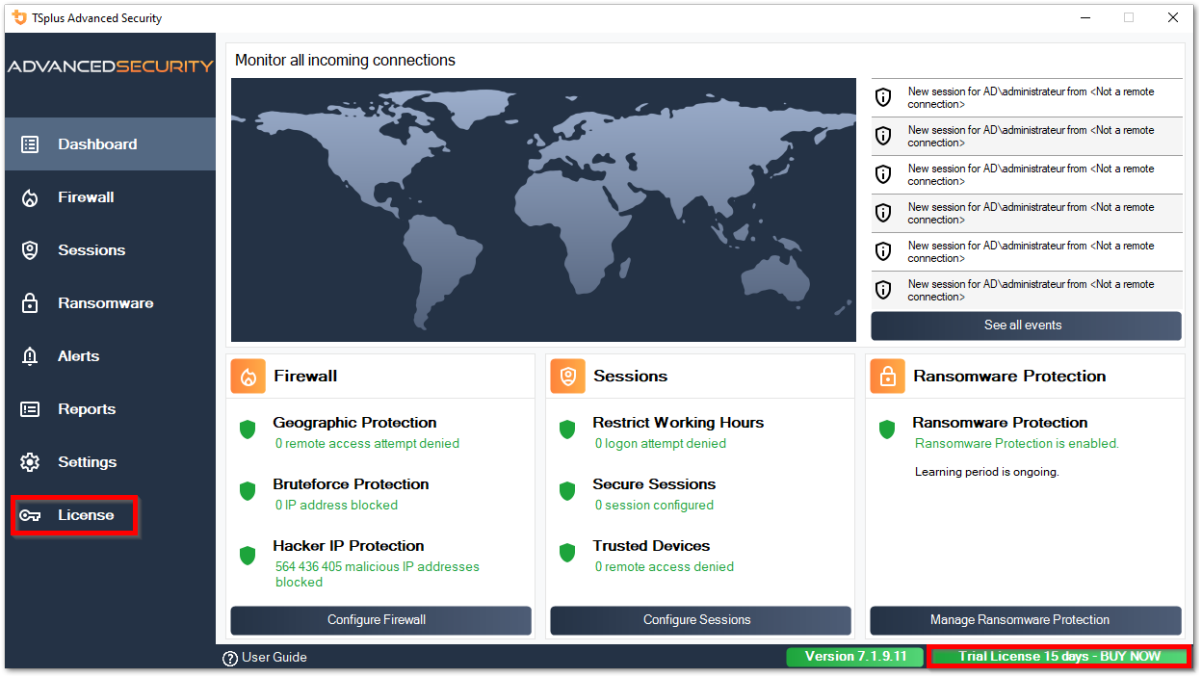
TSplus Advanced Security - Ativando sua licença

Passo 1: Ativando sua licença do modo Lite

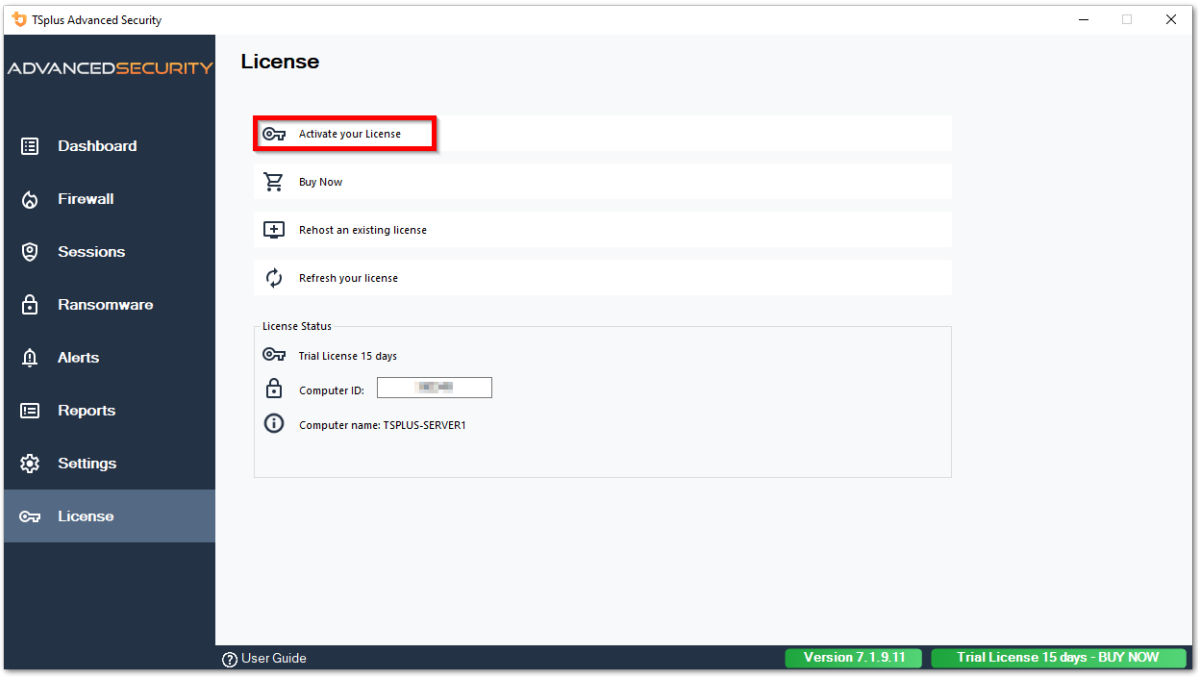
Clique no botão "Licença de Teste" para comprar uma licença ou na aba Licença se você já tiver uma licença e uma Chave de Ativação.



Em seguida, clique no botão “Ativar sua Licença”.

Você encontrará sua chave de ativação permanente **(XXXX-XXXX-XXXX-XXXX)** na nossa confirmação de pedido por e-mail.

Se você deseja ativar sua assinatura, insira sua chave de assinatura. **(S-XXXX-XXXX-XXXX-XXXX)** .



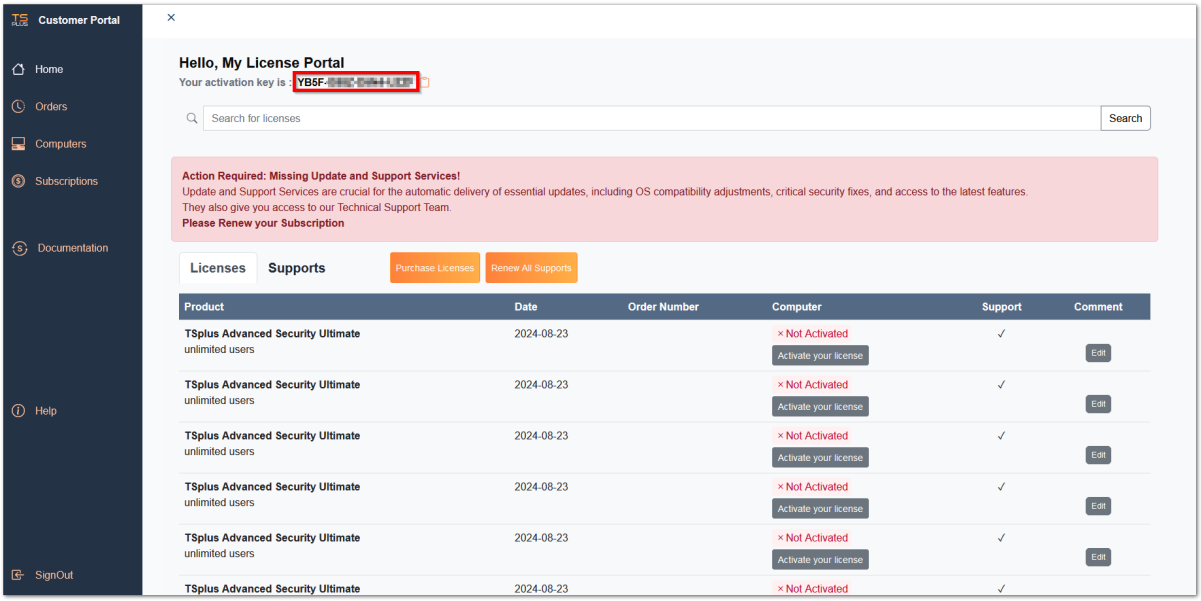
Se você não souber sua chave de ativação, por favor, prossiga para a etapa 2. Caso contrário, prossiga para a etapa 3.

Passo 2: Recupere sua chave de ativação no portal de Licenciamento

Para obter sua Chave de Ativação, conecte-se ao nosso Portal de Licenciamento e insira seu Endereço de Email e seu Número do Pedido:

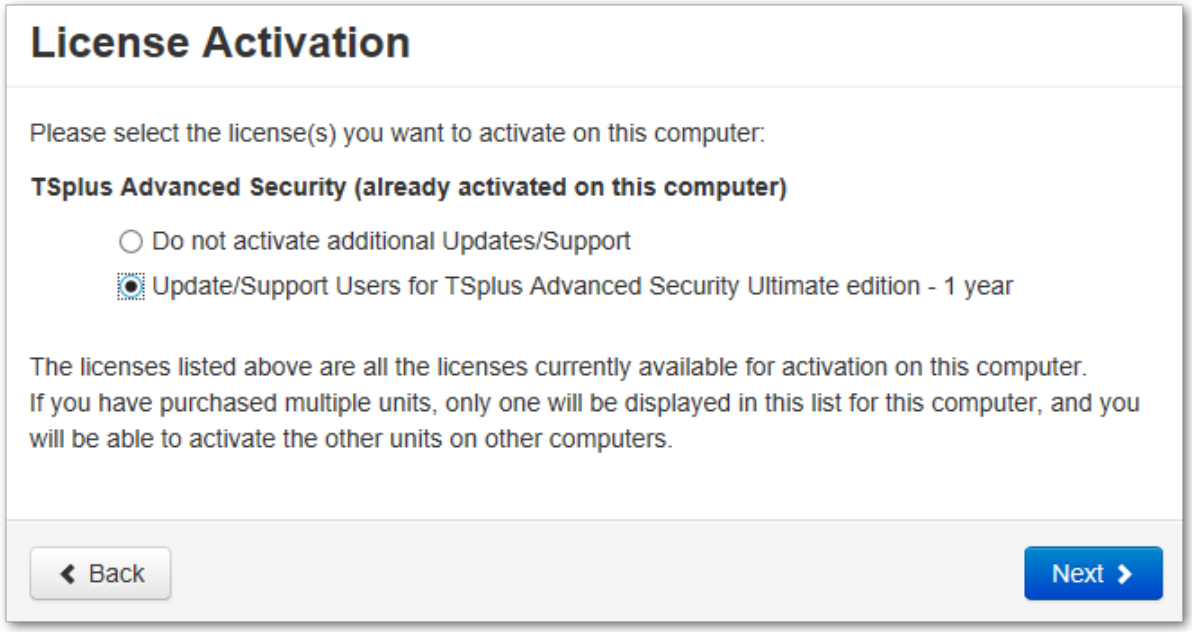
Baixe o Guia do Usuário do Portal do Cliente para mais informações sobre o seu portal do cliente.

Sua chave de ativação será exibida na parte superior do painel:

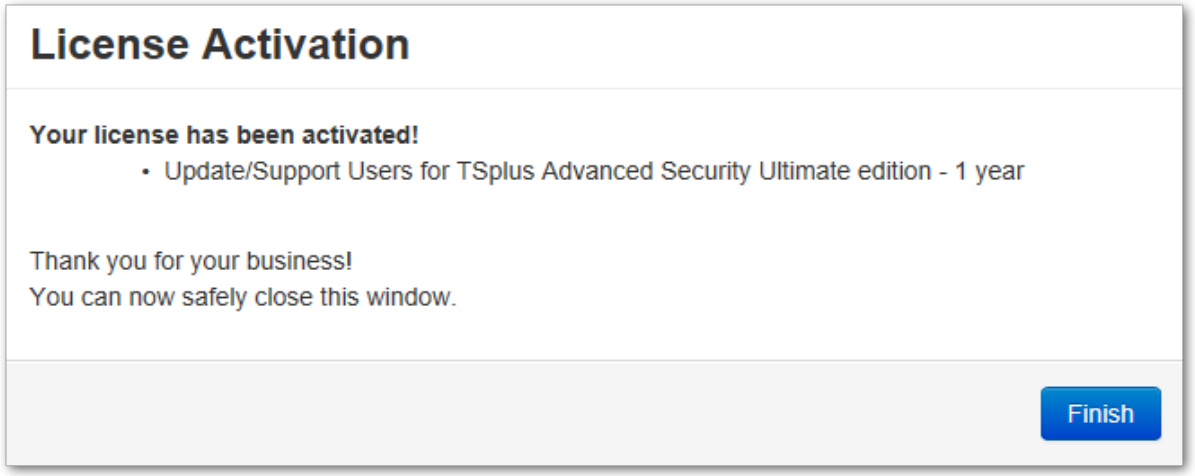


Passo 3: Selecione as licenças solicitadas e os serviços de Atualização e Suporte para os produtos instalados

Insira sua chave de ativação e clique em "Próximo".

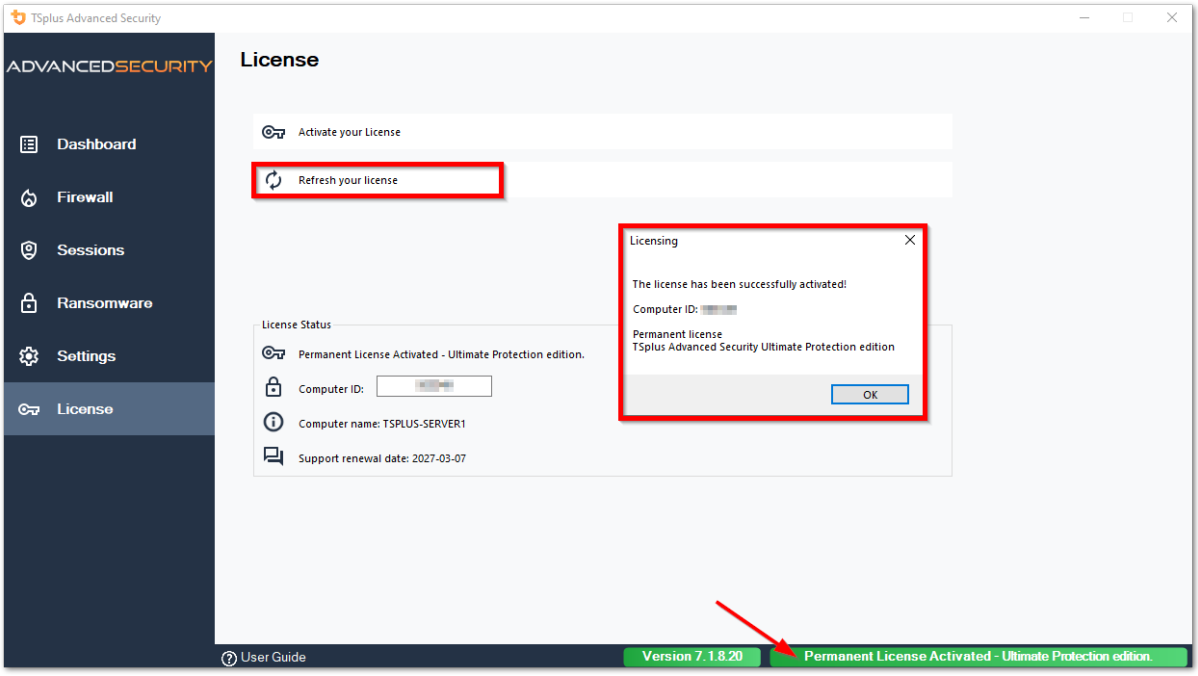


Verifique um ou mais itens e clique no botão "Próximo". Observe que você pode ativar vários produtos ao mesmo tempo marcando vários produtos e/ou assinaturas de suporte.



Todos os seus produtos selecionados e assinaturas de suporte estão agora ativados (neste exemplo, tanto o TSplus com suporte quanto o TSplus Advanced Security foram ativados ao mesmo tempo).

Atualize seu status de licenciamento clicando no botão correspondente.



Ativando sua licença (Offline)

Por favor, consulte o procedimento descrito para TSplus Remote Access: Ativando sua Licença TSplus (Offline)

Rehosting sua licença

Por favor, consulte o procedimento descrito para TSplus Remote Access: Rehosting sua Licença TSplus

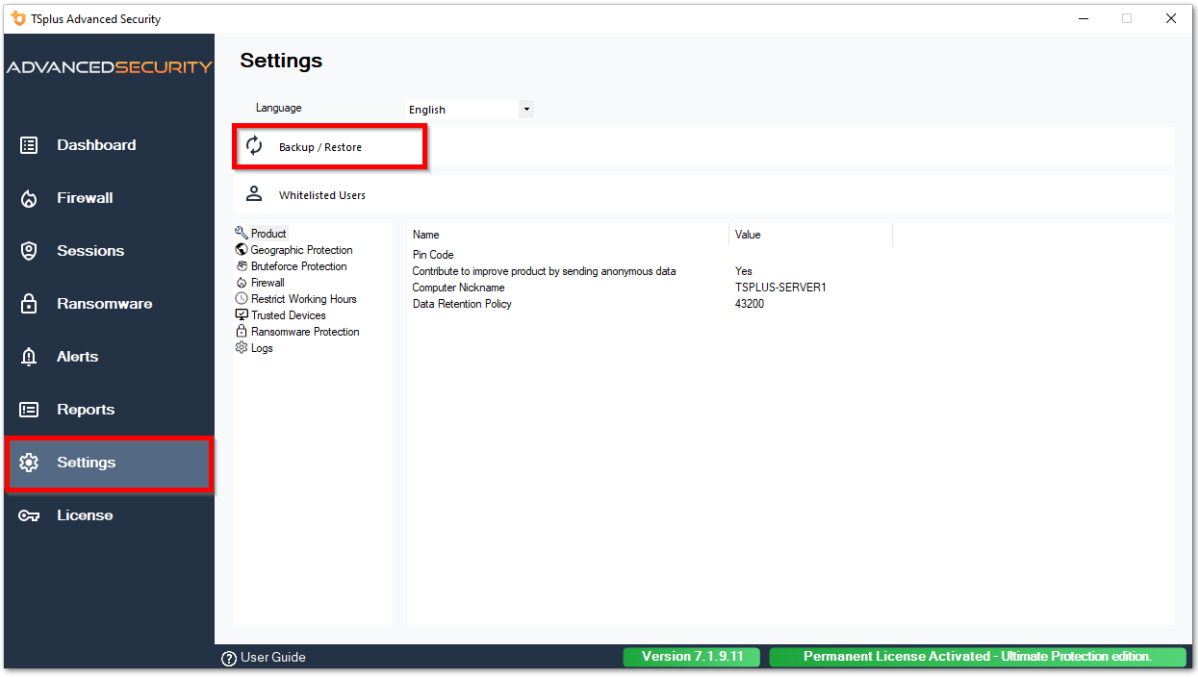
Nota: Você pode baixar um arquivo license.lic no Portal de Licenciamento para versões do TSplus Advanced Security abaixo. Consulte o Guia do Usuário do Portal do Cliente para mais informações.

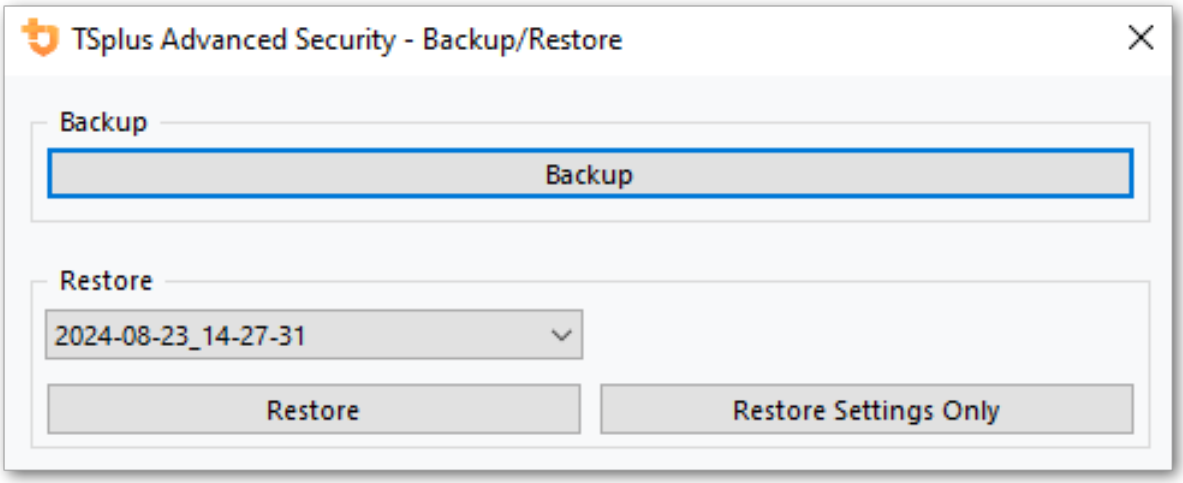
Obrigado por escolher o TSplus Advanced Security!

Avançado - Backup e Restauração

Backup e Restauração de Dados e Configurações

Você pode fazer backup ou restaurar os dados e configurações do TSplus Advanced Security clicando no botão “Backup / Restore” na parte superior:





O backup será salvo na pasta **arquivos** localizado no diretório de configuração do TSplus Advanced Security. Por padrão, o **arquivos** a pasta está localizada aqui: C:\Program Files (x86)\TSplus-Security\archives

Usando a linha de comando para fazer backup e restaurar

A utilização do comando é descrita abaixo:

- **Backup** TSplus-Security.exe /backup [caminho opcional para um diretório]

Por padrão, o backup será criado no diretório de arquivos localizado na pasta de configuração do TSplus Advanced Security. No entanto, o backup pode ser salvo em uma pasta especificada. Caminhos relativos e absolutos são permitidos.

- **Restaurar** TSplus-Security.exe /restore [caminho para um diretório de backup]

O diretório de backup especificado deve conter uma pasta de dados e uma pasta de configurações, conforme criado pelo comando /backup.

Configurando backups

Por favor, note que você pode especificar as seguintes configurações avançadas no registro:

- O diretório de backup pode ser especificado na chave do registro. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath Por padrão, o diretório "archives" do diretório de configuração do Advanced Security será utilizado.
-

O número máximo de backups disponíveis pode ser especificado na chave do registro. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives Por padrão, o Advanced Security mantém os últimos 3 backups.

Migre seus dados e configurações para outro computador

Por favor, siga os passos abaixo para migrar o Advanced Security do computador A para o computador B:

1. No computador A, clique no botão de Backup para criar um novo backup. As configurações e os dados serão salvos no diretório de arquivos, localizado no diretório de configuração do advanced-security (normalmente C:\Program Files (x86)\TSplus-Security\archives).

2. Copie a nova pasta de backup criada (por exemplo, chamada backup-2019-09-11_14-37-31), incluindo todo o conteúdo, do diretório de arquivos no computador A para o diretório de arquivos no computador B.

3. No computador B, na janela de Backup / Restauração, na seção "Restaurar", selecione o nome do backup relevante a ser restaurado.

4. Em seguida, clique em Restaurar Apenas Configurações para restaurar as configurações. Alternativamente, é possível clicar em Restaurar para restaurar todos os dados e configurações, o que não é recomendado para uma migração, mas é útil para restaurar a segurança avançada no computador A.

5. Aguarde no máximo 2 minutos para que as configurações sejam recarregadas pelos recursos de segurança avançada.

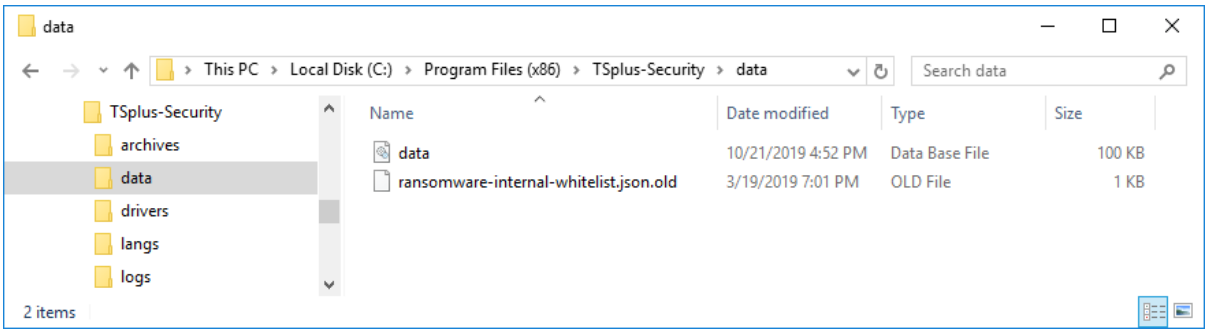
Banco de dados

Um banco de dados armazena Eventos, endereços IP, relatórios de ataques de Ransomware e listas de permissões de programas.

Este banco de dados está armazenado em **dados** pasta localizada no diretório de configuração do TSplus Advanced Security.

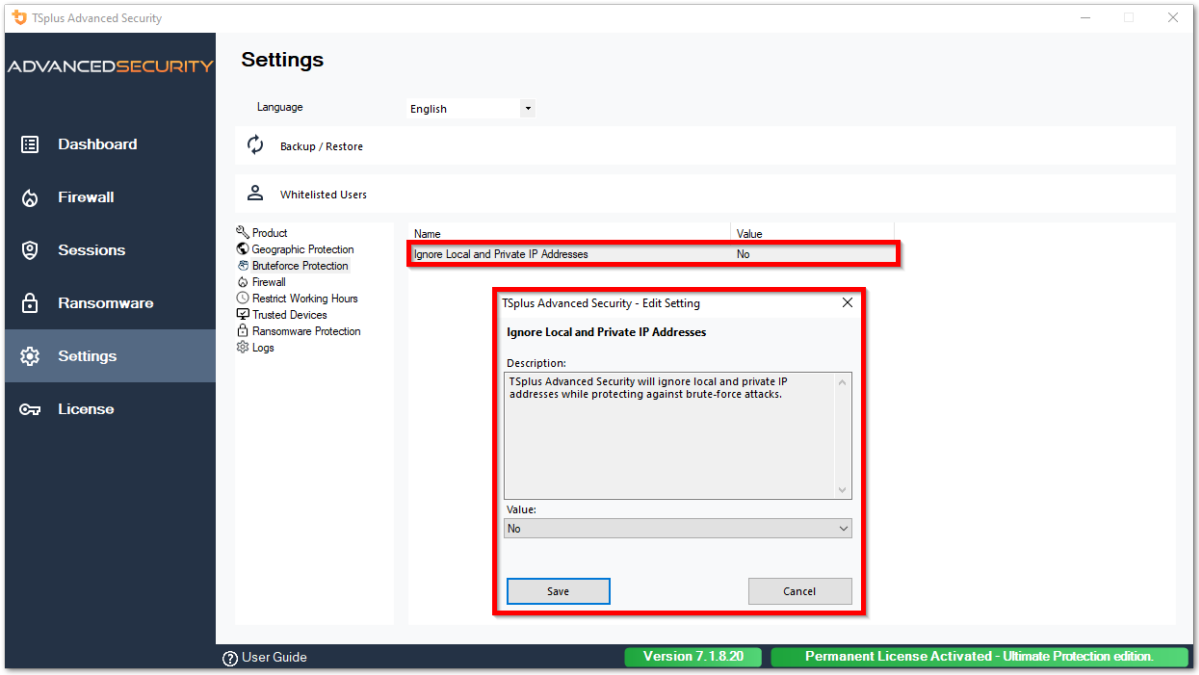
- Segurança Avançada da versão 5 e anterior à versão 5.3.10.6 usa um motor de banco de dados LiteDB .

- Segurança Avançada acima da versão 5.3.10.6 usa um motor de banco de dados SQLite .



Avançado - Proteção contra Bruteforce

O **Proteção contra Bruteforce** a guia permite que você Ignorar endereços IP locais e privados se desejar, alterando o valor padrão de "Não" para "Sim".

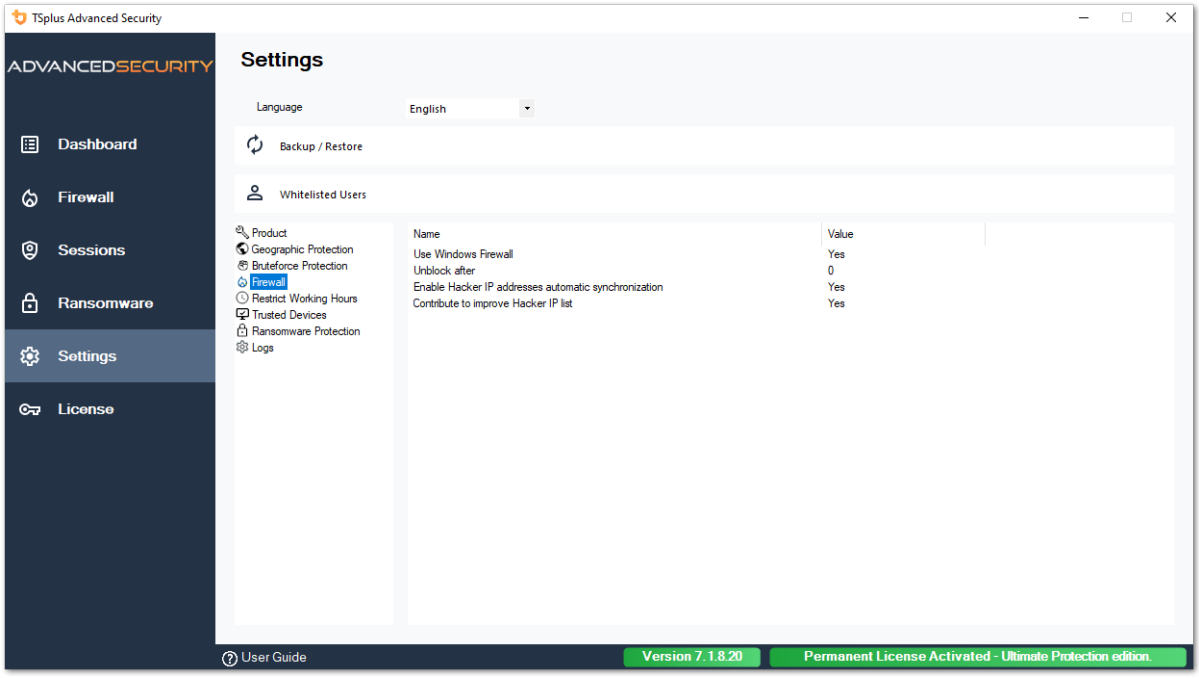


Avançado - Firewall

O **Firewall** a guia permite que você ative o **Firewall do Windows ou desative-o em favor do firewall integrado do TSplus Advanced Security** .

Desde a versão 4.4, um firewall embutido está incluído no TSplus Advanced Security.

