpeta donde se guardan los ficheros de uso común, como WalAgApi.dll, librerías de núcleo, etc. Durante la ejecución de los procesos locales se creará en esta carpeta una subcarpeta "Data".

Scheduler – carpeta donde se guardan los ficheros del planificador de tareas.

Scheduler\Config – carpeta donde se guardan los ficheros de tokens para el planificador de tareas.

WaHost – carpeta donde se guardan los ficheros del servicio del agente de administración. Durante la ejecución de los procesos locales se puede crear en esta carpeta una subcarpeta "Data".

WalConf – carpeta donde se guardan los ficheros del proceso local WalConf.

WalTest – carpeta donde se guardan los ficheros del proceso local WalTest.

WalLnChr – carpeta donde se guardan los ficheros del proceso local WalLnChr.

WalNtf – carpeta donde se guardan los ficheros del proceso local WalNtf.

WalPsEvt – carpeta donde se guardan los ficheros del proceso local WalPsEvt.

WalQtine – carpeta donde se guardan los ficheros del proceso local WalQtine.

WalReport – carpeta donde se guardan los ficheros del proceso local WalReport.

WalScan – carpeta donde se guardan los ficheros del proceso local WalScan.

WalSNet – carpeta donde se guardan los ficheros del proceso local WalSNet.

WalSysCf – carpeta donde se guardan los ficheros del plugin WalSysCf.

WalSysIn – carpeta donde se guardan los ficheros del plugin WalSysIn

WalSysUd – carpeta donde se guardan los ficheros del plugin WalSysUd

WalTask – carpeta donde se guardan los ficheros del plugin WalTask.

WalTest – carpeta donde se guardan los ficheros del proceso local WalTest.

WalUpd – carpeta donde se guardan los ficheros del proceso local WalUpd. Durante la ejecución del proceso local se creará en esta carpeta una subcarpeta "Data".

WalUpg – carpeta donde se guardan los ficheros del proceso local WalUpg. Durante la ejecución del proceso local se creará en esta carpeta una subcarpeta "Data".

WAPWInst – carpeta donde se guardan los ficheros del proceso que supervisa la instalación.

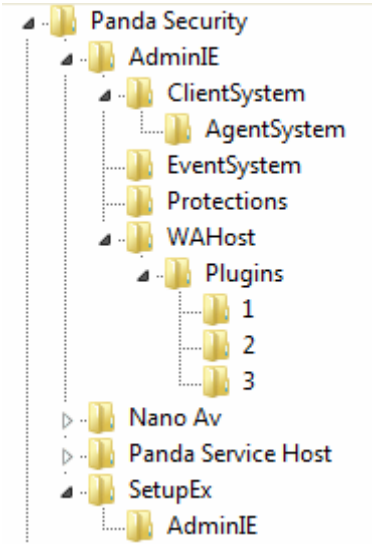
WasAgent – carpeta donde se guardan los ficheros del agente de comunicaciones. Al ejecutarse el agente se creará en esta carpeta una subcarpeta "Data".

WasAgent – carpeta raíz de instalación del agente de administración. Al ejecutarse el agente se creará en esta carpeta una subcarpeta "Data".

WasLpMng – carpeta donde se guardan los ficheros del gestor de procesos locales.

WasLpMng\Config – carpeta donde se guardan los ficheros de tokens para el gestor de procesos locales.

27.4.2 Árbol de Entradas de registro de Windows



`Panda Security` se refiere a la clave del registro de Windows

HKEY_LOCAL_MACHINE\SOFTWARE\Panda Security\

AdminIE

Carpeta dentro de la cual se crean todas las entradas de registro propias de Endpoint Protection.

ClientSystem

Clave de registro que contiene entradas de Panda Endpoint Agent. Estas entradas son:

- InstallPath – Contiene el directorio raíz en el que se ha instalado Panda Endpoint Agent (lo que arriba se denominaba "AdminIEClientPath").
- EventSystem - Contiene la configuración del sistema de eventos.
- Protections - Contiene información sobre la protección.

WAHost

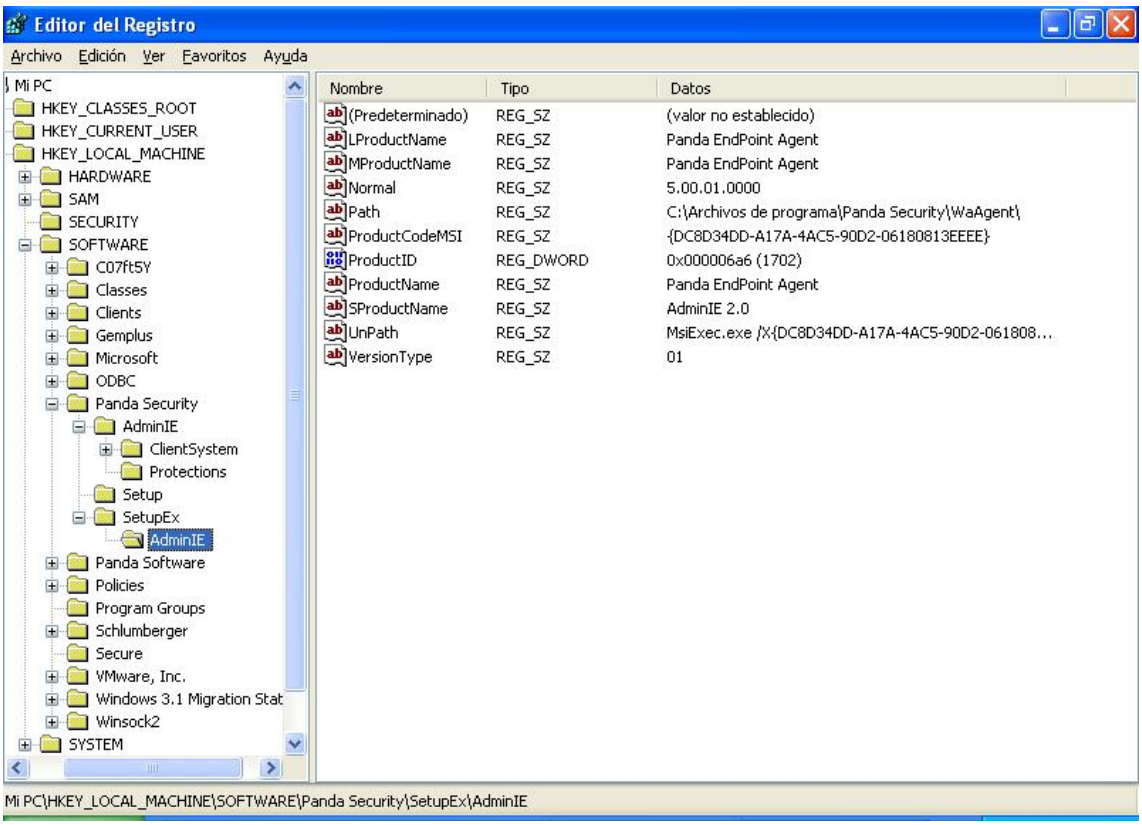
Contiene la configuración del servicio del agente de administración.

SetupEx

Carpeta dentro de la cual se crean todas las entradas de registro que serán utilizadas por los instaladores que emplean el Agente.

AdminIE

Clave de registro que contiene todas las entradas de Panda Endpoint Agent empleadas por los instaladores. Dichas entradas aparecen reflejadas en la siguiente captura:



El agente, durante su ejecución, creará la clave "AgentSystem" debajo de "ClientSystem". Dentro de esa clave se crearán diversas entradas. El instalador no se tiene que preocupar de nada salvo de borrar la clave "AgentSystem" y sus entradas en la desinstalación.

27.4.3 Distribución de ficheros

Todo equipo administrado lleva instalado el agente de administración. Junto con el agente se instalan también los procesos locales.

A continuación se presentan todas las rutas y ficheros del agente de administración y los procesos locales:

Agente de administración

El Agente se instala en <AdminIEClientPath>\WasAgent

- WasAgent.conf
- WasAgent.dll
- WaPIRes.exe
- WAInterface.dll
- Wa_AGPRX.dat
- LPTokens.dat
- INTEGRA.dat
- INTEGRA.bak (se genera durante la instalación, no se distribuye)
- INTEGRA.start (se genera durante la instalación, no se distribuye)
- AgentSystem.DAT
- Proxy.dat (se genera durante la instalación, no se distribuye)

Durante la ejecución del agente se crea dentro de esta carpeta la subcarpeta "Data", con los siguientes ficheros:

- MsiExec.log
- WasAgent.log
- WaHost.log
- WapWinst.log
- Counters.ini

Así mismo se creará la clave de registro "AgentSystem" debajo de "ClientSystem". Dentro de esa clave se crearán las entradas:

- Value1
- Value2
- Value3

Si la conexión a Internet se debe realizar a través de proxy, al solicitar al usuario los datos para realizar la conexión éstos se almacenarán en el fichero AgentSystem.dat dentro de la carpeta <AdminIEClientPath>\WasAgent.

Todo debe ser borrado en la desinstalación.

Proceso local WalConf

Se instala en < AdminIEClientPath >\WalConf

- WalConf.ini

- WalConf.dll

Durante la ejecución de este proceso local se creará el siguiente fichero:

Walconf.log

Proceso local WalLnChr

Se instalan en < AdminIEClientPath >\WalLnChr:

- Wallnchr.dat

- Wallnchr.dll

Durante la ejecución de este proceso local se crearán el siguiente fichero:

WalLnchr.log

Proceso local WalNtf

Se instala en < AdminIEClientPath >\WalNtf

- WalNtf.dat

- WalNtf.dll

- WalNtf.ini

Durante la ejecución de este proceso local se crearán el siguiente fichero:

WalNtf.log

27.4.3.1

Proceso local WalQtine

Se instala en < AdminIEClientPath >\WalQtine

- WalQtine.ini

- WalQtine.dll

Durante la ejecución de este proceso local se creará el siguiente fichero:

WalQtine.log

Proceso local WalReport

Se instala en < AdminIEClientPath >\WalReport

- WalReport.dll

- WalReport.ini

Durante la ejecución de este proceso local se creará el siguiente fichero:

- WalReport.log

Proceso local WalScan

Se instala en < AdminIEClientPath >\WalScan

- WalScan.dll

- WalScan.ini

Durante la ejecución de este proceso local se creará el siguiente fichero:

WalScan.log

Proceso local WalTest

Se instala en < AdminIEClientPath >\WalTest

- WalTest.dll

- WalTest.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- WalTest.dat

- WalTest.log

- Waltestlt.dat

- Waltestdf.dat

Proceso local WalUpd

Se instala en < AdminIEClientPath >\WalUpd

- WalUpd.dll

- WalUpd.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- Counters.ini

- WalUpd.log

También se generará el subdirectorio Data, que contendrá el subdirectorio Catalog que podrá llegar a disponer de los siguientes ficheros:

- WEB_GUID

- WEB_CATALOG

- LAST_GUID

- LAST_CATALOG

- LOCAL_CATALOG

- RUMOR_TABLE

- LOCAL_CATALOG.TMP

y el subdirectorio Files que contendrá de manera temporal los ficheros necesarios para realizar actualizaciones necesarias.

Proceso local WalUpg

Se instala en < AdminIEClientPath >\WalUpg

- WalUpg.dll

- WalUpg.ini

- PavGenUn.exe

- Settings.ini

- UpgradeDialog.exe

- WALPCSMInst.dll

- WAPILnchr.exe

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- Counters.ini

- WalUpg.dat

- WalUpg.log

- WAUPGTD.dat

- WAC_Installer.log

- Agent_Installer.log

- WAC_Installer_YYYY-MM-DD_HH.mm.SS.log

- Agent_Installer_YYYY-MM-DD_HH.mm.SS.log

- WAActions.DAT

- WAActM.DAT

- WAAdmR.dat

- WAAdmR.ini

- WAAFREP.DAT

Dentro se puede generar la carpeta WAActM donde se guardan ficheros descargados por el proceso local para ejecutar algunas acciones.

