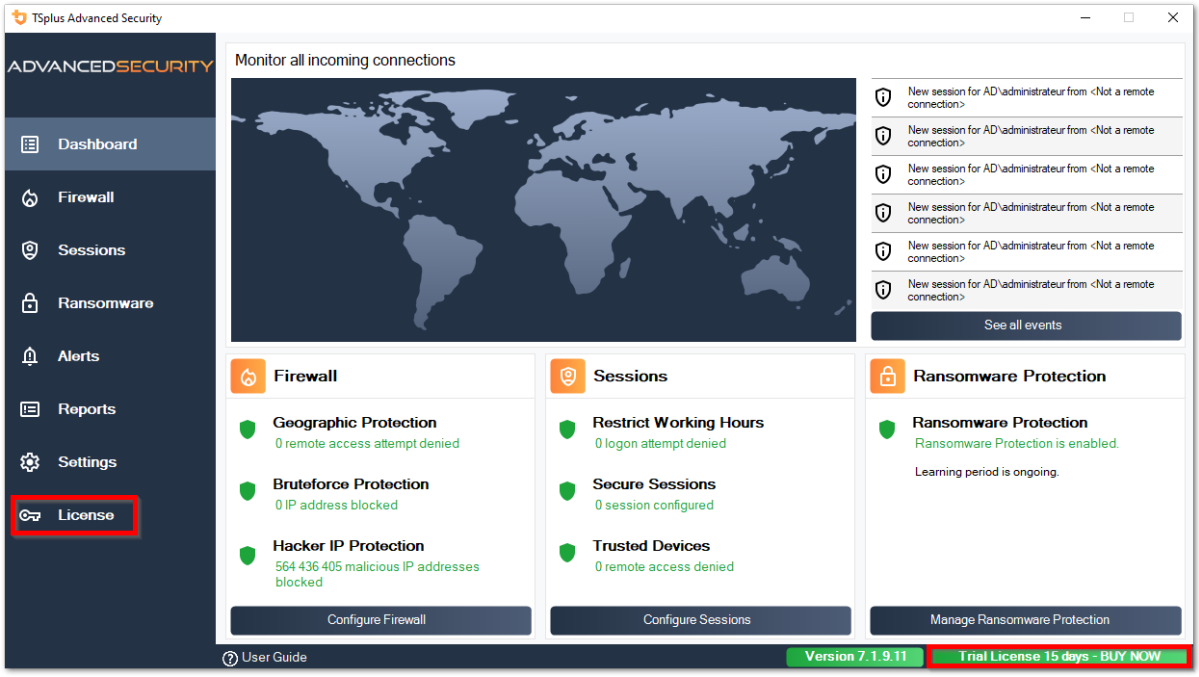
# TSplus Advanced Security - Activating your license

## Step 1: Activating your license from Lite mode

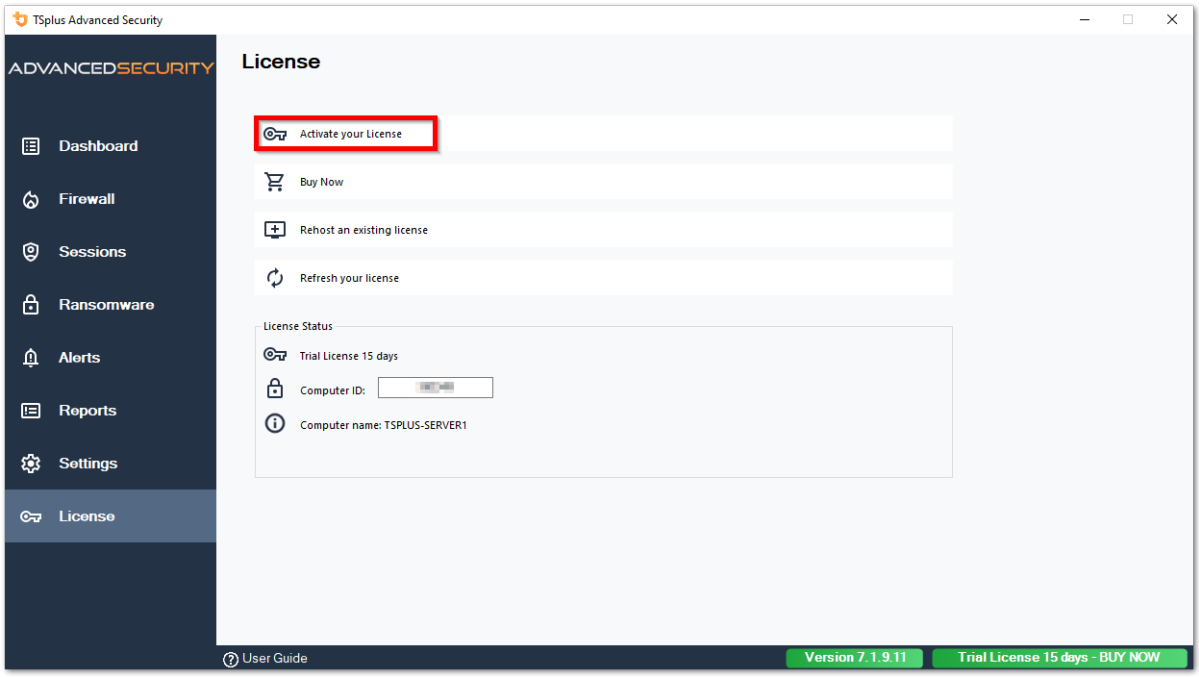
Click on the “Trial License” button to purchase a license or on the License tab if you already have a license and an Activation Key.




Then, click on the “Activate your License” button .

You will find your permanent activation key **(XXXX-XXXX-XXXX-XXXX)** in our order confirmation email.

If you wish to activate your subscription, please enter your subscription key **(S-XXXX-XXXX-XXXX-XXXX)**.



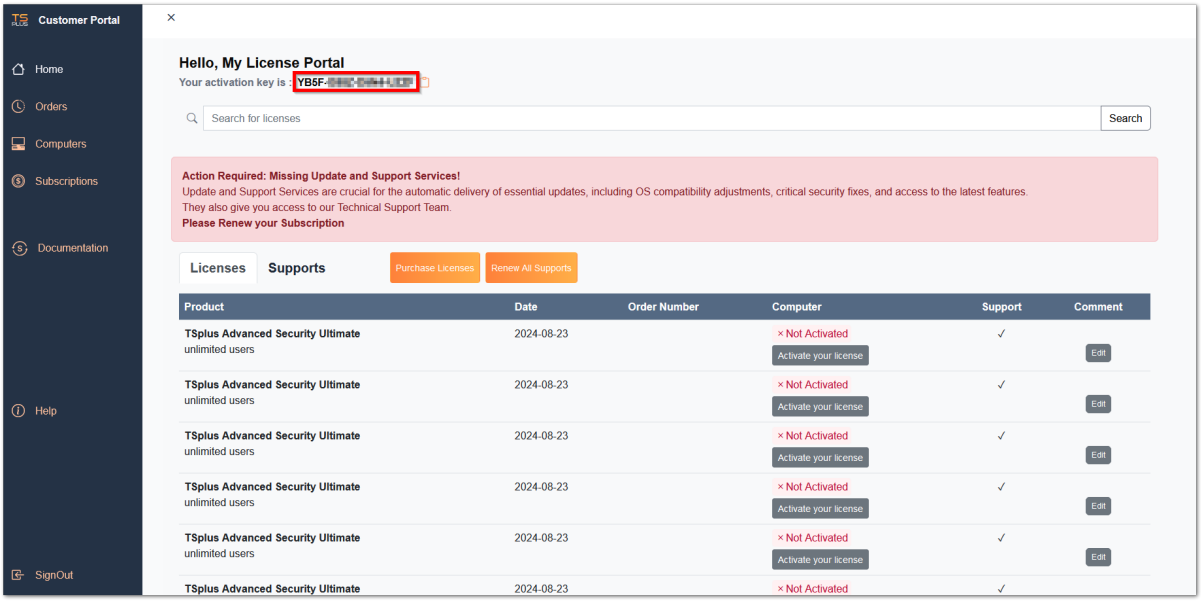

If you do not know you activation key, please proceed to step 2. Otherwise, proceed to step 3.

# Step 2: Retrieve your activation key from the Licensing portal

In order to get your Activation Key, connect to our Licensing Portal and enter your Email Address and your Order Number:

Download the Customer Portal User Guide for more information about your customer portal.

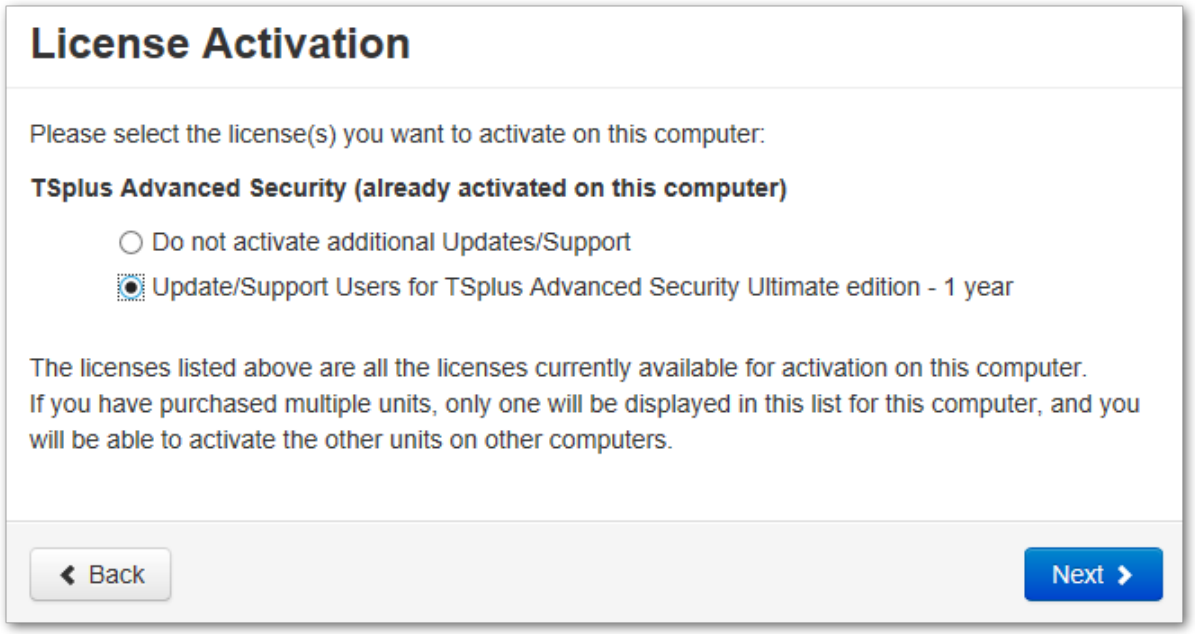
Your activation key will be displayed at the top of the dashboard:



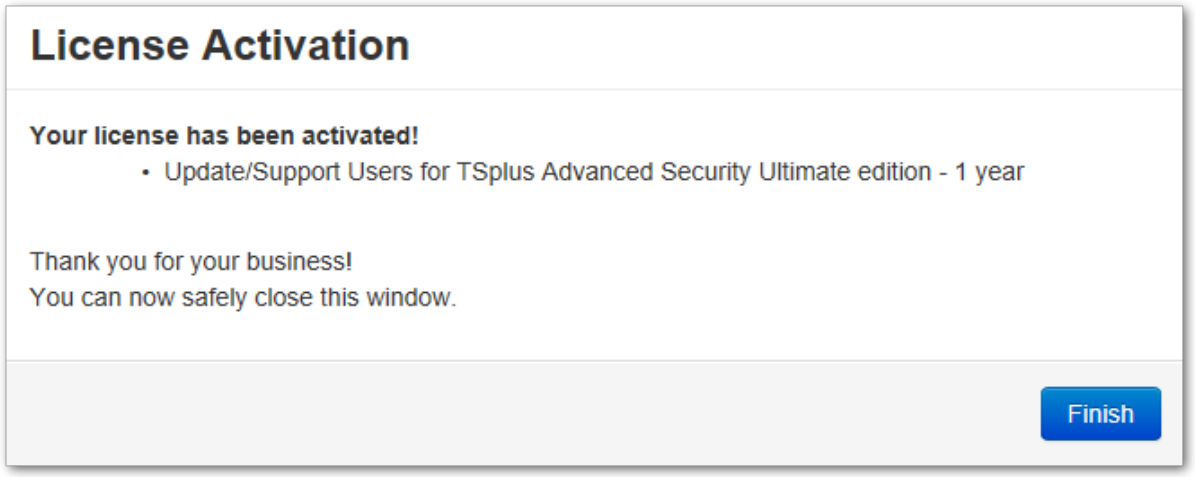

# Step 3: Select requested licences and Update &

# Support services for installed products

Enter your activation key and click on “Next”.

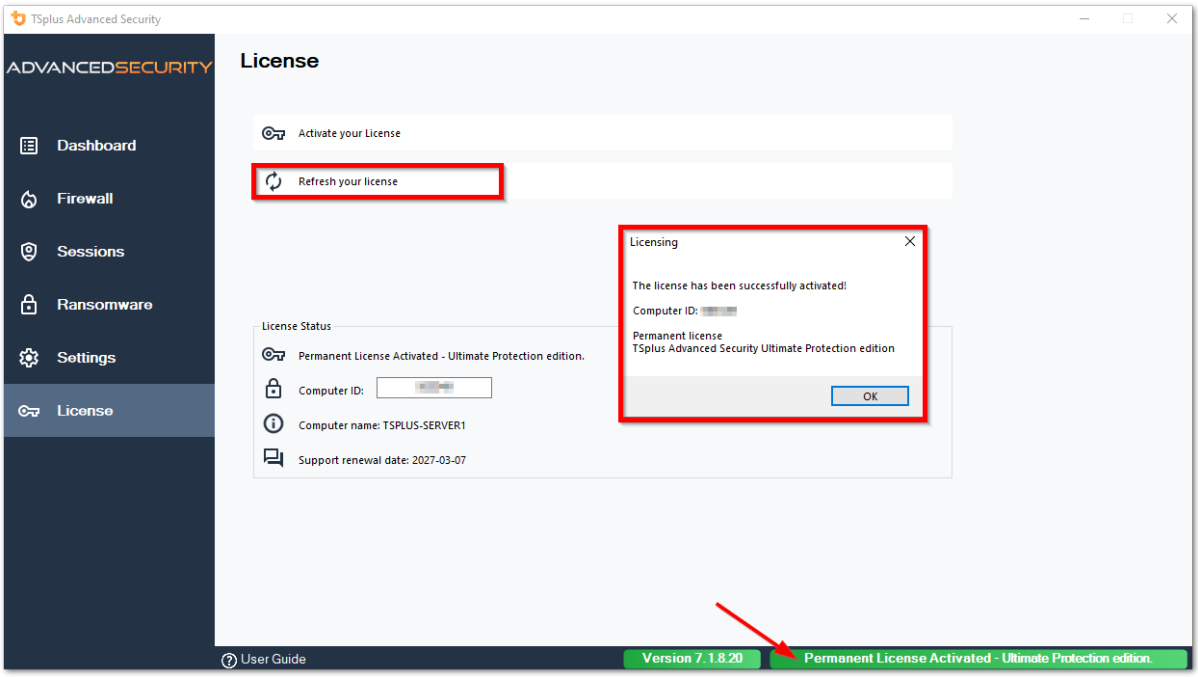



Check one or more items and click on the “Next” button. Please note that you can activate several products at the same time by checking several products and/or support subscriptions.




All your selected products and support subscriptions are now activated (in this example, both TSplus with support and TSplus Advanced Security have been activated at once).

Refresh your licensing status by clicking on the corresponding button.




# Activating your license (Offline)

Please refer to the procedure described for TSplus Remote Access: Activating your TSplus License (Offline)

# Rehosting your license

Please refer to the procedure described for TSplus Remote Access: Rehosting your TSplus License

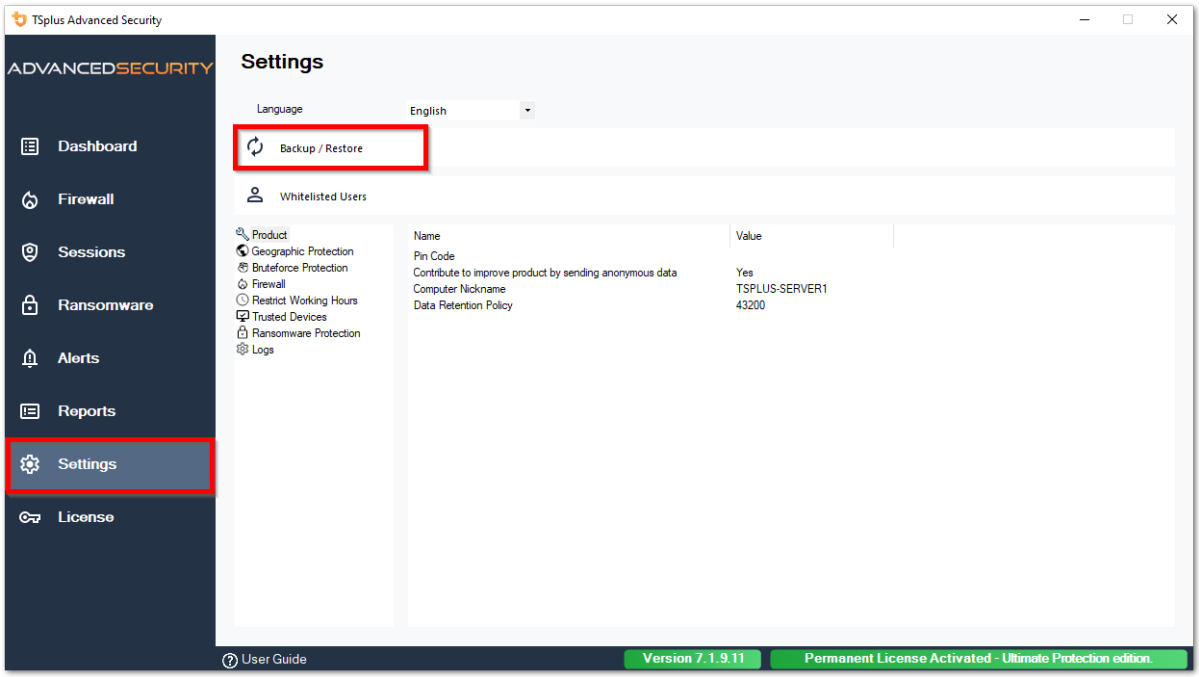
**Note:**: You can download a license.lic file on the Licensing Portal for TSplus Advanced Security versions below. Please refer to the Customer Portal User Guide for more information.

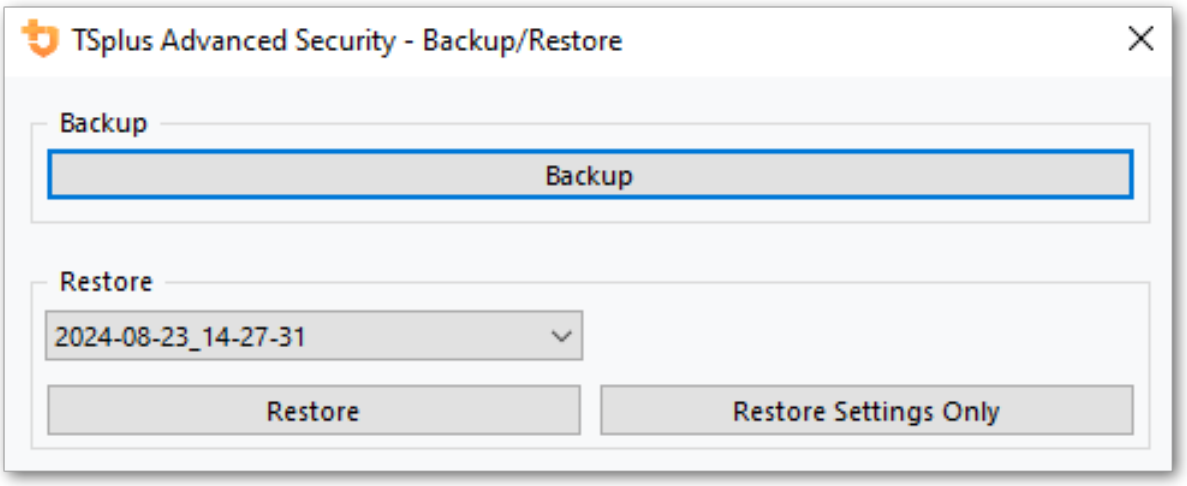
Thank you for choosing TSplus Advanced Security!

# Advanced - Backup and Restore

## Backup and Restore Data and Settings

You can backup or restore TSplus Advanced Security's data and settings by clicking on the button "Backup / Restore" on the top:




The backup will be saved in the folder **archives** located in TSplus Advanced Security's setup

directory. By default, the **archives** folder is located here: C:\Program Files (x86)\TSplus-Security\archives

# Using the command line to backup and restore

The command usage is described below:

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

By default, the backup will be created in the archives directory located in TSplus Advanced Security setup folder. However, the backup may be saved in a specified folder. Relative and absolute paths are allowed.

- **Restore**: TSplus-Security.exe /restore [path to a backup directory]

The specified backup directory must contain a data and a settings folder, as created by the /backup command.

# Configuring backups

Please note that you can specify the following advanced settings in the registry:

- The backup directory can be specified in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath. By default, the “archives” directory of the Advanced Security setup directory will be used.

- The maximum number of backups available can be specified in the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives. By default, Advanced Security keeps the last 3 backups.

# Migrate your data and settings to another computer

Please follow the steps below to migrate Advanced Security from computer A to computer B:

1. On computer A, please click on the Backup button to create a new backup. Settings and data will be saved in the archives directory, located in advanced-security setup directory (typically C:\Program Files (x86)\TSplus-Security\archives).

2. Copy the newly created backup folder (e.g. named backup-2019-09-11_14-37-31), including

all content, from the archives directory on computer A to the archives directory on computer B.

3. On computer B, from the Backup / Restore window, in the “Restore” section, select the relevant backup name to be restored.

4. Then, click on Restore Settings Only to restore the settings. Alternatively, it is possible to click on Restore to restore all data and settings, which is not recommended for a migration but useful to restore advanced-security on computer A.

5. Please wait at most 2 minutes for the settings to be reloaded by advanced-security features.

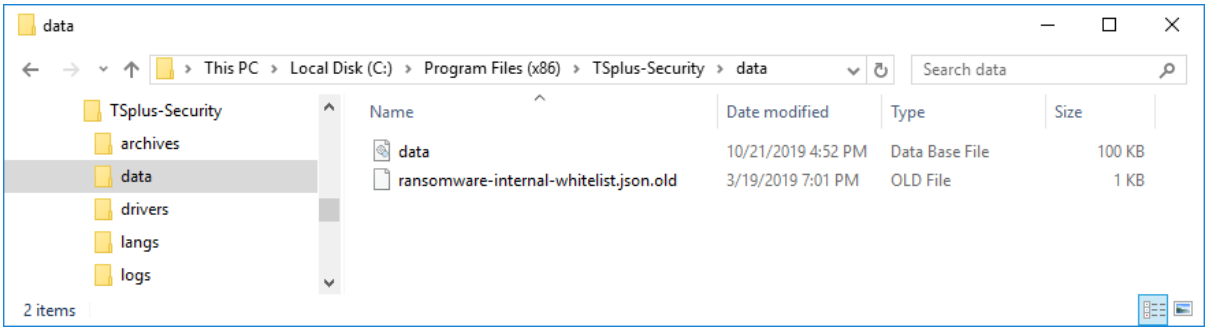
# Database

A database stores Events, IP addresses, Ransomware attacks reports and programs whitelists.

This database is stored in **data** folder located in TSplus Advanced Security’s setup directory.

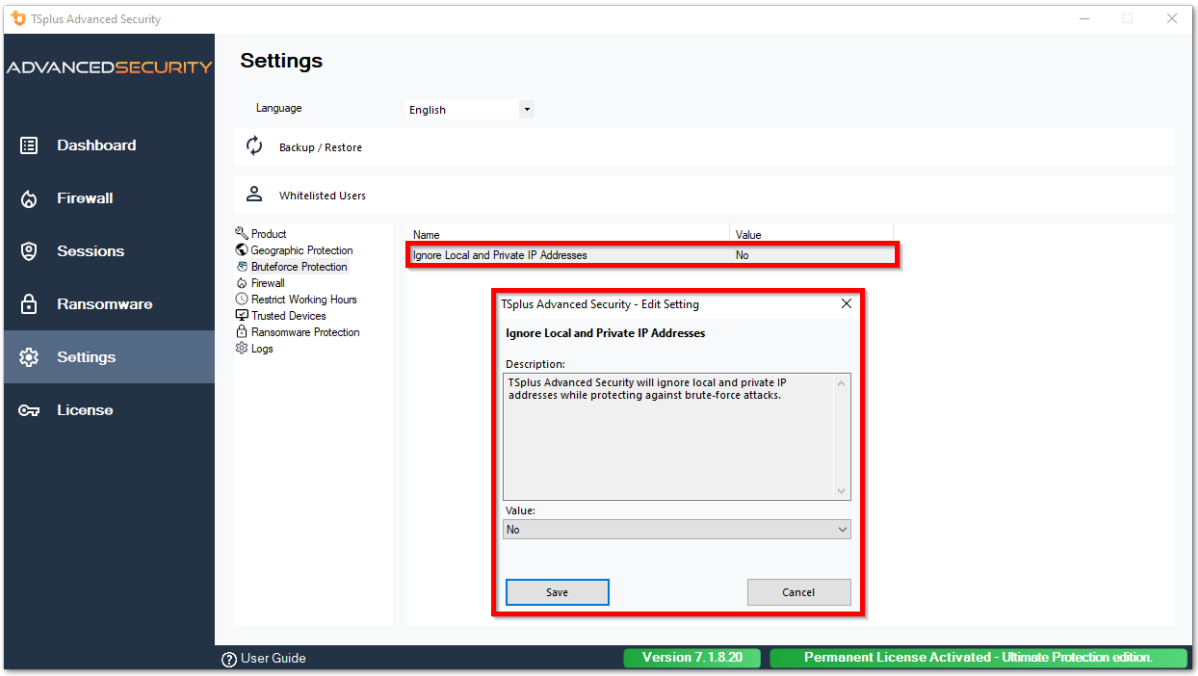
- Advanced Security from version 5 and prior to version 5.3.10.6 uses a LiteDB database engine.

- Advanced Security above version 5.3.10.6 uses a SQLite database engine.



# Advanced - Bruteforce Protection

The **Bruteforce Protection** tab allows you to Ignore Local and Private IP Addresses if you wish to, by changing the default value from “No” to “Yes”.

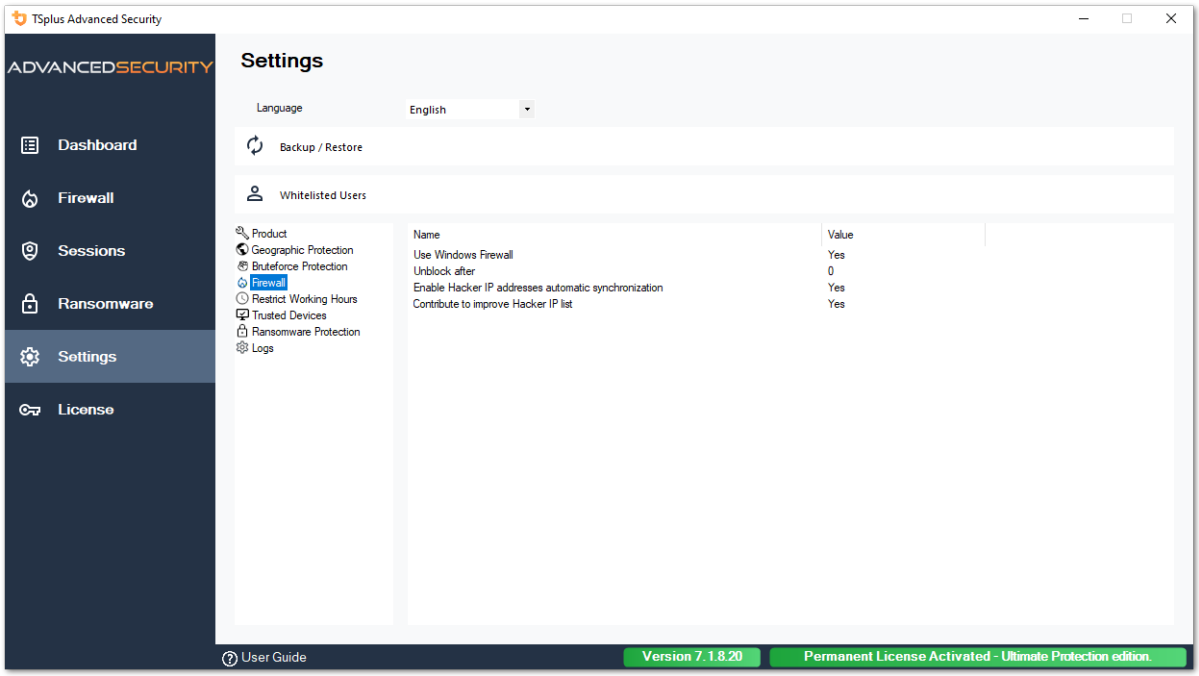


# Advanced - Firewall

The **Firewall** tab allows you to activate the **Windows Firewall or deactivate it in favor of the TSplus Advanced Security built-in firewall**.

**Since version 4.4, a built-in firewall is included in TSplus Advanced Security.**

As a general guidance, if Windows Firewall is activated on your server, then you should use it to enforce TSplus Advanced Security rules (default). If you installed another firewall, then you must activate TSplus Advanced Security built-in firewall.




**Use Windows Firewall** In order to activate the built-in firewall, go to Settings > Advanced > Product > Use Windows Firewall and set the value to: No If Yes, then the offending IP addresses will be blocked using Windows Firewall. TSplus Advanced Security firewall will be used otherwise.

