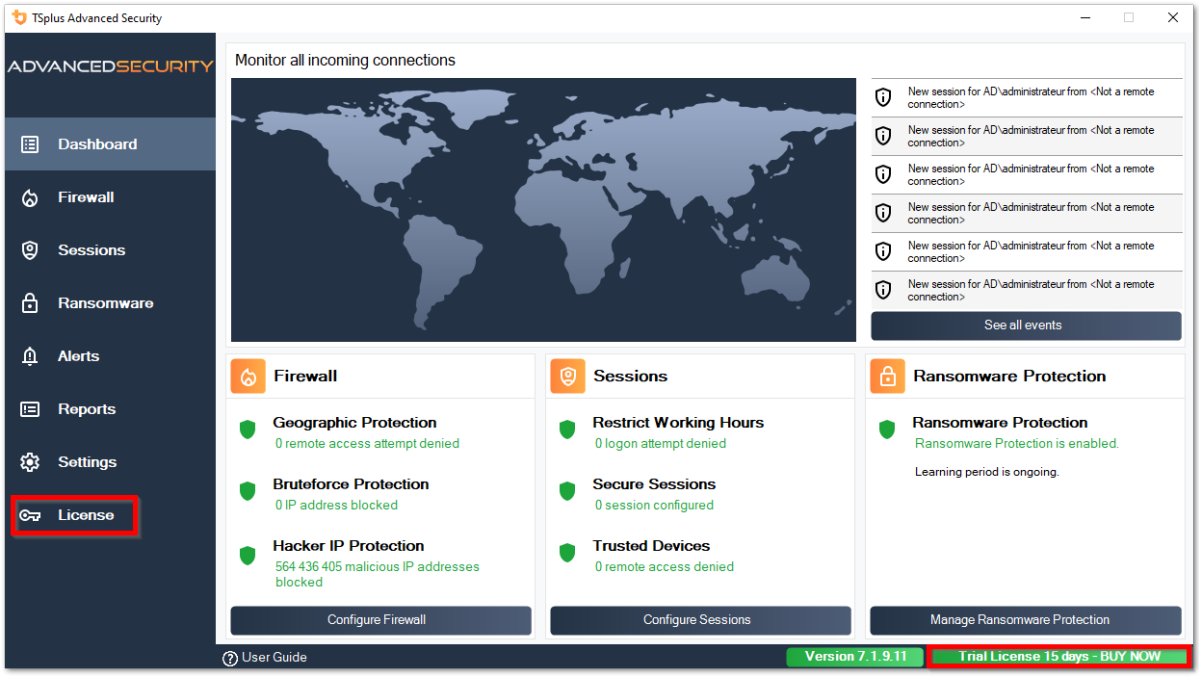
TSplus Advanced Security - Attivazione della tua licenza

Passo 1: Attivare la tua licenza dalla modalità Lite

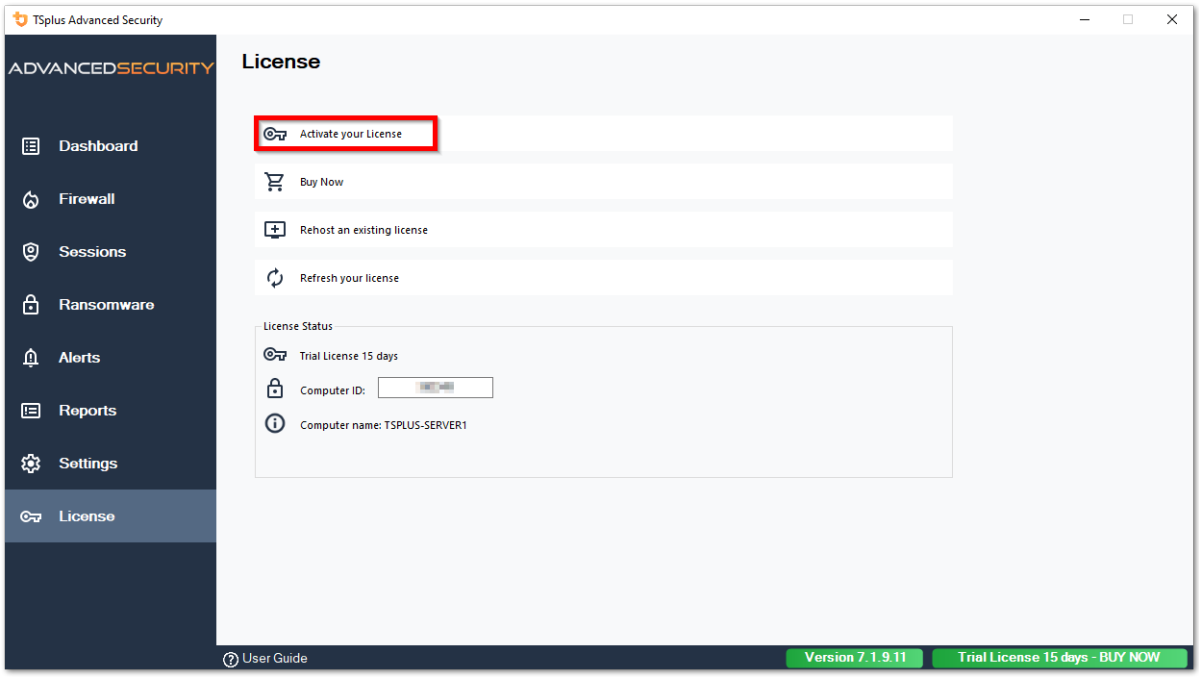
Clicca sul pulsante "Licenza di prova" per acquistare una licenza o sulla scheda Licenza se hai già una licenza e una Chiave di attivazione.



Poi, fai clic sul pulsante "Attiva la tua licenza".

Troverai la tua chiave di attivazione permanente **XXXX-XXXX-XXXX-XXXX** nella nostra email di conferma dell'ordine.

Se desideri attivare il tuo abbonamento, inserisci il tuo codice di abbonamento. **S-XXXX-XXXX-XXXX-XXXX** .



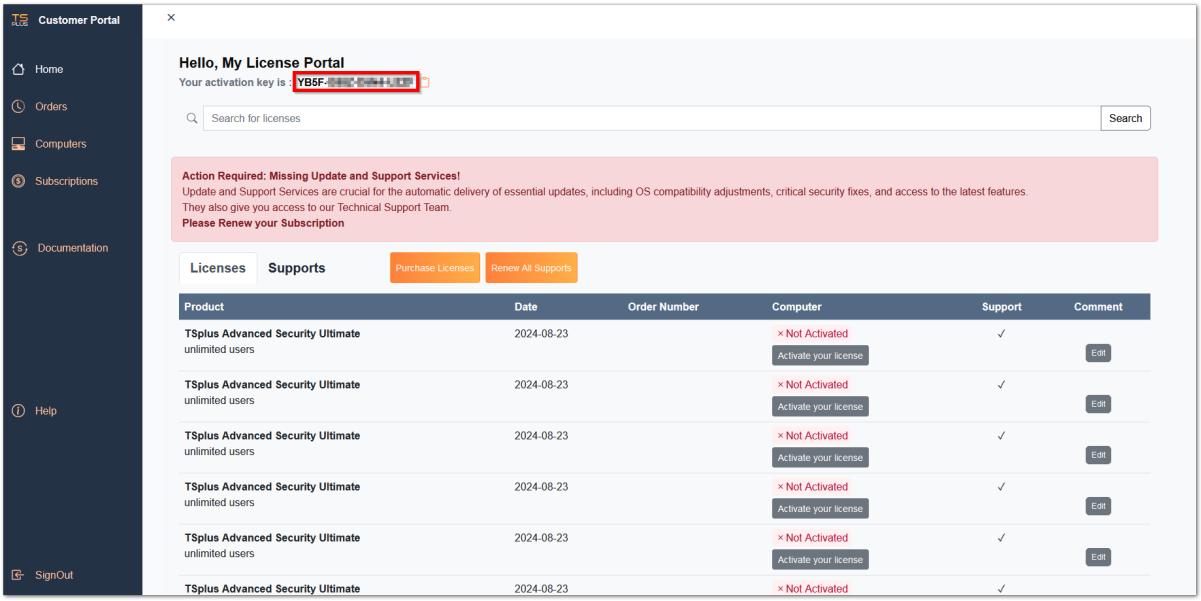
Se non conosci la tua chiave di attivazione, procedi al passo 2. Altrimenti, procedi al passo 3.

Passo 2: Recupera la tua chiave di attivazione dal portale di licenza

Per ottenere la tua Chiave di Attivazione, connettiti al nostro Portale di Licenza e inserisci il tuo indirizzo email e il tuo numero d'ordine:

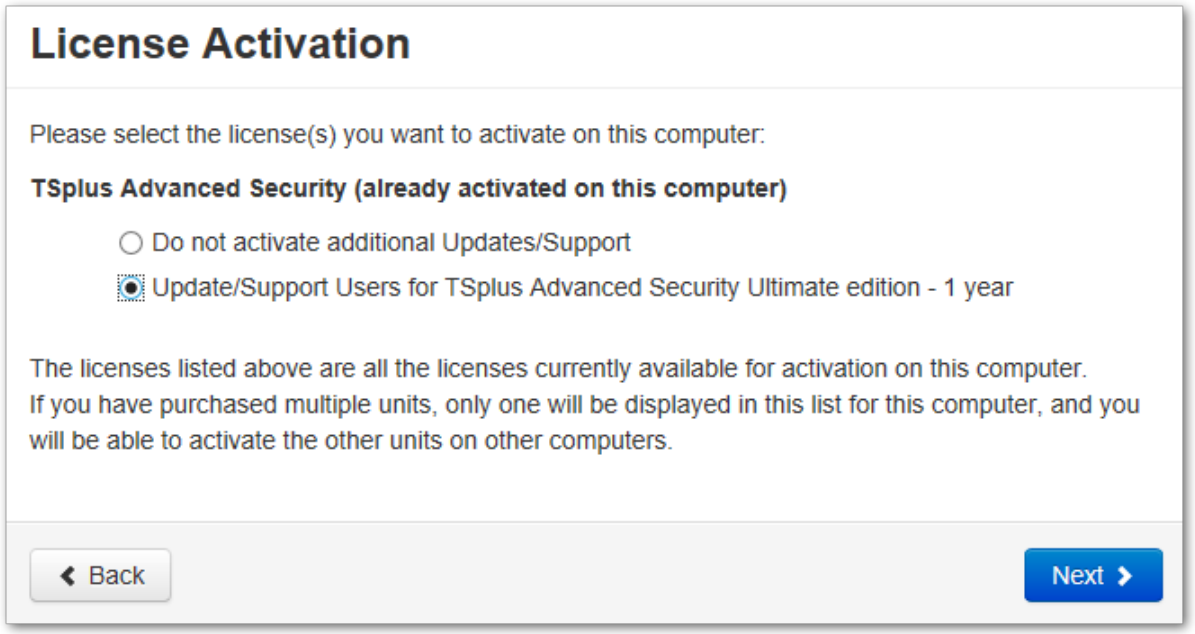
Scarica la Guida dell'Utente del Portale Clienti per ulteriori informazioni sul tuo portale clienti.

La tua chiave di attivazione verrà visualizzata nella parte superiore della dashboard:

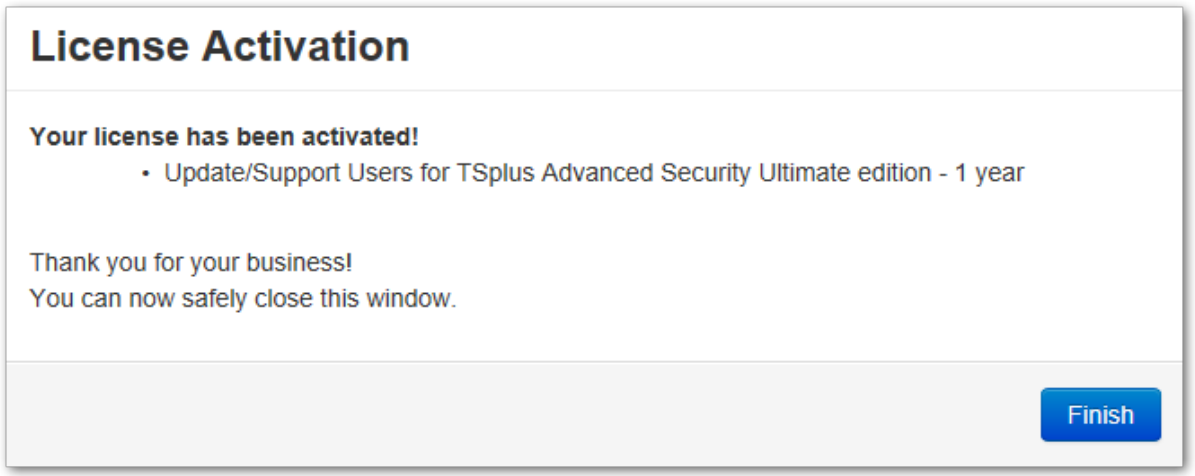


Passo 3: Seleziona le licenze richieste e i servizi di Aggiornamento e Supporto per i prodotti installati

Inserisci la tua chiave di attivazione e fai clic su "Avanti".

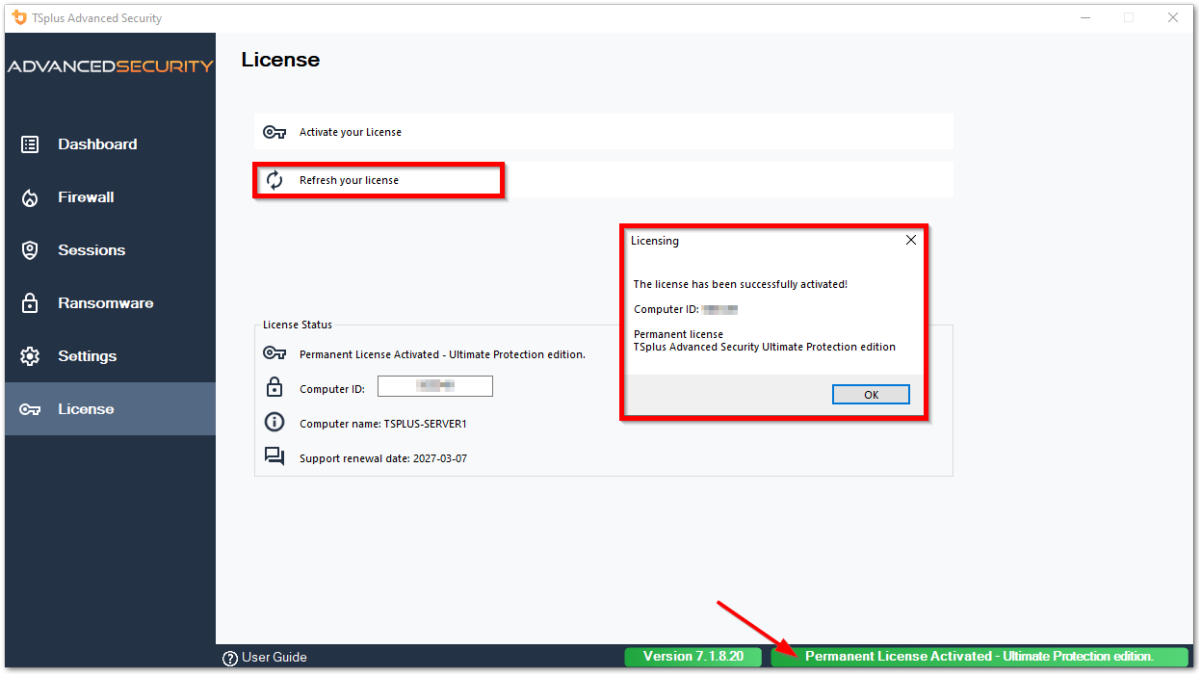


Controlla uno o più elementi e fai clic sul pulsante "Avanti". Si prega di notare che è possibile attivare più prodotti contemporaneamente selezionando diversi prodotti e/o abbonamenti di supporto.



Tutti i tuoi prodotti selezionati e gli abbonamenti al supporto sono ora attivati (in questo esempio, sia TSplus con supporto che TSplus Advanced Security sono stati attivati contemporaneamente).

Aggiorna il tuo stato di licenza facendo clic sul pulsante corrispondente.



Attivazione della tua licenza (Offline)

Si prega di fare riferimento alla procedura descritta per TSplus Remote Access: Attivazione della tua licenza TSplus (offline)

Riassegnare la tua licenza

Si prega di fare riferimento alla procedura descritta per TSplus Remote Access: Rehosting la tua licenza TSplus

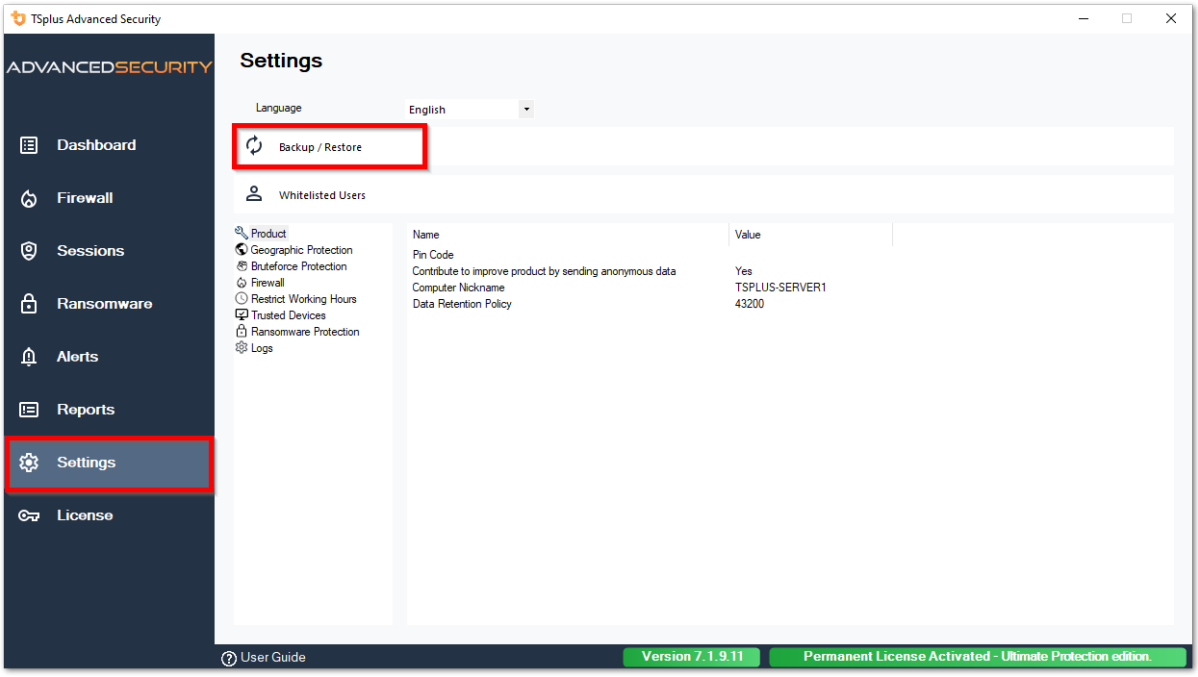
Nota: Puoi scaricare un file license.lic nel Portale di Licenza per le versioni di TSplus Advanced Security qui sotto. Si prega di fare riferimento a Guida dell'utente del portale clienti per ulteriori informazioni.

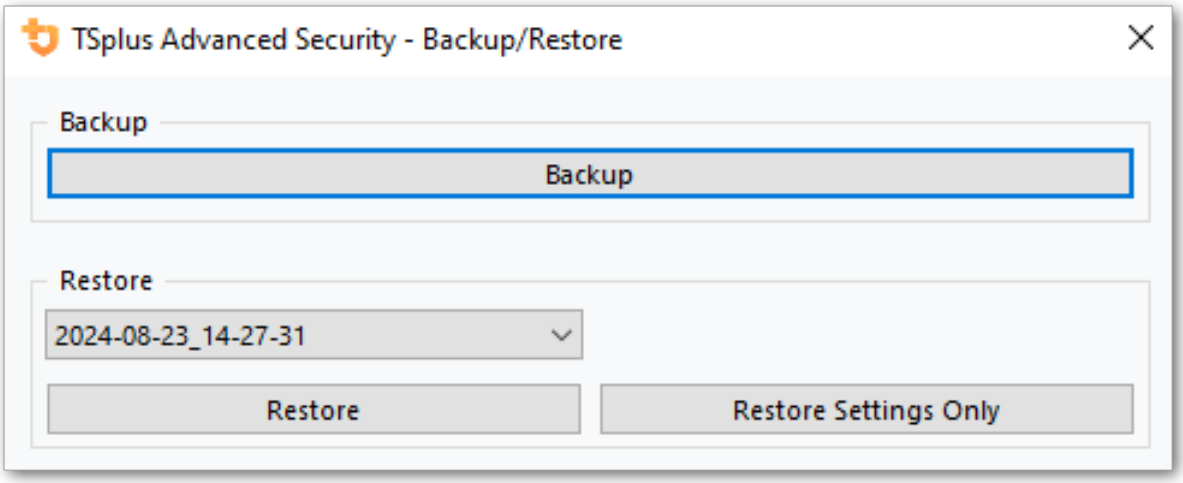
Grazie per aver scelto TSplus Advanced Security!

Avanzato - Backup e Ripristino

Backup e ripristino di dati e impostazioni

Puoi eseguire il backup o ripristinare i dati e le impostazioni di TSplus Advanced Security facendo clic sul pulsante "Backup / Ripristina" in alto:





Il backup verrà salvato nella cartella **archivi** situato nella directory di installazione di TSplus Advanced Security. Per impostazione predefinita, il **archivi** la cartella si trova qui: C:\Program Files (x86)\TSplus-Security\archives

Utilizzare la riga di comando per eseguire il backup e il ripristino

L'uso del comando è descritto di seguito:

- **Backup** TSplus-Security.exe /backup [percorso facoltativo a una directory]

Per impostazione predefinita, il backup verrà creato nella directory degli archivi situata nella cartella di installazione di TSplus Advanced Security. Tuttavia, il backup può essere salvato in una cartella specificata. Sono consentiti percorsi relativi e assoluti.

- **Ripristina** TSplus-Security.exe /restore [percorso a una directory di backup]

La directory di backup specificata deve contenere una cartella dati e una cartella impostazioni, come creato dal comando /backup.

Configurazione dei backup

Si prega di notare che è possibile specificare le seguenti impostazioni avanzate nel registro:

- La directory di backup può essere specificata nella chiave di registro. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath Per impostazione predefinita, verrà utilizzata la directory "archivi" della directory di installazione di Advanced Security.
-

Il numero massimo di backup disponibili può essere specificato nella chiave di registro. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives Per impostazione predefinita, Advanced Security mantiene gli ultimi 3 backup.

Migra i tuoi dati e impostazioni su un altro computer

Si prega di seguire i passaggi seguenti per migrare Advanced Security dal computer A al computer B:

1. Su computer A, fai clic sul pulsante Backup per creare un nuovo backup. Le impostazioni e i dati verranno salvati nella directory degli archivi, situata nella directory di configurazione di advanced-security (tipicamente C:\Program Files (x86)\TSplus-Security\archives).

2. Copia la nuova cartella di backup creata (ad esempio chiamata backup-2019-09-11_14-37-31), inclusi tutti i contenuti, dalla directory degli archivi sul computer A alla directory degli archivi sul computer B.

3. Su computer B, dalla finestra Backup / Ripristino, nella sezione "Ripristina", selezionare il nome del backup pertinente da ripristinare.

4. Poi, fai clic su Ripristina solo impostazioni per ripristinare le impostazioni. In alternativa, è possibile fare clic su Ripristina per ripristinare tutti i dati e le impostazioni, il che non è consigliato per una migrazione ma utile per ripristinare la sicurezza avanzata sul computer A.

5. Attendere al massimo 2 minuti affinché le impostazioni vengano ricaricate dalle funzionalità di sicurezza avanzata.

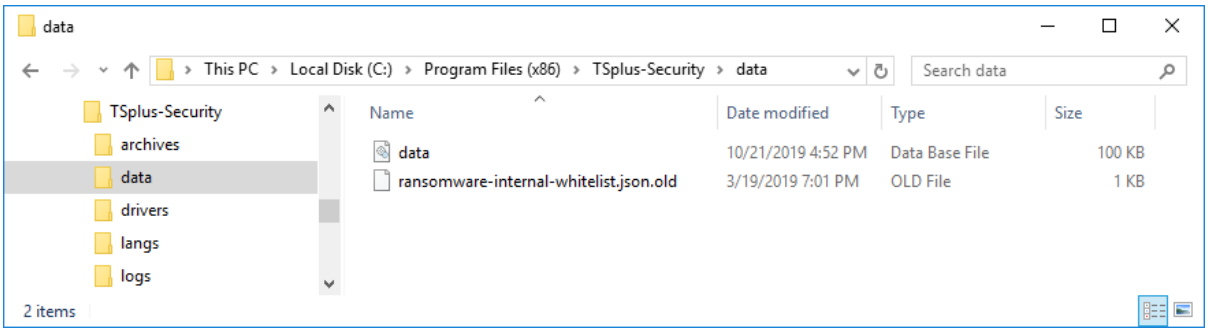
Database

Un database memorizza eventi, indirizzi IP, rapporti sugli attacchi ransomware e elenchi di programmi autorizzati.

Questo database è memorizzato in **dati** cartella situata nella directory di installazione di TSplus Advanced Security.

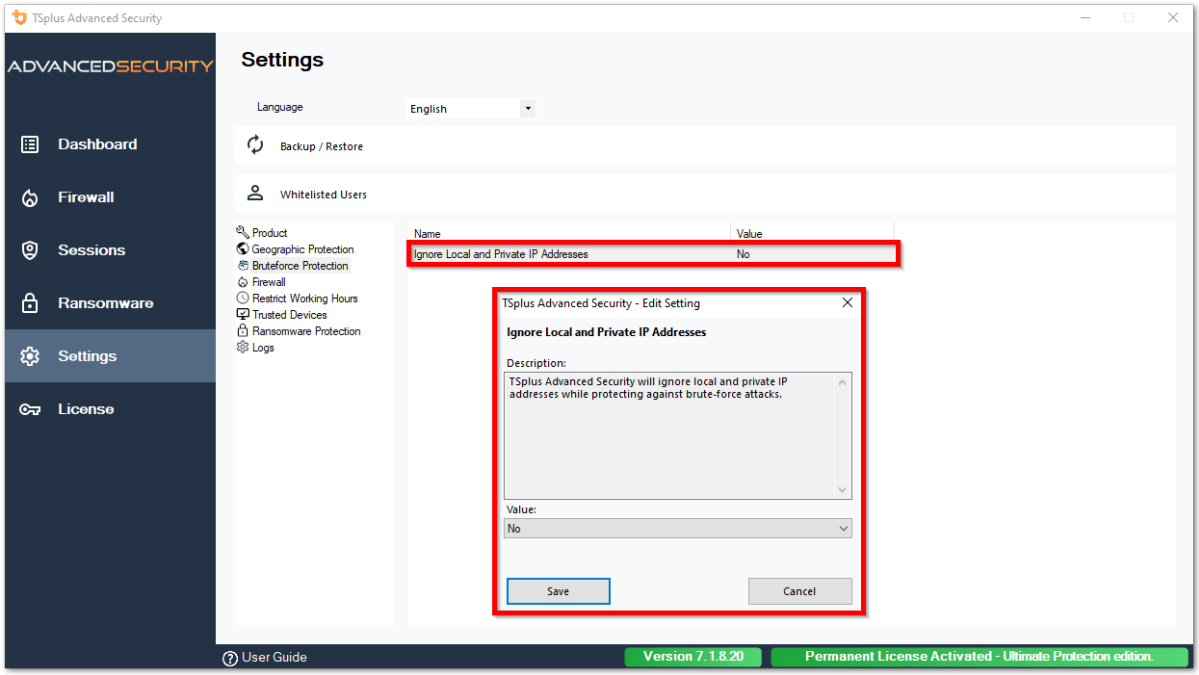
- Sicurezza Avanzata dalla versione 5 e prima della versione 5.3.10.6 utilizza un motore di database LiteDB .

- Advanced Security sopra la versione 5.3.10.6 utilizza un motore di database SQLite .



Protezione avanzata - Protezione da attacchi di forza bruta

Il **Protezione da attacchi di forza bruta** la scheda ti consente di Ignora indirizzi IP locali e privati se lo desideri, cambiando il valore predefinito da "No" a "Yes".

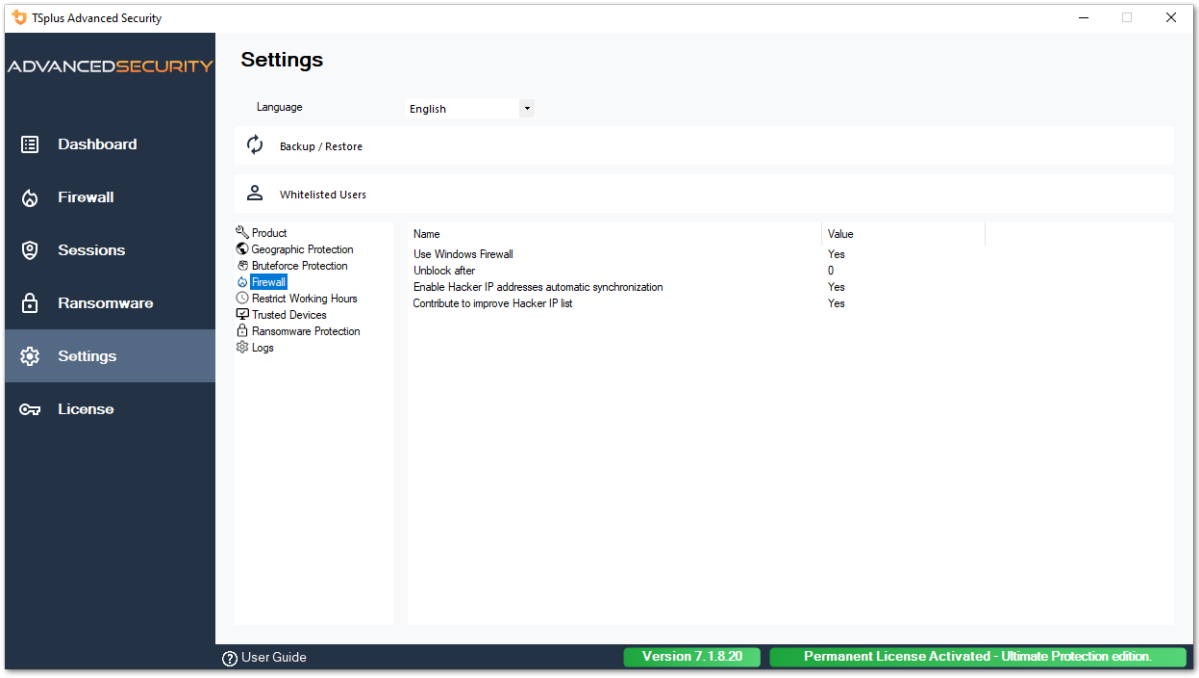


Avanzato - Firewall

Il **Firewall** la scheda consente di attivare il **Windows Firewall o disattivalo a favore del firewall integrato di TSplus Advanced Security** .

Dalla versione 4.4, è incluso un firewall integrato in TSplus Advanced Security.

