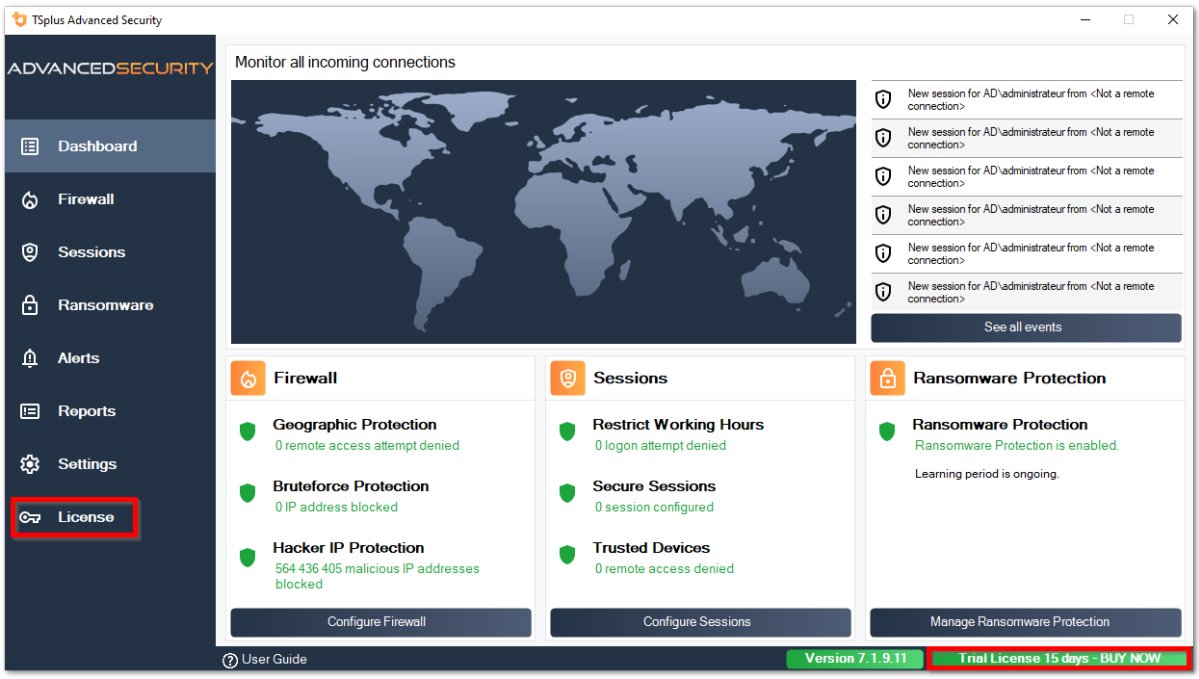
TSplus Advanced Security - Aktivierung Ihrer Lizenz

Schritt 1: Aktivierung Ihrer Lizenz aus dem Lite-Modus

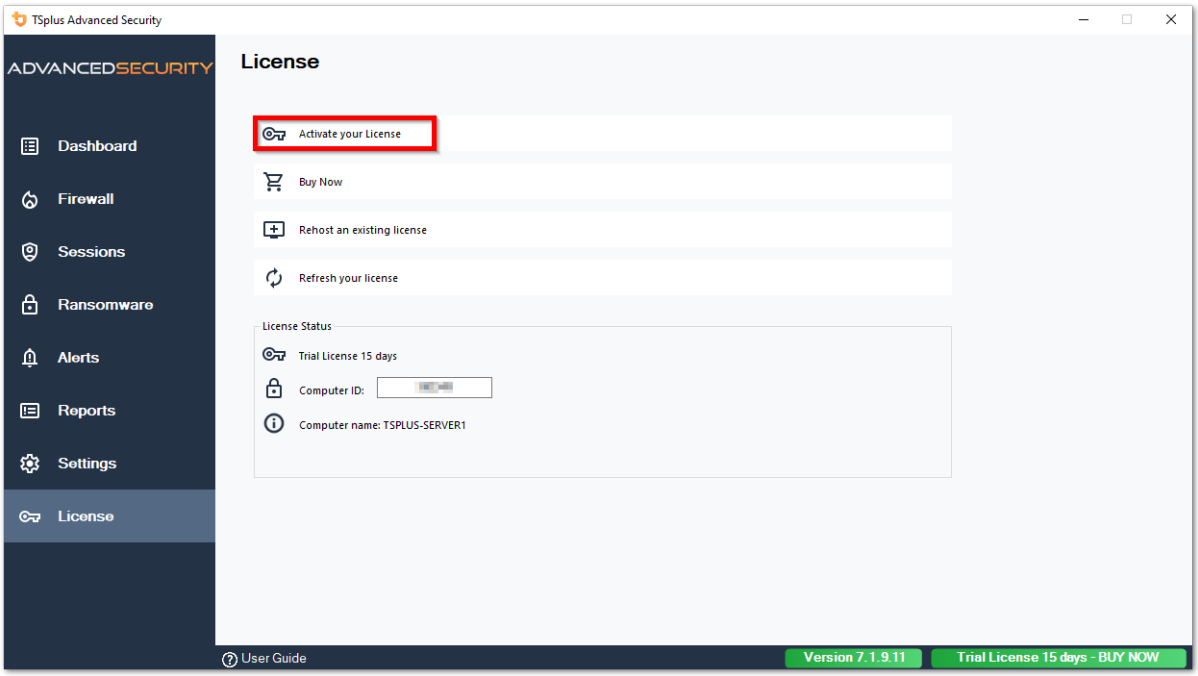
Klicken Sie auf die Schaltfläche „Testlizenz“, um eine Lizenz zu erwerben, oder auf die Registerkarte Lizenz, wenn Sie bereits eine Lizenz und einen Aktivierungsschlüssel haben.



Dann klicken Sie auf die Schaltfläche „Ihre Lizenz aktivieren“.

Sie finden Ihren permanenten Aktivierungsschlüssel. **(XXXX-XXXX-XXXX-XXXX)** in unserer Bestellbestätigungs-E-Mail.

Wenn Sie Ihr Abonnement aktivieren möchten, geben Sie bitte Ihren Abonnementschlüssel ein. **S-XXXX-XXXX-XXXX-XXXX** .



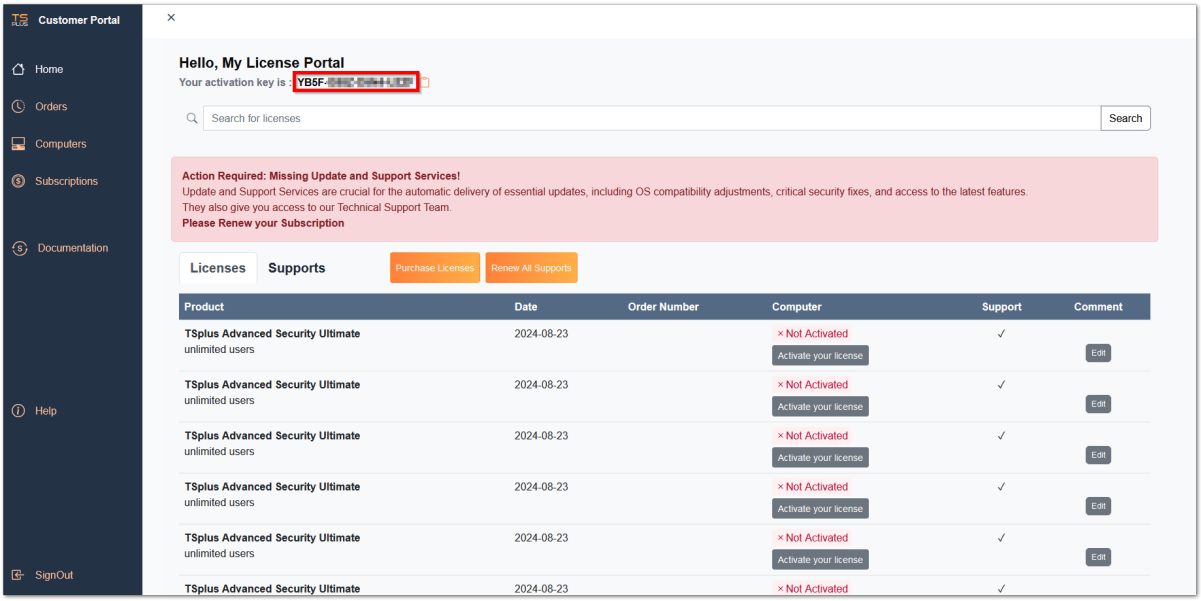
Wenn Sie Ihren Aktivierungsschlüssel nicht kennen, fahren Sie bitte mit Schritt 2 fort. Andernfalls fahren Sie mit Schritt 3 fort.

Schritt 2: Holen Sie sich Ihren Aktivierungsschlüssel vom Lizenzportal

Um Ihren Aktivierungsschlüssel zu erhalten, verbinden Sie sich mit unserem Lizenzportal und geben Sie Ihre E-Mail-Adresse und Ihre Bestellnummer ein:

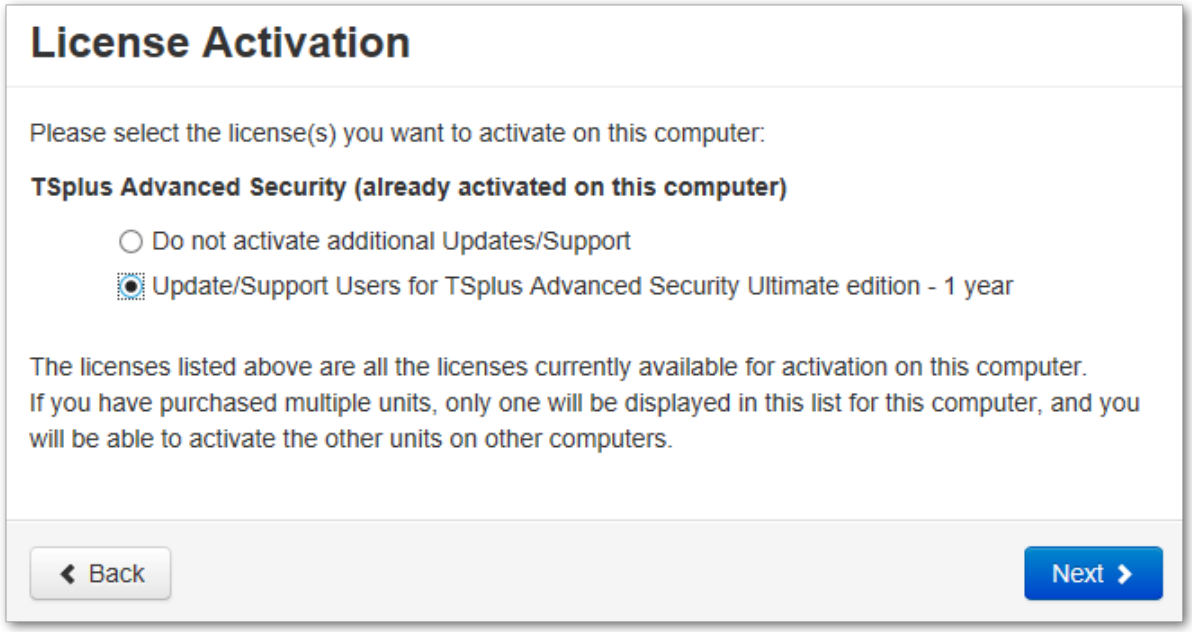
Laden Sie das Benutzerhandbuch für das Kundenportal herunter für weitere Informationen zu Ihrem Kundenportal.

Ihr Aktivierungsschlüssel wird oben im Dashboard angezeigt:

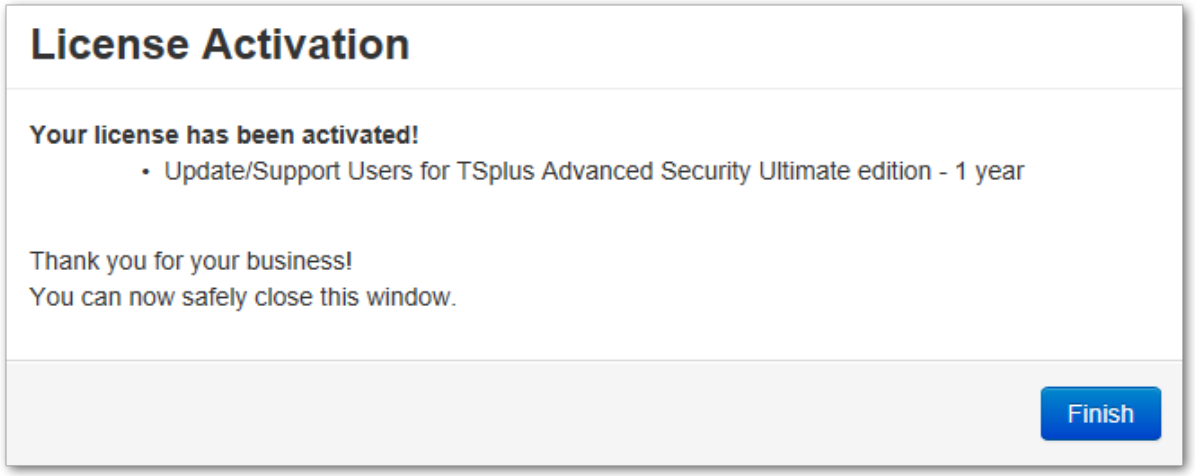


Schritt 3: Wählen Sie die angeforderten Lizenzen sowie Update- und Supportdienste für installierte Produkte aus

Geben Sie Ihren Aktivierungsschlüssel ein und klicken Sie auf „Weiter“.

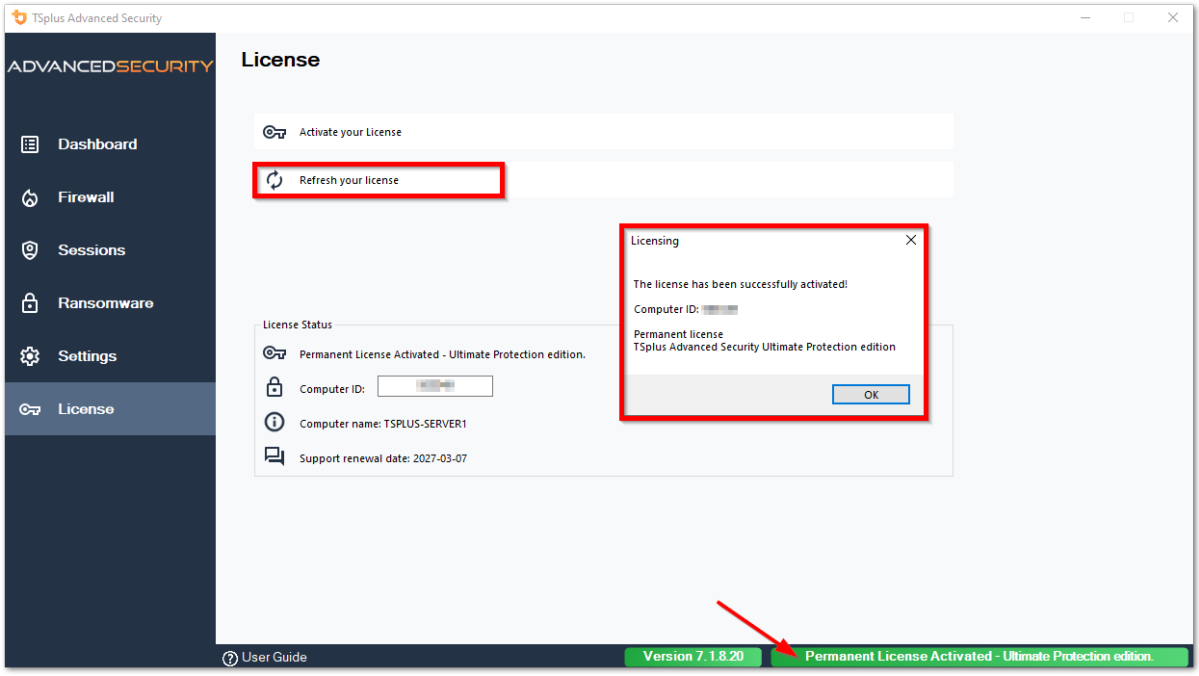


Überprüfen Sie eines oder mehrere Elemente und klicken Sie auf die Schaltfläche „Weiter“. Bitte beachten Sie, dass Sie mehrere Produkte gleichzeitig aktivieren können, indem Sie mehrere Produkte und/oder Support-Abonnements auswählen.



Alle Ihre ausgewählten Produkte und Support-Abonnements sind jetzt aktiviert (in diesem Beispiel wurden sowohl TSplus mit Support als auch TSplus Advanced Security gleichzeitig aktiviert).

Aktualisieren Sie Ihren Lizenzstatus, indem Sie auf die entsprechende Schaltfläche klicken.



Aktivierung Ihrer Lizenz (Offline)

Bitte beziehen Sie sich auf das beschriebene Verfahren für TSplus Remote Access: Aktivierung Ihrer TSplus-Lizenz (Offline)

Ihre Lizenz rehosting

Bitte beziehen Sie sich auf das beschriebene Verfahren für TSplus Remote Access: Rehosting Ihrer TSplus-Lizenz

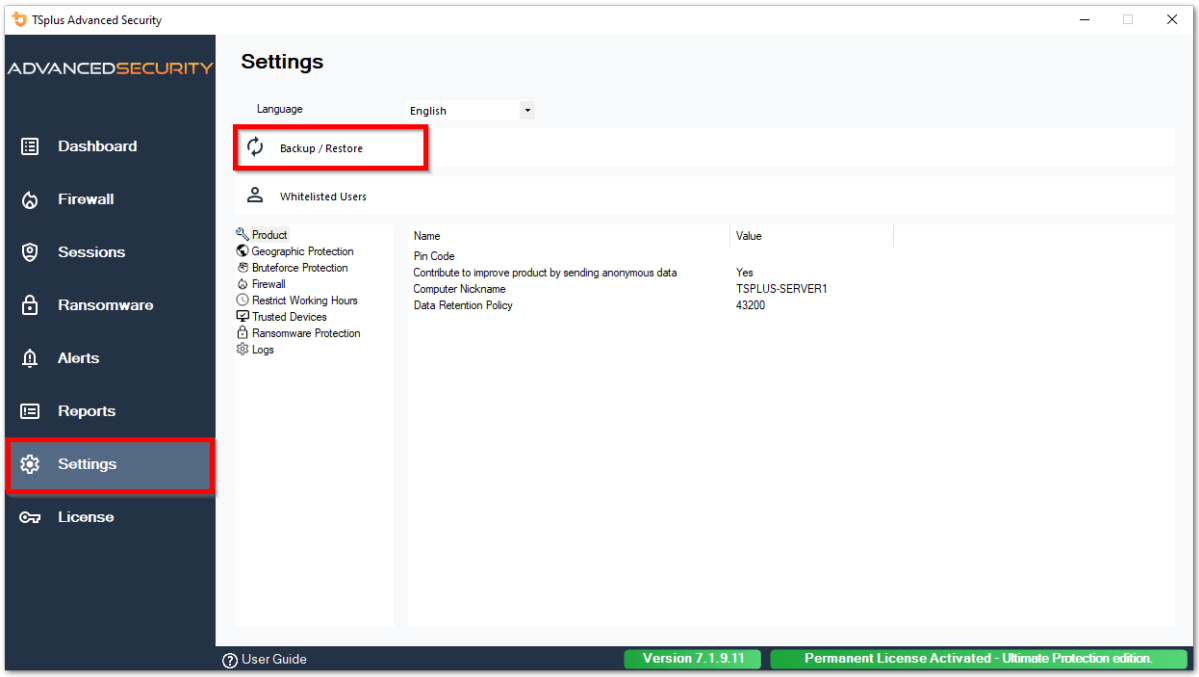
Hinweis: Sie können eine license.lic-Datei im Lizenzportal für TSplus Advanced Security-Versionen herunterladen. Bitte beziehen Sie sich auf die Kundenportal-Benutzerhandbuch für weitere Informationen.

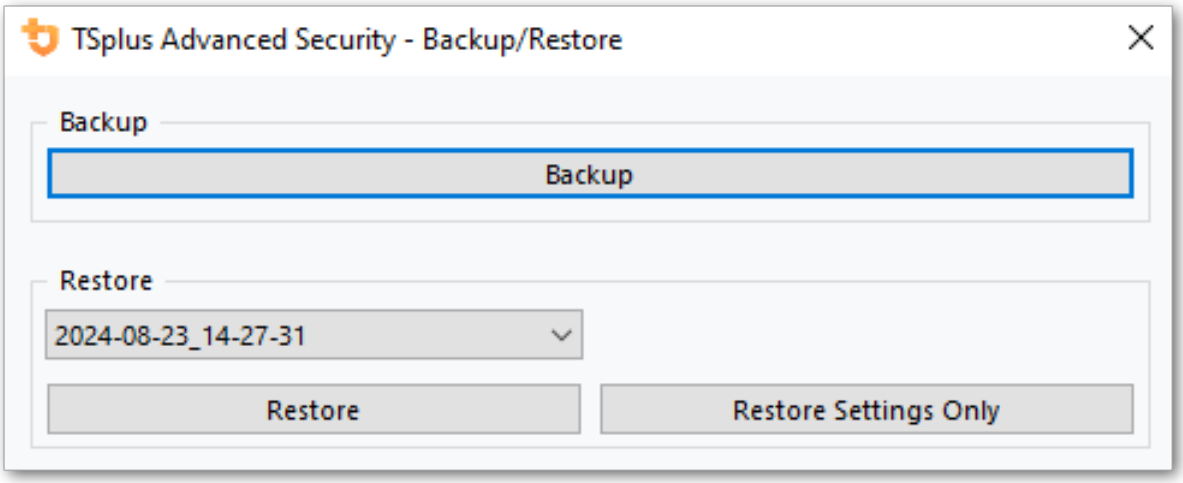
Vielen Dank, dass Sie sich für TSplus Advanced Security entschieden haben!

Erweitert - Backup und Wiederherstellung

Sichern und Wiederherstellen von Daten und Einstellungen

Sie können die Daten und Einstellungen von TSplus Advanced Security sichern oder wiederherstellen, indem Sie auf die Schaltfläche „Backup / Restore“ oben klicken:





Das Backup wird im Ordner gespeichert. **Archive** im Standard im Setup-Verzeichnis von TSplus Advanced Security. **Archive** Der Ordner befindet sich hier: C:\Program Files (x86)\TSplus-Security\archives

Die Verwendung der Befehlszeile zum Sichern und Wiederherstellen

Die Verwendung des Befehls wird unten beschrieben:

- **Sicherung** TSplus-Security.exe /backup [optional path to a directory]

Standardmäßig wird das Backup im Verzeichnis "Archive" erstellt, das sich im Ordner für die Einrichtung von TSplus Advanced Security befindet. Das Backup kann jedoch in einem angegebenen Ordner gespeichert werden. Relative und absolute Pfade sind erlaubt.

- **Wiederherstellen** TSplus-Security.exe /restore [Pfad zu einem Sicherungsverzeichnis]

Das angegebene Backup-Verzeichnis muss einen Daten- und einen Einstellungsordner enthalten, die durch den Befehl /backup erstellt wurden.

Backups konfigurieren

Bitte beachten Sie, dass Sie die folgenden erweiterten Einstellungen in der Registrierung angeben können:

- Das Backup-Verzeichnis kann im Registrierungsschlüssel angegeben werden. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath Standardmäßig wird das Verzeichnis „archives“ des Installationsverzeichnisses von Advanced Security verwendet.

- Die maximale Anzahl der verfügbaren Backups kann im Registrierungsschlüssel festgelegt werden. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives Standardmäßig behält Advanced Security die letzten 3 Sicherungen.

Migrieren Sie Ihre Daten und Einstellungen auf einen anderen Computer

Bitte folgen Sie den untenstehenden Schritten, um Advanced Security von Computer A auf Computer B zu migrieren:

1. Auf Computer A klicken Sie bitte auf die Schaltfläche Backup, um ein neues Backup zu erstellen. Einstellungen und Daten werden im Verzeichnis Archive gespeichert, das sich im Verzeichnis der Advanced Security-Einstellungen befindet (typischerweise C:\Program Files (x86)\TSplus-Security\archives).

2. Kopieren Sie den neu erstellten Sicherungsordner (z. B. benannt backup-2019-09-11_14-37-31), einschließlich aller Inhalte, vom Archivverzeichnis auf Computer A in das Archivverzeichnis auf Computer B.

3. Auf Computer B, im Fenster Backup / Wiederherstellung, im Abschnitt „Wiederherstellen“, wählen Sie den entsprechenden Backup-Namen aus, der wiederhergestellt werden soll.

4. Dann klicken Sie auf Nur Einstellungen wiederherstellen, um die Einstellungen wiederherzustellen. Alternativ können Sie auf Wiederherstellen klicken, um alle Daten und Einstellungen wiederherzustellen, was für eine Migration nicht empfohlen wird, aber nützlich ist, um die Advanced Security auf Computer A wiederherzustellen.

5. Bitte warten Sie maximal 2 Minuten, bis die Einstellungen von den Funktionen der erweiterten Sicherheit neu geladen werden.

Datenbank

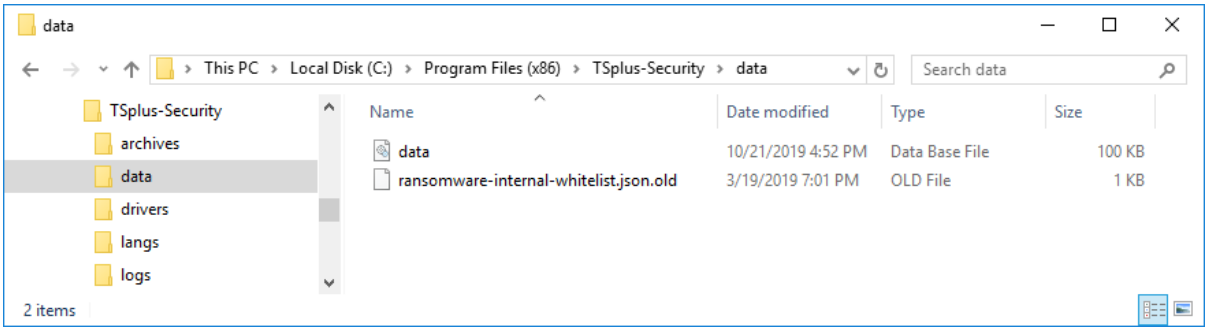
Eine Datenbank speichert Ereignisse, IP-Adressen, Berichte über Ransomware-Angriffe und Programme-Whitelists.

Diese Datenbank wird gespeichert in **Daten** Ordner, der sich im Installationsverzeichnis von

TSplus Advanced Security befindet.

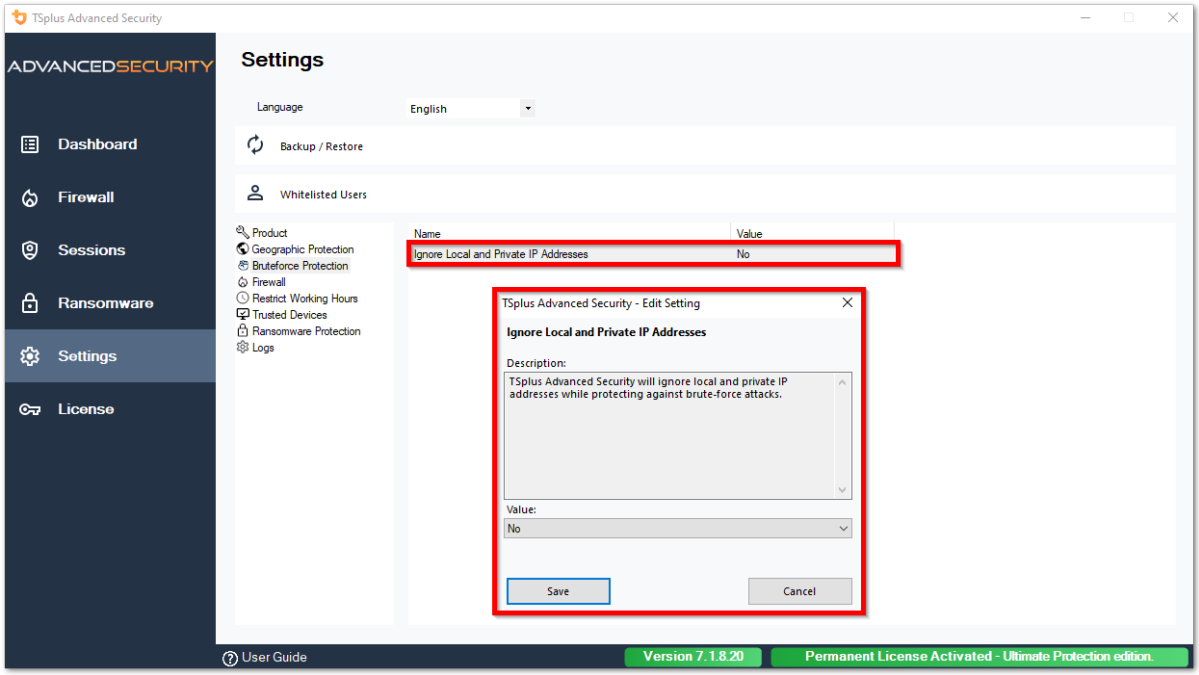
- Advanced Security ab Version 5 und vor Version 5.3.10.6 verwendet ein LiteDB-Datenbank-Engine .

- Advanced Security über Version 5.3.10.6 verwendet eine SQLite-Datenbank-Engine .



Erweiterte - Brute-Force-Schutz

Die **Bruteforce-Schutz** Tab ermöglicht es Ihnen, zu Ignorieren Sie lokale und private IP-Adressen wenn Sie möchten, indem Sie den Standardwert von „Nein“ auf „Ja“ ändern.

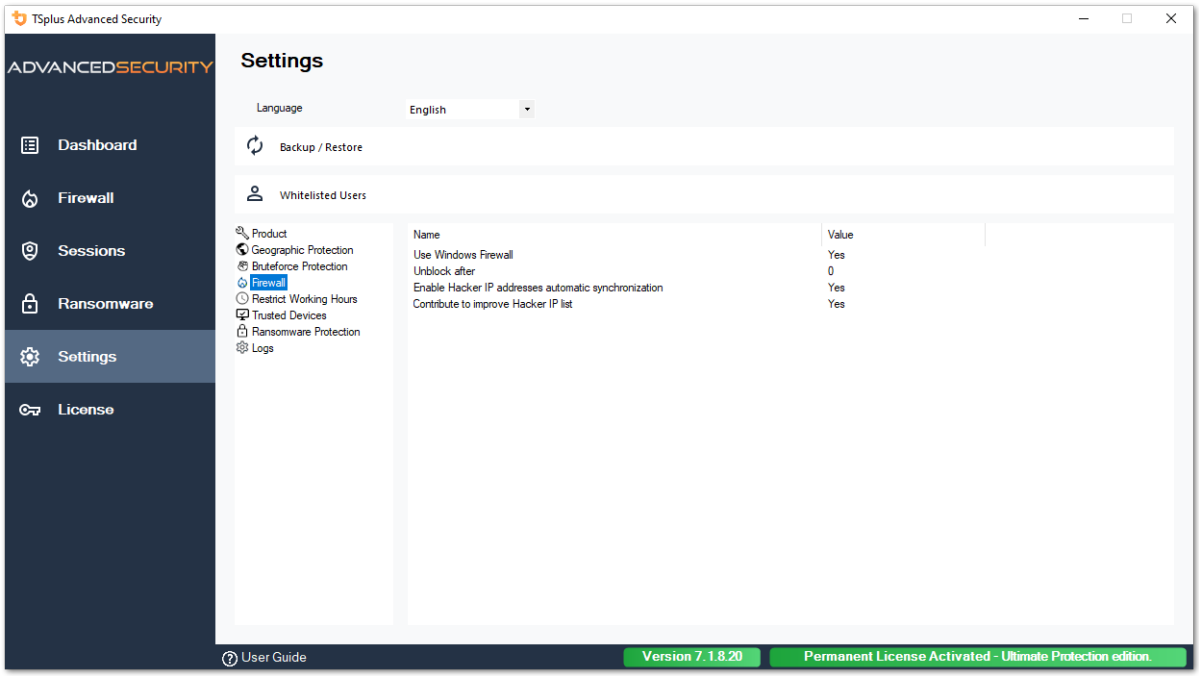


Erweitert - Firewall

Die **Firewall** Tab ermöglicht es Ihnen, die **Windows-Firewall oder deaktivieren Sie sie zugunsten der integrierten Firewall von TSplus Advanced Security** .

Seit Version 4.4 ist eine integrierte Firewall in TSplus Advanced Security enthalten.

Als allgemeine Anleitung, wenn die Windows-Firewall auf Ihrem Server aktiviert ist, sollten Sie diese verwenden, um die Regeln von TSplus Advanced Security (Standard) durchzusetzen. Wenn Sie eine andere Firewall installiert haben, müssen Sie die integrierte Firewall von TSplus Advanced Security aktivieren.