También se generará el subdirectorio Data que contendrá el subdirectorio Catalog que podrá llegar disponer de los siguientes ficheros:

- WEB_GUID

- WEB_CATALOG

- LAST_GUID

- LAST_CATALOG

- LOCAL_CATALOG

- RUMOR_TABLE

- LOCAL_CATALOG.TMP

- INSTALLED_PRODUCTS.TMP

y el subdirectorio Files que contendrá de manera temporal los instaladores necesarios para realizar las instalaciones/actualizaciones de los productos.

La subcarpeta AFRep incluirá un repositorio de ficheros descargados para hacer acciones relacionadas con la protección.

Proceso local WalSNet

Se instala en < AdminIEClientPath >\WalSNet

- WalSNet.dll

- WalSNet.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- WALSNet.log

- WALSNET.dat

Plugin WalTask

Se instala en < AdminIEClientPath >\WalTask

- WalTask.dll

- WalTask.ini

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- WalTask.log

- SCAN_TASKS.DAT

Plugin WalSysCf

Se instala en < AdminIEClientPath >\WalSysCf

- WalSysCf.dll

- WalSysCf.dat

Durante la ejecución de este proceso local se crearán el siguiente fichero:

- WalSysCf.log

Plugin WalSysUd

Se instala en < AdminIEClientPath >\WalSysUd

- WalSysUd\WalSysUd.dll

Gestor de procesos locales

Se instala en < AdminIEClientPath >\WasLpMng

- WapLpMng.exe

- WasLpMng.dll

- Config\Plugins.tok (en el subdirectorio config)

- WapLpmng.ini

- WasLpmng.ini

Durante el proceso de instalación se crearán los ficheros

- WapLpmng.log

- WasLpmng.log

Planificador de tareas

Se instala en < AdminIEClientPath >\Scheduler

- PavAt.exe

- PavSched.dll

- PavAt3Api.dll

- Config\tokens.tok (en el subdirectorio config)

Durante la ejecución de este proceso local se crearán los siguientes ficheros:

- Pavsched.cfg (generado durante el proceso de instalación)

- Tasklist.lst (se genera durante la instalación, no se distribuye)

Servicio principal

Se instala en < AdminIEClientPath >\WAHost

- WAHost.exe

- WAHostClt.dll

Librerías comunes

Se instala en < AdminIEClientPath >\Common

APIcr.dll

AVDETECT.INI

DATA

libxml2.dll

MiniCrypto.dll

msvcr100.dll

PavInfo.ini

pavsddl.dll

Platforms.ini

PSLogSys.dll

pssdet.dll

psspa.dll

putczip.dll

puturar.dll

putuzip.dll

WalAgApi.dll

WalCount.dll

WALExchInf.dll

WALLMIInf.dll

WALMNAPI.dll

WALOSInf.dll

WALRVNCInf.dll

WALTVNCInf.dll

WALTVWRInf.dll

WALUtils.dll

WalUtils.ini

WALUVNCInf.dll

WaPrxRepos.dll

WaPrxRepos.Ini

WCheckReq.dll

Durante su ejecución se creará la subcarpeta "Data" dentro de ésta, que contendrá las políticas propias de la protección para que estén disponibles cuando esta se instale.

Así mismo se crearán los siguientes ficheros:

- PavInfo

- WALExchInf.log

- WalUtils.log

- WALMNAPI.log

- WALLMIInf.log

- WALRVNCInf.log

- WALTVNCInf.log

- WALUtils.log

- WALTVWRInf.log

- WALUVNCInf.log

Servicios

Panda Endpoint Agent crea el servicio siguiente:

- WAHost.exe

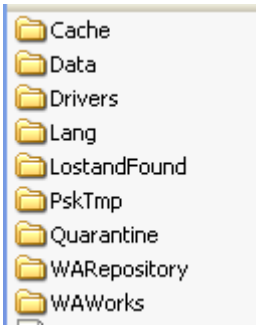
Los servicios se instalan llamando al ejecutable con la opción "-RegServer" y se desinstalan con la opción "-UnregServer"

27.5 Despliegue de Endpoint Protection

Estructura de directorios de EndPoint Protection

El usuario puede elegir la ruta donde desea instalar el producto. Por defecto, la ruta de instalación es la siguiente:

%allusersprofile%\Datos de programa\Panda Security\Panda Endpoint Protection\Quarantine



InstallPath: Ruta de instalación de EndPoint Protection. Contiene los ficheros necesarios para el funcionamiento de EndPoint Protection.

Cache: Contiene los ficheros de firmas locales.

Data: Contiene los ficheros de datos de la tecnología de análisis por comportamiento.

Drivers: Contiene binarios que se usan en la instalación / desinstalación de las unidades.

NNSNahs: Binarios para la instalación del driver intermediate del Firewall.

PSINDvct: Binarios para la instalación del driver de la tecnología Device Control.

Lang: Contiene los diccionarios con los diferentes idiomas.

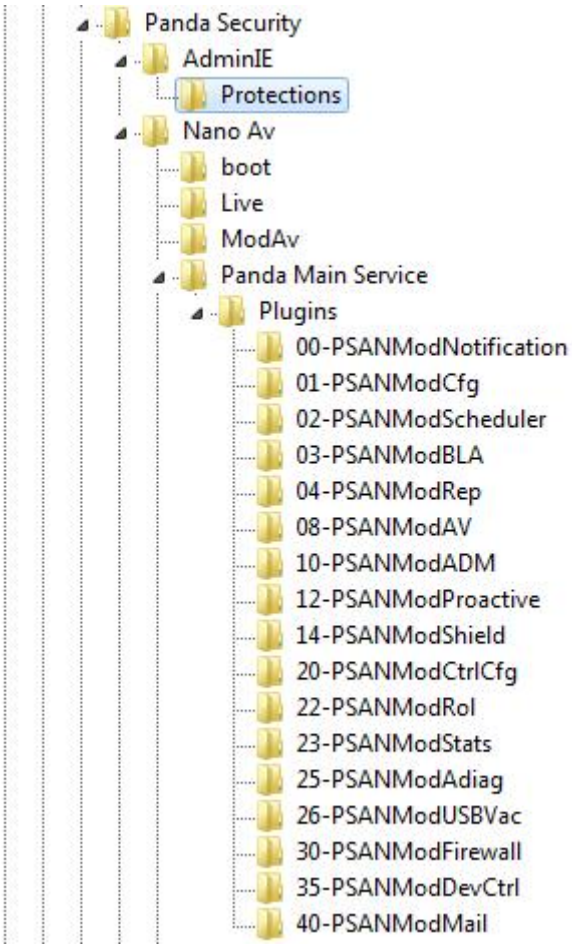
LostandFound: Contiene los elementos restaurados de la cuarentena, cuando han sido movidos por las protecciones de correo, o cuando no se han podido restaurar en su ruta original.

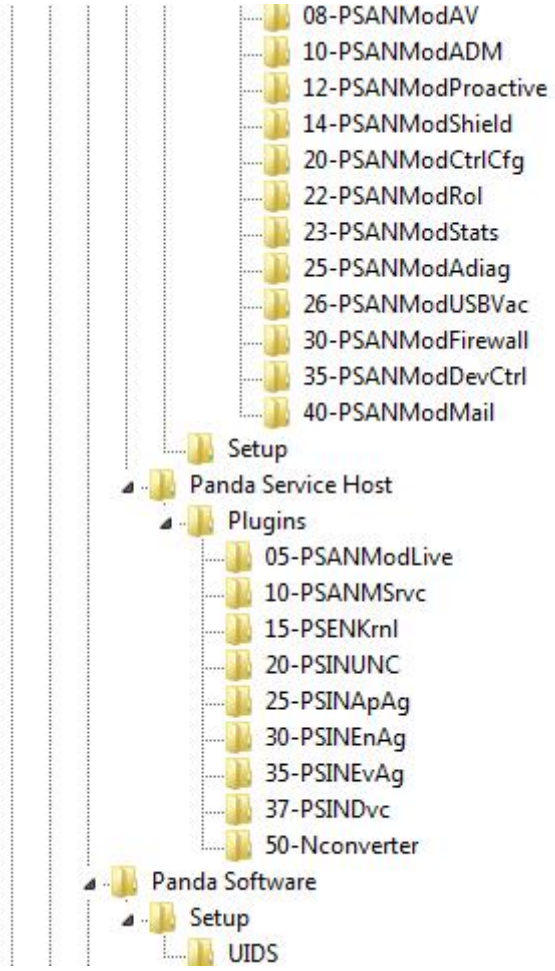
Quarantine: Los elementos que se han movido a cuarentena.

PskTmp: Ficheros temporales de configuración creados durante los análisis.

Entradas de registro

Entradas del registro en Panda Software





Panda Security: Clave en HKEY_LOCAL_MACHINE\Software\Panda Security bajo la que se encuentran las claves y valores de la protección.

AdminIE\Protections: Clave donde se encuentra el valor WAC que indica donde está instalado el cliente.

Nano Av\Boot: Mantenido por compatibilidad con versiones anteriores. Actualmente no se utiliza.

Nano AV\ModAV: Mantenido por compatibilidad con versiones anteriores. Actualmente no se utiliza.

Nano Av\Live: Clave donde se encuentra el valor DownloadFolder en el que se indica la carpeta de descargas del cliente

Nano Av\Panda Main Service: Clave donde se guardan los valores de carga de plugins del módulo principal del antivirus.

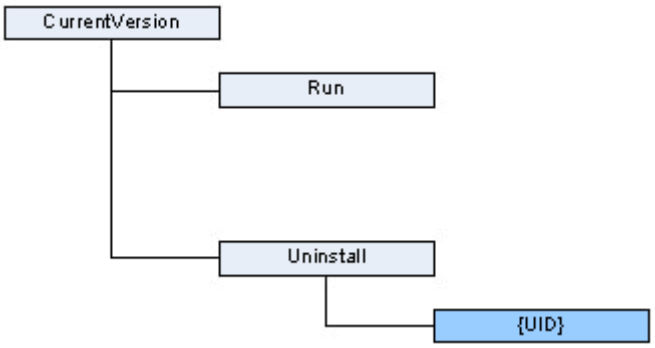
Nano Av\Setup: Contiene el Path de instalación de la protección

Panda Service Host: Contiene los plugins que se cargan en el servicio: sistema de actualización, el sistema principal del antivirus, el motor, el sistema de interceptación de ficheros y procesos, sistema de configuración del device control, firewall.

Panda Software\Setup: (nombre, versión, ID, ruta de instalación, etc).

Entradas del registro en Windows\CurrentVersion

En este apartado se podrán ver las entradas de registro que EndPoint Protection crea dentro de la clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion



CurrentVersion: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

Run: Clave del sistema donde está la ruta a aquellas aplicaciones lanzadas al inicio.

Unistall: Clave del sistema donde se almacena información relativa a los desinstaladotes de los productos instalados en el sistema.

Panda Universal Agent Endpoint: Clave con información necesaria para la desinstalación del producto.

Entradas del registro en Services

Services: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

NNSALPC: Driver del firewall.

NNSHTTP: Driver del firewall.

NNSIDS: Driver del firewall.

NNSNAHS: Driver del firewall.

NNSPICC: Driver del firewall.

NNSPIHS: Driver del firewall.

NNSPOP3: Driver del firewall.

NNSPROT: Driver del firewall.

NNSPRV: Driver del firewall.

NNSSMTP: Driver del firewall.

NNSSTRM: Driver del firewall.

NNSTLSC: Driver del firewall.

NNSHTTPS: Driver del firewall.

PRKPAVPROC: Driver usado para análisis de Rootkits.

PSBOOT.SYS: Driver que se encarga de operaciones a reinicio.

PSINAflt: Filtro de interceptación.

PSINDvct: Driver de Device Control.

DVCTPROV.sys: Driver de Device Control

PSINFile: Driver de interceptación de ficheros.

