TSplus Advanced Security Documentation



Table of Contents

Planning and Managing TSplus Advanced Security

- Getting Started
- <u>Pre-requisites</u>
- Installing Advanced Security
- <u>Updating Advanced Security</u>
- <u>Activating your license</u>

Using TSplus Advanced Security

- <u>Home</u>
- 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
- <u>Advanced > Logs</u>

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: <u>.NET Framework</u> 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: <u>Latest TSplus Advanced Security setup</u> program. Please download the setup program and follow the setup assistant 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 <u>contact us</u> should you face any hurdle or if you face any issue will configuring TSplus Advanced Security.

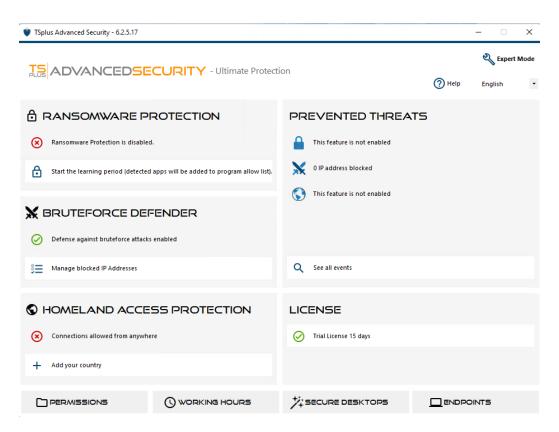
Once the installation has completed, a new icon is displayed on your Desktop. Double-click on this icon to open TSplus Advanced Security and start configuring the security features.



Please refer to the <u>documentation</u> for full installation instructions.

Step 2: Configuring TSplus Advanced Security

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



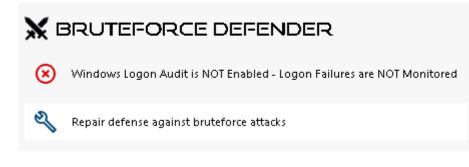
On the left column, the homepage allows a quick access to configure the Ransomware Protection, Bruteforce Defender and Homeland Access Protection features.

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



Start the learning period (detected apps will be added to program allow list).

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 <u>Homeland Access Protection</u>



You are all set! Don't forget to <u>activate your license</u> and to <u>update to the latest version</u> 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:

PRI	EVENTED THREATS
s	This feature is not enabled
X	0 IP address blocked
\bigcirc	673 remote accesses denied since 05 mai 2022 22:40:16
⊗	CloudSource IP Protection protects your computer against 614 348 888 IP addresses.
Q	See all events

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

Also, the <u>Hacker IP</u> 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 <u>Permissions</u> feature.
- Define period of time where users are authorized to login with the <u>Working Hours</u> feature. Users will be disconnected passed their allowed working hours.
- Customize and secure user sessions with the <u>Secure Desktop</u> 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 <u>Endpoint Protection</u>. 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: <u>.NET Framework</u> 4.5.3 or higher
- Microsoft Windows 7 SP1 and Windows 2008 R2 SP1 require an additonal update to support SHA2 Cross Signing (<u>KB4474419</u>). This update allows TSplus Advanced Security built-in firewall and ransomware protection to run properly.

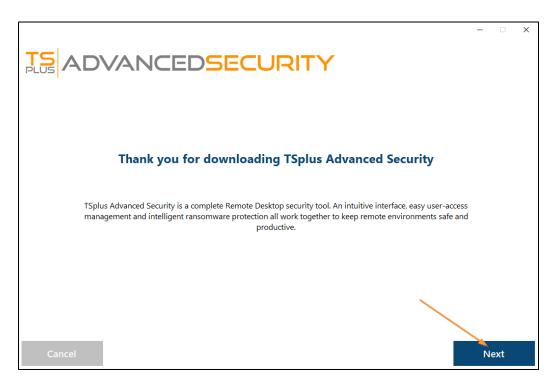
Note: These prerequisites will be automatically installed by the setup program if they are missing on the system.

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.

		-		×
	DVANCEDSECURITY			
1 202				
1	License Agreement			
	TSplus Advanced Security license agreement	^		
	Software You should carefully read the following terms and conditions before opening the software package, or if downloaded, before using such downloaded software. Opening the package or using the software, if downloaded, means you accept these terms and conditions and understand that they will be legally binding on you and TSplus Advanced Security. If you do not agree with these terms and conditions, or do not want them to be binding on you, you should promptly return the package unopened for a full refund or delete the downloaded software from any storage medium that it is stored on.			
	Ownership You acknowledge and agree that TSplus Advanced Security ("licensor") is the owner of all rights, title and interest in and to the enclosed disks and/or cdrom and/or the downloaded TSplus Advanced Security software, if downloaded, and the computer programs contained therein in machine readable object code form as well as the accompanying user documentation along with all subsequent copies thereof, regardless of the media or form in which they may exist (collectively the "software". The software is protected by copyright laws and international treat provisions, and this license agreement does not convey to you any interest in or to the software, digital content, or any accompanying printed materials, but only a limited right of us and limited reproduction which is revocable in accordance with the terms of this license agreement.			
	License Grant of license. Licensor hereby grants and you accept a nonexclusive license to use the software in accordance with the terms of this agreement.			
	Remote Desktop/Remote Assistance. The Software contains Remote Desktop and Remote Assistance technologies that enable the Software or applications installed on the TSplus Advanced Security Computer (Interestier referred to as a Host Device) to be accessed remotely from other Devices. You may use the Software's Remote Desktop feature to access the Host Device from any Device provided you acquire a separate Software license for that Device (for example, you may use any Windows XP based laptop to remotely access one TSplus Advanced Security Host Device(). When you are using Remote Assistance (or other software which provides similar functionality for a similar purpose) you may share a Session with other uses without any limit on the number of Device connections and without acquiring additional licenses for the Software – for Microsoft applications, you should consid	*		
		\backslash		
Cancel	Back	l a	gree	

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 <u>activate your license</u> and to <u>update to the latest version</u> to keep Advanced Security protection at its best!

Advanced installation scenarios

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

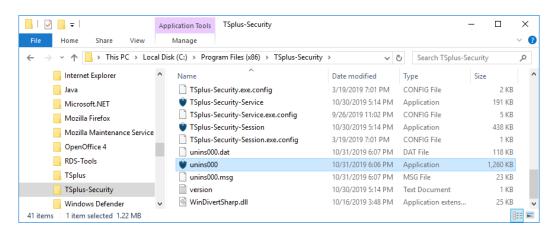
- Install silently, by providing the /VERYSILENT /SUPPRESSMSGBOXES parameters
- Prevent rebooting at the end of the setup, by providing the /NORESTART parameter. This parameter is usually used along with the above.
- Volume Licensing to activate your license directly while installing (please refer to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

Uninstall TSplus Advanced Security

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

📙 🛃 🥃 🗸 Program Files (x86)				- 0	×
File Home Share View					~ 🕐
\leftarrow \rightarrow \checkmark \Uparrow \blacksquare \rightarrow This PC \Rightarrow Local D	isk (C:) → Program Files (x86)	~ (う Search Pro	gram Files (x86)	P
Program Files (x86)	Name	Date modified	Туре	Size	^
Common Files	TSplus	11/7/2019 8:21 PM	File folder		
Foxit Software		11/7/2019 10:32 PM	File folder		
Google		7/15/2019 1:39 PM	File folder		
gs	📊 Windows Mail	7/1/2019 10:21 PM	File folder		
	📙 Windows Media Player	10/2/2019 3:25 PM	File folder		
Internet Explorer		7/16/2016 3:23 PM	File folder		
Java		7/16/2016 3:23 PM	File folder		
Microsoft.NET	Windows Photo Viewer	7/15/2019 1:39 PM	File folder		
Mozilla Firefox	Windows Portable Devices	7/16/2016 3:23 PM	File folder		
21 items 1 item selected	Mindows Dower Shell	7/16/2016 2.22 DM	Eile felder		

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.

Désinstallation - TSplus Advanced Security	
Optional tasks Select any optional tasks to be performed by the uninstall program.	٢
Would you like to unblock all previously blocked IP adresses? This may take up to one hour. Unblock IP addresses	
Uninstall An	nuler

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:

TSplus Advanced Security - 5	.4.11.22 — 🗆	×
	TS ADVANCEDSECURITY - Ultimate Protection	
С номе	Keep threats away from your Windows system.	
	Prevent, protect and fight cyber attacks.	
	0 Dec 12:13:17 A connection has been authorized for user DESKTOP-QVTJFVE\utilisateur from computer because this feature is no enabled for this user	ot
	0 Dec 12:13:17 O Alogon request has been granted for user DESKTOP-QVTJFVE\utilisateur because DESKTOP-QVTJFVE\utilisateur is allowed	
	0 Dec 11:09:08 A connection has been authorized for user DESKTOP-QVTJFVE/utilisateur from computer because this feature is no enabled for this user	ot
Č	0 Dec 11:09:08 O A logon request has been granted for user DESKTOP-QVTJFVE\utilisateur because DESKTOP-QVTJFVE\utilisateur is allowed	
	09 Dec 13:12:15 A connection has been authorized for user DESKTOP-QVTJFVE/utilisateur from computer because this feature is no enabled for this user	ot
SECURE DESKTOPS	System audit - 1 issue found on 12/10/2021 12:44:38 PM	
	Version 5.4.11.22 - New version available, click here to upgrade to 6.0.12.6	
SETTINGS	Trial License 14 days	
	English •	

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 <u>Backup and restore your data and settings</u>

TSplus Advanced Security - Activating your license

Step 1: Activating your license from Lite mode

Click on the "Trial License" button.

