



Version 7

Nouvelles fonctionnalités : Alertes de sécurité et rapports de protection

**Accédez à vos serveurs Bureau à
Distance et à vos Applicatifs
EN TOUTE SÉCURITÉ**

Maintenez votre serveur protégé

Que vous souhaitiez vous connecter à votre serveur Bureau Distant, votre serveur Applicatif ou encore votre ordinateur personnel depuis un site distant, TS2log Security est votre bouclier pour protéger ces machines contre les attaques extérieures et intérieures à votre réseau.

Notre produit est conçu pour sécuriser les accès à distance incluant toute tentative d'accès (rdp, web, ports applicatifs comme SQL, HF-SQL, SSH, FTP, SFTP, ...), surveiller les tentatives échouées de Login/Mot de passe (Attaque par Force Brute), bloquer les connexions interdites ou suspectes et prévenir les actions non autorisées comme dans le cas des ransomware et des cryptolockers.

Par ailleurs les identifiants et les mots de passe peuvent être dérobés d'autant plus facilement quand il s'agit de connexions nomades, ouvrant ainsi la voie royale au vol de données.

Le Tableau de Bord apporte un accès rapide aux fonctionnalités de sécurité et aux derniers événements

TS2log Security

ADVANCED SECURITY

Surveillez toutes les connexions entrantes

Tableau de bord

Pare-Feu

Sessions

Rançongiciels

Alertes

Rapports

Paramètres

Licence

Pare-Feu

- Protection Géographique**
1 049 tentatives de connexion à distance refusées
- Protection Anti-Attaques Automatiques**
0 adresse IP bloquée
- Protection contre les IP pirates**
564 436 405 adresses IP malveillantes bloquées

Configurer le Pare-Feu

Sessions

- Restriction des Heures de Travail**
Non configuré
- Sessions Sécurisées**
Non configuré
- Appareils de Confiance**
Non configuré

Configurer les Sessions

Protection Anti-Rançongiciels

Protection Anti-Rançongiciels
La protection contre les rançongiciels est activée.
La période d'apprentissage est en cours.

Gérer la Protection contre les Rançongiciels

Connexion distante refusée depuis 194.169.175.52 (Bulgaria)

Demande de connexion 194.169.175.52 refusée

Connexion distante refusée depuis 88.214.25.72 (Germany)

Connexion distante refusée depuis 88.214.25.72 (Germany)

Connexion distante refusée depuis 88.214.25.72 (Germany)

Demande de connexion 88.214.25.72 refusée

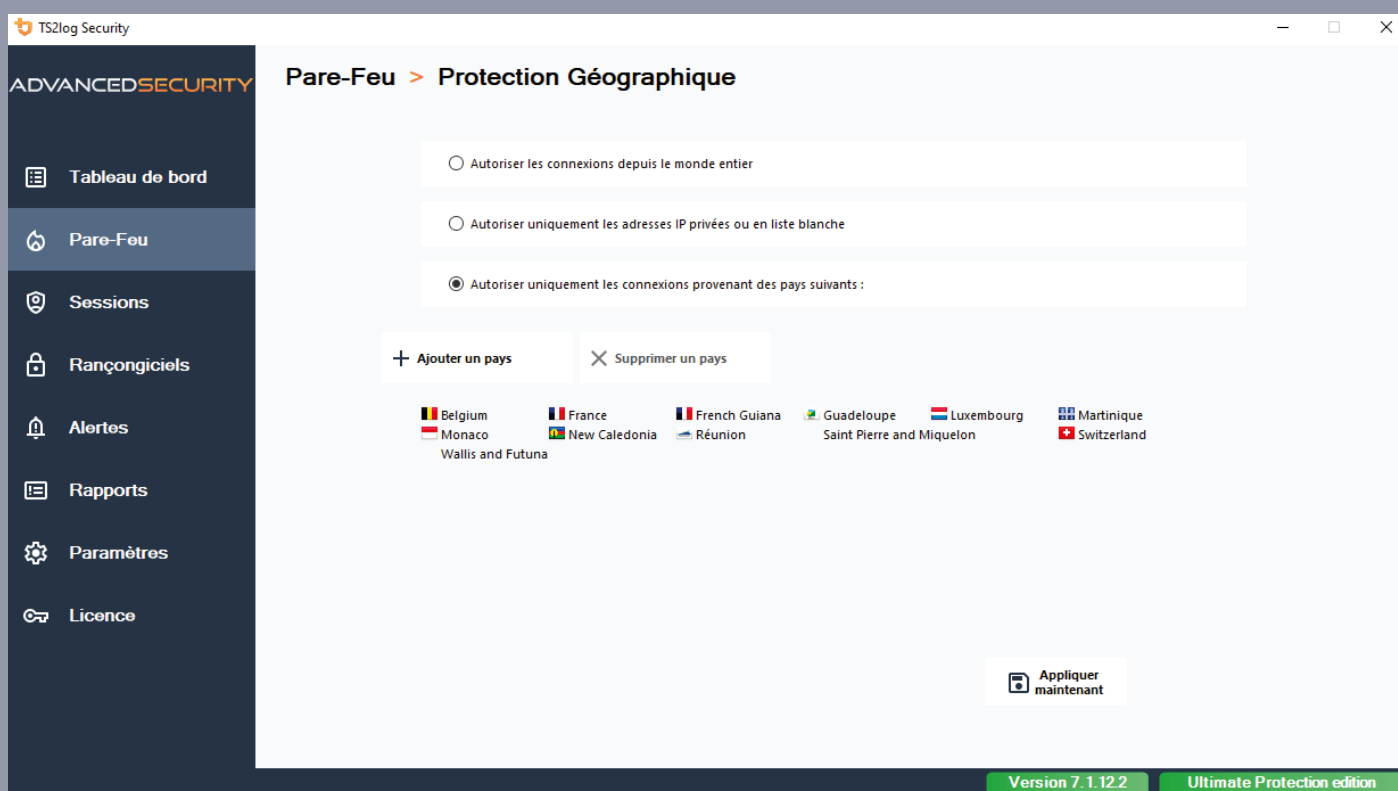
Voir tous les événements

Version 7.1.12.2

Ultimate Protection edition

Protection Géographique :

Vos utilisateurs sont situés, par exemple, en France, Canada, États-Unis, Angleterre. Pourquoi quelqu'un pourrait-il pouvoir ouvrir une session depuis la Chine, l'Inde ou l'Allemagne ? En un clin d'oeil avec TS2log-Security, vous protégez vos serveurs Bureau Distant des attaquants essayant d'ouvrir une session à partir de pays étrangers.