**Unblock after** Change this setting to automatically unblock IP addresses after a certain amount of time (in minutes). Default value is 0, disabling this feature. Value: 0

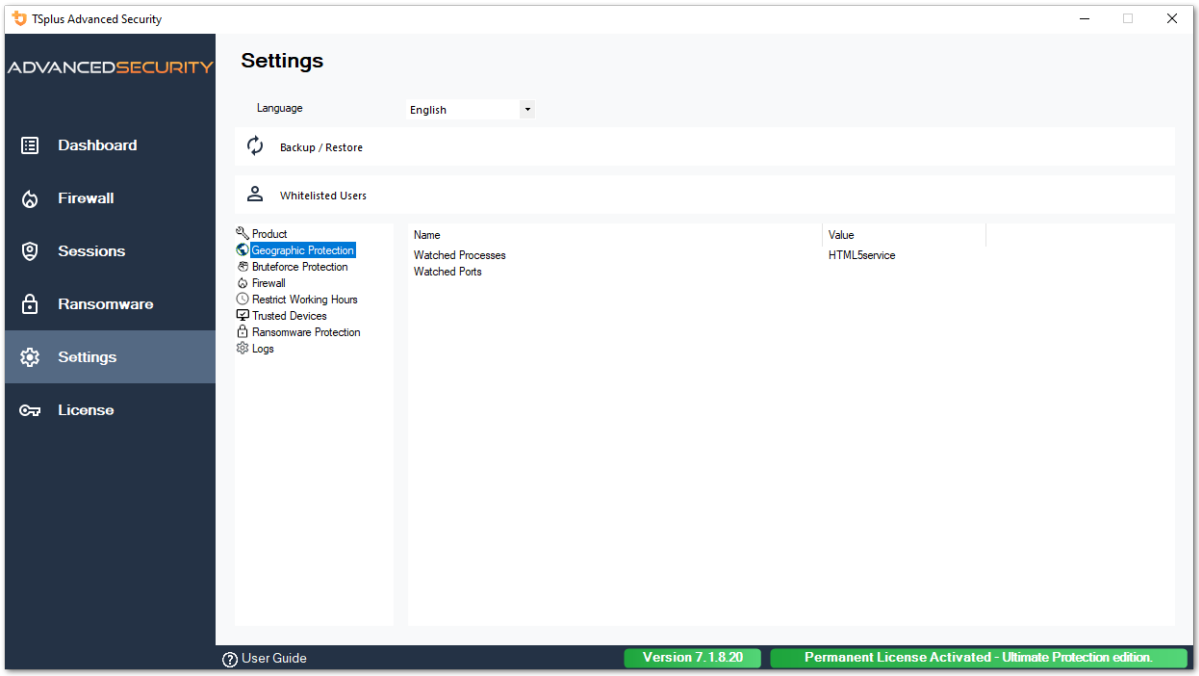
**Enable Hacker IP addresses automatic synchronization** Keep your machine protected against known threats such as on-line attacks, on-line service abuse, malware, botnets and other electronic activities with the Hacker IP Protection Support and Updates Services subscription is

required. Value: Yes

**Contribute to improve Hacker IP list** Allow TSplus Advanced Security to send anonymous usage statistics to enhance protection against Hacker IP.
Value: Yes

# Advanced - Geographic Protection

The **Geographic Protection** tab allows you to add or remove processes that are watched by the Geographic Protection feature.



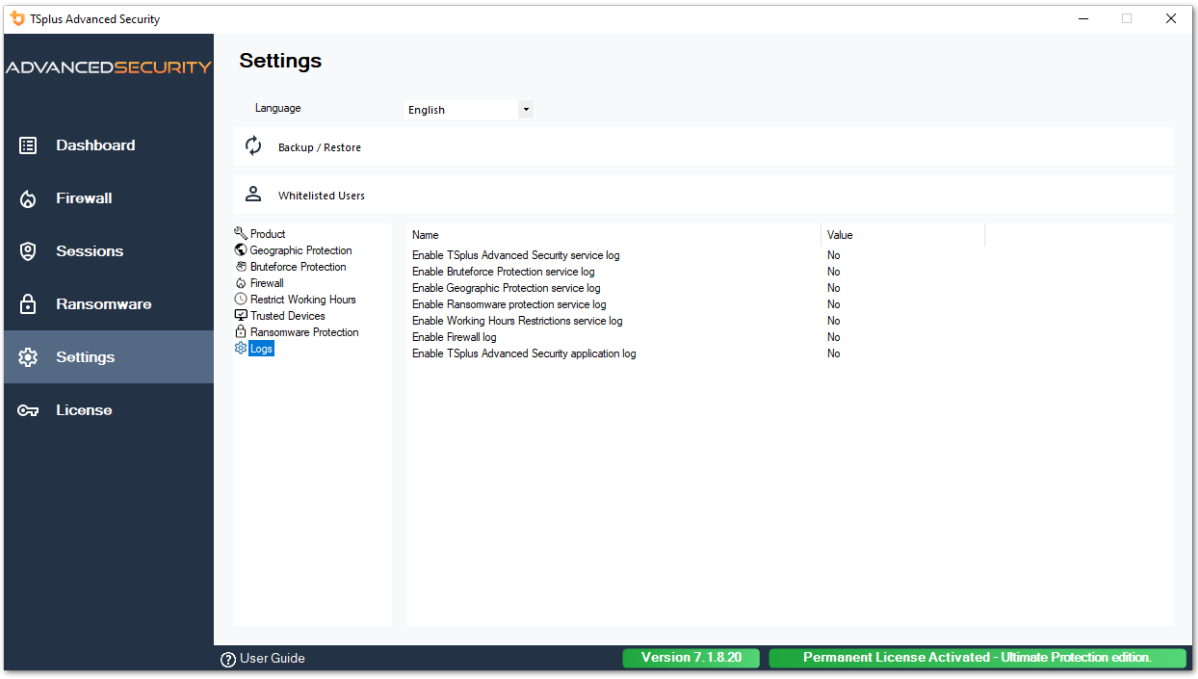

By default, the HTML5 service is watched.

The **Watched Ports** settings allows you to add ports watched by the Geographic Protection feature. By default, Geographic Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC ports. Geographic Protection supports the following VNC providers: Tight VNC, Ultra VNC, Tiger VNC and Real VNC, which are not related whatsoever with TSplus.

# Advanced - Logs

The **Logs** tab allows you to enable or disable service and features logs. Logs exist to find more easily the origin of the errors encountered on TSplus Advanced Security.

To retrieve the logs, open an Explorer and browse to the **logs** folder of TSplus Advanced Security's setup directory. By default, logs will be located here: **C:\Program Files (x86)\TSplus-Security\logs**




Enable or disable TSplus Advanced Security service and application logs, which are respectively the global configuration service that runs in the background and the log for the application interface.

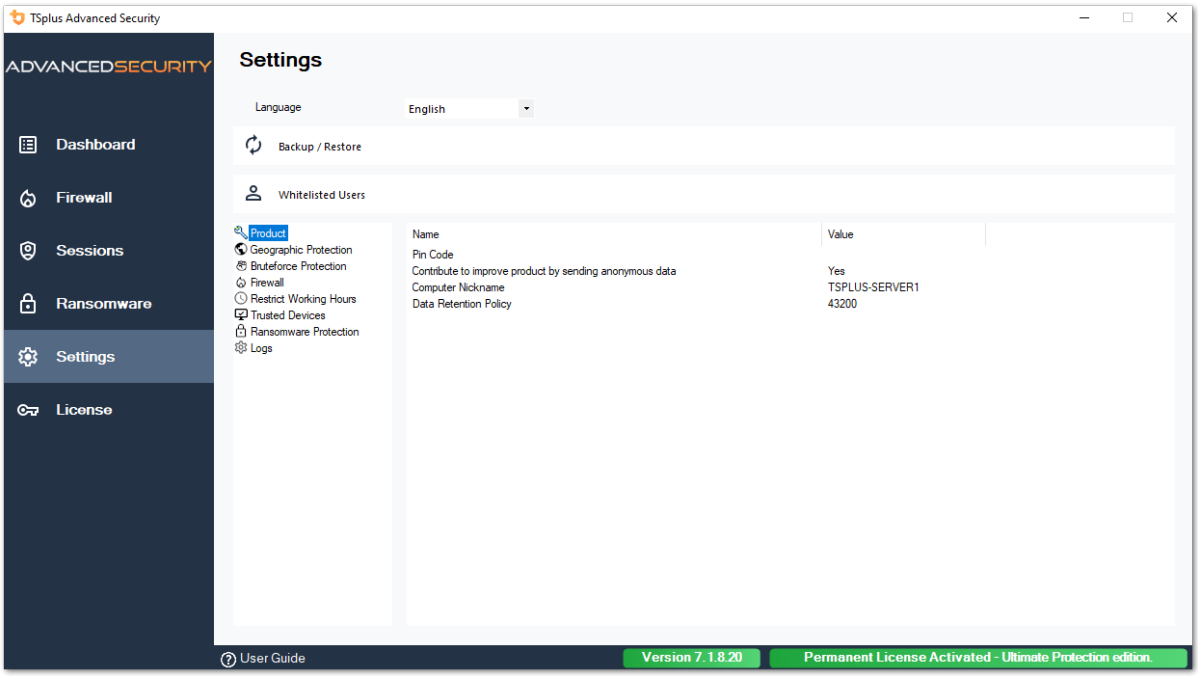
You can also enable logs corresponding to the respective TSplus Advanced Security's features:

- Service
- Bruteforce Protection
- Geographic Protection
- Ransomware Protection
- Restrict Working Hours
- Firewall..
- Application

All logs are disabled by default. Logs correspond to different components, our support team will tell you what value to put according to the problem encountered.

# Advanced - Product

The **Product** tab allows you to add a PIN code to the application:




Click on Save. The PIN code will be required the next time you will start the application.

You can also **contribute to improve the product**, by sending anonymous data (enabled by default): YES

The following data will be collected in case of a Ransomware attack:

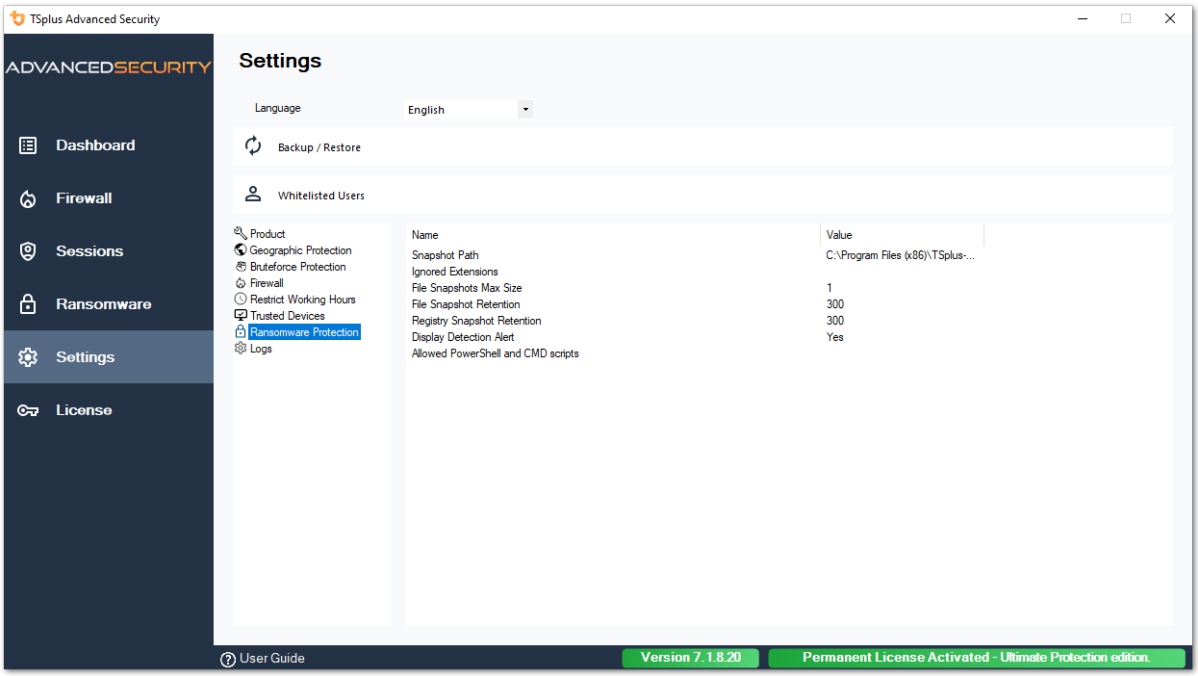
- TSplus Advanced Security's version.
- Windows version.
- Suspected files'paths that lead to the ransomware attack.

Modifying the **Computer nickname** is also possible.

The **Data Retention Policy** defines the period of time after which TSplus Advanced Security's events are removed from the database. A backup is performed before each database cleanup. This policy is defined in minutes. Default data retention policy is 259 200 minutes, or 6 months.

# Advanced - Ransomware Protection

The **Ransomware Protection** tab allows you to configure the snapshot properties and define ignored file extensions for the Ransomware Protection feature.




**Snapshot Path**: Define the directory where Ransomware Protection stores file snapshots.

Default value is: C:\Program Files (x86)\TSplus-Security\snapshots

**Ignored Extensions**: By default, Ransomware Protection ignores well-known extensions of temporary files for ransomware activity. See the list here. You can define custome extension names on the value field (semicolon separated):

**File Snapshot Max Size**: File Snapshots Max Size defines the maximum space allowed to retain file snapshots.

The size is expressed in percentage of total available space on the disk where Snapshot Path resides.

**File Snapshot Retention**: File Snapshot Retention defines, in seconds, the retention policy of a file snapshot.

Once the retention period has ended, the file snapshot is deleted. By defaut, 300 seconds (i.e. 5 minutes)

**Registry Snapshot Retention**: Registry Snapshot Retention defines, in seconds, the retention policy of a registry snapshot. Once the retention period has ended, the registry snapshot is deleted. By defaut, 300 seconds (i.e. 5 minutes)

**Display Detection Alert**: Display an alert message window on user's desktop when Ransomware Protection has detected and stopped an attack.

**Allowed PowerShell and CMD scripts**: Allowed PowerShell and CMD scripts lists the complete file paths of the PowerShell and CMD scripts allowed to be executed on the machine

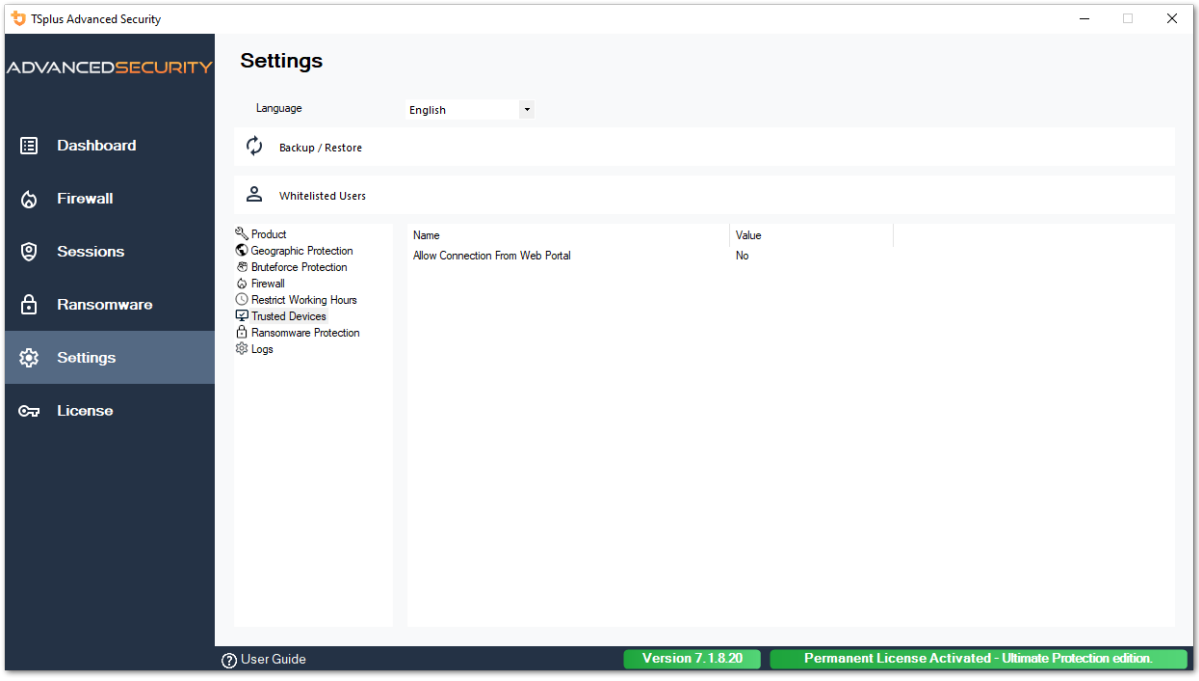
The execution of allowed scripts won't trigger the Ransomware protection (semicolon separated).

# Advanced - Trusted Devices

The **Trusted Devices** tab allows you to enable connections from the TSplus Remote Access' Web Portal.

**Note**:

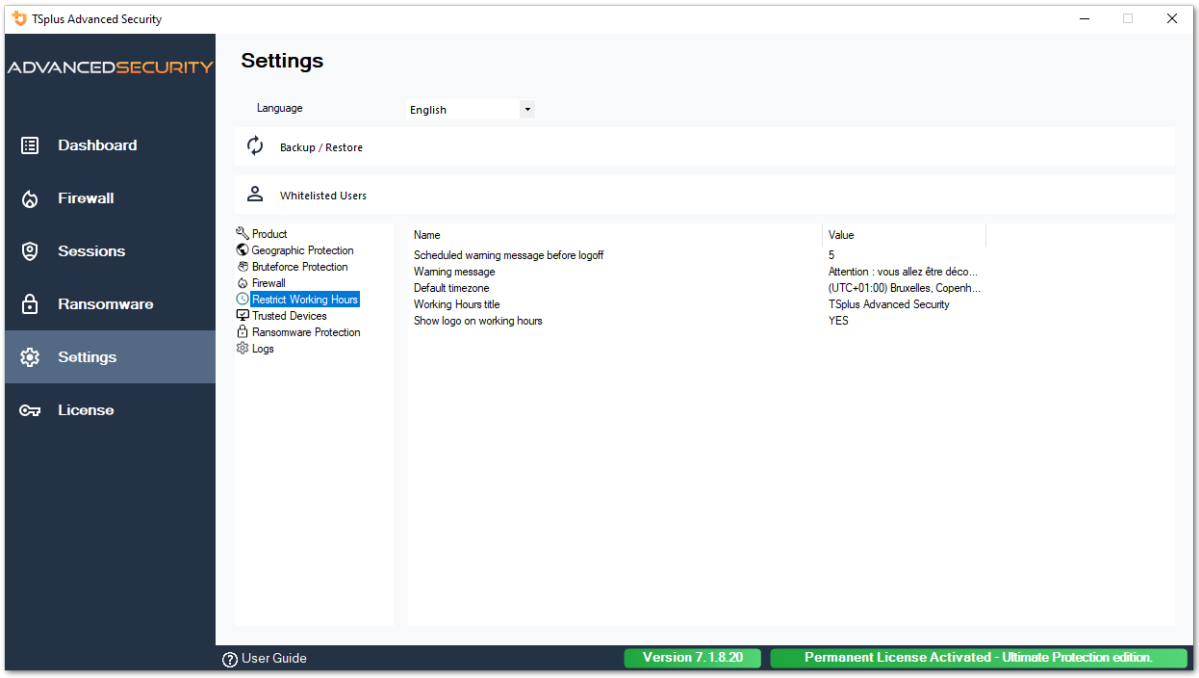
-Trusted Devices is not compatible with HTML5 sessions. -Trusted Devices is not compatible with iOS / Android mobile devices as they hide their real hostnames. -The hostname of the remote machine is defined by the machine itself. The machine is likely to conceal or modify it according to its configuration.




TSplus Advanced Security's Trusted Devices cannot resolve the client name if the connection is initiated from TSplus Remote Access' Web portal. Therefore, Trusted Devices will block any connections from Web Portal by default. Set this setting to "Yes" to allow connections from the Web portal. Please be aware that this action will diminish your server's security.

# Advanced - Restrict Working Hours

The **Restrict Working Hours** tab allows you to Schedule a warning message before the user is logged off.




**Warning message schedule** You can configure in number of minutes before the user is automatically disconnected. By default, it is set to 5 minutes.

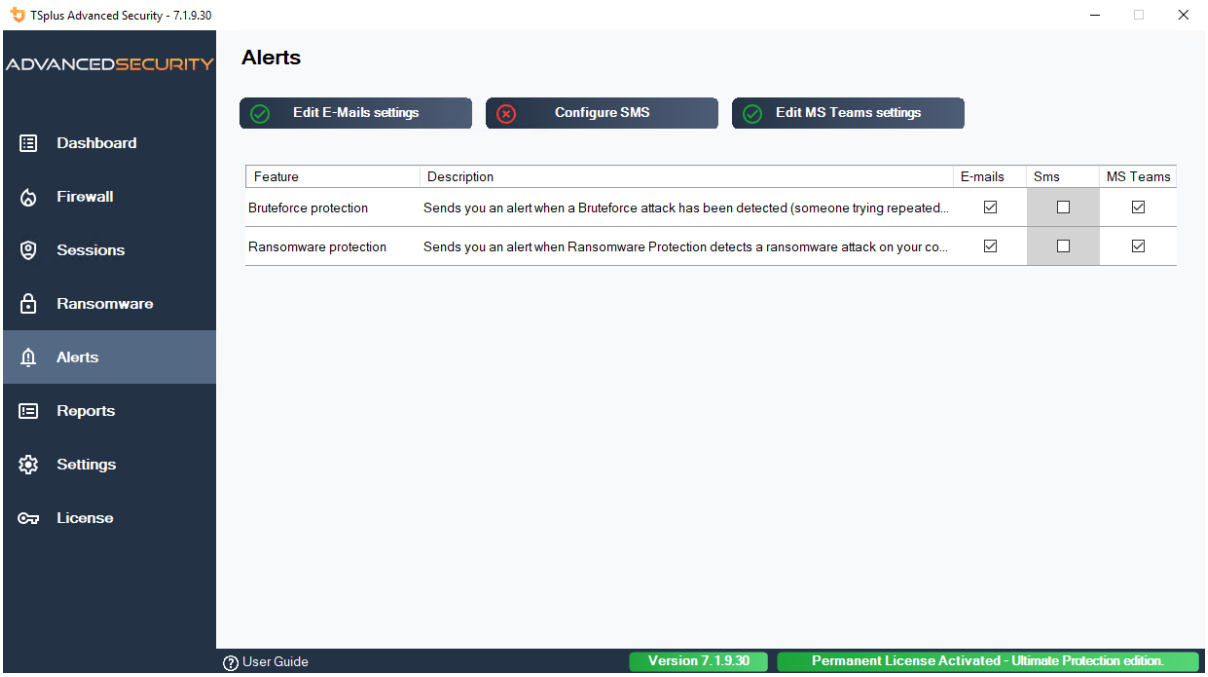
**Warning message** A warning message may be defined at your convenience, with placeholders named %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% and %ENDINGHOURS%, which will be respectively replaced by the current number of minutes before the session closes, the current day, the current day's starting and ending working hours.

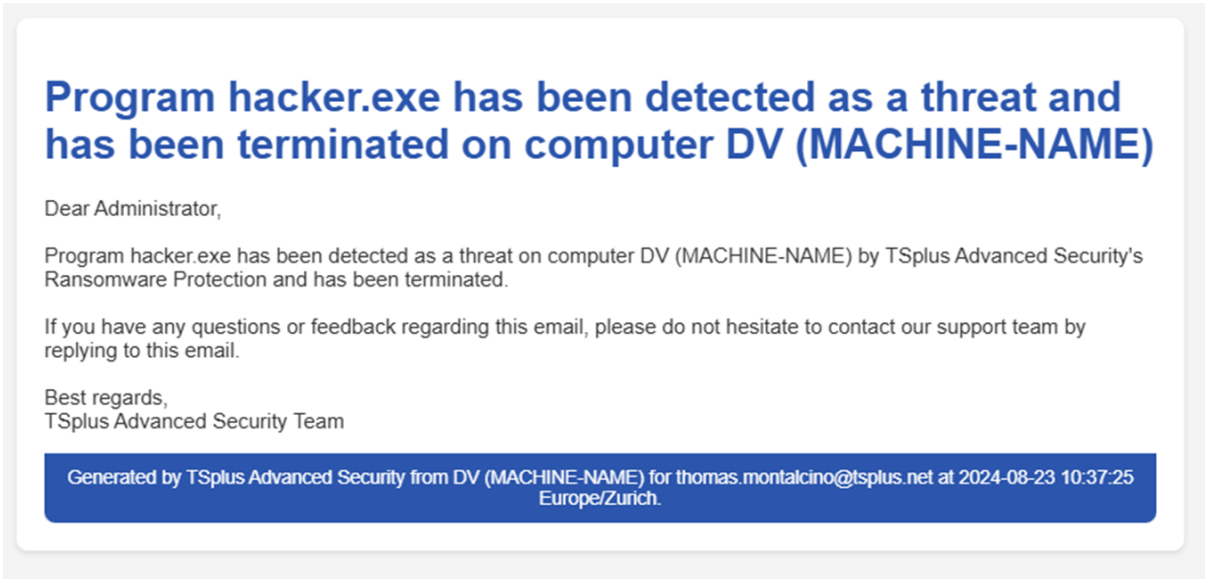
**Default server timezone** A default server timezone may be defined to apply the working hours rules accordingly by selecting the corresponding one on the drop-down list.

**Working hours title** Title of the form displayed to the end-user, when his/her working hours are ending (default: TSplus Advanced Security)

**Show logo on working hours** If set to "yes", the logo is shown in the form displayed to the end-user, when his/her working hours are ending (default: "yes")

# Alerts



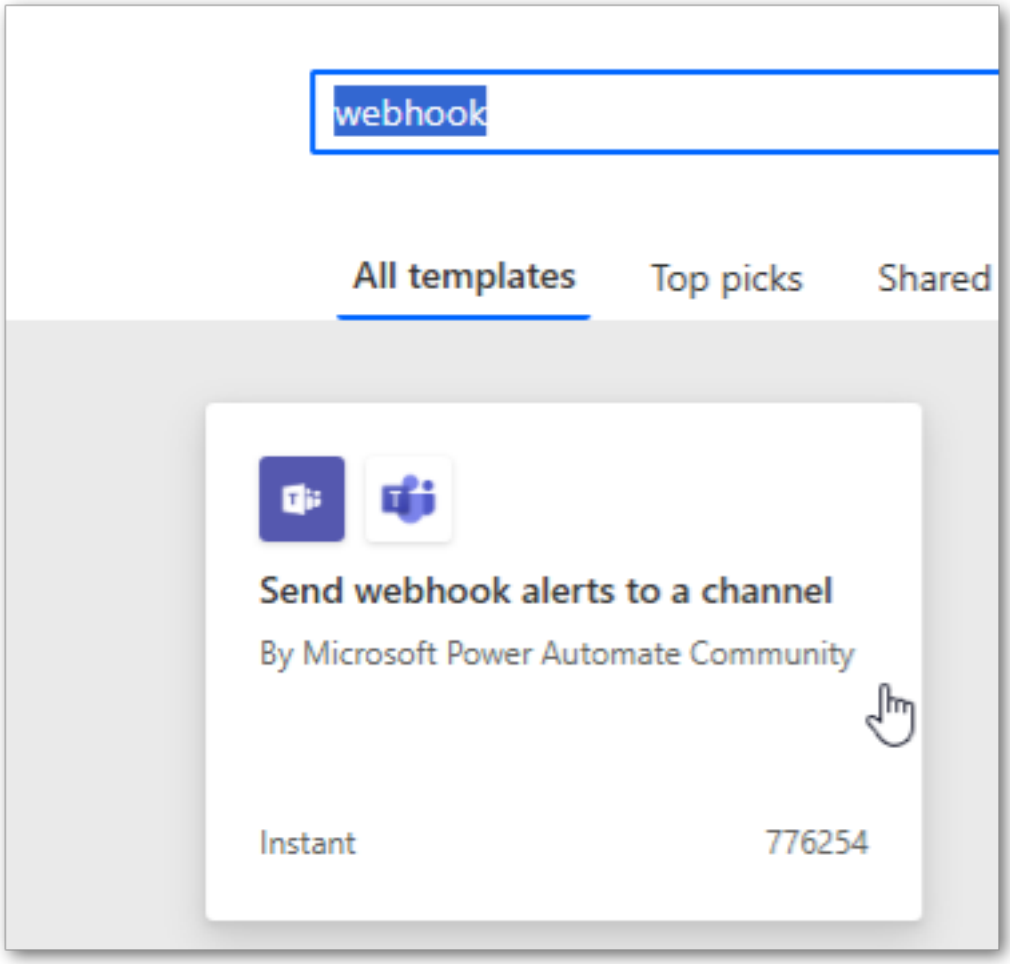




## Create a Alert in Microsoft Teams.

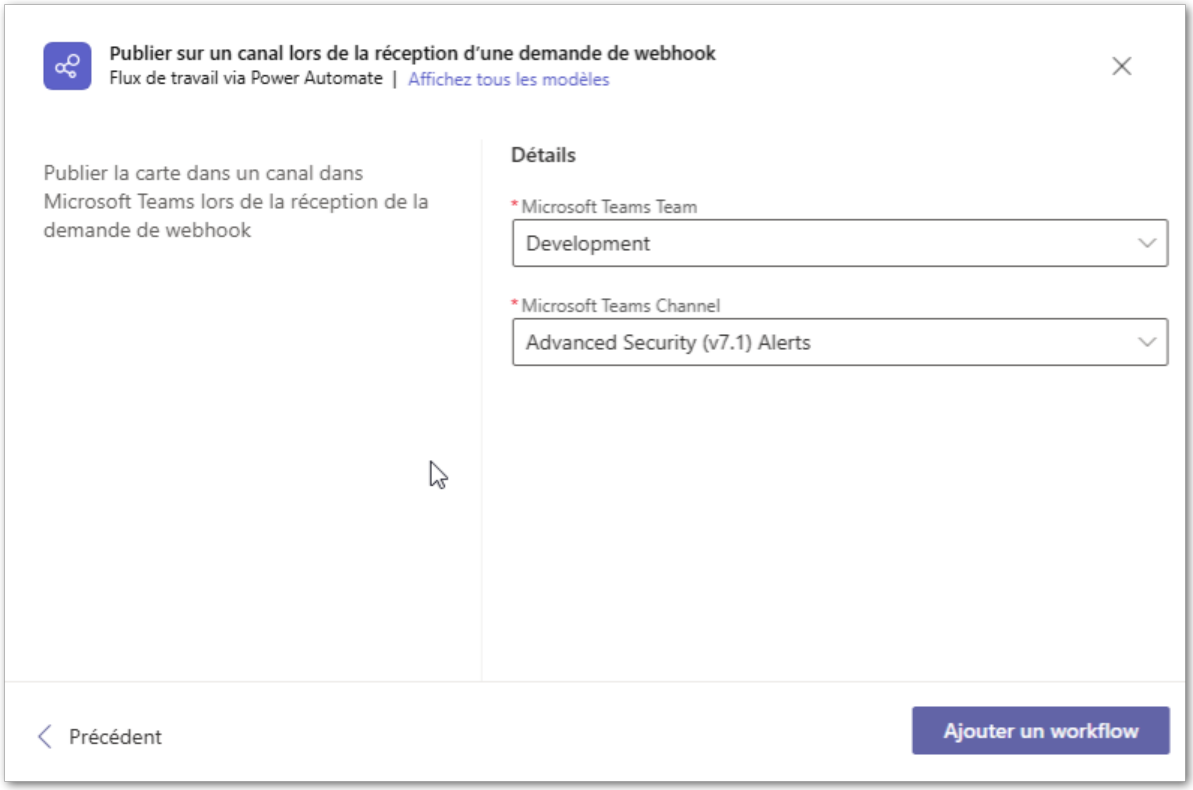
The first thing to do is create a workflow in the Teams channel you want to send alerts to. There are two ways to do this:

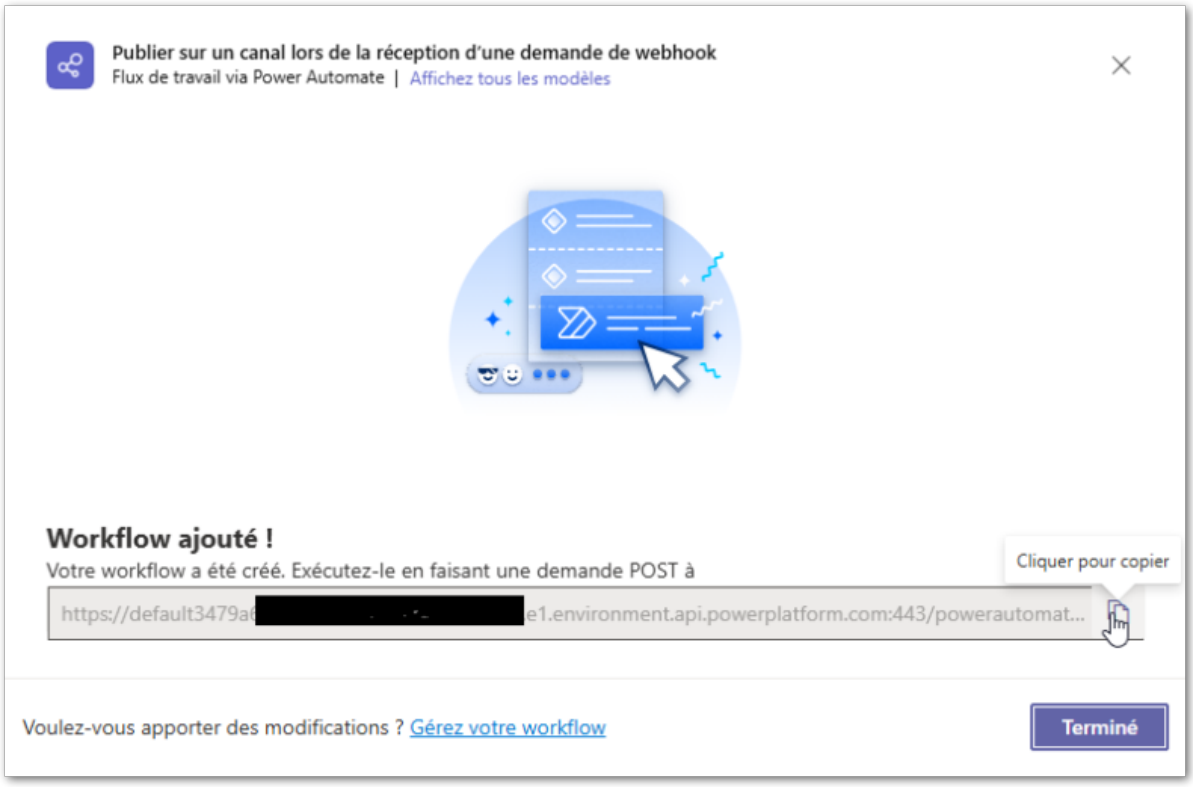
- in Power Automate (https://make.powerautomate.com/) > My Flows > New Flow
- directly in MS Teams; select the "…" icon next to the channel you want to use, then "Workflows"

You can create a flow with an existing template; search for "webhook" and you'll find "Send webhook alerts to a channel."