Windows-Firewall verwenden Um die integrierte Firewall zu aktivieren, gehen Sie zu Einstellungen > Erweitert > Produkt > Windows-Firewall verwenden und setzen Sie den Wert auf: Nein. Wenn Ja, werden die störenden IP-Adressen mit der Windows-Firewall blockiert. Andernfalls wird die TSplus Advanced Security-Firewall verwendet.

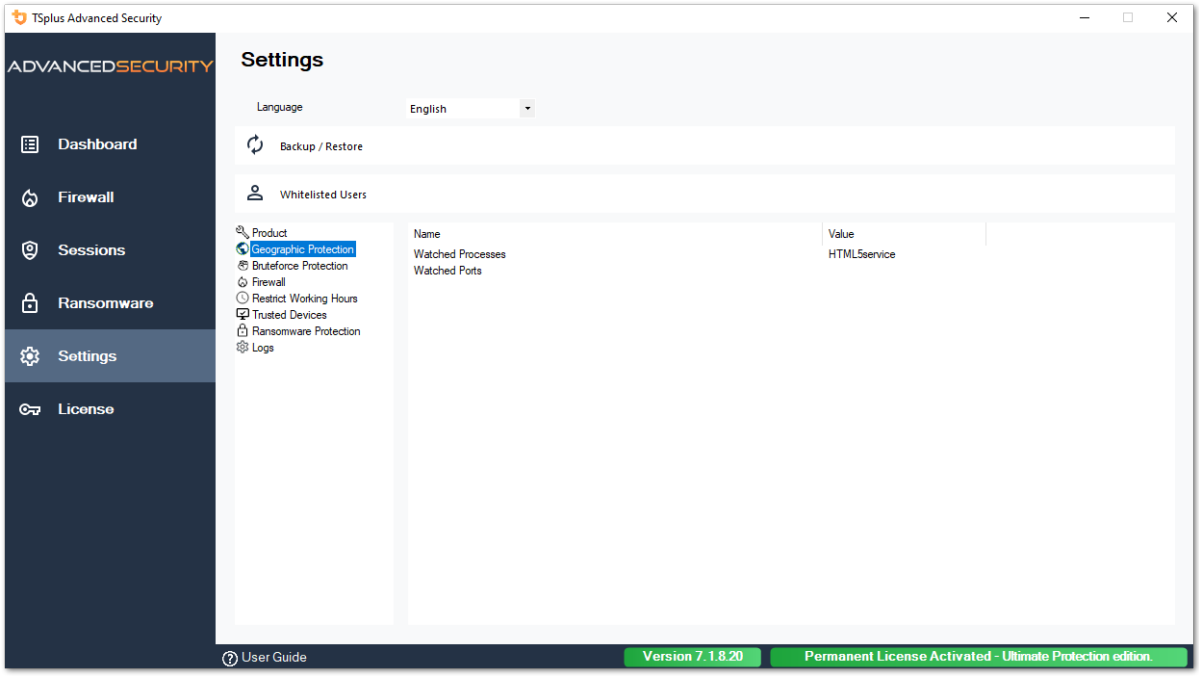
Unblock nach Ändern Sie diese Einstellung, um IP-Adressen nach einer bestimmten Zeit (in Minuten) automatisch zu entsperren. Der Standardwert ist 0, wodurch diese Funktion deaktiviert wird. Wert: 0

Hacker-IP-Adressen automatische Synchronisierung aktivieren Halten Sie Ihre Maschine gegen bekannte Bedrohungen wie Online-Angriffe, Missbrauch von Online-Diensten, Malware, Botnets und andere elektronische Aktivitäten mit dem Hacker-IP-Schutz geschützt. Ein Abonnement für die Support- und Update-Dienste ist erforderlich. Wert: Ja

Zur Verbesserung der Hacker-IP-Liste beitragen Erlauben Sie TSplus Advanced Security, anonyme Nutzungsstatistiken zu senden, um den Schutz gegen Hacker-IP zu verbessern. Wert: Ja

Erweiterte - Geografische Schutzmaßnahmen

Die **Geografischer Schutz** Tab ermöglicht es Ihnen, Prozesse hinzuzufügen oder zu entfernen, die von der überwacht werden. Geografischer Schutz Funktion.



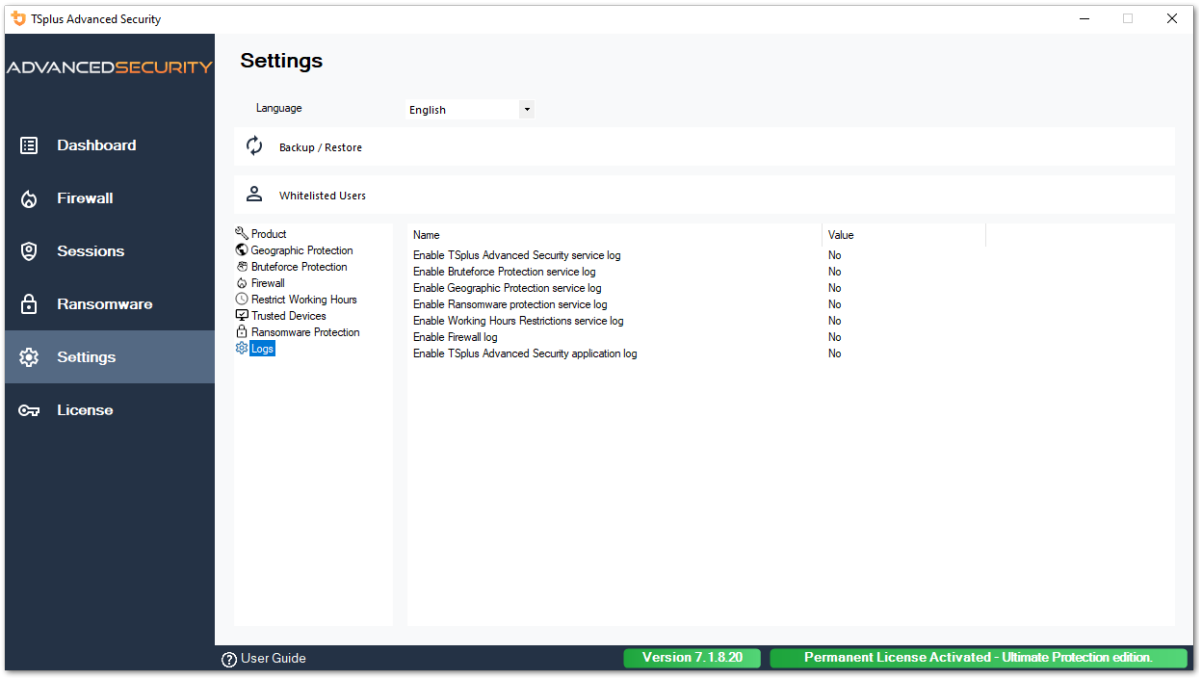
Standardmäßig wird der HTML5-Dienst überwacht.

Die **Beobachtete Ports** Einstellungen ermöglichen es Ihnen, Ports hinzuzufügen, die von der Geografischer Schutz Funktion. Standardmäßig hört Geographic Protection auf die Standardports, die für die Remoteverbindung zu einem Server verwendet werden. Diese Ports umfassen RDP (3389), Telnet (23) und VNC-Ports. Geographic Protection unterstützt die folgenden VNC-Anbieter: Tight VNC, Ultra VNC, Tiger VNC und Real VNC, die in keiner Weise mit TSplus in Verbindung stehen.

Erweiterte - Protokolle

Die **Protokolle** Tab ermöglicht es Ihnen, zu Dienst- und Funktionsprotokolle aktivieren oder deaktivieren Logs exist to find more easily the origin of the errors encountered on TSplus Advanced Security.

Um die Protokolle abzurufen, öffnen Sie einen Explorer und navigieren Sie zu der **Protokolle** Ordner des Installationsverzeichnisses von TSplus Advanced Security. Standardmäßig werden die Protokolle hier gespeichert: **C:\Program Files (x86)\TSplus-Security\logs**



Aktivieren oder deaktivieren TSplus Advanced Security-Dienste und Anwendungsprotokolle , die jeweils den globalen Konfigurationsdienst darstellen, der im Hintergrund läuft, und das Protokoll für die Anwendungsoberfläche.

Sie können auch Protokolle aktivieren, die den jeweiligen Funktionen von TSplus Advanced Security entsprechen:

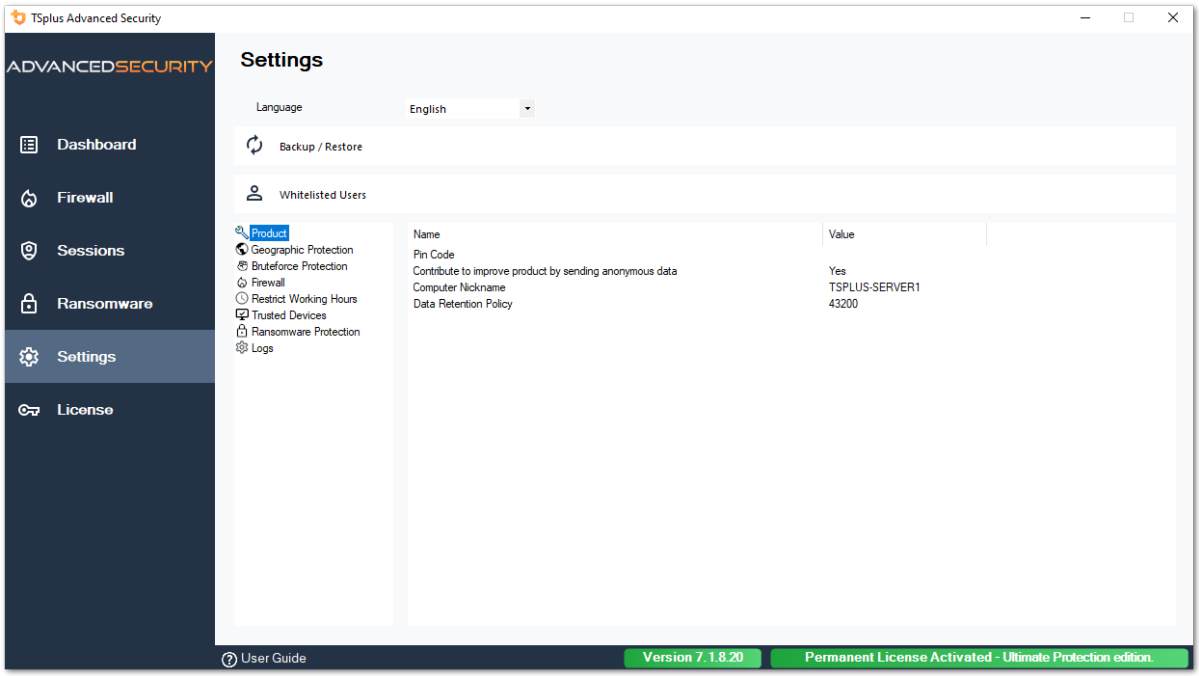
- Dienstleistung
- Bruteforce-Schutz
- Geografischer Schutz

- Ransomware-Schutz
- Arbeitszeiten einschränken
- Firewall..
- Anwendung

Alle Protokolle sind standardmäßig deaktiviert. Protokolle entsprechen verschiedenen Komponenten, unser Support-Team wird Ihnen sagen, welchen Wert Sie je nach aufgetretenem Problem eingeben sollen.

Fortgeschritten - Produkt

Die **Produkt** Tab ermöglicht es Ihnen, zu eine PIN-Code zur Anwendung hinzufügen :



Klicken Sie auf Speichern. Der PIN-Code wird beim nächsten Start der Anwendung benötigt.

Sie können auch **zur Verbesserung des Produkts beitragen** , indem anonyme Daten gesendet werden (standardmäßig aktiviert): JA

Die folgenden Daten werden im Falle eines Ransomware-Angriffs gesammelt:

- Die Version von TSplus Advanced Security.
- Windows-Version.
- Verdächtige Dateipfade, die zum Ransomware-Angriff führen.

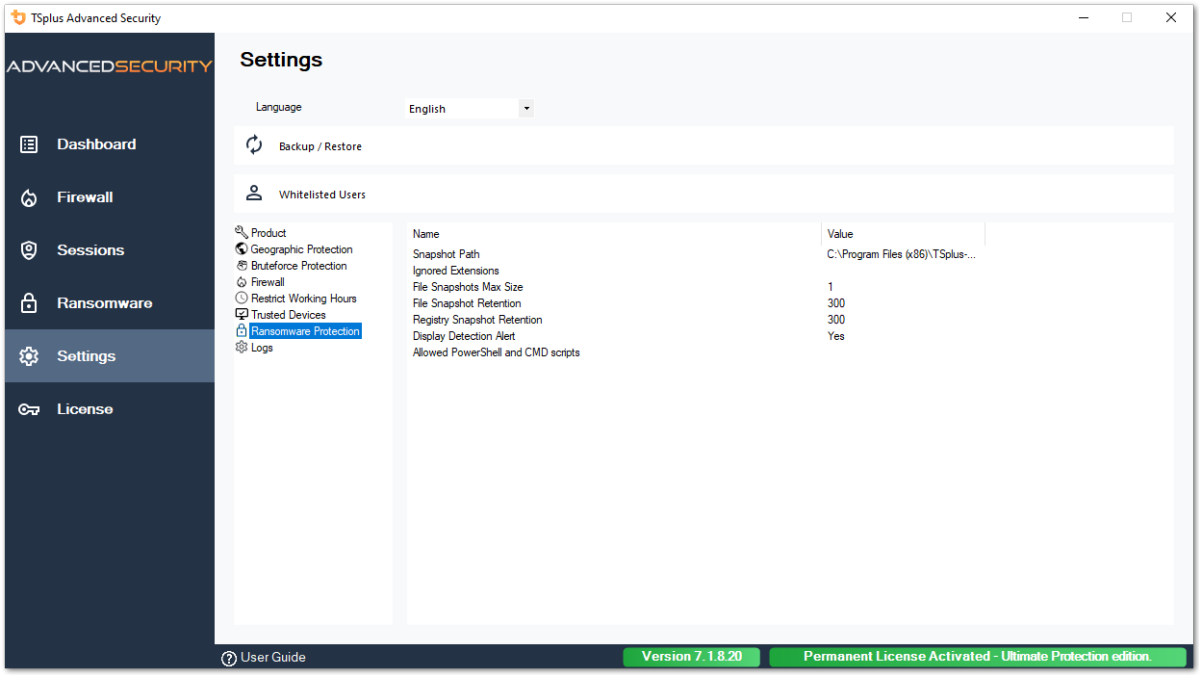
Ändern des **Computer-Spitzname** ist auch möglich.

Die **Datenaufbewahrungsrichtlinie** definiert den Zeitraum, nach dem die Ereignisse von TSplus Advanced Security aus der Datenbank entfernt werden. Ein Backup wird vor jeder Datenbankbereinigung durchgeführt. Diese Richtlinie ist in Minuten definiert. Die

standardmäßige Datenaufbewahrungsrichtlinie beträgt 259.200 Minuten oder 6 Monate.

Erweiterte - Ransomware-Schutz

Die **Ransomware-Schutz** Tab ermöglicht es Ihnen, zu konfigurieren Sie die Snapshot-Eigenschaften und definieren Sie ignorierte Dateierweiterungen für die Ransomware-Schutzfunktion.



Schnappschuss-Pfad Definieren Sie das Verzeichnis, in dem der Ransomware-Schutz Dateischnappschüsse speichert.

Der Standardwert ist: C:\Program Files (x86)\TSplus-Security\snapshots

Ignorierte Erweiterungen Standardmäßig ignoriert der Ransomware-Schutz bekannte Erweiterungen von temporären Dateien für Ransomware-Aktivitäten. Siehe die Liste hier Sie können benutzerdefinierte Erweiterungsnamen im Wertefeld (durch Semikolons getrennt) definieren:

Dateigrößenbeschränkung für Snapshot Dateisnapshots Maximalgröße definiert den maximalen Speicherplatz, der zur Aufbewahrung von Dateisnapshots zulässig ist.

Die Größe wird als Prozentsatz des insgesamt verfügbaren Speicherplatzes auf der Festplatte

angegeben, auf der sich der Snapshot-Pfad befindet.

Dateisnapshot-Aufbewahrung Datei-Snapshot-Aufbewahrung definiert in Sekunden die Aufbewahrungsrichtlinie eines Datei-Snapshots.

Sobald der Aufbewahrungszeitraum abgelaufen ist, wird der Dateisnapshot gelöscht. Standardmäßig 300 Sekunden (d.h. 5 Minuten)

Registrierungs-Snapshot-Aufbewahrung Registry Snapshot Retention definiert in Sekunden die Aufbewahrungsrichtlinie eines Registrierungssnapshots. Nach Ablauf der Aufbewahrungsfrist wird der Registrierungssnapshot gelöscht. Standardmäßig 300 Sekunden (d.h. 5 Minuten)

Anzeigeerkennungswarnung Zeigen Sie ein Warnmeldungsfenster auf dem Desktop des Benutzers an, wenn der Ransomware-Schutz einen Angriff erkannt und gestoppt hat.

Erlaubte PowerShell- und CMD-Skripte Erlaubte PowerShell- und CMD-Skripte listen die vollständigen Dateipfade der PowerShell- und CMD-Skripte auf, die auf dem Computer ausgeführt werden dürfen.

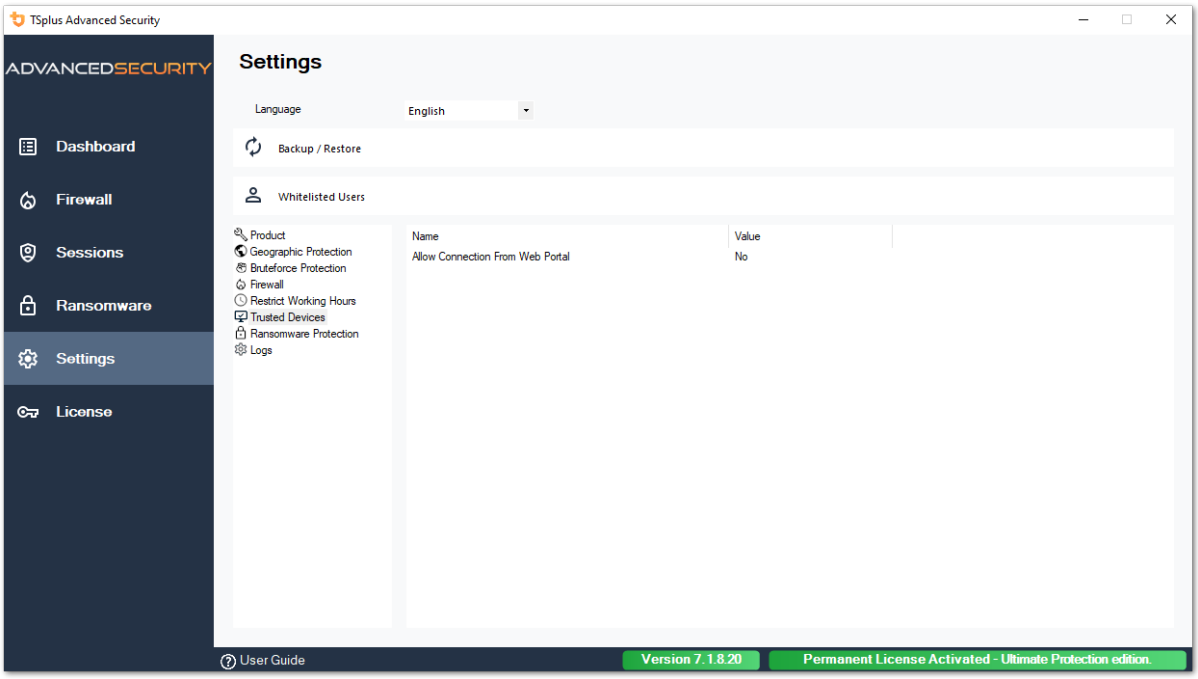
Die Ausführung erlaubter Skripte löst den Ransomware-Schutz nicht aus (durch Semikolons getrennt).

Erweiterte - Vertrauenswürdige Geräte

Die **Vertrauenswürdige Geräte** Tab ermöglicht es Ihnen, Verbindungen vom Webportal von TSplus Remote Access zu aktivieren.

Hinweis :

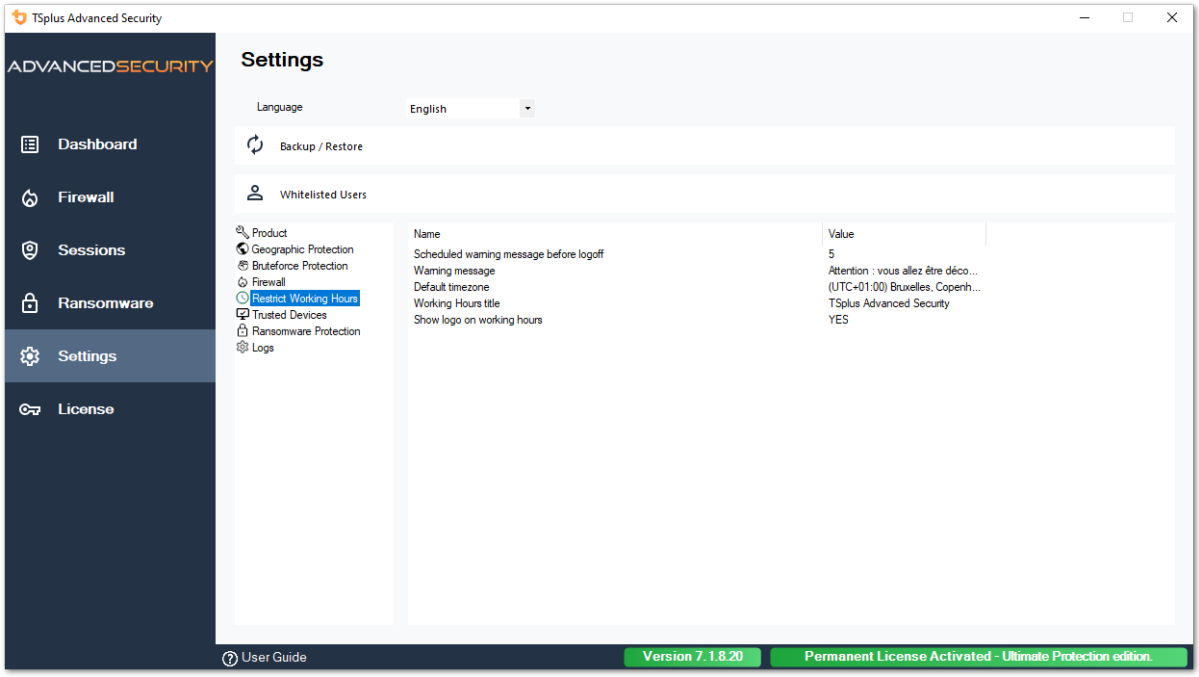
-Trusted Devices ist nicht mit HTML5-Sitzungen kompatibel. -Trusted Devices ist nicht mit iOS / Android-Mobilgeräten kompatibel, da diese ihre echten Hostnamen verbergen. -Der Hostname der Remote-Maschine wird von der Maschine selbst definiert. Die Maschine wird ihn wahrscheinlich gemäß ihrer Konfiguration verbergen oder ändern.



Die vertrauenswürdigen Geräte von TSplus Advanced Security können den Clientnamen nicht auflösen, wenn die Verbindung vom Webportal von TSplus Remote Access initiiert wird. Daher blockieren vertrauenswürdige Geräte standardmäßig alle Verbindungen vom Webportal. Setzen Sie diese Einstellung auf "Ja", um Verbindungen vom Webportal zuzulassen. Bitte beachten Sie, dass diese Aktion die Sicherheit Ihres Servers verringern wird.

Erweiterte - Arbeitszeiten einschränken

Die **Arbeitszeiten einschränken** Tab ermöglicht es Ihnen, zu Planen Sie eine Warnmeldung, bevor der Benutzer abgemeldet wird. .



Warnmeldung Zeitplan Sie können die Anzahl der Minuten konfigurieren, bevor der Benutzer automatisch getrennt wird. Standardmäßig ist es auf 5 Minuten eingestellt.

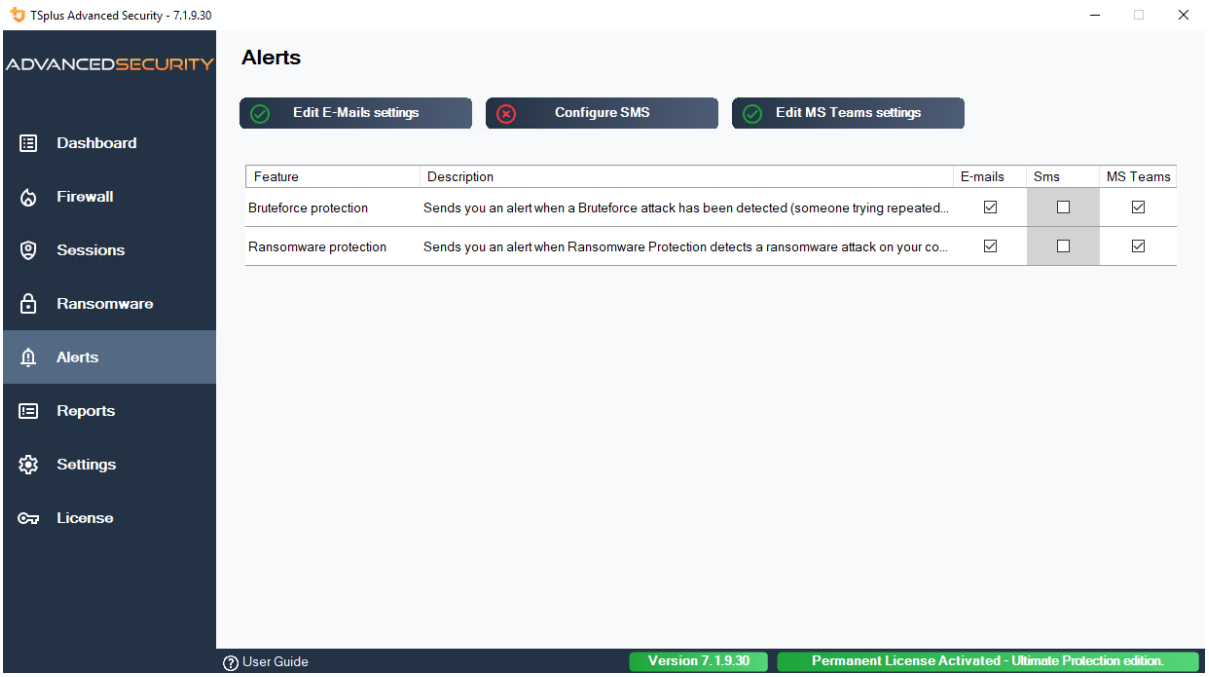
Warnmeldung Eine Warnmeldung kann nach Ihrem Ermessen definiert werden, mit Platzhaltern namens %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% und %ENDINGHOURS%, die jeweils durch die aktuelle Anzahl der Minuten vor dem Schließen der Sitzung, den aktuellen Tag, die aktuellen Arbeitszeiten am Tag sowie die Endzeiten ersetzt werden.

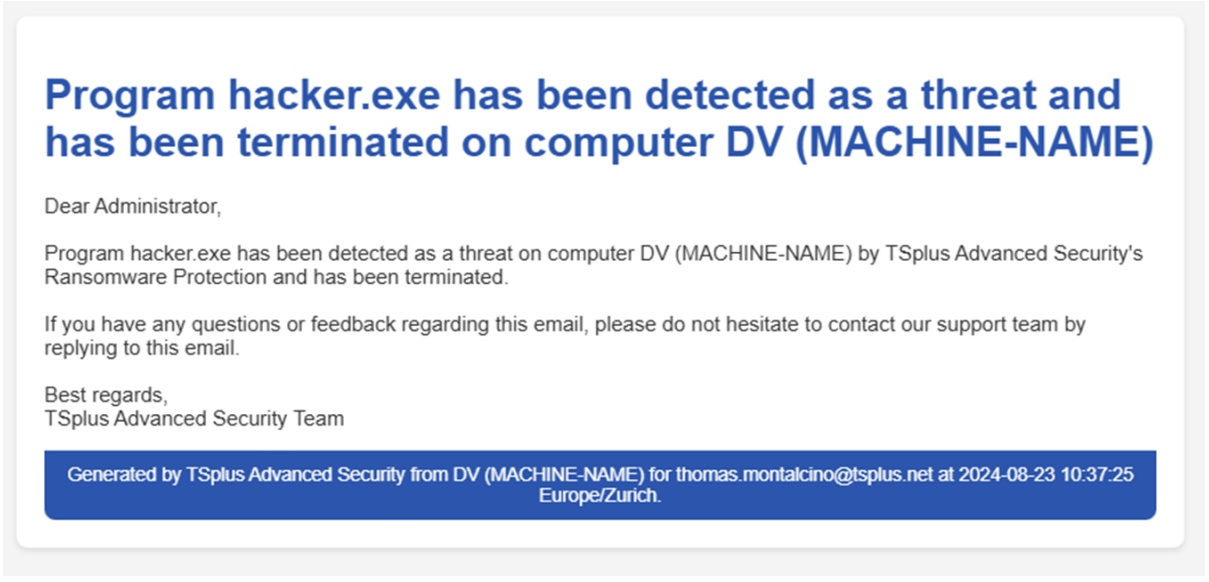
Standardzeitzone des Servers Eine Standardserverzeitzone kann definiert werden, um die Regeln für die Arbeitszeiten entsprechend anzuwenden, indem die entsprechende aus der Dropdown-Liste ausgewählt wird.

Arbeitszeiten Titel Titel des Formulars, das dem Endbenutzer angezeigt wird, wenn seine/ihre Arbeitszeiten enden (Standard: TSplus Advanced Security)

Logo während der Arbeitszeiten anzeigen Wenn auf "ja" gesetzt, wird das Logo in der Form angezeigt, die dem Endbenutzer angezeigt wird, wenn seine/ihre Arbeitszeiten enden (Standard: "ja")

Warnungen





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.

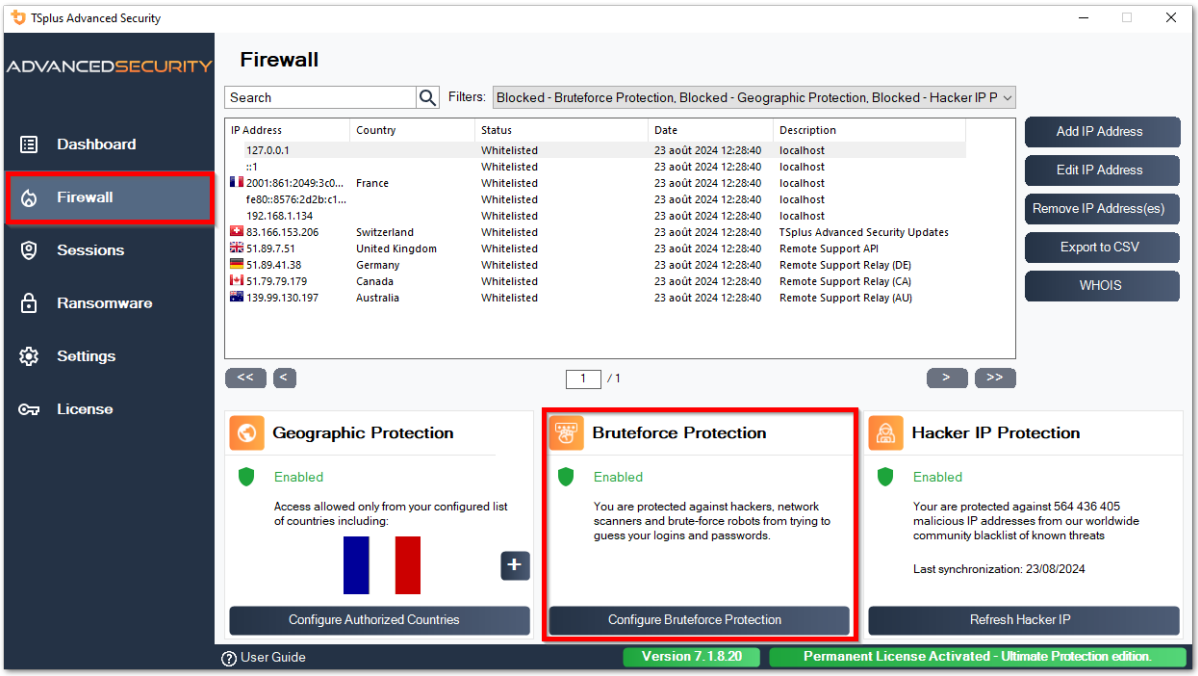
Best regards,
TSplus Advanced Security Team

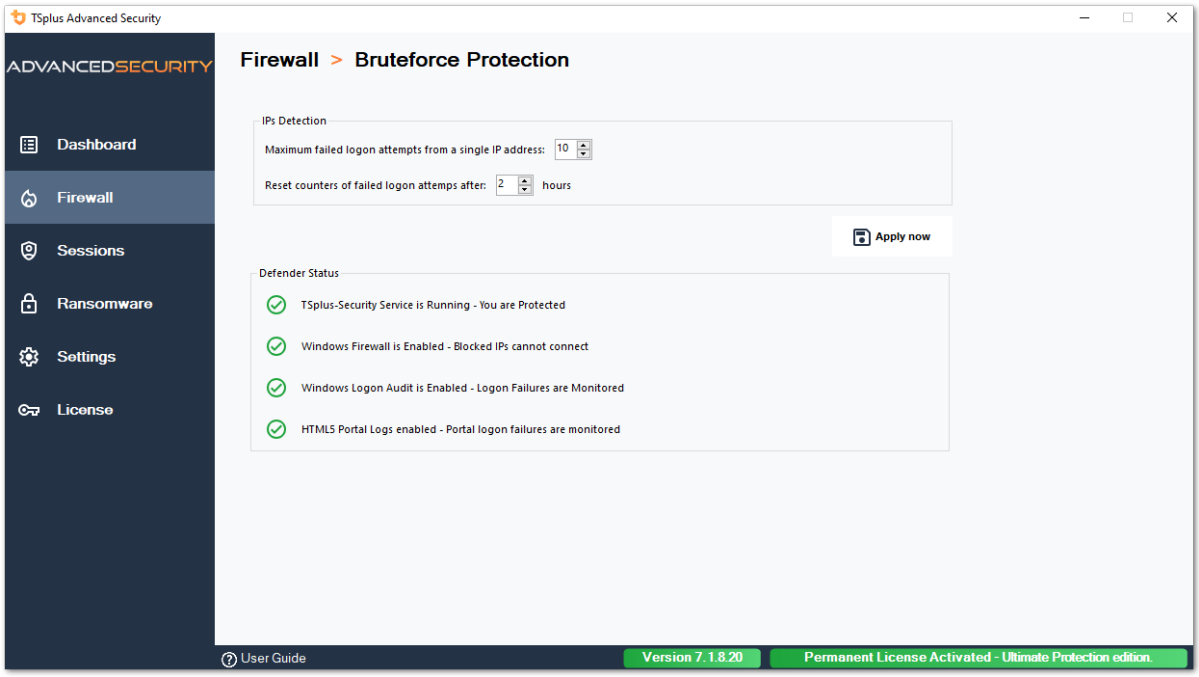
Generated by TSplus Advanced Security from DV (MACHINE-NAME) for thomas.montalcino@tsplus.net at 2024-08-23 10:37:25 Europe/Zurich.