Como orientação geral, se o Windows Firewall estiver ativado em seu servidor, você deve usá-lo para aplicar as regras do TSplus Advanced Security (padrão). Se você instalou outro firewall, deve ativar o firewall embutido do TSplus Advanced Security.



Use o Firewall do Windows Para ativar o firewall embutido, vá para Configurações > Avançado > Produto > Usar Firewall do Windows e defina o valor como: Não Se Sim, então os endereços IP ofensivos serão bloqueados usando o Firewall do Windows. O firewall do TSplus Advanced Security será utilizado caso contrário.

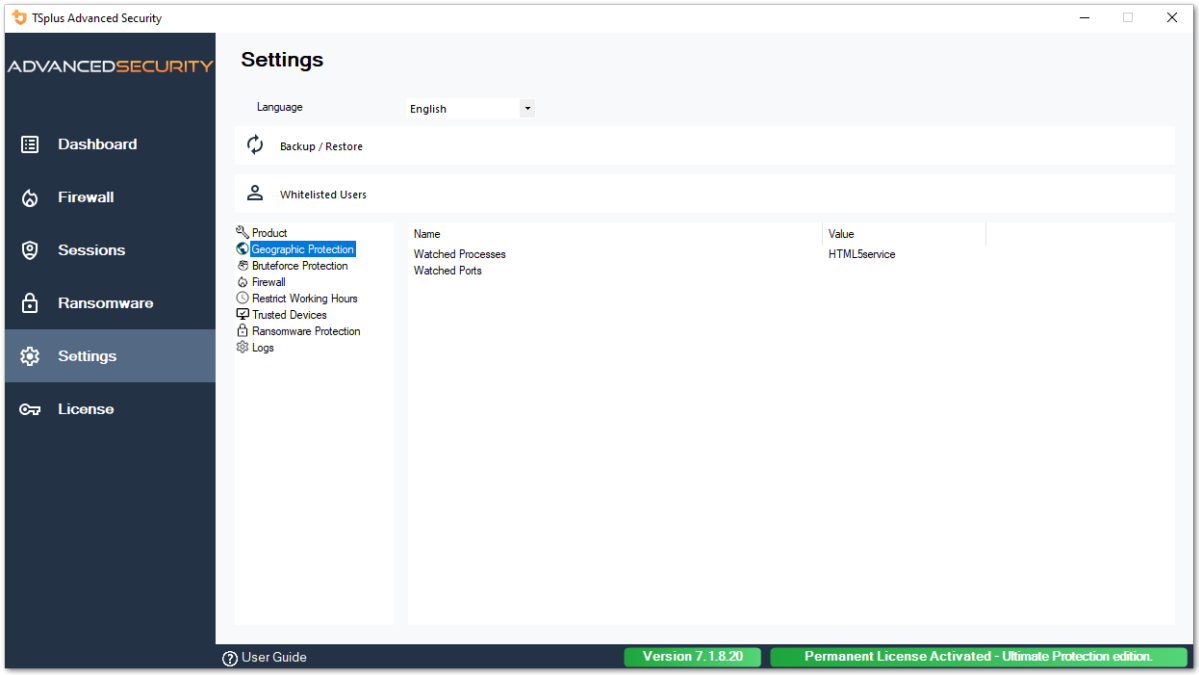
Desbloquear após Altere esta configuração para desbloquear automaticamente endereços IP após um determinado período de tempo (em minutos). O valor padrão é 0, desativando este recurso. Valor: 0

Ativar a sincronização automática de endereços IP de hackers Mantenha sua máquina protegida contra ameaças conhecidas, como ataques on-line, abuso de serviços on-line, malware, botnets e outras atividades eletrônicas com a Proteção de IP do Hacker. A assinatura dos Serviços de Suporte e Atualizações é necessária. Valor: Sim

Contribua para melhorar a lista de IPs de hackers Permitir que o TSplus Advanced Security envie estatísticas de uso anônimas para melhorar a proteção contra IPs de hackers.
Valor: Sim

Proteção Geográfica Avançada

O **Proteção Geográfica** a guia permite que você adicione ou remova processos que estão sendo monitorados pelo Proteção Geográfica recurso.



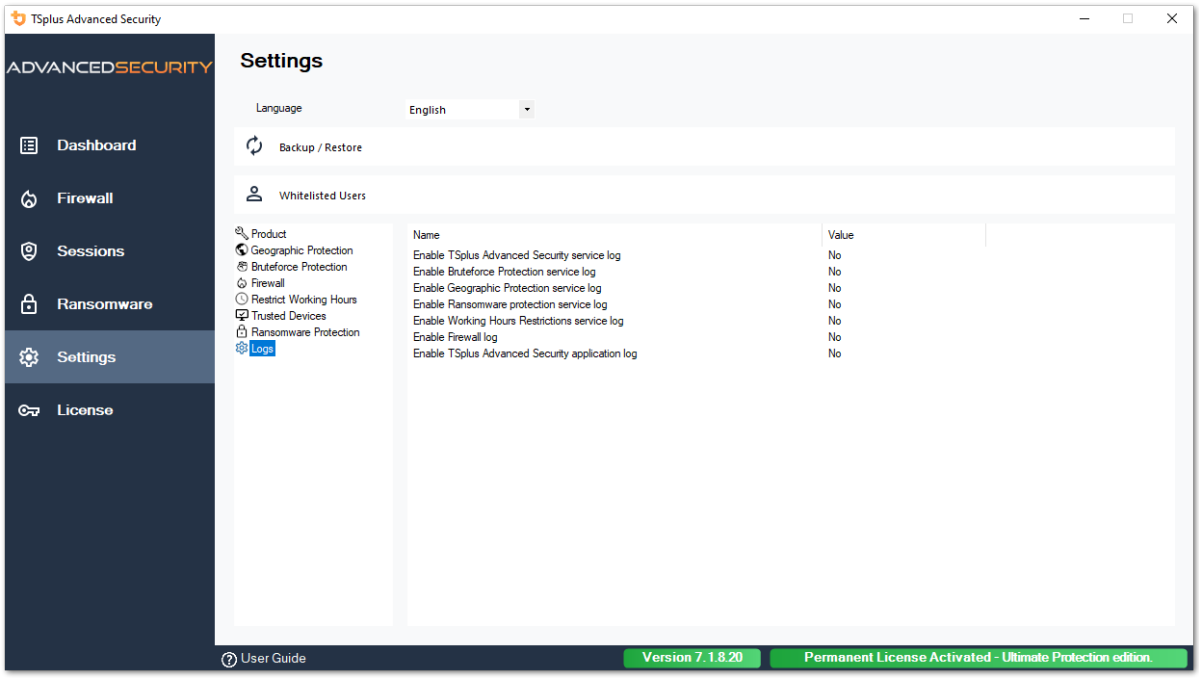
Por padrão, o serviço HTML5 é monitorado.

O **Portas Monitoradas** as configurações permitem que você adicione portas monitoradas pelo Proteção Geográfica feature. Por padrão, a Proteção Geográfica escuta as portas padrão usadas para se conectar remotamente a um servidor. Essas portas incluem RDP (3389), Telnet (23) e portas VNC. A Proteção Geográfica suporta os seguintes provedores de VNC: Tight VNC, Ultra VNC, Tiger VNC e Real VNC, que não estão relacionados de forma alguma com TSplus.

Avançado - Registros

O **Registros** a guia permite que você habilitar ou desabilitar logs de serviços e recursos Existem logs para encontrar mais facilmente a origem dos erros encontrados no TSplus Advanced Security.

Para recuperar os logs, abra um Explorer e navegue até o **registros** pasta do diretório de instalação do TSplus Advanced Security. Por padrão, os logs estarão localizados aqui: **C:\Program Files (x86)\TSplus-Security\logs**



Ativar ou desativar Serviço e logs de aplicativos do TSplus Advanced Security , que são respectivamente o serviço de configuração global que roda em segundo plano e o log para a interface do aplicativo.

Você também pode ativar logs correspondentes aos recursos do TSplus Advanced Security:

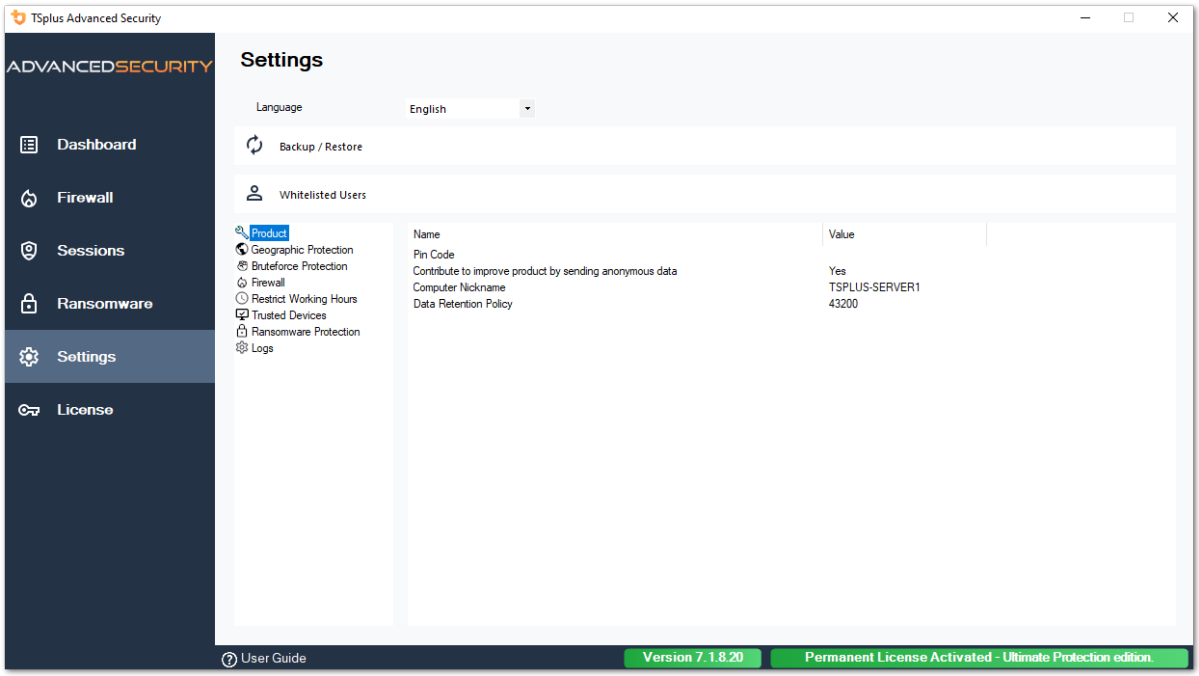
- Serviço
- Proteção contra Bruteforce
- Proteção Geográfica
- Proteção contra Ransomware

- Restringir Horário de Trabalho
- Firewall..
- Aplicativo

Todos os logs estão desativados por padrão. Os logs correspondem a diferentes componentes, nossa equipe de suporte informará qual valor colocar de acordo com o problema encontrado.

Avançado - Produto

O **Produto** a guia permite que você adicionar um código PIN ao aplicativo :



Clique em Salvar. O código PIN será necessário na próxima vez que você iniciar o aplicativo.

Você também pode **contribuir para melhorar o produto** , enviando dados anônimos (ativado por padrão): SIM

Os seguintes dados serão coletados em caso de um ataque de Ransomware:

- Versão do TSplus Advanced Security.
- Versão do Windows.
- Caminhos de arquivos suspeitos que levam ao ataque de ransomware.

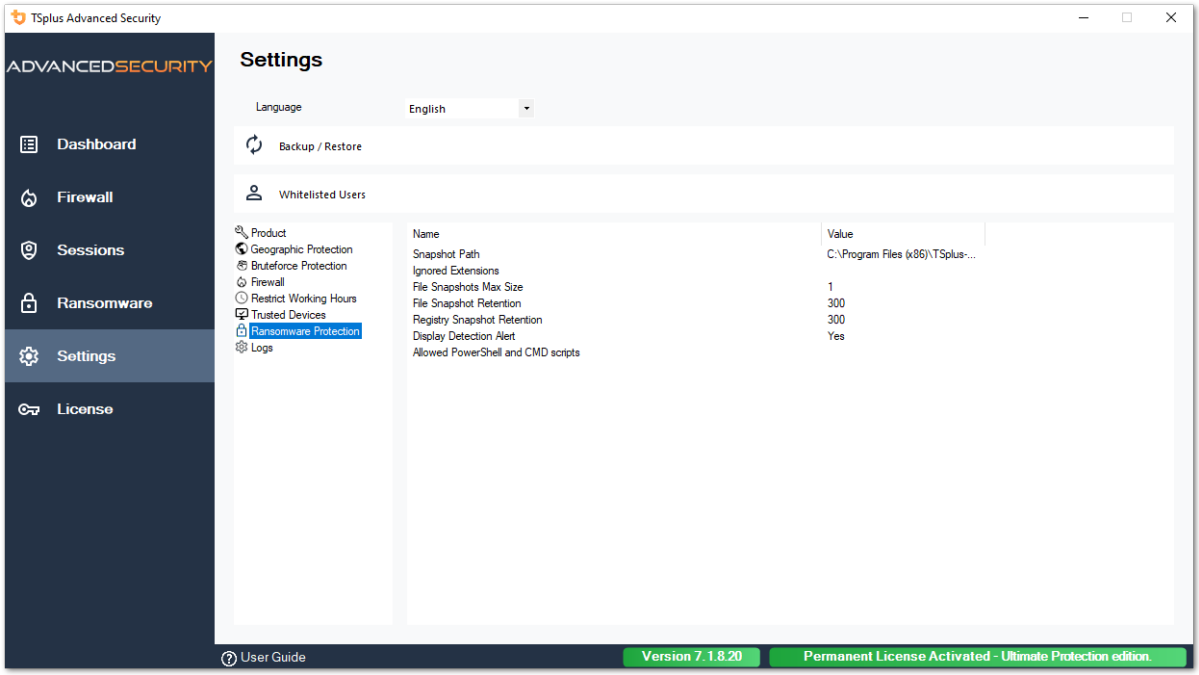
Modificando o **Apelido do computador** também é possível.

O **Política de Retenção de Dados** define o período de tempo após o qual os eventos do TSplus Advanced Security são removidos do banco de dados. Um backup é realizado antes de cada limpeza do banco de dados. Esta política é definida em minutos. A política de retenção de

dados padrão é de 259.200 minutos, ou 6 meses.

Proteção Avançada contra Ransomware

O **Proteção contra Ransomware** a guia permite que você configurar as propriedades do instantâneo e definir as extensões de arquivo ignoradas para o recurso de proteção contra ransomware.



Caminho do Instantâneo Defina o diretório onde a Proteção contra Ransomware armazena instantâneas de arquivos.

O valor padrão é: C:\Program Files (x86)\TSplus-Security\snapshots

Extensões Ignoradas Por padrão, a proteção contra ransomware ignora extensões bem conhecidas de arquivos temporários para atividade de ransomware. Veja a lista aqui Você pode definir nomes de extensão personalizados no campo de valor (separados por ponto e vírgula):

Tamanho Máximo do Snapshot do Arquivo Tamanho máximo de instantâneas de arquivo define o espaço máximo permitido para reter instantâneas de arquivo.

O tamanho é expresso em porcentagem do espaço total disponível no disco onde o Caminho do

Snapshot reside.

Retenção de Snapshot de Arquivo A retenção de instantâneos de arquivo define, em segundos, a política de retenção de um instantâneo de arquivo.

Uma vez que o período de retenção tenha terminado, o instantâneo do arquivo é excluído. Por padrão, 300 segundos (ou seja, 5 minutos)

Retenção de Snapshot do Registro A Retenção de Snapshot do Registro define, em segundos, a política de retenção de um snapshot do registro. Uma vez que o período de retenção tenha terminado, o snapshot do registro é excluído. Por padrão, 300 segundos (ou seja, 5 minutos)

Alerta de Detecção de Exibição Exibir uma janela de mensagem de alerta na área de trabalho do usuário quando a proteção contra ransomware detectar e parar um ataque.

Scripts do PowerShell e CMD permitidos Listas de scripts PowerShell e CMD permitidos mostram os caminhos completos dos arquivos dos scripts PowerShell e CMD que podem ser executados na máquina.

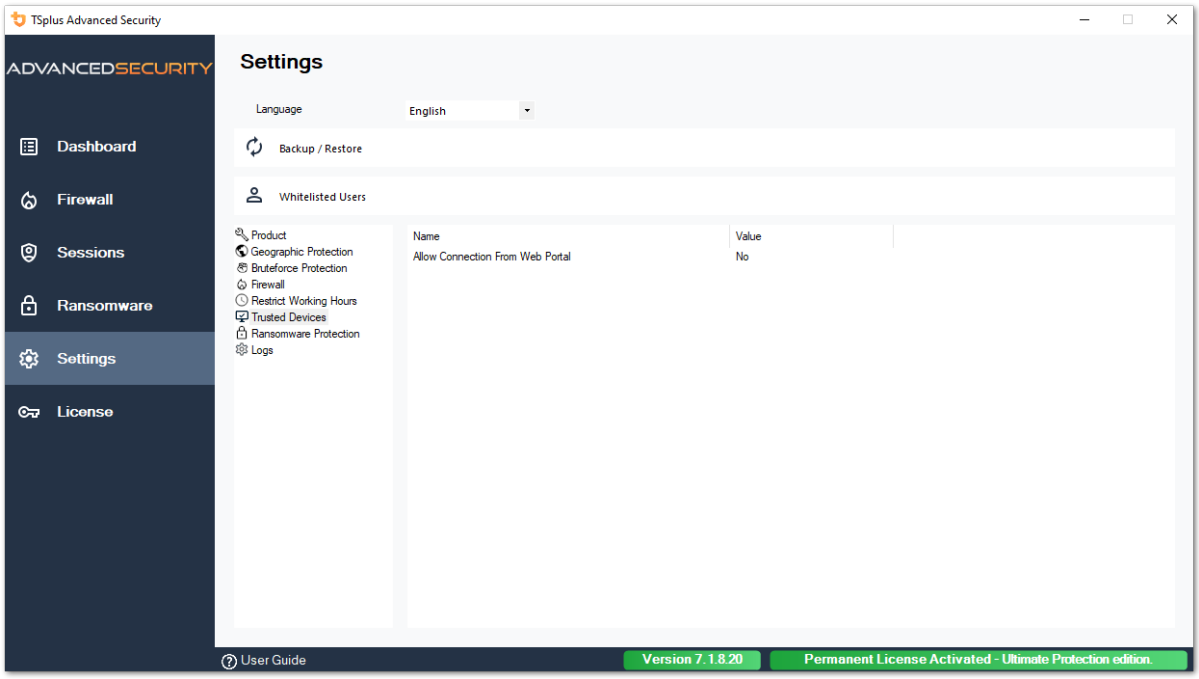
A execução de scripts permitidos não acionará a proteção contra Ransomware (separados por ponto e vírgula).

Avançado - Dispositivos Confiáveis

O **Dispositivos Confiáveis** a guia permite que você ative conexões a partir do Portal Web do TSplus Remote Access.

Nota :

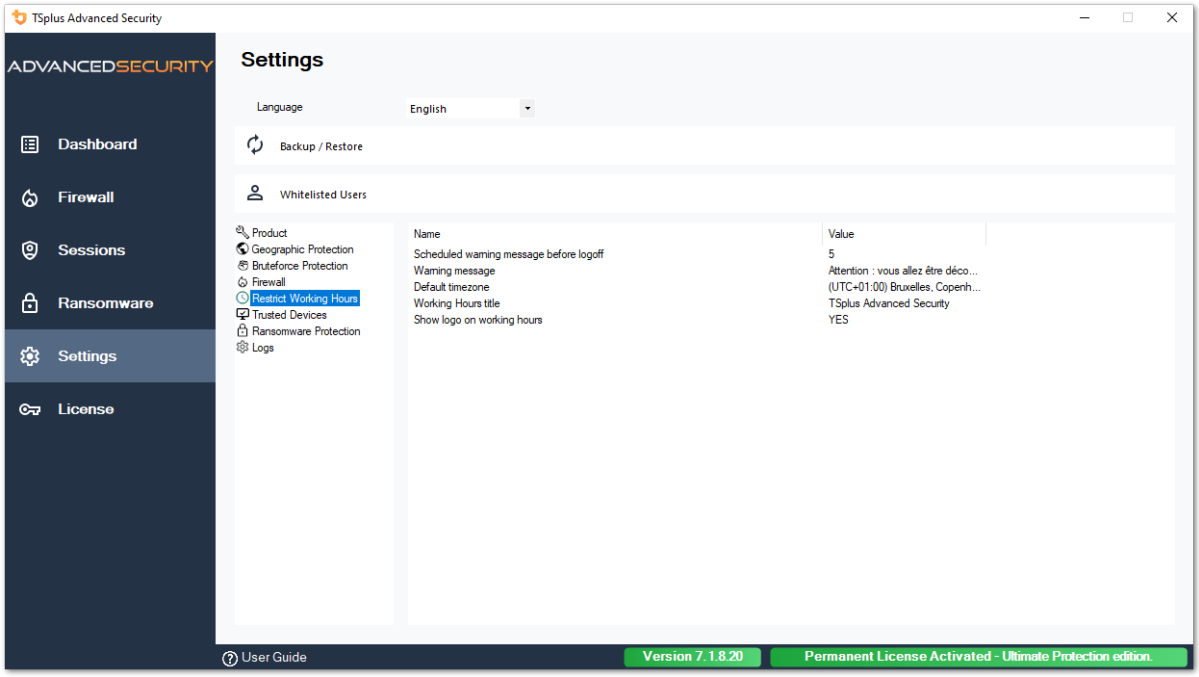
-Dispositivos Confiáveis não é compatível com sessões HTML5. -Dispositivos Confiáveis não é compatível com dispositivos móveis iOS / Android, pois eles ocultam seus nomes de host reais. -O nome do host da máquina remota é definido pela própria máquina. A máquina provavelmente ocultará ou modificará isso de acordo com sua configuração.



Os Dispositivos Confiáveis do TSplus Advanced Security não conseguem resolver o nome do cliente se a conexão for iniciada a partir do portal Web do TSplus Remote Access. Portanto, os Dispositivos Confiáveis bloquearão qualquer conexão do Portal Web por padrão. Defina esta configuração como "Sim" para permitir conexões a partir do portal Web. Esteja ciente de que essa ação diminuirá a segurança do seu servidor.

Avançado - Restringir Horários de Trabalho

O **Restringir Horário de Trabalho** a guia permite que você Agende uma mensagem de aviso antes que o usuário seja desconectado .



Mensagem de aviso agendada Você pode configurar em número de minutos antes que o usuário seja desconectado automaticamente. Por padrão, está definido para 5 minutos.

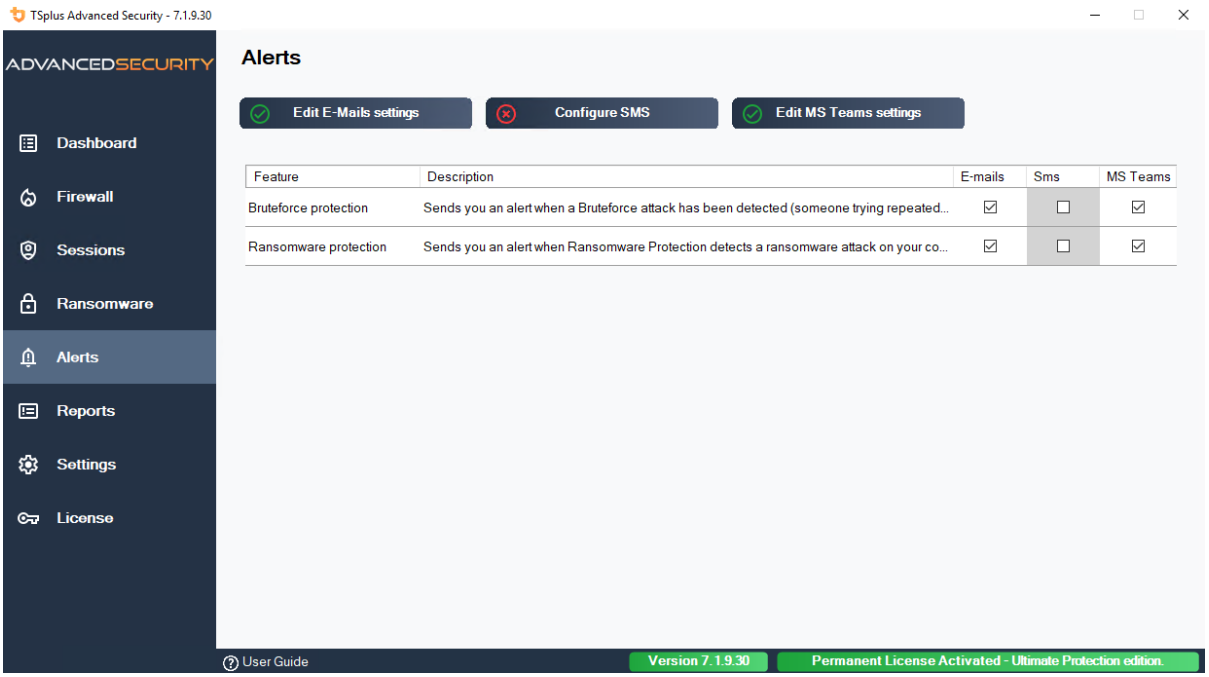
Mensagem de aviso Uma mensagem de aviso pode ser definida a seu critério, com marcadores nomeados %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% e %ENDINGHOURS%, que serão respectivamente substituídos pelo número atual de minutos antes do fechamento da sessão, o dia atual, o horário de início e o horário de término do dia atual.

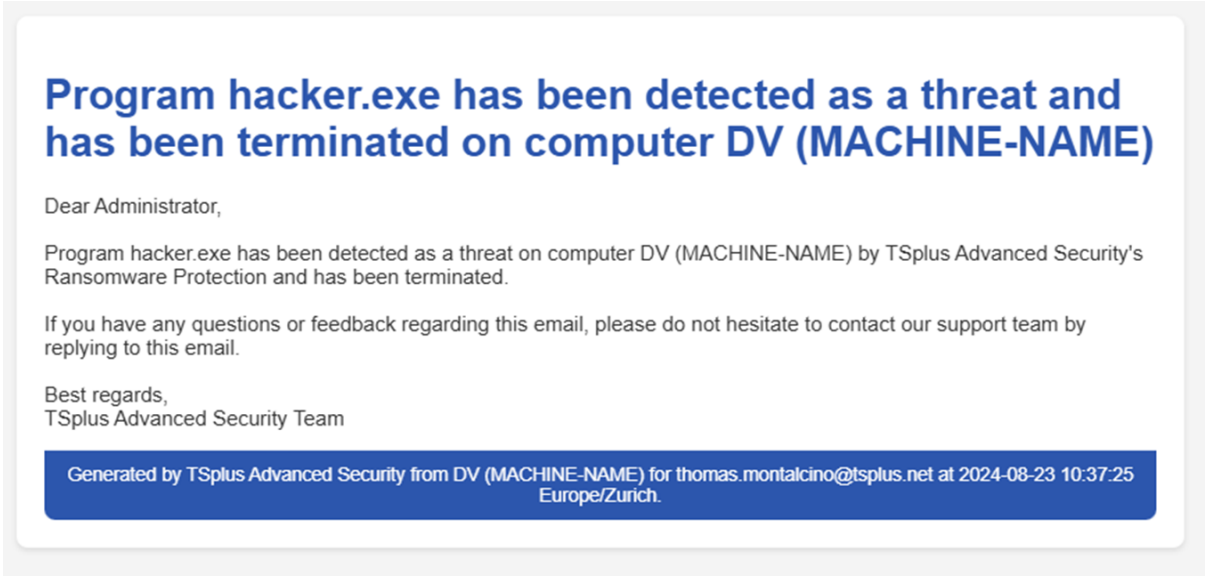
Fuso horário do servidor padrão Um fuso horário de servidor padrão pode ser definido para aplicar as regras de horário de trabalho de acordo, selecionando o correspondente na lista suspensa.

Horário de trabalho título Título do formulário exibido ao usuário final, quando suas horas de trabalho estão terminando (padrão: TSplus Advanced Security)

Mostrar logotipo durante o horário de trabalho Se definido como "sim", o logotipo é exibido na forma apresentada ao usuário final, quando suas horas de trabalho estão terminando (padrão: "sim")

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.

