Guía para maximizar los niveles de detección en las soluciones de ESET

Esta guía busca ayudar a los clientes de ZMA a maximizar sus niveles de detección de distintos tipos de malware y de esta manera, asegurar la protección de los equipos y su información ante nuevos códigos maliciosos u oleadas de distintos tipos de ataque como puede ser el Ransomware o cualquier otro malware.

Es importante destacar que dentro de una organización, aquellos equipos que no cuenten con una protección y se encuentren compartiendo recursos dentro de la red, pueden ser la puerta de entrada de infecciones para todos los equipos que conforman la red corporativa, ya sean estaciones de trabajo como servidores. Por ejemplo, un equipo desprotegido que se infectara con un Ransomware podría llegar a ocasionar el cifrado de todos los archivos del servidor en caso de que tuviera acceso. Por esto, es muy importante contar con la máxima protección en todos los dispositivos que conformen la red de la organización.

1. ¿Qué versión de producto tengo instalada?

Lo primero que hay que saber es con qué versión de las soluciones de ESET se cuenta instalada en los equipos. Para realizar esto, se debe acceder al Menú de Ayuda de los productos haciendo clic en “Acerca de”, o bien, se pueden seguir las instrucciones presentadas en este artículo de la Base de Conocimiento de ESET: http://soporte.eset-la.com/kb3040/

Además, dentro del Menú de Ayuda de los productos incluso se podrá buscar actualizaciones de forma directa desde los servidores de ESET.

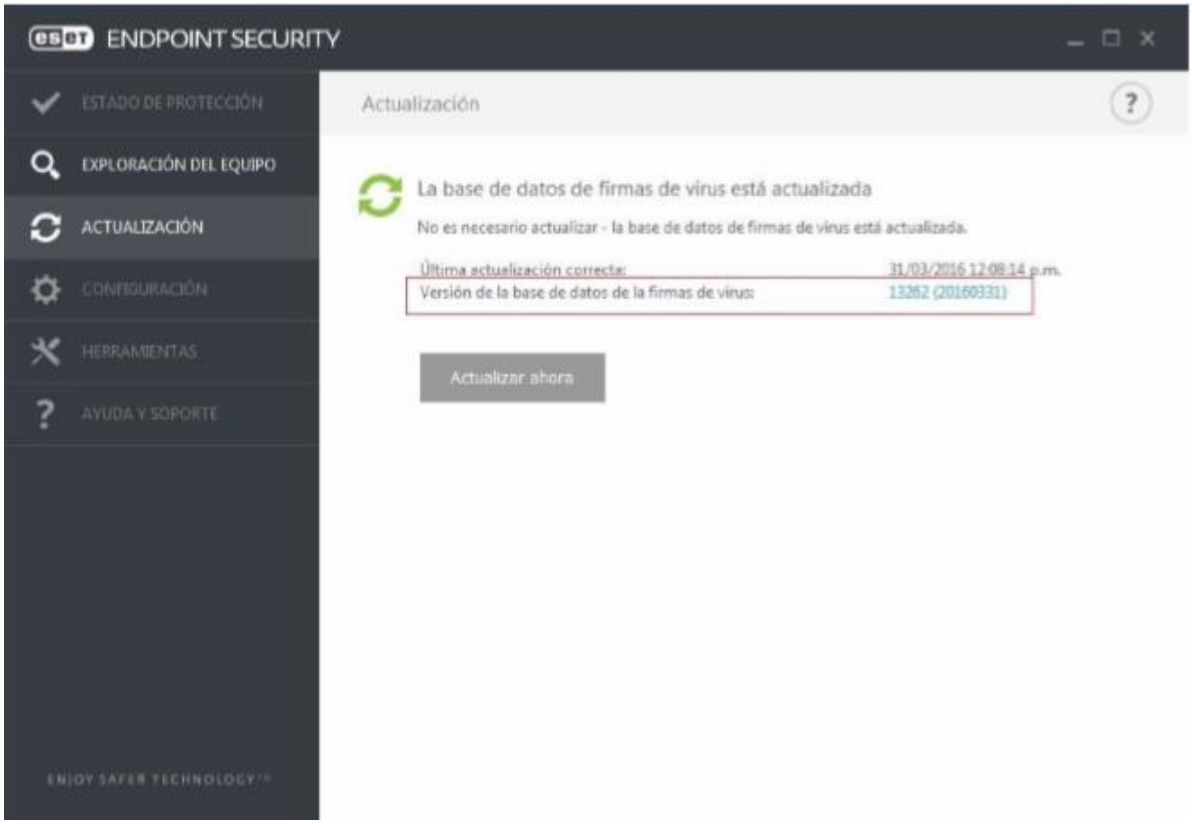
Es ideal que luego de esta prueba se pueda comprobar que se cuenta con la última versión disponible en el mercado (6.x).