Fill in the details (which channel to publish to). This is a little more convenient when creating the workflow directly from MS Teams.

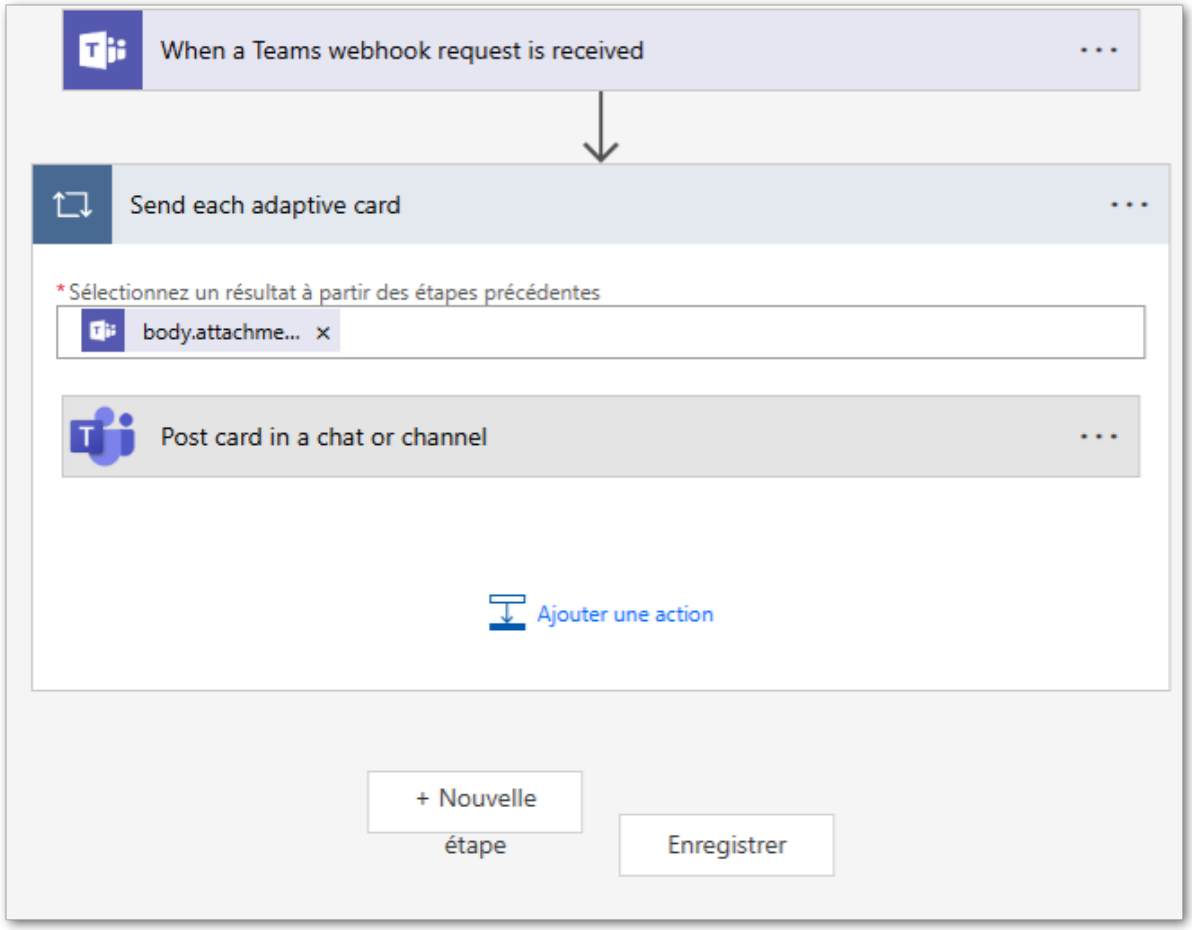


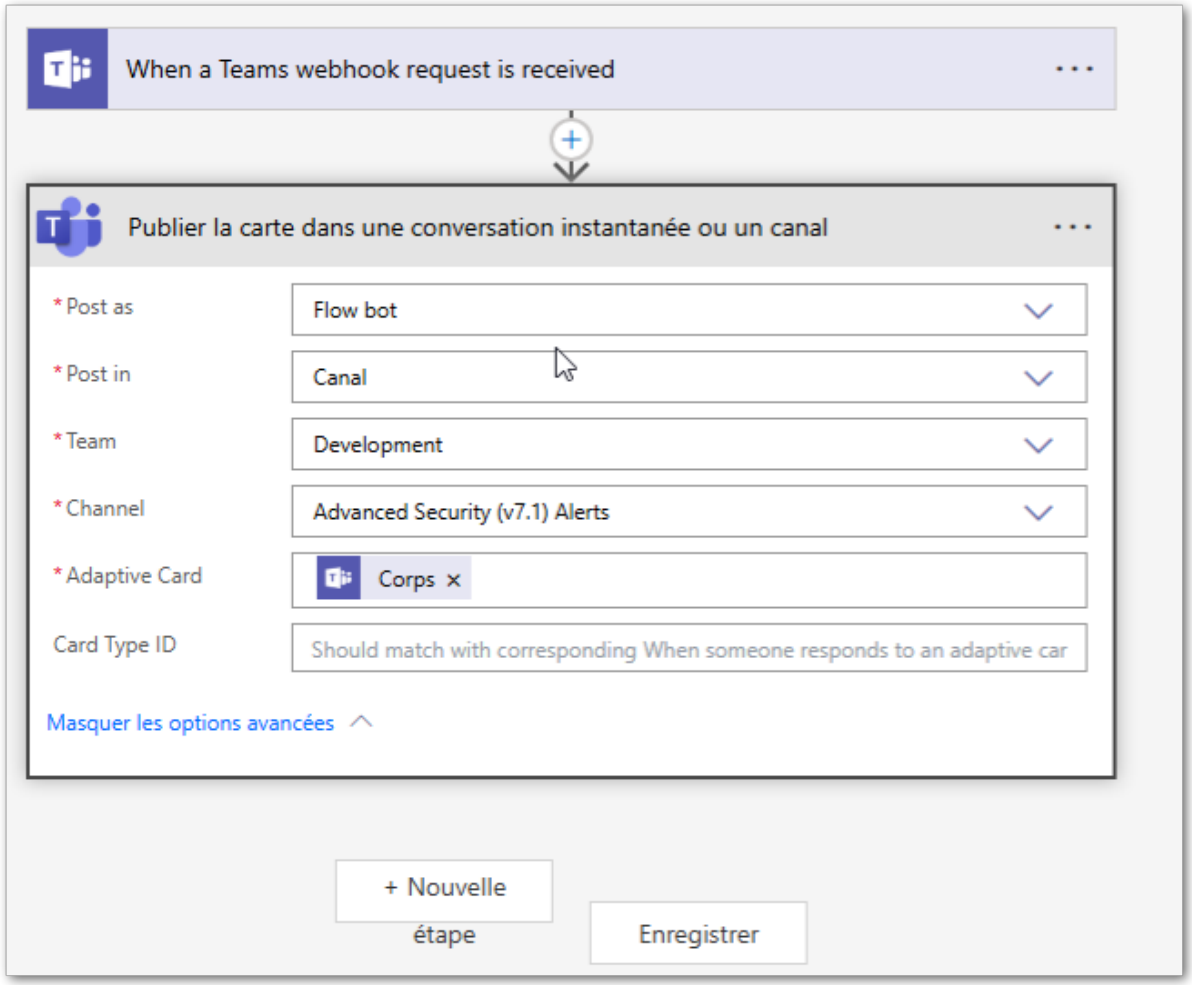

Copy the URL; this is the one you need to provide in Teams settings, in Advanced Security or Server Monitoring.

Finally, edit the flow you just created, remove the “Send every Adaptive Card” option, and replace it with the following component:

(before editing)



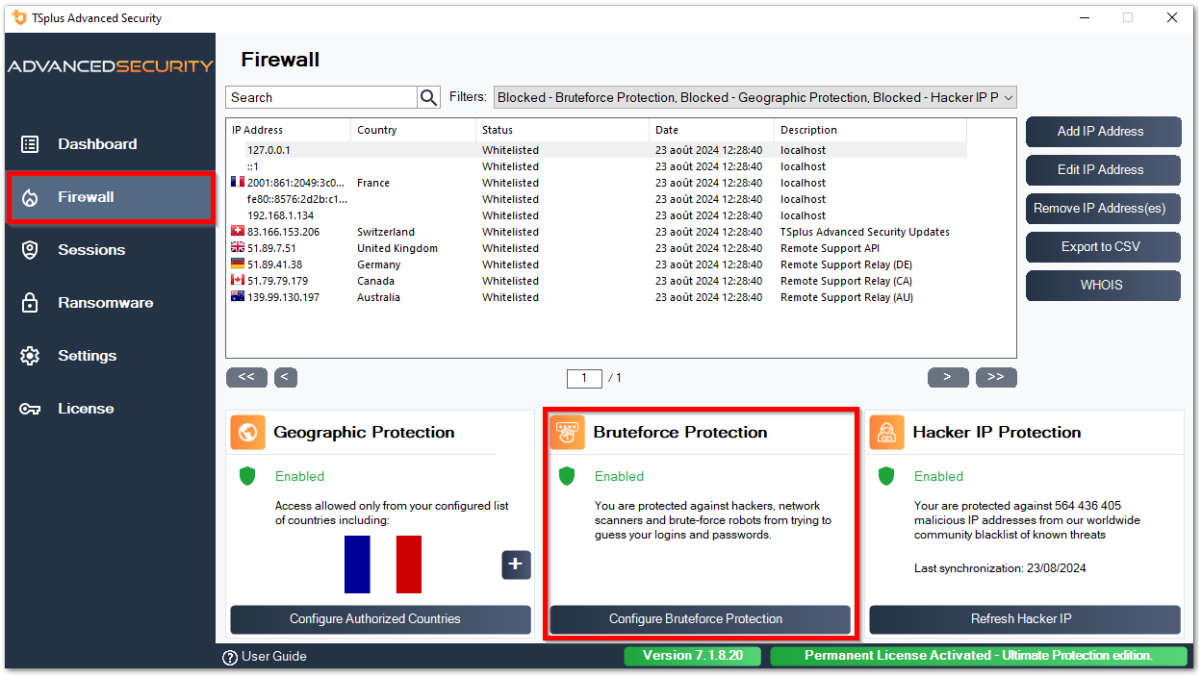

(after editing)

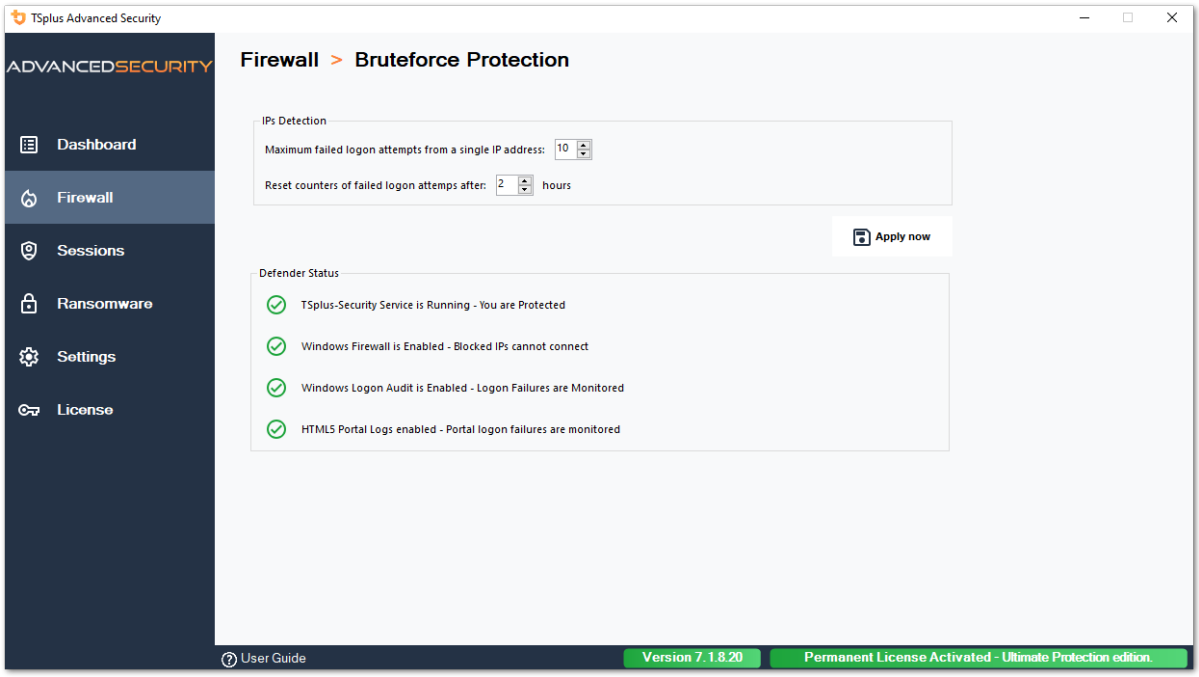


# Bruteforce Protection

The Bruteforce Protection enables you to protect your public server from hackers, network scanners and brute-force robots that try to guess your Administrator login and password. Using current logins and password dictionaries, they will automatically try to login to your server hundreds to thousands times every minute.

With this RDP Defender, you can monitor Windows failed login attempts and automatically blacklist the offending IP addresses after several failures.






- You can set the **maximum failed logon attempts from a single IP address inside the IPs Detection block** (by default, it is 10), as well as the time of reset for failed logon attempts counters (by default it is 2 hours).

- On the bottom of this window, you can see the **Defender status**, where you can check if the HTML5 Web Portal logon failures, the Windows Logon Failures are monitored and if the Windows Firewall and advanced-security service are enabled.

In this case, like in our example, all the status are ticked.

- **Manage Blocked IP addresses**: You can of course configure it to match your needs, for example by adding your own workstation IP address in the IPs Whitelist, so this tool never block you. You can add as many IP addresses as you want in the whitelist. These addresses will never be blocked by the bruteforce Protection.

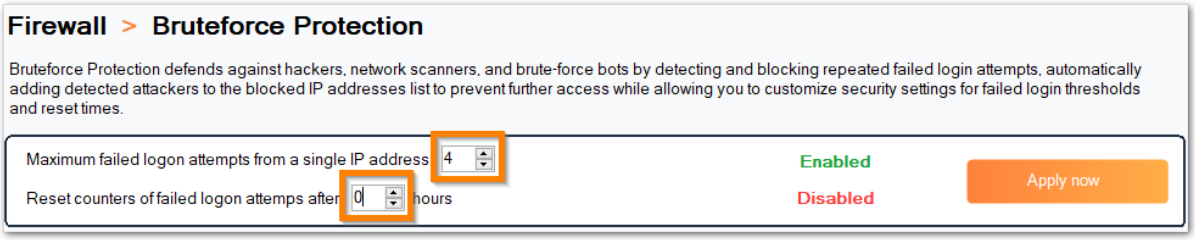
- You can **ignore Local and Private IP Addresses** by changing the default setting on the Settings > Advanced > Bruteforce tab

Note: If you ever notice that the Bruteforce Protection blocked 10 IP addresses per day and that now, it is not the case anymore; and blocks one, two or even doesn't block any address, it is actually normal. Indeed, before advanced-security installation, the server having an RDP port publicly available is known by all the robots, and many robots try the current passwords and the ones coming from dictionaries. When you install advanced-security, these robots are progressively being blocked, so that one day:

- Most of the active robots are already blocked and are not interested by the server, even the new ones.
- Also, the server does not appear anymore on the list of publicly known servers.

# Disable feature and block forever

- Disable the Bruteforce feature by setting the “Maximum failed logon attempts” parameter to 0.
- Block an IP address detected by Bruteforce indefinitely by setting the “Reset counter” parameter to 0.



# Command lines

We are pleased to provide you with a comprehensive set of command-line tools designed to enhance the flexibility and efficiency of our software. These tools enable users to script and automate various functionalities, tailoring the software to meet their specific needs and workflows.

Explore the possibilities and optimize your experience with our command-line options.

You only have to run the following command lines as an elevated Administrator. As a reminder, TSplus-Security.exe is located in the following folder **C:\Program Files (x86)\TSplus-Security** by default.

## License Management

To perform operation on licenses, please replace the program AdminTool.exe presented in the following documentation by the TSplus-Security.exe program located in Advanced Security setup directory (usually **C:\Program Files (x86)\TSplus-Security**).

- License activation
- License reset following cloning of a VM
- Volume license activation
- Enabling and disabling Volume license
- Volume license update
- Display remaining license credits for a Volume License key
- Display remaining support credits for a Volume License key

---

# Configure proxy server: /proxy /set

## Syntax:

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

## Description:

Command /proxy /set is used to configure a proxy server for Internet access.

## Parameters:

- /host: the destination host can be a predefined value (“ie” or “none”) or a user-defined value (e.g: 127.0.0.1 or proxy.company.org). This parameter is mandatory
- /port: the port number used to connect to the proxy server. Required if the hostname value is a custom user-defined value.
- /username: the username to connect to the proxy server. This setting is optional
- /password: the user’s password must be supplied if a username has been defined. However, its value can be empty

## Examples:

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

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

For more information, please go to How to configure a Proxy Server for Internet Access?

---

# Backup data and settings: /backup

## Syntax:

TSplus-Security.exe /backup [DestinationDirectoryPath]

## Description:

Command /backup is used to backup TSplus Advanced Security data and settings.

By default, the backup will be created in the archives directory located in Advanced Security setup directory (e.g.: C:\Program Files (x86)\TSplus-Security\archives).

## Parameters:

- DestinationDirectoryPath: to backup in another directory than the default one. Relative and absolute paths are allowed.

## Examples:

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

For more information, please go to Advanced - Backup and Restore

---

# Restore data and settings: /restore

## Syntax:

TSplus-Security.exe /restore [Backup Directory Path]

## Description:

Command /restore is used to restore TSplus Advanced Security data and settings.

The specified backup directory path must be created by the /backup command or from the Backup feature from the aplication.

## Parameters:

- Backup Directory Path: the path where is located the backup directory to restore.

## Examples:

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

For more information, please go to Advanced - Backup and Restore

---

# Remove and unblock all blocked IP addresses: /

# unblockall

## Syntax:

TSplus-Security.exe /unblockall

## Description:

Command /unblockall is used to remove all blocked IP addresses from TSplus Advanced Security's firewall and unblock them from Microsoft Windows Defender firewall if required.

## Examples:

TSplus-Security.exe /unblockall

For more information, please go to Firewall

---

# Remove and unblock specified IP addresses: / unblockips

## Syntax:

TSplus-Security.exe /unblockips [IP addresses]

## Description:

Command /unblockips is used to remove all specified blocked IP addresses from TSplus Advanced Security's firewall and unblock them from Microsoft Windows Defender firewall if required.

This command has no effect on IP addresses already blocked by Hacker IP protection. If you still want to unblock one of these addresses, please use the whitelist command.

## Parameters:

- IP addresses: the list of ip addresses or ip ranges to unblock (coma or semicolon separated).

## Examples:

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

For more information, please go to Firewall

---

# Block specified IP addresses: /blockips

## Syntax:

TSplus-Security.exe /blockips [IP addresses] [Optional Description]

## Description:

Command /blockips is used to block all specified IP addresses using TSplus Advanced Security's firewall and block them using Microsoft Windows Defender firewall if configured.

## Parameters:

- IP addresses: the list of ip addresses or ip ranges to block (coma or semicolon separated).
- Optional Description: an optional description which will be added for each entry.

## Examples:

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "John's workplaces"

For more information, please go to Firewall

---

# Add IP addresses to whitelist: /addwhitelistedip

## Syntax:

TSplus-Security.exe /addwhitelistedip [IP addresses] [Optional Description]

## Description:

Command /addwhitelistedip is used to add specified IP addresses to the authorized IP addresses of TSplus Advanced Security's firewall and unblock them from Microsoft Windows Defender firewall if required.

## Parameters:

- IP addresses: the list of ip addresses or ip ranges to whitelist (coma or semicolon separated).
- Optional Description: an optional description which will be added for each entry.

## Examples:

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "John's workplaces"

For more information, please go to Firewall

---

# Add a program or directory to Ransomware Protection auhorized list: /whitelist

## Syntax:

TSplus-Security.exe /whitelist add [Authorized Paths]

## Description:

Command /whitelist add is used to add specified program paths and directory paths to the authorized list of TSplus Advanced Security's Ransomware Protection.

## Parameters:

- Authorized Paths: the list of program paths and directory paths to add to TSplus Advanced Security's Ransomware Protection authoriaztion list (semicolon separated).

## Examples:

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

For more information, please go to Ransomware Protection Action

---

# Refresh Hacker IP Protection: /refreshipprotection

## Syntax:

TSplus-Security.exe /refreshipprotection

## Description:

Command /refreshipprotection is used to refresh the list of blocked IP ranges for the Hacker IP protection feature. Support and Updates Services subscription is required.

## Examples:

TSplus-Security.exe /refreshipprotection

For more information, please go to Hacker IP Protection

---

# Set log level: /setloglevel

## Syntax:

TSplus-Security.exe /setloglevel [Log Level]

## Description:

Command /setloglevel is used to set the log level for all Advanced Security's components.

## Parameters:

- Log Level: the log level among the following values : ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF

## Examples:

TSplus-Security.exe /setloglevel ALL

For more information, please go to Advanced > Logs

---

# Add trusted devices: /addtrusteddevices

## Syntax:

TSplus-Security.exe /addtrusteddevices [Trusted Devices Configuration]

## Description:

Command /addtrusteddevices is used to add trusted devices programmatically. Requires Ultimate edition.

## Parameters:

- Trusted Devices Configuration: The argument is composed of a list of trusted devices (semicolon separated), structured as follows:

Username and Devices are separated by the colon character (,).

**Username Details:**

User Type and Full Username are separated by the colon character (:). Accepted user types are "user" and "group".

Optional Keyword "disabled": if included, the trusted devices will be created, but restrictions will be disabled for this user. If not mentioned, restrictions are enabled by default.

**Device Details:**

Device Name and Optional Comment: separated by the equal sign character (=).

Devices are separated by the colon character (:).

## Examples:

TSplus-Security.exe /addtrusteddevices “user:WIN-A1BCDE23FGH\admin:disabled,device1name=this is a comment for device 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name:device4name=another comment;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name”

For more information, please go to Trusted Devices

---

# Enable configured trusted devices: / enabletrusteddevices

## Syntax:

TSplus-Security.exe /enabletrusteddevices [User or Groups]

## Description:

Command /enabletrusteddevices is used to enable all configured trusted devices for the specified users and groups.

## Parameters:

- User or Groups: The argument is a list of users and groups (semicolon separated). Within the username, the separation between the user type (“user” and “group” are the only accepted values) and the full username is done by a colon.

## Examples:

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

A1BCDE23FGH\johndoe;group:DESKTOP-A1BCDE23FGH\Administrators”

For more information, please go to Trusted Devices

---

# Disable all trusted devices: /disabletrusteddevices

## Syntax:

TSplus-Security.exe /disabletrusteddevices [User or Groups]

## Description:

Command /disabletrusteddevices is used to disable all configured trusted devices for the specified users and groups.

## Parameters:

- User or Groups: The argument is a list of users and groups (semicolon separated). Within the username, the separation between the user type (“user” and “group” are the only accepted values) and the full username is done by a colon.

## Examples:

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

For more information, please go to Trusted Devices

---

# Setup Ransomware Protection driver: /setup-driver

## Syntax:

TSplus-Security.exe /setup-driver

## Description:

Command /setup-driver installs the Ransomware Protection driver. This operation is normally perfomed during installation.

## Examples:

TSplus-Security.exe /setup-driver

For more information, please go to Ransomware Protection

---

# Uninstall Ransomware Protection driver: /uninstalldriver

## Syntax:

TSplus-Security.exe /uninstalldriver

## Description:

Command /uninstalldriver uninstall the Ransomware Protection driver. This operation is normally perfomed during Advanced Security uninstallation.

## Examples:

TSplus-Security.exe /uninstalldriver

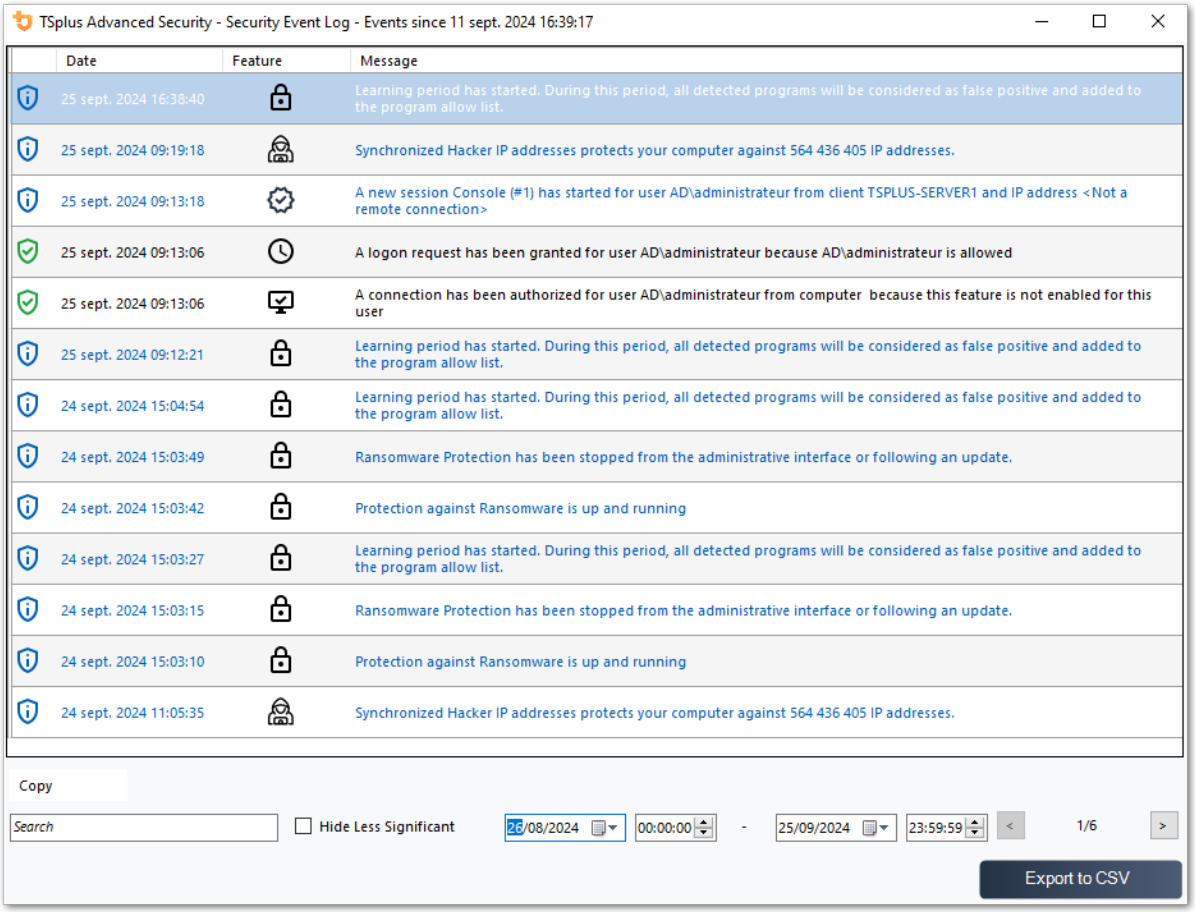
For more information, please go to Ransomware Protection

# Events

The security events are a great source of information as they display the operations performed by TSplus Advanced Security to protect your computer.

The Events window can be opened from the TSplus Advanced Security main window, by clicking directly on the last 5 events displayed or on the dashbord tab. The information displayed on the Events window are refreshed automatically every few seconds.

The list of security events presents 4 columns, which describes the severity, the date of the check or performed operation, the associated feature icon and the description.




The description of the event often explains why the action was performed or not. Retaliatory actions are often written in red and highlighted with a red shield icon.

