TSplus Advanced Security Documentation

Table of Contents

- Planning and Managing TSplus Advanced Security

- Getting Started
- Pre-requisites
- Installing Advanced Security
- Updating Advanced Security
- Activating your license

Using TSplus Advanced Security

- Home
- System Audit
- Homeland Access Protection
- Bruteforce Defender
- Blocked IP Addresses
- Ransomware Protection
- Permissions
- Working Hours Restriction
- Secure Desktop
- Endpoint Protection
- Hacker IP Protection
- Events

Settings

- Users Allow List
- Programs Allow List
- Advanced > Backup - Restore
- Advanced > Product
- Advanced > Homeland
- Advanced > Bruteforce
- Advanced > Firewall
- Advanced > Working Hours
- Advanced > Endpoints
- Advanced > Ransomware Protection
- Advanced > Logs

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.

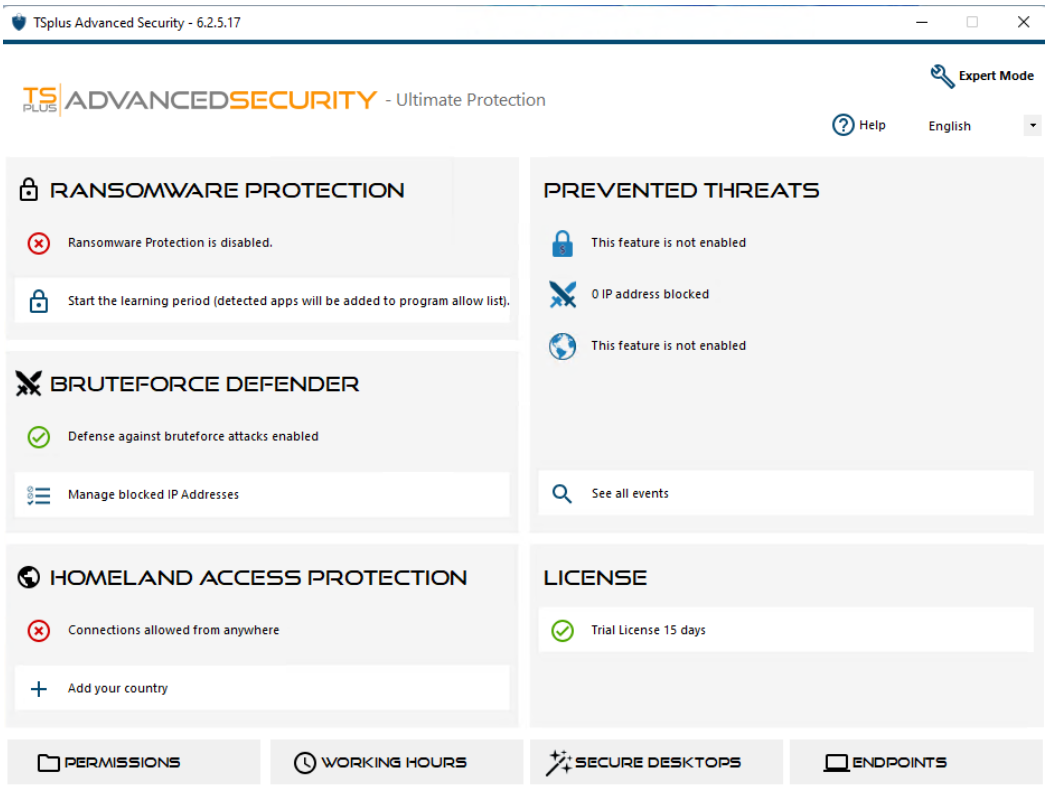
Any new installation starts a fully featured trial period of 15 days. Please do not hesitate to contact us should you face any hurdle or if you face any issue will configuring TSplus Advanced Security.

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.

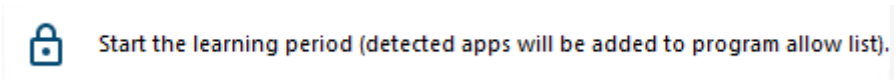
Step 2: Configuring TSplus Advanced Security

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

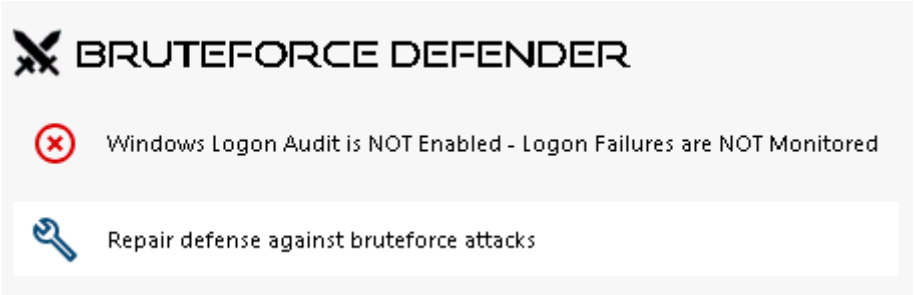


On the left column, the homepage allows a quick access to configure the Ransomware Protection, Bruteforce Defender and Homeland Access Protection features.

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 Defender 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.

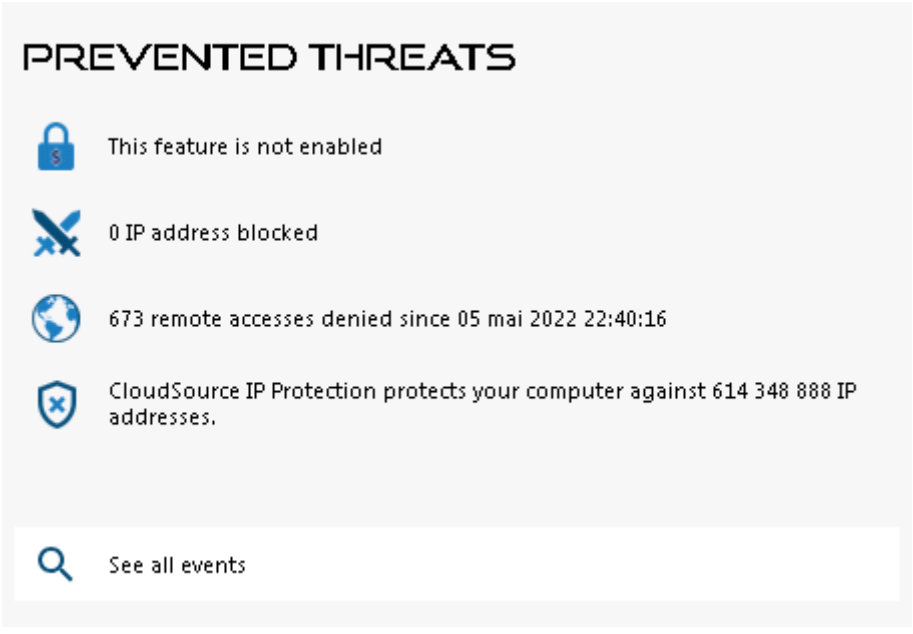


Finally, add your country in the list of authorized countries from where clients are allowed to connect. Click on the tile **Authorize connections from another country** and add your country to configure Homeland Access Protection

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 Advanced Security key features, prevented threats will be reported in the prevented threats section, as show below:



For example, Homeland Access Protection feature has prevented 673 unwanted connexions from unauthorized countries.

Also, the Hacker IP protection keeps the machine protected against known threats by blocking more than 600 000 000 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.

Step 5: Becoming an advanced user

Advanced Security has changed its look since version 6. A **Lite Mode** and an **Expert Mode** have been introduced. **Expert Mode** displays a more detailled interface with access to features and advanced settings.

Administrators can toggle between the two interface styles by clicking the button in the upper-right corner of the application.

Thank you for using TSplus Advanced Security!

TSplus Advanced Security - Prerequisites

Hardware Requirements

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

Operating System

TSplus Advanced Security is compatible with Microsoft Windows version 7, Service Pack 1 (build 6.1.7601) or Windows 2008 R2, Service Pack 1 (build 6.1.7601) or higher.

Software Requirements

TSplus Advanced Security requires the following prerequisites:

- Runtime: .NET Framework 4.5.3 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.

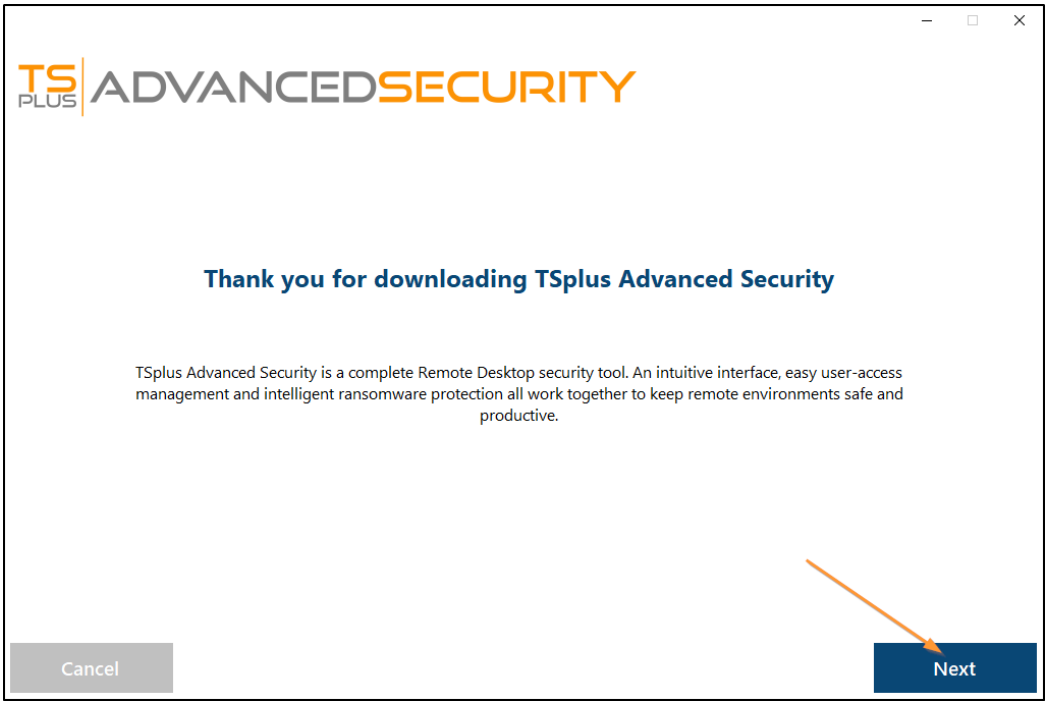
Note: These prerequisites will be automatically installed by the setup program if they are missing on the system.

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.

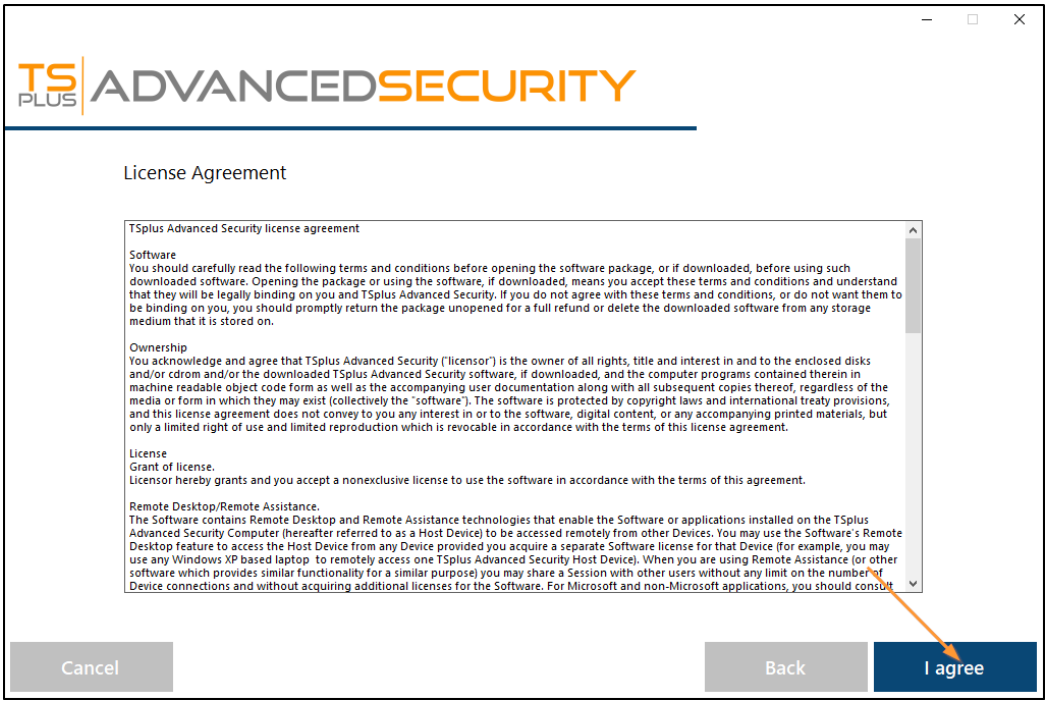


Select the setup assistant language if not detected automatically.

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

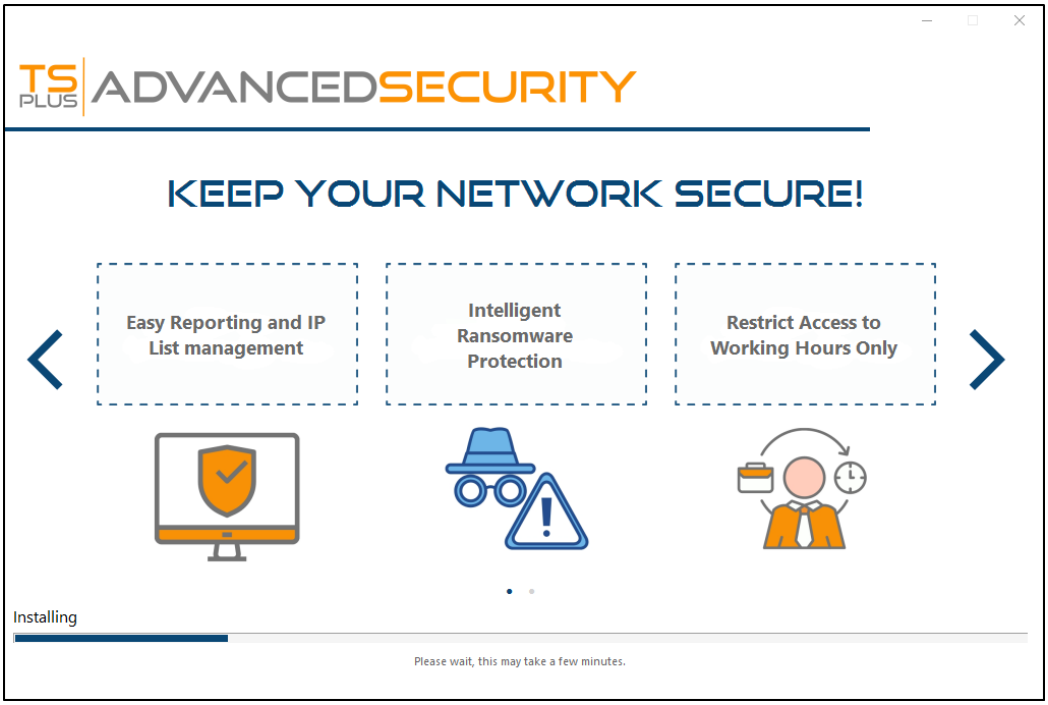
The Advanced option adds aditionnal steps which allows you to: * Only download setup (do not install) * Use custom proxy settings

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!

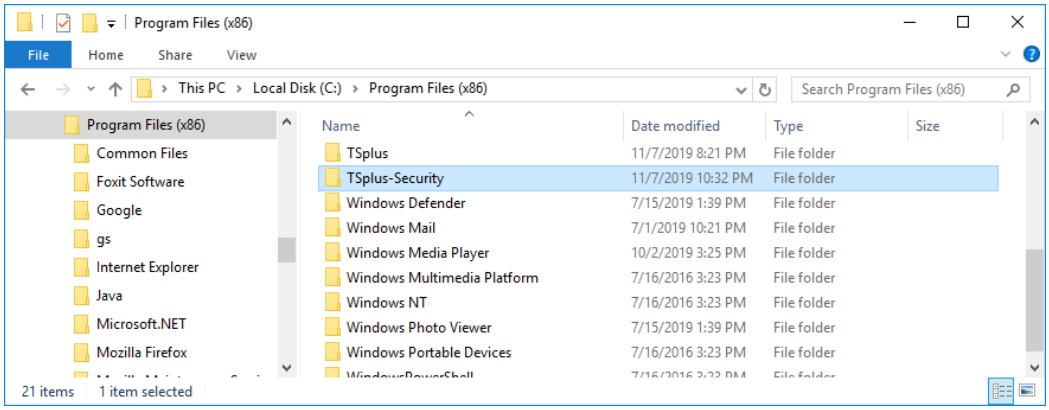
Advanced installation scenarios

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

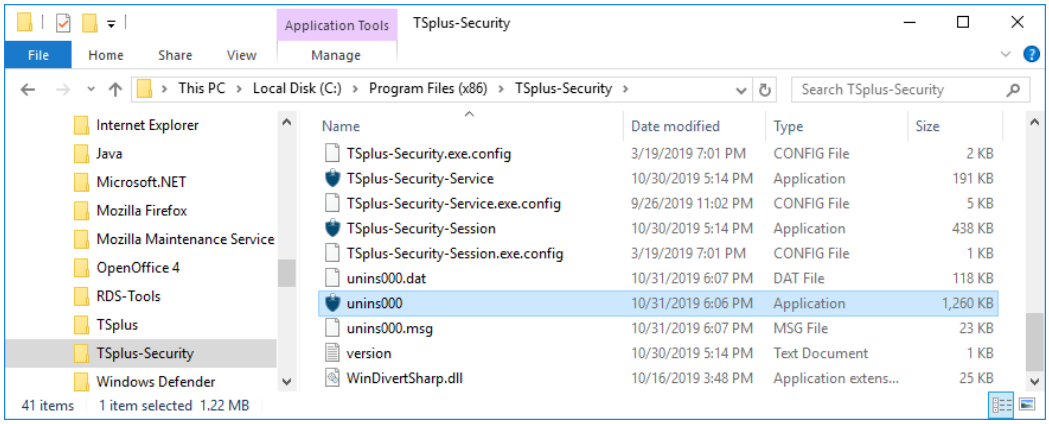
- Install silently, by providing the /VERYSILENT /SUPPRESSMSGBOXES parameters
- Prevent rebooting at the end of the setup, by providing the /NORESTART parameter. This parameter is usually used along with the above.
- Volume Licensing to activate your license directly while installing (please refer to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



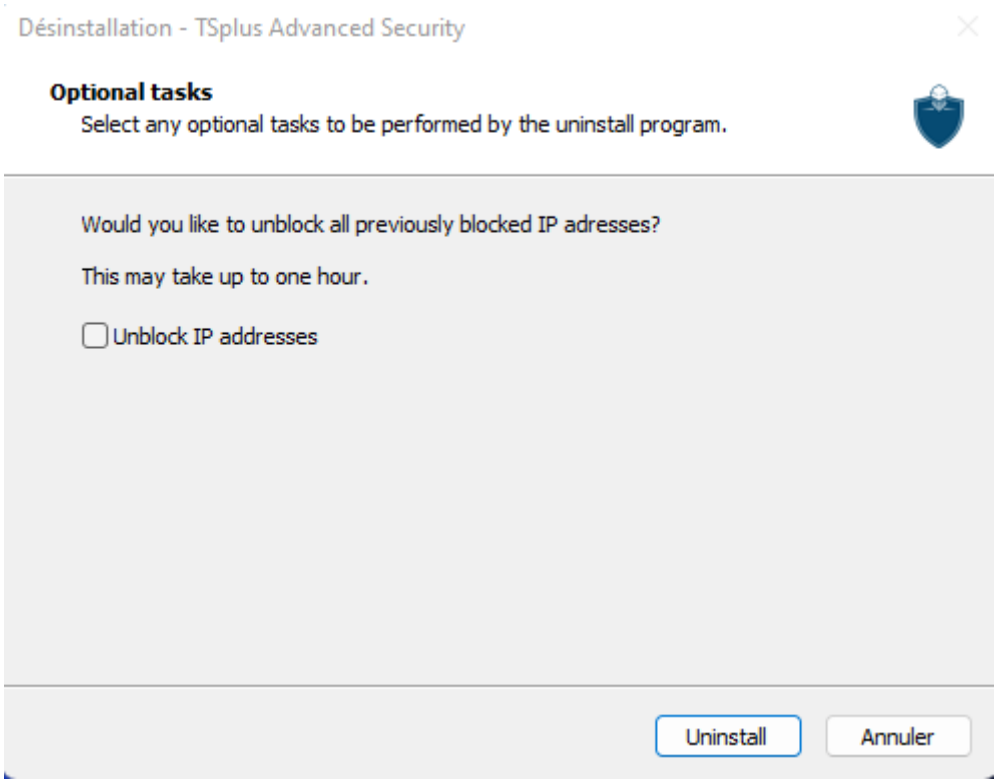
Then, double-click on the "unins000" application to execute the uninstall program.



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.

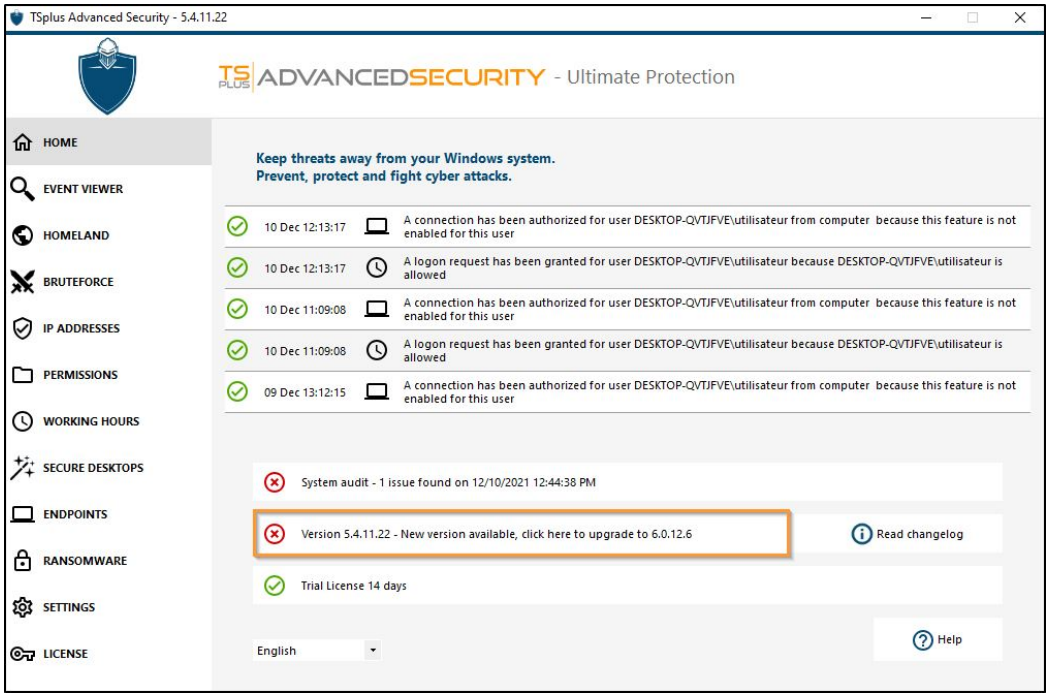
Important:: Please be mindful that removing all the rules can take up to one hour. Because of this, we would recommend to remove the rules directly from the Windows Firewall with Advanced Security console.



The software will be completely uninstalled from your machine.

Updating TSplus Advanced Security

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



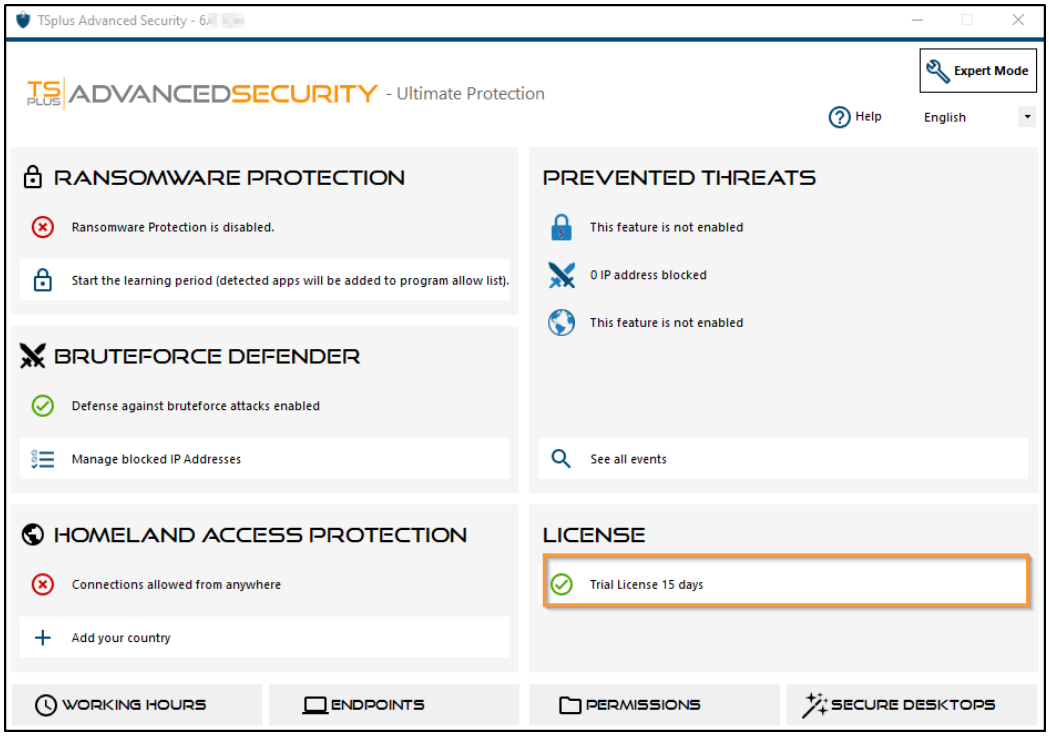
Then, TSplus Advanced Security downloads and applies the update.

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

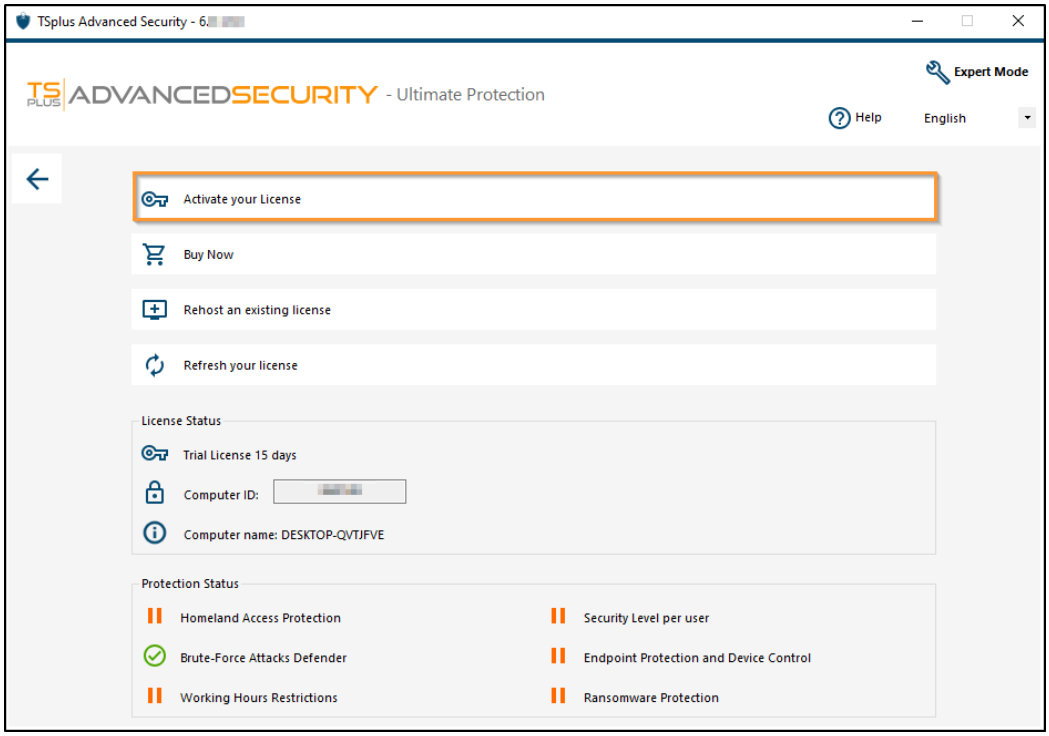
TSplus Advanced Security - Activating your license

Step 1: Activating your license from Lite mode

Click on the "Trial License" button.