PSINKNC: Driver de interceptación de kernel.

PSINProc: Driver de interceptación de procesos.

PSINProt: Driver protector (escudo, KRE).

PSKMAD: Driver de análisis de memoria.

Servicios

PSUAService: Servicio de control y gestión de tareas en las diferentes sesiones.

NanoServiceMain: Servicio principal del cliente para todas las protecciones.

CLOUDUPDATEREX: Servicio encargado de tareas de Upgrade.

Procesos

Aparte de los servicios mostrados en el punto anterior, los siguientes procesos pueden estar ejecutados en la máquina:

bspatch.exe

Proceso usado en el parcheo de los ficheros de firmas.

PAV2WSC.exe

Proceso usado para la actualización del estado del antivirus en el Windows Security Center.

PSANCU.exe

Proceso usado para realizar tareas de configuración durante la instalación y durante los upgrades del cliente.

PSINanoRun.exe

Proceso usado durante la instalación y upgrades del cliente.

PSNCSysAction.exe

Proceso que realiza las tareas de activación / desactivación del driver intermediate NNSNahs del firewall.

PSUAMain.exe

Proceso correspondiente a la traybar.

PSUNMain.exe

Proceso correspondiente interfaz del cliente.

Setup.exe

Proceso correspondiente a tareas de instalación y upgrades.

WAScanner.exe

Proceso que gestiona las tareas de análisis de background configuradas desde la consola Web.

28. Apéndice 3

Descubrimiento automático de equipos (Windows)

28.1 Introducción

Endpoint Protection dispone de un sistema de descubrimiento de equipos que permite que el administrador pueda tener una visión general de cuáles son los equipos de su red que no se encuentran protegidos.

Este sistema se basa en la configuración y ejecución de tareas de búsqueda, que se llevan a cabo desde un "equipo descubridor" que ha de reunir una serie de requisitos para poder actuar como tal.

Datos a tener en cuenta a la hora de crear una tarea de búsqueda

1. Se realizará una única ejecución por tarea de búsqueda.

2. La ejecución de la tarea de búsqueda comenzará una vez que el equipo descubridor se descargue la orden de descubrimiento desde el servidor de Endpoint Protection. Existirá, por tanto, un margen de tiempo entre la creación de la tarea y la ejecución de la misma.

3. Se podrá forzar el comienzo inmediato de la tarea si se realiza una actualización a través de la opción **Actualizar** del menú contextual de la protección en el equipo descubridor.

4. En caso contrario podrán pasar hasta un máximo de 4 horas antes de que comience a ejecutarse la tarea.

5. Es posible definir varias tareas de búsqueda para un mismo equipo descubridor. En esta caso las tareas se irán ejecutando de forma secuencial, en el orden en que se han definido.

6. Si se produce un reinicio de la máquina durante la ejecución de una tarea de descubrimiento, la tarea se ejecutará de nuevo a los 5 minutos del arranque. Previamente se validará contra el servidor que la tarea de descubrimiento sigue vigente.

Al configurar la tarea de búsqueda, es necesario proporcionar la siguiente información:

- Nombre de la tarea (de 50 caracteres como máximo)

- No se permitirá crear tareas con el mismo nombre dentro del mismo cliente.

- No se permitirá la introducción de los siguientes caracteres en el nombre de las tareas <, >, ", ', &

- Equipo desde donde se lanzará la tarea de descubrimiento de equipos ('equipo descubridor"), seleccionándolo de la lista de equipos protegidos.

Se podrá limitar el alcance del barrido de la red, eligiendo una de las siguientes opciones:

- La **subred del equipo** que realiza el descubrimiento (opción seleccionada por defecto).

- Uno o varios **rangos de direcciones IP (IPv4)** introducidos por el usuario. Si se introducen rangos con direcciones IP en común se realizará el descubrimiento una única vez.

- Uno o varios **dominios** introducidos por el usuario.

28.1.1 Requisitos que debe reunir el equipo descubridor

- Tener instalado el agente y la protección, y estar integrado correctamente en el servidor de Admin IE.

- Tener una versión de agente 5.05 o superior.

- No deberá estar en lista negra.

- Deberá haberse conectado durante las últimas 72 horas con el servidor de AdminIE.

- No deberá estar realizando una tarea de desinstalación, el equipo no podrá estar en ninguno de los siguientes estados en una tarea de desinstalación:

  - En espera

  - Iniciando

  - Desinstalando

- Debe disponer de conexión a Internet, ya sea directamente o a través de otros equipos (funcionalidad 'proxy')

A medida que se van sucediendo las acciones de la tarea de búsqueda, Endpoint Protection mostrará el estado en el que se encuentra la tarea.

Secuencia de acciones de la tarea de búsqueda y correspondencia con el estado de la tarea

El usuario ordenará desde la consola Web la ejecución de una tarea de descubrimiento de equipos, a partir de un equipo que ya cuenta con la protección instalada (equipo descubridor).

28.1.2

28.1.3 Estado de la tarea

Estado de la tarea: En espera

El equipo descubridor se descargará la orden de descubrimiento del servidor. El servidor tendrá constancia de esta acción y modificará el estado de la tarea.

Estado de la tarea: Iniciando

El equipo descubridor recalculará la prioridad de la nueva tarea, junto con las tareas que ya estuviesen a la espera de ser ejecutadas. Esperará a que le llegue el turno, según la lógica de prioridades.

Estado de la tarea: Iniciando

El equipo descubridor comprobará que cumple con los requisitos para poder ejecutar la tarea.

Estado de la tarea: Iniciando

Se enviará un mensaje al servidor indicando el comienzo de la ejecución de la tarea.

Estado de la tarea: En curso

El equipo descubridor realizará el barrido de la red, en busca de equipos.

Estado de la tarea: En curso

28.1.4 Secuencia de la tarea de búsqueda

Obtener la lista de equipos:

Por IP (Rangos de IP y Subred)

- Se hace un ping a cada IP mediante el protocolo ICMP.
- Se espera la respuesta a los ping.
- Se intenta resolver el nombre de las IP que responden.

Por dominio

- Se enumeran los equipos pertenecientes al dominio.
- Determinar si los equipos que tenemos en la lista tienen el agente instalado.
- Se envía un mensaje al agente.
- Se espera respuesta.
- Generar lista de equipos y enviar los resultados al servidor.

28.1.5 Resultados de la tarea de búsqueda

El equipo descubridor enviará siempre al servidor el listado completo de equipos no protegidos descubiertos, aunque no haya sufrido modificación con respecto al listado enviado anteriormente por el mismo equipo.

El listado de equipos descubiertos contendrá:

- Equipos sin agente instalado.
- Equipos integrados en otro cliente.

No hay forma de comunicar con agentes de otros clientes, por lo tanto, no se recibirá respuesta y se asumirá que el equipo no está protegido.

Equipos con agente inferior a 5.05.

El agente de estos equipos no está preparado para responder a los mensajes de descubrimiento y, por lo tanto, se considerarán como equipos no protegidos.

Equipos que tienen agente 5.05 ó superior pero que no hayan respondido al mensaje de descubrimiento durante el tiempo establecido.

El tiempo de espera de la respuesta será= 3 seg (Factor de espera)* Número de equipos que han respondido a petición del protocolo ICMP (ping) +30 seg (margen de seguridad).

Los equipos en lista negra (siempre y cuando tengan agente 5.05 o superior y estén integrados en clientes) no se considerarán equipos no protegidos descubiertos, y por lo tanto NO se incluirán en el listado de equipos descubiertos.

28.1.6 Detalle de los equipos no protegidos

De cada equipo descubierto, se obtendrá:

- Dirección IP, siempre.
- Nombre de equipo, si el equipo descubridor fue capaz de resolverlo.

Casos en los que el servidor puede NO tener constancia de la finalización de una tarea de descubrimiento

28.2 Caso 1

La tarea se encuentra en situación de "En espera", "Iniciando" o "En curso", y el equipo distribuidor se desinstala, elimina de la base de datos o es enviado a lista negra durante la ejecución de la tarea.

28.2.1 Consecuencias

El equipo descubridor no podrá informar al servidor sobre el resultado de dicha tarea.

En cuanto el servidor tenga constancia de que el equipo descubridor ha sido eliminado, desinstalado* o enviado a lista negra, la tarea de descubrimiento pasará a estado "Finalizado con error".

Se considerará que el equipo descubridor ha sido desinstalado en cuanto envíe el mensaje de fin de desinstalación, es decir, en cuanto termine de desinstalar la protección.

Además, si el equipo descubridor ha sido eliminado:

1. Se eliminará su nombre de la pantalla de configuración de la tarea de descubrimiento, y se mostrará un error que indique que el equipo ha sido eliminado.
2. Al eliminar el equipo, también se eliminará la información del grupo al que pertenecía dicho equipo. Por lo tanto, los usuarios monitorizadores o administradores

con permiso sobre dicha tarea (con permiso sobre el grupo del equipo descubridor), dejarán de visualizarla.

28.3 Caso 2

La tarea se encuentra en estado "En espera", "Iniciando" o "En curso", y el equipo descubridor es enviado a lista negra y posteriormente restaurado.

28.3.1 Consecuencias

1. El equipo continuará con la tarea que tenía pendiente, y por lo tanto, el estado de la tarea podrá cambiar, podrá pasar de 'Finalizado con Error' a 'Finalizada', siendo éste el único cambio de estado posible.

2. Si el equipo descubridor tiene algún problema de comunicación durante la ejecución de la tarea, no podrá informar al servidor sobre el estado y los resultados de dicha tarea.

3. La tarea no actualizará su estado, y se mantendrá en el estado en el que estaba ("En espera" "Iniciando" o "En Curso") hasta que sea eliminada.

4. Si se produce algún error durante la ejecución de la tarea, (tarea en estado "En espera", "Iniciando" o "En curso"): la tarea se mantendrá en el estado en el que estaba ("En espera" "Iniciando" o "En Curso") hasta que sea eliminada.

Ante la interrupción de la tarea, el comportamiento será el siguiente:

Si una vez iniciado el descubrimiento de equipos y, antes de que finalice, se apagase el equipo descubridor por cualquier motivo (a voluntad del usuario o fortuitamente), al volver a arrancar el equipo, el agente:

1. Chequeará contra el servidor la vigencia de la tarea.

2. En caso de seguir vigente, relanzará de nuevo el descubrimiento desde el principio.

3. En caso de no seguir vigente, por haberse superado el tiempo máximo de existencia de una tarea, abortará el descubrimiento.

4. Esperará 5 minutos a partir del reinicio del equipo para relanzar la tarea de descubrimiento.

29. Apéndice 4

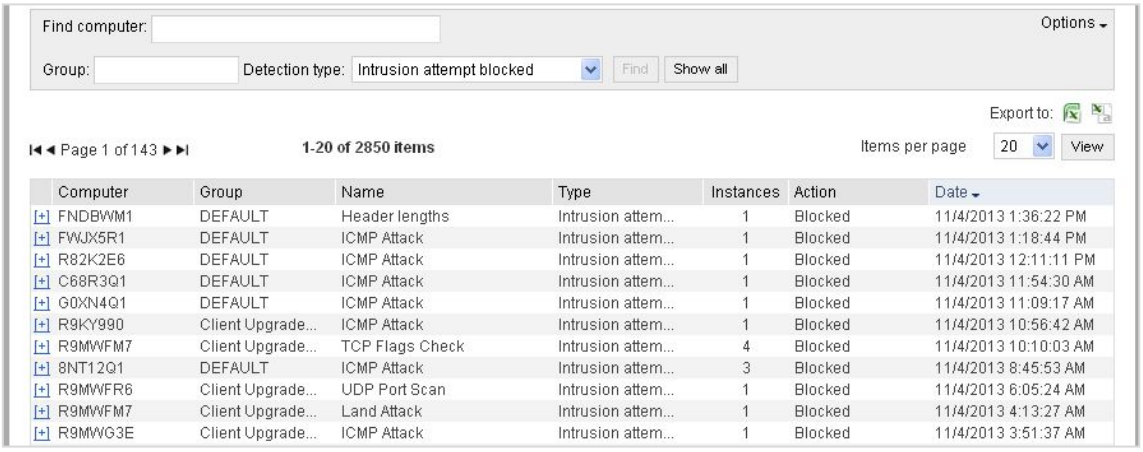
Detección del origen de los ataques

Categorías de ataques IDS

29.1 Detección del origen de los ataques

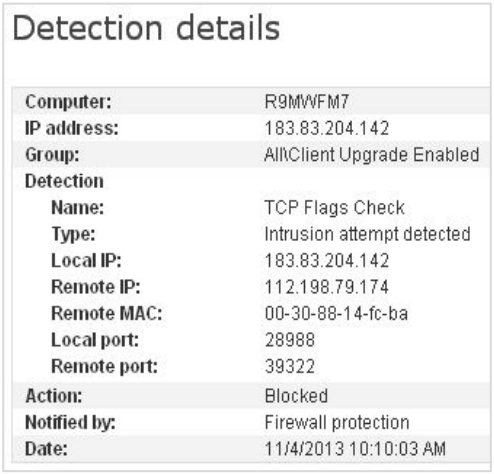
Desde la consola Web de Endpoint Protection es posible obtener información sobre el origen de los ataques IDS bloqueados (excepto en los casos de Drop Unsolicited Responses, SMURF, SYN Flood y UDP Flood).

