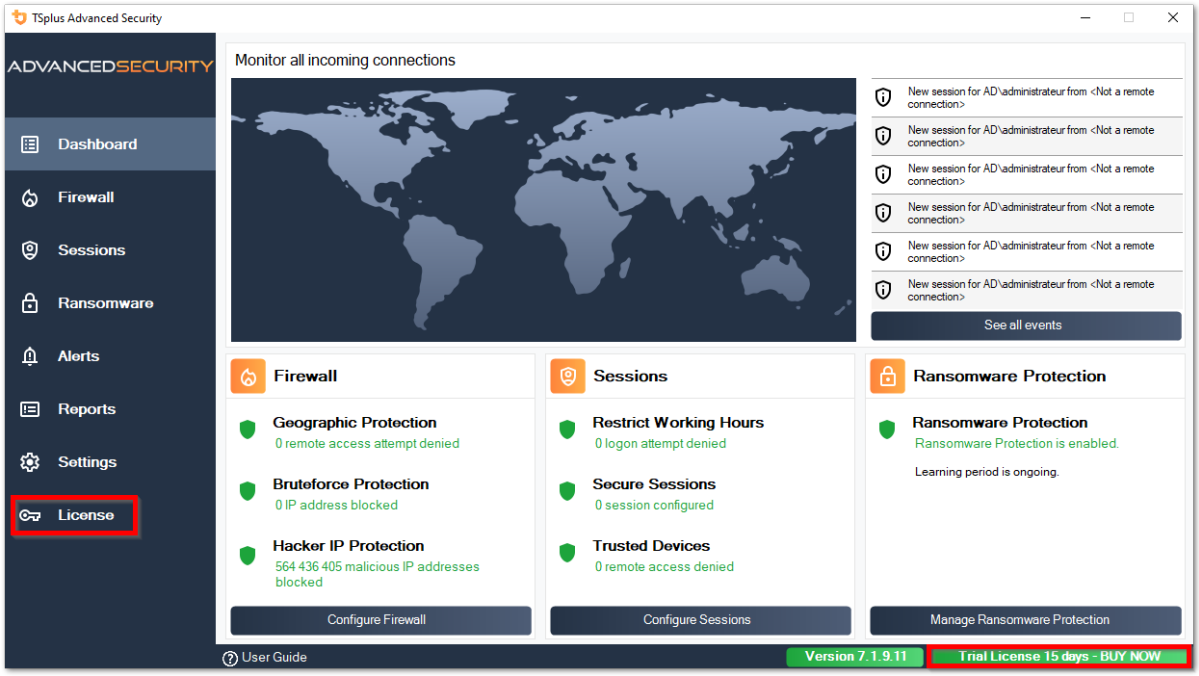
TSplus Advanced Security - Activando su licencia

Paso 1: Activar su licencia desde el modo Lite

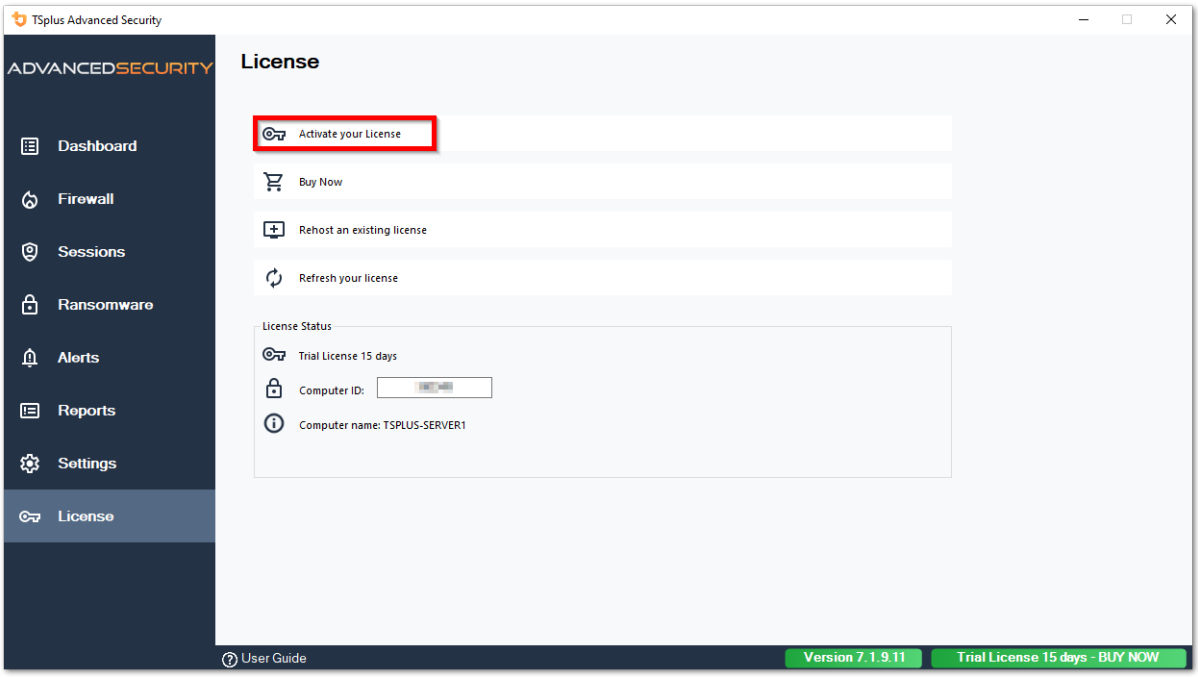
Haga clic en el botón "Licencia de prueba" para comprar una licencia o en la pestaña Licencia si ya tiene una licencia y una clave de activación.



Luego, haga clic en el botón "Activar su licencia".

Encontrará su clave de activación permanente. **(XXXX-XXXX-XXXX-XXXX)** en nuestro correo electrónico de confirmación de pedido.

Si desea activar su suscripción, ingrese su clave de suscripción. **S-XXXX-XXXX-XXXX-XXXX** .



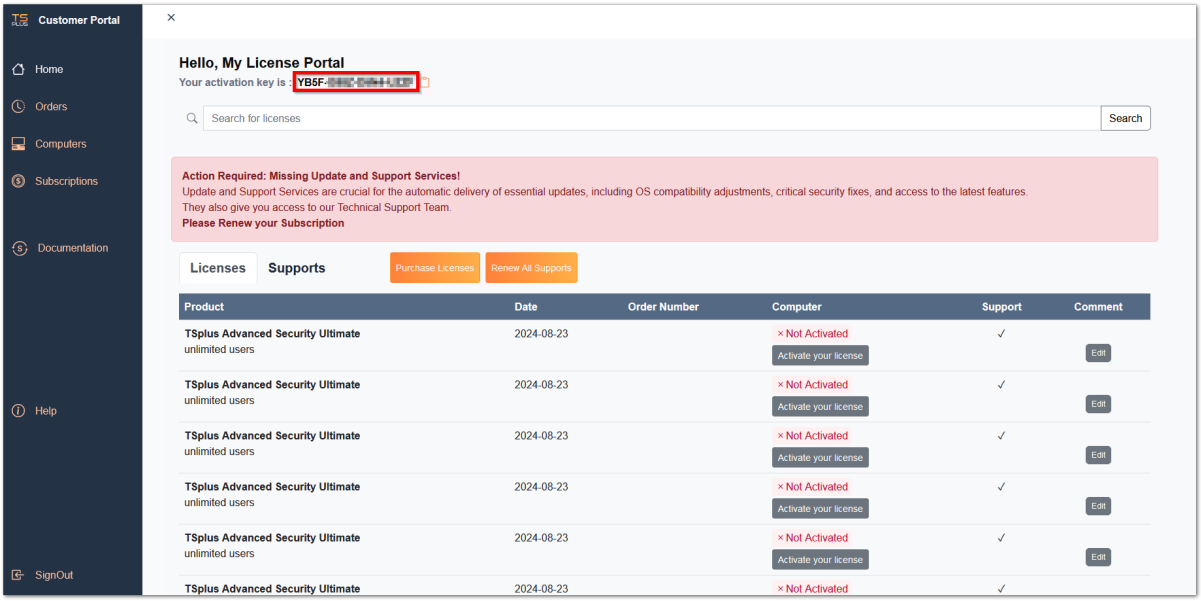
Si no conoce su clave de activación, por favor proceda al paso 2. De lo contrario, proceda al paso 3.

Paso 2: Recupere su clave de activación del portal de licencias

Para obtener su clave de activación, conéctese a nuestro Portal de Licencias y ingrese su dirección de correo electrónico y su número de pedido:

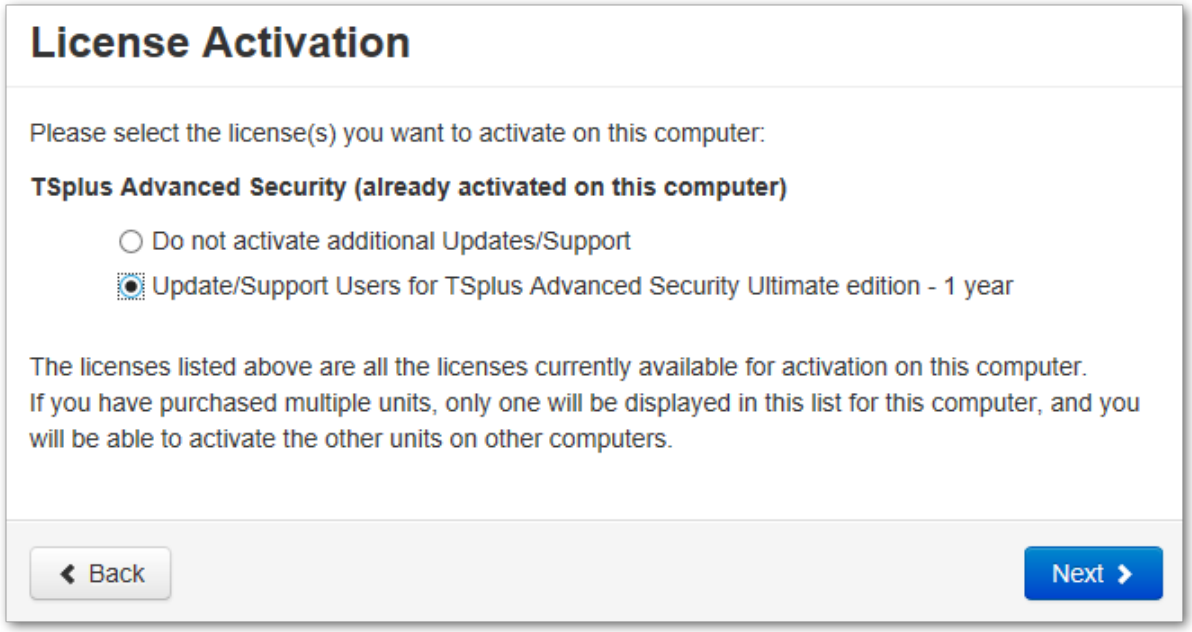
Descargar la Guía del Usuario del Portal del Cliente para más información sobre su portal de clientes.

Su clave de activación se mostrará en la parte superior del panel de control:

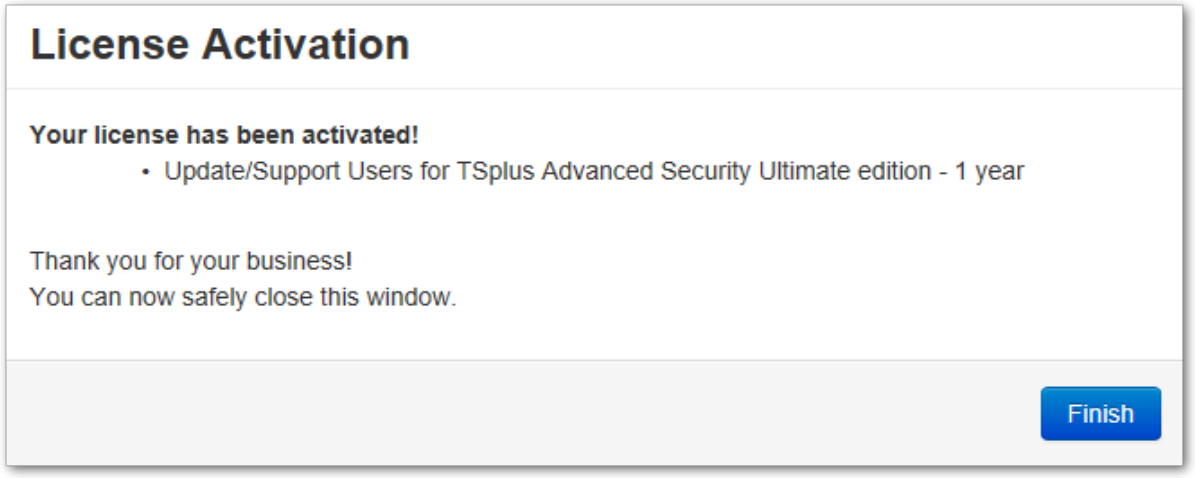


Paso 3: Seleccione las licencias solicitadas y los servicios de Actualización y Soporte para los productos instalados

Ingresa tu clave de activación y haz clic en "Siguiente".

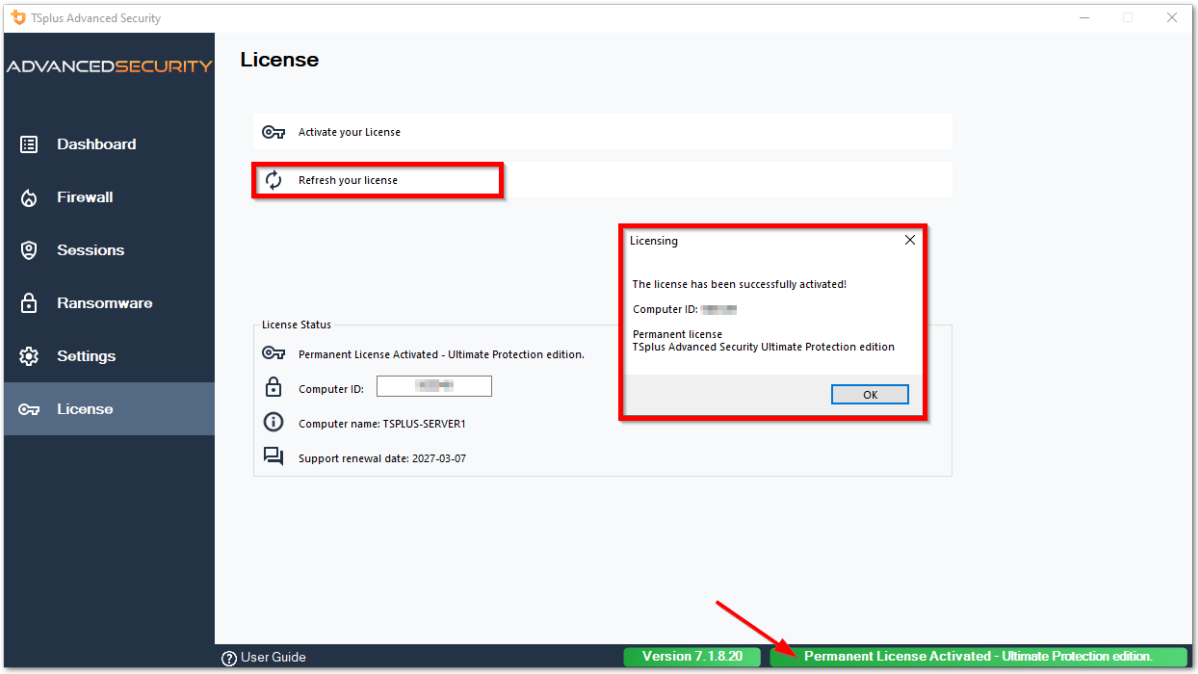


Marque uno o más elementos y haga clic en el botón "Siguiente". Tenga en cuenta que puede activar varios productos al mismo tiempo marcando varios productos y/o suscripciones de soporte.



Todos sus productos seleccionados y suscripciones de soporte están ahora activados (en este ejemplo, tanto TSplus con soporte como TSplus Advanced Security han sido activados a la vez).

Actualiza el estado de tu licencia haciendo clic en el botón correspondiente.



Activando su licencia (sin conexión)

Por favor, consulte el procedimiento descrito para TSplus Remote Access: Activando su licencia de TSplus (sin conexión)

Rehosting su licencia

Por favor, consulte el procedimiento descrito para TSplus Remote Access: Rehosting su

licencia de TSplus

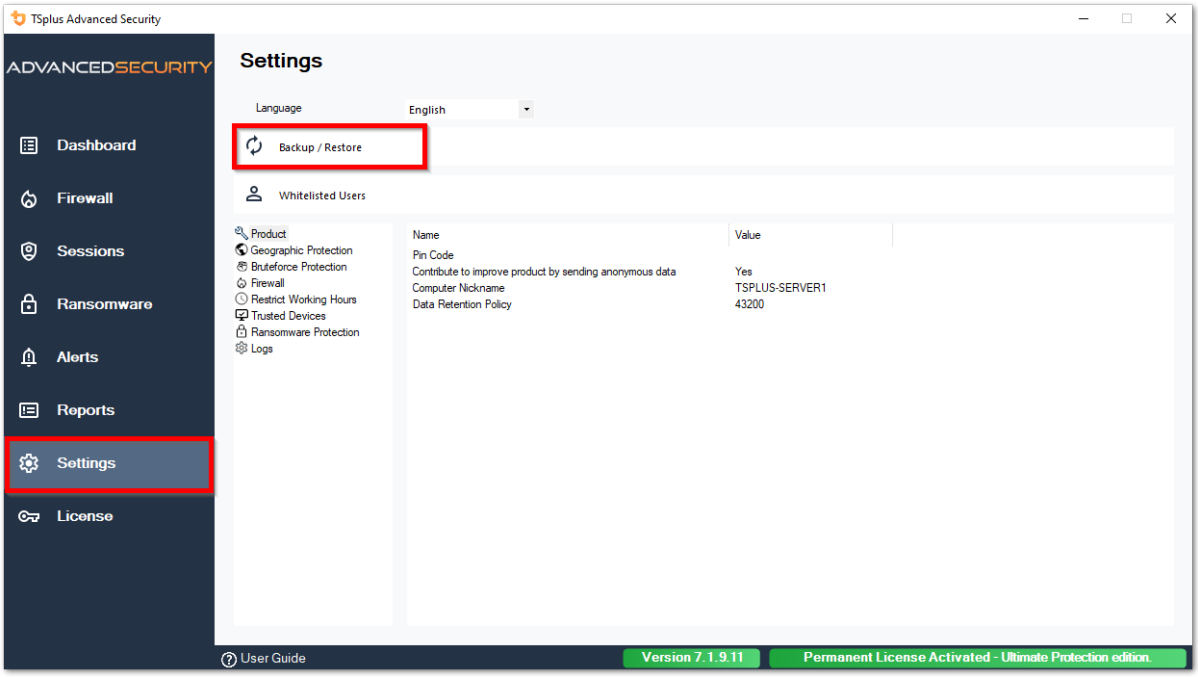
Nota: Puedes descargar un archivo license.lic en el Portal de Licencias para las versiones de TSplus Advanced Security a continuación. Por favor, consulta el Guía del usuario del portal del cliente para más información.

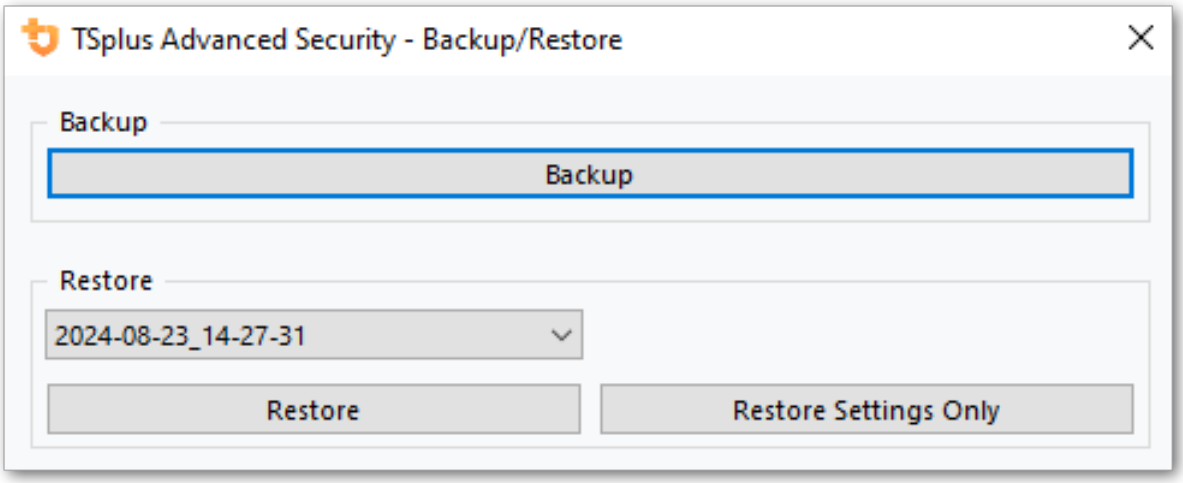
¡Gracias por elegir TSplus Advanced Security!

Avanzado - Copia de seguridad y restauración

Copia de seguridad y restauración de datos y configuraciones

Puedes hacer una copia de seguridad o restaurar los datos y configuraciones de TSplus Advanced Security haciendo clic en el botón "Copia de seguridad / Restaurar" en la parte superior:





La copia de seguridad se guardará en la carpeta **archivos** ubicado en el directorio de configuración de TSplus Advanced Security. Por defecto, el **archivos** la carpeta se encuentra aquí: C:\Program Files (x86)\TSplus-Security\archives

Usando la línea de comandos para hacer copias de seguridad y restaurar

El uso del comando se describe a continuación:

- **Copia de seguridad** TSplus-Security.exe /backup [ruta opcional a un directorio]

Por defecto, la copia de seguridad se creará en el directorio de archivos ubicado en la carpeta de configuración de TSplus Advanced Security. Sin embargo, la copia de seguridad puede guardarse en una carpeta especificada. Se permiten rutas relativas y absolutas.

- **Restaurar** TSplus-Security.exe /restore [ruta a un directorio de respaldo]

El directorio de respaldo especificado debe contener una carpeta de datos y una carpeta de configuraciones, como se creó con el comando /backup.

Configurando copias de seguridad

Tenga en cuenta que puede especificar la siguiente configuración avanzada en el registro:

- El directorio de respaldo se puede especificar en la clave del registro. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath Por defecto, se utilizará el directorio "archives" del directorio de configuración de Advanced Security.
-

Se puede especificar el número máximo de copias de seguridad disponibles en la clave del registro. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives Por defecto, Advanced Security mantiene las últimas 3 copias de seguridad.

Migra tus datos y configuraciones a otro ordenador

Por favor, siga los pasos a continuación para migrar Advanced Security de la computadora A a la computadora B:

1. En la computadora A, haga clic en el botón de Copia de seguridad para crear una nueva copia de seguridad. La configuración y los datos se guardarán en el directorio de archivos, ubicado en el directorio de configuración de seguridad avanzada (típicamente C:\Program Files (x86)\TSplus-Security\archives).

2. Copia la nueva carpeta de respaldo creada (por ejemplo, llamada backup-2019-09-11_14-37-31), incluyendo todo el contenido, desde el directorio de archivos en la computadora A al directorio de archivos en la computadora B.

3. En la computadora B, desde la ventana de Copia de seguridad / Restaurar, en la sección "Restaurar", seleccione el nombre de copia de seguridad relevante que se va a restaurar.

4. Luego, haga clic en Restaurar solo configuraciones para restaurar la configuración. Alternativamente, es posible hacer clic en Restaurar para restaurar todos los datos y configuraciones, lo cual no se recomienda para una migración, pero es útil para restaurar la seguridad avanzada en el equipo A.

5. Por favor, espere un máximo de 2 minutos para que la configuración se recargue mediante las funciones de seguridad avanzada.

Base de datos

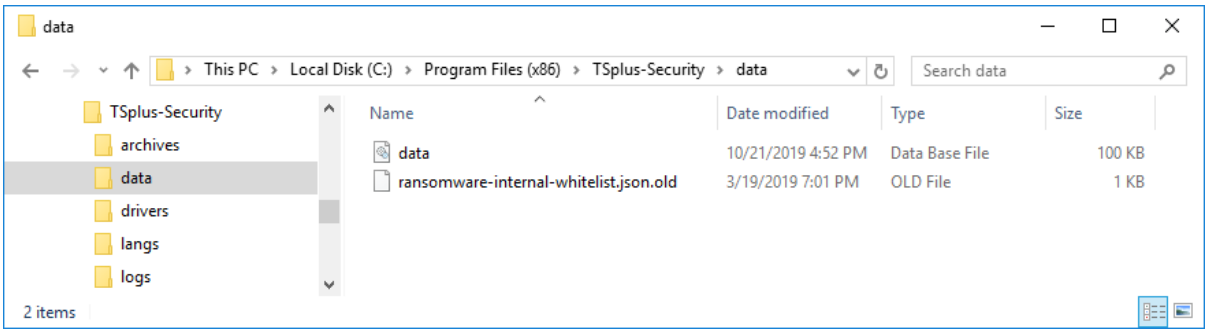
Una base de datos almacena eventos, direcciones IP, informes de ataques de ransomware y listas blancas de programas.

Esta base de datos se almacena en **datos** carpeta ubicada en el directorio de configuración de TSplus Advanced Security.

-

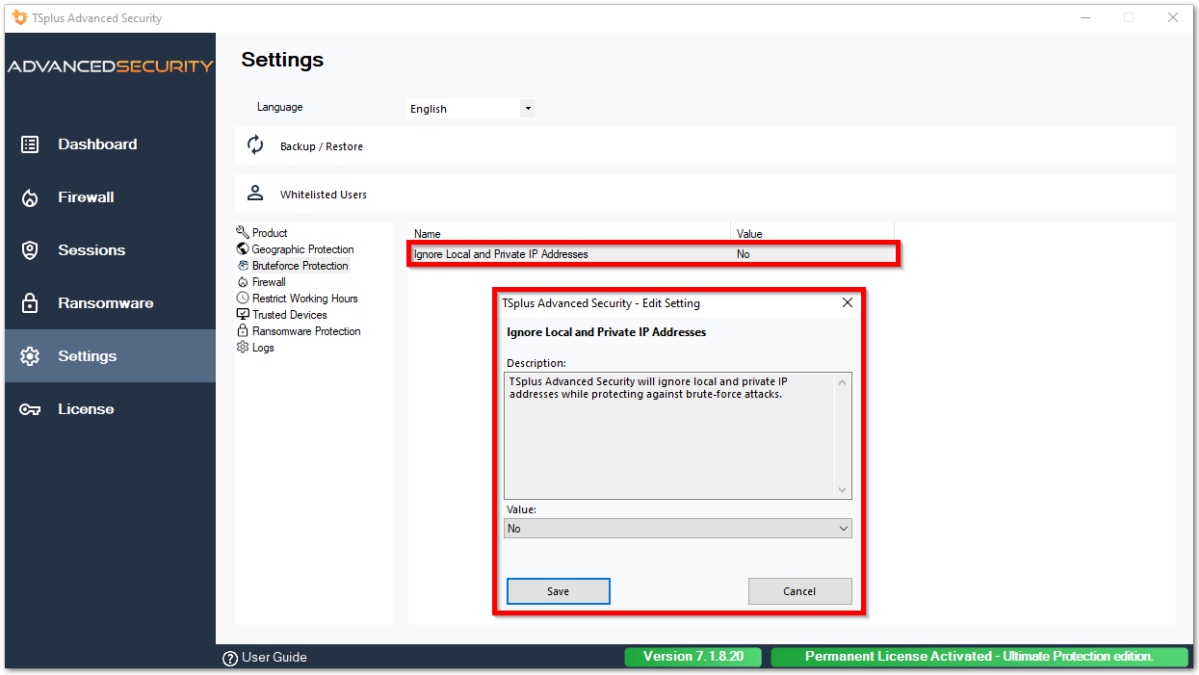
La Seguridad Avanzada de la versión 5 y anterior a la versión 5.3.10.6 utiliza un motor de base de datos LiteDB .

- Advanced Security superior a la versión 5.3.10.6 utiliza un motor de base de datos SQLite .



Protección contra ataques de fuerza bruta

El **Protección contra ataques de fuerza bruta** la pestaña te permite Ignorar direcciones IP locales y privadas si lo deseas, cambiando el valor predeterminado de "No" a "Sí".

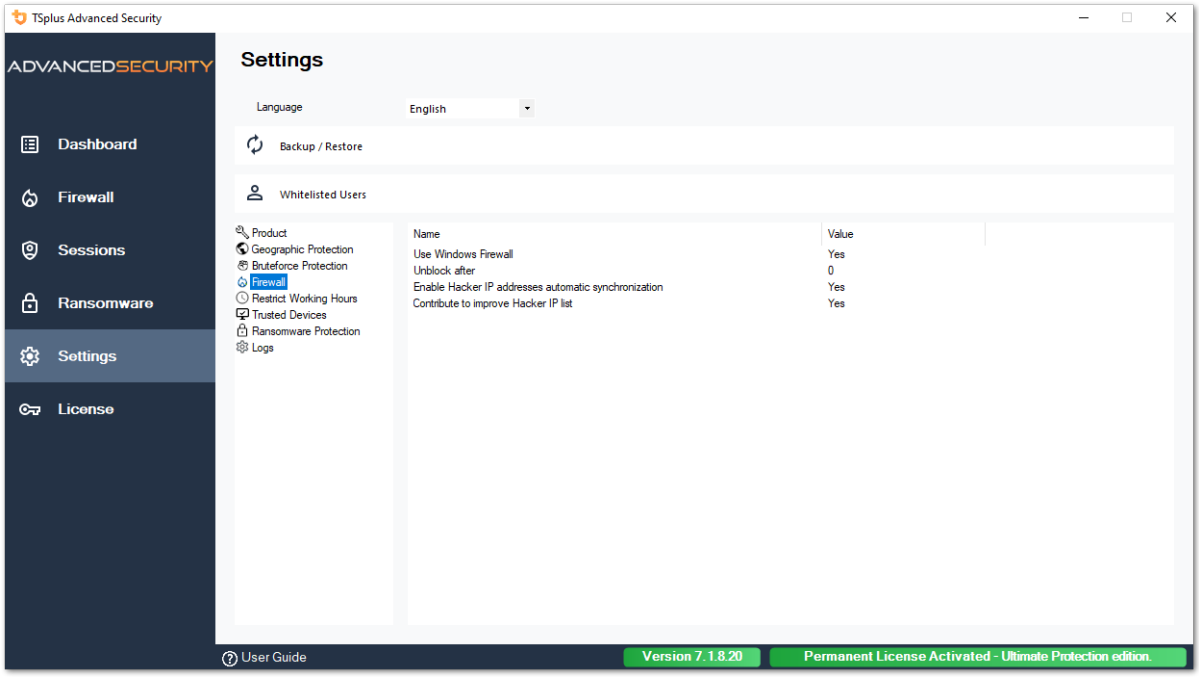


Avanzado - Cortafuegos

El **Cortafuegos** la pestaña te permite activar el **Firewall de Windows o desactívelo a favor del firewall integrado de TSplus Advanced Security** .

Desde la versión 4.4, se incluye un firewall integrado en TSplus Advanced Security.

Como regla general, si el Firewall de Windows está activado en su servidor, entonces debe usarlo para hacer cumplir las reglas de TSplus Advanced Security (predeterminado). Si instaló otro firewall, entonces debe activar el firewall integrado de TSplus Advanced Security.