Come regola generale, se il firewall di Windows è attivato sul tuo server, allora dovresti usarlo per applicare le regole di TSplus Advanced Security (predefinito). Se hai installato un altro firewall, allora devi attivare il firewall integrato di TSplus Advanced Security.



Usa Windows Firewall Per attivare il firewall integrato, vai su Impostazioni > Avanzate > Prodotto > Usa Windows Firewall e imposta il valore su: No. Se Sì, gli indirizzi IP problematici verranno bloccati utilizzando Windows Firewall. In caso contrario, verrà utilizzato il firewall di TSplus Advanced Security.

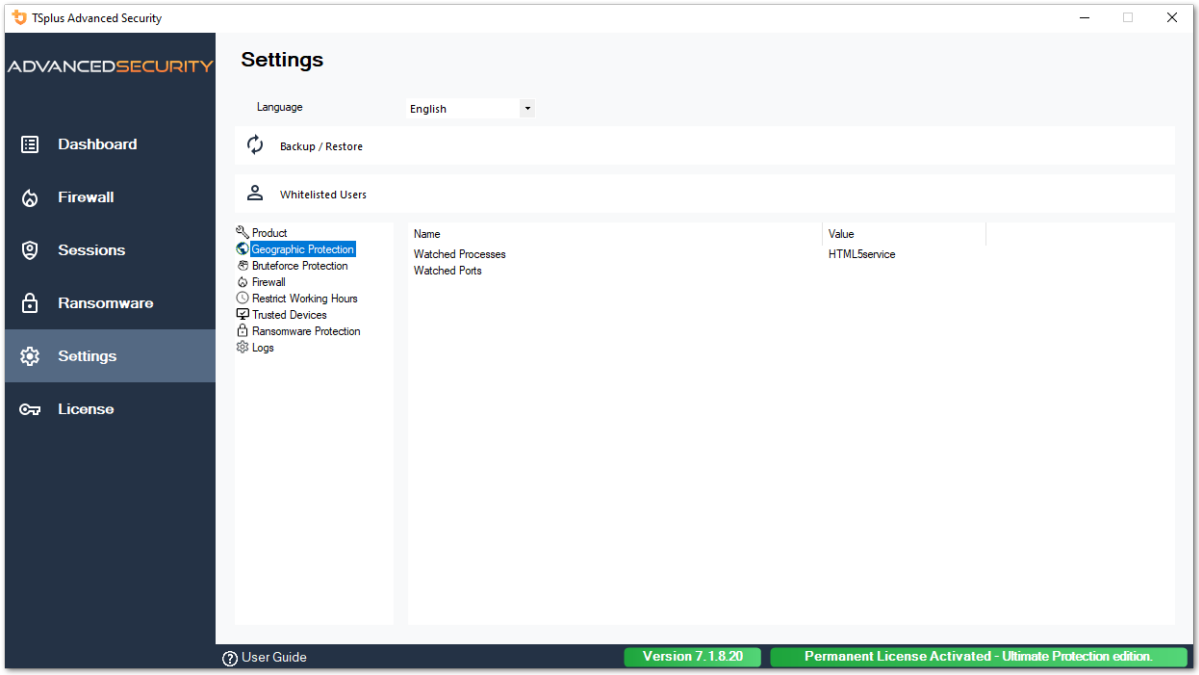
Sblocca dopo Cambia questa impostazione per sbloccare automaticamente gli indirizzi IP dopo un certo periodo di tempo (in minuti). Il valore predefinito è 0, disabilitando questa funzione. Valore: 0

Abilita la sincronizzazione automatica degli indirizzi IP degli hacker Mantieni la tua macchina protetta contro minacce conosciute come attacchi online, abuso di servizi online, malware, botnet e altre attività elettroniche con la Protezione IP Hacker. È richiesta l'abbonamento ai servizi di supporto e aggiornamenti. Valore: Sì

Contribuisci a migliorare l'elenco degli IP degli hacker Consenti a TSplus Advanced Security di inviare statistiche di utilizzo anonime per migliorare la protezione contro gli IP degli hacker.
Valore: Sì

Protezione geografica avanzata

Il **Protezione geografica** la scheda consente di aggiungere o rimuovere i processi che vengono monitorati da Protezione geografica funzionalità.



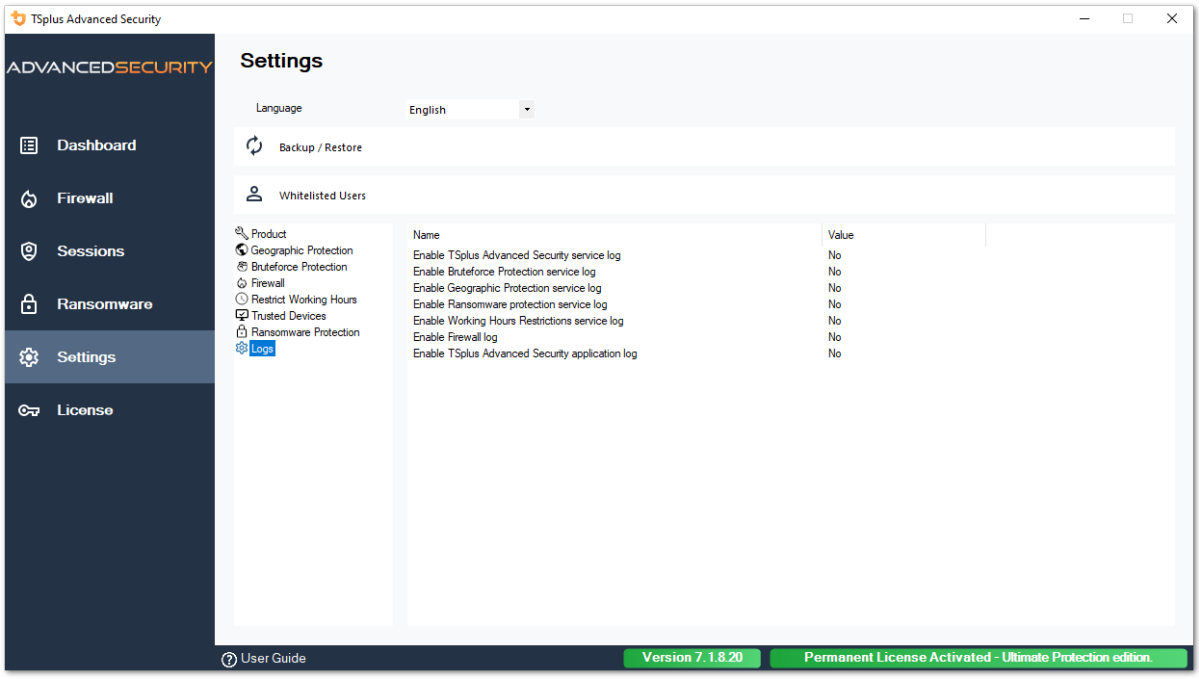
Per impostazione predefinita, il servizio HTML5 è monitorato.

Il **Porte monitorate** le impostazioni ti consentono di aggiungere porte monitorate da Protezione geografica feature. Per impostazione predefinita, la Protezione Geografica ascolta le porte predefinite utilizzate per connettersi in remoto a un server. Queste porte includono RDP (3389), Telnet (23) e le porte VNC. La Protezione Geografica supporta i seguenti fornitori VNC: Tight VNC, Ultra VNC, Tiger VNC e Real VNC, che non sono in alcun modo correlati a TSplus.

Avanzato - Registri

Il **Registri** la scheda ti consente di abilitare o disabilitare i registri di servizio e funzionalità I log esistono per trovare più facilmente l'origine degli errori riscontrati su TSplus Advanced Security.

Per recuperare i registri, apri un Esplora risorse e naviga verso il **registri** cartella della directory di installazione di TSplus Advanced Security. Per impostazione predefinita, i registri si troveranno qui: **C:\Program Files (x86)\TSplus-Security\logs**



Abilita o disabilita Servizi e registri delle applicazioni di TSplus Advanced Security , che sono rispettivamente il servizio di configurazione globale che funziona in background e il registro per l'interfaccia dell'applicazione.

Puoi anche abilitare i registri corrispondenti alle rispettive funzionalità di TSplus Advanced Security:

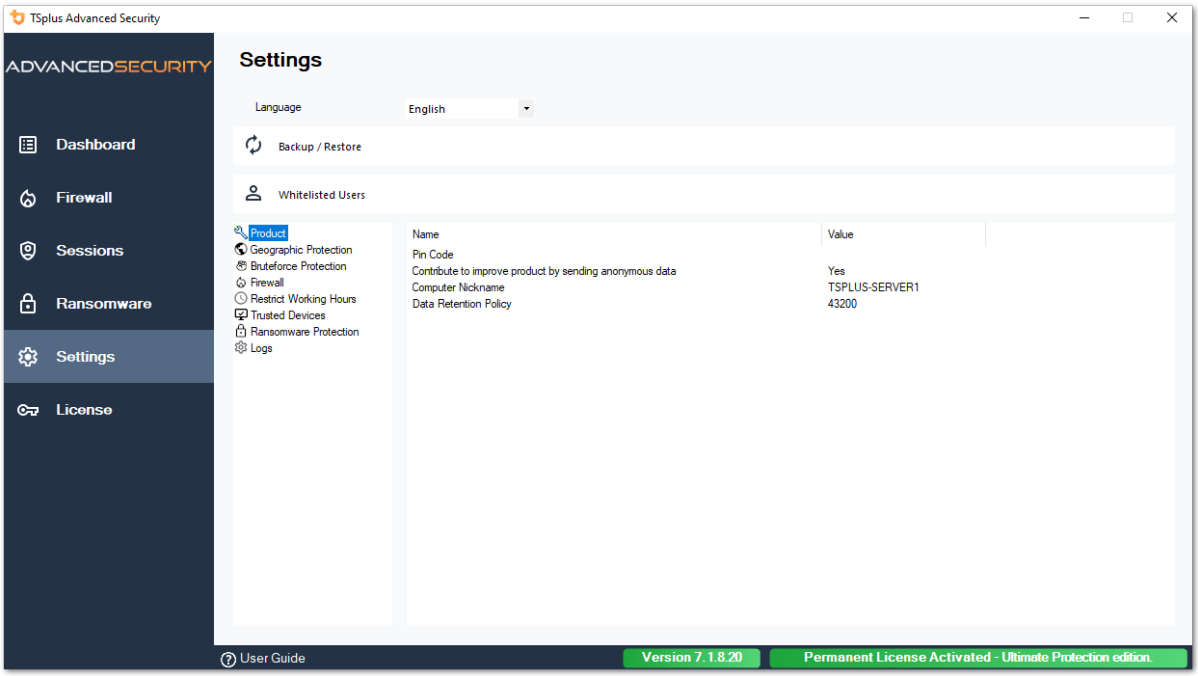
- Servizio
- Protezione da attacchi di forza bruta
- Protezione geografica
- Protezione da Ransomware

- Limitare l'orario di lavoro
- Firewall..
- Applicazione

Tutti i registri sono disabilitati per impostazione predefinita. I registri corrispondono a diversi componenti, il nostro team di supporto ti dirà quale valore inserire in base al problema riscontrato.

Avanzato - Prodotto

Il **Prodotto** la scheda ti consente di aggiungi un codice PIN all'applicazione :



Clicca su Salva. Il codice PIN sarà richiesto la prossima volta che avvii l'applicazione.

Puoi anche **contribuire a migliorare il prodotto** , inviando dati anonimi (attivato per impostazione predefinita): SÌ

I seguenti dati verranno raccolti in caso di un attacco di Ransomware:

- La versione di TSplus Advanced Security.
- Versione di Windows.
- Percorsi di file sospetti che portano all'attacco ransomware.

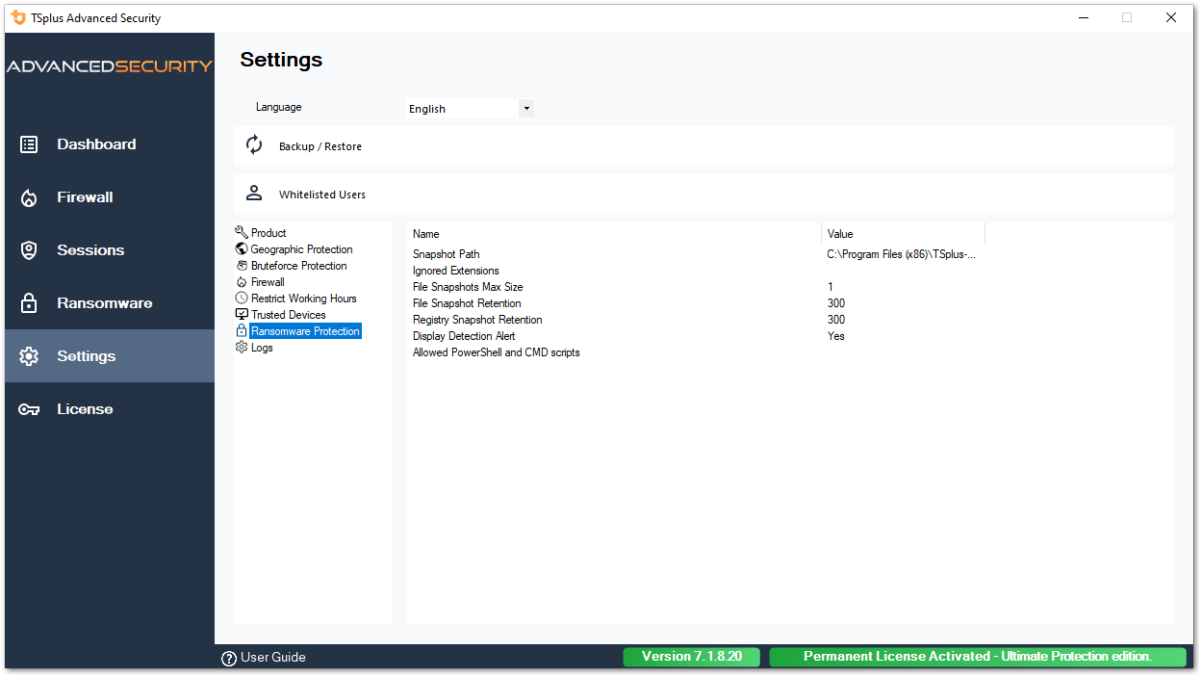
Modifica del **Nome del computer** è anche possibile.

Il **Politica di Conservazione dei Dati** definisce il periodo di tempo dopo il quale gli eventi di TSplus Advanced Security vengono rimossi dal database. Viene eseguito un backup prima di ogni pulizia del database. Questa politica è definita in minuti. La politica di conservazione dei dati

predefinita è di 259.200 minuti, ovvero 6 mesi.

Protezione avanzata - Ransomware

Il **Protezione da Ransomware** la scheda ti consente di configurare le proprietà dello snapshot e definire le estensioni di file ignorate per la funzione di protezione da ransomware.



Percorso dello snapshot Definire la directory in cui Ransomware Protection memorizza le istantanee dei file.

Il valore predefinito è: C:\Program Files (x86)\TSplus-Security\snapshots

Estensioni ignorate Per impostazione predefinita, la protezione da ransomware ignora le estensioni ben note dei file temporanei per l'attività di ransomware. Vedi l'elenco qui Puoi definire nomi di estensione personalizzati nel campo valore (separati da punto e virgola):

Dimensione massima dello snapshot del file File Snapshots Max Size definisce lo spazio massimo consentito per mantenere le istantanee dei file.

La dimensione è espressa in percentuale dello spazio totale disponibile sul disco in cui risiede il percorso Snapshot.

Ritenzione dello snapshot del file La retention dei file snapshot definisce, in secondi, la politica di retention di un file snapshot.

Una volta scaduto il periodo di conservazione, la snapshot del file viene eliminata. Per impostazione predefinita, 300 secondi (cioè 5 minuti)

Ritenzione della snapshot del registro La retention dello snapshot del registro definisce, in secondi, la politica di retention di uno snapshot del registro. Una volta scaduto il periodo di retention, lo snapshot del registro viene eliminato. Per impostazione predefinita, 300 secondi (cioè 5 minuti)

Avviso di rilevamento display Visualizza una finestra di messaggio di avviso sul desktop dell'utente quando la protezione da ransomware ha rilevato e bloccato un attacco.

Script PowerShell e CMD consentiti Elenco degli script PowerShell e CMD consentiti con i percorsi completi dei file degli script PowerShell e CMD autorizzati ad essere eseguiti sulla macchina

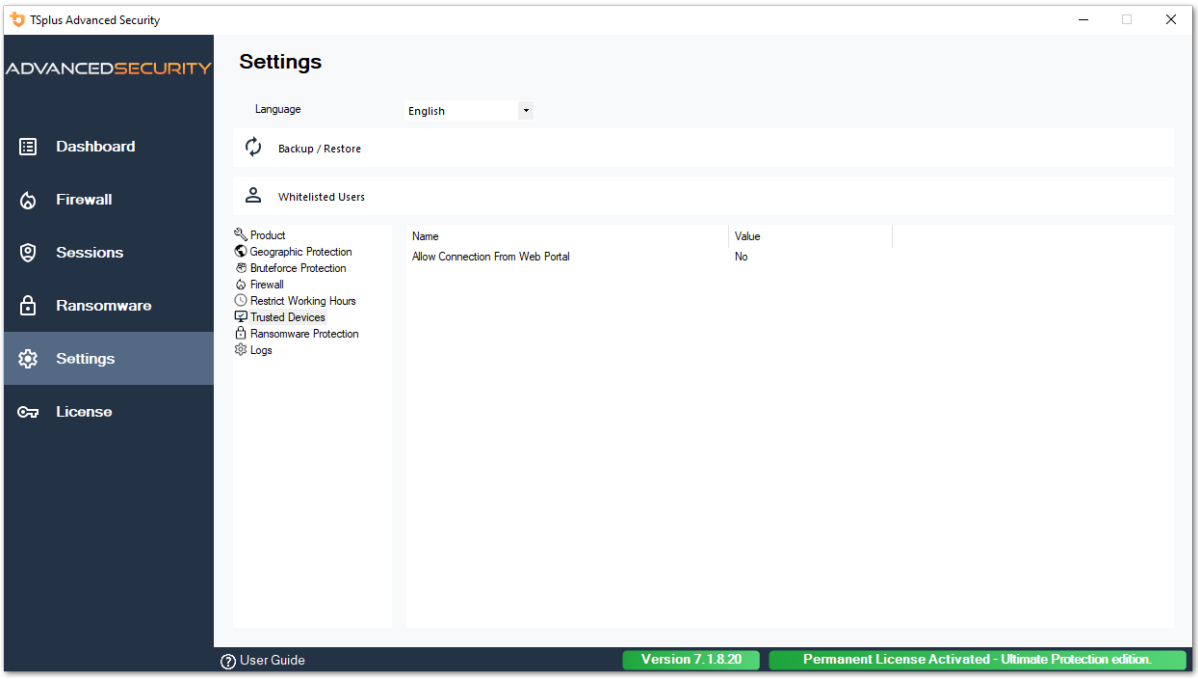
L'esecuzione di script consentiti non attiverà la protezione da Ransomware (separati da punto e virgola).

Avanzato - Dispositivi affidabili

Il **Dispositivi affidabili** la scheda consente di abilitare le connessioni dal Portale Web di TSplus Remote Access.

Nota :

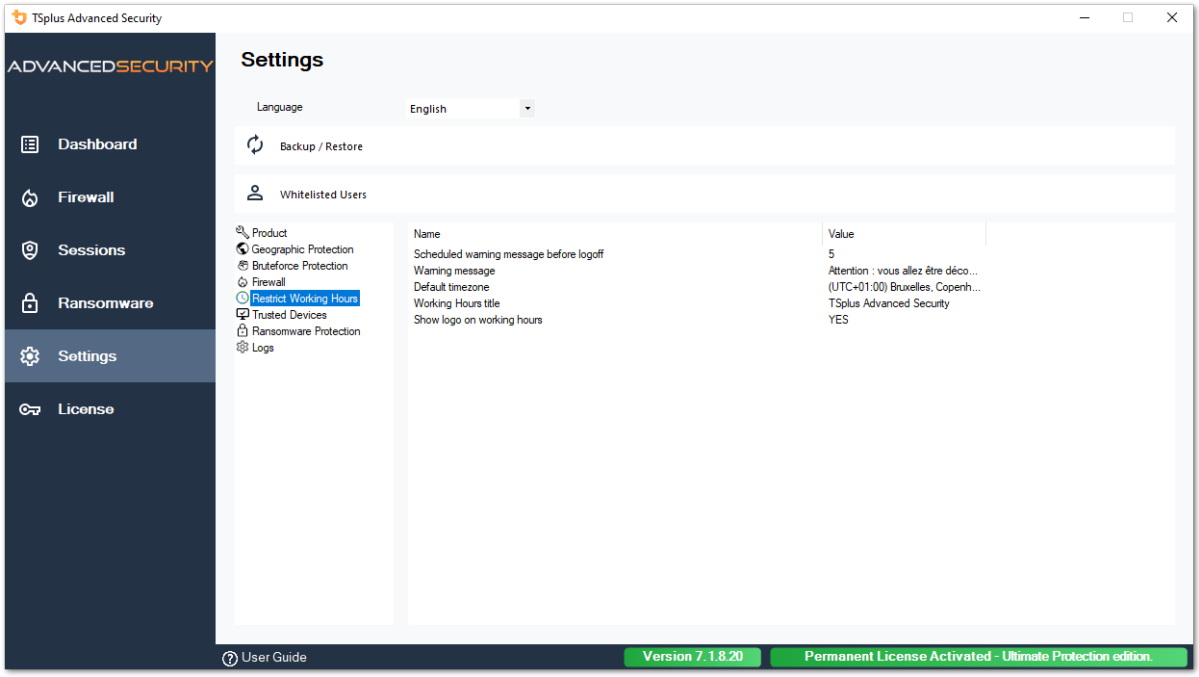
-Dispositivi fidati non è compatibile con le sessioni HTML5. -Dispositivi fidati non è compatibile con dispositivi mobili iOS / Android poiché nascondono i loro veri nomi host. -Il nome host della macchina remota è definito dalla macchina stessa. È probabile che la macchina lo nasconda o lo modifichi in base alla sua configurazione.



I dispositivi fidati di TSplus Advanced Security non possono risolvere il nome del client se la connessione è avviata dal portale Web di TSplus Remote Access. Pertanto, i dispositivi fidati bloccheranno per impostazione predefinita qualsiasi connessione dal portale Web. Imposta questa opzione su "Sì" per consentire le connessioni dal portale Web. Tieni presente che questa azione ridurrà la sicurezza del tuo server.

Avanzato - Limitare le ore lavorative

Il **Limitare l'orario di lavoro** la scheda ti consente di Pianifica un messaggio di avviso prima che l'utente venga disconnesso. .



Messaggio di avviso programma Puoi configurare il numero di minuti prima che l'utente venga disconnesso automaticamente. Per impostazione predefinita, è impostato su 5 minuti.

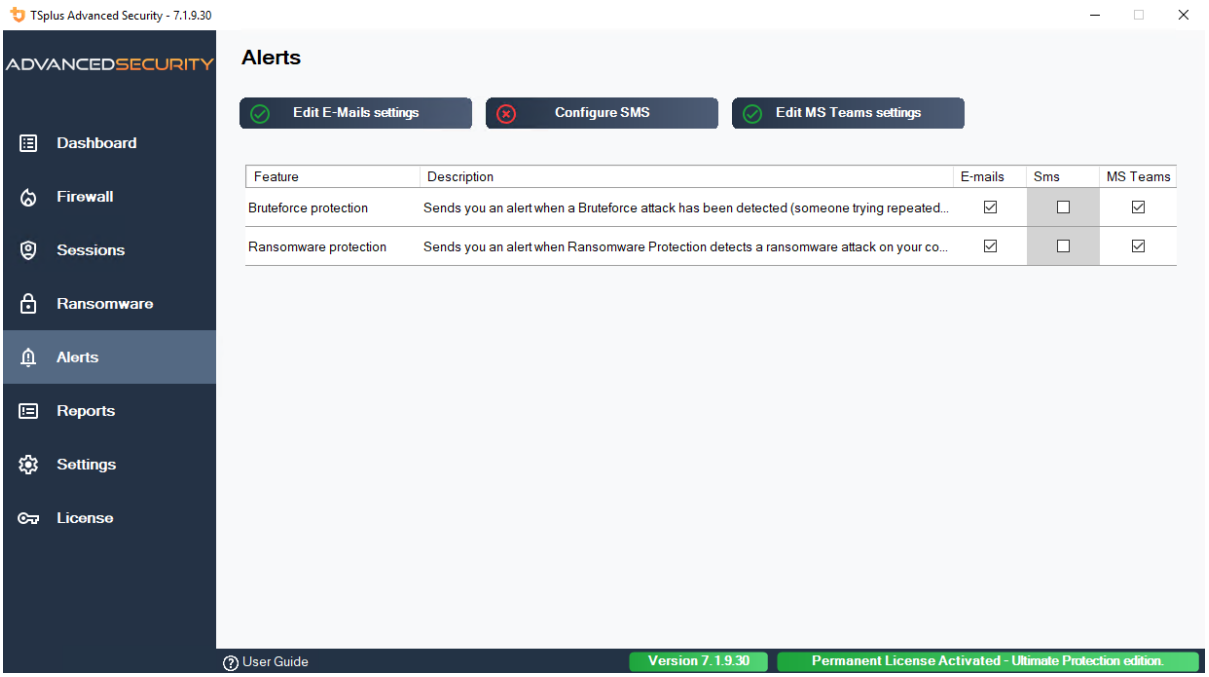
Messaggio di avviso Un messaggio di avviso può essere definito a tua discrezione, con segnaposto denominati %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% e %ENDINGHOURS%, che saranno rispettivamente sostituiti dal numero attuale di minuti prima della chiusura della sessione, dal giorno attuale, dall'orario di inizio e di fine lavorativo del giorno attuale.

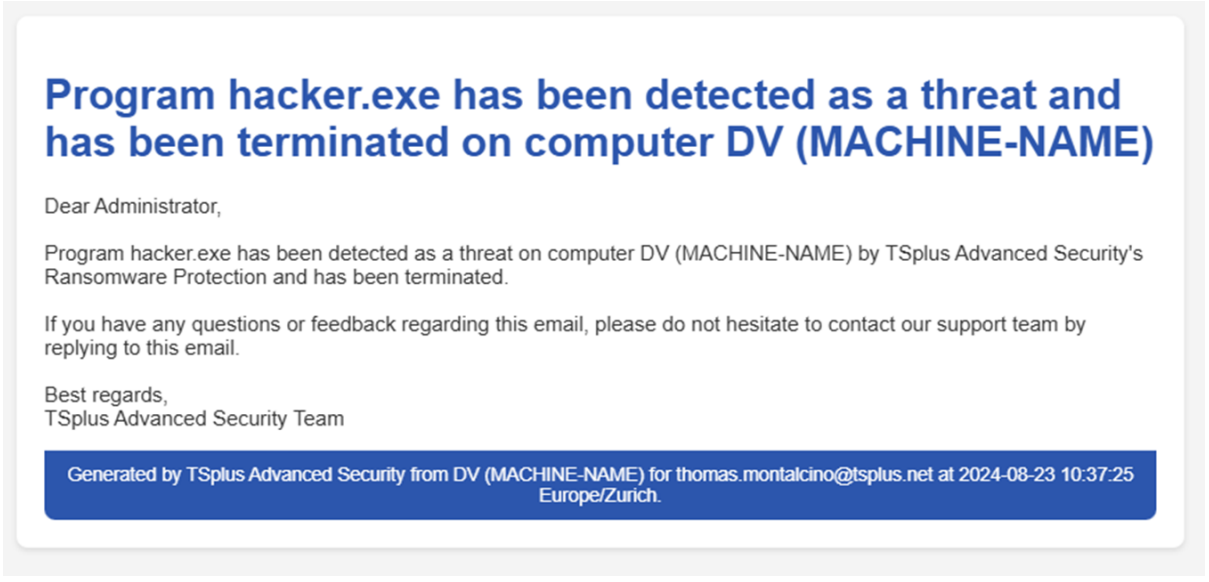
Fuso orario del server predefinito È possibile definire un fuso orario del server predefinito per applicare le regole degli orari di lavoro selezionando quello corrispondente nell'elenco a discesa.

Orari di lavoro titolo Titolo del modulo visualizzato all'utente finale, quando le sue ore lavorative stanno per finire (predefinito: TSplus Advanced Security)

Mostra logo durante l'orario lavorativo Se impostato su "sì", il logo viene mostrato nella forma visualizzata all'utente finale, quando le sue ore lavorative stanno per terminare (predefinito: "sì")

Avvisi





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.

