

Junio 2016

Guía Básica de Soporte Técnico

Productos Adaptive Defense/Endpoint Protection

Índice

1. Introducción	3
2. Alcance	3
3. Público objetivo	3
4. Requisitos previos y recomendaciones.....	3
5. Estructura y entrega del documento	4
6. Escenarios Comunes	6
IDP/Cuenta Panda	6
Errores de la consola Web	7
Errores del agente	8
Error al instalar/desinstalar la protección.....	9
Error al instalar/desinstalar el agente.....	10
Producto no actualizado (updates o upgrades).....	11
BSOD.....	12
Problemas con la protección avanzada (sólo para Adaptive Defense 360).....	12
Errores en la protección permanente del antivirus o errores al analizar	14
Errores de firewall, pérdida de la conexión a Internet o pérdida del acceso a recursos de red	15
Software de terceros.....	17
Malware.....	17
7. Anexo.....	22
URLs.....	22
Activación de los logs del agente	22
PSInfo	22
Comprobación de puertos.....	23

PSErrorTrace.....	23
La herramienta PSErrorTrace recoge información útil para diagnosticar y estudiar problemas de Endpoint Protection relacionados con la instalación, el análisis o la compatibilidad con software de terceros.....	23
Configurador local de la protección avanzada	24
NNSDiag.....	24
Desactivación de opciones de configuración	25
Cómo generar un archivo de volcado de memoria post-mortem (BSOD)	25
Lista de errores genéricos	28

1. Introducción

El propósito de esta guía es ayudar a los técnicos a proporcionar una primera línea de soporte al atender las consultas de los clientes.

Este documento se aplica a los siguientes productos:

- Endpoint Protection
- Endpoint Protection Plus
- Adaptive Defense 360

El motivo de emplear un único documento para distintos productos es que comparten sus tecnologías básicas. Es más, las mejoras o tecnologías compartidas introducidas en una de las soluciones son inmediatamente aplicadas al resto de productos. No obstante, debemos indicar que algunas de las secciones del documento pueden ser específicas de un producto en concreto, al referirnos a alguna de las tecnologías que lo diferencian del resto.

2. Alcance

El objetivo del documento no es cubrir el 100% de escenarios posibles, algo que resultaría imposible, sino las situaciones más habituales y conocidas a las que se enfrentan nuestros clientes. La mayoría de casos presentados en este documento terminan en una solución, o en una petición de información para escalar el caso a un nivel más alto de la estructura de soporte de cara a su análisis y resolución.

3. Público objetivo

El público objetivo de este documento es cualquier técnico que atienda consultas de clientes vía telefónica, email, chat, etc. En otras palabras, cualquier técnico que ofrezca soporte de Primer Nivel. Las herramientas y procedimientos sugeridos son los estándares para cualquiera que ofrezca soporte técnico a un usuario corporativo.

4. Requisitos previos y recomendaciones

Pese a que el documento pretende ser una guía fácil de seguir, existen una serie de requisitos previos que resultan altamente recomendables (si no obligatorios), antes de empezar con su uso. Estos son los más importantes, entre otros:

- Asegúrate de haber leído [la documentación del producto](#), así como la ayuda online, accesible desde la consola del producto.
- Haz un recorrido general del producto mediante acceso Web antes y durante el proceso de resolución de la consulta.
- Trabaja, siempre que sea posible, con la última versión del producto y recomienda al cliente que migre a dicha versión, ya que normalmente incluye correcciones a errores detectados en versiones anteriores.

5. Estructura y entrega del documento

El documento está estructurado siguiendo las áreas principales que puede identificar el técnico al recibir consultas/peticiones de nuestros clientes:

- IDP/Cuenta Panda
- Errores de la consola Web
- Errores del agente
- Error al instalar/desinstalar la protección
- Error al instalar/desinstalar el agente
- Producto no actualizado (updates o upgrades)
- BSOD
- Problemas con Adaptive Defense
- Errores en la protección permanente del antivirus o errores al analizar
- Errores de firewall, pérdida de la conexión a Internet o pérdida del acceso a recursos de red
- Consumo excesivo de recursos
- Software de terceros
- Malware

Este es un documento vivo que irá incluyendo cambios al objeto de mantener la guía actualizada.

Cada sección incluye las instrucciones y procedimientos más útiles a la hora de resolver el problema correspondiente.

Por último, se ha añadido un anexo con información sobre cómo utilizar las principales herramientas de soporte.

6. Escenarios Comunes

IDP/Cuenta Panda

Los productos Cloud para empresas de Panda delegan la gestión de las credenciales de acceso a un Proveedor de Identidades (IDP): una aplicación centralizada responsable de gestionar la identidad de los usuarios. Esto significa que, con una única Cuenta Panda, el administrador de red tendrá acceso simple y seguro a todos los productos de Panda que haya contratado.

Consulta el [diagrama de flujo del proceso de acceso a la consola](#) para ayudarte a resolver los escenarios más comunes.

Conceptos clave & Preguntas más frecuentes

¿Para qué sirve el correo de bienvenida?

Básicamente, para crear la Cuenta Panda, no para activarla. Puedes reenviar el correo de bienvenida desde Salesforce.

¿Qué es el usuario 'cool'?

El usuario 'cool' es la primera combinación dirección de email/contraseña una vez activada. Se muestra como el usuario predeterminado y no puede ser modificado ni eliminado.

¿Puedo utilizar la misma dirección de email para crear distintas Cuentas Panda?

No, una vez se utiliza una dirección de correo para crear una Cuenta Panda, NO es posible volver a utilizarla para crear una cuenta distinta.

Entonces, básicamente, para acceder a la consola se necesita una combinación activada dirección de email/contraseña, ¿no?

Así es. En caso de que se cree una cuenta pero no se active, no será posible acceder a la consola.

¿Cómo puedo activar mi Cuenta Panda?

Puedes activar tu Cuenta Panda desde el correo de activación que se envía automáticamente tras crear la cuenta.