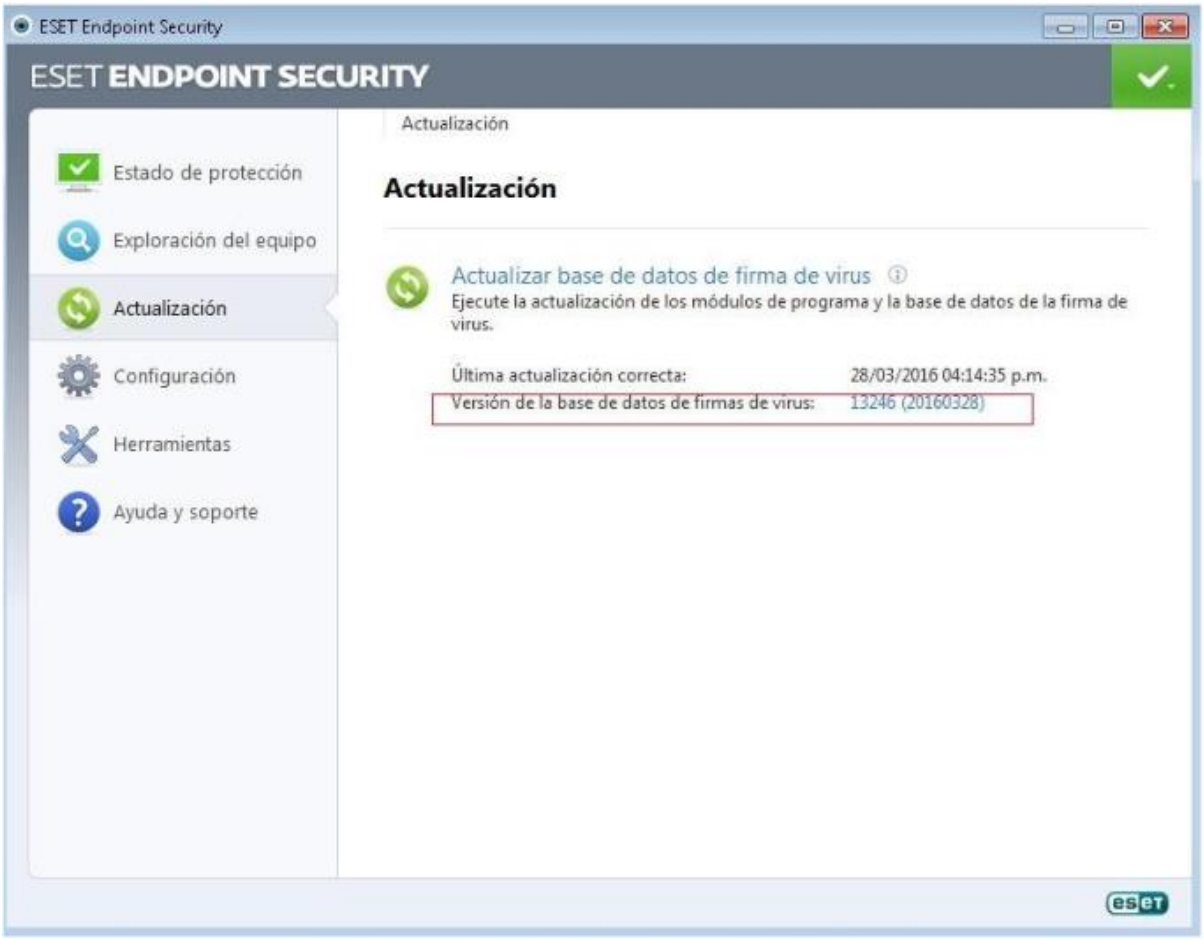
En caso que se cuente con una versión anterior, es ideal que en algún momento se planifique una actualización a la última versión de los productos. Si la versión instalada es la 4.x o incluso inferior, es ideal realizar la migración lo antes posible debido a que la última tecnología de detección de ESET (como ESET LiveGrid, Exploit Blocker, entre otras) solo se encuentran disponibles de la versión 5 en adelante.

