



© Panda Adaptive Defense 360

Guía de administración

Versión: 3.72.00-00

Autor: Panda Security

Fecha: 28/12/2020

Aviso legal.

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 2021. Todos los derechos reservados

Información de contacto.

Oficinas centrales:

Panda Security

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 España.

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

Acerca de la Guía de administración de Panda Adaptive Defense 360

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

<http://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSE360oAP-guia-ES.pdf>

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

<https://www.pandasecurity.com/enterprise/downloads/docs/product/help/adaptivedefense360/latest/es/index.htm>

Información sobre las novedades de la versión

Para conocer las novedades de la última versión de Panda Adaptive Defense 360 consulta la siguiente URL:

<http://info.pandasecurity.com/aether/?product=AD360&lang=es>

Documentación técnica no incluida en esta Guía de administración para módulos y servicios compatibles con Panda Adaptive Defense 360

- Para acceder a la Guía para el usuario de Panda Advanced Reporting Tool consulta la siguiente URL:

<https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/ADVANCEDREPORTINGTOOL-AETHER-Guia-ES.pdf>

- Para acceder a la Guía para el usuario de Panda Data Control consulta la siguiente URL:

<https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-AETHER-Guia-ES.pdf>

- Para acceder a las guías de Panda SIEMFeeder consulta las siguientes URLs:

<https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-ES.PDF>

<https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-ManualDescripcionEventos-ES.pdf>

Soporte técnico

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

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

<https://www.pandasecurity.com/spain/support/adaptive-defense-360-aether.htm>

- Para acceder al portal eKnowledge Base consulta la siguiente URL:

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

Encuesta sobre la Guía de administración de Panda Adaptive Defense 360

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

<https://es.surveymonkey.com/r/feedbackAD360GuideES>

Tabla de contenidos

Parte 1: Introducción a Panda Adaptive Defense 360

Capítulo 1: Prólogo	11
¿A quién está dirigida esta Guía de administración?	11
¿Que es Panda Adaptive Defense 360?	11
Iconos	12
Capítulo 2: Información básica de Panda Adaptive Defense 360-	13
Beneficios de Panda Adaptive Defense 360.....	14
Características de Panda Adaptive Defense 360	15
Características de la plataforma Aether	15
Principales beneficios de Aether.....	16
Arquitectura de Aether	17
Aether en los equipos de usuario	18
Componentes principales	19
Servicios Panda Adaptive Defense 360	22
Perfil de usuario del producto	25
Dispositivos e idiomas soportados.....	25
Capítulo 3: El ciclo de protección adaptativa-	27
Las nuevas necesidades de seguridad.....	28
El ciclo de protección adaptativa	28
Fase I: Protección completa del parque informático	29
Protección antivirus permanente e inteligencia colectiva.....	29
Protección contra técnicas de ocultación y virus de macro.....	30
Bloqueo de programas.....	30
Protección del correo y la Web	31
Cortafuegos y sistema de detección de intrusos (IDS)	31
Control de dispositivos	31
Filtrado de Spam, Virus y contenidos en servidores Exchange	31
Control de acceso a páginas Web	32
Fase II: Detección y monitorización.....	33
Protección permanente avanzada.....	33
Protección contra exploits	34
Detección de amenazas sin fichero y servicio THIS	35
Monitorización de ficheros de datos (Panda Data Control)	36
Parcheo de vulnerabilidades (Panda Patch Management)	36
Visibilidad del estado de la red	37
Fase III: Resolución y respuesta	38
Fase IV: Adaptación / Prevención.....	38

Parte 2: La consola web de administración

Capítulo 4: La consola de administración -	43
Beneficios de la consola web	44
Requisitos de la consola web	45
Federación con IDP	45
Estructura general de la consola Web.....	46
Menú superior (1).....	46
Menú lateral (2)	49

Panel central (3)	49
Acceso a Advanced Visualization Tool (4)	49
Elementos básicos de la consola web	50
Esquema general de la zona Estado	54
Gestión de listados	56
Plantillas, configuraciones y vistas	56
Secciones de los listados	60
Listados incluidos por defecto	64
Capítulo 5: Control y supervisión de la consola de administración - - - - -	67
Concepto de cuenta de usuario	68
Estructura de una cuenta de usuario	68
Verificación en dos pasos	69
Concepto de rol	70
Estructura de un rol	70
¿Por qué son necesarios los roles?	70
El rol Control total	71
El rol Solo lectura	71
Concepto de permiso	72
Descripción de los permisos implementados	72
Acceso a la configuración de cuentas de usuarios y roles	80
Crear y configurar cuentas de usuario	80
Crear, modificar y borrar usuarios	80
Listar los usuarios creados	80
Crear y configurar roles	81
Registro de la actividad de las cuentas de usuario	82
Registro de sesiones	82
Registro de acciones de usuario	83
Eventos del sistema	100

Parte 3: Despliegue y puesta en marcha

Capítulo 6: Instalación del software cliente - - - - -	105
Visión general del despliegue de la protección	106
Requisitos de instalación	109
Requisitos por plataforma	110
Requisitos de red	111
Instalación local del software cliente	111
Descarga del paquete de instalación desde la consola Web	111
Generar la URL de descarga	114
Instalar manualmente el software cliente	114
Instalación remota del software cliente	117
Requisitos de red y sistema operativo	117
Descubrir equipos	118
Visualizar equipos descubiertos	120
Detalle de los equipos descubiertos	124
Instalación remota de equipos descubiertos	126
Instalar con herramientas centralizadas	127
Línea de comandos del paquete de instalación	127
Despliegue desde Panda Systems Management	127
Despliegue con Microsoft Active Directory	128
Instalar mediante generación de imágenes gold	129
Creación de una imagen gold para entornos VDI persistentes	130
Creación de una imagen gold para entornos VDI no persistentes	131
Proceso de instalación en equipos Windows	133
Comprobar el despliegue	134

Desinstalar el software	135
Desinstalación manual	135
Desinstalación remota	137
Reinstalación remota	138

Capítulo 7: Licencias - - - - - 141

Definiciones y conceptos clave.....	142
Mantenimientos	142
Estado de los equipos	142
Estado de las licencias y grupos.....	142
Tipos de licencias	143
Asignar licencias	143
Liberar licencias	144
Procesos asociados a la asignación de licencias	144
Caso I: Equipos con licencia asignada y equipos excluidos	144
Caso II: Equipos sin licencia asignada	145
Paneles / widgets del módulo licencias	146
Listados del módulo Licencias.....	147
Licencias caducadas.....	150
Mensajes de caducidad próxima y vencida	150
Lógica de liberación de licencias caducadas	151
Buscar equipos según su estado de licencia	151

Capítulo 8: Actualización del software cliente - - - - - 153

Módulos actualizables en el software cliente	153
Actualización del motor de protección	154
Actualizaciones	154
Actualización del agente de comunicaciones.....	156
Actualización del conocimiento.....	156
Dispositivos Windows, Linux y macOS	156
Dispositivos Android.....	156

Parte 4: Gestión de los dispositivos de la red

Capítulo 9: Gestión de equipos y dispositivos - - - - - 159

La zona equipos	161
El panel Árbol de equipos.....	161
Árbol de filtros	162
Definición de filtro.....	162
Filtros predefinidos	163
Crear y organizar filtros	164
Configurar filtros.....	165
Casos de uso comunes	167
Árbol de grupos.....	168
Definición de grupo	169
Grupos de Directorio Activo	170
Crear y organizar grupos	170
Mover equipos entre grupos	172
Filtrar resultados por grupos	174
Tareas de análisis y desinfección	174
Listados disponibles para gestionar equipos	175
El panel Listado de equipos	175
El panel Mis listados	182
Información de equipo	189
Sección general (1)	190
Sección alertas de equipo (2)	190

Sección general en dispositivos Android	196
Sección Detalles (3)	197
Sección Hardware (4)	202
Sección Software (5)	203
Sección Configuración (6)	204
Barra de acciones (7).....	205
Iconos ocultos (8).....	205
 Capítulo 10: Gestión de configuraciones - - - - -	207
Estrategias para crear la estructura de configuraciones.....	208
Visión general para asignar configuraciones a equipos	208
Introducción a las clases de configuraciones.....	209
Perfiles de configuración modulares vs monolíticos	211
Crear y gestionar configuraciones.....	213
Asignación manual y automática de configuraciones	215
Asignación directa / manual de configuraciones	215
Asignación indirecta de configuraciones: las dos reglas de la herencia	217
Límites de la herencia	218
Sobre-escritura de configuraciones	218
Movimiento de grupos y equipos	220
Excepciones a la herencia indirecta	221
Visualizar las configuraciones asignadas	221
 Capítulo 11: Configuración remota del agente - - - - -	223
Configuración de los roles del agente Panda	224
Rol de Proxy	224
Rol de Caché / repositorio	225
Rol de descubridor	227
Configuración de listas de acceso a través de proxy.....	228
Configuración de las descargas mediante equipos caché	230
Configuración de la comunicación en tiempo real	231
Configuración del idioma del agente.....	232
Configuración de la visibilidad del agente	233
Configuración de contraseña y anti-tampering.....	233
Anti-tamper	233
Protección del agente mediante contraseña	234
 Parte 5: Gestión de la seguridad	
 Capítulo 12: Configuración de la seguridad en estaciones y servidores - - - - -	237
Acceso a la configuración y permisos necesarios	238
Introducción a la configuración de la seguridad	239
Configuración General	240
Alertas en los equipos	240
Actualizaciones.....	241
Desinstalar otros productos de seguridad.....	241
Archivos y rutas excluidas del análisis	241
Protección avanzada.....	242
Comportamiento.....	242
Anti exploit	243
Privacidad	245
Uso de la red	245
Antivirus.....	246
Amenazas a detectar	246
Tipos de archivos	247
Firewall (Equipos Windows)	247

Modo de funcionamiento	247
Tipo de red	248
Reglas de programa	249
Regla de conexión	251
Bloquear intrusiones	253
Control de dispositivos (Equipos Windows)	255
Dispositivos permitidos	256
Control de acceso a páginas web	257
Configurar horarios del control de accesos a páginas Web	257
Denegar el acceso a páginas Web	257
Lista de direcciones y dominios permitidos o denegados	258
Base de datos de URLs accedidas desde los equipos	258
Antivirus para servidores Exchange	259
Configuración de la protección Antivirus según el modo de análisis	259
Software a detectar	260
Escaneo inteligente de buzones	260
Restauración de mensajes con virus y otras amenazas	260
Anti spam para servidores Exchange	261
Acción para mensajes de spam	261
Direcciones y dominios permitidos	261
Direcciones y dominios de spam	261
Filtrado de contenidos para servidores Exchange	262
Registro de detecciones	262
 Capítulo 13: Configuración de seguridad Android - - - - -	265
Configuración de Dispositivos Android	266
Actualización	266
Antivirus	266
Antirrobo	267
 Capítulo 14: Panda Data Control (Supervisión de información sensible) - - - - -	269
Introducción al funcionamiento de Panda Data Control	272
Requisitos de Panda Data Control	274
Plataformas soportadas	274
Instalación del componente Microsoft Filter Pack	274
El proceso de indexación	274
Inventario de ficheros PII	275
Monitorización continua de ficheros	276
Búsqueda de ficheros	276
Propiedades y requisitos de las búsquedas	277
Crear una búsqueda	279
Búsquedas almacenadas	281
Visualizar los resultados de una búsqueda	281
Sintaxis de las búsquedas	283
Búsqueda de ficheros duplicados	286
Borrado y restauración de ficheros	287
Borrar ficheros de los equipos de la red	287
Restaurar ficheros previamente borrados por el administrador	288
Configuración de Panda Data Control	289
Requisitos para buscar y seguir documentos Microsoft Office	290
Información personal (inventario, búsquedas y seguimiento)	290
Monitorización de archivos por reglas	291
Opciones avanzadas de indexación	292
Escritura en unidades de almacenamiento extraíbles	293
Paneles / widgets del módulo Panda Data Control	294
Listados del módulo Panda Data Control	305
Extensiones de programas soportadas	321
Empaquetadores y algoritmos de compresión soportados	323

Entidades y países soportados	323

Capítulo 15: Panda Patch Management (Actualización de programas vulnerables) - 325

Funcionalidades de Panda Patch Management	327
Flujo general de trabajo	327
Comprobar que Panda Patch Management funciona correctamente	328
Comprobar que los parches publicados están instalados	328
Aislar los equipos con vulnerabilidades conocidas sin parchear	329
Descargar e instalar los parches	329
Descargar los parches de forma manual	334
Desinstalar los parches defectuosos	336
Comprobar el resultado de las tareas de instalación / desinstalación de parches	337
Excluir parches en todos o en algunos equipos	337
Comprobar que los programas no han entrado en EoL	338
Comprobar el histórico de instalaciones de parches y actualizaciones	338
Comprobar el nivel de parcheo de los equipos con incidencias	338
Configuración del descubrimiento de parches sin aplicar	339
Configuración general	339
Frecuencia de la búsqueda	340
Críticidad de los parches	340
Paneles / widgets en Panda Patch Management	340
Listados del módulo Panda Patch Management	347

Capítulo 16: Panda Full Encryption (Cifrado de dispositivos) - - - - - 371

Introducción a los conceptos de cifrado	372
Visión general del servicio de Panda Full Encryption	375
Características generales de Panda Full Encryption	375
Requisitos mínimos de Panda Full Encryption	376
Gestión de equipos según su estado de cifrado previo	377
Proceso de cifrado y descifrado	377
Comportamiento de Panda Full Encryption ante errores	382
Obtención de la clave de recuperación	382
Paneles / widgets del módulo Panda Full Encryption	383
Listados en Panda Full Encryption	389
Configuración del cifrado	393
Opciones de configuración de Panda Full Encryption	394
Filtros disponibles	395

Capítulo 17: Configuración del bloqueo de programas- - - - - 397

Configuración de Bloqueo de programas	398
Opciones de configuración de Bloqueo de programas	398
Listados del módulo Bloqueo de programas	399
Paneles / widgets del módulo Bloqueo de programas	400

Capítulo 18: Configuración de software autorizado- - - - - 403

Software autorizado y exclusiones de elementos	404
Configuración de Software autorizado	404
Opciones de configuración del módulo Software autorizado	405

Parte 6: Visibilidad y gestión de las amenazas

Capítulo 19: Visibilidad del malware y del parque informático - - - - - 411

Paneles / Widgets del módulo de seguridad	412
Listados del módulo de seguridad	428

Capítulo 20: Gestión de amenazas, elementos en clasificación y cuarentena- - - - 455

Introducción a las herramientas de gestión de amenazas.....	456
Permitir y volver a impedir la ejecución de elementos.....	460
Información de amenazas bloqueadas.....	463
Información de elementos bloqueados en clasificación.....	464
Listado de amenazas y programas desconocidos permitidos.....	471
Política de reclasificación.....	476
Cambiar la política de reclasificación.....	476
Trazabilidad de las reclasificaciones.....	477
Estrategias para supervisar la clasificación de ficheros.....	478
Gestión de la zona de backup / cuarentena.....	479

Capítulo 21: Análisis forense- - - - - 481

Detalle de los programas bloqueados.....	482
Detección del malware.....	482
Detección exploit.....	485
Detalle del programa bloqueado.....	487
Tablas de acciones.....	487
Grafos de ejecución.....	492
Ficheros exportados Excel.....	496
Interpretación de las tablas de acciones y grafos.....	499

Capítulo 22: Alertas - - - - - 505

Alertas por correo.....	505

Capítulo 23: Envío programado de informes y listados - - - - - 513

Características de los informes.....	514
Tipos de informes.....	514
Requisitos para generar informes.....	515
Acceso al envío de informes y listados.....	516
Gestión de informes.....	517
Información requerida para el envío de informes y listados.....	518
Contenido de los informes y listados.....	519

Parte 7: Resolución de incidencias de seguridad**Capítulo 24: Herramientas de resolución - - - - - 525**

Análisis y desinfección automática de equipos.....	526
Análisis y desinfección bajo demanda de equipos.....	527
Crear tareas desde el Árbol de equipos.....	527
Crear tareas desde el listado de equipos.....	528
Opciones de análisis.....	530
Listados generados por tareas de análisis.....	531
Listado Ver detecciones.....	533
Reiniciar equipos.....	533
Aislar un equipo.....	534
Estados de los equipos aislados.....	535
Aislar uno o varios equipos de la red de la organización.....	535
Quitar el aislamiento de un equipo.....	536
Opciones avanzadas.....	536
Comunicaciones permitidas y denegadas de un equipo aislado.....	536
Notificar un problema.....	537
Permitir el acceso externo a la consola Web.....	538

Capítulo 25: Tareas - - - - - 539

Introducción al sistema de tareas.....	539
Crear tareas desde la zona Tareas	540
Publicar tareas.....	542
Listado de tareas.....	543
Gestionar tareas	544
Resultados de una tarea	545
Ajuste automático de los destinatarios de una tarea	547

Parte 8: Información complementaria sobre Panda Adaptive Defense 360

Capítulo 26: Requisitos de hardware, software y red- - - - -	551
Funcionalidades por plataforma	552
Requisitos de plataformas Windows	554
Sistemas operativos soportados.....	554
Requisitos hardware	555
Otros requisitos	555
Requisitos de plataformas Windows Exchange.....	555
Requisitos de plataformas macOS.....	557
Requisitos de plataformas Linux	557
Requisitos de plataformas Android	559
Acceso a la consola web	559
Acceso a URLs del servicio	560

Capítulo 27: La cuenta Panda- - - - -	563
Crear una cuenta Panda para usuarios de Panda Security	563
Activar la Cuenta Panda	564
Crear y vincular una cuenta Panda con WatchGuard	565

Capítulo 28: Conceptos clave- - - - -	569



Parte 1

Introducción a Panda Adaptive Defense 360

Capítulo 1: Prólogo

Capítulo 2: Información básica de Panda Adaptive Defense 360

Capítulo 3: El ciclo de protección adaptativa

Capítulo 1

Prólogo

La Guía de administración contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto Panda Adaptive Defense 360.

CONTENIDO DEL CAPÍTULO

¿A quién está dirigida esta Guía de administración? - - - - -	11
¿Que es Panda Adaptive Defense 360? - - - - -	11
Panda Adaptive Defense 360	12
Plataforma Aether	12
Iconos - - - - -	12

¿A quién está dirigida esta Guía de administración?

Esta documentación está dirigida a los administradores de red que gestionan la seguridad informática de su organización.

Para interpretar correctamente la información ofrecida por el producto y extraer conclusiones que ayuden a fortalecer la seguridad de su empresa son necesarios conocimientos técnicos sobre entornos Windows a nivel de procesos, sistema de ficheros y registro, así como entender los protocolos de red utilizados con mayor frecuencia.

¿Que es Panda Adaptive Defense 360?

Panda Adaptive Defense 360 es un servicio gestionado que protege los equipos informáticos de las empresas, acota el alcance de los problemas de seguridad encontrados y ayuda a establecer planes de respuesta y prevención frente a las amenazas desconocidas y a los ataques dirigidos avanzados (APTs).

Panda Adaptive Defense 360 está dividido en dos áreas funcionales bien diferenciadas:

- Panda Adaptive Defense 360
- Plataforma Aether

Panda Adaptive Defense 360

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

Plataforma Aether

Es el ecosistema donde se ejecutan los productos de Panda Security. Aether entrega en tiempo real, de forma ordenada y con un gran nivel de detalle toda la información generada por Panda Adaptive Defense 360 sobre los procesos, los programas ejecutados por los usuarios y los dispositivos que pertenecen a la infraestructura IT de las organizaciones.

Aether es una plataforma eficiente, extensible y escalable, diseñada para cubrir las necesidades de la gran cuenta y de MSPs.

Iconos

En esta Guía de administración se utilizan los siguientes iconos;



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



Sugerencias y recomendaciones.



Consejo importante de cara a un uso correcto de las opciones de Panda Adaptive Defense 360.



Consulta en otra sección de la Guía de administración.

Capítulo 2

Información básica de Panda Adaptive Defense 360

Panda Adaptive Defense 360 es una solución completa de seguridad para puestos de usuario y servidores, formada por múltiples tecnologías que ofrecen a los clientes un completo servicio de protección contra el malware, sin necesidad de instalar, gestionar o mantener nuevos recursos hardware en la infraestructura de la organización.

CONTENIDO DEL CAPÍTULO

Beneficios de Panda Adaptive Defense 360	14
Ejecución de software lícito	14
Adaptación al entorno de la empresa	14
Alcance y solución de problemas de seguridad	14
Multiplataforma	14
Características de Panda Adaptive Defense 360	15
Características de la plataforma Aether	15
Principales beneficios de Aether	16
Plataforma de gestión Cloud	16
Comunicación con la plataforma en tiempo real	16
Multi producto y Multiplataforma	16
Configuraciones flexibles y granulares	17
Información completa y a medida	17
Arquitectura de Aether	17
Aether en los equipos de usuario	18
Agente de comunicaciones en tiempo real Panda	19
Componentes principales	19
Infraestructura de análisis Big Data	21
Servidor Web de la consola de administración	21
Equipos protegidos con Panda Adaptive Defense 360	22
Servicios Panda Adaptive Defense 360	22
Servicio 100% Attestation Service	22
Threat Hunting Investigation Service (THIS)	23
Servicio Panda Advanced Reporting Tool (opcional)	23
Servicio Panda SIEMFeeder (opcional)	23
Servicio Panda Data Control (opcional)	24
Servicio Panda Patch Management (opcional)	24

Servicio Panda Full Encryption (opcional)	24
Perfil de usuario del producto - - - - -	25
Dispositivos e idiomas soportados - - - - -	25
Compatibilidad con sistemas operativos	25
Compatibilidad con navegadores web	25
Idiomas soportados en la consola web	26

Beneficios de Panda Adaptive Defense 360

Panda Adaptive Defense 360 es una solución basada en múltiples tecnologías de protección que permite sustituir el producto de antivirus tradicional por un completo servicio de seguridad gestionada.

Ejecución de software lícito

Panda Adaptive Defense 360 supervisa y clasifica todos los procesos ejecutados en los equipos Windows del parque informático en base a su comportamiento y naturaleza. Gracias a este servicio los puestos de usuario y servidores son protegidos limitando la ejecución de los programas instalados a aquellos que han sido previamente certificados como seguros.

Adaptación al entorno de la empresa

A diferencia de los antivirus tradicionales, Panda Adaptive Defense 360 utiliza un nuevo concepto de seguridad que le permite adaptarse con precisión al entorno particular de cada empresa. Para ello, supervisa la ejecución de todas las aplicaciones y aprende constantemente de las acciones desencadenadas por los procesos lanzados en los puestos de usuario y servidores.

Tras un breve periodo de aprendizaje, Panda Adaptive Defense 360 es capaz de ofrecer un nivel de protección muy superior al de un antivirus tradicional.

Alcance y solución de problemas de seguridad

La oferta de seguridad se completa con herramientas monitorización, análisis forense y resolución, que acotan el alcance de los problemas detectados y los solucionan.

La monitorización aporta datos valiosos sobre el contexto en el que se sucedieron los problemas de seguridad. Con esta información, el administrador podrá determinar el alcance de los incidentes e implantar las medidas necesarias para evitar que vuelvan a producirse.

Multiplataforma

Panda Adaptive Defense 360 es un servicio multiplataforma alojado en la nube y compatible con Windows, macOS, Linux, Android y con entornos virtuales y VDI, tanto persistentes como no persistentes. Por esta razón es suficiente una única herramienta para cubrir la seguridad de todos los equipos de la empresa.

Panda Adaptive Defense 360 no necesita nueva infraestructura IT en la empresa para su gestión y mantenimiento, y por esta razón reduce el TCO de la solución a niveles muy bajos.

Características de Panda Adaptive Defense 360

Panda Adaptive Defense 360 ofrece un servicio de seguridad garantizada frente a amenazas y ataques avanzados dirigidos a las empresas a través de cuatro pilares:



Figura 2.1: Los cuatro pilares de la protección avanzada de Panda Adaptive Defense 360

- **Visibilidad:** trazabilidad de cada acción realizada por las aplicaciones en ejecución.
- **Detección:** monitorización constante de los procesos en ejecución y bloqueo en tiempo real de ataques Zero-day, ataques dirigidos y otras amenazas avanzadas, diseñadas para pasar desapercibidas a los antivirus tradicionales.
- **Resolución y Respuesta:** información forense para investigar en profundidad cada intento de ataque, y herramientas de mitigar sus efectos.

- **Prevención:** evita futuros ataques modificando la configuración de los distintos módulos de protección y parcheando las vulnerabilidades de los sistemas operativos y de las aplicaciones instaladas.

Características de la plataforma Aether

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

La plataforma Aether gestiona las comunicaciones con los agentes desplegados en los equipos protegidos de los clientes, y presenta en la consola de administración, de forma ordenada y comprensible, toda la información recogida por Panda Adaptive Defense 360 para su posterior análisis por parte del administrador de la red.

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

Principales beneficios de Aether

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

Plataforma de gestión Cloud

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

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

Comunicación con la plataforma en tiempo real

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

Multi producto y Multiplataforma

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

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

todo el espectro de dispositivos de la compañía: Aether Platform funciona para Windows, Linux, macOS y Android, además de entornos virtuales y VDI tanto persistentes como no persistentes.

Configuraciones flexibles y granulares

El nuevo modelo de configuración permite acelerar la gestión de los equipos mediante la reutilización de configuraciones, haciendo uso de mecanismos específicos como la herencia y la asignación de configuraciones a equipos individuales. El administrador de la red podrá asignar configuraciones mucho más específicas y con menor esfuerzo.

Información completa y a medida

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

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

Arquitectura de Aether

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

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

En la figura 2.2 se presenta un diagrama a alto nivel de Aether Platform.

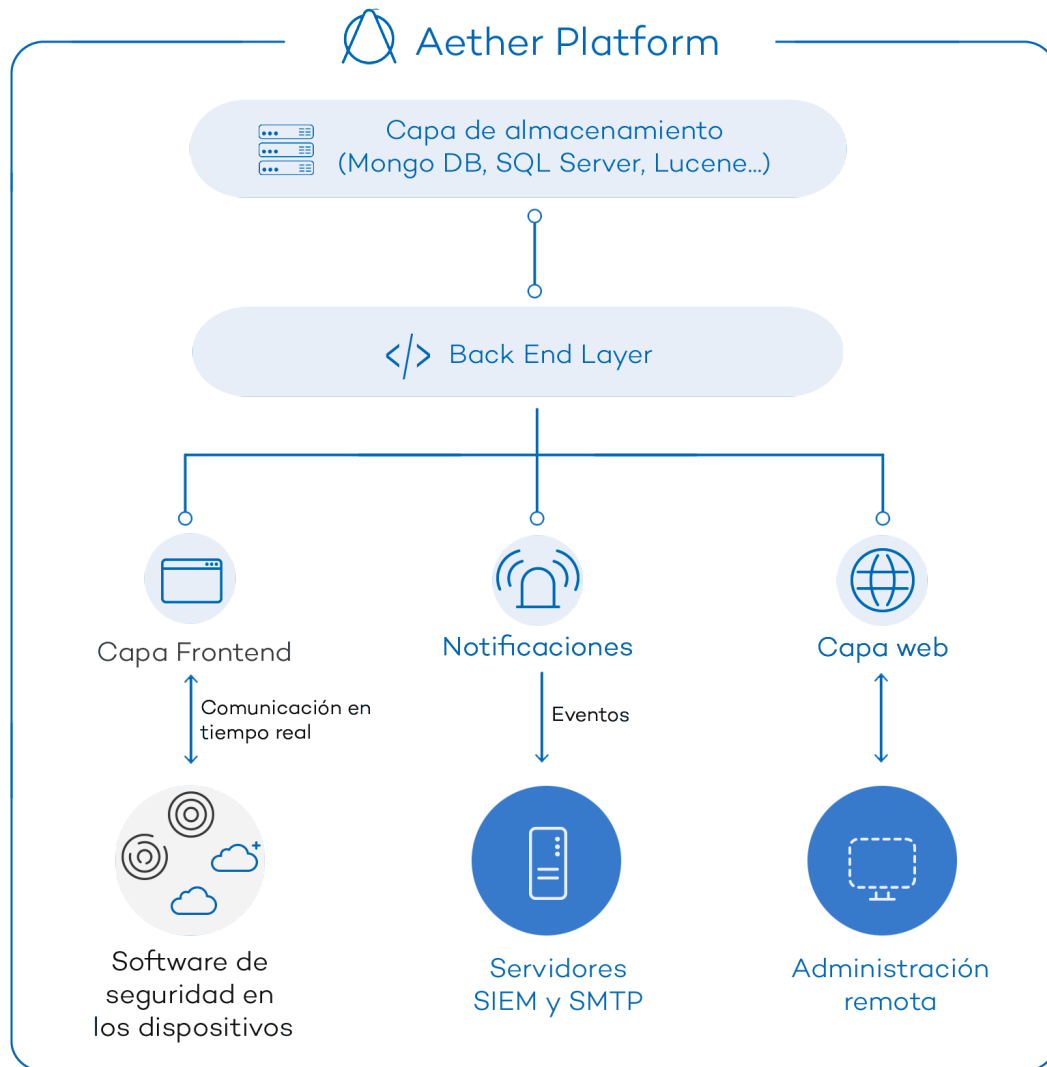


Figura 2.2: Estructura lógica de la plataforma Aether

Aether en los equipos de usuario

Los equipos de la red protegidos con Panda Adaptive Defense 360 llevan instalado un software, formado por dos módulos independientes pero relacionados, que aportan toda la funcionalidad de protección y gestión:

- **Módulo Agente de comunicaciones Panda (agente Panda):** es el encargado de servir de puente entre el módulo de protección y la nube, gestionando las comunicaciones, eventos y configuraciones de seguridad implementadas por el administrador desde la consola de administración.
- **Módulo Protección Panda Adaptive Defense 360:** es el encargado de proteger de forma efectiva el equipo del usuario. Para ello se sirve del agente de comunicaciones para recibir las configuraciones y emite estadísticas y datos de las detecciones y elementos analizado.

Agente de comunicaciones en tiempo real Panda

El agente Panda se encarga de las comunicaciones entre los equipos administrados y el servidor de Panda Adaptive Defense 360, y de establecer un diálogo entre los equipos que pertenecen a una misma red del cliente.

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

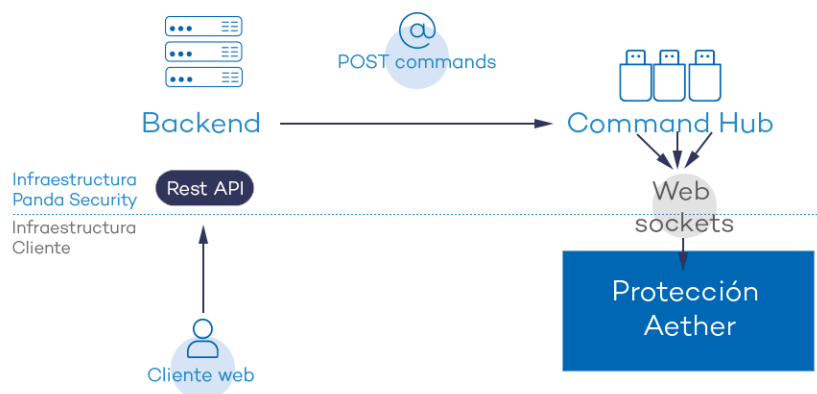


Figura 2.3: Recorrido de los comandos introducidos con la consola de administración

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

Las configuraciones establecidas por el administrador de la red mediante la consola de administración Panda Adaptive Defense 360 se envían mediante una API REST al backend; éste las reenvía al Command hub generando un comando POST, el cual finalmente ejecuta un push de la información a todos los dispositivos suscritos. Con un buen funcionamiento de las líneas de comunicación, los equipos recibirán la configuración en tiempo real.

Componentes principales

Panda Adaptive Defense 360 es un servicio de seguridad que se apoya en el análisis del comportamiento de los procesos ejecutados en los equipos del parque de cada cliente. En este análisis se aplican técnicas de Machine Learning en infraestructuras Big Data alojadas en la nube.

La figura 2.4 representa el esquema general de Panda Adaptive Defense 360 y los componentes que lo forman:

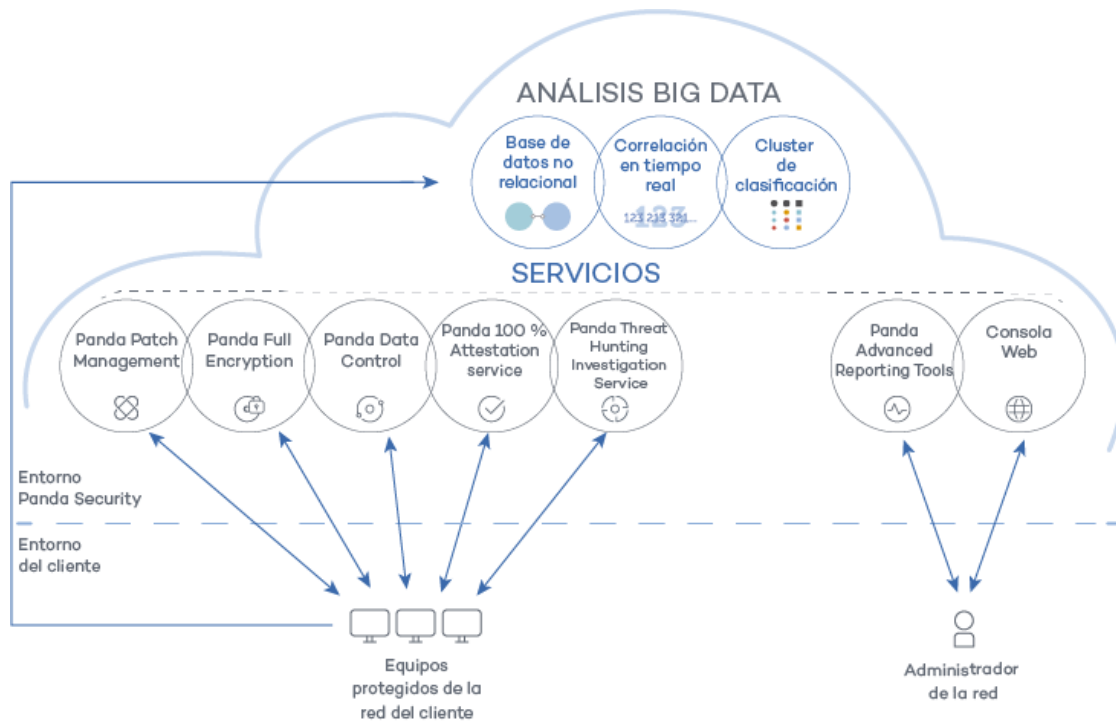


Figura 2.4: Esquema general Panda Adaptive Defense 360

- **Infraestructura de análisis big data,** formada por bases de datos no relacionales, servicios de correlación de eventos monitorizados en tiempo real y un cluster de clasificación de los procesos monitorizados.
- **Servicio 100% Attestation Service:** clasifica todos los procesos ejecutados en equipos Windows sin ambigüedades ni falsos positivos ni negativos.
- **Servicio Threat Hunting Investigation Service (THIS):** detecta amenazas y ataques de tipo “Living off the Land”, diseñados para evadir las protecciones instaladas en el equipo.
- **Panda SIEMFeeder (opcional):** integra Panda Adaptive Defense 360 con soluciones SIEM de proveedores externos.
- **Servicio Panda Data Control (opcional):** servicio de visibilidad, inventario y supervisión de la información personal que almacenan los ficheros PII.
- **Servicio Panda Advanced Reporting Tool (opcional):** servicio de informes para generar inteligencia de seguridad avanzada.
- **Servicio Panda Patch Management (opcional):** parcheo de sistemas operativos Windows y aplicaciones de terceros.
- **Servicio Panda Full Encryption (opcional):** cifra los dispositivos de almacenamiento interno de los equipos Windows para minimizar la exposición de datos en caso de pérdida o robo, o al desechar dispositivos de almacenamiento sin borrar completamente su contenido.
- **Consola web:** servidor de la consola de administración.

- Equipos protegidos mediante el software Panda Adaptive Defense 360 instalado.
- Equipo del administrador de red que accede a la consola Web.

Infraestructura de análisis Big Data

Es el clúster de servidores en la nube que recibe la telemetría generada en los equipos del parque informático del cliente. La telemetría está formada por las acciones ejecutadas por los programas del usuario y monitorizados por el módulo de protección, sus atributos estáticos y la información de contexto de ejecución. Todo ello forma flujo contante de información que se analiza en la nube mediante técnicas de inteligencia artificial para evaluar el comportamiento de dichos programas y emitir una clasificación por cada proceso en ejecución. Esta clasificación se devuelve al módulo de protección del equipo, y se toma como base para ejecutar las acciones configuradas con el objeto de mantenerlo protegido.

Las ventajas de este nuevo modelo de análisis de procesos frente al adoptado por los antivirus tradicionales basados en el envío de muestras al proveedor y análisis manual son:

- Todos los procesos de los equipos protegidos son monitorizados y analizados: se elimina la incertidumbre de los antivirus tradicionales, capaces únicamente de reconocer el malware sin considerar el resto de aplicaciones.
- El retraso en la clasificación de los procesos vistos por primera vez (ventana de oportunidad) es mínimo ya que Panda Adaptive Defense 360 envía en tiempo real las acciones que ejecuta cada proceso. Los servidores en la nube trabajan de forma constante con esta información, disminuyendo de manera sustancial el tiempo necesario para emitir una clasificación, y por tanto el tiempo de exposición a las amenazas.
- La monitorización continua de cada proceso permite a Panda Adaptive Defense 360 clasificar como malware elementos que inicialmente eran considerados goodwill. Este cambio de comportamiento es muy habitual en los ataques dirigidos y otras amenazas avanzadas diseñadas para operar por debajo del radar.
- El análisis en la nube libera al cliente de instalar y mantener infraestructura de hardware y software junto al pago de licencias y la gestión de garantías del hardware, con lo que el TCO de la solución desciende significativamente.

Servidor Web de la consola de administración

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



Para verificar si tu navegador es compatible con el servicio consulta "[Acceso a la consola web](#)" en la página 559.

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

Equipos protegidos con Panda Adaptive Defense 360

Panda Adaptive Defense 360 requiere de la instalación de un componente software en todas las máquinas del parque informático susceptibles de sufrir problemas de seguridad. Este componente está formado por dos módulos: el agente de comunicaciones Panda y el módulo de la protección Panda Adaptive Defense 360.



Panda Adaptive Defense 360 se instala sin problemas en máquinas con otras soluciones de seguridad de la competencia.

El módulo de la protección Panda Adaptive Defense 360 contiene las tecnologías encargadas de proteger los equipos del cliente. Panda Adaptive Defense 360 reúne en un mismo producto todos los recursos necesarios para detectar el malware de nueva generación y ataques dirigidos (APT), al tiempo que incorpora herramientas de gestión de la productividad y de resolución para desinfectar los equipos comprometidos y determinar el alcance de los intentos de intrusión en la red del cliente.

Servicios Panda Adaptive Defense 360

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

Servicio 100% Attestation Service

Este servicio incluido por defecto en el producto en equipos Windows tiene como objetivo permitir la ejecución únicamente de los programas certificados por Panda Security. Para conseguirlo, se utiliza una mezcla de tecnologías locales en el equipo del usuario y en la infraestructura de análisis big data que clasifican de forma automática el 99'98% de los procesos ejecutados. Para el resto de procesos se aplican clasificaciones manuales ejecutadas por expertos en malware. Con este enfoque se consiguen clasificar el 100% de los binarios ejecutados en los equipos de los clientes sin falsos positivos ni negativos.

Los ficheros ejecutables encontrados en el equipo del usuario y desconocidos para la plataforma se envían de forma automática a la infraestructura de análisis big data para su análisis.



Los ficheros desconocidos se envían una sola vez para todos los clientes que usan Panda Adaptive Defense 360, por lo tanto, el impacto en el rendimiento de la red del cliente es prácticamente nulo. Además, se han implementado mecanismos de gestión del ancho de banda y límites por equipo y hora.

Threat Hunting Investigation Service (THIS)

Servicio incluido por defecto en Panda Adaptive Defense y Panda Adaptive Defense 360 que detecta amenazas y ataques de tipo "Living off the Land", diseñados para evadir las protecciones instaladas en el equipo.

Este servicio está operado por un equipo de expertos en ciberseguridad, que utiliza la herramienta Orion, la plataforma de Threat Hunting avanzada desarrollada por Cytomic.

Gracias a la telemetría que se envía desde los dispositivos del cliente a Orion, el equipo de investigación puede analizar el funcionamiento del software de la empresa para detectar nuevos ataques y crear reglas avanzadas de hunting como hipótesis de trabajo. En caso de confirmarse una hipótesis, se contacta con el cliente para informarle del potencial ataque y darle las recomendaciones de actuación.

Si la hipótesis confirmada resulta en la detección de una nueva amenaza, ésta se consolidará en el fichero de firmas o en la Inteligencia Colectiva para distribuirse entre los equipos de los clientes de Panda Adaptive Defense 360.

Servicio Panda Advanced Reporting Tool (opcional)

Panda Adaptive Defense 360 envía de forma automática y transparente toda la información recogida de los equipos al servicio Panda Advanced Reporting Tool, un sistema de almacenamiento y explotación del conocimiento.

Las acciones de los procesos ejecutados en el parque de IT se envían a Panda Advanced Reporting Tool donde se estudian y relacionan para extraer inteligencia de seguridad. El administrador dispondrá de información adicional sobre las amenazas y sobre el uso que los usuarios dan a los equipos de la empresa. Esta nueva información se presenta de forma flexible y visual para favorecer su comprensión.

El servicio Panda Advanced Reporting Tool es accesible directamente desde el panel de control de la propia consola Web de Panda Adaptive Defense 360.



Consulta la Guía de usuario Panda Advanced Reporting Tool accesible desde la web de producto para configurar y sacar provecho del servicio de análisis de conocimiento y búsquedas avanzadas.

Servicio Panda SIEMFeeder (opcional)

Panda Adaptive Defense 360 se integra con las soluciones SIEM de proveedores externos implementadas por los clientes en sus infraestructuras de IT. La actividad de las aplicaciones que se ejecutan en el parque informático se entrega al servidor al SIEM, ampliada con todo el conocimiento ofrecido por Panda Adaptive Defense 360, y lista para ser utilizada.

A continuación, se listan los sistemas SIEM compatibles con Panda Adaptive Defense 360:

- QRadar
- AlienVault
- ArcSight
- LookWise
- Bitacora



Consulta la *Guía de usuario Panda SIEMFeeder* para una descripción detallada de la información recogida por Panda Adaptive Defense 360 y enviada al sistema SIEM del cliente.

Servicio Panda Data Control (opcional)

Es un módulo de seguridad integrado en la plataforma Panda Adaptive Defense 360 que ayuda a cumplir con las regulaciones en materia de retención de datos personales (PII) almacenados en la infraestructura IT de las empresas.

Panda Data Control descubre, audita y monitoriza en tiempo real el ciclo de vida completo de los ficheros PII almacenados en equipos Windows: desde datos en reposo, las operaciones efectuadas sobre ellos y su transferencia al exterior. Con esta información, Panda Data Control genera un inventario por cada equipo de la red que permite mostrar la evolución de los ficheros que contienen información personal.



Consulta “[Panda Data Control \(Supervisión de información sensible\)](#)” en la [página 269](#) para una descripción detallada del servicio.

Servicio Panda Patch Management (opcional)

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

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

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

Servicio Panda Full Encryption (opcional)

El cifrado de la información contenida en los dispositivos de almacenamiento interno de los equipos es un recuso fundamental a la hora de proteger los datos que contienen en caso de robo o pérdida y

cuando la empresa recicla dispositivos de almacenamiento sin borrar completamente. Panda Adaptive Defense 360 utiliza la tecnología BitLocker de Windows para cifrar el contenido de los discos duros a nivel de sector y gestiona de forma centralizada las claves de recuperación en caso de pérdida o cambio de configuración de hardware.

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

Perfil de usuario del producto

Aunque Panda Adaptive Defense 360 es un servicio gestionado que ofrece seguridad sin intervención del administrador de la red, también provee información muy detallada y comprensible sobre la actividad de los procesos ejecutados por los usuarios en toda la infraestructura de IT de la empresa. Esta información puede ser utilizada por el administrador para precisar el impacto de problemas de seguridad y adaptar sus protocolos, evitando así la repetición de situaciones similares en el futuro.

Dispositivos e idiomas soportados



Para una descripción detallada de las plataformas y requisitos consulta "[Requisitos de hardware, software y red](#)" en la página [551](#).

Compatibilidad con sistemas operativos

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

Compatibilidad con navegadores web

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

- Chrome
- Internet Explorer

- Microsoft Edge
- Firefox
- Opera

Idiomas soportados en la consola web

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

Capítulo 3

El ciclo de protección adaptativa

El malware de nueva generación está enfocado en pasar inadvertido dentro de los sistemas informáticos durante largos periodos de tiempo para poder obtener beneficios económicos de las empresas. El ciclo de protección adaptativa es el nuevo paradigma que surge en respuesta a esta evolución. Panda Adaptive Defense 360 implementa los recursos necesarios para detectar y proteger a las empresas de estas nuevas amenazas, así como resolver los problemas ocasionados y adaptar la estrategia de seguridad para evitar infecciones futuras.

CONTENIDO DEL CAPÍTULO

Las nuevas necesidades de seguridad	-28
El ciclo de protección adaptativa	-28
Fase I: Protección completa del parque informático	-29
Protección antivirus permanente e inteligencia colectiva	29
Protección contra técnicas de ocultación y virus de macro	30
Bloqueo de programas	30
Protección del correo y la Web	31
Cortafuegos y sistema de detección de intrusos (IDS)	31
Control de dispositivos	31
Filtrado de Spam, Virus y contenidos en servidores Exchange	31
Protección de buzones	32
Protección de transporte	32
Control de acceso a páginas Web	32
Fase II: Detección y monitorización	-33
Protección permanente avanzada	33
Audit	33
Hardening	33
Lock	34
Protección contra exploits	34
Detección de amenazas sin fichero y servicio THIS	35
Monitorización de ficheros de datos (Panda Data Control)	36
Parcheo de vulnerabilidades (Panda Patch Management)	36
Visibilidad del estado de la red	37
Fase III: Resolución y respuesta	-38
Respuesta	38
Resolución	38

Fase IV: Adaptación / Prevención **38**

Las nuevas necesidades de seguridad

En la actualidad se generan más de 200.000 nuevos virus diariamente, una parte muy sustancial de ellos diseñados para ejecutarse en los equipos de los usuarios durante periodos de tiempo alargados y en segundo plano, sin dar muestras de su existencia.

Esta nueva estrategia del malware está volviendo gradualmente ineficiente el enfoque tradicional de protección mediante archivos de identificadores locales o en la nube: el creciente número de malware desarrollado puede considerarse en si mismo un ataque global por fuerza bruta a los proveedores de seguridad, que busca ampliar la ventana de oportunidad sobrepasando los recursos que éstos dedican a analizar el malware. Por esta razón, la media de tiempo transcurrido desde que el primer equipo es infectado a nivel mundial hasta que los proveedores de seguridad son conscientes de este nuevo malware y consiguen identificarlo es cada vez mayor. Alimentar los archivos de identificadores y desplegarlos en los equipos de los usuarios incrementa todavía mas el tiempo total de exposición, especialmente en aquellos proveedores que todavía confían la seguridad de sus clientes en los ficheros de firmas y no han migrado su inteligencia de seguridad a la nube.

Con esta nueva situación, la estrategia de seguridad a adoptar pasa por minimizar el tiempo de exposición al malware, exposición estimada actualmente en 259 días para ataques dirigidos, cada vez más frecuentes y que tienen como principales objetivos el robo de datos y el espionaje industrial.

Panda Adaptive Defense 360 propone un nuevo enfoque de seguridad basado en el ciclo de protección adaptativa: un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución. Todos los servicios están integrados y centralizadas en una única consola Web de administración para mostrar el ciclo completo en tiempo real.

Con este nuevo enfoque se evitan o minimizan al máximo las brechas de seguridad, reduciendo de forma drástica las pérdidas de productividad y el riesgo de robo de información confidencial en las empresas; el administrador es liberado de la compleja tarea de determinar qué es peligroso y por qué razón, recuperando espacio y recursos para gestionar y vigilar el estado de la seguridad.

El departamento de IT podrá tomar decisiones que permitan adaptar la política de seguridad de la empresa con la misma agilidad que mutan los patrones de ataque del malware avanzado.

El ciclo de protección adaptativa

El objetivo de Panda Adaptive Defense 360 es el de facilitar al departamento de IT la creación de un espacio donde definir y establecer las políticas de seguridad de la empresa que respondan rápida y adecuadamente a los nuevos tipos de amenazas.

Este espacio es producto, 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: **con Panda Adaptive Defense 360 el departamento técnico de la empresa recibirá una clasificación sin ambigüedades de absolutamente todos los programas ejecutados en el parque informático gestionado.**

Por otra parte, el departamento de IT también recibirá un conjunto de herramientas para la visualización del estado de la seguridad, la resolución de los problemas ocasionados por el malware avanzado y el estudio de forma detallada del comportamiento de APTs y otras amenazas.

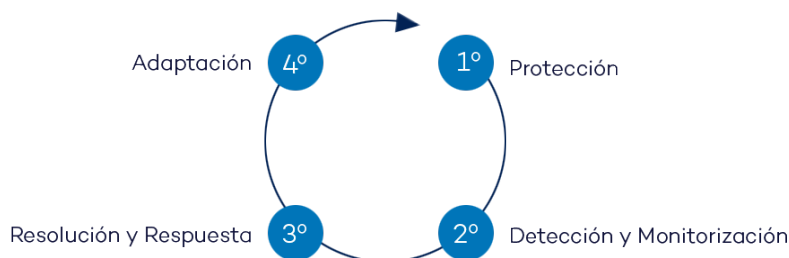


Figura 3.1: El ciclo de protección adaptativa

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, en caso de producirse brechas de seguridad revertir los equipos afectados a una situación previa, y conocer el alcance de aquellas para poder implementar las medidas de contingencia apropiadas. Todo este ciclo encaja dentro de un proceso de refinamiento contante, que resultará en un entorno informático seguro, flexible y productivo para los usuarios de la empresa.

Este ciclo constante de protección adaptativa implementado por las empresas con ayuda de Panda Adaptive Defense 360 se puede resumir en la figura 3.1.

Fase I: Protección completa del parque informático

La primera fase del ciclo de protección adaptativa incluye las herramientas necesarias para proteger y defender de forma efectiva el parque informático de ataques e intentos de infección.

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. 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. Por esta razón,

la protección de antivirus de Panda Adaptive Defense 360 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 Panda Adaptive Defense 360 instalada en los equipos consulta a la Inteligencia Colectiva cuando lo necesita, consiguiendo así maximizar su capacidad de detección y sin afectar negativamente al consumo de recursos.

Cuando se detecta un nuevo ejemplar de malware en el equipo de un miembro de la comunidad de usuarios, Panda Adaptive Defense 360 envía la información a los servidores de Inteligencia Colectiva alojados en la nube, de forma automática y anónima. Esta información es procesada para generar una solución no sólo al usuario afectado, sino también al resto de usuarios de la comunidad, en tiempo real.

Panda Adaptive Defense 360 utiliza la Inteligencia Colectiva para aumentar la capacidad de detección y evitar penalizaciones en el rendimiento del equipo del cliente. Todo el conocimiento está en la nube y todos los usuarios pueden beneficiarse de ello.



Para más información sobre el servicio de antivirus de Panda Adaptive Defense 360 en plataformas Windows, Linux y macOS consulta "[Configuración de la seguridad en estaciones y servidores](#)".

Para más información sobre el servicio de antivirus de Panda Adaptive Defense 360 en plataformas Android consulta "[Configuración de seguridad Android](#)".

Protección contra técnicas de ocultación y virus de macro

Al margen de la estrategia tradicional de detección que compara el payload del fichero objeto de estudio con el contenido en el fichero de firmas, Panda Adaptive Defense 360 implementa varios motores de detección que analizan 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 en macros maliciosas embebidas en ficheros ofimáticos como Word, Excel, PowerPoint etc.

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

Bloqueo de programas

Para incrementar la seguridad de partida en los equipos Windows de la red, el administrador podrá prohibir la ejecución de los programas que previamente haya clasificado como peligrosos o no compatibles con la actividad desarrollada en la empresa.

Las causas que pueden llevar a un administrador a prohibir la ejecución de un determinado programa pueden ser variadas: programas que consumen mucho ancho de banda, que acceden a contenidos susceptibles de contener amenazas de seguridad, o que acceden a contenidos que afectan al rendimiento de los usuarios o de sus equipos.

Protección del correo y la Web

Panda Adaptive Defense 360 se aleja del tradicional enfoque de seguridad basado en plugins que añaden la funcionalidad de protección a determinados programas (clientes de correo o navegadores). En su lugar, la protección intercepta 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: no se necesitan configuraciones específicas ni actualizaciones cuando los proveedores de los programas de correo y navegación publiquen nuevas versiones incompatibles con plugins anteriores.

Cortafuegos y sistema de detección de intrusos (IDS)

Panda Adaptive Defense 360 incorpora tres herramientas básicas para filtrar el tráfico de red que reciben o envían los equipos protegidos, que se ajustan de forma automática en función del tipo de red a la que se conecta la estación de trabajo o servidor:

- **Protección mediante reglas de sistema:** 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:** permiten o deniegan la comunicación de determinados programas instalados en el equipo de usuario con el resto de la red.
- **Sistema de detección de intrusos:** detecta y rechaza patrones de tráfico mal formado que afecten a la seguridad o al rendimiento del equipo protegido.

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.

Panda Adaptive Defense 360 permite establecer el comportamiento de estos dispositivos en los equipos protegidos, bloqueando su acceso o permitiendo su uso de forma parcial (solo lectura) o completa.

Filtrado de Spam, Virus y contenidos en servidores Exchange

Panda Adaptive Defense 360 analiza 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.

Eliminar el correo basura -spam- es una labor que requiere mucho tiempo y además supone un peligro de estafa. Panda Adaptive Defense 360 implementa una protección anti-spam para servidores Exchange para optimizar el tiempo de trabajo de los usuarios y aumentar la seguridad de los equipos de la red.

Panda Adaptive Defense 360 protege los servidores de correo Exchange mediante dos tecnologías:

- Protección de buzones.
- Protección de transporte.

Protección de buzones

Aplica a los servidores Exchange con el rol de Mailbox, y analiza las carpetas / buzones en background o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones manipula los diferentes elementos del cuerpo del mensaje analizado para sustituir aquellos clasificados como peligrosos por otros seguros e introducir únicamente los primeros en la cuarentena.

La protección de buzones analiza las carpetas de usuario del servidor Exchange en segundo plano, aprovechando los tiempos de menor carga del servidor. Este análisis se ejecuta de forma inteligente, evitando volver a analizar los mensajes ya examinados. Con cada nuevo archivo de identificadores publicado se analizarán los buzones y la cuarentena en segundo plano.

Protección de transporte

Aplica a los servidores Exchange con el rol de Acceso de clientes, Edge Transport y Mailbox y analiza el tráfico que atraviesa al servidor.

En la protección de transporte no se permite la manipulación del cuerpo de los mensajes. De esta forma, el cuerpo de un mensaje peligroso se trata como un único bloque y las acciones que Panda Adaptive Defense 360 permite ejecutar aplican al mensaje por completo: borrar el mensaje, meterlo en cuarentena, dejar pasar sin modificar etc.

Control de acceso a páginas Web

Panda Adaptive Defense 360 agrupa las páginas web en varias categorías para que el administrador de la red pueda restringir el acceso a las que considere oportunas, así como a las URLs que especifique de forma manual. Con esta protección se optimiza el ancho de banda de la red y la productividad de la organización, evitando el acceso a recursos web sin relación con la actividad desarrollada en la empresa.

Además, se permite definir una configuración de horarios para 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.

Fase II: Detección y monitorización

La segunda fase del ciclo de protección adaptativa asume que el malware o el ataque dirigido consiguió sortear las barreras establecidas en la fase de Protección e infectó con éxito una o varias máquinas de la red, pasando esta infección desapercibida para el usuario del equipo.

En esta fase, Panda Adaptive Defense 360 implementa una serie de tecnologías que permiten al administrador de la red localizar el problema.

Protección permanente avanzada

La protección avanzada monitoriza de forma continuada todos los procesos que se ejecutan en los equipos de la red del cliente. Panda Adaptive Defense 360 recoge todas las acciones desencadenadas por los procesos del usuario y los envía a la nube de Panda Security, donde se examinan mediante técnicas automáticas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) con un 99'9991 (menos de 1 error cada 100.000 ficheros analizados) de precisión, evitando de esta manera falsos positivos.

Para los casos más complicados Panda Security cuenta con un laboratorio de expertos especialistas en análisis de malware, con el único objetivo de clasificar todos los ejecutables localizados en el menor tiempo posible, desde la primera vez que fueron vistos en la red del cliente.

Panda Adaptive Defense 360 admite tres modos de bloqueo para los procesos que todavía no han sido clasificados (desconocidos) y para los ya clasificados como malware:

- Audit
- Hardening
- Lock

Audit

En el modo Audit Panda Adaptive Defense 360 solo informa de las amenazas detectadas, pero no bloquea ni desinfecta el malware encontrado. Este modo es útil para probar la solución de seguridad o para comprobar que la instalación del producto no compromete el buen funcionamiento del equipo.

Hardening

En aquellos entornos donde se producen cambios constantes del software instalado en los equipos de los usuarios o se ejecutan muchos programas desconocidos (como por ejemplo programas de creación propia) puede no ser viable esperar a que Panda Adaptive Defense 360 aprenda de ellos para clasificarlos.

El comportamiento del modo Hardening consiste en balancear el riesgo de infección de los equipos y la productividad de los usuarios, limitando el bloqueo de los programas desconocidos a aquellos que a priori se consideran peligrosos. De esta forma se distinguen cuatro escenarios:

- **Ficheros ya clasificados por Panda Adaptive Defense 360 como *goodware*:** se permite su ejecución.
- **Ficheros ya clasificados por Panda Adaptive Defense 360 como *malware*:** son enviados a cuarentena o desinfectados.
- **Ficheros sin clasificar que vienen del exterior (Internet, correo, dispositivos USB, otros equipos de la red del cliente):** se bloquea su ejecución hasta que el sistema emita una clasificación. En función de ésta se permitirá su ejecución (*goodware*) o serán movidos a cuarentena (*malware*).



*En muchas ocasiones la clasificación es casi inmediata; un programa descargado de Internet y desconocido para Panda Adaptive Defense 360 será bloqueado en un primer momento, pero minutos después se podrá ejecutar si resultó ser *goodware*.*

- **Ficheros sin clasificar ya instalados en el equipo del usuario antes de la implantación de Panda Adaptive Defense 360:** se permite su ejecución, aunque sus acciones se monitorizan y se envían al servidor para su estudio. Una vez clasificados se permitirá su ejecución (*goodware*) o se bloqueará (*malware*).

Lock

Para entornos donde la seguridad sea la máxima prioridad, y con el objetivo de ofrecer una protección de máximas garantías, Panda Adaptive Defense 360 incluye el modo Lock. En este modo se bloquea la ejecución del software en proceso de clasificación y todo aquel que ya ha sido clasificado como *malware*. Únicamente se permite ejecutar el software lícito.



Más del 99% de los programas encontrados en los equipos de los usuarios ya están clasificados en los sistemas de Panda Adaptive Defense 360 por lo que los bloqueos por desconocidos afectan a una minoría de programas. Para más información sobre la configuración de los distintos modos de bloqueo consulta "[Protección avanzada](#)" en la página [242](#).

Protección contra exploits

Panda Adaptive Defense 360 implementa tecnologías para proteger los equipos de la red frente a las amenazas que aprovechan vulnerabilidades en el software. Estas vulnerabilidades son utilizadas (explotadas) para provocar comportamientos anómalos en las aplicaciones, produciendo fallos de seguridad.

Las amenazas de tipo exploit utilizan tanto vulnerabilidades conocidas como de día cero (0-day) o desconocidas, como parte de una cadena de eventos conocida como CKC (Cyber Kill Chain), que ejecutan para comprometer los equipos de la red. Panda Adaptive Defense 360 bloquea de forma

efectiva y en tiempo real esta cadena de eventos para impedir que los ataques de tipo exploit prosperen y dejarlos sin efecto.

Para detectar las técnicas de explotación de vulnerabilidades usadas por los hackers, Panda Adaptive Defense 360 implementa nuevos hooks en el sistema operativo, que utiliza para monitorizar localmente y de forma constante las acciones de los procesos ejecutados en el equipo del usuario. Este enfoque se aleja del esquema tradicional implementado por otros productos de seguridad, que buscan patrones y detecciones estáticas de pares CVE - payload mediante ficheros de firmas.

Panda Adaptive Defense 360 ofrece una protección anti exploit generalista gracias a la constante adaptación de la tecnología encargada de detectar el uso de técnicas avanzadas de explotación de vulnerabilidades, algunas de las cuales se muestran a continuación:

- Attack Surface Reduction (ASR)
- Data Execution Prevention (DEP)
- Structured Exception Handling Overwrite Protection (SEHOP)
- NullPage Security Mitigation
- Heapspray Allocation
- Export Address Table Filtering (EAF)
- Mandatory Address Space Layout Randomization (ASLR)
- Bottom Up ASLR Security Mitigation
- Load Library Check - Return Oriented Programming (ROP)
- Memory Protection Check - Return Oriented Programming (ROP)
- Caller Checks - Return Oriented Programming (ROP)
- Simulate Execution Flow - Return Oriented Programming (ROP)
- Stack Pivot - Return Oriented Programming (ROP)
- EternalBlue
- Process Doppelganging

Detección de amenazas sin fichero y servicio THIS

Las amenazas fileless / malwareless sortean las estrategias tradicionales de detección de malware basadas en archivos de identificadores, evitando almacenar ficheros en el disco duro del equipo infectado. Estas amenazas únicamente residen en la memoria RAM del equipo, volviéndose muy complicadas de detectar y de cuantificar el alcance de sus acciones mediante procesos de análisis forense estándar.

La protección avanzada de Panda Adaptive Defense 360 es capaz de evitar esta estrategia monitorizando de forma continuada todos los procesos ejecutados y analizando su comportamiento. Los procesos que muestren una secuencia de acciones declarada como peligrosa serán clasificados

como malware, independientemente del número de ficheros que depositen en el sistema de almacenamiento del equipo de usuario o servidor. De esta misma manera, al quedar almacenadas todas las acciones del proceso en la nube de Panda Security, es posible ejecutar un análisis forense completo.

Adicionalmente, el servicio THIS pone a disposición de los analistas en ciberseguridad de Panda Security la herramienta Orion. Este servicio analiza la telemetría obtenida de la monitorización de los procesos ejecutados en los equipos de cada cliente y genera hipótesis, las cuales serán confirmadas o desechadas más adelante por analistas de nivel superior. Si una hipótesis se confirma y los patrones de acciones sospechosas detectados pertenecen a un ataque desconocido, la nueva clasificación se propagará a todos los clientes de Panda Security para mejorar su seguridad globalmente.

Monitorización de ficheros de datos (Panda Data Control)

Panda Adaptive Defense 360 registra todos los accesos a ficheros de datos del usuario por parte de los procesos ejecutados en el equipo. Aunque el malware consiga infectar el equipo, es posible precisar con exactitud qué ficheros modificó y en qué momento. También es posible determinar si envió ficheros fuera de la empresa a través de Internet, las direcciones IP de destino y otra información valiosa que facilita tanto el análisis forense posterior como las acciones de resolución. A continuación, se muestran los tipos de ficheros de datos que se monitorizan:

- Documentos de suites ofimáticas.
- Documentos en formato PDF.
- Documentos de aplicaciones CAD.
- BBDD de escritorio.
- Almacenes de contraseñas de navegadores.
- Almacenes de contraseñas de clientes de correo.
- Almacenes de contraseñas de clientes de FTP.
- Almacenes de contraseñas de Directorio Activo.
- Almacenes de certificados y certificados de usuario.
- Almacenes de Digital Wallet.
- Configuración de navegadores.
- Configuración de firewall.
- Configuración de GPO.

Parqueo de vulnerabilidades (Panda Patch Management)

Panda Patch Management mantiene de forma automática una base de datos de los parches y actualizaciones publicadas por los proveedores del software para los sistemas operativos Windows

instalados en el parque informático. Comparando esta base de datos con los parches ya instalados en los equipos se muestran aquellos que contienen software vulnerable, y que por lo tanto son susceptibles de recibir ataques de programas maliciosos para infectar la red de la empresa.

Para evitar esto, Panda Patch Management permite crear tareas programadas e inmediatas de parcheo de los equipos, reduciendo de esta forma la superficie de ataque de puestos de usuario y servidores.

Visibilidad del estado de la red

Panda Adaptive Defense 360 implementa recursos para poder valorar el estado de la seguridad de la red en un solo vistazo, a través de informes y de un panel de control (dashboard) formado por diferentes widgets.

Lo importante en esta etapa no solo es determinar si la red del cliente está siendo atacada y en qué grado o forma, sino contar con la información necesaria para poder valorar una probabilidad de infección.

En los paneles de Panda Adaptive Defense 360 se incluye información clave en este sentido:

- Cuáles son los procesos desconocidos para Panda Adaptive Defense 360 encontrados en los equipos de la red, y que están siendo investigados para su posterior clasificación en Panda Security, junto con una valoración preliminar de su peligrosidad.
- Actividad detallada en forma de listados de acciones de aquellos programas desconocidos que finalmente resultaron ser malware.
- Detecciones realizadas en los diferentes vectores de infección protegidos.

Con este módulo el administrador tiene una visión global de los procesos que se ejecutan en su red: por el lado del malware ya conocido que intentó infectar algún equipo y fue detenido en el módulo de protección; y por el lado del malware desconocido y diseñado para pasar inadvertido por las tecnologías de detección tradicionales, y que consiguió sortear los sistemas de detección configurados.

El administrador tendrá la posibilidad de reforzar la seguridad de su red impidiendo toda ejecución de software desconocido o, por el contrario, balancear el nivel de bloqueo en favor de una mayor flexibilidad a la hora de ejecutar ciertos programas no conocidos.



Para más información consulta “[Visibilidad del malware y del parque informático](#)” en la [página 411](#).

Fase III: Resolución y respuesta

En caso de producirse una brecha de seguridad, es necesario actuar en dos líneas: revertir de forma rápida el estado de los equipos afectados previo a la infección, y calcular el impacto del ataque: si hubo fuga de datos, hasta donde consiguió penetrar el ataque, qué equipos resultaron comprometidos etc. Panda Adaptive Defense 360 incorpora herramientas para estos dos escenarios.

Respuesta

Mediante la herramienta de análisis forense el administrador puede ver todas las acciones ejecutadas por el malware en el equipo infectado, así como información fundamental a la hora de valorar la peligrosidad de la amenaza: vector de infección (como llegó el malware a la red de la organización), patrón de propagación a otros equipos y accesos al disco duro en busca de información confidencial, entre otros.

Panda Adaptive Defense 360 genera un entorno seguro para que el administrador ejecute el análisis forense, aislando los equipos afectados de la red. De esta manera, se impiden las comunicaciones con el exterior para evitar la fuga de información, pero se mantiene la conexión con la nube de Panda Security para investigar el suceso sin desplazarse físicamente al equipo afectado.

Además, Panda Advanced Reporting Tool y Panda Data Control extienden y ayudan a interpretar los datos recogidos por Panda Adaptive Defense 360. El administrador tiene acceso a información representada gráficamente de todos los procesos ejecutados por el usuario, y no solo de los clasificados como malware. También se identifican los ficheros que contienen datos personales (PII) y los procesos que acceden a ellos y los envían fuera de la red de la organización.

Resolución

Panda Adaptive Defense 360 cuenta con herramientas de desinfección propias de un antivirus tradicional junto a la cuarentena, que almacena los elementos sospechosos o eliminados.



Para más información consulta "[Herramientas de resolución](#)" en la página [525](#).

Fase IV: Adaptación / Prevención

Una vez finalizado el estudio del incidente con las herramientas de Resolución y respuesta de la Fase III y localizadas las causas que propiciaron la infección, el administrador deberá ajustar la política de seguridad de la empresa para que no se vuelvan a producir situaciones equivalentes en el futuro.

La fase de Adaptación puede reunir una gran cantidad de iniciativas en función de los resultados revelados por el análisis forense: desde cursos de educación y sensibilización en el correcto uso de

Internet para los empleados de la empresa, hasta la reconfiguración de los routers corporativos o de los permisos de los usuarios en sus máquinas personales.

Desde el punto de vista de los dispositivos, Panda Adaptive Defense 360 puede reforzar la seguridad cambiando la configuración de la protección avanzada: si los usuarios de la empresa tienden a utilizar siempre el mismo software, o algunos de ellos suelen instalar programas de dudosa procedencia, una opción para minimizar el riesgo de estos equipos es implementar el modo Lock de la protección avanzada. De esta forma se limita la exposición al malware en los equipos más problemáticos impidiendo la ejecución de los programas que no sean legítimos.

Desde el punto de vista del equipo de usuario o servidor, Panda Adaptive Defense 360 puede reforzar la seguridad de múltiples maneras:

- **Cambio en la configuración de la protección avanzada.**

Si los usuarios de la empresa tienden a utilizar siempre el mismo software, o algunos de ellos suelen instalar programas de dudosa procedencia, una opción para minimizar el riesgo de estos equipos es implementar el modo Lock de la protección avanzada. De esta forma se limita la exposición al malware en los equipos más problemáticos y se impide la ejecución de los programas que no sean legítimos.

- **Cambio de la configuración de la protección antivirus**

Cambiar la frecuencia de los análisis bajo demanda o activar la protección de vectores de infección como Web o correo ayudarán a proteger los equipos que reciban malware por estas dos vías.

- **Limitación de la navegación Web a categorías concretas**

Reconfigurar las categorías accesibles a la navegación para limitar 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.

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

Un vector muy utilizado para ataques de tipo phishing es el correo. Refuerza la configuración del filtrado de contenidos y del filtro anti spam para limitar la cantidad de correo no solicitado que llega a los buzones de los usuarios, reduciendo así la superficie de ataque.

- **Bloqueo parcial o total de pen drives y otros dispositivos externos**

Otro de los vectores de infección más típicos son las memorias y los módems USB que los usuarios tienen en propiedad. Limita o bloquea completamente su uso para evitar la infección por estas vías.

- **Limitación de las comunicaciones (Firewall e IDS)**

El firewall es una herramienta orientada a reducir la superficie de exposición de los equipos y evita 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. Examina las acciones que desencadenó con la herramienta de análisis forense para generar nuevas reglas de cortafuegos que limiten la comunicación entre equipos o los protejan de ataques de red.

- **Cambio de la configuración de Panda Patch Management**

Cambiar la configuración de las tareas de parcheo permite minimizar el tiempo que los programas instalados incorporan vulnerabilidades aprovechables por el malware. Ampliar el número de tipos de parches a instalar incrementa la seguridad de la red, garantizando que todo el software instalado incorpora las últimas actualizaciones publicadas por los proveedores.

Desinstalar o actualizar los programas que han entrado en EoL minimiza la superficie de ataque de los equipos: se retira el software que ya no recibe actualizaciones de los proveedores, y por lo tanto tiene una mayor probabilidad de incorporar fallos y vulnerabilidades no resueltas y aprovechables por el malware.

- **Cifrado de la información contenida en los dispositivos de almacenamiento interno de los equipos con Panda Full Encryption.**

Minimiza la exposición de la información almacenada por la empresa en equipos susceptibles de ser robados o extraviados, y evita el acceso a datos confidenciales mediante herramientas de recuperación de ficheros borrados en unidades descartadas. Adicionalmente, para evitar la utilización de los discos duros en un equipo distinto al que cifró su contenido o cambiar su secuencia de arranque es recomendable utilizar el módulo TPM incorporado en la placa base del equipo o actualizar el hardware a uno que incluya este recurso.

- **Bloqueo de programas peligrosos, no relacionados con la actividad de la empresa o con un fuerte impacto en el rendimiento del equipo, de la infraestructura de red o del propio usuario.**

Minimiza la superficie de ataque de los equipos de la red impidiendo la ejecución de programas que acceden a contenidos susceptibles de contener virus y otras amenazas de seguridad. Mejora la productividad de los usuarios, del rendimiento de la red y de los equipos administrados impidiendo la ejecución de programas que descargan grandes volúmenes de datos o consumen muchos recursos del equipo del usuario.



Parte 2

La consola web de administración

Capítulo 4: La consola de administración

Capítulo 5: Control y supervisión de la consola de administración

Capítulo 4

La consola de administración

Panda Adaptive Defense 360 utiliza las últimas tecnologías de desarrollo web para ofrecer una consola de administración alojada en la nube que permite interactuar de manera cómoda y ágil con el servicio de seguridad. Sus principales características son:

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

CONTENIDO DEL CAPÍTULO

Beneficios de la consola web	-44
Requisitos de la consola web	-45
Federación con IDP	45
Estructura general de la consola Web	-46
Menú superior (1)	46
Botón Panda Cloud	47
Menú superior Estado	47
Menú superior Equipos	47
Menú superior Configuración	47
Menú superior Tareas	47
Menú superior Filtro por grupo	47
Menú superior Configuración General	48
Menú superior Cuenta de usuario	48
Menú lateral (2)	49
Panel central (3)	49
Acceso a Advanced Visualization Tool (4)	49
Elementos básicos de la consola web	-50
Menú de pestañas superior	50
Barra de acciones	50

- Herramientas de filtrado y búsqueda 50
- Elementos de configuración 51
- Botón de ordenación 52
- Menús de contexto 53
- Copiar, pegar y borrar contenidos 53
- Esquema general de la zona Estado 54**
- Gestión de listados 56**
- Plantillas, configuraciones y vistas 56
 - Plantillas de listado 57
- Secciones de los listados 60
 - Crear un listado personalizado 61
 - Copiar un listado 62
 - Exportar un listado 63
 - Exportar los detalles de un listado 63
 - Personalizar un listado 63
 - Programar el envío de un listado 64
 - Acciones sobre equipos en los listados 64
- Listados incluidos por defecto 64
 - Estaciones y portátiles desprotegidos 64
 - Servidores desprotegidos 65
 - Software 65
 - Hardware 65

Beneficios de la consola web

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

• Única herramienta para la gestión completa de la seguridad

El administrador podrá distribuir de forma centralizada el paquete de instalación Panda Adaptive Defense 360 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 y análisis forense en caso de incidentes de seguridad. Toda la funcionalidad se ofrece desde una única consola Web, favoreciendo la integración de las distintas herramientas y minimizando la complejidad de utilizar varios productos de distintos proveedores.

• Gestión centralizada de la seguridad para oficinas remotas y usuarios desplazados

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

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

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

Requisitos de la consola web

Si tu proveedor de seguridad es Panda Security, para acceder a la consola Web de Panda Adaptive Defense 360 utiliza la siguiente URL:

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

Si tu proveedor de seguridad es WatchGuard, para acceder a la consola Web de Panda Adaptive Defense 360:

- Accede a la URL <https://www.watchguard.com/> y haz clic en el botón **Log in** situado en la esquina superior derecha de la pantalla.
- Introduce tus credenciales de WatchGuard. Se mostrará la ventana **Support Center**.
- Haz clic en el menú superior **My watchguard**. Se mostrará un menú desplegable.
- Haz clic en la opción **Manage Panda Products**. Se mostrará la ventana de Panda Cloud con todos los servicios contratados.
- Haz clic en el panel asociado a Panda Adaptive Defense 360. Se mostrará la consola de administración.

Es necesario cumplir con el siguiente listado de requisitos:

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



Para más información sobre cómo crear una Cuenta Panda de acceso a la consola Web consulta "[La cuenta Panda](#)" en la página [563](#).

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

Federación con IDP

Panda Adaptive Defense 360 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 la consola web.

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

Estructura general de la consola Web

La consola Web cuenta con recursos que facilitan una experiencia de gestión homogénea y coherente, tanto para administrar la seguridad de la red como para resolver los incidentes y realizar un análisis forense.

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

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

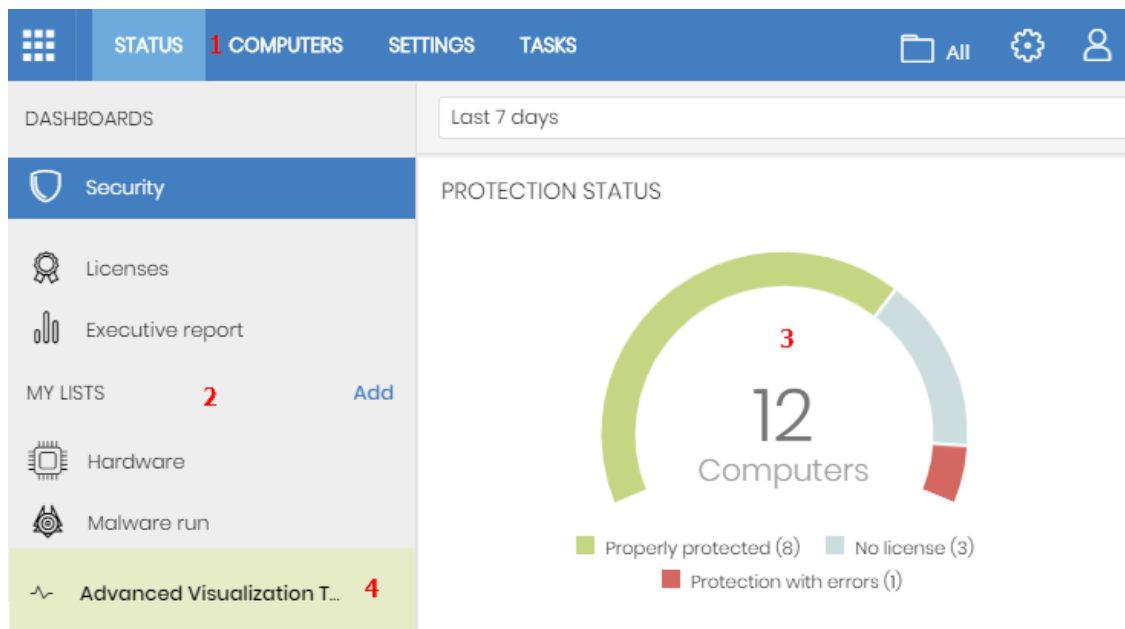


Figura 4.1: Vista general de la consola de administración Panda Adaptive Defense 360

Menú superior (1)

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

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

Botón Panda Cloud

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

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 "[Esquema general de la zona Estado](#)" en la página [54](#).

Menú superior Equipos

Ofrece las herramientas básicas para definir la estructura de los equipos de la red que mejor se ajuste a la configuración de seguridad diseñada para el parque informático. Elegir una correcta estructura de dispositivos es fundamental a la hora de asignar configuraciones de seguridad. Consulta "[La zona equipos](#)" en la página [161](#).

Menú superior Configuración

Permite al administrador de la red definir el comportamiento de Panda Adaptive Defense 360 en los equipos de usuario y servidores donde se encuentra instalado. La asignación de la configuración se establece de forma global para todos los equipos de la red, o únicamente para algunos equipos concretos mediante plantillas, dependiendo del tipo de configuración a establecer. Estas plantillas de configuración se pueden asignar a uno o más equipos de la red que tengan requerimientos de seguridad similares, permitiendo minimizar el tiempo del administrador dedicado a gestionar la seguridad de su red de equipos.



Consulta "[Gestión de configuraciones](#)" en la página [207](#) para obtener información detallada sobre cómo crear una configuración en Panda Adaptive Defense 360.

Menú superior Tareas

Permite la gestión de tareas de seguridad programadas para su ejecución en los intervalos de tiempo designados por el administrador. Consulta "[Tareas](#)" en la página [539](#).

Menú superior Filtro por grupo

Limita la información generada mostrada en la consola por los equipos que pertenezcan al grupo o grupos elegidos. Consulta "[Filtrar resultados por grupos](#)" en la página [174](#) para 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.

Entrada	Descripción
Ayuda online	Acceso a las ayudas web del producto.
Guía de administración de Panda Advanced Reporting Tool	Acceso a la guía para el administrador del módulo Panda Advanced Reporting Tool si está contratado.
Guía de administración de Panda Adaptive Defense 360	Acceso a la Guía de administración del producto Panda Adaptive Defense 360.
Guía de administración de Panda Data Control	Acceso a la guía para el administrador del módulo Panda Data Control si está contratado.
Soporte técnico	Carga la dirección web correspondiente al soporte técnico de Panda Adaptive Defense 360.
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).
Acuerdo sobre tratamiento de datos	Muestra el acuerdo de protección de datos de la plataforma según la normativa europea.
Novedades de Panda Adaptive Defense 360	Enlace a la página web de soporte que muestra los cambios y nuevas funcionalidades incluidas en la versión.
Idioma	Permite seleccionar el idioma en que se mostrará la consola de administración.
Acerca de...	Muestra la versión de los diferentes elementos de Panda Adaptive Defense 360. • Versión: versión del producto. • Versión de la protección: versión interna del módulo de protección instalado en los equipos. • Versión del agente: versión interna del módulo de comunicaciones instalado en los equipos.

Tabla 4.1: Menú Configuración general

Menú superior Cuenta de usuario

Muestra un menú desplegable con las siguientes entradas de configuración:

Entrada	Descripción
Cuenta	Nombre de la cuenta con la que se accedido a la consola.

Tabla 4.2: Menú Cuenta de usuario

Entrada	Descripción
Id de cliente	El identificador de cliente es el número con el que Panda identifica al cliente, se envía en el mail de bienvenida y se pide en las comunicaciones con soporte.
Dirección de correo	Dirección de correo utilizada para acceder a la consola.
Configurar mi perfil	Modifica la información de la cuenta principal del producto. Los usuarios que acceden a la consola de Panda Adaptive Defense 360 desde WGPortal no verán esta opción ya que la configuración de la cuenta se realizará desde la web de WatchGuard.
Cambiar de cuenta	Lista las cuentas accesibles por el administrador y permite seleccionar una para operar con la consola.
Cerrar sesión	Hace logout de la consola y devuelve el control a la pantalla de IdP.

Tabla 4.2: Menú Cuenta de usuario

Menú lateral (2)

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

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

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

tamaño original haz clic en el icono .

Panel central (3)

Recoge toda la información relevante de la zona y subzona elegidas por el administrador. En la figura [4.1](#) se muestra la zona **Estado** subzona **Seguridad**, formada por los widgets que permiten interpretar la información de seguridad recogida. Para obtener más detalle acerca de los widgets consulta "[Paneles / Widgets del módulo de seguridad](#)" en la página [412](#).

Acceso a Advanced Visualization Tool (4)

Data Control es el punto de entrada para la consola de gestión de los módulos Panda Data Control y Panda Advanced Reporting Tool. Ambos comparten una consola especialmente diseñada para mostrar gráficas avanzadas y tablas con información relevante sobre la actividad de los todos procesos ejecutados en los puestos de usuario y servidores.

Elementos básicos de la consola web

Menú de pestañas superior

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

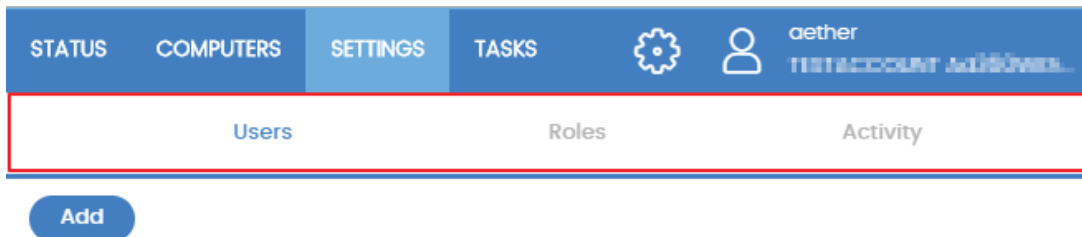


Figura 4.2: Menú de pestañas

Barra de acciones



Figura 4.3: Barra de acciones

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

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

Herramientas de filtrado y búsqueda

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

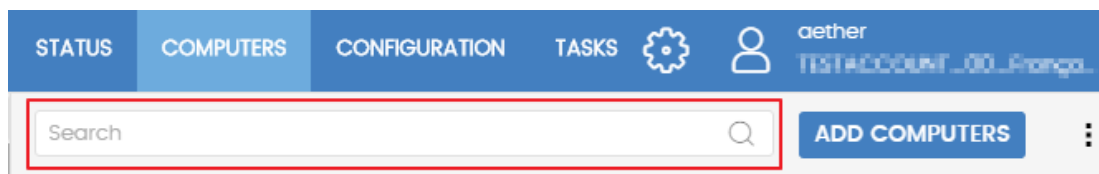


Figura 4.4: Herramienta de búsqueda

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

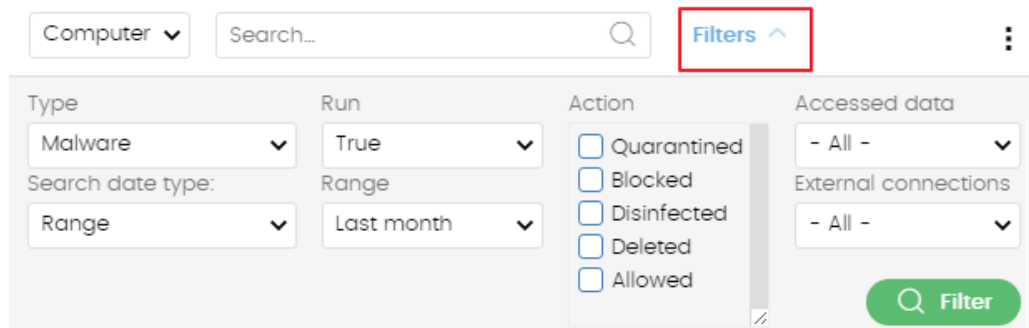


Figura 4.5: Sistema de filtrado de información en listados

Elementos de configuración

La consola web Panda Adaptive Defense 360 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)

Cancel

Edit settings 1

Save

Name:

WorkstationAndServer Settings

Description:

My Description

Recipients:

No recipients selected yet 2

Advanced protection (Windows computers)

Advanced protection

 3

Behavior

Operational mode

Lock 4

Audit

Hardening

Lock

Always enabled 5

Enable only during the following times:

Extensions:

Add extension 6

Figura 4.6: Controles para el manejo de la consola de administración

Botón de ordenación

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

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

Menús de contexto

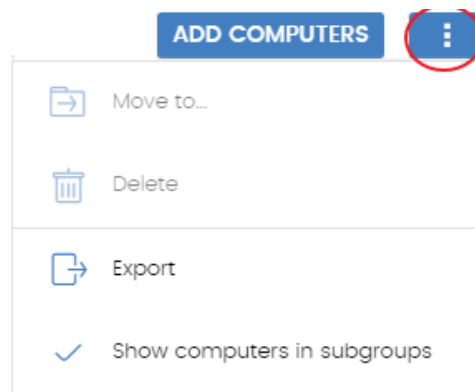


Figura 4.7: Menús de contexto

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

Copiar, pegar y borrar contenidos

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

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

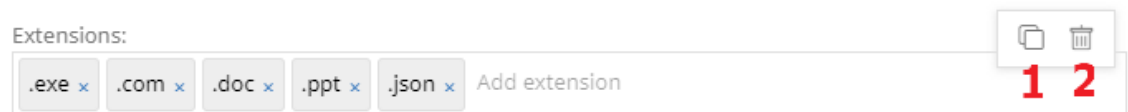


Figura 4.8: Botones Pegar y Borrar

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

Esquema general de la zona Estado

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

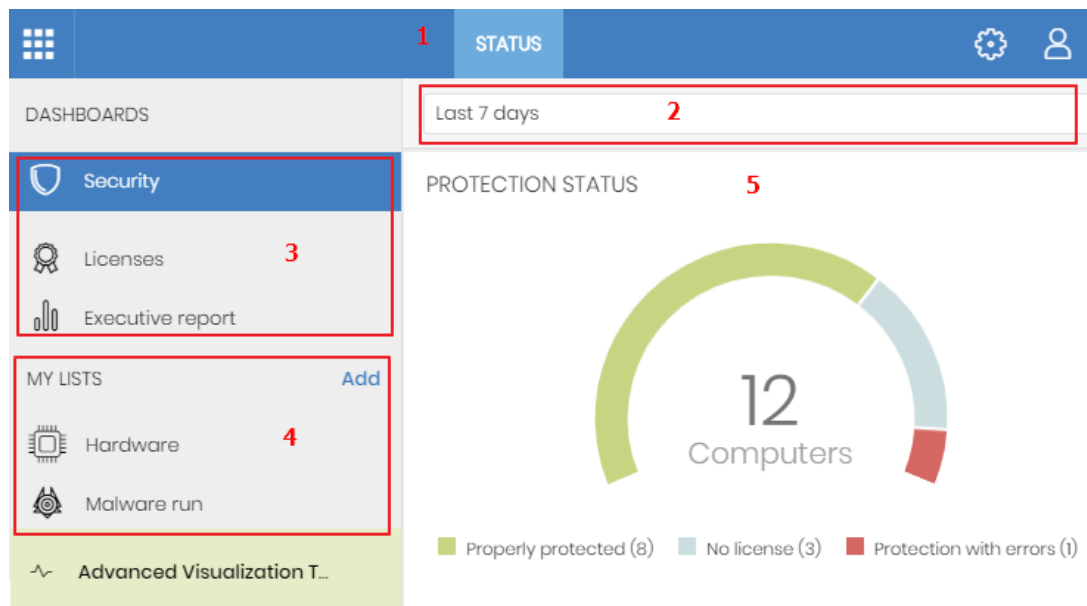


Figura 4.9: Ventana de Estado con el panel de control y acceso a los listados

• Acceso al panel de control (1)

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

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

• Selector del intervalo de tiempo (2)

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

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



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

- **Selector de panel (3)**

- **Seguridad:** estado de la seguridad del parque informático. Para más información sobre los widgets incluidos consulta "[Paneles / Widgets del módulo de seguridad](#)" en la página [412](#).
- **Accesos web y spam:** filtrado de la navegación y del correo no solicitado en servidores Microsoft Exchange. Para más información sobre los widgets incluidos consulta "[Paneles / Widgets del módulo de seguridad](#)" en la página [412](#).
- **Patch Management:** actualización del sistema operativo y del software instalado en los equipos. Para más información sobre los widgets incluidos consulta "[Paneles / Widgets del módulo de seguridad](#)" en la página [412](#).
- **Data Control:** seguimiento de la información personal almacenada en los equipos de la red. Para más información sobre los widgets incluidos consulta "[Introducción al funcionamiento de Panda Data Control](#)" en la página [272](#).
- **Panda Full Encryption:** estado del cifrado de los dispositivos de almacenamiento internos en los equipos. Para más información sobre los widgets incluidos consulta "[Paneles / Widgets del módulo de seguridad](#)" en la página [412](#).
- **Licencias:** estado de las licencias de Panda Adaptive Defense 360 asignadas a los equipos de la red. Consulta "[Licencias](#)" para obtener más información acerca de la gestión de licencias.
- **Informes programados:** consulta "[Envío programado de informes y listados](#)" en la página [513](#) para obtener más información acerca de la configuración y generación de informes.

- **Mis listados (4)**

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

- **Paneles informativos / Widgets (5)**

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

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

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

Panda Adaptive Defense 360 utiliza varios tipos de gráficas para mostrar la información de la forma más conveniente según el tipo de dato representado:

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

Gestión de listados

Panda Adaptive Defense 360 estructura la información recogida en dos niveles: un primer nivel que representa de forma gráfica los datos mediante paneles o widgets y un segundo nivel más detallado, donde la información se representa mediante listados compuestos por tablas. La mayor parte de los paneles tienen un listado asociado para que el administrador pueda acceder de forma rápida a un resumen gráfico de la información y después profundizar mediante los listados en caso de requerir mayor nivel de detalle.

Panda Adaptive Defense 360 soporta el envío programado de listados por correo electrónico. De esta forma, el administrador no necesita acceder a la consola Web para conocer el detalle de los eventos que se producen en la red. Además, esta funcionalidad facilita la compartición de información entre departamentos y permite habilitar la construcción de un repositorio externo con el histórico de todos los eventos que se han producido, mas allá de los límites de la consola Web. Con este repositorio, el equipo directivo podrá realizar un seguimiento de la información generada libre de interferencias de terceros.

Plantillas, configuraciones y vistas



Figura 4.10: Generación de tres listados a partir de una misma plantilla / fuente de datos

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

Una plantilla representa una fuente de datos sobre un apartado específico tratado por Panda Adaptive Defense 360.

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

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

Plantillas de listado

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

Grupo	Listado	Descripción
General	Licencias	Muestra en detalle el estado de las licencias de los equipos de la red. Consulta " Listados del módulo Licencias " en la página 147 .
	Equipos no administrados descubiertos	Muestra los equipos Windows de la red que no tienen el software Panda Adaptive Defense 360 instalado. Consulta " Visualizar equipos descubiertos " en la página 120 .
	Equipos con nombre duplicado	Muestra los equipos con el mismo nombre y pertenecen al mismo dominio. Consulta " Equipos con nombre duplicado " en la página 186 .
	Software	Muestra el software instalado en los equipos del parque informático. Consulta " Software " en la página 184 .
	Hardware	Muestra el hardware instalado en los equipos del parque informático. Consulta " Hardware " en la página 182 .
Seguridad	Estado de protección de los equipos	Muestra en detalle el estado del módulo de la protección instalada en los equipos. Consulta " Estado de protección de los equipos " en la página 429 .
	Actividad del malware y PUPS	Muestra el listado de las amenazas encontradas en los equipos protegidos con Panda Adaptive Defense 360. Consulta " Actividad de malware / PUP " en la página 433 .
	Actividad de exploits	Muestra el número de ataques por explotación de vulnerabilidades recibidos en los equipos Windows de la red. Consulta " Actividad de exploits " en la página 436 .
	Programas actualmente bloqueados en clasificación	Muestra una tabla con aquellos ficheros que, sin haber sido completada su clasificación, Panda Adaptive Defense 360 ha detectado de forma preliminar algún riesgo en su ejecución. Consulta " Actividad de malware / PUP " en la página 433 .

Tabla 4.3: Listado de plantillas disponibles en Panda Adaptive Defense 360

Grupo	Listado	Descripción
	Amenazas detectadas por el antivirus	Ofrece información consolidada y completa de todas las detecciones realizadas en todas las plataformas soportadas y desde todos los vectores de infección analizados. Consulta " Amenazas detectadas por el antivirus " en la página 439 .
	Intentos de intrusión bloqueados	Muestra los ataques de red bloqueados por el cortafuegos del equipo. Consulta " Intentos de intrusión bloqueados " en la página 446 .
	Dispositivos bloqueados	Muestra en detalle todos los equipos de la red que tienen establecida alguna limitación en el acceso a sus periféricos. Consulta " Dispositivos bloqueados " en la página 443 .
	Conexiones bloqueadas	Muestra las conexiones que fueron bloqueadas por el cortafuegos local. Consulta " Intentos de intrusión bloqueados " en la página 446 .
Patch Management	Estado de gestión de parches	Muestra en detalle todos los equipos de la red compatibles con Panda Patch Management Consulta " Estado de gestión de parches " en la página 348 .
	Parches disponibles	Muestra el detalle de todos los parches sin instalar en los equipos de la red y publicados por Panda Security. Consulta " Parches disponibles " en la página 346 .
	Historial de instalaciones	Muestra los parches que Panda Adaptive Defense 360 intentó instalar y los equipos que los recibieron en un intervalo determinado. Consulta " Historial de instalaciones " en la página 359 .
	Programas "End of Life"	Muestra la información relativa al "end of life" de los programas instalados en los equipos de la red, agrupados según el plazo restante. Consulta " Programas "End of Life" " en la página 358 .
	Parches excluidos	Muestra los pares equipo - parche que son excluidos de su instalación. Consulta " Parches excluidos " en la página 364 .
Control de actividad	Accesos a páginas web por categoría	Muestra las visitas de los usuarios de la red a las páginas web agrupadas por su categoría. Consulta " Categorías más accedidas (top 10) " en la página 425 .
	Accesos a páginas web por equipo	Muestra las visitas de los usuarios de la red a las páginas web agrupadas por dispositivo. Consulta " Categorías más accedidas por equipo (top 10) " en la página 426 .

Tabla 4.3: Listado de plantillas disponibles en Panda Adaptive Defense 360

Grupo	Listado	Descripción
	Programas bloqueados por el administrador	Muestra los intentos de ejecución de programas bloqueados por el administrador en los equipos de la red. Consulta " Listados del módulo Bloqueo de programas " en la página 399 .
Protección de datos	Estado del cifrado	Muestra toda la información referente a los equipos de la red compatibles con la funcionalidad de cifrado. Consulta " Estado del cifrado " en la página 389 .
	Estado de Data Control	Muestra el estado del módulo Panda Data Control de Panda Adaptive Defense 360. Consulta " Estado de Data Control " en la página 306 .
	Archivos con información personal	Muestra todos los ficheros PII encontrados, así como su tipo, localización y otra información relevante. Consulta " Archivos con información personal " en la página 311 .
	Equipos con información personal	Muestra el número de ficheros PII encontrados en cada uno de los equipos de la red. Consulta " Equipos con información personal " en la página 314 .
	Archivos eliminados por el administrador	Muestra el estado de los ficheros eliminados por el administrador mediante el módulo Panda Data Control. Consulta " Archivos eliminados por el administrador " en la página 318 .

Tabla 4.3: Listado de plantillas disponibles en Panda Adaptive Defense 360

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

Secciones de los listados

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

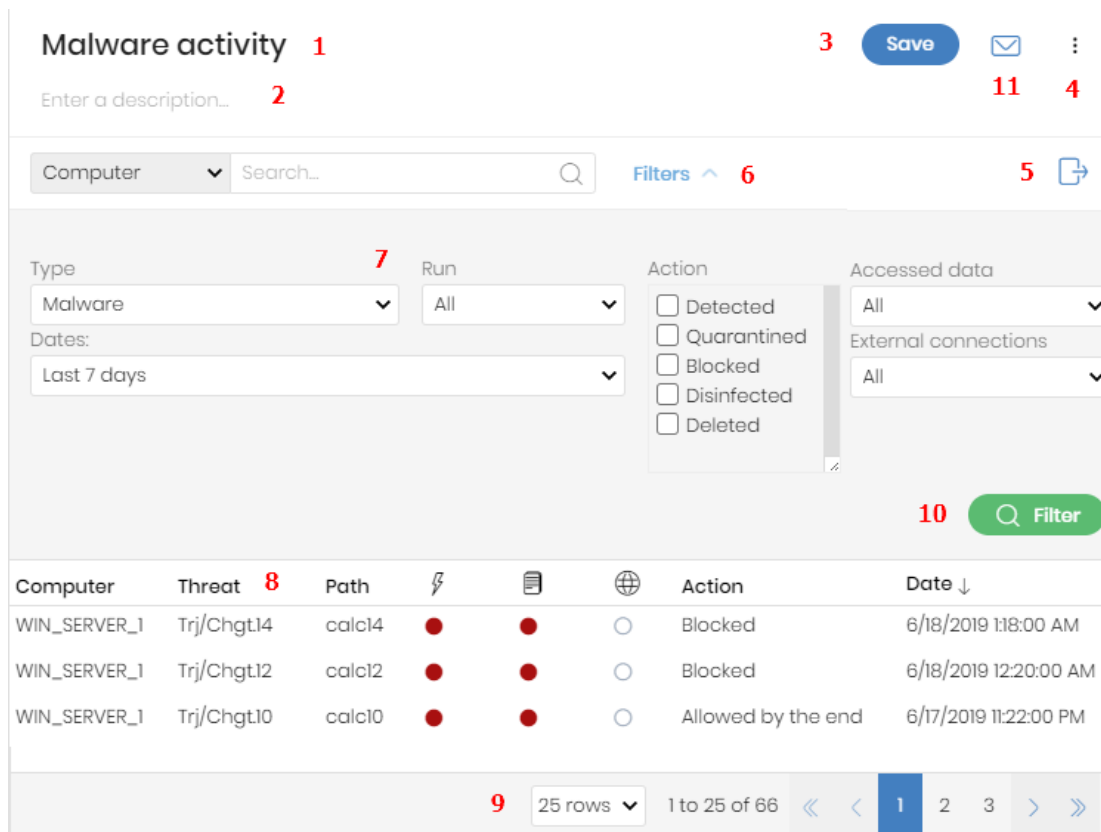


Figura 4.11: Elementos de las pantallas de listados

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

derecha para desplegar un menú con el nombre de las columnas.

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

Icono	Descripción
	Selector del número de filas mostradas por página.
	Intervalo de registros mostrados del total disponible.
	Retroceso a la primera página.
	Retroceso a la página anterior a la actual.
	Acceso directo por número de páginas.
	Avance a la siguiente página.
	Avance a la última página.

Tabla 4.4: Herramientas de paginación

- **Envío programado del listado (11):** Panda Adaptive Defense 360 permite el envío de correos electrónicos con el contenido del listado, adjuntando una exportación de los datos en formato csv. Consulta "[Envío programado de informes y listados](#)" en la página [513](#) para obtener más información.

Operaciones con listados

En el menú superior **Estado**, panel lateral **Mis listados** se muestran todos los listados que el administrador a creado previamente y los listados que Panda Adaptive Defense 360 incorpora por defecto. Consulta "[Listados incluidos por defecto](#)".

Crear un listado personalizado

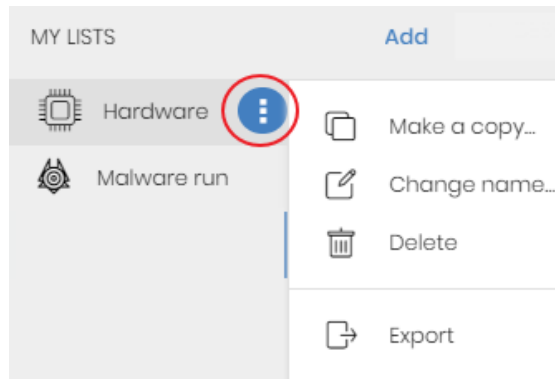
Hay varias formas de añadir un nuevo listado personalizado / vista:

- **Desde el panel lateral Mis listados**
 - Al hacer clic sobre el link **Añadir** del panel **Mis listados** se muestra una ventana con un desplegable que contiene las plantillas disponibles.
 - Elige una plantilla, configura las herramientas de filtrado, modifica el nombre y la descripción y pulsa el botón **Guardar (3)**.
- **Desde un panel del dashboard**
 - Haz clic en un widget en el panel de control para abrir su plantilla asociada.
 - Haz clic en el menú de contexto **(4)** y selecciona **Copiar**. Se creará un nuevo listado.
 - Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.

- **Desde un listado ya creado**

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

- **Desde el menú de contexto del panel Mis listados**



- Haz clic en el menú de contexto asociado al listado a copiar.

- Haz clic en **Hacer una copia**. Se creará una nueva vista de la plantilla con el nombre "copia de...".

- Modifica los filtros, el nombre y la descripción del listado y haz clic en el botón **Guardar (3)**.

Figura 4.12: Menú de contexto de los listados accesibles desde el Panel de listados

Borrar un listado

Puedes borrar un listado de varias maneras:

- **Desde el panel Mis listados**

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

- **Desde el propio listado**

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

Copiar un listado

Puedes copiar un listado de varias maneras:

- Desde el panel **Mis listados**:

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

- Desde el propio listado:

- Haz clic en el menú de contexto **(4)**.
- Haz clic en el icono  del menú desplegado.

Exportar un listado

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

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

Exportar los detalles de un listado

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

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

Personalizar un listado

- Asigna un nuevo nombre al listado **(1)**. Por defecto la consola forma un nuevo nombre para el listado añadiendo la cadena "Nuevo" al tipo de listado o "Copia" si el listado es la copia de uno anterior.
- Asigna una descripción **(2)**: este paso es opcional.
- Haz clic en el enlace **Filtros (6)** para desplegar las herramientas de búsqueda y filtrado.
- Haz clic en **Filtrar (10)** para aplicar el filtro configurado con el objetivo de comprobar si el filtrado configurado se ajusta a las necesidades. En el cuerpo del listado se mostrará la búsqueda

resultado.

- Haz clic en el botón **Guardar (3)**. El listado se añadirá en el panel de la izquierda bajo **Mis listados**, y será accesible a partir de ese momento haciendo clic en su nombre.

Programar el envío de un listado

- Desde el menú de contexto del panel **Listados**:
 - Haz clic en el menú de contexto del listado que quieres enviar y elige la opción **Programar envío**.
 - Se mostrará una ventana con la información necesaria para enviar de forma automática la información.
- Desde el propio listado:
 - Haz clic en el icono **(11)** . Se mostrará una ventana con la información necesaria para enviar de forma automática la información.



Consulta "**Envío programado de informes y listados**" en la página **513** para obtener más información

Acciones sobre equipos en los listados

En algunos listados como **Licencias** y **Estado de protección de los equipos** se incorporan casillas de selección por cada equipo. Al marcar uno o más equipos, se muestra la barra de acciones en la parte superior de la ventana, para facilitar la administración de los puestos de usuario y servidores seleccionados.

Listados incluidos por defecto

La consola de administración incluye varios listados pre generados:

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

Estaciones y portátiles desprotegidos

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

- Equipos en proceso de instalación del software Panda Adaptive Defense 360 o con error en la instalación.
- Equipos con la protección desactivada o en estado de error.

- Equipos sin licencia asignada o con licencia caducada.
- Consulta "[Estado de protección de los equipos](#)" en la página [429](#).

Servidores desprotegidos

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

- Servidores en proceso de instalación del software Panda Adaptive Defense 360 o con error en la instalación.
- Servidores con la protección desactivada o en estado de error.
- Servidores sin licencia asignada o con licencia caducada. Consulta "[Estado de protección de los equipos](#)" en la página [429](#).

Software

Muestra una relación de los programas instalados en el parque informático. Consulta "[Software](#)" en la página [184](#).

Hardware

Muestra una relación de los componentes hardware instalados en el parque informático. Consulta "[Hardware](#)" en la página [182](#).