🖤 TSplus Advanced Security - 6	– 🗆 X
	on ⑦ Help English •
RANSOMWARE PROTECTION Ransomware Protection is disabled. Start the learning period (detected apps will be added to program allow list).	PREVENTED THREATS This feature is not enabled O IP address blocked
BRUTEFORCE DEFENDER O Defense against bruteforce attacks enabled Manage blocked IP Addresses	See all events
HOMELAND ACCESS PROTECTION Connections allowed from anywhere Add your country	LICENSE Trial License 15 days

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

🖤 TSplus Advance	l Security - 6.		-	×
			🂐 Expert	Mode
PLUS		Help	English	•
4			_	
~	ලිතු Activate your License			
	Eus Now			
	Rehost an existing license			
	🗘 Refresh your license			
	License Status			
	Cr Trial License 15 days			
	Computer ID:			
	Computer name: DESKTOP-QVTJFVE			
	Protection Status			
	Homeland Access Protection			
	Brute-Force Attacks Defender I Endpoint Protection and Device Control			
	Working Hours Restrictions			

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.

🖤 TSplus Advanced Security - 6	04	- 🗆 X
	ADVANCEDSECURITY - Ultimate Protection	💐 Lite Mode English 🔹
М НОМЕ		
	ⓒ규 Activate your License	
	'문국 Buy Now	
	+ Rehost an existing license	
	Refresh your license	
	License Status	
	Computer ID:	
SECURE DESKTOPS	Computer name: DESKTOP-QVTJFVE	
	Protection Status	
	Homeland Access Protection	
SETTINGS	Brute-Force Attacks Defender Independent Endpoint Protection and Device Control	
ତିଳ୍ପ LICENSE	Working Hours Restrictions	

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

🖤 TSplus Advance	l Security - 6.		-	Х
			🌯 Expert	Mode
		Help	English	•
1			_	
←	Cr Activate your License			
	Eu Buy Now			
	+ Rehost an existing license			
	🗘 Refresh your license			
	License Status			
	Trial License 15 days			
	Computer ID:			
	Computer name: DESKTOP-QVTJFVE			
	Protection Status			
	Homeland Access Protection			
	Brute-Force Attacks Defender Indpoint Protection and Device Control	ы		
	Working Hours Restrictions			

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 <u>Licensing Portal</u> 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:

		You	ur activation key	is: NAQR-				
_icen	ces							
Application	Numéro de Série / Computer	Jours	Utilisateurs	Edition	Numéro de Commande	Date	Support?	Actions
TSplus	P30	-	3	Enterprise	11408	2020-01- 27	I Voir	E Détails
TSplus	P65	-	10	Enterprise	JWT19	2019-05- 29	I Voir	I Détails
TSplus	P24	-	25	Enterprise	JWT18	2018-10- 19	×	I Détails
TSplus	P6E	-	10	Enterprise	JWT17	2017-09-	x	i≣ Détails

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

Enter your activation key and click on "Next".

TSplus TSplus Enterprise edition - 5 users No Updates/Support	
○ No Updates/Support	
O Update/Support convices for TSplus Ev	
O opuale/support services for Topius E	nterprise edition - 5 users - 3 years
TSplus Advanced Security	
TSplus Advanced Security Ultimate edition	
The licenses listed above are all the licenses currently av If you have purchased multiple units, only one will be disp will be able to activate the other units on other computers	played in this list for this computer, and you

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.

has been activated!	
Splus Enterprise edition - 5 users	
Jpdate/Support services for TSplus Enterprise edition - 5 users - 3 years	
Splus Advanced Security Ultimate edition	
r your business!	
safely close this window.	
_	Finish
	e has been activated! TSplus Enterprise edition - 5 users Jpdate/Support services for TSplus Enterprise edition - 5 users - 3 years TSplus Advanced Security Ultimate edition or your business! v safely close this window.

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).

©;	Permanent license activated Enterprise edition - Unlimited users
e	Computer ID: 2222
	Computer name: DESKTOP-F304H4I
	End of support date: 5/14/2023
_	nse Status License Activated - Ultimate Protection edition
	nse Status License Activated - Ultimate Protection edition COMPUTERID 2222

Refresh your licensing status by clicking on the corresponding button.



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

License	×
License has been synchronized wit	th licensing portal
	ОК

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 <u>Customer Portal User Guide</u> for more information.

Thank you for choosing TSplus Advanced Security!

Home

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

Click on each tile to know more about each feature

🕈 TSplus Advanced Security - 6.	3.5.23	
Ŷ		المجمع Lite Mode
П НОМЕ		
S HOMELAND	23 mai 23:02:57 🔇 A remote connection was denied from IP address 87.251.67.64 (Poland). This IP address w Homeland on 06 mai 2022 03:42:37	as originally blocked by
BRUTEFORCE	23 mai 22:54:45 S Aremote connection was denied from IP address 87.251.67.64 (Poland). This IP address w Homeland on 06 mai 2022 03:42:37	ras originally blocked by
	1 23 mai 22:54:03 😥 Synchronized Hacker IP addresses protects your computer against 614 348 888 IP address	es.
	23 mai 22:48:47 S A remote connection has been authorized from IP address 212.106.118.150 because 212.1 with the authorized country France	106.118.150 is associated
	23 mai 22:40:15 A connection has been authorized for user NS204950\vmadmin from computer .A9HX6ZPI feature is not enabled for this user	PONMOG3 because this
ゲ SECURE DESKTOPS	System audit - 1 issue found on 23/05/2022 23:05:16	
	Version 6.3.5.23 - You are using the latest version	Read changelog
	License Activated - Ultimate Protection edition	
贷 SETTENGS		
CT LICENSE	End of support date: 2025-04-26	

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 <u>Security Events</u>. 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. <u>new version availability</u>
- 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.

TSplus Advanced Security - 6.3.5	5.23		- 0	×
	ADVANCEDSECURITY - Ultimate Protection	Help	💐 Lite Mo English	de •
М НОМЕ	A new feature is available! Keep your machine protected against known threats such as on-line attacks, on-line service abuss cybercrime activities with the Hacker IP Protection. Support and Updates Services subs		and other	x
	There is no event to display at this time. Why not trying one of the available security feature?			
BLOCKED IP ADDRESSES				
SECURE DESKTOPS	System audit - 2 issues found on 5/23/2022 11:05:05 PM			
		-		
	Version 6.3.5.23 - You are using the latest version	(i) Read cl	hangelog	
ស្រ្ហិ SETTINGS	V Trial License 15 days			
CT LICENSE				

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.

🖤 TSplus Advanced Security - System audit	×
Success - Service TSplus-Security should be running	
Success - You should allow TSplus Advanced Security to access Internet to check for updates	
Success - TSplus Advanced Security main programs should all exist	
Success - Windows Firewall should be enabled	
Success - Logging should be disabled in production use	
Success - Minimum Password Length must be greater than zero	
Success - Guest account should be disabled	
System audit - Latest check on 10/21/2019 7:39:36 PM	Run system audit

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.

🖤 TSplus Advanced Security - System audit	×
Success - Service TSplus-Security should be running	
Success - You should allow TSplus Advanced Security to access Internet to check for updates	
Success - TSplus Advanced Security main programs should all exist	
Success - Windows Firewall should be enabled	
Success - Logging should be disabled in production use	
Warning - Minimum Password Length must be greater than zero	
Success - Guest account should be disabled	
System audit - Latest check on 10/21/2019 7:39:36 PM	Run system audit

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		_		×
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp				
🗢 🔿 📶 🗙 🗟 🛛 🖬				
 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 Enforce password history Aximum password age Minimum password age Password must meet complexity requirements Store passwords using reversible encryption	Security Sett 0 passwords 0 0 days 0 characters Enabled Disabled	remem	bered

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.

🖤 TSplus Advanced Security		- 0	×
	ADVANCEDSECURITY - Ultimate Protection		
	Allow connections from anywhere		
S HOMELAND	Allow connections only from private and whitelisted IP addresses		
	Allow connections only from this list of countries:		
IP ADDRESSES	+ Add Country X Remove Country		
設 settings			
		Apply now	

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.

Add Country	- 🗆 X
Select Country	United States of America 🗸 🗸
Unblock all IP addresses b This action will be execute	locked by Homeland protection for the selected country. d when applying changes.

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

TSplus Advanced Security		- 0	×
	ADVANCEDSECURITY - Ultimate Protection		
HOME	O Allow connections from anywhere		
	Allow connections only from private and whitelisted IP addresses		
	Allow connections only from this list of countries:		
IP ADDRESSES	+ Add Country X Remove Country		
	France Ireland United States		
ស្ត្រី settings	_		1
	Ľ	Apply now	

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.

Confirmat	ion	×
	Please make sure that you have allowed at least your current location, or you will be instantly blocked when applying these settings. Are you sure you want to apply these settings?	
	Yes <u>N</u> o	

Restrict access from the internet

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

🖤 TSplus Advanced Security			_		×
	TE ADVANCEDSECURIT	Y - Ultimate Protection			
	O Allow connections from anywhere				
HOMELAND	Allow connections only from private and whether the second sec	hitelisted IP addresses			
	Allow connections only from this list of course	ntries:			
IP ADDRESSES	+ Add Country X Remove Country				
SETTINGS					
©규 LICENSE			Apply n	ow	

Disable Homeland Access Protection

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

TSplus Advanced Security		- 🗆	×
	ADVANCEDSECURITY - Ultimate Protection		
	Allow connections from anywhere		
	Allow connections only from private and whitelisted IP addresses		
BRUTEFORCE	Allow connections only from this list of countries:		
IP ADDRESSES	+ Add Country X Remove Country		
絞 settings			
		Apply now	

Unblocking blocked IP addresses

When an IP address gets blocked, it appears on the <u>IP Addresses</u>. 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 <u>IP Addresses</u> to avoid being blocked by either Homeland Access Protection or <u>Bruteforce Protection</u> 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 <u>Settings > Advanced > Homeland</u>.

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 <u>Settings > Advanced > Homeland</u>.

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. <u>Contact us</u>.

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 bruteforce 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.