Events window can be moved around and does not prevent you from using the other TSplus

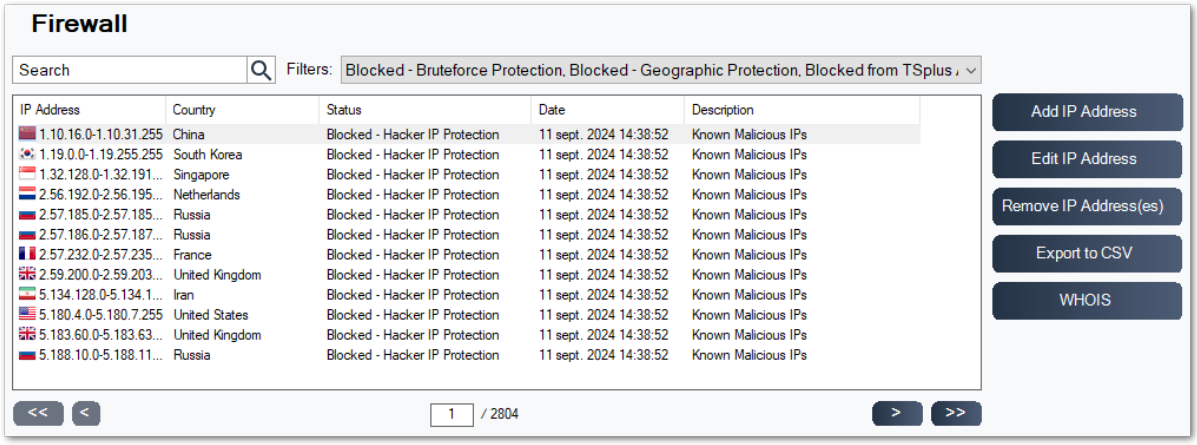
Advanced Security feature.

# Navigating and Searching through events

- A deep global search is now available in order to find specific events quickly.
- Next to the global search, 2 date and time pickers filters the displayed events according to the date the event was raised.
- On the right, arrows allows to change pages and navigate to view older events.

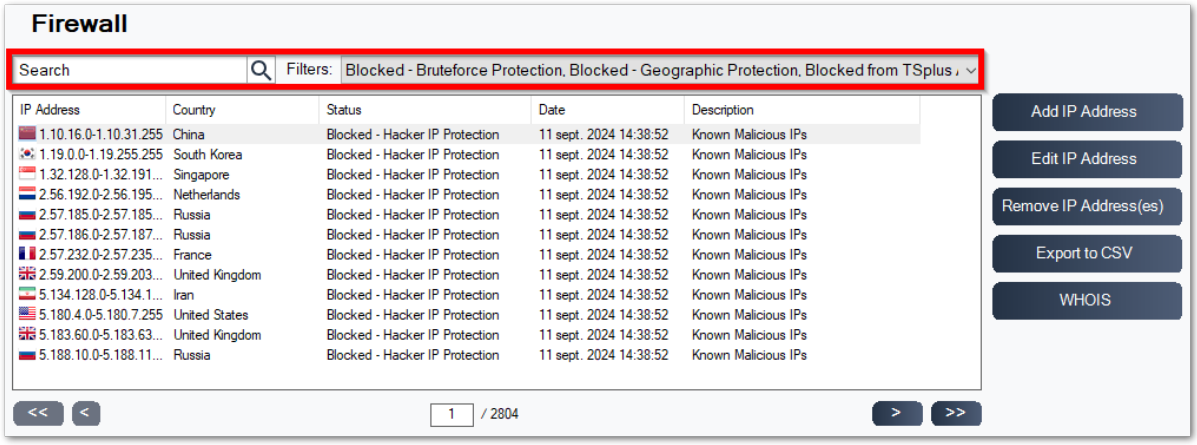
# Firewall

IP addresses management is easy with a single list to manage both blocked and whitelisted IP addresses:

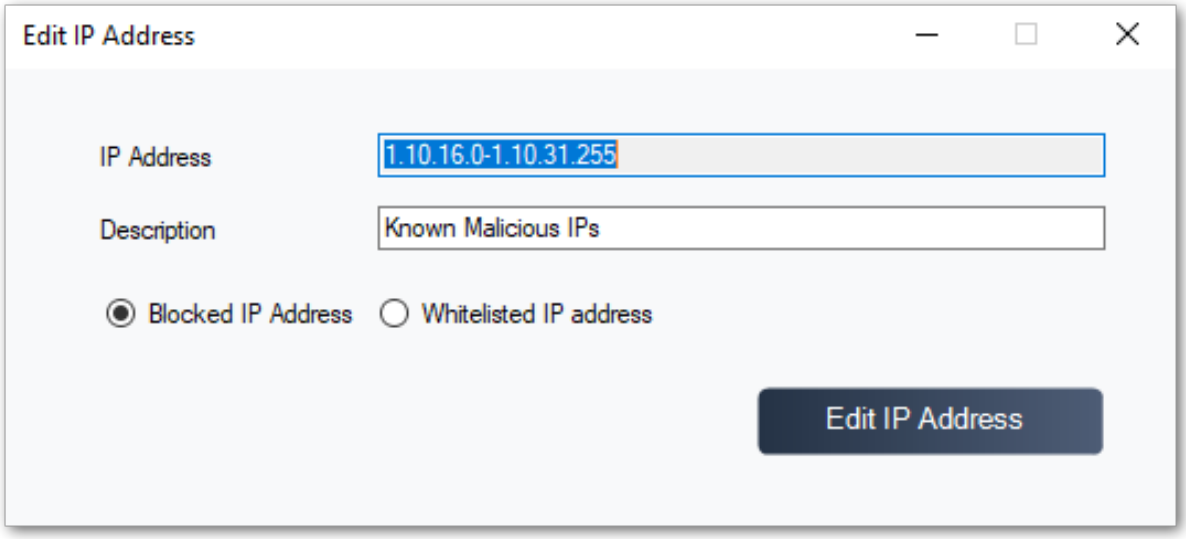



By default, IPV4, IPV6 and all server localhosts addresses are whitelisted.

A convenient search bar and filter provides search capabilities based on all the information provided.




Furthermore, administrators are able to perform actions on several selected IP addresses with a single click. Among the new features IP addresses management introduced, you will find the possibility to provide meaningful descriptions to any IP addresses:




Last but not least, administrators are now able to unblock and add to whitelist multiple blocked IP addresses in a single action, by clicking on the “Add Existing to Whitelist” tab.

# Using the command line to whitelist or block IP addresses and/or IP ranges

- In order to **whitelist** IP addresses or IP range(s), the command has this syntax :

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

You may whitelist several IP addresses, with a **comma or semi-colon delimiter**. Moreover, you can specify IP address ranges, instead of simple IP addresses. The syntax is : **x.x.x.x-y.y.y.y** Finally, you may indicate an optional description of the whitelist rule

Here is an example of a complete command : TSplus-Security.exe addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 “John’s workplaces”

- In order to **block** IP addresses or IP range(s), the command has a similar syntax :

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

- In order to **unblock** IP addresses or IP range(s), the command has a similar syntax :

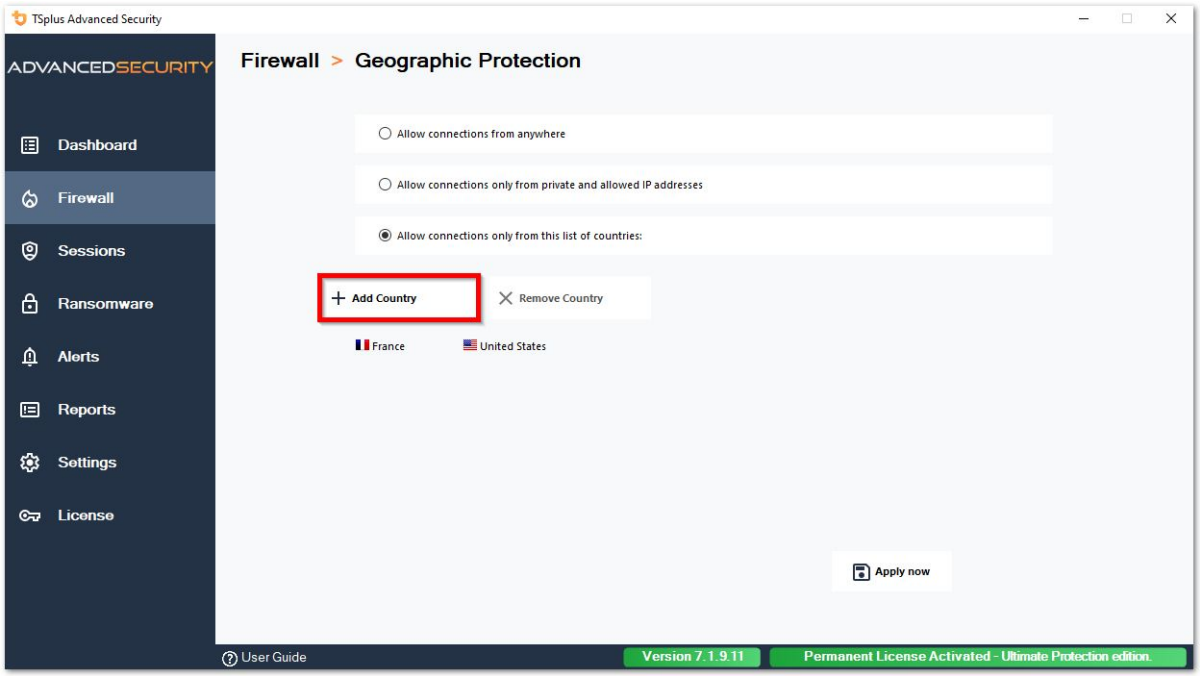
TSplus-Security.exe unblockips [ip addresses]

This command has no effect on IP addresses already blocked by Hacker IP protection. If you still want to unblock one of these addresses, please use the whitelist command.

# Geographic Protection

## Restrict access from other countries

To allow remote access from only specific countries, select the “Allow connections only from this list of countries” button and then click on the “Add country” button.

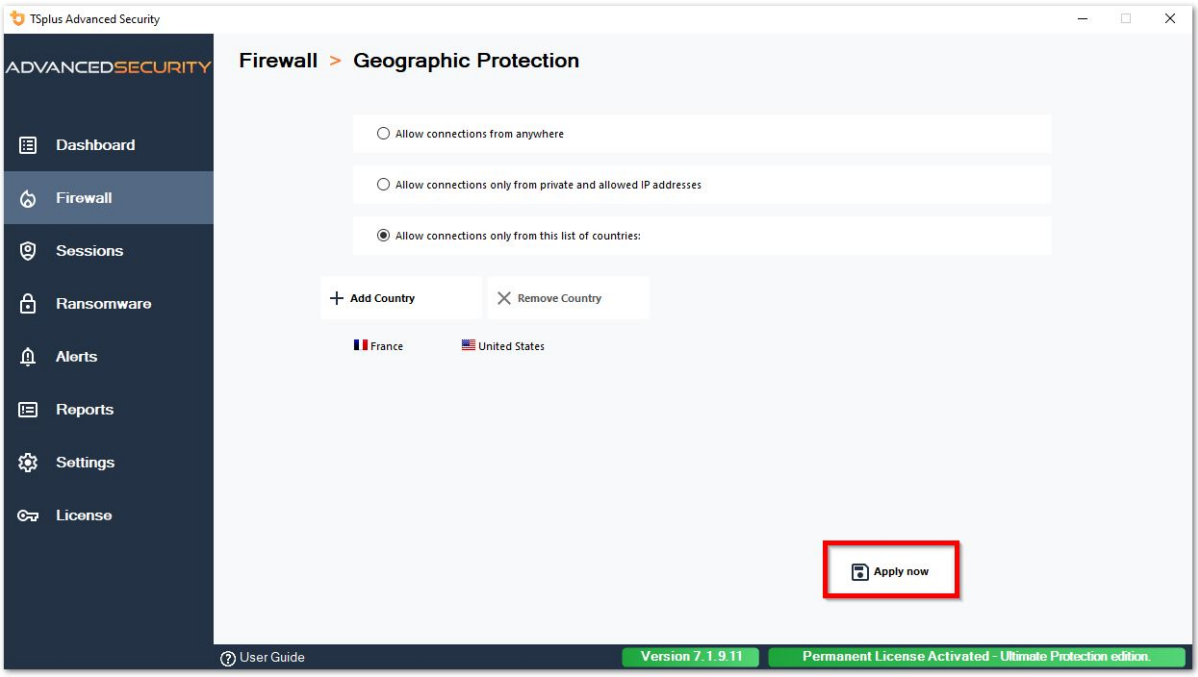



A popup offering a country list opens. Select the country you wish to add on the list.

You can choose to check the box below to unblock all previously blocked IP addresses for the selected country.

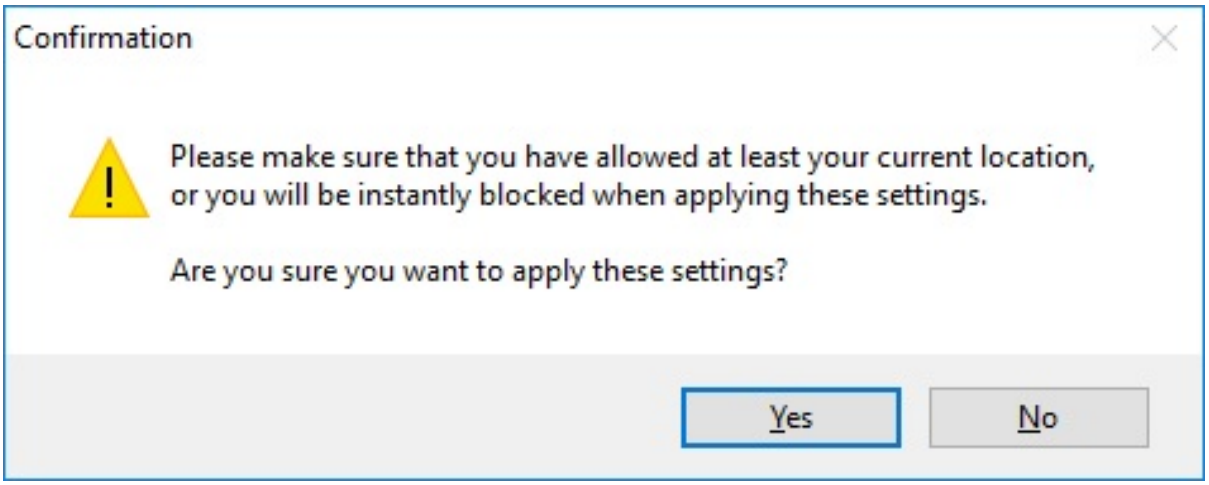
Click on the button “Add Country” to return to the feature main screen.

**Important: In order to save your changes, click on the “Apply” button.**



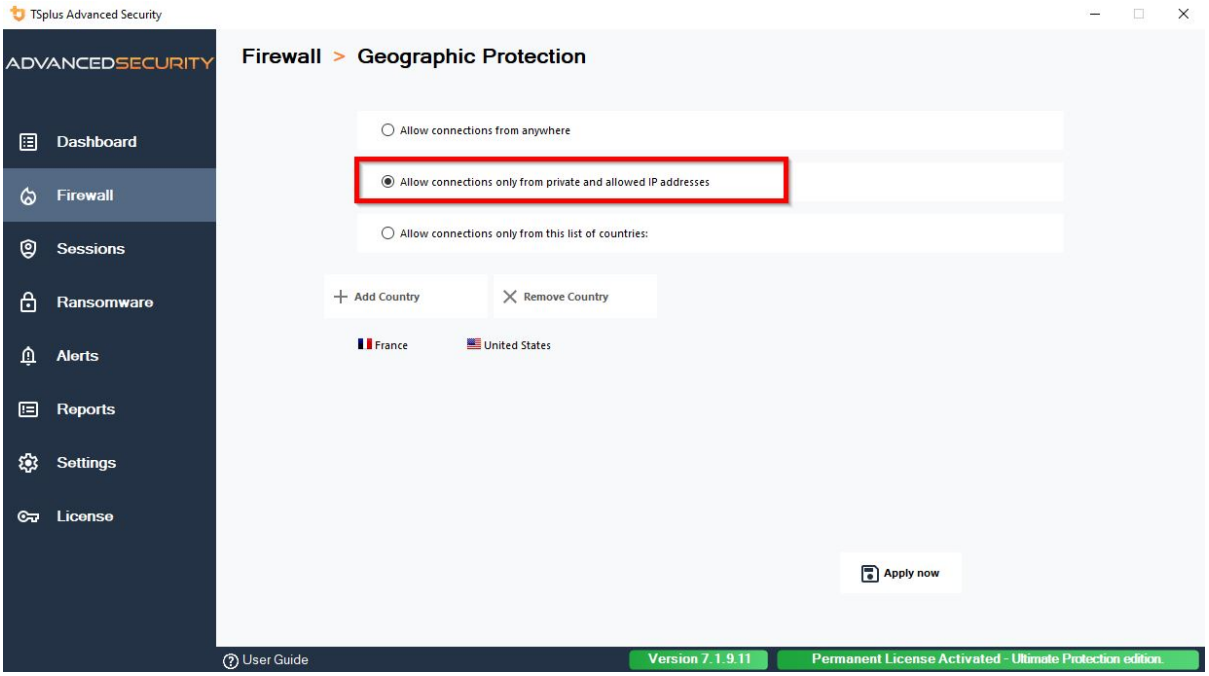

In this example, remote access is allowed for users connecting from United States and France.

A confirmation message appears to avoid blocking the connected user. Click “Yes” to confirm and apply the changes.



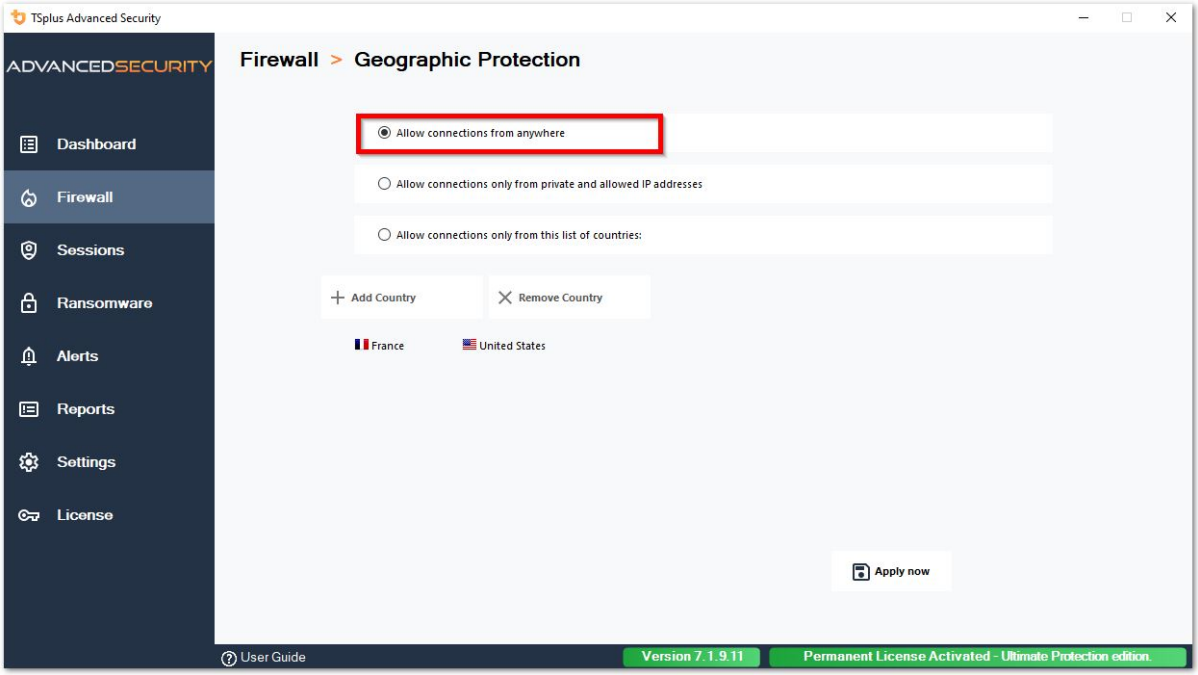

# Restrict access from the internet

Geographic Protection can be configured to restrict the access to your machine to only private and whitelisted IP addresses, as shown below:




# Disable Geographic Protection

By default, Geographic Protection allows access for users connecting from all over the world:




# Unblocking blocked IP addresses

When an IP address gets blocked, it appears on the Firewall tab. Blocked IP addresses can then be unblocked and eventually added to the list of allowed IP addresses.

If you get blocked, we recommend that you try connecting from any country you allowed on TSplus Advanced Security, for instance by connecting from another remote server or using a VPN service. You can also use a console session to connect, as this session is not a remote session and will not be blocked by TSplus Advanced Security.

**Important:**

- Check that you have selected the country where you are currently connected from. Otherwise, your IP address will be blocked quickly after applying the settings, thus disconnecting you without any hope of connecting back again from the same IP address.

- Consider adding your own IP address to the list of allowed IP Addresses to avoid being blocked by either Geographic Protection or Bruteforce Protection features.

# Undestanding Geographic Protection

Geographic Protection checks incoming TCP network connexion, both IPv4 and IPV6 (except when the legacy Windows API mode is configured).

**Processes:** Geographic Protection listens to connexions sent to the TSplus Remote Access'

Web server by default, if installed. The name of the corresponding process is HTML5 Service. If you wish to disable its monitoring or check connections destined to other processes, go to Settings > Advanced > Geographic Protection.

**Network ports:** by default, Geographic Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC. Geographic Protection supports the following VNC providers: Tight VNC, Ultra VNC, Tiger VNC and Real VNC, which are not related whatsoever with TSplus. If you wish to disable its monitoring or check connections destined to other ports, go to Settings > Advanced > Geographic Protection.

**Detection mechanisms:**

Geographic Protection detects inbound connections from unauthorized countries using three differents detection mechanisms:

- Windows API
- Event Tracing for Windows
- Built-In Firewall

On the one hand, Event Tracing for Windows is an efficient kernel-level tracing facility that capture network events in real time. Event Tracing for Windows is recommended with Windows Firewall enabled (default).

On the other hand, Windows API works great given any specific network configuration but may add a constant pressure on CPU depending on the amount of active connections. Please note that Windows API is not compatible with IPv6 yet.

Built-In Firewall enables user-mode capturing and dropping of network packets sent to the Windows network stack. When the Built-In Firewall is configured to block unwanted connections, it is recommended to use it to enforce Geographic Protection's allowed countries.

**Geolocation:** Advanced Security includes geolocation data published by MaxMind, available from http://www.maxmind.com. If you find an IP address not registered in its actual country, please contact MaxMind directly to fix the issue.

# Troubleshooting

If you ever notice that Geographic Protection does not block connections coming from a country which is actually not in the authorized countries' list, it is certainly because:

**Antivirus:** In order to block an IP address, Geographic Protection adds a blocking rule on the Windows firewall. So, firstly, the firewall must be active. You also have to check if some firewall parameters are not handled by an other program, like an antivirus. In this case, you will have to deactivate this program and restart the service "Windows Firewall". You can also contact your third-party program editor and ask them to find a way for their program to respect the rules when added to the Windows firewall. If you know any software editor's technical contact, we are ready

to develop these “connectors” for the firewall. Contact us.

**VPN:** In case the remote client uses a VPN, Geographic Protection will get an IP address chosen by the VPN provider. As you know, VPN providers use relays all around the globe to allow its users to browse anonymously. Some VPN providers allow users to define the relay’s country. Thus, users with VPN providers may be relayed through an unauthorized country. For example, if a VPN provider choses an IP from Sri Lanka, this country must be authorized by Geographic Protection. Also, if the VPN uses an internal corporate IP address, then the protection becomes irrelevant.

**Firewall / Proxy:** The purpose of an hardware firewall is to filter incoming and outgoing connections for large companies. As it is only a filter, it should not modify the originating IP address and therefore should not impact Geographic Protection. However, a proxy would definitively change the originating IP address to use a private network address, which will always be allowed by Geographic Protection. The primary purpose of this feature is to block access to a server opened to the Internet. If all connections comes from the corporate network, then the protection becomes irrelevant.

# Hacker IP Protection

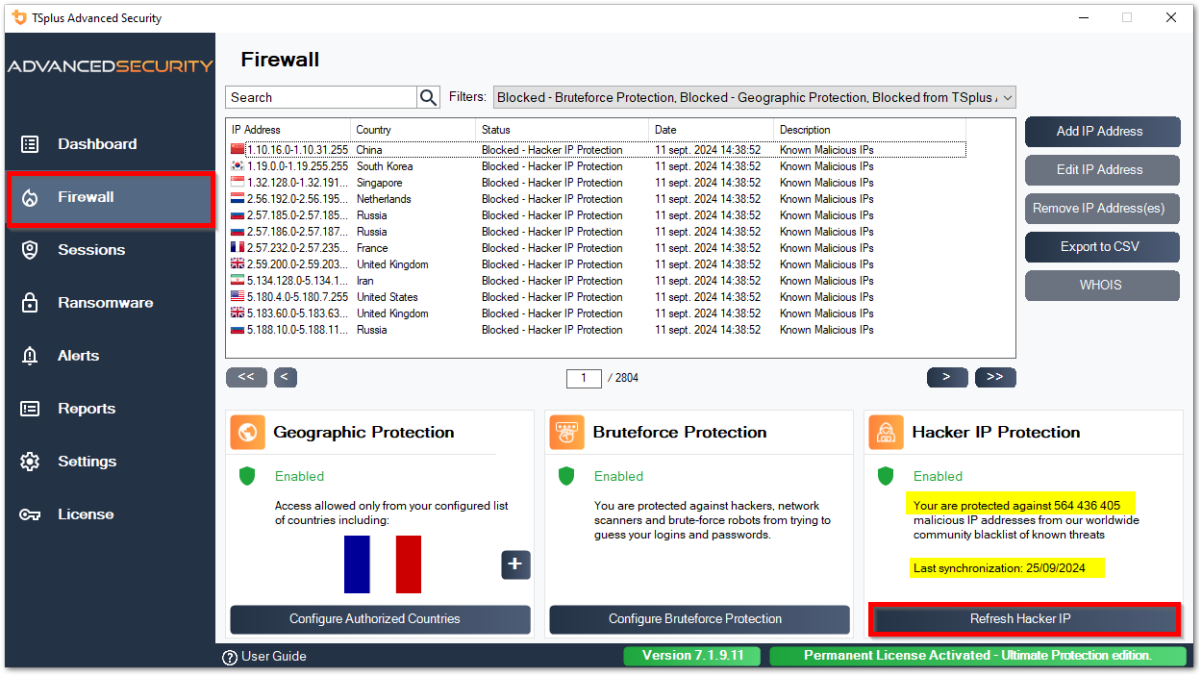
Keep your machine protected against known threats such as on-line attacks, on-line service abuse, malwares, botnets and other cybercrime activities with the Hacker IP Protection. The objective is to create a blacklist that can be safe enough to be used on all systems, with a firewall, to block access entirely, from and to its listed IPs

**Support and Updates Services subscription is required.**

The key prerequisite for this cause, is to have no false positives. All IPs listed should be bad and should be blocked, without exceptions. To accomplish this, Hacker IP Protection leverages the information provided by the community of Advanced Security's users.

Hacker IP Protection is updated automatically every day.

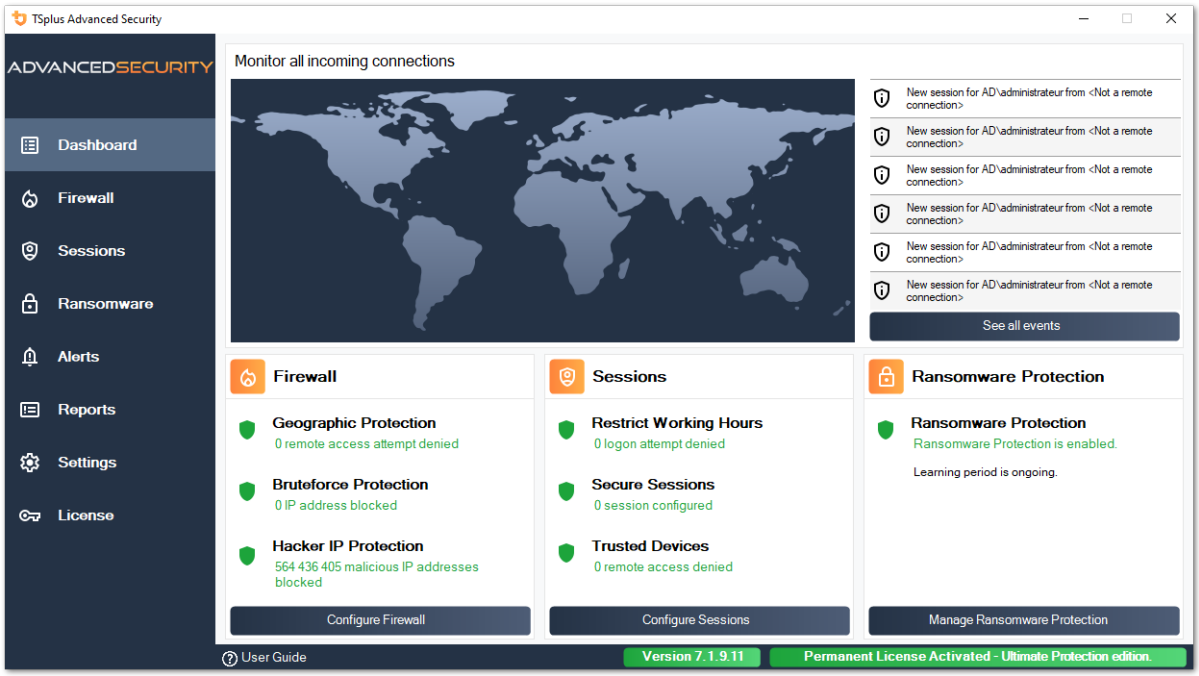
You can update manually from the "Blocked IP Addresses" tab, by clicking on the "Refresh Hacker IP" button:




As a result, the feature should create approx. 600 000 000 bloxking firewall rules in Windows Firewall.

# Dashboard

Click on each tile to know more about each feature




The menu bar on the left provides access to the different features. Each tile gives you access to the various features and settings offered by TSplus Advanced Security.

Advanced Security displays the six last Security Events. Click on any event to open the complete list of events in a separate window.

Below the last events, three tiles provide quick access to:

1. Firewall

2. Sessions

3. Ramsomware Protection

Please select your display language using the dropdown located in the top right corner, should the application did not detect your language.