Capítulo 5

Control y supervisión de la consola de administración

Panda Adaptive Defense implementa recursos 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:

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

CONTENIDO DEL CAPÍTULO

Concepto de cuenta de usuario	-68
Estructura de una cuenta de usuario	68
Verificación en dos pasos	69
Requisitos para activar 2FA	69
Activar 2FA	69
Acceder a la consola mediante una cuenta con 2FA activado	69
Forzar la activación de 2FA a todos los usuarios de la consola	70
Concepto de rol	-70
Estructura de un rol	70
¿Por qué son necesarios los roles?	70
El rol Control total	71
El rol Solo lectura	71
Concepto de permiso	-72
Descripción de los permisos implementados	72
Gestionar usuarios y roles	72
Asignar licencias	72
Modificar el árbol de equipos	72
Añadir, descubrir y eliminar equipos	73
Modificar configuración de red (proxys y caché)	73
Configurar ajustes por equipo (actualizaciones, contraseñas, etc.)	73
Reiniciar y reparar equipos	73
Aislar equipos	74
Configurar seguridad para estaciones y servidores	74
Ver configuraciones de seguridad para estaciones y servidores	74
Configurar seguridad para dispositivos Android	74
Ver configuraciones de seguridad para dispositivos Android	74
Utilizar la protección antirrobo para dispositivos Android localizar, borrar, bloquear, etc.	75

Visualizar detecciones y amenazas	75
Visualizar accesos a páginas web y spam	75
Lanzar análisis y desinfectar	75
Excluir temporalmente amenazas Malware, PUP y Bloqueados	75
Configurar gestión de parches	76
Visualizar configuraciones de gestión de parches.....	76
Instalar / desinstalar y excluir parches.....	76
Visualizar parches disponibles	76
Configurar bloqueo de programas	77
Ver configuraciones de bloqueo de programas	77
Configurar software autorizado	77
Ver configuración de software autorizado	77
Configurar Data Control	77
Ver configuraciones de Data Control.....	78
Buscar información en los equipos.....	78
Visualizar inventario de información personal	78
Eliminar y restaurar archivos	78
Configurar cifrado de equipos	78
Ver configuraciones de cifrado de equipos	79
Acceder a las claves de recuperación de unidades cifradas.....	79
Acceder a información avanzada de seguridad	79
Acceder a información de acceso a archivos	79
Acceder a información avanzada de Data Control.....	79
Acceso a la configuración de cuentas de usuarios y roles - - - - -	80
Crear y configurar cuentas de usuario - - - - -	80
Crear, modificar y borrar usuarios	80
Listar los usuarios creados.....	80
Crear y configurar roles	81
Limitaciones en la creación de usuarios y roles	81
Registro de la actividad de las cuentas de usuario- - - - -	82
Registro de sesiones	82
Registro de acciones de usuario	83
Eventos del sistema	100

Concepto de cuenta de usuario

Es un recurso gestionado por Panda Adaptive Defense 360, 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 web de Panda Adaptive Defense 360. Cada administrador de IT tiene una o mas cuentas de usuario personales.



Como norma general, la palabra “usuario” se refiere a la persona que utiliza un equipo o dispositivo. Aquí, sin embargo, se asocia a la cuenta de usuario que el administrador utiliza para acceder a la consola web.

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, regula el acceso a la consola de administración.
- **Rol asignado:** asignado una vez creada la cuenta de usuario, establece los equipos sobre los cuales la cuenta tiene capacidad de administración, y las acciones que puede ejecutar sobre los mismos.

Verificación en dos pasos

Panda Adaptive Defense 360 soporta el estándar 2FA (Two Factor Authentication) para añadir una capa de seguridad adicional a la establecida en el esquema básico "usuario - contraseña". De esta manera, cuando el administrador de la red accede a la consola web se introduce un nuevo elemento en el sistema de autenticación básico: un código que solo posee el propietario de la cuenta. Este código es aleatorio y únicamente puede generarse en un dispositivo concreto, normalmente el teléfono móvil o tablet personal del administrador del Panda Adaptive Defense 360.

Requisitos para activar 2FA

- Acceso a un teléfono móvil o tablet personal con cámara de fotos integrada.
- Aplicación Google Authenticator instalada, o una equivalente. Descarga la aplicación gratuita en el enlace <https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl>

Activar 2FA

- En el menú superior haz clic en la cuenta de usuario y en la opción **Configurar mi perfil**. Se abrirá la ventana de la **Cuenta Panda**.



Figura 5.1: Acceso a la Cuenta Panda

- Haz clic en el menú lateral **Inicio de sesión** y en el enlace **Activar** de la sección **Verificación en dos pasos**. Se mostrará la ventana de configuración de la aplicación Google Authenticator o equivalente instalada en el dispositivo móvil.
- Escanea el código QR mostrado en la ventana con la aplicación Google Authenticator o equivalente, introduce el código generado en el apartado **Introduce el código que te muestra la app** y haz clic en el botón **Verificar**. Desde este momento el dispositivo quedará enlazado al servicio Panda Adaptive Defense 360 y generará códigos de acceso aleatorios que caducarán cada poco tiempo.

Acceder a la consola mediante una cuenta con 2FA activado

Para acceder a la consola con una cuenta de usuario que tiene la funcionalidad 2FA activada introduce el usuario, contraseña y un código generado por el dispositivo vinculado a la cuenta.

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

Para forzar la activación de 2FA a todos los usuarios de la consola es necesario que la cuenta de usuario que forzará la activación tenga permisos de **Gestionar usuarios y roles** y que además tenga visibilidad completa sobre el parque. Consulta [“Gestionar usuarios y roles”](#) para una descripción de este permiso, y [“Estructura de un rol”](#) para configurar los grupos sobre los que tiene permisos el rol.

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

Concepto de 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 está autorizado a ver o modificar determinados recursos de la consola, dependiendo del rol asignado a la cuenta de usuario con la que accedió a Panda Adaptive Defense 360.

Una cuenta de usuario tiene un único rol asignado aunque un rol puede estar asignado a una o más cuentas de usuario.

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:** restringe 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 tiene acceso.
- **Juego de permisos:** determina las acciones concretas que las cuentas de usuario pueden ejecutar sobre los equipos que pertenecen a los grupos definidos con accesibles.

¿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 medianos o grandes con un parque informático amplio 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 administran 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 o servicio se puede asignar a un técnico experto en ese campo: por ejemplo, los servidores de correo Exchange se asignan a un grupo de técnicos especialistas, y de la misma forma, otros equipos como los dispositivos Android no serán visibles para este grupo.

- **Según los conocimientos o perfil del técnico.**

Según las capacidades del técnico o de su función dentro del departamento de IT, se puede asignar 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 permite delimitar perfectamente las funciones de la consola para cada técnico, en función de la cuenta de usuario con la que acceden al sistema.

El rol Control total

Una licencia de uso de Panda Adaptive Defense 360 incluye un rol de **Control total** predefinido. A este rol pertenece la cuenta de administración creada por defecto, y con ella es posible ejecutar todas las acciones disponibles en la consola sobre todos los equipos integrados en Panda Adaptive Defense 360.

El rol **Control total** no se puede borrar, modificar ni acceder a sus detalles. Cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola Web.

El rol Solo lectura

Este rol permite el acceso a todos los componentes de la consola, pero no permite crear, modificar o borrar configuraciones, tareas, etc. por lo que permite una visión total del entorno, pero sin ninguna interacción. 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.

El rol **Solo lectura** no se puede borrar, modificar ni acceder a sus detalles. Cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola Web.

Concepto de permiso

Un permiso regula el acceso a un aspecto concreto de la consola de administración. Existen varios permisos que establecen el acceso a otros tantos aspectos de la consola de Panda Adaptive Defense 360. Una configuración particular de todos los permisos disponibles forma un rol, que puede ser asignado a una o más cuentas de usuario.

Descripción de los permisos implementados

Gestionar usuarios y roles

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

Asignar licencias

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

Modificar el árbol de equipos

- **Al activar:** el usuario de la cuenta tiene pleno acceso al árbol de grupos y puede crear y eliminar grupos, y mover equipos a grupos ya creados.
- **Al activar con conflicto de permisos:** debido a los mecanismos de herencia que rigen el árbol de equipos, cualquier modificación en el mismo puede implicar un cambio de configuración para los dispositivos (consulta el apartado "[Asignación manual y automática de configuraciones](#)" en la página 215). Si alguno de los permisos que habilitan al administrador la asignación o cambio de configuraciones están desactivados, la consola web mostrará una advertencia indicando que, aunque el administrador no tiene permisos para cambiar configuraciones, éstas podrían hacerlo si se permite el movimiento de equipos en el árbol de equipos. Los permisos que permiten cambiar configuraciones son:
 - Modificar configuración de red (proxys y caché).
 - Modificar ajustes por equipo actualizaciones, contraseñas, etc.

- Configurar seguridad para estaciones y servidores.
- Configurar seguridad para dispositivos Android.
- Lanzar análisis y desinfectar.
- Configurar gestión de parches.
- Instalar y desinstalar parches.
- Configurar inventario, seguimiento y búsqueda de información sensible.
- **Al desactivar:** el usuario de la cuenta puede visualizar el árbol de carpetas y las configuraciones asignadas a cada grupo, pero no puede crear nuevos grupos ni mover equipos.

Añadir, descubrir y eliminar equipos

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

Modificar configuración de red (proxys y caché)

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

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

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

Reiniciar y reparar equipos

- **Al activar:** el usuario de la cuenta puede reiniciar equipos desde los listados de equipos en estaciones y servidores. También puede iniciar la reinstalación remota del software Panda Adaptive Defense 360 en equipos Windows.
- **Al desactivar:** el usuario de la cuenta deja de poder reiniciar equipos y de reinstalar remotamente el software Panda Adaptive Defense 360.

Aislar equipos

- **Al activar:** el usuario de la cuenta puede aislar y dejar de aislar equipos desde el menú superior **Equipos** y desde los listados **Licencias** y **Equipos protegidos** seleccionando en el menú de contexto o en barra de acciones **Aislar equipos**, para estaciones y servidores Windows.
- **Al desactivar:** el usuario de la cuenta deja de poder aislar equipos.

Configurar seguridad para estaciones y servidores

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

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

Ver configuraciones de seguridad para estaciones y servidores



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

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

Configurar seguridad para dispositivos Android

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

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 puede 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 deja de poder ver las configuraciones de dispositivos Android creadas, y tampoco podrá acceder a las configuraciones asignadas de cada dispositivo Android.

Utilizar la protección antirrobo para dispositivos Android localizar, borrar, bloquear, etc.

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

Visualizar detecciones y amenazas

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



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

Visualizar accesos a páginas web y spam

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

Excluir temporalmente amenazas Malware, PUP y Bloqueados

- **Al activar:** el usuario de la cuenta puede desbloquear, no volver a detectar, bloquear, dejar de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos en clasificación.
- **Al desactivar:** el usuario de la cuenta no podrá desbloquear, no volver a detectar, bloquear, dejar

de permitir y cambiar el comportamiento ante reclasificaciones de malware, PUP y desconocidos en clasificación.



Es necesario activar Visualizar detecciones y amenazas para poder ejercer completamente Excluir temporalmente amenazas Malware, PUP y Bloqueados.

Configurar gestión de parches

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

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

Visualizar configuraciones de gestión de parches



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

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

Instalar / desinstalar y excluir parches

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

Visualizar parches disponibles



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

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

Programas “End of life” e Historial de instalaciones.

Configurar bloqueo de programas

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

Al desactivar este permiso se mostrará el permiso **Ver configuraciones de bloqueo de programas**.

Ver configuraciones de bloqueo de programas



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar bloqueo de programas.

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

Configurar software autorizado

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

Al desactivar este permiso se mostrará el permiso **Ver configuración de software autorizado**.

Ver configuración de software autorizado



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar software autorizado.

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

Configurar Data Control

- **Al activar:** el usuario de la cuenta podrá crear, editar, borrar y asignar configuraciones de Panda

Data Control en equipos Windows.

- **Al desactivar:** el usuario de la cuenta dejará de poder crear, editar, borrar y asignar configuraciones de Panda Data Control en equipos Windows.

Ver configuraciones de Data Control



Este permiso solo es accesible cuando se ha deshabilitado el permiso Configurar inventario, seguimiento y búsqueda de información sensible.

- **Al activar:** el usuario de la cuenta podrá únicamente visualizar las configuraciones de Data Control, 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 Data Control creadas, y tampoco podrá acceder a las configuraciones asignadas de cada equipo.

Buscar información en los equipos

- **Al activar:** el usuario de la cuenta podrá acceder al widget de **Búsquedas** para localizar ficheros por nombre y contenido almacenados en los equipos de los usuarios.
- **Al desactivar:** el usuario de la cuenta dejará de poder acceder al widget Búsquedas.

Visualizar inventario de información personal

- **Al activar:** el usuario de la cuenta podrá acceder a los listados **Archivos con información personal** y **Equipos con información personal**, así como a los widgets **Archivos con información personal**, **Equipos con información personal** y **Archivos por tipo de información personal**.
- **Al desactivar:** el usuario de la cuenta dejará de tener acceso a los listados **Archivos con información personal** y **Equipos con información personal**, así como a los widgets **Archivos con información personal**, **Equipos con información personal** y **Archivos por tipo de información personal**.

Eliminar y restaurar archivos

- **Al activar:** el usuario de la cuenta puede acceder a la opción **Eliminar** del menú de contexto en el listado **Archivos con información personal** para borrar y restaurar ficheros.
- **Al desactivar:** el usuario de la cuenta no puede acceder a la opción **Eliminar** del menú de contexto en el listado **Archivos con información personal** y por lo tanto no puede borrar ni restaurar ficheros.

Configurar cifrado de equipos

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

configuraciones de cifrado para equipos Windows.

Ver configuraciones de cifrado de equipos



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

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

Acceder a las claves de recuperación de unidades cifradas

- **Al activar:** el usuario de la cuenta podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados y administrados por Panda Adaptive Defense 360.
- **Al desactivar:** el usuario de la cuenta no podrá visualizar las claves de recuperación para los equipos con dispositivos de almacenamiento cifrados.

Acceder a información avanzada de seguridad

- **Al activar:** el usuario de la cuenta podrá acceder a la herramienta Advanced Visualization Tool desde el menú superior **Estado**, panel izquierdo Advanced Visualization Tool pero la aplicación Data Access Control no es visible con este permiso.
- **Al desactivar:** se impide el acceso a la herramienta Advanced Visualization Tool.

Acceder a información de acceso a archivos

- **Al activar:** el usuario de la cuenta podrá acceder a la herramienta Advanced Visualization Tool desde el menú superior **Estado**, panel izquierdo **Advanced Visualization Tool**. La aplicación Data Access Control es accesible con este permiso.
- **Al desactivar:** se impide el acceso a la herramienta Advanced Visualization Tool.

Acceder a información avanzada de Data Control

- **Al activar:** el usuario de la cuenta podrá acceder a la consola extendida de Data Control desde el menú superior **Estado**, panel izquierdo **Advanced Visualization Tool**.
- **Al desactivar:** el usuario de la cuenta no podrá acceder a la consola extendida de Data Control desde el menú superior **Estado**, panel izquierdo **Advanced Visualization Tool**.

Acceso a la configuración de cuentas de usuarios y roles

En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**. Aparecerán dos entradas asociadas a la gestión de roles y cuentas de usuario:

- **Usuarios:** crea nuevas cuentas de usuario y definir su pertenencia a uno o varios roles.
- **Roles:** crea y modifica una nueva configuración de acceso a los recursos de Panda Adaptive Defense 360.

Solo se puede acceder a las pestañas de **Usuarios y roles** si el usuario tiene asignado el permiso **Gestionar usuarios y roles**.

Crear y configurar cuentas de usuario

Crear, modificar y borrar usuarios

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Usuarios** desde donde puedes 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 pertenece y una descripción de la cuenta. Al terminar 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 inhabilitar temporalmente el acceso de la cuenta a la consola web. De esta manera, esa cuenta tendrá denegado el acceso a la consola de administración, y si ya está conectado será expulsada de forma inmediata. También dejará de recibir alertas por correo en las direcciones de correo especificadas en su configuración.

Listar los usuarios creados

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará un listado con todas las cuentas de usuario creadas en

Panda Adaptive Defense 360 con la información mostrada a continuación:

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

Tabla 5.1: Listado de usuarios

Crear y configurar roles

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Roles** para realizar todas las acciones necesarias relativas a la creación y modificación de roles:
 - **Añadir nuevo rol:** haz clic en el botón **Añadir** e introduce 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 mostrar 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 cancela el proceso de borrado.

Limitaciones en la creación de usuarios y roles

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

- Una cuenta de usuario solo puede crear nuevos roles con los mismos permisos o menos de los que tiene asignada.
- Una cuenta de usuario sólo puede editar los permisos que tenga activos en los roles ya existentes. El resto permanecerán desactivados.
- Una cuenta de usuario no puede asignar un rol a un usuario si ese rol tiene más permisos asignados que la cuenta de usuario.
- Una cuenta de usuario no puede copiar un rol si ese rol tiene más permisos asignados que la cuenta

de usuario.

Registro de la actividad de las cuentas de usuario

Panda Adaptive Defense 360 registra todas las acciones efectuadas por los administradores de red en la consola web de gestión para determinar quién realizó un cambio, en que momento y sobre qué objeto.

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

Registro de sesiones

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

- **Campos mostrados en el listado de sesiones**

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

Tabla 5.2: Campos del listado sesiones

- **Campos mostrados en el fichero exportado**

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

Tabla 5.3: Campos del fichero exportado sesiones

- **Herramienta de búsqueda**

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

Tabla 5.4: Campos de filtrado para el listado de sesiones

Registro de acciones de usuario

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

- **Campos mostrados en el listado de acciones**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que ha producido la acción.	Fecha
Acción	Tipo de operación ejecutada.	Consulta la tabla Tipos de elemento y acciones
Tipo de elemento	Tipo del objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla Tipos de elemento y acciones
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla Tipos de elemento y acciones

Tabla 5.5: Campos del Registro de acciones

- **Campos mostrados en el fichero exportado**

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

Tabla 5.6: Campos del fichero exportado Registro de acciones

- **Herramienta de búsqueda**

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

Tabla 5.7: Campos de filtrado para el Registro de acciones

- **Tipos de elementos y acciones**

Tipo de elemento	Acción	Elemento
Acuerdo de licencia	Aceptar	Número de versión del EULA aceptado.
Cuenta	Actualizar consola	De Versión origen a Versión destino.
	Cancelar actualización de consola	De Versión origen a Versión destino.
Amenaza	Permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
	Dejar de permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
Búsqueda de información'	Lanzar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
Configuración - 'Control remoto'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Configuración de red'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.

Tabla 5.8: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
Configuración - 'Ajustes por equipo'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la Configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Bloqueo de programas'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Estaciones y servidores'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Dispositivos Android'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Información personal'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Patch Management'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Full Encryption'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.

Tabla 5.8: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Software autorizado'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Entornos VDI'	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Criterios para red de confianza'	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
Dispositivo	Editar nombre	Nombre del dispositivo sobre el que el usuario realizó la acción.
Envío programado	Crear	Nombre del envío programado sobre el que el usuario realizó la acción.
	Editar	Nombre del envío programado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del envío programado sobre el que el usuario realizó la acción.
Equipo	Eliminar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar nombre	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Cambiar Grupo	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Configuración de red'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Configuración de red'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tabla 5.8: Tipos de elemento y acciones

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

Tabla 5.8: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Revocar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar descubrimiento	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Descubrir ahora	Nombre del equipo sobre el que el usuario realizó la acción.
	Mover a su ruta de Active Directory	Nombre del equipo sobre el que el usuario realizó la acción.
	Aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Dejar de aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desinstalar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar agente	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar protección	Nombre del dispositivo sobre el que el usuario realizó la acción.
Equipo no administrado	Ocultar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Visibilizar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Instalar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
Filtro	Crear	Nombre del filtro sobre el que el usuario realizó la acción.
	Editar	Nombre del filtro sobre el que el usuario realizó la acción.
	Eliminar	Nombre del filtro sobre el que el usuario realizó la acción.
Grupo	Crear	Nombre del grupo sobre el que el usuario realizó la acción.

Tabla 5.8: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Editar	Nombre del grupo sobre el que el usuario realizó la acción.
	Eliminar	Nombre del grupo sobre el que el usuario realizó la acción.
	Cambiar Grupo-Padre	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Configuración de red'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Configuración de red'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.
	Sincronizar grupo	Nombre del grupo sobre el que el usuario realizó la acción.
	Mover equipos a su ruta de Active Directory	Nombre del grupo sobre el que el usuario realizó la acción.
Informes avanzados	Acceder	
Listado	Crear	Nombre del listado sobre el que el usuario realizó la acción.
	Editar	Nombre del listado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del listado sobre el que el usuario realizó la acción.
Parche	Excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.

Tabla 5.8: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Descargado manualmente"	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Requiere descarga manual"	Nombre del parche sobre el que el usuario realizó la acción.
Preferencia ante reclasificación de amenaza	Editar	
Preferencia para envío emails	Editar	
Preferencia de acceso de equipo de Panda Security S.L.	Editar	
Preferencia de acceso del distribuidor	Editar	
Preferencia para envío emails distribuidor	Editar	
Preferencia de verificación en dos pasos	Editar	
Rol	Crear	Nombre del rol sobre el que el usuario realizó la acción.
	Editar	Nombre del rol sobre el que el usuario realizó la acción.
	Eliminar	Nombre del rol sobre el que el usuario realizó la acción.
Tarea - Análisis de seguridad	Crear	Nombre de la tarea sobre el que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre el que el usuario realizó la acción.

Tabla 5.8: Tipos de elemento y acciones

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

Tabla 5.8: Tipos de elemento y acciones

- **Tipos de elementos y acciones**

Tipo de elemento	Acción	Elemento
Acuerdo de licencia	Aceptar	Número de versión del EULA aceptado.
Cuenta	Actualizar consola	De Versión origen a Versión destino.
	Cancelar actualización de consola	De Versión origen a Versión destino.
Amenaza	Permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
	Dejar de permitir	Nombre de la amenaza sobre la que el usuario realizó la acción.
Búsqueda de información'	Lanzar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la búsqueda sobre el que el usuario realizó la acción.
Configuración - 'Control remoto'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Configuración de red'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Ajustes por equipo'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la Configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Bloqueo de programas'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.

Tabla 5.9: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Estaciones y servidores'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Dispositivos Android'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Información personal'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Patch Management'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Full Encryption'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Software autorizado'	Crear	Nombre de la configuración sobre el que el usuario realizó la acción.
	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la configuración sobre el que el usuario realizó la acción.

Tabla 5.9: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
Configuración - 'Entornos VDI'	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
Configuración - 'Criterios para red de confianza'	Editar	Nombre de la configuración sobre el que el usuario realizó la acción.
Dispositivo	Editar nombre	Nombre del dispositivo sobre el que el usuario realizó la acción
Envío programado	Crear	Nombre del envío programado sobre el que el usuario realizó la acción.
	Editar	Nombre del envío programado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del envío programado sobre el que el usuario realizó la acción.
Equipo	Eliminar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar nombre	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Cambiar Grupo	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Configuración de red'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Configuración de red'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Proxy e idioma'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por equipo'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'dispositivos Android'	Nombre del dispositivo sobre el que el usuario realizó la acción.

Tabla 5.9: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Heredar configuración de 'dispositivos Android'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Información sensible'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Información sensible'	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Asignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desasignar licencia	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reiniciar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Bloquear	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Borrar datos	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Foto al ladrón	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Alarma remota	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Localizar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Designar Proxy Panda	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar Proxy Panda	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo caché	Nombre del equipo sobre el que el usuario realizó la acción.
	Designar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Configurar descubrimiento	Nombre del equipo sobre el que el usuario realizó la acción.
	Revocar equipo descubridor	Nombre del equipo sobre el que el usuario realizó la acción.
	Descubrir ahora	Nombre del equipo sobre el que el usuario realizó la acción.

Tabla 5.9: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Mover a su ruta de Active Directory	Nombre del equipo sobre el que el usuario realizó la acción.
	Aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Dejar de aislar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Desinstalar	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar agente	Nombre del dispositivo sobre el que el usuario realizó la acción.
	Reinstalar protección	Nombre del dispositivo sobre el que el usuario realizó la acción.
Equipo no administrado	Ocultar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Visibilizar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Editar descripción	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
	Instalar	Nombre del equipo no-administrado sobre el que el usuario realizó la acción.
Filtro	Crear	Nombre del filtro sobre el que el usuario realizó la acción.
	Editar	Nombre del filtro sobre el que el usuario realizó la acción.
	Eliminar	Nombre del filtro sobre el que el usuario realizó la acción.
Grupo	Crear	Nombre del grupo sobre el que el usuario realizó la acción.
	Editar	Nombre del grupo sobre el que el usuario realizó la acción.
	Eliminar	Nombre del grupo sobre el que el usuario realizó la acción.
	Cambiar Grupo-Padre	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Configuración de red'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Configuración de red'	Nombre del grupo sobre el que el usuario realizó la acción.

Tabla 5.9: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Asignar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Ajustes por Equipo'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Estaciones y servidores'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'dispositivos Android'	Nombre del grupo sobre el que el usuario realizó la acción.
	Asignar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.
	Heredar configuración de 'Información sensible'	Nombre del grupo sobre el que el usuario realizó la acción.
	Sincronizar grupo	Nombre del grupo sobre el que el usuario realizó la acción.
	Mover equipos a su ruta de Active Directory	Nombre del grupo sobre el que el usuario realizó la acción.
Informes avanzados	Acceder	
IOC	Crear (mediante importación)	Nombre del IOC sobre el que el usuario realizó la acción
	Eliminar	Nombre del IOC sobre el que el usuario realizó la acción
	Crear (mediante asistente)	Nombre del IOC sobre el que el usuario realizó la acción
	Editar	Nombre del IOC sobre el que el usuario realizó la acción.
Listado	Crear	Nombre del listado sobre el que el usuario realizó la acción.
	Editar	Nombre del listado sobre el que el usuario realizó la acción.
	Eliminar	Nombre del listado sobre el que el usuario realizó la acción.
Parche	Excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.

Tabla 5.9: Tipos de elemento y acciones

Tipo de elemento	Acción	Elemento
	Dejar de excluir para un equipo	Nombre del parche sobre el que el usuario realizó la acción.
	Dejar de excluir para todos los equipos	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Descargado manualmente"	Nombre del parche sobre el que el usuario realizó la acción.
	Marcar como "Requiere descarga manual"	Nombre del parche sobre el que el usuario realizó la acción.
Preferencia ante reclasificación de amenaza	Editar	
Preferencia para envío emails	Editar	
Preferencia de acceso de equipo de Panda Security S.L.	Editar	
Preferencia de acceso del distribuidor	Editar	
Preferencia para envío emails distribuidor	Editar	
Preferencia de verificación en dos pasos	Editar	
Rol	Crear	Nombre del rol sobre el que el usuario realizó la acción.
	Editar	Nombre del rol sobre el que el usuario realizó la acción.
	Eliminar	Nombre del rol sobre el que el usuario realizó la acción.
Tarea - Análisis de seguridad	Crear	Nombre de la tarea sobre el que el usuario realizó la acción.
	Editar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Eliminar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Cancelar	Nombre de la tarea sobre el que el usuario realizó la acción.
	Publicar	Nombre de la tarea sobre el que el usuario realizó la acción.

Tabla 5.9: Tipos de elemento y acciones

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

Tabla 5.9: Tipos de elemento y acciones

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

Tabla 5.9: Tipos de elemento y acciones

Eventos del sistema

Lista los eventos que se producen en Panda Adaptive Defense 360 y que no tienen una cuenta de usuario como origen, sino que son desencadenados por el propio sistema como respuesta las situaciones mostradas en la tabla 5.13.

- **Campos mostrados en el listado de eventos del sistema**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Panda Adaptive Defense 360.	Consulta la tabla 5.13
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta la tabla 5.13
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla 5.13

Tabla 5.10: Campos del listado Eventos del sistema

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Fecha	Fecha y hora en la que se ha producido el acceso.	Fecha
Evento	Acción que ejecutó Panda Adaptive Defense 360.	Consulta la tabla 5.13
Tipo	Tipo del objeto sobre el cual se ejecutó la acción.	Consulta la tabla 5.13
Elemento	Objeto de la consola sobre el cual se ejecutó la acción.	Consulta la tabla 5.13

Tabla 5.11: Campos del listado Eventos del sistema

- **Herramienta de búsqueda**

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

Tabla 5.12: Campos del listado Eventos del sistema

- **Tipos de elementos y acciones**

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

Tabla 5.13: Tipos de elementos y acciones



Parte 3

Despliegue y puesta en marcha

Capítulo 6: Instalación del software cliente

Capítulo 7: Licencias

Capítulo 8: Actualización del software cliente

Capítulo 6

Instalación del software cliente

La instalación es el proceso que distribuye Panda Adaptive Defense 360 en los equipos de la red de la organización. El paquete de instalación contiene todo el software necesario para activar el servicio de protección avanzado, la monitorización y la visibilidad del estado de la seguridad de los equipos, y no es necesaria la instalación de ningún otro programa.

Panda Adaptive Defense 360 ofrece varias herramientas que facilitan la instalación de la protección, que se detallan a continuación.

CONTENIDO DEL CAPÍTULO

Visión general del despliegue de la protección	106
Localiza los equipos desprotegidos en la red	107
Requisitos mínimos de la plataforma destino	107
Procedimiento de instalación	107
Desinstalar productos de la competencia y reiniciar equipos	107
Instalación en horario no laboral	109
Configuración por defecto de los equipos	109
Requisitos de instalación	109
Requisitos por plataforma	110
Requisitos de red	111
Instalación local del software cliente	111
Descarga del paquete de instalación desde la consola Web	111
Integración de equipos según su dirección IP	113
Generar la URL de descarga	114
Instalar manualmente el software cliente	114
Instalación en plataformas Windows x86 y ARM	114
Instalación en plataformas Linux con conexión a Internet	114
Instalación en plataformas Linux sin conexión a Internet	115
Instalación en Plataformas MacOS	115
Instalación en plataformas Android	116
Instalación remota del software cliente	117
Requisitos de red y sistema operativo	117
Equipos ocultos	118
Descubrir equipos	118
Asignar el rol de descubridor a un equipo de la red	119
Establecer el alcance del descubrimiento	119
Programar las tareas de descubrimiento	120
Lanzar las tareas de descubrimiento manuales	120

Visualizar equipos descubiertos	120
Equipos borrados	123
Detalle de los equipos descubiertos	124
Instalación remota de equipos descubiertos	126
Desde el listado de Equipos no administrados descubiertos	126
Desde la pantalla de detalles de equipo	126
Instalar con herramientas centralizadas - - - - -	127
Línea de comandos del paquete de instalación	127
Despliegue desde Panda Systems Management	127
Características y requisitos del componente	127
Despliegue con Microsoft Active Directory	128
Instalar mediante generación de imágenes gold - - - - -	129
Imágenes gold y Panda Adaptive Defense 360	130
Entornos no persistentes y Panda Adaptive Defense 360	130
Creación de una imagen gold para entornos VDI persistentes	130
Creación de una imagen gold para entornos VDI no persistentes	131
Preparación de la imagen gold	131
Ejecución del entorno VDI no persistente	132
Mantenimiento de la imagen gold para entornos VDI no persistentes	132
Mostrar los equipos no persistentes	133
Proceso de instalación en equipos Windows - - - - -	133
Comprobar el despliegue - - - - -	134
Visor de sucesos Windows	134
Desinstalar el software - - - - -	135
Desinstalación manual	135
Resultado de la desinstalación manual	137
Desinstalación remota	137
Reinstalación remota - - - - -	138
Requisitos de la funcionalidad de reinstalación remota	138
Acceso a la funcionalidad	138
Descubrimiento de equipos a reinstalar	138
Reinstalación en un equipo	138
Reinstalación en varios equipos	139
Ventana de selección Reinstalar la protección	139
Ventana de selección Reinstalar el agente	139
Códigos de error	140

Visión general del despliegue de la protección

El proceso de instalación comprende varios pasos, 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:

Localiza los equipos desprotegidos en la red

Localiza los equipos que no tienen instalada protección en la red del cliente o que tienen un producto de terceros que sea necesario sustituir o complementar con Panda Adaptive Defense 360 y comprueba que el número de licencias contratadas es suficiente.



Panda Adaptive Defense 360 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.

Requisitos mínimos de la plataforma destino

Los requisitos mínimos de cada plataforma se describen en "[Requisitos de red y sistema operativo](#)".

Procedimiento de instalación

Dependiendo del número total de equipos 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.

Desinstalar productos de la competencia y reiniciar equipos

Los servicios de protección de Panda Adaptive Defense 360 funcionan sin reiniciar el equipo en el caso de no tener un antivirus previamente instalado.



Algunas versiones anteriores de Citrix pueden requerir un reinicio del equipo o producirse un pequeño micro corte en las conexiones.

Para instalar Panda Adaptive Defense 360 en un equipo con una solución de seguridad de terceros, elige entre instalarlo sin retirar la otra protección o desinstalar la otra solución de seguridad y funcionar exclusivamente con Panda Adaptive Defense 360. Asigna una configuración de **Estaciones y servidores** con la opción **Desinstalar otros productos de seguridad** ajustada según tus necesidades. Coincidiendo con la búsqueda de actualizaciones, Panda Adaptive Defense 360 comprueba una vez al día la configuración establecida. Consulta el recurso web <https://www.pandasecurity.com/es/>

[support/card?id=50021](#) para obtener un listado de los productos de seguridad de terceros que Panda Adaptive Defense 360 desinstala de forma automática.



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 Panda Adaptive Defense 360 que quieras instalar, el comportamiento por defecto varía tal y como se muestra a continuación.

• **Versiones Trials**

No se desinstalarán por defecto las soluciones de seguridad de terceros para evaluar Panda Adaptive Defense 360.

• **Versiones comerciales**

Por defecto Panda Adaptive Defense 360 no se instala en un equipo que ya dispone de otra solución ajena a Panda Security. Si está disponible un desinstalador del producto, el antivirus de terceros se eliminará del equipo y se lanzará la instalación de Panda Adaptive Defense 360. En caso contrario, la instalación se detiene.

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



Consulta "[Configuración de la seguridad en estaciones y servidores](#)" en la [página 237](#) si quieres diseñar una configuración de seguridad. Consulta "[Asignación manual y automática de configuraciones](#)" en la [página 215](#) para asignar configuraciones a los equipos de la red.

• **Productos de protección antivirus de Panda Security**

Si el equipo está protegido previamente con Panda Endpoint Protection, Panda Endpoint Protection Plus o Panda Fusion se 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 serlo se requerirá un reinicio del equipo.

En la [tabla 6.1](#) se resume el comportamiento del equipo para completar la instalación de Panda Adaptive Defense 360.

Panda Adaptive Defense 360		Reinicio
Producto Anterior		
Ninguno	Trial o comercial	NO

Tabla 6.1: Probabilidad de reinicio al cambiar de producto de protección

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

Tabla 6.1: Probabilidad de reinicio al cambiar de producto de protección

Instalación en horario no laboral

Adicionalmente a la necesidad de reinicio del equipo de usuario descrita en el punto anterior, la instalación de Panda Adaptive Defense 360 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 fuera del horario laboral.

Configuración por defecto de los equipos

Con el objeto de proteger a los equipos de la red desde el primer momento, Panda Adaptive Defense 360 obliga a seleccionar el grupo de destino donde el equipo se integrará dentro del árbol de grupos, y la configuración de red de forma independiente. Esta selección se realiza al generar el instalador, consulta más adelante en la sección "[Instalación local del software cliente](#)".

Una vez instalado el software en el equipo, Panda Adaptive Defense 360 aplicará las configuraciones establecidas en el grupo al que pertenezca el equipo y, posteriormente, si la configuración de red del grupo seleccionado difiere de la indicada al generar el instalador, se generará una asignación manual. De esta forma será la configuración de red seleccionada en la instalación la que prevalece por encima de la asignada en el árbol de grupos.

Requisitos de instalación



Para una descripción completa de los requisitos por plataforma consulta "[Requisitos de hardware, software y red](#)" en la página 551.

Requisitos por plataforma

- **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 2019, Windows Server Core 2008 y superiores.
- **Versiones con procesador ARM:** Windows 10 Home y Pro.
- **Servidores Exchange:** 2003 al 2019.
- **Espacio para la instalación:** 650 Mbytes.
- **Certificados raíz actualizados** para utilizar el módulo Panda Patch Management y las comunicaciones en tiempo real con la consola de administración.

- **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.

- **Linux**

- **Sistemas operativos 64 bits:** Ubuntu 14.04 LTS y superiores, Fedora 23 y superiores, Debian 8 y superiores, RedHat 7 y superiores, CentOS 7 y superiores, LinuxMint 18 y superiores. No requiere sistema de ventanas instalado. Utiliza la herramienta `/usr/local/protection-agent/bin/pa_cmd` desde la línea de comandos.
- **Sistemas operativos 32 bits:** RedHat 6 y CentOS 6.
- **Kernel soportado:** hasta la versión 5.5.0 64 bits. En 32 bits 2.6.32-71 a 2.6.32-754. Versiones superiores del kernel no funcionarán.



Consulta la web de soporte en <https://www.pandasecurity.com/spain/support/card?id=700009> para comprobar la última versión del kernel de Linux soportada por Panda Adaptive Defense 360.

- **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. En equipos sin entorno gráfico la detección web y el filtrado web están deshabilitados.

Para instalar Panda Adaptive Defense 360 en plataformas Linux es necesario que el equipo tenga conexión a Internet durante todo el proceso. El script de instalación conectará con los repositorios apropiados dependiendo del sistema (rpm o deb) y se descargarán todos los paquetes necesarios

para finalizar la instalación con éxito. Consulta el apartado "[Instalación en plataformas Linux sin conexión a Internet](#)" para instalar Panda Adaptive Defense 360 en plataformas Linux aisladas de la red.

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

Requisitos de red

En su funcionamiento normal Panda Adaptive Defense 360 accede a varios recursos alojados en Internet. De forma general se requiere acceso a los puertos 80 y 443. Para un listado completo de las URLs que se acceden desde los equipos con el software Panda Adaptive Defense 360 instalado consulta "[Acceso a URLs del servicio](#)" en la página [560](#).

Instalación local del software cliente

Para descargar e instalar el software cliente en los equipos de la red sigue las tareas mostradas a continuación:

- Descargar del paquete de instalación desde la consola Web.
- Generar de URL de descarga.
- Instalar manualmente el software cliente.

Descarga del paquete de instalación desde la consola Web



Para más información sobre asignar configuraciones consulta "[Asignación manual y automática de configuraciones](#)" en la página [215](#).

Consiste en descargar el paquete de instalación directamente desde la consola de administración. Para ello sigue los pasos mostrados a continuación y consulta la figura [6.2](#):

- En la zona **Equipos** haz clic en el botón **Añadir equipo** y elige la plataforma a proteger: Windows, Linux, Android o macOS. La versión Windows incluye el paquete de instalación para procesadores

x86 y ARM

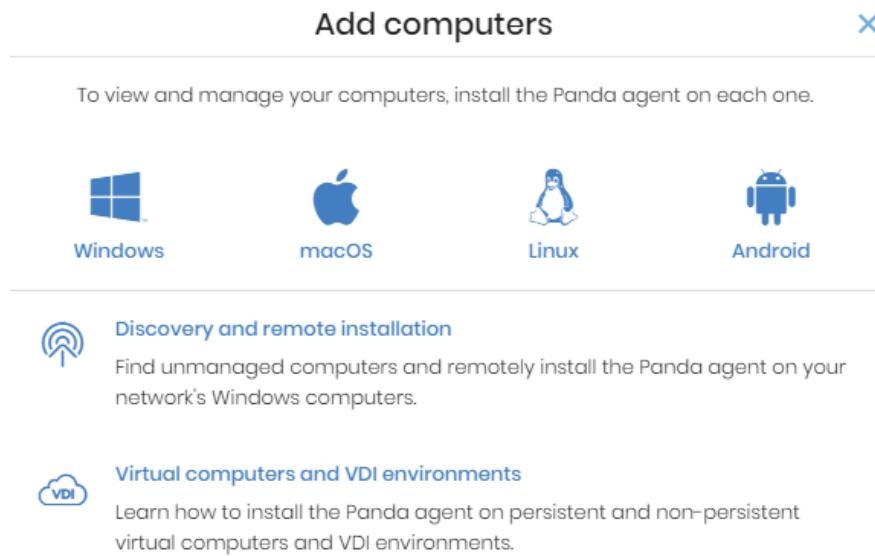


Figura 6.1: Ventana de selección de plataforma compatible con Panda Adaptive Defense 360

- Selecciona el grupo donde se integra el equipo en el árbol de carpetas:
 - 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)**. Para más información sobre los diferentes tipos de grupos consulta "[Tipos de grupos](#)" en la página [169](#).



Las políticas de seguridad asignadas a un equipo dependen del grupo al que pertenece. Si el administrador del directorio activo de la empresa mueve el equipo de una unidad organizativa a otra, este cambio se replicará en la consola de Panda Adaptive Defense 360 como un cambio de grupo. Por esta razón, las políticas de seguridad asignadas a ese equipo también podrían cambiar sin ser advertido por el administrador de la consola Web.

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

Selecciona la **Configuración de red (3)** que se aplicará al equipo a instalar. Para más información sobre crear nuevas configuraciones de red consulta "[Crear y gestionar configuraciones](#)" en la página [213](#).

- 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 selecciona de forma manual la configuración de red de entre las mostradas en el desplegable. Si la elección automática no se

ajusta a tus necesidades haz clic en el desplegable y elige otra de entre las disponibles.

Figura 6.2: Configuración del paquete de descarga

- 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.

Integración de equipos según su dirección IP

Al crear un grupo de equipos, Panda Adaptive Defense 360 permite la asignación de rangos de direcciones IPs e IPs individuales que determinan los equipos que formarán parte del grupo en el momento de su instalación. Consulta “[Crear y organizar grupos](#)” en la página 170 para obtener más información sobre la creación de grupos.

El objetivo de esta funcionalidad consiste en ahorrar tiempo al administrador organizando de forma automática los equipos recién integrados en el producto. Cuando un nuevo equipo se integra en Panda Adaptive Defense 360 se siguen los pasos mostrados a continuación:

- Si la opción elegida en la integración es **Seleccionar el grupo en función de la IP del equipo** Panda Adaptive Defense 360 ejecutará una búsqueda en profundidad para recuperar las IPs asociadas al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos** y las de todos sus hijos.
- Si se encuentra una única IP coincidente el equipo se moverá al grupo pertinente.
- Si hay varios grupos de IPs que coinciden con la IP del equipo se tomará siempre el grupo de mayor profundidad. Si existen varios grupos que coinciden con la IP con un mismo nivel de profundidad se elegirá el último de ellos.
- Si no existe ninguna coincidencia, el equipo se moverá al grupo indicado en el campo **Seleccionar a partir de qué grupo se añadirán los equipos**, y si este grupo no existe en el momento de la integración el equipo se moverá al grupo Todos.

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

Generar la URL de descarga

Este método permite la creación de una URL de descarga para enviar por correo a los usuarios que quieran iniciar una instalación manual en su equipo.

Para generar la URL de descarga, sigue los pasos que se indican en “[Descarga del paquete de instalación desde la consola Web](#)” en la página 111 y haz clic en el botón **Enviar por email (4)**.

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.

Instalar manualmente el software cliente



Para la instalación del software Panda Adaptive Defense 360 en el equipo de usuario se requieren permisos de administrador.

Instalación en plataformas Windows x86 y ARM

Para ejecutar el instalador descargado haz doble clic sobre su icono y sigue el asistente. Durante el proceso de instalación se mostrará una ventana con el progreso de la tarea. En los equipos Windows se le indicará al administrador de la red si el número de licencias libres no es suficiente como para asignar una al equipo en proceso de instalación. Independientemente de este hecho el equipo se integrará en el servicio aunque el equipo no estará protegido si no hay licencias disponibles.

El instalador es compatible con plataformas Windows que utilizan tanto microprocesadores de la familia x86 como ARM. Consulta “[Requisitos de plataformas Windows](#)” en la página 554.

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 con conexión a Internet

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

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

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


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

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

Comprueba que se han creado los siguientes directorios de instalación:

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

Instalación en plataformas Linux sin conexión a Internet

Los servidores o equipos de usuario sin acceso directo a Internet ni a través de un proxy Panda y con distribuciones instaladas no actualizadas utilizan el paquete de instalación completo. Este paquete incluye todas las librerías necesarias para el buen funcionamiento del agente.



Para obtener el paquete de instalación completo ponte en contacto con tu comercial asignado o con el equipo de soporte de Panda.

El instalador completo es compatible con las siguientes distribuciones:

- Redhat 6, 7, 8.
- CentOS 6, 7, 8.

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

- Protección 3.00.00.0050 y posteriores
- Agente 1.10.06.0050 y posteriores

Si se utiliza el paquete complete en una distribución no compatible, la instalación dará un error.

Para instalar el agente Panda Adaptive Defense 360 abre una terminal en la carpeta donde reside el paquete descargado y ejecuta el comando siguiente:

```
$./configure-repository.sh --no-deps
```

Para volver a la instalación con dependencias lanza el comando siguiente:

```
$./configure-repository.sh --deps
```

Instalación en Plataformas MacOS

Para instalar el producto en el equipo de usuario sigue los pasos mostrados a continuación:

- Guarda el instalador en el equipo y haz doble clic en el archivo .dmg
- Ejecuta el contenedor .pkg.

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

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

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

```
/Applications/Management-gent.app/Contents      /*/Library/ApplicationSupport/
ManagementAgent/
```



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

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:

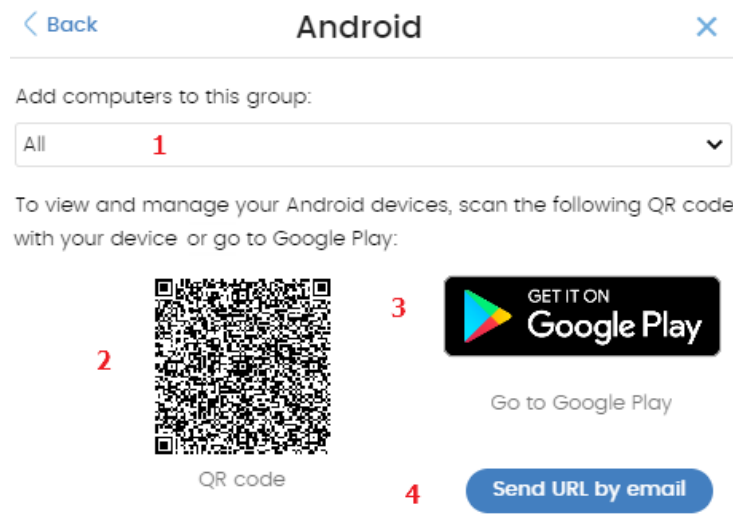


Figura 6.3: Instalación en dispositivos Android

- **Añadir los equipos al siguiente grupo (1):** especifica el grupo dentro del árbol de carpetas en el que se integrará el dispositivo una vez se haya instalado el software Panda Adaptive Defense 360.
- **Código QR (2):** código QR que contiene el enlace para descargar el software de la Google Play.
- **Acceso a la Google Play (3):** enlace directo de descarga del software Panda Adaptive Defense 360 de la Google Play.
- **Enviar URL por mail (4):** mensaje de correo con el enlace de descarga listo para enviar al usuario del dispositivo a proteger con Panda Adaptive Defense 360.

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.

- Sigue uno de los tres procedimientos descritos a continuación para descargar la aplicación Android:
 - **Mediante código QR:** haz clic en el código QR para agrandarlo, 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 enviar al usuario un mail con el enlace que le llevará a la ficha de la aplicación en Google Play, 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 enlace **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 conceder ciertos permisos de acceso a recursos del dispositivo móvil. Dependiendo de la versión de Android (6.0 en adelante), estos permisos se presentarán de forma progresiva según se necesiten, o por el contrario se mostrará una 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.

Instalación remota del software cliente

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 es compatible con plataformas Windows.

Requisitos de red y sistema operativo

Para poder instalar Panda Adaptive Defense 360 de forma remota, es necesario que los equipos cumplan con los requisitos indicados a continuación:

- Abrir los puertos UDP 21226 y 137 para el proceso `System`.
- Abrir el puerto TCP 445 para el proceso `System`.

- Habilitar el protocolo NetBIOS sobre TCP.
- Permitir las resoluciones DNS.
- Acceso al recurso de administración Admin\$. En las ediciones "Home" de Windows es necesario habilitar este recurso de forma explícita.
- Credenciales de administrador de dominio o de la cuenta de administrador local generada por defecto en la instalación del sistema operativo.
- Credenciales de administrador de dominio o de administrador local.
- Activar la Administración remota.



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

Adicionalmente, para que un equipo de la red con Panda Adaptive Defense 360 instalado pueda descubrir a otros equipos es necesario que:

- No estén ocultos por el administrador.
- No estén siendo ya administrados por Panda Adaptive Defense 360 sobre Aether Platform.
- Se encuentren en el mismo segmento de subred al que pertenece el equipo descubridor.

Equipos ocultos

Para evitar generar listados de equipos no administrados descubiertos muy extensos que incluyan dispositivos sin interés para la instalación de Panda Adaptive Defense 360, es posible ocultarlos de forma selectiva siguiendo los pasos mostrados a continuación:

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

Descubrir equipos

El descubrimiento de equipos se efectúa a través de un equipo con el rol de Descubridor asignado. Todos los equipos que cumplan los requisitos se mostrarán en el listado **Equipos no administrados descubiertos**, independientemente de si el sistema operativo o el tipo de dispositivo admite la instalación de Panda Adaptive Defense 360.

El primer equipo Windows que se integre en Panda Adaptive Defense 360 tendrá asignado el rol descubridor de forma automática.

Asignar el rol de descubridor a un equipo de la red

- Comprueba que el equipo descubridor tiene instalado Panda Adaptive Defense 360.
- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y pestaña **Descubrimiento**.
- Haz clic en el botón **Añadir equipo descubridor** y selecciona en el listado los equipos que lanzarán procesos de descubrimiento en la red.

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

Campo	Descripción
Nombre del equipo	Nombre del equipo descubridor.
Dirección IP	Dirección IP del equipo descubridor.
Configuración de la tarea de descubrimiento	Configuración de la tarea automática que se lanza para descubrir equipos en la red, si está configurada.
Última comprobación	Fecha y hora de la última vez que se lanzó una tarea de descubrimiento.
"El equipo está apagado o sin conexión"	Panda Adaptive Defense 360 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.

Tabla 6.2: Campos del detalle de un equipo con el rol descubridor asignado

Establecer el alcance del descubrimiento



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

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**, haz clic en el botón **Configurar** del equipo descubridor cuyo alcance de descubrimiento quieres modificar.

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

Programar las tareas de descubrimiento

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

- 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 Panda Adaptive Defense 360.
- Haz clic en **Aceptar**. El equipo configurado mostrará en su descripción la programación configurada.

Lanzar las tareas de descubrimiento manuales

- 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.

Visualizar equipos descubiertos

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

- **Widget Estado de protección:** desde el menú superior **Estado** accede al panel de control de Panda Adaptive Defense 360 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 Adaptive Defense 360**.
- **Panel Mis listados:** accede a la sección **Mis listados** desde el panel lateral y haz clic en el enlace **Agregar**. Selecciona en el desplegable el listado **Equipos no administrados descubiertos**.
- **Listado Equipos no administrados descubiertos**

Este listado contiene los equipos descubiertos en la red del cliente que no tienen instalado Panda Adaptive Defense 360 o que, habiéndose instalado correctamente su funcionamiento no es el correcto.

Campo	Descripción	Valores
Equipo	Nombre del equipo descubierto.	Cadena de caracteres
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	— No administrado: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. 📶 Instalando: el proceso de instalación se ha iniciado. 🔴 Error instalando: mensaje con el tipo de error producido en la instalación. Consulta “Sección alertas de equipo (2)” en la página 190 para una relación de mensajes de error y la explicación de cada uno de ellos. Si el error es de origen desconocido se mostrará su código de error asociado.
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Último descubridor	Nombre del dispositivo que descubrió más recientemente el puesto de trabajo o servidor.	Cadena de caracteres
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 6.3: Campos del listado de equipos no administrados descubiertos

Cuando el campo **Estado** muestra **Error instalando** y es un error de origen conocido, se añade una cadena de texto que lo describe. Consulta [“Sección alertas de equipo \(2\)”](#) en la página 190 para obtener un listado de los errores de instalación reportados por Panda Adaptive Defense 360.

• **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Tabla 6.4: Campos del fichero exportado Listado de Equipos no administrados descubiertos

Campo	Descripción	Valores
Nombre	Nombre del equipo descubierto.	Cadena de caracteres
IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección MAC	Dirección física del equipo.	Cadena de caracteres
Fabricante NIC	Marca de la tarjeta de red del equipo descubridor.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
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
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Última vez visto por	Nombre del equipo descubridor que vio por última vez al puesto.	Cadena de caracteres
Descripción	Descripción del equipo descubierto.	Cadena de caracteres
Estado	Estado en el que se encuentra el equipo con respecto al proceso de instalación.	• No administrado: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • Instalando: el proceso de instalación se ha iniciado. • Error instalando: mensaje con el tipo de error producido en la instalación. Consulta "Sección alertas de equipo (2)" en la página 190 para una relación de mensajes de error y la explicación de cada uno de ellos.
Error	Descripción del error encontrado.	Consulta "Sección alertas de equipo (2)" en la página 190.
Fecha error instalación	Fecha y hora en la que se produjo el error.	Fecha

Tabla 6.4: Campos del fichero exportado Listado de Equipos no administrados descubiertos

- **Herramienta de búsqueda**

Campo	Descripción	Valores
Buscar	Búsqueda por el nombre del equipo, IP, fabricante de la tarjeta de red o equipo descubridor.	Cadena de caracteres
Estado	Estado de la instalación de Panda Adaptive Defense 360.	• No administrado: el equipo ha sido localizado como candidato a la instalación, pero ésta aún no se ha iniciado. • Instalando: el proceso de instalación se ha iniciado. • Error instalando: mensaje con el tipo de error producido en la instalación.
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	• Últimas 24 horas • Últimos 7 días • Último mes

Tabla 6.5: Campos de filtrado para el listado Listado de Equipos no administrados descubiertos

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta [“Información de equipo”](#) en la página 189 para obtener más información.

Equipos borrados

Panda Adaptive Defense 360 no elimina de la lista **Equipos no administrados descubiertos** los dispositivos que una vez fueron detectados, pero ya no están accesibles por haberse retirado (avería, robo o cualquier otra razón).

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

- En el listado de **Equipos no administrados descubiertos** selecciona **Descubiertos** u **Ocultos** en el combo dependiendo del estado del dispositivo.
- Haz clic en las casillas correspondientes a los equipos a borrar.
 - Para borrar varios equipos haz clic en el menú de contexto general y en **Borrar**.
 - Para borrar un único equipo haz clic en el menú de contexto del equipo y en **Borrar**.



Un equipo que se elimina de la consola sin desinstalar el software Panda Adaptive Defense 360, y sin retirarse físicamente de la red volverá a aparecer en la siguiente tarea de descubrimiento. Borra únicamente los equipos que nunca más vayan a ser accesibles.

Detalle de los equipos descubiertos

1

Computer details

Last seen: 2 11/6/2017 10:59:20 AM

IP address: 192.168.1.1

Physical addresses 64:51:06:00:00:01

Discovered by

Computer	Last seen
WIN_DESKTOP_4	11/6/2017 10:59:18 AM
WIN_DESKTOP_12	3 11/6/2017 10:59:19 AM

Figura 6.4: Distribución de la información en un equipo descubierto

En el listado de **Equipos no administrados descubiertos**, 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.

Alertas de equipo

Estado	Tipo	Resolución
Error instalando el agente de Panda	Indica el motivo del error en la instalación del agente.	
	Credenciales incorrectas	Lanza de nuevo la instalación con unas credenciales que tengan suficientes privilegios para realizar la instalación.
	No es posible conectar con el equipo	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible descargar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible copiar el instalador del agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible instalar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
	No es posible registrar el agente	Verifica que el equipo está encendido y que cumple los requisitos de instalación remota.
Error instalando la protección de Panda Adaptive Defense 360	Indica el motivo del error en la instalación de la protección.	

Tabla 6.6: Campos del listado Equipos protegidos

Estado	Tipo	Resolución
	No hay suficiente espacio libre en el disco para realizar la instalación	Consulta "Requisitos hardware" en la página 555 para ver los requisitos de espacio necesarios para instalar Panda Adaptive Defense 360.
	El servicio de Windows Installer no está operativo	Comprueba que el servicio Windows Installer se esté ejecutando. Para y arranca el servicio.
	El usuario canceló la desinstalación de la protección de otro fabricante	Acepta la desinstalación del antivirus de terceros.
	Hay otra instalación en curso	Espera a que finalice la instalación previa.
	Error desinstalando automáticamente protecciones de otros fabricantes	Consulta Desinstaladores soportados para ver una lista de fabricantes con desinstalador soportado por Panda Security.
	Desinstalador no disponible para protección de otro fabricante	Contacta con el departamento de soporte para pedir un desinstalador.
Instalando agente de Panda	Una vez terminado el proceso de instalación el equipo dejará de aparecer en el listado de Equipos no administrados descubiertos.	
Equipo no administrado	El equipo no tiene el agente Panda instalado. Comprueba que se trata de un equipo compatible con Panda Adaptive Defense 360 y que cumple con los requisitos indicados en "Requisitos de hardware, software y red" en la página 551 .	

Tabla 6.6: Campos del listado Equipos protegidos

Detalles del equipo

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

Tabla 6.7: Filtros del listado de licencias

Descubierto por

Campo	Descripción
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.

Tabla 6.8: Filtros del listado de licencias

Instalación remota de equipos descubiertos

Para instalar de forma remota el software Panda Adaptive Defense 360 en uno o varios equipos distribuidos sigue los pasos mostrados a continuación:

Desde el listado de Equipos no administrados descubiertos

- Accede al listado de **Equipos no administrados descubiertos**.
 - Desde el panel lateral **Mis listados**, **Añadir**, selecciona el listado **Equipos no administrados descubiertos**.
 - Desde el menú superior **Estado** en el widget **Estado de la protección**, haz clic en el link **Se han descubierto x equipos que no están siendo administrados desde Panda Adaptive Defense 360**.
 - 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 no administrados descubiertos** selecciona **Descubiertos u Ocultos** en el combo, dependiendo del estado del dispositivo.
- 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 "[Descarga del paquete de instalación desde la consola Web](#)".
- 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 "[Descarga del paquete de instalación desde la consola Web](#)".

Instalar con herramientas centralizadas

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

Línea de comandos del paquete de instalación

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

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

A continuación, se muestra un ejemplo de instalación con parámetros

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

Despliegue desde Panda Systems Management

Para los clientes de Panda Systems Management el despliegue de Panda Adaptive Defense 360 está completamente automatizado a través de los componentes:

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

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

Características y requisitos del componente

Los componentes no tienen ningún requisito más allá de los indicados para Panda Systems Management y Panda Adaptive Defense 360.

El tamaño del componente es:

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

Una vez desplegado y ejecutado, el componente descargará el instalador Panda Adaptive Defense 360. Dependiendo de la versión, el tamaño varía entre 6 y 8 Mbytes por cada equipo a instalar.

Despliegue con Microsoft Active Directory



El método de despliegue mediante Microsoft Active Directory permite instalar el software de seguridad en un equipo por primera vez. No se soporta la actualización del software de seguridad ya instalado.

A continuación, se detallan los pasos para el despliegue del software Panda Adaptive Defense 360 en los equipos de una red Windows con Directorio Activo mediante GPO (Group Policy Object).

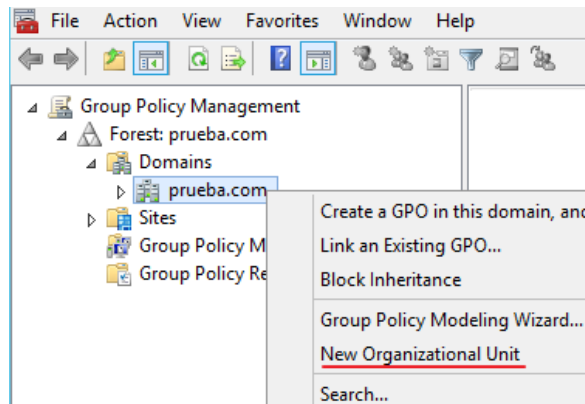


Figura 6.5: Nueva unidad organizativa

Administrador de políticas de grupo.

1. Descarga del paquete Panda Adaptive Defense 360 y comparte el instalador en la red.

- Coloca el instalador Panda Adaptive Defense 360 en una carpeta compartida que sea accesible por todos los equipos que vayan a recibir el software.

2. Crea una nueva UO (Unidad Organizativa) de nombre “Despliegue Aether”.

- Abre la mmc y agrega el snap-in

- Con el botón de la derecha en el nodo del dominio, haz clic en Nuevo y Unidad Organizativa para crear una unidad organizativa de nombre “Despliegue Aether”.
- Haz clic con el botón de la derecha del ratón en la unidad organizativa recién creada y selecciona en el menú Bloquear herencia.

3. Crea una nueva GPO con el paquete de instalación

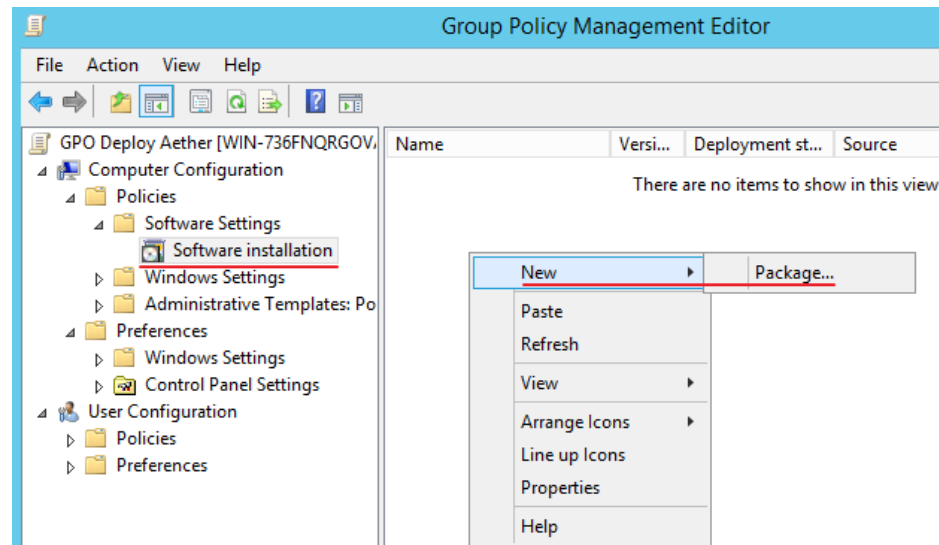


Figura 6.6: Nuevo paquete de instalación

- Haz clic con el botón de la derecha del ratón en la Unidad Organizativa recién creada y selecciona Crear una GPO en este, de nombre "GPO Despliegue Aether".
- Edita la GPO recién creada y añade el paquete de instalación que contiene el software Panda Adaptive Defense 360 en la rama Configuración del equipo, Políticas, Configuración de software, Instalación del software.
 - Con el botón de la derecha en el panel de la derecha, haz clic en Nuevo, Paquete.
 - Añade el fichero de instalación .msi de Panda Adaptive Defense 360.

4. Edita las propiedades del paquete

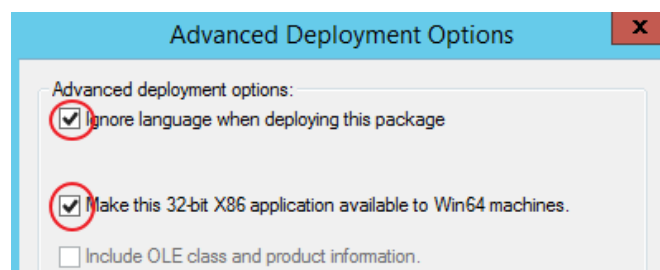


Figura 6.7: Configuración del despliegue

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

Instalar mediante generación de imágenes gold

En redes grandes formadas por muchos equipos homogéneos, el procedimiento de instalación del sistema operativo y del software que lo acompaña puede automatizarse generando una imagen

gold (también conocida como imagen "master", "base" o imagen "plataforma"). Posteriormente esta imagen se distribuye a todos los equipos de la red evitando una gran parte del proceso manual que supone instalar desde cero un equipo.

Para generar esta imagen es necesario instalar en un equipo de la red el sistema operativo ya actualizado junto a todo el software que el usuario vaya a necesitar, incluyendo las herramientas de seguridad.

Imágenes gold y Panda Adaptive Defense 360

La instalación del software Panda Adaptive Defense 360 lleva asociada la asignación automática de un identificador único que Panda Security utiliza para referenciar el equipo en la consola de administración. Si se genera una imagen gold con el software Panda Adaptive Defense 360 ya instalado y se copia en otros equipos, todos los equipos heredarán el mismo identificador, de forma que la consola mostrará un único equipo. Para evitar esta situación es necesario borrar este identificador con el programa `Panda Aether tool` accesible desde la página web de soporte de Panda Security en la siguiente URL:

<https://www.pandasecurity.com/spain/support/card?id=700050>



En esta URL además encontrarás el procedimiento detallado para preparar e instalar una imagen gold en entornos VDI persistentes y no persistentes.

Entornos no persistentes y Panda Adaptive Defense 360

En los entornos VDI no persistentes algunos parámetros del hardware virtual como por ejemplo la MAC de las tarjetas de red pueden cambiar en cada reinicio. Por esta razón la identificación de estos equipos y su posterior asignación de una licencia no pueden realizarse mediante el hardware ya que el sistema consideraría a un equipo como nuevo en cada reinicio y consumiendo una licencia adicional. Además, el sistema de almacenamiento de un equipo VDI no persistente se limpia en cada reinicio, perdiéndose el identificador de Panda Adaptive Defense 360 asignado.

Creación de una imagen gold para entornos VDI persistentes

En un entorno VDI persistente los equipos conservan entre reinicios la información que han salvado en el disco duro y por esta razón el proceso de creación de imagen gold solo requiere configuración de actualización de Panda Adaptive Defense 360.

Una vez instalado el sistema operativo actualizado e instalados todos los programas que los usuarios necesitarán sigue los pasos mostrados a continuación:

- Instala el software cliente Panda Adaptive Defense 360 en el equipo según los pasos mostrados en "[Instalación local del software cliente](#)".
- Comprueba que el equipo tiene conexión a Internet y asígnele una configuración con la

actualización de la protección y el conocimiento de Panda Adaptive Defense 360 activada. Consulta "[Gestión de configuraciones](#)" en la página 207 y "[Actualización del software cliente](#)" en la página 153 para crear y asignar una configuración al equipo respectivamente.

- Ejecuta la herramienta `Panda Aether tool` y haz clic en el botón **Start cache scan** para analizar el equipo y precargar la caché de goodwill de Panda Adaptive Defense 360.
- Haz clic en el botón **Unregister device** para borrar el identificador del equipo y asegúrate de que la casilla de selección **Is a gold image** NO está marcada.
- Apaga el equipo y genera la imagen con el software de administración de entornos virtuales que utilices.

Creación de una imagen gold para entornos VDI no persistentes

En un entorno VDI no persistente son necesarias dos configuraciones de actualización de Panda Adaptive Defense 360: una para actualizar la imagen gold en el momento de su preparación y mantenimiento, y otra para desactivar las actualizaciones en su ejecución ya que no tiene sentido consumir ancho de banda para actualizar Panda Adaptive Defense 360 si el sistema de almacenamiento del equipo se va a revertir a su estado original en cada reinicio.

Preparación de la imagen gold

Una vez instalado el sistema operativo actualizado y todos los programas que los usuarios necesitarán sigue los pasos mostrados a continuación:

- Instala el software cliente Panda Adaptive Defense 360 según los pasos mostrados en "[Instalación local del software cliente](#)".
- Comprueba que el equipo tiene conexión a Internet y asígnale una configuración con la actualización de la protección y el conocimiento de Panda Adaptive Defense 360 activada. Consulta "[Gestión de configuraciones](#)" en la página 207 y "[Actualización del software cliente](#)" en la página 153 para crear y asignar una configuración al equipo respectivamente.
- Ejecuta la herramienta `Panda Aether tool` y haz clic en el botón **Start cache scan** para analizar el equipo y precargar la caché de goodwill de Panda Adaptive Defense 360.
- Haz clic en el botón **Unregister device** para borrar el identificador del equipo y asegúrate de que la casilla de selección **Is a gold image** SI está marcada.
- Asigna al equipo una configuración que deshabilite la actualización de la protección y del conocimiento de Panda Adaptive Defense 360.
- Deshabilita el servicio Panda Endpoint Agent desde el panel de servicios de Windows para que no arranque automáticamente al usar esta imagen gold en las instancias virtuales.
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.
- En el menú superior **Configuración**, panel lateral **Entornos VDI** define el máximo número de equipos que estarán activos simultáneamente. Esto permitirá una gestión automática de las licencias que

consumen estas máquinas.

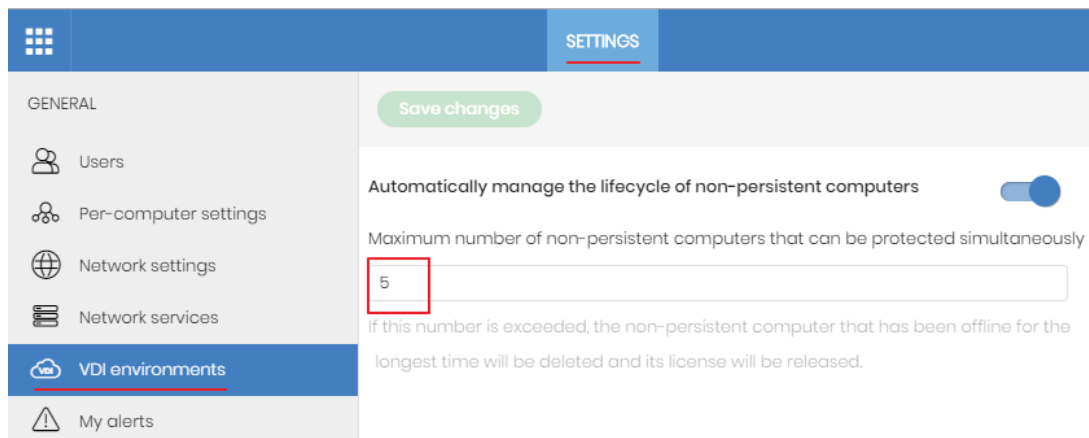


Figura 6.8: Configuración del numero de licencias asignadas a equipos VDI no persistentes

Ejecución del entorno VDI no persistente

Para que Panda Adaptive Defense 360 se ejecute con normalidad es necesario cambiar el tipo de inicio del servicio del agente de Panda, que previamente hemos deshabilitado en la imagen gold. Para ello sigue los pasos mostrados a continuación:

- Utiliza las herramientas de administración de GPO en un equipo físico conectada al dominio y crea una GPO para cambiar el tipo de inicio del servicio Panda Endpoint Agent.



Consulta la URL <https://www.microsoft.com/es-ES/download/details.aspx?id=21895> para conocer más detalles.

- Dentro de la configuración de GPO, navega a la siguiente ruta: Computer Configuration, Policies, Windows Settings, Security Settings, System Services, Panda Endpoint Agent.
- Cambia la configuración del servicio a automática para que se modifique en el siguiente arranque y así pueda integrarse con la consola.

Mantenimiento de la imagen gold para entornos VDI no persistentes

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

- Habilita el servicio Panda Endpoint Agent.
- Comprueba que el equipo tiene conexión a Internet y asígnele una configuración con la actualización de la protección y el conocimiento de Panda Adaptive Defense 360 activada.
- Ejecuta la herramienta `Panda Aether tool` y haz clic en el botón **Start cache scan** para analizar el equipo y precargar la caché de goodwill de Panda Adaptive Defense 360.

- Haz clic en el botón **Unregister device** para borrar el identificador del equipo y asegúrate de que la casilla de selección **Is a gold image** SI está marcada.
- Asigna al equipo una configuración que deshabilite la actualización de la protección y del conocimiento de Panda Adaptive Defense 360.
- Deshabilita el servicio Panda Endpoint Agent para que no arranque automáticamente al usar esta imagen gold en las instancias virtuales.
- Apaga el equipo para generar la imagen con el software de administración de entornos virtuales que utilices.
- Sustituye en el entorno VDI la imagen anterior por la nueva obtenida.
- Repite este proceso de mantenimiento una vez al mes por lo menos.

Mostrar los equipos no persistentes

Panda Adaptive Defense 360 identifica por el FQDN (Fully Qualified Domain Name) aquellos equipos cuyo identificador ha sido borrado mediante el programa `Panda Aether tool` y están marcados como imagen gold. Para obtener un listado de los equipos VDI no persistentes sigue los pasos mostrados a continuación:

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

Proceso de instalación en equipos Windows

Una vez instalado el agente, éste realizará una serie de procesos de comprobación de manera automática:

1. **Integración del agente en Aether:** el agente enviará la información del equipo a la nube de Panda para integrarlo en la plataforma.
2. **Descarga del instalador del módulo de la protección:** el agente descargará e instalará el módulo de protección.
3. **Descarga del fichero de firmas:** el agente descargará el fichero de firmas con el malware conocido.
4. **Descarga de configuraciones:** configuraciones predeterminadas y creadas por el administrador y que se aplica al equipo.
5. **Comprobar la conectividad con la nube de Panda:** en caso de error se reportará su tipo a los siguientes lugares:
 - **En la consola de instalación del agente:** se mostrará un mensaje de error y las URLs que fallaron. Haz clic en el botón **Reintentar** para realizar una nueva verificación.
 - **En el visor de sucesos de Windows (Eventlog):** se mostrará un mensaje de error y las URLs que fallaron.

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

Comprobar el despliegue

El administrador de la red dispone de tres formas complementarias para determinar el resultado del despliegue del software Panda Adaptive Defense 360 en la red gestionada:

- Mediante el widget **Estado de protección**. Consulta [“Estado de protección”](#) en la página 412.
- Mediante el listado **Estado de la seguridad de los equipos**. Consulta [“Estado de protección de los equipos”](#) en la página 429.
- Mediante el registro Aplicación del visor de sucesos en los equipos Windows.

Visor de sucesos Windows

El registro Aplicación del visor de sucesos recoge información extendida sobre el resultado de la instalación del agente en el equipo del usuario y sobre su funcionamiento una vez instalado. A continuación se muestra una tabla con la información suministrada por Panda Adaptive Defense 360 en cada campo del visor de sucesos.

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

Tabla 6.9: Códigos de resultado del procesos de instalación del agente en el visor de sucesos

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

Tabla 6.9: Códigos de resultado del procesos de instalación del agente en el visor de sucesos

Desinstalar el software

Puedes desinstalar el software Panda Adaptive Defense 360 de forma manual desde el panel de control del sistema operativo, o de forma remota desde la zona **Equipos** o desde los listados **Estado de la protección de los equipos** y **Licencias**.

Desinstalación manual

El propio usuario podrá ejecutar una desinstalación manual siempre y cuando el administrador de la protección no haya establecido una contraseña de desinstalación al configurar el perfil de la

protección para su PC. Si lo ha hecho, se necesitará autorización o disponer de las credenciales necesarias para poder desinstalar la protección.



Consulta **“Protección del agente mediante contraseña”** en la página **234** para establecer o eliminar la password de desinstalación del agente.

La instalación de Panda Adaptive Defense 360 incluye varios programas independientes, según sea la plataforma de destino:

- **Equipos Windows y macOS:** agente y protección.
- **Equipos Linux:** agente, protección y módulo del kernel.
- **Dispositivos Android:** protección.

Para desinstalar completamente Panda Adaptive Defense 360 es necesario quitar todos los módulos. Si se desinstala únicamente el módulo de la protección, transcurrido un tiempo el agente la reinstalará de forma automática.

- **Windows 8 o superior:**
 - Panel de Control > Programas > Desinstalar un programa.
 - También puedes desinstalar tecleando, en el menú Metro: “desinstalar un programa”.
- **Windows Vista, Windows 7, Windows Server 2003 y superiores:**
 - Panel de Control > Programas y características > Desinstalar o cambiar.
- **En Windows XP:**
 - Panel de Control > Agregar o quitar programas.
- **macOS:**
 - Finder > Aplicaciones > Arrastra el icono de la protección que deseas desinstalar a la papelera o ejecuta el comando `sudo sh /Applications/Protection-Agent.app/Contents/uninstall.sh`
 - El agente no se desinstala arrastrando el icono a la papelera, en su lugar es necesario ejecutar el comando `sudo sh /Applications/Management-Agent.app/Contents/uninstall.sh`
- **Dispositivos Android:**
 - Accede a Configuración de Android. Seguridad > Administradores de dispositivos.
 - Desactiva la casilla correspondiente a Panda Adaptive Defense 360. A continuación, Desactivar > Aceptar.
 - De nuevo en la pantalla de Configuración de Android selecciona Aplicaciones instaladas. Haz clic en Panda Adaptive Defense 360 > Desinstalar > Aceptar.

- **En Linux:**

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

- **Fedora:** Actividades > Software > Instalado

- **Ubuntu:** Software de Ubuntu > Instaladas

Se recomienda utilizar la línea de comandos para desinstalar el producto:

- **Ubuntu**

- **Agente:** `sudo dpkg -r management-agent`

- **Kernel:** `sudo dpkg -r protection-agent-dkms`

- **Protección:** `sudo dpkg -r protection-agent-corporate`

- **Fedora** (sustituye "version" por la build del maquete pulsando la tecla de tabulación)

- **Agente:** `sudo dnf remove management-agent-"version"`

- **Kernel:** `sudo dnf remove protection-agent-dkms-"version"`

- **Protección:** `sudo dnf remove protection-agent-corporate-"version"`

Resultado de la desinstalación manual

Al desinstalar el software Panda Adaptive Defense 360 (agente Panda y Protección) el equipo desaparecerá completamente de la consola de administración. Todos los contadores, entradas en informes e información de la actividad del equipo y de sus procesos se borrarán.

Si, posteriormente, el mismo equipo vuelve a ser integrado en la consola de administración mediante la reinstalación del software Panda Adaptive Defense 360, se recuperará toda la información previamente eliminada.

Desinstalación remota

Para desinstalar de forma remota un equipo Windows protegido con Panda Adaptive Defense 360 sigue los pasos mostrados a continuación:

- En la zona **Equipos**, o en los listados **Licencias** y **Estado de la protección de equipos** marca los equipos a desinstalar con las casillas de selección.
- En la barra de acciones haz clic en el botón **Eliminar**. Se mostrará una ventana de confirmación.
- En la ventana de confirmación haz clic en la casilla **Desinstalar el agente de Panda de los equipos seleccionados** para retirar por completo el software Panda Adaptive Defense 360.



La desinstalación remota solo se soporta en plataformas Windows. En plataformas Linux y macOS únicamente se retirará el equipo de la consola junto a todos los contadores, si bien en el próximo descubrimiento de la red el equipo será reincorporado a la consola, junto a toda su información.

Reinstalación remota

Para resolver algunas situaciones donde el software Panda Adaptive Defense 360 presente una mala funcionamiento, se permite su reinstalación remota desde la consola de administración, tanto para equipos de usuario como para servidores.

La reinstalación del software se realiza por separado para el agente y para el módulo de la protección.

Requisitos de la funcionalidad de reinstalación remota

- Equipo de usuario o servidor con sistema operativo Windows instalado.
- Un equipo con el rol de descubridor asignado en el mismo segmento de red que el equipo a reinstalar y que comunique con la nube de Panda Security.
- Tener las credenciales de una cuenta de administrador local o de dominio.

Acceso a la funcionalidad

Desde los listados mostrados a continuación accesibles en el menú superior **Estado**, haciendo clic en el enlace **Añadir** del panel lateral:

- “[Estado de protección de los equipos](#)” en la página [429](#).
- “[Estado de gestión de parches](#)” en la página [348](#).
- “[Estado de Data Control](#)” en la página [306](#).
- “[Estado del cifrado](#)” en la página [389](#).
- “[Listados del módulo Licencias](#)” en la página [147](#).
- “[Hardware](#)” en la página [182](#).

La funcionalidad también es accesible desde el listado de Equipos en el menú superior Equipos, haciendo clic en una rama del árbol de carpetas o filtros situado en el panel lateral.



Las opciones **Reinstalar la protección (requiere reinicio)** y **reinstalar agente** solo se mostrarán en equipos compatibles con esta funcionalidad.

Descubrimiento de equipos a reinstalar

Utiliza el listado **Equipos no administrados descubiertos** para localizar los dispositivos en los que es necesario realizar la reinstalación. Consulta “[Visualizar equipos descubiertos](#)” en la página [120](#).

Reinstalación en un equipo

- Localiza en el listado el equipo a reinstalar.
- En el menú de contexto asociado al equipo selecciona la opción **Reinstalar la protección (requiere**

reinicio)  o **Reinstalar el agente** , se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta "[Ventana de selección Reinstalar la protección](#)" y "[Ventana de selección Reinstalar el agente](#)".

Reinstalación en varios equipos

- Marca con las casillas de selección en el listado los equipos que reinstalarán su protección o agente.
- Selecciona en la barra de herramientas la opción **Reinstalar la protección (requiere reinicio)**  o **Reinstalar el agente** . Se mostrará una ventana donde el administrador configurará el tipo de reinstalación. Consulta "[Ventana de selección Reinstalar la protección](#)" y "[Ventana de selección Reinstalar el agente](#)".

Ventana de selección Reinstalar la protección

Al configurar la reinstalación de la protección se muestra una ventana flotante con dos opciones:

- **Reinstalar la protección inmediatamente (requiere reinicio):** el reinicio se producirá en el plazo de 1 minuto. Si el equipo de destino no está accesible en ese momento por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Panda Adaptive Defense 360 durante 1 hora.
- **Ofrecer un margen de tiempo antes de forzar la reinstalación:** el reinicio se producirá en el plazo configurado por el administrador. Si el equipo de destino no está accesible por encontrarse apagado o fuera de red, la petición de reinicio se mantendrá en el servidor Panda Adaptive Defense 360 durante 7 días.

En el momento en que el administrador inicia la reinstalación de la protección, el usuario del equipo recibe un mensaje emergente dándole la posibilidad de reiniciar el equipo en ese momento, o esperar a que finalice el tiempo definido por el administrador. Una vez que ha expirado el plazo, la protección se desinstalará y el equipo se reiniciará de forma automática para reinstalar la protección.

Si la desinstalación de la protección presenta algún tipo de problema, Panda Adaptive Defense 360 iniciará de forma transparente al usuario un desinstalador genérico que tratará de desinstalar nuevamente la protección y limpiar cualquier rastro en el equipo. Para ello es posible que se requiera un reinicio adicional.

Ventana de selección Reinstalar el agente

Al configurar la reinstalación del agente se muestra una ventana flotante que solicita la información siguiente:

- **Seleccionar el equipo con el rol de descubridor desde el cual se reinstalará el agente:**
 - Asegúrate de que el equipo descubridor se encuentra en el mismo segmento de red que el equipo a reinstalar.
 - Si el equipo descubridor está apagado, la petición se encolará hasta que sea visible de nuevo.

Las peticiones se encolan por un intervalo de 1 hora, transcurrido el cual se descartarán.

- **Credenciales para reinstalar los equipos:** introduce una o varias credenciales de instalación. Utiliza una cuenta de administración local del equipo o del dominio al que pertenece para completar la reinstalación con éxito.

Una vez introducida la información, el equipo con el rol de descubridor seguirá los pasos mostrados a continuación:

- Conectará con el equipo a reinstalar.
- Desinstalará el agente instalado en el equipo a reinstalar.
- Descargará un nuevo agente preconfigurado con el cliente, grupo y la configuración de red asignada al equipo, lo copiará y lo ejecutará remotamente en el equipo a reinstalar.
- Si hay algún problema en el transcurso de la operación se lanzará el desinstalador genérico y, si es necesario, se mostrará un mensaje al usuario con una cuenta atrás para el reinicio del equipo automático y un botón para reiniciar de forma manual e inmediata.

Códigos de error

Consulta "[Errores en el proceso de reinstalación del software de protección](#)" en la página [192](#) para obtener un listado de los mensajes de error y las acciones recomendadas para corregirlos.

Capítulo 7

Licencias

Para proteger los equipos de la red de las amenazas es necesario contratar licencias de Panda Adaptive Defense 360 en un número igual al número de puestos de usuario y servidores a proteger. Una licencia de Panda Adaptive Defense 360 solo se puede asignar a un único dispositivo en un momento concreto.

A continuación se detalla el proceso de gestión de licencias de Panda Adaptive Defense 360: su asignación a los equipos de la red, liberación y comprobación de su estado.

CONTENIDO DEL CAPÍTULO

- Definiciones y conceptos clave - - - - - 142**
 - Mantenimientos 142
 - Estado de los equipos 142
 - Estado de las licencias y grupos 142
 - Tipos de licencias 143
- Asignar licencias - - - - - 143**
 - Asignación automática 143
 - Asignación manual 143
- Liberar licencias - - - - - 144**
 - Liberación automática 144
 - Liberación manual 144
- Procesos asociados a la asignación de licencias - - - - - 144**
 - Caso I: Equipos con licencia asignada y equipos excluidos 144
 - Caso II: Equipos sin licencia asignada 145
- Paneles / widgets del módulo licencias - - - - - 146**
 - Acceso al panel de control 146
 - Permisos requeridos 146
 - Licencias 146
- Listados del módulo Licencias - - - - - 147**
 - Acceso al listado 147
 - Permisos requeridos 148
 - Licencias 148
- Licencias caducadas - - - - - 150**
 - Mensajes de caducidad próxima y vencida 150
 - Lógica de liberación de licencias caducadas 151
- Buscar equipos según su estado de licencia - - - - - 151**

Definiciones y conceptos clave

Para interpretar correctamente la información y las gráficas suministradas por Panda Adaptive Defense 360 que reflejan el estado de las licencias del producto es necesario conocer los términos mostrados en este apartado.



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

Mantenimientos

Las licencias contratadas por el cliente se agrupan en mantenimientos. Un mantenimiento es un conjunto de licencias con características comunes:

- **Tipo de Producto:** Panda Adaptive Defense 360, Panda Full Encryption, Panda Patch Management, Panda Adaptive Defense 360 con Panda Advanced Reporting Tool, Panda Adaptive Defense 360 con Panda Data Control, Panda Adaptive Defense 360 con Panda Advanced Reporting Tool y Panda Data Control.
- **Licencias contratadas:** número de licencias que pertenecen al mantenimiento.
- **Tipo de licencias:** NFR, Trial, Comercial, Suscripción.
- **Caducidad:** Fecha en la que las todas las licencias del mantenimiento caducan y los equipos dejarán de estar protegidos.

Estado de los equipos

Desde el punto de vista de las licencias, Panda Adaptive Defense 360 distingue tres estados en los equipos de la red:

- **Equipos con licencia:** equipos con una licencia válida en uso asignada.
- **Equipos sin licencia:** equipos que no tienen una licencia en uso, pero que son candidatos a tenerla.
- **Excluidos:** equipos que no compiten por la obtención de una licencia. Estos equipos no están ni estarán protegidos por Panda Adaptive Defense 360 aunque haya licencias sin asignar disponibles. Los equipos excluidos se seguirán mostrando en la consola y podrás utilizar algunas funcionalidades de gestión. Para excluir un equipo es necesario liberar su licencia de forma manual.



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

Estado de las licencias y grupos

Las licencias contratadas pueden tener dos estados:

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

Las licencias se agrupan por su estado en dos grupos:

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

Tipos de licencias

- **Licencias comerciales:** son las licencias estándar de Panda Adaptive Defense 360. Un equipo con una licencia comercial asignada tiene acceso a toda la funcionalidad del producto licenciado.
- **Licencias de prueba (Trial):** son licencias gratuitas de prueba, válidas por un periodo limitado de 30 días. Un equipo con una licencia de prueba asignada tiene acceso completo a la funcionalidad del producto.
- **Licencias NFR:** licencias Not For Resale, destinadas a personal interno y partners de Panda Security. No está permitida su venta ni uso por personal o partners ajenos a Panda Security.
- **Licencias de tipo suscripción:** licencias que no tienen fecha de caducidad. El servicio es de tipo "pago por uso".

Asignar licencias

Puedes asignar licencias de forma manual o automática.



Consulta "[Gestión de equipos y dispositivos](#)" en la [página 159](#) para obtener más información acerca de la herramienta de búsqueda y del árbol de carpetas y árbol de filtros.

Asignación automática

Al instalar el software Panda Adaptive Defense 360 en un equipo de la red, y siempre que existan licencias sin utilizar, el sistema le asignará de forma automática una licencia libre.

Asignación manual

Sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a asignar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar la ventana de detalle.
- En la pestaña **Detalles**, **Licencias** se mostrará el estado **Sin licencias**. Haz clic en el icono  y se asignará de forma automática una licencia libre.

Liberar licencias

Liberar una licencia es un proceso equivalente a la asignación de licencias.

Liberación automática

- Al desinstalar el software Panda Adaptive Defense 360 de un equipo de la red, el sistema recupera de forma automática una licencia y la devuelve al grupo de licencias sin usar.
- Al caducar un mantenimiento se liberan automáticamente licencias de los equipos siguiendo la lógica de licencias caducadas explicadas en “[Lógica de liberación de licencias caducadas](#)”.

Liberación manual

La liberación manual de una licencia asignada previamente a un equipo lo convierte en un equipo excluido. Aunque existan licencias libres, estas no son asignadas al equipo de forma automática.

Para liberar manualmente una licencia de Panda Adaptive Defense 360 de un equipo de la red sigue los pasos mostrados a continuación.

- En el menú superior **Equipos** localiza el dispositivo a liberar la licencia mediante el árbol de carpetas, el árbol de filtros o la herramienta de búsqueda.
- Haz clic en el equipo para mostrar su información.
- En la pestaña **Detalles, Licencias** se mostrará el estado del equipo. Haz clic en el icono  para liberar la licencia y devolverla al grupo de licencias sin utilizar.

Procesos asociados a la asignación de licencias

Caso I: Equipos con licencia asignada y equipos excluidos

Por defecto, a cada nuevo equipo integrado en la plataforma Aether se le asigna una licencia de producto Panda Adaptive Defense 360 de forma automática, pasando a tomar el estado de **equipo con licencia asignada**. Este proceso se repite hasta que el grupo de licencias sin usar número quede reducido a 0.

Al retirar una licencia de un equipo de forma manual, éste toma el estado de **equipo excluido**. A partir de ese momento el equipo no competirá por la asignación de una licencia de forma automática, en el caso de existir licencias sin usar.

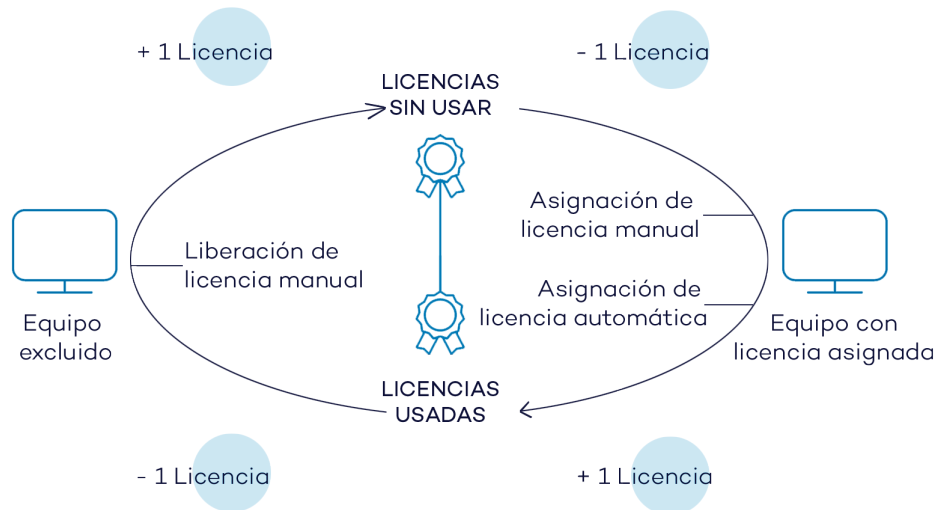


Figura 7.1: Modificación de los grupos de licencias en equipos con licencia asignada y excluidos

Caso II: Equipos sin licencia asignada

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

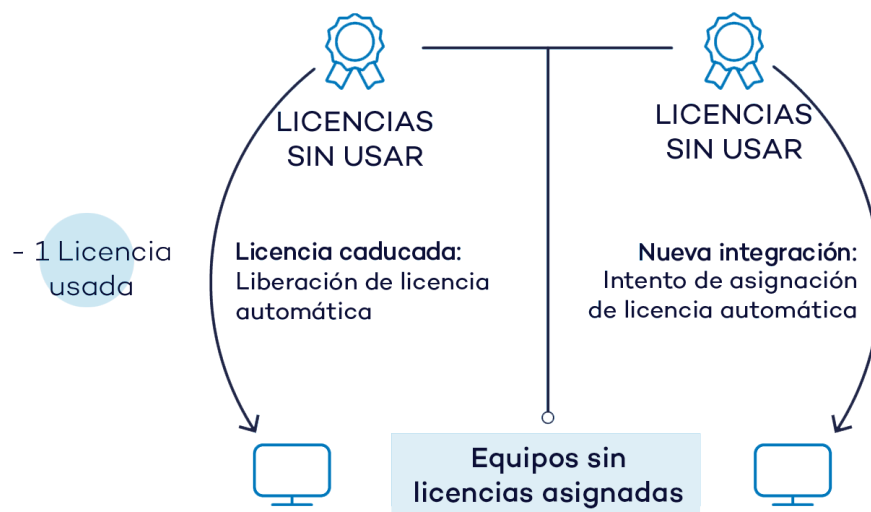


Figura 7.2: Equipos sin licencia asignada por caducar su mantenimiento y estar vacío el grupo de licencias sin usar

De la misma forma, en el momento en que una licencia asignada caduque, un equipo de la red pasará al estado **Sin licencia asignada**, siguiendo la lógica de licencias caducadas explicadas el “[Lógica de liberación de licencias caducadas](#)”.

Paneles / widgets del módulo licencias

Acceso al panel de control

Para acceder haz clic en el menú superior **Estado**, panel lateral **Licencias**.

Permisos requeridos

No se necesitan permisos adicionales para acceder a los widgets asociados al panel de licencias.

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

Licencias

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

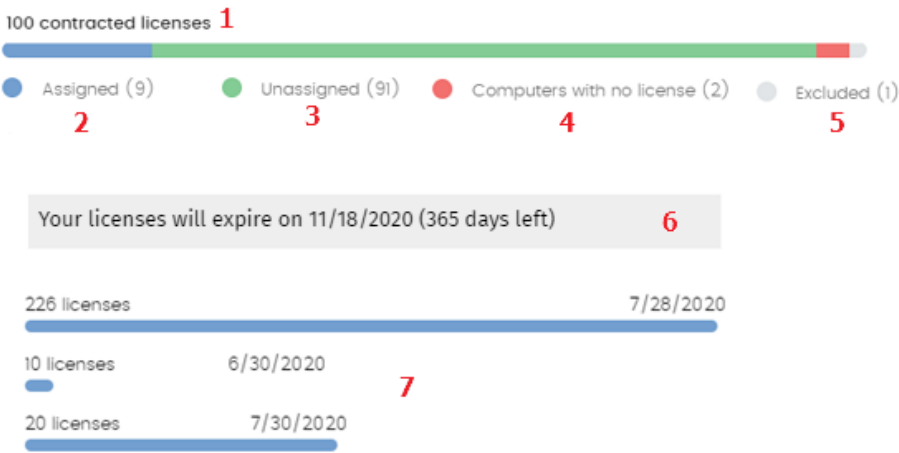


Figura 7.3: Panel de licencias mostrando tres mantenimientos

• Significado de las series

Zona activa	Descripción
Número de licencias contratadas totales (1)	Número máximo de equipos que se pueden proteger, en el caso de que todas las licencias contratadas sean asignadas.
Número de licencias asignadas (2)	Número de equipos protegidos con una licencia asignada.

Tabla 7.1: Descripción de las series de Licencias

Zona activa	Descripción
Número de licencias sin asignar (3)	Número de licencias contratadas pero que no se han asignado a ningún equipo y por lo tanto están sin utilizar.
Número de equipos sin licencia (4)	Equipos no protegidos por no disponer de licencias suficientes. El sistema les asignará licencia de forma automática si se adquieren nuevas licencias.
Número de equipos excluidos (5)	Equipos sin licencia asignada que no son candidatos a tenerla.
Caducidad de las licencias (6)	Si existe un único mantenimiento contratado, todas las licencias caducarán a la vez, en la fecha indicada.
Caducidad por mantenimiento (7)	Si un mismo producto ha sido contratado varias veces a lo largo del tiempo se mostrará una gráfica de barras horizontales con las licencias asociadas a cada contrato / mantenimiento y su fecha de caducidad independiente.

Tabla 7.1: Descripción de las series de Licencias

- **Filtros preestablecidos desde el panel**

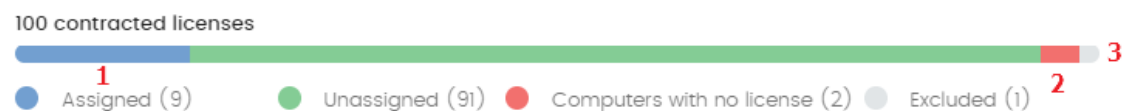


Figura 7.4: Zonas activas del panel licencias contratadas

Se muestra el listado **Licencias** con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro del panel:

Campo para filtrar	Valor
(1) Estado de licencia	Asignada
(2) Estado de licencia	Sin licencia
(3) Estado de licencia	Excluido

Tabla 7.2: Filtros del listado de licencias

Listados del módulo Licencias

Acceso al listado

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Licencias** y en el widget.
- ó
- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.

- Selecciona el listado **Licencias** de la sección **General** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

El acceso al listado **Licencias** no requiere permisos adicionales para el administrador.

Licencias

Muestra en detalle el estado de las licencias de los equipos de la red e incorpora filtros que ayudan a localizar los puestos de trabajo o dispositivos móviles en función de su estado.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	•  Licencia asignada •  Equipo sin licencia •  Equipo excluido
Última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security.	Fecha.

Tabla 7.3: Campos del listado Licencias

- **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el producto.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Servidor • Dispositivo móvil
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

Tabla 7.4: Campos del fichero exportado Licencias

Campo	Descripción	Valores
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.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o esta virtualizado.	Booleano
Versión del agente	Versión interna del componente agente que forma parte del software de cliente Panda Adaptive Defense 360.	Cadena de caracteres
Versión de la protección	Versión interna del componente protección que forma parte del software de cliente Panda Adaptive Defense 360.	Cadena de caracteres
Fecha de arranque del sistema	Fecha en la que el equipo se inició por última vez.	Fecha
Fecha instalación	Fecha en la que el software Panda Adaptive Defense 360 se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security.	Fecha
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • No asignada • Excluido
Grupo	Carpeta dentro del árbol de carpetas de Panda Security a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres

Tabla 7.4: Campos del fichero exportado Licencias

• **Herramienta de filtrado**

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Tipo de equipo	Finalidad del equipo en la red de la organización.	• Estación • Portátil • Servidor • Dispositivo móvil

Tabla 7.5: Campos de filtrado para el listado Licencias

Campo	Descripción	Valores
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Estado de licencia	Estado en el que se encuentra el equipo con respecto al sistema de licencias.	• Asignada • Sin licencia • Excluido

Tabla 7.5: Campos de filtrado para el listado Licencias

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta ["Información de equipo"](#) en la página 189 para obtener más información.

Licencias caducadas

Excepto los mantenimientos de tipo suscripción, todos los demás tienen asignada una fecha de caducidad, pasada la cual los equipos de la red dejarán de estar protegidos.

Mensajes de caducidad próxima y vencida

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

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



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

Lógica de liberación de licencias caducadas

Panda Adaptive Defense 360 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 posteriormente se reparten entre los equipos de la red.

En el momento en que un mantenimiento caduca, Panda Adaptive Defense 360 determina el número de licencias asignadas a ese mantenimiento. Acto seguido, se ordenan los equipos de la red con licencias asignadas utilizando como criterio de ordenación el campo **Última conexión**, que contiene la fecha en la que el equipo se conectó por última vez a la nube de Panda Security.

Los equipos candidatos a retirar su licencia de protección son aquellos no vistos en el periodo de tiempo más alejado. Así, se establece un sistema de prioridades donde la mayor probabilidad de retirar una licencia 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 Panda Adaptive Defense 360 que tengan licencias asignadas.

Buscar equipos según su estado de licencia

Panda Adaptive Defense 360 incluye la categoría **Licencia** para crear filtros que ayuden a localizar los equipos de la red que tengan un determinado estado de licencia.



Consulta "[Crear y organizar filtros](#)" en la página [164](#) para obtener más información acerca de cómo crear un filtro en Panda Adaptive Defense 360.

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

Categoría	Propiedad	Valor	Descripción
Licencia	Estado		Establece filtros según el estado de la licencia.
		Asignada	Lista los equipos con una licencia Panda Adaptive Defense 360 asignada.
		Sin asignar	Lista los equipos que no tiene una licencia Panda Adaptive Defense 360 asignada.

Tabla 7.6: Campos del listado Equipos protegidos

Categoría	Propiedad	Valor	Descripción
		Desasignada manualmente	El administrador de la red liberó la licencia Panda Adaptive Defense 360 previamente asignada al equipo.
		Desasignada automáticamente	El sistema liberó al equipo la licencia Panda Adaptive Defense 360 asignada previamente.

Tabla 7.6: Campos del listado Equipos protegidos

Capítulo 8

Actualización del software cliente

Panda Adaptive Defense 360 es un servicio cloud gestionado, y por lo tanto el administrador de la red 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 cliente instalado en los equipos de la red.

CONTENIDO DEL CAPÍTULO

Módulos actualizables en el software cliente	153
Actualización del motor de protección	154
Actualizaciones	154
Aplicar actualizaciones en rangos de horas	155
Aplicar actualizaciones en fechas determinadas	155
Reinicio de equipos	155
Actualización del agente de comunicaciones	156
Actualización del conocimiento	156
Dispositivos Windows, Linux y macOS	156
Dispositivos Android	156

Módulos actualizables en el software cliente

Los elementos instalados en el equipo del usuario son:

- Agente de comunicaciones Aether Platform.
- Motor de la protección Panda Adaptive Defense 360.
- Archivo de identificadores / fichero de firmas.

Dependiendo de la plataforma a actualizar, el procedimiento y las posibilidades de configuración varían tal y como se indica en la tabla 8.1.

Módulo	Plataforma			
	Windows	macOS	Linux	Android
Agente Panda	Bajo demanda			
Protección Panda Adaptive Defense 360	Configurable	Configurable	Configurable	No
Archivo de identificadores	Habilitar / Deshabilitar	Habilitar / Deshabilitar	Habilitar / Deshabilitar	No

Tabla 8.1: Formas de actualización según el componente del software cliente

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

Actualización del motor de protección

Para configurar la actualización del motor de protección crea y asigna un perfil de configuración de tipo **Ajustes por equipo**, accesible desde el menú superior **Configuración**, en el panel de la izquierda de la consola de administración.

Actualizaciones

Para habilitar la actualización automática del módulo de protección Panda Adaptive Defense 360 haz clic en el botón de activación **Actualizar automáticamente Panda Adaptive Defense 360 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 se aplicará la actualización:

- **En cualquier fecha:** las actualizaciones se aplicarán el día que estén disponibles. Esta opción no limita la actualización de Panda Adaptive Defense 360 a fechas concretas.
- **Los siguientes días de la semana:** utiliza las casillas de selección para establecer los días de la semana en los que Panda Adaptive Defense 360 se actualizará. La actualización se producirá el primer día de la semana que coincida con la selección del administrador en caso de haber una actualización disponible.
- **Los siguientes días del mes:** utiliza los desplegables para establecer un rango de días hábiles dentro del mes en los que Panda Adaptive Defense 360 se actualizará. La actualización se producirá el primer día del mes que coincida con los seleccionados por el administrador en caso de haber una actualización disponible.
- **Los siguientes días:** utiliza los desplegables para establecer un rango de días hábiles dentro del calendario en los que Panda Adaptive Defense 360 se actualizará. Los rangos definidos en esta opción se establecen de forma absoluta para casos en que el administrador quiera establecer rangos que no se repiten en el tiempo. De esta forma, se permite definir rangos de fechas concretas de actualización, pasadas las cuales dejan de tener efecto. Este método requiere redefinir los rangos de actualización de forma constante una vez hayan vencido.

Reinicio de equipos

Panda Adaptive Defense 360 permite definir la lógica de reinicios en caso de que sea necesario, mediante el desplegable situado al final de la pantalla de configuración:

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

Actualización del agente de comunicaciones

La actualización del agente Panda se ejecuta bajo demanda. Panda Adaptive Defense 360 incluirá una notificación en la consola de administración indicando la existencia de una nueva versión del agente, y el administrador podrá lanzar la actualización cuando lo desee.

La actualización del agente Panda no requiere reinicio del equipo del usuario y suele implicar cambios y mejoras en la consola de administración que facilitan la gestión de la seguridad.

Actualización del conocimiento

La configuración de la actualización del fichero de firmas en Panda Adaptive Defense 360 se realiza en el perfil de configuración de seguridad asignado al equipo, según sea su tipo.

Dispositivos Windows, Linux y macOS

La configuración se realiza en los perfiles de tipo **Estaciones y Servidores**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

En la pestaña **General** las opciones disponibles son:

- **Actualizaciones automáticas de conocimiento:** habilita o deshabilita la descarga del fichero de firmas. Si se deshabilita el fichero de firmas nunca será actualizado.



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

- **Realizar un análisis en segundo plano cada vez que se actualice el conocimiento:** lanza de forma automática un análisis cada vez que un fichero de firmas se descarga en el equipo. El análisis tendrá prioridad mínima para no interferir en el trabajo del usuario.

Dispositivos Android

La configuración se realiza en los perfiles **Dispositivos Android**, accesibles desde el panel de la izquierda en el menú superior **Configuración**.