Usar el Firewall de Windows Para activar el firewall integrado, ve a Configuración > Avanzado > Producto > Usar el firewall de Windows y establece el valor en: No. Si es Sí, entonces las direcciones IP ofensivas serán bloqueadas utilizando el firewall de Windows. De lo contrario, se utilizará el firewall de TSplus Advanced Security.

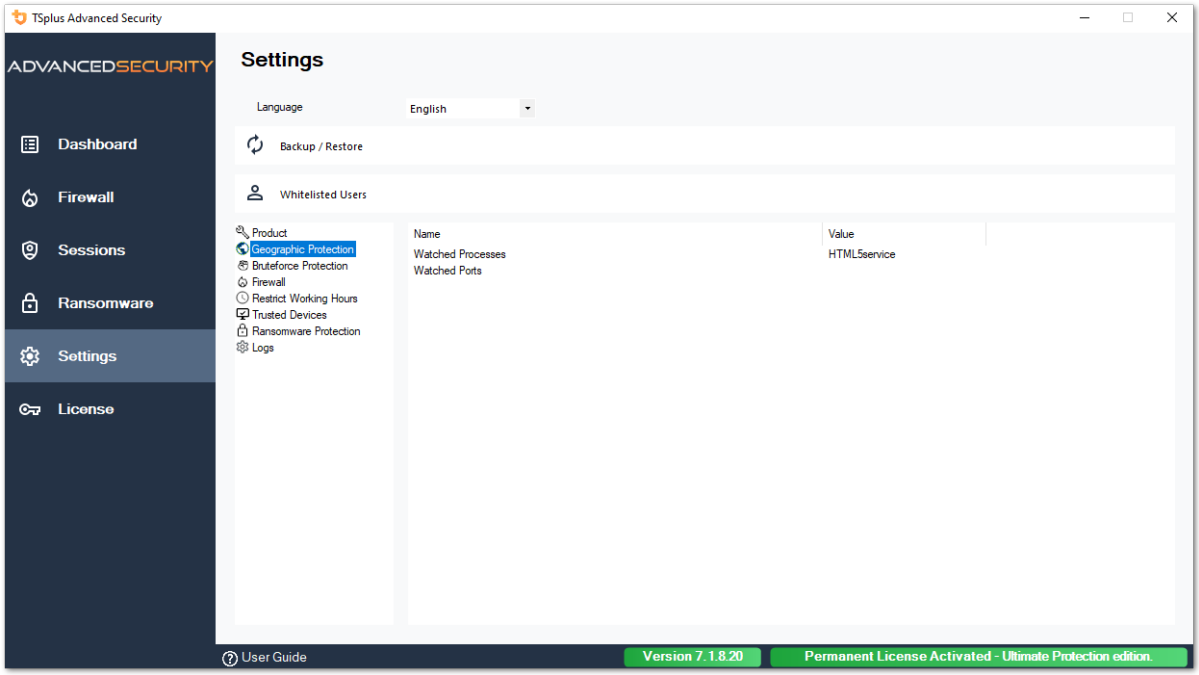
Desbloquear después Cambia esta configuración para desbloquear automáticamente las direcciones IP después de un cierto período de tiempo (en minutos). El valor predeterminado es 0, desactivando esta función. Valor: 0

Habilitar la sincronización automática de direcciones IP de hackers Mantenga su máquina protegida contra amenazas conocidas como ataques en línea, abuso de servicios en línea, malware, botnets y otras actividades electrónicas con la Protección de IP de Hacker. Se requiere una suscripción a los Servicios de Soporte y Actualizaciones. Valor: Sí.

Contribuir a mejorar la lista de IPs de hackers Permitir que TSplus Advanced Security envíe estadísticas de uso anónimas para mejorar la protección contra IP de hackers.
Valor: Sí

Protección Geográfica Avanzada

El **Protección Geográfica** la pestaña te permite agregar o eliminar procesos que son supervisados por el Protección Geográfica característica.



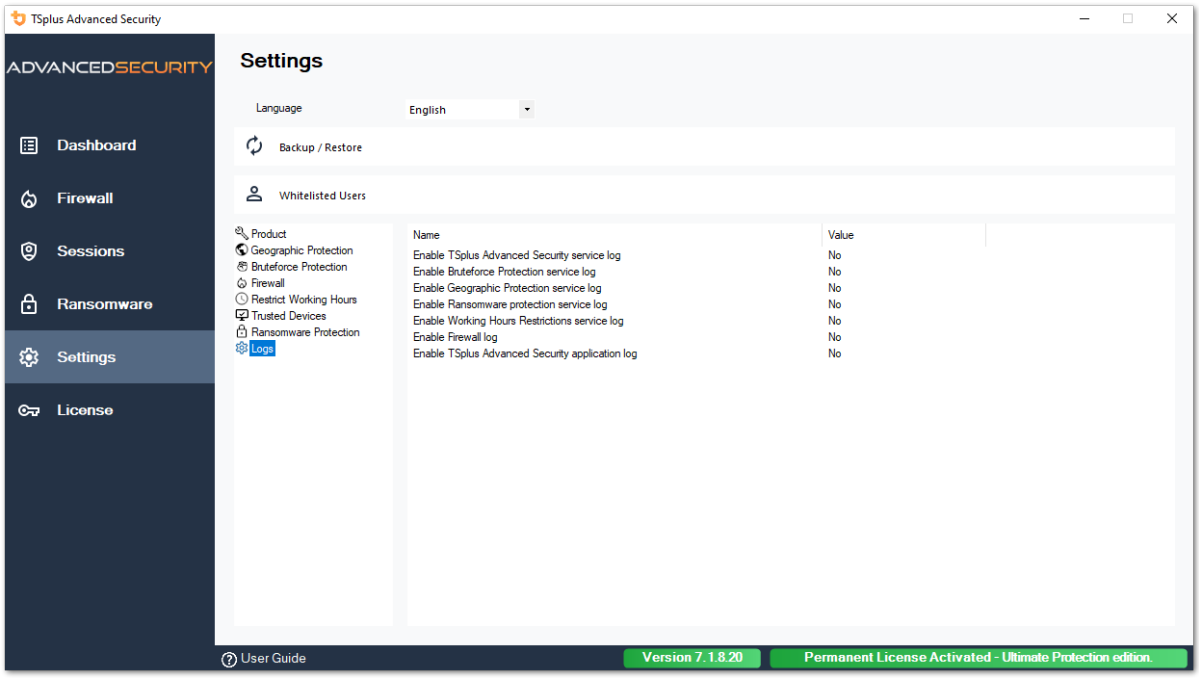
Por defecto, el servicio HTML5 es supervisado.

El **Puertos vigilados** la configuración te permite agregar puertos vigilados por el Protección Geográfica feature. Por defecto, Geographic Protection escucha los puertos predeterminados utilizados para conectarse de forma remota a un servidor. Estos puertos incluyen RDP (3389), Telnet (23) y puertos VNC. Geographic Protection es compatible con los siguientes proveedores de VNC: Tight VNC, Ultra VNC, Tiger VNC y Real VNC, que no están relacionados de ninguna manera con TSplus.

Avanzado - Registros

El **Registros** la pestaña te permite habilitar o deshabilitar los registros de servicios y funciones Existen registros para encontrar más fácilmente el origen de los errores encontrados en TSplus Advanced Security.

Para recuperar los registros, abre un Explorador y navega a la **registros** carpeta del directorio de instalación de TSplus Advanced Security. Por defecto, los registros se ubicarán aquí: **C:\Program Files (x86)\TSplus-Security\logs**



Habilitar o deshabilitar TSplus Advanced Security service y registros de aplicaciones , que son respectivamente el servicio de configuración global que se ejecuta en segundo plano y el registro para la interfaz de la aplicación.

También puede habilitar registros correspondientes a las características respectivas de TSplus Advanced Security:

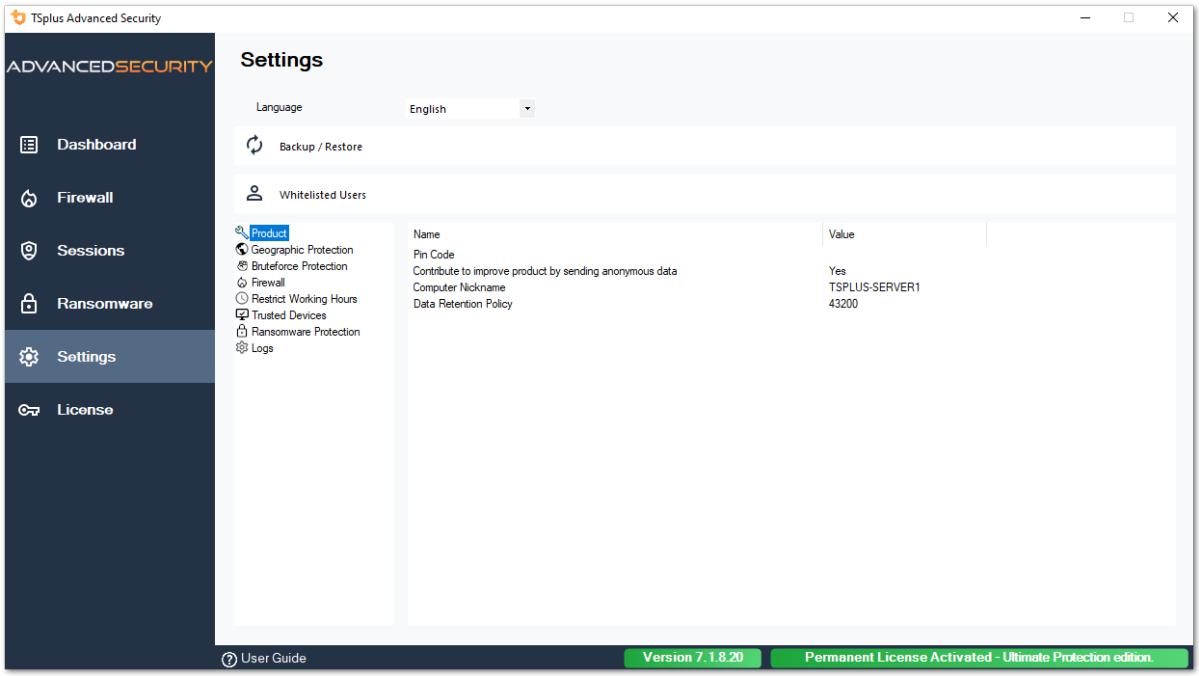
- Servicio
- Protección contra ataques de fuerza bruta
- Protección Geográfica

- Protección contra ransomware
- Restringir Horas de Trabajo
- Cortafuegos..
- Aplicación

Todos los registros están desactivados por defecto. Los registros corresponden a diferentes componentes, nuestro equipo de soporte le dirá qué valor poner según el problema encontrado.

Avanzado - Producto

El **Producto** la pestaña te permite agregar un código PIN a la aplicación :



Haga clic en Guardar. Se requerirá el código PIN la próxima vez que inicie la aplicación.

También puedes **contribuir a mejorar el producto** , enviando datos anónimos (activado por defecto): SÍ

Los siguientes datos se recopilarán en caso de un ataque de Ransomware:

- La versión de TSplus Advanced Security.
- Versión de Windows.
- Rutas de archivos sospechosos que conducen al ataque de ransomware.

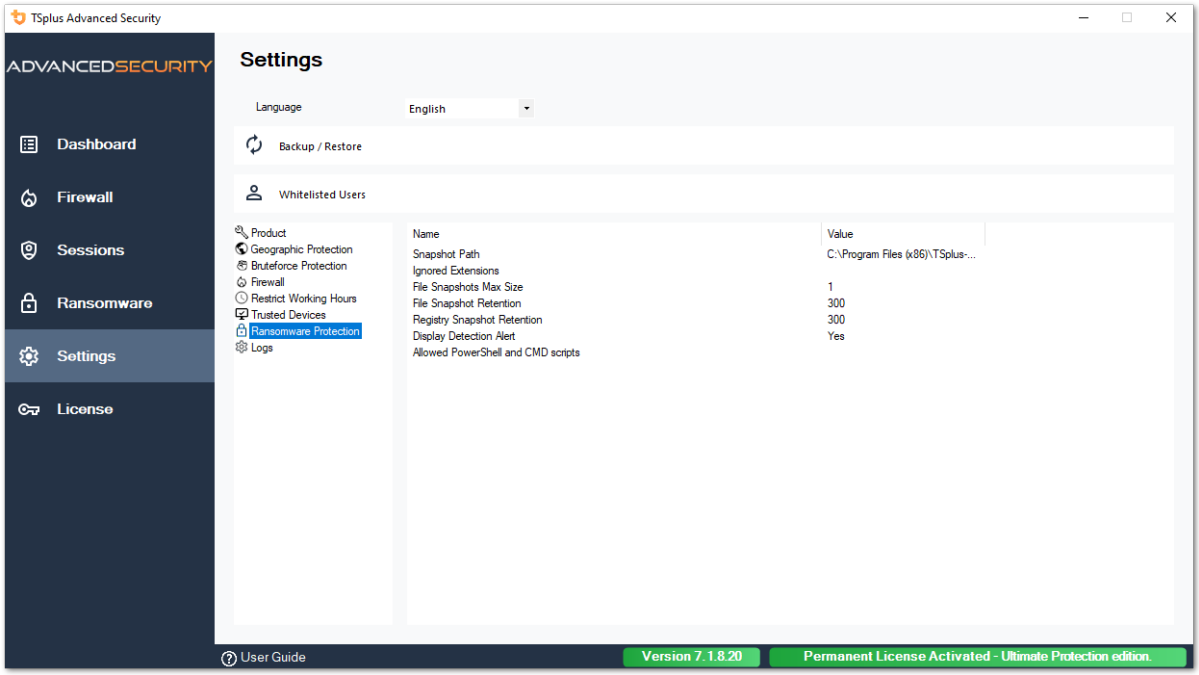
Modificando el **Apodo de la computadora** también es posible.

El **Política de Retención de Datos** define el período de tiempo después del cual los eventos de TSplus Advanced Security se eliminan de la base de datos. Se realiza una copia de seguridad antes de cada limpieza de la base de datos. Esta política se define en minutos. La

política de retención de datos predeterminada es de 259,200 minutos, o 6 meses.

Protección avanzada contra ransomware

El **Protección contra ransomware** la pestaña te permite configurar las propiedades de la instantánea y definir las extensiones de archivo ignoradas para la función de protección contra ransomware.



Ruta de instantánea Defina el directorio donde Ransomware Protection almacena instantáneas de archivos.

El valor predeterminado es: C:\Program Files (x86)\TSplus-Security\snapshots

Extensiones ignoradas Por defecto, la protección contra ransomware ignora las extensiones bien conocidas de archivos temporales para la actividad de ransomware. Vea la lista aquí Puede definir nombres de extensión personalizados en el campo de valor (separados por punto y coma):

Tamaño máximo de instantánea de archivo El tamaño máximo de los instantáneas de archivos define el espacio máximo permitido para retener instantáneas de archivos.

El tamaño se expresa en porcentaje del espacio total disponible en el disco donde reside la Ruta

de Instantánea.

Retención de instantáneas de archivos La retención de instantáneas de archivos define, en segundos, la política de retención de una instantánea de archivo.

Una vez que haya finalizado el período de retención, se elimina la instantánea del archivo. Por defecto, 300 segundos (es decir, 5 minutos)

Retención de instantáneas del registro La retención de instantáneas del registro define, en segundos, la política de retención de una instantánea del registro. Una vez que ha finalizado el período de retención, la instantánea del registro se elimina. Por defecto, 300 segundos (es decir, 5 minutos)

Alerta de detección de pantalla Mostrar una ventana de mensaje de alerta en el escritorio del usuario cuando la protección contra ransomware ha detectado y detenido un ataque.

Scripts de PowerShell y CMD permitidos Listas de scripts de PowerShell y CMD permitidos que muestran las rutas completas de los archivos de los scripts de PowerShell y CMD que se pueden ejecutar en la máquina.

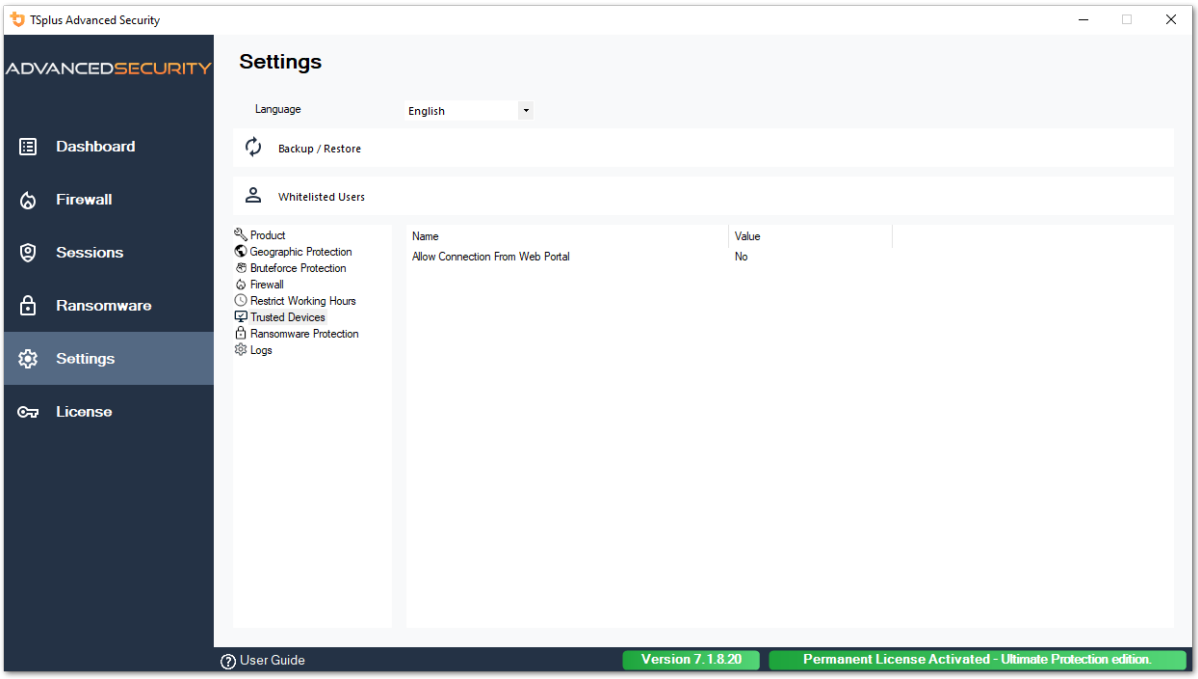
La ejecución de scripts permitidos no activará la protección contra ransomware (separados por punto y coma).

Avanzado - Dispositivos de confianza

El **Dispositivos de confianza** la pestaña permite habilitar conexiones desde el Portal Web de TSplus Remote Access.

Nota :

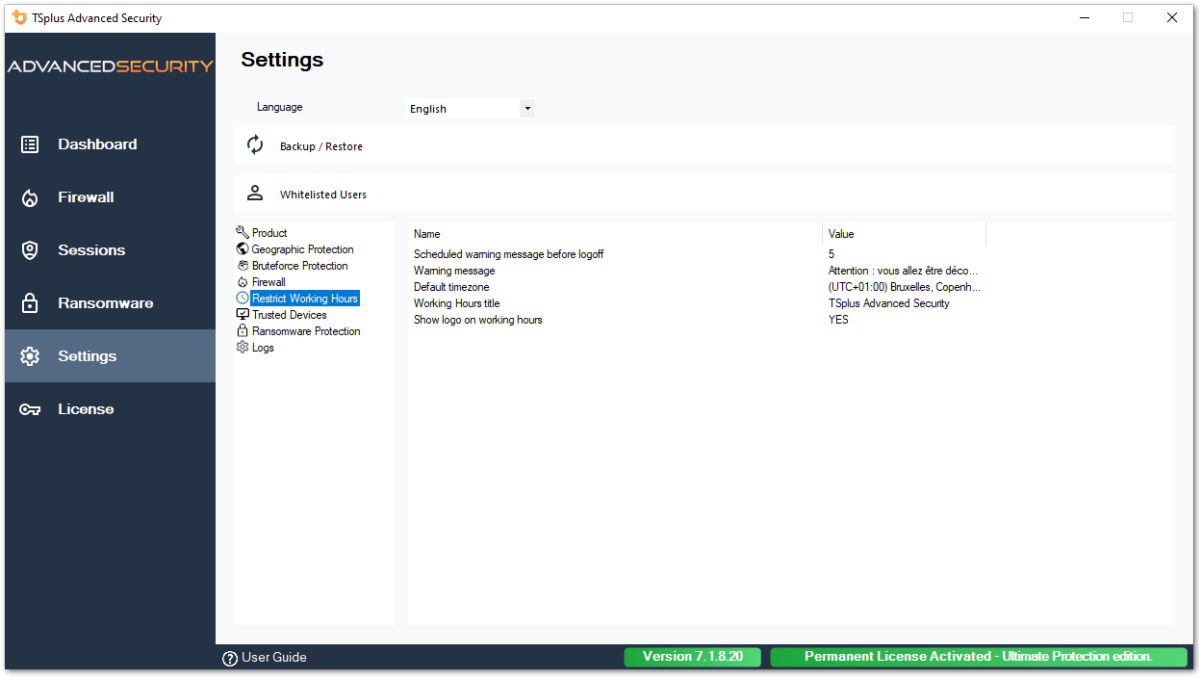
-Dispositivos de confianza no son compatibles con sesiones HTML5. -Dispositivos de confianza no son compatibles con dispositivos móviles iOS / Android ya que ocultan sus nombres de host reales. -El nombre de host de la máquina remota es definido por la propia máquina. Es probable que la máquina lo oculte o modifique según su configuración.



La función de Dispositivos de Confianza de TSplus Advanced Security no puede resolver el nombre del cliente si la conexión se inicia desde el portal web de TSplus Remote Access. Por lo tanto, los Dispositivos de Confianza bloquearán cualquier conexión desde el Portal Web por defecto. Establezca esta configuración en "Sí" para permitir conexiones desde el portal web. Tenga en cuenta que esta acción disminuirá la seguridad de su servidor.

Avanzado - Restringir Horas Laborales

El **Restringir Horas de Trabajo** la pestaña te permite Programe un mensaje de advertencia antes de que el usuario sea desconectado .



Mensaje de advertencia programado Puedes configurar el número de minutos antes de que el usuario sea desconectado automáticamente. Por defecto, está configurado en 5 minutos.

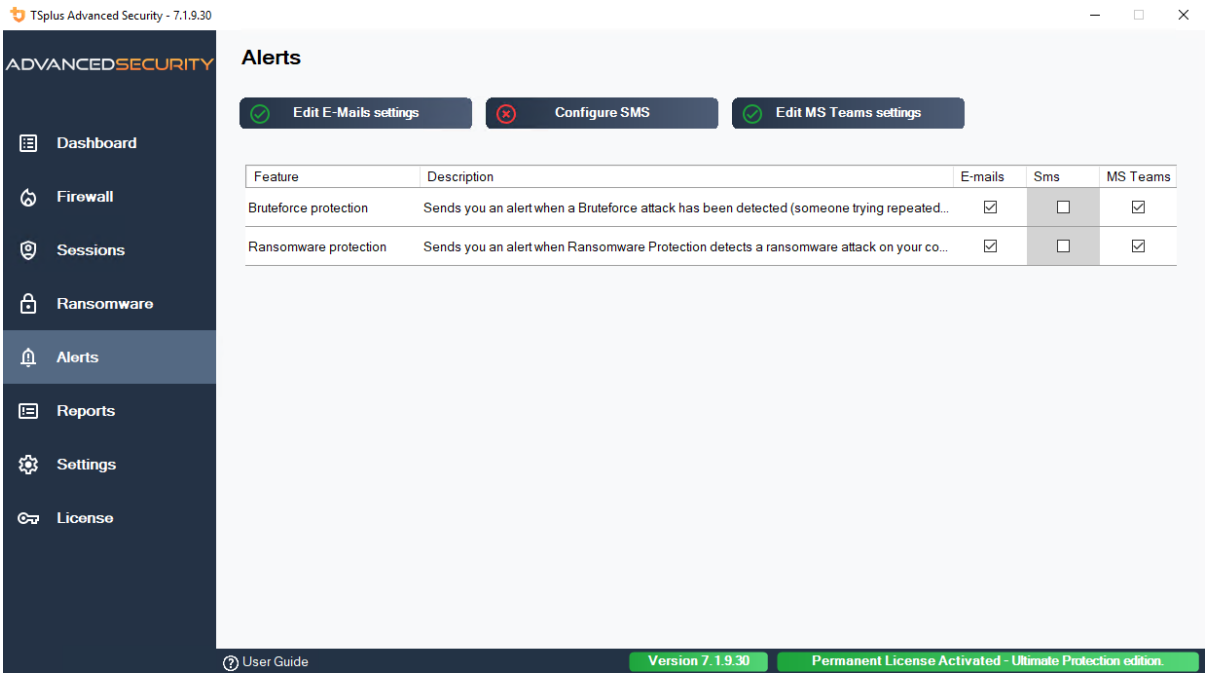
Mensaje de advertencia Se puede definir un mensaje de advertencia a su conveniencia, con marcadores de posición llamados %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% y %ENDINGHOURS%, que serán reemplazados respectivamente por el número actual de minutos antes de que la sesión se cierre, el día actual, las horas de trabajo de inicio y fin del día actual.

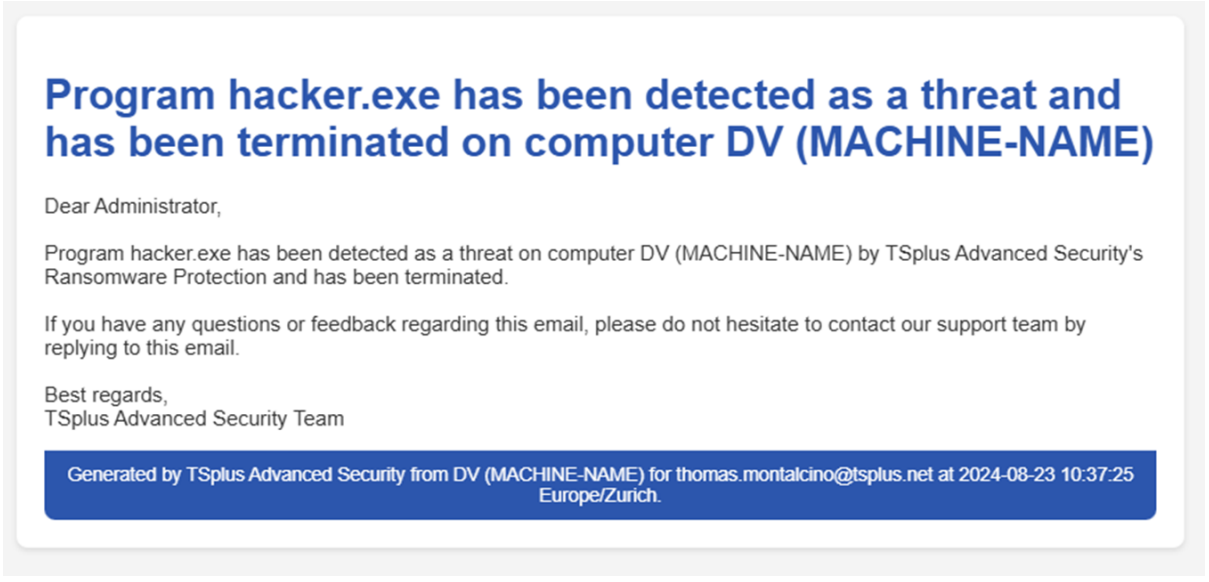
Zona horaria del servidor predeterminada Se puede definir una zona horaria de servidor predeterminada para aplicar las reglas de horario laboral en consecuencia seleccionando la correspondiente en la lista desplegable.

Horas de trabajo título Título del formulario mostrado al usuario final, cuando sus horas de trabajo están terminando (predeterminado: TSplus Advanced Security)

Mostrar logo en horario laboral Si se establece en "sí", el logo se muestra en la forma que se presenta al usuario final, cuando sus horas de trabajo están terminando (predeterminado: "sí")

Alertas





Program hacker.exe has been detected as a threat and has been terminated on computer DV (MACHINE-NAME)

Dear Administrator,

Program hacker.exe has been detected as a threat on computer DV (MACHINE-NAME) by TSplus Advanced Security's Ransomware Protection and has been terminated.

If you have any questions or feedback regarding this email, please do not hesitate to contact our support team by replying to this email.

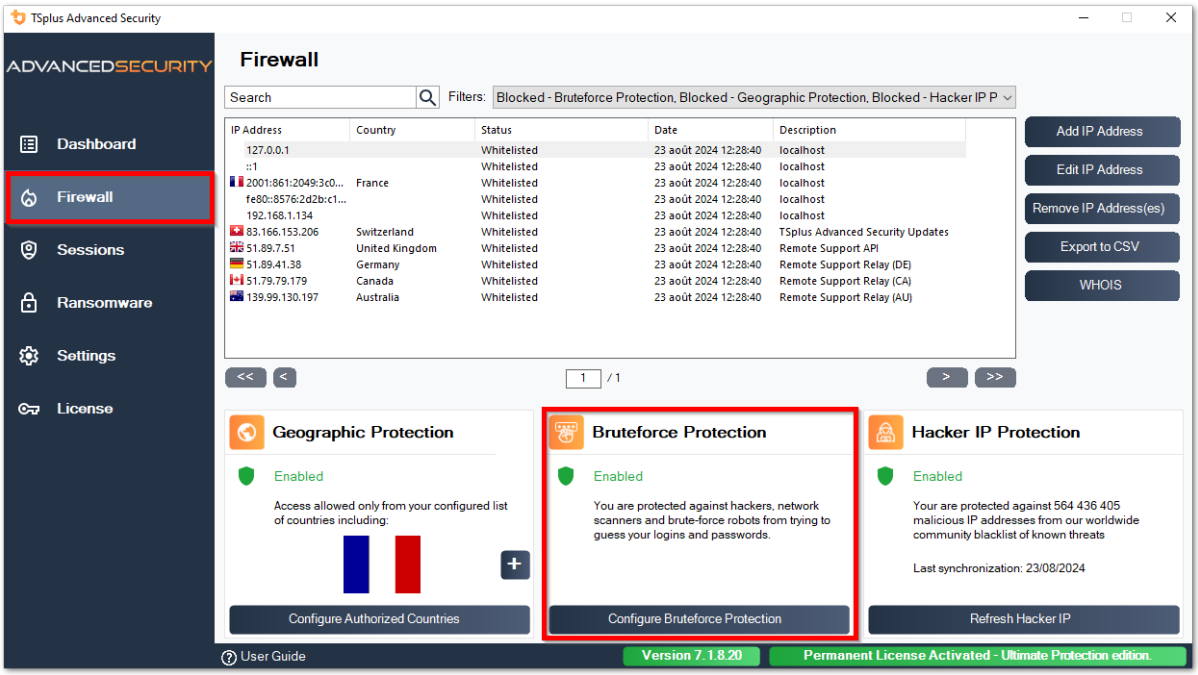
Best regards,
TSplus Advanced Security Team

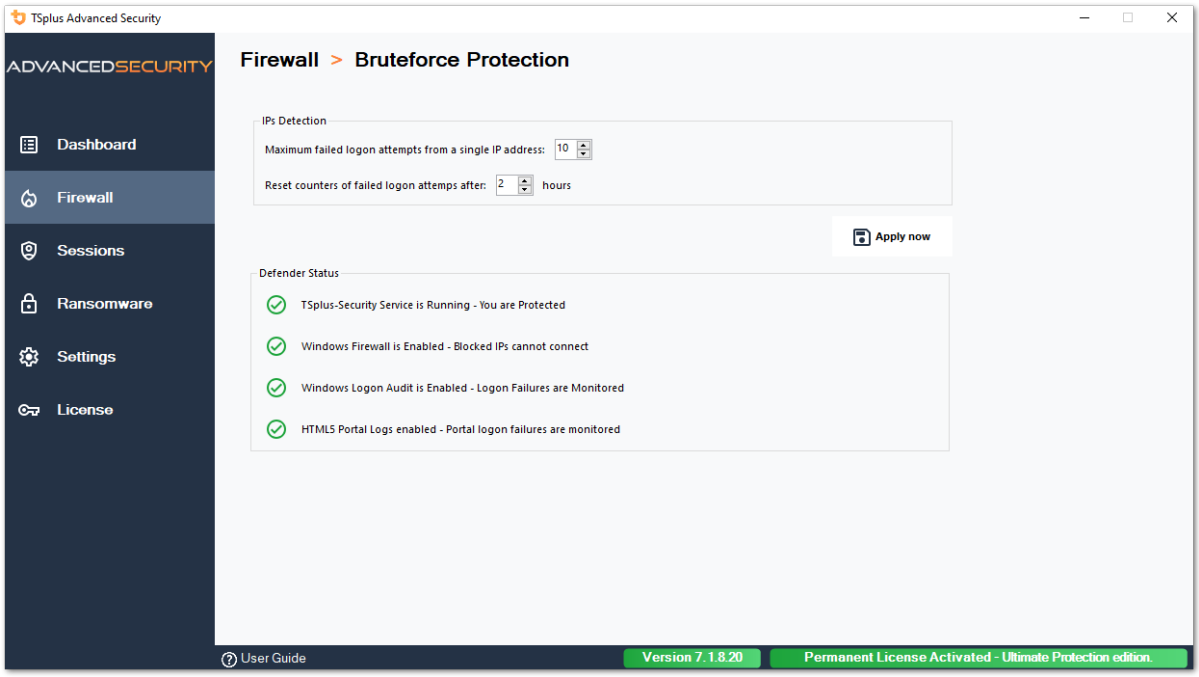
Generated by TSplus Advanced Security from DV (MACHINE-NAME) for thomas.montalcino@tsplus.net at 2024-08-23 10:37:25 Europe/Zurich.