En caso de que hayas perdido o borrado dicho correo, puedes hacer que vuelva a ser enviado mediante el Recordatorio de Claves: <https://accounts.pandasecurity.com/Web/Account/ResetPassword>

¿Está vinculada la Cuenta Panda a los mantenimientos del cliente?

Sí.

¿Qué sucede si creo un usuario desde la consola de AD360 y su dirección de correo no está activada?

La única forma en la que el usuario podrá iniciar sesión y acceder a los servicios de su mantenimiento será activando su usuario desde su dirección de correo.

Consulta la siguiente FAQ interna para más información:

- [¿Cómo poner en marcha Adaptive Defense y Endpoint Protection?](#)
- [Preguntas Frecuentes sobre la Cuenta Panda en los productos Panda Cloud](#)

Errores de la consola Web

Error al cargar el sitio Web

1- Error 404 o similar:

- Comprueba si puedes iniciar sesión desde tu propia máquina / entorno / consola
 - Si no puedes iniciar sesión, escala el caso describiendo las pruebas que has realizado.
 - Si sólo sucede en el entorno del cliente:
 - Intenta cargar otros sitios Web.
 - Prueba con otros navegadores Web. Si el problema continúa, escala el caso.

2- Error con las credenciales del cliente

- Comprueba las credenciales en tu máquina
 - Si consigues iniciar sesión:
 - Comprueba las credenciales con el cliente (número o carácter incorrecto).
 - Envía un correo con las credenciales correctas.
 - Limpia la caché del navegador de Internet.
 - Borra los archivos temporales de Internet.
 - Si no consigues iniciar sesión:
 - Solicita la información de cliente (credenciales) y notifica el caso a Soporte.

Para el resto de casos, y antes de notificar el caso a Soporte, comprueba que hayas incluido la información siguiente:

- ✓ Descripción del problema. Captura de pantalla del error/información visual.
- ✓ Pasos para reproducir la situación. Un vídeo sería lo más útil e ideal.
- ✓ Credenciales de la consola Web.

Errores del agente

- 1- Error relacionado con el proceso **WaHost.exe** (se muestra una ventana con el mensaje en el Escritorio).
 - Actualiza la consola del cliente a la última versión.
- 2- Código de error 3369 en el visor de eventos de Windows.
 - Es un aviso. La máquina no ha establecido comunicación con otros agentes de Endpoint Protection. Comprueba los puertos necesarios (consulta el [anexo](#) para más información): TCP 18226 y UDP 21226.
- 3- La configuración local es distinta a la del perfil de la consola Web.
 - Haz una sincronización <http://screencast.com/t/j5j5yUjxu9Z>
 - Desinstala el **Agente de Endpoint Protection (Panda Endpoint Agent)** desde **Panel de control – Agregar o quitar programas**.
 - Desinstala **Endpoint Protection** desde **Panel de control – Agregar o quitar programas**.
 - Descarga el paquete de instalación desde la consola Web e instálalo de nuevo.

Si el problema continúa, incluye por favor la **siguiente información al notificar el problema a**

Soporte:

- ✓ Descripción del problema,
- ✓ Activa los archivos de log al máximo nivel de registro. Consulta el [anexo](#) para ver cómo hacerlo.
- ✓ [PSInfo](#). Consulta el [anexo](#).

Error al instalar/desinstalar la protección

1- Error al instalar Endpoint Protection

- Comprueba los requisitos:
 - [Windows](#)
 - [Linux](#)
 - [OS X](#)
- Comprueba los códigos de error:
 - 2081, 2132 y 2133:
 - Consulta este [artículo](#) para saber cómo resolver el error 2081. La herramienta para resolver el error 2081 estará disponible próximamente en la sección Herramientas de [PSInfo](#).
 - En cuanto a los errores 2132 y 2133, comprueba si la siguiente opción está activada:
<http://screencast.com/t/JLhRUfj8dqNI>
 - Código de error 2093: Utiliza la siguiente [herramienta](#) incluida en [PSInfo](#).

2- Error al desinstalar Endpoint Protection

Ejecuta la [herramienta incluida](#) en [PSInfo](#) para lanzar el desinstalador genérico.

Si el problema continúa, incluye por favor la siguiente información al notificar el problema a Soporte:

- ✓ Descripción del problema.
- ✓ [PSInfo](#). Consulta el [anexo](#).

Error al instalar/desinstalar el agente

1- Error al instalar el agente de Endpoint Protection

- Comprueba los requisitos mínimos:
 - [Windows](#)
 - [Linux](#)
 - [OS X](#)
- Comprueba el código de error:
 - Código de error 1289
 - Comprueba que hay licencias libres en la consola Web.
 - Comprueba la existencia de equipos excluidos: Elimina los equipos excluidos para aumentar las licencias.
 - Código de error 5000:
Comprueba las URLs requeridas por EPP mediante la herramienta [URL Checker](#) incluida en [PSInfo](#). Haz clic [aquí](#) para ver las URLs requeridas por el servicio.
 - Código de error 3365:
Este error indica que estamos subiendo un nuevo catálogo. Es necesario esperar a que la nube sincronice el nuevo catálogo, por lo que recomendamos esperar 20 minutos.
- Error al extraer los archivos:
Comprueba los permisos de la carpeta **%temp%**. En caso de que no estén asignados, asigna permisos de escritura sobre la carpeta.
- El asistente de instalación finaliza sin error:
Ejecuta [Panda Cloud Cleaner](#) ya que, en algunos casos, esto puede indicar una posible infección.

2- Error al desinstalar el Agente de Endpoint Protection:

- Ejecuta el desinstalador genérico
 1. [Descarga](#)
 2. Ejecuta DG_WAGENT_7_XX.exe
 3. Reinicia

Si el problema continúa, incluye por favor la siguiente información al notificar la consulta a Soporte:

- ✓ Descripción del problema.
- ✓ [PSInfo](#). Consulta el [anexo](#).