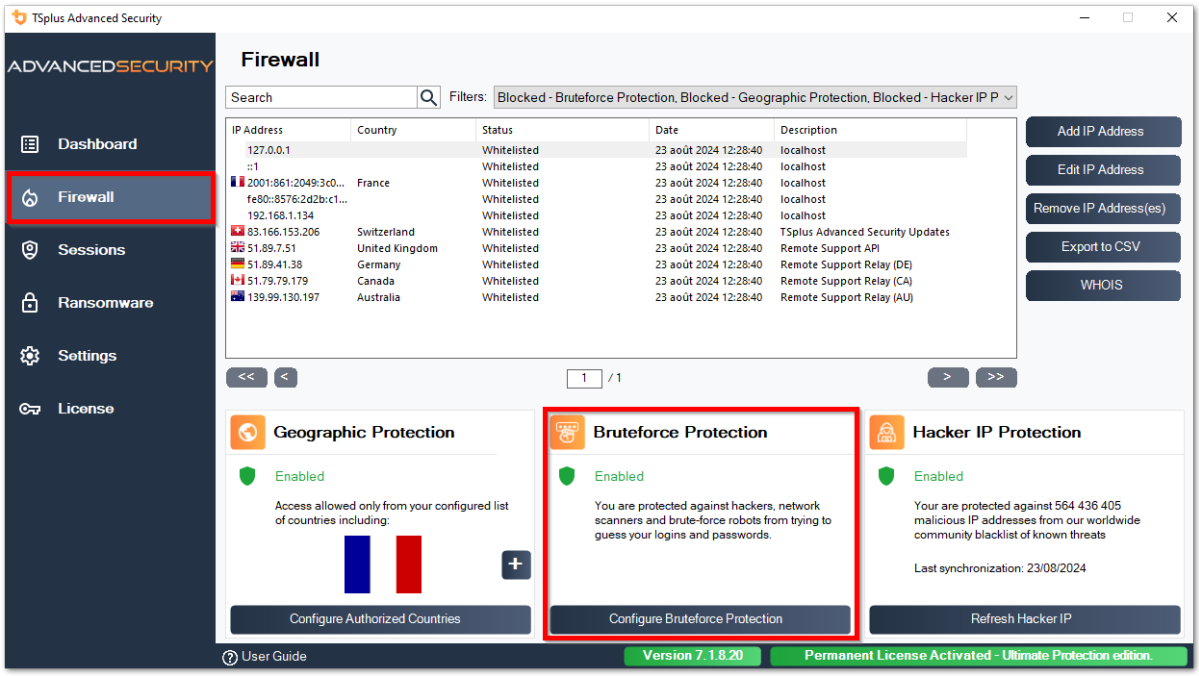
Best regards,
TSplus Advanced Security Team

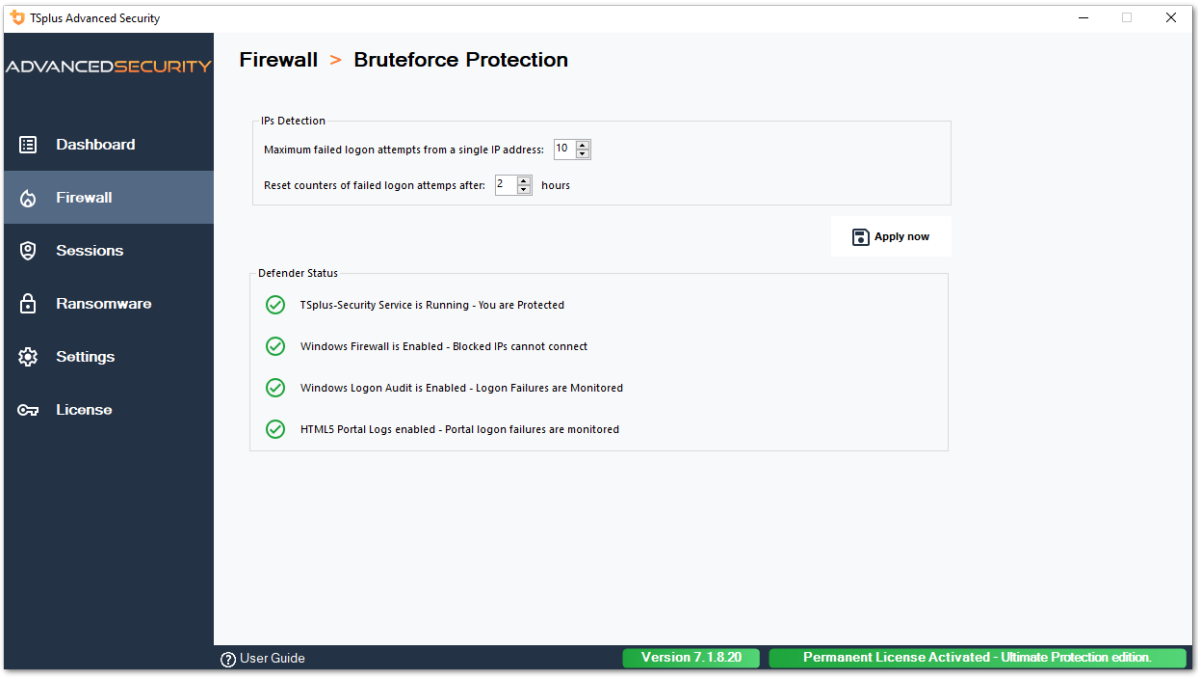
Generated by TSplus Advanced Security from DV (MACHINE-NAME) for thomas.montalcino@tsplus.net at 2024-08-23 10:37:25 Europe/Zurich.

Proteção contra Bruteforce

A Proteção contra Bruteforce permite que você proteja seu servidor público de hackers, scanners de rede e robôs de força bruta que tentam adivinhar seu login e senha de Administrador. Usando logins atuais e dicionários de senhas, eles tentarão automaticamente fazer login em seu servidor centenas a milhares de vezes a cada minuto.

Com este RDP Defender, você pode monitorar as tentativas de login com falha do Windows e automaticamente colocar em lista negra os endereços IP infratores após várias falhas.





- Você pode definir o **máximo de tentativas de logon falhadas de um único endereço IP dentro do bloco de Detecção de IPs** (por padrão, é 10), assim como o tempo de reinício para contadores de tentativas de logon falhadas (por padrão, é 2 horas).

- Na parte inferior desta janela, você pode ver o **Status do defensor** onde você pode verificar se as falhas de logon do Portal Web HTML5, as falhas de logon do Windows estão sendo monitoradas e se o Firewall do Windows e o serviço de segurança avançada estão habilitados.

Neste caso, como em nosso exemplo, todos os status estão marcados.

- **Gerenciar endereços IP bloqueados** Você pode, é claro, configurá-lo para atender às suas necessidades, por exemplo, adicionando o seu próprio endereço IP da estação de trabalho em o Lista de IPs permitidos , então esta ferramenta nunca o bloqueará. Você pode adicionar quantos endereços IP quiser na lista de permissões. Esses endereços nunca serão bloqueados pela Proteção contra Bruteforce.

- Você pode **ignorar endereços IP locais e privados** alterando a configuração padrão no Configurações > Avançado > Aba de proteção contra força bruta

Nota: Se você notar que a proteção contra bruteforce bloqueou 10 endereços IP por dia e que agora, isso não acontece mais; e bloqueia um, dois ou até não bloqueia nenhum endereço, isso é na verdade normal. De fato, antes da instalação do advanced-security, o servidor com uma

porta RDP disponível publicamente é conhecido por todos os robôs, e muitos robôs tentam as senhas atuais e as que vêm de dicionários. Quando você instala o advanced-security, esses robôs estão sendo progressivamente bloqueados, para que um dia:

- A maioria dos robôs ativos já está bloqueada e não está interessada no servidor, mesmo os novos.
- Além disso, o servidor não aparece mais na lista de servidores publicamente conhecidos.

Linhas de comando

Estamos satisfeitos em fornecer a você um conjunto abrangente de ferramentas de linha de comando projetadas para aumentar a flexibilidade e a eficiência do nosso software. Essas ferramentas permitem que os usuários criem scripts e automatizem várias funcionalidades, adaptando o software para atender às suas necessidades e fluxos de trabalho específicos.

Explore as possibilidades e otimize sua experiência com nossas opções de linha de comando.

Você só precisa executar as seguintes linhas de comando como um Administrador elevado. Como lembrete, TSplus-Security.exe está localizado na seguinte pasta **C:\Program Files (x86)\TSplus-Security** por padrão.

Gestão de Licenças

Para realizar operações em licenças, substitua o programa AdminTool.exe apresentado na documentação a seguir pelo programa TSplus-Security.exe localizado no diretório de configuração do Advanced Security (geralmente **C:\Program Files (x86)\TSplus-Security**).

- Ativação de licença
- Redefinição de licença após clonagem de uma VM
- Ativação de licença por volume
- Ativando e desativando a licença por volume
- Atualização de licença por volume
- Exibir créditos de licença restantes para uma chave de Licença por Volume
- Exibir créditos de suporte restantes para uma chave de Licença por Volume

---

Configurar servidor proxy: /proxy /set

Sintaxe:

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

Descrição:

Comando /proxy /set é usado para configurar um servidor proxy para acesso à Internet.

Parâmetros:

- /host o host de destino pode ser um valor predefinido (“ie” ou “none”) ou um valor definido pelo usuário (por exemplo: 127.0.0.1 ou proxy.company.org). Este parâmetro é obrigatório
- /port o número da porta usado para se conectar ao servidor proxy. Necessário se o valor do nome do host for um valor definido pelo usuário.
- /username o nome de usuário para se conectar ao servidor proxy. Esta configuração é opcional
- /password a senha do usuário deve ser fornecida se um nome de usuário tiver sido definido. No entanto, seu valor pode estar vazio

Exemplos:

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

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

Para mais informações, por favor, vá para Como configurar um Servidor Proxy para Acesso à Internet?

Backup de dados e configurações: /backup

Sintaxe:

TSplus-Security.exe /backup [CaminhoDoDiretórioDeDestino]

Descrição:

Comando /backup é usado para fazer backup dos dados e configurações do TSplus Advanced Security.

Por padrão, o backup será criado no diretório de arquivos localizado no diretório de configuração do Advanced Security (por exemplo: C:\Program Files (x86)\TSplus-Security\archives).

Parâmetros:

- DestinationDirectoryPath para fazer backup em outro diretório que não o padrão. Caminhos relativos e absolutos são permitidos.

Exemplos:

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

Para mais informações, por favor, vá para Avançado - Backup e Restauração

---

Restaurar dados e configurações: /restore

Sintaxe:

TSplus-Security.exe /restore [Caminho do Diretório de Backup]

Descrição:

Comando /restore é usado para restaurar dados e configurações do TSplus Advanced Security.

O caminho do diretório de backup especificado deve ser criado pelo comando /backup ou pela funcionalidade de Backup da aplicação.

Parâmetros:

- Backup Directory Path o caminho onde está localizado o diretório de backup para restaurar.

Exemplos:

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

Para mais informações, por favor, vá para Avançado - Backup e Restauração

---

Remover e desbloquear todos os endereços IP bloqueados: /unblockall

Sintaxe:

TSplus-Security.exe /desbloqueartodos

Descrição:

Comando /unblockall é usado para remover todos os endereços IP bloqueados do firewall do TSplus Advanced Security e desbloqueá-los do firewall do Microsoft Windows Defender, se necessário.

Exemplos:

TSplus-Security.exe /desbloqueartodos

Para mais informações, por favor, vá para Firewall

Remover e desbloquear endereços IP especificados: /unblockips

Sintaxe:

TSplus-Security.exe /desbloquearips [endereços IP]

Descrição:

Comando /unblockips é usado para remover todos os endereços IP bloqueados especificados do firewall do TSplus Advanced Security e desbloqueá-los do firewall do Microsoft Windows Defender, se necessário.

Este comando não tem efeito sobre os endereços IP já bloqueados pela proteção de IP do Hacker. Se você ainda quiser desbloquear um desses endereços, use o comando de whitelist.

Parâmetros:

- IP addresses a lista de endereços IP ou faixas de IP a serem desbloqueados (separados por vírgula ou ponto e vírgula).

Exemplos:

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 mais informações, por favor, vá para Firewall

Bloquear endereços IP especificados: /blockips

Sintaxe:

TSplus-Security.exe /blockips [endereços IP] [Descrição Opcional]

Descrição:

Comando /blockips é usado para bloquear todos os endereços IP especificados usando o firewall do TSplus Advanced Security e bloqueá-los usando o firewall do Microsoft Windows Defender, se configurado.

Parâmetros:

- IP addresses a lista de endereços IP ou faixas de IP a serem bloqueados (separados por vírgula ou ponto e vírgula).
- Optional Description uma descrição opcional que será adicionada para cada entrada.

Exemplos:

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Locais de trabalho do John”

Para mais informações, por favor, vá para Firewall

Adicionar endereços IP à lista de permissões: /addwhitelistedip

Sintaxe:

TSplus-Security.exe /addwhitelistedip [endereços IP] [Descrição Opcional]

Descrição:

Comando /addwhitelistedip é usado para adicionar endereços IP especificados aos endereços IP autorizados do firewall do TSplus Advanced Security e desbloqueá-los do firewall do Microsoft Windows Defender, se necessário.

Parâmetros:

- IP addresses a lista de endereços IP ou faixas de IP para adicionar à lista de permissões (separados por vírgula ou ponto e vírgula).
- Optional Description uma descrição opcional que será adicionada para cada entrada.

Exemplos:

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Locais de trabalho do John”

Para mais informações, por favor, vá para Firewall

Adicionar um programa ou diretório à lista autorizada de proteção contra ransomware: /whitelist

Sintaxe:

TSplus-Security.exe /whitelist add [Caminhos Autorizados]

Descrição:

Comando /whitelist add é usado para adicionar caminhos de programas e diretórios especificados à lista autorizada da Proteção contra Ransomware do TSplus Advanced Security.

Parâmetros:

- Authorized Paths a lista de caminhos de programas e caminhos de diretórios a serem adicionados à lista de autorização de Proteção contra Ransomware do TSplus Advanced Security (separados por ponto e vírgula).

Exemplos:

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

Para mais informações, por favor, vá para Ação de Proteção contra Ransomware

---

Atualizar Proteção de IP do Hacker: / refreshipprotection

Sintaxe:

TSplus-Security.exe /refreshipprotection

Descrição:

Comando /refreshipprotection é usado para atualizar a lista de intervalos de IP bloqueados para o recurso de proteção contra IPs de hackers. A assinatura de Serviços de Suporte e Atualizações é necessária.

Exemplos:

TSplus-Security.exe /refreshipprotection

Para mais informações, por favor, vá para Proteção de IP de Hacker

Definir nível de log: /setloglevel

Sintaxe:

TSplus-Security.exe /setloglevel [Nível de Log]

Descrição:

Comando /setloglevel é usado para definir o nível de log para todos os componentes do Advanced Security.

Parâmetros:

- Log Level o nível de log entre os seguintes valores: TODOS, DEBUG, INFORMAÇÃO, AVISO, ERRO, FATAL, DESLIGADO

Exemplos:

TSplus-Security.exe /setloglevel ALL

Para mais informações, por favor, vá para Avançado > Registros

---

Adicionar dispositivos confiáveis: /addtrusteddevices

Sintaxe:

TSplus-Security.exe /addtrusteddevices [Configuração de Dispositivos Confiáveis]

Descrição:

Comando /addtrusteddevices é usado para adicionar dispositivos confiáveis programaticamente. Requer edição Ultimate.

Parâmetros:

- Trusted Devices Configuration O argumento é composto por uma lista de dispositivos confiáveis (separados por ponto e vírgula), estruturada da seguinte forma:

Nome de usuário e dispositivos são separados pelo caractere dois-pontos (:).

Detalhes do Usuário:

Tipo de usuário e nome de usuário completo são separados pelo caractere dois-pontos (:). Os tipos de usuário aceitos são "usuário" e "grupo".

Palavra-chave opcional "desativada": se incluída, os dispositivos confiáveis serão criados, mas as restrições estarão desativadas para este usuário. Se não mencionada, as restrições estão ativadas por padrão.

Detalhes do Dispositivo:

Nome do Dispositivo e Comentário Opcional: separados pelo caractere de igual (=).

Dispositivos são separados pelo caractere de dois pontos (:).

Exemplos:

TSplus-Security.exe /addtrusteddevices “user:WIN-A1BCDE23FGH\admin:disabled,device1name=este é um comentário para o dispositivo 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name=device4name=outro comentário;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name”

Para mais informações, por favor, vá para Dispositivos Confiáveis

---

Ativar dispositivos confiáveis configurados: / enabletrusteddevices

Sintaxe:

TSplus-Security.exe /enabletrusteddevices [Usuário ou Grupos]

Descrição:

Comando /enabletrusteddevices é usado para habilitar todos os dispositivos confiáveis configurados para os usuários e grupos especificados.

Parâmetros:

- User or Groups O argumento é uma lista de usuários e grupos (separados por ponto e vírgula). Dentro do nome de usuário, a separação entre o tipo de usuário (“usuário” e “grupo” são os únicos valores aceitos) e o nome de usuário completo é feita por dois pontos.

Exemplos:

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

Para mais informações, por favor, vá para Dispositivos Confiáveis

---

Desativar todos os dispositivos confiáveis: /disabletrusteddevices

Sintaxe:

TSplus-Security.exe /disabletrusteddevices [Usuário ou Grupos]

Descrição:

Comando /disabletrusteddevices é usado para desativar todos os dispositivos confiáveis configurados para os usuários e grupos especificados.

Parâmetros:

- User or Groups O argumento é uma lista de usuários e grupos (separados por ponto e vírgula). Dentro do nome de usuário, a separação entre o tipo de usuário (“usuário” e “grupo” são os únicos valores aceitos) e o nome de usuário completo é feita por dois pontos.

Exemplos:

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

Para mais informações, por favor, vá para Dispositivos Confiáveis

---

Configurar o driver de proteção contra ransomware: /setup-driver

Sintaxe:

TSplus-Security.exe /setup-driver

Descrição:

Comando /setup-driver instala o driver de proteção contra ransomware. Esta operação é normalmente realizada durante a instalação.

Exemplos:

TSplus-Security.exe /setup-driver

Para mais informações, por favor, vá para Proteção contra Ransomware

---

Desinstalar o driver de proteção contra ransomware: /uninstalldriver

Sintaxe:

TSplus-Security.exe /desinstalardriver

Descrição:

Comando /uninstalldriver desinstalar o driver de proteção contra ransomware. Esta operação é normalmente realizada durante a desinstalação do Advanced Security.

Exemplos:

TSplus-Security.exe /desinstalardriver

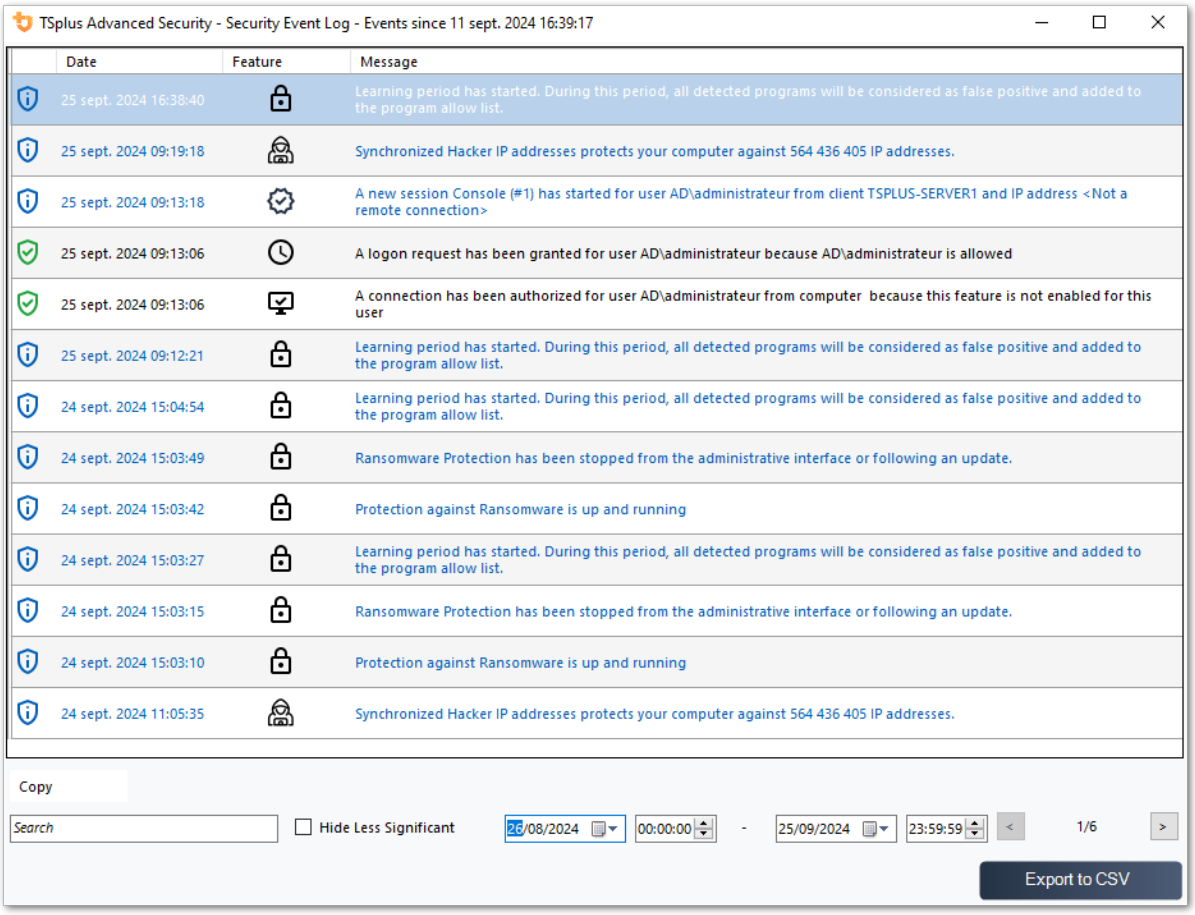
Para mais informações, por favor, vá para Proteção contra Ransomware

Eventos

Os eventos de segurança são uma ótima fonte de informação, pois exibem as operações realizadas pelo TSplus Advanced Security para proteger seu computador.

A janela de Eventos pode ser aberta a partir da janela principal do TSplus Advanced Security, clicando diretamente nos últimos 5 eventos exibidos ou na aba do painel. As informações exibidas na janela de Eventos são atualizadas automaticamente a cada poucos segundos.

A lista de eventos de segurança apresenta 4 colunas, que descrevem a gravidade, a data da verificação ou operação realizada, o ícone da funcionalidade associada e a descrição.



A descrição do evento muitas vezes explica por que a ação foi realizada ou não. Ações retaliatórias são frequentemente escritas em vermelho e destacadas com um ícone de escudo

vermelho.

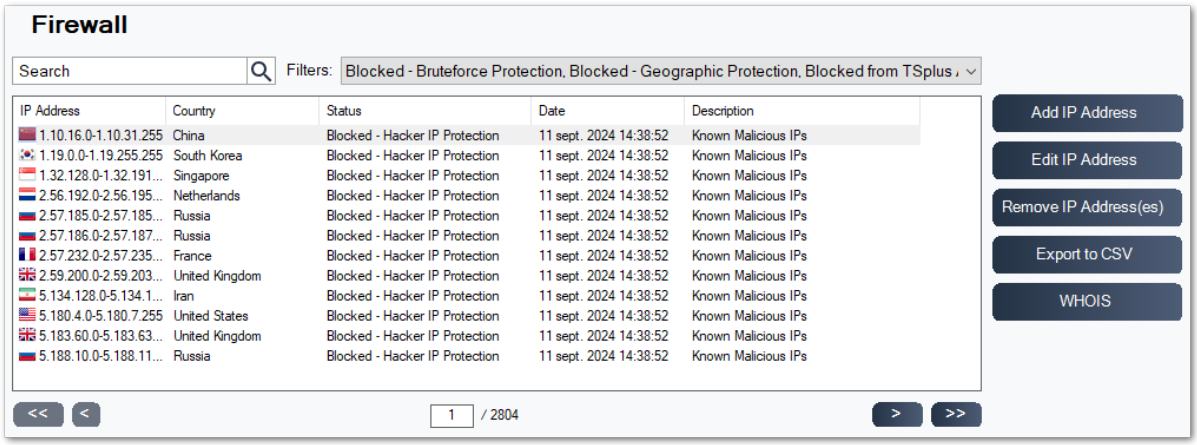
A janela de eventos pode ser movida e não impede você de usar o outro recurso do TSplus Advanced Security.

Navegando e Pesquisando através de eventos

- Uma busca global profunda agora está disponível para encontrar eventos específicos rapidamente.
- Ao lado da busca global, 2 filtros de seletores de data e hora filtram os eventos exibidos de acordo com a data em que o evento foi gerado.
- À direita, as setas permitem mudar de página e navegar para visualizar eventos mais antigos.

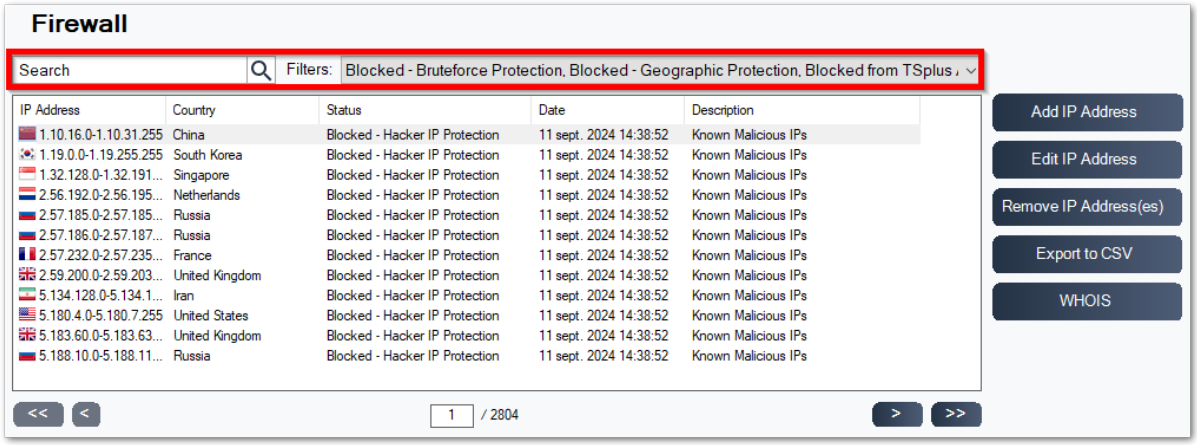
Firewall

A gestão de endereços IP é fácil com uma única lista para gerenciar tanto os endereços IP bloqueados quanto os endereços IP autorizados:



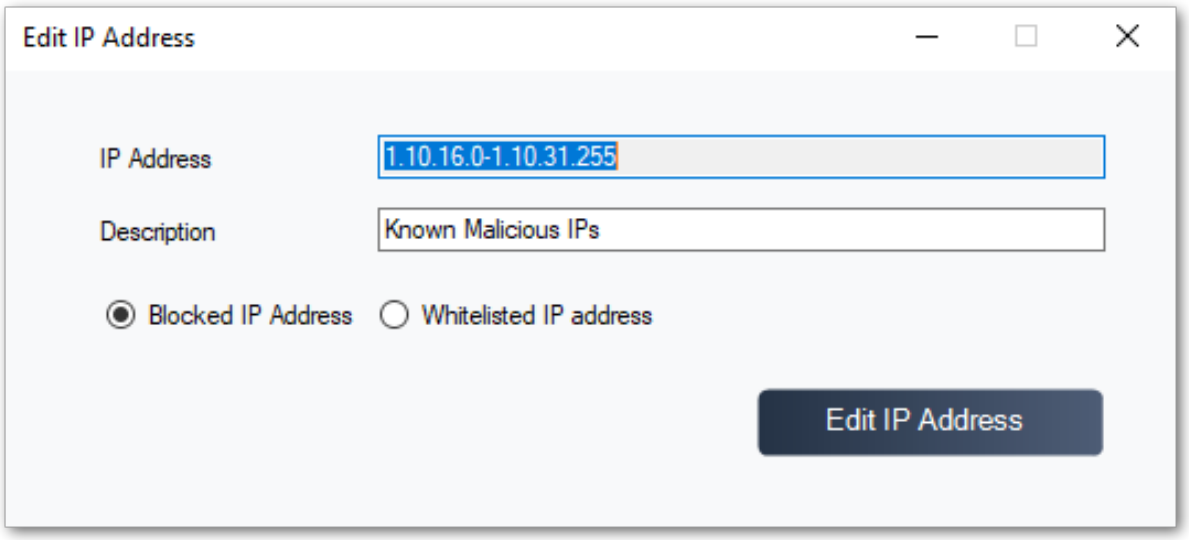
Por padrão, os endereços IPV4, IPV6 e todos os endereços de localhost do servidor são incluídos na lista de permissões.

Uma barra de pesquisa e filtro conveniente oferece capacidades de busca com base em todas as informações fornecidas.



Além disso, os administradores podem realizar ações em vários endereços IP selecionados com

um único clique. Entre os novos recursos introduzidos na gestão de endereços IP, você encontrará a possibilidade de fornecer descrições significativas para qualquer endereço IP.



Por último, os administradores agora podem desbloquear e adicionar a lista de permissões vários endereços IP bloqueados em uma única ação, clicando na guia “Adicionar Existente à Lista de Permissões”.

Usando a linha de comando para adicionar ou bloquear endereços IP e/ou faixas de IP

- Para poder **whitelist** endereços IP ou intervalo(s) de IP, o comando tem esta sintaxe:

TSplus-Security.exe addwhitelistedip [endereços IP] [descrição opcional]

Você pode adicionar vários endereços IP à lista de permissões, com um **vírgula ou delimitador de ponto e vírgula** Além disso, você pode especificar faixas de endereços IP, em vez de endereços IP simples. A sintaxe é: **x.x.x.x-y.y.y.y** Finalmente, você pode indicar uma descrição opcional da regra da lista de permissões.

Aqui está um exemplo de um 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 “Locais de trabalho do John”

- Para poder **bloquear** endereços IP ou intervalo(s) de IP, o comando tem uma sintaxe semelhante:

TSplus-Security.exe bloquear IPs [endereços IP] [descrição opcional]

- Para poder **desbloquear** endereços IP ou intervalo(s) de IP, o comando tem uma sintaxe semelhante:

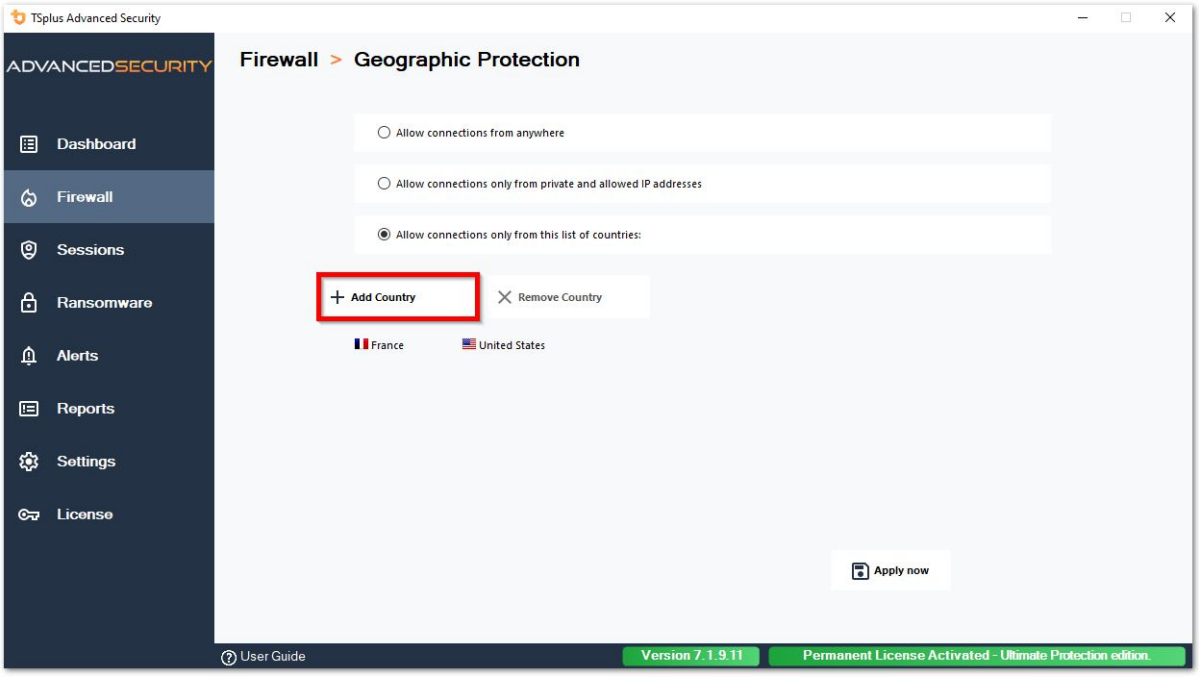
TSplus-Security.exe desbloquearips [endereços IP]

Este comando não tem efeito sobre os endereços IP já bloqueados pela proteção de IP do Hacker. Se você ainda quiser desbloquear um desses endereços, use o comando de whitelist.