Protección contra ataques de fuerza bruta

La protección contra ataques de fuerza bruta le permite proteger su servidor público de hackers, escáneres de red y robots de fuerza bruta que intentan adivinar su inicio de sesión y contraseña de Administrador. Utilizando inicios de sesión actuales y diccionarios de contraseñas, intentarán automáticamente iniciar sesión en su servidor cientos a miles de veces por minuto.

Con este RDP Defender, puedes monitorear los intentos de inicio de sesión fallidos de Windows y automáticamente poner en lista negra las direcciones IP infractoras después de varios fallos.





- Puedes configurar el **máximo de intentos de inicio de sesión fallidos desde una única dirección IP dentro del bloque de detección de IPs** por defecto, son 10, así como el tiempo de restablecimiento para los contadores de intentos de inicio de sesión fallidos (por defecto son 2 horas).

- En la parte inferior de esta ventana, puedes ver el **Estado del defensor** donde puedes verificar si los fallos de inicio de sesión del Portal Web HTML5, los fallos de inicio de sesión de Windows son monitoreados y si el Firewall de Windows y el servicio de seguridad avanzada están habilitados.

En este caso, al igual que en nuestro ejemplo, todos los estados están marcados.

- **Administrar direcciones IP bloqueadas** Puedes, por supuesto, configurarlo para que se ajuste a tus necesidades, por ejemplo, añadiendo tu propia dirección IP de estación de trabajo en el Lista blanca de IPs , por lo que esta herramienta nunca te bloqueará. Puedes agregar tantas direcciones IP como desees en la lista blanca. Estas direcciones nunca serán bloqueadas por la Protección contra ataques de fuerza bruta.

- Puedes **ignorar direcciones IP locales y privadas** cambiando la configuración predeterminada en el Configuración > Avanzado > pestaña de protección contra fuerza bruta

Nota: Si alguna vez notas que la Protección contra Bruteforce bloqueó 10 direcciones IP por día y que ahora, ese ya no es el caso; y bloquea una, dos o incluso no bloquea ninguna

dirección, en realidad es normal. De hecho, antes de la instalación de advanced-security, el servidor que tiene un puerto RDP disponible públicamente es conocido por todos los robots, y muchos robots intentan las contraseñas actuales y las que provienen de diccionarios. Cuando instalas advanced-security, estos robots son bloqueados progresivamente, de modo que un día:

- La mayoría de los robots activos ya están bloqueados y no están interesados en el servidor, incluso los nuevos.
- Además, el servidor ya no aparece en la lista de servidores conocidos públicamente.

Líneas de comando

Estamos complacidos de proporcionarle un conjunto completo de herramientas de línea de comandos diseñadas para mejorar la flexibilidad y eficiencia de nuestro software. Estas herramientas permiten a los usuarios crear scripts y automatizar diversas funcionalidades, adaptando el software para satisfacer sus necesidades y flujos de trabajo específicos.

Explora las posibilidades y optimiza tu experiencia con nuestras opciones de línea de comandos.

Solo tienes que ejecutar las siguientes líneas de comando como un Administrador elevado. Como recordatorio, TSplus-Security.exe se encuentra en la siguiente carpeta. **C:\Program Files (x86)\TSplus-Security** por defecto.

Gestión de Licencias

Para realizar operaciones en licencias, reemplace el programa AdminTool.exe presentado en la siguiente documentación por el programa TSplus-Security.exe ubicado en el directorio de configuración de Advanced Security (generalmente **C:\Program Files (x86)\TSplus-Security**).

- Activación de licencia
- Restablecimiento de licencia tras la clonación de una VM
- Activación de licencia por volumen
- Habilitar y deshabilitar la licencia por volumen
- Actualización de licencia por volumen
- Mostrar los créditos de licencia restantes para una clave de Licencia por Volumen
- Mostrar créditos de soporte restantes para una clave de licencia por volumen

---

Configurar servidor proxy: /proxy /set

Sintaxis:

TSplus-Security.exe /proxy /set [parámetros]

Descripción:

Comando /proxy /set se utiliza para configurar un servidor proxy para el acceso a Internet.

Parámetros:

- /host el host de destino puede ser un valor predefinido (“ie” o “none”) o un valor definido por el usuario (por ejemplo: 127.0.0.1 o proxy.company.org). Este parámetro es obligatorio
- /port el número de puerto utilizado para conectarse al servidor proxy. Requerido si el valor del nombre de host es un valor definido por el usuario personalizado.
- /username el nombre de usuario para conectarse al servidor proxy. Esta configuración es opcional
- /password la contraseña del usuario debe ser proporcionada si se ha definido un nombre de usuario. Sin embargo, su valor puede estar vacío

Ejemplos:

TSplus-Security.exe /proxy /set /host proxy.company.org /port 80 /username dummy /password pass@word1

TSplus-Security.exe /proxy /set /host ie

Para más información, por favor visite ¿Cómo configurar un servidor proxy para el acceso a Internet?

Copia de seguridad de datos y configuraciones: /backup

Sintaxis:

TSplus-Security.exe /backup [RutaDelDirectorioDeDestino]

Descripción:

Comando /backup se utiliza para respaldar los datos y configuraciones de TSplus Advanced Security.

Por defecto, la copia de seguridad se creará en el directorio de archivos ubicado en el directorio de configuración de Advanced Security (por ejemplo: C:\Program Files (x86)\TSplus-Security\archives).

Parámetros:

- DestinationDirectoryPath para hacer una copia de seguridad en otro directorio que no sea el predeterminado. Se permiten rutas relativas y absolutas.

Ejemplos:

TSplus-Security.exe /backup TSplus-Security.exe /backup “C:\Users\admin\mycustomfolder”

Para más información, por favor visite Avanzado - Copia de seguridad y restauración

---

Restaurar datos y configuraciones: /restore

Sintaxis:

TSplus-Security.exe /restore [Ruta del directorio de respaldo]

Descripción:

Comando /restore se utiliza para restaurar los datos y configuraciones de TSplus Advanced Security.

La ruta del directorio de respaldo especificado debe ser creada mediante el comando /backup o desde la función de respaldo de la aplicación.

Parámetros:

- Backup Directory Path la ruta donde se encuentra el directorio de respaldo para restaurar.

Ejemplos:

TSplus-Security.exe /restore “C:\Program Files (x86)\TSplus-Security\archives\backup-2025-03-11_21-45-51-setup” /silent

Para más información, por favor visite Avanzado - Copia de seguridad y restauración

---

Eliminar y desbloquear todas las direcciones IP bloqueadas: /unblockall

Sintaxis:

TSplus-Security.exe /desbloqueartodo

Descripción:

Comando /unblockall se utiliza para eliminar todas las direcciones IP bloqueadas del firewall de TSplus Advanced Security y desbloquearlas del firewall de Microsoft Windows Defender si es necesario.

Ejemplos:

TSplus-Security.exe /desbloqueartodo

Para más información, por favor visite Cortafuegos

Eliminar y desbloquear direcciones IP especificadas: /unblockips

Sintaxis:

TSplus-Security.exe /desbloquearips [direcciones IP]

Descripción:

Comando /unblockips se utiliza para eliminar todas las direcciones IP bloqueadas especificadas del firewall de TSplus Advanced Security y desbloquearlas del firewall de

Microsoft Windows Defender si es necesario.

Este comando no tiene efecto en las direcciones IP que ya están bloqueadas por la protección de IP de Hacker. Si aún desea desbloquear una de estas direcciones, utilice el comando de lista blanca.

Parámetros:

- IP addresses la lista de direcciones ip o rangos de ip a desbloquear (separados por coma o punto y coma).

Ejemplos:

TSplus-Security.exe /unblockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5

Para más información, por favor visite Cortafuegos

Bloquear direcciones IP específicas: /blockips

Sintaxis:

TSplus-Security.exe /blockips [direcciones IP] [Descripción opcional]

Descripción:

Comando /blockips se utiliza para bloquear todas las direcciones IP especificadas utilizando el firewall de TSplus Advanced Security y bloquearlas utilizando el firewall de Microsoft Windows Defender si está configurado.

Parámetros:

- IP addresses la lista de direcciones IP o rangos de IP para bloquear (separados por coma o punto y coma).
- Optional Description una descripción opcional que se añadirá para cada entrada.

Ejemplos:

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Los lugares de trabajo de John”

Para más información, por favor visite Cortafuegos

Agregar direcciones IP a la lista blanca: /addwhitelistedip

Sintaxis:

TSplus-Security.exe /addwhitelistedip [direcciones IP] [Descripción opcional]

Descripción:

Comando /addwhitelistedip se utiliza para agregar direcciones IP especificadas a las direcciones IP autorizadas del firewall de TSplus Advanced Security y desbloquearlas del firewall de Microsoft Windows Defender si es necesario.

Parámetros:

- IP addresses la lista de direcciones IP o rangos de IP para agregar a la lista blanca (separados por coma o punto y coma).
- Optional Description una descripción opcional que se añadirá para cada entrada.

Ejemplos:

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Lugares de trabajo de John”

Para más información, por favor visite Cortafuegos

Agregar un programa o directorio a la lista autorizada de protección contra ransomware: /whitelist

Sintaxis:

TSplus-Security.exe /whitelist add [Rutas Autorizadas]

Descripción:

Comando /whitelist add se utiliza para agregar rutas de programas y rutas de directorios especificados a la lista autorizada de la Protección contra Ransomware de TSplus Advanced Security.

Parámetros:

- Authorized Paths la lista de rutas de programas y rutas de directorios para agregar a la lista de autorización de Protección contra Ransomware de TSplus Advanced Security (separadas por punto y coma).

Ejemplos:

TSplus-Security.exe /whitelist add “C:\Windows\notepad.exe;C:\Program Files (x86)\Tsplus\Client\webserver”

Para más información, por favor visite Acción de Protección contra Ransomware

---

Actualizar la protección de IP de Hacker: / refreshipprotection

Sintaxis:

TSplus-Security.exe /refreshipprotection

Descripción:

Comando /refreshipprotection se utiliza para actualizar la lista de rangos de IP bloqueados para la función de protección de IP contra hackers. Se requiere una suscripción a los servicios de soporte y actualizaciones.

Ejemplos:

TSplus-Security.exe /refreshipprotection

Para más información, por favor visite Protección de IP de Hacker

---

Establecer nivel de registro: /setloglevel

Sintaxis:

TSplus-Security.exe /setloglevel [Nivel de registro]

Descripción:

Comando /setloglevel se utiliza para establecer el nivel de registro para todos los componentes de Advanced Security.

Parámetros:

- Log Level el nivel de registro entre los siguientes valores: TODOS, DEPURACIÓN, INFORMACIÓN, ADVERTENCIA, ERROR, FATAL, APAGADO

Ejemplos:

TSplus-Security.exe /setloglevel ALL

Para más información, por favor visite Avanzado > Registros

Agregar dispositivos de confianza: /addtrusteddevices

Sintaxis:

TSplus-Security.exe /addtrusteddevices [Configuración de Dispositivos de Confianza]

Descripción:

Comando /addtrusteddevices se utiliza para agregar dispositivos de confianza de forma programática. Requiere edición Ultimate.

Parámetros:

- Trusted Devices Configuration El argumento se compone de una lista de dispositivos de confianza (separados por punto y coma), estructurada de la siguiente manera:

Nombre de usuario y dispositivos están separados por el carácter de dos puntos (:).

Detalles del usuario:

Tipo de usuario y nombre de usuario completo están separados por el carácter dos puntos (:). Los tipos de usuario aceptados son "usuario" y "grupo".

Palabra clave opcional "deshabilitada": si se incluye, los dispositivos de confianza se crearán, pero las restricciones estarán deshabilitadas para este usuario. Si no se menciona, las restricciones están habilitadas por defecto.

Detalles del dispositivo:

Nombre del dispositivo y comentario opcional: separados por el signo igual (=).

Los dispositivos están separados por el carácter dos puntos (:).

Ejemplos:

TSplus-Security.exe /addtrusteddevices “user:WIN-A1BCDE23FGH\admin:disabled,device1name=este es un comentario para el dispositivo 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name:device4name=otro comentario;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name”

Para más información, por favor visite Dispositivos de confianza

---

Habilitar dispositivos de confianza

configurados: /enabletrusteddevices

Sintaxis:

TSplus-Security.exe /enabletrusteddevices [Usuario o Grupos]

Descripción:

Comando /enabletrusteddevices se utiliza para habilitar todos los dispositivos de confianza configurados para los usuarios y grupos especificados.

Parámetros:

- User or Groups El argumento es una lista de usuarios y grupos (separados por punto y coma). Dentro del nombre de usuario, la separación entre el tipo de usuario (“usuario” y “grupo” son los únicos valores aceptados) y el nombre de usuario completo se realiza mediante dos puntos.

Ejemplos:

TSplus-Security.exe /enabletrusteddevices “user:WIN-A1BCDE23FGH\admin;user:DESKTOP-A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators”

Para más información, por favor visite Dispositivos de confianza

---

Deshabilitar todos los dispositivos de confianza: /disabletrusteddevices

Sintaxis:

TSplus-Security.exe /disabletrusteddevices [Usuario o Grupos]

Descripción:

Comando /disabletrusteddevices se utiliza para deshabilitar todos los dispositivos de confianza

configurados para los usuarios y grupos especificados.

Parámetros:

- User or Groups El argumento es una lista de usuarios y grupos (separados por punto y coma). Dentro del nombre de usuario, la separación entre el tipo de usuario (“usuario” y “grupo” son los únicos valores aceptados) y el nombre de usuario completo se realiza mediante dos puntos.

Ejemplos:

TSplus-Security.exe /disabletrusteddevices “user:WIN-A1BCDE23FGH\admin;user:DESKTOP-A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators”

Para más información, por favor visite Dispositivos de confianza

---

Configurar el controlador de protección contra ransomware: /setup-driver

Sintaxis:

TSplus-Security.exe /setup-driver

Descripción:

Comando /setup-driver instala el controlador de protección contra ransomware. Esta operación normalmente se realiza durante la instalación.

Ejemplos:

TSplus-Security.exe /setup-driver

Para más información, por favor visite Protección contra ransomware

---

Desinstalar el controlador de protección contra ransomware: /uninstalldriver

Sintaxis:

TSplus-Security.exe /desinstalarcontrolador

Descripción:

Comando /uninstalldriver desinstalar el controlador de protección contra ransomware. Esta operación normalmente se realiza durante la desinstalación de Advanced Security.

Ejemplos:

TSplus-Security.exe /desinstalarcontrolador

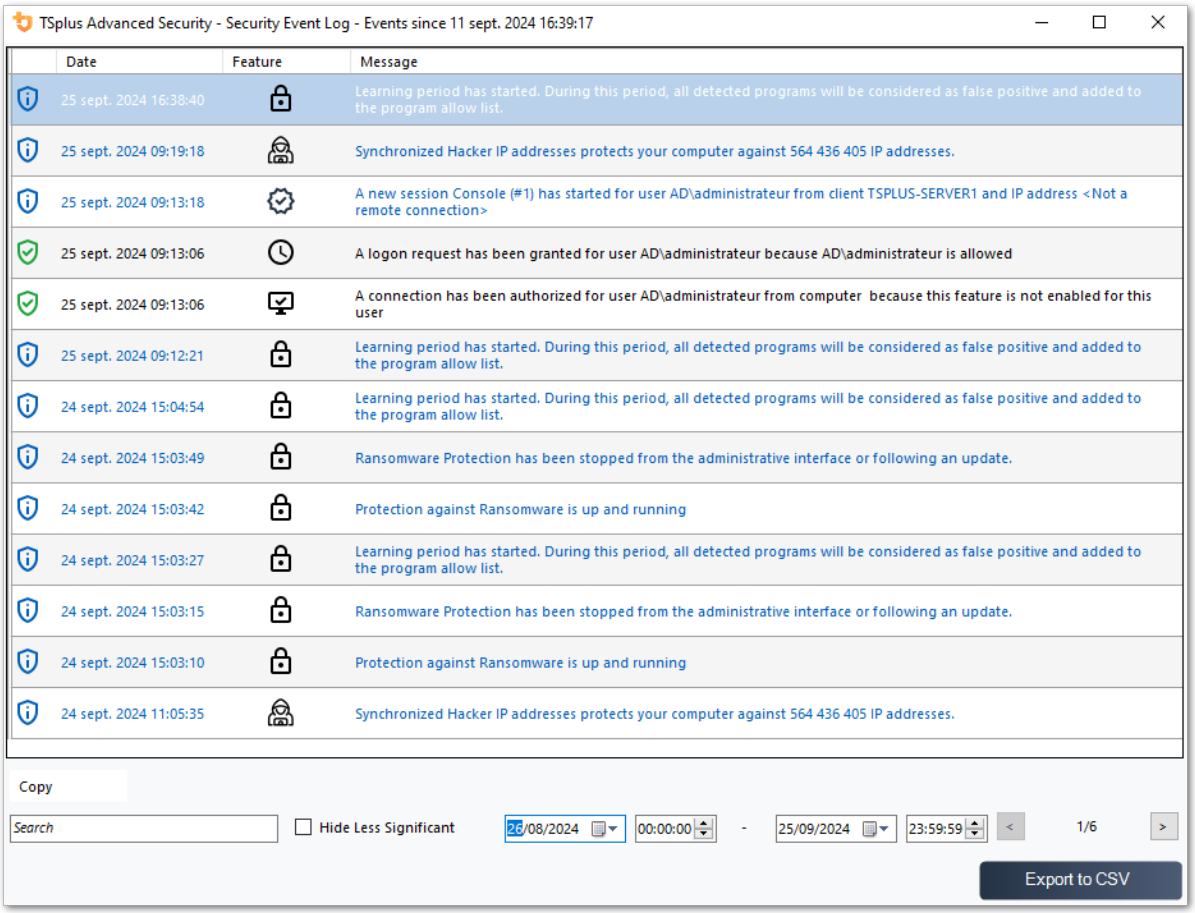
Para más información, por favor visite Protección contra ransomware

Eventos

Los eventos de seguridad son una gran fuente de información, ya que muestran las operaciones realizadas por TSplus Advanced Security para proteger su computadora.

La ventana de Eventos se puede abrir desde la ventana principal de TSplus Advanced Security, haciendo clic directamente en los últimos 5 eventos mostrados o en la pestaña del tablero. La información mostrada en la ventana de Eventos se actualiza automáticamente cada pocos segundos.

La lista de eventos de seguridad presenta 4 columnas, que describen la gravedad, la fecha de la verificación u operación realizada, el ícono de la función asociada y la descripción.



La descripción del evento a menudo explica por qué se realizó o no la acción. Las acciones de

represalia a menudo se escriben en rojo y se destacan con un ícono de escudo rojo.

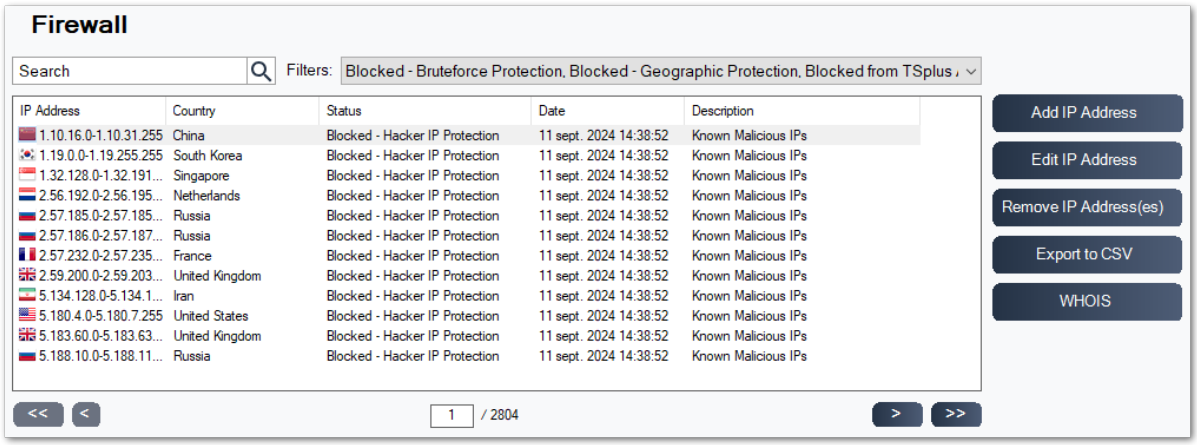
La ventana de eventos se puede mover y no impide que utilices la otra función de TSplus Advanced Security.

Navegando y buscando a través de eventos

- Una búsqueda global profunda ya está disponible para encontrar eventos específicos rápidamente.
- Junto a la búsqueda global, 2 filtros de selección de fecha y hora filtran los eventos mostrados de acuerdo con la fecha en que se generó el evento.
- A la derecha, las flechas permiten cambiar de página y navegar para ver eventos anteriores.

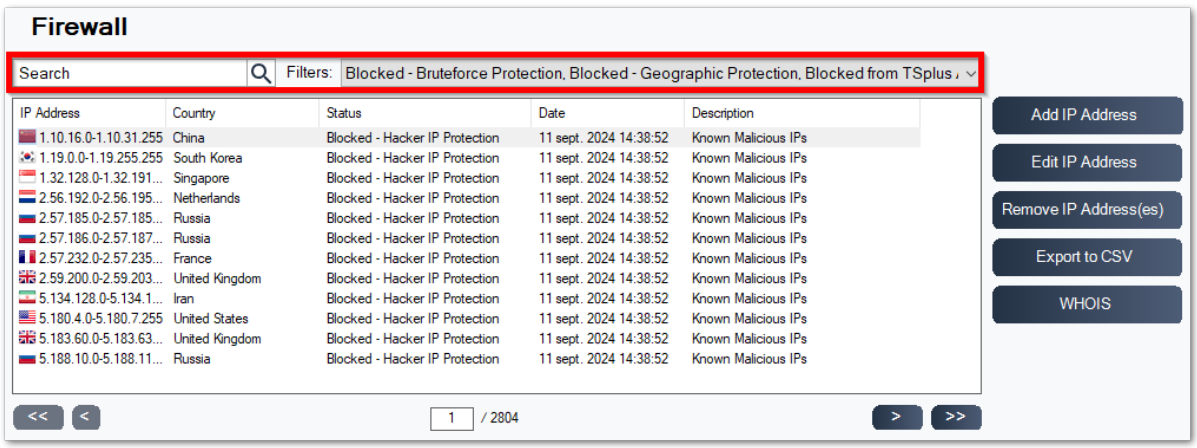
Cortafuegos

La gestión de direcciones IP es fácil con una sola lista para gestionar tanto las direcciones IP bloqueadas como las permitidas:



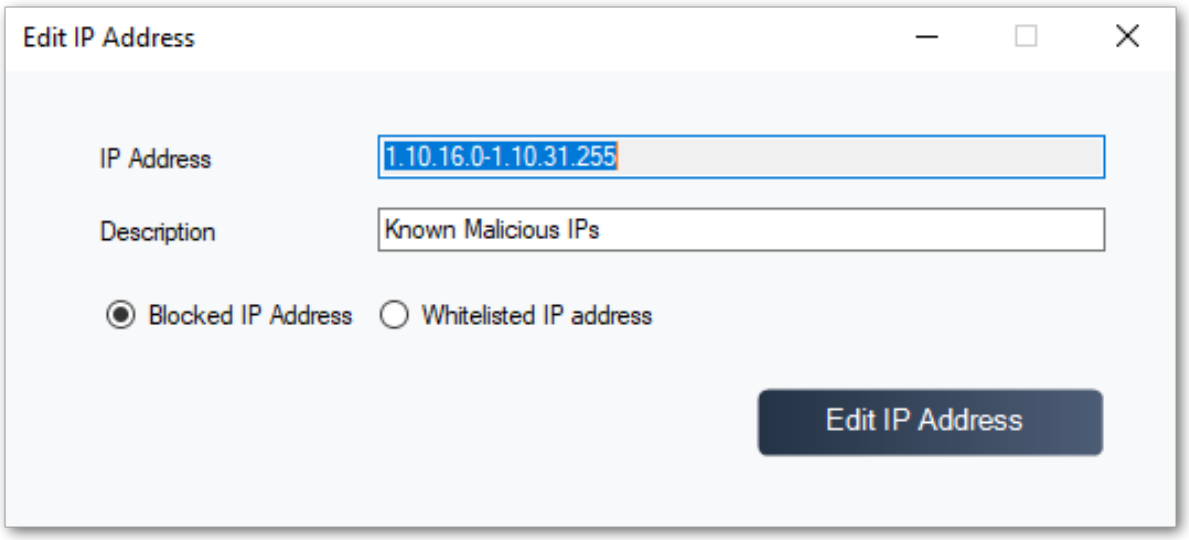
Por defecto, las direcciones IPV4, IPV6 y todas las direcciones de localhost del servidor están en la lista blanca.

Una barra de búsqueda y un filtro convenientes ofrecen capacidades de búsqueda basadas en toda la información proporcionada.



Además, los administradores pueden realizar acciones en varias direcciones IP seleccionadas

con un solo clic. Entre las nuevas funciones introducidas en la gestión de direcciones IP, encontrará la posibilidad de proporcionar descripciones significativas a cualquier dirección IP.



Por último, los administradores ahora pueden desbloquear y agregar a la lista blanca múltiples direcciones IP bloqueadas en una sola acción, haciendo clic en la pestaña "Agregar existente a la lista blanca".

Usando la línea de comandos para permitir o bloquear direcciones IP y/o rangos de IP

- Para poder **whitelist** Direcciones IP o rango(s) de IP, el comando tiene esta sintaxis :

TSplus-Security.exe addwhitelistedip [direcciones IP] [descripción opcional]

Puede agregar varias direcciones IP a la lista blanca, con un **coma o delimitador de punto y coma** Además, puedes especificar rangos de direcciones IP, en lugar de direcciones IP simples. La sintaxis es: **x.x.x.x-y.y.y.y** Finalmente, puede indicar una descripción opcional de la regla de la lista blanca.

Aquí hay un ejemplo de un comando completo: TSplus-Security.exe addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Los lugares de trabajo de John”

- Para poder **bloque** Direcciones IP o rango(s) de IP, el comando tiene una sintaxis similar:

TSplus-Security.exe bloquear IPs [direcciones IP] [descripción opcional]

- Para poder **desbloquear** Direcciones IP o rango(s) de IP, el comando tiene una sintaxis similar:

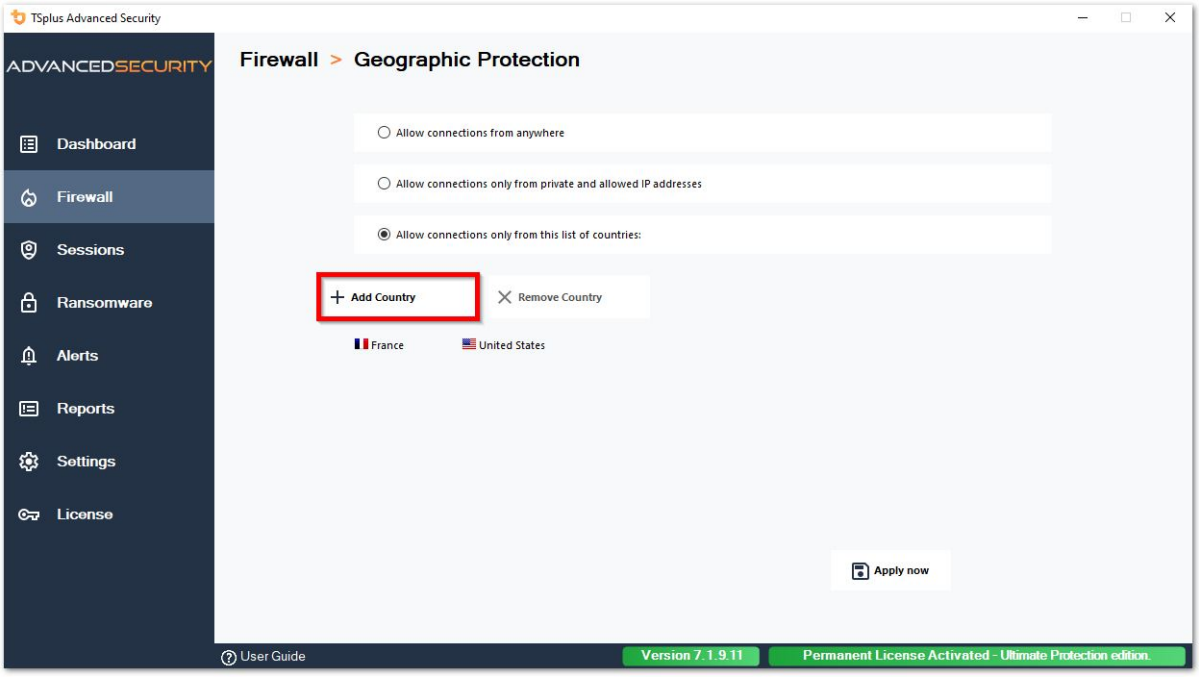
TSplus-Security.exe desbloquearips [direcciones IP]

Este comando no tiene efecto en las direcciones IP que ya están bloqueadas por la protección de IP de Hacker. Si aún desea desbloquear una de estas direcciones, utilice el comando de lista blanca.

