

Bulletin technique TS2log - Version 12.60 du 4 avril 2020

Objet : Nouveaux liens de téléchargement et conseils de sécurité

Bonjour,

Un nouveau lien de téléchargement de la version d'évaluation de TS2log est désormais à votre disposition. Elle remplace l'ancienne de manière définitive.

Elle vous permet de choisir plusieurs options que nous allons vous détailler ci-après.

De plus de nouveaux liens pour la mise à jour et pour le module de connexion sont disponibles.

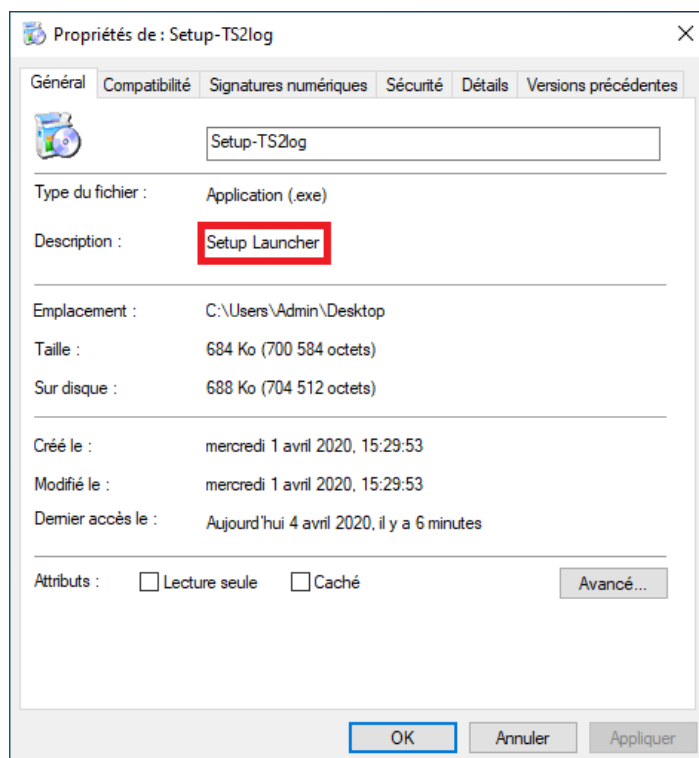
Par ailleurs, devant la recrudescence des cyberattaques autour du thème du Coronavirus ayant pour résultat l'infection de vos PC et serveurs Bureaux Distants par des « ransomware » et autres « cryptolocker », vous trouverez ci-dessous notre guide des bonnes pratiques ainsi que la checklist des points importants à contrôler avant d'autoriser l'accès à vos serveurs Bureaux Distants.

Nous restons bien sûr à votre disposition pour tout conseils et renseignements dont vous pourriez avoir besoin.