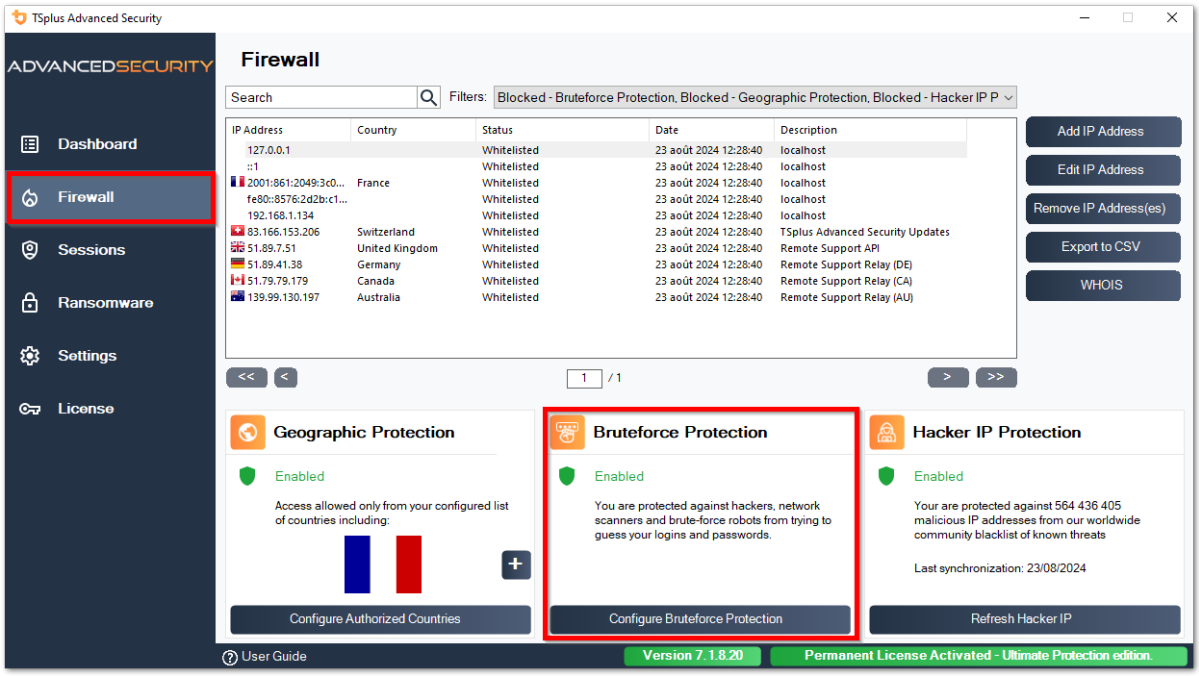
Best regards,
TSplus Advanced Security Team

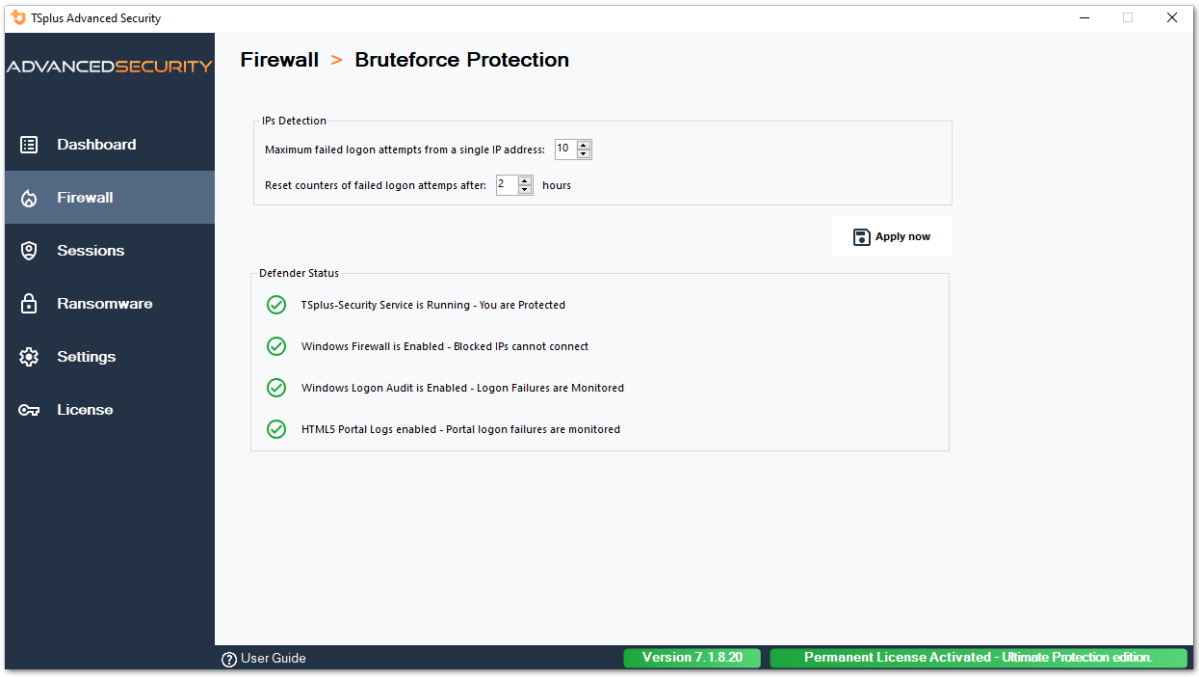
Generated by TSplus Advanced Security from DV (MACHINE-NAME) for thomas.montalcino@tsplus.net at 2024-08-23 10:37:25 Europe/Zurich.

Protezione da attacchi di forza bruta

La protezione contro il bruteforce ti consente di proteggere il tuo server pubblico da hacker, scanner di rete e robot di brute-force che cercano di indovinare il tuo login e password da amministratore. Utilizzando login attuali e dizionari di password, tenteranno automaticamente di accedere al tuo server centinaia o migliaia di volte al minuto.

Con questo RDP Defender, puoi monitorare i tentativi di accesso non riusciti di Windows e mettere automaticamente in blacklist gli indirizzi IP colpevoli dopo diversi fallimenti.





- Puoi impostare il **massimo numero di tentativi di accesso non riusciti da un singolo indirizzo IP all'interno del blocco di rilevamento degli IP** (di default, sono 10), così come il tempo di ripristino per i contatori dei tentativi di accesso non riusciti (di default sono 2 ore).

- In fondo a questa finestra, puoi vedere il **Stato del difensore** dove puoi controllare se i fallimenti di accesso al portale Web HTML5, i fallimenti di accesso a Windows sono monitorati e se il firewall di Windows e il servizio di sicurezza avanzata sono abilitati.

In questo caso, come nel nostro esempio, tutti gli stati sono selezionati.

- **Gestisci gli indirizzi IP bloccati** Puoi ovviamente configurarlo per soddisfare le tue esigenze, ad esempio aggiungendo il tuo indirizzo IP della workstation nel Whitelist IPs , quindi questo strumento non ti bloccherà mai. Puoi aggiungere quanti più indirizzi IP desideri nella whitelist. Questi indirizzi non saranno mai bloccati dalla protezione contro il bruteforce.

- Puoi **ignora indirizzi IP locali e privati** cambiando l'impostazione predefinita su Impostazioni > Avanzate > Scheda Bruteforce

Nota: Se noti mai che la Bruteforce Protection ha bloccato 10 indirizzi IP al giorno e che ora non è più così; e blocca uno, due o addirittura non blocca alcun indirizzo, è effettivamente normale. Infatti, prima dell'installazione di advanced-security, il server con una porta RDP pubblicamente disponibile è conosciuto da tutti i robot, e molti robot provano le password attuali e quelle provenienti dai dizionari. Quando installi advanced-security, questi robot vengono

progressivamente bloccati, in modo che un giorno:

- La maggior parte dei robot attivi è già bloccata e non è interessata al server, nemmeno i nuovi.
- Inoltre, il server non appare più nella lista dei server pubblicamente conosciuti.

Linee di comando

Siamo lieti di fornirti un insieme completo di strumenti da riga di comando progettati per migliorare la flessibilità e l'efficienza del nostro software. Questi strumenti consentono agli utenti di scrivere script e automatizzare varie funzionalità, personalizzando il software per soddisfare le loro esigenze e flussi di lavoro specifici.

Esplora le possibilità e ottimizza la tua esperienza con le nostre opzioni da riga di comando.

Devi solo eseguire le seguenti righe di comando come Amministratore elevato. Ricorda che TSplus-Security.exe si trova nella seguente cartella **C:\Program Files (x86)\TSplus-Security** per impostazione predefinita.

Gestione delle licenze

Per eseguire operazioni sulle licenze, si prega di sostituire il programma AdminTool.exe presentato nella seguente documentazione con il programma TSplus-Security.exe situato nella directory di installazione di Advanced Security (di solito **C:\Program Files (x86)\TSplus-Security**).

- Attivazione della licenza
- Ripristino della licenza a seguito della clonazione di una VM
- Attivazione della licenza volume
- Abilitare e disabilitare la licenza Volume
- Aggiornamento della licenza volume
- Visualizza i crediti di licenza rimanenti per una chiave di licenza volume
- Visualizza i crediti di supporto rimanenti per una chiave di licenza volume

---

Configura server proxy: /proxy /set

Sintassi:

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

Descrizione:

Comando /proxy /set viene utilizzato per configurare un server proxy per l'accesso a Internet.

Parametri:

- /host il host di destinazione può essere un valore predefinito (“ie” o “none”) o un valore definito dall'utente (ad es.: 127.0.0.1 o proxy.company.org). Questo parametro è obbligatorio
- /port il numero di porta utilizzato per connettersi al server proxy. Richiesto se il valore del nome host è un valore personalizzato definito dall'utente.
- /username il nome utente per connettersi al server proxy. Questa impostazione è facoltativa
- /password la password dell'utente deve essere fornita se è stato definito un nome utente. Tuttavia, il suo valore può essere vuoto

Esempi:

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

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

Per ulteriori informazioni, si prega di andare a Come configurare un server proxy per l'accesso a Internet?

Backup dei dati e delle impostazioni: /backup

Sintassi:

TSplus-Security.exe /backup [PercorsoDirectoryDestinazione]

Descrizione:

Comando /backup viene utilizzato per eseguire il backup dei dati e delle impostazioni di TSplus Advanced Security.

Per impostazione predefinita, il backup verrà creato nella directory degli archivi situata nella directory di configurazione di Advanced Security (ad es.: C:\Program Files (x86)\TSplus-

Security\archives).

Parametri:

- DestinationDirectoryPath per eseguire il backup in un'altra directory diversa da quella predefinita. Sono consentiti percorsi relativi e assoluti.

Esempi:

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

Per ulteriori informazioni, si prega di andare a Avanzato - Backup e Ripristino

---

Ripristina dati e impostazioni: /restore

Sintassi:

TSplus-Security.exe /restore [Percorso della directory di backup]

Descrizione:

Comando /restore viene utilizzato per ripristinare i dati e le impostazioni di TSplus Advanced Security.

Il percorso della directory di backup specificato deve essere creato dal comando /backup o dalla funzione di backup dell'applicazione.

Parametri:

- Backup Directory Path il percorso in cui si trova la directory di backup da ripristinare.

Esempi:

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

Per ulteriori informazioni, si prega di andare a Avanzato - Backup e Ripristino

---

Rimuovi e sblocca tutti gli indirizzi IP bloccati: /unblockall

Sintassi:

TSplus-Security.exe /unblockall

Descrizione:

Comando /unblockall viene utilizzato per rimuovere tutti gli indirizzi IP bloccati dal firewall di TSplus Advanced Security e sbloccarli dal firewall di Microsoft Windows Defender, se necessario.

Esempi:

TSplus-Security.exe /unblockall

Per ulteriori informazioni, si prega di andare a Firewall

Rimuovi e sblocca gli indirizzi IP specificati: /unblockips

Sintassi:

TSplus-Security.exe /unblockips [indirizzi IP]

Descrizione:

Comando /unblockips viene utilizzato per rimuovere tutti gli indirizzi IP bloccati specificati dal firewall di TSplus Advanced Security e sbloccarli dal firewall di Microsoft Windows Defender se necessario.

Questo comando non ha effetto sugli indirizzi IP già bloccati dalla protezione IP di Hacker. Se desideri ancora sbloccare uno di questi indirizzi, ti preghiamo di utilizzare il comando whitelist.

Parametri:

- IP addresses la lista degli indirizzi IP o delle gamme di IP da sbloccare (separati da virgola o punto e virgola).

Esempi:

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

Per ulteriori informazioni, si prega di andare a Firewall

Blocca gli indirizzi IP specificati: /blockips

Sintassi:

TSplus-Security.exe /blockips [indirizzi IP] [Descrizione opzionale]

Descrizione:

Comando /blockips viene utilizzato per bloccare tutti gli indirizzi IP specificati utilizzando il firewall di TSplus Advanced Security e bloccarli utilizzando il firewall di Microsoft Windows Defender se configurato.

Parametri:

- IP addresses la lista degli indirizzi IP o degli intervalli IP da bloccare (separati da virgola o punto e virgola).
- Optional Description una descrizione facoltativa che sarà aggiunta per ogni voce.

Esempi:

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Luoghi di lavoro di John”

Per ulteriori informazioni, si prega di andare a Firewall

Aggiungi indirizzi IP alla whitelist: /addwhitelistedip

Sintassi:

TSplus-Security.exe /addwhitelistedip [indirizzi IP] [Descrizione opzionale]

Descrizione:

Comando /addwhitelistedip viene utilizzato per aggiungere indirizzi IP specificati agli indirizzi IP autorizzati del firewall di TSplus Advanced Security e sbloccarli dal firewall di Microsoft Windows Defender se necessario.

Parametri:

- IP addresses la lista degli indirizzi IP o degli intervalli di IP da inserire nella whitelist (separati da virgola o punto e virgola).
- Optional Description una descrizione facoltativa che sarà aggiunta per ogni voce.

Esempi:

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Luoghi di lavoro di John”

Per ulteriori informazioni, si prega di andare a Firewall

Aggiungi un programma o una directory all'elenco autorizzato per la protezione da ransomware: /whitelist

Sintassi:

TSplus-Security.exe /whitelist add [Percorsi autorizzati]

Descrizione:

Comando /whitelist add viene utilizzato per aggiungere percorsi di programma e percorsi di directory specificati all'elenco autorizzato della Protezione da Ransomware di TSplus Advanced Security.

Parametri:

- Authorized Paths la lista dei percorsi di programma e dei percorsi di directory da aggiungere all'elenco di autorizzazione per la protezione da ransomware di TSplus Advanced Security (separati da punto e virgola).

Esempi:

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

Per ulteriori informazioni, si prega di andare a Azione di protezione da ransomware

---

Aggiorna la protezione IP degli hacker: / refreshipprotection

Sintassi:

TSplus-Security.exe /refreshipprotection

Descrizione:

Comando /refreshipprotection viene utilizzato per aggiornare l'elenco degli intervalli IP bloccati per la funzione di protezione IP contro gli hacker. È necessaria un'abbonamento ai servizi di supporto e aggiornamenti.

Esempi:

TSplus-Security.exe /refreshipprotection

Per ulteriori informazioni, si prega di andare a Protezione IP degli hacker

---

Imposta il livello di registrazione: /setloglevel

Sintassi:

TSplus-Security.exe /setloglevel [Livello di Log]

Descrizione:

Comando /setloglevel viene utilizzato per impostare il livello di registrazione per tutti i componenti di Advanced Security.

Parametri:

- Log Level il livello di registrazione tra i seguenti valori: TUTTO, DEBUG, INFO, AVVISO, ERRORE, FATALE, SPENTO

Esempi:

TSplus-Security.exe /setloglevel TUTTI

Per ulteriori informazioni, si prega di andare a Avanzato > Registri

---

Aggiungi dispositivi fidati: /addtrusteddevices

Sintassi:

TSplus-Security.exe /addtrusteddevices [Configurazione Dispositivi Affidabili]

Descrizione:

Comando /addtrusteddevices è utilizzato per aggiungere dispositivi fidati in modo programmatico. Richiede l'edizione Ultimate.

Parametri:

- Trusted Devices Configuration L'argomento è composto da un elenco di dispositivi fidati (separati da punto e virgola), strutturato come segue:

Nome utente e dispositivi sono separati dal carattere due punti (:).

Dettagli dell'utente:

Tipo utente e nome utente completo sono separati dal carattere due punti (:). I tipi di utente accettati sono "utente" e "gruppo".

Parola chiave opzionale "disabilitato": se inclusa, i dispositivi fidati verranno creati, ma le restrizioni saranno disabilitate per questo utente. Se non menzionato, le restrizioni sono abilitate per impostazione predefinita.

Dettagli del dispositivo:

Nome dispositivo e commento facoltativo: separati dal carattere uguale (=).

I dispositivi sono separati dal carattere due punti (:).

Esempi:

TSplus-Security.exe /addtrusteddevices “user:WIN-A1BCDE23FGH\admin:disabilitato,device1name=questo è un commento per il dispositivo 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name=device4name=un altro commento;group:DESKTOP-A1BCDE23FGH\Administrators:disabilitato,device5name”

Per ulteriori informazioni, si prega di andare a Dispositivi affidabili

---

Abilita i dispositivi fidati configurati: / enabletrusteddevices

Sintassi:

TSplus-Security.exe /enabletrusteddevices [Utente o Gruppi]

Descrizione:

Comando /enabletrusteddevices viene utilizzato per abilitare tutti i dispositivi fidati configurati per gli utenti e i gruppi specificati.

Parametri:

- User or Groups L'argomento è un elenco di utenti e gruppi (separati da punto e virgola). All'interno del nome utente, la separazione tra il tipo di utente ("utente" e "gruppo" sono i soli valori accettati) e il nome utente completo avviene tramite due punti.

Esempi:

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

Per ulteriori informazioni, si prega di andare a Dispositivi affidabili

---

Disabilita tutti i dispositivi fidati: / disabletrusteddevices

Sintassi:

TSplus-Security.exe /disabletrusteddevices [Utente o Gruppi]

Descrizione:

Comando /disabletrusteddevices viene utilizzato per disabilitare tutti i dispositivi fidati configurati per gli utenti e i gruppi specificati.

Parametri:

- User or Groups L'argomento è un elenco di utenti e gruppi (separati da punto e virgola). All'interno del nome utente, la separazione tra il tipo di utente ("utente" e "gruppo" sono i soli

valori accettati) e il nome utente completo avviene tramite due punti.

Esempi:

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

Per ulteriori informazioni, si prega di andare a Dispositivi affidabili

---

Imposta il driver di protezione da ransomware: /setup-driver

Sintassi:

TSplus-Security.exe /setup-driver

Descrizione:

Comando /setup-driver installa il driver di protezione da ransomware. Questa operazione viene normalmente eseguita durante l'installazione.

Esempi:

TSplus-Security.exe /setup-driver

Per ulteriori informazioni, si prega di andare a Protezione da Ransomware

---

Disinstallare il driver di protezione da ransomware: /uninstalldriver

Sintassi:

TSplus-Security.exe /disinstalla driver

Descrizione:

Comando /uninstalldriver disinstallare il driver di protezione da ransomware. Questa operazione viene normalmente eseguita durante la disinstallazione di Advanced Security.

Esempi:

TSplus-Security.exe /disinstalla driver

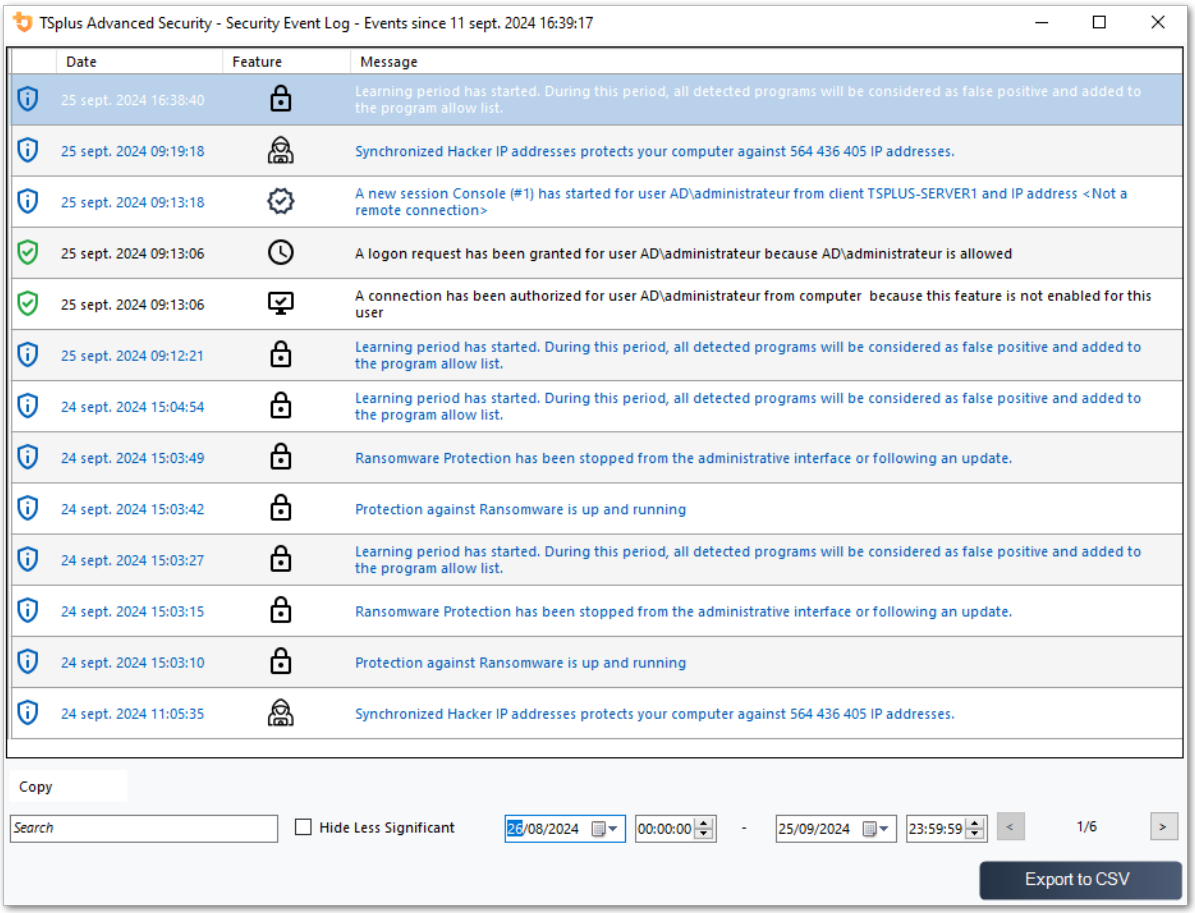
Per ulteriori informazioni, si prega di andare a Protezione da Ransomware

Eventi

Gli eventi di sicurezza sono una grande fonte di informazioni poiché mostrano le operazioni eseguite da TSplus Advanced Security per proteggere il tuo computer.

La finestra Eventi può essere aperta dalla finestra principale di TSplus Advanced Security, facendo clic direttamente sugli ultimi 5 eventi visualizzati o sulla scheda dashboard. Le informazioni visualizzate nella finestra Eventi vengono aggiornate automaticamente ogni pochi secondi.

La lista degli eventi di sicurezza presenta 4 colonne, che descrivono la gravità, la data del controllo o dell'operazione eseguita, l'icona della funzionalità associata e la descrizione.



La descrizione dell'evento spiega spesso perché l'azione è stata eseguita o meno. Le azioni

ritorsive sono spesso scritte in rosso e evidenziate con un'icona a scudo rosso.

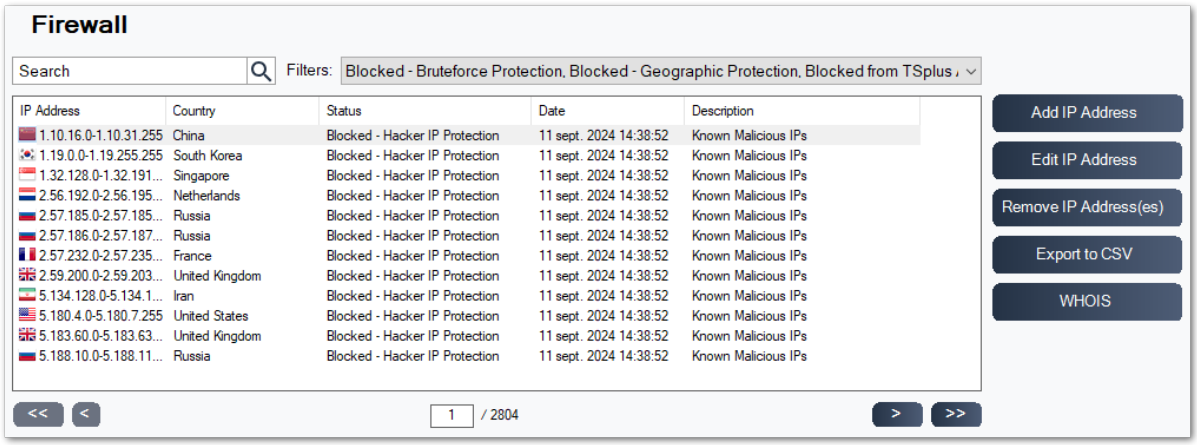
La finestra degli eventi può essere spostata e non impedisce di utilizzare le altre funzionalità di TSplus Advanced Security.

Navigare e cercare tra gli eventi

- Una ricerca globale approfondita è ora disponibile per trovare rapidamente eventi specifici.
- Accanto alla ricerca globale, 2 filtri di selezione di data e ora mostrano gli eventi in base alla data in cui è stato sollevato l'evento.
- A destra, le frecce consentono di cambiare pagina e navigare per visualizzare eventi precedenti.

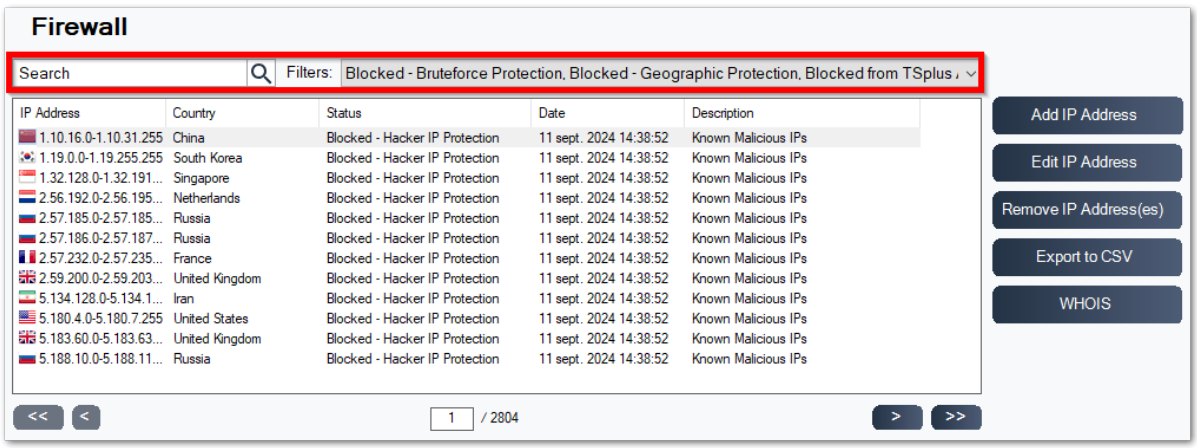
Firewall

La gestione degli indirizzi IP è facile con un'unica lista per gestire sia gli indirizzi IP bloccati che quelli autorizzati:



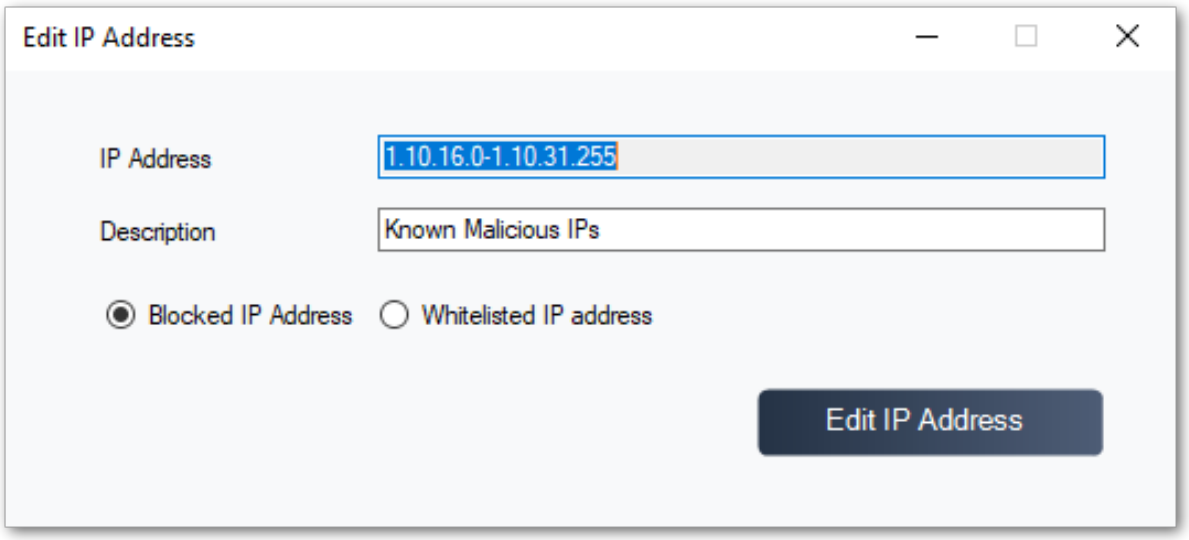
Per impostazione predefinita, gli indirizzi IPV4, IPV6 e tutti gli indirizzi localhost del server sono autorizzati.

Una comoda barra di ricerca e un filtro offrono capacità di ricerca basate su tutte le informazioni fornite.



Inoltre, gli amministratori possono eseguire azioni su più indirizzi IP selezionati con un solo clic.

Tra le nuove funzionalità introdotte nella gestione degli indirizzi IP, troverai la possibilità di fornire descrizioni significative a qualsiasi indirizzo IP.



Ultimo ma non meno importante, gli amministratori possono ora sbloccare e aggiungere a whitelists più indirizzi IP bloccati in un'unica azione, facendo clic sulla scheda "Aggiungi esistente a Whitelist".

Utilizzare la riga di comando per inserire nella whitelist o bloccare indirizzi IP e/o intervalli di IP

- Per poter **whitelist** Indirizzi IP o intervallo(i) di IP, il comando ha questa sintassi :

TSplus-Security.exe aggiungiipwhitelisted [indirizzi IP] [descrizione opzionale]

Puoi inserire nella lista bianca diversi indirizzi IP, con un **virgola o delimitatore punto e virgola** Inoltre, puoi specificare intervalli di indirizzi IP, invece di semplici indirizzi IP. La sintassi è: **x.x.x.x-y.y.y.y** Infine, puoi indicare una descrizione facoltativa della regola della whitelist.

Ecco un esempio di 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 “Luoghi di lavoro di John”

- Per poter **blocco** Indirizzi IP o intervallo(i) di IP, il comando ha una sintassi simile:

TSplus-Security.exe blocca IP [indirizzi IP] [descrizione opzionale]

- Per poter **sbloccare** Indirizzi IP o intervallo(i) di IP, il comando ha una sintassi simile:

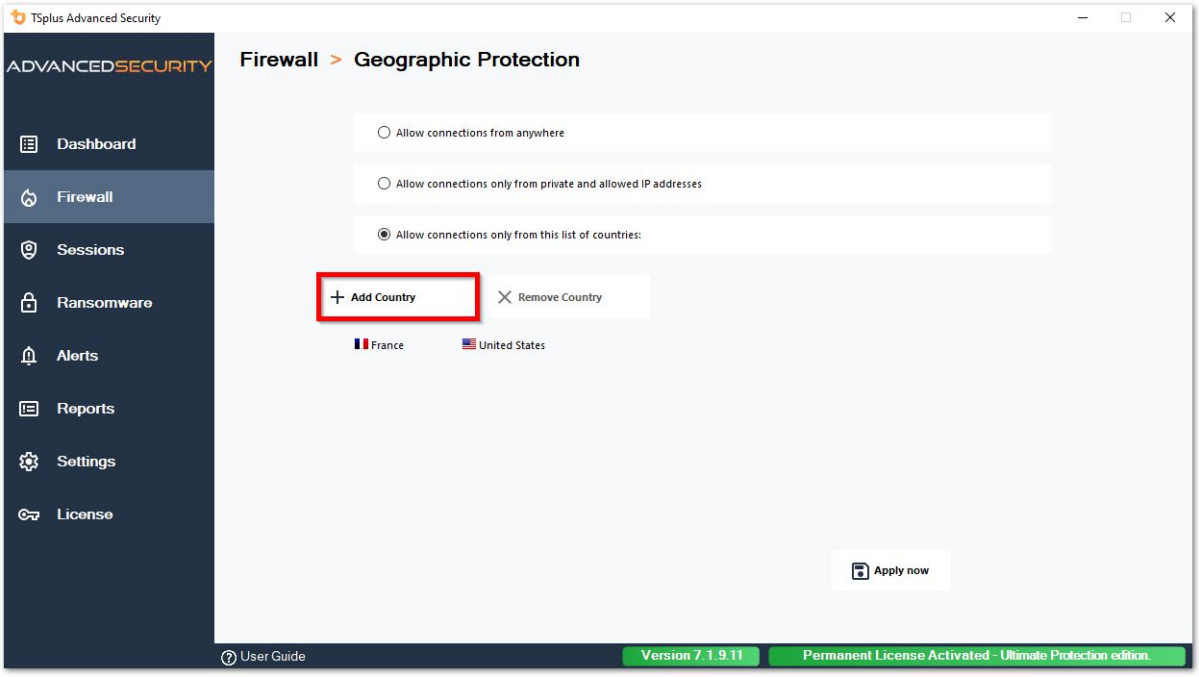
TSplus-Security.exe sbloccaip [indirizzi IP]

Questo comando non ha effetto sugli indirizzi IP già bloccati dalla protezione IP di Hacker. Se desideri ancora sbloccare uno di questi indirizzi, ti preghiamo di utilizzare il comando whitelist.