Protección Geográfica

Restringir el acceso desde otros países

Para permitir el acceso remoto solo desde países específicos, seleccione el botón “Permitir conexiones solo desde esta lista de países” y luego haga clic en el botón “Agregar país”.

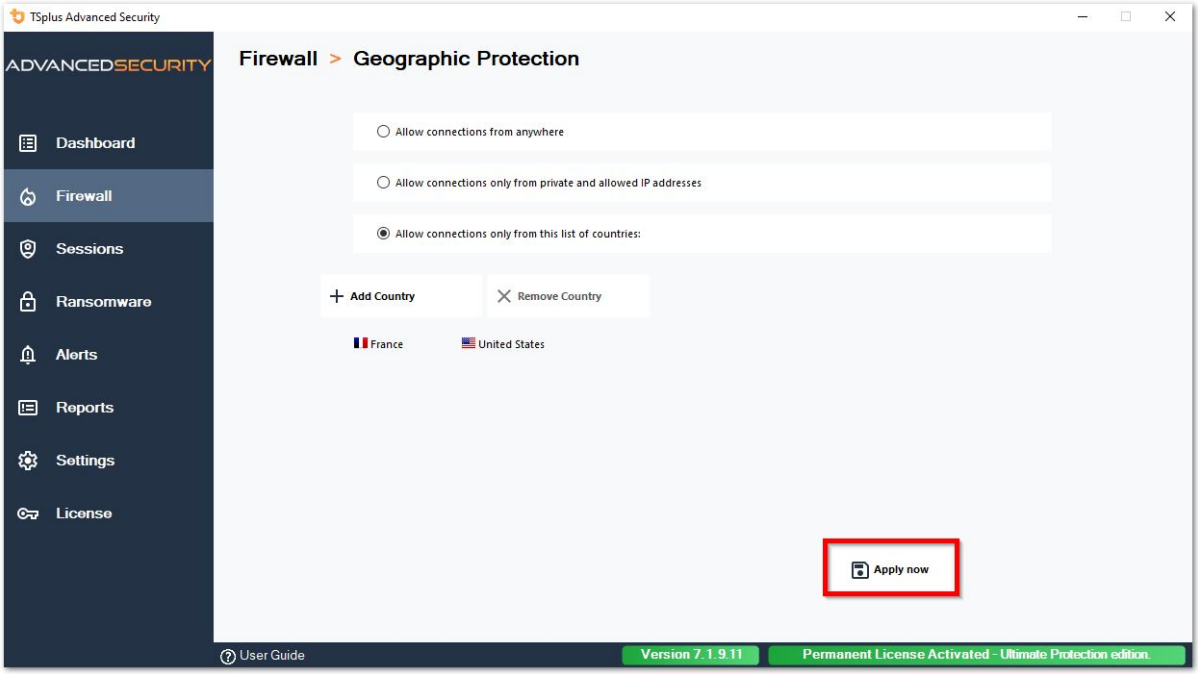


Se abre un popup que ofrece una lista de países. Seleccione el país que desea agregar a la lista.

Puedes elegir marcar la casilla a continuación para desbloquear todas las direcciones IP que fueron bloqueadas anteriormente para el país seleccionado.

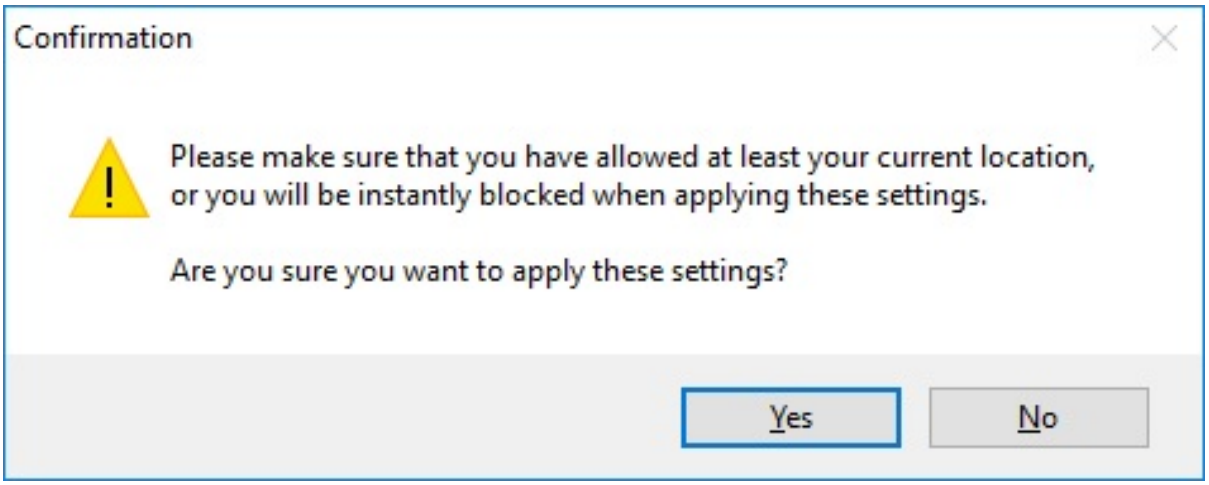
Haga clic en el botón "Agregar país" para volver a la pantalla principal de la función.

Importante: Para guardar sus cambios, haga clic en el botón “Aplicar”.



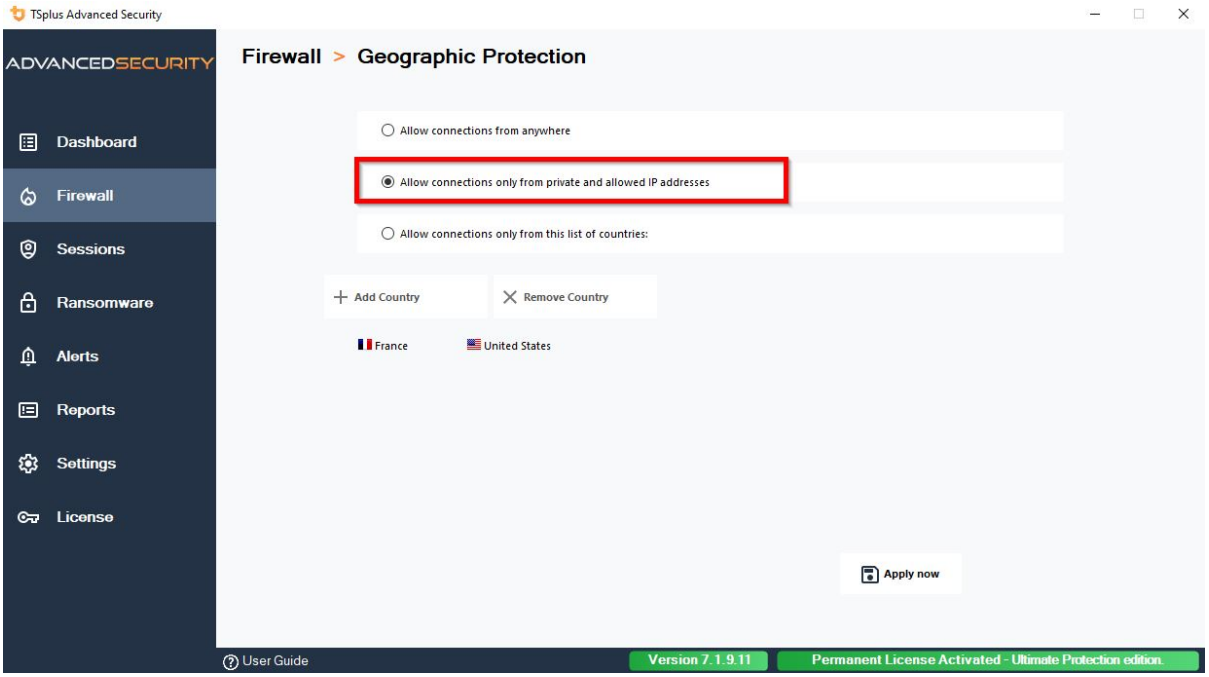
En este ejemplo, se permite el acceso remoto para los usuarios que se conectan desde Estados Unidos y Francia.

Aparece un mensaje de confirmación para evitar bloquear al usuario conectado. Haga clic en "Sí" para confirmar y aplicar los cambios.



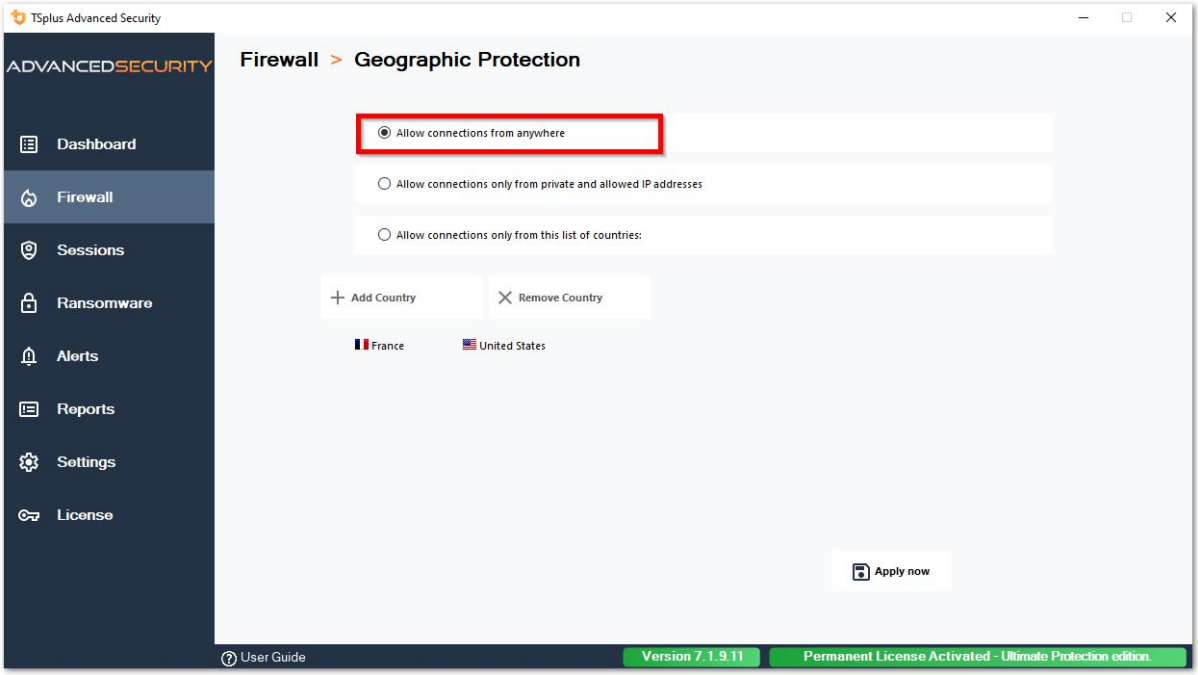
Restringir el acceso desde Internet

La Protección Geográfica se puede configurar para restringir el acceso a su máquina solo a direcciones privadas y direcciones IP en la lista blanca , como se muestra a continuación:



Desactivar la Protección Geográfica

Por defecto, la Protección Geográfica permite el acceso a los usuarios que se conectan desde todo el mundo:



Desbloqueo de direcciones IP bloqueadas

Cuando una dirección IP es bloqueada, aparece en el Pestaña de firewall Las direcciones IP bloqueadas pueden ser desbloqueadas y eventualmente añadidas a la lista de direcciones IP permitidas.

Si te bloquean, te recomendamos que intentes conectarte desde cualquier país que hayas permitido en TSplus Advanced Security, por ejemplo, conectándote desde otro servidor remoto o utilizando un servicio VPN. También puedes usar una sesión de consola para conectarte, ya que esta sesión no es una sesión remota y no será bloqueada por TSplus Advanced Security.

Importante:

- Verifique que ha seleccionado el país desde el que está conectado actualmente. De lo contrario, su dirección IP será bloqueada rápidamente después de aplicar la configuración, desconectándolo sin ninguna esperanza de volver a conectarse desde la misma dirección IP.
- Considere agregar su propia dirección IP a la lista de permitidos. Direcciones IP para evitar ser bloqueado por la Protección Geográfica o Protección contra ataques de fuerza bruta características.

Entendiendo la Protección Geográfica

La Protección Geográfica verifica las conexiones de red TCP entrantes, tanto IPv4 como IPV6

(excepto cuando se configura el modo de API de Windows heredado).

Procesos: La Protección Geográfica escucha las conexiones enviadas al servidor web de TSplus Remote Access de forma predeterminada, si está instalado. El nombre del proceso correspondiente es HTML5 Service. Si desea desactivar su monitoreo o verificar las conexiones destinadas a otros procesos, vaya a Configuración > Avanzado > Protección Geográfica .

Puertos de red: por defecto, Geographic Protection escucha los puertos predeterminados utilizados para conectarse de forma remota a un servidor. Estos puertos incluyen RDP (3389), Telnet (23) y VNC. Geographic Protection es compatible con los siguientes proveedores de VNC: Tight VNC, Ultra VNC, Tiger VNC y Real VNC, que no están relacionados de ninguna manera con TSplus. Si desea desactivar su monitoreo o verificar conexiones destinadas a otros puertos, vaya a Configuración > Avanzado > Protección Geográfica .

Mecanismos de detección:

La Protección Geográfica detecta conexiones entrantes de países no autorizados utilizando tres mecanismos de detección diferentes:

- API de Windows
- Seguimiento de eventos para Windows
- Cortafuegos Integrado

Por un lado, el seguimiento de eventos para Windows es una instalación de seguimiento a nivel de kernel eficiente que captura eventos de red en tiempo real. Se recomienda el seguimiento de eventos para Windows con el firewall de Windows habilitado (por defecto).

Por otro lado, la API de Windows funciona muy bien dada cualquier configuración de red específica, pero puede ejercer una presión constante en la CPU dependiendo de la cantidad de conexiones activas. Tenga en cuenta que la API de Windows aún no es compatible con IPv6.

El Firewall Integrado permite la captura y el bloqueo de paquetes de red enviados a la pila de red de Windows en modo de usuario. Cuando el Firewall Integrado está configurado para bloquear conexiones no deseadas, se recomienda utilizarlo para hacer cumplir los países permitidos de la Protección Geográfica.

Geolocalización: Advanced Security incluye datos de geolocalización publicados por MaxMind, disponibles en http://www.maxmind.com Si encuentra una dirección IP no registrada en su país actual, comuníquese directamente con MaxMind para solucionar el problema.

Solución de problemas

Si alguna vez notas que la Protección Geográfica no bloquea conexiones provenientes de un país que en realidad no está en la lista de países autorizados, es sin duda porque:

Antivirus: Para bloquear una dirección IP, la Protección Geográfica añade una regla de bloqueo en el firewall de Windows. Por lo tanto, primero, el firewall debe estar activo. También debes verificar si algunos parámetros del firewall no son gestionados por otro programa, como un antivirus. En este caso, tendrás que desactivar este programa y reiniciar el servicio "Firewall de Windows". También puedes contactar al editor de tu programa de terceros y pedirles que encuentren una manera para que su programa respete las reglas al ser añadido al firewall de Windows. Si conoces algún contacto técnico del editor de software, estamos listos para desarrollar estos "conectores" para el firewall. Contáctenos .

VPN: En caso de que el cliente remoto utilice una VPN, la Protección Geográfica obtendrá una dirección IP elegida por el proveedor de VPN. Como saben, los proveedores de VPN utilizan relés en todo el mundo para permitir que sus usuarios naveguen de forma anónima. Algunos proveedores de VPN permiten a los usuarios definir el país del relé. Así, los usuarios con proveedores de VPN pueden ser redirigidos a través de un país no autorizado. Por ejemplo, si un proveedor de VPN elige una IP de Sri Lanka, este país debe estar autorizado por la Protección Geográfica. Además, si la VPN utiliza una dirección IP corporativa interna, entonces la protección se vuelve irrelevante.

Firewall / Proxy: El propósito de un firewall de hardware es filtrar las conexiones entrantes y salientes para grandes empresas. Como solo es un filtro, no debería modificar la dirección IP de origen y, por lo tanto, no debería afectar la Protección Geográfica. Sin embargo, un proxy cambiaría definitivamente la dirección IP de origen para usar una dirección de red privada, que siempre será permitida por la Protección Geográfica. El propósito principal de esta función es bloquear el acceso a un servidor abierto a Internet. Si todas las conexiones provienen de la red corporativa, entonces la protección se vuelve irrelevante.

Protección de IP de Hacker

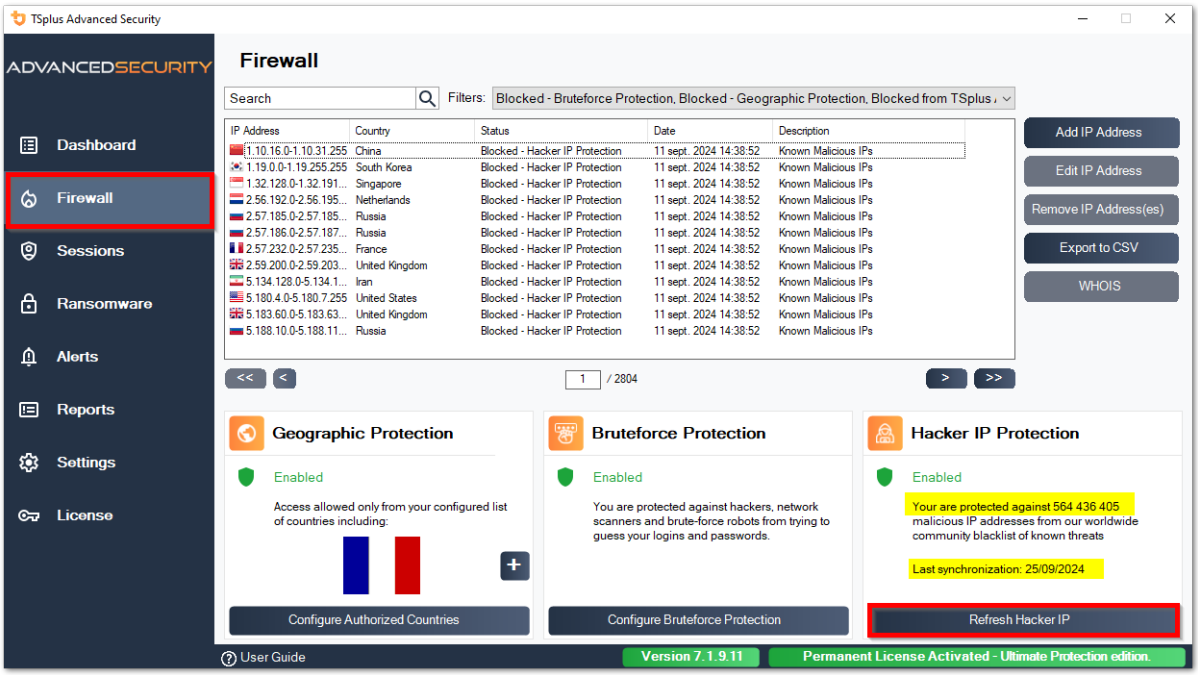
Mantenga su máquina protegida contra amenazas conocidas como ataques en línea, abuso de servicios en línea, malware, botnets y otras actividades de cibercrimen con la Protección de IP de Hacker. El objetivo es crear una lista negra que sea lo suficientemente segura para ser utilizada en todos los sistemas, con un firewall, para bloquear el acceso por completo, desde y hacia sus IPs listadas.

Se requiere una suscripción a los servicios de soporte y actualizaciones.

La clave para este objetivo es no tener falsos positivos. Todos los IPs listados deben ser malos y deben ser bloqueados, sin excepciones. Para lograr esto, la Protección de IP de Hacker aprovecha la información proporcionada por la comunidad de usuarios de Advanced Security.

La protección de IP de hackers se actualiza automáticamente todos los días.

Puedes actualizar manualmente desde la pestaña “Direcciones IP bloqueadas”, haciendo clic en el botón “Actualizar IP de hacker”:

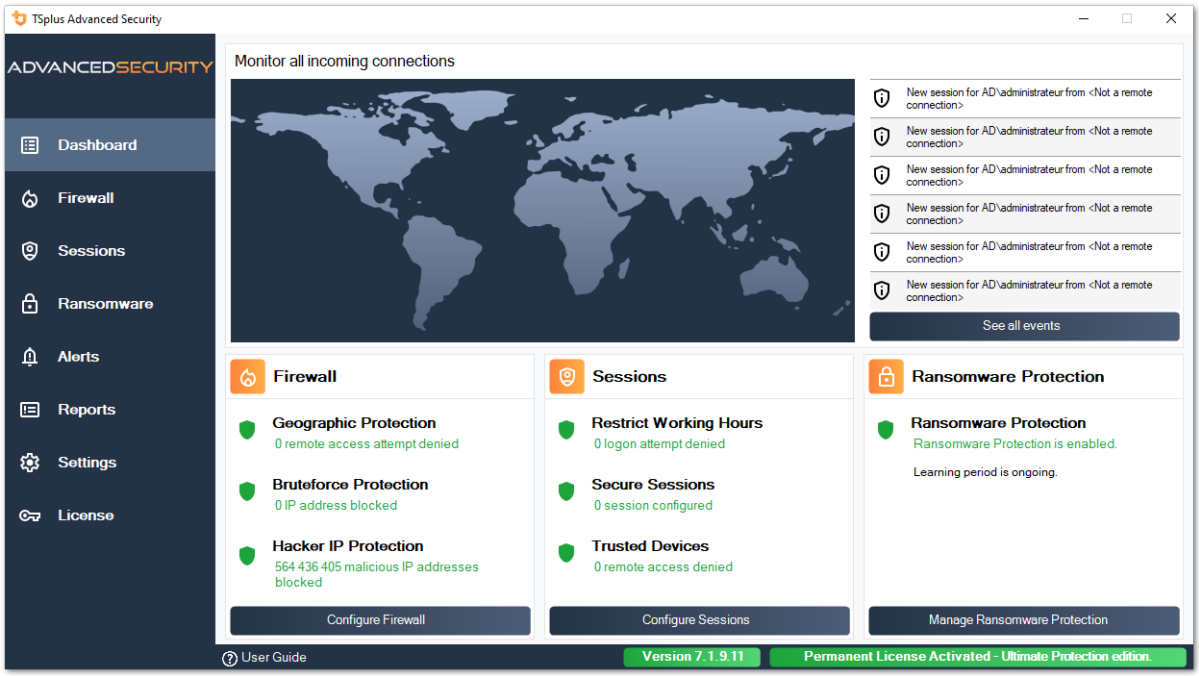


Como resultado, la función debería crear aproximadamente 600 000 000 reglas de firewall de

bloqueo en el Firewall de Windows.

Tablero

Haz clic en cada mosaico para saber más sobre cada función.



La barra de menú en la izquierda proporciona acceso a las diferentes funciones. Cada mosaico te da acceso a las diversas características y configuraciones ofrecidas por TSplus Advanced Security.

Advanced Security muestra los seis últimos Eventos de seguridad Haga clic en cualquier evento para abrir la lista completa de eventos en una ventana separada.

Debajo de los últimos eventos, tres mosaicos proporcionan acceso rápido a:

1. Cortafuegos

2. Sesiones

3.

Protección contra ransomware

Por favor, seleccione su idioma de visualización utilizando el menú desplegable ubicado en la esquina superior derecha, en caso de que la aplicación no haya detectado su idioma.

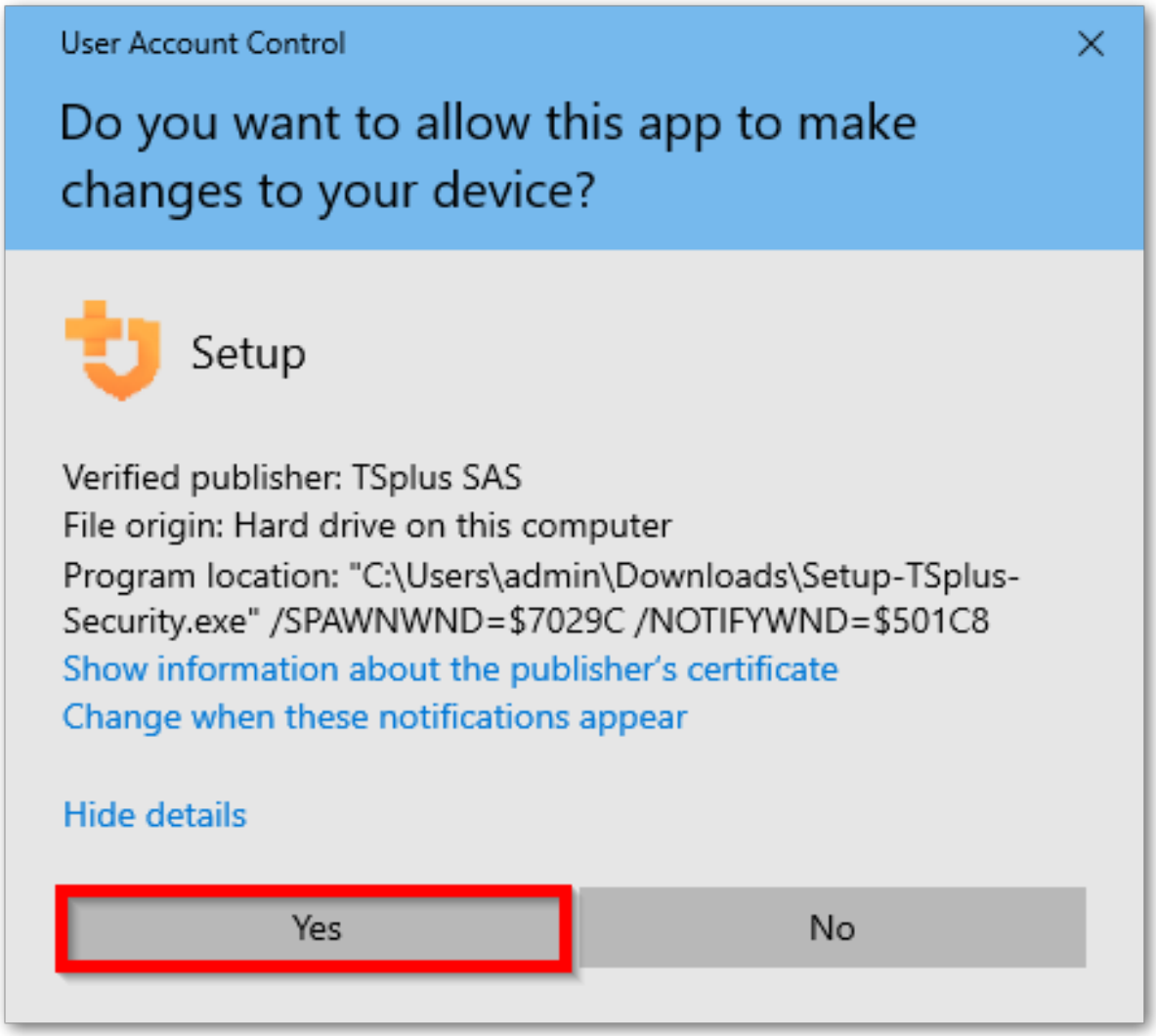
Finalmente, hacer clic en el botón "Ayuda" te redirigirá a esta documentación.

Instalando TSplus Advanced Security

Instalando Advanced Security

Ejecutar TSplus Advanced Security Setup program y luego **siga los pasos de instalación** .

Debes ejecutar el programa de instalación como Administrador y aceptar el acuerdo de licencia del software.



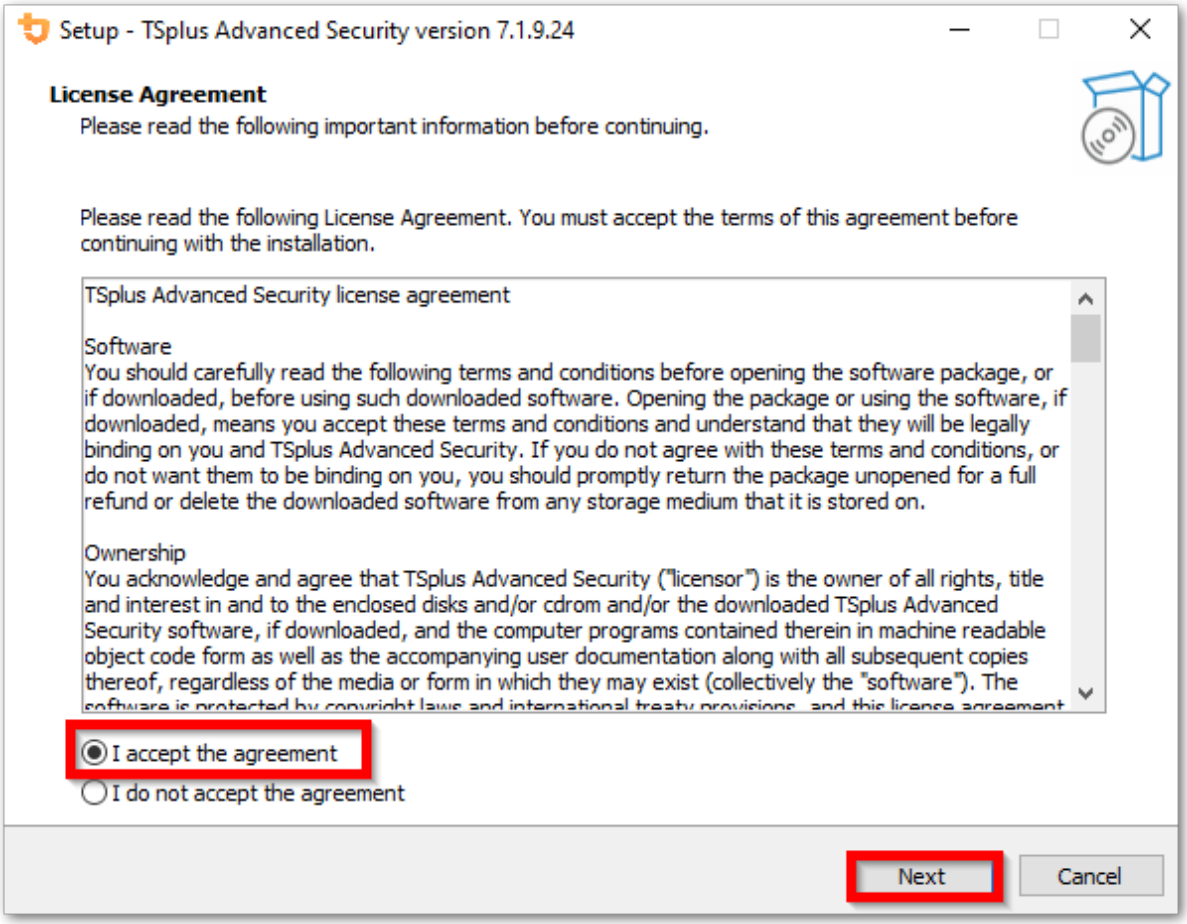
Seleccione el idioma del asistente de configuración si no se detecta automáticamente.

Luego, selecciona una de las dos opciones: **Recomendado** o **Avanzado** al hacer clic en las casillas correspondientes.