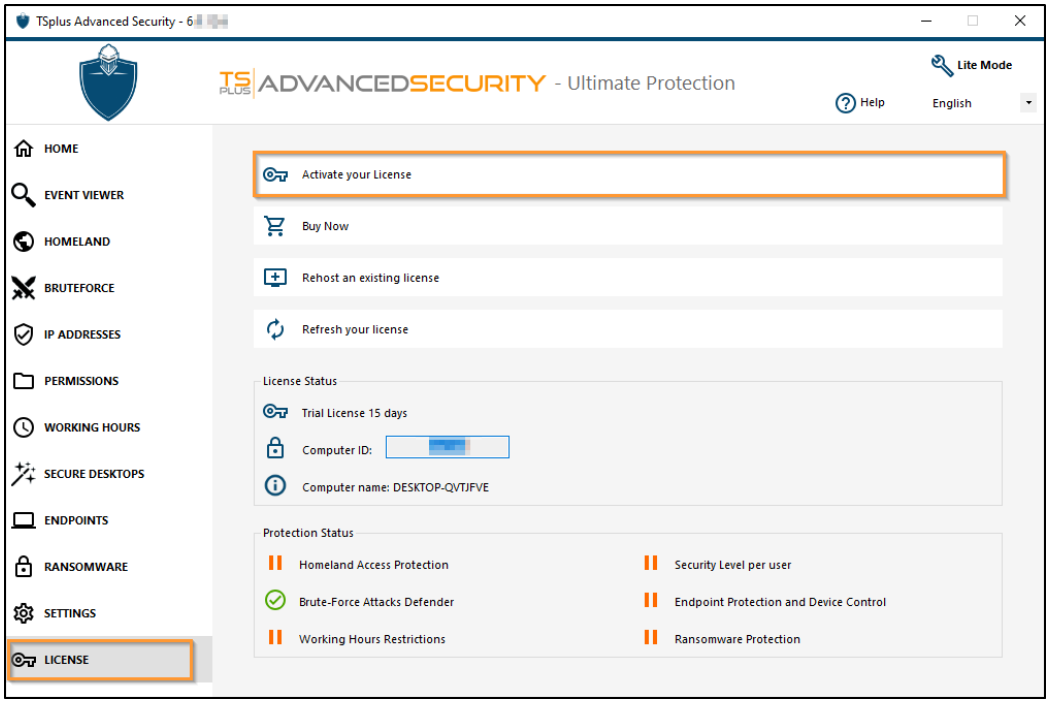
Then, click on the "Activate your License" button.



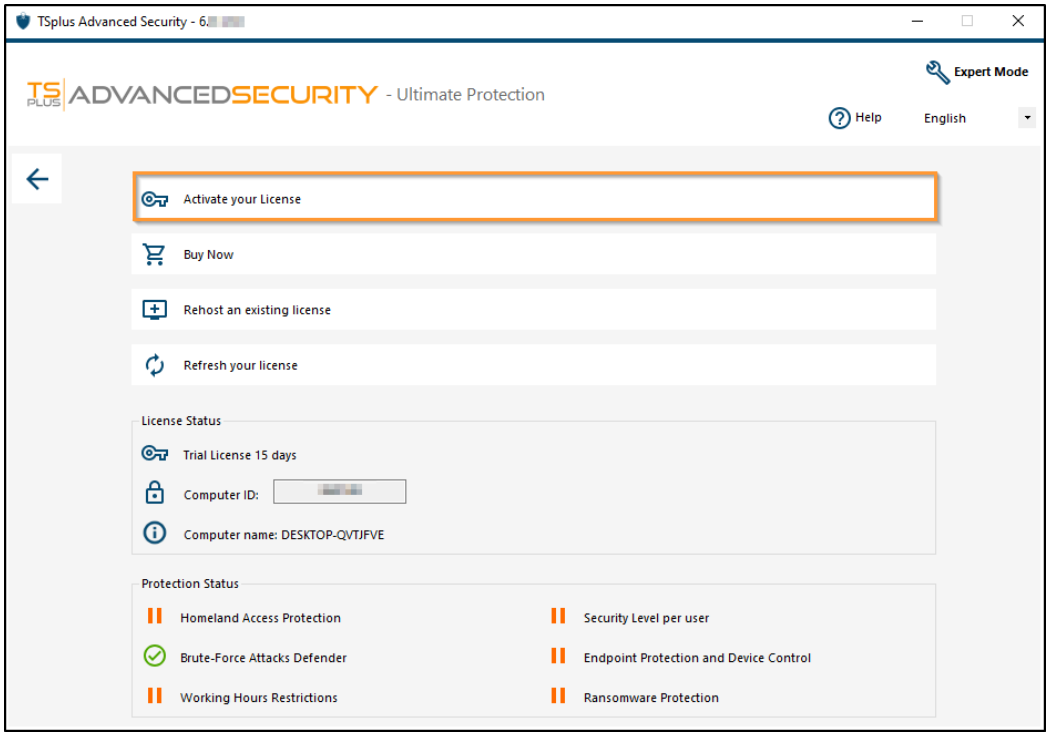
If you do not know you activation key, please proceed to step 2. Otherwise, proceed to step 3.

Step 1 bis: Activating your license from Expert mode

Click on the "License" tab.



Then, click on the "Activate your License" button.



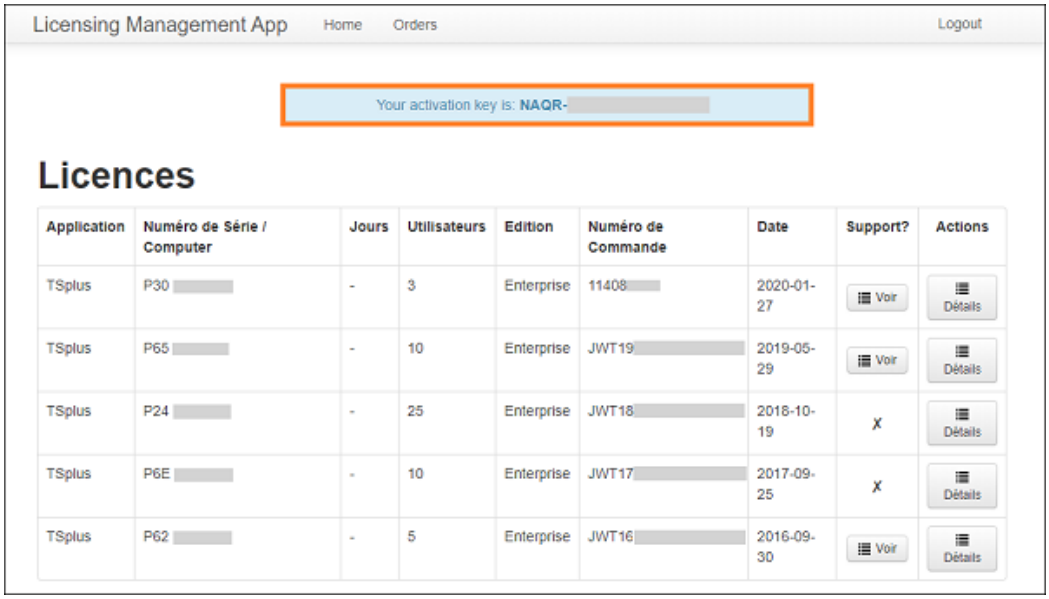
If you do not know you activation key, please proceed to step 2. Otherwise, proceed to step 3.

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:

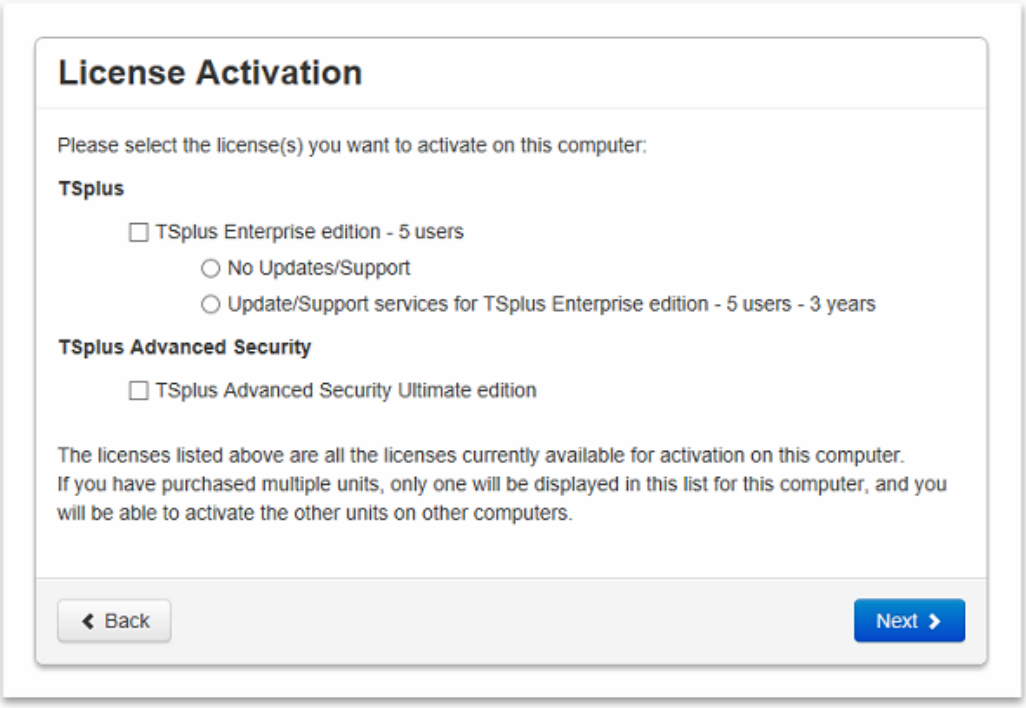
Download the Customer Portal User Guide for more information about your customer portal.

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

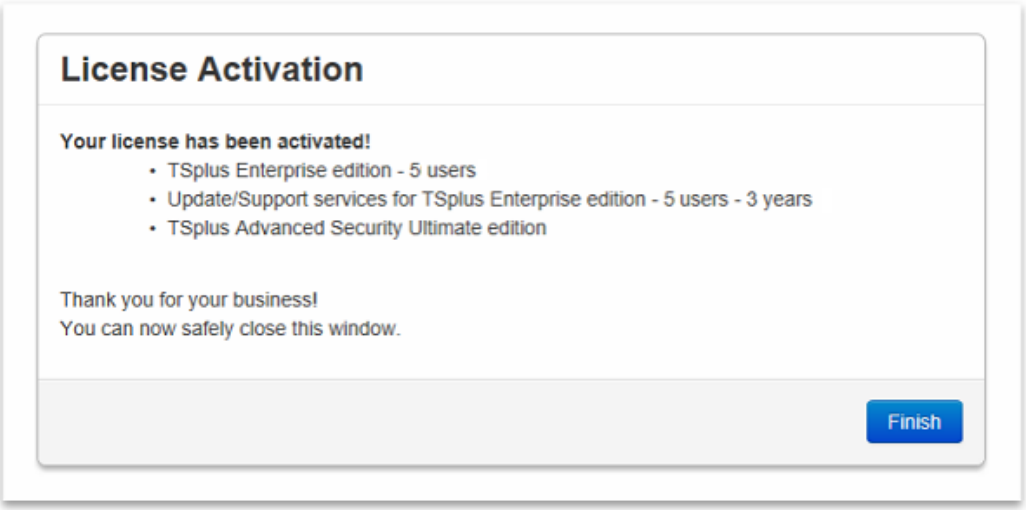


Step 3: Select requested licences and Update & Support services for installed products

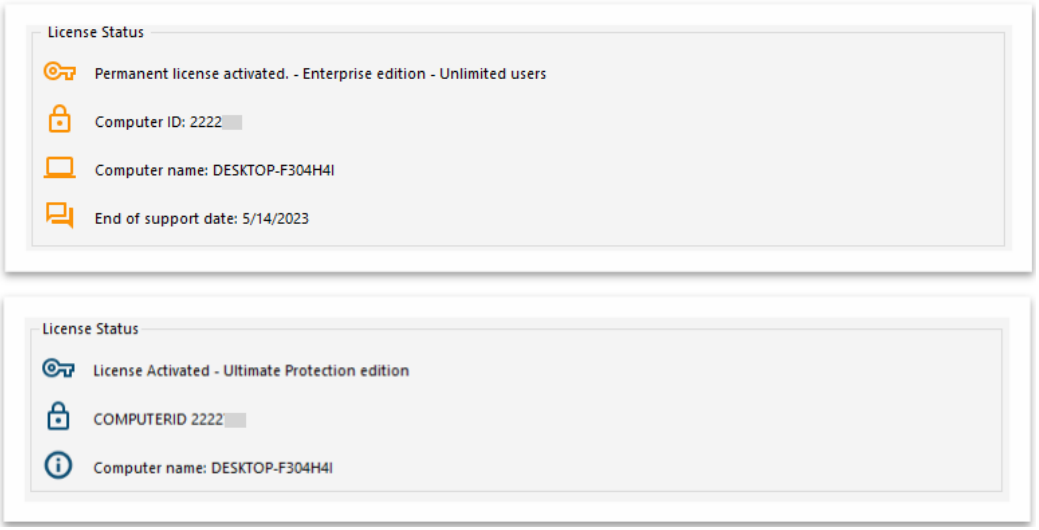
Enter your activation key and click on “Next”.



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.

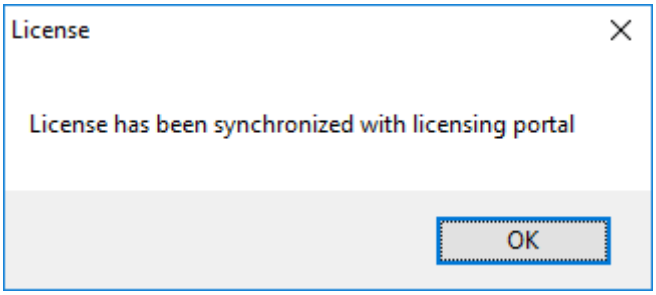


All your selected products and support subscriptions are now activated (in this example, both TSplus with support and TSplus Advanced Security have been activated at once).



Refresh your licensing status by clicking on the corresponding button.

As a result, your licensing information are synchronized with the Licensing portal.



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

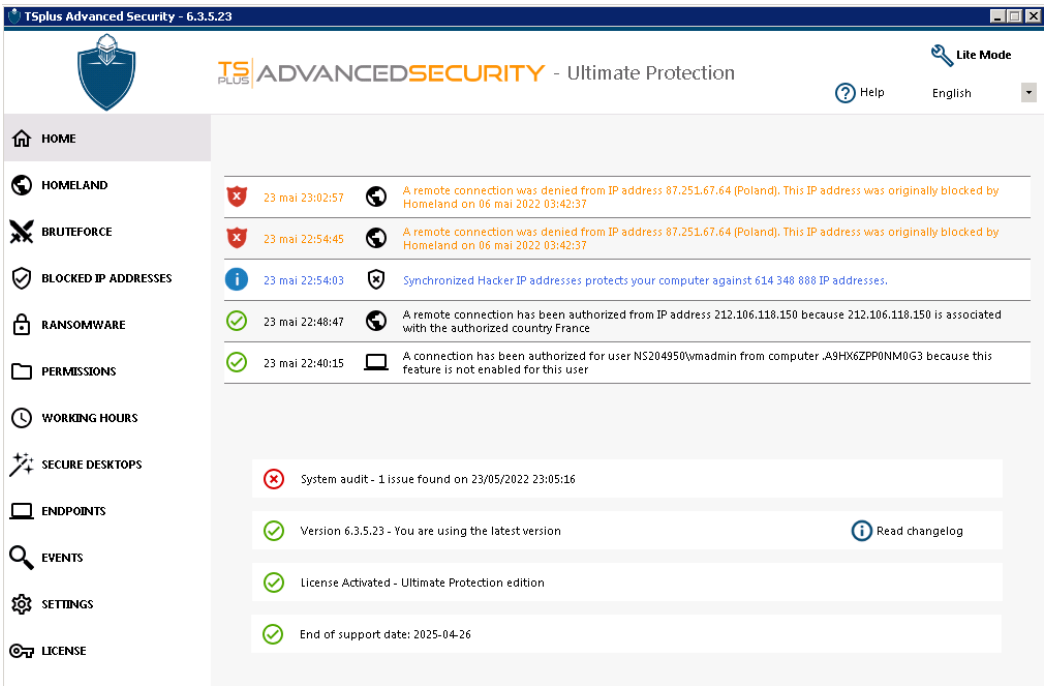
Note:: You can download a license.lic file on the Licensing Portal for TSplus Advanced Security versions below. Please refer to the Customer Portal User Guide for more information.

Thank you for choosing TSplus Advanced Security!

Home

This page describes the Expert mode. Please refer to the Getting Started page for a description of the Lite mode interface.

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 five 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. the system audit
2. new version availability
3. the license status.

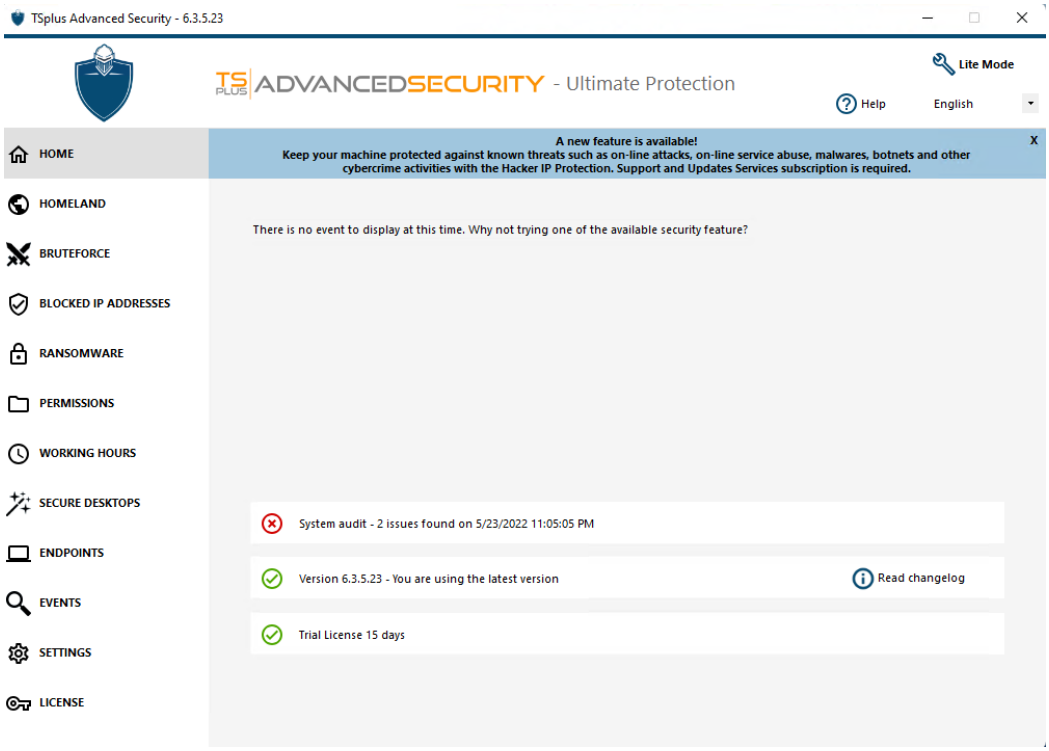
Please select your display language using the dropdown located in the top right corner, should the application did not detect your language.

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

System Audit

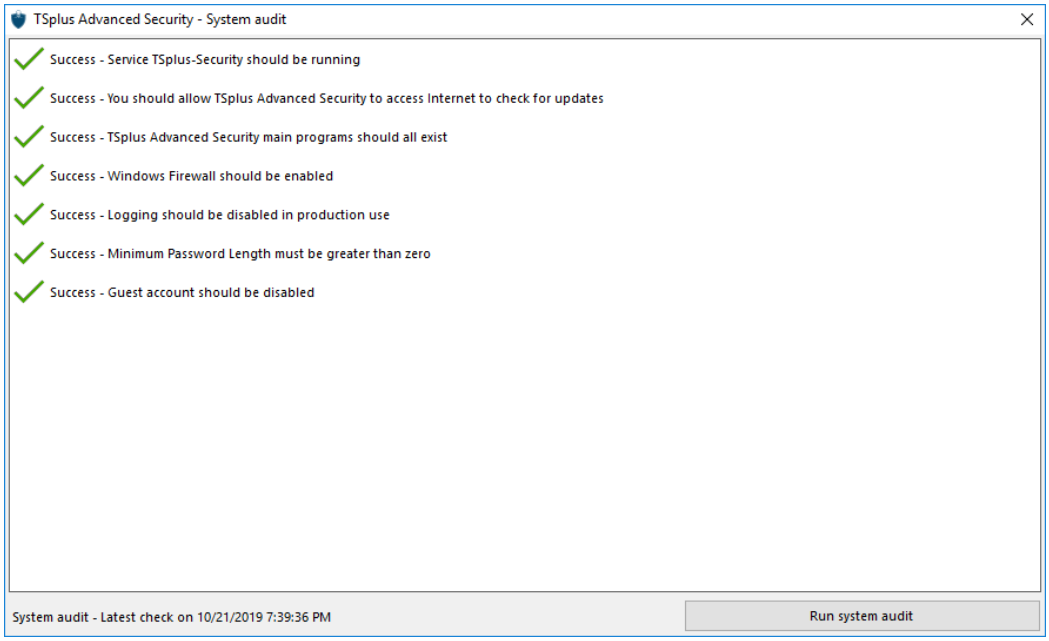
TSplus Advanced Security offers a System Audit located on the AdminTool dashboard.

The icon on the System Audit button turns red when an issue has been found. Please review them carefully.



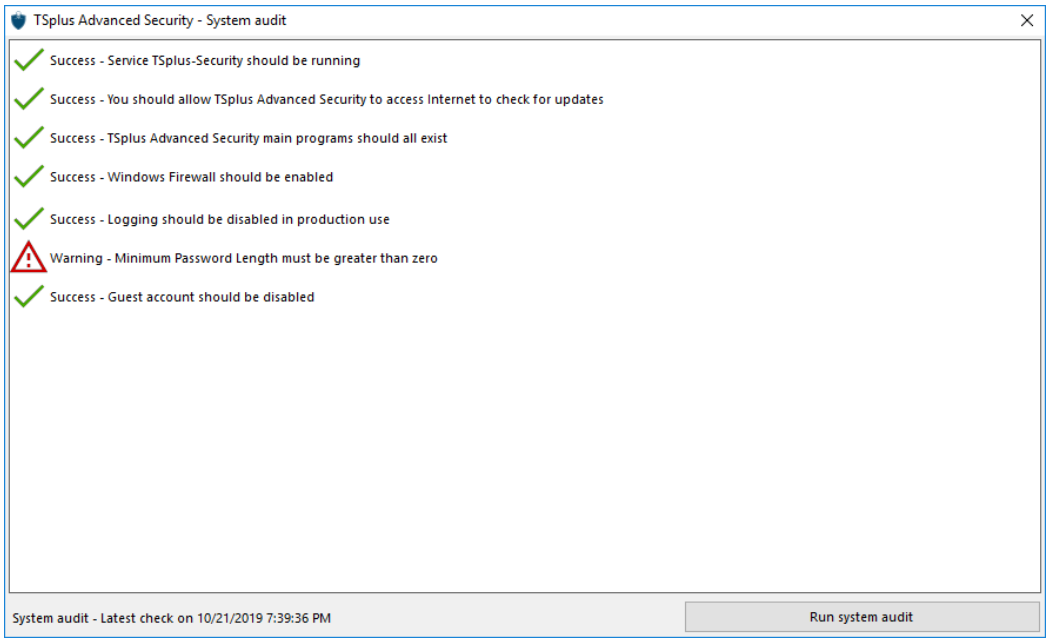
When you click on the system audit tile, you can see that it monitors:

- TSplus Advanced Security service is running.
- TSplus Advanced Security has access to the internet and is allowed to check for updates.
- TSplus Advanced Security main programs exist.
- Windows Firewall is enabled. This audit rule is not checked should Advanced Security be configured to use the built-in firewall.
- Logging is disabled.
- Windows minimum password length is greater than zero.
- Guest account is disabled.

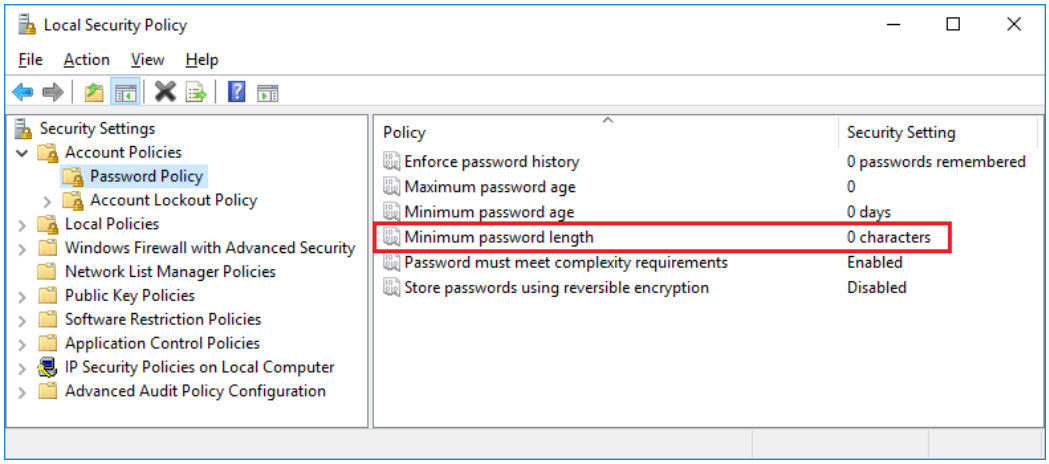


Fixing Minimum Password Length issue

The Minimum Password Length audit rule is implemented to alert administrators that an account may not have a password, which make intrusion very likely to happen in case the machine is facing the internet.