Para ello, puedes utilizar la opción de filtrado que está disponible en la ventana **Listado de detecciones** y filtrar utilizando el criterio **Tipo de detección**.



Computer	Group	Name	Type	Instances	Action	Date
[+] FNDBWM1	DEFAULT	Header lengths	Intrusion attem...	1	Blocked	11/4/2013 1:36:22 PM
[+] FWJX5R1	DEFAULT	ICMP Attack	Intrusion attem...	1	Blocked	11/4/2013 1:18:44 PM
[+] R82K2E6	DEFAULT	ICMP Attack	Intrusion attem...	1	Blocked	11/4/2013 12:11:11 PM
[+] C68R3Q1	DEFAULT	ICMP Attack	Intrusion attem...	1	Blocked	11/4/2013 11:54:30 AM
[+] G0XN4Q1	DEFAULT	ICMP Attack	Intrusion attem...	1	Blocked	11/4/2013 11:09:17 AM
[+] R9KY990	Client Upgrade...	ICMP Attack	Intrusion attem...	1	Blocked	11/4/2013 10:56:42 AM
[+] R9MWFM7	Client Upgrade...	TCP Flags Check	Intrusion attem...	4	Blocked	11/4/2013 10:10:03 AM
[+] 8NT12Q1	DEFAULT	ICMP Attack	Intrusion attem...	3	Blocked	11/4/2013 8:45:53 AM
[+] R9MWFR6	Client Upgrade...	UDP Port Scan	Intrusion attem...	1	Blocked	11/4/2013 6:05:24 AM
[+] R9MWFM7	Client Upgrade...	Land Attack	Intrusion attem...	1	Blocked	11/4/2013 4:13:27 AM
[+] R9MWG3E	Client Upgrade...	ICMP Attack	Intrusion attem...	1	Blocked	11/4/2013 3:51:37 AM

Además, al hacer clic en el signo (+) que aparece en el listado junto al nombre del equipo, se mostrará la ventana **Detalles de detección**, donde aparecen, entre otros, los siguientes datos:



Detection details

Computer:	R9MWFM7
IP address:	183.83.204.142
Group:	All\Client Upgrade Enabled
Detection	
Name:	TCP Flags Check
Type:	Intrusion attempt detected
Local IP:	183.83.204.142
Remote IP:	112.198.79.174
Remote MAC:	00-30-88-14-fc-ba
Local port:	28988
Remote port:	39322
Action:	Blocked
Notified by:	Firewall protection
Date:	11/4/2013 10:10:03 AM

Consulta el apartado Detalle de detecciones.

Si deseas más información sobre las categorías de los ataques IDS y las defensas que Endpoint Protection despliega contra ellos, visita los apartados Categorías de ataques IDS y Descripción de las defensas IDS.

29.2 Categorías de ataques IDS

29.2.1 Ataques DoS (Deny of Service)

Son ataques orientados a colapsar un dispositivo o servicio. Normalmente se basan en saturación de paquetes, bien por fuerza bruta o aprovechando vulnerabilidades conocidas de cierta aplicación, sistema operativo o dispositivo.

Algunos de estos ataques son:

- LAND attack
- SYN flood
- UDP flood
- ICMP attack
- Fragmentation control

29.2.2 Defensa de protocolo o aplicación

Este tipo de defensa está orientada a la protección de ciertos protocolos ante vulnerabilidades conocidas, se basan en el conocimiento del protocolo y su contexto para descartar peticiones no solicitadas.

Algunos de ellos son:

- Smart WINS
- Smart DNS
- Smart DHCP
- Smart ARP
- Header lengths
- ICMP attack
- Fragmentation control

29.2.3 Rastreo y descubrimiento

Esta protección trata de evitar o burlar comportamientos conocidos para el rastreo de dispositivos o el descubrimiento de vulnerabilidades.

Algunos de ellos son:

- TCP flags check
- TCP port scan
- UDP port scan
- ICMP filter echo request

- OS detection
- IP explicit path
- Fragmentation control

29.2.4 Descripción de las defensas IDS

IP explicit path

Se rechazan los paquetes IP que tengan la opción de "explicit route".

Land Attack

Comprueba intentos de denegación de servicios por loop de pila al detectar paquetes con direcciones remitente y destino iguales.

SYN flood

Controlando el estado de cada conexión y los tiempos de respuestas de las mismas detectamos la cantidad de conexiones entrantes que no se resuelven nunca, generando un aumento del control de estados hasta superar determinado límite, por lo que constituye un SynFlood. En este caso se deniegan nuevas conexiones. Si bien es posible que deneguemos nuevas conexiones legítimas, al menos se protege la integridad de las ya establecidas y de las conexiones salientes.

UDP Flood

Se rechazan los paquetes UDP que llegan a un determinado puerto si exceden en cantidad a un número determinado en un periodo determinado.

TCP Port Scan

Detector de port scanning para puertos TCP, es decir, detecta si un host intenta conectarse a varios puertos en un tiempo determinado. Detiene el ataque denegando las respuestas al host sospechoso. Adicionalmente filtra las respuestas para que el remitente ni siquiera obtenga respuesta de puerto cerrado.

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 como "SYN & FIN" y "NULL FLAGS" y a la de "OS identification" ya que muchas de estas pruebas se basan en respuestas a paquetes TCP inválidos.

Header lengths

- **IP:** Se rechazan los paquetes entrantes con un tamaño de cabecera IP que se salga de los límites establecidos.
- **TCP:** Se rechazan los paquetes entrantes con un tamaño de cabecera TCP que se salga de los límites establecidos.
- **Fragmentation control:** Realiza comprobaciones sobre el estado de los fragmentos de un paquete a reensamblar, protegiendo de ataques de agotamiento de memoria por ausencia de fragmentos, redireccionado de ICMP disfrazado de UDP y scanning de máquina disponible.

UDP Port Scan

Protección contra escaneo de puertos UDP.

Smart WINS

Se rechazan las respuestas WINS que no se corresponden con peticiones que nosotros hemos enviado.

Smart DNS

Se rechazan las respuestas DNS que no se corresponden con peticiones que nosotros hemos enviado.

Smart DHCP

Se rechazan las respuestas DHCP que no se corresponden con peticiones que nosotros hemos enviado.

Smart ARP

Se rechazan las respuestas ARP que no se corresponden con peticiones que nosotros hemos enviado.

ICMP Attack

Este filtro implementa varias comprobaciones:

- **SmallPMTU**: Mediante la inspección de los paquetes ICMP se detectan valores inválidos en PMTU utilizados para generar una denegación de servicio o ralentizar el tráfico saliente.
- **SMURF:** Se rechazan las respuestas ICMP no solicitadas si estás superan una determinada cantidad en un segundo.
- **Drop unsolicited ICMP replies**: Se rechazan todas las respuestas ICMP no solicitadas o que hayan sido caducadas por el timeout establecido.

ICMP Filter echo request

Se rechazan los "pings" entrantes.

OS Detection

Falsea datos en respuestas al remitente para engañar a los detectores de sistemas operativos. Esta defensa se complementa con la de "**TCP Flags Check**".

30. Apéndice 5

Detalles del despliegue, procesos, análisis y detecciones de la protección para Linux

30.1 Requisitos de instalación

Consulta el apartado Requisitos de instalación en sistemas Linux (capítulo 1)

30.2 Instalación

Para instalar la protección de forma que se integre correctamente en el servidor de Endpoint Protection es necesario descargar el instalador desde la consola, tal y como se ha comentado en el apartado Modos de instalación.

El nombre del instalador descargado es "LinuxWAAgent.run".

Después de descargar el instalador es necesario darle permiso de ejecución. Se puede hacer desde el explorador de archivos o ejecutando el comando ***# chmod +x LinuxWAAgent.run***

A continuación se puede ejecutar el instalador. Para que funcione correctamente la instalación se debe hacer como root. Para hacerla se puede hacer doble click sobre el instalador desde el explorador de ficheros o se puede ejecutar desde un terminal el siguiente comando:

 # ./LinuxWAAgent.run

El instalador descomprime los ficheros y a continuación ejecuta un shell script, post_install.sh, que se encarga de las tareas de post instalación, tales como: escribir ficheros de configuración, lanzar procesos etc.

Cuando termina la instalación deben estar en ejecución los siguientes procesos:

- PCOP_AgentService
- PCOPScheduler

Se puede comprobar el estado de los procesos ejecutando el comando: ***# ps aux | grep PCOP***

Despliegue

Cuando el producto se instala se crean en disco las siguientes carpetas y ficheros:

- Carpeta del agente "/opt/PCOPAgent"
- Carpeta de configuración "/etc/PCOPLinux"
- Fichero "pcopagent" en la carpeta /etc/init.d

Procesos

Como se ha comentado anteriormente, cuando la protección de Endpoint Protection está instalada en el equipo, normalmente habrá en ejecución dos procesos:

- PCOP_AgentService
- PCOPScheduler

Estos procesos se ejecutan como daemon y se lanzan automáticamente cuando se inicia el sistema operativo.

Se ha comprobado que al enviar el mensaje de integración si la integración falla, ya sea porque el mensaje no se puede enviar o porque el servidor devuelve un error de integración, el proceso PCOP_AgentService se detiene y no se hacen nuevos reintentos de integración hasta que el proceso se inicie de nuevo.

Para detener de forma manual los procesos se puede ejecutar el comando:

 # /opt/PCOPAgent/Stop-PCOP-Agent

Para iniciar de nuevo los procesos se debe ejecutar el comando: ***# /etc/init.d/pcopagent start***

Para su funcionamiento el producto deberá tener acceso a los siguientes dominios de Internet, tanto para comunicaciones HTTP como HTTPS:

- mp-agents-inst.pandasecurity.com
- mp-agents-sync.pandasecurity.com
- mp-agents-async.pandasecurity.com

Estos dominios podrían cambiar en futuras versiones del producto.

Es importante que tengas presente los requisitos que los diferentes equipos deben reunir y las URLs a las que es necesario que tengan acceso. Consulta el apartado Requisitos de instalación (capítulo 1)

30.3 Comunicación a través de proxy

Si la salida a Internet es a través de proxy, es necesario configurar el producto para que utilice el proxy adecuado. Para ello, se puede editar directamente el fichero proxy.conf indicando los datos del proxy en formato ***proxy:port:user:password***

Hay dos instancias de este fichero:

- /opt/PCOPAgent/proxy.conf

  Contiene la configuración utilizada por el agente para enviar los mensajes al servidor de Endpoint Protection.