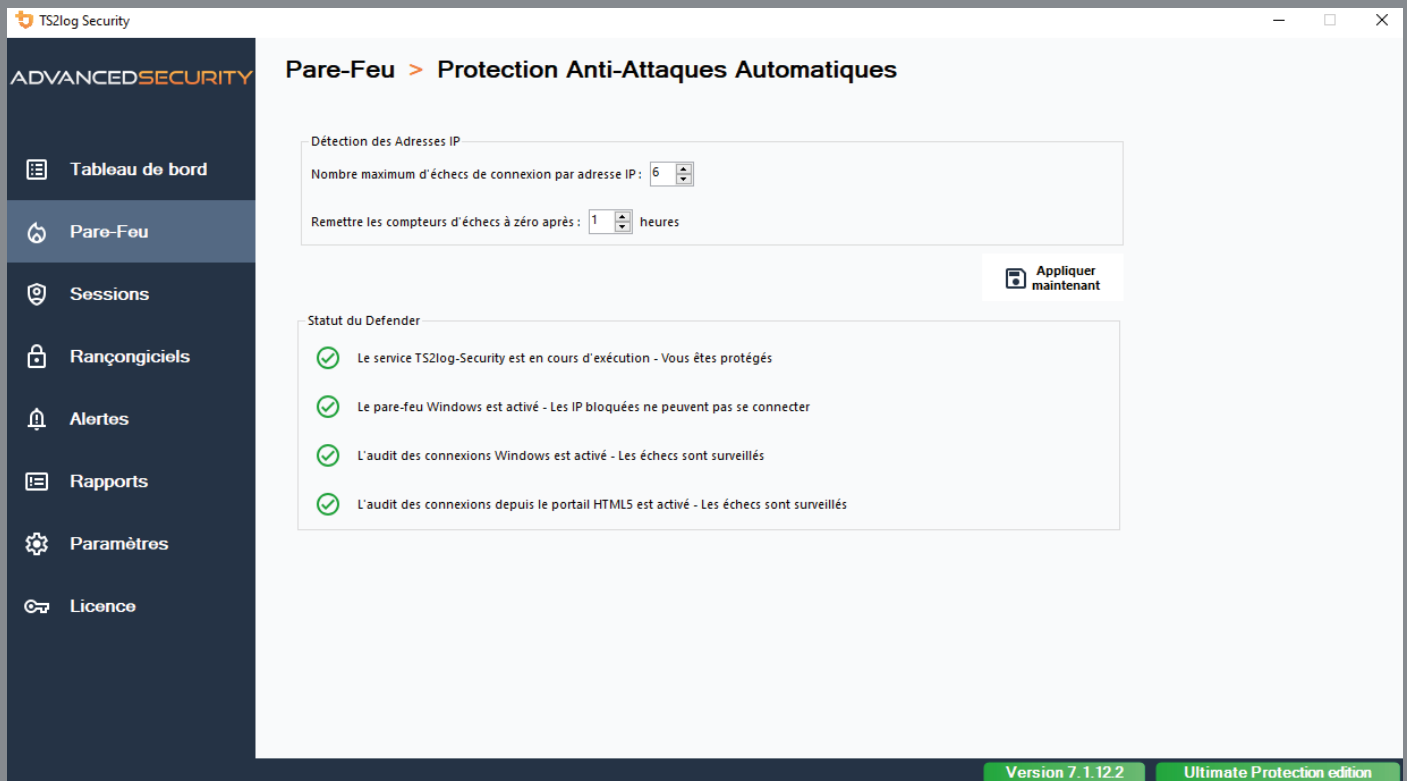


Cette fonctionnalité déclenche une analyse des flux entrants TCP/IP et bloque les flux en provenance des pays non-autorisés. Par exemple vous pouvez protéger les accès à votre serveur FTP ou à vos bases de données.

C'est extrêmement simple et puissant. Faites-le !

Protection Anti Brute Force

Si votre serveur Windows est publiquement accessible sur Internet, il existe une probabilité de 100% que les pirates informatiques, les scanners de réseau et les robots de Brute-Force tentent de deviner votre identifiant et votre mot de passe administrateur... pendant que vous lisez ces lignes.



À l'aide de mots-clés et autres dictionnaires de mots de passe, ils tentent de se connecter à votre serveur à haute fréquence (des milliers de fois par minute).

Non seulement cela est mauvais pour la sécurité de votre serveur, mais cela peut également consommer beaucoup de ses ressources (CPU et bande passante) !

TS2log Security protégera instantanément votre serveur en surveillant les tentatives de connexion échouées à Windows et établira automatiquement après plusieurs tentatives de connexion échouées la liste noire des adresses IP incriminées.

De plus, vous pouvez spécifier manuellement les adresses IP à autoriser/bloquer selon vos besoins.

Gestion globale des adresses IP

Gérez facilement les adresses IP à partir d'un seul endroit avec une seule liste pour les adresses IP bloquées et celles qui sont autorisées.

TS2log Security

ADVANCEDSECURITY

Pare-Feu

Rechercher Filtrer : Bloquée - Protection Anti-Attaques Automatiques, Bloquée - Protection Géographique, E

Adresse IP	Pays	Statut	Date	Description
194.169.175.52	Bulgaria	Bloquée - Protection Géographique	27 déc. 2024 21:08:04	
88.214.25.72	Germany	Bloquée - Protection Géographique	27 déc. 2024 21:07:00	
66.63.187.168	United States	Bloquée - Protection Géographique	27 déc. 2024 21:05:45	
194.169.175.58	Bulgaria	Bloquée - Protection Géographique	27 déc. 2024 21:00:07	
147.185.132.195	United States	Bloquée - Protection Géographique	27 déc. 2024 20:55:30	
31.13.224.36	Bulgaria	Bloquée - Protection Géographique	27 déc. 2024 20:49:46	
64.62.197.166	United States	Bloquée - Protection Géographique	27 déc. 2024 20:43:27	
64.62.197.161	United States	Bloquée - Protection Géographique	27 déc. 2024 20:41:55	
64.62.197.164	United States	Bloquée - Protection Géographique	27 déc. 2024 20:38:32	
64.62.197.162	United States	Bloquée - Protection Géographique	27 déc. 2024 20:38:31	

1 / 6

Protection Géographique

Activé

Accès permis seulement depuis la liste de pays que vous avez configurée dont :

Protection Anti-Attaques Automatiques

Activé

Vous êtes protégé contre les pirates informatiques, les scanners de réseau et les robots qui tentent de deviner vos identifiants et vos mots de passe.

Protection contre les IP pirates

Activé

Vous êtes protégé contre 564 436 405 adresses IP malveillantes figurant sur la liste noire des menaces connues établie par notre communauté mondiale

Dernière synchronisation : 27/12/2024

Version 7.1.12.2 Ultimate Protection edition

Cela signifie que toutes les IP détectées par les protections de Géo-restriktion et Brute Force sont centralisées pour être vérifiées, modifiées, ajoutées ou supprimées à votre convenance. Les listes d'adresses IP sont consultables, ce qui en facilite la gestion.

Depuis la version 6.30 vous bénéficiez d'une base de données d'adresses IP malveillantes qui est mise à jour quotidiennement.

Les règles de votre pare-feu sont mises à jour automatiquement

TS2log Security

ADVANCEDSECURITY

Pare-Feu

Rechercher Filtrer : Bloquée - Protection Anti-Attaques Automatiques, Bloquée - Protection Géographique, E

Adresse IP	Pays	Statut	Date	Description
194.169.175.52	Bulgaria	Bloquée - Protection Géographique	27 déc. 2024 21:08:04	
88.214.25.72	Germany	Bloquée - Protection Géographique	27 déc. 2024 21:07:00	
66.63.187.168	United States	Bloquée - Protection Géographique	27 déc. 2024 21:05:45	
194.169.175.58	Bulgaria	Bloquée - Protection Géographique	27 déc. 2024 21:00:07	
147.185.132.195	United States	Bloquée - Protection Géographique	27 déc. 2024 20:55:30	
31.13.224.36	Bulgaria	Bloquée - Protection Géographique	27 déc. 2024 20:49:46	
64.62.197.166	United States	Bloquée - Protection Géographique	27 déc. 2024 20:43:27	
64.62.197.161	United States	Bloquée - Protection Géographique	27 déc. 2024 20:41:55	
64.62.197.164	United States	Bloquée - Protection Géographique	27 déc. 2024 20:38:32	
64.62.197.162	United States	Bloquée - Protection Géographique	27 déc. 2024 20:38:31	

1 / 6

Protection Géographique

Activé

Accès permis seulement depuis la liste de pays que vous avez configurée dont :

Protection Anti-Attaques Automatiques

Activé

Vous êtes protégé contre les pirates informatiques, les scanners de réseau et les robots qui tentent de deviner vos identifiants et vos mots de passe.