2. ¿Qué debo verificar para maximizar la protección?

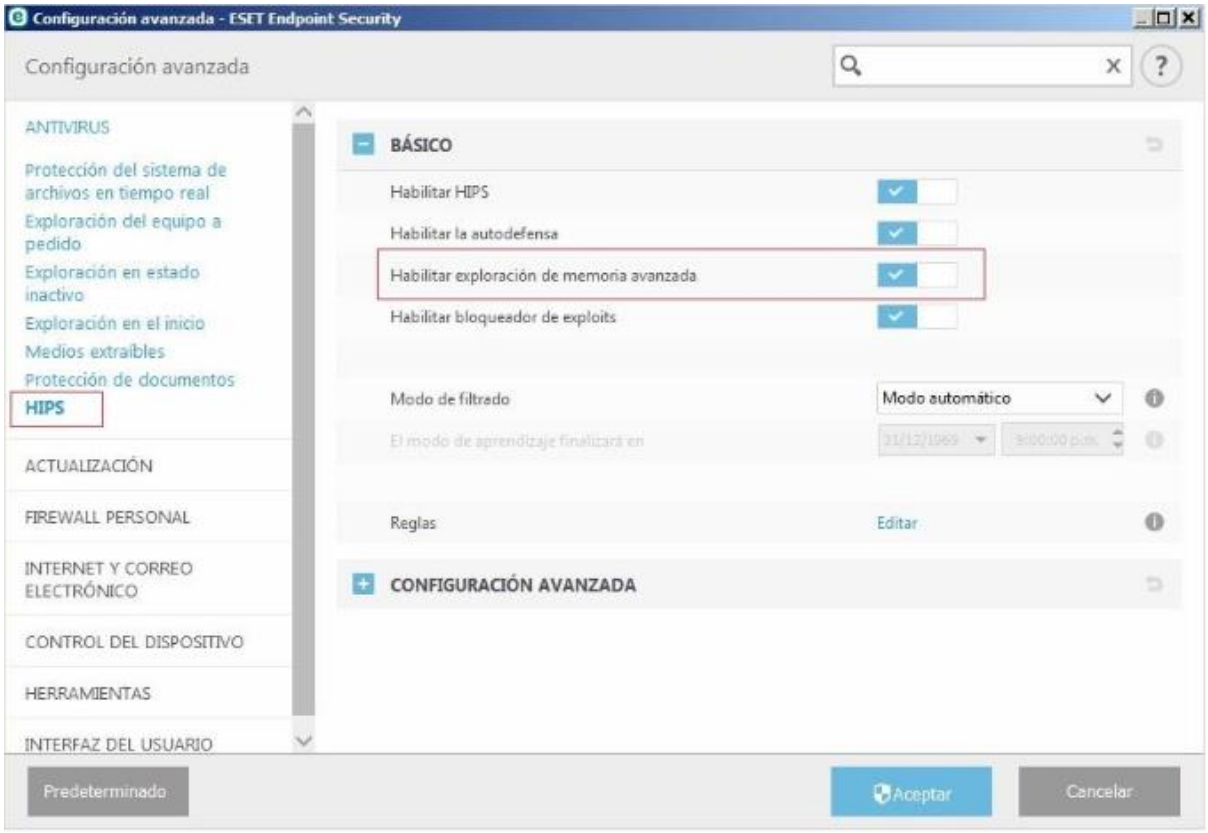
A continuación se listarán una serie de opciones o estados a revisar para asegurarse que se tiene la mejor configuración posible:

• Asegurarse que se encuentra la última base de firmas instalada y que se están realizando las actualizaciones correctamente