👻 TSplus Advanced Security		- 0	×
	TSplus Advanced Security - Ultimate Protection		
	IPs Detection Maximum failed logon attempts from a single IP address: 10 + Reset counters of failed logon attemps after: 2 + hours		
BRUTEFORCE		Apply Now	
IP ADDRESSES PERMISSIONS WORKING HOURS	Defender Status Image: TSplus-Security Service is Running - You are Protected Image: Windows Firewall is Enabled - Blocked IPs cannot connect Image: Windows Logon Audit is Enabled - Logon Failures are Monitored		
	HTML5 Portal Logs enabled - Portal logon failures are monitored		
	Manage blocked IP Addresses		
鉸 settings ⓒ규 license	~		

- 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 <u>IPs Whitelist</u>, 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 <u>Settings > Advanced ></u> <u>Bruteforce tab</u>

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:

								💐 Lite Ma	ode
	TS ADVAN	CEDSECU	I-(I Y - (litimate Prot	ection		(?) Help	English	
А номе	+ Add IP Address	🧷 Edit IP Ad	dress	× Remove IP Ad	dress(es)	🗘 Refre	esh Hacker IP	Q WHOR	s
	IPs in the allow list will be in	anored by TSplus Advanced	t Security and will	nat be blacked by Han	eland Access F	rotection or	Bruteforce Attacks	Defender features	
	614 349 459 IP address(es			,					
S BRUTEFORCE	· · ·						1	(_
K BROTEFORCE	IP Address	Country	Status 🔶		Date		Description		
~	89.58.5.246 494.5.175.15	Germany		meland Protection	23 mai 2022				
BLOCKED IP ADDRESSES		Iran		meland Protection	23 mai 2022				
	103.239.53.25	Iran Camhodia		meland Protection	23 mai 2022				
	61.194.228.1			meland Protection	23 mai 2022 23 mai 2022				
• RANSOMWARE	61.194.228.1 180.188.246.171	Japan		meland Protection					
	180.188.246.1/1 51.254.49.105	India Units d Kin a dam		meland Protection	23 mai 2022 23 mai 2022				
PERMISSIONS	93.174.89.131	United Kingdom Netherlands		meland Protection meland Protection	23 mai 2022 23 mai 2022				
—	223.71.167.165	China		meland Protection	23 mai 2022				
2	139.162.215.70	United Kingdom		meland Protection	23 mai 2022				
WORKING HOURS	34.159.36.90	Germany		meland Protection	25 mai 2022 17 mai 2022				
	181.214.206.204	Netherlands		meland Protection	17 mai 2022				
SECURE DESKTOPS	182,239,114,204	Hona Kona		meland Protection	17 mai 2022				
+	181.214.206.205	Netherlands		meland Protection	17 mai 2022				
	77.83.36.60	Ukraine		meland Protection	17 mai 2022				
ENDPOINTS	45.83.64.1	Germany		meland Protection	17 mai 2022				
	45.83.65.204	Germany		meland Protection	17 mai 2022				
	45.83.65.249	Germany		meland Protection	17 mai 2022				
CTENIS	159.65.200.34	Netherlands		meland Protection	17 mai 2022				
	81.163.41.37	Russia		meland Protection	17 mai 2022				
SETTINGS	186.122.149.142	Argentina		meland Protection	17 mai 2022				
-	52.233.251.139	Netherlands		meland Protection	17 mai 2022				Î

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:

								💐 Lite Mo	de
	TS ADVANC	EDSECU		Jitimate Pro	tection		Help	English	
HOME	+ Add IP Address	🧷 Edit IP A	ddress	X Remove IP A	ddress(es)	🗘 Refre	esh Hacker IP	Q WHOI	
) HOMELAND	IPs in the allow list will be igno.	red by TSplus Advanc	ed Security and will	not be blocked by Ho.	neland Access F	rotection or	Bruteforce Attacks	Defender features	
	614 349 459 IP address(es) bl	ncked							
BRUTEFORCE							1		
Conditioned		Country	Status 🔺		Date		Description		-
BLOCKED IP ADDRESSES	1.19.0.1-1.19.255.254			icker IP Protection	23 mai 2022		Know malicious		
BLOCKED IP ADDRESSES	1.32.128.1-1.32.191	Singapore		cker IP Protection	23 mai 2022		Know malicious		
	100.64.0.1-100.127			icker IP Protection	23 mai 2022		Know malicious		
RANSOMWARE	101.101.96.1-101.1			icker IP Protection	23 mai 2022		Know malicious		
RANSOMWARE	101.134.0.1-101.13			cker IP Protection	23 mai 2022		Know malicious		
	101.203.128.1-101			icker IP Protection	23 mai 2022		Know malicious		
PERMISSIONS	101.248.0.1-101.24			icker IP Protection	23 mai 2022		Know malicious		
	101.42.0.1-101.42.2	China		icker IP Protection	23 mai 2022		Know malicious		
	102.192.0.1-102.20			icker IP Protection	23 mai 2022		Know malicious		
) WORKING HOURS	102.208.0.1-102.21			cker IP Protection	23 mai 2022		Know malicious		
	102.212.0.1-102.21			icker IP Protection	23 mai 2022		Know malicious		
SECURE DESKTOPS	102.214.0.1-102.21			icker IP Protection	23 mai 2022		Know malicious		
SECORE DESKTOPS	102.215.0.1-102.21			icker IP Protection	23 mai 2022		Know malicious		
	102.215.128.1-102			icker IP Protection	23 mai 2022		Know malicious		
ENDPOINTS	102.215.160.1-102			cker IP Protection	23 mai 2022		Know malicious		
-	102.215.184.1-102			cker IP Protection	23 mai 2022		Know malicious		
	102.215.192.1-102	South Africa		icker IP Protection	23 mai 2022		Know malicious		
EVENTS	102.215.200.1-102			icker IP Protection	23 mai 2022		Know malicious		
	102.215.216.1-102			icker IP Protection	23 mai 2022		Know malicious		
SETTINGS	102.215.224.1-102			cker IP Protection	23 mai 2022		Know malicious		
5 SET 11435	102.216.20.1-102.2 102.216.23.1-102.2			icker IP Protection icker IP Protection	23 mai 2022 23 mai 2022		Know malicious Know malicious		1

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:

👻 Edit Description	— 🗆	Х
IP Address	125.212.233.172	
Description	Accountancy-Server	
	Edit Description	
	/ Luit Description	

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.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:

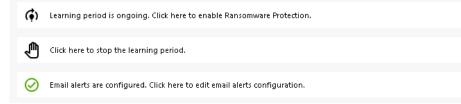
🖤 TSplus Advanced Security			_	×
	ADVANCEDSECURITY - Ultimate Protection			
М номе	Ransomware Protection is disabled. Click here to enable Ransomware Protection.			1
	Kansomware Protection is disabled. Click here to enable kansomware Protection.			<u>ا</u>
	Email alerts are not configured yet. Click here to configure email alerts.			
	The programs interrupted by Ransomware Protection are listed below: Date Interrupted Program	Review &	Act	7
IP ADDRESSES				
WORKING HOURS				
Overview	•			_
Snapshots	Manage programs whitelist			
Quarantine 🗸 🗸				

ŶТ	Splus Advanced Security - About Ransomware Protection	×						
	TSplus Advanced Security							
	About Ransomware Protection							
	TSplus Advanced Security Ransomware Protection observes in real time how programs interact with system and personal files.							
	To ensure a greater level of protection, TSplus Advanced Security Ransomware Protection creates bait files in key folders where ransomware often begins its attack.							
	often begins its attack. Therefore, a few hidden files may appear in the users' desktop and documents folders, as well as in other locations. We suggest to hide hidden files to regular users through your server settings or Group Policy.							
	Cancel Enable Ransomware Protection							

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.

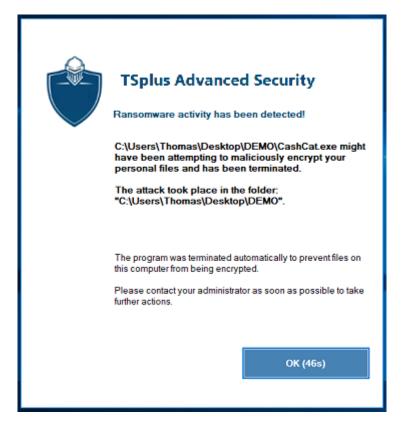


If you stop the Learning Period, it will deactivate the Ransomware Protection. Click on the "Ransomware Protection is disabled" button to reactivate the Learning Period.

Ransomware Protection 4

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			- 🗆 X
Ransomwa	are Protection	I	
 Ransomware Protection is enabled 	oled	Disable Ransomware Protection	Configure Email Alerts
Ransomware Protection Summary			1 1
Date	Interrupted Program		Review & Act
vendredi 5 octobre 2018 16:19:59	C:\Users\Thomas\De	sktop\DEMO\Ransomware\ransomware.exe	0
Whitelisted programs will be ignored	by Ransomware Protect	tion	
Program File Path			Remove
C:\Program Files (x86)\Notepad++\v C:\Program Files (x86)\TSplus-Se			×
C:\Program Files (xoo)\TSplus-Se	ecunty.exe		<u>^</u>
C:\Program Files (x86)\TSplus-Se	curity.exe		Add
	gram to the Ransomwar	re Protection program whitelist. This executable w	ill be able to create, change and delete your
		Apply now	
		- - / / / / / /	

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.

TSplus Advanced Security - 5.3	TSplus Advanced Security - Ransomware Protection Report	- 0	×	×
	Ransomware Protection Report			Γ
	Ransomware Protection has detected a ransomware attack on computer DESKTOP-BS41S8F at Saturda 11.14:39 PM in session DESKTOP-BS41S8P.(Thomas. The malicious program C\Ubers\Thomas\DesktOp\F \CashCat.exe has been terminated. Please review the report to take further action.			
С р номе	Details			
	Event Date: Saturday, March 13, 2021 1:14:39 PM			
	The attack took place in user session: DESKTOP-854158P\Thomas (Administrator) Executable File Path:			
	C\\Users\Thomas\Desktop\PLOP\CashCaf\CashCat.exe			1
**	The executable file has been moved into quarantine here:			
D IP ADDRESSES	C\Program Files (x86)\TSplus-Security\quarantine\CashCat.exe_2021-03-13T12.14.42.infected			
~	A memory dump is available here:			
PERMISSIONS	C:\Program Files (x86)\TSplus-Security\dumps\MiniDump_2021-13-313-14-39.mdmp			
WORKING HOURS	Review the files created during the attack and put into quarantine the dangerous ones:			
0		ut Into Quarantine	^	
74 SECURE DESKTOPS	Cr\Users\Thomas\Desktop\PLOP\CashCat\Lorem (psum - Copy (10) - Copy - Copy - Copy.zeppelin Cr\Users\Thomas\Desktop\PLOP\CashCat\Lorem (psum - Copy (10) - Copy - Copy.zeppelin	8		
	CI\Users\Thomas\Desktop\PLOP\CashCat\Lorem lpsum - Copy (10) - Copy.zeppelin	ō		
	C!\Users\Thomas\Desktop\PLOP\CashCat\Lorem lpsum - Copy (10).zeppelin C!\Users\Thomas\Desktop\PLOP\CashCat\Lorem lpsum - Copy (100) - Copy - Copy.zeppelin	8		
	Review the sensitive registry keys modified during the attack and edit the dangerous ones:	-	¥	
Overview	Registry Key Name Value	Old Value		
Snapshots	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ SecurityHealth C:\Windows\system32\SecurityHealth			
Quarantine				
×				-

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:

Email alerts are not configured yet. Click here to configure email alerts.