Protection contre les IP pirates

Activé

Vous êtes protégé contre 564 436 405 adresses IP malveillantes figurant sur la liste noire des menaces connues établie par notre communauté mondiale

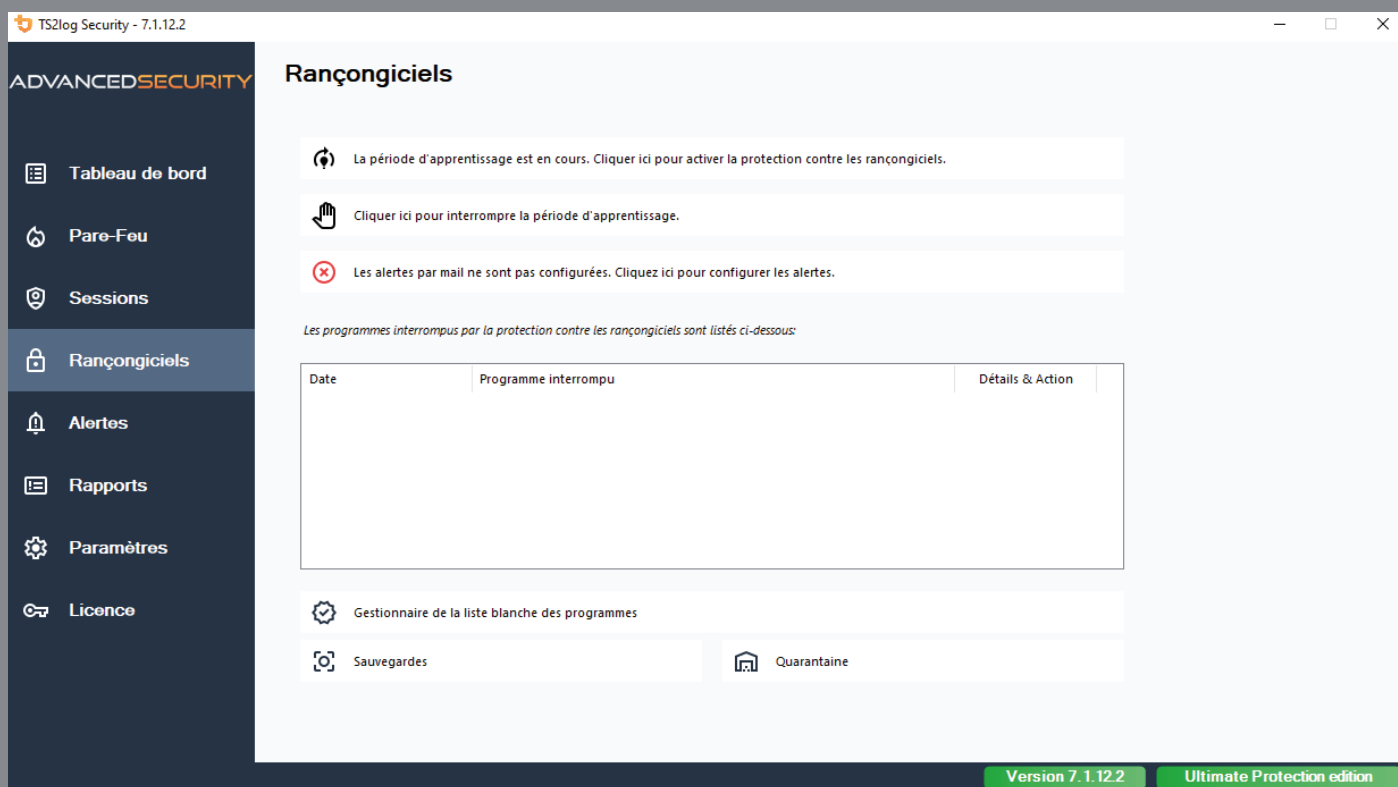
Dernière synchronisation : 27/12/2024

Version 7.1.12.2 Ultimate Protection edition

Protection Anti Rançongiciels

Stoppez les attaques de ransomware !

Les ransomwares sont la plus importante des cybermenaces actuelles.



Il est facile de les télécharger par erreur depuis un site Web compromis, de les ouvrir via des pages de publicité malveillantes ou de les recevoir en pièce jointe à partir d'emails spammés.

Leurs actions sur vos systèmes vont soit verrouiller complètement votre accès, soit crypter la majorité de vos fichiers jusqu'à ce que vous payiez la demande de rançon des cybercriminels.

Toutefois, cela ne garantit pas la restitution de vos données et peut paralyser vos activités commerciales ou même entraîner la perte définitive de vos données.

La protection anti-ransomware de TS2log Security détectera, bloquera et empêchera efficacement les attaques de ransomware.

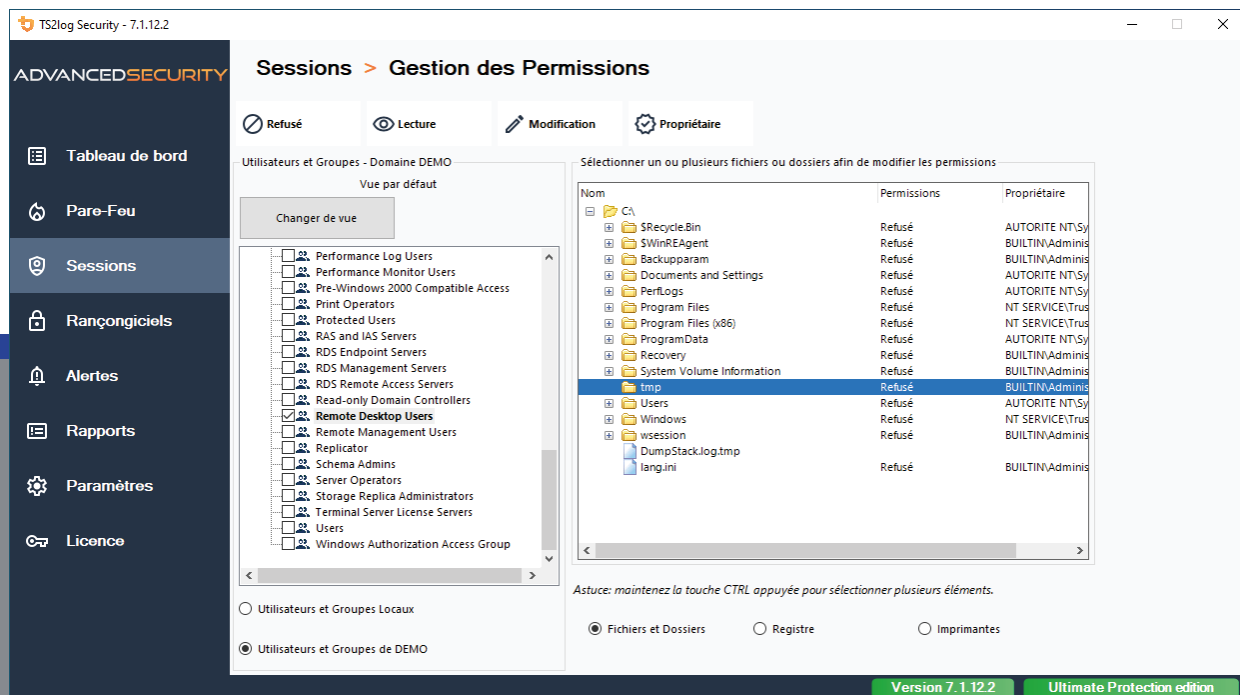
Vous éviterez des conséquences catastrophiques pour votre entreprise en supprimant rapidement le logiciel de ransomware.

