TSplus Advanced Security - Activation de votre licence

Étape 1 : Activer votre licence depuis le mode Lite

Cliquez sur le bouton « Licence d'essai » pour acheter une licence ou sur l'onglet Licence si vous avez déjà une licence et une clé d'activation.



Ensuite, cliquez sur le bouton « Activer votre licence ».

Vous trouverez votre clé d'activation permanente (XXXX-XXXX-XXXX) dans notre e-mail de confirmation de commande.

Si vous souhaitez activer votre abonnement, veuillez entrer votre clé d'abonnement. **S-XXXX-XXXX-XXXX**.

뉯 TSp	lus Advanced Security		-		×
ADV.	ANCEDSECURITY	License			
⊞	Dashboard	ලිද Activate your License			
ය	Firewall	문 Buy Now			
9	Sessions	Rehost an existing license			
₿	Ransomware	C Refresh your license			
Ŵ	Alerts	ලිත Trial License 15 days			
	Reports	Computer ID: Computer name: TSPLUS-SERVER1			
¢3	Settings				
©7	License				
		() User Guide Version 7.1.9.11	l License 15 days - l	BUY NOV	

Si vous ne connaissez pas votre clé d'activation, veuillez passer à l'étape 2. Sinon, passez à l'étape 3.

Étape 2 : Récupérez votre clé d'activation depuis le portail de licence

Pour obtenir votre clé d'activation, connectez-vous à notre <u>Portail de licence</u> et entrez votre adresse e-mail et votre numéro de commande :

<u>Téléchargez le guide de l'utilisateur du portail client</u> pour plus d'informations sur votre portail client.

Votre clé d'activation sera affichée en haut du tableau de bord :

The Customer Portal	×									
() Home	Hello, My License Portal Your activation key is YB6F-500 Control Control									
C Orders	Q Search for licenses	Q Search for licenses S								
- Computers										
Subscriptions	Action Required: Missing Update and Support Services! Update and Support Services are crucial for the automatic delive They also give you access to our Technical Support Team. Please Renew your Subscription	Action Required: Missing Update and Support Services! Update and Support Services are crucial for the automatic delivery of essential updates, including OS compatibility adjustments, critical security fixes, and access to the latest features. They also give you access to our Technical Support Team. Please Renew your Subscription								
S Documentation	Licenses Supports Purchase Licenses	Renew All Supports								
	Product	Date Order Nu	mber Computer	Support	Comment					
	TSplus Advanced Security Ultimate unlimited users	2024-08-23	× Not Activated Activate your license	~	Edit					
(i) Help	TSplus Advanced Security Ultimate unlimited users	2024-08-23	× Not Activated Activate your license	\checkmark	Edit					
	TSplus Advanced Security Ultimate unlimited users	2024-08-23	× Not Activated Activate your license	1	Edit					
	TSplus Advanced Security Ultimate unlimited users	2024-08-23	× Not Activated Activate your license	\checkmark	Edit					
7 0:0 4	TSplus Advanced Security Ultimate unlimited users	2024-08-23	× Not Activated Activate your license	\checkmark	Edit					
SignOut	TSplus Advanced Security Ultimate	2024-08-23	× Not Activated	~						

Étape 3 : Sélectionnez les licences demandées et les services de mise à jour et de support pour les produits installés

Entrez votre clé d'activation et cliquez sur « Suivant ».

License Activation
Please select the license(s) you want to activate on this computer:
TSplus Advanced Security (already activated on this computer)
 Do not activate additional Updates/Support Update/Support Users for TSplus Advanced Security Ultimate edition - 1 year
The licenses listed above are all the licenses currently available for activation on this computer. If you have purchased multiple units, only one will be displayed in this list for this computer, and you will be able to activate the other units on other computers.
< Back Next >

Cochez un ou plusieurs éléments et cliquez sur le bouton « Suivant ». Veuillez noter que vous pouvez activer plusieurs produits en même temps en cochant plusieurs produits et/ou abonnements de support.



Tous vos produits sélectionnés et abonnements de support sont maintenant activés (dans cet exemple, à la fois TSplus avec support et TSplus Advanced Security ont été activés en même temps).

Rafraîchissez votre statut de licence en cliquant sur le bouton correspondant.

t TS	olus Advanced Security		- 0	×
AD∖	ANCEDSECURITY	License		
≣ ⊗	Dashboard Firewall	 G₁ Activate your License C₂ Refresh your license 		
9	Sessions	Licensing ×		
₿	Ransomware	License Status Permanent license		
1 23	Settings	Cra Permanent License Activated - Ultimate Protection edition.		
ଙ	License	Computer ID: OK Computer name: TSPLUS-SERVER1		
		Support renewal date: 2027-03-07		
		Vser Guide Version 7.18.20 Permanent License Activated - Ultimate P	rotection edition.	

Activation de votre licence (Hors ligne)

Veuillez vous référer à la procédure décrite pour TSplus Remote Access : <u>Activer votre licence</u> <u>TSplus (hors ligne)</u>

Rehébergement de votre licence

Veuillez vous référer à la procédure décrite pour TSplus Remote Access : <u>Rehébergement de</u> <u>votre licence TSplus</u>

Remarque : Vous pouvez télécharger un fichier license.lic sur le Portail de Licences pour les versions de TSplus Advanced Security ci-dessous. Veuillez vous référer à la <u>Guide de</u> <u>l'utilisateur du portail client</u> pour plus d'informations.

Merci d'avoir choisi TSplus Advanced Security !

Avancé - Sauvegarde et restauration

Sauvegarder et restaurer les données et les paramètres

Vous pouvez sauvegarder ou restaurer les données et les paramètres de TSplus Advanced Security en cliquant sur le bouton « Sauvegarder / Restaurer » en haut :

🙂 TSp	lus Advanced Security					- 0	×
ADV.	ANCEDSECURITY	Settings					
⊞	Dashboard	Language	English •				
ଌ	Firewall	S Whitelisted Users	_				
0	Sessions	Noduct Geographic Protection Bruteforce Protection	Name Pin Code Contribute to improve product by sending anonymous data	Value Yes			
₿	Ransomware	 ➢ Firewall ③ Restrict Working Hours ☑ Trusted Devices ④ Researce Protoction 	Computer Nickname Data Retention Policy	TSPLUS-SERVER1 43200			
ŵ	Alerts	Cogs					
	Reports						
ф;	Settings						
©⊋	License						
		(?) User Guide	Version 7	7.1.9.11 Permanent	License Activated - Ultimate Prote	ction edition	

艾 TSplus Advanced Security - Backup/Restore				
Backup				
Backup				
Restore				
2024-08-23_14-27-31				
Restore Restore Settings Only				

La sauvegarde sera enregistrée dans le dossier **archives** situé dans le répertoire de configuration de TSplus Advanced Security. Par défaut, le **archives** le dossier est situé ici : C: \Program Files (x86)\TSplus-Security\archives

Utiliser la ligne de commande pour sauvegarder et restaurer

L'utilisation de la commande est décrite ci-dessous :

• Sauvegarde TSplus-Security.exe /backup [chemin optionnel vers un répertoire]

Par défaut, la sauvegarde sera créée dans le répertoire des archives situé dans le dossier de configuration de TSplus Advanced Security. Cependant, la sauvegarde peut être enregistrée dans un dossier spécifié. Des chemins relatifs et absolus sont autorisés.

• Restaurer TSplus-Security.exe /restore [chemin vers un répertoire de sauvegarde]

Le répertoire de sauvegarde spécifié doit contenir un dossier de données et un dossier de paramètres, comme créé par la commande /backup.

Configurer les sauvegardes

Veuillez noter que vous pouvez spécifier les paramètres avancés suivants dans le registre :

Le répertoire de sauvegarde peut être spécifié dans la clé de registre. HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\archivespath Par défaut, le répertoire « archives » du répertoire d'installation d'Advanced Security sera utilisé.

Le nombre maximum de sauvegardes disponibles peut être spécifié dans la clé de registre.

HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\RDS-Tools\knight\maxarchives Par défaut, Advanced Security conserve les 3 dernières sauvegardes.

Migrez vos données et paramètres vers un autre ordinateur

Veuillez suivre les étapes ci-dessous pour migrer Advanced Security de l'ordinateur A vers l'ordinateur B :

1.

Sur l'ordinateur A, veuillez cliquer sur le bouton Sauvegarder pour créer une nouvelle sauvegarde. Les paramètres et les données seront enregistrés dans le répertoire des archives, situé dans le répertoire de configuration de la sécurité avancée (généralement C: \Program Files (x86)\TSplus-Security\archives).

2.

Copiez le nouveau dossier de sauvegarde créé (par exemple nommé backup-2019-09-11_14-37-31), y compris tout le contenu, du répertoire des archives sur l'ordinateur A vers le répertoire des archives sur l'ordinateur B.

3.

Sur l'ordinateur B, depuis la fenêtre Sauvegarde / Restauration, dans la section « Restauration », sélectionnez le nom de sauvegarde pertinent à restaurer.

4.

Ensuite, cliquez sur Restaurer uniquement les paramètres pour restaurer les paramètres. Alternativement, il est possible de cliquer sur Restaurer pour restaurer toutes les données et paramètres, ce qui n'est pas recommandé pour une migration mais utile pour restaurer la sécurité avancée sur l'ordinateur A.

5.

Veuillez patienter au maximum 2 minutes pour que les paramètres soient rechargés par les fonctionnalités de sécurité avancées.

Base de données

Une base de données stocke des événements, des adresses IP, des rapports d'attaques par ransomware et des listes blanches de programmes.

Cette base de données est stockée dans **données** dossier situé dans le répertoire d'installation de TSplus Advanced Security.

Advanced Security à partir de la version 5 et avant la version 5.3.10.6 utilise un <u>moteur de</u> <u>base de données LiteDB</u>.

•

•

Advanced Security au-dessus de la version 5.3.10.6 utilise un <u>moteur de base de données</u> <u>SQLite</u>.

🔒 data				_		×
← → × ↑ 📙 > This PC > Loca	al Disk (C:) > Program Files (x86) > TSplus-Security	/ > data	ל Search data			Q
TSplus-Security	^ Name	Date modified	Туре	Size		
archives	🚳 data	10/21/2019 4:52 PM	Data Base File		100 KB	
🔒 data	📄 ransomware-internal-whitelist.json.old	3/19/2019 7:01 PM	OLD File		1 KB	
drivers						
langs						
🔥 logs	~					
2 items						:==

Avancé - Protection contre les attaques par force brute

Le **Protection contre les attaques par force brute** l'onglet vous permet de Ignorer les adresses IP locales et privées si vous le souhaitez, en changeant la valeur par défaut de "Non" à "Oui".

뉯 TSpl	us Advanced Security			_	X
ADV	ANCEDSECURITY	Settings			
		Language	English •		
⊞	Dashboard	Backup / Restore			
ଚ	Firewall	🗳 Whitelisted Users			
9	Sessions	Product Geographic Protection Bruteforce Protection	Name Value Ignore Local and Private IP Addresses No		
₿	Ransomware	 Firewall Restrict Working Hours Trusted Devices 	TSplus Advanced Security - Edit Setting		
:	Settings	☐ Ransomware Protection	Ignore Local and Private IP Addresses Description:		
ଟ୍ୟ	License		Tsplus Advanced Security will ignore local and private IP addresses while protecting against brute-force attacks. Value: No Save Cancel		
					_
		⑦ User Guide	Version 7.1.8.20 Permanent License Activated - Ultimate F	Protection ed	ition.

Avancé - Pare-feu

Le **Pare-feu** l'onglet vous permet d'activer le **Windows Firewall ou le désactiver en faveur du pare-feu intégré de TSplus Advanced Security**.

Depuis la version 4.4, un pare-feu intégré est inclus dans TSplus Advanced Security.

En règle générale, si le pare-feu Windows est activé sur votre serveur, vous devez l'utiliser pour appliquer les règles de TSplus Advanced Security (par défaut). Si vous avez installé un autre pare-feu, vous devez activer le pare-feu intégré de TSplus Advanced Security.

👈 TSp	olus Advanced Security					-		×
ADV	ANCEDSECURITY	Settings						
		Language	English 🔹					
⊞	Dashboard	Backup / Restore						
ଚ	Firewall	A Whitelisted Users						
0	Sessions	 Product Geographic Protection Bruteforce Protection 	Name Use Windows Firewall Unblock after		Value Yes 0			
٥	Ransomware	Restrict Working Hours Restrict Working Hours Trusted Devices	Enable Hacker IP addresses automatic synchr Contribute to improve Hacker IP list	onization	Yes Yes			
\$	Settings	ইি Logs						
ଚ୍ଚ	License							
		(?) User Guide		Version 7.1.8.20 P	ermanent License Activate	d - Ultimate Protection e	dition.	

Utiliser le pare-feu Windows Pour activer le pare-feu intégré, allez dans Paramètres > Avancé > Produit > Utiliser le pare-feu Windows et définissez la valeur sur : Non. Si Oui, alors les adresses IP problématiques seront bloquées à l'aide du pare-feu Windows. Le pare-feu TSplus Advanced Security sera utilisé sinon.

Débloquer après Changez ce paramètre pour débloquer automatiquement les adresses IP après un certain temps (en minutes). La valeur par défaut est 0, désactivant cette fonctionnalité. Valeur : 0

Activer la synchronisation automatique des adresses IP des hackers Gardez votre machine protégée contre les menaces connues telles que les attaques en ligne, l'abus de services en ligne, les logiciels malveillants, les botnets et d'autres activités électroniques avec la protection IP des hackers. Un abonnement aux services de support et de mises à jour est requis. Valeur : Oui

Contribuer à améliorer la liste des IP des hackers Autoriser TSplus Advanced Security à envoyer des statistiques d'utilisation anonymes pour améliorer la protection contre les IP des hackers.

Valeur : Oui

Protection géographique avancée

Le **Protection géographique** l'onglet vous permet d'ajouter ou de supprimer des processus qui sont surveillés par le Protection géographique fonctionnalité.