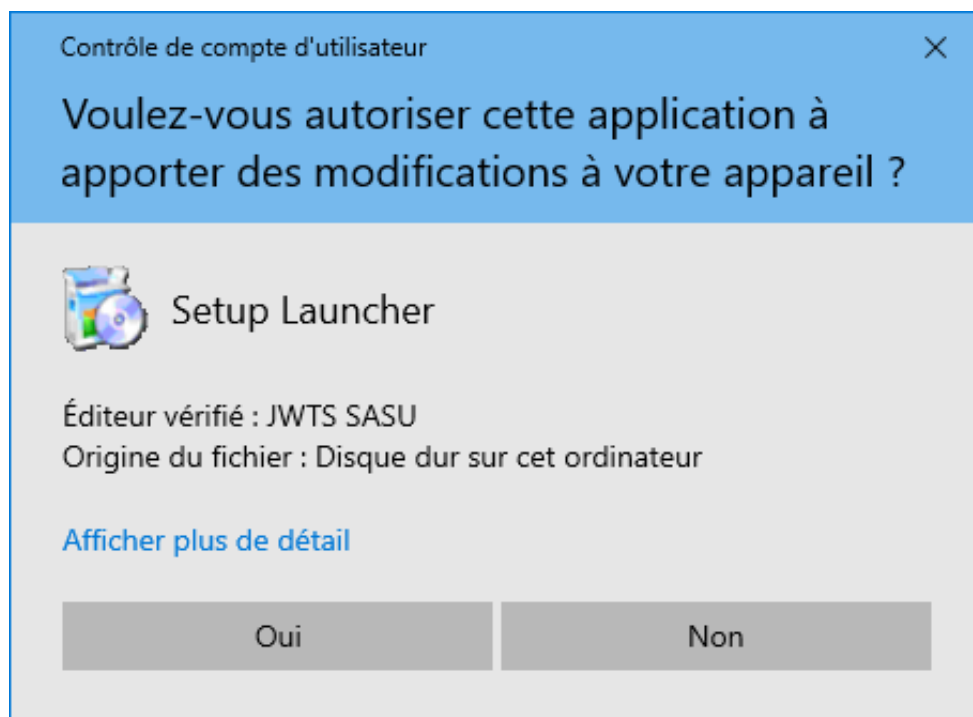
L'équipe Soft4Europe

Quand vous cliquez sur le lien suivant : [TS2log - version d'évaluation complète](#)