Gestion et inspection des permissions sur les fichiers et dossiers, le Registre et les Imprimantes

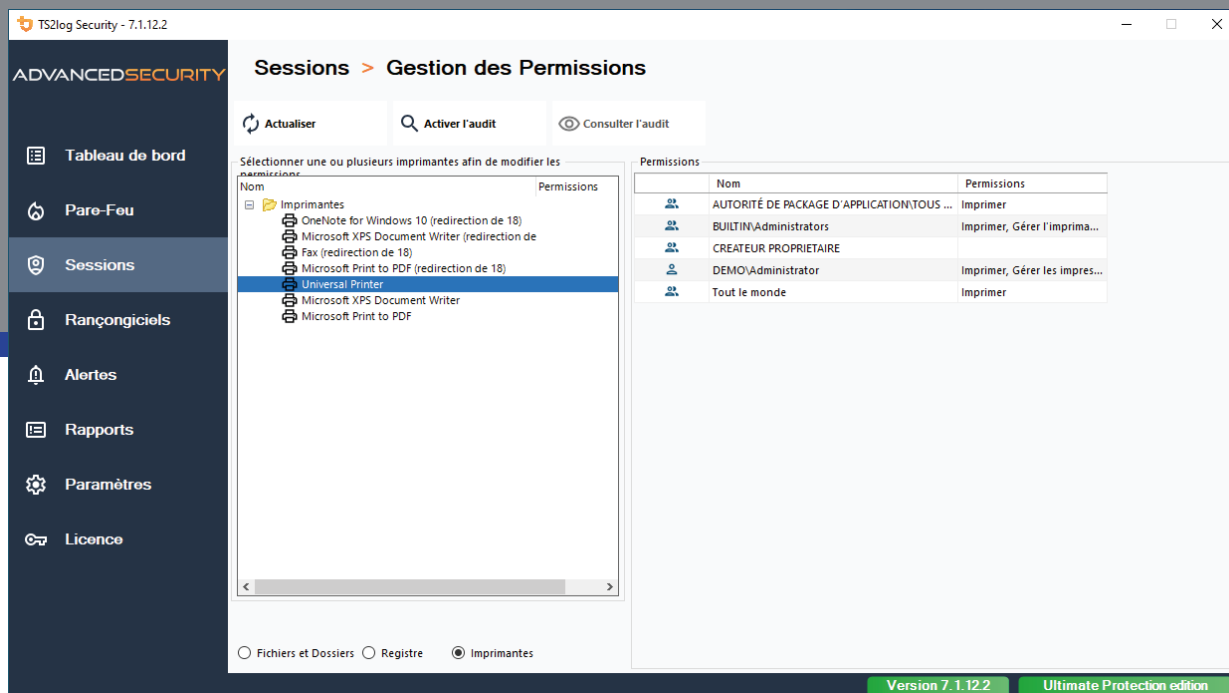
Le tableau de bord «Permissions» permet de visualiser et d'interagir de manière simplifiée sur les droits octroyés aux dossiers, fichiers, Registre Windows et sur les imprimantes déployées sur le serveur.

Tout est visible à un seul endroit, ce qui simplifie l'inspection des privilèges (Security Essentials) et leurs modifications (Ultimate Protection) pour chaque utilisateur ou groupe de sécurité.

L'onglet gestion permet la modification des permissions.



L'onglet Inspection autorise seulement la vérification des permissions



Restriction d'accès par plage horaire

Bien sûr, vos utilisateurs devraient être libres de se connecter et de travailler quand ils se trouvent au bureau.

Avec L'Édition Essentials, vous pouvez spécifier une plage horaire unique* pour les utilisateurs qui ne pourront ouvrir des sessions qu'à l'intérieur de cette plage horaire. Cela contribuera ainsi à renforcer votre politique de sécurité.

Restrictions de jour et d'heure.

N'autorisez les utilisateurs ou groupes à se connecter que pendant certains jours et plages horaires. Il est possible de sélectionner un fuseau horaire spécifique en fonction de l'emplacement géographique du bureau de votre utilisateur.

* Pour gérer de multiples plages horaires pour des utilisateurs ou des groupes, choisissez TS2log-Security Ultimate

TS2log Security - 7.1.12.2

ADVANCED SECURITY

Sessions > Restriction des Heures de Travail

Utilisateurs et Groupes - Ordinateur local

Vue par défaut

Changer de vue

- Access Control Assistance Operators
- Administrators
- Backup Operators
- Certificate Service DCOM Access
- Cryptographic Operators
- Device Owners
- Distributed COM Users
- Event Log Readers
- Guests
- Hyper-V Administrators
- IIS_IUSRS
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Power Users
- Print Operators
- RDS Endpoint Servers
- RDS Management Servers
- RDS Remote Access Servers
- Remote Desktop Users
- Remote Management Users
- Replicator
- Storage Replica Administrators
- System Managed Accounts Group
- Users

Non configuré pour cet utilisateur/groupe

Toujours autoriser

Toujours bloquer

Autoriser uniquement pendant ces plages horaires :

<input checked="" type="checkbox"/> Lundi:	09:00	à	17:30
<input checked="" type="checkbox"/> Mardi:	09:00	à	17:30
<input checked="" type="checkbox"/> Mercredi:	09:00	à	17:30
<input checked="" type="checkbox"/> Jeudi:	09:00	à	17:30
<input checked="" type="checkbox"/> Vendredi:	09:00	à	17:30
<input checked="" type="checkbox"/> Samedi:	09:00	à	13:30
<input type="checkbox"/> Dimanche:	09:00	à	17:30

Sélectionner le fuseau horaire pour cet utilisateur ou ce groupe (par défaut, le fuseau horaire (UTC+01:00) Amsterdam, Berlin, Berne, Rome, Stockholm, Vienne est appliqué) :

(UTC-02:00) Temps universel coordonné-02

Les utilisateurs en liste blanche pourront toujours se connecter.

Cette fonctionnalité empêche un utilisateur d'ouvrir une session en dehors de ses plages horaires autorisées, et le déconnecte automatiquement en cas de dépassement.

Version 7.1.12.2 Ultimate Protection edition

Autorisation des utilisateurs et des groupes

Gérez les autorisations de plage horaire pour des utilisateurs ou des groupes spécifiques. Si un utilisateur appartient à plusieurs groupes, les autorisations les plus permissives s'appliquent.