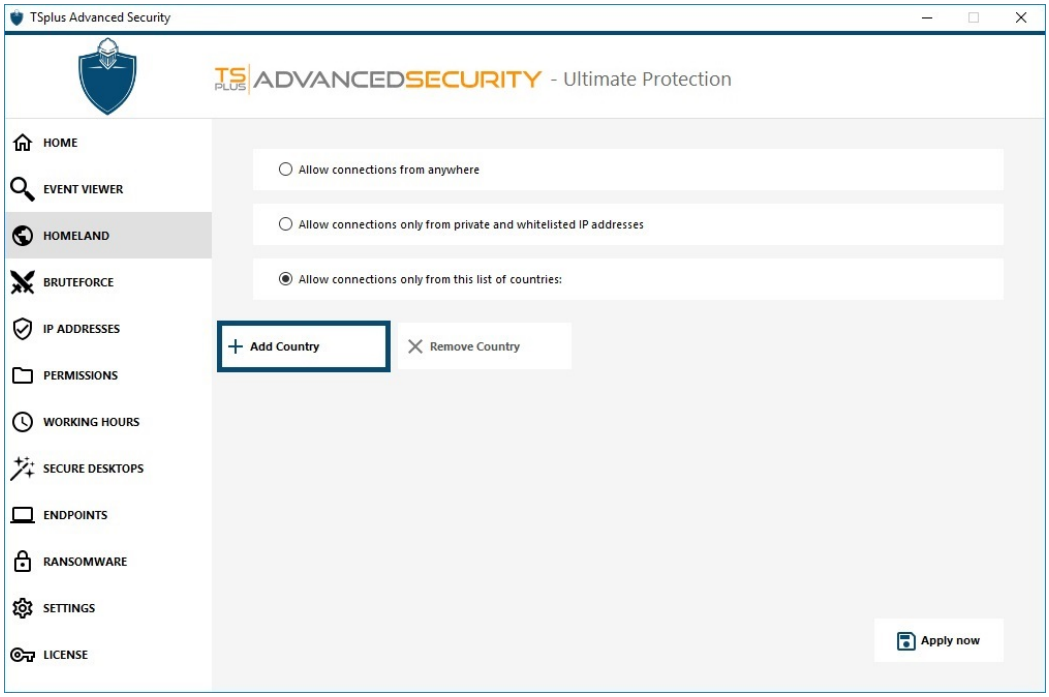
Please modify the minimum password length on your server, under Local Policy/Account Policies/Password Policy, to fix this major security issue:


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
0
Minimum password age
0 days
Minimum password length
0 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled

Homeland Access 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.

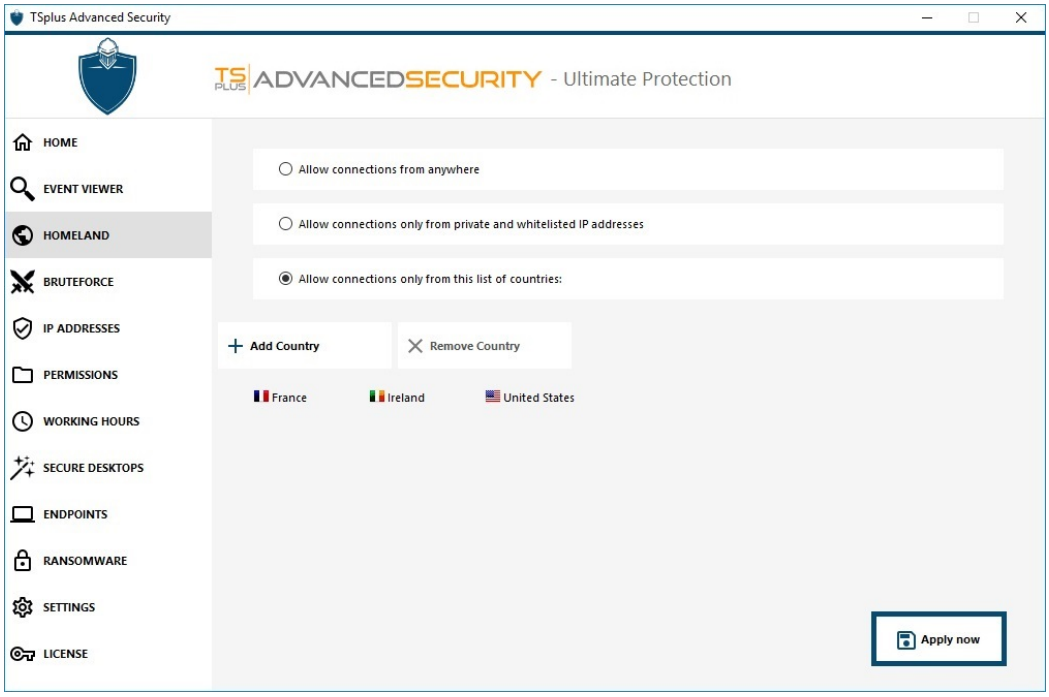


A popup offering a country list opens. Select the country you wish to add on the list.

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

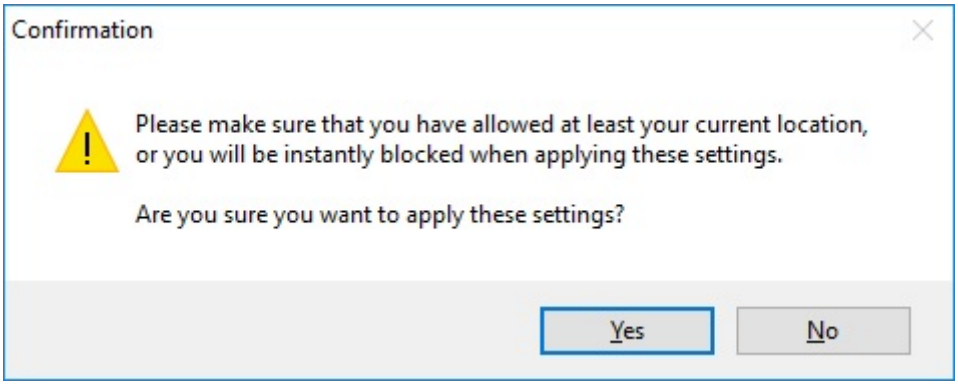
Click on the button "Add Country" to return to the feature main screen.

Important: In order to save your changes, click on the "Apply" button.



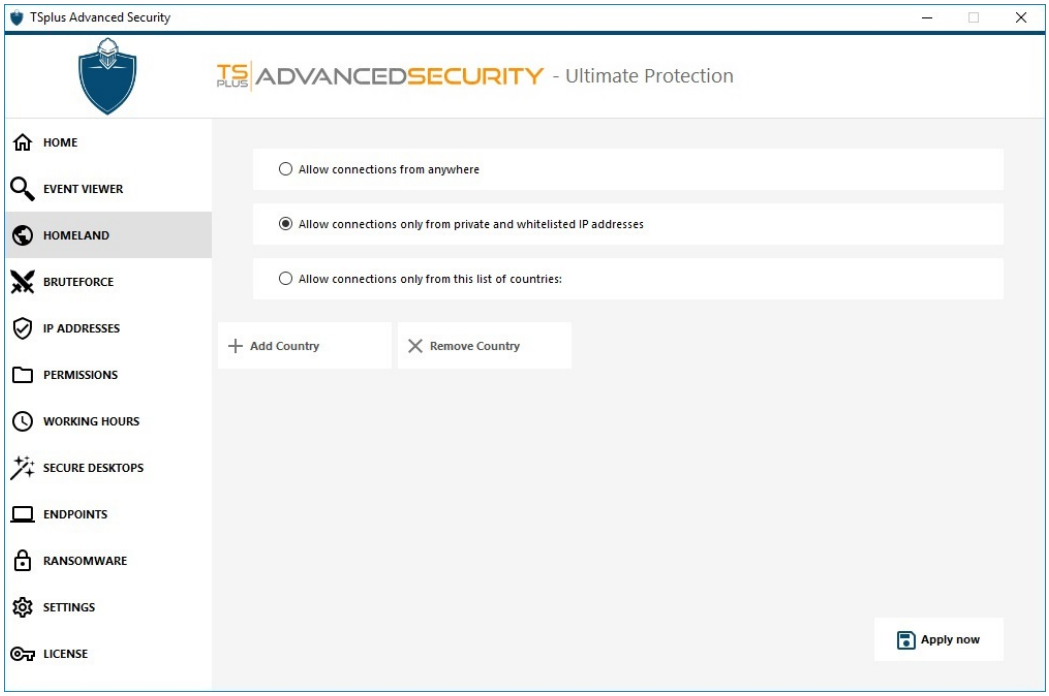
In this example, remote access is allowed for users connecting from United States, Ireland and France.

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



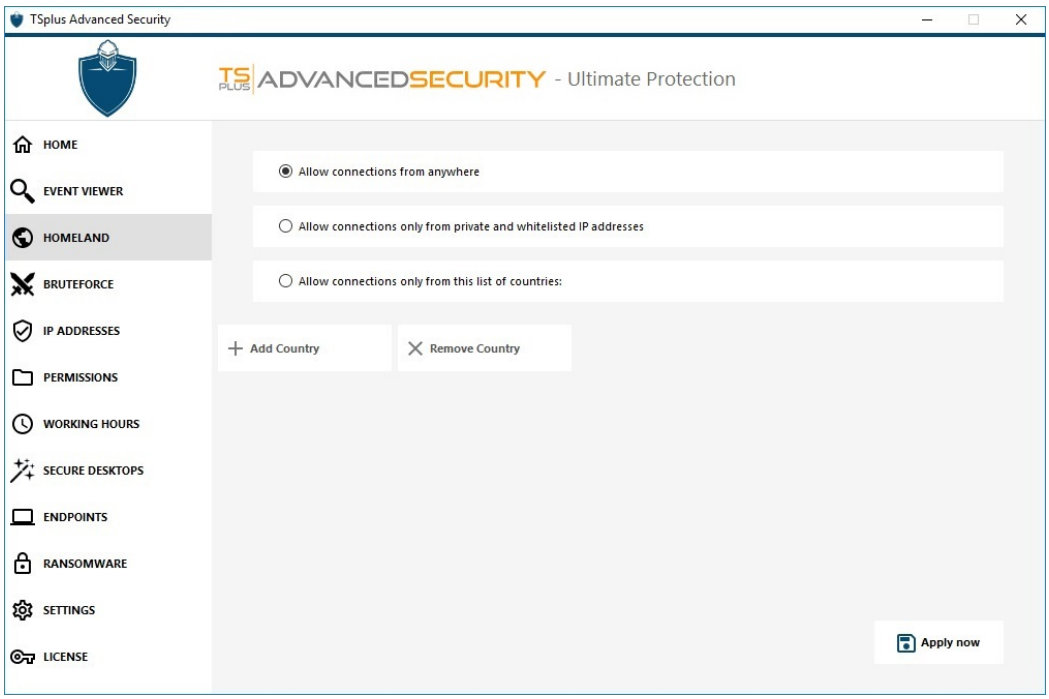
Restrict access from the internet

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



Disable Homeland Access Protection

By default, Homeland Access 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 IP Addresses. 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 Homeland Access Protection or Bruteforce Protection features.

Undestanding Homeland Access Protection

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

Processes: Homeland Access 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 > Homeland.

Network ports: by default, Homeland Access Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC. Homeland 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 > Homeland.

Detection mechanisms:

Homeland 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 Homeland'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 Homeland Access 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, Homeland Access 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.

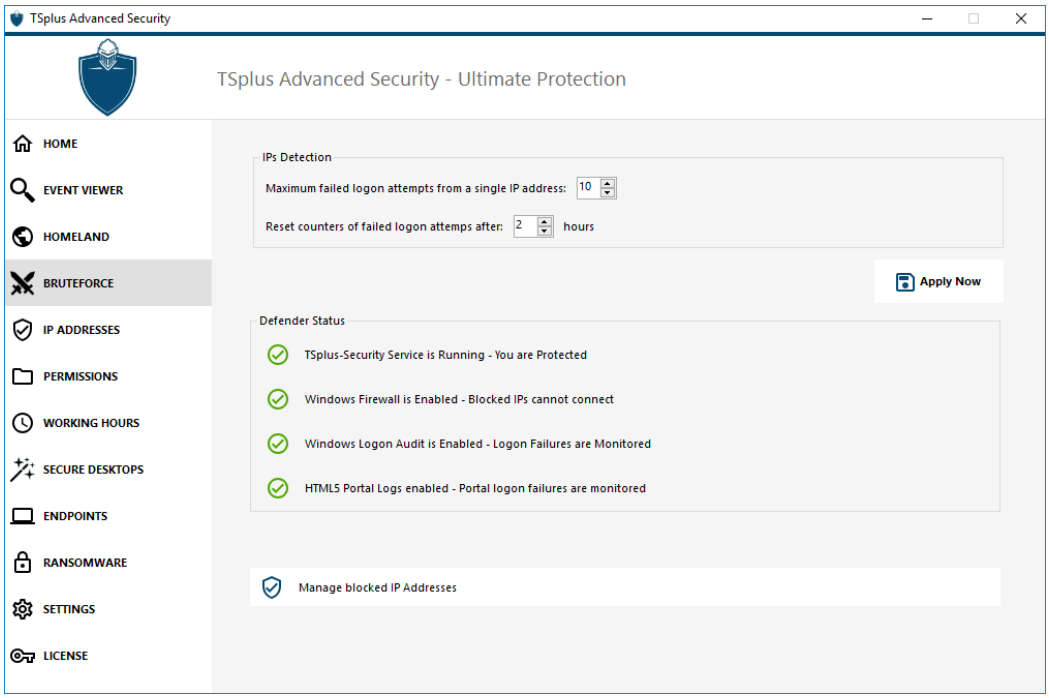
VPN: In case the remote client uses a VPN, Homeland Access Protection will get an IP address chosen by the VPN provider. As you know, VPN providers use relays all around the globe to allow its users to browse anonymously. Some VPN providers allow users to define the relay’s country. Thus, users with 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 Homeland Access 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 Homeland Access Protection. However, a proxy would definitively change the originating IP address to use a private network address, which will always be allowed by Homeland Access 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.

Bruteforce Attacks Defender

The Bruteforce Attacks Defender 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 brute-force attacks defender.

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

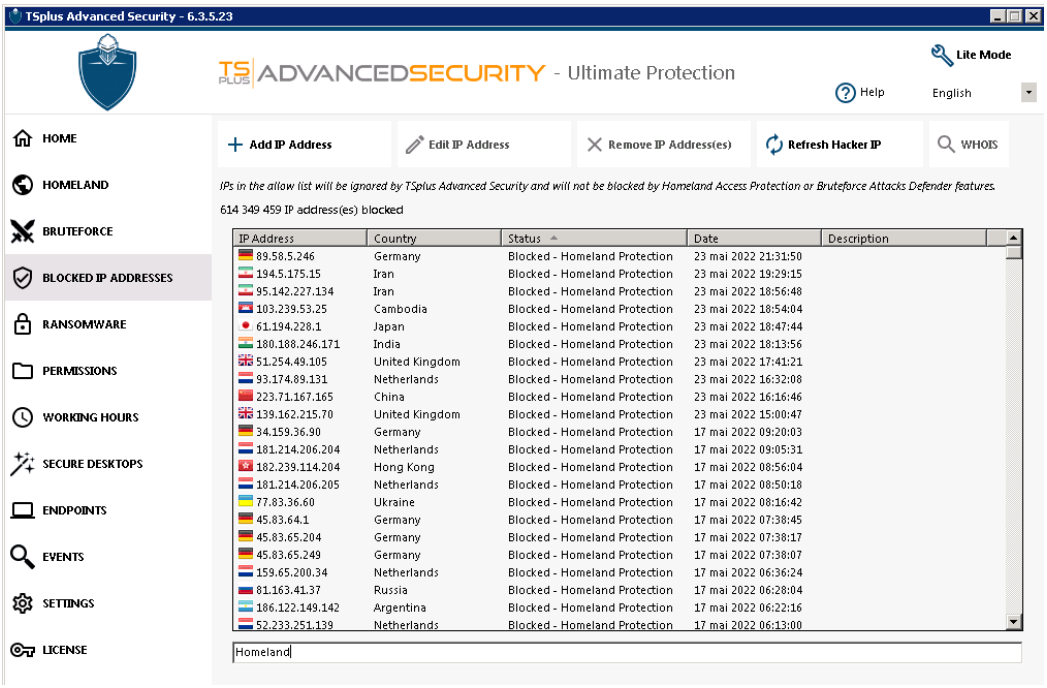
Note: If you ever notice that the Brute-Force Attacks Defender blocked 10 IP addresses per day and that now, it is not the case anymore; and blocks one, two or even doesn't block any address, it is actually normal. Indeed, before advanced-security installation, the server having an RDP port publicly 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.

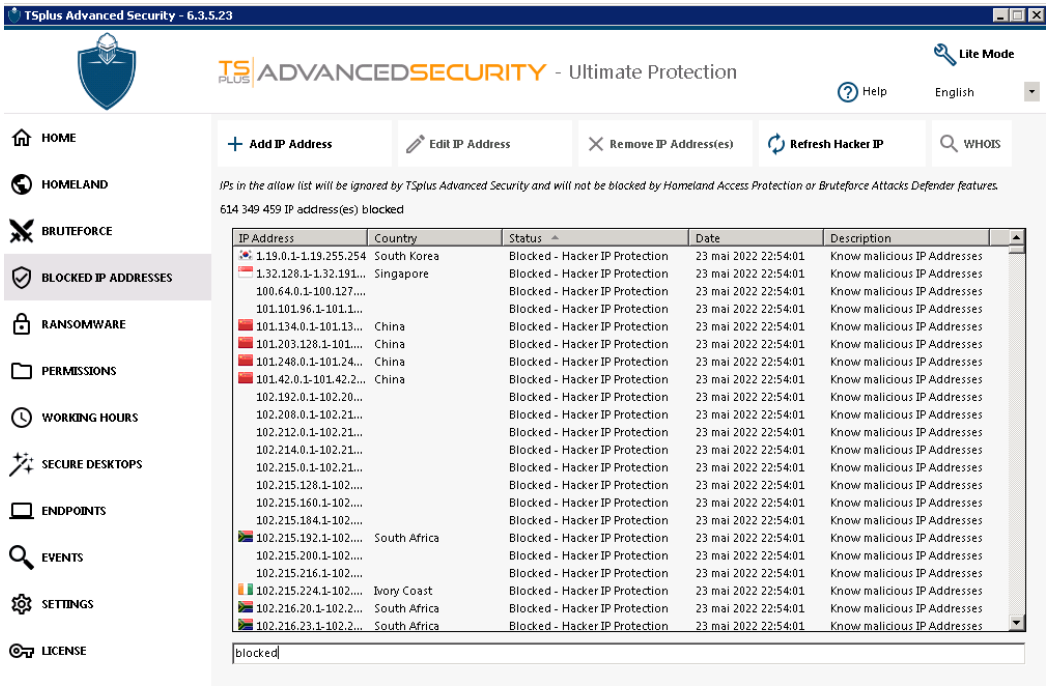
IP Addresses

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

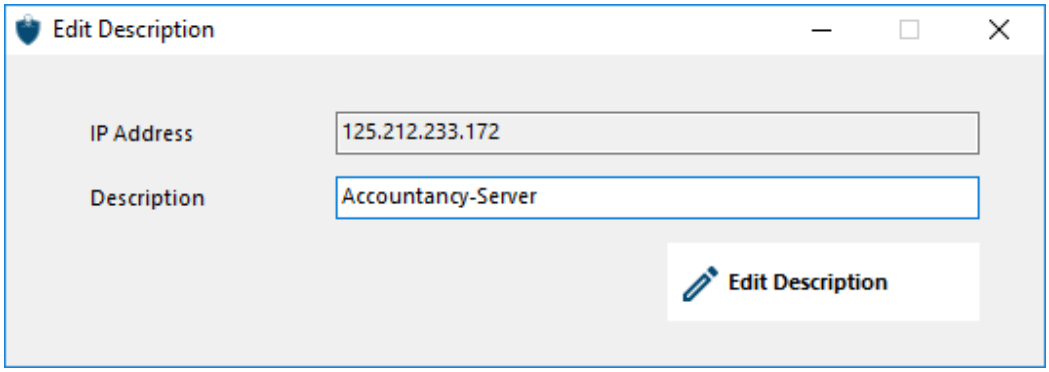


By default, IPV4, IPV6 and all server localhosts addresses are whitelisted.

A convenient search bar provide search capabilities based on all information provided. For example, if we searched for blocked addresses, by entering the word "blocked" on the search bar, all the blocked IPs will be visible:



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 **colon 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]

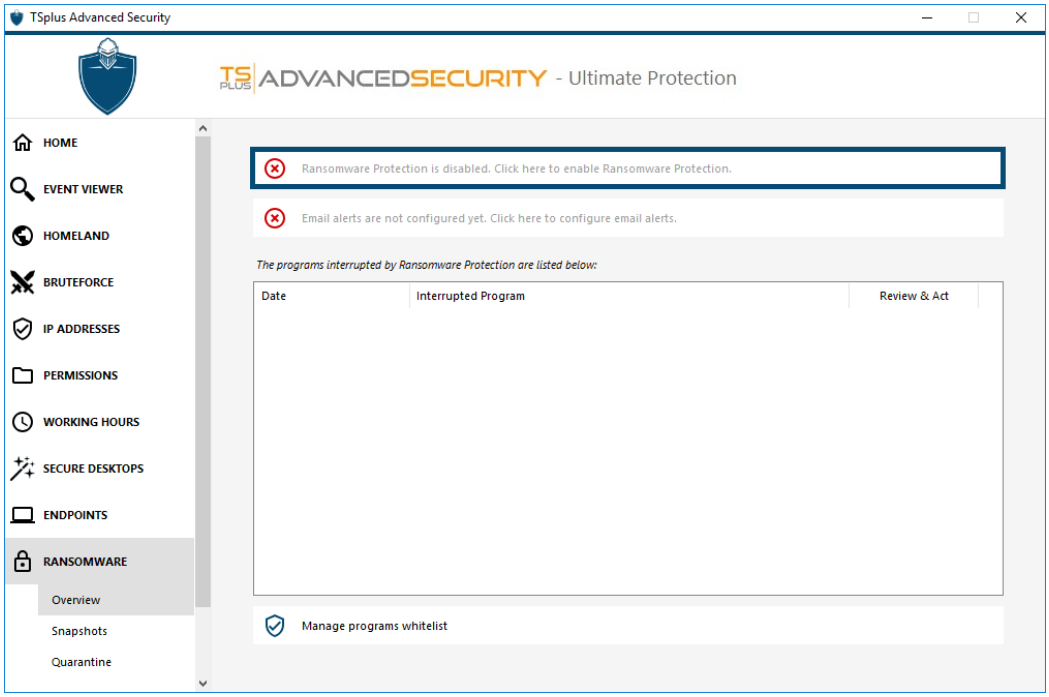
This command has no effect on IP addresses already blocked by Hacker IP protection. If you still want to unblock one of these addresses, please use the whitelist command.

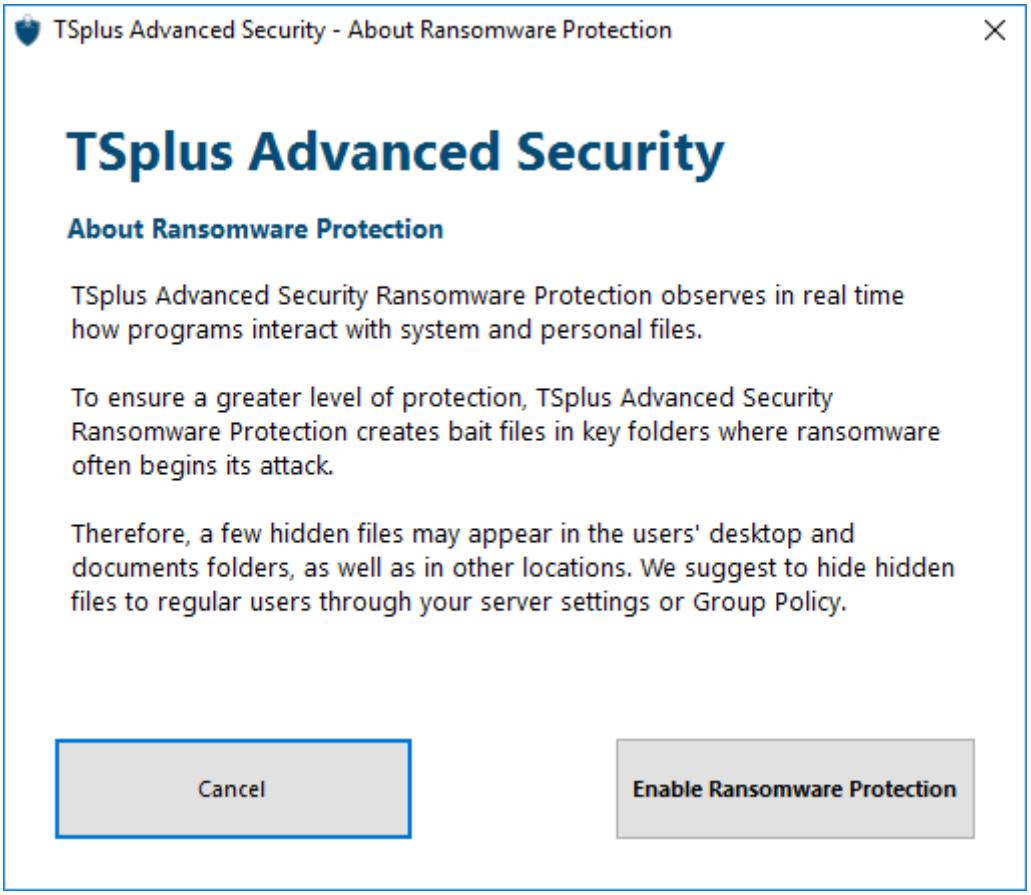
Ransomware Protection

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:

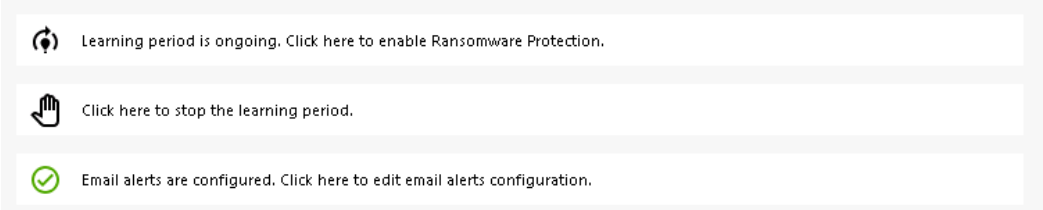




Learning Period

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.

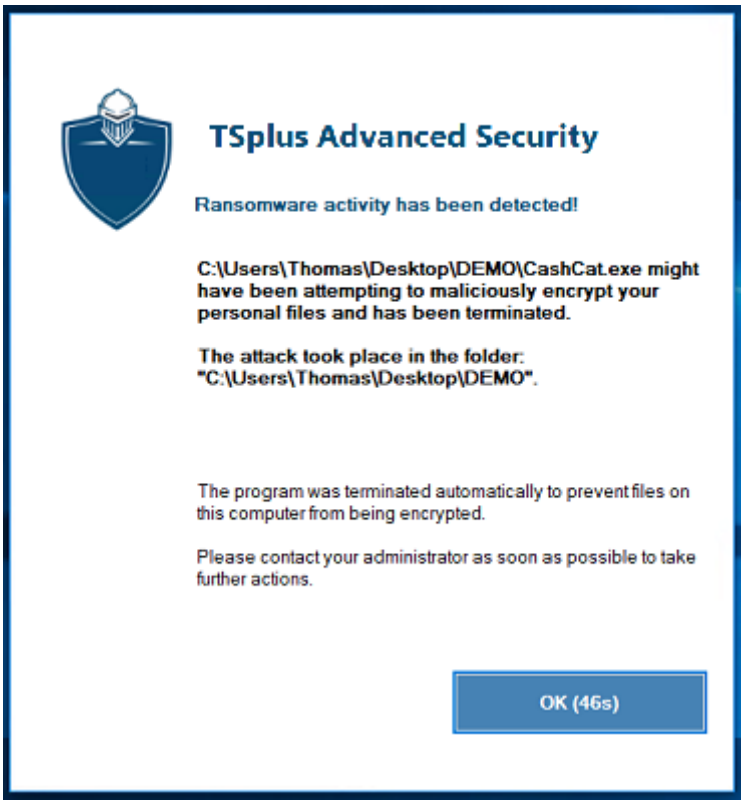
This feature allows to configure Ransomware Protection on a production server without disrupting its activity. We recommend to start with a 5 days Learning Period to identify all legit business applications.