Une application « Setup Launcher » va être téléchargée

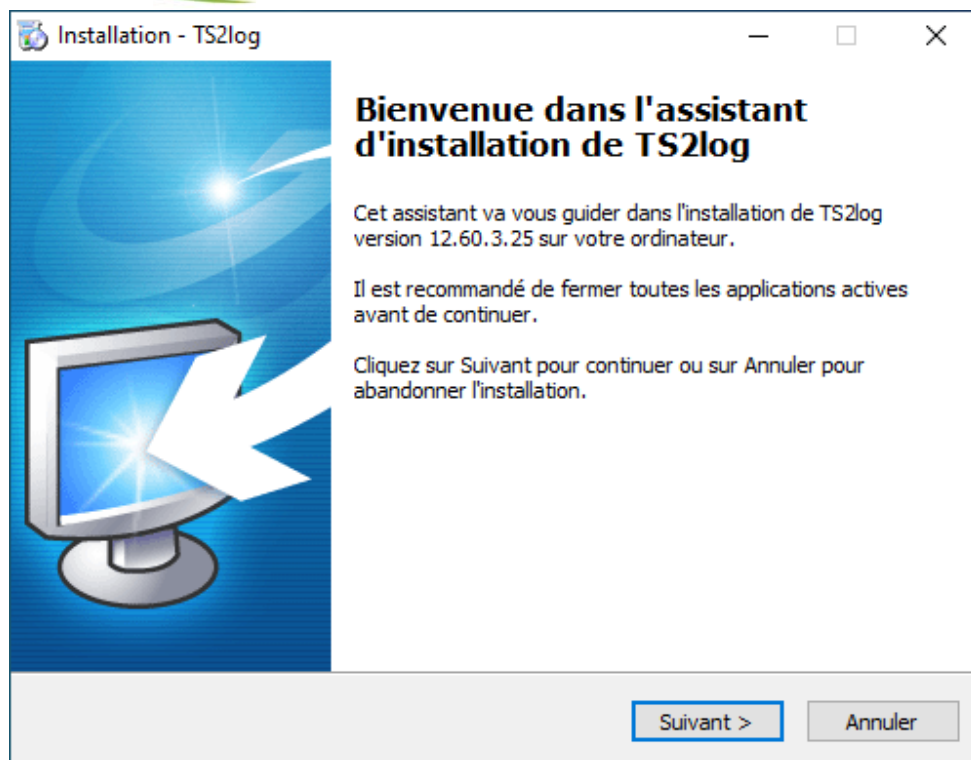


Exécuter ce « Setup Launcher » en mode administrateur

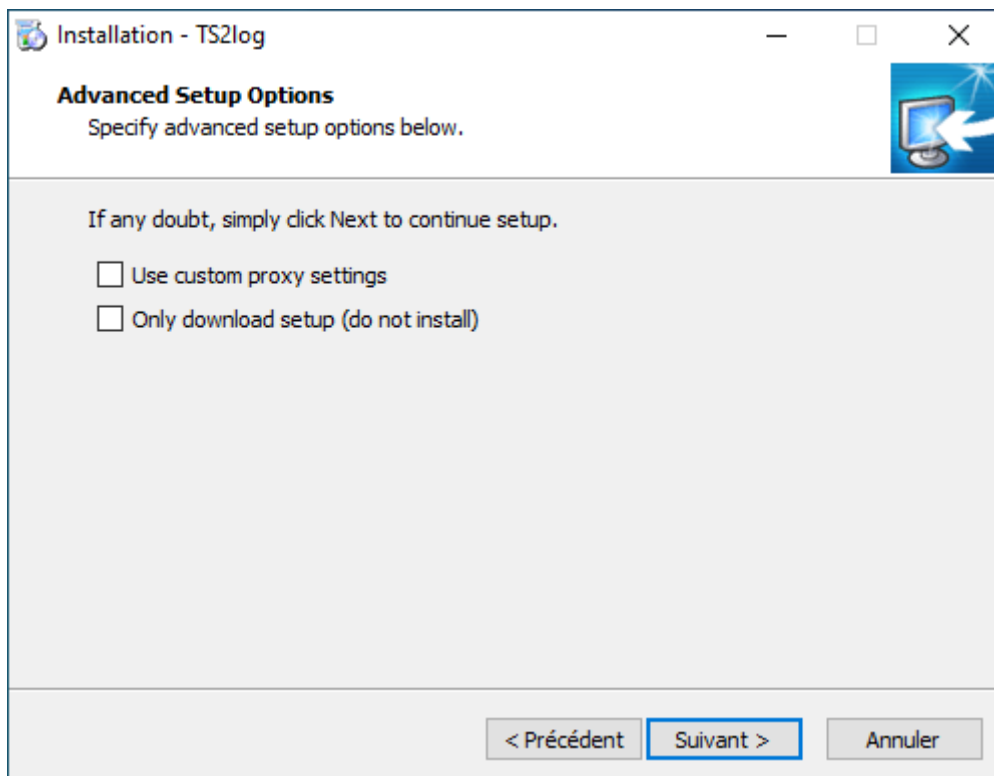


Sélectionner « Oui » pour « Autoriser cette application à apporter des modifications à votre appareil ».

L'assistant d'installation de TS2log démarre :



Ensuite cliquez sur suivant et la fenêtre ci-dessous apparaît :

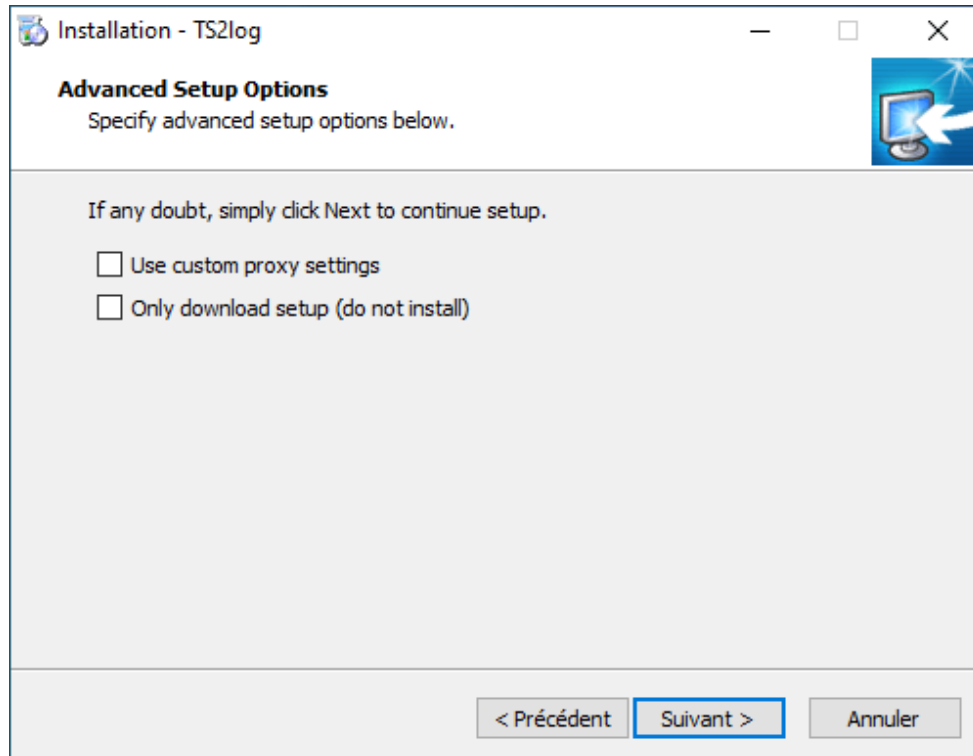


4 possibilités vous sont proposées :