Proteção Geográfica

Restringir o acesso de outros países

Para permitir o acesso remoto apenas de países específicos, selecione o botão “Permitir conexões apenas desta lista de países” e, em seguida, clique no botão “Adicionar país”.

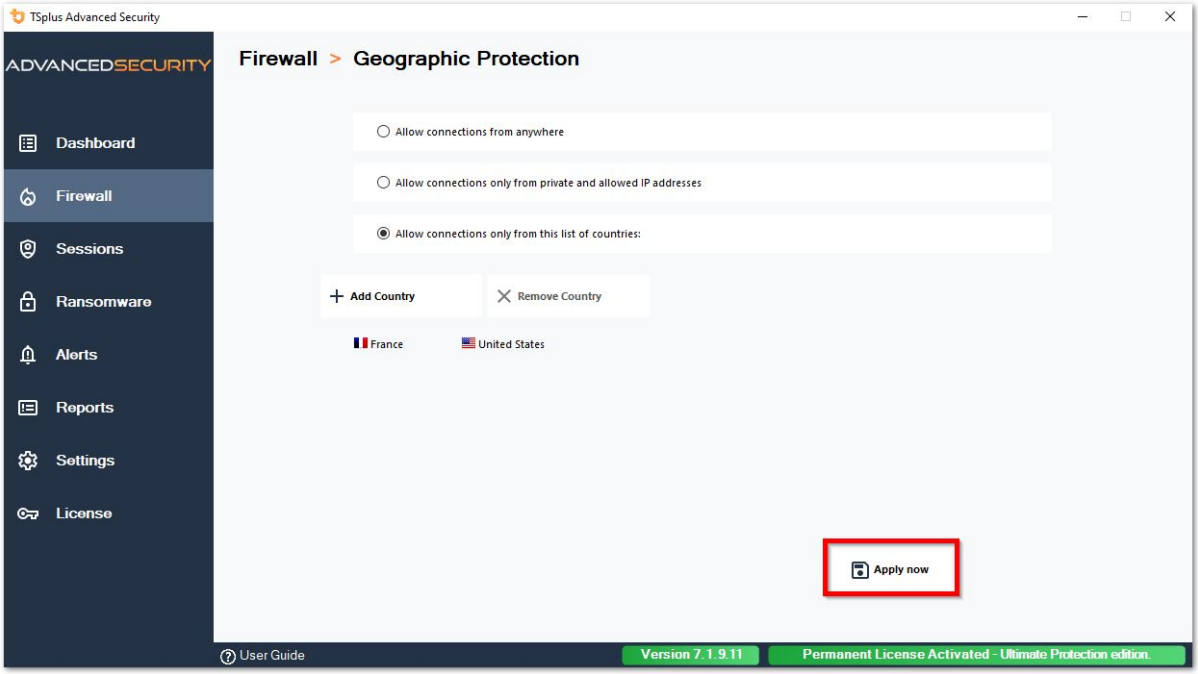


Uma janela pop-up com uma lista de países é aberta. Selecione o país que você deseja adicionar à lista.

Você pode optar por marcar a caixa abaixo para desbloquear todos os endereços IP anteriormente bloqueados para o país selecionado.

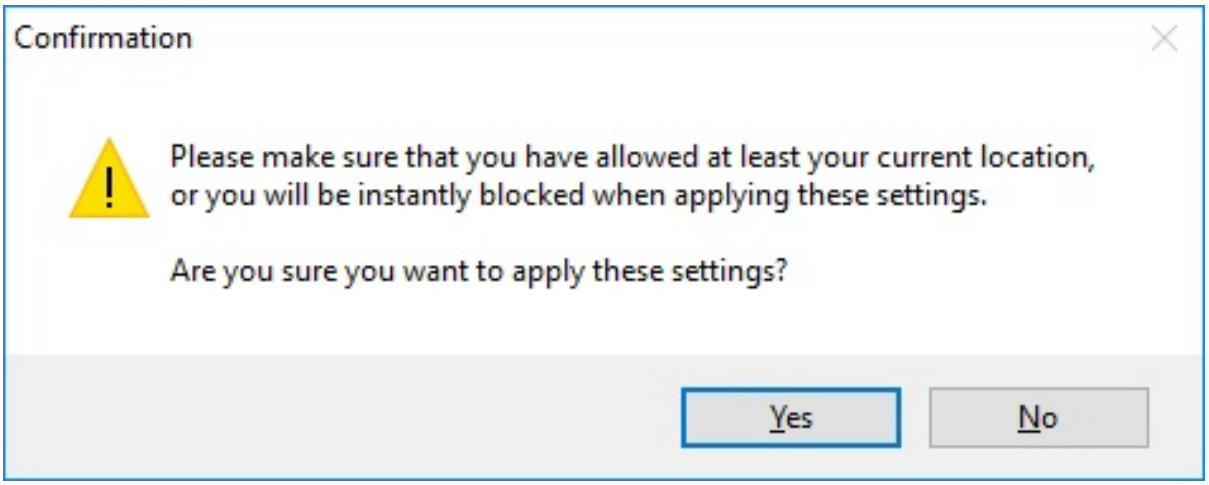
Clique no botão "Adicionar País" para retornar à tela principal do recurso.

Importante: Para salvar suas alterações, clique no botão “Aplicar”.



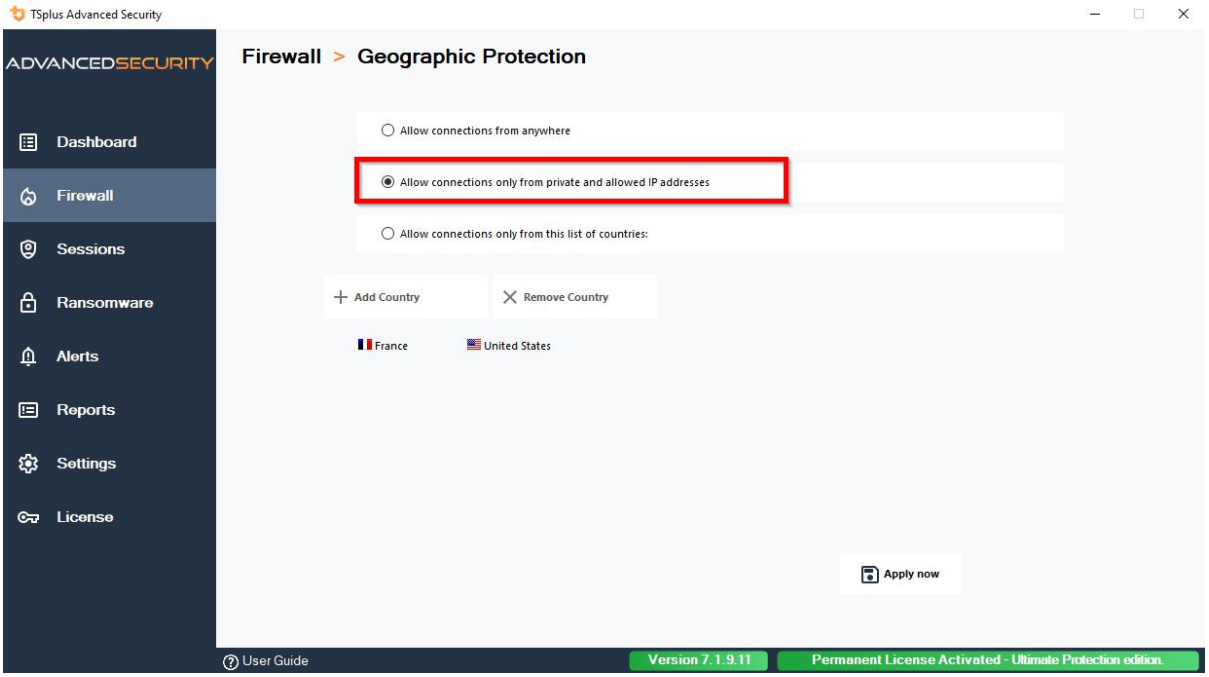
Neste exemplo, o acesso remoto é permitido para usuários que se conectam dos Estados Unidos e da França.

Uma mensagem de confirmação aparece para evitar o bloqueio do usuário conectado. Clique em "Sim" para confirmar e aplicar as alterações.



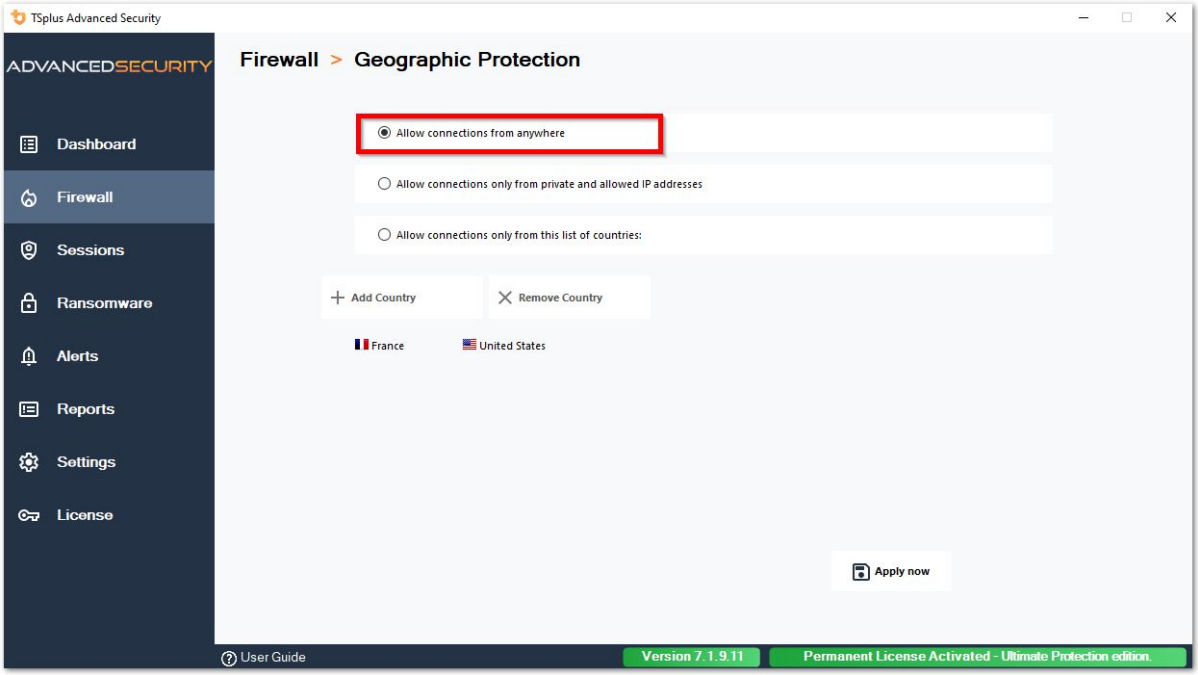
Restringir o acesso da internet

A Proteção Geográfica pode ser configurada para restringir o acesso à sua máquina apenas a redes privadas e endereços IP autorizados , como mostrado abaixo:



Desativar Proteção Geográfica

Por padrão, a Proteção Geográfica permite acesso para usuários conectando-se de todo o mundo:



Desbloqueando endereços IP bloqueados

Quando um endereço IP é bloqueado, ele aparece no Aba de firewall Endereços IP bloqueados podem ser desbloqueados e eventualmente adicionados à lista de endereços IP permitidos.

Se você for bloqueado, recomendamos que você tente se conectar de qualquer país que você permitiu no TSplus Advanced Security, por exemplo, conectando-se de outro servidor remoto ou usando um serviço de VPN. Você também pode usar uma sessão de console para se conectar, pois essa sessão não é uma sessão remota e não será bloqueada pelo TSplus Advanced Security.

Importante:

- Verifique se você selecionou o país de onde está atualmente conectado. Caso contrário, seu endereço IP será bloqueado rapidamente após a aplicação das configurações, desconectando-o sem qualquer esperança de reconectar-se novamente a partir do mesmo endereço IP.

- Considere adicionar seu próprio endereço IP à lista de permitidos. Endereços IP para evitar ser bloqueado por proteção geográfica ou Proteção contra Bruteforce recursos.

Entendendo a Proteção Geográfica

A Proteção Geográfica verifica a conexão de rede TCP de entrada, tanto IPv4 quanto IPV6 (exceto quando o modo de API do Windows legado está configurado).

Processos: A Proteção Geográfica escuta as conexões enviadas para o servidor Web do TSplus Remote Access por padrão, se instalado. O nome do processo correspondente é HTML5 Service. Se você deseja desativar sua monitorização ou verificar conexões destinadas a outros processos, vá para Configurações > Avançado > Proteção Geográfica .

Portas de rede: por padrão, a Proteção Geográfica escuta as portas padrão usadas para conectar-se remotamente a um servidor. Essas portas incluem RDP (3389), Telnet (23) e VNC. A Proteção Geográfica suporta os seguintes provedores de VNC: Tight VNC, Ultra VNC, Tiger VNC e Real VNC, que não estão relacionados de forma alguma com TSplus. Se você deseja desativar sua monitorização ou verificar conexões destinadas a outras portas, vá para Configurações > Avançado > Proteção Geográfica .

Mecanismos de detecção:

A Proteção Geográfica detecta conexões de entrada de países não autorizados usando três mecanismos de detecção diferentes:

- API do Windows
- Rastreamento de Eventos para Windows
- Firewall Integrado

Por um lado, o Event Tracing for Windows é uma instalação de rastreamento eficiente em nível de kernel que captura eventos de rede em tempo real. O Event Tracing for Windows é recomendado com o Firewall do Windows ativado (padrão).

Por outro lado, a API do Windows funciona muito bem em qualquer configuração de rede específica, mas pode adicionar uma pressão constante na CPU dependendo da quantidade de conexões ativas. Observe que a API do Windows ainda não é compatível com IPv6.

Firewall embutido permite a captura e o bloqueio de pacotes de rede enviados para a pilha de rede do Windows em modo de usuário. Quando o Firewall embutido é configurado para bloquear conexões indesejadas, é recomendável usá-lo para aplicar a proteção geográfica dos países permitidos.

Geolocalização: A Segurança Avançada inclui dados de geolocalização publicados pela MaxMind, disponíveis em http://www.maxmind.com Se você encontrar um endereço IP não registrado em seu país real, entre em contato diretamente com a MaxMind para resolver o problema.

Solução de problemas

Se você notar que a Proteção Geográfica não bloqueia conexões provenientes de um país que na verdade não está na lista de países autorizados, é certamente porque:

Antivírus: Para bloquear um endereço IP, a Proteção Geográfica adiciona uma regra de bloqueio no firewall do Windows. Portanto, primeiramente, o firewall deve estar ativo. Você também deve verificar se alguns parâmetros do firewall não estão sendo gerenciados por outro programa, como um antivírus. Nesse caso, você terá que desativar esse programa e reiniciar o serviço "Firewall do Windows". Você também pode entrar em contato com o editor do seu programa de terceiros e pedir que eles encontrem uma maneira de seu programa respeitar as regras ao ser adicionado ao firewall do Windows. Se você conhecer algum contato técnico de editor de software, estamos prontos para desenvolver esses "conectores" para o firewall. Entre em contato conosco .

VPN: Caso o cliente remoto utilize uma VPN, a Proteção Geográfica obterá um endereço IP escolhido pelo provedor de VPN. Como você sabe, os provedores de VPN usam relés em todo o mundo para permitir que seus usuários naveguem anonimamente. Alguns provedores de VPN permitem que os usuários definam o país do relé. Assim, usuários com provedores de VPN podem ser redirecionados através de um país não autorizado. Por exemplo, se um provedor de VPN escolher um IP do Sri Lanka, este país deve ser autorizado pela Proteção Geográfica. Além disso, se a VPN usar um endereço IP corporativo interno, então a proteção se torna irrelevante.

Firewall / Proxy: O propósito de um firewall de hardware é filtrar conexões de entrada e saída para grandes empresas. Como é apenas um filtro, não deve modificar o endereço IP de origem e, portanto, não deve impactar a Proteção Geográfica. No entanto, um proxy mudaria definitivamente o endereço IP de origem para usar um endereço de rede privada, que sempre será permitido pela Proteção Geográfica. O principal objetivo deste recurso é bloquear o acesso a um servidor aberto à Internet. Se todas as conexões vierem da rede corporativa, então a proteção se torna irrelevante.

Proteção de IP de Hacker

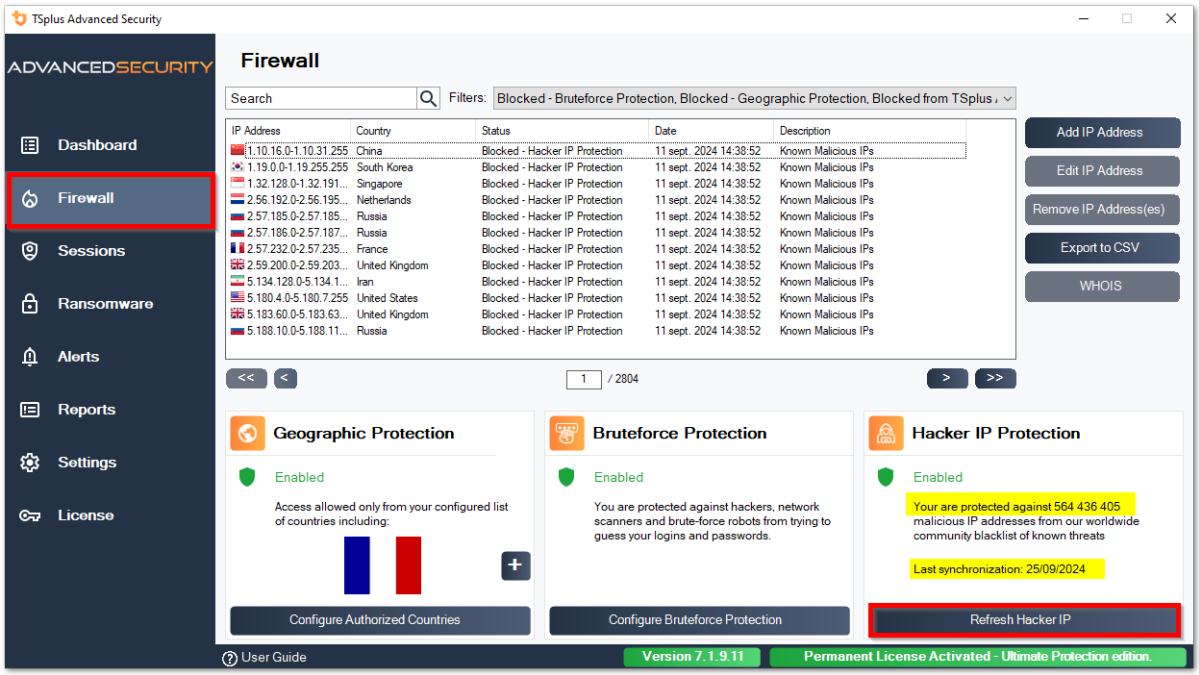
Mantenha sua máquina protegida contra ameaças conhecidas, como ataques online, abuso de serviços online, malwares, botnets e outras atividades de cibercrime com a Proteção de IP do Hacker. O objetivo é criar uma lista negra que possa ser segura o suficiente para ser usada em todos os sistemas, com um firewall, para bloquear o acesso totalmente, de e para seus IPs listados.

A assinatura dos serviços de suporte e atualizações é necessária.

A principal pré-requisito para esta causa é não ter falsos positivos. Todos os IPs listados devem ser ruins e devem ser bloqueados, sem exceções. Para alcançar isso, a Proteção de IPs de Hacker utiliza as informações fornecidas pela comunidade de usuários do Advanced Security.

A proteção de IP de hackers é atualizada automaticamente todos os dias.

Você pode atualizar manualmente na aba “Endereços IP Bloqueados”, clicando no botão “Atualizar IP do Hacker”:

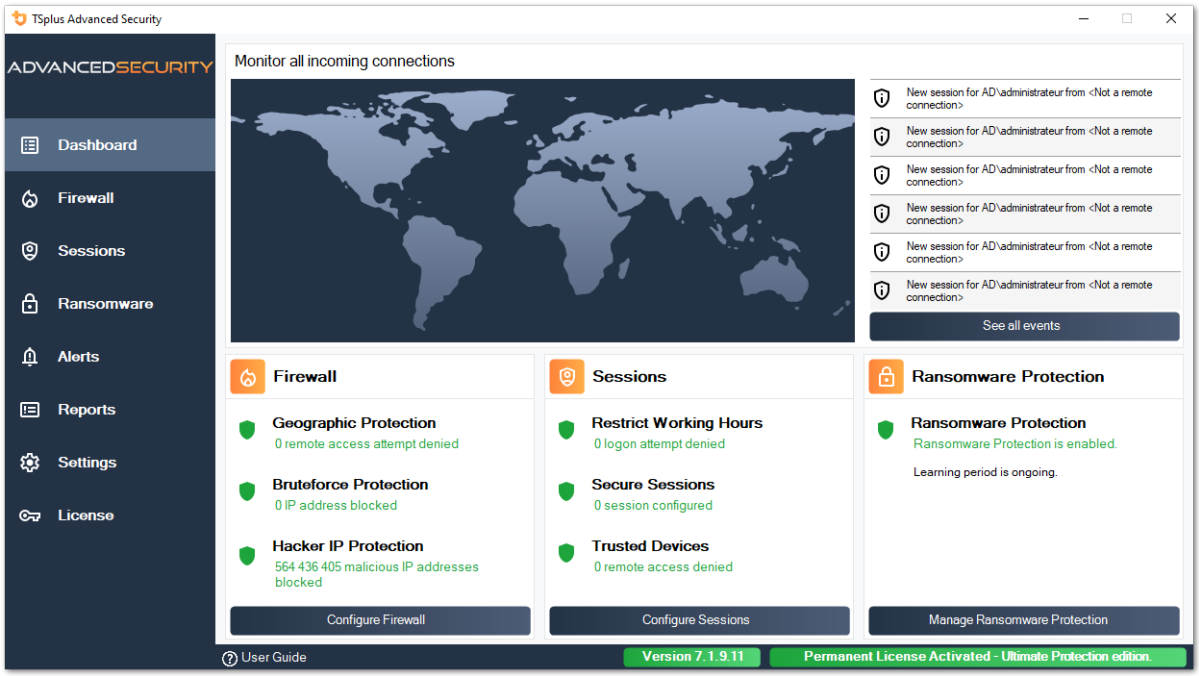


Como resultado, o recurso deve criar aproximadamente 600 000 000 regras de firewall

bloqueadoras no Windows Firewall.

Painel de Controle

Clique em cada bloco para saber mais sobre cada recurso



A barra de menu à esquerda fornece acesso aos diferentes recursos. Cada bloco oferece acesso às várias funcionalidades e configurações oferecidas pelo TSplus Advanced Security.

A Segurança Avançada exibe os seis últimos Eventos de Segurança Clique em qualquer evento para abrir a lista completa de eventos em uma janela separada.

Abaixo dos últimos eventos, três blocos oferecem acesso rápido a:

1. Firewall
2. Sessões
3. Proteção contra Ransomware

Por favor, selecione seu idioma de exibição usando o menu suspenso localizado no canto superior direito, caso o aplicativo não tenha detectado seu idioma.

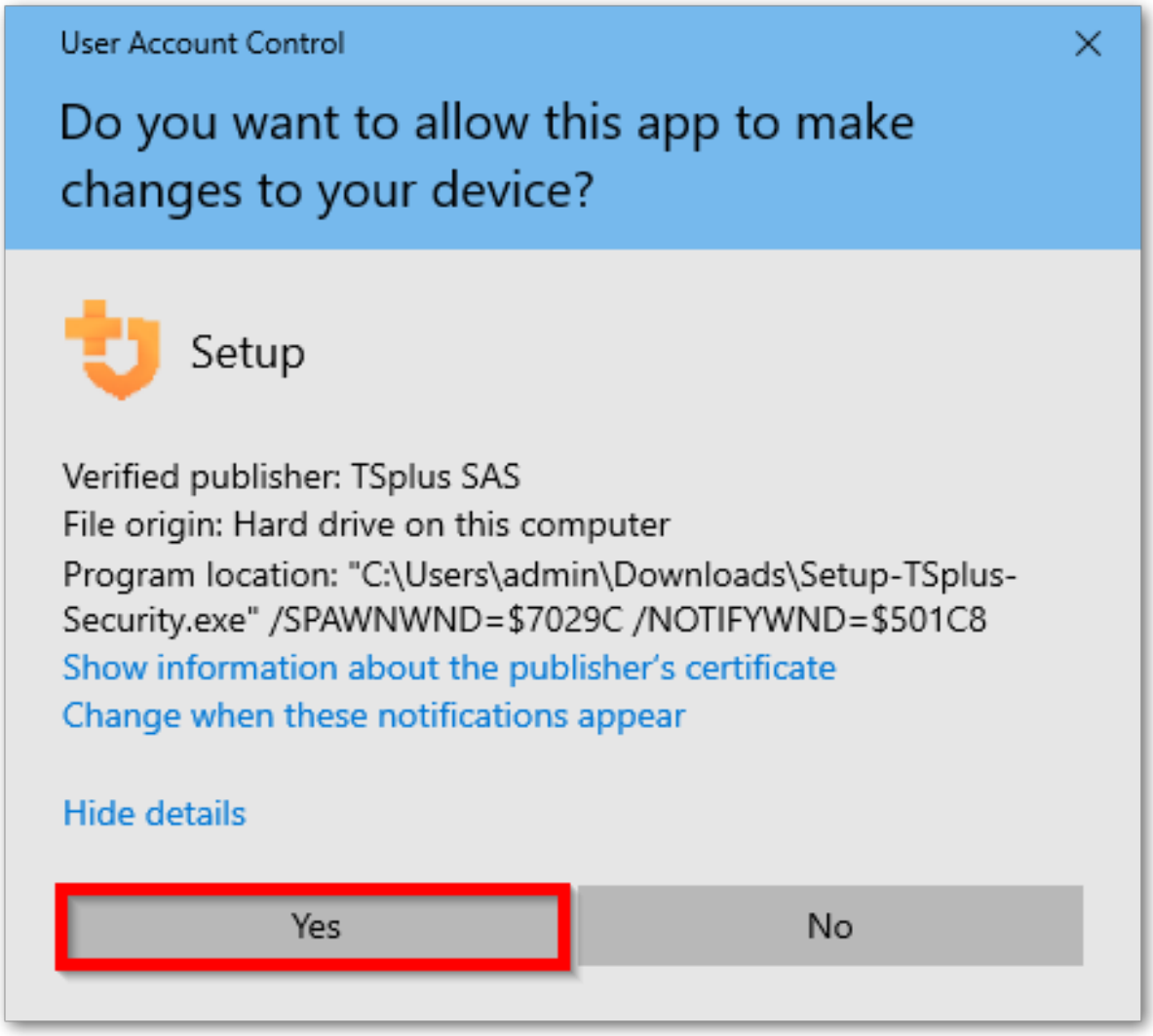
Finalmente, clicar no botão "Ajuda" o redirecionará para esta documentação.

Instalando TSplus Advanced Security

Instalando Advanced Security

Executar TSplus Advanced Security Setup program e então **siga os passos de instalação** .

Você deve executar o programa de instalação como Administrador e aceitar o contrato de licença do software.



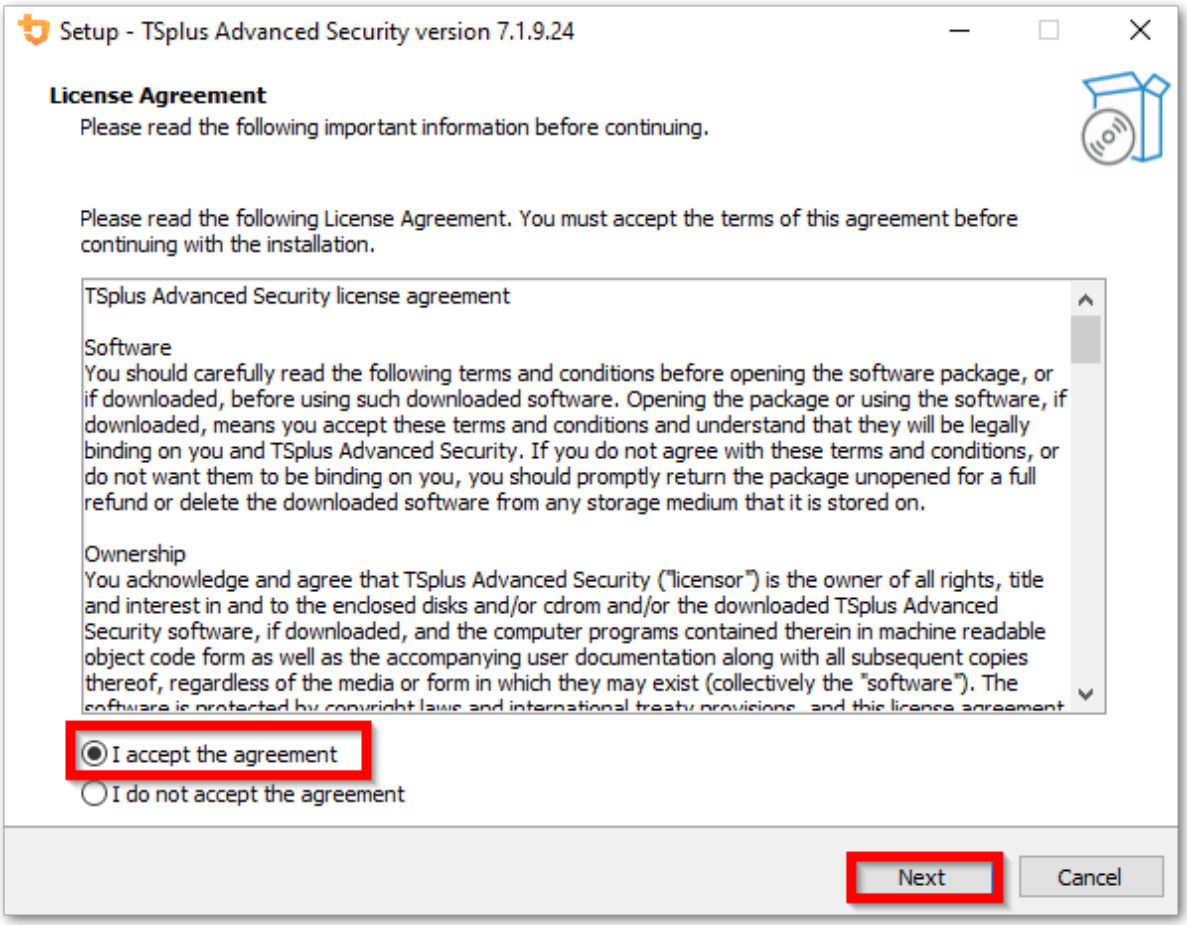
Selecione o idioma do assistente de configuração se não for detectado automaticamente.

Em seguida, selecione uma das duas opções: **Recomendado** ou **Avançado** clicando nas caixas correspondentes.