Bruteforce-Schutz

Der Bruteforce-Schutz ermöglicht es Ihnen, Ihren öffentlichen Server vor Hackern, Netzwerkscannern und Brute-Force-Robotern zu schützen, die versuchen, Ihren Administrator-Login und Ihr Passwort zu erraten. Mit aktuellen Logins und Passwortwörterbüchern werden sie automatisch versuchen, sich Hunderte bis Tausende Male pro Minute in Ihren Server einzuloggen.

Mit diesem RDP Defender können Sie fehlgeschlagene Windows-Anmeldeversuche überwachen und die betreffenden IP-Adressen nach mehreren Fehlversuchen automatisch auf die schwarze Liste setzen.





- Sie können die **maximale fehlgeschlagene Anmeldeversuche von einer einzelnen IP-Adresse innerhalb des IPs-Erkennungsblocks** (Standardmäßig beträgt es 10), sowie die Zeit für den Reset der Zähler für fehlgeschlagene Anmeldeversuche (Standardmäßig beträgt es 2 Stunden).

- Am unteren Rand dieses Fensters können Sie die **Status des Verteidigers** wo Sie überprüfen können, ob die Anmeldefehler des HTML5-Webportals, die Windows-Anmeldefehler überwacht werden und ob die Windows-Firewall und der Advanced Security-Dienst aktiviert sind.

In diesem Fall, wie in unserem Beispiel, sind alle Status angekreuzt.

- **Verwalten Sie blockierte IP-Adressen** Sie können es natürlich so konfigurieren, dass es Ihren Bedürfnissen entspricht, zum Beispiel indem Sie Ihre eigene Arbeitsstation-IP-Adresse in die IPs-Whitelist , sodass dieses Tool Sie niemals blockiert. Sie können so viele IP-Adressen zur Whitelist hinzufügen, wie Sie möchten. Diese Adressen werden niemals von der Bruteforce-Schutzfunktion blockiert.

- Sie können **ignorieren Sie lokale und private IP-Adressen** durch Ändern der Standardeinstellung auf dem Einstellungen > Erweitert > Bruteforce-Registerkarte

Hinweis: Wenn Sie jemals bemerken, dass der Bruteforce-Schutz 10 IP-Adressen pro Tag blockiert hat und das jetzt nicht mehr der Fall ist; und eine, zwei oder sogar keine Adresse

blockiert, ist das tatsächlich normal. Tatsächlich ist es so, dass vor der Installation von Advanced Security der Server mit einem öffentlich verfügbaren RDP-Port von allen Robotern erkannt wird, und viele Roboter versuchen die aktuellen Passwörter sowie die aus Wörterbüchern. Wenn Sie Advanced Security installieren, werden diese Roboter schrittweise blockiert, sodass eines Tages:

- Die meisten der aktiven Roboter sind bereits blockiert und interessieren sich nicht für den Server, selbst die neuen.
- Auch der Server erscheint nicht mehr auf der Liste der öffentlich bekannten Server.

Befehlszeilen

Wir freuen uns, Ihnen ein umfassendes Set von Befehlszeilenwerkzeugen zur Verfügung zu stellen, die darauf ausgelegt sind, die Flexibilität und Effizienz unserer Software zu verbessern. Diese Werkzeuge ermöglichen es den Benutzern, verschiedene Funktionen zu skripten und zu automatisieren, um die Software an ihre spezifischen Bedürfnisse und Arbeitsabläufe anzupassen.

Entdecken Sie die Möglichkeiten und optimieren Sie Ihr Erlebnis mit unseren Befehlszeilenoptionen.

Sie müssen nur die folgenden Befehlszeilen als erweiterter Administrator ausführen. Zur Erinnerung, TSplus-Security.exe befindet sich im folgenden Ordner. **C:\Program Files (x86)\TSplus-Security** standardmäßig.

Lizenzverwaltung

Um Operationen an Lizenzen durchzuführen, ersetzen Sie bitte das Programm AdminTool.exe, das in der folgenden Dokumentation angegeben ist, durch das Programm TSplus-Security.exe, das sich im Installationsverzeichnis von Advanced Security befindet (in der Regel **C:\Program Files (x86)\TSplus-Security**).

- Lizenzaktivierung
- Lizenzrücksetzung nach Klonen einer VM
- Volumenlizenzaktivierung
- Aktivieren und Deaktivieren der Volumenlizenz
- Volumenlizenzaktualisierung
- Verbleibende Lizenzguthaben für einen Volumenlizenzschlüssel anzeigen
- Verbleibende Supportguthaben für einen Volumenlizenzschlüssel anzeigen

---

Proxy-Server konfigurieren: /proxy /set

Syntax:

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

Beschreibung:

Befehl /proxy /set wird verwendet, um einen Proxy-Server für den Internetzugang zu konfigurieren.

Parameter:

- /host der Zielhost kann ein vordefinierter Wert (“ie” oder “none”) oder ein benutzerdefinierter Wert (z.B.: 127.0.0.1 oder proxy.company.org) sein. Dieses Parameter ist obligatorisch
- /port die Portnummer, die verwendet wird, um eine Verbindung zum Proxy-Server herzustellen. Erforderlich, wenn der Hostname-Wert ein benutzerdefinierter Wert ist.
- /username der Benutzername, um sich mit dem Proxy-Server zu verbinden. Diese Einstellung ist optional
- /password Das Passwort des Benutzers muss angegeben werden, wenn ein Benutzername definiert wurde. Sein Wert kann jedoch leer sein.

Beispiele:

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

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

Für weitere Informationen besuchen Sie bitte Wie konfiguriert man einen Proxy-Server für den Internetzugang?

Sichern Sie Daten und Einstellungen: /backup

Syntax:

TSplus-Security.exe /backup [ZielverzeichnisPfad]

Beschreibung:

Befehl /backup wird verwendet, um Daten und Einstellungen von TSplus Advanced Security zu

sichern.

Standardmäßig wird das Backup im Verzeichnis "archives" erstellt, das sich im Verzeichnis der Advanced Security-Installation befindet (z. B.: C:\Program Files (x86)\TSplus-Security\archives).

Parameter:

- DestinationDirectoryPath um in ein anderes Verzeichnis als das Standardverzeichnis zu sichern. Relative und absolute Pfade sind erlaubt.

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Erweitert - Backup und Wiederherstellung

---

Daten und Einstellungen wiederherstellen: /restore

Syntax:

TSplus-Security.exe /restore [Sicherungsordnerpfad]

Beschreibung:

Befehl /restore wird verwendet, um TSplus Advanced Security-Daten und -Einstellungen wiederherzustellen.

Der angegebene Pfad des Sicherungsverzeichnisses muss mit dem Befehl /backup oder über die Backup-Funktion der Anwendung erstellt werden.

Parameter:

- Backup Directory Path der Pfad, wo sich das Verzeichnis für die Sicherung befindet, um wiederherzustellen.

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Erweitert - Backup und Wiederherstellung

---

Entfernen und entsperren Sie alle blockierten IP-Adressen: /unblockall

Syntax:

TSplus-Security.exe /unblockall

Beschreibung:

Befehl /unblockall wird verwendet, um alle blockierten IP-Adressen aus der Firewall von TSplus Advanced Security zu entfernen und sie bei Bedarf von der Firewall von Microsoft Windows Defender zu entsperren.

Beispiele:

TSplus-Security.exe /unblockall

Für weitere Informationen besuchen Sie bitte Firewall

Entfernen und entsperren Sie die angegebenen IP-Adressen: /unblockips

Syntax:

TSplus-Security.exe /unblockips [IP-Adressen]

Beschreibung:

Befehl /unblockips wird verwendet, um alle angegebenen blockierten IP-Adressen aus der Firewall von TSplus Advanced Security zu entfernen und sie bei Bedarf von der Firewall von Microsoft Windows Defender zu entsperren.

Dieser Befehl hat keine Auswirkungen auf IP-Adressen, die bereits durch den Hacker-IP-Schutz blockiert sind. Wenn Sie eine dieser Adressen dennoch entsperren möchten, verwenden Sie bitte den Befehl zur Whitelist.

Parameter:

- IP addresses die Liste der IP-Adressen oder IP-Bereiche, die entsperrt werden sollen (durch Komma oder Semikolon getrennt).

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Firewall

Blockierte IP-Adressen: /blockips

Syntax:

TSplus-Security.exe /blockips [IP-Adressen] [Optionale Beschreibung]

Beschreibung:

Befehl /blockips wird verwendet, um alle angegebenen IP-Adressen mit der Firewall von TSplus Advanced Security zu blockieren und sie mit der Firewall von Microsoft Windows Defender zu blockieren, wenn sie konfiguriert ist.

Parameter:

- IP addresses die Liste der zu blockierenden IP-Adressen oder IP-Bereiche (durch Komma oder Semikolon getrennt).
- Optional Description : eine optionale Beschreibung, die für jeden Eintrag hinzugefügt wird.

Beispiele:

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Johns Arbeitsplätze”

Für weitere Informationen besuchen Sie bitte Firewall

IP-Adressen zur Whitelist hinzufügen: /addwhitelistedip

Syntax:

TSplus-Security.exe /addwhitelistedip [IP-Adressen] [Optionale Beschreibung]

Beschreibung:

Befehl /addwhitelistedip wird verwendet, um bestimmte IP-Adressen zu den autorisierten IP-Adressen der Firewall von TSplus Advanced Security hinzuzufügen und sie bei Bedarf von der Firewall von Microsoft Windows Defender zu entsperren.

Parameter:

- IP addresses die Liste der IP-Adressen oder IP-Bereiche, die auf die Whitelist gesetzt werden sollen (durch Komma oder Semikolon getrennt).
- Optional Description : eine optionale Beschreibung, die für jeden Eintrag hinzugefügt wird.

Beispiele:

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Johns Arbeitsplätze”

Für weitere Informationen besuchen Sie bitte Firewall

Fügen Sie ein Programm oder Verzeichnis zur

autorisierten Liste des Ransomware-Schutzes hinzu: /whitelist

Syntax:

TSplus-Security.exe /whitelist add [Autorisierte Pfade]

Beschreibung:

Befehl /whitelist add wird verwendet, um bestimmte Programm- und Verzeichnispfade zur autorisierten Liste des Ransomware-Schutzes von TSplus Advanced Security hinzuzufügen.

Parameter:

- Authorized Paths die Liste der Programm- und Verzeichnispfade, die zur Autorisierungsliste des Ransomware-Schutzes von TSplus Advanced Security hinzugefügt werden sollen (durch Semikolons getrennt).

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Ransomware-Schutzmaßnahme

---

Aktualisieren Sie den IP-Schutz vor Hackern: / refreshipprotection

Syntax:

TSplus-Security.exe /refreshipprotection

Beschreibung:

Befehl /refreshipprotection wird verwendet, um die Liste der blockierten IP-Bereiche für die

Hacker-IP-Schutzfunktion zu aktualisieren. Ein Abonnement für Support- und Update-Dienste ist erforderlich.

Beispiele:

TSplus-Security.exe /refreshipprotection

Für weitere Informationen besuchen Sie bitte Hacker-IP-Schutz

---

Protokollebene festlegen: /setloglevel

Syntax:

TSplus-Security.exe /setloglevel [Protokollstufe]

Beschreibung:

Befehl /setloglevel wird verwendet, um das Protokollierungsniveau für alle Komponenten von Advanced Security festzulegen.

Parameter:

- Log Level der Protokollierungsgrad unter den folgenden Werten: ALLE, DEBUG, INFO, WARN, FEHLER, FATAL, AUS

Beispiele:

TSplus-Security.exe /setloglevel ALL

Für weitere Informationen besuchen Sie bitte Erweiterte > Protokolle

---

Vertrauenswürdige Geräte hinzufügen: /addtrusteddevices

Syntax:

TSplus-Security.exe /addtrusteddevices [Konfiguration vertrauenswürdiger Geräte]

Beschreibung:

Befehl /addtrusteddevices wird verwendet, um vertrauenswürdige Geräte programmgesteuert hinzuzufügen. Erfordert die Ultimate Edition.

Parameter:

- Trusted Devices Configuration Das Argument besteht aus einer Liste vertrauenswürdiger Geräte (durch Semikolons getrennt), die wie folgt strukturiert ist:

Benutzername und Geräte sind durch das Zeichen Doppelpunkt (:) getrennt.

Benutzerdetails:

Benutzertyp und vollständiger Benutzername sind durch das Doppelpunktzeichen (:) getrennt. Akzeptierte Benutzertypen sind „Benutzer“ und „Gruppe“.

Optional Keyword „deaktiviert“: Wenn enthalten, werden die vertrauenswürdigen Geräte erstellt, aber die Einschränkungen für diesen Benutzer werden deaktiviert. Wenn nicht erwähnt, sind die Einschränkungen standardmäßig aktiviert.

Geräteeinstellungen:

Gerätename und optionale Bemerkung: getrennt durch das Gleichheitszeichen (=).

Geräte sind durch das Doppelpunktzeichen (:) getrennt.

Beispiele:

TSplus-Security.exe /addtrusteddevices “user:WIN-A1BCDE23FGH\admin:disabled,device1name=dies ist ein Kommentar für Gerät 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name:device4name=ein weiterer Kommentar;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name”

Für weitere Informationen besuchen Sie bitte Vertrauenswürdige Geräte

---

Aktivieren Sie konfigurierte vertrauenswürdige Geräte: /enabletrusteddevices

Syntax:

TSplus-Security.exe /enabletrusteddevices [Benutzer oder Gruppen]

Beschreibung:

Befehl /enabletrusteddevices wird verwendet, um alle konfigurierten vertrauenswürdigen Geräte für die angegebenen Benutzer und Gruppen zu aktivieren.

Parameter:

- User or Groups Das Argument ist eine Liste von Benutzern und Gruppen (durch Semikolons getrennt). Innerhalb des Benutzernamens erfolgt die Trennung zwischen dem Benutzertyp („Benutzer“ und „Gruppe“ sind die einzigen akzeptierten Werte) und dem vollständigen Benutzernamen durch einen Doppelpunkt.

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Vertrauenswürdige Geräte

---

Alle vertrauenswürdigen Geräte deaktivieren: /disabletrusteddevices

Syntax:

TSplus-Security.exe /disabletrusteddevices [Benutzer oder Gruppen]

Beschreibung:

Befehl /disabletrusteddevices wird verwendet, um alle konfigurierten vertrauenswürdigen Geräte für die angegebenen Benutzer und Gruppen zu deaktivieren.

Parameter:

- User or Groups Das Argument ist eine Liste von Benutzern und Gruppen (durch Semikolons getrennt). Innerhalb des Benutzernamens erfolgt die Trennung zwischen dem Benutzertyp („Benutzer“ und „Gruppe“ sind die einzigen akzeptierten Werte) und dem vollständigen Benutzernamen durch einen Doppelpunkt.

Beispiele:

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

Für weitere Informationen besuchen Sie bitte Vertrauenswürdige Geräte

---

Setup Ransomware-Schutztreiber: /setup-driver

Syntax:

TSplus-Security.exe /setup-driver

Beschreibung:

Befehl /setup-driver installiert den Ransomware-Schutztreiber. Dieser Vorgang wird normalerweise während der Installation durchgeführt.

Beispiele:

TSplus-Security.exe /setup-driver

Für weitere Informationen besuchen Sie bitte Ransomware-Schutz

---

Deinstallieren Sie den Ransomware-Schutztreiber: /uninstalldriver

Syntax:

TSplus-Security.exe /uninstalldriver

Beschreibung:

Befehl /uninstalldriver deinstallieren Sie den Ransomware-Schutztreiber. Dieser Vorgang wird normalerweise während der Deinstallation von Advanced Security durchgeführt.

Beispiele:

TSplus-Security.exe /uninstalldriver

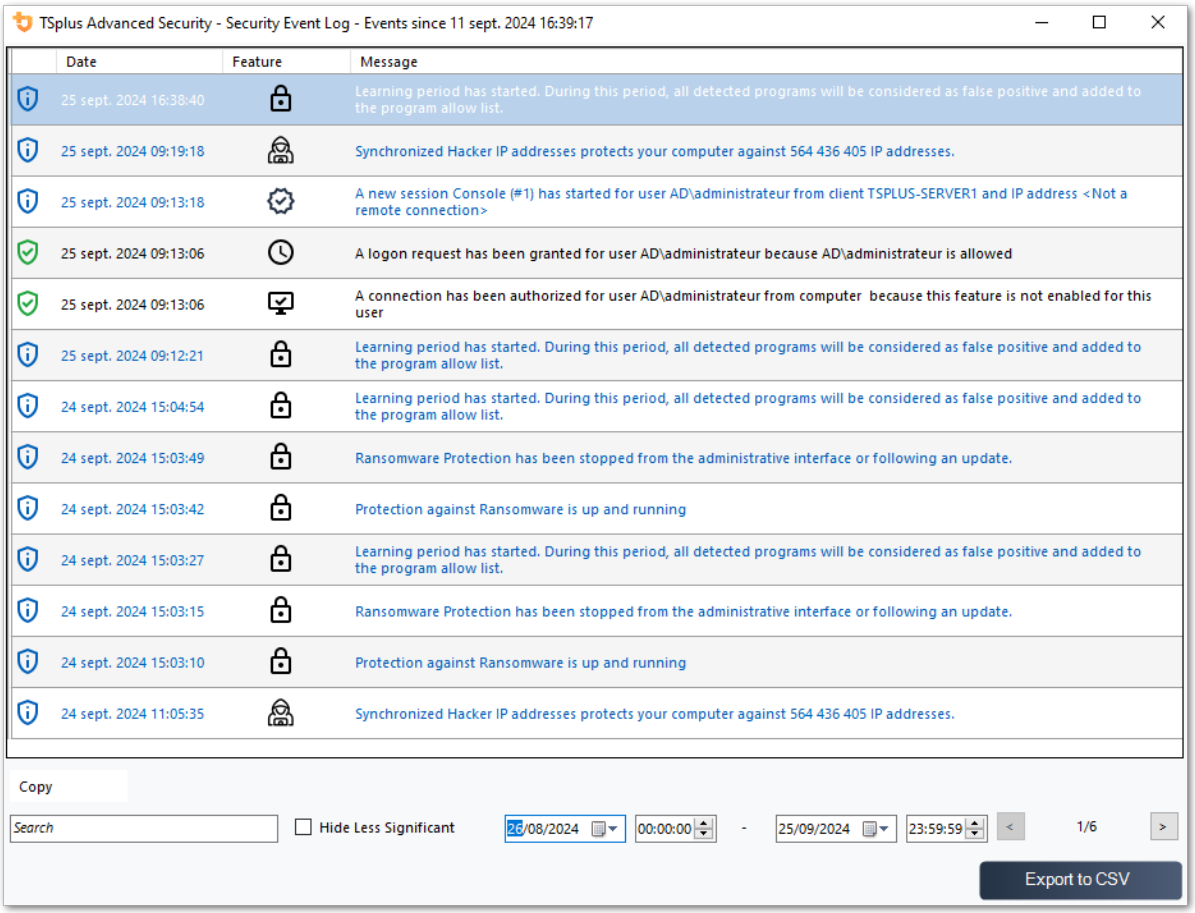
Für weitere Informationen besuchen Sie bitte Ransomware-Schutz

Veranstaltungen

Die Sicherheitsereignisse sind eine großartige Informationsquelle, da sie die von TSplus Advanced Security durchgeführten Operationen zum Schutz Ihres Computers anzeigen.

Das Ereignisfenster kann aus dem Hauptfenster von TSplus Advanced Security geöffnet werden, indem direkt auf die letzten 5 angezeigten Ereignisse oder auf die Dashboard-Registerkarte geklickt wird. Die im Ereignisfenster angezeigten Informationen werden alle paar Sekunden automatisch aktualisiert.

Die Liste der Sicherheitsereignisse enthält 4 Spalten, die die Schwere, das Datum der Überprüfung oder der durchgeführten Operation, das zugehörige Funktionssymbol und die Beschreibung darstellen.



Die Beschreibung des Ereignisses erklärt oft, warum die Aktion durchgeführt wurde oder nicht. Vergeltungsmaßnahmen sind oft in Rot geschrieben und mit einem roten Schildsymbol hervorgehoben.

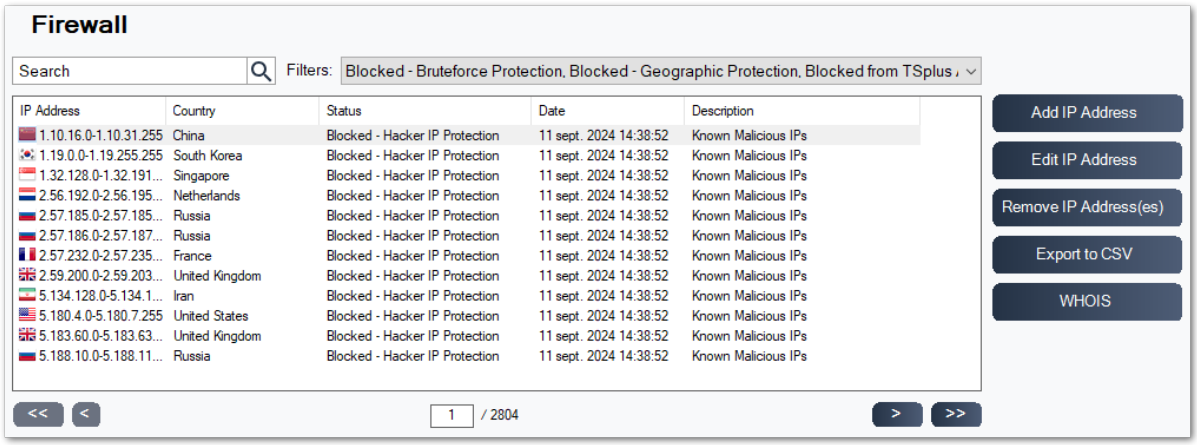
Das Ereignisfenster kann verschoben werden und hindert Sie nicht daran, die anderen Funktionen von TSplus Advanced Security zu nutzen.

Ereignisse navigieren und durchsuchen

- A deep global search is now available in order to find specific events quickly.
- Neben der globalen Suche filtern 2 Datums- und Zeitwähler die angezeigten Ereignisse nach dem Datum, an dem das Ereignis erstellt wurde.
- Auf der rechten Seite ermöglichen Pfeile das Wechseln von Seiten und das Navigieren, um ältere Ereignisse anzuzeigen.

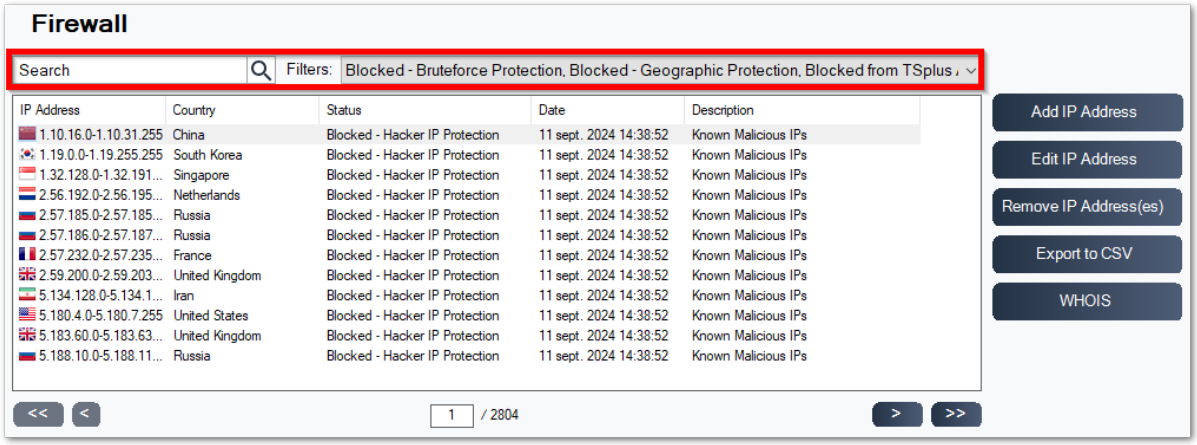
Firewall

Die Verwaltung von IP-Adressen ist einfach mit einer einzigen Liste, um sowohl blockierte als auch zugelassene IP-Adressen zu verwalten:



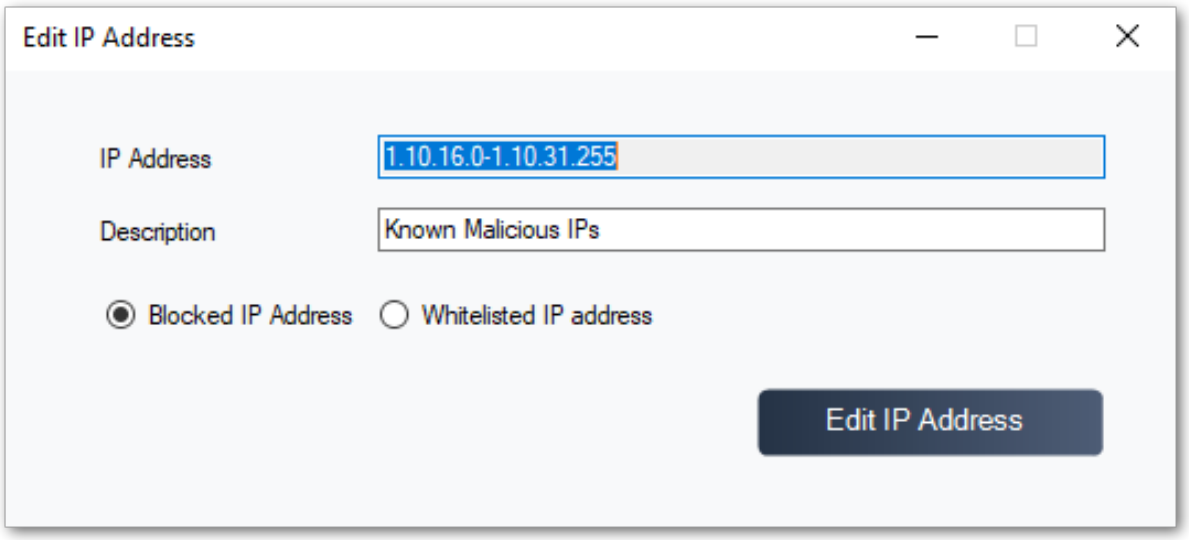
Standardmäßig sind IPV4, IPV6 und alle lokalen Serveradressen auf der Whitelist.

Eine praktische Suchleiste und ein Filter bieten Suchfunktionen basierend auf allen bereitgestellten Informationen.



Darüber hinaus können Administratoren mit einem einzigen Klick Aktionen auf mehreren ausgewählten IP-Adressen ausführen. Zu den neuen Funktionen des IP-Adressmanagements

gehört die Möglichkeit, aussagekräftige Beschreibungen für beliebige IP-Adressen bereitzustellen.



Zu guter Letzt können Administratoren jetzt mehrere blockierte IP-Adressen in einer einzigen Aktion entsperren und zur Whitelist hinzufügen, indem sie auf die Registerkarte „Vorhandene zur Whitelist hinzufügen“ klicken.

Die Verwendung der Befehlszeile zum Whitelisten oder Blockieren von IP-Adressen und/oder IP-Bereichen

- Um zu **whitelist** IP-Adressen oder IP-Bereiche, der Befehl hat diese Syntax:

TSplus-Security.exe addwhitelistedip [IP-Adressen] [optionale Beschreibung]

Sie können mehrere IP-Adressen auf die Whitelist setzen, mit einem **Komma oder Semikolon-Trennzeichen** Darüber hinaus können Sie IP-Adressbereiche angeben, anstelle von einfachen IP-Adressen. Die Syntax ist: **x.x.x.x-y.y.y.y** Schließlich können Sie eine optionale Beschreibung der Whitelist-Regel angeben.

Hier ist ein Beispiel für einen vollständigen Befehl : TSplus-Security.exe addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “Johns Arbeitsplätze”

- Um zu **Block** IP-Adressen oder IP-Bereiche, der Befehl hat eine ähnliche Syntax:

TSplus-Security.exe blockips [ip addresses] [optional description]

- Um zu **entsperren** IP-Adressen oder IP-Bereiche, der Befehl hat eine ähnliche Syntax:

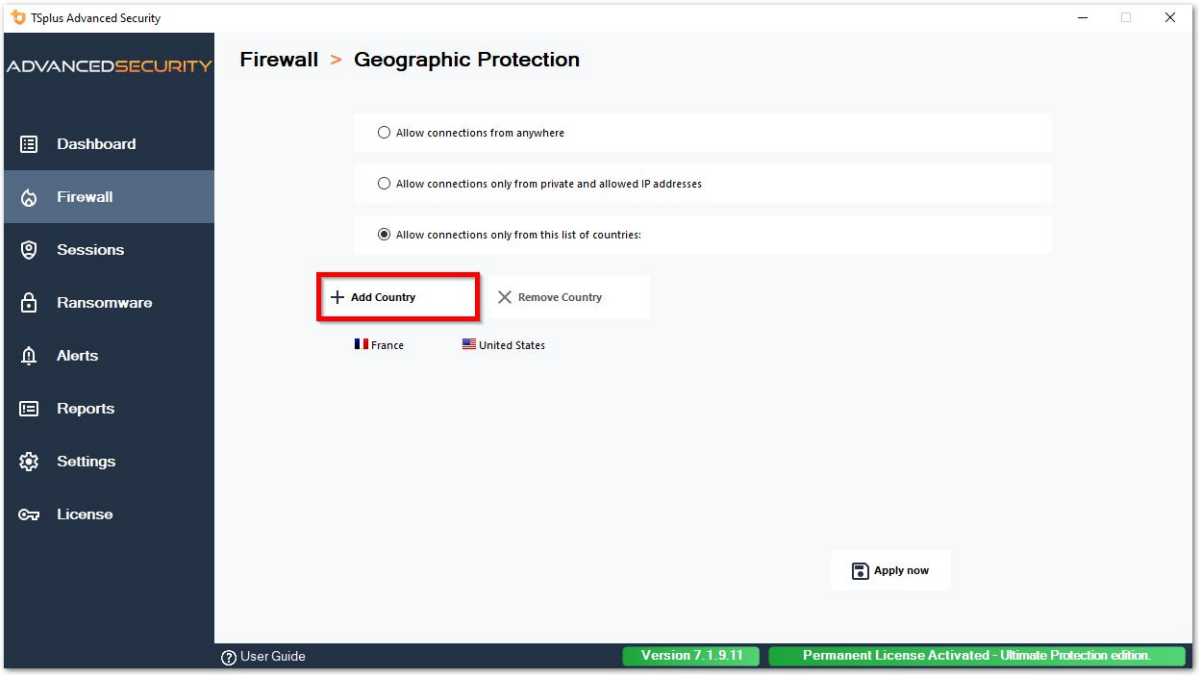
TSplus-Security.exe unblockips [IP-Adressen]

Dieser Befehl hat keine Auswirkungen auf IP-Adressen, die bereits durch den Hacker-IP-Schutz blockiert sind. Wenn Sie eine dieser Adressen dennoch entsperren möchten, verwenden Sie bitte den Befehl zur Whitelist.

