



Endpoint Protection

Endpoint Protection Plus

Guía para el administrador

Versión: 3.20.00-00

Autor: Panda Security

Fecha: 27/11/2017

Tabla de contenidos

1. PRÓLOGO	10
1.1. INTRODUCCIÓN	11
1.2. ¿A QUIÉN ESTÁ DIRIGIDA ESTA GUÍA?	11
1.3. ENDPOINT PROTECTION / ENDPOINT PROTECTION PLUS	11
1.4. ICONOS	11
2. INTRODUCCIÓN	13
2.1. INTRODUCCIÓN	14
2.2. BENEFICIOS PRINCIPALES DE ENDPOINT PROTECTION / PLUS SOBRE AETHER.	14
2.3. BENEFICIOS PRINCIPALES DE ENDPOINT PROTECTION PLUS SOBRE AETHER.	15
2.4. CARACTERÍSTICAS PRINCIPALES DE LA PLATAFORMA AETHER	16
2.4.1 PRINCIPALES BENEFICIOS DE AETHER	16
2.4.2 ARQUITECTURA DE AETHER	18
2.4.3 AETHER EN LOS EQUIPOS DE USUARIO	18
2.5. COMPONENTES PRINCIPALES DE LA ARQUITECTURA ENDPOINT PROTECTION / PLUS	20
2.5.1 SERVIDORES DE INTELIGENCIA COLECTIVA	21
2.5.2 SERVIDOR WEB DE LA CONSOLA DE ADMINISTRACIÓN	21
2.5.3 EQUIPOS PROTEGIDOS CON ENDPOINT PROTECTION / PLUS	22
2.6. PERFIL DE USUARIO DE ENDPOINT PROTECTION / PLUS SOBRE AETHER	22
2.7. DISPOSITIVOS E IDIOMAS SOPORTADOS EN ENDPOINT PROTECTION / PLUS SOBRE AETHER	22
2.8. RECURSOS Y DOCUMENTACIÓN DISPONIBLE	23
3. TECNOLOGÍAS ENDPOINT PROTECTION / PLUS	25
3.1. INTRODUCCIÓN	26
3.2. RECURSOS TÉCNICOS IMPLEMENTADOS EN ENDPOINT PROTECTION / PLUS	26
3.2.1 PROTECCIÓN CONTRA EXPLOITS	27
3.2.2 PROTECCIÓN ANTIVIRUS PERMANENTE E INTELIGENCIA COLECTIVA	27
3.2.3 PROTECCIÓN CONTRA TÉCNICAS AVANZADAS DE OCULTACIÓN Y VIRUS DE MACRO ...	28
3.2.4 PROTECCIÓN DEL CORREO Y LA WEB	29
3.2.5 PROTECCIÓN CON CORTAFUEGOS Y SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)	29
3.2.6 CONTROL DE DISPOSITIVOS	29
3.2.7 FILTRADO DE SPAM, VIRUS Y CONTENIDOS EN SERVIDORES EXCHANGE	30
3.2.8 CONTROL DE ACCESO A PÁGINAS WEB	31
3.2.9 VISIBILIDAD DEL ESTADO DE LA RED	31
3.2.10 TÉCNICAS DE DESINFECCIÓN	31
3.3. LA FASE DE ADAPTACIÓN	32
4. LA CONSOLA DE ADMINISTRACIÓN	34
4.1. INTRODUCCIÓN	35
4.1.1 REQUISITOS DE LA CONSOLA WEB	35
4.1.2 FEDERACIÓN CON IDP	36

4.2. CARACTERÍSTICAS GENERALES DE LA CONSOLA	36
4.3. ESTRUCTURA GENERAL DE LA CONSOLA WEB DE ADMINISTRACIÓN	36
4.3.1 MENÚ SUPERIOR (1).....	37
4.3.2 MENÚ LATERAL (2)	40
4.3.3 WIDGETS (3)	40
4.3.4 MENÚ DE PESTAÑAS SUPERIOR	40
4.3.5 HERRAMIENTAS DE FILTRADO Y BÚSQUEDA	40
4.3.6 BOTÓN DE VOLVER.....	41
4.3.7 ELEMENTOS DE CONFIGURACIÓN (8)	41
4.3.8 MENÚS DE CONTEXTO	42
4.3.9 LISTADOS	42
5. LICENCIAS	44
5.1. INTRODUCCIÓN	45
5.2. DEFINICIONES Y CONCEPTOS CLAVE PARA LA GESTIÓN DE LICENCIAS	45
5.2.1 MANTENIMIENTOS.....	45
5.2.2 ESTADO DE LOS EQUIPOS.....	45
5.2.3 ESTADO DE LAS LICENCIAS Y GRUPOS	46
5.2.4 TIPOS DE LICENCIAS	46
5.2.5 ASIGNACIÓN DE LICENCIAS	46
5.2.6 LIBERACIÓN DE LICENCIAS	47
5.2.7 PROCESOS DE ASIGNACIÓN Y LIBERACIÓN DE LICENCIAS	47
5.3. LICENCIAS CONTRATADAS	48
5.3.1 WIDGET	49
5.3.2 LISTADO DE LICENCIAS	50
5.4. LICENCIAS CADUCADAS	52
5.4.1 MENSAJES DE CADUCIDAD PRÓXIMA Y VENCIDA.....	53
5.4.2 LÓGICA DE LIBERACIÓN DE LICENCIAS CADUCADAS	53
5.5. LICENCIAS DE PRUEBA (TRIAL) SOBRE LICENCIAS COMERCIALES	53
5.6. BÚSQUEDA DE EQUIPOS SEGÚN EL ESTADO DE LA LICENCIA ASIGNADA	54
6. INSTALACIÓN DEL SOFTWARE ENDPOINT PROTECTION / PLUS	55
6.1. INTRODUCCIÓN	56
6.2. VISIÓN GENERAL DEL DESPLIEGUE DE LA PROTECCIÓN	56
6.3. REQUISITOS DE INSTALACIÓN	59
6.3.1 REQUISITOS POR PLATAFORMA.....	59
6.3.2 REQUISITOS DE RED	60
6.4. DESCARGA E INSTALACIÓN MANUAL DEL SOFTWARE ENDPOINT PROTECTION / PLUS	60
6.4.1 DESCARGA DEL PAQUETE DE INSTALACIÓN DESDE LA CONSOLA WEB.....	60
6.4.2 GENERACIÓN DE URL DE DESCARGA	61
6.4.3 INSTALACIÓN MANUAL DEL SOFTWARE ENDPOINT PROTECTION / PLUS	62
6.5. DESCUBRIMIENTO AUTOMÁTICO DE EQUIPOS E INSTALACIÓN REMOTA	64
6.5.1 REQUISITOS PARA INSTALAR ENDPOINT PROTECTION / PLUS EN LOS EQUIPOS	64
6.5.2 DESCUBRIMIENTO DE EQUIPOS	64
6.5.3 ALCANCE DEL DESCUBRIMIENTO	66
6.5.4 PROGRAMACIÓN DEL DESCUBRIMIENTO DE EQUIPOS	66
6.5.5 LISTADO DE EQUIPOS DESCUBIERTOS	67
6.5.6 DETALLES DEL EQUIPO DESCUBIERTO	71

6.5.7	INSTALACIÓN DE EQUIPOS	72
6.6.	INSTALACIÓN CON HERRAMIENTAS CENTRALIZADAS	73
6.7.	INSTALACIÓN MEDIANTE GENERACIÓN DE IMÁGENES	77
6.8.	DESINSTALACIÓN DEL SOFTWARE.....	77
7.	<u>GESTIÓN DE EQUIPOS Y DISPOSITIVOS.....</u>	<u>79</u>
7.1.	INTRODUCCIÓN	80
7.1.1	REQUISITOS PARA LA GESTIÓN DE EQUIPOS DESDE LA CONSOLA	80
7.2.	LA ZONA EQUIPOS	80
7.2.1	EL PANEL ÁRBOL DE EQUIPOS.....	82
7.2.2	EL PANEL LISTADO DE EQUIPOS.....	83
7.2.3	LISTADO DE EQUIPOS.....	84
7.3.	ÁRBOL DE FILTROS	87
7.3.1	¿QUÉ ES UN FILTRO?.....	87
7.3.2	AGRUPACIONES DE FILTROS	88
7.3.3	FILTROS PREDEFINIDOS.....	88
7.3.4	CREACIÓN Y ORGANIZACIÓN DE FILTROS	89
7.3.5	CONFIGURACIÓN DE FILTROS	90
7.3.6	REGLAS DE FILTRADO	91
7.3.7	OPERADORES LÓGICOS	91
7.3.8	AGRUPACIONES DE REGLAS DE FILTRADO.....	92
7.4.	ÁRBOL DE GRUPOS	93
7.4.1	¿QUÉ ES UN GRUPO?	94
7.4.2	TIPOS DE GRUPOS	94
7.4.3	ESTRUCTURA DE GRUPOS	94
7.4.4	GRUPOS DE DIRECTORIO ACTIVO	94
7.4.5	CREACIÓN Y ORGANIZACIÓN DE GRUPOS	95
7.4.6	MOVIMIENTO DE EQUIPOS ENTRE GRUPOS.....	96
7.5.	INFORMACIÓN DE EQUIPO	97
7.5.1	SECCIÓN GENERAL (1).....	98
7.5.2	SECCIÓN ALERTAS DE EQUIPO (2).....	98
7.5.3	SECCIÓN DETALLES (3)	99
7.5.4	SECCIÓN HARDWARE (4).....	100
7.5.5	SECCIÓN SOFTWARE (5).....	101
7.5.6	SECCIÓN CONFIGURACIÓN (6)	101
7.5.7	FORZAR SINCRONIZACIÓN (7)	102
7.5.8	MENÚ DE CONTEXTO	102
8.	<u>GESTIÓN DE CONFIGURACIONES.....</u>	<u>103</u>
8.1.	INTRODUCCIÓN	104
8.2.	¿QUÉ ES UNA CONFIGURACIÓN?	104
8.3.	VISIÓN GENERAL DE LA ASIGNACIÓN DE CONFIGURACIONES A EQUIPOS.....	104
8.3.1	DIFUSIÓN INMEDIATA DE LA CONFIGURACIÓN.....	105
8.3.2	ÁRBOL MULTINIVEL.....	105
8.3.3	HERENCIA	105
8.3.4	CONFIGURACIONES MANUALES	106
8.3.5	CONFIGURACIÓN POR DEFECTO	106
8.4.	PERFILES DE CONFIGURACIÓN MODULARES VS MONOLÍTICOS.....	106

8.5. INTRODUCCIÓN A LOS CUATRO TIPOS DE CONFIGURACIONES	109
8.6. CREACIÓN Y GESTIÓN DE CONFIGURACIONES.....	109
8.7. ASIGNACIÓN MANUAL Y AUTOMÁTICA DE CONFIGURACIONES A GRUPOS	110
8.7.1 ASIGNACIÓN DIRECTA / MANUAL DE CONFIGURACIONES.....	111
8.7.2 ASIGNACIÓN INDIRECTA DE CONFIGURACIONES: LAS DOS REGLAS DE LA HERENCIA. 113	
8.7.3 LÍMITES DE LA HERENCIA	114
8.7.4 SOBRE ESCRITURA DE CONFIGURACIONES.....	114
8.7.5 ELIMINACIÓN DE ASIGNACIONES MANUALES Y RESTAURACIÓN DE LA HERENCIA	118
8.7.6 MOVIMIENTO DE GRUPOS Y EQUIPOS	119
8.8. VISUALIZAR LAS CONFIGURACIONES ASIGNADAS.....	119
<u>9. CONFIGURACIÓN DEL AGENTE Y LA PROTECCIÓN LOCAL.....</u>	<u>122</u>
9.1. INTRODUCCIÓN	123
9.2. CONFIGURACIÓN DE LOS ROLES DEL AGENTE PANDA.....	123
9.2.1 ROL DE PROXY	123
9.2.2 ROL DE CACHE / REPOSITORIO.....	124
9.2.3 ROL DE DESCUBRIDOR	125
9.3. CONFIGURACIÓN DEL ACCESO A TRAVÉS DE PROXY	125
9.4. CONFIGURACIÓN DE LA COMUNICACIÓN EN TIEMPO REAL.....	127
9.5. CONFIGURACIÓN DEL IDIOMA DEL AGENTE.....	127
9.6. CONFIGURACIÓN DE CONTRASEÑA Y ANTI-TAMPERING.....	128
9.6.1 ANTI-TAMPER.....	128
9.6.2 PROTECCIÓN DEL AGENTE MEDIANTE CONTRASEÑA.....	128
<u>10. CONFIGURACIÓN DE SEGURIDAD PARA ESTACIONES Y SERVIDORES</u>	<u>129</u>
10.1. INTRODUCCIÓN	130
10.2. INTRODUCCIÓN A LA CONFIGURACIÓN DE ESTACIONES Y SERVIDORES.....	130
10.3. CONFIGURACIÓN GENERAL.....	131
10.3.1 ACTUALIZACIONES	131
10.3.2 DESINSTALAR OTROS PRODUCTOS DE SEGURIDAD.....	131
10.3.3 EXCLUSIONES	131
10.4. ANTIVIRUS	132
10.4.1 AMENAZAS A DETECTAR	132
10.4.2 TIPOS DE ARCHIVOS	132
10.5. FIREWALL (EQUIPOS WINDOWS)	133
10.5.1 MODO DE FUNCIONAMIENTO	133
10.5.2 TIPO DE RED	133
10.5.3 REGLAS DE PROGRAMA	134
10.5.4 REGLA DE CONEXIÓN	135
10.5.5 BLOQUEAR INTRUSIONES.....	137
10.6. CONTROL DE DISPOSITIVOS (EQUIPOS WINDOWS).....	139
10.6.1 EQUIPOS PERMITIDOS.....	140
10.6.2 EXPORTAR E IMPORTAR LISTAS DE DISPOSITIVOS PERMITIDOS	140
10.6.3 OBTENCIÓN DEL IDENTIFICADOR ÚNICO DEL DISPOSITIVO	140
10.7. CONTROL DE ACCESO A PÁGINAS WEB	141
10.7.1 CONFIGURAR HORARIOS DEL CONTROL DE ACCESOS A PÁGINAS WEB.....	141
10.7.2 DENEGAR EL ACCESO A PÁGINAS WEB	141
10.7.3 LISTA DE DIRECCIONES Y DOMINIOS PERMITIDOS O DENEGADOS	142

10.7.4 BASE DE DATOS DE URLS ACCEDIDAS DESDE LOS EQUIPOS.....	142
10.8. ANTIVIRUS PARA SERVIDORES EXCHANGE.....	143
10.9. ANTI SPAM PARA SERVIDORES EXCHANGE	144
10.9.1 ACCIÓN PARA MENSAJES DE SPAM	145
10.9.2 DIRECCIONES Y DOMINIOS PERMITIDOS	145
10.9.3 DIRECCIONES Y DOMINIOS DE SPAM.....	145
10.10. FILTRADO DE CONTENIDOS PARA SERVIDORES EXCHANGE.....	146
<u>11. CONFIGURACIÓN DE SEGURIDAD ANDROID.....</u>	<u>148</u>
11.1. INTRODUCCIÓN	149
11.2. INTRODUCCIÓN A LA CONFIGURACIÓN DE DISPOSITIVOS ANDROID	149
11.3. ACTUALIZACIONES	149
11.4. ANTIVIRUS	149
<u>12. ACTUALIZACIÓN DEL SOFTWARE.....</u>	<u>151</u>
12.1. INTRODUCCIÓN	152
12.2. CONFIGURACIÓN DE LA ACTUALIZACIÓN DEL MOTOR DE PROTECCIÓN	152
12.2.1 ACTUALIZACIONES	153
12.3. CONFIGURACIÓN DE LA ACTUALIZACIÓN DEL AGENTE DE COMUNICACIONES.....	154
12.4. CONFIGURACIÓN DE LA ACTUALIZACIÓN DEL CONOCIMIENTO.....	154
12.4.1 DISPOSITIVOS WINDOWS, LINUX Y MAC	154
12.4.2 DISPOSITIVOS ANDROID.....	155
<u>13. TAREAS.....</u>	<u>156</u>
13.1. INTRODUCCIÓN	157
13.2. CREACIÓN DE TAREAS	157
13.2.1 DESTINATARIOS DE LA TAREA	157
13.2.2 PROGRAMACIÓN HORARIA Y REPETICIÓN DE LA TAREA	157
13.3. PUBLICACIÓN DE TAREAS.....	159
13.4. GESTIÓN DE TAREAS	160
<u>14. VISIBILIDAD DEL MALWARE Y DEL PARQUE INFORMÁTICO</u>	<u>162</u>
14.1. INTRODUCCIÓN	163
14.2. ESQUEMA GENERAL DEL MENÚ ESTADO.....	163
14.3. PANELES / WIDGETS DISPONIBLES	165
14.3.1 ESTADO DE PROTECCIÓN	165
14.3.2 EQUIPOS SIN CONEXIÓN	168
14.3.3 PROTECCIÓN DESACTUALIZADA	169
14.3.4 AMENAZAS PERMITIDAS POR EL ADMINISTRADOR.....	170
14.3.5 AMENAZAS DETECTADAS POR EL ANTIVIRUS	171
14.3.6 FILTRADO DE CONTENIDOS EN SERVIDORES EXCHANGE	172
14.3.7 ACCESOS A PÁGINAS WEB.....	173
14.3.8 CATEGORÍAS MÁS ACCEDIDAS (TOP 10)	175
14.3.9 CATEGORÍAS MÁS ACCEDIDAS POR EQUIPO (TOP 10)	176
14.3.10 CATEGORÍAS MÁS BLOQUEADAS (TOP 10)	177

14.3.11	CATEGORÍAS MÁS BLOQUEADAS POR EQUIPO (TOP 10)	178
14.4.	INTRODUCCIÓN A LOS LISTADOS	180
14.4.1	PLANTILLAS, CONFIGURACIONES Y VISTAS	180
14.4.2	PANEL MIS LISTADOS	182
14.4.3	CREAR UN LISTADO PERSONALIZADO	183
14.4.4	BORRAR UN LISTADO	184
14.4.5	CONFIGURAR UN LISTADO PERSONALIZADO	184
14.5.	LISTADOS DISPONIBLES	185
14.5.1	LISTADO DE ESTADO DE PROTECCIÓN DE LOS EQUIPOS	185
14.5.2	LISTADO DE AMENAZAS PERMITIDAS POR EL ADMINISTRADOR	188
14.5.3	LISTADO HISTORIAL DE AMENAZAS PERMITIDAS POR EL ADMINISTRADOR	190
14.5.4	LISTADO DE AMENAZAS DETECTADAS POR EL ANTIVIRUS	192
14.5.5	LISTADO DE ACCESOS A PÁGINAS WEB POR CATEGORÍA	194
14.5.6	LISTADO DE ACCESOS A PÁGINAS WEB POR EQUIPO	195
14.5.7	LISTADO DE DISPOSITIVOS BLOQUEADOS	197
14.5.8	LISTADO DE LICENCIAS	199
14.5.9	LISTADO DE EQUIPOS NO ADMINISTRADOS DESCUBIERTOS	199
14.6.	LISTADOS INCLUIDOS POR DEFECTO	199
15.	<u>GESTIÓN DE ELEMENTOS EXCLUIDOS Y EN BACKUP / CUARENTENA</u>	201
15.1.	INTRODUCCIÓN	202
15.2.	ACCESO A LOS RECURSOS PARA LA GESTIÓN DE EXCLUSIONES	202
15.3.	AÑADIR UNA EXCLUSIÓN DE ELEMENTOS	203
15.3.1	EXCLUSIONES DE ELEMENTOS CLASIFICADOS COMO AMENAZAS	203
15.4.	GESTIÓN DE LOS ELEMENTOS EXCLUIDOS	203
15.5.	GESTIÓN DE LA ZONA DE BACKUP / CUARENTENA	204
15.5.1	VISUALIZACIÓN DE LOS ELEMENTOS EN CUARENTENA	205
15.5.2	RESTAURAR ELEMENTOS DE CUARENTENA	205
16.	<u>HERRAMIENTAS DE RESOLUCIÓN</u>	206
16.1.	INTRODUCCIÓN	207
16.2.	DESINFECCIÓN AUTOMÁTICA DE EQUIPOS	207
16.3.	ANÁLISIS / DESINFECCIÓN BAJO DEMANDA DE EQUIPOS	208
16.3.1	TAREAS DE ANÁLISIS PROGRAMADAS	208
16.3.2	ANÁLISIS INMEDIATO	208
16.4.	REINICIAR EQUIPOS	209
16.5.	NOTIFICAR UN PROBLEMA	210
16.6.	PERMITIR EL ACCESO EXTERNO A LA CONSOLA WEB	210
17.	<u>ALERTAS</u>	212
17.1.	INTRODUCCIÓN	213
17.2.	ALERTAS POR CORREO	213
17.2.1	CONFIGURACIÓN DE ALERTAS POR CORREO	213
17.2.2	VISIBILIDAD DEL ADMINISTRADOR Y ENVÍO DE ALERTAS	213
17.2.3	TIPOS DE ALERTAS	213

18. INFORMES	216
18.1. INTRODUCCIÓN	217
18.2. GENERACIÓN BAJO DEMANDA DE INFORMES EJECUTIVOS	217
18.2.1 INFORMACIÓN REQUERIDA PARA LA GENERACIÓN DE INFORMES BAJO DEMANDA..	217
18.3. ENVÍO PROGRAMADO DE INFORMES EJECUTIVOS.....	218
18.3.1 INFORMACIÓN REQUERIDA PARA LA GENERACIÓN DE INFORMES PROGRAMADOS..	218
19. CONTROL Y SUPERVISIÓN DE LA CONSOLA DE ADMINISTRACIÓN	220
19.1. INTRODUCCIÓN	221
19.2. ¿QUÉ ES UNA CUENTA DE USUARIO?	221
19.2.1 ESTRUCTURA DE UNA CUENTA DE USUARIO	221
19.2.2 ¿QUÉ ES EL USUARIO PRINCIPAL?.....	222
19.3. ¿QUÉ ES UN ROL?.....	222
19.3.1 ESTRUCTURA DE UN ROL	222
19.3.2 ¿POR QUÉ SON NECESARIOS LOS ROLES?.....	222
19.3.3 EL ROL CONTROL TOTAL.....	223
19.3.4 EL ROL MONITORIZACIÓN	223
19.4. ¿QUÉ ES UN PERMISO?	224
19.4.1 SIGNIFICADO DE LOS PERMISOS IMPLEMENTADOS	224
19.5. ACCESO A LA CONFIGURACIÓN DE CUENTAS DE USUARIOS Y ROLES	228
19.6. CREACIÓN Y CONFIGURACIÓN DE CUENTAS DE USUARIO	228
19.7. CREACIÓN Y CONFIGURACIÓN DE ROLES	229
19.8. REGISTRO DE LA ACTIVIDAD DE LAS CUENTAS DE USUARIO.....	229
19.8.1 REGISTRO DE ACCIONES.....	229
19.8.2 REGISTRO DE SESIONES.....	232
20. APÉNDICE I: REQUISITOS DE ENDPOINT PROTECTION / PLUS	234
20.1. REQUISITOS DE PLATAFORMAS WINDOWS.....	235
20.1.1 SISTEMAS OPERATIVOS SOPORTADOS	235
20.1.2 REQUISITOS HARDWARE.....	235
20.2. REQUISITOS DE PLATAFORMAS WINDOWS EXCHANGE	235
20.2.1 SISTEMAS OPERATIVOS SOPORTADOS	235
20.2.2 REQUISITOS HARDWARE Y SOFTWARE.....	236
20.2.3 VERSIONES EXCHANGE SOPORTADAS	236
20.3. REQUISITOS DE PLATAFORMAS MACOS.....	236
20.3.1 SISTEMAS OPERATIVOS SOPORTADOS	236
20.3.2 REQUISITOS HARDWARE.....	236
20.4. REQUISITOS DE PLATAFORMAS LINUX	237
20.4.1 DISTRIBUCIONES DE 64 BITS SOPORTADAS	237
20.4.2 VERSIÓN DE KERNEL SOPORTADA	237
20.4.3 GESTORES DE FICHEROS SOPORTADOS	237
20.4.4 REQUISITOS HARDWARE.....	237
20.4.5 DEPENDENCIAS DEL PAQUETE DE INSTALACIÓN	237
20.5. REQUISITOS DE PLATAFORMAS ANDROID	238
20.5.1 SISTEMAS OPERATIVOS SOPORTADOS	238
20.5.2 REQUISITOS HARDWARE.....	238
20.5.3 REQUISITOS DE RED	238

20.6. ACCESO A LA CONSOLA WEB.....	238
20.7. ACCESO A URLS DEL SERVICIO.....	238
<u>21. APÉNDICE II: CREACIÓN Y GESTIÓN DE CUENTAS PANDA</u>	<u>240</u>
21.1. INTRODUCCIÓN	241
21.2. CREACIÓN DE UNA CUENTA PANDA.....	241
21.3. ACTIVACIÓN DE LA CUENTA PANDA.....	241
<u>22. APÉNDICE III: LISTADO DE DES INSTALADORES.....</u>	<u>243</u>
<u>23. APÉNDICE IV: CONCEPTOS CLAVE.....</u>	<u>250</u>

1. Prólogo

¿A quién está dedicada esta guía?
Iconos

1.1. Introducción

Esta guía contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto **Endpoint Protection / Endpoint Protection Plus sobre Aether**.

1.2. ¿A quién está dirigida esta guía?

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

Endpoint Protection / Plus es un servicio gestionado que ofrece seguridad sin intervención activa y constante del administrador de la red, y provee información muy detallada del parque informático y del estado de la seguridad gracias a la nueva plataforma **Aether**, desarrollada por Panda Security. **Aether** es una plataforma eficiente, extensible y escalable para la gestión centralizada de las soluciones de seguridad de Panda Security, que cubre las necesidades de la gran cuenta y MSPs. **Aether** permite presentar toda la información generada por **Endpoint Protection / Plus** sobre los procesos, los programas ejecutados por los usuarios y los dispositivos instalados en la empresa en tiempo real, de forma ordenada y con un alto nivel de detalle.

1.3. Endpoint Protection / Endpoint Protection Plus

Esta guía cubre los productos **Endpoint Protection** y **Endpoint Protection Plus**. Debido a que comparten muchas características y ambos funcionan sobre la nueva plataforma **Aether**, esta guía se refiere a los dos productos con el nombre **Endpoint Protection / Plus** o **Endpoint Protection / Plus sobre Aether**. Las funcionalidades solo disponibles en **Endpoint Protection Plus** serán indicadas

mediante el icono .

1.4. Iconos

En esta guía se utilizan los siguientes iconos:



Aclaraciones e 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 / Plus**.



Consulta en otro capítulo o punto del manual.



Característica solo disponible en **Endpoint Protection Plus**.

2. Introducción

Características principales del producto
Características principales de la plataforma
Componentes principales de la arquitectura
 Servicios
 Perfil de usuario del producto
Dispositivos e idiomas soportados
 Recursos y documentación

2.1. Introducción

Endpoint Protection y **Endpoint Protection Plus** son dos soluciones de seguridad basadas en múltiples tecnologías de protección, que permiten sustituir el producto de antivirus *on premise* o *standalone* utilizado en la empresa por un completo servicio cloud gestionado desde la nube.

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

Endpoint Protection Plus permite además controlar la productividad de los usuarios de la organización, impidiendo el acceso a recursos web sin relación con la actividad de la empresa y filtrando el correo corporativo para evitar pérdidas de rendimiento provocadas por el spam.

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

Ambos productos son multiplataforma, alojados en la nube y compatibles con Windows, Linux, MacOS y Android; por esta razón, solo es necesaria una única herramienta para cubrir la seguridad de todos los dispositivos de la empresa.

2.2. Beneficios principales de Endpoint Protection / Plus sobre Aether.

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

- **Producto muy ligero**

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

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

- **Seguridad Multiplataforma**

Cubre todos los vectores de infección en equipos Windows, Linux, Mac OS X y Android.

- **Seguridad en todos los vectores de ataque:** navegación, correo, sistema de ficheros y control de los dispositivos conectados al PC.
- **Seguridad contra amenazas desconocidas:** tecnología anti-exploit, evita que el malware aproveche fallos desconocidos en el software para infectar equipos.
- **Análisis de comportamiento:** detección del malware desconocido.
- Seguridad en todas las plataformas: Windows, Linux, Mac OS X, Android y motores virtuales (Wmware, Virtual PC, MS Hyper-V, Citrix).

- **Fácil de Manejar**

Fácil gestión, sin mantenimientos ni necesidad de infraestructuras en la red del cliente.

- **Fácil de mantener:** no requiere infraestructura específica para alojar la solución, permitiendo dedicar tu equipo de IT a otras tareas más productivas.
- **Fácil de proteger a usuarios remotos:** cada equipo con **Endpoint Protection / Plus** se comunica con la nube; los usuarios desplazados y delegaciones remotas se protegen de forma natural, sin instalaciones ni configuraciones VPN particulares.
- **Fácil de desplegar:** múltiples métodos de despliegue y con desinstaladores automáticos de antivirus de la competencia, que facilitan una rápida migración desde soluciones de terceros.
- **Curva de aprendizaje muy suave:** interface web de gestión intuitivo y sencillo, con las opciones más utilizadas a un solo clic.

2.3. Beneficios principales de Endpoint Protection Plus sobre Aether.

El correo electrónico y la navegación son la principal puerta de entrada del malware en las organizaciones, y adicionalmente dos de los factores que más afectan a la productividad de los trabajadores.

El correo electrónico es una herramienta productiva de carácter crítico en las empresas, y el 95% del correo electrónico corporativo está infectado o es SPAM, siendo el método de ataque más utilizado, y por tanto requiriendo estar al día en las últimas tecnologías de protección.

La navegación por su lado sufre de las amenazas más recientes, tales como los bots, el phishing y el contenido activo malicioso, que atacan a los usuarios mientras navegan por Internet, infectando las redes de las empresas.

Endpoint Protection Plus es un producto que permite gestionar la seguridad de todos los equipos de la red, sin impacto negativo en el rendimiento de los dispositivos y al menor coste de propiedad posible. A los beneficios ya aportados por **Endpoint Protection** se añaden los indicados a continuación:

- **Máxima productividad**

Monitoriza y filtra el tráfico web y el spam de forma que la empresa pueda centrarse en su negocio y olvidarse de los comportamientos improductivos de los trabajadores.

- **Monitorización y filtrado de sitios Web:** Incrementa la productividad de la empresa monitorizando la navegación e impidiendo el acceso a las categorías web que consideres peligrosas o improductivas en horario de trabajo. Compatible con cualquier navegador web.
- **No más buzones saturados:** disminuye la superficie de ataque en los servidores Exchange mediante el filtrado de contenidos, aumentando la seguridad y la productividad de los usuarios con el motor antimalware y antispam, que evita el correo basura y los mensajes maliciosos.

2.4. Características principales de la plataforma Aether

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

Endpoint Protection / Plus ha sido desarrollado para sacar partido de los servicios suministrados por la plataforma **Aether**, permitiendo focalizar todo el esfuerzo en mejorar la seguridad de sus clientes. **Aether** por su parte, se encarga de gestionar las comunicaciones con los agentes desplegados y con el administrador de la solución a través de la consola de administración, y de la presentación y tratamiento de la información recogida por **Endpoint Protection / Plus** para su posterior análisis.

El funcionamiento de **Endpoint Protection / Plus sobre Aether** es totalmente transparente para el administrador y para los usuarios de la red, como corresponde a un diseño desarrollado desde la base.

Este diseño de la solución evita la instalación de nuevos agentes o productos en los equipos del cliente. De esta forma todos los productos de Panda Security que funcionen sobre la plataforma **Aether** comparten un mismo agente en el equipo del cliente y una misma consola web de administración, facilitando la gestión de los productos y permitiendo minimizar los recursos de los equipos.

2.4.1 Principales beneficios de Aether

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

- **Plataforma de gestión Cloud**

Aether es una plataforma que reside en la nube de Panda Security, lo cual incorpora importantes ventajas de cara a su manejo, funcionalidad y accesibilidad:

- No requiere servidores de gestión que alojen la consola de administración en las instalaciones del cliente: al funcionar desde la nube, es directamente accesible por todos los equipos suscritos al servicio, desde cualquier lugar y en cualquier momento, sin importar si están dentro de la oficina o desplazados.
- El administrador de la red puede acceder a la consola de administración desde cualquier momento y en cualquier lugar, simplemente con un navegador compatible desde un equipo portátil, un equipo de sobremesa o incluso un dispositivo móvil como una tablet o un smartphone.
- Es una plataforma ofrecida en régimen de alta disponibilidad, operativa el 99'99% del tiempo. El administrador de la red queda liberado de diseñar y desplegar costosos sistemas en redundancia para alojar las herramientas de gestión.

- **Comunicación con la plataforma en tiempo real**

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

- **Multi producto y Multiplataforma**

La integración de los productos de Panda Security en una misma plataforma permite ofrecer una serie de ventajas al administrador:

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

- **Configuraciones flexibles y granulares**

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

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

- **Información completa y a medida**

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

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

2.4.2 Arquitectura de Aether

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

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

En la Figura 1 se presenta un diagrama a alto nivel de **Aether Platform**.

2.4.3 Aether en los equipos de usuario

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

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

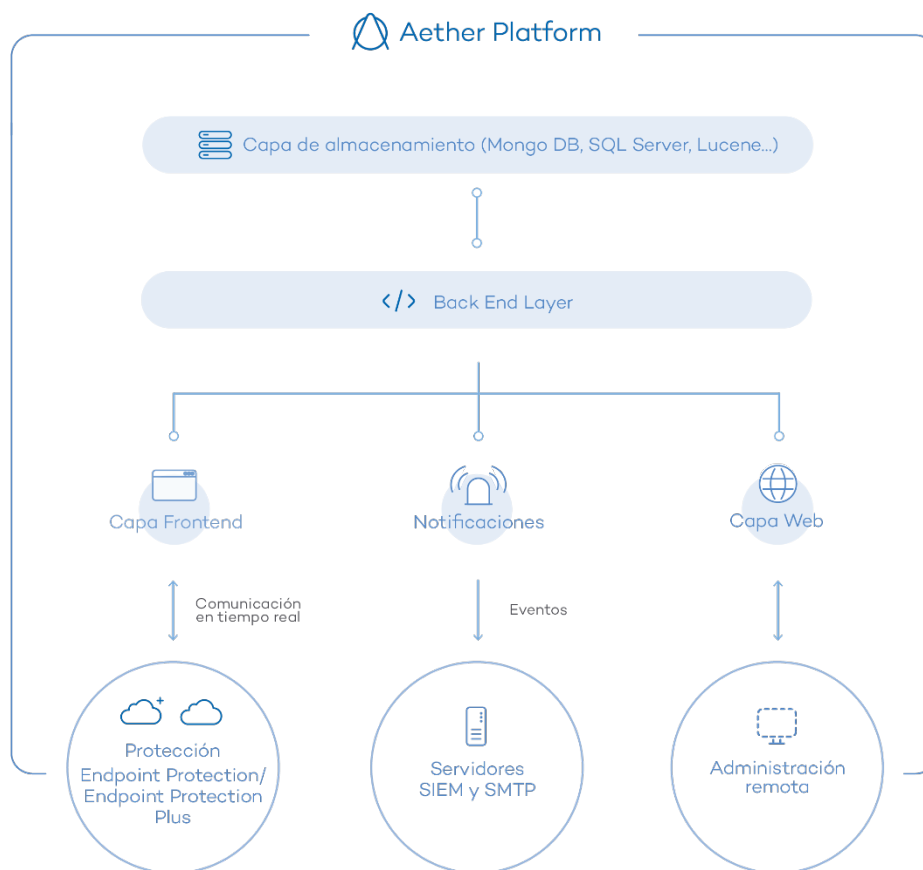


Figura 1: estructura lógica de la **plataforma Aether**

- **Agente de comunicaciones en tiempo real Panda**

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

Este módulo, además de la gestión de los procesos locales, es el encargado de recoger los cambios de configuración que el administrador haya realizado a través de la consola Web, y de aplicarlos sobre el módulo de protección **Endpoint Protection / Plus**.

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

Las configuraciones establecidas por el administrador de la red mediante la consola de administración **Endpoint Protection / Plus** son enviadas mediante la API REST al backend; éste las reenvía al Command hub generando un comando POST, el cual finalmente realizará un push de

la información a todos los dispositivos suscritos, recibiendo la configuración en el momento en ausencia de congestión en las líneas de comunicación y buen funcionamiento de elementos intermedios.

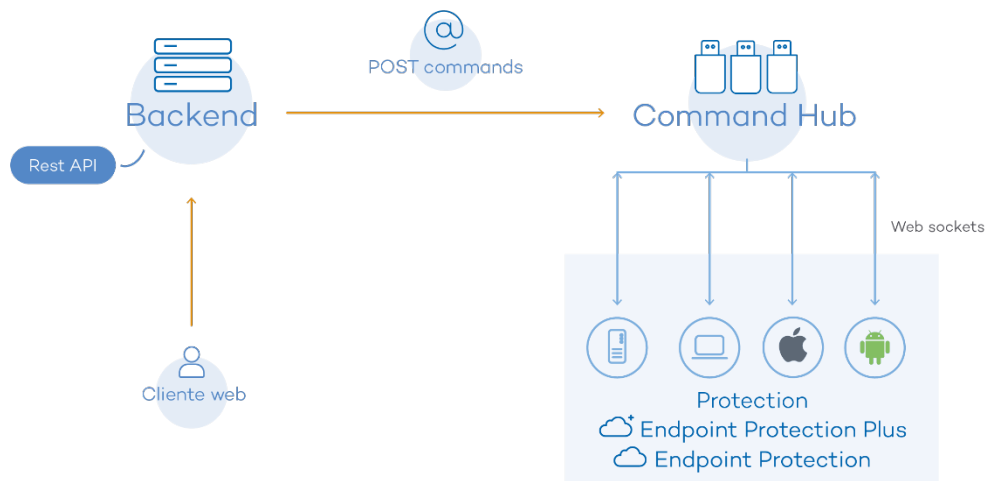


Figura 2: recorrido de los comandos introducidos con la consola de administración

2.5. Componentes principales de la arquitectura Endpoint Protection / Plus

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

En la Figura 3 se muestra el esquema general de **Endpoint Protection / Plus** y los componentes que lo forman:

Endpoint Protection / Plus está formado por los elementos mostrados a continuación:

- Servidores de Inteligencia colectiva
- Agente **Endpoint Protection / Plus** instalado en el dispositivo a proteger
- Protección **Endpoint Protection / Plus** instalado en el dispositivo a proteger
- Fichero de firmas
- Consola del administrador

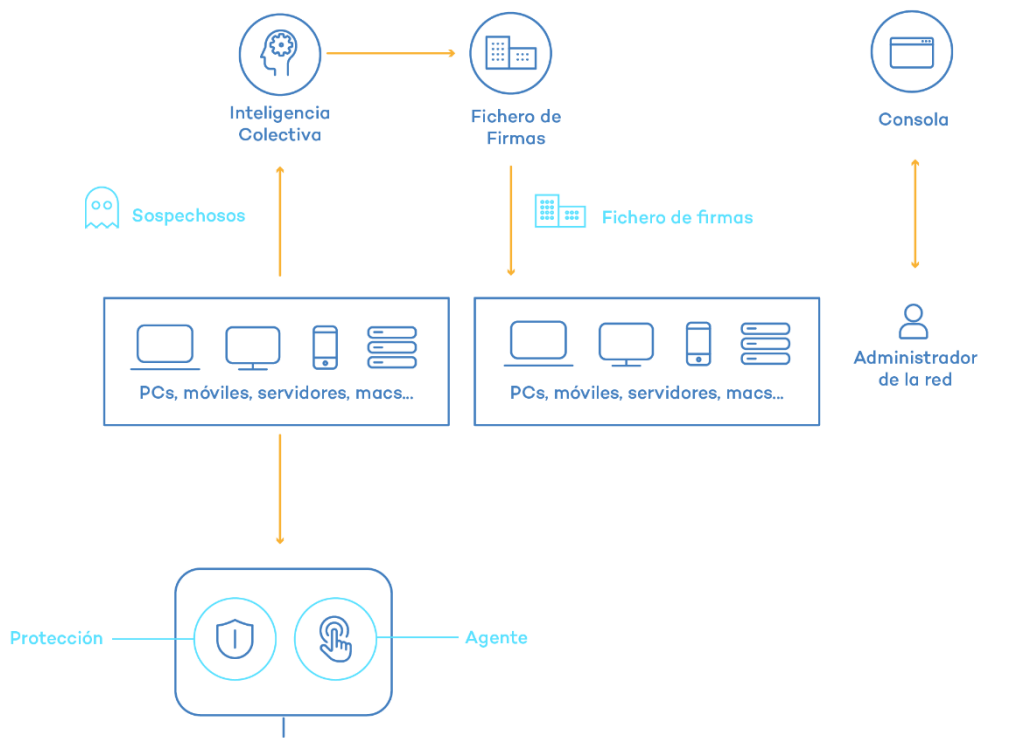


Figura 3: esquema general *Endpoint Protection / Plus*

A continuación, se introducen los distintos roles de la arquitectura mostrada.

2.5.1 Servidores de inteligencia colectiva

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

2.5.2 Servidor Web de la consola de administración

Toda la gestión de **Endpoint Protection / Plus** se realiza a través de la consola Web accesible para el administrador desde la URL <https://www.pandacloudsecurity.com/PandaLogin/>

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



Consulta el capítulo 4 La consola de administración para verificar si tu navegador es compatible con el servicio.

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

2.5.3 Equipos protegidos con Endpoint Protection / Plus

Endpoint Protection / Plus requiere de la instalación de un componente software en todas las máquinas del parque informático susceptibles de sufrir problemas de seguridad.

Este componente está formado por dos módulos: el agente de comunicaciones Panda y el módulo de la protección **Endpoint Protection / Plus**.

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



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

2.6. Perfil de usuario de Endpoint Protection / Plus sobre Aether

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

2.7. Dispositivos e idiomas soportados en Endpoint Protection / Plus sobre Aether



Para una descripción detallada de las plataformas y requisitos consulta el Apéndice I: Requisitos de Endpoint Protection / Plus .

Endpoint Protection / Plus es compatible con los siguientes sistemas operativos:

- Windows Workstation
- Windows Server
- Mac OS X
- Linux
- Tablets y móviles Android

La consola de administración se encuentra disponible en o idiomas y es compatible con los navegadores mostrados a continuación:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

Los idiomas soportados en la consola de administración son:

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

2.8. Recursos y documentación disponible

A continuación, se detalla una relación de recursos disponibles sobre **Endpoint Protection / Plus** sobre **Aether**

Guía para administradores de red

<http://resources.pandasecurity.com/enterprise/solutions/endpointprotection/ENDPOINTPROTECTI>

[ONoAP-guia-3.20.0-ES.pdf](#)

Página de producto

<http://www.pandasecurity.com/spain/enterprise/solutions/cloud-office-protection/>

Página de soporte de producto.

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

<http://www.pandasecurity.com/spain/support/cloud-office-protection-advanced.htm>

3. Tecnologías Endpoint Protection / Plus

El ciclo de protección adaptativa
Protección completa del parque informático
Detección y monitorización
Resolución y respuesta
Adaptación

3.1. Introducción

Durante los últimos años se ha producido una generalización del uso de Internet y todo tipo de dispositivos móviles. Ordenadores portátiles, servidores, smartphones, tablets y unidades de almacenamiento removible son frecuentemente utilizados en el entorno empresarial. El mundo corporativo se ha beneficiado de estos cambios, incrementando su productividad y eficiencia gracias a la automatización de procesos y a la mejora en las comunicaciones, tanto a nivel interno de la empresa como externo.

Al mismo tiempo, se han dado cambios muy importantes en la dinámica del malware: por una parte, se ha producido un crecimiento exponencial del número de elementos peligrosos que circulan por Internet; por otra, aumenta de forma constante el nivel de sofisticación de las tecnologías utilizadas y el comportamiento del malware. Como consecuencia de ello, hoy en día el malware trata de pasar desapercibido el mayor tiempo posible y tiene por meta, generalmente, la obtención de beneficios económicos.

En este panorama del malware, la nube se ha vuelto un recurso clave: la gran cantidad de las amenazas descubiertas necesitaría de enormes cantidades de recursos en los equipos a proteger, de forma que el impacto en el rendimiento de los dispositivos sería un hecho cierto.

Por esta razón, Panda Security lanza **Endpoint Protection / Plus**, un producto de seguridad para los equipos de usuario que se basa en la Inteligencia Colectiva: un sistema automático de detección y desinfección de malware que se retroalimenta con el conocimiento compartido de nuestros millones de usuarios. Gracias a la Inteligencia Colectiva, los ordenadores que forman parte de la Comunidad Panda comparten y se benefician al instante de toda la información de malware almacenada y permanentemente actualizada en la nube.

Panda Security fue la primera empresa de seguridad en contar con la tecnología, la infraestructura, el conocimiento y la experiencia para aplicar el modelo de Inteligencia Colectiva a sus productos disponibles en el mercado. De esta forma, proporciona a sus clientes máxima protección con mínimo impacto en los equipos.

Este capítulo ofrece una visión de las tecnologías implementadas en **Endpoint Protection / Plus** para gestionar la seguridad de la red de la empresa, teniendo en cuenta el nuevo panorama del malware descrito.

3.2. Recursos técnicos implementados en Endpoint Protection / Plus

El objetivo de **Endpoint Protection / Plus** es el de facilitar al departamento de IT la creación de un espacio donde poder definir y establecer las políticas de seguridad de empresa que respondan rápida y adecuadamente a los nuevos tipos de amenazas que emergen de forma constante. Este espacio es el resultado, por una parte, de la liberación de responsabilidades del equipo técnico en la compañía a la hora de decidir qué ficheros son seguros y cuales son peligrosos, y por qué

motivo. **Endpoint Protection / Plus** detecta todo tipo de amenazas de forma automática, sin necesidad de la intervención activa del administrador de la red ni de vigilar de forma constante el estado de la seguridad en la red, ahorrando tiempo y recursos al departamento de IT.

Por otra parte, el departamento de IT también recibirá un conjunto de herramientas para la visualización del estado de la seguridad y la resolución de los problemas ocasionados por el malware.

Con toda esta información y herramientas, el administrador podrá cerrar el ciclo completo de la seguridad en la empresa: monitorizar el estado del parque informático gestionado, revertir el sistema a la situación previa a las brechas de seguridad en caso de producirse, y conocer su alcance para poder implementar las medidas de contingencia apropiadas. Todo este ciclo se encaja dentro de un proceso de refinamiento contante, que resultará en un entorno informático seguro, flexible y productivo para los usuarios de la empresa.

3.2.1 Protección contra exploits

Endpoint Protection / Plus implementa tecnologías para proteger los equipos de la red frente a las amenazas que aprovechan vulnerabilidades en el software instalado. Estas vulnerabilidades son utilizadas (explotadas) para provocar comportamientos anómalos en las aplicaciones que los contienen, produciendo fallos de seguridad.

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 infecten el ordenador. La clave es utilizar las tecnologías heurísticas con gran capacidad de detección. Para ello, la nueva protección Anti-Exploit de **Endpoint Protection / Plus** analiza el comportamiento de los exploits en lugar de su morfología.

Endpoint Protection / Plus 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 / Plus** 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.

3.2.2 Protección antivirus permanente e inteligencia colectiva

La protección antivirus permanente es el módulo de seguridad tradicional que cubre los vectores de infección más utilizados por los hackers. Este módulo se alimenta tanto del archivo de identificadores publicado por Panda Security para su descarga en local como del acceso en tiempo real a la Inteligencia Colectiva.

En el contexto actual de crecimiento continuo del malware, los servicios alojados en la nube han cobrado especial importancia frente a las actualizaciones del fichero de firmas local, para gestionar con éxito la enorme cantidad de amenazas que surgen de forma constante. Por esta razón, la protección de antivirus de **Endpoint Protection / Plus** se basa fundamentalmente en la Inteligencia Colectiva, una plataforma de conocimiento en la nube que aumenta exponencialmente la capacidad de detección.

Esta plataforma 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. La protección **Endpoint Protection / Plus** instalada en los equipos realiza consultas a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos.

Cuando un nuevo ejemplar de malware es detectado en el equipo de un miembro de la comunidad de usuarios, **Endpoint Protection / Plus** se encarga de enviar la información necesaria a los servidores de Inteligencia Colectiva alojados en la nube, de forma 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.

Endpoint Protection / Plus se sirve de la Inteligencia Colectiva para aumentar la capacidad de detección y evitar penalizaciones en el rendimiento del equipo del cliente. Ahora todo el conocimiento está en la nube y, gracias a **Endpoint Protection / Plus**, todos los usuarios pueden beneficiarse de ello.



Consulta el capítulo 10 y 11 (Configuración de seguridad para estaciones y servidores y Configuración de seguridad Android) para más información sobre el servicio de antivirus de Endpoint Protection / Plus en las distintas plataformas soportadas.

3.2.3 Protección contra técnicas avanzadas de ocultación y virus de macro

Al margen de la tradicional estrategia de detección que compara el payload del fichero objeto de estudio con el contenido en el fichero de firmas, **Endpoint Protection / Plus** implementa varios motores de detección que permiten analizar el comportamiento de los procesos de forma local.

De esta manera se detectan comportamientos extraños en los principales motores de scripting (Visual basic Script, Javascript y Powershell) incorporados en todos los sistemas Windows actuales y utilizados como extensión de la línea de comandos. También se detectan macros maliciosas embebidas en ficheros ofimáticos como Word, Excel, PowerPoint etc.

También son detectadas las últimas técnicas de ejecución de malware sin fichero (los llamados FileLess Malware) que inyectan el payload del virus directamente en el proceso utilizado para la explotación de la vulnerabilidad. En estos casos, al no escribir ningún fichero en el disco duro se

reducen significativamente las probabilidades de detección en las soluciones de seguridad tradicionales.

Como complemento se incorporan además los tradicionales motores heurísticos y de detección de ficheros maliciosos por características estáticas.

3.2.4 Protección del correo y la Web

Endpoint Protection / Plus se aleja del tradicional enfoque de seguridad basado en plugins que añaden la funcionalidad de protección a determinados clientes de correo o navegadores. En su lugar, el funcionamiento de la protección consiste en una interceptación a bajo nivel de todas las comunicaciones que usan protocolos comunes como HTTP, HTTPS o POP3. De esta manera se ofrece una protección homogénea y permanente para todas las aplicaciones de correo y Web pasadas presentes y futuras, sin necesidad de configuraciones específicas ni de actualizaciones según los proveedores de los programas de correo y navegación vayan publicando nuevas versiones incompatibles con plugins anteriores.

3.2.5 Protección con cortafuegos y sistema de detección de intrusos (IDS)

Endpoint Protection / Plus ofrece tres herramientas básicas a la hora de filtrar el tráfico de red que recibe o envía el equipo protegido:

- **Protección mediante reglas de sistema:** se trata de reglas que describen las características de una comunicación entre dos equipos: puertos, IPs, protocolos etc. con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas establecidas.
- **Protección de programas:** establece un conjunto de reglas que permitan o denieguen la comunicación a determinados programas instalados en el equipo de usuario.
- **Sistema de detección de intrusos:** permite detectar patrones de tráfico malformado que afecten a la seguridad o al rendimiento del equipo protegido, rechazando dicho tráfico.

3.2.6 Control de dispositivos

Dispositivos de uso común como las llaves USB, las unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles también pueden constituir una vía de infección para los equipos.

Endpoint Protection / Plus permite determinar cuál será el comportamiento del dispositivo en los equipos protegidos, bloqueando su acceso o permitiendo su uso de forma parcial (solo lectura) o completa.

3.2.7 Filtrado de Spam, Virus y contenidos en servidores Exchange



Característica solo disponible en Endpoint Protection Plus.

Endpoint Protection Plus es capaz de analizar los servidores Exchange en busca de virus, herramientas de hacking y programas potencialmente no deseados, con destino los buzones de los usuarios de la red.

Por otra parte, la eliminación del correo basura -spam- es una labor que requiere dedicar mucho tiempo. El spam no solo supone un peligro de estafa, sino que además es una enorme pérdida de tiempo que el usuario no tiene por qué asumir. Para solucionar esta situación **Endpoint Protection Plus** implementa una protección anti-spam para servidores Exchange. De esta forma se consigue optimizar el tiempo de trabajo de los usuarios y aumentar la seguridad de los equipos de la red.

Endpoint Protection Plus protege los servidores de correo Exchange mediante dos tecnologías distintas:

- **Protección de buzones**

Se utiliza en los servidores Exchange con el rol de Mailbox, y permite analizar las carpetas / buzones en background o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones admite la manipulación de los diferentes elementos del cuerpo del mensaje analizado, lo que permite sustituir los elementos peligrosos encontrados por otros seguros, introducir únicamente los elementos peligrosos en cuarentena etc.

Además, la protección de buzones permite el análisis de las carpetas de usuario del servidor Exchange en segundo plano, aprovechando los tiempos de menor carga del servidor. Este análisis se realiza de forma inteligente evitando volver a analizar los mensajes ya examinados. El escenario típico habitual es el de tener que analizar los buzones y la cuarentena con cada nuevo archivo de identificadores publicado.

- **Protección de transporte**

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Mailbox, y permite analizar el tráfico que es atravesado por el servidor Exchange.

En la protección de transporte no se permite la manipulación del cuerpo de los mensajes. De esta forma el cuerpo de un mensaje peligroso es tratado como un solo bloque y las acciones que **Endpoint Protection / Plus** permite ejecutar aplican al mensaje por completo: borrar el mensaje, meterlo en cuarentena, dejar pasar sin modificar etc.

3.2.8 Control de acceso a páginas Web



Característica solo disponible en Endpoint Protection Plus.

Con esta protección, el administrador de la red podrá restringir el acceso a determinadas categorías Web, y configurar URLs a las que autorizará o restringirá el acceso. Esto contribuirá a la optimización del ancho de banda de la red y a la productividad del negocio.

Las páginas Web se agrupan en 64 categorías. Tan solo es necesario seleccionar aquellas categorías a denegar el acceso, pudiendo modificar las categorías seleccionadas posteriormente siempre que sea necesario.

Además, **Endpoint Protection / Plus** permite definir una configuración de horarios, con la que se podrá 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.

3.2.9 Visibilidad del estado de la red

Endpoint Protection / Plus ofrece una serie de recursos para poder valorar el estado de la seguridad de la red en un solo vistazo, a través de un panel de control (dashboard) formado por diferentes widgets y de los informes.

