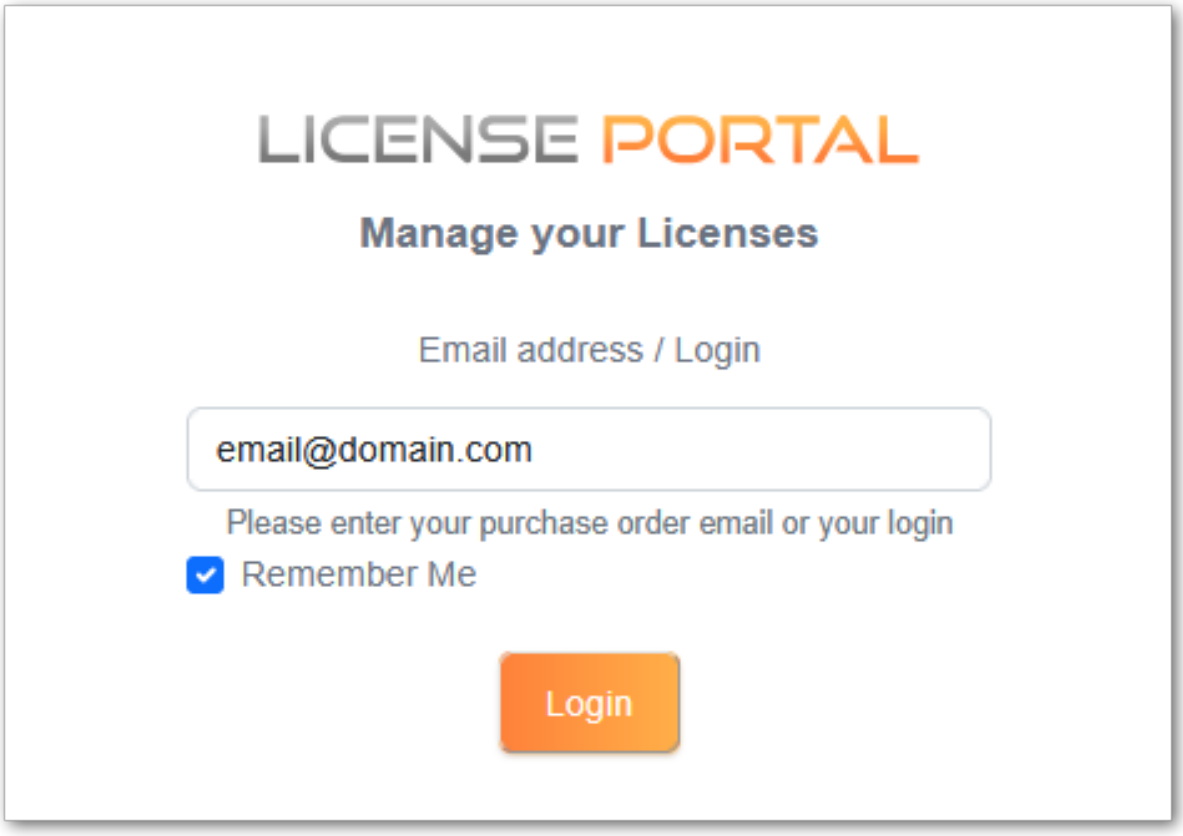
Activer votre licence permanente TSplus (hors ligne)

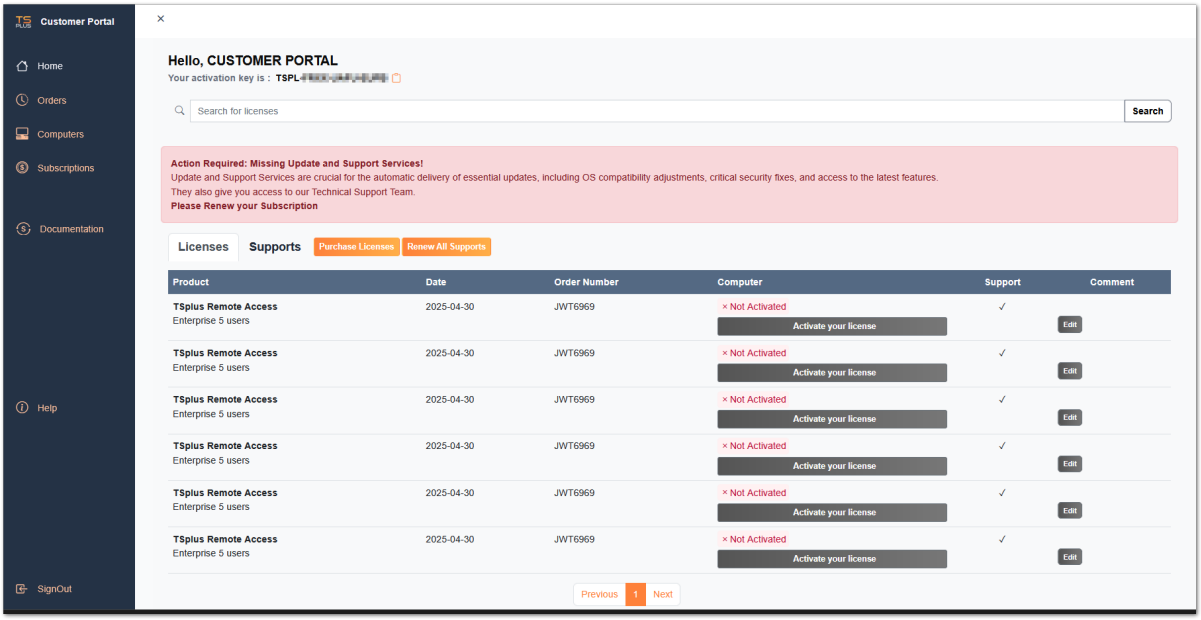
Récupérez votre clé d'activation

Lorsque vous commandez une licence, connectez-vous à notre Portail de licence et entrez votre adresse e-mail et votre numéro de commande.

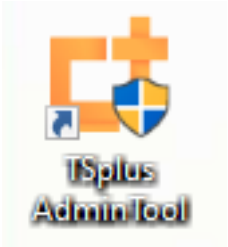


Téléchargez le guide de l'utilisateur du portail client pour plus d'informations sur son utilisation.

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



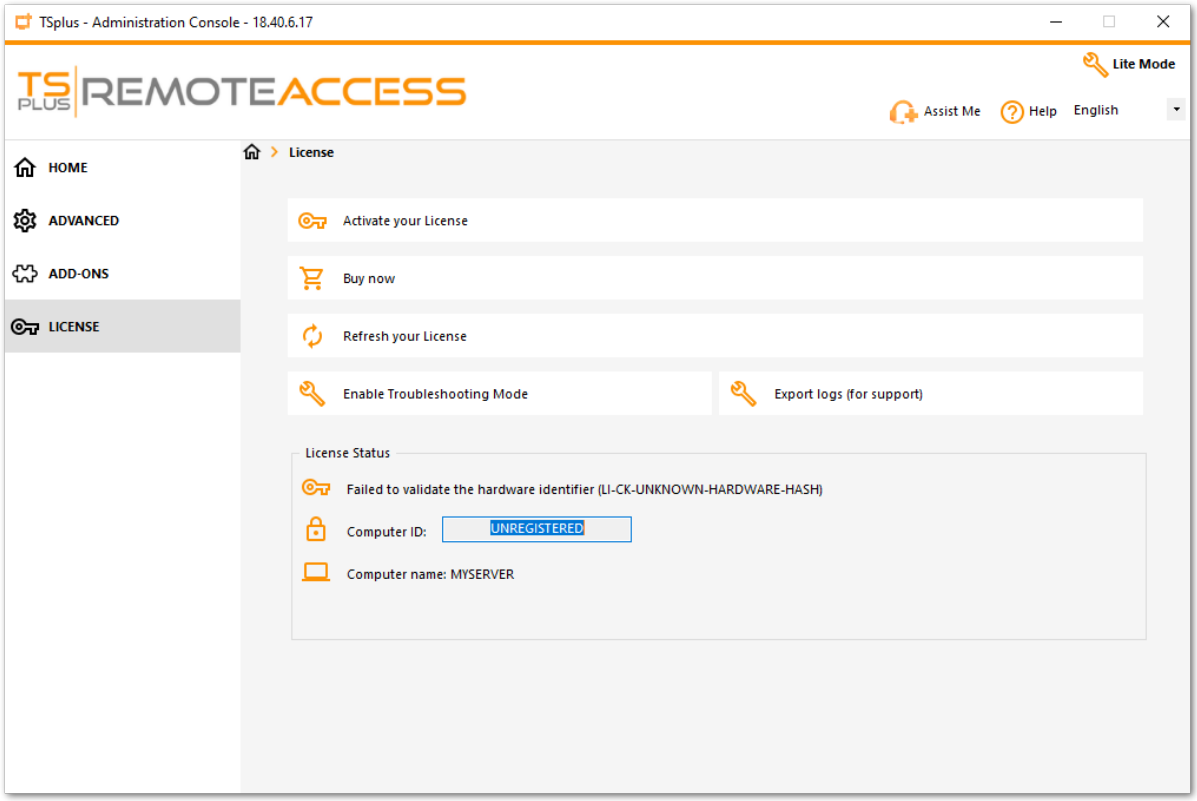
Localisez l'outil Administrateur sur votre bureau