Geografischer Schutz

Zugriff aus anderen Ländern einschränken

Um den Remote Access nur von bestimmten Ländern zuzulassen, wählen Sie die Schaltfläche „Verbindungen nur von dieser Liste von Ländern zulassen“ und klicken Sie dann auf die Schaltfläche „Land hinzufügen“.

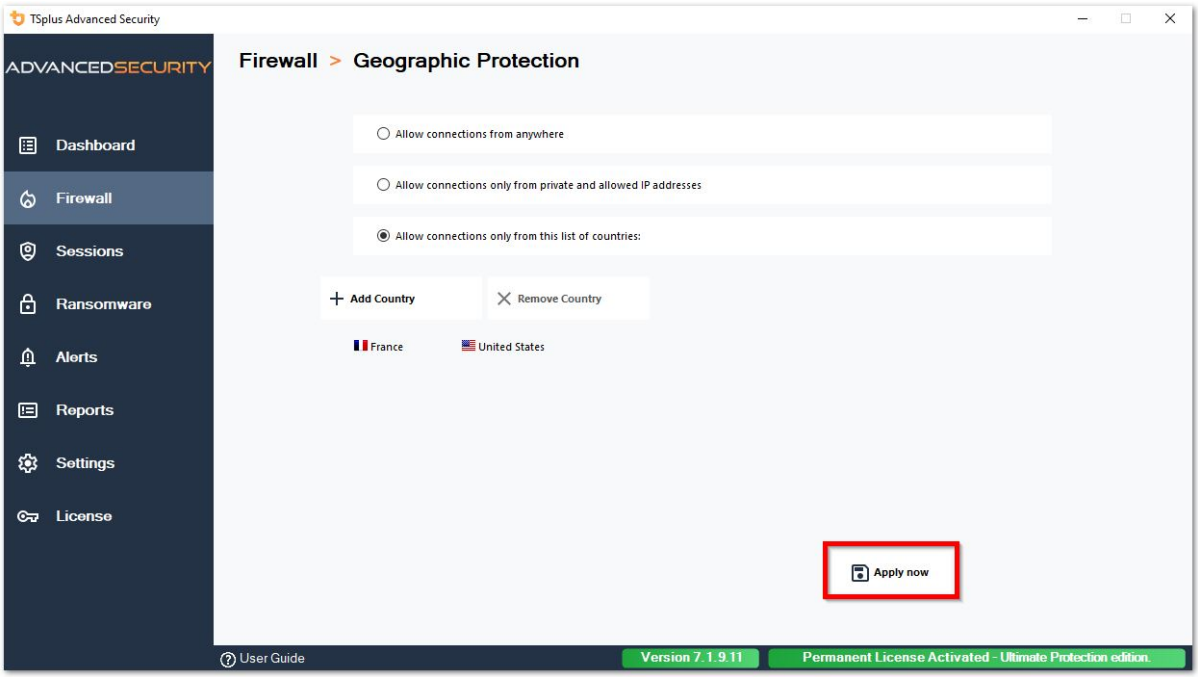


Ein Popup mit einer Länderliste öffnet sich. Wählen Sie das Land aus, das Sie zur Liste hinzufügen möchten.

Sie können das untenstehende Kästchen aktivieren, um alle zuvor blockierten IP-Adressen für das ausgewählte Land zu entsperren.

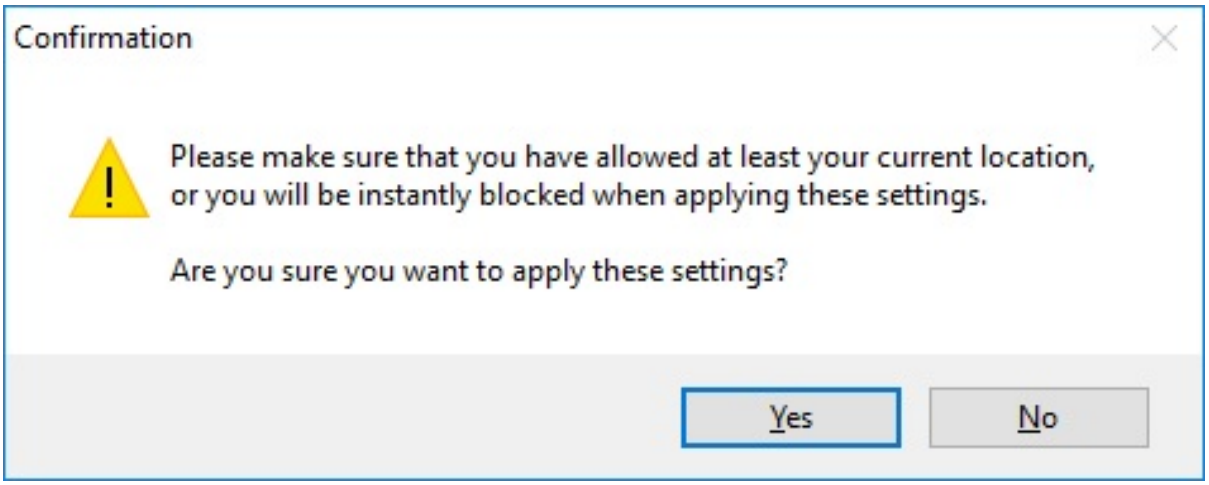
Klicken Sie auf die Schaltfläche „Land hinzufügen“, um zum Hauptbildschirm der Funktion zurückzukehren.

Wichtig: Um Ihre Änderungen zu speichern, klicken Sie auf die Schaltfläche „Übernehmen“.



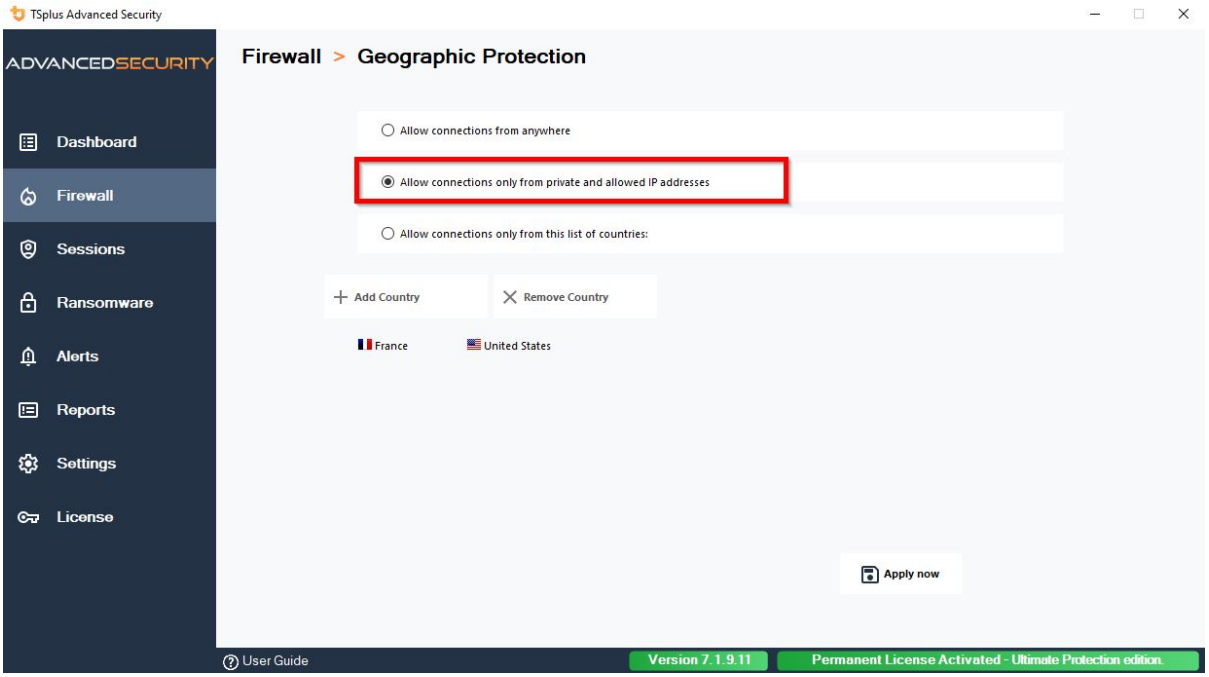
In diesem Beispiel ist der Remote Access für Benutzer, die sich aus den Vereinigten Staaten und Frankreich verbinden, erlaubt.

Eine Bestätigungsnachricht erscheint, um zu verhindern, dass der verbundene Benutzer blockiert wird. Klicken Sie auf „Ja“, um zu bestätigen und die Änderungen anzuwenden.



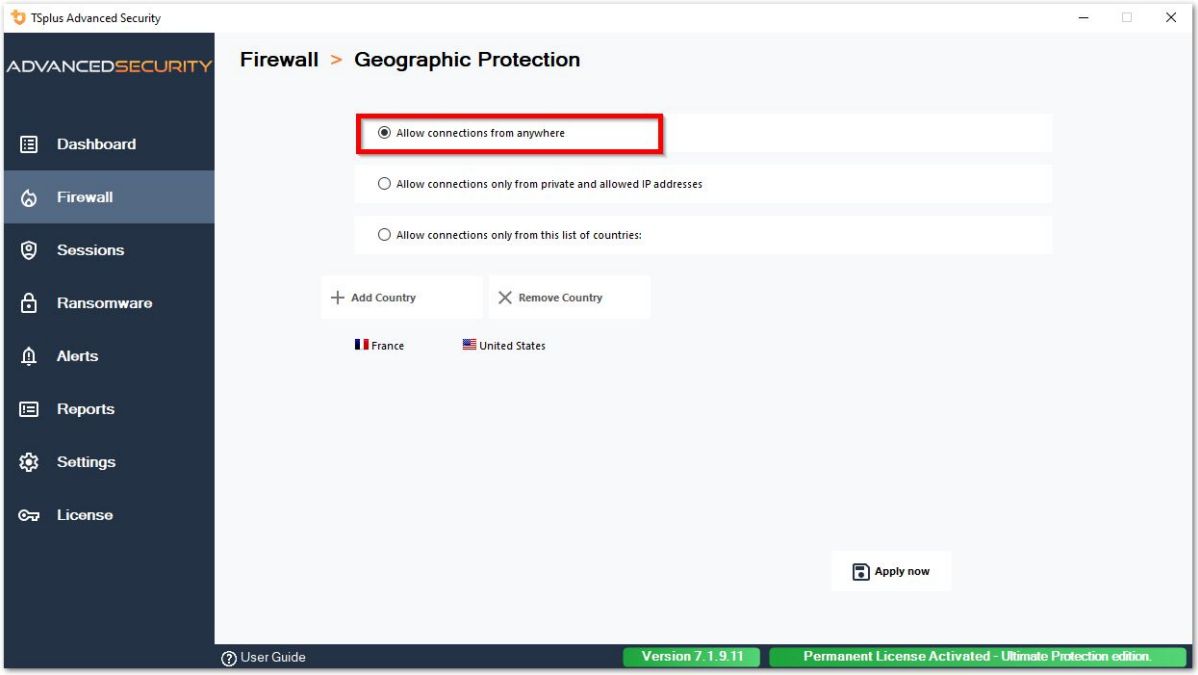
Zugriff aus dem Internet einschränken

Geografischer Schutz kann so konfiguriert werden, dass der Zugriff auf Ihre Maschine nur auf private und whitelisted IP-Adressen Please provide the text you would like to have translated.



Geografischen Schutz deaktivieren

Standardmäßig ermöglicht der geografische Schutz den Zugriff für Benutzer, die von überall auf der Welt eine Verbindung herstellen.



Entsperren blockierter IP-Adressen

Wenn eine IP-Adresse blockiert wird, erscheint sie auf dem Firewall-Registerkarte Blockierte IP-Adressen können dann wieder freigegeben und schließlich zur Liste der erlaubten IP-Adressen hinzugefügt werden.

Wenn Sie blockiert werden, empfehlen wir Ihnen, zu versuchen, sich von einem beliebigen Land zu verbinden, das Sie in TSplus Advanced Security erlaubt haben, zum Beispiel indem Sie sich von einem anderen Remote-Server oder über einen VPN-Dienst verbinden. Sie können auch eine Konsolensitzung verwenden, um sich zu verbinden, da diese Sitzung keine Remote-Sitzung ist und nicht von TSplus Advanced Security blockiert wird.

Wichtig:

- Überprüfen Sie, ob Sie das Land ausgewählt haben, von dem aus Sie derzeit verbunden sind. Andernfalls wird Ihre IP-Adresse schnell nach Anwendung der Einstellungen blockiert, wodurch Sie ohne Hoffnung, sich erneut von derselben IP-Adresse zu verbinden, getrennt werden.

- Erwägen Sie, Ihre eigene IP-Adresse zur Liste der erlaubten hinzuzufügen. IP-Adressen um zu vermeiden, dass Sie entweder durch Homeland Protection oder blockiert werden Bruteforce-Schutz Funktionen.

Geografischen Schutz verstehen

Geographic Protection überprüft eingehende TCP-Netzwerkverbindungen, sowohl IPv4 als auch IPV6 (es sei denn, der Legacy-Windows-API-Modus ist konfiguriert).

Prozesse: Geographic Protection hört standardmäßig auf Verbindungen, die an den Webserver von TSplus Remote Access gesendet werden, wenn es installiert ist. Der Name des entsprechenden Prozesses ist HTML5 Service. Wenn Sie die Überwachung deaktivieren oder Verbindungen zu anderen Prozessen überprüfen möchten, gehen Sie zu Einstellungen > Erweitert > Geografischer Schutz .

Netzwerkports: Standardmäßig hört Geographic Protection auf den Standardports, die für die Remoteverbindung zu einem Server verwendet werden. Diese Ports umfassen RDP (3389), Telnet (23) und VNC. Geographic Protection unterstützt die folgenden VNC-Anbieter: Tight VNC, Ultra VNC, Tiger VNC und Real VNC, die in keiner Weise mit TSplus verbunden sind. Wenn Sie die Überwachung deaktivieren oder Verbindungen zu anderen Ports überprüfen möchten, gehen Sie zu Einstellungen > Erweitert > Geografischer Schutz .

Erkennungsmechanismen:

Geographic Protection erkennt eingehende Verbindungen aus unbefugten Ländern mithilfe von drei verschiedenen Erkennungsmechanismen:

- Windows-API
- Ereignisverfolgung für Windows
- Integrierte Firewall

Einerseits ist die Ereignisverfolgung für Windows eine effiziente Kernel-Level-Verfolgungseinrichtung, die Netzwerkereignisse in Echtzeit erfasst. Die Ereignisverfolgung für Windows wird empfohlen, wenn die Windows-Firewall aktiviert ist (Standard).

Andererseits funktioniert die Windows-API hervorragend, wenn eine bestimmte Netzwerk-Konfiguration vorliegt, kann jedoch je nach Anzahl der aktiven Verbindungen einen konstanten Druck auf die CPU ausüben. Bitte beachten Sie, dass die Windows-API noch nicht mit IPv6 kompatibel ist.

Die integrierte Firewall ermöglicht das Erfassen und Blockieren von Netzwerkpaketen im Benutzermodus, die an den Windows-Netzwerk-Stack gesendet werden. Wenn die integrierte Firewall so konfiguriert ist, dass unerwünschte Verbindungen blockiert werden, wird empfohlen, sie zur Durchsetzung der erlaubten Länder des geografischen Schutzes zu verwenden.

Geolokalisierung: Advanced Security umfasst Geolokalisierungsdaten, die von MaxMind veröffentlicht werden, erhältlich bei http://www.maxmind.com Wenn Sie eine IP-Adresse finden, die nicht in ihrem tatsächlichen Land registriert ist, kontaktieren Sie bitte MaxMind direkt, um das Problem zu beheben.

Fehlerbehebung

Wenn Sie jemals feststellen, dass der geografische Schutz Verbindungen aus einem Land nicht blockiert, das tatsächlich nicht auf der Liste der autorisierten Länder steht, liegt das sicherlich daran, dass:

Antivirus: Um eine IP-Adresse zu blockieren, fügt Geographic Protection eine Blockierungsregel in der Windows-Firewall hinzu. Daher muss die Firewall zunächst aktiv sein. Sie müssen auch überprüfen, ob einige Firewall-Parameter nicht von einem anderen Programm, wie einem Antivirus, verwaltet werden. In diesem Fall müssen Sie dieses Programm deaktivieren und den Dienst „Windows-Firewall“ neu starten. Sie können auch den technischen Kontakt Ihres Drittanbieter-Programmeditors kontaktieren und ihn bitten, einen Weg zu finden, damit ihr Programm die Regeln respektiert, wenn es zur Windows-Firewall hinzugefügt wird. Wenn Sie einen technischen Kontakt eines Software-Editors kennen, sind wir bereit, diese „Connectoren“ für die Firewall zu entwickeln. Kontaktieren Sie uns .

VPN: Falls der Remote-Client ein VPN verwendet, erhält der Geographic Protection eine IP-Adresse, die vom VPN-Anbieter ausgewählt wurde. Wie Sie wissen, verwenden VPN-Anbieter Relais auf der ganzen Welt, um ihren Nutzern anonymes Surfen zu ermöglichen. Einige VPN-Anbieter erlauben es den Nutzern, das Land des Relais festzulegen. Daher können Nutzer mit VPN-Anbietern durch ein nicht autorisiertes Land geleitet werden. Wenn ein VPN-Anbieter beispielsweise eine IP aus Sri Lanka wählt, muss dieses Land von Geographic Protection autorisiert sein. Wenn das VPN zudem eine interne Unternehmens-IP-Adresse verwendet, wird der Schutz irrelevant.

Firewall / Proxy: Der Zweck einer Hardware-Firewall besteht darin, eingehende und ausgehende Verbindungen für große Unternehmen zu filtern. Da sie nur ein Filter ist, sollte sie die ursprüngliche IP-Adresse nicht ändern und daher keinen Einfluss auf den geografischen Schutz haben. Ein Proxy würde jedoch die ursprüngliche IP-Adresse definitiv ändern, um eine private Netzwerkadresse zu verwenden, die immer vom geografischen Schutz erlaubt wird. Der Hauptzweck dieser Funktion besteht darin, den Zugriff auf einen Server, der für das Internet geöffnet ist, zu blockieren. Wenn alle Verbindungen aus dem Unternehmensnetzwerk stammen, wird der Schutz irrelevant.

Hacker-IP-Schutz

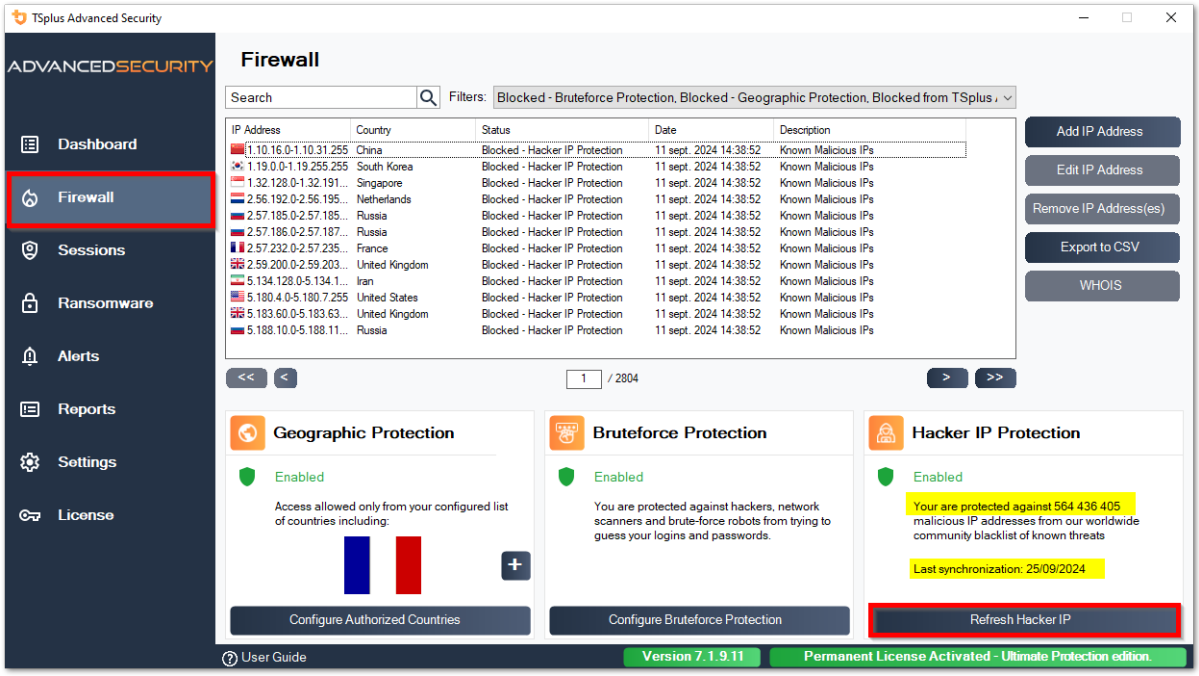
Halten Sie Ihre Maschine gegen bekannte Bedrohungen wie Online-Angriffe, Missbrauch von Online-Diensten, Malware, Botnets und andere Cyberkriminalitätsaktivitäten mit dem Hacker-IP-Schutz geschützt. Ziel ist es, eine Blacklist zu erstellen, die sicher genug ist, um auf allen Systemen verwendet zu werden, mit einer Firewall, um den Zugriff vollständig von und zu den aufgeführten IPs zu blockieren.

Support- und Aktualisierungsdienste-Abonnement ist erforderlich.

Die wichtigste Voraussetzung für diesen Zweck ist, keine Fehlalarme zu haben. Alle aufgeführten IPs sollten schlecht sein und sollten ohne Ausnahmen blockiert werden. Um dies zu erreichen, nutzt der Hacker-IP-Schutz die Informationen, die von der Community der Benutzer von Advanced Security bereitgestellt werden.

Hacker-IP-Schutz wird täglich automatisch aktualisiert.

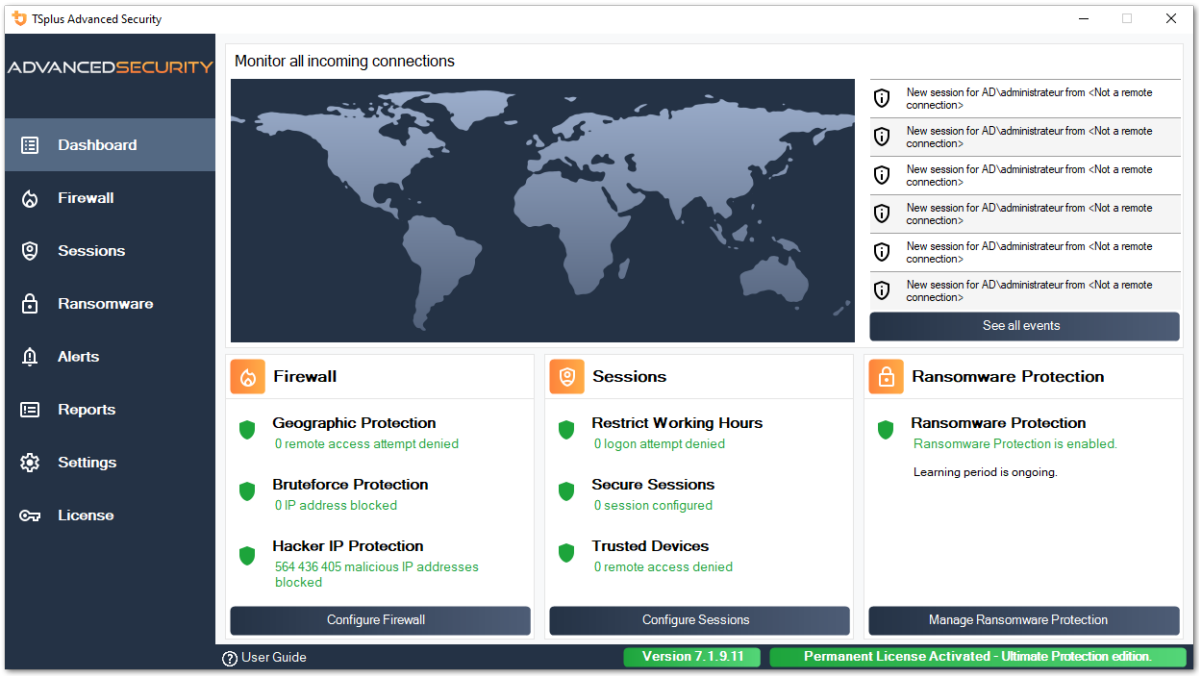
Sie können manuell über die Registerkarte „Blockierte IP-Adressen“ aktualisieren, indem Sie auf die Schaltfläche „Hacker-IP aktualisieren“ klicken:



Als Ergebnis sollte die Funktion etwa 600.000.000 blockierende Firewall-Regeln in der Windows-Firewall erstellen.

Dashboard

Klicken Sie auf jede Kachel, um mehr über jede Funktion zu erfahren.



Die Menüleiste auf der linken Seite bietet Zugriff auf die verschiedenen Funktionen. Jede Kachel gibt Ihnen Zugang zu den verschiedenen Funktionen und Einstellungen, die von TSplus Advanced Security angeboten werden.

Advanced Security zeigt die letzten sechs an Sicherheitsereignisse Klicken Sie auf ein beliebiges Ereignis, um die vollständige Liste der Ereignisse in einem separaten Fenster zu öffnen.

Unter den letzten Ereignissen bieten drei Kacheln schnellen Zugriff auf:

1. Firewall

2. Sitzungen

3. Ransomware-Schutz

Bitte wählen Sie Ihre Anzeigesprache über das Dropdown-Menü in der oberen rechten Ecke aus, falls die Anwendung Ihre Sprache nicht erkannt hat.

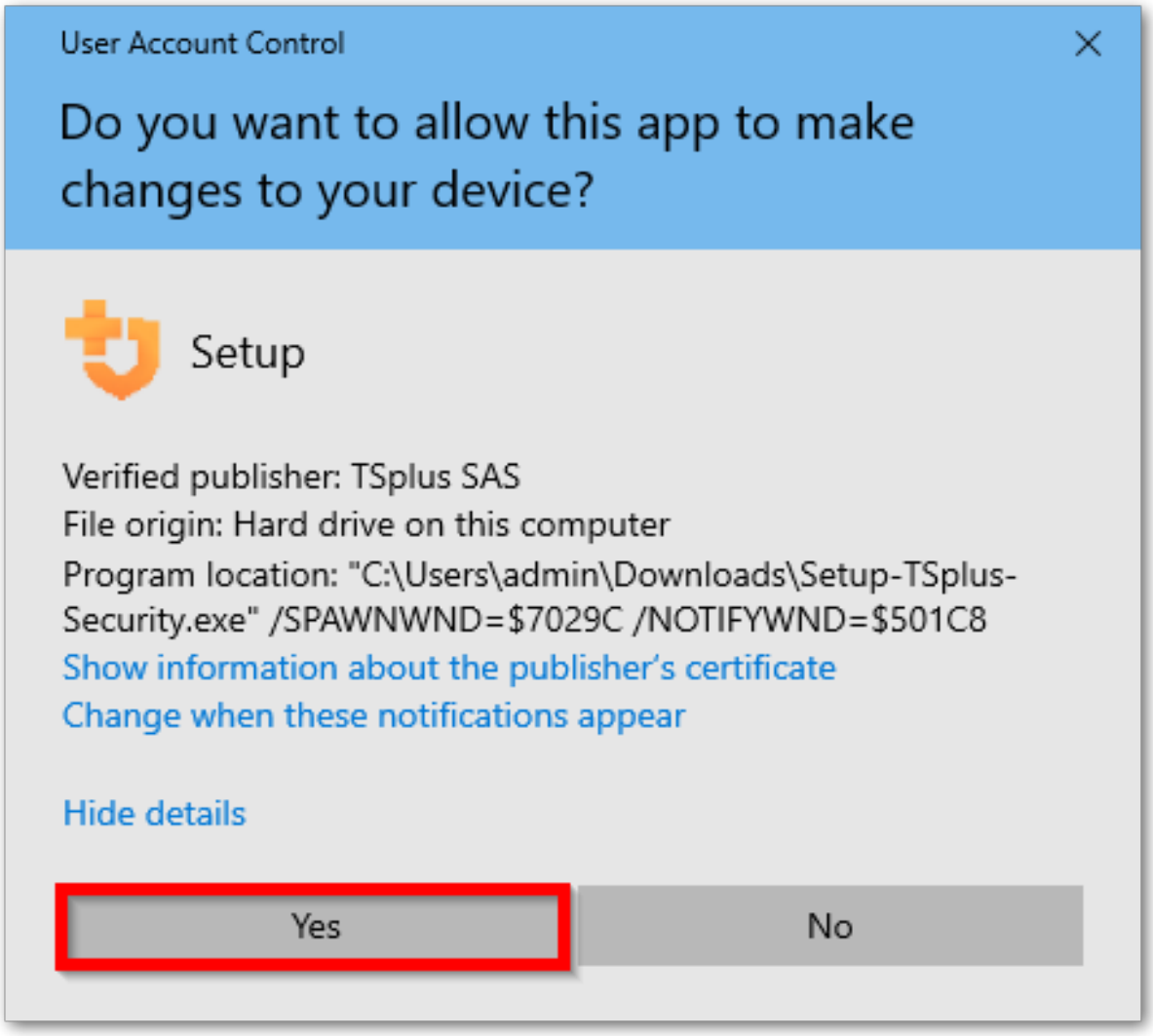
Schließlich wird ein Klick auf die Schaltfläche „Hilfe“ Sie zu dieser Dokumentation weiterleiten.

Installation von TSplus Advanced Security

Installation von Advanced Security

Ausführen TSplus Advanced Security Setup-Programm und dann **folge den Installationsschritten** .

Sie müssen das Installationsprogramm als Administrator ausführen und die Lizenzvereinbarung der Software akzeptieren.



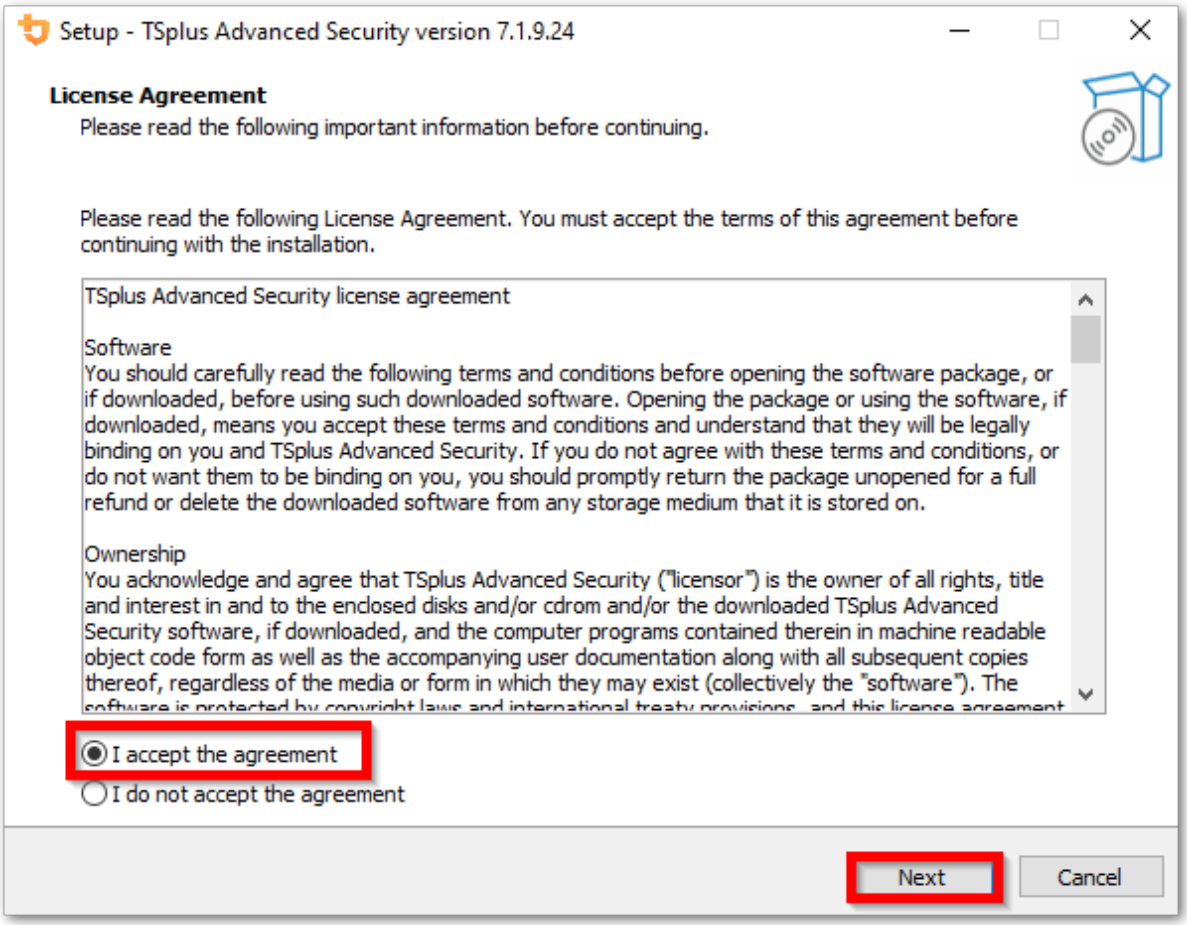
Wählen Sie die Sprache des Einrichtungsassistenten, falls sie nicht automatisch erkannt wird.