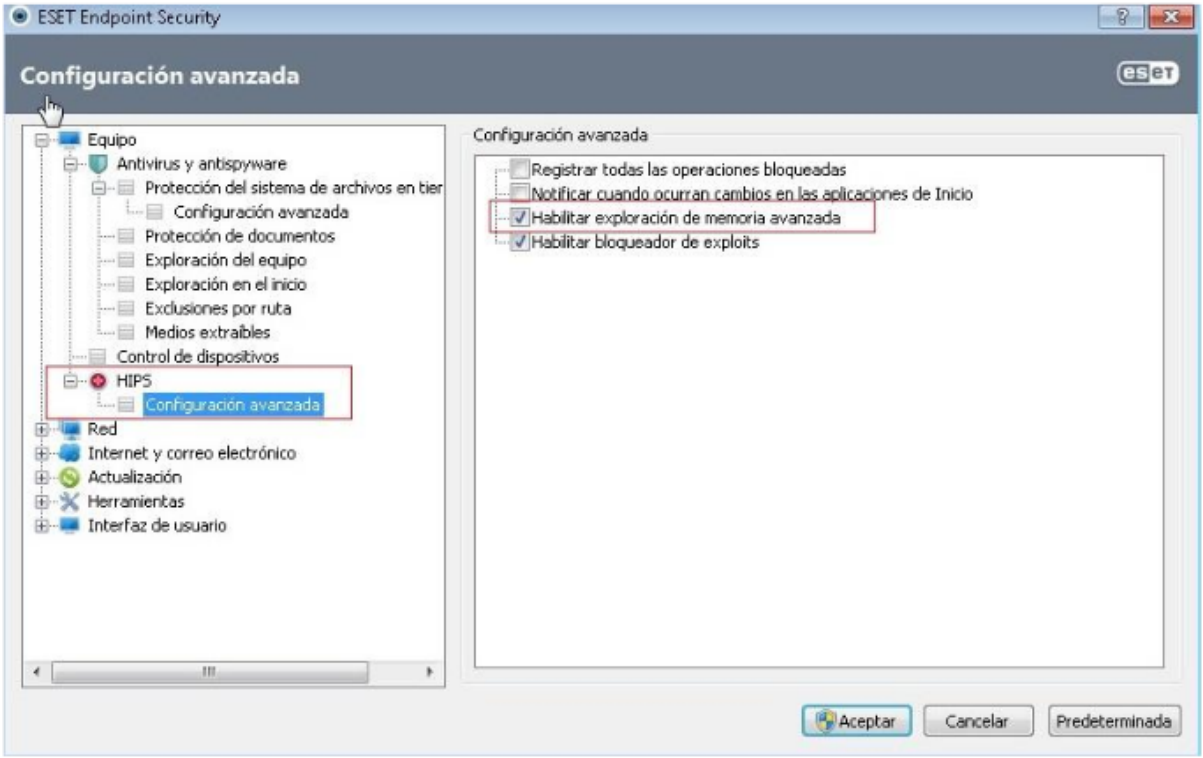




• Asegurarse que esté activo el módulo Advanced Memory Scanner dentro de la configuración del producto