- 0 - La configuration du Proxy
- 1 - Le téléchargement seul du Setup de TS2log
- 2 - Le téléchargement du Setup de TS2log, suivi de l'installation de TS2log
- 3 - La configuration du Proxy, suivi du téléchargement du Setup de TS2log

Option 0 :

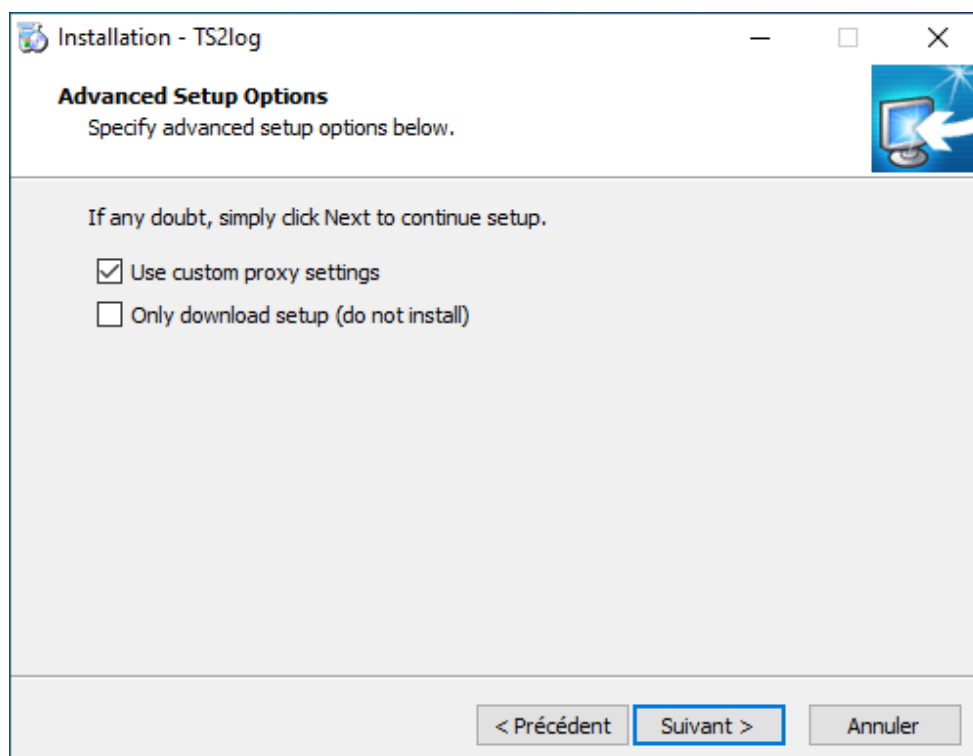
Si vous ne sélectionnez aucune des 2 options :



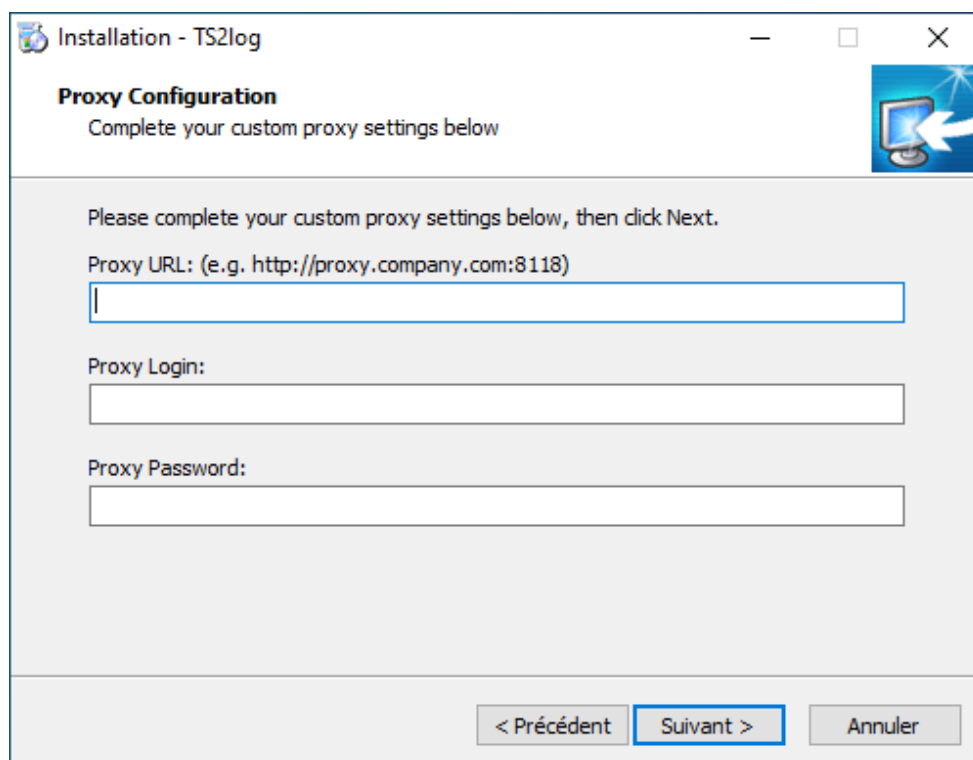
Si vous sélectionnez « Suivant », le téléchargement du Setup de TS2log démarre, puis s'enchaîne avec l'installation.