Dann wählen Sie eine der beiden Optionen aus: **Empfohlen** oder **Erweitert** indem Sie auf die entsprechenden Kästchen klicken.

Die erweiterte Option fügt zusätzliche Schritte hinzu, die es Ihnen ermöglichen, zu:

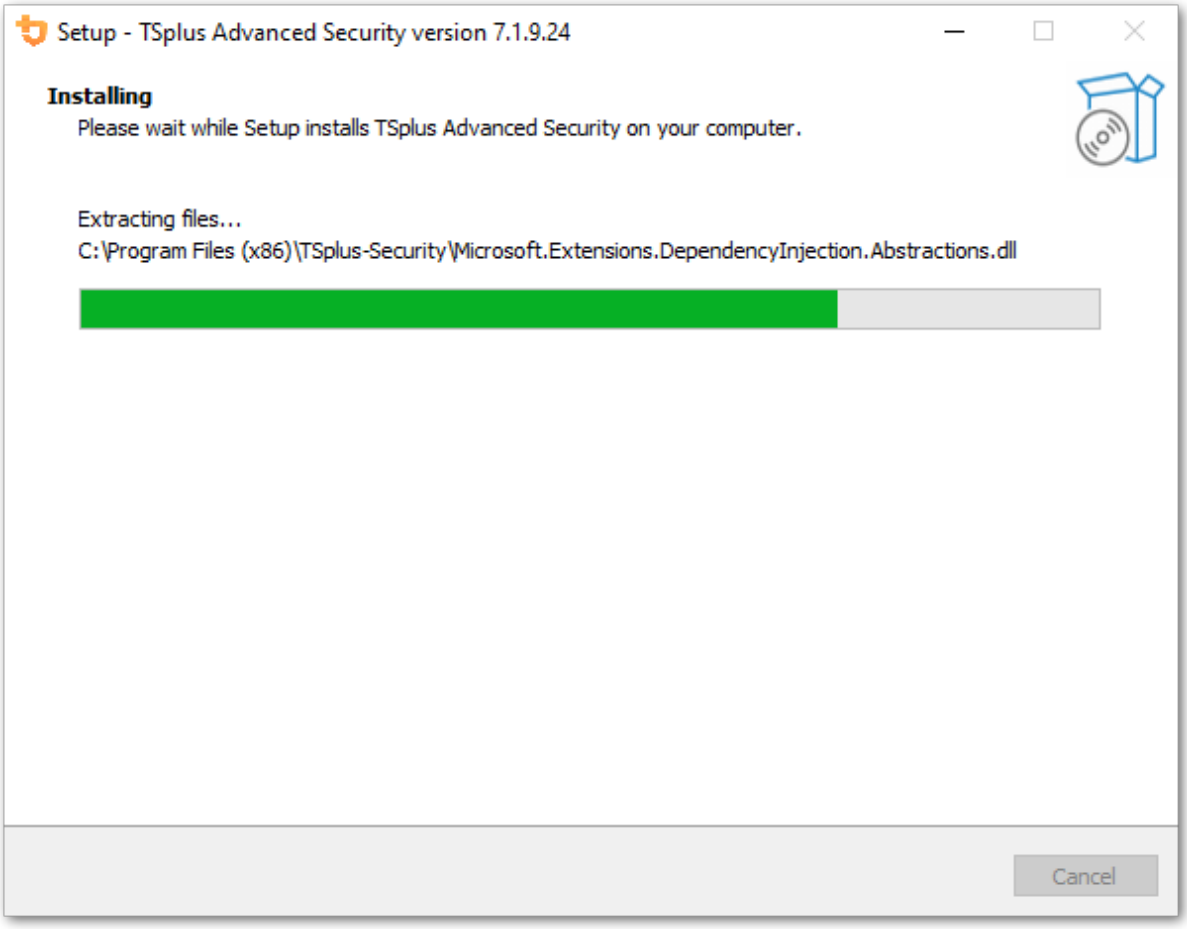
- Nur das Setup herunterladen (nicht installieren)
- Benutzerdefinierte Proxy-Einstellungen verwenden

Lesen Sie die Lizenzvereinbarung und klicken Sie auf „Ich stimme zu“, um die Installation fortzusetzen.



Das Programm wird auf Ihrem Computer installiert.

Eine Fortschrittsanzeige wird am unteren Rand angezeigt und berichtet über den Fortschritt der Installation.



Bitte haben Sie Geduld da es manchmal bis zu einigen Minuten dauern kann, bis die Software vollständig installiert ist.

Sobald die Installation abgeschlossen ist, können Sie mit der Verwendung von TSplus Advanced Security beginnen!

Die kostenlose Testversion ist voll funktionsfähig für 15 Tage. Vergessen Sie nicht zu aktivieren Sie Ihre Lizenz und zu aktualisieren Sie auf die neueste Version um den Schutz von Advanced Security optimal zu halten!

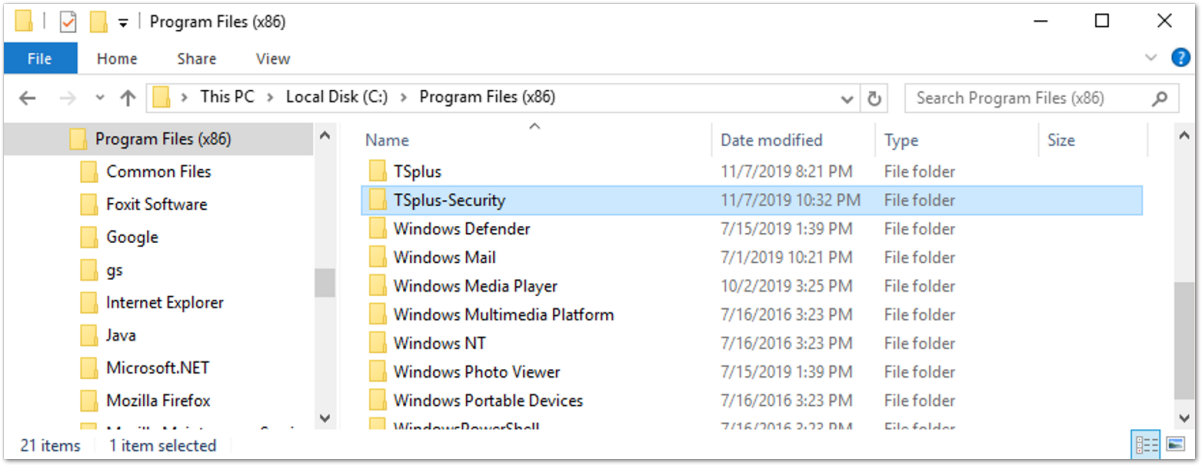
Erweiterte Installationsszenarien

Die TSplus Advanced Security Classic Setup-Programm behandelt die folgenden Szenarien, da es über die Befehlszeile ausgeführt werden kann:

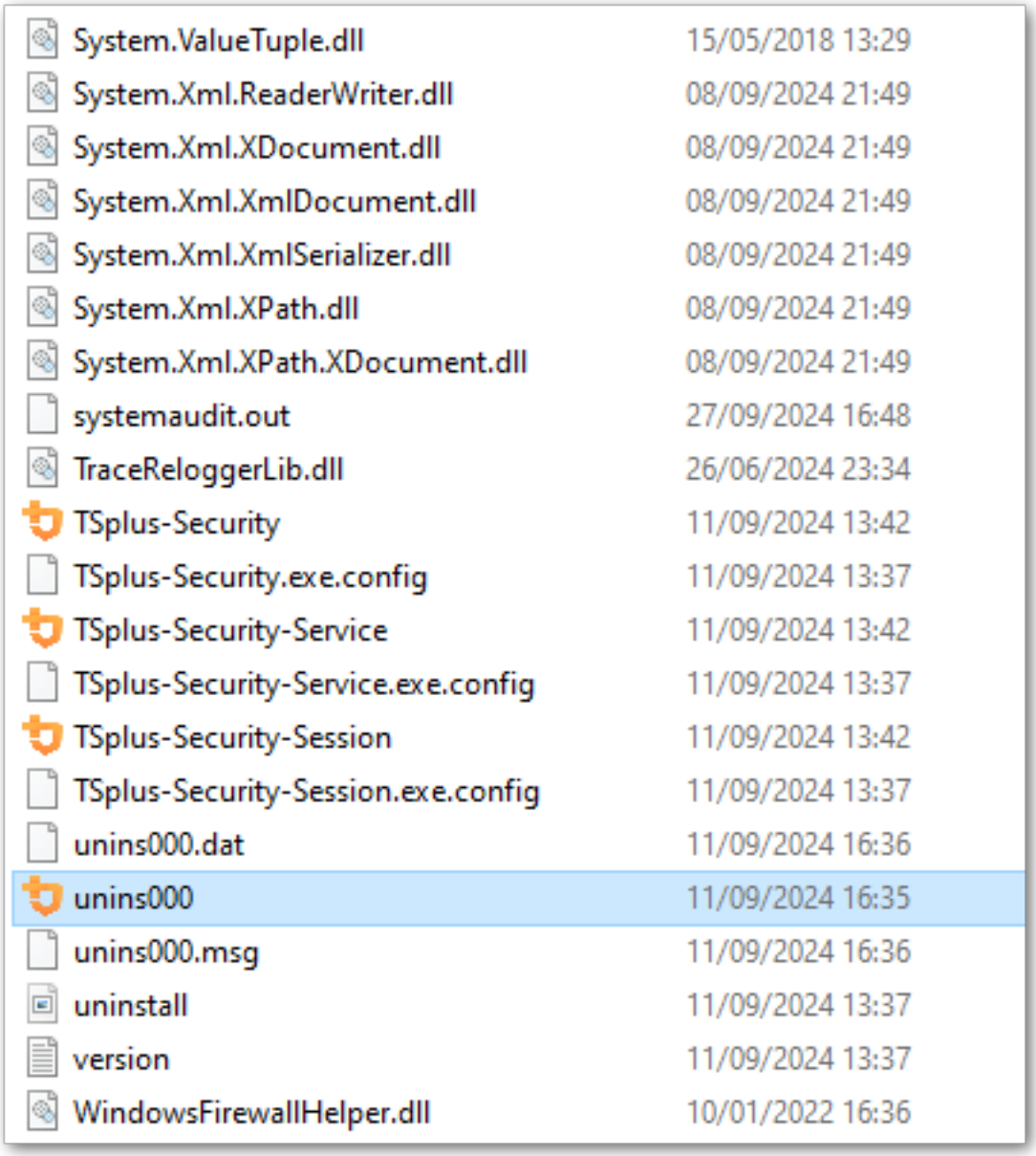
- Installieren Sie still, indem Sie die Parameter /VERYSILENT /SUPPRESSMSGBOXES bereitstellen.
- Verhindern Sie das Neustarten am Ende der Einrichtung, indem Sie den Parameter /NORESTART bereitstellen. Dieser Parameter wird normalerweise zusammen mit dem oben genannten verwendet.
- Volumenlizenzierung zur Aktivierung Ihrer Lizenz direkt während der Installation (bitte beachten Sie die Dokumentation oder kontaktieren Sie uns für weitere Informationen)

Deinstallieren Sie TSplus Advanced Security

Um TSplus Advanced Security vollständig zu deinstallieren, öffnen Sie das Verzeichnis C:\Program Files (x86)\TSplus-Security.



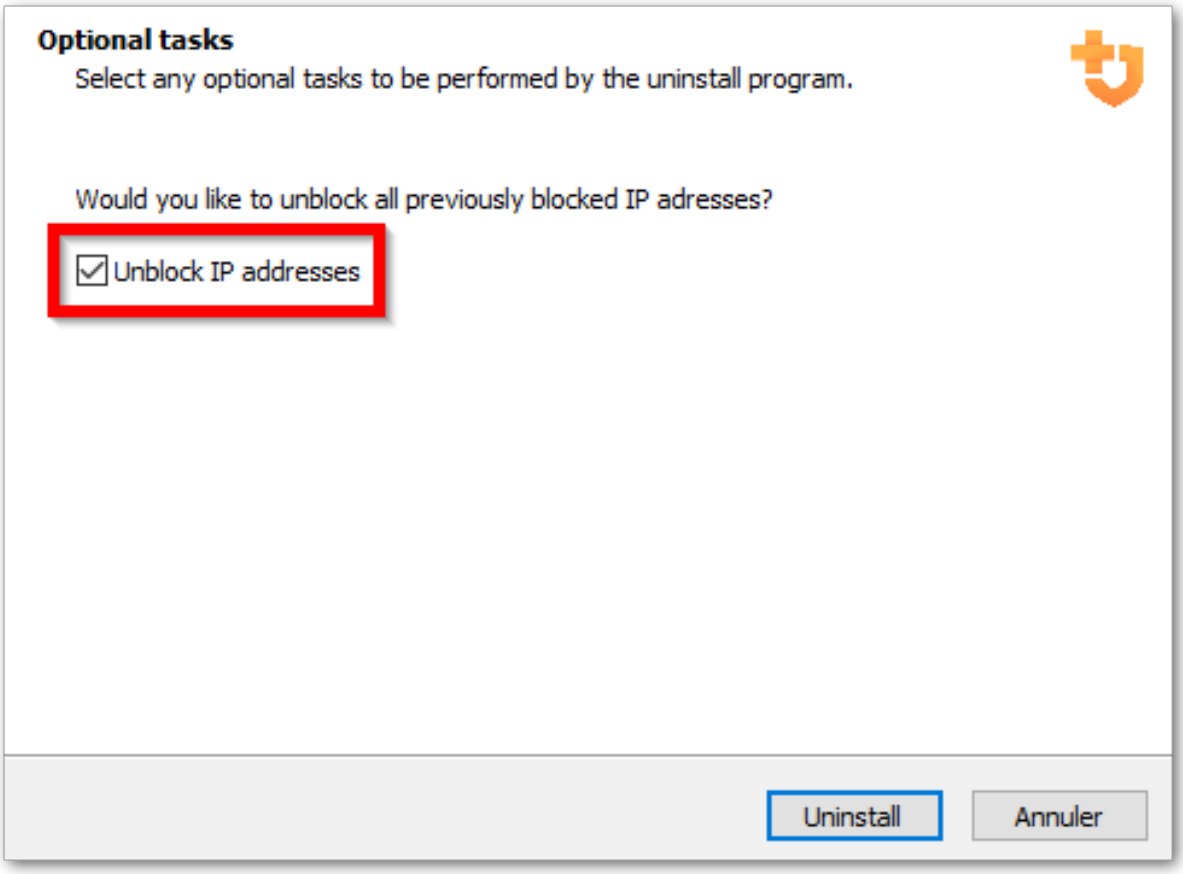
Dann doppelklicken Sie auf die Anwendung „unins000“, um das Deinstallationsprogramm auszuführen.



Klicken Sie im nächsten Fenster auf Ja, um TSplus Advanced Security und alle seine Komponenten vollständig zu entfernen.

Es sei denn, es wurde anders konfiguriert, fügt Advanced Security Blockierungsregeln zur Windows-Firewall hinzu. Klicken Sie auf „IP-Adressen entsperren“, um alle zuvor von Advanced Security blockierten IP-Adressen zu entsperren und zu entfernen.

Wichtig: Bitte beachten Sie, dass das Entfernen aller Regeln bis zu einer Stunde dauern kann. Aus diesem Grund empfehlen wir, die Regeln direkt über die Windows-Firewall mit der Konsole für erweiterte Sicherheit zu entfernen.



Die Software wird vollständig von Ihrem Computer deinstalliert.

Berechtigungsmanagement

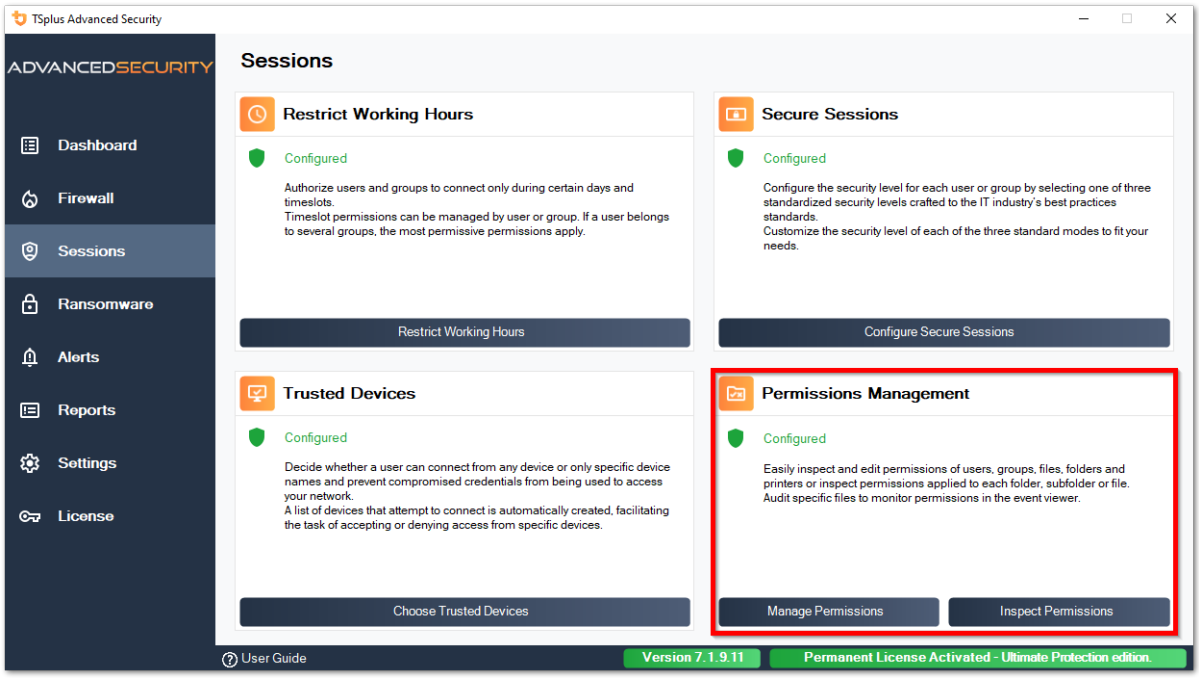
Seit Version 4.3 bietet TSplus Advanced Security eine Berechtigungsfunktion, die es dem Administrator ermöglicht, die Berechtigungen von Benutzern/Gruppen zu verwalten und/oder zu überprüfen.

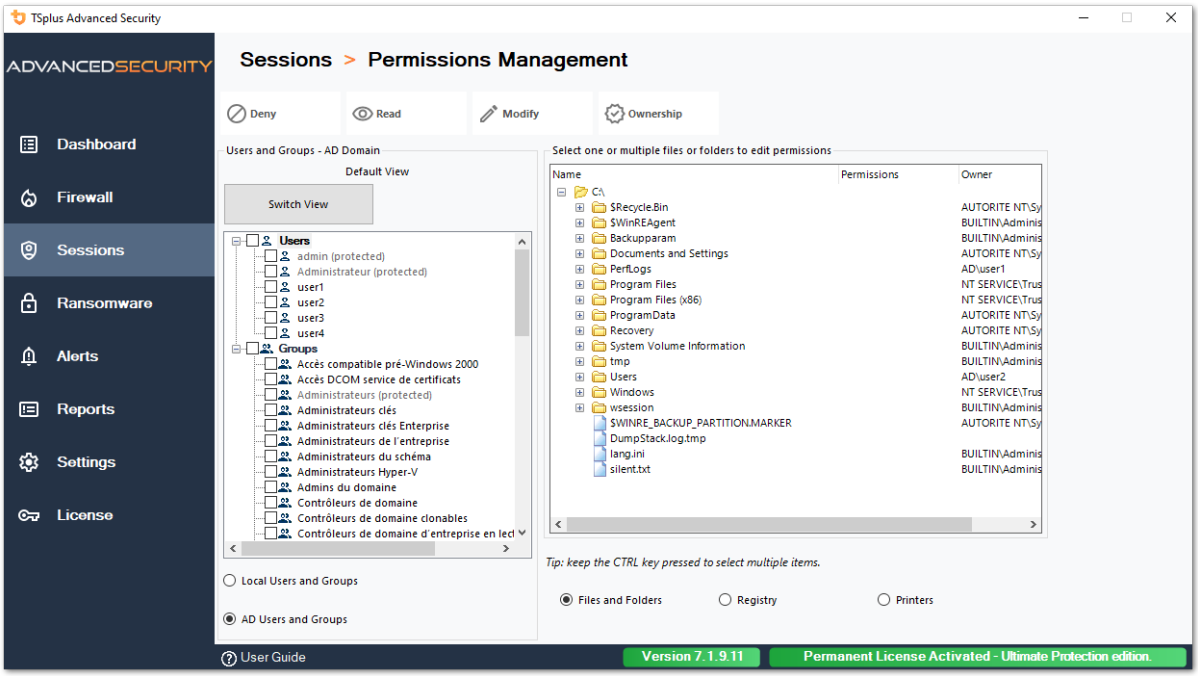
Auf dem Berechtigungs-Dashboard werden die Liste der Benutzer und Gruppen sowie die Liste der verfügbaren **Dateien, Ordner, Registrierungen und Drucker** werden nebeneinander angezeigt.

Alles ist auf einen Blick sichtbar, was es super einfach macht, um **Überprüfen** und **Verwalten/ Bearbeiten** Befugnisse für einen Benutzer zur gleichen Zeit und daher die Genauigkeit der Einschränkungen zu erhöhen.

Berechtigungen verwalten

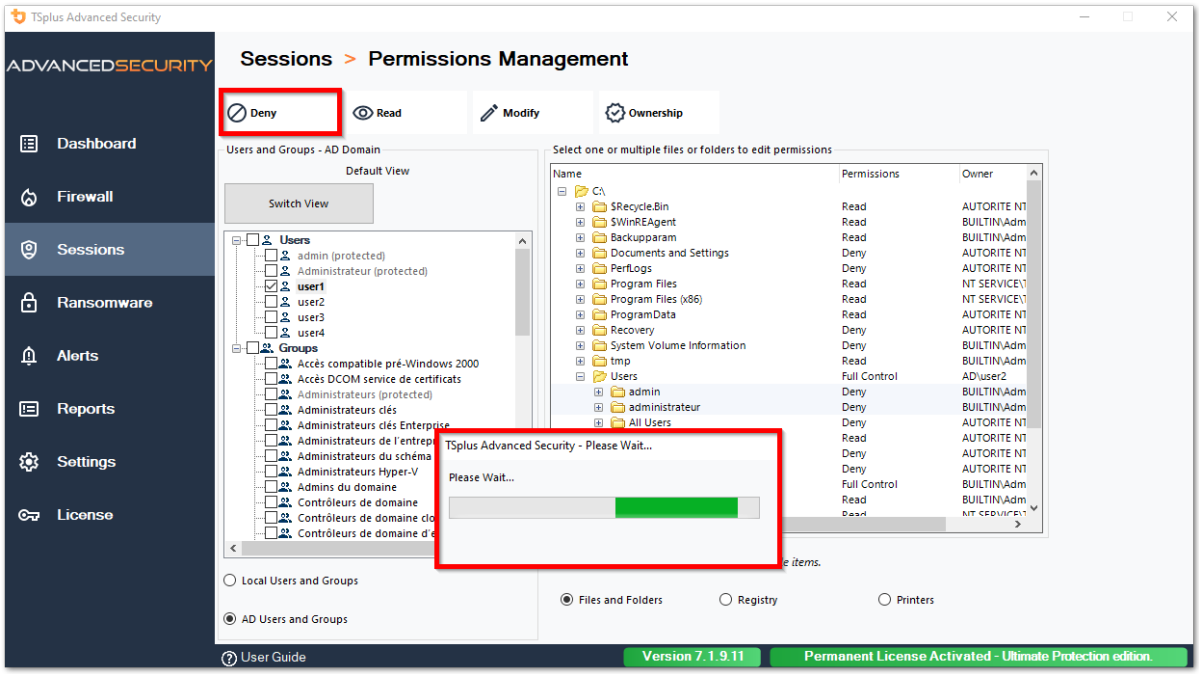
Im Tab "Verwalten" können Sie für jeden Benutzer oder jede Gruppe, die im linken Baumansicht ausgewählt ist, folgendes tun:



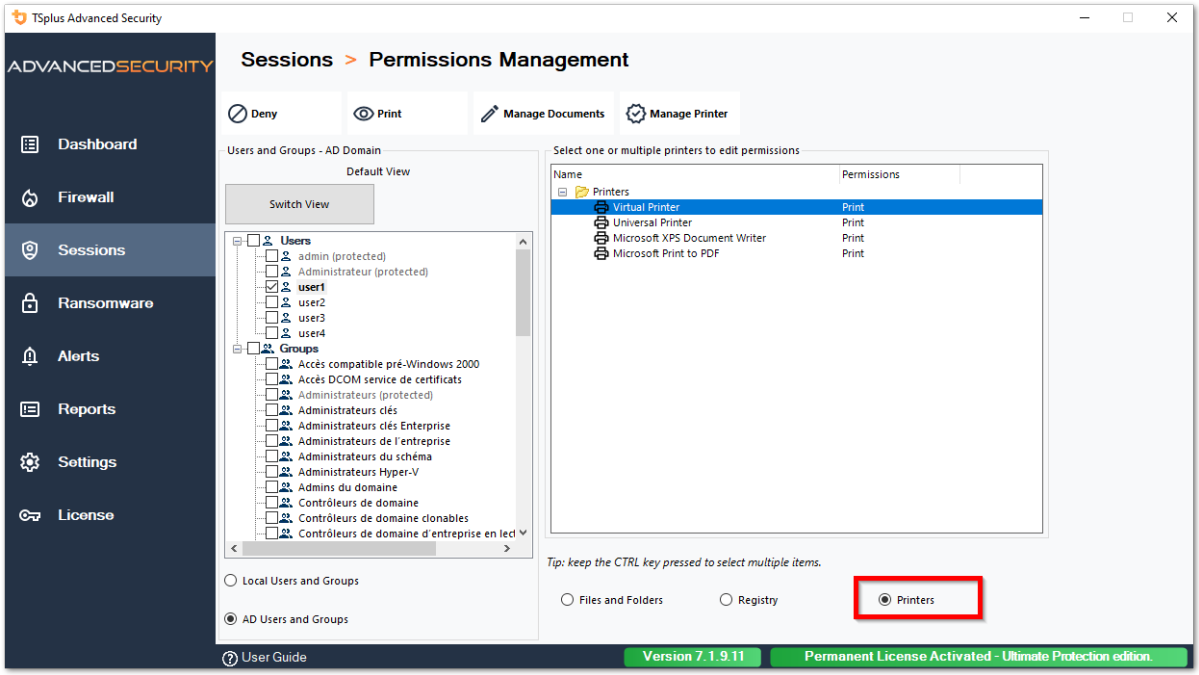


- **Verweigern** Wenn Sie auf die Schaltfläche Ablehnen klicken, wird dem ausgewählten Benutzer das Recht auf das ausgewählte Dateisystemobjekt verweigert. Wenn eine Datei ausgewählt ist, wird dem ausgewählten Benutzer das Recht verweigert, die ausgewählte Datei zu lesen (FileSystemRights.Read). Wenn ein Verzeichnis ausgewählt ist, wird dem ausgewählten Benutzer das Recht verweigert, den Inhalt des Verzeichnisses zu lesen und aufzulisten (FileSystemRights.Read und FileSystemRights.ListDirectory).
- **Lesen** Beim Klicken auf die Schaltfläche Lesen erhält der ausgewählte Benutzer das Recht auf das ausgewählte Dateisystemobjekt. Wenn eine Datei ausgewählt ist, erhält der ausgewählte Benutzer das Recht, die ausgewählte Datei zu lesen und auszuführen, wenn die Datei ein Programm ist (FileSystemRights.ReadAndExecute). Wenn ein Verzeichnis ausgewählt ist, erhält der ausgewählte Benutzer das Recht, den Inhalt des Verzeichnisses zu lesen und aufzulisten oder auszuführen (FileSystemRights.ReadAndExecute und FileSystemRights.ListDirectory und FileSystemRights.Traverse).
- **Ändern** Beim Klicken auf die Schaltfläche Ändern erhält der ausgewählte Benutzer die Berechtigung für das ausgewählte Dateisystemobjekt. Wenn eine Datei ausgewählt ist, erhält der ausgewählte Benutzer das Recht, die ausgewählte Datei zu ändern (FileSystemRights.Modify). Wenn ein Verzeichnis ausgewählt ist, erhält der ausgewählte Benutzer das Recht, den Inhalt des Verzeichnisses zu ändern und aufzulisten sowie neue Dateien oder Verzeichnisse zu erstellen (FileSystemRights.Modify und FileSystemRights.CreateDirectories und FileSystemRights.CreateFiles und FileSystemRights.ListDirectory und FileSystemRights.Traverse).
- **Eigentum** Wenn Sie auf die Schaltfläche Eigentum klicken, erhält der ausgewählte Benutzer die volle Kontrolle über das ausgewählte Dateisystemobjekt (FileSystemRights.FullControl).

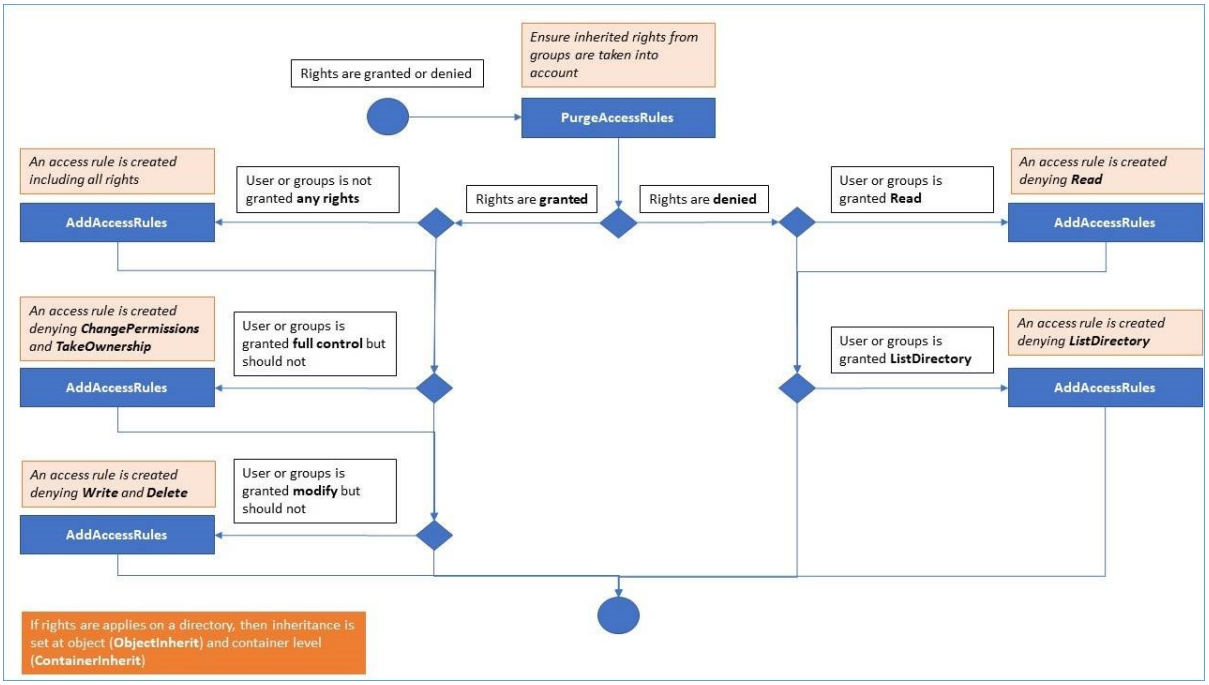
Die gleichen Berechtigungsoptionen sind für jedes Register möglich, indem Sie die entsprechende Schaltfläche unter der rechten Baumansicht auswählen.