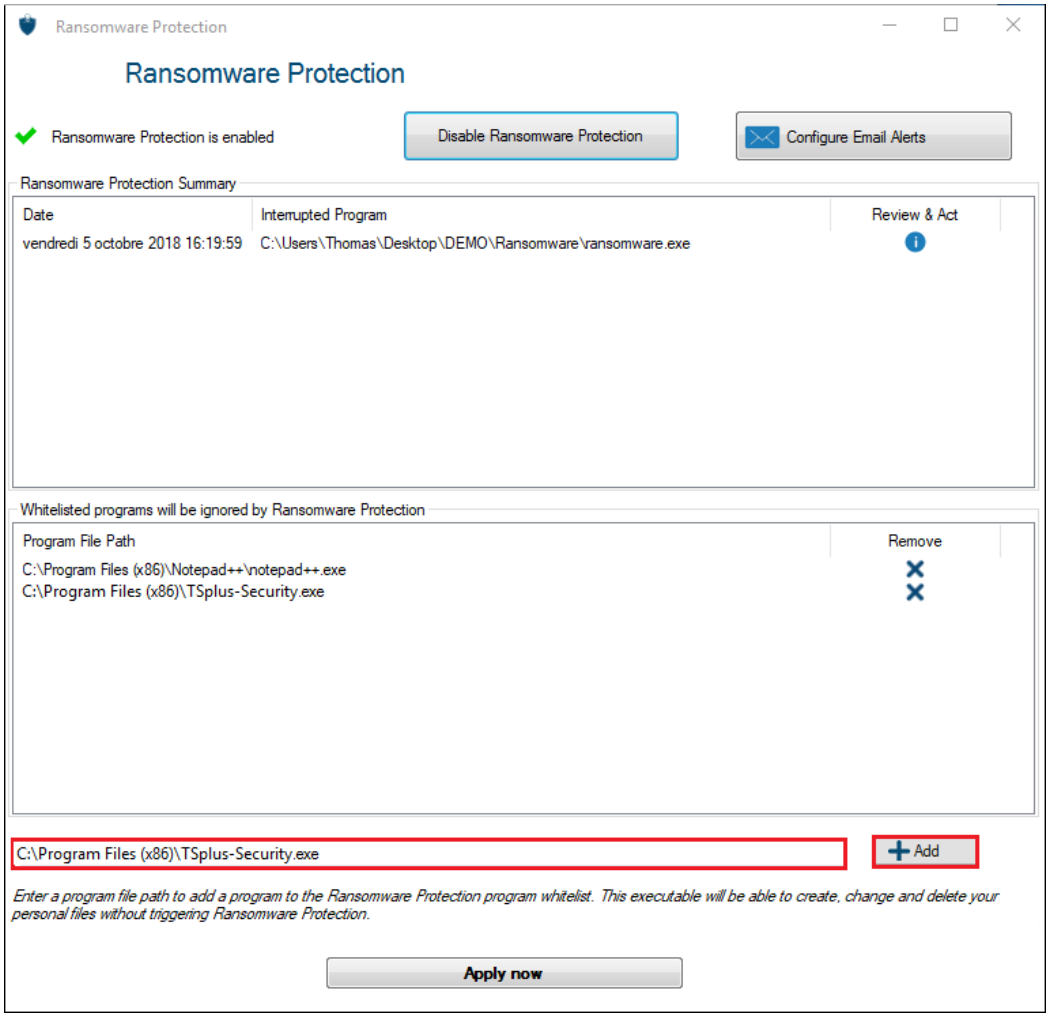
If you stop the Learning Period, it will deactivate the Ransomware Protection. Click on the "Ransomware Protection is disabled" button to reactivate the Learning Period.

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.



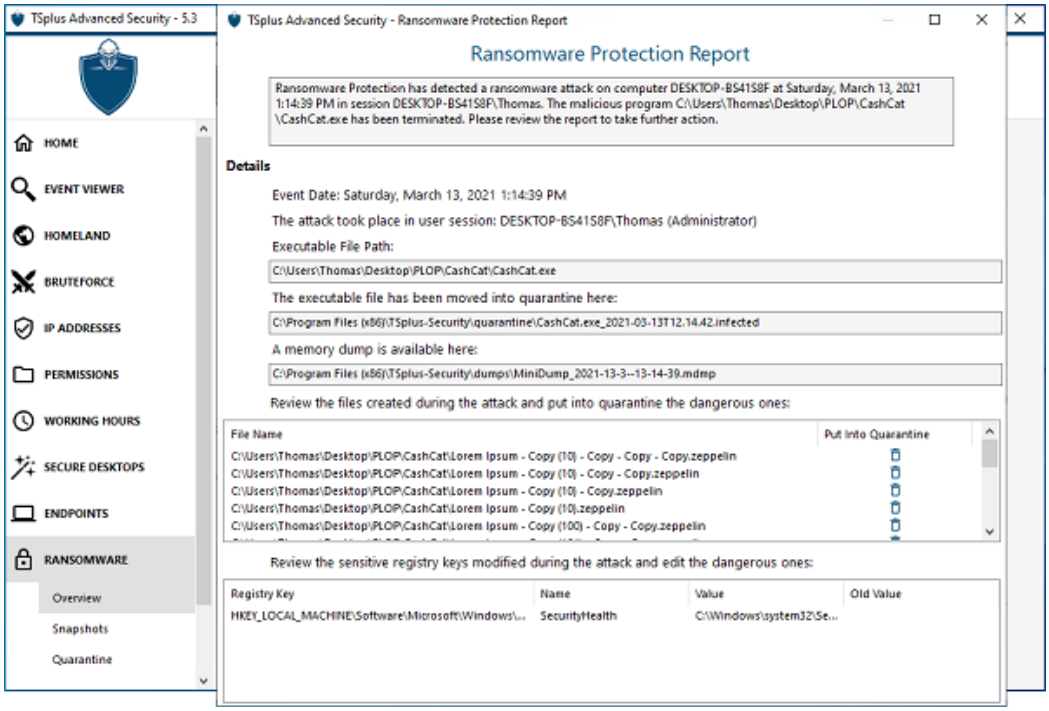
Only the administrator can whitelist them, by entering the path of the desired program on the bottom line and by clicking on "Add":



Ransomware Protection Report

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

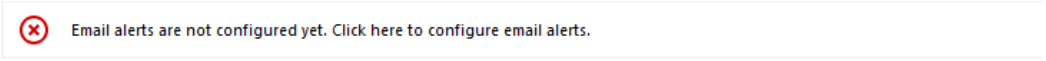
The administrator has access to information regarding the source of the attack and running processes, and therefore learns how to anticipate these threats.

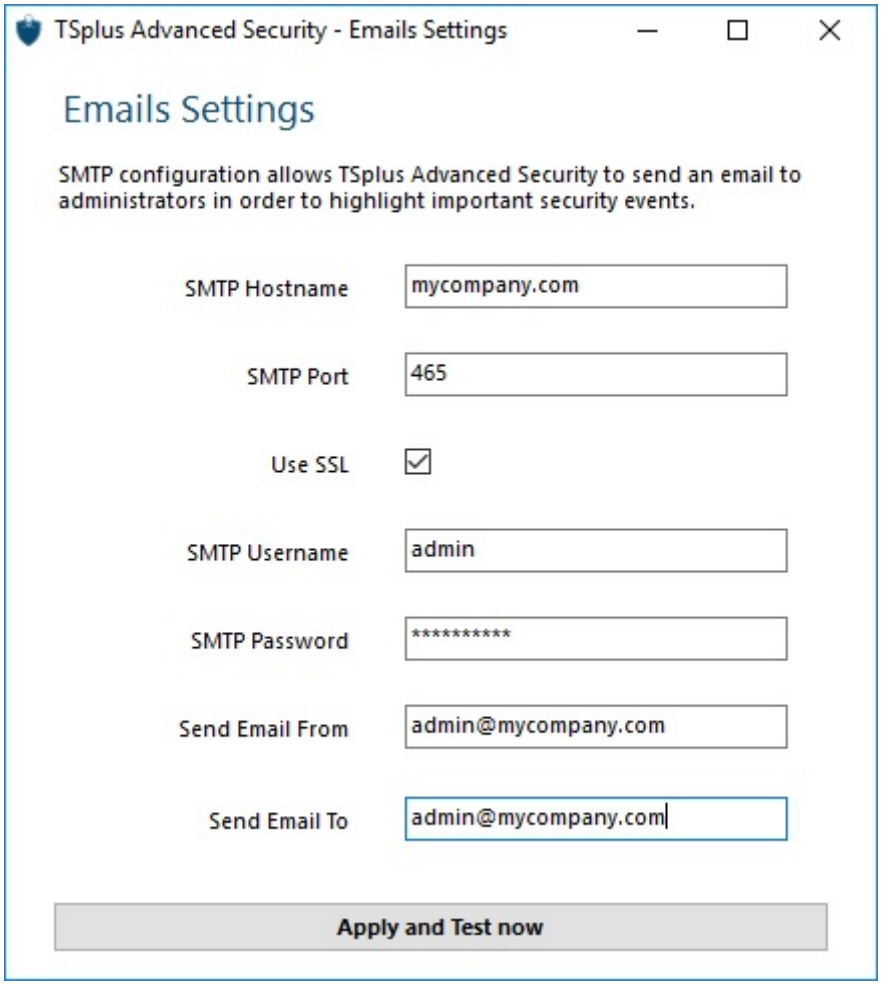


Note: Ransomware Protection observes how programs interact with system and personal files. To ensure a greater level of protection, Ransomware Protection creates bait files in key folders where ransomware often begins its attack. Therefore, a few hidden files may appear in the users' desktop and documents 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.

Add an SMTP configuration - Email Alerts

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:





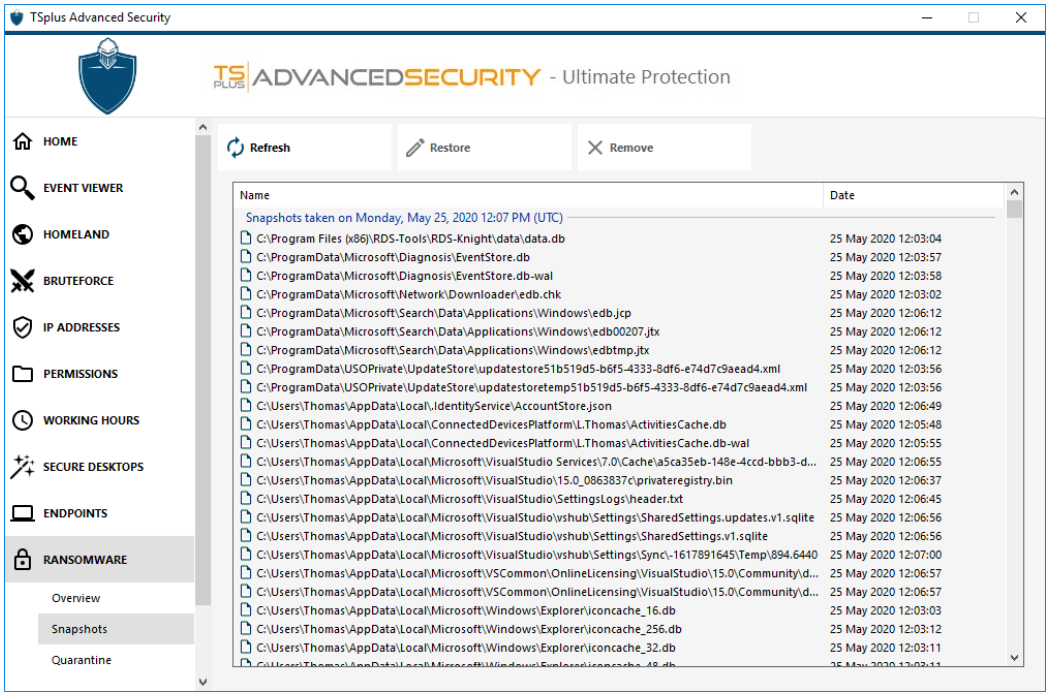
Enter your SMTP Hostname, Port and check the Use SSL box and change change the port from 25 to 465 if you wish to use SSL.

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

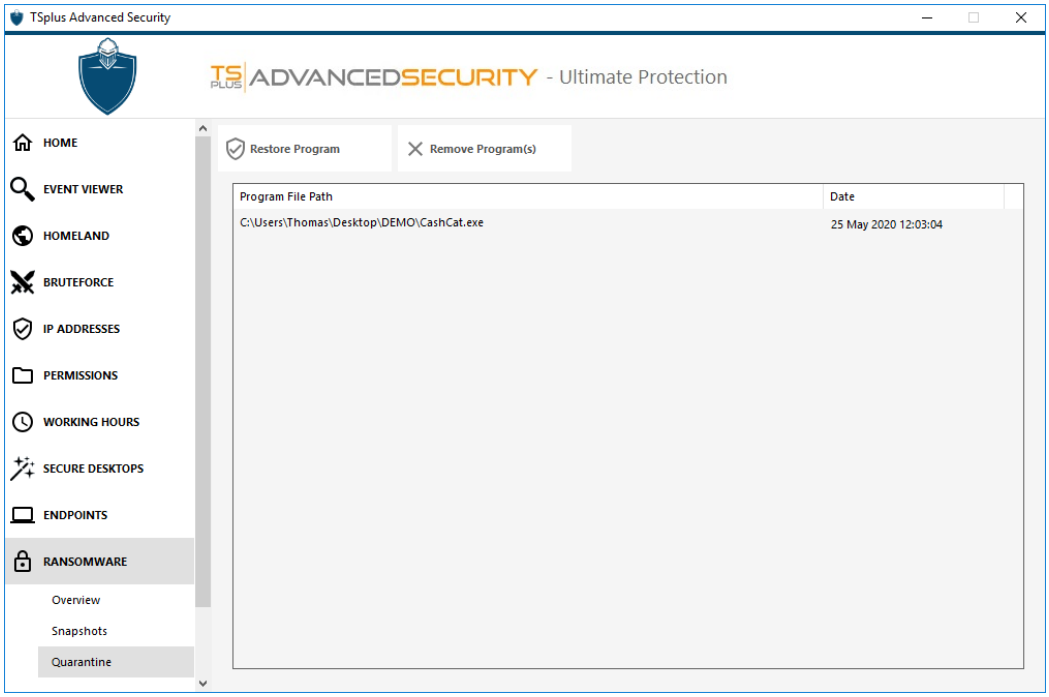
Snaphshots taken by Ransomware Protection are visible under the Snapshots tab:



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:



Each element can be restored or removed.

List of Ignored by Default File Extensions

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.

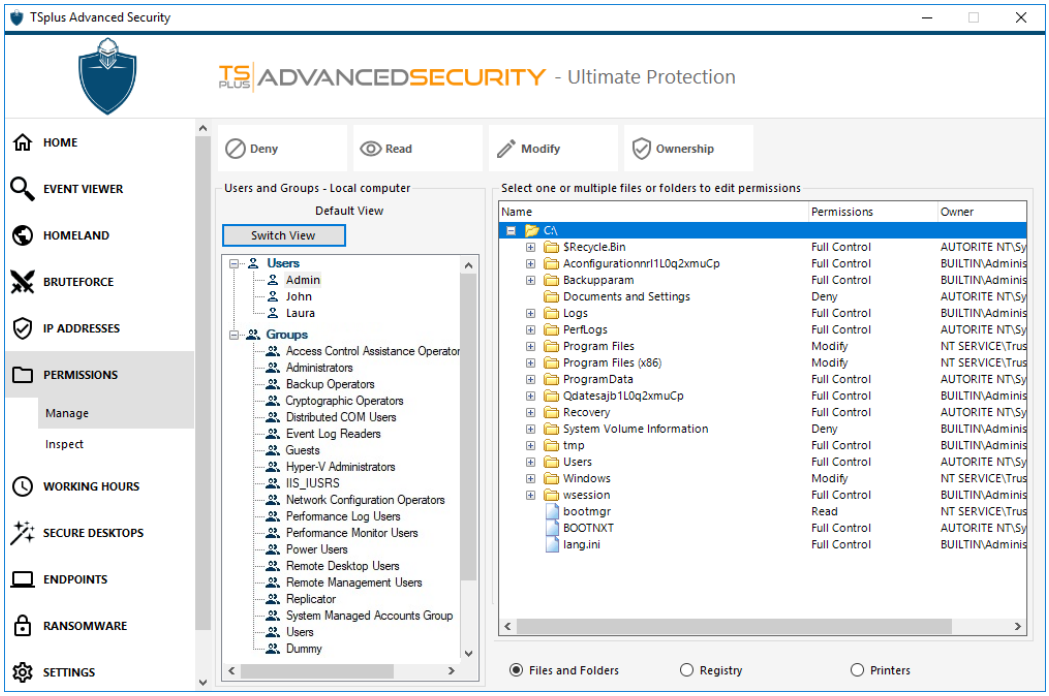
Permissions

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:

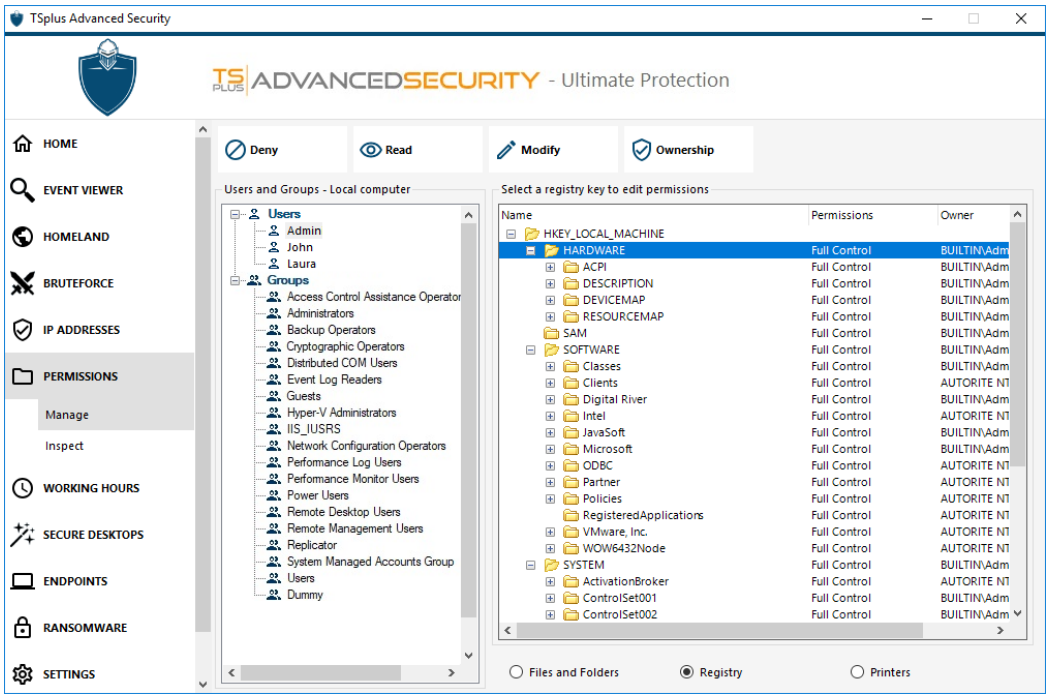


- **Deny** - When clicking on the Deny button, the selected user will be denied privilege on the selected filesystem object. If a file is selected, then the selected user is denied the privilege of reading the selected file (FileSystemRights.Read). If a directory is selected, then the selected user is 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

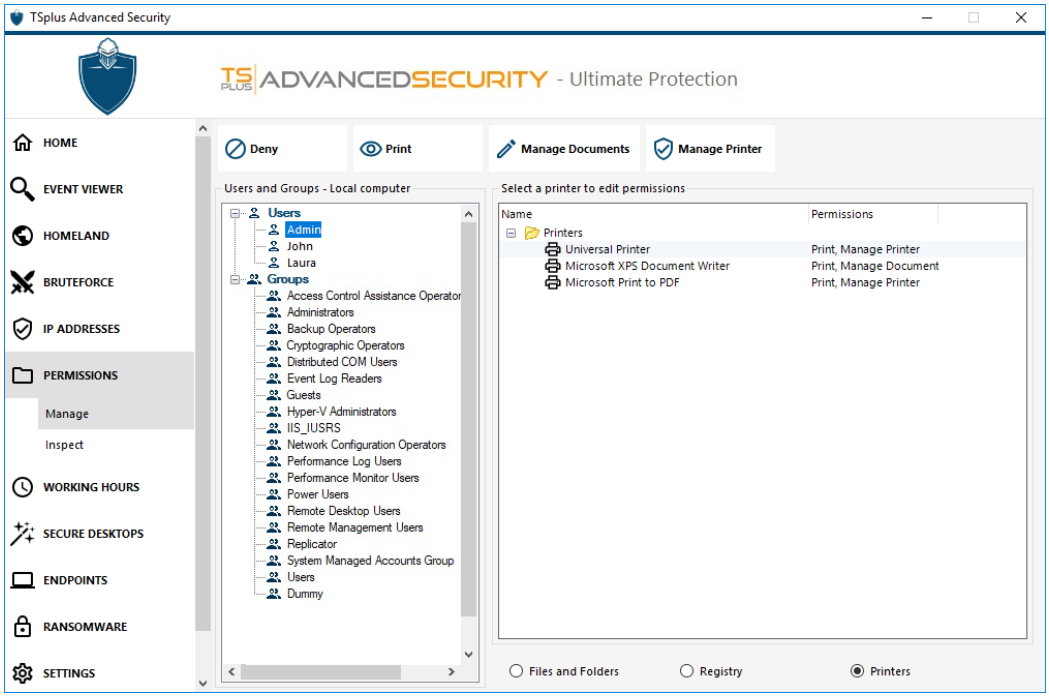
FileSystemRights.Traverse).

- **Ownership** - When clicking on the Ownership button, the selected user will be granted full control over the selected filesystem object (FileSystemRights.FullControl).

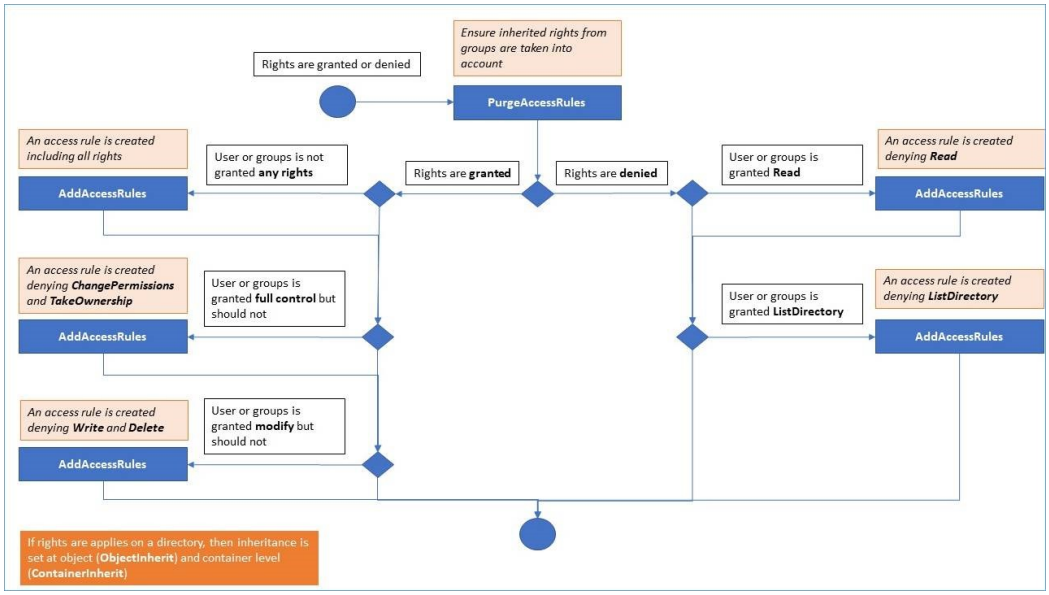
Same permissions options are possible for each Registry, by selecting the corresponding button under the right-tree view :



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:

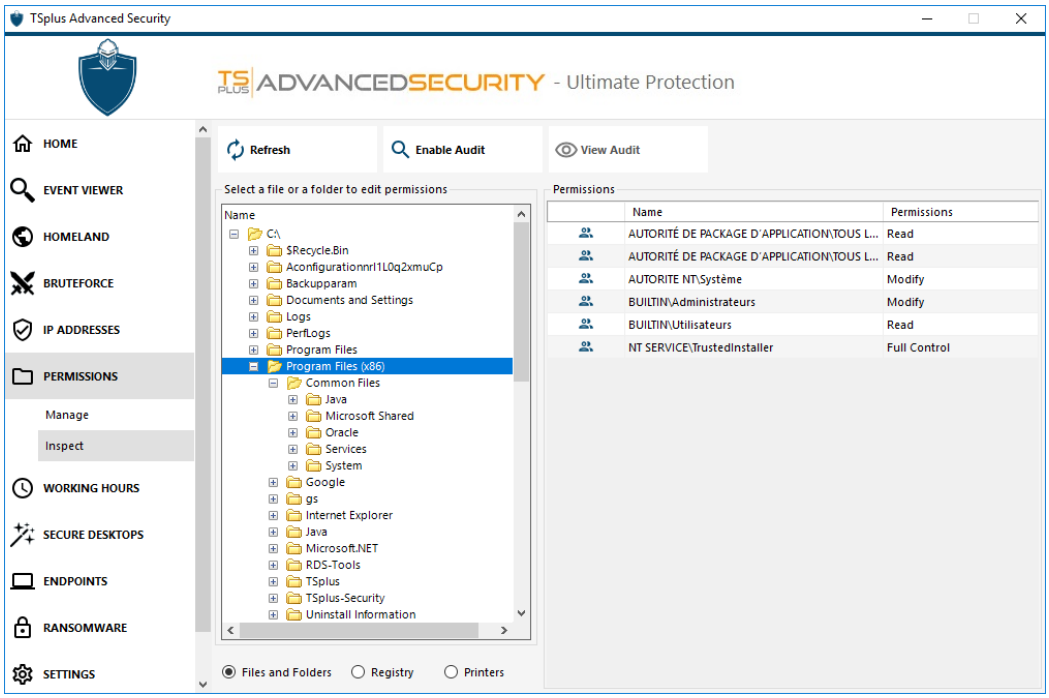


Documentation:

- 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

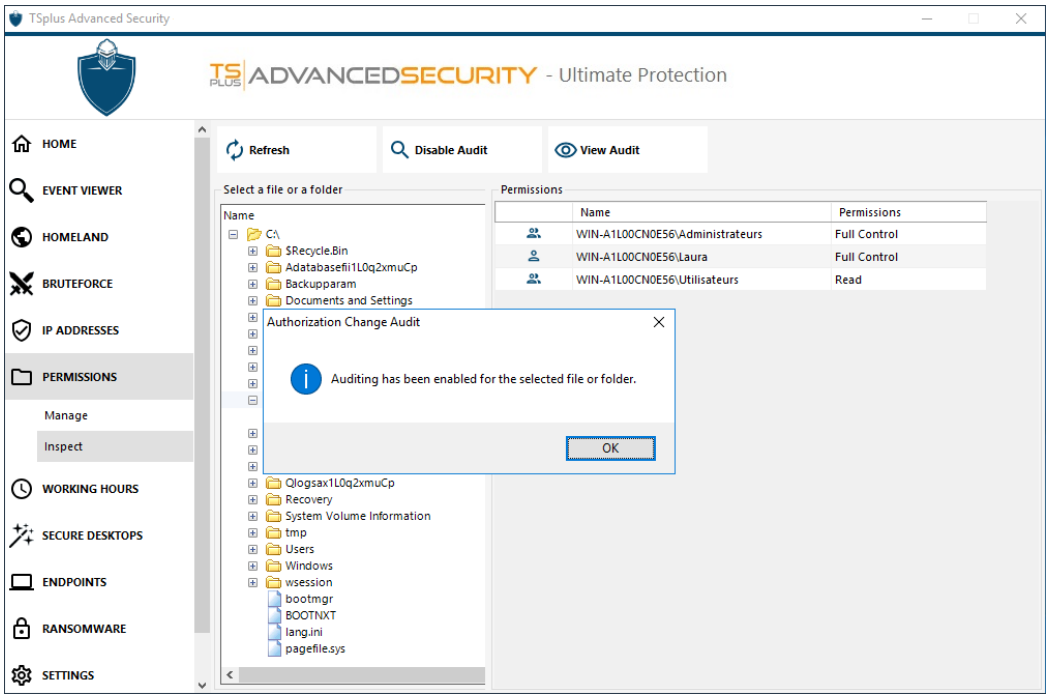
Inspect Permissions

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.