- /opt/PCOPAgent/Common/Binaries/PcopSigUpdater-bin/proxy.conf

  Contiene la configuración utilizada por el proceso encargado de la actualización de ficheros de firmas.

También es posible establecer la configuración de forma más visual, ejecutando el script proxyConf.sh desde la carpeta /opt/PCOPAgent o desde la carpeta

/opt/PCOPAgent/Common/Binaries/PcopSigUpdater-bin, en función del fichero de configuración de proxy que se quiera modificar.

En comunicaciones a través de proxy el único tipo de autenticación que se soporta es la autenticación básica.

30.3.1 Validación de usuario

Cuando el usuario no es válido o el equipo está en lista negra, Endpoint Protection no podrá operar normalmente, es decir, no se podrán enviar mensajes al servidor ni se actualizarán los ficheros de firmas.

30.3.2 Actualización de ficheros de firmas

Para permitir la actualización de ficheros de firmas debe estar permitido el acceso a siguientes dominios:

- http://acs.pandasoftware.com
- http://cloudav.downloads.pandasecurity.com
- http://cloudav.updates.pandasecurity.com

Consulta el apartado URLs necesarias.

30.4 Análisis

En consola, al igual que el agente de Windows, se pueden configurar análisis inmediatos, programados y periódicos para cada perfil, pero en el caso de Linux no está disponible aún el análisis de correo electrónico.

30.4.1 Análisis bajo demanda

En la configuración del perfil se pueden añadir análisis inmediatos, en los cuales se puede configurar el tipo de análisis que se soportan:

- De todo el equipo
- De los discos duros
- De otros elementos

Si selecciona **Otros elementos,** podrá añadir rutas a analizar siguiendo la sintaxis de rutas de Linux.

Los análisis bajo demanda se lanzarán inmediatamente después de descargarse la configuración del mismo, que podría llegar a tardar un máximo por defecto de 4h.

30.4.2 Análisis programados

En la configuración del perfil se pueden añadir análisis programados, en los cuales se puede configurar el tipo de análisis que se soportan:

- De todo el equipo
- De los discos duros
- De otros elementos

Se pueden configurar la fecha del análisis y la hora local de lanzamiento.

Si selecciona **Otros elementos** podrá añadir rutas a analizar, siguiendo la sintaxis de rutas de Linux.

Los análisis programados se lanzarán en el día y ahora programada pero después de descargarse la configuración del mismo, que podría llegar a tardar un máximo por defecto de 4h.

30.4.3 Análisis periódicos

En la configuración del perfil se pueden añadir análisis periódicos, en los cuales se puede configurar el tipo de análisis que se soportan:

- De todo el equipo
- De los discos duros
- De otros elementos

Si selecciona **Otros elementos** podrá añadir rutas a analizar, siguiendo la sintaxis de rutas de Linux.

Se puede configurar la fecha donde se quiere que comience la ejecución de estos análisis así como la hora local de lanzamiento. Además en este tipo de análisis se puede configurar la periodicidad del mismo:

- Diario
- Semanal
- Mensual

Los análisis periódicos se lanzarán en el día y ahora programados, con la periodicidad programada, pero deberá previamente descargarse la configuración del mismo, que podría llegar a tardar un máximo por defecto de 4h.

30.4.4 Lanzamiento manual de análisis

Es posible lanzar tareas de análisis de forma manual desde el equipo. Para ello se utilizará la protección PAVSL.

Para realizar un análisis y desinfección de ficheros, los parámetros que acepta el producto son los siguientes:

Pavsl.sh –cmp –heu –rpt [log] -noglk -prx [http(s)://user:password@maquina:puerto] [samples_path]

Donde:

Parámetro *cmp*: indica si se quiere entrar a recorrer o no ficheros comprimidos o empaquetados para analizar los elementos que contiene.

Parámetro *heu*: indica si se quiere realizar el análisis con tecnología heurística o no.

Parámetro *rpt*: indica el path donde se generará un fichero de log con los resultados del análisis.

Parámetro *noglk*: indica que se desea realizar el análisis sin consultar a la nube.

Parámetro *prx*: este parámetro va a ser la cadena de conexión necesario en caso de que exista un proxy para conectarse a internet.

El formato debe ser el siguiente:

http://user:password@máquina:puerto

o

https://user:password@máquina:puerto

Parámetro *samples_path*: indica el path del fichero o directorio (y subdirectorios que contenga) que se quiere analizar. Para múltiples paths de análisis, estos deberán de estar entre comillas y separados por coma (“path","path"). En caso de paths con espacios en blanco deberán estar

"escapados" al estilo de la Shell de Linux (\) y entre comillas (") tanto si es un análisis de un path simple o múltiple.

Algunos ejemplos de uso son:

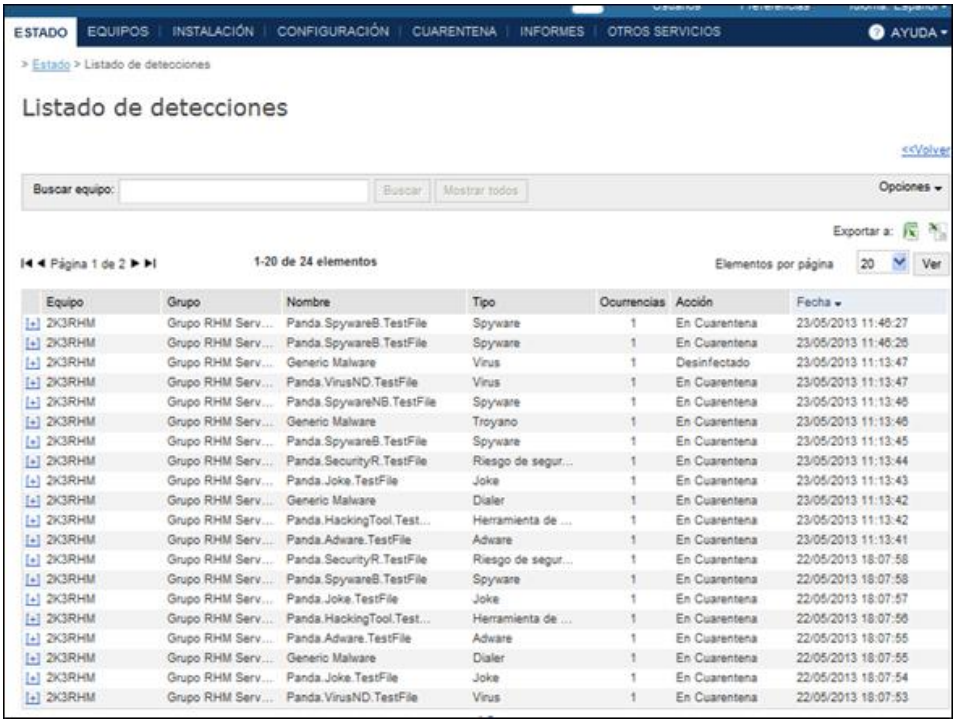
- pavsl.sh –cmp –heu –rpt /tmp/log /home/user/cebos
- pavsl.sh –cmp –heu –rpt /tmp/log "/home/user/cebos"," /home/user/cebos2"
- pavsl.sh –cmp –heu –rpt /tmp/log "/home/user/cebos\ virus"
- pavsl.sh –cmp –heu –rpt /tmp/log "/home/user/cebos\ virus","/home/user/malware"

Si se desea que las detecciones realizadas por el análisis manual se envíen al servidor es necesario que el log se genere en la carpeta /opt/PCOPAgent/Common/DATA/ScansLogs y que el nombre del fichero es de la forma SCAN_XXXX.log, siendo XXXX un número de 4 dígitos.

Por ejemplo:

pavsl.sh -cmp -heu -rpt /opt/PCOPAgent/Common/DATA/ScansLogs/SCAN_2000.log /home/user/cebos

Listado de detecciones
Mediante este proceso se recoge la información sobre las detecciones realizadas.



Por defecto, los informes de detecciones, si las hay, se envían cada 6h y se pueden ver en la consola Web, en la ventana **Estado** > **Lista de detecciones**, al igual que sucede con el sistema operativo Windows.

Actualizar a versión superior

Endpoint Protection para Linux no dispone de una funcionalidad de actualización de versión automática.

Si deseas actualizar la versión de Endpoint Protection, es necesario acceder a la consola Web para descargar la nueva versión y ejecutar el instalador de forma manual en el equipo.

No es necesario desinstalar previamente Endpoint Protection, ya que el instalador es capaz de actualizar a partir de una versión anterior.

30.5 Desinstalación

Endpoint Protection no dispone de un script de desinstalación por lo que para eliminarlo del sistema es necesario realizar de forma manual las siguientes acciones:

Parar los procesos

Para ello ejecutar el comando:

/opt/PCOPAgent/Stop-PCOP-Agent

Eliminar la carpeta /opt/PCOPAgent y su contenido.

Eliminar la carpeta /etc/PCOPLinux y su contenido.

Eliminar el servicio. La forma de hacer esta tarea depende de la distribución:

SUSE

chkconfig –del pcopagent

Debian / Ubuntu

update-rc.d -f pcopagent remove

Eliminar el fichero /etc/init.d/pcopagent.

31. Apéndice 6

Detalles del despliegue, procesos, análisis y detecciones de la protección para OS X

31.1 Requisitos de instalación

Por favor, consulta los requisitos de instalación de la protección para equipos con sistema OS X.

31.2 Instalación

Para instalar la protección de forma que se integre correctamente en el servidor de Endpoint Protection es necesario descargar el instalador desde la consola.

El nombre del instalador descargado es `MacWAAgent.dmg`. Cuando se hace doble click en este fichero en el equipo OS X, se abrirá mostrando su contenido:

MacWAAgent.pkg

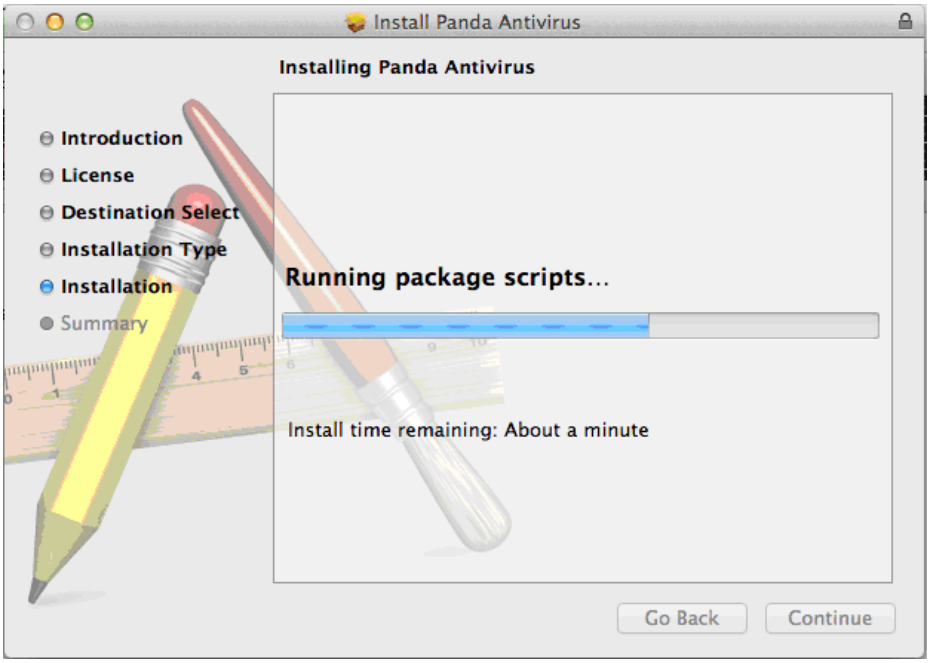
El fichero `MacWAAgent.pkg` es el instalador propiamente dicho. Para instalar el producto basta con hacer doble click sobre este fichero.