뉯 TSp	lus Advanced Security					-		×
ADV	ANCEDSECURITY	Settings						
		Language	English •					
	Dashboard	Backup / Restore						
ଚ	Firewall	Hitelisted Users						
0	Sessions	Product Geographic Protection Bruteforce Protection Engual	Name Watched Processes Watched Ports		Value HTML5service			
₿	Ransomware	Restrict Working Hours						
\$ 3	Settings	logs						
ଙ୍କ	License							
		🕐 User Guide		Version 7.1.8.20	Permanent License Activated	- Ultimate Protection	edition.	

Par défaut, le service HTML5 est surveillé.

Le **Ports surveillés** les paramètres vous permettent d'ajouter des ports surveillés par le Protection géographique fonctionnalité. Par défaut, la Protection Géographique écoute les ports par défaut utilisés pour se connecter à distance à un serveur. Ces ports incluent RDP (3389), Telnet (23) et les ports VNC. La Protection Géographique prend en charge les fournisseurs VNC suivants : Tight VNC, Ultra VNC, Tiger VNC et Real VNC, qui ne sont en aucun cas liés à TSplus.

Avancé - Journaux

Le **Journaux** l'onglet vous permet de activer ou désactiver les journaux de service et de fonctionnalités Des journaux existent pour trouver plus facilement l'origine des erreurs rencontrées sur TSplus Advanced Security.

Pour récupérer les journaux, ouvrez un Explorateur et parcourez le **journaux** dossier du répertoire d'installation de TSplus Advanced Security. Par défaut, les journaux seront situés ici : **C:\Program Files (x86)\TSplus-Security\logs**

👈 TS	plus Advanced Security					-		×
AD∖	ANCEDSECURITY	Settings						
		Language	English •					
⊞	Dashboard	Backup / Restore						
ଚ	Firewall	A Whitelisted Users						
0	Sessions	 Product Geographic Protection Bruteforce Protection Ensural 	Name Enable TSplus Advanced Security service log Enable Bruteforce Protection service log		Value No No			
₿	Ransomware	Restrict Working Hours Trusted Devices Response Protection	Enable Geographic Protection service log Enable Ransomware protection service log Enable Working Hours Restrictions service log		No No No			
\$	Settings		Enable Firewall log Enable TSplus Advanced Security application log		No No			
¢7	Liconso							
		(?) User Guide		Version 7.1.8.20 P	ermanent License Activate	ed - Ultimate Protection	edition.	

Activer ou désactiver Service et journaux d'application TSplus Advanced Security, qui sont respectivement le service de configuration global qui fonctionne en arrière-plan et le journal de l'interface de l'application.

Vous pouvez également activer les journaux correspondant aux fonctionnalités respectives de TSplus Advanced Security :

- Service
- Protection contre les attaques par force brute
- Protection géographique

- Protection contre les ransomwares
- Restreindre les heures de travail
- Pare-feu..
- Application

Tous les journaux sont désactivés par défaut. Les journaux correspondent à différents composants, notre équipe de support vous indiquera quelle valeur mettre en fonction du problème rencontré.

Avancé - Produit

Le Produit l'onglet vous permet de ajouter un code PIN à l'application :

뉯 TSp	lus Advanced Security			- 0	×
ADV.	ANCEDSECURITY	Settings			
		Language	English		
⊞	Dashboard	Backup / Restore			
ଚ	Firewall	🗳 Whitelisted Users			
0	Sessions	 Product Geographic Protection Bruteforce Protection 	Name Pin Code Contribute to improve product by sending anonymous data	Value Yes	
₿	Ransomware	Restrict Working Hours Trusted Devices Restrict Protection	Computer Nickname Data Retention Policy	TSPLUS-SERVER1 43200	
٤	Settings	ĝi Logs			
ଙ୍କ	License				
		⑦ User Guide	Version 7.1.8.20	Permanent License Activated - Ultimate Protection edi	tion.

Cliquez sur Enregistrer. Le code PIN sera requis la prochaine fois que vous démarrerez l'application.

Vous pouvez également **contribuer à améliorer le produit**, en envoyant des données anonymes (activé par défaut) : OUI

Les données suivantes seront collectées en cas d'attaque par Ransomware :

- La version de TSplus Advanced Security.
- Version Windows.
- Chemins des fichiers suspects menant à l'attaque par ransomware.

Modifier le Surnom de l'ordinateur est également possible.

Le **Politique de conservation des données** définit la période après laquelle les événements de TSplus Advanced Security sont supprimés de la base de données. Une sauvegarde est

effectuée avant chaque nettoyage de la base de données. Cette politique est définie en minutes. La politique de conservation des données par défaut est de 259 200 minutes, soit 6 mois.

Protection avancée contre les ransomwares

Le **Protection contre les ransomwares** l'onglet vous permet de configurer les propriétés de l'instantané et définir les extensions de fichiers ignorées pour la fonction de protection contre les ransomwares.

👈 TSp	lus Advanced Security						×
ADVANCEDSECURITY Settings		Settings					
		Language	English •				
⊞	Dashboard	Backup / Restore					
ෂ	Firewall	A Whitelisted Users					
9	Sessions	Product Geographic Protection Bruteforce Protection Enumel	Name Snapshot Path Ignored Extensions		Value C:\Program Files (x86)\TSplus 1 300 300		
₿	Ransomware	Restrict Working Hours Trusted Devices Resonware Protection	File Snapshots Max Size File Snapshot Retention Registry Snapshot Retention				
(2)	Settings	logs	Display Detection Alert Allowed PowerShell and CMD scripts		Yes		
ଙ୍କ	License						
							_
		🕐 User Guide		Version 7.1.8.20 P	ermanent License Activated -	Ultimate Protection editi	on.

Chemin de l'instantané Définir le répertoire où la protection contre les ransomwares stocke les instantanés de fichiers.

La valeur par défaut est : C:\Program Files (x86)\TSplus-Security\snapshots

Extensions ignorées Par défaut, la protection contre les ransomwares ignore les extensions bien connues des fichiers temporaires pour les activités de ransomware. <u>Voir la liste ici</u> Vous pouvez définir des noms d'extension personnalisés dans le champ de valeur (séparés par des points-virgules) :

Taille maximale de l'instantané de fichier La taille maximale des instantanés de fichiers définit l'espace maximum autorisé pour conserver les instantanés de fichiers.

La taille est exprimée en pourcentage de l'espace total disponible sur le disque où se trouve le

chemin de l'instantané.

Conservation des instantanés de fichiers La rétention des instantanés de fichiers définit, en secondes, la politique de rétention d'un instantané de fichier.

Une fois la période de rétention terminée, l'instantané du fichier est supprimé. Par défaut, 300 secondes (c'est-à-dire 5 minutes)

Conservation de l'instantané du registre La rétention de l'instantané du registre définit, en secondes, la politique de rétention d'un instantané du registre. Une fois la période de rétention terminée, l'instantané du registre est supprimé. Par défaut, 300 secondes (c'est-à-dire 5 minutes)

Alerte de détection d'affichage Afficher une fenêtre de message d'alerte sur le bureau de l'utilisateur lorsque la protection contre les ransomwares a détecté et arrêté une attaque.

Scripts PowerShell et CMD autorisés Liste des scripts PowerShell et CMD autorisés avec les chemins de fichiers complets des scripts PowerShell et CMD autorisés à être exécutés sur la machine

L'exécution des scripts autorisés ne déclenchera pas la protection contre les ransomwares (séparés par des points-virgules).

Avancé - Appareils de confiance

Le **Appareils de confiance** l'onglet vous permet d'activer les connexions depuis le portail Web de TSplus Remote Access.

Remarque :

- Les appareils de confiance ne sont pas compatibles avec les sessions HTML5. - Les appareils de confiance ne sont pas compatibles avec les appareils mobiles iOS / Android car ils cachent leurs véritables noms d'hôte. - Le nom d'hôte de la machine distante est défini par la machine elle-même. La machine est susceptible de le dissimuler ou de le modifier en fonction de sa configuration.

👈 TSp	lus Advanced Security					- 🗆	×
ADV	ANCEDSECURITY	Settings					
		Language	English •				
⊞	Dashboard	Backup / Restore					
ଚ	Firewall	A Whitelisted Users					
9	Sessions	 Product Geographic Protection Bruteforce Protection A Brownall 	Name Allow Connection From Web Portal	Value No			
₿	Ransomware	Restrict Working Hours Trusted Devices					
\$	Settings	资 Logs					
ଙ୍କ	License						
		🕐 User Guide		Version 7.1.8.20	Permanent License Activated - Ultimate F	Protection edition.	

La fonction des appareils de confiance de TSplus Advanced Security ne peut pas résoudre le nom du client si la connexion est initiée depuis le portail Web de TSplus Remote Access. Par conséquent, les appareils de confiance bloqueront par défaut toutes les connexions provenant du portail Web. Réglez ce paramètre sur « Oui » pour autoriser les connexions depuis le portail Web. Veuillez noter que cette action diminuera la sécurité de votre serveur.

Avancé - Restreindre les heures de travail

Le **Restreindre les heures de travail** l'onglet vous permet de Planifiez un message d'avertissement avant que l'utilisateur ne soit déconnecté.

뉯 TSp	lus Advanced Security					- 0	×
ADV	ANCEDSECURITY	Settings					
		Language	English •				
⊞	Dashboard	🗘 🛛 Backup / Restore					
ଚ	Firewall	A Whitelisted Users					
9	Sessions	 Product Geographic Protection Bruteforce Protection Enswall 	Name Scheduled warning message before logoff Warning message		Value 5 Attention : vous allez être déco		
٥	Ransomware	Restrict Working Hours	Default timezone Working Hours title Show logo on working hours		(UTC+01:00) Bruxelles, Copenh TSplus Advanced Security YES		
\$	Settings	logs					
©₽	License						
		(?) User Guide		Version 7.1.8.20	Permanent License Activated - U	timate Protection editi	DN.

Message d'avertissement de planification Vous pouvez configurer le nombre de minutes avant que l'utilisateur ne soit automatiquement déconnecté. Par défaut, il est réglé sur 5 minutes.

Message d'avertissement Un message d'avertissement peut être défini à votre convenance, avec des espaces réservés nommés %MINUTESBEFORELOGOFF%, %DAY%, %STARTINGHOURS% et %ENDINGHOURS%, qui seront respectivement remplacés par le nombre actuel de minutes avant la fermeture de la session, le jour actuel, les heures de travail de début et de fin du jour actuel.

Fuseau horaire du serveur par défaut Un fuseau horaire de serveur par défaut peut être défini pour appliquer les règles des heures de travail en sélectionnant le correspondant dans la liste déroulante.

Heures de travail titre Titre du formulaire affiché à l'utilisateur final, lorsque ses heures de travail se terminent (par défaut : TSplus Advanced Security)

Afficher le logo pendant les heures de travail Si défini sur « oui », le logo est affiché sous la forme présentée à l'utilisateur final, lorsque ses heures de travail se terminent (par défaut : « oui »)

Alertes



Program hacker.exe has been detected as a threat and has been terminated on computer DV (MACHINE-NAME)

Dear Administrator,

Program hacker.exe has been detected as a threat on computer DV (MACHINE-NAME) by TSplus Advanced Security's Ransomware Protection and has been terminated.

If you have any questions or feedback regarding this email, please do not hesitate to contact our support team by replying to this email.

Best regards, TSplus Advanced Security Team

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

Protection contre les attaques par force brute

La protection contre les attaques par force brute vous permet de protéger votre serveur public contre les hackers, les analyseurs de réseau et les robots de force brute qui essaient de deviner votre identifiant et votre mot de passe Administrateur. En utilisant des identifiants actuels et des dictionnaires de mots de passe, ils tenteront automatiquement de se connecter à votre serveur des centaines à des milliers de fois chaque minute.

Avec ce RDP Defender, vous pouvez surveiller les tentatives de connexion échouées sur Windows et automatiquement mettre sur liste noire les adresses IP fautives après plusieurs échecs.

👈 TSp	olus Advanced Security							- 🗆 🗙
ADV	ANCEDSECURITY	Firewall	Q Filters:	Blocked - Brute	force Protection, Blocked - Geogr	raphic Protection, Blo	ocked - Hacker IP P 🗸	
⊞	Dashboard	IP Address 127.0.0.1 ::1	Country S	Status Whitelisted Whitelisted	Date 23 août 2024 12:28:40 23 août 2024 12:28:40	Description localhost localhost		Add IP Address
්	Firewall	<pre>2001:861:2049:3c0 fe80::8576:2d2b:c1 192.168.1.134</pre>	France V	Whitelisted Whitelisted Whitelisted	23 août 2024 12:28:40 23 août 2024 12:28:40 23 août 2024 12:28:40	localhost localhost localhost		Remove IP Address(es)
0	Sessions	■ 83.166.153.206 51.89.7.51 ■ 51.89.41.38 ■ 51.79.79.179	Switzerland V United Kingdom V Germany V Canada V	Whitelisted Whitelisted Whitelisted	23 août 2024 12:28:40 23 août 2024 12:28:40 23 août 2024 12:28:40 23 août 2024 12:28:40 23 août 2024 12:28:40	TSplus Advanced Secu Remote Support API Remote Support Relay Remote Support Relay	urity Updates y (DE)	Export to CSV
₿	Ransomware	139.99.130.197	Australia V	Whitelisted	23 août 2024 12:28:40	Remote Support Relay	y (AU)	WHOIS
1 23	Settings				/1			
8	Liconso		d list	Bruteforce Protection Enabled You are protected against hackers scanners and brute-force robots fin guess your logins and passwords.	, network om trying to	Hacker IP Pro	patection gainst 564 436 405 ses from our woldwide of known threats : 23/08/2024	
Configure Authorized Countries				Configure Bruteforce Protection	n	Refresh I	tacker IP	
🕐 User Guide					Version 7.1.8.20	Permanent Li	icense Activated - Ulti	mate Protection edition.

🕁 TS	olus Advanced Security				- 0
AD∖	ANCEDSECURITY	Firewall > Bruteforce Protection			
		IPs Detection			
⊞	Dashboard	Maximum failed logon attempts from a single IP address:			
ය	Firewall	Reset counters of failed logon attemps after: 2 + hours			
â	C			Apply now	
ø	Sessions	Defender Status			
⋳	Ransomware	Splus-Security Service is Running - You are Protected			
:	Settings	Windows Firewall is Enabled - Blocked IPs cannot connect			
~		Windows Logon Audit is Enabled - Logon Failures are Monitored			
077	LICENSE	HTML5 Portal Logs enabled - Portal logon failures are monitored			
) User Guide	Version 7. 1.8.20	Permanent License Activated - Ultimate	Protection edition

Vous pouvez définir le **maximum d'échecs de connexion à partir d'une seule adresse IP dans le bloc de détection des IPs** (par défaut, c'est 10), ainsi que le temps de réinitialisation pour les compteurs de tentatives de connexion échouées (par défaut, c'est 2 heures).