👻 TSplus Advanced Security - En	nails Settings		×
Emails Settings			
SMTP configuration allows TSp administrators in order to high			0
SMTP Hostname	mycompany.com]
SMTP Port	465]
Use SSL			
SMTP Username	admin]
SMTP Password	********		
Send Email From	admin@mycomp	any.com]
Send Email To	admin@mycomp	any.com]
Apr	ly and Test now		

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

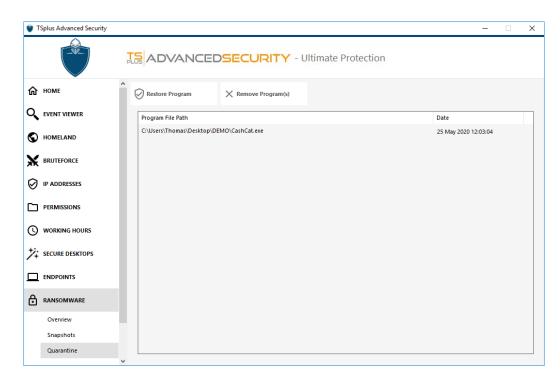
Snaphshots taken by Ransomware Protection are visible under the Snapshots tab:

TSplus Advanced Security				_	
		CEDSECURIT	Y - Ultimate Protection		
Номе	A Refresh	Restore	× Remove		
EVENT VIEWER	Name			Date	,
	Snapshots taken on	Monday, May 25, 2020 12:07 PM	4 (UTC)		
HOMELAND		86)\RDS-Tools\RDS-Knight\data\		25 May 2020 12:03:04	
		icrosoft\Diagnosis\EventStore.d		25 May 2020 12:03:04 25 May 2020 12:03:57	
		· · · · · · · · · · · · · · · · · · ·		25 May 2020 12:03:57 25 May 2020 12:03:58	
BRUTEFORCE					
				25 May 2020 12:03:02 25 May 2020 12:06:12	
IP ADDRESSES					
_			ore51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml	25 May 2020 12:06:12 25 May 2020 12:03:56	
PERMISSIONS			oretemp51b519d5-b6f5-4333-8df6-e74d7c9aead4.xml	25 May 2020 12:03:56	
				25 May 2020 12:05:30	
WORKING HOURS					
/			Platform\L.Thomas\ActivitiesCache.db-wal	25 May 2020 12:05:48 25 May 2020 12:05:55	
t.			tudio Services\7.0\Cache\a5ca35eb-148e-4ccd-bbb3-d		
SECURE DESKTOPS			tudio\15.0_0863837c\privateregistry.bin	25 May 2020 12:06:35	
		ppData\Local\Microsoft\VisualS		25 May 2020 12:06:45	
ENDPOINTS			tudio\vshub\Settings\SharedSettings.updates.v1.sqlite		
-			tudio\vshub\Settings\SharedSettings.v1.sqlite	25 May 2020 12:06:56	
			tudio\vshub\Settings\Sync\-1617891645\Temp\894.6440		
RANSOMWARE			mon\OnlineLicensing\VisualStudio\15.0\Community\d		
			mon\OnlineLicensing\VisualStudio\15.0\Community\d		
Overview		ppData\Local\Microsoft\Windo		25 May 2020 12:03:03	
Snapshots		ppData\Local\Microsoft\Windo		25 May 2020 12:03:12	
51105511015		ppData\Local\Microsoft\Windo		25 May 2020 12:03:12	
Ouarantine		ppData (Local Microsoft) Window		25 May 2020 12:03:11	~

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
- vsvvud
- iso
- dmg
- sparseimage
- cab
- msi
- mui
- dl_
- wim
- ost
- 0
- qtch
- ithmb
- vmdk
- vmem
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- menudata
- appicon
- appinfo
- pva
- pvs
- pvi

- pvm
- fdd
- hds
- drk
- mem
- nvram
- hdd
- pk3 pf
- pr • 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:

🖤 TSplus Advanced Security		- 🗆 X
	TS ADVANCEDSECURITY - Ultimate Protection	
П НОМЕ	Deny ③ Read	
	Users and Groups - Local computer Select one or multiple files or folders to edit permiss Default View Name	Permissions Owner
	Switch View	
	Bit Street A Bit Street A Bit Street A Bit Street Bit Street Bit Stree Bit Stree	Full Control AUTORITE NT\Sy Full Control BUILTIN\Adminis Full Control BUILTIN\Adminis Deny AUTORITE NT\Sy
IP ADDRESSES		Full Control BUILTIN\Adminis Full Control AUTORITE NT\Sy Modify NT SERVICE\Trus
		Modify NT SERVICE\Trus Full Control AUTORITE NT\Sy Full Control BUILTIN\Adminis
Manage	Distributed COM Users H Comments Comment	Full Control AUTORITE NT\Sy Deny BUILTIN\Adminis
Inspect		Full Control BUILTIN\Adminis Full Control AUTORITE NT\Sy
	- 2. IIS_IUSRS ⊕ Configuration Operators - 2. Network Configuration Operators ⊕ Configuration Operators	Modify NT SERVICE\Trus Full Control BUILTIN\Adminis Read NT SERVICE\Trus
	- 22. Performance Log Users BOOTNAT - 22. Performance Montor Users BOOTNAT - 22. Power Users Iang ini	Full Control AUTORITE NT/Sy Full Control BUILTIN/Adminis
	- 23. System Managed Accounts Group - 23. Users - 23. Durmy	>
袋 settings	Commy Files and Folders Registry	O Printers

- **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

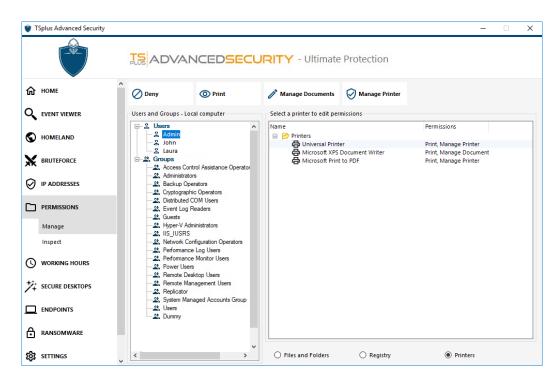
FileSystemRights.Traverse).

• **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 :

<u></u> тя	Splus Advanced Security					– 🗆 X
			IRITY - Ultim	nate Protection		
ŵ	HOME	Deny ORead	🧪 Modify	Ownership		
Q	EVENT VIEWER	Users and Groups - Local computer	Select a registry key	to edit permissions		
`		⊡≗ Users ∧	Name		Permissions	Owner 🔺
\odot	HOMELAND	& Admin	🖃 🃂 HKEY_LOCA	L MACHINE		
U	HOMILLAND	- 😤 John	🔲 📂 HARDW		Full Control	BUILTIN\Adm
		Laura	🕀 📄 ACP	1	Full Control	BUILTIN\Adm
X	BRUTEFORCE	Groups	🕀 🛅 DES	CRIPTION	Full Control	BUILTIN\Adm
~~		- 2. Access Control Assistance Operator	🕀 🛅 DEV	ICEMAP	Full Control	BUILTIN\Adm
\sim			🕀 🛅 RES	OURCEMAP	Full Control	BUILTIN\Adm
\oslash	IP ADDRESSES	Backup Operators	🗀 SAM		Full Control	BUILTIN\Adm
			🖃 📂 SOFTWA		Full Control	BUILTIN\Adm
~	PERMISSIONS	- 2. Distributed COM Users	🕀 🛅 Clas		Full Control	BUILTIN\Adm
	PERMISSIONS		🕀 📄 Clier		Full Control	AUTORITE NT
			🕀 🛅 Digi		Full Control	BUILTIN\Adm
	Manage		🕀 📄 Intel		Full Control	AUTORITE NT
	terre et		🕀 📄 Java		Full Control	BUILTIN\Adm
	Inspect		🕀 🗎 🗎 Micr		Full Control	BUILTIN\Adm
		- 2. Performance Log Osers	🕀 🛅 ODE		Full Control	AUTORITE NT
0	WORKING HOURS	Performance Monitor Users Power Users	😣 🚞 Part		Full Control	AUTORITE NT
\sim		- 2. Remote Desktop Users	🕀 🚞 Poli		Full Control	AUTORITE NT
±+.		Remote Management Users		isteredApplications	Full Control	AUTORITE NT
14	SECURE DESKTOPS		🗉 🧰 VMv		Full Control	AUTORITE NT
				W6432Node	Full Control	AUTORITE NT
	ENDPOINTS	- 2. Users	🖃 📂 SYSTEM	vationBroker	Full Control Full Control	BUILTIN\Adm AUTORITE NT
	ENDPOINTS	2 Dummy	⊞		Full Control	BUILTIN\Adm
		D aniny	⊕ Con ⊕ Con		Full Control	BUILTIN\Adm ¥
ሰ	RANSOMWARE		t in the second	0030002	run control	BUILTIN/Adm +
潋	SETTINGS	< >	O Files and Fold	ers Registry	O Printer	rs