A opção Avançada adiciona etapas adicionais que permitem que você:

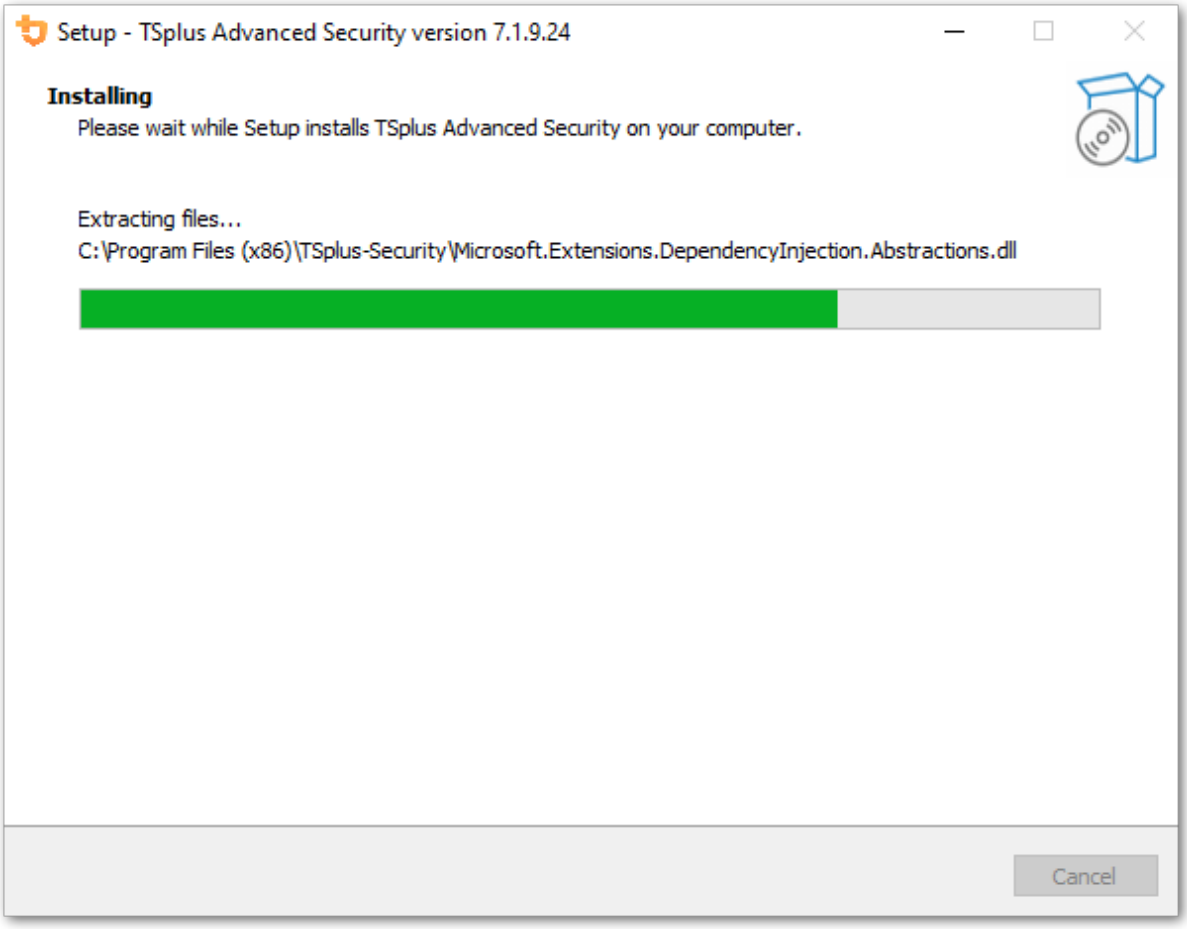
- Apenas baixe a configuração (não instale)
- Use configurações de proxy personalizadas

Leia o contrato de licença e clique em "Eu concordo" para retomar a instalação.



O programa será instalado no seu computador.

Uma barra de progresso é exibida na parte inferior e relata o progresso da instalação.



Por favor, seja paciente , pois pode levar alguns minutos para instalar o software completamente.

Uma vez que a instalação foi concluída, você pode começar a usar TSplus Advanced Security!

A versão de teste gratuita possui todos os recursos por 15 dias. Não se esqueça de ative sua licença e para atualize para a versão mais recente manter a proteção do Advanced Security em seu melhor!

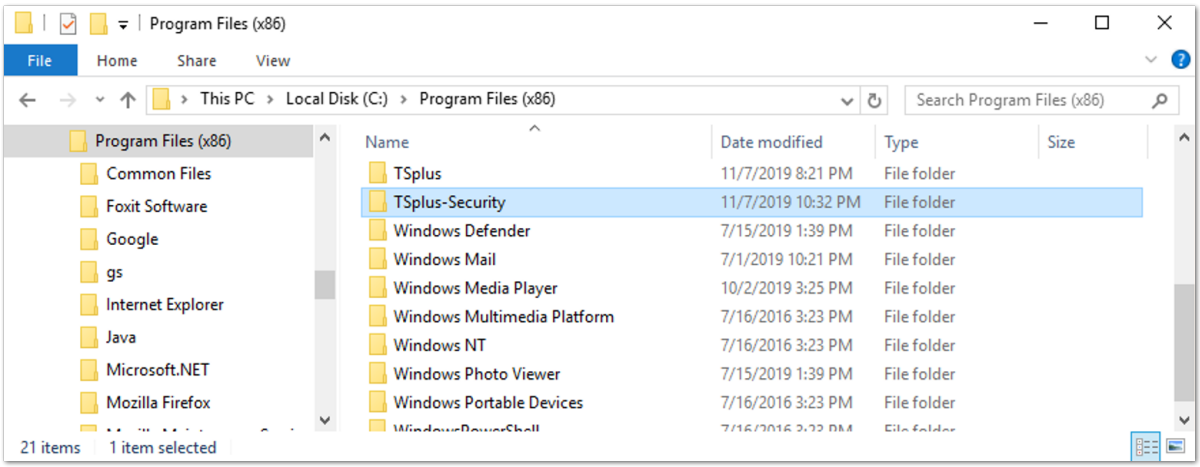
Cenários de instalação avançada

O TSplus Advanced Security Classic Setup program lida os seguintes cenários, pois pode ser executada a partir da linha de comando:

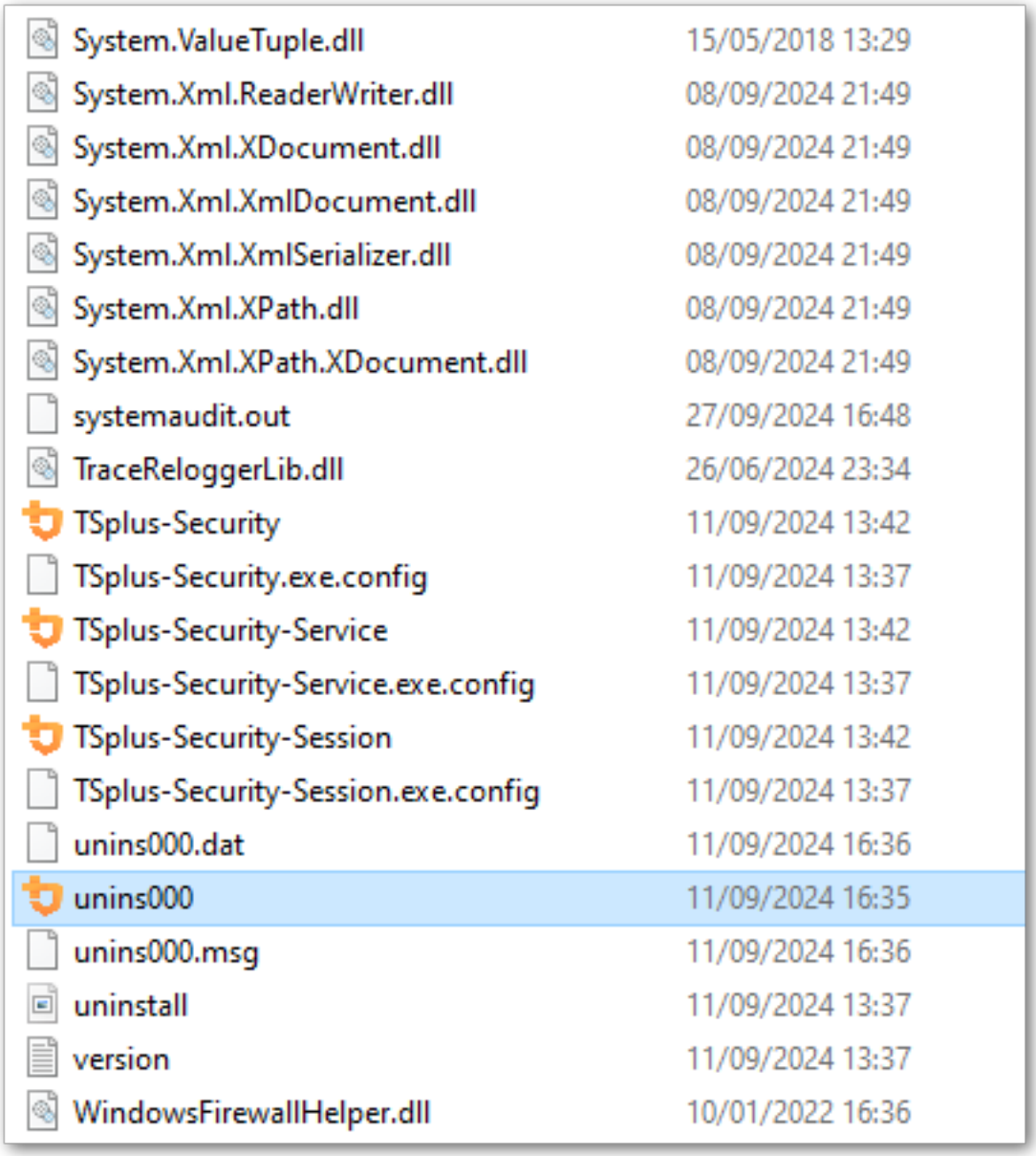
- Instale silenciosamente, fornecendo os parâmetros /VERYSILENT /SUPPRESSMSGBOXES
- Impedir a reinicialização ao final da configuração, fornecendo o parâmetro /NORESTART. Este parâmetro é geralmente usado junto com o acima.
- Licenciamento por volume para ativar sua licença diretamente durante a instalação (consulte a documentação ou contate-nos para mais informações)

Desinstalar TSplus Advanced Security

Para desinstalar completamente o TSplus Advanced Security, abra o diretório C:\Program Files (x86)\TSplus-Security.



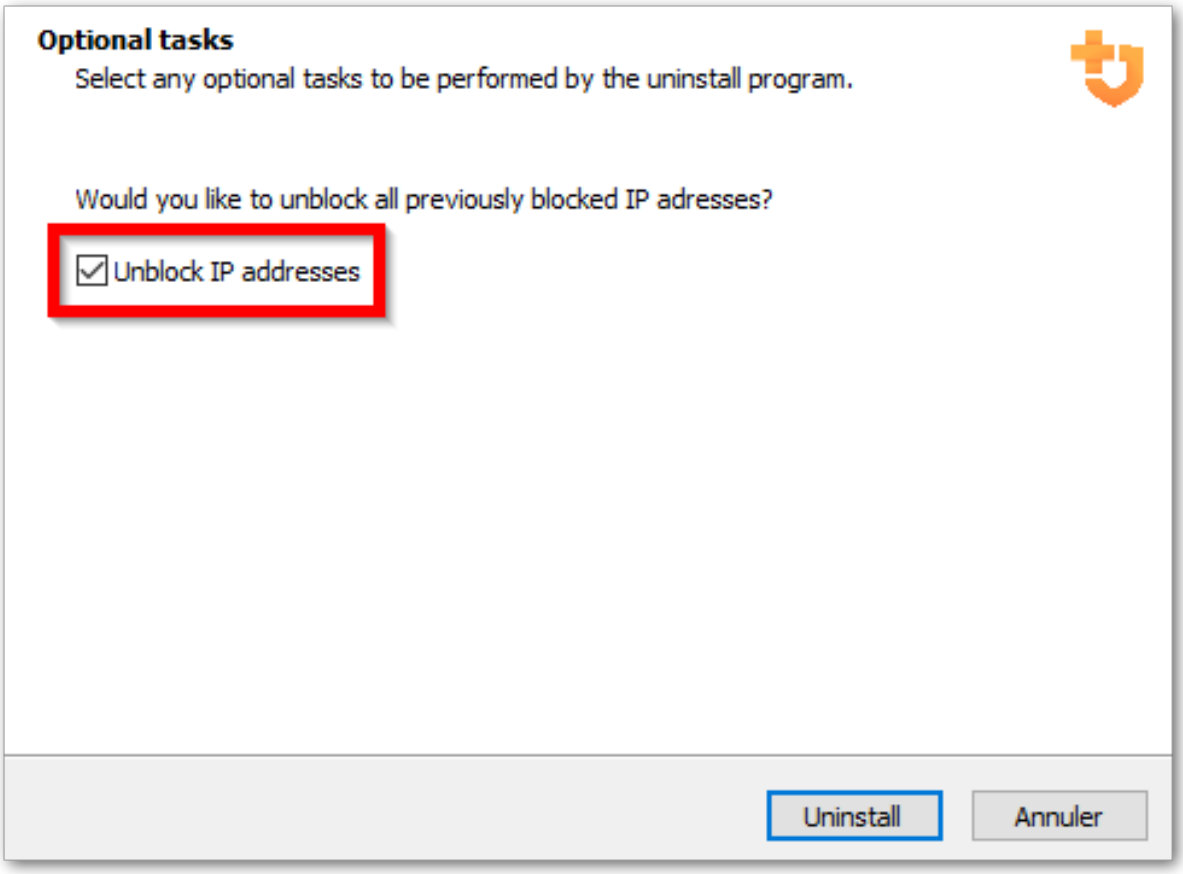
Em seguida, clique duas vezes no aplicativo “unins000” para executar o programa de desinstalação.



Clique em sim na próxima janela para remover completamente o TSplus Advanced Security e todos os seus componentes.

A menos que configurado de outra forma, o Advanced Security adiciona regras de bloqueio ao Firewall do Windows. Clique em “Desbloquear endereços IP” para desbloquear e remover todos os endereços IP anteriormente bloqueados pelo Advanced Security.

Importante: Por favor, tenha em mente que remover todas as regras pode levar até uma hora. Por causa disso, recomendamos remover as regras diretamente do console do Firewall do Windows com Segurança Avançada.



O software será completamente desinstalado do seu computador.

Gerenciamento de Permissões

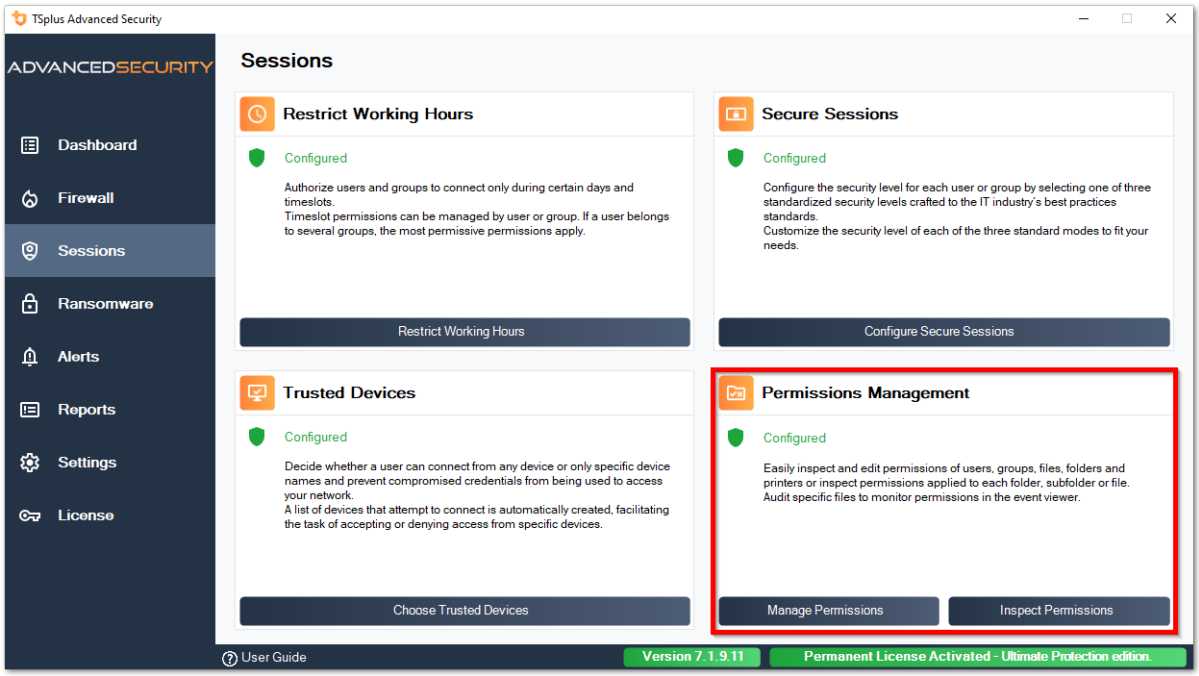
Desde a versão 4.3, o TSplus Advanced Security oferece uma funcionalidade de Permissões, permitindo ao administrador gerenciar e/ou inspecionar os privilégios de usuários/grupos.

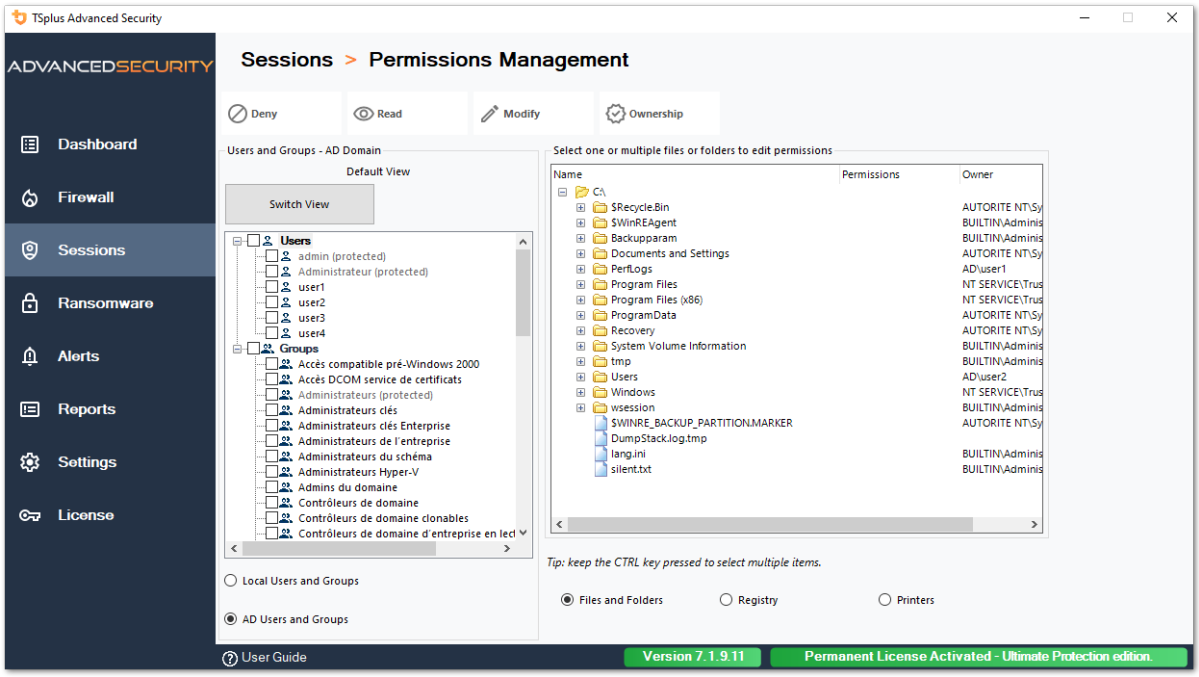
Na tela de permissões, a lista de usuários e grupos e a lista de disponíveis **arquivos, pastas, registros e impressoras** são mostrados lado a lado.

Tudo é visível de uma só vez, o que torna super fácil de **Inspecionar** e **Gerenciar/Editar** privilegios para um usuário por vez e, portanto, aumentar a precisão das restrições.

Gerenciar Permissões

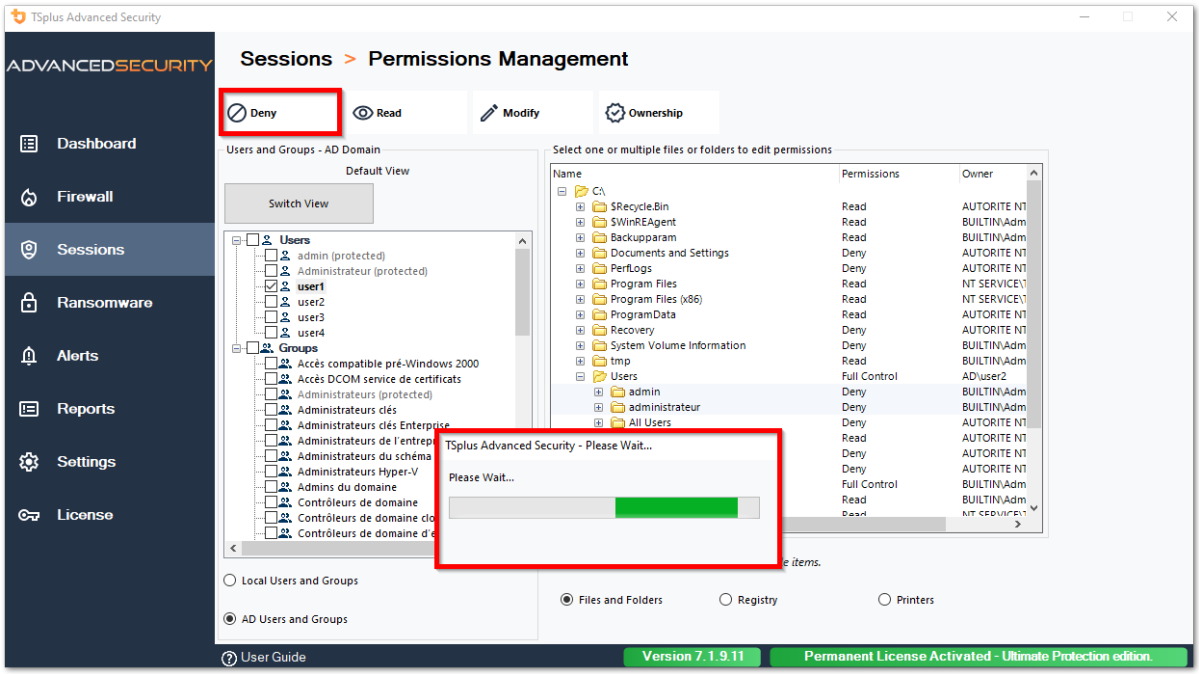
Na guia Gerenciar, para cada usuário ou grupo selecionado na visualização em árvore à esquerda, você pode:



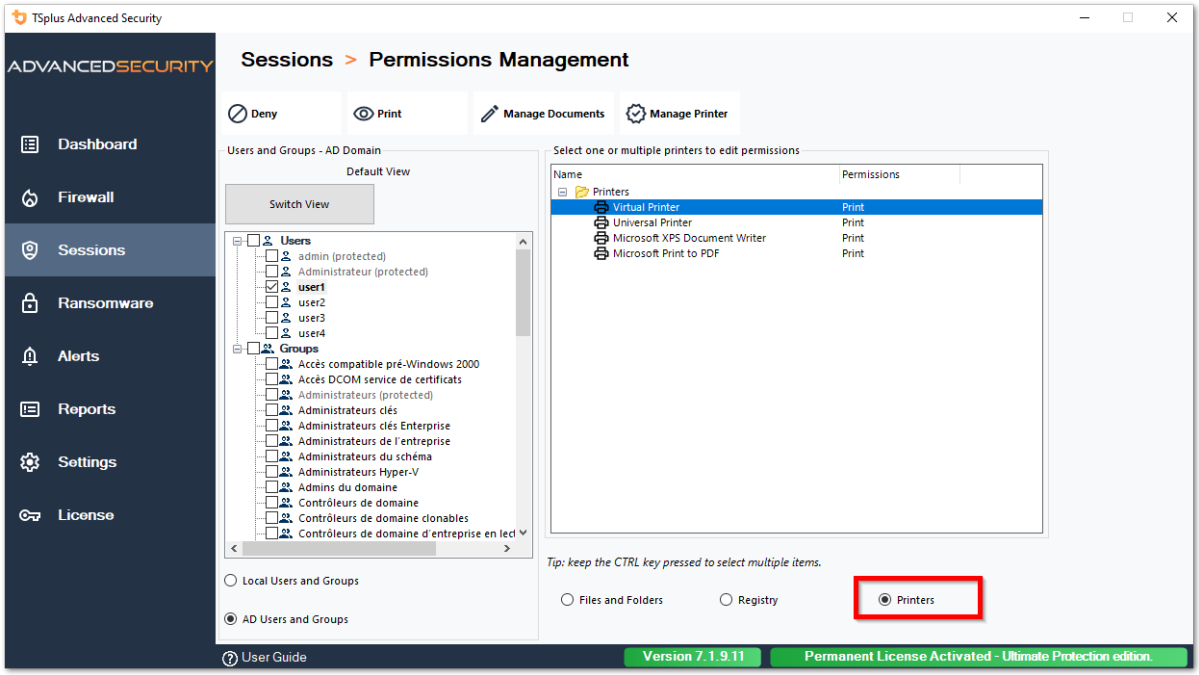


- **Negar** Ao clicar no botão Negar, o usuário selecionado terá o privilégio negado no objeto de sistema de arquivos selecionado. Se um arquivo for selecionado, o usuário selecionado terá negado o privilégio de ler o arquivo selecionado (FileSystemRights.Read). Se um diretório for selecionado, o usuário selecionado terá negado o privilégio de ler e listar o conteúdo do diretório (FileSystemRights.Read e FileSystemRights.ListDirectory).
- **Leia** Ao clicar no botão Ler, o usuário selecionado receberá privilégios sobre o objeto de sistema de arquivos selecionado. Se um arquivo for selecionado, o usuário selecionado receberá o privilégio de ler o arquivo selecionado e executar, se o arquivo for um programa (FileSystemRights.ReadAndExecute). Se um diretório for selecionado, o usuário selecionado receberá o privilégio de ler e listar ou executar o conteúdo do diretório (FileSystemRights.ReadAndExecute e FileSystemRights.ListDirectory e FileSystemRights.Traverse).
- **Modificar** Ao clicar no botão Modificar, o usuário selecionado receberá privilégios sobre o objeto de sistema de arquivos selecionado. Se um arquivo for selecionado, o usuário selecionado receberá o privilégio de modificar o arquivo selecionado (FileSystemRights.Modify). Se um diretório for selecionado, o usuário selecionado receberá o privilégio de modificar e listar o conteúdo do diretório, bem como criar novos arquivos ou diretórios (FileSystemRights.Modify e FileSystemRights.CreateDirectories e FileSystemRights.CreateFiles e FileSystemRights.ListDirectory e FileSystemRights.Traverse).
- **Propriedade** Ao clicar no botão de Propriedade, o usuário selecionado receberá controle total sobre o objeto de sistema de arquivos selecionado (FileSystemRights.FullControl).

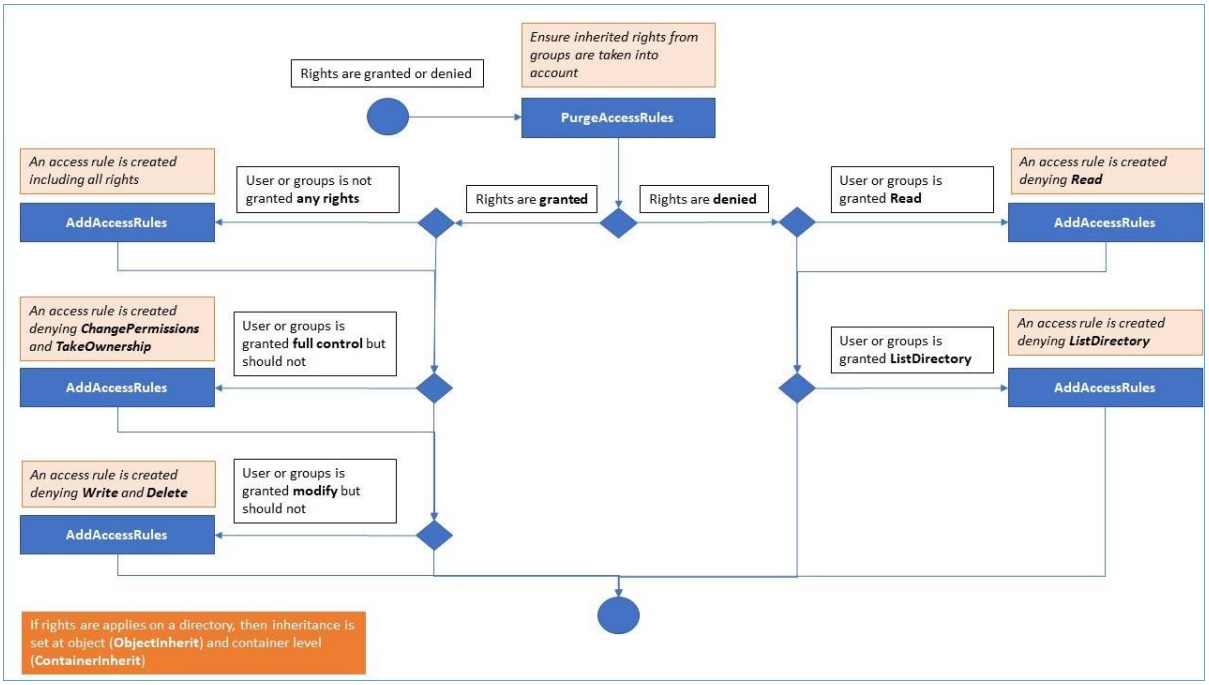
As opções de permissões são possíveis para cada Registro, selecionando o botão correspondente na visualização da árvore à direita:



E para cada impressora:



Por favor, note que todas as permissões negadas ou concedidas a um diretório são aplicadas recursivamente aos objetos do sistema de arquivos contidos por este diretório. O diagrama abaixo detalha as chamadas de API quando os direitos são aplicados a um objeto do sistema de arquivos.