Panda Adaptive Defense 360 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.



Parte 4

Gestión de los dispositivos de la red

Capítulo 9: Gestión de equipos y dispositivos

Capítulo 10: Gestión de configuraciones

Capítulo 11: Configuración remota del agente

Capítulo 9

Gestión de equipos y dispositivos

La consola web muestra los dispositivos administrados de forma ordenada y flexible, aplicando distintas estrategias que permiten localizarlos rápidamente para facilitar su gestión.

Para que un equipo de la red sea gestionable por Panda Adaptive Defense 360 se requiere como mínimo de la instalación del agente Panda en el equipo. Los equipos sin licencia pero con el agente Panda instalado, aparecerán en la consola de administración, aunque su protección estará desactualizada y no podrán ejecutar tareas, análisis ni otras acciones vinculadas con el servicio de protección.

CONTENIDO DEL CAPÍTULO

La zona equipos	161
Mostrar equipos en subgrupos	161
El panel Árbol de equipos	161
Árbol de filtros	162
Definición de filtro	162
Filtros predefinidos	163
Crear y organizar filtros	164
Crear carpetas	164
Crear filtros	164
Borrar filtros y carpetas	164
Mover y copiar filtros y carpetas	165
Renombrar filtros y carpetas	165
Configurar filtros	165
Reglas de filtrado	166
Operadores lógicos	166
Agrupaciones de reglas de filtrado	167
Casos de uso comunes	167
Equipos Windows según el procesador instalado (x86, x64, ARM64)	167
Equipos sin parches instalados	167
Equipos sin conectar con la nube de Panda Security en X días	168
Equipos aislados	168
Integración con otras herramientas de gestión	168
Árbol de grupos	168
Definición de grupo	169
Tipos de grupos	169
Grupos de Directorio Activo	170
Crear y organizar grupos	170

Crear grupos	170
Borrar grupos	171
Mover grupos	171
Renombrar grupos	171
Importar reglas de asignación por IPs en grupos ya creados	171
Exportar reglas de asignación por IPs	172
Mover equipos entre grupos	172
Mover conjuntos de equipos a grupos	172
Mover un único equipo a un grupo	173
Mover equipos desde grupos Active Directory	173
Mover equipos hacia grupos Active Directory	173
Restaurar la pertenencia de varios equipos a su grupo Active Directory	173
Filtrar resultados por grupos	174
Configurar el filtro de resultados por grupos	174
Tareas de análisis y desinfección	174
Análisis inmediato	174
Análisis programado	174
Listados disponibles para gestionar equipos - - - - -	175
El panel Listado de equipos	175
Acceso al listado	175
Permisos requeridos	175
Equipos	175
El panel Mis listados	182
Acceso al panel Mis listados	182
Permisos requeridos	182
Hardware	182
Software	184
Equipos con nombre duplicado	186
Información de equipo - - - - -	189
Sección general (1)	190
Sección alertas de equipo (2)	190
Sección general en dispositivos Android	196
Sección Detalles (3)	197
Seguridad	198
Protección de datos	199
Sección Hardware (4)	202
Sección Software (5)	203
Herramienta de búsqueda	203
Instalaciones y desinstalaciones	203
Sección Configuración (6)	204
Barra de acciones (7)	205
Iconos ocultos (8)	205

La zona equipos

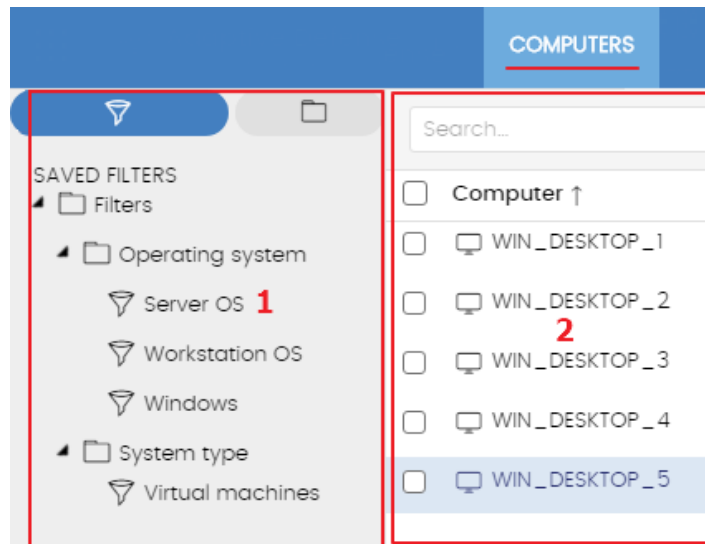


Figura 9.1: Vista general de los paneles en la zona Equipos

La zona **Equipos** es el área de la consola web donde se gestionan los dispositivos integrados en Panda Adaptive Defense 360.

Para acceder a la ventana de administración de equipos, haz clic en el menú superior **Equipos**. Se mostrarán dos zonas diferenciadas: el panel lateral con el **árbol de equipos (1)** y el panel central con el **listado de equipos (2)**. Ambos paneles trabajan de forma conjunta: al seleccionar una rama del árbol de equipos, el listado de equipos se actualiza con

todos sus equipos asignados.

Mostrar equipos en subgrupos

Para ampliar o limitar el listado de los equipos activa o desactiva la opción **Mostrar equipos de los subgrupos** disponible en el menú de contexto general.

- Si la opción está activada, al seleccionar una rama del árbol se mostrarán todos los equipos que pertenecen a ella y a todas las ramas de orden inferior.
- Si la opción está desactivada, al seleccionar una rama del árbol se mostrarán únicamente todos los equipos que pertenecen a ella.

El panel Árbol de equipos

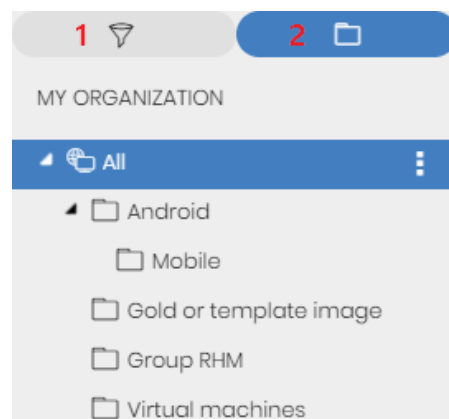


Figura 9.2: El panel Árbol de equipos

Panda Adaptive Defense 360 representa la estructura de equipos mediante el **Árbol de equipos**, que presenta dos vistas o árboles independientes:

- **Árbol de filtros (1)**: gestiona los equipos de la red mediante agrupaciones dinámicas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma automática.
- **Árbol de grupos (2)**: gestiona los equipos de la red mediante agrupaciones estáticas. La pertenencia de un equipo a una agrupación de este tipo se establece de forma manual.

Los dos árboles muestran el parque de dispositivos del cliente de distintas formas, con el objeto de favorecer la ejecución de tareas de diferentes tipos, tales como:

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



Para localizar equipos desprotegidos o de características determinadas relativas a la seguridad o al estado de la protección consulta “[Visibilidad del malware y del parque informático](#)” en la página 411. Para asignar perfiles de configuración de seguridad consulta “[Asignación manual y automática de configuraciones](#)” en la página 215. Para ejecutar tareas de resolución de problemas consulta “[Herramientas de resolución](#)” en la página 525.

Al pasar el puntero del ratón por las ramas del árbol de filtros y de grupos se muestra el icono de menú de contexto. Haz clic para desplegar un menú emergente con todas las operaciones disponibles sobre la rama del árbol seleccionada.

Árbol de filtros

Es una de las dos vistas del Árbol de equipos, y permite agrupar de forma dinámica los equipos en la red mediante reglas y condiciones que describen características de los dispositivos. Estas reglas se pueden combinar mediante operaciones lógicas para producir expresiones complejas.

Para acceder al Árbol de filtros haz clic en el icono del filtro  desde el panel de la izquierda. Al hacer clic en los diferentes elementos del árbol, el panel de la derecha se actualiza, presentando todos los equipos que cumplen con los criterios establecidos en el filtro seleccionado.

Definición de filtro

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



Un equipo puede pertenecer a más de un filtro.

Un filtro está constituido por un conjunto de reglas o condiciones que los equipos tendrán que satisfacer para pertenecer a aquél. En la medida en que el equipo cumpla con las características descritas formará parte del filtro; de la misma forma, cuando un equipo cambie su estado y no

cumpla los criterios de pertenencia, automáticamente dejará de formar parte de la agrupación descrita por el filtro.

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

Filtros predefinidos

Panda Adaptive Defense 360 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
Estaciones y servidores	Tipo de sistema	Lista los equipos físicos de sobremesa o servidores.
Portátiles	Tipo de sistema	Lista los equipos físicos portátiles.
Móviles y tablets	Tipo de sistema	Lista los dispositivos de tipo smartphone y tablet.
Virtuales	Tipo de sistema	Lista los equipos virtualizados.
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.
Linux	Sistema operativo	Lista todos los equipos con sistema operativo Linux 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.
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.

Tabla 9.1: Listado de filtros predefinidos

Nombre	Grupo	Descripción
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 9.1: Listado de filtros predefinidos

Crear y organizar filtros

Para crear y organizar filtros haz clic en el icono de menú de contexto de las ramas del árbol de filtros. Se mostrará un menú emergente con las opciones permitidas en esa rama en particular.

Crear carpetas

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



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

Crear filtros

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

- Selecciona el menú de contexto de la carpeta en el árbol donde será creado el filtro.
 - Si deseas crear una estructura jerárquica de filtros, crea carpetas contenedoras y mueve los filtros dentro de ellas. Una carpeta puede contener otras carpetas con filtros.
- Haz clic en **Añadir filtro**.
- Introduce el nombre del filtro. No es necesario que sea un nombre único. El resto de la configuración se detalla en "[Configurar filtros](#)".

Borrar filtros y carpetas

Para borrar un filtro o una carpeta haz clic en el menú de contexto de la rama a borrar y elige la opción **Eliminar**. La rama se borrará junto a todos sus descendientes.



No se permite borrar el nodo raíz Filtros.

Mover y copiar filtros y carpetas

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



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

Renombrar filtros y carpetas

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



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

Configurar filtros

Haz clic en el menú de contexto del filtro y elige la entrada **Editar filtro** del menú. Se mostrará la ventana de configuración de filtros.

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

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

The screenshot shows the 'Edit filter' interface with the following components:

- Block 1:** A text input field labeled 'Name:' containing 'sample filter'.
- Block 2:** A filter rule entry showing 'Computer' category, 'Name' property, 'Is equal to' operator, and 'Desktop-Luci' value.
- Block 3:** A dropdown menu showing the logical operator 'AND'.
- Block 4:** A list of filter rules with checkboxes. The first rule is selected, showing 'Hardware' category, 'CPU - Manufacturer' property, 'Contains' operator, and 'Intel' value. Below it is an 'OR' operator and another rule for 'Software' category, 'Installation date' property, 'Before' operator, and '9/17/2018' value.

Buttons at the bottom include 'Group', '+ New condition', 'OK', and 'Cancel'.

Figura 9.3: Vista general de configuración de un filtro

- **Nombre del filtro (1):** identifica al filtro.
- **Reglas de filtrado (2):** construye condiciones indivisibles de pertenencia al filtro. Una regla de filtrado únicamente comprueba una característica concreta de los equipos de la red.
- **Operadores lógicos (3):** combina dos reglas de filtrado mediante los operadores lógicos Y o O.
- **Agrupaciones (4):** varían el orden de evaluación de las reglas de filtrado configuradas y relacionadas mediante operadores lógicos.

Reglas de filtrado

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

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

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

Operadores lógicos

Para combinar dos reglas en un mismo filtro se utilizan los operadores lógicos Y y O. Al añadir una segunda regla y sucesivas a un filtro se mostrará de forma automática un desplegable con los operadores lógicos disponibles, que se aplicarán a las reglas adyacentes.

Agrupaciones de reglas de filtrado

Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores que relacionan las reglas de filtrado introducidas.

Para encerrar dos o más reglas en un paréntesis crea una agrupación marcando con las casillas de selección las reglas que formarán parte del grupo y haz clic en el botón **Agrupación**. Se mostrará una línea delgada que abarcará las reglas de filtrado que forman parte de la agrupación.

Mediante el uso de paréntesis se definen agrupaciones de varios niveles para poder anidar grupos de operandos en una expresión lógica.

Casos de uso comunes

A continuación se indican a modo de ejemplo algunos casos de uso de filtros muy utilizados por los administradores de redes:

Equipos Windows según el procesador instalado (x86, x64, ARM64)

Lista los equipos que tienen instalado el sistema operativo Windows y su microprocesador pertenece a la familia ARM.

Este filtro se compone de dos condiciones unidas mediante el operador Y:

- **Condición 1:**
 - **Categoría:** Equipo
 - **Propiedad:** Plataforma
 - **Condición:** Es igual a
 - **Valor:** Windows
- **Condición 2:**
 - **Categoría:** Equipo
 - **Propiedad:** Arquitectura
 - **Condición:** Es igual a
 - **Valor:** {nombre de la arquitectura: ARM64, x86, x64}

Equipos sin parches instalados

Lista los equipos que no tienen un determinado parche instalado. Consulta "[Panda Patch Management \(Actualización de programas vulnerables\)](#)" en la página 325 para obtener más información sobre Panda Patch Management.

- **Categoría:** Programas
- **Propiedad:** Nombre del software

- **Condición:** No contiene
- **Valor:** {Nombre del parche}

Equipos sin conectar con la nube de Panda Security en X días

Lista los equipos que no conectaron con la nube de Panda Security en el intervalo configurado:

- **Categoría:** Equipo
- **Propiedad:** Última conexión
- **Condición:** Antes de
- **Valor:** {Fecha en formato dd/mm/aa}

Equipos aislados

Lista los equipos que han sido aislados de la red. Consulta [“Aislar un equipo”](#).

- **Categoría:** Equipo
- **Propiedad:** Estado de aislamiento
- **Condición:** Es igual
- **Valor:** Aislado

Integración con otras herramientas de gestión

Muestra los equipos que coinciden con alguno de los nombres de equipo especificados en un listado obtenido por una herramienta de terceros. Cada línea del listado deberá terminar con un retorno de carro y será considerada como un nombre de equipo.

- **Categoría:** Equipo
- **Propiedad:** Nombre
- **Condición:** En
- **Valor:** listado de nombres de equipo

Árbol de grupos

El árbol de grupos reúne de forma estática los equipos en la red en las agrupaciones definidas por el administrador.

Para acceder al árbol de grupos:

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

Definición de grupo

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



El máximo nivel de profundidad del árbol es 10.

Tipos de grupos

Tipo de grupo	Descripción
Grupo raíz	Grupo padre del que cuelgan el resto de carpetas.
Grupos nativos	Grupos estándar de Panda Adaptive Defense 360 que soportan todas las operaciones (movimiento, renombrado, borrado etc.) Pueden contener otros grupos nativos y equipos.
Grupos IP	Grupo nativo con IPs o rangos de IPs asociados para acelerar la integración de nuevos equipos en el servicio de seguridad.
Grupos Directorio Activo	Replican la estructura del Directorio Activo instalado en la empresa, por esta razón tienen limitadas algunas operaciones. Pueden contener otros grupos de Directorio Activo y equipos.
Grupo raíz del directorio activo	Abarca todos los dominios del Directorio Activo configurados en la red de la organización. Contiene grupos de dominio Directorio Activo.
Grupo de dominio Active Directory	Ramas del Directorio Activo que representan dominios. Contienen otros grupos de dominio Directorio Activo, grupos Directorio Activo y equipos.

Tabla 9.2: Tipos de grupos en Panda Adaptive Defense 360

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



En un momento determinado un equipo solo puede pertenecer a un grupo, a diferencia de los filtros donde un equipo puede pertenecer a varios simultáneamente.

Grupos de Directorio Activo

Para las organizaciones que tienen instalado un servidor de Directorio Activo en la red, Panda Adaptive Defense 360 puede obtener de forma automática la estructura configurada y replicarla en el árbol de grupos: los agentes Panda reportan a la consola Web el grupo del Directorio Activo al que pertenecen y, conforme se despliegan los agentes en los equipos, el árbol se completará con las distintas unidades organizativas. De esta manera, bajo la rama  se presentará una distribución de los equipos familiar para el administrador, con el objeto de acelerar la localización de dispositivos y su gestión.

Para mantener la coherencia entre el Directorio activo de la empresa y el árbol representado en la consola de administración, los grupos de directorio activo no son modificables desde la consola de Panda Adaptive Defense 360: únicamente cambiarán cuando lo haga la estructura de Directorio Activo de la empresa. Los cambios se replicarán en la consola Web de Panda Adaptive Defense 360 transcurrido un máximo de una hora.

Si el administrador de la red mueve en la consola de Panda Adaptive Defense 360 un equipo que reside en un grupo de tipo Directorio Activo a un grupo nativo o al grupo raíz se romperá la sincronización con el Directorio Activo de la empresa. Cualquier cambio de grupo en el Directorio Activo de la empresa que afecte a ese equipo no se replicará en la consola de Panda Adaptive Defense 360.

Para restablecer la sincronización de un equipo y así continuar replicando la estructura original del Directorio Activo de la empresa en la consola de Panda Adaptive Defense 360 consulta "[Restaurar la pertenencia de varios equipos a su grupo Active Directory](#)".

Crear y organizar grupos

Para acceder a las operaciones disponibles sobre grupos haz clic en el icono de menú de contexto de las ramas del árbol de grupos. Se mostrará un menú emergente con las opciones permitidas para esa rama en particular.

Crear grupos

- Selecciona el menú de contexto del grupo padre del cual dependerá el grupo a crear, y haz clic en **Añadir grupo**.
- Introduce el nombre del grupo en la caja de texto **Nombre** y haz clic en el botón Añadir.



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

Si deseas que los equipos sobre los cuales se va a instalar un agente Panda Adaptive Defense 360 se muevan a un determinado grupo según su IP sigue los pasos mostrados a continuación:

- Haz clic en el enlace **Añadir reglas de asignación automática por IPs**, se mostrará una caja de texto donde añadir las IPs de los equipos que serán movidos al grupo.
- Especifica IPs individuales separadas por comas o rangos de IPs separados por un guion.

El movimiento del equipo se efectuará únicamente en el momento de la instalación del agente Panda Adaptive Defense 360. Si posteriormente el equipo cambia de IP éste permanecerá en el grupo asignado inicialmente.

Borrar grupos

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



No se permite borrar el nodo raíz Todos.

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

Mover grupos

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



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

Renombrar grupos

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



No es posible renombrar el grupo raíz Todos ni grupos Directorio Activo.

Importar reglas de asignación por IPs en grupos ya creados

Para añadir direcciones IP a un grupo nativo ya creado sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo nativo que no sea el grupo Todos y haz clic en la

opción **Importar reglas de asignación por IPs**. Se mostrará una ventana para poder arrastrar un fichero con las direcciones IP.

- El fichero deberá contener una o más líneas de texto con el formato mostrado a continuación:

- Para direcciones IP independientes añadir una línea por cada una de ellas a asignar:

```
.\Grupo\Grupo\Grupo (tabulación) IP
```

- Para rangos de IPs, añadir una línea por cada rango a asignar:

```
.\Grupo\Grupo\Grupo (tabulación) ExtremoInferiorIP-ExtremoSuperiorIP
```

- Todos las rutas indicadas son interpretadas por Panda Adaptive Defense 360 como relativas a la rama del árbol seleccionada.
- Si los grupos indicados en el fichero no existieran, Panda Adaptive Defense 360 los creará y asignará la direcciones IP indicadas.
- Haz clic en **Importar**. Las IPs se asignarán a los grupos indicados en el fichero y el árbol de grupos actualizará sus iconos para mostrar el cambio de tipo de grupo.



Las direcciones IP previamente asignadas a un grupo IP se borrarán al importar un fichero con nuevos pares grupo - IP.

Una vez terminado el procedimiento, todos los equipos nuevos que se integren en Panda Adaptive Defense 360 se moverán al grupo indicado según su dirección IP.

Exportar reglas de asignación por IPs

Para exportar un fichero con las reglas de grupos IP ya asignadas sigue los pasos mostrados a continuación:

- Selecciona el menú de contexto de un grupo IP, y haz clic en la opción **Exportar reglas de asignación por IPs**. Se descargará un fichero .csv con las reglas de asignación de IPs establecidas en el grupo IP y en todos sus descendientes.
- El formato del fichero .csv es el indicado en el punto "[Importar reglas de asignación por IPs en grupos ya creados](#)".

Mover equipos entre grupos

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

Mover conjuntos de equipos a grupos

- Selecciona el grupo **Todos** para listar todos los equipos administrados o utiliza la herramienta de búsqueda para localizar los equipos a mover.
- Selecciona con las casillas los equipos en el panel de listado de equipos.

- Haz clic en el icono  situado a la derecha de la barra de búsqueda. Se mostrará un menú desplegable con la opción **Mover a**. Haz clic para mostrar el árbol de grupos destino.
- Selecciona el grupo destino del árbol de grupos mostrado.

Mover un único equipo a un grupo

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

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

Mover equipos desde grupos Active Directory

Un equipo que reside en un grupo Directorio Activo está sincronizado con el Directorio Activo de la empresa y por tanto no es posible moverlo a otro grupo de tipo Directorio Activo desde la consola de Panda Adaptive Defense 360. En este caso será necesario mover el equipo en el Directorio Activo de la empresa y esperar como máximo 1 hora hasta que la consola Panda Adaptive Defense 360 se sincronice. Sin embargo, un equipo que reside en un grupo de tipo Directorio Activo sí puede moverse a un grupo nativo.



Al mover un equipo desde un grupo de tipo Directorio Activo a un grupo nativo se dejarán de sincronizar los cambios del grupo de origen. Consulta "[Grupos de Directorio Activo](#)".

Mover equipos hacia grupos Active Directory

No es posible mover un equipo desde un grupo nativo a un grupo Directorio Activo específico. El único movimiento que se permite es mover el equipo al grupo de tipo Directorio Activo en el que reside dentro del servidor de Directorio Activo de la empresa. Para ello haz clic en el menú de contexto del equipo y selecciona **Mover a su ruta de Active Directory**.

Restaurar la pertenencia de varios equipos a su grupo Active Directory

Para restablecer la pertenencia de equipos a su grupo Directorio Activo original haz clic en el menú de contexto de un grupo de Directorio Activo y selecciona la opción **Recuperar los equipos de esta rama de Active Directory**. Todos los equipos que pertenecen a ese grupo en el Directorio Activo de la

empresa y que el administrador movió a otros grupos dentro de la consola Panda Adaptive Defense 360 serán devueltos a su grupo original.

Filtrar resultados por grupos

La función de filtrar resultados por grupos muestra en la consola únicamente la información generada por los equipos de la red que pertenecen a los grupos elegidos por el administrador. Es una forma rápida de establecer un filtro que afecta de forma transversal a toda la consola (listados, paneles de control y configuraciones) y que ayuda a resaltar los datos de interés para el administrador.

Configurar el filtro de resultados por grupos

Para configurar el filtrado de resultados por grupos sigue los pasos mostrados a continuación:

- Haz clic en el botón del menú superior. Se desplegará una ventana con el árbol de grupos.
- Selecciona los grupos que se mostrarán de entre el árbol de equipos y pulsa en el botón **Aceptar**.

La consola mostrará únicamente la información generada de los equipos que pertenecen a los grupos seleccionados.



Figura 9.4: Filtrar resultados por grupos

Filtrar equipos no afecta a la visibilidad de tareas, ni al envío de alertas por email, ni al envío programado de informes ejecutivos.

Tareas de análisis y desinfección

El árbol de grupos permite asignar tareas de análisis inmediatas o programadas a todos los equipos que pertenecen a un grupo y a sus grupos descendientes.



Para ampliar el detalle de los tipos de análisis consulta la sección “[Opciones de análisis](#)” en la página [530](#).

Análisis inmediato

Haz clic en la entrada **Analizar ahora** para lanzar un análisis inmediato sobre los equipos que pertenecen al grupo o a alguno de los subgrupos. Se mostrará una ventana con el tipo de análisis a ejecutar: **Todo el ordenador** o **Áreas críticas**.

Análisis programado

Haz clic en la entrada **Programar análisis** para crear una tarea programada de análisis.

Listados disponibles para gestionar equipos

El panel Listado de equipos

Acceso al listado

- Haz clic en el menú superior **Equipos**. Se mostrará el panel lateral izquierdo el árbol de equipos o de carpetas y en el panel lateral derecho un listado con todos los equipos administrados en la red.
- Haz clic en un elemento del árbol de grupos o de filtros en el panel lateral izquierdo. El panel derecho se refrescará con el contenido del elemento seleccionado.

Computer ↑	IP address	Group	Operating system	Last connection
☐ WIN_DESKTOP_1	192.168.0.162	Workstation	Windows 7 Enterprise	4/10/2018 5:41:52 AM
☐ WIN_DESKTOP_2	192.168.0.86	Workstation	Windows 8.1 Enterprise SP4	4/10/2018 5:41:52 AM
☐ WIN_DESKTOP_3	192.168.0.19	Workstation	Windows Server 2012 R2 Datacenter	4/10/2018 5:41:53 AM
☐ WIN_DESKTOP_4	192.168.0.202	Workstation	Windows Server 2008 R2 Enterprise	4/10/2018 5:41:55 AM
☐ WIN_LAPTOP_1	192.168.0.164	Laptop	Windows Small Business Server 2003 SP2	4/10/2018 5:41:54 AM
☐ WIN_SERVER_1	192.168.0.40	SUPPORT	Windows 2003 Web SP2	4/7/2018 5:41:51

25 rows 1 to 12 of 12

Figura 9.5: El panel Listado de equipos

Permisos requeridos

El acceso al panel **Listado de equipos** no requiere permisos adicionales para el administrador.

Equipos

El listado de equipos muestra los puestos de usuario y servidores correspondientes al grupo o filtro seleccionado en el árbol de equipos. Además, incluye herramientas que permiten gestionar uno o varios equipos simultáneamente.

A continuación, se muestra un esquema del panel listado de equipos:

- **(1)** Listado de equipos que pertenecen a la rama del árbol seleccionada.
- **(2) Herramienta de búsqueda:** localiza equipos por su nombre, descripción, dirección IP o último usuario registrado, admitiendo coincidencias parciales sin tener en cuenta mayúsculas y minúsculas.
- **(3)** Menú de contexto general: aplica una misma acción a varios equipos.

- **(4)** Casillas de selección de equipos.
- **(5)** Sistema de paginación en la parte inferior del panel.
- **(6)** Menú de contexto del equipo.

El listado de equipos es configurable para poder adaptar la información mostrada a las necesidades del administrador.

Para añadir o quitar columnas haz clic en el menú de contexto  situado en la parte superior derecha y elige la opción **Añadir o eliminar columnas**. Se mostrarán las columnas disponibles y el enlace

Columnas por defecto  para restaurar la configuración del listado a sus valores iniciales.

Por cada equipo se incluye la información mostrada a continuación:

Campo	Descripción	Valores
Equipo	Nombre del equipo y su tipo.	Cadena de caracteres: •  Puesto de trabajo o servidor •  Equipo portátil •  Dispositivo móvil (smartphone o tablet Android)
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Ruta del directorio Activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Dirección IP •  Equipo en proceso de entrar en aislamiento •  Equipo aislado •  Equipo en proceso de salir del aislamiento
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo y su tipo.	Cadena de caracteres: •  Grupo •  Grupo IP

Tabla 9.3: Campos del Listado de equipos

Campo	Descripción	Valores
		•  Dominio AD o raíz del Directorio Activo •  Unidad Organizativa •  Raíz del árbol de grupos
Sistema operativo	Nombre y versión del sistema operativo instalado en el equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado del equipo a la nube de Panda Security.	Fecha
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres

Tabla 9.3: Campos del Listado de equipos

• **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Lista separada por comas de todas las direcciones IP de las tarjetas instaladas en el equipo.	Cadena de caracteres
Direcciones físicas (MAC)	Lista separada por comas 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 Panda Adaptive Defense 360 a la que pertenece el equipo	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Fecha arranque del sistema	Fecha en la que se inicio el equipo por última vez.	Fecha

Tabla 9.4: Campos del fichero exportado Listado de equipos

Campo	Descripción	Valores
Fecha de instalación	Fecha en la que el Software Panda Adaptive Defense 360 se instaló con éxito en el equipo.	Fecha
Fecha de última conexión	Fecha más reciente en la que el equipo contactó con la nube.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Máquina virtual	Indica si el equipo es físico o está virtualizado.	Booleano
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o por el contrario se regenera a su estado original.	Booleano
Servidor Exchange	Versión del servidor de correo instalada en el servidor.	Cadena de caracteres
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de última actualización	Fecha de la última actualización de la protección.	Fecha
Licencias	Producto licenciado en el equipo.	Panda Adaptive Defense 360
Configuración de red	Nombre de la configuración de red que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de red.	Cadena de caracteres
Seguridad para estaciones y servidores	Nombre de la configuración de seguridad que afecta al puesto de trabajo o servidor.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
Seguridad para dispositivos Android	Nombre de la configuración de seguridad que afecta al dispositivo móvil.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguridad.	Cadena de caracteres
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.	Cadena de caracteres

Tabla 9.4: Campos del fichero exportado Listado de equipos

Campo	Descripción	Valores
Data Control	Nombre de la configuración de seguimiento de información personal (Panda Data Control) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de seguimiento de información personal.	Cadena de caracteres
Gestión de parches	Nombre de la configuración de parcheo (Panda Patch Management) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de parcheo.	Cadena de caracteres
Cifrado	Nombre de la configuración de cifrado (Panda Full Encryption) que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de cifrado.	Cadena de caracteres
Bloqueo de programas	Nombre de la configuración de programas bloqueados por el administrador que afecta al equipo.	Cadena de caracteres
Configuración heredada de	Nombre de la carpeta donde fue asignada la configuración de bloqueo de programas.	Cadena de caracteres
Estado de aislamiento	Muestra el estado del aislamiento del equipo.	• Aislado • Aislado • Dejando de aislar • No aislado
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Último usuario logueado	Nombres de las cuentas de usuario separados por coma que mantienen una sesión interactiva abierta en equipos Windows.	Cadena de caracteres
Acción solicitada	Petición pendiente de ejecutar o en ejecución.	• Reinicio • Reinstalación de protección • Reinstalación de agente
Error en la acción solicitada	Tipo de error reportado en la acción solicitada.	• Credenciales incorrectas • Equipo descubridor no disponible

Tabla 9.4: Campos del fichero exportado Listado de equipos

Campo	Descripción	Valores
		- No es posible conectar con el equipo - Sistema operativo no soportado - No es posible descargar el instalador del agente - No es posible copiar el instalador del agente - No es posible desinstalar el agente - No es posible instalar el agente - No es posible registrar el agente - Requiere intervención del usuario
Último proxy utilizado	Método de acceso empleado por Panda Adaptive Defense 360 en su última conexión con la nube de Panda Security. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.	Cadena de caracteres

Tabla 9.4: Campos del fichero exportado Listado de equipos

• Herramientas de filtrado

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres.

Tabla 9.5: Filtros disponibles en el listado Equipos

• Herramientas de gestión

Al marcar uno o más equipos con las casillas de selección (4), la herramienta de búsqueda (2) se oculta para mostrarse en su lugar la barra de Acciones (7).



Figura 9.6: Barra de acciones solapando a la herramienta de búsqueda

Al hacer clic en la casilla de selección situada a la altura de la cabecera de la tabla **(4)** se marcarán todos los equipos de la página actual del listado y se mostrará el mensaje **Seleccionar las xx** filas del listado, que permite marcar todos los equipos del listado independientemente de la paginación.

Acción	Descripción
 Actualizar información del equipo	Fuerza el envío desde el agente instalado en el equipo de la siguiente información: • Comprobación de acciones pendientes. • Comprobación de tareas. • Comprobación de configuraciones aplicadas. • Envío de información de estado. Este icono solo se muestra en los equipos que tienen activada la funcionalidad Comunicación en tiempo real . Consulta " Configuración de la comunicación en tiempo real " en la página 231.
 Mover a	Muestra una ventana con el árbol de grupos. Elige un grupo como destino de los equipos seleccionados. Los equipos heredarán las configuraciones asignadas al grupo de destino. Consulta " Crear y gestionar configuraciones " en la página 213.
 Mover a su ruta de directorio activo	Mueve los equipos seleccionados al grupo que se corresponde con la unidad organizativa del directorio activo de la empresa.
 Eliminar	Borra el equipo de la consola y desinstala el software de cliente Panda Adaptive Defense 360. Consulta " Desinstalar el software " en la página 135.
 Analizar ahora	Consulta " Tareas de análisis y desinfección " para una introducción a las tareas de análisis o " Tareas " para una descripción completa.
 Programar análisis	Consulta " Tareas de análisis y desinfección " para una introducción a las tareas de análisis o " Tareas " en la página 539 para una descripción completa.
 Reiniciar	Reinicia el equipo. Consulta " Reiniciar equipos " en la página 533.
 Aislar equipo	Impide todas las comunicaciones del equipo excepto las necesarias para conectar con la nube de Panda Security. Consulta " Aislar uno o varios equipos de la red de la organización " en la página 535.
 Dejar de aislar equipo	Restaura las comunicaciones del equipo. Consulta " Quitar el aislamiento de un equipo " en la página 536.
 Programar instalación de parches	Consulta " Panda Patch Management (Actualización de programas vulnerables) " para obtener información sobre cómo instalar parches en equipos Windows.
 Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Consulta " Reinstalación remota " en la página 138 para obtener más información.
 Seleccionados	Anula la selección actual de equipos.

Tabla 9.6: Herramientas para gestionar equipos

El panel Mis listados

Acceso al panel Mis listados

- Haz clic en el menú superior **Estado** y en el panel lateral **Mis listados**. Se mostrará una ventana con todos los listados disponibles.
- Selecciona en el grupo **General** el listado **Hardware**, **Software** o **Equipos con nombre duplicado**.



Consulta "[Gestión de listados](#)" en la página 56 para obtener información sobre los tipos de listados y como operar con ellos.

Consulta el capítulo correspondiente al grupo al que pertenece cada listado para obtener información acerca de sus campos y de las herramientas de filtrado y búsqueda que implementan.

Permisos requeridos

El acceso al panel **Mis listados** no requiere permisos adicionales para el administrador.

Hardware

Contiene los componentes hardware instalados en cada equipo del parque informático. Un mismo componente hardware se mostrará de forma independiente cada vez que sea detectado en un equipo.

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo que contiene el componente hardware.	Cadena de caracteres: • Puesto de trabajo o servidor. • Equipo portátil. • Dispositivo móvil (smartphone o tablet Android).
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
CPU	Marca y modelo del microprocesador instalado en el equipo. Se indica el número de núcleos / cores instalados entre paréntesis.	Cadena de caracteres
Memoria	Cantidad total de memoria RAM instalada.	Cadena de caracteres
Capacidad de disco	Suma de la capacidad de todos los discos duros internos conectados al equipo.	Cadena de caracteres

Tabla 9.7: Campos del Listado de hardware

Campo	Descripción	Valores
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha
Menú de contexto	Herramientas de gestión. Consulta " Herramientas de gestión " en la página 180.	

Tabla 9.7: Campos del Listado de hardware

• Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Sistema	Nombre del modelo hardware del equipo.	Cadena de caracteres
CPU-X	Marca, modelo y características de la CPU numerada X.	Cadena de caracteres
CPU-X Número de núcleos	Número de núcleos o cores de la CPU numerada X.	Numérico

Tabla 9.8: Campos del fichero exportado Hardware

Campo	Descripción	Valores
CPU-X Número de procesadores lógicos	Número de núcleos lógicos mostrados al sistema operativo por el sistema de HyperThreading / SMT (Simultaneous MultiThreading).	Numérico
Memoria	Suma de todos los bancos de memoria RAM instalados en el equipo.	Cadena de caracteres
Disco-X Capacidad	Espacio total del medio de almacenamiento interno numerado X.	Cadena de caracteres
Disco-X Particiones	Numero de particiones reportadas al sistema operativo del medio de almacenamiento interno numerado X.	Numérico
Versión de especificación del TPM	Versiones de las APIs compatibles con el chip TPM.	Cadena de caracteres
BIOS - número de serie	Número de serie de la BIOS del equipo.	Cadena de caracteres

Tabla 9.8: Campos del fichero exportado Hardware

• **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Marca del sistema operativo.	• Windows • Android

Tabla 9.9: Filtros disponibles en el Listado de hardware

Software

Contiene todos los programas instalados en los equipos de la red. Por cada paquete se indica el número de equipos que lo tienen instalado e información sobre la versión y su fabricante.

Al hacer clic en un paquete software se abrirá el **"Equipos"** en la página **175** filtrado por el paquete seleccionado, para mostrar los equipos que lo tienen instalado.

Campo	Descripción	Valores
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres

Tabla 9.10: Campos del Listado de software

Campo	Descripción	Valores
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 9.10: Campos del Listado de software

• **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Versión	Versión interna del paquete software.	Cadena de caracteres
Equipos	Número de equipos que contienen el paquete encontrado.	Numérico

Tabla 9.11: Campos del Listado de software

• **Campos mostrados en el excel de detalle**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Equipo que contiene el paquete encontrado.	Numérico
Nombre	Nombre del paquete software encontrado en el parque.	Cadena de caracteres
Editor	Fabricante del paquete software.	Cadena de caracteres
Fecha de instalación	Fecha en la que se instaló el software.	Fecha
Tamaño	Tamaño del software instalado.	Numérico
Versión	Versión interna del paquete software.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 9.12: Campos del listado exportado de detalle

- **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Marca del sistema operativo.	• Windows • Linux • macOS • Android

Tabla 9.13: Filtros disponibles en el Listado de software

- **Ventana listado de equipos**

Al hacer clic en una de las filas del listado se mostrará el listado de equipos filtrado por el paquete de software seleccionado. Consulta **"Equipos"** en la página **175** para obtener más información.

Equipos con nombre duplicado

Muestra los equipos detectados en la red con el mismo nombre y que pertenecen al mismo dominio. De cada grupo de equipos duplicados Panda Adaptive Defense 360 considerará correcto el equipo con la fecha de conexión a la nube de Panda Security más reciente, y el resto como erróneos. El equipo considerado correcto se excluirá del listado para que el administrador seleccione y elimine el resto de equipos de una vez.

Para eliminar los equipos duplicados selecciónalos mediante las casillas de selección y la opción **Eliminar** del menú de herramientas. Se mostrará una ventana preguntando si quieres desinstalar el agente Panda Adaptive Defense 360 o no.



Borrar equipos del listado **Equipos con nombre duplicado** sin desinstalar el agente Panda Adaptive Defense 360 únicamente los borra de la consola de Panda Adaptive Defense 360. Un equipo así eliminado volverá a aparecer en la consola de Panda Adaptive Defense 360 al ponerse en contacto con la nube. Ante un borrado masivo de equipos sin tener la seguridad de cuales están realmente duplicados se recomienda no desinstalar previamente el agente de ningún equipo y comprobar qué equipos reaparecen en la consola.

Campo	Descripción	Valores
Equipo	Nombre y tipo del equipo	Cadena de caracteres: •  Puesto de equipo o servidor •  Equipo portátil. •  Dispositivo móvil (smartphone o tablet Android).
Dirección IP	Dirección principal del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel del parche aplicado.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 ala nube de Panda Security.	Fecha

Tabla 9.14: Campos del Listado de Equipos con nombre duplicado

• **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del agente instalado en el equipo.	Cadena de caracteres

Tabla 9.15: Campos del fichero exportado Equipos con nombre duplicado

Campo	Descripción	Valores
Versión de la protección	Versión interna del módulo de protección instalado en el equipo.	Cadena de caracteres
Fecha de instalación	Fecha en la que el Software Panda Adaptive Defense 360 se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha
Plataforma	Tipo de sistema operativo instalado.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Directorio Activo	Ruta completa del equipo en el Directorio Activo de la empresa.	Cadena de caracteres
Servidor Exchange	Versión del servidor de correo instalada en el servidor.	Cadena de caracteres
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.	Cadena de caracteres
Fecha arranque del sistema	Fecha en la que se inició el equipo por última vez.	Fecha

Tabla 9.15: Campos del fichero exportado Equipos con nombre duplicado

• **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Plataforma	Marca del sistema operativo.	• Todos • Windows • Linux • macOS • Android
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días

Tabla 9.16: Filtros disponibles en el listado Equipos con nombre duplicado

Campo	Descripción	Valores
		• Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días

Tabla 9.16: Filtros disponibles en el listado Equipos con nombre duplicado

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta ["Información de equipo"](#) para obtener más información.

Información de equipo

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

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



Figura 9.7: Vista general de la información de equipo

- **General (1):** información que ayuda a identificar el equipo.
- **Alertas de equipo (2):** mensajes con problemas potenciales asociados al equipo.
- **Detalles (3):** resumen ampliado del hardware, software y seguridad configurada en el equipo.
- **Hardware (4):** hardware instalado en el equipo, componentes y periféricos conectados, su consumo y uso.
- **Software (5):** paquetes de software instalados en el equipo, su versión y un registro de cambios.
- **Configuración (6):** configuraciones de seguridad y otras asignadas al equipo.
- **Barra de herramientas (7):** agrupa las operaciones disponibles para aplicar sobre el equipo

administrado.

- **Iconos ocultos (8)**: si la ventana no es lo suficientemente grande, parte de las herramientas se ocultan agrupadas.

Sección general (1)

Contiene la siguiente información para todos los tipos de dispositivo:

Campo	Descripción
Nombre del equipo e icono indicando el tipo de equipo	Nombre del equipo.
IP	Dirección IP del equipo.
Ruta del directorio activo	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 instalado en el equipo.
Rol del equipo	Indica si el equipo hace las funciones de descubridor, caché o proxy.

Tabla 9.17: Campos de la sección general de la información del equipo

Sección alertas de equipo (2)

Las alertas describen los problemas encontrados en los equipos de la red en lo que respecta al funcionamiento de Panda Adaptive Defense 360 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.

Equipos aislados

Alerta	Descripción	Referencia
Equipo aislado	El administrador ha aislado el equipo y se bloquean todas las conexiones excepto aquellas necesarias para el buen funcionamiento de Panda Adaptive Defense 360.	Consulta " Aislar un equipo " en la página 534 .
Estamos intentando aislar este equipo	El servidor Panda Adaptive Defense 360 está tratando de aislar el equipo pero la operación todavía no se ha completado por estar el equipo apagado o sin conexión a Internet.	Consulta el widget " Equipos sin conexión " en la página 415 .

Tabla 9.18: Alertas relacionadas con la funcionalidad de aislar equipos

Alerta	Descripción	Referencia
Estamos intentando dejar de aislar este equipo	El servidor Panda Adaptive Defense 360 está tratando de retirar el aislamiento del equipo pero la operación todavía no se ha completado por estar el equipo apagado o sin conexión a Internet.	Consulta el widget " Equipos sin conexión " en la página 415 .

Tabla 9.18: Alertas relacionadas con la funcionalidad de aislar equipos

Licencias

Alerta	Descripción	Referencia
Equipo sin licencia	No hay licencias libres para asignar al equipo. Retira una licencia asignada o adquiere más licencias de Panda Adaptive Defense 360.	Consulta " Liberar licencias " en la página 144 .
	Hay licencias libres pero no se han asignado a este equipo.	Consulta " Asignar licencias " en la página 143 .

Tabla 9.19: Alertas relacionadas con la asignación de licencias

Errores en el proceso de instalación del software de protección



Los errores ocurridos durante el proceso de instalación del software de protección se refleja mediante un código de error, su código extendido de error asociado y un subcódigo extendido de error, si están disponibles. Consulta la tabla [19.22](#) para más información.

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha producido un error instalando la protección en el equipo. En el caso de errores de origen conocido se mostrará una descripción de la causa que lo motiva. Si el origen es desconocido se mostrará el código de error asociado.	Consulta " Requisitos de instalación " en la página 109 .
	El equipo requiere un reinicio para completar la instalación debido a una desinstalación previa.	Consulta " Reiniciar equipos " en la página 533 .
Error instalando Data Control	Se ha producido un error instalando Panda Data Control en el equipo.	Consulta " Requisitos de Panda Data Control " en la página 274 .
Error instalando la protección y Data Control	Se ha producido un error instalando la protección y el módulo en el equipo.	Consulta " Requisitos de instalación " en la página 109 y " Requisitos de Panda Data Control " en la página 274 .

Tabla 9.20: Alertas relacionadas con la instalación del software Panda Adaptive Defense 360

Alerta	Descripción	Referencia
Error instalando el gestor de parches	Se ha producido un error instalando el módulo de gestión de parches.	Consulta “Comprobar que Panda Patch Management funciona correctamente” en la página 328.
Error instalando el módulo de cifrado	Se ha producido un error instalando el módulo de cifrado.	Consulta “Requisitos mínimos de Panda Full Encryption” en la página 376.
Error instalando el agente de Panda	Credenciales incorrectas.	Consulta “Instalación remota de equipos descubiertos” en la página 126.
	El equipo descubridor no está disponible.	Consulta el widget “Equipos sin conexión” en la página 415 y “Asignar el rol de descubridor a un equipo de la red” en la página 119.
	No es posible conectar con el equipo destinatario del paquete de instalación por estar apagado o no cumplir con los requisitos de hardware y de red.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de instalación” en la página 109.
	El sistema operativo del equipo no está soportado.	Consulta “Requisitos de instalación” en la página 109.
	No es posible descargar el instalador del agente por un fallo de red.	Consulta “Requisitos de red” en la página 111.
	No es posible copiar el instalador del agente en el equipo por falta de espacio.	Consulta “Requisitos por plataforma” en la página 110.
	No es posible instalar el agente por no cumplirse los requisitos de instalación remota o el equipo está apagado.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de instalación” en la página 109.
	No es posible registrar el agente.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de instalación” en la página 109.
Error comunicando con servidores.	El equipo no puede conectar con alguno de los servidores de la nube de Panda.	Para más información consulta “Requisitos de hardware, software y red” en la página 551.

Tabla 9.20: Alertas relacionadas con la instalación del software Panda Adaptive Defense 360

Errores en el proceso de reinstalación del software de protección



Los errores ocurridos durante el proceso de reinstalación del software de protección se reflejan mediante un código de error, su código extendido de error asociado y un subcódigo extendido de error, si están disponibles. Consulta la tabla 19.22 para más información.

Alerta	Descripción	Referencia
Pendiente de reinstalación de la protección	El administrador solicitó la reinstalación de la protección de este equipo pero todavía no se ha realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
Pendiente de reinstalación del agente	El administrador solicitó la reinstalación del agente en este equipo pero todavía no se ha realizado porque el equipo está apagado, sin conexión o porque todavía no ha terminado el plazo configurado antes de forzar el reinicio.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
Error instalando el agente de Panda	Credenciales incorrectas.	
	Equipo descubridor no disponible.	Consulta el widget “Equipos sin conexión” en la página 415
	No es posible conectar con el equipo por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
	Sistema operativo no soportado por no cumplir con los requisitos de instalación remota.	Consulta “Requisitos de la funcionalidad de reinstalación remota” en la página 138
	No es posible descargar el instalador del agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
	No es posible copiar el instalador del agente por no estar encendido o no cumplir los requisitos de instalación remota.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
	No es posible desinstalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
	No es posible instalar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
	No es posible registrar el agente por no estar encendido o no cumplir con los requisitos de instalación remota.	Consulta el widget “Equipos sin conexión” en la página 415 y “Requisitos de la funcionalidad de reinstalación remota” en la página 138
	Requiere intervención del usuario.	

Tabla 9.21: Alertas relacionadas con la reinstalación del agente Panda Adaptive Defense 360

Errores de funcionamiento del software Panda Adaptive Defense 360

Alerta	Descripción	Referencia
Equipo desprotegido	Se ha detectado un error en la protección de Exchange Server. Reinicia el equipo para solucionar el problema.	Consulta " Reiniciar equipos " en la página 533 .
Equipo desprotegido	Se ha detectado un error en las protecciones antivirus y avanzada. Reinicia el equipo para solucionar el problema.	Consulta " Reiniciar equipos " en la página 533 .
Error en Data Control	Se ha detectado un error en Panda Data Control. Reinicia el equipo para solucionar el problema.	Consulta " Reiniciar equipos " en la página 533 .
Error cifrando el equipo	No se puede cifrar el equipo por un error.	Consulta " Reiniciar equipos " en la página 533 .

Tabla 9.22: Alertas relacionadas con el mal funcionamiento del software Panda Adaptive Defense 360

Acción del usuario o del administrador pendiente

Alerta	Descripción	Referencia
Cifrado pendiente de acción del usuario	Para completar el proceso de cifrado es necesario que el usuario reinicie el equipo o introduzca las credenciales de cifrado.	Consulta " Reiniciar equipos " en la página 533 . Consulta " Proceso de cifrado y descifrado " en la página 377 .
Pendiente de reinicio	El administrador ha solicitado el reinicio de este equipo pero todavía no se ha completado por falta de conexión o por no haberse cumplido el plazo para ejecutar un inicio forzoso.	Consulta el widget " Equipos sin conexión " en la página 415 .
Reinstalando la protección	El administrador ha solicitado la reinstalación de la protección en este equipo y todavía no se ha completado por estar el equipo apagado, sin conexión, sin completar el plazo configurado antes del reinicio o por estar el proceso en curso.	Consulta " Reinstalación remota " en la página 138 .
Equipo desprotegido	La protección de Exchange Server está desactivada. Activa la protección.	Consulta " Asignación manual y automática de configuraciones " en la página 215 , " Crear y gestionar configuraciones " en la página 213 y " Antivirus para servidores Exchange " en la página 259 .

Tabla 9.23: Alertas relacionadas con la falta de acción del usuario o administrador de la red

Alerta	Descripción	Referencia
Equipo desprotegido	Las protecciones antivirus y avanzada están desactivadas. Activa la protección.	Consulta " Asignación manual y automática de configuraciones " en la página 215, " Crear y gestionar configuraciones " en la página 213 y " Antivirus " en la página 246 y " Protección avanzada " en la página 242.
Equipo sin conexión desde hace X días	Es posible que el equipo esté apagado o no se cumplan los requisitos de acceso a la red.	Consulta " Requisitos de red " en la página 111.
Protección desactualizada	La protección necesita que el usuario local reinicie manualmente el equipo para completar la instalación*.	* solo reproducible en las versiones Windows Home y Starter.
El administrador ha cambiado el estado de las protecciones desde la consola local	El administrador cambió la configuración de la protección desde el propio agente instalado en el equipo del usuario o servidor. De esta forma, la configuración actual no coincide con la establecida desde la consola web.	

Tabla 9.23: Alertas relacionadas con la falta de acción del usuario o administrador de la red

Equipo desactualizado

Alerta	Descripción	Referencia
Protección desactualizada	La protección requiere que el equipo se reinicie para terminar la actualización.	Consulta " Reiniciar equipos " en la página 533.
	Se ha producido un error intentando actualizar la protección. Comprueba que se cumplen los requisitos de hardware y de red.	Consulta " Requisitos de instalación " en la página 109 y el espacio disponible en disco en " Sección Hardware (4) ".
	Las actualizaciones están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta " Actualización del motor de protección " en la página 154.

Tabla 9.24: Alertas relacionadas con el software Panda Adaptive Defense 360 desactualizado

Alerta	Descripción	Referencia
Conocimiento sobre malware y otras amenazas desactualizado	Las actualizaciones de conocimiento están desactivadas para este equipo. Asigna un perfil de configuración con las actualizaciones activadas.	Consulta “ Actualización del conocimiento ” en la página 156.

Tabla 9.24: Alertas relacionadas con el software Panda Adaptive Defense 360 desactualizado

Sección general en dispositivos Android

En los dispositivos Android la sección general (1) y la sección de alertas de equipo (2) se sustituyen por el panel de antirrobo, que le permite al administrador lanzar acciones remotas sobre los dispositivos gestionados.



Consulta “[Antirrobo](#)” en la página 267 para activar la funcionalidad antirrobo en los dispositivos Android y la configuración del modo privado.

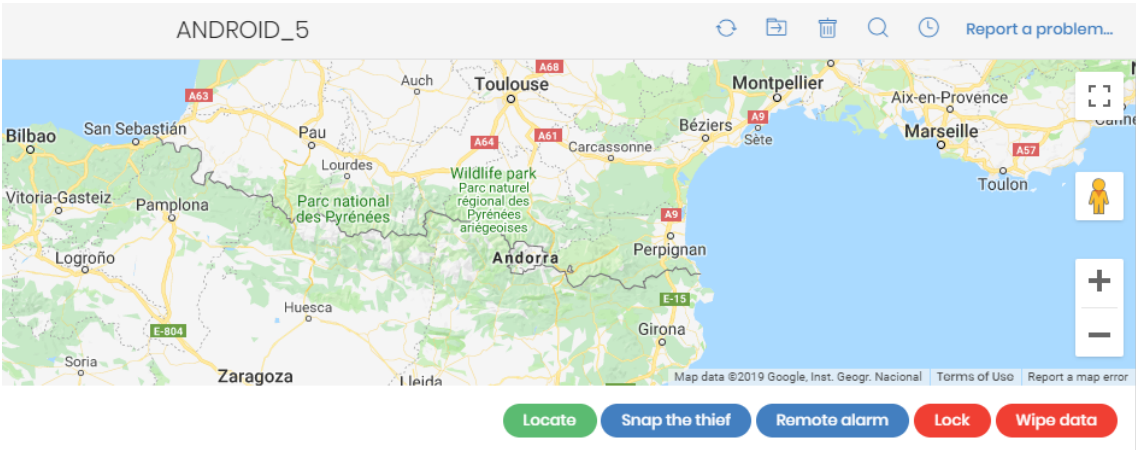


Figura 9.8: Panel de antirrobo mostrado en dispositivos Android

Las acciones disponibles son:

Acción	Descripción
Localizar	Modo privado activado: la consola muestra una ventana donde se solicita al administrador el número que el usuario del dispositivo tecleó al activar el modo privado. Si el número es correcto el servidor Panda Adaptive Defense 360 solicita al dispositivo sus coordenadas y el mapa de la consola se actualiza con la nueva posición. Modo privado desactivado: el servidor Panda Adaptive Defense 360 solicita directamente al dispositivo sus coordenadas y el mapa de la consola se actualiza con la nueva posición.

Tabla 9.25: Acciones soportadas por el módulo antirrobo para Android

Acción	Descripción
Foto al ladrón	Muestra una ventana donde el administrador puede introducir la dirección de correo a la que se enviará la fotografía y permite elegir el momento en el que se realizará: • Ahora: el agente Panda Adaptive Defense 360 enviará la fotografía a la cuenta de correo indicada en el momento de recibir la petición. • Al tocar la pantalla: el agente Panda Adaptive Defense 360 enviará la fotografía a la cuenta de correo indicada en el momento en que el usuario o el ladrón toquen la pantalla del terminal.
Alarma remota	Muestra una ventana donde el administrador podrá introducir un mensaje para el usuario y un número de contacto. Una vez enviada la petición el mensaje se mostrará en el dispositivo del usuario junto a la reproducción de un sonido al máximo volumen, aunque el dispositivo esté bloqueado. Haz clic en la casilla de selección No reproducir ningún sonido si únicamente quieres mostrar el mensaje.
Bloquear	La consola pide un código de 4 dígitos y acto seguido el dispositivo del usuario quedará bloqueado. Para desbloquearlo es necesario el código de 4 dígitos previamente establecido por el administrador.
Borrar datos	El dispositivo se formatea y se devuelve a su estado original, destruyendo todos los datos y aplicaciones que contenía.

Tabla 9.25: Acciones soportadas por el módulo antirrobo para Android

Sección Detalles (3)

La información se divide en los siguientes apartados:

- **Equipo:** información de la configuración del dispositivo ofrecida por el agente Panda.
- **Seguridad:** estado de las protecciones de Panda Adaptive Defense 360.
- **Protección de datos:** estado de los módulos que protegen el contenido de los datos almacenados en el equipo.

Equipo

Campo	Descripción
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.

Tabla 9.26: Campos de la sección detalles del equipo

Campo	Descripción
Grupo	Grupo dentro del árbol de grupos al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón Cambiar .
Sistema operativo	Sistema operativo instalado en el equipo.
Servidor de correo	Versión del servidor Microsoft Exchange instalada en el equipo.
Máquina virtual	Indica si el equipo es físico o esta virtualizado.
Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o por el contrario se regenera a su estado original.
Licencias	Licencias de productos de Panda Security instalados en el equipo. Consulta " Licencias " en la página 141 para más información.
Versión del agente	Versión interna del agente Panda instalado en el equipo.
Fecha de arranque del sistema	Fecha en la que se inició el equipo por ultima vez.
Fecha de instalación	Fecha en la que se instaló el sistema operativo del equipo por última vez.
Último proxy utilizado	Método de acceso empleado por Panda Adaptive Defense 360 en su ultima conexión con la nube de Panda Security. Este dato no se actualiza de forma inmediata y puede tardar hasta 1 hora en reflejar su valor correcto.
Última conexión del agente con la infraestructura Panda Security	Fecha de la última conexión del software de cliente con la nube de Panda Security. Como mínimo el agente de comunicaciones contactará cada 4 horas.
Último chequeo de la configuración	Fecha en la que Panda Adaptive Defense 360 comprobó por última vez la configuración en la nube de Panda Security en busca de cambios.
Último usuario logueado	Nombre de las cuentas de usuario propietarias de las sesiones activas en el equipo.

Tabla 9.26: Campos de la sección detalles del equipo

Seguridad

En esta sección se indican el estado (Activado, Desactivado, Error) de las distintas tecnologías de Panda Adaptive Defense 360 que protegen al equipo del malware.

Campo	Descripción
Protección avanzada	Protección frente a amenazas avanzadas, APTs y exploits.
Antivirus de archivos	Protección del sistema de ficheros.
Antirrobo	Acciones para mitigar la exposición de datos ante robos de dispositivos móviles Android.

Tabla 9.27: Campos de la sección detalles de la seguridad

Campo	Descripción
Antivirus de correo	Protección de los protocolos empleados en el envío y recepción de correos electrónicos.
Antivirus para navegación web	Protección frente al malware descargado de páginas web con el navegador instalado en el equipo.
Firewall	Protección frente a tráfico de red generado por aplicaciones.
Control de dispositivos	Protección frente a la infección mediante dispositivos externos de almacenamiento o que permiten conectar el equipo a Internet sin pasar por la infraestructura de comunicaciones de la organización (módems).
Control de acceso a páginas web	Protección frente a la navegación por páginas web no autorizadas por el administrador.
Gestión de parches	Instalación de parches y actualizaciones de sistemas operativos Windows y aplicaciones de terceros. Detección del estado del parcheo de los equipos y desinstalación de los parches problemáticos.
Bloqueo de programas	Bloqueo de la ejecución de los programas que el administrador considere peligrosos o no compatibles con la actividad desarrollada en la empresa.
Última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se publicaron nuevos parches.
Antivirus para servidores Exchange	Protección frente a virus recibidos en servidores Microsoft Exchange.
Anti-spam para servidores Exchange	Protección frente a los correos electrónicos no deseados en servidores Microsoft Exchange.
Filtrado de contenidos para servidores Exchange	Protección frente a los correos recibidos en servidores Microsoft Exchange que llevan ficheros adjuntos con extensiones peligrosas.
Versión de la protección	Versión interna del módulo de la protección instalado en el equipo.
Versión de actualización del conocimiento	Fecha de la última descarga del fichero de firmas en el equipo.

Tabla 9.27: Campos de la sección detalles de la seguridad

Protección de datos

En esta sección se indica el estado de los módulos que protegen los datos almacenados en el equipo.

Campo	Descripción
Seguimiento de información personal	Monitorización de los ficheros que contienen datos susceptibles de poder identificar a usuarios o clientes de la empresa (módulo Panda Data Control).

Tabla 9.28: Campos de la sección Protección de datos

Campo	Descripción
Permitir búsquedas de información en este equipo	Indica si el equipo tiene asignado un perfil de configuración que le permita recibir búsquedas de ficheros y reportar sus resultados.
Inventario de información personal	Si se permiten búsquedas de ficheros por contenido, es necesario que Panda Data Control examine todos los ficheros de los medios de almacenamiento soportados para recuperar su contenido y generar una base de datos.
Estado de indexación	• No indexado • Indexado • Indexado (solo el texto) • Indexado (todo el contenido) • Indexando
Cifrado de discos duros	Estado del módulo de cifrado: • No disponible: el equipo no es compatible con Panda Full Encryption. • Sin información: el equipo todavía no ha enviado información del módulo de cifrado. • Activado: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • Desactivado: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • Error: la configuración establecida por el administrador no permite aplicar un método de autenticación soportado por Panda Full Encryption en la versión del sistema operativo instalada en el equipo. • Error instalando: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • Sin licencia: el equipo no tiene una licencia de Panda Full Encryption asignada. Obtener la clave de recuperación: muestra una ventana con los identificadores de los medios de almacenamiento cifrados del equipo. Al hacer clic en cualquier de ellos se muestra la clave de recuperación. Consulta "Obtención de la clave de recuperación" en la página 382. Estado del proceso de cifrado: • Desconocido: alguna unidad no tiene un estado conocido. • Discos no cifrados: alguna de las unidades compatibles con la tecnología de cifrado no está cifrada ni en proceso de cifrado. • Discos cifrados: todas las unidades compatibles con la tecnología de cifrado están cifradas. • Cifrando: al menos una unidad del equipo está siendo cifrada.

Tabla 9.28: Campos de la sección Protección de datos

Campo	Descripción
	• Descifrando: al menos una unidad del equipo está siendo descifrada. • Cifrado por el usuario: todos los medios de almacenamiento se encuentran cifrados por el usuario. • Cifrado por el usuario (parcialmente): algunos de los medios de almacenamiento se encuentran cifrados por el usuario.
Método de autenticación	• Desconocido: método de autenticación no compatible con los soportados por Panda Patch Management. • Procesador de seguridad (TPM). • Procesador de seguridad (TPM) + Contraseña. • Contraseña: método de autenticación por PIN, PIN extendido o passphrase. • USB método de autenticación por llave USB. • Sin cifrar: ninguna de las unidades compatibles con la tecnología de cifrado está cifrada ni en proceso de cifrado.
Fecha de cifrado	Fecha del proceso de cifrado completado más antigua dentro de la primera vez que se cifró de forma total el equipo.
Cifrado de unidades de almacenamiento extraíbles	Estado del módulo de cifrado: • No disponible: el equipo no es compatible con Panda Full Encryption. • Sin información: el equipo todavía no ha enviado información del módulo de cifrado. • Activado: el equipo tiene asignada una configuración que establece el cifrado de sus dispositivos de almacenamiento y no se han producido errores. • Desactivado: el equipo tiene asignada una configuración que establece el descifrado de sus dispositivos de almacenamiento y no se han producido errores. • Error: la configuración establecida por el administrador no permite aplicar un método de autenticación soportado por Panda Full Encryption en la versión del sistema operativo instalada en el equipo. • Error instalando: error en la descarga o instalación de los ejecutables necesarios para gestionar el servicio de cifrado en caso de no estar disponibles previamente en el equipo. • Sin licencia: el equipo no tiene una licencia de Panda Full Encryption asignada. Ver dispositivos cifrados de este equipo: muestra una ventana con los identificadores de los medios de almacenamiento externos cifrados del equipo. Al hacer clic en cualquier de ellos se muestra la clave de recuperación. Consulta "Obtención de la clave de recuperación" en la página 382.

Tabla 9.28: Campos de la sección Protección de datos

Sección Hardware (4)

Contiene información sobre los recursos hardware instalados en el equipo:

Campo	Descripción	Valores
CPU	Información del microprocesador instalado en el equipo y serie temporal con el consumo de CPU en diferentes periodos e intervalos según la selección del desplegable.	- Intervalos de 5 minutos para la última hora. - Intervalos de 10 minutos para las 3 últimas horas. - Intervalos de 40 minutos para las últimas 24 horas.
Memoria	Información sobre las características de los chips de memoria instalados y serie temporal con el consumo de memoria en diferentes periodos e intervalos según la selección del desplegable.	- Intervalos de 5 minutos para la última hora. - Intervalos de 10 minutos para las 3 últimas horas. - Intervalos de 40 minutos para las últimas 24 horas.
Disco	Información sobre las características del sistema de almacenamiento masivo y un gráfico de tarta con el porcentaje de espacio libre y ocupado en el momento de la consulta.	- ID de dispositivo - Tamaño - Tipo - Particiones - Revisión de firmware - Número de serie - Nombre
BIOS	Información sobre la versión de la BIOS instalada en el equipo.	- Versión - Fecha de fabricación - Número de serie - Nombre - Fabricante
TPM	Información del chip de seguridad integrado en la placa base del equipo. Para poder ser utilizado por Panda Adaptive Defense 360 el TPM debe de estar activado, habilitado y ser propietario.	Versión del fabricante: versión interna del chip. Versión de especificación: versiones de las APIs compatibles. Versión Fabricante Activado: el TPM está preparado para recibir comandos. Se utiliza en sistemas con varios TPMs.

Tabla 9.29: Campos de la sección hardware de la información del equipo

Campo	Descripción	Valores
		• Habilitado: el TPM esta preparado para funcionar ya que ha sido activado desde la BIOS. • Propietario: el sistema operativo puede interactuar con el TPM.

Tabla 9.29: Campos de la sección hardware de la información del equipo

Sección Software (5)

Contiene información del software instalado en el equipo, de las actualizaciones del sistema operativo Windows y un histórico de sus movimientos.

Herramienta de búsqueda

- Introduce el nombre o editor en la caja de texto **Buscar** y pulsa la tecla Enter para efectuar una búsqueda. A continuación se muestra la información del software encontrado:

Campo	Descripción
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha de instalación	Fecha en la que se instaló el programa por última vez.
Tamaño	Tamaño del programa instalado.
Versión	Versión interna del programa instalado.

Tabla 9.30: Campos de la sección software de la información del equipo

- Para limitar la búsqueda selecciona en el desplegable el tipo de software que se mostrará:
 - Solo programas
 - Solo actualizaciones
 - Todo el software

Instalaciones y desinstalaciones

- Haz clic en el link **Instalaciones y desinstalaciones** para mostrar un histórico de los cambios

efectuados en el equipo:

Campo	Descripción
Evento	•  Software desinstalado en el equipo. •  Software instalado en el equipo.
Nombre	Nombre del programa instalado.
Editor	Empresa que desarrolló el programa.
Fecha	Fecha en la que se instaló o desinstaló el programa.
Versión	Versión interna del programa instalado.

Tabla 9.31: Campos de la sección Instalaciones y desinstalaciones

Sección Configuración (6)

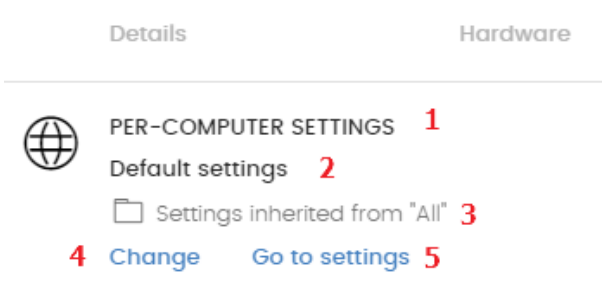


Figura 9.9: Ejemplo de asignación heredada y manual

Muestra toda la información relevante de la asignación de configuraciones al equipo, y permite su gestión y modificación:

• **(1) Nombre de la categoría de la configuración:** indica el tipo de configuración. Consulta [“Introducción a las clases de configuraciones”](#) en la [página 209](#) para conocer los distintos tipos de configuraciones disponibles en Panda Adaptive Defense 360.

- **(2) Nombre de la configuración asignada.**
- **(3) Método de asignación de la configuración:** directamente al equipo o heredada de un grupo superior.
- **(4) Botón para cambiar la asignación de la configuración.**
- **(5) Botón para editar el contenido de la configuración.**

 Consulta [“Crear y gestionar configuraciones”](#) en la [página 213](#) para crear, editar y modificar perfiles de configuración.

Barra de acciones (7)

Recurso que agrupa múltiples operaciones disponibles para aplicar sobre los equipo administrados:

Acción	Descripción
 Mover a	Mueve el equipo a un grupo estándar.
 Mover a su ruta de Active Directory	Mueve el equipo a su grupo Directorio Activo original.
 Eliminar	Libera la licencia de Panda Adaptive Defense 360 y elimina el equipo de la consola Web.
 Analizar ahora	Programa una tarea de análisis de ejecución inmediata. Consulta " Análisis y desinfección bajo demanda de equipos " en la página 527.
 Programar análisis	Programa una tarea de análisis. Consulta " Análisis y desinfección bajo demanda de equipos " en la página 527.
 Aislar equipo	Impide las comunicaciones con el exterior para facilitar las tareas de análisis forense remoto al administrador, en el caso de que el equipo haya sido comprometido. Consulta " Aislar uno o varios equipos de la red de la organización " en la página 535.
 Dejar de aislar equipo	Restaura las comunicaciones con el exterior. Consulta " Quitar el aislamiento de un equipo " en la página 536.
 Programar instalación de parches	Crea una tarea que instalará los parches publicados y no aplicados en el equipo. Consulta " Descargar e instalar los parches " en la página 329.
 Reiniciar	Reinicia el equipo de forma inmediata. Consulta " Reiniciar equipos " en la página 533.
 Reinstalar la protección (requiere reinicio)	Reinstala la protección en caso de mal funcionamiento. Consulta " Reinstalación remota " en la página 138 para obtener más información.
Notificar un problema	Abre un ticket de mantenimiento con el departamento técnico de Panda Security. Consulta " Notificar un problema " en la página 537.

Tabla 9.32: Acciones disponibles en la ventana de información del equipo

Iconos ocultos (8)

Dependiendo del tamaño de la ventana y del número de iconos a mostrar, parte de ellos pueden quedar ocultos bajo el icono . Haz clic para desplegar el menú con los iconos restantes.

Capítulo 10

Gestión de configuraciones

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 Panda Adaptive Defense 360 en los equipos que administran.

CONTENIDO DEL CAPÍTULO

Estrategias para crear la estructura de configuraciones	208
Visión general para asignar configuraciones a equipos	208
Difusión inmediata de la configuración	209
Árbol multinivel	209
Herencia	209
Configuraciones manuales	209
Configuración por defecto	209
Introducción a las clases de configuraciones	209
Perfiles de configuración modulares vs monolíticos	211
Caso práctico: Creación de configuraciones para varias delegaciones	211
Crear y gestionar configuraciones	213
Crear configuraciones	214
Ordenar configuraciones	214
Copiar, borrar y editar configuraciones	215
Asignación manual y automática de configuraciones	215
Asignación directa / manual de configuraciones	215
Desde el árbol de grupos	215
Desde el panel listado de equipos	216
Desde el propio perfil de configuración	216
Asignación indirecta de configuraciones: las dos reglas de la herencia	217
Límites de la herencia	218
Sobre-escritura de configuraciones	218
Hacer que todos hereden esta configuración	219
Mantener todas las configuraciones	220
Movimiento de grupos y equipos	220
Movimiento de equipos individuales	220
Movimiento de grupos	220
Excepciones a la herencia indirecta	221
Visualizar las configuraciones asignadas	221
Mostrar las configuraciones en el árbol de grupos	221
Mostrar las configuraciones en la definición de la configuración	222
Mostrar las configuraciones en la pestaña configuración del equipo	222
Mostrar las configuraciones en el listado de equipos exportado	222

Estrategias para crear la estructura de configuraciones

El administrador de la red creará tantos perfiles como variaciones de configuraciones sean necesarias para gestionar la seguridad de la red. Se genera una nueva configuración por cada grupo de equipos con necesidades de protección similares:

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

Visión general para asignar configuraciones a equipos

La asignación de configuraciones a los equipos de la red es un proceso de cuatro pasos:

1. Crear los grupos que reúnan equipos del mismo tipo o con idénticos requisitos de conectividad y seguridad.
2. Asignar los equipos de la red a su grupo correspondiente.
3. Asignar los distintos tipos de configuraciones a los grupos creados.
4. Difundir las configuraciones a todos los equipos de la red.

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

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



Para obtener más información sobre el manejo del árbol de grupos y asignación de equipos a grupos consulta “[El panel Árbol de equipos](#)” en la página 161.

Difusión inmediata de la configuración

Una vez que una configuración es asignada a un grupo, esa configuración se aplicará a los equipos del grupo de forma inmediata y automática, siguiendo las reglas de la herencia mostradas en “[Asignación indirecta de configuraciones: las dos reglas de la herencia](#)”. La configuración así establecida se aplica a los equipos sin retardos, en cuestión de unos pocos segundos.



Para desactivar la difusión inmediata de la configuración consulta “[Configuración de la comunicación en tiempo real](#)” en la página [231](#).

Árbol multinivel

En empresas de tamaño mediano y grande, la variedad de configuraciones puede ser muy alta. Para facilitar la gestión de parques informáticos grandes, Panda Adaptive Defense 360 permite generar árboles de grupos de varios niveles para que el administrador pueda gestionar los equipos de la red con la suficiente flexibilidad.

Herencia

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

Configuraciones manuales

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

Configuración por defecto

Inicialmente todos los equipos en el árbol de grupos heredan la configuración establecida en el nodo raíz **Todos**. Este nodo tiene asignadas las configuraciones por defecto creadas en Panda Adaptive Defense 360 para proteger a los equipos desde el primer momento, incluso antes de que el administrador haya accedido a la consola para establecer una configuración de seguridad.

Introducción a las clases de configuraciones

Panda Adaptive Defense 360 distribuye la configuración a aplicar en los equipos administrados a lo largo de varias clases de perfiles, cada una de las cuales cubre un área concreta de la seguridad.

A continuación se muestra una introducción a cada una de las clases soportadas en Panda Adaptive Defense 360:

Panda Adaptive Defense 360 permite configurar los siguientes aspectos del servicio:

Configuración	Descripción
Usuarios	Gestiona las cuentas que podrán acceder a la consola de administración, así como las acciones permitidas dentro de ella (roles) y su actividad. Consulta " Control y supervisión de la consola de administración " en la página 67 .
Ajustes por equipo	Define las plantillas de configuración donde se indica cada cuanto se actualizará el software de seguridad Panda Adaptive Defense 360 instalado en los equipos de usuario y servidores. También establece la configuración global frente a manipulaciones externas y desinstalaciones no autorizadas. Consulta " Configuración remota del agente " en la página 223
Configuración de red	Define plantillas de configuración que establecen el idioma del software Panda Adaptive Defense 360 instalado en los equipos de usuario y servidores, y el tipo de conexión que se utilizará para conectar con la nube de Panda Security. Consulta " Configuración remota del agente " en la página 223 .
Servicios de red	Define el comportamiento del software Panda Adaptive Defense 360 en lo referente a la comunicación con los equipos vecinos de la red del cliente: • Proxy: define de forma global los equipos que realizarán tareas de proxy para facilitar el acceso a la nube de equipos con Panda Adaptive Defense 360 instalado y aislados de la red. Consulta "Rol de Proxy" en la página 224. • Caché: define de forma global los repositorios de ficheros de firmas, parches de seguridad y componentes utilizados para actualizar el software Panda Adaptive Defense 360 instalado en los equipos de la red. Consulta "Rol de Caché / repositorio" en la página 225. • Descubrimiento: define de forma global los equipos de la red encargados de rastrear la aparición de dispositivos sin proteger. Consulta "Rol de descubridor" en la página 227.
Entornos DVI	Define el número de equipos alojados en infraestructuras de virtualización no persistentes para facilitar la asignación de licencias.
Mis Alertas	Establece el tipo de alertas que el administrador recibirá en su buzón de correo. Consulta " Alertas " en la página 505 .
Estaciones y servidores	Define plantillas de configuración que establecen el comportamiento de Panda Adaptive Defense 360 para proteger a los equipos de la red frente a las amenazas y el malware. Consulta " Configuración de la seguridad en estaciones y servidores " en la página 237 .
Bloqueo de programas	Define plantillas de configuración que establecen el comportamiento de Panda Adaptive Defense 360 para bloquear la ejecución de programas. Consulta " Configuración del bloqueo de programas " en la página 397 .

Tabla 10.1: Descripción de las configuraciones disponibles en Panda Adaptive Defense 360

Configuración	Descripción
Software autorizado	Define plantillas para evitar el bloqueo de los programas desconocidos en clasificación. Consulta " Configuración de software autorizado " en la página 403.
Dispositivos Android	Define plantillas de configuración que establecen el comportamiento de Panda Adaptive Defense 360 para proteger a los tablets y teléfonos móviles Android frente a las amenazas y el malware y al robo de estos dispositivos. Consulta " Configuración de seguridad Android " en la página 265.
Gestión de parches	Define las plantillas de configuración que establecen el comportamiento del descubrimiento de nuevos parches de seguridad publicados por los proveedores de software y del sistema operativo Windows. Consulta " Panda Patch Management (Actualización de programas vulnerables) " en la página 325.
Data Control	Define las plantillas de configuración que permiten realizar un seguimiento de la información personal contenida en los sistemas de almacenamiento. Consulta " Panda Data Control (Supervisión de información sensible) " en la página 269.
Cifrado	Define las plantillas de configuración que permiten cifrar el contenido de los dispositivos de almacenamiento interno. Consulta " Panda Full Encryption (Cifrado de dispositivos) " en la página 371.

Tabla 10.1: Descripción de las configuraciones disponibles en Panda Adaptive Defense 360

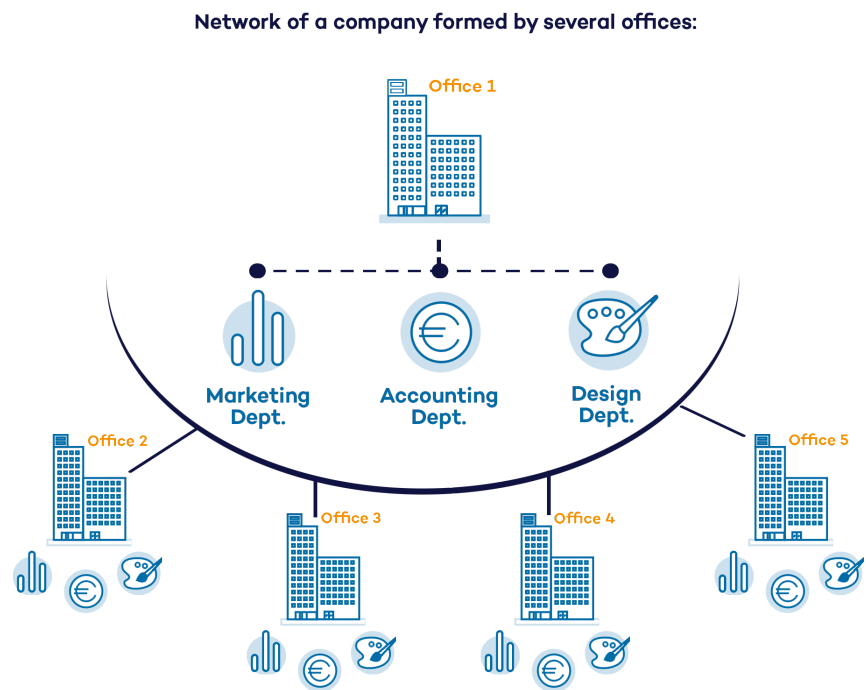
Perfiles de configuración modulares vs monolíticos

Con el soporte de las distintas clases de perfiles, Panda Adaptive Defense 360 adopta un enfoque modular para crear y distribuir las configuraciones a aplicar en los equipos administrados. El objetivo de utilizar perfiles modulares y no un único perfil de configuración monolítico que abarque toda la configuración es el de reducir el número de perfiles distintos que el administrador tendría que manejar en la consola y así minimizar el tiempo de gestión. El enfoque modular permite generar configuraciones más pequeñas y ligeras, frente a perfiles monolíticos que fomentan la aparición de muchos perfiles de configuración muy largos y redundantes, con muy pocas diferencias entre sí.

Caso práctico: Creación de configuraciones para varias delegaciones

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

departamento de diseño, otro para el departamento de contabilidad y otra para el departamento de marketing.



Con un perfil monolítico son necesarios 15 perfiles de configuración distintos (5 oficinas x 3 clases de configuración en cada oficina = 15) para dar servicio a todos los departamentos de todas las delegaciones de la empresa.



Como Panda Adaptive Defense 360 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



Crear y gestionar configuraciones

Haz clic en el menú superior Configuración para crear, copiar y borrar configuraciones. En el panel de la izquierda se encuentran las entradas correspondientes a las clases de configuraciones posibles (1). En el panel de la derecha se muestran los perfiles de configuración ya creados (2) de la clase

seleccionada y los botones para añadir (3), copiar (4) y eliminar perfiles (5). Utiliza la barra de búsqueda (6) para localizar los perfiles ya creados de forma rápida.

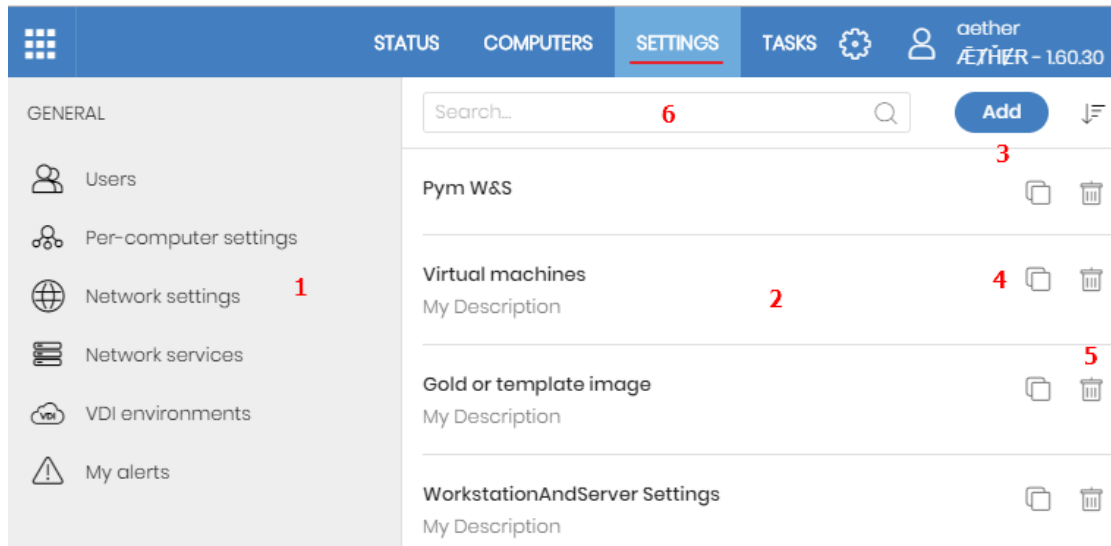


Figura 10.1: Pantalla para crear y gestionar configuraciones



Las configuraciones creadas desde Panda Partner Center, se muestran con la etiqueta en verde Panda Partner Center. Al posicionarse sobre ella se muestra el mensaje: "Esta configuración está gestionada desde Panda Partner Center".

Las configuraciones creadas desde Panda Partner Center son de sólo lectura, y únicamente permiten cambiar los destinatarios. Para más información, consulta la sección Configuraciones para productos basados en Panda, en el manual de [Panda Partner Center](#).

Crear configuraciones

Haz clic sobre el botón **Añadir** para mostrar la ventana de creación de configuraciones. Todos los perfiles tienen un nombre principal y una descripción que se muestran en los listados de configuraciones.

Ordenar configuraciones

Haz clic en el icono  (7) para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Copiar, borrar y editar configuraciones

- Para copiar y borrar un perfil de configuración utiliza los iconos **(4)** y **(5)**. Si el perfil ha sido asignado a uno o más equipos se impedirá su borrado hasta que sea liberado.
- Haz clic en el perfil de configuración para editarlo.



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

Asignación manual y automática de configuraciones

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

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

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

Asignación directa / manual de configuraciones

Consiste en establecer de forma directa los perfiles de configuración a equipos o grupos. De esta manera es el administrador el que, de forma manual, asigna una configuración a un grupo o equipo.

Una vez creados los perfiles de configuración, estos se asignan de tres maneras posibles:

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



Para obtener más información sobre el árbol de grupos consulta "[Árbol de grupos](#)" en la página [168](#).

Desde el árbol de grupos

Para asignar un perfil de configuración a un conjunto de equipos que pertenecen a un grupo:

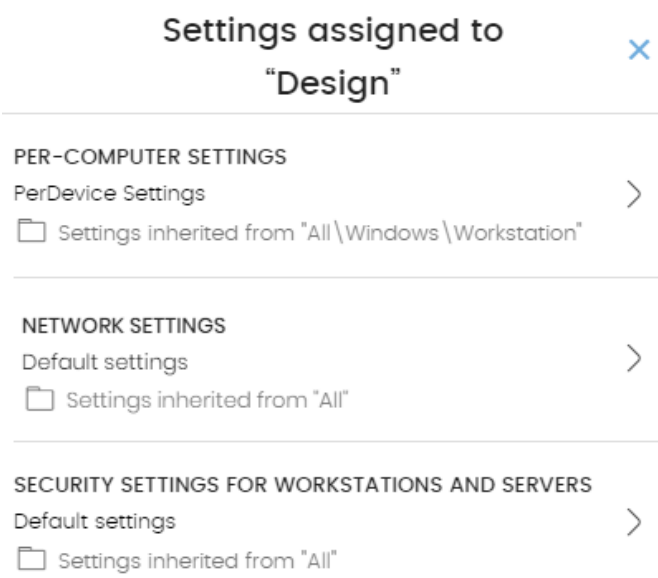


Figura 10.2: Ejemplo de asignación heredada y manual

- Haz clic en el menú superior **Equipos** y selecciona el árbol de grupos en el panel izquierdo.
- Haz clic en el menú contextual en la rama apropiada del árbol de grupos.
- Haz clic en el menú emergente **Configuraciones**, se mostrará una ventana con el nombre de los perfiles ya asignados al grupo seleccionado, separados por su clase, y el tipo de asignación:
 - **Manual / Asignación directa:** mediante la leyenda **Asignada directamente a este grupo**.
 - **Heredada / Asignación indirecta:** mediante la leyenda **Configuración heredada de** y el nombre del grupo

del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.

- Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al grupo. La configuración se propagará de forma inmediata a todos los equipos miembros del grupo y sus descendientes.

Desde el panel listado de equipos

Para asignar un perfil de configuración a un equipo concreto:

- En el menú superior **Equipos** haz clic en el grupo o filtro donde reside el equipo a asignar la configuración. Haz clic sobre el equipo en la lista de equipos mostrada en el panel derecho para ver la pantalla detalles de equipo.
- Haz clic en la pestaña **Configuración**. Se mostrarán los perfiles asignados al equipo separados por su clase, y el tipo de asignación:
 - **Manual / Asignación directa:** mediante la leyenda **Asignada directamente a este grupo**.
 - **Heredada / Asignación indirecta:** mediante la leyenda **Configuración heredada de** y el nombre del grupo del cual se hereda la configuración, junto con la ruta completa para llegar al mismo.
- Haz clic en una de las clases disponibles, selecciona la nueva configuración y haz clic en **Aceptar** para asignar la configuración al equipo. La configuración se aplicará de forma inmediata.

Desde el propio perfil de configuración

La forma más rápida de asignar una configuración a varios equipos que pertenecen a grupos distintos es a través del propio perfil de configuración.

Para asignar equipos o grupos de equipos a un perfil de configuración:

- En el menú superior **Configuración**, panel lateral, haz clic en la clase de perfil que quieres asignar.

- Selecciona la configuración a asignar y haz clic en el botón **Destinatarios**. Se mostrará una ventana dividida en dos secciones: **Grupos de equipos** y **Equipos adicionales**.
- Haz clic en los botones  para añadir equipos individuales o grupos de equipos al perfil de configuración.
- Haz clic en el botón **Atrás**. El perfil quedará asignado a los equipos seleccionados y la nueva configuración se aplicará de forma inmediata.



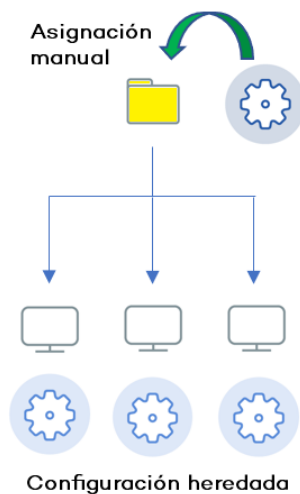
Al retirar un equipo de la lista de equipos asignados a una configuración, el equipo volverá a heredar las configuraciones asignadas al grupo al que pertenece. La consola de administración resaltará este hecho mostrando una ventana de advertencia antes de aplicar los cambios.

Asignación indirecta de configuraciones: las dos reglas de la herencia

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

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

- **Regla de la herencia automática**

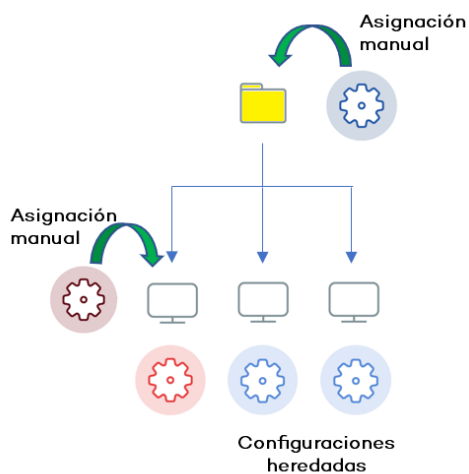


Un grupo o equipo hereda de forma automática las configuraciones del grupo del cual depende (grupo padre o de orden superior).

La asignación de configuración es manual sobre el grupo padre y todos sus descendientes (equipos y otros grupos con equipos en su interior) reciben la configuración de forma automática.

Figura 10.3: Herencia / asignación indirecta

- **Regla de la prioridad manual**

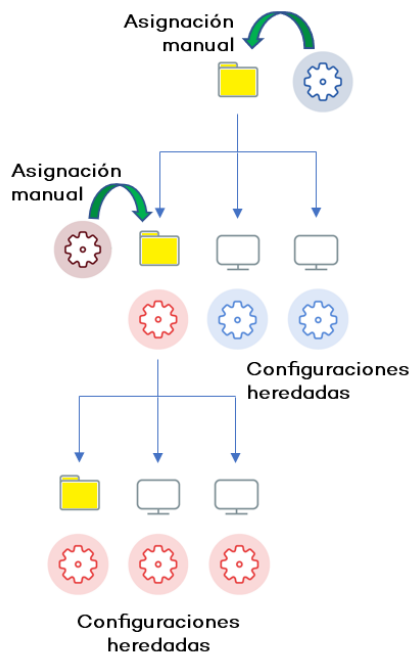


Una configuración manual prevalece sobre una configuración heredada.

Los equipos reciben las configuraciones heredadas por defecto pero si se establece una configuración manual sobre un grupo o equipo, todos sus descendientes recibirán la configuración manual, y no la configuración heredada de orden superior.

Figura 10.4: Prevalencia de configuración manual sobre heredada

Límites de la herencia



La configuración asignada a un grupo (manual o heredada) se propaga a todos los elementos de la rama del árbol hasta que se encuentra una asignación manual.

Este nodo y todos sus descendientes reciben la configuración manual asignada, y no la establecida en el nodo de orden superior.

Figura 10.5: Limite de la herencia

Sobre-escritura de configuraciones

La regla de la prioridad manual indica que las configuraciones manuales prevalecen sobre las configuraciones heredadas en un escenario típico donde primero se establece la configuración

sobre el nodo de orden superior para que todos sus descendientes la hereden, y posteriormente se asignan de forma manual aquellas configuraciones especiales sobre ciertos nodos de orden inferior.

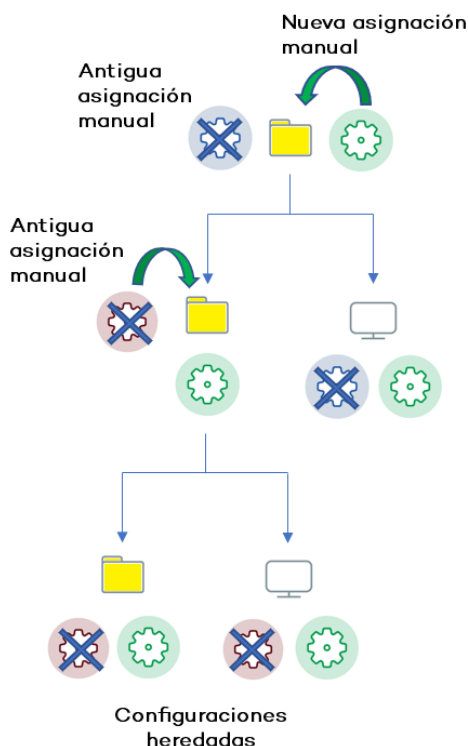


Figura 10.6: Sobre escritura de configuraciones manuales

Sin embargo, es frecuente que una vez establecidas las configuraciones heredadas y manuales, haya un cambio de configuración en un nodo de orden superior. Se distinguen dos casos:

- **No hay configuraciones manuales en los nodos descendientes:** el nodo padre recibe una nueva configuración que se propaga a todos sus nodos descendientes.
- **Sí hay configuraciones manuales en algún nodo descendiente:** el nodo padre recibe una configuración que intenta propagar a todos los nodos descendientes, pero el sistema de herencia no permite asignar una configuración de forma automática sobre un nodo que recibió anteriormente una configuración manual.

De esta manera, cuando el sistema detecta un cambio de configuración que tenga que propagar a los nodos subordinados, y alguno de estos tenga una configuración manual (sin importar el nivel en el que se encuentre) se presentará la pantalla de selección, preguntando al administrador sobre el

comportamiento a seguir: **Hacer que todos hereden esta configuración** o **Mantener todas las configuraciones**.

Hacer que todos hereden esta configuración



¡Utiliza esta opción con mucho cuidado, esta acción no tiene vuelta atrás! Todas las configuraciones manuales que dependan del nodo padre se perderán y se aplicará la configuración heredada de forma inmediata en los equipos. El comportamiento de Panda Adaptive Defense 360 podrá cambiar en muchos equipos de la red.

La nueva asignación directa se propaga mediante la herencia a todo el árbol por completo, sobrescribiendo la asignación directa anterior y llegando hasta los nodos hijos de último nivel.

Mantener todas las configuraciones

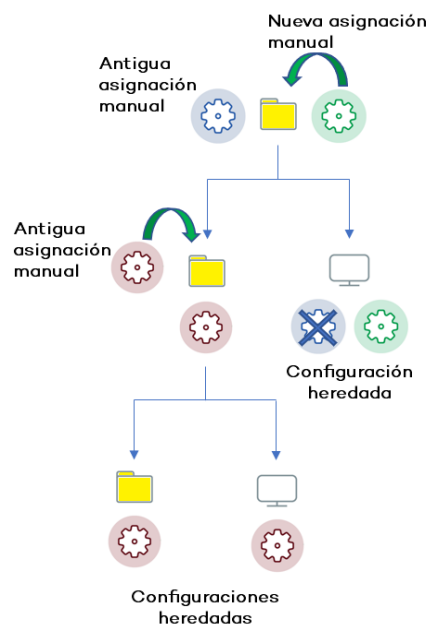


Figura 10.7: Mantener las configuraciones manuales

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

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 configuración se detiene en el primer nodo subordinado del árbol que tiene asignada una configuración manual.

• Eliminar asignaciones manuales y restaurar la herencia

Para eliminar una asignación manual aplicada sobre una carpeta y volver a heredar la configuración de la rama padre:

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

Movimiento de grupos y equipos

Al mover un equipo o grupo de equipos a otra rama del árbol con una configuración aplicada, el comportamiento de Panda Adaptive Defense 360 con respecto a las configuraciones que tomará el equipo o grupo movido varía en función de si se trata de grupos completos o equipos individuales.

Movimiento de equipos individuales

Se respetan las configuraciones manuales establecidas sobre los equipos movidos, y se sobrescriben de forma automática las configuraciones heredadas con las configuraciones establecidas en el nuevo grupo padre.

Movimiento de grupos

Se muestra una ventana con la pregunta **¿Quieres que las configuraciones asignadas a este grupo mediante herencia, sean sustituidas por las del nuevo grupo padre?**

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

Excepciones a la herencia indirecta

A los equipos que se integran en la consola Web dentro de un grupo de tipo nativo, Panda Adaptive Defense 360 les asigna la configuración de red del grupo de destino mediante el mecanismo estándar de asignación indirecta / herencia. Sin embargo, si un equipo se integra en la consola Web dentro de un grupo de tipo IP o de tipo directorio activo, la asignación de la configuración de red se produce de forma manual. Este cambio en la forma de asignar la configuración de red repercute a su vez en un cambio de comportamiento al mover posteriormente ese equipo de un grupo a otro: ya no heredará de forma indirecta la configuración de red asignada al grupo de destino, sino que conservará la suya propia.

Este comportamiento particular de la herencia, se debe a que en empresas de tamaño medio y grande, el departamento que administra la seguridad puede no ser el mismo que el que administra el directorio activo de la empresa. Por esta razón, un cambio de grupo efectuado por el departamento técnico que mantiene el directorio activo puede desembocar de forma inadvertida en un cambio de configuración de red dentro de la consola de Panda Adaptive Defense 360. Esta situación podría dejar sin conectividad al agente de protección instalado en el equipo y, por lo tanto, en una menor protección. Al asignar de forma manual la configuración de red, se impiden cambios de configuración cuando el equipo cambia de grupo en la consola de Panda Adaptive Defense 360, debido a un cambio de grupo del directorio activo de la empresa.

Visualizar las configuraciones asignadas

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

- En el árbol de grupos.
- En la pantalla de definición de la configuración.
- En la pestaña **Configuración** del equipo.
- En el listado de equipos exportado.

Mostrar las configuraciones en el árbol de grupos

- Haz clic en el menú superior **Equipos** y en la pestaña  situada en la parte superior del panel lateral para mostrar el árbol de grupos.

- Selecciona el menú de contexto de la rama elegida y haz clic en el menú emergente **Configuraciones** para mostrar una ventana con las configuraciones asignadas a la carpeta.

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

- **Tipo de configuración:** indica la clase a la que pertenece la configuración mostrada.
- **Nombre de la configuración:** nombre asignado por el administrador en la creación de la configuración.
- **Tipo de herencia aplicada:**
 - **Configuración heredada de...:**  la configuración fue asignada a la carpeta padre indicada, y los equipos que pertenecen a la rama actual la heredan.
 - **Asignada directamente a este grupo:**  la configuración de los equipos es la que el administrador asignó de forma manual a la carpeta.

Mostrar las configuraciones en la definición de la configuración

- Haz clic en el menú superior **Configuraciones** y selecciona el tipo de configuración en el menú lateral.
- Selecciona una configuración en el listado de configuraciones.
- Si la configuración está asignada a uno o más equipos o grupos, se mostrará el botón **Ver equipos**.
- Haz clic en el botón **Ver equipos**. Se mostrará la zona **Equipos** con un único listado formado por todos los equipos que tienen la configuración asignada, tanto si se asignó de forma individual o mediante grupos de equipos. En la parte superior de la ventana se mostrará el criterio de filtrado establecido.

Mostrar las configuraciones en la pestaña configuración del equipo

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

Mostrar las configuraciones en el listado de equipos exportado

Desde el árbol de equipos (árbol de grupos o árbol de filtros) haz clic en el menú contextual y elige la opción **Exportar**.



Consulta "[Campos mostrados en el fichero exportado](#)" en la página [177](#).

Capítulo 11

Configuración remota del agente

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

- El papel o rol que el equipo representa para el resto de puestos y servidores protegidos.
- Las protecciones frente al tampering o manipulación indebida del software cliente Panda Adaptive Defense 360 por parte de amenazas avanzadas y APTs.
- La visibilidad del agente en el equipo de usuario o servidor y su idioma.
- Configuración de las comunicaciones de los equipos con la nube de Panda Security.

CONTENIDO DEL CAPÍTULO

Configuración de los roles del agente Panda	224
Rol de Proxy	224
Requisitos para asignar el rol de proxy a un equipo	224
Asignar el rol de proxy a un equipo	225
Retirar el rol de proxy a un equipo	225
Rol de Caché / repositorio	225
Elementos cacheados	225
Dimensionamiento de un nodo caché	226
Asignar el rol de caché a un equipo	226
Retirar el rol de caché a un equipo	226
Establecer la unidad de almacenamiento	226
Rol de descubridor	227
Configuración de listas de acceso a través de proxy	228
Configurar una lista de acceso	229
Mecanismo de fallback	229
Configuración de las descargas mediante equipos caché	230
Requisitos para usar un equipo con el rol de caché en modo automático	230
Descubrimiento de nodos caché	231
Configuración del método de asignación de nodos caché	231
Configuración de la comunicación en tiempo real	231
Requisitos para comunicación en tiempo real	231
Deshabilitar las comunicaciones en tiempo real	232
Configuración del idioma del agente	232
Configuración de la visibilidad del agente	233
Configuración de contraseña y anti-tampering	233
Anti-tamper	233

Habilitar / Inhabilitar anti-tamper 233

Protección del agente mediante contraseña 234

Asignar una contraseña local 234

Configuración de los roles del agente Panda

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

- Proxy
- Descubridor
- Caché

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



Solo los equipos con sistema operativo Windows instalado pueden adquirir el rol de Proxy, Descubridor o Caché.

Rol de Proxy

Para los equipos que no tienen acceso directo a Internet, Panda Adaptive Defense 360 permite la utilización del proxy instalado en la red de la organización. En el caso de no existir ningún proxy disponible, puedes asignar el rol de proxy a un equipo con Panda Adaptive Defense 360 instalado.



No se permite la descarga de parches y actualizaciones del módulo Panda Patch Management a través de un equipo con el rol de proxy asignado. Los equipos que descarguen parches deberán de tener acceso a la nube de Panda Security directamente o a través de un proxy corporativo.

Requisitos para asignar el rol de proxy a un equipo

- Panda Adaptive Defense 360 instalado en un equipo con sistema operativo Windows.
- Soporte para el formato de ficheros 8+3. Consulta el artículo de la MSDN [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778996\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778996(v=ws.10)?redirectedfrom=MSDN) para habilitar esta funcionalidad.

Asignar el rol de proxy a un equipo



En las máquinas designadas como Proxy Panda Adaptive Defense 360, el puerto TCP 3128 no podrá ser utilizado por otras aplicaciones. Además, la configuración del cortafuegos del equipo deberá permitir el tráfico entrante y saliente por ambos puertos.

- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.
- Haz clic en el botón **Añadir servidor proxy**. Se mostrará una ventana con todos los equipos administrados por Panda Adaptive Defense 360 que cumplen los requisitos para ejercer de proxy en la red.
- Utiliza la caja de búsqueda para localizar el equipo y haz clic sobre el mismo para agregarlo al listado de equipos con el rol de proxy asignado.

Retirar el rol de proxy a un equipo

- Haz clic en el menú superior **Configuración**, panel lateral **Servicios de red** y en la pestaña **Proxy**. Se mostrarán todos los equipos con el rol de proxy ya asignado.
- Haz clic en el icono  del equipo que quieres retirar el rol de proxy.



Para configurar el uso de un equipo con el rol de proxy asignado consulta "[Configuración de listas de acceso a través de proxy](#)" en la página [228](#).

Rol de Caché / repositorio

Panda Adaptive Defense 360 permite asignar el rol de caché a uno o más puestos de la red. Estos equipos descargan y almacenan de forma automática todos los ficheros que necesitan otros puestos con Panda Adaptive Defense 360 instalado. Esto produce un ahorro de ancho de banda, ya que cada equipo no descargará de forma independiente las actualizaciones, sino que se hará una única vez de forma centralizada.

Elementos cacheados

Un equipo con el rol de cache asignado puede cachear los elementos siguientes durante un periodo de tiempo variable dependiendo de su tipo:

- **Archivo de identificadores:** hasta que dejan de ser válidos.
- **Paquetes de instalación:** hasta que dejan de ser válidos.
- **Parches de actualización para** Panda Patch Management: 30 días.

Dimensionamiento de un nodo caché

El dimensionamiento de un equipo con el rol de caché asignado depende completamente del número de conexiones simultáneas en los picos de carga y del tipo de tráfico que gestione (descargas de ficheros de firmas, instaladores etc.). Como aproximación un equipo con el rol de caché asignado puede servir en torno a 1000 equipos de forma simultánea.

Asignar el rol de caché a un equipo

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- Haz clic en el botón **Añadir equipo caché**.
- Utiliza la herramienta de búsqueda situada en la parte superior de la ventana para localizar equipos candidatos a asignar el rol de caché.
- Selecciona un equipo de la lista y pulsa **Aceptar**.

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

Retirar el rol de caché a un equipo

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

Establecer la unidad de almacenamiento

Es posible configurar el agente Panda Adaptive Defense 360 para almacenar los elementos a cachear en un volumen / unidad concreta del equipo, aunque la ruta de la carpeta dentro del volumen es fija. Para configurar esta característica sigue los pasos mostrados a continuación:

- En el menú superior **Configuración**, panel lateral **Servicios de red** haz clic en la pestaña superior **Caché**.
- En un equipo con el rol de caché asignado y que ya haya reportado a la nube su estado haz clic en el enlace **Cambiar**. Se mostrará una ventana con las unidades locales disponibles.
- Por cada unidad se muestra el nombre del volumen, la unidad asignada, el espacio ocupado y el

espacio libre.

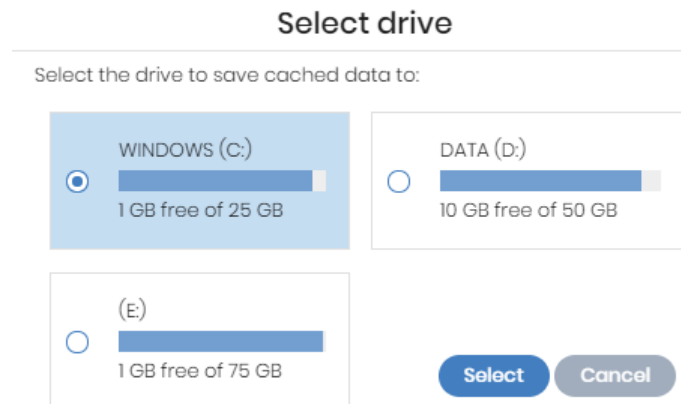


Figura 11.1: Ventana de selección de volumen en un equipo con el rol de caché asignado

- Para ver los porcentajes de espacio ocupado y libre pasa el ratón por encima de las barras y se mostrará un tooltip con la información.
- Indica con el selector la unidad con 1 Gigabyte libre o más que almacenará los elementos cacheados, y haz clic en el botón **Seleccionar**. Panda Adaptive Defense 360 comenzará a copiar los elementos ya cacheados y, una vez completado el proceso, los borrará de su ubicación original.