Producto no actualizado (updates o upgrades)

- 1- Los archivos de firmas no están actualizados
 - Comprueba si el problema afecta a una o varias máquinas:
 - Comprueba que el cliente tenga suficientes licencias.
 - Comprueba la red del cliente (proxy, firewall, etc.).
 - Comprueba nuestras [URLs](#) y si el problema continua, abre [PSInfo](#) y utiliza la herramienta interna para las URLs:
<http://screencast.com/t/rfA4ibQQ>
<http://screencast.com/t/UU2umO7czyd>
<http://screencast.com/t/Qw4lXgl1w>
 - Comprueba en la consola Web si la conexión a Internet está correctamente configurada.
 - Si la máquina carece de conexión a Internet, utiliza la herramienta URLChecker en la máquina WaProxy/máquina que centraliza las comunicaciones con el servidor.
<http://screencast.com/t/Wl6KMX6avh3M>
 - Comprueba que nuestros puertos de comunicación interna están permitidos (Consulta el [anexo](#) para más información):
 - Puerto TCP 18226
 - Puerto UDP 21226
 - Fuerza una sincronización (<http://screencast.com/t/j5j5yUjxu97>)
 - Utiliza la herramienta [PSInfo](#) añadiendo el [parámetro update](#).
 - La consola Web muestra un escudo rojo con la fecha 1/1/1900
 - Desinstala el Agente de Endpoint Protection.
 - Desinstala Endpoint Protection.
 - Descarga el paquete de instalación desde la consola Web e instálalo de nuevo.
- 2- El producto no está actualizado
 - Utiliza la herramienta [PSInfo](#) añadiendo el [siguiente parámetro](#) en el apartado de descripción.
 - Comprueba que las actualizaciones están activadas en la consola Web
<http://screencast.com/t/GUJnhB1g>
 - Comprueba la red del cliente.
 - Proxy
 - Firewall
 - Utiliza URLChecker
 - Si la máquina no tiene acceso a Internet, no es posible actualizar la protección.
 - Comprueba que nuestros puertos de comunicación interna están permitidos (Ver [anexo](#) para más información):
 - Puerto TCP 18226
 - Puerto UDP 21226

Si el problema continúa, incluye por favor la **siguiente información al notificar la consulta a**

Soporte:

- ✓ Describe el problema.
- ✓ Activa los archivos de log al máximo nivel de registro. Consulta el [anexo](#) para ver cómo hacerlo.
- ✓ [PSInfo](#). Consulta el [anexo](#).
- ✓ Describe la red del cliente (proxy, firewall...)

BSOD

- 1- Identifica el problema. ¿Se muestra el nombre del driver?
- 2- ¿Está instalada la última versión del producto en el equipo?
- 3- Desinstala el producto y comprueba si se resuelve el problema.
- 4- Instala la última versión del producto.
- 5- Comprueba qué estaba haciendo el usuario antes de comprobar el archivo DMP.
- 6- Comprueba que la tarjeta de vídeo tiene los últimos drivers instalados.
- 7- Comprueba que los chipsets de la placa madre están actualizados.

Si el problema continúa, incluye por favor la siguiente información:

- ✓ Descripción del problema.
- ✓ [PSInfo](#). Consulta el [anexo](#).
- ✓ Archivo DMP completo. Consulta el anexo para saber cómo obtener un archivo completo de volcado de memoria.

Problemas con la protección avanzada (sólo para Adaptive Defense 360)

El paso siguiente sólo se aplica a las siguientes situaciones:

- Consumo excesivo de recursos o ralentización de las máquinas.
- Error en la protección avanzada.
- Incompatibilidad con software de terceros o el binario está siendo bloqueado.

Abre la [herramienta de configuración local de la protección avanzada](#) para activar o desactivar esta funcionalidad.

- El problema desaparece tras desactivar la funcionalidad.
 - Vuelve a activar la opción con la herramienta y reproduce la situación recogiendo trazas con PSErrortrace.
 - Toma un [PSInfo](#).
 - Adjunta, en caso de que sea posible, una copia del software con los pasos necesarios para reproducir la consulta.
- El problema no desaparece tras desactivar la funcionalidad.
 - Toma un [PSInfo](#) activando los logs del agente y forzando una sincronización.
 - Adjunta, en caso de que sea posible, una copia del software con los pasos necesarios para reproducir la consulta.

En el caso de elementos de terceros que estén siendo bloqueados por la protección avanzada, abre la consola Web y comprueba si dichos elementos aparecen en el panel [Elementos actualmente bloqueados en clasificación](#). Si el elemento bloqueado es necesario para las actividades diarias de la empresa, selecciona el botón [No volver a bloquear](#) para definir una exclusión hasta que el elemento sea clasificado.

Errores en la protección permanente del antivirus o errores al analizar

- 1- Error en el icono del antivirus en la bandeja del sistema
 - En caso de que exista un software de seguridad de terceros, desinstálalo.
 - En caso de que haya otros productos de Panda instalados, ejecuta el desinstalador [genérico](#) de Panda.
 - Instalación o actualización incorrecta
 - Desinstala el Agente de Endpoint Protection.
 - Desinstala Endpoint Protection.
 - Descarga el paquete de instalación desde la consola Web e instálalo de nuevo.
 - Descarta una posible infección de malware ejecutando [Panda Cloud Cleaner](#).
 - Asegúrate de que el sistema operativo está actualizado. Considera la posibilidad de realizar una actualización de Windows (Windows Update).

- 2- Icono de error de la protección en la consola Web
 - Solicita al cliente que fuerce una comunicación entre el agente y la consola Web, siguiendo estos pasos:
 - Utiliza la herramienta [PSInfo](#) añadiendo el [siguiente parámetro](#) en el apartado de descripción.
 - Haz clic con el botón derecho sobre el icono de la bandeja del sistema, y haz una sincronización <http://screencast.com/t/j5j5yUjxu9Z>
 - Desinstala el agente de Endpoint Protection y vuelve a instalarlo.