Protezione geografica

Limita l'accesso da altri paesi

Per consentire l'accesso remoto solo da paesi specifici, selezionare il pulsante "Consenti connessioni solo da questo elenco di paesi" e poi fare clic sul pulsante "Aggiungi paese".

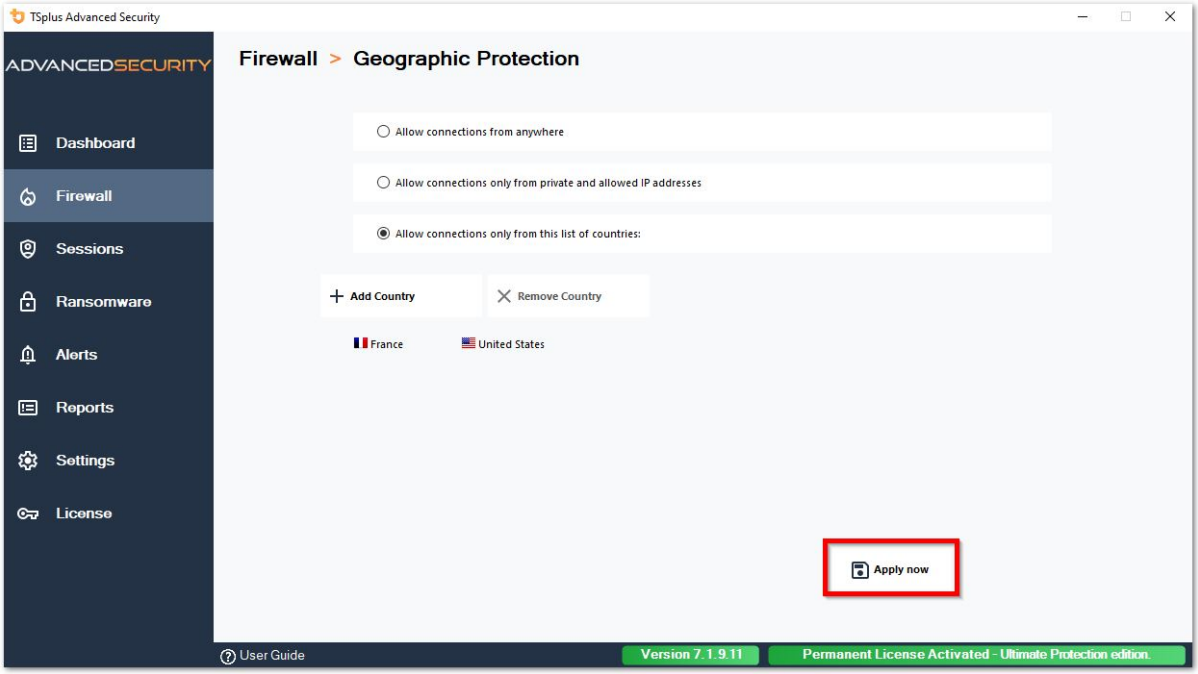


Si apre un popup che offre un elenco di paesi. Seleziona il paese che desideri aggiungere all'elenco.

Puoi scegliere di selezionare la casella qui sotto per sbloccare tutti gli indirizzi IP precedentemente bloccati per il paese selezionato.

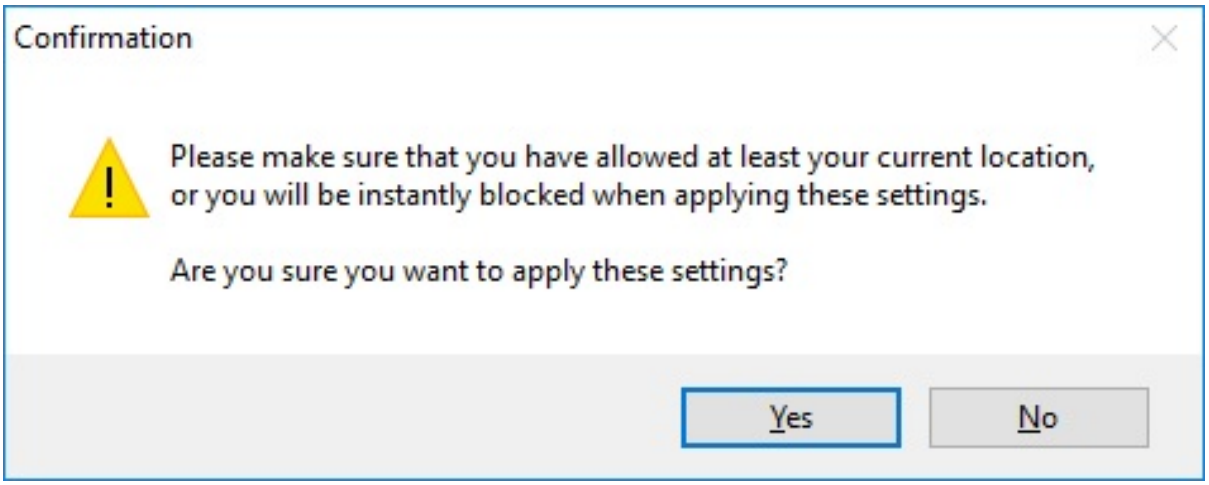
Clicca sul pulsante "Aggiungi Paese" per tornare alla schermata principale della funzionalità.

Importante: Per salvare le modifiche, fare clic sul pulsante “Applica”.



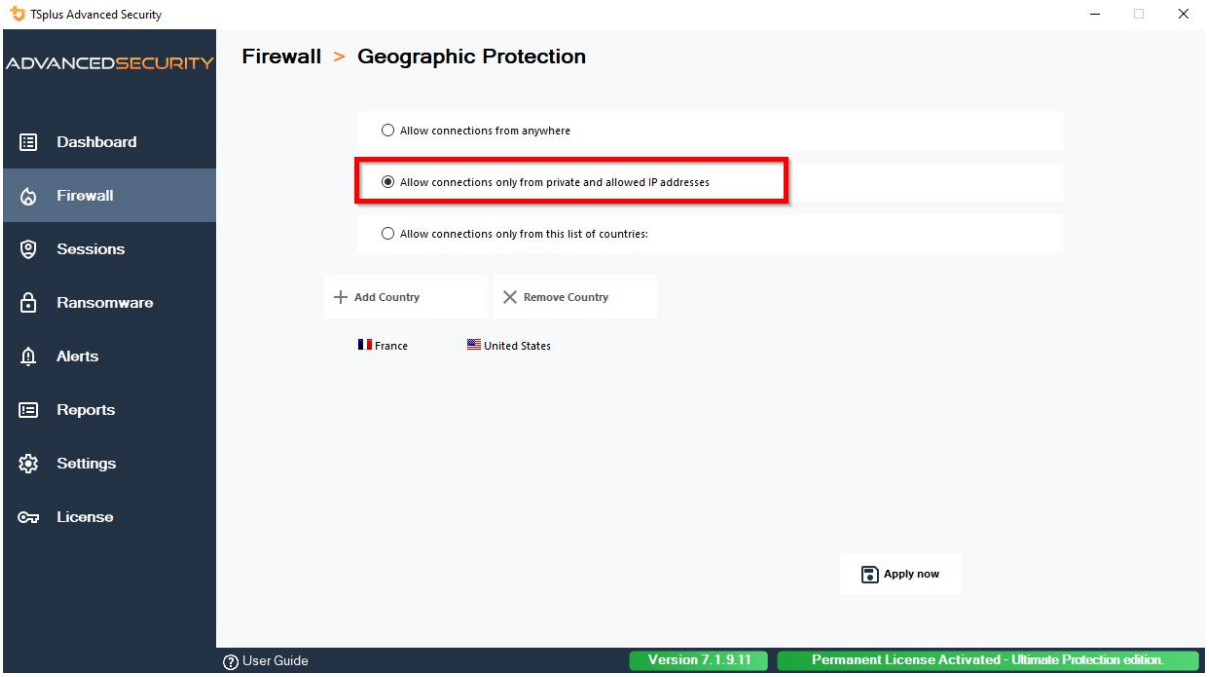
In questo esempio, l'accesso remoto è consentito per gli utenti che si connettono dagli Stati Uniti e dalla Francia.

Un messaggio di conferma appare per evitare di bloccare l'utente connesso. Clicca su "Sì" per confermare e applicare le modifiche.



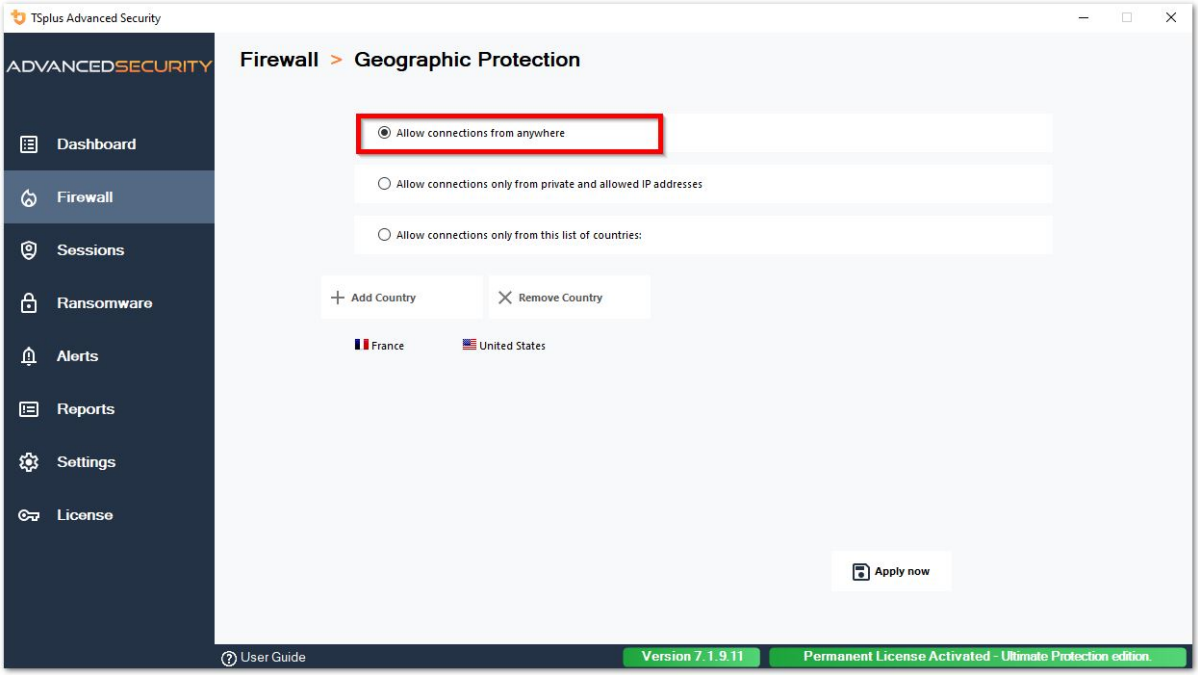
Limita l'accesso da Internet

La protezione geografica può essere configurata per limitare l'accesso al tuo computer solo a indirizzi privati e indirizzi IP autorizzati , come mostrato di seguito:



Disabilita la protezione geografica

Per impostazione predefinita, la Protezione Geografica consente l'accesso agli utenti che si connettono da tutto il mondo:



Sblocco degli indirizzi IP bloccati

Quando un indirizzo IP viene bloccato, appare su di esso Scheda Firewall Gli indirizzi IP bloccati possono quindi essere sbloccati e eventualmente aggiunti all'elenco degli indirizzi IP consentiti.

Se vieni bloccato, ti consigliamo di provare a connetterti da qualsiasi paese che hai autorizzato su TSplus Advanced Security, ad esempio collegandoti da un altro server remoto o utilizzando un servizio VPN. Puoi anche utilizzare una sessione console per connetterti, poiché questa sessione non è una sessione remota e non sarà bloccata da TSplus Advanced Security.

Importante:

- Controlla di aver selezionato il paese da cui sei attualmente connesso. In caso contrario, il tuo indirizzo IP verrà bloccato rapidamente dopo aver applicato le impostazioni, disconnettendoti senza alcuna possibilità di riconnetterti dallo stesso indirizzo IP.

- Considera di aggiungere il tuo indirizzo IP alla lista degli autorizzati. Indirizzi IP per evitare di essere bloccati da Protezione Geografica o Protezione da attacchi di forza bruta caratteristiche.

Comprendere la Protezione Geografica

La protezione geografica controlla le connessioni di rete TCP in entrata, sia IPv4 che IPV6

(eccetto quando è configurata la modalità API di Windows legacy).

Processi: La Protezione Geografica ascolta le connessioni inviate al server Web di TSplus Remote Access per impostazione predefinita, se installato. Il nome del processo corrispondente è HTML5 Service. Se desideri disabilitare il suo monitoraggio o controllare le connessioni destinate ad altri processi, vai a Impostazioni > Avanzate > Protezione geografica .

Porte di rete: per impostazione predefinita, Geographic Protection ascolta le porte predefinite utilizzate per connettersi da remoto a un server. Queste porte includono RDP (3389), Telnet (23) e VNC. Geographic Protection supporta i seguenti fornitori di VNC: Tight VNC, Ultra VNC, Tiger VNC e Real VNC, che non sono in alcun modo correlati a TSplus. Se desideri disabilitare il suo monitoraggio o controllare le connessioni destinate ad altre porte, vai a Impostazioni > Avanzate > Protezione geografica .

Meccanismi di rilevamento:

La Protezione Geografica rileva le connessioni in entrata da paesi non autorizzati utilizzando tre diversi meccanismi di rilevamento:

- API di Windows
- Tracciamento eventi per Windows
- Firewall integrato

Da un lato, l'Event Tracing for Windows è una struttura di tracciamento a livello di kernel efficiente che cattura eventi di rete in tempo reale. L'Event Tracing for Windows è consigliato con il firewall di Windows abilitato (predefinito).

D'altra parte, l'API di Windows funziona bene data qualsiasi configurazione di rete specifica, ma potrebbe esercitare una pressione costante sulla CPU a seconda del numero di connessioni attive. Si prega di notare che l'API di Windows non è ancora compatibile con IPv6.

Il Firewall integrato consente la cattura e il blocco dei pacchetti di rete inviati allo stack di rete di Windows in modalità utente. Quando il Firewall integrato è configurato per bloccare le connessioni indesiderate, si consiglia di utilizzarlo per applicare i paesi consentiti dalla Protezione Geografica.

Geolocalizzazione: Advanced Security include dati di geolocalizzazione pubblicati da MaxMind, disponibili da http://www.maxmind.com Se trovi un indirizzo IP non registrato nel suo paese attuale, contatta direttamente MaxMind per risolvere il problema.

Risoluzione dei problemi

Se noti mai che la Protezione Geografica non blocca le connessioni provenienti da un paese che in realtà non è nella lista dei paesi autorizzati, è certamente perché:

Antivirus: Per bloccare un indirizzo IP, la Protezione Geografica aggiunge una regola di blocco

sul firewall di Windows. Quindi, innanzitutto, il firewall deve essere attivo. Devi anche controllare se alcuni parametri del firewall non sono gestiti da un altro programma, come un antivirus. In questo caso, dovrai disattivare questo programma e riavviare il servizio "Windows Firewall". Puoi anche contattare l'editore del tuo programma di terze parti e chiedere loro di trovare un modo affinché il loro programma rispetti le regole quando viene aggiunto al firewall di Windows. Se conosci un contatto tecnico di un editore di software, siamo pronti a sviluppare questi "connettori" per il firewall. Contattaci .

VPN: Nel caso in cui il client remoto utilizzi una VPN, la Protezione Geografica otterrà un indirizzo IP scelto dal fornitore della VPN. Come sapete, i fornitori di VPN utilizzano relay in tutto il mondo per consentire ai propri utenti di navigare in modo anonimo. Alcuni fornitori di VPN consentono agli utenti di definire il paese del relay. Pertanto, gli utenti con fornitori di VPN possono essere instradati attraverso un paese non autorizzato. Ad esempio, se un fornitore di VPN sceglie un IP dallo Sri Lanka, questo paese deve essere autorizzato dalla Protezione Geografica. Inoltre, se la VPN utilizza un indirizzo IP aziendale interno, allora la protezione diventa irrilevante.

Firewall / Proxy: Lo scopo di un firewall hardware è filtrare le connessioni in entrata e in uscita per le grandi aziende. Poiché è solo un filtro, non dovrebbe modificare l'indirizzo IP di origine e quindi non dovrebbe influenzare la Protezione Geografica. Tuttavia, un proxy cambierebbe definitivamente l'indirizzo IP di origine per utilizzare un indirizzo di rete privata, che sarà sempre consentito dalla Protezione Geografica. Lo scopo principale di questa funzionalità è bloccare l'accesso a un server aperto a Internet. Se tutte le connessioni provengono dalla rete aziendale, allora la protezione diventa irrilevante.

Protezione IP degli hacker

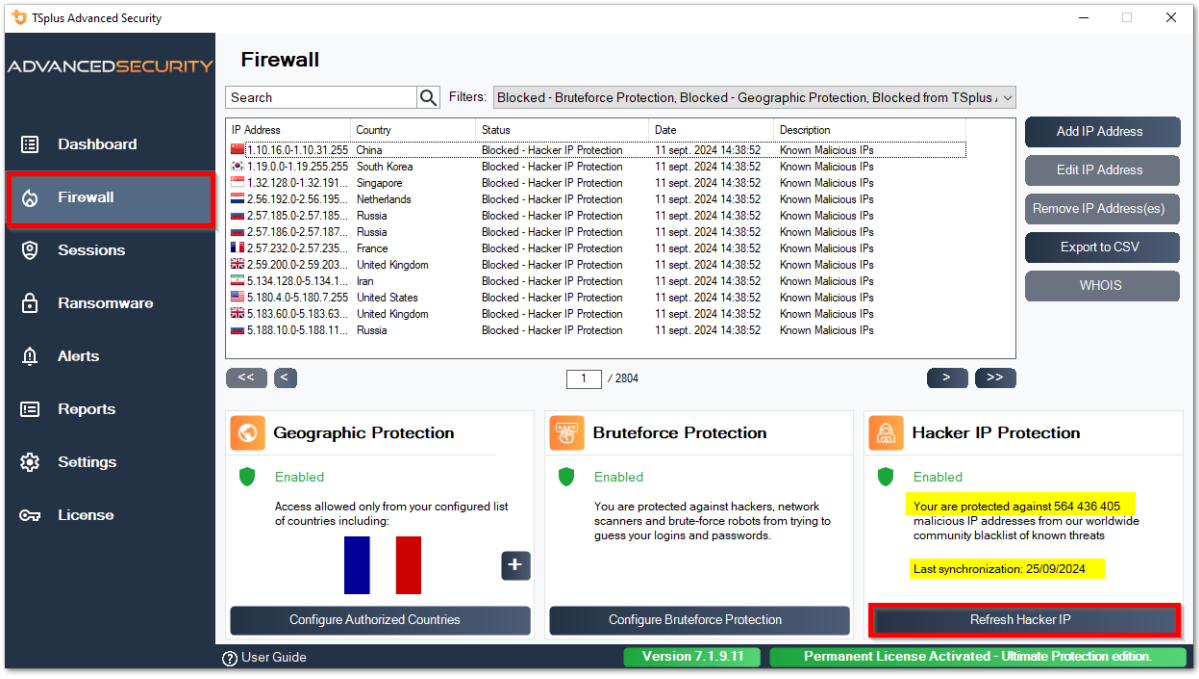
Mantieni la tua macchina protetta contro minacce conosciute come attacchi online, abuso di servizi online, malware, botnet e altre attività di cybercriminalità con la Protezione IP Hacker. L'obiettivo è creare una blacklist che possa essere sufficientemente sicura da essere utilizzata su tutti i sistemi, con un firewall, per bloccare completamente l'accesso, da e verso i suoi IP elencati.

È necessaria un'abbonamento ai servizi di supporto e aggiornamenti.

La condizione fondamentale per questa causa è non avere falsi positivi. Tutti gli IP elencati devono essere dannosi e devono essere bloccati, senza eccezioni. Per raggiungere questo obiettivo, Hacker IP Protection sfrutta le informazioni fornite dalla comunità degli utenti di Advanced Security.

La protezione degli IP degli hacker viene aggiornata automaticamente ogni giorno.

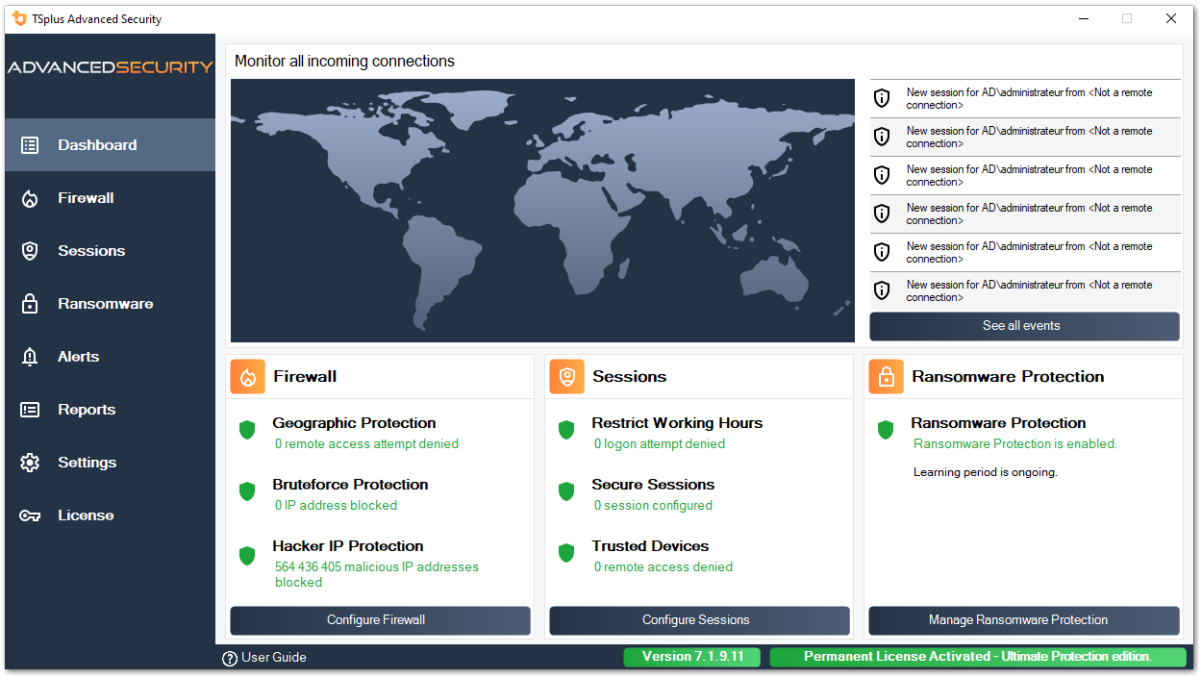
Puoi aggiornare manualmente dalla scheda “Indirizzi IP bloccati”, facendo clic sul pulsante “Aggiorna IP hacker”:



Di conseguenza, la funzione dovrebbe creare circa 600 000 000 regole di firewall di blocco in Windows Firewall.

Cruscotto

Clicca su ogni riquadro per saperne di più su ciascuna funzionalità



La barra dei menu a sinistra fornisce accesso alle diverse funzionalità. Ogni riquadro ti dà accesso alle varie funzionalità e impostazioni offerte da TSplus Advanced Security.

Advanced Security visualizza gli ultimi sei Eventi di Sicurezza Clicca su qualsiasi evento per aprire l'elenco completo degli eventi in una finestra separata.

Sotto gli ultimi eventi, tre riquadri offrono accesso rapido a:

1. Firewall
2. Sessioni
3. Protezione da Ransomware

Seleziona la tua lingua di visualizzazione utilizzando il menu a discesa situato nell'angolo in alto a destra, nel caso in cui l'applicazione non abbia rilevato la tua lingua.

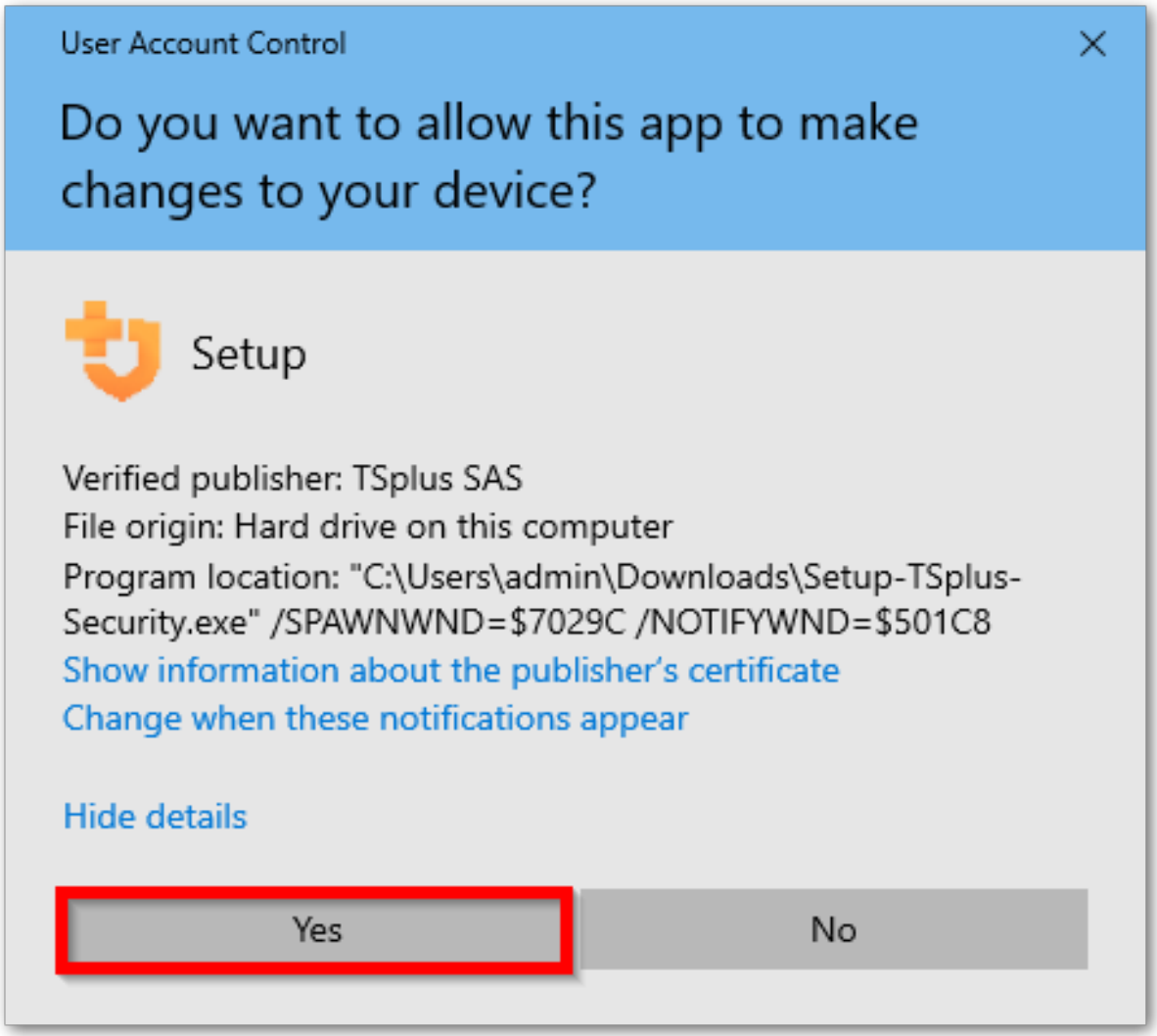
Infine, cliccando sul pulsante "Aiuto" verrai reindirizzato a questa documentazione.

Installazione di TSplus Advanced Security

Installazione di Advanced Security

Esegui TSplus Advanced Security Setup program e poi **segui i passaggi di installazione** .

Devi eseguire il programma di installazione come Amministratore e accettare il contratto di licenza del software.



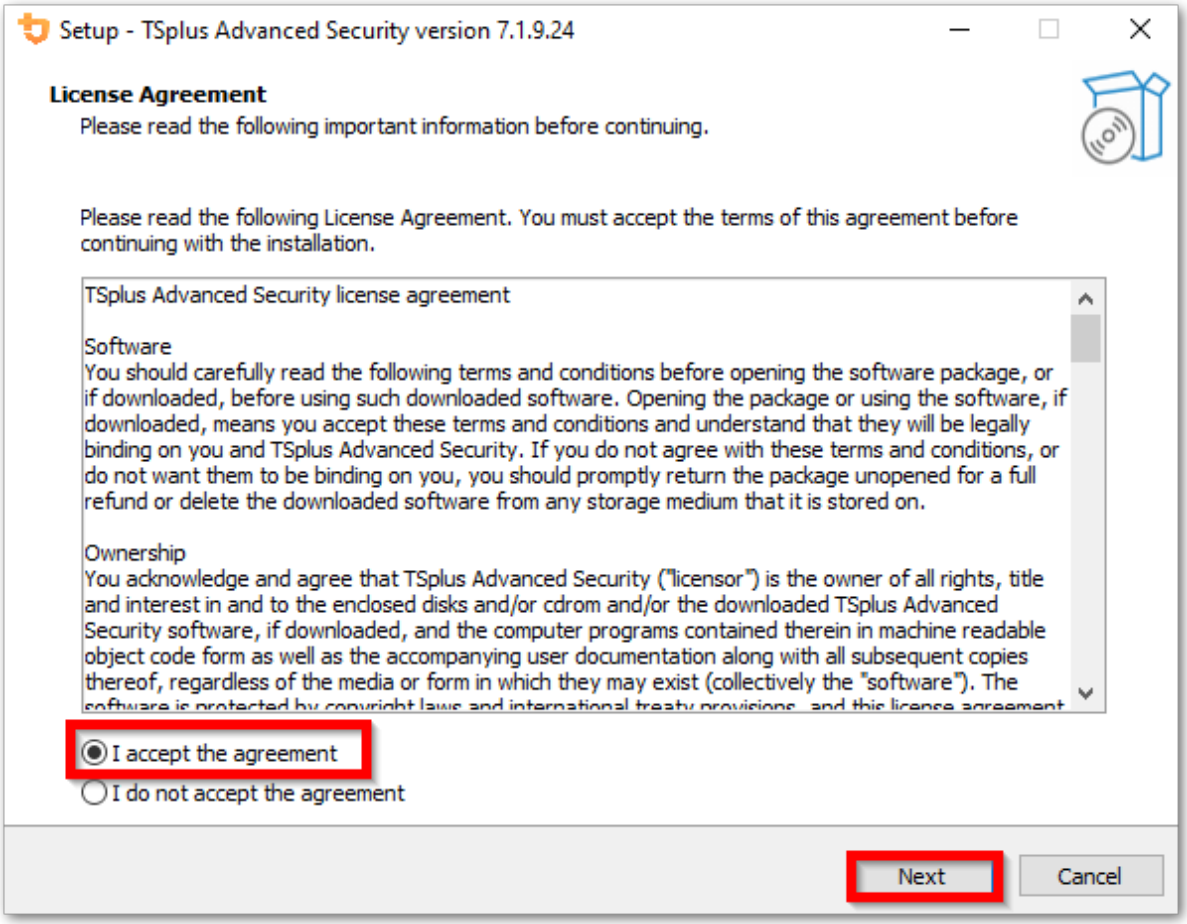
Seleziona la lingua dell'assistente di configurazione se non rilevata automaticamente.