En los paneles de **Endpoint Protection / Plus** se puede encontrar información clave sobre las detecciones realizadas en los diferentes vectores de infección protegidos.



Consulta el capítulo 14 Visibilidad del malware y del parque informático para más información sobre Visibilidad y monitorización de equipos y procesos.

3.2.10 Técnicas de desinfección

En caso de producirse una brecha de seguridad, el administrador tiene que ser capaz de revertir de forma rápida el estado de los equipos afectados previo a la infección.

Para ello **Endpoint Protection / Plus** cuenta con herramientas de desinfección avanzadas junto a la cuarentena, que almacena los elementos sospechosos o eliminados.



Consulta el capítulo 16 Herramientas de resolución para más información.

3.3. La Fase de Adaptación

Una vez solucionados las incidencias de seguridad con las herramientas de Resolución, el administrador deberá de ajustar la política de seguridad de la empresa para que situaciones equivalentes no vuelvan a producirse en un futuro.

Desde el punto de vista del equipo, **Endpoint Protection / Plus** puede reforzar la seguridad de múltiples maneras:

- **Cambiando de la configuración de la protección antivirus**

Programar un mayor número de análisis o activar la protección de vectores de infección como Web o correo ayudarán a proteger los equipos que reciban malware por estas dos vías.

- **Limitando la navegación Web a categorías concretas**



Característica solo disponible en Endpoint Protection Plus.

Reconfigurar las categorías accesibles a la navegación limita el acceso a páginas de origen dudoso, cargadas de publicidad y propensas a ofrecer descargas en apariencia inocentes (descarga de libros, programas piratas etc) pero que pueden infectar de malware los equipos.

- **Filtrando la llegada de correo con Phishing o Spam**



Característica solo disponible en Endpoint Protection Plus.

Un vector muy utilizado para ataques de tipo phishing es el correo. Reforzando la configuración del filtrado de contenidos y del filtro antiSpam se limita la cantidad de correo no solicitado que llega a los buzones de los usuarios, reduciendo la superficie de ataque.

- **Bloqueando parcial o totalmente pen drives y otros dispositivos externos**

Otro de los vectores de infección más típicos son las memorias y los módems USB que los usuarios se traen de casa. Limitando o bloqueando completamente su uso evitará la infección por estas vías.

- **Limitando con el Firewall y el Sistema de detección de intrusos (IDS) la comunicación de los programas instalados**

El firewall es una herramienta orientada a reducir la superficie de exposición de los equipos, evitando la comunicación de programas que, de por sí, no son malware pero que pueden suponer una ventana abierta a la entrada del mismo. Si se ha detectado una intrusión de malware por programas de tipo chat o P2P, una correcta configuración de las reglas del firewall evitará la comunicación de estos programas con el exterior.

El firewall y el IDS también pueden ser utilizados para minimizar la propagación del malware una vez ha infectado al primero de los equipos de la red.

4. La consola de administración

Características generales de la consola
Estructura general de la consola web de administración

4.1. Introducción

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

- **Única herramienta para la gestión completa de la seguridad.**

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

- **Gestión centralizada de la seguridad para todas las oficinas y usuarios desplazados**

La consola Web está alojada en la nube de forma que no es necesario instalar nueva infraestructura en las oficinas del cliente ni configuraciones de VPNs o redirecciones de puertos en los routers corporativos. Tampoco serán necesarias inversiones en hardware, licencias de sistemas operativos o bases de datos, ni gestión de mantenimientos / garantías para asegurar el funcionamiento del servicio.

- **Gestión de la seguridad desde cualquier lugar y en cualquier momento**

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

4.1.1 Requisitos de la consola Web

La consola Web es accesible a través de la siguiente URL:

<https://www.pandacloudsecurity.com/PandaLogin/>

Para acceder a la consola Web de administración es necesario cumplir con el siguiente listado de requisitos:

- Contar con unas credenciales validas (usuario y contraseña).



Consulta el Apéndice II: Creación y gestión de cuentas Panda para más información sobre cómo crear una Cuenta Panda de acceso a la consola Web.

- Un navegador compatible certificado.
- Conexión a internet y comunicación por el puerto 443.

4.1.2 Federación con IDP

Endpoint Protection / Plus delega la gestión de las credenciales en un Proveedor de Identidades (Identity Provider, IDP), una aplicación centralizada responsable de gestionar las identidades de los usuarios.

De esta forma con una única Cuenta Panda el administrador de la red tendrá acceso a todos los productos contratados con Panda Security de forma segura y sencilla.

4.2. Características generales de la consola

Endpoint Protection / Plus utiliza la consola de administración para interactuar con el servicio, aplicando los siguientes beneficios:

- **Diseño responsive / adaptativo:** la consola web se adapta al dispositivo utilizado para el acceso y a su tamaño, ocultando y recolocando dinámicamente elementos.
- **Sin recarga de páginas:** se utiliza tecnología Ajax para navegar y mostrar los listados de manera que se evitan las recargas de páginas completas.
- **Flexible:** se ofrece una interface fácilmente adaptable a las necesidades del administrador, permitiendo almacenar los ajustes realizados para los posteriores accesos.
- **Homogénea:** los recursos implementados en la consola de administración siguen unos patrones de usabilidad bien definidos que permiten minimizar la curva de aprendizaje del administrador.
- **Exportación de listados:** todos los listados son exportables en formato csv con campos extendidos para su posterior consulta.

4.3. Estructura general de la consola Web de administración

La consola Web de administración cuenta con recursos que facilitan al administrador una experiencia de gestión homogénea y coherente, tanto en la administración de la seguridad de la red como en las tareas de resolución.

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

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

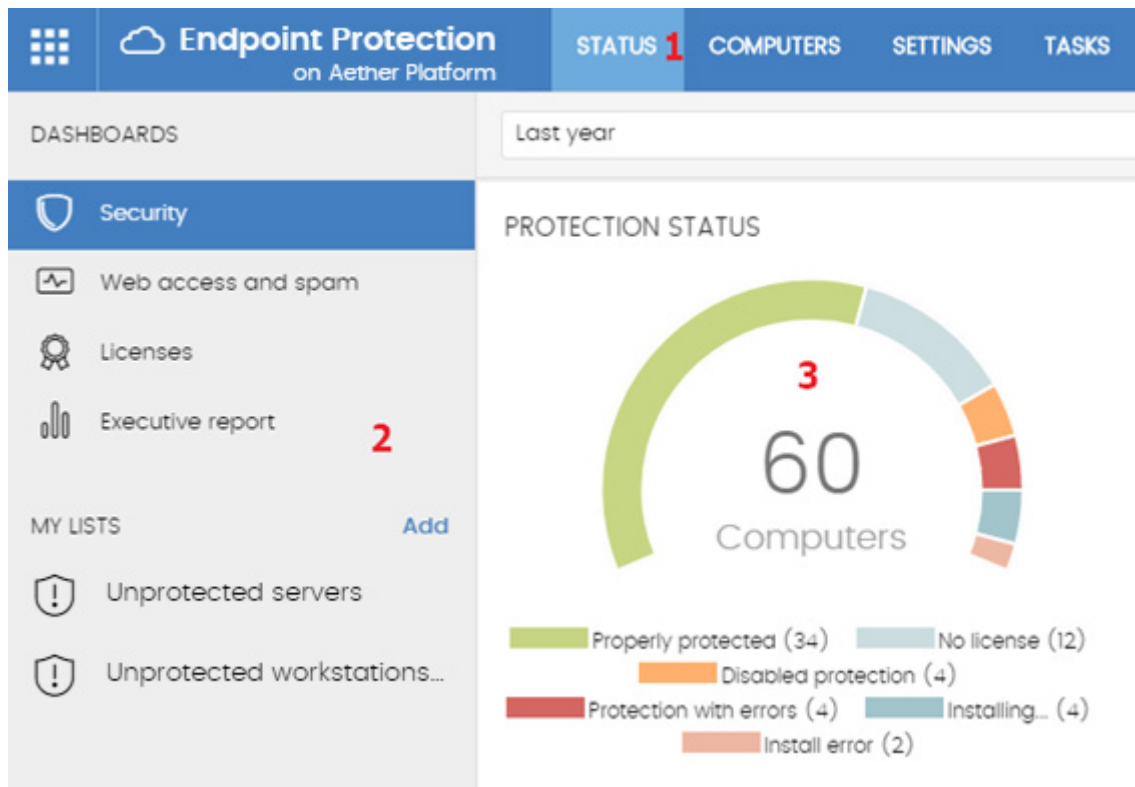



Figura 4: vista general de la consola de administración *Endpoint Protection / Plus*

4.3.1 Menú superior (1)

Muestra las 7 zonas de la consola en las que la consola de administración divide toda su funcionalidad:

- Botón Panda Cloud
- Estado
- Equipos
- Configuración
- Tareas
- Configuración general
- Cuenta de usuario

Botón Panda Cloud

Haz clic en el botón  situado en el lateral izquierdo del menú superior. Desde aquí puedes elegir el producto de seguridad contratado para gestionarlo, así como modificar la configuración de tu Cuenta Panda.

Menú superior Estado

El menú superior **Estado** muestra el panel de control de la consola, desde la cual el administrador tiene acceso de un vistazo a toda la información de seguridad, tanto en forma gráfica mediante widgets como mediante los listados situados en el menú lateral.



Consulta el capítulo 7 Gestión de equipos y dispositivos para obtener más información.

Menú superior Equipos

El menú superior **Equipos** ofrece las herramientas básicas para que el administrador de la red pueda definir la estructura de los equipos de la red que mejor se ajuste a la configuración de la seguridad del parque informático.

Elegir una correcta estructura de dispositivos es fundamental a la hora de asignar configuradores de seguridad de forma fácil y sencilla.



Consulta el capítulo 8 Gestión de configuraciones para obtener más información.

Menú superior Configuración

Permite crear configuraciones de varios tipos:

- **Usuarios:** permite gestionar los usuarios que podrán acceder a la consola de administración, así como las acciones que podrá realizar dentro de la misma.



Consulta el capítulo 19 Control y supervisión de la consola de administración para obtener más información.

- **Ajustes por equipos:** permite definir las actualizaciones del software Endpoint Protection / Plus y su contraseña de administración.
- **Proxy e idioma:** permite crear la configuración de salida a internet y de idioma del software instalado en los equipos de la red.
- **Estaciones y servidores:** permite crear los perfiles de configuraciones que serán asignados a los dispositivos en el Menú superior **Equipos**.



Consulta el capítulo 10 Gestión de configuraciones para estaciones y servidores para obtener más información.

- **Dispositivos Android:** permite crear los perfiles de configuraciones que serán asignados a tablets y teléfonos móviles Android en el Menú Superior **Equipos**.



Consulta el capítulo 11 Configuración de seguridad Android para obtener más información.

Menú superior Tareas

Permite la gestión de tareas de seguridad programadas para su ejecución en los intervalos de tiempo designados por el administrador.



Consulta el capítulo 13 Tareas para obtener más información.

Menú superior Configuración General

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

- **Guía avanzada de administración**
- **Soporte técnico:** lanza el navegador con la dirección de la web de soporte técnico de Panda Security para **Endpoint Protection / Plus sobre Aether**.
- **Buzón de sugerencias:** lanza la herramienta de correo local instalada en equipo para mandar un mensaje de correo al departamento de soporte técnico de Panda Security.
- **Acuerdo de licencia:** Muestra el EULA (End User License Agreement).
- **Idioma:** permite seleccionar el idioma en que se mostrara la consola de administración.
- **Acerca de...:** muestra la versión de los diferentes elementos de **Endpoint Protection / Plus**.
 - **Versión:** versión del producto.
 - **Versión de la protección:** Versión interna del módulo de protección instalado en los equipos.
 - **Versión del agente:** Versión interna del módulo de comunicaciones instalado en los equipos.

Menú superior Cuenta de usuario

Muestra un menú desplegable con las siguientes entradas de configuración:

- **Configurar mi perfil:** permite cambiar la información de la cuenta principal del producto.
- **Cambiar de cuenta:** lista las cuentas accesibles por el administrador y permite seleccionar una nueva cuenta para operar con la consola.
- **Cerrar sesión:** hace logout de la consola de administración y devuelve al usuario a la pantalla de IdP.

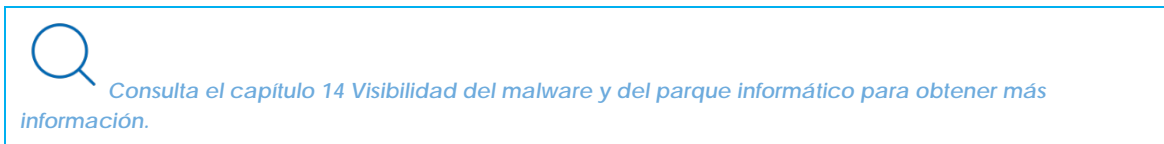
4.3.2 Menú lateral (2)

El menú lateral permite la selección de las diferentes subzonas dentro de la zona elegida, actuando como un selector de segundo nivel con respecto al menú superior.

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

4.3.3 Widgets (3)

Los widgets son representaciones gráficas de datos que permiten interpretar de un vistazo la información recogida relativa a un determinado aspecto de la seguridad de la red. Los widgets son accesibles, mostrando pequeños tooltips al pasar el rato por sus zonas activas y permiten ampliar la información al hacer clic, mostrando desgloses completos de la información mostrada.



4.3.4 Menú de pestañas superior

En las zonas de la consola más complejas se utiliza un selector de tercer nivel en forma de pestañas que permite mostrar la información de forma ordenada.

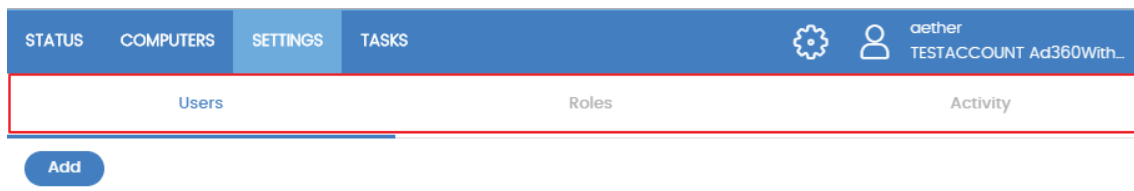


Figura 5: menú de pestañas

4.3.5 Herramientas de filtrado y búsqueda

Las herramientas de filtrado y búsqueda permiten mostrar los subconjuntos de información que interesan al administrador.

Algunas herramientas de filtrado son generales y aplican a toda la zona de la consola mostrada, como por ejemplo en el Menú superior **Estado** o Menú superior **Equipos**.

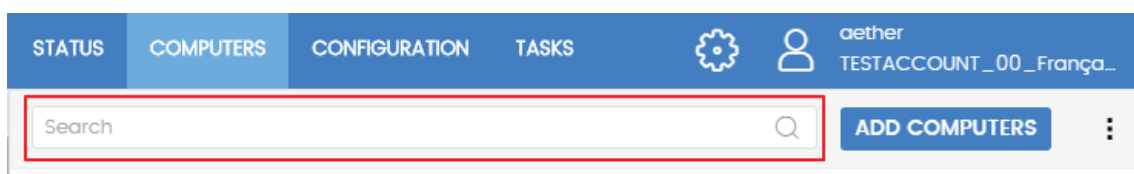


Figura 6: herramienta de búsqueda

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

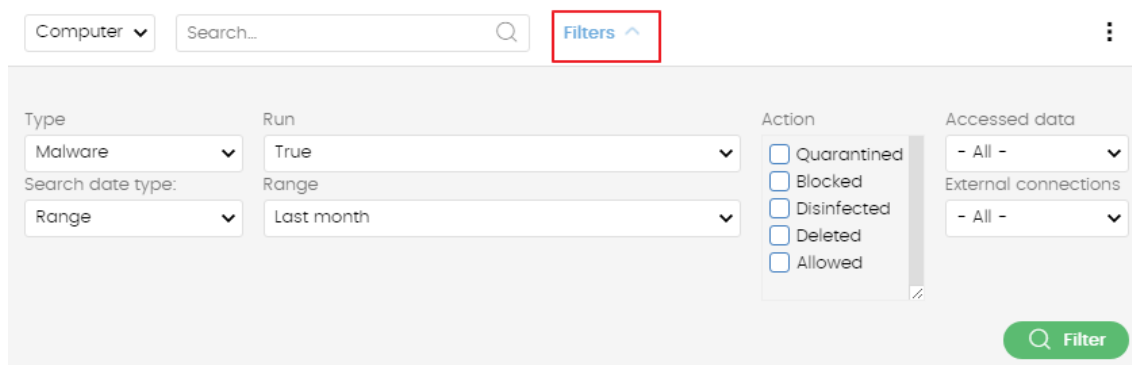


Figura 7: sistema de filtrado de información en listados

4.3.6 Botón de volver

Para facilitar la navegación de la consola a través de los diferentes niveles de presentación se incorpora un botón **Volver** que lleva a la página anterior. La etiqueta del botón varía si la página anterior era una zona distinta a la actual. En este caso se mostrará la zona abandonada en vez de **Volver**.

4.3.7 Elementos de configuración (8)

La consola Web **Endpoint Protection / Plus** utiliza controles estándar para introducir configuraciones, como son:

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

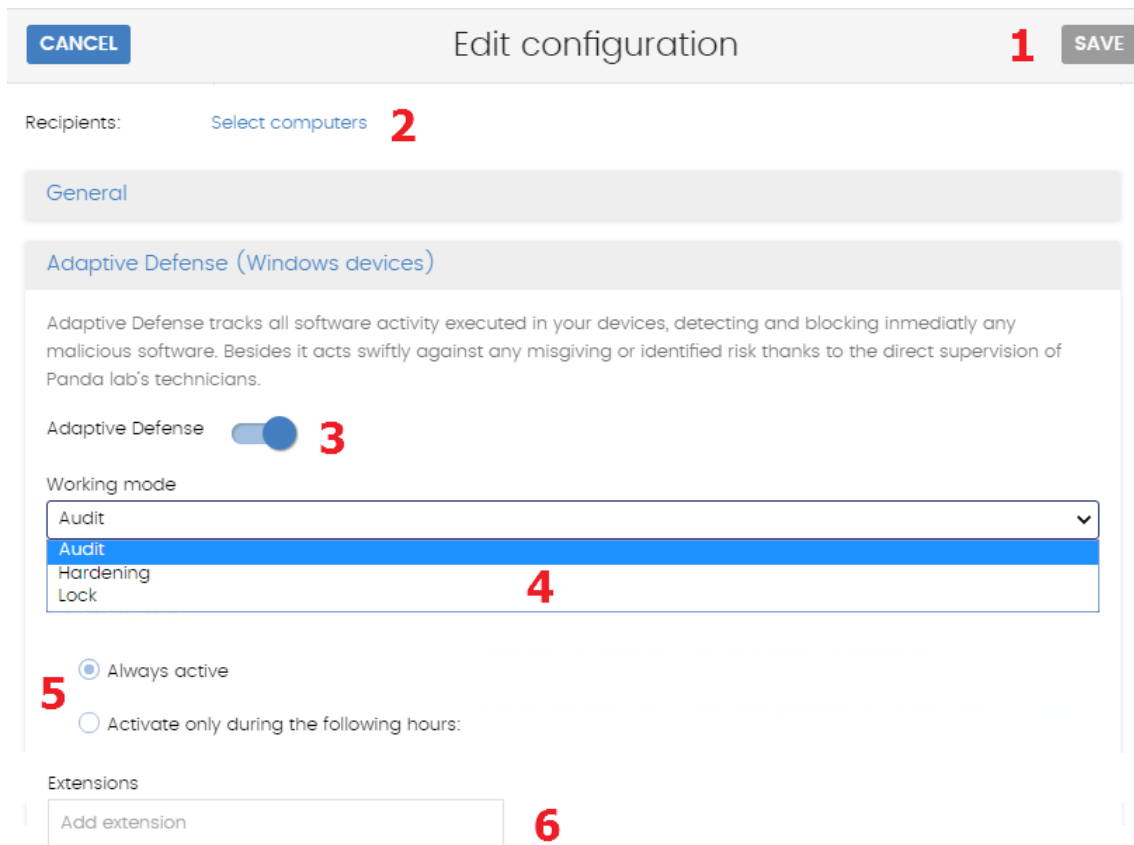



Figura 8: controles para el manejo de la consola de administración

4.3.8 Menús de contexto

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

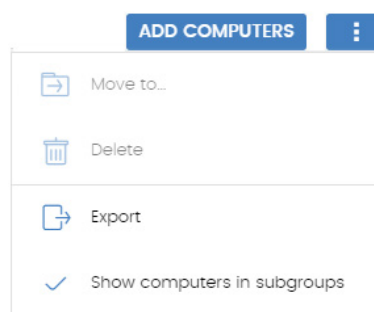


Figura 9: menús de contexto

4.3.9 Listados

Los listados presentan la información en forma de tabla y están acompañados de un conjunto de herramientas comunes que facilitan su navegación.

Executed malware **1** **3**

2 Filters ^

Type: **4** Malware

Date search type: Range Range: Last month

Search: Host Name Run: True

Action: Moved quarantine, Blocked, Cleaned, Deleted, Allowed

Accessed data: - All - External connections: - All -

5 FILTER

Host Name	Threat	File path	⚡	📄	🌐	Action	Date
Machine_Cus tomer_1_id38	Malware Name 2	Malware Path Sample 2	●	●	○	Deleted	3/10/2017 1:00:00 AM
Machine_Cus tomer_1_id38	Malware Name 14	Malware Path Sample 14	●	●	○	Allowed	3/15/2017 12:18:00 AM
Machine_Cus tomer_1_id38	Malware Name 8	Malware Path Sample 8	●	●	○	Cleaned	3/14/2017 9:24:00 PM
Machine_Cus tomer_1_id38	Malware Name 10	Malware Path Sample 10	●	●	○	Blocked	3/14/2017 10:22:00 PM
Machine_Cus tomer_1_id38	Malware Name 4	Malware Path Sample 4	●	●	○	Blocked	3/14/2017 7:28:00 PM

6 **7** 10 entries **8** 1 to 10 of 2140 **9** **10** **11** **12** **13**

Figura 10: elementos de las pantallas de listados

- **Nombre del listado (1):** permite identificar el tipo de datos que se muestran en el listado.
- **Link de herramientas de filtrado y búsqueda (2):** al hacer clic se despliega un panel con los controles de búsqueda y filtrado.
- **Menú de contexto (3):** muestra un menú desplegable con las opciones de exportación.
- **Bloque de controles de filtrado y búsqueda (4):** permiten refinar los datos mostrados en el listado.
- **Criterio de ordenación (5):** haciendo clic en el nombre de las columnas se permite la ordenación de la información mostrada, tomando como referente esa columna. Haciendo clic varias veces en el nombre de la columna se cambia el sentido de la ordenación (ascendente o descendente). El sentido de ordenación se muestra mediante una fecha ascendente ↑ o descendente ↓.
- **Paginación (6):** en el pie de la página se incluyen una serie de controles que permiten navegar la información mostrada.
 - Selector del número de filas mostradas por página **(7)**
 - Intervalo de registros mostrados del total disponible **(8)**
 - Retroceso a la primera página **(9)**
 - Retroceso a la página anterior a la actual **(10)**
 - Acceso directo a las 5 páginas posteriores a la visualizada **(11)**
 - Avance a la siguiente página **(12)**
 - Avance a la última página **(13)**

5. Licencias

- Gestión de licencias
- Definiciones y conceptos clave
- Resumen del estado de las licencias contratadas
- Licencias contratadas
- Licencias caducadas
- Licencias de prueba (trial)
- Búsqueda de equipos según el estado de licencia

5.1. Introducción

Para beneficiarse de los servicios de seguridad avanzada de **Endpoint Protection / Plus** es necesario adquirir y asignar licencias del producto a los diferentes equipos de la red a proteger, de acuerdo con las necesidades de seguridad en la empresa.

En este capítulo se tratará la gestión de licencias de **Endpoint Protection / Plus**, cómo asignarlas a los equipos de la red, liberarlas y comprobar su estado.

Para la puesta en marcha del servicio **Endpoint Protection / Plus** es necesaria la contratación de licencias en un número igual o superior a los equipos que se quieran proteger. Una licencia de **Endpoint Protection / Plus** es asignada a un único equipo (estación de trabajo, dispositivo móvil o servidor).



Para contratar y/o renovar licencias consulta con tu partner asignado.

5.2. Definiciones y conceptos clave para la gestión de licencias

A continuación, se describen los términos necesarios para interpretar las gráficas y la información suministrada por **Endpoint Protection / Plus** que refleja el estado de las licencias de los equipos.

5.2.1 Mantenimientos

Las licencias contratadas se agrupan en mantenimientos. Un mantenimiento es un conjunto de licencias con las características comunes, mostradas a continuación:

- **Tipo de Producto:** Endpoint Protection / Plus, Endpoint Protection / Plus with Advanced Reporting Tools.
- **Licencias contratadas:** número de licencias contratadas en el mantenimiento
- **Tipo de licencias:** *NFR*, Trial, Comercial, Suscripción.
- **Caducidad:** Fecha en la que las licencias caducan y los equipos dejarán de estar protegidos.

5.2.2 Estado de los equipos

Desde el punto de vista de las licencias, **Endpoint Protection / Plus** distingue tres estados en los equipos de la red:

- **Equipos con licencia:** el equipo tiene una licencia válida en uso.
- **Equipos sin licencia:** el equipo no tiene una licencia en uso, pero es candidato a tenerla.
- **Excluidos:** equipos a los que se ha decidido no aplicarles la licencia. Estos equipos no serán protegidos por **Endpoint Protection / Plus**, aunque se mostrarán en la consola y se podrá

utilizar algunas funcionalidades de gestión. Para excluir un equipo es necesario liberar su licencia de forma manual.



Es importante distinguir entre el número de equipos sin licencia asignada (candidatos a tenerla en caso de haber licencias sin asignar) y el número de equipos excluidos (sin posibilidad de tener una licencia asignada, aunque haya licencias disponibles).

5.2.3 Estado de las licencias y grupos

Las licencias contratadas pueden tener dos estados:

- **Asignada:** es una licencia usada por un equipo de la red.
- **Sin asignar:** es una licencia que no está siendo usada por ningún equipo de la red.

Las licencias se agrupan por su estado en dos grupos:

- **Grupo de licencias usadas:** formado por todas las licencias asignadas a equipos.
- **Grupo de licencias sin usar:** formado por las licencias sin asignar.

5.2.4 Tipos de licencias

- **Licencias comerciales:** son las licencias estándar de **Endpoint Protection / Plus**. Un equipo con una licencia comercial asignada tiene acceso a toda la funcionalidad del producto licenciado.
- **Licencias de prueba (Trial):** son licencias gratuitas de prueba, válidas por un periodo limitado de 30 días. Un equipo con una licencia de prueba asignada tiene acceso de prueba a toda la funcionalidad del producto.
- **Licencias NFR:** licencias *Not For Resale*, destinadas a personal interno y partners de Panda Security. No está permitida su venta ni uso por personal o partners ajenos a Panda Security.
- **Licencias de tipo suscripción:** licencias que no tienen fecha de caducidad. El servicio es de tipo "pago por uso".

5.2.5 Asignación de licencias

La asignación de licencias se puede realizar de dos maneras: automática o manualmente.

Asignación automática


Al instalar el software **Endpoint Protection / Plus** en un equipo de la red, y siempre que existan licencias sin utilizar, el sistema asignará de forma automática una licencia libre.

Asignación manual

Para asignar manualmente una licencia de **Endpoint Protection / Plus** a un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a asignar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.

- Haz clic en el equipo para mostrar la ventana de detalle.
- En la pestaña **Detalles** se muestra el apartado **Licencias**, donde se mostrará el **estado Sin**

licencias. Haciendo clic en el icono  se asignará de forma automática una licencia libre.

5.2.6 Liberación de licencias

De forma equivalente a la asignación de licencias, la liberación de licencias se puede realizar de dos maneras: automática o manual.

Liberación automática

Al desinstalar el software **Endpoint Protection / Plus** de un equipo de la red el sistema recuperará de forma automática una licencia y la devolverá al grupo de licencias sin usar.


Igualmente, al caducar un mantenimiento se desasignarán automáticamente licencias de los equipos siguiendo la lógica de licencias caducadas explicadas más adelante en este capítulo.

Liberación manual

La liberación manual de una licencia asignada previamente a un equipo lo convertirá en un equipo excluido. De esta forma, aunque existan licencias libres, estas no serán asignadas al equipo de forma automática.

Para liberar manualmente una licencia de **Endpoint Protection / Plus** de un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a liberar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar su información.
- En la pestaña **Detalles** se muestra el apartado **Licencias**, donde se mostrará el estado

Endpoint Protection / Plus. Haciendo clic en el icono  se liberará la licencia y se devolverá al grupo de licencias sin utilizar.

5.2.7 Procesos de asignación y liberación de licencias

Caso I: Equipos con licencia asignada y equipos excluidos

Por defecto, a cada nuevo equipo integrado en la plataforma Aether se le asigna una licencia de producto **Endpoint Protection / Plus** de forma automática, pasando a tomar el estado de equipo con licencia asignada. Este proceso se mantiene hasta que el número de licencias contratadas queda reducido a 0.

Los equipos que ven retirada de forma manual su licencia asignada, toman el estado de equipos excluidos, y a partir de ese momento no compiten por la asignación de una licencia de forma automática, en el caso de existir licencias sin usar.

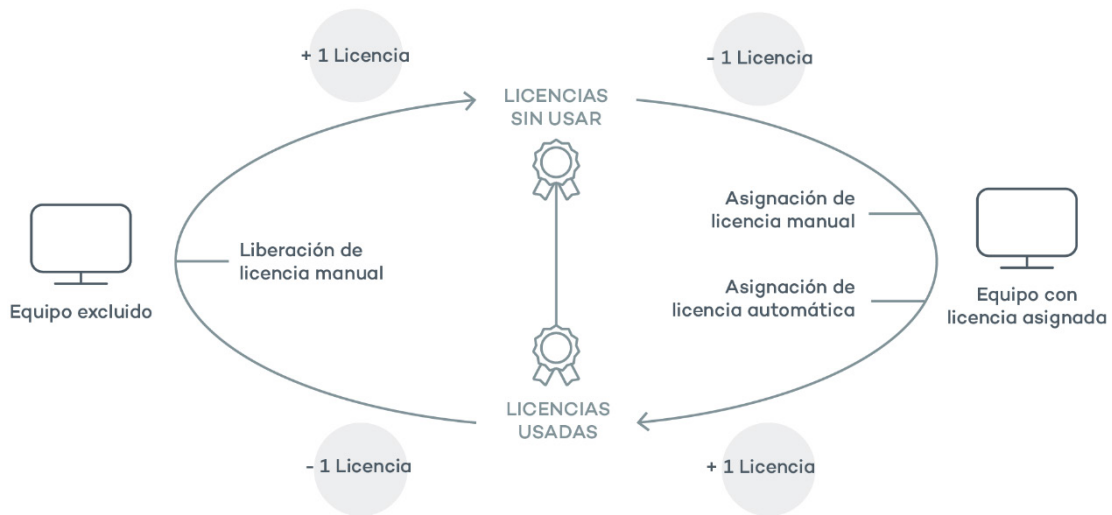


Figura 11: modificación de los grupos de licencias en equipos con licencia asignada y excluidos

Caso II: Equipos sin licencia asignada

En el momento en que nuevos equipos se incorporen a la plataforma Aether y el grupo de licencias sin usar este a 0, los equipos pasarán al estado Equipos sin licencia. En el momento en que nuevas licencias estén disponibles estos equipos tomarán una licencia de forma automática.

De la misma forma, en el momento en que una licencia asignada caduque un equipo de la red pasará al estado Sin licencia asignada, siguiendo la lógica de licencias caducadas explicadas más adelante en este capítulo.

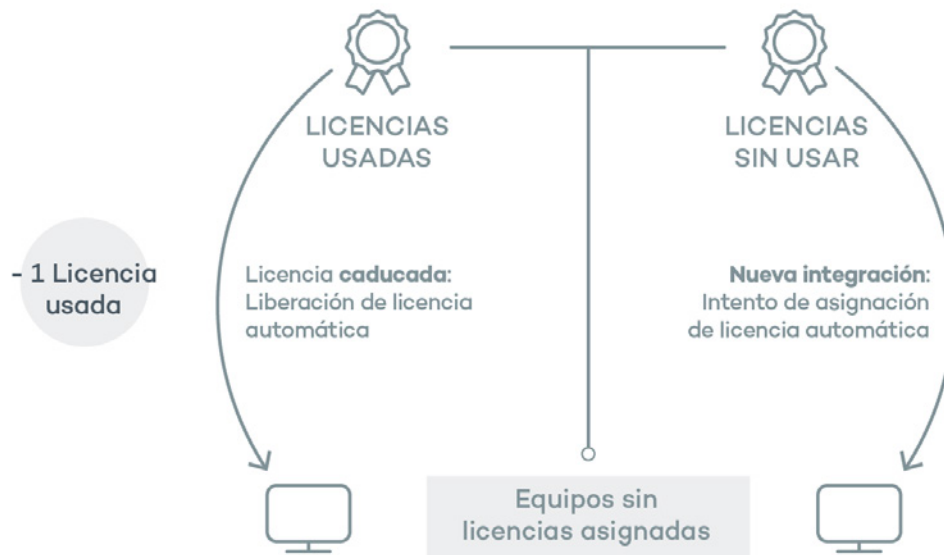


Figura 12: equipos sin licencia asignada por caducidad del mantenimiento y por grupo de licencias sin usar vacío en el momento de la integración

5.3. Licencias contratadas

Para visualizar el detalle de las licencias contratadas haz clic en el menú superior **Estado** y después en el menú lateral **Licencias**. Se mostrará una ventana con dos graficas: **Licencias contratadas** y **Caducidad de licencias**.

5.3.1 Widget

El panel representa como se distribuyen las licencias del producto contratado.

- Nombre del producto contratado (1)
- Número de licencias contratadas totales (2)
- Número de licencias asignadas (3)
- Número de licencias sin asignar (4)
- Número de equipos sin licencia (5)
- Número de equipos excluidos (6)
- Caducidad de las licencias (7)
- Caducidad por mantenimiento (8)

Nombre del producto contratado (1)

Indica el producto y los servicios contratados. Cada producto diferente se muestra de forma independiente. Si se ha contratado el mismo producto varias veces (varios mantenimientos de un mismo producto) se mostrarán de forma agrupada, indicando las diferentes fechas de caducidad de las licencias mediante un diagrama de barras horizontales.

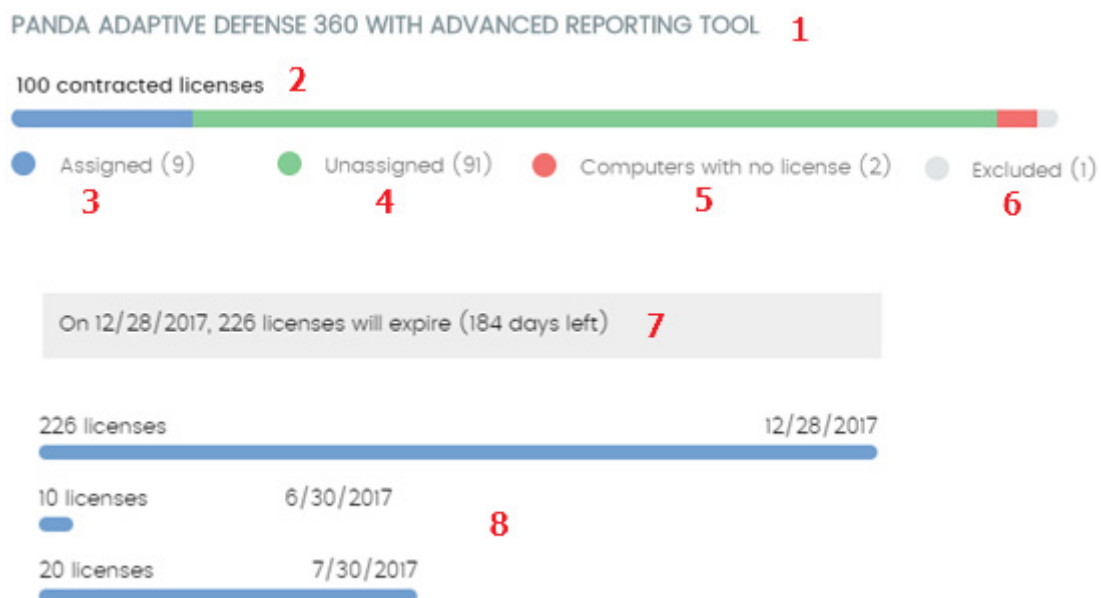


Figura 13: panel de licencias con 3 mantenimientos

Número de licencias contratadas totales (2)

Representa el número máximo de equipos que se pueden proteger, en el caso de que todas las

licencias contratadas sean asignadas.

Asignadas (3)

Es el número de equipos protegidos con una licencia asignada.

Sin asignar (4)

Es el número de licencias contratadas pero que no se han asignado a ningún equipo y por lo tanto no se están utilizando.

Equipos sin licencia (5)

Equipos no protegidos por no disponer de licencias suficientes. Se les asignará licencia de forma automática si se adquieren nuevas licencias.

Equipos excluidos (6)

Equipos sin licencia asignada que no son candidatos a tenerla.

Caducidad de las licencias (7)

Si existe un único mantenimiento contratado, todas las licencias caducarán a la vez, en la fecha indicada.

Caducidad de los mantenimientos (8)

Si un mismo producto ha sido contratado varias veces a lo largo del tiempo se mostrará una gráfica de barras horizontales con las licencias asociadas a cada contrato / mantenimiento y su fecha de caducidad independiente.

5.3.2 Listado de Licencias

Este listado muestra en detalle el estado de las licencias de los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles según su estado de licenciamiento.




Campo	Comentario	Valores
Equipo	Nombre del equipo	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Estado de licencia		 Licencia asignada  Equipo sin licencia  Equipo excluido
Ultima conexión	Fecha del ultimo envío del estado del equipo a la nube de Panda Security	Fecha

Tabla 1: campos del listado Equipos protegidos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el producto	Cadena de caracteres
Tipo de equipo		Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado	Cadena de caracteres
Plataforma	Sistema operativo instalado en el equipo	Windows Linux MacOS Android
Directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado	Booleano
Versión del agente		Cadena de caracteres
Versión de la protección		Cadena de caracteres
Fecha de arranque del sistema		Fecha
Fecha instalación	Fecha en la que el software Endpoint Protection / Plus se instaló con éxito en el equipo	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security	Fecha
Estado de licencia		Asignada No asignada Excluido
Grupo	Carpeta dentro del árbol de carpetas de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres

Campo	Comentario	Valores
Descripción		Cadena de caracteres

Tabla 2: campos del fichero exportado Licencias

Herramienta de filtrado

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo	Cadena de caracteres
Tipo de equipo		Estación Portátil Dispositivo móvil Servidor
Plataforma	Sistema operativo instalado en el equipo	Todos Windows Linux MacOS Android
Ultima conexión	Fecha del último envío del estado del equipo a la nube de Panda Security	Todos Más de 72 horas Más de 7 días Más de 30 días
Estado de licencia		Asignada Sin licencia Excluido

Tabla 3: campos de filtrado para el listado Licencias

Filtros pre establecidos desde el panel



Figura 14: zonas activas del panel licencias contratadas

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- (1) Filtra por **Estado de licencia** = Asignada
- (2) Filtra por **Estado de licencia** = No Asignada
- (3) Filtra por **Estado de licencia** = Excluido

5.4. Licencias caducadas

Excepto los mantenimientos de tipo suscripción, todos los demás tienen asignada una fecha de

caducidad, pasada la cual los equipos de la red dejarán de estar protegidos.

5.4.1 Mensajes de caducidad próxima y vencida

A los 30 días de vencer el mantenimiento, el panel Licencias contratadas mostrará un mensaje con los días que quedan para finalizar el mantenimiento y el número de licencias que se verán afectadas.

Adicionalmente, se mostrará un mensaje por cada mantenimiento caducado, avisando en el plazo de los 30 últimos días del número de licencias que ya no son funcionales.



Si todos los productos y mantenimientos están caducados se denegará el acceso a la consola de administración.

5.4.2 Lógica de liberación de licencias caducadas

Endpoint Protection / Plus no mantiene una relación de pertenencia estricta entre mantenimientos de licencias y equipos. Los equipos con licencias asignadas no pertenecen a un mantenimiento concreto u otro; en su lugar todas las licencias de todos los mantenimientos se suman en un único grupo de licencias disponibles, que se reparten posteriormente entre los equipos de la red.

En el momento en que un mantenimiento caduca, se determina el número de licencias asignadas a ese mantenimiento. Acto seguido, se ordenan los equipos de la red con licencia asignada utilizando como criterio de ordenación el campo Última conexión, que contiene la fecha en la que el equipo se conectó por última vez a la nube de Panda Security.

Los equipos candidatos a retirar su licencia de protección son aquellos no vistos en el periodo de tiempo más grande. Así, se establece un sistema de prioridades donde la mayor probabilidad de retirar una licencia se asigna a los equipos que no han sido utilizados recientemente.



La lógica de liberación de licencias caducadas afecta a todos los dispositivos compatibles con Endpoint Protection / Plus que tengan licencias asignadas.

5.5. Licencias de prueba (trial) sobre licencias comerciales

En el caso de tener licencias comerciales de **Endpoint Protection**, **Endpoint Protection / Plus** o **Fusion** sobre la plataforma Aether y obtener una trial de **Endpoint Protection / Plus**, se producirán una serie de ajustes, tanto en la consola de administración como en el software instalado en los equipos de la red:

- Se creará un mantenimiento nuevo de tipo trial, con la duración contratada para la

prueba y un número de licencias igual a la suma de las licencias disponibles previamente y las licencias contratadas para la trial.

- Los mantenimientos comerciales aparecen desactivados temporalmente mientras dure el periodo de trial, pero el ciclo de caducidad y renovación se mantiene intacto.
- Se habilitará la funcionalidad asociada al producto en pruebas sin necesidad de actualizar los equipos de la red.
- **Endpoint Protection / Plus** por defecto, se activará en todos los equipos con el modo de protección Audit. En caso de no querer activar **Endpoint Protection / Plus** en todos los puestos o en caso de querer establecer un modo de protección distinto se podrá hacer estableciendo la configuración oportuna.
- Una vez terminado el periodo de prueba el mantenimiento creado para la trial se elimina, el mantenimiento comercial se reactivará y los equipos de la red sufrirán un downgrade automático, manteniendo las configuraciones previas.

5.6. Búsqueda de equipos según el estado de la licencia asignada

Endpoint Protection / Plus incluye la categoría "licencia" en el árbol de filtros, que permite localizar los equipos de la red que tengan un determinado estado de licencia.



Consulta el capítulo 7 Gestión de equipos y dispositivos para obtener más información acerca de cómo crear un filtro en Endpoint Protection / Plus.

A continuación, se muestran las propiedades de la categoría **Licencias** para crear filtros que generen listados de equipos con información relevante sobre licencias.

- **Propiedad – Estado de la licencia:** permite establecer un filtro según el estado de la licencia.
 - **Asignada:** lista los equipos con una licencia **Endpoint Protection / Plus** asignada.
 - **Sin asignar:** lista los equipos que no tiene una licencia **Endpoint Protection / Plus** asignada.
 - **Desasignada manualmente:** el administrador de la red liberó la licencia **Endpoint Protection / Plus** previamente asignada al equipo.
 - **Desasignada automáticamente:** el sistema liberó al equipo la licencia **Endpoint Protection / Plus** asignada previamente.
- **Propiedad - Nombre de la licencia:** muestra a todos los equipos con una licencia **Endpoint Protection / Plus** asignada.
- **Propiedad – Tipo:** lista los equipos con licencia **Endpoint Protection / Plus** según su tipo.
 - **Release:** lista los equipos con licencias **Endpoint Protection / Plus** comerciales.
 - **Trial:** lista los equipos con licencias **Endpoint Protection / Plus** de prueba.

6. Instalación del software Endpoint Protection / Plus

- Visión general del despliegue de la protección
 - Requisitos de instalación
 - Instalación manual
 - Descubrimiento e instalación remota
 - Instalación con herramientas centralizadas
 - Instalación mediante generación de imágenes
 - Desinstalación de la protección

6.1. Introducción

La instalación es el proceso que distribuye **Endpoint Protection / Plus** en los equipos de la red del cliente. Todo el software necesario para activar el servicio de protección avanzado, la monitorización y la visibilidad del estado de la seguridad de la red se encuentra en el interior del paquete de instalación: no se requiere la instalación de ningún otro programa en la red del cliente.

Es importante instalar el software **Endpoint Protection / Plus** en todos los equipos de la red del cliente para evitar brechas de seguridad que puedan ser aprovechadas por los atacantes mediante malware dirigido específicamente a equipos vulnerables.

Endpoint Protection / Plus ofrece varias herramientas que facilitan la instalación de la protección, que se mostrarán a lo largo de este capítulo.

6.2. Visión general del despliegue de la protección

El proceso de instalación comprende una serie de pasos a seguir, dependiendo del estado de la red en el momento del despliegue y del número de equipos a proteger. Para desarrollar un despliegue con garantías de éxito es necesario elaborar una planificación que comprenda los puntos enumerados a continuación:

Localizar los equipos desprotegidos en la red

El administrador deberá de localizar los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con **Endpoint Protection / Plus**.

Una vez localizados, se deberá de comprobar que el número de licencias contratadas es suficiente.



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

Determinar si se cumplen los requisitos mínimos de la plataforma destino

Los requisitos mínimos de cada plataforma se describen más adelante en este capítulo, en la sección correspondiente a cada plataforma.

Determinar el procedimiento de instalación

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

- Herramienta de despliegue centralizado.
- Instalación manual utilizando la herramienta **Enviar URL por mail**.
- Programa de instalación compartido en una carpeta accesible por los usuarios de la red.
- Instalación remota desde la consola de administración.

Determinar si será necesario un reinicio para completar la instalación

Todos los servicios de protección de **Endpoint Protection / Plus** comenzarán a funcionar sin necesidad de reiniciar los equipos en el caso de equipos sin antivirus previamente instalado.



Es posible que se requiera un reinicio del cliente o se produzca un pequeño micro corte en la conexión con algunas versiones anteriores de Citrix.

Si deseas instalar **Endpoint Protection / Plus** 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 / Plus**.



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

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

- **Versiones Trials**

En la instalación de versiones de evaluación, por defecto **Endpoint Protection / Plus** no desinstalará las soluciones de seguridad de terceros. De esta forma, podrás evaluar **Endpoint Protection / Plus** comprobando cómo registra amenazas avanzadas que pasan inadvertidas para el antivirus tradicional instalado.

- **Versiones comerciales**

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



Puedes consultar una lista de los antivirus que Endpoint Protection / Plus desinstala automáticamente en el Apéndice III: Listado de desinstaladores. Si la solución a desinstalar no está en la lista, será necesaria su desinstalación manual.

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



Consulta el capítulo 10 Configuración de seguridad para estaciones y servidores si quieres diseñar una configuración de seguridad. Consulta el capítulo 8 Gestión de configuraciones para asignar configuraciones a los equipos de la red.

- **Productos de protección antivirus de Panda Security**

Si el equipo está protegido previamente con Endpoint Protection, Endpoint Protection / Plus o Panda Fusion se procederá a la desinstalación automática del agente de comunicaciones para instalar el agente Panda y, posteriormente, el sistema comprobará si es necesaria una actualización de la protección. En caso de ser necesaria se requerirá un reinicio del equipo.

En la Tabla 4 se resumen las condiciones necesarias para que se produzca un reinicio.

Producto Anterior	Endpoint Protection / Plus sobre Aether	Reinicio
Ninguno	Trial o comercial	NO
Adaptive Defense Legacy, Adaptive Defense 360 Legacy, Endpoint Protection / Plus legacy, Panda Fusion Legacy	Comercial	PROBABLE (solo si requiere actualización de la protección)
Antivirus de terceros	Trial	NO (por defecto los dos productos conviven)
Antivirus de terceros	Comercial	POSIBLE (se puede requerir un reinicio para completar la desinstalación del producto de terceros)
Sistemas Citrix	Trial o comercial	POSIBLE (en versiones anteriores)

Tabla 4: probabilidad de reinicio al cambiar de producto de protección

Establecer si es necesario la instalación en horario no laboral

Adicionalmente a la necesidad de reinicio del equipo de usuario descrita en el punto anterior, la instalación de **Endpoint Protection / Plus** provoca un micro corte de menos de 4 segundos de duración sobre las conexiones establecidas por los programas en funcionamiento. Las aplicaciones que no implementen mecanismos para detectar cortes de conexión requerirán un reinicio. Si no es posible este reinicio y además la aplicación no se comporta adecuadamente tras el micro corte, se recomienda la instalación del software **Endpoint Protection / Plus** fuera del horario laboral.

Determinar la configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, **Endpoint Protection / Plus** obliga a seleccionar por una parte el grupo de destino en la que el equipo se integrará dentro del árbol de grupos, y por otra la configuración de Proxy e idioma de forma independiente. Esta selección se realiza al generar el instalador, consulta el punto Descarga del software **Endpoint Protection / Plus** para más información.

Una vez instalado el software en el equipo, **Endpoint Protection / Plus** aplicará las configuraciones establecidas en el grupo al que pertenece el equipo y, posteriormente, si la configuración de proxy e idioma del grupo seleccionado difiere de la indicada al generar el instalador, se generará una asignación manual de forma que sea esta configuración de proxy e idioma la que prevalezca, antes que la asignada en el grupo del árbol de grupos.

6.3. Requisitos de instalación



Para una descripción completa de los requisitos por plataforma consulta el capítulo 20 Apéndice I: Requisitos de Endpoint Protection / Plus.

6.3.1 Requisitos por plataforma

Requisitos plataformas Windows

- **Estaciones de trabajo:** Windows XP SP3 y superiores, Windows Vista, Windows 7, Windows 8 y superiores, y Windows 10.
- **Servidores:** Windows 2003 SP2 y superiores, Windows 2008, Windows Small Business Server 2011 y superiores, Windows Server 2012 R2, Windows Server 2016, Windows Server Core 2008 y superiores.
- **Servidores Exchange:** 2003 al 2016.
- **Espacio para la instalación:** 650 Mbytes.

Requisitos plataformas MacOS

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

- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

Requisitos plataformas Linux

- **Sistemas operativos 64 bits:** Ubuntu 14.04 LTS y superiores, Fedora 23 y superiores. Solo 64 bits.
- **Kernel soportado:** hasta la versión 4.10 64 bits.
- **Espacio para la instalación:** 100 Mbytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

Requisitos plataformas Android

- Sistemas operativos: Android 4.0 y superiores.
- **Espacio para la instalación:** 10 Mbytes (dependiendo del modelo de dispositivo se requerirá espacio adicional).



Consulta la web de soporte para comprobar la última versión del kernel de Linux soportada por Endpoint Protection / Plus. Versiones superiores del kernel no funcionarán.

6.3.2 Requisitos de red

Endpoint Protection / Plus accede a varios recursos alojados en internet. De forma general se requiere acceso a los puertos 80 y 443. Para un listado completo de las URLs que se acceden desde los equipos con el software **Endpoint Protection / Plus** instalado consulta el Apéndice I: Requisitos de Endpoint Protection / Plus.

6.4. Descarga e instalación manual del software Endpoint Protection / Plus

6.4.1 Descarga del paquete de instalación desde la consola Web



Consulta el capítulo 7 para obtener más información sobre los diferentes tipos de grupos, el capítulo 8 para asignar configuraciones a equipos y ramas del árbol, y el capítulo 9 para crear nuevas configuraciones de Proxy e idioma.

Consiste en descargar el paquete de instalación directamente desde la consola de administración. Para ello sigue los pasos mostrados a continuación:

- En la ventana **Equipos** haz clic en el botón **Añadir equipo** y elige la plataforma a proteger: Windows, Linux, Android o MacOS (Figura 15).

- Selecciona donde será integrado el equipo en el árbol de carpetas (Figura 16):
 - Para integrar el equipo en un grupo nativo haz clic en **Añadir los equipos al siguiente grupo (1)** y selecciona el destino en el árbol de carpetas mostrado.
 - Para integrar el equipo en un grupo Directorio Activo haz clic en **Añadir los equipos en su ruta de Directorio Activo (2)**.
- Selecciona la configuración de proxy e idioma **(3)** que se aplicará al equipo a instalar. Si quieres integrar el puesto en un grupo nativo, se seleccionará de forma automática la configuración asignada a la carpeta donde residirá. Si has elegido integrarlo en un grupo Directorio Activo deberás seleccionar de forma manual la configuración de proxy e idioma de entre las mostradas en el desplegable. Si la elección automática se ajusta a tus necesidades haz clic en el desplegable y elige otra de entre las disponibles.

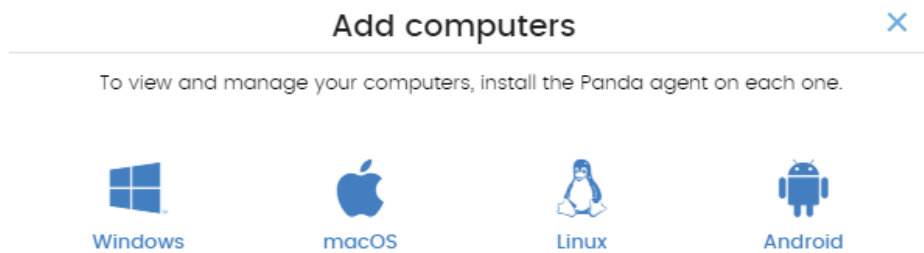


Figura 15: ventana de selección de la plataforma a descargar

- Finalmente haz clic en el botón **Descargar instalador (5)** para iniciar la descarga del paquete apropiado. El instalador contiene un asistente que guiará al usuario en los pasos necesarios para completar la instalación del software.

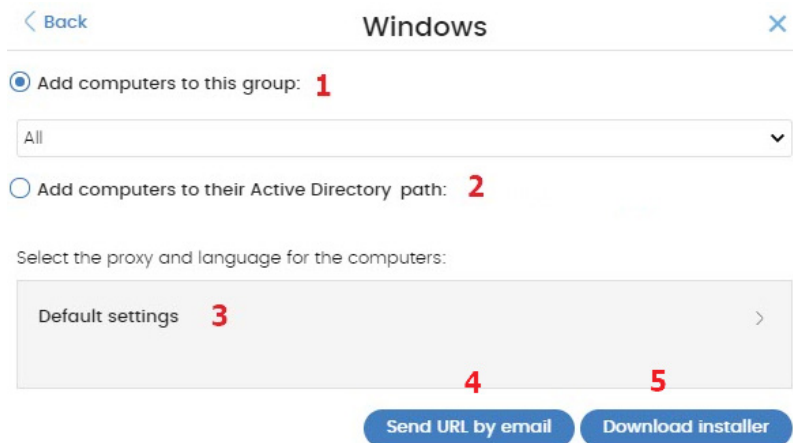


Figura 16: configuración del paquete de descarga

6.4.2 Generación de URL de descarga

Este método permite la creación de una URL de descarga que podrá ser enviada por correo a los usuarios para iniciar una instalación manual en cada equipo.