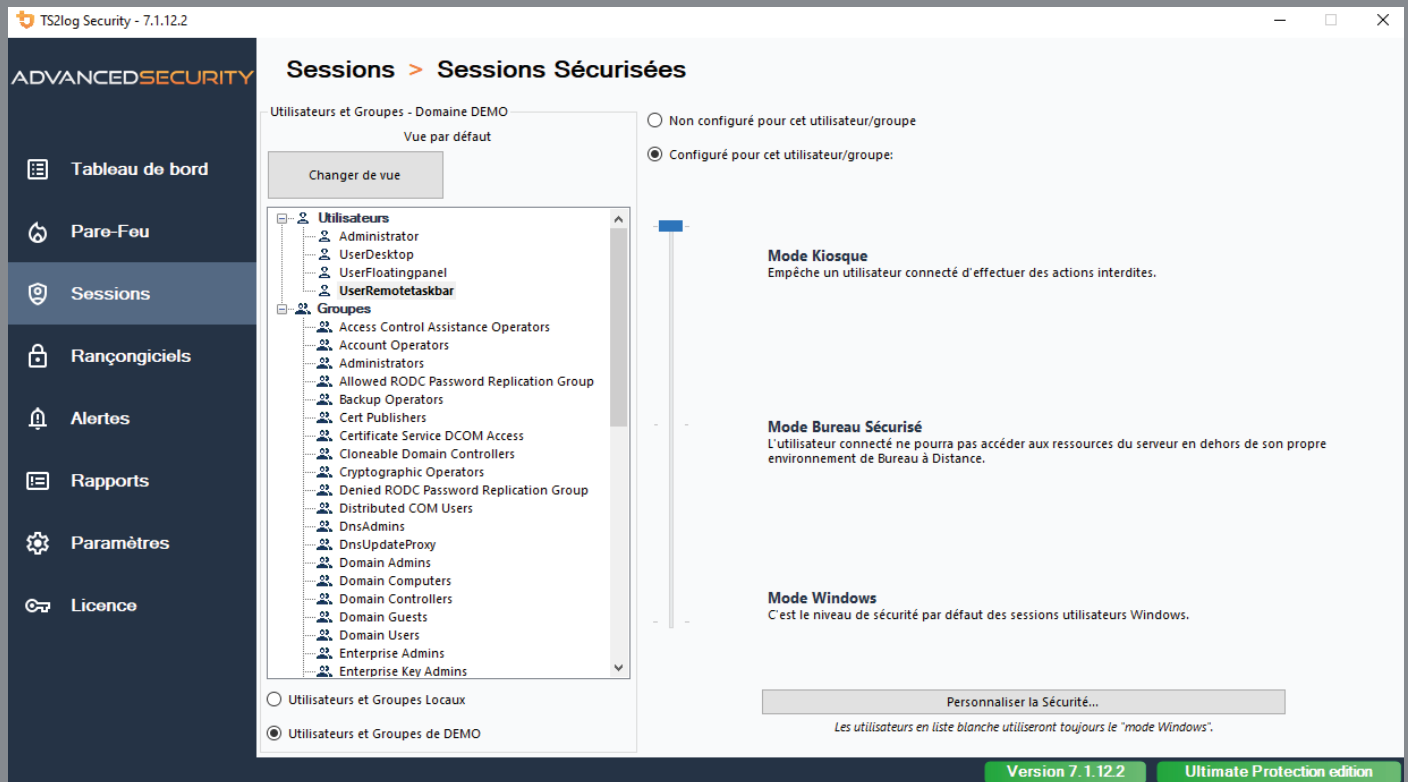
Déconnexion automatisée

Les sessions utilisateurs peuvent être automatiquement déconnectées à la fin du créneau horaire autorisé.

Avertissement de déconnexion

Programmez un message d'avertissement pour informer l'utilisateur avant qu'il ne soit automatiquement déconnecté.

Définissez facilement les règles des droits des utilisateurs grâce à 3 niveaux de sécurité personnalisables :



Windows fournit de nombreuses et puissantes GPO, mais cela vous coûtera plusieurs jours d'effort pour trouver, configurer et affiner les règles de sécurité attendues.

3 Niveaux de sécurisation des sessions Utilisateurs

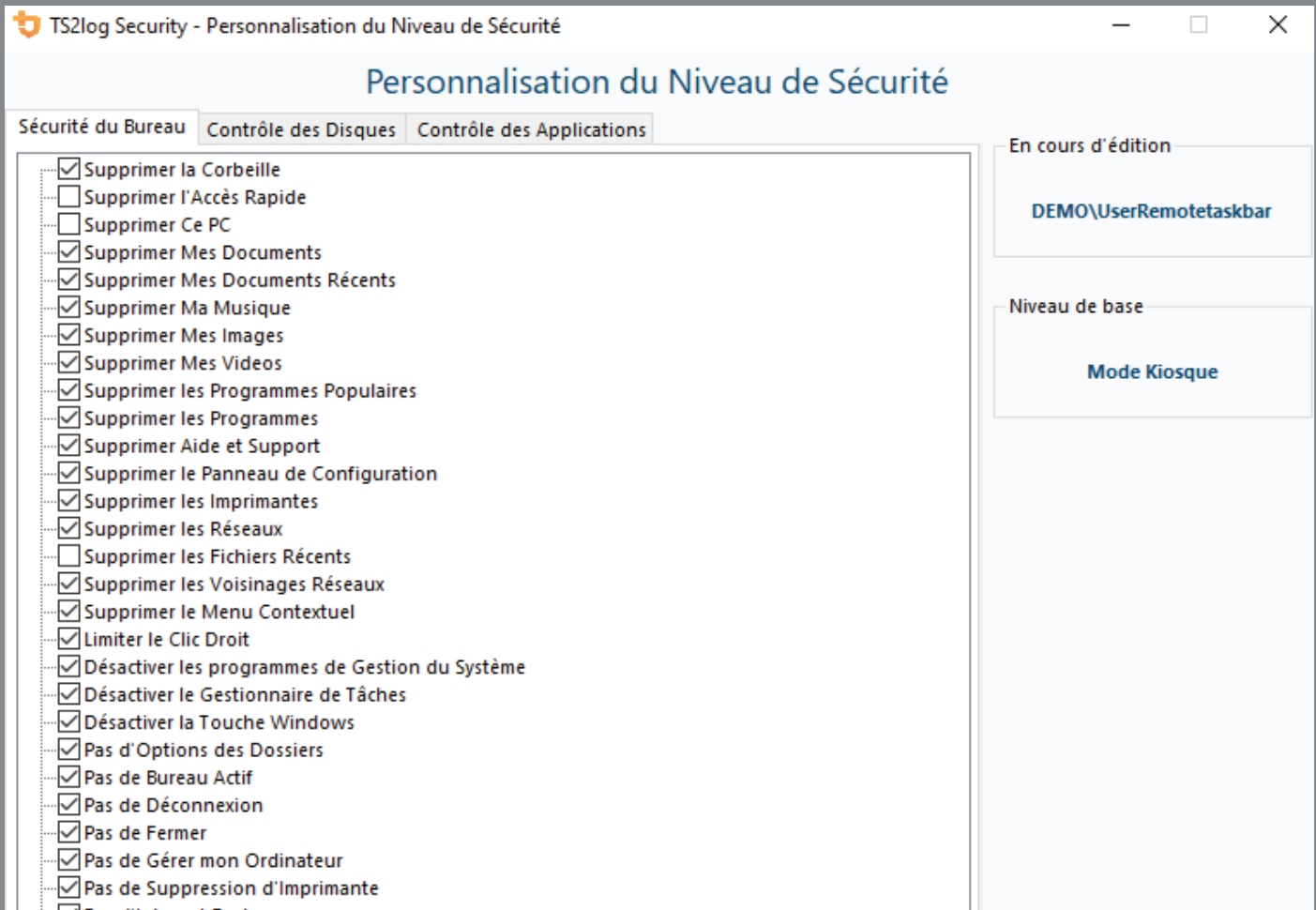
Vous pouvez configurer le niveau de sécurité pour chaque utilisateur ou groupe en sélectionnant l'un des trois niveaux de sécurité standardisés conçus selon les meilleures pratiques de l'industrie informatique :

Mode Windows : accès à la session Windows par défaut

Mode bureau sécurisé : accès aux documents, imprimantes, clé Windows et déconnexion de session

Mode Kiosque : empêche un utilisateur connecté d'exécuter des actions interdites.

Personnaliser le niveau de sécurité



Les administrateurs peuvent facilement personnaliser le niveau de sécurité de chacun des trois modes standard en fonction de leurs propres besoins.

Sélectionnez ou désélectionnez simplement des dossiers, des disques et des applications.

Limitez la possibilité de cliquer avec le bouton droit et d'accéder au menu contextuel pour empêcher les utilisateurs d'effectuer des actions indésirables.