Poi, seleziona una delle due opzioni: **Consigliato** o **Avanzato** cliccando sulle caselle corrispondenti.

L'opzione Avanzata aggiunge passaggi aggiuntivi che ti consentono di:

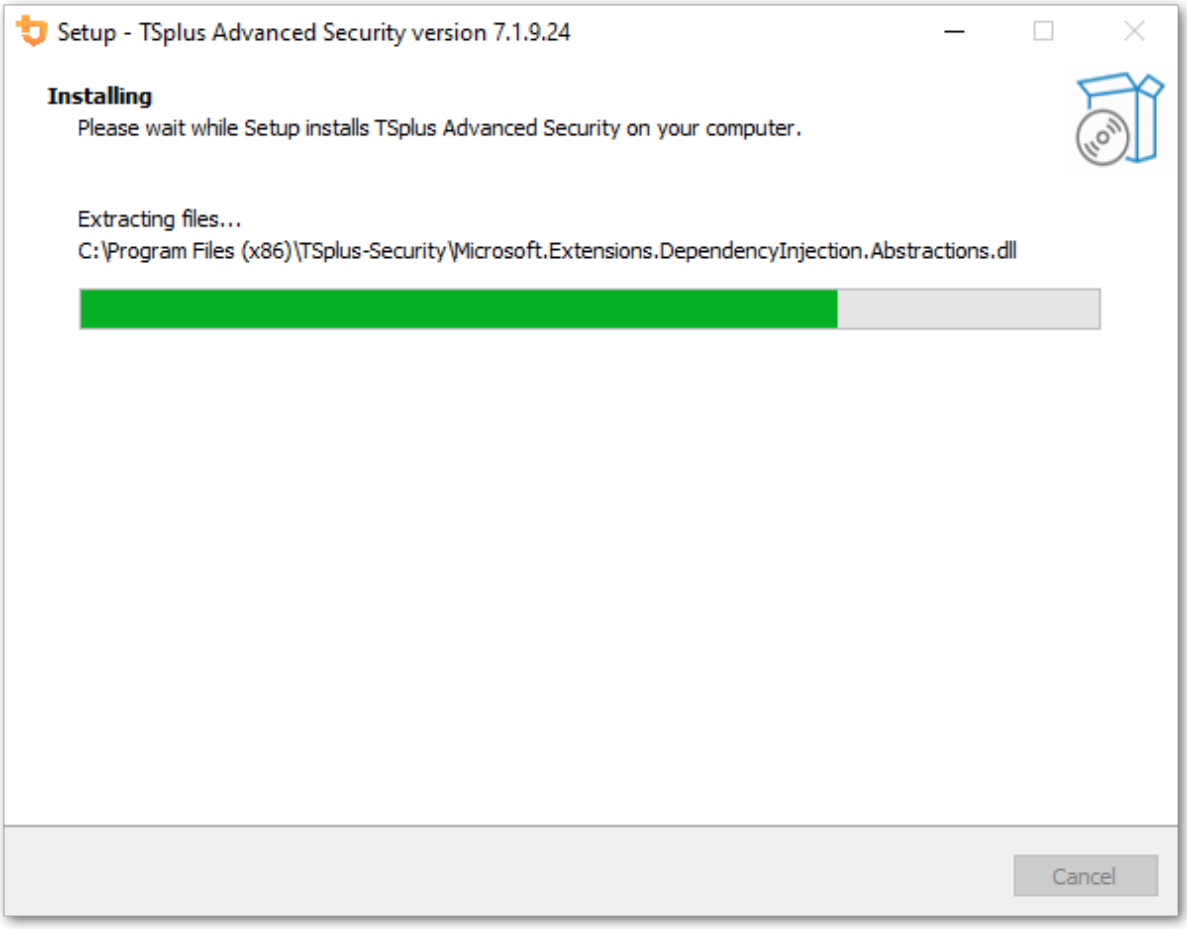
- Scarica solo il programma di installazione (non installare)
- Usa impostazioni proxy personalizzate

Leggi il contratto di licenza e fai clic su "Accetto" per riprendere l'installazione.



Il programma verrà installato sul tuo computer.

Una barra di avanzamento viene visualizzata in basso e riporta il progresso dell'installazione.



Per favore, sii paziente , poiché a volte può richiedere fino a pochi minuti per installare completamente il software.

Una volta completata l'installazione, puoi iniziare a utilizzare TSplus Advanced Security!

La versione di prova gratuita è completamente funzionale per 15 giorni. Non dimenticare di attiva la tua licenza e a aggiornare all'ultima versione per mantenere la protezione di Advanced Security al meglio!

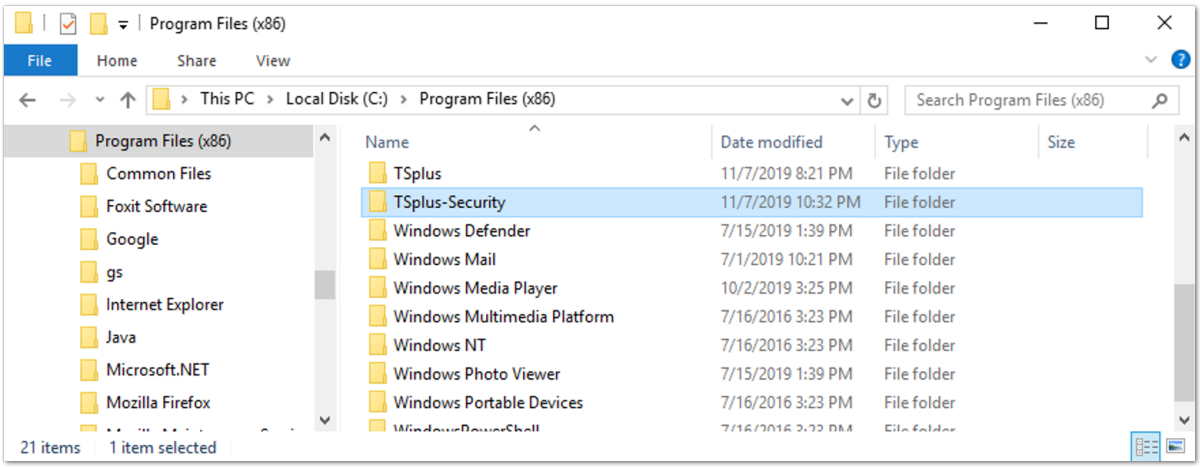
Scenari di installazione avanzati

Il TSplus Advanced Security Classic Setup program gestisce i seguenti scenari poiché può essere eseguito dalla riga di comando:

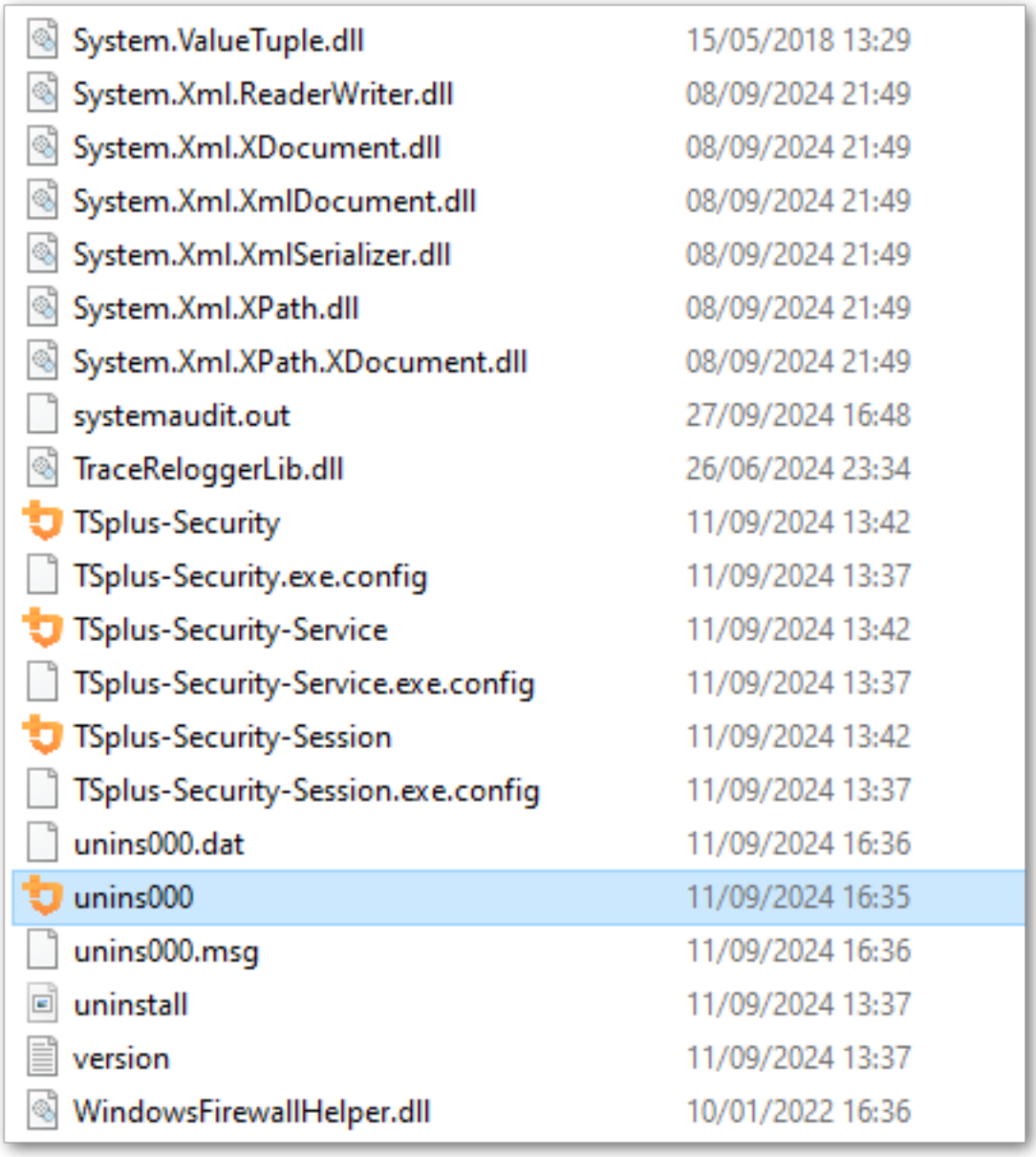
- Installa silenziosamente, fornendo i parametri /VERYSILENT /SUPPRESSMSGBOXES
- Impedire il riavvio al termine della configurazione, fornendo il parametro /NORESTART. Questo parametro è solitamente utilizzato insieme a quanto sopra.
- Licenza in volume per attivare la tua licenza direttamente durante l'installazione (si prega di fare riferimento alla documentazione o contattaci per ulteriori informazioni

Disinstallare TSplus Advanced Security

Per disinstallare completamente TSplus Advanced Security, aprire la directory C:\Program Files (x86)\TSplus-Security.



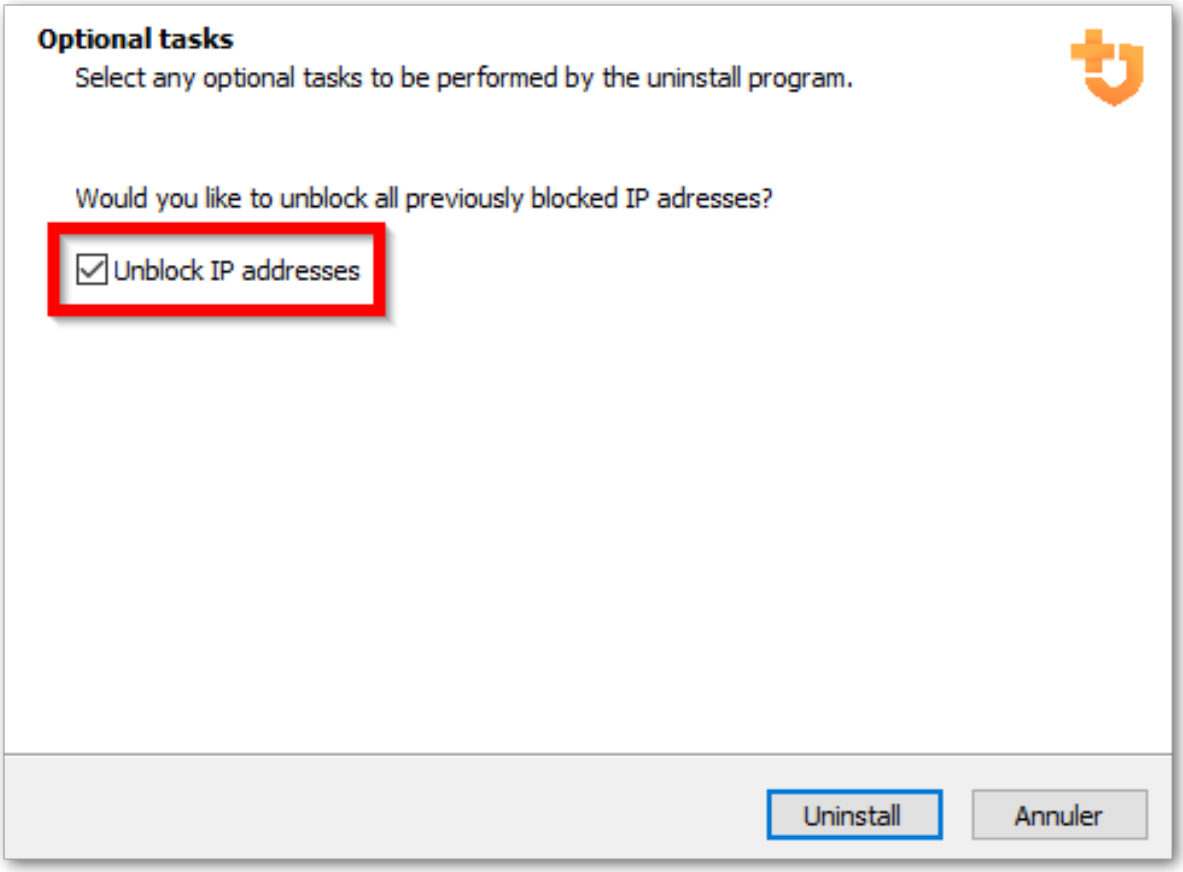
Poi, fai doppio clic sull'applicazione "unins000" per eseguire il programma di disinstallazione.



Clicca su sì nella finestra successiva per rimuovere completamente TSplus Advanced Security e tutti i suoi componenti.

A meno che non sia configurato diversamente, Advanced Security aggiunge regole di blocco al Windows Firewall. Clicca su "Sblocca indirizzi IP" per sbloccare e rimuovere tutti gli indirizzi IP precedentemente bloccati da Advanced Security.

Importante: Si prega di tenere presente che rimuovere tutte le regole può richiedere fino a un'ora. Per questo motivo, raccomandiamo di rimuovere le regole direttamente dalla console di Windows Firewall con Sicurezza Avanzata.



Il software verrà completamente disinstallato dal tuo computer.

Gestione delle autorizzazioni

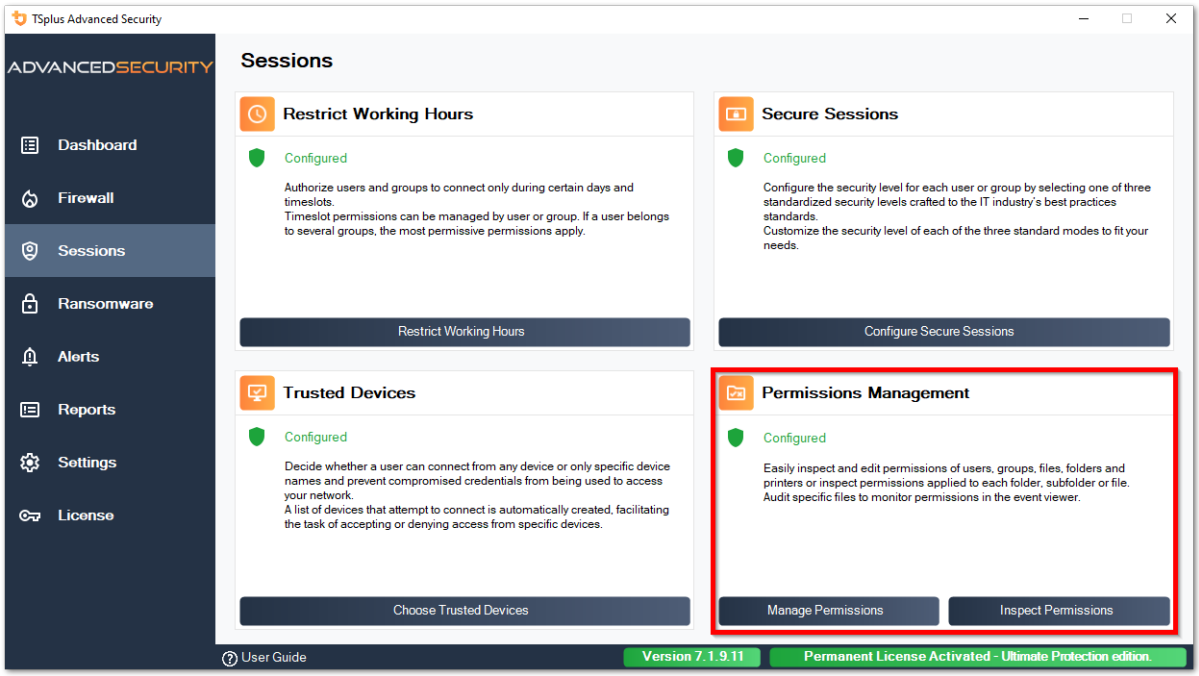
Dalla versione 4.3, TSplus Advanced Security offre una funzionalità di Permessi, che consente all'amministratore di gestire e/o ispezionare i privilegi di utenti/gruppi.

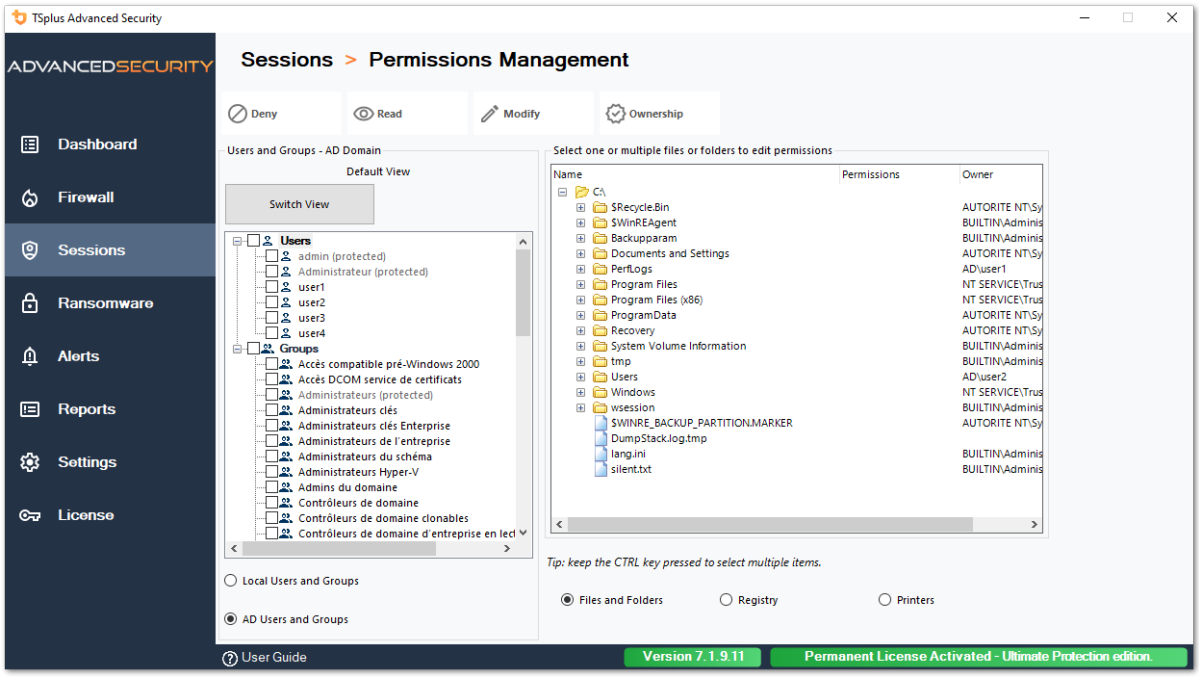
Nella dashboard delle autorizzazioni, l'elenco degli utenti e dei gruppi e l'elenco di disponibili **file, cartelle, registri e stampanti** sono mostrati affiancati.

Tutto è visibile a colpo d'occhio, il che rende super facile. **Ispeziona** e **Gestisci/Modifica** privilegi per un utente alla volta e quindi per aumentare l'accuratezza delle restrizioni.

Gestire le autorizzazioni

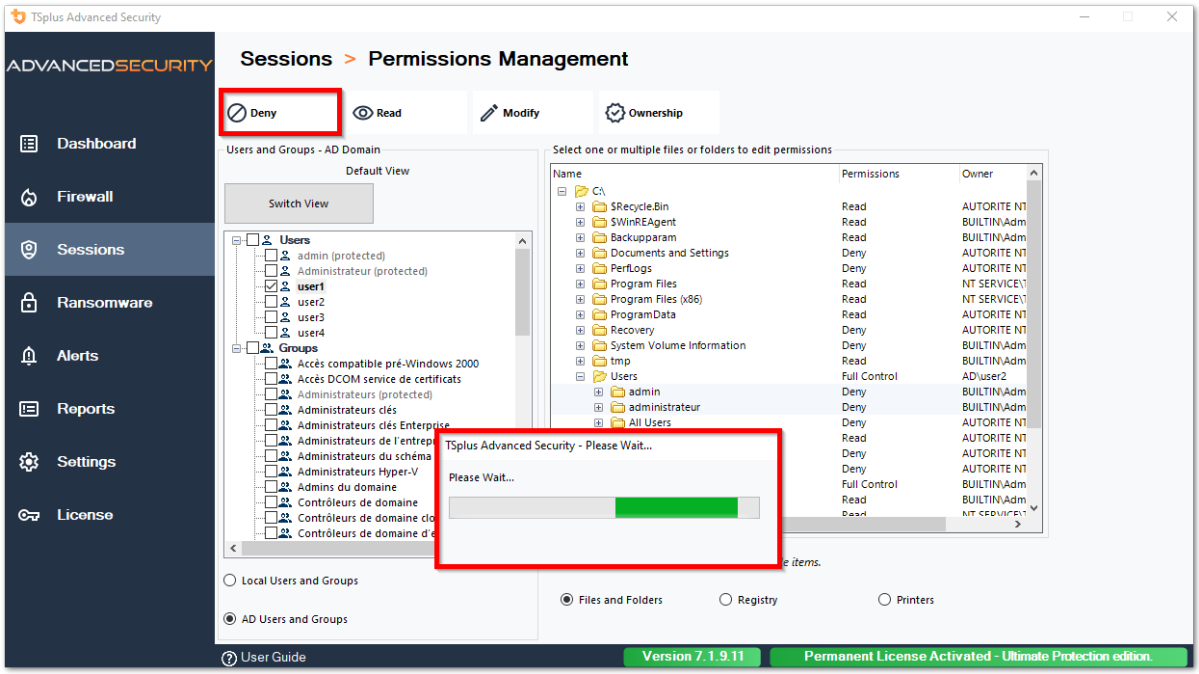
Nella scheda Gestisci, per ogni utente o gruppo selezionato nella vista ad albero a sinistra, puoi:



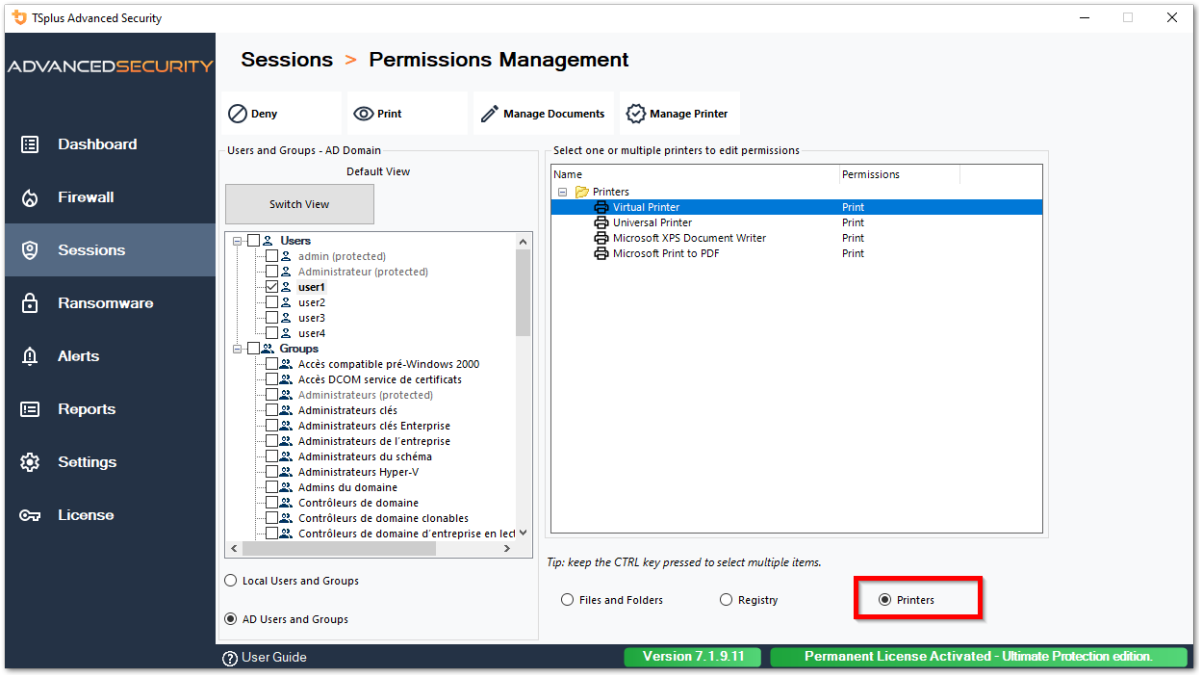


- **Negare** Quando si fa clic sul pulsante Negare, all'utente selezionato verrà negato il privilegio sull'oggetto filesystem selezionato. Se è selezionato un file, all'utente selezionato verrà negato il privilegio di leggere il file selezionato (FileSystemRights.Read). Se è selezionata una directory, all'utente selezionato verrà negato il privilegio di leggere e elencare il contenuto della directory (FileSystemRights.Read e FileSystemRights.ListDirectory).
- **Leggi** Quando si fa clic sul pulsante Leggi, all'utente selezionato verrà concessa l'autorizzazione sull'oggetto filesystem selezionato. Se è selezionato un file, all'utente selezionato viene concessa l'autorizzazione di leggere il file selezionato ed eseguire se il file è un programma (FileSystemRights.ReadAndExecute). Se è selezionata una directory, all'utente selezionato viene concessa l'autorizzazione di leggere e elencare o eseguire il contenuto della directory (FileSystemRights.ReadAndExecute e FileSystemRights.ListDirectory e FileSystemRights.Traverse).
- **Modifica** Quando si fa clic sul pulsante Modifica, all'utente selezionato verrà concessa l'autorizzazione sull'oggetto filesystem selezionato. Se è selezionato un file, all'utente selezionato viene concessa l'autorizzazione di modificare il file selezionato (FileSystemRights.Modify). Se è selezionata una directory, all'utente selezionato viene concessa l'autorizzazione di modificare e elencare il contenuto della directory, nonché di creare nuovi file o directory (FileSystemRights.Modify e FileSystemRights.CreateDirectories e FileSystemRights.CreateFiles e FileSystemRights.ListDirectory e FileSystemRights.Traverse).
- **Proprietà** Quando si fa clic sul pulsante Proprietà, all'utente selezionato verrà concessa il pieno controllo sull'oggetto filesystem selezionato (FileSystemRights.FullControl).

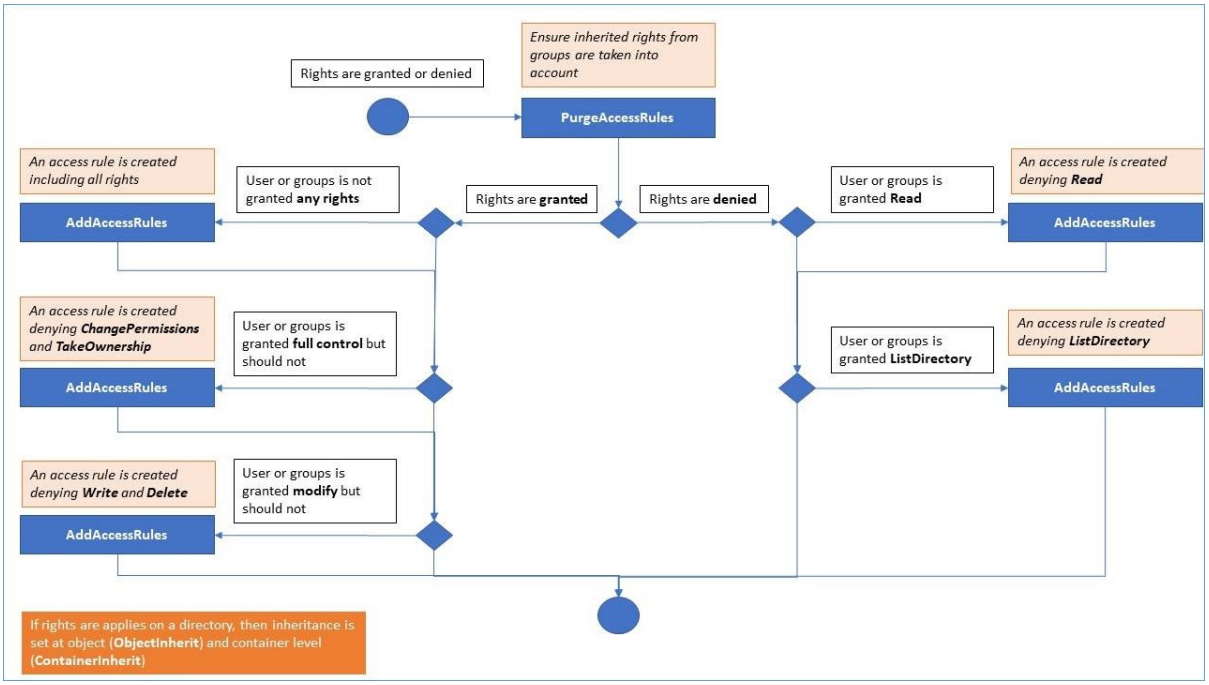
Le stesse opzioni di autorizzazione sono possibili per ciascun Registro, selezionando il pulsante corrispondente sotto la vista ad albero di destra:



E per ogni stampante:



Si prega di notare che tutte le autorizzazioni negate o concesse a una directory vengono applicate in modo ricorsivo agli oggetti del filesystem contenuti in questa directory. Il diagramma sottostante dettaglia le chiamate API quando i diritti vengono applicati a un oggetto del filesystem.