Si vous ne trouvez pas le raccourci de l'outil d'administration, il devrait se trouver dans le dossier du bureau sur le compte administrateur utilisé pour télécharger TSplus. Vous pouvez également trouver le dossier TSplus à ce chemin : ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Double-cliquez dessus, puis cliquez sur l'onglet de licence.

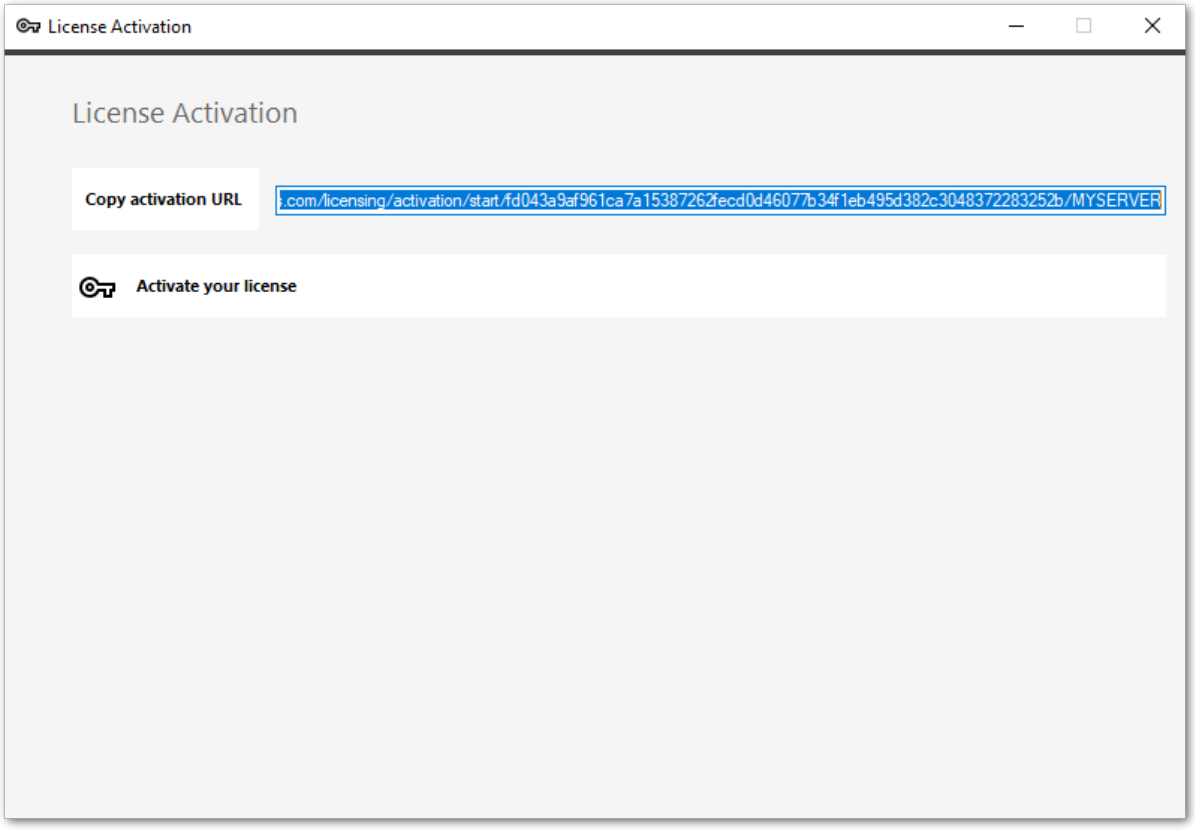
Ici, vous pouvez voir l'état de votre licence TSplus, ainsi que votre ID d'ordinateur et le nom de votre ordinateur "NON ENREGISTRÉ".



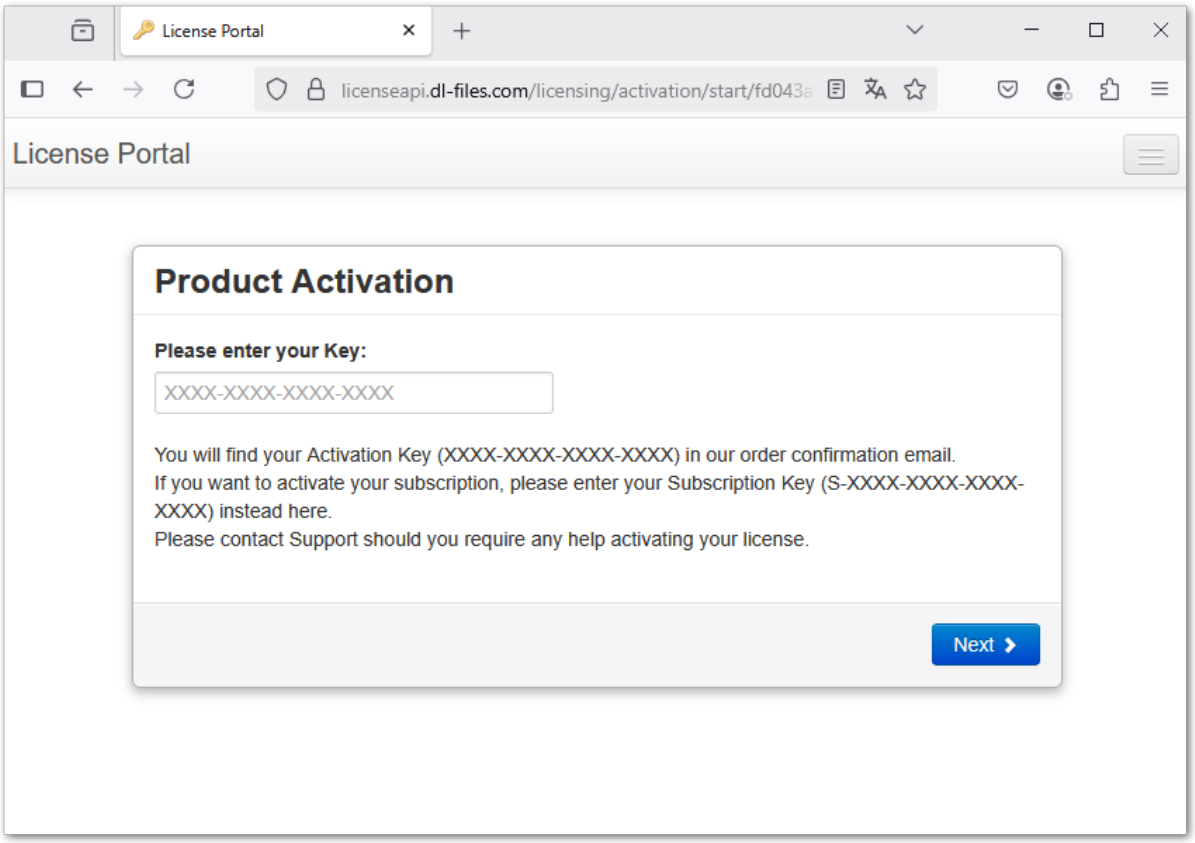
Activez vos licences sur un serveur TSplus hors ligne

Cliquez sur le bouton « Activer votre licence ». Une fenêtre contextuelle apparaît et affiche une adresse URL assez longue.