La opción Avanzada agrega pasos adicionales que te permiten:

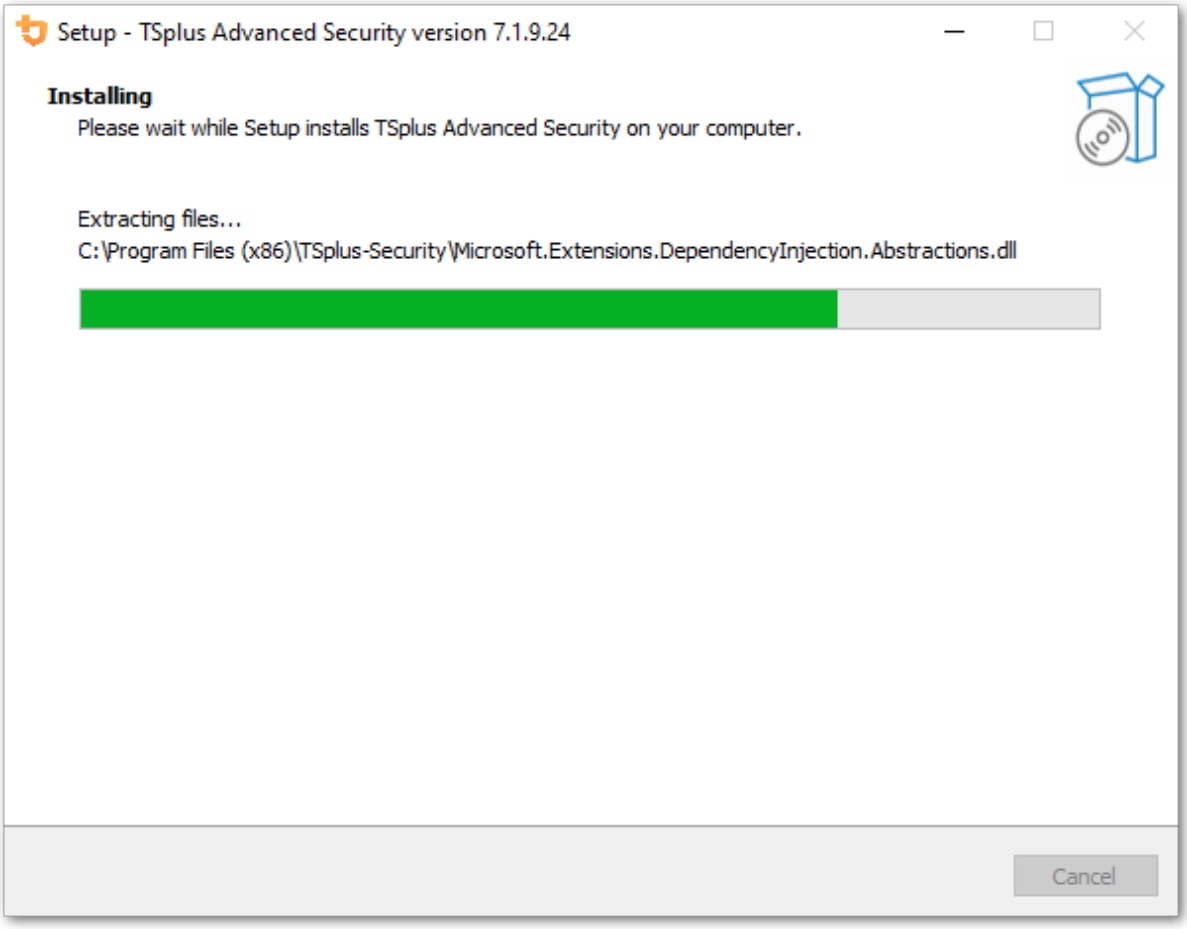
- Solo descarga la configuración (no instales)
- Usar configuraciones de proxy personalizadas

Lea el acuerdo de licencia y haga clic en "Acepto" para reanudar la instalación.



El programa se instalará en su computadora.

Se muestra una barra de progreso en la parte inferior que informa sobre el avance de la instalación.



Por favor, sea paciente , ya que a veces puede tardar hasta unos minutos en instalar completamente el software.

Una vez que se haya completado la instalación, ¡puede comenzar a usar TSplus Advanced Security!

La versión de prueba gratuita está completamente equipada durante 15 días. No olvides activar su licencia y a actualizar a la última versión para mantener la protección de Advanced Security en su mejor nivel!

Escenarios de instalación avanzada

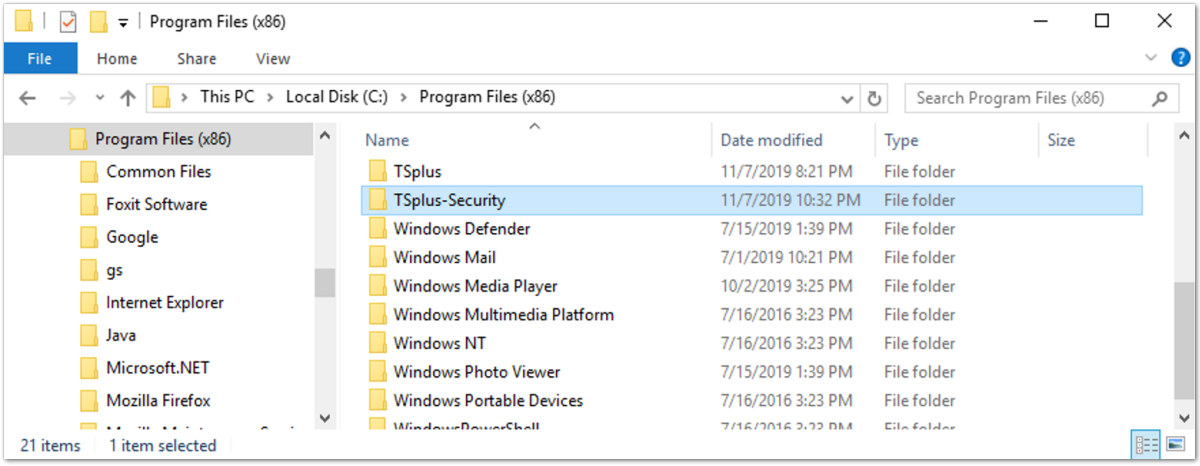
El TSplus Advanced Security Classic Setup program maneja los siguientes escenarios ya que se puede ejecutar desde la línea de comandos:

- Instalar en silencio, proporcionando los parámetros /VERYSILENT /SUPPRESSMSGBOXES
- Evite reiniciar al final de la configuración, proporcionando el parámetro /NORESTART. Este parámetro se utiliza generalmente junto con el anterior.
- Licenciamiento por volumen para activar su licencia directamente durante la instalación (consulte la documentación o contáctenos para más información

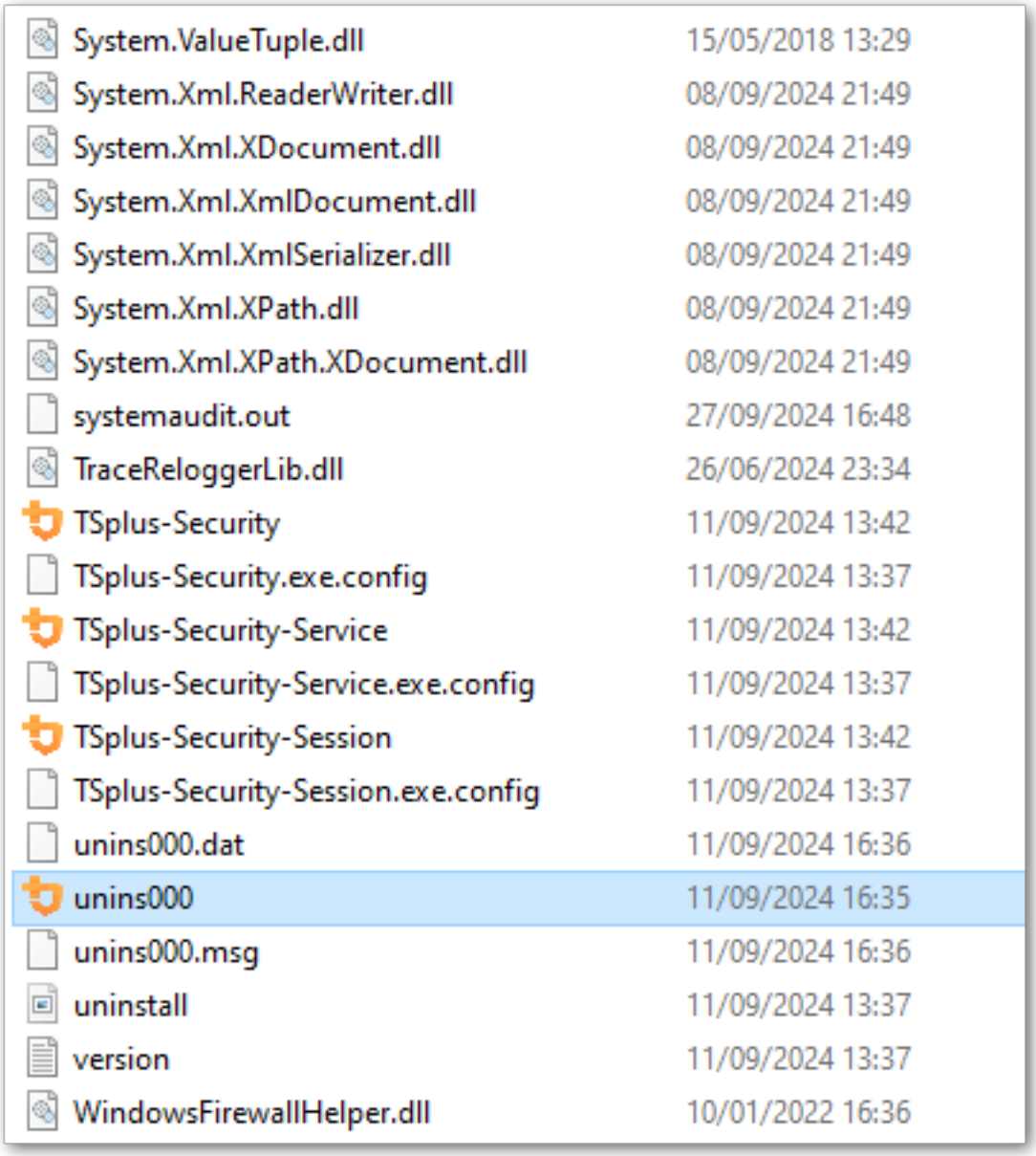
Desinstalar TSplus Advanced Security

Para desinstalar completamente TSplus Advanced Security, abre el directorio C:\Program Files

(x86)\TSplus-Security.



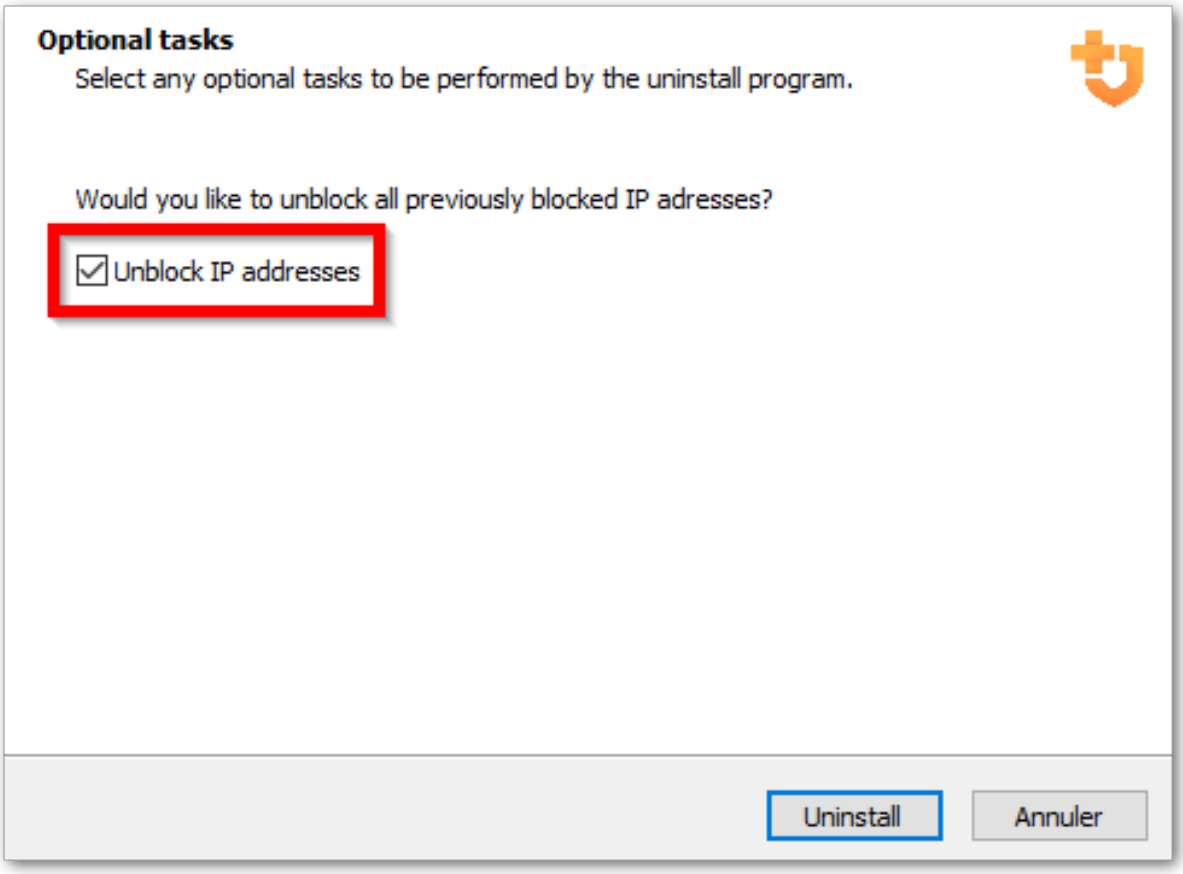
Luego, haz doble clic en la aplicación “unins000” para ejecutar el programa de desinstalación.



Haga clic en sí en la siguiente ventana para eliminar completamente TSplus Advanced Security y todos sus componentes.

A menos que se configure de otra manera, Advanced Security agrega reglas de bloqueo al Firewall de Windows. Haga clic en "Desbloquear direcciones IP" para desbloquear y eliminar todas las direcciones IP que fueron bloqueadas previamente por Advanced Security.

Importante: Por favor, tenga en cuenta que eliminar todas las reglas puede tardar hasta una hora. Debido a esto, le recomendamos que elimine las reglas directamente desde la consola de Firewall de Windows con Seguridad Avanzada.



El software se desinstalará completamente de su máquina.

Gestión de permisos

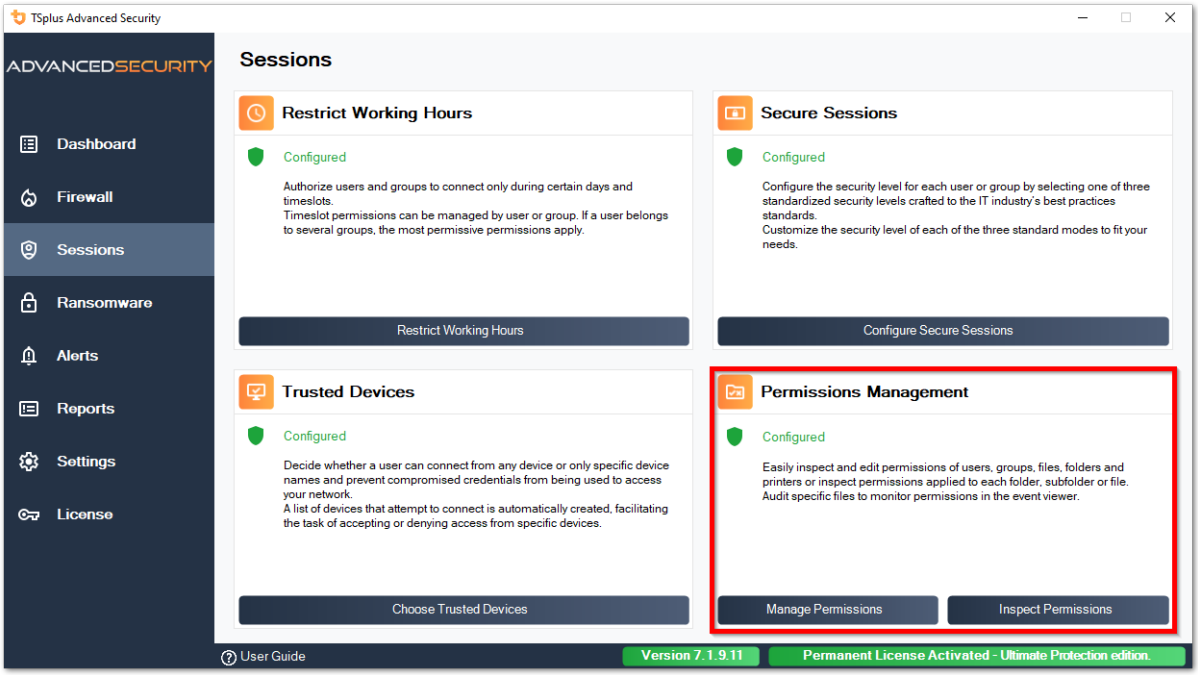
Desde la versión 4.3, TSplus Advanced Security ofrece una funcionalidad de Permisos, que permite al administrador gestionar y/o inspeccionar los privilegios de usuarios/grupos.

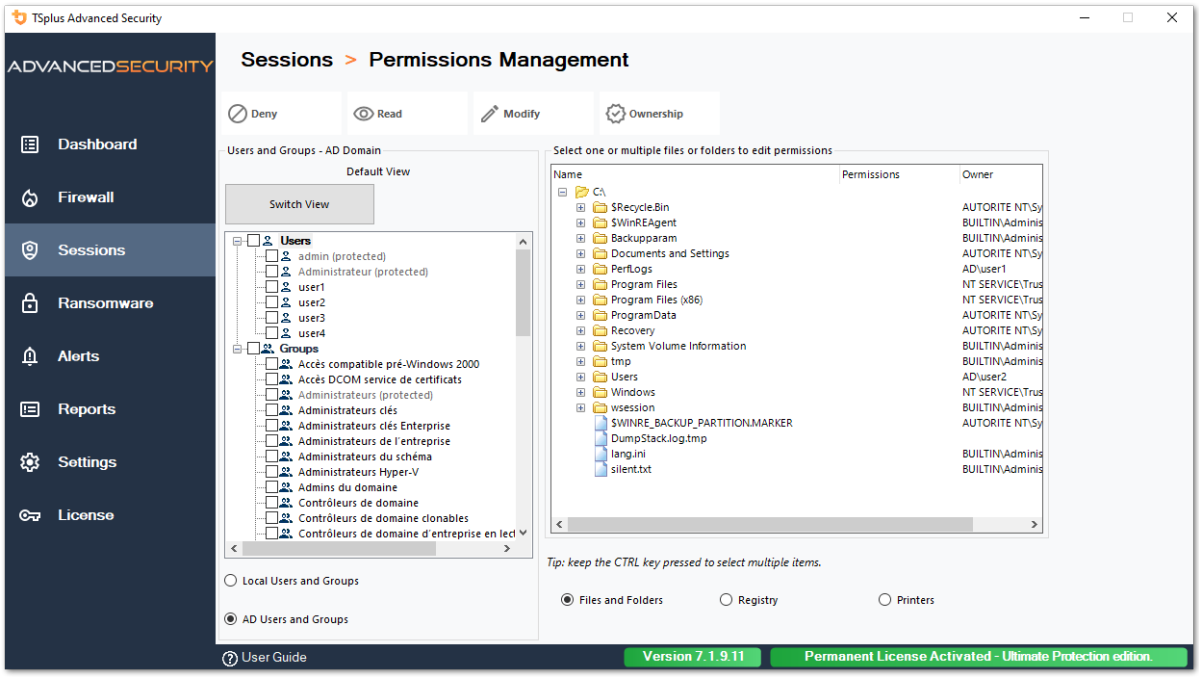
En el panel de permisos, la lista de usuarios y grupos y la lista de disponibles **archivos, carpetas, registros e impresoras** se muestran uno al lado del otro.

Todo es visible de un vistazo, lo que lo hace muy fácil de **Inspeccionar** y **Administrar/Editar** privilegios para un usuario a la vez y, por lo tanto, aumentar la precisión de las restricciones.

Administrar permisos

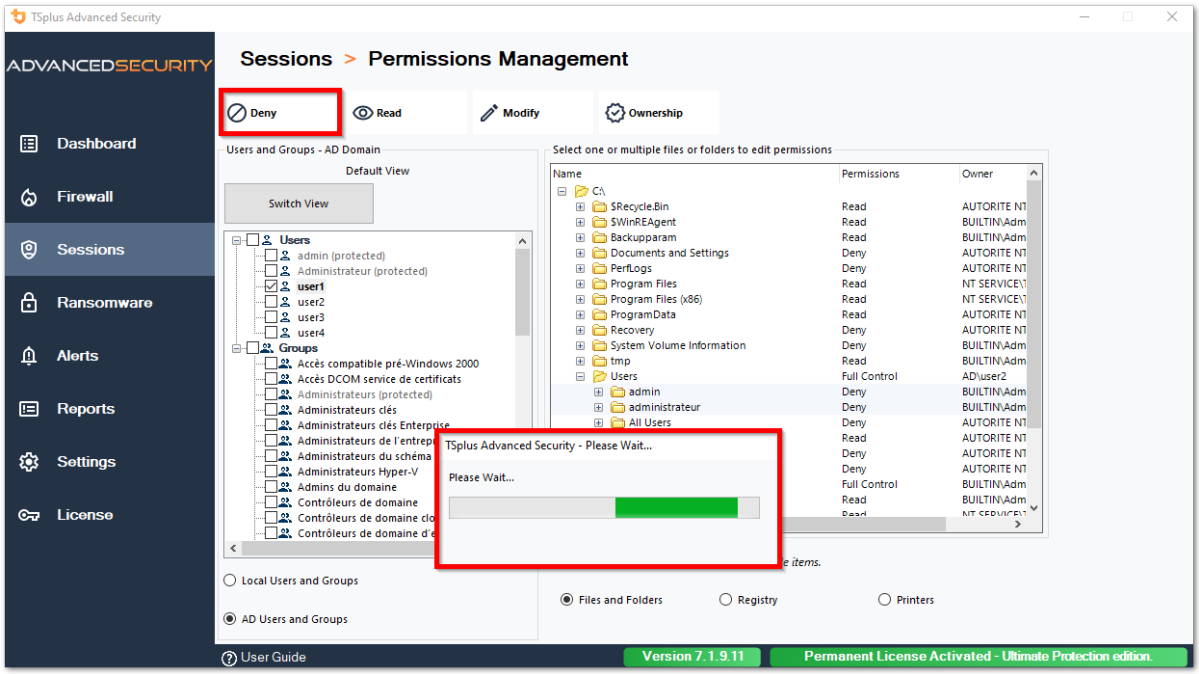
En la pestaña Administrar, para cada usuario o grupo seleccionado en la vista de árbol de la izquierda, puedes:



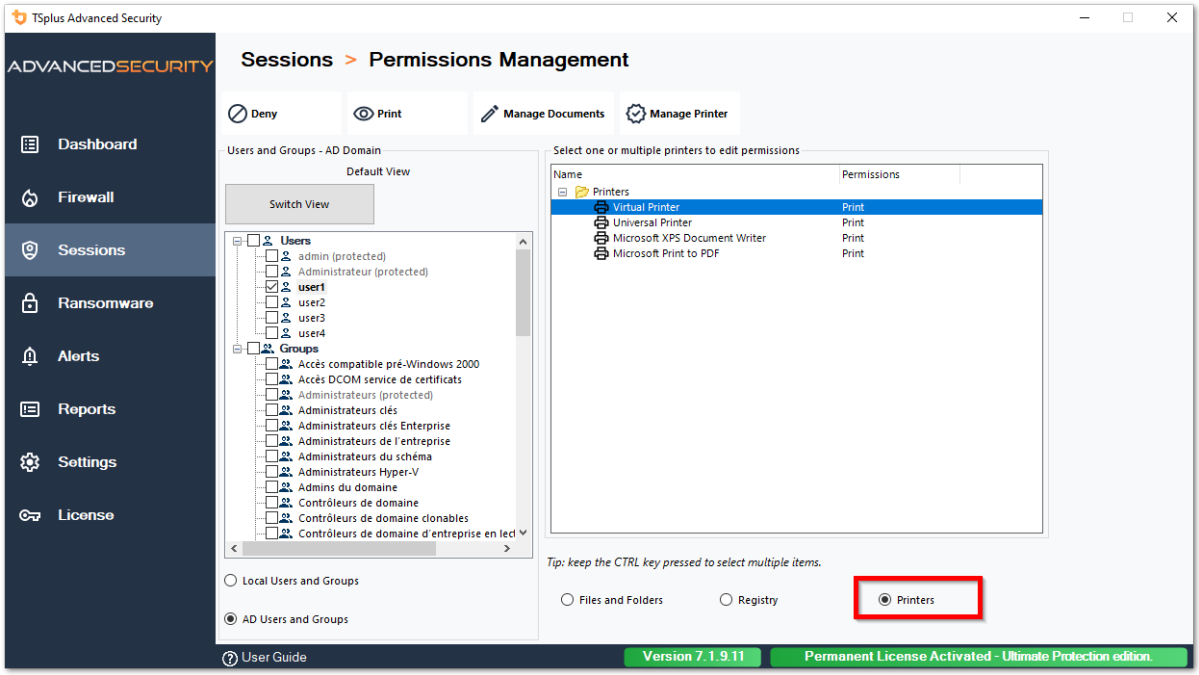


- **Denegar** Al hacer clic en el botón Denegar, al usuario seleccionado se le negará el privilegio sobre el objeto del sistema de archivos seleccionado. Si se selecciona un archivo, entonces al usuario seleccionado se le niega el privilegio de leer el archivo seleccionado (FileSystemRights.Read). Si se selecciona un directorio, entonces al usuario seleccionado se le niega el privilegio de leer y listar el contenido del directorio (FileSystemRights.Read y FileSystemRights.ListDirectory).
- **Leer** Al hacer clic en el botón Leer, se otorgará al usuario seleccionado privilegios sobre el objeto del sistema de archivos seleccionado. Si se selecciona un archivo, se le otorga al usuario seleccionado el privilegio de leer el archivo seleccionado y ejecutarlo si el archivo es un programa (FileSystemRights.ReadAndExecute). Si se selecciona un directorio, se le otorga al usuario seleccionado el privilegio de leer y listar o ejecutar el contenido del directorio (FileSystemRights.ReadAndExecute y FileSystemRights.ListDirectory y FileSystemRights.Traverse).
- **Modificar** Al hacer clic en el botón Modificar, se otorgará al usuario seleccionado privilegios sobre el objeto del sistema de archivos seleccionado. Si se selecciona un archivo, se otorgará al usuario seleccionado el privilegio de modificar el archivo seleccionado (FileSystemRights.Modify). Si se selecciona un directorio, se otorgará al usuario seleccionado el privilegio de modificar y listar el contenido del directorio, así como crear nuevos archivos o directorios (FileSystemRights.Modify y FileSystemRights.CreateDirectories y FileSystemRights.CreateFiles y FileSystemRights.ListDirectory y FileSystemRights.Traverse).
- **Propiedad** Al hacer clic en el botón de Propiedad, el usuario seleccionado recibirá control total sobre el objeto del sistema de archivos seleccionado (FileSystemRights.FullControl).

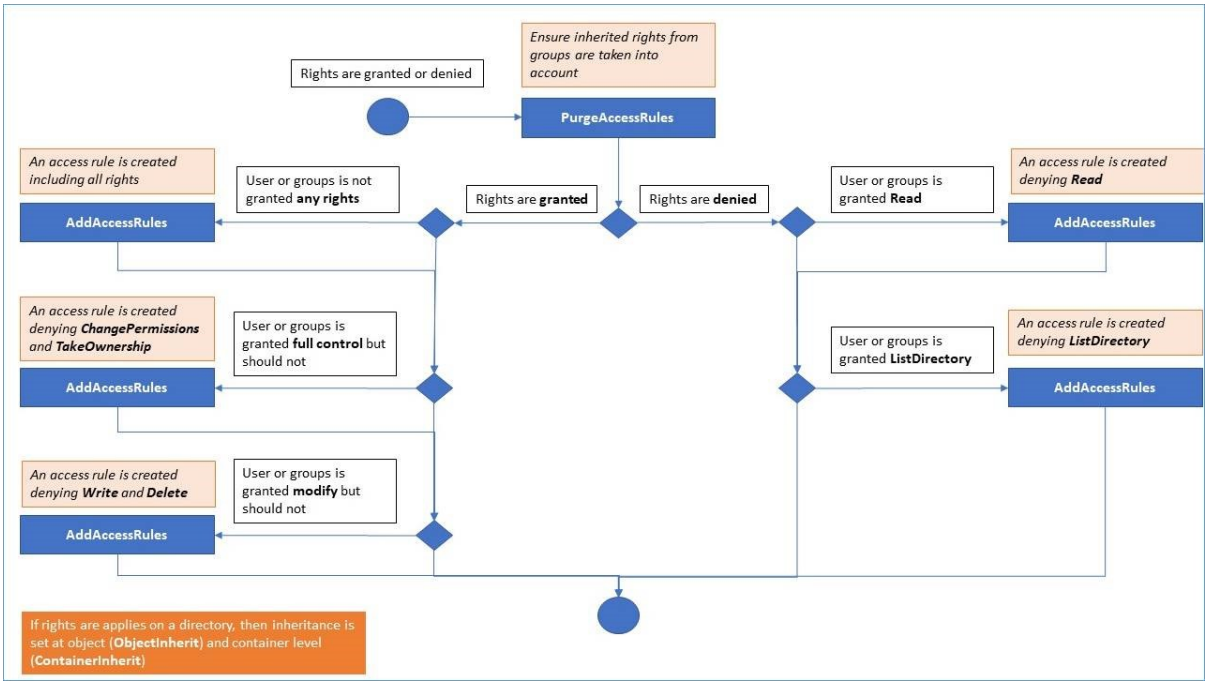
Las mismas opciones de permisos son posibles para cada Registro, seleccionando el botón correspondiente en la vista del árbol derecho:



Y para cada impresora:



Tenga en cuenta que todos los permisos denegados o concedidos a un directorio se aplican de forma recursiva a los objetos del sistema de archivos contenidos en este directorio. El diagrama a continuación detalla las llamadas a la API cuando se aplican derechos a un objeto del sistema de archivos.