*Solo es posible seleccionar la unidad donde se almacenarán los elementos a cachear en los equipos que hayan reportado su estado al servidor Panda Adaptive Defense 360. Si no se cumple esta condición se tomará por defecto la unidad que almacena los ficheros de instalación de Panda Adaptive Defense 360. Una vez reportado se mostrará el enlace **Cambiar** en el equipo con el rol de cache asignado y se podrá modificar la unidad de almacenamiento. Un equipo puede tardar en reportar su estado varios minutos.*

Si no hay espacio suficiente o se produce algún error de escritura al cambiar la unidad de almacenamiento se mostrará un mensaje debajo del equipo con el nodo caché asignado, indicando la fuente del problema.

Rol de descubridor

En el menú superior **Configuración**, panel lateral **Servicios de red**, la pestaña **Descubrimiento** está directamente relacionada con el procedimiento de instalación y despliegue de Panda Adaptive Defense 360 en la red del cliente.



Consulta “[Descubrir equipos](#)” en la página 118 para obtener más información acerca del proceso de descubrimiento e instalación de Panda Adaptive Defense 360.

Configuración de listas de acceso a través de proxy



El acceso a Internet a través de proxy solo está disponible en sistemas operativos Windows.

Panda Adaptive Defense 360 permite asignar a los equipos de la red uno o más métodos de conexión con el exterior, en función de los recursos existentes en la infraestructura IT de la compañía.

Panda Adaptive Defense 360 maneja una lista de métodos de acceso configurable por el administrador, que recorre cuando necesita conectar con la nube de Panda Security. Una vez seleccionado, el método de acceso elegido no cambia hasta que éste queda inaccesible, momento en el cual Panda Adaptive Defense 360 seguirá recorriendo la lista hasta encontrar uno nuevo que sea válido. Si llega al final de la lista volverá a iniciar el recorrido hasta que todos los métodos de conexión hayan sido probados al menos una vez.

Los tipos de conexión soportados por Panda Adaptive Defense 360 son:

Tipo de proxy	Descripción
No usar proxy	Acceso directo a Internet. Los equipos acceden de forma directa a la nube de Panda Security para descargar las actualizaciones y enviar los reportes de estado del equipo. En este caso, el software Panda Adaptive Defense 360 utilizará la configuración del equipo para comunicarse con Internet.
Proxy corporativo	Acceso a Internet vía proxy instalado en la red de la organización. • Dirección: dirección IP del servidor de proxy. • Puerto: puerto del servidor de proxy. • El proxy requiere autenticación: habilitar si el proxy requiere información de usuario y contraseña. • Usuario: cuenta de un usuario del proxy que permita su uso. • Contraseña: contraseña de la cuenta de usuario.
Descubrimiento automático de proxy a través de Web Proxy Autodiscovery Protocol (WPAD)	Pregunta a la red mediante DNS o DHCP para recuperar la url de descubrimiento que apunta al archivo PAC de configuración. Alternativamente se puede indicar directamente el recurso HTTP o HTTPS donde se encuentra el archivo PAC de configuración.

Tabla 11.1: Tipos de acceso a la red soportados por Panda Adaptive Defense 360

Tipo de proxy	Descripción
Proxy Panda Adaptive Defense 360	Acceso a través del agente Panda Adaptive Defense 360 instalado en un equipo de la red. Centraliza todas las comunicaciones de la red a través de un equipo con un agente Panda instalado. Para configurar la salida de un equipo a través de un proxy Panda Adaptive Defense 360 haz clic en el enlace Seleccionar equipo . Se desplegará una ventana con el listado de equipos disponibles que tienen el rol de proxy en la red. Selecciona uno de la lista y haz clic en el botón Añadir .

Tabla 11.1: Tipos de acceso a la red soportados por Panda Adaptive Defense 360



Es posible configurar una lista de accesos formada por varios equipos con el rol de proxy asignado. Asigna previamente el rol de proxy Panda Adaptive Defense 360 a uno o más equipos de la red con Panda Adaptive Defense 360 instalado siguiendo los pasos indicados en “[Asignar el rol de proxy a un equipo](#)”.

Configurar una lista de acceso

Para configurar una lista de acceso crea una configuración de tipo Configuración de red:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección **Proxy** haz clic en el icono Se mostrará una ventana con los tipos de conexión disponibles.
- Selecciona un tipo de conexión (tabla 11.1) y haz clic en el botón **Aceptar**. El tipo de conexión se añadirá a la lista.
- Para modificar el orden de los métodos de conexión selecciona un elemento haciendo clic en la casilla de selección y utiliza las flechas y para subirlo o bajarlo.
- Para borrar un método de conexión haz clic en el icono .
- Para modificar un método de conexión selecciónalo con las casillas de selección y haz clic en el icono Se mostrará una ventana donde editar la configuración del método.

Mecanismo de fallback

Cuando un agente Panda no puede conectar con la plataforma Aether y ha probado todos los métodos de conexión indicados en su lista de acceso configurada, ejecutará la siguiente lógica de fallback para restaurar la conexión mediante otro método disponible:

- **Internet Explorer:** Panda Adaptive Defense 360 intenta recuperar la configuración de proxy de Internet Explorer impersonado como el usuario que inició sesión 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:** Panda Adaptive Defense 360 lee la configuración del proxy por defecto.
- **Conexión directa:** Panda Adaptive Defense 360 intenta conectarse directamente a la nube de Panda Security.

Configuración de las descargas mediante equipos caché



El acceso a equipos con el rol de caché asignado para acelerar las actualizaciones y las descargas de parches solo está disponible en sistemas operativos Windows.

La utilización de un equipo con el rol de caché puede establecerse de dos maneras:

- **Método automático:** el equipo que inicia la descarga utiliza los equipos con el rol de caché descubiertos en la red y que cumplan con los requisitos indicados en [“Requisitos para usar un equipo con el rol de caché en modo automático”](#). Si se encuentran varios equipos caché se balancearán las descargas para no sobrecargar a un único equipo caché.
- **Método manual:** el administrador establece de forma manual el equipo de la red con el rol de caché que será utilizado para descargar datos de la nube de Panda Security. El comportamiento de un nodo cache asignado de forma manual tiene las siguientes diferencias con respecto al modo automático:
 - Si un equipo tiene varios nodos cache asignados de forma manual no se repartirán las descargas.
 - Si el primer equipo caché no está accesible se recorrerá la lista hasta encontrar un equipo que funcione. Si no se encuentra ningún equipo se intentará la salida directa a Internet.

Requisitos para usar un equipo con el rol de caché en modo automático

- El equipo con el rol de cache asignado y el equipo que descarga elementos de éste deben estar en la misma subred. Si un equipo caché tiene varias tarjetas de red podrá servir de repositorio en cada uno de los segmentos a los que esté conectado.



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

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

Descubrimiento de nodos caché

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

Adicionalmente, cada cierto tiempo los equipos de la red con el método automático de asignación configurado preguntarán si existe algún nodo con el rol de caché instalado.

Configuración del método de asignación de nodos caché

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y elige una configuración.
- En la sección **Caché** elige una opción:
 - **Utilizar automáticamente los equipos caché vistos en la red:** los equipos que reciben esta configuración buscarán de forma automática los nodos caché de su segmento de red.
 - **Utilizar los siguientes equipos caché (por orden de preferencia):** haz clic en el icono ⊕ para añadir equipos con el rol de caché asignado y configurar una lista de nodos caché. Los equipos que reciban esta configuración conectarán con los nodos caché indicados en la lista para realizar las descargas.

Configuración de la comunicación en tiempo real

Panda Adaptive Defense 360 se comunica en tiempo real con la plataforma Aether para recuperar las configuraciones establecidas en la consola sobre los equipos protegidos, transcurriendo unos pocos segundos desde que el administrador asigna una configuración a un equipo hasta que éste la aplica.

Las comunicaciones en tiempo real entre los equipos protegidos y el servidor Panda Adaptive Defense 360 requieren el mantenimiento de una conexión abierta por cada puesto de forma permanente. Desactiva las comunicaciones en tiempo real cuando el número de conexiones abiertas afecte al rendimiento del proxy instalado en la red, o cuando el impacto en el consumo de ancho de banda sea elevado al cambiar simultáneamente las configuraciones de un gran número de equipos.

Requisitos para comunicación en tiempo real

- Las comunicaciones en tiempo real son compatibles con todos los sistemas operativos soportados por Aether excepto Windows XP y Windows 2003.
- Si el equipo accede a Internet mediante un proxy corporativo, se requiere que las conexiones https no sean manipuladas. Muchos proxys utilizan técnicas Man in the Middle para analizar las

conexiones https o funcionar como proxys caché. En estos casos la comunicación en tiempo real no funcionará.

Deshabilitar las comunicaciones en tiempo real

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

Al deshabilitar las comunicaciones en tiempo real, los equipos se comunicarán con el servidor Panda Adaptive Defense 360 cada 15 minutos.

Configuración del idioma del agente

Para asignar el idioma del agente Panda a uno o varios equipos es necesario crear una configuración de tipo **Configuración de red**:

- Haz clic en el menú superior **Configuración**, menú lateral **Configuración de red** y en el botón **Añadir** o selecciona una configuración ya creada para modificarla.
- En la sección idioma elige el idioma de entre los disponibles:
 - Alemán
 - Español
 - Finlandés
 - Francés
 - Húngaro
 - Inglés
 - Italiano
 - Japonés
 - Portugués
 - Ruso
 - Sueco



Si se produce un cambio de idioma y la consola local de Panda Adaptive Defense 360 estaba abierta se pedirá un reinicio de la consola local. Este procedimiento no afecta a la seguridad del equipo.

Configuración de la visibilidad del agente

Para las empresas donde el servicio de seguridad sea 100% administrado por el departamento de IT no es necesario que el icono del agente Panda Adaptive Defense 360 sea visible en el área de notificaciones de los equipos de la red. Para ocultar o mostrar el icono sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Preferencias** y activa o desactiva la opción **Mostrar icono en la bandeja del sistema**.

Configuración de contraseña y anti-tampering

Anti-tamper

Muchas amenazas avanzadas incorporan técnicas para desactivar el software de seguridad de los equipos. La protección Anti-tamper evita la modificación no autorizada del funcionamiento de la protección impidiendo que el software se detenga, pause o se desinstale mediante el establecimiento de una contraseña.

Para evitar estos problemas, la protección Anti-tamper de Panda Adaptive Defense funciona de la siguiente manera:

- La configuración de **Ajustes de equipo** creada por defecto incluye una contraseña pre calculada única para cada cliente. Esta contraseña no se puede cambiar ya que las configuraciones por defecto son de solo lectura.
- En las configuraciones de **Ajustes por equipo** generadas por el usuario la opción de anti-tamper puede ser desactivada o activada, dependiendo de las medidas de seguridad que se quieran aplicar.

Las contraseñas creadas para las configuraciones de seguridad deben tener entre 6 y 15 caracteres.

Habilitar / Inhabilitar anti-tamper

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

activar o desactivar esta funcionalidad de las configuraciones creadas.



Al desactivar la opción de seguridad **Activar protección anti-tamper** o **Solicitar contraseña para desinstalar la protección de los equipos** aparecerá un aviso de seguridad cuando se guarde la configuración. No es recomendable desactivar estas opciones de seguridad.

Protección del agente mediante contraseña

Para evitar que el usuario modifique las características de protección o desinstale completamente el software Panda Adaptive Defense 360, el administrador puede establecer una contraseña local que cubra ambos casos.

Asignar una contraseña local

- Haz clic en el menú superior **Configuración**, panel lateral **Ajustes por equipo**.
- Haz clic en una configuración existente o selecciona **Añadir** para crear una nueva.
- Despliega la sección **Seguridad** frente a manipulaciones no deseadas de las protecciones:
 - **Solicitar contraseña para desinstalar Aether desde los equipos:** evita que el usuario desinstale el software Panda Adaptive Defense 360 protegiéndolo con una contraseña.
 - **Permitir activar/desactivar temporalmente las protecciones desde la consola de los equipos:** permite administrar las capacidades de seguridad del equipo desde la consola local. Requiere el establecimiento de una contraseña.



Si un equipo pierde la licencia asignada, de manera manual o por caducidad o cancelación, las protecciones anti-tampering y las protección por contraseña contra las desinstalación quedarán desactivadas.



Parte 5

Gestión de la seguridad

Capítulo 12: Configuración de la seguridad en estaciones y servidores

Capítulo 13: Configuración de seguridad Android

Capítulo 14: Panda Data Control (Supervisión de información sensible)

Capítulo 15: Panda Patch Management (Actualización de programas vulnerables)

Capítulo 16: Panda Full Encryption (Cifrado de dispositivos)

Capítulo 17: Configuración del bloqueo de programas

Capítulo 18: Configuración de software autorizado

Capítulo 12

Configuración de la seguridad en estaciones y servidores

Panda Adaptive Defense 360 ofrece todas las funcionalidades de protección incluidas en el producto mediante las configuraciones de seguridad para estaciones y servidores. El administrador de la red podrá proteger los activos de la empresa frente a amenazas informáticas de muy diversa índole, asignando configuraciones de seguridad a los equipos de la red.

A continuación se explican todos los parámetros incluidos en la configuración de seguridad para estaciones y servidores. También se indican algunas recomendaciones prácticas para asegurar los puestos de trabajo de la red y minimizar los inconvenientes ocasionados al usuario.



Para obtener información adicional sobre los distintos apartados del módulo Estaciones y servidores consulta las referencias siguientes:

- “**Crear y gestionar configuraciones**” en la página **213**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.
- “**Control y supervisión de la consola de administración**” en la página **67**: gestión de cuentas de usuario y asignación de permisos.

CONTENIDO DEL CAPÍTULO

Acceso a la configuración y permisos necesarios	238
Acceso a la configuración	238
Introducción a la configuración de la seguridad	239
Configuración General	240
Alertas en los equipos	240
Actualizaciones	241
Desinstalar otros productos de seguridad	241
Archivos y rutas excluidas del análisis	241
Ficheros en disco	241
Excluir archivos adjuntos de correo	242
Protección avanzada	242
Comportamiento	242

Modo de funcionamiento (Sólo Windows)	242
Detectar actividad maliciosa (Sólo Linux)	243
Anti exploit	243
Funcionamiento de la protección anti-exploits	243
Configuración de la detección anti - exploits	244
Privacidad	245
Uso de la red	245
Antivirus - - - - -	246
Amenazas a detectar	246
Tipos de archivos	247
Firewall (Equipos Windows) - - - - -	247
Modo de funcionamiento	247
Tipo de red	248
Configurar criterios para determinar el tipo de red	248
Reglas de programa	249
Regla de conexión	251
Bloquear intrusiones	253
Control de dispositivos (Equipos Windows) - - - - -	255
Activar el control de dispositivos	255
Dispositivos permitidos	256
Exportar e importar listas de dispositivos permitidos	256
Obtener el identificador único del dispositivo	256
Cambio de nombre de los dispositivos	256
Control de acceso a páginas web - - - - -	257
Configurar horarios del control de accesos a páginas Web	257
Denegar el acceso a páginas Web	257
Denegar el acceso a páginas de categoría desconocida	258
Lista de direcciones y dominios permitidos o denegados	258
Base de datos de URLs accedidas desde los equipos	258
Antivirus para servidores Exchange - - - - -	259
Configuración de la protección Antivirus según el modo de análisis	259
Protección de buzones	259
Protección de transporte	260
Software a detectar	260
Escaneo inteligente de buzones	260
Restauración de mensajes con virus y otras amenazas	260
Anti spam para servidores Exchange - - - - -	261
Acción para mensajes de spam	261
Direcciones y dominios permitidos	261
Direcciones y dominios de spam	261
Filtrado de contenidos para servidores Exchange - - - - -	262
Registro de detecciones - - - - -	262

Acceso a la configuración y permisos necesarios

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Estaciones y servidores**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Estaciones y servidores**.

Permisos requeridos

Permiso	Tipo de acceso
Configurar seguridad para estaciones y servidores	Crear, modificar, borrar, copiar o asignar las configuraciones de Estaciones y servidores.
Ver configuraciones de seguridad para estaciones y servidores	Visualizar las configuraciones de Estaciones y servidores.

Tabla 12.1: Permisos requeridos para acceder a la configuración Estaciones y servidores

Introducción a la configuración de la seguridad

Las configuraciones de seguridad para estaciones y servidores se dividen en varios apartados. Al hacer clic en cada uno de ellos se mostrará un desplegable con la información asociada. A continuación, se muestran las diferentes secciones con una breve explicación.

Sección	Descripción
General	Establece el comportamiento de las actualizaciones, desinstalaciones de los antivirus de otros fabricantes y los ficheros excluidos en el equipo del usuario o servidor protegido que no se analizarán.
Protección avanzada	Establece el comportamiento de la protección avanzada y de la protección anti exploit frente a APTs, amenazas dirigidas y malware avanzado o que utiliza exploits.
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	Regula las visitas del usuario a categorías de páginas web.
Antivirus para servidores Exchange	Analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de amenazas.
Anti spam para servidores Exchange	Analiza los mensajes entrantes y salientes de los servidores de correo Exchange en busca de correo no deseado.
Filtrado de contenidos para servidores Exchange	Regula el tipo de contenidos que puede recibir el servidor Exchange.

Tabla 12.2: Descripción de los módulos disponibles en Panda Adaptive Defense 360

No todas las funcionalidades se encuentran disponibles en todas las plataformas soportadas. A continuación se muestra un resumen de las funcionalidades de seguridad incluidas en Panda Adaptive Defense 360 por plataforma compatible:

Funcionalidad	Windows	macOS	Linux	Windows Exchange
Protección avanzada	X		X	
Protección Anti-exploit	X			
Antivirus	X	X	X	X
Cortafuegos & IDS	X			
Protección Email	X			
Protección Web	X	X	X	
Control de dispositivos	X			
Filtrado Web	X	X	X	
Anti-spam				X
Filtrado de contenidos				X

Tabla 12.3: Funcionalidades de seguridad por plataforma

Configuración General

La configuración general establece el comportamiento de Panda Adaptive Defense 360 relativo a las actualizaciones, desinstalación de programas de la competencia y exclusiones de ficheros y carpetas que no se analizarán.

Alertas en los equipos

Campo	Descripción
Mostrar alertas de malware, firewall y control de dispositivos	Introduce un mensaje descriptivo para informar al usuario del motivo de la alerta. El agente Panda Adaptive Defense 360 mostrará una ventana desplegable con el contenido del mensaje
Mostrar alertas cada vez que el control de acceso a páginas web bloquee una página	Muestra una ventana emergente en el equipo del usuario o servidor cada vez que Panda Adaptive Defense 360 bloquea el acceso a una página web.

Tabla 12.4: Campos Alertas en los equipos

Actualizaciones



Consulta "[Actualización del software cliente](#)" en la página [153](#) para obtener información acerca de los procedimientos necesarios para actualizar el agente, la protección y el fichero de firmas de software cliente instalado en el equipo del usuario.

Desinstalar otros productos de seguridad



Consulta "[Visión general del despliegue de la protección](#)" en la página [106](#) para establecer el comportamiento de la instalación de la protección en el caso de que otro producto de seguridad esté instalado previamente en el equipo del usuario.

Consulta [Desinstaladores soportados](#) para obtener un listado de todos los productos de la competencia que Panda Adaptive Defense 360 desinstala automáticamente del equipo del usuario.

Archivos y rutas excluidas del análisis

Configura los elementos del equipo que no serán bloqueados, borrados o desinfectados en busca de malware.



Esta configuración desactiva tanto a la protección antivirus como la protección avanzada. Debido a que el uso de esta configuración genera potenciales agujeros de seguridad, Panda recomienda limitar su uso, quedando éste restringido a evitar problemas del rendimiento.

Ficheros en disco

Indica los ficheros en el disco de los equipos protegidos que no serán borrados o desinfectados por Panda Adaptive Defense 360.

Campo	Descripción
Extensiones	Extensiones de ficheros que no serán analizadas.
Carpetas	Carpetas cuyo contenido no será analizado.
Archivos	Ficheros que no serán analizados. Se permite el uso de los caracteres comodín '*' y '?'. Tabla 12.5: Ficheros en disco que no serán analizados por Panda Adaptive Defense 360

Campo	Descripción
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.

Tabla 12.5: Ficheros en disco que no serán analizados por Panda Adaptive Defense 360

Excluir archivos adjuntos de correo

Especifica la lista de extensiones de ficheros que no son analizados en caso de encontrarse como adjuntos en mensajes de correo.

Protección avanzada

Comportamiento

La protección avanzada activa la monitorización de los procesos ejecutados en equipos Windows, macOS y Linux, y el envío de toda la telemetría generada a la nube de Panda Security. Esta información se incorpora a los procesos de investigación encargados de clasificar los ficheros como goodwill o malware, sin ambigüedades ni lugar para sospechosos. Gracias a esta tecnología es posible detectar malware desconocido y amenazas avanzadas como APTs en equipos Windows y Linux.

Junto a las funcionalidades de detección avanzada, Panda ofrece el servicio 100% Attestation Service para equipos Windows, que clasifica todos los ficheros encontrados en el parque informático del cliente, eliminando de esta forma la categoría de "desconocidos".

Modo de funcionamiento (Sólo Windows)

Campo	Descripción
Auditoria	Solo se informa de las amenazas detectadas, pero no se bloquea ni se desinfecta el malware encontrado.
Hardening	Ejecuta los programas desconocidos ya instalados en el equipo del usuario. Bloquea los programas desconocidos que vienen de fuentes no fiables como Internet, otros equipos de la red o unidades de almacenamiento externas hasta su clasificación. Los programas clasificados como malware serán desinfectados o eliminados.
Lock	Bloquea la ejecución de todos los programas desconocidos hasta que estén clasificados y los programas ya clasificados como malware.

Tabla 12.6: Modos de funcionamiento de la protección avanzada para Windows

- **Informar a los usuarios de los equipos de los bloqueos:** introduce un mensaje descriptivo para informar al usuario cuando un fichero ha sido bloqueado por el módulo de protección avanzada o por el de anti-exploit. El agente Panda Adaptive Defense 360 mostrará una ventana desplegable

con el contenido del mensaje. Para configurar un mensaje informativo y dejar la decisión de ejecutar o no el elemento haz clic en el selector **Dar a los usuarios de los equipos la opción de ejecutar los programas desconocidos bloqueados (recomendado sólo para usuarios avanzados o administradores)**.

Detectar actividad maliciosa (Sólo Linux)

Panda Adaptive Defense 360 envía la telemetría obtenida de la monitorización de actividad de equipos y servidores macOS y Linux a la nube de Panda. Con esta información Panda Adaptive Defense 360 realiza detecciones contextuales que permiten detener amenazas avanzadas.

Campo	Descripción
Auditar	Se informa de las amenazas detectadas pero no se bloquea el malware encontrado. Para evitar inconvenientes en equipos muy específicos Auditar es la opción por defecto.
Bloquear	Se informa y se bloquean las amenazas detectadas. Activa esta opción si estás seguro de que la actividad detectada pertenece a un malware.
No detectar	No se informa ni se detecta el malware.

Tabla 12.7: Modos de funcionamiento de la protección para Linux

Anti exploit



La protección anti exploit está deshabilitada por defecto para mejorar la compatibilidad con soluciones de seguridad de terceros que también incorporen este tipo de tecnología. En esta situación, ni los ataques de tipo exploit ni el malware de tipo Metasploit serán detectados / bloqueados, aunque el resto de módulos de protección detectarán y bloquearán las acciones consideradas peligrosas para el sistema. Habilita la protección anti exploit de forma gradual en aquellos equipos con soluciones de seguridad de terceros para comprobar su buen funcionamiento.

La tecnología anti exploit no está disponible en sistemas Windows ARM.

La protección anti exploit bloquea de forma automática y sin intervención del usuario en la mayor parte de los casos los intentos de explotación de vulnerabilidades de procesos instalados en el equipo del usuario.

Funcionamiento de la protección anti-exploits

Los equipos de la red pueden contener procesos de origen conocido y fiable pero con fallos de programación. Son conocidos como "procesos vulnerables" debido a que interpretan de forma incorrecta ciertas secuencias de datos que reciben del usuario o de otros procesos.

Cuando un proceso vulnerable recibe un determinado patrón de información conocido por los hackers, se produce un mal funcionamiento interno que deriva en una inyección de fragmentos de código preparados por el hacker en las regiones de memoria gestionadas por el proceso vulnerable. Un proceso así afectado recibe el nombre de "proceso comprometido". La inyección de código provoca que el proceso comprometido ejecute acciones para las que no fue programado, generalmente peligrosas y que comprometen la seguridad del equipo.

La protección anti-exploit de Panda Adaptive Defense 360 detecta la inyección de código malicioso en los procesos vulnerables ejecutados por el usuario, bloqueándola mediante dos cursos de acción diferentes, dependiendo del exploit encontrado:

- **Bloqueo del exploit**

Detecta la inyección de código en el proceso vulnerable cuando todavía no se ha completado. El proceso no llega a comprometerse y el riesgo del equipo es nulo, con lo que no requiere detener el proceso afectado ni reiniciar el equipo de usuario. No implica pérdida de información por parte del proceso afectado.

El usuario puede recibir una notificación del bloqueo dependiendo de la configuración establecida por el administrador.

- **Detección del exploit**

Detecta la inyección de código en el proceso vulnerable cuando ya se ha producido. Debido a que el proceso vulnerable ya contiene el código malicioso, es imperativo cerrarlo antes de que ejecute acciones que puedan poner en peligro la seguridad del equipo.

Independientemente del tiempo transcurrido desde la detección hasta el cierre del proceso Panda Adaptive Defense 360 considera en riesgo el equipo, aunque su cuantificación depende del tiempo transcurrido en cerrar el proceso afectado y del diseño del malware. Panda Adaptive Defense 360 puede cerrar el proceso de forma automática para minimizar los efectos adversos, o delegar en el usuario la decisión, pidiéndole permiso de forma explícita para descargarlo de la memoria.

Si el administrador ha configurado el cierre automático para minimizar la posibilidad de efectos adversos, el usuario puede sufrir la pérdida de información manejada por el proceso afectado. Si, por el contrario, el administrador ha delegado en el usuario la decisión, el usuario podrá retrasar el cierre de la aplicación y minimizar la posibilidad perdida de información.

En los casos en que no sea posible cerrar el proceso afectado se pedirá permiso al usuario para reiniciar el equipo completo.

Configuración de la detección anti - exploits

- **Anti-exploit:** habilita la protección contra exploits.
- **Inyección avanzada de código:** detecta mecanismos avanzados de inyección de código en

procesos en ejecución.

Campo	Descripción
Auditar	Notifica en la consola Web la detección del exploit, pero no toma acciones contra él ni informa al usuario del equipo.
Bloquear	Bloquea los ataques de tipo exploit. Puede requerir el cierre del proceso afectado por el exploit. • Informar del bloqueo al usuario del equipo: el usuario recibe una notificación, pero el proceso comprometido se cierra de forma automática si es necesario. • Pedir permiso al usuario: el usuario recibe una petición de autorización para el cierre del proceso comprometido por el exploit en caso de ser necesario. Esta opción resulta útil para que el usuario pueda salvar la información antes producirse el cierre del proceso. Si se requiere el reinicio del equipo siempre se pide confirmación al usuario, independientemente de la configuración Pedir permiso al usuario.

Tabla 12.8: Modo de funcionamiento de la protección avanzada anti-exploit en Panda Adaptive Defense 360



Dado que muchos exploits continúan ejecutando código malicioso hasta que no se produce el cierre del proceso, la incidencia no se marcará como resuelta en el panel de elementos maliciosos y exploit de la consola Web hasta que el programa haya sido cerrado.

Privacidad

Panda Adaptive Defense 360 incluye el nombre, la ruta completa de los ficheros y el usuario que inició la sesión en el equipo cuando envía los archivos a la nube de Panda Security para su análisis. Esta información se utiliza posteriormente en los informes y las herramientas de análisis forense mostrados en la consola Web. Para no enviar que esta información desactiva la casilla apropiada en la pestaña **Privacidad**.

Uso de la red

Los ficheros ejecutables desconocidos encontrados en el equipo del usuario se envían a la nube de Panda Security para su análisis. El impacto en el ancho de banda de la red del cliente está configurado de forma predeterminada para pasar desapercibido:

- Se envía un máximo de 50 Mbytes por hora y agente.
- Un fichero concreto desconocido se envía una sola vez para todos los clientes que usan Panda Adaptive Defense 360.
- Se implementan mecanismos de gestión del ancho de banda con el objetivo de evitar un uso intensivo de los recursos de red.

Para configurar el número máximo de megabytes que un agente podrá enviar en una hora introduce el valor y haz clic en **Ok**. Para establecer transferencias ilimitadas deja el valor a 0.

Antivirus

Esta sección configura el comportamiento general del motor de antivirus basado en ficheros de firmas.

Campo	Descripción
Protección de archivos	Activa o desactiva la protección antivirus que afecta al sistema de ficheros.
Protección de correo	Activa o desactiva la protección antivirus que afecta al cliente de correo instalado en el equipo del usuario. Panda Adaptive Defense 360 detectará las amenazas recibidas por el protocolo POP3 y sus variantes cifradas.
Protección web	Activa o desactiva la protección antivirus que afecta al cliente web instalado en el equipo del usuario. Panda Adaptive Defense 360 detectará las amenazas recibidas por el protocolo HTTP y sus variantes cifradas.

Tabla 12.9: Módulos de protección antivirus disponibles en Panda Adaptive Defense 360

La acción que ejecuta Panda Adaptive Defense 360 ante un fichero de tipo malware o sospechoso se define en los laboratorios de Panda Security:

- **Ficheros conocidos como malware desinfectable:** sustituir el fichero original por una copia desinfectada.
- **Ficheros conocidos como malware no desinfectable:** se guarda una copia de seguridad y el fichero original se elimina.

Amenazas a detectar

Configura el tipo de amenazas que Panda Adaptive Defense 360 busca y elimina en el sistema de archivos, cliente de correo y web instalados en el equipo del usuario.

Campo	Descripción
Detectar virus	Ficheros que contienen patrones identificados por el fichero de firmas como peligrosos.
Detectar herramientas de hacking y PUPs	Programas no deseados (programas que contienen publicidad intrusiva, barras de navegación etc.) y herramientas utilizadas por los hackers para ganar acceso a los sistemas.
Bloquear acciones maliciosas	Activa tecnologías anti exploit y heurísticas para analizar localmente el comportamiento de los procesos y buscar actividades sospechosas
Detectar Phishing	Ataques basados en el engaño por web y correo.

Tabla 12.10: Tipos de malware detectados por la protección antivirus de Panda Adaptive Defense 360

Campo	Descripción
No detectar amenazas en las siguientes direcciones y dominios	Lista blanca de direcciones y dominios que no se analizarán en busca de ataques por phishing. Se compara a nivel de sub cadenas y sin tener en cuenta las mayúsculas y minúsculas por lo que para incluir una dirección en la lista blanca es suficiente con indicar una parte de la misma.

Tabla 12.10: Tipos de malware detectados por la protección antivirus de Panda Adaptive Defense 360

Tipos de archivos

Indica los tipos de archivos que Panda Adaptive Defense 360 analiza:

Campo	Descripción
Analizar comprimidos en disco	Descomprime los ficheros empaquetados y analiza su contenido en busca de malware.
Analizar comprimidos en mensajes de correo	Descomprime los ficheros adjuntos que viajan en los correos electrónicos y analiza su contenido en busca de malware.
Analizar todos los archivos independientemente de su extensión cuando son creados o modificados (No recomendado)	Por cuestiones de rendimiento no se recomienda analizar todos los ficheros ya que técnicamente muchos tipos de ficheros de datos no pueden presentar amenazas a la seguridad del equipo.

Tabla 12.11: Tipos de archivos analizados por la protección antivirus de Panda Adaptive Defense 360

Firewall (Equipos Windows)

Panda Adaptive Defense 360 incluye tres herramientas para filtrar el tráfico de red que recibe o envía un equipo protegido:

- **Protección mediante reglas de sistema:** describen características de las comunicaciones establecidas por el equipo (puertos, IPs, protocolos etc.), con el objetivo de permitir o denegar los flujos de datos que coincidan con las reglas configuradas.
- **Protección de programas:** permite o deniega la comunicación a determinados programas instalados en el equipo de usuario.
- **Sistema de detección de intrusos:** detecta y rechaza patrones de tráfico mal formado que afectan a la seguridad o al rendimiento del equipo protegido.

Modo de funcionamiento

Se accede mediante el control **La configuración firewall la establece el usuario de cada equipo:**

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

equipos a través de perfiles de configuración.

Tipo de red

Los equipos de usuario portátiles pueden conectarse a redes con un grado de seguridad muy diverso según se trate de accesos públicos, como la red wifi de un cibercafé, o de redes gestionadas o de acceso limitado, como la red de una empresa. Para ajustar el comportamiento por defecto del cortafuegos, el administrador de la red puede seleccionar de forma manual el tipo de red al que se conectan usualmente los equipos del perfil configurado, o puede dejar a Panda Adaptive Defense 360. la elección de la red mas apropiada.

Tipo de red	Descripción
Red pública	Redes que se encuentran en cibercafés, aeropuertos, etc. Implica establecer limitaciones en el nivel de visibilidad de los equipos protegidos y en su utilización, sobre todo a la hora de compartir archivos, recursos y directorios.
Red de confianza	Redes que se encuentran en oficinas y domicilios. El equipo es perfectamente visible para el resto de usuarios de la red, y viceversa. No hay limitaciones para compartir archivos, recursos y directorios.
Detectar automáticamente	El tipo de red (red pública o red de confianza) se selecciona de forma automática en función de una serie de criterios que el equipo del usuario debe de cumplir. Haz clic en el enlace Configurar reglas para determinar cuándo un equipo está conectado a una red de confianza .

Tabla 12.12: Tipos de red compatibles con el cortafuegos

El comportamiento de Panda Adaptive Defense 360 según la red seleccionada se traduce en un mayor o menor número de reglas añadidas de forma automática. Estas reglas se pueden ver en Reglas de programa y Reglas de conexión como "reglas de Panda".



El tipo de red es un concepto aplicable a cada interface de red del equipo de forma independiente. Es posible que equipos con varias interfaces de red tengan distintos tipos de red asignados y por lo tanto las reglas del cortafuegos serán diferentes para cada interface de red.

Configurar criterios para determinar el tipo de red

Panda Adaptive Defense 360 permite añadir uno o más criterios que el equipo protegido por el cortafuegos deberá de cumplir para seleccionar de forma automática la configuración **Red de confianza**. Si ninguna de estas condiciones se cumplen el tipo de red establecido en el interface de red será **Red pública**.

Un criterio es una regla que determina si una interface de red del equipo se considera que está conectado a una red de confianza. Esta asociación se realiza mediante la resolución de un dominio definido previamente en un servidor DNS interno de la empresa: si el equipo es capaz de conectar con el servidor DNS de la empresa y resolver el dominio configurado querrá decir que está conectado

a la red de la empresa, y por lo tanto el cortafuegos puede asumir que el equipo se encuentra en una red de confianza.

A continuación se muestra un ejemplo de configuración completo:

- En este ejemplo se utilizará "miempresa.com" como la zona principal del cliente que quiere que sus equipos detecten de forma automática si están conectados a la red corporativa.
- Añade el registro de tipo A "criteriocortafuegos" en la zona "miempresa.com" del servidor DNS interno de la red, sin especificar dirección IP ya que no tendrá ninguna utilidad.
- Según esta configuración, "criteriocortafuegos.miempresa.com" será el dominio que Panda Adaptive Defense 360 intentará resolver para comprobar que se encuentra dentro de la red corporativa.
- Reinicia el servidor DNS para cargar la nueva configuración si fuera necesario, y comprueba que "criteriocortafuegos.miempresa.com" se resuelve correctamente desde todos los segmentos de la red interna con las herramientas nslookup, dig o host.
- En la consola de Panda Adaptive Defense 360 haz clic en el enlace **Configurar reglas para determinar cuándo un equipo está conectado a una red de confianza**. Se mostrará una ventana con los siguientes campos a completar:
 - **Nombre del criterio:** indica un nombre descriptivo de la regla a configurar. Por ejemplo "micriterioDNS".
 - **Servidor DNS:** indica la dirección IP del servidor DNS de la red interna de la empresa que recibirá la petición de resolución.
 - **Dominio:** indica la petición que el equipo enviará al servidor DNS para su resolución. Introduce "criteriocortafuegos.miempresa.com".
 - Haz clic en el botón **Aceptar**, en el botón **Guardar** y nuevamente en el botón **Guardar**.
- Una vez configurado y aplicado el criterio el equipo intentará resolver el dominio "criteriocortafuegos.miempresa.com" en el servidor DNS especificado cada vez que se produzca un evento en la interface de red (conexión desconexión, cambio de IP etc.). Si la resolución DNS es correcta se asignará a la interface de red que se utilizó la configuración asignada a la red de confianza.

Reglas de programa

En esta sección se configuran los programas del usuario que comunican con la red y los que tienen bloqueado el envío y recepción de datos.

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

1. Establecer la acción por defecto.

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

Tabla 12.13: Tipos de acción por defecto en el cortafuegos para los programas instalados en el equipo del usuario

2. Activar reglas de Panda.

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

3. Añadir reglas para definir el comportamiento específico de una aplicación.



Figura 12.1: Controles de edición de reglas de red

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

Al crear una regla es necesario indicar los siguientes campos:

- **Descripción:** descripción de la regla.
- **Programa:** selecciona el programa cuyo comportamiento en red se va a controlar.
- **Conexiones permitidas para este programa:** define las características del tráfico que se controlará:

Campo	Descripción
Permitir conexiones entrantes y salientes	El programa se podrá conectar a la red (Internet y redes locales) y también se permitirá que otros se conecten a él. Existen ciertos tipos de programas que requieren este tipo de permisos para funcionar correctamente: programas de intercambio de archivos, aplicaciones de chat, navegadores de Internet, etc.
Permitir conexiones salientes	El programa se podrá conectar a la red, pero no aceptará conexiones externas por parte de otros usuarios o aplicaciones.

Tabla 12.14: Modos de comunicación de los programas permitidos

Campo	Descripción
Permitir conexiones entrantes	El programa aceptará conexiones externas de programas o usuarios procedentes de Internet, pero no tendrá permisos para establecer nuevas conexiones.
Denegar todas las conexiones	El programa no podrá acceder a la red.

Tabla 12.14: Modos de comunicación de los programas permitidos

- **Permisos avanzados:** define las características exactas del tráfico que es aceptado o denegado.

Campo	Descripción
Acción	Establece la acción que ejecutará Panda Adaptive Defense 360 si la regla coincide con el tráfico examinado. • Permitir: permite el tráfico. • Denegar: bloquea el tráfico. Hace un <code>Drop</code> de la conexión.
Sentido	Establece la dirección del tráfico para protocolos orientados a conexión, como TCP. • Salientes: tráfico con origen el equipo de usuario y destino otro equipo de la red. • Entrantes: tráfico con destino el equipo de usuario y origen otro equipo de la red.
Zona	La regla solo se aplica si la zona indicada coincide con la zona configurada en " Tipo de red ". Las reglas que tengan en campo Zona a Todos se aplican siempre sin tener en cuenta la zona configurada en el perfil de protección.
Protocolo	Especifica el protocolo de nivel 3 del tráfico generado: • Todos • TCP • UDP
IP	• Todos: no tiene en cuenta los campos IP de origen y destino de la conexión. • Personalizado: define la IP de origen o destino del tráfico a controlar. Especifica más de una IP separadas por ',' o utiliza el carácter '-' para establecer rangos de IPs. Selecciona en el desplegable si las direcciones IP son IPv4 o IPv6. No es posible mezclar tipos de direcciones IP en una misma regla. • Puertos: selecciona el puerto de la comunicación. Elige Personalizado para añadir varios puertos separados por comas y rangos de puertos utilizando guiones.

Tabla 12.15: Modos avanzados de comunicación de los programas permitidos

Regla de conexión

Son reglas tradicionales de filtrado de tráfico TCP/IP. Panda Adaptive Defense 360 extrae el valor de ciertos campos de las cabeceras de cada paquete que reciben o envían los equipos protegidos, y explora el listado de reglas introducido por el administrador. Si alguna regla coincide con el tráfico examinado se ejecuta la acción asociada.

Las reglas de conexiones afectan a todo el sistema, independientemente del proceso que las gestione, y son prioritarias con respecto a las reglas por programa, configuradas anteriormente.

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

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

Acción		Descripción
Permitir		Estrategia permisiva basada en aceptar por defecto las conexiones cuyo comportamiento no ha sido definido mediante reglas en el paso 3. Este es el modo básico de configuración: todas las conexiones no descritas mediante reglas son automáticamente aceptadas.
Denegar		Estrategia restrictiva basada en denegar por defecto las conexiones cuyo comportamiento no ha sido definido mediante reglas en el paso 3. Este es el modo avanzado de funcionamiento: todas las conexiones no descritas mediante reglas son automáticamente denegadas.

Tabla 12.16: Tipos de acción por defecto en el cortafuegos para las conexiones gestionadas en el equipo del usuario

2. Activar reglas de Panda

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

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

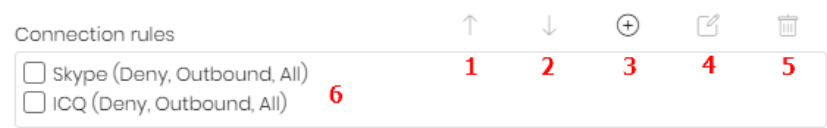


Figura 12.2: Controles de edición de reglas de red

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

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

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

Campo		Descripción
Nombre de regla		Asigna un nombre único a la regla.
Descripción		Descripción del tipo de tráfico filtrado por la regla.

Tabla 12.17: Campos de las reglas de conexión

Campo	Descripción
Sentido	Establece la dirección del tráfico para protocolos orientados a conexión, como TCP. • Salientes: tráfico saliente. • Entrantes: tráfico entrante.
Zona	La regla solo se aplica si la zona indicada coincide con la zona configurada en "Tipo de red". Las reglas que tengan en campo Zona a Todos se aplican siempre sin tener en cuenta la zona configurada en el perfil de protección.
Protocolo	Especifica el protocolo del tráfico. Según la elección se mostrarán unos controles u otros para identificarlo de forma precisa: • TCP, UDP, TCP/UDP: describe reglas TCP y / o UDP incluyendo puertos locales y remotos. • Puertos locales: puerto de la conexión utilizado en el equipo del usuario. Selecciona Personalizado para añadir varios puertos separados por comas y rangos de puertos utilizando guiones. • Puertos remotos: puerto de la conexión utilizado en el equipo remoto. Selecciona Personalizado para añadir varios puertos separados por comas y rangos de puertos utilizando guiones. • Servicios ICMP: crea reglas que describen mensajes ICMP, indicando su tipo y subtipo. • Servicios ICMPv6: crea reglas que describen mensajes ICMP sobre IPv6, indicando su tipo y subtipo. • Tipos IP: crea reglas para el protocolo IP y otros protocolos se orden superior.
Direcciones IP	Direcciones IP de origen o destino del tráfico. Especifica varias direcciones IP separadas por coma o mediante rangos con guión. Selecciona en el desplegable si las direcciones IP son IPv4 o IPv6. No es posible mezclar tipos de direcciones IP en una misma regla.
Direcciones MAC	Direcciones MAC de origen o destino del tráfico.

Tabla 12.17: Campos de las reglas de conexión



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

Bloquear intrusiones

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

A continuación, se detallan los tipos de tráfico mal formado soportados y una explicación de cada uno de ellos:

Campo	Descripción
IP explicit path	Rechaza los paquetes IP que tengan la opción de "explicit route". Son paquetes IP que no se encaminan en función de su dirección IP de destino, en su lugar la información de encaminamiento es fijada de ante mano.
Land Attack	Comprueba intentos de denegación de servicios mediante bucles infinitos de pila TCP/IP al detectar paquetes con direcciones origen y destino iguales.
SYN flood	Controla los el numero de inicios de conexiones TCP por segundo para no comprometer los recursos del equipo atacado. Pasado cierto limite las conexiones se rechazan.
TCP Port Scan	Detecta conexiones simultáneas a varios puertos del equipo protegido en un tiempo determinado y filtra tanto la petición de apertura como la respuesta al equipo sospechoso, para que el origen del tráfico de escaneo no obtenga información del estado de los puertos.
TCP Flags Check	Detecta paquetes TCP con combinaciones de flags inválidas. Actúa como complemento a las defensas de "Port Scanning" al detener ataques de este tipo, tales como "SYN & FIN" y "NULL FLAGS" y los de "OS identification" ya que muchas de estas pruebas se basan en respuesta a paquetes TCP inválidos.
Header lengths	• IP: rechaza los paquetes entrantes con un tamaño de cabecera IP que se salga de los límites establecidos. • TCP: rechaza los paquetes entrantes con un tamaño de cabecera TCP que se salga de los límites establecidos. • Fragmentation control: comprueba el estado de los fragmentos de los paquetes a reensamblar, protegiendo al equipo de ataques por consumo excesivo de memoria en ausencia de fragmentos, del redireccionado de ICMP disfrazado de UDP y del escaneo de equipos.
UDP Flood	Rechaza los paquetes UDP que llegan a un determinado puerto si superan un limite en un periodo establecido.
UDP Port Scan	Protección contra escaneo de puertos UDP.
Smart WINS	Rechaza las respuestas WINS que no se corresponden con peticiones que el equipo ha solicitado.
Smart DNS	Rechaza las respuestas DNS que no se corresponden con peticiones que el equipo ha solicitado.
Smart DHCP	Rechaza las respuestas DHCP que no se corresponden con peticiones que el equipo ha solicitado.

Tabla 12.18: Tipos de tráfico mal formado soportados

Campo	Descripción
ICMP Attack	• SmallPMTU: detecta valores inválidos en el tamaño de los paquetes ICMP para generar una denegación de servicio o ralentizar el tráfico saliente. • SMURF: rechaza las respuestas ICMP no solicitadas si estás superan un límite en un intervalo. Este tipo de ataque envía grandes cantidades de tráfico ICMP (echo request) a la dirección de broadcast de la red con la dirección de origen cambiada (spoofing) apuntando a la dirección de la víctima. La mayoría de los equipos de la red responderán a la víctima, multiplicando el tráfico por cada equipo de la subred. • Drop unsolicited ICMP replies: rechaza todas las respuestas ICMP no solicitadas o que han expirado por el timeout establecido.
ICMP Filter echo request	Rechaza las peticiones de Echo request.
Smart ARP	Rechaza las respuestas ARP que no se corresponden con peticiones que el equipo protegido ha solicitado para evitar escenarios de tipo ARP caché poison.
OS Detection	Falsea datos para engañar a los detectores de sistemas operativos y así evitar posteriores ataques dirigidos a aprovechar las vulnerabilidades asociadas al sistema operativo detectado. Esta defensa se complementa con la de "TCP Flags Check".

Tabla 12.18: Tipos de tráfico mal formado soportados

Control de dispositivos (Equipos Windows)

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

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

Activar el control de dispositivos

- Marca la casilla **Activar control de dispositivos**.
- Elige en el desplegable correspondiente el nivel de autorización a aplicar para el tipo de dispositivo a limitar su uso.
 - En el caso de las llaves USB y las unidades CD/DVD elige entre **Bloquear**, **Permitir lectura** o **Permitir lectura y escritura**.
 - Para Bluetooth, dispositivos de imágenes, módems USB y teléfono móviles las opciones son **Permitir** y **Bloquear**.

Dispositivos permitidos

Gestiona mediante una lista blanca aquellos dispositivos individuales que sí están permitidos cuando toda su familia esté bloqueada:

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

Exportar e importar listas de dispositivos permitidos

Despliega las opciones de **Exportar** e **Importar** del menú de contexto .

Obtener el identificador único del dispositivo

Para gestionar dispositivos sin esperar a que el usuario los conecte a su equipo o para poder excluirlos de forma manual, es necesario obtener el identificador de estos dispositivos:

- En el Administrador de dispositivos de Windows selecciona el dispositivo del que se va a obtener el identificador. Haz clic con el botón derecho del ratón sobre el nombre del dispositivo y accede a **Propiedades**.
- Accede a la pestaña **Detalles**.
- En el desplegable **Propiedad** selecciona **Ruta de acceso a la instancia del dispositivo**. En el campo **Valor**, se encuentra el identificador único del dispositivo.

En el supuesto de que no se muestre ningún valor Ruta de acceso a instancia del dispositivo, no será posible obtener el identificador del dispositivo. En este caso puedes utilizar como identificador el correspondiente al hardware del dispositivo:

- En el desplegable **Propiedad**, selecciona **Identificador de hardware** y se mostrará el identificador correspondiente.



Este identificador no identifica de forma única a cada dispositivo, sino que representa a todos los dispositivos de la misma gama.

Apunta todos los identificadores de dispositivo en un fichero de texto según se indica en **[“Exportar e importar listas de dispositivos permitidos”](#)**.

Cambio de nombre de los dispositivos

El nombre asignado por Panda Adaptive Defense 360 a los dispositivo del equipo puede llevar en ocasiones a confusión, o a impedir al administrador identificarlos correctamente. Para solucionar este problema es posible asignar nombres personalizados a los dispositivos:

- En la sección **Dispositivos permitidos** selecciona el dispositivo a cambiar de nombre.
- Haz clic en el icono . Se mostrará una ventana donde introducir el nuevo nombre del dispositivo.
- Haz clic en el botón **Aceptar**. La lista **Dispositivos permitidos** se actualizará con el nuevo nombre.

Control de acceso a páginas web

Con esta protección el administrador de la red restringe el acceso a determinadas categorías Web y a URLs individuales a las que autoriza o restringe el acceso. Esta estrategia optimiza del ancho de banda de la red y mejora la productividad en 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**.

Configurar horarios del control de accesos a páginas Web

Restringe el acceso a determinadas categorías de páginas Web y listas negras durante las horas de trabajo, y autorízalo en horario no laborable o en el fin de semana.

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

A continuación, selecciona las horas en las que el control horario estará activado. Para activarlo sólo en un horario determinado, marca la casilla correspondiente y utiliza la cuadrícula para señalar las horas.

- 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**.

Denegar el acceso a páginas Web

Panda Adaptive Defense 360 agrupa las páginas web que tiene clasificadas según su temática y contenido en más de 160 categorías. Para impedir la navegación de paginas web selecciona la categoría o categorías a las que pertenecen.

Cuando el usuario visite una página Web que pertenezca a una categoría denegada, se mostrará en su navegador un aviso indicando el motivo.

Denegar el acceso a páginas de categoría desconocida

Para denegar el acceso a páginas no categorizadas 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. Añade las páginas Web desconocidas que sean necesarias a la lista blanca de exclusiones para evitar esta situación.

Lista de direcciones y dominios permitidos o denegados

Especifica mediante una lista blanca las páginas web a las que siempre se permite acceder, y mediante una lista negra las páginas a las que nunca se permite, independientemente de la categoría a la que pertenezcan:

- 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 obtener una coincidencia.

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.

Antivirus para servidores Exchange

Para activar la protección de servidores Exchange es necesario disponer de un número de licencias igual a la cantidad de buzones en la compañía que requieren protección.

La protección para servidores Exchange es aplicable a las versiones 2003, 2007, 2010, 2013, 2016 y 2019, y está formada por tres módulos:

- Antivirus
- Anti-spam
- Filtrado de contenidos

Configuración de la protección Antivirus según el modo de análisis

Según el momento en el que Panda Adaptive Defense 360 efectúa el análisis dentro del flujo de correo, se distinguen dos formas de protección: protección de buzones y protección de transporte.

La tabla 12.19 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	NO	NO
Transporte	2003, 2007, 2010, 2013, 2016, 2019	2003, 2007, 2010, 2013, 2016, 2019	2003, 2007, 2010, 2013, 2016, 2019

Tabla 12.19: 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 analiza las carpetas / buzones en segundo plano o cuando el mensaje es recibido y almacenado en la carpeta del usuario.

La protección de buzones es compatible con el módulo Antivirus en los servidores Microsoft Exchange 2003, 2007 y 2010.

Panda Adaptive Defense 360 ejecuta la acción configurada 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 Panda Adaptive Defense 360 recibirá el mensaje original con los adjuntos desinfectados o, en caso de que no fuera posible su desinfección, con un fichero "security_alert.txt" adjuntado describiendo el motivo de la detección.

Protección de transporte

Se utiliza en servidores Exchange con el rol de Acceso de clientes, Edge Transport y Hub, y analiza el tráfico que atraviesa al servidor Microsoft Exchange en busca de virus, herramientas de hacking y programas potencialmente no deseados sospechosos, con destino a buzones situados en el servidor Exchange.

La protección de transporte es compatible con todas las versiones de Microsoft Exchange desde 2003 y no permite manipular los mensajes analizados; si el correo contiene un elemento peligroso se introduce íntegro en cuarentena. El usuario protegido con Panda Adaptive Defense 360 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.

Software a detectar

Haz clic en los botones de activación para detectar diferentes tipos de amenazas:

- Detectar virus
- Detectar herramientas de hacking y PUPs

Escaneo inteligente de buzones

El escaneo inteligente de buzones aprovecha los momentos de baja actividad del servidor Exchange para examinar los correos almacenados en sus buzones. Además, sólo comprueba los archivos que no han sido previamente analizados con el fichero de firmas descargado. Cuando el fichero de firmas se actualiza, Panda Adaptive Defense 360 lanzará otro escaneo inteligente de buzones de forma automática.

Restauración de mensajes con virus y otras amenazas

Configura el servidor SMTP que reenviará los mensajes restaurados desde la consola de administración. Para ello completa los siguientes campos:

Campo	Descripción
Servidor SMTP	Dirección IP o dominio del servidor de correo.
El servidor requiere autenticación	Haz clic en el botón de activación si el servidor SMTP no es "open relay".
Usuario	Cuenta de usuario con permisos para enviar correos en el servidor.
Contraseña	Contraseña de la cuenta de usuario con permisos para enviar correos en el servidor.

Tabla 12.20: Configuración del servidor de correo para el reenvío de mensajes con amenazas detectadas

Si no se configura ningún servidor SMTP, los mensajes se restaurarán en una carpeta del disco duro del servidor Exchange.

Anti spam para servidores Exchange

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

Al activar la protección Anti Spam Panda Adaptive Defense 360 muestra una ventana emergente sugiriendo añadir varias reglas de exclusión para mejorar el rendimiento del servidor de correo.

Acción para mensajes de spam

Selecciona la acción a realizar con los mensajes de spam:

Acción	Descripción
Dejar pasar el mensaje	Añade la etiqueta Spam al asunto de los mensajes. Esta será la opción configurada por defecto.
Mover el mensaje a...	Reenvía el mensaje a una dirección de correo electrónico gestionada por el servidor Microsoft Exchange y le añade la etiqueta "Spam" al asunto.
Borrar el mensaje	Borra el mensaje del servidor de correo.
Marcar con SCL (Spam Confidence Level)	SCL es una marca que el módulo de protección anti spam añade a las cabeceras de los mensajes de correo, y que representa la probabilidad de que el mensaje sea spam a través de una escala comprendida entre el 0 y el 9, ordenada de menor a mayor probabilidad. Panda Adaptive Defense 360 no ejecuta ninguna acción sobre los mensajes marcados con SCL, que se tratarán posteriormente en función del umbral configurado en el Directorio Activo por el administrador de la red.

Tabla 12.21: Acciones permitidas por Panda Adaptive Defense 360 frente a los mensajes de spam

Direcciones y dominios permitidos

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

Añade varias direcciones y dominios separados por el carácter ",".

Direcciones y dominios de spam

Son 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 que pertenece 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 que pertenece 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 se encuentra en lista negra y un subdominio de este 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 consideran incluidos en lista blanca todos sus subdominios.

Filtrado de contenidos para servidores Exchange

Filtra los mensajes de correo electrónico en función de la extensión de los archivos adjuntos incluidos en ellos.

Una vez establecida la lista de mensajes susceptibles de albergar adjuntos sospechosos, indica qué acción ejecutará la protección sobre ellos:

Acción	Descripción
Acción a realizar	Borra los mensajes o los desvía a otra dirección de correo electrónico para analizar posteriormente 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 a bloquear.
Considerar archivos adjuntos peligrosos todos los que tienen doble extensión, excepto en los siguientes casos	Impide la entrada de todos los mensajes de correo electrónico con adjuntos de doble extensión, excepto aquellos que tengan las extensiones seleccionadas. Utiliza los botones Añadir , Eliminar , Vaciar o Restaurar para configurar la lista de dobles extensiones permitidas.

Tabla 12.22: Acciones permitidas por el filtrado de contenidos para servidores Microsoft Exchange

Registro de detecciones

Todas las detecciones producidas en un servidor Exchange son almacenadas localmente en un archivo CSV con 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:

```
%ProgramData%\Panda Security\Panda Security Protection\Exchange
```

excepto en Windows 2003 que se almacena en la carpeta:

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

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

Campo	Descripción
Date	Fecha de la llegada del correo al servidor Exchange.
From	Origen del mensaje de correo.
To	Destinatario del mensaje de correo.
Subject	Asunto del mensaje de correo.
Attachments	Listado con los ficheros adjuntos al correo.
Protection	Módulo de protección que desencadenó la acción ejecutada sobre el mensaje. • AntiSpam • Content Filter • Antimalware
Action	Acción ejecutada sobre el mensaje. • Borrado • Modificado • SCL Tagged

Tabla 12.23: Campos del fichero ExchangeLogDetections

Capítulo 13

Configuración de seguridad Android

Panda Adaptive Defense 360 centraliza en el menú superior **Configuración** toda la configuración de los parámetros de seguridad para smartphones y tablets. Haz clic en el panel de la izquierda **Dispositivos Android** para mostrar un listado con todas las configuraciones de seguridad ya creadas o para crear nuevas.

A continuación se muestran todos los parámetros incluidos en la configuración de seguridad y antirrobo para dispositivos Android y se indican algunas recomendaciones prácticas para asegurar móviles y tablets, minimizando los inconvenientes en su manejo al usuario.



Para obtener información adicional sobre los distintos apartados del módulo Dispositivos Android consulta las referencias siguientes:

- “**Crear y gestionar configuraciones**” en la página **213**: información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.
- “**Control y supervisión de la consola de administración**” en la página **67**: gestión de cuentas de usuario y asignación de permisos.

CONTENIDO DEL CAPÍTULO

Configuración de Dispositivos Android	266
Acceso a la configuración	266
Permisos requeridos	266
Actualización	266
Antivirus	266
Exclusiones	266
Antirrobo	267
Comportamiento	267
Privacidad	267

Configuración de Dispositivos Android

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Dispositivos Android**.
- Haz clic en el botón Añadir, se abrirá la ventana de configuración de Dispositivos Android.

Permisos requeridos

Permiso	Tipo de acceso
Configurar seguridad para dispositivos Android	Crear, modificar, borrar, copiar o asignar las configuraciones de Dispositivos Android.
Ver configuraciones de seguridad para dispositivos Android	Visualizar las configuraciones de Dispositivos Android.

Tabla 13.1: Permisos requeridos para acceder a la configuración Dispositivos Android

Actualización

Establece el tipo de conexión que utilizará el dispositivo para descargar las actualizaciones de la nube de Panda Security



La configuración de las actualizaciones se describe en "[Actualización del software cliente](#)" en la página [153](#).

Antivirus

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

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

Exclusiones

Excluye del análisis 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.

Antirrobo

La configuración de antirrobo permite enviar acciones a los dispositivos para evitar la filtración de los datos que contienen o favorecer su localización en caso de pérdida o robo del terminal.

Haz clic en el selector **Protección antirrobo** para activar la funcionalidad.



Consulta "[Sección general en dispositivos Android](#)" en la página 196 para obtener información sobre las acciones antirrobo disponibles en Panda Adaptive Defense 360.

Comportamiento

Establece las funcionalidades antirrobo del dispositivo Android:

Campo	Descripción
Informar de la localización del dispositivo	El dispositivo envía sus coordenadas GPS al servidor Panda Adaptive Defense 360.
Sacar foto al tercer intento de desbloqueo y enviarla por email	Si el usuario del dispositivo falla tres veces consecutivas al desbloquearlo se tomará una fotografía y se enviará por correo electrónico a las direcciones de correo separadas por coma introducidas en la caja de texto.

Tabla 13.2: Funcionalidades antirrobo de dispositivos Android

Privacidad

Permite al usuario activar el modo privacidad, que impide la toma de fotografías y el registro de las coordenadas GPS del dispositivo y posterior envío al servidor de Panda Adaptive Defense 360.

Capítulo 14

Panda Data Control (Supervisión de información sensible)

Los ficheros clasificados como PII (Personally Identifiable Information) son archivos sin estructura interna con información que permite identificar a personas relacionadas con la empresa (clientes, trabajadores, proveedores, etc.). Esta información es de carácter personal y su tipo es muy variado, como pueden ser números de la seguridad social, números de teléfono y direcciones de correo electrónico, entre otros.

Panda Data Control es el módulo de seguridad de Panda Adaptive Defense 360 que permite a las empresas cumplir con las regulaciones sobre protección de datos, como por ejemplo la GDPR. Además, supervisa y mejora la visibilidad de la información personal (PII) almacenada en la infraestructura IT de las organizaciones.

Para ello, Panda Data Control ofrece tres funcionalidades clave:

- Genera un inventario diario y completo de ficheros PII que incluye información básica, como puede ser su nombre, extensión y el nombre del equipo donde se encontró.
- Descubre, audita y monitoriza en tiempo real el ciclo de vida de los ficheros PII: desde los datos en reposo, las operaciones efectuadas sobre ellos y su llegada y comunicación hacia el exterior.
- Ofrece herramientas de búsqueda flexible por contenido y borrado de ficheros duplicados que contienen datos personales, con el objetivo de limitar su almacenamiento y difusión en la red de la

empresa.



Para obtener información adicional sobre los distintos apartados del módulo Panda Data Control consulta las referencias siguientes:

- “[Crear y gestionar configuraciones](#)” en la página [213](#): información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.
- “[Control y supervisión de la consola de administración](#)” en la página [67](#): gestión de cuentas de usuario y asignación de permisos.
- “[Gestión de listados](#)” en la página [56](#): información sobre como gestionar listados.



Consulta la [Guía de administración de Panda Data Control](#) para obtener más información sobre la consola de gestión específica para este servicio.

CONTENIDO DEL CAPÍTULO

Introducción al funcionamiento de Panda Data Control - - - - -272

Entidad 272

Fichero PII 272

Ficheros sin estructura interna y componentes IFilter 272

Proceso de indexación 273

Proceso de normalización 273

Inventario de ficheros PII 273

Búsquedas de ficheros 273

Seguimiento de las acciones sobre ficheros PII 273

Requisitos de Panda Data Control - - - - -274

Plataformas soportadas 274

Instalación del componente Microsoft Filter Pack 274

Microsoft Filter Pack y Microsoft Office 274

Instalación independiente del Microsoft Filter Pack 274

El proceso de indexación - - - - -274

Configurar el alcance, momento y tipo de indexación 275

Inventario de ficheros PII - - - - -275

Visualizar el inventario 275

Monitorización continua de ficheros - - - - -276

Monitorización de ficheros PII 276

Monitorización de ficheros designados por el administrador 276

Búsqueda de ficheros - - - - -276

Requisitos de las búsquedas 276

Widget de búsquedas 276

Propiedades y requisitos de las búsquedas 277

Propiedades de las búsquedas 277

Proceso de normalización 278

Crear una búsqueda 279

Crear una búsqueda libre 279

Crear una búsqueda guiada 280

Búsquedas almacenadas 281

Cambiar el nombre de una búsqueda almacenada 281

Hacer una copia de una búsqueda almacenada 281

Volver a lanzar una búsqueda almacenada 281

Cancelar y eliminar búsquedas almacenadas 281

Editar búsquedas almacenadas 281

Visualizar los resultados de una búsqueda 281

Sintaxis de las búsquedas	283
Sintaxis admitida en búsquedas rápidas	283
Sintaxis admitida en búsquedas guiadas	284
Entidades disponibles	284
Sintaxis de las búsquedas con entidades	285
Consejos para construir búsquedas compatibles con la normalización	285
Búsqueda de ficheros duplicados - - - - -	286
Definición de fichero duplicado	286
Búsqueda de ficheros duplicados	286
Borrado y restauración de ficheros - - - - -	287
Borrar ficheros de los equipos de la red	287
Estados de la acción de borrado	287
Backup de ficheros borrados por Panda Data Control	287
Borrado de ficheros	287
Visualizar ficheros borrados	288
Restaurar ficheros previamente borrados por el administrador	288
Estados de la acción de restaurar	289
Restaurar ficheros borrados	289
Configuración de Panda Data Control - - - - -	289
Acceso a la configuración	289
Requisitos para buscar y seguir documentos Microsoft Office	290
Información personal (inventario, búsquedas y seguimiento)	290
Exclusiones	290
Monitorización de archivos por reglas	291
Reglas de monitorización	291
Opciones avanzadas de indexación	292
Indexar el siguiente contenido	293
Programar períodos de indexación	293
Escritura en unidades de almacenamiento extraíbles	293
Paneles / widgets del módulo Panda Data Control - - - - -	294
Acceso al panel de control	294
Estado del despliegue	294
Equipos sin conexión	296
Estado de la actualización	297
Estado de la indexación	298
Características activadas en los equipos	299
Archivos eliminados por el administrador	300
Archivos con información personal	301
Equipos con información personal	303
Archivos por tipo de información personal	304
Listados del módulo Panda Data Control - - - - -	305
Acceso a los listados	305
Permisos requeridos	306
Estado de Data Control	306
Archivos con información personal	311
Equipos con información personal	314
Archivos eliminados por el administrador	318
Extensiones de programas soportadas - - - - -	321
Empaquetadores y algoritmos de compresión soportados - - - - -	323
Entidades y países soportados - - - - -	323
Países soportados	324

Introducción al funcionamiento de Panda Data Control

Para una correcta comprensión de los procesos involucrados en el descubrimiento y seguimiento de la información personal almacenada en los equipos de la empresa, es necesario asimilar algunos conceptos relativos a las tecnologías utilizadas en Panda Data Control.

Entidad

Cada pieza o grupo de palabras con significado propio referido a un tipo concreto de información personal recibe el nombre de "entidad". Entidades comúnmente analizadas son el DNI, nombres y apellidos y números de teléfono, entre otras.

Debido a la naturaleza ambigua y variable del lenguaje natural en sus múltiples idiomas, una misma entidad puede presentarse de formas muy diferentes, por lo que es necesario aplicar algoritmos flexibles y adaptables para su detección. De manera general, el análisis de entidades busca formatos o expresiones predefinidas, y utiliza el contexto local en torno a esa detección, o la presencia o ausencia de determinadas palabras clave, para evitar falsos positivos. Consulta "[Entidades y países soportados](#)".

Fichero PII

Una vez realizada la identificación de entidades se evalúa el contexto en el que aparecen para determinar si con la información que aportan es posible identificar a una persona concreta. En tal caso, el fichero será susceptible de ser protegido por protocolos específicos de tratamiento y acceso a los datos que permitan a la empresa cumplir con la normativa vigente (GDPR, PCI, etc.). Esta evaluación combina un modelo Machine learning supervisado con un modelo experto basado en ponderación de entidades y análisis del contexto global del documento, para clasificar a un fichero con entidades detectadas como un fichero PII a proteger.

Ficheros sin estructura interna y componentes IFilter

Para clasificar un fichero como PII, Panda Data Control analiza archivos sin estructura (ficheros de texto en múltiples formatos, hojas de cálculo, ficheros de presentación Powerpoint etc.) en busca de entidades. Para interpretar correctamente el contenido de estos archivos se requieren algunos componentes de terceros fabricantes instalados en el equipo del usuario. Estos componentes reciben el nombre de "IFilters" y no forman parte del paquete de instalación de Panda Adaptive Defense 360. Microsoft Search, Microsoft Exchange Server y Microsoft Sharepoint Server entre otros servicios del sistema operativo y productos independientes utilizan los componentes IFilter para indexar los ficheros del usuario y habilitar búsquedas por contenido.

Cada formato de fichero compatible con Panda Data Control tiene su propio componente IFilter asociado, y muchos de ellos forman parte de la instalación básica de Windows, aunque otros tienen que ser instalados o actualizados de forma manual.

Microsoft Filter Pack es un paquete de distribución gratuito que contiene todos los componentes IFilter asociados a la suite de ofimática Microsoft Office. Una vez instalado, Panda Data Control será capaz de analizar el contenido de todos los formatos de fichero soportados por la suite. Consulta [“Instalación del componente Microsoft Filter Pack”](#).

Proceso de indexación

Es el proceso de inspección y almacenaje del contenido de todos los ficheros soportados por Panda Data Control con el fin de generar un inventario de ficheros PII y permitir búsquedas de ficheros por contenido. El proceso de indexación es una tarea de bajo impacto en el rendimiento del equipo, aunque su finalización puede alargarse en el tiempo. Por esta razón el administrador puede programar su inicio o limitarla para acelerar su finalización y para mejorar el resultado de los resultados devueltos por las búsquedas. Consulta [“El proceso de indexación”](#).

Proceso de normalización

Al ejecutar el proceso de indexación Panda Data Control aplica ciertas reglas para homogeneizar los datos recogidos. El objetivo de este proceso es almacenar de forma individual cada palabra y facilitar su posterior búsqueda, así como reducir su tiempo de ejecución. Las reglas a aplicar en el proceso de normalización varían si se trata de almacenar una entidad o texto plano. Consulta [“Proceso de normalización”](#).

Inventario de ficheros PII

Una vez indexado el equipo e identificadas las entidades y los ficheros PII, Panda Data Control construye un inventario accesible por el administrador de la red con los nombres de los ficheros y sus características, que se envía al servidor Panda Adaptive Defense 360 una vez al día. Consulta [“Inventario de ficheros PII”](#).



Panda Data Control no envía el contenido de los ficheros PII al servidor Panda Adaptive Defense 360. Únicamente se envían sus atributos (nombre, extensión etc.) y el número y tipo de entidades descubiertas.

Búsquedas de ficheros

Panda Data Control localiza ficheros por su nombre, extensión o contenido en las unidades de almacenamiento indexadas de los equipos de la red.

Las búsquedas se ejecutan en tiempo real: tan pronto como el administrador lanza una búsqueda, ésta se despliega en los equipos de la red y comienza a reportar resultados conforme se van produciendo, sin esperar a completar la ejecución por completo. Consulta [“Búsqueda de ficheros”](#).

Seguimiento de las acciones sobre ficheros PII

Panda Data Control monitoriza los eventos realizadas sobre los ficheros PII y los envía a la consola Advanced Visualization Tool. Esta herramienta muestra la evolución de los ficheros PII permitiendo

determinar si fueron copiados, movidos, enviados por correo, etc. Para obtener más información sobre Advanced Visualization Tool consulta la Guía de administración de Panda Data Control en <https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-Guia-ES>.

Requisitos de Panda Data Control

Plataformas soportadas

Panda Data Control es compatible con la plataforma Microsoft Windows desde la versión XP SP3 en adelante y Windows 2003 SP1 y superiores. Otros sistemas operativos como Linux o macOS no están soportados.

Instalación del componente Microsoft Filter Pack

Microsoft Filter Pack y Microsoft Office

El componente Microsoft Filter Pack viene incluido en la suite de ofimática Office, aunque solo se instalarán de forma automática los componentes IFilter que se corresponden con los productos de la suite instalados en el equipo del usuario. Para tener la seguridad de que todos los componentes estén disponibles en el equipo en su versión 2010, consulta el punto “[Instalación independiente del Microsoft Filter Pack](#)”.

Instalación independiente del Microsoft Filter Pack

Para instalar el Microsoft Filter Pack haz clic en la siguiente URL:

<https://www.microsoft.com/en-us/download/details.aspx?id=17062>

El paquete es compatible con Windows XP SP3, Windows 2013 SP1 y superiores, aunque en algunos casos se requerirá la instalación de la librería Microsoft Core XML Services 6.0.

El proceso de indexación

Es el proceso de inspección y almacenaje del contenido de todos los ficheros soportados por Panda Data Control. Este proceso es imprescindible para poder generar el inventario de ficheros PII y también para buscar ficheros en los equipos por su contenido, y se configura de forma transparente al activar alguna de estas dos funcionalidades. La información indexada se almacena de forma local en el equipo de cada usuario en la ruta %ProgramData%\Panda Security\Panda Security Protection\indexstore.

Aunque el proceso de indexado es una tarea de bajo impacto en el rendimiento del equipo, puede alargarse en el tiempo. Por esta razón, Panda Data Control está configurado para lanzar una única

vez el proceso en el momento en que se activa el módulo en cada equipo de la red, y cada vez que la tecnología de detección de entidades cambie para soportar mejoras.

Una vez terminada la indexación, Panda Data Control comienza a monitorizar la creación de nuevos ficheros y el borrado y modificación de los ya existentes para actualizar el índice. La información con las nuevas entidades detectadas se envía al servidor Panda Adaptive Defense 360 cada 24 horas.

Configurar el alcance, momento y tipo de indexación

Es posible excluir los resultados de ciertas carpetas o ficheros, o incluso variar la precisión de las búsquedas devueltas por Panda Data Control.

- Para no devolver información de ciertas carpetas o ficheros consulta "[Exclusiones](#)".
- Para variar la precisión de las búsquedas consulta "[Indexar el siguiente contenido](#)".
- Para determinar la franja horaria en la que se ejecutará el proceso de indexado consulta "[Programar períodos de indexación](#)".

Inventario de ficheros PII



Panda Data Control no envía el contenido de los ficheros PII al servidor Panda Adaptive Defense 360. Únicamente se envían sus atributos (nombre, extensión etc.) y el número y tipo de entidades descubiertas.

El inventario de ficheros PII muestra los ficheros PII que Panda Data Control ha encontrado en la red del cliente.

Para activar el inventario consulta "[Información personal \(inventario, búsquedas y seguimiento\)](#)".

Visualizar el inventario

Panda Data Control incorpora varios recursos para controlar los ficheros PII encontrados en la red y determinar el tipo de entidades que contienen.

- Para obtener estadísticas del número de ficheros PII encontrados consulta "[Archivos con información personal](#)".
- Para obtener estadísticas del número de equipos con ficheros PII encontrados consulta "[Equipos con información personal](#)".
- Para obtener un listado con el detalle de los ficheros PII encontrados consulta "[Archivos con información personal](#)".
- Para obtener un listado con el detalle de los equipos que contienen ficheros PII consulta "[Equipos con información personal](#)".

Monitorización continua de ficheros

Monitorización de ficheros PII

Panda Data Control recopila todos los eventos relativos a la creación, modificación o borrado de ficheros PII para poder visualizar la actividad realizada y detectar situaciones peligrosas, tales como robo de datos, acceso no autorizada a información, etc.

Para visualizar las acciones realizadas sobre los ficheros PII accede a **Advanced Visualization Tool** desde la parte inferior del panel lateral del menú superior **Estado**. Consulta la Guía para el usuario de Panda Data Control en <https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/DATACONTROL-AETHER-Guia-ES.pdf> para obtener toda la información necesaria.

Para activar la monitorización de las acciones efectuadas sobre los ficheros PII consulta "[Información personal \(inventario, búsquedas y seguimiento\)](#)".

Monitorización de ficheros designados por el administrador

Además de monitorizar de forma automática los ficheros clasificados por Panda Data Control como PII, el administrador puede añadir mediante reglas nuevos tipos de ficheros para monitorizar. Consulta "[Monitorización de archivos por reglas](#)" para más información.

Búsqueda de ficheros

Requisitos de las búsquedas

Para realizar una búsqueda de ficheros en los equipos de la red es necesario cumplir con los siguientes requisitos:

- La cuenta de usuario que lanza la búsqueda desde la consola web tiene que tener asignado un rol con el permiso **Buscar información en los equipos**. Consulta "[Control y supervisión de la consola de administración](#)" en la página [67](#) para obtener más información sobre los roles.
- Los equipos sobre los que se ejecutan las búsquedas deben de contar con una licencia de Panda Data Control asignada.
- Los equipos sobre los que se ejecutan las búsquedas deben de tener asignada una configuración de Data Control con la opción **Permitir realizar búsquedas de información en los equipos** habilitada. Consulta "[Configuración de Panda Data Control](#)".

Widget de búsquedas

Es el punto de entrada para toda la funcionalidad, y permite visualizar búsquedas y gestionarl

Para acceder al widget **Búsquedas** haz clic en el menú superior **Estado**, panel lateral **Data Control**

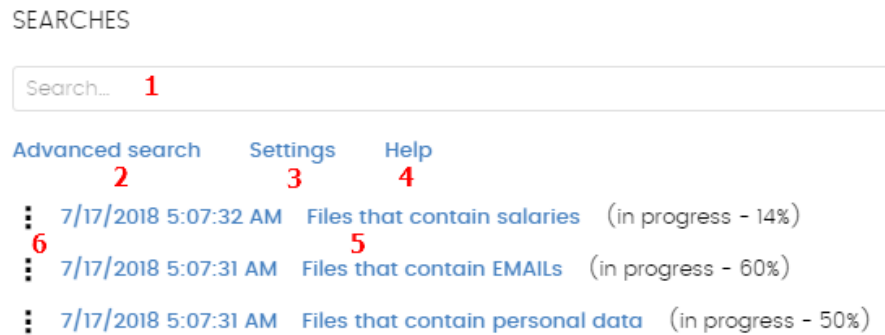


Figura 14.1: Panel Búsquedas

El widget contiene los controles mostrados a continuación:

- **(1) Caja de texto** para introducir los términos a buscar. Consulta [“Sintaxis de las búsquedas”](#) para una descripción de los comandos aceptados por Panda Data Control.
- **(2) Búsqueda avanzada:** limita el ámbito de búsqueda.
- **(3) Configuración:** acceso al listado de perfiles de configuración de Data Control. Para más información consulta [“Configuración de Panda Data Control”](#).
- **(4) Ayuda:** enlace a la página web de soporte de Panda Security donde se muestra la sintaxis de las búsquedas de Panda Data Control actualizada con los últimos cambios introducidos.
- **(5) Búsquedas almacenadas:** búsquedas definidas anteriormente y que pueden ser relanzadas en el parque informático.
- **(6) Menú de contexto de la búsqueda:** permite editar el nombre de la búsqueda, cambiar sus parámetros, volverla a lanzar y eliminarla.

Propiedades y requisitos de las búsquedas

Para completar con éxito una búsqueda es necesario cumplir con los siguientes requisitos:

- La cuenta de usuario que lanza la búsqueda desde la consola web tiene que tener asignado un rol con el permiso **Buscar información en los equipos**. Consulta [“Control y supervisión de la consola de administración”](#) en la página 67 para obtener más información sobre los roles.
- Los equipos sobre los que se efectúan las búsquedas deben de contar con una licencia de Panda Data Control asignada.
- Los equipos sobre los que se efectúan las búsquedas deben de tener asignada una configuración de Data Control con la opción **Permitir realizar búsquedas de información en los equipos** habilitada.

Propiedades de las búsquedas

- El número de búsquedas concurrentes por cada cuenta de usuario es 10. Pasado este número se mostrará un mensaje de error en la consola web.

- El número máximo de búsquedas guardadas por cuenta de usuario es 30. Pasado este número se mostrará un mensaje de error en la consola web.
- El número máximo de resultados en total por cada búsqueda es 10.000. Los resultados más allá de este número no se mostrarán en la consola web.
- El número máximo de resultados por cada equipo es 10.000 / número de equipos sobre los que se ejecuta la búsqueda. De esta forma, si se busca sobre un parque de 100 equipos, el número máximo de resultados mostrados será $10.000 / 100 = 100$ resultados por equipo.
- El número mínimo de resultados mostrados por equipo, independientemente del número de equipos de la red es 10.
- El número máximo de equipos sobre los que se ejecutan búsquedas de forma simultánea es 50. Si el número total de equipos que participaran en la búsqueda es mayor, las búsquedas más allá de este límite se mantendrán en espera hasta que las primeras se vayan completando.

Proceso de normalización



El proceso de normalización no influye en la detección de entidades.

Panda Data Control aplica una serie de reglas a los datos recibidos del proceso de indexación para homogeneizarlos. Debido a que las búsquedas ejecutadas por el administrador se aplican sobre los datos ya normalizados, es necesario conocer estas reglas dado que pueden influir en los resultados mostrados en la consola web.

- **Transformación de las cadenas a minúsculas**

Antes de almacenar una cadena en la base de datos, ésta se transforma a minúsculas.

- **Caracteres de separación**

Panda Data Control detecta un grupo de caracteres especiales que considera como separadores entre palabras y que retira completamente del índice, excepto si esos caracteres forma parte de una entidad:

- **Retorno de carro:** \r
- **Salto de línea:** \n
- **Tabulador:** \t
- **Caracteres:** " : ; ! ? - + _ * = () [] { } , . | % \ / ' "

Por ejemplo "Panda.Data(Control)" se almacenará como tres palabras sueltas sin los caracteres de puntuación: "panda", "data" y "control".

- **Normalización de entidades**

El proceso de normalización de entidades sigue reglas independientes:

Entidad	Caracteres de separación	Configuración de la indexación
• Cuentas bancarias • Tarjetas de crédito • Número de identidad personal • Números de teléfono • Números de carnet de conducir • Números de pasaporte • Números de la seguridad social	Se eliminan. La entidad se almacena en el índice como un único elemento.	No se tiene en cuenta
• Direcciones IP • Direcciones de correo electrónico	Se respetan. La entidad se almacena en el índice como un único elemento.	No se tiene en cuenta
• Nombres y apellidos • Direcciones físicas	Se utilizan como carácter separador. La entidad se almacena en el índice como varios elementos.	Si se tiene en cuenta

Tabla 14.1: Reglas de normalización de entidades

- **Ejemplos de normalización de entidades**

- "1.42.67.116-C" se almacena como la entidad de tipo IDCARD "14267116C".
- "192.168.1.1" se almacena como la entidad de tipo IP "192.168.1.1".
- "Calle Santiago de Compostela 5 1º Izquierda" se almacenará como "calle", "santiago", "de", "compostela", "izquierda" si el método de indexación es **Solo texto** o como "calle", "santiago", "de", "compostela", "5", "1", "izquierda" si el método de indexación es **Todo**.

Crear una búsqueda

Crear una búsqueda libre

- Haz clic en el menú superior **Estado**, panel lateral **Data Control**.
- Introduce en la caja de texto del widget **Búsquedas** los términos de búsqueda según la sintaxis mostrada en "[Sintaxis de las búsquedas](#)".
- Haz clic en el icono  o pulsa la tecla Enter.

Una vez introducida la búsqueda se abrirá la ventana **Resultados de la búsqueda**. Consulta "[Búsquedas almacenadas](#)" para editar la búsqueda introducida.

Crear una búsqueda guiada

- Haz clic en el menú superior **Estado**, panel lateral **Data Control**.
- Haz clic en el enlace **Búsqueda avanzada**.
- Elige en el selector **Búsqueda guiada**.
- Configura los parámetros de la búsqueda.
- **Parámetros de búsqueda avanzada:**

Parámetro	Descripción
Nombre de la búsqueda	Establece un nombre para la búsqueda almacenada.
Buscar archivos con	Introduce el contenido a buscar. Se incluyen tres cajas de texto. • Todas estas palabras o frases exactas: busca los ficheros que contienen todas las palabras o entidades indicadas. • Alguna de estas palabras o frases exactas: busca los ficheros que contienen alguna o todas las palabras o entidades indicadas. • Ninguna de estas palabras o frases exactas: busca los ficheros que no contienen ninguna de las palabras.
Información personal	Marca las casillas de selección para indicar las entidades que deberán aparecer en los ficheros PII buscados. • Todos: todas las entidades seleccionadas deberán detectarse en el fichero PII (lógica AND) para que el fichero se incluya en la lista de encontrados. • Alguno: algunas o todas las entidades seleccionadas deberán detectarse en el fichero PII (lógica OR) para que el fichero se incluya en la lista de encontrados.
Limitar la búsqueda a	Equipos: • Todos: busca el contenido introducido en todos los equipos que tengan una licencia de Panda Data Control asignada y esté habilitada la opción de búsqueda en su configuración. • Los siguientes equipos: muestra un listado de los equipos que tengan una licencia de Panda Data Control asignada. Indica con las casillas de selección los equipos en los que se buscará el contenido introducido. • Los siguientes grupos de equipos: muestra el árbol de grupos con la jerarquía de equipos configurada en Panda Adaptive Defense 360. Indica con la casilla de selección los grupos donde se buscará el contenido introducido.
Cancelar automáticamente la búsqueda	Indica el tiempo de espera para los equipos apagados o sin conexión antes de cancelar la búsqueda.

Tabla 14.2: Parámetros de la búsqueda avanzada

Búsquedas almacenadas

Tanto las búsquedas libres como las guiadas se almacenan para poder ser lanzadas posteriormente de forma rápida.

Una vez creada una nueva búsqueda, ésta aparecerá en el widget **Búsquedas** con la fecha y hora de su creación, junto al nombre y una leyenda indicando su estado (**En curso**, **Cancelada**) o sin estado (**Finalizada**).

Cambiar el nombre de una búsqueda almacenada

Haz clic en el menú de contexto (6 en la figura 14.1) de la búsqueda y elige **Cambiar nombre**.

Hacer una copia de una búsqueda almacenada

Para duplicar una búsqueda almacenada haz clic en el menú de contexto (6 en la figura 14.1) de la búsqueda y elige **Hacer una copia**. Se mostrará la ventana de configuración de la búsqueda y se renombrará a "Copia de ".

Volver a lanzar una búsqueda almacenada

Haz clic en el menú de contexto de la búsqueda (6 en la figura 14.1) y elige **Relanzar búsqueda**. El estado de la búsqueda cambiará e indicará el porcentaje de la tarea realizada.

Cancelar y eliminar búsquedas almacenadas

Haz clic en el menú de contexto de la búsqueda (6 en la figura 14.1) y elige **Cancelar** para interrumpir la búsqueda o en **Borrar** para cancelarla y borrarla del widget **Búsquedas**.

Editar búsquedas almacenadas

Haz clic en el menú de contexto (6 en la figura 14.1) y elige **Editar búsqueda** para abrir la ventana de búsqueda avanzada con sus parámetros cargados y modificarla.

Visualizar los resultados de una búsqueda

Para visualizar el resultado de una búsqueda accede al listado **Buscar en los equipos** de dos formas:

- Haciendo clic en una búsqueda almacenada.
- Creando una nueva búsqueda.

Este listado muestra los equipos que contienen la cadena de búsqueda introducida, junto al nombre del fichero encontrado y otra información útil.

- **Cabecera de listado**

Configura los parámetros de la búsqueda rápida:

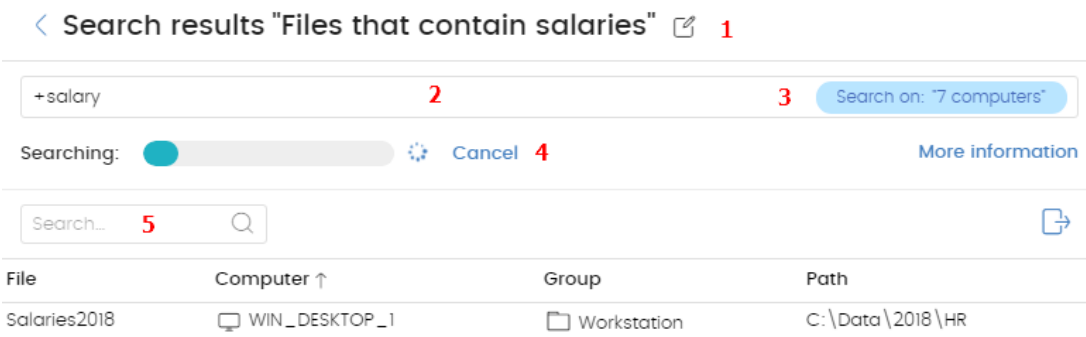


Figura 14.2: Ventana Resultados de una búsqueda

- **(1) Icono** : cambia el nombre de la búsqueda.
 - **(2) Caja de texto**: contenido de la búsqueda.
 - **(3) Buscar en: "x equipos"**: abre la ventana de búsqueda avanzada para refinarla.
 - **(4) Buscando**: estado de la búsqueda (**En curso**, **Cancelada**). Si la búsqueda no se ha iniciado o ha terminado no se indica el estado.
 - **(5) Caja de texto Buscar**: filtra los resultados mostrados en la tabla de resultados por el nombre de equipo.
- **Campos del listado**

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Panda Adaptive Defense 360 al que pertenece el equipo.	Cadena de caracteres
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres

Tabla 14.3: Campos del listado Búsqueda de información personal en los equipos

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Archivo	Nombre del fichero encontrado.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró el fichero.	Cadena de caracteres
Grupo	Grupo de Panda Adaptive Defense 360 al que pertenece el equipo.	Cadena de caracteres

Tabla 14.4: Campos del fichero exportado Búsqueda de información personal en los equipos

Campo	Comentario	Valores
Ruta	Ruta dentro del dispositivo de almacenamiento donde se encuentra el fichero.	Cadena de caracteres
DNI's	Indica si se detectó una o más entidades del tipo Documento Nacional de Identidad o equivalentes (Documento de identidad, Cédula de identidad / ciudadanía, Registro civil etc.) en el fichero.	Booleano
Pasaportes	Indica si se detectó una o más entidades del tipo Pasaporte en el fichero.	Booleano
Tarjeta de crédito	Indica si se detectó una o más entidades del tipo Número de tarjeta de crédito en el fichero.	Booleano
Cuentas bancarias	Indica si se detectó una o más entidades del tipo Número de cuenta bancaria en el fichero.	Booleano
Permisos de conducir	Indica si se detectó una o más entidades del tipo Permiso de conducir en el fichero.	Booleano
Números de la Seguridad Social	Indica si se detectó una o más entidades del tipo Número de la seguridad social en el fichero.	Booleano
Direcciones de correo electrónico	Indica si se detectó una o más entidades del tipo Dirección de correo electrónico en el fichero.	Booleano
IPs	Indica si se detectó una o más entidades del tipo Dirección IP en el fichero.	Booleano
Nombres y apellidos	Indica si se detectó una o más entidades del tipo Nombre y apellidos en el fichero.	Booleano
Direcciones	Indica si se detectó una o más entidades del tipo Dirección en el fichero.	Booleano
Números de teléfono	Indica si se detectó una o más entidades de tipo Número de teléfono en el fichero.	Booleano

Tabla 14.4: Campos del fichero exportado Búsqueda de información personal en los equipos

Sintaxis de las búsquedas

Panda Data Control permite búsquedas flexibles de ficheros por contenido utilizando texto plano y modificadores para acotar el ámbito de los resultados.

Sintaxis admitida en búsquedas rápidas

- **Palabra**: busca "palabra" en el contenido del documento y en los metadatos.
- **PalabraA PalabraB**: busca "palabraa" o "palabrab" (operador OR) en el contenido del documento.
- **"PalabraA PalabraB"**: busca "palabraa" y "palabrab" seguidas en el contenido del documento.

- **+PalabraA +PalabraB:** busca "palabraa" y "palabrab" en el contenido del documento.
- **+Palabraa -Palabrab:** busca "palabraa" y no "palabrab" en el contenido del documento.
- **Palabra*:** busca todas las palabras que empiezan por "palabra". El carácter "*" solo se permite al final de la cadena de caracteres a buscar.
- **Pa?abra:** busca todas las palabras que empiezan por "pa", terminan por "abra" y tienen entre los dos grupos un único carácter alfabético. El carácter "?" puede ir colocando en cualquier punto de la cadena de caracteres a buscar.
- **Palabra~:** busca todas las palabras que contienen la cadena de caracteres "palabra".

Sintaxis admitida en búsquedas guiadas

En las búsquedas guiadas no se utilizan los caracteres "+" y "-". En su lugar las palabras a buscar se distribuyen en las diferentes cajas de texto presentadas en la pantalla. Si utilizas los caracteres "+" y "-", éstos formarán parte de la búsqueda.

Entidades disponibles

Para acotar el ámbito de los resultados Panda Data Control admite el uso de calificadores para indicar entidades o características del fichero en las búsquedas rápidas y avanzadas. Los calificadores disponibles son:

Calificador	Descripción
PiiType	Especifica si un tipo de entidad fue detectada en el fichero.
HasPii	Indica que el fichero contiene entidades detectadas.
Filename	Indica el nombre del fichero.
FileExtension	Indica la extensión del fichero.

Tabla 14.5: Calificadores disponibles

Los valores admitidos para los calificadores son:

Calificador	Descripción
PiiType:BANKACCOUNT	Ficheros que contienen una o más entidades de tipo Cuenta bancaria.
PiiType:CREDITCARD	Ficheros que contienen una o más entidades de tipo Tarjeta de crédito.
PiiType:IDCARD	Ficheros que contienen una o más entidades de tipo Documento de identidad (documento nacional de identidad, Cédula de identidad / ciudadanía, Registro civil etc.).
PiiType:SSN	Ficheros que contienen una o más entidades de tipo Número de la seguridad social.
PiiType:IP	Ficheros que contienen una o más entidades de tipo Dirección IP.

Tabla 14.6: Valores admitidos en los calificadores

Calificador	Descripción
PiiType:EMAIL	Ficheros que contienen una o más entidades de tipo Dirección de correo electrónico.
PiiType:PHONE	Ficheros que contienen una o más entidades de tipo Teléfono.
PiiType:ADDRESS	Ficheros que contienen una o más entidades de tipo Dirección.
PiiType:FULLNAME	Ficheros que contienen una o más entidades de tipo Nombre y apellidos.
PiiType:PASSPORT	Ficheros que contienen una o más entidades de tipo Número de pasaporte.
PiiType:DRIVERLIC	Ficheros que contienen una o más entidades de tipo Numero de licencia / permiso de conducción.
HasPii:True	Ficheros que contienen alguna entidad detectada.
Filename:"nombre del fichero"	Ficheros que tienen como nombre la cadena indicada.
Fileextension:"extensión del fichero"	Ficheros que tienen como extensión la cadena indicada.

Tabla 14.6: Valores admitidos en los calificadores

Sintaxis de las búsquedas con entidades

Las entidades se pueden utilizar en todos los tipos de búsqueda (rápida o guiada) de forma individual o combinadas con otras cadenas de caracteres.

- **PiiType:IDCARD**: busca todos los ficheros con alguna entidad detectada de tipo Documento de identidad.
- **+PiiType:IDCARD +“Empresa”**: busca el fichero que contiene el listado de documentos de identidad (con alguna detección de entidad IDCARD) de la empresa (que contenga la cadena de caracteres “Empresa”).
- **+Filename:analisis* +fileextension:docx -PiiType:fullname**: busca todos los ficheros de análisis (su nombre empieza por la palabra “análisis”) en formato Word (extensión docx) y no están firmados (no se detectó ninguna entidad de tipo Fullname – Nombre y apellidos).

Consejos para construir búsquedas compatibles con la normalización

- Utiliza preferiblemente letras en minúsculas.
- Ten en cuenta la configuración establecida sobre el contenido de los ficheros a indexar y los ficheros excluidos, ya que de ello dependerá el número de resultados mostrados en las búsquedas.
- Para buscar **números de cuentas bancarias, números de tarjetas de crédito, números de identidad, números de la seguridad social, números de pasaporte, números de permiso** elimina los caracteres de separación de la búsqueda.
- Para buscar **direcciones IP y direcciones de correo electrónico** introdúcelas tal cual.
- Para buscar **números de teléfono** elimina los caracteres de separación, introduciendo el código del

país si es necesario, sin el signo "+".

- Para buscar **direcciones físicas** elimina los caracteres numéricos.

Búsqueda de ficheros duplicados

Con el objetivo de ayudar a centralizar la información sensible en un único punto, y por tanto minimizar la exposición de este tipo de datos, Panda Data Control incluye la funcionalidad de búsqueda de ficheros duplicados y posterior borrado.

Definición de fichero duplicado

Se considera a dos ficheros como duplicados cuando su contenido es idéntico, independientemente del proceso de normalización descrito en "[Proceso de normalización](#)" ni de la configuración establecida por el administrador en "[Indexar el siguiente contenido](#)". En la comparación no se consideran ni el nombre ni la extensión de los ficheros.

Búsqueda de ficheros duplicados

Para buscar un fichero duplicado sigue los pasos mostrados a continuación:

- Desde el panel lateral **Mis listados**:
 - En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
 - Elige el listado **Archivos con información personal**. Se mostrará el listado de ficheros PII encontrados en la red.
- Desde el widget **Archivos con información personal**:
 - En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos con información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Desde el widget **Archivos por tipo de información personal**:
 - En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos por tipo de información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
 - En el menú de contexto asociado al archivo que se quiere buscar, haz clic en la opción **Buscar copias de archivo**. Se abrirá un nuevo listado con todos los ficheros duplicados encontrados en la red.

Borrado y restauración de ficheros

Borrar ficheros de los equipos de la red

Panda Data Control permite borrar los ficheros indexados y mostrados en el inventario de los equipos de la red. El borrado de ficheros es una operación asíncrona que inicia el administrador de la red desde la consola, y se produce cuando el agente recibe una petición desde el servidor Panda Adaptive Defense 360 y se cumplen las siguientes condiciones:

- El fichero no está en uso.
- El contenido del fichero no ha cambiado con respecto al almacenado en inventario.
- El fichero no ha sido borrado por el usuario en el periodo comprendido entre la generación del inventario y la acción de borrado por parte del administrador.
- El equipo está online. Si esta condición no se cumple, Panda Data Control marcará el fichero como **Pendiente de eliminar** hasta que el equipo se conecte al servidor Panda Adaptive Defense 360.

Estados de la acción de borrado

Al ser una operación asíncrona, el borrado de ficheros admite los estados mostrados a continuación:

- **Eliminado:** el fichero se ha movido a la zona de backup de Panda Adaptive Defense 360.
- **Pendiente de eliminar:** Panda Data Control está esperando a que el equipo se conecte al servidor Panda Adaptive Defense 360 para ejecutar la tarea de borrado.
- **Error:** el fichero no se ha podido borrar por un error.

Backup de ficheros borrados por Panda Data Control

Los ficheros borrados por Panda Data Control no se eliminan definitivamente del disco duro de los equipos. En su lugar se mueven a un área de backup donde residen durante 30 días, pasados los cuales el fichero es eliminado por completo.

Esta área es excluida automáticamente del inventario, de las búsquedas y de la monitorización de ficheros, y es inaccesible para el software instalado en el equipo de usuario.

Borrado de ficheros

Para borrar uno o varios ficheros sigue los pasos mostrados a continuación:

- Desde el panel lateral **Mis listados**:
 - En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
 - Elige el listado **Archivos con información personal**. Se mostrará el listado de ficheros PII encontrados en la red.
- Desde el widget **Archivos con información personal**:

- En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos con información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Desde el widget **Archivos por tipo de información personal**:
 - En el menú superior **Estado**, panel lateral **Data Control**, haz clic en una serie del widget **Archivos por tipo de información personal**. Se mostrará el listado **Archivos con información personal** con un criterio de filtrado establecido.
- Para borrar varios ficheros:
 - Haz clic en las casillas de selección asociadas a los ficheros que quieres borrar.
 - Haz clic en el icono  de la parte superior de la ventana. Se mostrará una ventana pidiendo confirmación.
- Para borrar un único fichero:
 - Utiliza el menú de contexto asociado al fichero que quieres eliminar y haz clic en la opción **Eliminar**. Se mostrará una ventana pidiendo confirmación.
- Si confirmas el borrado del fichero, éste se mostrará en el listado de ficheros en rojo y con el icono  indicando que está pendiente de borrado.

Visualizar ficheros borrados

Para visualizar los ficheros borrados por el administrador sigue los pasos mostrados a continuación:

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
- Elige el listado **Archivos eliminados por el administrador**. Se mostrará el listado de ficheros PII encontrados en la red que el administrador borró o restauró previamente.

Restaurar ficheros previamente borrados por el administrador

Panda Data Control permite restaurar a su ruta original los ficheros previamente borrados por el administrador desde la consola, en tanto en cuanto estos ficheros permanezcan en el área de backup (30 días desde su borrado). La restauración de ficheros es una operación asíncrona que inicia el administrador de la red desde la consola y se produce cuando el agente recibe una petición desde el servidor Panda Adaptive Defense 360 y se cumplen las siguientes condiciones:

- **El fichero permanece en la zona de backup:** los ficheros borrados permanecen en el área de backup durante 30 días, transcurridos los cuales se procede a eliminar el fichero definitivamente sin posibilidad de restauración.
- **No existe otro fichero en la ruta de restauración con el mismo nombre el fichero:** si existe otro fichero con el mismo nombre en la ruta de restauración Panda Data Control seguirá restaurando el fichero, pero lo hará en la carpeta `Lost&Found`.
- **La ruta de restauración existe:** si la ruta de restauración no existe, Panda Data Control seguirá restaurando el fichero, pero lo hará en la carpeta `Lost&Found`.

- **El equipo está online:** si el equipo está offline Panda Data Control marcará el fichero como **Pendiente de restaurar** hasta que se conecte al servidor Panda Adaptive Defense 360.

Estados de la acción de restaurar

Al ser una operación asíncrona, la restauración de ficheros admite los estados mostrados a continuación:

- Restaurado
- Pendiente de restaurar
- Error

Restaurar ficheros borrados

Para restaurar los ficheros borrados por el administrador sigue los pasos mostrados a continuación:

- **Acceso a la funcionalidad de restauración:**
 - En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana con todos los listados disponibles.
 - Elige el listado **Archivos eliminados por el administrador**. Se mostrará el listado de ficheros PII encontrados en la red que el administrador borró o restauró previamente.
-
- En el menú superior **Estado**, panel lateral **Data Control** haz clic en el widget **Archivos eliminados por el administrador**. Se abrirá el listado **Archivos eliminados por el administrador** sin filtros preconfigurados.
- **Para restaurar varios ficheros:**
 - Haz clic en las casillas de selección asociadas a los ficheros que quieres recuperar.
 - Haz clic en el icono  de la parte superior de la ventana. Se mostrará una ventana pidiendo confirmación.
 - Si confirmas la recuperación del fichero, éste pasará al estado **Restaurando**.
- **Para restaurar un único fichero:**
 - Utiliza el menú de contexto asociado al fichero que quieres recuperar.
 - Haz clic en la opción **Restaurar**. Se mostrará una ventana pidiendo confirmación.
 - Si confirmas la recuperación del fichero, éste pasará al estado **Restaurando**.

Configuración de Panda Data Control

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Data Control**.

- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Añadir configuración**.

Permisos requeridos

Permiso	Tipo de acceso
Configurar Data Control	Crear, modificar, borrar, copiar o asignar las configuraciones de Data Control.
Ver configuraciones de Data Control	Visualizar las configuraciones de Data Control.

Tabla 14.7: Permisos requeridos para acceder a la configuración Data Control

Requisitos para buscar y seguir documentos Microsoft Office

Para localizar los equipos que no tienen instalado alguno o ninguno de los componentes iFilter haz clic en el enlace **Comprobar ahora** de la pantalla de configuración. Se abrirá la zona **Equipos** con un listado filtrado por el criterio **Equipos sin Microsoft Filter Pack**.

Información personal (inventario, búsquedas y seguimiento)

- **Generar y mantener actualizado el inventario de información personal:** muestra los ficheros PII detectados en la red utilizando los widgets del dashboard y los listados. Consulta "[Paneles / widgets del módulo Panda Data Control](#)" y "[Listados del módulo Panda Data Control](#)". Para que los ficheros PII almacenados en un equipo concreto se muestren es necesario que el proceso de inventariado se haya completado para ese equipo.
- **Realizar el seguimiento de información personal en disco:** monitoriza las acciones de los procesos ejecutadas sobre ficheros PII almacenados en el equipo.
- **Realizar el seguimiento de información personal en correo:** monitoriza las acciones ejecutadas sobre la información personal almacenada en mensajes de correo electrónico.



El seguimiento de información personal en el correo electrónico es compatible cuentas Microsoft Exchange y clientes Microsoft Outlook 2013 y 2016.

- **Permitir realizar búsquedas de información en los equipos:** localiza ficheros por su nombre o contenido, siempre que hayan sido previamente indexados. Al hacer clic en este botón Panda Data Control comenzará el proceso de indexación de los ficheros almacenados en los equipos de los usuarios. Consulta "[Búsqueda de ficheros](#)".

Exclusiones

El administrador puede excluir del proceso de búsqueda a aquellos ficheros almacenados en los equipos de la red cuyo contenido no considere oportuno tener en cuenta.

- **Extensiones:** excluye a los ficheros con las extensiones indicadas.

- **Archivos:** excluye del proceso a los ficheros con el nombre indicado. Se pueden utilizar los caracteres comodín * y ?.
- **Carpetas:** excluye del proceso a todos los ficheros contenidos en las carpetas indicadas. Se pueden utilizar variables del sistema y los caracteres comodín * y ?.

Monitorización de archivos por reglas

Mediante reglas definidas por el administrador, Panda Data Control puede monitorizar archivos que no están clasificados como PII. El sistema almacena hasta diez reglas, que deben tener un nombre único.

- **Monitorizar archivos en disco**

Monitoriza las acciones que se producen sobre los archivos seleccionados en **Reglas de monitorización**.

- **Monitorizar archivos en correo**

Monitoriza las acciones que se ejecutan sobre los adjuntos en mensajes de correo, que cumplan las reglas indicadas en **Reglas de monitorización**.

Reglas de monitorización

Muestra la lista de extensiones predeterminadas sobre las que se aplica la monitorización. Se pueden añadir otras extensiones a la lista o eliminar las que ya están. Esta lista es común para todas las reglas que se han creado.



Cuando se asigna una propiedad de tipo "extensión del archivo" a una regla, la monitorización se producirá únicamente sobre los archivos que coincidan con la extensión, y no sobre el listado completo de extensiones.

Para crear una regla de monitorización haz clic en el icono +, se abrirá la ventana **Añadir reglas de monitorización** donde introducir los criterios de configuración de la regla.