Copiez cette URL dans le navigateur d'un ordinateur connecté à Internet et accédez-y afin de récupérer un fichier de licence :

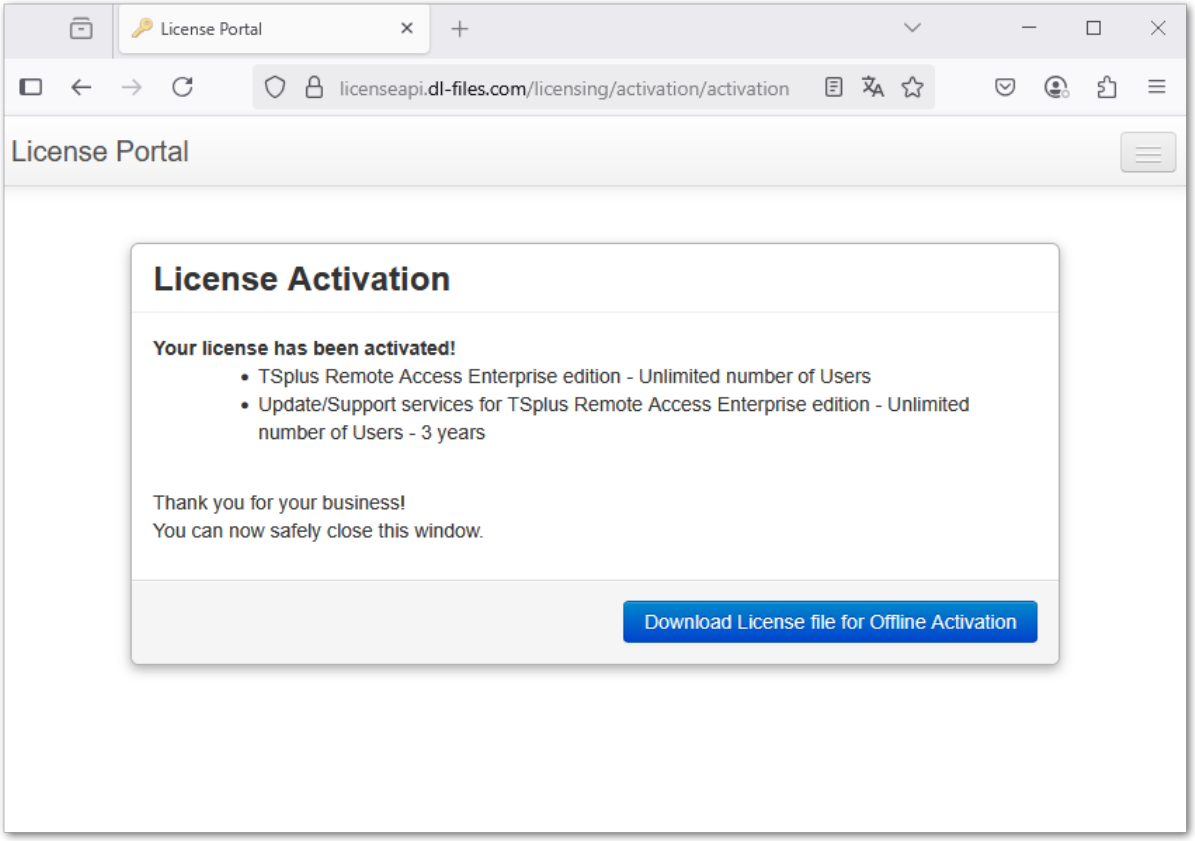


Entrez votre clé d'activation :