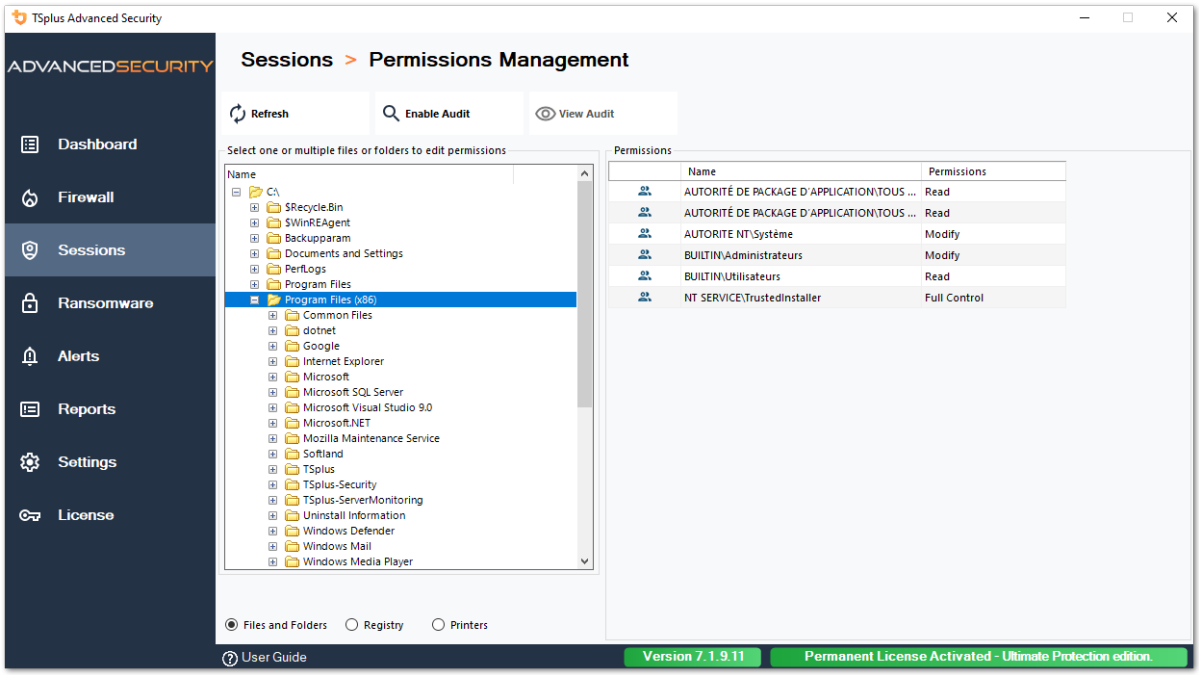


Documentação :

- Segurança de Objetos: https://docs.microsoft.com/pt-br/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- Direitos do Sistema de Arquivos: https://docs.microsoft.com/pt-br/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

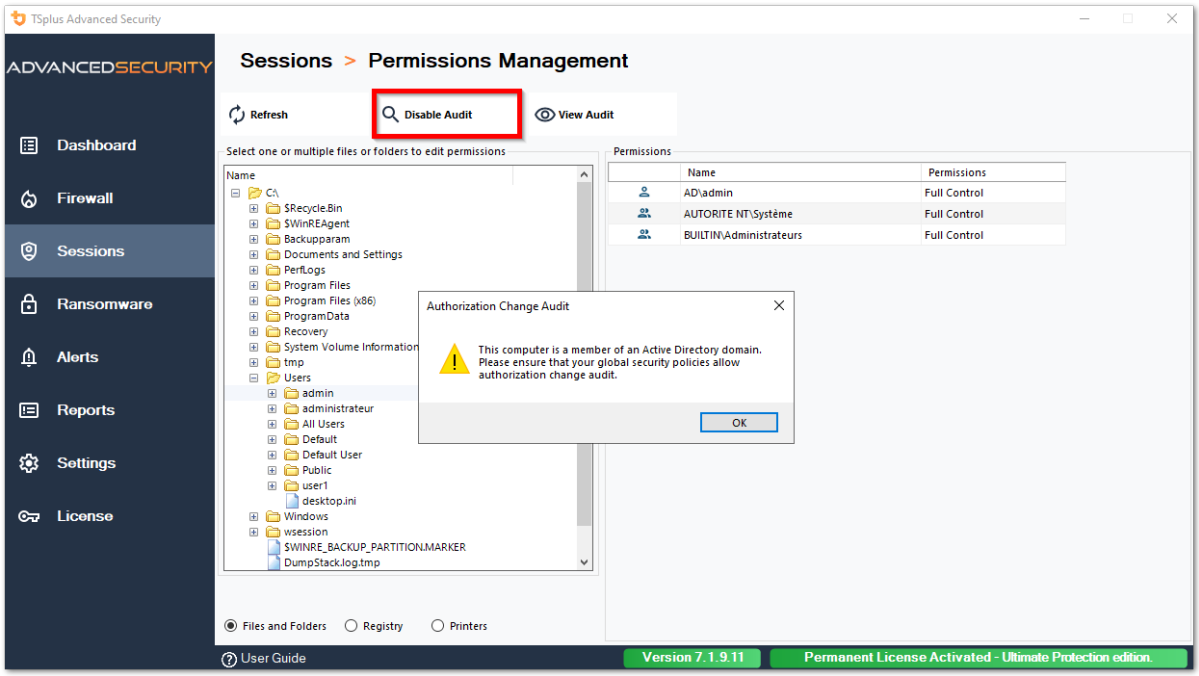
Inspecionar Permissões

Na guia Inspecionar, para cada pasta, subpasta ou arquivo selecionado na visualização em árvore à esquerda, você pode ver as permissões atribuídas correspondentes a usuários ou grupos na visualização em árvore à direita.

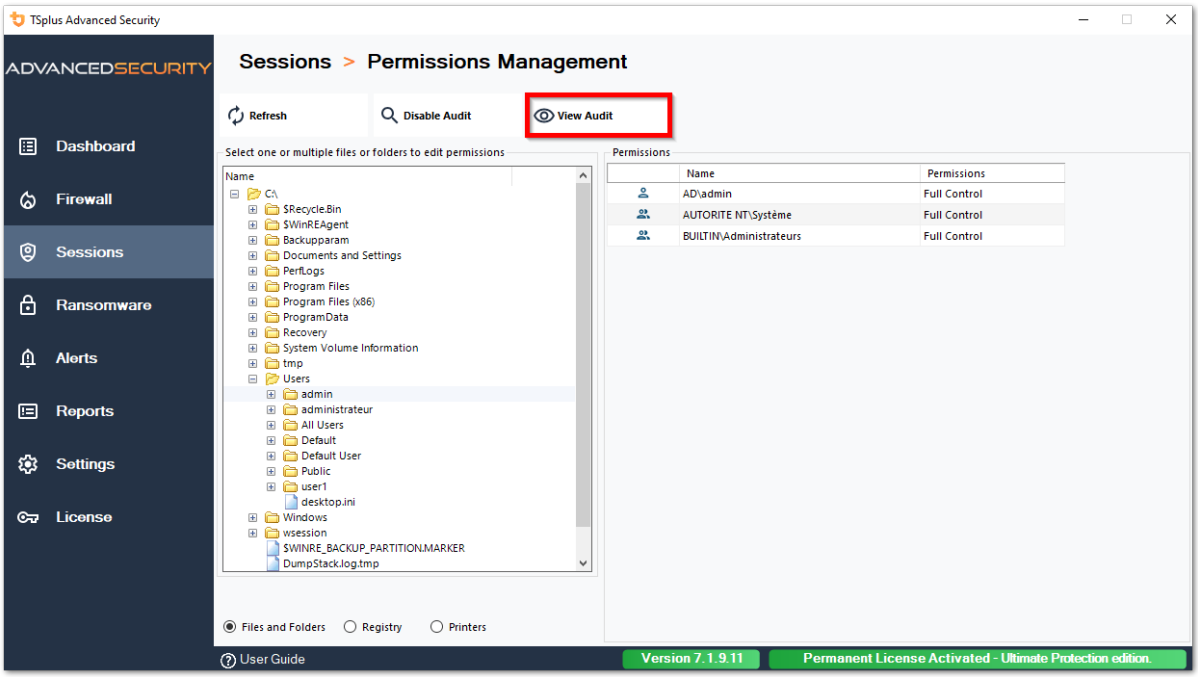


Você pode atualizar o status das pastas para que elas sejam atualizadas em tempo real.

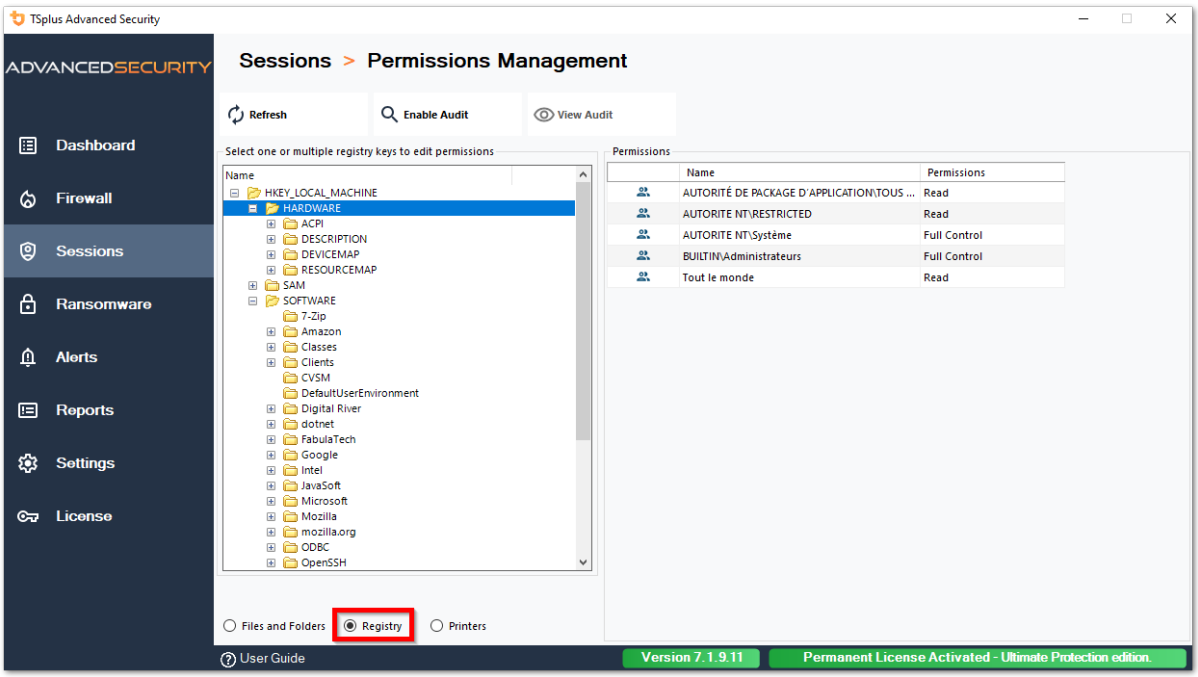
Uma auditoria pode ser ativada selecionando a pasta, subpasta ou arquivo desejado e clicando no botão “Ativar Auditoria” na parte superior:

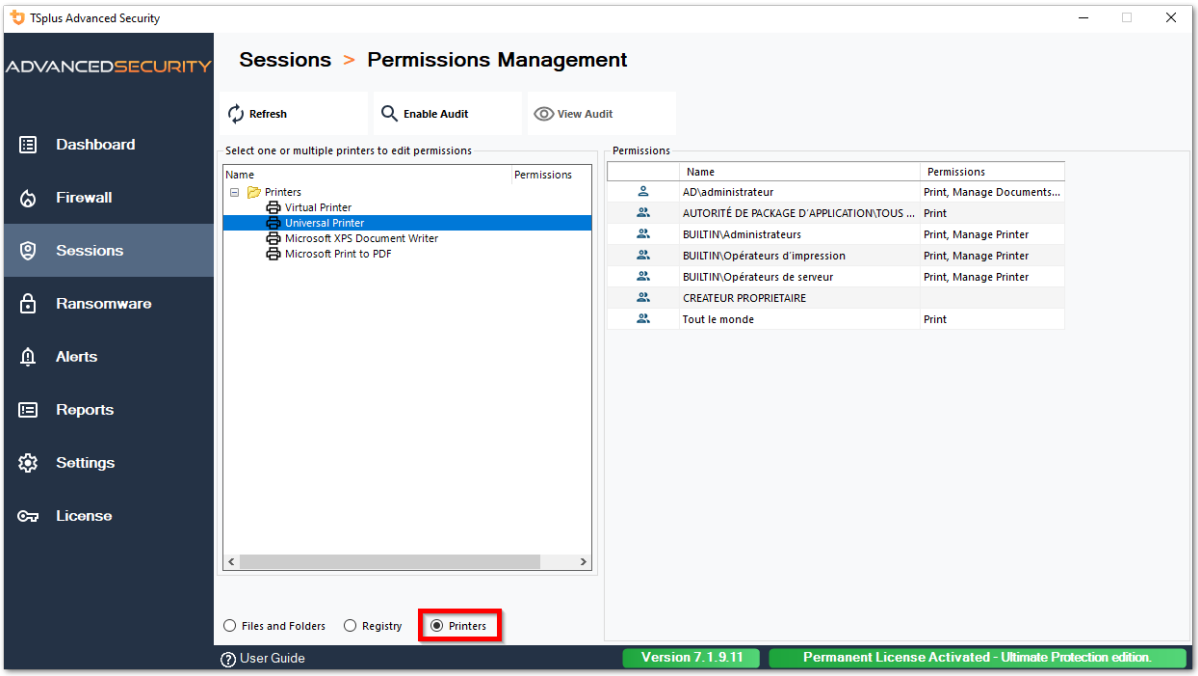


O botão "Ver Auditoria" permite que você veja a auditoria correspondente no Visualizador de Eventos:



As mesmas possibilidades de inspeção estão disponíveis para cada registro e impressora ao selecionar o botão correspondente na visualização da árvore à esquerda:




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 - Pré-requisitos

Requisitos de Hardware

TSplus Advanced Security suporta arquiteturas de 32 bits e 64 bits.

Sistema Operacional

Seu hardware deve usar um dos sistemas operacionais abaixo:

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

Ambas as arquiteturas de 32 e 64 bits são suportadas.

Requisitos de Software

TSplus Advanced Security requer os seguintes pré-requisitos:

- Tempo de execução: .NET Framework 4.7.2 ou superior
- Microsoft Windows 7 SP1 e Windows 2008 R2 SP1 requerem uma atualização adicional para suportar a assinatura cruzada SHA2 (KB4474419 Esta atualização permite que o firewall integrado do TSplus Advanced Security e a proteção contra ransomware funcionem corretamente.

Nota: Esses pré-requisitos serão instalados automaticamente pelo programa de instalação se estiverem ausentes no sistema.

TSplus Advanced Security - Introdução

Pré-requisitos

TSplus Advanced Security requer os seguintes pré-requisitos.

- Sistema operacional: Microsoft Windows versão 7, Service Pack 1 (build 6.1.7601) ou Windows 2008 R2, Service Pack 1 (build 6.1.7601) ou superior.

O seguinte **os pré-requisitos serão instalados automaticamente pelo programa de instalação** se ausente:

- Tempo de execução: .NET Framework 4.5.3 ou superior
- Microsoft Windows 7 SP1 e Windows 2008 R2 SP1 requerem uma atualização adicional para suportar SHA2 Cross Signing (KB4474419 Esta atualização permite que o firewall integrado do TSplus Advanced Security e a proteção contra ransomware funcionem corretamente.

Por favor, consulte o documentação para mais detalhes sobre os pré-requisitos.

Passo 1: Instalação

A versão mais recente do programa de instalação do TSplus Advanced Security está sempre disponível aqui: Último programa de instalação do TSplus Advanced Security Por favor, baixe o programa de instalação e siga o assistente de configuração.

O programa de configuração do TSplus Advanced Security geralmente não requer que você reinicie seu sistema para concluir a instalação.

Qualquer nova instalação inicia um período de teste completo de 15 dias. Por favor, não hesite em contate-nos caso enfrente algum obstáculo ou se tiver algum problema ao configurar o TSplus Advanced Security.

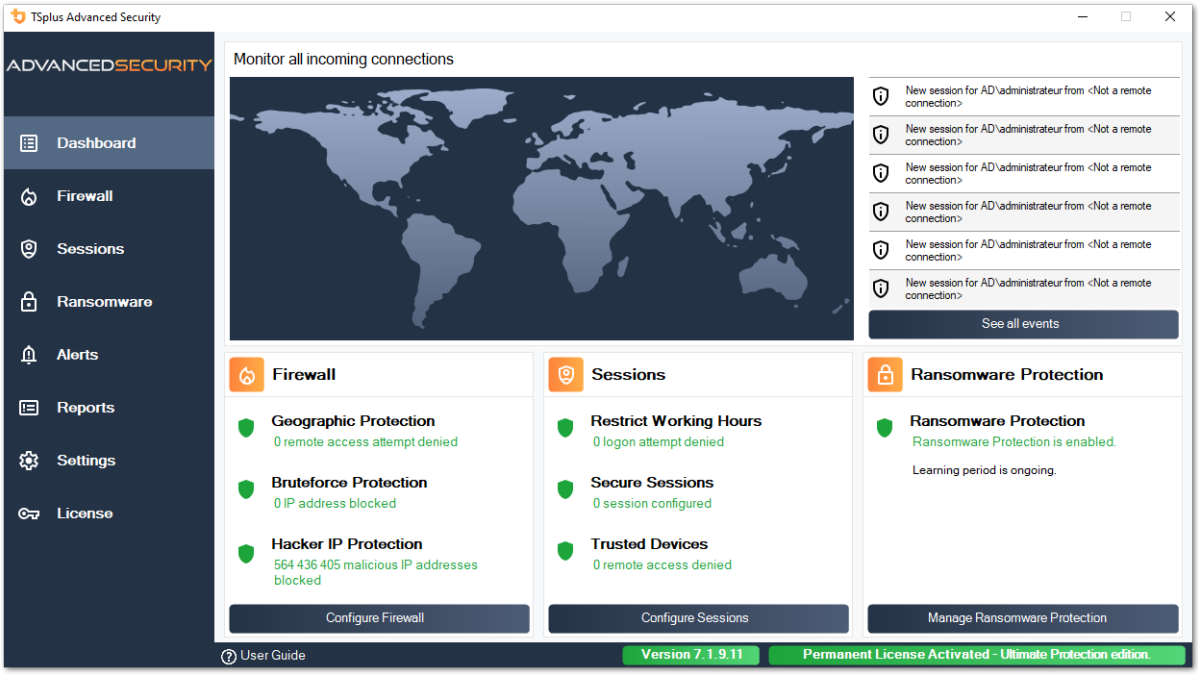
Uma vez que a instalação foi concluída, um novo ícone é exibido na sua área de trabalho.

Clique duas vezes neste ícone para abrir o TSplus Advanced Security e começar a configurar os recursos de segurança.

Por favor, consulte o documentação para instruções de instalação completas.

Passo 2: Configurando TSplus Advanced Security

Você lançou TSplus Advanced Security e começou a configurar recursos para proteger seu servidor contra atividades maliciosas e impor políticas de segurança robustas.



Na coluna da esquerda, a página inicial permite um acesso rápido para configurar os recursos de proteção contra ransomware, proteção contra bruteforce e proteção geográfica.

Iniciar Proteção contra Ransomware período de aprendizado para permitir que o Advanced Security identifique aplicativos e comportamentos legítimos em seu sistema clicando no seguinte bloco:

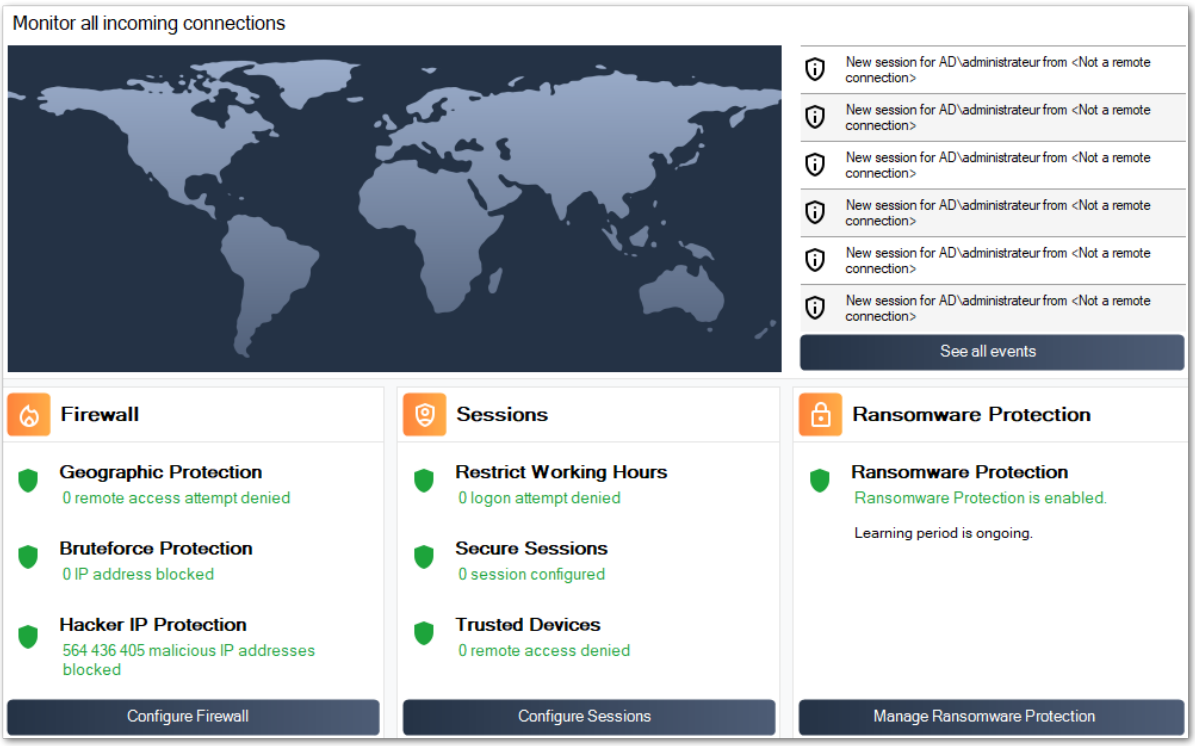
Proteção contra Bruteforce geralmente está em funcionamento após a instalação. Caso contrário, clique em o **Repetir defesa contra ataques de força bruta** Título para resolver problemas e aplicar a configuração do sistema necessária. Por padrão, este recurso bloqueia atacantes após 10 tentativas de login falhadas.

Finalmente, adicione seu país à lista de países autorizados de onde os clientes podem se conectar. Clique no bloco **Autorizar conexões de outro país** e adicione seu país para configurar Proteção Geográfica

Você está pronto! Não se esqueça de ative sua licença e para atualize para a versão mais recente manter a proteção do Advanced Security em seu melhor!

Passo 3: Revisando ameaças prevenidas

Agora que você configurou os principais recursos de segurança avançada, as ameaças evitadas serão relatadas no Painel.



Além disso, o Hacker IP a proteção mantém a máquina protegida contra ameaças conhecidas, bloqueando mais de 500.000.000 de endereços IP maliciosos conhecidos.

Todos os eventos de segurança pode ser exibido clicando em **Veja todos os eventos** azulejo.

Passo 4: Aproveitando outros recursos de segurança para aumentar a proteção

Na parte inferior, quatro outros recursos de segurança podem ser acessados e configurados para aprimorar a proteção do seu dispositivo.

- Ajuste e monitore os privilégios de acesso em seus sistemas de arquivos locais, impressoras e chaves de registro para garantir que cada usuário tenha acesso aos recursos relevantes, com o Permissões recurso.

- Defina o período de tempo em que os usuários estão autorizados a fazer login com o Working Hours feature. Os usuários serão desconectados após suas horas de trabalho permitidas.

- Personalize e proteja as sessões de usuário com o Desktop Seguro recurso. Personalize, oculte, negue o acesso a itens da interface da sessão para usuários locais.

- Valide o nome do cliente remoto quando um usuário se conectar à sua máquina com Proteção de Endpoint Este recurso valida os nomes das máquinas clientes para cada usuário conectado remotamente.

Há mais! Mudar para o modo avançado concede acesso a mais recursos.

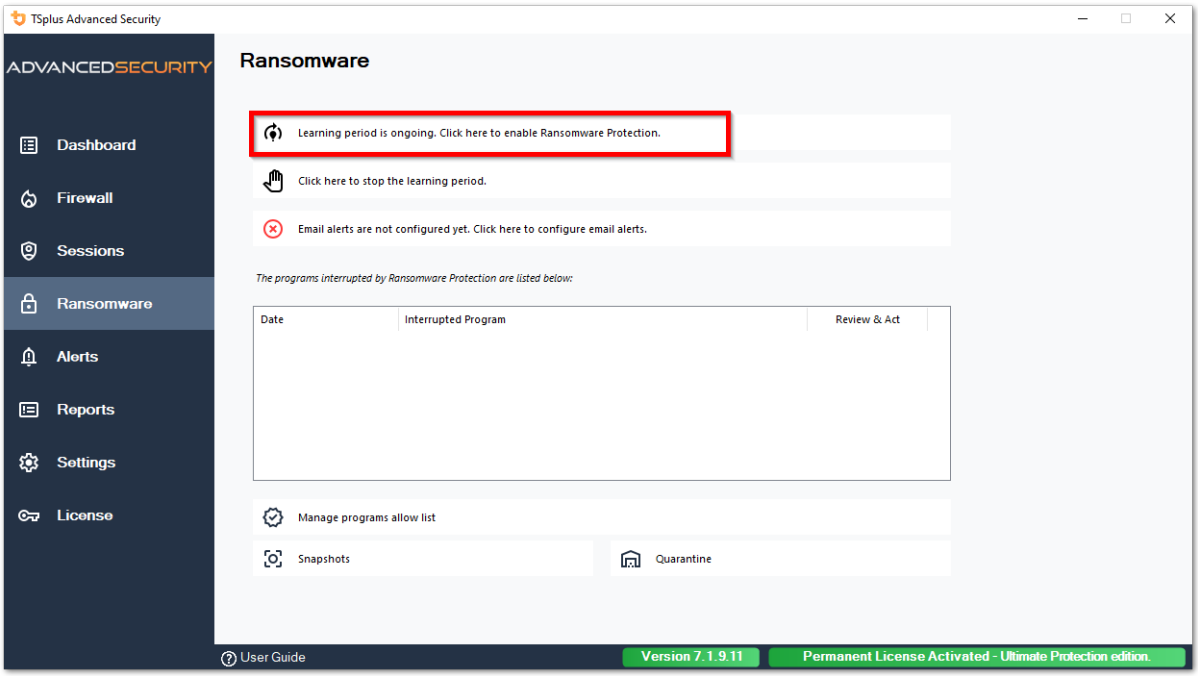
Obrigado por usar o TSplus Advanced Security!

Proteção contra Ransomware

A Proteção contra Ransomware permite que você DETECTE, BLOQUEIE e PREVINA ataques de ransomware de forma eficiente. TSplus Advanced Security reage assim que detecta ransomware em sua sessão. Possui tanto **análise estática e comportamental** :

- O **análise estática** habilita o software a reagir imediatamente quando um nome de extensão é alterado,
- O **análise comportamental** analisa como um programa interagirá com arquivos e detectará novas variantes de ransomware.

Você pode ativá-lo clicando em “Ativar Proteção contra Ransomware” na aba de Proteção contra Ransomware:

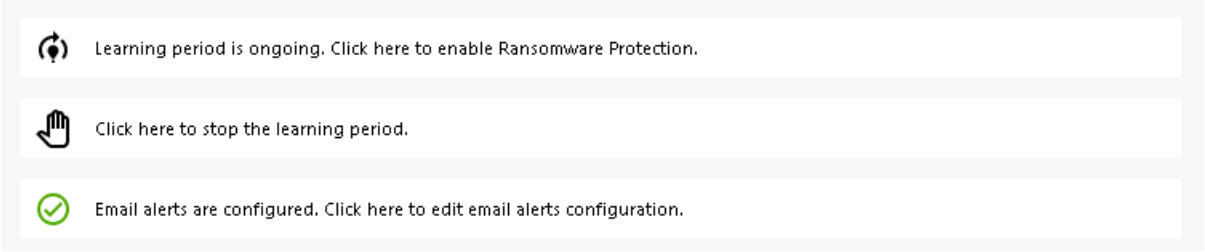


Período de Aprendizagem

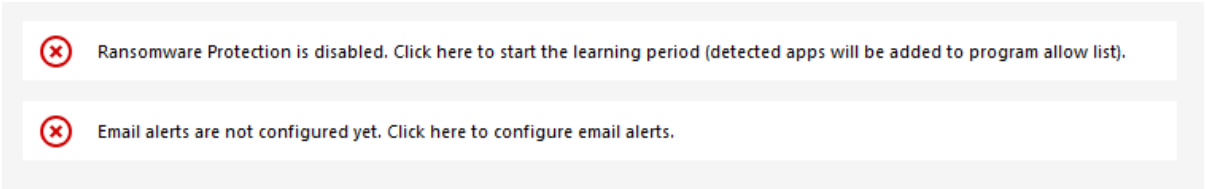
Após ativar o recurso de Proteção contra Ransomware, o Período de Aprendizado é ativado automaticamente. Durante o Período de Aprendizado, todos os programas detectados pelo recurso de Proteção contra Ransomware serão considerados como falsos positivos e poderão

retomar sua execução. Os programas detectados como falsos positivos serão adicionados automaticamente à lista de programas permitidos.

Este recurso permite configurar a proteção contra ransomware em um servidor de produção sem interromper sua atividade. Recomendamos começar com um período de aprendizado de 5 dias para identificar todos os aplicativos comerciais legítimos.