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:

	Rights are granted or	r denied groups are to account	ted rights from oken into		
An access rule is created including all rights AddAccessRules	User or groups is not granted any rights	Rights are granted	Rights are denied	User or groups is granted Read	An access rule is created denying Read AddAccessRules
An access rule is created denying ChangePermissions and TakeOwnership AddAccessRules	User or groups is granted full control but should not	•		User or groups is granted ListDirectory	An access rule is created denying ListDirectory AddAccessRules
An access rule is created denying Write and Delete AddAccessRules	User or groups is granted modify but should not	•			
If rights are applies on a director set at object (ObjectInherit) an (ContainerInherit)				_	

Documentation:

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

<u></u> т	Splus Advanced Security						- [×
	Ê		EDSECURITY	🖊 - Ultim	ate Protectio	n		
ŵ	НОМЕ	Refresh	Q Enable Audit	O View #	Audit			
Q	EVENT VIEWER	Select a file or a folder to ed	it permissions	Permissions				
		Name	^		Name		Permissions	
O	HOMELAND	🗉 📂 CA		2		AGE D'APPLICATION\TOUS L		
			111.0g2xmuCp	2	AUTORITÉ DE PACK	AGE D'APPLICATION\TOUS L	Read	
\mathbf{X}	BRUTEFORCE	Backupparam		2	AUTORITE NT\Systè	me	Modify	
~~		Documents and	Settings	2	BUILTIN\Administra	teurs	Modify	
\square	IP ADDRESSES	Cogs DerfLogs		2	BUILTIN\Utilisateur	5	Read	
V	in Abbitesses	Program Files		2	NT SERVICE\Trustee	dinstaller	Full Control	
	PERMISSIONS	Program Files (x8) Program Files (x8)) Common File						
	Manage	⊞ 🛅 Java ⊞ 🛅 Microsoft	Shared					
	Inspect	Gracle Gracle Gracle Gracle						
0	WORKING HOURS	 Image: Big System Image: Big System						
萍	SECURE DESKTOPS	⊕ Internet Explain ⊕ ☐ Java ⊕ ☐ Microsoft.NE						
	ENDPOINTS	Image: Barrier Bar						
₿	RANSOMWARE	Constall Info	rmation V					
繱	SETTINGS	Files and Folders	Registry O Printers					

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:

Ŷ T	Splus Advanced Security			– 🗆 X
	Û		JRITY - Ultimate Protection	
ŵ	HOME	Refresh Q Disable A	Audit 🔘 View Audit	
Q	EVENT VIEWER	Select a file or a folder	Permissions	
		Name	Name	Permissions
\odot	HOMELAND	🖃 🃂 CA	WIN-A1L00CN0E56\Administrateurs	Full Control
		🗉 🧰 SRecycle.Bin	WIN-A1L00CN0E56\Laura	Full Control
$\mathbf{\vee}$	BRUTEFORCE	Adatabasefii1L0q2xmuCp Backupparam	WIN-A1L00CN0E56\Utilisateurs	Read
×X	DRUTLIORCE	Documents and Settings		
Ø	IP ADDRESSES	Authorization Change Audit	X	
	PERMISSIONS		led for the selected file or folder.	
	Manage			
	Inspect	€ €	ОК	
0	WORKING HOURS			
埣	SECURE DESKTOPS			
	ENDPOINTS	Windows Description Windows Description Description		
∂	RANSOMWARE	BOOTNXT lang.ini pagefile.sys		
繱	SETTINGS	<	-	

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

🖤 TSplus Advanced Security				-	
		ECURITY	- Ultimate Protection		
М НОМЕ	Refresh Q Disa	ble Audit	O View Audit		
	Select a file or a folder	Permissio	ins		
	Name		Name	Permissions	
	🖃 📂 CA	2	WIN-A1L00CN0E56\Administrateurs	Full Control	
•	🕀 🧰 SRecycle.Bin	2	WIN-A1L00CN0E56\Utilisateurs	Read	
IP ADDRESSES	 Image: Book of the second seco				
	Program Files Common Files Fichiers communs				
Manage	Internet Explorer				
Inspect	Constall Information Durinstall Information During VMware During Windows Defender				
	Windows Media Player Windows Multimedia Player				
Ź↓ SECURE DESKTOPS	 				
	Windows Portable Device Device Windows Sidebar Device Windows Apps	s			
	WindowsPowerShell desktop.ini Program Files (x86)				
SETTINGS	Program Data	-			

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

Ŷ T	Splus Advanced Security					-
	٢		CEDSECURIT	<mark>Y</mark> - Ultim	nate Protection	
ሴ	HOME	A Refresh	Q Enable Audit	O Viev	/ Audit	
Q	EVENT VIEWER	Select a registry key to e	edit permissions	Permissio	ns	
•		Name	^		Name	Permissions
O	HOMELAND	😑 📂 HKEY_LOCAL_M		음	AUTORITÉ DE PACKAGE D'APPLICATIO	N\TOUS L Read
-		HARDWARE		옰	AUTORITE NT\RESTRICTED	Read
×	BRUTEFORCE	E CFI	т	2	AUTORITE NT\Système	Full Control
5		FAC:		음	BUILTIN\Administrateurs	Full Control
3	IP ADDRESSES			2	Tout le monde	Read
-	PERMISSIONS Manage	Constant	MAP			
	Inspect	🖃 🃂 SYSTEM				
J	WORKING HOURS	Activatic	Set001 Set002 reConfig			
萍	SECURE DESKTOPS	 Image: Book of the second seco	dDevices			
	ENDPOINTS	Resource Resource Resource RNG				
0	RANSOMWARE	<	>			
礅	SETTINGS	Files and Folders	Registry O Printers			

<u></u> т	Splus Advanced Security					– 🗆 X
			EDSECURITY	🖊 - Ultima	ate Protection	
ŵ	НОМЕ	🗘 Refresh	Q Enable Audit	O View /	Audit	
Q	EVENT VIEWER	Select a printer to edit perm	issions	Permissions		
•		Name			Name	Permissions
\odot	HOMELAND	🖃 📂 Printers		2	AUTORITÉ DE PACKAGE D'APPLICATION\TOUS L	Print
-		Universal Printer Microsoft XPS D		2	BUILTIN\Administrateurs	Print, Manage Printer
\mathbf{X}	BRUTEFORCE	Microsoft Print t		2	CREATEUR PROPRIETAIRE	
				2	Tout le monde	Print
Ø	IP ADDRESSES					
	PERMISSIONS					
	Manage					
	Inspect					
0	WORKING HOURS					
埣	SECURE DESKTOPS					
ㅁ	ENDPOINTS					
₿	RANSOMWARE	<	>			
鐐	SETTINGS	○ Files and Folders ○	Registry			

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:

۷	TSplus Adv	vanced Security		- 🗆 X
٢	ADVANCEDSECU	JRITY - Ultimate Prote	ection	
П номе	Users and Groups Advanced View	O Not configured for this user/grou	цр	
	Switch View Add user/group	 Always authorize Always block 		
	Subsers	O Authorize only during these time	ranges:	
	- 2 GRYFFINDOR\harry - 2 GRYFFINDOR\hermione	🧹 Monday:	09:00 to 17:30	A V
BRUTEFORCE	- & GRYFFINDOR\ron - & HUFFLEPUFF\cedric	✓ Tuesday:	09:00 to 17:30	A V
IP ADDRESSES	- & HUFFLEPUFF\helga - & RAVENCLAW\cho	✓ Wednesday:	09:00 to 17:30	× v
	- 올 RAVENCLAW\luna - 올 RAVENCLAW\rowena	Thursday:	09:00 to 17:30	×
-	SLYTHERIN\draco	Friday:	09:00 to 17:30	× •
	- ≗ TEACHER\albus ≗ TEACHER\minerva	Sunday:	09:00 to 17:30	×
才 secure desktops	Z TEACHER\severus		UTC+01:00) Brussels, Copenhagen, Madrid, P	
		default):		
_				×
		Whitelisted users will always be able to This feature prevents a user from openir	o connect. ng a new session outside of his authorized time re	anaes, and loa him off
袋 settings		automatically when his working hours of	are over.	
ල්සු license				

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 <u>Settings > Advanced > Working Hours</u>.

Users/Groups rules priorities

When a user opens a new session on the server:

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

🖤 TSplus Advanced Security		- D >
٢		RITY - Ultimate Protection
	Users and Groups - Local computer	Not configured for this user/group
M HOME	E- & Users	
Q EVENT VIEWER	옾 Administrateur 옾 Caleb	Configured for this user/group:
- CHENT MENER		
	Laura (whitelisted)	-
		Kiosk Mode
	-2. Administrateurs	Prevent a connected user from running prohibited actions.
**	- 2 Duplicateurs	
IP ADDRESSES		
~		
PERMISSIONS	Opérateurs d'impression	
		Secured Desktop Mode
WORKING HOURS	Opérateurs de configuration réseau	The connected user will not be allowed to browse server resources behind his own Remote Desktop boundaries.
	Opérateurs de sauvegarde Serveurs Accès Distant RDS	Kenter Desktop boundares.
SECURE DESKTOPS	- Serveurs Gestion RDS	
	Serveurs RDS Endpoint	
	- System Managed Accounts Group	
0	Utilisateurs Utilisateurs avec pouvoir	Windows Mode
	Utilisateurs de gestion à distance	- This is the default Windows user session security model.
<i>.</i>	Utilisateurs de l'Analyseur de perfor 2. Utilisateurs du Bureau à distance	
SETTINGS		
	Utilisateurs du modèle COM distribi	Customize Security Level
UCENSE	< >	Whitelisted users will always use "Windows Mode".