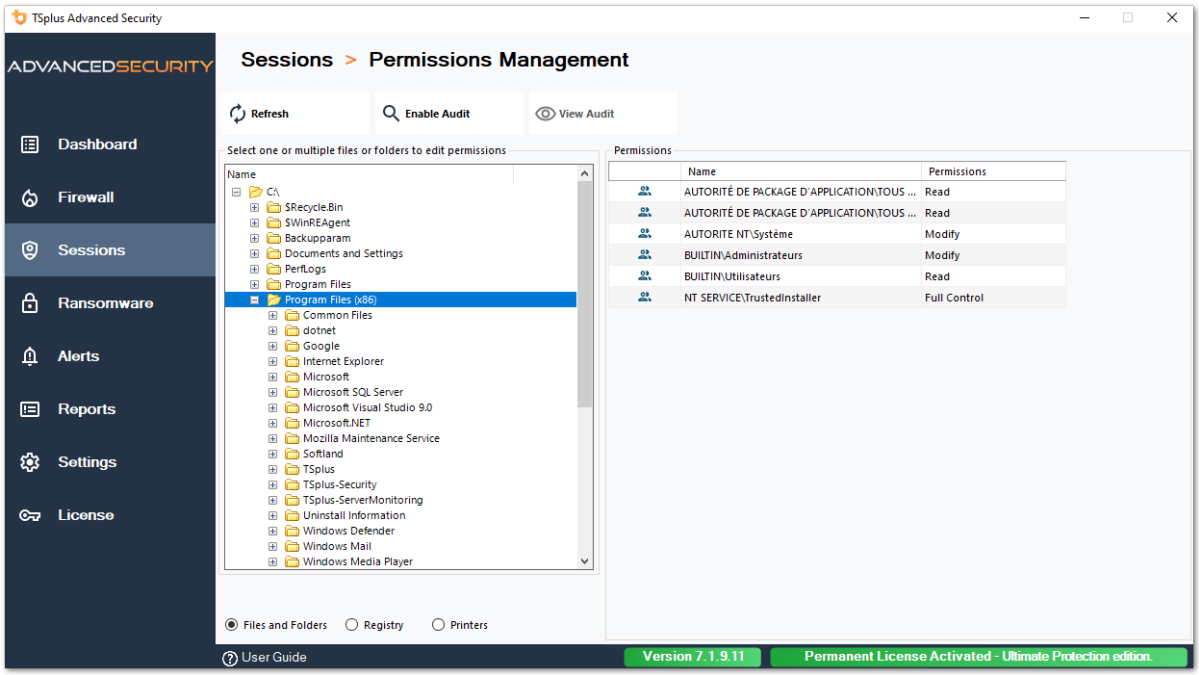


Documentación :

- Seguridad del Objeto: https://docs.microsoft.com/es-es/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- Derechos del sistema de archivos: https://docs.microsoft.com/es-es/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

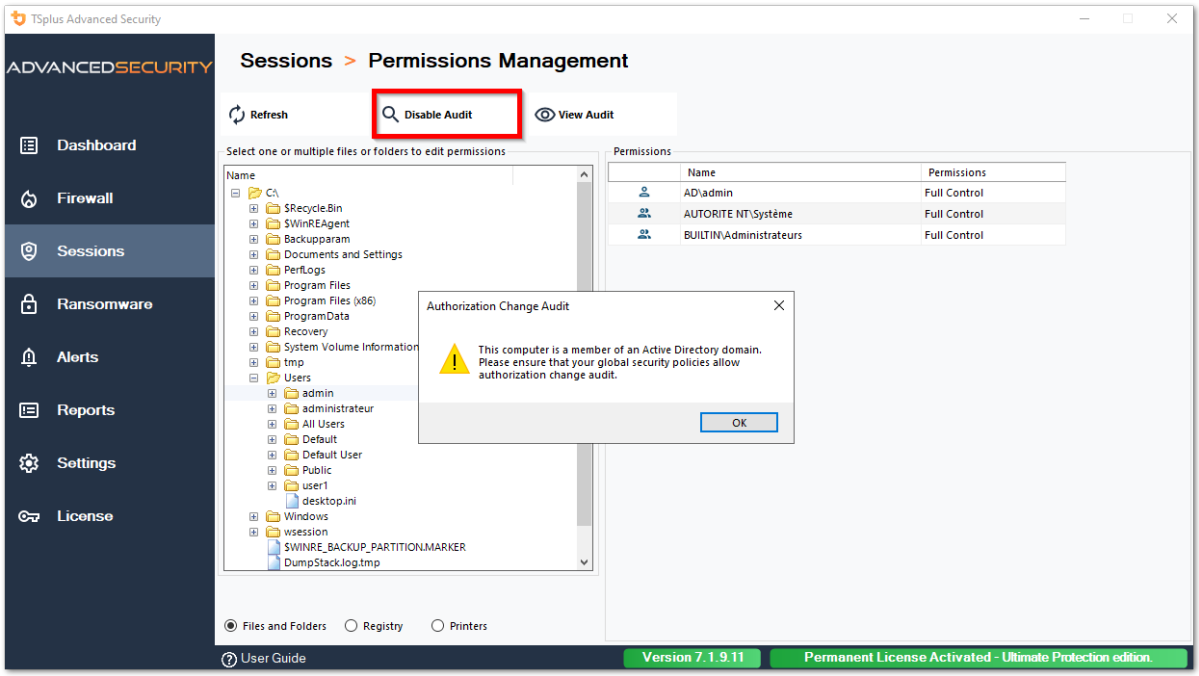
Inspeccionar permisos

En la pestaña Inspeccionar, para cada carpeta, subcarpeta o archivo seleccionado en la vista de árbol de la izquierda, puedes ver los permisos atribuidos correspondientes a usuarios o grupos en la vista de árbol de la derecha.

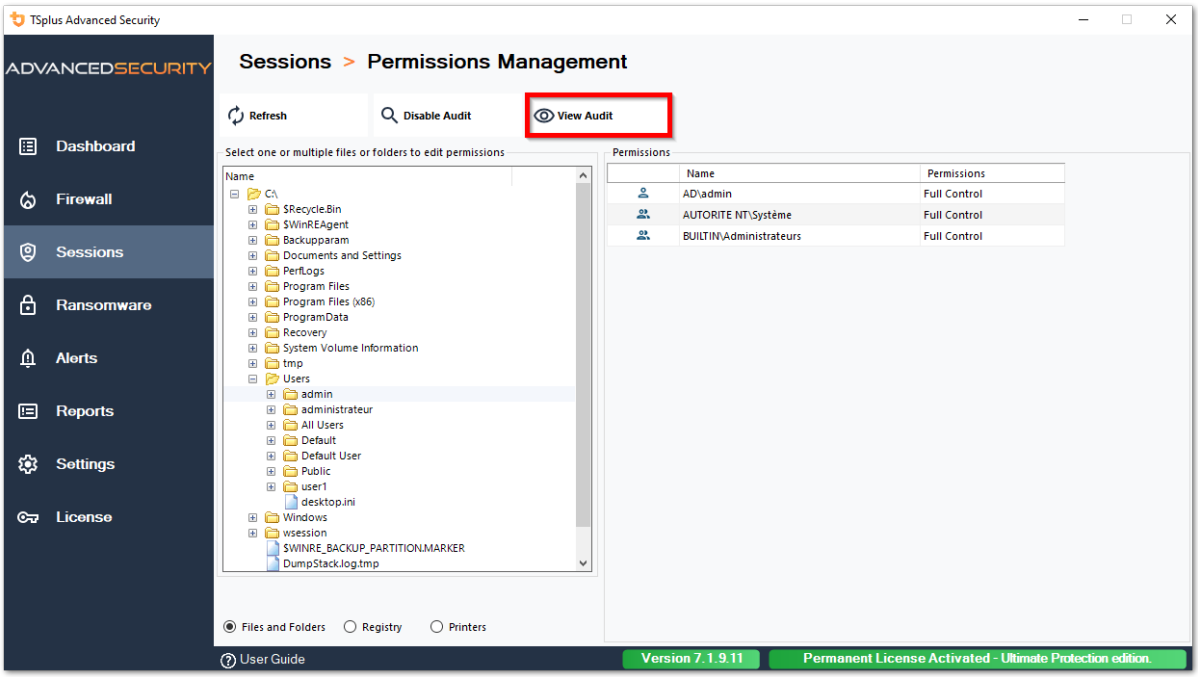


Puedes actualizar el estado de las carpetas para que se actualicen en tiempo real.

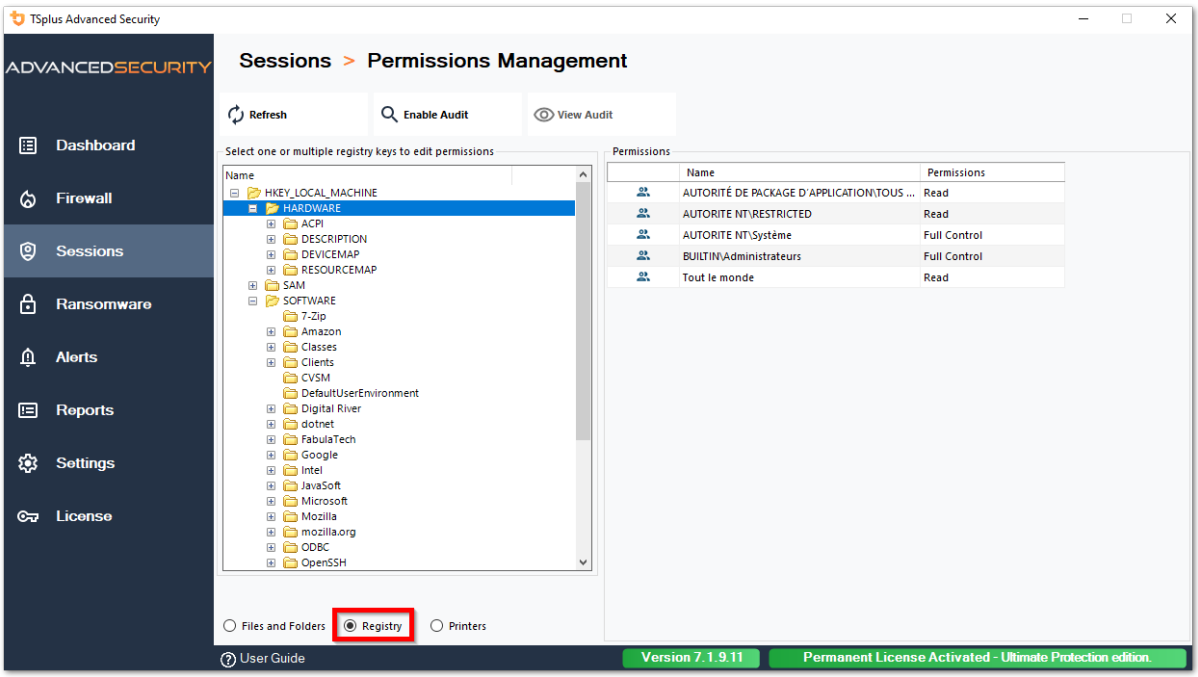
Se puede habilitar una auditoría seleccionando la carpeta, subcarpeta o archivo deseado y haciendo clic en el botón “Habilitar auditoría” en la parte superior:

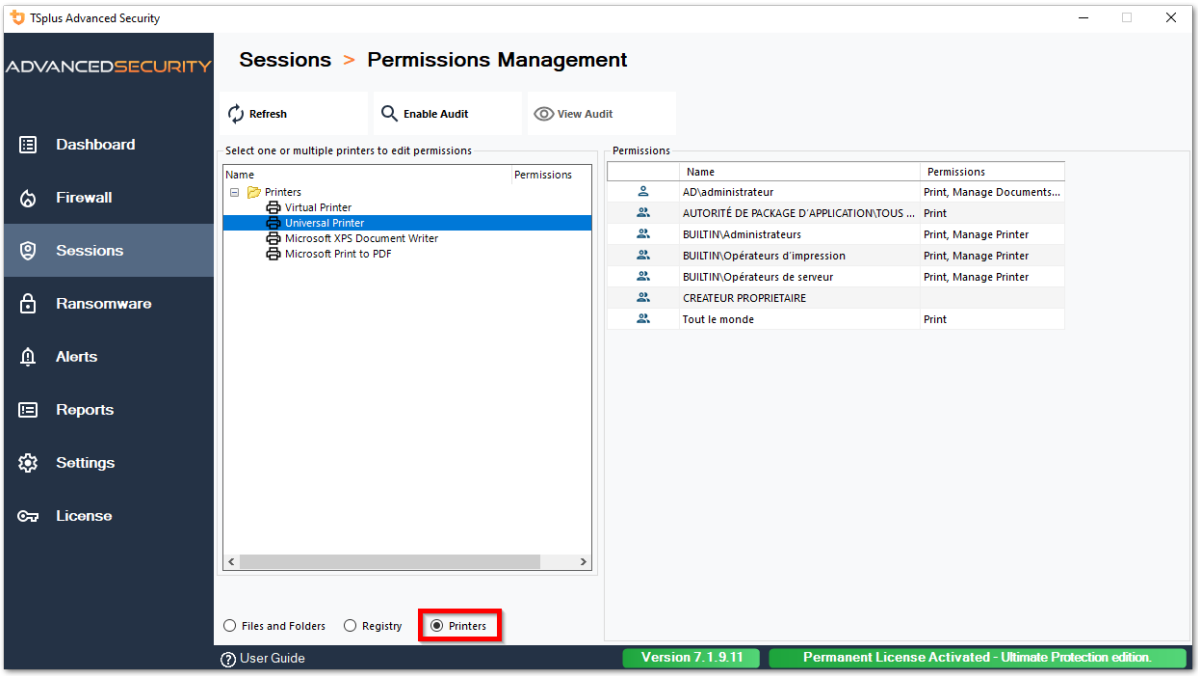


El botón "Ver auditoría" te permite ver la auditoría correspondiente en el Visor de eventos:



Las mismas posibilidades de inspección están disponibles para cada registro e impresora al seleccionar el botón correspondiente en la vista del árbol izquierdo:




TSplus Advanced Security
ADVANCEDSECURITY
Dashboard
Firewall
Sessions
Ransomware
Alerts
Reports
Settings
License
Sessions > Permissions Management
Refresh
Enable Audit
View Audit
Select one or multiple printers to edit permissions
Name
Permissions
Printers
Virtual Printer
Universal Printer
Microsoft XPS Document Writer
Microsoft Print to PDF
Permissions
Name
Permissions
AD\administrateur
Print, Manage Documents...
AUTORITÉ DE PACKAGE D'APPLICATION\TOUS ...
Print
BUILTIN\Administrateurs
Print, Manage Printer
BUILTIN\Opérateurs d'impression
Print, Manage Printer
BUILTIN\Opérateurs de serveur
Print, Manage Printer
CREATEUR PROPRIETAIRE
Tout le monde
Print
Files and Folders
Registry
Printers
User Guide
Version 7.1.9.11
Permanent License Activated - Ultimate Protection edition.

TSplus Advanced Security - Prerrequisitos

Requisitos de hardware

TSplus Advanced Security admite arquitecturas de 32 bits y 64 bits.

Sistema Operativo

Su hardware debe utilizar uno de los sistemas operativos a continuación:

- Windows **7 Pro**
- Windows **8/8.1 Pro**
- Windows **10 Pro**
- Windows **11 Pro**
- Windows **Server 2008 SP2/Small Business Server SP2 o 2008 R2 SP1**
- Windows **Server 2012 o 2012 R2**
- Windows **Server 2016**
- Windows **Servidor 2019**
- Windows **Server 2022**
- Windows **Servidor 2025**

Ambas arquitecturas de 32 y 64 bits son compatibles.

Requisitos del software

TSplus Advanced Security requiere los siguientes requisitos previos:

- Tiempo de ejecución: .NET Framework 4.7.2 o superior
- Microsoft Windows 7 SP1 y Windows 2008 R2 SP1 requieren una actualización adicional para soportar la firma cruzada SHA2 (KB4474419 Esta actualización permite que el firewall integrado de TSplus Advanced Security y la protección contra ransomware funcionen correctamente.

Nota: Estos requisitos se instalarán automáticamente mediante el programa de instalación si faltan en el sistema.

TSplus Advanced Security - Introducción

Requisitos

TSplus Advanced Security requiere los siguientes requisitos previos.

- Sistema operativo: Microsoft Windows versión 7, Service Pack 1 (compilación 6.1.7601) o Windows 2008 R2, Service Pack 1 (compilación 6.1.7601) o superior.

Lo siguiente **los requisitos se instalarán automáticamente mediante el programa de instalación** si falta:

- Tiempo de ejecución: .NET Framework 4.5.3 o superior

- Microsoft Windows 7 SP1 y Windows 2008 R2 SP1 requieren una actualización adicional para soportar la firma cruzada SHA2 (KB4474419 Esta actualización permite que el firewall integrado de TSplus Advanced Security y la protección contra ransomware funcionen correctamente.

Por favor, consulte el documentación para más detalles sobre los requisitos previos.

Paso 1: Instalación

El último programa de instalación de TSplus Advanced Security siempre está disponible aquí: Último programa de instalación de TSplus Advanced Security Por favor, descargue el programa de instalación y siga el asistente de configuración.

TSplus Advanced Security setup programe no suele requerir reiniciar su sistema para completar la instalación.

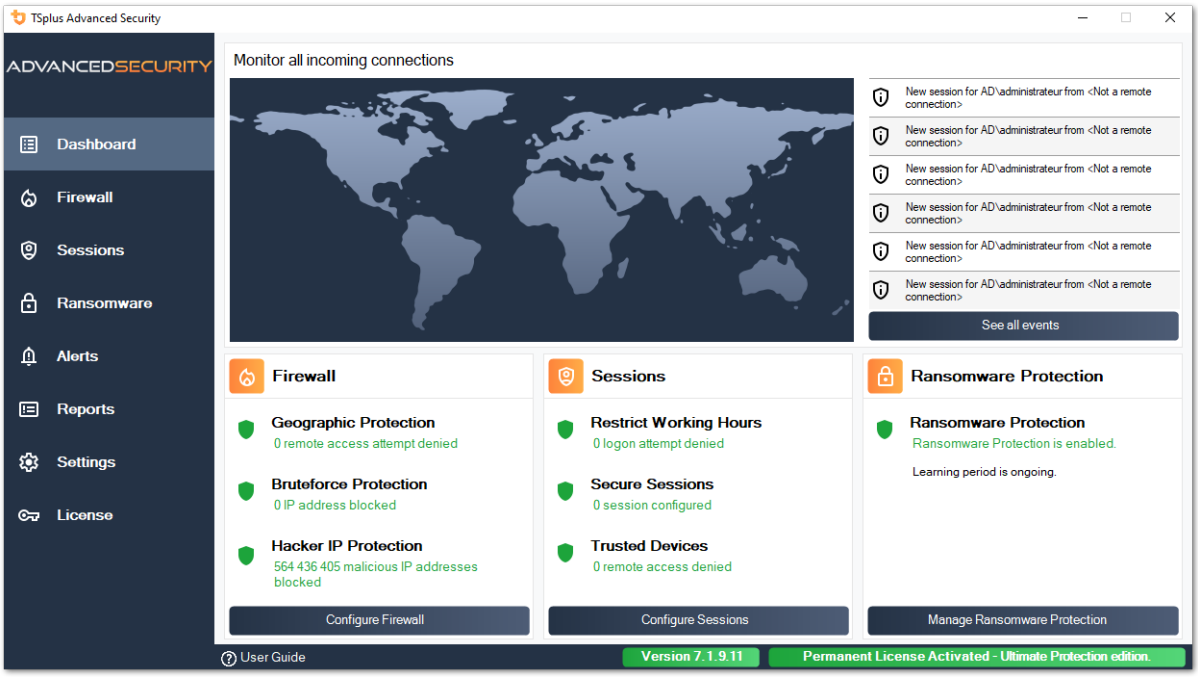
Cualquier nueva instalación comienza un período de prueba completo de 15 días. No dude en contáctenos si enfrenta algún obstáculo o si tiene algún problema al configurar TSplus Advanced Security.

Una vez que se complete la instalación, se mostrará un nuevo ícono en su Escritorio. Haga doble clic en este ícono para abrir TSplus Advanced Security y comenzar a configurar las funciones de seguridad.

Por favor, consulte el documentación para obtener instrucciones completas de instalación.

Paso 2: Configuración de TSplus Advanced Security

Has lanzado TSplus Advanced Security y comenzado a configurar características para proteger su servidor de actividades maliciosas y hacer cumplir políticas de seguridad sólidas.



En la columna izquierda, la página de inicio permite un acceso rápido para configurar las funciones de protección contra ransomware, protección contra bruteforce y protección geográfica.

Inicio Protección contra ransomware el período de aprendizaje de para permitir que Advanced Security identifique aplicaciones y comportamientos legítimos en su sistema haciendo clic en el siguiente mosaico:

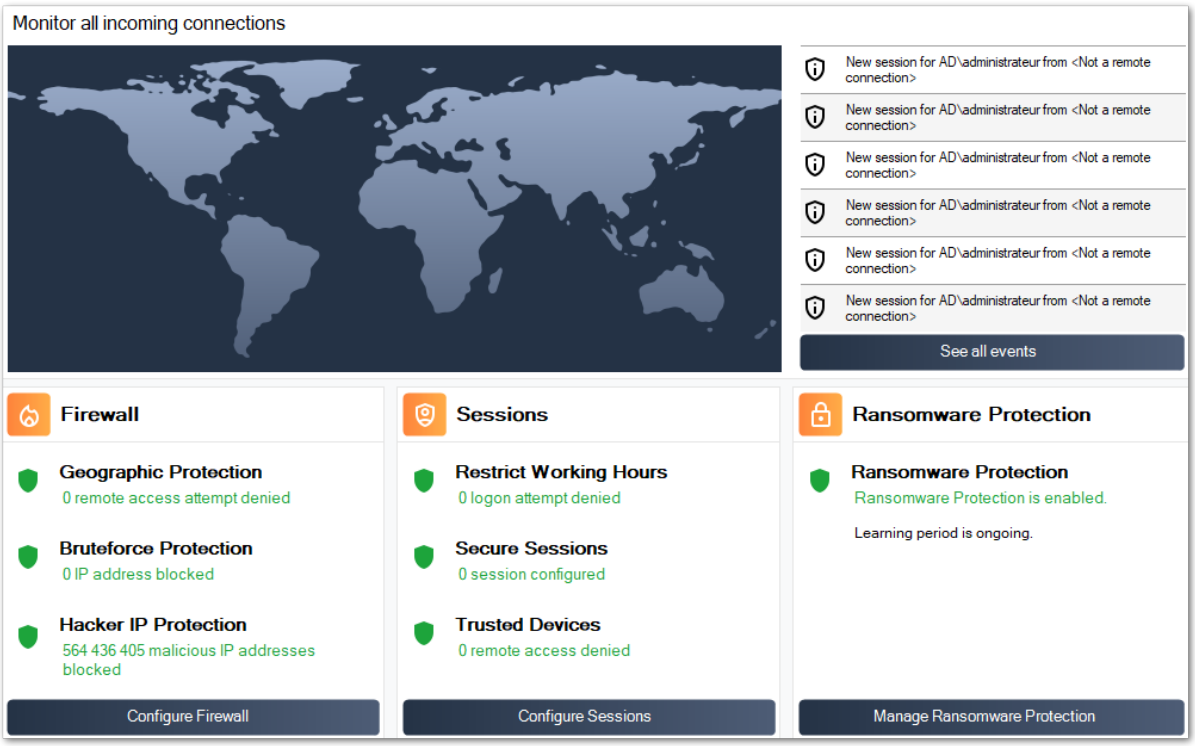
Protección contra ataques de fuerza bruta suele estar en funcionamiento tras la instalación. De lo contrario, haga clic en el **Repetir defensa contra ataques de fuerza bruta** título para resolver problemas y aplicar la configuración del sistema requerida. Por defecto, esta función bloquea a los atacantes después de 10 intentos de inicio de sesión fallidos.

Finalmente, agrega tu país a la lista de países autorizados desde donde se permite a los clientes conectarse. Haz clic en el mosaico. **Autorizar conexiones desde otro país** y añade tu país para configurar Protección Geográfica

¡Estás listo! No olvides que activar su licencia y a actualizar a la última versión para mantener la protección de Advanced Security en su mejor nivel!

Paso 3: Revisar amenazas prevenidas

Ahora que has configurado las funciones clave de seguridad avanzada, las amenazas evitadas se informarán en el Panel de control.



También, el Hacker IP la protección mantiene la máquina protegida contra amenazas conocidas al bloquear más de 500 000 000 direcciones IP maliciosas conocidas.

Todo el eventos de seguridad se puede mostrar haciendo clic en el **Ver todos los eventos** azulejo.

Paso 4: Aprovechando otras características de seguridad para mejorar la protección

En la parte inferior, se pueden acceder y configurar cuatro otras características de seguridad para mejorar la protección de su máquina.

- Ajuste y supervise los privilegios de acceso en sus sistemas de archivos locales, impresoras y claves del registro para garantizar que cada usuario tenga acceso a los recursos relevantes, con el Permisos característica.

- Definir el período de tiempo en el que los usuarios están autorizados a iniciar sesión con el Working Hours Los usuarios serán desconectados una vez que hayan pasado sus horas de trabajo permitidas.

- Personaliza y asegura las sesiones de usuario con el Escritorio Seguro función. Personalizar, ocultar, denegar el acceso a elementos de la interfaz de sesión para usuarios locales.

- Valide el nombre del cliente remoto cuando un usuario se conecte a su máquina con Protección de Endpoint Esta función valida los nombres de las máquinas cliente para cada usuario conectado remotamente.

¡Hay más! Cambiar a modo avanzado te otorga acceso a más capacidades.

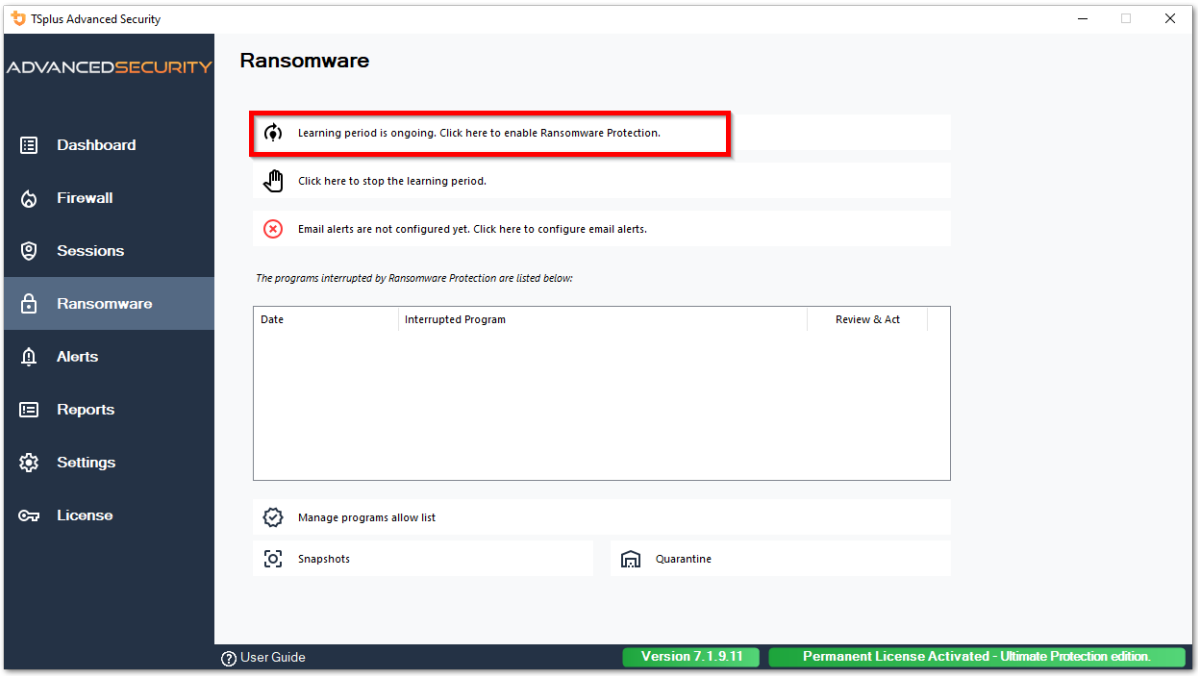
¡Gracias por utilizar TSplus Advanced Security!

Protección contra ransomware

La protección contra ransomware le permite detectar, bloquear y prevenir de manera eficiente los ataques de ransomware. TSplus Advanced Security reacciona tan pronto como detecta ransomware en su sesión. Posee tanto **análisis estático y de comportamiento** :

- El **análisis estático** habilita el software para reaccionar inmediatamente cuando se cambia el nombre de una extensión,
- El **análisis de comportamiento** mira cómo un programa interactuará con archivos y detectará nuevas variantes de ransomware.

Puedes habilitarlo haciendo clic en "Habilitar protección contra ransomware" en la pestaña de protección contra ransomware:

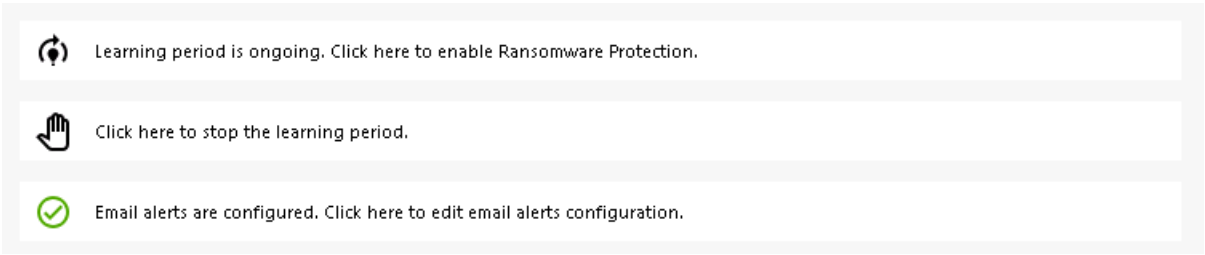


Período de Aprendizaje

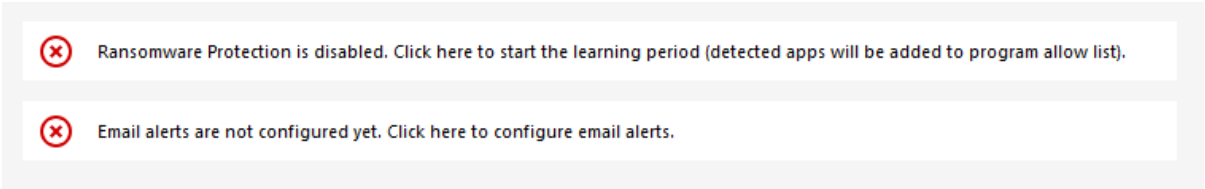
Después de habilitar la función de Protección contra Ransomware, el Período de Aprendizaje se activa automáticamente. Durante el Período de Aprendizaje, todos los programas detectados por la función de Protección contra Ransomware se considerarán como falsos positivos y

podrán reanudar su ejecución. Los programas detectados como falsos positivos se agregarán automáticamente a la lista de programas permitidos.

Esta función permite configurar la protección contra ransomware en un servidor de producción sin interrumpir su actividad. Recomendamos comenzar con un período de aprendizaje de 5 días para identificar todas las aplicaciones comerciales legítimas.