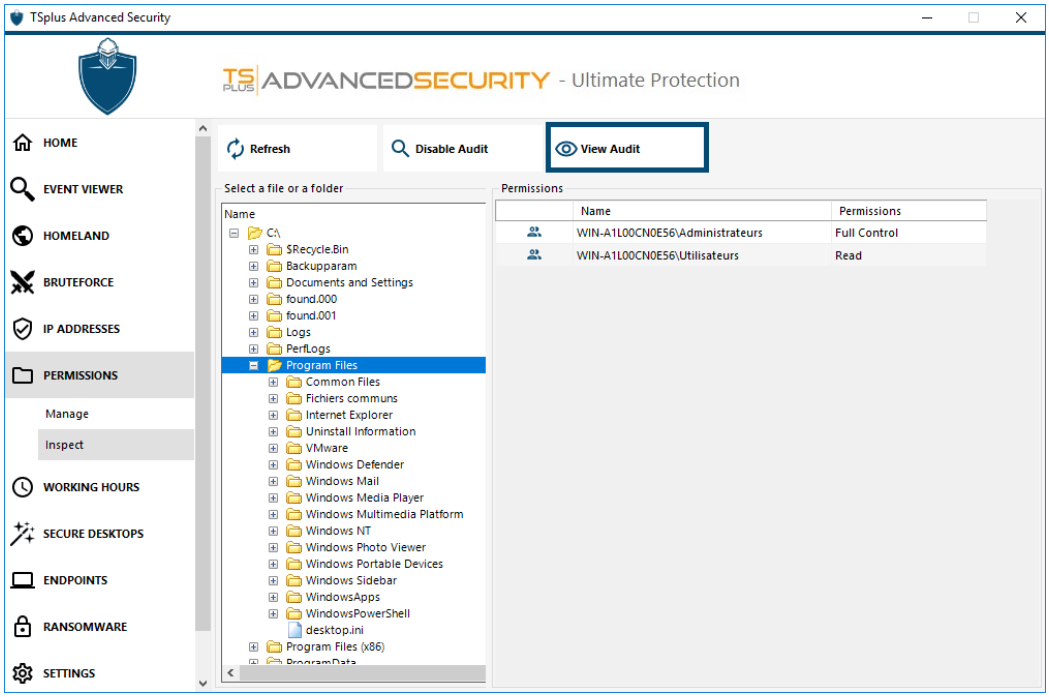


You can refresh the status of the folders for them to be updated in real-time.

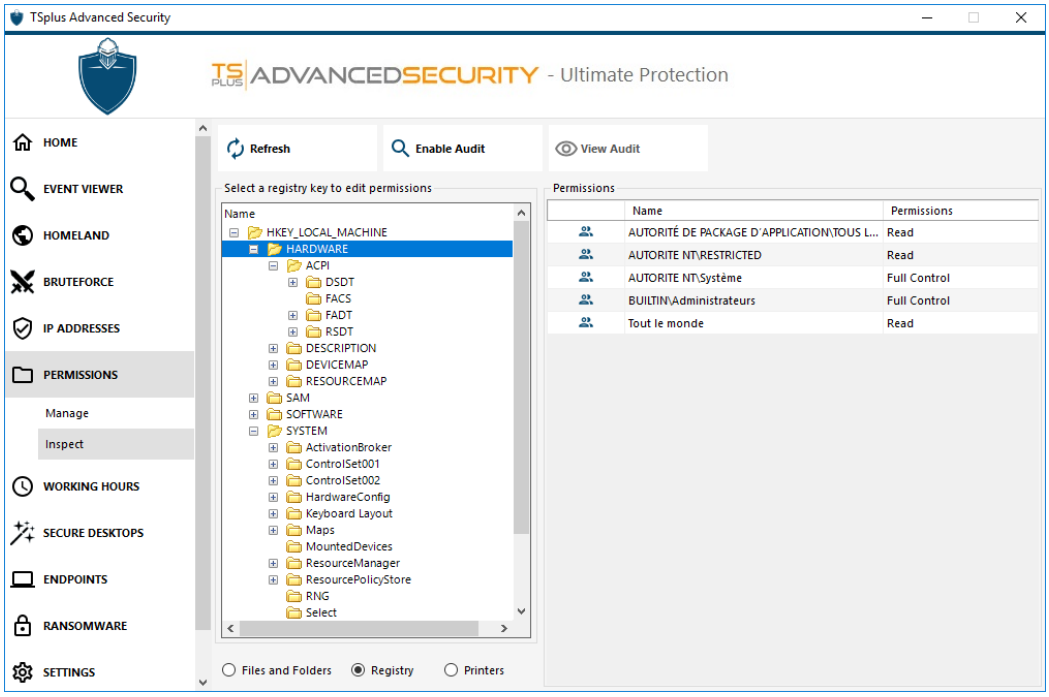
An Audit can be enabled by selecting the desired folder, subfolder or file and click on the "Enable Audit" button at the top:

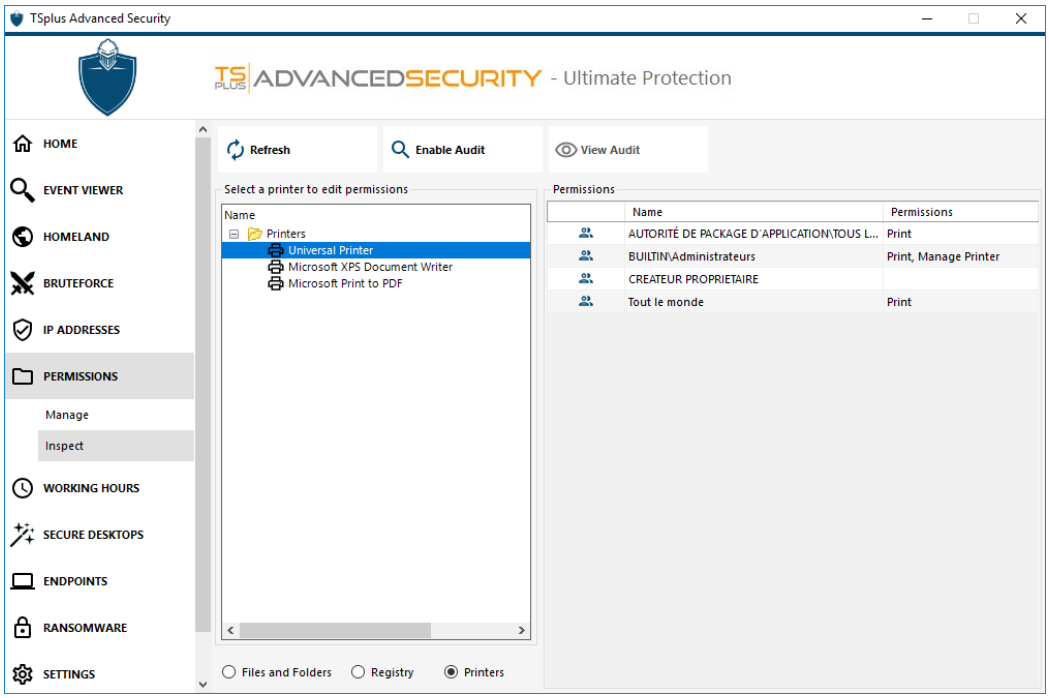


The "View Audit" button allows you to see the corresponding audit on the Event Viewer:



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


TSplus Advanced Security
ADVANCEDSECURITY - Ultimate Protection
HOME
EVENT VIEWER
HOMELAND
BRUTEFORCE
IP ADDRESSES
PERMISSIONS
Manage
Inspect
WORKING HOURS
SECURE DESKTOPS
ENDPOINTS
RANSOMWARE
SETTINGS
Refresh
Enable Audit
View Audit
Select a registry key to edit permissions
Name
HKEY_LOCAL_MACHINE
HARDWARE
ACPI
DSDT
FACS
FADT
RSDT
DESCRIPTION
DEVICEMAP
RESOURCEMAP
SAM
SOFTWARE
SYSTEM
ActivationBroker
ControlSet001
ControlSet002
HardwareConfig
Keyboard Layout
Maps
MountedDevices
ResourceManager
ResourcePolicyStore
RNG
Select
Files and Folders
Registry
Printers
Permissions
Name
Permissions
AUTORITÉ DE PACKAGE D'APPLICATION\TOUS L...
Read
AUTORITE NT\RESTRICTED
Read
AUTORITE NT\Système
Full Control
BUILTIN\Administrateurs
Full Control
Tout le monde
Read


TSplus Advanced Security
ADVANCEDSECURITY - Ultimate Protection
HOME
EVENT VIEWER
HOMELAND
BRUTEFORCE
IP ADDRESSES
PERMISSIONS
Manage
Inspect
WORKING HOURS
SECURE DESKTOPS
ENDPOINTS
RANSOMWARE
SETTINGS
Refresh
Enable Audit
View Audit
Select a printer to edit permissions
Name
Printers
Universal Printer
Microsoft XPS Document Writer
Microsoft Print to PDF
Files and Folders
Registry
Printers
Permissions
Name
Permissions
AUTORITÉ DE PACKAGE D'APPLICATION\TOUS L...
Print
BUILTIN\Administrateurs
Print, Manage Printer
CREATEUR PROPRIETAIRE
Tout le monde
Print

Working Hours Restriction

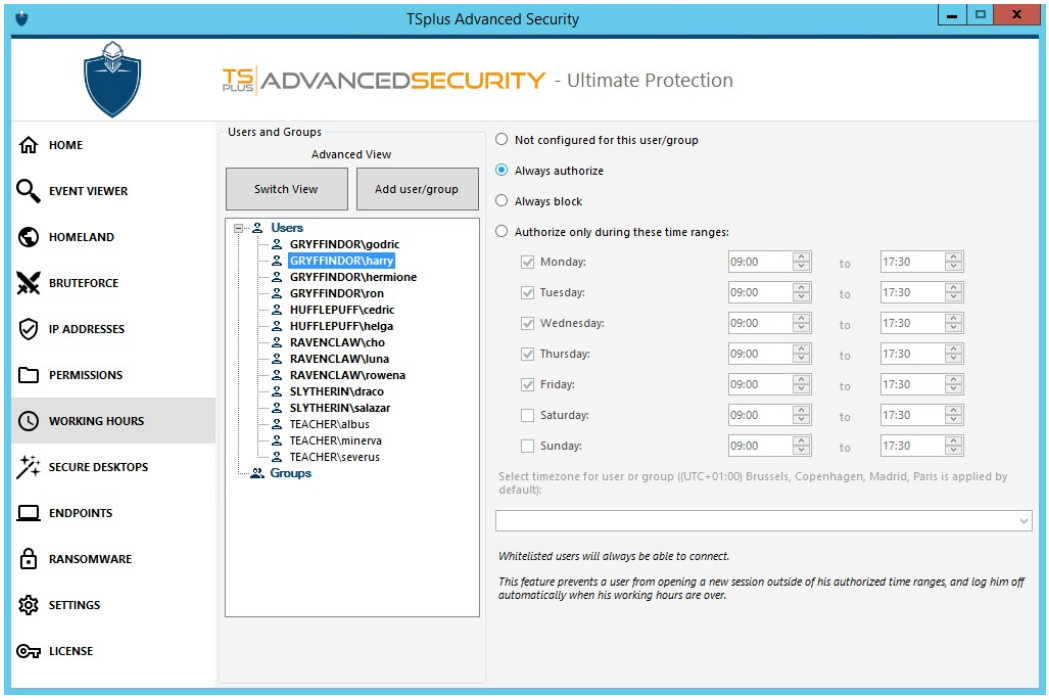
You can configure working hours restrictions per user or per group.

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:

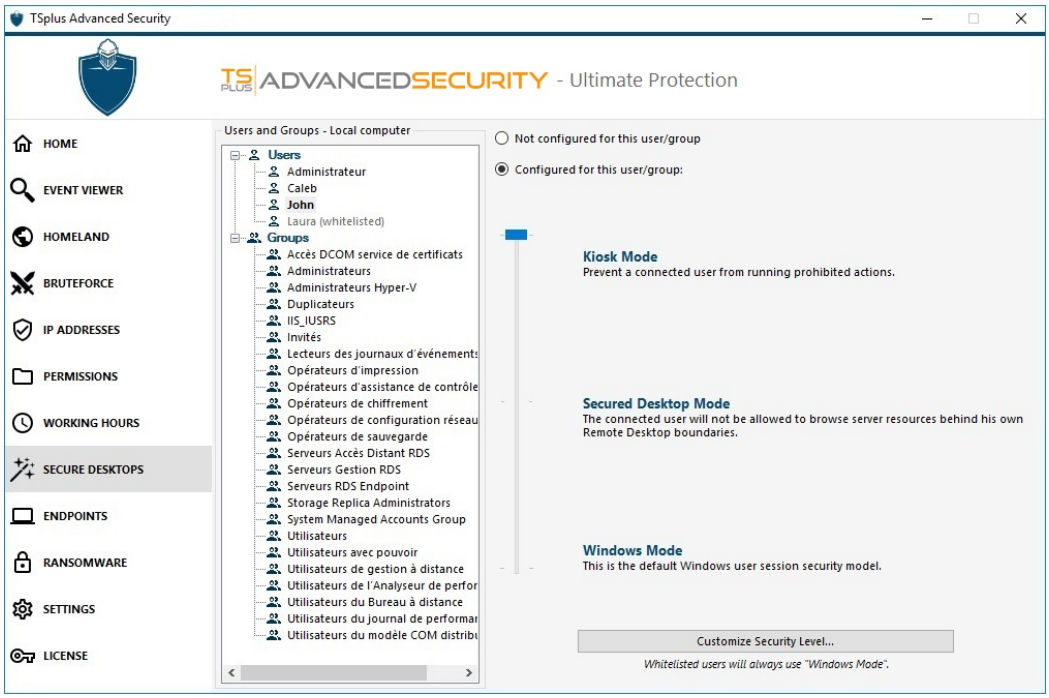
1) if this user has Working Hours Restrictions directly defined for himself, then these rules are enforced.
2) if this user does not have Working Hours Restrictions directly defined for himself, then TSplus Advanced Security will load any existing Working Hours Restrictions for all the groups of this 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.

Secure Desktop

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

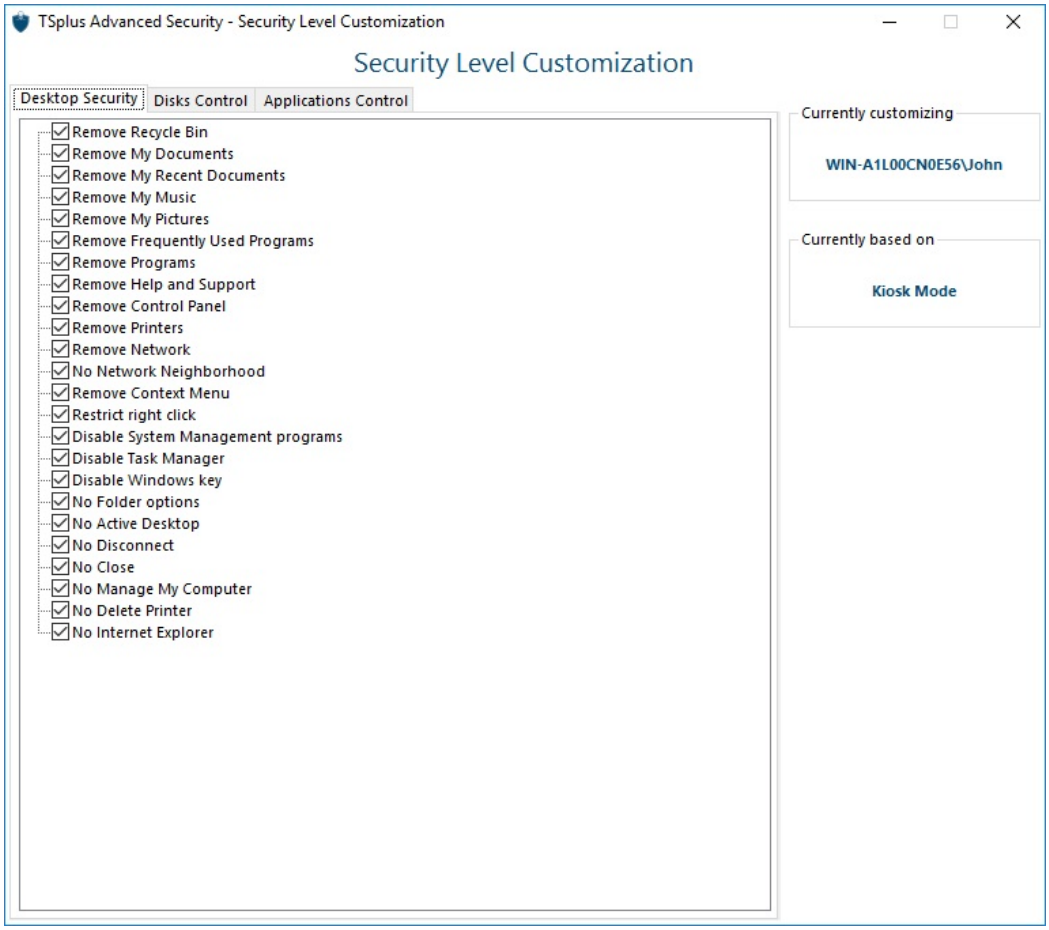
- The **Windows Mode**, where the user has access to a default Windows session.
- The **Secured Desktop Mode**, where the user has no access to the Control Panel, programs, disks, browser, no right-click...: no access to the server resources. He just has access to documents, printers, Windows key and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



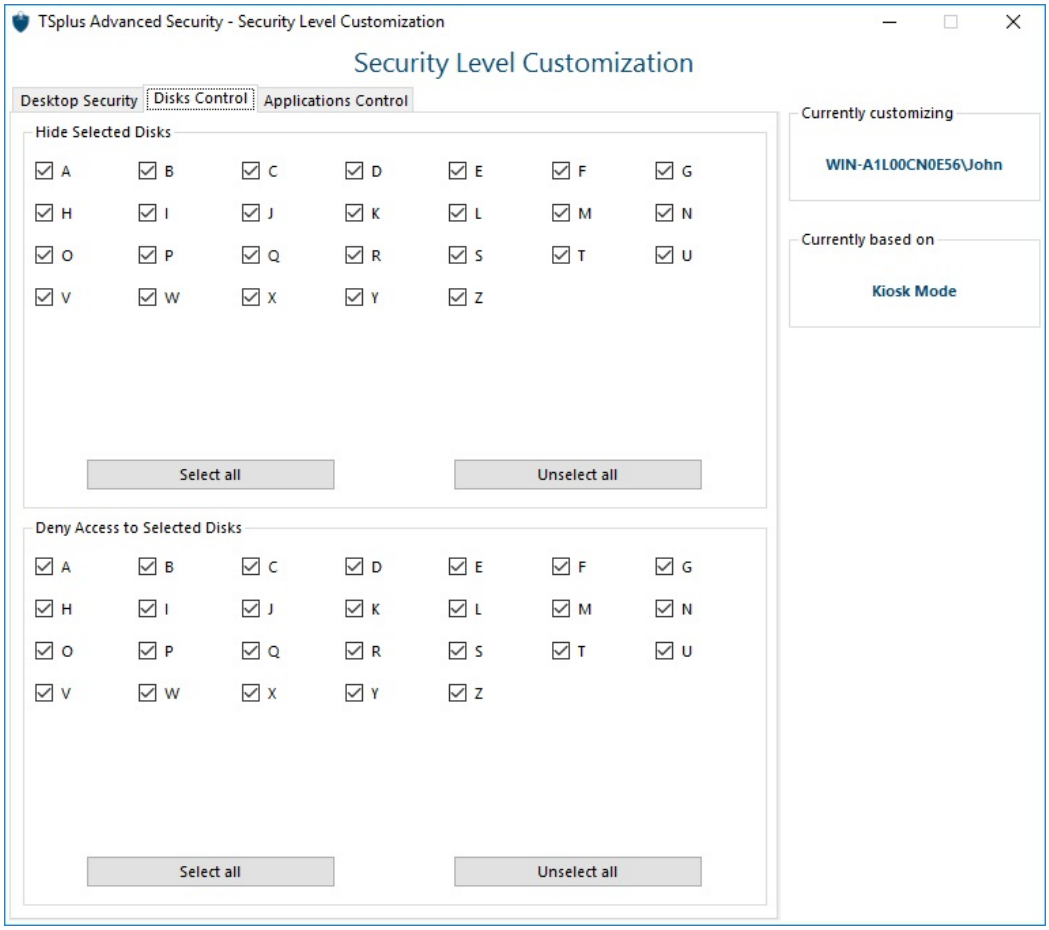
Customization

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

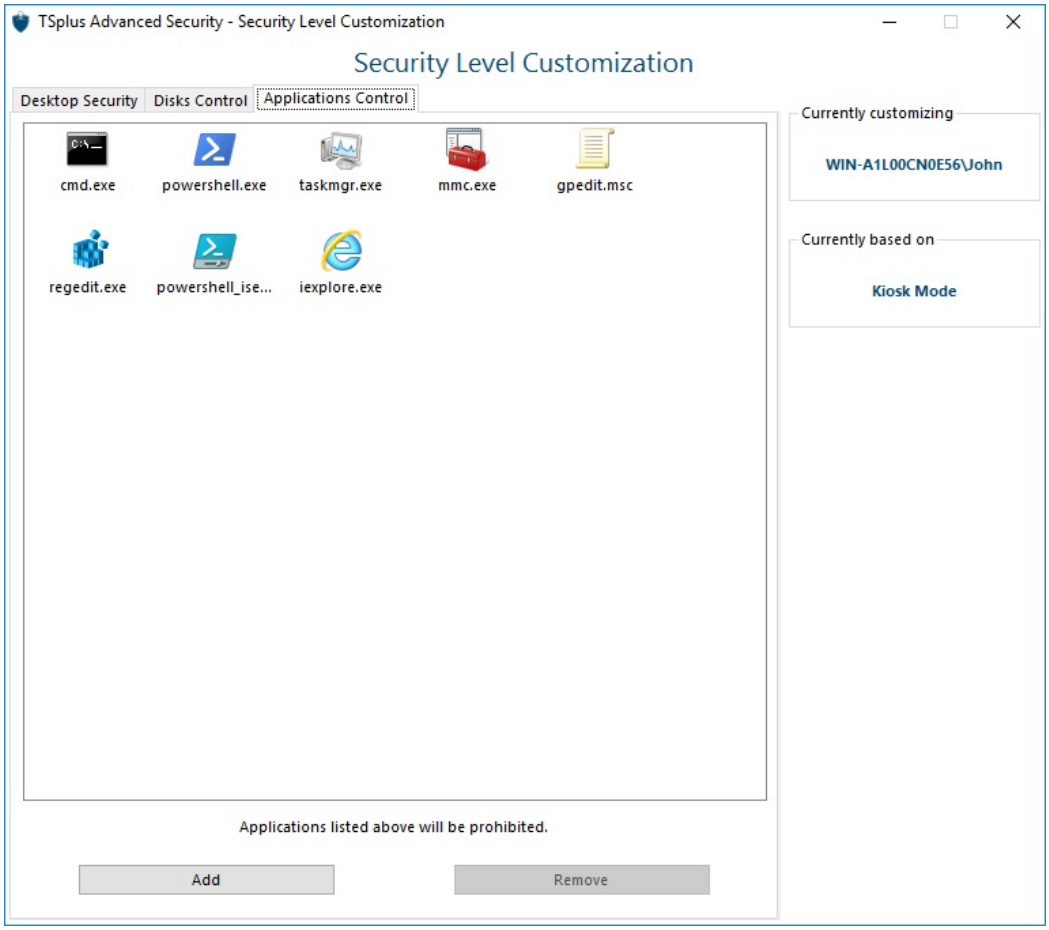
Desktop Security:



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.

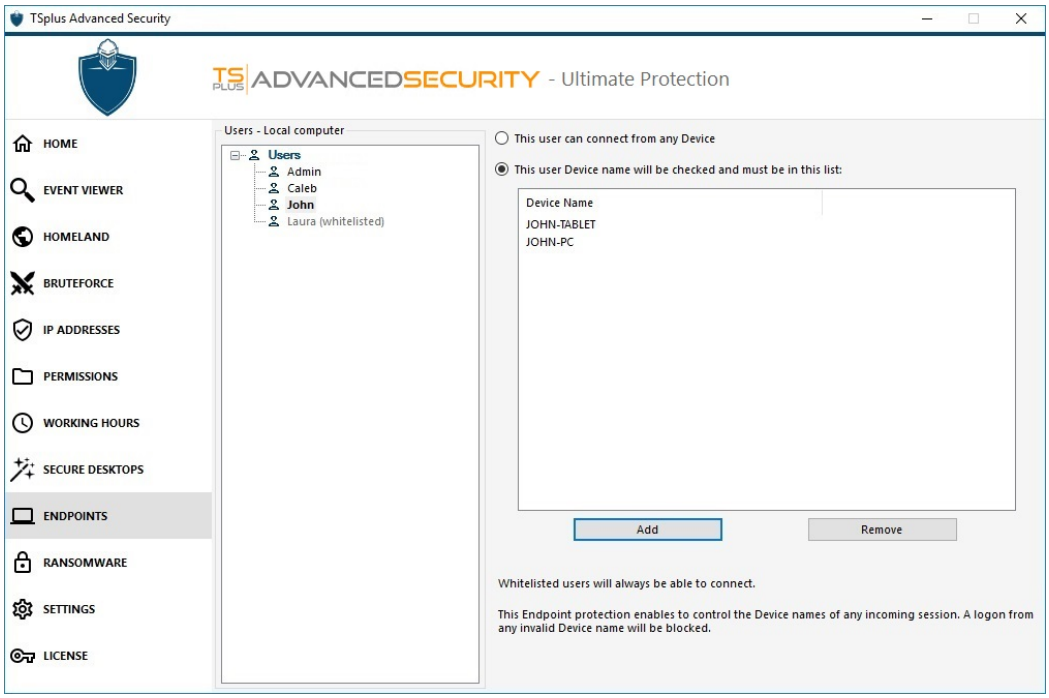
For instance if a first group has a rule to remove the Recycle Bin icon from the desktop, but this rule is disabled for a second group, then the user will have the Recycle Bin icon on his desktop. The same priority rules will apply on every custom rule (Desktop Security, Disks Control and Applications 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

Endpoint Protection and Device Control

The endpoint protection and device control 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, John will be using the device names John-PC and John-Tablet.