generalInformations.plist

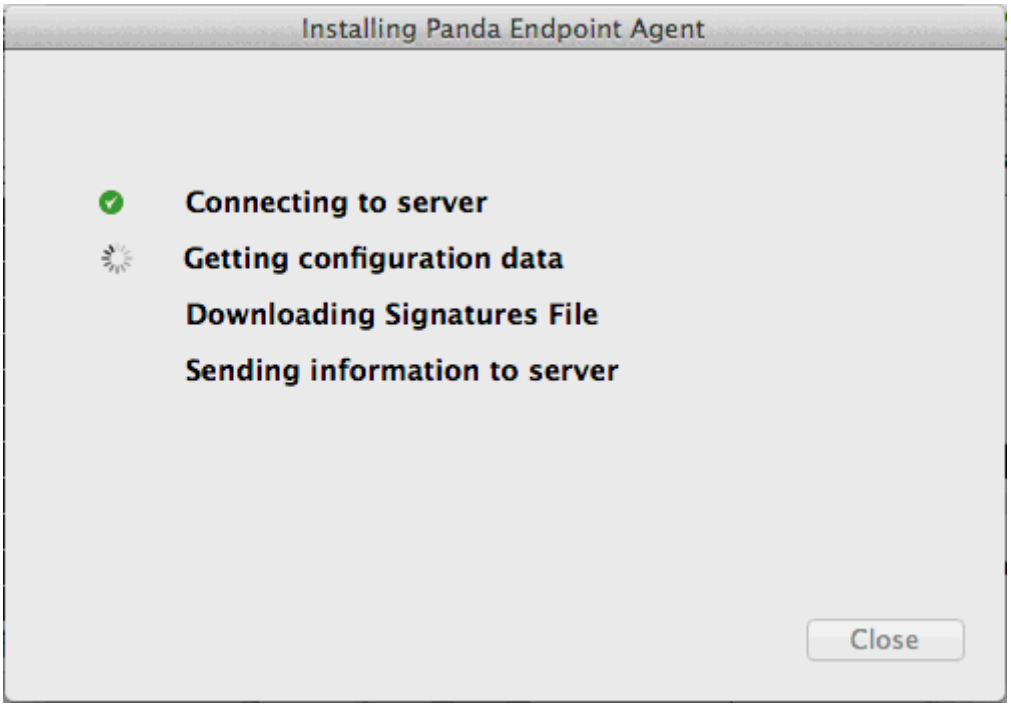
El fichero `generalInformations.plist` es un fichero de configuración que contiene la información necesaria para que el producto pueda integrarse contra el servidor de Endpoint Protection.

31.3 Proceso de instalación

Al hacer doble click sobre el fichero `MacWAAgent.pkg` aparecerá un asistente que guiará al usuario en el proceso de instalación.



Cuando el asistente esté finalizando la instalación, aparecerá una ventana con la secuencia de pasos que se debe llevar a cabo para integrar el sistema contra el servidor de Endpoint Protection.



Los pasos se irán marcando como realizados conforme se vayan completando:

- **Connecting to server** envía un mensaje de integración al servidor.
- **Getting configuration data** envía un mensaje para obtener las políticas de configuración.
- **Downloading Signature File** actualiza los ficheros de firmas.
- **Sending information to server** manda un mensaje de estado con la información actualizada.

Despliegue

Cuando el producto se instala en el sistema de archivos se crean las siguientes carpetas y ficheros:

- Applications

Se crea la aplicación **Panda Antivirus**.

- Carpeta /Library/Preferences/Intego

/Library/Preferences/Intego

```
├──────.no–intego–menu
└─┬──VirusBarrier
  ├──────Archives.plist
  ├──────Behavioral.plist
  ├──────Devices.plist
  ├──────Events.plist
  ├──────MountedPaths.plist
  ├─┬────Panda
  │ ├──────configuration.plist
  │ ├──────generalInformations.plist
  │ ├──────integration
  │ └──────settings.plist
  ├──────quarantine
  ├──────RealTimeScanner.plist
  ├──────Scanner.plist
  ├──────Schedules.plist
  ├──────TrustedItems.plist
  └──────Welcome.plist
```

- Carpeta /var/log/intego

```
/var/log/intego
├─┬────panda
│ └──────daemon.log
└──────virusbarrier.db
```

Si se activa la opción de guardar los mensajes a disco dentro de la carpeta /var/log/intego/panda se crearan subcarpetas cuyo nombre seguirá el formato **YYYY-MM-DD hh.mm.ss**.

31.4 Procesos

31.4.1 Comunicación a través de proxy

Si la salida a Internet es a través de proxy, es necesario configurar el producto para que utilice el proxy adecuado.

La configuración se establece en la consola de Endpoint Protection y se descarga junto con el instalador, en el fichero `generalInformations.plist`.

31.4.2 Mensajes al servidor de Endpoint Protection

El agente puede mandar al servidor de Endpoint Protection los siguientes tipos mensajes:

- Integración
- Obtención de políticas de configuración
- Validación de usuario
- Información de estado
- Reportes de detección

Además se conectará a su propio servidor de ficheros para descargar los ficheros de firmas que necesita la protección.

31.5 Protección instalada y funcionando: procesos en ejecución

Cuando la protección de Endpoint Protection está instalada y funcionando estarán en ejecución los siguientes procesos:

- /Library/Intego/virusbarrier.bundle/Contents/MacOS/VirusBarrier Alert.app/Contents/MacOS/VirusBarrier Alert

Este proceso muestra la interfaz gráfica de los análisis realizados por el residente de ficheros y de los análisis programados.

- /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarrierpalert.app/Contents/MacOS/virusbarrierpalert

Durante la instalación muestra la ventana "Installing Panda Endpoint Agent" en la que se muestra cómo se van realizando las acciones de conectar con el servidor, obtener configuración, descargar ficheros de firmas y enviar información al servidor.

- /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarrierb

Se encarga de los análisis del residente de ficheros.

- /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarriers

Es el proceso que realiza las detecciones de malware.

- /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarrierl

Se encarga de la gestión de los logs.

- /Library/Intego/TaskManager/TaskManagerDaemon

Se encarga de tareas en segundo plano, como la programación.

- /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarrierp

Se encarga de la comunicación con el servidor.

- /Library/Intego/virusbarrier.bundle/Contents/MacOS/virusbarrierd

Se encarga de la configuración del producto.

31.6 Integración

El mensaje de integración se envía tras la instalación del producto, cuando se inicia la secuencia de instalación.

Si hay algún problema que impida la integración del equipo, el servidor devolverá un código de error en su respuesta y en la ventana de progreso de la integración se mostrará uno de los siguientes errores:

- 1300 - The specified client does not exist (El cliente especificado no existe)
- 1301 - The client's licenses have expired (Las licencias del cliente han caducado)
- 1302 - The client does not have sufficient licenses (El cliente no tiene suficientes licencias)
- 1303 - The administration agent version is no longer supported (La versión del agente de administración ya no es compatible)
- 1304 - The group of computers no longer exists (El grupo de equipos ya no existe)
- 1305 - The maximum number of installations per group has been exceded (Ha excedido el número máximo de instalaciones por grupo)
- 1298 - Integration error (Error de integración)

31.7 Información de estado

Cada 12 horas se comprobará si la información del informe de estado ha cambiado y de ser así se enviará el informe. En caso de no cambiar la información, se enviará al menos un mensaje de estado al día.

Solo se enviarán informes de estado completos. No existe la posibilidad de que se envíen informes de estado reducidos.

El formato del mensaje de estado es el mismo que se usa en las protecciones Windows o Linux.

31.8 Validación de usuario

La validación del usuario sigue una lógica equivalente a la que se sigue en Windows. El tiempo que transcurre entre validaciones contra el servidor depende de la situación en que se encuentre el equipo:

- Cada 15 días cuando faltan más de 30 para la fecha de expiración de la licencia.
- Cada vez que se ejecute el proceso de validación si estamos en el periodo de los 30 días anteriores y posteriores a la expiración de la licencia.
- Cada 5 días si han transcurrido más de 30 días desde la fecha de expiración y estamos en el periodo de los 165 días posteriores a esa fecha.
- Cada 5 días si el equipo está en lista negra.
- No se valida si han transcurrido más de 165 días desde la fecha de expiración.

Cuando el usuario no es válido o el equipo está en lista negra el producto no podrá operar normalmente, es decir, no se podrán enviar mensajes al servidor ni se actualizarán los ficheros de firmas. Únicamente se podrá validar de nuevo el usuario de forma periódica para recuperar el funcionamiento normal en caso de que el usuario vuelva a estar en estado válido de nuevo.

31.9 Configuración

Por defecto la comprobación del cambio de políticas se realizará cada 4 horas.

31.10Actualización del fichero de firmas

La protección para equipos con OS X utiliza su propio sistema de fichero de firmas. El producto actualiza de forma automática los ficheros de firmas que necesita.

La comprobación de si es necesario actualizar los ficheros de firmas se hará por defecto cada hora.

31.10.1 Análisis

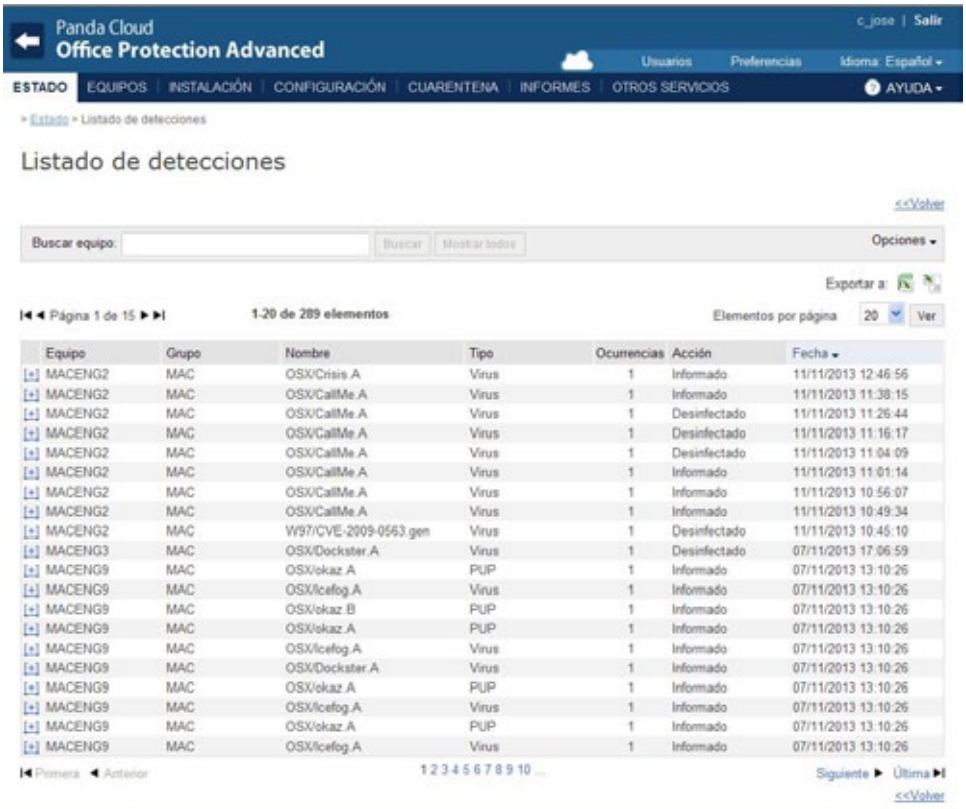
Desde la consola de Endpoint Protection solo es posible activar o desactivar el residente de ficheros en la protección para sistemas OS X. No es posible definir análisis bajo demanda para que se ejecuten en todas las máquinas de un perfil.

Sin embargo sí es posible definir análisis programados en la consola local. Las detecciones realizadas por estos análisis se reportan al servidor de la misma forma que las detecciones realizadas por el residente.