Und für jeden Drucker:



Bitte beachten Sie, dass alle Berechtigungen, die einem Verzeichnis verweigert oder gewährt werden, rekursiv auf die im Verzeichnis enthaltenen Dateisystemobjekte angewendet werden. Das Diagramm unten zeigt die API-Aufrufe, wenn Rechte auf ein Dateisystemobjekt angewendet werden.

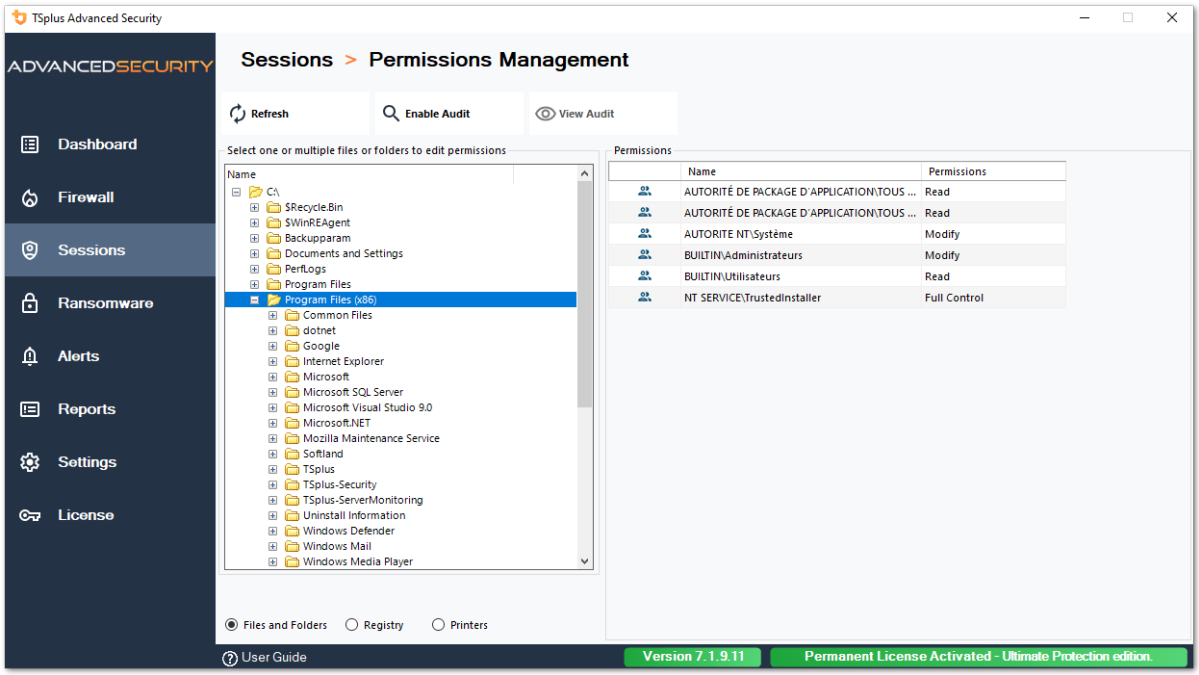


Dokumentation :

- Objektsicherheit: https://docs.microsoft.com/de-de/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- Dateisystemrechte: https://docs.microsoft.com/de-de/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

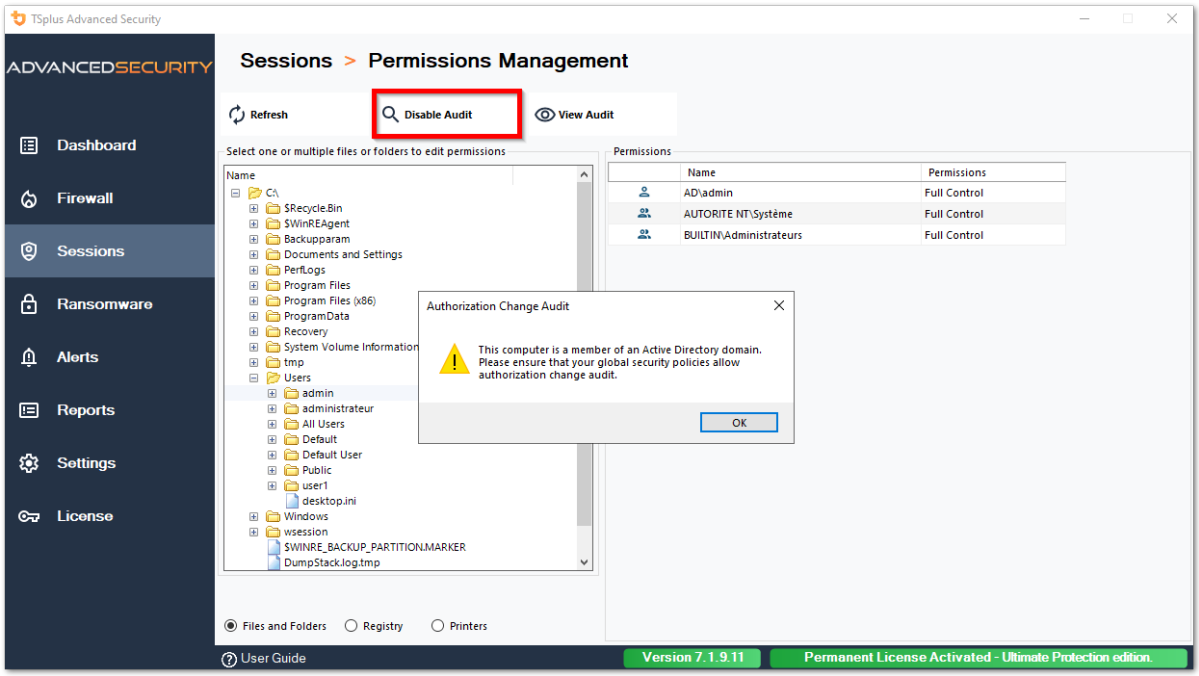
Berechtigungen überprüfen

Im Tab "Überprüfen" können Sie für jeden Ordner, Unterordner oder jede Datei, die im linken Baumansicht ausgewählt ist, die entsprechenden zugewiesenen Berechtigungen für Benutzer oder Gruppen in der rechten Baumansicht sehen.

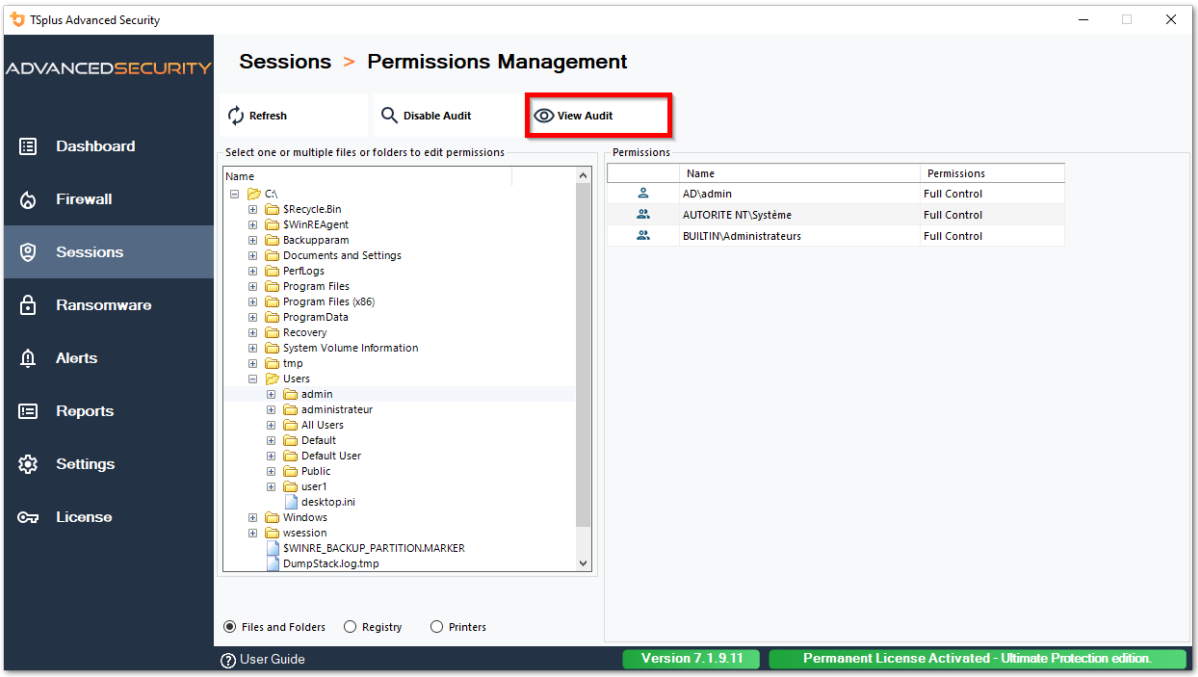


Sie können den Status der Ordner aktualisieren, damit sie in Echtzeit aktualisiert werden.

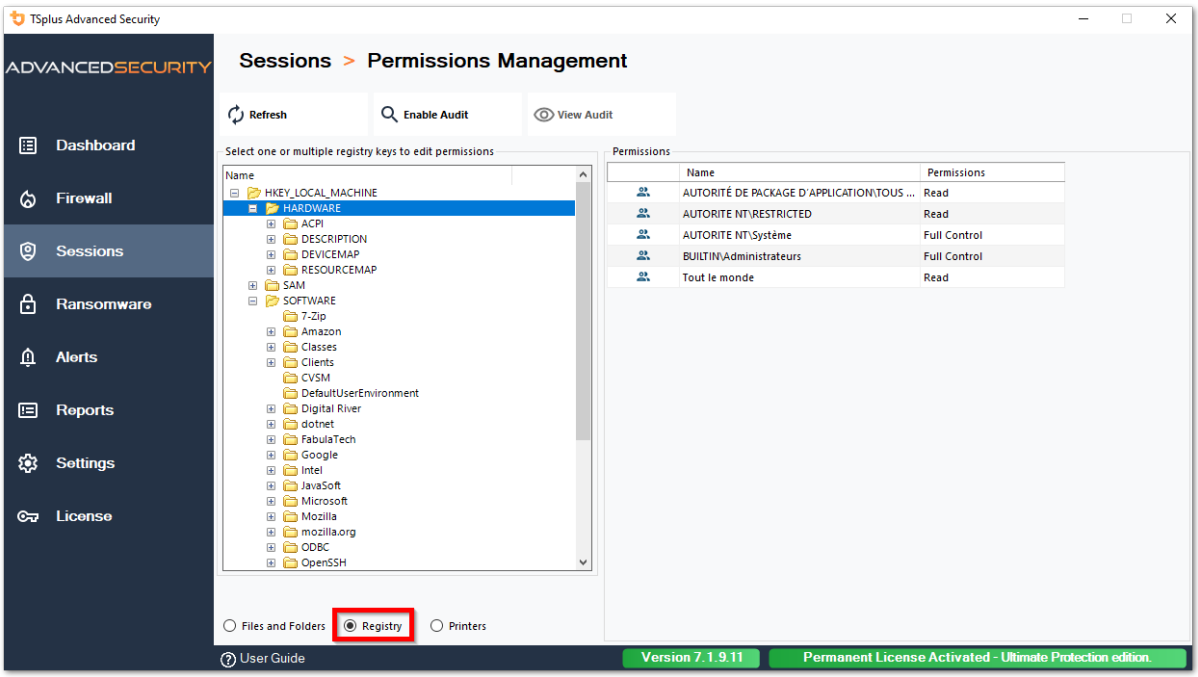
Eine Audit kann aktiviert werden, indem der gewünschte Ordner, Unterordner oder die Datei ausgewählt und auf die Schaltfläche „Audit aktivieren“ oben geklickt wird.

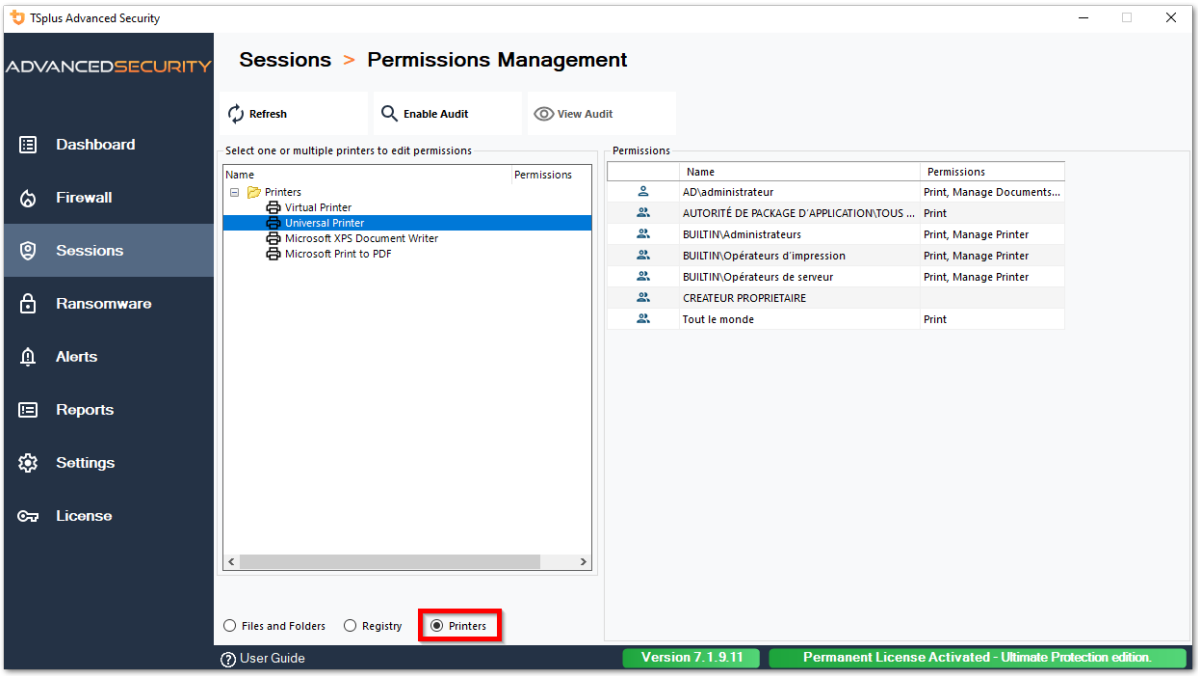


Der Button „Audit anzeigen“ ermöglicht es Ihnen, das entsprechende Audit im Ereignisprotokoll zu sehen:



Die gleichen Inspektionsmöglichkeiten sind für jedes Register und jeden Drucker verfügbar, indem Sie die entsprechende Schaltfläche unter der linken Baumansicht auswählen.




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 - Voraussetzungen

Hardware-Anforderungen

TSplus Advanced Security unterstützt 32-Bit- und 64-Bit-Architekturen.

Betriebssystem

Ihre Hardware muss eines der folgenden Betriebssysteme verwenden:

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

Sowohl 32- als auch 64-Bit-Architekturen werden unterstützt.

Softwareanforderungen

TSplus Advanced Security erfordert die folgenden Voraussetzungen:

- Laufzeit: .NET Framework 4.7.2 oder höher

- Microsoft Windows 7 SP1 und Windows 2008 R2 SP1 benötigen ein zusätzliches Update, um SHA2 Cross Signing zu unterstützen. KB4474419 Dieses Update ermöglicht es der integrierten Firewall und dem Ransomware-Schutz von TSplus Advanced Security,

ordnungsgemäß zu funktionieren.

Hinweis: Diese Voraussetzungen werden vom Installationsprogramm automatisch installiert, wenn sie im System fehlen.

TSplus Advanced Security - Erste Schritte

Voraussetzungen

TSplus Advanced Security erfordert die folgenden Voraussetzungen.

- Betriebssystem: Microsoft Windows Version 7, Service Pack 1 (Build 6.1.7601) oder Windows 2008 R2, Service Pack 1 (Build 6.1.7601) oder höher.

Die folgenden **Die Voraussetzungen werden automatisch vom Installationsprogramm installiert.** wenn fehlend:

- Laufzeit: .NET Framework 4.5.3 oder höher
- Microsoft Windows 7 SP1 und Windows 2008 R2 SP1 benötigen ein zusätzliches Update, um SHA2 Cross Signing zu unterstützen. KB4474419 Dieses Update ermöglicht es der integrierten Firewall und dem Ransomware-Schutz von TSplus Advanced Security, ordnungsgemäß zu funktionieren.

Bitte beziehen Sie sich auf die Dokumentation für weitere Details zu den Voraussetzungen.

Schritt 1: Installation

Das neueste TSplus Advanced Security-Setup-Programm ist hier immer verfügbar: Neueste TSplus Advanced Security-Setup-Programm Bitte laden Sie das Installationsprogramm herunter und folgen Sie dem Installationsassistenten.

TSplus Advanced Security-Setup-Programm erfordert normalerweise keinen Neustart Ihres Systems, um die Installation abzuschließen.

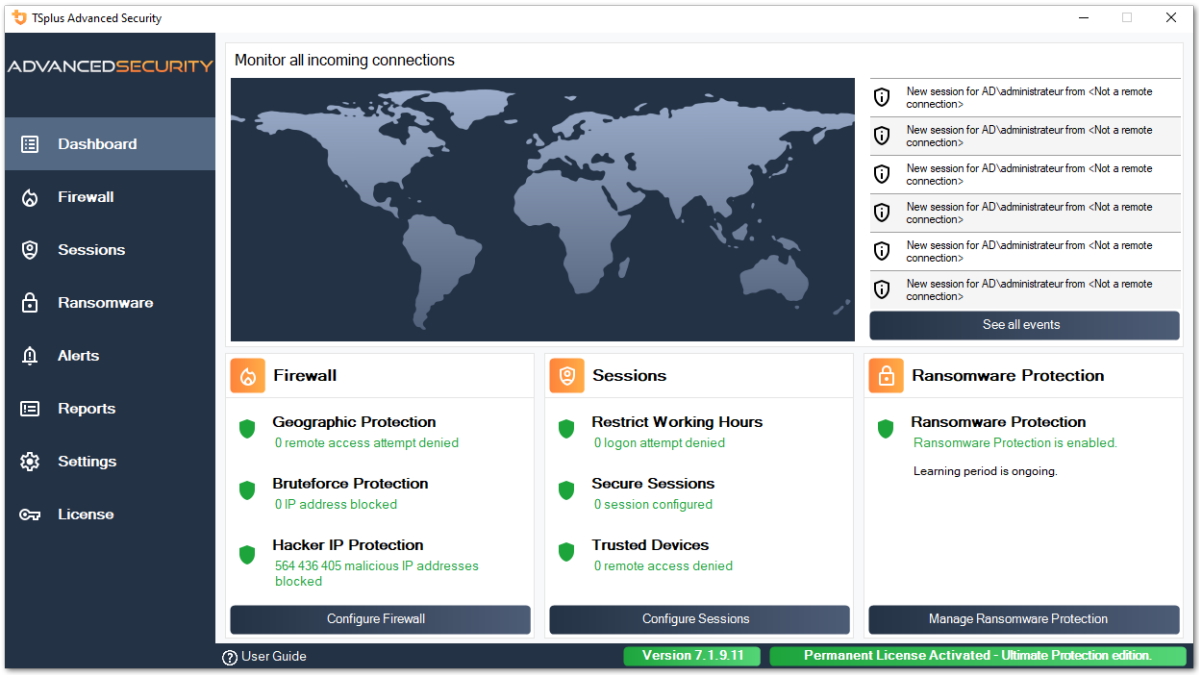
Jede neue Installation beginnt mit einer voll funktionsfähigen Testphase von 15 Tagen. Bitte zögern Sie nicht, um kontaktieren Sie uns Sollten Sie auf ein Hindernis stoßen oder ein Problem bei der Konfiguration von TSplus Advanced Security haben.

Sobald die Installation abgeschlossen ist, wird ein neues Symbol auf Ihrem Desktop angezeigt. Doppelklicken Sie auf dieses Symbol, um TSplus Advanced Security zu öffnen und die Sicherheitsfunktionen zu konfigurieren.

Bitte beziehen Sie sich auf die Dokumentation für vollständige Installationsanweisungen.

Schritt 2: Konfiguration von TSplus Advanced Security

Sie haben gestartet TSplus Advanced Security und begonnen, Funktionen zu konfigurieren, um Ihren Server vor böswilligen Aktivitäten zu schützen und strenge Sicherheitsrichtlinien durchzusetzen.



In der linken Spalte ermöglicht die Startseite einen schnellen Zugriff zur Konfiguration der Funktionen Ransomware-Schutz, Bruteforce-Schutz und geografischer Schutz.

Start Ransomware-Schutz der Lernzeitraum von ’s, um Advanced Security zu ermöglichen, legitime Anwendungen und Verhaltensweisen auf Ihrem System zu identifizieren, indem Sie auf das folgende Feld klicken:

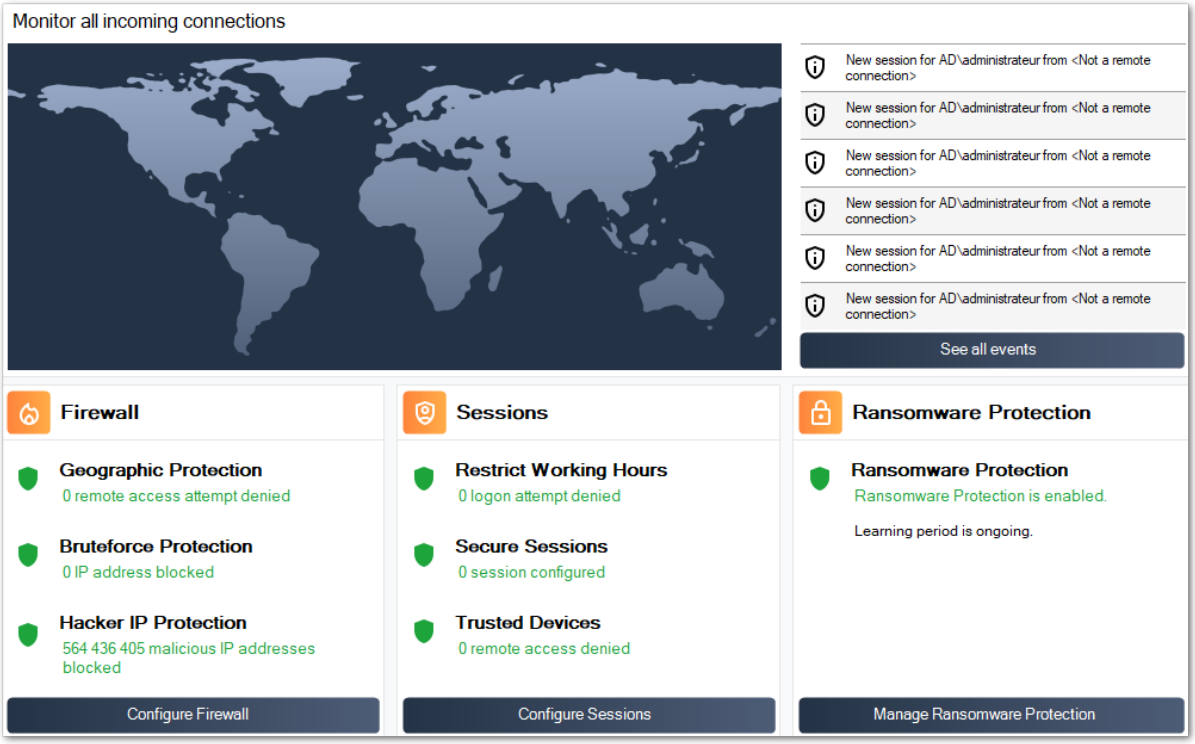
Bruteforce-Schutz ist normalerweise nach der Installation betriebsbereit. Andernfalls klicken Sie auf die **Wiederholte Verteidigung gegen Brute-Force-Angriffe** Titel zur Behebung von Problemen und Anwendung der erforderlichen Systemkonfiguration. Standardmäßig blockiert diese Funktion Angreifer nach 10 fehlgeschlagenen Anmeldeversuchen.

Fügen Sie schließlich Ihr Land zur Liste der autorisierten Länder hinzu, von denen aus Kunden eine Verbindung herstellen dürfen. Klicken Sie auf die Kachel. **Verbindungen aus einem anderen Land autorisieren** und fügen Sie Ihr Land hinzu, um es zu konfigurieren Geografischer Schutz

Sie sind bereit! Vergessen Sie nicht, zu aktivieren Sie Ihre Lizenz und zu aktualisieren Sie auf die neueste Version um den Schutz von Advanced Security optimal zu halten!

Schritt 3: Überprüfung der verhinderten Bedrohungen

Jetzt, da Sie die wichtigsten Funktionen der erweiterten Sicherheit konfiguriert haben, werden vermiedene Bedrohungen im Dashboard gemeldet.



Auch die Hacker-IP Der Schutz hält die Maschine gegen bekannte Bedrohungen geschützt, indem mehr als 500.000.000 bekannte bösartige IP-Adressen blockiert werden.

Alle die Sicherheitsereignisse kann durch Klicken auf die **Alle Veranstaltungen anzeigen** Fliese.

Schritt 4: Nutzung anderer Sicherheitsfunktionen zur Verbesserung des Schutzes

Am unteren Ende können vier weitere Sicherheitsfunktionen aufgerufen und konfiguriert werden, um den Schutz Ihres Geräts zu verbessern.

- Passen Sie die Zugriffsrechte auf Ihren lokalen Dateisystemen, Druckern und Registrierungsschlüsseln an und überwachen Sie diese, um sicherzustellen, dass jeder

Benutzer Zugriff auf relevante Ressourcen hat, mit dem Berechtigungen Funktion.

- Definieren Sie den Zeitraum, in dem Benutzer autorisiert sind, sich mit dem anzumelden. Working Hours Funktion. Benutzer werden nach ihren erlaubten Arbeitszeiten getrennt.

- Passen Sie Benutzersitzungen an und sichern Sie sie mit dem Sicherer Desktop Funktion. Passen Sie die Sitzungsschnittstelle für lokale Benutzer an, indem Sie Elemente anpassen, ausblenden oder den Zugriff verweigern.

- Überprüfen Sie den Namen des Remote-Clients, wenn ein Benutzer eine Verbindung zu Ihrem Computer herstellt mit Endpoint-Schutz Diese Funktion validiert die Client-Maschinenamen für jeden remote verbundenen Benutzer.

Es gibt mehr! Der Wechsel in den erweiterten Modus gewährt Ihnen Zugriff auf weitere Funktionen.

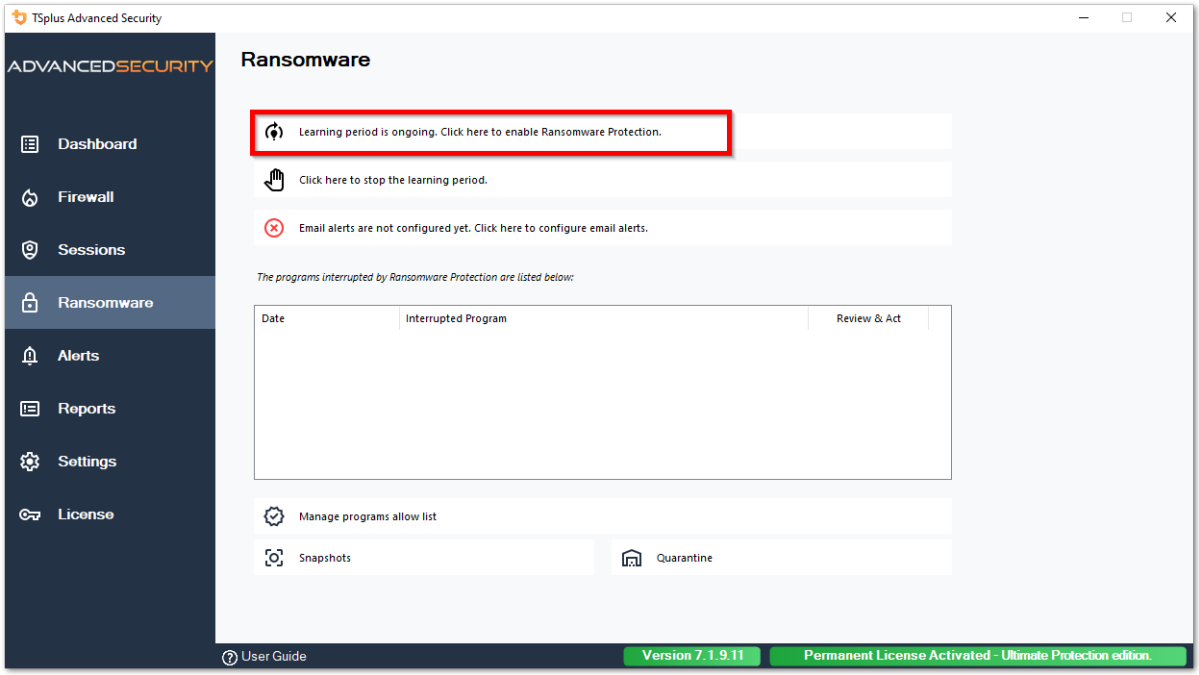
Vielen Dank, dass Sie TSplus Advanced Security verwenden!

Ransomware-Schutz

Der Ransomware-Schutz ermöglicht es Ihnen, Ransomware-Angriffe effizient ZU ERKENNEN, ZU BLOCKIEREN und ZU VERHINDERN. TSplus Advanced Security reagiert, sobald es Ransomware in Ihrer Sitzung erkennt. Es verfügt über sowohl **statische und verhaltensbasierte Analyse** :

- Die **statische Analyse** ermöglicht es der Software, sofort zu reagieren, wenn sich der Name einer Erweiterung ändert,
- Die **verhaltensanalyse** schaut sich an, wie ein Programm mit Dateien interagiert und neue Varianten von Ransomware erkennt.

Sie können es aktivieren, indem Sie auf die Schaltfläche „Ransomware-Schutz aktivieren“ im Tab für Ransomware-Schutz klicken:

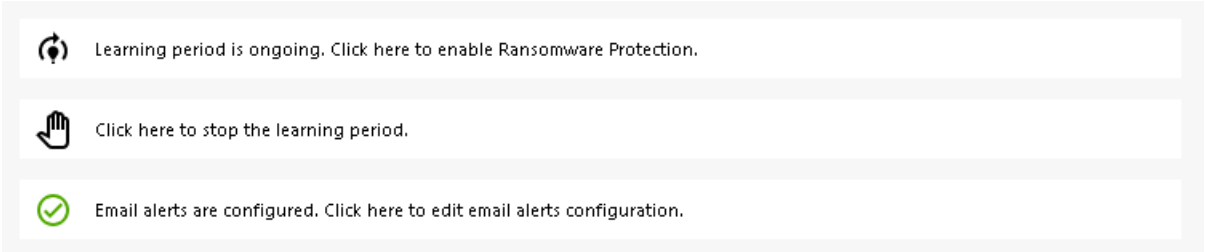


Lernzeit

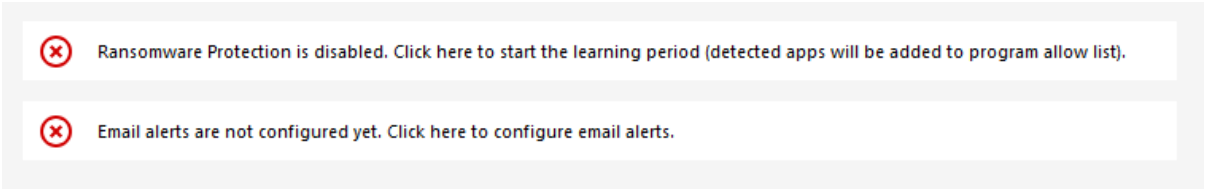
Nach der Aktivierung der Ransomware-Schutzfunktion wird der Lernzeitraum automatisch aktiviert. Während des Lernzeitraums werden alle Programme, die von der Ransomware-

Schutzfunktion erkannt werden, als falsch positiv betrachtet und können ihre Ausführung wieder aufnehmen. Die als falsch positiv erkannten Programme werden automatisch zur Liste der erlaubten Programme hinzugefügt.

Diese Funktion ermöglicht die Konfiguration des Ransomware-Schutzes auf einem Produktionsserver, ohne dessen Aktivität zu stören. Wir empfehlen, mit einer Lernphase von 5 Tagen zu beginnen, um alle legitimen Geschäftsanwendungen zu identifizieren.