El método de distribución de la URL de descarga implementado de forma directa en **Endpoint Protection / Plus** es mediante correo, haciendo clic en el botón **Enviar por email (3)**.

De la misma manera que en la descarga desde la consola web, es necesario establecer la pertenencia del equipo a un grupo dentro del árbol de grupos y la asignación de una configuración de Proxy e idioma que prevalecerá por encima de la designada en el grupo.

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.

6.4.3 Instalación manual del software Endpoint Protection / Plus



Para la instalación del software Endpoint Protection / Plus en el equipo de usuario se requieren permisos de administrador.

Instalación en plataformas Windows

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

Instalación en plataformas Linux

Abre una terminal en la carpeta donde reside el paquete descargado y ejecuta el siguiente comando:

```
sudo sh "nombre_del_paquete"
```

Instalación en plataformas MacOS

Abre una terminal en la carpeta donde reside el paquete descargado y ejecuta el siguiente comando:

```
sudo sh "nombre_del_paquete"
```

Instalación en plataformas Android

Al hacer clic en el botón **Añadir equipo** del menú superior **Equipos** y seleccionar el icono de Android, se mostrará una ventana con la información mostrada a continuación:

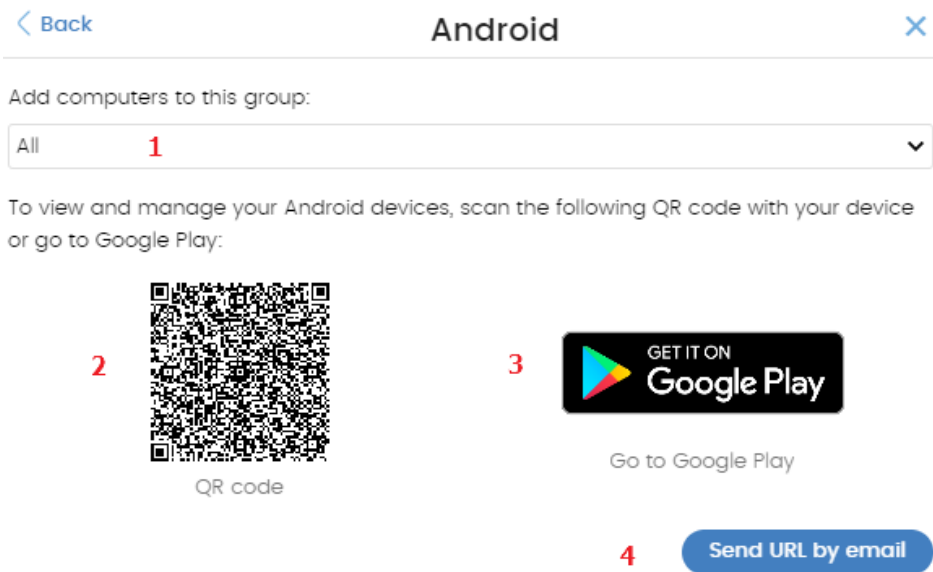


Figura 17: pantalla de selección de plataforma

- **Añadir los equipos al siguiente grupo (1):** permite especificar el grupo dentro del árbol de carpetas en el que se integrará el dispositivo una vez se haya instalado el software **Endpoint Protection / Plus**.
- **Código QR (2):** código QR que contiene el link para descargar el software de la Google Play.
- **Acceso a la Google Play (3):** link directo de descarga del software Endpoint Protection / Plus de la Google Play.
- **Enviar URL por mail (4):** mensaje de correo con el link de descarga listo para enviar al usuario del dispositivo a proteger con **Endpoint Protection / Plus**.

Para instalar el software en el dispositivo del usuario sigue los pasos mostrados a continuación:

- Selecciona el grupo dentro del árbol de carpetas donde se integrará el dispositivo. El código QR se actualizará de forma automática con la nueva selección.
- Descarga la aplicación Android siguiendo uno de los tres procedimientos descritos a continuación:
 - **Mediante código QR:** haz clic en el código QR para agrandararlo, enfoca la cámara del dispositivo a la pantalla y, mediante una aplicación de lectura de códigos QR, escanéalo. En la pantalla del terminal aparecerá una URL de la Google Play que mostrará la ficha de la aplicación lista para su descarga. Pulsando la URL se mostrará la ficha de la aplicación lista para su descarga.



QR Barcode Scanner y Barcode Scanner son dos aplicaciones para la lectura de códigos QR gratuitas y disponibles en la Google Play.

- **Mediante correo electrónico:** haz clic en el link **Enviar URL por email** para generar un mail con el link correcto al usuario. El usuario deberá de seleccionar el link que le llevará a la Google Play con la ficha de la aplicación lista para su descarga.
 - **Mediante la consola de administración:** si has accedido a la consola de administración desde el propio dispositivo, haz clic en el link **Acceso a la Google Play**. Se mostrará la ficha de la aplicación lista para su descarga.
- Una vez instalada la aplicación se le pedirá al usuario que acepte la concesión de permisos de administrador para la aplicación. Dependiendo de la versión de Android (6.0 en adelante), estos permisos se presentarán de forma progresiva según se vayan necesitando, o por el contrario se mostrará una única ventana la primera vez que se ejecute la aplicación, solicitando todos los permisos necesarios de una sola vez.

Una vez terminado el procedimiento el dispositivo aparecerá en el grupo seleccionado dentro del árbol de carpetas.

6.5. Descubrimiento automático de equipos e instalación remota

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



La instalación remota solo es compatible con plataformas Windows.

6.5.1 Requisitos para instalar Endpoint Protection / Plus en los equipos

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

- **Para que un equipo pueda ser descubierto:** el puerto UDP 137 tiene que estar abierto para el proceso *System*.
- **Para que un equipo pueda ser instalado de forma remota:** el puerto TCP 445 tiene que estar abierto para el proceso *System*



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

6.5.2 Descubrimiento de equipos

El descubrimiento de equipos se efectúa a través de un equipo con el rol de *Descubridor*.

Requisitos para encontrar equipos desprotegidos en la red

El listado de equipos descubiertos contiene los puestos de usuario y servidores que cumplen con los siguientes requisitos:

- Responden al ping (*echo request, echo reply*).
- Devuelven correctamente el nombre NetBios de la máquina (*NetBios Name Service en ejecución en el puerto 137 TCP/UDP*).
- No están ocultos por el administrador.
- No están siendo administrados por **Panda Endpoint Protection / Plus sobre Aether Platform**.



Todos los equipos que cumplan los requisitos indicados se mostrarán en el listado de equipos descubiertos, independientemente de si el sistema operativo o el tipo de dispositivo admite la instalación de Panda Endpoint Protection / Plus.

Asignación del rol de descubridor a un equipo de la red

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

Características del equipo descubridor

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

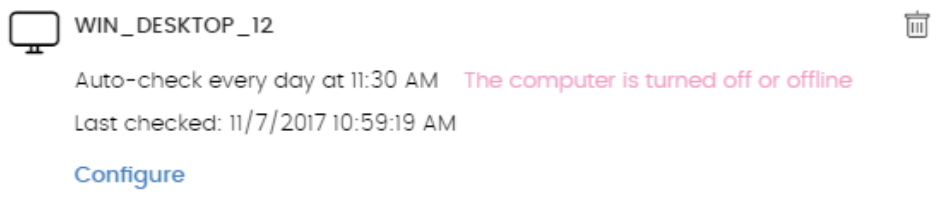


Figura 18: información mostrada en cada equipo descubridor

Nombre del equipo

- **Configuración de la tarea de descubrimiento:** configuración de la tarea automática que se lanza para descubrir equipos en la red, si está configurada.
- **Ultima comprobación:** fecha y hora de la última vez que se lanzó una tarea de descubrimiento.
- **El equipo está apagado o sin conexión:** **Endpoint Protection / Plus** no es capaz de conectar con el equipo descubridor.
- **Configurar:** establece el alcance y tipo de descubrimiento (automático o manual). Si es automático, la tarea de descubrimiento se ejecutará una vez al día.

6.5.3 Alcance del descubrimiento

Para limitar el alcance del descubrimiento de equipos en la red sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, selecciona el equipo descubridor a configurar el alcance de descubrimiento.
- En la sección **Limitar el alcance del descubrimiento** selecciona un criterio:
 - **Buscar solo en la subred del equipo descubridor**: el equipo descubridor utiliza la máscara configurada en la interface para efectuar un barrido completo de la subred a la que pertenece.
 - **Buscar solo en los siguientes rangos de direcciones IPs**: define varios rangos de búsqueda en la red separados por comas. Separa el inicio y el final del rango mediante el carácter guion '-'
 - **Buscar sólo equipos de los siguientes dominios**: la búsqueda queda limitada a los dominios Windows indicados separados por comas.

6.5.4 Programación del descubrimiento de equipos

Programación de tareas de descubrimiento

Las tareas de descubrimiento de equipos se pueden programar para ser lanzadas por los equipos descubridores de forma automática cada cierto tiempo.

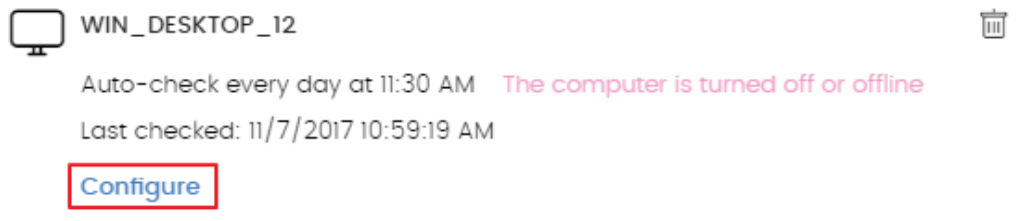


Figura 19: acceso a la ventana de configuración de la tarea de descubrimiento

- **Ejecución automática de la tarea de descubrimiento:**
 - En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
 - En el desplegable **Ejecutar automáticamente** elige **Todos los días**.
 - Elige la hora a la que se ejecutará la tarea.
 - Marca en la casilla para tomar la hora local del equipo o la hora del servidor **Endpoint Protection / Plus**.
 - Haz clic en **Aceptar**. El equipo configurado mostrará en su descripción la programación configurada.

- **Ejecución manual de la tarea de descubrimiento:**
 - En el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Descubrimiento**, haz clic en el enlace **Configurar** del equipo descubridor a configurar.
 - En el desplegable **Ejecutar** automáticamente elige **No**.
 - Haz clic en **Aceptar**. El equipo mostrará un enlace **Comprobar ahora** que el administrador podrá utilizar para lanzar una tarea de descubrimiento bajo demanda.

6.5.5 Listado de equipos descubiertos

Contiene los dispositivos encontrados y no administrados por **Panda Endpoint Protection / Plus**.

Existen dos formas de acceder al listado de equipos descubiertos:

- Desde el widget **Estado de protección**
- Desde **Mis listados**

- **Widget Estado de la protección**

Desde el menú superior **Estado** se accede al panel de control de **Panda Endpoint Protection / Plus** donde se encuentra el widget **Estado de la protección**. En su parte inferior se mostrará el enlace **Se han descubierto x equipos que no están siendo administrados desde Panda Endpoint Protection / Plus**.

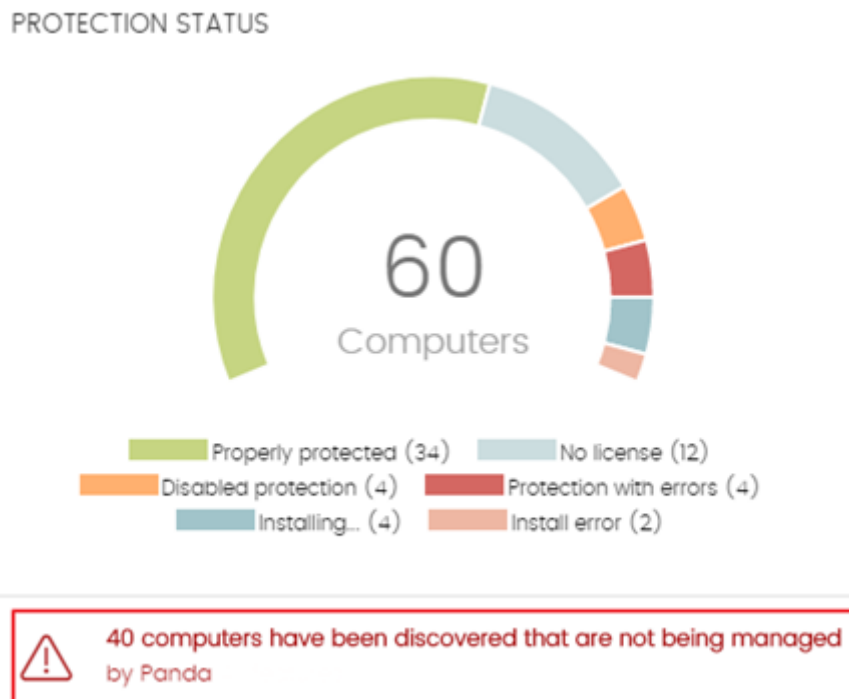


Figura 20: acceso al listado de equipos descubiertos desde el widget Estado de la protección

- **Listado general**

Accede a la sección **Mis listados** desde el menú lateral y haz clic en el enlace **Agregar**. Selecciona en el desplegable el listado **Equipos no administrados descubiertos**.

Descripción de la tabla de equipos descubiertos

Campo	Comentario	Valores
Equipo	Nombre del equipo descubierta	Cadena de caracteres
Estado	Indica el estado en el que se encuentra el equipo con respecto al proceso de instalación	<ul style="list-style-type: none"> — Descubierto: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado  Instalando: el proceso de instalación se ha iniciado Error instalando: mensaje con el tipo de error producido en la instalación. Consulta más adelante la relación de mensajes de error y una explicación de cada uno de ellos.
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor	Cadena de caracteres
Descubierto por	Nombre del equipo descubridor	Cadena de caracteres
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez	Fecha

Tabla 5: campos del listado de equipos descubiertos

A continuación, se muestran los mensajes de error:

- **Credenciales incorrectas:** introduce unas credenciales con permisos para instalar el agente.
- **Equipo descubridor no disponible:**
 - El equipo que descubrió al puesto de usuario o servidor ha sido borrado y por lo tanto la instalación no se puede ejecutar.
- **No es posible conectar con el equipo:**
 - El equipo está apagado.
 - El firewall impide la conexión.
 - El equipo no tiene un sistema operativo compatible.

- **No es posible descargar el instalador del agente:**
 - El paquete descargado está corrupto.
 - No existe un paquete de instalación para el sistema operativo del puesto o servidor.
 - No hay espacio suficiente en el equipo para descargar el paquete del agente.
 - La descarga del paquete del agente es muy lenta y se ha cancelado.
- **No es posible copiar el agente.**
 - No hay espacio suficiente en el equipo para copiar el paquete del agente.
- **No es posible instalar el agente.**
 - No hay espacio suficiente en el equipo para instalar el agente.
 - Ya hay un agente instalado en el equipo. Si es la misma versión, se lanza en modo reparación.
- **No es posible registrar el agente.**
 - El equipo esté pendiente de reiniciar para desinstalar el agente.
 - **Panda Endpoint Protection** está instalado en el equipo remoto.

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Equipo	Nombre del equipo descubierto	Cadena de caracteres
IP	Dirección IP principal del equipo	Cadena de caracteres
Dirección MAC	Dirección física del equipo	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Primera vez visto	Fecha en la que el equipo fue descubierto por primera vez	Cadena de caracteres
Primera vez visto por	Nombre del equipo descubridor que vio por primera vez al puesto de usuario	Cadena de caracteres
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez	Fecha
Ultima vez visto por	Nombre del equipo descubridor que vio por última vez al puesto	Cadena de caracteres

Tabla 6: campos del fichero exportado Listado de equipos descubiertos

Herramienta de búsqueda

Campo	Comentario	Valores
Buscar	Búsqueda por el nombre del equipo, IP, fabricante de la tarjeta de red o equipo descubridor	Cadena de caracteres
Estado	Estado de la instalación de Endpoint Protection / Plus	Descubierto: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado Instalando: el proceso de instalación se ha iniciado Error instalado
Ultima vez visto	Fecha en la que el equipo fue descubierto por última vez	Últimas 24 horas Últimos 7 días Último mes

Tabla 7: campos de filtrado para el listado Accesos a páginas web por equipo

Equipos ocultos

Para evitar generar listados de equipos descubiertos muy extensos que incluyan dispositivos sin interés para la instalación de **Endpoint Protection / Plus**, es posible ocultarlos de forma selectiva siguiendo los pasos mostrados a continuación:

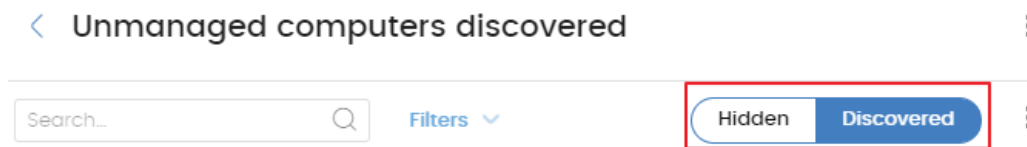


Figura 21: selección del tipo de listado de equipos descubiertos (Ocultos y Descubiertos)

- En el listado de equipos descubiertos selecciona **Descubierto** en el combo (1) y haz clic en **Filtrar**.
- Haz clic en las casillas correspondientes a los equipos a ocultar (2).
- Para ocultar varios equipos haz clic en el menú de contexto general y en **Ocultar y no volver a descubrir** (3).
- Para ocultar un único equipo haz clic en el menú de contexto del equipo y en **Ocultar y no volver a descubrir** (4).

Equipos borrados

Endpoint Protection / Plus no elimina de la lista de equipos descubiertos los dispositivos que una vez fueron detectados, pero ya no están accesibles por haberse retirado, avería, robo o cualquier otra razón.

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

- En el listado de equipos descubiertos selecciona **Descubiertos** u **Ocultos** en el combo dependiendo del estado del dispositivo (1).

- Haz clic en las casillas correspondientes a los equipos a borrar (2).
- Para borrar varios equipos haz clic en el menú de contexto general y en **Borrar (3)**.
- Para borrar un único equipo haz clic en el menú de contexto del equipo y en **Borrar (4)**.



Un equipo borrado, pero no retirado físicamente de la red volverá a aparecer en la siguiente tarea de descubrimiento. Borra únicamente los equipos que nunca más vayan a ser accesibles.

6.5.6 Detalles del equipo descubierto

Haz clic en un equipo descubierto para ver su ventana de detalle dividida en 3 secciones:

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

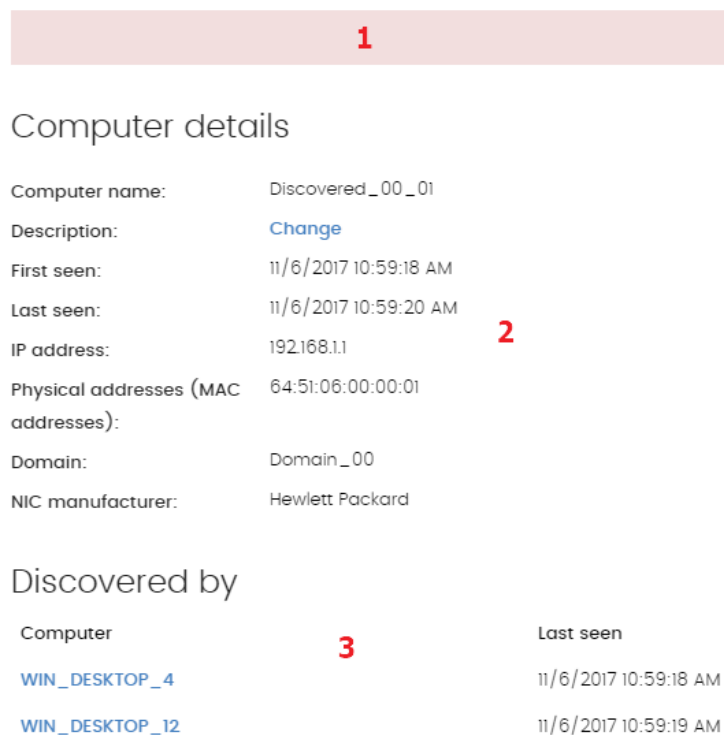


Figura 22: distribución de la información en un equipo descubierto

Alertas de equipo

- **Error instalando el agente de Panda**: indica el motivo del error en la instalación del agente.
 - Credenciales incorrectas. Lanza de nuevo la instalación con unas credenciales con suficientes privilegios para realizar la instalación.
 - Equipo descubridor no disponible.
 - No es posible conectar con el equipo. Verifica que el equipo está encendido y que

cumple los requisitos de instalación remota.

- No es posible descargar el instalador del agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
 - No es posible copiar el instalador del agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
 - No es posible instalar el agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
 - No es posible registrar el agente. Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
- **Instalando agente de Panda:** una vez terminado el proceso de instalación el equipo dejará de aparecer en el listado de equipos descubiertos.
 - **Equipo oculto.**
 - **Equipo no administrado:** el equipo no tiene el agente Panda instalado.

Detalles del equipo

- **Nombre del equipo.**
- **Descripción:** permite asignar una descripción al equipo, aunque no esté administrado todavía.
- **Primera vez visto:** fecha y hora de la primera vez que el equipo fue descubierto.
- **Última vez visto:** fecha y hora de la primera vez que el equipo fue descubierto.
- **Dirección IP.**
- **Direcciones físicas (MAC).**
- **Dominio:** dominio Windows al que pertenece el equipo.
- **Fabricante NIC:** fabricante de la tarjeta de red instalada en el equipo.

Descubierto por

- **Equipo:** nombre del equipo descubridor que vio al equipo no administrado.
- **Última vez visto:** fecha y hora de la primera vez que el equipo fue visto por el equipo descubridor.

6.5.7 Instalación de equipos

Para instalar de forma remota el software **Endpoint Protection / Plus** en uno o varios equipos distribuidos sigue los pasos mostrados a continuación:

Desde el listado de equipos descubiertos

- Accede al listado de equipos descubiertos.
 - Desde el panel lateral **Mis ficheros, Añadir**, selecciona el listado **Equipos no administrados descubiertos**.
 - Desde el menú superior **Estado** en el widget **Estado de la protección**, haz clic en el link **Se han descubierto x equipos que no están siendo administrados desde Panda Endpoint Protection / Plus**.

- Desde el menú superior **Equipos** haz clic en **Añadir equipos** y selecciona **Descubrimiento e instalación remota**. Se mostrará una ventana con un asistente. Haz clic en el link **Ver equipos no administrados descubiertos**.
- En el listado de equipos descubiertos selecciona **Descubiertos** u **Ocultos** en el combo, dependiendo del estado del dispositivo **(1)**.
- Haz clic en las casillas correspondientes a los equipos a instalar.
- Para instalar varios equipos haz clic en el menú de contexto general y en **Instalar agente de Panda**.
- Para instalar un único equipo haz clic en el menú de contexto del equipo y en **Instalar agente de Panda**.
- Configura la instalación según los pasos descritos en el punto 6.4.
- Introduce una o varias credenciales de instalación. Es necesario utilizar una cuenta de administración local del equipo o del dominio al que pertenece para completar la instalación con éxito.

Desde la pantalla de detalles de equipo

Al hacer clic en un equipo descubierto se mostrará su detalle y en la parte superior el botón **Instalar agente de Panda**. Sigue los pasos descritos en el punto 6.4.3 Instalación manual del software Endpoint Protection / Plus.

6.6. Instalación con herramientas centralizadas

Con la ayuda de herramientas de terceros, es posible la instalación del software Windows **Endpoint Protection / Plus** de forma centralizada en redes de tamaño medio o grande. A continuación, se detallan los pasos para el despliegue del software **Endpoint Protection / Plus** en los equipos de una red Windows con Directorio Activo mediante GPO (Group Policy Object).

1 Descarga de Endpoint Protection / Plus y compartición del instalador en la red

- Coloca el instalador **Endpoint Protection / Plus** en una carpeta compartida que sea accesible por todos los equipos que vayan a recibir el software.

2 Crea un nueva OU (Organizational Unit) de nombre "Endpoint Protection".

- Abre el applet "Active Directory Users and Computers" en el Directorio Activo de la red

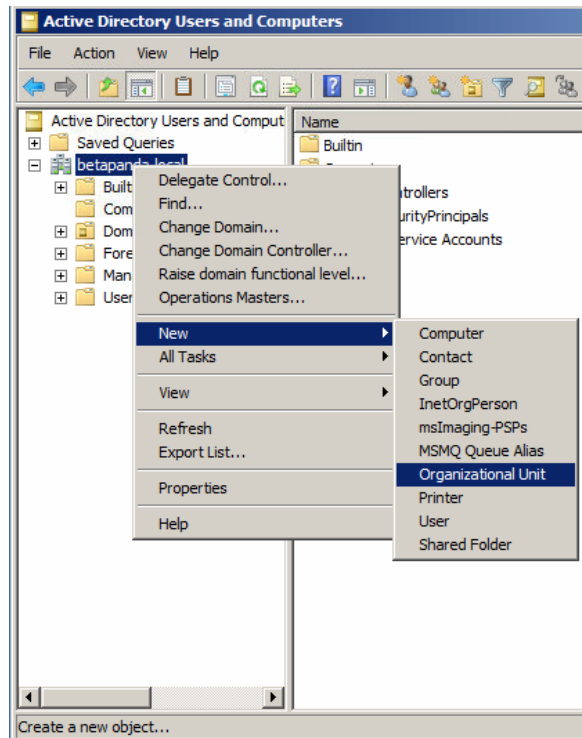


Figura 23: creación de una unidad organizativa

- Abre el snap-in Group Policy Management y en Domains selecciona la OU recién creada para bloquear la herencia.

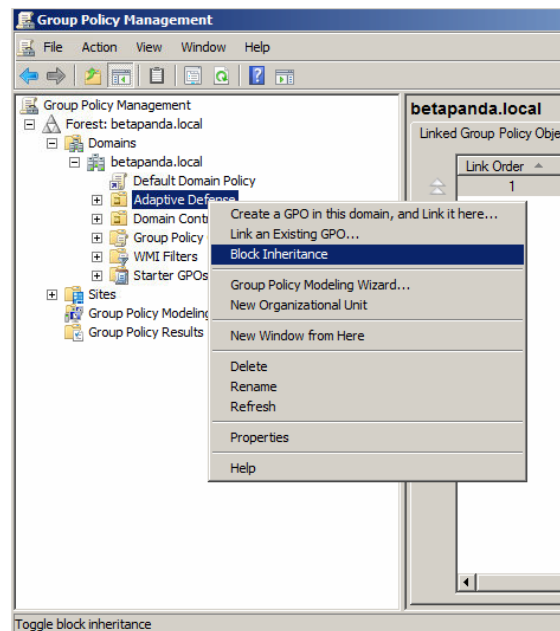


Figura 24: bloqueo de herencia

- Crea una nueva GPO en la OU "Endpoint Protection".

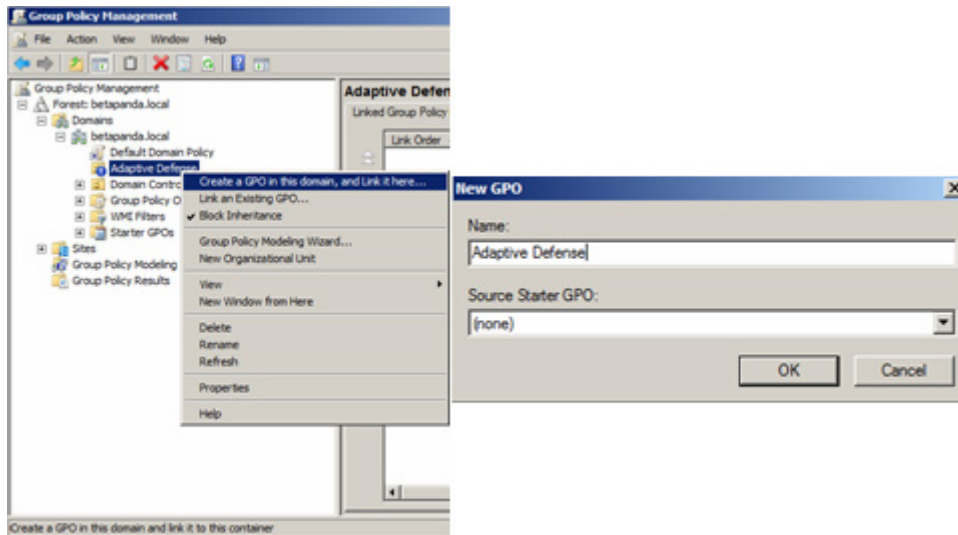


Figura 25: creación de una GPO

3 Añade un nuevo paquete de instalación a la GPO recién creada

- Edita la GPO.

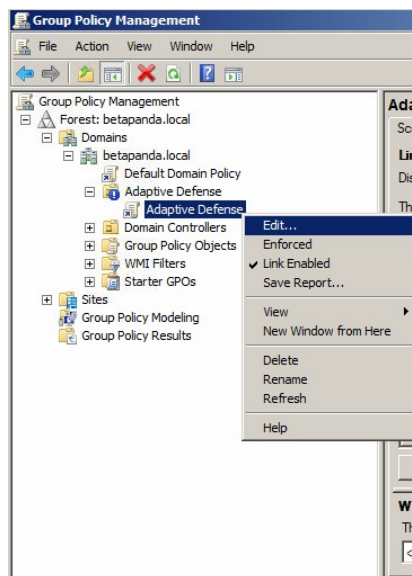


Figura 26: edición de la GPO recién creada

- Añade un nuevo paquete de instalación que contendrá el software **Endpoint Protection / Plus**. Para ello pedirá añadir el instalador a la GPO.

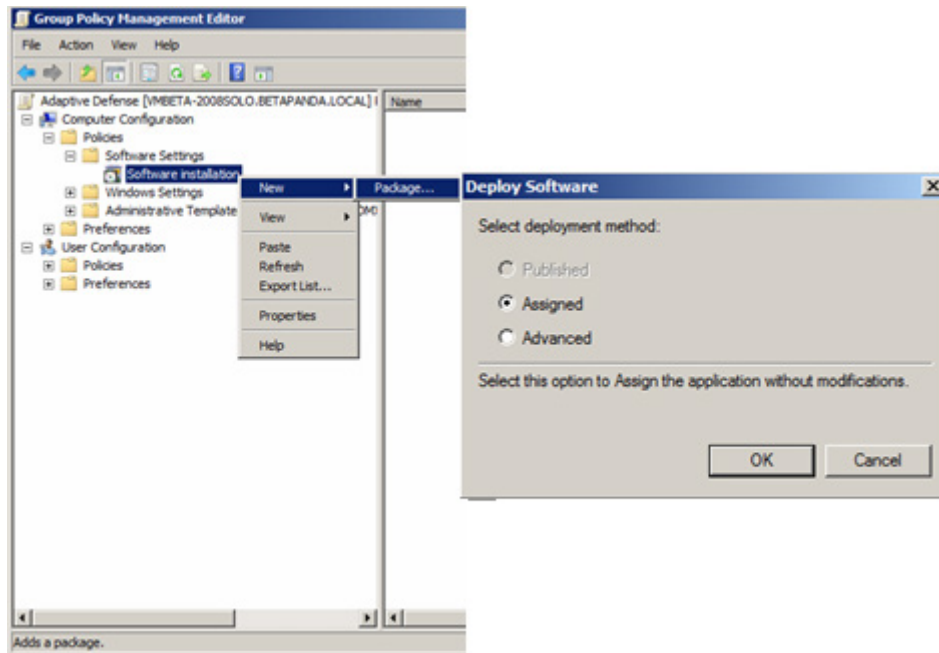


Figura 27: asignación de un nuevo paquete de despliegue

4 Edita las propiedades de despliegue

- En el menú propiedades, pestaña Deployment, Advanced selecciona la casilla que evita la comprobación entre el sistema operativo de destino y el definido en el instalador.

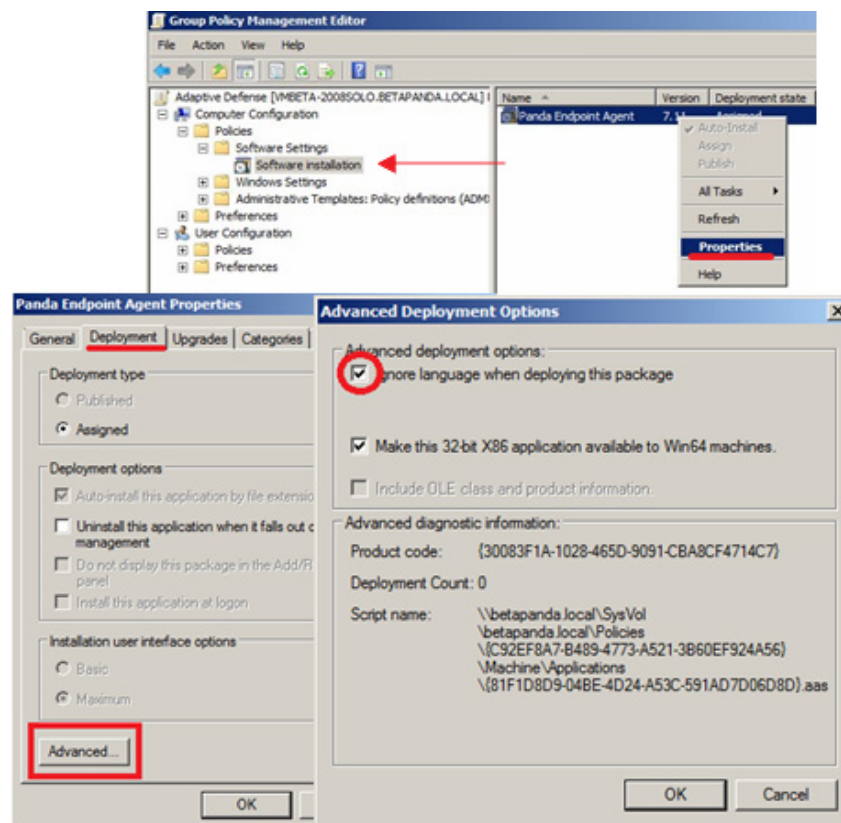


Figura 28: configuración del paquete de despliegue

- Finalmente añade en la OU Endpoint Protection creada anteriormente en Active Directory Users and Computers a todos los equipos de la red que se quiera enviar el agente.

6.7. Instalación mediante generación de imágenes

En redes grandes formadas por muchos equipos homogéneos, el procedimiento de instalación del sistema operativo y de las herramientas que lo acompañan puede automatizarse.

Esta automatización consiste en generar una imagen base (también conocida como “master”, imagen “gold” o imagen “plataforma”) instalando el sistema operativo ya actualizado en un equipo virtual o físico junto a todo el software que el usuario vaya a necesitar, incluyendo las herramientas de seguridad. Una vez el equipo está preparado para funcionar, se extrae una copia del disco duro que se volcará posteriormente en el resto de equipos de la red, reduciendo el tiempo de despliegue de forma muy sustancial.

Si el administrador sigue este procedimiento de despliegue automatizado y **Endpoint Protection / Plus** forma parte de la imagen base, serán necesarios algunos pasos adicionales sobre el procedimiento mostrado anteriormente para su correcto funcionamiento.

La instalación del software **Endpoint Protection / Plus** en cualquier equipo lleva asociada la asignación automática de un identificador único que es utilizado por Panda Security para referenciar al equipo en la consola de administración. Si posteriormente se genera una imagen base con el software **Endpoint Protection / Plus** ya instalado y se clona en otros equipos, todos los equipos que reciban esa imagen heredarán el mismo identificador de **Endpoint Protection / Plus**, de forma que la consola mostrará un solo equipo.

Para evitar esta situación es necesaria la utilización de un programa que borre el identificador generado al instalar el software en el equipo. Este programa se llama `reintegra.zip` y se puede descargar de la página de soporte de la web de Panda Security.

<http://www.pandasecurity.com/spain/support/card?id=500201>

En esta página además encontrarás instrucciones precisas sobre el procedimiento de instalación del agente **Endpoint Protection / Plus** en una imagen base.

6.8. Desinstalación del software

La desinstalación de **Endpoint Protection / Plus** 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, se necesitará autorización o disponer de las credenciales necesarias para poder desinstalar la protección.

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 y superiores:

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

En Windows XP:

- Panel de Control > Agregar o quitar programas.

En macOS:

- Finder > Aplicaciones > Arrastre el icono de la aplicación que desea desinstalar a la papelera.

En dispositivos Android:

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

En Linux

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

7. Gestión de equipos y dispositivos

[La zona equipos](#)
[El árbol de filtros](#)
[El árbol de grupos](#)
[Información de equipo](#)

7.1. Introducción

La consola de administración permite mostrar los equipos administrados de forma ordenada y flexible, aplicando distintas estrategias que ayudan al administrador a localizar rápidamente las máquinas para facilitar su gestión.

7.1.1 Requisitos para la gestión de equipos desde la consola

Para que un equipo de la red sea gestionable por la consola de administración se requiere como mínimo de la instalación del agente Panda en el equipo.

Al igual que otros productos de Panda Security basados en **Aether, Endpoint Protection / Plus** entrega el agente de comunicaciones Panda en el paquete de instalación para todas las plataformas compatibles.

Los equipos sin licencia **Endpoint Protection / Plus**, pero con el agente Panda instalado aparecerán en la consola de administración, aunque su protección estará desactualizada y no podrán ejecutar tareas, análisis ni otros recursos propios de **Endpoint Protection / Plus**.



Los equipos con la licencia caducada seguirán analizando en busca de amenazas, pero no actualizarán el fichero de firmas. En este estado, Endpoint Protection / Plus no será una solución efectiva para la protección frente a amenazas y Panda Security recomienda encarecidamente la renovación de los servicios contratados para mantener el parque IT debidamente protegido.

7.2. La zona Equipos

Para acceder a la ventana de administración de equipos haz clic en el menú superior **Equipos**. Se mostrarán dos zonas bien diferenciados: el panel lateral con un **Árbol de equipos (1)** y el panel central con un **Listado de equipos (2)**. Ambos paneles trabajan de forma conjunta y su funcionamiento se muestra a lo largo de este capítulo.

Al seleccionar un elemento del **Árbol de equipos**, el **Listado de equipos** se actualiza con todos los equipos asignados a la rama del árbol elegida.

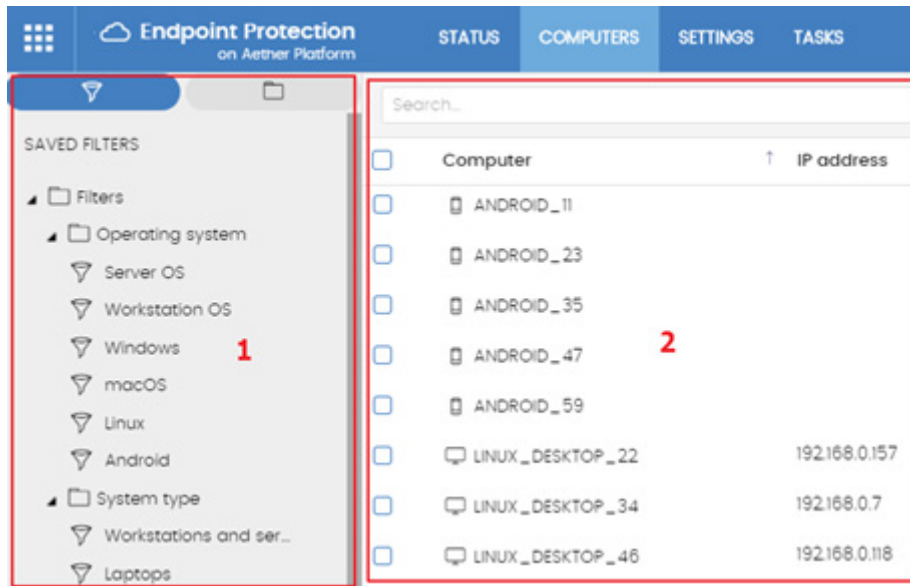


Figura 29: vista general de los paneles en la zona Equipos

Mostrar equipos en subgrupos

Es posible limitar el listado de los equipos mostrando únicamente los que pertenecen a la rama del árbol seleccionada, o por el contrario mostrar todos los equipos que cuelgan de la rama seleccionada y de ramas de orden inferior. Para definir este comportamiento haz clic en el menú de contexto y selecciona la opción **Mostrar equipos de los subgrupos**.

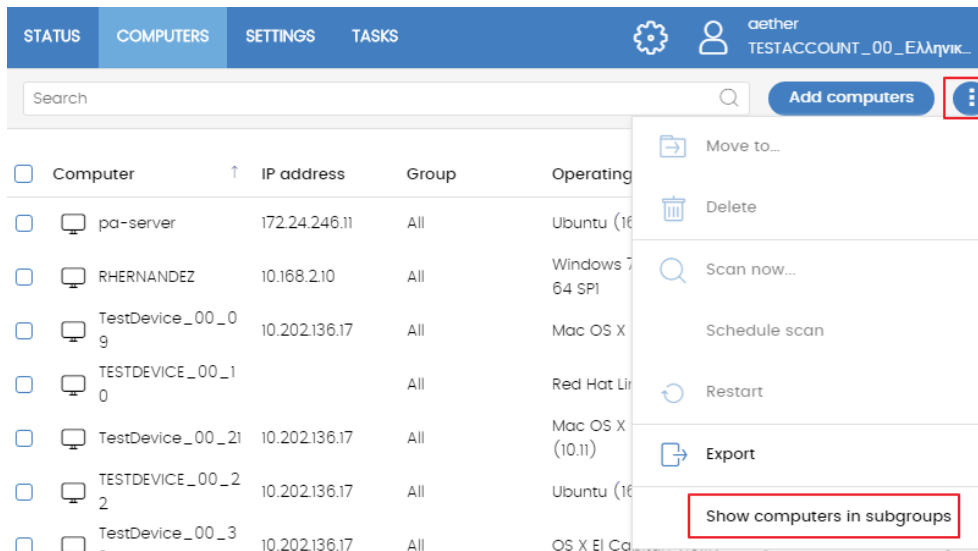


Figura 30: habilitar el listado de equipos pertenecientes a ramas dependientes

7.2.1 El panel Árbol de equipos

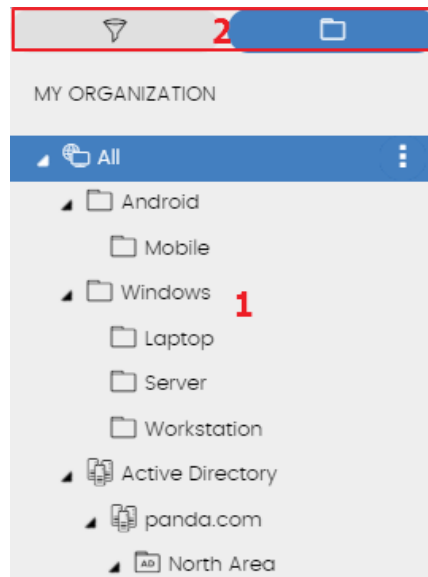




Figura 31: el panel Árbol de equipos

Endpoint Protection / Plus representa la estructura de equipos mediante el Árbol de equipos (1), que presenta dos vistas o árboles independientes (2):

- **Árbol de filtros** : permite gestionar los equipos de la red mediante agrupaciones dinámicas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma automática.
- **Árbol de grupos** : gestiona los equipos de la red mediante agrupaciones estáticas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma manual.

Los dos árboles muestran el parque de equipos y dispositivos Android del cliente de formas alternativas, con el objeto de favorecer la ejecución de tareas de distintos tipos, tales como:

- Localizar equipos que cumplan con características determinadas, relativas al hardware, software o a la seguridad.
- Asignar perfiles de configuración de seguridad de forma ágil.
- Ejecutar acciones de resolución sobre grupos de equipos.



Para localizar equipos desprotegidos o de características determinadas relativas a la seguridad o al estado de la protección consulta el capítulo 14 Visibilidad del malware y del parque informático. Para asignar perfiles de configuración de seguridad consulta el capítulo 8 Gestión de configuraciones. Para ejecutar tareas de resolución de problemas consulta el capítulo 16 Herramientas de resolución.

Al pasar el puntero del ratón por las ramas del árbol de filtros y de grupos se muestra el icono de menú de contexto, haciendo clic se desplegará un menú emergente con todas las operaciones disponibles sobre esta rama del árbol en particular.

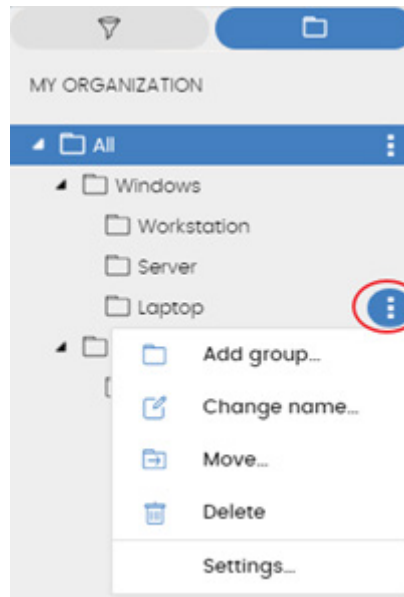


Figura 32: menú emergente con las operaciones disponibles de la rama seleccionada

7.2.2 El panel Listado de equipos

Incluye la información mostrada a continuación:

- (1) Listado de equipos que pertenecen a la rama del árbol seleccionada.
- (2) Herramienta de búsqueda. Permite localizar equipos por su nombre. Se admiten coincidencias parciales sin tener en cuenta mayúsculas y minúsculas
- (3) Menú de contexto que permite aplicar una misma acción a varios equipos.
- (4) Casillas de selección de equipos.
- (5) Sistema de paginación en la parte inferior del panel.

Search 2 <input type="text" value=""/>						Add computers 3
<input type="checkbox"/>	Computer	↑ IP address	Group	Operating system	Last connection	
<input type="checkbox"/>	pa-server	172.24.246.11	All	Ubuntu (16.4)	4/24/2017 10:54:29 AM	⋮
<input type="checkbox"/>	RHERNANDEZ	10.168.2.10	All	Windows 7 Professional 64 SPI	4/24/2017 10:48:01 AM	⋮
<input type="checkbox"/>	TestDevice_00_09	10.202.136.17	All	Mac OS X Lion (10.11)	4/13/2017 8:49:41 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_10	10.202.136.17	All	Red Hat Linux (16.10)	4/24/2017 2:49:44 AM	⋮
<input type="checkbox"/>	TestDevice_00_21	10.202.136.17	All	Mac OS X Snow Leopard (10.11)	4/20/2017 8:50:21 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_22	10.202.136.17	All	Ubuntu (16.10)	4/24/2017 2:50:25 AM	⋮
<input type="checkbox"/>	TestDevice_00_33	10.202.136.17	All	OS X El Capitan (10.11)	4/24/2017 2:51:01 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_34	10.202.136.17	All	Red Hat Linux (16.10)	4/24/2017 2:51:04 AM	⋮
<input type="checkbox"/>	TestDevice_00_45	10.202.136.17	All	OS X Mavericks (10.11)	4/13/2017 8:51:41 AM	⋮
<input type="checkbox"/>	TESTDEVICE_00_46	10.202.136.17	All	Ubuntu (16.10)	4/24/2017 2:51:45 AM	⋮

Figura 33: el panel Listado de equipos

7.2.3 Listado de equipos

Por cada equipo se incluye la información mostrada a continuación

Campo	Comentario	Valores
Equipo	Nombre del equipo y su tipo	Cadena de caracteres Equipo de sobremesa (puesto de trabajo, servidor Windows, Linux o MacOS) Equipo portátil Dispositivo móvil (smart-phone o tablet Android)
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Endpoint Protection / Plus a la que pertenece el equipo y su tipo	Cadena de caracteres Grupo Dominio AD o raíz del Directorio Activo Unidad Organizativa Raíz del árbol de grupos

Campo	Comentario	Valores
Sistema operativo		Cadena de caracteres
Ultima conexión	Fecha del ultimo envío del estado del equipo a la nube de Panda Security	Fecha

Tabla 8: campos del Listado de equipos

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Direcciones IP	Listado de todas las direcciones IP de las tarjetas instaladas en el equipo	Cadena de caracteres
Direcciones físicas (MAC)	Listado de todas las direcciones físicas de las tarjetas instaladas en el equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha arranque del sistema		Fecha
Fecha de instalación	Fecha en la que el Software Endpoint Protection / Plus se instaló con éxito en el equipo	Fecha
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube	Fecha
Plataforma	Tipo de sistema operativo instalado	Windows Linux MacOS Android

Campo	Comentario	Valores
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado	Booleano
Servidor Exchange	Versión del servidor de correo instalada en el servidor	Cadena de caracteres
Versión de la protección		Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección	Fecha
Licencias	Producto licenciado en el equipo	Endpoint Protection / Plus
Configuración de proxy e idioma	Nombre de la configuración de proxy e idioma que afecta al equipo	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de proxy e idioma	Cadena de caracteres
Configuración de seguridad para estaciones y servidores	Nombre de la configuración de seguridad que afecta al puesto de trabajo o servidor	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad	Cadena de caracteres
Configuración de seguridad para dispositivos Android	Nombre de la configuración de seguridad que afecta al dispositivo móvil	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad	Cadena de caracteres
Ajustes por equipo	Nombre de la configuración de ajustes que afecta al equipo	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de ajustes	
Descripción		Cadena de caracteres

Tabla 9: campos del fichero exportado Listado de equipos

Herramientas de filtrado

Campo	Comentario	Valores
Equipo	Nombre del equipo	Cadena de caracteres

Tabla 10: campos de filtrado para el Listado de equipos

7.3. Árbol de filtros

El árbol de filtros es una de las dos vistas del árbol de equipos, y permite agrupar de forma dinámica los equipos en la red mediante reglas y condiciones que describen características de los dispositivos, y operaciones lógicas que las combinan, para producir reglas complejas.

El árbol de filtros es accesible desde el panel de la izquierda, haciendo clic en el icono de filtro.

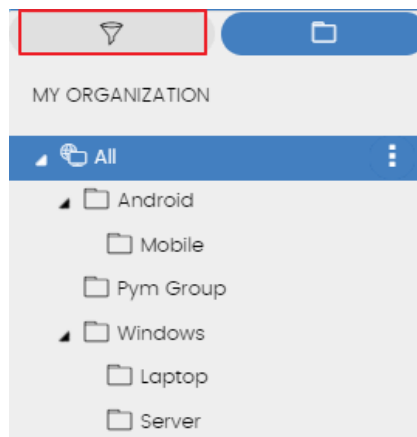


Figura 34: acceso al árbol de filtros

Al hacer clic en los diferentes elementos del árbol, el panel de la derecha se actualiza, presentando todos los equipos que cumplen con los criterios establecidos en el filtro seleccionado.

7.3.1 ¿Qué es un filtro?

Los filtros son agrupaciones dinámicas de equipos. La pertenencia de un equipo a un filtro se determina de forma automática cuando el equipo en cuestión cumple con las condiciones de pertenencia al filtro que haya configurado el administrador.



Un equipo puede pertenecer a más de un filtro.

De esta forma un filtro está constituido por una serie de reglas o condiciones que los equipos tendrán que satisfacer para pertenecer a aquél. En la medida en que el equipo cumpla con las características descritas formará parte del filtro; de la misma forma, cuando un equipo cambie su

estado y no cumpla los criterios de pertenencia, automáticamente dejará de formar parte de la agrupación descrita por el filtro.

7.3.2 Agrupaciones de filtros

Los filtros se pueden ordenar de forma manual agrupándolos en carpetas, con el criterio que el administrador considere oportuno.

7.3.3 Filtros predefinidos

Endpoint Protection / Plus incorpora filtros de uso muy común que el administrador puede utilizar desde el primer momento para ordenar y localizar equipos en la red. Los filtros predeterminados se pueden modificar o borrar.



No es posible recuperar un filtro predeterminado que haya sido borrado.

Nombre	Grupo	Descripción
Equipos de escritorio y servidores	Tipo de máquina	Lista los equipos físicos de sobremesa o servidores
Móviles y tablets	Tipo de máquina	Lista los dispositivos smartphones y tablets
Máquinas virtuales	Tipo de máquina	Lista los equipos virtualizados
SO de servidores	Sistema operativo	Lista los equipos con un Sistema operativo de tipo Servidor instalado
SO de estaciones	Sistema operativo	Lista los equipos con un Sistema operativo de tipo estación de trabajo
Windows	Sistema operativo	Lista todos los equipos con sistema operativo Windows instalado
MacOS	Sistema operativo	Lista todos los equipos con sistema operativo MacOS instalado
Android	Sistema operativo	Lista todos los dispositivos equipos con sistema operativo Android instalado
Java	Software	Lista todos los equipos que tiene instalado el SDK JRE Java

Nombre	Grupo	Descripción
Adobe Acrobat Reader	Software	Lista todos los equipos que tiene instalado el software Acrobat Reader
Adobe Flash Player	Software	Lista todos los equipos que tiene instalado el plugin de reproducción Flash
Google Chrome	Software	Lista todos los equipos que tiene instalado el navegador Chrome
Mozilla Firefox	Software	Lista todos los equipos que tiene instalado el navegador Firefox
Servidores exchange	Software	Lista los equipos que tienen instalado el servidor de correo Microsoft Exchange Server

Tabla 11: listado de filtros predefinidos

7.3.4 Creación y organización de filtros

Todas las operaciones están disponibles haciendo clic en el icono de menú de contexto de las ramas del árbol de filtros. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Creación de filtros

Para crear un filtro es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto de la carpeta en el árbol donde será creado el filtro.



Los filtros no se pueden anidar si no es utilizando una carpeta contenedora. Si se selecciona un filtro en el árbol, el nuevo filtro que se cree lo hará a su mismo nivel, compartiendo su carpeta contenedora.

- Haz clic en **Añadir filtro**.
- Indica el nombre del filtro. No es necesario que sea un nombre único. El resto de la configuración de un filtro se detalla más adelante en este capítulo.

Creación de carpetas

Haz clic en el menú de contexto de la rama donde quieras crear la carpeta y haz clic en **Añadir carpeta**. Introduce el nombre de la carpeta y haz clic en **Aceptar**.