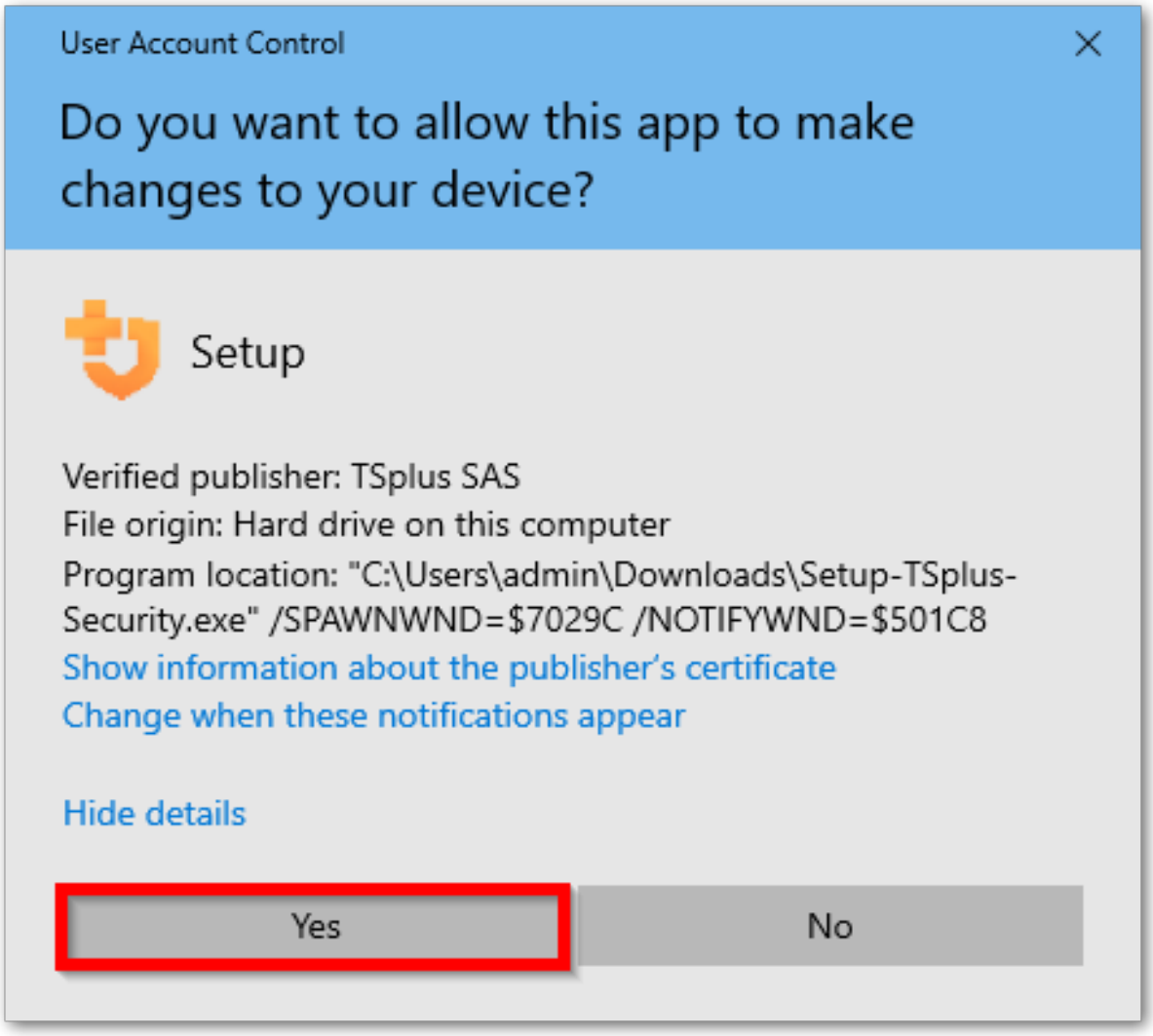
Finally, clicking on the “Help” button will redirect you to this documentation.

# Installing TSplus Advanced Security

## Installing Advanced Security

**Run** TSplus Advanced Security Setup program and then **follow the installation steps**.

You must run the setup program as an Administrator and accept the software's license agreement.



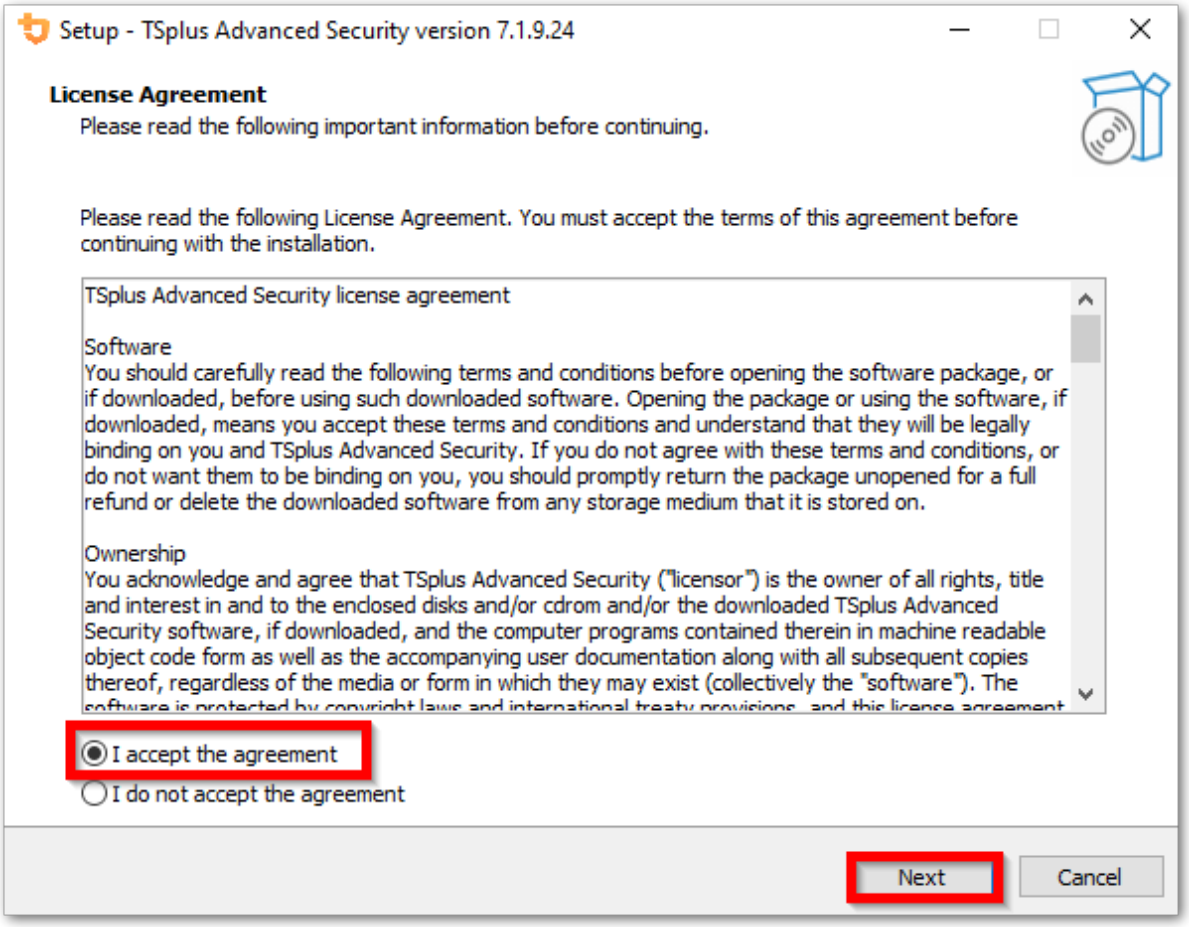

Select the setup assistant language if not detected automatically.

Then, select one of the two options: **Recommended** or **Advanced** by clicking on the corresponding boxes.

The Advanced option adds aditionnal steps which allows you to:

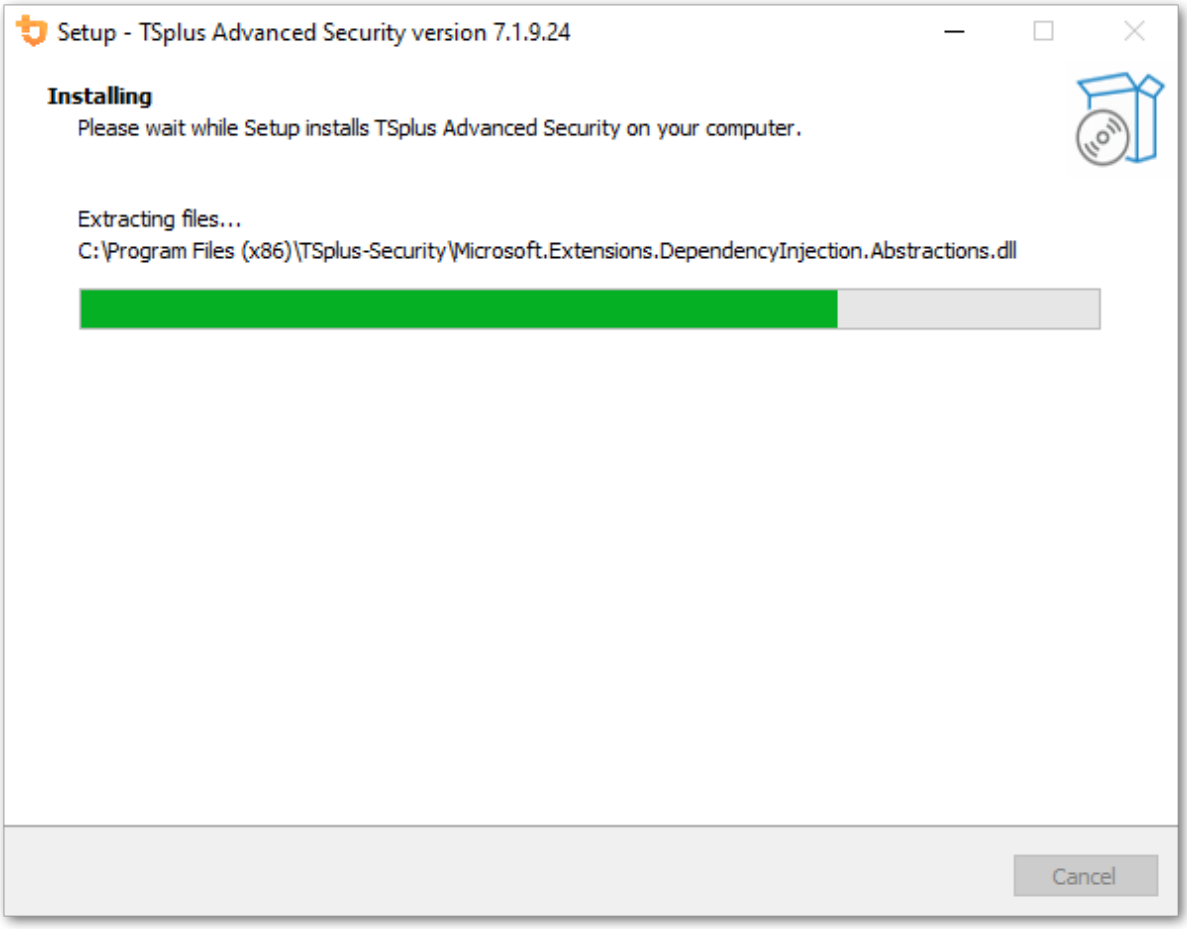
- Only download setup (do not install)
- Use custom proxy settings

Read the licensing agreement and click “I agree” to resume installation.




The program will install on your computer.

A progress bar is displayed at the bottom and reports the progress of the installation.




**Please be patient**, as it can sometimes take up to a few minutes to fully install the software.

Once the installation has completed, you can start using TSplus Advanced Security!

The free trial version is fully featured for 15 days. Don't forget to activate your license and to update to the latest version to keep Advanced Security protection at its best!

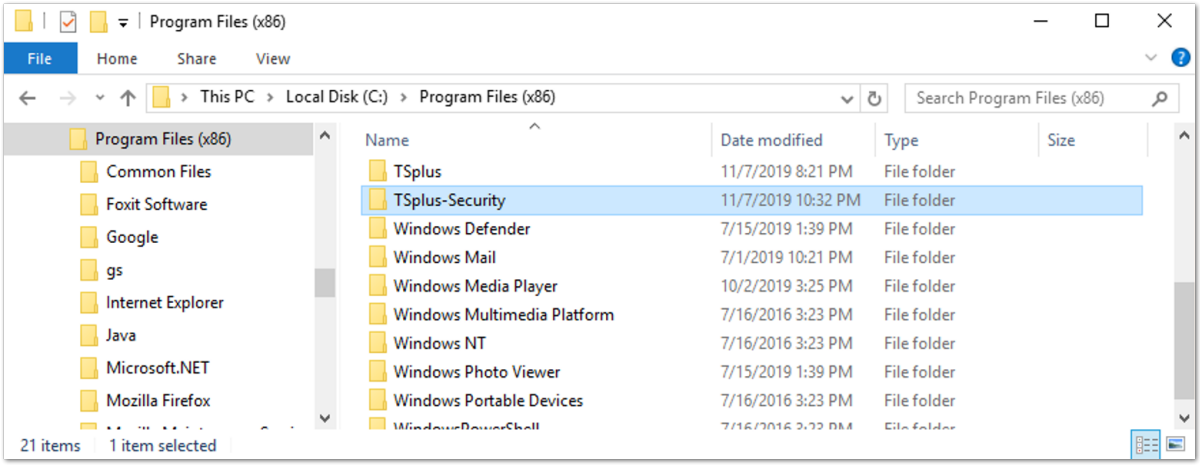
# Advanced installation scenarios

The TSplus Advanced Security Classic Setup program handles the following scenarios as it can be executed from the command line:

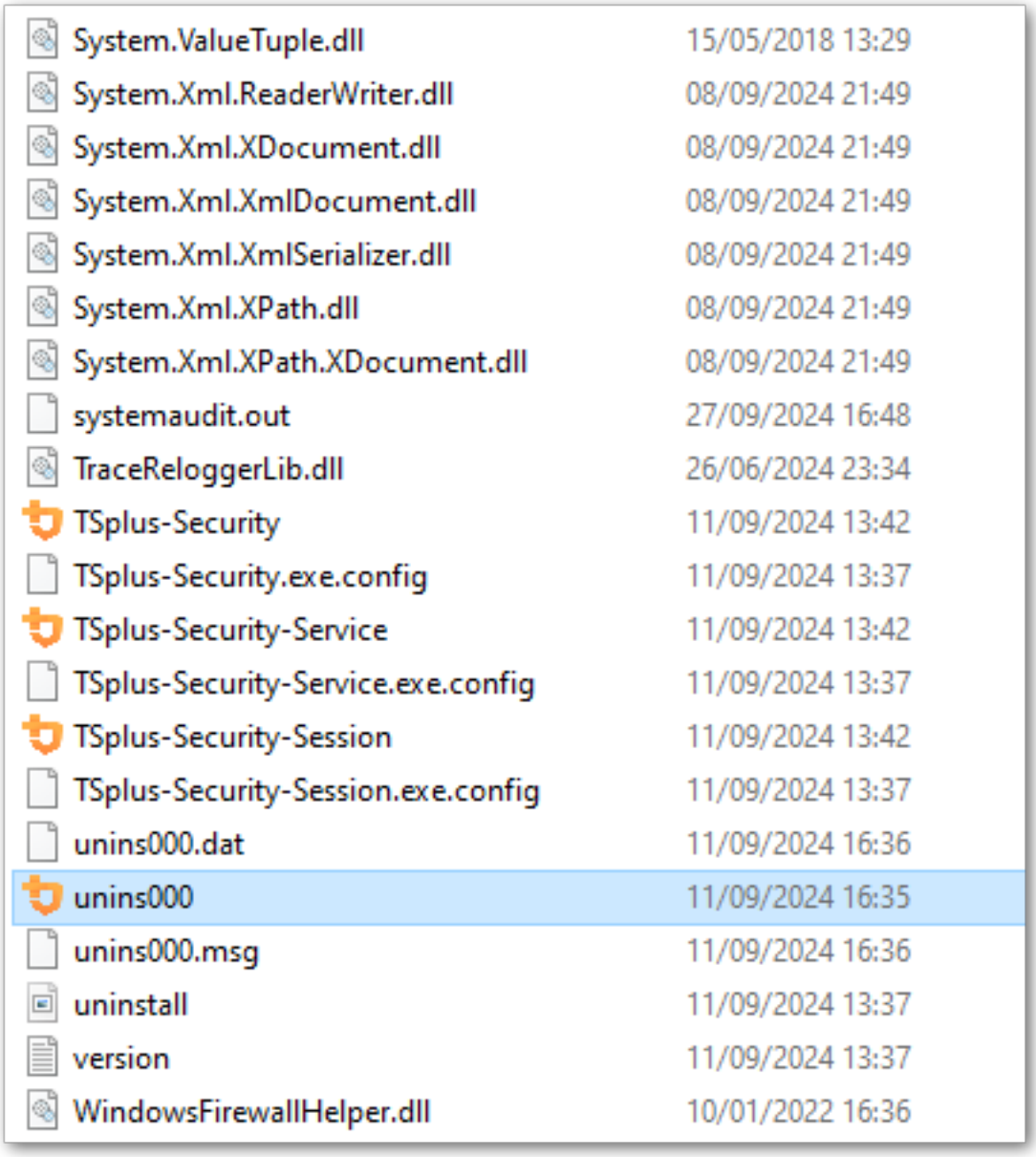
- Install silently, by providing the /VERYSILENT /SUPPRESSMSGBOXES parameters
- Prevent rebooting at the end of the setup, by providing the /NORESTART parameter. This parameter is usually used along with the above.
- Volume Licensing to activate your license directly while installing (please refer to the documentation or contact us for more information)

# Uninstall TSplus Advanced Security

In order to completely uninstall TSplus Advanced Security, open the directory C:\Program Files (x86)\TSplus-Security.



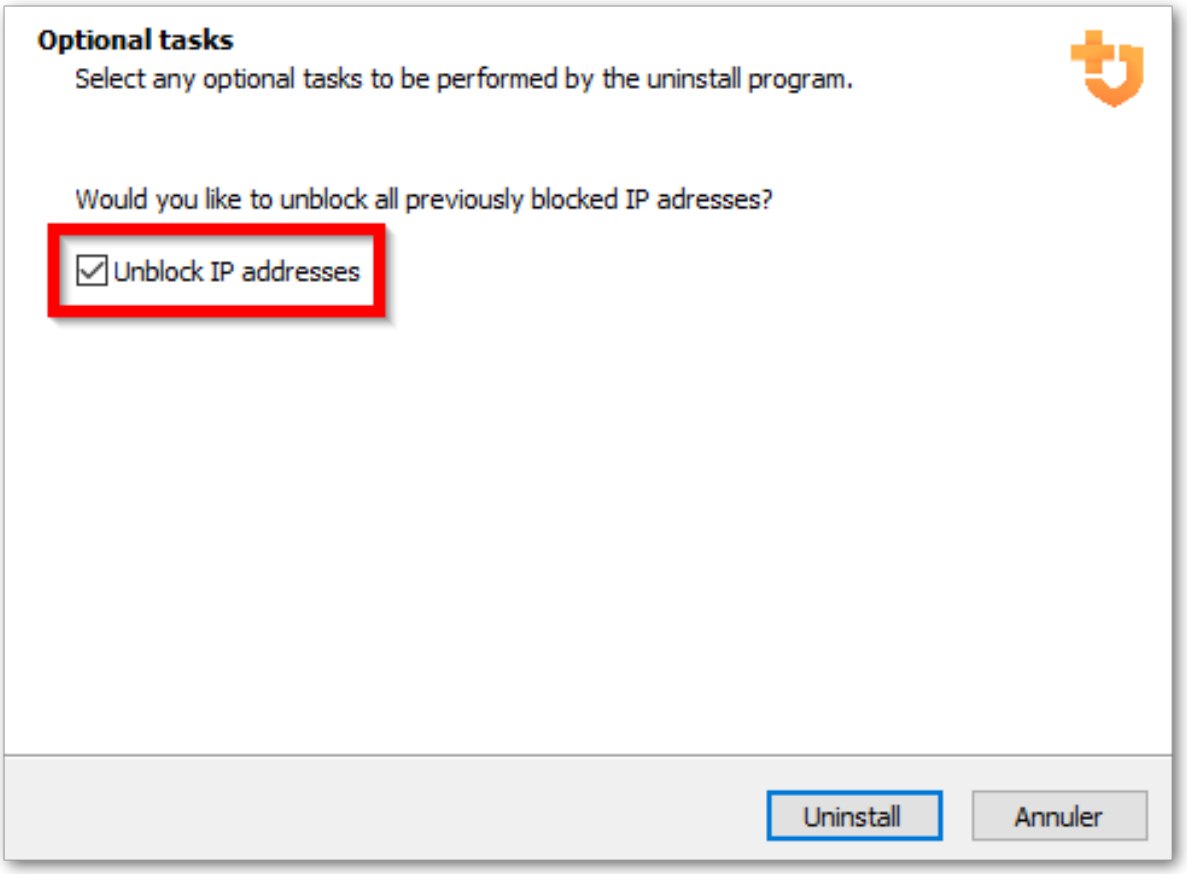

Then, double-click on the "unins000" application to execute the uninstall program.




Click on yes on the next window to completely remove TSplus Advanced Security and all of its components.

Unless configured otherwise, Advanced Security adds blocking rules to the Windows Firewall. Click “Unblock IP addresses” to unblock and remove all the IP addresses previously blocked by Advanced Security.

**Important:**: Please be mindful that removing all the rules can take up to one hour. Because of this, we would recommend to remove the rules directly from the Windows Firewall with Advanced Security console.




The software will be completely uninstalled from your machine.

# Permissions Management

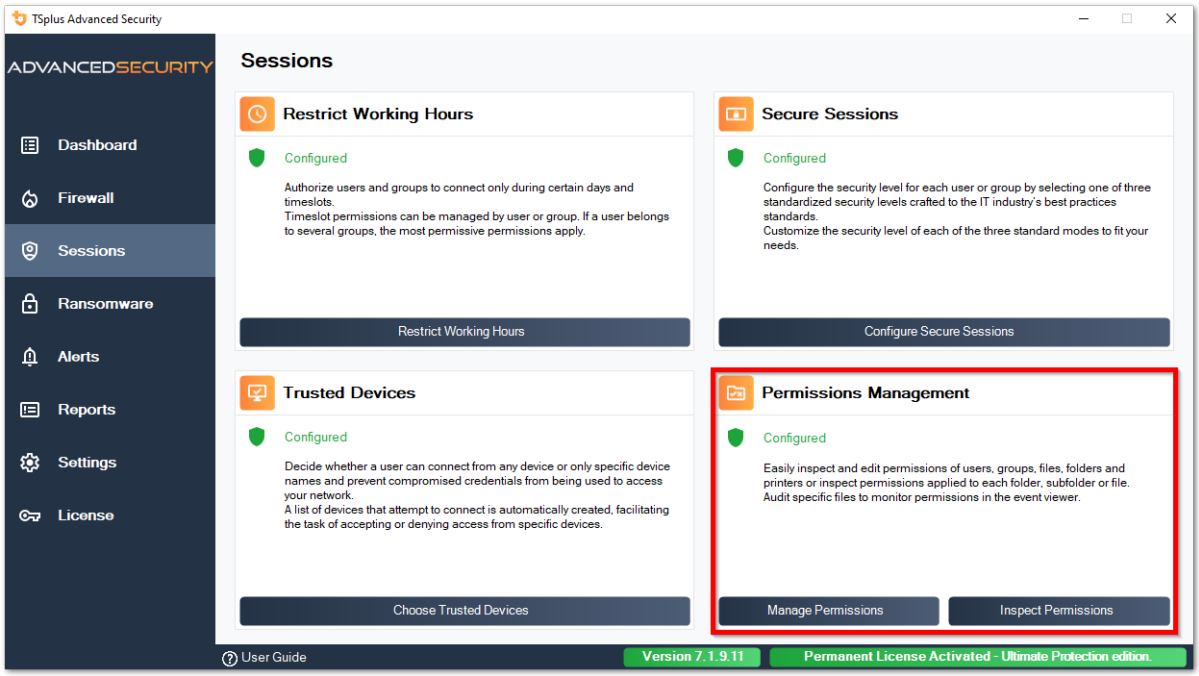
Since version 4.3, TSplus Advanced Security offers a Permissions functionality, allowing the administrator to manage and/or inspect users/groups privileges.

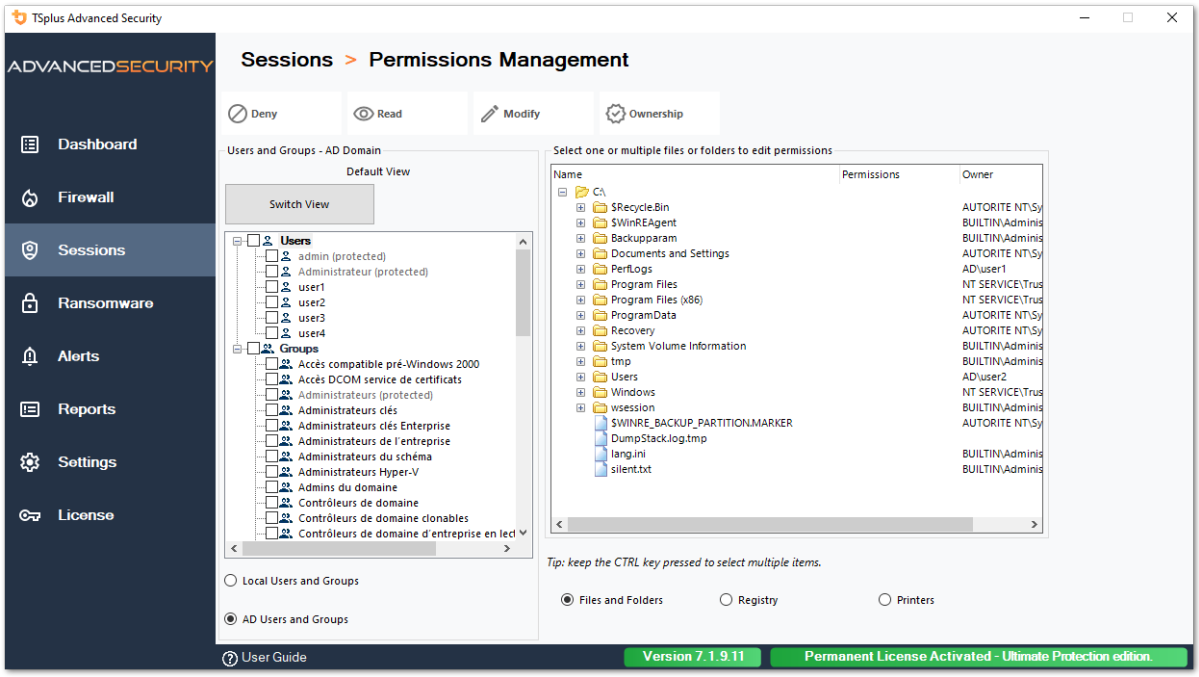
On the Permissions dashboard, the list of users and groups and the list of available **files, folders registries and printers** are showed side-by-side.

Everything is visible at one sight, which makes it super easy to **Inspect** and **Manage/Edit** privileges for one user at a time and therefore to increase the accuracy of the restrictions.

## Manage Permissions

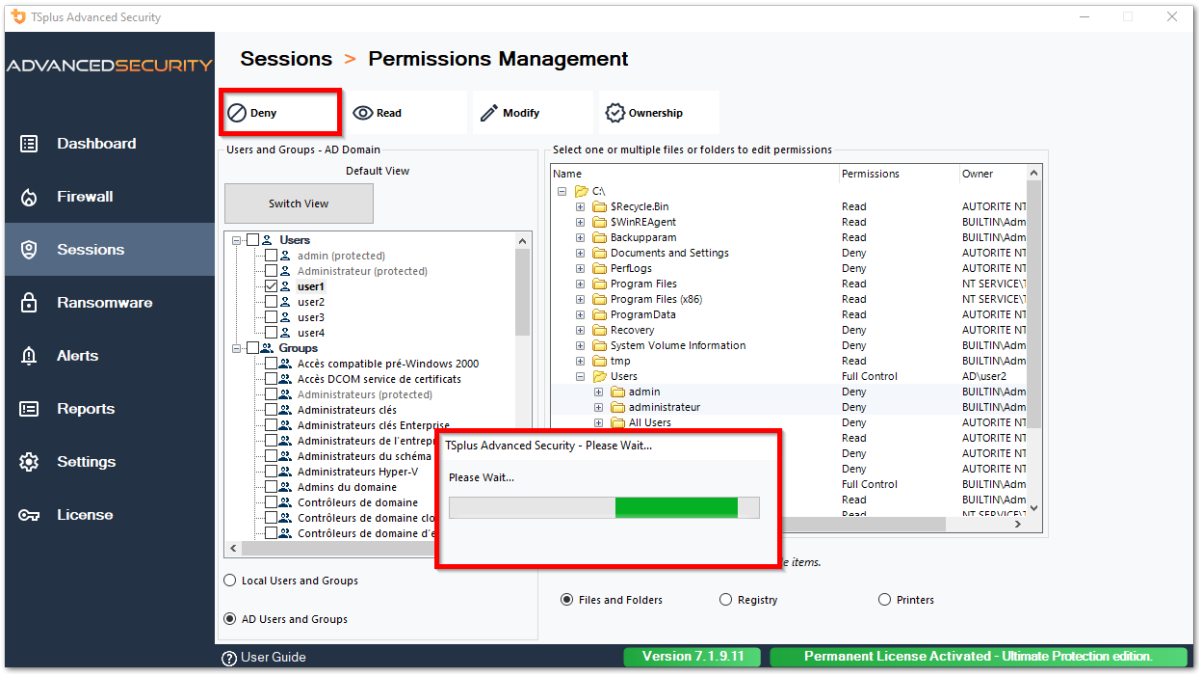
On the Manage tab, for each user or group selected on the left tree view, you can:



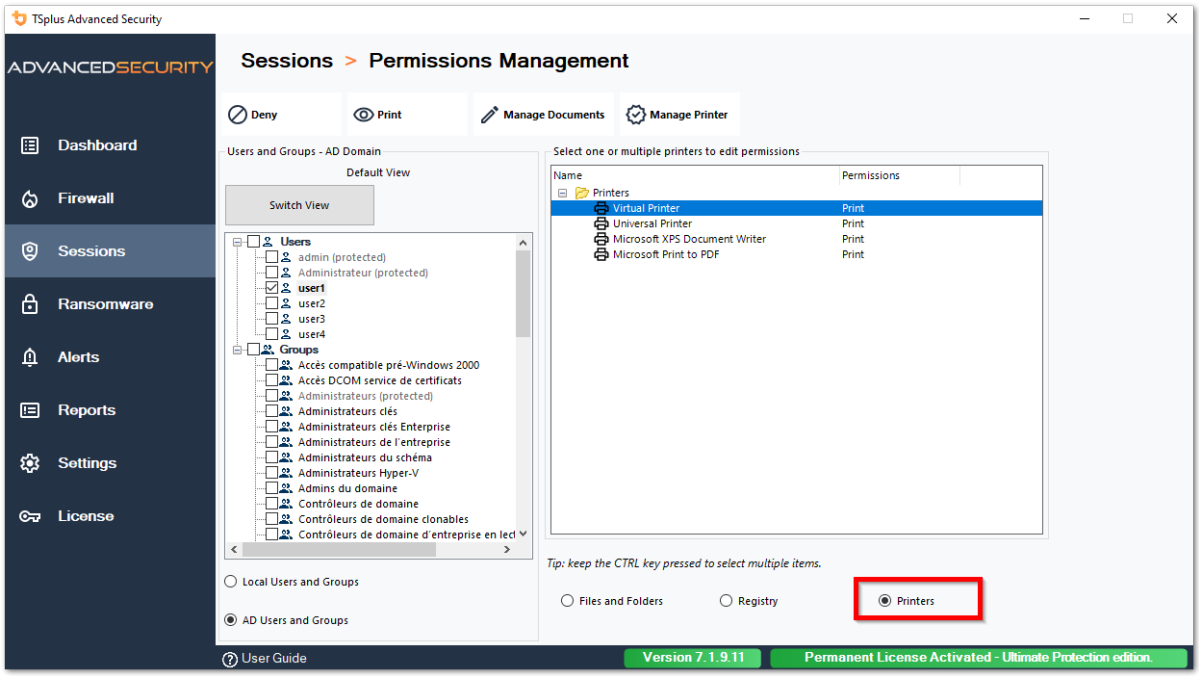



- **Deny** - When clicking on the Deny button, the selected user will be denied privilege on the selected filesystem object. If a file is selected, then the selected user is denied the privilege of reading the selected file (FileSystemRights.Read). If a directory is selected, then the selected user is denied the privilege of reading and listing the directory content (FileSystemRights.Read and FileSystemRights.ListDirectory).
- **Read** - When clicking on the Read button, the selected user will be granted privilege on the selected filesystem object. If a file is selected, then the selected user is granted the privilege of reading the selected file and executing if the file is a program (FileSystemRights.ReadAndExecute) . If a directory is selected, then the selected user is granted the privilege of reading and listing or executing the directory content (FileSystemRights.ReadAndExecute and FileSystemRights.ListDirectory and FileSystemRights.Traverse).
- **Modify** - When clicking on the Modify button, the selected user will be granted privilege on the selected filesystem object. If a file is selected, then the selected user is granted the privilege of modifying the selected file (FileSystemRights.Modify) . If a directory is selected, then the selected user is granted the privilege of modifying and listing the directory content, as well as creating new files or directories (FileSystemRights.Modify and FileSystemRights.CreateDirectories and FileSystemRights.CreateFiles and FileSystemRights.ListDirectory and FileSystemRights.Traverse).
- **Ownership** - When clicking on the Ownership button, the selected user will be granted full control over the selected filesystem object (FileSystemRights.FullControl).