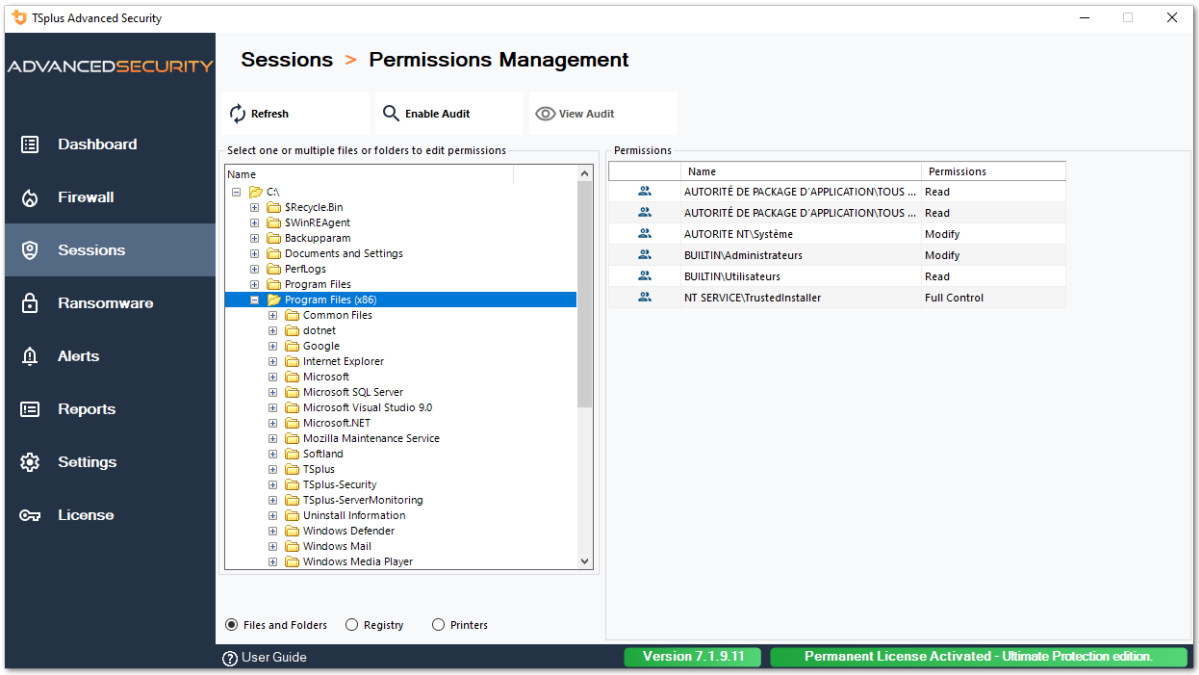


Documentazione :

- Sicurezza degli oggetti: https://docs.microsoft.com/it-it/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- FileSystemRights: https://docs.microsoft.com/it-it/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

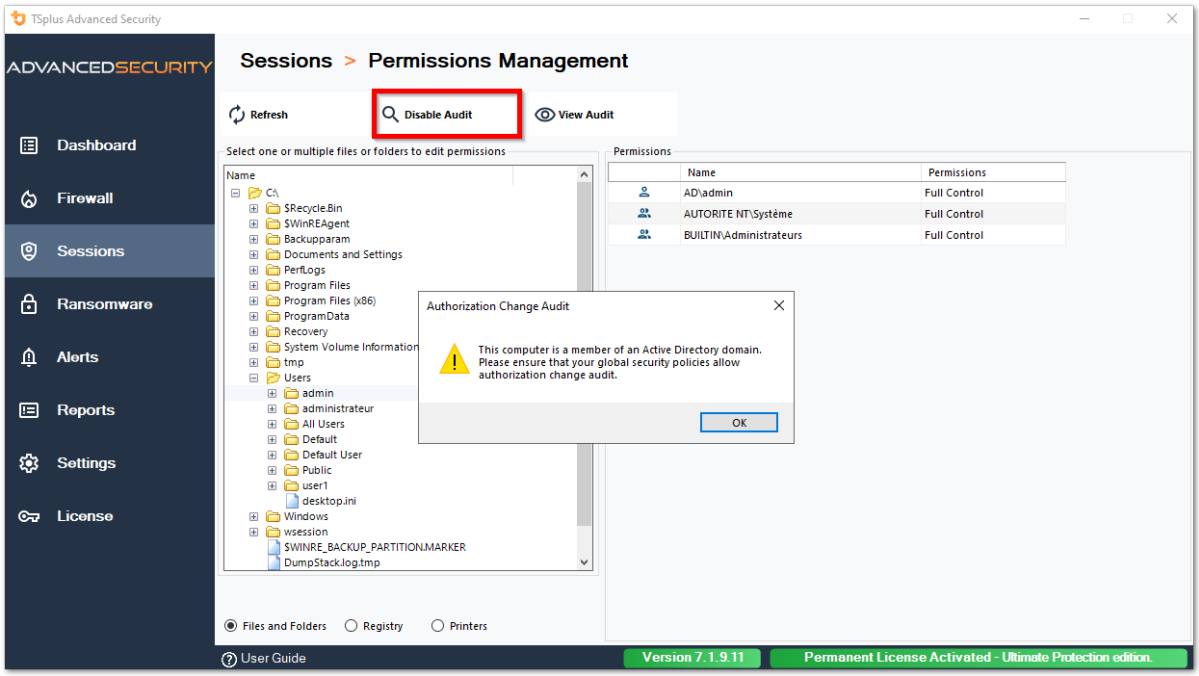
Ispeziona autorizzazioni

Nella scheda Ispeziona, per ogni cartella, sottocartella o file selezionato nella vista ad albero a sinistra, puoi vedere i corrispondenti permessi attribuiti agli utenti o ai gruppi nella vista ad albero a destra.

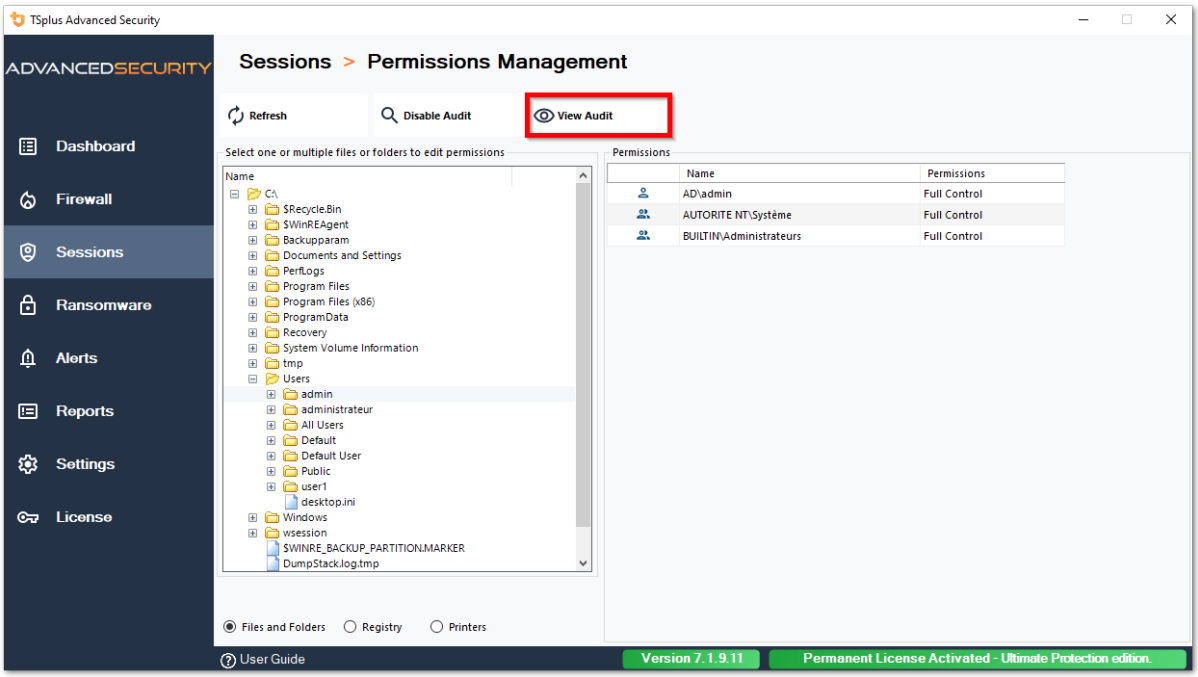


Puoi aggiornare lo stato delle cartelle affinché vengano aggiornate in tempo reale.

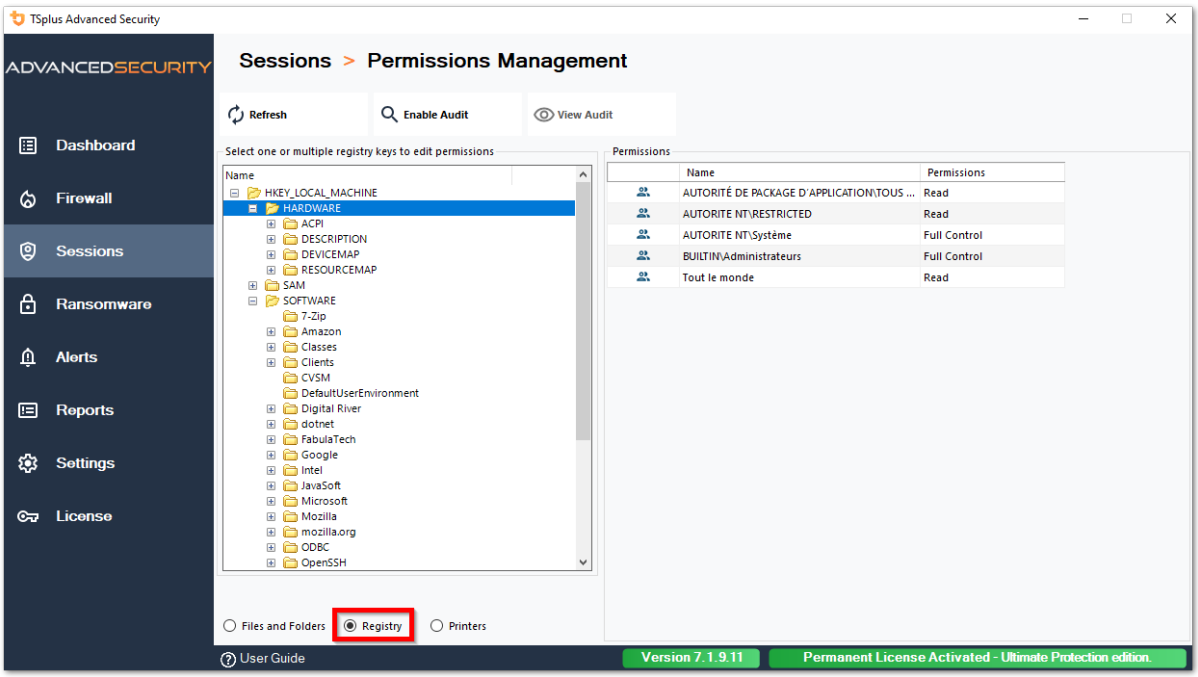
Un audit può essere abilitato selezionando la cartella, la sottocartella o il file desiderato e facendo clic sul pulsante "Abilita audit" in alto:

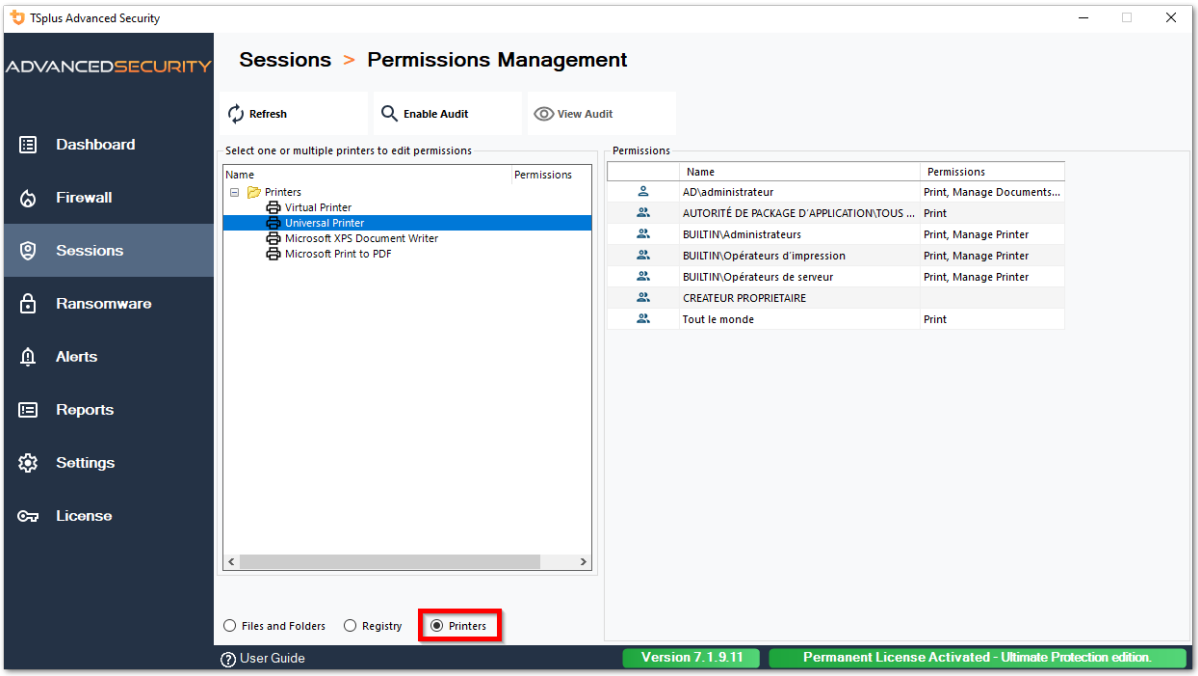


Il pulsante "Visualizza Audit" consente di visualizzare l'audit corrispondente nel Visualizzatore eventi:



Le stesse possibilità di ispezione sono disponibili per ogni registro e stampante selezionando il pulsante corrispondente sotto la vista ad albero a sinistra:




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 - Requisiti preliminari

Requisiti hardware

TSplus Advanced Security supporta architetture a 32 bit e 64 bit.

Sistema Operativo

Il tuo hardware deve utilizzare uno dei sistemi operativi seguenti:

- 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 **Server 2019**
- Windows **Server 2022**
- Windows **Server 2025**

Sia le architetture a 32 che a 64 bit sono supportate.

Requisiti software

TSplus Advanced Security richiede i seguenti prerequisiti:

- Runtime: .NET Framework 4.7.2 o superiore
- Microsoft Windows 7 SP1 e Windows 2008 R2 SP1 richiedono un aggiornamento aggiuntivo per supportare la firma incrociata SHA2 KB4474419 Questo aggiornamento consente al firewall integrato di TSplus Advanced Security e alla protezione contro il ransomware di

funzionare correttamente.

Nota: Questi prerequisiti saranno installati automaticamente dal programma di installazione se mancanti nel sistema.

TSplus Advanced Security - Inizio rapido

Prerequisiti

TSplus Advanced Security richiede i seguenti requisiti.

- Sistema operativo: Microsoft Windows versione 7, Service Pack 1 (build 6.1.7601) o Windows 2008 R2, Service Pack 1 (build 6.1.7601) o superiore.

Il seguente **i requisiti verranno installati automaticamente dal programma di installazione** se mancante:

- Runtime: .NET Framework 4.5.3 o superiore
- Microsoft Windows 7 SP1 e Windows 2008 R2 SP1 richiedono un aggiornamento aggiuntivo per supportare la firma incrociata SHA2 KB4474419 Questo aggiornamento consente al firewall integrato di TSplus Advanced Security e alla protezione contro il ransomware di funzionare correttamente.

Si prega di fare riferimento al documentazione per ulteriori dettagli sui requisiti.

Passo 1: Installazione

L'ultimo programma di installazione di TSplus Advanced Security è sempre disponibile qui: Ultimo programma di installazione di TSplus Advanced Security Si prega di scaricare il programma di installazione e seguire la procedura guidata di installazione.

Il programma di installazione di TSplus Advanced Security di solito non richiede di riavviare il sistema per completare l'installazione.

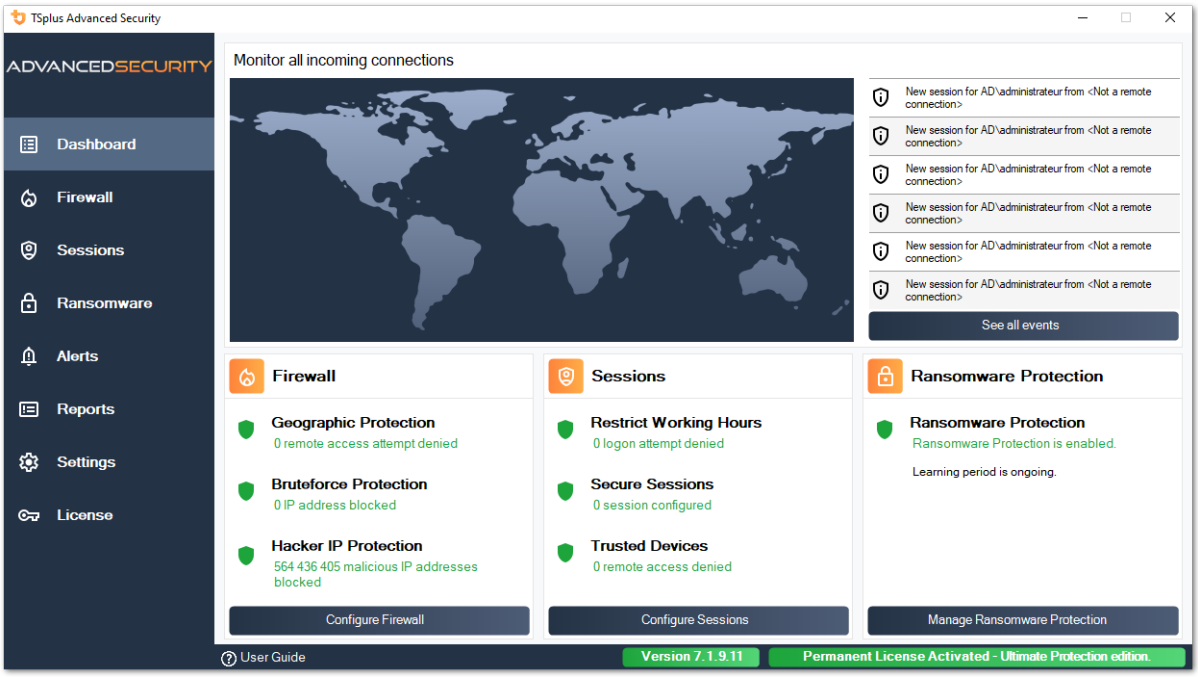
Qualsiasi nuova installazione avvia un periodo di prova completo di 15 giorni. Si prega di non esitare a contattaci se dovessi affrontare qualche ostacolo o se hai problemi nella configurazione di TSplus Advanced Security.

Una volta completata l'installazione, viene visualizzata una nuova icona sul Desktop. Fai doppio clic su questa icona per aprire TSplus Advanced Security e iniziare a configurare le funzionalità di sicurezza.

Si prega di fare riferimento al documentazione per le istruzioni complete di installazione.

Passo 2: Configurare TSplus Advanced Security

Hai lanciato TSplus Advanced Security e ha iniziato a configurare le funzionalità per proteggere il tuo server da attività dannose e applicare politiche di sicurezza rigorose.



Nella colonna di sinistra, la homepage consente un accesso rapido per configurare le funzionalità di Ransomware protection, Bruteforce protection e Geographic protection.

Inizio Protezione da Ransomware periodo di apprendimento di per consentire ad Advanced Security di identificare applicazioni e comportamenti legittimi sul tuo sistema facendo clic sulla seguente piastrella:

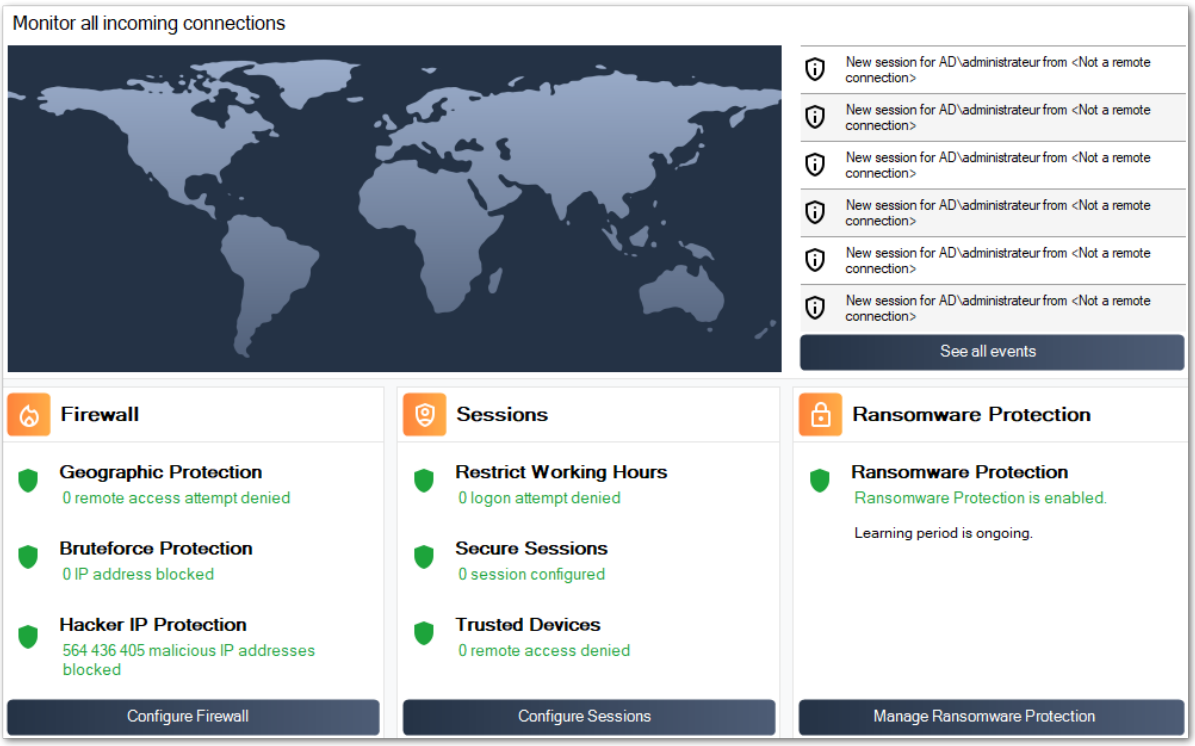
Protezione da attacchi di forza bruta è solitamente operativo dopo l'installazione. In caso contrario, fai clic su **Difesa ripetuta contro attacchi di forza bruta** titolo per risolvere problemi e applicare la configurazione di sistema richiesta. Per impostazione predefinita, questa funzione blocca gli attaccanti dopo 10 tentativi di accesso non riusciti.

Infine, aggiungi il tuo paese nell'elenco dei paesi autorizzati da cui i clienti possono connettersi. Clicca sulla piastrella **Autorizza connessioni da un altro paese** e aggiungi il tuo paese per configurare Protezione geografica

Sei tutto pronto! Non dimenticare di attiva la tua licenza e a aggiornare all'ultima versione per mantenere la protezione di Advanced Security al meglio!

Passaggio 3: Revisione delle minacce bloccate

Ora che hai configurato le principali funzionalità di sicurezza avanzata, le minacce evitate verranno segnalate nel Dashboard.



Inoltre, il Hacker IP la protezione mantiene la macchina protetta contro minacce conosciute bloccando più di 500.000.000 indirizzi IP malevoli noti.

Tutti i eventi di sicurezza può essere visualizzato facendo clic su **Vedi tutti gli eventi** piastrella.

Passo 4: Sfruttare altre funzionalità di sicurezza per migliorare la protezione

In fondo, è possibile accedere e configurare altre quattro funzionalità di sicurezza per migliorare la protezione della tua macchina.

- Regola e monitora i privilegi di accesso sui tuoi file system locali, stampanti e chiavi di registro per garantire che ogni utente abbia accesso alle risorse pertinenti, con il Permessi funzionalità.
- Definire il periodo di tempo in cui gli utenti sono autorizzati ad accedere con il Working Hours Funzione. Gli utenti verranno disconnessi superati i loro orari di lavoro consentiti.
-

Personalizza e proteggi le sessioni utente con il Desktop Sicuro funzione. Personalizza, nascondi, nega l'accesso agli elementi dell'interfaccia della sessione per gli utenti locali.

- Convalida il nome del client remoto quando un utente si connette al tuo computer con Protezione degli endpoint Questa funzione convalida i nomi delle macchine client per ogni utente connesso in remoto.

C'è di più! Passare alla modalità avanzata ti concede l'accesso a ulteriori funzionalità.

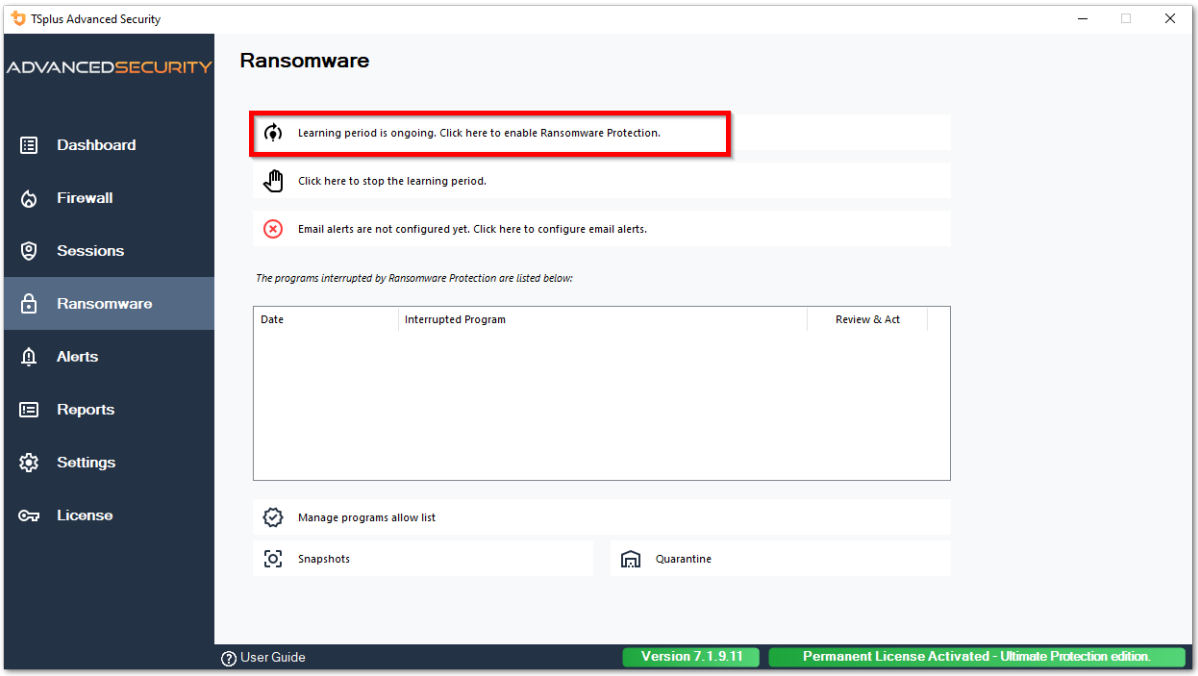
Grazie per utilizzare TSplus Advanced Security!

Protezione da Ransomware

La protezione da ransomware ti consente di rilevare, bloccare e prevenire in modo efficiente gli attacchi ransomware. TSplus Advanced Security reagisce non appena rileva ransomware nella tua sessione. Possiede sia **analisi statica e comportamentale** :

- Il **analisi statica** abilita il software a reagire immediatamente quando viene modificato un nome di estensione,
- Il **analisi comportamentale** osserva come un programma interagirà con i file e rileverà nuovi ceppi di ransomware.

Puoi attivarlo facendo clic su "Abilita protezione da ransomware" nella scheda Protezione da ransomware:

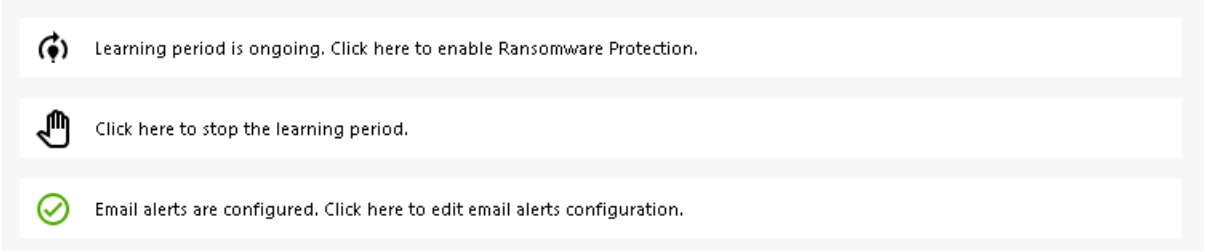


Periodo di apprendimento

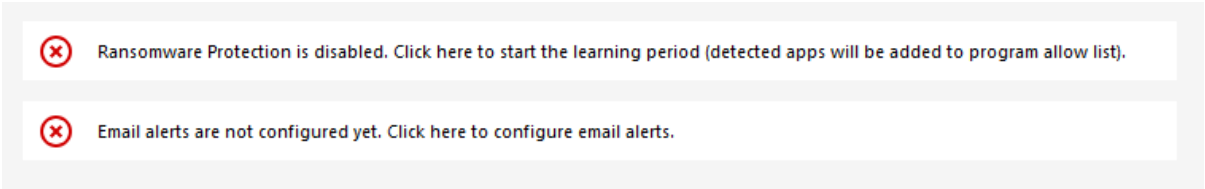
Dopo aver attivato la funzione di protezione da ransomware, il periodo di apprendimento viene attivato automaticamente. Durante il periodo di apprendimento, tutti i programmi rilevati dalla funzione di protezione da ransomware saranno considerati falsi positivi e potranno riprendere la

loro esecuzione. I programmi rilevati come falsi positivi verranno aggiunti automaticamente all'elenco dei programmi consentiti.

Questa funzione consente di configurare la protezione da ransomware su un server di produzione senza interrompere la sua attività. Raccomandiamo di iniziare con un periodo di apprendimento di 5 giorni per identificare tutte le applicazioni aziendali legittime.