En bas de cette fenêtre, vous pouvez voir le **Statut du défenseur** où vous pouvez vérifier si les échecs de connexion au portail Web HTML5, les échecs de connexion Windows sont surveillés et si le pare-feu Windows et le service de sécurité avancée sont activés.

Dans ce cas, comme dans notre exemple, tous les statuts sont cochés.

•

Gérer les adresses IP bloquées Vous pouvez bien sûr le configurer pour qu'il corresponde à vos besoins, par exemple en ajoutant votre propre adresse IP de station de travail dans le <u>Liste blanche des IPs</u>, donc cet outil ne vous bloque jamais. Vous pouvez ajouter autant d'adresses IP que vous le souhaitez dans la liste blanche. Ces adresses ne seront jamais bloquées par la protection contre les attaques par force brute.

•

Vous pouvez **ignorer les adresses IP locales et privées** en modifiant le paramètre par défaut sur le <u>Paramètres > Avancé > Onglet de protection contre les attaques par force brute</u>

Remarque : Si vous remarquez un jour que la protection contre les attaques par force brute bloque 10 adresses IP par jour et qu'à présent, ce n'est plus le cas ; et qu'elle bloque une, deux ou même aucune adresse, c'est en fait normal. En effet, avant l'installation de la sécurité avancée, le serveur ayant un port RDP disponible publiquement est connu de tous les robots, et de nombreux robots essaient les mots de passe actuels et ceux provenant de dictionnaires. Lorsque vous installez la sécurité avancée, ces robots sont progressivement bloqués, de sorte qu'un jour :

- La plupart des robots actifs sont déjà bloqués et ne s'intéressent pas au serveur, même les nouveaux.
- De plus, le serveur n'apparaît plus sur la liste des serveurs connus publiquement.

Lignes de commande

Nous sommes heureux de vous fournir un ensemble complet d'outils en ligne de commande conçus pour améliorer la flexibilité et l'efficacité de notre logiciel. Ces outils permettent aux utilisateurs de script et d'automatiser diverses fonctionnalités, adaptant le logiciel pour répondre à leurs besoins et flux de travail spécifiques.

Explorez les possibilités et optimisez votre expérience avec nos options de ligne de commande.

Vous devez uniquement exécuter les lignes de commande suivantes en tant qu'administrateur élevé. En rappel, TSplus-Security.exe se trouve dans le dossier suivant. C:\Program Files (x86)\TSplus-Security par défaut.

Gestion des licences

Pour effectuer des opérations sur les licences, veuillez remplacer le programme AdminTool.exe présenté dans la documentation suivante par le programme TSplus-Security.exe situé dans le répertoire d'installation d'Advanced Security (généralement **C:\Program Files (x86)\TSplus-Security**).

- Activation de la licence
- <u>Réinitialisation de la licence suite au clonage d'une VM</u>
- <u>Activation de licence en volume</u>
- <u>Activer et désactiver la licence en volume</u>
- <u>Mise à jour de la licence en volume</u>
- <u>Afficher les crédits de licence restants pour une clé de licence en volume</u>
- <u>Afficher les crédits de support restants pour une clé de licence en volume</u>

Configurer le serveur proxy : /proxy /set

Syntax :

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

Description:

Commande /proxy /set est utilisé pour configurer un serveur proxy pour l'accès à Internet.

Paramètres :

- /host le serveur de destination peut être une valeur prédéfinie ("ie" ou "none") ou une valeur définie par l'utilisateur (par exemple : 127.0.0.1 ou proxy.company.org). Ce paramètre est obligatoire
- /port le numéro de port utilisé pour se connecter au serveur proxy. Requis si la valeur du nom d'hôte est une valeur personnalisée définie par l'utilisateur.
- /username le nom d'utilisateur pour se connecter au serveur proxy. Ce paramètre est facultatif
- /password le mot de passe de l'utilisateur doit être fourni si un nom d'utilisateur a été défini.
 Cependant, sa valeur peut être vide

Exemples :

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

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

Pour plus d'informations, veuillez vous rendre sur <u>Comment configurer un serveur proxy pour</u> <u>l'accès à Internet ?</u>

Sauvegarder les données et les paramètres : / backup

Syntax :

TSplus-Security.exe /backup [DestinationDirectoryPath]

Description:

Commande /backup est utilisé pour sauvegarder les données et les paramètres de TSplus Advanced Security.

Par défaut, la sauvegarde sera créée dans le répertoire des archives situé dans le répertoire de configuration d'Advanced Security (par exemple : C:\Program Files (x86)\TSplus-Security\archives).

Paramètres :

 DestinationDirectoryPath pour sauvegarder dans un autre répertoire que celui par défaut. Les chemins relatifs et absolus sont autorisés.

Exemples :

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

Pour plus d'informations, veuillez vous rendre sur <u>Avancé - Sauvegarde et restauration</u>

Restaurer les données et les paramètres : / restore

Syntax :

TSplus-Security.exe /restore [Chemin du répertoire de sauvegarde]

Description:

Commande /restore est utilisé pour restaurer les données et les paramètres de TSplus Advanced Security.

Le chemin du répertoire de sauvegarde spécifié doit être créé par la commande /backup ou à partir de la fonction de sauvegarde de l'application.

Paramètres :

• Backup Directory Path le chemin où se trouve le répertoire de sauvegarde à restaurer.

Exemples :

Pour plus d'informations, veuillez vous rendre sur <u>Avancé - Sauvegarde et restauration</u>

Supprimer et débloquer toutes les adresses IP bloquées : /unblockall

Syntax :

TSplus-Security.exe /unblockall

Description:

Commande /unblockall est utilisé pour supprimer toutes les adresses IP bloquées du pare-feu de TSplus Advanced Security et les débloquer du pare-feu de Microsoft Windows Defender si nécessaire.

Exemples :

TSplus-Security.exe /unblockall

Pour plus d'informations, veuillez vous rendre sur Pare-feu

Supprimer et débloquer les adresses IP spécifiées : /unblockips

Syntax :

TSplus-Security.exe /debloquerips [adresses IP]

Description:

Commande /unblockips est utilisé pour supprimer toutes les adresses IP bloquées spécifiées du pare-feu de TSplus Advanced Security et les débloquer du pare-feu de Microsoft Windows Defender si nécessaire.

Cette commande n'a aucun effet sur les adresses IP déjà bloquées par la protection IP contre les hackers. Si vous souhaitez toujours débloquer l'une de ces adresses, veuillez utiliser la commande de liste blanche.

Paramètres :

• IP addresses la liste des adresses IP ou des plages d'adresses IP à débloquer (séparées par des virgules ou des points-virgules).

Exemples :

TSplus-Security.exe /unblockips 1.1.1.1;2.2.2;3.3.3.1-3.3.6.12;5.5.5.5

Pour plus d'informations, veuillez vous rendre sur Pare-feu

Bloquer les adresses IP spécifiées : /blockips

Syntax :

TSplus-Security.exe /blockips [adresses IP] [Description optionnelle]

Description :

Commande /blockips est utilisé pour bloquer toutes les adresses IP spécifiées en utilisant le pare-feu de TSplus Advanced Security et les bloquer en utilisant le pare-feu de Microsoft Windows Defender si configuré.

Paramètres :

- IP addresses la liste des adresses IP ou des plages d'adresses IP à bloquer (séparées par des virgules ou des points-virgules).
- Optional Description : une description optionnelle qui sera ajoutée pour chaque entrée.

Exemples :

TSplus-Security.exe /blockips 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "Lieux de travail de John"

Pour plus d'informations, veuillez vous rendre sur Pare-feu

Ajouter des adresses IP à la liste blanche : / addwhitelistedip

Syntax :

TSplus-Security.exe /addwhitelistedip [adresses IP] [Description optionnelle]

Description :

Commande /addwhitelistedip est utilisé pour ajouter des adresses IP spécifiées aux adresses IP autorisées du pare-feu de TSplus Advanced Security et les débloquer du pare-feu de Microsoft Windows Defender si nécessaire.

Paramètres :

- IP addresses la liste des adresses IP ou des plages d'adresses IP à mettre sur liste blanche (séparées par des virgules ou des points-virgules).
- Optional Description : une description optionnelle qui sera ajoutée pour chaque entrée.

Exemples :

TSplus-Security.exe /addwhitelistedip 1.1.1.1;2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "Lieux de travail de John"

Pour plus d'informations, veuillez vous rendre sur Pare-feu

Ajouter un programme ou un répertoire à la liste autorisée de protection contre les ransomwares : /whitelist

Syntax :

TSplus-Security.exe /whitelist add [Chemins autorisés]

Description:

Commande /whitelist add est utilisé pour ajouter des chemins de programme et des chemins de répertoire spécifiés à la liste autorisée de la protection contre les ransomwares de TSplus Advanced Security.

Paramètres :

 Authorized Paths la liste des chemins de programme et des chemins de répertoire à ajouter à la liste d'autorisation de la protection contre les ransomwares de TSplus Advanced Security (séparés par des points-virgules).

Exemples:

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

Pour plus d'informations, veuillez vous rendre sur <u>Action de protection contre les ransomwares</u>

Actualiser la protection IP des hackers : / refreshipprotection

Syntax :

TSplus-Security.exe /refreshipprotection

Description:

Commande /refreshipprotection est utilisé pour actualiser la liste des plages d'IP bloquées pour la fonction de protection contre les IP des hackers. Un abonnement aux services de support et de mises à jour est requis.
Exemples :

TSplus-Security.exe /refreshipprotection

Pour plus d'informations, veuillez vous rendre sur Protection des IP des hackers

Définir le niveau de journalisation : /setloglevel

Syntax :

TSplus-Security.exe /setloglevel [Niveau de journal]

Description :

Commande /setloglevel est utilisé pour définir le niveau de journalisation pour tous les composants d'Advanced Security.

Paramètres :

 Log Level le niveau de journal parmi les valeurs suivantes : ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF

Exemples :

TSplus-Security.exe /setloglevel ALL

Pour plus d'informations, veuillez vous rendre sur <u>Avancé > Journaux</u>

Ajouter des appareils de confiance : / addtrusteddevices

Syntax :

TSplus-Security.exe /addtrusteddevices [Configuration des appareils de confiance]

Description :

Commande /addtrusteddevices est utilisé pour ajouter des appareils de confiance de manière programmatique. Nécessite l'édition Ultimate.

Paramètres :

• Trusted Devices Configuration L'argument est composé d'une liste de dispositifs de confiance (séparés par des points-virgules), structurée comme suit :

Nom d'utilisateur et appareils sont séparés par le caractère deux-points (:).

Détails de l'utilisateur :

Type d'utilisateur et nom d'utilisateur complet sont séparés par le caractère deux-points (:). Les types d'utilisateur acceptés sont "utilisateur" et "groupe".

Mot clé optionnel "désactivé" : s'il est inclus, les appareils de confiance seront créés, mais les restrictions seront désactivées pour cet utilisateur. S'il n'est pas mentionné, les restrictions sont activées par défaut.

Détails de l'appareil :

Nom de l'appareil et commentaire optionnel : séparés par le caractère égal (=).

Les appareils sont séparés par le caractère deux-points (:).

Exemples:

TSplus-Security.exe /addtrusteddevices "user:WIN-A1BCDE23FGH\admin:disabled,device1name=c'est un commentaire pour l'appareil 1:device2name:device3name;user:DESKTOP-A1BCDE23FGH\johndoe,device1name:device4name=un autre commentaire;group:DESKTOP-A1BCDE23FGH\Administrators:disabled,device5name"

Pour plus d'informations, veuillez vous rendre sur <u>Appareils de confiance</u>

Activer les appareils de confiance configurés : /

enabletrusteddevices

Syntax :

TSplus-Security.exe /enabletrusteddevices [Utilisateur ou groupes]

Description:

Commande /enabletrusteddevices est utilisé pour activer tous les appareils de confiance configurés pour les utilisateurs et groupes spécifiés.

Paramètres :

 User or Groups L'argument est une liste d'utilisateurs et de groupes (séparés par des pointsvirgules). Au sein du nom d'utilisateur, la séparation entre le type d'utilisateur ("utilisateur" et "groupe" sont les seules valeurs acceptées) et le nom d'utilisateur complet se fait par un deuxpoints.

Exemples :

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

Pour plus d'informations, veuillez vous rendre sur <u>Appareils de confiance</u>

Désactiver tous les appareils de confiance : / disabletrusteddevices

Syntax :

TSplus-Security.exe /disabletrusteddevices [Utilisateur ou groupes]

Description:

Commande /disabletrusteddevices est utilisé pour désactiver tous les appareils de confiance

configurés pour les utilisateurs et groupes spécifiés.

Paramètres :

 User or Groups L'argument est une liste d'utilisateurs et de groupes (séparés par des pointsvirgules). Au sein du nom d'utilisateur, la séparation entre le type d'utilisateur ("utilisateur" et "groupe" sont les seules valeurs acceptées) et le nom d'utilisateur complet se fait par un deuxpoints.

Exemples :

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

Pour plus d'informations, veuillez vous rendre sur <u>Appareils de confiance</u>

Configurer le pilote de protection contre les ransomwares : /setup-driver

Syntax :

TSplus-Security.exe /setup-driver

Description:

Commande /setup-driver installe le pilote de protection contre les ransomwares. Cette opération est normalement effectuée lors de l'installation.

Exemples :

TSplus-Security.exe /setup-driver

Pour plus d'informations, veuillez vous rendre sur Protection contre les ransomwares

Désinstaller le pilote de protection contre les ransomwares : /uninstalldriver

Syntax :

TSplus-Security.exe /uninstalldriver

Description :

Commande /uninstalldriver désinstaller le pilote de protection contre les ransomwares. Cette opération est normalement effectuée lors de la désinstallation de la sécurité avancée.