- Introduce los campos de nombre y descripción.
- Completa los términos de la condición.

Propiedad	Operador	Valor
Nombre de archivo	Igual a / No es igual a	• Campo de texto con comodines * y ?.

Tabla 14.8: Campos para configurar una condición

Propiedad	Operador	Valor
Ruta del archivo	Igual / No es igual a	- Campo de texto con comodines * y ?. - Cuando se especifica una ruta del sistema de ficheros el separador es por defecto \.
Contenido del archivo	Igual a / No es igual a	Campo de texto con comodines * y ?.
Extensión del archivo	Igual a / No es igual a	- Campo de texto sin comodines. - Las extensiones de ficheros se deben poner sin punto delante.

Tabla 14.8: Campos para configurar una condición

- **Nueva condición:** añade más condiciones a la regla. Se aplicarán los operadores lógicos Y/O.
- **Operadores lógicos**

Para combinar dos condiciones o más en una misma regla se utilizan los operadores lógicos Y y O. Al añadir una segunda condición y sucesivas a una regla, se mostrará de forma automática un desplegable con los operadores lógicos disponibles, que se aplicarán a las condiciones adyacentes.

- **Agrupaciones de condiciones de regla**

Los paréntesis en una expresión lógica se utilizan para variar el orden de evaluación de los operadores que relacionan las condiciones de las reglas introducidas.

Para encerrar dos o más condiciones en un paréntesis crea una agrupación marcando con las casillas de selección las condiciones consecutivas que formarán parte del grupo y haz clic en el botón **Agrupar condiciones**. Se mostrará una línea delgada que abarcará las reglas de reglas de monitorización que forman parte de la agrupación.

Mediante el uso de paréntesis se definen agrupaciones de varios niveles para poder anidar grupos de operandos en una expresión lógica.

Opciones avanzadas de indexación

Para ver el estado de la indexación haz clic en el enlace **Ver estado de indexación de los equipos**. Se abrirá el "[Estado de Data Control](#)".

Indexar el siguiente contenido

Establece el tipo de contenido que se considerará a la hora de generar el inventario y que se devolverá como resultado de las búsquedas.



Los equipos que ya tengan un índice generado y reciban un cambio de configuración borrarán el índice y reiniciarán el proceso de indexado desde el principio.

Selecciona el tipo de indexación dependiendo de si únicamente quieres generar un inventario de ficheros PII o, por el contrario, también deseas lanzar búsquedas por contenido:

- **Indexar solo el texto:** se indexa solo el texto a no ser que forme parte de una entidad reconocida por Panda Data Control. Las búsquedas por contenido producidas con este tipo de índice serán más limitadas, por lo tanto, está recomendado si el administrador únicamente quiere generar el inventario de ficheros PII.
- **Indexar todo el contenido:** se indexan tanto los textos como los caracteres numéricos. Se recomienda cuando el administrador además de mantener el inventario de ficheros PII quiere realizar búsquedas precisas por contenido.



*Panda Data Control buscará sobre los contenidos del fichero según la configuración **Contenido del índice en los equipos** asignada. Si los equipos tienen configuraciones de indexación distintas, el resultado de las búsquedas pueden no ser homogéneo.*

Programar períodos de indexación

Configura la franja horaria en la que el proceso de indexación se iniciará en caso de ser necesario:

- **Siempre activado:** no se indica una franja horaria y el proceso de indexación se iniciará en el momento que sea necesario.
- **Activar sólo durante las siguientes horas:** indica mediante un calendario mensual los días y horas en los que el proceso de indexación podrá iniciarse.
- Utiliza los botones **Vaciar** y **Seleccionar todo** para limpiar el calendario o marcarlo por completo (equivalente a **Siempre activado**).

Escritura en unidades de almacenamiento extraíbles

Limita el acceso a la escritura de medios de almacenamiento externos USB.

- Permitir escritura sólo en unidades extraíbles cifradas: al activar esta opción, el usuario solo puede escribir en medios de almacenamiento externo USB que estén previamente cifrados con Panda Full

Encryption o BitLocker.



Las configuraciones de **Control de dispositivos** en **Estaciones y servidores** tienen precedencia sobre las configuraciones establecidas en **Data Control**. De esta manera, si **Control de dispositivos** está activado y no permite la lectura y escritura de la unidad USB, no será posible su escritura, independientemente de que esté o no cifrada. Consulta "[Control de dispositivos \(Equipos Windows\)](#)" en la página 255 para obtener más información acerca de esta configuración.

Paneles / widgets del módulo Panda Data Control

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **Data Control**.

Permisos requeridos

Permiso	Acceso a Widgets
Sin permisos	• Estado del despliegue • Equipos sin conexión • Estado de la actualización • Estado de la indexación • Características activadas en los equipos • Archivos eliminados por el administrador
Visualizar inventario de información personal	• Archivos con información personal • Archivos por tipo de información personal • Equipos con información personal
Buscar información en los equipos	• Búsquedas

Tabla 14.9: Permisos requeridos para el acceso a los widgets de Panda Data Control

Estado del despliegue

Muestra los equipos donde Panda Data Control está funcionando correctamente y aquellos que presentan algún tipo de error. El estado de los equipos se representa mediante un círculo con distintos

colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

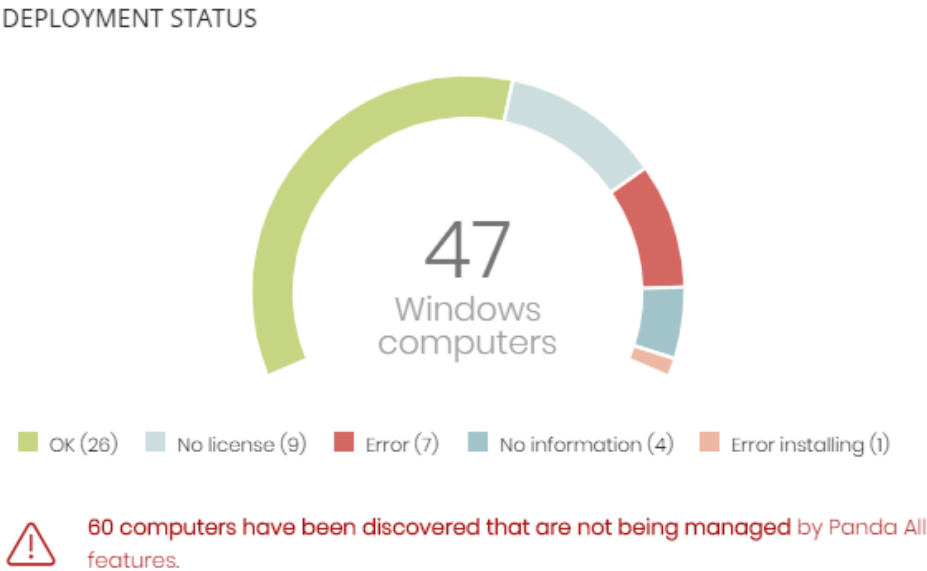


Figura 14.3: Panel Estado del despliegue

• Significado de las series

Serie	Descripción
Ok	Equipos con Panda Data Control instalado, licenciado y funcionando correctamente.
Error	Equipos con Panda Data Control instalado donde el módulo no responde a las peticiones enviadas desde los servidores de Panda Security.
Sin licencia	Equipos no gestionados por Panda Data Control debido a la falta de licencias suficientes, o a la no asignación de licencias disponibles.
Error instalando	Equipos cuya instalación no se pudo completar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con un agente sin actualizar.
Parte central	Suma de todos equipos compatibles con Panda Data Control.

Tabla 14.10: Descripción de la serie Estado del despliegue

• Filtros preestablecidos desde el panel

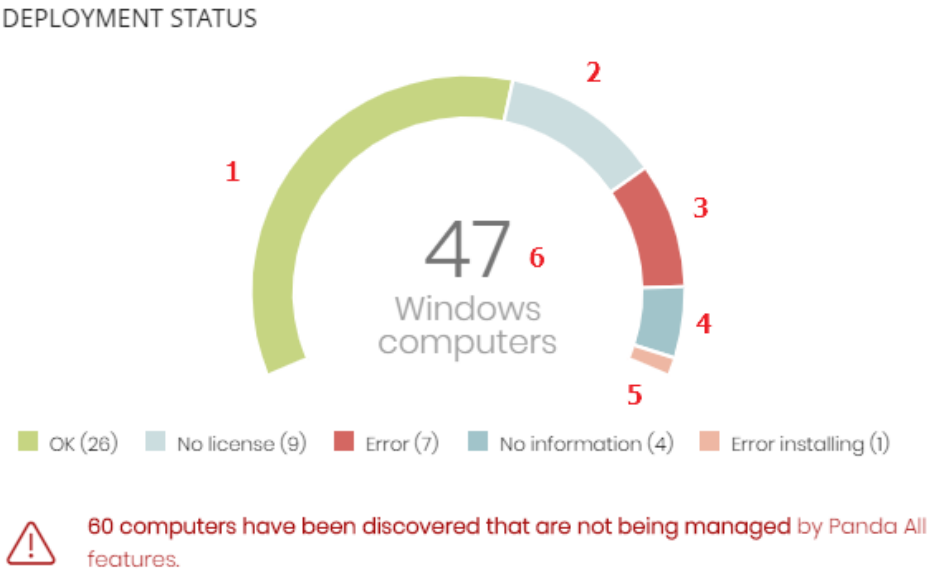


Figura 14.4: Zonas activas del panel Estado del despliegue

Al hacer clic en las zonas indicadas en la figura 14.4 se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de Data Control = Correcto.
(2)	Estado de Data Control = Sin licencia.
(3)	Estado de Data Control = Error.
(4)	Estado de Data Control = Sin información.
(5)	Estado de Data Control = Error instalando.
(6)	Sin filtros.

Tabla 14.11: Definición de filtros del listado Estado de Data Control

Equipos sin conexión

Muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.

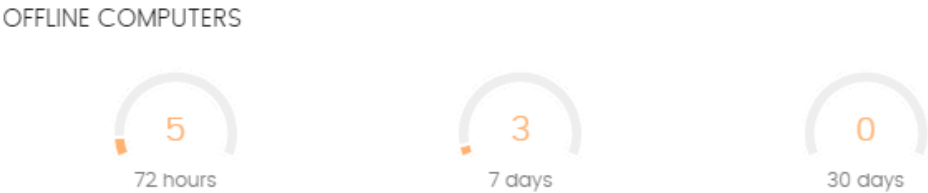


Figura 14.5: Panel Equipos sin conexión

• Significado de las series

Serie	Descripción
72 horas	Número de equipos que no enviaron su estado en las últimas 72 horas.
7 días	Número de equipos que no enviaron su estado en las últimas 7 días.
30 días	Número de equipos que no enviaron su estado en las últimas 30 días.

Tabla 14.12: Descripción de la serie Equipos sin conexión

• Filtros preestablecidos desde el panel

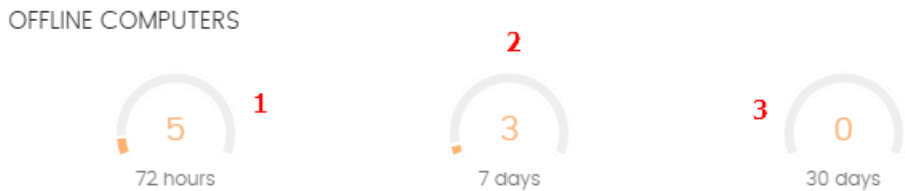


Figura 14.6: Zonas activas del panel Equipos sin conexión

Al hacer clic en las zonas indicadas en la figura 14.6 se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 72 horas.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 14.13: Definición de filtros del listado Estado de Data Control

Estado de la actualización

Muestra el estado de los equipos con respecto a la actualización del motor de Panda Data Control.

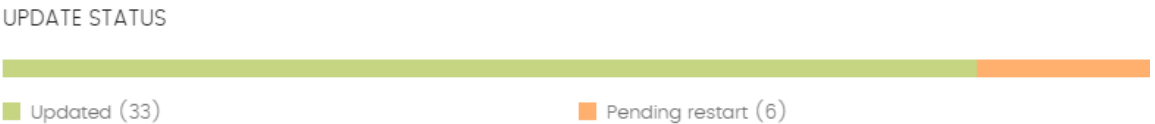


Figura 14.7: Panel Estado de la actualización

• Significado de las series

Serie	Descripción
Actualizados	Número de equipos con el motor Panda Data Control actualizado.
Desactualizados	Número de equipos con el motor Panda Data Control desactualizado.

Tabla 14.14: Descripción de la serie Estado de la actualización

Serie	Descripción
Pendientes de reinicio	Número de equipos que han descargado el motor Panda Data Control pero todavía no se han reiniciado, con lo que todavía no se ha actualizado.

Tabla 14.14: Descripción de la serie Estado de la actualización

• Filtros preestablecidos desde el panel

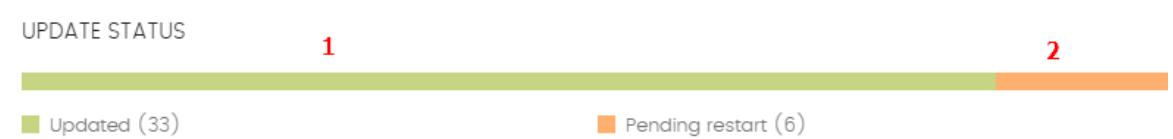


Figura 14.8: Zonas activas del panel Estado de la actualización

Al hacer clic en las zonas indicadas en la figura 14.8 se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = Si.
(2)	Protección actualizada = Pendiente de reinicio.
(3)	Protección actualizada = No.

Tabla 14.15: Definición de filtros del listado Estado de Data Control

Estado de la indexación

Muestra el estado de los equipos con respecto al estado de indexación de las unidades de almacenamiento conectadas.

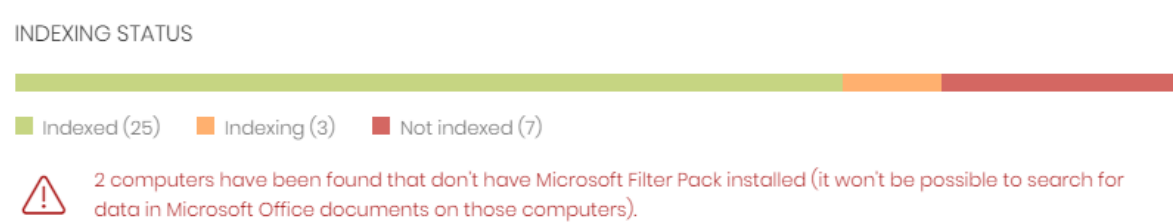


Figura 14.9: Panel Estado de la indexación

• Significado de las series

Serie	Descripción
Indexado	Número de equipos con los contenidos de las unidades de almacenamiento completamente indexados. Requiere que las búsquedas y/o el inventario estén activados. Consulta “ Configuración de Panda Data Control ”.
No indexado	Número de equipos con los contenidos de las unidades de almacenamiento sin indexar. Requiere que las búsquedas y/o el inventario estén activados. Consulta “ Configuración de Panda Data Control ”.

Tabla 14.16: Descripción de la serie Estado de la indexación

Serie	Descripción
Indexando	Número de equipos con contenidos en proceso de indexación. Requiere que las búsquedas y/o el inventario estén activados. Consulta "Configuración de Panda Data Control".

Tabla 14.16: Descripción de la serie Estado de la indexación

• Filtros preestablecidos desde el panel

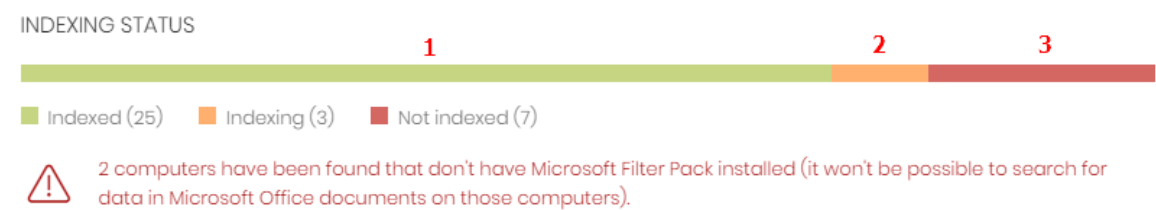


Figura 14.10: Zonas activas del panel Estado de la indexación

Al hacer clic en las zonas indicadas en la figura 14.10 se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de indexación = Indexado.
(2)	Estado de indexación = Indexando.
(3)	Estado de indexación = No indexado.

Tabla 14.17: Definición de filtros del listado Estado de Data Control

Características activadas en los equipos

Refleja el número total de equipos en la red que tienen instalado y correctamente licenciado Panda Data Control, y que han reportado el estado **Activado** para cada una de las tres funcionalidades.

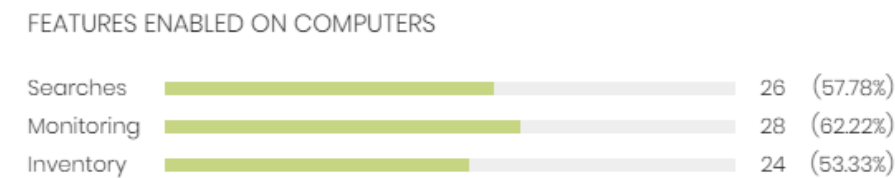


Figura 14.11: Panel Características activadas en los equipos

• Significado de las series

Serie	Descripción
Búsquedas	Muestra el número de equipos que reportan como activada la funcionalidad de búsqueda por contenido de ficheros PII.

Tabla 14.18: Descripción de la serie Características activadas en los equipos

Serie	Descripción
Seguimiento	Muestra el número de equipos que reportan como activada la funcionalidad de monitorización de ficheros PII.
Inventario	Muestra el número de equipos que reportan como activada la funcionalidad de inventario de ficheros PII.

Tabla 14.18: Descripción de la serie Características activadas en los equipos

• Filtros preestablecidos desde el panel

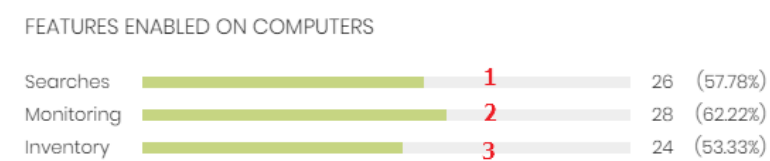


Figura 14.12: Zonas activas del panel Características activadas en los equipos

Al hacer clic en las zonas indicadas en la figura 14.12 se abre el listado **Estado de Data Control** con los filtros preestablecidos mostrados a continuación.

Zona activa	Filtro
(1)	Búsqueda de información en los equipos activada = Si.
(2)	Seguimiento de información personal activada = Si.
(3)	Inventario de información personal activado= Si.

Tabla 14.19: Definición de filtros del listado Estado de Data Control

Archivos eliminados por el administrador

Muestra los distintos estados por los que pasan los ficheros eliminados por el administrador.

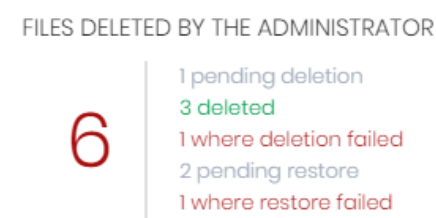


Figura 14.13: Panel Archivos eliminados por el administrador

• Significado de las series

Serie	Descripción
Pendientes de eliminar	Archivos marcados para borrar pero que todavía no se ha ejecutado la tarea.

Tabla 14.20: Descripción de la serie Archivos eliminados por el administrador

Serie	Descripción
Eliminados	Archivos borrados que permanecen en el área de backup de Panda Adaptive Defense 360.
Con error al eliminar	Archivos sobre los que no fue posible ejecutar la tarea de borrado.
Pendientes de restaurar	Archivos marcados para restaurar pero que todavía no se ha ejecutado la tarea.
Restaurados	Archivos que han sido movidos desde el área de backup a su ubicación original.

Tabla 14.20: Descripción de la serie Archivos eliminados por el administrador

• Filtros preestablecidos desde el panel

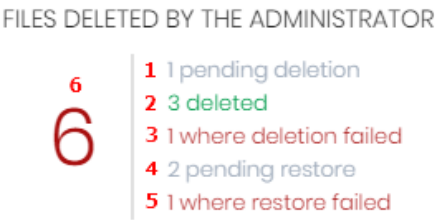


Figura 14.14: Zonas activas del panel Archivos eliminados por el administrador

Al hacer clic en las zonas indicadas en la figura 14.14 se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Archivos con información personal.	Pendiente de eliminar.
(2)	Archivos eliminados por el administrador.	Estado = Eliminado.
(3)	Archivos con información personal.	Error eliminando.
(4)	Archivos eliminados por el administrador.	Estado = Pendiente de restaurar.
(5)	Archivos eliminados por el administrador.	Estado = Error restaurando.
(6)	Archivos eliminados por el administrador.	Estado = todos.

Tabla 14.21: Definición de filtros del listado Archivos eliminados por el administrador

Archivos con información personal

Muestra el número de ficheros con información personal encontrados en la red y el total de ficheros encontrados en el último inventario diario generado.

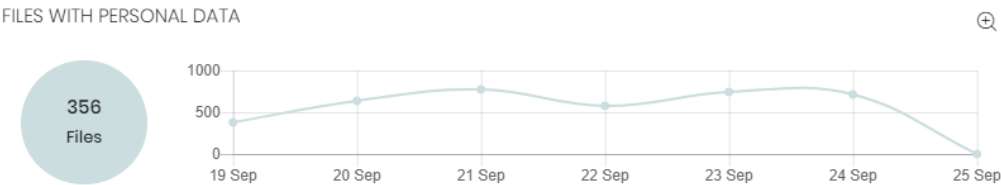


Figura 14.15: Panel Archivos con información personal

• Significado de las series

Serie	Descripción
Burbuja	Número total de ficheros PII encontrados según el último inventario enviado por cada equipo.
Linea	Número de ficheros PII encontrados en los inventarios diarios generados en las fechas indicadas en el eje de las Xs, y en todos los equipos de la red.

Tabla 14.22: Descripción de la serie Archivos con información personal

• Filtros preestablecidos desde el panel

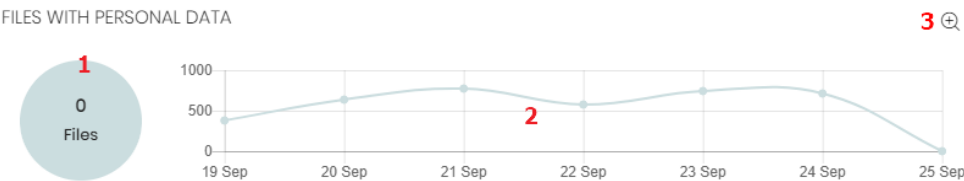


Figura 14.16: Zonas activas del panel Archivos con información personal

Al hacer clic en las zonas indicadas en la figura 14.16 se abre el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Fecha 1 = fecha elegida y Fecha 2 = fecha actual.
(3)	Se abre una nueva ventana con una ampliación del widget.

Tabla 14.23: Definición de filtros del listado Archivos con información personal

• Ampliación de la gráfica Archivos con información personal

Al hacer clic sobre el icono se abre una ventana con una ampliación del widget **Archivos con información personal** representando mediante una serie independiente el número de ficheros PII que contienen cada una de las entidades soportadas.

Para configurar el widget:

- Haz clic en la leyenda para activar o desactivar una serie.
- Haz clic en el enlace **Ocultar todos los datos** para mostrar el número de ficheros PII que contienen cualquier tipo de entidad.
- Haz clic en **Mostrar todos los datos** para mostrar el número de ficheros PII que contienen cada tipo de entidad por separado.

Equipos con información personal

Muestra el número de equipos de usuario y servidores que contienen ficheros con información personal en el último inventario diario generado.



Figura 14.17: Panel Archivos con información personal

• Significado de las series

Serie	Descripción
Burbuja	Número de equipos con ficheros PII encontrados según los últimos datos enviados por cada equipo.
Linea	Número total de equipos con ficheros PII encontrados en los inventarios diarios generados en las fechas indicadas en el eje de las Xs.

Tabla 14.24: Descripción de la serie Equipos con información personal

• Filtros preestablecidos desde el panel



Figura 14.18: Zonas activas del panel Archivos con información personal

Al hacer clic en las zonas indicadas en la figura 14.18 se abre el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Fecha 1 = fecha elegida y Fecha 2 = fecha actual.

Tabla 14.25: Definición de filtros del listado Archivos con información personal

Archivos por tipo de información personal

Muestra el número de archivos PII encontrados por cada tipo de entidad soportada en el último inventario diario generado.

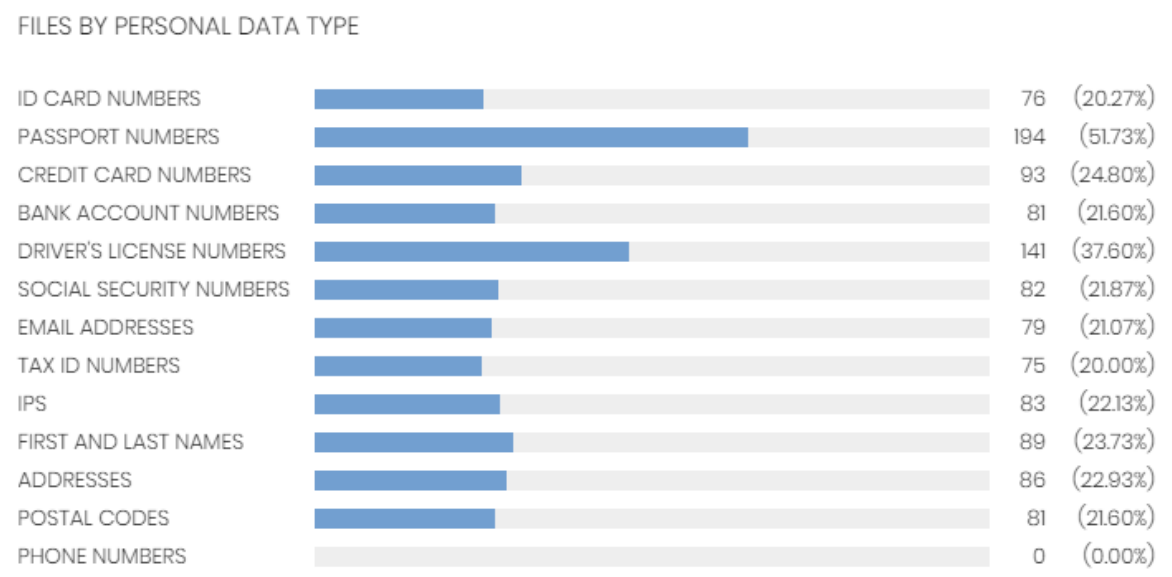


Figura 14.19: Panel Archivos por tipo de información personal

• Significado de las series

Serie	Descripción
Serie	Número total de ficheros PII encontrados en el último inventario diario generado por cada tipo de entidad soportada, y porcentaje de ficheros sobre el total de ficheros PII detectados.

Tabla 14.26: Descripción de la serie Archivos por tipo de información personal

• Filtros preestablecidos desde el panel

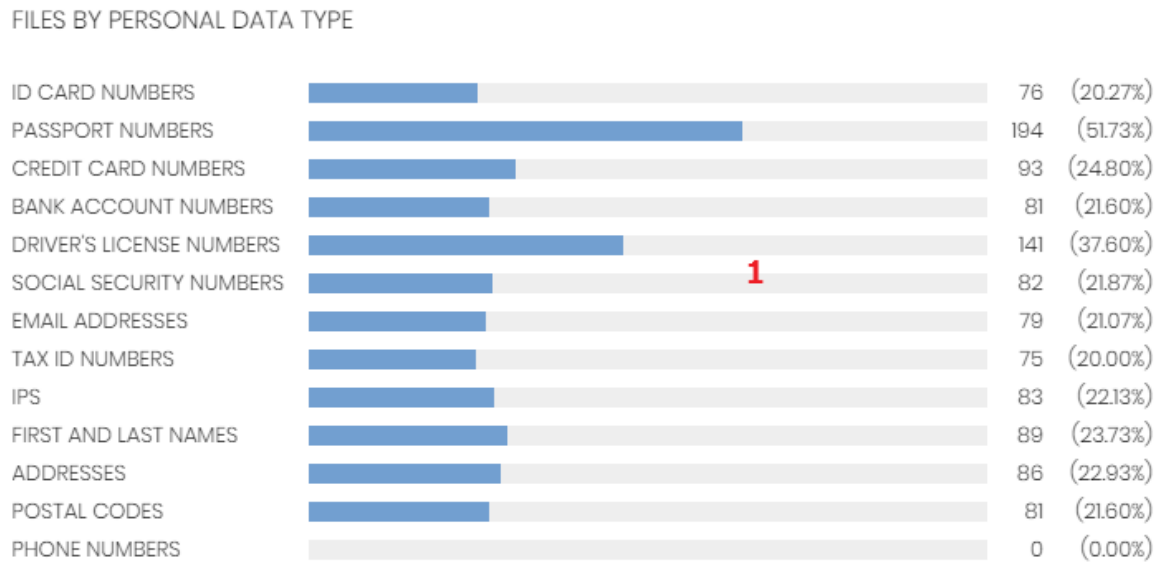


Figura 14.20: Zonas activas del panel Archivos por tipo de información personal

Haz clic en el widget para abrir el listado **Archivos con información personal** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Información personal = tipo de entidad seleccionada.

Tabla 14.27: Definición de filtros del listado Archivos con información personal

Listados del módulo Panda Data Control

Acceso a los listados

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Data Control** y en el widget relacionado.
- ó
- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Protección de datos** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

Permiso	Acceso a listados
Sin permisos	Estado de Data Control
Visualizar inventario de información personal	- Archivos con información personal - Equipos con información personal - Archivos eliminados por el administrador

Tabla 14.28: Permisos requeridos para acceder a los listados de Panda Data Control

Estado de Data Control

Muestra todos los equipos de la red e incorpora filtros relativos al estado del módulo Panda Data Control para localizar aquellos puestos de trabajo o dispositivos móviles que cumplen los criterios establecidos en el panel.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Seguimiento de información personal	Indica si Panda Data Control puede realizar un seguimiento de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	 Error instalando y Error  Desactivado  Activado  Sin licencia  Sin información
Inventario	Indica si Panda Data Control puede generar un inventario de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	 Error instalando y Error  Desactivado  Activado  Sin licencia  Sin información
Búsquedas	Indica si Panda Data Control puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	 Error instalando y Error  Desactivado  Instalando  Activado  Sin licencia  Sin información

Tabla 14.29: Campos del listado Estado de Data Control

Campo	Comentario	Valores
Actualizado	Indica si el módulo de Panda Data Control instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se indica la versión de la protección instalada.	•  Actualizado •  Pendiente de reinicio •  No actualizado
Microsoft Filter Pack	Indica si todos los componentes necesarios del paquete Microsoft Filter Pack están instalados o no en el equipo.	•  Instalado •  No instalado •  Información no disponible
Estado de indexación	Indica el estado del proceso de indexación de ficheros.	•  Indexando •  Indexado (Solo texto o Todo el contenido) •  No indexado •  No disponible
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha

Tabla 14.29: Campos del listado Estado de Data Control



Para visualizar los datos del listado gráficamente accede a uno de los siguientes widgets: “Estado del despliegue”, “Equipos sin conexión”, “Estado de la actualización”, “Características activadas en los equipos”, o “Estado de la indexación”.

• **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 14.30: Campos del fichero exportado Estado de Data Control

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el Software Panda Adaptive Defense 360 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
Fecha de la última actualización	Fecha de la última actualización del agente.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • Android
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	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
Seguimiento de información personal	Indica si Panda Data Control puede realizar un seguimiento de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información
Inventario de información	Indica si Panda Data Control puede generar un inventario de los ficheros con información personal en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	• Error instalando • Error • Desactivado • Correcto • Sin licencia • Sin información

Tabla 14.30: Campos del fichero exportado Estado de Data Control

Campo	Comentario	Valores
Búsquedas	Indica si Panda Data Control puede buscar ficheros en los dispositivos de almacenamiento del equipo, y si no es posible, indica la causa.	- Error instalando - Error - Desactivado - Correcto - Sin licencia - Sin información
Microsoft Filter Pack	Indica si todos los componentes necesarios del paquete Microsoft Filter Pack están instalados o no en el equipo.	- Instalado - No instalado - No disponible
Estado de indexación	Indica el estado del proceso de indexación de ficheros.	- Indexando - Indexado - No indexado - No disponible
Tipo de indexación	Muestra el tipo de indexación configurado en el equipo.	- Solo el texto - Todo el contenido
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	- Aislado - No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Panda Data Control y se produjo el error.	Fecha
Error instalación	Motivo del error de instalación.	Cadena de caracteres

Tabla 14.30: Campos del fichero exportado Estado de Data Control

• **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	- Estación - Portátil - Dispositivo móvil - Servidor
Buscar equipo	Filtra los equipos según su nombre.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Data Control a la nube de Panda Security.	- Todos - Hace menos de 24 horas - Hace menos de 3 días - Hace menos de 7 días

Tabla 14.31: Campos de filtrado para el listado Estado de Data Control

Campo	Comentario	Valores
		- Hace menos de 30 días - Hace más de 3 días - Hace más de 7 días - Hace más de 30 días
Protección actualizada	Filtra los equipos según la versión de la protección instalada.	- Todos - Si - No - Pendiente de reinicio
Estado de indexación	Filtra los equipos según el estado del proceso de indexación de ficheros.	- Todos - Indexando - Indexado - No indexado - No disponible
Tipo de indexación	Muestra los equipos que tienen configurado un tipo concreto de indexación.	- Todos - Solo el texto - Todo el contenido
Microsoft Filter Pack	Filtra los equipos si tienen o no instalados todos los componentes necesarios del paquete Microsoft Filter Pack.	- Todos - Falso - Verdadero
Estado de Data Control	Filtra los equipos según el estado del módulo Panda Data Control.	- Instalando... - Sin información - Correcto - Seguimiento de información personal desactivado - Búsqueda de información en el equipo desactivado - Error - Error Instalando - Sin licencia - Seguimiento de información personal activada

Tabla 14.31: Campos de filtrado para el listado Estado de Data Control

Campo	Comentario	Valores
		• Búsqueda de información en los equipos activada • Inventario de información personal activado • Inventario de información personal desactivado

Tabla 14.31: Campos de filtrado para el listado Estado de Data Control

Archivos con información personal

Muestra todos los ficheros PII encontrados, así como su tipo, localización y otra información relevante.

Dado que Panda Data Control solo retiene el último inventario completo de cada equipo, aquellos que estuvieran apagados en el momento de su generación solo mostrarán información en el listado

Archivos con información personal si el campo **Última vez visto** abarca la fecha en la que se generó el inventario de esos equipos.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Cadena de caracteres
Ruta	Ruta completa de la carpeta donde se almacena el fichero dentro del equipo.	Cadena de caracteres
Información personal	Tipo de información personal contenida en el fichero.	•  Entidad documento de identidad •  Entidad Pasaporte •  Entidad Tarjeta de crédito •  Entidad Cuenta bancaria •  Entidad Número de la seguridad social •  Entidad Permiso de conducir •  Entidad Dirección de correo electrónico

Tabla 14.32: Campos del listado Archivos con información personal

Campo	Comentario	Valores
		- Entidad Dirección IP - Entidad Nombre y Apellido - Entidad Direcciones - Entidad Teléfono móvil
Última vez visto	Fecha en la que se tomó la última fotografía del sistema de ficheros del equipo.	Fecha

Tabla 14.32: Campos del listado Archivos con información personal



Para visualizar los datos del listado gráficamente accede al widget “Archivos por tipo de información personal”.

• Campos mostrados en fichero exportado

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Cadena de caracteres
Ruta	Ruta completa de la carpeta donde se almacena el fichero dentro del equipo.	Cadena de caracteres
DNIs	Entidad Documento de identidad.	Booleano
Pasaportes	Entidad Número de pasaporte.	Booleano
Tarjetas de crédito	Entidad Número de tarjeta de crédito.	Booleano
Cuentas bancarias	Entidad Numero de cuenta bancaria.	Booleano
Permisos de conducir	Entidad Permiso de conducir.	Booleano
Números de la Seguridad Social	Entidad Número de la seguridad social.	Booleano
Direcciones de correo electrónico	Entidad Dirección de correo electrónico.	Booleano
IPs	Entidad Dirección IP.	Booleano
Nombres y apellidos	Entidad Nombre y apellidos.	Booleano
Direcciones	Entidad Dirección física.	Booleano
Números de teléfono	Entidad Número de teléfono.	Booleano

Tabla 14.33: Campos del fichero exportado Archivos con información personal

Campo	Comentario	Valores
Última vez visto	Fecha en la que el fichero fue incluido por última vez en el inventario diario.	Fecha
Estado	Estado del fichero.	• Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando
Error	• El fichero está en uso. • El contenido del fichero ha cambiado con respecto al almacenado en el inventario. • El fichero ha sido borrado por el usuario desde que se generó el inventario y la acción de borrado por parte del administrador. • Error al intentar eliminar el fichero.	Cadena de caracteres

Tabla 14.33: Campos del fichero exportado Archivos con información personal

• **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor
Última vez visto	Muestra el inventario de los equipos que fueron vistos por última vez dentro del rango de fechas especificado.	• Todos • Últimas 24 horas • Últimos 7 días • Último mes • Último año
Información personal	Especifica el tipo de entidad que se buscará en el fichero PII.	• DNIs • Tarjetas de crédito • Permisos de conducir • Direcciones de correo electrónico • IPs • Direcciones

Tabla 14.34: Campos de filtrado para el listado Archivos con información personal

Campo	Comentario	Valores
		- Números de teléfonos - Pasaportes - Cuentas bancarias - Números de la seguridad social - NIFs - Nombres y apellidos

Tabla 14.34: Campos de filtrado para el listado Archivos con información personal

Equipos con información personal

Muestra el número de ficheros PII encontrados en cada uno de los equipos de la red. Dependiendo de la configuración de los filtros **Fecha 1** y **Fecha 2** el listado puede utilizarse para mostrar información de varios tipos:

- Si los campos **Fecha 1** y **Fecha 2** están establecidos, el listado muestra la variación en el número de ficheros PII encontrados en cada uno de los equipos de la red entre las dos fechas. Por lo tanto, el listado presenta una evolución en el número de ficheros PII encontrados en cada equipo de la red.
- Si los campos **Fecha 1** y **Fecha 2** están vacíos, el listado muestra los ficheros PII encontrados en cada equipo de la red, según haya sido el resultado del último inventario completo generado.
- Si el campo **Fecha 1** está establecido, el listado muestra los ficheros PII encontrados en cada equipo de la red, según haya sido el resultado del inventario completo creado en la fecha indicada.

Para ver el listado de ficheros PII encontrado en un equipo haz clic en el nombre del equipo. Se abrirá el listado **Archivos con información personal** filtrado por el nombre del equipo elegido.

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Archivos (fecha)	Nombre del archivo.	Cadena de caracteres
Variación	Muestra la diferencia en el número de ficheros PII encontrados entre las fechas establecidas en Fecha 1 y Fecha 2. Si el número es positivo se mostrará el icono ↑. Si el número es negativo se muestra el icono ↓.	Numérico

Tabla 14.35: Campos del listado Equipos con información personal



Para visualizar los datos del listado gráficamente accede al widget **“Equipos con información personal”**.

- **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Fecha 1	Fecha inicial utilizada en la evolución de ficheros PII.	Fecha
Fecha de inventario	Fecha en la que se generó el inventario completo del equipo.	Fecha
Archivos con información personal	Número de ficheros PII encontrados en la fecha indicada en Fecha 1.	Numérico
Pasaportes	Número de ficheros PII que contienen la entidad Pasaporte encontrada en la fecha indicada en Fecha 1.	Numérico
Tarjetas de crédito	Número de ficheros que contienen la entidad Tarjeta de crédito encontrada en la fecha indicada en Fecha 1.	Numérico
Cuentas bancarias	Número de ficheros que contienen la entidad Cuentas bancarias encontrada en la fecha indicada en Fecha 1.	Numérico
Permisos de conducir	Número de ficheros que contienen la entidad Permisos de conducir encontrada en la fecha indicada en Fecha 1.	Booleano
Números de la Seguridad Social	Número de ficheros que contienen la entidad Números de la Seguridad social encontrada en la fecha indicada en Fecha 1.	Numérico
Direcciones de correo electrónico	Número de ficheros que contienen la entidad Direcciones de correo electrónico encontrada en la fecha indicada en Fecha 1.	Numérico
NIFs	Número de ficheros que contienen la entidad NIF encontrada en la fecha indicada en Fecha 1.	Numérico
IPs	Número de ficheros que contienen la entidad IP encontrada en la fecha indicada en Fecha 1.	Numérico
Nombres y apellidos	Número de ficheros que contienen la entidad Nombre y apellidos encontrada en la fecha indicada en Fecha 1.	Numérico
Direcciones	Número de ficheros que contienen la entidad Dirección encontrada en la fecha indicada en Fecha 1.	Numérico

Tabla 14.36: Campos del fichero exportado Equipos con información personal

Campo	Comentario	Valores
Números de teléfono	Número de ficheros que contienen la entidad Número de teléfono encontrada en la fecha indicada en Fecha 1.	Numérico
Fecha 2	Fecha inicial utilizada en la evolución de ficheros PII.	Fecha
Fecha de inventario	Fecha en la que se generó el inventario completo del equipo.	Fecha
Archivos con información personal	Número de ficheros PII encontrados en la fecha indicada en Fecha 2.	Numérico
Pasaportes	Número de ficheros que contienen la entidad Pasaporte encontrada en la fecha indicada en Fecha 2.	Numérico
Tarjetas de crédito	Número de ficheros que contienen la entidad Tarjeta de crédito encontrada en la fecha indicada en Fecha 2.	Numérico
Cuentas bancarias	Número de ficheros que contienen la entidad Cuentas bancarias encontrada en la fecha indicada en Fecha 2.	Numérico
Permisos de conducir	Número de ficheros que contienen la entidad Permisos de conducir encontrada en la fecha indicada en Fecha 2.	Booleano
Números de la Seguridad Social	Número de ficheros que contienen la entidad Números de la Seguridad social encontrada en la fecha indicada en Fecha 2.	Numérico
Direcciones de correo electrónico	Número de ficheros que contienen la entidad Direcciones de correo electrónico encontrada en la fecha indicada en Fecha 2.	Numérico
NIFs	Número de ficheros que contienen la entidad NIF encontrada en la fecha indicada en Fecha 2.	Numérico
IPs	Número de ficheros que contienen la entidad IP encontrada en la fecha indicada en Fecha 2.	Numérico
Nombres y apellidos	Número de ficheros que contienen la entidad Nombre y apellidos encontrada en la fecha indicada en Fecha 2.	Numérico
Direcciones	Número de ficheros que contienen la entidad Dirección encontrada en la fecha indicada en Fecha 2.	Numérico
Números de teléfono	Número de ficheros que contienen la entidad Número de teléfono encontrada en la fecha indicada en Fecha 2.	Numérico

Tabla 14.36: Campos del fichero exportado Equipos con información personal

- **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar	Filtra el listado por el nombre del equipo.	Cadena de caracteres
Fecha 1	Primera fecha a comparar.	Fecha
Fecha 2	Segunda fecha comparar.	Fecha
Tipo de equipo	Filtra los equipos según su clase.	• Estación • Portátil • Servidor
Información personal	Especifica el tipo de entidad que se buscará en el fichero PII.	• DNIs • Tarjetas de crédito • Permisos de conducir • Direcciones de correo electrónico • IPs • Direcciones • Números de teléfonos • Pasaportes • Cuentas bancarias • Números de la seguridad social • NIFs • Nombres y apellidos
Variación	Muestra los equipos cuya variación en el número de ficheros es positiva o negativa.	• Positivo: el número de ficheros encontrados en Fecha 2 es superior a Fecha 1. • Negativo: el número de ficheros encontrados en Fecha 2 es inferior a Fecha 1. • Todos

Tabla 14.37: Campos de filtrado para el listado Equipos con información personal

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta ["Información de equipo"](#) en la página 189 para obtener más información.

Archivos eliminados por el administrador

Muestra el estado de los ficheros que han recibido en el pasado tareas de borrado o restauración y que todavía permanecen en los equipos de la red, de forma accesible o en la zona de backup.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.38: Campos del listado Archivos eliminados por el administrador



Para visualizar los datos del listado gráficamente accede al widget “[Archivos eliminados por el administrador](#)”

• Campos mostrados en fichero exportado (historial)

Incluye las acciones de borrado y restauración que el administrador ejecutó sobre los ficheros de la red.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal

Tabla 14.39: Campos del listado Archivos eliminados por el administrador

Campo	Comentario	Valores
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.39: Campos del listado Archivos eliminados por el administrador

• **Campos mostrados en fichero exportado (historial detallado)**

Incluye todas las acciones de borrado y restauración que el administrador ejecutó sobre los ficheros de la red a lo largo del tiempo.

Campo	Comentario	Valores
Fecha	Fecha en la que el fichero cambió de estado.	Fecha
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Archivo	Nombre del archivo.	Archivos con información personal
Ruta	Localización del archivo dentro del sistema de ficheros del equipo.	Cadena de caracteres
Efectuado por	Cuenta de la consola de administración que originó el cambio de estado del fichero.	Cadena de caracteres
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.40: Campos del listado Archivos eliminados por el administrador

• Herramienta de filtrado

Campo	Comentario	Valores
Estado	Estado del fichero.	• Todos • Eliminado • Pendiente de eliminar • Restaurado • Pendiente de restaurar • Error restaurando

Tabla 14.41: Campos de filtrado para el listado Archivos eliminados por el administrador

Extensiones de programas soportadas

Nombre de la suite	Producto	Extensiones
Office	Word	• DOC • DOT • DOCX • DOCM • RTF
	Excel	• XLS • XLSM • XLSX • XLSB • CSV
	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM • POTX • PPTM • PPTX • POTM
OpenOffice	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW
	Draw	• ODG • OTG • STD
	Math	• ODF • SXM
	Base	• ODB
	Impress	• OTP • ODP • STI • SXI

Tabla 14.42: Listado de extensiones de programas soportadas

Nombre de la suite	Producto	Extensiones
	Calc	• OTS • ODS • SXC
Texto plano		TXT
Navegadores web	• Internet Explorer • Chrome • Opera • Otros	• HTM • HTML • MHT • OTH
Cliente de correo	• Outlook • Outlook Express	EML
Otros	Adobe Acrobat Reader	PDF
	Extensible Markup Language	XML
	Contribute	STC
	ArcGIS Desktop	SXD

Tabla 14.42: Listado de extensiones de programas soportadas

Empaquetadores y algoritmos de compresión soportados

Nombre del compresor / empaquetador / algoritmo	Extensiones
7-ZIP	7Z
bzip2	BZ2
gzip	GZ
Bihex	HQX
LHARC	• LHA • LZH
Lempel-Ziv & Haruyasu	LZH
Lempel-Ziv-Oberhumer / lzop	LZO
Multi-Purpose Internet Mail	MME
Lotus Notes Traveler	NTS
Winrar	RAR
Tar	TAR
Tar & Gzip	TGZ
Uuencode	• UU • UUE
XXEncoding	• XX • XXE
PkZip / PKWare	ZIP

Tabla 14.43: Listado de extensiones de empaquetadores / compresores soportados

Entidades y países soportados

Panda Data Control soporta las entidades mostradas a continuación:

- Cuentas bancarias.
- Tarjetas de crédito.
- Número de identidad personal.
- Direcciones IP.
- Direcciones de correo electrónico.
- Números de teléfono.
- Números de carnet de conducir.

- Números de pasaporte.
- Números de la seguridad social.
- Nombres y apellidos.
- Direcciones físicas.

Países soportados

El formato de las distintas entidades reconocidas varía dependiendo del país. Panda Data Control soporta la detección de entidades de los países mostrados a continuación:

- Alemania
- Austria
- Bélgica
- Dinamarca
- España
- Finlandia
- Francia
- Hungría
- Irlanda
- Italia
- Noruega
- Países Bajos
- Portugal
- Reino Unido
- Suecia
- Suiza

Capítulo 15

Panda Patch Management (Actualización de programas vulnerables)

Panda Patch Management es un módulo integrado en la plataforma Aether que localiza los equipos de la red que contienen software con vulnerabilidades conocidas, y los actualiza de forma automática y centralizada. De esta forma minimiza la superficie de ataque, evitando que el malware aproveche fallos del software instalado en los equipos de los usuarios y servidores para infectarlos.

Panda Patch Management es compatible con sistemas operativos Windows y detecta aplicaciones de terceros pendientes de actualizar o en EoL (End of Life), así como los parches y actualizaciones publicados por Microsoft para todos sus productos (sistemas operativos, bases de datos, suites ofimáticas, etc.).



Los equipos Windows XP SP3 y Windows Server 2003 SP2 requieren un equipo con el rol de caché / repositorio instalado en el mismo segmento de red para poder reportar y e instalar los parches pendientes. Un equipo Windows XP SP3 o Windows Server 2003 SP2 con el rol de caché / repositorio asignado tampoco podrá descargar parches.

Panda Patch Management no es compatible con sistemas Windows ARM.



Para obtener información adicional sobre los distintos apartados del módulo Panda Patch Management consulta las referencias siguientes:

- “[Crear y gestionar configuraciones](#)” en la página [213](#): información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.
- “[Control y supervisión de la consola de administración](#)” en la página [67](#): gestión de cuentas de usuario y asignación de permisos.
- “[Gestión de listados](#)” en la página [56](#): información sobre como gestionar listados.

CONTENIDO DEL CAPÍTULO

Funcionalidades de Panda Patch Management	-327
Flujo general de trabajo	-327
Comprobar que Panda Patch Management funciona correctamente	328
Comprobar que los parches publicados están instalados	328
Aislar los equipos con vulnerabilidades conocidas sin parchear	329
Descargar e instalar los parches	329
Caso I: desde el listado Parches disponibles	331
Caso II: desde el árbol de equipos	331
Caso III: desde el listado Parches disponibles	331
Caso IV: desde el árbol de equipos	332
Caso V: desde el listado Parches disponibles	332
Caso VI: desde el menú superior Tareas	332
Descargar los parches de forma manual	334
Identifica los parches que requieren una descarga manual	334
Obtén la URL de descarga	334
Integra el parche descargado en el repositorio de parches	335
Habilita el parche descargado para su instalación	335
Deshabilita un parche para su instalación	335
Desinstalar los parches defectuosos	336
Requisitos para desinstalar un parche instalado	336
Desinstalar un parche ya instalado	336
Comprobar el resultado de las tareas de instalación / desinstalación de parches	337
Excluir parches en todos o en algunos equipos	337
Comprobar que los programas no han entrado en EoL	338
Comprobar el histórico de instalaciones de parches y actualizaciones	338
Comprobar el nivel de parcheo de los equipos con incidencias	338
Configuración del descubrimiento de parches sin aplicar	-339
Acceso a la configuración	339
Permisos requeridos	339
Configuración general	339
Frecuencia de la búsqueda	340
Criticidad de los parches	340
Paneles / widgets en Panda Patch Management	-340
Acceso al panel de control	340
Permisos requeridos	340
Estado de gestión de parches	340
Tiempo desde la última comprobación	342
Programas "End of life"	344
Últimas tareas de instalación de parches	345
Parches disponibles	346
Listados del módulo Panda Patch Management	-347
Acceso a los listados	347
Estado de gestión de parches	348
Parches disponibles	352
Programas "End of Life"	358
Historial de instalaciones	359
Parches excluidos	364
Resultados tarea de instalación / desinstalación de parches	368
Ver parches instalados / desinstalados	370

Funcionalidades de Panda Patch Management

Toda la funcionalidad de Panda Patch Management se concentra en los puntos de la consola de administración mostrados a continuación:

- **Configuración del descubrimiento de parches a aplicar:** a través del perfil de configuración **Gestión de parches**, accesible desde el panel lateral en el menú superior **Configuración**. Consulta "[Configuración del descubrimiento de parches sin aplicar](#)".
- **Configuración de las exclusiones de parches:** desde el listado **Parches disponibles**. Consulta "[Excluir parches en todos o en algunos equipos](#)".
- **Visibilidad del estado de actualización del parque IT:** mediante widgets en un panel de control independiente, accesible desde el menú superior **Estado**, panel lateral **Patch Management**. Consulta "[Estado de gestión de parches](#)".
- **Listados de parches pendientes de aplicar:** desde los listados **Estado de gestión de parches**, **Parches disponibles** y **Programas "End of Life"** accesibles desde el menú superior **Estado**, panel lateral **Mis listados**, **Añadir**. Consulta "[Listados del módulo Panda Patch Management](#)".
- **Histórico de parches instalados:** desde el listado **Historial de instalaciones**, accesible desde el menú superior **Estado**, panel lateral **Mis listados**, **Añadir**. Consulta "[Historial de instalaciones](#)".
- **Parcheo de equipos:** desde el menú superior **Tareas** y creando una tarea programada de tipo **Instalar parches**. También se pueden parchear los equipos desde los menús de contexto del árbol de grupos en el menú superior **Equipos**, de los listados y desde **Detalle de equipo**. Consulta "[Descargar e instalar los parches](#)".
- **Desinstalación de parches:** elige una de las opciones siguientes:
 - Desde el widget **Últimas tareas de instalación de parches**, haz clic en el link **Ver historial de instalaciones**. Consulta "[Últimas tareas de instalación de parches](#)".
 - Desde el menú superior **Estado** haz clic en el panel lateral **Mis listados** **Añadir** y selecciona el listado **Historial de instalaciones**. Consulta "[Historial de instalaciones](#)".
 - Desde en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en **Ver parches instalados**.
- Al hacer clic en el parche se muestra su información asociada y el botón **Desinstalar** si es compatible con su desinstalación. Consulta "[Desinstalar un parche ya instalado](#)".

Flujo general de trabajo

Panda Patch Management es una herramienta integral que gestiona el parcheo y actualización de los sistemas operativos y programas instalados en los equipos de la red. Para conseguir reducir de forma eficiente la superficie de ataque de los equipos, es necesario seguir los pasos mostrados a continuación:

- Comprobar que Panda Patch Management funciona correctamente en los equipos instalados.

- Comprobar que los parches publicados están instalados.
- Aislar los equipos con vulnerabilidades conocidas sin parchear.
- Instalar los parches seleccionados.
- Desinstalación (Rollback) de los parches que muestran un mal funcionamiento.
- Excluir parches en todos o en algunos equipos.
- Comprobar que los programas instalados en los equipos no han entrado en EoL.
- Comprobar puntualmente el histórico de instalaciones de parches y actualizaciones.
- Comprobar puntualmente el estado del parcheo de equipos con incidencias.

Comprobar que Panda Patch Management funciona correctamente

Sigue los pasos mostrados a continuación:

- Comprueba que los equipos de la red tienen una licencia asignada de Panda Patch Management y que el módulo está instalado y en funcionamiento. Utiliza el widget ["Estado de gestión de parches"](#).
- Comprueba que los equipos con una licencia de Panda Patch Management asignada se comunican con la nube de Panda Security. Utiliza el widget ["Tiempo desde la última comprobación"](#).
- Comprueba que los equipos donde se instalarán los parches tienen el servicio Windows Update en ejecución con las actualizaciones automáticas desactivadas.



Activa la configuración **Desactivar Windows Update en los equipos** en el perfil de configuración de Gestión de parches para que Panda Adaptive Defense 360 pueda gestionar correctamente el servicio. Consulta ["Configuración general"](#).

Comprobar que los parches publicados están instalados

Los parches y actualizaciones se publican de forma constante según los proveedores del software instalado en la red detectan vulnerabilidades y las corrigen. Estos parches tienen asociada una criticidad y un tipo.

- Para obtener una visión general de los parches pendientes de instalar según su tipo y criticidad utiliza el widget ["Criticidad de los parches"](#).
- Para ver los parches pendientes de instalación en un equipo o grupo de equipos:
 - En el árbol de equipos (menú superior **Equipos**, pestaña **Carpeta** en el panel lateral) haz clic en el menú de contexto de un grupo que contenga equipos Windows y selecciona **Visualizar parches disponibles**. Se mostrará el listado ["Parches disponibles"](#) filtrado por el grupo.

ó

- En el panel de equipos (menú superior **Equipos**, panel derecho) haz clic en el menú de contexto de un equipo y selecciona **Visualizar parches disponibles**. Se mostrará el listado ["Parches disponibles"](#) filtrado por el equipo.

- Para obtener una visión global detallada de los parches pendientes de instalar:
 - En el menú superior **Estado** haz clic en el panel lateral **Mis listados, Añadir** y selecciona el listado “**Parches disponibles**”.
 - Utiliza la herramienta de filtrado para acotar la búsqueda.
- Para buscar los equipos que no tienen instalado un parche concreto:
 - En el menú superior **Estado** haz clic en el panel lateral **Mis listados, Añadir** y selecciona el listado “**Parches disponibles**”.
 - Utiliza la herramienta de filtrado para acotar la búsqueda.
 - Haz clic en el menú de contexto del equipo – parche a buscar y selecciona el menú **Visualizar equipos** con el parche disponible para su instalación.

Aislar los equipos con vulnerabilidades conocidas sin parchear

Para aislar un equipo que todavía no ha recibido un parche ya publicado que corrige una vulnerabilidad conocida:

- En el menú superior **Estado** haz clic en el link **Añadir** del panel lateral y selecciona el listado “**Parches disponibles**”.
- Haz clic en el menú de contexto de un parche y elige en el menú desplegable la opción **Aislar equipo**.

Descargar e instalar los parches

Para instalar los parches y actualizaciones Panda Patch Management utiliza la infraestructura de tareas implementada en Panda Adaptive Defense 360.



*La instalación de parches publicados por Microsoft no se completará con éxito si el servicio Windows Update está parado en el equipo del usuario o servidor. Sin embargo, para no solapar la actividad de Panda Patch Management con la del servicio Windows Updates es recomendable que la configuración de éste se establezca de forma que no tenga actividad en el equipo. Consulta “**Configuración General**” en la página 240 para más información.*

Los parches y actualizaciones se instalan mediante tareas rápidas o programadas. Las tareas rápidas instalan el parche en tiempo real pero no reinician el equipo del usuario, aunque sea requisito para completar la instalación. Las tareas programadas permiten configurar los parámetros de la actualización de parches. Consulta “**Tareas**” en la página 539 para obtener información general sobre las Tareas en Panda Adaptive Defense 360.

- **Descarga de parches y ahorro de ancho de banda**

Antes de la instalación de un parche es necesaria su descarga desde los servidores del proveedor de software. Esta descarga se produce de forma transparente e independiente en cada equipo cuando se lanza la tarea de instalación. Para minimizar el ancho de banda consumido se puede aprovechar la infraestructura de nodos caché / repositorios instalada en la red del cliente.



No es posible descargar parches ni actualizaciones a través de un nodo con el rol proxy asignado. Consulta la sección “[Configuración de los roles del agente Panda](#)” en la página [224](#) para obtener más información sobre los roles de Panda Adaptive Defense 360.

Los nodos caché / repositorio almacenan los parches durante un periodo máximo de 30 días, transcurrido el cual se eliminarán. Si un equipo solicita a un nodo caché la descarga de un parche y éste no lo tiene en su repositorio, el equipo dará un tiempo al nodo caché para que lo descargue. Este tiempo depende del tamaño del parche a descargar. Si no es posible la descarga, el equipo la iniciará de forma directa.

Una vez aplicados los parches en los equipos, éstos se borrarán del medio de almacenamiento donde residen.

- **Secuencia de tareas de instalación**

Las tareas de instalación de parches pueden requerir la descarga de parches desde los servidores del proveedor si los nodos con el rol de caché / repositorio no los tienen previamente almacenados. En este escenario, las tareas inmediatas inician la descarga de los parches necesarios en el momento en que éstas se crean, de forma que puede darse un alto consumo de ancho de banda si afectan a muchos equipos, o el volumen de la descarga es alto.

Las tareas programadas de instalación de parches comienzan la descarga de parches en el momento en que se indica en su configuración, pero si varias tareas coinciden en el punto de inicio se introduce un retardo aleatorio de hasta un máximo de 2 minutos para evitar el solapamiento de descargas y minimizar hasta cierto punto el consumo de ancho de banda.

- **Interrupción de las tareas de instalación de parches**

Las tareas de instalación de parches pueden cancelarse si el proceso de instalación en el equipo no se ha iniciado todavía. Si la instalación ya ha comenzado no se podrá cancelar la tarea, ya que podría causar errores en los equipos.

- **Estrategias de instalación de parches**

La consola de administración es una herramienta muy flexible que permite instalar los parches de múltiples maneras. De forma general se siguen las estrategias siguientes:

- Para instalar uno o varios parches concretos utiliza el listado “[Parches disponibles](#)” y configura la herramienta de filtrado.

- Para instalar todos los parches de una criticidad concreta o asociados a un programa o fabricante, utiliza las tareas inmediatas o programadas.
- Para instalar parches en equipos concretos o en un grupo utiliza el Árbol de grupos.

A continuación, se indican las combinaciones posibles de parches y destinos, y se describen los pasos a ejecutar en cada una de ellas.

Destino / parche	Uno o varios parches específicos	Uno, varios o todos los tipos de parches
Uno o varios equipos	Caso I: desde el listado Parches disponibles	Caso II: desde el árbol de equipos
Un grupo	Caso III: desde el listado Parches disponibles	Caso IV: desde el árbol de equipos
Varios o todos los grupos	Caso V: desde el listado Parches disponibles	Caso VI: desde el menú superior Tareas

Tabla 15.1: Instalación de parches según el destino y el conjunto de parches instalado

Caso I: desde el listado Parches disponibles

Para instalar uno o más parches concretos en uno o varios equipos:

- En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado "**Parches disponibles**".
- Utiliza la herramienta de filtrado para acotar la búsqueda.
- Haz clic en las casillas de selección de los equipos – parches a instalar y selecciona **Instalar** en la barra de acciones para crear una tarea rápida o **Programar instalación** para crear una tarea programada.

Caso II: desde el árbol de equipos

Para instalar uno varios o todos los tipos de parches en uno o varios equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el grupo al que pertenecen los equipos. Si los equipos pertenecen a varios grupos haz clic en el grupo raíz Todos.
- Haz clic en las casillas de selección de los equipos que recibirán el grupo de parches.
- En la barra de acciones haz clic en **Programar la instalación de parches**.
- Configura la tarea, haz clic en el botón **Guardar** y publícala.

Caso III: desde el listado Parches disponibles

Para instalar un parche concreto en un grupo de equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el menú de contexto del grupo.

- Haz clic en el menú **Visualizar parches disponibles**. Se mostrará el listado "**Parches disponibles**" filtrado por el grupo.
- Utiliza el campo **Parche** de la herramienta de filtrado para listar únicamente el parche a instalar.
- Selecciona todos los equipos del listado con las casillas de selección.
- Haz clic en **Instalar** en la barra de acciones para crear una tarea rápida o **Programar instalación** para crear una tarea programada.

Para instalar varios parches concretos en un grupo de equipos repite el punto anterior tantas veces como parches se quieran instalar.

Caso IV: desde el árbol de equipos

Para instalar uno, varios o todos los tipos de parches en un grupo de equipos:

- En el menú superior **Equipos**, pestaña **Carpetas** del árbol de equipos (panel izquierdo) haz clic en el menú de contexto del grupo.
- Haz clic en el menú **Programar instalación de parches**. Se mostrará la ventana de la tarea.
- Configura la tarea con el tipo o tipos de parches que se instalarán en el grupo, haz clic en el botón **Guardar** y publícala.

Caso V: desde el listado Parches disponibles

Para instalar un parche concreto en varios grupos de equipos:

- En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona el listado "**Parches disponibles**".
- Utiliza la herramienta de filtrado para acotar la búsqueda del parche.
- Haz clic en la casilla del parche a instalar y selecciona **Programar instalación** para crear una tarea.
- Haz clic en el menú superior **Tareas** y edita la tarea creada en el punto anterior.
- En el campo **Destinatarios** añade los grupos que recibirán el parche en **Grupos de equipos** y elimina los **Equipos Adicionales**.
- Haz clic en **Atrás**, configura la tarea y haz clic en **Guardar**.
- Publica la tarea.

Para instalar varios parches concretos en varios grupos de equipos repite el apartado anterior tantas veces como parches tengas que instalar.

Caso VI: desde el menú superior Tareas

Para instalar uno, varios o todos los tipos de parches en varios o todos los grupos de equipos:

- En el menú superior haz clic en **Tareas**, haz clic en **Añadir tarea** y selecciona **Instalar parches**.
- Establece el campo **Destinatarios** para determinar los equipos y grupos que recibirán la tarea de instalación.

- Indica la programación horaria de la tarea. Consulta "[Programación horaria y repetición de la tarea](#)" en la página [541](#) para obtener más información.
- Indica el nivel de criticidad de los parches a instalar.
- Indica qué productos recibirán parches utilizando las casillas de selección en el árbol de productos. Dado que el árbol de productos es un recurso vivo que cambia a lo largo del tiempo, ten en cuenta las siguientes reglas al seleccionar los elementos del árbol:
 - Al seleccionar un nodo se marcarán todos sus nodos hijos y sus descendientes. Por ejemplo, al seleccionar Adobe se seleccionarán todos los nodos que quedan por debajo de este nodo.
 - Si seleccionas un nodo y posteriormente Panda Patch Management agrega de forma automática un nuevo nodo hijo en la rama seleccionada, este nodo también quedará seleccionado de forma automática. Por ejemplo, si seleccionas el nodo Adobe se seleccionarán todos sus nodos hijos, y si posteriormente dentro de Adobe Panda Patch Management agrega un nuevo nodo (un nuevo programa o familia de programas), éste quedará seleccionado de forma automática. Por el contrario, si se seleccionan manualmente algunos nodos hijo individuales de Adobe y Panda Patch Management añade un nuevo nodo hijo, éste no se seleccionará de forma automática.
 - Los programas a parchear se evalúan en el momento en que se ejecuta la tarea, no en el momento de su creación o configuración. Esto implica que si Panda Patch Management agrega una nueva entrada en el árbol después de que el administrador haya configurado una tarea de parcheo, y esta entrada es seleccionada de forma automática según la regla del punto anterior, se instalarán los parches asociados a ese nuevo programa en el momento en que se ejecute la tarea.
- Establece las opciones de reinicio en el caso de que sea un requisito reiniciar el puesto de trabajo o servidor para completar la instalación del parche:
 - **No reiniciar automáticamente:** al terminar la tarea de instalación de parches se le muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora** y **Recordar más tarde**. En caso de elegir ésta última, se volverá a mostrar a las 24 horas siguientes.
 - **Reiniciar automáticamente solo las estaciones de trabajo:** al terminar la tarea de instalación de parches se muestra al usuario del equipo una ventana con las opciones **Reiniciar ahora**, **Botón de minimizar** y **Cuenta atrás de 4 horas**. Cada 30 minutos se maximizará la pantalla como recordatorio de la proximidad del reinicio. Cuando falte menos de una hora para el reinicio el botón de minimizar se deshabilitará. Cuando la cuenta atrás se haya completado el equipo se reiniciará automáticamente.
 - **Reiniciar automáticamente solo los servidores:** el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica solo a equipos de tipo servidor.
 - **Reiniciar automáticamente tanto las estaciones de trabajo como los servidores:** el comportamiento es idéntico a la opción **Reiniciar automáticamente solo las estaciones de trabajo** pero aplica tanto a estaciones de trabajo como a servidores.
- Haz clic en **Guardar** y publica la tarea.

Descargar los parches de forma manual

En algunos casos Panda Patch Management no puede obtener una URL de descarga para iniciar la instalación del parche de forma automática. El motivo de este escenario es diverso: puede ser debido a que el parche es de pago, o porque no es un parche público y requiere un registro previo del usuario a la descarga, entre otras razones. Debido a los EULAs que protegen a muchos parches, éstos no pueden ser descargados por Panda Security para su redistribución, de forma que será el propio administrador el encargado de descargar de forma manual el parche y compartirlo en la red para que los equipos se actualicen.

Panda Patch Management implementa un mecanismo mediante el cual integra estas descargas manuales en la consola web para que el administrador pueda añadir los parches descargados manualmente.

Para añadir un parche de forma manual al repositorio es necesario disponer la URL de descarga del parche proporcionada por el proveedor del producto a actualizar. Una vez tengas la URL sigue los pasos mostrados a continuación:

- Identifica los parches que requieren una descarga manual.
- Obtén la URL de descarga del proveedor.
- Integra el parche descargado en el repositorio de parches.
- Habilita el parche descargado para su instalación.
- Opcional: deshabilita un parche ya habilitado para su instalación

Identifica los parches que requieren una descarga manual

- Desde el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una lista con todos los listados disponibles.
- Elige el listado **Parches disponibles** y configura los siguientes filtros:
 - **Instalación:** Requiere descarga manual.
 - **Mostrar parches no descargables:** Sí.
- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches reportados por Panda Patch Management como necesarios para actualizar los equipos de la red y que no son descargables de forma automática.

Obtén la URL de descarga

- Con el listado de parches no descargables que se indica en "[Identifica los parches que requieren una descarga manual](#)" haz clic en un parche concreto. Se mostrarán los detalles del parche.
- Haz clic en el campo **URL de descarga** para iniciar la descarga del parche y guarda el nombre del fichero que aparece en el campo **Nombre del archivo**.

Integra el parche descargado en el repositorio de parches

- Localiza en la red un equipo con Panda Adaptive Defense 360 instalado y el rol de caché asignado y copia el fichero descargado en la ruta siguiente:

c:\Programdata\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy.



Si la unidad de almacenamiento del equipo ha cambiado a otra diferente de la establecida por defecto en el proceso de instalación del software Panda Adaptive Defense 360, accede a la siguiente ruta:

x:\Panda Security\Panda Aether Agent\Repository\ManuallyDeploy

Siendo x la unidad donde reside el repositorio del equipo. Consulta “[Establecer la unidad de almacenamiento](#)” para mas información.

- Si la carpeta **ManuallyDeploy** no existe, créala con permisos de administrador para lectura y escritura.
- Si es necesario, renombra el parche recién copiado con el nombre obtenido en el campo **Nombre de archivo** indicado en “[Obtén la URL de descarga](#)”.

Habilita el parche descargado para su instalación

- Una vez copiado el parche en el repositorio vuelve al listado **Parches disponibles** y haz clic en el menú de contexto asociado al parche descargado manualmente.
- Elige la opción **Marcar como descargado manualmente**  del menú desplegable. A partir de este momento el parche pasará del estado previo **Requiere descarga manual** al estado **Pendiente (descargado manualmente)** para todos los equipos que requieran su instalación. Una vez en estado **Pendiente (descargado manualmente)** se habilitarán todas las opciones necesarias en el menú de contexto del parche para poder instalarse de la misma forma que un parche descargado automáticamente. Consulta “[Descargar e instalar los parches](#)”.



Panda Patch Management no comprueba que un parche en estado Pendiente (descargado manualmente) realmente exista en algún equipo con el rol de caché asignado. De igual manera, tampoco comprueba que todos los equipos de la red que deberían recibir el parche tienen asignado un equipo caché con el parche copiado en su repositorio. Es responsabilidad del administrador asegurarse de que los equipos caché que se utilizarán en la descarga de parches tienen en la carpeta ManuallyDeploy los parches necesarios descargables de forma manual.

Deshabilita un parche para su instalación

Para retirar del repositorio un parche previamente integrado sigue los pasos mostrados a continuación:

- En el listado **Parches disponibles** configura un filtro de las siguientes características:
 - **Instalación:** Pendiente (descargado manualmente).
 - **Mostrar parches no descargables:** Si.
- Haz clic en el botón **Filtrar**. El listado mostrará todos los parches descargados de forma manual y habilitados para su instalación.
- Haz clic en el menú de contexto asociado al parche habilitado para su instalación y elige la opción **Marcar como "Requiere descarga manual"** . A partir de este momento el parche dejará de pertenecer al repositorio de parche instalables y perderá las opciones de su menú de contexto.

Desinstalar los parches defectuosos

En alguna ocasión puede suceder que los parches publicados por los proveedores del software no funcionen correctamente. Aunque se recomienda seleccionar un reducido grupo de equipos de prueba previo al despliegue en toda la red, Panda Patch Management también soporta la desinstalación de parches (Rollback).

Requisitos para desinstalar un parche instalado

- El rol del administrador tiene el permiso **Instalar / desinstalar** parche habilitado. Consulta "[Instalar / desinstalar y excluir parches](#)" en la página 76 para obtener más información.
- La instalación del parche a desinstalar finalizó completamente.
- El parche se puede desinstalar. No todos los parches soportan esta funcionalidad.

Desinstalar un parche ya instalado

- Accede a la pantalla de desinstalación del parche:
 - En el menú superior **Estado** haz clic en el panel lateral **Mis listados Añadir** y selecciona "[Historial de instalaciones](#)".
 - Accede al listado de parches instalados en el menú superior **Tareas**, selecciona la tarea que instaló el parche a desinstalar y haz clic en el link **Ver parches instalados**, situado en la parte superior derecha de la ventana de la tarea.
 - Accede al widget "[Últimas tareas de instalación de parches](#)" en el menú superior **Estado**, menú lateral **Patch Management** y haz clic en el link **Historial de instalaciones**.
- Selecciona de la lista el parche a desinstalar.
- Si el parche se puede desinstalar, se mostrará el botón **Desinstalar el parche**. Haz clic en el botón para mostrar la ventana de selección de equipos:
 - Selecciona **Desinstalar en todos los equipos** para eliminar el parche de todos los equipos de la red.
 - Selecciona **Desinstalar solo en...** para eliminar el parche del equipo indicado.
- Panda Patch Management creará una tarea de ejecución inmediata que desinstalará el parche.

- Si el parche requiere el reinicio del equipo de usuario para completar su desinstalación, se esperará a que el usuario lo reinicie de forma manual.



Un parche desinstalado volverá a mostrarse en los listados de parches disponibles a no ser que haya sido excluido. Si has configurado una tarea programada de instalación de parches y el parche no ha sido excluido, éste se volverá a instalar en su próxima ejecución. Si el parche ha sido retirado por el proveedor, no se volverá a mostrar ni a instalar. Consulta "[Excluir parches en todos o en algunos equipos](#)".

Comprobar el resultado de las tareas de instalación / desinstalación de parches

Para consultar las tareas de instalación / desinstalación, haz clic en el menú superior **Tareas** se puede consultar aquellas que han instalado o desinstalado parches en los equipos. Ambas ofrecen la posibilidad de Ver resultados para ver en detalle sobre qué equipos se ha realizado cada una de las acciones y qué parches se han instalado/desinstalado. Consulta "[Resultados tarea de instalación / desinstalación de parches](#)" y "[Ver parches instalados / desinstalados](#)" para más información.

Excluir parches en todos o en algunos equipos

Para evitar la instalación de los parches que han tenido un mal funcionamiento o que cambian de forma importante las características del programa que los recibe, el administrador de la red puede excluirlos a discreción. Para ello sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Estado** y en el panel lateral **Añadir** en la zona **Mis listados**. Elige el listado **Parches disponibles**. Este listado muestra una línea por cada par equipo - parche disponible. Un parche disponible es aquel que no ha sido instalado en algún equipo de la red o que ha sido desinstalado.
- Para excluir un único parche haz clic en el menú de contexto asociado al parche  y elige la opción **Excluir** . Se mostrará una ventana emergente para seleccionar el tipo de exclusión.
 - **Excluir solo para el equipo X:** excluye el parche elegido en el equipo indicado en el listado.
 - **Excluir para todos los equipos:** el parche elegido se excluirá de todos los equipos de la red.
- Para excluir varios parches y/o un único parche de varios equipos selecciónalos con las casillas de selección, haz clic en la barra de acciones y elige la opción **Excluir** . Se mostrará una ventana emergente para seleccionar el tipo de exclusión:
 - **Excluir solo para los equipos seleccionados:** excluye los parches elegidos en los equipos indicados en el listado.

- **Excluir para todos los equipos:** los parches elegidos se excluirán de todos los equipos de la red.



Los parches excluidos hacen referencia a una versión concreta del parche, de forma que si se excluye un determinado parche y posteriormente el proveedor del software publica otro posterior, éste último no se excluirá automáticamente.

Comprobar que los programas no han entrado en EoL

Los programas que han entrado en EoL no reciben ningún tipo de actualización por parte de los proveedores de software, de forma que se recomienda sustituirlos por alternativas equivalentes o por versiones más avanzadas.

Para localizar los programas actualmente en EOL o que entrarán en EOL en breve:

- Haz clic en el menú superior **Estado**, panel lateral **Patch Management**:
- En el widget “**Programas “End of life”**” se muestra la información dividida en tres series:
 - **Actualmente en EOL:** programas instalados en la red que ya no reciben actualizaciones de sus respectivos proveedores.
 - **Actualmente o en 1 año en EOL:** programas instalados en la red que ya están en EOL o que entrarán en EOL en el plazo de un año.
 - **Con fecha EOL conocida:** programas instalados en la red que tienen fecha EOL conocida.

Para localizar todos los programas con información de EOL conocida:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir**.
- Selecciona el “**Programas “End of Life”**”.

El listado contiene una entrada por cada par equipo – programa en EoL.

Comprobar el histórico de instalaciones de parches y actualizaciones

Para determinar si un parche concreto está instalado en los equipos de la red:

- Haz clic en el menú superior **Estado**, panel lateral **Mis listados, Añadir**.
- Selecciona “**Historial de instalaciones**”.

El listado contiene una entrada por cada par equipo – parche instalado, junto con información sobre su nombre, versión, programa o sistema operativo al que afecta y criticidad / tipo del parche.

Comprobar el nivel de parcheo de los equipos con incidencias

Panda Patch Management relaciona los equipos que tienen incidencias detectadas con su nivel de parcheo, de forma que es posible determinar si un equipo infectado o con amenazas detectadas tiene o no aplicados todos los parches que se han publicado.

Para ver si un equipo con una incidencia detectada tiene parches pendientes de instalación:

- En el menú superior **Estado**, widgets **Amenazas detectadas por el antivirus**, **Actividad del malware**, **Actividad de PUPs**, **Actividad de Exploits** y **Programas actualmente bloqueados en clasificación** haz clic en una amenaza - equipo. Se mostrará la información de la amenaza detectada en el equipo.
- En la sección **Equipo afectado** haz clic en el botón **Visualizar parches disponibles**. Se mostrará el listado **Parches disponibles** filtrado por el equipo.
- Selecciona todos los parches disponibles para este equipo y haz clic en la barra de acciones **Instalar** para crear una tarea inmediata que parcheará el equipo.



Debido a que este proceso puede implicar descargas de parches desde los servidores del proveedor del software a parchear, y por lo tanto retrasar su aplicación en el tiempo, se recomienda aislar el equipo de la red si el equipo ha sido infectado y muestra tráfico de red en su ciclo de vida. De esta forma se minimiza el riesgo de propagación de la infección en la red del cliente mientras el proceso de parcheo se completa. Consulta "[Análisis forense](#)" en la página 481 para obtener más información acerca del ciclo de vida del malware y "[Aislar uno o varios equipos de la red de la organización](#)" en la página 535.

Configuración del descubrimiento de parches sin aplicar

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Gestión de parches**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Gestión de parches	Crear, modificar, borrar, copiar o asignar las configuraciones de Gestión de parches.
Ver configuraciones de parches	Visualizar las configuraciones de Gestión de parches.

Tabla 15.2: Permisos requeridos para acceder a la configuración Gestión de parches

Configuración general

- Haz clic en **Desactivar Windows Update en los equipos** para que Panda Patch Management gestione las actualizaciones de forma exclusiva y sin interferencias con la configuración local de Windows Update.
- Haz clic en el selector **Buscar parches automáticamente** para activar la búsqueda de parches. Si el selector no está activado los parches pendientes de instalación no se mostrarán en los listados, aunque las tareas de instalación de parches podrán aplicarlos de forma independiente.

Frecuencia de la búsqueda

Buscar parches con la siguiente frecuencia establece cada cuanto tiempo Panda Patch Management consulta los parches instalados en los equipos y los compara con las bases de datos de parches disponibles.

Críticidad de los parches

Establece la criticidad de los parches que Panda Patch Management busca en las bases de datos de parches disponibles.



La criticidad de cada parche está establecida por cada proveedor del software afectado por la vulnerabilidad. Este criterio de clasificación no es uniforme y se recomienda comprobar previamente la descripción del parche para aquellos que no estén clasificados como “críticos”, con el objetivo de evitar su instalación si no se padecen los síntomas descritos.

Paneles / widgets en Panda Patch Management

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior Estado, panel lateral **Panda Patch Management**.

Permisos requeridos

Permisos	Acceso al widget
Sin permisos	- Estado de gestión de parches - Tiempo desde la última comprobación
Instalar, desinstalar y excluir parches	- Programas “End Of Life” - Parches disponibles - Últimas tareas de instalación de parches
Visualizar parches disponibles	- Programas “End Of Life” - Parches disponibles - Últimas tareas de instalación de parches

Tabla 15.3: Permisos requeridos para los widgets de Gestión de parches

Estado de gestión de parches

Muestra los equipos donde Panda Patch Management está funcionando correctamente y aquellos con errores o problemas en la instalación o en la ejecución del módulo. El estado del módulo se

representa mediante un círculo con distintos colores y contadores asociados. El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

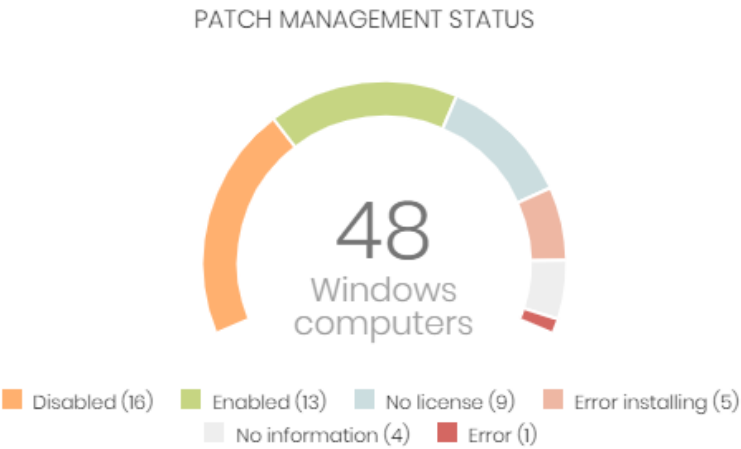


Figura 15.1: Panel de Estado de gestión de parches

• Significado de las series

Serie	Descripción
Activado	Indica el porcentaje de equipos en los que Panda Patch Management se instaló sin errores, su ejecución no presenta problemas y la configuración asignada permite buscar parches automáticamente.
Desactivado	Indica el porcentaje de equipos en los que Panda Patch Management se instaló sin errores, su ejecución no presenta problemas y la configuración asignada no permite buscar parches automáticamente.
Sin licencia	Equipos sin servicio de gestión de parches debido a que no se dispone de licencias suficientes, o no se les ha asignado una licencia disponible.
Error instalando	Indica los equipos donde el módulo no se pudo instalar.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con el agente sin actualizar.
Error	El módulo Panda Patch Management no responde a las peticiones del servidor y su configuración difiere de la establecida en la consola web.
Parte central	Refleja el número de total de equipos compatibles con el módulo Panda Patch Management.

Tabla 15.4: Descripción de la serie Estado de gestión de parches

• Filtros preestablecidos desde el panel

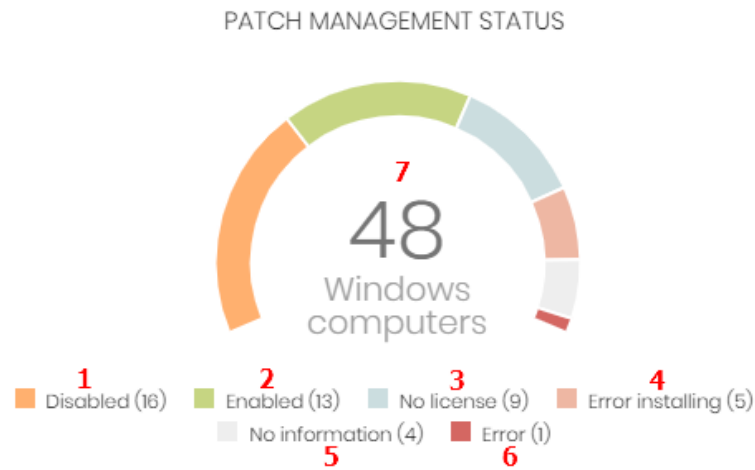


Figura 15.2: Zonas activas del panel Estado de gestión de parches

Al hacer clic en las zonas indicadas en la figura 15.2 se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de gestión de parches = Desactivado.
(2)	Estado de gestión de parches = Activado.
(3)	Estado de gestión de parches = Sin licencia.
(4)	Estado de gestión de parches = Error instalando.
(5)	Estado de gestión de parches = Sin información.
(6)	Estado de gestión de parches = Error.
(7)	Sin filtro.

Tabla 15.5: Definición de filtros del listado Estado de gestión de parches

Tiempo desde la última comprobación

Muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo para comprobar su estado de parcheo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.



Figura 15.3: Panel Tiempo desde la última comprobación

• Significado de las series

Serie	Descripción
72 horas	Número de equipos que no comprobaron su estado de parcheo en las últimas 72 horas.
7 días	Número de equipos que no comprobaron su estado de parcheo en las últimas 7 días.
30 días	Número de equipos que no comprobaron su estado de parcheo en los últimos 30 días.

Tabla 15.6: Descripción de la serie Tiempo desde la última comprobación

• Filtros preestablecidos desde el panel



Figura 15.4: Zonas activas del panel Tiempo desde la ultima comprobación

Al hacer clic en las zonas indicadas en la figura 15.4 se abre el listado **Estado de gestión de parches** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 3 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(2)	Última conexión = Hace más de 7 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.
(3)	Última conexión = Hace más de 30 días y Estado de gestión de parches = Activado o Desactivado o Sin información o Error.

Tabla 15.7: Definición de filtros del listado Estado de gestión de parches

Programas “End of life”

Muestra la información relativa al “end of life” de los programas instalados en los equipos de la red, agrupados según el plazo restante.

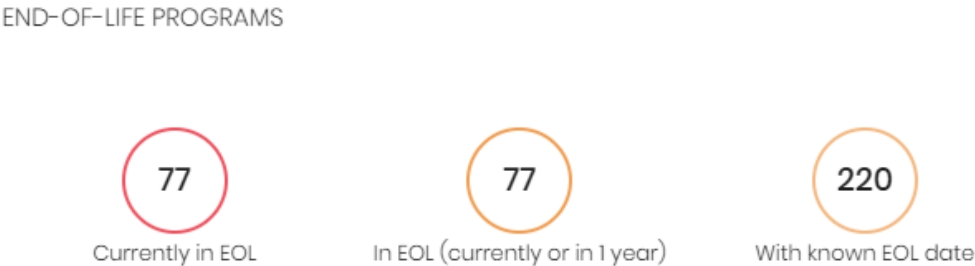


Figura 15.5: Panel Programas “End of life”

• Significado de las series

Serie	Descripción
Actualmente en EOL	Programas instalados en el parque informático que ya entraron en EOL.
Actualmente o en 1 año en EOL	Programas instalados en el parque informático que ya han entrado en EOL o entrarán dentro de un año.
Con fecha EOL conocida	Programas instalados en el parque informático cuya fecha de EOL es conocida.

Tabla 15.8: Descripción de la serie Programas “End of life”

• Filtros preestablecidos desde el panel



Figura 15.6: Zonas activas del panel Programas “End of life”

Al hacer clic en las zonas indicadas en la figura 15.6 se abre el listado **Programas “End Of Life”** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Fecha de inventario = Actualmente en “End Of Life”.

Tabla 15.9: Definición de filtros del listado Programas “End Of Life”

Zona activa	Filtro
(2)	Fecha de inventario = Actualmente o en 1 año en "End Of Life".
(3)	Fecha de inventario = Todos.

Tabla 15.9: Definición de filtros del listado Programas "End Of Life"

Últimas tareas de instalación de parches



Consulta "[Gestionar tareas](#)" en la página [544](#) para obtener más información sobre como modificar una tarea ya creada.

Muestra un listado de las últimas tareas de instalación de parches y actualizaciones creadas. Este widget está formado por varios enlaces que permiten gestionar las tareas de instalación de parches:

LAST PATCH INSTALLATION TASKS



- [Install .NET Framework 4.5.1 \(6.3\) patch on 6 computers](#) In progress
- [New task \(install patches\): Install patches with the following criticality](#) In progress

[View all](#) [View installation history](#)

Figura 15.7: Panel de Últimas tareas de instalación de parches

- Haz clic en una tarea para editar su configuración.
- Haz clic en el enlace **Ver todas** para acceder directamente al menú superior **Tareas** donde se muestran todas las tareas creadas.
- Haz clic en el enlace **Ver historial de instalaciones** para acceder al listado **Historial de instalaciones** con todas las tareas de instalación de parches terminadas con éxito o con error.
- Haz clic en el menú de contexto asociado a una tarea para mostrar una lista desplegable con las opciones siguientes:
 - **Cancelar:** interrumpe la tarea antes de iniciar el proceso de instalación de parches en el equipo.
 - **Ver resultados:** muestra los resultados de la tarea.

Parches disponibles

Muestra un recuento de parejas parche - equipo sin aplicar, distribuido por la categoría del parche. Cada parche no aplicado se contabiliza tantas veces como equipos no lo tengan instalado.

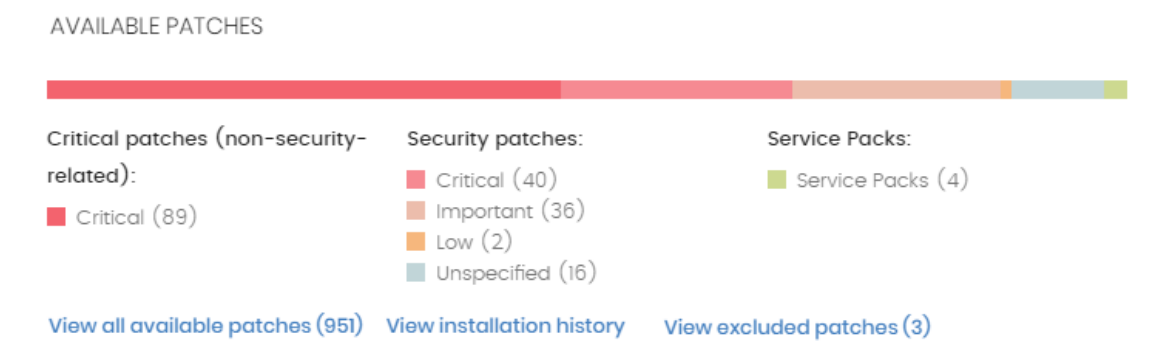


Figura 15.8: Panel Parches disponibles

• Significado de las series

Serie	Descripción
Parches de seguridad - Críticos	Número de parches clasificados como de importancia crítica relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos seguridad - Importantes	Número de parches clasificados de importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad - Baja	Número de parches clasificados como de importancia baja relativos a la seguridad del sistema y que no han sido aplicados todavía.
Parches críticos de seguridad – No clasificados	Número de parches sin determinar su importancia relativos a la seguridad del sistema y que no han sido aplicados todavía.
Otros parches (no de seguridad)	Número de parches no relativos a la seguridad del sistema y que no han sido aplicados todavía.
Service Packs	Número de paquetes de parches y actualizaciones que no han sido aplicados todavía.
Ver todos los parches disponibles	Número de parches de cualquier importancia relativos o no a la seguridad del sistema y que no han sido aplicados todavía.
Ver parches excluidos	Número de parches excluidos de su instalación.

Tabla 15.10: Descripción de la serie Parches disponibles

• Filtros preestablecidos desde el panel

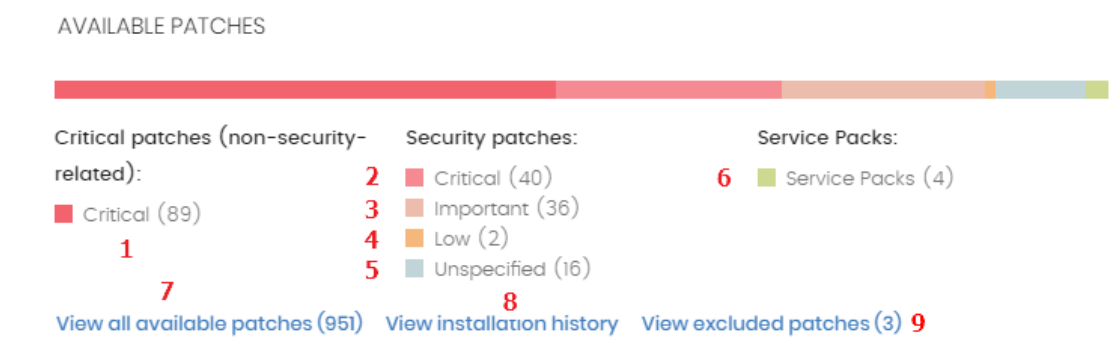


Figura 15.9: Zonas activas del panel Parches disponibles

Al hacer clic en las zonas indicadas en la figura 15.9 se abre un listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Parches disponibles	Criticidad = Critica (de seguridad).
(2)	Parches disponibles	Criticidad = Importante (de seguridad).
(3)	Parches disponibles	Criticidad = Baja (de seguridad).
(4)	Parches disponibles	Criticidad = No clasificado (de seguridad).
(5)	Parches disponibles	Criticidad = Otros parches (no de seguridad).
(6)	Parches disponibles	Criticidad = Service Pack.
(7)	Parches disponibles	Sin filtros.
(8)	Historial de instalaciones	Sin filtros.
(9)	Parches excluidos	Sin filtros.

Tabla 15.11: Definición de filtros del listado Parches disponibles

Listados del módulo Panda Patch Management

Acceso a los listados

El acceso a los listados se podrá hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Patch Management** y en el widget relacionado.

ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Gestión de parches** para ver su plantilla asociada. Modifícala y

haz clic en **Guardar**. El listado se añadirá al panel lateral.

Los listados de instalación o desinstalación de parches se pueden consultar desde el widget **Historial de instalaciones**, haciendo clic en **Ver historial de instalaciones**.

Los listados **Resultados tarea de instalación / desinstalación de parches** y **Ver parches instalados / desinstalados** se pueden consultar desde el menú superior **Tareas**, haciendo clic en **Ver resultados** en una tarea de instalación o desinstalación.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	Estado de gestión de parches
Instalar, desinstalar y excluir parches	Acceso a los listados y a los menús de contexto para instalar y desinstalar parches: - Parches disponibles - Historial de instalaciones - Programas "End Of Life" - Parches excluidos - Resultados tarea de instalación / desinstalación de parches - Ver parches instalados / desinstalados
Visualizar parches disponibles	Acceso de solo lectura a los listados: - Parches disponibles - Historial de instalaciones - Programas "End Of Life" - Parches Exclusivos - Resultados tarea de instalación / desinstalación de parches - Ver parches instalados / desinstalados

Tabla 15.12: Permisos requeridos para los listados de Gestión de parches

Estado de gestión de parches

Este listado muestra en detalle todos los equipos de la red compatibles con Panda Patch Management, incorporando filtros que permiten localizar aquellos puestos de trabajo y servidores que no estén recibiendo el servicio por alguno de los conceptos mostrados en el panel asociado.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres

Tabla 15.13: Campos del listado Estado de gestión de parches

Campo	Comentario	Valores
Gestión de parches	Estado del módulo.	•  Activado •  Desactivado •  Error instalando (motivo del error) •  Sin licencia •  Sin información •  Error
Última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha

Tabla 15.13: Campos del listado Estado de gestión de parches



Para visualizar los datos del listado gráficamente accede al widget “Estado de gestión de parches”.

• Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo con software desactualizado.	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 Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres

Tabla 15.14: Campos del fichero exportado Estado de gestión de parches

Campo	Comentario	Valores
Versión del agente		Cadena de caracteres
Fecha instalación	Fecha en la que el módulo Panda Patch Management se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha
Plataforma	Sistema operativo instalado en el equipo.	• Windows • Linux • macOS • 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
Protección actualizada	Indica si el módulo de la protección instalado en el equipo es la última versión publicada.	Booleano
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Estado de gestión de parches	Estado del módulo.	• Activado • Desactivado • Error instalando • Sin licencia • Sin información • Error
Requiere reinicio	El equipo no se ha reiniciado para completar la instalación de uno o más parches descargados.	Booleano
Fecha de la última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	Fecha
Estado de aislamiento	Indica si el equipo ha sido aislado de la red o se comunica con sus equipos vecinos de forma normal.	• Aislado • No aislado
Fecha error instalación	Fecha en la que se intentó la instalación del módulo Panda Patch Management y se produjo el error.	Fecha

Tabla 15.14: Campos del fichero exportado Estado de gestión de parches

Campo	Comentario	Valores
Error instalación	Motivo del error de instalación.	- Error en la descarga - Error en la ejecución

Tabla 15.14: Campos del fichero exportado Estado de gestión de parches

• **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor
Última comprobación	Fecha en la que Panda Patch Management consultó a la nube para comprobar si se han publicado nuevos parches.	- Todos - Hace más de 3 días - Hace más de 7 días - Hace más de 30 días
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha
Pendiente de reinicio para completar instalación de parches	El equipo no se ha reiniciado para completar la instalación de uno o más descargados.	Booleano
Estado de gestión de parches	Estado del módulo.	- Activado - Desactivado - Error instalando - Sin licencia - Sin información - Error

Tabla 15.15: Campos de filtrado para el listado Estado de gestión de parches

• **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta ["Información de equipo"](#) en la página 189 para obtener más información.

Parches disponibles

Muestra el detalle de los parches disponibles y la información sobre los parches que están en proceso de instalación. Cada línea del listado refleja un par parche – equipo de la red.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Criticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Instalación	Indica el estado de la instalación del parche: • Pendiente: el parche está disponible para el equipo y no ha completado su instalación. • Requiere descarga manual: el parche requiere que el administrador descargue de forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta "Descargar los parches de forma manual".	

Tabla 15.16: Campos del listado Parches disponibles

Campo	Comentario	Valores
	• Pendiente (descargado manualmente): el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta "Descargar los parches de forma manual". • Pendiente de reinicio: el parche ha sido instalado pero el equipo no ha sido reiniciado. Algunos parches pueden no aplicarse hasta realizar este proceso.	
Menú de contexto	Despliega un menú de acciones: • Instalar: crea una tarea inmediata de instalación del parche en el equipo elegido. • Programar instalación: crea una tarea configurable de instalación del parche elegido. • Aislar equipo: aísla el equipo de la red. • Visualizar parches disponibles del equipo: filtra el listado por el equipo elegido para mostrar todos los parches disponibles que aun no se han instalado. • Visualizar equipos con el parche disponible: muestra todos los equipos que tienen disponible el parche elegido para su aplicación.	

Tabla 15.16: Campos del listado Parches disponibles



Para visualizar los datos del listado gráficamente accede al widget "[Parches disponibles](#)".

• **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo con software desactualizado.	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
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres

Tabla 15.17: Campos del fichero exportado Parches disponibles

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Versión	Numero de versión del programa desactualizado.	Numérico
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Críticidad	Importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha
Es descargable	Indica si el parche está disponible para su descarga o requiere un contrato adicional con el proveedor del software para acceder a aquel.	Booleano
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico

Tabla 15.17: Campos del fichero exportado Parches disponibles

Campo	Comentario	Valores
Estado	Indica el estado de la instalación del parche: • Pendiente: el parche está disponible para el equipo y no ha completado su instalación. • Pendiente (descargado manualmente): el parche ya fue descargado de forma manual y forma parte del repositorio de parches. Consulta "Descargar los parches de forma manual". • Requiere descarga manual: el parche requiere que el administrador descargue de forma manual el parche y lo copie en un equipo con el rol de cache asignado. Consulta "Descargar los parches de forma manual".	Cadena de caracteres
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres
URL de descarga	Recurso HTTP en la infraestructura del proveedor del software para descargar el parche.	Cadena de caracteres

Tabla 15.17: Campos del fichero exportado Parches disponibles

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Críticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad)

Tabla 15.18: Campos de filtrado para el listado Parches disponibles

Campo	Comentario	Valores
		- Moderada (de seguridad) - Baja (de seguridad) - No clasificado (de seguridad) - Service Pack
Instalación	Muestra los parches que se encuentran en proceso de instalación filtrándolos por la etapa en la que se encuentran.	- Pendiente - Requiere descarga manual - Pendiente (descargado manualmente) - Pendiente de reinicio
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Panda Patch Management debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano

Tabla 15.18: Campos de filtrado para el listado Parches disponibles

• Ventana Parche detectado

Al hacer clic en una de las filas del listado se mostrará la ventana **Parche detectado**, en la que se mostrarán dos tipos de contenidos:

- Información sobre el parche disponible y el botón **Instalar parche**.
- Información sobre el parche en proceso de instalación. Se mostrará un texto de **Pendiente de reinicio** junto al botón de **Instalar parche**.

Al hacer clic en el botón **Instalar parche** se mostrará una ventana emergente para establecer los destinatarios de la tarea de instalación del parche:

- **El equipo actual:** la tarea tiene como destinatario el equipo seleccionado en el listado.
- **Instalar en todos los equipos del filtro seleccionado:** selecciona del desplegable un filtro del árbol de filtros para determinar los equipos que recibirán la tarea de instalación del parche.
- **Instalar en todos los equipos:** todos los equipos recibirán la tarea de instalación del parche seleccionado.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base, etc.).	Cadena de caracteres

Tabla 15.19: Campos de la ventana Parche detectado

Campo	Comentario	Valores
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Críticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Equipo	Nombre del equipo con software desactualizado.	• Cadena de caracteres
Estado de instalación	Indica si el parche ya forma parte del repositorio de parches aplicables a los equipos o si requiere la descarga e integración manual por parte del administrador en el repositorio de parches.	• Pendiente • Requiere descarga manual • Pendiente (descargado manualmente) • Pendiente de reinicio
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
URL de la descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Nombre del archivo	Nombre del archivo que contiene el parche.	Cadena de caracteres

Tabla 15.19: Campos de la ventana Parche detectado

Programas “End of Life”

Muestra los programas que ya no tienen soporte por parte de sus proveedores y que por tanto son un objetivo especialmente vulnerable para el malware y las amenazas.

Campo	Comentario	Valores
Equipo	Nombre del equipo con software en EoL.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha (en rojo si el equipo entró en EOL)

Tabla 15.20: Campos del listado Programas EoL



Para visualizar los datos del listado gráficamente accede al widget “Programas “End of life””.

• Campos mostrados en fichero exportado

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa en EoL.	Cadena de caracteres
Versión	Versión del programa en EoL.	Cadena de caracteres
EoL	Fecha en la que el programa entró en EoL.	Fecha
Última vez visto	Fecha en la que el equipo fue descubierto por última vez.	Fecha

Tabla 15.21: Campos del fichero exportado Programas EoL

- **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fecha inventario	Fecha en la que el programa entrará en EOL.	• Todos • Actualmente en "End of life" • Actualmente o en "End of life" en 1 año

Tabla 15.22: Campos de filtrado para el listado Programas Eol

- **Ventana Detalles del programa**

Al hacer clic en uno de los programas del listado se accede a la ventana de **Detalles del programa**:

Campo	Comentario	Valores
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Familia	Bundle, suit o grupo de programas al que pertenece el software.	Cadena de caracteres
Editor/Empresa	Empresa que diseñó o publicó el programa.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
EOL	Fecha en la que el programa entró en EoL.	Fecha

Tabla 15.23: Campos de la ventana Detalles del programa

Historial de instalaciones

Muestra los parches que Panda Patch Management intentó instalar y los equipos que los recibieron en un intervalo determinado.

Campo	Comentario	Valores
Fecha	Fecha en la que se instaló el parche o actualización.	Fecha
Equipo	Nombre del equipo que recibió el parche o actualización.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Versión	Versión del programa o sistema operativo que recibió el parche.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres

Tabla 15.24: Campos del listado Historial de instalaciones

Campo	Comentario	Valores
Críticidad	Importancia del parche instalado.	- Otros parches - Crítica - Importante - Moderada - Baja - No clasificado - Service Pack
Instalación	Estado de la instalación del parche o actualización.	- Instalado - Requiere reinicio - Error - Desinstalado - El parche ya no es requerido
Menú de contexto ⋮	Muestra un desplegable con opciones.	Ver tarea: muestra la configuración de la tarea asociada a la instalación o desinstalación del parche seleccionado.

Tabla 15.24: Campos del listado Historial de instalaciones



Para visualizar los datos del listado gráficamente accede al widget “**Últimas tareas de instalación de parches**”.

• **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción		Cadena de caracteres

Tabla 15.25: Campos del fichero exportado Historial de instalaciones

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Fecha	Última fecha de intento de instalación.	Fecha
Programa	Nombre del programa o versión del sistema operativo Windows que recibió el parche.	Cadena de caracteres
Versión	Versión del programa o sistema operativo que recibió el parche.	Cadena de caracteres
Parche	Nombre del parche instalado.	Cadena de caracteres
Críticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador de KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y sus requisitos si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Instalación	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado

Tabla 15.25: Campos del fichero exportado Historial de instalaciones

Campo	Comentario	Valores
Error de instalación	El módulo de Panda Patch Management no se instaló correctamente.	• Imposible realizar la descarga: instalador no disponible • Imposible realizar la descarga: fichero corrupto • Espacio insuficiente en disco
URL de descarga	URL para descargar el parche de forma individual.	Cadena de caracteres
Código de resultado	Código resultado de la instalación del parche. Puede indicar el éxito o el motivo del fracaso de la operación. Consulta la documentación del proveedor para interpretar el código de resultado.	Númerico

Tabla 15.25: Campos del fichero exportado Historial de instalaciones

• **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Desde	Fecha de inicio para el intervalo de búsqueda.	Fecha
Hasta	Fecha de finalización para el intervalo de búsqueda.	Fecha
Críticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Tabla 15.26: Campos de filtrado para el listado Historial de instalaciones

Campo	Comentario	Valores
Instalación	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
CVE	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres

Tabla 15.26: Campos de filtrado para el listado Historial de instalaciones

• **Ventana Parche instalado**

Al hacer clic en una de las filas del listado se mostrará la ventana Parche instalado con información detallada del parche.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Críticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Fecha de instalación	Fecha en la que el parche se instaló con éxito en el equipo.	Fecha

Tabla 15.27: Campos de la ventana Parche instalado

Campo	Comentario	Valores
Resultado	Estado de la instalación del parche o actualización.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones especiales y problemas solucionados.	Cadena de caracteres

Tabla 15.27: Campos de la ventana Parche instalado

Parches excluidos

Este listado muestra los parches que el administrador ha marcado como excluidos para evitar su instalación en los equipos de la red. Se muestra una línea por cada par parche - equipo excluido, excepto en el caso de exclusiones para todos los equipos de la red, que se mostrarán en una única línea.