- 3- Error al analizar
 - Comprueba si se muestra un código de error y haz una captura de pantalla del error.
 - Comprueba si el problema es aleatorio o no.
 - Comprueba si siempre falla en el mismo archivo o carpeta. Si se trata de un archivo temporal, elimínalo.
 - Comprueba si sucede con la última versión del producto.
 - Si se trata de un problema aleatorio:
 - Inicia el **Desfragmentador de disco**.
 - Ejecuta un **chkdsk**.
 - Ejecuta un **scandisk**.
 - Comprueba que la máquina está actualizada (**Windows Update**).

Notifica el caso con la siguiente información:

- ✓ Descripción del problema
- ✓ [PSInfo](#)
- ✓ PSErrortrace. Consulta el [anexo](#).

Errores de firewall, pérdida de la conexión a Internet o pérdida del acceso a recursos de red

- 1- Error en la protección firewall del endpoint
 - Error en la interfaz local (error o aspa roja al abrir la interfaz local).
 - Comprueba el firewall de Windows y desactívalo.
 - Comprueba cualquier otro software de firewall que pueda estar instalado y desactívalo
 - Comprueba Endpoint Protection e instala la última versión en caso necesario.
 - Error en la consola Web
 - Fuerza una sincronización.
 - Vuelve a comprobar la consola Web y en caso de que no haya cambiado la fecha de la última conexión <http://screencast.com/t/vDXO6kM5Ac>, reinstala el Agente de Endpoint Protection.

- 2- Pérdida de la conexión a Internet o del acceso a carpetas compartidas
 - Pérdida del acceso a red.
 - Comprueba que está instalada la última versión de Endpoint Protection.
 - Desactiva **Network Activity Hook Server Driver**. <http://screencast.com/t/HldoPlu3Ba>
Si el problema se soluciona, está relacionado con nuestra tecnología firewall de Endpoint Protection. En tal caso, notifica el caso a Soporte con la información requerida.
 - Pulsa la tecla de Windows + R y teclea **cmd**.
 - Ejecuta este comando: **netsh winsock reset**

- 3- Pérdida de conexión con software de terceros
 - Comprueba el modo de administración de la protección firewall:
 - Si se administra desde la consola Web:
 - Añade una regla para dicho software.
 - Haz una sincronización en local para aplicar la nueva regla.
 - Si se administra desde el host local.
 - Comprueba la configuración del firewall. <http://screencast.com/t/EklBy4cSA>
 - Restaura las reglas <http://screencast.com/t/SJSVFX6wj>

Si el problema continúa, incluye por favor la siguiente información:

- ✓ Descripción del problema.
- ✓ [PSInfo](#). Consulta el [anexo](#).
- ✓ [NNSDiag](#). Consulta el [anexo](#).
- ✓ Describe la topología de red.

Consumo excesivo de recursos

- 1- Comprueba que el cliente tiene la última versión de Endpoint Protection instalada.
- 2- Asegúrate de que el problema está causado por nuestro producto.
 - **Inicio – Ejecutar** (tecla de Windows + R). Teclea **services.msc**
 - Detén nuestros servicios:
 - Panda Cloud Office Protection Service
 - Panda Endpoint Administration Agent
 - Panda Product Service
 - Si el problema persiste estando nuestros servicios detenidos, desinstala el producto para asegurarte de que el problema no está relacionado con nuestro producto.
- 3- El problema se resuelve tras detener el servicio Panda Cloud Office Protection Service. Sigue estos pasos:
 - Accede a la consola Web y selecciona el perfil utilizado en la máquina que tiene el problema.
 - Desactiva esta opción <http://screencast.com/t/vuDpCiWh>
 - Desactiva la opción de analizar archivos comprimidos <http://screencast.com/t/DM7BXEyXMc>
 - Añade exclusiones <http://screencast.com/t/lnYyqblI>
 - Extensión
 - Carpeta
 - Archivos
- 4- Utiliza la herramienta [PCOP_protectionerror](#) para averiguar qué tecnología está causando el problema:
 - Protección de archivos. Detén cada driver para averiguar cual de ellos está causando el problema.
 - Firewall. Detén cada driver para averiguar cual de ellos está causando el problema.
- 5- El problema sólo sucede en una máquina.
 - Desinstala el Agente de Endpoint Protection.
 - Desinstala Endpoint Protection.
 - Descarga el paquete de instalación desde la consola Web e instálalo de nuevo.
- 6- Desactiva las opciones de configuración. Consulta el [anexo](#) para obtener más información sobre este paso.

Si el problema continúa, **incluye por favor la siguiente información:**

- ✓ Descripción del problema.
- ✓ [PSInfo](#). Consulta el [anexo](#).
- ✓ Ejecuta PErrortrace si el problema está relacionado con Panda Cloud Office Protection Service. Consulta el [anexo](#).
- ✓ Ejecuta [NNSDiag](#) si el problema está relacionado con nuestra tecnología Firewall. Consulta el [anexo](#).

Software de terceros

Si el problema está causado por software de terceros bloqueado por la protección avanzada de Adaptive Defense 360, consulta la sección que explica [cómo administrar los elementos bloqueados](#).

- 1- Error al ejecutar software desde una carpeta compartida.
 - a. En estaciones de trabajo.
 - i. Consulta el anexo y utiliza la herramienta Advanced Protection Local Configurator.
 - ii. Desactiva el módulo de Adaptive Defense. En caso de que esto resuelva el problema, escala el caso. En caso contrario, continúa con el paso siguiente.
 - iii. Desactiva el hook del firewall de Panda (<http://screencast.com/t/HldoPlu3Ba>).
En caso de que esto resuelva el problema, escala el caso.
 - b. En el lado del servidor del otro fabricante:
 - i. Consulta el anexo y utiliza la herramienta Advanced Protection Local Configurator.
 - ii. Desactiva el módulo de Adaptive Defense. En caso de que esto resuelva el problema, notifica el caso a Soporte. En caso contrario, continúa con el paso siguiente.
 - iii. Desactiva el hook del firewall de Panda.