Customization

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

Desktop Security:

Pesktop Security Disks Control Applications Control Currently custor Remove Recycle Bin WIN-A1L0C Remove My Documents Remove My Recent Documents WIN-A1L0C Remove My Music Currently custor Win-A1L0C Remove My Music Currently custor Win-A1L0C Remove My Pictures Remove My Pictures Currently base Remove Programs Currently base Kios Remove Help and Support Kios Kios Remove Network No Network Neighborhood Remove Network No Network Neighborhood Remove Context Menu Restrict right click Disable Task Manager Disable System Management programs Disable Vindows key No No Active Desktop No Active Desktop No No Close M No Disconnect No Disconnet No Internet Explorer	
Remove Recycle Bin WIN-A1L00 Remove My Documents WIN-A1L00 Remove My Music Currently Used Programs Remove My Pictures Currently Used Programs Remove Help and Support Kios Remove Printers Remove Printers Remove Control Panel Kios Remove Network Disable System Management programs Disable Task Manager Disable System Management programs No No Active Desktop No Active Desktop No Disconnect No No Ranage My Computer No Delete Printer No Delete Printer	tomining
Remove My Recent Documents WIN-A1LOC Remove My Music Currently Used Programs Remove Programs Currently base Remove Programs Kios Remove Control Panel Kios Remove Network Disable System Management programs Disable System Management programs Disable System Manager No Rolder options No Active Desktop No Close No Delete Printer	stomizing
 Remove My Recent Documents Remove My Nusic Remove My Pictures Remove Frequently Used Programs Remove Programs Remove Programs Remove Programs Remove Programs Remove Printers Remove Printers Remove Context Menu Restrict right Click Disable System Management programs Disable System Manager Disable System Manager Disable System Manager No Folder options No Active Desktop No Close No Manage My Computer No Delete Printer 	
Remove My Pictures Currently Used Programs Remove Frequently Used Programs Currently base Remove Programs Kios Remove Control Panel Kios Remove Printers Remove Network No Network Neighborhood Programs Restrict right click Disable System Management programs Disable Task Manager Disable Task Manager No No Folder options No Active Desktop No Disconnect No No Ranage My Computer No Delete Printer No Delete Printer	UUCINUE36/JONI
Remove Frequently Used Programs Remove Programs Remove Help and Support Remove Control Panel Remove Printers Remove Network No Network Neighborhood Restrict right click Disable System Management programs Disable System Manager Disable Task Manager No Folder options No Active Desktop No Close No Manage My Computer No Delete Printer	
Remove Programs Kios Remove Help and Support Kios Remove Control Panel Kios Remove Printers Remove Network No Network Neighborhood Disable System Management programs Disable System Management programs Disable System Management programs Disable System Manager No Folder options No Folder options No Active Desktop No Disconnect No Close No Delete Printer No Delete Printer	
Remove Help and Support Kios Remove Control Panel Kios Remove Printers Kios Remove Network Kios No Network Neighborhood Kios Restrict right click Kios Disable System Management programs Kios Disable System Management programs Kios No Folder options Kios No Active Desktop Kios No Close No Disconnect No Delete Printer No Delete Printer	sed on
Remove Control Panel Nos Remove Printers Remove Network No Network Neighborhood Remove Context Menu Restrict right click Disable System Management programs Disable Task Manager Remove Collect Menu No Folder options No Folder options No Disconnect No Close No Close No Close No Close Pointer No Disconnect	
Remove Printers Remove Network No Network Neighborhood Remove Context Menu Restrict right click Disable System Management programs Disable System Manager Disable Windows key No Folder options No Active Desktop No Disconnect No Disconnect No Close No Close No Delete Printer	osk Mode
Remove Network No Network No Network Neighborhood Remove Context Menu Restrict right click Disable System Management programs Disable System Manager Disable Task Manager Disable Windows key No Folder options No Active Desktop No Active Desktop No Disconnect No Close No Manage My Computer No Delete Printer	
Wo Network Neighborhood Remove Context Menu Restrict right click Disable System Management programs Disable Task Manager Disable Windows key No Folder options No Disconnect No Close No Kanage My Computer No Delete Printer	
Vermove Context Menu Restrict right click Disable System Management programs Disable Task Manager Disable Windows key No Folder options No Active Desktop No Disconnect No Disconnect No Close No Close No Conse No Delete Printer	
Visable System Management programs Disable Task Manager Disable Windows key No Folder options No Active Desktop No Disconnect No Close No Manage My Computer No Delete Printer	
Disable Task Manager Disable Windows key No Folder options No Active Desktop No Disconnect No Close No Close No Manage My Computer No Delete Printer	
Disable Windows key No Folder options No Active Desktop No Disconnect No Close No Cose No Manage My Computer No Delete Printer	
Vio Folder options Vio Active Desktop Vio Disconnect Vio Close Vio Manage My Computer Vio Delete Printer	
🖓 No Active Desktop 🖓 No Disconnect 🖓 No Close 🖓 No Manage My Computer 🖓 No Delete Printer	
🗹 No Disconnect 🗸 No Close 🗸 No Manage My Computer 🖉 No Delete Printer	
∑ No Manage My Computer ∑ No Delete Printer	
No Delete Printer	
No Internet Explorer	

Disks Control:

			Secu	rity Level	Customiz	zation	
esktop Se	curity Disks Co	ontrol Applic	ations Control				Currently customizing
Hide Sele	cted Disks						
A 🔽	В	∠ c	D	E	F	G	WIN-A1L00CN0E56\John
И		V J	К	✓ L	м	⊠ N	
⊘	P	Q	R	✓ s	Г	V	Currently based on
V	✓ w	X	V Y	✓ z			Kiosk Mode
		ct all			Unselect all		
Dami Ann	ess to Selected [Diala					
	В	C C	D	E	F	G	
⊠н		V J	К	<u>ا</u> ا	м 1	<u>м</u>	
	P	⊠ Q	R	⊠ s	Г	ν	
\sim 0	⊻ w	✓ X	Y 🗸	☑ z			
∑ o ∑ v							

Applications Control:

sktop Security	Disks Control Ap			Customization	
C:5_	Σ	plications Contro			
	2	E A J			Currently customizing
	powershell.exe	taskmgr.exe	mmc.exe	gpedit.msc	WIN-A1L00CN0E56\John
regedit.exe	powershell_ise	iexplore.exe			Currently based on Kiosk Mode
	Applic	ations listed abov	e will be prohibit	ted. Remove	

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.

TSplus Advanced Security		– 🗆 X
	TS ADVANCEDSE	
ф номе	Users - Local computer	O This user can connect from any Device
	E-2 Users -2 Admin	This user Device name will be checked and must be in this list:
	- 2 Caleb	Device Name
	···· 올 John ···· 올 Laura (whitelisted)	JOHN-TABLET
HOMELAND		JOHN-PC
IP ADDRESSES		
		Add Remove
		Whitelisted users will always be able to connect.
SETTINGS		This Endpoint protection enables to control the Device names of any incoming session. A logon from any invalid Device name will be blocked.
ତିଳ୍ଫ LICENSE		

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:

				DITY	Ultimate Dear				💐 Lite M	od
			EDSECC	JI-(11 Y -	Ultimate Pro	lection		Help	English	
1	HOME	+ Add IP Address	D Edit IP A	ddress	× Remove IP A	ddress(es)	() Refre	sh Hacker IP	Q WHOI	s
)	HOMELAND	IPs in the allow list will be ign	ored by TSplus Advanc	ed Security and wi	i not be blocked by Ho.	neland Access i	Protection or	Bruteforce Attacks I	Defender features	s
		614 349 459 IP address(es) b	locked							
	BRUTEFORCE	IP Address	Country	Status		Date		Description		_
`		1.19.0.1-1.19.255.254			acker IP Protection	23 mai 2022	12,19,01	Know malicious	ID Addresses	-
		1.32.128.1-1.32.191			acker IP Protection	23 mai 2022		Know malicious		
)	BLOCKED IP ADDRESSES	100.64.0.1-100.127	Singapore		lacker IP Protection	23 mai 2022		Know malicious		
		101.101.96.1-101.1			lacker IP Protection	23 mai 2022		Know malicious		
₿ R	RANSOMWARE	101.134.0.1-101.13	China		lacker IP Protection	23 mai 2022		Know malicious		
		101.203.128.1-101	China		lacker IP Protection	23 mai 2022		Know malicious		
		101.248.0.1-101.24			lacker IP Protection	23 mai 2022		Know malicious		
]	PERMISSIONS	101.42.0.1-101.42.2			lacker IP Protection	23 mai 2022		Know malicious		
		102.192.0.1-102.20	china		lacker IP Protection	23 mai 2022		Know malicious		
`	WORKING HOURS	102.208.0.1-102.21			lacker IP Protection	23 mai 2022		Know malicious		
'	WORKING HOURS	102.212.0.1-102.21			lacker IP Protection	23 mai 2022		Know malicious		
		102.214.0.1-102.21			acker IP Protection	23 mai 2022	23:18:01	Know malicious	IP Addresses	
י פ י כ	SECURE DESKTOPS	102.215.0.1-102.21		Blocked - H	acker IP Protection	23 mai 2022	23:18:01	Know malicious	IP Addresses	
		102,215,128,1-102,		Blocked - H	acker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
		102.215.160.1-102		Blocked - H	lacker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
ī	ENDPOINTS	102.215.184.1-102			lacker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
		102.215.192.1-102	South Africa	Blocked - H	lacker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
	EVENTS	102.215.200.1-102		Blocked - H	lacker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
•		102.215.216.1-102		Blocked - H	lacker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
		102.215.224.1-102	Ivory Coast	Blocked - H	lacker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
3	SETTINGS	102.216.20.1-102.2		Blocked - H	lacker IP Protection	23 mai 2023	23:18:01	Know malicious	IP Addresses	
		E 102.216.23.1-102.2	South Africa	Ringkod H	lacker IP Protection	23 mai 2022	23:18:01	Know malicious	TD Addresses	

As a result, the feature should create approx. 600 000 000 blocking 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.