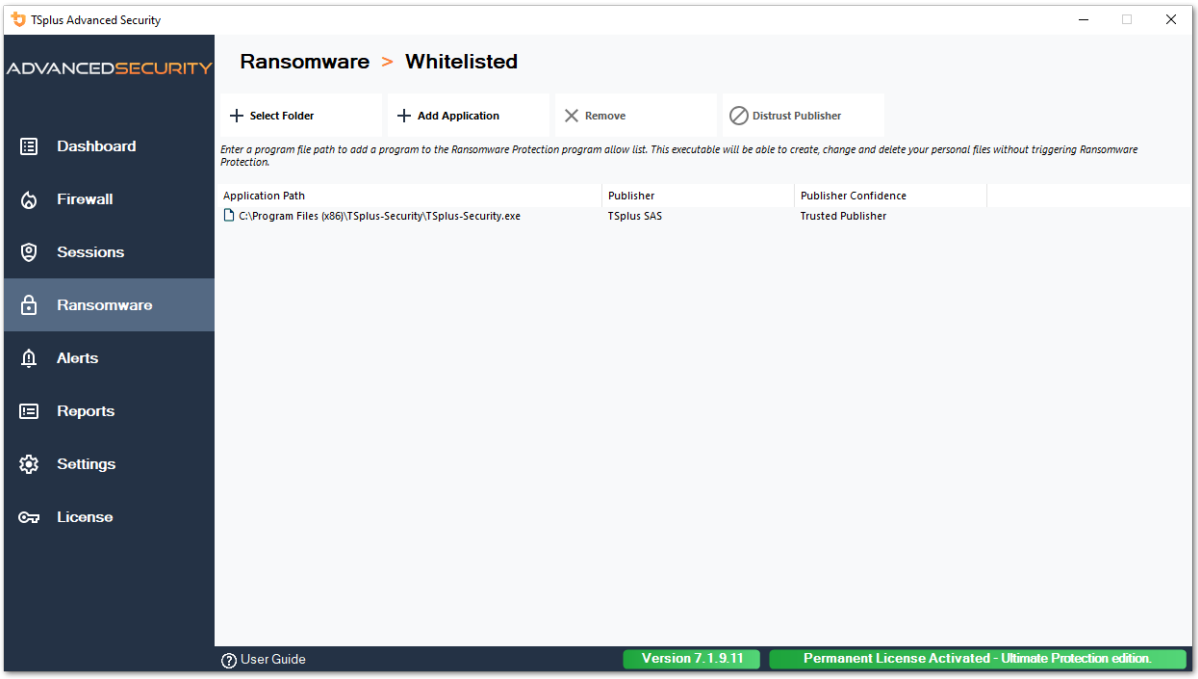
Wenn Sie die Lernphase stoppen, wird der Ransomware-Schutz deaktiviert. Klicken Sie auf die Schaltfläche „Ransomware-Schutz ist deaktiviert“, um die Lernphase reaktivieren.



Ransomware-Schutzmaßnahme

Es scannt schnell Ihre Festplatte(n) und zeigt die Datei(en) oder das Programm(e) an, die dafür verantwortlich sind, zusätzlich zu einer Liste der infizierten Elemente. TSplus Advanced Security stoppt automatisch den Angriff und quarantänisiert das Programm(e) zusammen mit den vor seiner Intervention verschlüsselten Datei(en).

Nur der Administrator kann sie auf die Whitelist setzen, indem er den Pfad des gewünschten Programms in die untere Zeile eingibt und auf „Hinzufügen“ klickt.



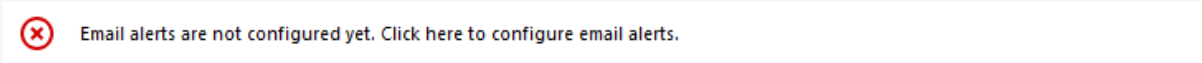
Ransomware-Schutzbericht

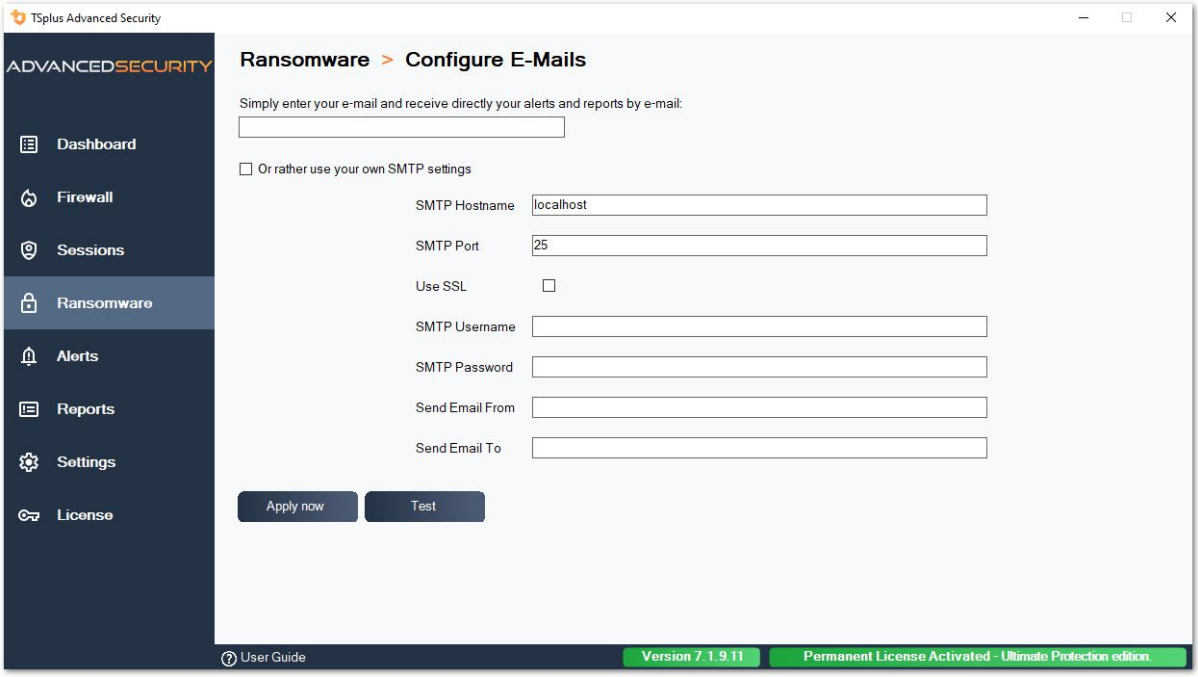
TSplus Advanced Security verhindert katastrophale Ereignisse für Unternehmen, indem es Ransomware in einem frühen Stadium entfernt.

Der Administrator hat Zugriff auf Informationen über die Quelle des Angriffs und die laufenden Prozesse und lernt daher, wie man diese Bedrohungen antizipiert.

Hinweis Ransomware-Schutz beobachtet, wie Programme mit System- und persönlichen Dateien interagieren. Um ein höheres Schutzniveau zu gewährleisten, erstellt Ransomware-Schutz Köderdateien in wichtigen Ordnern, in denen Ransomware häufig ihren Angriff beginnt. Daher können einige versteckte Dateien in den Desktop- und Dokumentenordnern der Benutzer sowie an anderen Orten erscheinen. Wenn es ein bösartiges Verhalten erkennt, stoppt es die Ransomware sofort (oder fragt, ob der angemeldete Benutzer ein Administrator ist). Ransomware-Schutz verwendet reine verhaltensbasierte Erkennungstechniken und verlässt sich nicht auf Malware-Signaturen, wodurch es Ransomware erfassen kann, die noch nicht existiert.

Sie können Ihre SMTP-Einstellungen konfigurieren, damit TSplus Advanced Security Ihnen E-Mail-Benachrichtigungen sendet, um wichtige Sicherheitsereignisse hervorzuheben, indem Sie auf die Schaltfläche unter der Ransomware-Aktivierung klicken:





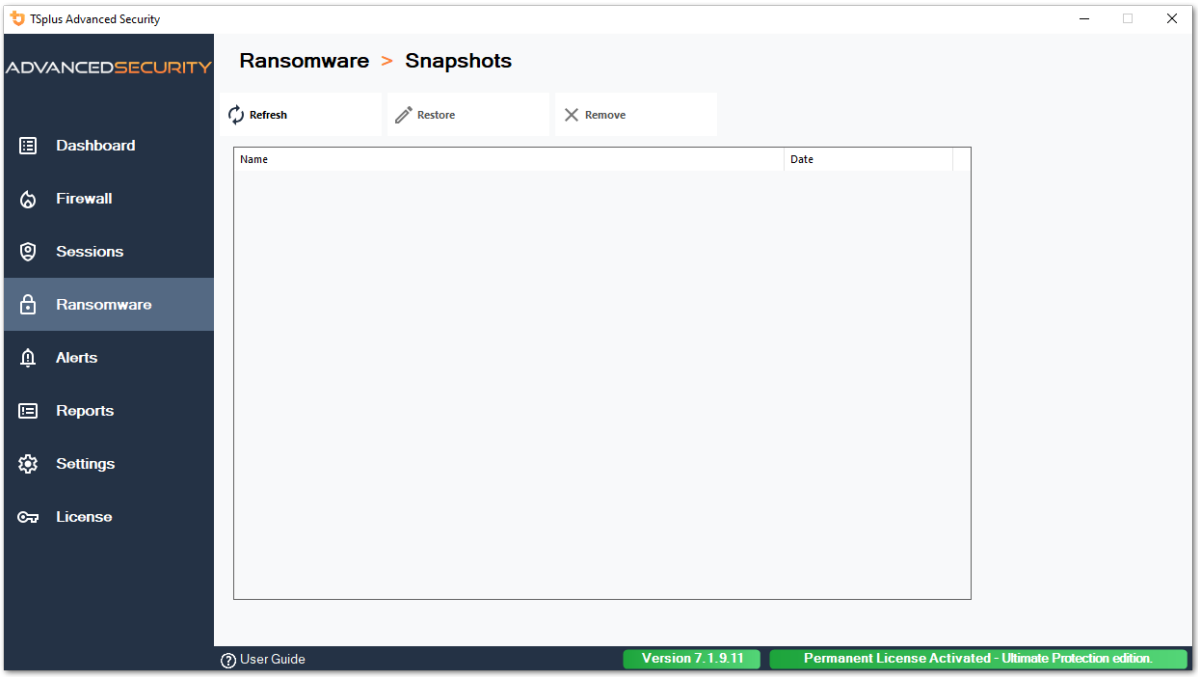
Geben Sie Ihren SMTP-Hostnamen, Port ein und aktivieren Sie das Kontrollkästchen "SSL verwenden" und ändern Sie den Port von 25 auf 465, wenn Sie SSL verwenden möchten.

Geben Sie den SMTP-Benutzernamen und das Passwort sowie die Absender- und Empfängeradressen ein.

E-Mail-Einstellungen können validiert werden, indem ein Test gesendet wird, wenn die SMTP-Einstellungen gespeichert werden.

Schnappschüsse

Snapshots, die von Ransomware Protection erstellt wurden, sind unter dem Tab "Snapshots" sichtbar:

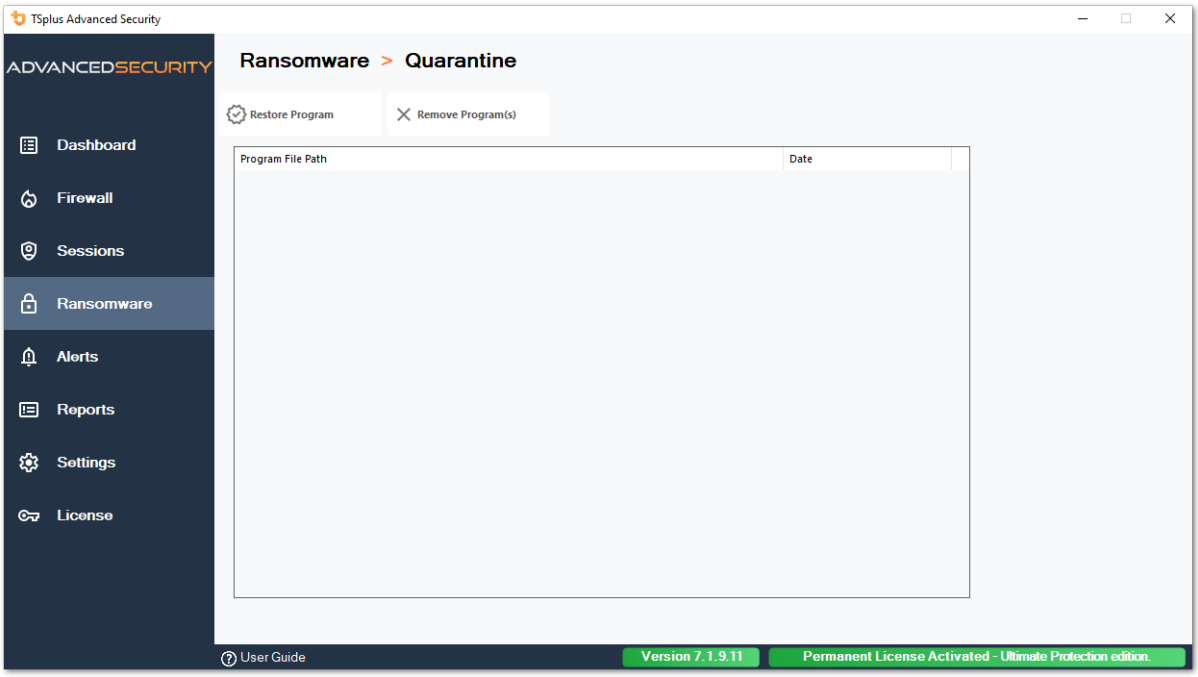


Die Liste kann durch Klicken auf die entsprechende Schaltfläche aktualisiert werden. Jedes Element kann wiederhergestellt oder entfernt werden.

Quarantäne

Quarantäneprogramme sind unter dem Tab Quarantäne sichtbar:
Potenziell unerwünschte Programme werden unbegrenzt in Quarantäne gehalten, bis Sie eine Entscheidung über die zu ergreifende Maßnahme treffen.

Auf diese Weise gewährleistet Advanced Security die Sicherheit Ihres Geräts, während Sie die Möglichkeit haben, quarantänisierte Elemente nach Ihren Wünschen zu verwalten.
Dies kann nützlich sein, wenn Sie eine Datei oder ein Programm abrufen müssen, das neutralisiert wurde. **Diese Entscheidung erfolgt auf eigenes Risiko.**
Sie können auch dauerhaft alle Dateien oder Programme, die Sie auswählen, direkt aus dem Quarantäneordner im Installationsverzeichnis von Advanced Security löschen.



Jedes Element kann wiederhergestellt oder entfernt werden.

Ignorierte Dateien werden nicht verwendet, um mögliche bösartige Aktionen zu erkennen, und werden nicht gespeichert, wenn sie geändert werden. Die Idee ist, jegliche Operationen an großen oder irrelevanten Dateien (wie Protokolldateien) auszuschließen.

- sys
- dll
- exe
- tmp
- ~tmp
- temp
- Cache
- lnk
- 1
- 2
- 3
- 4
- 5
- LOG1
- LOG2
- customDestinations-ms
- Protokoll
- wab~
- vmc
- vhd
- vhdx
- vdi
- vo1

- vo2
- vsv
- vud
- iso
- dmg
- Sparseimage
- Kabine
- msi
- mui
- dl_
- wim
- ost
- o
- qtch
- ithmb
- vmdk
- vmem
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- Menüdaten
- App-Icon
- App-Informationen
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- drk
- Speicher
- nvram
- hdd
- pk3
- pf
- trn
- automatischeZielorte-ms

Achtung bezüglich der Backup-Dateierweiterung

Die Dateierweiterung, die zum Speichern von modifizierten Dateien verwendet wird, ist: **Schnappschuss.** Der Treiber verbietet jegliche Änderungs- oder Löschaktionen an diesen Dateien, außer durch den TSplus Advanced Security-Dienst. Das Stoppen des Dienstes löscht die gesicherten Dateien. Um diese Dateien manuell zu löschen, müssen Sie den Treiber

vorübergehend entladen.

Sicherungskonfiguration

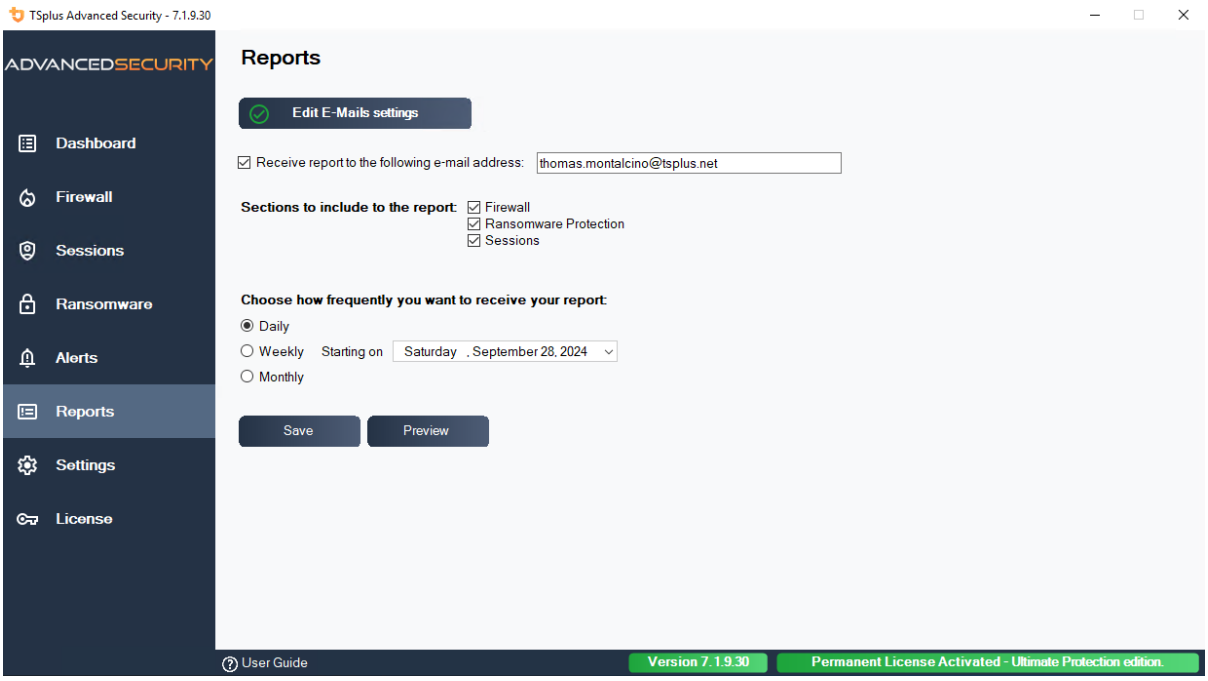
Standardmäßig befindet sich das Verzeichnis der gespeicherten Dateien im Installationsverzeichnis von TSplus Advanced Security und wird „Snapshots“ genannt. Es ist jedoch möglich, einen anderen Speicherort für dieses Verzeichnis festzulegen. Dies ermöglicht es dem Administrator, ein Verzeichnis auf einer schnelleren Festplatte (SSD) oder auf einer größeren Festplatte entsprechend seinen Bedürfnissen zu definieren. Der Pfad des Sicherungsverzeichnisses darf kein UNC-Pfad in der Form von sein:

\\ \ \

Backup-Dienstprogramme zur Whitelist hinzufügen

Wir empfehlen, Backup-Utilities in die Whitelist aufzunehmen.

Berichte


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.

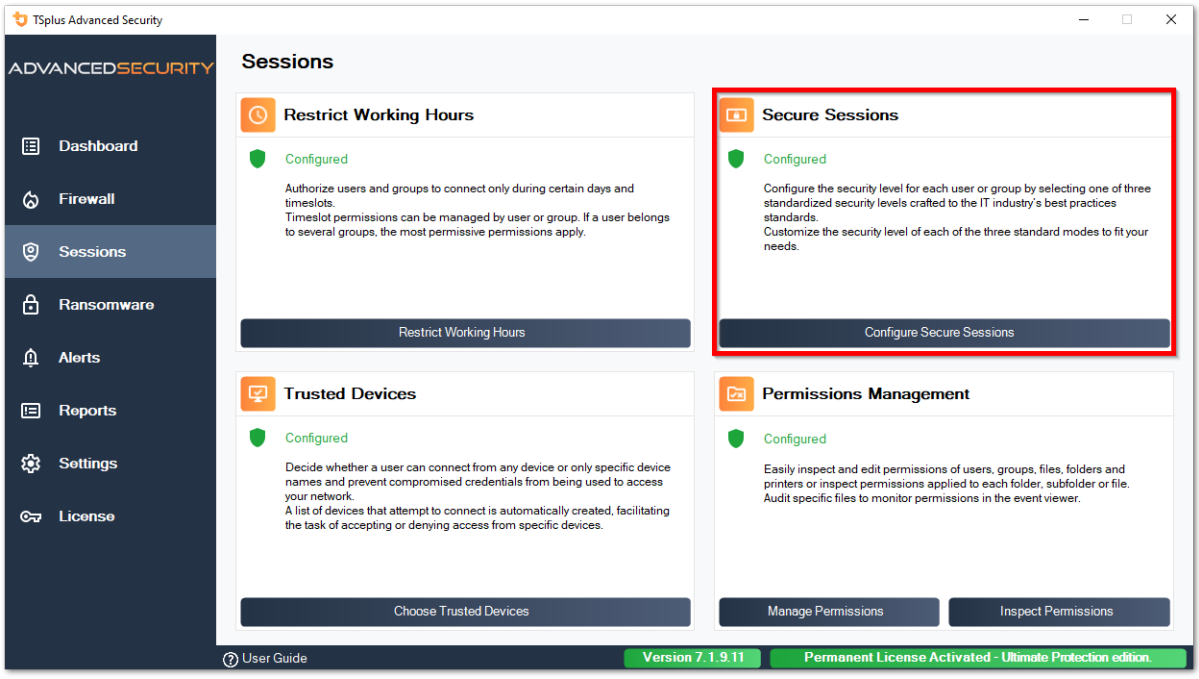
Sichere Sitzungen

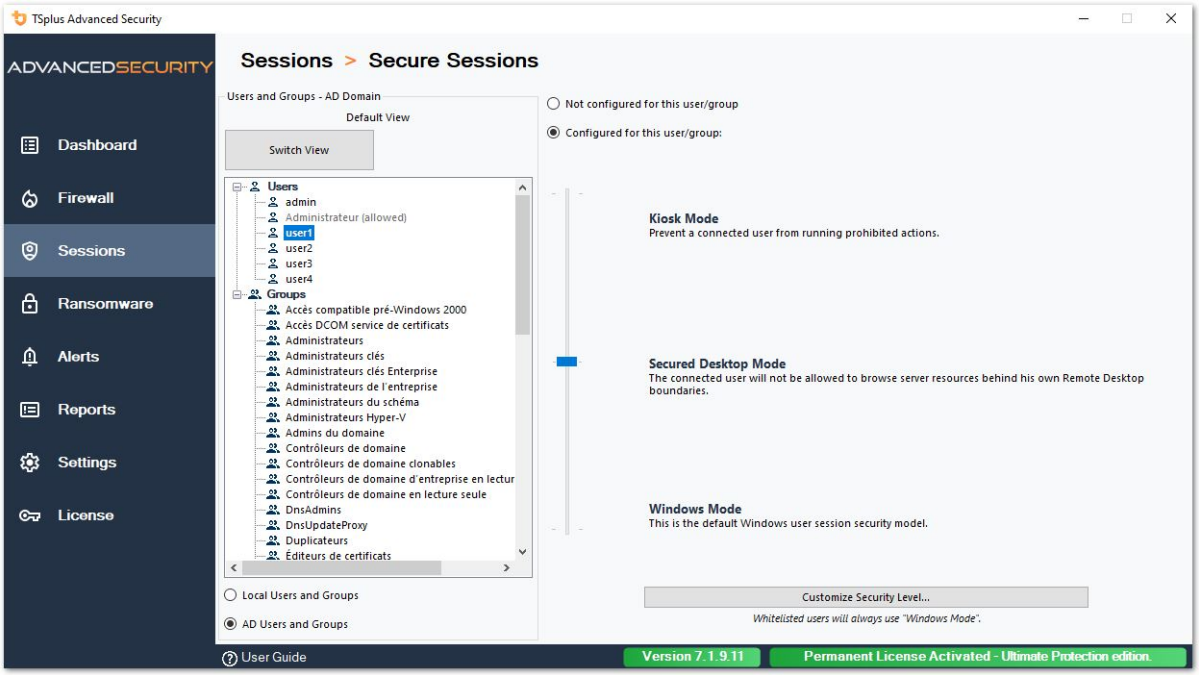
Warnung

- Sichere Sitzungen werden sehr wahrscheinlich mit den von Active Directory definierten Sicherheitsrichtlinien in Konflikt stehen.
- Der Hauptzweck von Secure Sessions besteht darin, die Benutzeroberfläche anzupassen, nicht Zugriffsberechtigungen anzuwenden. Seine Verwendung sollte mit der Funktion Berechtigungen kombiniert werden, um den Zugriff auf verschiedene Laufwerke zu sichern.

Sie können das Sicherheitsniveau für jeden Benutzer oder jede Gruppe konfigurieren. Es gibt drei Sicherheitsniveaus:

- Die **Windows-Modus** , wo der Benutzer Zugriff auf eine standardmäßige Windows-Sitzung hat.
- Die **Sichere Sitzungsmodus** wo der Benutzer keinen Zugriff auf die Systemsteuerung, Programme, Laufwerke, den Browser, kein Rechtsklick hat…: kein Zugriff auf die Serverressourcen. Er hat nur Zugriff auf Dokumente, Drucker, die Windows-Taste und kann seine Sitzung trennen.
- Die **Kiosk-Modus** ist die sicherste, bei der der Benutzer in seiner Sitzung sehr eingeschränkte Aktionen hat.

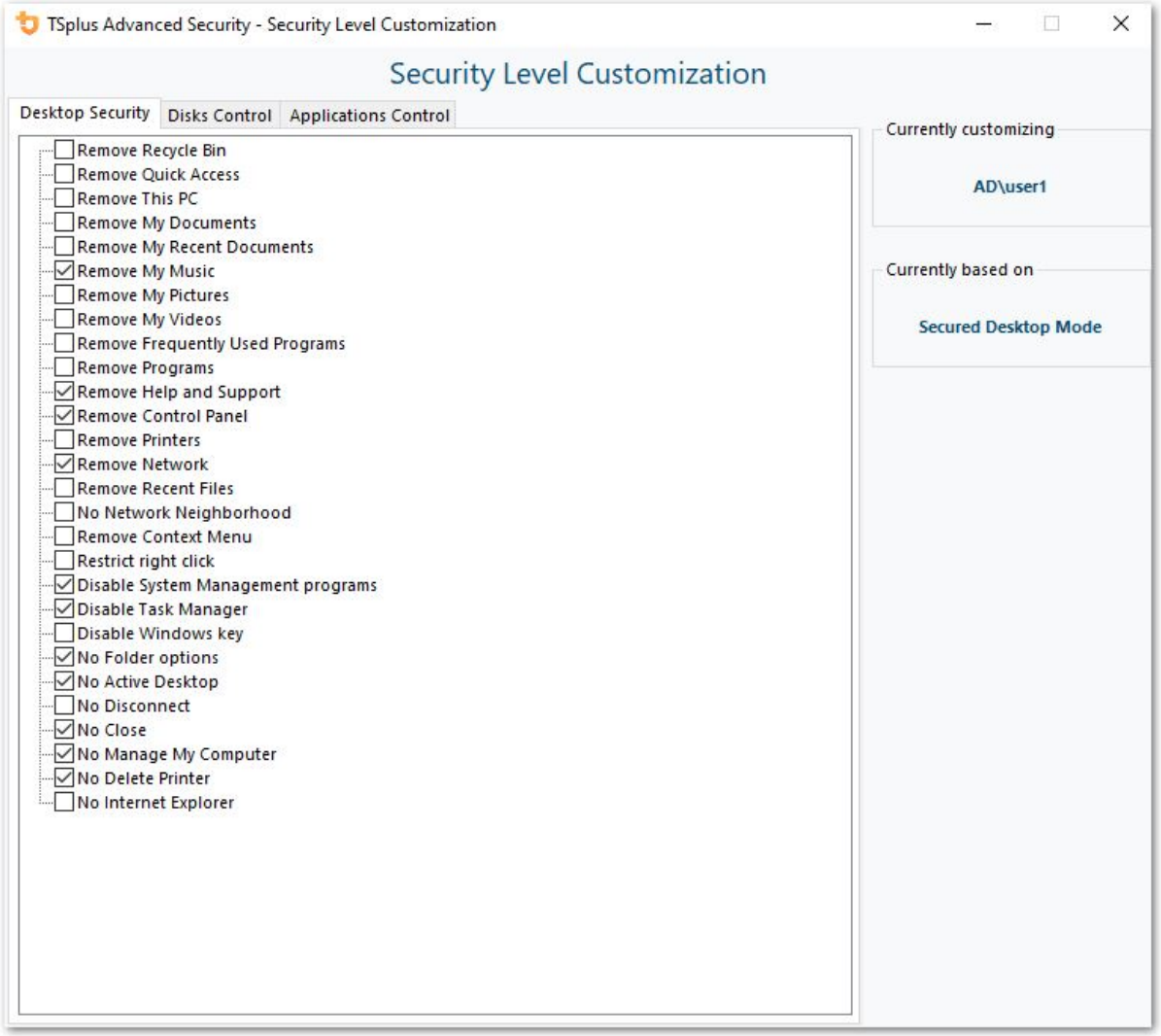




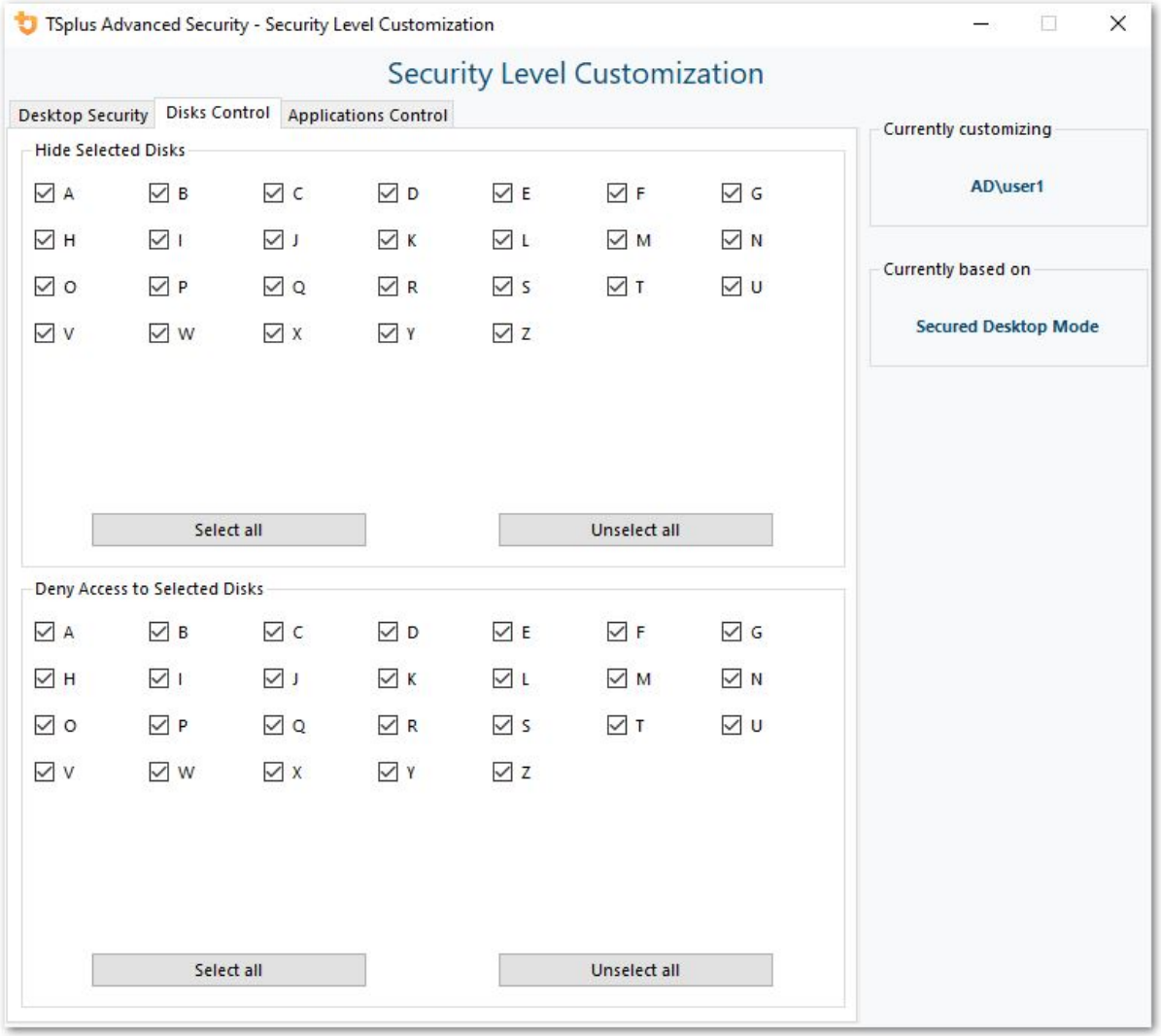
Anpassung

In jedem Modus haben Sie die Möglichkeit, die Sicherheit auf drei Ebenen anzupassen:

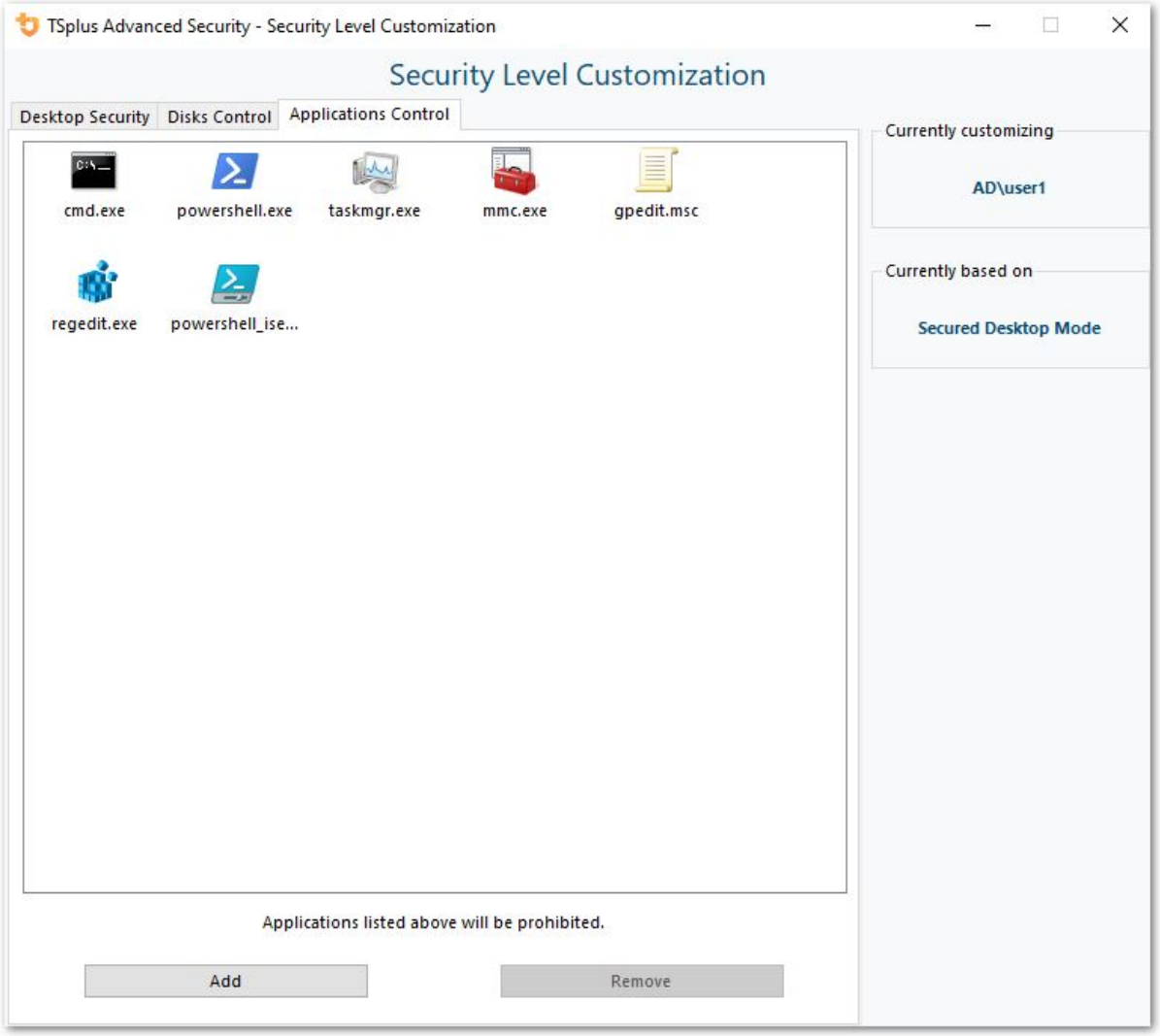
Desktop-Sicherheit:



Festplattensteuerung:



Anwendungssteuerung:



Benutzer-/Gruppenregelprioritäten

Wenn ein Benutzer eine neue Sitzung auf dem Server öffnet:

1. Wenn dieser Benutzer ein direkt für ihn definiertes Sicherheitsniveau hat, wird dieses Sicherheitsniveau durchgesetzt.
2. Wenn dieser Benutzer kein direkt für ihn definiertes Sicherheitsniveau hat, lädt TSplus Advanced Security die vorhandenen Sicherheitseinstellungen für alle Gruppen dieses Benutzers und behält die permissiveren Regeln bei.