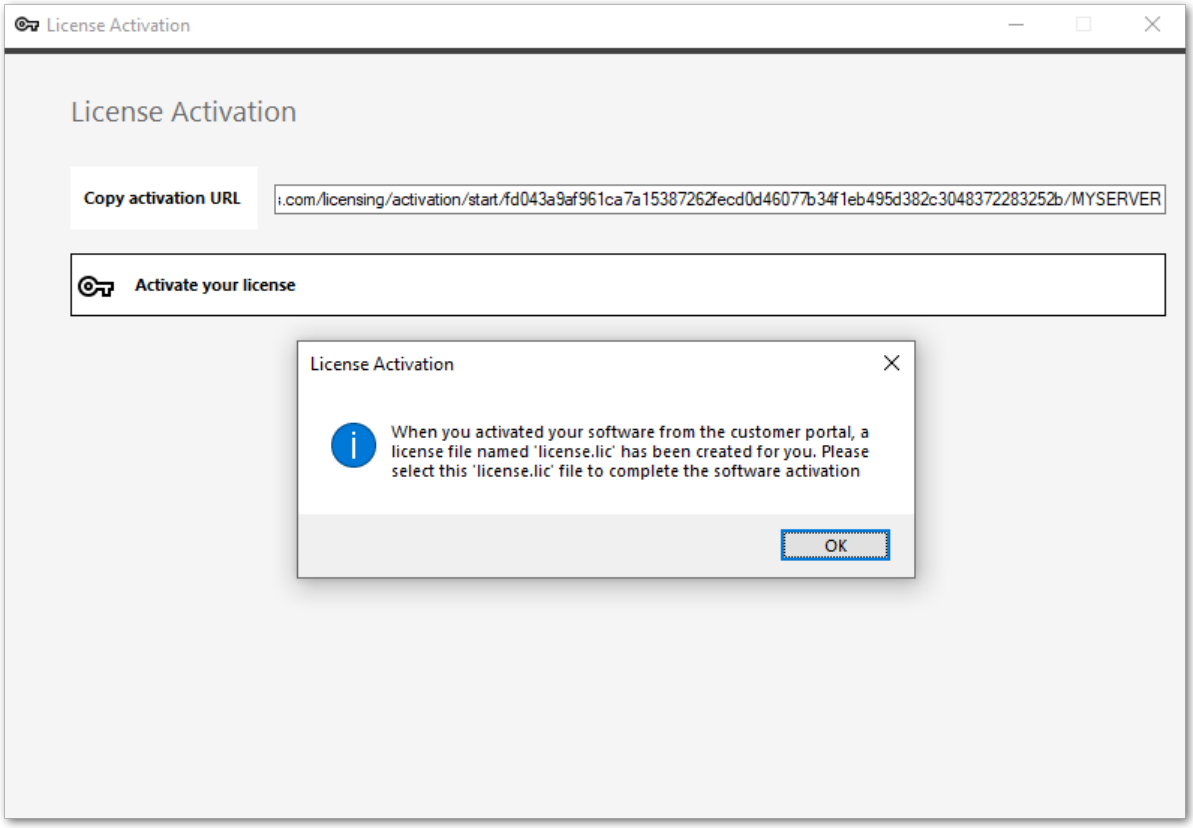


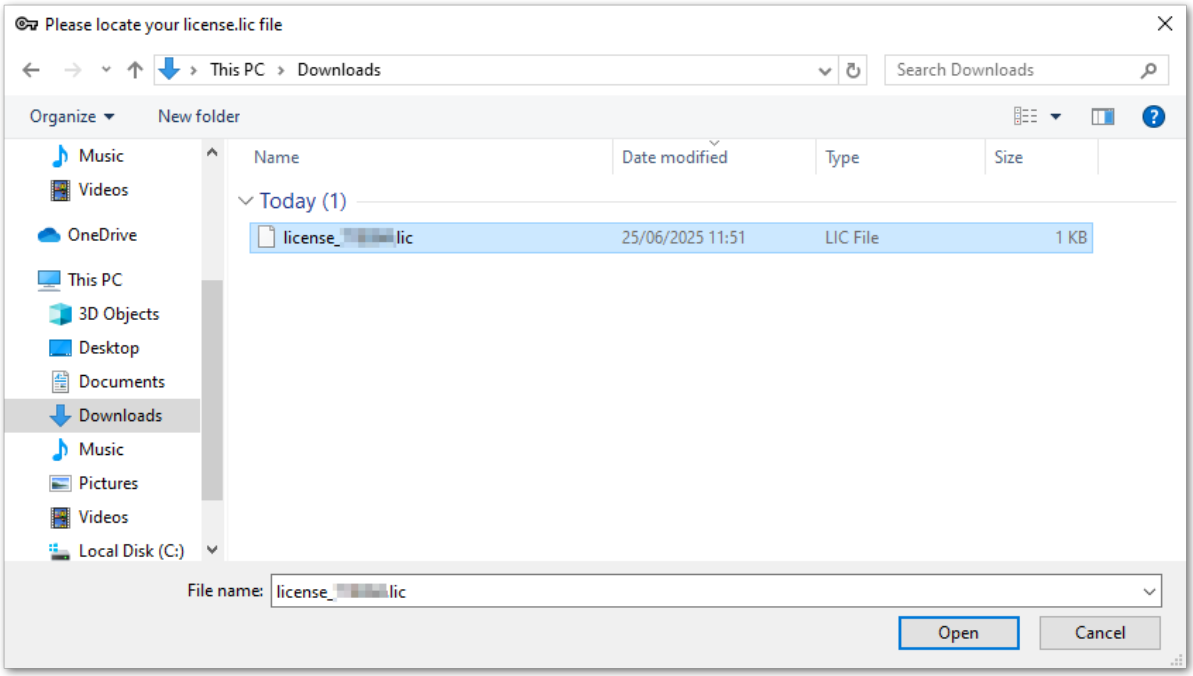
Votre licence est alors validée. Téléchargez le fichier de licence en cliquant sur le bouton

correspondant :

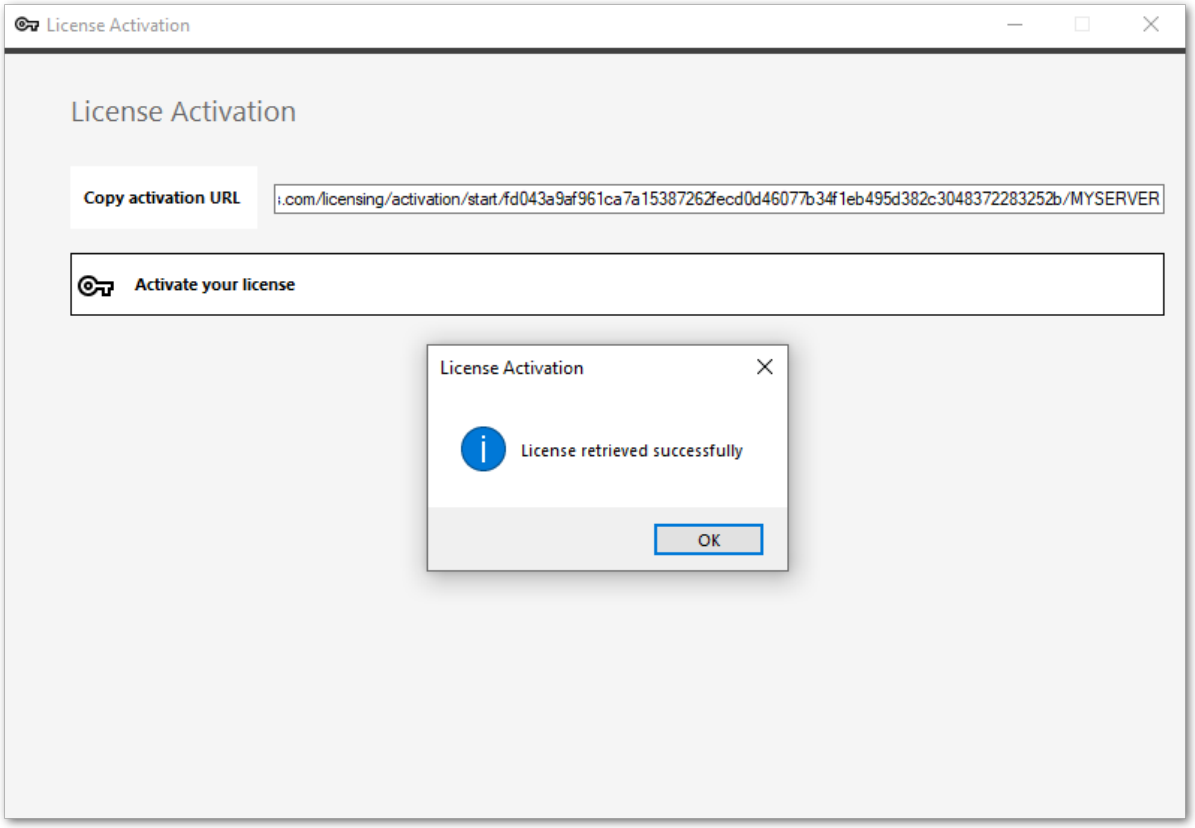


Ce fichier de licence doit ensuite être copié sur le serveur afin de terminer le processus d'activation hors ligne :





Un message confirmera que votre licence a été récupérée avec succès :

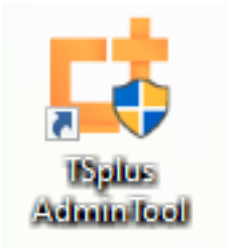


Vous devrez ensuite sélectionner les licences / support correspondants à activer et un message confirmant que tous vos produits/support sont désormais activés.

N.B Vous pouvez toujours télécharger des fichiers license.lic sur le Portail de Licences pour les Versions Héritées de TSplus. Téléchargez le guide de l'utilisateur du portail client .

Activer votre licence TSplus (en ligne) permanente ou par abonnement.

Localisez l'outil Administrateur sur votre bureau :