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 the Endpoint Protection and Device Control 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: Endpoint Protection is not compatible with HTML5 connections.

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

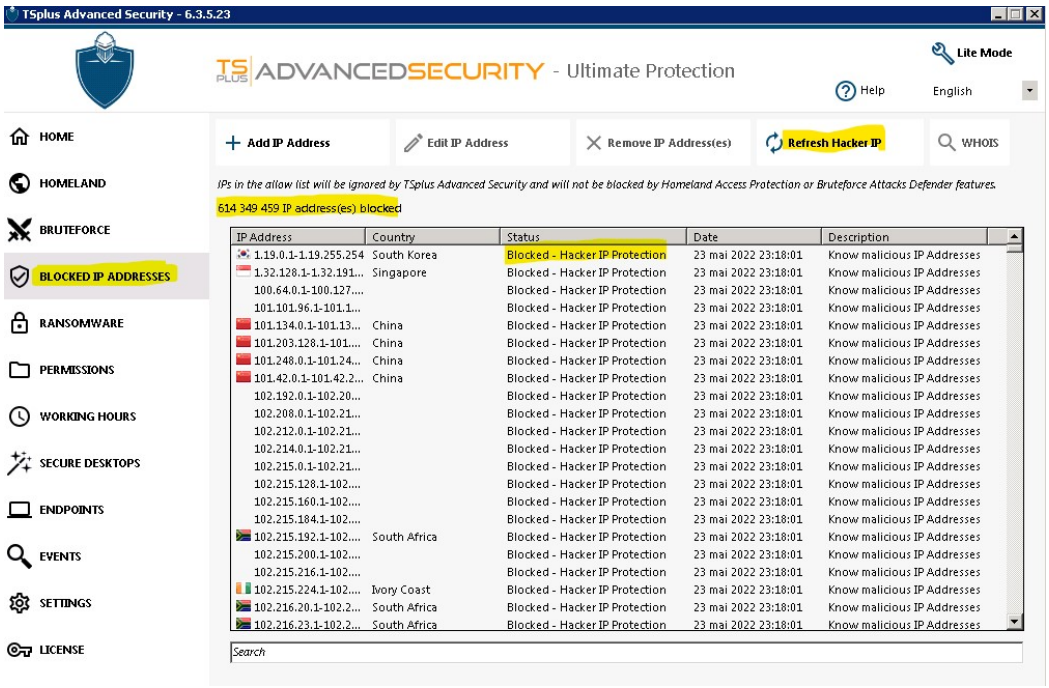
Support and Updates Services subscription is required.

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.

An event is displayed each time the Hacker IP lists has been synchronized:

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



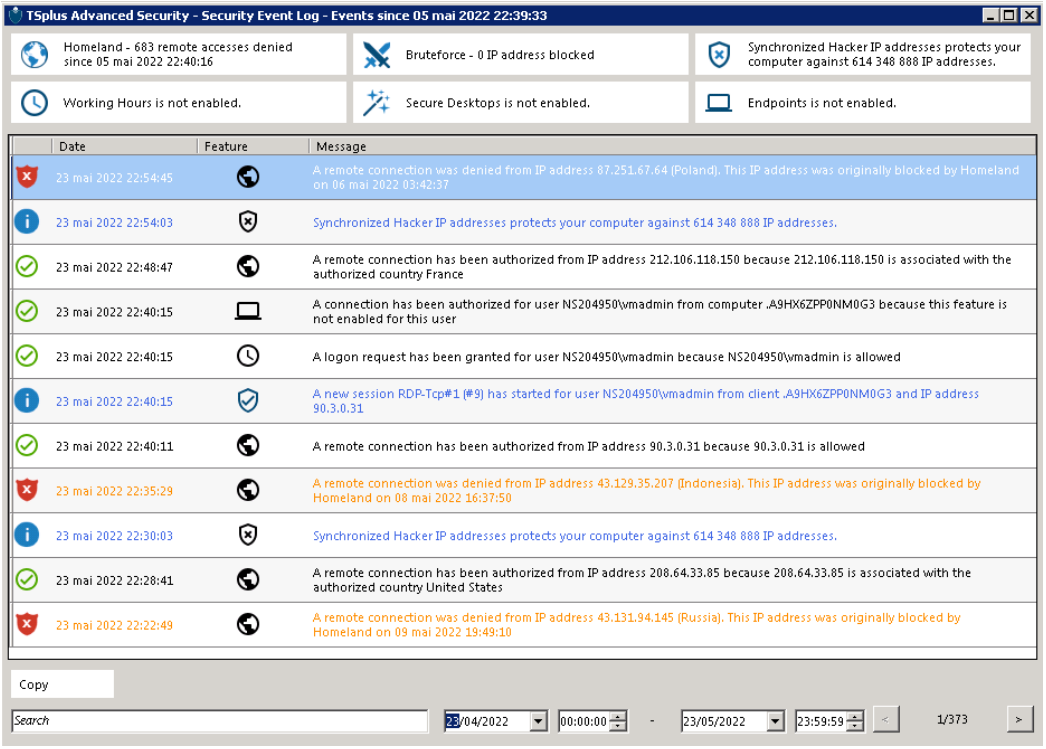
As a result, the feature should create approx. 600 000 000 bloxking firewall rules in Windows Firewall.

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 Events 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.



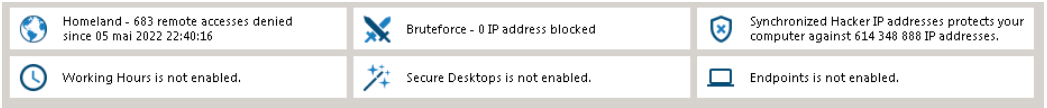
The example above ilustrates real life denied connection attempts blocked by TSplus Advanced Security.

The description of the event often explains why the action was performed or not. As illustrated, 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.

Following feature status at a glance

The 6 tiles at the top of the window displays a status for each corresponding TSplus Advanced Security features.



In the example above, **Homeland Protection** status shows 673 blocked connections since May 2022. Also, the example warns that the **Endpoint Protection** feature is not enabled. The status are displayed according to the security events recorded. The window title highlights the oldest security events.

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.

Interacting with events

Finally, it is also possible to act on the event by clicking on a button located in the bottom menu, or right-clicking on the desired event:

- Copy the event message
- Copy the IP Address
- Unblock the IP address
- Unblock and add to IP addresses allow list

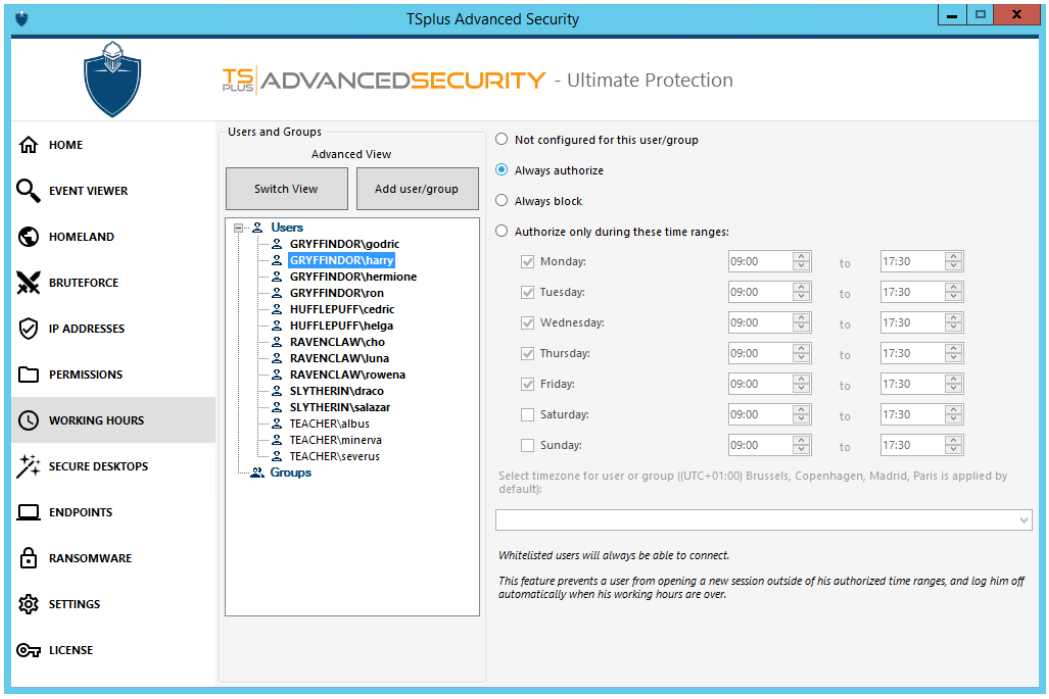
Settings - Users Allow List

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:

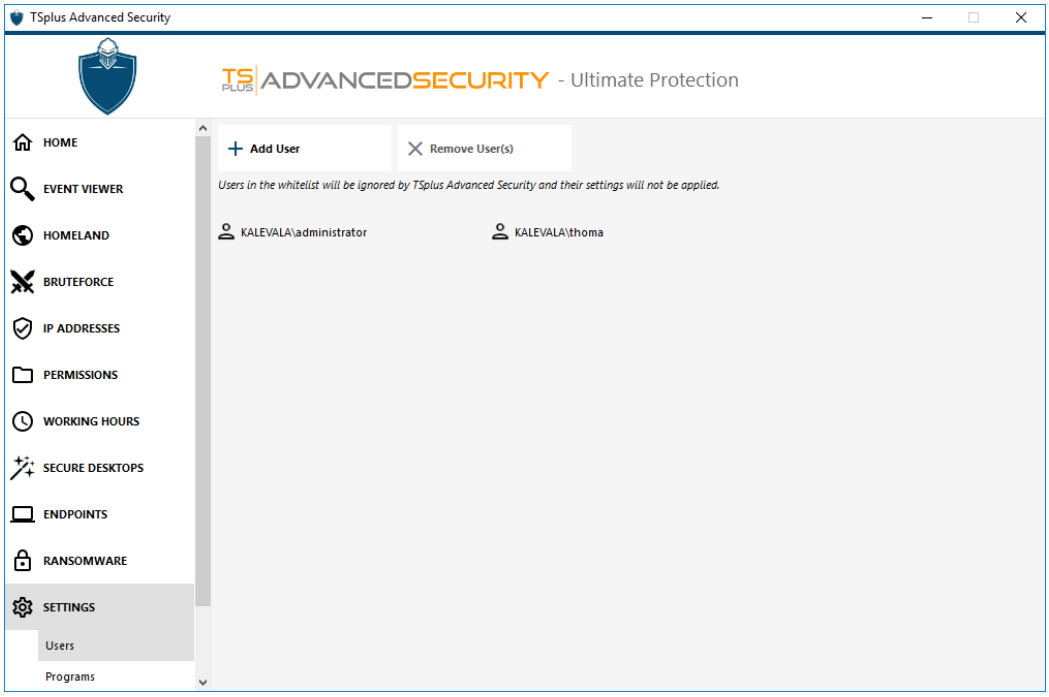


Users Whitelist

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

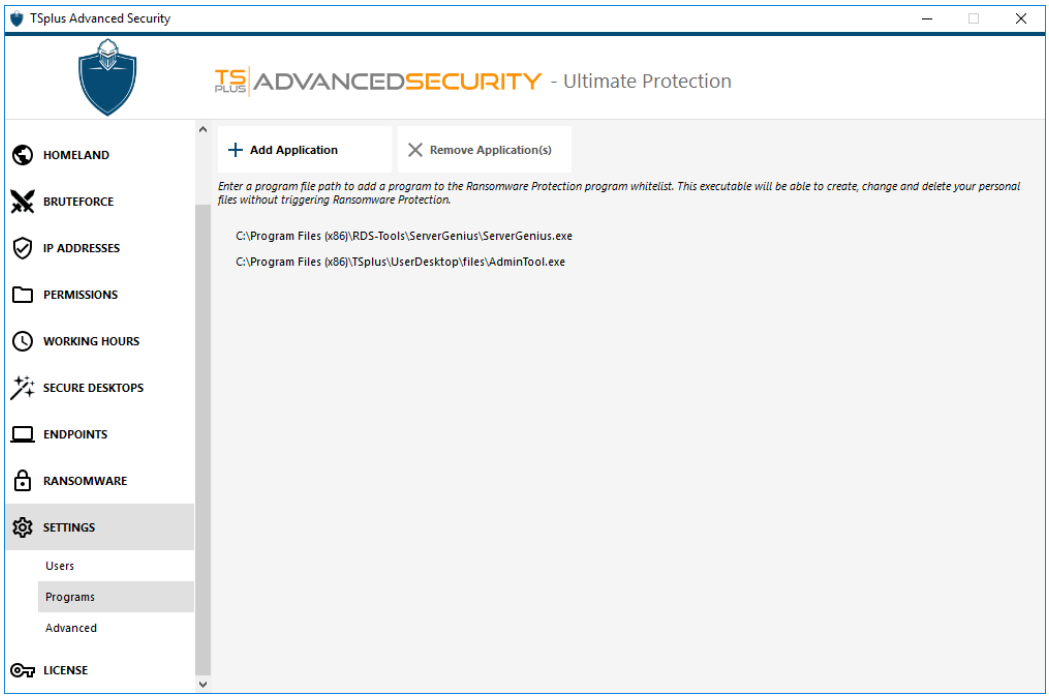
Users on the whitelist are ignored by TSplus Advanced Security and their settings will not be applied.

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


TSplus Advanced Security
ADVANCEDSECURITY - Ultimate Protection
HOME
EVENT VIEWER
HOMELAND
BRUTEFORCE
IP ADDRESSES
PERMISSIONS
WORKING HOURS
SECURE DESKTOPS
ENDPOINTS
RANSOMWARE
SETTINGS
Users
Programs
Add User
Remove User(s)
Users in the whitelist will be ignored by TSplus Advanced Security and their settings will not be applied.
KALEVALA\administrator
KALEVALA\thoma

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 Ransomware Protection*. By default, all Microsoft programs are whitelisted.

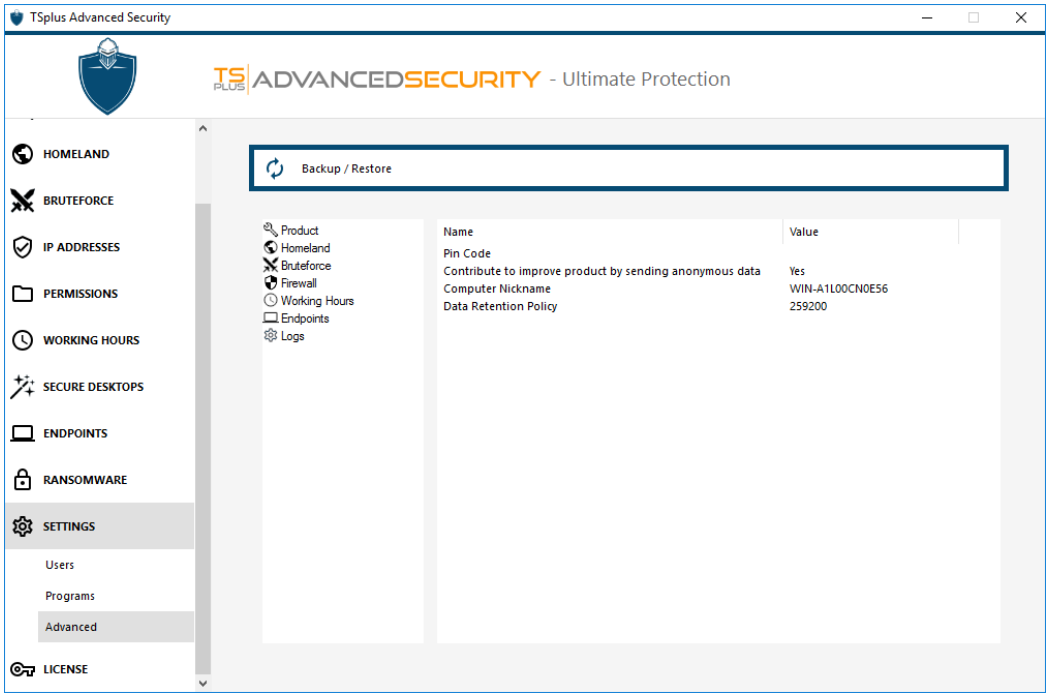


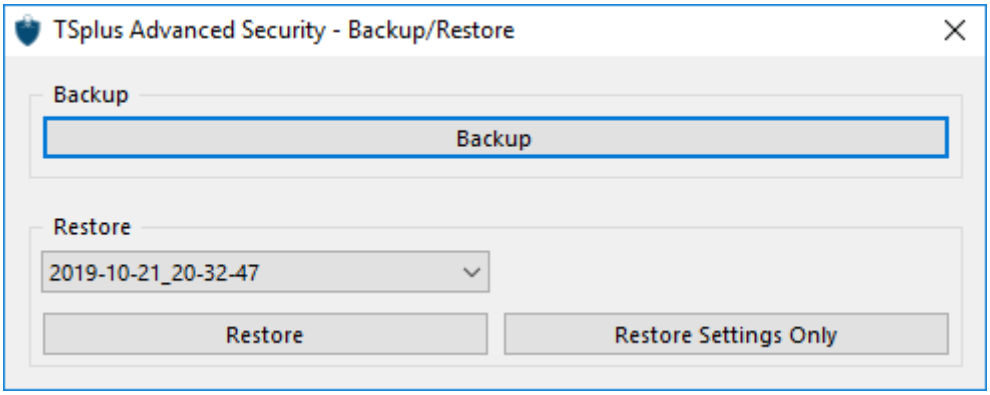
Click on the "Add Application" button to add a program. You can also remove them by selecting application(s) and clicking on the Remove Application(s) button.

Advanced - Backup and Restore Data and Settings

Backup and Restore Data and Settings

You can Backup or Restore advanced-security data and settings by clicking on the button "Backup / Restore" on the top:





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 *HKEYLOCALMACHINE\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 *HKEYLOCAL 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.

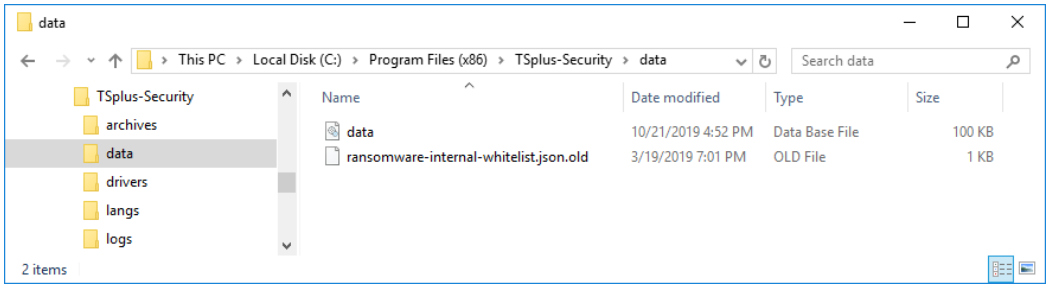
5. Please wait at most 2 minutes for the settings to be reloaded by advanced-security features.

Database

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

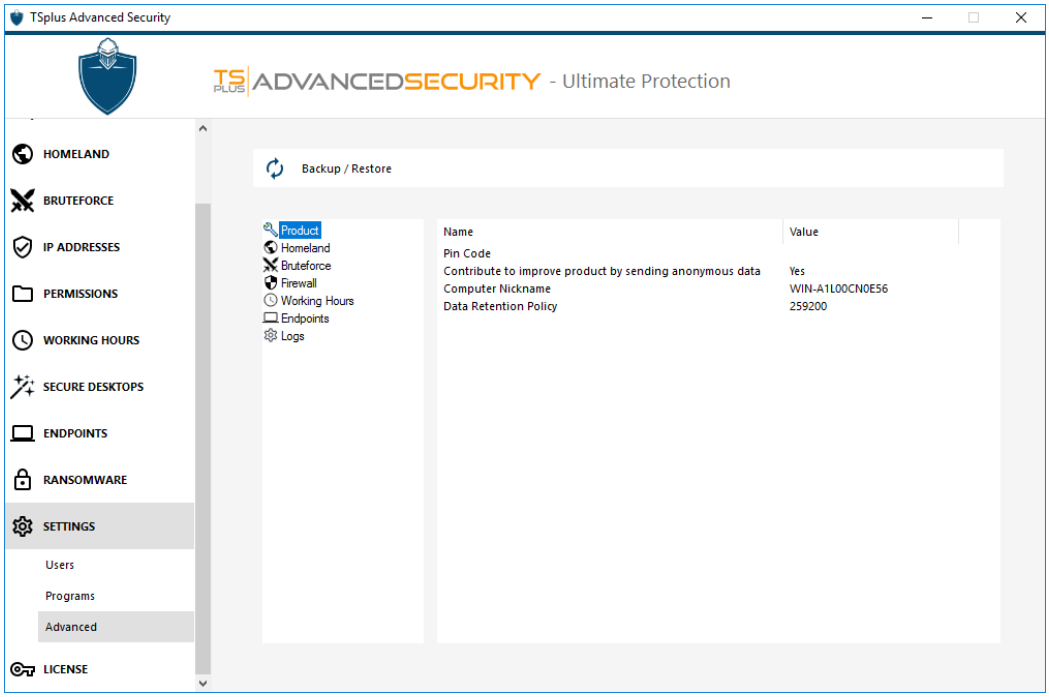
This database is stored in .\data directory.

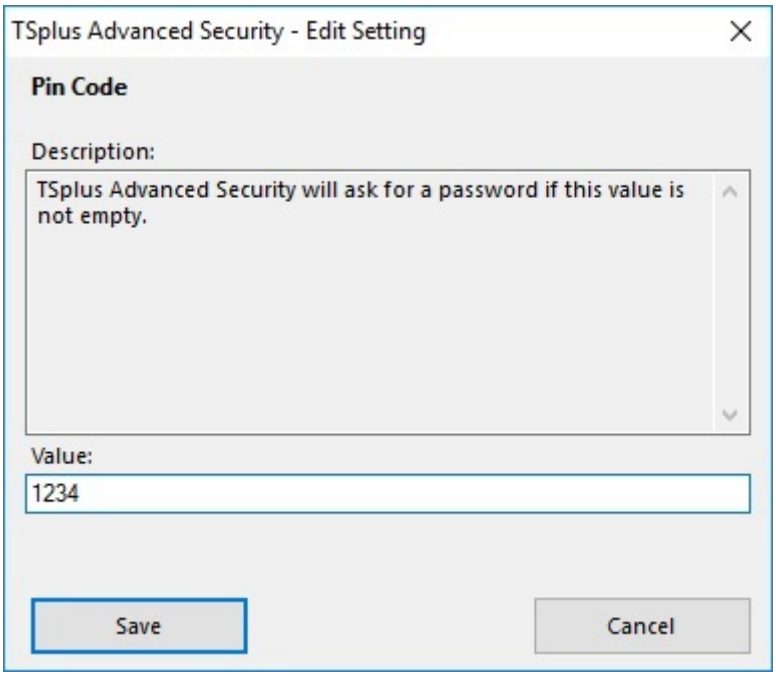
- Advanced Security from version 5 and prior to version 5.3.10.6 uses a LiteDB database engine.
- Advanced Security above version 5.3.10.6 uses a SQLite database engine.