Wenn beispielsweise eine erste Gruppe die Regel hat, das Symbol für den Papierkorb vom Desktop zu entfernen, diese Regel jedoch für eine zweite Gruppe deaktiviert ist, hat der Benutzer das Symbol für den Papierkorb auf seinem Desktop. Die gleichen Prioritätsregeln gelten für jede benutzerdefinierte Regel (Desktop-Sicherheit, Festplattenkontrolle und Anwendungssteuerung) sowie für das Hauptsicherheitsniveau (der Windows-Modus wird als permissiver angesehen als der gesicherte Desktop-Modus, der als permissiver angesehen wird als der Kiosk-Modus).

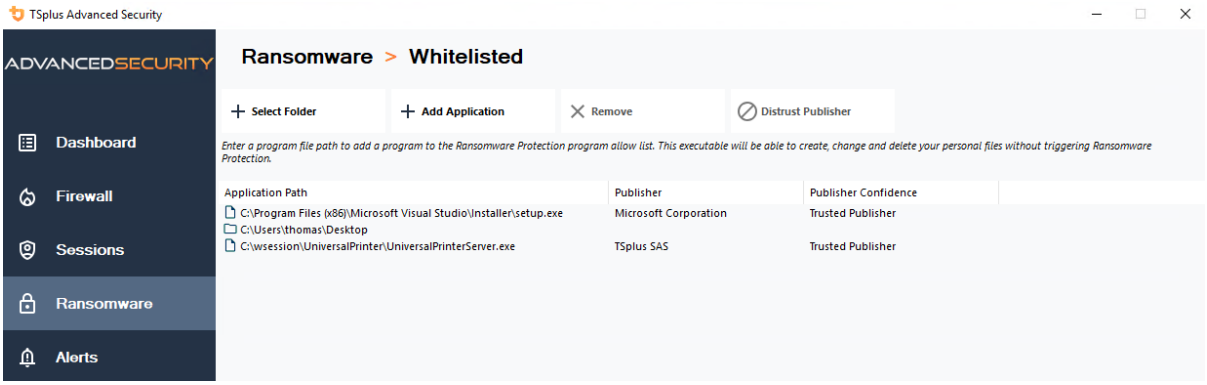
Hinweis: Um das Rechtsklicken überall zu deaktivieren, müssen Sie die folgenden beiden

Optionen auswählen:

- Rechtsklick einschränken
- Kontextmenü entfernen

Einstellungen - Programme Zulassungsliste

Auf dem **Programme-Registerkarte** , Sie können Programme zur Liste der erlaubten Programme hinzufügen, die nicht von der Ransomware-Schutzfunktion von TSplus Advanced Security überprüft werden. Standardmäßig sind alle Microsoft-Programme auf der Whitelist.



Klicken Sie auf die Schaltfläche „Anwendung hinzufügen“, um ein Programm hinzuzufügen. Sie können sie auch entfernen, indem Sie die Anwendung(en) auswählen und auf die Schaltfläche Anwendung(en) entfernen klicken.

Einstellungen - Benutzerzulassungsliste

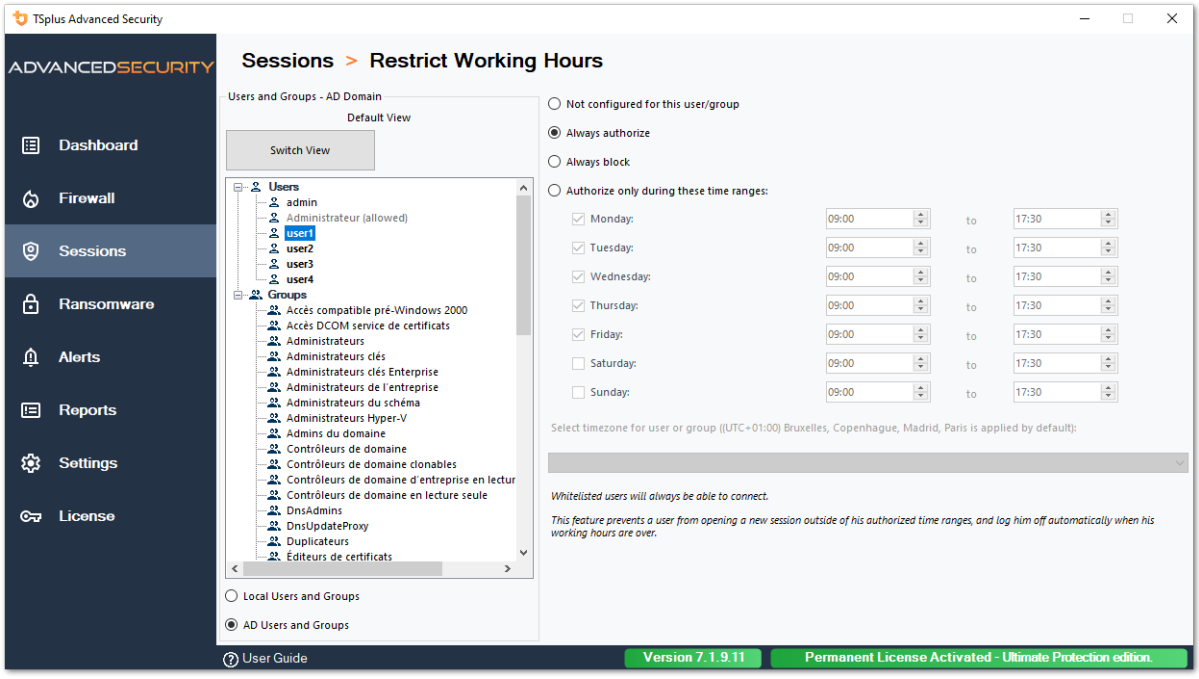
Erweiterte Ansicht

Mit der erweiterten Ansicht können Sie Benutzer und Gruppen aus allen zugänglichen Domänen hinzufügen und verwalten.

Sie können die Ansicht von der Standardansicht zur Erweiterten Ansicht wechseln, indem Sie die Schaltfläche „Ansicht wechseln“ verwenden.

Die erweiterte Ansicht wird verwendet, um alle aktuell konfigurierten Benutzer und Gruppen anzuzeigen und zu verwalten. Sie ermöglicht es Ihnen auch, neue Benutzer und Gruppen zur Liste hinzuzufügen, um sie ebenfalls zu konfigurieren, indem Sie den Windows AD-Suchauswähler verwenden. Sie können dies tun, indem Sie auf die Schaltfläche „Benutzer/Gruppen hinzufügen“ klicken. Sie können dann jeden verfügbaren Benutzer aus allen zugänglichen Domänen von Ihrem Server hinzufügen.

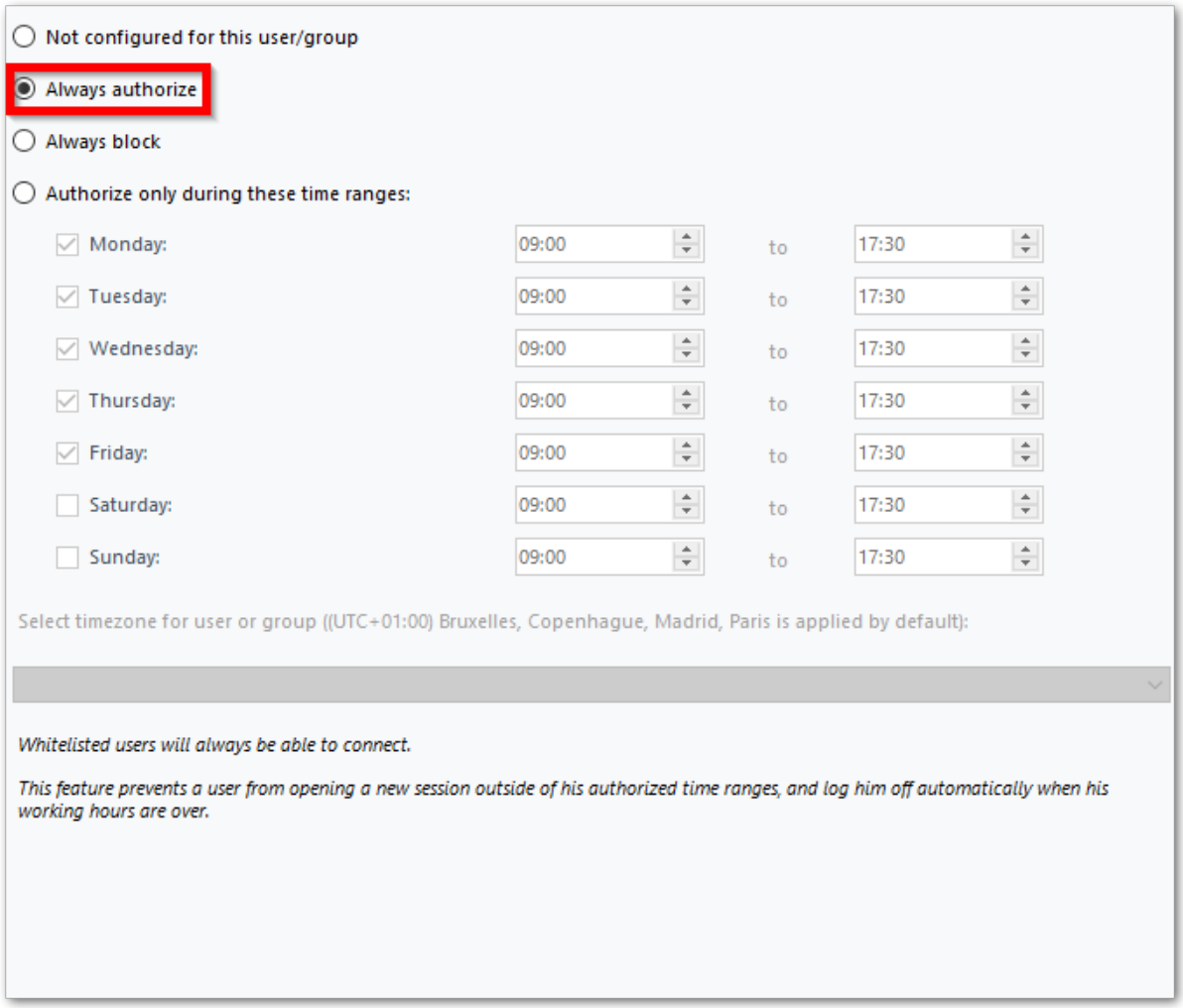
Die erweiterte Ansicht ist auf den Funktionen Berechtigungen, Arbeitszeiten, sichere Desktops verfügbar. Beispiel:



Die **Benutzer-Whitelist** Tab gibt dem Administrator die Möglichkeit, zu Benutzer zur Whitelist hinzufügen/entfernen .

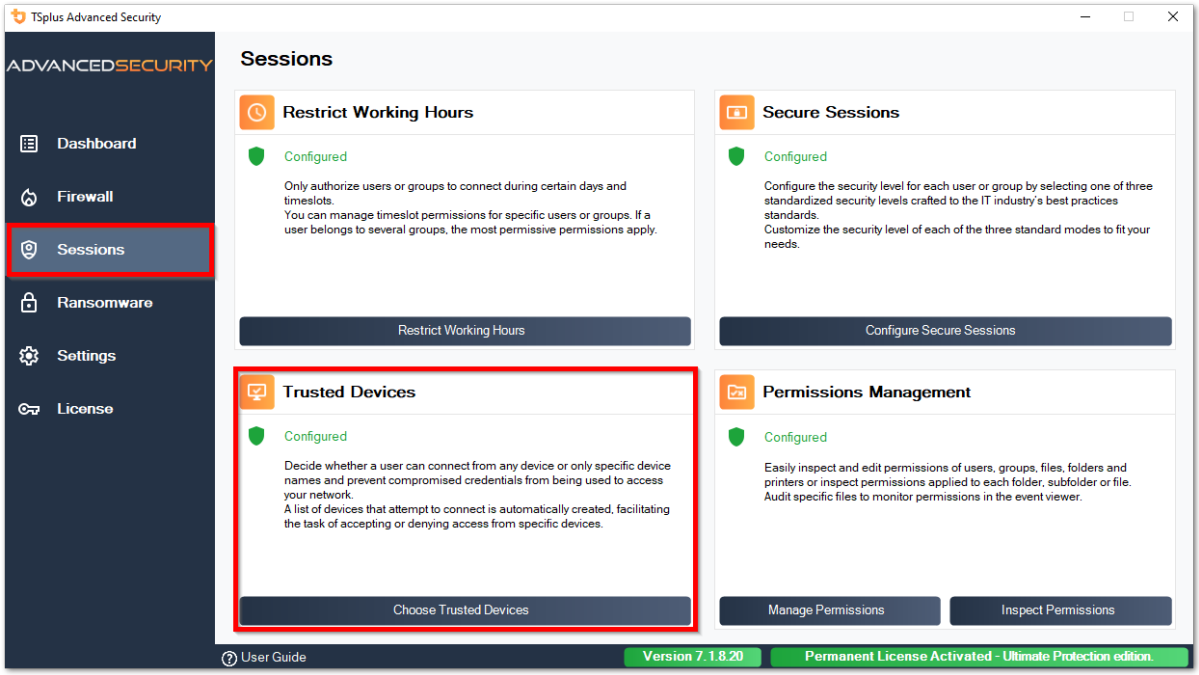
Benutzer auf der Whitelist werden von TSplus Advanced Security ignoriert und ihre Einstellungen werden nicht angewendet.

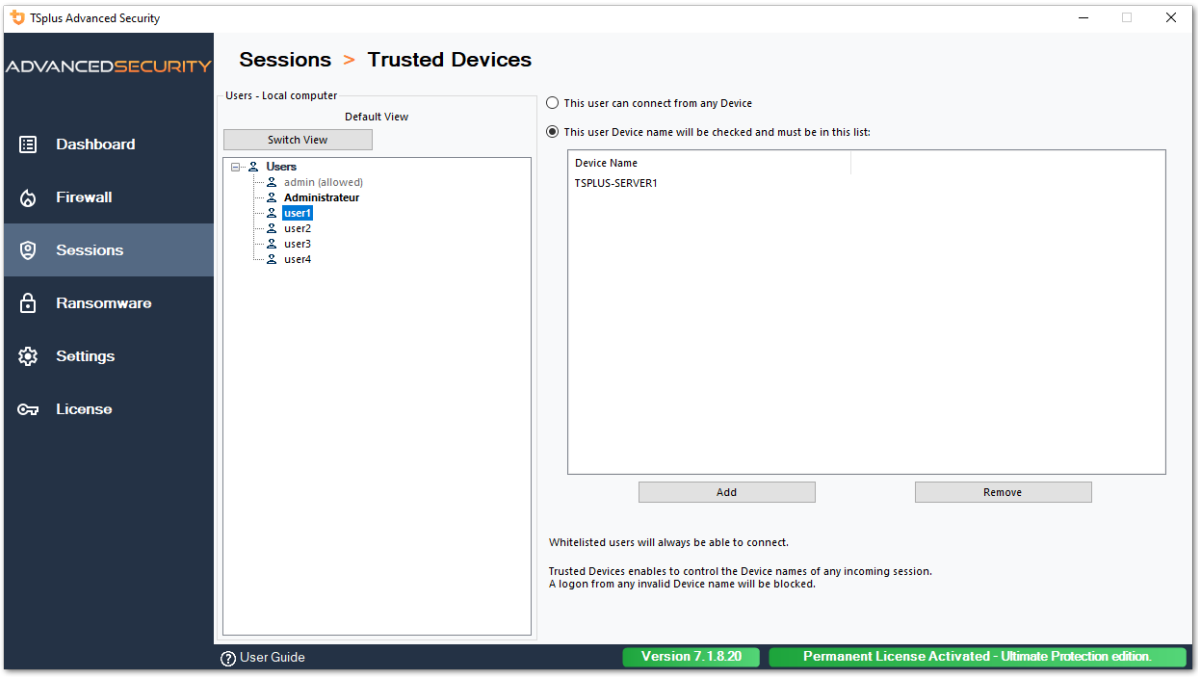
Der Benutzer, der TSplus Advanced Security installiert hat, wird automatisch zur Whitelist hinzugefügt:



Vertrauenswürdige Geräte

Trusted Devices ermöglicht es Ihnen, die Geräte der Benutzer zu steuern, indem jeder Benutzer nur ein oder mehrere spezifische Gerät(e) verwenden darf, die bei jeder eingehenden Sitzung überprüft werden. Ein Anmeldeversuch von einem ungültigen Gerätenamen wird blockiert.





In diesem Beispiel, **Benutzer1** wird den Gerätenamen verwenden **TSPLUS-SERVER1** nur.

Automatische Ausfüllung des Gerätebezeichnungsfelds

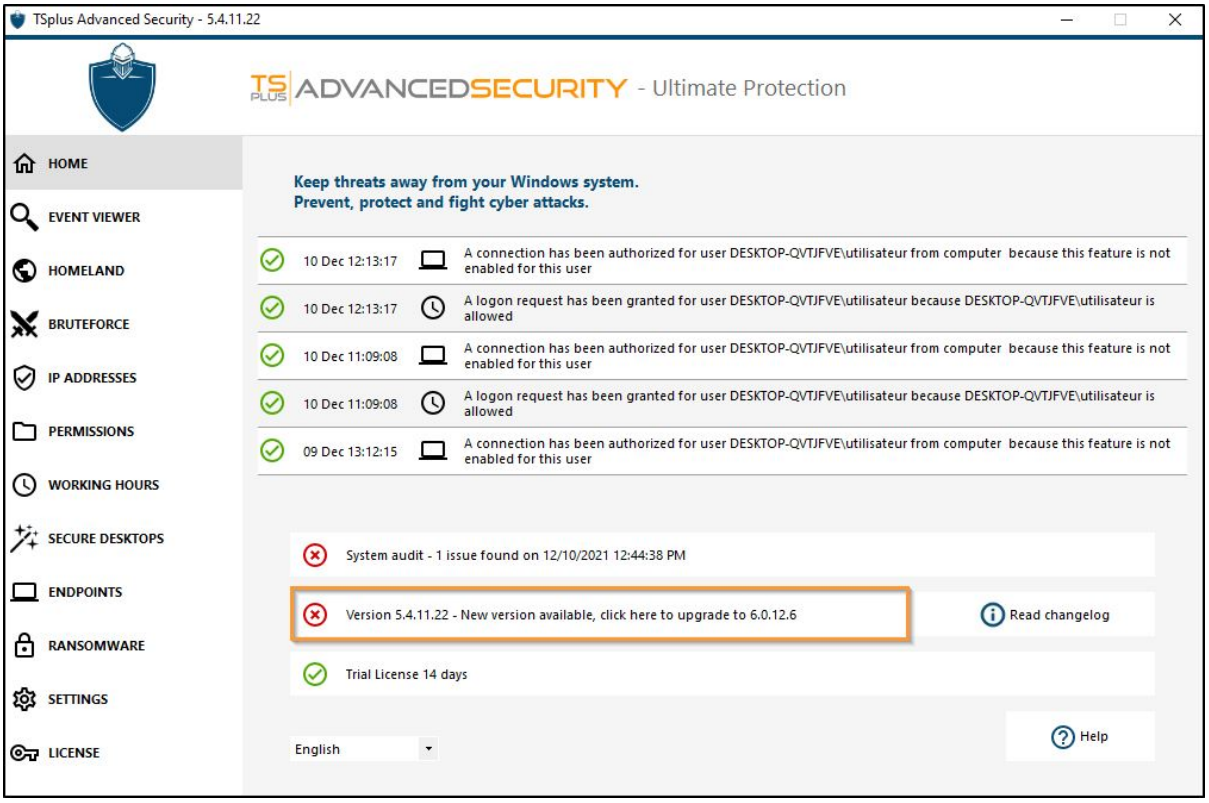
Sie werden möglicherweise feststellen, dass das Feld für den Gerätenamen bereits für einige Benutzer mit einem Gerätenamen ausgefüllt ist. Um dem Administrator zu helfen, wird TSplus Advanced Security automatisch den Namen des zuletzt verwendeten Geräts speichern, das von einem Benutzer, der die Funktion Vertrauenswürdige Geräte nicht aktiviert hat, zur Verbindung mit dem Server verwendet wurde. Nach einem Arbeitstag wird der Gerätename der meisten Benutzer von Advanced Security bekannt sein, sodass Sie die Funktion Endpoint Protection schnell aktivieren können, ohne den Namen jedes Arbeitsplatzes des Benutzers überprüfen zu müssen.

Hinweis Trusted Devices ist nicht mit HTML5-Verbindungen kompatibel.

Aktualisierung von TSplus Advanced Security

Überprüfen Sie unsere Fehlerbehebungen und Verbesserungen, indem Sie auf klicken Änderungsprotokoll

Das Aktualisieren von TSplus Advanced Security ist einfach und kann durch Klicken auf das entsprechende Kachel auf der Startseite erfolgen:



Dann lädt TSplus Advanced Security das Update herunter und wendet es an.

Hinweis: Ihre Daten und Einstellungen werden immer vor einem Update gesichert und können im Verzeichnis „archives“ im Setup-Ordner von TSplus Advanced Security gefunden werden. Sichern und Wiederherstellen Ihrer Daten und Einstellungen

Arbeitszeiten einschränken

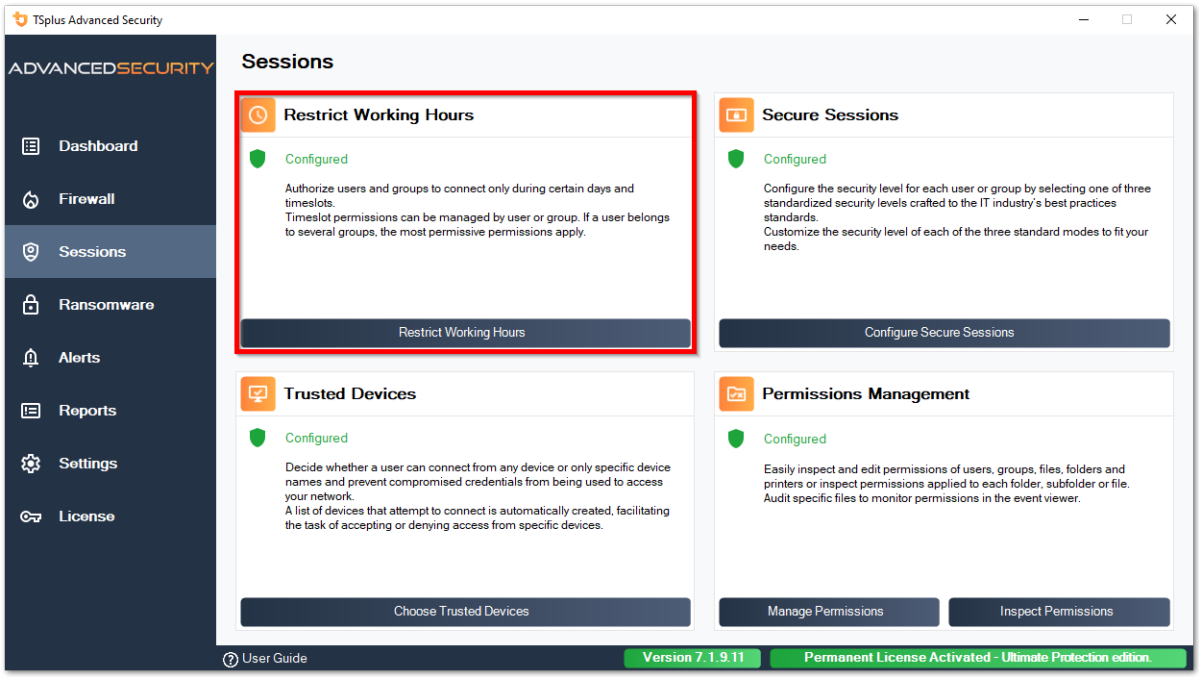
Sie können Arbeitszeitbeschränkungen pro Benutzer oder pro Gruppe konfigurieren.

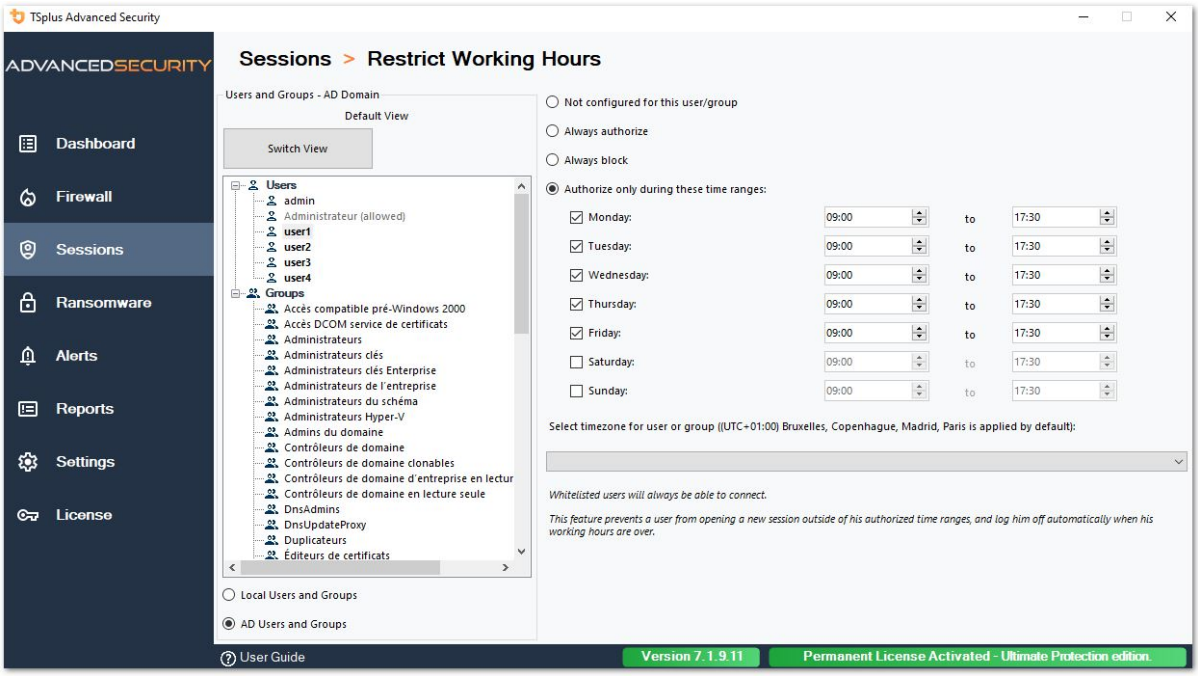
Wählen Sie die gewünschte Einschränkung aus:

- Immer autorisieren Sie diesen Benutzer/diese Gruppe den Zugriff.
- Immer blockieren Sie den Zugriff dieses Benutzers/dieser Gruppe.

oder nur während bestimmter Zeiträume autorisieren.

Sie können es Tag für Tag konfigurieren und den von Ihnen bevorzugten Zeitraum auswählen:





Es ist möglich, eine bestimmte Zeitzone je nach Standort des Büros Ihres Benutzers auszuwählen.

Eine automatische Trennung am Ende der konfigurierten Arbeitszeit erfolgt.

Es ist möglich, eine Warnmeldung zu planen, bevor der Benutzer von TSplus abgemeldet wird. Einstellungen > Erweitert > Arbeitszeiten .

###Benutzer-/Gruppenregeln Prioritäten

Wenn ein Benutzer eine neue Sitzung auf dem Server öffnet:

1. wenn dieser Benutzer direkt für sich selbst definierte Arbeitszeitenbeschränkungen hat, dann werden diese Regeln durchgesetzt.

2. Wenn dieser Benutzer keine direkt definierten Arbeitszeitbeschränkungen für sich selbst hat, wird TSplus Advanced Security alle bestehenden Arbeitszeitbeschränkungen für alle Gruppen dieses Benutzers laden und die permissiveren Regeln beibehalten. Zum Beispiel, wenn eine erste Gruppe eine Regel hat, die die Verbindung am Montag blockiert, eine zweite Gruppe eine Regel hat, die die Verbindung am Montag von 9 Uhr bis 17 Uhr autorisiert, und eine dritte Gruppe eine Regel hat, die die Verbindung am Montag von 8 Uhr bis 15 Uhr autorisiert, dann wird der Benutzer in der Lage sein, am Montag von 8 Uhr bis 17 Uhr eine Verbindung herzustellen.

Warnung: Diese Funktion verwendet die Serverzeit. Die Verwendung der Arbeitsstation des Benutzers und/oder der Zeitzone wäre sinnlos, da der Benutzer nur seine Zeitzone

ändern müsste, um eine Sitzung außerhalb seiner autorisierten Arbeitszeiten zu öffnen.