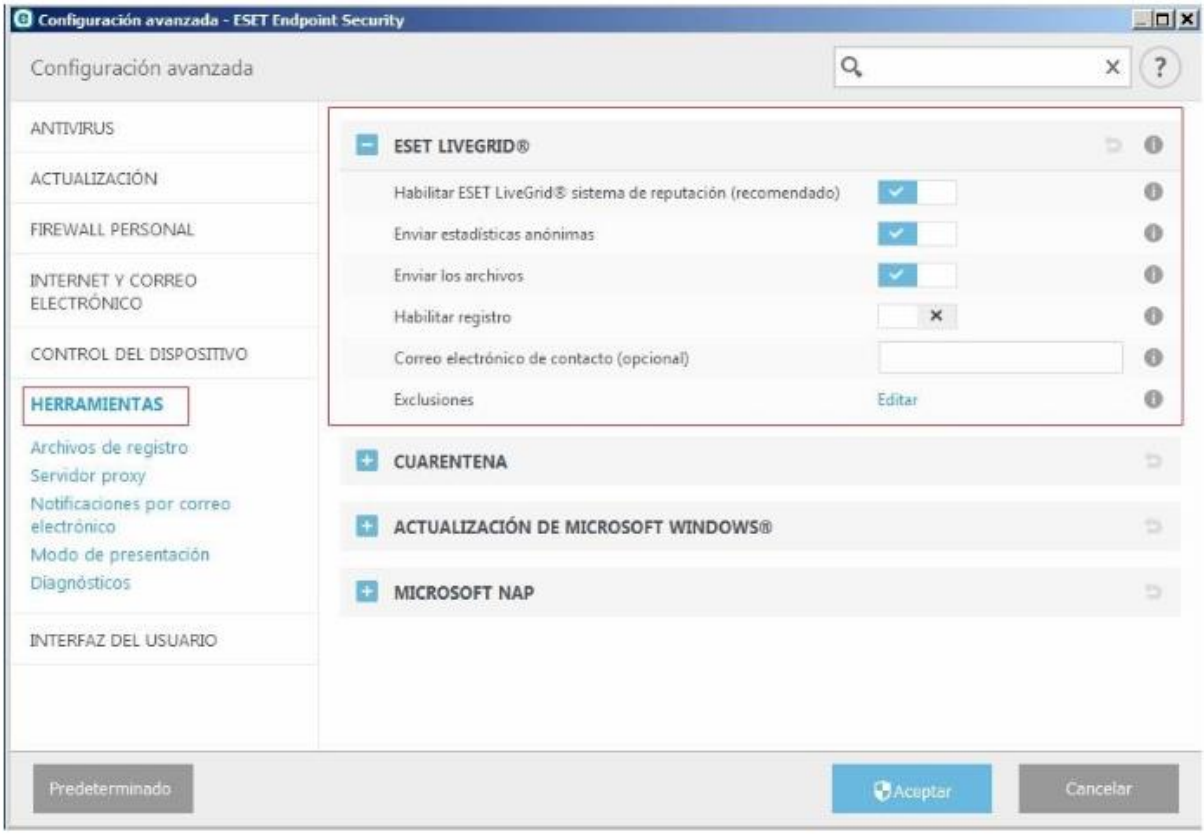


Habilitación de Advanced Memory Scanner en la versión 6

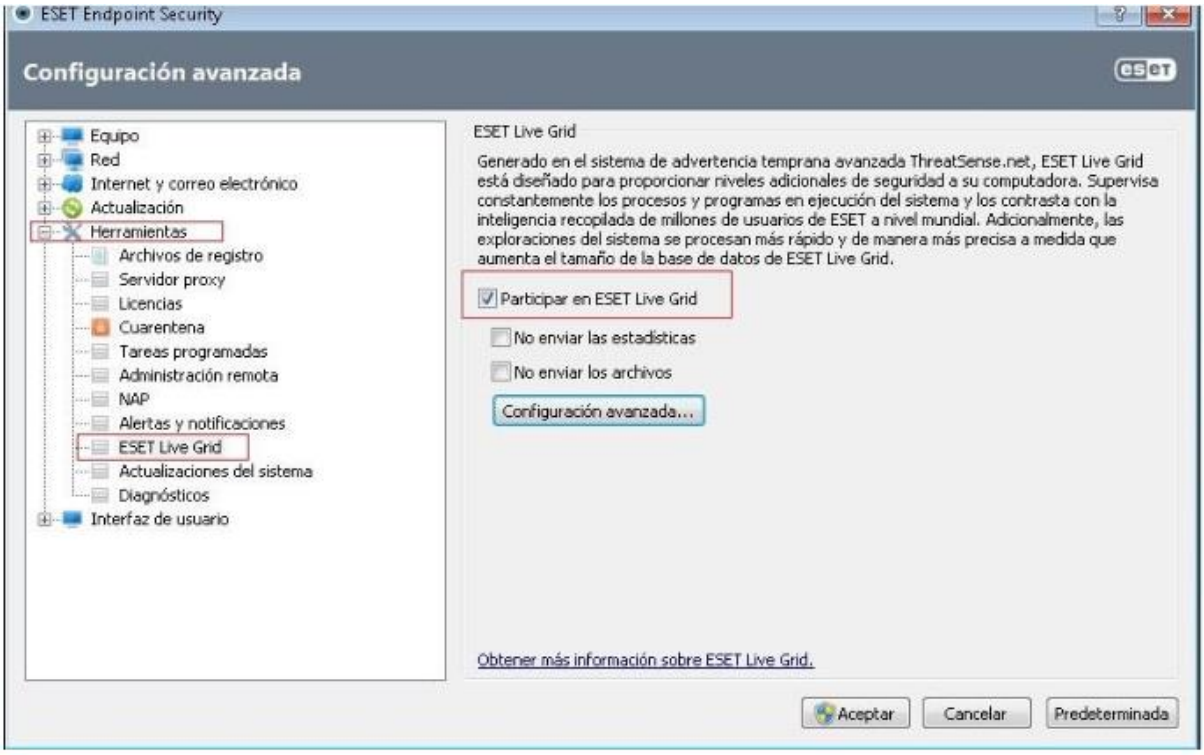


Habilitación de Advanced Memory Scanner en la versión 5

• Asegurarse que esté activo y funcional ESET LiveGrid, ya que las soluciones de ESET utilizan esta funcionalidad para realizar algunos análisis comparando de forma inmediata con la base de malware de ESET en la nube y, de esta manera, se mejora la protección ante el malware nuevo hasta que sea incluido en la próxima base de firmas de virus. Con ESET LiveGrid se puede reducir a minutos la protección ante códigos maliciosos desconocidos, mientras que con la base de firmas tradicional se tardaría algunas horas.