Advanced - Product Settings

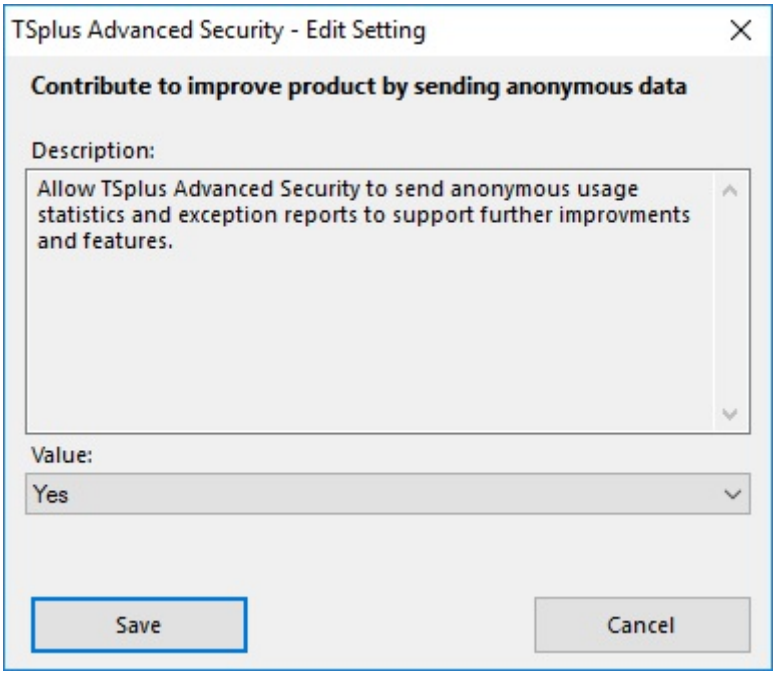
The **Product tab** allows you to *add a PIN code to the Administration Tool*:





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

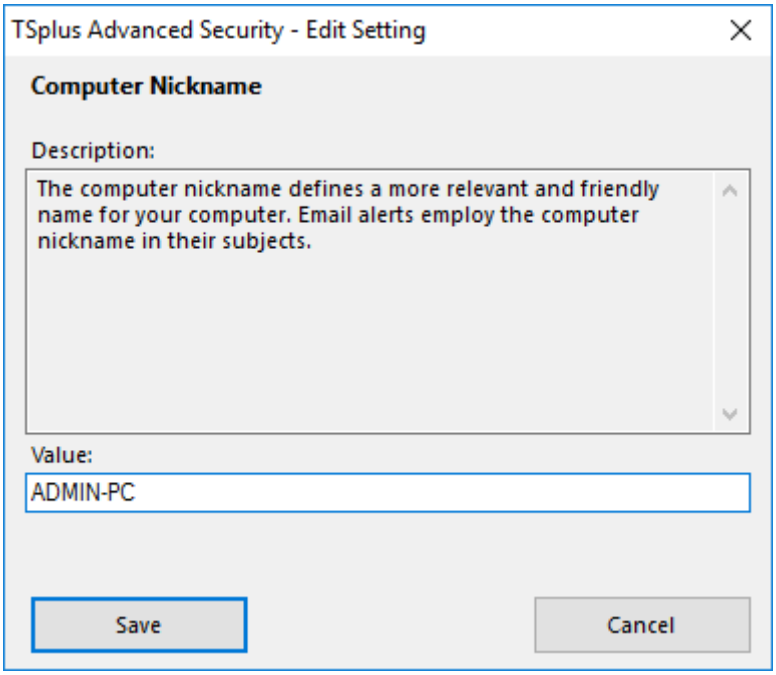
You can also **contribute to improve the product**, by sending anonymous data (enabled by default):



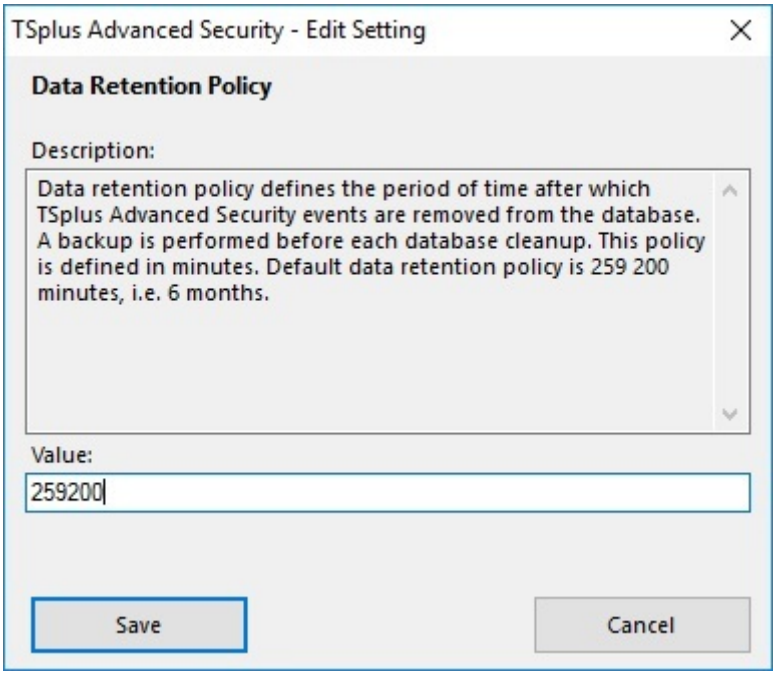
The following data will be collected in case of a Ransomware attack:

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

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

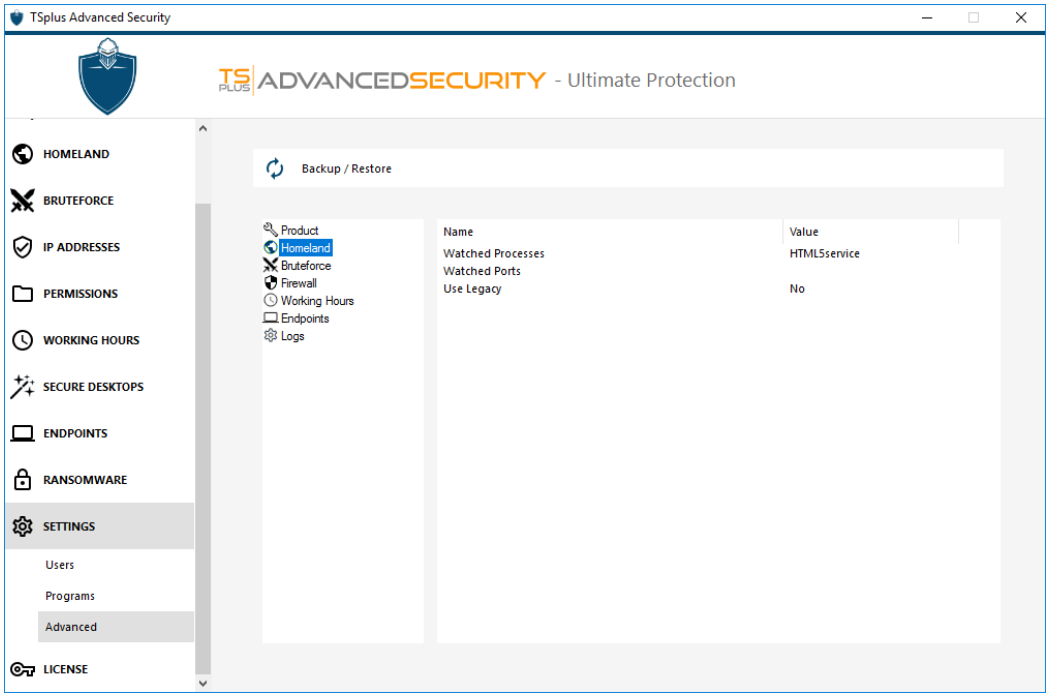


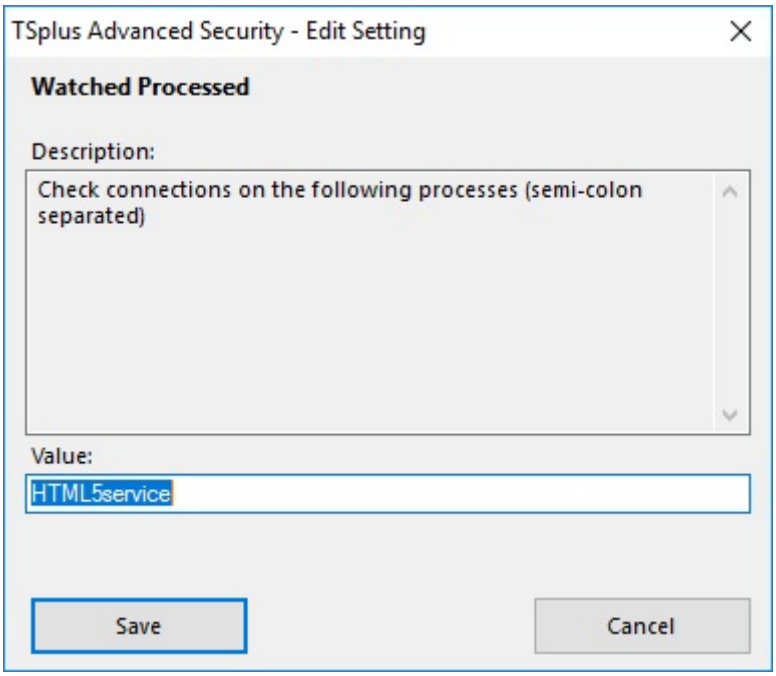
The **Data Retention Policy** defines the period of time after which TSplus Advanced Security events are removed from the database. A backup is performed before each database cleanup. This policy is defined in minutes.
Default data retention policy is 259 200 minutes, i.e. 6 months.


TSplus Advanced Security - Edit Setting
Data Retention Policy
Description:
Data retention policy defines the period of time after which TSplus Advanced Security 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, i.e. 6 months.
Value:
259200
Save
Cancel

Advanced - Homeland Settings

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

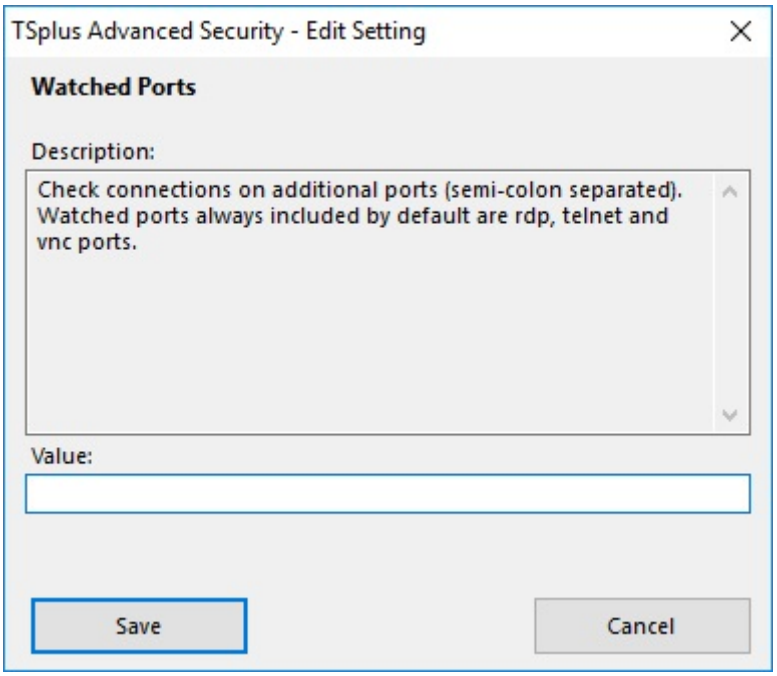




By default, the HTML5 service is watched.

The **Watched Ports** settings allows you to add ports watched by the *Homeland Protection Feature*. By default, Homeland Access Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC. Homeland supports the following VNC providers: Tight VNC, Ultra VNC, Tiger VNC

and Real VNC, which are not related whatsoever with TSplus.

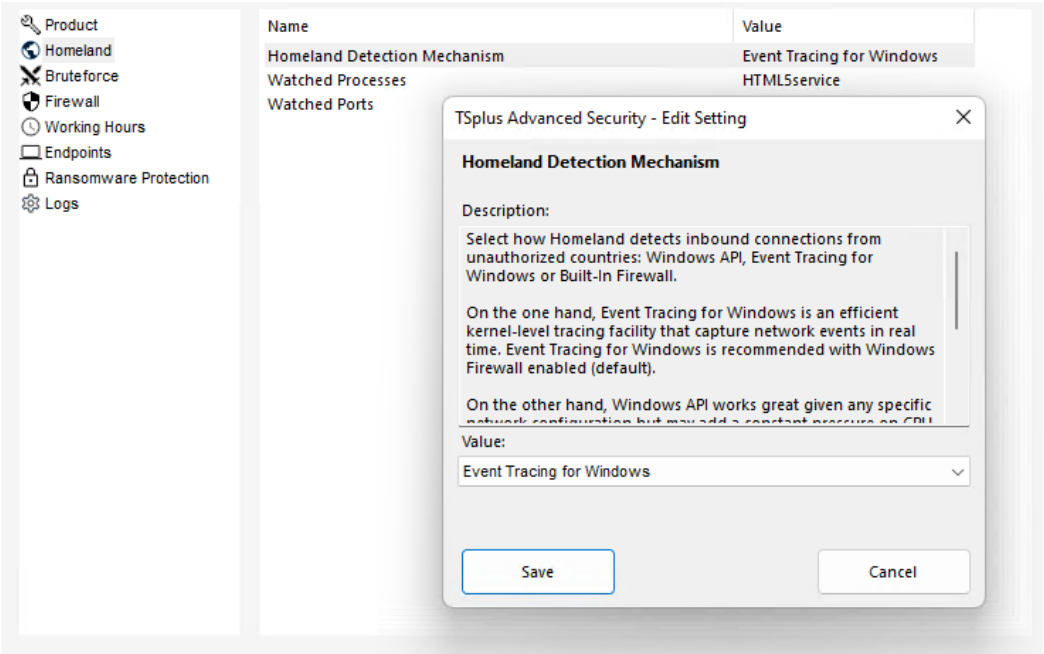


The **Homeland Detection Mechanism** setting defines how Homeland detects inbound connections from unauthorized countries, using one of the three differents detection mechanisms: - Windows API - Event Tracing for Windows - Built-In Firewall

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).

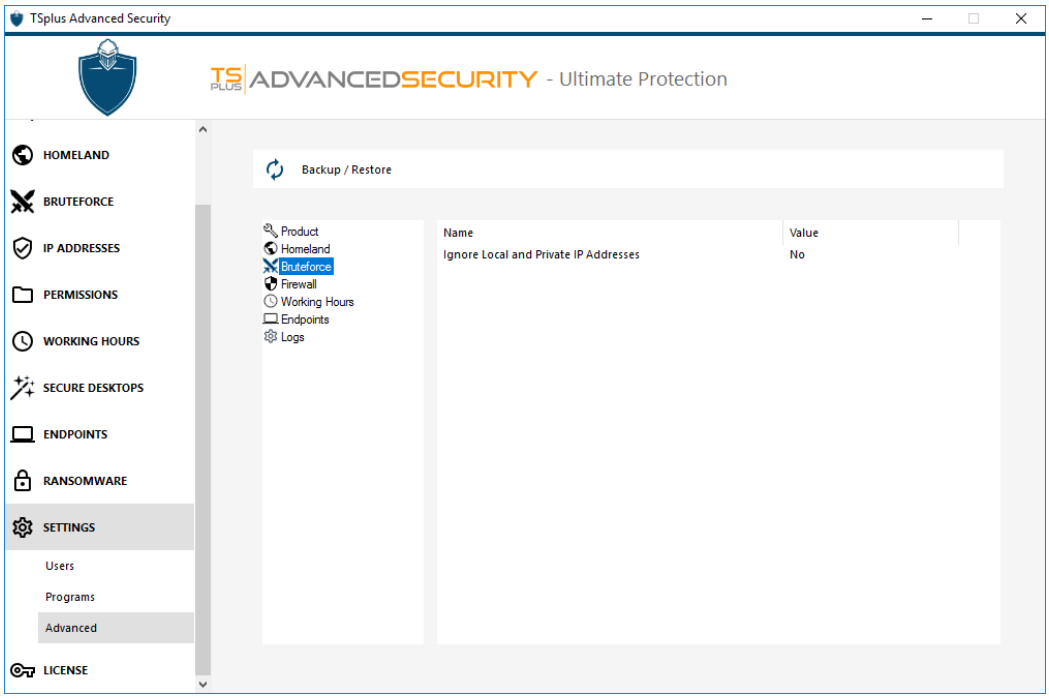
On the other hand, Windows API works great given any specific network configuration but may add a constant pressure on CPU depending on the amount of active connections. Please note that Windows API is not compatible with IPv6 yet.

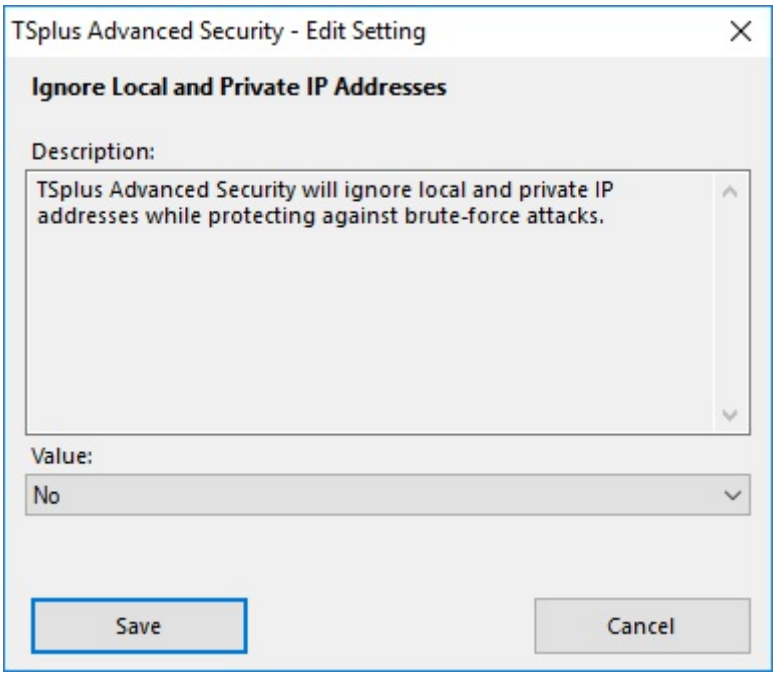
Built-In Firewall enables user-mode capturing and dropping of network packets sent to the Windows network stack. When the Built-In Firewall is configured to block unwanted connections, it is recommended to use it to enforce Homeland's allowed countries.


Product
Homeland
Bruteforce
Firewall
Working Hours
Endpoints
Ransomware Protection
Logs
Name
Value
Homeland Detection Mechanism
Event Tracing for Windows
Watched Processes
HTML5service
Watched Ports
TSplus Advanced Security - Edit Setting
Homeland Detection Mechanism
Description:
Select how Homeland detects inbound connections from unauthorized countries: Windows API, Event Tracing for Windows or 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
Value:
Event Tracing for Windows
Save
Cancel

Advanced - Bruteforce Settings

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





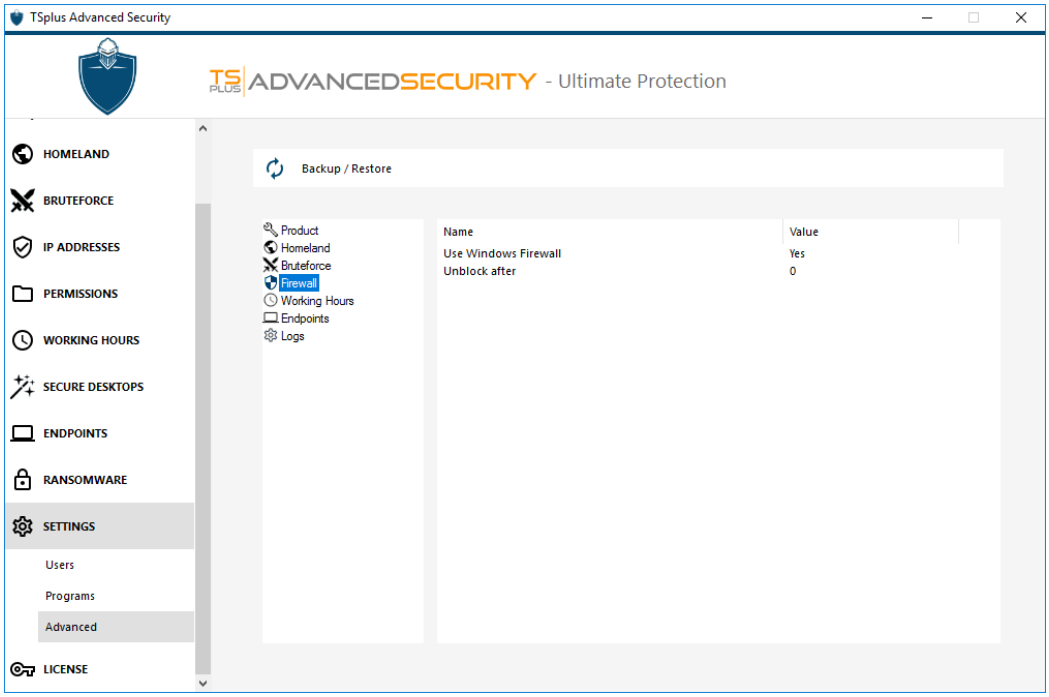
Advanced - Firewall Settings

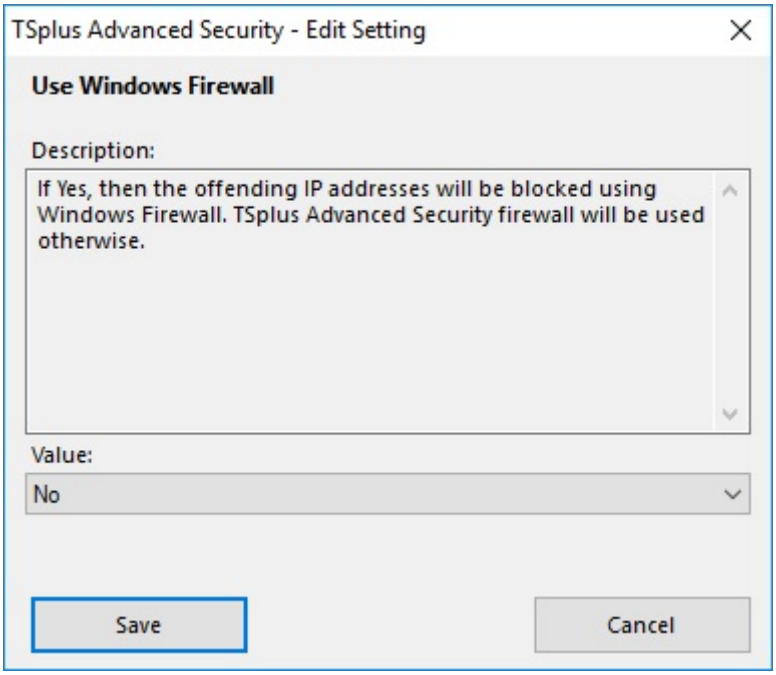
The **Firewall tab** allows you to activate the **Windows Firewall or deactivate it in favor of the TSplus Advanced Security built-in firewall**.

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

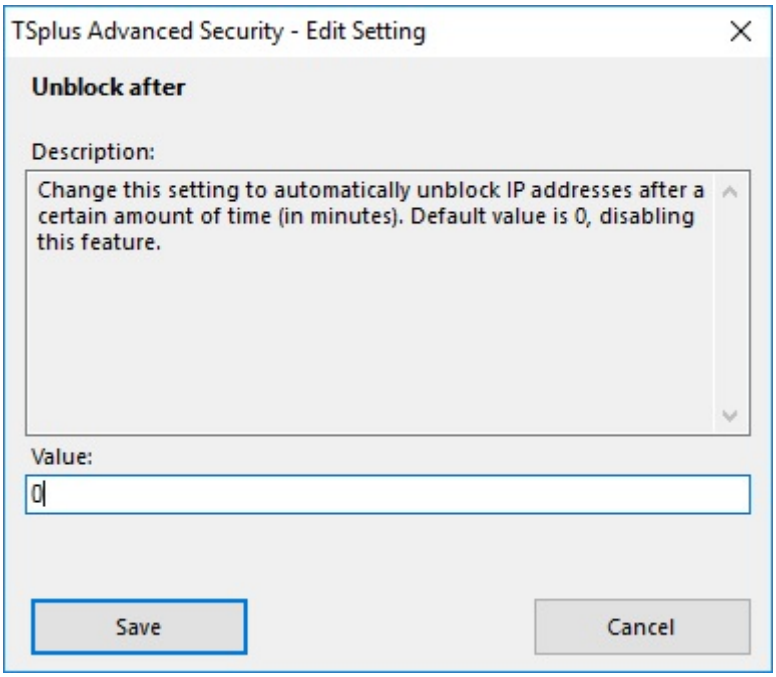
As a general guidance, if Windows Firewall is activated on your server, then you should use it to enforce TSplus Advanced Security rules (default). If you installed another firewall, then you must activate TSplus Advanced Security built-in firewall.

In order to activate the built-in firewall, go to **Settings** > **Advanced** > **Product** > **Use Windows Firewall** and set the value to No:

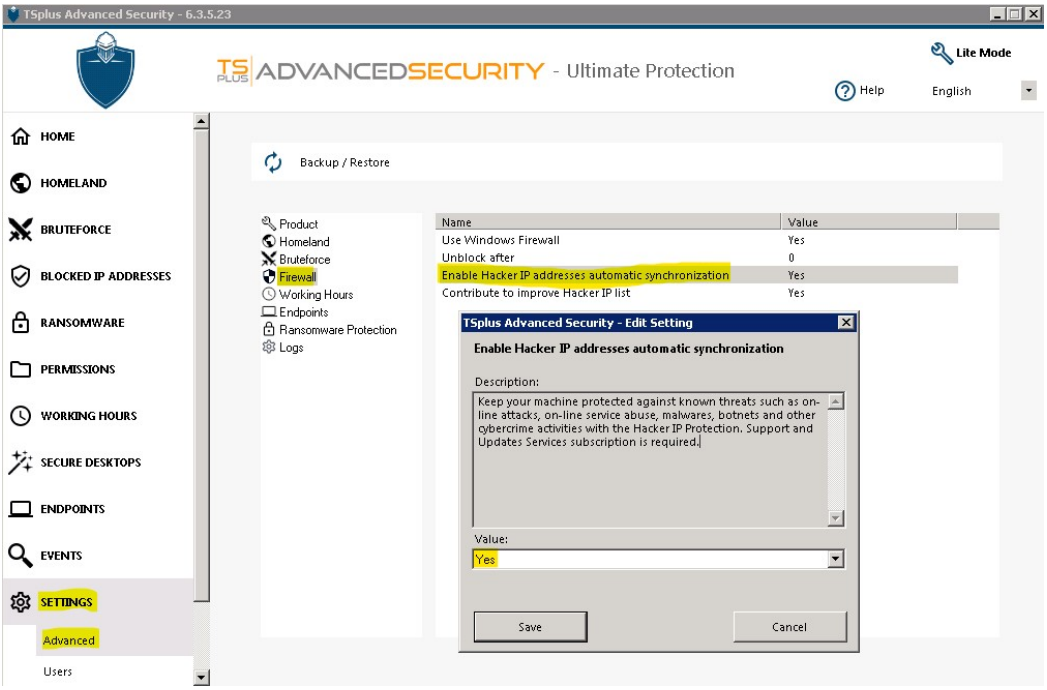




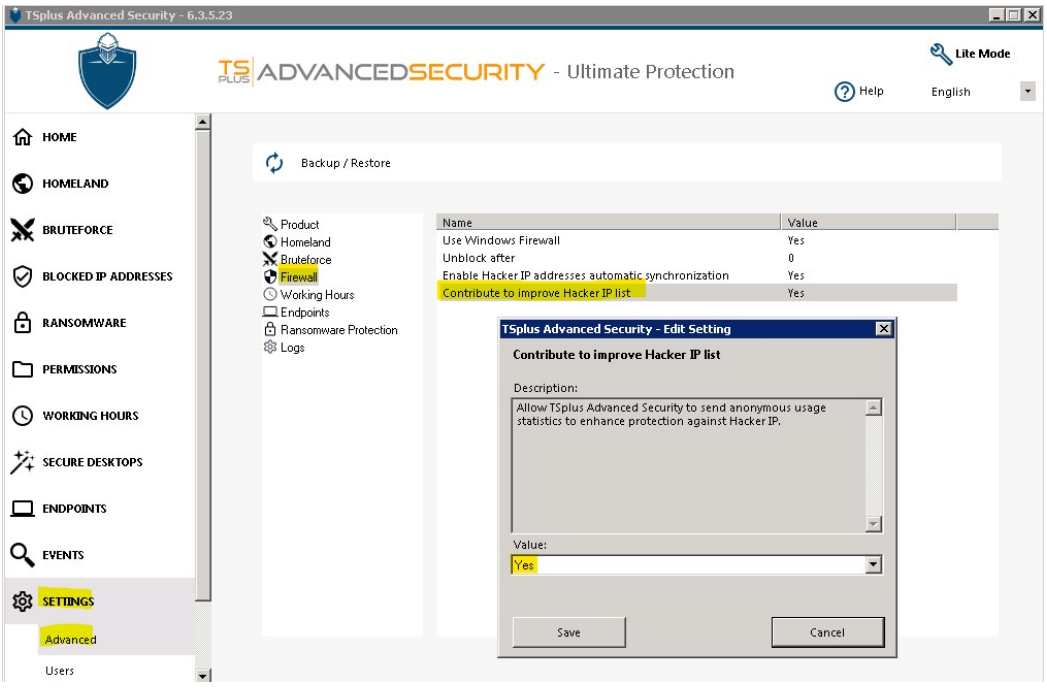
The **Unblock after** setting allows you to automatically unblock IP addresses after a certain amount of time (in minutes). Default value is 0, disabling this feature:



The **Enable Hacker IP addresses automatic synchronization** setting keeps your machine protected by allowing Advanced Security to daily fetch an updated version of the Hacker IP list and update the firewall rules created by Hacker IP Protection. You can prevent automatic synchronization by setting its value to "No". Default value is "yes".