Para analizar este tipo de problemas necesitamos los siguientes datos:

- ✓ Software de terceros.
- ✓ Pasos necesarios para reproducir la consulta.
- ✓ Captura de pantalla del error.
- ✓ [PSInfo](#).
- ✓ [PSErrortrace](#), si el problema está relacionado con el servicio Panda Cloud Office Protection Service.
- ✓ [NNSDiag](#) si el problema está relacionado con nuestra tecnología Firewall.

Malware

A continuación explicamos cómo tratar los problemas de malware en:

- Adaptive Defense/Adaptive Defense 360
- Endpoint Protection/Endpoint Protection Plus

Los procedimientos que explicamos a continuación indican qué verificar, qué datos recoger y cómo notificar los problemas de malware a Soporte.

Cómo tratar los problemas de malware con Adaptive Defense/Adaptive Defense 360

Cuando Adaptive Defense o Adaptive Defense 360 notifican un problema de malware, lo más probable es que nos encontremos con uno de los siguientes escenarios:

- Escenario 1: Equipo infectado
- Escenario 2: Detección o bloqueo incorrecto

Comprueba cada uno de ellos para saber qué pasos seguir:

Escenario 1 - Equipo infectado

Recogida de información

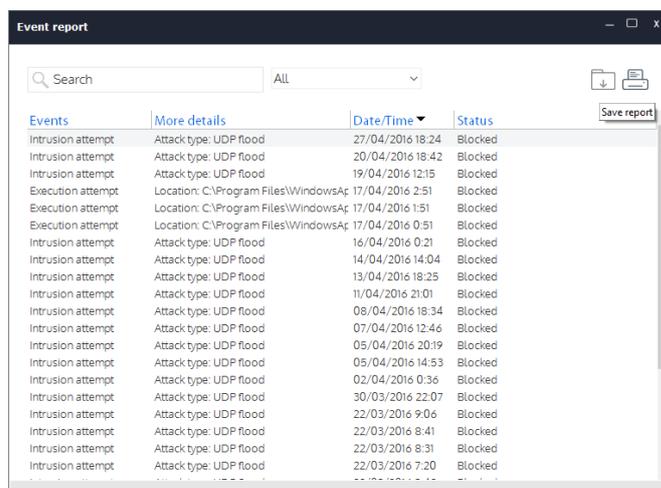
Para notificar infecciones de malware en el endpoint a Soporte, recoge la siguiente información del cliente:

- Número y nombre de la Cuenta de Cliente
- Nombre del equipo
- Fecha estimada de la infección
- Origen de la infección:
 - Spam con un adjunto malicioso. En tal caso, adjunta el correo sospechoso.
 - Acceso a un sitio Web.
 - Origen desconocido: El cliente sólo sabe que los archivos están infectados.
- [PSInfo](#)

Escenario 2 – Detección incorrecta

Recogida de información

- Número y nombre de la Cuenta de Cliente
- Nombre del equipo
- Exportación del informe del antivirus del equipo



Events	More details	Date/Time	Status
Intrusion attempt	Attack type: UDP flood	27/04/2016 18:24	Blocked
Intrusion attempt	Attack type: UDP flood	20/04/2016 18:42	Blocked
Intrusion attempt	Attack type: UDP flood	19/04/2016 12:15	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 2:51	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 1:51	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 0:51	Blocked
Intrusion attempt	Attack type: UDP flood	16/04/2016 0:21	Blocked
Intrusion attempt	Attack type: UDP flood	14/04/2016 14:04	Blocked
Intrusion attempt	Attack type: UDP flood	13/04/2016 18:25	Blocked
Intrusion attempt	Attack type: UDP flood	11/04/2016 21:01	Blocked
Intrusion attempt	Attack type: UDP flood	08/04/2016 18:34	Blocked
Intrusion attempt	Attack type: UDP flood	07/04/2016 12:46	Blocked
Intrusion attempt	Attack type: UDP flood	05/04/2016 20:19	Blocked
Intrusion attempt	Attack type: UDP flood	05/04/2016 14:53	Blocked
Intrusion attempt	Attack type: UDP flood	02/04/2016 0:36	Blocked
Intrusion attempt	Attack type: UDP flood	30/03/2016 22:07	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 9:06	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 8:41	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 8:31	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 7:20	Blocked

- [PSInfo](#)

Cómo tratar problemas de detección de malware con Endpoint Protection/Endpoint Protection Plus

Escenario 1: Equipo infectado

Para tratar los casos más habituales de infección, consulta la guía [Cómo tratar los problemas de malware según su tipo](#).

Si la infección persiste, sigue los siguientes pasos como regla general:

- Ejecuta [Panda Cloud Cleaner](#)

Si la infección persiste, recoge la siguiente información y notifica el caso a Soporte:

- Ficheros de log de Panda Cloud Cleaner. En la ruta de instalación de Panda Cloud Cleaner (por defecto **%Archivos de programa\PandaSecurity\PandaCloudCleaner**), localiza y crea una copia del archivo **Nombre_Aleatorio.pad**.
NOTA: Ten en cuenta que en los sistemas operativos de 64 bits, la carpeta es **%Archivos de programa(x86)\PandaSecurity\PandaCloudCleaner**
- Número y nombre de la Cuenta de Cliente
- Nombre del equipo
- Exportación del informe del antivirus del equipo

Events	More details	Date/Time	Status
Intrusion attempt	Attack type: UDP flood	27/04/2016 18:24	Blocked
Intrusion attempt	Attack type: UDP flood	20/04/2016 18:42	Blocked
Intrusion attempt	Attack type: UDP flood	19/04/2016 12:15	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 2:51	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 1:51	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 0:51	Blocked
Intrusion attempt	Attack type: UDP flood	16/04/2016 0:21	Blocked
Intrusion attempt	Attack type: UDP flood	14/04/2016 14:04	Blocked
Intrusion attempt	Attack type: UDP flood	13/04/2016 18:25	Blocked
Intrusion attempt	Attack type: UDP flood	11/04/2016 21:01	Blocked
Intrusion attempt	Attack type: UDP flood	08/04/2016 18:34	Blocked
Intrusion attempt	Attack type: UDP flood	07/04/2016 12:46	Blocked
Intrusion attempt	Attack type: UDP flood	05/04/2016 20:19	Blocked
Intrusion attempt	Attack type: UDP flood	05/04/2016 14:53	Blocked
Intrusion attempt	Attack type: UDP flood	02/04/2016 0:36	Blocked
Intrusion attempt	Attack type: UDP flood	30/03/2016 22:07	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 9:06	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 8:41	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 8:31	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 7:20	Blocked

- [PSInfo](#).