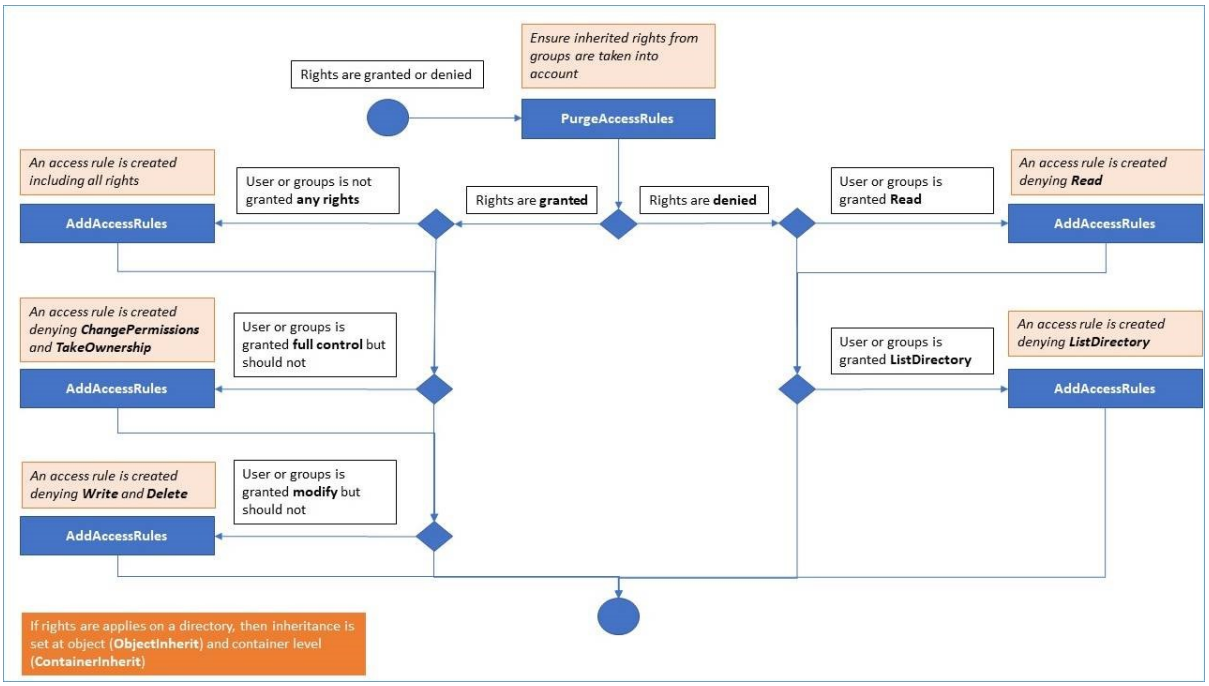
Same permissions options are possible for each Registry, by selecting the corresponding button under the right-tree view :




And for each Printer:




Please note that all permissions denied or granted to a directory are applied recursively to the filesystem objects contained by this directory. The diagram below details the API calls when rights are applied to a filesystem object:

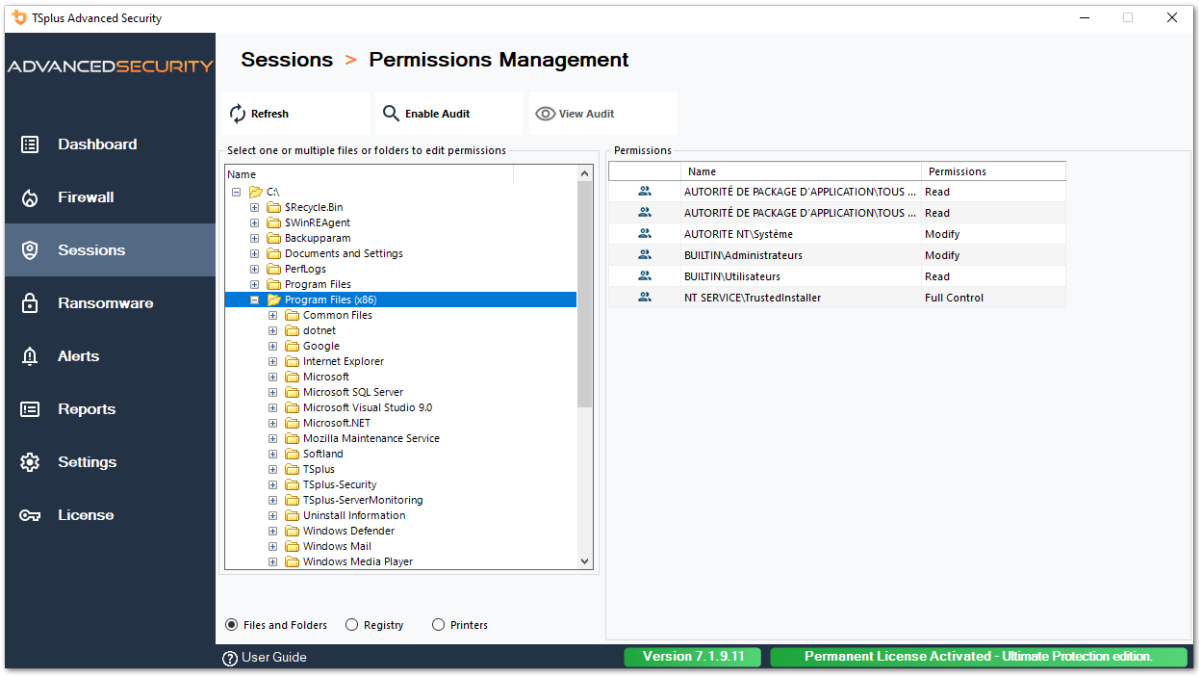



**Documentation**:

- Object Security: https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- FileSystemRights: https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

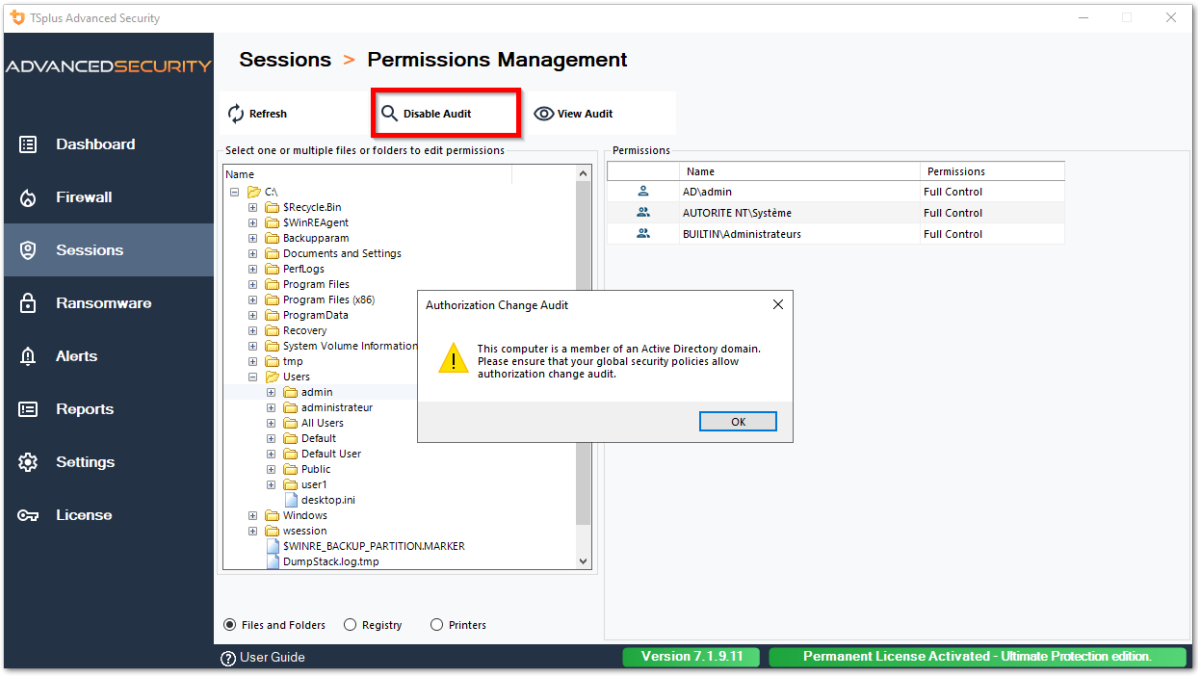
# Inspect Permissions

On the Inspect tab, for each folder, subfolder or file selected on the left tree view, you can see the corresponding attributed permissions to users or groups on the right tree view.

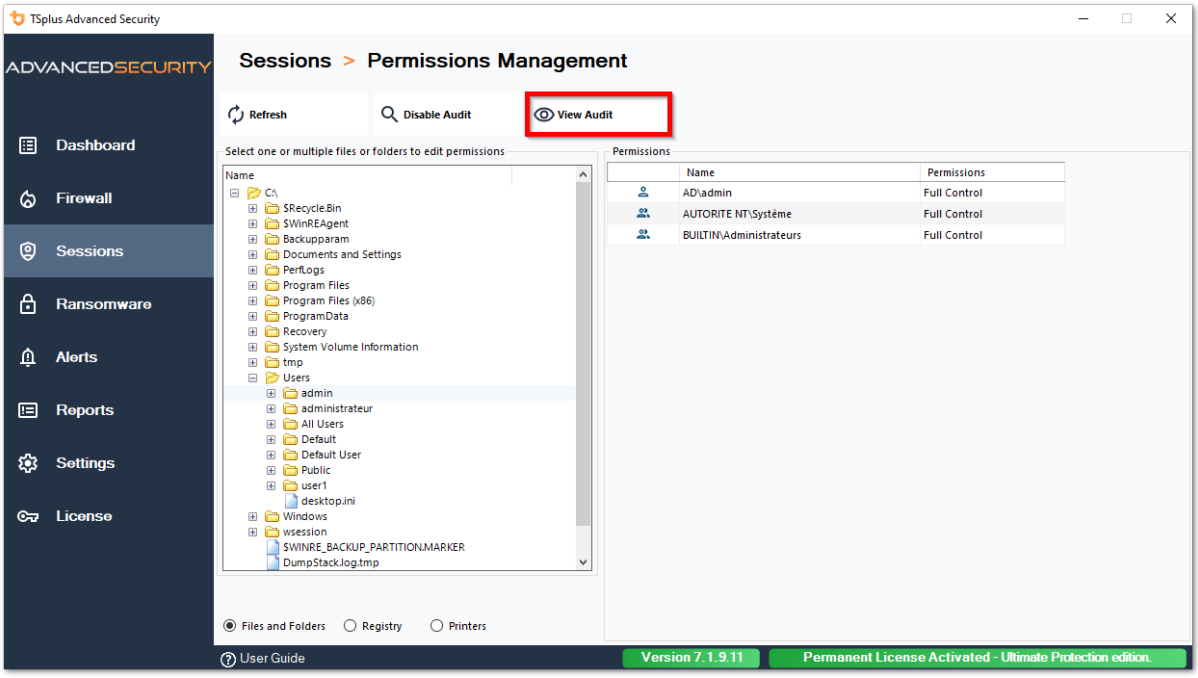


You can refresh the status of the folders for them to be updated in real-time.

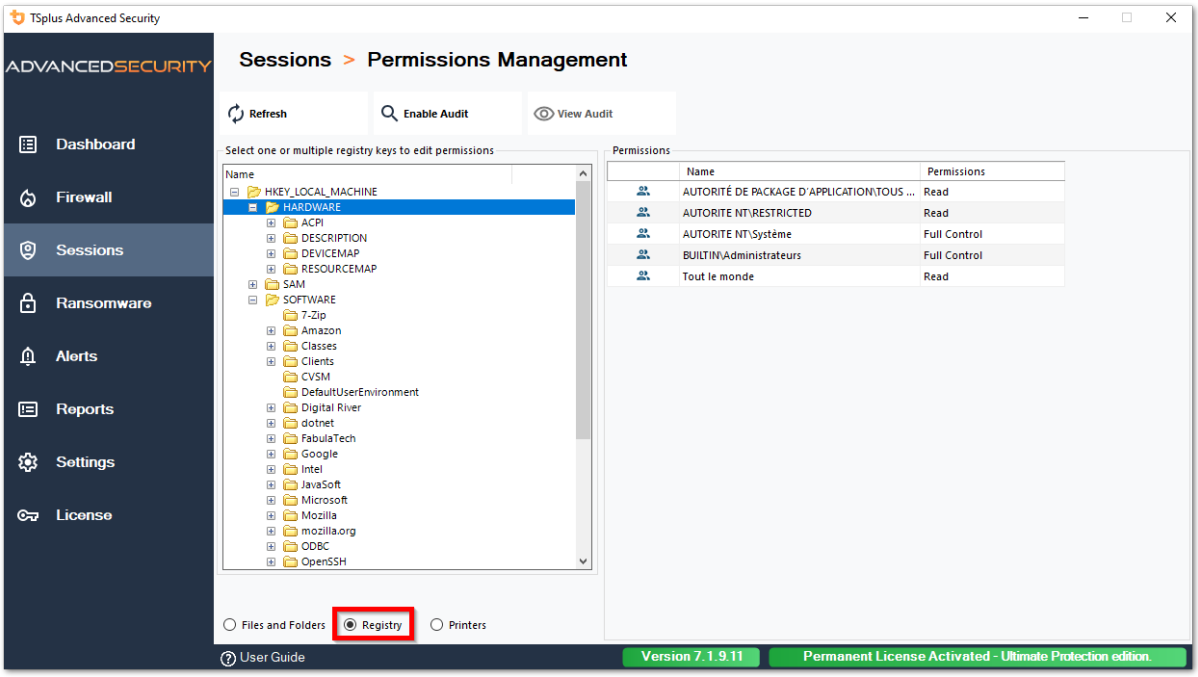
An Audit can be enabled by selecting the desired folder, subfolder or file and click on the “Enable Audit” button at the top:

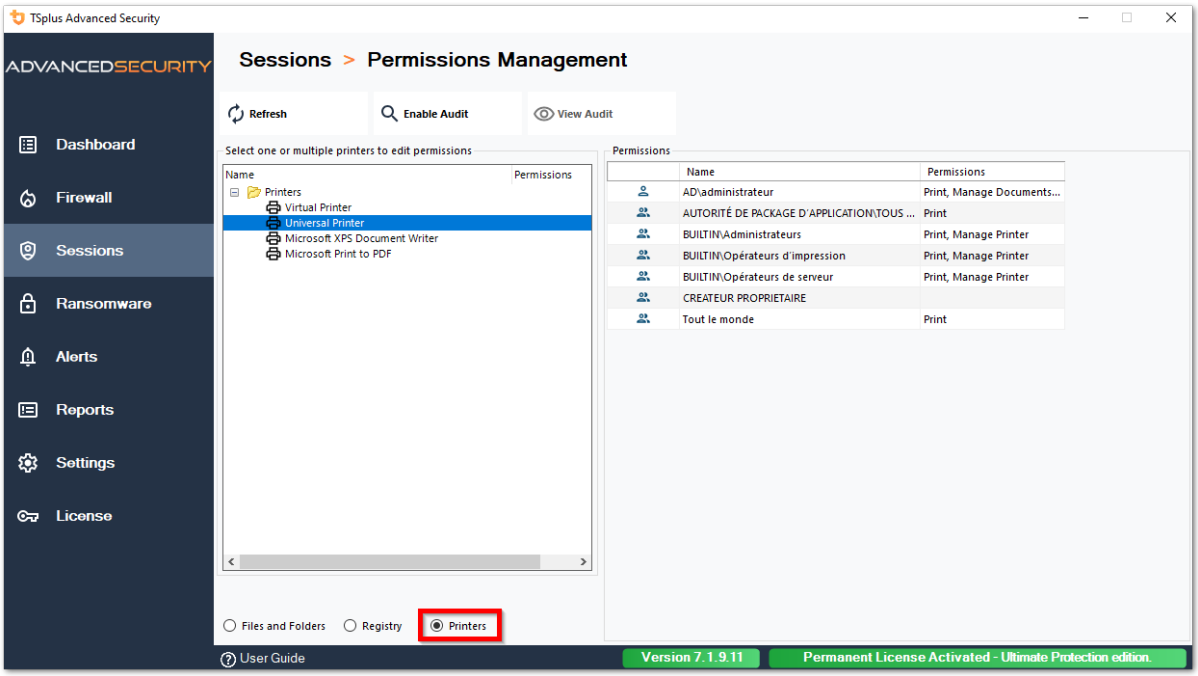



The “View Audit” button allows you to see the corresponding audit on the Event Viewer:




Same Inspections possibilities are available for each registry and printer by selecting the corresponding button under the left-tree view :


TSplus Advanced Security
ADVANCEDSECURITY
Sessions > Permissions Management
Refresh
Enable Audit
View Audit
Dashboard
Firewall
Sessions
Ransomware
Alerts
Reports
Settings
License
Select one or multiple registry keys to edit permissions
Name
HKEY_LOCAL_MACHINE
HARDWARE
ACPI
DESCRIPTION
DEVICEMAP
RESOURCEMAP
SAM
SOFTWARE
7-Zip
Amazon
Classes
Clients
CVSM
DefaultUserEnvironment
Digital River
dotnet
FabulaTech
Google
Intel
JavaSoft
Microsoft
Mozilla
mozilla.org
ODBC
OpenSSH
Permissions
Name
Permissions
AUTORITÉ DE PACKAGE D'APPLICATION\TOUS ...
Read
AUTORITE NT\RESTRICTED
Read
AUTORITE NT\Système
Full Control
BUILTIN\Administrateurs
Full Control
Tout le monde
Read
Files and Folders
Registry
Printers
User Guide
Version 7.1.9.11
Permanent License Activated - Ultimate Protection edition.


TSplus Advanced Security
ADVANCEDSECURITY
Sessions > Permissions Management
Refresh
Enable Audit
View Audit
Dashboard
Firewall
Sessions
Ransomware
Alerts
Reports
Settings
License
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 - Prerequisites

## Hardware Requirements

TSplus Advanced Security supports 32-bit and 64-bit architectures.

## Operating System

**Your hardware must use one of the operating systems below:**

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

**Both 32 and 64 bits architectures are supported.**

## Software Requirements

TSplus Advanced Security requires the following prerequisites:

- Runtime: .NET Framework 4.7.2 or higher

- Microsoft Windows 7 SP1 and Windows 2008 R2 SP1 require an additonal update to support SHA2 Cross Signing (KB4474419). This update allows TSplus Advanced Security built-in firewall and ransomware protection to run properly.

**Note:** These prerequisites will be automatically installed by the setup program if they are missing on the system.

# TSplus Advanced Security - Getting Started

## Prerequisites

TSplus Advanced Security requires the following prerequisites.

- Operating system: Microsoft Windows version 7, Service Pack 1 (build 6.1.7601) or Windows 2008 R2, Service Pack 1 (build 6.1.7601) or higher.

The following **prerequisites will be automatically installed by the setup program** if missing:

- Runtime: .NET Framework 4.5.3 or higher

- Microsoft Windows 7 SP1 and Windows 2008 R2 SP1 require an additional update to support SHA2 Cross Signing (KB4474419). This update allows TSplus Advanced Security built-in firewall and ransomware protection to run properly.

Please refer to the documentation for more details about prerequisites.

## Step 1: Installation

The latest TSplus Advanced Security setup program is always available here: Latest TSplus Advanced Security setup program. Please download the setup program and follow the setup assitant wizard.

TSplus Advanced Security setup programe does not usually require to reboot your system to complete the installation.

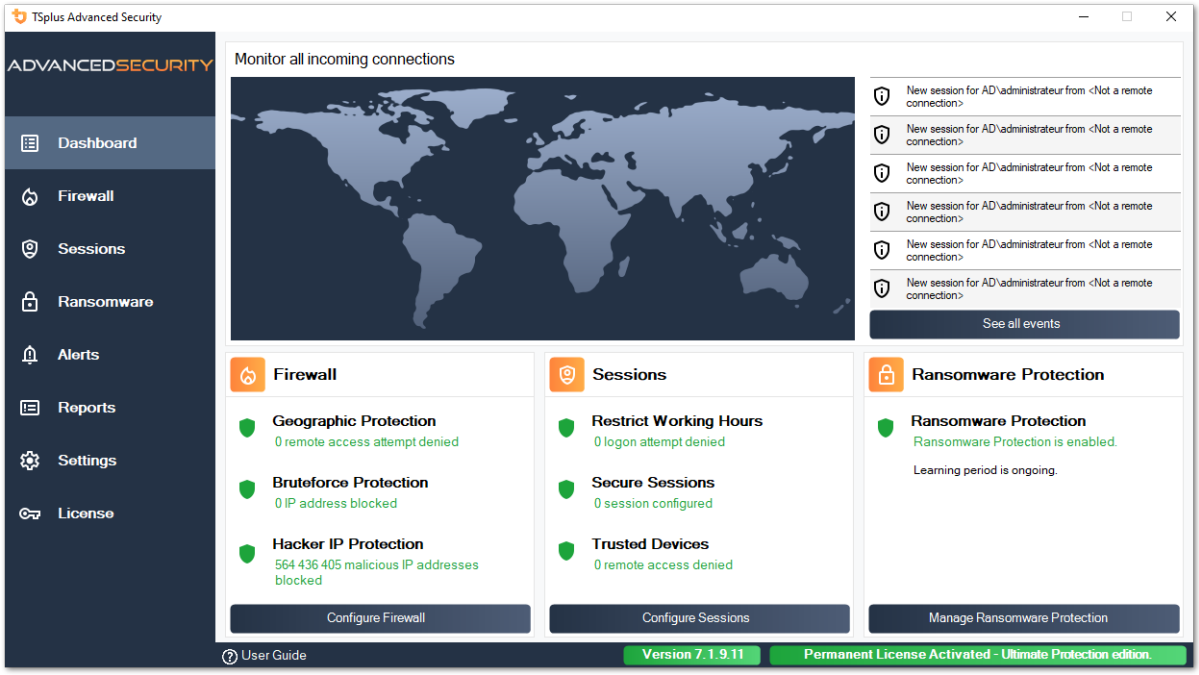
Any new installation starts a fully featured trial period of 15 days. Please do not hesitate to contact us should you face any hurdle or if you face any issue will configuring TSplus Advanced Security.

Once the installation has completed, a new icon is displayed on your Desktop. Double-click on this icon to open TSplus Advanced Security and start configuring the security features.

Please refer to the documentation for full installation instructions.

# Step 2: Configuring TSplus Advanced Security

You have launch TSplus Advanced Security and begun configuring features to protect your server from malicious activities and enforce strong security policies.




On the left column, the homepage allows a quick access to configure the Ransomware Protection, Bruteforce Protection and Geographic Protection features.

Start Ransomware Protection's learning period to allow Advanced Security to identify legit applications and behaviors on your system by clicking on the following tile:

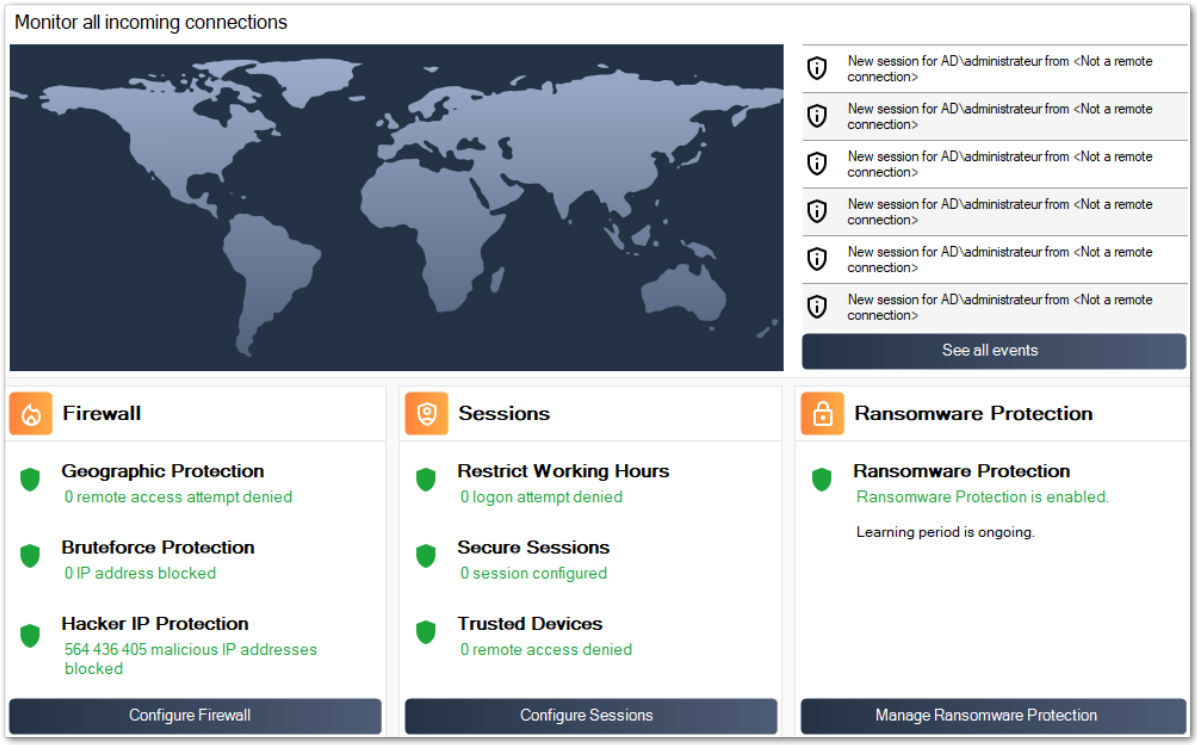
Bruteforce Protection is usually up-and-running following installation. Otherwise, click on the **Repear defense against bruteforce attacks** tile to resolve issues and applys the required system configuration. By default, this feature blocks attaquants following 10 failed login attempts.

Finally, add your country in the list of authorized countries from where clients are allowed to connect. Click on the tile **Authorize connections from another country** and add your country to configure Geographic Protection

You are all set! Don’t forget to activate your license and to update to the latest version to keep Advanced Security protection at its best!

# Step 3: Reviewing prevented threats

Now that you have configured the key advanced security features, avoided threats will be reported in the Dashboard.




Also, the Hacker IP protection keeps the machine protected against known threats by blocking more than 500 000 000 known malicious IP addresses.

All the security events can be displayed by clicking on the **See all events** tile.

## Step 4: Leveraging other security feature to enhance protection

At the bottom, four other security features can be accessed and configure to enhance your machine's protection.

- Adjust and monitor access privileges on your local filesystems, printers and registry keys to ensure every user has access to relevant resources, with the Permissions feature.
- Define period of time where users are authorized to login with the Working Hours feature. Users will be disconnected passed their allowed working hours.
- Customize and secure user sessions with the Secure Desktop feature. Customize, hide, deny access from items of the session interface for local users.
- Validate the name of the remote client when a user connects to your machine with Endpoint Protection. This feature validates client machine names for each remotly connected user.

There is more! Switching to advanced mode grant you access to more capabilities.

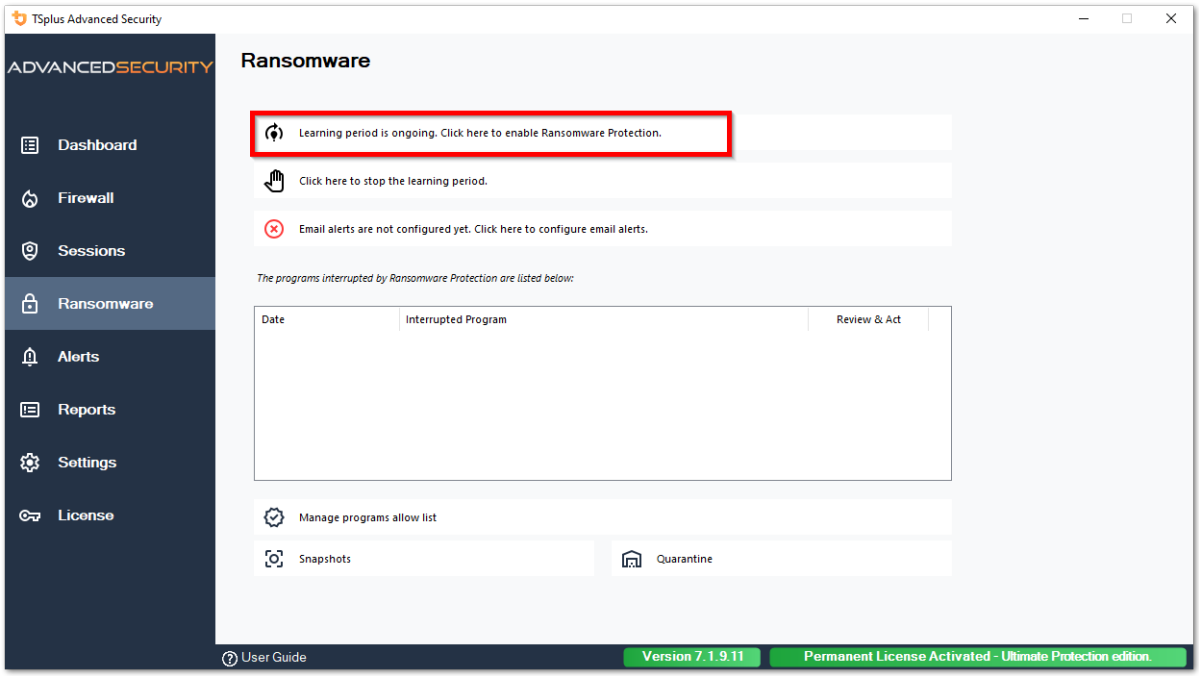
Thank you for using TSplus Advanced Security!