Campo	Comentario	Valores
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía: •  Si el parche se ha excluido para un único equipo se incluye el nombre del equipo. •  Si el parche se ha excluido para todos los equipos de la cuenta se incluye el literal "(Todos)".	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres

Tabla 15.28: Campos del listado Parches excluidos

Campo	Comentario	Valores
Parche	Nombre del parche excluido.	Cadena de caracteres
Críticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 15.28: Campos del listado Parches excluidos



Para visualizar los datos del listado gráficamente accede al widget **"Parches disponibles"**.

• **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Dependiendo del destino de la exclusión el contenido de este campo varía: • Si el parche se ha excluido para un único equipo indica el nombre del equipo. • Si el parche se ha excluido para todos los equipos de la cuenta indica el literal "(Todos)".	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción del equipo asignada por el administrador de la red.	Cadena de caracteres

Tabla 15.29: Campos del fichero exportado Parches excluidos

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Versión	Versión del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Criticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs (Common Vulnerabilities and Exposures)	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Identificador KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga (KB)	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Excluido por	Cuenta de usuario de la consola de administración que excluyó el parche.	Cadena de caracteres
Excluido desde	Fecha en la que se excluyó el parche.	Cadena de caracteres

Tabla 15.29: Campos del fichero exportado Parches excluidos

- **Herramienta de filtrado**

Campo	Comentario	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo con un parche excluido.	Cadena de caracteres
Programa	Nombre del programa al que pertenece el parche excluido.	Cadena de caracteres
Parche	Nombre del parche excluido.	Cadena de caracteres
Mostrar parches no descargables	Indica los parches que no son descargables directamente por Panda Patch Management debido a requisitos adicionales del proveedor (aceptación de EULA, introducción de credenciales, captchas etc.).	Booleano
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Críticidad	Importancia del parche instalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack

Tabla 15.30: Campos de filtrado para el listado Parches excluidos

- **Ventana Parche excluido**

Al hacer clic en una de las filas del listado se mostrará la ventana Parche excluido con información detallada del parche marcado para no instalarse en los equipos de la red.

Campo	Comentario	Valores
Parche	Nombre del parche o actualización e información adicional (fecha de publicación, número de la Knowledge base etc.).	Cadena de caracteres

Tabla 15.31: Campos de la ventana Parche instalado

Campo	Comentario	Valores
Programa	Nombre del programa desactualizado o versión del sistema operativo Windows con parches pendientes de aplicar.	Cadena de caracteres
Críticidad	Indica la importancia de la actualización y tipo.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
CVEs	Número del caso CVE (Common Vulnerabilities and Exposures) que describe la vulnerabilidad asociado al parche.	Cadena de caracteres
Equipo	Nombre del equipo con software desactualizado.	Cadena de caracteres
Fecha de publicación	Fecha en la que el parche se liberó para su descarga y aplicación.	Fecha
Tamaño de la descarga	Tamaño del parche en formato comprimido. La aplicación de parches y actualizaciones puede requerir más espacio en el dispositivo de almacenamiento del equipo que el indicado en este campo.	Numérico
Identificador de la KB	Nombre del artículo de la Knowledge Base de Microsoft que describe las vulnerabilidades corregidas por el parche y los requisitos para su instalación si los hubiera.	Cadena de caracteres
Descripción	Notas que incluye el fabricante sobre los efectos que produce aplicar el parche, condiciones especiales y problemas solucionados.	Cadena de caracteres

Tabla 15.31: Campos de la ventana Parche instalado

Resultados tarea de instalación / desinstalación de parches

Este listado muestra los resultados de tareas de instalación o desinstalación de parches en los equipos de la red.

Campo	Descripción	Valores
Nombre	Nombre del equipo en el que se realizó la instalación / desinstalación del parche.	Cadena de caracteres

Tabla 15.32: Campos de resultados de tarea de instalación / desinstalación

Campo	Descripción	Valores
Grupo	Grupo de Panda Adaptive Defense 360 al que pertenece el equipo.	Cadena de caracteres
Estado	Estado de la tarea.	• Pendiente • En curso • Finalizada • Con error • Cancelada (no se pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Parches instalados / desinstalados	Número de parches instalados / desinstalados.	Cadena de caracteres.
Fecha comienzo	Fecha en la que se inicio la instalación.	Fecha
Fecha fin	Fecha en la que se finalizo la instalación.	Fecha

Tabla 15.32: Campos de resultados de tarea de instalación / desinstalación



Para visualizar los datos del listado gráficamente accede al widget “Últimas tareas de instalación de parches”.

• **Herramientas de filtrado**

Campo	Descripción	Valores
Estado	Estado de la tarea de instalación / desinstalación.	• Pendiente • En curso • Finalizada • Con error • Cancelada (no se pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)

Tabla 15.33: Filtros disponibles en listado Resultados tarea de instalación / desinstalación de parches

Campo	Descripción	Valores
Parches aplicados / desinstalados	Equipos en los que se han instalado / desinstalado parches.	• Todos • Sin parches instalados / desinstalados • Con parches instalados / desinstalados

Tabla 15.33: Filtros disponibles en listado Resultados tarea de instalación / desinstalación de parches

Ver parches instalados / desinstalados

Muestra los parches instalados en los equipos y otra información adicional.

Campo	Descripción	Valores
Equipo	Nombre del equipos en el que se realizó la instalación / desinstalación.	Cadena de caracteres
Grupo	Grupo de Panda Adaptive Defense 360 al que pertenece el equipo.	Cadena de caracteres
Programa	Programa que recibe el parche.	Cadena de caracteres
Versión	Versión del programa.	Cadena de caracteres
Parche	Parche instalado / desinstalado.	Cadena de caracteres
Críticidad	Relevancia del parche instalado / desinstalado.	• Otros parches (no de seguridad) • Crítica (de seguridad) • Importante (de seguridad) • Moderada (de seguridad) • Baja (de seguridad) • No clasificado (de seguridad) • Service Pack
Resultado	Indica si el proceso se ha completado correctamente o ha sucedido algún error.	• Instalado • Requiere reinicio • Error • El parche ya no es requerido • Desinstalado
Fecha	Fecha de ejecución del proceso.	Fecha

Tabla 15.34: Campos de resultado de instalación / desinstalación de parches



Para visualizar los datos del listado gráficamente accede al widget **“Últimas tareas de instalación de parches”**.

Capítulo 16

Panda Full Encryption (Cifrado de dispositivos)

Panda Full Encryption es un módulo integrado en la plataforma Aether que cifra el contenido de los medios de almacenamiento conectados a los equipos administrados por Panda Adaptive Defense 360. Su objetivo es minimizar la exposición de la información de las empresas, tanto en casos de pérdida o robo de los equipos como al descartar sistemas de almacenamiento en uso sin borrar previamente su contenido.

Panda Full Encryption es compatible con ciertas versiones de sistemas operativos Windows 7 en adelante (consulta "[Versiones del sistema operativo compatibles](#)") y permite controlar el estado del cifrado de los equipos de la red, gestionando de forma centralizada sus claves de recuperación. Además, aprovecha recursos hardware como los chips TPM, ofreciendo una gran flexibilidad a la hora de elegir el sistema de autenticación más adecuado en cada caso.



Para obtener información adicional sobre los distintos apartados del módulo Panda Full Encryption consulta las referencias siguientes:

- "[Crear y gestionar configuraciones](#)" en la página [213](#): información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.
- "[Control y supervisión de la consola de administración](#)" en la página [67](#): gestión de cuentas de usuario y asignación de permisos.
- "[Gestión de listados](#)" en la página [56](#): información sobre como gestionar listados.

CONTENIDO DEL CAPÍTULO

Introducción a los conceptos de cifrado	372
TPM	372
PIN y PIN extendido / mejorado	373
Passphrase	373
Llave USB	373
Clave de recuperación	373
BitLocker	374
Partición de sistema	374
Algoritmo de cifrado	375
Visión general del servicio de Panda Full Encryption	375
Características generales de Panda Full Encryption	375

Tipos de autenticación soportados	375
Tipo de dispositivos de almacenamiento compatibles	376
Requisitos mínimos de Panda Full Encryption - - - - -	376
Versiones del sistema operativo compatibles	376
Requisitos hardware	377
Gestión de equipos según su estado de cifrado previo - - - - -	377
Administración de equipos por Panda Full Encryption	377
Desinstalación del agente Panda Adaptive Defense 360	377
Proceso de cifrado y descifrado - - - - -	377
Cifrado de volúmenes sin cifrado previo	377
Cifrado de volúmenes ya cifrados previamente	380
Cifrado de nuevos volúmenes	380
Descifrado de volúmenes	380
Modificación local de la configuración de BitLocker	381
Cifrado y descifrado de discos duros externos y llaves USB	381
Comportamiento de Panda Full Encryption ante errores - - - - -	382
Obtención de la clave de recuperación - - - - -	382
Paneles / widgets del módulo Panda Full Encryption - - - - -	383
Acceso al panel de control	383
Permisos requeridos	383
Estado del cifrado	383
Equipos compatibles con cifrado	385
Equipos cifrados	386
Métodos de autenticación aplicados	387
Listados en Panda Full Encryption - - - - -	389
Acceso a los listados	389
Permisos requeridos	389
Estado del cifrado	389
Configuración del cifrado - - - - -	393
Acceso a la configuración	393
Permisos requeridos	394
Opciones de configuración de Panda Full Encryption	394
Cifrar todos los discos duros de los equipos	394
Solicitar una contraseña para acceder al equipo	394
No cifrar los equipos que requieren un USB para autenticarse	395
Cifrar sólo el espacio utilizado	395
Ofrecer cifrado de unidades de almacenamiento extraíbles	395
Filtros disponibles - - - - -	395

Introducción a los conceptos de cifrado

Panda Full Encryption utiliza las herramientas integradas en los sistemas operativos Windows para gestionar el cifrado en los equipos de la red gestionados con Panda Adaptive Defense 360.

Para una correcta comprensión de los procesos involucrados en el cifrado y descifrado de la información, es necesario presentar algunos conceptos relativos a la tecnología de cifrado utilizada.

TPM

TPM (Trusted Platform Module, módulo de plataforma segura) es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la

información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación.

Además, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

La versión mínima de TPM soportada por Panda Full Encryption es la 1.2. y Panda Security recomienda su uso en combinación con otros sistemas de autenticación soportados. En algunos escenarios es posible que el TPM esté deshabilitado en la BIOS del equipo y sea necesario su activación manual.

PIN y PIN extendido / mejorado

PIN (Personal Identification Number, número de identificación personal) es una secuencia de 8 a 20 números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible.

Si el hardware es compatible, Panda Full Encryption utilizará un PIN extendido o PIN mejorado compuesto por letras y números para incrementar la complejidad de la contraseña.

Debido a que el PIN Extendido se pide en el proceso de inicio del equipo previo a la carga del sistema operativo, las limitaciones de la BIOS pueden restringir la entrada de teclado a la tabla ASCII de 7 bits. Adicionalmente, los teclados que utilizan una distribución distinta a la dispuesta en el mapa de caracteres EN-US, tales como teclados QWERTZ o AZERTY, pueden provocar el fallo en la introducción del PIN Extendido. Por esta razón Panda Full Encryption controla que los caracteres introducidos por el usuario pertenecen al mapa EN-US antes de establecer el PIN Extendido en el proceso de cifrado del equipo.

Passphrase

Es una contraseña de 8 a 255 caracteres alfanuméricos equivalente al PIN Extendido.

Llave USB

Permite almacenar la clave de acceso en un dispositivo USB formateado con NTFS, FAT o FAT32. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.



Algunos PCs antiguos no son capaces de acceder a las unidades USB en el proceso de arranque, comprueba que los equipos de tu organización tienen acceso a las unidades USB desde la BIOS.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Panda Full Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de

recuperación de 48 dígitos. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo. Cada volumen cifrado tendrá su propia clave de recuperación independiente.



Panda Full Encryption únicamente almacena las claves de recuperación de los equipos que gestiona. La consola de administración no mostrará las claves de recuperación de los equipos cifrados por el usuario y no gestionados por Panda Security.

La clave de recuperación se solicita en los escenarios mostrados a continuación:

- Cuando se introduce errónea y repetidamente el PIN o la passphrase en el proceso de inicio del equipo.
- Cuando un equipo protegido con TPM detecta un cambio en la secuencia de arranque (disco duro protegido por TPM y conectado en otro equipo).
- Cuando se ha cambiado la placa base del equipo y por lo tanto el TPM.
- Al desactivar, deshabilitar o borrar el contenido del TPM.
- Al cambiar los valores de configuración de arranque del equipo.
- Al cambiar el proceso de arranque del equipo:
 - Actualización de la BIOS.
 - Actualización del firmware.
 - Actualización de la UEFI.
 - Modificación del sector de arranque.
 - Modificación del registro maestro de arranque (master boot record).
 - Modificación del gestor de arranque (boot manager).
 - Cambio del firmware implementado en ciertos componentes que forman parte del proceso de arranque del equipo (tarjetas de vídeo, controladores de discos, etc.) conocido como Option ROM.
 - Cambio de otros componentes que intervienen en las fases iniciales del arranque del sistema.

BitLocker

Es el software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo. Panda Full Encryption instala BitLocker automáticamente en aquellas versiones de servidor que no lo incluyan pero sean compatibles.

Partición de sistema

Es una zona pequeña del disco duro de 1.5 gigabytes aproximadamente que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio. Panda Full Encryption crea automáticamente esta partición de sistema si no existiera previamente.

Algoritmo de cifrado

El algoritmo de cifrado elegido en Panda Full Encryption es el AES-256 aunque los equipos con volúmenes cifrados por el usuario que utilicen otro algoritmo de cifrado también son compatibles.

Visión general del servicio de Panda Full Encryption

El proceso general de cifrado abarca varios apartados que el administrador deberá conocer para gestionar correctamente los recursos de la red susceptibles de contener información delicada o comprometedoras en caso de robo, pérdida o descarte del volumen sin borrar:

- **Cumplimiento de los requisitos mínimos de hardware y software:** consulta "[Requisitos mínimos de Panda Full Encryption](#)" para ver las limitaciones y particularidades del cifrado en cada plataforma compatible.
- **Estado previo del cifrado en el equipo del usuario:** dependiendo de si BitLocker estaba siendo usado previamente en el equipo del usuario, el proceso de integración en Panda Full Encryption puede variar ligeramente.
- **Asignación de configuraciones de cifrado:** establece el estado (cifrado o no cifrado) de los equipos de la red y el o los métodos de autenticación.
- **Interacción del proceso de cifrado con el usuario del equipo:** el proceso de cifrado inicial requiere de la colaboración del usuario para completarse de forma correcta. Consulta "[Cifrado de volúmenes sin cifrado previo](#)".
- **Visualización del estado de cifrado del parque informático:** mediante los widgets / paneles incluidos en el menú superior **Estado**, panel lateral **Full Encryption**. Consulta "[Paneles / widgets del módulo Panda Full Encryption](#)" para una descripción completa de los widgets incluidos en Panda Full Encryption. También se soportan filtros para localizar equipos en los listados según su estado. Consulta "[Filtros disponibles](#)".
- **Restricción de los permisos de cifrado a los administradores de la seguridad:** el sistema de roles mostrado en "[Descripción de los permisos implementados](#)" en la página 72 abarca la funcionalidad de cifrado y visualización del estado de los equipos de la red.
- **Obtención de la clave de recuperación:** en los casos en que el usuario haya olvidado el PIN / passphrase o el TPM haya detectado una situación anómala el administrador de la red podrá obtener de forma centralizada la clave de recuperación y enviársela al usuario. Consulta "[Obtención de la clave de recuperación](#)".

Características generales de Panda Full Encryption

Tipos de autenticación soportados

Dependiendo de la existencia o no de TPM y de la versión del sistema operativo, Panda Full Encryption admite distintas combinaciones de métodos de autenticación, mostrados a continuación de forma ordenada según la recomendación de Panda Security:

- **TPM + PIN:** compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS y el establecimiento de un PIN.
- **Solo TPM:** compatible con todas las versiones de Windows soportadas, requiere el chip TPM habilitado en la BIOS excepto en Windows 10, donde se habilita de forma automática.
- **Dispositivo USB:** requiere una llave USB y un equipo que pueda acceder a dispositivos USBs en el arranque. Necesario en equipos Windows 7 sin TPM.
- **Passphrase:** solo disponible en equipos Windows 8 y posteriores sin TPM.

Panda Full Encryption utiliza por defecto un método de autenticación que incluya el uso de TPM si se encuentra disponible. Si se elige una combinación de autenticación no incluida en el listado anterior, la consola de administración mostrará una ventana de advertencia indicando que el equipo permanecerá sin cifrar.

Tipo de dispositivos de almacenamiento compatibles

Panda Full Encryption cifra todos los dispositivos internos de almacenamiento masivo:

- Unidades de almacenamiento fijas del equipo (sistema y datos).
- Discos duros virtuales (VHD) pero únicamente el espacio utilizado independientemente de lo indicado en la consola de administración.
- Discos duros extraíbles.
- Llaves USB.

No se cifrarán:

- Discos duros internos dinámicos.
- Particiones de tamaño muy reducido.
- Otros dispositivos de almacenamiento externo.

Requisitos mínimos de Panda Full Encryption

Los requisitos mínimos se dividen en:

- Versiones del sistema operativo Windows y familias compatibles.
- Requisitos de hardware.

Versiones del sistema operativo compatibles

- Windows 7 (Ultimate, Enterprise)
- Windows 8/8.1 (Pro, Enterprise)
- Windows 10 (Pro, Enterprise, Education)
- Windows Server 2008 R2 y superiores (incluyendo a las ediciones Server Core)

Requisitos hardware

- TPM 1.2 y superiores si se utiliza este método de autenticación.
- Llave USB y equipo compatible con la lectura de dispositivos USB desde la BIOS en sistemas Windows 7 sin TPM.

Gestión de equipos según su estado de cifrado previo

Administración de equipos por Panda Full Encryption

Para que un equipo de la red se considere gestionado por Panda Full Encryption es necesario que se cumplan las condiciones siguientes:

- El equipo cumple con los requisitos mínimos descritos en “[Requisitos mínimos de Panda Full Encryption](#)”.
- El equipo ha recibido al menos una vez una configuración desde la consola de administración que establezca el cifrado de los volúmenes y éste se ha completado con éxito.

Los equipos que previamente tenían cifrado alguno de sus volúmenes y no han recibido una configuración que cifre sus unidades no serán gestionados por Panda Full Encryption y por lo tanto el administrador no tendrá acceso a la clave de recuperación ni al estado del equipo.

Por el contrario, los equipos que han recibido una configuración que cifre sus unidades, independientemente de su estado anterior (cifrado o no) serán administrados por Panda Full Encryption.

Desinstalación del agente Panda Adaptive Defense 360

Independientemente de si el equipo estaba siendo administrado por Panda Full Encryption o no, si los dispositivos de almacenamiento estaban cifrados, al desinstalar Panda Adaptive Defense 360 se dejarán tal y como están. No obstante, se perderá el acceso centralizado a la clave de recuperación.

Si posteriormente el equipo se reintegra en Panda Adaptive Defense 360 se mostrará la última clave de recuperación almacenada.

Proceso de cifrado y descifrado

Cifrado de volúmenes sin cifrado previo

El proceso de cifrado se inicia cuando el agente Panda Adaptive Defense 360 instalado en el equipo de usuario se descarga una configuración de tipo Cifrado. En ese momento se le mostrará al usuario una ventana informativa que le guiará en todo el proceso.

El número de pasos total varía dependiendo del tipo de autenticación elegida por el administrador y del estado previo del equipo. Si cualquiera de los pasos termina en un error, el agente lo reportará a la consola de administración y el proceso se detendrá.



No se permitirá el cifrado de equipos desde una sesión de escritorio remoto ya que es necesario el reinicio del equipo y la introducción de una clave antes de la carga del sistema operativo, operaciones que no son posibles con un sistema de escritorio remoto estándar.

El proceso de cifrado se iniciará cuando la instalación o desinstalación en curso de parches gestionados por el módulo Panda Full Encryption haya finalizado.

A continuación se muestra el proceso completo de cifrado y se indica si se muestra feedback al usuario del equipo y si es necesario el reinicio de la máquina:

Paso	Proceso en el equipo	Interacción con el usuario
1	El agente recibe una configuración del módulo de cifrado que pide cifrar el contenido de los dispositivos de almacenamiento instalados.	Ninguno
2	Si el equipo es de tipo servidor y no tiene las herramientas de BitLocker instaladas éstas se descargan y se instalan.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la instalación de BitLocker o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. Requiere reinicio.
3	Si el equipo no estaba cifrado previamente se crea la partición de sistema.	Se muestra una ventana pidiendo permiso para reiniciar el equipo y completar la creación de la partición de sistema o posponer. Si se elige posponer el proceso se detiene y se volverá a preguntar en el siguiente inicio de sesión. Requiere reinicio.
4	Si existe una directiva de grupo definida previamente por el administrador de la red que colisione con las establecidas por Panda Full Encryption se mostrará un error y el proceso terminará. Las directivas de grupo configuradas por Panda Full Encryption son:	Si el administrador no ha definido directivas de grupo globales que entren en colisión con las directivas locales definidas por Panda Full Encryption no se mostrará ningún mensaje.

Tabla 16.1: Pasos para el cifrado de volúmenes sin cifrar previamente

Paso	Proceso en el equipo	Interacción con el usuario
	En el Editor de Directivas de grupo local, navega la ruta siguiente: Directiva equipo local > Configuración del equipo > Plantillas administrativas > Componentes de Windows > Cifrado de unidad BitLocker > Unidades del sistema operativo. Marca a Sin definir las políticas de grupo indicadas para evitar este error.	
5	Preparación del TPM si existe y si el método de autenticación elegido involucra a éste componente y no estaba habilitado previamente desde la BIOS.	Requiere confirmar un reinicio para que el usuario pueda entrar en la BIOS del equipo y habilitar el TPM. En sistemas operativos Windows 10 no es necesario modificar la BIOS pero se requiere el reinicio igualmente. El reinicio del paso 3, en caso de haberlo, se juntará con el actual.
6	Preparación del dispositivo USB si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir un dispositivo USB para almacenar la contraseña de inicio de equipo.
7	Almacenamiento del PIN si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir el PIN. Si se utilizan caracteres alfanuméricos y el hardware no es compatible se mostrará el error "-2144272180". En este caso introduce un PIN numérico.
8	Almacenamiento de la passphrase si el método de autenticación elegido involucra a este componente.	Se requiere al usuario introducir la passphrase.
9	Se genera la clave de recuperación y se envía a la nube de Panda Security. Una vez que la clave se ha recibido, el proceso continúa en el equipo del usuario.	Ninguno.
10	Comprobación de que el hardware del equipo es compatible con la tecnología de cifrado, e inicio del cifrado.	Se requiere confirmar un reinicio para hacer el chequeo del hardware utilizado en los distintos métodos de autenticación elegidos. Requiere reinicio.
11	Cifrado de volúmenes.	Comienza el proceso de cifrado en segundo plano sin ocasionar molestias al usuario del equipo. La duración depende del volumen de datos a cifrar. Una duración media del tiempo de cifrado se sitúa en torno a las 2-3 horas. El usuario puede utilizar y apagar el equipo normalmente. El proceso de cifrado se reanudará en el siguiente encendido del equipo.

Tabla 16.1: Pasos para el cifrado de volúmenes sin cifrar previamente

Paso	Proceso en el equipo	Interacción con el usuario
12	El proceso de cifrado se completa de forma silenciosa y a partir de ese momento el proceso de cifrado y descifrado es transparente para el usuario.	Dependiendo del método de autenticación elegido el usuario puede necesitar introducir una llave USB, un PIN, una passphrase o nada en el inicio del equipo.

Tabla 16.1: Pasos para el cifrado de volúmenes sin cifrar previamente

Cifrado de volúmenes ya cifrados previamente

En el caso de que algún volumen del equipo ya estuviera cifrado, Panda Full Encryption modifica algunos parámetros para habilitar su gestión centralizada. A continuación se indican las acciones realizadas:

- Si el método de autenticación elegido por el usuario no coincide con el especificado en la configuración, éste se cambiará, solicitándole al usuario las claves o recursos hardware necesarios. Si no es posible asignar un método de autenticación compatible con la plataforma y con la configuración especificada por el administrador, el equipo quedará cifrado por el usuario y no será gestionado por Panda Full Encryption.
- Si el algoritmo de cifrado utilizado no está soportado (distinto de AES-256) se dejará sin cambios para evitar el descifrado y cifrado completo el volumen pero el equipo será administrado por Panda Full Encryption.
- Si existen tanto volúmenes cifrados como sin cifrar, se cifrarán todos los volúmenes aplicando el mismo método de autenticación.
- Si el método de autenticación elegido previamente involucra la introducción de una contraseña y es compatible con los métodos soportados por Panda Full Encryption, se volverá a pedir la contraseña al usuario para unificar el método de autenticación en todos los volúmenes.
- Si el usuario eligió una configuración de cifrado distinta a la establecida por el administrador (cifrado únicamente de los sectores ocupados frente al cifrado completo del volumen) el volumen se dejará sin cambios para minimizar el proceso de cifrado.
- Al final de todo el proceso el dispositivo pasa a ser gestionado por Panda Full Encryption y se genera la clave de recuperación para su posterior envío a la nube de Panda Security.

Cifrado de nuevos volúmenes

Si una vez completado el proceso de cifrado el usuario del equipo crea un nuevo volumen, Panda Full Encryption lo cifrará inmediatamente respetando la configuración asignada por el administrador de la red.

Descifrado de volúmenes

Se distinguen tres casos:

- Si Panda Full Encryption cifra un equipo, a partir de ese momento el administrador podrá asignar una configuración para descifrarlo.

- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Panda Full Encryption y se le asigna una configuración de cifrado se considerará cifrado por Panda Full Encryption y se podrá descifrar asignando una configuración desde la consola de administración.
- Si un equipo ya estaba cifrado por el usuario antes de la instalación de Panda Full Encryption y nunca se le ha asignado una configuración de cifrado no se considerará cifrado por Panda Full Encryption y no se podrá descifrar asignando una configuración desde la consola de administración.

Modificación local de la configuración de BitLocker

El usuario del equipo tiene acceso a la configuración local de BitLocker desde las herramientas de Windows pero los cambios que efectúe serán revertidos de forma inmediata a la configuración establecida por el administrador de la red a través de la consola de administración. El comportamiento de Panda Full Encryption ante un cambio de esta naturaleza se muestra a continuación:

- **Desactivar el desbloqueo automático de una unidad:** se revierte a la configuración de bloqueo automático.
- **Quitar la contraseña de un volumen:** se pedirá la nueva contraseña.
- **Descifrar un volumen previamente cifrado por Panda Full Encryption:** se cifrará automáticamente el volumen.
- **Cifrar una unidad descifrada:** si la configuración de Panda Full Encryption implica descifrar las unidades la acción del usuario prevalece y no se descifrá la unidad.

Cifrado y descifrado de discos duros externos y llaves USB

Como el usuario del equipo puede conectar y desconectar medios de almacenamiento externos en cualquier momento, el comportamiento de Panda Full Encryption para este tipo de dispositivos difiere en los puntos siguientes:

- Si el equipo del usuario o servidor no dispone de BitLocker, el agente no descargará los paquetes necesarios, y por lo tanto el dispositivo no se cifrará ni mostrará ningún aviso al usuario.
- Si el equipo dispone de BitLocker, solo se mostrará un mensaje emergente al usuario ofreciendo la posibilidad de cifrarlo en las siguientes situaciones:
 - Cada vez que conecte un dispositivo de almacenamiento USB sin cifrar.
 - Si hay un dispositivo conectado en el equipo y sin cifrar cuando el administrador activa la configuración desde la consola web.
- El mensaje de cifrado se mostrará al usuario durante 5 minutos, transcurridos los cuales dejará de ser visible. Tanto si el usuario acepta el cifrado como si no, el dispositivo podrá ser utilizado de forma normal, a no ser que se haya establecido previamente una configuración que impida el uso de estos dispositivos sin cifrar. Consulta [“Escritura en unidades de almacenamiento extraíbles”](#) en la página 293.
- Cifrar en un dispositivo USB no requiere crear una partición de sistema.

- Si el dispositivo de almacenamiento externo ya está cifrado por otra solución distinta de Panda Full Encryption, al conectarlo al equipo no se mostrará el mensaje de cifrado y se podrá usar con normalidad. Panda Full Encryption no enviará las claves de recuperación a la consola web.
- Si se ha establecido una configuración de control de dispositivos que impida la conexión de este tipo de hardware, no se mostrará el mensaje de cifrado en el equipo del usuario. Consulta "[Control de dispositivos \(Equipos Windows\)](#)" en la página 255.
- No se permitirá la escritura en dispositivos USB si está establecida la configuración **Escritura en unidades de almacenamiento extraíbles** de Panda Data Control y el dispositivo no ha sido cifrado con BitLocker o con Panda Full Encryption. Consulta "[Escritura en unidades de almacenamiento extraíbles](#)" en la página 293.
- Para descifrar un dispositivo cifrado por Panda Full Encryption el usuario puede utilizar BitLocker de forma manual.
- Solo se cifra el espacio utilizado.
- Todas las particiones del dispositivo se cifran con la misma clave.



Retirar un dispositivo USB cuando el proceso de cifrado no se ha completado puede corromper todo su contenido.

Comportamiento de Panda Full Encryption ante errores

- **Errores en el test de hardware:** el test de hardware se ejecuta cada vez que se inicia el equipo hasta que sea superado, momento en el que el equipo comenzará el cifrado automáticamente.
- **Error al crear la partición de sistema:** muchos errores al crear la partición de sistema son subsanables por el propio usuario del equipo (por ejemplo la falta de espacio). Periódicamente Panda Full Encryption intentará crear la partición de forma automática.
- **Negativa a activar el chip TPM por parte del usuario:** el equipo mostrará un mensaje en cada proceso de inicio pidiéndole al usuario la activación del chip TPM. Hasta que esta condición no sea resuelta el proceso de cifrado no comenzará.

Obtención de la clave de recuperación

En los casos en que el usuario haya perdido el PIN / passphrase / dispositivo USB o el chip TPM haya detectado un cambio en la cadena de inicio del equipo, será necesaria la introducción de la clave de recuperación. Panda Full Encryption mantiene todas las claves de recuperación de los equipos de la red cuyo cifrado gestiona.

Para obtener la clave de recuperación de un equipo sigue los pasos mostrados a continuación:

- En el menú superior **Equipos** haz clic en el equipo cuyas claves quieres recuperar.
- En la pestaña **Detalles**, sección **Protección de datos**, haz clic en el enlace **Obtener la clave de**

- recuperación.** Se mostrará una ventana con los identificadores de volumen cifrados.
- Haz clic en un identificador de volumen para mostrar su contraseña de recuperación.

Paneles / widgets del módulo Panda Full Encryption

Acceso al panel de control

Para acceder haz clic en el menú superior **Estado**, panel lateral Full Encryption.

Permisos requeridos

No se necesitan permisos adicionales para acceder a los widgets asociados a **Panda Full Encryption**.

Estado del cifrado

Muestra el total de equipos compatibles con Panda Full Encryption así como su estado con respecto a la tecnología de cifrado.

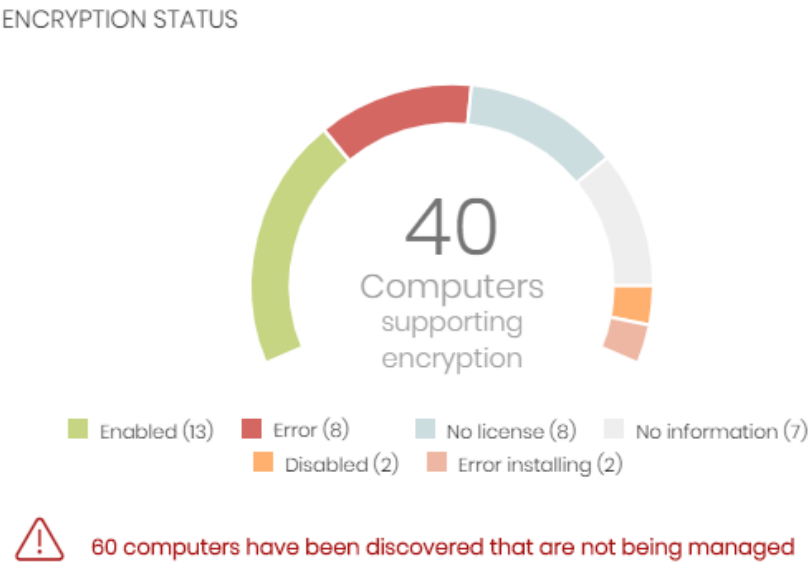


Figura 16.1: Panel de Estado del cifrado

• **Significado de las series**

Serie	Descripción
Activado	Equipos con Panda Full Encryption instalado, con una configuración que indica cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Desactivado	Equipos con Panda Full Encryption instalado, con una configuración que indica no cifrar el equipo y sin reporte de errores de cifrado ni de instalación.
Error	No se ha podido realizar la acción que el administrador ha indicado en la configuración de cifrado o descifrado.

Tabla 16.2: Descripción de la serie Estado del cifrado

Serie	Descripción
Error instalando	No se ha podido descargar e instalar BitLocker si fue necesario.
Sin licencia	Equipo compatible con Panda Full Encryption pero sin licencia asignada.
Sin información	Equipos con licencia recientemente asignada y que todavía no han reportado su estado al servidor, o equipo con un agente sin actualizar.

Tabla 16.2: Descripción de la serie Estado del cifrado

• Filtros preestablecidos desde el panel

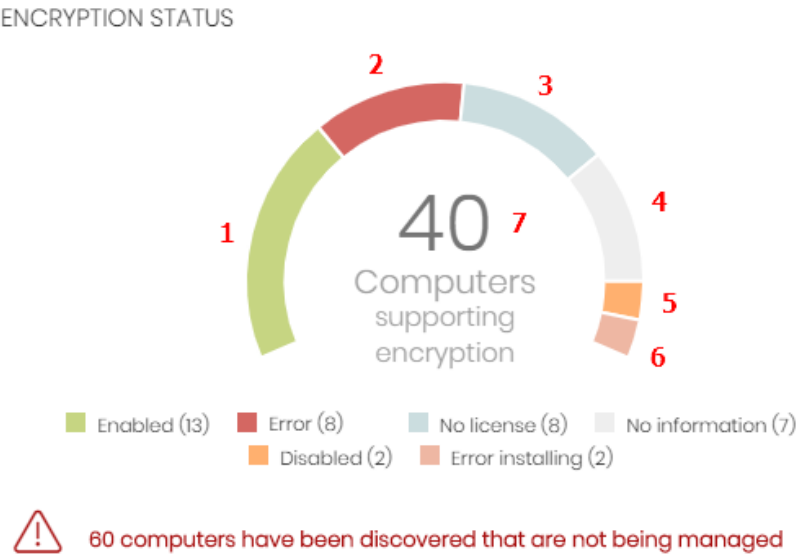


Figura 16.2: Zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en la figura 16.2 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado del cifrado = Activado.
(2)	Estado del cifrado = Error.
(3)	Estado del cifrado = Sin licencia.
(4)	Estado del cifrado = Sin información.
(5)	Estado del cifrado = Desactivado.
(6)	Estado del cifrado = Error instalando.
(7)	Sin filtros.

Tabla 16.3: Definición de filtros del listado Estado del cifrado

Equipos compatibles con cifrado

Muestra los equipos compatibles y no compatibles con la tecnología de filtrado agrupados en series según su tipo.

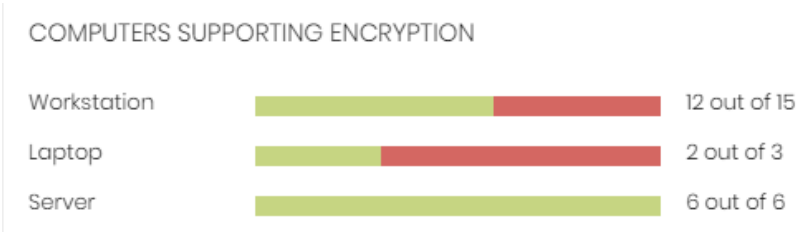


Figura 16.3: Panel de Equipos compatibles con cifrado

• Significado de las series

Serie	Descripción
Estación - verde	Dispositivos de tipo estación compatibles con cifrado.
Estación - rojo	Dispositivos de tipo estación no compatibles con cifrado.
Portátil - verde	Dispositivos de tipo portátil compatibles con cifrado.
Portátil - rojo	Dispositivos de tipo portátil no compatibles con cifrado.
Servidor - verde	Dispositivos de tipo servidor compatibles con cifrado.
Servidor - rojo	Dispositivos de tipo servidor no compatibles con cifrado.

Tabla 16.4: Descripción de la serie Equipos compatibles con cifrado

• Filtros preestablecidos desde el panel

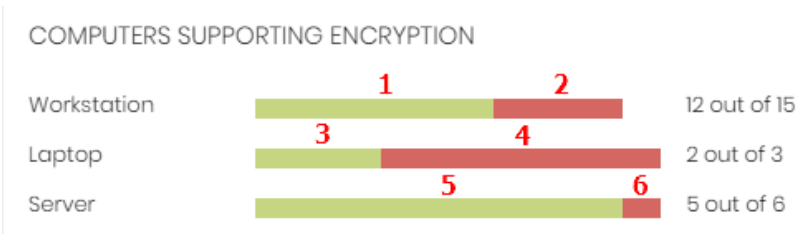


Figura 16.4: Zonas activas del panel Estado del cifrado

Al hacer clic en las zonas indicadas en la figura 16.4 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Tipo de equipo = Estación.
(2)	Listado de equipos con filtro No compatibles con cifrado.
(3)	Tipo de equipo = Portátil.
(4)	Listado de equipos con filtro No compatibles con cifrado.

Tabla 16.5: Definición de filtros del listado Estado del cifrado

Zona activa	Filtro
(5)	Tipo de equipo = Servidor.
(6)	Listado de equipos con filtro No compatibles con cifrado.

Tabla 16.5: Definición de filtros del listado Estado del cifrado

Equipos cifrados

Muestra el estado del proceso de cifrado en los equipos de la red compatibles con Panda Full Encryption.

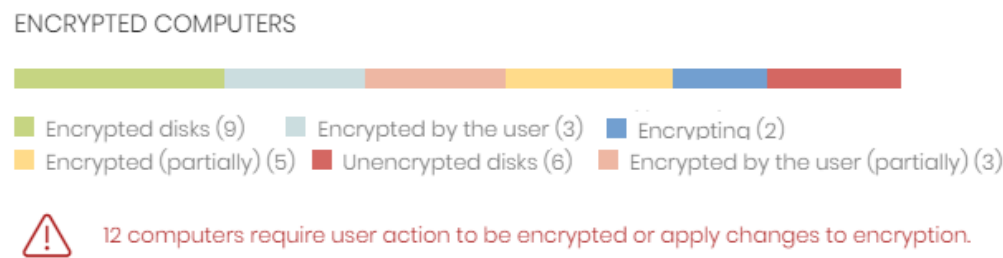


Figura 16.5: Panel Equipos cifrados

• Significado de las series

Serie	Descripción
Desconocido	Medios de almacenamiento cifrados con un método de autenticación no soportado por Panda Full Encryption.
Discos no cifrados	Ninguno de los medios de almacenamiento del equipo están cifrados ni por el usuario ni por Panda Full Encryption.
Discos cifrados	Todos los medios de almacenamiento del equipo están cifrados por Panda Full Encryption.
Cifrando	Al menos un medio de almacenamiento del equipo está en proceso de cifrado.
Descifrando	Al menos un medio de almacenamiento del equipo está en proceso de descifrado.
Cifrado por el usuario	Todos los medios de almacenamiento se encuentran cifrados pero alguno de ellos o todos fueron cifrados por el usuario.
Cifrado por el usuario (parcialmente)	Alguno de los medios de almacenamiento se encuentran cifrados por el usuario y el resto permanece sin cifrar o está cifrado por Panda Full Encryption.
Cifrado (parcialmente)	Al menos uno de los medios de almacenamiento del equipo está cifrado por Panda Full Encryption pero el resto permanece sin cifrar.

Tabla 16.6: Descripción de la serie Equipos cifrados

• Filtros preestablecidos desde el panel

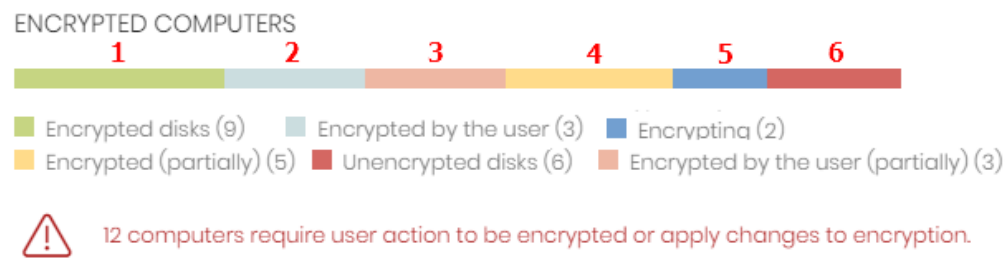


Figura 16.6: Zonas activas del panel Equipos Cifrados

Al hacer clic en las zonas indicadas en la figura 16.6 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Cifrado de discos = Discos cifrados.
(2)	Cifrado de discos = Cifrado por el usuario.
(3)	Cifrado de discos = Cifrado por el usuario (parcialmente).
(4)	Cifrado de discos = Cifrado (parcialmente).
(5)	Cifrado de discos = Cifrando.
(6)	Cifrado de discos = Discos no cifrados.
(7)	Cifrado de discos = Descifrando.
(8)	Cifrado de discos = Desconocido.

Tabla 16.7: Definición de filtros del listado Estado del cifrado

Métodos de autenticación aplicados

Muestra los equipos con el cifrado configurado en la red agrupados por el tipo de autenticación elegido.

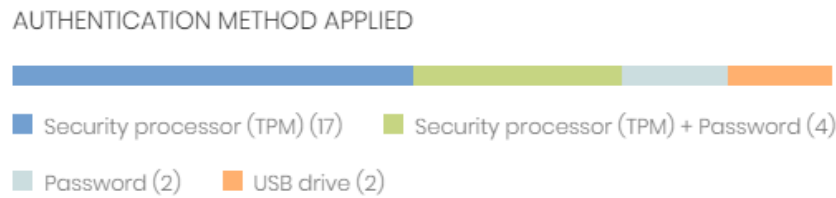


Figura 16.7: Panel Métodos de autenticación

• Significado de las series

Serie	Descripción
Desconocido	El método de autenticación elegido por el usuario del equipo no está soportado por Panda Full Encryption.
Procesador de seguridad (TPM)	El método de autenticación utilizado es TPM.
Procesador de seguridad (TPM) + Contraseña	El método de autenticación utilizado es TPM y PIN o passphrase solicitado en el inicio del equipo.
Contraseña	El método de autenticación elegido es PIN o passphrase solicitado en el inicio del equipo.
USB	El método de autenticación elegido es dispositivo USB conectado en el arranque del equipo.
Sin cifrar	Ninguno de los dispositivos de almacenamiento del equipo está cifrado.

Tabla 16.8: Descripción de la serie Métodos de autenticación aplicado

• Filtros preestablecidos desde el panel

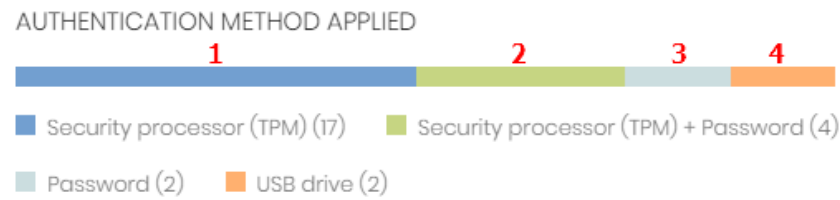


Figura 16.8: Zonas activas del panel Métodos de autenticación aplicado

Al hacer clic en las zonas indicadas en la figura 16.8 se abre el listado **Estado del cifrado** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Método de autenticación = Procesador de seguridad (TPM)
(2)	Método de autenticación= Procesador de seguridad (TPM) + Contraseña
(3)	Método de autenticación = Contraseña
(4)	Método de autenticación = USB
(5)	Método de autenticación = Desconocido
(6)	Método de autenticación = Sin cifrar

Tabla 16.9: Definición de filtros del listado

Listados en Panda Full Encryption

Acceso a los listados

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Full Encryption y** en el widget relacionado.

ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona un listado de la sección **Protección de datos** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

El acceso al listado **Estado del cifrado** no requiere permisos adicionales para el administrador.

Estado del cifrado

Este listado muestra todos los equipos de la red gestionados por Panda Adaptive Defense 360 y compatibles con Panda Full Encryption. Incorpora filtros relativos al módulo para controlar el estado del cifrado en el parque informático.

Campo	Comentario	Valores
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo y versión instalada en el equipo de usuario o servidor.	Cadena de caracteres
Cifrado de discos duros	Estado del módulo Panda Full Encryption.	• Sin información • Activado • Desactivado • Error • Error instalando • Sin licencia
Estado de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados

Tabla 16.10: Campos del listado Estado de cifrado

Campo	Comentario	Valores
		• Cifrando • Descifrando • Cifrado por el usuario • Cifrado por el usuario (parcialmente) • Cifrado (parcialmente)
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Sin cifrar
Última conexión	Fecha de la última vez que el agente se conectó con la nube de Panda Security.	Fecha

Tabla 16.10: Campos del listado Estado de cifrado



Para visualizar los datos del listado gráficamente accede al widget **"Equipos cifrados"**.

• **Campos mostrados en fichero exportado**

Campo	Comentario	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor
Equipo	Nombre del equipo compatible con la tecnología de cifrado.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres;
Descripción	Descripción asignada al equipo.	Cadena de caracteres

Tabla 16.11: Campos del fichero exportado

Campo	Comentario	Valores
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Panda.	Cadena de caracteres
Fecha de instalación	Fecha en la que el software Panda Adaptive Defense 360 se instaló con éxito en el equipo.	Fecha
Fecha de la última conexión		Fecha
Plataforma	Sistema operativo instalado en el equipo.	Cadena de caracteres
Sistema operativo	Sistema operativo del equipo, versión interna y nivel de parche aplicado.	Cadena de caracteres
Protección actualizada	El módulo de la protección instalado en el equipo es la última versión publicada.	Booleano
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Booleano
Fecha de la última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Cifrado de discos duros	Estado del módulo Panda Full Encryption.	• Sin información • Activado • Desactivado • Error • Error instalando • Sin licencia
Estados de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	• Desconocido • Discos no cifrados • Discos cifrados • Cifrando • Descifrando • Cifrado por el usuario • Cifrado (parcialmente) • Cifrado por el usuario (parcialmente)
Acciones de cifrado pendientes del usuario	El usuario tiene pendiente introducir información o reiniciar el equipo para completar el proceso de cifrado de los volúmenes.	Booleano

Tabla 16.11: Campos del fichero exportado

Campo	Comentario	Valores
Métodos de autenticación	Método de autenticación seleccionado para cifrar los discos.	• Todos • Desconocido • Procesador de seguridad (TPM) • Procesador de seguridad (TPM) + Contraseña • Contraseña • USB • Sin cifrar
Fecha de cifrado	Fecha del volumen más antiguo cifrado dentro de la primera que vez se consideró al equipo como completamente cifrado (se cifraron todos sus volúmenes compatibles).	Fecha
Versión de especificación del TPM	Versión de las especificaciones TPM soportadas por el chip incluido en el equipo.	Cadena de caracteres
Fecha error instalación cifrado	Fecha del último error de instalación reportado.	Fecha
Error instalación cifrado	Se ha producido un error al instalar el módulo Panda Full Encryption en el equipo.	Cadena de caracteres
Fecha error cifrado	Última fecha en la que se reportó un error de cifrado en el equipo.	
Error cifrado	El proceso de cifrado devolvió un error.	Cadena de caracteres

Tabla 16.11: Campos del fichero exportado

• **Herramienta de filtrado**

Campo	Comentario	Valores
Fecha de cifrado desde	Limite inferior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Fecha de cifrado hasta	Limite superior del rango de fechas en la que se consideró al equipo como completamente cifrado.	Fecha
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor

Tabla 16.12: Campos de filtrado para el listado

Campo	Comentario	Valores
Estado de los discos	Estado de los medios de almacenamiento interno del equipo con respecto al cifrado.	- Desconocido - Discos no cifrados - Discos cifrados - Cifrando - Descifrando - Cifrado por el usuario - Cifrado (parcialmente) - Cifrado por el usuario (parcialmente)
Cifrado de discos duros	Estado del módulo Panda Full Encryption.	- Sin información - Activado - Desactivado - Error - Error Instalando - Sin licencia
Método de autenticación	Método de autenticación seleccionado para cifrar los discos.	- Todos - Desconocido - Procesador de seguridad (TPM) - Procesador de seguridad (TPM) + Contraseña - Contraseña - USB - Sin cifrar
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha

Tabla 16.12: Campos de filtrado para el listado

- **Ventana detalle del equipo**

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta [“Información de equipo”](#) en la página 189 para obtener más información.

Configuración del cifrado

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Cifrado**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración.

Permisos requeridos

Permiso	Tipo de acceso
Configurar cifrado de equipos.	Crear, modificar, borrar, copiar o asignar las configuraciones de Cifrado.
Ver configuraciones de cifrado de equipos	Visualizar las configuraciones de Cifrado.

Tabla 16.13: Permisos requeridos para acceder a la configuración de Cifrado

Opciones de configuración de Panda Full Encryption

Cifrar todos los discos duros de los equipos

Indica si los dispositivos de almacenamiento interno del equipo serán cifrados o no. Dependiendo del estado anterior del equipo, el comportamiento de Panda Full Encryption será diferente:

- Si el equipo está cifrado por Panda Full Encryption y se deshabilita **Cifrar todos los discos duros de los equipos**, se descifrarán todos los volúmenes cifrados.
- Si el equipo está cifrado pero no por Panda Full Encryption y se deshabilita **Cifrar todos los discos duros de los equipos** los volúmenes no sufren ningún cambio.
- Si el equipo está cifrado pero no por Panda Full Encryption y se habilita **Cifrar todos los discos duros de los equipos** se adecuará la configuración interna de cifrado para que coincida con los métodos soportados en Panda Full Encryption evitando volver a cifrar el volumen. Consulta "[Cifrado de volúmenes ya cifrados previamente](#)".
- Si el equipo no está cifrado y se habilita **Cifrar todos los discos duros de los equipos** se cifrarán todos los volúmenes según el proceso mostrado en "[Cifrado de volúmenes sin cifrado previo](#)".

Solicitar una contraseña para acceder al equipo

Habilita la autenticación por contraseña en el arranque del equipo. Dependiendo de la plataforma y de la existencia de hardware TPM se permitirá el uso de dos tipos de contraseña:

- **Equipos con TPM:** se pedirá una contraseña de tipo PIN.
- **Equipos sin TPM:** se pedirá una contraseña de tipo passphrase.



Si estableces esta configuración a No y el equipo no tiene acceso a un procesador de seguridad TPM compatible, sus medios de almacenamiento no se cifrarán.

No cifrar los equipos que requieren un USB para autenticarse

Para evitar la utilización de dispositivos USB soportados por Panda Full Encryption en la autenticación, el administrador puede deshabilitar su uso.



Solo los equipos Windows 7 sin TPM están en posición de utilizar el método de autenticación por USB. Si el administrador deshabilita el uso de USBs, estos equipos no serán cifrados.

Cifrar sólo el espacio utilizado

El administrador puede minimizar el tiempo de cifrado empleado restringiendo la protección a los sectores del disco duro que están siendo utilizados. Los sectores liberados tras borrar un fichero continuarán cifrados pero el espacio libre previo al cifrado del disco duro permanecerá sin cifrar, siendo accesible por terceros mediante herramientas de recuperación de ficheros borrados.

Ofrecer cifrado de unidades de almacenamiento extraíbles

Muestra al usuario una ventana con la posibilidad de cifrar los medios de almacenamiento masivo externos y llaves USB cuando los conecta al equipo. Consulta "[Cifrado y descifrado de discos duros externos y llaves USB](#)" para obtener más información acerca del comportamiento y los requisitos de esta configuración.

Filtros disponibles

Para localizar los equipos de la red que coincidan con alguno de los estados de cifrado definidos en Panda Full Encryption utiliza los recursos del árbol de filtros mostrados en "[Árbol de filtros](#)" en la página [162](#) con los campos mostrados a continuación:

- Cifrado:
 - Acciones de cifrado pendientes del usuario.
 - Cifrado de discos.
 - Fecha de cifrado.
 - Método de autenticación.
 - Tiene acciones pendientes de cifrado del usuario.
- Configuración:
 - Cifrado.
- Equipo:
 - Tiene TPM.
- Hardware:

- TPM - Activado.
- TPM - Fabricante.
- TPM - Propietario.
- TPM - Versión.
- TPM - Versión de especificación.
- Módulos:
 - Cifrado.

Capítulo 17

Configuración del bloqueo de programas

Para incrementar la seguridad de base en los equipos Windows de la red, el administrador puede bloquear la ejecución de los programas que considere peligrosos o no compatibles con la actividad desarrollada en la empresa. Las causas que pueden llevar a un administrador a prohibir la ejecución de un determinado programa pueden ser:

- Programas que por sus altos requisitos consumen mucho ancho de banda o establecen un número de conexiones desproporcionadamente grande, poniendo en peligro el rendimiento de la conectividad de la empresa si son ejecutados por muchos usuarios simultáneos.
- Programas que permiten acceder a contenidos susceptibles de contener amenazas de seguridad o que están protegidos por licencias que la empresa no ha adquirido previamente.
- Programas que permiten acceder a contenidos no relacionados con la actividad de la empresa y que pueden afectar al ritmo de trabajo de los usuarios.



Para obtener información adicional sobre los distintos apartados del módulo Bloqueo de programas consulta las referencias siguientes:

- “[Crear y gestionar configuraciones](#)” en la página [213](#): información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.
- “[Control y supervisión de la consola de administración](#)” en la página [67](#): gestión de cuentas de usuario y asignación de permisos.
- “[Gestión de listados](#)” en la página [56](#): información sobre como gestionar listados.

CONTENIDO DEL CAPÍTULO

Configuración de Bloqueo de programas	398
Acceso a la configuración	398
Opciones de configuración de Bloqueo de programas	398
Listados del módulo Bloqueo de programas	399
Acceso a los listados	399
Permisos requeridos	399
Programas bloqueados por el administrador	399
Paneles / widgets del módulo Bloqueo de programas	400
Acceso al panel de control	400

Permisos requeridos 401

Programas bloqueados por el administrador 401

Configuración de Bloqueo de programas

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Bloqueo de programas**.
- Haz clic en el botón **Añadir**, se abrirá la ventana de configuración de **Bloqueo de programas**.



Las configuraciones de bloqueo de programas solo se pueden asignar a puestos de trabajo o servidores Windows.

Permisos requeridos

Permiso	Tipo de acceso
Configurar bloqueo de programas	Crear, modificar, borrar, copiar o asignar las configuraciones de Bloqueo de programas.
Ver configuraciones de bloqueo de programas	Visualizar las configuraciones de Bloqueo de programas.

Tabla 17.1: Permisos requeridos para acceder a la configuración Bloqueo de programas

Opciones de configuración de Bloqueo de programas

Para crear una nueva configuración o modificar una existente introduce la información mostrada a continuación:

Campo	Descripción
Nombres de los programas a bloquear	Nombres de los ficheros que Panda Adaptive Defense 360 impedirá su ejecución. En esta caja de texto acepta listas de nombres de ficheros copiadas / pegadas y separados por retorno de carro. No se admiten comodines para evitar configuraciones demasiado amplias que comprometan el buen funcionamiento del equipo.
Código MD5 de los programas a bloquear	MD5 de los ficheros que Panda Adaptive Defense 360 impedirá su ejecución. En esta caja de texto acepta listas de MD5s copiadas / pegadas y separados por retorno de carro.
Informar a los usuarios de los equipos de los bloqueados	Introduce un mensaje descriptivo para informar al usuario de que un fichero se ha bloqueado. El agente Panda Adaptive Defense 360 mostrará una ventana desplegable con el contenido del mensaje.

Tabla 17.2: Configuración de una política de seguridad Bloqueo de programas



No bloquee programas del sistema operativo o componentes que sean necesarios para poder ejecutar correctamente los programas de usuario.

Panda Adaptive Defense 360 no bloqueará ninguno de sus programas o módulos para garantizar el correcto funcionamiento de la solución de seguridad instalada.

Listados del módulo Bloqueo de programas

Acceso a los listados

El acceso a los listados se puede hacer siguiendo dos rutas:

- Desde el menú superior **Estado**, haz clic en el panel de la izquierda **Seguridad y** en el widget relacionado.

ó

- Desde el menú superior **Estado**, haz clic en el enlace **Añadir** del panel lateral. Se mostrará una ventana emergente con los listados disponibles.
- Selecciona el listado **Programas bloqueados por el administrador** de la sección **Control de actividad** para ver su plantilla asociada. Modifícala y haz clic en **Guardar**. El listado se añadirá al panel lateral.

Permisos requeridos

Permiso	Acceso a listados
Visualizar detecciones y amenazas	• Programas bloqueados por el administrador

Tabla 17.3: Permisos requeridos para acceder a los listados de Programas bloqueados

Programas bloqueados por el administrador

Muestra el detalle de los programas bloqueados por Panda Adaptive Defense 360 en los equipos de usuario y servidores.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Ruta	Ruta y nombre del programa bloqueado por el administrador en el equipo del usuario.	Cadena de caracteres
Fecha	Fecha en la que Panda Adaptive Defense 360 bloqueó el programa.	Fecha

Tabla 17.4: Campos del listado Programas bloqueados por el administrador



Para visualizar los datos del listado gráficamente accede al widget **"Programas bloqueados por el administrador"**.

• **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Ruta	Ruta y nombre del programa bloqueado por el administrador en el equipo del usuario.	Cadena de caracteres
Hash	MD5 del programa bloqueado por el administrador.	Cadena de caracteres
Fecha	Fecha en la que Panda Adaptive Defense 360 bloqueó el programa.	Fecha
Usuario logeado	Cuenta de usuario del sistema operativo que lanza el programa bloqueado.	Cadena de caracteres
Acción	Acción ejecutada por Panda Adaptive Defense 360.	Cadena de caracteres "Bloquear"

Tabla 17.5: Campos del fichero exportado Programas bloqueados por el administrador

• **Herramienta de filtrado**

Campo	Descripción	Valores
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fechas	Intervalo de fechas en el que se ha producido el bloqueo del programa.	- Últimas 24 horas - Últimos 7 días - Último mes

Tabla 17.6: Campos de filtrado para el listado Programas bloqueados por el administrador

Paneles / widgets del módulo Bloqueo de programas

Acceso al panel de control

Para acceder al panel de control haz clic en el menú superior **Estado**, panel lateral **Seguridad**.

Permisos requeridos

Permiso	Acceso a Widgets
Visualizar detecciones y amenazas	Programas bloqueados por el administrador

Tabla 17.7: Permisos requeridos para el acceso a los widgets de Programas bloqueados

Programas bloqueados por el administrador

Muestra el número de intentos de ejecución registrados en el parque informático y bloqueados por Panda Adaptive Defense 360 según la configuración establecida por el administrador de la red.

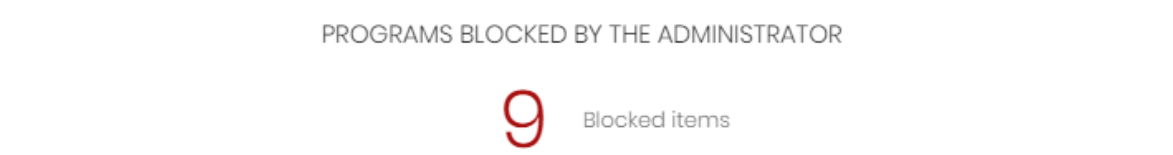


Figura 17.1: Panel Programas bloqueados por el administrador

• Significado de las series

Serie	Descripción
Bloqueados	Número de intentos de ejecución registrados en el parque informático y bloqueados por Panda Adaptive Defense 360 en el intervalo configurado.

Tabla 17.8: Descripción de la serie Programas bloqueados por el administrador

• Filtros preestablecidos desde el panel

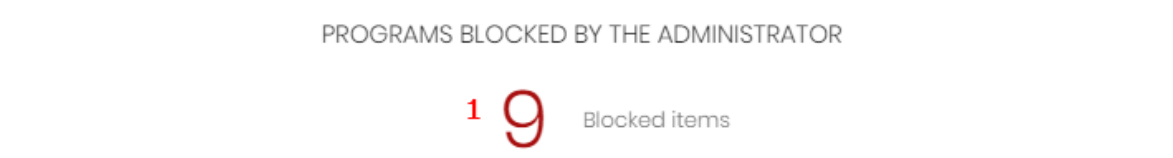


Figura 17.2: Zonas activas del panel Programas bloqueados por el administrador

Al hacer clic en las zonas indicadas en la figura 17.2 se abre el listado **Programas bloqueados por el administrador** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.

Tabla 17.9: Definición de filtros del listado Programas bloqueados por el administrador

Capítulo 18

Configuración de software autorizado

En los modos hardening y lock de la protección avanzada, Panda Adaptive Defense 360 impide la ejecución de los programas desconocidos para la inteligencia de Panda hasta que se completa su clasificación. En casos muy concretos esta funcionalidad puede generar inconvenientes y retrasos menores para el usuario, sobre todo cuando el administrador de la red conoce el origen del programa y la naturaleza de su bloqueo:

- Programas de nicho muy específico y con un número de usuarios muy bajo.
- Programas que se actualizan automáticamente desde la Web del fabricante y sin intervención.
- Programas que distribuyen su funcionalidad a lo largo de cientos de librerías que son cargadas en memoria y, por tanto, bloqueadas conforme el usuario las va utilizando desde los distintos menús del programa.
- Programas que siguen el modelo cliente-servidor, donde la parte del cliente se almacena en un recurso de red compartido.
- Software polimórfico que genera nuevos ficheros ejecutables dinámicamente.



Para obtener información adicional sobre los distintos apartados del módulo Software autorizado consulta las referencias siguientes:

- “[Crear y gestionar configuraciones](#)” en la página [213](#): información sobre crear, modificar, borrar o asignar configuraciones a los equipos de la red.
- “[Control y supervisión de la consola de administración](#)” en la página [67](#): gestión de cuentas de usuario y asignación de permisos.
- “[Protección avanzada](#)” en la página [242](#): configuración de los modos lock y hardening.

CONTENIDO DEL CAPÍTULO

Software autorizado y exclusiones de elementos	404
Configuración de Software autorizado	404
Acceso a la configuración	404
Funcionamiento del módulo Software autorizado	405
Opciones de configuración del módulo Software autorizado	405

Crear una regla de software autorizado	405
Borrar una regla de software autorizado	406
Modificar una regla de software autorizado	406
Copiar una regla de software autorizado	406
Calcular el MD5 de uno o más ficheros	406
Obtener la huella digital sha1 de un programa firmado	407

Software autorizado y exclusiones de elementos

Panda Adaptive Defense 360 permite evitar el bloqueo de programas mediante tres funcionalidades:

- **Mediante Archivos y rutas excluidas del análisis:** evita el análisis de ciertos elementos del equipo. No provoca bloqueos en la ejecución del software desconocido, pero puede suponer un agujero de seguridad y no se recomienda su uso excepto en casos de problemas de rendimiento. Consulta "[Archivos y rutas excluidas del análisis](#)" en la página 241.
- **Desbloqueo de programas en clasificación:** ejecuta temporalmente los programas bloqueados pero tiene un enfoque reactivo: hasta que el programa no ha sido bloqueado, el administrador no puede proceder a su desbloqueo. Dado que un mismo software puede estar formado por varios componentes, y cada uno de ellos requerir un desbloqueo individual, el ciclo de bloqueos y desbloqueos se puede extender a lo largo del tiempo.
- **Configuración de software autorizado:** desbloquea programas desconocidos en clasificación de forma proactiva: el administrador asigna una configuración para aquellos programas de origen conocido que el usuario podrá utilizar siempre que no se detecte ningún peligro. Es el método de desbloqueo recomendado.

Configuración de Software autorizado

Acceso a la configuración

- Haz clic en el menú superior **Configuración**, menú lateral **Software autorizado**.
- Haz clic en el botón **Añadir**, se abrirá la ventana **Añadir configuración**.



Las configuraciones de Software autorizado solo se pueden asignar a puestos de trabajo o servidores Windows.

Permisos requeridos

Permiso	Tipo de acceso
Configurar software autorizado	Crear, modificar, borrar, copiar o asignar las configuraciones de Software autorizado.

Tabla 18.1: Permisos requeridos para acceder a la configuración Software autorizado

Permiso	Tipo de acceso
Ver configuraciones de software autorizado	Visualizar las configuraciones de Software autorizado.

Tabla 18.1: Permisos requeridos para acceder a la configuración Software autorizado

Funcionamiento del módulo Software autorizado

Los usuarios de la red podrán ejecutar el software desconocido que se encuentre en proceso de clasificación siempre que el administrador de la red lo haya permitido mediante una regla de software autorizado.

Cuando el proceso de análisis termine, Panda Adaptive Defense 360 emitirá una clasificación del programa (goodware o malware). Si el programa resulta ser una amenaza, quedará bloqueada su ejecución independientemente de que pertenezca a una configuración de software autorizado.

Opciones de configuración del módulo Software autorizado

Una configuración de software autorizado está formada por una o más reglas, cada una de ellas describe un único software o una familia de programas a los que Panda Adaptive Defense 360 permitirá su ejecución cuando ésta ha sido bloqueada por no conocerse su clasificación.

Crear una regla de software autorizado

Haz clic en el enlace [+](#) **Autorizar programas** para crear una regla con la información mostrada a continuación, y haz clic en el botón **Autorizar**:

Campo	Descripción
Nombre	Nombre de la regla.
MD5	MD5 de los ficheros cuya ejecución permitirá Panda Adaptive Defense 360. Consulta el apartado " Calcular el MD5 de uno o más ficheros ".
Nombre del producto	Es el campo Nombre producto de la cabecera del archivo a desbloquear. Para obtener el valor, haz clic con el botón derecho del ratón en el programa y elige Propiedades, Detalles .
Ruta del archivo	Ruta donde se almacena el programa en el equipo de usuario o servidor. Acepta variables de entorno.
Nombre del archivo	Nombre del archivo. Acepta los comodines * y ?.
Versión del archivo	Es el campo Versión de la cabecera del archivo a desbloquear. Para obtener el valor, haz clic con el botón derecho del ratón en el programa y elige Propiedades, Detalles .
Firma	Es la huella digital sha1 correspondiente a la firma del archivo. Consulta el apartado " Obtener la huella digital sha1 de un programa firmado ".

Tabla 18.2: Configuración de una regla de software autorizado

Borrar una regla de software autorizado

- Haz clic en el icono  situado a la derecha de la regla de software autorizado a borrar.
- Haz clic en el botón **Guardar** situado en la parte superior derecha de la ventana para actualizar la configuración de software autorizado.

Modificar una regla de software autorizado

- Haz clic sobre el nombre de la regla de software autorizado. Se mostrará la ventana **Autorizar programas**.
- Modifica las propiedades de la regla y haz clic en el botón **Autorizar**.
- Haz clic en el botón **Guardar** situado en la parte superior derecha de la ventana. La configuración de software autorizado se actualizará.

Copiar una regla de software autorizado

- Haz clic en el icono  situado a la derecha de la regla de software autorizado a copiar. Se mostrará la ventana **Autorizar programas**. El campo **Nombre** contiene el nombre de la regla con el prefijo "copia de".
- Modifica las propiedades de la regla y haz clic en el botón **Autorizar**.
- Haz clic en el botón **Guardar** situado en la parte superior derecha de la ventana. La configuración de software autorizado se actualizará.

Calcular el MD5 de uno o más ficheros

Existen multitud de herramientas en el mercado que calculan el código MD5 de un fichero. En este apartado se utilizará la herramienta PowerShell incluida en Windows 10.

- Abre la carpeta que contiene los ficheros, haz clic en el menú **Archivo** del explorador y elige **Abrir Windows PowerShell**. Se mostrará una ventana con la línea de comandos.

```
PS C:\Windows> Get-FileHash -Algorithm md5 -path *.*.exe
```

Algorithm	Hash	Path
MD5	B28629E512290B02B36588B39A42B8A4	C:\Windows\bfsvc.exe
MD5	800EF617DDC3C635CD25E20E0EC39CC6	C:\Windows\explorer.exe
MD5	67094590E3D57130C587CD6D8AFB6597	C:\Windows\HelpPane.exe
MD5	DF73D52FDCE65F90A2E49EFB5248C77C	C:\Windows\hh.exe
MD5	06E6C0482562459ADB462CA9008262F8	C:\Windows\notepad.exe
MD5	BD2DF000DAFEE5CF6A9E10B5333C7F3A	C:\Windows\py.exe
MD5	89666526F2188CB3F65622D8AFD9356F	C:\Windows\pyw.exe
MD5	29409008DF22243BB320333F9FD5C060	C:\Windows\regedit.exe
MD5	5B6E47C03F5178388813AB87C27DEF6D	C:\Windows\spWow64.exe
MD5	CAA192BFD85F2A131EBD649B7062DE3	C:\Windows\winhlp32.exe
MD5	1D27F61CC5D659247D2E0C11C5386DE	C:\Windows\write.exe

Figura 18.1: Línea de comandos con el resultado del comando Get-FileHas

- Escribe el siguiente comando y sustituye \$file por la ruta de los ficheros. Se admiten los comodines *

y ?.

```
PS c:\carpeta> Get-FileHash -Algorithm md5 -path $files
```

- Para copiar los códigos MD5 al portapapeles, presiona la tecla **Alt** y sin soltarla, selecciónalos con el ratón. Una vez hecho, pulsa la combinación de teclas **Control + c**.
- Para pegar todos los códigos MD5 desde el portapapeles a la consola de Panda Adaptive Defense 360, haz clic en el campo **MD5** de la regla de software autorizado y pulsa la combinación de teclas **Control + v**.
- Haz clic en el botón **Autorizar** y en el botón **Guardar** situado en la parte superior derecha de la pantalla. La configuración de software autorizado se actualizará.

Obtener la huella digital sha1 de un programa firmado

- Haz clic con el botón derecho del ratón sobre el fichero y elige **Propiedades** en el menú de contexto.
- En la ventana **Propiedades** haz clic en la pestaña **Firmas digitales**.
- Elige en **Lista de firmas** la firma que tenga el campo **Algoritmo implícito** a sha1 y haz clic en el botón **Detalles**. Se mostrará la ventana **Detalles de la firma digital**.
- En la ventana **Detalles de la firma digital**, selecciona la pestaña **General** y haz clic en el botón **Ver certificado**. Se abrirá la ventana **Certificado**.
- En la ventana **Certificado**, haz clic en la pestaña **Ruta de certificación** y comprueba que está seleccionado el último nodo de la ruta de certificación.
- En la ventana **Certificado**, haz clic en la pestaña **Detalles** y selecciona el campo **Huella digital**.
- Selecciona la cadena de caracteres que se muestra en la caja de texto inferior y presiona **Control + c** para copiarla al portapapeles.
- Haz clic en el campo **Firma** de la regla de software autorizado y pulsa la combinación de teclas **Control + v** para pegar la huella digital desde el portapapeles a la consola de Panda Adaptive Defense 360.
- Haz clic en el botón **Autorizar** y en el botón **Guardar** situado en la parte superior derecha de la pantalla. La configuración de software autorizado se actualizará.



Parte 6

Visibilidad y gestión de las amenazas

Capítulo 19: Visibilidad del malware y del parque informático

Capítulo 20: Gestión de amenazas, elementos en clasificación y cuarentena

Capítulo 21: Análisis forense

Capítulo 22: Alertas

Capítulo 23: Envío programado de informes y listados

Capítulo 19

Visibilidad del malware y del parque informático

Panda Adaptive Defense 360 ofrece al administrador tres grandes grupos de herramientas para visualizar el estado de la seguridad y del parque informático que gestiona:

- El panel de control, con información actualizada en tiempo real.
- Listados personalizables de incidencias, malware detectado y dispositivos gestionados junto a su estado.
- Informes con información del estado del parque informático, recogida y consolidada a lo largo del tiempo.



Los informes consolidados se tratan en “[Envío programado de informes y listados](#)” en la [página 513](#).

Las herramientas de visualización y monitorización determinan en tiempo real el estado de la seguridad de la red y el impacto de las brechas de seguridad que se puedan producir para facilitar la adopción de las medidas de seguridad apropiadas.

CONTENIDO DEL CAPÍTULO

Paneles / Widgets del módulo de seguridad	412
Estado de protección	412
Equipos sin conexión	415
Protección desactualizada	416
Actividad de malware / PUP	417
Actividad de exploits	418
Clasificación de todos los programas ejecutados y analizados	419
Amenazas detectadas por el antivirus	420
Filtrado de contenidos en servidores Exchange	423
Accesos a páginas web	424
Categorías más accedidas (top 10)	425
Categorías más accedidas por equipo (top 10)	426
Categorías más bloqueadas (top 10)	427
Categorías más bloqueadas por equipo (Top 10)	428
Listados del módulo de seguridad	428
Estado de protección de los equipos	429

Actividad de malware / PUP 433

Actividad de exploits 436

Amenazas detectadas por el antivirus 439

Dispositivos bloqueados 443

Intentos de intrusión bloqueados 446

Accesos a páginas web por categoría 451

Accesos a páginas web por equipo 452

Paneles / Widgets del módulo de seguridad

Para acceder a los paneles que muestran el estado de la seguridad y a sus listados asociados haz clic en el menú superior **Estado** y en el menú lateral **Seguridad** .

A continuación, se detallan los distintos widgets implementados en el dashboard de Panda Adaptive Defense 360, las distintas áreas y zonas activas incorporadas y los tooltips y su significado.

Estado de protección

Muestra los equipos donde Panda Adaptive Defense 360 funciona correctamente y aquellos con errores y problemas en la instalación o en la ejecución del módulo de protección. El estado de los equipos es representado mediante un círculo con distintos colores y contadores asociados.



La suma de los porcentajes de las diferentes series puede resultar más de un 100% debido a que los estados no son mutuamente excluyentes y un mismo equipo puede encontrarse en varias series a la vez.

El panel representa en porcentaje y de forma gráfica los equipos que comparten un mismo estado.

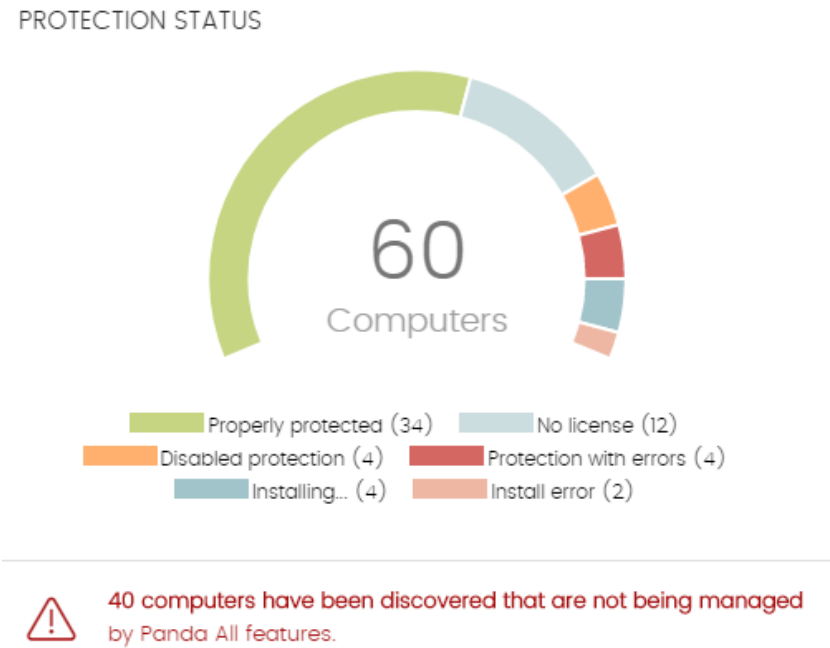


Figura 19.1: Panel de Estado de protección

• Descripción de las series

Serie	Descripción
Correctamente protegido	Porcentaje de equipos en los que Panda Adaptive Defense 360 se instaló sin errores y su ejecución no presenta problemas.
Instalando...	Porcentaje de equipos en los que Panda Adaptive Defense 360 se encuentra en proceso de instalación.
Sin licencia	Equipos sin protección por la falta de suficientes licencias, o por no haberse asignado una licencia disponible.
Protección desactivada	Equipos sin activar la protección antivirus ni la protección avanzada, si ésta última se encuentra disponible para el sistema operativo del equipo en particular.
Protección con error	Equipos con Panda Adaptive Defense 360 instalado cuyo módulo de protección no responde a las peticiones desde los servidores de Panda Security.
Error instalando	Equipos cuya instalación no se pudo completar.
Parte central	Equipos con un agente Panda instalado.

Tabla 19.1: Descripción de la serie Equipos desprotegidos

• Filtros preestablecidos desde el panel

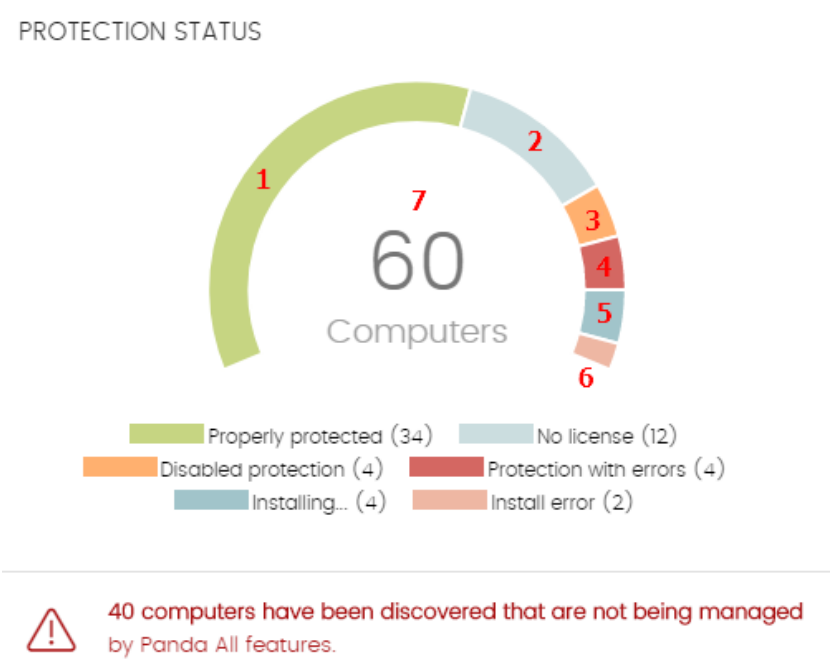


Figura 19.2: Zonas activas del panel Estado de protección

Haz clic en las zonas indicadas en la figura 19.2 para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Estado de protección = Correctamente protegido.
(2)	Estado de protección = Instalando...
(3)	Estado de protección = Protección desactivada.
(4)	Estado de protección = Protección con error.
(5)	Estado de protección = Sin licencia.
(6)	Estado de protección = Error instalando.
(7)	Sin filtro.

Tabla 19.2: Definición de filtros del listado Estado de protección de los equipos

Equipos sin conexión

Muestra los equipos de la red que no han conectado con la nube de Panda Security en un determinado periodo de tiempo. Estos equipos son susceptibles de tener algún tipo de problema y requerirán una atención especial por parte del administrador.



Figura 19.3: Panel Equipos sin conexión

• Descripción de las series

Serie	Descripción
72 horas	Número de equipos que no enviaron su estado en las últimas 72 horas.
7 días	Número de equipos que no enviaron su estado en las últimas 7 días.
30 días	Número de equipos que no enviaron su estado en las últimas 30 días.

Tabla 19.3: Descripción de la serie Equipos sin conexión

• Filtros preestablecidos desde el panel



Figura 19.4: Zonas activas del panel Equipos sin conexión

Haz clic en las zonas indicadas en la figura 19.4 para abrir el listado **Equipos sin conexión** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Última conexión = Hace más de 72 horas.
(2)	Última conexión = Hace más de 7 días.
(3)	Última conexión = Hace más de 30 días.

Tabla 19.4: Definición de los filtros del listado Equipos sin conexión

Protección desactualizada

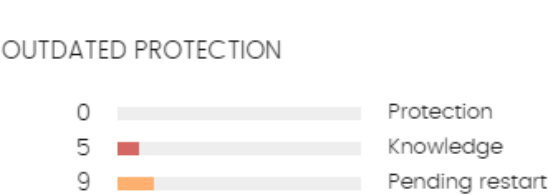


Figura 19.5: Panel Protección desactualizada

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.

• Descripción de las series

El panel muestra el porcentaje y el número de equipos vulnerables por estar desactualizados, divididos en tres conceptos:

Serie	Descripción
Protección	Desde hace 7 días el equipo tiene un motor de protección instalado anterior a la última versión publicada por Panda Security.
Conocimiento	Desde hace 3 días el equipo no se actualiza con el fichero de firmas publicado.
Pendiente de reinicio	El equipo requiere un reinicio para completar la actualización.

Tabla 19.5: Descripción de la serie Protección desactualizada

• Filtros preestablecidos desde el panel

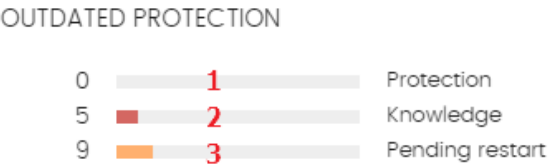


Figura 19.6: Zonas activas del panel Protección desactualizada

Haz clic en las zonas indicadas en la figura 19.6 para abrir el listado **Estado de protección de los equipos** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Protección actualizada = No.
(2)	Conocimiento = No.
(3)	Protección actualizada = Pendiente de reinicio.

Tabla 19.6: Definición de los filtros del listado Equipos con protección desactualizada

Actividad de malware / PUP

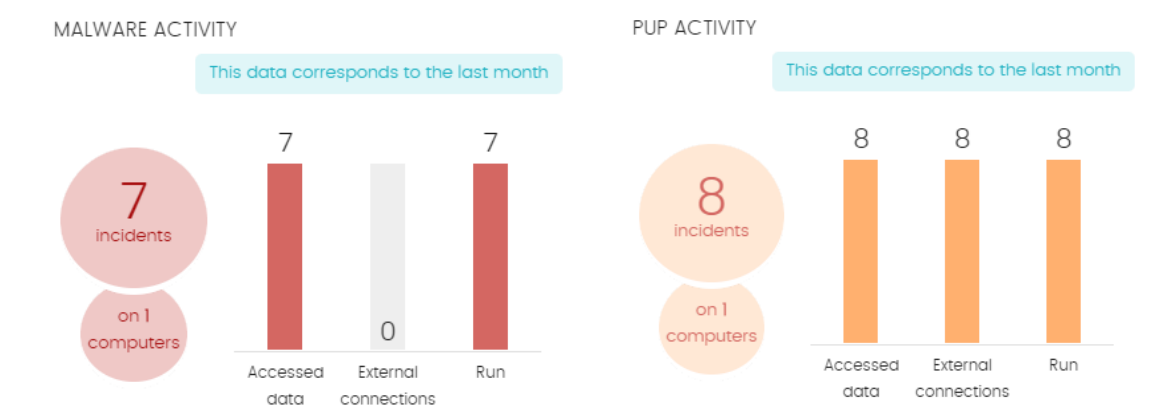


Figura 19.7: Panel de Actividad de malware / PUP

Muestra las incidencias detectadas en los procesos ejecutados por los equipos de usuario y servidores Windows, así como en sus sistemas de ficheros. Estas incidencias son reportadas tanto por el análisis en tiempo real como por las tareas de análisis bajo demanda.

Panda Adaptive Defense 360 genera una incidencia en el panel Actividad de malware / PUP atendiendo a las siguientes reglas:

- Por cada pareja equipo - amenaza - tipo de amenaza distinta encontrada en la red.
- Solo se registra la primera incidencia si se repite varias veces en los primeros 5 minutos.
- Una misma incidencia se registra como máximo 2 veces cada 24 horas.

Descripción de las series

Serie	Descripción
Número de incidencias	Número de incidencias / avisos en Número de equipos detectadas.
Acceso a datos	Número de avisos que incluyen uno o varios accesos a información del usuario contenida en el disco duro de su equipo.
Conexiones exteriores	Número de avisos que establecieron conexiones con otros equipos.
Ejecutado	Número de muestras malware que se llegaron a ejecutar.

Tabla 19.7: Descripción de la serie Actividad de malware / PUP



Actividad de malware, Actividad de PUPs y Actividad de exploits muestran datos con un intervalo máximo de 1 mes. En el caso de que el administrador establezca un periodo de tiempo mayor se mostrará un texto explicativo en la parte superior del panel.

• Filtros preestablecidos desde el panel

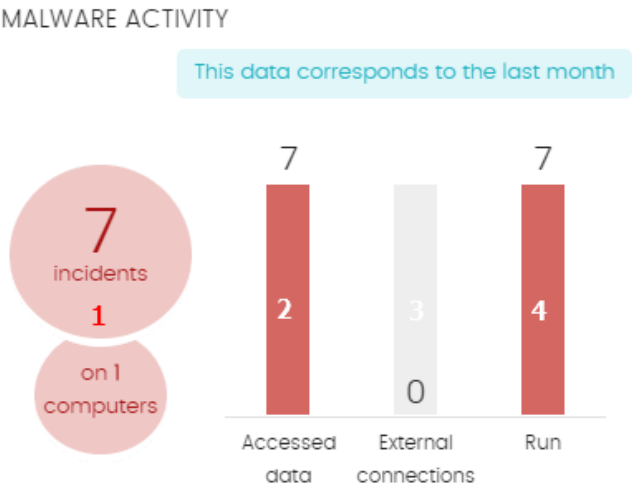


Figura 19.8: Zonas activas del panel Actividad de malware / PUP

Haz clic en las zonas indicadas en la figura 19.8 para abrir el listado **Actividad del malware y PUPs** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Tipo de amenaza = (Malware O PUP).
(2)	Acceso a datos = Verdadero.
(3)	Conexiones externas = Verdadero.
(4)	Ejecutado = Verdadero.

Tabla 19.8: Definición de los filtros del listado Actividad de malware / PUP

Actividad de exploits

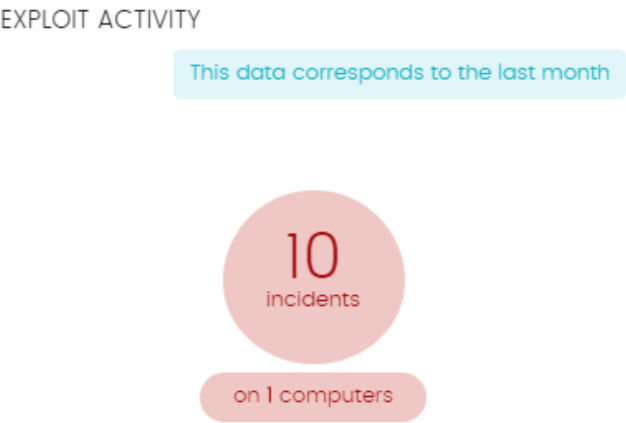


Figura 19.9: Panel de Actividad de exploits

Muestra el número de ataques por explotación de vulnerabilidades recibidos en los equipos Windows de la red. Panda Adaptive Defense 360 genera una incidencia en el panel Actividad de exploits por

cada pareja equipo -exploit distinto encontrada en la red. Si el ataque se repite, se generarán un máximo de 10 incidencias cada 24 horas por cada equipo - exploit encontrado.

- **Descripción de las series**

Serie	Descripción
Número de incidencias / ataques	Número de incidencias / ataques en Número de equipos detectadas.

Tabla 19.9: Descripción de la serie Actividad de exploits

- **Filtros preestablecidos desde el panel**

Al hacer clic en cualquier zona del widget se mostrará el listado **Actividad de exploits** filtrado por el último mes.

Clasificación de todos los programas ejecutados y analizados

CLASSIFICATION OF ALL PROGRAMS RUN AND SCANNED



Figura 19.10: Panel de Clasificación de todos los programas ejecutados y analizados

Localiza de forma rápida el porcentaje de aplicaciones goodware y malware vistas y clasificadas en la red del cliente, para el intervalo de tiempo establecido por el administrador.

- **Descripción de las series**

El panel consta de cuatro barras horizontales junto al número de eventos asociado y el porcentaje sobre el total.



Este panel muestra datos de elementos clasificados para todo el parque informático, y no solo de aquellos equipos sobre los cuales el administrador tenga permisos según sus credenciales de acceso a la consola. Los elementos no clasificados no se muestran en este panel.

Serie	Descripción
Aplicaciones confiables	Aplicaciones vistas en el parque del cliente que han sido analizadas y su clasificación ha sido goodware.
Aplicaciones maliciosas	Programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware o ataques dirigidos.

Tabla 19.10: Descripción de la serie Clasificación de todos los programas ejecutados y analizados

Serie	Descripción
Exploits	Número de intentos de explotación de aplicaciones detectados en la red.
Aplicaciones potencialmente no deseadas	Programas que han intentado ejecutarse o han sido analizados en el parque del cliente, y han sido clasificadas como malware de tipo PUP.

Tabla 19.10: Descripción de la serie Clasificación de todos los programas ejecutados y analizados

• Filtros preestablecidos desde el panel

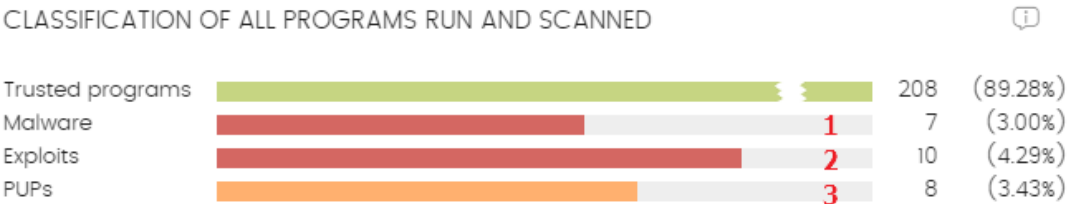


Figura 19.11: Zonas activas del panel Clasificación de todos los programas ejecutados y analizados

Haz clic en las zonas indicadas en la figura 19.11 para abrir diferentes listados sin filtros preestablecidos:

Zona activa	Filtro
(1)	Listado Actividad del malware.
(2)	Listado Actividad de exploit.
(3)	Listado Actividad de PUPs.

Tabla 19.11: Listados accesibles desde el panel Clasificación de todos los programas ejecutados y analizados

Amenazas detectadas por el antivirus

Consolida todos los intentos de intrusión que Panda Adaptive Defense 360 gestionó en el periodo de tiempo establecido.

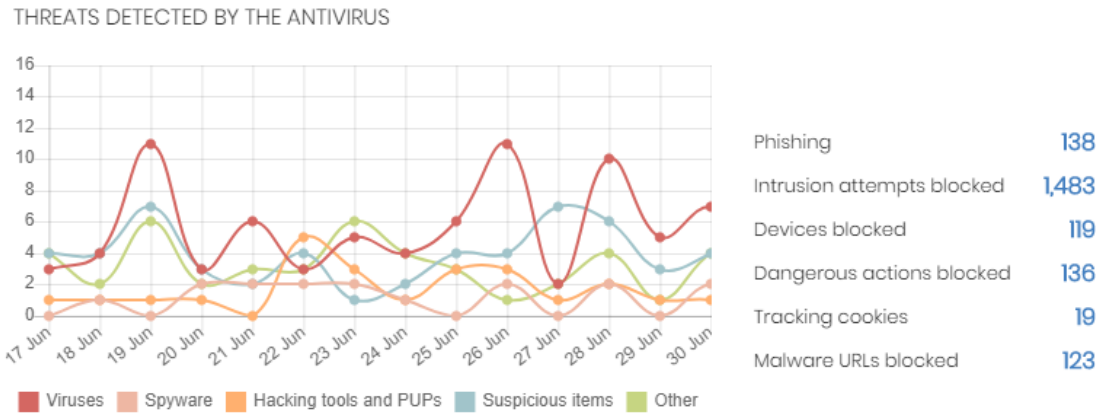


Figura 19.12: Panel Amenazas detectadas por el antivirus

Los datos reflejados abarcan todos los vectores de infección y todas las plataformas soportadas, de manera que el administrador pueda disponer de información concreta (volumen, tipo, forma de ataque) relativa a la llegada de malware a la red, durante el intervalo de tiempo determinado.

- **Descripción de las series**

Este panel está formado por dos secciones: un gráfico de líneas y un listado resumen.

El diagrama de líneas representa las detecciones encontradas en el parque informático a lo largo del tiempo separadas por tipo de malware:

Serie	Descripción
Virus y spyware	Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.
Herramientas de hacking y PUPs	Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.
Sospechosos	Programa que, tras un análisis de su comportamiento realizado en el equipo del usuario por la protección de Panda Adaptive Defense 360, tiene una alta probabilidad de ser considerado malware.
Phishing	Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito o cuentas bancarias.
Otros	Hoax, Worms, Troyanos y otros tipos de virus.

Tabla 19.12: Descripción de la serie Amenazas detectadas por el antivirus

El listado de la derecha muestra los eventos relevantes que requieren una supervisión por parte del administrador en busca de síntomas o situaciones potenciales de peligro.

Serie	Descripción
Acciones peligrosas bloqueadas	Detecciones realizadas por análisis del comportamiento local.
Intentos de intrusión bloqueados	Detección de tráfico de red mal formado cuyo objetivo es provocar un error de ejecución en algún componente del equipo que origine un comportamiento indeseado en el sistema.
Dispositivos bloqueados	Intento de uso por parte del usuario del equipo de un dispositivo restringido según la configuración establecida por el administrador de la red en el módulo Control de dispositivos.
Tracking cookies	Cookies detectadas para registrar la navegación de los usuarios.
URL con malware bloqueadas	Direcciones Web que apuntaban a páginas con malware.

Tabla 19.13: Descripción de la serie Amenazas detectadas por el antivirus

• Filtros preestablecidos desde el panel

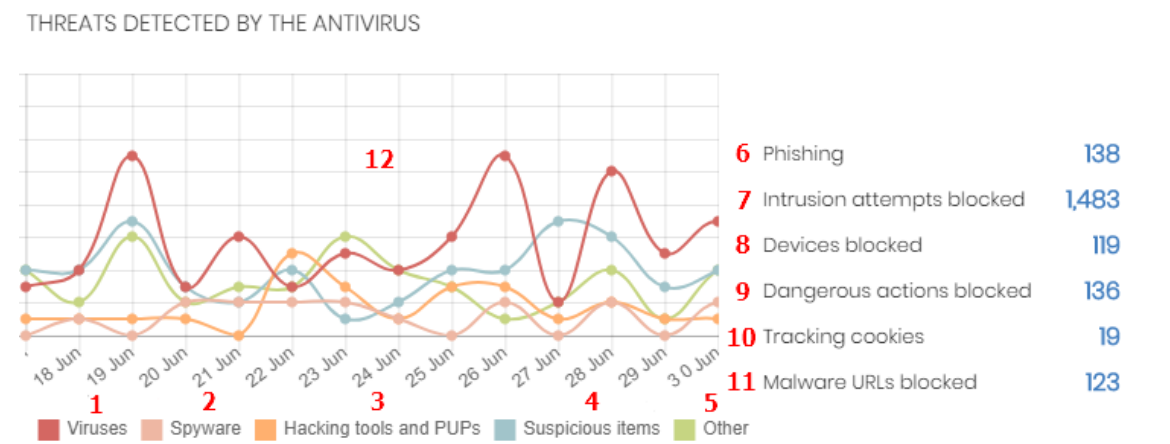


Figura 19.13: Zonas activas del paneyl Amenazas detectadas por el antivirus

Haz clic en las zonas indicadas en la figura 19.13 para abrir el listado con los filtros preestablecidos mostrados a continuación:

Zona activa	Listado	Filtro
(1)	Amenazas detectadas por el antivirus	Tipo de amenaza = Virus.
(2)	Amenazas detectadas por el antivirus	Tipo de amenaza = Spyware.
(3)	Amenazas detectadas por el antivirus	Tipo de amenaza = Herramientas de hacking y PUPs.
(4)	Amenazas detectadas por el antivirus	Tipo de amenaza = Sospechosos.
(5)	Amenazas detectadas por el antivirus	Tipo de amenaza = Otros.
(6)	Amenazas detectadas por el antivirus	Tipo de amenaza = Phishing.
(7)	Intentos de intrusión bloqueados	Sin filtro.
(8)	Dispositivos bloqueados	Sin filtro.
(9)	Amenazas detectadas por el antivirus	Tipo de amenaza = Acciones peligrosas bloqueadas.
(10)	Amenazas detectadas por el antivirus	Tipo de amenaza = Tracking cookies.
(11)	Amenazas detectadas por el antivirus	Tipo de amenaza = URLs con malware.
(12)	Amenazas detectadas por el antivirus	Sin filtro.

Tabla 19.14: Definición de los filtros del listado Amenazas detectadas por el antivirus

Filtrado de contenidos en servidores Exchange

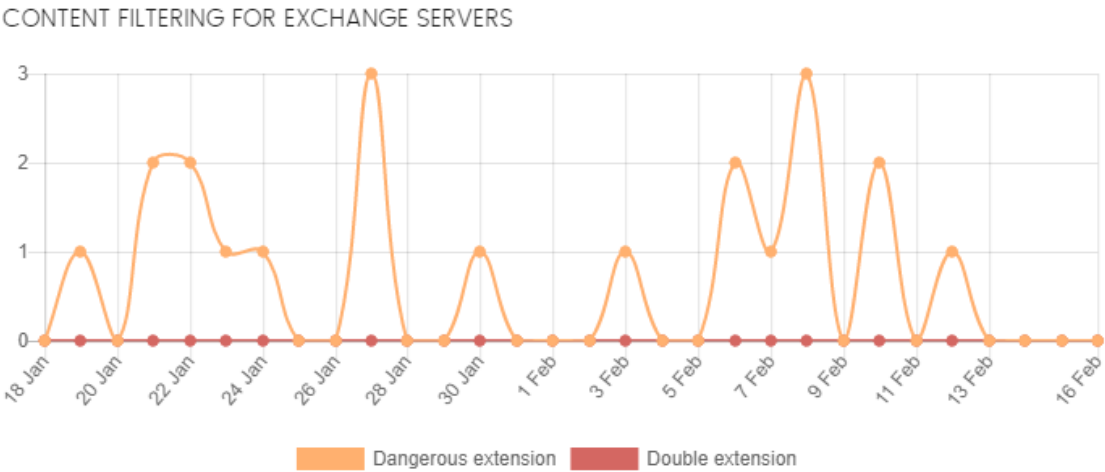


Figura 19.14: Panel Filtrado de contenidos en servidores Exchange

Muestra la cantidad de mensajes que fueron bloqueados por el filtro de contenidos del servidor Exchange.

• Descripción 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.

Al pasar el ratón por las series se muestra un tooltip con la siguiente información:

Serie	Descripción
Extensión peligrosa	Número de mensajes filtrados por contener adjuntos con extensión peligrosa.
Doble extensión	Número de mensajes filtrados por contener adjuntos con doble extensión.

Tabla 19.15: Descripción de la serie Filtrado de contenidos en servidores Exchange

Accesos a páginas web

WEB ACCESS

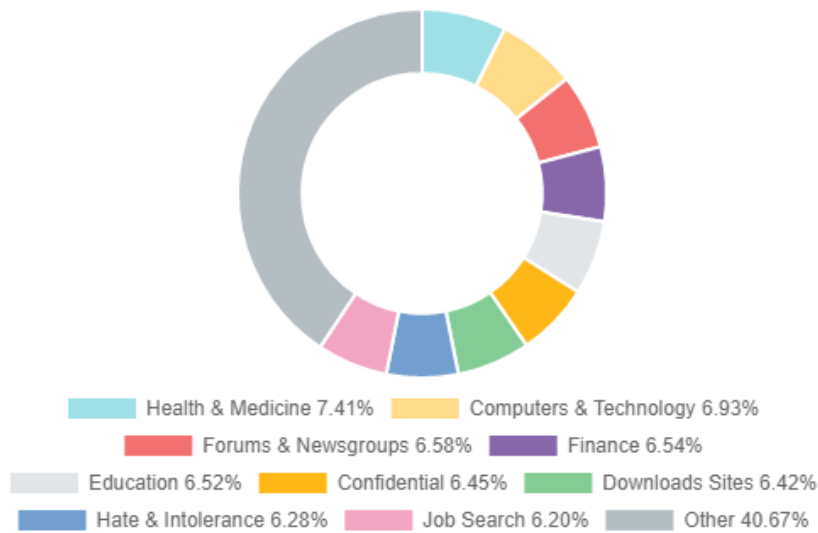


Figura 19.15: Panel Accesos a páginas web

Muestra mediante un gráfico de tarta la distribución de categorías Web solicitadas por los usuarios de la red.

• Descripción de las series

El panel de tipo tarta muestra los 10 grupos de páginas web más importantes que Panda Adaptive Defense 360 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.

- **Filtros preestablecidos desde la tabla**

Haz clic en las categorías mostradas en la figura 19.15 para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
Cualquiera	Categoría = Categoría seleccionada.

Tabla 19.16: Definición de los filtros Accesos a páginas web por equipo

Categorías más accedidas (top 10)

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		

Detalla 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.

Figura 19.16: Panel Categorías más accedidas

- **Filtros preestablecidos desde el panel**

Se muestra el listado **Accesos a páginas web por equipo** con filtros preestablecidos en función del lugar donde el administrador hizo clic dentro de la tabla.

Zona activa	Filtro
Categoría	Categoría = Categoría seleccionada.
Ver informe completo	Muestra el listado Accesos a paginas web por categoría sin filtros.

Tabla 19.17: Definición de los filtros del listado Accesos a páginas web por equipo

Categorías más accedidas por equipo (top 10)

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		

En este panel se detallan el número de accesos ordenados por categorías de los 10 equipos que más han visitado la web.

Figura 19.17: panel Categorías más accedidas por equipo (Top 10)

• Filtros preestablecidos desde el panel

Haz clic en las distintas zonas de la figura 19.17 para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
Equipo	Equipo = Equipo seleccionado.
Categoría	Categoría = Categoría seleccionada.
Ver listado completo	Sin filtro.

Tabla 19.18: Definición de los filtros del listado Accesos a páginas web por equipo

Categorías más bloqueadas (top 10)

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

Indica 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.

[See full report](#)

Figura 19.18: Zonas activas del panel Categorías más bloqueadas

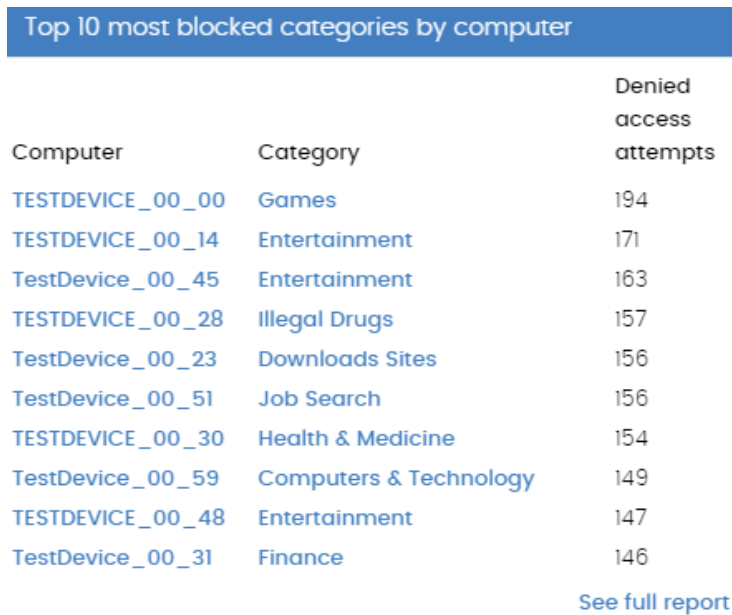
- **Filtros preestablecidos desde el panel**

Haz clic en las distintas zonas de la figura 19.18 para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
Categoría	Categoría = Categoría seleccionada.
Ver listado completo	Muestra el listado Accesos a paginas web por categoría sin filtros.

Tabla 19.19: Definición de los filtros de Accesos a páginas web por equipo

Categorías más bloqueadas por equipo (Top 10)



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.

Figura 19.19: Panel categorías más bloqueadas por equipo (Top 10)

Filtros preestablecidos desde el panel

Haz clic en las distintas zonas de la figura 19.19 para abrir el listado **Accesos a páginas web por equipo** con los filtros preestablecidos mostrados a continuación:

Zona activa		Filtro
Equipo		Nombre de equipo = Equipo.
Categoría		Categoría = categoría seleccionada.
Ver listado completo		Sin filtro.

Tabla 19.20: Definición de los filtros de Accesos a páginas web por equipo

Listados del módulo de seguridad

Los listados de seguridad muestran la información de la actividad relativa a la protección de los equipos de la red recogida por Panda Adaptive Defense 360, y cuentan con un grado de detalle muy alto al contener la información en bruto utilizada para generar los widgets.

Para acceder a los listados de seguridad elige uno de los dos procedimientos mostrados a continuación:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad** y en widget para abrir su listado asociado. Dependiendo del lugar donde se haga clic dentro del widget se aplicará un filtro distinto asociado al listado.

o

- En el menú superior **Estado**, panel lateral **Mis listados** haz clic en el enlace **Añadir**. Se mostrará una ventana donde se muestran todos los listados disponibles en Panda Adaptive Defense 360.
- Haz clic en un listado de la sección **Seguridad**. Se mostrará el listado apropiado sin filtros establecidos.