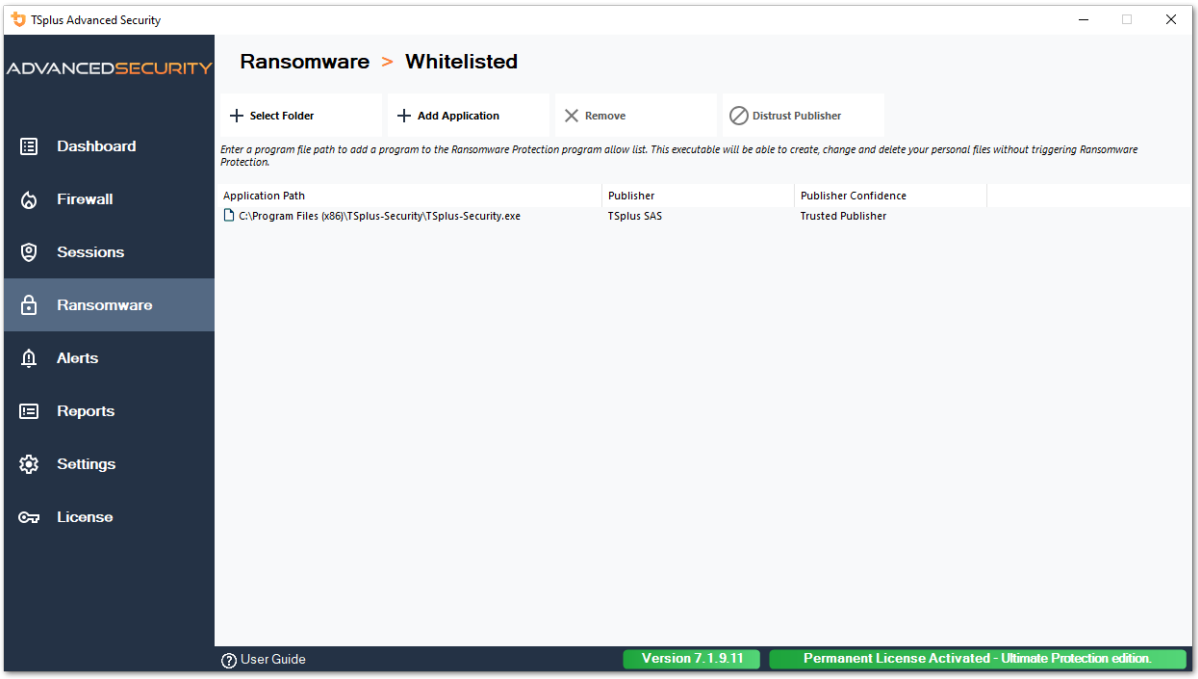
Se você parar o Período de Aprendizado, isso desativará a Proteção contra Ransomware. Clique no botão “A Proteção contra Ransomware está desativada” para reativar o Período de Aprendizado.



Ação de Proteção contra Ransomware

Ele escaneia rapidamente seu(s) disco(s) e exibe o(s) arquivo(s) ou programa(s) responsável(is), além de fornecer uma lista dos itens infectados. TSplus Advanced Security interrompe automaticamente o ataque e coloca em quarentena o(s) programa(s) junto com o(s) arquivo(s) criptografado(s) antes de sua intervenção.

Apenas o administrador pode adicioná-los à lista de permissões, inserindo o caminho do programa desejado na linha inferior e clicando em "Adicionar":



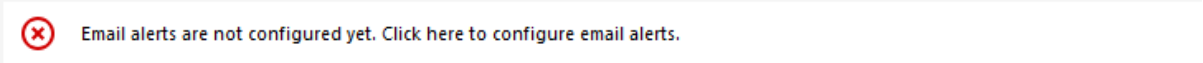
Relatório de Proteção contra Ransomware

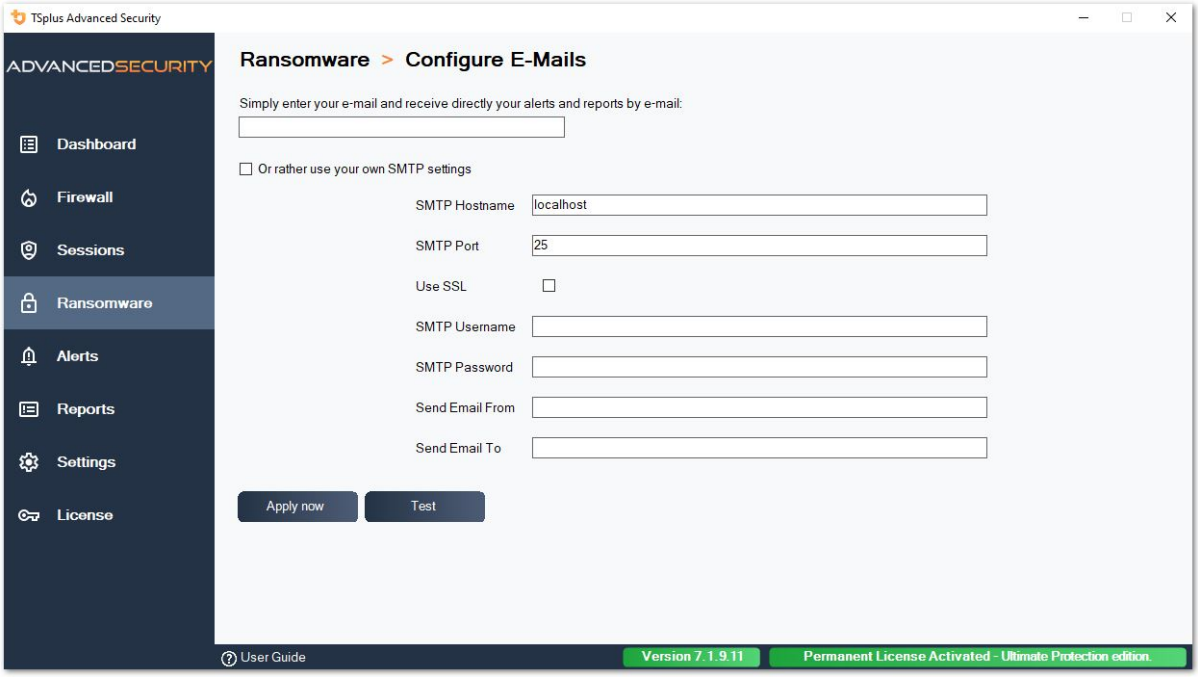
TSplus Advanced Security previne eventos catastróficos para empresas ao remover ransomware em um estágio inicial.

O administrador tem acesso a informações sobre a origem do ataque e os processos em execução, e, portanto, aprende a antecipar essas ameaças.

Nota A Proteção contra Ransomware observa como os programas interagem com arquivos do sistema e pessoais. Para garantir um nível maior de proteção, a Proteção contra Ransomware cria arquivos isca em pastas-chave onde o ransomware frequentemente inicia seu ataque. Portanto, alguns arquivos ocultos podem aparecer nas pastas de desktop e documentos dos usuários, assim como em outros locais. Quando detecta um comportamento malicioso, interrompe o ransomware imediatamente (ou pergunta se o usuário logado é um administrador). A Proteção contra Ransomware utiliza técnicas de detecção comportamental puras e não depende de assinaturas de malware, permitindo capturar ransomware que ainda não existe.

Você pode configurar suas configurações SMTP para que o TSplus Advanced Security envie alertas por e-mail para destacar eventos de segurança importantes clicando no botão abaixo do de ativação de Ransomware:





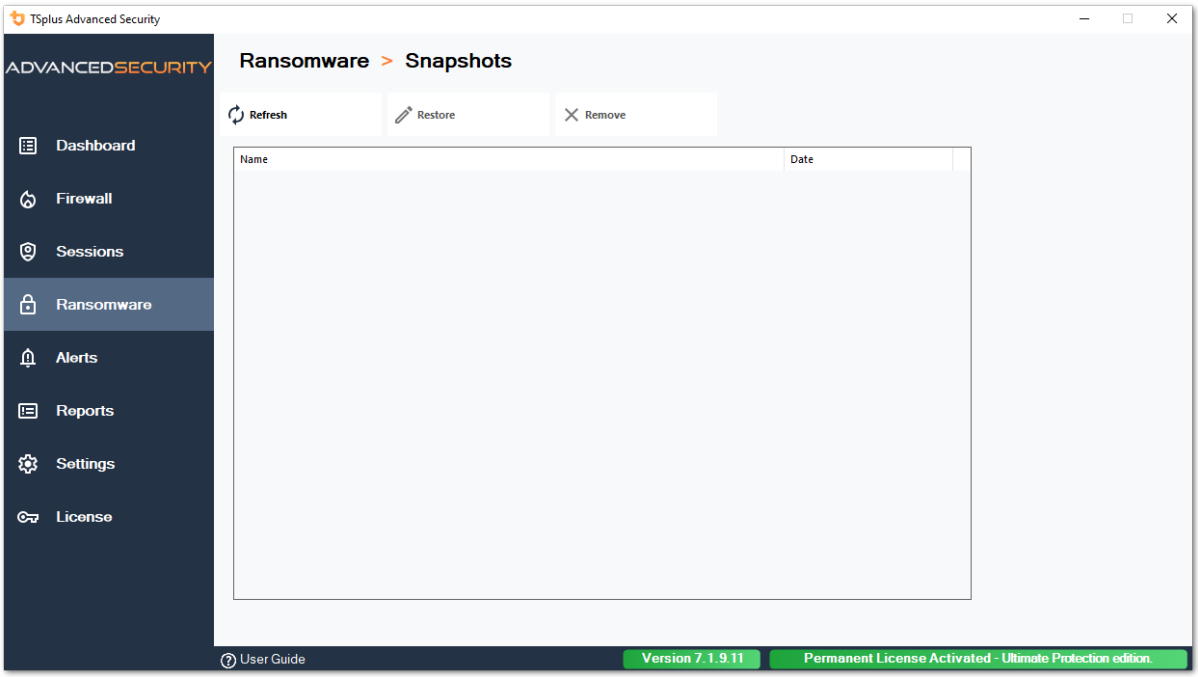
Insira seu nome de host SMTP, porta e marque a caixa Usar SSL e altere a porta de 25 para 465 se desejar usar SSL.

Insira o nome de usuário e a senha SMTP, bem como os endereços do remetente e do destinatário.

As configurações de e-mail podem ser validadas enviando um teste ao salvar as configurações SMTP.

Capturas de tela

Snapshots tirados pela proteção contra ransomware são visíveis na aba de Snapshots:

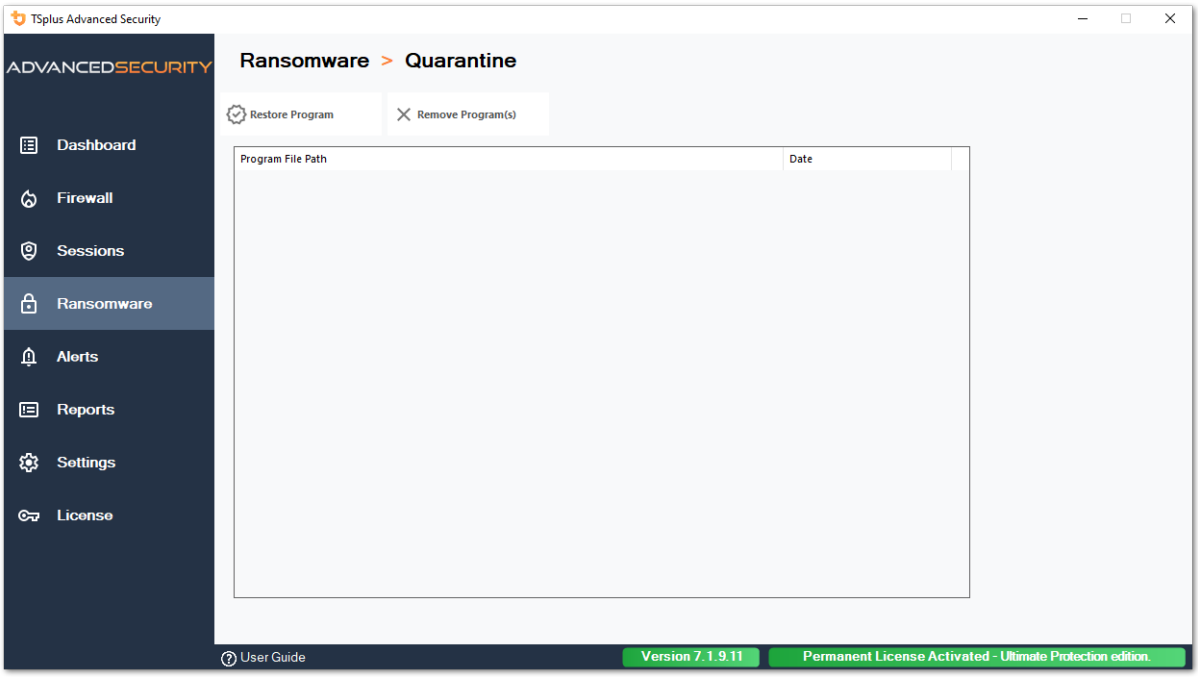


A lista pode ser atualizada clicando no botão correspondente. Cada elemento pode ser restaurado ou removido.

Quarentena

Programas em quarentena são visíveis na aba Quarentena:
Programas potencialmente indesejados são mantidos em quarentena indefinidamente até que você decida qual ação tomar.

Dessa forma, o Advanced Security garante a segurança da sua máquina enquanto lhe oferece a opção de gerenciar itens em quarentena conforme você desejar.
Isso pode ser útil se você precisar recuperar um arquivo ou programa que foi neutralizado. **Esta decisão é tomada por sua própria conta e risco.**
Você também pode excluir permanentemente quaisquer arquivos ou programas que escolher diretamente da pasta de quarentena localizada no diretório de instalação do Advanced Security.



Cada elemento pode ser restaurado ou removido.

Arquivos ignorados não são usados para detectar possíveis ações maliciosas e não são salvos quando são modificados. A ideia é excluir qualquer operação em arquivos grandes ou irrelevantes (como arquivos de log).

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

- vo2
- vsv
- vud
- iso
- dano
- imagem esparsa
- cabo
- msi
- mui
- dl_
- wim
- ost
- o
- qtch
- ithmb
- vmdk
- memória virtual
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- menudata
- ícone do aplicativo
- informações do aplicativo
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- drk
- mem
- nvram
- hdd
- pk3
- pf
- trn
- automaticDestinations-ms

Cuidado com a extensão de arquivos de backup

A extensão de arquivo usada para salvar arquivos modificados é: **instantâneo.** O driver proíbe qualquer ação de modificação ou exclusão nesses arquivos, exceto pelo serviço TSplus Advanced Security. Parar o serviço exclui os arquivos de backup. Para excluir esses arquivos manualmente, você deve descarregar temporariamente o driver.

Configuração do Arquivo de Backup

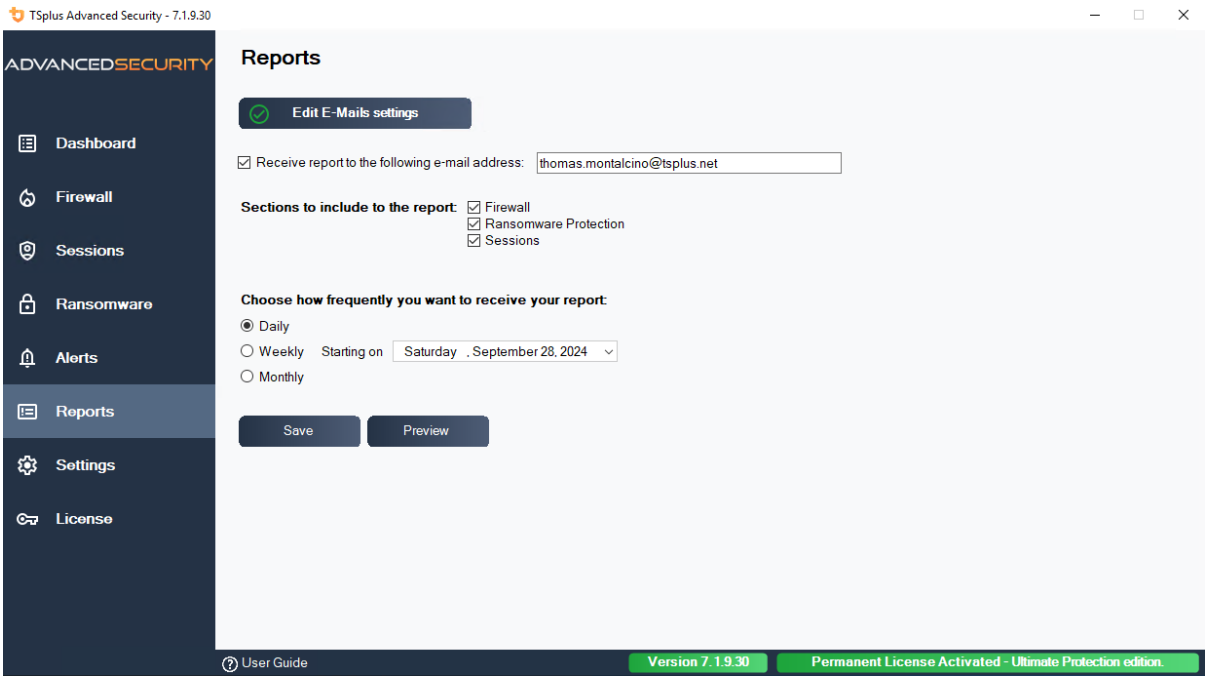
Por padrão, o diretório de arquivos salvos está localizado no diretório de instalação do TSplus Advanced Security e é chamado de “snapshots”. No entanto, é possível definir outro local para este diretório. Isso pode permitir que o administrador defina um diretório localizado em um disco mais rápido (SSD) ou em um disco maior de acordo com suas necessidades. O caminho do diretório de backup não deve ser um caminho UNC, na forma de:

\\ \ \

Adicionando Utilitários de Backup à Lista Branca

Recomendamos adicionar utilitários de backup na lista de permissões.

Relatórios


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.

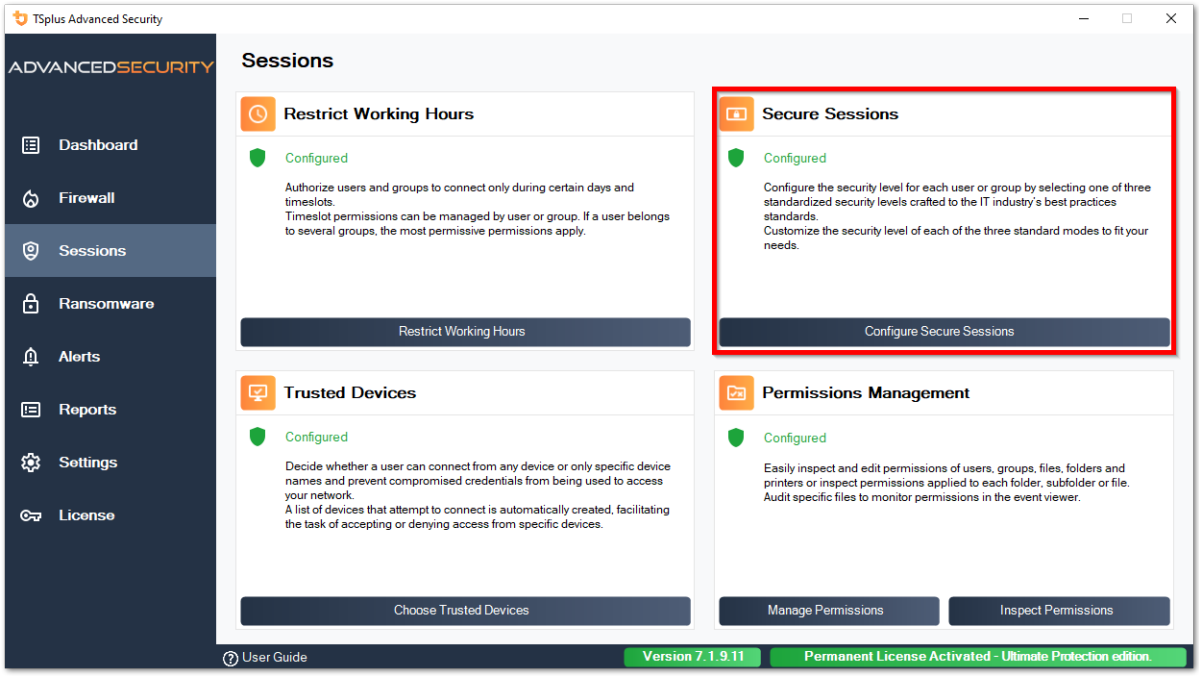
Sessões Seguras

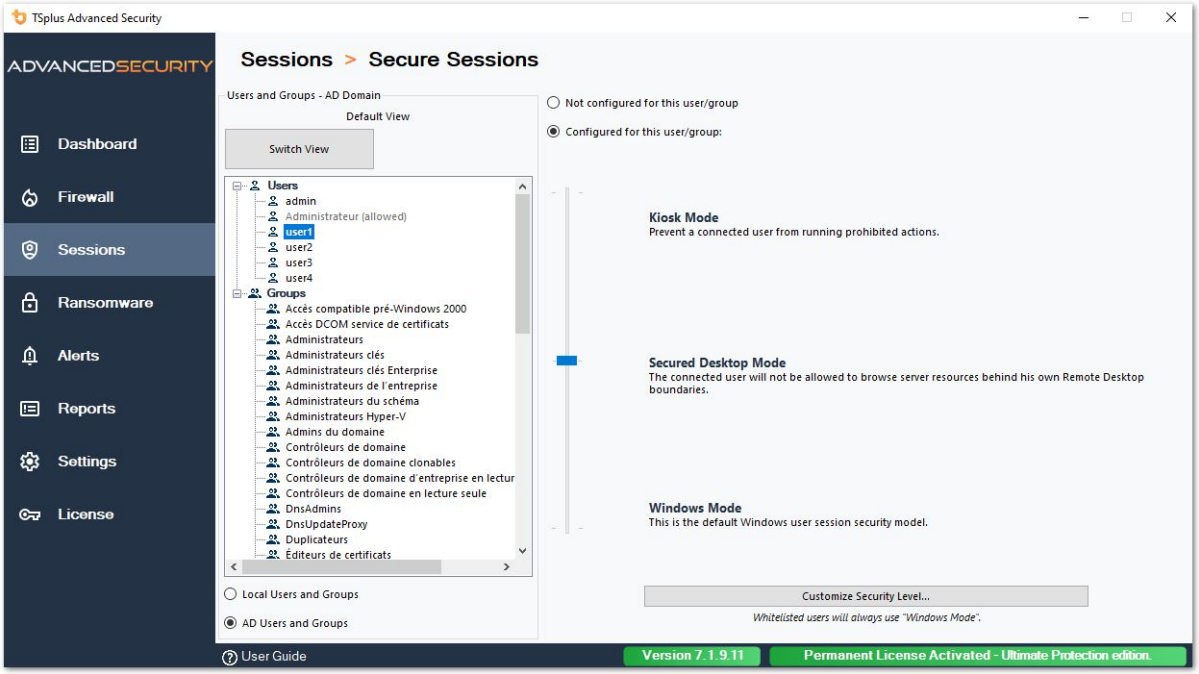
Atenção

- Sessões Seguras provavelmente entrarão em conflito com as políticas de segurança definidas pelo Active Directory.
- O principal objetivo das Sessões Seguras é personalizar a interface do usuário, não aplicar permissões de acesso. Seu uso deve ser combinado com o recurso de Permissões para garantir o acesso a diferentes unidades.

Você pode configurar o nível de segurança para cada usuário ou grupo. Existem três níveis de segurança:

- O **Modo Windows** , onde o usuário tem acesso a uma sessão padrão do Windows.
- O **Modo de Sessões Seguras** onde o usuário não tem acesso ao Painel de Controle, programas, discos, navegador, sem clique com o botão direito…: sem acesso aos recursos do servidor. Ele tem apenas acesso a documentos, impressoras, tecla do Windows e pode desconectar sua sessão.
- O **Modo Kiosk** é o mais seguro, onde o usuário tem ações muito limitadas em sua sessão.

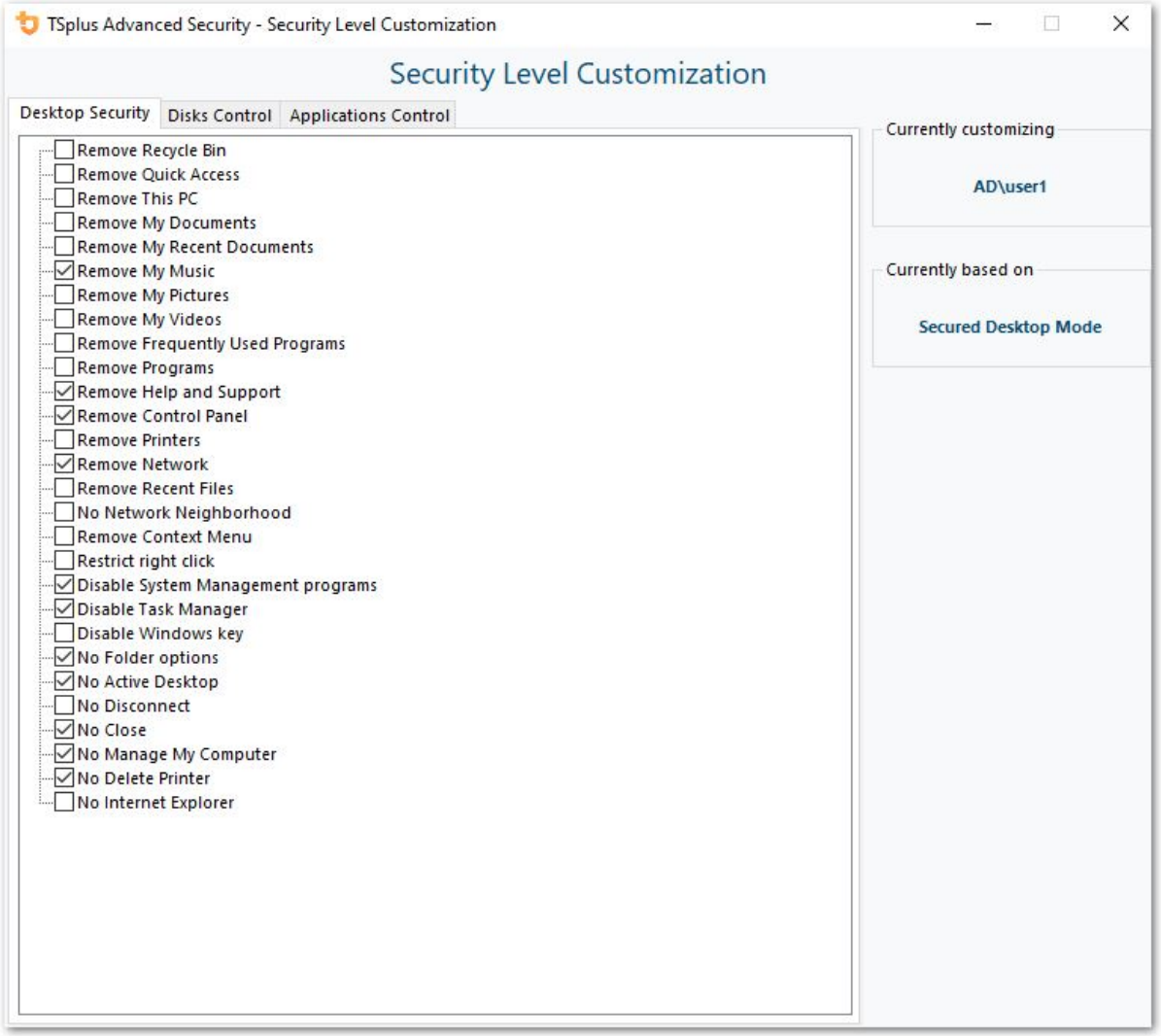




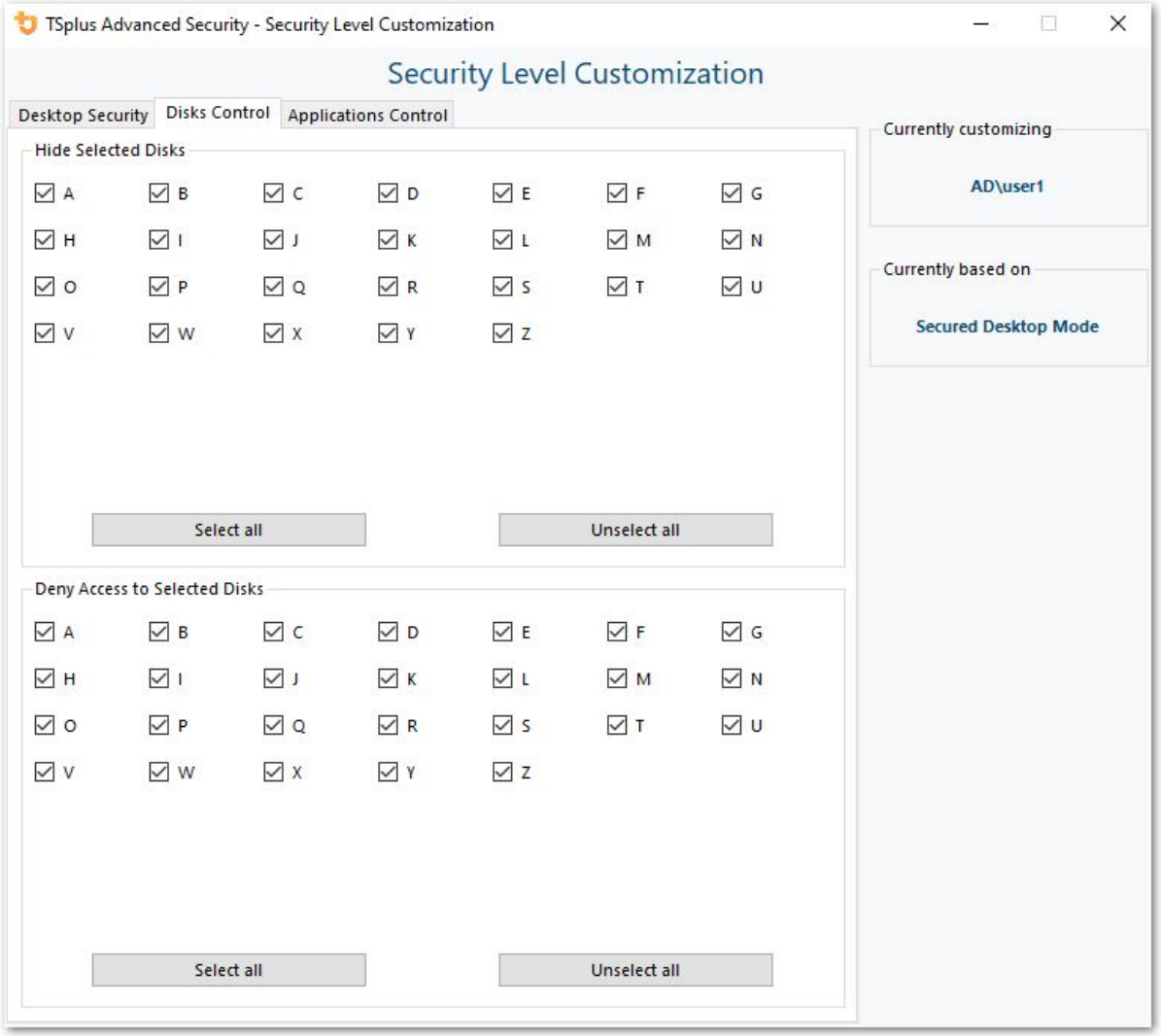
Personalização

Em qualquer modo, você tem a possibilidade de personalizar a segurança em três níveis:

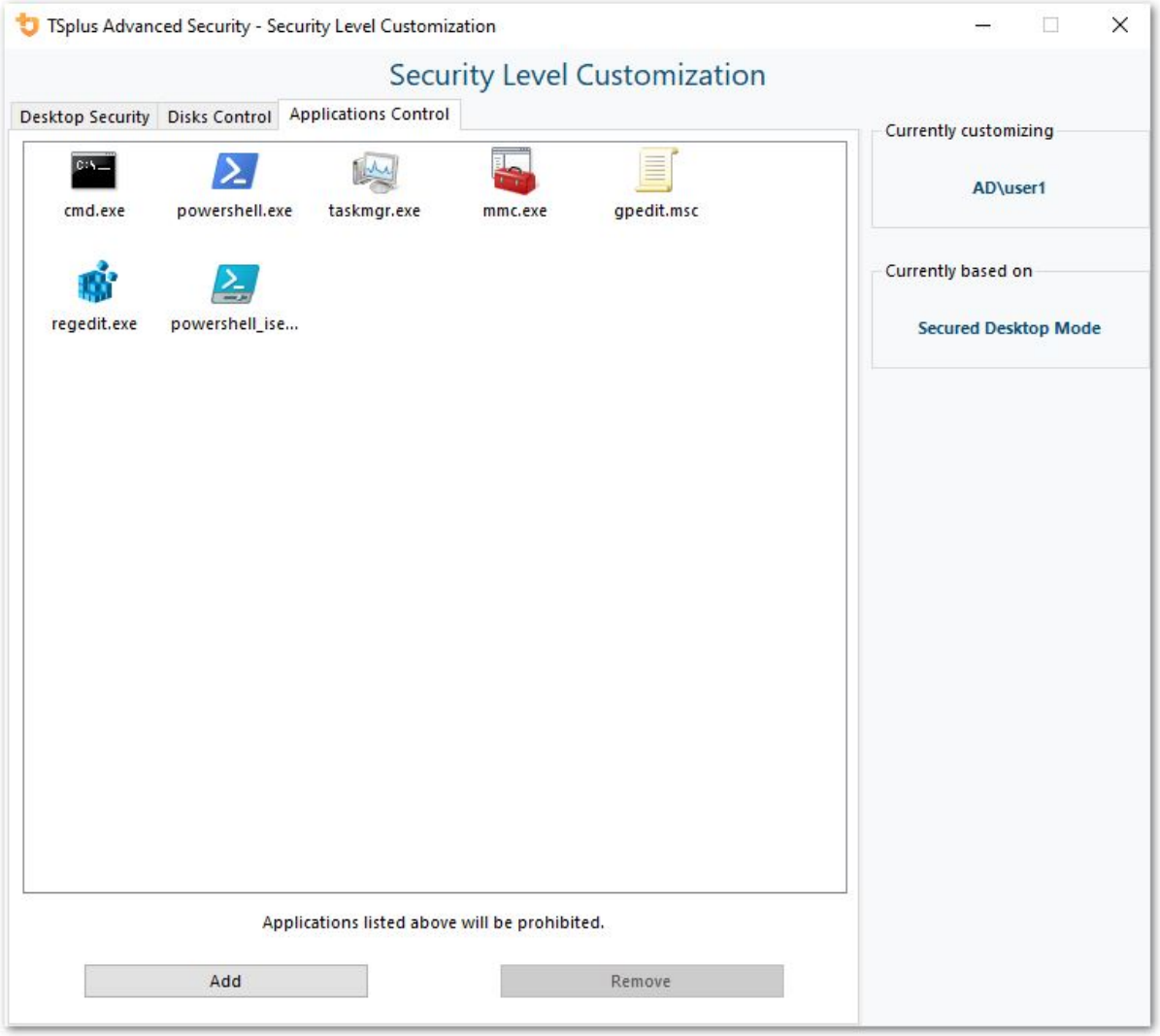
Segurança de Desktop:



Controle de Discos:



Controle de Aplicações:



Prioridades das regras de Usuários/Grupos

Quando um usuário abre uma nova sessão no servidor:

1. Se este usuário tiver um Nível de Segurança definido diretamente para si, então esse Nível de Segurança é aplicado.
2. Se este usuário não tiver um Nível de Segurança definido diretamente para si, então o TSplus Advanced Security carregará quaisquer configurações de Nível de Segurança existentes para todos os grupos deste usuário e manterá as regras mais permissivas.