\bigcirc	Homeland - 683 remote accesses denied since 05 mai 2022 22:40:16		Bruteforce - 0 IP address blocked	Synchronized Hacker IP addresses protects you computer against 614 348 888 IP addresses.
0	Working Hours is not	enabled.	🖄 Secure Desktops is not enabled.	Endpoints is not enabled.
	Date	Feature	Message	
X		\odot		
Ð	23 mai 2022 22:54:03	۲	Synchronized Hacker IP addresses protects your computer :	against 614 348 888 IP addresses.
0	23 mai 2022 22:48:47	S	A remote connection has been authorized from IP address authorized country France	212.106.118.150 because 212.106.118.150 is associated with the
0	23 mai 2022 22:40:15		A connection has been authorized for user NS204950\vmac not enabled for this user	dmin from computer .A9HX6ZPP0NM0G3 because this feature is
0	23 mai 2022 22:40:15	S	A logon request has been granted for user NS204950\vmac	dmin because NS204950\vmadmin is allowed
Ð	23 mai 2022 22:40:15	\oslash	A new session RDP-Tcp#1 (#9) has started for user NS20495 90.3.0.31	i0\vmadmin from client .A9HX6ZPP0NM0G3 and IP address
0	23 mai 2022 22:40:11	S	A remote connection has been authorized from IP address	90.3.0.31 because 90.3.0.31 is allowed
×	23 mai 2022 22:35:29	S	A remote connection was denied from IP address 43.129.35 Homeland on 08 mai 2022 16:37:50	.207 (Indonesia). This IP address was originally blocked by
Ð	23 mai 2022 22:30:03	8	Synchronized Hacker IP addresses protects your computer a	against 614 348 888 IP addresses.
0	23 mai 2022 22:28:41	S	A remote connection has been authorized from IP address authorized country United States	208.64.33.85 because 208.64.33.85 is associated with the
×	23 mai 2022 22:22:49	S	A remote connection was denied from IP address 43.131.94 Homeland on 09 mai 2022 19:49:10	.145 (Russia). This IP address was originally blocked by
Сору				

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.

Homeland - 683 remote accesses denied since 05 mai 2022 22:40:16	Bruteforce - 0 IP address blocked	Synchronized Hacker IP addresses protects your computer against 614 348 888 IP addresses.
Working Hours is not enabled.	🔀 Secure Desktops is not enabled.	Endpoints is not enabled.

TS ADVANCEDSECURITY

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

	Date	Feature	Message							
Ø	23 mai 2022 23:02:57	\odot	A remote connection w on 06 mai 2022 03:42:3		d). This IP address was originally blocked by Homeland					
Ø	23 mai 2022 22:54:45	S	A remote connection w on 06 mai 2022 03:42:3		d). This IP address was originally blocked by Homeland					
0	23 mai 2022 22:54:03	⊗	Synchronized Hacker If	Paddresses protects your computer against 614	4 348 888 IP addresses.					
\oslash	23 mai 2022 22:48:47	S	A remote connection h authorized country Fra	mote connection has been authorized from IP address 212.106.118.150 because 212.106.118.150 is associated with the horized country France						
\oslash	23 mai 2022 22:40:15		A connection has been not enabled for this us		computer .A9HX6ZPP0NM0G3 because this feature is					
\oslash	23 mai 2022 22:40:15	Q	A logon request has b	A logon request has been granted for user NS204950\vmadmin because NS204950\vmadmin is allowed						
0	23 mai 2022 22:40:15	\oslash	A new session RDP-Tcp 90.3.0.31	#1 (#9) has started for user NS204950\vmadmir	n from client .A9HX6ZPP0NM0G3 and IP address					
0	23 mai 2022 22:40:11		A remote connection		ise 90.3.0.31 is allowed					
S		U	A remote connection	Сору	55 30.5.0.51 IS allowed					
x	23 mai 2022 22:35:29		A remote connection Homeland on 08 ma	Copy IP Address	a). This IP address was originally blocked by					
-			Homeland on U8 ma	Unblock IP address						
0	23 mai 2022 22:30:03	⊗	Synchronized Hacke	Unblock and add to IP addresses allow list	: 888 IP addresses.					
\oslash	23 mai 2022 22:28:41	S	A remote connection h authorized country Un	as been authorized from IP address 208.64.33.8 ited States	15 because 208.64.33.85 is associated with the					
Сору	/ Copy IP A	idress Unbl	ock IP address Unblock a	nd 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:

۷		Splus Advanced	Security					x
		SECURIT	' Y - Ultimate Prot	tection				
П НОМЕ	Users and Groups Advanced View	0 N	ot configured for this user/gr	oup				
	Switch View Add u	er/group	ways authorize ways block					
	SRYFFINDOR\godric		uthorize only during these tin	ne ranges:				
	-2 GRYFFINDOR\harry -2 GRYFFINDOR\harry		Monday:	09:00	to		~	
BRUTEFORCE	-2 GRYFFINDOR\ron -2 HUFFLEPUFF\cedric		✓ Tuesday:	09:00	to	17:30	~ ~	
IP ADDRESSES	- & HUFFLEPUFF\helga - & RAVENCLAW\cho		Vednesday:	09:00	to		~	
	- 2 RAVENCLAW\luna - 2 RAVENCLAW\rowena		Thursday:	09:00			^ ~	
	- 2 SLYTHERIN\draco	2	Friday:	09:00	to		~	
	- 🚨 TEACHER\albus		Saturday:	09:00	to		<u>^</u>	
 ✓ SECURE DESKTOPS	EACHER\minerva Severus		Sunday:	09:00			^ ~	
74 SECONE DESKIOLS	Groups	Selec	t timezone for user or group ult):	((UTC+01:00) Brussels, Cope	nhagen, M	ladrid, Paris is	applied	by
								~
		White	elisted users will always be able :	to connect.				
			eature prevents a user from oper natically when his working hour		his authorize	ed time ranges,	and log I	him off
SETTINGS			ļ					
	L						_	_

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:

👻 T:	Splus Advanced Security		-	×
	Û			
ŵ	HOME	+ Add User × Remove User(s)		
Q,	EVENT VIEWER	Users in the whitelist will be ignored by TSplus Advanced Security and their settings will not be applied.		
Q	HOMELAND	S KALEVALA\administrator		
⋇	BRUTEFORCE			
Ø	IP ADDRESSES			
	PERMISSIONS			
U	WORKING HOURS			
萍	SECURE DESKTOPS			
	ENDPOINTS			
₿	RANSOMWARE			
鐐	SETTINGS			
	Users			
	Programs	v		

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.

Û T	Splus Advanced Security	– 🗆 X
	٢	ADVANCEDSECURITY - Ultimate Protection
S	HOMELAND	Add Application X Remove Application(s)
╳	BRUTEFORCE	Enter a program file path to add a program to the Ransomware Protection program whitelist. This executable will be able to create, change and delete your personal files without triggering Ransomware Protection.
Ø	IP ADDRESSES	C:\Program Files (x86)\RDS-Tools\ServerGenius\ServerGenius.exe C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
	PERMISSIONS	
0	WORKING HOURS	
萍	SECURE DESKTOPS	
	ENDPOINTS	
₿	RANSOMWARE	
鐓	SETTINGS	
	Users	
	Programs	
	Advanced	
©7	LICENSE	•

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:

	^				1
	🗘 🛛 Backup / Restore				1
BRUTEFORCE	Roduct				
IP ADDRESSES	Homeland Bruteforce	Name Pin Code Contribute to improve product by sending anonymous data	Value Yes		
	 Firewall Working Hours Endpoints 	Computer Nickname Data Retention Policy	WIN-A1L00CN0E56 259200		
	🕸 Logs				
SECURE DESKTOPS					
RANSOMWARE					
SETTINGS					
Users					
Programs					
Advanced					
	•				
		ackup/Restore		×	

	Backup	
Restore		

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 <u>SQLite database engine</u>.

data				- 0
$\leftarrow \rightarrow$ \checkmark \uparrow \square \Rightarrow This PC :	Local Disk (C:) > Program Files (x86)	> TSplus-Security > data 🛛 🗸	ප Search data	
TSplus-Security	^ Name	Date modified	Туре	Size
archives	🚳 data	10/21/2019 4:52 PM	Data Base File	100 KB
data	ransomware-internal-wh	nitelist.json.old 3/19/2019 7:01 PM	OLD File	1 KB
drivers				
langs				
logs	~			
2 items				

Advanced - Product Settings

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

<u></u> Ф Т	Splus Advanced Security				- 0	×
	Ŵ	TS ADVANCEDS	ECURITY - Ultimate Protection			
Q	HOMELAND	A Backup / Restore				
×	BRUTEFORCE					
Ø	IP ADDRESSES	≪ <mark>∖ Product</mark> ♥ Homeland ₩ Bruteforce	Name Pin Code Contribute to improve product by sending anonymous data	Value Yes		
	PERMISSIONS	 Firewall Working Hours Endpoints 	Computer Nickname Data Retention Policy	WIN-A1L00CN0E56 259200		
0	WORKING HOURS	章 Logs				
萍	SECURE DESKTOPS					
	ENDPOINTS					
⋳	RANSOMWARE					
繱	SETTINGS					
	Users					
	Programs					
	Advanced					
©.	LICENSE	v				

plus Advanced Security - Edit Setting	×
Pin Code	
Description:	
TSplus Advanced Security will ask for a password if this value is not empty.	~
	v
Value:	
1234	

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):

Contribute to improve product by sending anonymous data	
Description:	
Allow TSplus Advanced Security to send anonymous usage statistics and exception reports to support further improvments and features.	~ >
Value:	
Yes	~

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:

TSplus Advanced Security - Edit Setting	×
Computer Nickname	
Description:	
The computer nickname defines a more relevant and fr name for your computer. Email alerts employ the comp nickname in their subjects.	
	\sim
Value:	,
ADMIN-PC	
Save	Cancel

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 databa A backup is performed before each database cleanup. This po is defined in minutes. Default data retention policy is 259 200 minutes, i.e. 6 months.	olicy
Value:	
259200	

Advanced - Homeland Settings

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

TSplus Advanced Security			-	- 🗆	×
;	ADVANCED <mark>S</mark>	ECURITY - Ultimate Prot	ection		
• HOMELAND	🗘 🛛 Backup / Restore				
IP ADDRESSES	Product Homeland Houteforce	Name Watched Processes Watched Ports	Value HTML5service		
	Firewall S Working Hours	Use Legacy	No		
	回 Endpoints 総 Logs				
☆ SECURE DESKTOPS					
SETTINGS					
Users					
Programs					
Advanced					
ତଙ୍କ LICENSE					

TSplus Advanced Security - Edit Setting	×
Watched Processed	
Description:	
Check connections on the following processes (semi-colon separated)	^
Value:	~
HTML5service	
Save Cancel	

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.