Al hacer clic en una entrada del listado se mostrará la ventana de detalle, que se ajustará al tipo de información mostrada.

Estado de protección de los equipos

Muestra en detalle todos los equipos de la red, incorporando filtros que permiten localizar aquellos puestos de trabajo o dispositivos móviles que no estén protegidos por alguno de los conceptos mostrados en el panel asociado.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	• Cadena de caracteres •  Grupo Todos •  Grupo nativo •  Grupo Directorio activo
Protección avanzada	Estado de la protección avanzada.	•  Instalando •  Error. Si es conocido se mostrará su origen, si es desconocido se mostrará el código de error •  Activado •  Desactivado •  Sin licencia
Antivirus	Estado de la protección antivirus	•  Instalando •  Error. Si es conocido se mostrará su origen, si es desconocido se mostrará el código de error •  Activado •  Desactivado •  Sin licencia

Tabla 19.21: Campos del listado Estado de protección de los equipos

Campo	Descripción	Valores
Protección actualizada	El módulo de la protección instalado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se muestra la versión de la protección instalada.	• Actualizado • No actualizado (7 días sin actualizar desde la publicación) • Pendiente de reinicio.
Conocimiento	El fichero de firmas descargado en el equipo coincide con la última versión publicada o no. Al pasar el puntero del ratón por encima del campo se muestra la fecha de actualización de la versión descargada.	• Actualizado • No actualizado (3 días sin actualizar desde la publicación)
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	Fecha

Tabla 19.21: Campos del listado Estado de protección de los equipos

• **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Versión del agente	Versión interna del módulo agente Panda.	Cadena de caracteres
Fecha instalación	Fecha en la que el Software Panda Adaptive Defense 360 se instaló con éxito en el equipo.	Fecha

Tabla 19.22: Campos del fichero exportado Estado de protección de los equipos

Campo	Descripción	Valores
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
Protección actualizada	El módulo de la protección instalado en el equipo es la última versión publicada.	Binario
Versión de la protección	Versión interna del módulo de protección.	Cadena de caracteres
Conocimiento actualizado	El fichero de firmas descargado en el equipo es la última versión publicada.	Binario
Fecha de última actualización	Fecha de la descarga del fichero de firmas.	Fecha
Protección avanzada Antivirus de archivos Antivirus de correo Antivirus para navegación web FirewallControl de dispositivos Control de acceso a páginas web Antivirus para servidores Exchange Anti-spam para servidores Exchange Filtrado de contenidos para servidores Exchange	Estado de la protección asociada.	• No instalado • Error: si es conocido se mostrará su origen, si es desconocido se mostrará el código de error • Activado • Desactivado • Sin licencia
Estado de aislamiento	El equipo esta aislado de la red.	• Aislado • No aislado
Fecha de error	Se produjo un error en la instalación de Panda Adaptive Defense 360 en la fecha y hora indicadas.	Fecha
Error instalación	Descripción del error producido en la instalación de Panda Adaptive Defense 360 en el equipo.	Cadena de caracteres

Tabla 19.22: Campos del fichero exportado Estado de protección de los equipos

Campo	Descripción	Valores
Código error instalación	Muestra código que permite detallar el error producido durante la instalación.	Los códigos se muestran separados por “;”: • Código de error • Código extendido error • Subcódigo extendido error
Otros productos de seguridad	Nombre del antivirus de terceros fabricantes encontrado en el equipo en el momento de la instalación de Panda Adaptive Defense 360.	Cadena de caracteres

Tabla 19.22: Campos del fichero exportado Estado de protección de los equipos

• **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Servidor • Dispositivo móvil
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Última conexión	Fecha del último envío del estado de Panda Adaptive Defense 360 a la nube de Panda Security.	• Todos • Hace menos de 24 horas • Hace menos de 3 días • Hace menos de 7 días • Hace menos de 30 días • Hace más de 3 días • Hace más de 7 días • Hace más de 30 días
Protección actualizada	La protección instalada coincide con la última versión publicada o no.	• Todos • Si • No • Pendiente de reinicio
Plataforma	Sistema operativo instalado en el equipo.	• Todos • Windows • Linux • macOS • Android

Tabla 19.23: Campos de filtrado para el listado Estado de protección de los equipos

Campo	Descripción	Valores
Conocimiento	Indica si el fichero de firmas encontrado en el equipo es o no el último publicado.	Binario
Estado de protección	Estado del módulo de protección instalado en el equipo.	• Instalando... • Correctamente protegido • Protección con error • Protección desactivada • Sin licencia • Error instalando
Estado de aislamiento	Configuración del aislamiento del equipo.	• No aislado • Aislado • Aislando • Dejando de aislar

Tabla 19.23: Campos de filtrado para el listado Estado de protección de los equipos

• Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta ["Información de equipo"](#) en la página 189 para obtener más información.

Actividad de malware / PUP

Muestra el listado de las amenazas encontradas en los equipos protegidos con Panda Adaptive Defense 360. Este detalle es necesario para poder localizar el origen de los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado.	Cadena de caracteres
Ejecutado alguna vez	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Ha accedido a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Se ha comunicado con equipos externos	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario

Tabla 19.24: Campos del listado de Actividad del malware / PUP

Campo	Comentario	Valores
Acción	Acción aplicada sobre el malware.	• Movido a cuarentena • Bloqueado • Desinfectado • Eliminado • Detectado
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha

Tabla 19.24: Campos del listado de Actividad del malware / PUP

• **Campos mostrados en fichero exportado**



En el menú de contexto de Listado de actividad Malware / PUP se muestra un desplegable con dos entradas diferentes: Exportar y Exportar listado y detalles. En este apartado se muestra el contenido de Exportar. Para obtener información sobre Exportar listado y detalles consulta “[Ficheros exportados Excel](#)” en la página 496

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Amenaza	Nombre de la amenaza detectada.	Cadena de caracteres
Ruta	Ruta completa donde reside el fichero infectado.	Cadena de caracteres
Acción	Acción aplicada sobre el malware.	• Movido a cuarentena • Bloqueado • Desinfectado • Eliminado • Permitido
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario
Excluido	La amenaza ha sido excluida por el administrador para permitir su ejecución.	Binario
Fecha	Fecha de la detección de la amenaza en el equipo.	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar.	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual la amenaza se ha ejecutado.	Cadena de caracteres

Campo	Comentario	Valores
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Equipo origen de la infección	Nombre del equipo si el intento de infección viene de un equipo de la red del cliente.	Cadena de caracteres
IP origen de la infección	Dirección IP del equipo si el intento de infección viene de un equipo de la red del cliente.	Cadena de caracteres
Usuario origen de la infección	Usuario registrado en la máquina origen de la infección.	Cadena de caracteres

Tabla 19.25: Campos del fichero exportado Actividad del malware / PUP

• **Herramienta de filtrado**

Campo	Comentario	Valores
Buscar	• Equipo: dispositivo donde se realizó la detección. • Amenaza: nombre de la amenaza. • Hash: Cadena resumen de identificación del archivo. • Origen de la infección: busca por el usuario, la IP o el nombre del equipo origen del fichero infectado.	Cadena de caracteres
Tipo	Tipo de amenaza a mostrar.	• Malware • PUP
Fechas	Establece un intervalo de fechas desde el día presente hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año
Ejecutado	La amenaza se llegó a ejecutar y el equipo puede estar comprometido.	Binario
Acción	Acción aplicada sobre la amenaza.	• Movid a cuarentena • Bloqueado • Desinfectado • Eliminado • Permitido
Acceso a datos	La amenaza ha accedido a datos que residen en el equipo del usuario.	Binario
Conexiones externas	La amenaza se comunica con equipos remotos para enviar o recibir datos.	Binario

Tabla 19.26: Campos de filtrado para el listado Actividad del malware / PUP

• **Ventana de detalle**

Muestra información detallada del programa clasificado como malware / PUP. Consulta "[Detección del malware](#)" en la página [482](#).

Actividad de exploits

Muestra el listado de equipos con programas comprometidos por intentos de explotación de vulnerabilidades. Este detalle es necesario para poder localizar el origen los problemas, determinar la gravedad de las incidencias y, si procede, tomar las medidas necesarias de resolución y de actualización de la política de seguridad de la compañía.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Programa comprometido	Programa que recibió el ataque de tipo exploit.	Cadena de caracteres
Técnica de exploit	Identificador de la técnica utilizada para explotar las vulnerabilidades de los programas.	Cadena de caracteres
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Acción	• Permitido: la protección anti-exploit está configurada en modo "Auditar". El exploit se ejecutó. • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose. • Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. • Pendiente de reinicio: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando.	Enumeración
Fecha	Fecha de la detección del intento de exploit en el equipo.	Fecha

Tabla 19.27: Campos del listado de Actividad de exploits

• **Campos mostrados en fichero exportado**



En el menú de contexto de Actividad de exploits se muestra un desplegable con dos entradas diferentes: Exportar y Exportar listado y detalles. En este apartado se muestra el contenido de Exportar. Para obtener información sobre Exportar listado y detalles consulta “[Ficheros exportados Excel](#)” en la página 496

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se ha detectado a la amenaza.	Cadena de caracteres
Programa comprometido	Programa que recibió el ataque de tipo exploit.	Cadena de caracteres
Técnica de exploit	Identificador de la técnica utilizada para explotar las vulnerabilidades de los programas.	Enumeración
Usuario	Cuenta de usuario bajo la cual se ejecutaba el programa que recibió el exploit.	Cadena de caracteres
Acción	• Permitido: la protección anti-exploit está configurada en modo “Auditar”. El exploit se ejecutó. • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose. • Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. • Pendiente de reinicio: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando.	Enumeración
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Fecha	Fecha de la detección del intento de exploit en el equipo.	Fecha

Tabla 19.28: Campos del fichero exportado Actividad de exploits

- **Herramienta de búsqueda**

Campo	Comentario	Valores
Buscar	• Equipo: dispositivo donde se realizó la detección. • Hash: Cadena resumen de identificación del programa comprometido. • Programa comprometido: nombre del fichero comprometido o de su ruta.	Enumeración
Fechas	Intervalo de fechas desde el día presente hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes
Exploit ejecutado	El exploit se llegó a ejecutar o fue bloqueado antes de afectar al programa vulnerable.	Binario
Acción	• Permitido: la protección anti-exploit está configurada en modo "Auditar". El exploit se ejecutó. • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continuara ejecutándose. • Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. • Pendiente de reinicio: se informó al usuario de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto éste se seguirá ejecutando.	Enumeración

Tabla 19.29: Campos de filtrado para el listado Actividad de exploits

- **Ventana de detalle**

Muestra información detallada del programa clasificado como exploit. Consulta "[Detección exploit](#)" en la página [485](#).

Amenazas detectadas por el antivirus

El listado de detecciones ofrece información consolidada y completa de todas las detecciones realizadas en todas las plataformas soportadas y desde todos los vectores de infección analizados, utilizados por los hackers para intentar infectar equipos en la red.

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	- Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
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.
Ruta	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Acción	Acción desencadenada por Panda Adaptive Defense 360.	- Borrado - Desinfectado - En cuarentena - Bloqueado - Proceso terminado
Fecha	Fecha de la detección.	Fecha

Tabla 19.30: Campos del listado Amenazas detectadas por el antivirus

• Campos mostrados en fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres

Tabla 19.31: Campos del fichero exportado Amenazas detectadas por el antivirus

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Nombre malware	Nombre de la amenaza detectada.	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza detectada.	• Virus • 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 Panda Adaptive Defense 360 detectó la amenaza en el equipo y en la fecha indicada.	Numérico
Acción	Acción desencadenada por Panda Adaptive Defense 360.	• Movido a cuarentena • Borrado • Bloqueado • Proceso terminado
Detectado por	Motor que detectó la amenaza.	• Control de dispositivos • Protección de Antispam para Exchange • Protección de Contenido para Exchange • Protección de Buzones para Exchange • Protección de Transporte para Exchange • Protección de ficheros

Tabla 19.31: Campos del fichero exportado Amenazas detectadas por el antivirus

Campo	Descripción	Valores
		• Firewall • Protección de correo • Protección avanzada • Análisis bajo demanda • Control de acceso Web • Protección Web
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Excluido	La amenaza ha sido excluida del análisis por el administrador para permitir su ejecución.	Binario
Fecha	Fecha de la detección.	Fecha
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo donde se realizó la detección.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador de la red.	Cadena de caracteres

Tabla 19.31: Campos del fichero exportado Amenazas detectadas por el antivirus

• **Herramienta de filtrado**

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Fechas	• Rango: establece un intervalo de fechas desde el día presente hacia el pasado. • Rango personalizado: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Tipo de Amenazas	Clase de amenaza.	• Virus • Spyware • Herramientas de hacking y PUPs • Phishing

Tabla 19.32: Campos de filtrado para el listado Amenazas detectadas por el antivirus

Campo	Descripción	Valores
		- Sospechosos - Acciones peligrosas bloqueadas - Tracking cookies - URLs con malware - Otros

Tabla 19.32: Campos de filtrado para el listado Amenazas detectadas por el antivirus

• **Ventana de detalle**

Muestra información detallada del virus detectado.

Campo	Descripción	Valores
Amenaza	Nombre de la amenaza.	Cadena de caracteres
Acción	Acción que ejecutó Panda Adaptive Defense 360.	- Movido a cuarentena - Borrado - Bloqueado - Proceso terminado
Equipo	Nombre del equipo donde se realizó la detección. Incluye un enlace a la ventana Detalles del equipo	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Servidor - Dispositivo móvil
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.	Cadena de caracteres
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.	Cadena de caracteres
Nombre	Nombre de la amenaza.	Cadena de caracteres
Tipo de amenaza	Clase de la amenaza.	Cadena de caracteres
Tipo de malware	Clase de malware.	- Virus - Spyware - Herramientas de hacking y PUPs - Phishing

Tabla 19.33: Detalle del listado de Amenazas detectadas por el antivirus

Campo	Descripción	Valores
		- Sospechosos - Acciones peligrosas bloqueadas - Tracking cookies - URLs con malware - Otros.
Detectado por	Módulo que realizó la detección.	
Fecha	Fecha de la detección.	Fecha

Tabla 19.33: Detalle del listado de Amenazas detectadas por el antivirus

Dispositivos bloqueados

Este listado muestra en detalle todos los equipos de la red que tienen limitado el acceso a alguno de los periféricos conectados.

Campo	Descripción	Valores
Equipo	Nombre del equipo desprotegido.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	- Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
Nombre	Nombre que el administrador asigna de forma manual al dispositivo para facilitar su identificación.	Cadena de caracteres
Tipo	Familia del dispositivo afectado por la configuración de seguridad.	- Unidades de almacenamiento extraíbles - Dispositivos de captura de imágenes - Unidades de CD/DVD - Dispositivos Bluetooth - 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 19.34: Campos del listado Dispositivos bloqueados

• **Campos mostrados en fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Nombre original	Nombre del periférico conectado al equipo y afectado por la configuración de seguridad.	Cadena de caracteres
Nombre	Nombre asignado al dispositivo por el administrador.	Cadena de caracteres
Tipo	Clase de dispositivo.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Id. de instancia	Identificador del dispositivo afectado.	Cadena de caracteres
Número de detecciones	Número de veces que se detectó una operación no permitida sobre el dispositivo.	Numérico
Acción	Tipo de acción efectuada sobre el dispositivo.	• Bloquear • Permitir Lectura • Permitir Lectura y escritura
Detectado por	Módulo que detectó la operación no permitida.	Control de dispositivos
Fecha	Fecha en la se detectó la operación no permitida.	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 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

Tabla 19.35: Campos del fichero exportado Dispositivos bloqueados

Campo	Descripción	Valores
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 19.35: Campos del fichero exportado Dispositivos bloqueados

• **Herramienta de filtrado**

Campo	Descripción	Valores
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Buscar equipo	Nombre del equipo.	Cadena de caracteres
Fechas	• Rango: establece un intervalo de fechas desde el día presente hacia el pasado. • Rango personalizado: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Tipo de dispositivo	Familia del dispositivo afectado por la configuración de seguridad.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Nombre	Nombre del dispositivo.	Cadena de caracteres

Tabla 19.36: Campos de filtrado para el listado Dispositivos bloqueados

• **Ventana de detalle**

Muestra información detallada del dispositivo bloqueado.

Campo	Descripción	Valores
Dispositivo	Nombre del dispositivo bloqueado.	Cadena de caracteres
Acción	Acción que ejecutó Panda Adaptive Defense 360.	• Movido a cuarentena • Borrado • Bloqueado • Proceso terminado
Equipo	Nombre del equipo donde se realizó el bloqueo del dispositivo.	Cadena de caracteres

Tabla 19.37: Detalle del listado Dispositivos bloqueados

Campo	Descripción	Valores
Tipo de equipo	Clase del equipo.	• Estación • Portátil • Servidor • Dispositivo móvil
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Nombre original	Nombre del dispositivo bloqueado.	Cadena de caracteres
Nombre	Nombre asignado por el administrador al dispositivo. Se puede modificar al hacer clic en el icono 	Cadena de caracteres
Tipo de dispositivo	Categoría del dispositivo.	• Unidades de almacenamiento extraíbles • Dispositivos de captura de imágenes • Unidades de CD/DVD • Dispositivos Bluetooth • Módems • Dispositivos móviles
Id. de instancia	Identificador del dispositivo afectado.	Cadena de caracteres
Bloqueado por	Módulo que realizó la detección.	Control de dispositivos
Número de detecciones	Número de bloqueos detectados.	Numérico
Fecha	Fecha de la detección.	Fecha

Tabla 19.37: Detalle del listado Dispositivos bloqueados

Intentos de intrusión bloqueados

Este listado muestra los ataques de red recibidos por los equipos y bloqueados por el módulo de cortafuegos.

Campo	Descripción	Valores
Equipo	Nombre del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP	Dirección IP del interface red principal del equipo que recibió el ataque de red.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres

Tabla 19.38: Campos del listado Intentos de intrusión bloqueados

Campo	Descripción	Valores
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta "Bloquear intrusiones" en la página 253 para obtener más información acerca de cada uno de los ataques enumerados.	• Todos los intentos de intrusión • ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit pathLand attack • Smart DNS • ICMP filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Fecha	Fecha y hora en la que Panda Adaptive Defense 360 registró el ataque en el equipo.	Fecha

Tabla 19.38: Campos del listado Intentos de intrusión bloqueados

• **Campos mostrados en el fichero exportado**

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	Cadena de caracteres
Equipo	Nombre del equipo que recibió el ataque de red.	Cadena de caracteres
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta "Bloquear intrusiones" en la página 253 para obtener más información acerca de cada uno de los ataques enumerados.	• ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit path • Land attack • Smart DNS

Tabla 19.39: Campos del fichero exportado Intentos de intrusión bloqueados

Campo	Descripción	Valores
		• ICM filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Dirección IP local	Dirección IP del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP remota	Dirección IP del equipo que inició el ataque de red.	Cadena de caracteres
MAC remota	Dirección física del equipo que inició el ataque de red, siempre que se encuentre en el mismo segmento de red que el equipo que recibió el ataque.	Cadena de caracteres
Puerto Local	Si el ataque es TCP o UDP indica el puerto donde se recibió el intento de intrusión.	Numérico
Puerto remoto	Si el ataque es TCP o UDP indica el puerto desde donde se envió el intento de intrusión.	Numérico
Número de detecciones	Número de intentos de intrusión del mismo tipo recibidos.	Numérico
Acción	Acción ejecutada por el cortafuegos según su configuración. Consulta " Firewall (Equipos Windows) " en la página 247.	Bloquear
Detectado por	Motor de detección que realizó la detección del ataque de red.	Firewall
Fecha	Fecha en la que se registró el ataque de red.	Fecha
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP del interface red principal del equipo que recibió el ataque de red.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 19.39: Campos del fichero exportado Intentos de intrusión bloqueados

- **Herramienta de filtrado**

Campo	Descripción	Valores
Fechas	• Rango: establece un intervalo de fechas desde el día presente hacia el pasado. • Rango personalizado: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta " Bloquear intrusiones " en la página 253 para obtener más información acerca de cada uno de los ataques enumerados.	• Todos los intentos de intrusión • ICMP attack • UDP port scan • Header lengths • UDP flood • TCP flags check • Smart WINS • IP explicit pathLand attack • Smart DNS • ICMP filter echo request • OS detection • Smart DHCP • SYN flood • Smart ARP • TCP port scan
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor

Tabla 19.40: Campos de filtrado para el listado Intentos de intrusión bloqueados

- **Ventana de detalle**

Muestra información detallada del ataque de red detectado.

Campo	Descripción	Valores
Tipo de intrusión	Indica el tipo de intrusión detectado. Consulta " Bloquear intrusiones " en la página 253 para obtener más información acerca de cada uno de los ataques enumerados.	• ICMP attack • UDP port scan • Header lengths • UDP flood

Tabla 19.41: Detalle del listado de Intentos de intrusión bloqueados

Campo	Descripción	Valores
		- TCP flags check - Smart WINS - IP explicit path - Land attack - Smart DNS - ICM filter echo request - OS detection - Smart DHCP - SYN flood - Smart ARP - TCP port scan
Acción	Acción que ejecutó Panda Adaptive Defense 360.	Bloqueado
Equipo	Nombre del equipo donde se realizó la detección.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Dispositivo móvil - Servidor
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dirección IP local	Dirección IP del equipo que recibió el ataque de red.	Cadena de caracteres
Dirección IP remota	Dirección IP del equipo que inició el ataque de red.	Cadena de caracteres
MAC remota	Dirección física del equipo que inició el ataque de red, siempre que se encuentre en el mismo segmento de red que el equipo que recibió el ataque.	Cadena de caracteres
Puerto local	Si el ataque es TCP o UDP indica el puerto donde se recibió el intento de intrusión.	Numérico
Puerto remoto	Si el ataque es TCP o UDP indica el puerto desde donde se envió el intento de intrusión.	Numérico
Detectado por	Módulo que realizó la detección.	Firewall
Número de detecciones	Número de veces que se repitió de forma sucesiva el mismo tipo de ataque entre los mismos equipos origen y destino.	Numérico
Fecha	Fecha de la detección.	Fecha

Tabla 19.41: Detalle del listado de Intentos de intrusión bloqueados

Accesos a páginas web por categoría

Campo	Descripción	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 19.42: Campos del listado Accesos a páginas web por categoría

• Campos mostrados en el fichero exportado

Campo	Descripción	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 19.43: Campos del fichero exportado Accesos a páginas web por equipo

• Herramienta de filtrado

Campo	Descripción	Valores
Fechas	• Rango: permite establecer un intervalo de fechas desde el día presente hacia el pasado. • Fecha personalizada: permite establecer una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes • Último año

Tabla 19.44: Campos de filtrado para el listado Accesos a páginas web por equipo

Campo	Descripción	Valores
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas.

Tabla 19.44: Campos de filtrado para el listado Accesos a páginas web por equipo

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	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	- Cadena de caracteres  Grupo Todos  Grupo nativo  Grupo Directorio activo
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

Tabla 19.45: Campos del listado Accesos a páginas web por equipo

• Campos mostrados en el fichero exportado

Campo	Descripción	Valores
Cliente	Cuenta del cliente a la que pertenece el servicio.	Cadena de caracteres
Tipo de equipo	Clase del dispositivo.	- Estación - Portátil - Dispositivo móvil - Servidor
Equipo	Nombre del equipo.	Cadena de caracteres
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas

Tabla 19.46: Campos del fichero exportado Accesos a páginas web por equipo

Campo	Descripción	Valores
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
Grupo	Grupo dentro del árbol de grupos de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Dirección IP	Dirección IP principal del equipo.	Cadena de caracteres
Dominio	Dominio Windows al que pertenece el equipo.	Cadena de caracteres
Descripción	Descripción asignada al equipo por el administrador.	Cadena de caracteres

Tabla 19.46: Campos del fichero exportado Accesos a páginas web por equipo

- **Herramienta de búsqueda**

Campo	Descripción	Valores
Fechas	• Rango: establece un intervalo de fechas desde el día presente hacia atrás. • Rango personalizado: establece una fecha concreta del calendario.	• Últimas 24 horas • Últimos 7 días • Último mes
Categoría	Categoría a la que pertenece la página accedida.	Enumeración de las categorías soportadas.
Tipo de equipo	Clase del dispositivo.	• Estación • Portátil • Dispositivo móvil • Servidor
Equipo	Nombre del equipo.	Cadena de caracteres

Tabla 19.47: Campos de filtrado para el listado Accesos a páginas web por equipo

Capítulo 20

Gestión de amenazas, elementos en clasificación y cuarentena

Panda Adaptive Defense 360 incorpora la capacidad de equilibrar la eficacia del servicio de seguridad con el impacto que perciben los usuarios protegidos en su actividad diaria. Este equilibrio se consigue a través de herramientas que permiten gestionar los bloqueos de ejecución de los diferentes tipos de programas encontrados:

- Programas clasificados como malware.
- Programas clasificados como PUPs.
- Programas clasificados como Exploits.
- Programas clasificados como virus.
- Programas desconocidos en proceso de clasificación.



Para obtener más información sobre permitir la ejecución de programas desconocidos en proceso de clasificación consulta [“Configuración de software autorizado”](#) en la página [403](#).

Para obtener más información sobre los modos de protección avanzados hardening y lock consulta [“Protección permanente avanzada”](#).

CONTENIDO DEL CAPÍTULO

Introducción a las herramientas de gestión de amenazas	456
Desbloquear / dejar de permitir los procesos desconocidos	456
Permitir / dejar de permitir la ejecución de malware, PUP o Exploit	457
Cambiar la política de reclasificación.	457
Gestionar el backup / cuarentena	457
Comportamiento del software de seguridad	458
Permitir y volver a impedir la ejecución de elementos	460
Desbloquear elementos desconocidos pendientes de clasificación	460
Permitir ejecutar elementos clasificados como malware, PUP o Exploit	461

Restaurar / no volver a detectar programas clasificados como virus	462
Dejar de permitir la ejecución de elementos previamente permitidos	463
Información de amenazas bloqueadas - - - - -	463
Información de elementos bloqueados en clasificación - - - - -	464
Panel Programas actualmente bloqueados en clasificación	464
Listado de Programas actualmente bloqueados en clasificación	466
Listado Historial de programas bloqueados	468
Listado de amenazas y programas desconocidos permitidos - - - - -	471
Programas permitidos por el administrador	472
Listado Historial de Programas permitidos por el administrador	473
Política de reclasificación - - - - -	476
Cambiar la política de reclasificación	476
Trazabilidad de las reclasificaciones	477
Trazabilidad mediante el Historial de Programas bloqueados	477
Trazabilidad mediante alertas	477
Estrategias para supervisar la clasificación de ficheros - - - - -	478
Configurar el equipo de pruebas	478
Instalar el software	478
Reclasificar los programas bloqueados	478
Enviar el programa directamente a la nube de Panda Security	478
Gestión de la zona de backup / cuarentena - - - - -	479
Visualizar los elementos en cuarentena	479
Restaurar elementos de cuarentena	480

Introducción a las herramientas de gestión de amenazas

El administrador de la red puede variar el comportamiento de Panda Adaptive Defense 360 con respecto a las amenazas encontradas y los ficheros desconocidos en proceso de clasificación mediante las herramientas siguientes:

- Desbloquear / dejar de permitir los procesos desconocidos.
- Permitir / dejar de permitir la ejecución de programas clasificados como malware, PUP, virus o Exploit.
- Cambiar la política de reclasificación de Panda Adaptive Defense 360.
- Gestionar el backup / cuarentena.

Desbloquear / dejar de permitir los procesos desconocidos

Panda Adaptive Defense 360 analiza y clasifica en la nube los procesos desconocidos de forma automática dentro de las primeras 24 horas a partir de su descubrimiento en el equipo del usuario o servidor. Este proceso emite una categoría no ambigua (goodware o malware) compartida para todos los clientes de Panda Security, de forma que todos se benefician del conocimiento acumulado hasta la fecha.

Para reforzar la protección de los equipos de la red, Panda Adaptive Defense 360 incorpora los modos **Hardening** y **Lock** en el perfil de configuración avanzada. En ambos modos, Panda Adaptive Defense 360 bloquea los procesos durante el tiempo de clasificación, para evitar potenciales

situaciones de peligro. Esto impide a los usuarios ejecutar los procesos bloqueados hasta que se termina el proceso de clasificación. El proceso de clasificación se puede realizar de dos formas:

- **Análisis automatizado:** cubre la mayor parte de los casos y en produce tiempo real.
- **Análisis manual:** si el análisis automatizado no puede clasificar el proceso desconocido con el 99'999% de certeza, un experto en análisis de malware estudiará de forma manual la muestra. En estos casos, el análisis puede demorarse por un corto espacio de tiempo.

En los casos donde la clasificación no es inmediata, el administrador puede asumir ciertos riesgos y permitir la ejecución del fichero sin esperas. Para ello Panda Adaptive Defense 360 implementa dos estrategias:

- **Desbloqueo reactivo:** el administrador permite la ejecución de un programa desconocido en clasificación después de que el usuario ha intentado utilizarlo y Panda Adaptive Defense 360 lo ha detectado y bloqueado. Consulta "[Permitir y volver a impedir la ejecución de elementos](#)".
- **Desbloqueo proactivo:** se produce cuando el administrador quiere garantizar de antemano que un conjunto determinado de programas no son bloqueados si son desconocidos para Panda Adaptive Defense 360. El objetivo del desbloqueo proactivo es evitar un posible impacto negativo en el rendimiento de los usuarios. Consulta "[Configuración de software autorizado](#)" en la página [403](#).

Permitir / dejar de permitir la ejecución de malware, PUP o Exploit

El administrador puede permitir la ejecución del software que implemente algunas funcionalidades valoradas por los usuarios pero que ha sido clasificado como una amenaza. Este es el caso, por ejemplo, de PUPs, programas generalmente en forma de barras de navegador, que ofrecen capacidades de búsqueda al tiempo que recolectan información privada del usuario o confidencial de la empresa con objetivos publicitarios. Consulta "[Permitir y volver a impedir la ejecución de elementos](#)".

Cambiar la política de reclasificación.

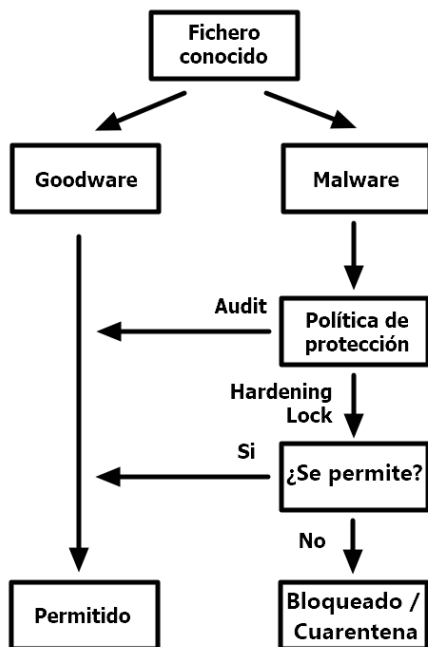
Cuando el administrador desbloquea un elemento desconocido previamente bloqueado por Panda Adaptive Defense 360, al cabo de un tiempo el proceso de clasificación cataloga al elemento como malware o goodware. Si se trata de goodware, no se requiere ningún tipo de consideración adicional, ya que Panda Adaptive Defense 360 seguirá permitiendo su ejecución. Por el contrario, si se trata de malware, se aplica la política de reclasificación, que permite al administrador definir el comportamiento de Panda Adaptive Defense 360. Consulta "[Política de reclasificación](#)".

Gestionar el backup / cuarentena

El administrador puede recuperar los elementos considerados como amenazas y, por lo tanto, eliminados de los equipos de los usuarios.

Comportamiento del software de seguridad

- **Ficheros conocidos**



Si el fichero está clasificado como malware / PUP / exploit y se aplica una política de protección avanzada distinta de **Audit**, los ficheros son bloqueados, a no ser que el administrador permita su ejecución.

Figura 20.1: Diagrama de acciones para procesos conocidos y ya clasificados

- **Ficheros desconocidos**

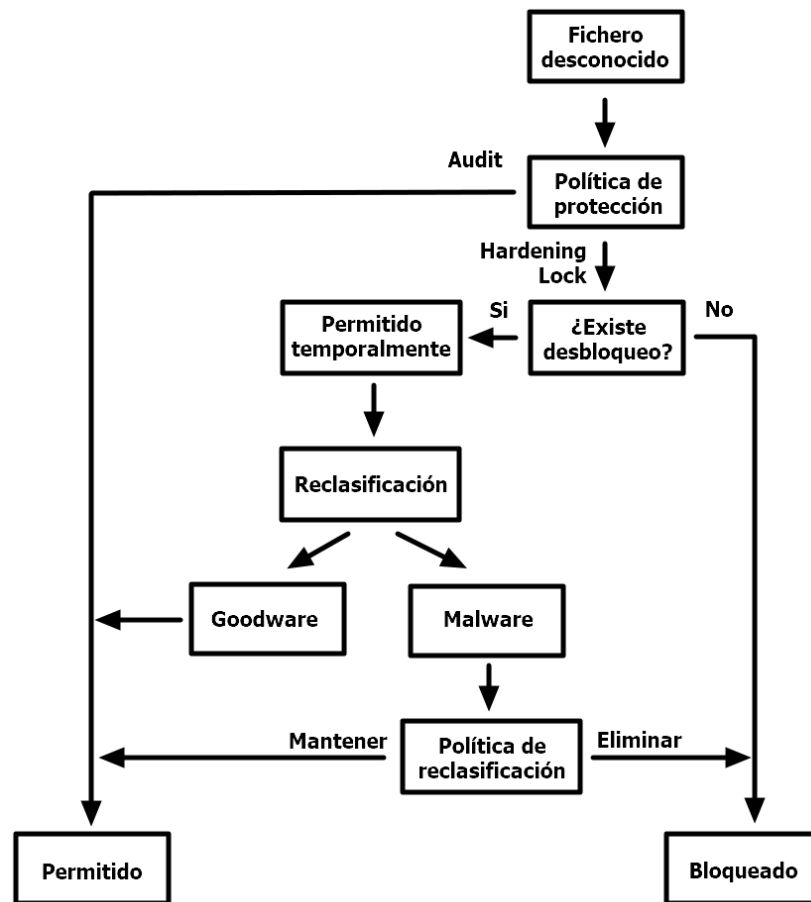


Figura 20.2: Diagrama de acciones para procesos desconocidos

En el caso de los ficheros desconocidos en proceso de clasificación y una política de protección avanzada distinta de **Audit**, el comportamiento de Panda Adaptive Defense 360 es el siguiente:

- Si el administrador no ha establecido un desbloqueo, los ficheros se bloquearán.
 - Si una vez clasificado el resultado es goodware, se permite ejecutar el fichero.
 - Si una vez clasificado el resultado es malware, se bloquea la ejecución del fichero.
- Si el administrador ha establecido un desbloqueo, el fichero se podrá ejecutar mientras se completa el proceso de clasificación. Una vez terminado:
 - Si el fichero es goodware se sigue permitiendo ejecutar el proceso.
 - Si el fichero es malware se permite o se impide ejecutar el proceso dependiendo de la política de reclasificación elegida por el administrador. Consulta "[Política de reclasificación](#)"

Permitir y volver a impedir la ejecución de elementos

Dependiendo del tipo de programa que el administrador quiere permitir ejecutar, se utilizan los paneles siguientes:

- **Programas actualmente bloqueados en clasificación:** desbloquea elementos en clasificación.
- **Actividad del Malware:** permite la ejecución de programas clasificados como malware.
- **Actividad de PUP:** permite la ejecución de programas clasificados como PUP.
- **Actividad de Exploits:** permite la ejecución de técnicas de explotación.
- **Amenazas detectadas por el antivirus:** restaura de la cuarentena los elementos eliminados por Panda Adaptive Defense 360 al coincidir con una firma incluida en el archivo de identificadores.

Desbloquear elementos desconocidos pendientes de clasificación



De forma general se desaconseja desbloquear la ejecución de elementos sin clasificar, ya que pueden representar un riesgo para la integridad de los sistemas de IT de la empresa y sus datos.

Si los usuarios no pueden esperar a que Panda Adaptive Defense 360 complete la clasificación para liberar el bloqueo de forma automática, el administrador puede desbloquearlos manualmente.

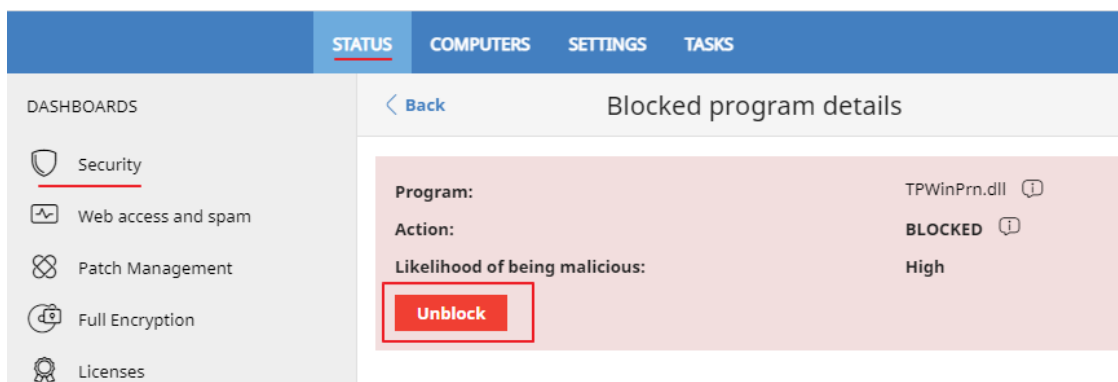


Figura 20.3: Desbloquear un elemento desconocido en clasificación

Para permitir ejecutar un elemento desconocido en clasificación:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Programas actualmente bloqueados en clasificación** y selecciona el elemento a desbloquear en el listado.
- Haz clic en el botón **Desbloquear**. Se mostrará una ventana advirtiendo del peligro que supone desbloquear un elemento desconocido, junto a una valoración provisional de su peligrosidad.
- Haz clic en el botón **Desbloquear**. Panda Adaptive Defense 360 ejecutará las siguientes acciones:
 - El elemento podrá ser ejecutado en todos los equipos gestionados del parque informático.

- Además de permitir ejecutar el elemento, se permite la ejecución automática de toda la cadena de librerías y binarios utilizados en el programa, excepto aquellas ya conocidas y clasificadas como amenazas.
- El elemento se retira del listado **Programas actualmente bloqueados en clasificación**.
- El elemento se incorpora al listado **Programas permitidos por el administrador**.
- El elemento se incorpora al listado **Historial de programas permitidos por el administrador**.
- Panda Adaptive Defense 360 continuará analizando el elemento hasta completar su clasificación.

Permitir ejecutar elementos clasificados como malware, PUP o Exploit



De forma general se desaconseja desbloquear la ejecución de elementos clasificados como amenazas, ya que representan un riesgo evidente para la integridad de los sistemas de IT de la empresa y sus datos.

Si los usuarios requieren cierta funcionalidad incluida en un programa que ha sido clasificado como una amenaza, y el administrador considera que el peligro para la integridad del parque IT administrador es bajo, puede permitir su ejecución.

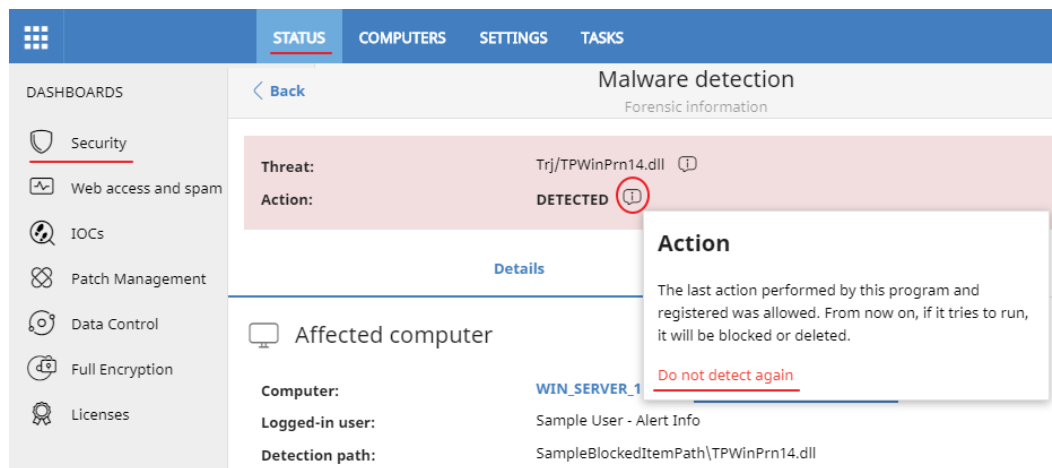


Figura 20.4: Permitir la ejecución de una amenaza

Para permitir la ejecución de un programa clasificado como malware, PUP o Exploit:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en panel **Actividad de malware / PUP / Exploit** y selecciona la amenaza que quieres permitir su ejecución.
- Haz clic en el icono ⓘ del campo **Acción**. Se mostrará un ventana explicando la acción tomada por Panda Adaptive Defense 360.
- Haz clic en el enlace **No volver a detectar**. Panda Adaptive Defense 360 ejecutará las siguientes acciones:

- El elemento podrá ser ejecutado en todos los equipos gestionados por el administrador. En el caso de exploits, se permitirá la ejecución de la técnica de explotación específicamente permitida, y únicamente ejecutada desde el programa detectado.
- Además de permitir ejecutar el elemento, se permite la ejecución automática de toda la cadena de librerías y binarios utilizados en el programa, excepto aquellas ya conocidas y clasificadas como amenazas.
- El elemento se incorpora al listado **Programas permitidos por el administrador**.
- El elemento deja de generar incidentes en los paneles **Actividad de malware / PUP / Exploits**

Restaurar / no volver a detectar programas clasificados como virus

Si los usuarios requieren cierta funcionalidad incluida en un programa que ha sido clasificado por el fichero de firmas como una amenaza, y el administrador considera que el peligro para la integridad del parque IT administrador es bajo, puede permitir su ejecución:

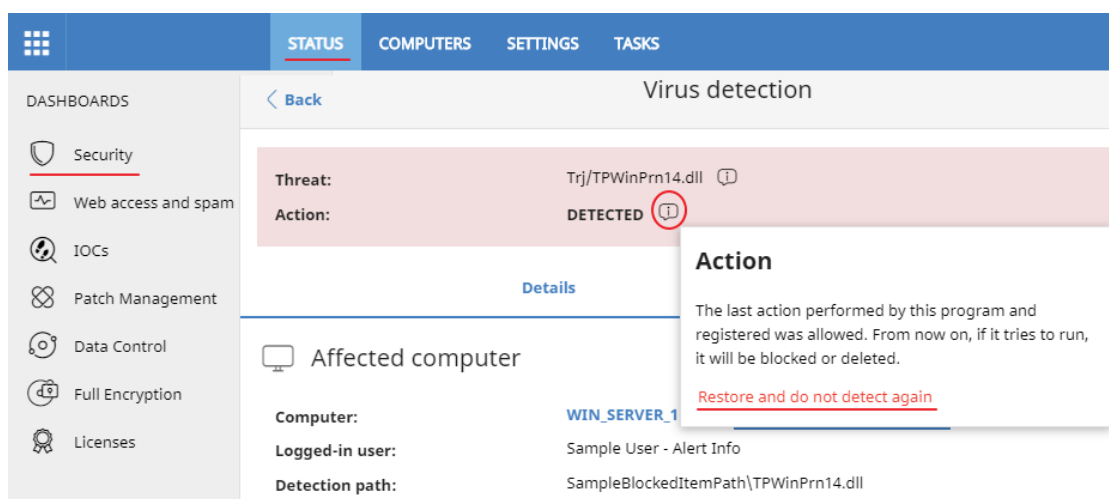


Figura 20.5: Restaurar y no volver a detectar una amenaza

Para restaurar desde la cuarentena / backup un programa borrado y no volver a detectarlo:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Amenazas detectadas por el antivirus** y selecciona el elemento que quieres permitir su ejecución.
- Haz clic en el icono ⓘ del campo **Acción**. Se mostrará un ventana explicando la acción tomada por Panda Adaptive Defense 360.
- Haz clic en el enlace **Restaurar y no volver a detectar**. Panda Adaptive Defense 360 ejecutará las siguientes acciones:
 - El elemento se copia desde la cuarentena / backup a su ubicación original en los equipos del parque informático.
 - El elemento podrá ser ejecutado y no generará detecciones.
 - El programa se incorpora al listado **Programas permitidos por el administrador**.

Dejar de permitir la ejecución de elementos previamente permitidos

Para volver a bloquear un elemento previamente permitido por el administrador:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el tipo de elemento a dejar de permitir dentro del panel **Programas permitidos por el administrador: malware, PUP, exploit o en clasificación**.
- En el listado **Programas permitidos por el administrador** haz clic en el icono  situado a la derecha del elemento que quieres dejar de permitir su ejecución.

Al hacer clic en el icono  asociado al elemento, Panda Adaptive Defense 360 ejecuta las acciones siguientes:

- El elemento se retira del listado **Programas permitidos por el administrador**.
- Se añade una entrada al listado **Historial de programas permitidos por el administrador** indicando como **Acción** el valor **Exclusión eliminada por el usuario**.
- Si es un elemento clasificado como malware, PUP, exploit o virus volverá a aparecer su listado correspondiente:
 - **Actividad de malware**
 - **Actividad de PUP**
 - **Actividad de exploits**
 - **Amenazas detectadas por el antivirus**.
- Si es un elemento clasificado como virus volverá aparecer en el listado **Amenazas detectadas por el antivirus**.
- Si es un elemento clasificado como malware, PUP, exploit o virus volverá a generar incidentes.
- Si es un elemento desconocido en proceso de clasificación, volverá a aparecer en el listado **Programas actualmente bloqueados en clasificación**.

Información de amenazas bloqueadas

El administrador de la red dispone de varios paneles y listados para obtener información sobre los programas clasificados como una amenaza:

- **Clasificación de todos los programas ejecutados y analizados:** consulta "[Clasificación de todos los programas ejecutados y analizados](#)" en la página [419](#) .
- **Actividad de malware:** consulta "[Actividad de malware / PUP](#)" en la página [417](#).
- **Actividad de PUPs:** consulta "[Actividad de malware / PUP](#)" en la página [417](#).
- **Actividad de exploit:** consulta "[Actividad de exploits](#)" en la página [418](#).

Información de elementos bloqueados en clasificación

El administrador de la red dispone de varios paneles y listados para obtener información sobre los programas bloqueados en clasificación:

- El panel **Programas actualmente bloqueados en clasificación**.
- El listado **Programas actualmente bloqueados en clasificación**.
- El listado **Historial de programas bloqueados**.

Panel Programas actualmente bloqueados en clasificación

CURRENTLY BLOCKED PROGRAMS BEING CLASSIFIED



Figura 20.6: Panel de Programas actualmente bloqueados en clasificación

Muestra todos los elementos bloqueados que aún no han sido clasificados desde la puesta en marcha del servicio en el cliente hasta el momento actual.



*Este widget no se ve afectado por la selección del intervalo de tiempo establecida por el administrador en el menú superior **Estado**, panel lateral **Seguridad**.*

Cada programa diferente bloqueado en clasificación se representa mediante un círculo con las características siguientes:

- Cada elemento bloqueado en clasificación con un MD5 diferente se representa con círculo.
- El color del círculo representa el grado de peligrosidad asignado temporalmente al elemento.
- El tamaño de cada burbuja representa el número de equipos diferentes donde se intentó ejecutar el programa desconocido bloqueado. El tamaño de cada burbuja **no** representa la cantidad de intentos de ejecución en los equipos de la red.

- **Descripción de las series**

Las aplicaciones bloqueadas se muestran con el código de colores indicado a continuación:

Serie	Descripción
Naranja	Aplicaciones con probabilidad media de ser malware.
Naranja oscuro	Aplicaciones con probabilidad alta de ser malware.
Rojo	Aplicaciones con probabilidad muy alta de ser malware.

Tabla 20.1: Descripción de la serie Programas actualmente bloqueados en clasificación

Al pasar el ratón por encima cada círculo se amplía, mostrando su nombre completo y una serie de iconos que representan acciones clave:



- **Carpeta:** el programa ha leído datos del disco duro del usuario.
- **Bola del mundo:** el programa estableció una conexión con otro equipo.

Figura 20.7: Representación gráfica de un programa en clasificación

• Filtros preestablecidos desde el panel

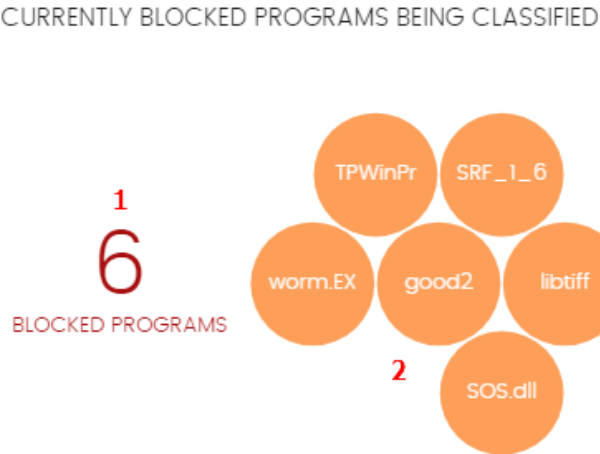


Figura 20.8: Zonas activas del panel Programas actualmente bloqueados en clasificación

Haz clic en las zonas indicadas en la figura 20.8 para abrir el listado **Programas actualmente bloqueados en clasificación** con los filtros preestablecidos mostrados a continuación:

Zona activa	Filtro
(1)	Sin filtros.
(2)	Buscar = Hash.

Tabla 20.2: Definición de los filtros del listado Programas actualmente bloqueados en clasificación

Listado de Programas actualmente bloqueados en clasificación

Muestra una tabla con los todos ficheros bloqueados por no haberse completado su clasificación.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Ha accedido a datos 📄	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Se ha comunicado con equipos externos 🌐	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento del descubrimiento del fichero desconocido.	• Audit • Hardening • Lock
Probabilidad de que sea malicioso	Posibilidad de que finalmente el fichero desconocido sea una amenaza.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha

Tabla 20.3: Campos del listado Programas actualmente bloqueados

• Campos mostrados en fichero exportado



En el menú de contexto de **Programas actualmente bloqueados en clasificación** se muestra un desplegable con dos entradas: **Exportar** y **Exportar listado y detalles**. En este apartado se muestra el contenido de **Exportar**. Para obtener información sobre **Exportar listado y detalles**, consulta "[Ficheros exportados Excel](#)".

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Amenaza	Nombre del fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres
Modo de protección	Modo en el que se encontraba la protección en el momento del descubrimiento del fichero desconocido.	• Audit • Hardening • Lock
Acceso a datos	El fichero desconocido ha accedido a ficheros que residen en el equipo del usuario.	Booleano
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Probabilidad de que sea malicioso	Posibilidad de que el fichero desconocido sea una amenaza cuando se complete su clasificación.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha
Tiempo de exposición	Tiempo que la amenaza ha permanecido en el parque del cliente sin clasificar.	Fecha
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Equipo origen de la amenaza	Nombre del equipo si el programa bloqueado viene de un equipo de la red del cliente.	Cadena de caracteres
IP origen de la amenaza	Dirección IP del equipo si el programa bloqueado viene de un equipo de la red del cliente.	Cadena de caracteres
Usuario origen de la amenaza	Usuario registrado en el equipo origen del programa bloqueado.	Cadena de caracteres

Tabla 20.4: Campos del fichero exportado Programas actualmente bloqueados

- **Herramienta de filtrado**

Campo	Comentario	Valores
Fechas	Establece un intervalo de fechas desde el momento actual hacia el pasado.	• Últimas 24 horas • Últimos 7 días • Último mes
Buscar	• Equipo: dispositivo donde reside el elemento desconocido. • Amenaza: nombre del archivo. • Hash: Cadena resumen de identificación del archivo. • Origen de la amenaza: permite buscar por el usuario, la IP o el nombre del equipo origen del elemento bloqueado.	Enumeración
Modos de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Hardering • Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano

Tabla 20.5: Campos de filtrado para el listado Programas actualmente bloqueados

- **Ventana de detalle**

Muestra información detallada del programa bloqueado. Consulta [“Detección del malware”](#) en la página 482.

Listado Historial de programas bloqueados

Muestra un histórico de todos los eventos que se han producido a lo largo del tiempo relativos a los procesos que han sido bloqueados por ser desconocidos.

Este listado no tiene un panel asociado y es accesible únicamente mediante el botón **Historial** del listado **Programas actualmente bloqueados en clasificación**, situado en la esquina superior derecha.

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Ruta	Nombre del fichero desconocido y ruta en el equipo del usuario.	Cadena de caracteres

Tabla 20.6: Campos del listado Historial de programas bloqueados

Campo	Comentario	Valores
Acción	Acción ejecutada por Panda Adaptive Defense 360.	• Bloqueado • Reclasificado a GW • Reclasificado a MW • Reclasificado a PUP
Ha accedido a datos 	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Se ha comunicado con equipos externos 	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Audit • Hardening • Lock
Excluido	El fichero desconocido ha sido desbloqueado / excluido por el administrador para permitir su ejecución.	Booleano
Probabilidad de que sea malicioso	Posibilidad de que el fichero desconocido sea una amenaza cuando se complete su clasificación.	• Media • Alta • Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha

Tabla 20.6: Campos del listado Historial de programas bloqueados

• **Campos mostrados en fichero exportado**



En el menú de contexto de **Historial de programas bloqueados** se muestra un desplegable con dos entradas diferentes: **Exportar** y **Exportar listado y detalles**. En este apartado se muestra el contenido de **Exportar**. Para obtener información sobre **Exportar listado y detalles** consulta ["Ficheros exportados Excel"](#).

Campo	Comentario	Valores
Equipo	Nombre del equipo donde se encontró el fichero desconocido.	Cadena de caracteres
Amenaza	Nombre del fichero desconocido.	Cadena de caracteres
Ruta	Ruta en el equipo del usuario del fichero desconocido.	Cadena de caracteres

Tabla 20.7: Campos del fichero exportado Historial de programas bloqueados

Campo	Comentario	Valores
Modo de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	- Audit - Hardening - Lock
Acción	Acción ejecutada por Panda Adaptive Defense 360.	- Bloqueado - Reclasificado a GW - Reclasificado a MW - Reclasificado a PUP
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano
Excluido	El fichero desconocido ha sido desbloqueado por el administrador para permitir su ejecución.	Booleano
Probabilidad de que sea malicioso	Posibilidad de que el fichero desconocido sea una amenaza cuando se complete su clasificación.	- Media - Alta - Muy Alta
Fecha	Fecha en la que se detectó por primera vez el fichero desconocido.	Fecha
Tiempo de exposición	Tiempo que el fichero desconocido ha permanecido en el parque del cliente sin clasificar.	Fecha
Usuario	Cuenta de usuario bajo la cual el programa se ha ejecutado.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo.	Cadena de caracteres
Equipo origen de la amenaza	Equipo origen del programa bloqueado.	Cadena de caracteres
IP origen de la amenaza	IP origen del programa bloqueado.	Cadena de caracteres
Usuario origen de la amenaza	Usuario origen del programa bloqueado.	Cadena de caracteres

Tabla 20.7: Campos del fichero exportado Historial de programas bloqueados

- Herramienta de filtrado**

Campo	Comentario	Valores
Buscar	Equipo: dispositivo donde reside el fichero desconocido. Amenaza: nombre de la amenaza.	Enumeración

Tabla 20.8: Campos del fichero exportado Historial de programas bloqueados

Campo	Comentario	Valores
	• Hash: cadena resumen de identificación del archivo. • Origen de la amenaza: permite buscar por el usuario, la IP o el nombre del equipo origen de la amenaza.	
Fechas	Establece un intervalo de fechas desde el momento actual hacia atrás.	• Últimas 24 horas • Últimos 7 días • Último mes
Acción	Acción desencadenada por Panda Adaptive Defense 360.	• Bloqueado • Reclasificado a GW • Reclasificado a MW • Reclasificado a PUP
Excluido	El fichero desconocido ha sido desbloqueado por el administrador para permitir su ejecución.	Booleano
Modos de protección	Modo en el que se encontraba la protección avanzada en el momento de la detección del fichero desconocido.	• Hardening • Lock
Acceso a datos	El fichero desconocido ha accedido a datos que residen en el equipo del usuario.	Booleano
Conexiones externas	El fichero desconocido se comunica con equipos remotos para enviar o recibir datos.	Booleano

Tabla 20.8: Campos del fichero exportado Historial de programas bloqueados

- **Ventana de detalle**

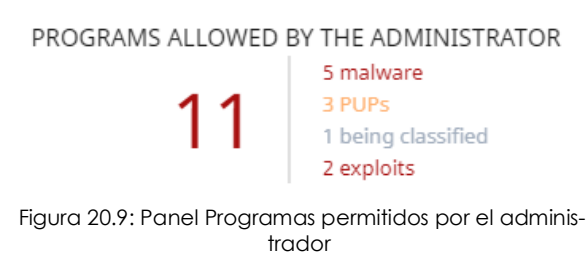
Muestra información detallada del programa bloqueado. Consulta ["Detección del malware"](#).

Listado de amenazas y programas desconocidos permitidos

El administrador de la red dispone de varios paneles y listados para obtener información sobre los programas que inicialmente fueron bloqueados por Panda Adaptive Defense 360 y cuya ejecución ha sido permitida:

- El panel **Programas permitidos por el administrador**.
- El listado **Programas permitidos por el administrador**.
- El listado **Historial de programas permitidos por el administrador**.

Programas permitidos por el administrador



Muestra los programas permitidos por el administrador a los que previamente Panda Adaptive Defense 360 impidió su ejecución al estar clasificados como una amenaza (malware, PUP o exploit), o por ser desconocidos y estar en proceso de clasificación.

• Descripción de las series

El panel representa el número total de elementos que el administrador excluyó del bloqueo, desagregados por su tipo:

- Malware
- PUP
- Exploit
- En clasificación

• Filtros preestablecidos desde el panel



Figura 20.10: Zonas activas del panel Programa permitidos por el administrador

Haz clic en las zonas indicadas en la figura 20.10 para abrir el listado **Programas permitidos por el administrador** con los filtros preestablecidos mostrados a continuación:.

Zona activa	Filtro
(1)	Sin filtros.
(2)	Clasificación = malware.
(3)	Clasificación = PUP.
(4)	Clasificación = Exploit.
(5)	Clasificación = En clasificación (bloqueados y sospechosos).

Tabla 20.9: Definición de los filtros del listado Programas permitidos por el administrador

Listado Historial de Programas permitidos por el administrador

Muestra un histórico de todos eventos que se han producido a lo largo del tiempo relativos a las amenazas y ficheros desconocidos en clasificación cuya ejecución permitió el administrador. El listado muestra el ciclo de estados completo de un fichero, desde que entra en el listado de **Programas permitidos por el administrador** hasta que lo abandona, pasando por todos los cambios de estado intermedios que Panda Adaptive Defense 360 o el administrador provoque.

Este listado no tiene un panel asociado, y es accesible únicamente mediante el botón **Historial** del listado **Programas permitidos por el administrador**, situado en la esquina superior derecha.

Campo	Descripción	Valores
Programa	Nombre del fichero que contiene código malicioso y que se permite su ejecución.	Cadena de caracteres
Clasificación	Tipo de la amenaza a la que se permitió su ejecución.	- Malware - PUP - Goodware - Exploit - En clasificación
Amenaza	Nombre del malware o PUP cuya ejecución se permite. Si es un elemento desconocido se indica el nombre del fichero en su lugar. Si es un exploit se indica la técnica de explotación utilizada.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo. Vacío si es un exploit.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido. Exclusión eliminada por el usuario: el administrador permitió bloquear de nuevo el elemento. Exclusión eliminada por reclasificación: Panda Adaptive Defense 360 aplica la acción asociada a la categoría obtenida de la reclasificación. Exclusión añadida por el usuario: el administrador permitió ejecutar el elemento. Exclusión mantenida por reclasificación: Panda Adaptive Defense 360 no bloqueó el elemento al reclasificarlo.	Enumeración
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 20.10: Campos del listado Historial de Programas permitidos por el administrador

• **Campos incluidos en fichero exportado**

Campo	Descripción	Valores
Programa	Nombre y ruta del fichero que contiene código malicioso cuya ejecución se permitió.	Cadena de caracteres
Tipo actual	Último tipo de la amenaza que se permitió su ejecución.	• Malware • PUP • Exploit • Bloqueado • Sospechoso
Tipo original	Tipo del fichero cuando se produjo el evento.	• Malware • PUP • Exploit • Bloqueado • Sospechoso
Amenaza	Nombre del malware o PUP cuya ejecución se permite. Si es un elemento desconocido, se indica el nombre del fichero en su lugar. Si es un exploit, se indica la técnica de explotación utilizada.	Cadena de caracteres
Hash	Cadena resumen de identificación del archivo. Vacío si es un exploit.	Cadena de caracteres
Acción	Acción aplicada sobre el elemento permitido. • Exclusión eliminada por el usuario: el administrador permitió bloquear de nuevo el elemento. • Exclusión eliminada por reclasificación: Panda Adaptive Defense 360 aplica la acción asociada a la categoría obtenida de la reclasificación. • Exclusión añadida por el usuario: el administrador permitió ejecutar el elemento. • Exclusión mantenida por reclasificación: Panda Adaptive Defense 360 no bloqueó el elemento al reclasificarlo.	Enumeración
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 20.11: Campos del fichero exportado Historial de Programas permitidos por el administrador

- Herramienta de filtrado

Campo	Descripción	Valores
Buscar	• Usuario: cuenta de usuario de la consola que inició el cambio en el fichero permitido. • Programa: nombre del fichero que contiene la amenaza. • Hash: cadena resumen de identificación del archivo.	Enumeración
Clasificación	Tipo del fichero en el momento en el que clasificó por última vez.	• Todos • Malware • PUP • Goodware • Exploit • En clasificación (Bloqueados y sospechoso)
Clasificación original	Tipo del fichero en el momento en el que se comenzó a permitir su bloqueo.	• Todos • Malware • PUP • En clasificación (Bloqueado) • En clasificación (Sospechoso) • Exploit
Acción	Acción aplicada sobre el elemento permitido. • Exclusión eliminada por el usuario: el administrador permitió bloquear de nuevo el elemento. • Exclusión eliminada por reclasificación: Panda Adaptive Defense 360 aplica la acción asociada a la categoría obtenida de la reclasificación. • Exclusión añadida por el usuario: el administrador permitió ejecutar el elemento. • Exclusión mantenida por reclasificación: Panda Adaptive Defense 360 no bloqueó el elemento al reclasificarlo.	Enumeración

Tabla 20.12: Campos de filtrado para el listado Historial de Programas permitidos por el administrador

Política de reclasificación



Figura 20.11: Comportamiento de Panda Adaptive Defense 360 ante la política de reclasificación elegida y el resultado de la clasificación

La política de reclasificación establece el comportamiento de Panda Adaptive Defense 360 cuando un elemento desbloqueado por el administrador cambia su clasificación y es necesario tomar una nueva decisión.

En los casos en los que el administrador permite ejecutar un elemento desconocido, Panda Adaptive Defense 360 lo clasificará como malware o goodware pasado un período de tiempo. Si se trata de goodware, no se requiere ningún tipo de consideración adicional ya que Panda Adaptive Defense 360 permite su ejecución. Por el contrario, si se trata de malware, se aplica la política de reclasificación, que permite al administrador definir el comportamiento de Panda Adaptive Defense 360 a seguir.

Cambiar la política de reclasificación

La política de reclasificación es general para todos los equipos de la red e independiente de la configuración de seguridad.

Para cambiar la acción que ejecuta Panda Adaptive Defense 360 cuando se produce una reclasificación de archivos:

- Haz clic en el menú superior **Estado** y en el panel lateral **Seguridad**.
- Haz clic en el tipo de elemento en el panel **Programas permitidos por el administrador**:
 - Malware
 - PUPs
 - En clasificación
 - Exploits
- Haz clic en el enlace **Cambiar comportamiento**. Se mostrará una ventana emergente con la política de reclasificación a aplicar.
 - **Eliminar de la lista de programas permitidos por el administrador**: si el fichero desconocido es goodware, se sigue ejecutando de forma normal. Si el fichero es malware, la exclusión se elimina de forma automática y el fichero queda nuevamente bloqueado, a no ser que el administrador

genere una nueva exclusión manual para ese fichero.

- **Mantener en la lista de Programas permitidos por el administrador:** se muestra en el listado **Programas permitidos por el administrador** una franja de color rojo que indica que esta elección puede dar lugar a situaciones potencialmente peligrosas. Tanto si el fichero desconocido se ha clasificado como **goodware** o **malware**, la exclusión se mantiene y el fichero se sigue ejecutando.



Panda Security desaconseja el uso de esta configuración por el riesgo de abrir un agujero de seguridad que permita ejecutar malware en los equipos de la red.

Trazabilidad de las reclasificaciones

Si el administrador elige la política **Mantener en la lista de Programas permitidos por el administrador**, necesita conocer si Panda Adaptive Defense 360 ha reclasificado un elemento desconocido con el fin de saber si un programa permitido fue reclasificado como **malware**.

Trazabilidad mediante el Historial de Programas bloqueados

Para visualizar el histórico de reclasificaciones y eventos de un fichero desbloqueado:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel **Programas actualmente bloqueados en clasificación**
- Haz clic en el enlace **Ver historial de bloqueos**. Se mostrará el listado **Historial de programas bloqueados**.
- Utiliza el buscador para indicar el nombre de la amenaza. En el campo **Acción** se detalla el tipo de evento producido. Consulta "[Listado Historial de programas bloqueados](#)".

Trazabilidad mediante alertas



Para obtener el detalle de las alertas recibidas consulta "[Alertas](#)" en la página [505](#).

El administrador puede recibir notificaciones por correo en el momento en que se producen los bloqueos por ficheros desconocidos. También se envía información de las reclasificaciones de los ficheros que previamente ha desbloqueado.

Para habilitar las notificaciones por correo en bloqueos de ficheros desconocidos:

- Haz clic en el menú superior **Configuración** y en el panel lateral **Mis alertas**.
- Habilita los siguientes tipos de alertas:
 - Programas bloqueados en proceso de clasificación.
 - Clasificaciones de archivos que han sido permitidos por el administrador.

Estrategias para supervisar la clasificación de ficheros

Muchos departamentos de IT controlan la instalación de programas en los equipos de la red. En estos casos, el administrador puede querer minimizar el impacto del software desconocido en el trabajo de los usuarios, pero sin realizar concesiones en materia de seguridad.

A continuación se presenta una estrategia de instalación del software por etapas, para preparar de antemano la ejecución del software nuevo antes de su instalación y uso masivo:

- Configurar el PC de pruebas.
- Instalar el software.
- Reclasificar los programas bloqueados.
- Enviar el programa directamente a la nube de Panda Security.

Configurar el equipo de pruebas

El objetivo es determinar si el software a utilizar en la red ya es conocido como malware, o es desconocido para Panda Security. Para ello, utiliza el equipo de un usuario de la red o un equipo dedicado en exclusiva a este objetivo. Este equipo debe tener asignada inicialmente una configuración de seguridad avanzada **Hardening**.

Instalar el software

Instala el software y ejecútalo de forma normal. Si Panda Adaptive Defense 360 encuentra algún módulo o programa desconocido, lo bloqueará y mostrará una ventana emergente en el equipo. Además, se añadirá un nuevo elemento en el panel **Programas actualmente bloqueados en clasificación**. Internamente, Panda Adaptive Defense 360 registrará los eventos generados por el uso del programa y enviará los binarios a la nube para poder estudiarlos.

Si no se han presentado bloqueos en el modo Hardening, cambia la configuración a modo Lock y vuelve a ejecutar el programa recién instalado. Si aparecen nuevos bloqueos, el panel **Programas actualmente bloqueados en clasificación** los reflejará.

Reclasificar los programas bloqueados

En el momento en que Panda Adaptive Defense 360 emite una clasificación de los programas bloqueados, se envía una notificación por correo al administrador avisando del desbloqueo si la clasificación es goodwill, o su bloqueo por considerarse una amenaza. Cuando todos los procesos han sido reclasificados como goodwill, el software instalado será apto para su ejecución en el parque informático.

Enviar el programa directamente a la nube de Panda Security

Debido a que Panda Adaptive Defense 360 está preparado para no impactar en el rendimiento de la red en el caso de tener que enviar ficheros a la nube de Panda Security, su envío puede demorarse

en el tiempo. Si quieres acelerar el proceso, ponte el contacto con el departamento de soporte de Panda Security.

Gestión de la zona de backup / cuarentena

La cuarentena en Panda Adaptive Defense 360 es el área de backup donde se copian los elementos clasificados como amenaza que han sido eliminados.

La cuarentena se almacena en el propio equipo del usuario, en el directorio `Quarantine` dentro de la carpeta donde se instaló el software. Se trata de un área cifrada e inaccesible al resto de procesos del equipo, de manera que no es posible el acceso ni la ejecución de los programas allí contenidos de forma directa, si no es a través de la consola Web.



La cuarentena es compatible con las plataformas Windows, macOS y Linux.

El departamento de Panda Labs en Panda Security establece la acción a ejecutar en función de la clasificación y tipo de elemento detectado. De esta forma, se pueden producir las situaciones siguientes:

- **Elementos maliciosos desinfectables:** se desinfectan y se restauran a su ubicación original.
- **Elementos maliciosos no desinfectables:** se mueven a la cuarentena y permanecen allí durante 7 días.
- **Elementos no maliciosos:** si se clasificó de forma errónea un elemento que es *goodware* (falso positivo), se restaura desde la cuarentena automáticamente a su ubicación original.
- **Elementos sospechosos:** se almacena en la cuarentena durante 30 días. Si finalmente resulta ser *goodware*, se restaura automáticamente.



Panda Adaptive Defense 360 no borra ningún fichero del equipo del usuario. Todos los elementos eliminados son enviados al área de backup.

Visualizar los elementos en cuarentena

Para obtener un listado de los elementos introducidos en la cuarentena:

- Haz clic en el menú superior **Estado**, panel lateral **Seguridad**.
- Haz clic en el panel apropiado según el tipo de elemento a restaurar de la cuarentena:
 - Actividad de malware.
 - Actividad de PUP.
 - Actividad de exploits.

- Amenazas detectadas por el antivirus.
- En los filtros del listado haz clic en las casillas de selección **Movido a cuarentena** y **Eliminado** del campo **Acción** y haz clic en el botón **Filtrar**.

Restaurar elementos de cuarentena

- Haz clic en el menú superior **Estado** y en el panel lateral **Seguridad**.
- Haz clic en el panel apropiado según el tipo de elemento a restaurar de la cuarentena:
 - Actividad de malware
 - Actividad de PUPs
 - Actividad de Exploits
 - Amenazas detectadas por el Antivirus
- En el listado, selecciona la amenaza cuyo campo **Acción** muestre **Movido a Cuarentena** o **desinfectado**.
- Haz clic en el icono ⓘ del campo **Acción**. Se mostrará una ventana que explica el motivo del movimiento del elemento a cuarentena.
- Haz clic en el enlace **Restaurar y no volver a detectar**. El elemento se moverá a su ubicación original. Se restaurarán también los permisos, propietario, entradas del registro referidas al fichero y otra información.

Capítulo 21

Análisis forense

Panda Adaptive Defense 360 incorpora un conjunto de tecnologías avanzadas que permiten detectar y bloquear la ejecución del malware desconocido o especialmente diseñado para pasar inadvertido en las estaciones de trabajo y servidores de las compañías. Estas tecnologías recogen una gran cantidad de información sobre las acciones ejecutadas en los equipos del cliente gracias a la monitorización permanente de todos los procesos en funcionamiento. Con esta información es posible determinar hasta qué punto ha sido comprometida la red del cliente, y así poder ayudar al administrador de la red a tomar las medidas apropiadas.

La consola Web pone a disposición del administrador toda esta información a través de varios recursos, dependiendo del grado de detalle que se necesite:

- Páginas de detalle extendido.
- Tablas de acciones.
- Diagramas de grafos.
- Ficheros Excel.

CONTENIDO DEL CAPÍTULO

Detalle de los programas bloqueados	482
Detección del malware	482
Información general	483
Equipo afectado	483
Impacto de la amenaza en el equipo	483
Origen de la infección	484
Apariciones en otros equipos	484
Detección exploit	485
Información general	485
Equipo afectado	486
Impacto del exploit en el equipo	486
Detalle del programa bloqueado	487
Información general	487
Equipo	487
Programa bloqueado	487
Tablas de acciones	487
Sujeto y predicado de las acciones	490
Grafos de ejecución	492
Diagramas	493
Nodos	493

Líneas y flechas 495

La línea temporal (Timeline) 495

Filtros 496

Recolocar los nodos y zoom general del grafo 496

Ficheros exportados Excel --496

Interpretación de las tablas de acciones y grafos --499

Ejemplo 1: actividad del malware Trj/OCJ.A 499

Ejemplo 2: comunicación con equipos externos en BetterSurf 501

Ejemplo 3: acceso al registro con PasswordStealer.BT 502

Ejemplo 4: acceso a datos confidenciales en Trj/Chgt.F 503

Detalle de los programas bloqueados

Panda Adaptive Defense 360 permite visualizar el detalle extendido de los programas cuando son bloqueados por alguna de las tecnologías de detección avanzada que incorpora.

Para acceder al detalle extendido de las amenazas avanzadas haz clic en el menú superior **Estado**, añade uno de los listados mostrados a continuación y haz clic en uno de los elementos del listado:

- **Actividad de Malware y PUPs** para abrir la ventana **Detección del malware**.
- **Actividad de Exploits** para abrir la ventana **Detección de exploit**.
- **Programas actualmente bloqueados en clasificación** para abrir la ventana **Detalles del programa bloqueado**.
- **Programas bloqueados por el administrador** para abrir la ventana **Detalle del programa bloqueado**.

Dependiendo del tipo de amenaza se añadirá la pestaña **Detalles** a la ventana para mostrar información extendida.

Detección del malware

La ventana se divide en secciones siguientes:

- Información general.
- Equipo afectado.
- Impacto de la amenaza en el equipo.
- Origen de la infección.
- Apariciones en otros equipos.

Información general

Campo	Descripción
Amenaza	Nombre de la amenaza y hash que la identifica.
Acción	Tipo de acción que Panda Adaptive Defense 360 ha ejecutado sobre el elemento. • Movido a Cuarentena. • Bloqueado. • Desinfectado. • Eliminado.

Tabla 21.1: Campos de la sección Información general en Detección de malware, PUP y programas bloqueados en clasificación

Equipo afectado



Consulta [“Gestión de amenazas, elementos en clasificación y cuarentena”](#) para obtener información sobre las acciones que el administrador puede ejecutar sobre los elementos encontrados.

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Visualizar parches disponibles	Si el módulo Panda Patch Management está activado muestra los parches y actualizaciones pendientes de instalar en el equipo.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Modo de protección	Configuración de la protección avanzada en el momento de producirse la detección (Audit, Hardening, Lock).
Ruta de detección	Ruta del sistema de ficheros donde reside la amenaza.

Tabla 21.2: Campos de la sección Equipo afectado en Detección de malware, PUP y programas bloqueados en clasificación

Impacto de la amenaza en el equipo

Campo	Descripción
Amenaza	Nombre de la amenaza detectada y cadena resumen de identificación del archivo (hash). Haz clic en los dos botones para ampliar información en Internet mediante el buscador Google y la web de Virustotal. Si la amenaza es de reciente aparición se mostrará la leyenda Nueva amenaza .

Tabla 21.3: Campos de la sección Impacto de la amenaza en el equipo en Detección de malware, PUP y programas bloqueados en clasificación

Campo	Descripción
Actividad	Resumen de las acciones más importantes ejecutadas por el malware: • Se ha ejecutado ⚡ • Ha accedido a datos 📄 • Ha intercambiado datos con otros equipos 🌐 • Ver detalle de actividad completo: al hacer clic se muestra la pestaña Actividad tratada en “Tablas de acciones”. • Ver gráfica de actividad: al hacer clic se muestra la gráfica de Actividad tratada en “Grafos de ejecución”.
Fecha de detección	Fecha en la que Panda Adaptive Defense 360 detectó la amenaza en la red del cliente.
Tiempo de exposición	Tiempo que la amenaza ha permanecido sin clasificar en la red del cliente.

Tabla 21.3: Campos de la sección Impacto de la amenaza en el equipo en Detección de malware, PUP y programas bloqueados en clasificación

Origen de la infección

Campo	Descripción
Equipo origen de la amenaza	Si el intento de infección viene de un equipo de la red del cliente, indica el nombre del equipo.
IP origen de la amenaza	Si el intento de infección viene de un equipo de la red del cliente, indica la dirección IP del equipo.
Usuario origen de la amenaza	Usuario conectado en la máquina origen de la infección.

Tabla 21.4: Campos de la sección Origen de la infección en Detección de malware, PUP y programas bloqueados en clasificación

Apariciones en otros equipos

Muestra todos los equipos de la red donde fue visto el malware detectado.

Campos	Descripción
Equipo	Nombre del equipo.
Ruta del archivo	Ruta y nombre del fichero que contiene el malware.
Fecha primera aparición	Fecha en la que la amenaza fue detectada por primera vez en ese equipo.

Tabla 21.5: Campos de la sección Apariciones en otros equipos en Detección de malware, PUP y programas bloqueados en clasificación

Detección exploit

La ventana se divide en 5 secciones:

- Información general.
- Equipo afectado.
- Impacto de la amenaza en el equipo.
- Origen de la infección.
- Apariciones en otros equipos.

Información general

Campo	Descripción	Valores
Programa comprometido	Nombre del programa que recibió el intento de explotación de una vulnerabilidad y hash que lo identifica.	• Ruta: ruta del programa afectado por el exploit. • Versión: versión del programa afectado por el exploit. • Hash: hash del programa afectado por el exploit.
Técnica	Identificador de la técnica utilizada para explotar las vulnerabilidades de los programas.	Enlace a la descripción de la técnica utilizada por el exploit.
Acción	Muestra el tipo de acción que Panda Adaptive Defense 360 ha ejecutado sobre el programa afectado por el exploit. • Permitido: la protección anti-exploit está configurada en modo Audit. El exploit se ejecutó. • Bloqueado: el exploit fue bloqueado antes de su ejecución. • Permitido por el usuario: se preguntó al usuario del equipo si finalizar el proceso comprometido y el usuario decidió permitir que el exploit continúe ejecutándose.	Enumeración Consulta "Permitir ejecutar elementos clasificados como malware, PUP o Exploit" en la página 461 para obtener información de como gestionar los bloqueos de la amenazas detectadas.

Tabla 21.6: Campos de la sección Información general en Detección exploit

Campo	Descripción	Valores
	• Proceso finalizado: el exploit fue eliminado, pero se llegó a ejecutar parcialmente. • Pendiente de reinicio: se informó al usuario del equipo de la necesidad de reiniciar el equipo para eliminar completamente el exploit. Mientras tanto el exploit se seguirá ejecutando.	

Tabla 21.6: Campos de la sección Información general en Detección exploit

Equipo afectado

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.
Ruta del programa comprometido	Ruta del programa que recibió el intento de explotación de una vulnerabilidad.

Tabla 21.7: Campos de la sección Equipo afectado en Detección exploit

Impacto del exploit en el equipo

Campo	Descripción
Programa comprometido	Ruta y nombre del programa que recibió el intento de explotación. Si Panda Adaptive Defense 360 detectó que el programa no está actualizado a la última versión publicada por el proveedor, mostrará el aviso  Programa vulnerable .
Actividad	• Se ha ejecutado : el exploit se llegó a ejecutar antes de ser detectado por Panda Adaptive Defense 360. • Ver detalle de actividad completo: al hacer clic se muestra la pestaña Actividad tratada en "Tablas de acciones". • Ver gráfica de actividad: al hacer clic se muestra la gráfica de Actividad tratada en "Grafos de ejecución".
Fecha de detección	Fecha en la que Panda Adaptive Defense 360 detectó el exploit en la red del cliente.
Posible origen del exploit	Ruta y nombre del programa que posiblemente inició el exploit.

Tabla 21.8: Campos de la sección Impacto del exploit en el equipo en Detección exploit

Detalle del programa bloqueado

La ventana se divide en las secciones siguientes:

- Información general.
- Equipo.
- Programa bloqueado.

Información general

Campo	Descripción
Programa bloqueado	Nombre del programa bloqueado por el administrador.

Tabla 21.9: Campos de la sección Información general en Detalle del programa bloqueado

Equipo

Campo	Descripción
Equipo	Nombre del equipo donde se detectó la amenaza, dirección IP y carpeta a la que pertenece en el árbol de grupos.
Usuario logueado	Usuario del sistema operativo bajo el cual se cargó y ejecutó o la amenaza.

Tabla 21.10: Campos de la sección Equipo en Detalle del programa bloqueado

Programa bloqueado

Campo	Descripción
Nombre	Nombre del programa bloqueado por el administrador.
Ruta	Ruta del programa bloqueado por el administrador dentro del equipo del usuario o servidor.
Hash	Hash del programa bloqueado por el administrador.
Fecha de detección	Fecha en la que Panda Adaptive Defense 360 bloqueó la ejecución del programa.

Tabla 21.11: Campos de la sección Programa bloqueado en Detalle del programa bloqueado

Tablas de acciones

Panda Adaptive Defense 360 permite visualizar las acciones de los programas cuando son detectados por alguna de las tecnologías de detección avanzada que incorpora.

Para acceder a la tabla de acciones de las amenazas avanzadas haz clic en el menú superior **Estado**, añade uno de los listados mostrados a continuación y haz clic en uno de los elementos del listado:

- **Actividad de Malware y PUPs** para abrir la ventana **Detección del malware**.
- **Actividad de Exploits** para abrir la ventana **Detección de exploit**.
- **Programas actualmente bloqueados en clasificación** para abrir la ventana **Detalles del programa bloqueado**.
- **Bloqueos por políticas avanzadas de seguridad** para abrir la ventana **Bloqueo por política avanzada de seguridad**.

Haz clic en la pestaña **Actividad** para mostrar la tabla de acciones de la amenaza.

La información de la amenaza se muestra en una tabla de acciones, que incluye los eventos producidos más relevantes.



La cantidad de acciones ejecutadas por un proceso es muy alta, visualizarlas todas dificultaría la extracción de información útil para realizar un análisis forense.

El contenido de la tabla se presenta inicialmente ordenado por fecha, de esta forma es más fácil seguir el curso de la amenaza.

La tabla de acciones contiene los campos mostrados a continuación:

Campo	Comentario	Valores
Fecha	Fecha de la acción registrada.	Fecha
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado.	Numérico
Acción	Tipo de acción registrada en el sistema y línea de comandos asociada a la ejecución de la acción.	• Descargado de • Comunica con • Accede a datos • Accede • Es accedido por • LSASS.EXE abre • LSASS.EXE es abierto por • Es ejecutado por • Ejecuta • Es creado por

Tabla 21.12: Campos de la tabla de acciones de una amenaza

Campo	Comentario	Valores
		• Crea • Es modificado por • Modifica • Es cargado por • Carga • Es borrado por • Borra • Es renombrado por • Renombra • Es matado por • Mata proceso • Proceso suspendido • Crea hilo remoto • Hilo inyectado por • Es abierto por • Abre • Crea • Es creado por • Crea clave apuntando a Exe • Modifica clave apuntando a Exe. • Intenta detener • Finalizado por
Path/URL/ Clave de Registro / IP:Puerto	Entidad de la acción. Según el tipo de acción contiene diferentes valores.	• Clave del registro: acciones que impliquen modificación del registro de Windows. • IP:Puerto: acciones que implican una comunicación con un equipo local o remoto. • Path: acciones que implican acceso al disco duro del equipo. • URL: acciones que implican el acceso a una URL.

Tabla 21.12: Campos de la tabla de acciones de una amenaza

Campo	Comentario	Valores
Hash del Fichero/Valor del Registro / Protocolo-Dirección/ Descripción	Campo que complementa a la entidad.	• Hash del Fichero: para todas las acciones que implican acceso a un fichero. • Valor del Registro: para todas las acciones que implican un acceso al registro. • Protocolo-Dirección: para todas las acciones que implican una comunicación con un equipo local o remoto. Los valores posibles son: • TCP • UDP • Bidirectional • Unknown • Descripción
Confiable	El fichero está firmado digitalmente.	Binario

Tabla 21.12: Campos de la tabla de acciones de una amenaza

Sujeto y predicado de las acciones

El formato utilizado para presentar la información en el listado de acciones mantiene cierto paralelismo con el lenguaje natural:

- Todas las acciones tienen como sujeto el fichero clasificado como amenaza. Este dato no se indica en cada línea de la tabla de acciones porque es común para todas las líneas.
- Todas las acciones tienen un verbo que relaciona el sujeto (la amenaza clasificada) con un complemento, llamado entidad. La entidad se corresponde con el campo **Path/URL/Clave de Registro /IP:Puerto** de la tabla.
- La entidad se complementa con un segundo campo que añade información a la acción, indicado en el campo **Hash del Fichero/Valor del Registro /Protocolo-Dirección/Descripción**.

En la tabla 21.13 se muestran dos acciones de ejemplo de un mismo malware hipotético:

Fecha	Nº veces	Acción	Path/URL/ Registro/IP	Hash/Registro/ Protocolo/Descripción	Confiable
3/30/ 2015 4:38:40 PM	1	Comunica con	54.69.32.99:80	TCP-Bidirectional	NO
3/30/ 2015 4:38:45 PM	1	Carga	PROGRAM_FILES \ MOVIES TOOLBAR\SAFETYNTN	9994BF035813FE8EB6BC98 E CCBD5B0E1	NO

Tabla 21.13: Listado de acciones de una amenaza de ejemplo

La primera acción indica que el malware (sujeto) se conecta (Acción **Comunica con**) con la dirección IP 54.69.32.99:80 (entidad) mediante el protocolo TCP-Bidireccional.

La segunda acción indica que el malware (sujeto) carga (Acción **Carga**) la librería PROGRAM_FILES\MOVIES TOOLBAR\SAFETYNTN\SAFETYCRT.DLL con hash 9994BF035813FE8EB6BC98ECCBD5B0E1.

Al igual que en el lenguaje natural, en Panda Adaptive Defense 360 se implementan dos tipos de oraciones:

- **Activa:** son acciones predicativas (con un sujeto y un predicado) relacionados por un verbo en forma activa. En estas acciones, el verbo de la acción relaciona el sujeto, que siempre es el proceso clasificado como amenaza y un complemento directo, la entidad, que puede ser de múltiples tipos según la acción. Ejemplos de acciones activas son:
 - Comunica con
 - Carga
 - Crea
- **Pasiva:** son acciones donde el sujeto (el proceso clasificado como amenaza) pasa a ser sujeto paciente (que recibe la acción, no la ejecuta) y el verbo aparece en forma pasiva (ser + participio). En este caso el verbo pasivo relaciona el sujeto pasivo que recibe la acción con la entidad, que es la que ejecuta la acción. Ejemplos de acciones pasivas son:
 - Es creado por
 - Descargado de

La tabla 21.14 muestra una acción pasiva de ejemplo para un malware hipotético:

Fecha	Nº veces	Acción	Path/URL/ Registro/IP	Hash/Registro/ Protocolo/Descripción	Confiable
3/30/2015 4:51:46 PM	1	Es ejecutado por	WINDOWS \explorer.exe	7522F548A84ABAD8FA516D E5AB3931EF	NO

Tabla 21.14: Ejemplo de acción pasiva

En esta acción el malware (sujeto pasivo) es ejecutado (acción pasiva **Es ejecutado por**) por el programa WINDOWS | \explorer.exe (entidad) de hash 7522F548A84ABAD8FA516DE5AB3931EF.



Las acciones de tipo activa permiten inspeccionar en detalle los pasos que ha ejecutado la amenaza. Por el contrario, las acciones de tipo pasivo suelen reflejar el vector de infección utilizado por el malware (qué proceso lo ejecutó, qué proceso lo copió al equipo del usuario etc.).

Grafos de ejecución

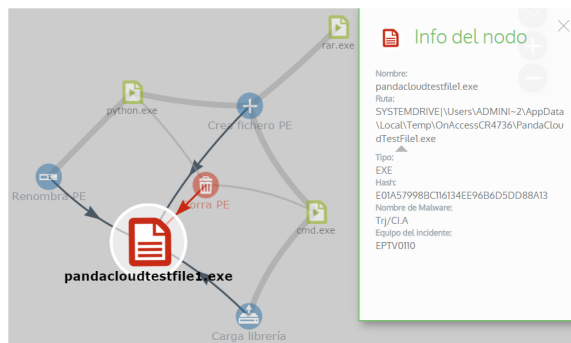


Figura 21.1: Amenaza representada mediante grafos

Panda Adaptive Defense 360 permite visualizar las acciones de los programas en un grafo cuando son detectados por alguna de las tecnologías de detección avanzada que incorpora.

Para acceder al grafo de ejecución de las amenazas avanzadas haz clic en el menú superior **Estado**, añade uno de los listados mostrados a continuación y haz clic en uno de los elementos del listado:

- **Actividad de Malware y PUPs** para abrir la ventana **Detección del malware**.
- **Actividad de Exploits** para abrir la ventana **Detección de exploit**.
- **Programas actualmente bloqueados en clasificación** para abrir la ventana **Detalles del programa bloqueado**.
- **Bloqueos por políticas avanzadas de seguridad** para abrir la ventana **Bloqueo por política avanzada de seguridad**.

Haz clic en la pestaña **Actividad** y **Ver gráfica de actividad** para mostrar el grafo de ejecución de la amenaza.

Los grafos de ejecución representan de forma visual la información mostrada en las tablas de acciones, poniendo énfasis en el enfoque temporal. Los grafos se utilizan inicialmente para tener, de un solo vistazo, una idea general de las acciones desencadenadas por la amenaza.

Diagramas

La cadena de acciones en la vista de grafos de ejecución se representa mediante dos elementos:

- **Nodos:** en su mayoría acciones o elementos informativos.
- **Líneas y flechas:** unen los nodos de acción e informativos para establecer un orden temporal y asignar a cada nodo el rol de “sujeto” o “predicado”.

Nodos

Muestran la información mediante su icono asociado, color y un panel descriptivo que se muestra a la derecha de la pantalla cuando se seleccionan con el ratón.

El código de colores utilizado es:

- **Rojo:** elemento no confiable, malware, amenaza.
- **Naranja:** elemento desconocido, no catalogado.
- **Verde:** elemento confiable, goodwill.

La tabla 21.15 lista los nodos de tipo acción junto con una breve descripción:

Símbolo	Descripción	Símbolo	Descripción
	• Fichero descargado. • Fichero comprimido creado.		Fichero ejecutable borrado.
	Socket / comunicación usada.		Librería cargada.
	La monitorización comenzó.		Servicio instalado.
	Proceso creado.		Fichero ejecutable renombrado.

Tabla 21.15: Representación gráfica de acciones en el diagrama de grafos

Símbolo	Descripción	Símbolo	Descripción
	- Fichero ejecutable creado. - Librería creada. - Clave en el registro creada.		Proceso detenido o cerrado.
	- Fichero ejecutable modificado. - Clave de registro modificada.		Hilo creado remotamente.
	Fichero ejecutable mapeado para escritura.		Fichero comprimido abierto.

Tabla 21.15: Representación gráfica de acciones en el diagrama de grafos

La tabla 21.16 lista los nodos de tipo descriptivo junto con una breve descripción:

Símbolo	Descripción
	Nombre de fichero y extensión. Verde: goodwill. Naranja: no catalogado. Rojo: malware/PUP.
	Equipo interno (está en la red corporativa). Verde: confiable. Naranja: desconocido. Rojo: no confiable.
	Equipos externos. Verde: confiable. Naranja: desconocido. Rojo: no confiable.
	País asociado a la IP de un equipo externo.
	Fichero y extensión.
	Clave del registro.

Tabla 21.16: Tipos de nodo en el diagrama de grafos

Líneas y flechas

Las líneas del diagrama de grafos relacionan los diferentes nodos y ayudan a establecer visualmente el orden de ejecución de las acciones.

Los dos atributos de una línea son:

- **Grosor de la línea:** número de veces que ha aparecido la relación en el diagrama. A mayor número de veces mayor tamaño de la línea.
- **Flecha:** dirección de la relación entre los dos nodos.

La línea temporal (Timeline)

Controla la visualización de la cadena de acciones ejecutadas por la amenaza a lo largo del tiempo. Mediante los botones situados en la parte inferior de la pantalla visualiza el momento preciso donde la amenaza ejecutó cierta acción, y recupera información extendida para ayudar en los procesos de análisis forense.

Es posible seleccionar un intervalo concreto de la línea temporal arrastrando los selectores de intervalo hacia la izquierda o derecha para abarcar la franja más interesante.

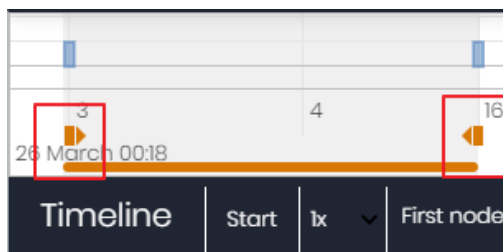


Figura 21.2: Selectores del intervalo temporal a presentar

Una vez seleccionado el intervalo, el grafo mostrará únicamente las acciones y nodos que caigan en dentro de él. El resto de acciones y nodos quedará difuminado en el diagrama.

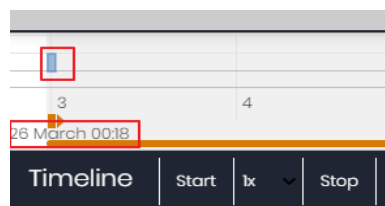


Figura 21.3: Timestamp, fecha y acciones de la amenaza

Las acciones de la amenaza se representan en la línea temporal como barras verticales acompañadas del time stamp, que marca la hora y minuto donde ocurrieron.

Para poder ver la ejecución completa de la amenaza y la cadena de acciones que ejecutó, se utilizan los siguientes controles:

- **Iniciar:** comienza la ejecución de la Timeline a velocidad 1x.

Los grafos y las líneas de acciones irán apareciendo según se vaya recorriendo la línea temporal.

- **1x:** establece la velocidad de recorrido de la línea temporal.
- **Detener:** detiene la ejecución de la línea temporal.
- **+ y -:** zoom in y zoom out de la línea temporal.
- **< y >:** mueve la selección del nodo al inmediatamente anterior o posterior.

- **Zoom inicial:** recupera el nivel de zoom inicial si se modificó con los botones + y –.
- **Seleccionar todos los nodos:** mueve los selectores temporales para abarcar toda la línea temporal.
- **Primer nodo:** establece el intervalo temporal en el inicio, paso necesario para iniciar la visualización de la Timeline completa.



Para poder visualizar el recorrido completo de la Timeline primero selecciona "Primer nodo" y después "Iniciar". Para ajustar la velocidad de recorrido selecciona el botón 1x.

Filtros

En la parte superior del diagrama de grafos se encuentran los controles para filtrar la información que se mostrará.

- **Acción:** desplegable que selecciona un tipo de acción de entre todas las ejecutadas por la amenaza. El diagrama solo mostrará los nodos que coincidan con el tipo de acción seleccionada y aquellos nodos adyacentes relacionados con esta acción.
- **Entidad:** desplegable que selecciona una entidad (contenido del campo Path/URL/Entrada de registro /IP:Puerto).

Recolocar los nodos y zoom general del grafo

Para mover el grafo en las cuatro direcciones y hacer zoom in o zoom out utiliza los controles situados en la parte superior derecha del grafo.



Para hacer zoom in y zoom out más fácilmente utiliza la rueda central del ratón.

- El símbolo abandona la vista de grafos.
- Para ocultar la zona de botones Timeline a fin de ganar espacio de la pantalla haz clic en el icono situado en la parte inferior derecha del grafo.
- El comportamiento del grafo representando en pantalla es configurable mediante el panel accesible al seleccionar el botón situado en la zona superior izquierda del grafo.

Ficheros exportados Excel

Panda Adaptive Defense 360 permite exportar a un fichero Excel el detalle extendido de los programas cuando son detectados por alguna de las tecnologías de detección avanzada que incorpora.

Para obtener el fichero Excel con el detalle extendido de las amenazas avanzadas detectadas sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Estado y** añade uno de los listados siguientes:
 - **Actividad de Malware y PUPs.**
 - **Actividad de Exploits.**
 - **Programas actualmente bloqueados en clasificación.**
- Haz clic en el menú de contexto situado en la parte superior derecha del listado y elige la opción **Exportar listado y detalles.** Se descargará un fichero Excel con los detalles extendidos de todas las amenazas mostradas en el listado.

Campo	Descripción	Valores
Fecha	Fecha de la acción registrada.	Fecha
Hash	Cadena resumen de identificación de la amenaza.	Cadena de caracteres
Amenaza	Nombre de la amenaza.	Cadena de caracteres
Usuario	Cuenta de usuario bajo la cual se ejecutó la amenaza.	Cadena de caracteres
Equipo	Nombre del equipo donde se encontró la amenaza.	Cadena de caracteres
Ruta	Nombre de la amenaza y ruta en el equipo del usuario.	Cadena de caracteres
Acceso a datos	La amenaza ha accedido a ficheros que residen en el equipo del usuario.	Binario
Acción	Tipo de acción registrada en el sistema.	• Descargado de • Comunica con • Accede a datos • Accede • Es accedido por • LSASS.EXE abre • LSASS.EXE es abierto por • Es ejecutado por • Ejecuta • Es creado por • Crea • Es modificado por • Modifica • Es cargado por • Carga • Es borrado por

Tabla 21.17: Campos del fichero exportado Listado y detalles

Campo	Descripción	Valores
		• Borra • Es renombrado por • Renombra • Es matado por • Mata proceso • Proceso suspendido • Crea hilo remoto • Hilo inyectado por • Es abierto por • Abre • Crea • Es creado por • Crea clave apuntando a Exe • Modifica clave apuntando a Exe • Intenta detener • Finalizado por
Línea de comandos	Línea de comandos asociada a la ejecución de la acción.	Cadena de caracteres
Fecha del evento	Fecha y hora en la que el evento se registró en el equipo del cliente.	Cadena de caracteres
Nº veces	Número de veces que se ejecutó la acción. Una misma acción ejecutada varias veces de forma consecutiva solo aparece una vez en el listado de acciones con el campo Nº veces actualizado.	Numérico
Path/URL/Clave de Registro / IP:Puerto	Entidad de la acción. Según sea el tipo de acción podrá contener diferentes valores.	• Clave del registro: acciones que implican modificación del registro de Windows. • IP:Puerto: acciones que implican una comunicación con un equipo local o remoto. • Path: acciones que implican acceso al disco duro del equipo. • URL: acciones que implican el acceso a una URL.

Tabla 21.17: Campos del fichero exportado Listado y detalles

Campo	Descripción	Valores
Hash del Fichero/Valor del Registro / Protocolo-Dirección/ Descripción	Campo que complementa a la entidad.	• Hash del Fichero: acciones que implican acceso a un fichero. • Valor del Registro: acciones que implican un acceso al registro. • Protocolo-Dirección: acciones que implican una comunicación con un equipo local o remoto. Los valores posibles son: • TCP • UDP • Bidirectional • UnKnown • Descripción
Confiable	El fichero está firmado digitalmente.	Binario

Tabla 21.17: Campos del fichero exportado Listado y detalles

Interpretación de las tablas de acciones y grafos

Las tablas de acciones y grafos de actividad son representaciones de los volcados de evidencias recogidas en el equipo del usuario, que deberán ser interpretadas por el administrador de la red. Por esta razón se requieren ciertos conocimientos técnicos para poder extraer pautas e información clave en cada situación.

A continuación, se ofrecen unas directrices básicas para interpretar las tablas de acciones mediante varios ejemplos de amenazas reales.



El nombre de las amenazas aquí indicadas puede variar entre diferentes proveedores de seguridad. Para identificar un malware concreto se recomienda utilizar su hash.

Ejemplo 1: actividad del malware Trj/OCJ.A

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso los datos relevantes son los siguientes:

- **Amenaza:** Trj/OCJ.A

- **Equipo:** XP-BARCELONA1
- **Ruta de detección:** TEMP|\Rar\$EXa0.946\appnee.com.patch.exe

- **Actividad**

La pestaña **Actividad** contiene acciones ya que el modo de Panda Adaptive Defense 360 configurado era Hardening y el malware ya residía en el equipo en el momento en que Panda Adaptive Defense 360 se instaló, siendo desconocido en el momento de su ejecución.

- **Hash**

Con la cadena de hash se podrá obtener más información de recursos web como Virus total para tener una idea general de la amenaza y funcionamiento.

- **Ruta de detección**

La ruta donde se detectó el malware por primera vez en el equipo pertenece a un directorio temporal y contiene la cadena RAR: la amenaza procede de un fichero empaquetado que el programa WinRAR descomprimió temporalmente en el directorio, y dió como resultado el ejecutable appnee.com.patch.exe.

- **Pestaña Actividad**

Paso	Fecha	Acción	Ruta
1	3:17:00	Es creado por	PROGRAM_FILES \WinRAR\WinRAR.exe
2	3:17:01	Es ejecutado por	PROGRAM_FILES \WinRAR\WinRAR.exe
3	3:17:13	Crea	TEMP \bassmod.dll
4	3:17:34	Crea	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\AMTLIB.DLL.BAK
5	3:17:40	Modifica	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\amtlib.dll
6	3:17:40	Borra	PROGRAM_FILES \ADOBE\ACROBAT 11.0\ACROBAT\AMTLIB.DLL.BAK
7	3:17:41	Crea	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\ACROBAT.DLL.BAK
8	3:17:42	Modifica	PROGRAM_FILES \Adobe\ACROBAT 11.0\Acrobat\Acrobat.dll
9	3:17:59	Ejecuta	PROGRAM_FILES \Google\ Chrome\Application\chrome.exe

Tabla 21.18: Listado de acciones Trj/OCJ.A

Los pasos 1 y 2 indican que el malware fue descomprimido por el WinRAR.Exe y ejecutado desde el mismo programa: el usuario abrió el fichero comprimido e hizo clic en el binario que contiene.

Una vez en ejecución, en el paso 3 el malware crea una dll (bassmod.dll) en una carpeta temporal y otra (paso 4) en el directorio de instalación del programa Adobe Acrobat 11. En el paso 5 también modifica una dll de Adobe, quizá para aprovechar algún tipo de exploit del programa.

Después de modificar otras dlls lanza una instancia de Chrome y en ese momento termina la Timeline; Panda Adaptive Defense 360 catalogó el programa como amenaza después de esa cadena de acciones sospechosas y detuvo su ejecución.

En la Timeline no aparecen acciones sobre el registro, de modo que es muy probable que el malware no sea persistente o no haya podido ejecutarse hasta el punto de sobrevivir a un reinicio del equipo.

El programa Adobe Acrobat 11 ha resultado comprometido, de modo que se recomienda su reinstalación. Gracias a que Panda Adaptive Defense 360 monitoriza ejecutables tanto si son goodwill como malware, la ejecución de un programa comprometido será detectada en el momento en que desencadene acciones peligrosas, terminando en su bloqueo.

Ejemplo 2: comunicación con equipos externos en BetterSurf

BetterSurf es un programa potencialmente no deseado que modifica el navegador instalado en el equipo del usuario e inyecta anuncios en las páginas Web que visite.

En la pestaña **Detalles** se muestra la información fundamental del malware encontrado. En este caso se cuenta con los siguientes datos:

- **Nombre:** PUP/BetterSurf
- **Equipo:** MARTA-CAL
- **Ruta de detección:** PROGRAM_FILES\VEROBLOCKANDSURF\N4CD190.EXE
- **Tiempo de permanencia:** 11 días 22 horas 9 minutos 46 segundos
- **Tiempo de exposición**

En este caso el tiempo de exposición ha sido muy largo: durante casi 12 días el malware ha estado latente en la red del cliente. Este comportamiento es cada vez más usual, y puede deberse a varios motivos: que el malware no haya realizado ninguna acción sospechosa hasta muy tarde, o que simplemente el usuario descargó el fichero, pero tardó en ejecutarlo. En ambos casos la amenaza no era conocida anteriormente, con lo cual no se disponía de una firma con la que el sistema antivirus pueda compararla.

- **Pestaña Actividad**

Paso	Fecha	Acción	Ruta
1	08/03/2015 11:16	Es creado por	TEMP\08c3b650-e9e14f.exe
2	18/03/2015 11:16	Es creado por	SYSTEM\services.exe
3	18/03/2015 11:16	Carga	PROGRAM_FILES\VEROBLOF\N4Cd190.dll

Tabla 21.19: Listado de acciones PUP/BetterSurf

Paso	Fecha	Acción	Ruta
4	18/03/2015 11:16	Carga	SYSTEM \BDL.dll
5	18/03/2015 11:16	Comunica con	127.0.0.1:13879
6	18/03/2015 11:16	Comunica con	37.58.101.205:80
7	18/03/2015 11:17	Comunica con	5.153.39.133:80
8	18/03/2015 11:17	Comunica con	50.97.62.154:80
9	18/03/2015 11:17	Comunica con	50.19.102.217:80

Tabla 21.19: Listado de acciones PUP/BetterSurf

Se puede apreciar como el malware establece comunicación con varias IPs. La primera de ellas (paso 5) es el propio equipo y el resto son IPs del exterior a las que se conecta por el puerto 80, de las cuales probablemente se descarguen los contenidos de publicidad.

La principal medida de prevención en este caso será bloquear las IPs en el cortafuegos corporativo.



Antes de añadir reglas para el bloqueo de IPs en el cortafuegos corporativo se recomienda consultar las IPs a bloquear en el RIR asociado (RIPE, ARIN, APNIC etc.) para comprobar la red del proveedor al que pertenecen. En muchos casos la infraestructura remota utilizada por el malware es compartida con servicios legítimos alojados en proveedores, tales como Amazon y otros, de modo que bloquear IPs equivaldría a bloquear también el acceso a páginas Web legítimas.