Option 1 :

Si vous sélectionnez "Use custom proxy settings":



Dans ce cas, en sélectionnant « Suivant », vous aurez la possibilité de paramétrer votre Proxy, si votre infrastructure en possède un :

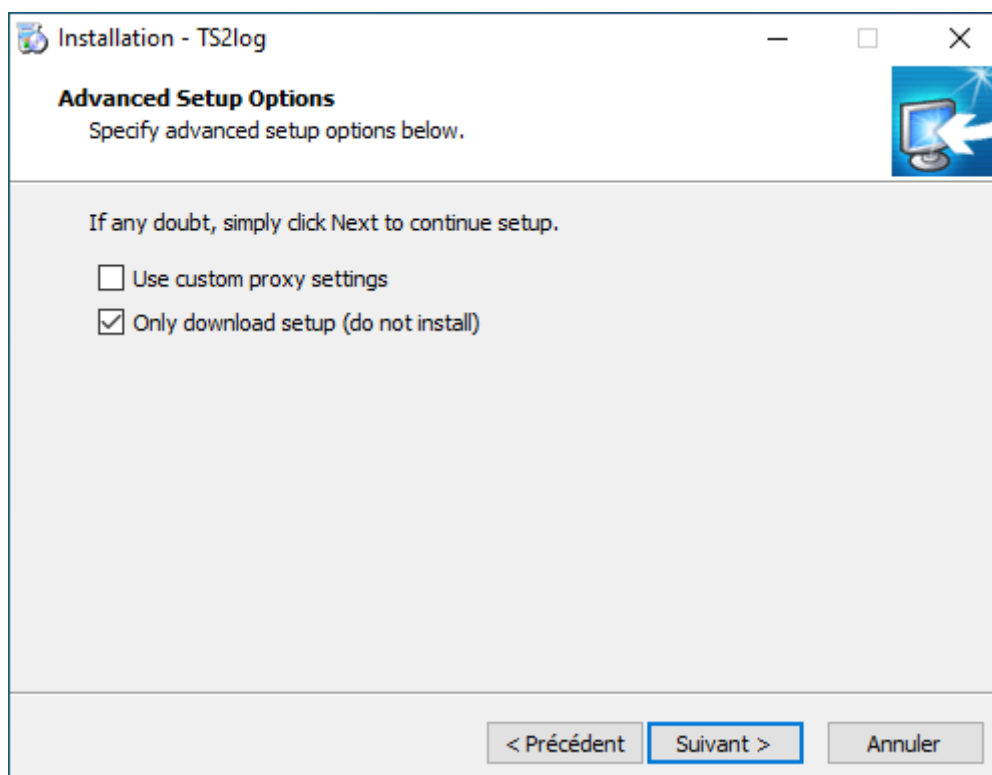


The screenshot shows a window titled "Installation - TS2log" with a "Proxy Configuration" section. The text reads: "Complete your custom proxy settings below". Below this, there is a prompt: "Please complete your custom proxy settings below, then click Next." followed by three input fields: "Proxy URL: (e.g. http://proxy.company.com:8118)", "Proxy Login:", and "Proxy Password:". At the bottom right, there are three buttons: "< Précédent", "Suivant >" (highlighted with a blue border), and "Annuler".