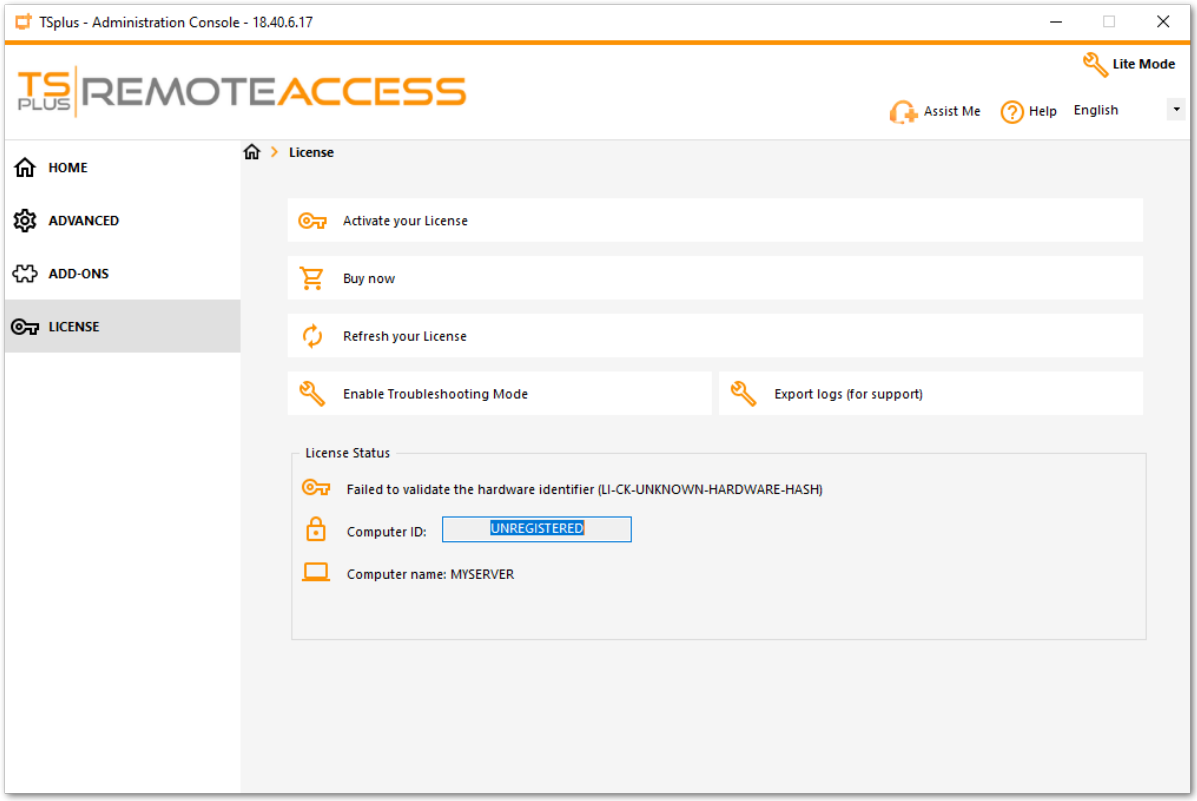


- Si vous ne trouvez pas le raccourci de l'outil d'administration, il devrait se trouver dans le dossier du bureau sur le compte administrateur utilisé pour télécharger TSplus. Vous pouvez également trouver le dossier TSplus à ce chemin : ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Double-cliquez dessus, puis cliquez sur l'onglet de licence.

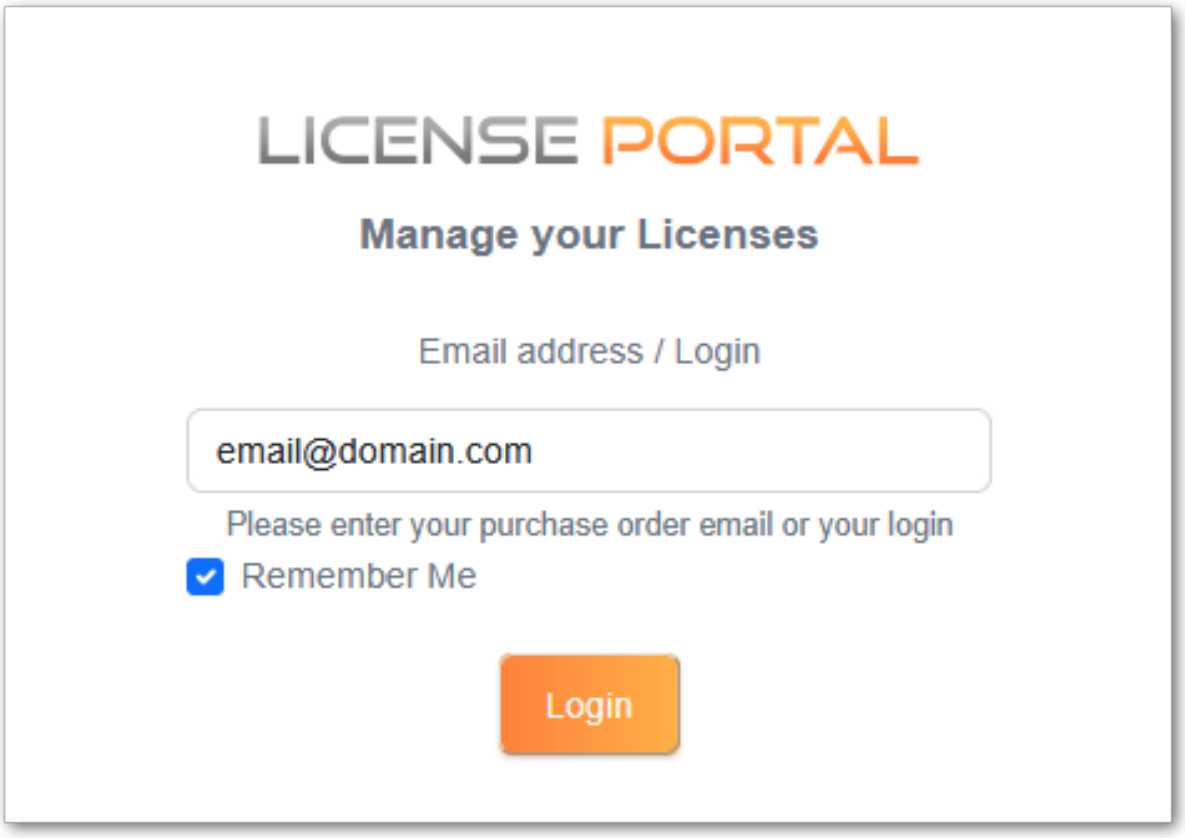
Ici, vous pouvez voir l'état de votre licence TSplus, ainsi que votre ID d'ordinateur et le nom de votre ordinateur :

si cela affiche "NON ENREGISTRÉ", cela signifie que votre serveur n'est pas connecté à Internet et que vous devez vérifier l'accès web de votre serveur avant de continuer.



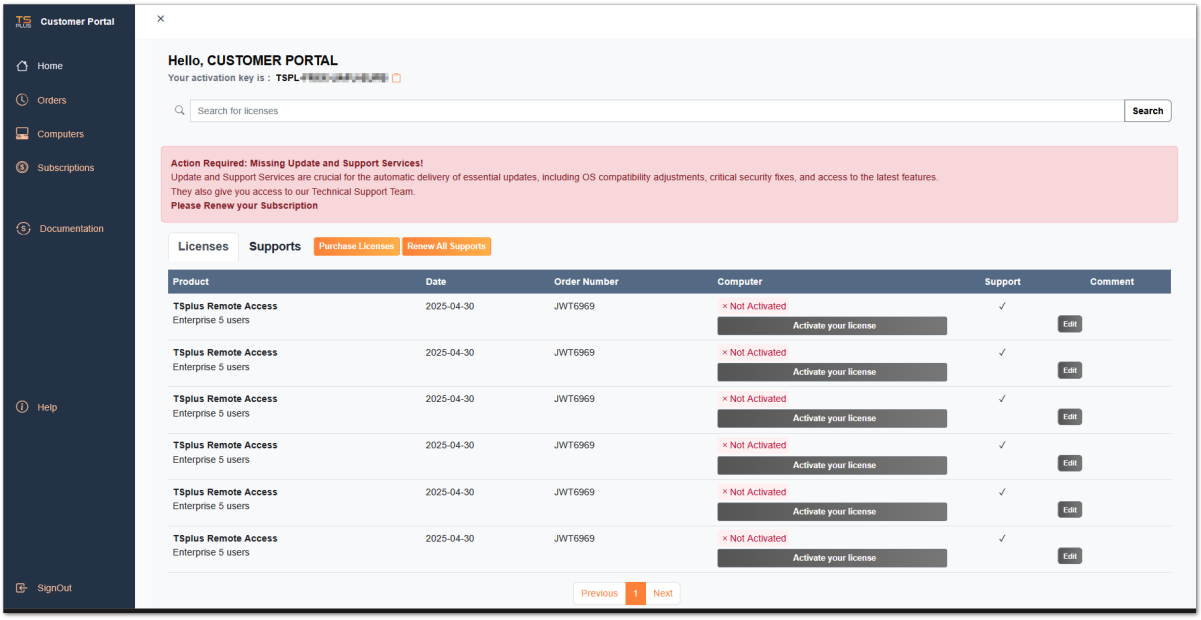
Activez vos licences sur un serveur TSplus en ligne

Lorsque vous commandez une licence, connectez-vous à notre Portail de licence et entrez votre adresse e-mail et votre numéro de commande :



Téléchargez le guide de l'utilisateur du portail client pour plus d'informations sur son utilisation.