Escenario 2 – Detección incorrecta

Recogida de información

- Número y nombre de la Cuenta de Cliente
- Nombre del equipo
- Exportación del informe del antivirus del equipo

Events	More details	Date/Time	Status
Intrusion attempt	Attack type: UDP flood	27/04/2016 18:24	Blocked
Intrusion attempt	Attack type: UDP flood	20/04/2016 18:42	Blocked
Intrusion attempt	Attack type: UDP flood	19/04/2016 12:15	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 2:51	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 1:51	Blocked
Execution attempt	Location: C:\Program Files\WindowsAp	17/04/2016 0:51	Blocked
Intrusion attempt	Attack type: UDP flood	16/04/2016 0:21	Blocked
Intrusion attempt	Attack type: UDP flood	14/04/2016 14:04	Blocked
Intrusion attempt	Attack type: UDP flood	13/04/2016 18:25	Blocked
Intrusion attempt	Attack type: UDP flood	11/04/2016 21:01	Blocked
Intrusion attempt	Attack type: UDP flood	08/04/2016 18:34	Blocked
Intrusion attempt	Attack type: UDP flood	07/04/2016 12:46	Blocked
Intrusion attempt	Attack type: UDP flood	05/04/2016 20:19	Blocked
Intrusion attempt	Attack type: UDP flood	05/04/2016 14:53	Blocked
Intrusion attempt	Attack type: UDP flood	02/04/2016 0:36	Blocked
Intrusion attempt	Attack type: UDP flood	30/03/2016 22:07	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 9:06	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 8:41	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 8:31	Blocked
Intrusion attempt	Attack type: UDP flood	22/03/2016 7:20	Blocked

- Muestra del archivo detectado erróneamente como malware.
- [PSInfo](#).

7. Anexo

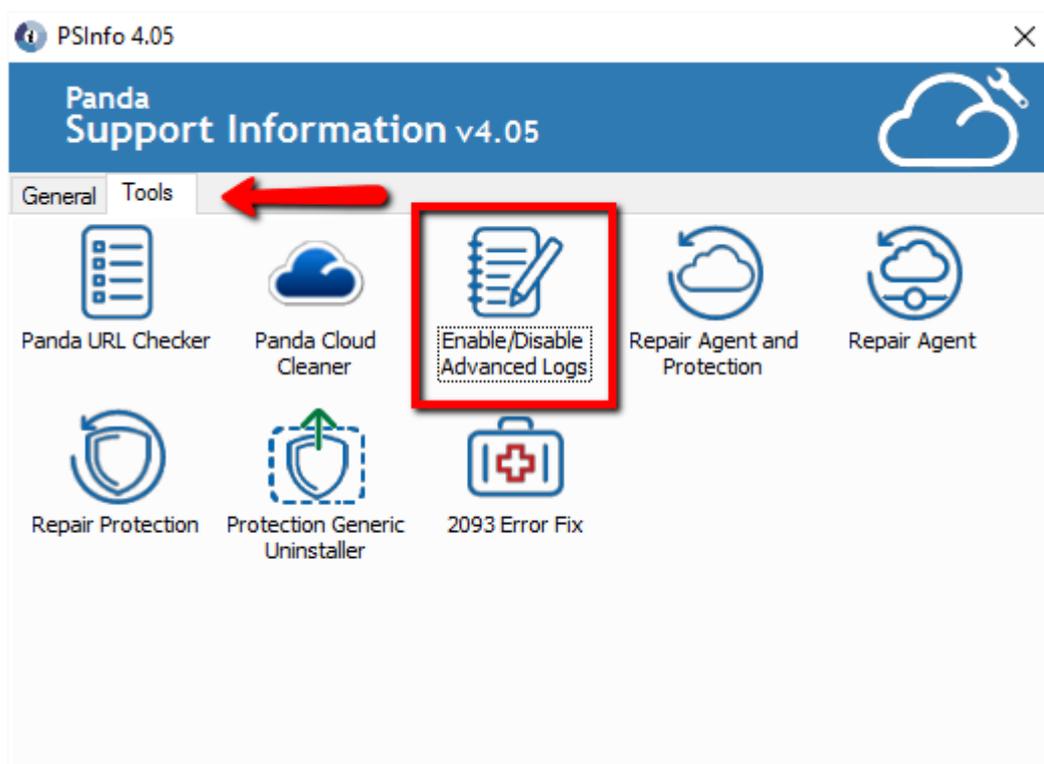
Este anexo incluye las herramientas y procedimientos a utilizar en los procesos de resolución de incidencias.

URLs

Consulta el artículo de Soporte [¿Cuáles son las URLs necesarias para el correcto funcionamiento del producto?](#)

Activación de los logs del agente

Cómo activar los archivos de log al máximo nivel de registro. Utiliza la opción **Enable/Disable Advanced Logs** de la herramienta [PSInfo](#).



PSInfo
[Enlace](#)

Comprobación de puertos

Nuestro producto utiliza el puerto TCP 18226 y el puerto UDP 21226. Dichos puertos se emplean para establecer comunicaciones con otros agentes de Endpoint Protection. Si necesitas comprobar si la comunicación es correcta, sigue los siguientes pasos:

- Tecla de Windows + R
- Teclea **cmd** y pulsa la tecla **Intro**
- **telnet nombremáquinadestino 18226**
- **telnet direcciónIPmáquinadestino 18226**

De esta forma podrás comprobar si el puerto está permitido o denegado.