Exemples:

TSplus-Security.exe /uninstalldriver

Pour plus d'informations, veuillez vous rendre sur <u>Protection contre les ransomwares</u>

Événements

Les événements de sécurité sont une excellente source d'information car ils affichent les opérations effectuées par TSplus Advanced Security pour protéger votre ordinateur.

La fenêtre Événements peut être ouverte depuis la fenêtre principale de TSplus Advanced Security, en cliquant directement sur les 5 derniers événements affichés ou sur l'onglet tableau de bord. Les informations affichées dans la fenêtre Événements sont actualisées automatiquement toutes les quelques secondes.

La liste des événements de sécurité présente 4 colonnes, qui décrivent la gravité, la date de la vérification ou de l'opération effectuée, l'icône de fonctionnalité associée et la description.

t T	Splus Advanced Security	- Security Event Lo	g - Events since 11 sept. 2024 16:39:17 — 🗆 🗙
	Date	Feature	Message
0		⋳	Learning period has started. During this period, all detected programs will be considered as false positive and added to the program allow list.
0	25 sept. 2024 09:19:18	A	Synchronized Hacker IP addresses protects your computer against 564 436 405 IP addresses.
0	25 sept. 2024 09:13:18	\odot	A new session Console (#1) has started for user AD\administrateur from client TSPLUS-SERVER1 and IP address <not a="" connection="" remote=""></not>
0	25 sept. 2024 09:13:06	Q	A logon request has been granted for user AD\administrateur because AD\administrateur is allowed
0	25 sept. 2024 09:13:06	Ţ	A connection has been authorized for user AD\administrateur from computer because this feature is not enabled for this user
0	25 sept. 2024 09:12:21	ð	Learning period has started. During this period, all detected programs will be considered as false positive and added to the program allow list.
0	24 sept. 2024 15:04:54	⋳	Learning period has started. During this period, all detected programs will be considered as false positive and added to the program allow list.
0	24 sept. 2024 15:03:49	⋳	Ransomware Protection has been stopped from the administrative interface or following an update.
0	24 sept. 2024 15:03:42	⋳	Protection against Ransomware is up and running
0	24 sept. 2024 15:03:27	⋳	Learning period has started. During this period, all detected programs will be considered as false positive and added to the program allow list.
0	24 sept. 2024 15:03:15	⋳	Ransomware Protection has been stopped from the administrative interface or following an update.
0	24 sept. 2024 15:03:10	⋳	Protection against Ransomware is up and running
0	24 sept. 2024 11:05:35	â	Synchronized Hacker IP addresses protects your computer against 564 436 405 IP addresses.
Сору	/		
Search	1	Hid	e Less Significant 25/08/2024 □▼ 00:00:00 ♀ - 25/09/2024 □▼ 23:59:59 ♀ < 1/6 >
			Export to CSV

La description de l'événement explique souvent pourquoi l'action a été effectuée ou non. Les

actions de représailles sont souvent écrites en rouge et mises en évidence avec une icône de bouclier rouge.

La fenêtre des événements peut être déplacée et ne vous empêche pas d'utiliser les autres fonctionnalités de TSplus Advanced Security.

Naviguer et rechercher à travers les événements

•

Une recherche globale approfondie est maintenant disponible afin de trouver rapidement des événements spécifiques.

•

À côté de la recherche globale, 2 filtres de sélecteurs de date et d'heure affichent les événements en fonction de la date à laquelle l'événement a été soulevé.

•

À droite, des flèches permettent de changer de page et de naviguer pour voir des événements plus anciens.

Pare-feu

La gestion des adresses IP est facile avec une liste unique pour gérer à la fois les adresses IP bloquées et les adresses IP autorisées :

Firewall					
Search	Q Filter	rs: Blocked - Bruteforce Prote	ection, Blocked - Geog	raphic Protection, Blocked from TSplus i \sim]
IP Address	Country	Status	Date	Description	Add IP Address
1.10.16.0-1.10.31.255	China	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
1.19.0.0-1.19.255.255	South Korea	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	Edit IP Address
1.32.128.0-1.32.191	Singapore	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
2.56.192.0-2.56.195	Netherlands	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
= 2.57.185.0-2.57.185	Russia	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	Remove IP Address(es)
2.57.186.0-2.57.187	Russia	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
2.57.232.0-2.57.235	France	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	Export to CSV
2.59.200.0-2.59.203	United Kingdom	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
5.134.128.0-5.134.1	Iran	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	WHOIS
5.180.4.0-5.180.7.255	United States	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
5.183.60.0-5.183.63	United Kingdom	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
5.188.10.0-5.188.11	Russia	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
		1 / 2804)

Par défaut, les adresses IPV4, IPV6 et tous les localhost de serveur sont sur liste blanche.

Une barre de recherche pratique et un filtre offrent des capacités de recherche basées sur toutes les informations fournies.

Firewall					
Search	Q Fil	ters: Blocked - Bruteforce Prot	ection, Blocked - Geog	raphic Protection, Blocked from TSplu	5, ~
IP Address	Country	Status	Date	Description	Add IP Address
1.10.16.0-1.10.31.255	China	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
1.19.0.0-1.19.255.255	South Korea	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	Edit IP Address
1.32.128.0-1.32.191	Singapore	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
2.56.192.0-2.56.195	Netherlands	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
2.57.185.0-2.57.185	Russia	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	Remove IP Address(es)
2.57.186.0-2.57.187	Russia	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
2.57.232.0-2.57.235	France	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	Export to CSV
2.59.200.0-2.59.203	United Kingdom	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
5.134.128.0-5.134.1	Iran	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	WHOIS
5.180.4.0-5.180.7.255	United States	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
5.183.60.0-5.183.63	United Kingdom	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
5.188.10.0-5.188.11	Russia	Blocked - Hacker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs	
< <		1 / 2804			>> `

De plus, les administrateurs peuvent effectuer des actions sur plusieurs adresses IP sélectionnées en un seul clic. Parmi les nouvelles fonctionnalités de gestion des adresses IP

introduites, vous trouverez la possibilité de fournir des descriptions significatives à toutes les adresses IP.

Edit IP Address		_	-	×
IP Address	1.10.16.0-1.10.31.255			
Description	Known Malicious IPs			
Blocked IP Address	O Whitelisted IP address			
	1	Edit IP /	Address	

Dernier point mais non des moindres, les administrateurs peuvent désormais débloquer et ajouter plusieurs adresses IP bloquées à la liste blanche en une seule action, en cliquant sur l'onglet « Ajouter un existant à la liste blanche ».

Utiliser la ligne de commande pour ajouter ou bloquer des adresses IP et/ou des plages d'adresses IP

• Pour pouvoir whitelist Adresses IP ou plage(s) d'IP, la commande a cette syntaxe :

TSplus-Security.exe ajouteripwhitelistée [adresses IP] [description optionnelle]

Vous pouvez ajouter plusieurs adresses IP à la liste blanche, avec un **virgule ou point-virgule délimiteur** De plus, vous pouvez spécifier des plages d'adresses IP, au lieu de simples adresses IP. La syntaxe est : **x.x.x.y.y.y.y** Enfin, vous pouvez indiquer une description optionnelle de la règle de liste blanche.

Voici un exemple d'une commande complète : TSplus-Security.exe addwhitelistedip 1.1.1.1;2.2.2.2;3.3.3.1-3.3.6.12;5.5.5.5 "lieux de travail de John"

• Pour pouvoir **bloc** adresses IP ou plage(s) d'IP, la commande a une syntaxe similaire :

TSplus-Security.exe bloque les IP [adresses IP] [description optionnelle]

• Pour pouvoir débloquer adresses IP ou plage(s) d'IP, la commande a une syntaxe similaire :

TSplus-Security.exe débloquerips [adresses IP]

Cette commande n'a aucun effet sur les adresses IP déjà bloquées par la protection IP contre les hackers. Si vous souhaitez toujours débloquer l'une de ces adresses, veuillez utiliser la commande de liste blanche.

Protection géographique

Restreindre l'accès depuis d'autres pays

Pour autoriser l'accès à distance uniquement depuis des pays spécifiques, sélectionnez le bouton « Autoriser les connexions uniquement à partir de cette liste de pays » puis cliquez sur le bouton « Ajouter un pays ».

뉯 TS	olus Advanced Security				×
ADV	ANCEDSECURITY	Firewall > Geographic Protection			
⊞	Dashboard	Allow connections from anywhere			
්	Firewall	Allow connections only from private and allowed IP addresses			
9	Sessions	Allow connections only from this list of countries:			
٥	Ransomware	+ Add Country X Remove Country			
ŵ	Alerts	France 🔤 United States			
E	Reports				
٩	Settings				
ଙ୍କ	License				
		Apply now			
		() User Guide Version 7.1.9.11 Permanent License Activated - Ultimate	Protection e	dition.	

Une fenêtre contextuelle s'ouvrant avec une liste de pays. Sélectionnez le pays que vous souhaitez ajouter à la liste.

Vous pouvez choisir de cocher la case ci-dessous pour débloquer toutes les adresses IP précédemment bloquées pour le pays sélectionné.

Cliquez sur le bouton « Ajouter un pays » pour revenir à l'écran principal de la fonctionnalité.



Important : Pour enregistrer vos modifications, cliquez sur le bouton « Appliquer ».

뉯 TSJ	plus Advanced Security								×
ADV	ANCEDSECURITY	Firewall >	Geographic I	Protection					
□	Dashboard		Allow connection	s from anywhere					
େ	Firewall		Allow connection	s only from private and allov	ved IP addresses				
9	Sessions		Allow connection	s only from this list of count	ies:				
⋳	Ransomware	+	Add Country	X Remove Country					
ŵ	Alerts		📕 France 📕 U	United States					
	Reports								
\$	Settings								
ଙ୍କ	License								
						Apply now			
		⑦ User Guide		1	Version 7.1.9.11	Permanent License Activated - Ultimate I	Protection (edition.	

Dans cet exemple, l'accès à distance est autorisé pour les utilisateurs se connectant des États-Unis et de la France.

Un message de confirmation apparaît pour éviter de bloquer l'utilisateur connecté. Cliquez sur « Oui » pour confirmer et appliquer les modifications.



Restreindre l'accès depuis Internet

La protection géographique peut être configurée pour restreindre l'accès à votre machine uniquement aux adresses privées et <u>adresses IP sur liste blanche</u> D'accord, je suis prêt à traduire le texte que vous fournirez. Veuillez me donner le texte à traduire.

👈 TSp	olus Advanced Security		- 0	×
ADV	ANCEDSECURITY	Firewall > Geographic Protection		
⊞	Dashboard	Allow connections from anywhere		
ଌ	Firewall	Allow connections only from private and allowed IP addresses		
9	Sessions	Allow connections only from this list of countries:		
⋳	Ransomware	+ Add Country X Remove Country		
Ŵ	Alerts	France 🔤 United States		
	Reports			
:	Settings			
©⊒	License			
		Apply now		
		(2) User Guide Version 7.1.9.11 Permanent License Activated - Ultimate F	Protection edition	

Désactiver la protection géographique

Par défaut, la protection géographique permet l'accès aux utilisateurs se connectant du monde entier :

뉯 TSp	olus Advanced Security		-		×
ADV	ANCEDSECURITY	Firewall > Geographic Protection			
	Dashboard	Allow connections from anywhere			
େ	Firewall	Allow connections only from private and allowed IP addresses			
9	Sessions	Allow connections only from this list of countries:			
⋳	Ransomware	+ Add Country X Remove Country			
Ŵ	Alerts	France United States			
	Reports				
\$	Settings				
ଙ୍କ	License				
		Apply now			
		(2) User Guide Version 7.1.9.11 Permanent License Activated - Ultimate	Protection (edition.	

Déblocage des adresses IP bloquées

Lorsque l'adresse IP est bloquée, elle apparaît sur le <u>Onglet Pare-feu</u> Les adresses IP bloquées peuvent ensuite être débloquées et éventuellement ajoutées à la liste des adresses IP autorisées.

Si vous êtes bloqué, nous vous recommandons d'essayer de vous connecter depuis n'importe quel pays que vous avez autorisé sur TSplus Advanced Security, par exemple en vous connectant depuis un autre serveur distant ou en utilisant un service VPN. Vous pouvez également utiliser une session de console pour vous connecter, car cette session n'est pas une session distante et ne sera pas bloquée par TSplus Advanced Security.

Important :

•

Vérifiez que vous avez sélectionné le pays depuis lequel vous êtes actuellement connecté. Sinon, votre adresse IP sera rapidement bloquée après l'application des paramètres, vous déconnectant ainsi sans espoir de vous reconnecter à partir de la même adresse IP.

Considérez ajouter votre propre adresse IP à la liste des autorisés. <u>Adresses IP</u> pour éviter d'être bloqué par la Protection Géographique ou <u>Protection contre les attaques par force</u> <u>brute</u> caractéristiques.

Comprendre la protection géographique

La protection géographique vérifie les connexions réseau TCP entrantes, à la fois IPv4 et IPV6 (sauf lorsque le mode API Windows hérité est configuré).

Processus : La protection géographique écoute les connexions envoyées au serveur Web de TSplus Remote Access par défaut, si installé. Le nom du processus correspondant est HTML5 Service. Si vous souhaitez désactiver sa surveillance ou vérifier les connexions destinées à d'autres processus, allez à <u>Paramètres > Avancé > Protection géographique</u>.

Ports réseau : par défaut, Geographic Protection écoute les ports par défaut utilisés pour se connecter à distance à un serveur. Ces ports incluent RDP (3389), Telnet (23) et VNC. Geographic Protection prend en charge les fournisseurs VNC suivants : Tight VNC, Ultra VNC, Tiger VNC et Real VNC, qui ne sont en aucun cas liés à TSplus. Si vous souhaitez désactiver sa surveillance ou vérifier les connexions destinées à d'autres ports, allez à <u>Paramètres > Avancé > Protection géographique</u>.

Mécanismes de détection :

La protection géographique détecte les connexions entrantes en provenance de pays non autorisés à l'aide de trois mécanismes de détection différents :

- API Windows
- Suivi des événements pour Windows
- Pare-feu intégré

D'une part, le traçage d'événements pour Windows est une installation de traçage efficace au niveau du noyau qui capture les événements réseau en temps réel. Le traçage d'événements pour Windows est recommandé avec le pare-feu Windows activé (par défaut).