31.10.2 Listado de detecciones

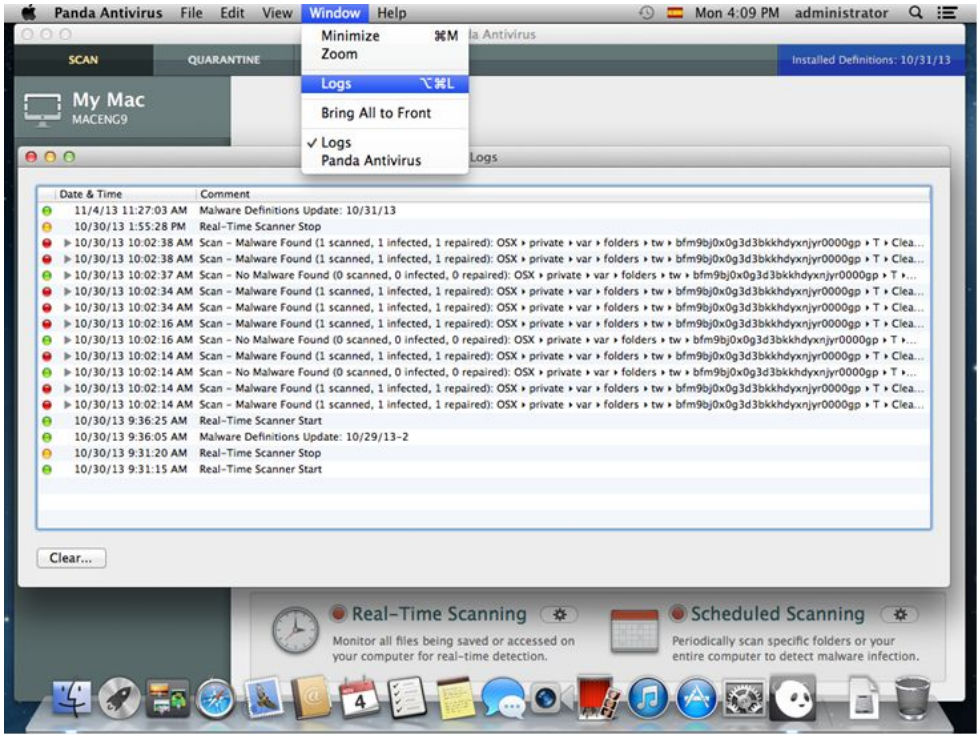
Cada 6 horas, por defecto, se comprueba si hay nuevos reportes de detección que enviar al servidor.

Los reportes se enviarán al servidor en mensajes con un máximo de 20 elementos. Estos reportes se muestran en la consola Web, en el menú **Estado** > **Lista de detecciones**, de igual manera que los reportes de la protección para Windows.



31.11Log de detecciones

Es posible consultar un log de las detecciones realizadas por el producto desde la consola local. Para ello hay que desplegar el menú Window y seleccionar la opción Logs.



31.11.1 Actualizar a versión superior

El producto no dispone de una funcionalidad de actualización automática.

Para actualizar el producto a una versión superior es necesario acceder a la consola de Endpoint Protection y descargar la nueva versión para, a continuación, ejecutar el instalador de forma manual en el equipo.

No es necesario desinstalar previamente la versión anterior, ya que el instalador es capaz de actualizar a partir de una versión anterior.

31.12Desinstalación

El producto dispone de un script de desinstalación para eliminarlo del sistema. Su ejecución se lanza desde el terminal, mediante el siguiente comando:

sudo /bin/sh /Library/Intego/virusbarrier.bundle/Contents/Resources/Uninstall.sh

También es posible desinstalar la aplicación simplemente abriendo la carpeta *Applications* y arrastrando su icono correspondiente a la papelera de reciclaje.

32. Apéndice 7

Instalación de Systems Management en equipos con Endpoint Protection

32.1 Introducción

Systems Management (http://www.pandasecurity.com/spain/enterprise/solutions/cloud-systems-management/) te permitirá monitorizar en todo momento el software instalado en los equipos que conforman tu parque informático, además de solucionar problemas de forma remota y configurar alertas para todos tus dispositivos.

Desde Panda Cloud podrás:

- Activar la versión de prueba de Systems Management a clientes que aún no dispongan de licencias de este producto. Mediante esta opción, además de activar la versión de prueba, instalarás Systems Management en los equipos de dichos clientes que tengan instalado Endpoint Protection/ Plus.
- Ofrecer a los clientes que ya disponen de licencias de Systems Management la posibilidad de Instalar Systems Management en su parque informático de forma rápida y sencilla.

32.2 Activar la versión de prueba de Systems Management

Para poder visualizar el botón de **Probar ahora** Systems Management en la pantalla de Panda Cloud, deberás cumplir los siguientes requisitos:

- Disponer de licencias de Endpoint Protection/ Plus (ya sean comerciales o de evaluación).
- Estar en versión 6.70 o superior.
- No disponer de licencias de Systems Management de ningún tipo.

Accede a Panda Cloud (https://www.pandacloudsecurity.com).

Haz clic en el botón **Probar ahora.** Puede ocurrir lo siguiente:

Si has accedido a la consola de Panda Cloud con el usuario por defecto (es decir, el usuario cuyas credenciales se te enviaron en el correo de bienvenida y que tienen el formato xxxx@pandamanagedprotection.com), visualizarás una pantalla en la que se te informará sobre la necesidad de instalar un agente en tus equipos.

Por defecto, este agente se instalará en todos los perfiles existentes en Endpoint Protection/ Plus.

Si deseas seleccionar los perfiles en los que quieres realizar la instalación del agente de Systems Management, haz clic en **Ajustes**.

Es necesario seleccionar al menos un perfil, en caso contrario el botón Iniciar prueba estará deshabilitado.

Después de hacer clic en el botón **Iniciar prueba**, se te activará la versión de prueba de Systems Management (para comprobarlo, confirma que el icono de Systems Management está accesible en la sección **Mis servicios**).

A continuación comenzará la instalación del agente de Systems Management en los perfiles seleccionados. Esta acción puede tardar hasta 12 horas.

La versión de prueba de Systems Management le proporcionará 500 licencias de Systems Management de 30 días de duración.

Si has accedido a la consola de Panda Cloud con un usuario que no sea el usuario por defecto, visualizarás un mensaje indicándote que únicamente el usuario por defecto puede activar la versión de prueba.

32.3 Finalizar la versión de prueba de Systems Management

Finalizar la versión de prueba de forma automática

Transcurridos 30 días después de la fecha de caducidad de la versión de prueba, Systems Management se desinstalará de todos los equipos en los que haya sido instalado.

Información técnica sobre el despliegue automático de Systems Management

Además de los aspectos de instalación que puedes controlar desde la consola de Panda Cloud y que se han mencionado anteriormente, a continuación se detalla el procedimiento y los procesos para desplegar Systems Management en los equipos en los que ya está instalado Endpoint Protection y que reúnen los requisitos necesarios (Consulta los requisitos en el Capítulo 1)

Procedimiento de despliegue

Nada más seleccionar el perfil, se modifica la política con los datos de Systems Management que tiene el cliente en cuyos equipos vamos a instalar.

Al lanzar un proceso `Walconf`, en los equipos del cliente se descargará dicha política, que, a su vez, realizará una modificación en el fichero `Walupg.ini`, insertando en él las entradas necesarias para que el agente de Systems Management se despliegue automáticamente la próxima vez que se lance un `Walupg`.

Las entradas insertadas en el fichero `walupg.ini` son:

- En la sección *[INSTALLED]* se añade un nuevo campo *PCSM=NOT* que indica que se va a instalar PCSM.
- Se añade una nueva sección *[PCSM]*, que será utilizada para introducir la información del perfil de PCSM y el ID del cliente correspondiente.

La próxima vez que se lance un `Walupg`, éste detectará que la entrada *PCSM* de *[INSTALLED]* ha cambiado a *NOT*, y comenzará el proceso de instalación.

Durante el proceso, lo primero que se comprobará es si ya está instalado el agente de Systems Management. Para ello se ha creado una nueva dll llamada (`WALPCSMInst.dll`).

El agente ya está instalado

Si el agente ya estuviera instalado, a la entrada *PCSM* se le modificará el valor a *Installed* por lo que ya no sería necesario instalarlo de nuevo.

El agente no está instalado

Si el agente no estuviera instalado, se sigue el proceso de instalación normal, es decir, se descargará el instalador (*GenericPCSMInstaller.exe*) desde la web de PCSM.

Este instalador está personalizado para el perfil de Systems Management del cliente, así, una vez descargado se instalará, utilizando para ello los parámetros obtenidos de la política mencionada anteriormente que contiene la información del perfil de Systems Management y el ID del cliente.

En caso de realizarse la conexión a través de un proxy, se utilizarán los datos configurados desde la consola de Endpoint Protection para ese cliente o los del Internet Explorer del equipo.

Fin de la instalación

Una vez que la instalación se ha realizado correctamente, es necesario cambiar el valor de *PCSM* del `walupg.ini`. El valor que se le adjudicará será el de la versión más actualizada de Endpoint Protection (que no tiene por qué corresponderse con la real de Systems Management).

Como es habitual, se realiza una copia del instalador en una carpeta nueva, llamada *Installers,* dentro del directorio de `WalUpg`.

Para terminar, se envía la información de rumor si está configurado.

Rumor

Para la distribución del instalador de Systems Management, el rumor funcionará exactamente igual que con el instalador del agente o de la protección.

Desplegar de nuevo el agente de Systems Management en equipos en los que se ha desplegado automáticamente con anterioridad

Si se desinstala manualmente -vía Panel de Control -el agente de Systems Management de un equipo en el que se había desplegado automáticamente, no se volverá a desplegar, ya que la entrada *PCSM* de `Walupg.ini` tendrá el valor correspondiente (*Installed* o el número de versión).

Si se desea volver a desplegar el agente en equipos asignados a un perfil para el que ya se ha desplegado previamente, habrá que eliminar la opción de despliegue automático de ese perfil desde la consola de Panda Cloud.

De esta forma, cuando se inicie la actualización de la configuración de todos los equipos que contengan el agente, se eliminarán del fichero `walupg.ini` las entradas para el despliegue automático. A continuación, si se selecciona este perfil para realizar el despliegue automático, el proceso comenzará de nuevo.

32.4 ¿Cómo es la instalación si ya dispones de licencias de Systems Management?

Si ya dispones de licencias de Systems Management (ya sean licencias de prueba o licencias comerciales), podrás realizar el despliegue de Systems Management de forma rápida y sencilla desde la pantalla de Panda Cloud, siempre y cuando cumplas los siguientes requisitos:

- Disponer de licencias de Endpoint Protection/ Plus (ya sean licencias comerciales o licencias de evaluación).
- Estar en versión 6.70 o superior.

En la pantalla de Panda Cloud, debajo del icono de acceso al producto se mostrará un botón llamado **Ajustes** que puedes utilizar para seleccionar el/los perfiles en los que deseas realizar la instalación de Systems Management.

Es importante que tengas en cuenta que:

- Por defecto, estarán seleccionados todos los perfiles. No obstante, podrás seleccionar los que creas conveniente.
- Si modificas la configuración de un perfil y seleccionas NO instalar automáticamente Systems Management, en los equipos nuevos que posteriormente se incluyan en el perfil no se instalará Systems Management; sin embargo, en los equipos ya existentes en el perfil y que ya tenían Systems Management instalado, no se desinstalará Systems Management.
- El proceso de instalación puede tardar hasta 12 horas.

Será imprescindible seleccionar al menos un perfil; en caso contrario, el botón Aceptar estará deshabilitado.

Instalación de Systems Management en función de los permisos

- Los usuarios con permisos de control total podrán instalar Systems Management en cualquier perfil.
- Los usuarios con permiso de administrador solo podrán realizar la instalación en equipos asignados a perfiles sobre los que tengan permiso de edición. Un usuario administrador tiene permiso de edición sobre un perfil si tiene permiso sobre todos los grupos de equipos asociados a ese perfil.
- Los usuarios con permiso de monitorización no podrán realizar la instalación.