# Ransomware Protection

The Ransomware Protection enables you to efficiently DETECT, BLOCK and PREVENT ransomware attacks. TSplus Advanced Security reacts as soon as it detects ransomware on your session. It possesses both **static and behavioral analysis**:

- The **static analysis** enables the software to react immediately when an extension name changed,
- The **behavorial analysis** looks at how a program will interact with files and detect new strain of ransomware.

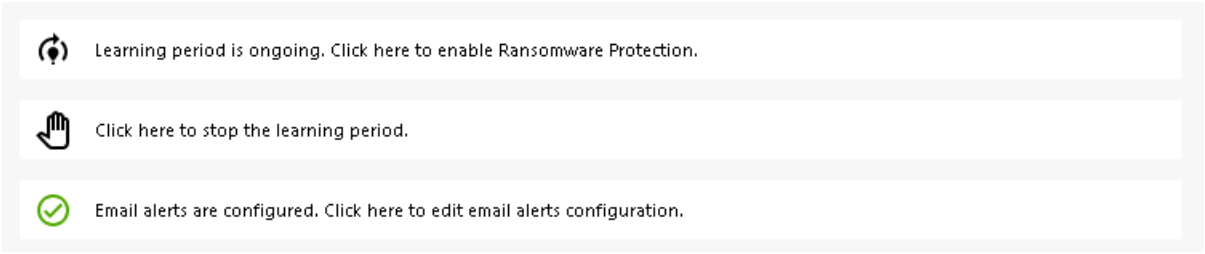
You can enable it by clicking on the “Enable Ransomware Protection” on the Ransomware Protection tab:



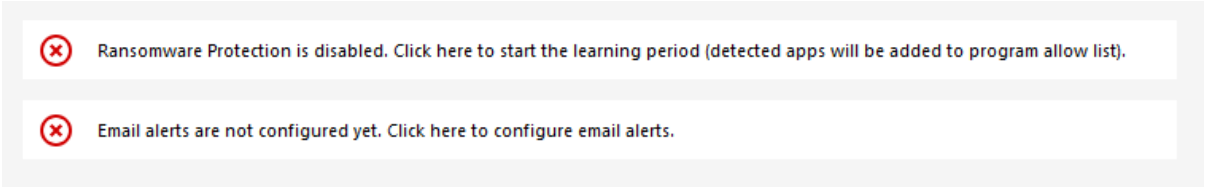

# Learning Period

After enabling the Ransomware Protection feature, the Learning Period is automatically activated. During the Learning Period, all programs detected by the Ransomware Protection feature will be considered as false positive and will be able to resume their execution. The programs detected as false positive will be automatically added to the list of allowed programs.

This feature allows to configure Ransomware Protection on a production server without disrupting its activity. We recommend to start with a 5 days Learning Period to identify all legit business applications.



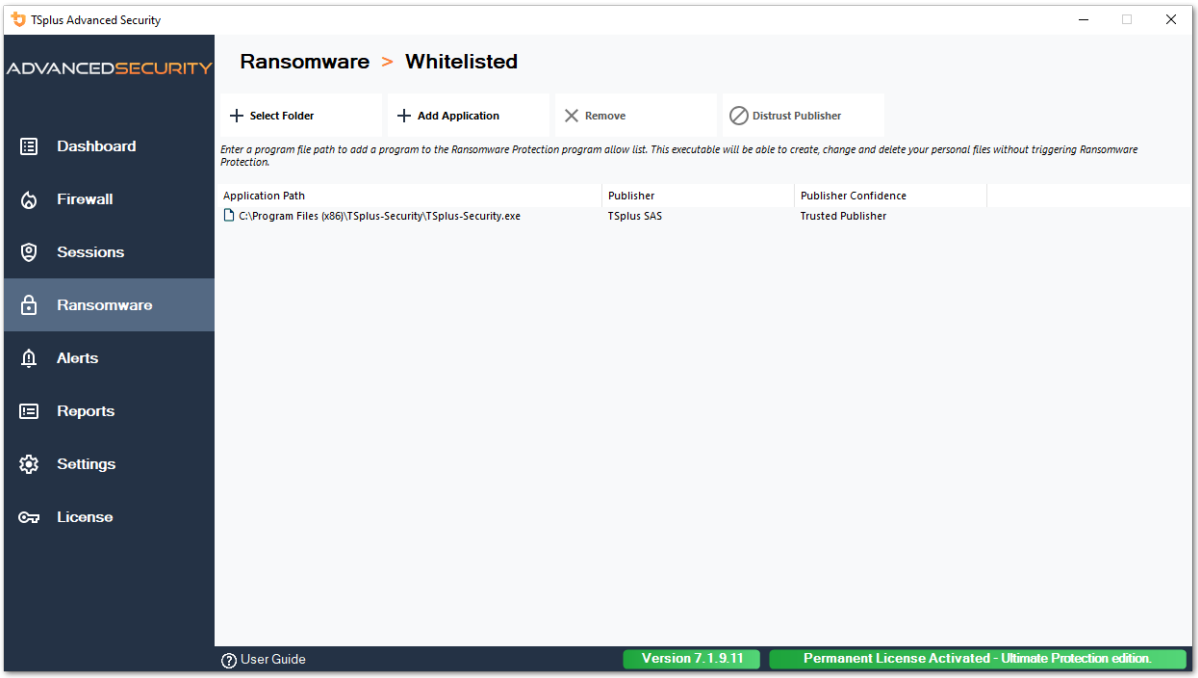

If you stop the Learning Period, it will deactivate the Ransomware Protection. Click on the “Ransomware Protection is disabled” button to reactivate the Learning Period.




# Ransomware Protection Action

It quickly scans your disk(s) and displays the file(s) or program(s) responsible, in addition to providing a list of the infected items. TSplus Advanced Security automatically stops the attack and quarantines the program(s) along with the file(s) encrypted before its intervention.

Only the administrator can whitelist them, by entering the path of the desired program on the bottom line and by clicking on “Add”:



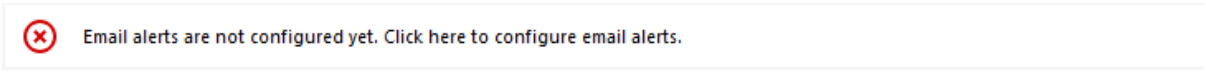
# Ransomware Protection Report

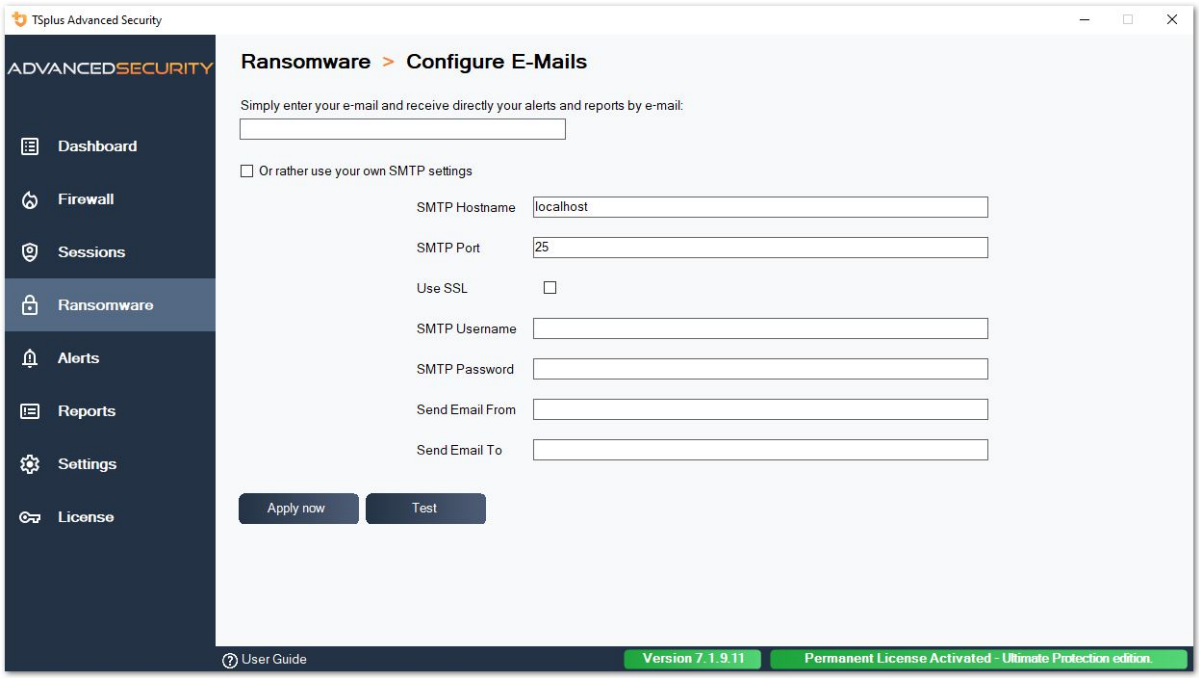
TSplus Advanced Security prevents catastrophic events for businesses by removing ransomware at an early stage.

The administrator has access to information regarding the source of the attack and running processes, and therefore learns how to anticipate these threats.

Note: Ransomware Protection observes how programs interact with system and personal files. To ensure a greater level of protection, Ransomware Protection creates bait files in key folders where ransomware often begins its attack. Therefore, a few hidden files may appear in the users' desktop and documents folders, as well as in other locations. When it detects a malicious behaviour, it stops the ransomware immediately (or ask if the logged user is an administrator). Ransomware Protection uses pure behavioural detection techniques and does not rely on malware signatures, allowing it to catch ransomware which does not exist yet.

You can configure your SMTP settings in order for TSplus Advanced Security to send you email alerts to highlight important security events  by clicking on the button below the Ransomware activation one:



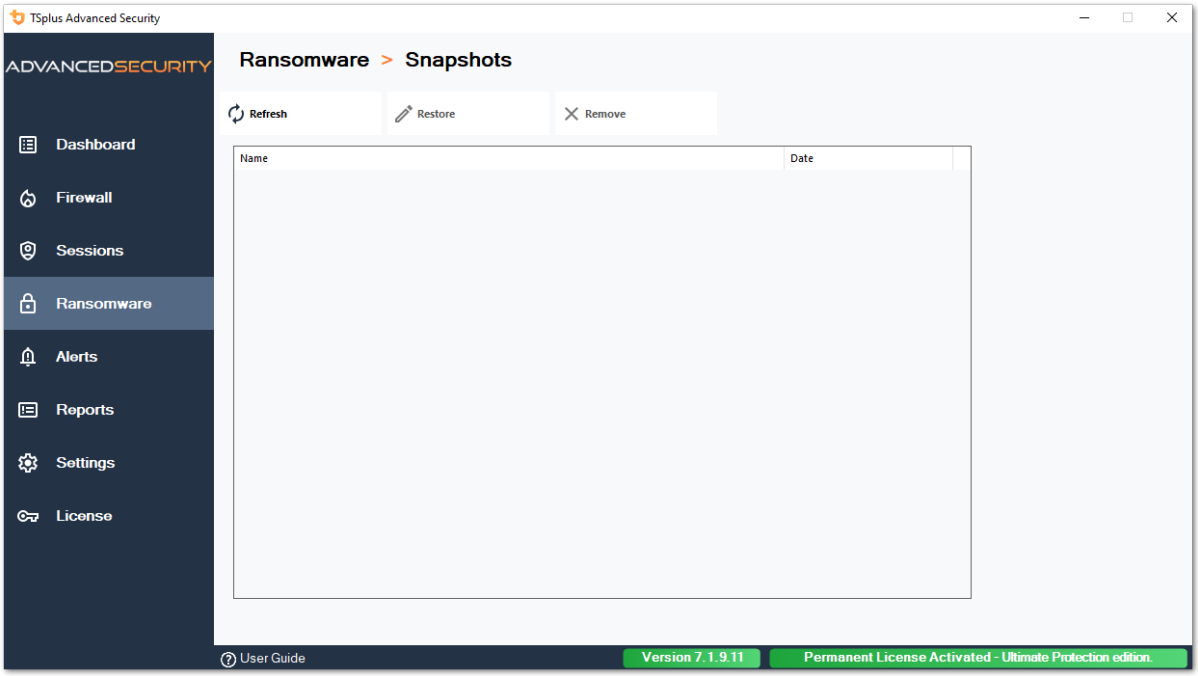

Enter your SMTP Hostname, Port and check the Use SSL box and change change the port from 25 to 465 if you wish to use SSL.

Enter the SMTP Username and Password, as well as the sender and receiver addresses.

Email Settings can be validated by sending a test when saving SMTP settings.

# Snapshots

Snaphshots taken by Ransomware Protection are visible under the Snapshots tab:

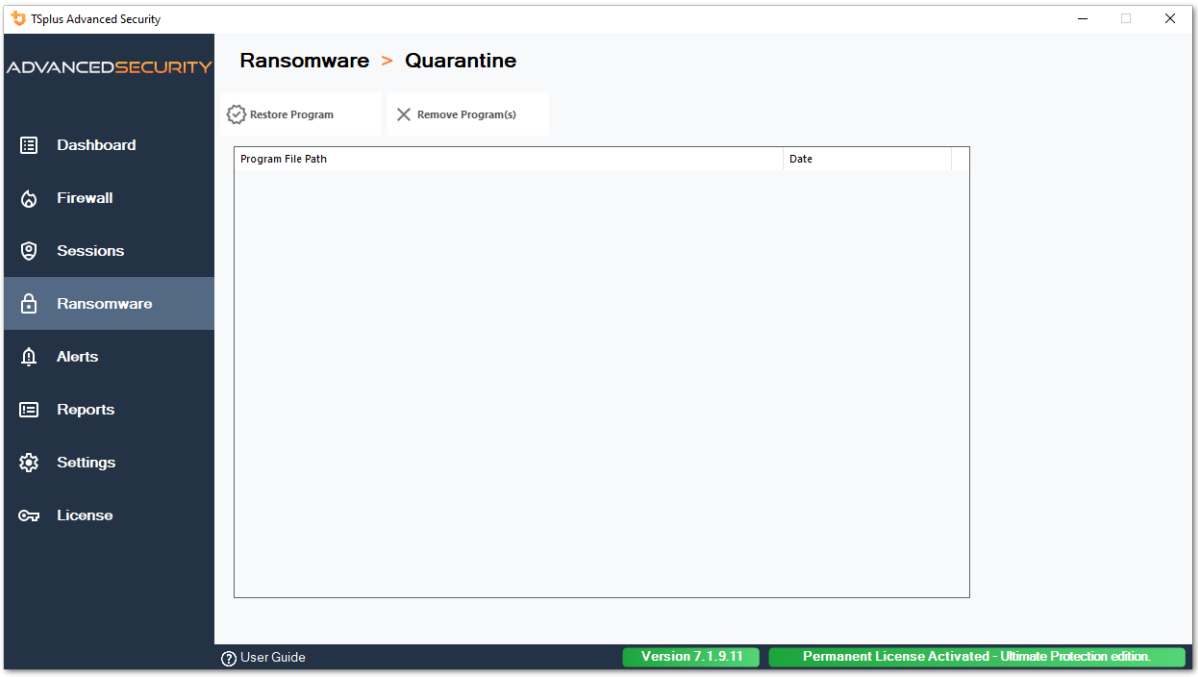



The list can be refreshed by clicking on the corresponding button. Each element can be restored or removed.

# Quarantine

Quarantined programs are visible under the Quarantine tab:
Potentially unwanted programs are kept in quarantine indefinitely until you decide on the action to take.

This way, Advanced Security ensures the safety of your machine while giving you the option to manage quarantined items as you choose.
This can be useful if you need to retrieve a file or program that was neutralized. **This decision is made at your own risk.**
You can also permanently delete any files or programs you choose directly from the quarantine folder located in the Advanced Security installation directory.




Each element can be restored or removed.

Ignored files are not used to detect possible malicious actions and are not saved when they are modified. The idea is to exclude any operation on large or irrelevant files (such as log files).

- sys
- dll
- exe
- tmp
- ~tmp
- temp
- cache
- lnk
- 1
- 2
- 3
- 4
- 5
- LOG1
- LOG2
- customDestinations-ms
- log
- 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
- appicon
- appinfo
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- drk
- mem
- nvram
- hdd
- pk3
- pf
- trn
- automaticDestinations-ms

# Caution about Backup Files Extension

The file extension used for saving modified files is: **snapshot.** The driver prohibits any modification or deletion action on these files other than by the TSplus Advanced Security service. Stopping the service deletes the backed up files. In order to delete these files manually, you must temporarily unload the driver.

# Backup File Configuration

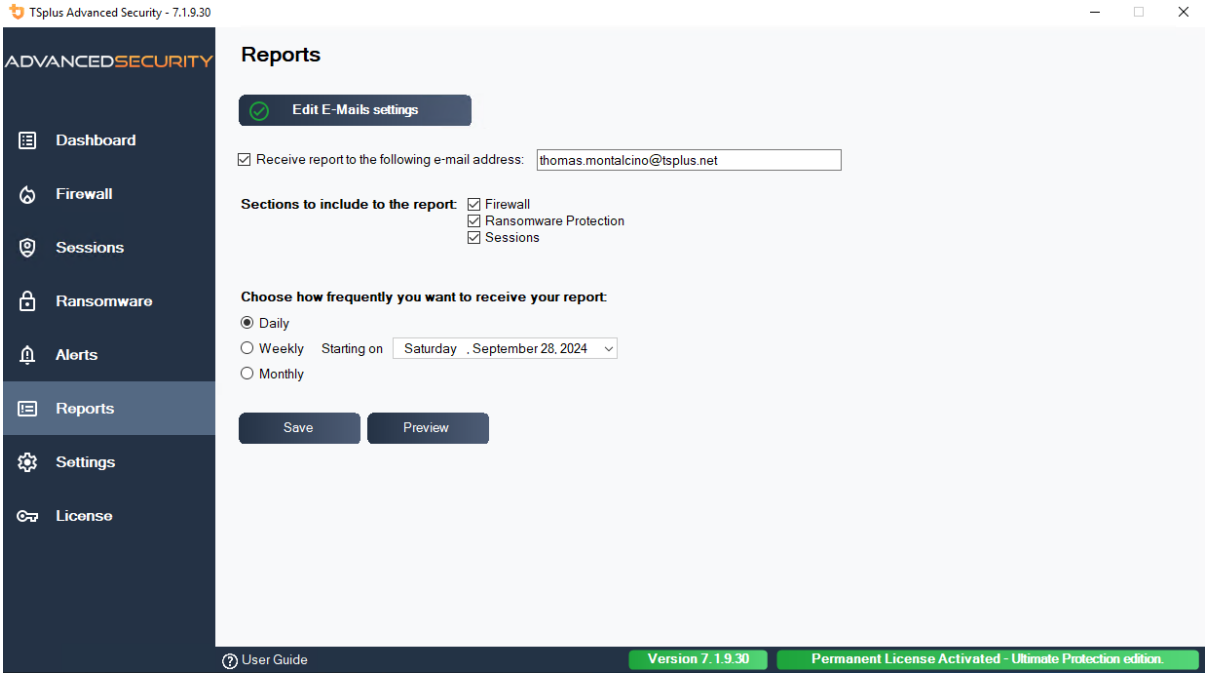
By default, the directory of saved files is located in the installation directory of TSplus Advanced Security and is called “snapshots”. However, it is possible to define another location for this directory. This can allow the administrator to define a directory located on a faster disk (SSD) or on a larger disk according to his needs. The backup directory path must not be a UNC path, in the form of:

\\<computer name>\<backup directory>\

# Adding Backup Utilities to the Whitelist

We recommend adding backup utilities in the Whitelist.

# Reports


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.

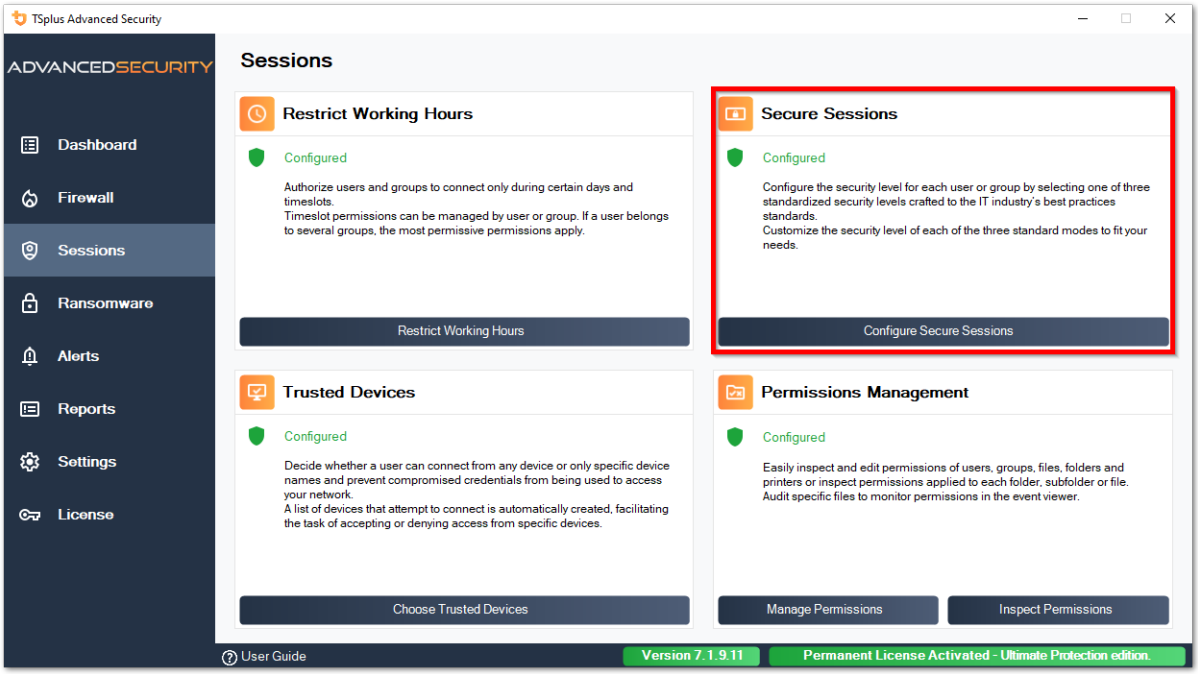
# Secure Sessions

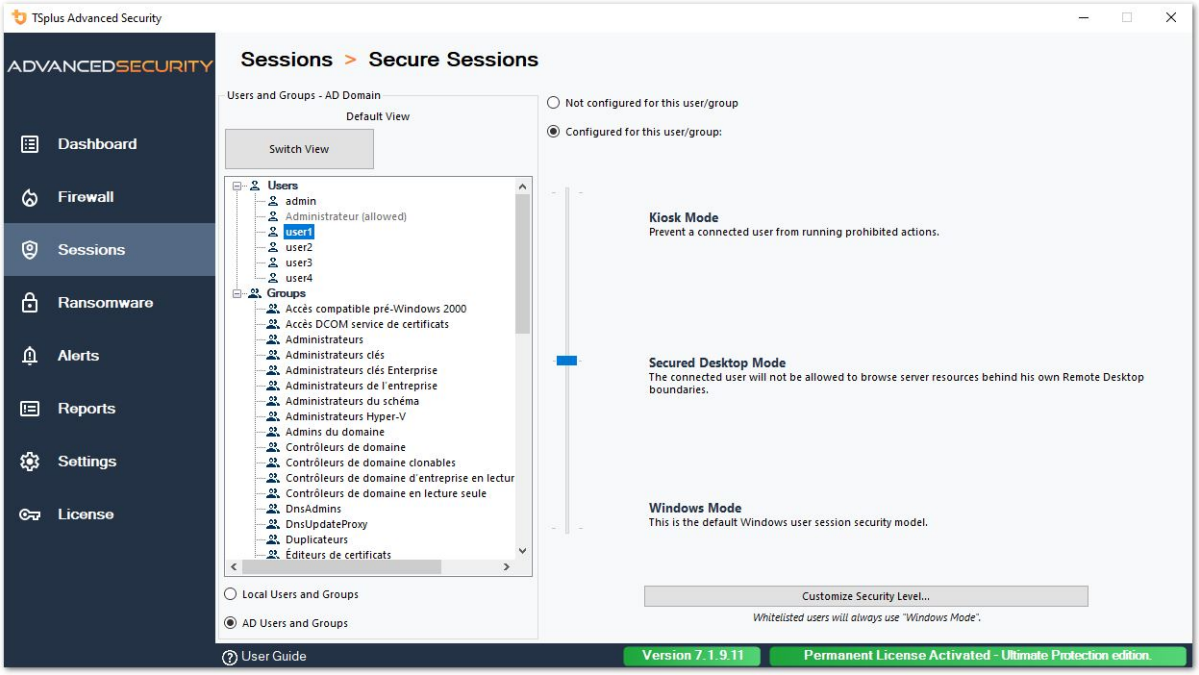
## Warning

- Secure Sessions is very likely to conflict with the security policies defined by Active Directory.
- Secure Sessions's primary purpose is to customize the user interface, not to apply access permissions. Its use should be combined with the Permissions feature to secure access to different drives.

You can configure the security level for each user or group. There are three security levels:

- The **Windows Mode**, where the user has access to a default Windows session.
- The **Secured Sessions Mode**, where the user has no access to the Control Panel, programs, disks, browser, no right-click…: no access to the server resources. He just has access to documents, printers, Windows key and can disconnect his session.
- The **Kiosk Mode** is the most secure one, where the user has very limited actions in his session.

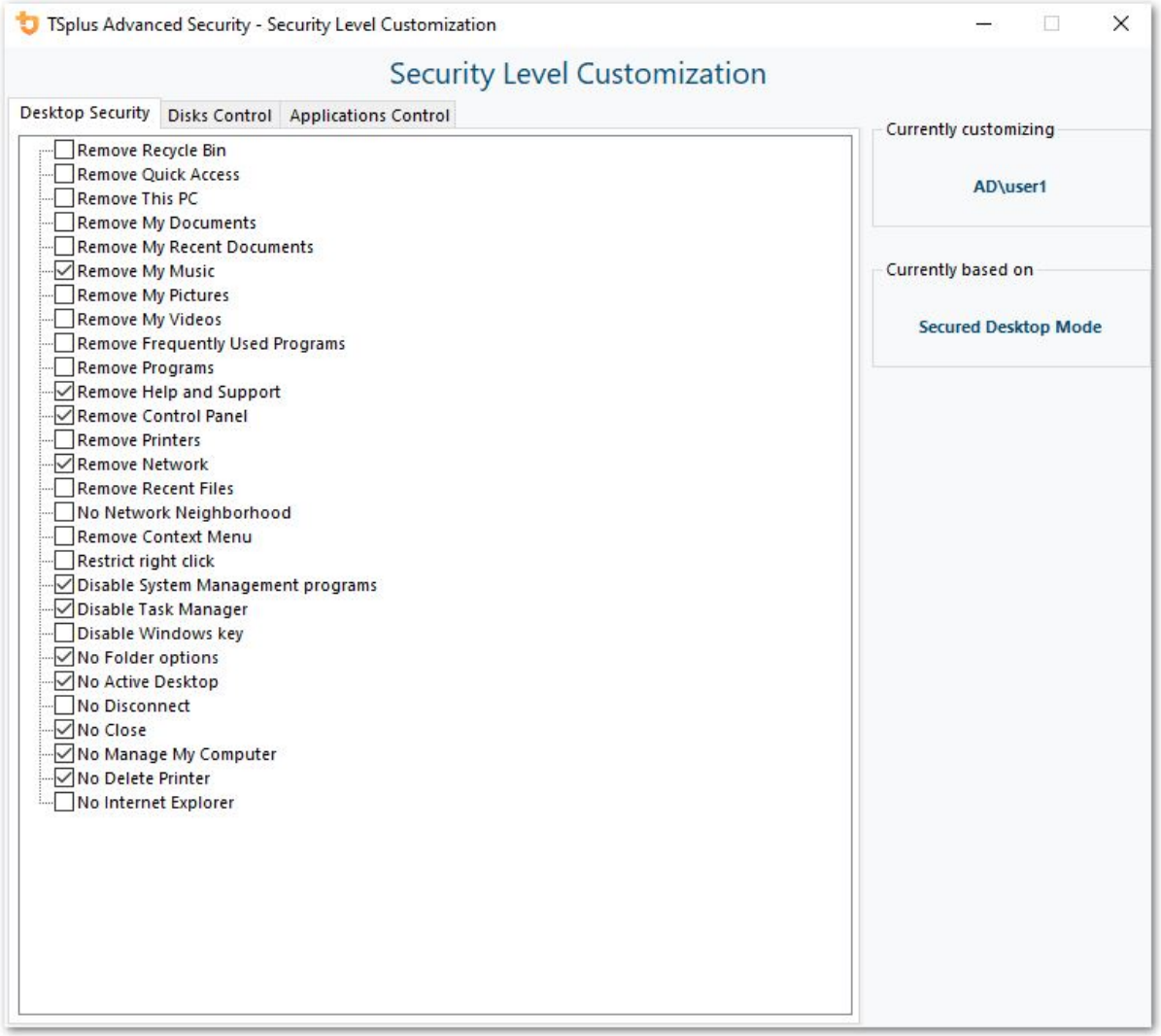




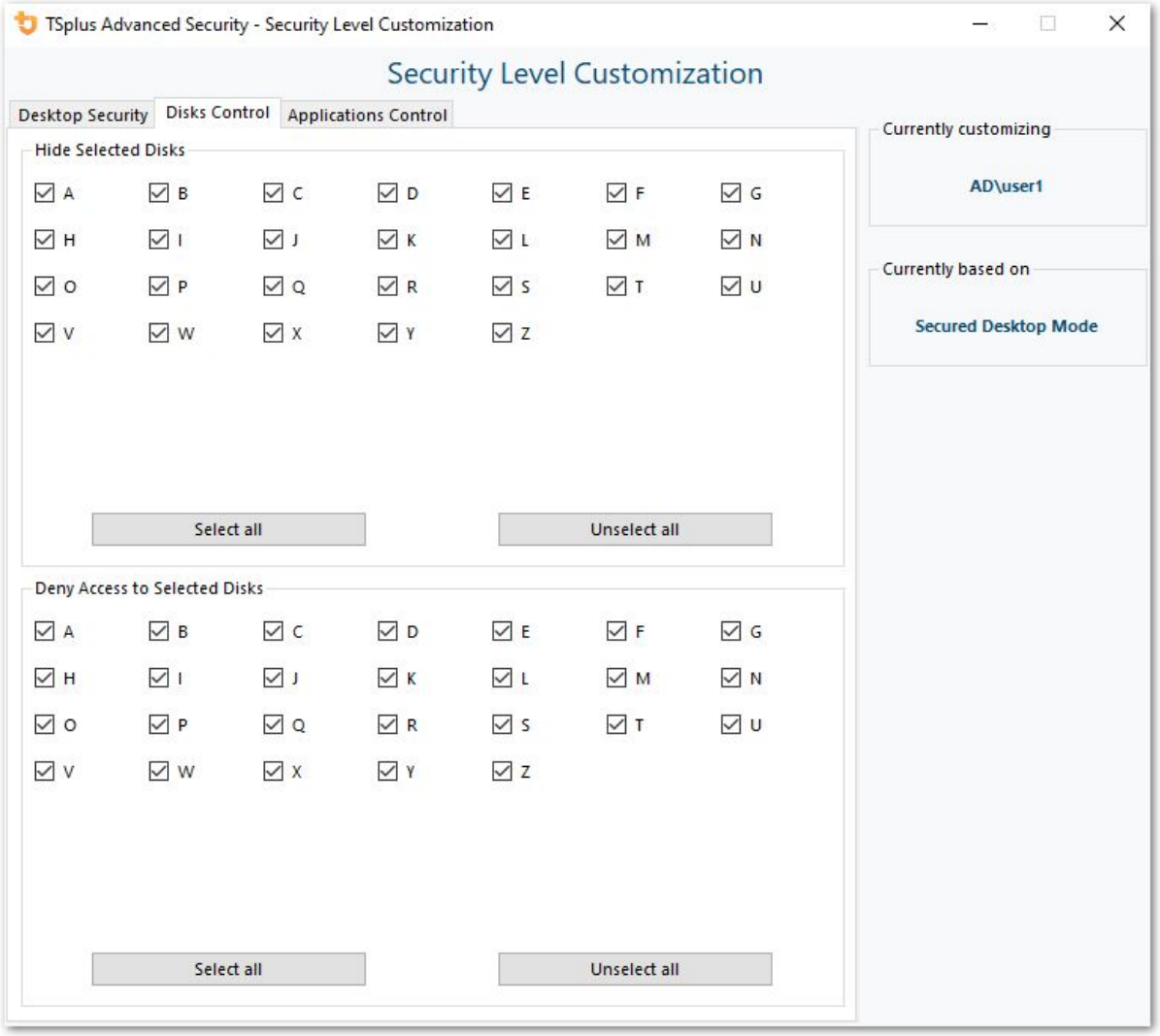

# Customization

In any mode, you have the possibility to customize the security on three levels:

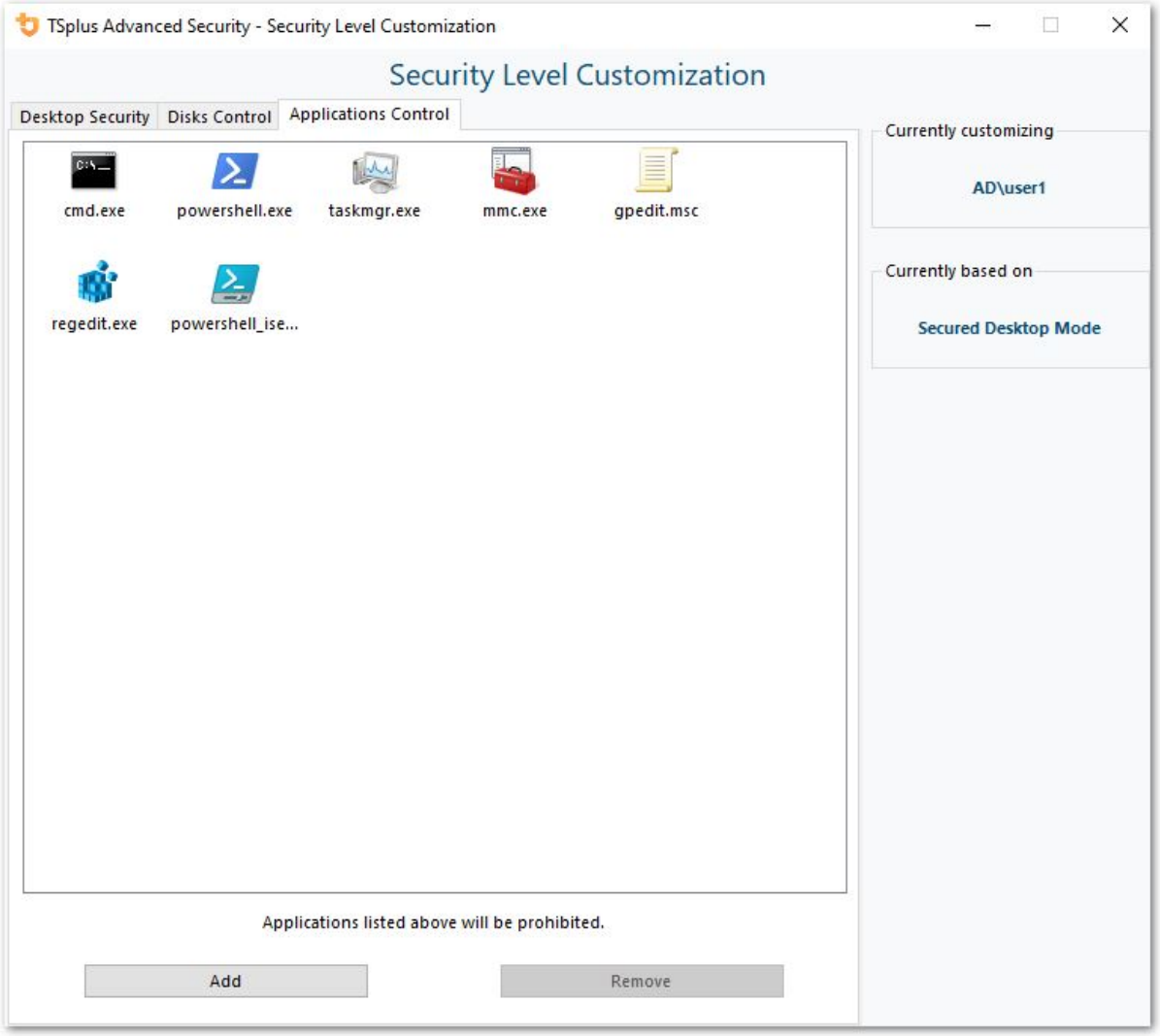
**Desktop Security:**




## Disks Control:




## Applications Control:




# Users/Groups rules priorities

When a user opens a new session on the server:

1. If this user has a Security Level directly defined for himself, then this Security Level is enforced.
2. If this user does not have a Security Level directly defined for himself, then TSplus Advanced Security will load any existing Security Level settings for all the groups of this user, and keep the more permissive rules.

For instance if a first group has a rule to remove the Recycle Bin icon from the desktop, but this rule is disabled for a second group, then the user will have the Recycle Bin icon on his desktop. The same priority rules will apply on every custom rule (Desktop Security, Disks Control and Applications Control) as well as for the principal Security Level (the Windows Mode being considered more permissive than the Secured Desktop Mode, which is considered more permissive than the Kiosk Mode).

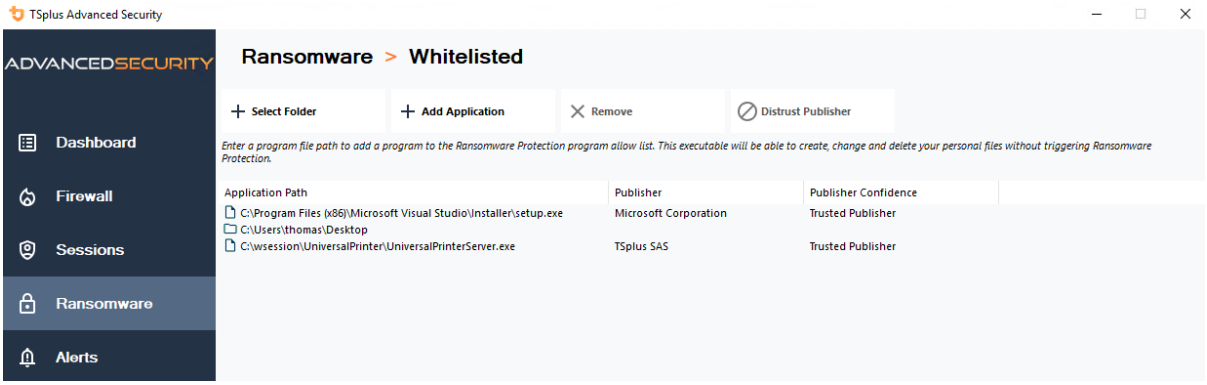
N.B : In order to disable the right click everywhere, you must select the following two options:

- Restrict Right Click

- Remove Context Menu

# Settings - Programs Allow List

On the **Programs tab**, you can add programs to the list of allowed programs, that won't be checked by TSplus Advanced Security's Ransomware Protection. By default, all Microsoft programs are whitelisted.




Click on the "Add Application" button to add a program. You can also remove them by selecting application(s) and clicking on the Remove Application(s) button.

# Settings - Users Allow List

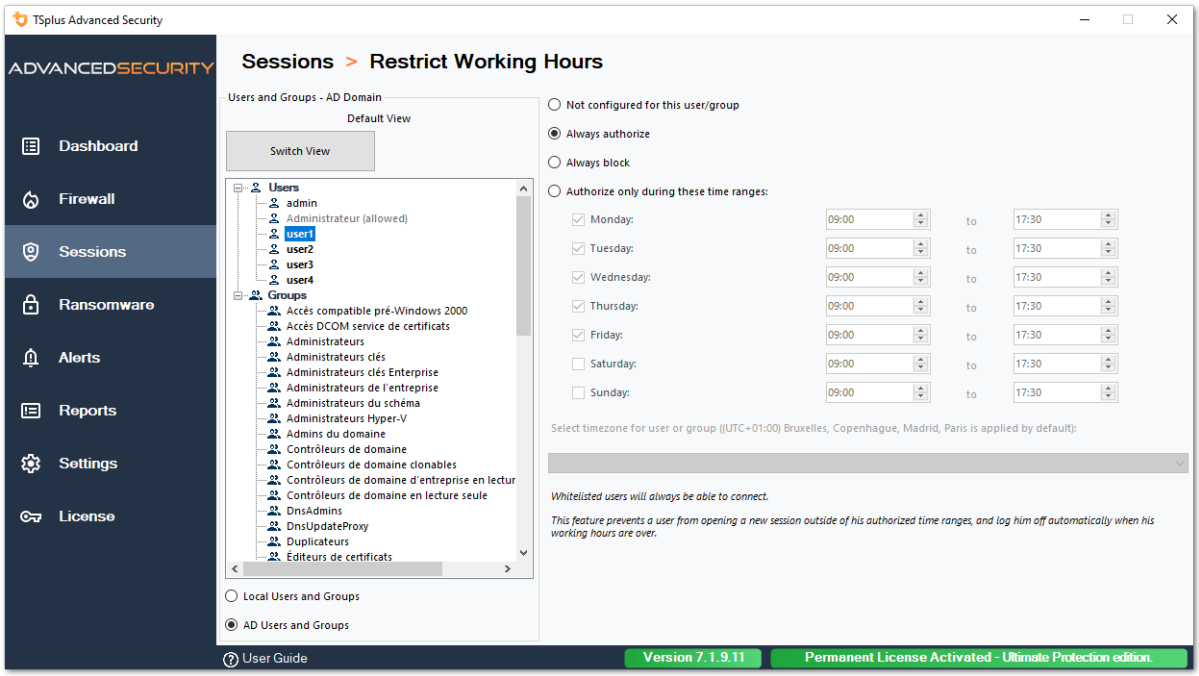
## Advanced View

With the Advanced view, add and manage users and groups from every accessible domains.

You can switch view from the Default view to the Advanced View using the “Switch View” button.

The Advanced view is used to display and manage every current configured user and groups. It also allows you to add new user and group to the list to configure them as well, using the windows AD search picker. You can do so by clicking on the “Add user/group” button.You will then be able to add any user available from any accessible domains from your server.

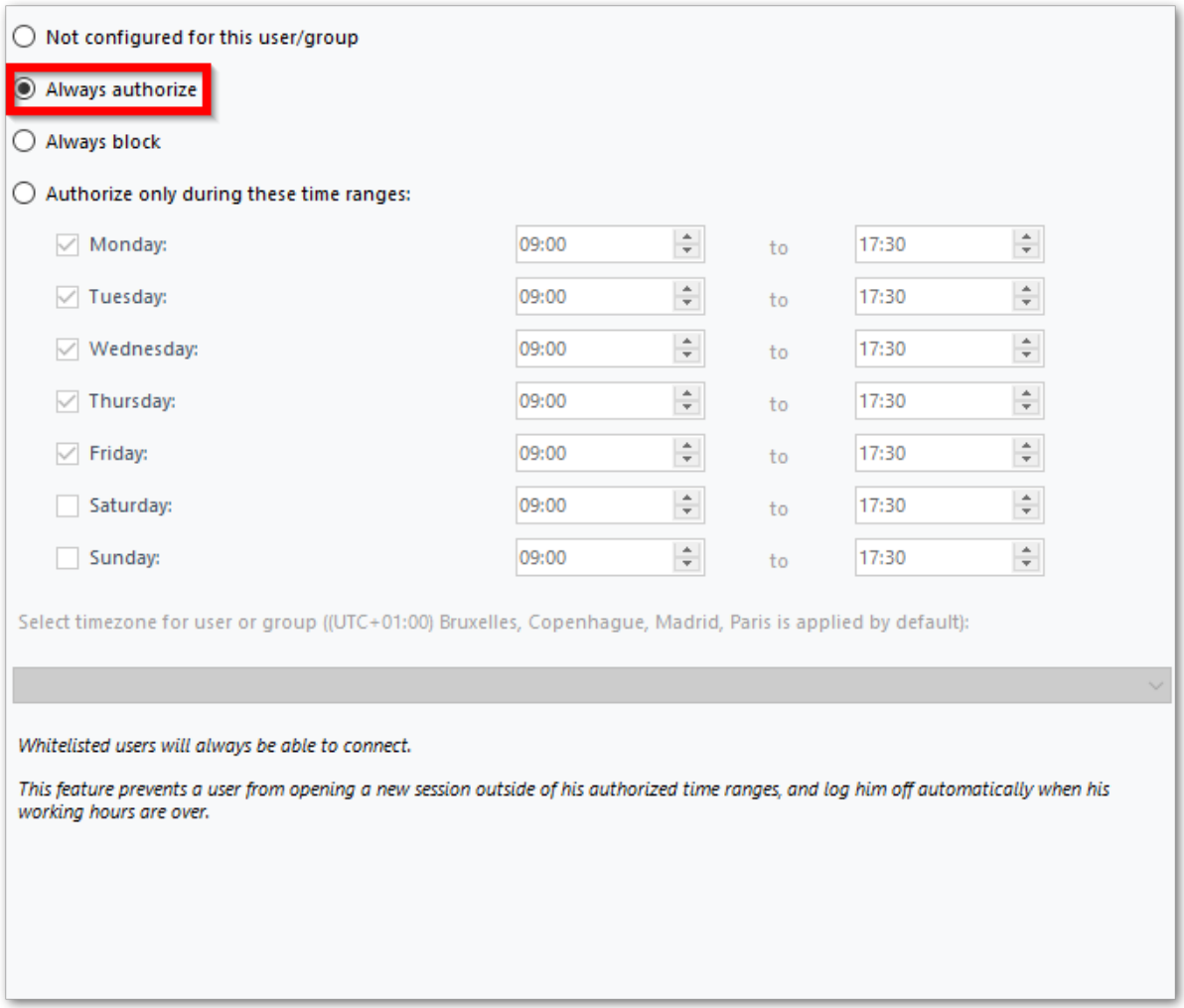
The Advanced View is available on the Permissions, Working Hours, Secure Desktops features. Example:




The **Users Whitelist** tab gives the Administrator the possibility to add/remove users from the whitelist.

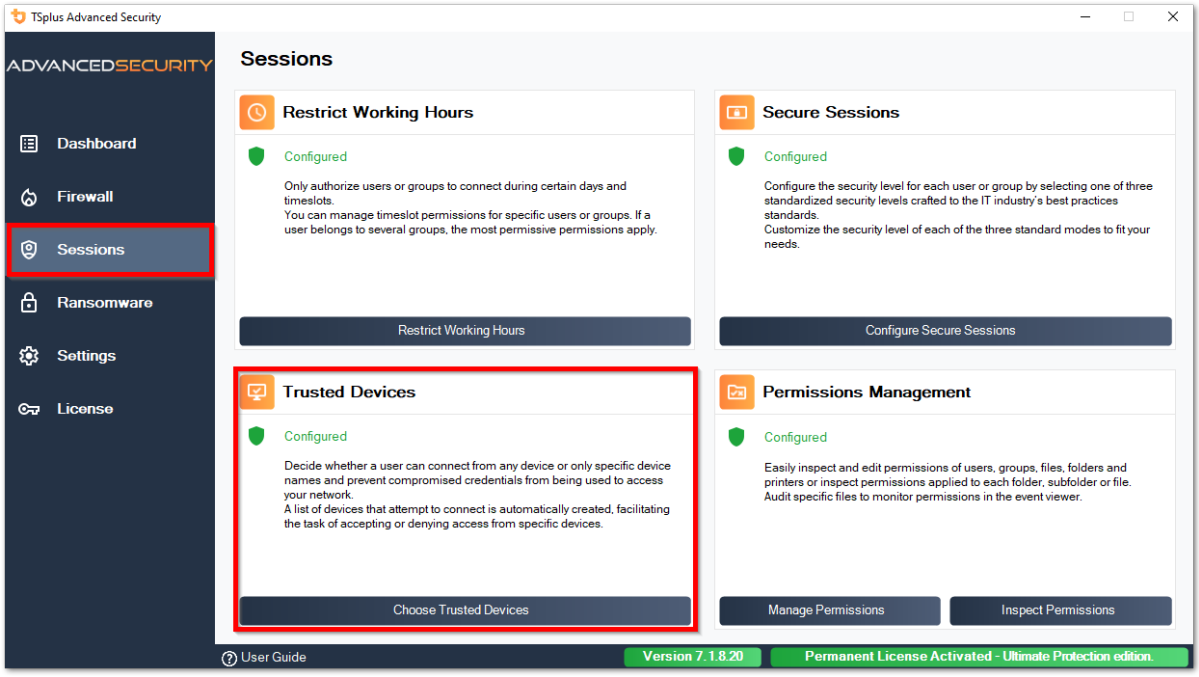
Users on the whitelist are ignored by TSplus Advanced Security and their settings will not be applied.

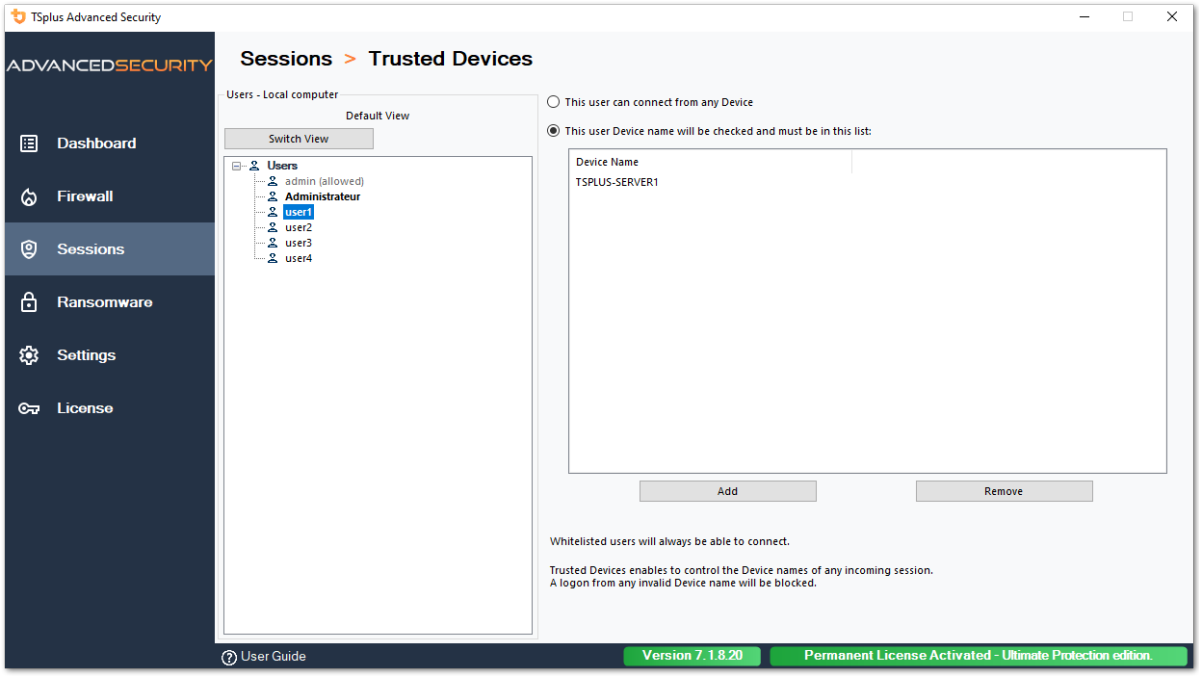
The user who installed TSplus Advanced Security is automatically added to the Whitelist:



# Trusted Devices

Trusted Devices allows you to control users device by allowing each user to use only one or multiple specific device(s), which will be checked on any incoming session. A logon from any invalid device name will be blocked.



On this example, **User1** will be using the device name **TSPLUS-SERVER1** only.

# Auto-fill of device name field

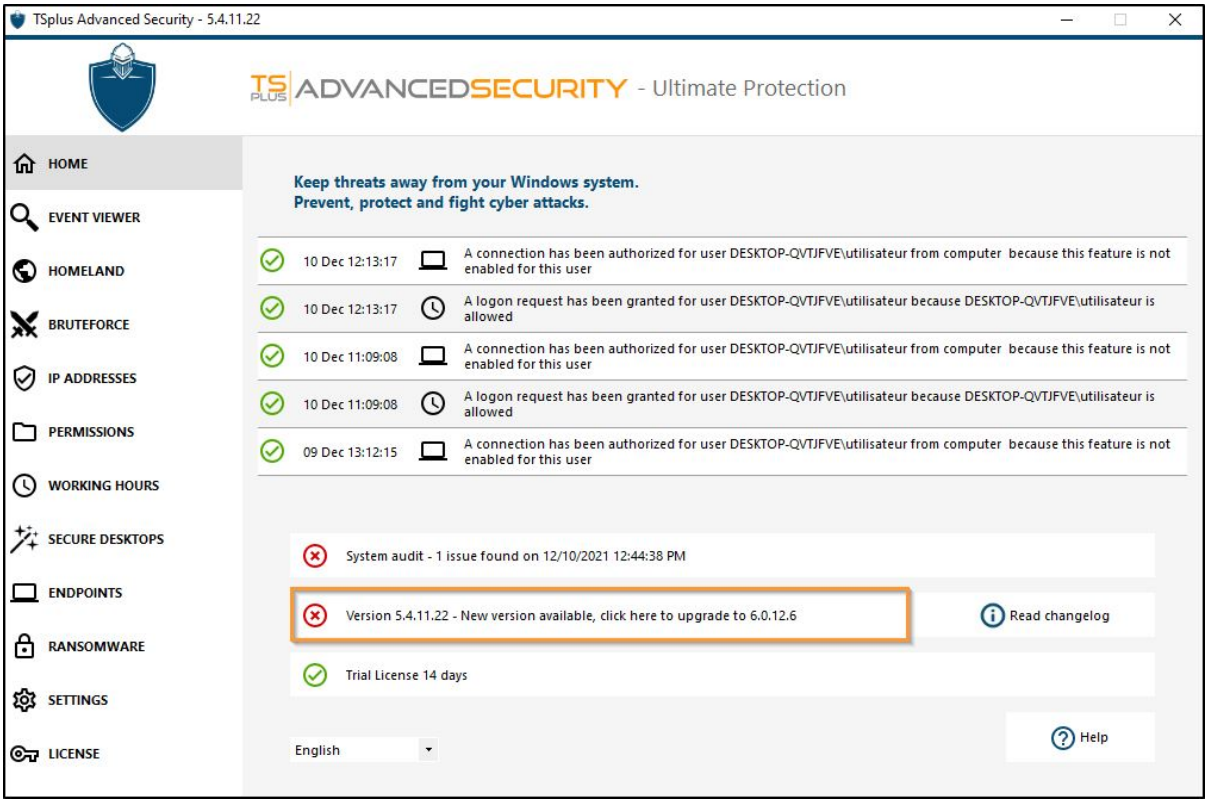
You might notice that the Device Name field is already filled with a device name for some users. In order to help the administrator, TSplus Advanced Security will automatically save the name of the latest device used to connect to the server by any user who does not have Trusted Devices feature enabled. After one working day, the device name of most users will be known by advanced-security, thus allowing you to quickly enable the Endpoint Protection feature without having to check every user's workstation name.

Note: Trusted Devices is not compatible with HTML5 connections.

# Updating TSplus Advanced Security

Check out our fixes and improvements by clicking on Changelog

Updating TSplus Advanced Security is easy and can be done by clicking on the corresponding tile, from the Homepage:




Then, TSplus Advanced Security downloads and applies the update.

**Note:** your data and settings are always backup before an update and can be found in the “archives” directory, in TSplus Advanced Security setup folder. See Backup and restore your data and settings

# Restrict Working Hours

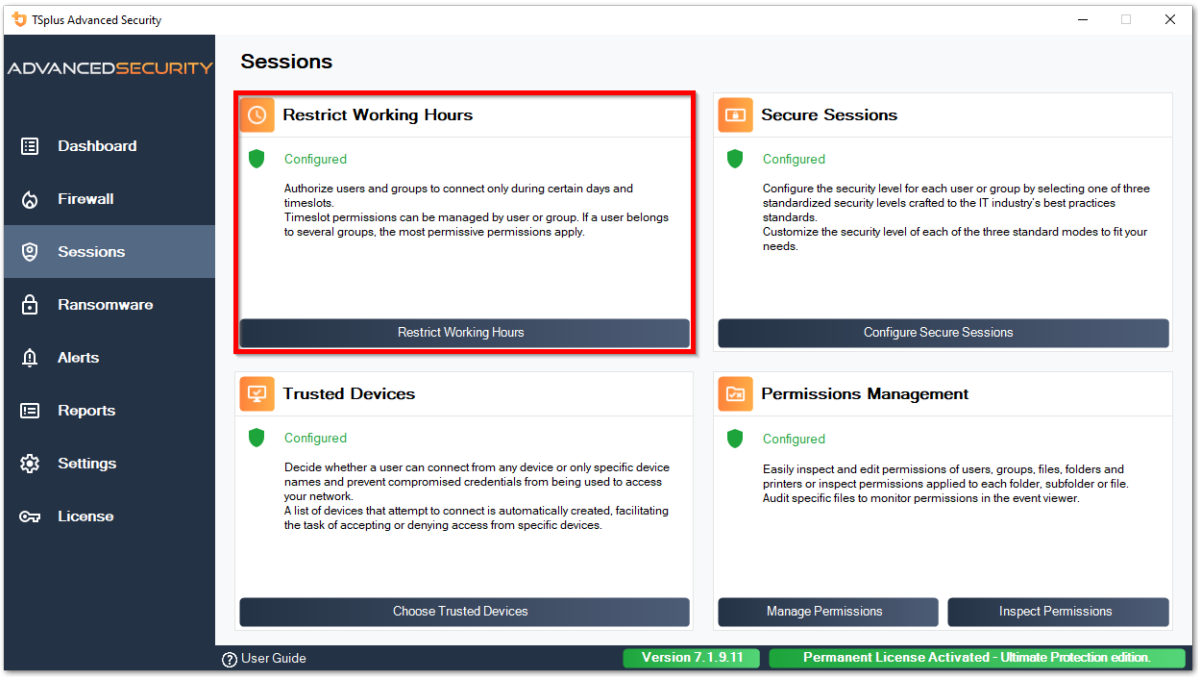
You can configure working hours restrictions per user or per group.

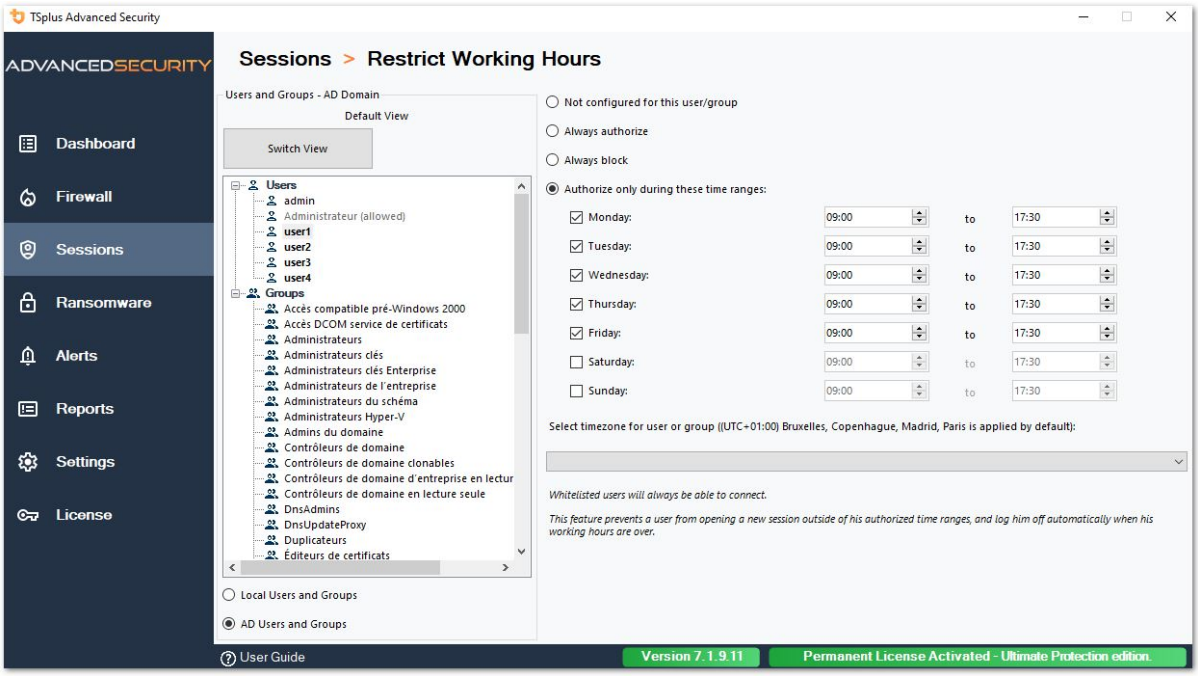
Choose the restriction of your choice:

- Always authorize this user/group access
- Always block this user/group access

or Authorize only during specific time ranges.

You can configure it day by day and select the time range of your preference:






It is possible to select a specific timezone depending on your user's office location.

An automatic disconnection at the end of the configured work time is made.

It is possible to schedule a warning message before the user is logged off from Settings > Advanced > Working Hours.

###Users/Groups rules priorities

When a user opens a new session on the server:

1. if this user has Working Hours restrictions directly defined for himself, then these rules are enforced.

2. if this user does not have Working Hours restrictions directly defined for himself, then TSplus Advanced Security will load any existing Working Hours restrictions for all the groups of this user, and keep the more permissive rules. For instance if a first group has a rule to block the connection on Monday, a second group has a rule to authorize the connection on Monday from 9 AM to 5 PM and a third group has a rule to authorize the connection on Monday from 8AM to 3PM, then the user will be able to open a connection on Monday from 8AM to 5PM.

**Warning: This feature uses server's time. Using the user's workstation time and/or time-zone would be pointless, as all the user would only have to change its time-zone to open a session outside his authorized hours.**