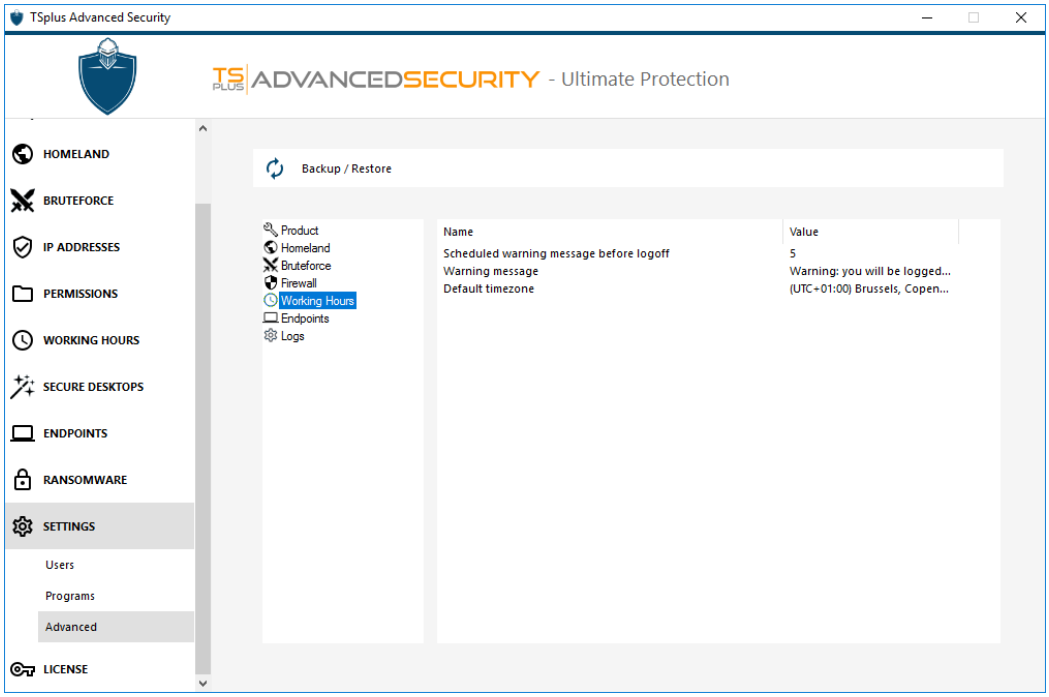


The **Contribute to improve Hacker IP list** setting allows TSplus Advanced Security to send anonymous usage statistics to enhance protection against Hacker IP. You can prevent sending anonymous usage data by setting its value to "No". Default value is "yes".

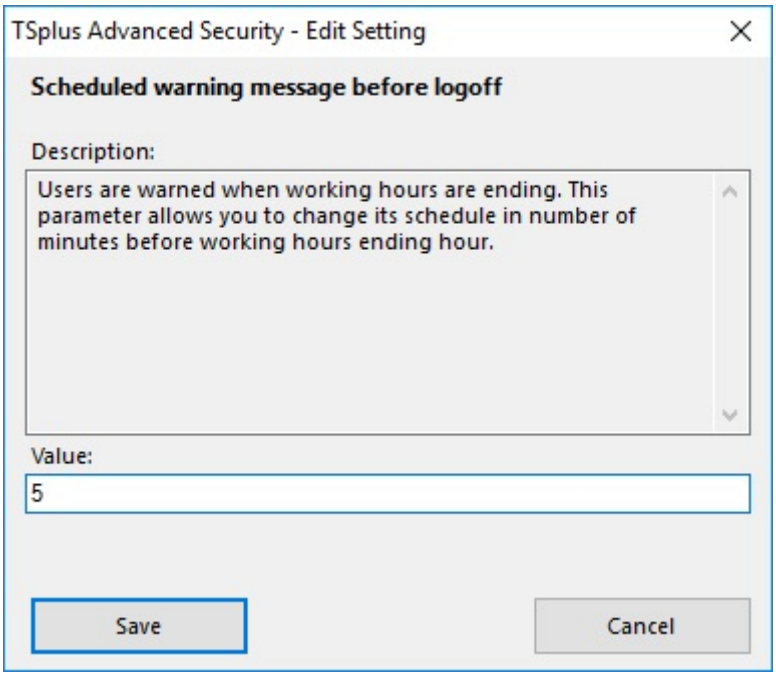


Advanced - Working Hours Settings

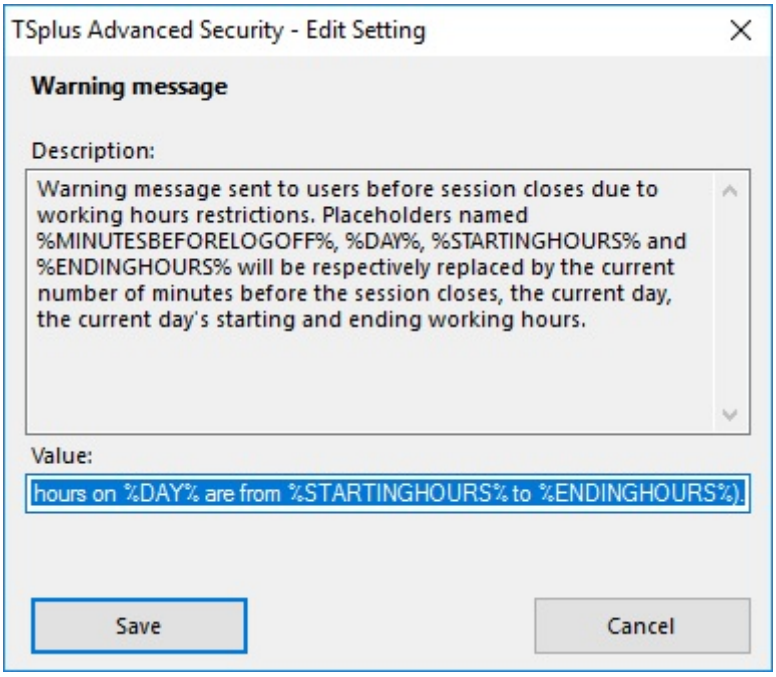
The **Working Hours tab** allows you to *schedule and modify a warning message before the user is logged off*.



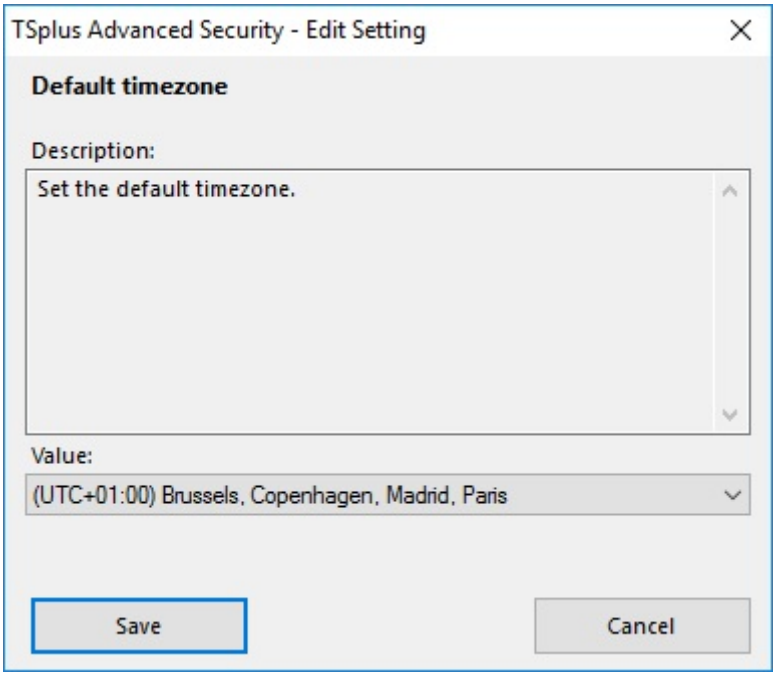
You can configure the warning message schedule in number of minutes before the user is automatically disconnected. By default, it is set to 5 minutes.



Modify the Warning message 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.

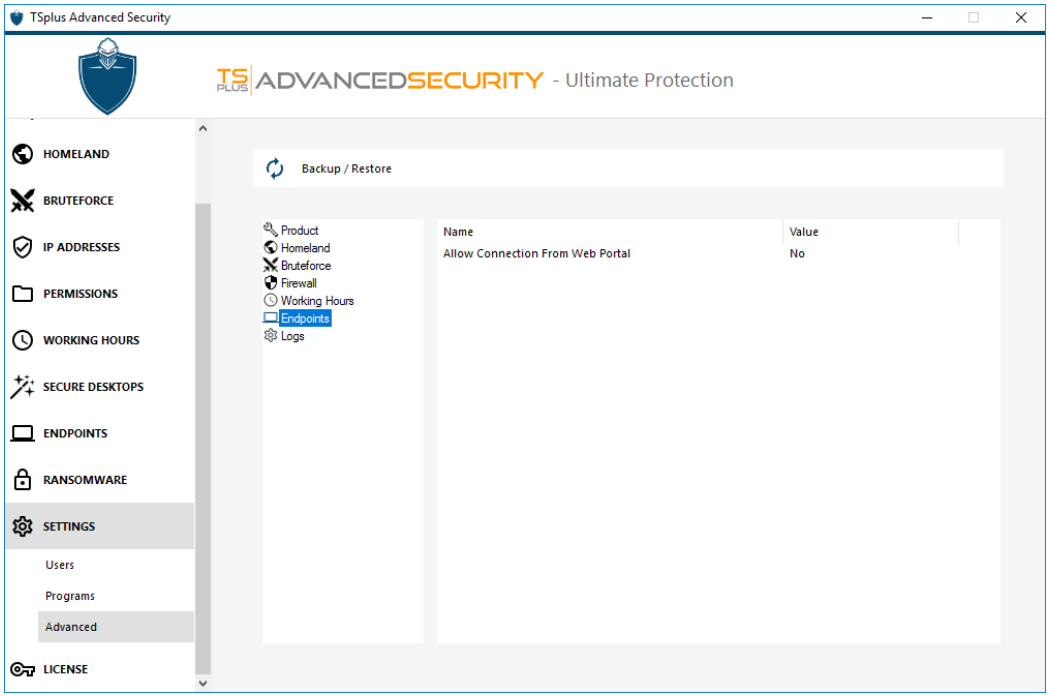


Set the **Default server timezone** by selecting the corresponding one on the drop-down list:

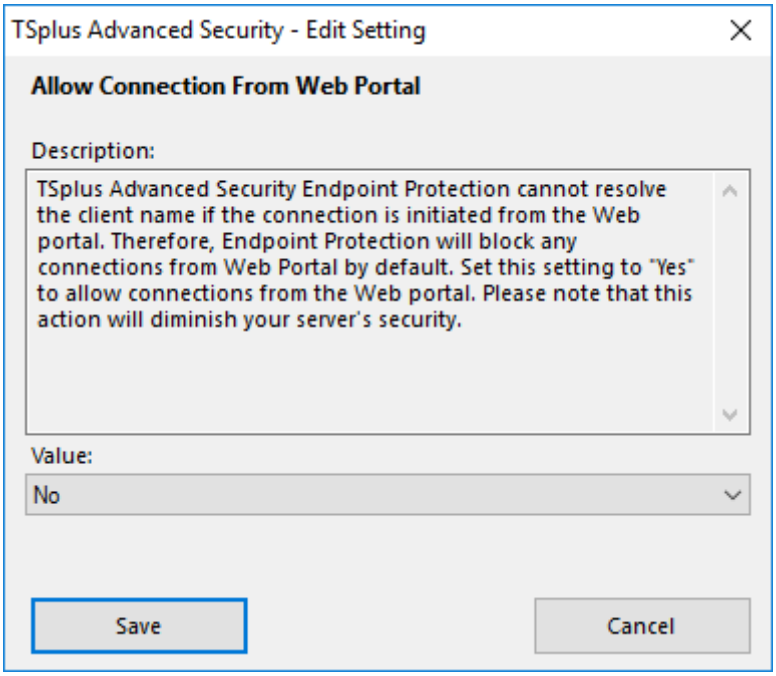


Advanced - Endpoints Settings

The **Endpoints tab** allows you to enable connections from the Web Portal for Endpoints Protection users.

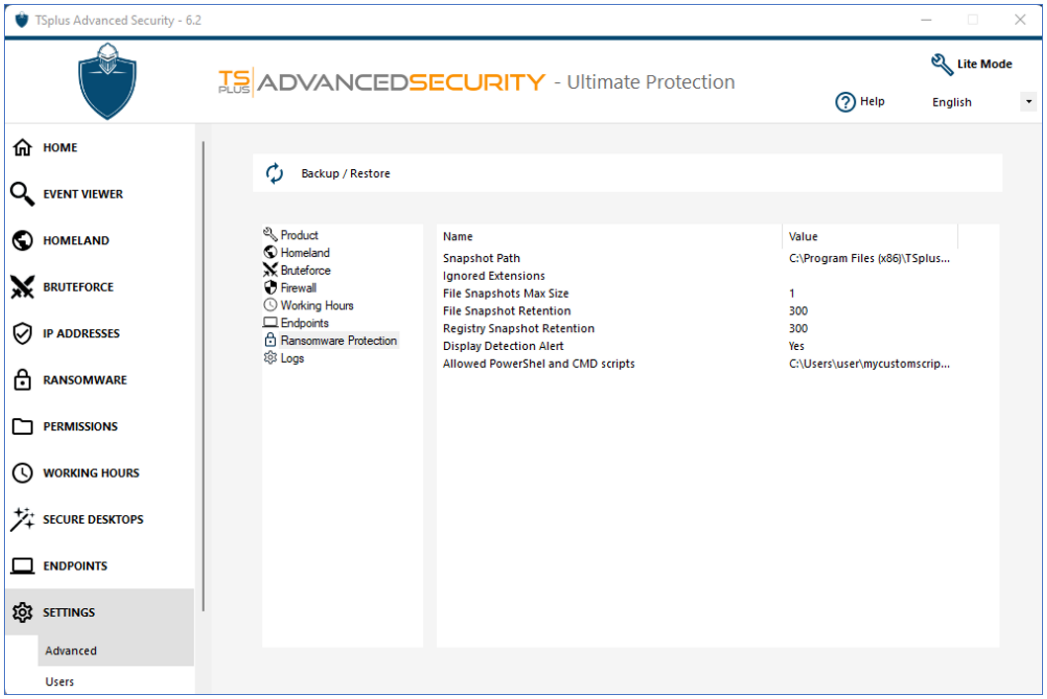


TSplus Advanced Security Endpoint Protection cannot resolve the client name if the connection is initiated from the Web portal. Therefore, Endpoint Protection will block any connections from Web Portal by default. Set this setting to "Yes" to allow connections from the Web portal. Please be aware that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

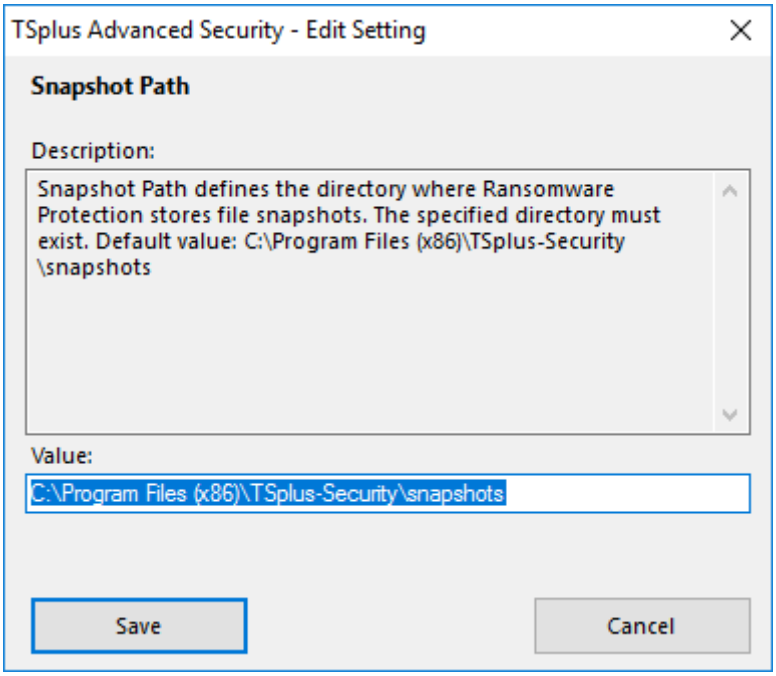


Advanced - Ransomware Settings

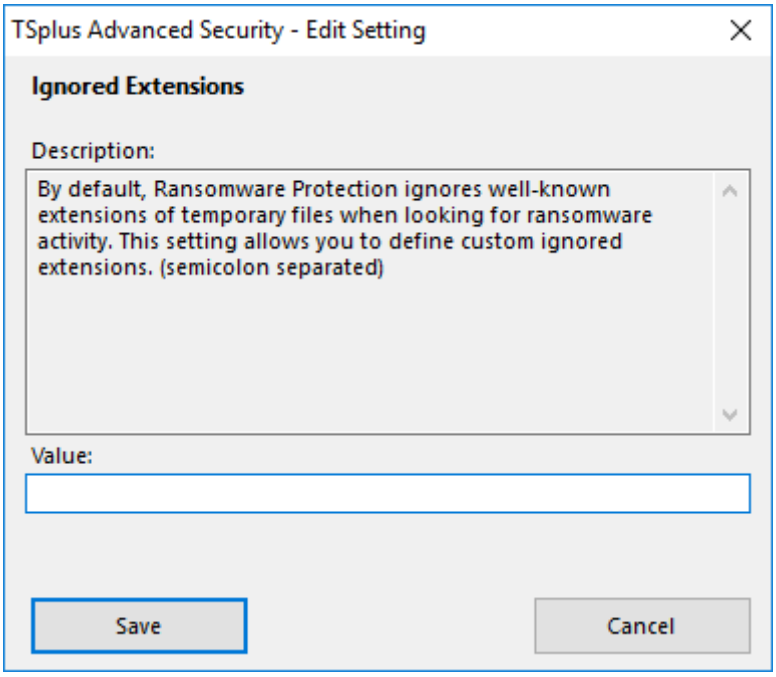
The **Ransomware tab** allows you to *configure the snapshot properties and define ignored file extensions* for the Ransomware Protection feature.



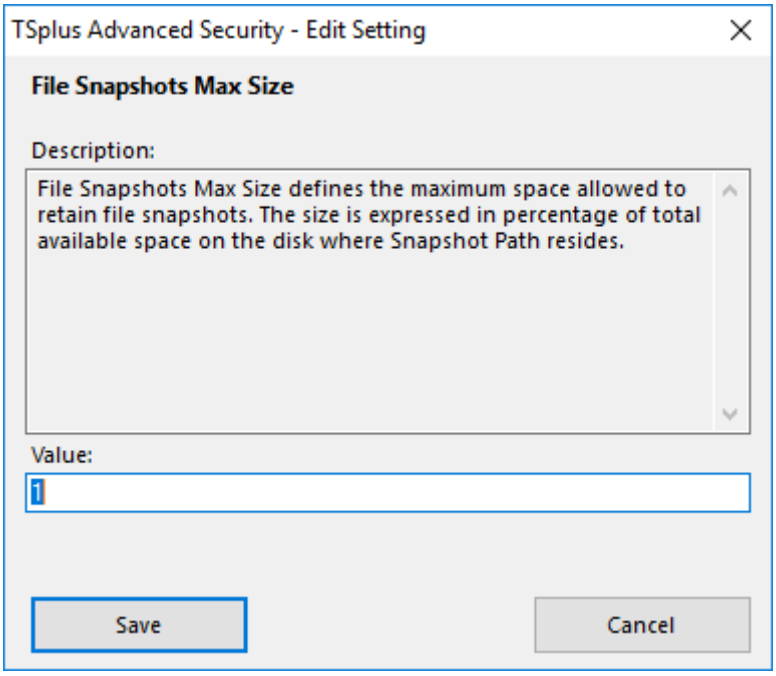
Snapshot Path: Define the directory where Ransomware Protection stores file snapshots.
Default value is: C:\Program Files (x86)\TSplus-Security\snapshots



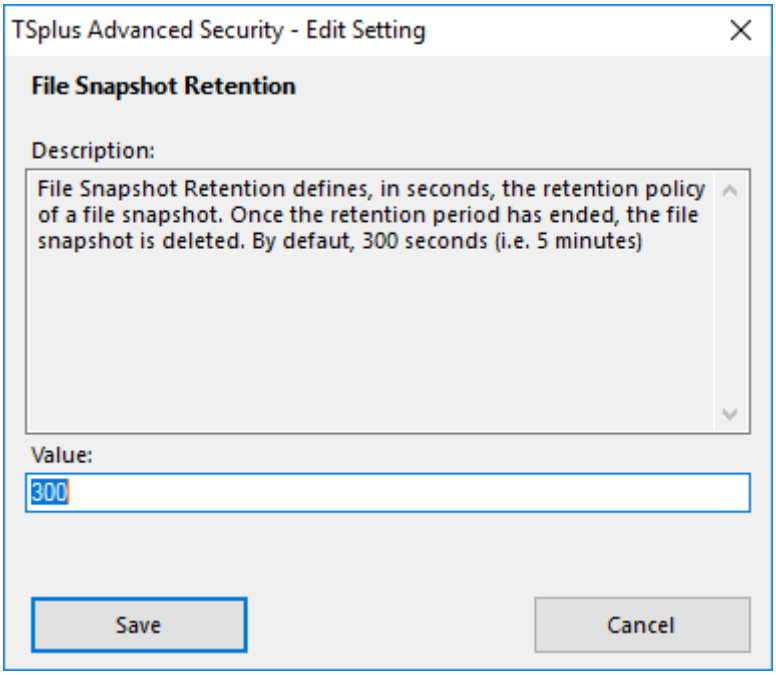
Ignored Extensions: By default, Ransomware Protection ignores well-known extensions of temporary files for ransomware activity. See the list here. You can define custome extension names on the value field (semicolon separated):



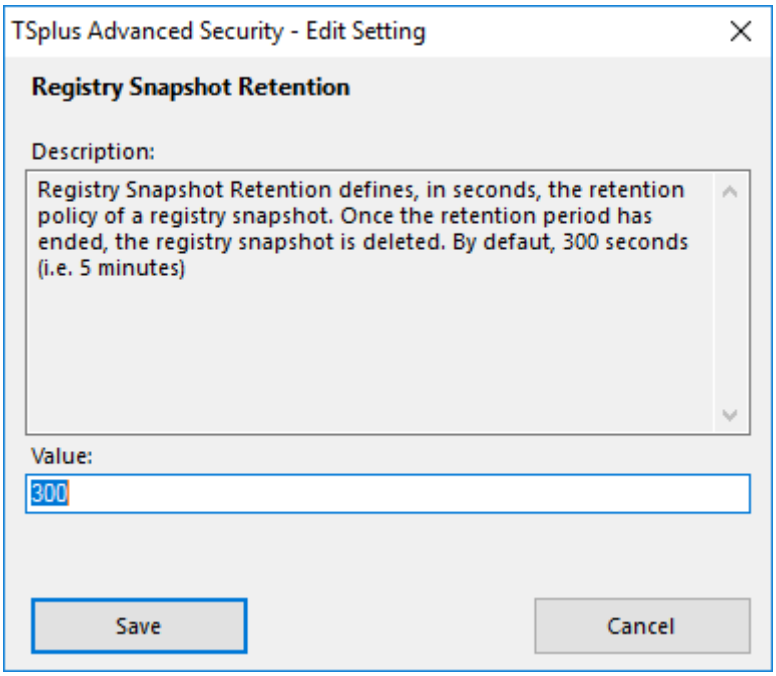
File Snapshot Max Size: File Snapshots Max Size defines the maximum space allowed to retain file snapshots. The size is expressed in percentage of total available space on the disk where Snapshot Path resides.



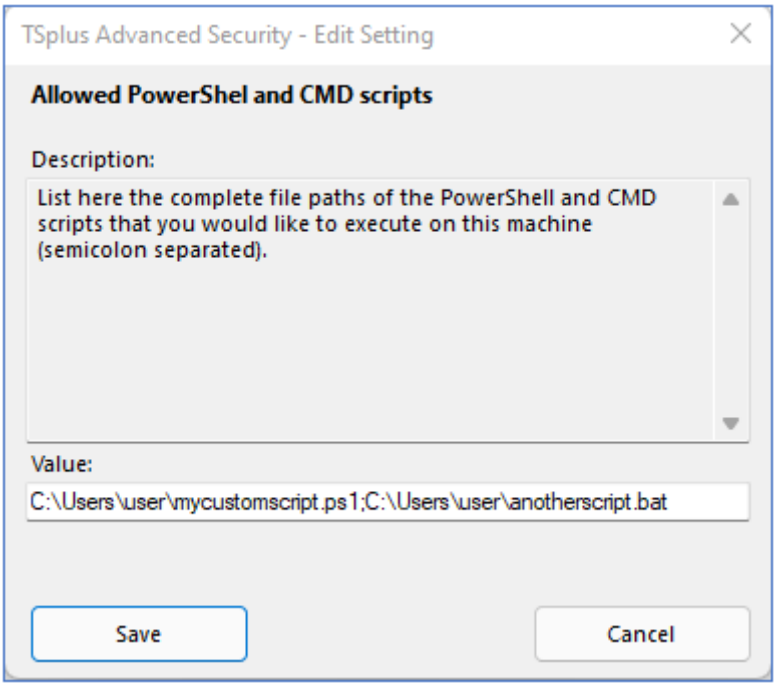
File Snapshot Retention: File Snapshot Retention defines, in seconds, the retention policy of a file snapshot. Once the retention period has ended, the file snapshot is deleted. By defaut, 300 seconds (i.e. 5 minutes)



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)



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).

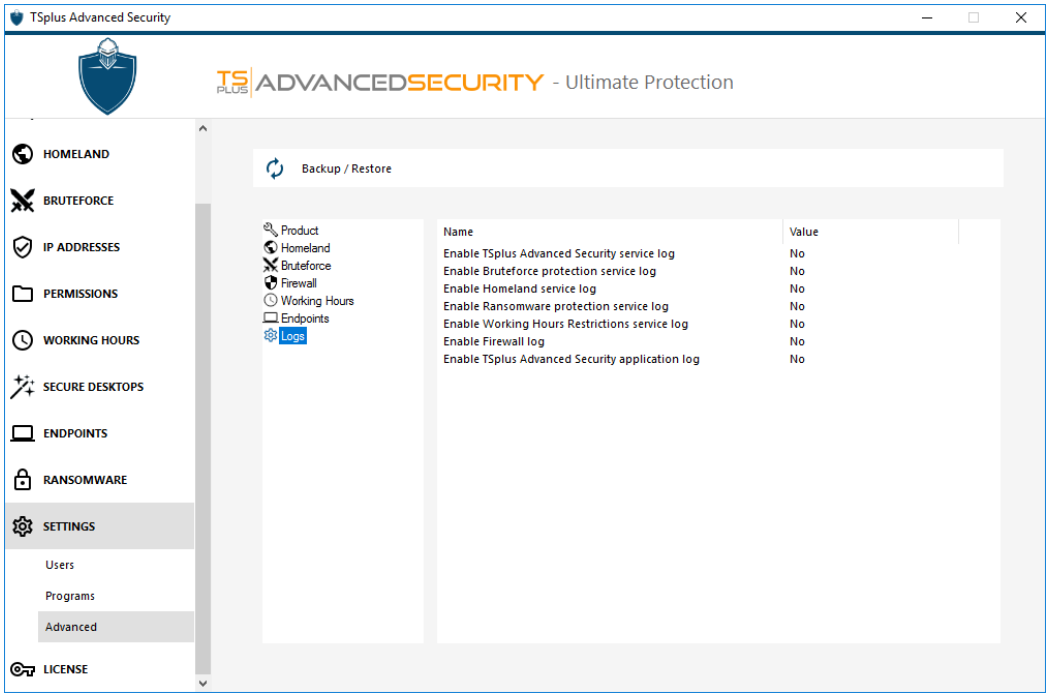

TSplus Advanced Security - Edit Setting
Allowed PowerShel and CMD scripts
Description:
List here the complete file paths of the PowerShell and CMD scripts that you would like to execute on this machine (semicolon separated).
Value:
C:\Users\user\mycustomscript.ps1;C:\Users\user\anotherscript.bat
Save
Cancel

Advanced - Logs Settings

The **Logs tab** allows you to *enable or disable service and functionalities 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 head here:

C:\Program Files (x86)\RDS-Tools\RDS-Knight\logs
or
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 features :

- Bruteforce Protection
- Homeland
- Ransomware protection
- Working Hours
- Firewall

They are disabled by default.

Logs correspond to different components, our support team will tell you what value to put according to the problem encountered.