33. Apéndice 8

Lista de desinstaladores

Computer Associates

eTrust AntiVirus 8.1.655, 8.1.660, 7.1*

eTrust 8.0

Avast

Avast! Free Antivirus 2014

Avast! 8.x Free Antivirus

Avast! 7.x Free Antivirus

Avast! 6.x Free Antivirus

Avast! 5.x Free Antivirus

Avast! 4 Free Antivirus

Avast! 4 Small Business Server Edition

Avast! 4 Windows Home Server Edition 4.8

AVG

AVG Internet Security 2013 (32bit- Edition)

AVG Internet Security 2013 (64bit- Edition)

AVG AntiVirus Business Edition 2013 (32bit- Edition)

AVG AntiVirus Business Edition 2013 (64bit- Edition)

AVG CloudCare 2.x

AVG Anti-Virus Business Edition 2012

AVG Internet Security 2011

AVG Internet Security Business Edition 2011 32bits*

AVG Internet Security Business Edition 2011 64bits (10.0.1375)*

AVG Anti-Virus Network Edition 8.5*

AVG Internet Security SBS Edition 8

Anti-Virus SBS Edition 8.0

AVGFree v8.5, v8, v7.5, v7.0

Avira

Avira AntiVir PersonalEdition Classic 7.x, 6.x

Avira AntiVir Personal Edition 8.x

Avira Antivir Personal - Free Antivirus 10.x, 9.x

Avira Free Antivirus 2012, 2013

Avira AntiVir PersonalEdition Premium 8.x, 7.x, 6.x

Avira Antivirus Premium 2013, 2012, 10.x, 9.x

CA

CA Total Defense for Business Client V14 (32bit- Edition)

CA Total Defense for Business Client V14 (64bit- Edition)

CA Total Defense R12 Client (32bit- Edition)

CA Total Defense R12 Client (64bit- Edition)

Bit Defender

BitDefender Business Client 11.0.22

BitDefender Free Edition 2009 12.0.12.0*

Bit Defender Standard 9.9.0.082

Check Point

Check Point Endpoint Security 8.x (32 bits)

Check Point Endpoint Security 8.x (64 bits)

Eset

ESET NOD32 Antivirus 3.0.XX (2008)*, 2.70.39*, 2.7*

ESET Smart Security 3.0*

ESET Smart Security 5 (32 bits)

ESET NOD32 Antivirus 4.X (32 bits)

ESET NOD32 Antivirus 4.X (64 bits)

ESET NOD32 Antivirus 5 (32 bits)

ESET NOD32 Antivirus 5 (64 bits)

ESET NOD32 Antivirus 6 (32 bits)

ESET NOD32 Antivirus 6 (64 bits)

ESET NOD32 Antivirus 7 (32 bits)

ESET NOD32 Antivirus 7 (64 bits)

Frisk

F-Prot Antivirus 6.0.9.1

F-Secure

F-secure PSB Workstation Security 10.x

F-Secure PSB for Workstations 9.00*

F-Secure Antivirus for Workstation 9

F-Secure PSB Workstation Security 7.21

F-Secure Protection Service for Business 8.0, 7.1

F-Secure Internet Security 2009

F-Secure Internet Security 2008

F-Secure Internet Security 2007

F-Secure Internet Security 2006

F-Secure Client Security 9.x

F-Secure Client Security 8.x

Antivirus Client Security 7.1

F-Secure Antivirus for Workstation 8

Kaspersky

Kaspersky Endpoint Security 10 for Windows (32bit- Edition)

Kaspersky Endpoint Security 10 for Windows (64bit- Edition)

Kaspersky Endpoint Security 8 for Windows (32bit- Edition)

Kaspersky Endpoint Security 8 for Windows (64bit- Edition)

Kaspersky Anti-Virus 2010 9.0.0.459*

Kaspersky® Business Space Security

Kaspersky® Work Space Security

Kaspersky Internet Security 8.0, 7.0, 6.0 (con Windows Vista+UAC, es necesario desactivar UAC)

Kaspersky Anti-Virus 8*

Kaspersky® Anti-virus 7.0 (con Windows Vista+UAC, es necesario desactivar UAC)

Kaspersky Anti-Virus 6.0 for Windows Workstations*

McAfee

McAfee SaaS Endpoint Protection 6.x, 5.X

McAfee VirusScan Enterprise 8.8, 8.7i, 8.5i, 8.0i, 7.1.0

McAfee Internet Security Suite 2007

McAfee Total Protection Service 4.7*

McAfee Total Protection 2008

Norman

Norman Security Suite 10.x (32bit- Edition)

Norman Security Suite 10.x (64bit- Edition)

Norman Security Suite 9.x (32bit- Edition)

Norman Security Suite 9.x (64bit- Edition)

Norman Endpoint Protection 8.x/9.x

Norman Virus Control v5.99

Norton

Norton Antivirus Internet Security 2008*

Norton Antivirus Internet Security 2007

Norton Antivirus Internet Security 2006

Microsoft

Microsoft Security Essentials 1.x

Microsoft Forefront EndPoint Protection 2010

Microsoft Security Essentials 4.x

Microsoft Security Essentials 2.0

Microsoft Live OneCare

Microsoft Live OneCare 2.5*

MicroWorld Technologies

eScan Corporate for Windows 9.0.824.205

PcTools

Spyware Doctor with AntiVirus 9.x

Sophos

Sophos Anti-virus 9.5

Sophos Endpoint Security and Control 10.2

Sophos Endpoint Security and Control 9.5

Sophos Anti-virus 7.6

Sophos Anti-virus SBE 2.5*

Sophos Security Suite

Symantec

Symantec.cloud - Endpoint Protection.cloud 21.x (32bits)

Symantec.cloud - Endpoint Protection.cloud 21.x (64bits)

Symantec EndPoint Protection 12.x (32bits)

Symantec EndPoint Protection 12.x (64bits)

Symantec EndPoint Protection 11.x (32bits)

Symantec EndPoint Protection 11.x (64bits)

Symantec Antivirus 10.1

Symantec Antivirus Corporate Edition 10.0, 9.x, 8.x

Trend Micro

Trend Micro Worry-Free Business Security 8.x (32bit- Edition)

Trend Micro Worry-Free Business Security 8.x (64bit- Edition)

Trend Micro Worry-Free Business Security 7.x (32bit- Edition)

Trend Micro Worry-Free Business Security 7.x (64bit- Edition)

Trend Micro Worry-Free Business Security 6.x (32bit- Edition)

Trend Micro Worry-Free Business Security 6.x (64bit- Edition)

Trend Micro Worry-Free Business Security 5.x

PC-Cillin Internet Security 2006

PC-Cillin Internet Security 2007*

PC-Cillin Internet Security 2008*

Trend Micro OfficeScan Antivirus 8.0

Trend Micro OfficeScan 7.x

Trend Micro OfficeScan 8.x

Trend Micro OfficeScan 10.x

Comodo Antivirus

Comodo Antivirus V 4.1 32bits

Panda Security

Panda Cloud Antivirus 3.x

Panda Cloud Antivirus 2.X

Panda Cloud Antivirus 1.X

Panda for Desktops 4.50.XX

Panda for Desktops 4.07.XX

Panda for Desktops 4.05.XX

Panda for Desktops 4.04.10

Panda for Desktops 4.03.XX y anteriores

Panda for File Servers 8.50.XX

Panda for File Servers 8.05.XX

Panda for File Servers 8.04.10

Panda for File Servers 8.03.XX y anteriores

Panda Global Protection 2015*

Panda Internet Security 2015*

Panda Antivirus Pro 2015*

Panda Gold Protection*

Panda Free Antivirus

Panda Global Protection 2014*

Panda Internet Security 2014*

Panda Antivirus Pro 2014*

Panda Gold Protection*

Panda Global Protection 2013*

Panda Internet Security 2013*

Panda Antivirus Pro 2013*

Panda Global Protection 2012*

Panda Internet Security 2012*

Panda Antivirus Pro 2012*

Panda Global Protection 2011*

Panda Internet Security 2011*

Panda Antivirus Pro 2011*

Panda Antivirus for Netbooks (2011)*

Panda Global Protection 2010

Panda Internet Security 2010

Panda Antivirus Pro 2010

Panda Antivirus for Netbooks

Panda Global Protection 2009

Panda Internet Security 2009

Panda Antivirus Pro 2009

Panda Internet Security 2008

Panda Antivirus+Firewall 2008

Panda Antivirus 2008

Panda Internet Security 2007

Panda Antivirus + Firewall 2007

Panda Antivirus 2007

*Productos Panda 2015, 2014, 2013, 2012 necesitan un reinicio para completar la desinstalación.

*Comodo AntiVirus V 4.1 32 bits - En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción Permitir.

F-Secure PSB for Workstations 9.00 - Durante el proceso de instalación del agente de PCOP en Windows 7 y Windows Vista, el usuario debe intervenir seleccionando la opción Permitir.

* AVG Internet Security Business Edition 2011 32bits - Durante el proceso de instalación del agente de PCOP, el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

** AVG Internet Security Business Edition 2011 64bits (10.0.1375) - Durante el proceso de instalación del agente de PCOP, el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

* Kaspersky Anti-Virus 6.0 for Windows Workstations:

Durante el proceso de instalación del agente de PCOP en sistemas operativos de 64 bits el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

Para poder hacer la desinstalación, la protección de Kaspersky no debe tener password.

En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción Permitir.

* F-Secure PSB for Workstations 9.00 - Durante el proceso de instalación del agente de PCOP, el usuario debe intervenir seleccionando la opción Permitir en dos ventanas de F-Secure PSB for Workstations 9.00.

* AVG Anti-Virus Network Edition 8.5 - Durante el proceso de instalación del agente de PCOP el usuario debe intervenir seleccionando en dos ventanas de AVG Anti-Virus Network Edition 8.5 la opción Permitir.

* Productos Panda Antivirus 2011 - No se desinstalan en Windows Vista x64. En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Panda Cloud Antivirus 1.4 Pro y Panda Cloud Antivirus 1.4 Free - En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Trend Micro - PC-Cillin Internet Security 2007 y 2008 no se puede desinstalar automáticamente en Windows Vista x64.

* Trend Micro - PC-Cillin Internet Security 2007 y 2008 no se pueden desinstalar automáticamente en Windows Vista x86 teniendo UAC activado.

* ESET NOD32 Antivirus 3.0.XX (2008) no se desinstala automáticamente en plataformas de 64 bits.

* ESET Smart Security 3.0 no se desinstala automáticamente en plataformas de 64 bits.

* ESET NOD32 Antivirus 2.7 tras la instalación de agente de PCOP el equipo se reiniciará automaticamente sin mostrar ningún aviso, ni pedir confirmación al usuario.

* ESET NOD32 Antivirus 2.70.39 tras la instalación de agente de PCOP el equipo se reiniciará automaticamente sin mostrar ningún aviso, ni pedir confirmación al usuario.

* Sophos Anti-virus SBE 2.5 no se desinstala correctamente en Windows 2008.

* eTrust Antivirus 7.1. no se desinstala en sistemas operativos de 64bits (Windows 2003 64bits y Windows XP 64bits).

* Norton Antivirus Internet Security 2008 no se puede desinstalar en Windows Vista con UAC activado.

* Kaspersky Anti-Virus 2010 9.0.0.459. En sistemas con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* Kaspersky Anti-Virus 8 . En Windows Vista con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

* BitDefender Free Edition 2009 12.0.12.0. En Windows Vista con UAC activado, durante el proceso de desinstalación el usuario debe intervenir seleccionando en la ventana del UAC la opción de permitir.

*McAfee Total Protection Service 4.7. El desinstalador no funciona en sistemas con UAC activado. Además, en sistemas de 32 bits es necesaria la intervención del usuario.

* Microsoft Live OneCare 2.5. No desinstala en Windows Small Business Server 2008.

En caso de tener instalado un programa que no se encuentra incluido en el listado, consulte con el proveedor correspondiente cómo desinstalarlo antes de instalar la protección de Endpoint Protection.

euskaltel

Endpoint Protection