D'autre part, l'API Windows fonctionne très bien avec n'importe quelle configuration réseau spécifique, mais peut exercer une pression constante sur le CPU en fonction du nombre de connexions actives. Veuillez noter que l'API Windows n'est pas encore compatible avec IPv6.

Le pare-feu intégré permet la capture et le blocage en mode utilisateur des paquets réseau envoyés à la pile réseau Windows. Lorsque le pare-feu intégré est configuré pour bloquer les connexions indésirables, il est recommandé de l'utiliser pour appliquer les pays autorisés par la protection géographique.

Géolocalisation : Advanced Security inclut des données de géolocalisation publiées par MaxMind, disponibles à partir de <u>http://www.maxmind.com</u> Si vous trouvez une adresse IP non enregistrée dans son pays d'origine, veuillez contacter MaxMind directement pour résoudre le problème.

Dépannage

Si vous remarquez un jour que la Protection Géographique ne bloque pas les connexions provenant d'un pays qui n'est en réalité pas dans la liste des pays autorisés, c'est certainement

parce que :

Antivirus : Pour bloquer une adresse IP, la protection géographique ajoute une règle de blocage sur le pare-feu Windows. Donc, tout d'abord, le pare-feu doit être actif. Vous devez également vérifier si certains paramètres du pare-feu ne sont pas gérés par un autre programme, comme un antivirus. Dans ce cas, vous devrez désactiver ce programme et redémarrer le service "Pare-feu Windows". Vous pouvez également contacter l'éditeur de votre programme tiers et leur demander de trouver un moyen pour leur programme de respecter les règles lorsqu'il est ajouté au pare-feu Windows. Si vous connaissez un contact technique d'un éditeur de logiciels, nous sommes prêts à développer ces "connecteurs" pour le pare-feu. <u>Contactez-nous</u>.

VPN : Dans le cas où le client distant utilise un VPN, la Protection Géographique obtiendra une adresse IP choisie par le fournisseur de VPN. Comme vous le savez, les fournisseurs de VPN utilisent des relais partout dans le monde pour permettre à leurs utilisateurs de naviguer anonymement. Certains fournisseurs de VPN permettent aux utilisateurs de définir le pays du relais. Ainsi, les utilisateurs avec des fournisseurs de VPN peuvent être relayés à travers un pays non autorisé. Par exemple, si un fournisseur de VPN choisit une IP du Sri Lanka, ce pays doit être autorisé par la Protection Géographique. De plus, si le VPN utilise une adresse IP interne d'entreprise, alors la protection devient sans objet.

Pare-feu / Proxy : Le but d'un pare-feu matériel est de filtrer les connexions entrantes et sortantes pour les grandes entreprises. Étant donné qu'il ne s'agit que d'un filtre, il ne doit pas modifier l'adresse IP d'origine et ne doit donc pas avoir d'impact sur la protection géographique. Cependant, un proxy changerait définitivement l'adresse IP d'origine pour utiliser une adresse de réseau privé, ce qui sera toujours autorisé par la protection géographique. Le principal objectif de cette fonctionnalité est de bloquer l'accès à un serveur ouvert à Internet. Si toutes les connexions proviennent du réseau de l'entreprise, alors la protection devient sans objet.

Protection des IP des hackers

Gardez votre machine protégée contre les menaces connues telles que les attaques en ligne, l'abus de services en ligne, les malwares, les botnets et d'autres activités de cybercriminalité avec la protection IP des hackers. L'objectif est de créer une liste noire qui puisse être suffisamment sécurisée pour être utilisée sur tous les systèmes, avec un pare-feu, pour bloquer complètement l'accès, depuis et vers ses IPs répertoriées.

L'abonnement aux services de support et de mises à jour est requis.

La condition préalable essentielle pour cette cause est de ne pas avoir de faux positifs. Tous les IP répertoriés doivent être mauvais et doivent être bloqués, sans exceptions. Pour y parvenir, la protection des IP des hackers s'appuie sur les informations fournies par la communauté des utilisateurs d'Advanced Security.

La protection des IP des hackers est mise à jour automatiquement chaque jour.

Vous pouvez mettre à jour manuellement depuis l'onglet « Adresses IP bloquées », en cliquant sur le bouton « Actualiser l'IP du hacker » :

뉯 TSp	lus Advanced Security								- 🗆 X
ADV.	ANCEDSECURITY	Firewall							
		Search	Q Filter	rs: Blocked	- Bruteforce Prot	ection, Blocked - Geog	raphic Protection, Blo	cked from TSplus $i \sim$	
		IP Address	Country	Status		Date	Description		Add IP Address
	Dashboard	1.10.16.0-1.10.31.255	China	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		
_		1.19.0.0-1.19.255.255 1.32.128.0.1.32.191	South Korea	Blocked - Hac Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52 11 sept. 2024 14:38:52	Known Malicious IPs		Edit IP Address
ය	Firewall	2.56.192.0-2.56.195	Netherlands	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		
Ľ		= 2.57.185.0-2.57.185	Russia	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		Remove IP Address(es)
~		2 .57.186.0-2.57.187	Russia	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		5 11 001/
ାଷ	Sessions	2.5/.232.0-2.5/.235	France	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52 11 sept. 2024 14:38:52	Known Malicious IPs		Export to USV
		5.134.128.0-5.134.1	Iran	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		MHOIR
A	Ransomware	5.180.4.0-5.180.7.255	United States	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		WIIOIS
	Ransonnaro	\$5.183.60.0-5.183.63	United Kingdom	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		
		5.188.10.0-5.188.11	Russia	Blocked - Hac	ker IP Protection	11 sept. 2024 14:38:52	Known Malicious IPs		
Ŵ	Alerts								
		<< <			1 / 2804				
	Reports								
	Корона	Geograph	ic Protection		Brutef	orce Protection	(e	Hacker IP Pro	otection
~	Settings								
~~	Solungs	Enabled			Enabled	l.		Enabled	
~	Liconco	Access allowed	d only from your configu	red list	You are p	protected against hackers	s, network	Your are protected as	gainst 564 436 405
0.7	LICENSE	of countries inc	cluding:		scanners	and brute-force robots fr	om trying to	malicious IP address	es from our worldwide
					guess yo	ur logins and passwords		community blackhart	or known threats
				+				Last synchronization	: 25/09/2024
		Configure A	uthorized Countries		Config	gure Bruteforce Protecti	on	Refresh H	tacker IP
		(?) User Guide				Version 7.1.9.11	Permanent Lie	cense Activated - Ulti	mate Protection edition.

En conséquence, la fonctionnalité devrait créer environ 600 000 000 de règles de pare-feu bloquantes dans le pare-feu Windows.

Tableau de bord



Cliquez sur chaque tuile pour en savoir plus sur chaque fonctionnalité

La barre de menu à gauche donne accès aux différentes fonctionnalités. Chaque tuile vous permet d'accéder aux diverses fonctionnalités et paramètres offerts par TSplus Advanced Security.

Advanced Security affiche les six derniers <u>Événements de sécurité</u> Cliquez sur un événement pour ouvrir la liste complète des événements dans une fenêtre séparée.

Sous les derniers événements, trois tuiles offrent un accès rapide à :

1.

Pare-feu

2.

Sessions

Veuillez sélectionner votre langue d'affichage à l'aide du menu déroulant situé dans le coin supérieur droit, si l'application n'a pas détecté votre langue.

Enfin, cliquer sur le bouton « Aide » vous redirigera vers cette documentation.

Installer TSplus Advanced Security

Installer Advanced Security

Exécuter <u>TSplus Advanced Security Setup program</u> et ensuite **suivez les étapes** d'installation .

Vous devez exécuter le programme d'installation en tant qu'administrateur et accepter le contrat de licence du logiciel.

User Account Control	×
Do you want to allow th changes to your device	nis app to make ?
뮟 Setup	
Verified publisher: TSplus SAS	
File origin: Hard drive on this con	nputer
Security.exe" /SPAWNWND=\$70	in\Downloads\Setup-TSplus- 29C /NOTIFYWND=\$501C8
Show information about the pub	lisher's certificate
Change when these notifications	appear
Hide details	
Yes	No

Sélectionnez la langue de l'assistant de configuration si elle n'est pas détectée automatiquement.

Ensuite, sélectionnez l'une des deux options : **Recommandé** ou **Avancé** en cliquant sur les cases correspondantes.

L'option Avancée ajoute des étapes supplémentaires qui vous permettent de :

- Téléchargez uniquement le programme d'installation (ne pas installer)
- Utiliser des paramètres de proxy personnalisés

Lisez le contrat de licence et cliquez sur « J'accepte » pour reprendre l'installation.



Le programme s'installera sur votre ordinateur.

Une barre de progression est affichée en bas et indique l'avancement de l'installation.

to Satura TCalus Advanced Security version 710.24	_	~
Setup - Topius Advanced Security Version 7.1.9.24		
Installing Please wait while Setup installs TSplus Advanced Security on your computer.		
Extracting files C:\Program Files (x86)\TSplus-Security\Microsoft.Extensions.DependencyInjection.Abstractions.dll		
	C	ancel

Veuillez patienter car cela peut parfois prendre jusqu'à quelques minutes pour installer complètement le logiciel.



Une fois l'installation terminée, vous pouvez commencer à utiliser TSplus Advanced Security!

La version d'essai gratuite est entièrement fonctionnelle pendant 15 jours. N'oubliez pas de <u>activez votre licence</u> et à <u>mettez à jour vers la dernière version</u> pour maintenir la protection Advanced Security à son meilleur !

Scénarios d'installation avancés

Le <u>TSplus Advanced Security Classic Setup program</u> gère les scénarios suivants car il peut être exécuté à partir de la ligne de commande :

- Installer silencieusement, en fournissant les paramètres /VERYSILENT / SUPPRESSMSGBOXES
- Empêcher le redémarrage à la fin de l'installation en fournissant le paramètre /NORESTART. Ce paramètre est généralement utilisé avec ce qui précède.
- Volume Licensing pour activer votre licence directement lors de l'installation (veuillez vous référer à la documentation ou <u>contactez-nous</u> pour plus d'informations

Désinstaller TSplus Advanced Security

Pour désinstaller complètement TSplus Advanced Security, ouvrez le répertoire C:\Program

Files (x86)\TSplus-Security.

I Image: State View				- 0	× ~ 2
$\leftarrow \rightarrow \checkmark \uparrow$ \rightarrow This PC > Local Di	sk (C:) > Program Files (x86)	~ (ل Search Proo	jram Files (x86)	م
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	📙 Windows Defender	7/15/2019 1:39 PM	File folder		
	Windows Mail	7/1/2019 10:21 PM	File folder		
Jeterat Fordance	📙 Windows Media Player	10/2/2019 3:25 PM	File folder		
Internet Explorer	📙 Windows Multimedia Platform	7/16/2016 3:23 PM	File folder		
Java	Windows NT	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	Windows DowerShell	7/16/2016 2:22 014	Eile folder		

Ensuite, double-cliquez sur l'application "unins000" pour exécuter le programme de désinstallation.

System.ValueTuple.dll	15/05/2018 13:29
System.Xml.ReaderWriter.dll	08/09/2024 21:49
System.Xml.XDocument.dll	08/09/2024 21:49
System.Xml.XmlDocument.dll	08/09/2024 21:49
System.Xml.XmlSerializer.dll	08/09/2024 21:49
System.Xml.XPath.dll	08/09/2024 21:49
System.Xml.XPath.XDocument.dll	08/09/2024 21:49
systemaudit.out	27/09/2024 16:48
TraceReloggerLib.dll	26/06/2024 23:34
💙 TSplus-Security	11/09/2024 13:42
TSplus-Security.exe.config	11/09/2024 13:37
💙 TSplus-Security-Service	11/09/2024 13:42
TSplus-Security-Service.exe.config	11/09/2024 13:37
💙 TSplus-Security-Session	11/09/2024 13:42
TSplus-Security-Session.exe.config	11/09/2024 13:37
unins000.dat	11/09/2024 16:36
🤠 unins000	11/09/2024 16:35
unins000.msg	11/09/2024 16:36
🖻 uninstall	11/09/2024 13:37
version	11/09/2024 13:37
WindowsFirewallHelper.dll	10/01/2022 16:36

Cliquez sur oui dans la fenêtre suivante pour supprimer complètement TSplus Advanced Security et tous ses composants.

À moins d'une configuration différente, Advanced Security ajoute des règles de blocage au parefeu Windows. Cliquez sur « Débloquer les adresses IP » pour débloquer et supprimer toutes les adresses IP précédemment bloquées par Advanced Security.

Important : Veuillez noter que la suppression de toutes les règles peut prendre jusqu'à une heure. Pour cette raison, nous vous recommandons de supprimer les règles directement à partir de la console Windows Firewall avec Advanced Security.

Optional tasks Select any optional tasks to be performed by the uninstall program.	t
Would you like to unblock all previously blocked IP adresses?	
Uninstall	nuler

Le logiciel sera complètement désinstallé de votre machine.

Gestion des autorisations

Depuis la version 4.3, TSplus Advanced Security propose une fonctionnalité de Permissions, permettant à l'administrateur de gérer et/ou d'inspecter les privilèges des utilisateurs/groupes.

Sur le tableau de bord des autorisations, la liste des utilisateurs et des groupes et la liste des disponibles **fichiers, dossiers, registres et imprimantes** sont affichés côte à côte.

Tout est visible d'un seul coup d'œil, ce qui le rend super facile à **Inspecter** et **Gérer/Modifier** privilèges pour un utilisateur à la fois et donc pour augmenter la précision des restrictions.