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

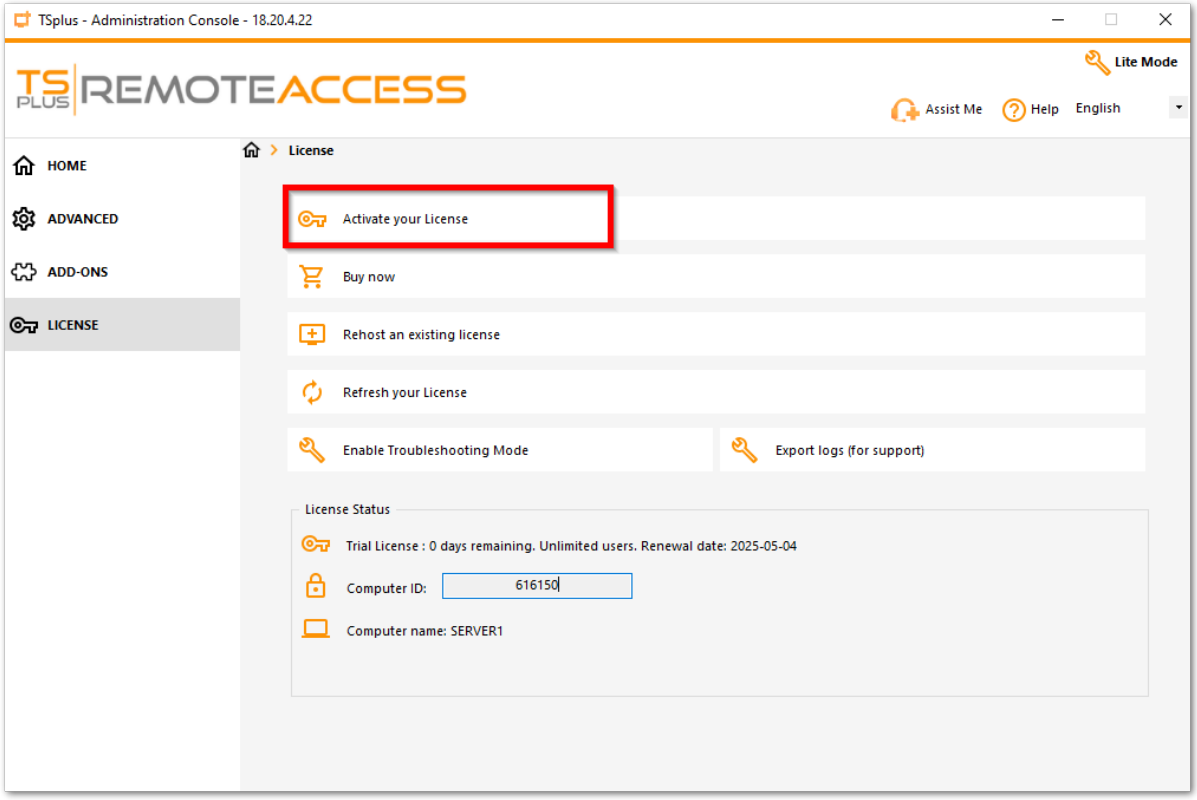


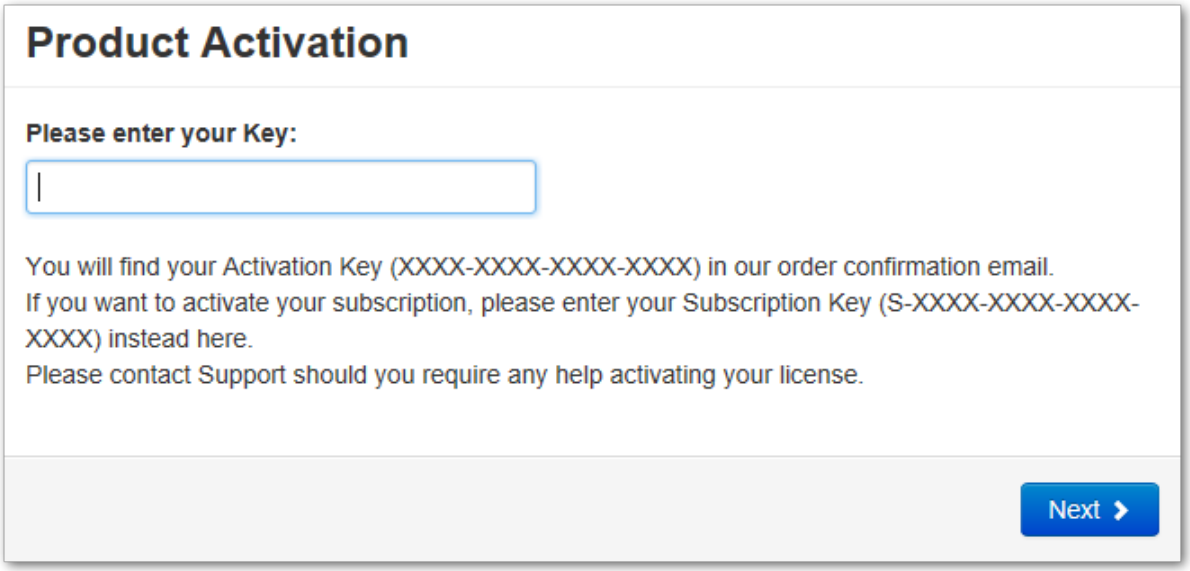
Vous pouvez ensuite aller à la tuile de licence de l'AdminTool, cliquer sur le bouton « Activer votre licence », entrer cette clé d'activation et cliquer sur « Suivant ».

Vous trouverez votre clé d'activation permanente **(XXXX-XXXX-XXXX-XXXX)** dans notre e-mail