Ensuite, le téléchargement du Setup de TS2log démarre, puis s'enchaîne avec l'installation.

Option 2 :

Si vous sélectionnez « Only download setup (do not install) » :



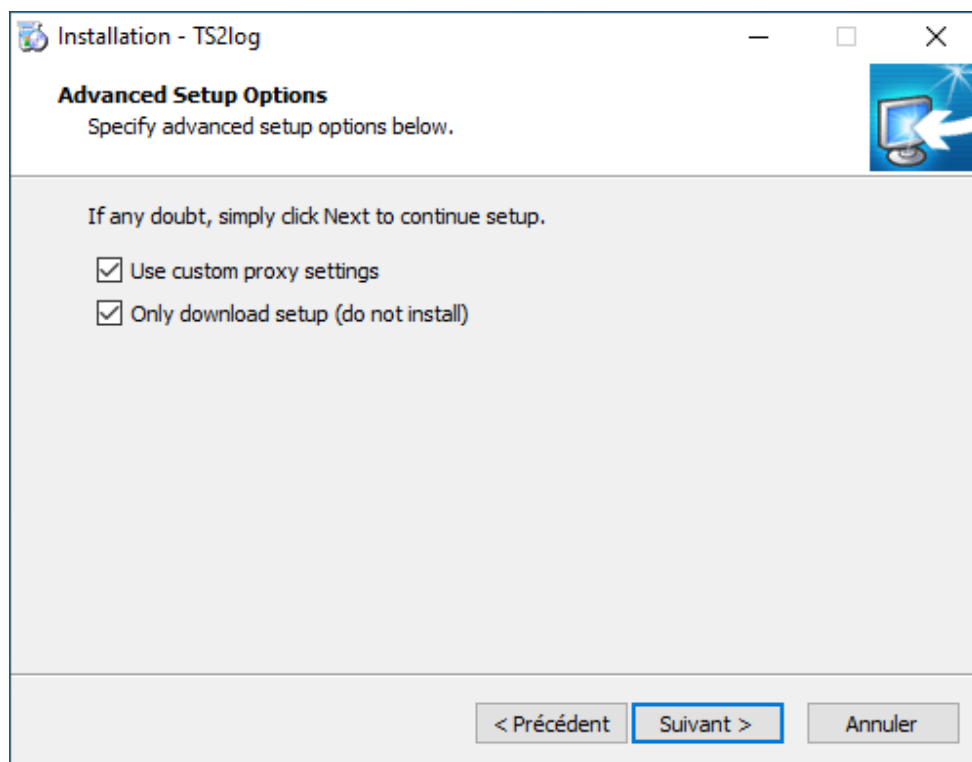
The screenshot shows a window titled "Installation - TS2log" with an "Advanced Setup Options" section. The text reads: "Specify advanced setup options below." Below this, there is a prompt: "If any doubt, simply click Next to continue setup." followed by two checkboxes: "Use custom proxy settings" (unchecked) and "Only download setup (do not install)" (checked). At the bottom right, there are three buttons: "< Précédent", "Suivant >" (highlighted with a blue border), and "Annuler".

Dans ce cas, en sélectionnant « Suivant », vous ne téléchargerez que le setup d'installation.

De cette manière, vous aurez la possibilité de l'exécuter plus tard, ou de l'installer sur un poste physique différent.

Option 3 :

Si vous sélectionnez « Use custom proxy settings », ainsi que « Only download setup » :



Dans ce dernier cas, vous pourrez configurer votre serveur Proxy, puis télécharger le Setup de TS2log, pour une installation ultérieure.

D'autres URLs sont à votre disposition :

Lien pour l'Update Release, c'est-à-dire le fichier de mise à jour.

Ce dernier ne s'installera que si votre licence possède des droits de support et de mise à jour en cours de validité. La date de fin de support est indiquée en bas de l'onglet Accueil.

[TS2log – Mise à jour](#)

Lien pour le téléchargement du module de connexion.

Ce dernier est nécessaire quand vous générez vos clients de connexion, via le générateur de connexion de TS2log

[TS2log – Module de connexion](#)

VÉRIFICATIONS

Via la console d'administration de TS2log accédez à l'onglet « ACCUEIL » :

Selon votre mode de connexion distante utilisé :

- **Modifiez la valeur** du port RDP, par défaut (3389).
- **Modifiez la valeur** du port HTTPS, par défaut (443).