Por exemplo, se um primeiro grupo tem uma regra para remover o ícone da Lixeira da área de trabalho, mas essa regra está desativada para um segundo grupo, então o usuário terá o ícone da Lixeira em sua área de trabalho. As mesmas regras de prioridade se aplicarão a cada regra personalizada (Segurança da Área de Trabalho, Controle de Discos e Controle de Aplicativos), assim como para o Nível de Segurança principal (o Modo Windows sendo considerado mais permissivo do que o Modo de Área de Trabalho Segura, que é considerado mais permissivo do que o Modo Quiosque).

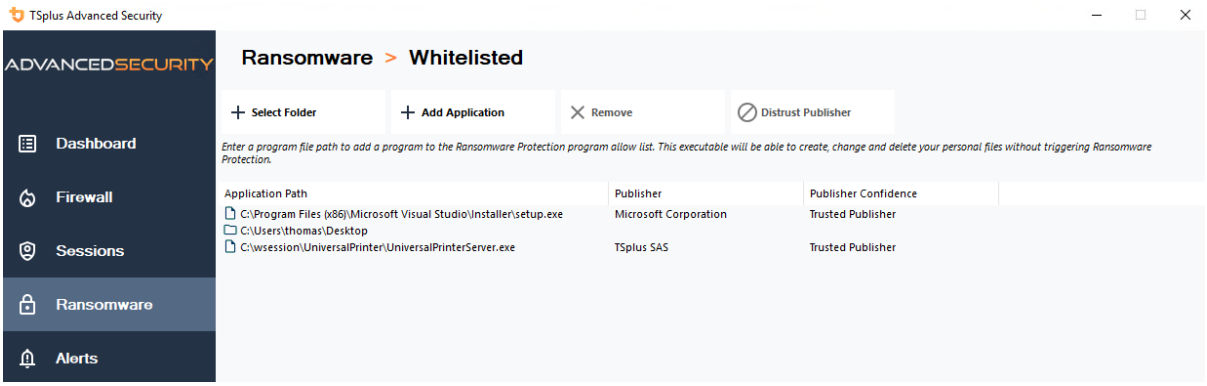
N.B : Para desativar o clique direito em todos os lugares, você deve selecionar as seguintes

duas opções:

- Restringir Clique Direito
- Remover Menu de Contexto

Configurações - Lista de Permissão de Programas

No On the **Aba de Programas** , você pode adicionar programas à lista de programas permitidos, que não serão verificados pela Proteção contra Ransomware do TSplus Advanced Security Por padrão, todos os programas da Microsoft estão na lista de permissões.



Clique no botão "Adicionar Aplicativo" para adicionar um programa. Você também pode removê-los selecionando o(s) aplicativo(s) e clicando no botão Remover Aplicativo(s).

Configurações - Lista de Permissão de Usuários

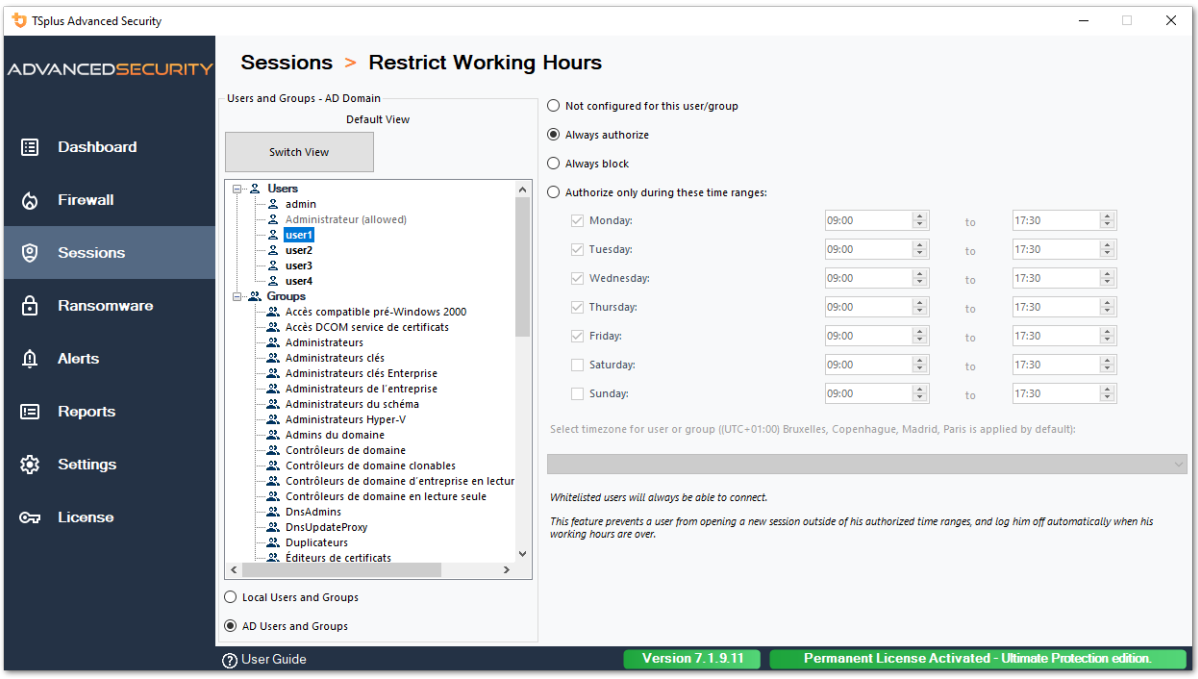
Visualização Avançada

Com a visualização Avançada, adicione e gerencie usuários e grupos de todos os domínios acessíveis.

Você pode alternar a visualização da visualização padrão para a visualização avançada usando o botão “Alternar Visualização”.

A visualização Avançada é usada para exibir e gerenciar todos os usuários e grupos configurados atualmente. Ela também permite que você adicione novos usuários e grupos à lista para configurá-los, utilizando o seletor de pesquisa do AD do Windows. Você pode fazer isso clicando no botão “Adicionar usuário/grupo”. Você poderá então adicionar qualquer usuário disponível de quaisquer domínios acessíveis do seu servidor.

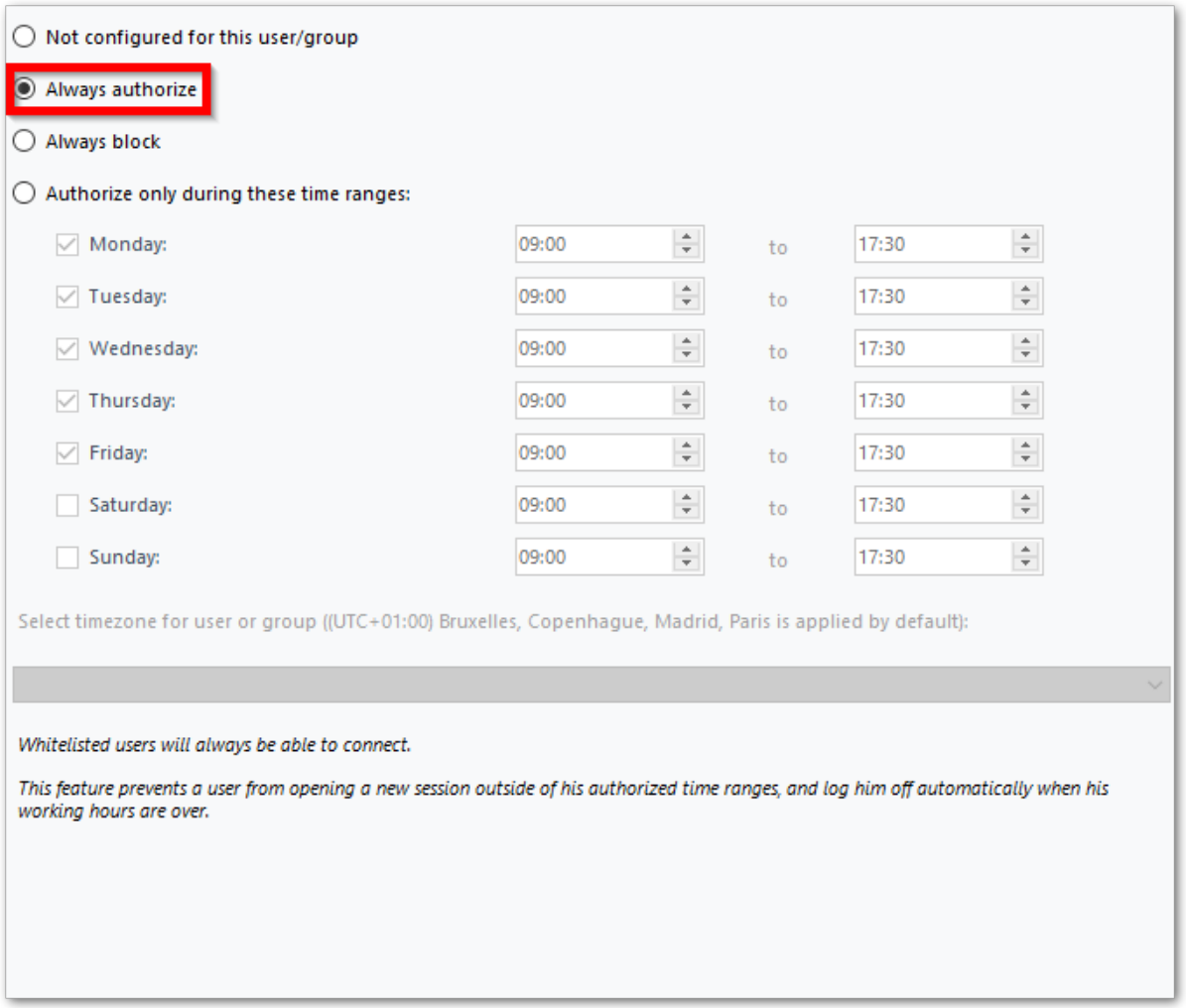
A Visualização Avançada está disponível nos recursos de Permissões, Horário de Trabalho e Are desktops Seguros. Exemplo:



O **Lista de Permissão de Usuários** a guia dá ao Administrador a possibilidade de adicionar/ remover usuários da lista de permissões .

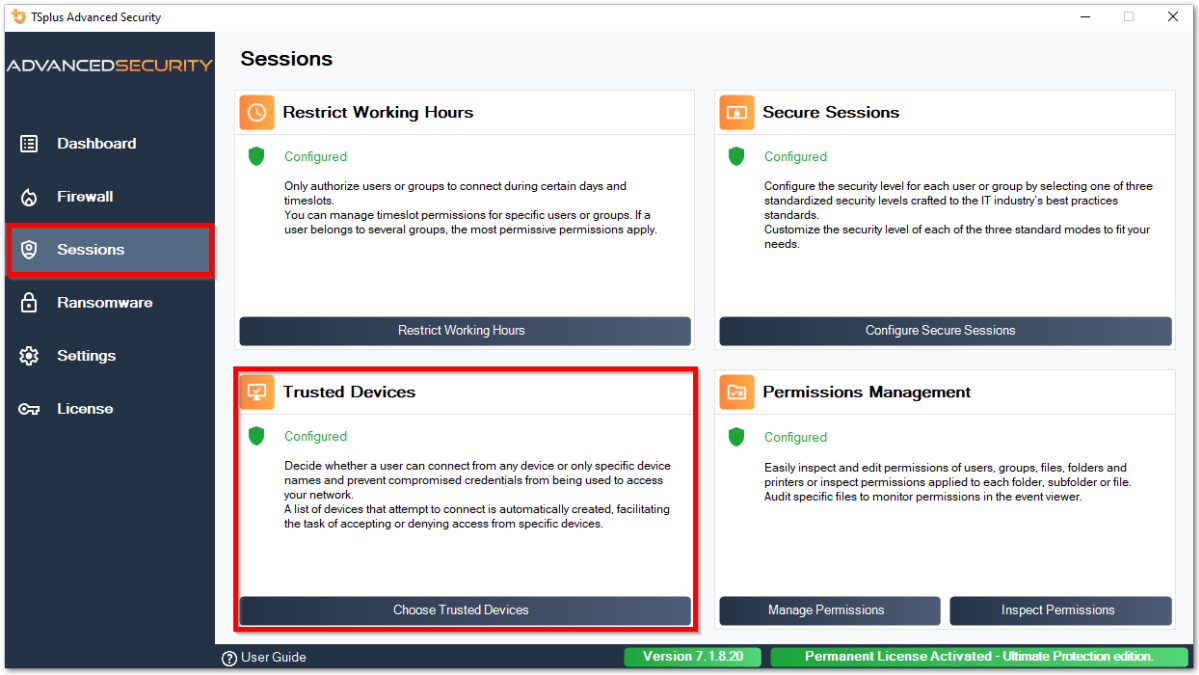
Usuários na lista de permissões são ignorados pelo TSplus Advanced Security e suas configurações não serão aplicadas.

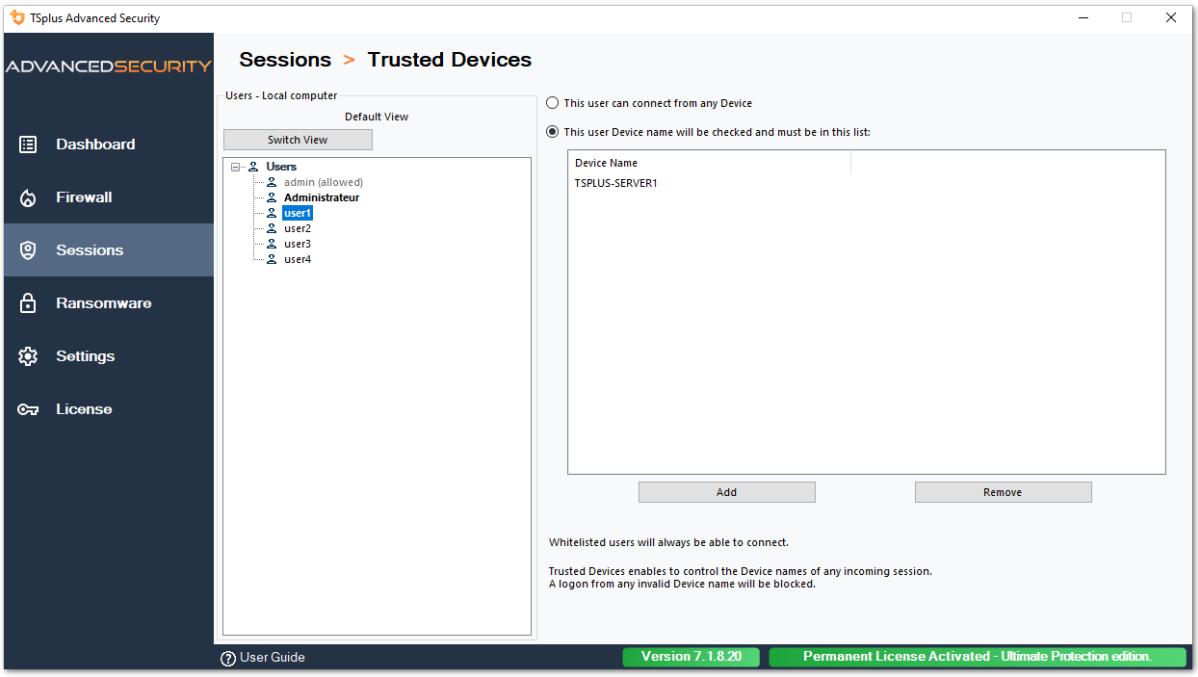
O usuário que instalou o TSplus Advanced Security é adicionado automaticamente à lista de permissões:



Dispositivos Confiáveis

Dispositivos Confiáveis permite que você controle o dispositivo dos usuários, permitindo que cada usuário utilize apenas um ou vários dispositivos específicos, que serão verificados em qualquer sessão de entrada. Um logon de qualquer nome de dispositivo inválido será bloqueado.





Neste exemplo, **User1** usará o nome do dispositivo **TSPLUS-SERVER1** somente.

Preenchimento automático do campo de nome do dispositivo

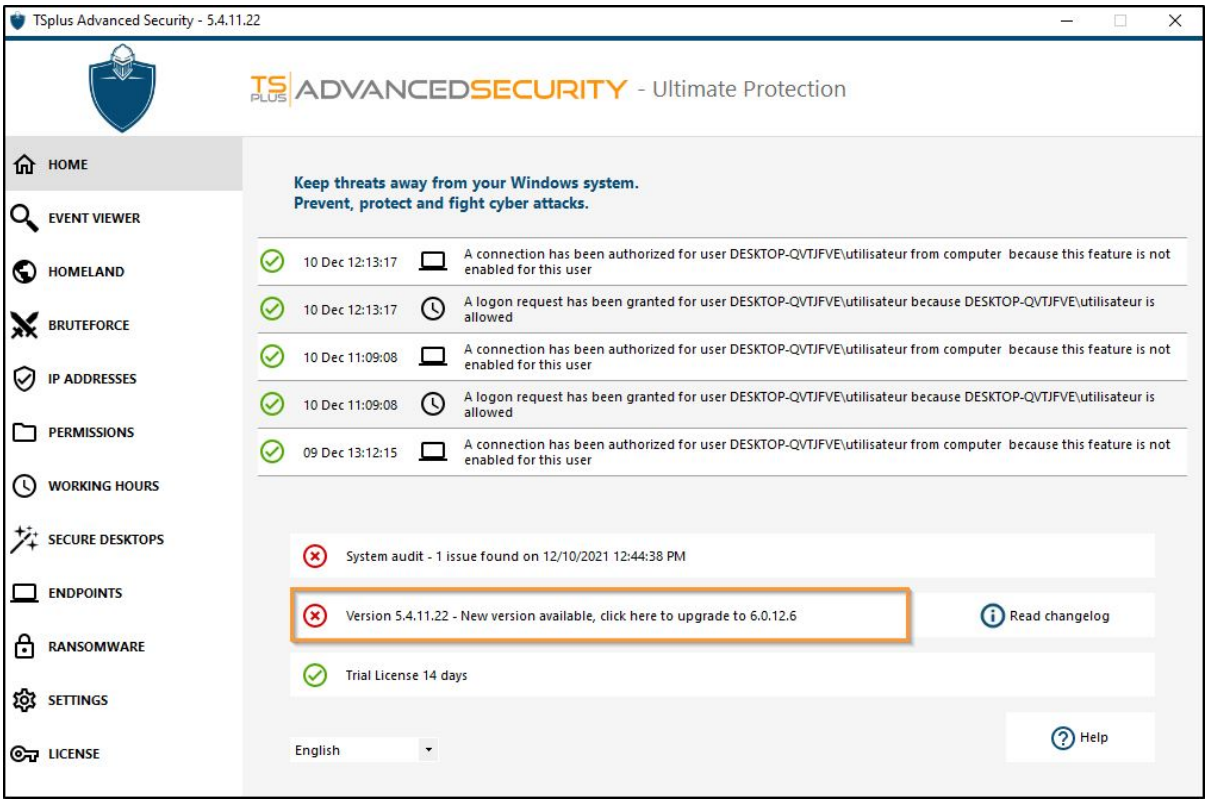
Você pode notar que o campo Nome do Dispositivo já está preenchido com um nome de dispositivo para alguns usuários. Para ajudar o administrador, o TSplus Advanced Security salvará automaticamente o nome do último dispositivo usado para se conectar ao servidor por qualquer usuário que não tenha o recurso Dispositivos Confiáveis habilitado. Após um dia útil, o nome do dispositivo da maioria dos usuários será conhecido pelo advanced-security, permitindo assim que você ative rapidamente o recurso de Proteção de Endpoint sem precisar verificar o nome da estação de trabalho de cada usuário.

Nota Dispositivos Confiáveis não é compatível com conexões HTML5.

Atualizando TSplus Advanced Security

Confira nossas correções e melhorias clicando em Registro de alterações

Atualizar o TSplus Advanced Security é fácil e pode ser feito clicando no bloco correspondente, a partir da Página Inicial:



Em seguida, o TSplus Advanced Security baixa e aplica a atualização.

Nota: seus dados e configurações são sempre copiados antes de uma atualização e podem ser encontrados no diretório “archives”, na pasta de configuração do TSplus Advanced Security. Veja Backup e restaure seus dados e configurações

Restringir Horário de Trabalho

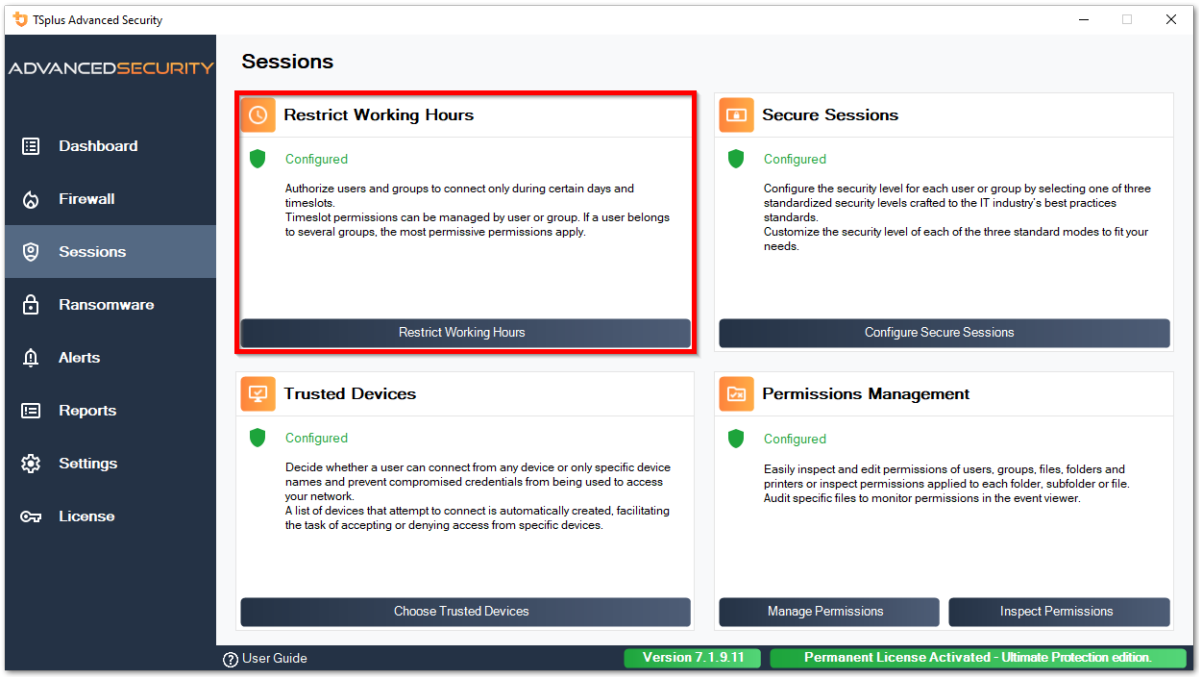
Você pode configurar restrições de horário de trabalho por usuário ou por grupo.

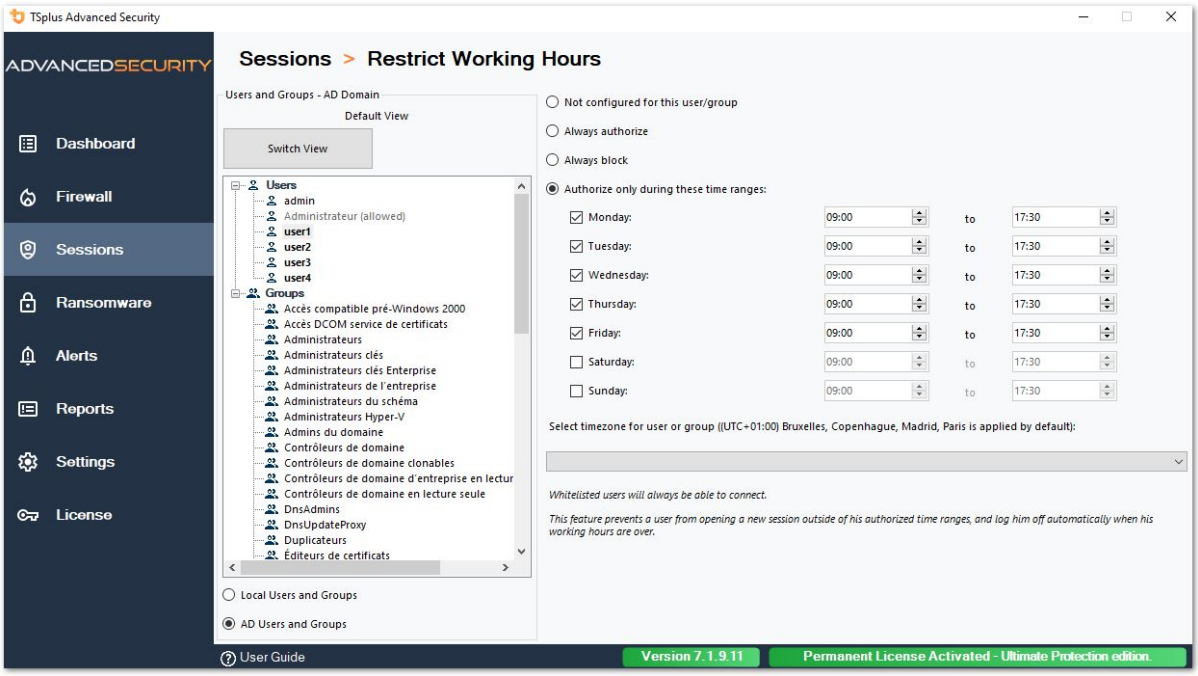
Escolha a restrição de sua escolha:

- Sempre autorize o acesso deste usuário/grupo
- Sempre bloqueie o acesso deste usuário/grupo

ou autorize apenas durante intervalos de tempo específicos.

Você pode configurá-lo dia a dia e selecionar o intervalo de tempo de sua preferência:





É possível selecionar um fuso horário específico dependendo da localização do escritório do seu usuário.

Uma desconexão automática ao final do horário de trabalho configurado é realizada.

É possível agendar uma mensagem de aviso antes que o usuário seja desconectado de Configurações > Avançado > Horário de Trabalho .

###Prioridades das regras de Usuários/Grupos

Quando um usuário abre uma nova sessão no servidor:

1. se este usuário tiver restrições de Horário de Trabalho diretamente definidas para si, então essas regras são aplicadas.

2. se este usuário não tiver restrições de Horário de Trabalho definidas diretamente para si, então o TSplus Advanced Security carregará quaisquer restrições de Horário de Trabalho existentes para todos os grupos deste usuário e manterá as regras mais permissivas. Por exemplo, se um primeiro grupo tiver uma regra para bloquear a conexão na segunda-feira, um segundo grupo tiver uma regra para autorizar a conexão na segunda-feira das 9h às 17h e um terceiro grupo tiver uma regra para autorizar a conexão na segunda-feira das 8h às 15h, então o usuário poderá abrir uma conexão na segunda-feira das 8h às 17h.

Atenção: Este recurso utiliza o horário do servidor. Usar o horário da estação de trabalho do usuário e/ou o fuso horário seria inútil, pois tudo o que o usuário teria que fazer seria alterar seu fuso horário para abrir uma sessão fora de suas horas autorizadas.