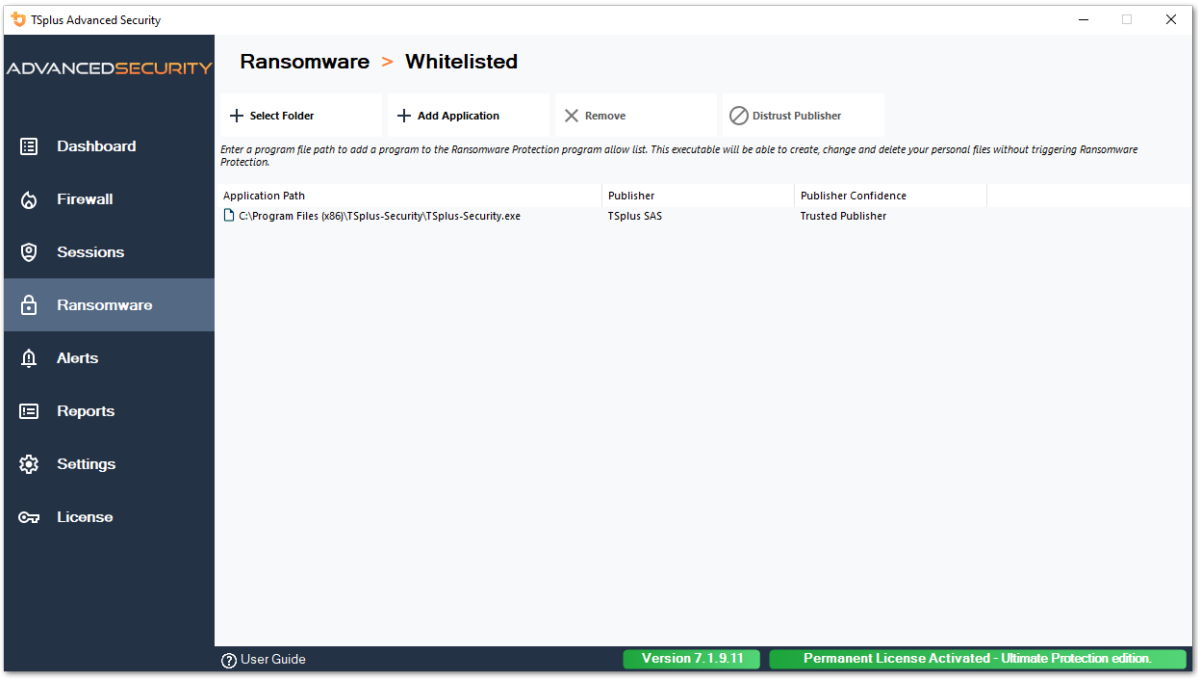
Se interrompi il Periodo di Apprendimento, disattiverà la Protezione da Ransomware. Clicca sul pulsante "La Protezione da Ransomware è disabilitata" per riattivare il Periodo di Apprendimento.



Azione di protezione da ransomware

Scansiona rapidamente il tuo disco o i tuoi dischi e visualizza il file o i programmi responsabili, oltre a fornire un elenco degli elementi infetti. TSplus Advanced Security interrompe automaticamente l'attacco e mette in quarantena il programma o i file crittografati prima del suo intervento.

Solo l'amministratore può inserirli nella whitelist, inserendo il percorso del programma desiderato nella riga in basso e cliccando su "Aggiungi":



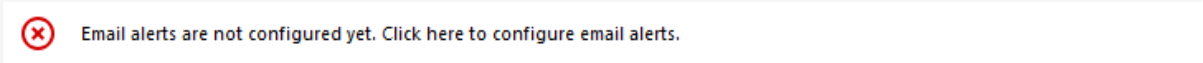
Rapporto di protezione da ransomware

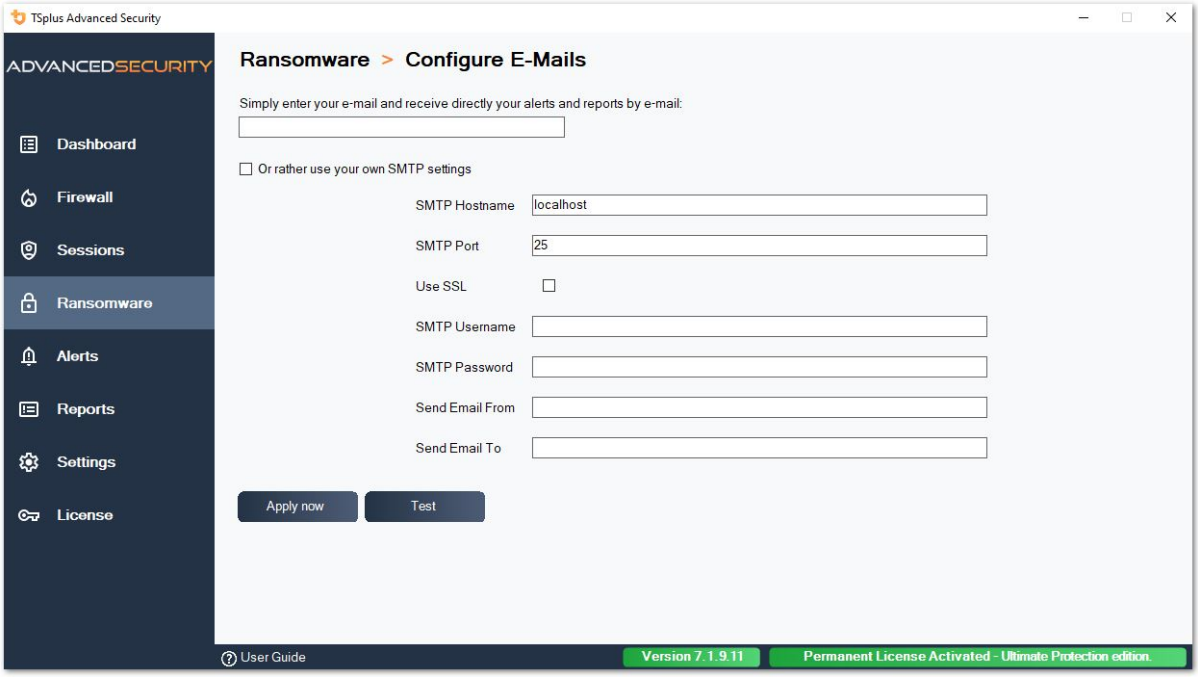
TSplus Advanced Security previene eventi catastrofici per le aziende rimuovendo il ransomware in una fase iniziale.

L'amministratore ha accesso a informazioni riguardanti la fonte dell'attacco e i processi in esecuzione, e quindi apprende come anticipare queste minacce.

Nota La Protezione da Ransomware osserva come i programmi interagiscono con i file di sistema e personali. Per garantire un livello di protezione maggiore, la Protezione da Ransomware crea file esca in cartelle chiave dove il ransomware inizia spesso il suo attacco. Pertanto, alcuni file nascosti possono apparire nelle cartelle desktop e documenti degli utenti, così come in altre posizioni. Quando rileva un comportamento malevolo, ferma immediatamente il ransomware (o chiede se l'utente connesso è un amministratore). La Protezione da Ransomware utilizza tecniche di rilevamento comportamentale puro e non si basa su firme di malware, permettendole di catturare ransomware che non esiste ancora.

Puoi configurare le impostazioni SMTP affinché TSplus Advanced Security ti invii avvisi via email per evidenziare eventi di sicurezza importanti facendo clic sul pulsante sotto quello di attivazione del Ransomware:





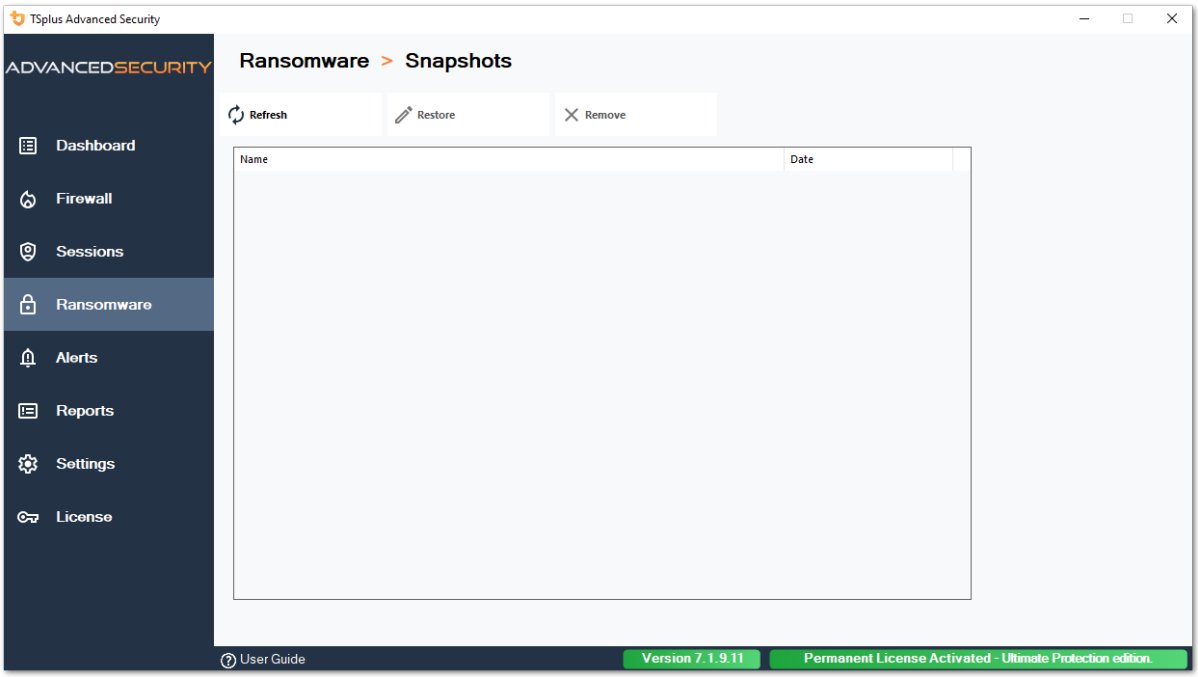
Inserisci il tuo nome host SMTP, la porta e seleziona la casella Usa SSL e cambia la porta da 25 a 465 se desideri utilizzare SSL.

Inserisci il nome utente e la password SMTP, così come gli indirizzi del mittente e del destinatario.

Le impostazioni email possono essere convalidate inviando un test durante il salvataggio delle impostazioni SMTP.

Snapshot

Le istantanee scattate da Ransomware Protection sono visibili nella scheda Istantanee:

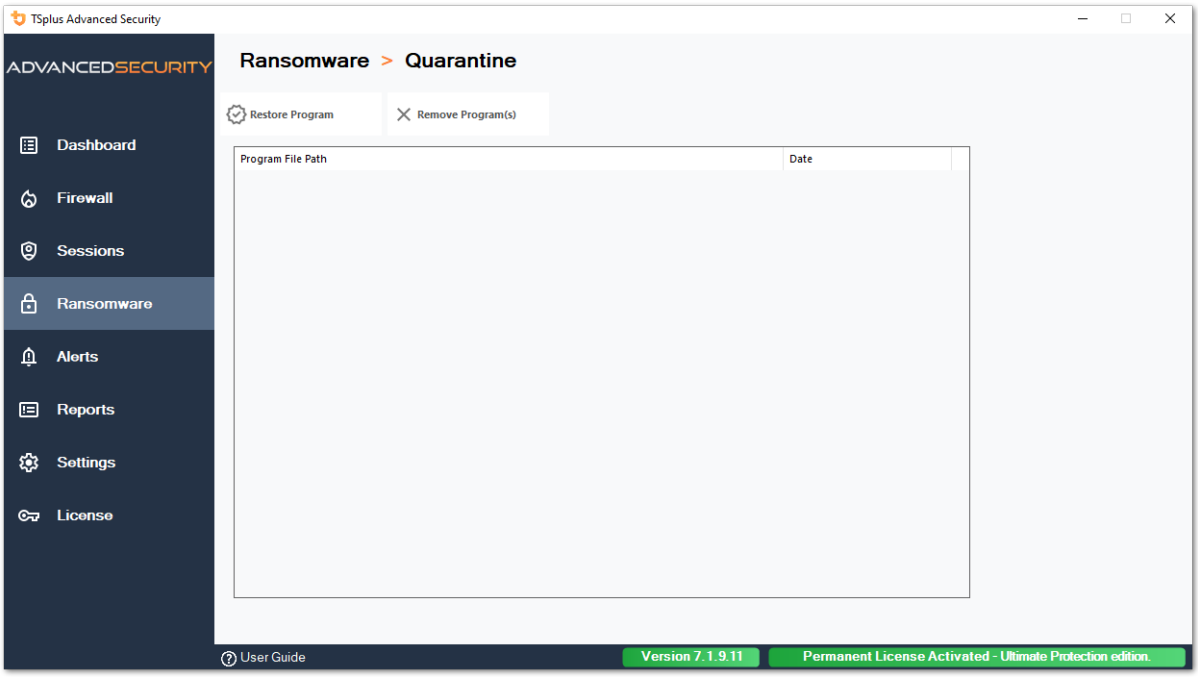


La lista può essere aggiornata facendo clic sul pulsante corrispondente. Ogni elemento può essere ripristinato o rimosso.

Quarantena

I programmi in quarantena sono visibili nella scheda Quarantena:
I programmi potenzialmente indesiderati vengono mantenuti in quarantena indefinitamente fino a quando non decidi quale azione intraprendere.

In questo modo, Advanced Security garantisce la sicurezza della tua macchina mentre ti offre la possibilità di gestire gli elementi in quarantena come preferisci.
Questo può essere utile se hai bisogno di recuperare un file o un programma che è stato neutralizzato. **Questa decisione è presa a proprio rischio.**
Puoi anche eliminare permanentemente qualsiasi file o programma che scegli direttamente dalla cartella di quarantena situata nella directory di installazione di Advanced Security.



Ogni elemento può essere ripristinato o rimosso.

I file ignorati non vengono utilizzati per rilevare possibili azioni dannose e non vengono salvati quando vengono modificati. L'idea è escludere qualsiasi operazione su file di grandi dimensioni o irrilevanti (come i file di log).

- sys
- 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
- dmg
- sparseimage
- cab
- msi
- mui
- dl_
- wim
- ost
- o
- qtch
- ithmb
- vmdk
- vmem
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- menudata
- icona dell'app
- appinfo
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- drk
- mem
- nvram
- hdd
- pk3
- pf
- trn
- automaticDestinations-ms

Attenzione riguardo all'estensione dei file di backup

L'estensione del file utilizzata per salvare i file modificati è: **istantanea.** Il driver vieta qualsiasi azione di modifica o eliminazione su questi file se non eseguita dal servizio TSplus Advanced Security. Fermare il servizio elimina i file di backup. Per eliminare questi file manualmente, è necessario scaricare temporaneamente il driver.

Configurazione del file di backup

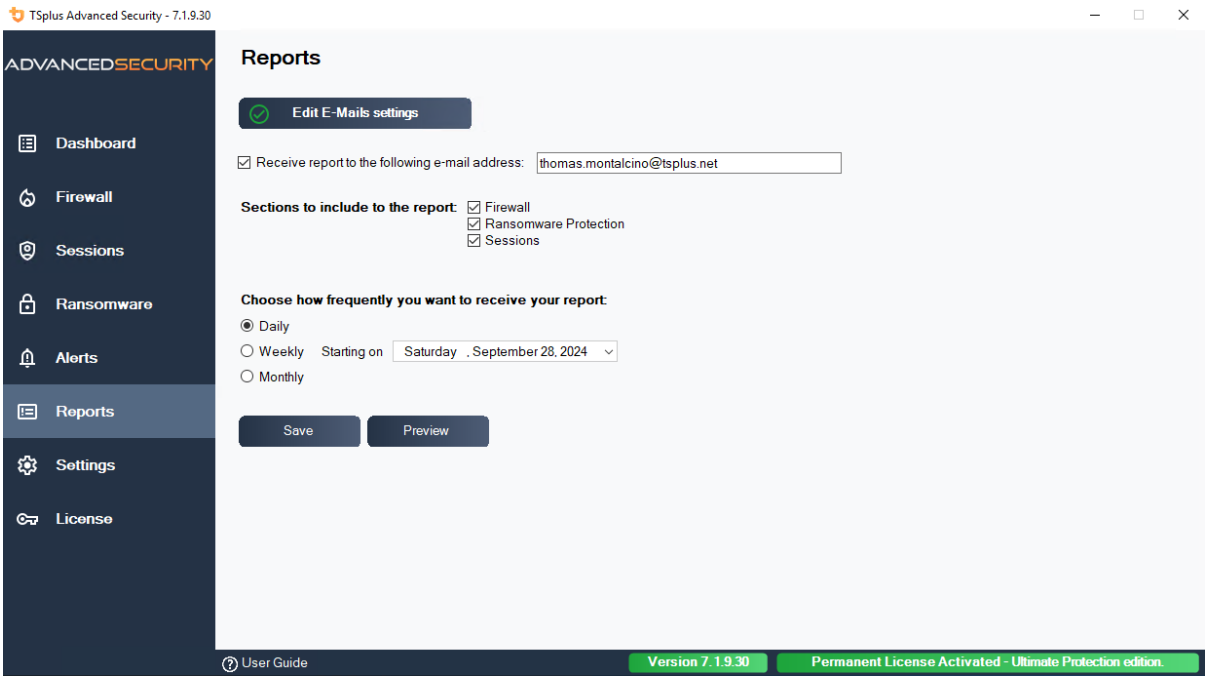
Per impostazione predefinita, la directory dei file salvati si trova nella directory di installazione di TSplus Advanced Security e si chiama "snapshots". Tuttavia, è possibile definire un'altra posizione per questa directory. Questo può consentire all'amministratore di definire una directory situata su un disco più veloce (SSD) o su un disco più grande in base alle proprie esigenze. Il percorso della directory di backup non deve essere un percorso UNC, nella forma di:

\\ \ \

Aggiunta di utilità di backup alla whitelist

Raccomandiamo di aggiungere utilità di backup nella whitelist.

Reportistica



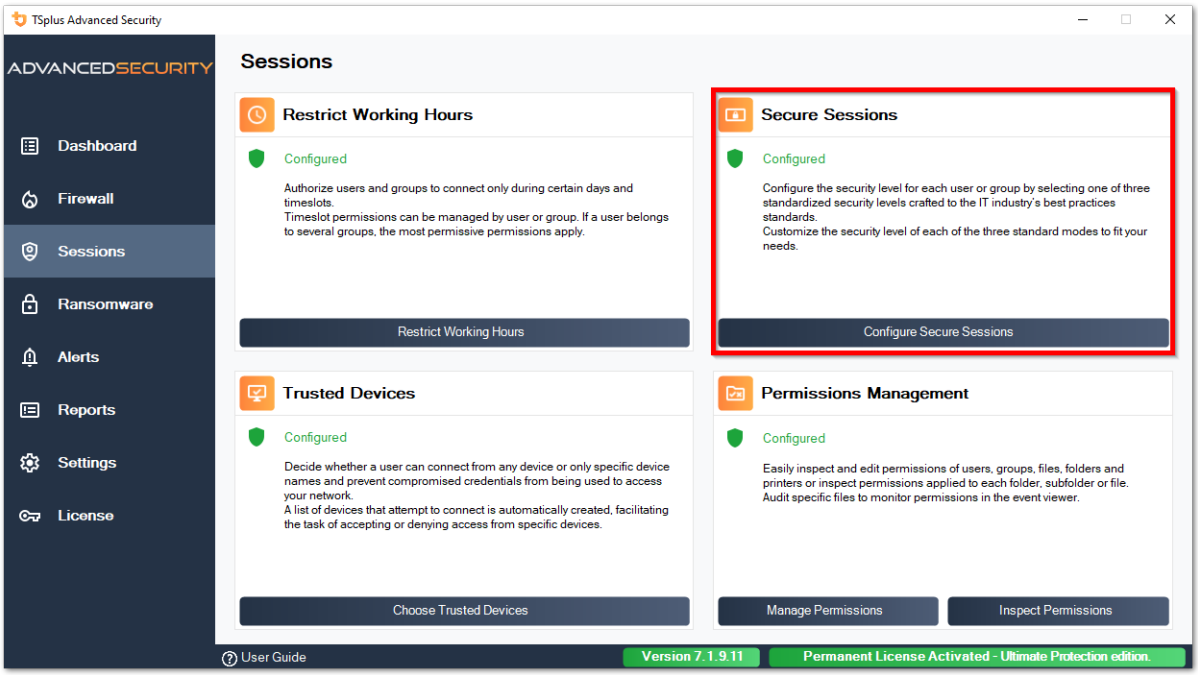
Sessioni Sicure

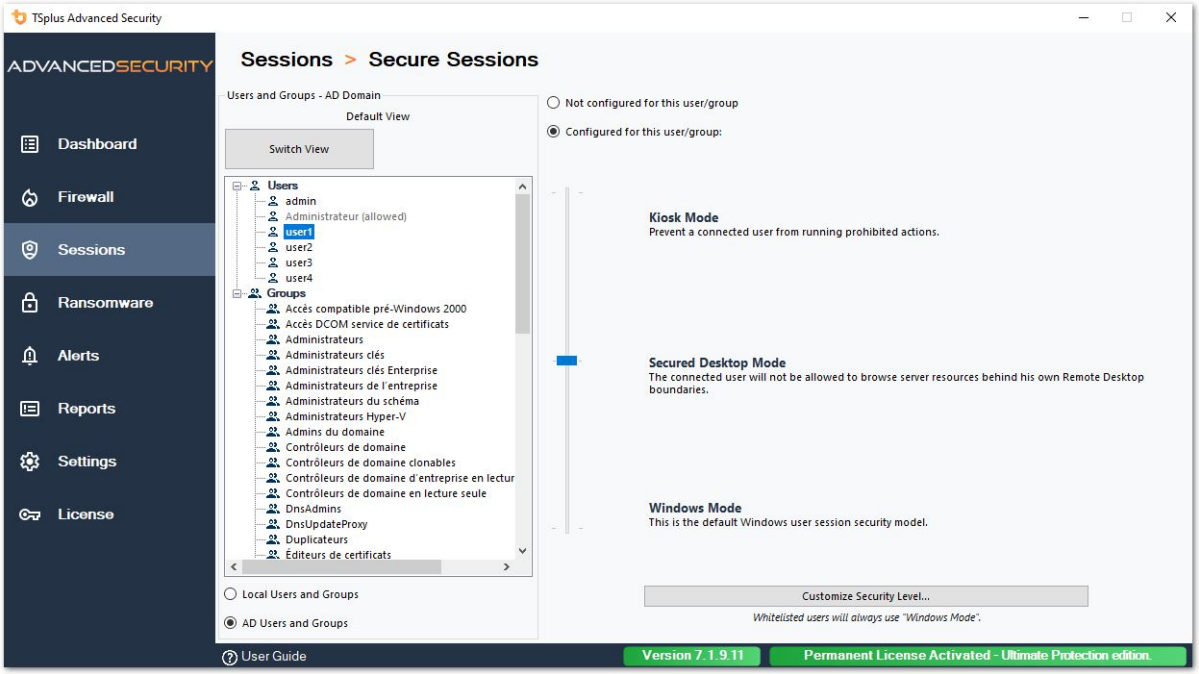
Attenzione

- Le sessioni sicure sono molto probabilmente in conflitto con le politiche di sicurezza definite da Active Directory.
- Lo scopo principale delle Sessioni Sicure è personalizzare l'interfaccia utente, non applicare le autorizzazioni di accesso. Il suo utilizzo dovrebbe essere combinato con la funzione Permessi per garantire l'accesso a diverse unità.

Puoi configurare il livello di sicurezza per ogni utente o gruppo. Ci sono tre livelli di sicurezza:

- Il **Modalità Windows** dove l'utente ha accesso a una sessione Windows predefinita.
- Il **Modalità Sessioni Sicure** dove l'utente non ha accesso al Pannello di Controllo, ai programmi, ai dischi, al browser, nessun clic destro…: nessun accesso alle risorse del server. Ha solo accesso ai documenti, alle stampanti, al tasto Windows e può disconnettere la sua sessione.
- Il **Modalità Kiosk** è il più sicuro, dove l'utente ha azioni molto limitate nella sua sessione.

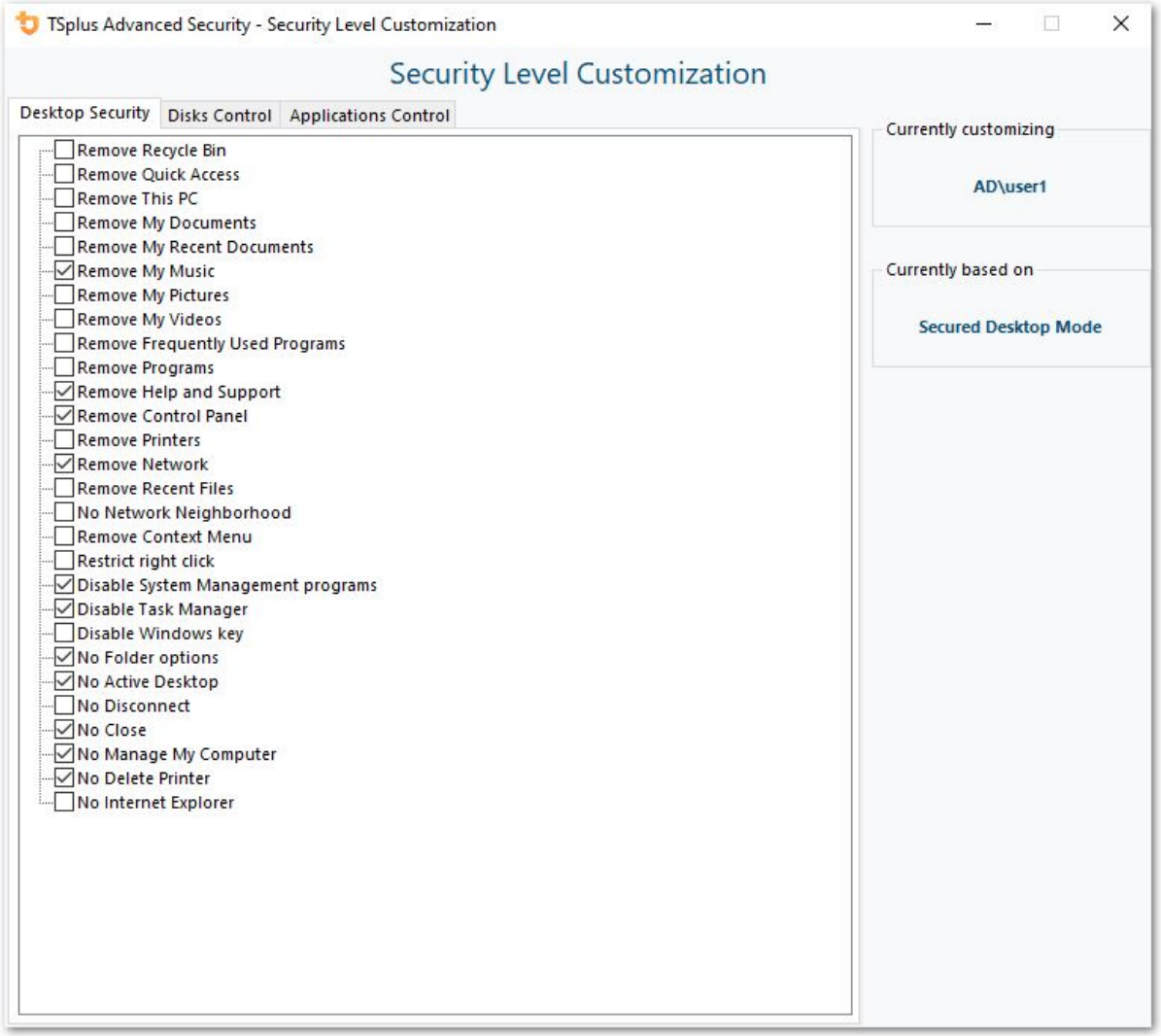




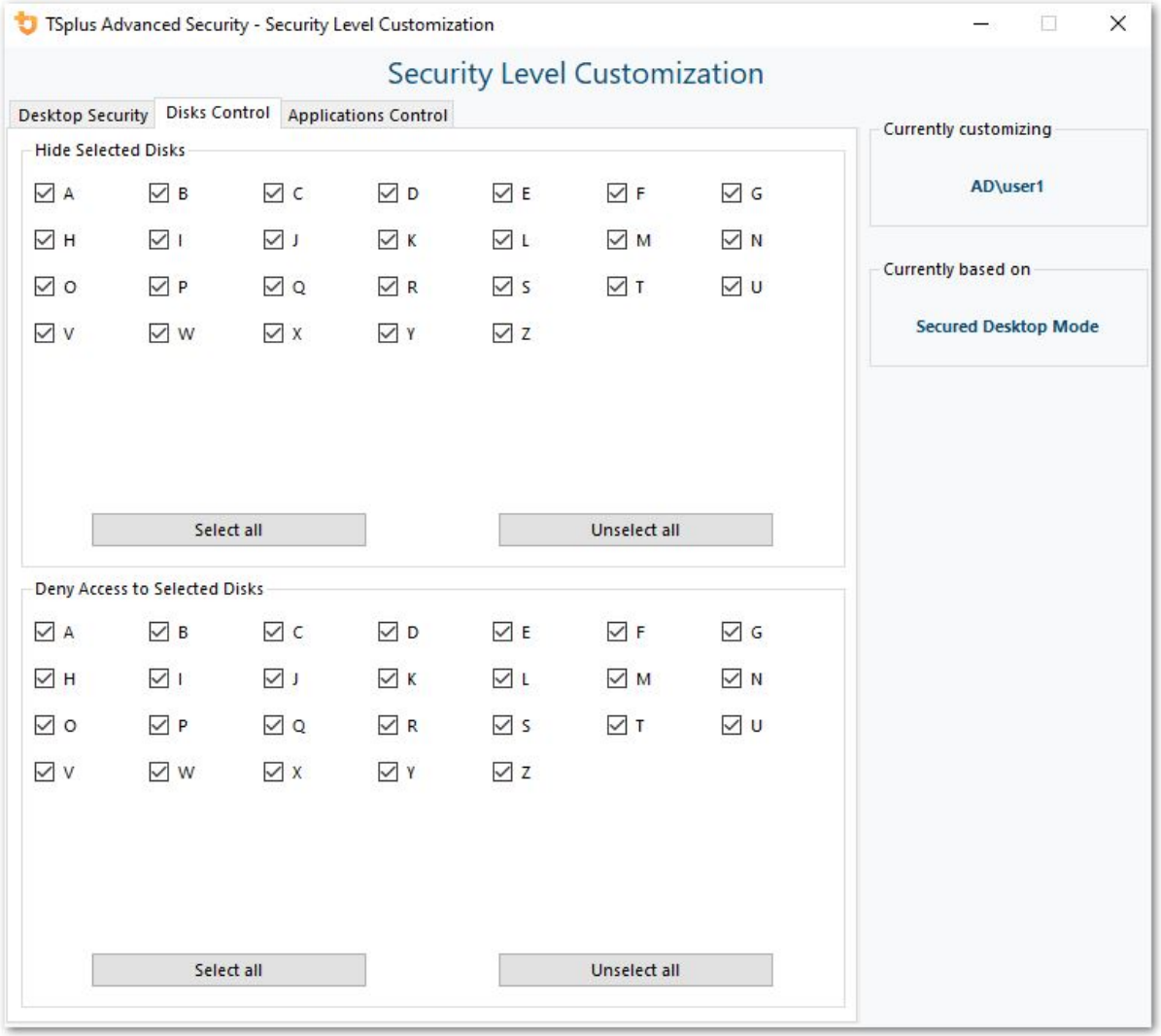
Personalizzazione

In qualsiasi modalità, hai la possibilità di personalizzare la sicurezza su tre livelli:

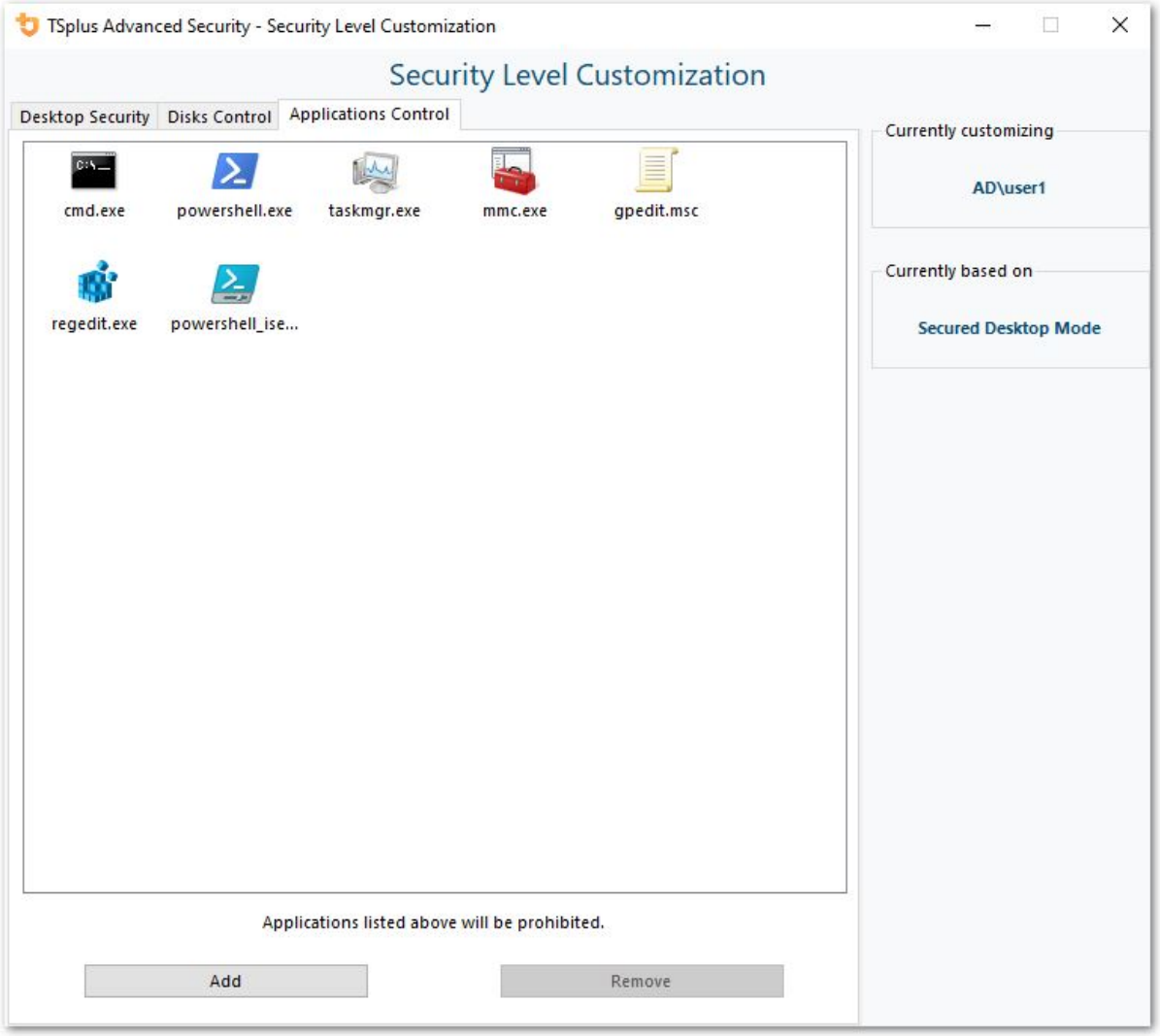
Sicurezza del Desktop:



Controllo dei dischi:



Controllo delle applicazioni:



Priorità delle regole per utenti/gruppi

Quando un utente apre una nuova sessione sul server:

1. Se questo utente ha un Livello di Sicurezza direttamente definito per sé, allora questo Livello di Sicurezza è applicato.
2. Se questo utente non ha un Livello di Sicurezza direttamente definito per sé, allora TSplus Advanced Security caricherà eventuali impostazioni di Livello di Sicurezza esistenti per tutti i gruppi di questo utente e manterrà le regole più permissive.