Gérer les autorisations

Sur l'onglet Gérer, pour chaque utilisateur ou groupe sélectionné dans l'arborescence à gauche, vous pouvez :





- Refuser Lorsque vous cliquez sur le bouton Refuser, l'utilisateur sélectionné se verra refuser le privilège sur l'objet système de fichiers sélectionné. Si un fichier est sélectionné, l'utilisateur sélectionné se voit refuser le privilège de lire le fichier sélectionné (FileSystemRights.Read). Si un répertoire est sélectionné, l'utilisateur sélectionné se voit refuser le privilège de lire et de lister le contenu du répertoire (FileSystemRights.Read et FileSystemRights.ListDirectory).
- Lire Lorsque vous cliquez sur le bouton Lire, l'utilisateur sélectionné se verra accorder des privilèges sur l'objet système de fichiers sélectionné. Si un fichier est sélectionné, l'utilisateur sélectionné se voit accorder le privilège de lire le fichier sélectionné et d'exécuter si le fichier est un programme (FileSystemRights.ReadAndExecute). Si un répertoire est sélectionné, l'utilisateur sélectionné se voit accorder le privilège de lire et de lister ou d'exécuter le contenu du répertoire (FileSystemRights.ReadAndExecute et FileSystemRights.ListDirectory et FileSystemRights.Traverse).
- Modifier Lorsque vous cliquez sur le bouton Modifier, l'utilisateur sélectionné se verra accorder des privilèges sur l'objet système de fichiers sélectionné. Si un fichier est sélectionné, l'utilisateur sélectionné se voit accorder le privilège de modifier le fichier sélectionné (FileSystemRights.Modify). Si un répertoire est sélectionné, l'utilisateur sélectionné se voit accorder le privilège de modifier et de lister le contenu du répertoire, ainsi que de créer de nouveaux fichiers ou répertoires (FileSystemRights.Modify et FileSystemRights.CreateDirectories et FileSystemRights.CreateFiles et FileSystemRights.ListDirectory et FileSystemRights.Traverse).
- Propriété Lorsque vous cliquez sur le bouton Propriété, l'utilisateur sélectionné se verra accorder un contrôle total sur l'objet système de fichiers sélectionné (FileSystemRights.FullControl).

Les mêmes options de permissions sont possibles pour chaque registre, en sélectionnant le bouton correspondant sous la vue arborescente de droite :

👈 TSp	lus Advanced Security					-		×
ADVANCEDSECURITY Sessions > Permissions Management								
		🖉 Deny 💿 Read	🧨 Modify	🐼 Ownership				
⊞	Dashboard	Users and Groups - AD Domain		Select one or multiple files or folders to ea	dit permissions			
		Default View		Name	Permissions Owner	^		
ය	Firewall	Switch View		E 📂 C:\ 🗈 🧰 \$Recycle.Bin	Read AUTORITE	ти		
				🗄 🛅 SWinREAgent	Read BUILTIN/Ad	m		
Ø	Sessions	Users	^	Backupparam Documents and Settings	Deny AUTORITE			
Ŭ		Administrateur (protected)		🗉 🛅 PerfLogs	Deny AUTORITE I	TV		
		user1		🗉 🚞 Program Files	Read NT SERVICE	×1		
Ö	Ransomware	user2		Program Files (x86) Program Data	Read NT SERVICE			
		user3		Programbata	Deny AUTORITE			
				Give System Volume Information	Deny BUILTIN\Ad	m		
Û	Alerts	Accès compatible pré-Windows 20	00	🗉 🧰 tmp	Read BUILTIN\Ad	m		
		Accès DCOM service de certificats		😑 📂 Users	Full Control AD\user2			
				🖽 🛅 admin	Deny BUILTIN\Ad	m		
	Reports			🗄 🛅 administrateur	Deny BUILTIN\Ad	m		
		Administrateurs clés Enterprise		All Users	Pead AUTORITE			
		Administrateurs de l'entrepit TSpl	us Advanced Se	curity - Please Wait	Deny AUTORITE	T		
1 23	Settings	Administrateurs du scriena			Deny AUTORITE	TV		
		Plea	ise Wait		Full Control BUILTIN\Ad	m		
		Contrôleurs de domaine			Read BUILTIN\Ad	m		
⊙⊐	License				Dasid NT CEDVICE	N7		
		Contrôleurs de domaine d'e				<u> </u>		
		<						
					e liems.			
		C Local users and Groups			0.851			
		AD Users and Groups		Files and Folders O Regi	stry O Printers			
		 User Guide 		Version 7. <u>1.9.11</u>	Permanent License Activated - U	imate Prote <u>ctio</u>	1 editio <u>n.</u>	
		0						

Et pour chaque imprimante :

뉯 тар	olus Advanced Security								-		_
AD∨	ANCEDSECURITY	Sessions	> Permissi	ons Mar	agemei	nt					
		⊘ Deny	O Print	🥂 Manag	e Documents	🐼 Manage Pr	inter				
⊞	Dashboard	Users and Groups - AD	Domain		Select one o	r multiple printers	to edit permissions				
			Default View		Name			Permissions			
ය	Firewall	Switch View			Print	ers Virtual Printer		Print			
					출	Universal Printer		Print			
Ø	Sessions	Users	rotected)	^	E E	Microsoft XPS Doci Microsoft Print to P	ument Writer PDF	Print Print			
×.			rateur (protected)								
A	Danaamwara	user1									
Ŀ	Ransomware	user3									
		user4									
ŵ	Alerts	Groups	mpatible pré-Windows	2000							
			OM service de certificat	s							
Ē	Reports	Administ	rateurs (protected) trateurs clés								
-			rateurs clés Enterprise								
-5-		Administ	rateurs de l'entreprise								
103	Settings	- Administ	rateurs Hyper-V								
			du domaine								
©⊐	License	Controle	eurs de domaine eurs de domaine clonabl	es							
			urs de domaine d'entre	prise en lect 🛩							
		<		>	Tip: keep the	CTRL key pressed	to select multiple iter	ms.			
		O Local Users and Gro	ups				,,				
					O Files an	nd Folders	Registry	Printers			
		AD Users and Group	05								
		 User Guide 				Version 7	.1.9.11	Permanent License Activate	ed - Ultimate Protecti	ion edition	n. –

Veuillez noter que toutes les autorisations refusées ou accordées à un répertoire sont appliquées de manière récursive aux objets du système de fichiers contenus dans ce répertoire. Le diagramme ci-dessous détaille les appels API lorsque des droits sont appliqués à un objet du système de fichiers :



Documentation :

- Sécurité des objets : <u>https://docs.microsoft.com/fr-fr/dotnet/api/</u> system.security.accesscontrol.objectsecurity?view=netframework-4.5.2
- Droits du système de fichiers : <u>https://docs.microsoft.com/fr-fr/dotnet/api/</u> system.security.accesscontrol.filesystemrights?view=netframework-4.5.2

Inspecter les autorisations

Dans l'onglet Inspecter, pour chaque dossier, sous-dossier ou fichier sélectionné dans l'arborescence de gauche, vous pouvez voir les autorisations attribuées correspondantes aux utilisateurs ou groupes dans l'arborescence de droite.



Vous pouvez actualiser le statut des dossiers pour qu'ils soient mis à jour en temps réel.

Un audit peut être activé en sélectionnant le dossier, le sous-dossier ou le fichier souhaité et en cliquant sur le bouton « Activer l'audit » en haut :

🔁 TSp	olus Advanced Security								- 0	×
ADV	ANCEDSECURITY	Sessions > Perm	issions Manag	jemo	ent					
Ē	Dashboard	C Refresh Q Dis	sable Audit	/iew Au	dit					
		Name	o euro permissions		Permissions	Name	Permission	5		
~	Firewall	E 🎅 CA			2	AD\admin	Full Contro	1		
Ŵ	T II O Wall	Green SRecycle.Bin			2	AUTORITE NT\Système	Full Contro	1		
		SwinkEAgent Backupparam			2	BUILTIN\Administrateu	rs Full Contro			
9	Sessions	Documents and Settings								
٥	Ransomware		Authorization Change Aud	it		×				
ţ	Alerts	System Volume Information Definition Definition	This computer is Please ensure tha authorization chi	a memb at your g ange au	er of an Active global security udit.	Directory domain. policies allow				
⊞	Reports	icia admin icia administrateur icia administrateur icia All Users icia Default				ОК				
\$	Settings	Constant User Default User Default User Default User Default User Default user1 dectop ini								
©7	License		O Printers	~						
		(?) User Guide			Vers	ion 7.1.9.11	Permanent License Activate	ed - Ultimate <u>Prote</u>	ection e <u>dit</u> i	ion.

Le bouton « Voir l'audit » vous permet de voir l'audit correspondant dans le Visualiseur d'événements :



Les mêmes possibilités d'inspection sont disponibles pour chaque registre et imprimante en sélectionnant le bouton correspondant sous la vue arborescente de gauche :