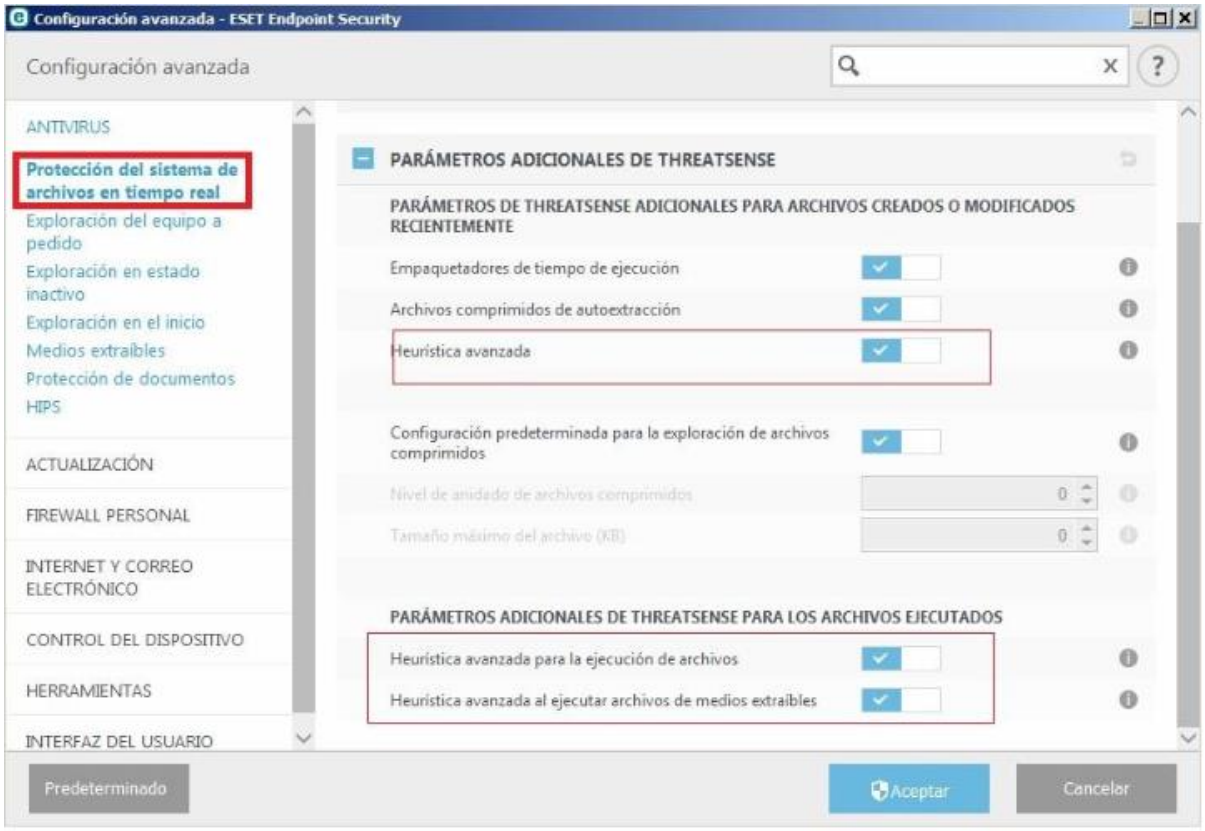


Habilitación de ESET LiveGrid en versión 6

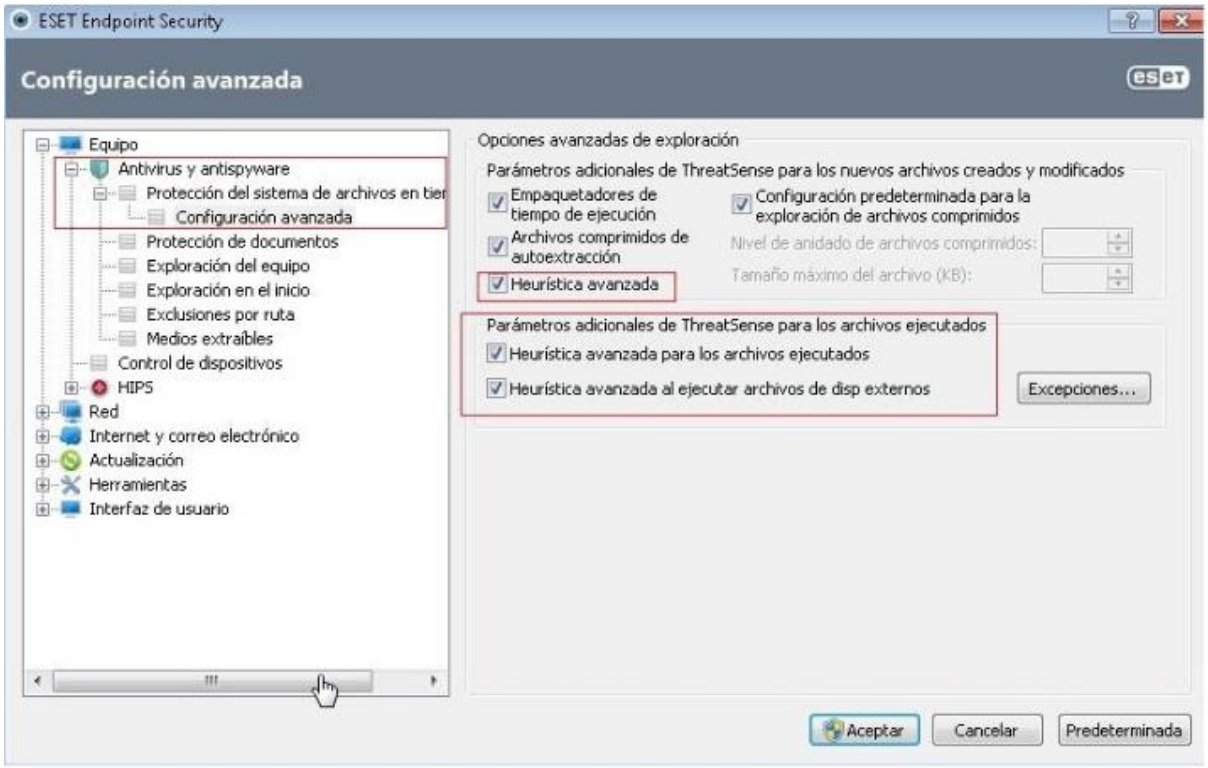


Habilitación de ESET LiveGrid en versión 5

• Una vez que ESET LiveGrid esté