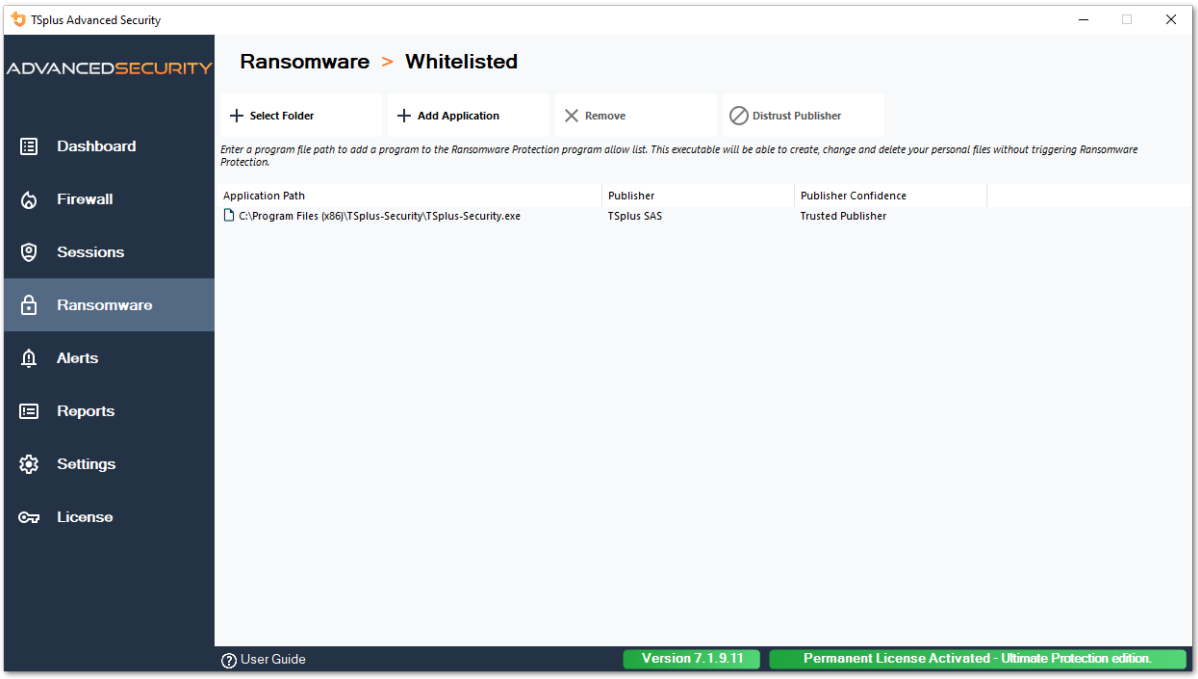
Si detienes el Período de Aprendizaje, desactivará la Protección contra Ransomware. Haz clic en el botón “La Protección contra Ransomware está desactivada” para reactivar el Período de Aprendizaje.



Acción de Protección contra Ransomware

Escanea rápidamente su(s) disco(s) y muestra el(los) archivo(s) o programa(s) responsables, además de proporcionar una lista de los elementos infectados. TSplus Advanced Security detiene automáticamente el ataque y pone en cuarentena el(los) programa(s) junto con el(los) archivo(s) cifrado(s) antes de su intervención.

Solo el administrador puede agregarlos a la lista blanca, ingresando la ruta del programa deseado en la línea inferior y haciendo clic en "Agregar":



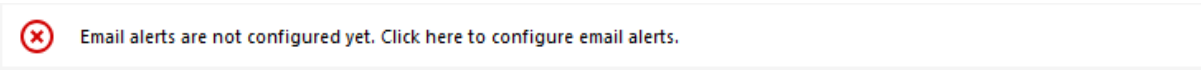
Informe de Protección contra Ransomware

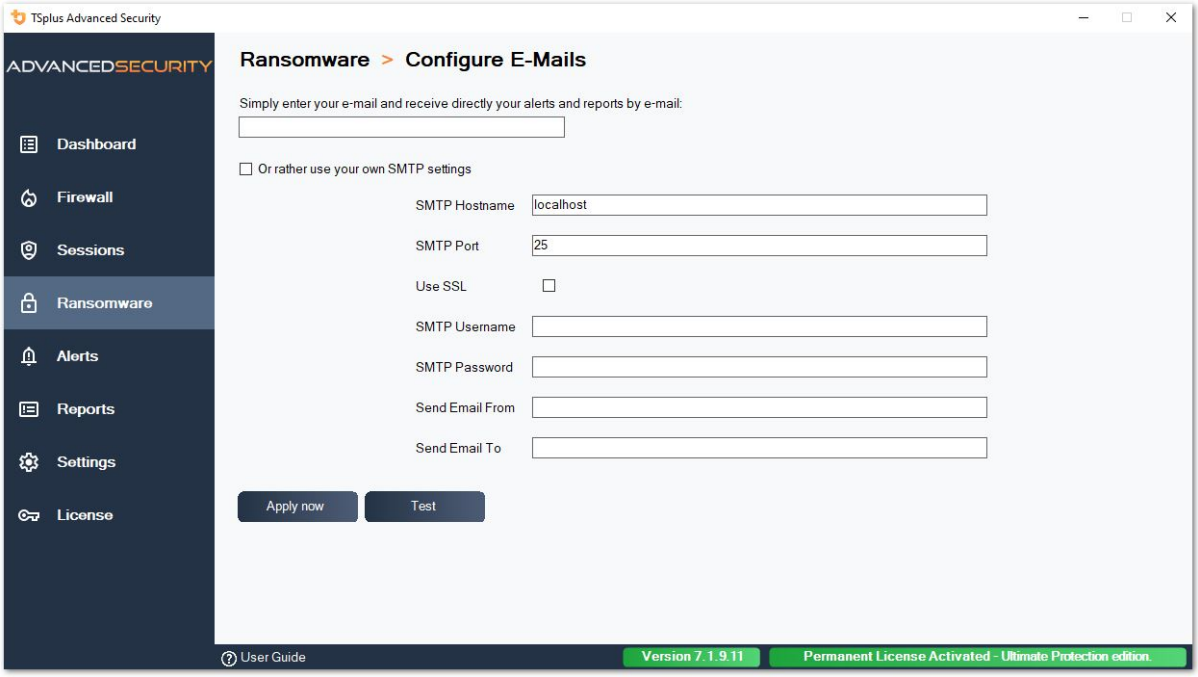
TSplus Advanced Security previene eventos catastróficos para las empresas al eliminar el ransomware en una etapa temprana.

El administrador tiene acceso a información sobre la fuente del ataque y los procesos en ejecución, y por lo tanto aprende a anticipar estas amenazas.

Nota La Protección contra Ransomware observa cómo los programas interactúan con los archivos del sistema y personales. Para garantizar un mayor nivel de protección, la Protección contra Ransomware crea archivos trampa en carpetas clave donde el ransomware a menudo comienza su ataque. Por lo tanto, pueden aparecer algunos archivos ocultos en el escritorio y en las carpetas de documentos de los usuarios, así como en otras ubicaciones. Cuando detecta un comportamiento malicioso, detiene el ransomware de inmediato (o pregunta si el usuario conectado es un administrador). La Protección contra Ransomware utiliza técnicas de detección puramente conductuales y no se basa en firmas de malware, lo que le permite atrapar ransomware que aún no existe.

Puedes configurar tus ajustes de SMTP para que TSplus Advanced Security te envíe alertas por correo electrónico que resalten eventos de seguridad importantes haciendo clic en el botón debajo del de activación de Ransomware.





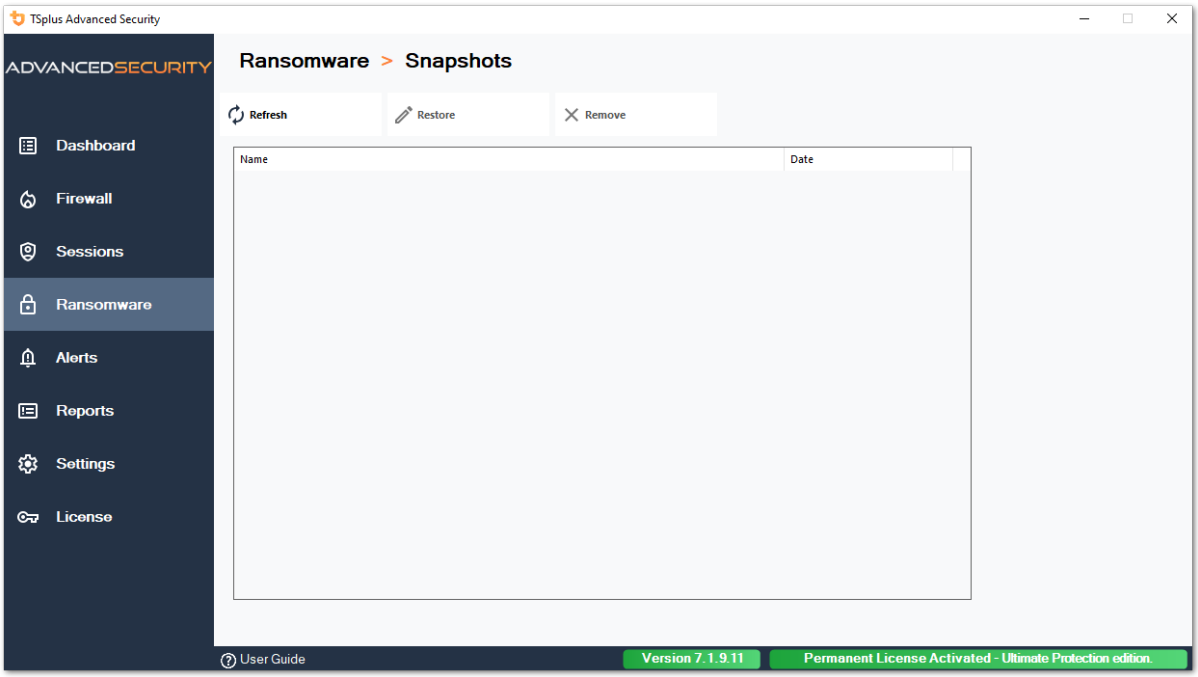
Ingresa tu nombre de host SMTP, puerto y marca la casilla Usar SSL y cambia el puerto de 25 a 465 si deseas usar SSL.

Ingrese el nombre de usuario y la contraseña SMTP, así como las direcciones del remitente y del destinatario.

Los ajustes de correo electrónico se pueden validar enviando una prueba al guardar la configuración de SMTP.

Instantáneas

Las instantáneas tomadas por la protección contra ransomware son visibles en la pestaña de instantáneas:

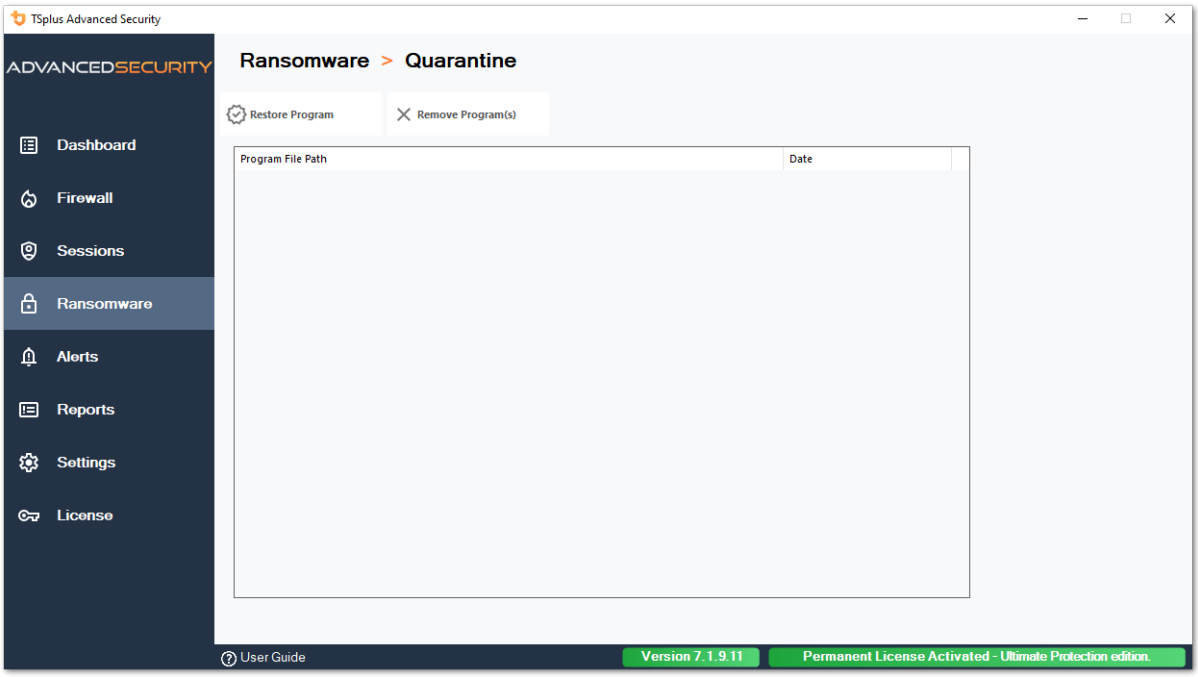


La lista se puede actualizar haciendo clic en el botón correspondiente. Cada elemento se puede restaurar o eliminar.

Cuarentena

Los programas en cuarentena son visibles en la pestaña de Cuarentena:
Los programas potencialmente no deseados se mantienen en cuarentena indefinidamente hasta que decida qué acción tomar.

De esta manera, Advanced Security garantiza la seguridad de su máquina mientras le brinda la opción de gestionar los elementos en cuarentena según su elección.
Esto puede ser útil si necesitas recuperar un archivo o programa que fue neutralizado. **Esta decisión se toma bajo su propio riesgo.**
También puede eliminar permanentemente cualquier archivo o programa que elija directamente desde la carpeta de cuarentena ubicada en el directorio de instalación de Advanced Security.



Cada elemento puede ser restaurado o eliminado.

Los archivos ignorados no se utilizan para detectar posibles acciones maliciosas y no se guardan cuando se modifican. La idea es excluir cualquier operación en archivos grandes o irrelevantes (como los archivos de registro).

- sistema
- dll
- exe
- tmp
- ~tmp
- temp
- caché
- lnk
- 1
- 2
- 3
- 4
- 5
- LOG1
- LOG2
- customDestinations-ms
- registro
- wab~
- vmc
- vhd
- vhdx
- vdi
- vo1

- vo2
- vsv
- vud
- iso
- dmg
- imagen dispersa
- cab
- msi
- mui
- dl_
- wim
- ost
- o
- qtch
- ithmb
- vmdk
- vmem
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- menudata
- icono de la aplicación
- información de la aplicación
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- drk
- mem
- nvram
- hdd
- pk3
- pf
- trn
- automaticDestinations-ms

Precaución sobre la extensión de archivos de copia de seguridad

La extensión de archivo utilizada para guardar archivos modificados es: **instantánea.** El controlador prohíbe cualquier acción de modificación o eliminación en estos archivos, excepto

por el servicio de TSplus Advanced Security. Detener el servicio elimina los archivos respaldados. Para eliminar estos archivos manualmente, debe descargar temporalmente el controlador.

Configuración del archivo de respaldo

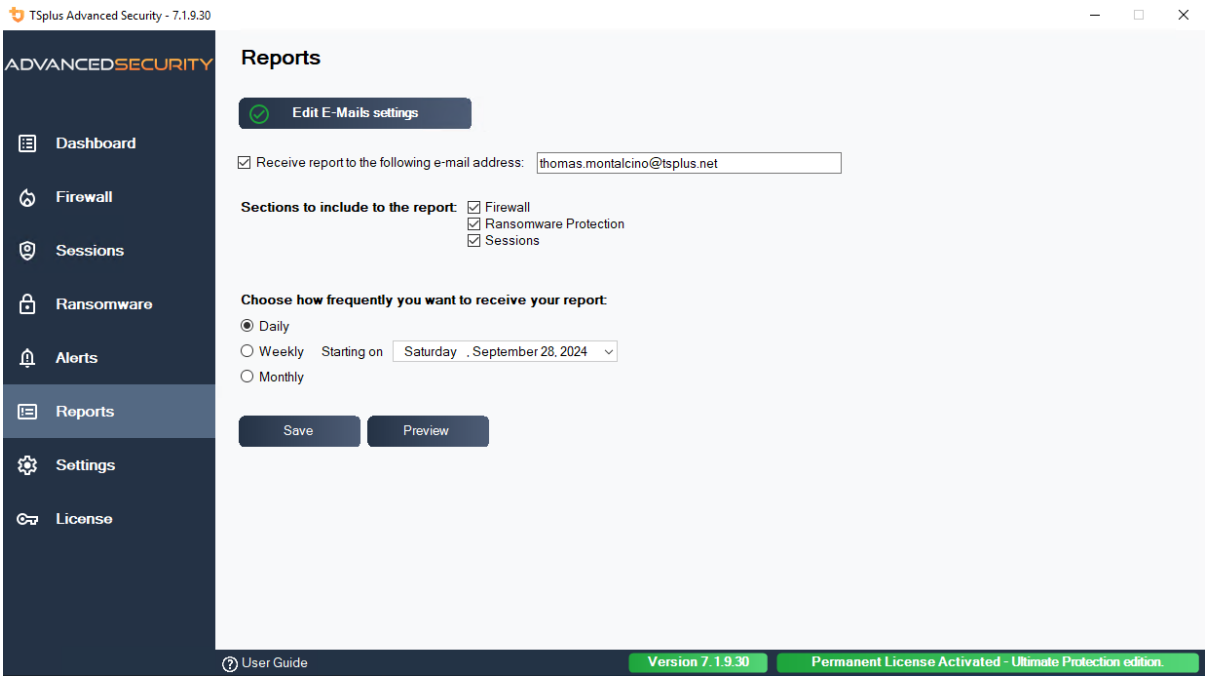
Por defecto, el directorio de archivos guardados se encuentra en el directorio de instalación de TSplus Advanced Security y se llama “snapshots”. Sin embargo, es posible definir otra ubicación para este directorio. Esto puede permitir al administrador definir un directorio ubicado en un disco más rápido (SSD) o en un disco más grande según sus necesidades. La ruta del directorio de respaldo no debe ser una ruta UNC, en la forma de:

\\ \ \

Agregar utilidades de respaldo a la lista blanca

Recomendamos agregar utilidades de respaldo en la lista blanca.

Informes


TSplus Advanced Security - 7.1.9.30
ADVANCEDSECURITY
Dashboard
Firewall
Sessions
Ransomware
Alerts
Reports
Settings
License
Reports
Edit E-Mails settings
Receive report to the following e-mail address:
thomas.montalcino@tsplus.net
Sections to include to the report:
Firewall
Ransomware Protection
Sessions
Choose how frequently you want to receive your report:
Daily
Weekly
Starting on
Saturday , September 28, 2024
Monthly
Save
Preview
User Guide
Version 7.1.9.30
Permanent License Activated - Ultimate Protection edition.

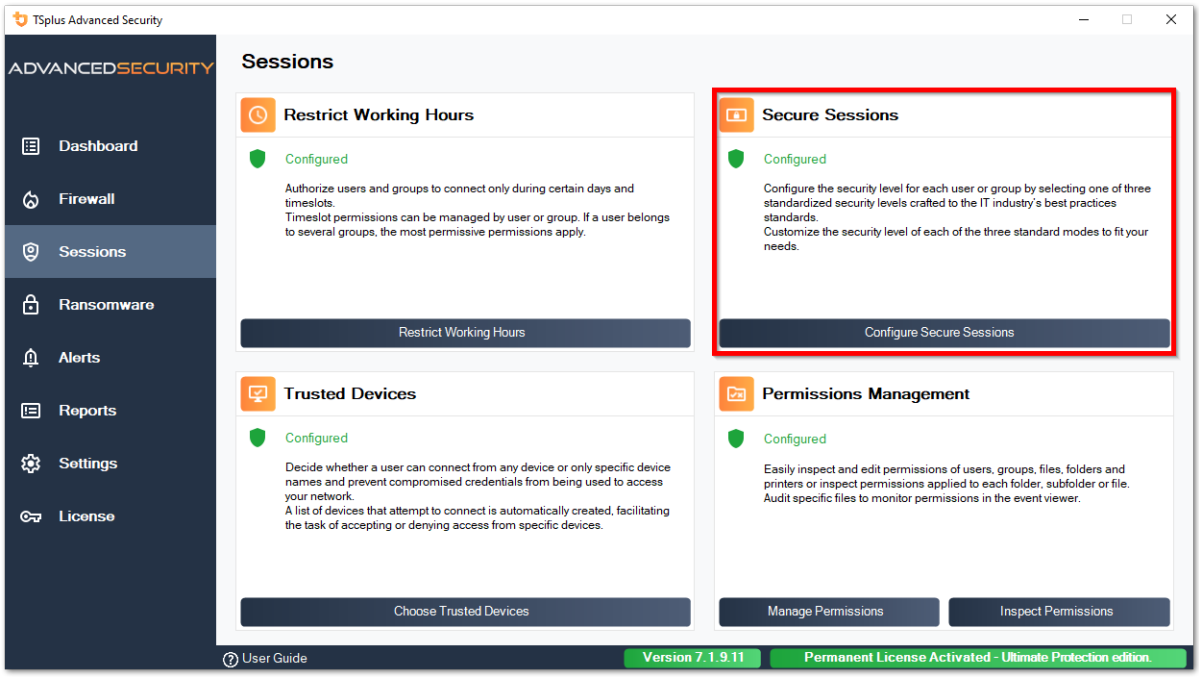
Sesiones Seguras

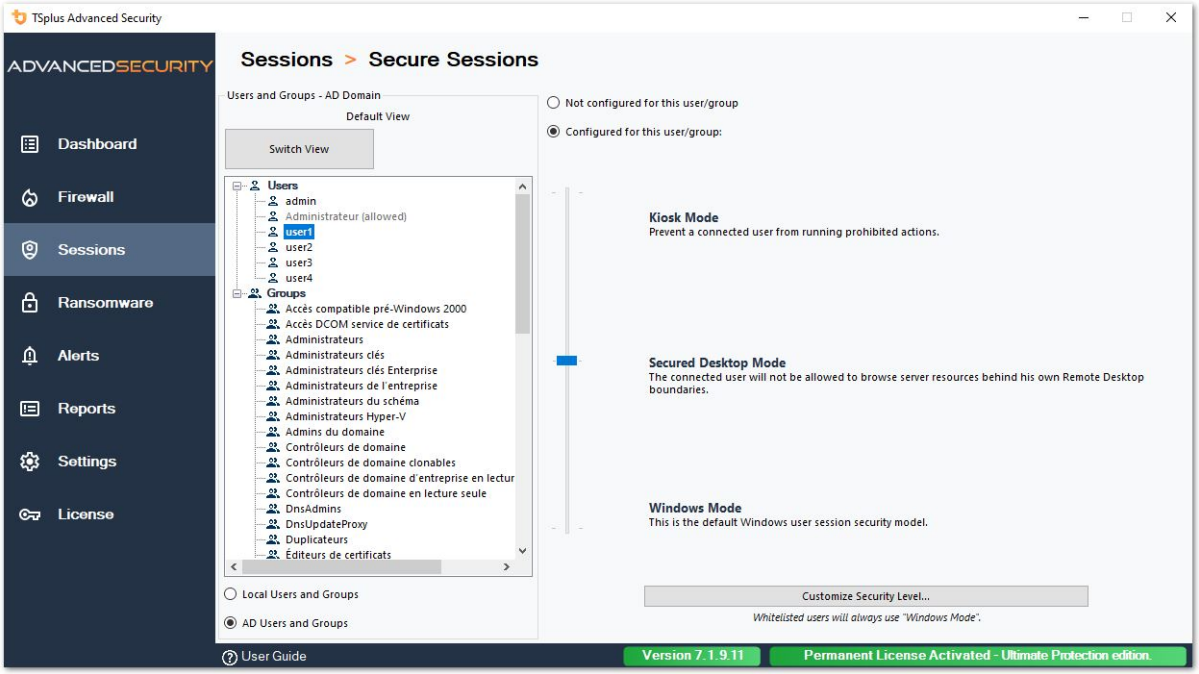
Advertencia

- Las sesiones seguras probablemente entrarán en conflicto con las políticas de seguridad definidas por Active Directory.
- El propósito principal de las Sesiones Seguras es personalizar la interfaz de usuario, no aplicar permisos de acceso. Su uso debe combinarse con la función de Permisos para asegurar el acceso a diferentes unidades.

Puedes configurar el nivel de seguridad para cada usuario o grupo. Hay tres niveles de seguridad:

- El **Modo Windows** donde el usuario tiene acceso a una sesión predeterminada de Windows.
- El **Modo de Sesiones Aseguradas** donde el usuario no tiene acceso al Panel de Control, programas, discos, navegador, sin clic derecho…: sin acceso a los recursos del servidor. Solo tiene acceso a documentos, impresoras, la tecla de Windows y puede desconectar su sesión.
- El **Modo Kiosco** es el más seguro, donde el usuario tiene acciones muy limitadas en su sesión.

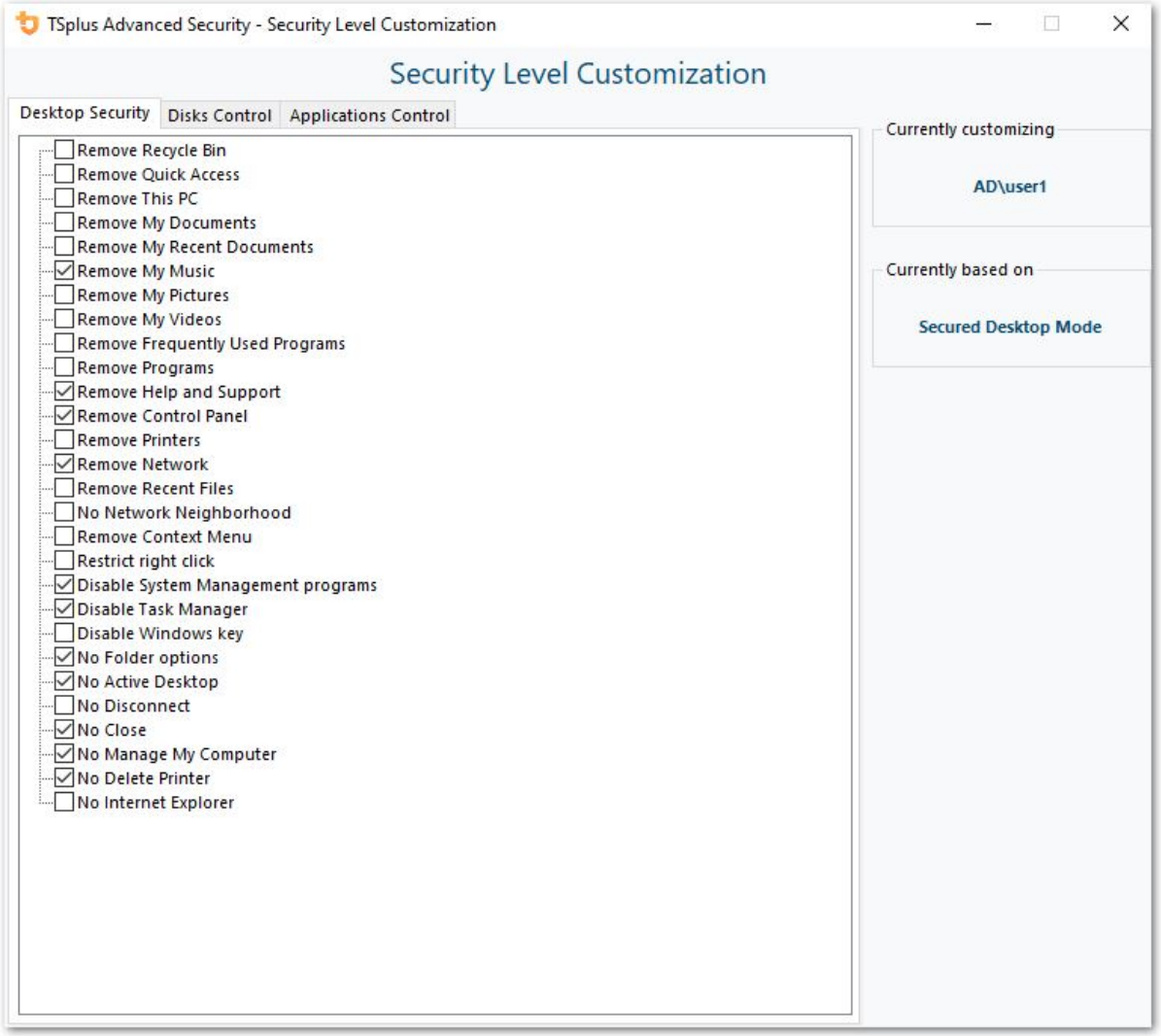




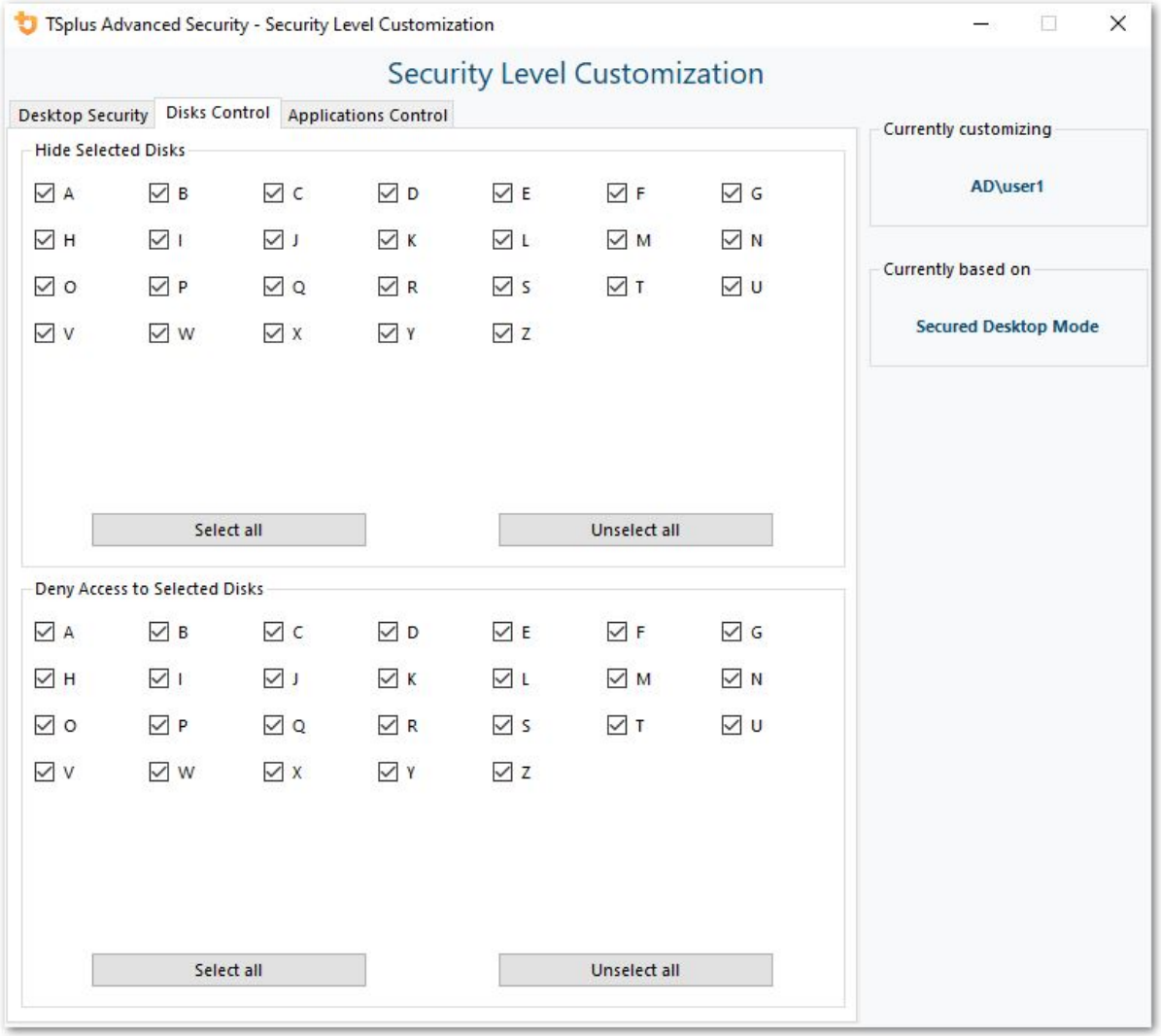
Personalización

En cualquier modo, tienes la posibilidad de personalizar la seguridad en tres niveles:

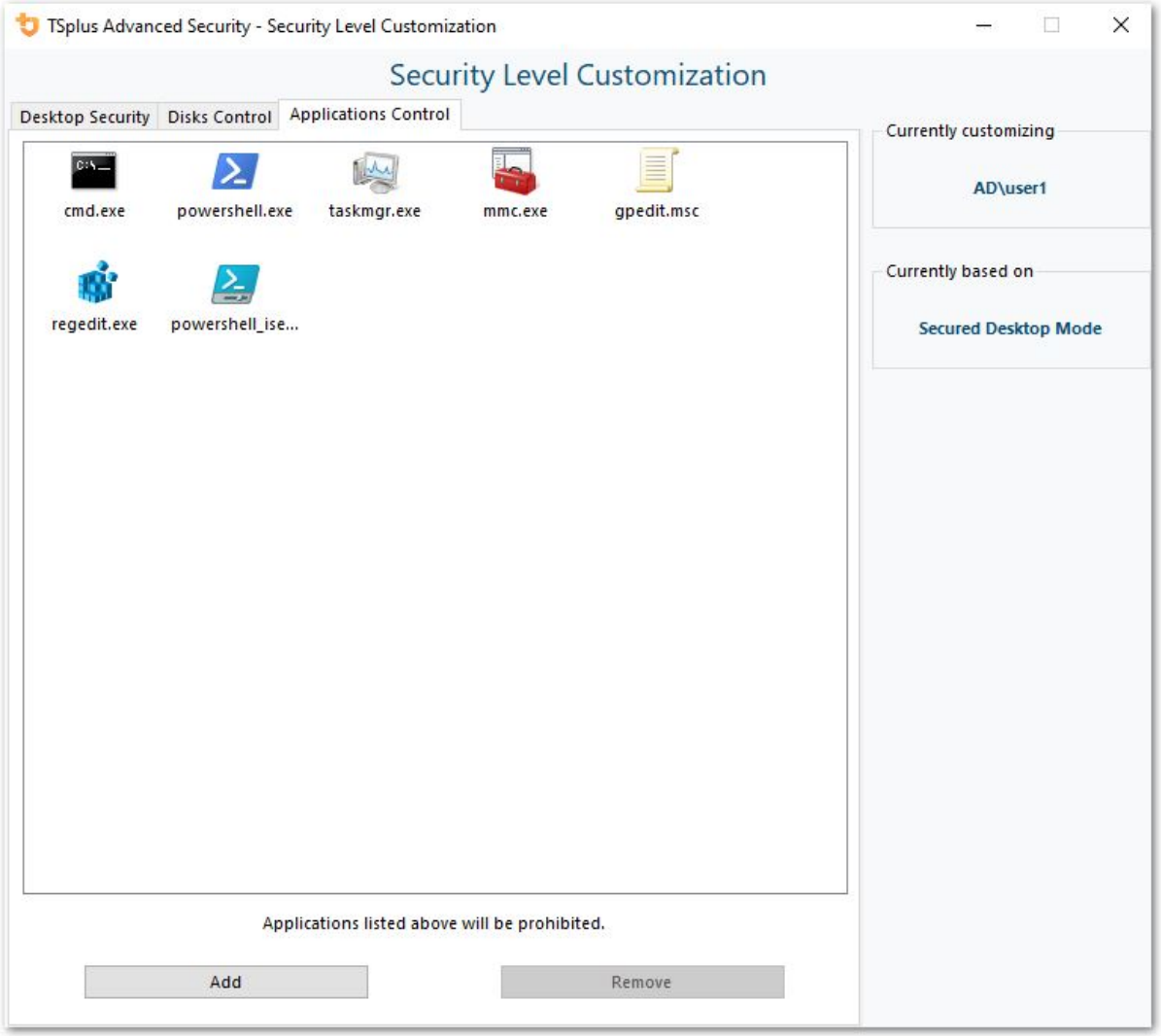
Seguridad de Escritorio:



Control de discos:



Control de Aplicaciones:



Prioridades de reglas de usuarios/grupos

Cuando un usuario abre una nueva sesión en el servidor:

1. Si este usuario tiene un Nivel de Seguridad definido directamente para él, entonces este Nivel de Seguridad se aplica.
2. Si este usuario no tiene un Nivel de Seguridad definido directamente para él, entonces TSplus Advanced Security cargará cualquier configuración de Nivel de Seguridad existente para todos los grupos de este usuario y mantendrá las reglas más permisivas.