뉯 TSp	lus Advanced Security							-		×
ADV.	ANCEDSECURITY	Sessions > I	Permissions Ma	anageme	ent					
		🗘 Refresh	Q Enable Audit	O View Aud	lit					
⊞	Dashboard	Select one or multiple registry	v keys to edit permissions		Permissions					
		Name		^		Name	Permissions			
~	Firowall	🗉 📂 HKEY_LOCAL_MACHIN	E		2	AUTORITÉ DE PACKAGE D'APPLICATION\TOUS	Read			
w	i iiowali	😑 芦 HARDWARE			2	AUTORITE NT\RESTRICTED	Read			
		ACPI ACPI ACPI ACPI			2	AUTORITE NT\Système	Full Control			
9	Sessions	DEVICEMAP				BUILTIN\Administrateurs	Full Control			
		🗷 🛅 RESOURCEMA	Р		2	Tout le monde	Read			
۹	-	E SAM								
	Ransomware	T-Zip								
		🗉 🛅 Amazon								
Ŵ	Alerts	Classes Clients								
, T		CVSM								
		🛅 DefaultUserEn	vironment							
	Reports	Digital River								
		Gothet Gothet FabulaTech								
~	Settings	🗷 🛅 Google								
~~~	Settings	E Contel								
		JavaSoft     Microsoft								
©⊒	License	🗉 🛅 Mozilla								
		🗄 🚞 mozilla.org								
		ODBC      OpenSSH		~						
		Files and Folders     Re	egistry O Printers							
		(?) User Guide			Versi	on 7.1.9.11 Permanent Licens	se Activated - Ultimate Pr	otection e	dition.	

뉯 TSp	lus Advanced Security							-		×
	ANCEDSECURITY	Sessions >	Permissions Ma	anageme	ent					
		🗘 Refresh	Q Enable Audit	O View Aud	lit					
⊞	Dashboard	- Select one or multiple printer	s to edit permissions		Permissions					
		Name	Pe	ermissions		Name	Permissions			
ය	Firewall	🖃 📂 Printers		6	AD\administrateur	Print, Manage Documents				
		Virtual Printer			2	AUTORITÉ DE PACKAGE D'APPLICATION\TOUS	Print			
~		A Microsoft XPS Do	cument Writer		2	BUILTIN\Administrateurs	Print, Manage Printer			
w w	Sessions	Hicrosoft Print to	PDF		2	BUILTIN\Opérateurs d'impression	Print, Manage Printer			
					2	BUILTIN\Opérateurs de serveur	Print, Manage Printer			
A	Ransomware				2	CREATEUR PROPRIETAIRE				
					2	Tout le monde	Print			
Ŵ	Alerts									
▣	Reports									
¢3	Settings									
©77	License									
		<		>						
		Files and Folders     R	egistry 🖲 Printers							
		⑦ User Guide			Versi	on 7.1.9.11 Permanent Licens	e Activated - Ultimate Pr	otection	edition	

# **TSplus Advanced Security - Prérequis**

## **Exigences matérielles**

TSplus Advanced Security prend en charge les architectures 32 bits et 64 bits.

# Système d'exploitation

Votre matériel doit utiliser l'un des systèmes d'exploitation ci-dessous :

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

Les architectures 32 et 64 bits sont toutes deux prises en charge.

# **Exigences logicielles**

TSplus Advanced Security nécessite les prérequis suivants :

•

Temps d'exécution : <u>.NET Framework</u> 4.7.2 ou supérieur

•

Microsoft Windows 7 SP1 et Windows 2008 R2 SP1 nécessitent une mise à jour supplémentaire pour prendre en charge la signature croisée SHA2. <u>KB4474419</u> Cette mise à jour permet au pare-feu intégré de TSplus Advanced Security et à la protection contre les ransomwares de fonctionner correctement.

**Remarque :** Ces prérequis seront automatiquement installés par le programme d'installation s'ils sont manquants sur le système.
## TSplus Advanced Security - Guide de démarrage

### Prérequis

TSplus Advanced Security nécessite les prérequis suivants.

• Système d'exploitation : Microsoft Windows version 7, Service Pack 1 (build 6.1.7601) ou Windows 2008 R2, Service Pack 1 (build 6.1.7601) ou supérieur.

La suite **les prérequis seront automatiquement installés par le programme d'installation** si manquant :

Temps d'exécution : ...NET Framework 4.5.3 ou supérieur

•

•

Microsoft Windows 7 SP1 et Windows 2008 R2 SP1 nécessitent une mise à jour supplémentaire pour prendre en charge la signature croisée SHA2 (<u>KB4474419</u> Cette mise à jour permet au pare-feu intégré de TSplus Advanced Security et à la protection contre les ransomwares de fonctionner correctement.

Veuillez vous référer à la <u>documentation</u> pour plus de détails sur les prérequis.

## Étape 1 : Installation

Le dernier programme d'installation de TSplus Advanced Security est toujours disponible ici : _ <u>Dernier programme d'installation de TSplus Advanced Security</u> Veuillez télécharger le programme d'installation et suivre l'assistant de configuration.

Le programme d'installation de TSplus Advanced Security ne nécessite généralement pas de redémarrer votre système pour compléter l'installation.

Toute nouvelle installation commence une période d'essai complète de 15 jours. N'hésitez pas à <u>contactez-nous</u> si vous rencontrez un obstacle ou si vous avez un problème lors de la

configuration de TSplus Advanced Security.

Une fois l'installation terminée, une nouvelle icône s'affiche sur votre bureau. Double-cliquez sur cette icône pour ouvrir TSplus Advanced Security et commencer à configurer les fonctionnalités de sécurité.



Veuillez vous référer à la <u>documentation</u> pour des instructions d'installation complètes.

## Étape 2 : Configuration de TSplus Advanced Security

Vous avez lancé <u>TSplus Advanced Security</u> et a commencé à configurer des fonctionnalités pour protéger votre serveur contre les activités malveillantes et appliquer des politiques de sécurité strictes.



Dans la colonne de gauche, la page d'accueil permet un accès rapide à la configuration des fonctionnalités de protection contre les ransomwares, de protection contre les attaques par force brute et de protection géographique.

Démarrer <u>Protection contre les ransomwares</u> période d'apprentissage pour permettre à Advanced Security d'identifier les applications et comportements légitimes sur votre système en cliquant sur le carreau suivant :



<u>Protection contre les attaques par force brute</u> est généralement opérationnel après l'installation. Sinon, cliquez sur le **Défense répétée contre les attaques par force brute** titre pour résoudre les problèmes et appliquer la configuration système requise. Par défaut, cette fonctionnalité bloque les attaquants après 10 tentatives de connexion échouées.



Enfin, ajoutez votre pays à la liste des pays autorisés à partir desquels les clients peuvent se connecter. Cliquez sur la tuile. **Autoriser les connexions depuis un autre pays** et ajoutez votre pays pour configurer <u>Protection géographique</u>



Vous êtes prêt ! N'oubliez pas de <u>activez votre licence</u> et à <u>mettez à jour vers la dernière</u> <u>version</u> pour maintenir la protection Advanced Security à son meilleur !

### Étape 3 : Révision des menaces empêchées

Maintenant que vous avez configuré les fonctionnalités clés de sécurité avancée, les menaces évitées seront signalées dans le tableau de bord.



Aussi, le <u>Hacker IP</u> La protection maintient la machine protégée contre les menaces connues en bloquant plus de 500 000 000 d'adresses IP malveillantes connues.

Tout le <u>événements de sécurité</u> peut être affiché en cliquant sur le **Voir tous les événements** carreau.

# Étape 4 : Tirer parti d'autres fonctionnalités de sécurité pour améliorer la protection

En bas, quatre autres fonctionnalités de sécurité peuvent être accessibles et configurées pour améliorer la protection de votre machine.

Ajustez et surveillez les privilèges d'accès sur vos systèmes de fichiers locaux, imprimantes et clés de registre pour garantir que chaque utilisateur a accès aux ressources pertinentes, avec

le <u>Permissions</u> fonctionnalité.

•

Définir la période de temps pendant laquelle les utilisateurs sont autorisés à se connecter avec le <u>Working Hours</u> fonctionnalité. Les utilisateurs seront déconnectés après leurs heures de travail autorisées.

•

Personnalisez et sécurisez les sessions utilisateur avec le <u>Bureau sécurisé</u> fonctionnalité. Personnalisez, cachez, refusez l'accès aux éléments de l'interface de session pour les utilisateurs locaux.

•

Validez le nom du client distant lorsqu'un utilisateur se connecte à votre machine avec _ <u>Protection des points de terminaison</u> Cette fonctionnalité valide les noms des machines clientes pour chaque utilisateur connecté à distance.

Il y a plus ! Passer en mode avancé vous donne accès à plus de fonctionnalités.

Merci d'utiliser TSplus Advanced Security!

## **Protection contre les ransomwares**

La protection contre les ransomwares vous permet de détecter, bloquer et prévenir efficacement les attaques par ransomware. TSplus Advanced Security réagit dès qu'il détecte un ransomware sur votre session. Il possède à la fois **analyse statique et comportementale** :

- Le **analyse statique** permet au logiciel de réagir immédiatement lorsqu'un nom d'extension est modifié,
- Le **analyse comportementale** examine comment un programme interagira avec les fichiers et détectera une nouvelle souche de ransomware.

Vous pouvez l'activer en cliquant sur « Activer la protection contre les ransomwares » dans l'onglet de protection contre les ransomwares :

뉯 TSp	lus Advanced Security					×
ADV	ANCEDSECURITY	Ransomware				
⊞	Dashboard	( Learning period is ongoing. Click here to enable Ransomwa	are Protection.			
ଌ	Firewall	Click here to stop the learning period.				
9	Sessions	Email alerts are not configured yet. Click here to configure	email alerts.			
₿	Ransomware	Date Interrupted Program		Review & Act		
Ų	Alerts					
	Reports					
\$	Søttings					
©7	License	Manage programs allow list				
		[O] Snapshots	Quarantine			
		🕐 User Guide	Version 7.1.9.11	Permanent License Acti	vated - Ultimate Protection editio	Π.

#### Période d'apprentissage

Après avoir activé la fonction de protection contre les ransomwares, la période d'apprentissage est automatiquement activée. Pendant la période d'apprentissage, tous les programmes détectés par la fonction de protection contre les ransomwares seront considérés comme des

faux positifs et pourront reprendre leur exécution. Les programmes détectés comme faux positifs seront automatiquement ajoutés à la liste des programmes autorisés.

Cette fonctionnalité permet de configurer la protection contre les ransomwares sur un serveur de production sans perturber son activité. Nous recommandons de commencer par une période d'apprentissage de 5 jours pour identifier toutes les applications commerciales légitimes.



Si vous arrêtez la période d'apprentissage, cela désactivera la protection contre les ransomwares. Cliquez sur le bouton « La protection contre les ransomwares est désactivée » pour réactiver la période d'apprentissage.



#### Action de protection contre les ransomwares

Il scanne rapidement votre disque(s) et affiche le(s) fichier(s) ou programme(s) responsable(s), en plus de fournir une liste des éléments infectés. TSplus Advanced Security arrête automatiquement l'attaque et met en quarantaine le(s) programme(s) ainsi que le(s) fichier(s) chiffré(s) avant son intervention.

Seul l'administrateur peut les ajouter à la liste blanche, en saisissant le chemin du programme souhaité sur la ligne du bas et en cliquant sur « Ajouter » :



#### Rapport de protection contre les ransomwares

TSplus Advanced Security empêche des événements catastrophiques pour les entreprises en éliminant les ransomwares à un stade précoce.

L'administrateur a accès à des informations concernant la source de l'attaque et les processus en cours, et apprend donc à anticiper ces menaces.

Remarque La protection contre les ransomwares observe comment les programmes interagissent avec les fichiers système et personnels. Pour garantir un niveau de protection supérieur, la protection contre les ransomwares crée des fichiers leurres dans des dossiers clés où les ransomwares commencent souvent leur attaque. Par conséquent, quelques fichiers cachés peuvent apparaître dans les dossiers de bureau et de documents des utilisateurs, ainsi que dans d'autres emplacements. Lorsqu'il détecte un comportement malveillant, il stoppe immédiatement le ransomware (ou demande si l'utilisateur connecté est un administrateur). La protection contre les ransomwares utilise des techniques de détection comportementale pures et ne s'appuie pas sur des signatures de logiciels malveillants, ce qui lui permet de détecter des ransomwares qui n'existent pas encore.

Vous pouvez configurer vos paramètres SMTP afin que TSplus Advanced Security vous envoie des alertes par e-mail pour mettre en évidence des événements de sécurité importants en cliquant sur le bouton sous celui d'activation de Ransomware :

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

👈 TSp	lus Advanced Security		- 1		×
ADV	ANCEDSECURITY	Ransomware > Configure E-Mails			
		Simply enter your e-mail and receive directly your alerts and reports by e-mail:			
⊞	Dashboard	Or rather use your own SMTP settings			
ଚ	Firewall	SMTP Hostname localhost			
9	Sessions	SMTP Port 25			
₿	Ransomware	Use SSL			
â	Alerts	SMTP Username			
Ē	Poporto	SMTP Password			
	Reports	Send Email To			
<b>1</b>	Settings				
©⊒	License	Apply now Test			
	a di seconda	(?) User Guide Version 7.1.9.11 Permanent License Activated - Ultimat	e Protection er	lition.	

Entrez votre nom d'hôte SMTP, le port et cochez la case Utiliser SSL, puis changez le port de 25 à 465 si vous souhaitez utiliser SSL.

Entrez le nom d'utilisateur et le mot de passe SMTP, ainsi que les adresses de l'expéditeur et du destinataire.

Les paramètres de messagerie peuvent être validés en envoyant un test lors de l'enregistrement des paramètres SMTP.

#### Instantanés

Les instantanés pris par la protection contre les ransomwares sont visibles sous l'onglet Instantanés :

👈 TSp	lus Advanced Security						-		×
ADV	ANCEDSECURITY	Ransomware	> Snapshots						
	Deathered	C Refresh	🧨 Restore	X Remove					
	Dasnboard	Name			Date				
ଚ	Firewall								
9	Sessions								
₿	Ransomware								
ΰ	Alerts								
	Reports								
<b>1</b> 23	Settings								
©7	License								
		⑦ User Guide		Version 7.1	.9.11 Permanent	License Activated -	Ultimate Protection	edition.	

La liste peut être actualisée en cliquant sur le bouton correspondant. Chaque élément peut être restauré ou supprimé.

### Quarantaine

Les programmes mis en quarantaine sont visibles sous l'onglet Quarantaine : Les programmes potentiellement indésirables sont conservés en quarantaine indéfiniment jusqu'à ce que vous décidiez de l'action à entreprendre.

De cette manière, Advanced Security garantit la sécurité de votre machine tout en vous offrant la possibilité de gérer les éléments mis en quarantaine comme vous le souhaitez.

Cela peut être utile si vous devez récupérer un fichier ou un programme qui a été neutralisé. **Cette décision est prise à vos propres risques.** 

Vous pouvez également supprimer définitivement tous les fichiers ou programmes de votre choix directement depuis le dossier de quarantaine situé dans le répertoire d'installation d'Advanced Security.

👈 TSp	lus Advanced Security		- 0	×
ADV	ANCEDSECURITY	Ransomware > Quarantine		
□	Dashboard	Restore Program X Remove Program(s)		
ය	Firewall	Program File Falth		
9	Sessions			
∂	Ransomware			
Ŵ	Alerts			
	Reports			
\$ <u></u>	Settings			
ଙ୍କ	License			
		() User Guide Version 7.1.9.11 Permanent License Activated - Ultimate	Protection editi	on.

Chaque élément peut être restauré ou supprimé.

Les fichiers ignorés ne sont pas utilisés pour détecter d'éventuelles actions malveillantes et ne sont pas sauvegardés lorsqu'ils sont modifiés. L'idée est d'exclure toute opération sur des fichiers volumineux ou non pertinents (comme les fichiers journaux).

- système
- dll
- exe
- tmp
- ~tmp
- temp
- cache
- Ink
- 1
- 2
- 3
- 4
- 5
- LOG1
- LOG2
- customDestinations-ms
- journal
- wab~
- vmc
- vhd
- vhdx
- vdi
- vo1

- vo2
- vsv
- vud
- iso
- dmg
- image clairsemée
- cab
- msi
- mui
- dl_
- wim
- ost
- 0
- qtch
- ithmb
- vmdk
- vmem
- vmsd
- vmsn
- vmss
- vmx
- vmxf
- menudonnées
- icône d'application
- informations sur l'application
- pva
- pvs
- pvi
- pvm
- fdd
- hds
- drk
- mémoire
- nvram
- disque dur
- pk3
- pf
- trn
- automaticDestinations-ms

# Avertissement concernant l'extension des fichiers de sauvegarde

L'extension de fichier utilisée pour enregistrer les fichiers modifiés est : **instantané**. Le pilote interdit toute action de modification ou de suppression sur ces fichiers, sauf par le service TSplus

Advanced Security. Arrêter le service supprime les fichiers sauvegardés. Pour supprimer ces fichiers manuellement, vous devez décharger temporairement le pilote.