Attention, si vous utilisez le mode Web, ne pas modifier le port HTTP, par défaut (80), si vous désirez utiliser notre certificat gratuit « Let's Encrypt » qui s'appuie sur ce port. Ce port sera ensuite redirigé vers le port HTTPS pour des raisons de sécurité.

Sur votre serveur, selon l'OS utilisé, vérifier que « Tout le monde » ne soit pas membre du groupe « Utilisateurs du Bureau à distance », si tel est le cas, veillez à supprimer « Tout le monde » de ce groupe.

SÉCURITÉ

Pour sécuriser vos accès, il est conseillé, via la console d'administration de TS2log, onglet « SESSIONS » de :

- Cochez « Limiter l'accès au groupe Utilisateurs Bureau à Distance », puis de mettre les Utilisateurs/Groupes autorisés à se connecter, en tant que membre du groupe « Utilisateurs du Bureau à distance ».
- Cocher « Autoriser uniquement les utilisateurs avec au moins 1 application » si vous utilisez la publication d'application. Ne pas utiliser cette option si vous ne faites que du bureau distant.

The screenshot shows the administration interface of TS2log. On the left is a navigation menu with icons and labels: ACCUEIL (Home), APPLICATIONS, IMPRESSION (Printer), WEB (Globe), FERME (Calendar), SESSIONS (Person icon), Paramètres, Permissions, and Générateur de Clients. The 'SESSIONS' menu item is highlighted. On the right, the 'Restrictions Client Bureau à Distance Microsoft' section contains four radio button options: 'Autoriser les connexions venant d'un client RDP de tout le monde' (selected), 'Autoriser les connexions venant d'un client RDP des administrateurs seulement', 'Rejeter les sessions venant d'un client RDP', and 'Refuser l'accès depuis l'extérieur (réseau local uniquement)'. Below this is the 'Options avancées de sécurité du serveur' section with several checkboxes: 'Limiter l'accès au groupe Utilisateurs Bureau à Distance' (checked), 'Cryptage de bout-en-bout', 'Bloquer temporairement les accès à ce serveur', 'Désactiver l'UAC et améliorer Windows', 'Accepter les clés Windows' (checked), 'Autoriser uniquement les utilisateurs avec au moins 1 application assignée' (checked), and 'Autoriser le COPIER/COLLER à l'intérieur d'une session' (checked). Red arrows point from the 'SESSIONS' menu item to the 'Options avancées de sécurité du serveur' section.

CONSEILS

Dès l'instant où vous autorisez des connexions distantes depuis l'extérieur via votre modem routeur, votre serveur à de grande chance de subir des cybers attaques. Il est donc impératif d'exercer des règles d'accès au dit serveur. Depuis la version 12, vous bénéficiez au travers de la console d'administration TS2log (AdminTools : onglet « EXTENSIONS ») d'un lien d'installation de notre solution de restriction d'Accès « TS2log Security ». Cette solution intervient comme une protection complémentaire de votre antivirus et autre dispositif de sécurité (Firewall) déjà installés sur votre serveur, en filtrant et en analysant les connexions distantes.

Voici les principales fonctions de **TS2log Security** :

- **Restriction Géographique RDP :**

Analyse des flux TCP/IP et blocage des flux en provenance des pays non autorisés

- **Restriction d'accès limitée aux heures de travail :**

Interdit aux utilisateurs de se connecter en dehors des plages horaires que vous aurez défini.

- **Protection contre les attaques de Brute-Force :**

Blacklistage automatique des adresses IP attaquantes à partir de x tentatives échouées de « login/mot de passe ».

- **Gestion des Permissions :**

Vérifiez facilement les autorisations des utilisateurs et des groupes sur les dossiers et les fichiers.

- **Sécurisation de l'accès en un clic :**

Fournit un environnement utilisateur hautement sécurisé. Gestion facilitée des droits (GPO) des utilisateurs

- **Filtrage sur le nom du poste de travail :**

limite l'accès par périphérique (nom NetBIOS du périphérique). Liste blanche des collaborateurs autorisés.

- **Protection contre les rançongiciels :**

Détecte et bloque les attaques de ransomware.

Recevez votre version d'évaluation de [TS2log Security](#) :

Guide des [BONNES PRATIQUES](#) de sécurité avec votre serveur TS2log