Ejemplo 3: acceso al registro con PasswordStealer.BT

PasswordStealer.BT es un troyano que registra la actividad del usuario en el equipo y envía la información obtenida al exterior. Entre otras cosas, es capaz de capturar la pantalla del usuario, registrar las teclas pulsadas y enviar ficheros a un servidor C&C (Command & Control).

En la pestaña **Detalles** se muestra la información fundamental de la amenaza encontrada. En este caso se cuenta con los siguientes datos relevantes:

- **Ruta de la detección:** APPDATA|\microsoftupdates\micupdate.exe

Por el nombre y la localización del ejecutable, el malware se hace pasar por una actualización de Microsoft. Este malware en concreto no tiene capacidad para contagiar equipos por sí mismo, requiere que el usuario ejecute de forma manual la amenaza.

- **Pestaña Actividad**

El modo de Panda Adaptive Defense 360 configurado era Hardening; el malware ya residía en el equipo en el momento en que Panda Adaptive Defense 360 se instaló y era desconocido en el momento de su ejecución.

- **Tabla de acciones**

Paso	Fecha	Acción	Ruta
1	31/03/2015 23:29	Es ejecutado por	PROGRAM_FILESX86 \internet explorer\iexplore.exe
2	31/03/2015 23:29	Es creado por	INTERNET_CACHE \Content.IE5\QGV8PV80\ index[1].php
3	31/03/2015 23:30	Crea clave apuntando a Exe	\REGISTRY\USER\S-1-5[...]9-5659\Software\Microsoft\Windows\CurrentVersion\Run?MicUpdate
4	31/03/2015 23:30	Ejecuta	SYSTEMX86 \notepad.exe
5	31/03/2015 23:30	Hilo inyectado por	SYSTEMX86 \notepad.exe

Tabla 21.20: Listado de acciones PasswordStealer.BT

En este caso el malware es creado en el paso 2 por una página Web y ejecutado por el navegador Internet Explorer.



El orden de las acciones tiene una granularidad de 1 microsegundo. Por esta razón, las acciones ejecutadas dentro del mismo microsegundo pueden aparecer desordenadas en la Timeline, como sucede en el paso 1 y paso 2.

Una vez ejecutado, el malware se hace persistente en el equipo del usuario en el paso 3, añadiendo una rama en el registro que lanzará el programa en el inicio del sistema. Después comienza a ejecutar acciones propias del malware, tales como arrancar un notepad e inyectar código en uno de sus hilos.

Como acción de resolución en este caso, y en ausencia de un método de desinfección conocido, se puede minimizar el impacto de este malware borrando la entrada del registro. Es muy posible que en un equipo infectado el malware impida modificar dicha entrada; dependiendo del caso sería necesario arrancar el equipo en modo seguro o con un CD de arranque para borrar dicha entrada.

Ejemplo 4: acceso a datos confidenciales en Trj/Chgt.F

Trj/Chgt.F fue publicado por wikileaks a finales de 2014 como herramienta utilizada por las agencias gubernamentales de algunos países para realizar espionaje selectivo.

En este ejemplo se muestra directamente a la pestaña **Actividad** para observar el comportamiento de esta amenaza avanzada.

- **Tabla de acciones**

Paso	Fecha	Acción	Ruta
1	4/21/2015 2:17:47	Es ejecutado por	SYSTEMDRIVE \Python27\pythonw.exe

Tabla 21.21: Listado de acciones Trj/Chgt.F

Paso	Fecha	Acción	Ruta
2	4/21/2015 2:18:01	Accede a datos	#.XLS
3	4/21/2015 2:18:01	Accede a datos	#.DOC
4	4/21/2015 2:18:03	Crea	TEMP \doc.scr
5	4/21/2015 2:18:06	Ejecuta	TEMP \doc.scr
6	4/21/2015 2:18:37	Ejecuta	PROGRAM_FILES\Microsoft Office\Office12\WINWORD.EXE
7	4/21/2015 8:58:02	Comunica con	192.168.0.1:2042

Tabla 21.21: Listado de acciones Trj/Chgt.F

Inicialmente el malware es ejecutado por el intérprete de Python (paso 1) para luego acceder a un documento de tipo Excel y otro de tipo Word (paso 2 y 3). En el paso 4 se ejecuta un fichero de extensión `scr`, probablemente un salvapantallas con algún tipo de fallo o error que provoque una situación anómala en el equipo aprovechada por el malware.

En el paso 7 se produce una conexión de tipo TCP. La dirección IP es privada de modo que se estaría conectando a la red del propio cliente.

En este caso se deberá comprobar el contenido de los ficheros accedidos para evaluar la pérdida de información, aunque viendo la Timeline la información accedida no parece haber sido extraída de la red del cliente.

Panda Adaptive Defense 360 desinfectará por sí mismo la amenaza y bloqueará de forma automática posteriores ejecuciones del malware en este y en otros clientes.

Capítulo 22

Alertas

El sistema de alertas es un recurso utilizado por Panda Adaptive Defense 360 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:

- Detección de malware, PUP o exploits.
- Detección de ataques de red.
- Intento de uso de dispositivos externos no autorizados
- Reclasificación de elementos desconocidos, malware o PUP.
- Bloqueo de procesos desconocidos para Panda Adaptive Defense 360 y en proceso de clasificación.
- Cambios en el estado de las licencias.
- Errores de instalación y desprotegidos.

CONTENIDO DEL CAPÍTULO

Alertas por correo	505
Acceso a la configuración de alertas	506
Configuración de alertas	506
Nivel de acceso del administrador y envío de alertas	506
Cambios de estado (1)	510
Dejar de recibir alertas por correo	511

Alertas por correo

Son mensajes generados por Panda Adaptive Defense 360 cuando se producen determinados eventos y enviados a las cuentas de correo configuradas como destinatarios, generalmente mantenidas por los administradores de la red.

Acceso a la configuración de alertas

Desde el menú superior **Configuración**, en el panel de la izquierda **Mis alertas** se accede al menú de **Alertas** por correo en el que se establecen las opciones de las alertas por correo.

Configuración de alertas

La configuración de las alertas se divide en tres partes:

- **Enviar alertas en los siguientes casos:** selecciona que eventos generan una alerta. Consulta la tabla [22.1](#) para más información.
- **Enviar alertas a la siguiente dirección:** introduce las direcciones de correo que recibirán la alerta.
- **Enviar las alertas en el siguiente idioma:** elige el idioma del mensaje de alerta entre los soportados por la consola:
 - Alemán
 - Español
 - Francés
 - Inglés
 - Italiano
 - Japonés
 - Magiar
 - Portugués
 - Ruso
 - Sueco

Nivel de acceso del administrador y envío de alertas

Las alertas se definen de forma independiente por cada usuario de la consola. El contenido de una alerta queda limitado por la visibilidad de los equipos administrados que tiene asignado el rol de la cuenta de usuario.

Tipos de alertas

Tipo	Frecuencia	Condición	Información contenida
Detecciones de malware (solo protección en tiempo real)	Máximo 2 mensajes por equipo – malware – día.	• Por cada malware detectado en tiempo real en el equipo. • Solo en equipos Windows.	• Primer o segundo mensaje. • Nombre del programa malicioso. • Nombre del equipo. • Grupo. • Fecha y hora UTC.

Tabla 22.1: Tabla de alertas

Tipo	Frecuencia	Condición	Información contenida
			• Ruta del programa malicioso. • Hash. • Tabla de acciones de programa. • Listado de equipos donde fue previamente visto el malware.
Detecciones de exploits	Máximo de 10 alertas al día por equipo y exploit	• Por cada detección de exploit que se produzca. • Solo en equipos Windows.	• Nombre, ruta y hash del programa que recibió el intento de explotación. • Nombre del equipo. • Grupo. • Fecha y hora UTC. • Acción ejecutada. • Nivel de riesgo del equipo. • Valoración de la seguridad del programa atacado. • Tabla de acciones de programa. • Posible origen del exploit.
Detecciones de PUP	Máximo 2 mensajes por equipo – PUP – día.	• Por cada PUP detectado en tiempo real en el equipo. • Solo en equipos Windows.	• Primer o segundo mensaje. • Nombre del programa malicioso. • Nombre del equipo. • Grupo. • Fecha y hora UTC.

Tabla 22.1: Tabla de alertas

Tipo	Frecuencia	Condición	Información contenida
			- Ruta del programa malicioso. - Hash. - Tabla de acciones de programa. - Listado de equipos donde fue previamente visto el malware.
Programas bloqueados en proceso de clasificación	Por cada programa desconocido detectado en el sistema de ficheros en tiempo real.	Solo en equipos Windows.	- Nombre del programa desconocido. - Nombre del equipo. - Grupo. - Fecha y hora UTC. - Ruta del programa desconocido. - Hash. - Tabla de acciones de programa. - Listado de equipos donde fue previamente visto el programa desconocido.
Programas bloqueados por el administrador	Por cada programa bloqueado.	Solo en equipos Windows.	- Nombre del programa - Hash - Ruta del programa - Nombre del equipo - Grupo al que pertenece el equipo - Usuario que lanzó el programa - Fecha del bloqueo
Clasificaciones de archivos que han sido permitidos por el administrador	Los archivos permitidos por el administrador son aquellos que han sido bloqueados por ser desconocidos para Panda Adaptive Defense 360 o por haber sido clasificados como amenazas, pero el administrador permite su ejecución. El sistema genera un correo de alerta cada vez que una clasificación se completa, ya que es posible que la acción emprendida por el sistema puede cambiar después de la clasificación, según se indica en la política de reclasificación configurada por el administrador. Consulta "Política de reclasificación" en la página 476 para obtener más información sobre las políticas de reclasificación.		

Tabla 22.1: Tabla de alertas

Tipo	Frecuencia	Condición	Información contenida
URLs con malware bloqueadas	Cada 15 minutos	• Cuando se producen detecciones de URL que apuntan a malware.	• Número de URL que apuntan a malware detectadas en el intervalo de tiempo. • Número de equipos afectados.
Detecciones de phishing	Cada 15 minutos	• Cuando se produzcan detecciones de phishing.	• Número de ataques de phishing detectadas en el intervalo de tiempo. • Número de equipos afectados.
Intentos de intrusión bloqueados	Cada 15 minutos	• Cuando se producen intentos de intrusión bloqueados por el módulo IDS. • Compatible con equipos Windows.	• Número de intentos de intrusión bloqueados en el intervalo de tiempo. • Número de equipos afectados.
Dispositivos bloqueados	Cada 15 minutos	• Se producen accesos por parte del usuario a dispositivos y periféricos bloqueados por el administrador. • Compatible con equipos Windows, Linux, macOS y Android.	• Número de accesos bloqueados a dispositivos. • Número de equipos afectados.
Equipos con error en la protección	Cada vez que se detecte el hecho relevante	• Por cada equipo desprotegido de la red. • Equipos con la protección en estado de error o fallo en la instalación de la protección	• Nombre del equipo. • Grupo. • Descripción. • Sistema operativo. • Dirección IP. • Ruta del directorio activo. • Dominio. • Fecha y hora UTC. • Motivo de la desprotección: Protección con error o Error instalando.

Tabla 22.1: Tabla de alertas

Tipo	Frecuencia	Condición	Información contenida
Equipos sin licencia	Cada vez que se detecte el hecho relevante	Por cada equipo que intenta licenciarse, pero no lo consigue por falta de licencias libres.	- Nombre del equipo. - Descripción. - Sistema operativo - Dirección IP - Grupo - Ruta del directorio activo - Dominio. - Fecha y hora UTC. - Motivo de la desprotección: equipo sin licencia.
Errores durante la instalación	Cada vez que se detecte el hecho relevante	- Por cada uno de los equipos de la red, cada vez que se crea una nueva situación que derive en el cambio de estado (1) de protegido a desprotegido. - Si en un mismo momento se detectan varios motivos que derivan en el cambio de estado en un mismo equipo, solo se genera una alerta con todos los motivos.	- Nombre del equipo. - Estado de la protección. - Razón del cambio del estado de la protección.
Equipos no administrados descubiertos	Cada vez que se detecte el hecho relevante	- Cada vez que un equipo descubridor termina un descubrimiento. - El descubrimiento ha encontrado equipos no vistos anteriormente en la red.	- Nombre del equipo descubridor. - Número de equipos descubiertos. - Enlace al listado de los equipos descubiertos en la consola.

Tabla 22.1: Tabla de alertas

Cambios de estado (1)

Las razones de cambio de estado que generan una alerta son:

- **Protección con error:** sólo se contempla el estado de las protecciones antivirus y protección avanzada, en aquellas plataformas que las soporten, y cuando las licencias del cliente las incluyan.

- **Error instalando:** se enviará alerta cuando se haya producido un error en la instalación que requiera de la intervención del usuario (e.g., no hay espacio en disco), y no ante errores transitorios que podrían solucionarse autónomamente tras varios reintentos.
- **Sin licencia:** cuando el equipo no ha recibido una licencia tras registrarse, por no haber libres en ese momento.

Las razones de cambio de estado que no generan una alerta son:

- **Sin licencia:** cuando el administrador ha quitado la licencia al dispositivo o cuando Panda Adaptive Defense 360 haya retirado la licencia automáticamente al equipo por haberse reducido el número de licencias contratadas.
- **Instalando:** por no resultar útil recibir una alerta cada vez que se instala un equipo.
- **Protección desactivada:** este estado es consecuencia de un cambio de configuración voluntario.
- **Protección desactualizada:** no implica necesariamente que el equipo este desprotegido, pese a estar desactualizado.
- **Pendiente de reinicio:** no implica necesariamente que el equipo este desprotegido.
- **Desactualizado el conocimiento:** no implica necesariamente que el equipo este desprotegido.

Dejar de recibir alertas por correo

Si el destinatario de las alertas por correo quiere dejar de recibirlas pero no tiene acceso a la consola de Panda Adaptive Defense 360 o no tiene permisos suficientes para modificar la configuración, puede darse de baja del servicio si sigue los pasos mostrados a continuación:

- Haz clic en el enlace del pie de mensaje **“Si no deseas recibir más mensajes de este tipo, pincha aquí.”**. Se mostrará una ventana pidiendo la dirección de correo del usuario. El enlace tiene una caducidad de 15 días.
- Si se ha introducido una dirección de correo que pertenece a alguna configuración de Panda Adaptive Defense 360 se envía un correo al usuario para confirmar la baja de notificaciones para esa cuenta.
- Haz clic en el enlace del nuevo correo para retirar la cuenta de correo de todas la configuraciones en las que aparezca. El enlace tiene una caducidad de 24 horas.

Capítulo 23

Envío programado de informes y listados

Panda Adaptive Defense 360 envía por correo electrónico toda la información de seguridad que se produce en los equipos que protege. Este método de entrega facilita la compartición de información entre los distintos departamentos de la empresa, así como permite guardar un histórico de todos los eventos producidos por la plataforma, más allá de los límites de capacidad de la consola Web. De esta forma, es posible realizar un seguimiento completo del estado de la seguridad sin necesidad de que el administrador tenga que acudir a la consola web, ahorrando tiempo de gestión.

El envío automático de informes por correo electrónico permite entregar a las personas interesadas toda la información de los eventos de seguridad generados, sin dejar espacio a manipulaciones para poder evaluar de forma precisa el estado de la seguridad de la red.

CONTENIDO DEL CAPÍTULO

Características de los informes	514
Según el intervalo de tiempo abarcado	514
Según la forma de envío	514
Según el formato de salida	514
Según su contenido	514
Tipos de informes	514
Requisitos para generar informes	515
Vistas de listados	515
Informes ejecutivos	515
Listado de dispositivos filtrado	515
Acceso al envío de informes y listados	516
Desde la sección Informes programados	516
Desde una vista de listado	516
Desde un filtro	516
Gestión de informes	517
Listado de Informes programados	517
Crear Informes programados	517
Ordenar Informes programados	517
Borrar y editar Informes programados	517
Información requerida para el envío de informes y listados	518
Contenido de los informes y listados	519
Vistas de listados	519
Listados de dispositivos	520
Informe ejecutivo	520

Características de los informes

Según el intervalo de tiempo abarcado

Dependiendo del momento en el que se produce la información incluida en el informe se distinguen dos tipos:

- **Informes consolidados:** reúnen en un solo documento toda la información generada en un intervalo de fechas.
- **Informes instantáneos:** contienen información que refleja el estado de la seguridad de la red en un momento concreto.

Según la forma de envío

Panda Adaptive Defense 360 genera y envía informes de forma automática según la configuración establecida en el programador de tareas o de forma manual bajo demanda.

Con el envío de informes automáticos, los destinatarios obtendrán de forma automática y sin necesidad de acudir a la consola Web la información producida en el parque de equipos gestionado.

Según el formato de salida

Dependiendo del tipo de informe Panda Adaptive Defense 360 entrega informes en formato pdf y /o csv.

Según su contenido

Dependiendo del tipo de informe su contenido será configurable, permitiendo abarcar más o menos módulos soportados por Panda Adaptive Defense 360 o estableciendo filtros para limitar la información a equipos que cumplan con determinadas características.

Tipos de informes

Panda Adaptive Defense 360 permite generar 3 tipos de documentos, cada uno de ellos con sus características asociadas:

- Vistas de listados
- Informes ejecutivos
- Listados de dispositivos

A continuación se resumen las características de cada tipo de informe:

Tipo	Intervalo	Envío	Contenido	Salida
Vistas de listados	Instantáneo	Automático	Configurable mediante búsquedas	csv
Informes ejecutivos	Consolidado	Automático y bajo demanda	Configurable por categorías y por grupos	pdf, csv, excel, word
Listados de dispositivos	Instantáneo	Automático	Configurable mediante filtros	csv

Tabla 23.1: Resumen de tipos de informes y sus características

Requisitos para generar informes



Los usuarios con el rol de solo lectura podrán previsualizar los informes ejecutivos pero no podrán programar el envío de nuevos informes.

A continuación se detallan las tareas previas que el administrador deberá realizar antes de poder utilizar la funcionalidad de envío de informes y listados programados.

Vistas de listados

El administrador deberá de crear previamente una vista y configurar las herramientas de búsqueda hasta que el listado muestre la información que considere relevante. Una vez hecho esto podrá crear un informe programado. Consulta "[Gestión de listados](#)" en la página [56](#), para obtener información de cómo crear vistas de listados con búsquedas asociadas.

Informes ejecutivos

No es necesaria la ejecución de ninguna tarea previa: su contenido se determina en el momento de configurar el informe programado.

Listado de dispositivos filtrado

El administrador deberá crear un filtro o utilizar uno de los filtros ya creados en Panda Adaptive Defense 360. Consulta "[Árbol de filtros](#)" en la página [162](#) para obtener más información acerca del manejo y configuración de los filtros.

Acceso al envío de informes y listados

Desde la sección Informes programados

Para acceder al listado de tareas que envían informes y listados haz clic en el menú superior **Estado**, panel lateral **Informes programados**. Se mostrará una pantalla con las herramientas necesarias para buscar tareas de envío ya creadas, editarlas, borrarlas o crear nuevas.

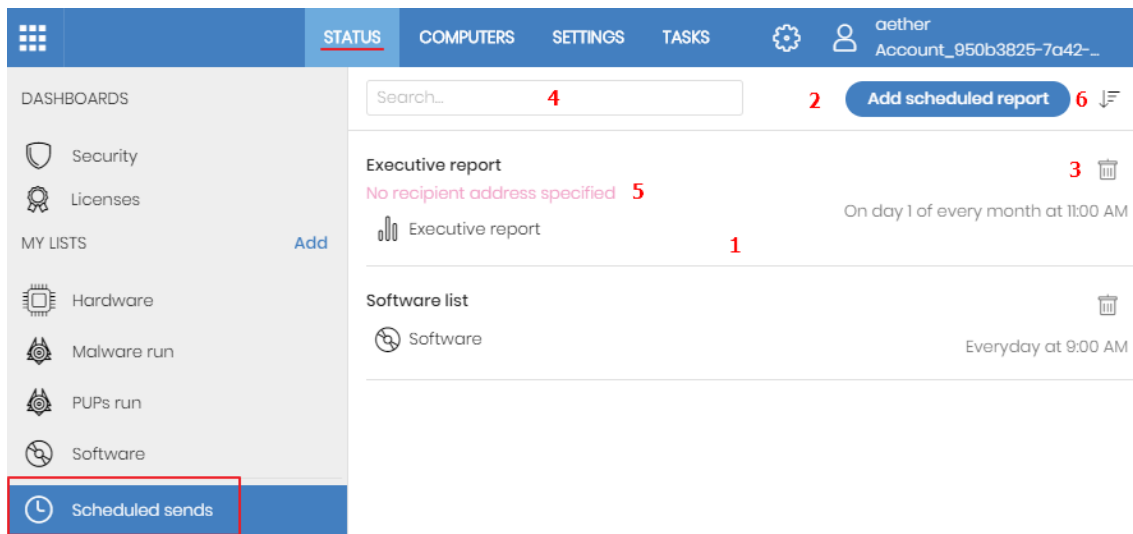


Figura 23.1: Ventana para gestionar los informes programados

Desde una vista de listado

Las vistas de listados se almacenan en el panel lateral izquierda del menú superior **Estado**, y cada una de ellas puede enviarse de forma programada siguiendo los pasos mostrados a continuación:

- **Desde el menú de contexto:** haz clic en el menú de contexto de la vista de listado y en la opción **Programar informe** . Se mostrará la ventana de información requerida explicada en "[Información requerida para el envío de informes y listados](#)".
- **Desde la propia vista del listado:** haz clic en el icono situado en la esquina superior derecha de la ventana. Se mostrará la ventana de información requerida explicada en "[Información requerida para el envío de informes y listados](#)".

Al completarse la creación del informe programado se mostrará un mensaje emergente en la esquina superior derecha de la pantalla indicado la generación de una nueva tarea de envío.

Desde un filtro

- En el menú superior **Equipos** haz clic en la pestaña para mostrar el árbol de filtros.
- Al hacer clic en un filtro, el listado de dispositivos se actualizará para mostrar los dispositivos cuyos atributos satisfagan las condiciones impuestas por el filtro seleccionado.
- Haz clic en el icono del menú de contexto asociado al filtro y selecciona la opción **Programar**

Informe. Se mostrará la ventana de información requerida explicada en "[Información requerida para el envío de informes y listados](#)".

Al completarse la creación del informe programado se mostrará un mensaje emergente en la esquina superior o inferior derecha de la pantalla indicado la generación de una nueva tarea de envío y un enlace para ver el listado de informes programados. Consulta "[Listado de Informes programados](#)".

Gestión de informes

Para crear, borrar, editar y listar informes programados haz clic en el menú superior **Estado** y en el menú lateral **Informes programados**.

Listado de Informes programados

En el panel de la derecha se muestran los informes programados ya creados (Figura [23.1 1](#)).

Todas las tareas de envío incluye un nombre y debajo una serie de mensajes que indican si faltan datos por indicar en la configuración del informe programado (Figura [23.1 5](#)).

Crear Informes programados

Haz clic sobre el botón **Añadir Informe programado** (Figura [23.1 2](#)) para mostrar la ventana de configuración.

Consulta "[Información requerida para el envío de informes y listados](#)" para obtener información sobre los datos que el administrador debe aportar al crear un informe programado.

Ordenar Informes programados

Haz clic en el icono  (6) para desplegar un menú de contexto con las opciones de ordenación disponibles:

- Ordenado por fecha de creación
- Ordenado por nombre
- Ascendente
- Descendente

Borrar y editar Informes programados

Para borrar y editar un informe programado sigue los pasos mostrados a continuación:

- Para borrar un informe programado utiliza el icono  (Figura [23.1 3](#)).

- Haz clic en el nombre del informe programado para editarlo.



Una vista de listado o listado filtrado que tenga configurado un informe programado no podrá borrarse hasta que el informe programado sea eliminado.

Los listados enviados por un informe programado se corresponden a una vista de listado o a un listado filtrado concretos. Si éstos son modificados, el informe programado se actualizará con la nueva configuración.

Información requerida para el envío de informes y listados

Campo	Descripción
Nombre	Nombre de la entrada que se mostrará en el listado de informes programados.
Enviar automáticamente	Frecuencia de envío del informe o listado: • Todos los días: el envío se producirá todos los días a la hora seleccionada. • Todas la semanas: el envío se producirá todas las semanas a la hora y día de la semana seleccionados. • Todos los meses: el envío se producirá todos los meses en el día del mes y hora seleccionados.
Tipo de informe	Tipo de informe que se enviará: • Informe ejecutivo • Vista de listado • Listado de dispositivos
Previsualizar informe	Este enlace solo se muestra cuando el tipo de informe elegido es Informe ejecutivo. Al hacer clic se abrirá una nueva pestaña en el navegador con el contenido del informe para previsualizarlo antes de configurar su informe programado, descargarlo o imprimirlo mediante la barra de herramientas superior. Para los listados el formato elegido es csv y por lo tanto la opción de previsualizar no estará disponible.
Fechas	Intervalo de tiempo que abarca el informe. • Último año • Último mes • Últimos 7 días • Últimas 24 horas Este campo solo se muestra cuando el tipo de informe es Informe ejecutivo. En los listados se incluyen datos pertenecientes al momento en el que se generan.

Tabla 23.2: Información para generar informes bajo demanda

Campo	Descripción
Equipos	De qué equipos se extraen datos para generar el informe ejecutivo: • Todos los equipos. • Los grupos seleccionados: muestra el árbol de grupos para seleccionar de forma individual los grupos mediante las casillas de selección. Este campo solo está disponible cuando el tipo de informe es Informe ejecutivo.
Para	Direcciones de correo separadas por comas que recibirán el informe.
CC	Direcciones de correo en copia separadas por comas que reciben el informe.
CCO	Direcciones de correo en copia oculta separadas por comas que recibirán el informe.
Asunto	Frase resumen que describe el correo.
Formato	• Para vistas de listado: adjunta un fichero en formato csv al correo. • Para informes ejecutivos: formato (Pdf, Excel, Word) del fichero adjunto al correo electrónico que contiene el informe.
Idioma	Idioma en el que se envía el informe.
Contenido	Tipo de información que incluye el informe: • Tabla de contenidos: índice de los distintos apartados dentro del informe. • Estado de licencias: muestra la información de las licencias contratadas, consumidas y su fecha de caducidad. Consulta "Licencias" en la página 146. • Estado de seguridad: funcionamiento del software Panda Adaptive Defense 360 en los equipos de la red donde ha sido instalado. • Detecciones: muestra las amenazas detectadas en la red. • Acceso web y Spam: muestra la actividad web de los usuarios. Consulta "Paneles / Widgets del módulo de seguridad" en la página 412. • Gestión de parches: muestra el estado del parcheo de los equipos. Consulta "Paneles / widgets en Panda Patch Management" en la página 340. • Cifrado: muestra el estado del cifrado en los equipos de la red. Consulta "Paneles / widgets del módulo Panda Full Encryption" en la página 383.

Tabla 23.2: Información para generar informes bajo demanda

Contenido de los informes y listados

Vistas de listados

El contenido de los listados enviados equivale a la opción **Exportar** de una vista de listado, y contiene el fichero csv correspondiente al listado elegido. Consulta "[Gestión de listados](#)" en la página [56](#) para

obtener información sobre los tipos de listados disponibles en Panda Adaptive Defense 360 y su contenido.



El listado incluirá los equipos visibles para la cuenta de usuario que modificó por última vez el informe programado.

Listados de dispositivos

El contenido del informe enviado se corresponde con el listado de dispositivos filtrados por un criterio. Consulta “Equipos” en la página 175 para obtener información sobre el contenido del fichero csv enviado y “Árbol de filtros” en la página 162 para obtener información acerca del manejo y configuración de los filtros.

Informe ejecutivo

Dependiendo de la configuración establecida en el campo **Contenido**, el informe ejecutivo contendrá los datos mostrados a continuación:

Campo	Descripción
Tabla de contenidos	Muestra un índice con enlaces a las distintas secciones incluidas en el informe ejecutivo.
Contenido	Tipo de información que incluye el informe: • Estado de licencias: muestra la información de las licencias contratadas, consumidas y su fecha de caducidad. Consulta “Licencias” en la página 146. • Estado de seguridad la red: funcionamiento de software Panda Adaptive Defense 360 en los equipos de la red donde ha sido instalado. Incluye el widget Estado de protección e información sobre los Equipos conectados, Protecciones actualizado y Conocimiento actualizado. • Detecciones: muestra las amenazas detectadas en la red. Incluye los widgets y listados mostrados a continuación: • Clasificación de todos los programas ejecutados y analizados • Equipos con más detecciones (top 10) • Actividad del malware • Actividad de PUPs • Actividad de exploits • Últimas detecciones de malware • Últimas detecciones de PUPs • Últimas detecciones de exploits

Tabla 23.3: Contenido del informe ejecutivo

Campo	Descripción
	• Amenazas detectadas por el antivirus • Filtrado de contenidos en Exchange servers • Acceso web y Spam: 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) • Spam detectado en Exchange Server. Consulta "Paneles / Widgets del módulo de seguridad" en la página 412. • Gestión de parches: muestra el estado del parcheo de los equipos. Incluye los widgets y listados mostrados a continuación: • Estado de gestión de parches. • Equipos con más parches disponibles (top 10): listado de los 10 equipos de la red que tiene más parches disponibles sin instalar agrupados por su tipo: parches de seguridad, parches no de seguridad y Service Packs. • Parches más críticos (top 10). listado de los 10 parches más críticos ordenado por el número de equipos afectados. Consulta "Paneles / widgets en Panda Patch Management" en la página 340 • Data Control: muestra el estado del despliegue de Panda Data Control y los equipos con mayor cantidad de ficheros PII detectados en la red. • Estado del despliegue: indica el estado de las licencias del módulo y las funcionalidades activadas en los equipos de la red. • Archivos por tipo de información personal: muestra el número de archivos PII encontrados por cada tipo de entidad soportada en el último inventario diario generado. • Equipos por información personal: muestra el número de equipos con archivos PII encontrados en la red por cada tipo de entidad soportada en el último inventario diario generado. • Equipos con más archivos con información personal (top 10): muestra los equipos que contienen el mayor número de ficheros PII en la red. Consulta "Paneles / widgets del módulo Panda Data Control" en la página 294

Tabla 23.3: Contenido del informe ejecutivo

Campo	Descripción
	• Cifrado: muestra el estado del cifrado de los equipos. Incluye los widgets y listados mostrados a continuación: • Estado del cifrado • Equipos compatibles con cifrado • Equipos cifrados • Método de autenticación aplicado • Últimos equipos cifrados: listado de los 10 equipos que han sido cifrados recientemente por Panda Full Encryption, ordenados por 'Fecha de cifrado'. Cada línea del listado contiene el nombre del equipo, grupo al que pertenece, sistema operativo instalado, método de autenticación configurado y fecha de cifrado. Consulta "Paneles / widgets del módulo Panda Full Encryption" en la página 383.

Tabla 23.3: Contenido del informe ejecutivo



Parte 7

Resolución de incidencias de seguridad

Capítulo 24: Herramientas de resolución

Capítulo 25: Tareas

Capítulo 24

Herramientas de resolución

Panda Adaptive Defense 360 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 24.1 muestra las herramientas disponibles por plataforma y sus características.

Herramienta de resolución	Plataforma	Tipo	Acción
Análisis y desinfección automático de equipos	Windows, macOS, Linux, Android	Automático	Detecta y desinfecta el malware cuando se registra un movimiento en el sistema de ficheros (copia, movimiento, ejecución) o en un vector de infección soportado.
Análisis y desinfección bajo demanda de equipos	Windows, macOS, Linux, Android	Automático (Programado) / Manual	Detecta y desinfecta el malware en el sistema de ficheros cuando lo requiera el administrador: en franjas horarias concretas o cuando cree la tarea de resolución.
Reinicio bajo demanda	Windows	Manual	Fuerza un reinicio del equipo para aplicar actualizaciones, completar desinfecciones manuales y corregir errores detectados en la protección.
Aislamiento de equipos	Windows	Manual	Aísla el equipo de la red, impidiendo la extracción de información confidencial y la propagación de la amenaza a los equipos vecinos.

Tabla 24.1: Herramientas de resolución disponibles en Panda Adaptive Defense 360

CONTENIDO DEL CAPÍTULO

Análisis y desinfección automática de equipos

Comportamiento según la configuración de la protección

Análisis y desinfección bajo demanda de equipos

Crear tareas desde el Árbol de equipos

Tareas inmediatas

526

527

527

527

528

Tareas programadas 528

Crear tareas desde el listado de equipos 528

Menú de contexto asociado al equipo 529

Casillas de selección y la barra de acciones 529

Opciones de análisis 530

Listados generados por tareas de análisis 531

Acceso a los listados 531

Listado Ver detecciones 533

Reiniciar equipos - 533

Aislar un equipo - 534

Estados de los equipos aislados 535

Aislar uno o varios equipos de la red de la organización 535

Quitar el aislamiento de un equipo 536

Opciones avanzadas 536

Permitir procesos 536

Mostrar mensaje personalizado 536

Comunicaciones permitidas y denegadas de un equipo aislado 536

Procesos y servicios permitidos en un equipo aislado 537

Comunicaciones bloqueadas en un equipo aislado 537

Notificar un problema - 537

Permitir el acceso externo a la consola Web - 538

Análisis y desinfección automática de equipos

Los módulos de protección Panda Adaptive Defense 360 detecta y desinfecta de forma automática las amenazas encontradas en los equipos protegidos y recibidas en los siguientes vectores de infección:



La desinfección automática no requiere de la intervención del administrador, si bien es necesario que esté seleccionada la casilla **Protección de archivos** en la configuración de seguridad asignada al equipo. Consulta “[Configuración de la seguridad en estaciones y servidores](#)” en la página 237 para más información sobre los modos de bloqueo y las configuraciones disponibles en el módulo antivirus de Panda Adaptive Defense 360.

- **Protección avanzada:** bloquea la ejecución del malware desconocido.
- **Web:** malware que se recibe mediante una descarga producida por el navegador web.
- **Correo:** malware que se recibe como adjunto de un correo en el cliente instalado en el equipo.
- **Sistema de ficheros:** cuando se ejecuta, se mueve o se copia un fichero que contiene una amenaza conocida o desconocida y reside en el sistema de almacenamiento del equipo.
- **Red:** intentos de intrusión recibidos por la red y bloqueados por el cortafuegos.
- **Protección Exchange:** detección de malware y spam recibidos en los buzones del servidor de correo.

Ante la detección de una amenaza conocida, Panda Adaptive Defense 360 desinfecta de forma automática los elementos afectados siempre y cuando exista un método de desinfección conocido. En su defecto, el elemento se moverá a cuarentena.

Comportamiento según la configuración de la protección

Si los módulos de antivirus y protección avanzada están activados, Panda Adaptive Defense 360 ejecutará las acciones mostradas a continuación en el orden indicado:

Modo de protección avanzada	Protección antivirus	Comportamiento
Audit	Activado	Detección, Desinfección o Cuarentena.
Hardening, Lock	Activado	Detección, Bloqueo de desconocidos, Desinfección o Cuarentena.
Audit	Desactivado	Detección.
Hardening, Lock	Desactivado	Detección, Bloqueo de desconocidos.

Tabla 24.2: Comportamiento del producto frente a las amenazas según la configuración del motor Protección avanzada y Protección antivirus

Análisis y desinfección bajo demanda de equipos



Consulta "**Tareas**" en la página **539** para obtener información sobre la gestión de tareas ejecutadas en los equipos y servidores de la red, como visualizar sus resultados y cómo modificar sus parámetros configurados.

Para analizar y desinfectar bajo demanda un equipo se ofrecen dos posibilidades:

- Mediante la creación de tareas de análisis programadas.
- Mediante un análisis inmediato.

Crear tareas desde el Árbol de equipos

El árbol de equipos permite definir de forma rápida tareas de análisis para grupos completos de equipos.

- Haz clic en el menú superior **Equipos** y en el panel lateral haz clic en el botón  para elegir la vista carpetas del Árbol de equipos.
- Dentro del árbol de equipos haz clic en el menú de contexto asociado al grupo de equipos destinatario de la tarea de análisis. Se mostrará el menú contextual de la rama del árbol elegida.
- En el menú contextual haz clic en una de las dos opciones:
 - **Analizar ahora:** crea una tarea con destinatario el grupo de equipos elegido, para su ejecución inmediata.
 - **Programar análisis:** muestra la zona **Tareas** para crear una nueva tarea repetida en el tiempo y / o aplazada. La plantilla de tarea estará parcialmente completada: el campo **Destinatarios**

incluye el grupo elegido en el Árbol de Equipos. Completa el resto de la configuración tal y como se describe en "[Crear tareas desde la zona Tareas](#)" en la página 540.

Tareas inmediatas

Las tareas inmediatas (entrada **Analizar ahora** del menú de contexto) tienen las siguientes características:

- Permiten elegir el tipo de análisis (**Todo el ordenador** o **Áreas críticas**). Consulta el punto "[Programación horaria y repetición de la tarea](#)" en la página 541 para obtener más información.
- **No requieren especificar el momento de ejecución ni la repetición:** son tareas puntuales que se ejecutan en el momento de su definición.
- **No requieren la publicación de la tarea:** Panda Adaptive Defense 360 publica de forma automática estas tareas.
- Para informar del éxito o fracaso en la creación de la tarea inmediata se muestra un mensaje emergente en la consola de administración.

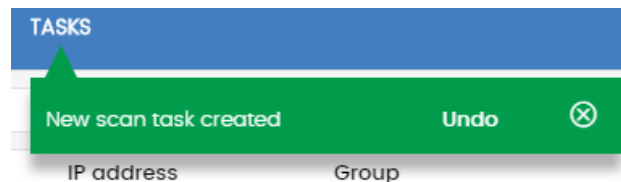


Figura 24.1: Mensaje emergente de creación de una nueva tarea de análisis

Tareas programadas

Las tareas programadas (entrada **Programar análisis** en el menú de contexto) son idénticas a las tareas creadas desde la zona **Tareas** y mostradas en "[Crear tareas desde la zona Tareas](#)" en la página 540, si bien el campo destinatarios aparece completado con el grupo del Árbol de equipos seleccionado. Por lo tanto, es necesario indicar el momento de ejecución de la tarea, la repetición y publicar la tarea para su activación.

Crear tareas desde el listado de equipos

La zona **Equipos** permite crear tareas de forma similar al árbol de equipos o la zona **Tareas**. En este caso, puedes elegir de forma independiente equipos que pertenecen a un mismo grupo o subgrupos.

Según sea del número de equipos destinatarios de la tarea, elige uno de los dos recursos mostrados a continuación:

- **Menú de contexto asociado al equipo:** un único equipo destinatario.
- **Casillas de selección y barra de acciones:** uno o varios equipos pertenecientes a un grupo o

subgrupos.

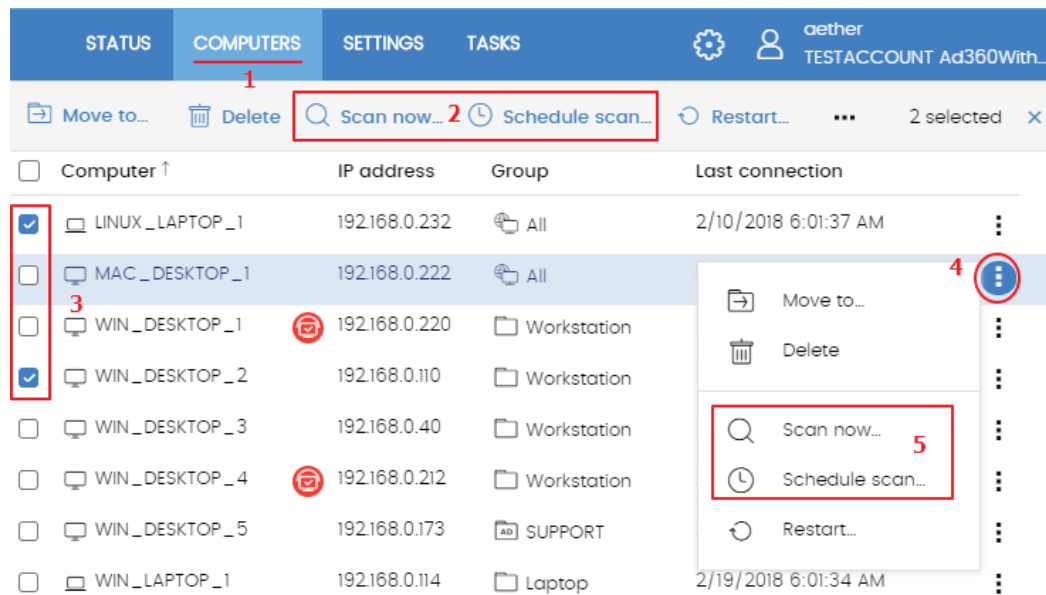


Figura 24.2: Menús de contexto y barra de acciones disponibles para la creación rápida de tareas

Menú de contexto asociado al equipo

- Haz clic en el menú superior **Equipos (1)** y elige el grupo del Árbol de equipos al que pertenece el equipo a analizar.
- En el listado de equipos haz clic en el menú de contexto del equipo destinatario de la tarea de análisis. **(4)**
- En el menú de contexto haz clic en una de las dos ramas **(5)**:
 - **Analizar ahora**: crea una tarea con destinatario el equipo elegido para ejecutarse inmediatamente.
 - **Programar análisis**: muestra la zona **Tareas** con una plantilla de tarea parcialmente completada. En el campo destinatarios se incluye el equipo elegido. Completa el resto de la configuración tal y como se describe en el punto “[Crear tareas desde la zona Tareas](#)” en la página [540](#).

Casillas de selección y la barra de acciones

- Haz clic en el menú superior **Equipos (1)** y elige el grupo del árbol de equipos al que pertenece el equipo o equipos a analizar.
- Selecciona los equipos destinatarios de la tarea con las casillas de verificación **(3)**. Se mostrará la barra de acciones **(2)** en la parte superior de la ventana.
- Haz clic en uno de los dos iconos:
 - **Analizar ahora** : crea una tarea con destinatario el grupo de equipos elegido para ejecutarse inmediatamente.

- **Programar análisis** : muestra la zona **Tareas** con una plantilla de tarea parcialmente completada. En el campo destinatarios se incluye el grupo elegido en el **Árbol de Equipos**. Completa el resto de la configuración tal y como se describe en [“Crear tareas desde la zona Tareas”](#) en la página 540.

Opciones de análisis

Las opciones de análisis configuran los parámetros del motor de antivirus a la hora de escanear el sistema de ficheros de los equipos:

Valor	Descripción
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: indica las rutas de los dispositivos de almacenamiento masivo que se analizarán. Se admite el uso de variables de entorno. Se analizará la ruta indicada y todas las carpetas y ficheros que cuelguen de ella.
Detectar virus	Detecta los programas que se introducen en los ordenadores y producen efectos nocivos. Esta opción está siempre activada.
Detectar herramientas de hacking y PUPs	Detecta los programas utilizados por los hackers para causar perjuicios a los usuarios de un ordenador y los programas potencialmente no deseados.
Detectar archivos sospechosos	En los análisis programados el software del equipo se analiza de forma estática, si llegar a ejecutarlo. Esto reduce las posibilidades de detectar ciertos tipos de amenazas. Para mejorar el ratio de detección de este tipo de análisis, activa los algoritmos heurísticos.
Analizar archivos comprimidos	Descomprime y analiza los archivos empaquetados.
Excluir del análisis los siguientes archivos	• No analizar los archivos excluidos para las protecciones permanentes: los archivos que el administrador ha marcado para permitir su ejecución no serán analizados, junto a los archivos ya excluidos de forma global en la consola. • Extensiones: introduce las extensiones de los archivos que no se analizarán separados por comas.

Tabla 24.3: Opciones de análisis

Valor	Descripción
	• Archivos: introduce el nombre de los archivos que no se analizarán separados por comas. • Directorios: introduce el nombre de las carpetas que no se analizarán separados por comas.

Tabla 24.3: Opciones de análisis

Listados generados por tareas de análisis

Las tareas de análisis generan listados con los resultados.

Acceso a los listados

Para acceder a estos listados sigue los pasos a continuación:

- Desde el menú superior **Tareas**, haz clic en la **Ver resultados** en la tarea de análisis para acceder al listado **Resultados de tarea**.
- En el listado de **Resultados de Tarea**, selecciona **Ver Detecciones** para acceder al listado.

Permisos requeridos

Permisos	Acceso a listados
Sin permisos	Listado Resultados de la tarea de análisis .
Ver detecciones y amenazas	Acceso a los listados Ver Detecciones dentro de la tarea.

Tabla 24.4: Permisos requeridos para los listados de tareas de análisis

Listado Resultados tarea de análisis

Este listado muestra las detecciones de malware realizada sobre los equipos de la red:

Campo	Descripción	Valores
Equipo	Nombre del equipo analizado.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Detecciones	Número de elementos encontrados en el equipo.	Cadena de caracteres

Tabla 24.5: Campos del listado de Resultado de tarea de análisis

Campo	Descripción	Valores
Estado	Estado de la tarea de análisis en el equipo.	• Todos los estados • Pendiente • En curso • Finalizado • Con error • Cancelada (no pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Fecha de comienzo	Fecha en la que comenzó el análisis del equipo.	Fecha
Fecha de fin	Fecha en la que finalizó el análisis del equipo.	Fecha

Tabla 24.5: Campos del listado de Resultado de tarea de análisis

• **Herramientas de filtrado**

Campo	Comentario	Valores
Estado	Según el estado de la tarea	• Todos los estados • Pendiente • En curso • Finalizado • Con error • Cancelada (no pudo iniciar a la hora programada) • Cancelada • Cancelando • Cancelada (tiempo máximo superado)
Detecciones	Equipos con detecciones de malware o sin ellas	• Todos • Con detecciones • Sin detecciones

Tabla 24.6: Filtros Resultado de tareas de análisis

Listado Ver detecciones

Este listado muestra el detalle de cada una de las detecciones de malware encontradas por la tarea de análisis.

Campo	Descripción	Valores
Equipo	Nombre del equipo.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Tipo de amenaza	Función del archivo detectado.	• Virus • Spyware • Tracking Cookies • Herramientas de hacking y PUPs • Phishing • Acciones peligrosas bloqueadas • URLs con malware • Otros
Ruta	Ubicación de la amenaza en los equipos.	Cadena de caracteres
Acción	Acción realizada en el equipo.	• Movido a cuarentena • Borrado • Desinfectado • En cuarentena • Bloqueado • Proceso terminado
Fecha	Fecha en la que se realizó la acción.	Fecha

Tabla 24.7: Campos del listado Ver detecciones

• Ventana detalle del equipo

Al hacer clic en una de las filas del listado se mostrará la ventana de detalle del equipo. Consulta ["Información de equipo"](#) en la página 189 para obtener más información.

Reiniciar equipos

Para mantener los equipos actualizados a la última versión de la protección, o si se detecta algún error en la protección, el administrador puede reiniciar los equipos involucrados desde la consola web:

- Selecciona el menú superior **Equipos** y localiza el equipo desde el panel de equipos situado a la derecha.

- **Para reiniciar un único equipo:** selecciona el menú de contexto del equipo en el listado de equipos.
- **Para reiniciar varios equipos:** mediante las casillas de selección, marca los equipos que quieres reiniciar y haz clic en el icono  de la barra de acciones.



Para los equipos que estén apagados Panda Adaptive Defense 360 guardará la orden de reinicio hasta 7 días, momento en el cual si el equipo no se ha iniciado se desechará.

Aislar un equipo

Panda Adaptive Defense 360 aísla bajo demanda los equipos de la red para evitar la propagación de las amenazas y la comunicación y extracción de información confidencial.



Esta función solo es compatible con estaciones y servidores Windows. No soporta equipos Linux, macOS o Android.

Cuando un equipo está aislado, sus comunicaciones quedan restringidas a los servicios mostrados a continuación:

- El acceso al equipo desde la consola para que el administrador pueda analizar el problema y resolverlo mediante las herramientas suministradas por Panda Adaptive Defense 360.
- El acceso a los dispositivos y su control remoto mediante Panda Systems Management para que el administrador pueda recoger información extendida y resolver los problemas mediante las herramientas de gestión remota (escritorio remoto, línea de comandos remota, visor de sucesos remoto etc.).



Para obtener un listado de las herramientas de gestión remota disponibles en Panda Security consulta la Guía de administración de Panda Systems Management en <https://www.pandasecurity.com/rfiles/enterprise/documentation/pcsm/docswebpage/SYSTEMSMANAGEMENT-Manual-ES.pdf>

El resto de productos y servicios instalados en el equipo de usuario o servidor dejarán de poder comunicarse por red a no ser que el administrador establezca excepciones. Consulta "[Opciones avanzadas](#)" en la página [536](#).

Estados de los equipos aislados

Las operaciones **Aislar un equipo** y **Dejar de Aislar un equipo** se ejecutan en tiempo real, pero el proceso puede retrasarse si el equipo no está conectado a Internet. Para reflejar su situación exacta, Panda Adaptive Defense 360 distingue los 4 estados a través de los iconos mostrados a continuación:

Icono	Descripción
Aislando 	El administrador lanzó una petición para aislar uno o más equipos y se está procesando.
Aislado 	El proceso de aislamiento se completó y el equipo tiene restringidas sus comunicaciones.
Dejando de aislar 	El administrador lanzó una petición para dejar de aislar uno o más equipos y se está procesando.
No aislado	El proceso para retirar el aislamiento del equipo se completó. Las comunicaciones se permiten acorde la configuración definida en otros módulos, productos, o en el propio sistema operativo.

Tabla 24.8: Estados de los equipos aislados

Estos iconos acompañan a la columna dirección IP en los listados de **Licencias**, **Estado de la protección** y en la zona **Equipos**.

Aislar uno o varios equipos de la red de la organización

Para aislar uno o varios equipos de la red:

- Haz clic en el menú superior **Equipos** o elige uno de los siguientes listados de equipos:
 - Listado **Estado de protección**.
 - Listado **Licencias**.
- Indica los equipos a aislar con las casillas de selección.
- En la barra de acciones selecciona **Aislar un equipo**. Se mostrará una ventana con un link a **Opciones avanzadas**.
- En **Opciones avanzadas** indica los programas que se seguirán comunicando con el resto de la red a pesar del aislamiento del equipo (exclusión de aislamiento).
- Haz clic en el botón **Aceptar**. El equipo cambiará de estado a **Intentando aislar el equipo**.
- Para aislar un grupo de equipos:
 - Haz clic en el menú superior **Equipos**.
 - En el Árbol de equipos haz clic en la vista de carpetas y selecciona el grupo a aislar.
 - En el menú de contexto selecciona la entrada **Aislar equipos** y haz clic en el botón **Aceptar**.
 - Para aislar todos los equipos de la red despliega el menú de contexto del nodo **Todos**.

Quitar el aislamiento de un equipo

- Sigue los pasos indicados en el punto "[Aislar uno o varios equipos de la red de la organización](#)".
- En la barra de acciones selecciona **Dejar de aislar un equipo**.
- El equipo cambiará de estado a **Intentando dejar de aislar el equipo**.

Opciones avanzadas

Permitir procesos

Al aislar un equipo, solo se permite la comunicación de los procesos correspondientes a los productos de Panda Security. El resto de procesos, incluyendo a los programas de usuario, no podrán comunicarse con los equipos de la organización.

Para excluir a ciertos programas de este comportamiento:

- Haz clic en el enlace **Opciones avanzadas** de la ventana flotante mostrada al aislar un equipo.
- En la caja de texto **Permitir los siguientes procesos** indica los programas a excluir del aislamiento.

Los programas indicados en **Permitir los siguientes procesos** podrán comunicarse con libertad con el resto de equipos de la organización o con el exterior, según indique la configuración del resto de módulos de Panda Adaptive Defense 360, de otros productos instalados en el equipo, o del cortafuegos del sistema operativo.

Para acelerar la configuración, la consola de administración retiene la última configuración de procesos excluidos del aislamiento introducida por el administrador. De esta manera, en la caja de texto de un equipo excluido no se mostrará su configuración específica de procesos excluidos, sino la última configuración que utilizó el administrador en cualquier otro equipo.

Mostrar mensaje personalizado

Introduce un mensaje descriptivo para informar al usuario de que su equipo ha sido aislado de la red. El agente Panda Adaptive Defense 360 mostrará una ventana desplegable con el contenido del mensaje. Para configurar un mensaje informativo pero sin que se le muestre al usuario haz clic en el selector **Prefiero no mostrar ningún mensaje en esta ocasión**. Hasta que no desactives el selector los mensajes no se mostrarán.

Comunicaciones permitidas y denegadas de un equipo aislado

Panda Adaptive Defense 360 deniega todas las comunicaciones en un equipo aislado excepto las necesarias para poder realizar un análisis forense remoto y utilizar las herramientas de resolución implantadas en Panda Adaptive Defense 360 y en Panda Systems Management. A continuación, se indican las comunicaciones permitidas y denegadas.

Procesos y servicios permitidos en un equipo aislado

- Procesos de sistema:
 - Los servicios necesarios para formar parte de la red corporativa: obtención de IP por DHCP, ARP, nombre de equipo por WINS, DNS etc.
- Procesos de Panda Adaptive Defense 360:
 - Comunicación con el Gateway por defecto.
 - Comunicación con la nube de Panda Security para el funcionamiento de los motores de protección, descarga de ficheros de firmas y administración remota mediante la consola web.
 - Descubrimiento de equipos en máquinas aisladas con el rol de descubridor asignado.
 - Servidor de ficheros en una máquina aislada con el rol de caché asignado.
 - Proxy de conexiones en una máquina con el rol de proxy Panda asignado.
- Procesos de Panda Systems Management entre la máquina aislada y la máquina del administrador:
 - Herramientas de acceso remoto.
 - Monitorización por SNMP de dispositivos no compatibles con Panda Systems Management con el rol Nodo de conexión asignado.

Comunicaciones bloqueadas en un equipo aislado

Todas las comunicaciones que no estén incluidas en el punto anterior son denegadas, entre ellas:

- Conexión con el servicio Windows Update del sistema operativo.
- Políticas de Windows Update y Patch Management de Panda Systems Management.



El módulo Panda Patch Management sí permanece operativo en un equipo aislado.

- Comunicación con la red de scripts y módulos desarrollados por el administrador o integrados desde la ComStore de Panda Systems Management.
- Navegación web, ftp, correo y otros protocolos de Internet.
- Transferencia de ficheros por SMB entre los PCs de la red.
- Instalación remota de equipos con Panda Adaptive Defense 360.

Notificar un problema

En algunas ocasiones es posible que el software Panda Adaptive Defense 360 instalado en los equipos de la red presente un mal funcionamiento. Algunos de los síntomas pueden ser:

- Fallos en el reporte del estado del equipo.

- Fallos en la descarga de conocimiento o de las actualizaciones del motor.
- Motor de protección en estado de error.

Si Panda Adaptive Defense 360 presenta un mal funcionamiento en alguno de los equipos de la red, es posible contactar con el departamento de soporte de Panda Security a través de la consola y enviar de forma automatizada toda la información necesaria para efectuar un diagnóstico. Para ello haz clic en el menú superior Equipos, selecciona el equipo que presente errores y haz clic en el menú de contexto. Se desplegará un menú con la opción Indícanos el problema.

Permitir el acceso externo a la consola Web

Para aquellos problemas que el administrador de la red no pueda resolver, existe la posibilidad de habilitar el acceso a la consola únicamente para equipo de soporte de Panda Security:

- Haz clic en el menú superior **Configuración**, panel lateral **Usuarios**.
- En la pestaña usuarios haz clic en el control **Permitir al equipo de Panda Security S.L acceder a mi consola**.

Capítulo 25

Tareas

Una tarea es un recurso implementado en Panda Adaptive Defense 360 que permite establecer dos características a la ejecución de un proceso: la repetición y el aplazamiento de su inicio.

- **Repetición:** configura la tarea para su ejecución de forma puntual o repetida a lo largo del tiempo.
- **Aplazamiento:** configura la tarea para ser ejecutada en el momento en que se define (tarea inmediata), o aplazada en el tiempo (tarea programada).

CONTENIDO DEL CAPÍTULO

Introducción al sistema de tareas	539
Accesibilidad del sistema de tareas	539
Secuencia completa para lanzar una tarea	540
Tipos de procesos ejecutados por una tarea	540
Crear tareas desde la zona Tareas	540
Destinatarios de la tarea (2)	541
Programación horaria y repetición de la tarea	541
Publicar tareas	542
Listado de tareas	543
Gestionar tareas	544
Modificar tareas publicadas	544
Cancelar tareas publicadas	544
Borrar tareas	545
Copiar tareas	545
Resultados de una tarea	545
Ajuste automático de los destinatarios de una tarea	547
Tareas inmediatas	547
Tareas programadas de ejecución única	548
Tareas programadas de ejecución repetida	548

Introducción al sistema de tareas

Accesibilidad del sistema de tareas

Dependiendo de la necesidad o no de configurar todos los parámetros de una tarea, ésta se puede crear desde varios lugares dentro de la consola:

- Menú superior **Tareas**

- Árbol de equipos en el menú superior **Equipos**
- Listados asociados a los distintos módulos soportados.

El árbol de equipos y los listados permiten programar y lanzar tareas de forma ágil, sin necesidad de pasar por todo el proceso de configuración y publicación descrito en “[Secuencia completa para lanzar una tarea](#)”, perdiendo algo de flexibilidad en su definición.

Secuencia completa para lanzar una tarea

El recurso principal para crear una tarea se encuentra en la zona **Tareas**, accesible desde el menú superior de la consola. En esta ventana se definen las tareas desde cero, controlando todos los aspectos del proceso.

El proceso para lanzar una tarea consta de tres pasos:

- **Crear y configurar la tarea:** establece los equipos afectados, las características de la tarea, el momento en que será lanzada, el número de veces que se ejecutará y su comportamiento en caso de error.
- **Publicar la tarea:** las tareas creadas se introducen en el programador de procesos de Panda Adaptive Defense 360 para lanzarse en el momento marcado por su configuración.
- **Ejecutar la tarea:** el programador lanza el proceso en los equipos cuando se alcanzan las condiciones especificadas en la definición de la tarea.

Tipos de procesos ejecutados por una tarea

Panda Adaptive Defense 360 ejecuta como tarea los procesos siguientes:

- Análisis y desinfección de ficheros. Consulta “[Análisis y desinfección bajo demanda de equipos](#)” en la página [527](#).
- Instalación de parches y actualizaciones del sistema operativo y de los programas instalados en el equipo. Consulta “[Panda Patch Management \(Actualización de programas vulnerables\)](#)” en la página [325](#).

Crear tareas desde la zona Tareas

- Haz clic el menú superior **Tareas**. Se mostrará un listado con todas las tareas y su estado.
- Haz clic en el botón **Añadir tarea** y elige el tipo de tarea en el desplegable: se mostrará una ventana con los datos de la tarea, distribuidos en varias zonas:
 - **Información general (1):** nombre de la tarea y descripción.
 - **Destinatarios (2):** equipos que recibirán la tarea.
 - **Programación (3):** configuración del momento en que se lanzará la tarea.
 - **Configuración (4):** establece las acciones a ejecutar por la tarea. Esta sección varía según el tipo

de tarea y se detalla en la documentación asociada al módulo relacionado.

Cancel **New task** **Save**

Name: New scan task **1**

Description: Description

Recipients: No recipients selected yet **2**

Starts: ☐ As soon as possible

7/2/2020 9:00 AM ☒ Computer's local time

3 If the computer is turned off at the scheduled time, run the task as soon as
1 week

Maximum run time: No limit

Repeat: Every week

Scan options

Scan type **4** Critical areas (recommended)
Scans the memory, running processes, cookies, etc.

Detect viruses: ☒

Detect hacking tools and PUPs: ☒

Figura 25.1: Vista general de la ventana Nueva tarea para una tarea de tipo análisis

Destinatarios de la tarea (2)

- Haz clic en el enlace **Destinatarios (No se ha asignado a ningún equipo)** para abrir una nueva ventana donde seleccionar los equipos que recibirán la tarea configurada.
- Haz clic en el botón **+** para agregar equipos individuales o grupos de equipos, y en el botón **🗑️** para eliminarlos.



Para acceder a la ventana de selección de equipos es necesario guardar previamente la tarea. Si la tarea no ha sido guardada se mostrará una ventana de advertencia.

- Haz clic en el botón **Ver equipos** para verificar los equipos que recibirán la tarea.

Programación horaria y repetición de la tarea

Se establece mediante tres parámetros:

- **Empieza:** marca el inicio de la tarea.

Valor	Descripción
Lo antes posible (activado)	La tarea se lanza en el momento si el equipo está disponible (encendido y accesible desde la nube), o cuando se encuentre disponible dentro del margen definido en el desplegable Equipo apagado .
Lo antes posible (desactivado)	La tarea se lanza en la fecha seleccionada en el calendario, indicando si se tiene en cuenta la hora del equipo o la hora del servidor Panda Adaptive Defense 360.
Equipo apagado	Si el equipo está apagado o inaccesible, la tarea no se podrá lanzar. El sistema de programación de tareas permite establecer la caducidad de la tarea en función del intervalo de tiempo definido por el administrador, desde 0 (la tarea caduca de forma inmediata si el equipo no está disponible) a infinito (la tarea siempre está activa y se espera a que el equipo esté disponible de forma indefinida): • No ejecutar: la tarea se cancela si en el momento del lanzamiento el equipo no está encendido o no es accesible. • Dar un margen de: define un intervalo de tiempo dentro del cual, si el equipo inicialmente no estaba disponible y vuelve a estarlo, la tarea será lanzada. • Ejecutar cuando se encienda: no establece ningún intervalo de tiempo sino que se espera de forma indefinida a que el equipo esté accesible para lanzar la tarea.

Tabla 25.1: Comportamiento del inicio de la tarea si el equipo no está disponible

- **Tiempo máximo de ejecución:** indica el tiempo máximo que la tarea puede tardar en completarse, transcurrido el cual se cancelará con error si no ha terminado.

Valor	Descripción
Sin límite	La duración de la ejecución de la tarea no está definida, pudiéndose extender hasta el infinito.
1, 2, 8 o 24 horas	La duración de la ejecución de la tarea está acotada. Transcurrido el tiempo indicado, la tarea se cancela con error si no ha terminado.
Repetir	Establece un intervalo de repetición cada día, semana, mes o año tomando como referencia la fecha indicada en Empieza . Al establecer el campo a No , se configura una tarea de ejecución puntual o única.

Tabla 25.2: Configuración de la duración de la tarea

Publicar tareas

Una vez creada y configurada, la tarea aparecerá en el listado de tareas configuradas, pero mostrará la etiqueta **Sin publicar**, indicando que no está activa.

Haz clic en el enlace **Publicar** para introducir la tarea en el programador de Panda Adaptive Defense 360, encargado de marcar el momento en que se lanzan las tareas según su configuración.

Listado de tareas

Haz clic en el menú superior **Tareas** para listar tareas creadas, su tipo, estado y otra información relevante.

Campo	Comentario	Valores
Icono	Tipo de la tarea	•  Tarea de tipo instalación o desinstalación de parches •  Tarea de tipo análisis bajo demanda •  Tarea de tipo desinfección
Nombre	Nombre de la tarea creada	Cadena de caracteres
Programación	Cuando se ejecuta la tarea.	Cadena de caracteres
Estado	• Sin destinatarios: la tarea no se ejecutará porque no tiene destinatarios asignados. Asigna uno o más equipos a la tarea. • Sin publicar: la tarea no se ejecutará porque no ha entrado en la cola del programador. Publica la tarea para que el programador de procesos planifique su ejecución. • En curso: la tarea se está ejecutando. • Cancelada: la tarea fue cancelada de forma manual. No implica que todos los procesos en ejecución en los diferentes equipos se hayan detenido. • Finalizada: todos los equipos terminaron la ejecución de la tarea asignada, independientemente de que haya finalizado con éxito o con error. Este estado solo se da en las tareas de ejecución puntual o única.	Cadena de caracteres

Tabla 25.3: Campos del listado Tareas creadas

• Herramienta de filtrado

Campo	Comentario	Valores
Tipo de tarea	Clase de la tarea	- Análisis - Desinfección - Instalación de parches - Desinstalación de parches - Todos
Buscar tarea	Nombre de la tarea	Cadena de caracteres
Programación	Frecuencia de la repetición de la tarea	- Todos - Inmediata - Una vez - Programada
Ordenar listado 	Criterio de ordenación de las tareas creadas.	- Ordenar por fecha de creación - Ordenar por nombre - Ascendente - Descendente

Tabla 25.4: Campos de filtrado para el listado Tareas creadas

Gestionar tareas

Haz clic en el menú superior **Tareas** para borrar, copiar, cancelar o visualizar los resultados de las tareas creadas.

Modificar tareas publicadas

Haz clic en el nombre de la tarea creada para mostrar su ventana de configuración, donde es posible modificar algunos de sus parámetros.



Las tareas publicadas solo admiten cambio de nombre y de descripción. Para modificar otros parámetros de una tarea publicada, es necesario copiarla previamente.

Cancelar tareas publicadas

Haz clic en el enlace **Cancelar**. La tarea se cancelará, aunque no se borrará de la ventana de tareas para poder acceder a sus resultados.

Borrar tareas

Las tareas ejecutadas no se eliminan automáticamente, para ello es necesario hacer clic en las casillas de selección y después en el icono .



Al borrar una tarea se borrarán también sus resultados.

Copiar tareas

Para crear una nueva con su misma configuración haz clic en el icono .

Resultados de una tarea

Al hacer clic en el enlace **Ver resultados** de una tarea publicada se mostrarán los resultados obtenidos hasta ese momento y una herramienta de filtrado que permite localizar equipos específicos que recibieron la tarea.

Algunos de los campos incluidos en el listado de resultados son específicos de cada tarea. Estos campos se incluyen en la documentación del módulo correspondiente. A continuación se muestran los campos comunes a todos los listados de resultados.

Campo	Descripción	Valores
Equipo	Nombre del equipo donde se registró un evento de ejecución de tarea.	Cadena de caracteres
Grupo	Carpeta dentro del árbol de carpetas de Panda Adaptive Defense 360 a la que pertenece el equipo.	Cadena de caracteres
Estado	Estado del proceso asignado por la tarea para su ejecución en el equipo: • Pendiente: la tarea fue publicada correctamente pero el equipo no la ha recibido todavía; si la ha recibido, no ha iniciado su ejecución por estar programada para un momento posterior. • En curso: la tarea se está ejecutando en el equipo. • Finalizada: la tarea terminó con éxito.	Cadena de caracteres

Tabla 25.5: Campos comunes en el resultado de una tarea

Campo	Descripción	Valores
	• Con error: la tarea terminó con error. • Cancelada (no se pudo iniciar a la hora programada): la tarea estaba programada para iniciar su ejecución pero en ese momento el equipo estaba apagado o en un estado que impedía su ejecución. • Cancelada: el proceso fue cancelado en el equipo. • Cancelando: la tarea se canceló pero el equipo todavía no ha completado la orden de cancelar el proceso. • Cancelada (tiempo máximo superado): la tarea se canceló automáticamente al expirar el tiempo máximo establecido para su ejecución.	
Fecha de comienzo	Fecha de inicio de la tarea.	Fecha
Fecha fin	Fecha de finalización de la tarea.	Fecha

Tabla 25.5: Campos comunes en el resultado de una tarea

• **Herramienta de filtrado de tareas**

Campo	Descripción	Valores
Fecha	Desplegable con las fechas en las que la tarea pasó a estado activo según su programación configurada. Una tarea activa puede iniciarse en el momento o esperar a que el equipo esté disponible. Esta fecha se indica en la columna fecha.	Fecha
Estado	• Pendiente: la tarea todavía no se ha iniciado por no haber alcanzado la ventana de ejecución configurada. • En progreso: la tarea se está ejecutando en este momento. • Con éxito: la tarea terminó con éxito. • Con error: la tarea terminó con error.	Enumeración

Tabla 25.6: Filtros de búsqueda en los resultados de una tarea

Campo	Descripción	Valores
	• Cancelada (no se pudo iniciar a la hora programada): el equipo no estaba disponible en el momento del inicio de la tarea o en el intervalo definido. • Cancelada: la tarea fue cancelada de forma manual. • Cancelada (tiempo máximo expirado): la tarea duró más tiempo que el indicado en la configuración de la tarea y se canceló.	

Tabla 25.6: Filtros de búsqueda en los resultados de una tarea

Ajuste automático de los destinatarios de una tarea

Si el administrador establece un grupo de equipos como destinatario de una tarea, el conjunto final de equipos sobre los que se ejecutará puede variar debido a que los grupos son entidades dinámicas que varían a lo largo del tiempo.

De esta manera, una tarea definida en el momento T1 y asignada a un grupo tendrá como destinatarios los equipos que forman el grupo seleccionado, pero en el momento de ejecución posterior T2, los miembros de ese grupo pueden haber cambiado.

A la hora de resolver qué equipos pertenecen al grupo asignado a la tarea, se distinguen tres casos según su tipo:

- Tareas inmediatas.
- Tareas programadas de ejecución puntual o única.
- Tareas programadas de ejecución repetida.

Tareas inmediatas

Estas tareas se crean, se publican y se lanzan de forma atómica e inmediata una única vez. El grupo destinatario se evalúa en el momento en que el administrador crea la tarea. Los equipos afectados aparecerán en estado **Pendiente** en la tarea.

- **Añadir equipos al grupo destinatario**

No se permite añadir nuevos equipos. Aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea.

- **Quitar equipos del grupo destinatario**

Sí se pueden retirar equipos del grupo destinatario. Para cancelar la tarea mueve los equipos a otro grupo.

Tareas programadas de ejecución única

Estas tareas admiten dos estados con respecto a la posibilidad de cambiar a los integrantes del grupo de equipos destinatario:

- **Tareas cuya ejecución comenzó hace menos de 24 horas**

En las primeras 24 horas de la ejecución, el administrador puede añadir o retirar equipos a los grupos destinatarios. Se marca un plazo de 24 horas para abarcar todos los husos horarios en aquellas multinacionales con presencia en varios países.

- **Tareas cuya ejecución comenzó hace más de 24 horas**

Una vez cumplido el plazo de 24 horas no será posible añadir nuevos equipos y, aunque se asignen nuevos equipos al grupo destinatario, éstos no recibirán la tarea. Para cancelar las tareas en curso sobre equipos muévelos fuera del grupo destinatario.

Tareas programadas de ejecución repetida

Estas tareas permiten agregar o eliminar equipos destinatarios en cualquier momento hasta su cancelación o finalización.

Las tareas programadas de ejecución repetida no muestran los equipos destinatarios en estado **Pendiente** de forma automática, sino que éstos se irán mostrando de forma progresiva a medida que la plataforma Aether reciba información del estado de la tarea de cada equipo.



Parte 8

Información complementaria sobre Panda Adaptive Defense 360

Capítulo 26: Requisitos de hardware, software y red

Capítulo 27: La cuenta Panda

Capítulo 28: Conceptos clave

Capítulo 26

Requisitos de hardware, software y red

Panda Adaptive Defense 360 es un servicio cloud y como tal, Panda Security mantiene en sus instalaciones toda la infraestructura necesaria para proteger los equipos de sus clientes sin necesidad de desplegar software o hardware adicional en las redes de las organizaciones. No obstante, es necesario cumplir con ciertos requisitos mínimos en los equipos a proteger y en la red de la organización para garantizar un correcto funcionamiento del producto.

CONTENIDO DEL CAPÍTULO

Funcionalidades por plataforma	552
Requisitos de plataformas Windows	554
Sistemas operativos soportados	554
Estaciones de trabajo con microprocesador x86 y x64	554
Equipos con microprocesador ARM	554
Servidores con microprocesador x86 y x64	554
IoT y Windows Embedded Industry	555
Requisitos hardware	555
Otros requisitos	555
Requisitos de plataformas Windows Exchange	555
Sistemas operativos soportados	555
Requisitos hardware y software	556
Versiones Exchange soportadas	556
Requisitos de plataformas macOS	557
Sistemas operativos soportados	557
Requisitos hardware	557
Requisitos de plataformas Linux	557
Distribuciones de 64 bits soportadas	557
Versión de kernel de 64 bits soportada	558
Distribuciones de 32 bits soportadas	558
Versión de kernel de 32 bits soportada	558
Gestores de ficheros soportados	558
Requisitos hardware	558
Requisitos de plataformas Android	559
Sistemas operativos soportados	559
Requisitos hardware	559
Requisitos de red	559
Acceso a la consola web	559
Acceso a URLs del servicio	560
Puertos	561

Funcionalidades por plataforma

Características disponibles		Windows	Linux	macOS	Android
General	Consola web	X	X	X	X
	Dashboards	X	X	X	X
	Organización de los equipos por filtros	X	X	X	X
	Organización de los equipos en grupos	X	X	X	X
	Idiomas disponibles en agente	11	11	11	16
Listados e informes	Frecuencia de envío de detecciones al servidor	15 min	15 min	15 min	Tras fin análisis
	Listado de detecciones	X	X	X	X
	Informe ejecutivo	X	X	X	X
	Informe ejecutivo programado	X	X	X	X
Protecciones	Protección permanente AV (en tiempo real)	X	X	X	X
	Protección avanzada	X	X	X	
	Anti-tamper	X			
	Anti-exploit	X			
	Firewall	X			
	Control de dispositivos	X			
	Control de acceso a páginas web	X		X	
Información de hardware y software	Información y listado de hardware	X	X		X
	Información y listado de software	X	X	X	X

Tabla 26.1: Funcionalidades por plataforma

Características disponibles		Windows	Linux	macOS	Android
Configuraciones	Registro de cambios de software	X	X	X	X
	Información de los parches instalados del SO	X			
	Seguridad para estaciones y servidores	X	X	X	NA
	Contraseña para desinstalar y acciones en local	X			
	Asignar múltiples proxies	X			NA
	Actuar como Proxy Panda	X			NA
	Utilizar Proxy Panda	X			NA
	Actuar como Repositorio/Cache	X			NA
	Utilizar Repositorio/Cache	X			NA
	Descubre equipos desprotegidos	X			
Acciones remotas desde Consola Web	Alertas por correo ante infecciones	X			X
	Alertas por correo ante equipos desprotegidos	X			X
	Acciones en tiempo real	X	X	X	X
	Análisis bajo demanda	X	X	X	X
	Análisis programados	X	X	X	X
	Instalación remota del agente de Panda	X			
	Posibilidad de reinstalar agente de protección	X			
	Reiniciar	X	X	X	
	Aislar equipos	X			

Tabla 26.1: Funcionalidades por plataforma

Características disponibles		Windows	Linux	macOS	Android
	Bloqueo de programas por hash y nombre	X			
	Reportar un incidencia (PSInfo)	X			X
Actualizaciones	Actualizaciones de firmas	X	X	X	X
	Actualizaciones de la protección	X	X	X	X
	Programar la actualización de la protección	X	X	X	Google Play

Tabla 26.1: Funcionalidades por plataforma

Requisitos de plataformas Windows

Sistemas operativos soportados

Estaciones de trabajo con microprocesador x86 y x64

- Windows XP SP3 (32 bits)
- Windows Vista (32 y 64-bit)
- Windows 7 (32 y 64-bit)
- Windows 8 (32 y 64-bit)
- Windows 8.1 (32 y 64-bit)
- Windows 10 (32 y 64-bit)

Equipos con microprocesador ARM

- Windows 10 Pro
- Windows 10 Home

Servidores con microprocesador x86 y x64

- 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 y 2019
- Windows Server Core 2008, 2008 R2, 2012 R2, 2016 y 2019

IoT y Windows Embedded Industry

- Windows XP Embedded
- Windows Embedded for Point of Service
- Windows Embedded POSReady 2009, 7, 7 (64 bits)
- Windows Embedded Standard 2009, 7, 7 (64 bits), 8, 8 (64 bits),
- Windows Embedded Pro 8, 8 (64 bits)
- Windows Embedded Industry 8, 8 (64 bits), 8.1, 8.1 (64 bits)
- Windows IoT Core 10, 10 (64 bits)
- Windows IoT Enterprise 10, 10 (64 bits)

Requisitos hardware

- **Procesador:** CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM:** 1 Gbyte
- **Espacio libre en el disco duro para la instalación:** 650 Mbytes

Otros requisitos

Para un funcionamiento correcto del producto es necesario mantener actualizados los certificados raíz de los equipos de usuario y servidores. En caso de no cumplir con este requisito, algunas funcionalidades como la comunicación en tiempo real de los agentes con la consola de administración y el módulo Panda Patch Management podrían dejar de funcionar.

Requisitos de plataformas Windows Exchange

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.
- **Exchange 2019:** Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 y Windows

Server 2019.

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)

- Exchange 2019

<https://docs.microsoft.com/es-es/Exchange/plan-and-deploy/system-requirements?view=exchserver-2019>

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
- Microsoft Exchange Server 2019 Standard y Enterprise

Requisitos de plataformas macOS

Sistemas operativos soportados

- macOS 10.10 Yosemite
- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11.0 Big Sur

Requisitos hardware

- **Procesador:** Intel Core 2 Duo
- **Memoria RAM:** 2 Gbyte
- **Espacio libre en el disco duro para la instalación:** 400 Mbytes
- **Puertos:** se requieren los puertos 3127, 3128, 3129 y 8310 libres para el funcionamiento del filtrado web y la detección web de malware.

Requisitos de plataformas Linux

Panda Adaptive Defense 360 se instala tanto en estaciones de trabajo como en servidores Linux. Si no está presente un entorno gráfico en el momento de la instalación las protecciones URL filter y Web filter quedarán deshabilitadas. En equipos sin entorno gráfico utiliza la herramienta `/usr/local/protection-agent/pa_cmd` para controlar la protección.

Para completar la instalación de Panda Adaptive Defense 360 en plataformas Linux es necesario que el equipo tenga conexión a Internet durante todo el proceso.

Distribuciones de 64 bits soportadas

- Ubuntu 14.04 LTS, 14.10, 15.04, 15.10, 16.0.4 LTS, 16.10, 17.04, 17.10, 18.04, 18.10 y 19.04
- Fedora 23, 24, 25, 26, 27, 28, 29, 30 y 31
- Debian 8, 9 y 10
- RedHat 7, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8, 8.0, 8.1
- CentOS 7, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8, 8.0, 8.1
- LinuxMint 18, 18.1, 18.2, 18.3, 19, 19.1, 19.2

Versión de kernel de 64 bits soportada

- **Versión mínima soportada:** 3.10
- **Versión máxima soportada:** 5.5.0 64 bits

Distribuciones de 32 bits soportadas

- RedHat 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10
- CentOS 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10

Versión de kernel de 32 bits soportada

- **Versión mínima soportada:** 2.6.32-71
- **Versión máxima soportada:** 2.6.32-754



Para más información sobre las distribuciones y kernels soportados en Linux consulta <https://www.pandasecurity.com/es/support/card?id=700009#show2>.

Gestores de ficheros soportados

- Nautilus
- Pcmannfm
- Dolphin

Requisitos hardware

- **Procesador:** CPU compatible x86 o x64 y con soporte SSE2.
- **Memoria RAM:** 1.5 Gbytes
- **Espacio libre en el disco duro para la instalación:** 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.
- **Dependencias del paquete de instalación**

El agente Linux descargará en el proceso de instalación todos los paquetes necesarios para satisfacer las dependencias. De forma general los paquetes necesarios en el sistema para poder funcionar son 3:

- Libcurl
- OpenSSL

- Gcc y las utilidades de compilación (make, makeconfig etc.) en Fedora



El proceso de instalación en Fedora incluye la compilación de los módulos necesarios para el buen funcionamiento del agente Panda Adaptive Defense 360.

Para mostrar las dependencias del agente ejecuta los comandos mostrados a continuación en una terminal según la distribución de destino:

- Para distribuciones basadas en Debian: `dpkg --info paquete.deb`
- Para distribuciones basadas en Fedora: `rpm --qRp paquete.rpm`

Requisitos de plataformas Android

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
- Pie 9.0
- Android 10

Requisitos hardware

Se requiere un mínimo de 10 megabytes de espacio en la memoria interna del dispositivo. Dependiendo del modelo es posible que el espacio requerido sea superior.

Requisitos de red

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

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

Acceso a URLs del servicio

Para el correcto funcionamiento de Panda Adaptive Defense 360 es necesario que las URL mostradas a continuación sean accesibles desde los equipos protegidos de la red.

Nombre de producto	URLs
Panda Adaptive Defense 360	• https://*.pandasecurity.com • Descarga de instaladores, desinstalador genérico y políticas. • Comunicaciones de agente (registro, configuración, tareas, acciones, estados comunicación en tiempo real). • Comunicaciones de protección con Inteligencia colectiva. • Descarga de ficheros de firmas en Android. • http://*.pandasecurity.com • Descarga de ficheros de firmas (salvo Android). • https://*.windows.net • Contadores de rendimiento (cpu, memoria, disco etc.) • Notificaciones cada 15 minutos en caso de no disponer de comunicación en tiempo real.
Certificados raiz	• http://*.globalsign.com • http://*.digicert.com
Antispam y filtrado web	• http://*.pand.ctmail.com • http://download.ctmail.com • https://rp.cloud.threatseeker.com
Panda Data Control	• https://pandasecurity.devo.com
Panda Patch Management	• Todas las URLs contenidas en el recurso https://forums.ivanti.com/s/article/URL-Exception-List-for-Ivanti-Patch-for-SCCM • https://content.ivanti.com

Tabla 26.2: URLs de acceso al servicio

Nombre de producto	URLs
Testeo de la actividad	• http://proinfo.pandasoftware.com/connectiontest.html Para versiones de protección Windows superiores a 8.00.16 • http://*.pandasoftware.com Para el test de conectividad.

Tabla 26.2: URLs de acceso al servicio

Puertos

- Port 80 (HTTP)
- Port 443 (HTTPS, websocket)
- Puerto 8080 (acceso desde Orion)

Descarga de parches y actualizaciones (Panda Patch Management)

Consulta la pagina de soporte <https://www.pandasecurity.com/spain/support/card?id=700044> para obtener un listado completo de las urls accesibles desde los equipos de la red que recibirán los parches o desde los equipos con rol de caché / repositorio.

Capítulo 27

La cuenta Panda

La Cuenta Panda ofrece al administrador un mecanismo de auto gestión de credenciales y acceso 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 Panda Adaptive Defense 360.



Los usuarios que tienen acceso a la cuenta Panda son aquellos que fueron dados de alta inicialmente en Panda Security, tanto si posteriormente han sido migrados al proveedor WatchGuard como si no. Los usuarios que pertenecen al proveedor de seguridad WatchGuard desde el inicio no tiene acceso a la cuenta Panda.

CONTENIDO DEL CAPÍTULO

Crear una cuenta Panda para usuarios de Panda Security - - - - -	563
Recepción del mensaje de correo	563
Rellenar el formulario	564
Activar la Cuenta Panda - - - - -	564
Modificar la cuenta Panda	565
Crear y vincular una cuenta Panda con WatchGuard - - - - -	565
Crear una cuenta Panda automáticamente al asignar una licencia comercial de producto Panda Security	566
Vincular una cuenta Panda a la cuenta WatchGuard al asignar una licencia comercial de producto Panda Security	566

Crear una cuenta Panda para usuarios de Panda Security

Para crear una nueva Cuenta Panda es necesario seguir el procedimiento descrito a continuación.

Recepción del mensaje de correo

- Al adquirir Panda Adaptive Defense 360 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 donde crear la Cuenta Panda.

Rellenar 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** para terminar y recibir un mensaje de correo electrónico en la dirección especificada en el formulario. Utiliza ese mensaje para activar la cuenta.

Activar 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 de 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. Si botón no funciona, copia en el navegador el enlace que se muestra en el mensaje.
- La primera vez que accedes a la Cuenta Panda el sistema 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 Cytomic Central. Desde aquí puedes acceder a la consola Web de Panda Adaptive Defense 360. Para ello, utiliza el icono de acceso directo que encontrarás en **Mis servicios**.

Modificar la cuenta Panda

Si tu proveedor de seguridad asociado es Panda Security, haz clic en la opción **Edit account** en Cytomic Central.



Figura 27.1: Editar cuenta de usuario

Si tu proveedor de seguridad asociado es WatchGuard, accede a la web <https://watchguard.com/>

Crear y vincular una cuenta Panda con WatchGuard



Para obtener más información sobre cómo activar y vincular la cuenta Panda al activar una licencia comercial, consulta <https://www.pandasecurity.com/es/support/card?id=300003>.

Para que un usuario de WatchGuard pueda gestionar los productos de Aether, es necesario cumplir con los siguientes requisitos:

- Tener una cuenta de usuario en WatchGuard.
- Tener una cuenta de usuario en Panda Adaptive Defense 360.
- Vincular ambas cuentas.

Los usuarios que pertenecen al proveedor de seguridad WatchGuard desde el inicio, crean una cuenta Panda automáticamente al activar por primera vez una licencia comercial de un producto de Panda Security.

Los usuarios que pertenecen al proveedor de seguridad WatchGuard pero que inicialmente pertenecían a Panda Security, ya tienen creada la cuenta Panda y solo tienen que vincularla con su cuenta WatchGuard.

Crear una cuenta Panda automáticamente al asignar una licencia comercial de producto Panda Security

- Accede a la web <https://watchguard.com/activate> e introduce la clave de licencia del producto Panda Security.
- Haz clic en **I need a Panda account**. Se mostrará una ventana con el identificador de la cuenta y el nombre. Guarda esta información para más adelante.
- Haz clic en **Submit** y **Continue**. Se mostrará el **Centro de Soporte de WatchGuard**.
- Si la página web lo solicita, introduce de nuevo la clave de licencia del producto Panda Security. Se mostrará el asistente **Activar producto**.
- Para aceptar las condiciones de uso de la licencia haz clic en el botón **Siguiente**.
- En el desplegable **Select a license** selecciona la opción **New license** y haz clic en el botón **Next**.
- Introduce un nombre descriptivo que te permita identificar el producto en la web de WatchGuard y haz clic en el botón **Next**.
- Selecciona la casilla **I accept the enduser license agreement** y haz clic en **Next**. Se mostrará la página **Activación Completada** y tu licencia se añadirá al pool de licencias correspondiente en Panda Adaptive Defense 360.
- Para acceder a Panda Adaptive Defense 360, haz clic en **Manage Your Panda Product** y a continuación haz clic en **Accept and continue** para aceptar el Acuerdo de Licencia de Usuario Final.

Vincular una cuenta Panda a la cuenta WatchGuard al asignar una licencia comercial de producto Panda Security

- Accede a la web <https://watchguard.com/activate> e introduce la clave de licencia del producto Panda Security.
- Haz clic en **Link my Panda account**. Se mostrará la ventana de Cytomic Central solicitando las credenciales de Panda Adaptive Defense 360 enviadas en el correo de bienvenida.
- Introduce las credenciales y haz clic en el botón **Log in**. Se mostrará una ventana indicando que las cuentas están vinculadas.
- Haz clic en **Continue**. Se mostrará el **Centro de Soporte de WatchGuard**.
- Si la página web lo solicita, introduce de nuevo la clave de licencia del producto Panda Security. Se mostrará el asistente **Activar producto**.
- Para aceptar las condiciones de uso de la licencia haz clic en el botón **Siguiente**.
- En el desplegable **Select a license** selecciona la opción **New license** y haz clic en el botón **Next**.
- Introduce un nombre descriptivo que te permita identificar el producto en la web de WatchGuard y haz clic en el botón **Next**.
- Selecciona la casilla **I accept the enduser license agreement** y haz clic en **Next**. Se mostrará la página **Activación Completada** y tu licencia se añadirá al pool de licencias correspondiente en

Panda Adaptive Defense 360.

- Para acceder a Panda Adaptive Defense 360, haz clic en **Manage Your Panda Product** y a continuación haz clic en **Accept and continue** para aceptar el Acuerdo de Licencia de Usuario Final.

Capítulo 28

Conceptos clave

100% Attestation Service

Servicio de Panda Adaptive Defense 360 incluido en la licencia básica que clasifica el 100% de los procesos ejecutados en los equipos de usuario y servidores para emitir una valoración sin ambigüedades (goodware o malware, sin sospechosos).

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 de cliente Panda Adaptive Defense 360. Se encarga de las comunicaciones entre los equipos de la red y los servidores en la nube de Panda Security, además de gestionar los procesos locales.

Alerta

Ver ["Incidencia"](#).

Análisis forense

Conjunto de técnicas y procesos ejecutados por el administrador de la red con herramientas especializadas para seguir la ejecución de un programa malicioso y determinar las consecuencias de la infección.

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.

Antirrobo

Conjunto de tecnologías incorporadas en Panda Adaptive Defense 360 que facilitan la localización de los dispositivos móviles extraviados y minimizan la exposición de los datos que contienen en caso de robo.

Anti-tamper

Conjunto de tecnologías que evitan la manipulación de los procesos de Panda Adaptive Defense 360 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.

APT (Advanced Persistent Threat)

Conjunto de estrategias emprendidas por hackers orientadas a infectar la red del cliente, utilizando múltiples vectores de infección de forma simultánea para pasar inadvertidos a los antivirus tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial de la empresa para chantaje, robo de propiedad intelectual etc.).

ASLR (Address Space Layout Randomization)

Técnica implementada por el sistema operativo para mitigar los efectos de ataques de tipo exploit basados en desbordamiento de buffer. Mediante ASLR el sistema operativo introduce aleatoriedad a la hora de asignar direcciones de memoria para reservar espacio destinado a la pila, el heap y las librerías cargadas por los procesos. De esta forma, se dificulta la utilización ilegítima de llamadas a funciones del sistema por desconocer la dirección física de memoria donde residen.

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.

Audit

Modo de configuración de Panda Adaptive Defense 360 para visualizar la actividad de los procesos ejecutados en los equipos protegidos de la red sin desencadenar ninguna acción de protección (desinfección o bloqueo).

Backup

Área de almacenamiento de ficheros maliciosos no desinfectables, así como de spyware y herramientas de hacking detectadas. Todos los programas eliminados del sistema por ser clasificados como amenazas se copian de forma temporal en el área de backup / cuarentena durante un periodo de entre 7 y 30 días según su tipo.

BitLocker

Software instalado en algunas versiones de los equipos Windows 7 y superiores encargado de gestionar el cifrado y descifrado de los datos almacenados en los volúmenes del equipo y utilizado por Panda Full Encryption.

Bloquear

Acción de Panda Adaptive Defense 360 que impide la ejecución de los programas instalados en el equipo del usuario debido a uno de los motivos siguientes:

- Programas clasificados como amenaza.
- Programas desconocidos para Panda Adaptive Defense 360 y la política de protección avanzada esta configurada como lock o como hardening y su origen es no confiable.
- Programas bloqueados por políticas establecidas por el administrador.

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.

Caché / Repositorio (rol)

Equipos que descargan y almacenan de forma automática todos los ficheros necesarios para que otros equipos con Panda Adaptive Defense 360 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.

Cambio de comportamiento

Al clasificar como malware o goodware un programa que el administrador permitió su ejecución cuando todavía era desconocido, Panda Adaptive Defense 360 se puede comportar de dos maneras:

- Eliminarlo de la lista de Programas permitidos: si se ha clasificado como goodware seguirá pudiéndose ejecutar, si se ha clasificado como malware, se impedirá su ejecución.
- Mantener en la lista de Programas permitidos: se seguirá permitiendo su ejecución independientemente de que se trate de malware o goodware.

Ciclo de protección adaptativa

Nuevo enfoque de seguridad basado en la integración de un conjunto de servicios de protección, detección, monitorización, análisis forense y resolución, todos ellos centralizados en una única consola de administración accesible desde cualquier lugar y en cualquier momento.

Ciclo de vida del malware

Detalle de todas las acciones desencadenadas por un programa malicioso, desde que fue visto por primera vez en un equipo del cliente hasta su clasificación como malware y posterior desinfección.

Clave de recuperación

Cuando se detecta una situación anómala en un equipo protegido con Panda Full Encryption o en el caso de que hayamos olvidado la contraseña de desbloqueo, el sistema pedirá una clave de recuperación de 48 dígitos. Esta clave se gestiona desde la consola de administración y debe ser introducida para completar el inicio del equipo. Cada volumen cifrado tendrá su propia clave de recuperación independiente.

Configuración

Ver "[Perfil de configuración](#)".

Control de dispositivos

Módulo que define el comportamiento del equipo protegido al conectar dispositivos extraíbles o de almacenamiento masivo, para minimizar la superficie de exposición del equipo.

Control de acceso a páginas web

Tecnología que controla y filtra 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 Panda Adaptive Defense 360, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible. Con la consola web el administrador puede desplegar el software de protección, establecer las configuraciones de seguridad y visualizar el estado de la protección. También permite utilizar herramientas de análisis forense que establecen el alcance de los problemas de seguridad.

Cuarentena

Ver "[Backup](#)".

Cuenta de usuario

Ver "[Usuario \(consola\)](#)".

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Desbloqueado (programa)

Programas inicialmente bloqueados por no haber obtenido todavía una clasificación, pero que el administrador de la red permite su ejecución de forma selectiva y temporal para minimizar las molestias a los usuarios de la red.

Desbordamiento de buffer

Fallo en la gestión de los buffers de entrada de un proceso. En estos casos, si el volumen de datos recibido es mayor que el tamaño del buffer reservado, los datos sobrantes no se descartan, sino que se escriben en zonas de memoria adyacentes al buffer. Estas zonas de memoria pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.

Descubridor (rol)

Equipos capaces descubrir puestos de usuario y servidores no administrados para iniciar una instalación remota del agente Panda Adaptive Defense 360.

DEP

Característica de los sistemas operativos que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.

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).

Entidad

Predicado o complemento incluido en las tablas de acciones del módulo análisis forense.

Entidad (Panda Data Control)

Conjunto de datos que tomados como una unidad adquieren un significado propio.

EoL (End Of Life)

Término utilizado para indicar el final del ciclo de vida de un producto. A partir de la fecha indicada el producto ya no recibirá actualizaciones ni parches que corrijan sus defectos, convirtiéndose en un objetivo claro para los hackers.

Equipos sin licencia

Equipos cuya licencia ha caducado o no ha sido posible asignar una licencia válida por haberse superado el número máximo permitido de instalaciones de la protección. Estos equipos no están protegidos, pero son visibles en la consola web de administración.

Excluido (programa)

Son programas inicialmente bloqueados por haber sido clasificados como malware o PUP, pero que el administrador de la red permite su ejecución de forma selectiva y temporal excluyéndolos del análisis.

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, es una tecnología que bloquea el tráfico de red que coincide con patrones definidos por el administrador mediante reglas. De esta manera se limita o impide la comunicación de ciertas aplicaciones que se ejecutan en los equipos, restringiéndose la superficie de exposición del equipo.

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.

FQDN (Fully Qualified Domain Name)

Es un nombre de dominio que especifica la localización de forma precisa y sin ambigüedades dentro del árbol de jerarquía del sistema de nombres DNS. El FQDN especifica todos los niveles del dominio incluyendo el nivel superior y la zona raíz (root).

Fragmentación

En redes de transmisión de datos, cuando la MTU del protocolo subyacente es menor que el tamaño del paquete a transmitir, los encaminadores dividen el paquete en piezas más pequeñas (fragmentos) que se encaminan de forma independiente y se ensamblan en el destino en el orden apropiado.

GDPR (General Data Protection Regulation)

Normativa que regula la protección de los datos de los ciudadanos que viven en la Unión Europea. Consulta el enlace <http://www.privacy-regulation.eu/es/index.htm> para acceder al reglamento completo.

Geolocalizar

Posicionar en un mapa un dispositivo en función de sus coordenadas.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

Grafo de actividad / grafo de ejecución

Representación visual de las acciones ejecutadas por las amenazas, poniendo énfasis en el enfoque temporal.

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.

Hardening

Modo de configuración de Panda Adaptive Defense 360 que bloquea los programas clasificados como malware y los ficheros desconocidos cuyo origen es una fuente no fiable:

- Internet.
- Unidades externas de almacenamiento
- Otros equipos de la red del cliente.

Heap Spraying

Head Spray es una técnica utilizada para facilitar la explotación de vulnerabilidades por parte de un proceso malicioso independiente.

Debido a la constante mejora de los sistemas operativos, la explotación de vulnerabilidades se ha convertido en un proceso muy aleatorio. Debido a que el comienzo de la región de memoria heap de un proceso es predecible, y las posteriores reservas de espacio son secuenciales, Head Spray aporta predictibilidad a los ataques, sobrescribiendo porciones de la región de memoria heap del proceso objetivo. Estas porciones de memoria serán referenciadas más adelante por un proceso malicioso para ejecutar el ataque.

Esta técnica es muy empleada para explotar vulnerabilidades de navegadores y sus plugins correspondientes.

Herencia

Método de asignación automática de configuraciones sobre todos los grupos descendientes de un grupo padre, ahorrando tiempo de gestión. También llamado Asignación automática de configuraciones o Asignación indirecta de configuraciones.

Herramienta de hacking

Programa utilizado por hackers para causar perjuicios a los usuarios de un ordenador, pudiendo provocar el control del ordenador afectado, obtención de información confidencial, chequeo de puertos de comunicaciones, etc.

Hoaxes

Falsos mensajes de alarma sobre amenazas que no existen y que llegan normalmente a través del correo electrónico.

ICMP (Internet Control Message Protocol)

Protocolo de control y notificación de errores utilizado por el protocolo IP en Internet.

Identificador

Palabra clave utilizada en las búsquedas de Panda Data Control que permite seleccionar un tipo de entidad.

IDP (Identity Provider)

Servicio centralizado responsable de gestionar las identidades de los usuarios.

IFilter

Librería del sistema operativo que permite el acceso al contenido de ficheros ofimáticos.

Incidencia

Mensaje relativo a la protección avanzada de Panda Adaptive Defense 360, susceptible de requerir la intervención del administrador. Las incidencias se reciben mediante la consola de administración y el correo electrónico (alertas), y el usuario del equipo protegido mediante mensajes generados por el agente que se visualizan en el escritorio de su dispositivo.

Indexar

Proceso que analiza el contenido de los ficheros y lo almacena en una base de datos de rápido acceso para acelerar su búsqueda.

Informes avanzados

Ver "[Adware](#)".

IP (Internet Protocol)

Principal protocolo de comunicación en Internet para el envío y recepción de los datagramas generados en el nivel de enlace subyacente.

Inventario

Base de datos mantenida por Panda Data Control con los ficheros clasificados como PII encontrados en el parque informático.

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.

Llave USB

Dispositivo utilizado en equipos con volúmenes cifrados que permite almacenar la clave en una memoria portátil. De esta forma, no se requiere introducir ninguna contraseña en el proceso de inicio del equipo, aunque es necesario que el dispositivo USB que almacena la contraseña esté conectado en el equipo.

Lock

Modo de configuración de Panda Adaptive Defense 360 que bloquea los programas desconocidos y los ya clasificados como amenazas.

Machine learning

Es una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas para capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos.

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.

Microsoft Filter Pack

Paquete de librerías IFilter que abarca todos los formatos de fichero generados por la suite de ofimática Microsoft Office.

MTU (Maximum transmission unit)

Tamaño máximo del paquete que el protocolo subyacente puede transportar.

Normalización

En Panda Data Control, es una tarea que forma parte del proceso de indexación de textos, y que consiste en eliminar todos los caracteres innecesarios (generalmente caracteres separadores o delimitadores) antes de almacenarlos en la base de datos.

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.

Parche

Pequeños programas publicados por los proveedores de software que modifican sus programas corrigiendo fallos y añadiendo nuevas funcionalidades.

Panda Advanced Reporting Tool

Servicio avanzado de explotación del conocimiento generado en tiempo real por los productos Panda Adaptive Defense y Panda Adaptive Defense 360. Facilita el descubrimiento de amenazas desconocidas, ataques dirigidos y APTs, representando los datos de actividad de los procesos ejecutados por los usuarios y poniendo el énfasis en los eventos relacionados con la seguridad y la extracción de información.

Panda Data Control

Módulo compatible con Panda Adaptive Defense 360 que descubre ficheros PII en la red de la empresa y monitoriza su acceso para cumplir con las regulaciones de almacenamiento de datos vigentes, tales como la GDPR.

Panda Full Encryption

Módulo compatible con Panda Adaptive Defense 360 que cifra el contenido de los dispositivos de almacenamiento interno del equipo. Su objetivo es minimizar la exposición de los datos de la empresa ante la pérdida o robo, o en caso de sustitución y retirada de los dispositivos de almacenamiento sin formatear.

Panda Patch Management

Módulo compatible con Panda Adaptive Defense 360 que parchea y actualiza los programas instalados en los equipos de usuario y servidores para eliminar las vulnerabilidades producidas por fallos de programación, minimizando así su superficie de ataque.

Panda SIEMFeeder

Módulo compatible con Panda Adaptive Defense 360 que envía al servidor SIEM de la empresa toda la telemetría generada por los procesos ejecutados en los equipos de usuario y servidores.

Partición de sistema

Zona del disco duro que permanece sin cifrar y que es necesaria para que el equipo complete correctamente el proceso de inicio en los equipos con Panda Full Encryption activado.

Partner

Empresa que ofrece productos y servicios de Panda Security.

Passphrase

También llamado Enhanced PIN (PIN mejorado) o PIN extendido, es una contraseña equivalente al PIN pero que permite añadir caracteres alfanuméricos. Se aceptan letras en mayúscula y minúscula, números, espacios en blanco y símbolos.

Payload

En informática y telecomunicaciones es el conjunto de datos transmitidos útiles, que se obtienen de excluir cabeceras, información de control y otros datos que son enviados para facilitar la entrega del mensaje.

En seguridad informática referida a amenazas de tipo exploit, payload es la parte del código del malware que realiza la acción maliciosa en el sistema, como borrar los ficheros o enviar datos al exterior, frente a la parte del encargado de aprovechar una vulnerabilidad (el exploit) que permite ejecutar el payload.

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.

PII (Personally Identifiable Information)

Ficheros que contienen datos que pueden ser utilizados para identificar o localizar a personas concretas.

PIN (Personal Identification Number, número de identificación personal)

Secuencia de números que actúa como contraseña simple y es requerida en el inicio de un equipo que tenga un volumen cifrado. Sin el PIN la secuencia de arranque no se completa y el acceso al equipo no es posible.

Proceso comprometido

Son aquellos procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo de usuario.

Proceso vulnerable

Son programas que, debido a fallos de programación, no son capaces de interpretar correctamente los datos recibidos de otros procesos. Al recibir una secuencia de datos especialmente diseñada (exploit), los hackers pueden provocar un mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del equipo del usuario.

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 Panda Adaptive Defense 360 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.

Protección avanzada

Tecnología de monitorización continua y recogida de información de los procesos ejecutados en los equipos de la red para su posterior envío de a la nube de Panda Security. Allí, se analiza mediante técnicas de Machine Learning en entornos Big Data para emitir una clasificación (goodware o malware) precisa.

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 Panda Adaptive Defense 360.

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.

Reclasificación de elementos

Ver Cambio de comportamiento.

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 para esconder evidencias y utilidades en sistemas previamente comprometidos.

ROP

ROP es una técnica de ejecución de exploits que permite a un atacante ejecutar código arbitrario en presencia de defensas como DEP o ASLR.

Los ataques tradicionales basados en desbordamiento de pila consistían en sobrescribir regiones de memoria enviando bloques de datos a la entrada de programas que no controlaban debidamente el tamaño de los datos recibidos. Estos ataques dejaron de funcionar cuando técnicas como DEP fueron implementadas de forma masiva en los sistemas operativos: en esta nueva situación el sistema operativo impide la ejecución del "código desbordado" ya que reside en regiones de memoria marcadas como de no ejecución (datos). ROP sobrescribe la pila de llamadas (call stack) de un proceso para ejecutar zonas de código del propio proceso, conocidas como "gadgets". Así, el atacante puede "armar" un flujo de ejecución alternativo al del proceso original, formado por partes de código del proceso atacado.

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.

SIEM (Security Information and Event Management)

Software que ofrece almacenamiento y análisis en tiempo real de las alertas generadas por los dispositivos de red.

Software cliente Panda Adaptive Defense 360

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 Panda Adaptive Defense 360, 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.

Threat hunting

Conjunto de tecnologías y recursos humanos especializados que permiten detectar los movimientos laterales y otros indicadores tempranos de las amenazas, antes de que ejecuten acciones nocivas para la empresa.

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 de los datos 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.

TPM (Trusted Platform Module, módulo de plataforma segura)

Es un chip que se incluye en algunas placas base de equipos de sobremesa, portátiles y servidores. Su principal objetivo es proteger la información sensible de los usuarios, almacenando claves y otra información utilizada en el proceso de autenticación.

Además, el TPM es el responsable de detectar los cambios en la cadena de inicio del equipo, impidiendo por ejemplo el acceso a un disco duro desde un equipo distinto al que se utilizó para su cifrado.

UDP (User Datagram Protocol)

Protocolo del nivel de transporte dentro de la pila de protocolos de Internet, no confiable y no orientado a la conexión para el envío y recepción de paquetes IP.

Usuario (consola)

Recurso formado por un conjunto de información que Panda Adaptive Defense 360 utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Personal de la empresa que utiliza equipos informáticos para desarrollar su trabajo.

Variable de entorno

Cadena compuesta por información del entorno, como la unidad, la ruta de acceso o el nombre de archivo, asociada a un nombre simbólico que pueda utilizar Windows. La opción Sistema del Panel de control o el comando set del símbolo del sistema permiten definir variables de entorno.

VDI (Virtual Desktop Infrastructure)

Solución de virtualización de escritorio que consiste en alojar máquinas virtuales en un centro de datos al cual los usuarios acceden desde un terminal remoto con el objetivo de centralizar y simplificar la gestión y reducir los costes de mantenimiento. Se distinguen dos grupos de entornos VDI:

- **Persistente:** el espacio de almacenamiento asignado a cada usuario se respeta entre reinicios, incluyendo el software instalado, datos y actualizaciones del sistema operativo.
- **No persistente:** el espacio de almacenamiento asignado a cada usuario se elimina cuando la instancia VDI se reinicia, restaurándose a su estado inicial y deshaciendo todos los cambios efectuados.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de su infección. Durante este periodo de tiempo el malware puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia.

Virus

Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

VPN (Virtual Private Network)

Tecnología de red que permite interconectar redes privadas (LAN) utilizando un medio público, como puede ser Internet.

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 Panda Adaptive Defense 360.