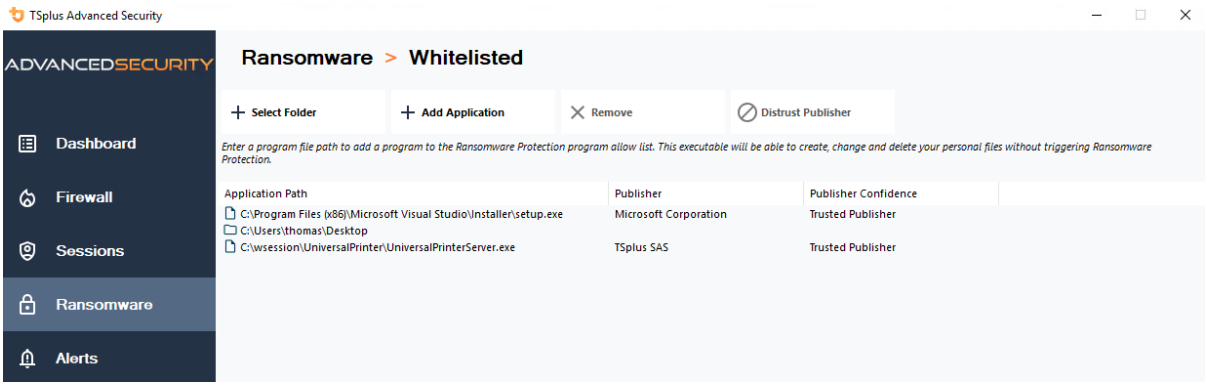
Ad esempio, se un primo gruppo ha una regola per rimuovere l'icona del Cestino dal desktop, ma questa regola è disabilitata per un secondo gruppo, allora l'utente avrà l'icona del Cestino sul suo desktop. Le stesse regole di priorità si applicheranno a ogni regola personalizzata (Sicurezza del Desktop, Controllo dei Dischi e Controllo delle Applicazioni) così come per il Livello di Sicurezza principale (la Modalità Windows è considerata più permissiva rispetto alla Modalità Desktop Sicuro, che è considerata più permissiva rispetto alla Modalità Chiosco).

N.B : Per disabilitare il clic destro ovunque, è necessario selezionare le seguenti due opzioni:

- Limita il clic destro
- Rimuovi il menu di contesto

Impostazioni - Elenco dei programmi consentiti

Sul **Scheda Programmi** puoi aggiungere programmi all'elenco dei programmi consentiti, che non verranno controllati dalla Protezione Ransomware di TSplus Advanced Security Per impostazione predefinita, tutti i programmi Microsoft sono autorizzati.



Clicca sul pulsante "Aggiungi Applicazione" per aggiungere un programma. Puoi anche rimuoverli selezionando l'applicazione(i) e cliccando sul pulsante Rimuovi Applicazione(i).

Impostazioni - Elenco autorizzato utenti

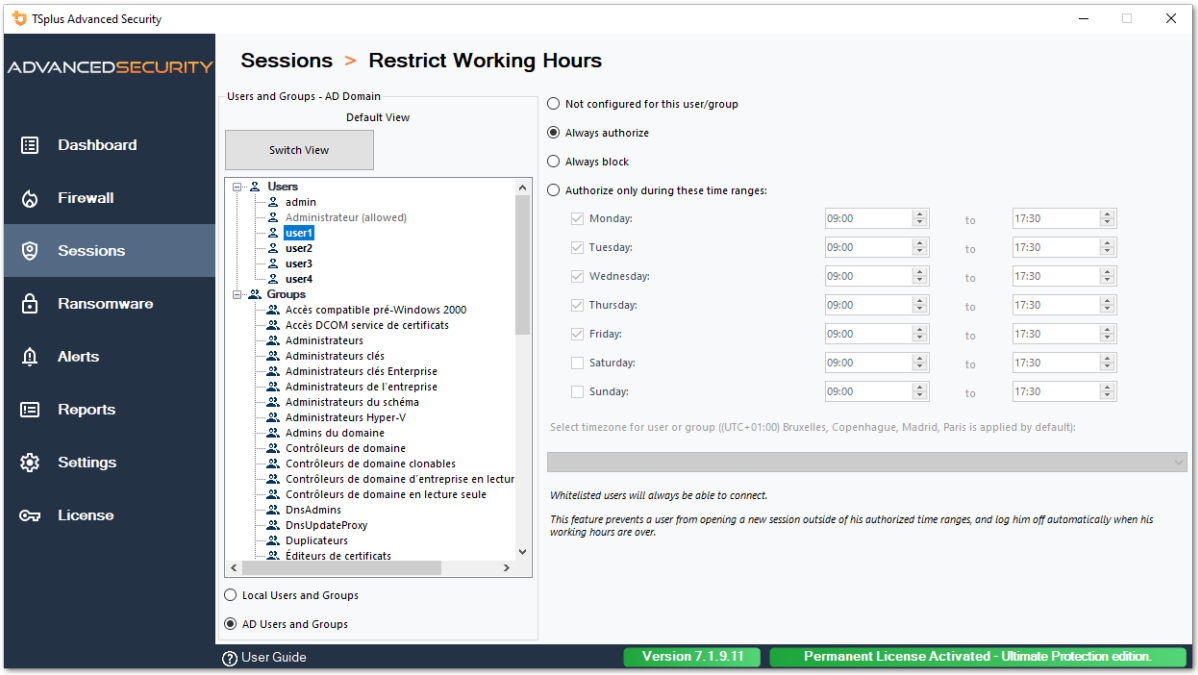
Visualizzazione Avanzata

Con la visualizzazione avanzata, aggiungi e gestisci utenti e gruppi da tutti i domini accessibili.

Puoi passare dalla visualizzazione predefinita alla visualizzazione avanzata utilizzando il pulsante "Cambia visualizzazione".

La vista avanzata viene utilizzata per visualizzare e gestire tutti gli utenti e i gruppi configurati attualmente. Consente inoltre di aggiungere nuovi utenti e gruppi all'elenco per configurarli, utilizzando il selettore di ricerca AD di Windows. Puoi farlo facendo clic sul pulsante "Aggiungi utente/gruppo". Sarai quindi in grado di aggiungere qualsiasi utente disponibile da qualsiasi dominio accessibile dal tuo server.

La Vista Avanzata è disponibile sulle funzionalità Permessi, Orari di Lavoro, Desktop Sicuri. Esempio:

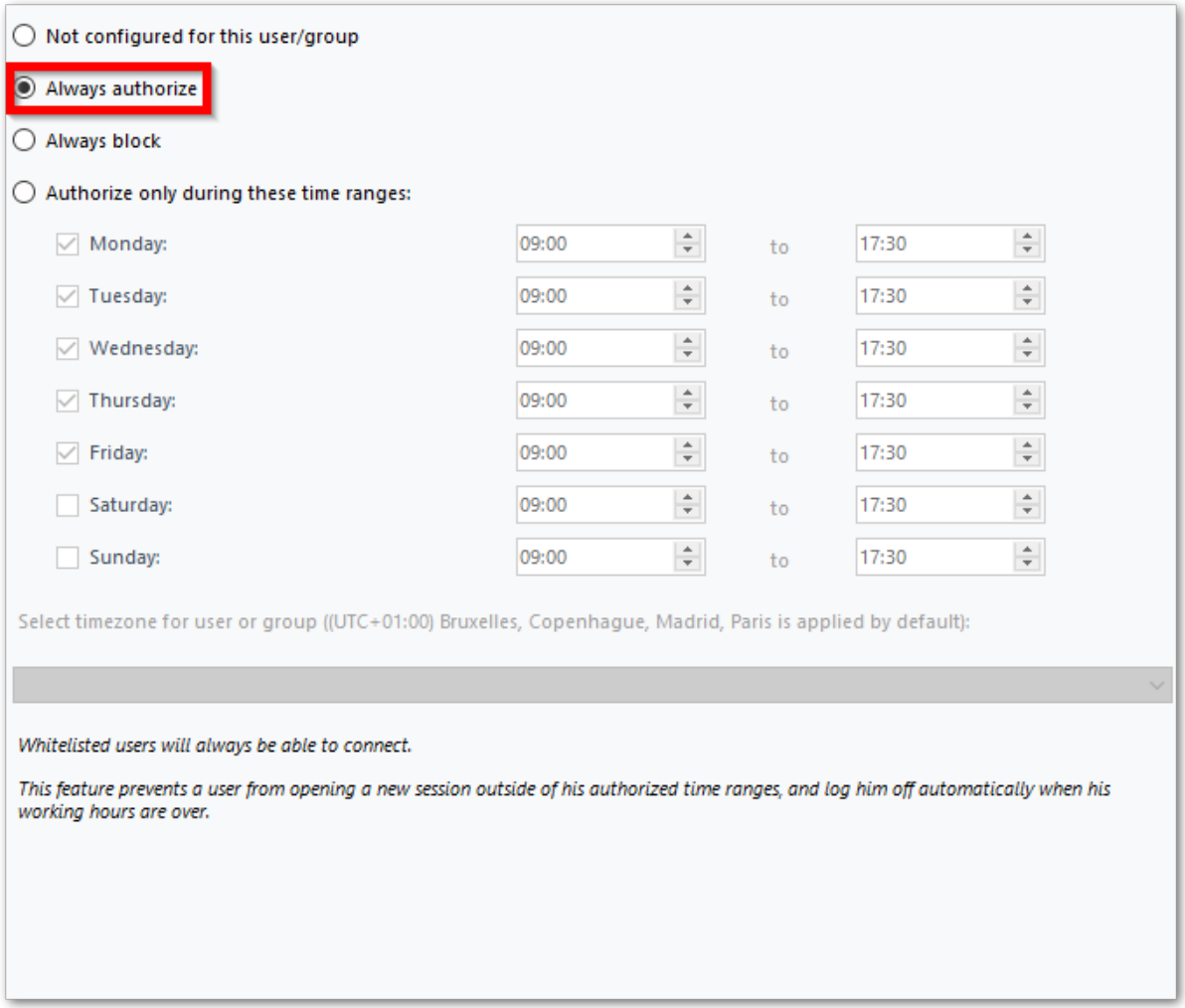


Il **Whitelist degli utenti** la scheda offre all'Amministratore la possibilità di aggiungere/

rimuovere utenti dalla whitelist .

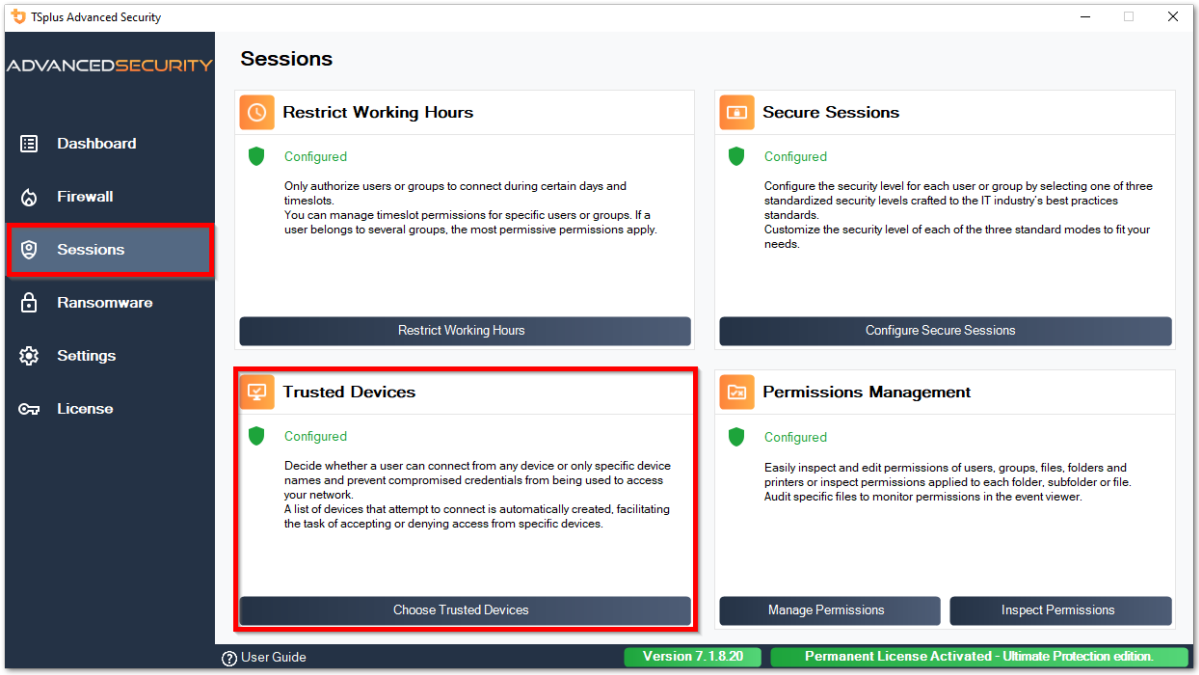
Gli utenti nella whitelist sono ignorati da TSplus Advanced Security e le loro impostazioni non verranno applicate.

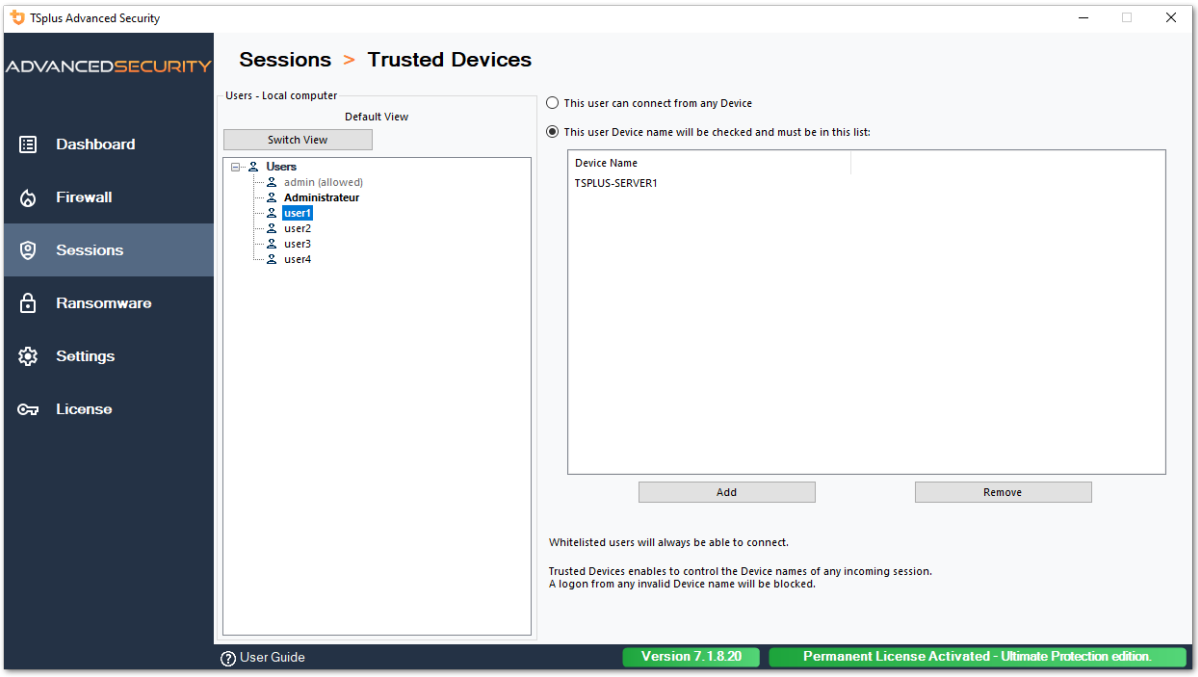
L'utente che ha installato TSplus Advanced Security viene automaticamente aggiunto alla whitelist:



Dispositivi affidabili

Dispositivi fidati consente di controllare i dispositivi degli utenti permettendo a ciascun utente di utilizzare solo uno o più dispositivi specifici, che verranno verificati in ogni sessione in arrivo. Un accesso da qualsiasi nome di dispositivo non valido sarà bloccato.





In questo esempio, **User1** utilizzerà il nome del dispositivo **TSPLUS-SERVER1** solo.

Compilazione automatica del campo nome dispositivo

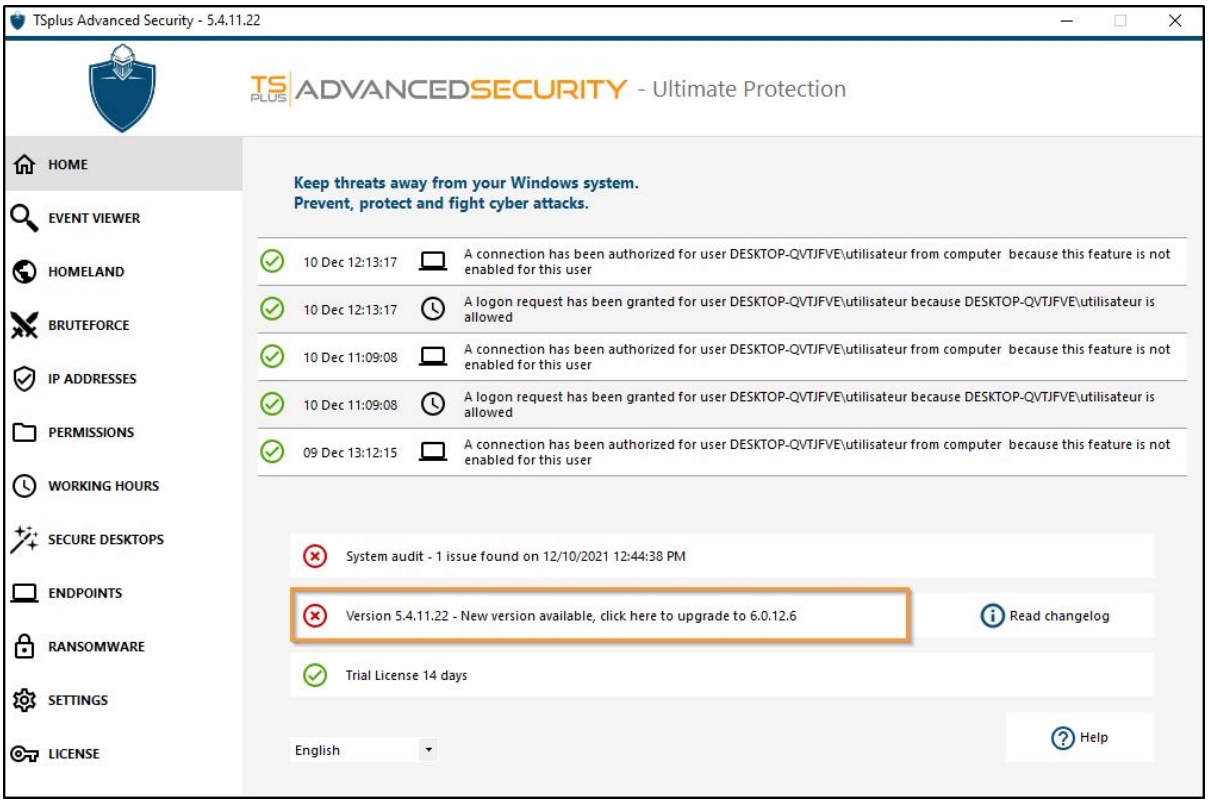
Potresti notare che il campo Nome dispositivo è già compilato con un nome dispositivo per alcuni utenti. Per aiutare l'amministratore, TSplus Advanced Security salverà automaticamente il nome dell'ultimo dispositivo utilizzato per connettersi al server da parte di qualsiasi utente che non ha abilitato la funzione Dispositivi attendibili. Dopo un giorno lavorativo, il nome del dispositivo della maggior parte degli utenti sarà conosciuto da advanced-security, consentendoti così di abilitare rapidamente la funzione di Protezione degli endpoint senza dover controllare il nome della workstation di ogni utente.

Nota Dispositivi fidati non è compatibile con le connessioni HTML5.

Aggiornamento TSplus Advanced Security

Controlla le nostre correzioni e miglioramenti facendo clic su Registro delle modifiche

Aggiornare TSplus Advanced Security è facile e può essere fatto cliccando sulla relativa piastrella, dalla Homepage:



Poi, TSplus Advanced Security scarica e applica l'aggiornamento.

Nota: i tuoi dati e impostazioni vengono sempre salvati prima di un aggiornamento e possono essere trovati nella directory “archivi”, nella cartella di installazione di TSplus Advanced Security. Vedi Esegui il backup e ripristina i tuoi dati e impostazioni

Limitare l'orario di lavoro

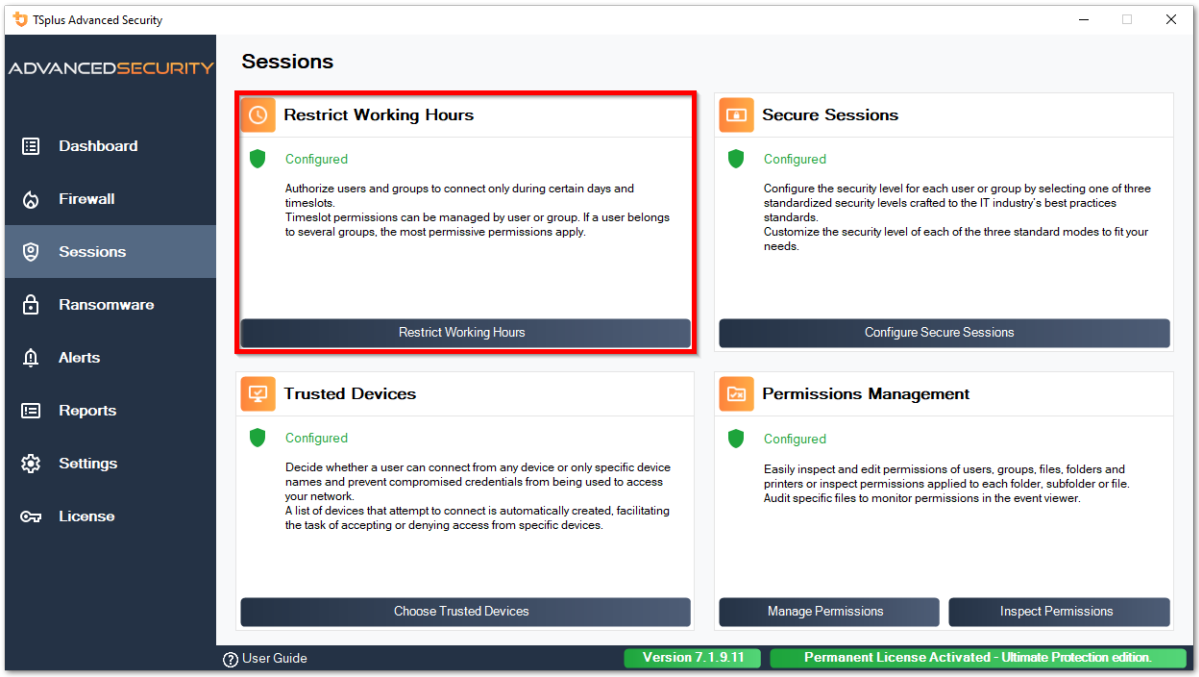
Puoi configurare le restrizioni sugli orari di lavoro per utente o per gruppo.

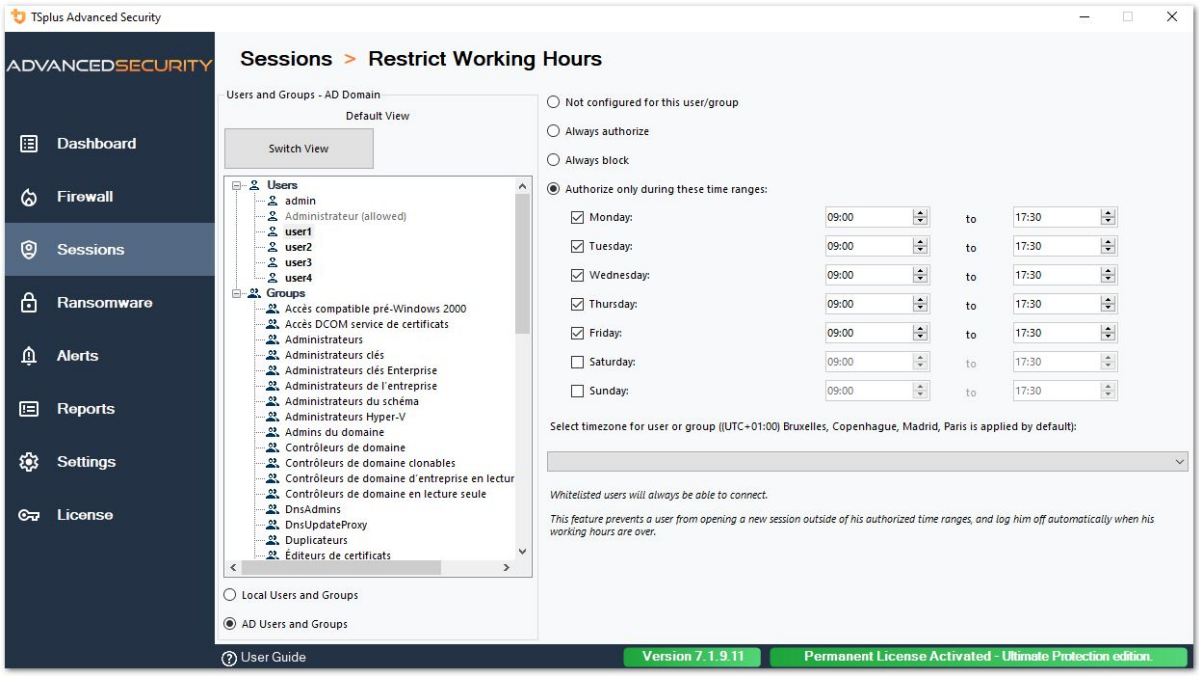
Scegli la restrizione di tua scelta:

- Autorizza sempre l'accesso a questo utente/gruppo
- Blocca sempre l'accesso di questo utente/gruppo

o Autorizza solo durante intervalli di tempo specifici.

Puoi configurarlo giorno per giorno e selezionare l'intervallo di tempo di tua preferenza:





È possibile selezionare un fuso orario specifico a seconda della posizione dell'ufficio dell'utente.

Viene effettuata una disconnessione automatica al termine dell'orario di lavoro configurato.

È possibile pianificare un messaggio di avviso prima che l'utente venga disconnesso da Impostazioni > Avanzate > Orari di lavoro .

###Priorità delle regole per utenti/gruppi

Quando un utente apre una nuova sessione sul server:

1. se questo utente ha restrizioni di Working Hours direttamente definite per sé stesso, allora queste regole sono applicate.

2. se questo utente non ha restrizioni di Working Hours direttamente definite per sé, allora TSplus Advanced Security caricherà eventuali restrizioni di Working Hours esistenti per tutti i gruppi di questo utente e manterrà le regole più permissive. Ad esempio, se un primo gruppo ha una regola per bloccare la connessione il lunedì, un secondo gruppo ha una regola per autorizzare la connessione il lunedì dalle 9:00 alle 17:00 e un terzo gruppo ha una regola per autorizzare la connessione il lunedì dalle 8:00 alle 15:00, allora l'utente sarà in grado di aprire una connessione il lunedì dalle 8:00 alle 17:00.

Attenzione: Questa funzione utilizza l'ora del server. Utilizzare l'ora della workstation dell'utente e/o il fuso orario sarebbe inutile, poiché l'utente dovrebbe solo cambiare il proprio fuso orario per aprire una sessione al di fuori delle sue ore autorizzate.