Una carpeta no puede colgar de un filtro. Si seleccionas un filtro antes de crear la carpeta, ésta se creará al mismo nivel que el filtro, compartiendo su carpeta padre.

Borrado de filtros y carpetas

Haz clic en el menú de contexto de la rama a borrar y haz clic en **Eliminar**. La rama se borrará junto a todos sus descendientes.



No se permite borrar el nodo raíz Filtros.

Movimiento y copia de filtros y carpetas

Para mover o copiar un filtro o carpeta sigue los pasos mostrados a continuación:

- Haz clic en el menú de contexto de la rama a copiar o mover.
- Haz clic en **Mover** o **Hacer una copia**. Se mostrará una ventana emergente con el árbol de filtros de destino.
- Selecciona la carpeta de destino y pulsa **Aceptar**.



No es posible copiar carpetas de filtros. Únicamente se permite la copia de filtros.

Renombrar filtros y carpetas

Para renombrar un filtro o carpeta sigue los pasos mostrados a continuación:

- Haz clic en el menú de contexto de la rama a renombrar.
- Haz clic en **Renombrar**.
- Introduce el nuevo nombre.



No es posible renombrar la carpeta raíz. Para renombrar un filtro es necesario editarlo.

7.3.5 Configuración de filtros

La ventana de configuración de filtros es accesible al crear un nuevo filtro o editar uno existente.

Un filtro está formado por una o más reglas, relacionados entre sí mediante operadores lógicos **Y** / **O**. Un equipo formará parte de un filtro si cumple con los valores especificados en las reglas del filtro.

El esquema general de un filtro se compone de cuatro bloques:

- **Nombre del filtro (1)**: identifica al filtro.
- **Reglas de filtrado (2)**: permite construir condiciones atómicas de pertenencia al filtro. Una regla de filtrado únicamente comprueba una característica de los equipos de la red.
- **Operadores lógicos (3)**: Permiten combinar dos reglas de filtrado mediante los operadores

lógicos Y o O.

- **Agrupaciones (4):** permiten variar el orden de evaluación de las reglas de filtrado configuradas y relacionadas mediante operadores lógicos.

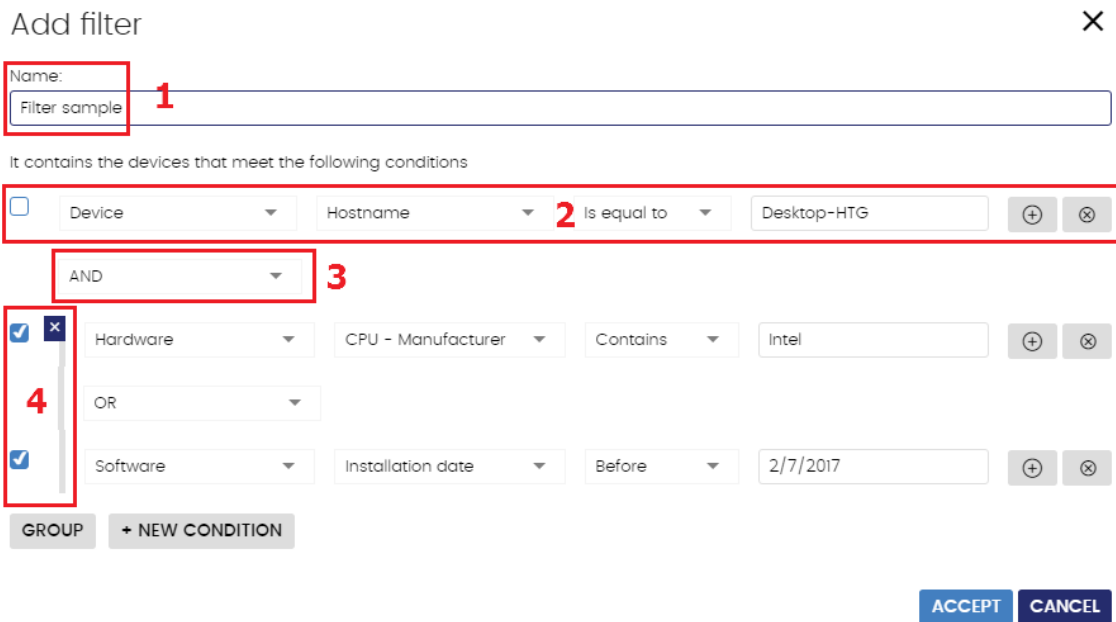


Figura 35: vista general de configuración de un filtro

7.3.6 Reglas de filtrado

Una regla de filtrado se compone de los elementos mostrados a continuación:

- **Categoría (1):** agrupa las propiedades en secciones para facilitar su localización.
- **Propiedad (2):** característica del equipo que determinará su pertenencia al filtro
- **Operador (3):** establece el modo de comparación del contenido de la propiedad del equipo con el valor de referencia que establezca el administrador para el filtro.
- **Valor (4):** contenido de la propiedad. Dependiendo del tipo de propiedad el campo valor cambiará para ajustarse a entradas de tipo fecha, literales etc.



Figura 36: elementos de una regla de filtrado

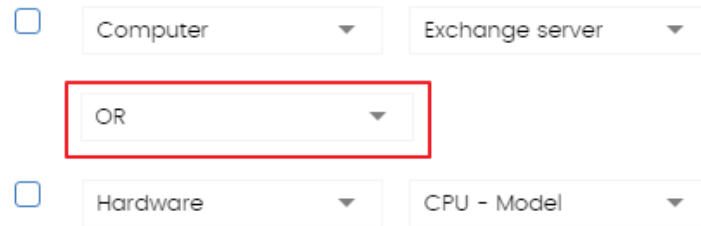
Para añadir reglas de filtrado a un filtro haz clic en el icono  y para borrarlas en el icono



7.3.7 Operadores lógicos

Para combinar dos reglas en un mismo filtro se utilizan los operadores lógicos Y y O. Es posible encadenar de esta forma varias reglas de filtrado mediante operadores lógicos: de forma

automática, al añadir una segunda regla y posteriores se mostrará un desplegable con los operadores lógicos disponibles que se aplicarán a las reglas que lo rodean.



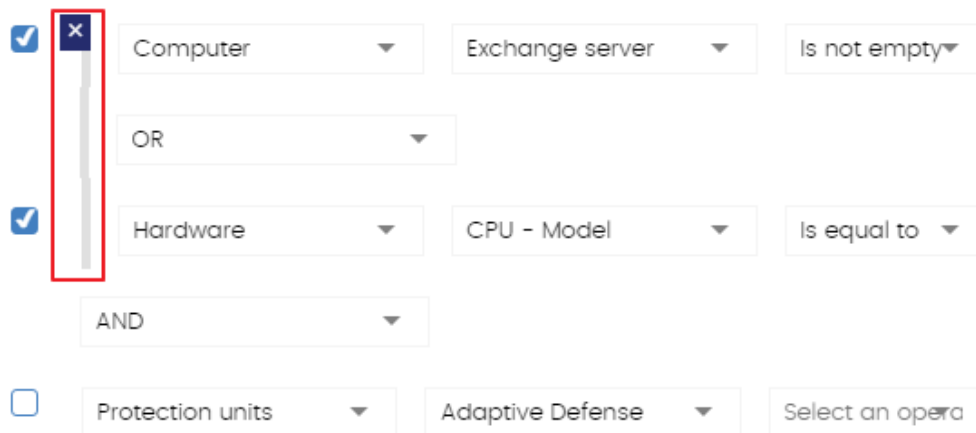
The screenshot shows a configuration interface with two rows of rule components. The first row contains a checkbox, a dropdown menu with 'Computer', and another dropdown menu with 'Exchange server'. Below this is a dropdown menu with 'OR' selected, which is highlighted with a red rectangular box. The second row contains a checkbox, a dropdown menu with 'Hardware', and another dropdown menu with 'CPU - Model'.

Figura 37: operador lógico O

7.3.8 Agrupaciones de reglas de filtrado

Una agrupación equivale al uso de paréntesis en una expresión lógica. Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores, en este caso, de las reglas de filtrado introducidas.

De este modo, para encerrar dos o más reglas en un paréntesis, es necesario crear una agrupación seleccionando con las casillas las reglas que sean necesarias y haciendo clic en el botón **Agrupación**. Se mostrará una línea delgada que abarcará las reglas de filtrado que forman parte de la agrupación.



The screenshot shows a configuration interface with several rule components. On the left, there are two checked checkboxes. A vertical red box highlights a group of three components: a blue 'X' icon, a dropdown menu with 'Computer', and another dropdown menu with 'Exchange server'. Below this is a dropdown menu with 'OR'. Below that is another checked checkbox, a dropdown menu with 'Hardware', and another dropdown menu with 'CPU - Model'. Below this is a dropdown menu with 'AND'. At the bottom, there is an unchecked checkbox, a dropdown menu with 'Protection units', and another dropdown menu with 'Adaptive Defense'.

Figura 38: agrupación de reglas equivalente a (Regla 1 O Regla 2) Y Regla 3

Se pueden definir agrupaciones de varios niveles de la misma forma que se pueden anidar grupos de operandos en una expresión lógica mediante el uso de paréntesis.

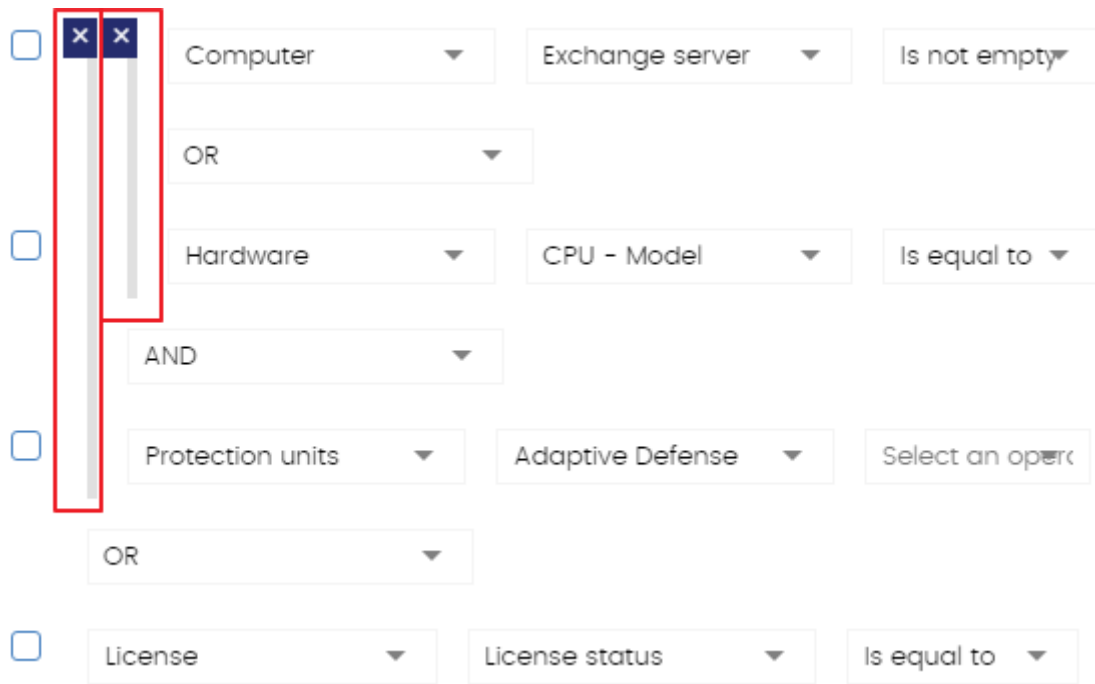


Figura 39: agrupación anidada equivalente a ((Regla 1 Y Regla 2) Y Regla 3) O Regla 4

7.4. Árbol de grupos

El árbol de grupos permite reunir de forma estática los equipos en la red en las agrupaciones que el administrador considere oportunas.

El árbol de grupos es accesible desde el panel de la izquierda, haciendo clic en el icono de carpeta.

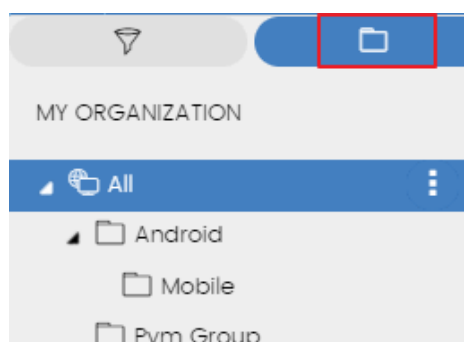


Figura 40: acceso al árbol de grupos

Al hacer clic en las diferentes ramas del árbol, el panel de la derecha se actualiza, presentando todos los equipos que contienen el grupo seleccionado y sus subgrupos.






7.4.1 ¿Qué es un grupo?

Un grupo es un contenedor de equipos asignados de forma manual por el administrador. El árbol de grupos admite crear una estructura de n-niveles compuesta por grupos, subgrupos y equipos.



El máximo nivel de profundidad del árbol es 10.

7.4.2 Tipos de grupos

- **Grupo raíz** : es el grupo padre del que cuelgan el resto de carpetas.
- **Grupos nativos** : son los grupos estándar de **Endpoint Protection / Plus** y soportan todas las operaciones (movimiento, renombrado, borrado etc.) Contiene otros grupos estándar y equipos.
- **Grupos Directorio Activo** : son grupos que replican la estructura del Directorio Activo instalado en la empresa. Tienen limitadas algunas operaciones. Contiene otros grupos de Directorio Activo y equipos.
- **Grupo raíz del directorio activo** : abarca todos los dominios del Directorio Activo configurados en la red de la organización. Contiene grupos de dominio Directorio Activo.
- **Grupo de dominio Active Directory** : ramas del Directorio Activo que representan dominios. Contienen otros grupos de dominio Directorio Activo, grupos Directorio Activo y equipos.


7.4.3 Estructura de grupos

Dependiendo del tamaño de la organización, de lo homogéneos que sean los equipos gestionados y de la presencia o no de un servidor de Directorio Activo en la red de la empresa, la estructura de grupos pasara de un árbol plano de un único nivel para los casos más sencillos, hasta una compleja estructura de varios niveles, para redes grandes formadas por equipos muy heterogéneos.



A diferencia de los filtros, un equipo solo puede pertenecer a una única carpeta.

7.4.4 Grupos de Directorio Activo

Para las organizaciones que tienen instalado un servidor de Directorio Activo en la red, **Endpoint Protection / Plus** puede obtener de forma automática la estructura configurada y replicarla en el árbol de grupos. De esta manera, bajo la rama  se presentará una distribución de los equipos familiar para el administrador, con el objeto de acelerar la localización de dispositivos y su gestión.

Endpoint Protection / Plus replica de forma automática la estructura de Directorio Activo instalada en la organización: los agentes Panda reportan a la consola Web el grupo del Directorio Activo al que pertenecen y, conforme se despliegan los agentes, el árbol se completa con las distintas unidades organizativas.

Por esta razón, el árbol de Directorio Activo es inmutable desde la consola de **Endpoint Protection / Plus** únicamente cambiará cuando lo haga la estructura de Directorio Activo subyacente. Los cambios se replicarán en la consola Web de **Endpoint Protection / Plus** transcurrido un máximo de 15 minutos.

7.4.5 Creación y organización de grupos

Todas las operaciones están disponibles haciendo clic en el icono de menú de contexto de las ramas del árbol de grupos. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Creación de grupos

Selecciona el menú de contexto del grupo padre del cual dependerá el grupo a crear, y haz clic en **Añadir grupo**.



No es posible crear grupos de Directorio Activo en el árbol de grupos, Solo se replicarán los grupos y unidades organizativas creadas en el servidor de Directorio Activo de la empresa.

Borrado de grupos

Selecciona el menú de contexto del grupo a borrar. Si el grupo contiene subgrupos o equipos asignados, la consola de administración mostrará un error.



No se permite borrar el nodo raíz Todos.

Para borrar los grupos vacíos de tipo Directorio Activo que cuelgan de uno dado, haz clic en el menú de contexto del grupo y selecciona **Eliminar grupos vacíos**.

Movimiento de grupos

Para mover un grupo es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto del grupo a mover.
- Haz clic en **Mover**. Se mostrará una ventana emergente con el árbol de grupos de destino.
- Selecciona el grupo de destino y pulsa **Aceptar**.



No se permite el movimiento del nodo raíz Todos ni de grupos Directorio Activo.

Renombrar grupos

Para renombrar un grupo es necesario seguir los pasos mostrados a continuación:

- Selecciona el menú de contexto del grupo a renombrar.
- Haz clic en **Cambiar nombre**.
- Introduce el nuevo nombre.




No es posible renombrar el grupo raíz Todos.

7.4.6 Movimiento de equipos entre grupos

Para mover uno o varios equipos a un grupo, el administrador puede seguir varias estrategias:


Movimiento de conjuntos de equipos a grupos

Para mover varios equipos a la vez a un grupo, sigue los pasos mostrados a continuación:

- Selecciona el grupo **Todos** para listar todos los equipos administrados o utiliza la herramienta de búsqueda para localizar los equipos a mover.
- Selecciona con las casillas los equipos en el panel de listado de equipos.
- Haz clic en el icono  situado a la derecha de la barra de búsqueda. Se mostrará un menú desplegable con la opción **Mover a**. Haciendo clic se mostrará el árbol de grupos destino.
- Selecciona el grupo destino del árbol de grupos mostrado.

Movimiento de un único equipo a un grupo

Para asignar un único equipo a un grupo se pueden seguir varias estrategias:

- Seguir el método mostrado más arriba para asignar conjuntos de equipos a grupos, pero seleccionando un único equipo.
- Selecciona con la casilla el equipo dentro del panel de listado de equipos que quieras asignar y haz clic en el icono de menú  situado en la parte derecha de la fila de ese equipo.
- Desde la ventana de detalles del propio equipo a mover:
 - Dentro en el panel de listado de equipos haz clic en el equipo que quieras mover para mostrar la ventana de detalles.
 - Localiza el campo **Grupo** y haz clic en el botón **Cambiar**. Se mostrará una ventana con el árbol de grupos de destino.
 - Selecciona el grupo destino y haz clic en **Aceptar**.

Movimiento de equipos desde grupos Active Directory

Un equipo que reside en un grupo Directorio Activo puede moverse a un grupo estándar, pero nunca a otro grupo Directorio Activo.

Movimiento de equipos hacia grupos Active Directory

No es posible mover un equipo desde un grupo nativo a un grupo Directorio Activo en particular, solo puedes devolverlo a su grupo Directorio Activo al que pertenece. Para ello haz clic en el menú de contexto del equipo y selecciona **Mover a su ruta de Active Directory**.

Restaurar la pertenencia de varios equipos a su grupo Active Directory

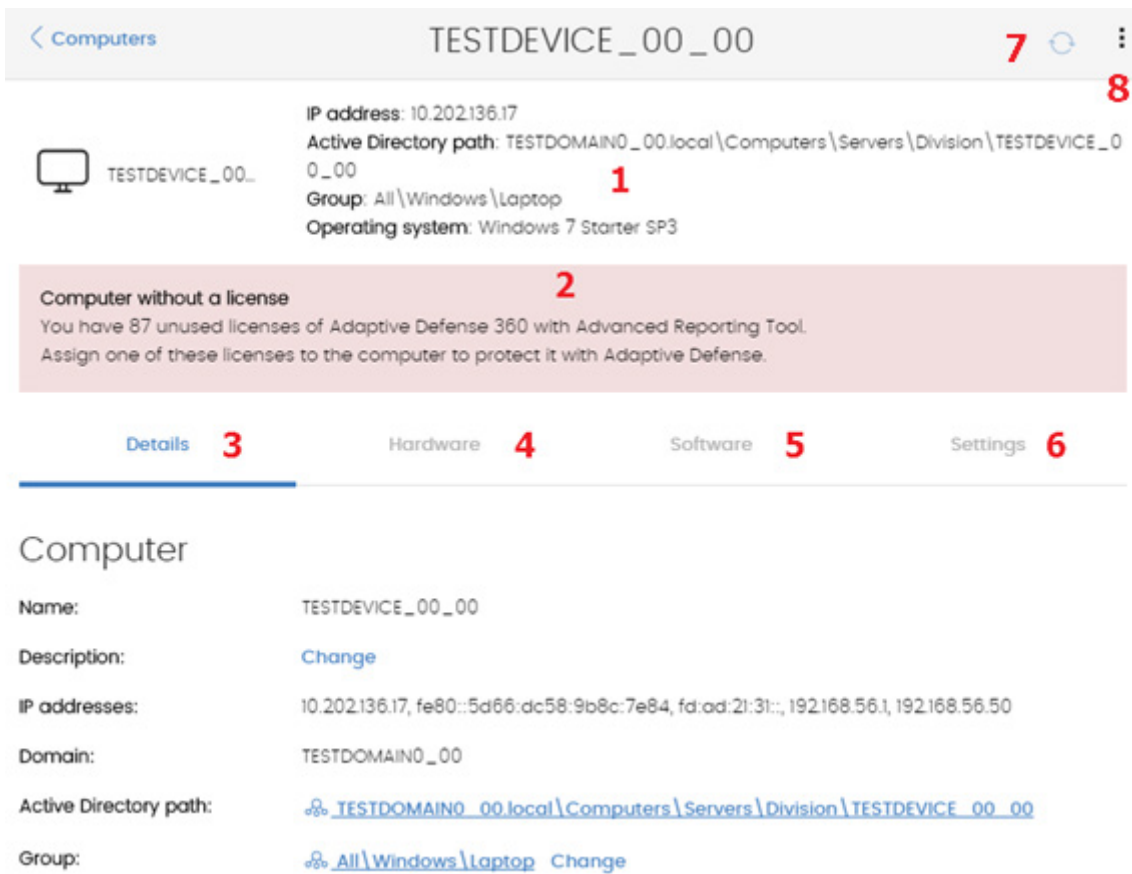
Para restablecer la pertenencia de equipos a su grupo Directorio Activo original haz clic en el menú de contexto de un grupo de Directorio Activo y selecciona la opción **Mover a su ruta de Active Directory**. Todos los equipos que pertenecen a ese grupo en el Directorio Activo de la empresa y que el administrador movió a otros grupos dentro de la consola **Endpoint Protection / Plus** serán devueltos a su grupo original.

7.5. Información de equipo

Al seleccionar un equipo en el panel de listado de equipos se mostrará una ventana con el detalle de la información del hardware y software instalado, así como de la configuración de seguridad asignada.

La ventana de detalle del equipo se divide en 6 secciones:

- **General (1)**: muestra información para ayudar en la identificación del equipo.
- **Alertas de equipo (2)**: muestra potenciales problemas asociados al equipo.
- **Detalles (3)**: muestra un resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Hardware (4)**: muestra el hardware instalado en el equipo, sus componentes y periféricos conectados, así como su consumo y utilización.
- **Software (5)**: muestra los paquetes de software instalados en el equipo, así como su versión y un registro de cambios.
- **Configuración (6)**: muestra las configuraciones de seguridad y otras asignadas al equipo.



TESTDEVICE_00_00 7

IP address: 10.202.136.17
 Active Directory path: TESTDOMAIN0_00.local\Computers\Servers\Division\TESTDEVICE_00_00
 Group: All\Windows\Laptop
 Operating system: Windows 7 Starter SP3

Computer without a license
 You have 87 unused licenses of Adaptive Defense 360 with Advanced Reporting Tool. Assign one of these licenses to the computer to protect it with Adaptive Defense.

[Details](#) [Hardware](#) [Software](#) [Settings](#)

Computer
 Name: TESTDEVICE_00_00
 Description: [Change](#)
 IP addresses: 10.202.136.17, fe80::5d66:dc58:9b8c:7e84, fd:ad:21:31::, 192.168.56.1, 192.168.56.50
 Domain: TESTDOMAIN0_00
 Active Directory path: [TESTDOMAIN0_00.local\Computers\Servers\Division\TESTDEVICE_00_00](#)
 Group: [All\Windows\Laptop](#) [Change](#)

Figura 41: vista general de la información de equipo

7.5.1 Sección general (1)

Contiene la siguiente información:

- **Nombre del equipo e icono** indicando el tipo de equipo.
- **IP:** Dirección IP del equipo.
- **Ruta del directorio activo:** muestra la ruta completa del equipo en el Directorio Activo de la empresa.
- **Grupo:** carpeta del árbol de grupos a la que pertenece el equipo.
- **Sistema operativo:** versión completa del sistema operativo instalada en la máquina.
- **Rol del equipo:** indica si el equipo hace las funciones de descubridor, cache o proxy.

7.5.2 Sección alertas de equipo (2)

Las alertas describen los problemas encontrados en los equipos de la red en lo que respecta al funcionamiento de **Endpoint Protection / Plus** y su motivo, así como indicaciones para solucionarlos. A continuación, se muestra un resumen de los tipos de alertas generadas y las acciones recomendadas para su resolución.

Equipo desprotegido:

- **Protecciones desactivadas:** se mostrará un mensaje indicando que la protección antivirus o la protección Exchange están desactivadas. Se recomienda asignar una configuración de

protección al equipo con las protecciones activadas. Consulta el capítulo 8 para asignar una configuración de seguridad y el capítulo 10 para crear configuraciones de seguridad.

- **Protección con error:** se mostrará un mensaje indicando que la protección antivirus o la protección Exchange están en estado erróneo. Reinicia el equipo o reinstala el software. Consulta el capítulo 6 para instalar el software en el equipo y el capítulo 16 para reiniciar el equipo.
- **Fallo en la instalación:** el equipo está desprotegido porque la instalación terminó en error. Consulta el capítulo 6 para reinstalar el software en el equipo.
- **Instalación en proceso:** el equipo estará desprotegido hasta que no termine la instalación de **Endpoint Protection / Plus**. Espera unos minutos hasta que la instalación se haya completado.

Equipo desactualizado:

- **Protección pendiente de reinicio:** la actualización del motor de seguridad se ha descargado, pero es necesario un reinicio para que se aplique en el equipo. Consulta el capítulo 16 para reiniciar el equipo de forma remota.
- **Actualizaciones de la protección desactivadas:** el software no recibirá ninguna mejora y la seguridad puede verse comprometida en un futuro. Consulta el capítulo 8 para crear y asignar una configuración de tipo Ajustes por equipo que permita la actualización del software.
- **Actualizaciones de conocimiento desactivadas:** el software no recibirá ninguna actualización del fichero de firmas y su seguridad puede verse comprometida en el corto plazo. Consulta el capítulo 10 y 11 para crear configuraciones de seguridad que permitan la actualización del fichero de firmas.
- **Error en la actualización del conocimiento:** la descarga del fichero de firmas falló. Consulta este mismo capítulo para comprobar el espacio libre en el disco duro del equipo. Consulta el capítulo 16 para reiniciar el equipo. Consulta el capítulo 6 para reinstalar el software en el equipo.

Sin conexión desde...

El equipo no se ha conectado a la nube de Panda Security en varios días. Comprueba la conectividad del equipo y la configuración del cortafuegos de la red. Consulta el capítulo 10 Configuración de seguridad para estaciones y servidores para comprobar si se cumplen los requisitos de conectividad. Consulta el capítulo 6 para reinstalar el software en el equipo.

Pendiente de reinicio

El administrador ha solicitado un reinicio que todavía no se ha producido.

7.5.3 Sección Detalles (3)

La información mostrada en esta pestaña se divide en dos apartados: **Equipo** con la información de la configuración del dispositivo ofrecida por el agente Panda, y **Seguridad**, con el estado de las protecciones de **Endpoint Protection / Plus**.

- **Equipo**
 - **Nombre:** nombre del equipo.
 - **Descripción:** texto descriptivo asignado por el administrador.

- **Direcciones físicas (MAC):** dirección física de las tarjetas de red instaladas.
- **Direcciones IP:** listado con todas las direcciones IP (principal y alias).
- **Dominio:** dominio Windows al que pertenece el equipo. Vacío si no pertenece a un dominio.
- **Ruta de directorio activo:** ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.
- **Grupo:** grupo dentro del Árbol de grupos al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón **Cambiar**.
- **Sistema operativo.**
- **Servidor de correo:** versión del servidor Microsoft Exchange instalada en el equipo.
- **Máquina virtual:** indica si el equipo es físico o esta virtualizado.
- **Licencias:** licencias de productos de Panda Security instalados en el equipo. Para obtener más información consulta el capítulo 5.
- **Versión del agente.**
- **Fecha de arranque del sistema.**
- **Fecha de instalación.**
- **Última conexión** del agente con la infraestructura de Panda Security. Como mínimo el agente de comunicaciones contactará cada 4 horas.
- **Seguridad:** en esta sección se indican el estado (Activado, Desactivado, Error) de las distintas tecnologías de **Endpoint Protection / Plus**.
 - **Antivirus de archivos**
 - **Antivirus de correo**
 - **Antivirus para navegación web**
 - **Protección firewall**
 - **Control de dispositivos**
 - **Control de acceso a páginas web (solo Endpoint Protection Plus)**
 - **Versión de la protección**
 - **Versión de actualización del conocimiento:** fecha de la última descarga del fichero de firmas en el equipo.



Para obtener información sobre los datos relativos a la seguridad de los equipos protegidos consulta el capítulo 14 Visibilidad del malware y del parque informático.

7.5.4 Sección Hardware (4)

Contiene la siguiente información:

- **CPU:** información del microprocesador instalado en el equipo y una gráfica de líneas con el consumo de CPU en diferentes periodos e intervalos según la selección:
 - Intervalos de 5 minutos para la última hora.
 - Intervalos de 10 minutos para las 3 últimas horas.

- Intervalos de 40 minutos para las últimas 24 horas.
- **Memoria:** información sobre las características de los chips de memoria instalados y una gráfica de líneas con el consumo de memoria en diferentes periodos e intervalos según la selección:
 - Intervalos de 5 minutos para la última hora.
 - Intervalos de 10 minutos para las 3 últimas horas.
 - Intervalos de 40 minutos para las últimas 24 horas.
- **Disco:** información sobre las características del sistema de almacenamiento masivo y un gráfico de tarta con el porcentaje de espacio libre y ocupado en el momento de la consulta.

7.5.5 Sección Software (5)

Contiene un listado del software instalados en el equipo y de las actualizaciones del sistema operativo Windows y otros programas de Microsoft. El listado contiene la siguiente información:

- **Nombre:** nombre del programa.
- **Editor:** empresa que desarrolló el programa.
- **Fecha de instalación**
- **Tamaño**
- **Versión**



Herramienta de búsqueda

La herramienta que permite localizar paquetes de software instalado mediante coincidencias parciales o completas en todos los campos mostrados anteriormente.

Mediante el control desplegable es posible limitar la búsqueda para localizar únicamente las actualizaciones, el software instalado o ambos conceptos.

Registro de cambios

El registro de cambios es un listado que muestra todos los eventos de instalación y desinstalación de software sucedidos en el intervalo de fechas configurado. Por cada evento se muestra la siguiente información:

- **Evento:** Instalación  o desinstalación .
- **Nombre:** nombre del paquete de software que provoco el evento.
- **Editor:** empresa que desarrolló el programa.
- **Versión**
- **Fecha**

7.5.6 Sección Configuración (6)

La sección **Configuración** muestra los perfiles asociados al equipo y se tratan en el capítulo 8 Gestión de configuraciones.

7.5.7 Forzar sincronización (7)

Envía los cambios pendientes del equipo a la nube.

7.5.8 Menú de contexto

Agrupar múltiples operaciones sobre el equipo:

- **Mover a:** mueve el equipo a un grupo estándar.
- **Mover a su ruta de Active Directory:** mueve el equipo a su grupo Directorio Activo original.
- **Eliminar:** libera la licencia de **Endpoint Protection / Plus** y elimina el equipo de la consola Web.
- **Desinfectar:** programa una tarea de desinfección de ejecución inmediata. Consulta el capítulo 16 Herramientas de resolución para obtener más información.
- **Analizar ahora:** programa una tarea de análisis de ejecución inmediata. Consulta el capítulo 16 Herramientas de resolución para más información.
- **Programar análisis.** Programa una tarea de análisis. Consulta el capítulo 13 Tareas para más información.
- **Reiniciar:** reinicia el equipo de forma inmediata. Consulta el capítulo 16 Herramientas de resolución para obtener más información.
- **Notificar un problema:** abre un ticket de mantenimiento con el departamento técnico de Panda Security. Consulta el capítulo 16 Herramientas de resolución para obtener más información.

8. Gestión de configuraciones

- Qué es una configuración
- Visión general de la asignación de configuraciones
- Perfiles de configuración modulares vs monolíticos
- Introducción a los cuatro tipos de configuraciones
- Creación y gestión de configuraciones
- Asignación manual y automática de configuraciones
- Visualizar las configuraciones asignadas

8.1. Introducción

En este capítulo se tratan los recursos implementados en **Endpoint Protection / Plus** para la gestión de configuraciones de los equipos de la red.

8.2. ¿Qué es una configuración?

Las configuraciones, también llamados “perfiles de configuración” o simplemente “perfiles”, ofrecen a los administradores un modo rápido de establecer los parámetros de seguridad, productividad y conectividad gestionados por **Endpoint Protection / Plus** en los equipos que administran.

El administrador de la red creará tantos perfiles como variaciones de configuraciones sean necesarias. Una nueva configuración viene dada por la existencia de equipos heterogéneos en la red de la empresa:

- Equipos de usuario manejados por personas con distintos niveles de conocimientos en informática requerirán configuraciones más o menos estrictas frente a la ejecución de software, acceso a internet o a periféricos.
- Usuarios con diferentes tareas a desempeñar y por lo tanto diferentes usos y necesidades, requerirán configuraciones que permitan el acceso a diferentes recursos.
- Usuarios que manejen información confidencial o delicada para la empresa requerirán un nivel de protección superior frente a amenazas e intentos de sustracción de la propiedad intelectual de la compañía.
- Equipos en distintas delegaciones requerirán configuraciones distintas que les permitan conectarse a internet utilizando diferentes infraestructuras de comunicaciones.
- Servidores críticos para el funcionamiento de la empresa requerirán configuraciones de seguridad específicas.

8.3. Visión general de la asignación de configuraciones a equipos

De forma general, la asignación de configuraciones a los equipos de la red es un proceso de cuatro pasos:

- 1 **Creación de los grupos que reúnan equipos del mismo tipo o con idénticos requisitos de conectividad y seguridad.**
- 2 **Asignación de los equipos a su grupo correspondiente.**
- 3 **Asignación de configuraciones a los grupos.**
- 4 **Difusión inmediata y automática de la configuración a los equipos de la red.**

Todas estas operaciones se realizan desde el árbol de grupos, accesible desde el menú superior **Equipos**. El árbol de grupos es la herramienta principal para asignar configuraciones de forma rápida y sobre conjuntos amplios de equipos.

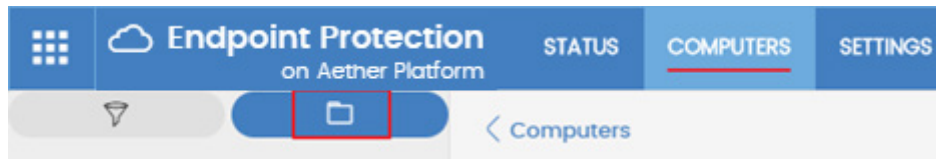


Figura 42: acceso al árbol de grupos

Por lo tanto, la estrategia principal del administrador consiste en reunir todos los equipos similares en un mismo grupo y crear tantos grupos como conjuntos diferentes de equipos existan en la red que gestiona.



Para obtener más información sobre el manejo del árbol de grupos y asignación de equipos a grupos consulta el capítulo 7.

8.3.1 Difusión inmediata de la configuración

Una vez que una configuración es asignada a un grupo, esa configuración se aplicará a los equipos del grupo de forma inmediata y automática, siguiendo las reglas de la herencia mostradas más adelante en este capítulo. La configuración así establecida se aplica a los equipos sin retardos, en cuestión de unos pocos segundos.



Para desactivar la difusión inmediata de la configuración consulta el capítulo 9.

8.3.2 Árbol multinivel

En empresas de tamaño mediano y grande, la variedad de configuraciones puede ser muy alta. Para facilitar la gestión de parques informáticos grandes, **Endpoint Protection / Plus** permite generar árboles de grupos de varios niveles de forma que el administrador pueda gestionar con facilidad los equipos de la red.

8.3.3 Herencia

En redes de tamaño amplio es muy probable que el administrador quiera reutilizar configuraciones ya establecidas en grupos de orden superior dentro del árbol de grupos. El mecanismo de herencia permite asignar una configuración sobre un grupo y, de forma automática, sobre todos los grupos que dependen de éste, ahorrando tiempo de gestión.

8.3.4 Configuraciones manuales

Para evitar la propagación de configuraciones en todos los niveles inferiores de una rama del árbol, o asignar una configuración distinta a la recibida mediante la herencia sobre un determinado equipo dentro de una rama, es posible asignar de forma manual configuraciones a equipos individuales o a grupos.

8.3.5 Configuración por defecto

Inicialmente todos los equipos en el árbol de grupos heredan la configuración establecida en el nodo raíz **Todos**.

El nodo raíz **Todos** tiene asignadas las configuraciones por defecto mostradas a continuación:

- Configuración por defecto (Proxy e idioma)
- Configuración por defecto (Ajustes por equipo)
- Configuración por defecto (Configuración para estaciones y servidores)
- Configuración por defecto (Configuración para dispositivos Android)

De esta manera, los equipos estarán protegidos desde el primer momento, incluso antes de que el administrador haya accedido a la consola para establecer una configuración de seguridad.

8.4. Perfiles de configuración modulares vs monolíticos

Endpoint Protection / Plus utiliza un enfoque modular a la hora de crear y distribuir las configuraciones a aplicar en los equipos administrados. Para ello utiliza cuatro tipos de perfil independientes, que cubren otras tantas áreas de configuración.

Los cuatro tipos de perfiles se muestran a continuación:

- Configuración de proxy e idioma
- Configuración de ajustes por equipo
- Configuración para estaciones y servidores
- Configuración para dispositivos Android

El objetivo de utilizar este enfoque modular y no un único perfil de configuración monolítico que abarque toda la configuración, es el de reducir el número de perfiles creados en la consola de gestión. El enfoque modular permite generar configuraciones lo más pequeñas y ligeras posible, frente a perfiles monolíticos que fomentan la aparición de muchos perfiles de configuración muy largos y redundantes, con muy pocas diferencias entre sí. De esta manera, se minimiza el tiempo que el administrador tendrá que dedicar a gestionar todos los perfiles creados.

Con perfiles modulares es posible combinar varias configuraciones para construir una única configuración que se ajuste a las necesidades del usuario, con un número de perfiles distintos mínimo.

Caso práctico: Creación de configuraciones para varias delegaciones

En este caso práctico tenemos una empresa con 5 delegaciones, cada una de ellas tiene una infraestructura de comunicaciones distinta y por tanto una configuración de proxy diferente. Además, dentro de cada delegación se requieren 3 configuraciones de seguridad diferentes, una para el departamento de diseño, otro para el departamento de contabilidad y otra para el departamento de marketing.



Si **Endpoint Protection / Plus** implementara todos los parámetros de configuración en un único perfil monolítico, serían necesarios 15 perfiles de configuración distintos ($5 \times 3 = 15$) para dar servicio a todos los departamentos de todas las delegaciones de la empresa.

Perfil monolítico



Como **Endpoint Protection / Plus** separa la configuración de proxy de la de seguridad, el número de perfiles a crear se reduce (5 perfiles de proxy + 3 perfiles de departamento = 8) ya que los perfiles de seguridad por departamento de una delegación se pueden reutilizar y combinar con los perfiles de proxy en otras delegaciones.

Perfil modular Proxy e idioma



Perfil modular Seguridad



8.5. Introducción a los cuatro tipos de configuraciones



Consulta el capítulo 9 10, y 11 para obtener más información sobre la configuración del agente Panda y sobre las protecciones para las distintas plataformas compatibles.

Proxy e idioma

Define el idioma del agente instalado en el equipo de usuario y configura su forma de conectar con internet para pasar a través de un servidor de proxy.

Configuración de Ajustes por equipo

Define varios parámetros del agente Panda:

- Intervalo de actualizaciones del software **Endpoint Protection / Plus** en los equipos. Consulta el capítulo 12 Actualización del Software para obtener más información
- Contraseña de instalación en los equipos de usuario.
- Protección anti-tamper.

Configuración de Estaciones y servidores

Define la configuración de seguridad de los equipos de la red Windows, macOS y Linux, tanto de los puestos de trabajo como servidores.

Configuración de Dispositivos Android

Este tipo de perfil define la configuración de seguridad de dispositivos Android (tablets y smartphones).

8.6. Creación y gestión de configuraciones

Haz clic en el menú superior **Configuración** para crear, copiar y borrar configuraciones. En el panel de la izquierda se encuentran las cuatro entradas correspondientes a los cuatro tipos de perfil de configuración posibles **(1)**, **(2)**, **(3)** y **(4)**. En el panel de la derecha se muestran los perfiles de configuración ya creados **(5)** del tipo seleccionado y los botones para **Añadir (6)**, copiar **(7)** y eliminar perfiles **(8)**.

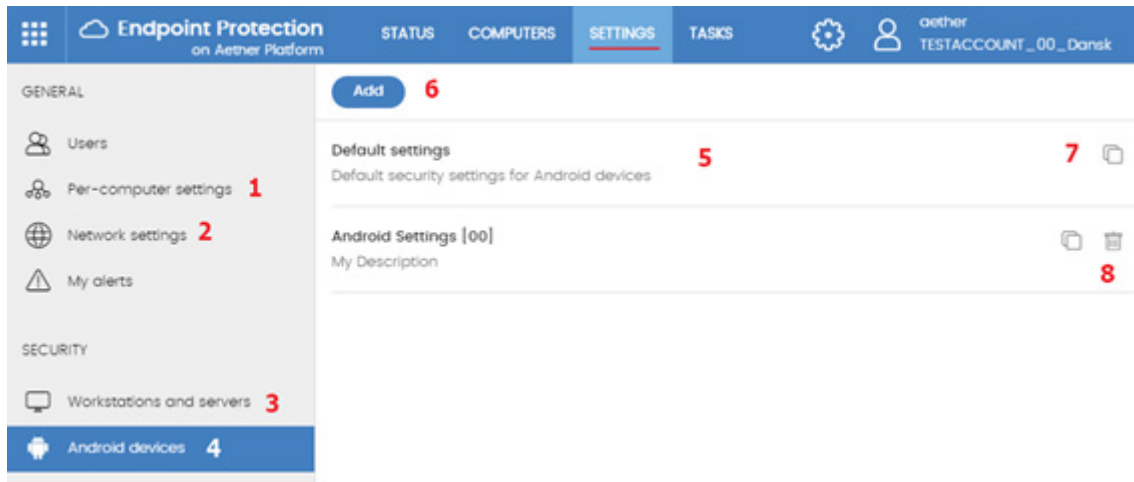


Figura 43: pantalla para la creación y gestión de configuraciones

Creación de configuraciones

Al hacer clic sobre el botón **Añadir** se muestra la ventana de creación de configuraciones. Todos los perfiles tienen un nombre principal y una descripción que son mostradas en los listados de configuraciones.

Copia y borrado de configuraciones

Mediante los iconos (7) y (8) es posible copiar y borrar un perfil de configuración, pero si ha sido asignado a uno o más equipos se impedirá su borrado hasta que sea liberado.

Haciendo clic en el perfil de configuración se permite su edición.



Antes de modificar un perfil comprueba que la nueva configuración sea correcta ya que, si el perfil ya está asignado a equipos de la red, esta nueva configuración se propagará y aplicará de forma automática y sin retardos.

8.7. Asignación manual y automática de configuraciones a grupos

Una vez creados los perfiles de configuración, éstos pueden ser asignados a los equipos de la red siguiendo dos estrategias diferentes:

- Mediante asignación manual (asignación directa).
- Mediante asignación automática a través de la herencia (asignación indirecta).

Ambas estrategias son complementarias y es muy recomendable que el administrador comprenda las ventajas y limitaciones de cada mecanismo para poder definir una estructura de equipos lo más simple y flexible posible, con el objetivo de minimizar las tareas de mantenimiento diarias.

8.7.1 Asignación directa / manual de configuraciones

La asignación manual consiste en la asignación de forma directa de perfiles de configuración a equipos o grupos. De esta manera es el administrador el que, de forma manual, asigna una configuración a un grupo o equipo.

Una vez creados los perfiles de configuración, estos son asignados de tres maneras posibles:

- Desde el menú superior **Equipos**, en el árbol de grupos mostrado en el panel de la izquierda.
- Desde el detalle del equipo en el panel de listado de equipos, accesible desde el menú superior **Equipos**.
- Desde el propio perfil de configuración creado o editado.



Para obtener más información sobre el árbol de grupos consulta el capítulo 7.

Desde el árbol de grupos

Para asignar un perfil de configuración a un conjunto de equipos que pertenecen a un grupo, haz clic menú superior **Equipos**, selecciona el árbol de grupos en el panel izquierdo y sigue los pasos mostrados a continuación:

- Haz clic en el menú contextual en la rama apropiada del árbol de grupos.
- Haz clic en el menú emergente **Configuraciones**, se mostrará una ventana con los perfiles ya asignados al grupo seleccionado y el tipo de asignación:
 - **Manual / Asignación directa:** mediante la leyenda **Asignada directamente a este grupo**.
 - **Heredada / Asignación indirecta:** mediante la leyenda **Configuración heredada de** y el nombre del grupo junto con la ruta completa para llegar al mismo, y que recibió la configuración manual de la cual se hereda.
- Elige la nueva configuración y haz clic en **Aceptar** para asignar la configuración al grupo.
- La configuración se propagará de forma inmediata a todos los miembros del grupo y sus descendientes.
- Los cambios se aplicarán en los equipos afectados de forma inmediata.

Desde el panel listado de equipos

Para asignar un perfil de configuración a un equipo en concreto sigue los pasos mostrados a continuación:

- En el menú superior **Equipos** haz clic en el grupo o filtro donde reside el equipo a asignar la configuración. Haz clic sobre el equipo en la lista de equipos mostrada en el panel derecho para ver la pantalla detalles de equipo.
- Haz clic en la pestaña **Configuración**. Se mostrarán los perfiles asignados al equipo y el tipo de asignación:
 - **Manual / Asignación directa:** mediante la leyenda **Asignada directamente a este**

grupo.

- **Heredada / Asignación indirecta:** mediante la leyenda **Configuración heredada de** y el nombre del grupo junto con la ruta completa para llegar al mismo, y que recibió la configuración manual de la cual se hereda.

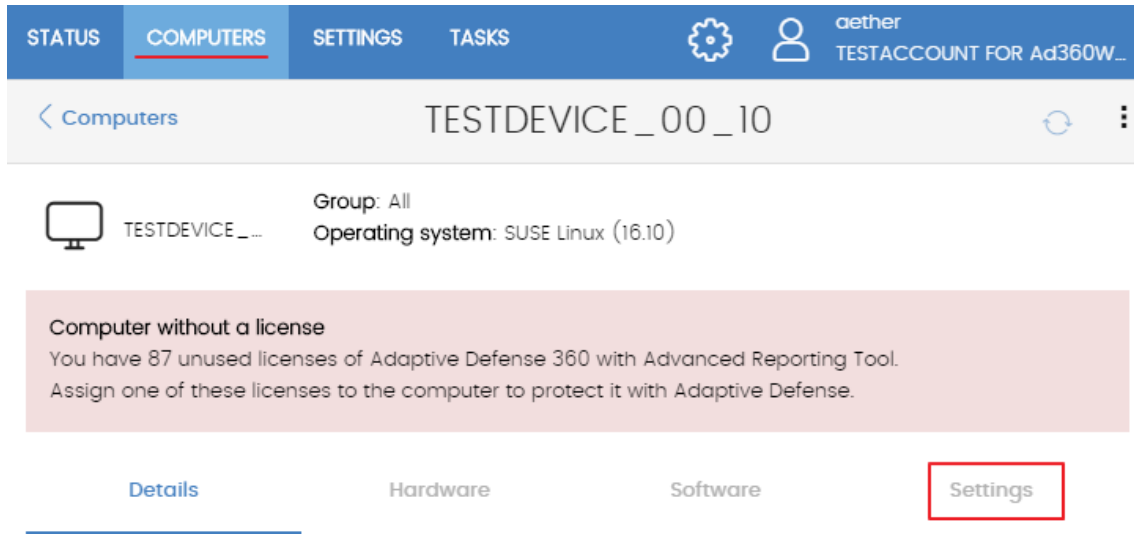



Figura 44: acceso a las configuraciones desde la ficha de equipo

- Selecciona la nueva configuración. Ésta se aplicará de forma automática al equipo.

Desde el propio perfil de configuración

Si quieres asignar una configuración a uno o varios equipos con completa libertad y sin necesidad de que pertenezcan a un mismo grupo, sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, haz clic en el panel de la izquierda el tipo de perfil que quieres asignar.
- Selecciona la configuración de entre las disponibles y haz clic en el botón **Seleccionar equipos**. Se mostrarán los equipos que ya tienen asignado ese perfil.
- Haz clic en el botón  para añadir los equipos que quieras añadir.
- Haz clic en el botón **Añadir**. El perfil quedará asignado a los equipos seleccionados y la nueva configuración se aplicará entre los equipos de forma inmediata.



Al retirar un equipo de la lista de equipos asignados a una configuración, el equipo retirado volverá a heredar las configuraciones asignadas de forma directa o indirecta del grupo al que pertenece. La consola de administración resaltará este hecho mostrando una ventana de advertencia antes de aplicar los cambios.

8.7.2 Asignación indirecta de configuraciones: las dos reglas de la herencia

La asignación indirecta de configuraciones se realiza a través del mecanismo de la herencia, que permite propagar de forma automática un mismo perfil de configuración a todos los equipos subordinados del nodo sobre el cual se asignó la configuración.

Las reglas que rigen la interacción entre los dos tipos de asignaciones (manuales / directas y automática / herencia) se muestran a continuación por orden de prioridad:

- 1 **Regla de la herencia automática:** un grupo o equipo hereda de forma automática las configuraciones del grupo del cual depende (grupo padre o de orden superior).



Figura 45: ejemplo de herencia / asignación indirecta. El grupo padre recibe una configuración que se propaga a sus nodos hijos

- 2 **Regla de la prioridad manual:** Una configuración manual prevalece sobre una configuración heredada.

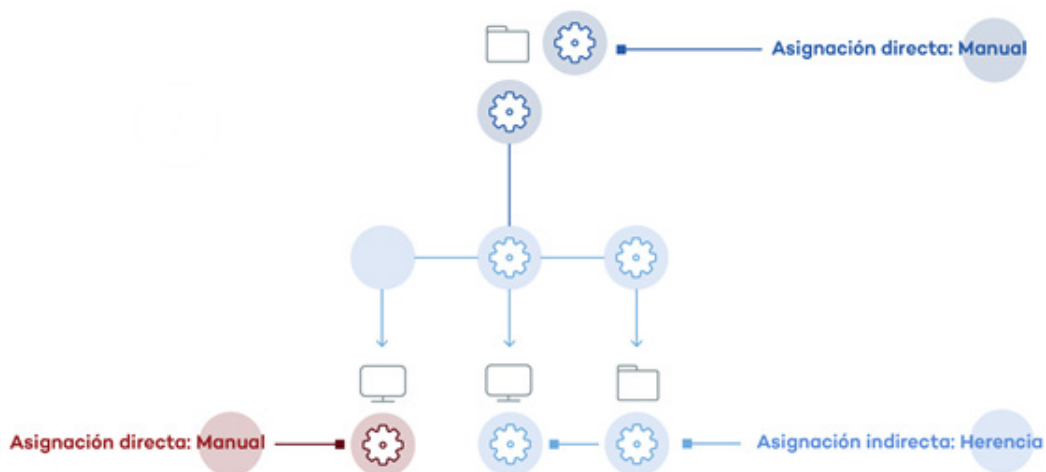


Figura 46: ejemplo de prioridad de la asignación directa sobre indirecta. La configuración heredada se sobrescribe con la configuración manual del nodo.

8.7.3 Límites de la herencia

La configuración asignada a un grupo (manual o heredada) se heredará a todos los elementos de la rama del árbol sin limite, hasta que se encuentre una asignación manual.

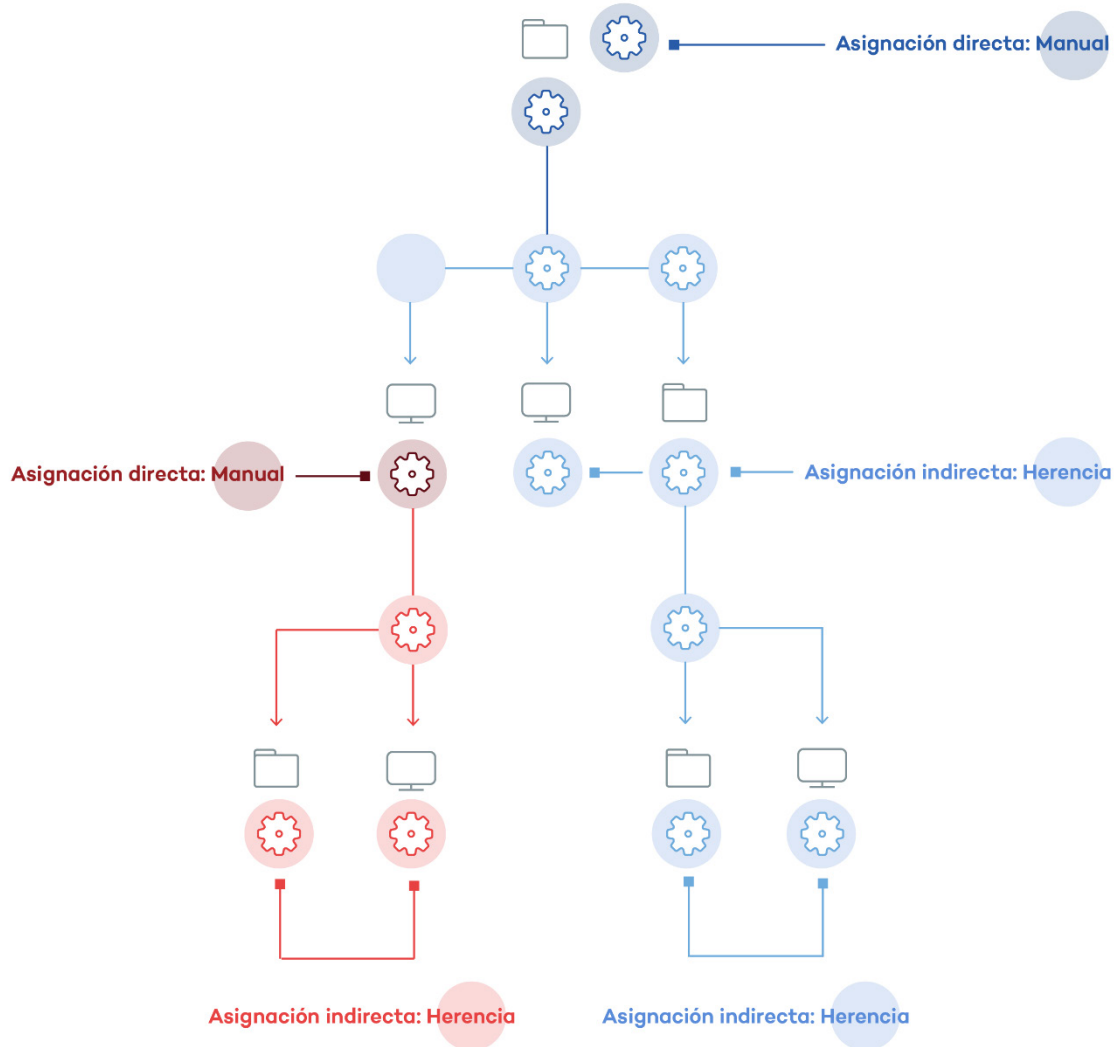


Figura 47: ejemplo de herencia limitada por asignación manual / directa. La configuración del nodo padre se hereda a sus descendientes, pero se detiene ante una configuración manual

8.7.4 Sobre escritura de configuraciones

Como se ha visto en el punto anterior, la regla 2 (prioridad manual) dicta que las configuraciones manuales prevalecen sobre las configuraciones heredadas. Esto es así en un escenario típico donde primero se establecen las configuraciones heredadas sobre todos los elementos del árbol, y luego se asignan de forma manual aquellas configuraciones especiales sobre ciertos elementos.