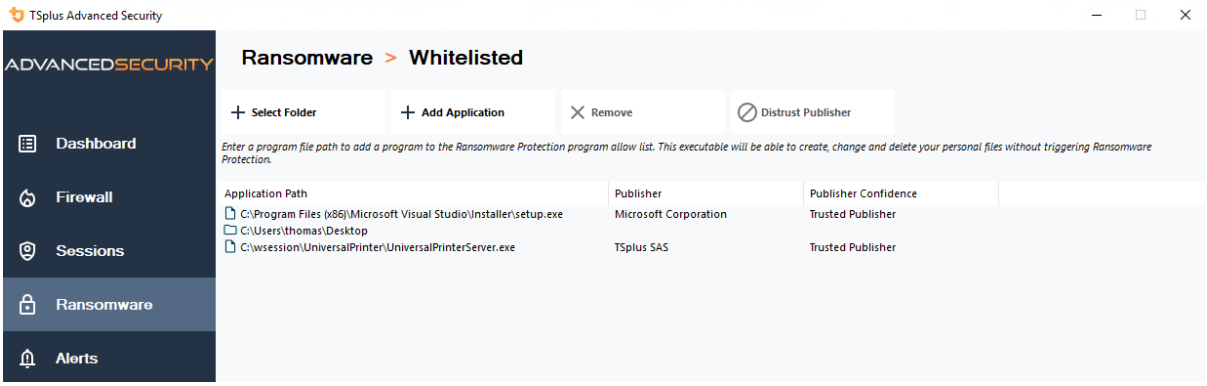
Por ejemplo, si un primer grupo tiene una regla para eliminar el icono de la Papelera de reciclaje del escritorio, pero esta regla está desactivada para un segundo grupo, entonces el usuario tendrá el icono de la Papelera de reciclaje en su escritorio. Las mismas reglas de prioridad se aplicarán a cada regla personalizada (Seguridad del Escritorio, Control de Discos y Control de Aplicaciones), así como al Nivel de Seguridad principal (el Modo Windows se considera más permisivo que el Modo Escritorio Seguro, que se considera más permisivo que el Modo Kiosco).

N.B : Para deshabilitar el clic derecho en todas partes, debe seleccionar las siguientes dos opciones:

- Restringir clic derecho
- Eliminar menú contextual

Configuración - Lista de Permisos de Programas

En el **Pestaña de programas** , puedes agregar programas a la lista de programas permitidos, que no serán verificados por la Protección contra Ransomware de TSplus Advanced Security Por defecto, todos los programas de Microsoft están en la lista blanca.



Haga clic en el botón "Agregar aplicación" para añadir un programa. También puede eliminarlos seleccionando la(s) aplicación(es) y haciendo clic en el botón Eliminar aplicación(es).

Configuración - Lista de Permisos de Usuarios

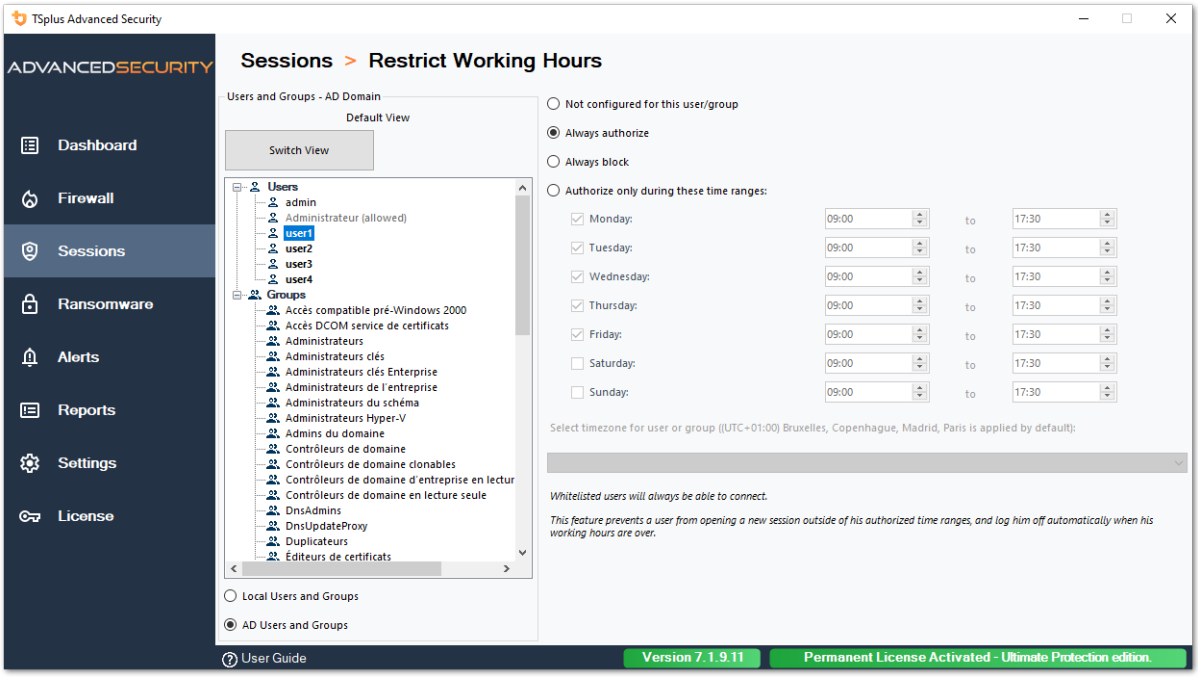
Vista Avanzada

Con la vista avanzada, agrega y gestiona usuarios y grupos de todos los dominios accesibles.

Puedes cambiar la vista de la vista predeterminada a la vista avanzada utilizando el botón "Cambiar vista".

La vista avanzada se utiliza para mostrar y gestionar todos los usuarios y grupos configurados actualmente. También te permite agregar nuevos usuarios y grupos a la lista para configurarlos, utilizando el selector de búsqueda de AD de Windows. Puedes hacerlo haciendo clic en el botón "Agregar usuario/grupo". Luego podrás agregar cualquier usuario disponible de los dominios accesibles desde tu servidor.

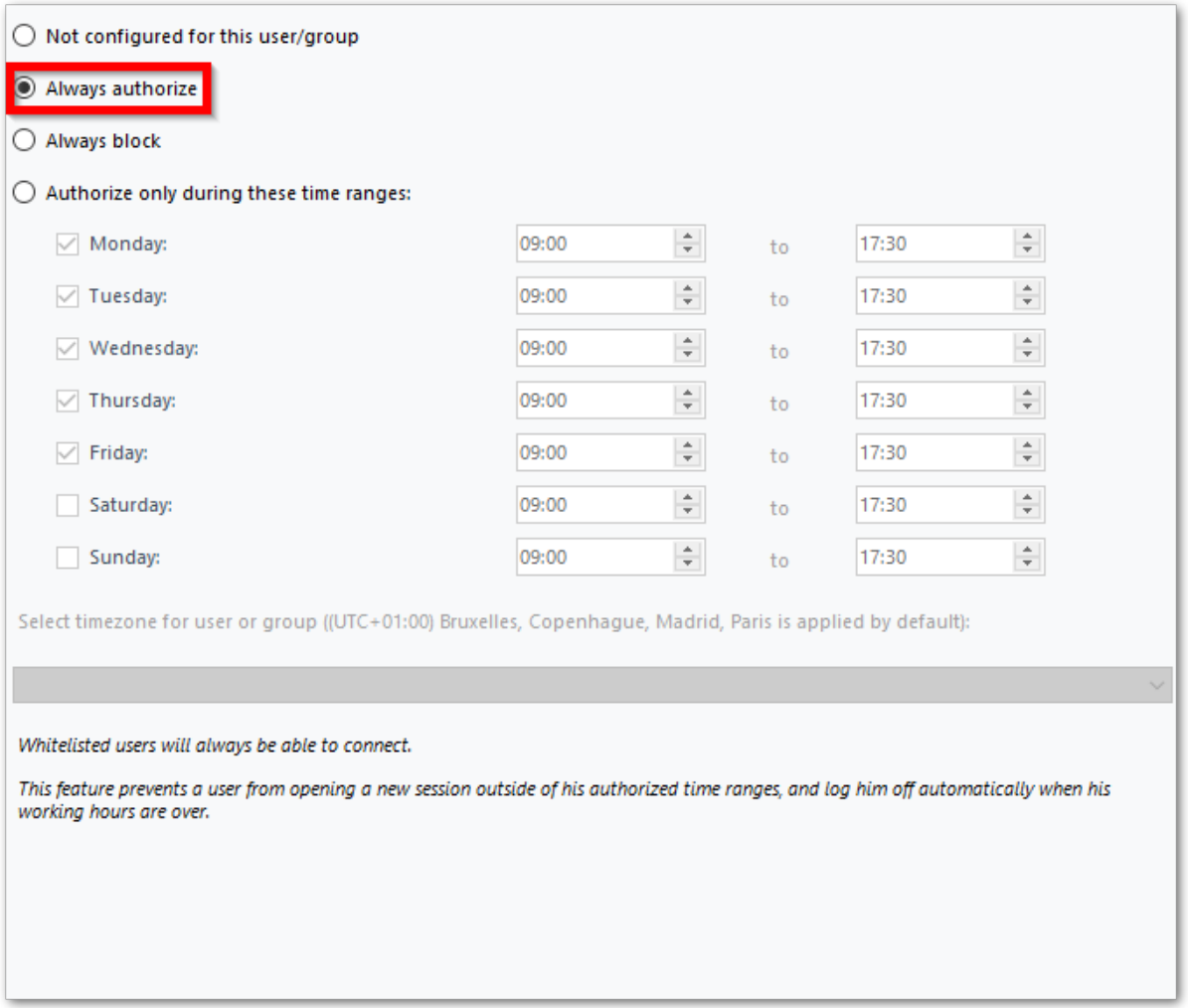
La Vista Avanzada está disponible en las funciones de Permisos, Horarios de Trabajo y Escritorios Seguros. Ejemplo:



El **Usuarios en la lista blanca** el tab le da al Administrador la posibilidad de agregar/quitar usuarios de la lista blanca .

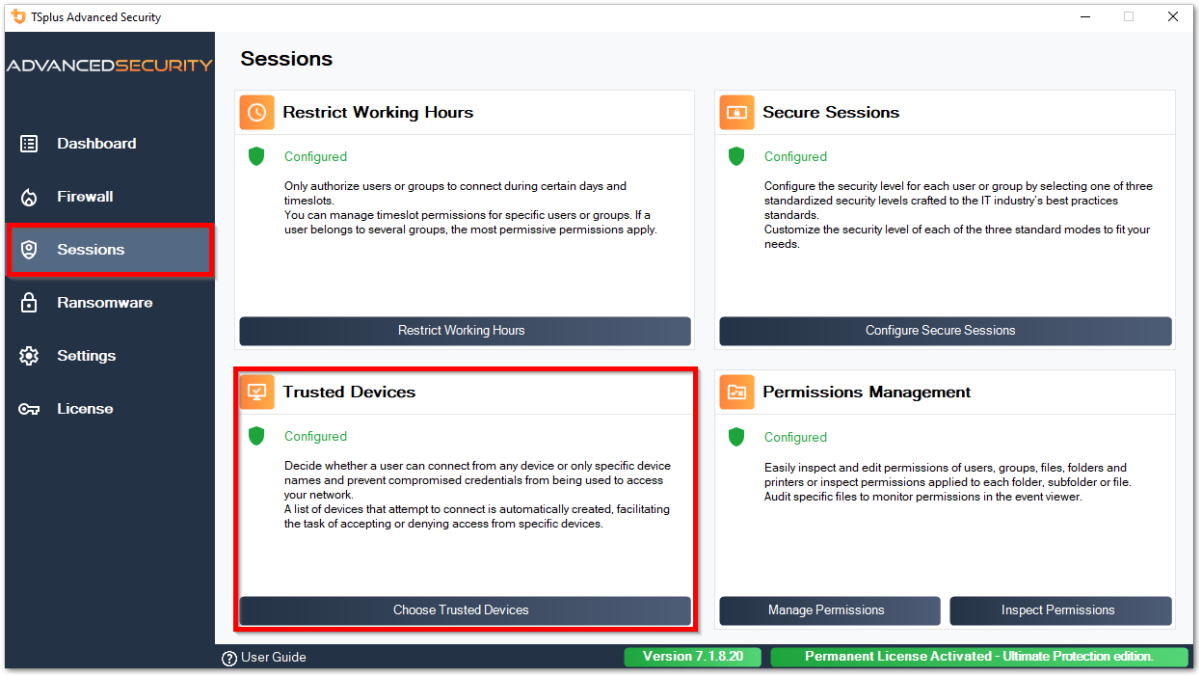
Los usuarios en la lista blanca son ignorados por TSplus Advanced Security y sus configuraciones no se aplicarán.

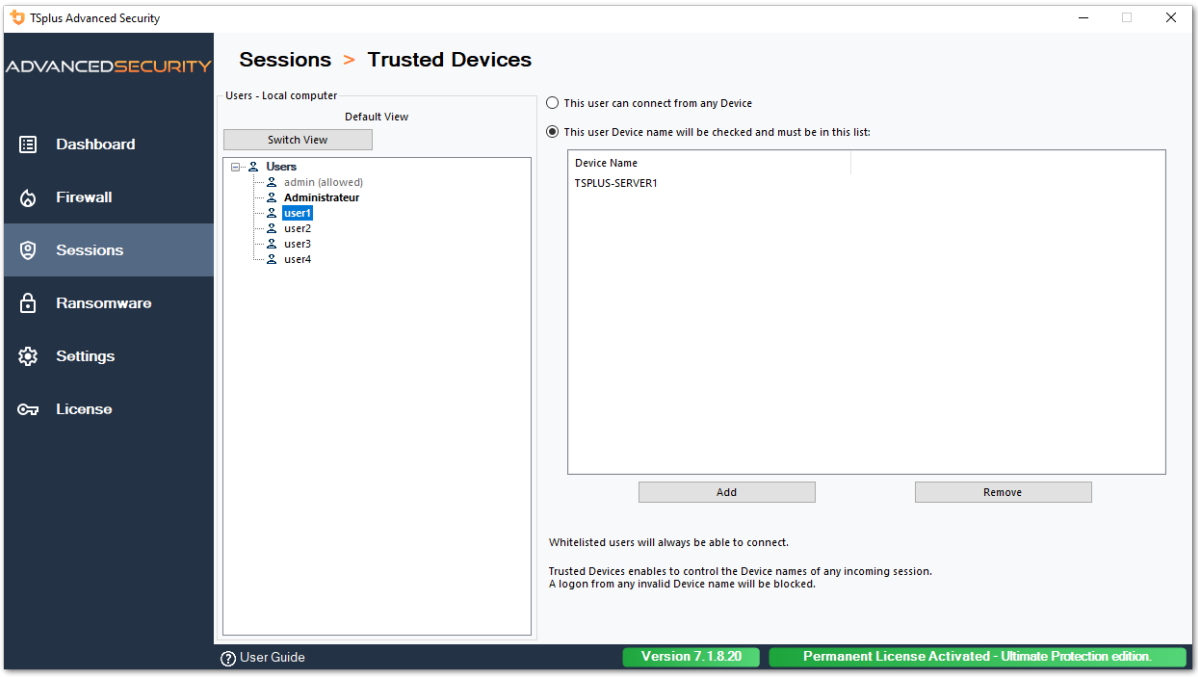
El usuario que instaló TSplus Advanced Security se agrega automáticamente a la lista blanca:



Dispositivos de confianza

Trusted Devices le permite controlar el dispositivo de los usuarios al permitir que cada usuario utilice solo uno o varios dispositivos específicos, los cuales serán verificados en cualquier sesión entrante. Un inicio de sesión desde cualquier nombre de dispositivo no válido será bloqueado.





En este ejemplo, **Usuario1** se estará utilizando el nombre del dispositivo **TSPLUS-SERVER1** solo.

Autocompletar el campo de nombre del dispositivo

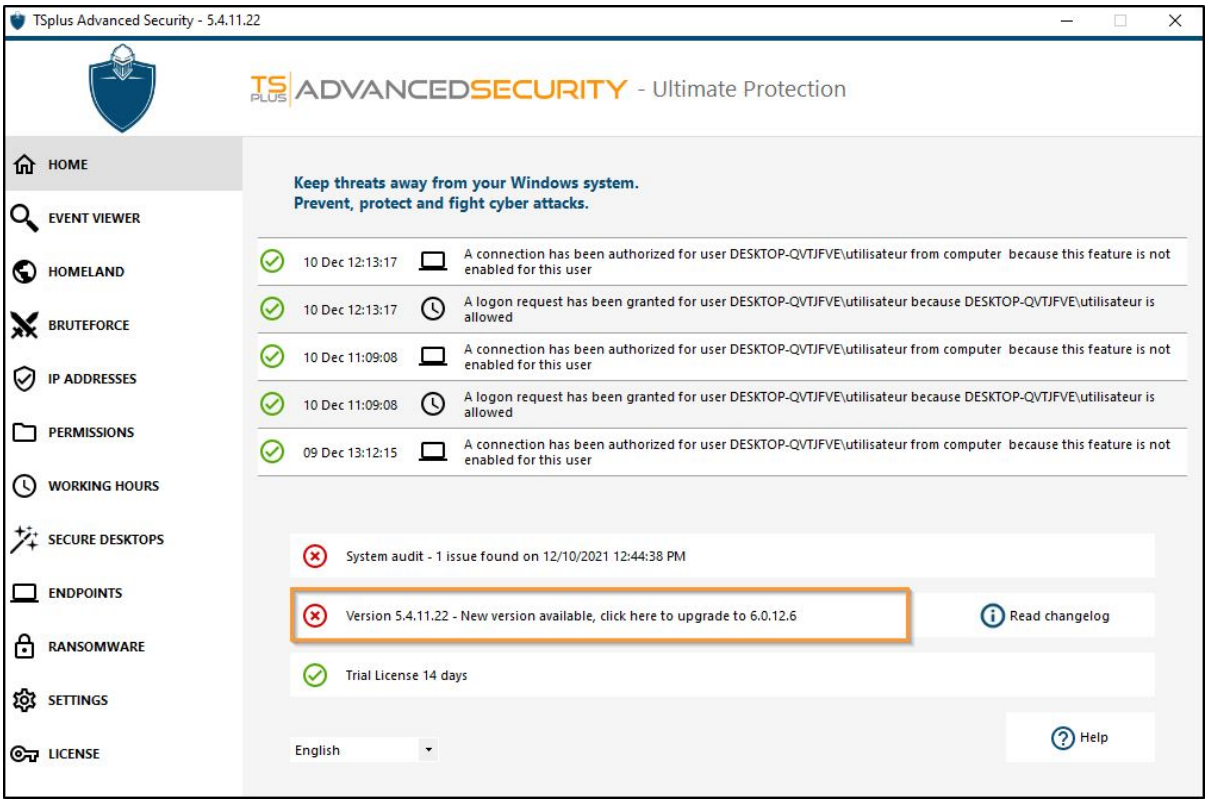
Es posible que notes que el campo Nombre del dispositivo ya está lleno con un nombre de dispositivo para algunos usuarios. Para ayudar al administrador, TSplus Advanced Security guardará automáticamente el nombre del último dispositivo utilizado para conectarse al servidor por cualquier usuario que no tenga habilitada la función Dispositivos de confianza. Después de un día hábil, el nombre del dispositivo de la mayoría de los usuarios será conocido por advanced-security, lo que te permitirá habilitar rápidamente la función de Protección de Endpoint sin tener que verificar el nombre de la estación de trabajo de cada usuario.

Nota Dispositivos de confianza no es compatible con conexiones HTML5.

Actualizando TSplus Advanced Security

Consulta nuestras correcciones y mejoras haciendo clic en Historial de cambios

Actualizar TSplus Advanced Security es fácil y se puede hacer haciendo clic en el mosaico correspondiente, desde la Página de inicio:



Luego, TSplus Advanced Security descarga y aplica la actualización.

Nota: sus datos y configuraciones siempre se respaldan antes de una actualización y se pueden encontrar en el directorio “archivos”, en la carpeta de configuración de TSplus Advanced Security. Ver Haga una copia de seguridad y restaure sus datos y configuraciones

Restringir Horas de Trabajo

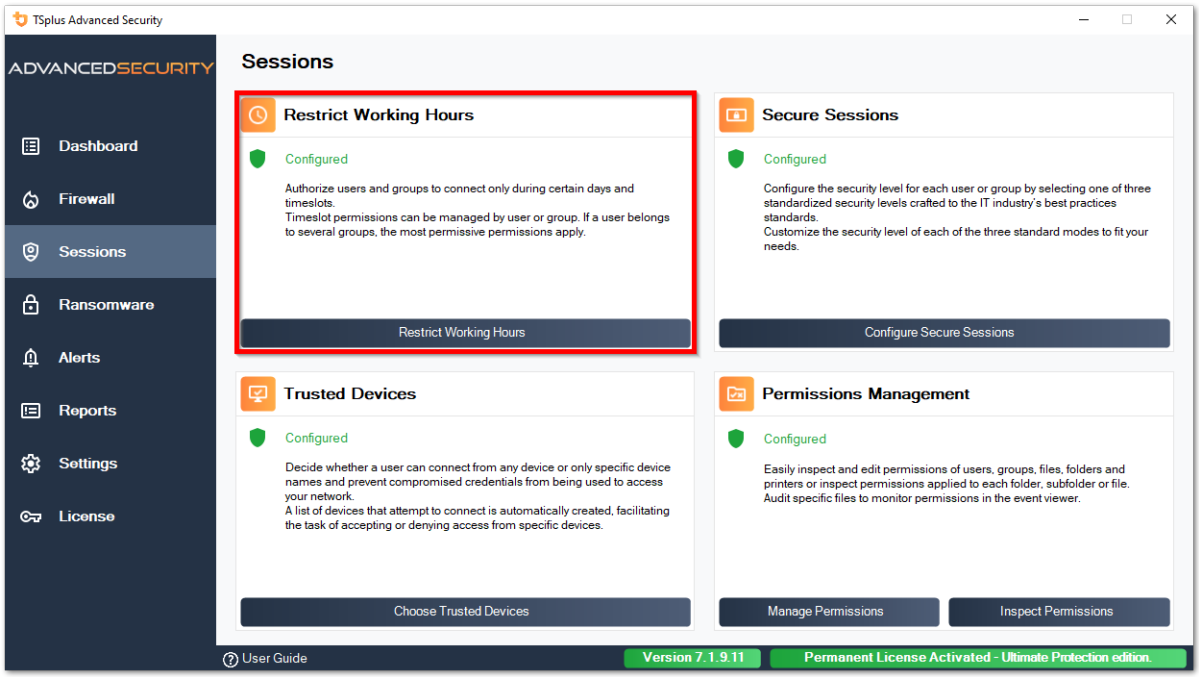
Puedes configurar restricciones de horas laborales por usuario o por grupo.

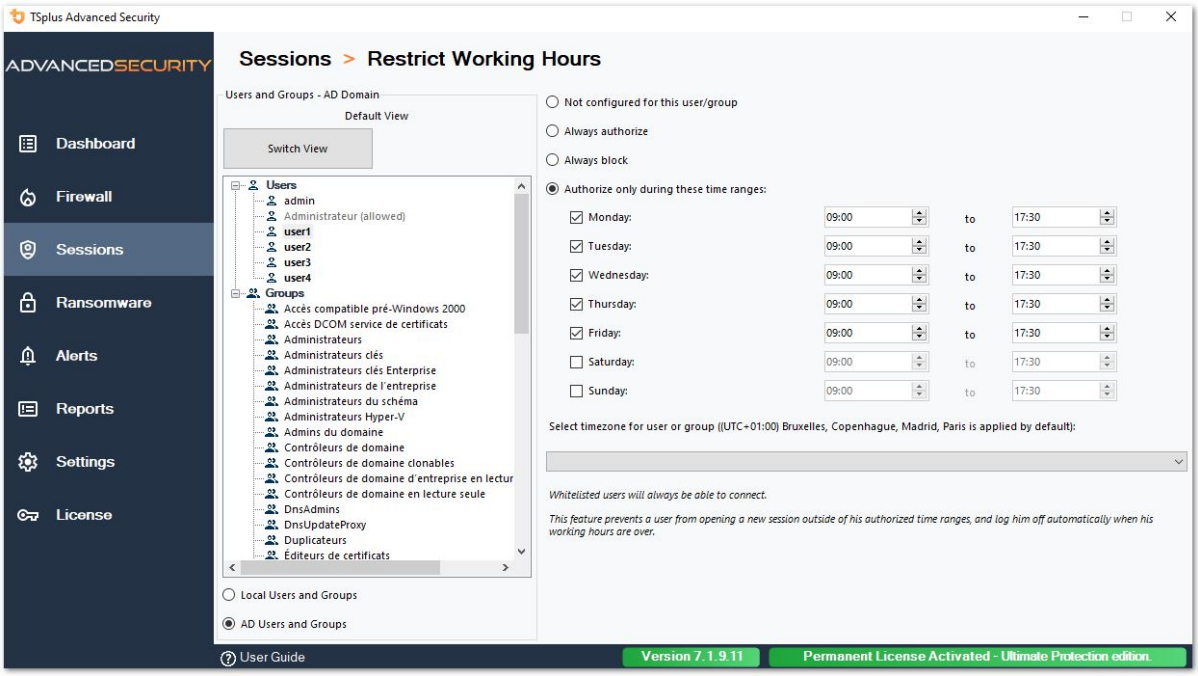
Elija la restricción de su elección:

- Siempre autoriza el acceso de este usuario/grupo
- Siempre bloquee el acceso de este usuario/grupo

o Autorizar solo durante rangos de tiempo específicos.

Puedes configurarlo día a día y seleccionar el rango de tiempo de tu preferencia:





Es posible seleccionar una zona horaria específica según la ubicación de la oficina de su usuario.

Se realiza una desconexión automática al final del tiempo de trabajo configurado.

Es posible programar un mensaje de advertencia antes de que el usuario cierre sesión en Configuración > Avanzado > Horario Laboral .

###Prioridades de reglas de usuarios/grupos

Cuando un usuario abre una nueva sesión en el servidor:

1. si este usuario tiene restricciones de Horario Laboral definidas directamente para él, entonces se aplican estas reglas.

2. si este usuario no tiene restricciones de Working Hours definidas directamente para él, entonces TSplus Advanced Security cargará cualquier restricción de Working Hours existente para todos los grupos de este usuario y mantendrá las reglas más permisivas. Por ejemplo, si un primer grupo tiene una regla para bloquear la conexión el lunes, un segundo grupo tiene una regla para autorizar la conexión el lunes de 9 AM a 5 PM y un tercer grupo tiene una regla para autorizar la conexión el lunes de 8 AM a 3 PM, entonces el usuario podrá abrir una conexión el lunes de 8 AM a 5 PM.

Advertencia: Esta función utiliza la hora del servidor. Usar la hora de la estación de trabajo del usuario y/o la zona horaria sería inútil, ya que todo lo que el usuario tendría que hacer sería cambiar su zona horaria para abrir una sesión fuera de su horario

autorizado.