### Configuration du fichier de sauvegarde

Par défaut, le répertoire des fichiers sauvegardés est situé dans le répertoire d'installation de TSplus Advanced Security et s'appelle « snapshots ». Cependant, il est possible de définir un autre emplacement pour ce répertoire. Cela peut permettre à l'administrateur de définir un répertoire situé sur un disque plus rapide (SSD) ou sur un disque plus grand selon ses besoins. Le chemin du répertoire de sauvegarde ne doit pas être un chemin UNC, sous la forme de :

// //

## Ajouter des utilitaires de sauvegarde à la liste blanche

Nous recommandons d'ajouter des utilitaires de sauvegarde dans la liste blanche.

## **Rapports**



## Sessions sécurisées

#### **Avertissement**

- Les sessions sécurisées sont très susceptibles de entrer en conflit avec les politiques de sécurité définies par Active Directory.
- Le principal objectif des sessions sécurisées est de personnaliser l'interface utilisateur, et non d'appliquer des autorisations d'accès. Son utilisation doit être combinée avec la fonctionnalité des autorisations pour sécuriser l'accès à différents lecteurs.

Vous pouvez configurer le niveau de sécurité pour chaque utilisateur ou groupe. Il existe trois niveaux de sécurité :

- Le Mode Windows où l'utilisateur a accès à une session Windows par défaut.
- Le Mode de sessions sécurisées où l'utilisateur n'a pas accès au Panneau de configuration, aux programmes, aux disques, au navigateur, pas de clic droit... : pas d'accès aux ressources du serveur. Il a juste accès aux documents, aux imprimantes, à la touche Windows et peut déconnecter sa session.
- Le **Mode Kiosque** est le plus sécurisé, où l'utilisateur a des actions très limitées dans sa session.





#### Personnalisation

Dans n'importe quel mode, vous avez la possibilité de personnaliser la sécurité à trois niveaux :

Sécurité de bureau :

Security Le	/el Customization
ktop Security Disks Control Applications Control	Currently customizing
Remove Recycle Bin	
Remove Quick Access	AD)user1
Remove This PC	AD (USEI I
Remove My Documents	
Remove My Recent Documents	
Remove My Music	Currently based on
Remove My Pictures	
Remove My Videos	Secured Desktop Mode
Remove Frequently Used Programs	20
Remove Programs	
Remove Help and Support	
Remove Control Panel	
Remove Printers	
Remove Network	
Remove Recent Files	
No Network Neighborhood	
Remove Context Menu	
Restrict right click	
Disable 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	
No Internet Explorer	

#### Contrôle des disques :

뉯 TSplus A	dvanced Secu	rity - Security l	evel Customiz	ation			- 🗆 X
			Secu	rity Leve	l Customiz	zation	
Desktop Sec	urity Disks Co	ontrol Applic	ations Control				Currently customizing
Hide Selec	ted Disks						100000
A	В	⊠ c	D	E	F	G	AD\user1
⊠н	<b>∠</b> I	L \	К	Δ Γ	M	N 🗹	
⊠ o	P P	Q	R	✓ s	Т	υ 🗹	Currently based on
V	⊻ w	∠ x	✓ Y	✓ z			Secured Desktop Mode
Deny Acce	Sele ss to Selected I	ct all Disks			Unselect all		
						ØG	
~ *		E1 *	<u> </u>	E 2			
	Sele	ct all			Unselect all		

Contrôle des applications :

💙 TSplus Advanced Security - Security Level Customization	- 🗆 X
Security Level Customization	
Desktop Security Disks Control Applications Control	Currently customizing
Image: cmd.exe     powershell.exe     taskmgr.exe     mmc.exe     gpedit.msc	AD\user1
regedit.exe powershell_ise	Currently based on Secured Desktop Mode
Applications listed above will be prohibited.	
Add Remove	

#### Priorités des règles des utilisateurs/groupes

Lorsque un utilisateur ouvre une nouvelle session sur le serveur :

- 1. Si cet utilisateur a un niveau de sécurité directement défini pour lui-même, alors ce niveau de sécurité est appliqué.
- Si cet utilisateur n'a pas de niveau de sécurité directement défini pour lui-même, alors TSplus Advanced Security chargera tous les paramètres de niveau de sécurité existants pour tous les groupes de cet utilisateur et conservera les règles les plus permissives.

Par exemple, si un premier groupe a une règle pour supprimer l'icône de la Corbeille du bureau, mais que cette règle est désactivée pour un deuxième groupe, alors l'utilisateur aura l'icône de la Corbeille sur son bureau. Les mêmes règles de priorité s'appliqueront à chaque règle personnalisée (Sécurité du Bureau, Contrôle des Disques et Contrôle des Applications) ainsi qu'au niveau de sécurité principal (le mode Windows étant considéré comme plus permissif que le mode Bureau Sécurisé, qui est considéré comme plus permissif que le mode Kiosque).

N.B : Pour désactiver le clic droit partout, vous devez sélectionner les deux options suivantes :

- Restreindre le clic droit
- Supprimer le menu contextuel

## Paramètres - Liste des programmes autorisés

Sur le **Onglet Programmes** vous pouvez ajouter des programmes à la liste des programmes autorisés, qui ne seront pas vérifiés par la protection contre les ransomwares de TSplus Advanced Security Par défaut, tous les programmes Microsoft sont sur liste blanche.

뉯 тรр	olus Advanced Security									-		$\times$
	ANCEDSECURITY	Ransomware	> Whitelisted									
		+ Select Folder	+ Add Application	× Re	move	Ø Distrust	Publisher					
⊞	Dashboard	Enter a program file path to add a p Protection.	rogram to the Ransomware Protectio	n prograr	n allow list. This executable	e will be able to	create, change and c	lelete your personal file	es without triggerii	ng Ransor	nware	
ය	Firewall	Application Path			Publisher		Publisher Confid	ence				
		C:\Program Files (x86)\Microso C:\Users\thomas\Desktop	oft Visual Studio\Installer\setup.ex	e	Microsoft Corporation		Trusted Publishe	r				
9	Sessions	C:\wsession\UniversalPrinter\	Universal Printer Server. exe		TSplus SAS		Trusted Publishe	r				
₿	Ransomware											
Ŵ	Alerts											

Cliquez sur le bouton « Ajouter une application » pour ajouter un programme. Vous pouvez également les supprimer en sélectionnant l(es) application(s) et en cliquant sur le bouton Supprimer l(es) application(s).

## Paramètres - Liste des utilisateurs autorisés

#### Vue avancée

Avec la vue Avancée, ajoutez et gérez des utilisateurs et des groupes de tous les domaines accessibles.

Vous pouvez passer de la vue par défaut à la vue avancée en utilisant le bouton « Changer de vue ».

La vue avancée est utilisée pour afficher et gérer tous les utilisateurs et groupes configurés actuellement. Elle vous permet également d'ajouter de nouveaux utilisateurs et groupes à la liste pour les configurer, en utilisant le sélecteur de recherche AD de Windows. Vous pouvez le faire en cliquant sur le bouton « Ajouter un utilisateur/groupe ». Vous pourrez alors ajouter tout utilisateur disponible depuis n'importe quel domaine accessible depuis votre serveur.

La vue avancée est disponible sur les fonctionnalités Permissions, Working Hours, Secure Desktops. Exemple :

👈 TSp	lus Advanced Security				- 🗆 X
	ANCEDSECURITY	Sessions > Restrict Working	Hours		
	Dashboard	Users and Groups - AD Domain Default View Switch View	Not configured for this user/group     Always authorize		
ය	Firewall	S Users     S admin     A dministrateur (allowed)	Always block     Authorize only during these time ranges:     Monday:	09:00	to 17:30
0	Sessions	- 옾 <mark>user1</mark> - 옾 user2 - 옾 user3	Tuesday:	09:00	to 17:30
ð	Ransomware	2 user4     2. Groups     2. Accès compatible pré-Windows 2000     2. Accès Compatible pré-Windows 2000     2. Accès DCOM caprice de certificats	<ul> <li>✓ Wednesday:</li> <li>✓ Thursday:</li> </ul>	09:00	to 17:30 👻
Ŵ	Alerts	<ul> <li>22. Administrateurs</li> <li>23. Administrateurs clés</li> <li>24. Administrateurs clés Enterprise</li> </ul>	<ul> <li>Friday:</li> <li>Saturday:</li> </ul>	09:00	to 17:30 +
	Reports	Administrateurs de l'entreprise     Administrateurs du schéma     Administrateurs Hyper-V     Administrateurs Hyper-V     Administrateurs Hyper-V	Sunday:	09:00 🔷	to 17:30
\$	Settings	2. Contrôleurs de domaine     2. Contrôleurs de domaine clonables     2. Contrôleurs de domaine d'entreprise en lectur     2. Contrôleurs de domaine en lecture seule	Whitelisted users will always be able to connect.		~
ଙ୍କ	License	- 2. DnsAdmins - 2. DnsUpdateProxy - 2. Duplicateurs - 2. Éditeurs de certificats <	This feature prevents a user from opening a new sess working hours are over.	sion outside of his authorized time rang	ges, and log him off automatically when his
		<ul> <li>Local Users and Groups</li> <li>AD Users and Groups</li> </ul>			
		(?) User Guide	Version 7.1.9.11	Permanent License Activ	vated - Ultimate Protection edition.

Le **Liste blanche des utilisateurs** le tab donne à l'administrateur la possibilité de ajouter/ retirer des utilisateurs de la liste blanche .

Les utilisateurs sur la liste blanche sont ignorés par TSplus Advanced Security et leurs paramètres ne seront pas appliqués.

L'utilisateur qui a installé TSplus Advanced Security est automatiquement ajouté à la liste blanche :

O Not configured for this user/group					
Always authorize					
O Always block					
○ Authorize only during these time ranges:					
Monday:	09:00	*	to	17:30	
✓ Tuesday:	09:00	*	to	17:30	
✓ Wednesday:	09:00	*	to	17:30	
✓ Thursday:	09:00	*	to	17:30	
Friday:	09:00	*	to	17:30	* *
Saturday:	09:00	*	to	17:30	* *
Sunday:	09:00	*	to	17:30	* *
Select timezone for user or group ((UTC+01:00) Bruxell	es, Copenhague	e, Madrid, F	Paris is app	lied by default):	
					~
Whitelisted users will always be able to connect.	trida of his outbo	riand times of	man and l	as him off sutam	atically when his
working hours are over.	side of his dutho	rizeu time ri	inges, ana i	og nim off aatom	acculy when his

## Appareils de confiance

Trusted Devices vous permet de contrôler les appareils des utilisateurs en autorisant chaque utilisateur à n'utiliser qu'un ou plusieurs appareils spécifiques, qui seront vérifiés lors de toute session entrante. Une connexion à partir de tout nom d'appareil invalide sera bloquée.



👈 TSp	lus Advanced Security		-		×
ADV	ANCEDSECURITY	Sessions > Trusted Devices			
□	Dashboard Firewall Sessions Ransomware	Users - Local computer Default View Switch View - 2. Users - 2. doministrateur - 2. user3 - 2. user3 - 2. user3 - 2. user4	This user can connect from any Device     This user Device name will be checked and must be in this list:     Device Name     TSPLUS-SERVER1		
ŵ	Settings				
ଟ୍ୟ	Liconso		Add     Remove       Whitelisted users will always be able to connect.     Trusted Devices enables to control the Device names of any incoming session.       A logon from any invalid Device name will be blocked.		
		⑦ User Guide	Version 7.1.8.20 Permanent License Activated - Ultimate Protection	on editio	i.

Dans cet exemple, User1 utilisera le nom de l'appareil TSPLUS-SERVER1 seulement.

## Remplissage automatique du champ de nom de l'appareil

Vous pourriez remarquer que le champ Nom de l'appareil est déjà rempli avec un nom d'appareil pour certains utilisateurs. Afin d'aider l'administrateur, TSplus Advanced Security enregistrera automatiquement le nom du dernier appareil utilisé pour se connecter au serveur par tout utilisateur qui n'a pas la fonctionnalité Appareils de confiance activée. Après une journée de travail, le nom de l'appareil de la plupart des utilisateurs sera connu par advanced-security, permettant ainsi d'activer rapidement la fonctionnalité Protection des points de terminaison sans avoir à vérifier le nom de la station de travail de chaque utilisateur.

Remarque Les appareils de confiance ne sont pas compatibles avec les connexions HTML5.

## Mise à jour de TSplus Advanced Security

Découvrez nos corrections et améliorations en cliquant sur <u>Journal des modifications</u>

Mettre à jour TSplus Advanced Security est facile et peut être fait en cliquant sur la tuile correspondante, depuis la page d'accueil :

TSplus Advanced Security - 5.4.		
	ADVANCEDSECURITY - Ultimate Protection	
<b>М</b> 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 enabled for this user	s feature is not
	10 Dec 12:13:17     A logon request has been granted for user DESKTOP-QVTJFVE\utilisateur because	utilisateur is
IP ADDRESSES	10 Dec 11:09:08     A connection has been authorized for user DESKTOP-QVTJFVE\utilisateur from computer because this enabled for this user	s feature is not
	10 Dec 11:09:08     A logon request has been granted for user DESKTOP-QVTJFVE\utilisateur because DESKTOP-QVTJFVE\utilisateur from computer because this     A connection has been authorized for user DESKTOP-QVTJFVE\utilisateur from computer because this	s feature is not
	enabled for this user	
大 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	elog
SETTINGS	V Iriai License 14 days	
CT LICENSE	English •	Help

Ensuite, TSplus Advanced Security télécharge et applique la mise à jour.

**Remarque :** vos données et paramètres sont toujours sauvegardés avant une mise à jour et peuvent être trouvés dans le répertoire « archives », dans le dossier de configuration de TSplus Advanced Security. Voir <u>Sauvegardez et restaurez vos données et paramètres</u>

## Restreindre les heures de travail

Vous pouvez configurer des restrictions d'heures de travail par utilisateur ou par groupe.

Choisissez la restriction de votre choix :

- Toujours autoriser l'accès à cet utilisateur/groupe.
- Toujours bloquer l'accès de cet utilisateur/groupe

ou Autoriser uniquement pendant des plages horaires spécifiques.

Vous pouvez le configurer jour par jour et sélectionner la plage horaire de votre choix :



🙂 TSp	lus Advanced Security	-						- 1	×
ADV	ANCEDSECURITY	Sessions > Restrict Working	Hours						
⊞	Dashboard	Users and Groups - AD Domain Default View Switch View	Not configured for this user/group     Always authorize     Always block						
ଚ	Firewall	- S Users	Authorize only during these time ranges: Monday:	09:00		to	17:30		
0	Sessions	···· ≳ user1 ···· ≳ user2 ···· ≳ user3	Tuesday:	09:00	÷	to	17:30		
₿	Ransomware	S user4     Groups     Accès compatible pré-Windows 2000	✓ Wednesday: ✓ Thursday:	09:00	÷	to to	17:30 17:30	÷	
ŵ	Alerts	Acces DCOM service de certificats      Administrateurs      Administrateurs clés      Administrateurs clés Enterprise	✓ Friday: ☐ Saturday:	<b>09:00</b>	\$	to to	17:30 17:30	÷	
	Reports	- X Administrateurs de l'entreprise X Administrateurs du schéma - X Administrateurs Hyper-V - X Admins du domaine	Sunday: Select timezone for user or group ((UTC+01:00	09:00 )) Bruxelles, Copenhag	e, Madrid, P	to aris is app	17:30 blied by defaul	¢.	
٤	Settings	—	Whitelisted users will always be able to connect.						~
ଟ୍ୟ	License		This feature prevents a user from opening a new so working hours are over.	ession outside of his auth	orized time ra	inges, and	log him off auto	matically wh	en his
		<ul> <li>Local Users and Groups</li> <li>AD Users and Groups</li> </ul>							
		() User Guide	Version 7.1.9.11	Permanent L	icense Act	tivated ·	Ultimate Pr	otection ed	ition.

Il est possible de sélectionner un fuseau horaire spécifique en fonction de l'emplacement du bureau de votre utilisateur.

Une déconnexion automatique à la fin du temps de travail configuré est effectuée.

Il est possible de programmer un message d'avertissement avant que l'utilisateur ne soit déconnecté de <u>Paramètres > Avancé > Heures de travail</u>.

###Priorités des règles des utilisateurs/groupes

Lorsque un utilisateur ouvre une nouvelle session sur le serveur :

1.

si cet utilisateur a des restrictions d'heures de travail directement définies pour lui-même, alors ces règles sont appliquées.

#### 2.

si cet utilisateur n'a pas de restrictions d'heures de travail directement définies pour lui-même, alors TSplus Advanced Security chargera toutes les restrictions d'heures de travail existantes pour tous les groupes de cet utilisateur et conservera les règles les plus permissives. Par exemple, si un premier groupe a une règle pour bloquer la connexion le lundi, un deuxième groupe a une règle pour autoriser la connexion le lundi de 9h à 17h et un troisième groupe a une règle pour autoriser la connexion le lundi de 8h à 15h, alors l'utilisateur pourra ouvrir une connexion le lundi de 8h à 17h.

Avertissement : Cette fonctionnalité utilise l'heure du serveur. Utiliser l'heure de la station de travail de l'utilisateur et/ou le fuseau horaire serait inutile, car l'utilisateur n'aurait qu'à changer son fuseau horaire pour ouvrir une session en dehors de ses heures

autorisées.