Sin embargo, es frecuente que una vez establecidas las configuraciones heredadas y manuales, haya un cambio de configuración heredada en un nodo de orden superior que afecta a la configuración manual de un descendiente.

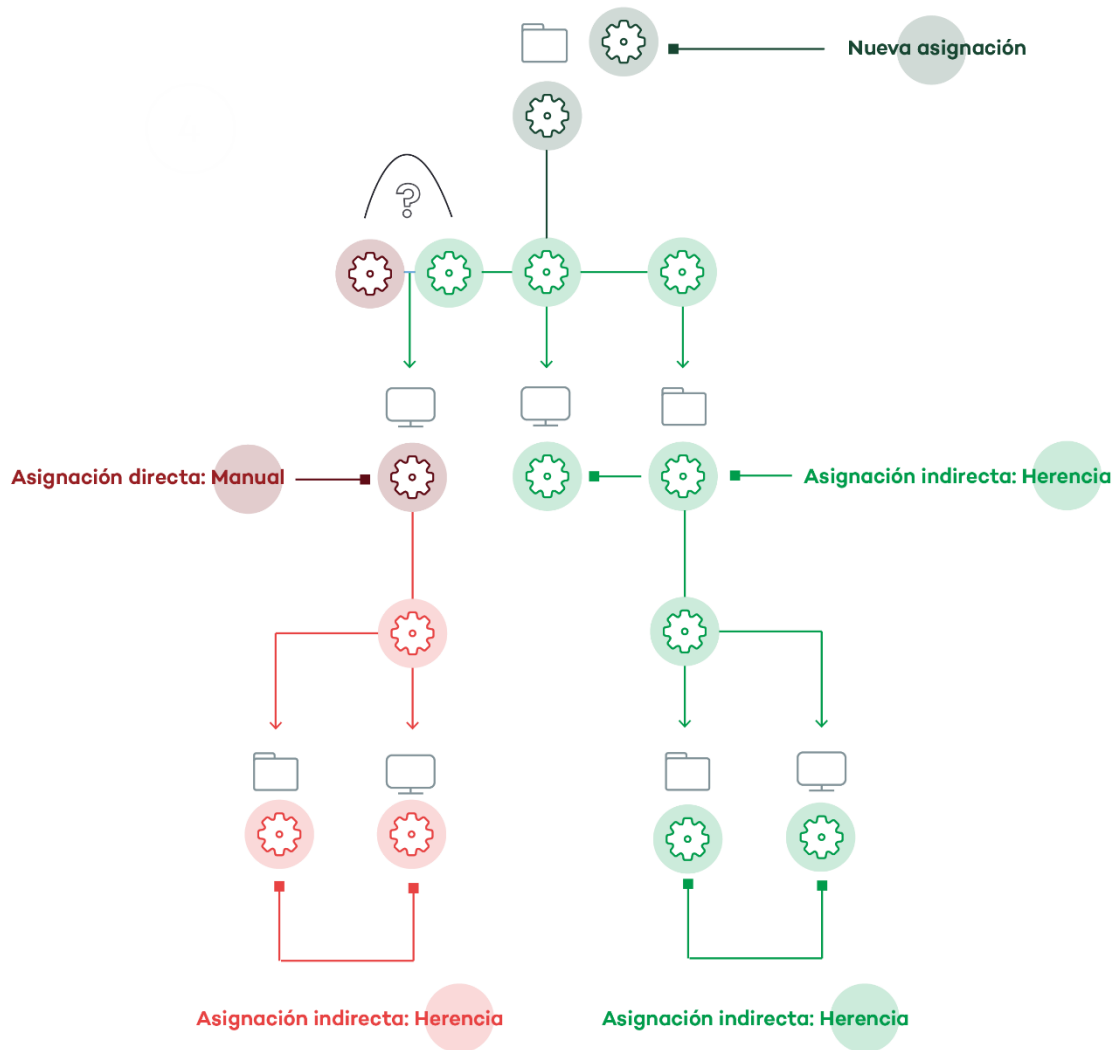


Figura 48: cambio de configuración heredada de nivel superior existiendo previamente una configuración manual en un nodo inferior

En este caso, **Endpoint Protection / Plus** pregunta al administrador si las configuraciones manuales establecidas previamente se mantendrán o se sobrescribirán mediante la herencia:

- Si las configuraciones heredadas tienen prioridad, la nueva configuración se heredará a todos los elementos subordinados, independientemente de si tienen configuraciones manuales establecidas o no, borrando por lo tanto las configuraciones manuales si las hubiera
- Si las configuraciones manuales tienen prioridad, la nueva configuración solo se heredará en aquellos grupos donde no se haya establecida ninguna configuración manual previa, conservando las configuraciones manuales existentes.

Some subgroups and/or computers have settings that have been directly assigned to them, instead of inherited from this group.

What do you want to do with the settings directly assigned to your subgroups and/or computers?

Keep all settings

Make all inherit these settings

Figura 49: ventana de selección del comportamiento en cambios de configuración que se propagarán sobre una rama con grupos configurados manualmente

De esta manera, cuando el sistema detecte un cambio de configuración que tenga que propagar a los nodos subordinados, y alguno de estos tenga una configuración manual (sin importar el nivel en el que se encuentre) se presentará la pantalla de selección, preguntando al administrador sobre el comportamiento a seguir: **Hacer que todos hereden esta configuración** o **Mantener todas las configuraciones**.

Hacer que todos hereden esta configuración



¡Utiliza esta opción con mucho cuidado, esta acción no tiene vuelta atrás! Todas las configuraciones manuales que cuelguen del nodo se perderán y se aplicará la configuración heredada de forma inmediata en los equipos. El comportamiento de Endpoint Protection / Plus podrá cambiar en muchos equipos de la red.

La nueva asignación directa (1) se propagará mediante la herencia a todo el árbol por completo, sobrescribiendo la asignación directa anterior (2) y llegando hasta los nodos hijos de ultimo nivel (3) y (4).

Mantener todas las configuraciones

La nueva configuración solo se propagará a aquellos nodos subordinados que no tengan configuraciones manuales establecidas.

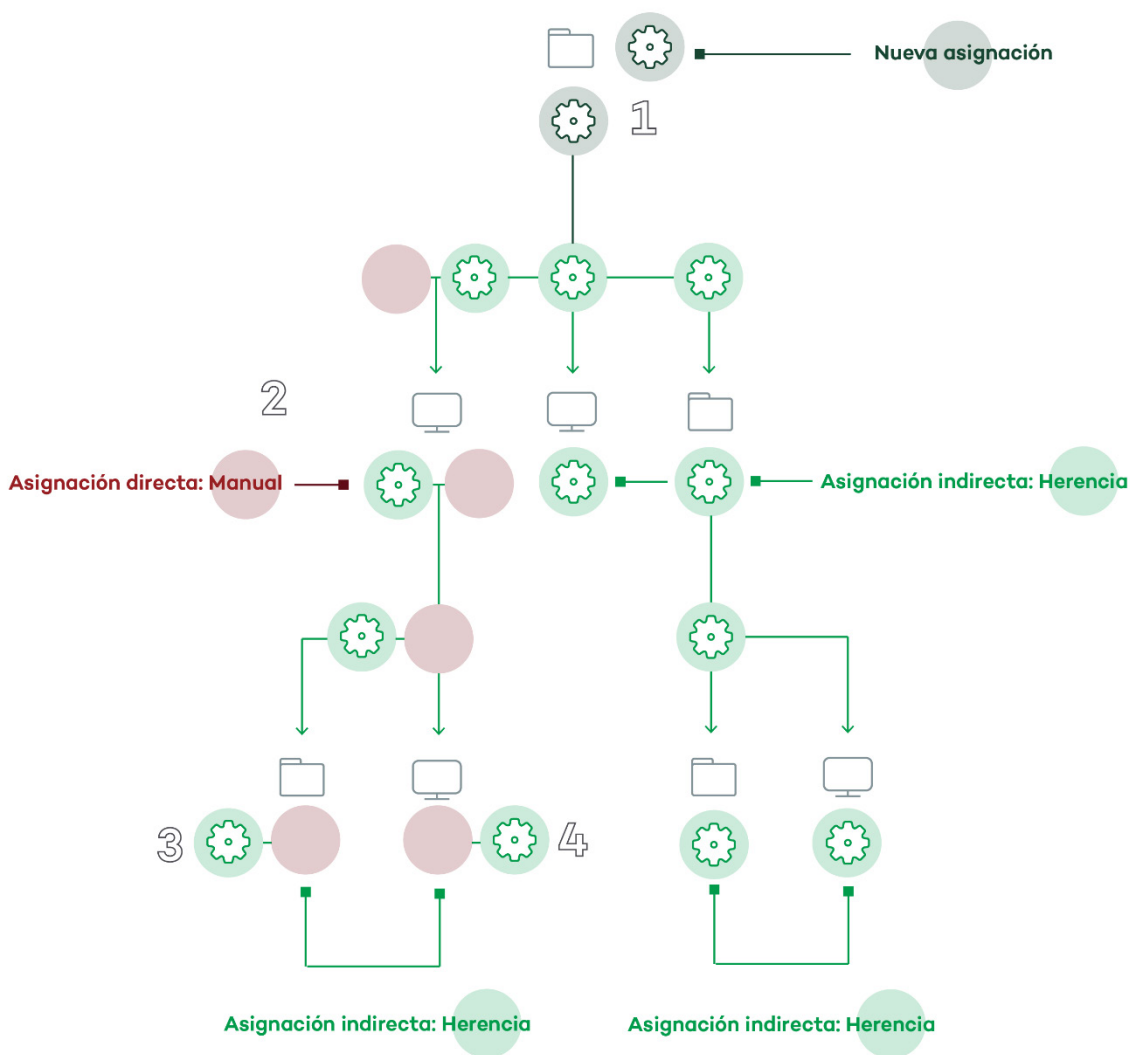


Figura 50: las configuraciones manuales se invalidan y se hereda la configuración establecida en el nodo padre

Si eliges la opción de mantener las configuraciones establecidas de forma manual, la propagación de la nueva configuración heredada se detiene en el primer nodo configurado manualmente. Aunque los nodos subordinados a un nodo configurado de forma manual heredan su configuración, la propagación de la nueva configuración se detiene en el primer nodo del árbol que tiene la configuración manual. En la figura, la propagación de la configuración establecida en (1) se detiene en el nodo (2), de modo que los nodos (3) y (4) no reciben esa nueva configuración, aun utilizando el mecanismo de la herencia para recoger su configuración.

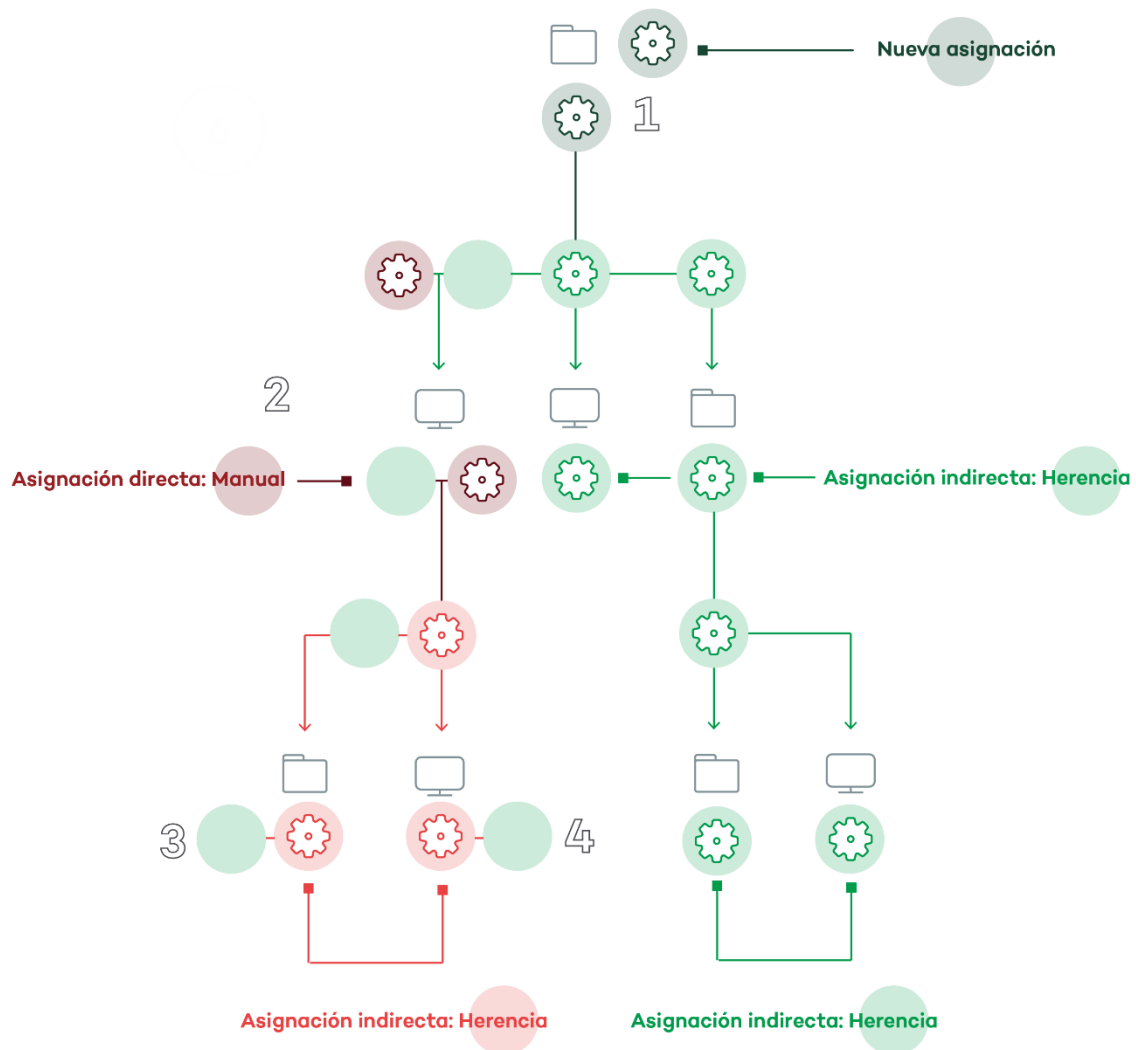


Figura 51: las configuraciones manuales se mantienen

8.7.5 Eliminación de asignaciones manuales y restauración de la herencia

Para eliminar una asignación manual realizada sobre una carpeta y volver a heredar la configuración de la rama padre, es necesario seguir los pasos mostrados a continuación:

- En el menú superior **Equipos** haz clic en el grupo que tiene la asignación manual a eliminar, en el árbol de grupos situados en el panel izquierdo.
- Haz clic en el icono de menú contextual de la rama apropiada. Se mostrará una ventana emergente con las configuraciones asignadas. Elige el perfil que esté asignado de forma manual y se quiera eliminar.
- Se desplegará un listado con todos los perfiles disponibles para realizar una nueva asignación manual, y al final de la lista se mostrará el botón **Heredar del grupo padre** junto con información de la configuración que se heredaría si se pulsara el botón, y el grupo del cual se heredaría.

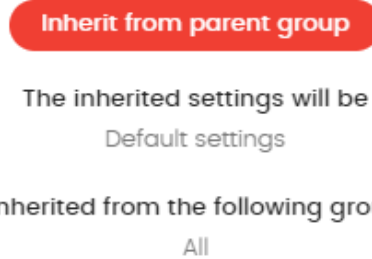


Figura 52: botón para eliminar una configuración manual y restablecer la herencia

8.7.6 Movimiento de grupos y equipos

Al mover un equipo o grupo de equipos a otra rama del árbol, el comportamiento de **Endpoint Protection / Plus** con respecto a las configuraciones a aplicar varía en función de si los elementos movidos son grupos completos o equipos individuales.

Movimiento de equipos individuales

En el caso de movimiento de equipos individuales, **Endpoint Protection / Plus** respeta las configuraciones manuales establecidas sobre los equipos movidos, y sobrescribe de forma automática las configuraciones heredadas con las configuraciones establecidas en el nuevo grupo padre.

Movimiento de grupos

En el caso de movimiento de grupos, **Endpoint Protection / Plus** mostrará una ventana con la pregunta "¿Quieres que las configuraciones asignadas a este grupo mediante herencia, sean sustituidas por las del nuevo grupo padre?"

- En el caso de contestar **SI** el procedimiento será el mismo que en el movimiento de equipos: las configuraciones manuales se respetarán y las heredadas se sobrescribirán con las configuraciones establecidas en el grupo padre.
- En el caso de contestar **NO**, las configuraciones manuales se seguirán respetando, pero las configuraciones heredadas originales del grupo movido prevalecerán, pasando de esta forma a ser configuraciones manuales.

8.8. Visualizar las configuraciones asignadas

La consola de administración implementa hasta cuatro formas de mostrar los perfiles de configuración asignados a un grupo o equipo:

- En el árbol de grupos
- En los listados de configuraciones
- En la pestaña **Configuración** del equipo
- En el listado de equipos exportado

Árbol de grupos

Seleccionando el menú de contexto de la rama apropiada y haciendo clic en el menú emergente **Configuraciones** se mostrará una ventana con las configuraciones asignadas.

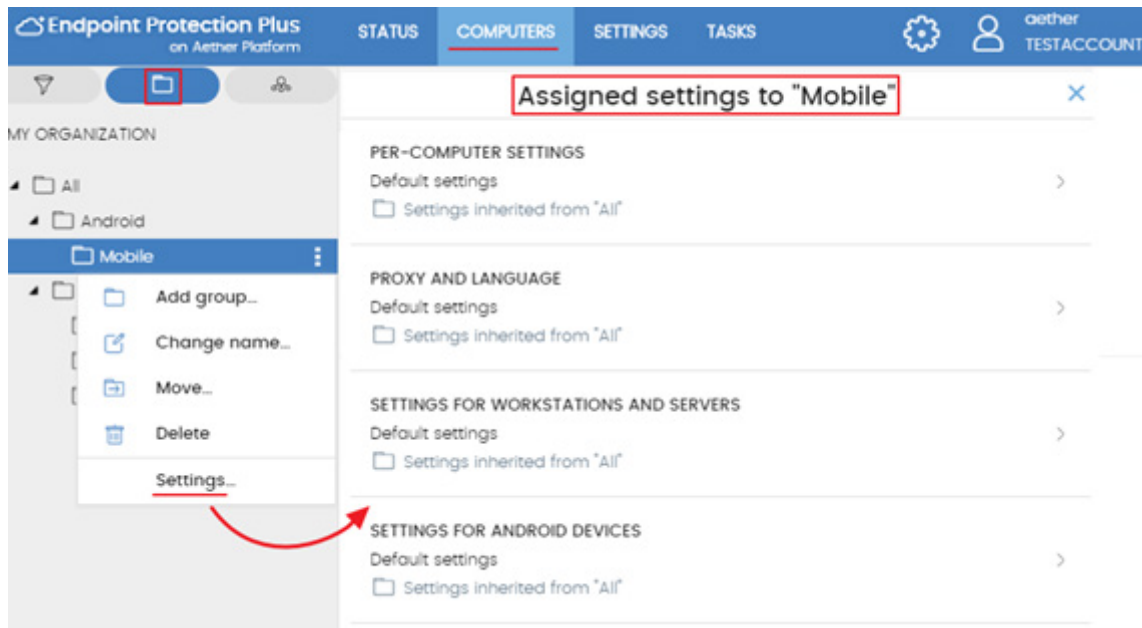




Figura 53: configuraciones asignadas desde el árbol de grupos

A continuación, se indica la información mostrada por cada entrada:

- **Tipo de configuración:**
 - Configuración de proxy e idioma
 - Configuración de ajustes por equipo
 - Configuración para estaciones y servidores
 - Configuración para dispositivos Android
- **Nombre de la configuración:** nombre asignado por el administrador en la creación de la configuración.
- **Tipo de herencia aplicada:**
 - **Configuración heredada de...:**  la configuración fue asignada a la carpeta padre indicada, y los equipos que pertenecen a la rama actual la heredan.
 - **Asignada directamente a este grupo:**  la configuración de los equipos es la que el administrador asigno de forma manual a la carpeta.

Pestaña configuración del equipo

En el menú superior **Equipos**, seleccionando un equipo del panel de la derecha se mostrará la ventana de detalle. En la pestaña **Configuración** se listan los perfiles asignados al equipo.

Exportar listado de equipos

Desde el árbol de equipos (árbol de grupos o árbol de filtros) es posible exportar el listado de equipos mostrado en formato csv, haciendo clic en el menú contextual y eligiendo la opción Exportar. En el listado csv se incluyen los siguientes campos informativos:

- Configuración de proxy e idioma
- Configuración heredada de
- Configuración de seguridad para estaciones y servidores
- Configuración heredada de
- Configuración de seguridad para dispositivos Android
- Configuración heredada de
- Ajuste por equipo
- Configuración heredada de

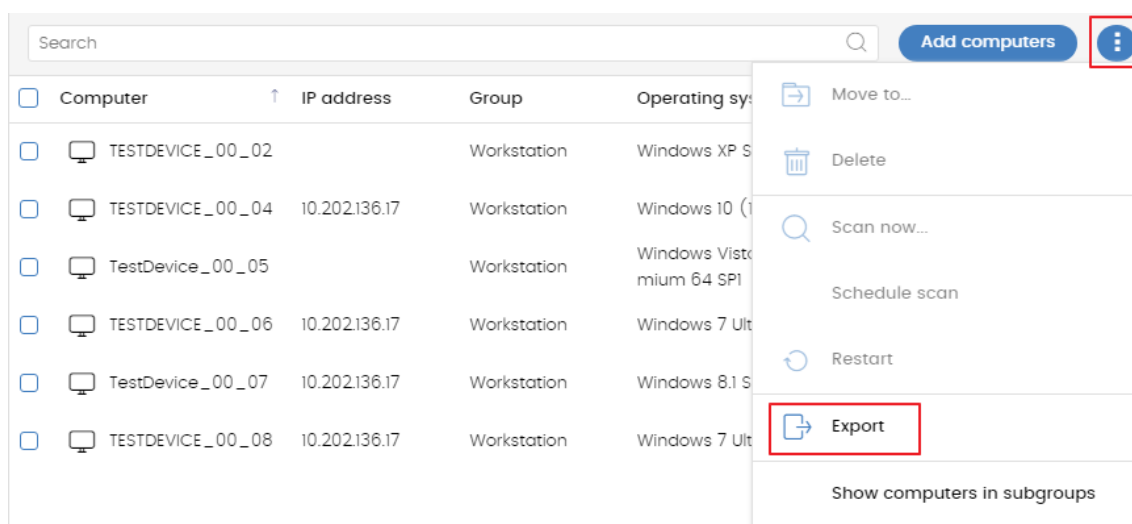


Figura 54: exportación del listado de equipos en formato csv



Consulta el capítulo 7 para obtener una descripción completa de todos los campos del fichero csv exportado.

9. Configuración del agente y la protección local

Roles del agente
Acceso vía proxy
Comunicación en tiempo real
Idiomas
Contraseña y anti-tampering

9.1. Introducción

El administrador puede cambiar el funcionamiento de varios aspectos del agente Panda instalado en los equipos de la red:

- El papel o rol que el equipo representa para el resto de puestos y servidores protegidos.
- Las protecciones frente al *tampering* o manipulación indebida del software **Endpoint Protection / Plus** por parte de amenazas avanzadas y APTs.
- Configuración del tipo de comunicación de los equipos con la nube de **Panda Security**.

9.2. Configuración de los roles del agente Panda

El agente Panda instalado en los equipos de la red puede tener tres roles diferentes:

- Proxy
- Descubridor
- Cache

Para asignar un rol a un equipo con el agente Panda ya instalado haz clic en el menú superior **Configuración** y en el panel lateral **Configuración de red**. Se mostrarán tres pestañas: **Proxy e idioma**, **Cache** y **Descubrimiento**.

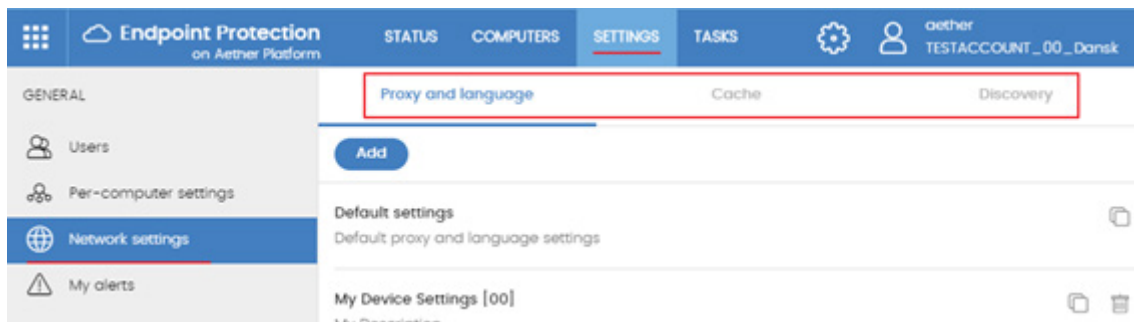


Figura 55: pantalla de selección de configuración de rol

9.2.1 Rol de Proxy


Para los equipos que no tienen acceso directo a internet, **Panda Endpoint Protection / Plus** permite la utilización del proxy instalado en la red. En el caso de no existir ningún proxy accesible, es posible asignar el rol de proxy a un equipo con **Endpoint Protection / Plus** instalado.

Asignar el rol de proxy a un equipo

- Haz clic en la pestaña **Proxy e idioma** y selecciona una configuración de tipo **Proxy e idioma** ya generada o crea una nueva.
- Despliega la sección **Proxy** y selecciona **Endpoint Protection / Plus proxy**.

- Haz clic en **Seleccionar equipo**.
- En la ventana de selección de equipo haz clic en **Añadir proxy**. Se mostrará un listado de todos los equipos administrados que no tengan el rol de proxy previamente asignado.
- Selecciona los equipos que servirán de proxy para el resto de puestos y servidores protegidos con **Endpoint Protection / Plus**.

Retirar el rol de cache a un equipo

- Haz clic en la pestaña **Proxy e idioma** y selecciona una configuración de tipo **Proxy e idioma** ya generada o crea una nueva.
- Despliega la sección **Proxy** y selecciona **Endpoint Protection / Plus proxy**
- Haz clic en **Seleccionar equipo**.
- Haz clic en el icono  del equipo que quieres retirar el rol de proxy.

9.2.2 Rol de Cache / repositorio


Endpoint Protection / Plus permite asignar el rol de caché a uno o más puestos de la red. Estos equipos descargan y almacenan de forma automática todos los ficheros necesarios para que otros puestos con **Endpoint Protection / Plus** instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección, sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Asignar el rol de cache a un equipo

- Haz clic en la pestaña superior **Cache** dentro de **Configuración, Configuración de red**.
- Haz clic en el botón **Añadir equipo caché**.
- Utiliza la herramienta de búsqueda situada en la parte superior de la ventana para localizar rápidamente equipos candidatos a tener el rol de cache.
- Selecciona uno o varios equipos de la lista y pulsa **Aceptar**.

A partir de ese momento el equipo seleccionado adoptará el rol de caché y comenzará la descarga de todos los archivos necesarios, manteniendo sincronizado su repositorio de forma automática. El resto de los puestos de la subred contactarán con el cache para la descarga de actualizaciones.

Retirar el rol de cache a un equipo

- Haz clic en el menú superior **Configuración**, panel lateral **Configuración de red**, pestaña **Caché**.
- Haz clic en el icono  del equipo que quieres retirar el rol caché.

Requisitos y limitaciones de un equipo con rol cache

- Se requieren como máximo 2 Gigabytes adicionales de espacio en disco para almacenar todas las descargas.

- El ámbito de un equipo con rol de cache está limitado al segmento de red al que esté conectada su interface. Si un equipo cache tiene varias tarjetas de red podrá servir de repositorio en cada uno de los segmentos a los que esté conectado.



Se recomienda asignar un equipo como rol cache en cada segmento de la red de la compañía.

- El resto de equipos descubrirán de forma automática la presencia de un nodo cache y redirigirán hacia él sus peticiones de actualización.
- Se requiere la asignación de una licencia de protección al nodo cache para su funcionamiento.
- La configuración del cortafuegos debe de permitir el tráfico SSDP (uPnP) entrante y saliente en el puerto UDP 21226 y 18226 TCP.

Descubrir nodos cache

En el momento de la asignación del rol al equipo, éste lanzará un broadcast hacia los segmentos de red a los que pertenecen sus interfaces. Los puestos recibirán la publicación del servicio y, en el caso de que en un mismo segmento haya más de un nodo cache designado, los equipos se conectarán al más adecuado en función de los recursos libres que posea.

Adicionalmente, cada cierto tiempo los equipos de la red preguntarán si existe algún nodo con el rol de cache instalado.

9.2.3 Rol de descubridor

La pestaña **Descubrimiento** está directamente relacionada con el procedimiento de instalación y despliegue de **Endpoint Protection / Plus** en la red del cliente. Consulta el capítulo 6 para obtener más información acerca del proceso de descubrimiento e instalación de **Endpoint Protection / Plus**.

9.3. Configuración del acceso a través de proxy

Configurar el uso de proxy

Para configurar la salida de uno o varios equipos a través de un proxy es necesario crear una configuración de tipo **Proxy e idioma**. Sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma**.
- Haz clic en el botón **Editar** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** elige el tipo de proxy a asignar a los equipos.
 - **No usar proxy**: acceso directo a Internet.
 - **Proxy corporativo**: acceso a Internet vía proxy instalado en la red de la organización.
 - **Proxy Panda Endpoint Protection / Plus**: acceso a través del agente **Endpoint Protection / Plus** instalado en un equipo de la red.

- **No usar proxy**

Los equipos sin una configuración de proxy acceden de forma directa a la nube de Panda Security para descargar las actualizaciones y enviar los reportes de estado del equipo. El software **Endpoint Protection / Plus** utilizará la configuración del equipo para comunicarse con Internet.

- **Proxy corporativo**

- **Dirección:** dirección IP del servidor de proxy.
- **Puerto:** puerto del servidor de proxy.
- **El proxy requiere autenticación:** habilitar si el proxy requiere información de usuario y contraseña.
- **Usuario**
- **Contraseña**

- **Proxy de Panda Endpoint Protection / Plus**

Permite centralizar todas las comunicaciones de la red a través de un equipo con un agente Panda instalado.

Para configurar el envío de las comunicaciones del equipo a un proxy **Panda Endpoint Protection / Plus** haz clic en el link **Seleccionar equipo** para desplegar una ventana con el listado de equipos disponibles que tienen el rol de proxy en la red.



En las máquinas designadas como Proxy Panda Endpoint Protection / Plus, los puertos UDP 21226 y TCP 3128 no podrán ser utilizados por otras aplicaciones. Adicionalmente la configuración del cortafuegos del equipo deberá de permitir el tráfico entrante y saliente por ambos puertos.

Mecanismo de fallback

Cuando un agente Panda no puede conectar con la plataforma **Aether** se ejecuta la siguiente lógica de fallback para restaurar la conexión mediante otro camino disponible:

- Si la salida a internet estaba configurada a través de proxy corporativo o proxy Panda Endpoint Protection / Plus y no responde, se intenta el acceso directo.
- Internet Explorer: el agente Panda intenta recuperar la configuración de proxy de Internet Explorer impersonado como el usuario logeado en el equipo.
 - Si la configuración de las credenciales para el uso del proxy está definida de forma explícita este método de acceso no se podrá utilizar.
 - Si la configuración de proxy de Internet Explorer utiliza PAC (Proxy Auto-Config) se recupera la URL del archivo de configuración, siempre que el protocolo de acceso al recurso sea HTTP o HTTPS.

- WinHTTP / WinInet: se lee la configuración del proxy por defecto.
- WPAD (Web Proxy Autodiscovery Protocol): se pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración.

9.4. Configuración de la comunicación en tiempo real

Las comunicaciones en tiempo real entre los equipos protegidos y el servidor **Endpoint Protection / Plus** requieren el mantenimiento de una conexión abierta por cada puesto de forma permanente. En aquellos casos donde el número de conexiones abiertas afecte al rendimiento del proxy instalado en la red, o el impacto en el consumo de ancho de banda sea elevado al cambiar simultáneamente las configuraciones de un gran número de equipos, puedes desactivar las comunicaciones en tiempo real.

Deshabilitar las comunicaciones en tiempo real

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma**.
- Haz clic en el botón **Editar** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** despliega la sección **Opciones avanzadas**.
- Desactiva la casilla **Activar la comunicación en tiempo real**.

Al deshabilitar las comunicaciones en tiempo real, los equipos se comunicarán con el servidor **Endpoint Protection / Plus** cada 15 minutos.

9.5. Configuración del idioma del agente

Para asignar el idioma del agente Panda a uno o varios equipos es necesario crear una configuración de tipo **Proxy e idioma**. Sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red**, pestaña **Proxy e idioma**.
- Haz clic en el botón editar o selecciona una configuración ya creada para modificarla.
- En la sección idioma elige el idioma de entre los disponibles:
 - Español
 - Inglés
 - Sueco
 - Francés
 - Italiano
 - Alemán
 - Portugués

- Húngaro
- Ruso
- Japonés
- Finlandés (consola local)



Si se produce un cambio de idioma y la consola local de Endpoint Protection / Plus estaba abierta se pedirá un reinicio de la consola local. Este procedimiento no afecta a la seguridad del equipo.

9.6. Configuración de contraseña y anti-tampering

9.6.1 Anti-tamper

Muchas amenazas avanzadas incorporan técnicas para desactivar el software de seguridad instalado en los equipos y así sortear todas sus funcionalidades de protección. Este comportamiento también es práctica habitual de los hackers y **Endpoint Protection / Plus** incorpora tecnología *anti-tamper* que impide la modificación no autorizada del funcionamiento de la solución.

Habilitar anti-tamper

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes de equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**:
 - **Activar anti-tamper**: impide que los usuarios o ciertos tipos de malware puedan detener las protecciones. Requiere el establecimiento de una contraseña ya que es posible que el administrador o el equipo de soporte necesiten detener temporalmente desde la consola local las protecciones para diagnosticar problemas.

9.6.2 Protección del agente mediante contraseña

Para evitar que el usuario modifique las características de protección o desinstale completamente el software **Endpoint Protection / Plus**, el administrador puede establecer una contraseña local que cubra ambos casos.

Asignar una contraseña local

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes de equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad frente a manipulaciones no deseadas de las protecciones**:
 - **Solicitar contraseña para desinstalar Aether desde los equipos**: evita que el usuario desinstale el software Endpoint Protection / Plus protegiéndolo con una contraseña.
 - **Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos**: permite administrar las capacidades de seguridad del equipo desde la consola local. Requiere el establecimiento de una contraseña.

10. Configuración de seguridad para estaciones y servidores

- Introducción a la configuración de estaciones y servidores
- Configuración general
 - Antivirus
 - Firewall
 - Control de dispositivos
 - Control de acceso a páginas web
 - Antivirus para servidores Exchange
 - Anti Spam para servidores Exchange
 - Filtrado de contenidos para servidores Exchange

10.1. Introducción

Endpoint Protection / Plus centraliza en el menú superior **Configurar** toda la configuración de seguridad para estaciones de trabajo y servidores. Haciendo clic en el panel de la izquierda **Estaciones y servidores** se mostrará un listado con todas las configuraciones de seguridad ya creadas.

En este capítulo explican todos los parámetros incluidos en la configuración de seguridad para estaciones y servidores. También se indicarán algunas recomendaciones prácticas para asegurar los puestos de trabajo de la red, minimizando los inconvenientes en su manejo al usuario.

10.2. Introducción a la configuración de estaciones y servidores

La configuración para estaciones y servidores se divide en 8 apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con su configuración asociada. A continuación, se muestran los 8 apartados con una breve explicación.

- **General:** establece el comportamiento de las actualizaciones, desinstalaciones de la competencia y exclusiones de ficheros que no se analizarán.
- **Antivirus:** establece el comportamiento de la protección antimalware tradicional frente a virus y amenazas.
- **Firewall (Dispositivos Windows):** establece el comportamiento del cortafuegos y del IDS que protege al equipo de los ataques de red.
- **Control de dispositivos (Dispositivos Windows):** determina el acceso del usuario a los periféricos conectados al equipo.
- **Control de acceso a páginas web (solo Endpoint Protection Plus):** regula las visitas del usuario a categorías de páginas web.
- **Antivirus para servidores Exchange (solo Endpoint Protection Plus):** analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de amenazas.
- **Anti spam para servidores Exchange (solo Endpoint Protection Plus):** analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de correo no deseado.
- **Filtrado de contenidos para servidores Exchange (solo Endpoint Protection Plus):** regula el tipo de contenidos que puede recibir el servidor Exchange.

Funcionalidad	Windows	Mac OS X	Linux	Windows Exchange
Antivirus	X	X	X	X
Firewall & IDS	X			
Protección de correo	X			
Protección web	X	X	X	
Control de dispositivos	X			

Control de acceso a páginas web	X	X	X
Anti-Spam			X
Filtrado de contenidos			X

Tabla 12: funcionalidades de seguridad por plataforma de usuario

10.3. Configuración General

La configuración general permite establecer el comportamiento de **Endpoint Protection / Plus** en lo relativo a las actualizaciones, desinstalación de programas de la competencia y exclusiones de ficheros y carpetas que no se analizarán por el antivirus tradicional.

10.3.1 Actualizaciones

Consulta el capítulo 12 Actualización del Software para obtener información acerca de los procedimientos necesarios para actualizar el agente, la protección y el fichero de firmas de software instalado en el equipo del usuario.

10.3.2 Desinstalar otros productos de seguridad

Consulta el capítulo 6 Instalación del software Endpoint Protection / Plus para establecer el comportamiento de la instalación de la protección en el caso de que otro producto de seguridad este instalado previamente en el equipo del usuario.



Consulta el Apéndice III: Listado de desinstaladores para obtener un listado de todos los productos de la competencia que Endpoint Protection / Plus es capaz de desinstalar automáticamente del equipo del usuario.

10.3.3 Exclusiones

Exclusiones configura los elementos del equipo que no serán analizados en busca de malware.

Ficheros en disco

Se indican los ficheros en el disco de los equipos protegidos que no serán analizados por **Endpoint Protection / Plus**.

- **Extensiones:** permite especificar extensiones de ficheros que no serán analizadas.
- **Carpetas:** permite especificar carpetas cuyo contenido no será analizado.
- **Ficheros:** permite especificar ficheros específicos que no serán analizados.
- **Exclusiones recomendadas para Exchange:** al hacer clic en el botón **Añadir**, se cargan de forma automática las exclusiones recomendadas por Microsoft para optimizar el

rendimiento del producto en servidores Exchange.

Excluir archivos adjuntos de correo:

Permite especificar una lista de extensiones de ficheros que no serán analizados en el caso de encontrarse como adjuntos en mensajes de correo.

10.4. Antivirus

En esta sección podrás configurar el comportamiento general del motor de antivirus basado en ficheros de firmas.

- **Protección de archivos:** activa o desactiva la protección antivirus relativa al sistema de ficheros.
- **Protección de correo:** activa o desactiva la protección antivirus relativa al cliente de correo instalado en el equipo del usuario.
- **Protección web:** activa o desactiva la protección antivirus relativa al cliente web instalado en el equipo del usuario.

La acción a ejecutar por **Endpoint Protection / Plus** ante un fichero de tipo malware o sospechoso queda definida en los laboratorios de Panda Security y sigue las siguientes reglas:

- **Ficheros conocidos como malware desinfectable:** se desinfectan y se elimina el fichero original quedando sustituido por una copia desinfectada y sin peligro para el usuario.
- **Ficheros conocidos como malware no desinfectable:** Para los casos en los que no sea posible una desinfección se guarda una copia de seguridad y el fichero original se elimina.

10.4.1 Amenazas a detectar

Permite configurar el tipo de amenazas que **Endpoint Protection / Plus** buscará y eliminará en el sistema de archivos, cliente de correo y web instalados en el equipo del usuario.

- **Detectar virus**
- **Detectar herramientas de hacking y PUPs**
- **Bloquear acciones maliciosas:** activa tecnologías anti exploit y heurísticas que analizan localmente el comportamiento de los procesos, buscando actividades sospechosas.
- **Detectar Phishing**

10.4.2 Tipos de archivos

En esta sección se establecen los tipos de archivos que **Endpoint Protection / Plus** analizará:

- **Analizar comprimidos en disco**
- **Analizar comprimidos en mensajes de correo**

- **Analizar todos los archivos independientemente de su extensión cuando son creados o modificados (No recomendado):** por cuestiones de rendimiento no se recomienda analizar todos los ficheros ya que muchos tipos de ficheros de datos no pueden presentar amenazas a la seguridad del equipo.

10.5. Firewall (Equipos Windows)

Endpoint Protection / Plus ofrece tres herramientas básicas para filtrar el tráfico de red que recibe o envía los equipos protegidos:

- **Protección mediante reglas de sistema:** son las reglas que describen características de las comunicaciones establecidas por el equipo (puertos, IPs, protocolos etc), con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas configuradas.
- **Protección de programas:** establece un conjunto de reglas que permitan o denieguen la comunicación a determinados programas instalados en el equipo de usuario.
- **Sistema de detección de intrusos:** permite detectar y rechazar patrones de tráfico malformado que afecten a la seguridad o al rendimiento del equipo protegido.

10.5.1 Modo de funcionamiento

Se distinguen dos modos de funcionamiento, accesibles mediante el control **La configuración firewall la establece el usuario de cada equipo:**

- **Activado** (firewall en modo usuario o auto administrado): el propio usuario podrá configurar desde la consola local el firewall de su equipo.
- **Desactivado** (firewall en modo administrador): el administrador configura el cortafuegos de los equipos a través de perfiles de configuración.

10.5.2 Tipo de red

Los equipos de usuario portátiles pueden conectarse a redes con un grado de seguridad muy diverso, según se trate de accesos públicos como la red wifi de un cibercafé, o redes gestionadas o de acceso limitado como la red de la empresa. Para ajustar el comportamiento por defecto del cortafuegos, el administrador de la red deberá de seleccionar el tipo de red al que se conectan usualmente los equipos del perfil configurado.

- **Red pública:** son las redes que se encuentran en cibercafés, aeropuertos, etc. Implica establecer limitaciones en el nivel de visibilidad de los equipos protegidos y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.
- **Red de confianza:** son las redes que se encuentran en oficinas y domicilios. El equipo es perfectamente visible para el resto de usuarios de la red, y viceversa. No hay limitaciones al compartir archivos, recursos y directorios.

La variación del comportamiento del software **Endpoint Protection / Plus** según la red seleccionada se refleja en la consola en el número de reglas añadidas de forma automática. Estas reglas se pueden ver en **Reglas de programa** y **Reglas de conexión** como **reglas de Panda**.

10.5.3 Reglas de programa

En esta sección se establecen los programas del usuario que se podrán comunicar con la red y los que tendrán bloqueado el envío y recepción de datos.

Para desarrollar una correcta estrategia de protección es necesario seguir los pasos mostrados a continuación, en el orden indicado:

1 Establecer la acción por defecto.

- **Permitir:** establece una estrategia permisiva basada en aceptar por defecto las conexiones de todos los programas cuyo comportamiento no haya sido definido explícitamente mediante una regla en el paso 3. Este es el modo configurado por defecto y considerado el más básico.
- **Denegar:** establece una estrategia restrictiva basada en denegar por defecto las conexiones de los programas cuyo comportamiento no haya sido definido explícitamente mediante una regla en el paso 3. Este es el modo avanzado de funcionamiento ya que requiere añadir reglas con todos los programas que los usuarios utilizan de forma habitual; de otro modo las comunicaciones de esos programas serán denegadas, afectando probablemente a su buen funcionamiento.

2 Activar reglas de Panda

Activa las reglas generadas automáticamente por Panda Security para el tipo de red definido anteriormente.

3 Añade reglas para definir el comportamiento específico de una aplicación

Los controles situados a la derecha permiten subir (1), bajar (2), añadir (3), editar (4) y borrar (5) reglas de programas. Las casillas de selección (6) permiten determinar sobre qué reglas se realizarán las acciones.

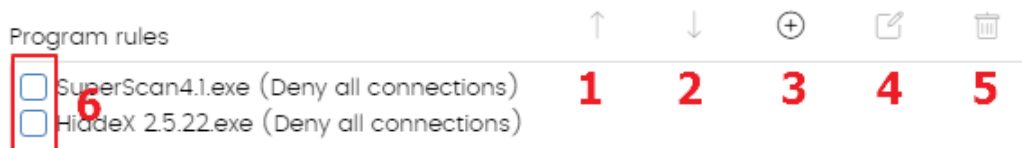


Figura 56: controles de edición de reglas de programa

Al crear una regla es necesario indicar los siguientes campos:

- **Descripción**
- **Programa:** permite seleccionar el programa cuyo comportamiento en red se va a controlar.
- **Conexiones permitidas para este programa:**

- **Permitir conexiones 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 conexiones salientes:** El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.
- **Permitir conexiones entrantes:** El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos de salida.
- **Denegar todas las conexiones:** El programa no podrá acceder a la red.
- **Permisos avanzados:**
 - **Acción:** Establece la acción que ejecutará **Endpoint Protection / Plus** si la regla coincide con el tráfico examinado.
 - **Permitir:** permite el tráfico.
 - **Denegar:** bloquea el tráfico. Se hace un Drop de la conexión.
 - **Sentido:** establece la dirección del tráfico para protocolos orientados a conexión como TCP.
 - **Salientes:** tráfico con origen el equipo de usuario y destino otro equipo de la red.
 - **Entrantes:** tráfico con destino el equipo de usuario y origen otro equipo de la red.
 - **Zona**
 - **Protocolo:** permite especificar el protocolo de nivel 3 del tráfico generado por el programa a controlar.
 - **Todos**
 - **TCP**
 - **UDP**
 - **IPs:**
 - **Todos:** la regla no tiene en cuenta los campos IP de origen y destino de la conexión.
 - **Personalizado:** permite definir la IP de origen o destino del tráfico a controlar. Especifica más de una IP separadas por ',' o utiliza el carácter '-' para establecer rangos de IPs.
 - **Puertos:** permite seleccionar el puerto de la comunicación. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.

10.5.4 Regla de conexión

Las reglas de conexiones son reglas tradicionales de filtrado de tráfico TCP/IP. **Endpoint Protection / Plus** extrae el valor de ciertos campos de las cabeceras de cada paquete que reciben o envían los equipos protegidos, y explora el listado de reglas introducido por el administrador. Si alguna regla coincide con el tráfico examinado se ejecuta la acción asociada.

Las reglas de conexiones afectan a todo el sistema, independientemente del proceso que las gestione, y son prioritarias con respecto a las reglas configuradas anteriormente para la conexión de los programas a la red.

Para desarrollar una correcta estrategia de protección frente a tráfico no deseado o peligroso es necesario seguir los pasos mostrados a continuación, en el orden que se indica:

1 Establecer la acción por defecto del cortafuegos, situada en Reglas para programas.

- **Permitir:** establece una estrategia permisiva basada en aceptar por defecto las conexiones cuyo comportamiento no haya sido definido mediante reglas en el paso 3. Este es el modo básico de configuración: todas las conexiones no descritas mediante reglas serán automáticamente aceptadas.
- **Denegar:** establece una estrategia restrictiva basada en denegar por defecto las conexiones cuyo comportamiento no haya sido definido mediante reglas en el paso 3. Este es el modo avanzado de funcionamiento: todas las conexiones no descritas mediante reglas serán automáticamente denegadas.

2 Activar reglas de Panda

Activa las reglas generadas automáticamente por Panda Security para el tipo de red definido anteriormente.

3 Añade reglas que describan conexiones de forma específica junto a una acción asociada.

Los controles situados a la derecha permiten subir (1), bajar (2), añadir (3), editar (4) y borrar (5) reglas de conexión. Las casillas de selección (6) permiten determinar sobre que reglas se realizarán las acciones.



Figura 57: controles de edición de reglas de red

El orden de las reglas en la lista es un elemento a tener en cuenta: su aplicación se evalúa en orden descendente y, por lo tanto, al desplazar una regla hacia arriba o abajo en la lista, se modificará la prioridad en su aplicación.

A continuación, se describen los campos que forman una regla de sistema:

- **Nombre de regla**
- **Descripción**
- **Acción:** Establece la acción que ejecutará **Endpoint Protection / Plus** si la regla coincide con el tráfico examinado.
 - **Permitir:** permite el tráfico.
 - **Denegar:** bloquea el tráfico. Se hace un Drop de la conexión.

- **Sentido:** establece la dirección del tráfico para protocolo orientados a conexión como TCP.
 - **Salientes:** tráfico saliente.
 - **Entrantes:** tráfico entrante.
- **Zona**
- **Protocolo:** permite especificar el protocolo de la regla. Según la elección se mostrarán unos controles u otros para identificar de forma precisa el protocolo en cuestión:
 - **TCP, UPD, TCP/UDP:** permite describir reglas TCP y / o UDP incluyendo puertos locales y remotos.
 - **Puertos locales:** permite especificar el puerto de la conexión utilizado en el equipo del usuario. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
 - **Puertos remotos:** permite especificar el puerto de la conexión utilizado en el equipo remoto. Selecciona **Personalizado** para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.
 - **ICMP:** permite crear reglas que describen mensajes ICMP, indicando su tipo y subtipo.
 - **IP Types:** permite crear reglas para el protocolo IP y otros protocolos de orden superior.
- **Direcciones IP:** especifica las direcciones IP de origen o destino del tráfico.
- **Direcciones MAC:** especifica las direcciones MAC de origen o destino del tráfico.



Las direcciones MAC de origen y destino se reescriben cada vez que el tráfico atraviesa un proxy, enrutador etc. Los paquetes llegarán al destino con la MAC del último dispositivo que manipuló el tráfico.

10.5.5 Bloquear intrusiones

El módulo IDS permite detectar y rechazar tráfico mal formado y especialmente preparado para impactar en el rendimiento o la seguridad del equipo a proteger. Este tipo de tráfico puede provocar un mal funcionamiento de los programas del usuario que lo reciben, resultando en problemas de seguridad y permitiendo la ejecución de aplicaciones de forma remota por parte del hacker, extracción y robo de información etc.

Endpoint Protection / Plus identifica 15 tipos de patrones genéricos que pueden ser activados o desactivados haciendo clic en la casilla apropiada. A continuación, se detallan los tipos de tráfico mal formado soportados y una explicación de cada uno de ellos:

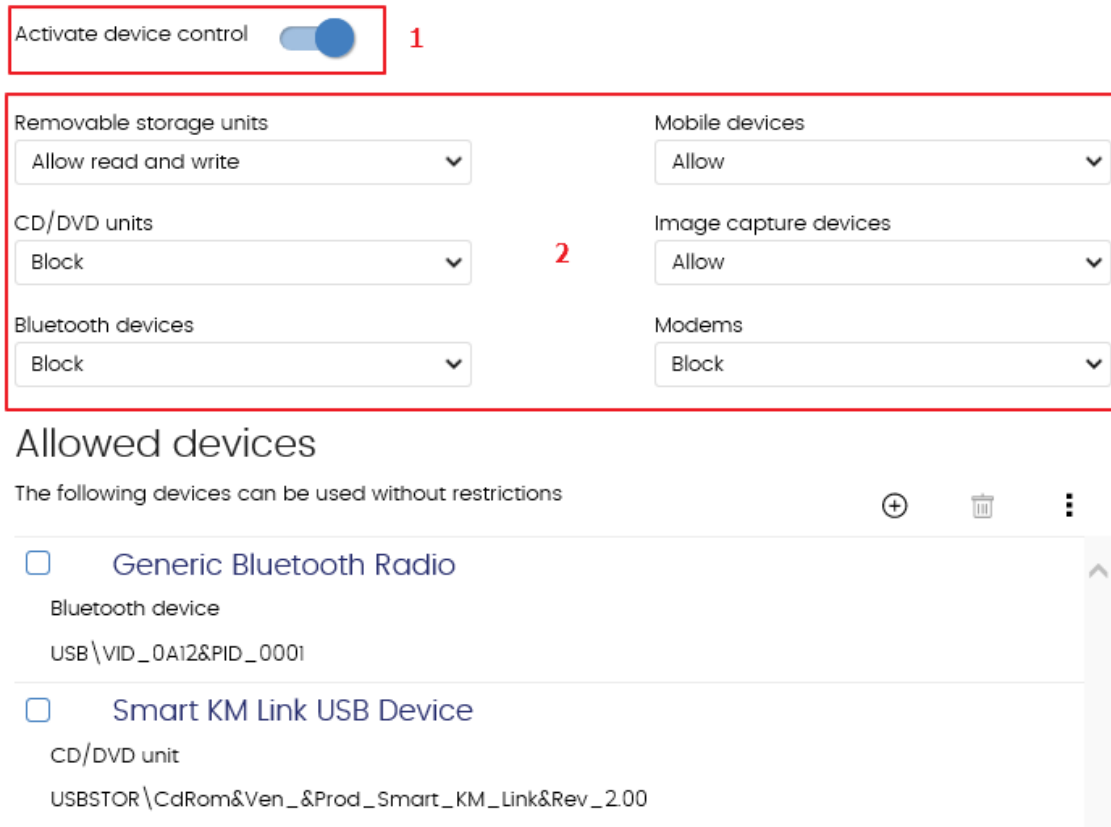
- **IP explicit path:** Se rechazan los paquetes IP que tengan la opción de "explicit route". Son paquetes IP que no se encaminan en función de su dirección IP de destino, en su lugar la información de encaminamiento es fijada de ante mano.
- **Land Attack:** Comprueba intentos de denegación de servicios mediante bucles infinitos de pila TCP/IP al detectar paquetes con direcciones origen y destino iguales.
- **SYN flood:** lanza inicios de conexión TCP de forma masiva para obligar al equipo a comprometer recursos para cada una de esas conexiones. Se establece un límite máximo de conexiones TCP abiertas para evitar una sobrecarga del equipo atacado.