PSErrorTrace

La herramienta PSErrorTrace recoge información útil para diagnosticar y estudiar problemas de Endpoint Protection relacionados con la instalación, el análisis o la compatibilidad con software de terceros.

Sigue las siguientes instrucciones:

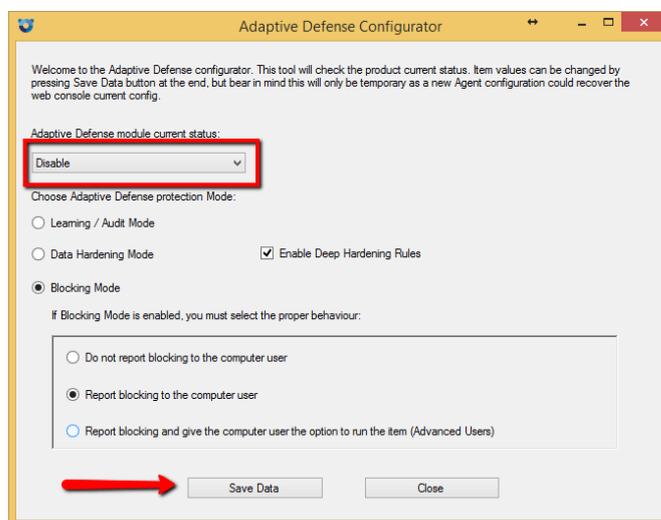
1. [Descarga](#) PsErrorTrace.exe y ejecuta el archivo con privilegios elevados.
2. Haz clic en el botón **Inicio**.
3. Selecciona el tipo de operación que se estaba realizando cuando se produjo el problema (instalación, activación, apertura de un programa, análisis, etc.) y haz clic en **Continuar**.
4. Introduce tu dirección de email y una descripción del problema y haz clic en **Continuar**.
5. A continuación se te pedirá que reproduzcas el problema que se ha producido (detención del análisis, fallo en la instalación, etc.). Cuando estés listo para hacerlo, haz clic en **Iniciar**.
6. Una vez hayas reproducido el problema y el botón no esté desactivado, haz clic en **Finalizar**.
7. Selecciona **Salir** y haz clic en **Sí** para guardar el informe **PsErrorTrace.PSInfo** en el equipo.
8. Por último, envía el archivo **PsErrorTrace.PSInfo** a Soporte.

Configurador local de la protección avanzada

La herramienta [panda_adaptivedefense360.exe](#) comprueba la configuración del producto y permite realizar cambios en la protección avanzada de forma local. Esto permite determinar si el problema está causado por la protección avanzada (Minerva) o acotar hasta llegar a averiguar con qué configuración se produce el problema.

La herramienta verifica si se ha instalado el producto correcto y comprueba que el servicio se esté ejecutando.

Elije la opción de desactivación y guarda los cambios.



NNSDiag

NNSDiag recoge información útil para el diagnóstico de problemas relacionados con las tecnologías firewall de Endpoint Protection.

Con el fin de acotar el problema y ofrecer una solución, es necesario obtener y estudiar ciertos datos. Sigue las siguientes instrucciones:

1. [Descarga y extrae el archivo nnsdiag.zip](#) y ejecuta **nnsdiag.exe**.
2. Sigue los pasos indicados en el asistente.
3. Es muy importante NO reiniciar el equipo durante estas pruebas.
4. Una vez ha finalizado el proceso, la herramienta guarda la información recogida. Envía a Soporte Técnico el archivo **NNSDiagResults.zip** resultante.

Desactivación de opciones de configuración

En la interfaz local, puedes activar un panel de administración local de forma temporal para ayudarte a encontrar dónde está un problema. Para activar dicho panel, sigue los siguientes pasos:

1. Accede a la consola Web y selecciona el perfil afectado por el problema.
2. Accede a la opción **Windows y Linux** y haz clic en la pestaña **Opciones avanzadas**.
<http://screencast.com/t/sicv22Z9Do7>
3. Accede a la opción **Contraseña de administración** y actívala.
<http://screencast.com/t/2qoAXdoEf>
4. A continuación, accede a la maquina local y haz una sincronización.
<http://screencast.com/t/INGyWghvvOa>
5. Accede a la interfaz local y haz clic en **Panel de Administrador**.
<http://screencast.com/t/SQNX4AVs4>
6. Introduce la contraseña establecida y haz clic en **Iniciar sesión**. Activa y desactiva los módulos para determinar cual de ellos está causando el problema.
<http://screencast.com/t/7FcZYIP8>
7. Al salir, selecciona durante cuánto tiempo quieres mantener los cambios.
<http://screencast.com/t/E929b3IX>

Cómo generar un archivo de volcado de memoria post-mortem (BSOD)

Sigue las instrucciones que aparecen a continuación para generar automáticamente un archivo de volcado de memoria post-mortem que recoja información sobre errores.

1. Descarga e instala las Herramientas de Depuración de Microsoft para Windows:
<http://msdn.microsoft.com/windows/hardware/hh852363>
2. Sigue los siguientes pasos para establecer **WinDBG** como depurador predeterminado:
 1. Abre un símbolo del sistema. Para ello, accede a **Inicio** -> **Ejecutar**, teclea **cmd** y haz clic en **Aceptar**.

- Accede al directorio de instalación **WinDBG**.

Para ello, teclea los comandos que aparecen a continuación y pulsa **Intro** después de cada comando:

```
cd\  
cd "Archivos de programa"  
cd Windows Kits  
cd 8.0  
cd Debuggers  
cd x86 (si dispones de un sistema operativo de 32-bits) o cd x64 (si dispones de un  
sistema operativo de 64-bits)  
Windbg -l
```

WinDbg -l

Nota: El carácter 'l' es la 'i' mayúscula.