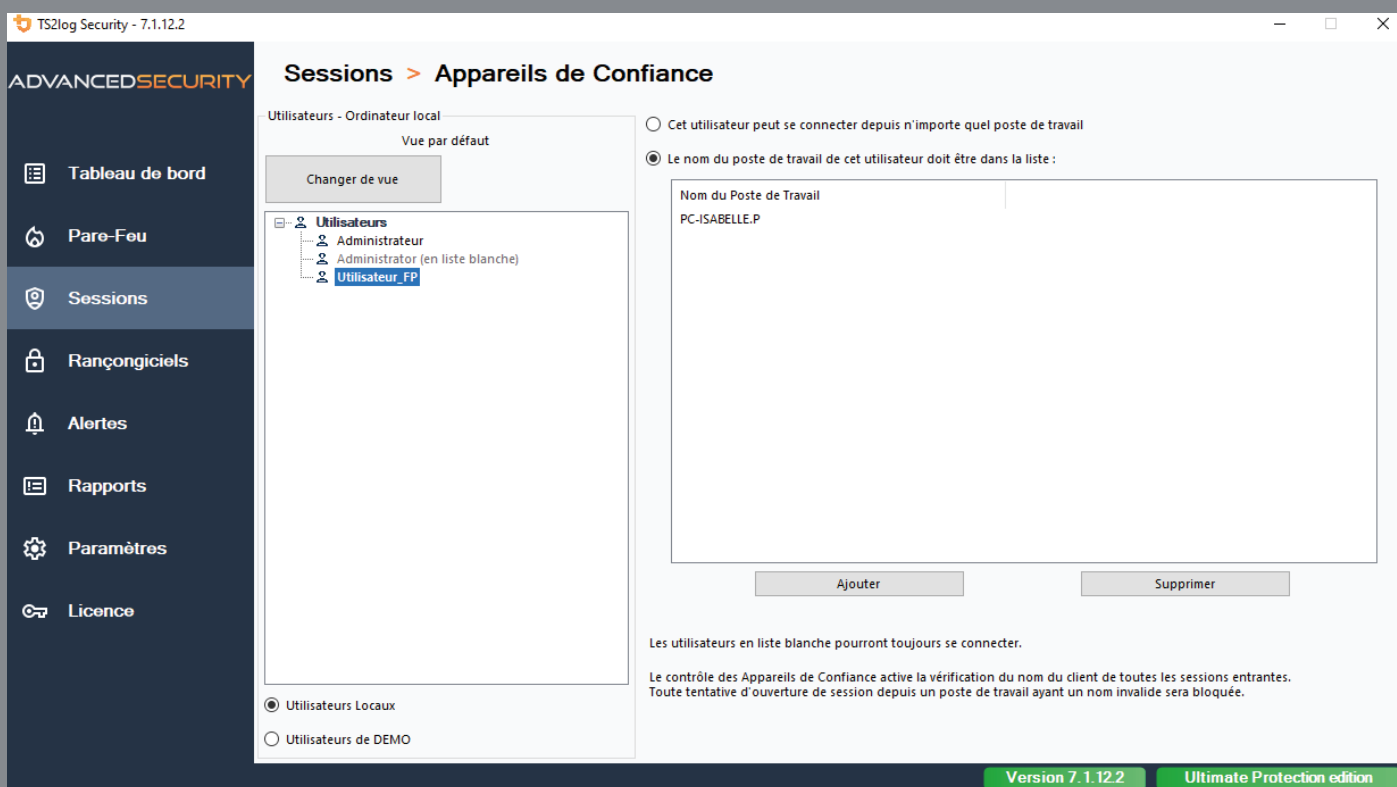
Restriction d'accès par Appareils de confiance

Contrôle de l'appareil

Les administrateurs peuvent décider si un utilisateur peut se connecter à partir de n'importe quel appareil ou uniquement à partir de noms d'appareils spécifiques. TS2log Security crée automatiquement une liste des appareils qui tentent de se connecter, facilitant la tâche de l'administrateur d'accepter ou de refuser l'accès à des appareils spécifiques.

Protection des terminaux

En associant des appareils à des comptes d'utilisateurs, TS2log Security empêche l'utilisation d'informations d'identification compromises pour accéder à votre réseau, car l'attaquant aurait besoin d'un appareil autorisé pour se connecter.



The screenshot displays the 'Sessions > Appareils de Confiance' configuration page in the TS2log Security interface. The left sidebar contains navigation options: Tableau de bord, Pare-Feu, Sessions, Rançongiciels, Alertes, Rapports, Paramètres, and Licence. The main content area is titled 'Utilisateurs - Ordinateur local' and includes a 'Changer de vue' button. Below this, a tree view shows a list of users: Administrateur, Administrator (en liste blanche), and Utilisateur_FP. At the bottom of this list, there are radio buttons for 'Utilisateurs Locaux' (selected) and 'Utilisateurs de DEMO'. To the right, there are two radio button options: 'Cet utilisateur peut se connecter depuis n'importe quel poste de travail' (unselected) and 'Le nom du poste de travail de cet utilisateur doit être dans la liste :'. Below these options is a text input field containing 'PC-ISABELLE.P'. At the bottom of the input field are 'Ajouter' and 'Supprimer' buttons. A note at the bottom states: 'Les utilisateurs en liste blanche pourront toujours se connecter. Le contrôle des Appareils de Confiance active la vérification du nom du client de toutes les sessions entrantes. Toute tentative d'ouverture de session depuis un poste de travail ayant un nom invalide sera bloquée.' The bottom right corner of the interface shows 'Version 7.1.12.2' and 'Ultimate Protection edition'.

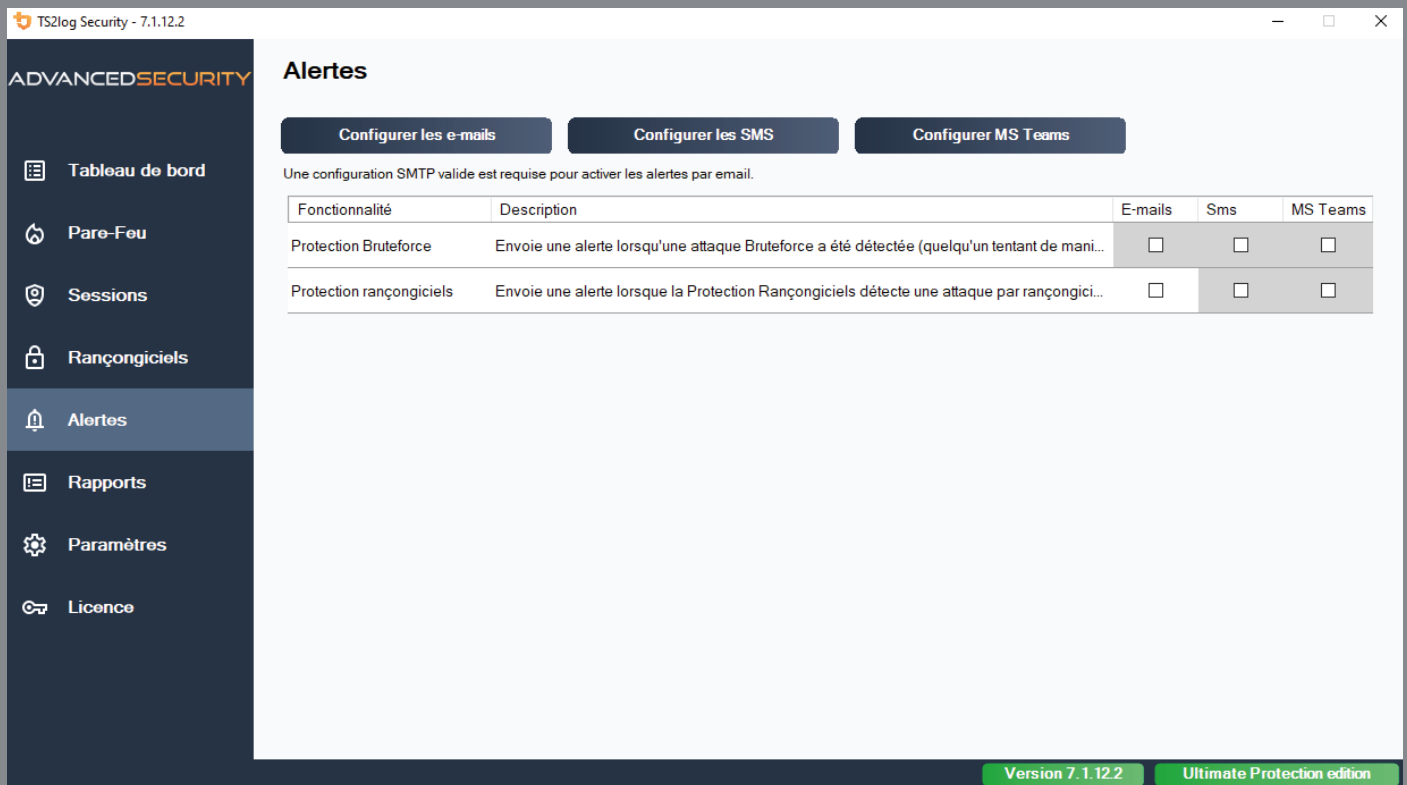
Comment ça marche ?