- **TCP Port Scan:** detecta si un equipo intenta conectarse a varios puertos del equipo protegido en un tiempo determinado. Se filtran tanto las peticiones de apertura de puerto como las respuestas al equipo sospechoso, para que el origen del tráfico de escaneo no obtenga información del estado de los puertos.
- **TCP Flags Check:** Detecta paquetes TCP con combinaciones de flags inválidas. Actúa como complemento a las defensas de "Port Scanning" al detener ataques de este tipo como "SYN & FIN" y "NULL FLAGS" y los 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 al equipo de ataques por consumo excesivo de memoria en ausencia de fragmentos, redireccionado de ICMP disfrazado de UDP y scanning de máquina disponible.
- **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.
- **UDP Port Scan:** Protección contra escaneo de puertos UDP.
- **Smart WINS:** Se rechazan las respuestas WINS que no se corresponden con peticiones que el equipo haya solicitado.
- **Smart DNS:** Se rechazan las respuestas DNS que no se corresponden con peticiones que el equipo haya solicitado.
- **Smart DHCP:** Se rechazan las respuestas DHCP que no se corresponden con peticiones que el equipo haya solicitado.
- **ICMP Attack:** Este filtro implementa varias comprobaciones:
 - **SmallPMTU:** Mediante la inspección de los paquetes ICMP se detectan valores inválidos en el tamaño del paquete utilizados para generar una denegación de servicio o ralentizar el tráfico saliente.
 - **SMURF:** Envío de grandes cantidades de tráfico ICMP (echo request) a la dirección de broadcast de la red con la dirección de origen cambiada (spoofing) a la dirección de la víctima. La mayoría de los equipos de la red responderán a la víctima, multiplicando el tráfico por cada equipo de la subred. Se rechazan las respuestas ICMP no solicitadas si éstas superan una determinada cantidad en un segundo.
 - **Drop unsolicited ICMP replies:** Se rechazan todas las respuestas ICMP no solicitadas o que hayan expirado por el timeout establecido.
- **ICMP Filter echo request:** se rechazan las peticiones de Echo request.
- **Smart ARP:** Se rechazan las respuestas ARP que no se corresponden con peticiones que el equipo protegido haya solicitado para evitar escenarios de tipo ARP cache poison.
- **OS Detection:** Falsea datos en respuestas al remitente para engañar a los detectores de sistemas operativos y así evitar posteriores ataques dirigidos a aprovechar las vulnerabilidades asociadas al sistema operativo detectado. Esta defensa se complementa con la de "TCP Flags Check".

10.6. Control de dispositivos (Equipos Windows)

Dispositivos de uso común como llaves USB, unidades de CD/DVD, dispositivos de imágenes, bluetooth, módems o teléfonos móviles pueden constituir también una vía de infección para los equipos de la red.

Control de dispositivos permite definir el comportamiento del equipo protegido al conectar u operar con un dispositivo extraíble o de almacenamiento masivo. Para ello, hay que seleccionar el dispositivo o dispositivos que se desea autorizar y asignar un nivel de utilización.



Activate device control 1

Removable storage units	Mobile devices
Allow read and write	Allow
CD/DVD units	Image capture devices
Block	Allow
Bluetooth devices	Modems
Block	Block

2

Allowed devices

The following devices can be used without restrictions

- Generic Bluetooth Radio**
Bluetooth device
USB\VID_0A12&PID_0001
- Smart KM Link USB Device**
CD/DVD unit
USBSTOR\CdRom&Ven_&Prod_Smart_KM_Link&Rev_2.00

Figura 58: configuración del control de dispositivos

Para activar el control de dispositivos sigue los pasos mostrados a continuación:



- Marca la casilla **Activar control de dispositivos (1)**.
- Elige en el desplegable correspondiente el nivel de autorización a aplicar para el tipo de dispositivo a limitar su uso **(2)**.
 - En el caso de las llaves USB y las unidades CD/DVD se puede 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**.

10.6.1 Equipos permitidos

Se puede dar el caso de no permitirse el uso de una familia dispositivos y que, sin embargo, sea necesario autorizar el uso de un dispositivo concreto perteneciente a esa familia.

Esta situación se puede solucionar elaborando una "lista blanca": una lista de dispositivos cuyo uso se permitirá, aunque pertenezcan a grupos de dispositivos que se hayan marcado como no autorizados.

Para ello **Endpoint Protection / Plus** crea un listado de dispositivos conectados por cada equipo.

Haz clic en icono  de **Equipos permitidos** para mostrar un listado con todos los dispositivos conectados a los equipos del parque informático. Elige aquellos que quieras excluir del bloqueo general previamente configurado. Con el botón  podrás borrar exclusiones ya creadas.

10.6.2 Exportar e importar listas de dispositivos permitidos

Una vez la lista de dispositivos permitidos esté finalizada podrás exportarla a un archivo de texto. Esta operación también puede realizarse a la inversa: es decir, configurar en un archivo de texto la lista con los datos de los dispositivos que se desean permitir y a continuación importar esa lista desde la consola Web de **Endpoint Protection / Plus**.

Para exportar e importar listados de exclusiones ya configurados despliega las opciones de **Exportar**

e **Importar** del menú de contexto .

10.6.3 Obtención del identificador único del dispositivo

En el caso de querer utilizar dispositivos sin restricciones, pero sin esperar a que el usuario conecte los dispositivos en su equipo para poder excluirlos de forma manual, es posible obtener el identificador de estos dispositivos. Para ello sigue los pasos mostrados a continuación:

- En el Administrador de dispositivos de Windows, accede a las propiedades del dispositivo USB que quieres identificar de forma única para excluirlo.
- Accede a la pestaña Detalles y seleccionamos la propiedad Recursos en el desplegable Propiedad. A continuación, debería mostrarse un valor llamado CM_DEVCAP_UNIQUEID.
- De nuevo en el desplegable Propiedad, selecciona Ruta de acceso a instancia del dispositivo y obtendrás el identificador único de dispositivo.

En el supuesto de que no se muestre ningún valor denominado CM_DEVCAP_UNIQUEID no será posible realizar la identificación del dispositivo de forma única. Lo que sí podremos hacer es utilizar como identificador el correspondiente al hardware del dispositivo.

En el desplegable Propiedad selecciona Identificador de hardware y se mostrará el identificador correspondiente, que será el que podrás utilizar. En este caso, al usar este identificador se excluirá

del control de dispositivos a todos los productos USB de la gama que posean ese identificador, ya que no habrá manera de diferenciar a unos de otros.

Una vez tengas los identificadores únicos podrás elaborar una lista blanca e importarla tal y como se ha mostrado en el punto anterior.

10.7. Control de acceso a páginas web



Característica solo disponible en Endpoint Protection Plus.

Con esta protección el administrador de la red podrá restringir el acceso a determinadas categorías Web y configurar URLs individuales a las que autorizará o restringirá el acceso. Esto contribuirá a la optimización del ancho de banda de la red y a la productividad de la empresa.

Para activar o desactivar el control de acceso páginas web haz clic en el botón **Activar el control de acceso a páginas web**.

10.7.1 Configurar horarios del control de accesos a páginas Web

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 activar el control horario de accesos a páginas Web elija la opción **Activar solo durante las siguientes horas**.

A continuación, selecciona las horas en las que se quiera 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.

- Para seleccionar días completos haz clic en el día de la semana.
- Para seleccionar una misma hora en todos los días de la semana haz clic en la hora
- Para seleccionar todos los días del mes haz clic en el botón **Seleccionar todo**
- Para limpiar toda la selección y comenzar de cero haz clic en el botón **Vaciar**

10.7.2 Denegar el acceso a páginas Web

Endpoint Protection / Plus agrupa las páginas web en 64 categorías. Tan solo es necesario seleccionar aquellas categorías a las que se desea denegar el acceso.

Para ello selecciona las categorías a denegar el acceso. Cuando el usuario visite una página Web que pertenezca a una categoría denegada, se le mostrará en el navegador un aviso indicando el motivo.

Denegar el acceso a páginas de categoría desconocida

Es posible denegar el acceso a páginas no categorizadas, Para ello haz clic en el botón de activación **Denegar acceso a las páginas cuya categoría sea desconocida**.



Las webs internas o alojadas en intranets y accesibles a través de los puertos 80 u 8080 pueden ser clasificadas como pertenecientes a una categoría desconocida, y por tanto ser denegado su acceso. Para mitigar esta situación el administrador podrá añadir las páginas Web desconocidas que sean necesarias a la lista blanca de exclusiones.

10.7.3 Lista de direcciones y dominios permitidos o denegados

Es posible especificar listas de páginas Web a las que siempre se permitirá (lista blanca) o denegará (lista negra) el acceso, independientemente de la categoría a la que pertenezcan.

Podrás modificar ambas listas en cualquier momento.

- Introduce en la caja de texto la URL del dominio o dirección.
- Haz clic en **Añadir**.
- Utiliza los botones **Eliminar** y **Vaciar** para modificar la lista.
- Finalmente, haz clic en **Aceptar** para guardar la configuración.

La coincidencia de las URLs indicadas en lista blanca y lista negra puede ser completa o parcial. En caso de URLs largas es suficiente con indicar el comienzo de la URL para conseguir una coincidencia.

10.7.4 Base de datos de URLs accedidas desde los equipos

Cada equipo de la red recopila información sobre las URLs visitadas. Esta información solo se puede consultar desde el propio equipo durante un plazo de 30 días.

Los datos almacenados son:

- Identificador del usuario.
- Protocolo (http o https).
- Dominio
- URL
- Categorías devueltas.
- Acción (Permitir/denegar).

- Fecha de acceso.
- Contador acumulado de accesos por categoría y dominio.

10.8. Antivirus para servidores Exchange



Característica solo disponible en Endpoint Protection Plus.

Si se disponen de licencias apropiadas se podrá activar la protección para servidores Exchange desde la consola de administración y asignarlas a cualquier servidor Exchange gestionado.

La protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013 y 2016 y está formada por tres módulos:

- Antivirus
- Anti-spam
- Filtrado de contenidos.

Además, según el momento en el que **Endpoint Protection / Plus** efectúa el análisis dentro del flujo de correo, se distinguen dos formas de protección: protección de buzones y protección de transporte.

La Tabla 13 muestra las combinaciones de módulo de protección, modo de análisis y versiones de Exchange soportados.

Módulo de protección / modo de análisis	Antivirus	AntiSpam	Filtrado de contenidos
Buzón	2003, 2007, 2010		
Transporte	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016	2003, 2007, 2010, 2013, 2016

Tabla 13: módulos de protección, modos de análisis y versiones Microsoft Exchange soportadas

Protección de buzones

Se utiliza en los servidores Exchange con el rol de Mailbox y permite analizar las carpetas / buzones en background o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones solo se ofrece para el módulo Antivirus en los servidores Microsoft Exchange 2003, 2007 y 2010.

Protección de transporte

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Hub, y permite analizar el tráfico que es atravesado por el servidor Microsoft Exchange.

Analiza en busca de virus, herramientas de hacking y programas potencialmente no deseados sospechosos, con destino a buzones situados en el servidor Exchange.

El administrador tiene la posibilidad de activar o desactivar la protección de buzones y/o de transporte haciendo clic en la casilla apropiada.

Protección de los buzones

El comportamiento de la protección de los buzones es ligeramente diferente según se trate de Exchange 2013 – 2016 y el resto de versiones.

En Exchange 2013 y 2016 no se permite manipular el mensaje; si el correo contiene un elemento peligroso se introduce íntegro en cuarentena. El usuario protegido con **Endpoint Protection / Plus** recibirá un mensaje con el asunto original, pero con el cuerpo sustituido por un mensaje de advertencia indicando que, en caso de querer recuperar el mensaje original, contacte con el administrador de la red.

En el resto de versiones de Exchange se realiza la acción programada por Panda Security ante la detección de un elemento clasificado como malware: desinfectar el adjunto si es posible o introducirlo en cuarentena si no es posible. El usuario protegido con **Endpoint Protection / Plus** recibirá el mensaje con los adjuntos desinfectados o, en caso de que no fuera posible su desinfección, un fichero "security_alert.txt" de sustitución, describiendo el motivo de la detección.

10.9. Anti spam para servidores Exchange



Característica solo disponible en Endpoint Protection Plus

Para activar o desactivar esta protección, utiliza el botón de activación **Detectar Spam**.

Al activar la protección Anti Spam **Endpoint Protection / Plus** muestra una ventana emergente sugiriendo añadir varias reglas de exclusión para mejorar el rendimiento del servidor de correo.

10.9.1 Acción para mensajes de spam

Selecciona la acción a realizar con los mensajes de spam:

- **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

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. 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 el Directorio Activo. De esta forma la protección adjudica al mensaje el valor SCL correspondiente y posteriormente se procede a su entrega.

A continuación, será el administrador, en función del umbral determinado en el Directorio Activo, quien seleccione la acción que finalmente se realizará con el mensaje.

10.9.2 Direcciones y dominios permitidos

Son listas de direcciones y dominios cuyos mensajes no serán analizados por la protección anti-spam (lista blanca).

Puedes añadir varias direcciones y dominios separados por el carácter " , ".

10.9.3 Direcciones y dominios de spam

Son listas de dominios y direcciones cuyos mensajes serán interceptados por la protección y eliminados (lista negra).

Al configurar las listas es importante tener en cuenta:

- Si un dominio se encuentra en lista negra y una dirección perteneciente a dicho dominio se encuentra en lista blanca, se permitirá dicha dirección, pero no el resto de direcciones del dominio.
- Si un dominio se encuentra en lista blanca y una dirección perteneciente a dicho dominio se encuentra en lista negra, dicha dirección no será aceptada, pero sí el resto de direcciones de dicho dominio.
- Si un dominio (por ejemplo: domain.com) se encuentra en lista negra y un subdominio de este (ej: mail1.domain.com) se encuentra en lista blanca, se permitirán direcciones de dicho subdominio, pero no el resto de direcciones del dominio o de otros subdominios diferentes.

- Si un dominio se encuentra en lista blanca también se considerarán incluidos en lista blanca todos sus subdominios.

10.10. Filtrado de contenidos para servidores Exchange



Característica solo disponible en Endpoint Protection Plus.

El filtrado de contenidos 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.

- **Acción a realizar:** selecciona si deseas borrar los mensajes o desviarlos a otra dirección de correo electrónico. Esto puede resultar útil para analizar a posteriori los adjuntos recibidos
- **Considerar archivos adjuntos peligrosos los que tienen las siguientes extensiones:** considera como peligrosos los archivos adjuntos con alguna extensión concreta. Una vez marcada la casilla, utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de extensiones que deseas bloquear.
- **Considerar archivos adjuntos peligrosos todos los que tienen doble extensión, excepto en los siguientes casos:** 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 seleccionadas. Utiliza los botones **Añadir**, **Eliminar**, **Vaciar** o **Restaurar** para configurar la lista de dobles extensiones permitidas.

Registro de detecciones

Todas las detecciones producidas en un servidor Exchange son almacenadas localmente en un archivo CSV. De esta forma se ofrece al administrador la posibilidad de obtener información adicional acerca de la imposibilidad de entrega de los mensajes a sus destinatarios.

El fichero recibe el nombre `ExchangeLogDetections.csv` y se almacena en la carpeta.

```
%AllUsersProfile%\Panda Security\Panda Cloud Office Protection\Exchange
```

El contenido del fichero se dispone en formato tabular con la siguiente distribución de campos:

- **Date:** fecha de la llegada del correo al servidor Exchange
- **From**
- **To**
- **Subjet**

- **Attachments:** listado con los ficheros adjuntos al correo.
- **Protection**
- **Action**

11. Configuración de seguridad Android

Configuración de dispositivos Android
Actualizaciones
Antivirus

11.1. Introducción

Endpoint Protection / Plus centraliza en el menú superior **Configuración** toda la configuración de los parámetros de seguridad para smartphones y tablets. Haciendo clic en el panel de la izquierda **Dispositivos Android** se mostrará un listado con todas las configuraciones de seguridad ya creadas.

En este capítulo se repasarán todos los parámetros incluidos en la configuración de seguridad para dispositivos Android, al tiempo que se mostrarán algunas recomendaciones prácticas para asegurar móviles y tablets, minimizando los inconvenientes en su manejo al usuario.

11.2. Introducción a la configuración de dispositivos Android

La configuración para dispositivos Android se divide en 3 apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con su configuración asociada. A continuación, se muestran los apartados con una breve explicación:

- **Actualizaciones:** permite establecer el tipo de conexión que utilizara el dispositivo para descargar las actualizaciones de la nube de Panda Security.
- **Antivirus:** permite establecer la configuración del antivirus.
- **Antirrobo:** habilita o deshabilita las características antirrobo implementadas en Endpoint Protection / Plus.

11.3. Actualizaciones

La configuración de las actualizaciones se describe en el capítulo 12 Actualización del Software.

11.4. Antivirus

La protección antivirus para smartphones Android protege a móviles y tablets frente a la instalación de aplicaciones con malware y PUPs analizando bajo demanda o de forma permanente tanto el dispositivo móvil como las tarjetas de memoria SD conectadas.

Haz clic en el botón de activación **Activar protección permanente antivirus** para activar la detección de malware.

Exclusiones

La protección para Android permite realizar exclusiones de cualquiera de las aplicaciones instaladas. Introduce los nombres de los paquetes a excluir separados por el carácter ", "

Para localizar el nombre del paquete correspondiente a una aplicación instalada búscala en la Google Play. En la URL de su ficha se mostrará el parámetro id, que contiene la cadena que identifica de forma única a la aplicación.

12. Actualización del Software

Actualización del motor de protección
Actualización del agente de comunicaciones
Actualización del conocimiento
Cache de actualizaciones

12.1. Introducción

Endpoint Protection / Plus es un servicio cloud gestionado y por lo tanto el cliente no necesita ejecutar tareas de actualización de la infraestructura de back-end encargada de soportar el servicio de protección; sin embargo, sí es necesaria la actualización del software instalado en los equipos de la red del cliente.

Los elementos instalados en el equipo del usuario son tres:

- Agente de comunicaciones Panda
- Motor de la protección **Endpoint Protection / Plus**
- Archivo de identificadores / fichero de firmas para la protección antivirus tradicional

Dependiendo de la plataforma a actualizar, el procedimiento y las posibilidades de configuración varían tal y como se indica en la Tabla 14:

Módulo	Plataforma			
	Windows	Mac OS X	Linux	Android
Agente Panda	Bajo demanda			
Protección Endpoint Protection / Plus	Configurable	Configurable	Configurable	No
Archivo de identificadores	Habilitar / Deshabilitar	Habilitar / Deshabilitar	Habilitar / Deshabilitar	No

Tabla 14: tipos de actualización por plataforma y módulo

- **Bajo demanda:** el administrador puede iniciar la actualización una vez que esté disponible, pudiendo de esta forma retrasarla hasta el momento que considere oportuno.
- **Configurable:** el administrador podrá definir ventanas de actualización recurrentes y en el futuro mediante la consola, siendo posible además desactivar la actualización.
- **Habilitar / Deshabilitar:** El administrador puede desactivar la actualización. Si la actualización está activada ésta se producirá automáticamente cuando esté disponible.
- **No:** El administrador no puede influir en el proceso de actualización. Las actualizaciones se efectuarán cuando estén disponibles y no es posible deshabilitarlas.

12.2. Configuración de la actualización del motor de protección

La configuración de la actualización del motor de protección **Endpoint Protection / Plus** se realiza creando y asignando un perfil de configuración de tipo ajustes por equipo, accesible desde el menú superior **Configuración**, en el panel de la izquierda de la consola de administración.

12.2.1 Actualizaciones

Para habilitar la actualización automática del módulo de protección **Endpoint Protection / Plus** haz clic en el botón de activación **Actualizar automáticamente Aether en los dispositivos**. Esta acción habilitará el resto de configuraciones de la página. Si esta opción está deshabilitada, el módulo de protección no se actualizará nunca.



Se desaconseja totalmente deshabilitar la actualización del motor de protección. Los equipos con la protección sin actualizar serán más vulnerables en el medio plazo frente a las amenazas avanzadas y el malware.

Aplicar actualizaciones en rangos de horas

Indica los siguientes parámetros para que los equipos apliquen las actualizaciones disponibles dentro de un rango de horas concreto:

- Hora de inicio
- Hora de fin

Para aplicar las actualizaciones en cualquier momento haz clic en la casilla de selección **A cualquier hora**.

Aplicar actualizaciones en fechas determinadas

Utiliza el desplegable para indicar las fechas en las que la actualización se aplicará:

- **En cualquier fecha:** las actualizaciones se aplicarán el día que estén disponibles. Esta opción no limita la actualización de **Endpoint Protection / Plus** a fechas concretas.
- **Los siguientes días de la semana:** utiliza las casillas de selección para establecer los días de la semana en los que **Endpoint Protection / Plus** se actualizará. La actualización se producirá el primer día de la semana que coincida con la selección del administrador en caso de haber una actualización disponible.
- **Los siguientes días del mes:** utiliza los desplegables para establecer un rango de días hábiles dentro del mes en los que **Endpoint Protection / Plus** se actualizará. La actualización se producirá el primer día del mes que coincida con los seleccionados por el administrador en caso de haber una actualización disponible.
- **Los siguientes días:** utiliza los desplegables para establecer un rango de días hábiles dentro del calendario en los que **Endpoint Protection / Plus** se actualizará. Los rangos definidos en esta opción se establecen de forma absoluta para casos en que el administrador quiera establecer rangos que no se repiten en el tiempo. De esta forma, se permite definir rangos de fechas concretas de actualización, pasadas las cuales dejan de tener efecto. Este método requiere redefinir los rangos de actualización de forma constante una vez hayan vencido.

Reinicio de equipos

Endpoint Protection / Plus permite definir la lógica de reinicios en caso de que sea necesario, mediante el desplegable situado al final de la pantalla de configuración:

- **No reiniciar automáticamente:** se mostrará al usuario una ventana en intervalos de tiempo cada vez más cortos, aconsejando el reinicio de la máquina para aplicar la actualización.
- **Reiniciar automáticamente sólo las estaciones de trabajo.**
- **Reiniciar automáticamente sólo los servidores.**
- **Reiniciar automáticamente tanto estaciones de trabajo como servidores.**

12.3. Configuración de la actualización del agente de comunicaciones

La actualización del agente Panda se realiza bajo demanda. **Endpoint Protection / Plus** incluirá una notificación en la consola de administración indicando la disponibilidad de una nueva versión disponible del agente, y el administrador podrá lanzar la actualización cuando lo desee.

La actualización del agente Panda no requiere reinicio del equipo del usuario y suele implicar cambios y mejoras en la consola de administración que facilitan la gestión de la seguridad.

12.4. Configuración de la actualización del conocimiento

La configuración de la actualización del fichero de firmas en **Endpoint Protection / Plus** se realiza en el perfil de configuración de seguridad asignado al equipo, según sea su tipo.

12.4.1 Dispositivos Windows, Linux y Mac

La configuración se realiza en los perfiles de tipo **Estaciones y Servidores**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

En la pestaña **General** las opciones disponibles son:

- **Actualizaciones automáticas de conocimiento:** Permite habilitar o deshabilitar la descarga del fichero de firmas. Si se deshabilita el fichero de firmas nunca será actualizado.



Se desaconseja totalmente deshabilitar la actualización del conocimiento. Los equipos con la protección sin actualizar serán más vulnerables frente a las amenazas.

- **Realizar un análisis en segundo plano cada vez que se actualice el conocimiento:** permite lanzar de forma automática un análisis cada vez que un fichero de firmas se descargue en el equipo. El análisis tendrá prioridad mínima para no interferir en el trabajo del usuario.

12.4.2 Dispositivos Android

La configuración se realiza en los perfiles **Dispositivos Android**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

Endpoint Protection / Plus permite limitar las actualizaciones del Software de forma que no consuman datos de conexiones móviles sujetas a tarificación.

Haz clic en el botón de activación para restringir las actualizaciones a aquellos momentos en que el smartphone o tablet tenga conexión wifi disponible.

13. Tareas

Creación de tareas
Publicación de tareas
Gestión de tareas

13.1. Introducción

Las tareas son un recurso implementado en **Endpoint Protection / Plus** que permite lanzar bajo demanda análisis de seguridad sobre grupos de equipos, aplazados en el tiempo o programados para fechas concretas.

El proceso de lanzamiento de una tarea se divide en tres pasos, mostrados a continuación.



- **Creación y configuración de la tarea**, donde se determinan los equipos afectados, las características del análisis, el momento en que será lanzado, el número de veces que se ejecutará y el comportamiento en caso de error.
- **Publicación de la tarea una vez creada**, paso necesario para activar las tareas introduciéndolas en el programador de tareas de **Endpoint Protection / Plus** para ser lanzadas en el momento marcado por su configuración.
- **Ejecución de la tarea** cuando se alcancen las condiciones especificadas en su definición.

13.2. Creación de tareas

Para crear una nueva tarea, desde el menú superior haz clic en **Tareas**. Accederás a una ventana donde están listadas todas las tareas creadas, indicando su estado. Para crear una tarea nueva haz clic en el botón **Añadir** y elige **Análisis programado** en el desplegable; se mostrará una ventana con los datos de la tarea, distribuidos en cuatro zonas:

- **Información general**: nombre de la tarea y descripción.
- **Destinatarios**: equipos que recibirán la tarea.
- **Programación**: configuración del momento en que se lanzará la tarea.
- **Opciones de análisis**: configuración del análisis bajo demanda.

13.2.1 Destinatarios de la tarea

Haciendo clic en el link **Destinatarios de la tarea** se abre una nueva ventana donde se pueden seleccionar los equipos que recibirán la tarea configurada. Haz clic en el botón  para agregar un nuevo equipo y en el botón  para eliminar los equipos seleccionados.



Es necesario salvar previamente la tarea para poder acceder a la ventana de selección de equipos.

13.2.2 Programación horaria y repetición de la tarea

La programación horaria se especifica mediante tres parámetros:

- **Empieza:** marca el comienzo de la tarea.
- **Tiempo máximo de ejecución:** indica el tiempo máximo que la tarea puede tardar en completarse, vencido el cual se cancelará con error si no ha terminado.
- **Repetir:** establece cada cuanto tiempo la tarea se vuelve a activar, tomando como referencia la fecha marcada en **Empieza**

Empieza

- **Lo antes posible (activado):** la tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o en el momento en que se encuentre disponible dentro del margen definido en el desplegable **Equipo apagado**.
- **Lo antes posible (desactivado):** la tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor **Endpoint Protection / Plus**.
- **Equipo apagado:** Si el equipo está apagado o inaccesible, la tarea de análisis no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea, retrasar el lanzamiento un intervalo de tiempo definido por el usuario, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida).
 - **No ejecutar:** el análisis se cancela si en el momento del lanzamiento el equipo no está encendido.
 - **Dar un margen de:** permite definir un intervalo de tiempo dentro del cual, si la máquina inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada.
 - **Ejecutar cuando encienda:** no establece ningún intervalo de tiempo, se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tiempo máximo de ejecución

- **Sin limite:** la duración de la ejecución de la tarea no está definida, pudiéndose extenderse hasta el infinito.
- **1,2, 8 o 24 horas:** la duración de la ejecución de la tarea está acotada. Transcurrido el tiempo indicado, la tarea se cancela con error si no ha terminado previamente.
- **Repetir:** establece un intervalo de repetición cada día, semana mes o año tomando como referencia la fecha indicada en **Empieza**.

Opciones de análisis

Las opciones de análisis permiten configurar los parámetros del motor de antivirus a la hora de realizar el escaneo del sistema de ficheros de los equipos. Se encuentran disponibles las opciones mostradas a continuación:

- **Tipo de análisis**
 - **Todo el ordenador:** Análisis profundo del equipo incluyendo a todos los dispositivos de almacenamiento conectados.
 - **Áreas críticas:** análisis rápido del equipo que incluye
 - %WinDir%\system32
 - %WinDir%\SysWow64
 - Memoria

- Sistema de arranque
- Cookies
- **Elementos específicos:** permite introducir rutas de los dispositivos de almacenamiento masivo. Se admite el uso de variables de entorno. Se analizará la ruta indicada y todas las carpetas y ficheros que cuelguen de ella.
- **Detectar virus:** detección de programas que se pueden introducir en los ordenadores produciendo efectos nocivos. Esta opción está siempre activada.
- **Detectar herramientas de hacking y PUPs:** detección de programas que pueden ser utilizados por un hacker para causar perjuicios a los usuarios de un ordenador y detección de programas potencialmente no deseados.
- **Detectar archivos sospechosos:** en los análisis programados el software del equipo es analizado de forma estática, si ejecución. De este modo puede ser necesario activar los algoritmos de análisis heurístico para detectar todos los tipos de amenazas.
- **Analizar archivos comprimidos**
- **Excluir del análisis los siguientes archivos**
 - No analizar los archivos excluidos para las protecciones permanentes: los archivos marcados por el administrador como permitida su ejecución no serán analizados, junto a los archivos ya excluidos de forma global en la consola.
 - Extensiones
 - Archivos
 - Directorios

13.3. Publicación de tareas

Una vez creada y configurada la tarea se añadirá al listado de tareas configuradas, pero no quedará activada hasta que la tarea sea publicada, haciendo clic en el botón **Publicar ahora**.

En el momento en que una tarea se publica, entrará en el programador de tareas de **Endpoint Protection / Plus**, el cual marcará el momento en que se lanzará la tarea según su configuración.

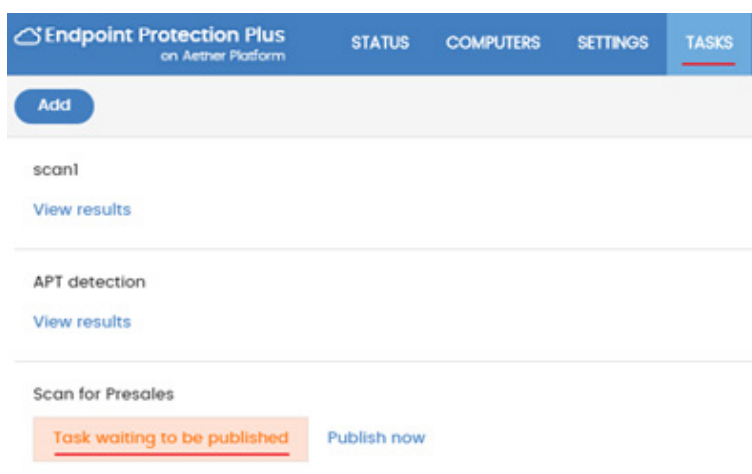


Figura 59: publicación de tareas

13.4. Gestión de tareas

El administrador tiene la posibilidad de borrar tareas, copiarlas, cancelarlas o visualizar los resultados haciendo clic en los iconos indicados a continuación.

Modificación de tareas publicadas

Haciendo clic en el nombre de la tarea creada se mostrará la ventana de configuración de la tarea, donde es posible modificar cualquier parámetro de la misma.




Las tareas publicadas solo admiten cambio de nombre y de descripción. Para modificar una tarea publicada es necesario copiarla.

Cancelación de las tareas publicadas

Para cancelar una tarea ya publicada haz clic en el link **Cancelar**. La tarea se cancelará, aunque no se borrará de la ventana de tareas para poder acceder a sus resultados.


Borrado de tareas

Las tareas ejecutadas no se eliminan automáticamente, para ello es necesario hacer clic en el icono .



Al borrar una tarea se borrarán también sus resultados.

Copia de tareas

Haciendo clic en el icono  de una tarea se creará una nueva con su misma configuración.

Ver los resultados de una tarea

Una tarea publicada permite mostrar los resultados obtenidos hasta el momento haciendo clic en el link **Ver resultados**. Se abrirá una ventana con los resultados y una serie de filtros que permiten localizar los datos importantes de forma fácil.

Los campos de la tabla de tareas se muestran en la Tabla 15:

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se registró un evento de análisis programado	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres

Campo	Comentario	Valores
Estado	<p>Pendiente: la tarea intento iniciar el análisis, pero la máquina no estaba disponible en ese momento. Se establece un periodo de espera según su configuración</p> <p>En progreso: el análisis se está realizando en este momento</p> <p>Con éxito: el análisis termino con éxito</p> <p>Fallida: el análisis termino con error</p> <p>Expirada: La tarea no llegó a comenzar por haber expirado el plazo configurado</p> <p>Cancelada: La tarea fue cancelada de forma manual</p>	Cadena de caracteres
Fecha de comienzo	Fecha de inicio del análisis	Fecha
Fecha fin	Fecha de finalización del análisis	Fecha
Detecciones	Número de detecciones realizadas en el equipo	Numérico

Tabla 15: parámetros de filtrado sobre el resultado de tareas

Los filtros de búsqueda se muestran en la Tabla 16:

Campo	Comentario	Valores
Fecha	Desplegable con las fechas en las que la tarea pasó a estado activo según su programación configurada. Una tarea activa puede lanzar un análisis en el momento o esperar a que la máquina esté disponible. Esta fecha se indica en la columna fecha	Fecha
Detecciones	Especifica si se muestran los equipos con alguna detección o los equipos limpios en la lista de tareas.	Binario
Estado	<p>Pendiente: la tarea todavía no se ha iniciado por no haber alcanzado la ventana de ejecución configurada</p> <p>En progreso: el análisis se está realizando en este momento</p> <p>Con éxito: el análisis termino con éxito</p> <p>Con error: el análisis termino con error</p> <p>Cancelada (no se puedo iniciar a la hora programada)</p> <p>Cancelada: La tarea fue cancelada de forma manual</p>	Enumeración

Tabla 16: filtros de búsqueda de tareas

14. Visibilidad del malware y del parque informático

- Esquema general del menú Estado
- Paneles / Widgets disponibles
- Introducción a los listados
- Listados disponibles
- Listados incluidos por defecto

14.1. Introducción

Endpoint Protection / Plus le ofrece al administrador tres grandes grupos de herramientas para visualizar el estado de la seguridad y del parque informático que gestiona:

- El panel de control, con información actualizada en tiempo real.
- Listados personalizables de incidencias, malware detectado y dispositivos gestionados junto a su estado.
- Informes con información del estado del parque informático, recogida y consolidada a lo largo del tiempo.



Los informes consolidados se tratarán en el capítulo 18 Informes.

Las herramientas de visualización y monitorización determinan en tiempo real el estado de la seguridad de la red y el impacto de las brechas de seguridad que se puedan producir para facilitar la adopción de las medidas de seguridad apropiadas.

14.2. Esquema general del menú Estado

El menú **Estado** reúne las principales herramientas de visibilidad y está formado por varias secciones, mostradas a continuación.



Figura 60: ventana de Estado con el panel de control y acceso a los listados

Acceso al panel de control (1)

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

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

Selector del intervalo de tiempo (2)

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

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



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

Selector de panel (3)

- **Seguridad:** estado de la seguridad del parque informático.
- **Accesos web y spam:** filtrado de la navegación y del correo no solicitado en servidores Microsoft Exchange.
- **Licencias:** consulta el capítulo 5 para obtener más información acerca de la gestión de licencias.
- **Informe ejecutivo:** consulta el capítulo 18 para obtener más información acerca de la configuración y generación de informes.

Este capítulo trata de los recursos contenidos en las secciones **Seguridad** y **Accesos web y spam**.

Mis listados (4)

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

Paneles informativos / Widgets (5)

El panel de control está formado por widgets o paneles informativos centrados en un único aspecto de la seguridad de la red.

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

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

THREATS DETECTED BY THE ANTIVIRUS

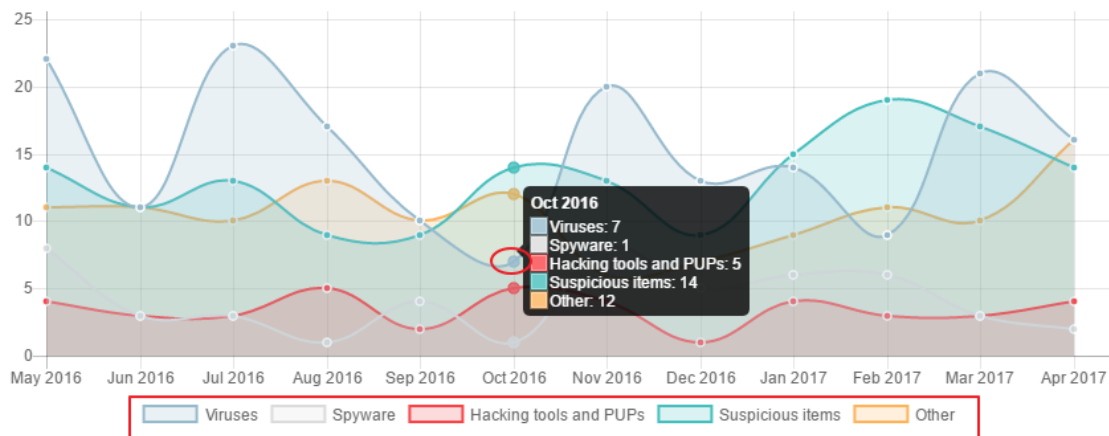


Figura 61: tooltips con información extendida y leyendas de las series representadas

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

- Gráficos de tarta
- Histogramas
- Gráficas de líneas

Haciendo clic en los elementos se mostrarán los listados de información detallada.

14.3. Paneles / Widgets disponibles

A continuación, se detallan los distintos widgets implementados en el dashboard de **Endpoint Protection / Plus**, las distintas áreas y zonas activas incorporadas y los tooltips y su significado.

14.3.1 Estado de protección

Estado de protección muestra tanto los equipos donde **Endpoint Protection / Plus** está funcionando correctamente como aquellos con errores y problemas en la instalación o en la ejecución del módulo de protección. El estado de los equipos es representado mediante un círculo con distintos colores y contadores asociados.

PROTECTION STATUS



40 computers have been discovered that are not being managed by Panda

Figura 62: panel de Equipos desprotegidos

El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.



La suma de los porcentajes de las diferentes series puede resultar más de un 100% debido a que los estados no son mutuamente excluyentes y un mismo equipo puede encontrarse en varias series a la vez.

- **Significado de las series**
 - **Correctamente protegido:** indica el porcentaje de equipos en los que **Endpoint Protection / Plus** se instaló sin errores y su ejecución no presenta problemas.
 - **Instalando:** indica el porcentaje de equipos en los que **Endpoint Protection / Plus** se encuentra en proceso de instalación.
 - **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, o no se les ha asignado una licencia disponible.
 - **Protección desactivada:** son equipos que no tienen activada la protección antivirus.
 - **Protección con error:** incluye a todos los equipos con **Endpoint Protection / Plus** instalado pero que, por alguna razón, el módulo de la protección no responde a las peticiones desde los servidores de Panda Security.
 - **Error instalando:** indica los equipos cuya instalación no se pudo completar.
 - **Parte central:** en la parte central del gráfico de tarta se indican los equipos desprotegidos del total de equipos vistos por **Endpoint Protection / Plus**. Para que un equipo sea visible tiene que tener el agente Panda instalado

- Filtros pre establecidos desde el panel

PROTECTION STATUS



40 computers have been discovered that are not being managed by Panda

Figura 63: zonas activas del panel Equipos desprotegidos

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- (1) Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Correctamente protegido
- (2) Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Instalando...
- (3) Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Protección desactivada
- (4) Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Protección con error
- (5) Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Sin licencia
- (6) Listado **Estado de protección de los equipos** filtrado por **Estado de protección** = Error instalando
- (7) Listado **Estado de protección de los equipos** sin filtros

14.3.2 Equipos sin conexión

OFFLINE COMPUTERS



Figura 64: panel Equipos sin conexión

Equipos sin conexión muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

- **Significado de las series**
 - **72 horas:** número de equipos que no enviaron su estado en las últimas 72 horas.
 - **7 días:** número de equipos que no enviaron su estado en las últimas 7 días.
 - **30 días:** número de equipos que no enviaron su estado en las últimas 30 días.

- **Filtros pre establecidos desde el panel**

OFFLINE COMPUTERS



Figura 65: zonas activas del panel Equipos sin conexión

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Equipos sin conexión** filtrado por **Última conexión** = Hace más de 72 horas
- **(2)** Listado **Equipos sin conexión** filtrado por **Última conexión** = Hace más de 7 días
- **(3)** Listado **Equipos sin conexión** filtrado por **Última conexión** = Hace más de 30 días

14.3.3 Protección desactualizada

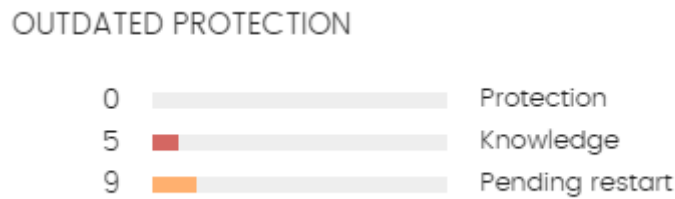


Figura 66: panel de Protección desactualizada

Protección desactualizada muestra los equipos cuya última versión del fichero de firmas instalada difiere en más de 3 días del fichero publicado por Panda Security. También muestra los equipos cuya versión del motor de protección difiere en más de 7 días del publicado por Panda Security. Por lo tanto, estos equipos pueden ser vulnerables frente a los ataques de amenazas.

- **Significado de las series**

El panel muestra el porcentaje y el número de equipos vulnerables por estar desactualizados, divididos en tres conceptos:

- **Protección:** desde hace 7 días el equipo tiene un motor de protección instalado anterior a la última versión publicada por Panda Security.
- **Conocimiento:** desde hace 3 días el equipo no se actualiza con el fichero de firmas publicado.
- **Pendiente de reinicio:** el equipo requiere un reinicio para completar la actualización.

- **Filtros pre establecidos desde el panel**

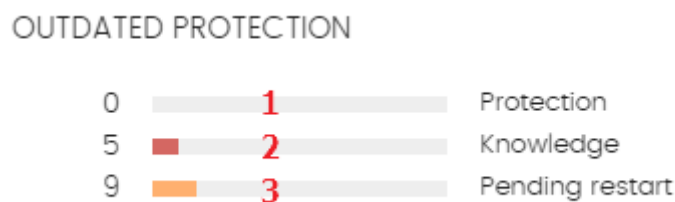


Figura 67: zonas activas de Protección desactualizada

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

- **(1)** Listado **Estado de protección de los equipos** filtrado por **Protección actualizada = No**
- **(2)** Listado **Estado de protección de los equipos** filtrado por **Conocimiento = No**
- **(3)** Listado **Estado de protección de los equipos** filtrado por **Protección actualizada = Pendiente de reinicio**

14.3.4 Amenazas permitidas por el administrador

THREATS ALLOWED BY THE ADMINISTRATOR



Figura 68: panel Amenazas permitidas por el administrador

Endpoint Protection / Plus elimina de forma automática o desinfecta si es posible todos los programas clasificados como malware.

En el caso de que el administrador quiera permitir la ejecución de un elemento ya clasificado como amenaza, **Endpoint Protection / Plus** implementa recursos para restaurar los ficheros eliminados.

- **Significado de las series**

El panel representa el número total de elementos que el administrador excluyó del bloqueo, desagregados en tres conceptos:

- Malware
- PUP
- En clasificación

- **Filtros pre establecidos desde el panel**

THREATS ALLOWED BY THE ADMINISTRATOR



Figura 69: zonas activas del panel Amenazas permitidas por el administrador

- (1) Listado **Amenazas permitidas por el administrador** sin filtros
- (2) Listado **Amenazas permitidas por el administrador** filtrado por **Clasificación actual** = malware
- (3) Listado **Amenazas permitidas por el administrador** filtrado por **Clasificación actual** = PUP
- (4) Listado **Amenazas permitidas por el administrador** filtrado por **Clasificación actual** = En clasificación (bloqueados y sospechosos)

14.3.5 Amenazas detectadas por el antivirus

THREATS DETECTED BY THE ANTIVIRUS

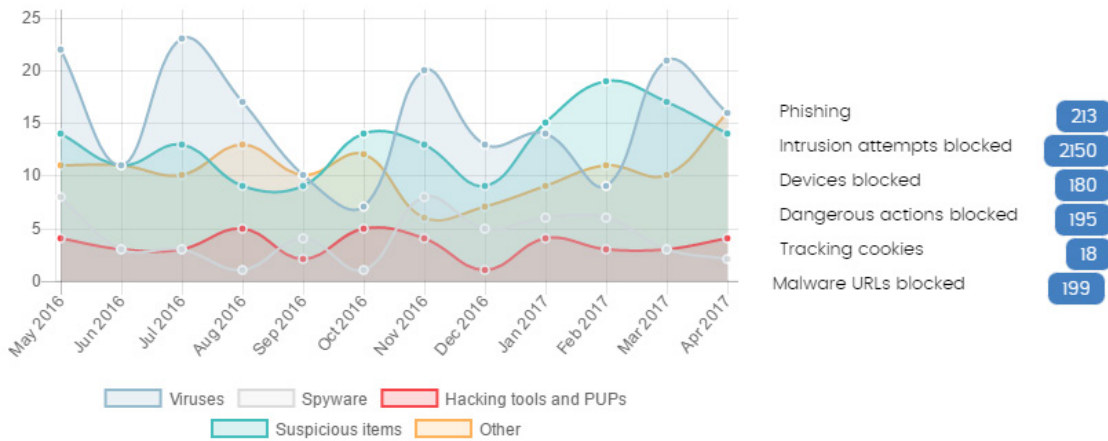


Figura 70: panel Amenazas detectadas por el antivirus

Amenazas detectadas por el antivirus consolida todos los intentos de intrusión que **Endpoint Protection / Plus** gestionó en el periodo de tiempo establecido.

Los datos reflejados abarcan todos los vectores de infección y todas las plataformas soportadas, de manera que el administrador pueda disponer de datos concretos (volumen, tipo, forma de ataque) relativos a la llegada de malware a la red, durante un intervalo de tiempo determinado.

- **Significado de las series**

Este panel está formado por dos secciones: un gráfico de líneas y un listado resumen.

El diagrama de líneas representa las detecciones encontradas en el parque informático a lo largo del tiempo separadas por tipo de malware:

- **Virus y spyware**
- **Herramientas de hacking y PUPs**
- **Sospechosos**
- **Phising**
- **Otros**

En el eje de las Ys se muestran las ocurrencias y en el de las Xs las fechas.

El listado de la derecha muestra eventos relevantes que el administrador puede querer revisar en busca de síntomas o situaciones potenciales de peligro.

- **Intentos de intrusión bloqueados:** son ataques detenidos por el Cortafuegos y el Sistema de prevención de intrusos

- **Dispositivos bloqueados:** periféricos bloqueados por el módulo de Control de dispositivos
- **Operaciones peligrosas bloqueadas:** detecciones realizadas por análisis del comportamiento local
- **Tracking cookies:** cookies detectadas para registrar la navegación de los usuarios
- **URL con malware bloqueadas:** direcciones Web que apuntaban a páginas con malware

- **Filtros pre establecidos desde el panel**

El listado se muestra con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel.

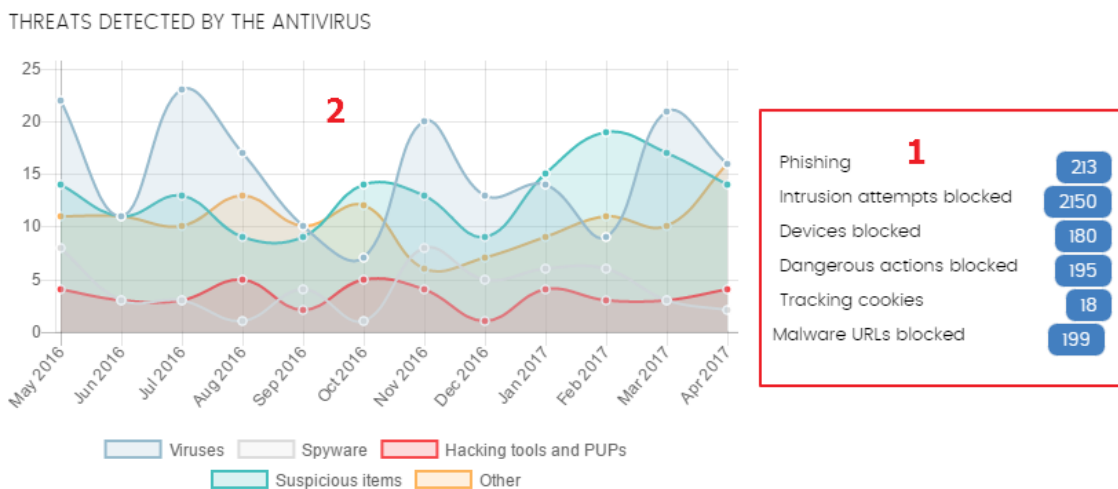


Figura 71: zonas activas del panel Amenazas detectadas por el antivirus

- **(1)** Listado **Amenazas detectadas por el antivirus** filtrado por **Tipo de amenaza** = (Phishing O Intentos de intrusión bloqueados O dispositivos bloqueados O Acciones peligrosas bloqueadas O Tracking cookies O URLs con malware)
- **(2)** Listado **Amenazas detectadas por el antivirus** sin filtro

14.3.6 Filtrado de contenidos en servidores Exchange

Característica solo disponible en Endpoint Protection Plus.

Este panel muestra la cantidad de mensajes que fueron bloqueados por el filtro de contenidos del servidor Exchange.

- **Significado de las series**

Este panel presenta dos series de datos de tipo histórico: el número de mensajes filtrados por contener adjuntos con extensión peligrosa, y por doble extensión.

CONTENT FILTERING FOR EXCHANGE SERVERS

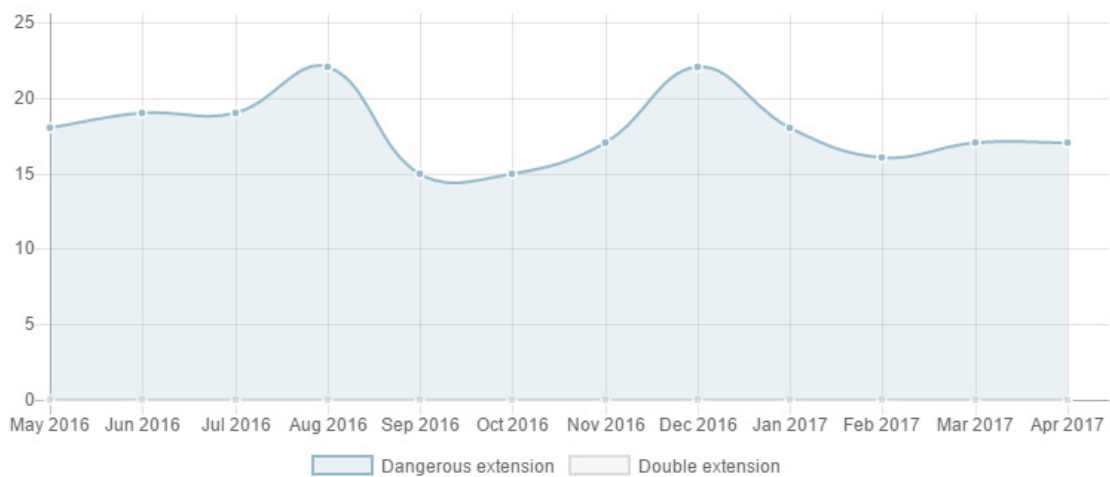


Figura 72: panel Filtrado de contenidos en servidores Exchange

Al pasar el ratón por las series se muestra un tooltip con la siguiente información:

- **Extensión peligrosa:** número de mensajes filtrados por contener adjuntos con extensión peligrosa.
- **Doble extensión:** número de mensajes filtrados por contener adjuntos con doble extensión.

14.3.7 Accesos a páginas web



Característica solo disponible en Endpoint Protection Plus.

Este panel muestra mediante un gráfico de tarta la distribución de categorías Web solicitadas por los usuarios de la red.

- **Significado de las series**

El panel de tipo tarta muestra los 10 grupos de páginas web más importantes que **Endpoint Protection / Plus** soporta a la hora de categorizar las páginas web navegadas por los usuarios de la red:

- **Odio e intolerancia**
- **Actividades criminales**
- **Búsqueda de empleo**
- **Contactos y anuncios personales**
- **Finanzas**

- Confidencial
- Ocio y espectáculos
- Gobierno
- Drogas ilegales
- Otros

En la zona de la leyenda del panel se muestran los porcentajes de peticiones que encajan con cada categoría.