activo, también se recomienda asegurarse que la detección mediante Heurística Avanzada también se encuentre activa.



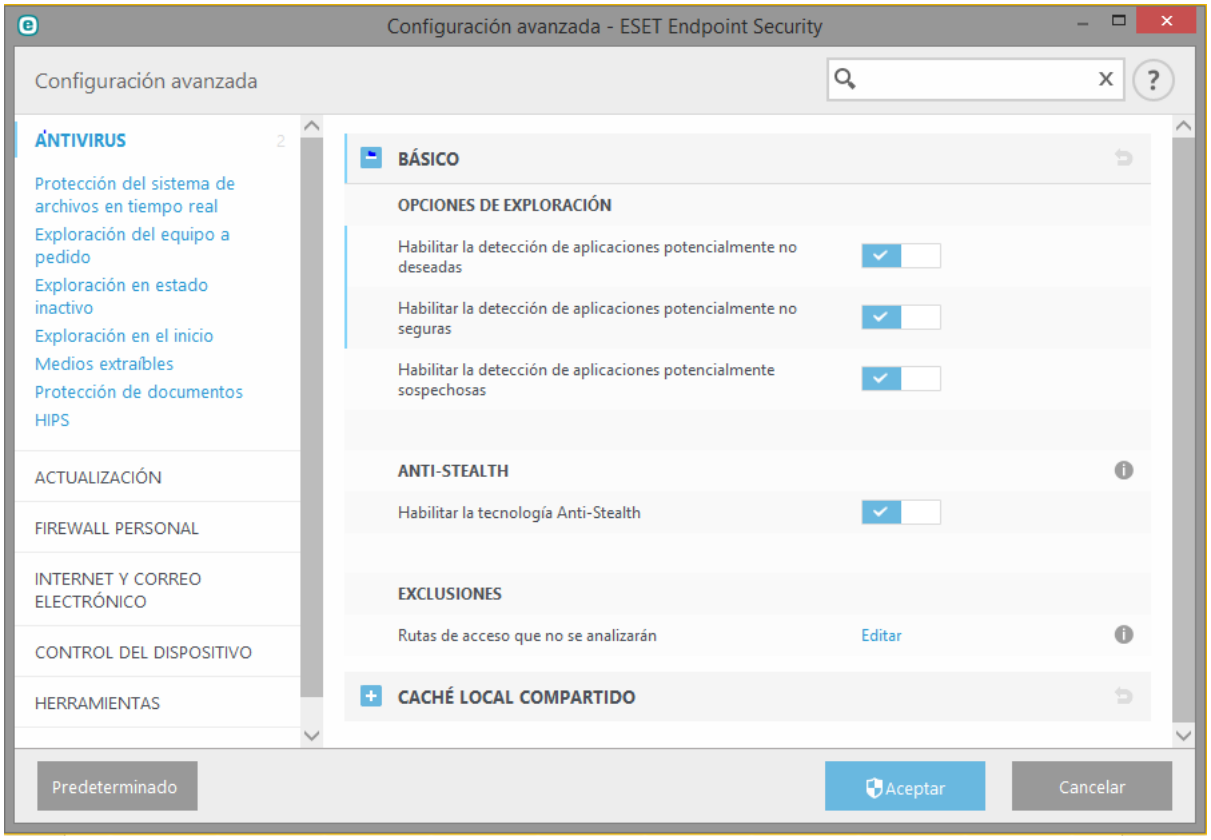
Habilitación de Heurística Avanzada en versión 6