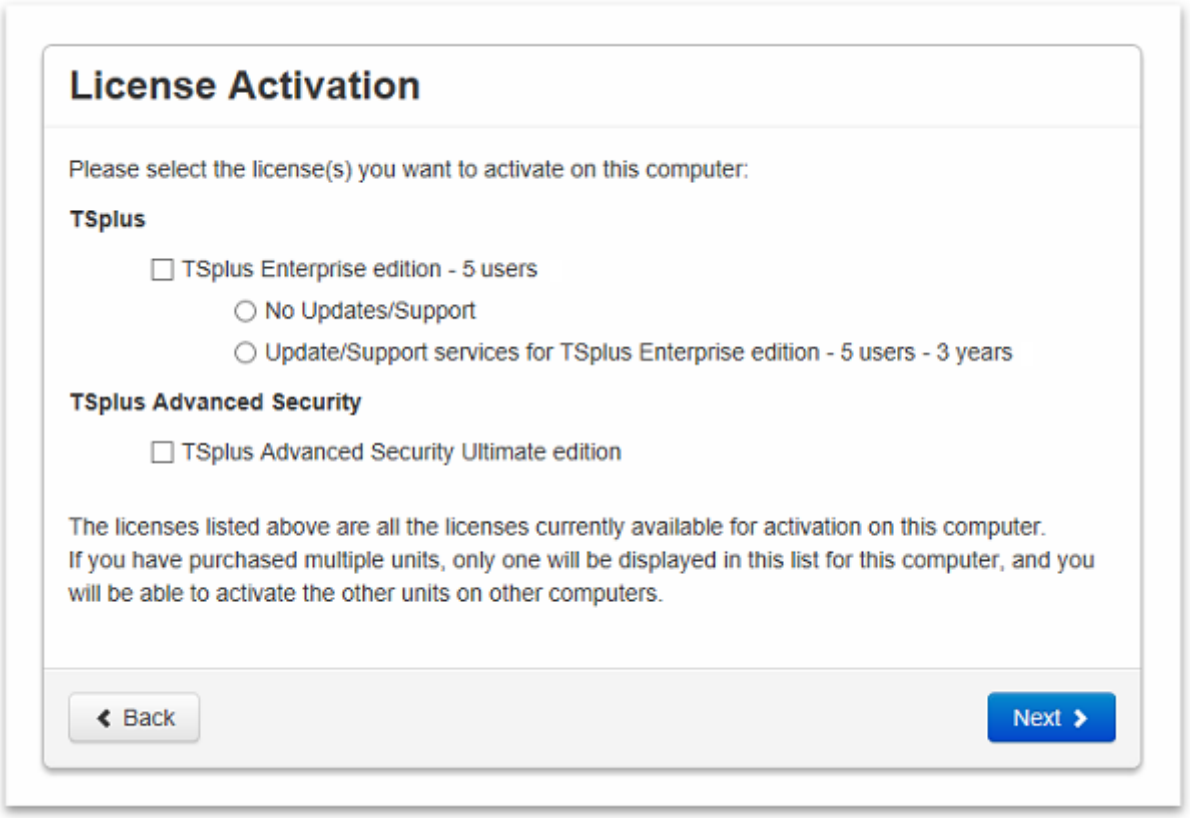
de confirmation de commande.

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

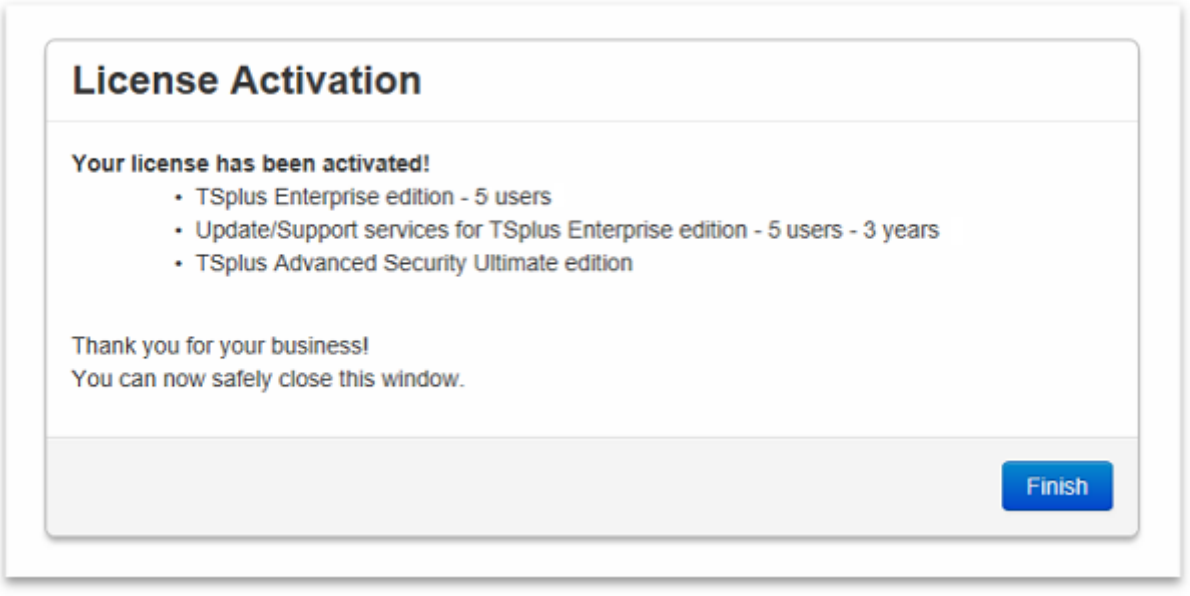




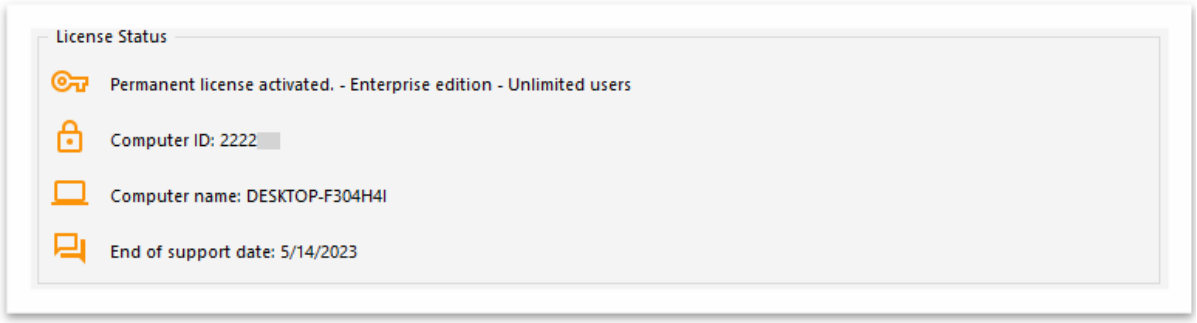
Vous obtiendrez une liste de toutes les licences/soutiens disponibles assignés à cette clé d'activation, c'est-à-dire toutes les licences/soutiens non encore activés :



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/support !



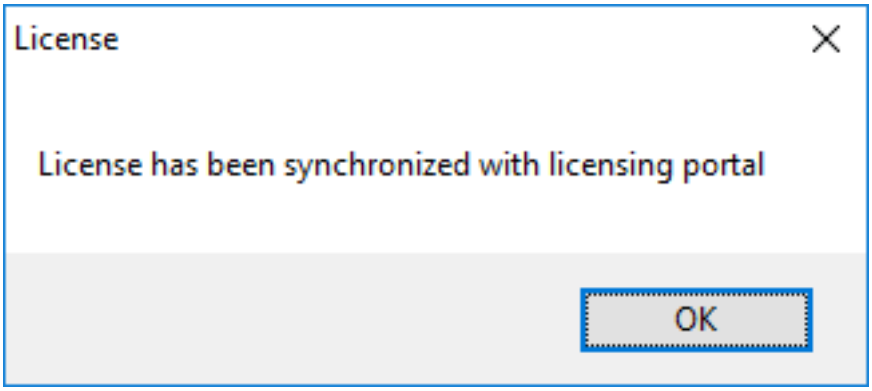
Tous vos produits/support sont maintenant activés (dans cet exemple, à la fois TSplus avec support et TSplus Advanced Security ont été activés en même temps).





Rafraîchissez vos données de licence en cliquant sur le bouton correspondant en bas de la page, cela synchronisera les informations avec notre portail de licences :





N.B Vous pouvez toujours télécharger des fichiers license.lic sur le Portail de Licences pour les Versions Héritées de TSplus. Téléchargez le guide de l'utilisateur du portail client .

Problème d'activation :

Erreur de page ou le bouton « SUIVANT » ne fonctionne pas. Voici quelques solutions.

Désactivez votre antivirus pendant l'activation de la licence et vérifiez les paramètres de votre pare-feu et de votre antivirus.