Splus Advanced Security - Edit Setting Watched Ports	×
Description:	
Check connections on additional ports (semi-colon separated) Watched ports always included by default are rdp, telnet and vnc ports.	. ^
Value:	~
lue:	~
Save Cancel	

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.

2 Product	Name	Value	
Homeland Bruteforce	Homeland Detection M Watched Processes	Aechanism Event Tracing for Windows HTML5service	
 Firewall Working Hours Endpoints Ransomware Protection Logs 	Watched Ports	TSplus Advanced Security - Edit Setting	×
		Homeland Detection Mechanism	
		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 protects capture for 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".

🖤 TSplus Advanced Security				- 0	×
		ECURITY - Ultimate Protection			
	A Backup / Restore				
IP ADDRESSES	 № Product ♥ Homeland ₩ Bruteforce 	Name Ignore Local and Private IP Addresses	Value No		
	Firewall				
	ロー Endpoints 総 Logs				
段 SETTINGS					
Users					
Programs					
Advanced					
ତଙ୍ଗ LICENSE	•				

^
V

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:

ŷ T	Splus Advanced Security				-	×
			ECURITY - Ultimate Pro	otection		
Q	HOMELAND	A Backup / Restore				
⋇	BRUTEFORCE					
Ø	IP ADDRESSES	Noduct S Homeland M Bruteforce	Name Use Windows Firewall Unblock after	Value Yes O		
	PERMISSIONS	Firewall Working Hours				
0	WORKING HOURS	교 Endpoints Logs				
萍	SECURE DESKTOPS					
□	ENDPOINTS					
⋳	RANSOMWARE					
钧	SETTINGS					
	Users					
	Programs					
	Advanced					
©⊤	LICENSE	•				

Splus Advanced Security - Edit Setting	×
Use Windows Firewall	
Description:	
If Yes, then the offending IP addresses will be blocked using Windows Firewall. TSplus Advanced Security firewall will be u otherwise.	sed
Value:	~
No	~
Save Cance	I

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:

Splus Advanced Security - Edit Setting	×
Unblock after	
Description:	
Change this setting to automatically unblock IP addresses after certain amount of time (in minutes). Default value is 0, disabling this feature.	
	v
Value:	
0	

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".

TSplus Advanced Security - 6.3.	5.23				. 🗆 X
		SECURITY - Ultimate Protection		💐 Lite Mo	de
	ADVANCED		(?) Help	English	•
û номе	- Backup / Restore				
	Normaland	Name Use Windows Firewall	Value Yes		
	Bruteforce Firewall S Working Hours	Unblock after Enable Hacker IP addresses automatic synchronization Contribute to improve Hacker IP list	0 Yes Yes		
	Endpoints Bansomware Protection B Logs	TSplus Advanced Security – Edit Setting Enable Hacker IP addresses automatic synchroniz	×		
	iga Logs	Description:			
		Keep your machine protected against known threat: line attacks, on-line service abuse, malwares, botnet cybercrime activities with the Hacker IP Protection. Si Updates Services subscription is required.	s and other		
		opuaces services subscription is required,			
			_		
		Value: Yes	•		
段 SETTINGS —]				
Advanced		Save	Cancel		
Users	1				

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".

Comparison CEDSECURITY - Ultimate Protection Orego Help English	_
(2) Help English	
	•
HOME Backup / Restore Backup / Restore	
BRUTEFORCE Name Value C Homeland Use Windows Firewall Yes Butleforce Unblock after 0	I
BLOCKED IP ADDRESSES BLOCKED IP ADDRESSES Contribute to Improve Hacker IP list Yes	
RANSOMWARE Endpoints Bransomware Protection Toplus Advanced Security - Edit Setting Solution	
PERMISSIONS Contribute to improve Hacker IP list Description:	
WORKING HOURS Allow TSplus Advanced Security to send anonymous usage statistics to enhance protection against Hacker IP.	
*/: secure desktops	
Value: Yes:	
хар setungs	
Advanced Save Cancel	

Advanced - Working Hours Settings

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

Ŷ T	Splus Advanced Security			-	×
	٢	TS ADVANCED	ECURITY - Ultimate Protection		
S	HOMELAND	A Backup / Restore			
×	BRUTEFORCE				
Ø	IP ADDRESSES	≪s Product S Homeland S Bruteforce	Name Scheduled warning message before logoff Warning message	Value 5 Warning: you will be logged	
	PERMISSIONS	Firewall Vorking Hours	Default timezone	(UTC+01:00) Brussels, Copen	
0	WORKING HOURS	교 Endpoints 왕 Logs			
萍	SECURE DESKTOPS				
□	ENDPOINTS				
⋳	RANSOMWARE				
鐐	SETTINGS				
	Users				
	Programs				
	Advanced				
☞	LICENSE	*			

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.

Splus Advanced Security - Edit Setti	ng X
Scheduled warning message before	ore logoff
Description:	
Users are warned when working he parameter allows you to change its minutes before working hours end	schedule in number of
Value:	~
5	
Save	Cancel

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.

TSplus Advanced Security - Edit Setting	×
Warning message	
Description:	
Warning message sent to users before session closes due to working hours restrictions. Placeholders named %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% and %ENDINGHOURS% 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.	~
Value:	
hours on %DAY% are from %STARTINGHOURS% to %ENDINGHOUR	S%).
Save Cancel	

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

Default timezone	
Description:	
Set the default timezone.	^
	v
Value	
Value:	
Value: (UTC+01:00) Brussels, Copenhagen, Madrid, Paris	

Advanced - Endpoints Settings

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

Ŷ T	Splus Advanced Security				-	\times
	Û		ECURITY - Ultimate Protection			
Q	HOMELAND	A Backup / Restore				
Ж	BRUTEFORCE					
0	IP ADDRESSES	ి _స Product ✔ Homeland ✔ Bruteforce	Name Allow Connection From Web Portal	Value No		
	PERMISSIONS	Firewall				
0	WORKING HOURS	回 Endpoints 総 Logs				
萍	SECURE DESKTOPS					
□	ENDPOINTS					
⋳	RANSOMWARE					
ŝ	SETTINGS					
	Users					
	Programs					
	Advanced					
©7	LICENSE	~				

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.

TSplus Advanced Security - Edit Setting	\times		
Allow Connection From Web Portal			
Description:			
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 note that this action will diminish your server's security.			
Value:			
No	\sim		
Save Cancel			

Advanced - Ransomware Settings

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

Ŷ	TSplus Advanced Security - 6.	2			_	×
	Ê		SECURITY - Ultimate Protection	() Help	💐 Lite Mo	ode •
_	HOME EVENT VIEWER	🗘 🛛 Backup / Restore				
X ⊘	HOMELAND BRUTEFORCE IP ADDRESSES	 Product Homeland Bruteforce Frewall Working Hours Endpoints Arasomware Protection Icgs 	Name Snapshot Path Ignored Extensions File Snapshots Max Size File Snapshot Retention Registry Snapshot Retention Display Detection Alert Allowed PowerShel and CMD scripts	Value C:\Program Files (x86)\1 1 300 300 Yes C:\Users\user\mycustor		
8 [] (0	RANSOMWARE PERMISSIONS WORKING HOURS					
	SECURE DESKTOPS ENDPOINTS SETTINGS					
	Advanced Users					

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

TSplus Advanced Security - Edit Setting	×
Snapshot Path	
B	
Description:	
Snapshot Path defines the directory where Ransomware Protection stores file snapshots. The specified directory must exist. Default value: C:\Program Files (x86)\TSplus-Security \snapshots	
Value:	· ·
C:\Program Files (x86)\TSplus-Security\snapshots	
Save Cancel	

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

TSplus Advanced Security - Edit Setting	×	
Ignored Extensions		
Description:		
By default, Ransomware Protection ignores well-known extensions of temporary files when looking for ransomware activity. This setting allows you to define custom ignored extensions. (semicolon separated)		
Value:	~	
Save Can	icel	

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.

TSplus Advanced Security - Edit Setting	\times	
File Snapshots Max Size		
Provide Hand		
Description:		
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.		
	\sim	
Value:		
0		
Save Cancel		

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)

TSplus Advanced Security - Edit Setting	Х	
File Snapshot Retention		
Description		
Description:		
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)		
	~	
Value:		
300		
Save Cancel		

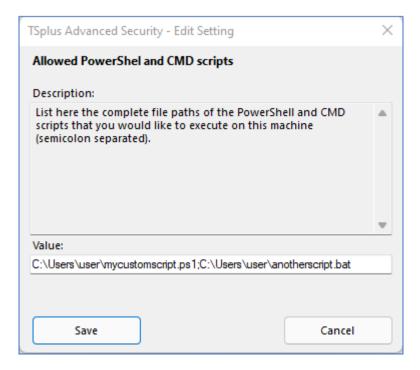
Registry Snapshot Retention: Registry Snapshot Retention defines, in seconds, the retention policy of a registry snapshot.

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

TSplus Advanced Security - Edit Setting	×
Registry Snapshot Retention	
Description:	
Description.	
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 second (i.e. 5 minutes)	
	× .
Value:	
300	
Save Cancel	

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 - 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

TSplus Advanced Security				_)
		DSECURITY - Ultimate Protection			
HOMELAND	A Backup / Restore				
BRUTEFORCE					
IP ADDRESSES	Product Homeland	Name Enable TSplus Advanced Security service log Enable Bruteforce protection service log	Value No No		
	 Firewall Working Hours Endpoints 	Enable Homeland service log Enable Ransomware protection service log	No No		
	袋 Logs	Enable Working Hours Restrictions service log Enable Firewall log Enable TSplus Advanced Security application log	No No No		
SECURE DESKTOPS					
ENDPOINTS					
SETTINGS					
Users					
Programs					
Advanced					

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.