WEB ACCESS

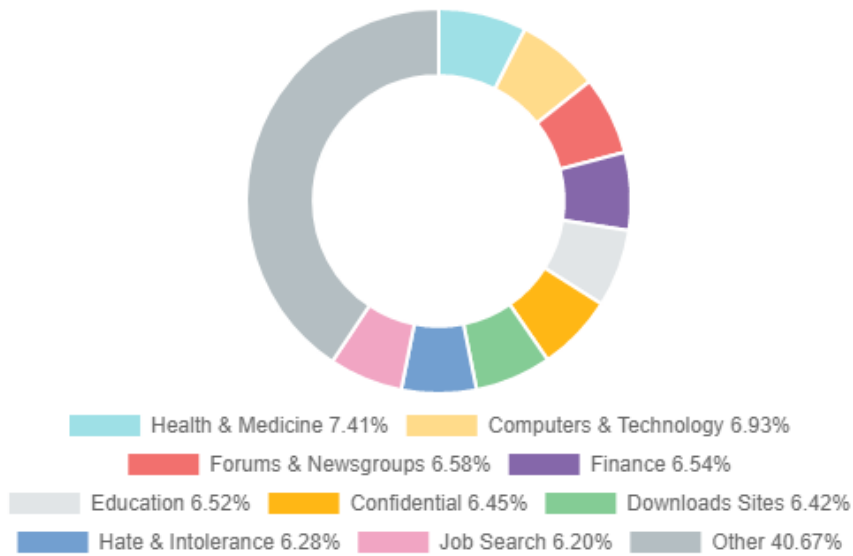


Figura 73: panel Accesos a páginas web

- Filtros pre establecidos desde el panel

WEB ACCESS

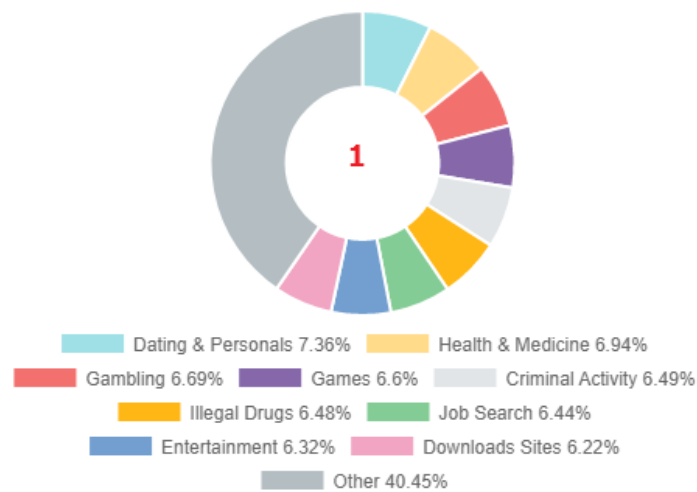


Figura 74: zonas activas del panel Accesos a páginas web

- (1) Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada

14.3.8 Categorías más accedidas (top 10)



Característica solo disponible en Endpoint Protection Plus

Top 10 most accessed categories		
Category	Access attempts	Computers
Job Search	4848	60
Computers & Technology	4800	62
Illegal Drugs	4759	60
Entertainment	4647	61
Health & Medicine	4578	60
Criminal Activity	4566	60
Forums & Newsgroups	4512	60
Downloads Sites	4495	60
Games	4471	60
Dating & Personals	4424	60

[See full report](#)

Figura 75: panel Categorías más accedidas

En este panel se destalla en número de accesos y el número de equipos que han accedido a las 10 categorías de páginas más visitadas.

Cada categoría indica el número de accesos totales en el rango de fechas seleccionado, y el número de equipos que han accedido una o más veces a esa categoría.

- **Filtros pre establecidos desde el panel**

Al hacer clic en cada una de las categorías del panel se establece un filtro.

- (1) Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada
- (2) Listado **Accesos a páginas web por equipo** sin filtrar

Top 10 most accessed categories		
Category	Access attempts	Computers
Job Search	4848	60
Computers & Technology	4800	62
Illegal Drugs	4759	60
Entertainment	4647	61
Health & Medicine 1	4578	60
Criminal Activity	4566	60
Forums & Newsgroups	4512	60
Downloads Sites	4495	60
Games	4471	60
Dating & Personals	4424	60

[See full report](#)

Figura 76: zonas activas del panel Categorías mas accedidas (Top 10)

14.3.9 Categorías más accedidas por equipo (top 10)



Característica solo disponible en Endpoint Protection Plus.

Top 10 most accessed categories by computer		
Computer	Category	Access attempts
RHERNANDEZ	Computers & Technology	339
admins-mini-5.synapse.com	Computers & Technology	215
TestDevice_00_45	Entertainment	169
TESTDEVICE_00_04	Illegal Drugs	168
TESTDEVICE_00_36	Hate & Intolerance	167
TESTDEVICE_00_14	Entertainment	163
TESTDEVICE_00_22	Downloads Sites	157
TESTDEVICE_00_08	Hate & Intolerance	153
TestDevice_00_43	Games	151
TESTDEVICE_00_40	Job Search	151

[See full report](#)

Figura 77: panel Categorías más accedidas por equipo (Top 10)

En este panel se detallan en número de accesos ordenados por categorías de los 10 equipos que más han visitado a la web.

- Filtros pre establecidos desde el panel

Top 10 most accessed categories by computer		
Computer 1	Category 2	Access attempts
RHERNANDEZ	Computers & Technology	339
admins-mini-5.synapse.com	Computers & Technology	215
TestDevice_00_45	Entertainment	169
TESTDEVICE_00_04	Illegal Drugs	168
TESTDEVICE_00_36	Hate & Intolerance	167
TESTDEVICE_00_14	Entertainment	163
TESTDEVICE_00_22	Downloads Sites	157
TESTDEVICE_00_08	Hate & Intolerance	153
TestDevice_00_43	Games	151
TESTDEVICE_00_40	Job Search	151

[See full report](#)

Figura 78: zonas activas del panel Categorías más accedidas por equipo (Top 10)

Al hacer clic en los elementos mostrados se establece un tipo de filtro diferente.

- (1) Listado **Accesos a páginas web por equipo** filtrado por **Equipo** = Equipo seleccionado
- (2) Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada

14.3.10 Categorías más bloqueadas (top 10)



Característica solo disponible en Endpoint Protection Plus.

Top 10 most blocked categories		
Category	Denied access attempts	Computers
Entertainment	4946	60
Illegal Drugs	4870	60
Games	4693	60
Downloads Sites	4678	60
Forums & Newsgroups	4569	60
Government	4538	60
Health & Medicine	4499	60
Education	4469	60
Confidential	4447	60
Criminal Activity	4435	60

[See full report](#)

Figura 79: panel Categorías más bloqueadas (Top 10)

En este panel se indican las 10 categorías de páginas más bloqueadas de la red, junto al número de accesos bloqueados y el número de equipos que realizaron la visita y fueron bloqueados

- Filtros pre establecidos desde el panel

Top 10 most blocked categories		
Category	Denied access attempts	Computers
Entertainment	4946	60
Illegal Drugs	4870	60
Games	4693	60
Downloads Sites 1	4678	60
Forums & Newsgroups	4569	60
Government	4538	60
Health & Medicine	4499	60
Education	4469	60
Confidential	4447	60
Criminal Activity	4435	60

[See full report](#)

Figura 80: ponas activas del panel Categorías más bloqueadas (Top 10)

- (1) Listado **Accesos a páginas web por equipo** filtrado **por Categoría** = Categoría seleccionada

14.3.11 Categorías más bloqueadas por equipo (Top 10)



Característica solo disponible en Endpoint Protection Plus

El panel muestra los 10 pares equipo – categoría con mayor número de accesos bloqueados de la red, indicando el nombre del equipo, la categoría y el número de accesos denegados por cada par equipo – categoría.

Top 10 most blocked categories by computer		
Computer	Category	Denied access attempts
TESTDEVICE_00_00	Games	194
TESTDEVICE_00_14	Entertainment	171
TestDevice_00_45	Entertainment	163
TESTDEVICE_00_28	Illegal Drugs	157
TestDevice_00_23	Downloads Sites	156
TestDevice_00_51	Job Search	156
TESTDEVICE_00_30	Health & Medicine	154
TestDevice_00_59	Computers & Technology	149
TESTDEVICE_00_48	Entertainment	147
TestDevice_00_31	Finance	146

[See full report](#)

Figura 81: panel categorías más bloqueadas por equipo (Top 10)

- Filtros pre establecidos desde el panel

Top 10 most blocked categories by computer		
Computer	Category	Denied access attempts
TESTDEVICE_00_00	Games	194
TESTDEVICE_00_14	Entertainment	171
TestDevice_00_45	Entertainment	163
TESTDEVICE_00_28	Illegal Drugs	157
TestDevice_00_23	Downloads Sites	156
TestDevice_00_51	Job Search	156
TESTDEVICE_00_30	Health & Medicine	154
TestDevice_00_59	Computers & Technology	149
TESTDEVICE_00_48	Entertainment	147
TestDevice_00_31	Finance	146

[See full report](#)

Figura 82: zonas activas del panel Categorías más bloqueadas por equipo (Top 10)

- (1) Listado **Accesos a páginas web por equipo** filtrado por **Nombre de equipo** = Equipo seleccionado
- (2) Listado **Accesos a páginas web por equipo** filtrado por **Categoría** = Categoría seleccionada

14.4. Introducción a los listados

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

14.4.1 Plantillas, configuraciones y vistas

Los listados en **Endpoint Protection / Plus** son, en realidad, *Plantillas*, que admiten una o más *Configuraciones*. Una plantilla puede entenderse como una fuente de datos sobre un tema específico.

Una *Configuración* es una asignación específica de valores a las herramientas de búsqueda y filtrado asociada a cada plantilla.

La *Configuración* de una *Plantilla* da como resultado una *Vista de listado* o simplemente, "*Listado*", que el administrador puede modificar y copiar para poder consultar posteriormente. De esta forma el administrador puede ahorrar tiempo definiendo búsquedas y filtros sobre *Listados* que más tarde volverá a utilizar.

Plantillas de listado

Existen 8 plantillas correspondientes a otros tantos tipos de información, resumidos a continuación:

- Amenazas detectadas por el antivirus
- Intentos de intrusión bloqueados
- Dispositivos bloqueados
- Accesos a páginas web por categoría (solo **Endpoint Protection Plus**)
- Accesos a páginas web por equipo (solo **Endpoint Protection Plus**)
- Estado de protección de los equipos
- Licencias
- Equipos no administrados descubiertos

Adicionalmente, existen otras plantillas accesibles directamente desde el menú de contexto de ciertos listados o desde algunos widgets del panel de control. El acceso a estos listados se indica en su descripción.

Configuraciones

En el actual contexto de listados, una configuración especifica un filtro de información definido por el administrador asociado a una plantilla. Cada plantilla tiene diferentes filtros de información según el tipo de datos que muestra.



Figura 83: generación de tres listados a partir de una misma plantilla / fuente de datos

El administrador puede establecer tantas configuraciones de filtros sobre una misma plantilla como quiera, con el objetivo de facilitar las diferentes lecturas de una misma fuente de datos.

Vistas de listado / listados

La unión de una *Plantilla* y una *Configuración* da como resultado una vista particular del listado. Una plantilla puede tener varias vistas asociadas, si el administrador ha creado otras tantas configuraciones tomando como base una misma plantilla.

Copy of Malware run 1
Save 5

Enter a description... 2

Computer Search... Filters 3 ⋮ 6

Type

Malware

Search date type:

Range

Run

True

Range

Last month

Action

- Quarantined
- Blocked
- Disinfected
- Deleted
- Allowed

Accessed data

- All -

External connections

- All -

4

Filter 7

Computer	Threat	Path				Action	Date
Machine_Cu stomer_1_01 4a	Malware Nam e 14	Malware Path Sample 14	●	●	○	Blocked	4/24/2017 2:1 8:00 AM
Machine_Cu stomer_1_01 4a	Malware Nam e 12	Malware Path Sample 12	●	●	○	Blocked	4/24/2017 1:2 0:00 AM
Machine_Cu stomer_1_01 4a	Malware Nam e 10	Malware Path Sample 10	●	●	○	Deleted	4/24/2017 12: 22:00 AM

Figura 84: vista general de un listado

14.4.2 Panel Mis listados

Todos los listados creados se muestran en el panel izquierdo bajo la rama **Mis listados**, en el menú superior **Estado**.

Endpoint Protection
on Aether Platform

DASHBOARDS

Security

Licenses

Executive report

MY LISTS Add

- Unprotected servers
- Unprotected workstations...

Figura 85: panel lateral Mis listados

14.4.3 Crear un listado personalizado

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

- Desde el panel lateral Mis listados

Al hacer clic sobre el link **Añadir** del panel **Mis listados** se muestra una ventana con un desplegable que contiene las 8 plantillas disponibles (Figura 86).

- Desde un panel del dashboard
 - Haz clic en un widget en el panel de control para abrir su plantilla asociada
 - Haz clic en el menú de contexto (6) y selecciona **Copiar**. Se creará un nuevo listado.
 - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar** (5)
- Desde un listado ya creado
 - Haz una copia de un listado ya generado mediante el menú contextual (6) y haz clic en **Copiar**.

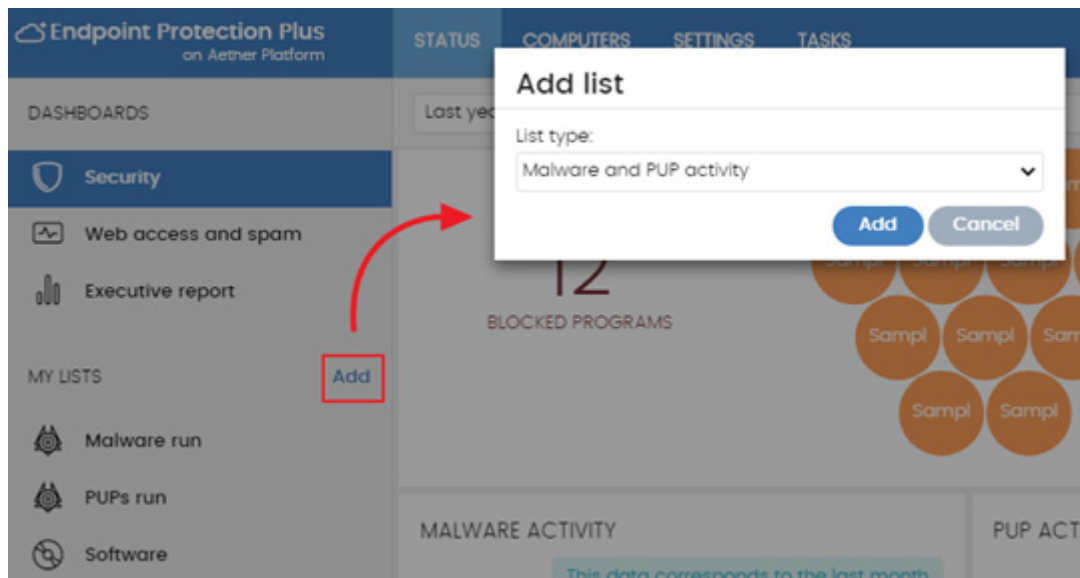


Figura 86: listados disponibles

- Desde el menú de contexto del panel Mis listados

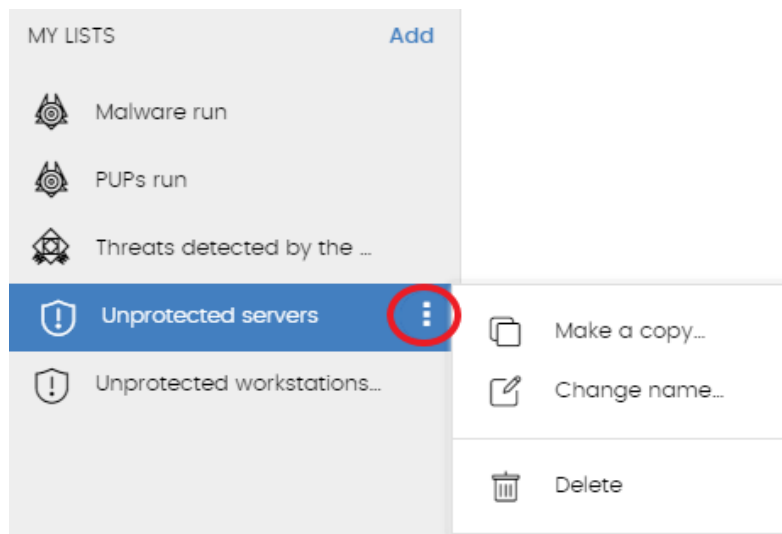




Figura 87: menú de contexto de los listados accesibles desde el Panel de listados

- Haz clic en el menú de contexto asociado al listado a copiar.
- Haz clic en **Hacer una copia**.
- Se creará una nueva vista de la plantilla que podrás modificar a tu gusto.

14.4.4 Borrar un listado

Puedes borrar un listado de dos maneras posibles:

- Desde el panel mis listados
 - Haz clic el menú de contexto asociado al nombre del listado en el panel **Mis Listados**.
 - Haz clic en el icono  .
- Desde el propio listado
 - Haz clic en el menú de contexto (6).
 - Haz clic en el icono  del menú desplegado.

14.4.5 Configurar un listado personalizado

- Asigna un nuevo nombre al listado (1). Por defecto la consola forma un nuevo nombre para el listado añadiendo la cadena "Nuevo" al tipo de listado o "Copia" si el listado es la copia de uno anterior.
- Asigna una descripción (2): este paso es opcional.
- Haz clic en el link **Filtros** (3) para desplegar el bloque de búsqueda y configuración.

- Ajusta el filtro de información **(4)** para mostrar los datos relevantes.
- Haz clic en **Filtrar (7)** para aplicar el filtro configurado con el objetivo de comprobar si el filtrado configurado se ajusta a las necesidades. En el cuerpo del listado **(8)** se mostrará la búsqueda resultado.
- Haz clic en el botón **Guardar (5)**. El listado se añadirá en el panel de la izquierda bajo **Mis listados**, y será accesible a partir de ese momento haciendo clic en su nombre.

Además, en el botón de menú **(6)** se incluye la opción de exportar el listado en formato csv y la opción de hacer una copia del listado.



La exportación de listados en formato csv amplía la información mostrada en los listados de la consola Web. Estos campos están documentados más adelante en cada listado.

14.5. Listados disponibles

14.5.1 Listado de Estado de protección de los equipos

Este listado muestra en detalle todos los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles que no estén protegidos por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo desprotegido	Cadena de caracteres
Antivirus	Estado de la protección antivirus	 No instalado  Error  Activado  Desactivado  Sin licencia
Protección actualizada	<p>Indica si el módulo de la protección instalado en el equipo coincide con la última versión publicada o no.</p> <p>Al pasar el puntero del ratón por encima del campo se indica la versión de la protección instalada</p>	 Actualizado  No actualizado (7 días sin actualizar desde la publicación)  Pendiente de reinicio
Conocimiento	Indica si el fichero de firmas descargado en el equipo coincide con la última versión publicada o no.	 Actualizado


Campo	Comentario	Valores
	Al pasar el puntero del ratón por encima del campo se indica la fecha de actualización de la versión descargada	 No actualizado (3 días sin actualizar desde la publicación)
Ultima conexión	Fecha del ultimo envío del estado de Endpoint Protection / Plus a la nube de Panda Security	Fecha

Tabla 17: campos del listado Estado de protección de los equipos

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el Software Endpoint Protection / Plus se instaló con éxito en el equipo	Fecha
Fecha de la última actualización	Fecha de la última actualización del agente	Fecha
Plataforma	Sistema operativo instalado en el equipo	Windows Linux MacOS Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor	Cadena de caracteres

Campo	Comentario	Valores
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada	Binario
Versión de la protección	Versión interna del módulo de protección	Cadena de caracteres
Conocimiento actualizado	Indica si el fichero de firmas descargado en el equipo es la última versión publicada	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas	Fecha
Antivirus de archivo	Estado de la protección asociada	No instalado
Antivirus de correo		Error
Antivirus de navegación web		Activado
Protección firewall		Desactivado
Control de dispositivos		Sin licencia
Antivirus para Exchange server		
Antispam para Exchange server		
Control de acceso a páginas web		

Tabla 18: campos del fichero exportado Estado de protección de los equipos

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo	Estación Portátil Móvil Servidor
Buscar equipo	Nombre del equipo	Cadena de caracteres
Ultima conexión	Fecha del último envío del estado de Endpoint Protection / Plus a la nube de Panda Security	Todos Más de 72 horas Más de 7 días Más de 30 días
Protección actualizada	Indica si la protección tiene la última versión publicada o no	Todos Si No Pendiente de reinicio
Plataforma	Sistema operativo instalado en el equipo	Todos Windows Linux Mac Android
Conocimiento	Estado de la actualización del fichero de firmas para la protección antivirus	Binario

Campo	Comentario	Valores
Motivo de desprotección		No instalado Protección con error Activado Protección Desactivada Sin licencia Sin protección

Tabla 19: campos de filtrado para el listado Estado de protección de los equipos

14.5.2 Listado de Amenazas permitidas por el administrador

Este listado muestra en detalle todos los elementos en clasificación o clasificados como amenazas que el administrador actualmente está permitiendo su ejecución.



Este listado solo es accesible desde el widget Amenazas permitidas por el administrador.


Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo	Tipo del fichero	Malware PUP Bloqueado Bloqueado reclasificado a Malware / PUP Bloqueado reclasificado a Goodware
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Permitido por	Usuario de la consola que creó la exclusión	Cadena de caracteres
Permitido desde	Fecha en la que el administrador creó la exclusión del fichero	Fecha
Borrar 	Permite retirar la exclusión del fichero	

Tabla 20: campos del listado Amenazas permitidas por el administrador

Campos incluidos en fichero exportado

Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo actual	Tipo del fichero en el momento en el que se accede al listado	Malware PUP Bloqueado Bloqueado reclasificado a Malware / PUP Bloqueado reclasificado a Goodware
Tipo original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo	Malware PUP Bloqueado Bloqueado reclasificado a Malware / PUP Bloqueado reclasificado a Goodware1
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Permitido por	Usuario de la consola que creó la exclusión	Cadena de caracteres
Permitido desde	Fecha en la que el administrador creó la exclusión del fichero	Fecha

Tabla 21: campos del fichero exportado Amenazas permitidas por el administrador

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	Amenaza: Nombre del malware o PUP Permitido por: Usuario de la consola que creó la exclusión Archivo: Nombre del fichero que contiene la amenaza Hash: Cadena resumen de identificación del archivo	Cadena de caracteres
Clasificación actual	Tipo del fichero en el momento en el que se accede al listado	Malware PUP Goodware En clasificación (Bloqueados y sospechoso)

Campo	Comentario	Valores
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo	Malware PUP Bloqueado Sospechoso

Tabla 22: Campos de filtrado para el listado Amenazas permitidas por el administrador

14.5.3 Listado Historial de amenazas permitidas por el administrador

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a las amenazas y ficheros desconocidos en clasificación que el administrador permitió su ejecución.

Este listado no tiene su panel correspondiente y es accesible únicamente mediante el botón **Historial** del listado **Amenazas permitidas por el administrador**, situado en la esquina superior derecha.

Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo	Tipo de la amenaza que se permitió su ejecución	Malware PUP Bloqueado Sospechoso
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido	Exclusión eliminada por el usuario Exclusión eliminada por reclasificación Exclusión añadida por el usuario Exclusión mantenida por reclasificación
Usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido	Cadena de caracteres
Fecha	Fecha en la que se produjo el evento	Fecha

Tabla 23: Campos del listado Historial de amenazas permitidas por el administrador

Campos incluidos en fichero exportado

Campo	Comentario	Valores
Amenaza	Nombre del malware o PUP que se permite su ejecución. Si es un elemento desconocido se indica el nombre del fichero en su lugar	Cadena de caracteres
Tipo actual	Ultimo tipo de la amenaza que se permitió su ejecución	Malware PUP Bloqueado Sospechoso
Tipo original	Tipo del fichero cuando se produjo el evento	
Archivo	Nombre del fichero desconocido o que contiene la amenaza	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido	Exclusión eliminada por el usuario Exclusión eliminada por reclasificación Exclusión añadida por el usuario Exclusión mantenida por reclasificación
Usuario	Cuenta de usuario de la consola que inicio el cambio en el fichero permitido	Cadena de caracteres
Fecha	Fecha en la que se produjo el evento	Fecha

Tabla 24: campos del fichero exportado Historial de amenazas permitidas por el administrador

Herramienta de filtrado

Campo	Comentario	Valores
Buscar	<p>Usuario: Cuenta de usuario de la consola que inicio el cambio en el fichero permitido</p> <p>Archivo: Nombre del fichero que contiene la amenaza</p> <p>Hash: Cadena resumen de identificación del archivo</p>	Cadena de caracteres
Clasificación actual	Tipo del fichero en el momento en el que se accede al listado	Malware PUP Goodware En clasificación (Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo	Malware PUP Bloqueado

Campo	Comentario	Valores
		Sospechoso
Acción	Acción aplicada sobre el elemento permitido	Exclusión eliminada por el usuario Exclusión eliminada por reclasificación Exclusión añadida por el usuario Exclusión añadida por reclasificación

Tabla 25: campos de filtrado para el listado Historial de amenazas permitidas por el administrador

14.5.4 Listado de Amenazas detectadas por el antivirus

El listado de detecciones ofrece información consolidada y completa de todas las detecciones hechas en todas las plataformas soportadas y desde todos los vectores de infección analizados, utilizados por los hackers para intentar infectar equipos en la red.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se realizó la detección	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Grupo	Grupo dentro del árbol de grupos de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
Ruta	Ruta del sistema de ficheros donde reside la amenaza	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza detectada	Virus Spyware Herramientas de hacking y PUPs Phising Sospechosos Acciones peligrosas bloqueadas Tracking cookies URLs con malware Otros
Acción	Acción desencadenada por Endpoint Protection / Plus	Borrado Desinfectado En cuarentena Bloqueado Proceso terminado
Fecha	Fecha de la detección	Fecha

Tabla 26: campos del listado Amenazas detectadas por el antivirus

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Móvil Servidor
Equipo	Nombre del equipo donde se realizó la detección	Cadena de caracteres
Nombre malware	Nombre de la amenaza detectada	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza detectada	Virus Spyware Herramientas de hacking y PUPs Phising Sospechosos Acciones peligrosas bloqueadas Tracking cookies URLs con malware Otros
Tipo de malware	Subclase de la amenaza detectada	Cadena de caracteres
Número de detecciones	Número de veces que Endpoint Protection / Plus detectó la amenaza en el equipo y en la fecha indicada.	Numérico
Acción	Acción desencadenada por Endpoint Protection / Plus	Borrado Bloqueado Proceso terminado
Detectado por	Determina el motor que realizó la detección	Antivirus: la amenaza fue detectada por el motor de antivirus.
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza	Cadena de caracteres
Excluido	La amenaza ha sido excluida del análisis por el administrador para permitir su ejecución	Binario
Fecha	Fecha de la detección	Fecha
Grupo	Grupo dentro del árbol de grupos de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo donde se realizó la detección	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 27: campos del fichero exportado Amenazas detectadas por el antivirus

Herramienta de filtrado

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se realizó la detección	Cadena de caracteres
Tipo de fecha de búsqueda	<p>Rango: permite establecer un intervalo de fechas desde el día1 presenta hacia atrás</p> <p>Fecha personalizada: permite establecer una fecha concreta del calendario</p>	Últimas 24 horas Últimos 7 días Último mes Último año
Tipo de equipo	Clase del dispositivo	Estación Portátil Móvil Servidor
Tipo de Amenazas	Clase de amenaza	Virus Spyware Herramientas de hacking y PUPs Phising Sospechosos Acciones peligrosas bloqueadas Tracking cookies URLs con malware Otros
Equipo	Nombre del equipo donde se realizó la detección	Cadena de caracteres

Tabla 28: Campos de filtrado para el listado Amenazas detectadas por el antivirus

14.5.5 Listado de Accesos a páginas web por categoría



Característica solo disponible en Endpoint Protection Plus.

Campo	Comentario	Valores
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Dispositivos permitidos	Número de equipos que han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Número de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico

Campo	Comentario	Valores
Equipos denegados	Número de equipos que no han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 29: campos del listado Accesos a páginas web por categoría

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría.	Numérico
Dispositivos permitidos	Número de equipos que han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico
Accesos denegados	Número de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico
Equipos denegados	Número de equipos que no han podido acceder a páginas pertenecientes a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 30: campos del fichero exportado Accesos a páginas web por equipo

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de fecha de búsqueda	Rango: permite establecer un intervalo de fechas desde el día presente hacia atrás Fecha personalizada: permite establecer una fecha concreta del calendario	Últimas 24 horas Últimos 7 días Último mes Último año
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas

Tabla 31: campos de filtrado para el listado Accesos a páginas web por equipo

14.5.6 Listado de Accesos a páginas web por equipo



El acceso a páginas web por equipo lista todos los equipos encontrados en la red indicando el número de accesos permitidos y denegados por cada categoría accedida.

Campo	Comentario	Valores
Equipo	Nombre del equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Grupo	Grupo dentro del árbol de grupos de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría,	Numérico
Accesos denegados	Numero de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico

Tabla 32: campos del listado Accesos a páginas web por equipo

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Móvil Servidor
Grupo	Grupo dentro del árbol de grupos de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Equipo	Nombre del equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Accesos permitidos	Número de accesos que se han permitido a la categoría de página indicada en el campo Categoría,	Numérico
Accesos denegados	Numero de accesos que se han denegado a la categoría de página indicada en el campo Categoría.	Numérico
Descripción		Cadena de caracteres

Tabla 33: campos del fichero exportado Accesos a páginas web por equipo

Herramienta de búsqueda

Campo	Comentario	Valores
Tipo de fecha de búsqueda	Rango: permite establecer un intervalo de fechas desde el día presente hacia atrás Fecha personalizada: permite establecer una fecha concreta del calendario	Últimas 24 horas Últimos 7 días Último mes Último año
Categoría	Categoría a la que pertenece la página accedida	Enumeración de las categorías soportadas
Tipo de equipo	Clase del dispositivo	Estación Portátil Móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres

Tabla 34: campos de filtrado para el listado Accesos a páginas web por equipo

14.5.7 Listado de Dispositivos bloqueados

Este listado muestra en detalle todos los equipos de la red que tienen limitado el acceso a alguno de los periféricos conectados.

Campo	Comentario	Valores
Equipo	Nombre del equipo desprotegido	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
Tipo	Familia del dispositivo afectado por la configuración de seguridad	Unidades de almacenamiento extraíbles Dispositivos de captura de imágenes Unidades de CD/DVD Dispositivos Bluetooth Módems Dispositivos móviles
Acción	Tipo de acción efectuada sobre el dispositivo	Bloquear Permitir Lectura Permitir Lectura y escritura
Fecha	Fecha en la se aplicó la acción	Fecha

Tabla 35: campos del listado Dispositivos bloqueados

Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio	Cadena de caracteres
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Equipo	Nombre del equipo	Cadena de caracteres
Nombre	Nombre del periférico conectado al equipo y afectado por la configuración de seguridad	Cadena de caracteres
Id. de instancia	Identificador del dispositivo afectado	Cadena de caracteres
Número de detecciones	Número de veces que se detectó una operación no permitida sobre el dispositivo	Numérico
Acción	Tipo de acción efectuada sobre el dispositivo	Bloquear Permitir Lectura Permitir Lectura y escritura
Detectado por	Módulo que detectó la operación no permitida	Control de dispositivos
Fecha	Fecha en la se detectó la operación no permitida	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Endpoint Protection / Plus a la que pertenece el equipo	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 36: campos del fichero exportado Dispositivos bloqueados

Herramienta de filtrado

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo	Estación Portátil Dispositivo móvil Servidor
Buscar equipo	Nombre del equipo	Cadena de caracteres
Tipo de fecha de búsqueda	Rango: permite establecer un intervalo de fechas desde el	Últimas 24 horas Últimos 7 días

	día1 presenta hacia atrás	Último mes
	Rango personalizado: permite establecer una fecha concreta del calendario	
Tipo de dispositivo	Familia del dispositivo afectado por la configuración de seguridad	Unidades de almacenamiento extraíbles Dispositivos de captura de imágenes Unidades de CD/DVD Dispositivos Bluetooth Módems Dispositivos móviles

Tabla 37: campos de filtrado para el listado Dispositivos bloqueados

14.5.8 Listado de Licencias

El listado de **Licencias** se trata en el capítulo 5 Licencias.

14.5.9 Listado de Equipos no administrados descubiertos

El listado de **Equipos no administrados descubiertos** se trata en el capítulo 6.

14.6. Listados incluidos por defecto

La consola de administración incluye cuatro listados pre generados:

- Estaciones y portátiles desprotegidos
- Servidores desprotegidos

Estaciones y portátiles desprotegidos

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

- Equipos en proceso de instalación del software **Endpoint Protection / Plus** o con error en la instalación
- Equipos con la protección desactivada o en estado de error
- Equipos sin licencia asignada o con licencia caducada

Servidores desprotegidos

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

- Servidores en proceso de instalación del software **Endpoint Protection / Plus** o con error en la instalación

- Servidores con la protección desactivada o en estado de error
- Servidores sin licencia asignada o con licencia caducada

15. Gestión de elementos excluidos y en backup / cuarentena

[Recursos para la gestión de exclusiones](#)

[Añadir una exclusión de elementos](#)

[Gestión de los elementos excluidos](#)

[Gestión de la cuarentena](#)

15.1. Introducción

Endpoint Protection / Plus es capaz de equilibrar la eficacia del servicio de seguridad ofrecido, con el impacto sobre la actividad diaria que percibirán los usuarios protegidos. Este equilibrio se consigue a través de varias herramientas configurables por el administrador:

- Gestión de la ejecución de los procesos clasificados como amenazas
- Gestión de la zona de backup / cuarentena

Gestión de la ejecución de los procesos clasificados como malware

En otras situaciones el administrador puede querer permitir la ejecución de ciertos tipos de malware que, a pesar de estar considerados como amenazas, implementan algunas funcionalidades valoradas por los usuarios. Este es el caso por ejemplo de PUPs, programas generalmente en forma de barras de navegador, que ofrecen capacidades de búsquedas al tiempo que recolectan información privada del usuario o confidencial de la empresa con objetivos publicitarios.

Gestión de la cuarentena

Finalmente, el administrador puede querer tener acceso a los elementos considerados como amenazas y, por lo tanto, eliminados de los equipos de los usuarios.

15.2. Acceso a los recursos para la gestión de exclusiones


La gestión de exclusiones se realiza desde distintas pantallas de la consola de administración, por este motivo se muestra a continuación una guía de referencia que permita localizar cada uno de los recursos de forma rápida.

Todos los recursos mostrados son accesibles desde el Menú superior **Estado (1)**, haciendo clic en los widgets apropiados del panel de control.

Listados

- **Para listar los elementos actualmente excluidos de bloqueos:** Panel Amenazas permitidas por el administrador **(1)**.
- **Para listar un histórico de los elementos actualmente excluidos:** Panel Amenazas permitidas por el administrador **(1)**, menú contextual Histórico.
- **Para listar los cambios de estado de un elemento excluido:** Panel Amenazas permitidas por el administrador **(1)**, menú contextual Histórico.

Añadir y eliminar

- **Para añadir una exclusión sobre una amenaza:** Panel **Amenazas detectadas por el antivirus (2)**, selección de una amenaza, **Restaurar y No volver a detectar**.
- **Para eliminar una exclusión:** Panel Amenazas permitidas por el administrador **(1)**, selección de una amenaza con el icono  .

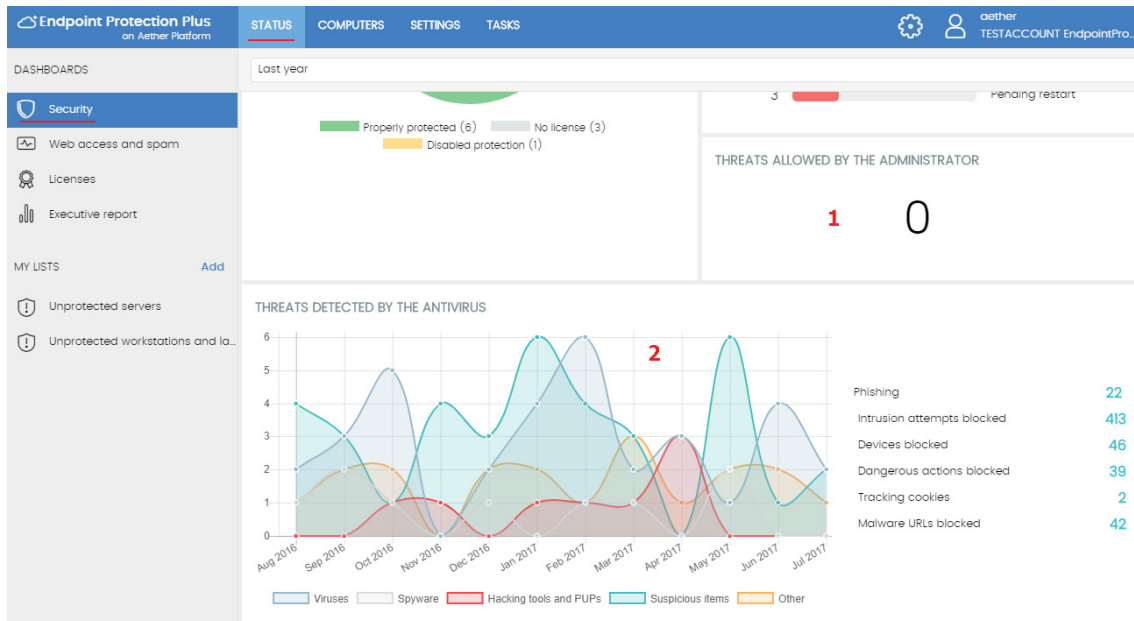


Figura 88: acceso a las herramientas de gestión de exclusiones desde el panel de control

15.3. Añadir una exclusión de elementos

Si el administrador quiere permitir la ejecución de un fichero ya clasificado como amenaza, el control de exclusiones se realizará desde el panel **Amenazas detectadas por el antivirus**.

15.3.1 Exclusiones de elementos clasificados como amenazas

Al excluir un elemento clasificado como malware se está permitiendo la ejecución de un programa que **Endpoint Protection / Plus** ya ha clasificado de forma efectiva como dañino o peligroso para el sistema.

Desde el panel **Amenazas detectadas por el antivirus** el administrador puede utilizar el botón **Restaurar y no volver a detectar** seleccionando previamente la amenaza que quiere permitir su ejecución.

Una vez excluido el elemento se añadirá al listado de **Amenazas y otros elementos excluidos**, tal y como se indica en el siguiente punto.

15.4. Gestión de los elementos excluidos

La gestión de todos los elementos excluidos y el comportamiento del sistema ante reclasificaciones, tanto de procesos conocidos y clasificados como de sospechosos se realiza desde el panel **Amenazas permitidas por el administrador**.

Este panel permite visualizar y gestionar los ficheros actualmente permitidos, así como acceder a un histórico de los elementos excluidos.

Listado de exclusiones en curso

Amenazas permitidas por el administrador muestra los elementos que tienen una exclusión activa. Todos los elementos que aparecen listados tienen permitida su ejecución.

Historial

Haciendo clic en el menú de contexto, **Historial** podrás visualizar el histórico de cambios realizado sobre los ficheros excluidos en **Endpoint Protection / Plus**. El listado permite ver el ciclo de estados completo de un fichero, desde que entra en el listado de **Amenazas permitidas por el administrador** hasta que sale del mismo, pasando por los cambios de estado intermedios que el sistema o el administrador pueda haber aplicado.

15.5. Gestión de la zona de backup / cuarentena

La cuarentena en **Endpoint Protection / Plus** es el área de backup donde se copian los elementos eliminados por haber sido clasificados como amenaza.

El almacenamiento de los elementos eliminados se realiza en el propio equipo del usuario, en el directorio `quarantine` de la carpeta donde se instaló el software. Se trata de una carpeta inaccesible al resto de procesos del equipo y cifrada, de manera que no es posible el acceso ni la ejecución de los programas allí contenidos de forma directa, si no es a través de la consola Web.



La cuarentena es compatible con las plataformas Windows, Mac OS X y Linux. No se soporta en dispositivos Android

El envío de elementos al área de backup es automático y establecido por el departamento de Panda Labs en Panda Security, según sea su clasificación después de haber efectuado su análisis.

Una vez que los elementos sospechosos han sido enviados a Panda Security para su análisis, se pueden producir cuatro 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, permanecerán en la cuarentena durante 7 días.
- Si se comprueba que no se trata de elementos perjudiciales, son restaurados directamente a su ubicación.
- Si se comprueba que son elementos sospechosos se almacenan durante 30 días como máximo. Si finalmente resultan ser *goodware* se restauran automáticamente.



Endpoint Protection / Plus no borra ningún fichero del equipo del usuario. Todos los elementos eliminados son en realidad enviados al área de backup.

15.5.1 Visualización de los elementos en cuarentena

El administrador puede visualizar los elementos introducidos en la cuarentena mediante el widget o el listado Amenazas detectadas por el antivirus.

Con ayuda de las herramientas de filtrado se puede obtener el listado de elementos introducidos en cuarentena, reflejados en el campo **Acción** como "Movido a cuarentena" o "Eliminado".

15.5.2 Restaurar elementos de cuarentena

Para restaurar un elemento en cuarentena haz clic en el botón **Restaurar y no volver a detectar**. Esta acción no solo copiará el fichero a su ubicación original, sino que restaurará los permisos, propietario, entradas del registro referidas al fichero y otra información referida al fichero.

16. Herramientas de resolución

Desinfección automática de equipos
Análisis / desinfección bajo demanda de
equipos
Reiniciar equipos
Notificar un problema
Acceso externo a la consola

16.1. Introducción

Endpoint Protection / Plus cuenta con varias herramientas de resolución que permiten al administrador solucionar los problemas encontrados en las fases de Protección, Detección y Monitorización del ciclo de protección adaptativa.

Algunas de estas herramientas son automáticas y no necesitan que el administrador intervenga, otras sin embargo requieren la ejecución de acciones concretas a través de la consola Web.

La Tabla 38 muestra las herramientas disponibles por plataforma y su tipo (automático o manual).

Herramienta de resolución	Plataforma	Tipo	Objetivo
Desinfección automática de equipos	Windows, Mac OS X, Linux, Android	Automático	Desinfectar o mover a cuarentena el malware encontrado en el momento de la infección de los equipos.
Análisis / Desinfección bajo demanda de equipos	Windows, Mac OS X, Linux, Android	Automático (programado) Manual	Analizar, desinfectar o mover a cuarentena el malware encontrado en los equipos protegidos en el momento que lo requiera el administrador o en franjas horarias concretas
Reinicio bajo demanda	Windows	Manual	Fuerza un reinicio del equipo para aplicar actualizaciones, completar desinfecciones manuales y corregir errores detectados en la protección

Tabla 38: herramientas de resolución disponibles en **Endpoint Protection / Plus**

16.2. Desinfección automática de equipos

La desinfección automática es realizada en tiempo real por la Protección antivirus.

Ante una detección de malware **Endpoint Protection / Plus** desinfectará de forma automática los elementos afectados siempre y cuando exista un método de desinfección conocido. En su defecto, el elemento se moverá a cuarentena.

La desinfección automática no requiere de la intervención del administrador, si bien es necesario que esté seleccionada la casilla **Protección de archivos** en la configuración de seguridad asignada al equipo.



Consulta el capítulo 10 *Configuración de seguridad para estaciones y servidores* para más información sobre los modos de bloqueo en **Endpoint Protection / Plus** y configuraciones disponibles en el módulo antivirus.

16.3. Análisis / Desinfección bajo demanda de equipos

El análisis y desinfección bajo demanda de ficheros se realiza de dos maneras: mediante la creación de tareas de análisis programadas y mediante un análisis inmediato.

16.3.1 Tareas de análisis programadas

Las tareas de análisis programadas se pueden crear de tres maneras en la consola de administración:

- Desde el menú superior **Tareas**
- Desde el menú superior **Equipos**
- Desde la pestaña **Detalle** del equipo



Consulta el capítulo 13 Tareas para obtener más información sobre las Tareas programadas de análisis y su creación desde el menú superior Tareas.

Creación de tareas programadas de análisis desde el menú superior Equipos

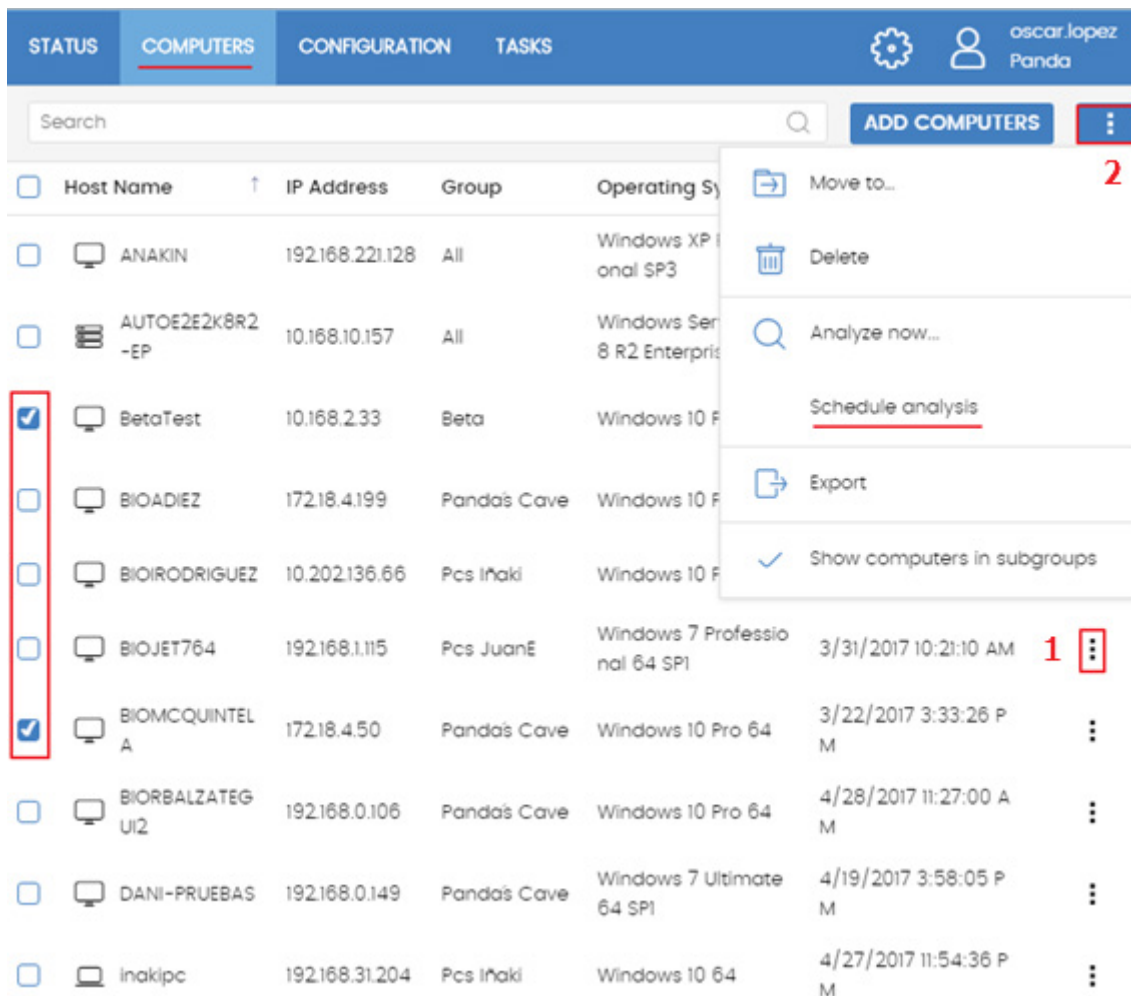
- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la izquierda.
- Para programar una tarea de análisis en un único equipo: selecciona el menú de contexto del equipo en el listado de equipos **(1)**.
- Para programar una tarea de análisis en varios equipos: mediante las casillas de selección, marca los equipos que quieres analizar y haz clic el menú de contexto global **(2)**.
- Selecciona en el menú desplegable la opción **Programar análisis**.

Creación de tareas programadas desde Detalle del equipo

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la izquierda.
- Haz clic en el equipo a analizar para mostrar la ventana de detalle.
- En el menú de contexto selecciona la opción **Programar análisis**.

16.3.2 Análisis inmediato

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la izquierda.
- Para lanzar un análisis inmediato en un único equipo: selecciona el menú de contexto del equipo en el listado de equipos.
- Para lanzar un análisis inmediato en varios equipos: mediante las casillas de selección, marca los equipos que quieres analizar y haz clic el menú de contexto global.
- Selecciona en el menú desplegable la opción **Analizar ahora**.



The screenshot shows the Panda management console interface. At the top, there are navigation tabs: STATUS, COMPUTERS (selected), CONFIGURATION, and TASKS. On the right, there is a user profile for 'oscar.lopez Panda'. Below the navigation is a search bar and an 'ADD COMPUTERS' button. The main area displays a table of computers with columns: Host Name, IP Address, Group, Operating System, and a date/time column. A red box highlights the 'Equipos' menu icon in the top right corner. A context menu is open over the table, showing options: Move to..., Delete, Analyze now..., Schedule analysis (underlined), Export, and Show computers in subgroups. A red box also highlights the '1' icon in the date/time column of the 'BIOJET764' row.

<input type="checkbox"/>	Host Name	IP Address	Group	Operating System		
<input type="checkbox"/>	ANAKIN	192.168.221.128	All	Windows XP Professional SP3		
<input type="checkbox"/>	AUTOE2E2K8R2-EP	10.168.10.157	All	Windows Server 8 R2 Enterprise		
<input checked="" type="checkbox"/>	BetaTest	10.168.2.33	Beta	Windows 10 F		
<input type="checkbox"/>	BIOADIEZ	172.18.4.199	Panda's Cave	Windows 10 F		
<input type="checkbox"/>	BIOIRODRIGUEZ	10.202.136.66	Pcs Iñaki	Windows 10 F		
<input type="checkbox"/>	BIOJET764	192.168.1.115	Pcs JuanE	Windows 7 Professional 64 SP1	3/31/2017 10:21:10 AM	1
<input checked="" type="checkbox"/>	BIOMCQUINTELA	172.18.4.50	Panda's Cave	Windows 10 Pro 64	3/22/2017 3:33:26 PM	
<input type="checkbox"/>	BIORBALZATEGUI2	192.168.0.106	Panda's Cave	Windows 10 Pro 64	4/28/2017 11:27:00 AM	
<input type="checkbox"/>	DANI-PRUEBAS	192.168.0.149	Panda's Cave	Windows 7 Ultimate 64 SP1	4/19/2017 3:58:05 PM	
<input type="checkbox"/>	Inakipc	192.168.31.204	Pcs Iñaki	Windows 10 64	4/27/2017 11:54:36 PM	

Figura 89: creación de tareas programadas desde el menú Equipos

16.4. Reiniciar equipos

Para mantener los equipos actualizados a la última versión de la protección, o si se detecta algún error en la protección, el administrador podrá actuar remotamente desde la consola Web y reiniciar los equipos involucrados.

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la izquierda.
- Para reiniciar un único equipo: selecciona el menú de contexto del equipo en el listado de equipos.
- Para reiniciar varios equipos: mediante las casillas de selección, marca los equipos que quieres reiniciar y haz clic el menú de contexto global.
- Selecciona en el menú desplegable la opción **Reiniciar**.

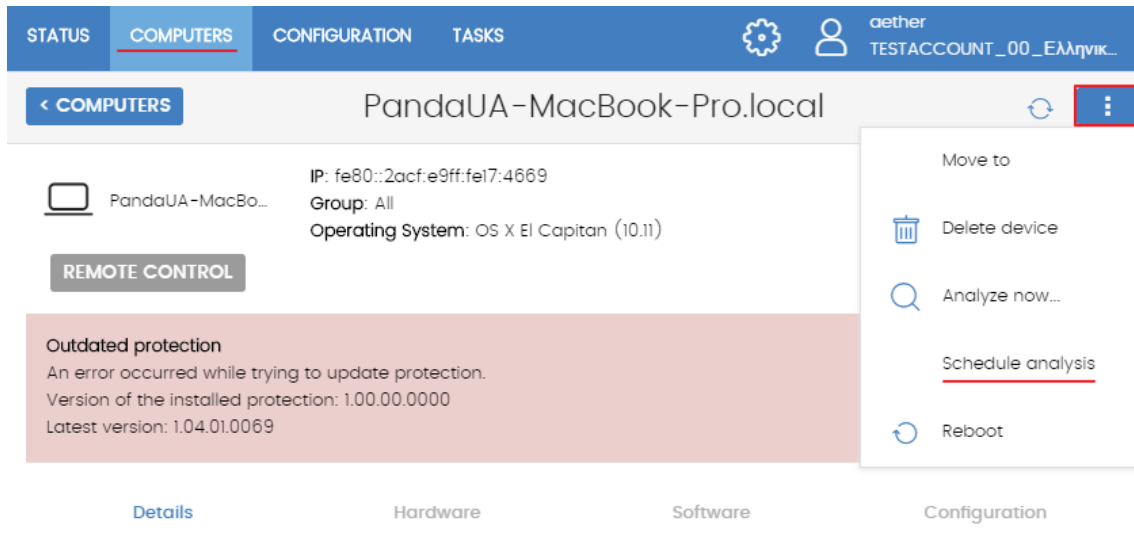


Figura 90: análisis programado desde el detalle de equipo

16.5. Notificar un problema

En algunas ocasiones es posible que el software **Endpoint Protection / Plus** instalado en los equipos de la red presente un mal funcionamiento. Algunos de los síntomas pueden ser:

- Fallos en el reporte del estado del equipo
- Fallos en la descarga de conocimiento o de las actualizaciones del motor
- Motor en estado de error

Si **Endpoint Protection / Plus** presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Panda Security a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior **Equipos**, selecciona los equipos que presenten errores y haz clic en el menú de contexto. Se desplegará un menú con la opción **Indícanos el problema**.

16.6. Permitir el acceso externo a la consola Web

Para aquellos problemas que el administrador de la red no pueda resolver, existe la posibilidad de habilitar el acceso a la consola únicamente para equipo de soporte de Panda Security. Sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Usuarios**.
- En la pestaña usuarios haz clic en el control Permitir al equipo de Panda Security S.L. acceder a mi consola.

17. Alertas

Alertas por correo

17.1. Introducción

El sistema de alertas es un recurso utilizado por **Endpoint Protection / Plus** para comunicar de forma rápida al administrador situaciones de importancia para el buen funcionamiento del servicio de seguridad.

En conjunto, las alertas informan al administrador de las situaciones mostradas a continuación:

- Cambios en el estado de las licencias
- Errores de instalación y desprotegidos

17.2. Alertas por correo

Las alertas por correo son mensajes enviados por **Endpoint Protection / Plus** a las cuentas de correo de los administradores. El sistema genera mensajes cuando se producen determinados eventos, que se enviaron a las cuentas de correo configuradas como destinatarios.

17.2.1 Configuración de alertas por correo

Desde el menú superior **Configuración**, en el panel de la izquierda **Alertas** se muestra la ventana de configuración.

Desde esta ventana el administrador podrá indicar las direcciones de correo que recibirán los mensajes en **Enviar las alertas a la siguiente dirección**, así como habilitar o deshabilitar de forma global cada una de las alertas a enviar, y explicadas en el punto siguiente.

17.2.2 Visibilidad del administrador y envío de alertas

Las alertas se definen de forma independiente por cada usuario de la consola. El contenido de una alerta queda limitado por la visibilidad de los equipos administrados que tiene el rol del usuario.