TS2log Security Ultimate enregistrera le nom de l'ordinateur distant à chaque connexion. L'administrateur peut décider de restreindre l'accès pour cette connexion au nom NetBios du poste de travail (ou plusieurs).

Toute tentative de connexion à partir d'un autre ordinateur sera automatiquement détectée et rejetée. Cette fonctionnalité est opérationnelle uniquement lors d'une connexion RDP via un client de connexion ou en RemoteApp.

Alertes de sécurité

Votre équipe sera informée en temps-réel grâce aux alertes de TS2log Security concernant les tentatives d'intrusion. Les notifications peuvent être envoyées par e-mail, SMS ou via un canal Microsoft Teams.



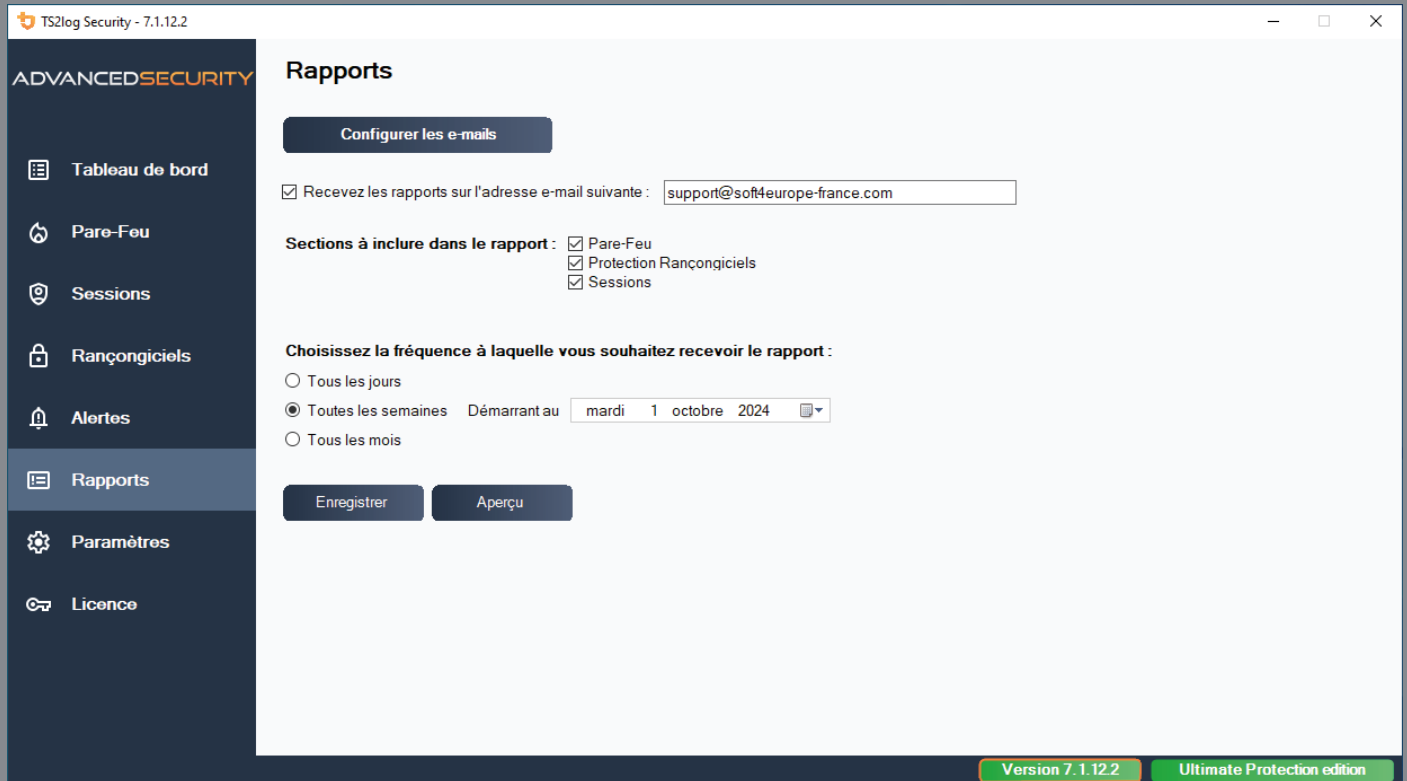
The screenshot displays the 'Alertes' (Alerts) configuration page in the TS2log Security application. The interface includes a dark sidebar with navigation options: Tableau de bord, Pare-Feu, Sessions, Rançongiciels, Alertes (selected), Rapports, Paramètres, and Licence. The main content area features three configuration buttons: 'Configurer les e-mails', 'Configurer les SMS', and 'Configurer MS Teams'. A note states: 'Une configuration SMTP valide est requise pour activer les alertes par email.' Below this is a table with columns for 'Fonctionnalité', 'Description', 'E-mails', 'Sms', and 'MS Teams'. The table lists two security features: 'Protection Bruteforce' and 'Protection rançongiciels', each with checkboxes for the three notification methods.

Fonctionnalité	Description	E-mails	Sms	MS Teams
Protection Bruteforce	Envoie une alerte lorsqu'une attaque Bruteforce a été détectée (quelqu'un tentant de mani...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Protection rançongiciels	Envoie une alerte lorsque la Protection Rançongiciels détecte une attaque par rançongici...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Version 7.1.12.2 Ultimate Protection edition

Rapports de Protection

Recevez des rapports concernant les événements clés de la protection de votre serveur directement par e-mail. Personnalisez la fréquence de réception et sélectionnez les événements que vous souhaitez inclure dans les rapports.



The screenshot displays the 'Rapports' (Reports) configuration page in the TS2log Security application. The interface is in French and includes a sidebar with navigation options: Tableau de bord, Pare-Feu, Sessions, Rançongiciels, Alertes, Rapports (selected), Paramètres, and Licence. The main content area is titled 'Rapports' and features a 'Configurer les e-mails' button. Below this, there is a checkbox for 'Recevez les rapports sur l'adresse e-mail suivante:' with the email address 'support@soft4europe-france.com' entered in the adjacent text field. The 'Sections à inclure dans le rapport:' section has three checked options: Pare-Feu, Protection Rançongiciels, and Sessions. The 'Choisissez la fréquence à laquelle vous souhaitez recevoir le rapport:' section offers three radio button options: 'Tous les jours', 'Toutes les semaines' (selected), and 'Tous les mois'. The 'Toutes les semaines' option is further configured with 'Départant au' set to 'mardi 1 octobre 2024'. At the bottom of the configuration area, there are 'Enregistrer' and 'Aperçu' buttons. The footer of the application window shows 'Version 7.1.12.2' and 'Ultimate Protection edition'.

Événements de sécurité

Depuis le Tableau de Bord, vous aurez accès à l'historique des événements de sécurité de TS2log Security. Un module de filtrage permet une exportation des événements au format csv.

TS2log Security - Événements de Sécurité - Événements depuis le 13 déc. 2024 18:44:50

Date	Fonctionnalité	Message
28 déc. 2024 21:59:18		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:17		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:14		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:12		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:10		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:08		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:06		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:04		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:59:00		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:58:59		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:58:56		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:58:54		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.
28 déc. 2024 21:58:52		Une connexion distante a été refusée depuis l'adresse IP 195.3.221.113 (Poland). Cette adresse IP a été initialement bloquée par Protection Géographique le 27 déc. 2024 20:27:17.