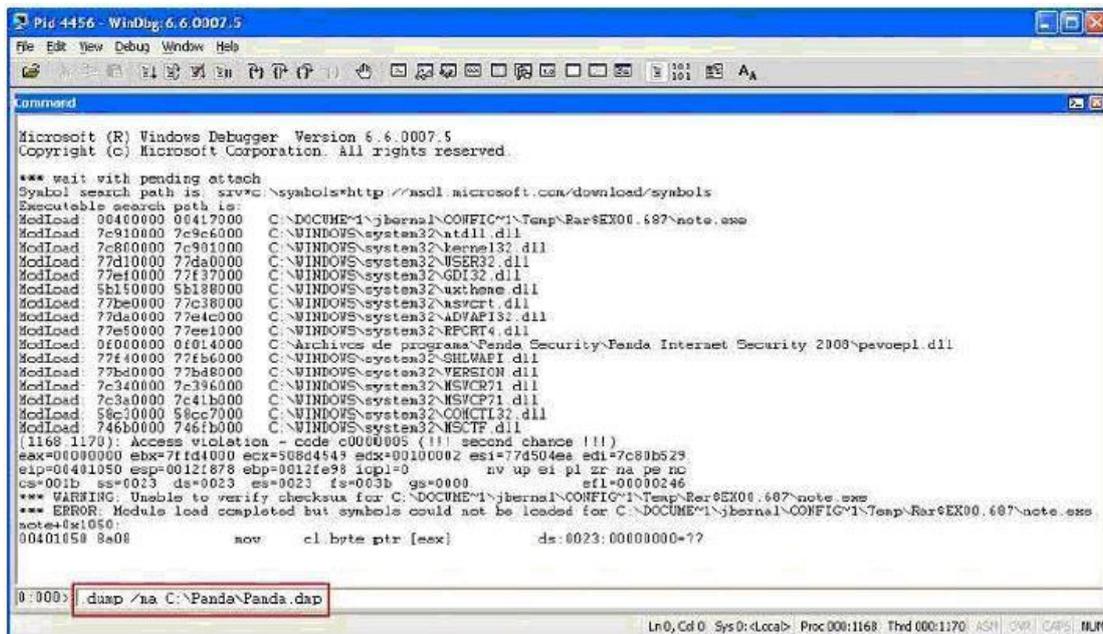
```

c:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>cd "Windows Kits"
C:\Documents and Settings\Windows Kits>cd 8.0
C:\Documents and Settings\Windows Kits\8.0>cd Debuggers
C:\Documents and Settings\Windows Kits\8.0\Debuggers>cd x86
C:\Documents and Settings\Windows Kits\8.0\Debuggers\x86>windbg -l
C:\Documents and Settings\Windows Kits\8.0\Debuggers\x86>_
  
```

- Crea una carpeta de nombre Panda en la unidad **C:** para almacenar el archivo de volcado (**C:\Panda**).

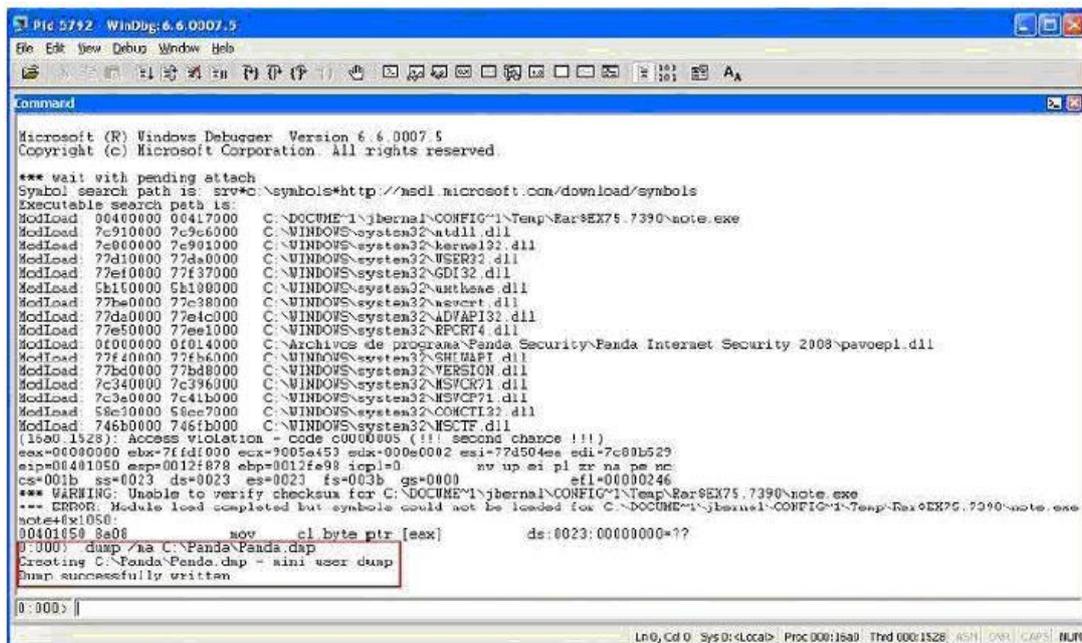
A partir de ese momento, cada vez que se muestre un mensaje de error, se mostrará la siguiente ventana de **WinDBG**:



4. Al final de la ventana, donde pone 0: 000>, introduce el siguiente comando:

.dump /na C:\Panda\Panda.dmp

Si el volcado se genera correctamente, se mostrará el mensaje **'Dump successfully written'** al final de la pantalla.



Una vez completados estos pasos, se generará automáticamente un archivo de

nombre **Panda.dmp** en el directorio C:\Panda.

5. Comprime el archivo **dmp** y envíanoslo para su análisis.

Lista de errores genéricos

La siguiente página muestra una lista de los errores más comunes que se pueden producir al trabajar con los productos Endpoint Protection y Adaptive Defense:

[Lista de los errores más comunes de Endpoint Protection](#)