17.2.3 Tipos de alertas

Equipos con error en la protección y errores durante la instalación

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada equipo desprotegido de la red
- Equipos con la protección en estado de error o fallo en la instalación de la protección

El mensaje de correo mostrará la información siguiente:

- Nombre del equipo desprotegido
- Grupo al que pertenece el equipo

- Información relativa al equipo (Nombre, descripción, sistema operativo, dirección IP, Grupo, ruta del directorio activo, dominio).
- Fecha y hora en formato UTC
- Motivo de la desprotección: **Protección con error** o **Error instalando**.

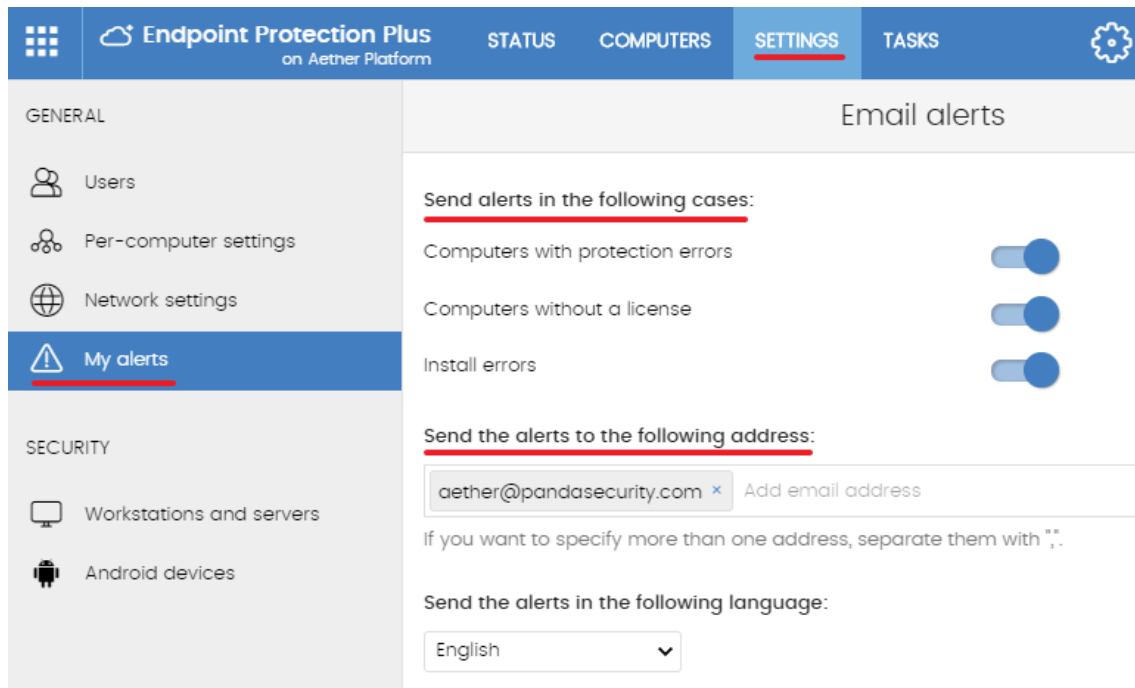


Figura 91: pantalla de configuración de las alertas

Equipos sin licencia

Se generará un mensaje de este tipo en las condiciones mostradas a continuación:

- Por cada equipo que intenta licenciarse, pero no lo consigue por falta de licencias libres.

El mensaje de correo mostrará la información siguiente:

- Nombre del equipo desprotegido
- Grupo al que pertenece el equipo
- Información relativa al equipo (Nombre, descripción, sistema operativo, dirección IP, Grupo, ruta del directorio activo, dominio)
- Fecha y hora en formato UTC
- Motivo de la desprotección: **Equipo sin licencia**

Adicionalmente, se generará un único mensaje en las condiciones mostradas a continuación:

- Por cada mantenimiento que caduque.

El mensaje de correo mostrará la información siguiente:

- Número de equipos que se han quedado sin licencia
- Número de licencias que han caducado, asignadas al mantenimiento
- Nombre del producto asignado al mantenimiento caducado
- Fecha de caducidad del mantenimiento

18. Informes

Roles y generación de informes
Generación bajo demanda de informes
ejecutivos
Envío programado de informes ejecutivos

18.1. Introducción

Endpoint Protection / Plus permite generar y enviar de forma automática o manual informes ejecutivos que consolidan toda la información recogida en el periodo de tiempo establecido por el administrador.

18.2. Generación bajo demanda de informes ejecutivos

En el menú superior **Estado**, haz clic en el panel izquierdo **Informe ejecutivo** para mostrar la ventana de configuración de informes. La consola web muestra dos pestañas: **Visualizar** y **Programar**, haz clic en la pestaña **Visualizar** para configurar la generación de un informe ejecutivo bajo demanda.

18.2.1 Información requerida para la generación de informes bajo demanda

Será necesario suministrar la información mostrada a continuación:

- **Información de las siguientes fechas:** indica el intervalo de tiempo que abarcará el informe
 - **Último mes**
 - **Últimos 7 días**
 - **Últimas 24 horas**
- **Información de los siguientes equipos:** especifica de qué equipos se extraerán datos para generar el informe ejecutivo.
 - **Todos los equipos**
 - **Equipos seleccionados:** muestra el árbol de grupos, permitiendo seleccionar de forma individual los grupos mediante las casillas de selección.
- **Incluir el siguiente contenido:** permite seleccionar el tipo de información que será incluida en el informe.
 - **Estado de las licencias:** muestra la información de las licencias contratadas y consumidas. Consulta el capítulo 5 Licencias.
 - **Estado de la red:** muestra el funcionamiento de software **Endpoint Protection / Plus** en los equipos de la red donde ha sido instalado. Incluye los widgets **Equipos desprotegidos** y **Protección desactualizada** del panel de control. Consulta el capítulo 14 Visibilidad del malware y del parque informático para obtener más información.
 - **Detecciones:** muestra las amenazas detectadas en la red. Incluye los widgets, **Amenazas detectadas por el antivirus** y **Filtrado de contenidos en Exchange servers** (solo **Endpoint Protection Plus**) del panel de control. Consulta el capítulo 14 Visibilidad del malware y del parque informático para obtener más información.
 - **Acceso web y Spam** (solo **Endpoint Protection Plus**): muestra la actividad web de los usuarios. Incluye los widgets **Accesos a páginas web**, **Categorías más accedidas (Top 10)**, **Categorías más accedidas por equipo (Top 10)**, **Categorías más bloqueadas (Top 10)**, **Categorías más bloqueadas por equipo (Top 10)** y **Spam detectado en Exchange Server**. Consulta el capítulo 14 Visibilidad del malware y del parque informático para obtener más información.

Una vez completada la información haz clic en el botón **Visualizar** para abrir una ventana independiente con el contenido del informe.




Comprueba que ni navegador ni ninguna extensión instalada impidan la visualización de pop ups.

18.3. Envío programado de informes ejecutivos

En el menú superior **Estado**, haz clic en el panel izquierdo **Informe ejecutivo** para mostrar la ventana de configuración de informes. La consola web muestra dos pestañas: **Visualizar** y **Programar**, haz clic en la pestaña **Programar** para configurar la generación periódica de un informe ejecutivo.

18.3.1 Información requerida para la generación de informes programados

La ventana de informes programados muestra una lista de todos los informes previamente configurados. Para agregar un nuevo informe programado haz clic en el botón **Añadir**. Para borrar un informe previamente generado haz clic en el icono . Para editar un informe previamente creado haz clic en su nombre.

Para configurar un informe programado será necesario suministrar la información mostrada a continuación:

- **Nombre:** nombre del informe programado que se mostrará en la lista de informes configurados.
- **Enviar automáticamente:** permite programar el envío del informe o guardar la configuración sin enviarla, para poder generarlo de forma manual más adelante.
- **Fecha y ritmo de envío:** permite especificar la fecha del envío y cada cuanto tiempo se producirá. Selecciona **Todos los días**, **Todas las semanas** o **Todos los meses**. Dependiendo de la selección se ajustará el contenido de los desplegados mostrados para poder definir con precisión la fecha de envío.
- **La siguiente información:** al hacer clic en esta zona la ventana cambia y muestra los parámetros de configuración **Fechas**, **Equipos** y **Contenidos**:
 - **Información de las siguientes fechas:** indica el intervalo de tiempo que abarcará el informe.
 - **Último mes**
 - **Últimos 7 días**
 - **Últimas 24 horas**
 - **Información de los siguientes equipos:** especifica de qué equipos se extraerán datos para generar el informe ejecutivo.
 - **Todos los equipos**
 - **Equipos seleccionados:** muestra el árbol de grupos, permitiendo seleccionar de forma individual los grupos mediante las casillas de selección.

- **Incluir el siguiente contenido:** permite seleccionar el tipo de información que será incluida en el informe.
 - **Estado de las licencias:** muestra la información de las licencias contratadas y consumidas. Consulta el capítulo 5 Licencias.
 - **Estado de la red:** muestra el funcionamiento de software **Endpoint Protection / Plus** en los equipos de la red donde ha sido instalado. Incluye los widgets **Equipos desprotegidos** y **Protección desactualizada** del panel de control. Consulta el capítulo 14 Visibilidad del malware y del parque informático para obtener más información.
 - **Detecciones:** muestra las amenazas detectadas en la red. Incluye los widgets, **Amenazas detectadas por el antivirus** y **Filtrado de contenidos en Exchange servers** (solo **Endpoint Protection Plus**) del panel de control.
 - **Acceso web y Spam** (solo **Endpoint Protection Plus**): muestra la actividad web de los usuarios. Incluye los widgets **Accesos a páginas web**, **Categorías más accedidas (Top 10)**, **Categorías más accedidas por equipo (Top 10)**, **Categorías más bloqueadas (Top 10)**, **Categorías más bloqueadas por equipo (Top 10)** y **Spam detectado en Exchange Server**. Consulta el capítulo 14 Visibilidad del malware y del parque informático para obtener más información.
- **Para:** introduce las direcciones de correo separadas por comas que recibirán el informe.
- **CC**
- **CCO:** introduce las direcciones de correo ocultas que recibirán el informe.
- **Asunto:** especifica el campo asunto del correo electrónico.
- **Formato:** selecciona el formato (Pdf, Excel, Word) del fichero adjunto al correo electrónico que contendrá el informe.
- **Idioma:** selecciona el idioma en el que se enviará el informe.

19. Control y supervisión de la consola de administración

¿Qué es una cuenta de usuario?

¿Qué es un rol?

¿Qué es un permiso?

Acceso a la configuración de cuentas de usuario y roles

Creación y configuración de cuentas de usuario

Creación y configuración de roles

Registro de la actividad

19.1. Introducción

En este capítulo se detallan los recursos implementados en **Endpoint Protection / Plus** para controlar y supervisar las acciones realizadas por los administradores de red que acceden a la consola web de gestión.

Esta supervisión y control se implementa en forma de tres recursos, mostrados a continuación:

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

19.2. ¿Qué es una cuenta de usuario?

Es un recurso gestionado por **Endpoint Protection / Plus**, formado por un conjunto de información que el sistema utiliza para regular el acceso de los administradores a la consola web, y establecer las acciones que éstos podrán realizar sobre los equipos de los usuarios.

Las cuentas de usuario son utilizadas únicamente por los administradores de IT que acceden a la consola **Endpoint Protection / Plus**. Generalmente, cada administrador de IT tiene una única cuenta de usuario personal, pudiéndose crear tantas cuentas de usuario como se considere necesarias.



A diferencia del resto del documento, donde la palabra "usuario" se refiere a la persona que utiliza un equipo o dispositivo, en este capítulo "usuario" se asocia a la cuenta de usuario que el administrador utiliza para acceder a la consola web.

19.2.1 Estructura de una cuenta de usuario

Una cuenta de usuario está formada por los siguientes elementos:

- **Login de la cuenta:** asignada en el momento de la creación de la cuenta, su objetivo es identificar al administrador que accede a la consola.
- **Contraseña de la cuenta:** asignada una vez creada la cuenta, permite regular el acceso a la consola de administración.
- **Rol asignado:** seleccionable una vez creada la cuenta de usuario, permite determinar los equipos sobre los cuales la cuenta tendrá capacidad de administración, y las acciones que podrá ejecutar sobre los mismos.

19.2.2 ¿Qué es el usuario principal?

El usuario principal es la cuenta de usuario suministrada por Panda Security al cliente en el momento de provisionar el servicio **Endpoint Protection / Plus**. Esta cuenta tiene asignado el rol **Control total** explicado más abajo en este mismo capítulo.

La configuración del usuario principal no se puede editar ni borrar.

19.3. ¿Qué es un rol?

Un rol es una configuración específica de permisos de acceso a la consola, que se aplica a una o más cuentas de usuario. De esta forma, un administrador concreto estará autorizado a ver o modificar determinados recursos de la consola, dependiendo del rol asignado a la cuenta de usuario con la que accedió a **Endpoint Protection / Plus**.

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

19.3.1 Estructura de un rol

Un rol está formado por los siguientes elementos:

- **Nombre del rol:** designado en el momento de la creación del rol, su objetivo es meramente identificativo.
- **Grupos sobre los que tiene permisos:** permite restringir el acceso a determinados equipos de la red. Para configurar esta restricción es necesario especificar las carpetas del árbol de grupos a las cuales la cuenta de usuario tendrá acceso.
- **Juego de permisos:** permite determinar las acciones concretas que las cuentas de usuario podrán ejecutar sobre los equipos que pertenezcan a los grupos definidos con accesibles.

19.3.2 ¿Por qué son necesarios los roles?

En un departamento de IT de tamaño pequeño, todos los técnicos van a acceder a la consola como administradores sin ningún tipo de límite; sin embargo, en departamentos de IT de mediano o gran tamaño con un parque informático grande para administrar, es muy posible que sea necesario organizar o segmentar el acceso a los equipos, aplicando tres criterios:

- **Según la cantidad de equipos a administrar.**

Redes de tamaño medio/grande o redes pertenecientes a delegaciones de una misma empresa pueden requerir distribuir y asignar equipos a técnicos concretos. De esta forma, los dispositivos de una delegación administrados por un técnico en particular serán invisibles para los técnicos que administren los dispositivos de otras delegaciones.

También pueden existir restricciones de acceso a datos delicados de ciertos usuarios. En estos casos se suele requerir una asignación muy precisa de los técnicos que van a poder manipular los dispositivos que los contienen.

- **Según el cometido del equipo a administrar.**

Según la función que desempeñe, un equipo puede asignarse a un técnico experto en ese campo: por ejemplo, los servidores de correo Exchange pueden ser asignados a un grupo de técnicos especialistas, y de la misma forma otros equipos como los dispositivos Android podrían no ser visibles para este grupo.

- **Según los conocimientos o perfil del técnico.**

Según las capacidades del técnico o su función dentro del departamento de IT, puede asignarse únicamente un acceso de monitorización/validación (solo lectura) o, por el contrario, uno más avanzado, como el de modificación de las configuraciones de seguridad de los equipos. Por ejemplo, es frecuente encontrar en compañías grandes un determinado grupo de técnicos dedicados únicamente a desplegar software en los equipos de la red.

Estos tres criterios se pueden solapar, dando lugar a una matriz de configuraciones muy flexible y fácil de establecer y mantener, que permita delimitar perfectamente las funciones de la consola para cada técnico, en función de la cuenta de usuario con la que accedan al sistema.

19.3.3 El rol Control total

Una licencia de uso de **Endpoint Protection / Plus** viene con un rol de **Control total** predefinido. A este rol pertenece la cuenta de administración creada por defecto, y con ella es posible realizar absolutamente todas las acciones disponibles en la consola.

El rol **Control total** no puede borrarse, modificarse ni visualizarse, y cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola.

19.3.4 El rol Monitorización

El rol **Monitorización** está especialmente indicado para aquellos administradores de red encargados de la vigilancia del parque informático, pero que no poseen los permisos suficientes para realizar modificaciones, como por ejemplo editar configuraciones o lanzar análisis bajo demanda.

Los permisos activados para el rol de **Monitorización** son los siguientes:

- Ver configuraciones de seguridad para estaciones y servidores
- Ver configuraciones de seguridad para dispositivos Android
- Visualizar detecciones de amenazas

- Visualizar accesos a páginas web y spam (solo **Endpoint Protection Plus**)
- Acceso a informes avanzados

19.4. ¿Qué es un permiso?

Un permiso regula el acceso a un aspecto concreto de la consola de administración. Existen 15 permisos que establecen el acceso a otros tantos aspectos de la consola de **Endpoint Protection / Plus**. Una configuración particular de todos los permisos disponibles genera un rol, que podrá ser asignado a una o más cuentas de usuario.

Los permisos implementados en **Endpoint Protection / Plus** se listan a continuación:

- Gestionar usuarios y roles
- Asignar licencias
- Modificar el árbol de equipos
- Añadir, descubrir y eliminar equipos
- Configurar proxys e idioma
- Modificar ajustes por equipo (actualizaciones, contraseñas etc)
- Reiniciar equipos
- Configurar seguridad para estaciones y servidores
- Ver configuraciones de seguridad para para estaciones y servidores
- Configurar seguridad para dispositivos Android
- Ver configuraciones de seguridad para dispositivos Android
- Visualizar detecciones y amenazas
- Visualizar accesos a páginas web y spam (solo **Endpoint Protection Plus**)
- Lanzar análisis y desinfectar
- Excluir temporalmente amenazas (Malware, PUP y Bloqueados)

19.4.1 Significado de los permisos implementados

A continuación, se detallan los permisos existentes, indicando la funcionalidad de cada uno de ellos.

Gestionar usuarios y roles

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

Asignar licencias

- **Al activar:** el usuario de la cuenta podrá asignar y retirar licencias de los equipos gestionados.

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

Modificar el árbol de equipos

- **Al activar:** el usuario de la cuenta tiene pleno acceso al árbol de grupos, pudiendo crear y eliminar grupos, y mover equipos a grupos ya creados.
- **Al desactivar:** el usuario de la cuenta puede visualizar el árbol de carpetas y las configuraciones asignadas a cada grupo, pero no puede crear nuevos grupos ni mover equipos. Podrá cambiar la configuración de un grupo, ya que esta acción queda regulada con el permiso **Configurar seguridad para estaciones y servidores**, o **Configurar seguridad para dispositivos Android**.

Añadir, descubrir y eliminar equipos

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

Configurar proxys e idioma

- **Al activar:** el usuario de la cuenta podrá crear nuevas configuraciones de tipo **Proxy e Idioma**, editar o borrar las existentes y asignarlas a los equipos integrados en la consola.
- **Al desactivar:** el usuario de la cuenta dejará de poder crear nuevas configuraciones de tipo **Proxy e Idioma**, borrar las existentes o cambiar la asignación de los equipos integrados a la consola.



Puesto que un cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Proxy e Idioma asignada, al desactivar Configurar Proxys e idioma se obliga también a desactivar el permiso Modificar el árbol de equipos,

Modificar ajustes por equipo (actualizaciones, contraseñas etc)

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



Puesto que un cambio de carpeta de un equipo en el árbol de carpetas puede provocar un cambio de configuración de Ajustes por equipo asignado, al desactivar Ajustes por equipo se obliga también a desactivar el permiso Modificar el árbol de equipos,

Reiniciar equipos

- **Al activar:** el usuario de la cuenta podrá reiniciar equipos desde el menú superior **Equipos** y seleccionando en el menú de contexto **Reiniciar**, para estaciones y servidores Windows, Linux y MacOS.
- **Al desactivar:** el usuario de la cuenta dejará de poder reiniciar equipos.

Configurar seguridad para estaciones y servidores

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



Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de Estaciones y servidores, al desactivar Configurar seguridad para estaciones y servidores se obliga también a desactivar el permiso Modificar el árbol de equipos,

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

Ver configuraciones de seguridad para estaciones y servidores



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

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

Configurar seguridad para dispositivos Android

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



Puesto que el cambio de grupo de un equipo en el árbol de grupos puede provocar un cambio de configuración de dispositivos Android, al desactivar Configurar seguridad para dispositivos Android se obliga también a desactivar el permiso Modificar el árbol de equipos,

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

Ver configuraciones de seguridad para dispositivos Android



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

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

Visualizar detecciones y amenazas

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



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

Visualizar accesos a páginas web y spam



Característica solo disponible en Endpoint Protection Plus.

- **Al activar:** el usuario de la cuenta podrá acceder a los paneles y listados de la sección **Accesos web y spam** en el menú superior **Estado**.
- **Al desactivar:** el usuario de la cuenta ya no podrá acceder a los paneles y listados de la sección **Accesos web y spam** en el menú superior **Estado**.

Lanzar análisis y desinfectar

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

Excluir temporalmente amenazas (Malware, PUP y Bloqueados)

- **Al activar:** el usuario de la cuenta puede restaurar y no volver a detectar o dejar de permitir amenazas ya clasificadas.

- **Al desactivar:** el usuario de la cuenta no podrá restaurar amenazas ya detectadas ni dejar de permitir amenazas.



Es necesario activar *Visualizar detecciones y amenazas* para poder ejercer completamente *Excluir temporalmente amenazas (Malware, PUP, Bloqueados)*.

19.5. Acceso a la configuración de cuentas de usuarios y roles

En el menú superior **Configuración**, y haciendo clic en el panel de la izquierda **Usuarios**, aparecen dos entradas asociadas a la gestión de roles y cuentas de usuario:

- **Usuarios:** permite crear nuevas cuentas de usuario y definir su pertenencia a uno o varios roles.
- **Roles:** permite crear y modificar una nueva configuración de acceso a los recursos de **Endpoint Protection / Plus**.

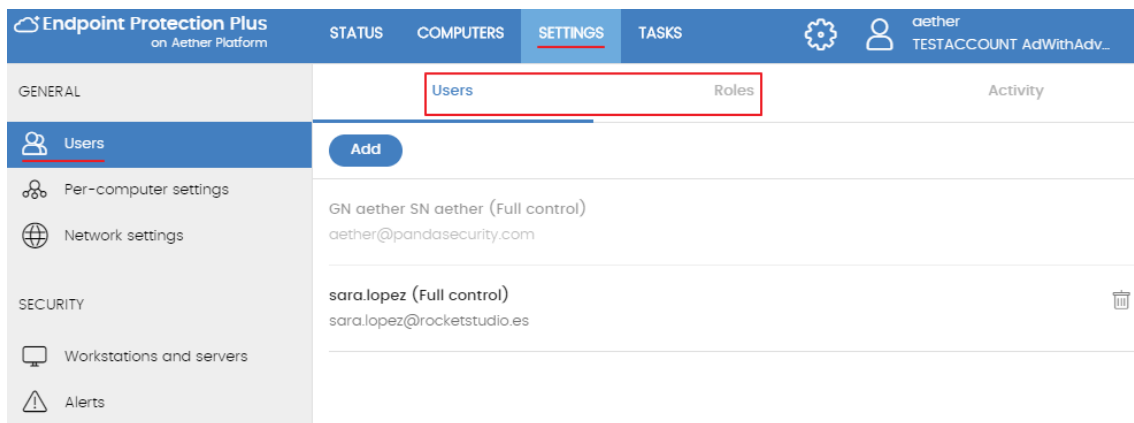



Figura 92: acceso a la configuración de usuarios y roles

Las pestañas de **Usuarios y roles** solo son accesibles si el usuario tiene el permiso **Gestionar usuarios y roles**.

19.6. Creación y configuración de cuentas de usuario



En el menú superior **Configuración**, haciendo clic en el panel de la izquierda **Usuarios** y después en la pestaña **Usuarios**, podrás realizar todas las acciones necesarias relativas a la creación y modificación de cuentas de usuario.

- **Añadir nueva cuenta de usuario:** haz clic en el botón **Añadir** para añadir un nuevo usuario, establecer la cuenta de correo para el acceso, el rol al que pertenecerá y una descripción de la cuenta. El sistema enviará un correo a la cuenta para generar la contraseña de acceso.

- **Editar una cuenta de usuario:** haz clic en el nombre del usuario para mostrar una ventana con todos los datos de la cuenta editables.
- **Borrar o desactivar cuentas de usuarios:** haz clic sobre el icono  de una cuenta de usuario para borrarla. Haz clic en una cuenta de usuario y selecciona el interruptor **Bloquear este usuario para** inhabilitada temporalmente el acceso de la cuenta a la consola web. De esta manera, esa cuenta verá denegado el acceso a la consola de administración, y si ya estuviera logeado será expulsado de forma inmediata.

19.7. Creación y configuración de roles

En el menú superior **Configuración**, haciendo clic en el panel de la izquierda **Usuarios** y después en la pestaña **Roles**, podrás realizar todas las acciones necesarias relativas a la creación y modificación de roles.

- **Añadir nuevo rol:** haz clic en el botón **Añadir**. Se pedirá el nombre del rol, una descripción opcional, una selección sobre los equipos accesibles y una configuración concreta de los permisos.
- **Editar un rol:** haz clic en el nombre del rol para mostrará una ventana con todas sus configuraciones editables.
- **Copiar un rol:** haz clic en el icono  para mostrar una ventana con un nuevo rol configurado de la misma forma que el original.
- **Borrar rol:** haz clic sobre el icono  de un rol para borrarlo. Si al borrar un rol éste ya tiene cuentas de usuario asignadas, se cancelará el proceso de borrado.

19.8. Registro de la actividad de las cuentas de usuario

Endpoint Protection / Plus registra todas las acciones efectuadas por los administradores de red en la consola web de gestión. De esta forma es fácil determinar quién realizó un cambio, en que momento y sobre qué objeto.

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

19.8.1 Registro de acciones

La sección de acciones permite listar todas las acciones ejecutadas por las cuentas de usuario, exportar las acciones a formato csv y filtrar la información.

Campos mostrados en el listado de acciones

Campo	Comentario	Valores
Fecha	Fecha y hora en la que se produjo la acción	Fecha
Usuario	Cuenta de usuario que ejecuto la acción	Cadena de caracteres
Acción	Tipo de operación que se realizó	Acceder Añadir envío Asignar licencia Bloquear Borrar Cambiar 'Ajustes por equipo' Cambiar 'Configuración de Seguridad' Cambiar Grupo Cambiar Grupo-Padre Cambiar 'Proxy e idioma' Cancelar Configurar descubrimiento Crear Desasignar licencia Dejar de permitir Desbloquear Descubrir ahora Designar equipo caché Designar equipo descubridor Designar Proxy Panda Editar Editar descripción Editar envío Editar nombre Eliminar Eliminar envío Heredar 'Ajustes por equipo' Heredar 'Configuración de Seguridad' Heredar 'Proxy e idioma' Instalar Localizar Mover a su ruta de Active Directory Mover equipos a su ruta de Active Directory Ocultar Permitir Publicar Reiniciar Restaurar comunicaciones Revocar equipo caché Revocar equipo descubridor Revocar Proxy Panda Sincronizar grupo Visibilizar
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción	Amenaza Configuración Dispositivo Android Equipo Equipo no administrado Filtro

		Grupo Grupo de dispositivos Informe ejecutivo Informes avanzados Listado Preferencia para envío emails Rol Tarea - Análisis de seguridad Usuario
Elemento	Objeto de la consola sobre el cual se ejecutó la acción	Cadena de caracteres

Tabla 39: campos del Registro de acciones

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Fecha	Fecha y hora en la que se produjo la acción	Fecha
Usuario	Cuenta de usuario que ejecuto la acción	Cadena de caracteres
Acciones		Acceder Añadir envío Asignar licencia Bloquear Borrar Cambiar 'Ajustes por equipo' Cambiar 'Configuración de Seguridad' Cambiar Grupo Cambiar Grupo-Padre Cambiar 'Proxy e idioma' Cancelar Configurar descubrimiento Crear Desasignar licencia Dejar de permitir Desbloquear Descubrir ahora Designar equipo caché Designar equipo descubridor Designar Proxy Panda Editar Editar descripción Editar envío Editar nombre Eliminar Eliminar envío Heredar 'Ajustes por equipo' Heredar 'Configuración de Seguridad' Heredar 'Proxy e idioma' Instalar Localizar Mover a su ruta de Active Directory Mover equipos a su ruta de Active Directory Ocultar

Campo	Comentario	Valores
		Permitir Publicar Reiniciar Restaurar comunicaciones Revocar equipo caché Revocar equipo descubridor Revocar Proxy Panda Sincronizar grupo Visibilizar
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción	Amenaza Configuración Dispositivo Android Equipo Equipo no administrado Filtro Grupo Grupo de dispositivos Informe ejecutivo Informes avanzados Listado Preferencia para envío emails Rol Tarea - Análisis de seguridad Usuario
Elemento	Objeto de la consola sobre el cual se ejecutó la acción	Cadena de caracteres

Tabla 40: campos del fichero exportado Registro de acciones

Herramienta de búsqueda

Campo	Comentario	Valores
Desde		Fecha
Hasta		Fecha
Usuarios		Listado de cuentas de usuario creados en la consola de administración

Tabla 41: campos de filtrado para el Registro de acciones

19.8.2 Registro de sesiones

La sección de sesiones permite listar todos los accesos a la consola de administración, exportarlos a formato csv y filtrar la información.

Campos mostrados en el listado de sesiones

Campo	Comentario	Valores
Fecha	Fecha y hora en la que se produjo el acceso	Fecha
Usuario	Cuenta de usuario que accedió	Cadena de caracteres
Actividad		Iniciar sesión Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso	Cadena de caracteres

Tabla 42: campos del listado sesiones

Campos mostrados en el fichero exportado

Campo	Comentario	Valores
Fecha	Fecha y hora en la que se produjo el acceso	Fecha
Usuario	Cuenta de usuario que accedió	Cadena de caracteres
Actividad		Iniciar sesión Cerrar sesión
Dirección IP	Dirección IP desde donde se produce el acceso	Cadena de caracteres

Tabla 43: campos del fichero exportado sesiones

Herramienta de búsqueda

Campo	Comentario	Valores
Desde		Fecha
Hasta		Fecha
Usuarios		Listado de cuentas de usuario creados en la consola de administración

Tabla 44: campos de filtrado para el listado de sesiones

20. Apéndice I: Requisitos de Endpoint Protection / Plus

Plataformas Windows
Plataformas Windows Exchange
Plataformas MacOS
Plataformas Linux
Plataformas Android
Acceso a la consola web
Acceso a URLs del servicio

20.1. Requisitos de plataformas Windows

20.1.1 Sistemas operativos soportados

Estaciones de trabajo

- Windows XP SP3 (32 bits)
- Windows Vista
- Windows 7
- Windows 8 (32 y 64-bit)
- Windows 8.1 (32 y 64-bit)
- Windows 10 (32 y 64-bit).

Servidores

- Windows 2003 (32, 64-bit y R2) SP2 y superiores
- Windows 2008 (32 y 64-bit) y 2008 R2
- Windows Small Business Server 2011, 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server Core 2008, 2008 R2, 2012 R2 y 2016

20.1.2 Requisitos hardware

- **Procesador:** Pentium 1 Ghz
- **Memoria RAM:** 1 Gbyte
- **Espacio libre en el disco duro para la instalación:** 650 Mbytes

20.2. Requisitos de plataformas Windows Exchange

20.2.1 Sistemas operativos soportados

- Exchange 2003: Windows Server 2003 32 bits SP2+ y Windows Server 2003 R2 32 bits
- Exchange 2007: Windows Server 2003 64 bits SP2+, Windows Server 2003 R2 64 bits, Windows 2008 64 bits y Windows 2008 R2
- Exchange 2010: Windows 2008 64 bits y Windows 2008 R2
- Exchange 2013: Windows Server 2012 y Windows Server 2012 R2
- Exchange 2016: Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016.

20.2.2 Requisitos hardware y software

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

- Exchange 2016

[https://technet.microsoft.com/es-es/library/aa996719\(v=exchg.160\).aspx](https://technet.microsoft.com/es-es/library/aa996719(v=exchg.160).aspx)

20.2.3 Versiones Exchange soportadas

- Microsoft Exchange Server 2003 Standard y Enterprise (SP1 / SP2)
- Microsoft Exchange Server 2007 Standard y Enterprise (SP0 / SP1 / SP2 / SP3)
- Microsoft Exchange Server 2007 incluido en Windows SBS 2008
- Microsoft Exchange Server 2010 Standard y Enterprise (SP0 / SP1 / SP2)
- Microsoft Exchange Server 2010 incluido en Windows SBS 2011
- Microsoft Exchange Server 2013 Standard y Enterprise
- Microsoft Exchange Server 2016 Standard y Enterprise

20.3. Requisitos de plataformas MacOS

20.3.1 Sistemas operativos soportados

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- MacOS 10.13 High Sierra

20.3.2 Requisitos hardware

- **Procesador:** Intel Core 2 Duo.
- **Memoria RAM:** 2 Gbyte.

- **Espacio libre en el disco duro para la instalación:** 400 Mbytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 sin usar en el equipo para el funcionamiento del filtrado web y la detección web de malware.

20.4. Requisitos de plataformas Linux

20.4.1 Distribuciones de 64 bits soportadas

- Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS y 16.10
- Fedora 23, 24 y 25

20.4.2 Versión de kernel soportada

Desde la 3.13 hasta la 4.10

20.4.3 Gestores de ficheros soportados

- Nautilus
- Pcmmanfm
- dolphin

20.4.4 Requisitos hardware

- **Procesador:** Pentium 1 Ghz.
- **Memoria RAM:** 1.5 Gbytes.
- **Espacio libre en el disco duro para la instalación:** 100 Mbytes.
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 sin usar en el equipo para el funcionamiento del filtrado web y la detección web de malware.

20.4.5 Dependencias del paquete de instalación

debconf (>= 0.5) debconf-2.0	libfreetype6 (>= 2.3.5)	libpng12-0 (1.2.13-4)	(>= libxcb1
dkms (>= 1.95)	libgcc1 (>= 1:4.1.1)	libsm6, libssl1.0.0 (1.0.0)	(>= libxrender1
libc6 (>= 2.17)	libgl1-mesa-glx libgl1	libstdc++6 (>= 4.6)	make
libc6-dev	libice6 (>= 1:1.0.0)	libstdc++6:i386	notify-osd
libcurl3:i386	libltdl7 (>= 2.4.2)	libuuid1 (>= 2.16)	notification-daemon
libcups2	libnl-3-200 (>= 3.2.7)	libuuid1:i386	python-nautilus (>= 1.1-4)
libdbus-1-3 (>= 1.1.1)	libnl-genl-3-200 (3.2.7)	(>= libx11-6	zlib1g (>= 1:1.1.4)
libfontconfig1 (>= 2.9.0)	libnotify-bin (>= 0.7.6)	libx11-xcb1	

Tabla 45: librerías requeridas para la instalación

20.5. Requisitos de plataformas Android

20.5.1 Sistemas operativos soportados

- Ice Cream Sandwich 4.0
- Jelly Bean 4.1 - 4.2 - 4.3
- KitKat 4.4
- Lollipop 5.0/5.1
- Marshmallow 6.0
- Nougat 7.0 - 7.1
- Oreo 8.0

20.5.2 Requisitos hardware

Se requiere un mínimo de 10 megabytes de espacio en la memoria interna del dispositivo. Dependiendo del modelo es posible que el espacio requerido sea superior.

20.5.3 Requisitos de red

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

20.6. Acceso a la consola web

La consola de administración es accesible con la última versión de los navegadores compatibles mostrados a continuación:

- Chrome
- Internet Explorer
- Microsoft Edge
- Firefox
- Opera

20.7. Acceso a URLs del servicio

Para el correcto funcionamiento de **Endpoint Protection / Plus** es necesario que las URL mostradas a continuación sean accesibles desde los equipos protegidos de la red

- https://*.pandasecurity.com
- http://*.pandasecurity.com
- https://*.windows.net

- <https://pandasecurity.logtrust.com>
- http://*.pandasoftware.com

Tráfico de entrada y salida (Antispam y filtrado URL)

- http://*.pand.ctmail.com
- <http://download.ctmail.com>

Puertos

- Port 80 (HTTP, websocket)
- Port 443 (HTTPS)

21. Apéndice II: Creación y gestión de cuentas Panda

Creación de una cuenta Panda
Activación de la cuenta Panda

21.1. Introducción

La Cuenta Panda ofrece al administrador un mecanismo de creación y acceso seguro a los servicios contratados con Panda Security, frente al método estándar de recepción de credenciales por correo electrónico.

Con una Cuenta panda es el propio administrador quien crea y activa el método de acceso a la consola Web de **Endpoint Protection / Plus**.

21.2. Creación de una Cuenta Panda

Para crear una nueva Cuenta Panda es necesario seguir el procedimiento descrito a continuación.

Recepción del mensaje de correo

- Al adquirir **Endpoint Protection / Plus** recibirás un mensaje de correo electrónico procedente de Panda Security.
- Haz clic en el vínculo que contiene el mensaje para acceder a la Web desde la que podrás crear la Cuenta Panda.

Rellena el formulario

- Rellena con tus datos el formulario mostrado.
- Utiliza el desplegable situado en la esquina inferior derecha si deseas que la página se muestre en otro idioma.
- Accede al acuerdo de licencia y la política de privacidad haciendo clic en el vínculo correspondiente.
- Haz clic en **Crear** cuando hayas terminado para recibir un mensaje de correo electrónico en la dirección especificada en el formulario. Utilizando ese mensaje podrás activar la cuenta.

21.3. Activación de la 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 utilizada para crear la Cuenta Panda.

- Ve a la bandeja de entrada y localiza el mensaje.
- 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.
- La primera vez que se acceda a la Cuenta Panda se solicitará una confirmación de contraseña. Después, haz clic en el botón **Activar cuenta**.

- Introduce los datos necesarios y haz clic en **Guardar datos**. Si prefieres facilitar los datos en otra ocasión, utiliza la opción **Ahora no**.
- Acepta el acuerdo de licencias y haz clic en **Aceptar**.

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

22. Apéndice III: Listado de des instaladores

Al lanzar la instalación del producto **Endpoint Protection / Plus** es posible que se detecten otros productos de seguridad instalados en el equipo. En este caso, antes de instalar la protección, **Endpoint Protection / Plus** desinstalará automáticamente los productos que aparecen en la Tabla 45:

Fabricante	Nombre del producto
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)
Bitdefender	BitDefender Endpoint Protection 6.x 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)

Fabricante	Nombre del producto
	ESET NOD32 Antivirus 7 (32 bits) ESET NOD32 Antivirus 7 (64 bits)
eScan	eScan Anti-Virus (AV) Edition for Windows 14.x eScan Internet Security for SMB 14.x eScan Corporate for Windows 14.x
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
iSheriff	iSheriff Endpoint Security 5.x
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 LiveSafe 2016 x86 / x64 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*

Fabricante	Nombre del producto
MicroWorld Technologies	eScan Corporate for Windows 9.0.824.205
PC Tools	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 22.x Symantec.cloud - Endpoint Protection.cloud 21.x (32bits) Symantec.cloud - Endpoint Protection.cloud 21.x (64bits) Symantec EndPoint Protection 14.x (32bits) Symantec EndPoint Protection 14.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 Trend Micro OfficeScan 11.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 2017* Panda Internet Security 2017*

Fabricante	Nombre del producto
	Panda Antivirus Pro 2017* Panda Gold Protection 2017*
	Panda Global Protection 2016* Panda Internet Security 2016* Panda Antivirus Pro 2016* Panda Gold Protection 2016*
	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

Tabla 46: listado de desinstaladores

*Productos Panda 2017, 2016, 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 Endpoint Protection en Windows 7 y Windows Vista, el usuario debe intervenir seleccionando la opción Permitir.

* AVG Internet Security Business Edition 2011 32 bits - Durante el proceso de instalación del agente de Endpoint Protection, el usuario debe intervenir seleccionando en varias ventanas la opción Permitir.

** AVG Internet Security Business Edition 2011 64 bits (10.0.1375) - Durante el proceso de instalación del agente de Endpoint Protection, 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 Endpoint Protection 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 Endpoint Protection, 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 Endpoint Protection el equipo se reiniciará automáticamente sin mostrar ningún aviso, ni pedir confirmación al usuario.

* ESET NOD32 Antivirus 2.70.39 tras la instalación de agente de Endpoint Protection el equipo se reiniciará automáticamente 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.

23. Apéndice IV: Conceptos Clave

Adaptador de red

Hardware que permite la comunicación entre diferentes equipos conectados a través de una red de datos. Un equipo puede tener más de un adaptador de red instalado y es identificado en el sistema mediante un número de identificación único.

Adware

Programa que, una vez instalado o mientras se está instalando, ejecuta, muestra o descarga automáticamente publicidad en el equipo.

Agente Panda

Uno de los dos módulos del software Endpoint Protection / Plus, se encarga de las comunicaciones entre los equipos de la red y los servidores en la nube de Panda Security, además de la gestión de los procesos locales.

Alerta

Ver Incidencia.

Análisis heurístico

Análisis estático formado por un conjunto de técnicas que inspeccionan el programa sospechoso en base a cientos de características del archivo para determinar la probabilidad de que pueda llevar a cabo acciones maliciosas o dañinas cuando se ejecute en el equipo del usuario.

Anti-tamper

Conjunto de tecnologías que evitan la manipulación de los procesos de **Endpoint Protection / Plus** por parte de amenazas avanzadas y APT que buscan sortear las capacidades de protección de la herramienta de seguridad instalada.

Anti Spam

Tecnología que busca correos no deseados en función de su contenido.

Antivirus

Módulo de protección basado en tecnologías tradicionales (fichero de firmas, análisis heurístico, anti exploit etc), que detecta y elimina virus informáticos y otras amenazas.

Árbol de carpetas

Estructura jerárquica formada por agrupaciones estáticas, utilizada para organizar el parque de equipos y facilitar la asignación de configuraciones.

Árbol de filtros

Colección de filtros agrupados en carpetas que facilitan la organización del parque de equipos y la asignación de configuraciones.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

ARP (Address Resolution Protocol)

Protocolo utilizado para resolver direcciones del nivel de red a direcciones del nivel de enlace. En redes IP traduce las direcciones IP a direcciones físicas MAC.

Asignación automática de configuraciones

Ver Herencia.

Asignación indirecta de configuraciones

Ver Herencia.

Asignación manual de configuraciones

Asignación de una configuración a un grupo de forma directa, en contraposición al establecimiento de configuraciones automático o indirecto, que utiliza el recurso de la herencia para fijar configuraciones sin intervención del administrador.

Backup

Área de almacenamiento de ficheros maliciosos no desinfectables, así como de spyware y herramientas de hacking detectadas. Todos los programas eliminados del sistema por ser clasificados como amenazas se copian de forma temporal en el área de backup / cuarentena durante un periodo de entre 7 y 30 días según el tipo.

Broadcast

Transmisión de paquetes en redes de datos a todos los nodos de la subred: un paquete de datos llegará a todos los equipos dentro de la misma subred sin necesidad de enviarlo de forma individual a cada nodo. Los paquetes de broadcast no atraviesan encaminadores y utilizan un direccionamiento distinto para diferenciarlos de los paquetes unicast.

Cache / Repositorio (rol)

Equipos que descargan y almacenan de forma automática todos los ficheros necesarios para que otros equipos con **Endpoint Protection / Plus** instalado puedan actualizar el archivo de identificadores, el agente y el motor de protección sin necesidad de acceder a Internet. De esta manera se produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada

Configuración

Ver Perfil de configuración.

Control de dispositivos

Módulo que permite definir el comportamiento del equipo protegido al conectar dispositivos extraíbles o de almacenamiento masivo, para minimizar la superficie de exposición del equipo.

Control de acceso a páginas web

Tecnología que permite controlar y filtrar las URLs solicitadas por los navegadores de la red con el propósito de denegar o permitir su acceso, tomando como referencia una base de datos de URLs dividida en categorías o temas.

Consola Web

Herramienta de gestión del servicio de seguridad avanzada **Endpoint Protection / Plus**, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador podrá desplegar el software de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección.

Cuarentena

Ver Backup.

Cuenta de usuario

Ver Usuario.

Descubridor (rol)

Equipos capaces descubrir puestos de usuario y servidores no administrados para iniciar una instalación remota del agente **Endpoint Protection / Plus**.

Desinfectable

Fichero infectado por malware del cual se conoce el algoritmo necesario para poder revertirlo a su estado original.

DHCP

Servicio que asigna direcciones IP a los nuevos equipos conectados a la red.

Dialer

Programa que marca un número de tarificación adicional (NTA), utilizando para ello el módem. Los NTA son números cuyo coste es superior al de una llamada nacional.

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

Dirección MAC

Identificador hexadecimal de 48 bits que corresponde de forma única a una tarjeta o interfaz de red.

Directorio Activo

Implementación propietaria de servicios LDAP (Lightweight Directory Access Protocol, Protocolo Ligero/Simplificado de Acceso a Directorios) para máquinas Microsoft Windows. Permite el acceso a un servicio de directorio para buscar información diversa en entornos de red.

Distribución Linux

Conjunto de paquetes de software y bibliotecas que conforman un sistema operativo basado en el núcleo Linux.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

Dominio

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios está centralizada en un servidor llamado Controlador Principal de Dominio (PDC) o Directorio Activo (AD).

Equipos sin licencia

Equipos cuya licencia ha caducado o no ha sido posible asignar una licencia válida por haberse superado el número máximo permitido de instalaciones de la protección. Estos equipos no están protegidos, pero son visibles en la consola web de administración.

Excluido (programa)

Son programas inicialmente eliminados por haber sido clasificados como malware o PUP, pero que el administrador de la red permite su ejecución de forma selectiva y temporal excluyéndolos del análisis.

Exploit

De forma general un exploit es una secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de provocar el fallo, el proceso comprometido interpretará por error parte de la secuencia de datos como código ejecutable, desencadenando acciones peligrosas para la seguridad del equipo.

Firewall

También conocido como cortafuegos. Tecnología que bloquea el tráfico de red que coincide con patrones definidos por el administrador mediante reglas. De esta manera se limita o impide la comunicación de ciertas aplicaciones que se ejecutan en los equipos, restringiéndose la superficie de exposición del equipo.

Filtro

Contenedor de equipos de tipo dinámico que agrupa de forma automática aquellos elementos que cumplen con todas las condiciones definidas por el administrador. Los filtros simplifican la asignación de configuraciones de seguridad y facilitan la administración de los equipos del parque informático.

Fragmentación

En redes de transmisión de datos, cuando la MTU del protocolo subyacente es menor que el tamaño del paquete a transmitir, los encaminadores dividen el paquete en piezas más pequeñas (fragmentos) que se encaminan de forma independiente y se ensamblan en el destino en el orden apropiado.

Funcionalidad Peer To Peer (P2P)

Modo de transferencia de información utilizando el ancho de banda de la red de forma más eficiente entre nodos que adoptan el rol de cliente y servidor de forma simultánea, estableciendo comunicaciones bidireccionales directas.

En **Endpoint Protection / Plus** los equipos con el archivo de identificadores ya actualizado aplican funcionalidades Peer To Peer para reducir el consumo de ancho de la conexión a Internet, compartiéndolo a nivel local con otros equipos que también necesitan actualizarlo.

Funcionalidad Proxy

Esta funcionalidad permite el funcionamiento de **Endpoint Protection / Plus** en equipos sin acceso a Internet, ejecutando los accesos a través de otro agente instalado en una máquina de su misma subred.

Geolocalizar

Posicionar en un mapa un dispositivo en función de sus coordenadas.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grupo

Contenedor de tipo estático que agrupa a uno o más equipos de la red. La pertenencia de un equipo a un grupo se establece de forma manual. Los grupos se utilizan para simplificar la asignación de configuraciones de seguridad y para facilitar la administración de los equipos del parque informático.

Grupo de trabajo

Arquitectura de redes Windows donde la gestión de los recursos compartidos, permisos y usuarios residen en cada uno de los equipos de forma independiente.

Herencia

Método de asignación automática de configuraciones sobre todos los grupos descendientes de un grupo padre, ahorrando tiempo de gestión. También llamado Asignación automática de configuraciones o Asignación indirecta de configuraciones.

Herramienta de hacking

Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

ICMP (Internet Control Message Protocol)

Protocolo de control y notificación de errores utilizado por el protocolo IP en Internet.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

IP feeds

Servicio de entrega de bloques de direcciones IP utilizadas por las redes de bots descubiertas y analizadas por Panda Security.

Joke

Broma con el objetivo de hacer pensar a los usuarios que han sido afectados por un virus.

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

Malware freezer

Comportamiento del backup / cuarentena cuyo objetivo es evitar la pérdida de datos por falsos positivos. Todos los ficheros clasificados como malware o sospechosos son enviados a la zona de backup / cuarentena, evitando su borrado completo en previsión de un fallo en la clasificación que derive en pérdida de datos.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

MTU (Maximum transmission unit)

Tamaño máximo del paquete que el protocolo subyacente puede transportar.

Nube (Cloud Computing)

Tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.

OU (Organizational Unit)

Forma jerárquica de clasificar y agrupar objetos almacenados en directorios.

Partner

Empresa que ofrece productos y servicios de Panda Security.

PDC (Primary Domain Controller)

Es un rol adoptado por servidores en redes Microsoft de tipo Dominio, que gestiona de forma centralizada la asignación y validación de las credenciales de los usuarios para el acceso a los recursos de red. En la actualidad el Directorio Activo cumple esta función.

Perfil de configuración

Un perfil es una configuración específica de la protección o de otro aspecto del equipo administrado. Este perfil es posteriormente asignado a un grupo o grupos y aplicado a todos los equipos que lo forman.

Phishing

Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.

Programas potencialmente no deseados (PUP)

Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.

Protección (módulo)

Una de las dos partes que componen el software Endpoint Protection / Plus que se instala en los equipos. Contiene las tecnologías encargadas de proteger el parque informático y las herramientas de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Protocolo

Conjunto de normas y especificaciones utilizadas para el intercambio de datos entre ordenadores. Uno de los más habituales es el protocolo TCP- IP.

Proxy

Software que hace de intermediario de las comunicaciones establecidas entre dos equipos, un cliente situado en una red interna (por ejemplo, una intranet) y un servidor en una extranet o en internet.

Proxy (rol)

Equipo que hace la función de pasarela, conectando a otros puestos de usuario y servidores sin salida directa a internet con la nube de **Endpoint Protection / Plus**.

Puerto

Identificador numérico asignado a un canal de datos abierto por un proceso en un dispositivo a través del cual tienen lugar las transferencias de información (entradas / salidas) con el exterior.

QR (Quick Response), código

Representación gráfica en forma de matriz de puntos que almacena de forma compacta información.

Red pública

Redes desplegadas en locales abiertos al público como cafeterías, aeropuertos, etc. Debido a su naturaleza pública se recomienda establecer límites en el nivel de visibilidad de los equipos que se conectan a este tipo de redes ellas, y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.

Red de confianza

Redes desplegadas en locales privados, tales como oficinas y domicilios. Los equipos conectados son generalmente visibles por sus vecinos y no es necesario establecer limitaciones al compartir archivos, recursos y directorios.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para visualizarlas.

RIR (Regional Internet Registry)

Organización que supervisa la asignación y el registro de direcciones IP y de sistemas autónomos (AS, Autonomous System) dentro de una región particular del mundo.

Rol

Configuración específica de permisos que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

Rootkits

Programa diseñado para ocultar objetos como procesos, archivos o entradas del Registro de Windows (incluyendo los suyos propios). Este tipo de software es utilizado esconder evidencias y utilidades en sistemas previamente comprometidos.

Samples feed

Servicio de entrega de malware normalizado y automatizaciones mediante una API REST para empresas con laboratorio propio de estudio de malware.

SCL (Spam Confidence Level)

Valor normalizado asignado a un mensaje que refleja la probabilidad de que sea Spam, evaluando características tales como su contenido, cabeceras y otros.

Servidor Exchange

Servidor de correo desarrollado por 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.

Servidor SMTP

Servidor que utiliza el protocolo SMTP -o protocolo simple de transferencia de correo- para el intercambio de mensajes de correo electrónicos entre los equipos.

Software Endpoint Protection / Plus

Programa que se instala en los equipos a proteger. Se compone de dos módulos: el agente Panda y la protección.

Sospechoso

Programa que, tras un análisis de su comportamiento realizado en el equipo del usuario por la protección de **Endpoint Protection / Plus**, tiene una alta probabilidad de ser considerado malware.

Spam

El término correo basura hace referencia a mensajes no solicitados, habitualmente de tipo publicitario y generalmente enviados en grandes cantidades, que perjudican de alguna manera al receptor.

SSL (Secure Sockets Layer)

Protocolo criptográfico diseñado para la transmisión segura de datos por red.

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.

SYN

Bandera (flag) en el campo TOS (Type Of Service) de los paquetes TCP que los identifican como paquetes de inicio de conexión.

Tarea

Conjunto de acciones programadas para ejecutarse con una frecuencia y en un intervalo de tiempo configurables.

TCO (Total Cost of Ownership, Coste total de Propiedad)

Estimación financiera que mide los costes directos e indirectos de un producto o sistema.

Tiempo de exposición (dwell time)

Tiempo que una amenaza ha permanecido sin ser detectada en un equipo de la red.

TLS (Transport Layer Security)

Nueva versión del protocolo SSL 3.0.

Topología de red

Mapa físico o lógico de los nodos que conforman una red para comunicarse.

Trojanos

Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario.

TCP (Transmission Control Protocol)

Principal protocolo del nivel de transporte dentro de la pila de protocolos de Internet, orientado a la conexión para el envío y recepción de paquetes IP.

UDP (User Datagram Protocol)

Protocolo del nivel de transporte dentro de la pila de protocolos de Internet, no confiable y no orientado a la conexión para el envío y recepción de paquetes IP.

Usuario (consola)

Recurso formado por un conjunto de información que Endpoint Protection / Plus utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red

Usuario (red)

Trabajadores de la empresa que utilizan equipos informáticos para desarrollar su trabajo.

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.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Virus

Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

Widget (Panel)

Panel que contiene un gráfico configurable y que representa un aspecto concreto de la seguridad de la red del cliente. El conjunto de widgets forma el Dashboard o panel de control de **Endpoint Protection / Plus**



Endpoint Protection



Endpoint Protection Plus

Ni los documentos ni los programas a los que usted pueda acceder pueden ser copiados, reproducidos, traducidos o transferidos por cualquier medio electrónico o legible sin el permiso previo y por escrito de Panda Security, Santiago de Compostela, 12, 48003 Bilbao (Bizkaia), ESPAÑA.

Marcas registradas. Windows Vista y el logotipo de Windows son marcas o marcas registradas de Microsoft Corporation en los Estados Unidos y otros países. Todos los demás nombres de productos pueden ser marcas registradas de sus respectivas compañías.

© Panda Security 2017. Todos los derechos reservados.