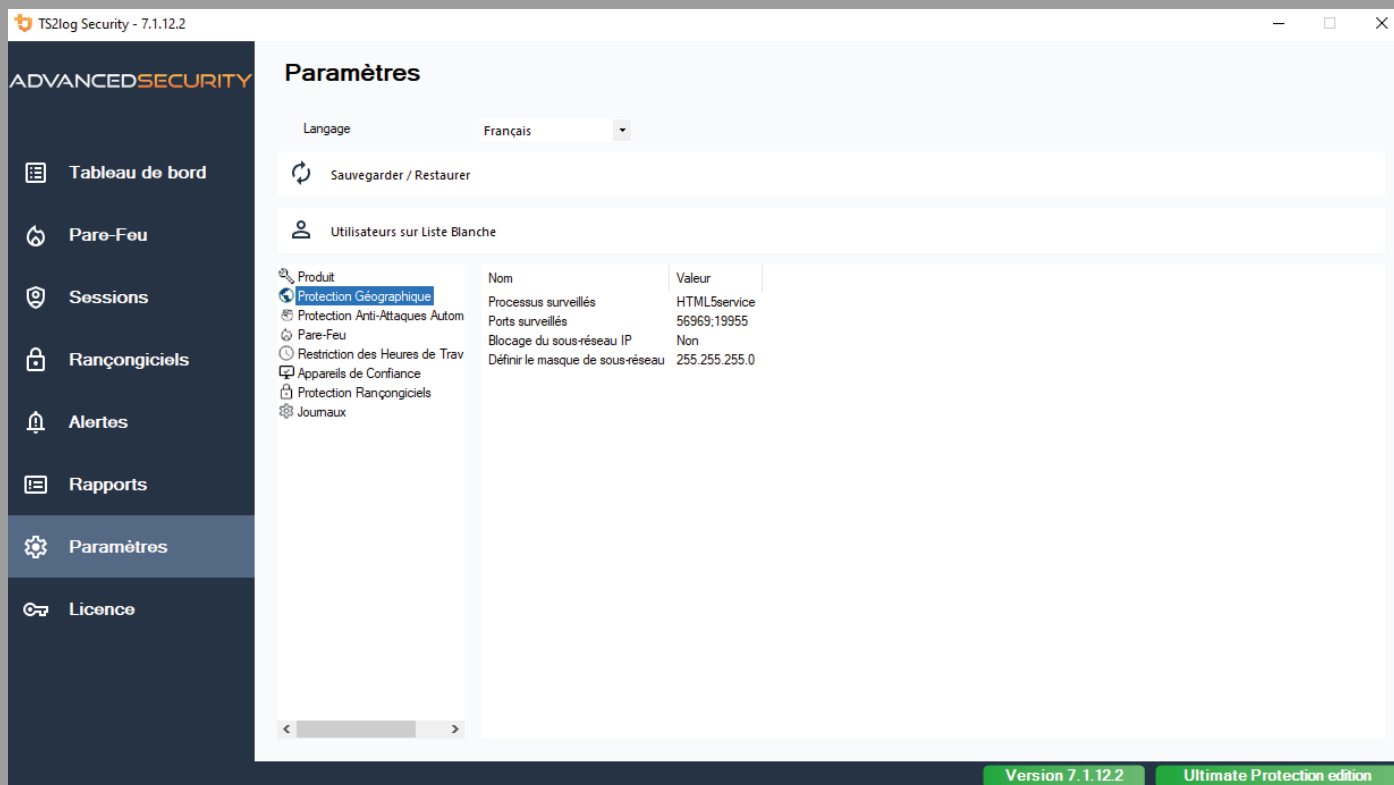
Copier

Rechercher Cacher Moins Importants 01/12/2024 00:00:00 - 28/12/2024 23:59:59 < 28/27352 >

Exporter au format CSV

Paramètres de l'Application

Au sein de cet onglet, vous aurez la possibilité de configurer nombre d'options de TS2log Security.



Avancé :

Une option de sauvegarde/restauration est disponible

D'autres options sont disponibles telles que la mise en place d'un code PIN (Produit) pour l'ouverture sécurisée de la console d'administration de TS2log Security, la modification du message d'alerte (Heures de travail) l'activation des Logs, et bien plus encore.

Utilisateurs :

Grâce à cette fonctionnalité, vous pourrez ajouter ou supprimer des utilisateurs en liste blanche. Par défaut, l'Administrateur du poste y sera inséré.

Programmes :

Idem pour les dossiers et applications, que vous pourrez ajouter ou supprimer de la liste blanche

The screenshot displays the 'Licence' section of the TS2log Security interface. The window title is 'TS2log Security - 7.1.12.2'. The left sidebar contains the following menu items: 'Tableau de bord', 'Pare-Feu', 'Sessions', 'Rançongiciels', 'Alertes', 'Rapports', 'Paramètres', and 'Licence'. The main content area is titled 'Licence' and features three buttons: 'Activer votre licence', 'Rafraichir votre licence', and 'Activer l'enregistrement des logs'. Below these is a button for 'Exporter les logs pour le support'. A 'Statut de la licence' box shows: 'Licence Permanente Activée - Ultimate Protection edition', 'ID de machine: 413973', and 'Nom de l'ordinateur: SRV-DEMO-S4E'. A warning message states: 'Attention : Votre service de Mise à jour et de Support TS2log Security expirera le 2025-01-01.' The bottom right corner shows 'Version 7.1.12.2' and 'Ultimate Protection edition'.

Dans cette rubrique, vous aurez la possibilité d'activer votre licence ou de la rafraichir en cas de modification de cette dernière (éditions et support).

Dans la seconde partie, sera remonté :

- L'édition de la licence.
- L'ID de votre machine.
- Le nom du poste Windows.
- La date de fin de la maintenance (Mise à jour, correctifs et nouvelles fonctionnalités) associée à votre Licence TS2log

Ainsi que le statut de vos protections.

Fonctionnalité	Description	Édition Essentials	Édition Ultimate
Géo-restriction	Choisissez la zone géographique (pays) à partir desquels les connexions seront autorisées	✓	✓
Restriction Horaire	Choisissez les horaires auxquels l'ensemble des utilisateurs auront accès à votre serveur» avec la version Essentials	✓	
Restriction Horaire	Choisissez les horaires auxquels chaque utilisateur / Groupe d'utilisateurs auront accès à votre serveur» pour la version Ultimate		✓
Bloque les attaques de Force Brute	Blacklistage automatique des IP attaquantes	✓	✓
Gestion globale des adresses IP	Gérez les adresses IP bloquées et autorisées avec une seule liste	✓	✓
Protection IP contre les hackers	Depuis la version 6.3.6.8, TS2log intègre une base de données de plusieurs centaines de millions d'adresses IP dangereuses	✓	✓
Alertes de Sécurité	Restez informé avec des alertes concernant les événements de sécurité. Recevez des notifications par e-mail, SMS ou Microsoft Teams.	✓	✓
Rapports de Protection	Recevez des rapports par e-mail concernant les événements clés de protection de votre serveur. Personnalisez la fréquence et sélectionnez les événements que vous souhaitez inclure dans les rapports.	✓	✓
Inspection de permissions	Inspection centralisée des permissions sur les fichiers et dossiers	✓	
Modification des permissions	Modification des permissions : Ouverture - Lecture - Modification		✓
Droit des Utilisateurs	Configurez le niveau de sécurité pour chaque utilisateur ou groupe		✓
Restriction par périphérique d'accès	Associez les identifiants de connexion au nom NetBios de la machine qui se connecte. Uniquement en RDP.		✓
Anti-Ransomware	Détectez, bloquez et prévenez efficacement les attaques de ransomwares		✓