• Asegurarse que no hay ningún tipo de exclusión de archivos o sitios web dentro del producto. Idealmente no se recomienda utilizar exclusiones salvo que sea alguna excepción puntual y necesaria, y que también se encuentre muy bien documentada.

• Asegurarse que los productos cuenten con una protección con contraseña, con el objetivo de que los usuarios no puedan modificar ninguna configuración del producto.

• Si tiene versión 6.2 de los productos de ESET tiene que tener en cuenta que debe habilitar la opción de Aplicaciones Potencialmente no deseadas.



• Finalmente, y como medida adicional, empresas que cuenten con la solución de ESET para entornos de correo electrónico con Microsoft Exchange Server (ESET Mail Security), también se recomienda que activen la detección de adjuntos potencialmente peligrosos para evitar la propagación de malware vía spam

3. ¿La red tendrá un peor rendimiento si activo todas estas funcionalidades?

No, de la forma que están desarrolladas las soluciones de ESET, a pesar de activar algunas funcionalidades que garantizarán una maximización en la detección de malware, no se verá ningún impacto en el rendimiento de los equipos o la red.

4. ¿Cómo puedo garantizar que ESET LiveGrid esté realmente funcionando además de estar activo?

En algunos casos específicos debido la configuración y la infraestructura de red, es posible que a pesar de que ESET LiveGrid esté activado, su funcionamiento no sea óptimo. En este sentido, no está demás garantizar su funcionamiento en lo que respecta a la detección de malware en sitios web y correos electrónicos.

Para esto, se ponen a disposición los siguientes pasos a seguir, utilizando un archivo de prueba para probar este tipo de tecnologías:

• Con ESET LiveGrid activo, descargue el archivo CloudCar desde el sitio web de AMTSO (Anti-Malware Testing Standards Organization) ubicado en: http://www.amtso.org/feature-settings-check-cloud-lookups/ • El archivo debería ser bloqueado previo a la descarga por el módulo de protección web y en caso que sea descargado, quiere decir que ESET LiveGrid no está funcionando correctamente. • En caso que el archivo no se haya podido descargar, temporalmente desactivar la protección web para descargar el archivo y guardarlo en el disco. • Una vez descargado el CloudCar, volver a activar la protección web • Abrir el cliente de correo electrónico y enviarse un correo a uno mismo con el archivo CloudCar adjunto. • El archivo debería ser sido bloqueado y eliminado por la solución de ESET. • En caso que el archivo haya sido recibido sin inconvenientes, quiere decir que ESET LiveGird no está funcionando correctamente.

Finalmente, si alguna de estas pruebas de detección falló y se pudo comprobar que ESET LiveGrid no tiene el funcionamiento óptimo, es ideal ponerse en contacto con ZMA a través del centro de soporte (http://soporte.zma.la) o mediante el envío de un correo a helpdesk@zma.la para solucionar el problema.