Vérifiez votre navigateur pour le message OK en cliquant sur ce lien : https://licenseapi.dl-files.com/licensing/ping

Si vous avez un problème avec un programme antivirus, la procédure consiste à exclure les répertoires suivants : C:\Program Files (x86)\TSplus et C:\wsession

URLs à autoriser dans votre antivirus et votre pare-feu pour les mises à jour : setup.dl-files.com dl-files.com secure-download-file.com

Licence / Télémétrie : 93.88.241.55 Mises à jour : 51.254.22.117 Mises à jour de compatibilité TSplus / Vérifier les mises à jour / Voir le journal des modifications : 83.166.153.206

Ports à autoriser : (Port 3389 pour RDP depuis WAN, Port 80 pour HTTP et 443 pour HTTPS)

Vérifiez vos paramètres de sécurité Internet
Panneau de configuration > Options Internet > Niveau personnalisé Scripts > Scripts actifs > Activer

Code d'alerte fatal 40 70

Si vous rencontrez des codes d'alerte fatale 40/70 TLS dans le Visualiseur d'événements lors de chaque tentative de synchronisation ou de mise à jour.

Certaines suites de chiffrement TLS peuvent être désactivées. Vous pouvez utiliser des logiciels gratuits comme **IIS Crypto 4.0** pour les vérifier et les activer.

Activer votre licence de support

La version 15 de TSplus a introduit une nouvelle et facile façon de gérer votre contrat de support annuel.

L'abonnement de support est disponible uniquement pour les licences perpétuelles. Les licences d'abonnement incluent des mises à jour.

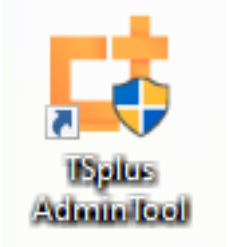
Les services de support incluent notre service de support Ticket/Email mondial, l'accès au Forum, le réhébergement de licences, le support FAQ et le support des tutoriels.

Les services de mise à jour comprennent la livraison de codes de mise à jour, le droit d'installer et d'utiliser toute nouvelle version, correctif et mise à jour.

Nous investissons chaque jour pour améliorer TSplus et résoudre tous les problèmes connus. Nous recommandons donc à tous nos clients de maintenir leur installation de TSplus à jour. Le tarif annuel n'est pas cher et est disponible sur notre page de boutique.

Étape Un

Localisez l'outil d'administration sur votre bureau :



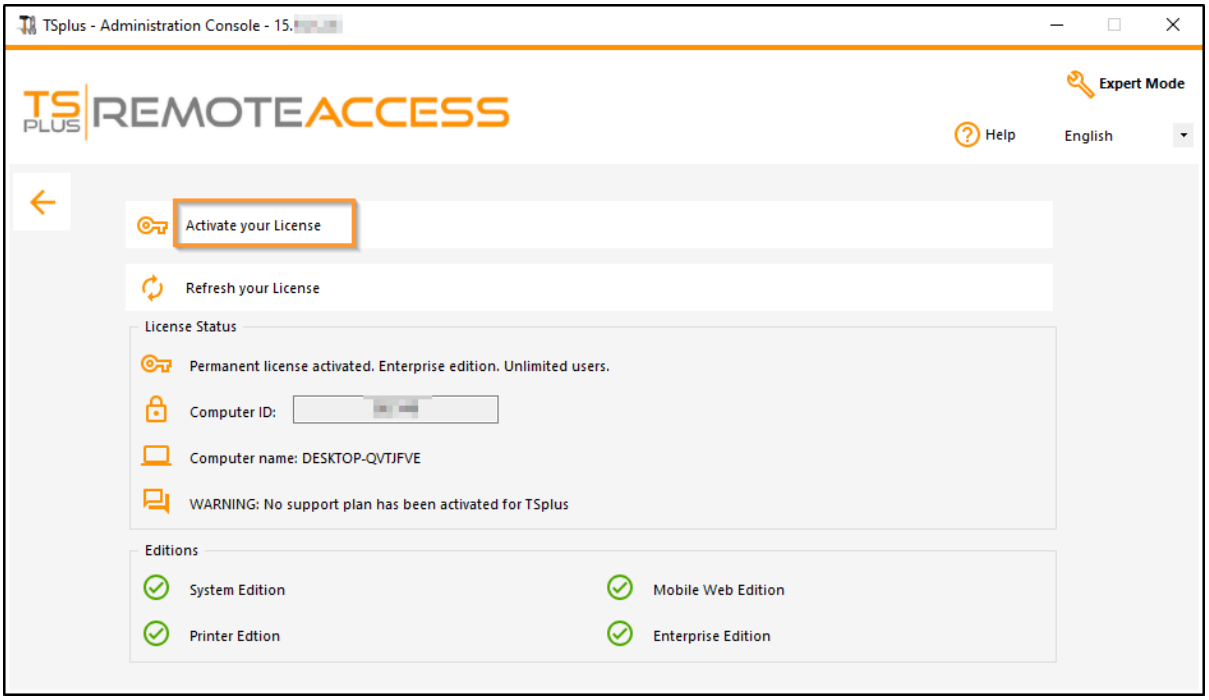
Double-cliquez dessus, puis cliquez sur la tuile de licence.

- Si vous ne trouvez pas le raccourci de l'outil d'administration, il devrait se trouver dans le dossier du bureau sur le compte administrateur utilisé pour télécharger TSplus. Vous pouvez également trouver le dossier TSplus à ce chemin : ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Cliquez sur l'onglet Licence Vous pouvez maintenant voir le numéro de série :

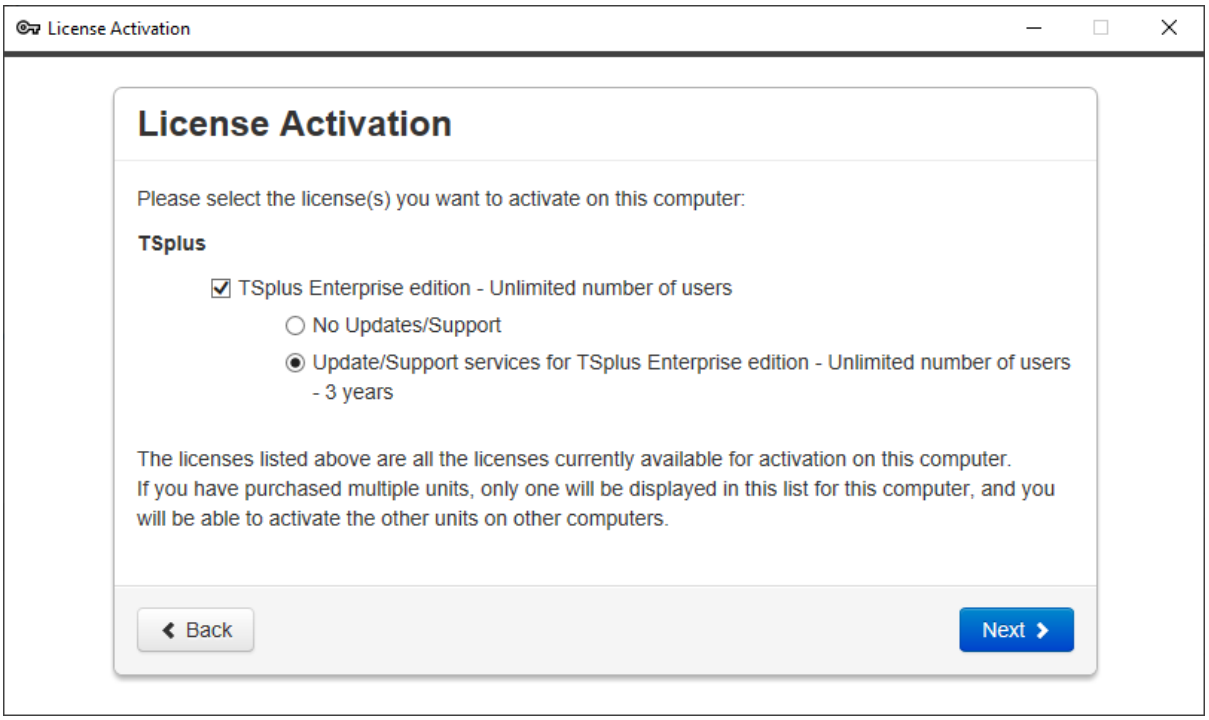
Étape Deux

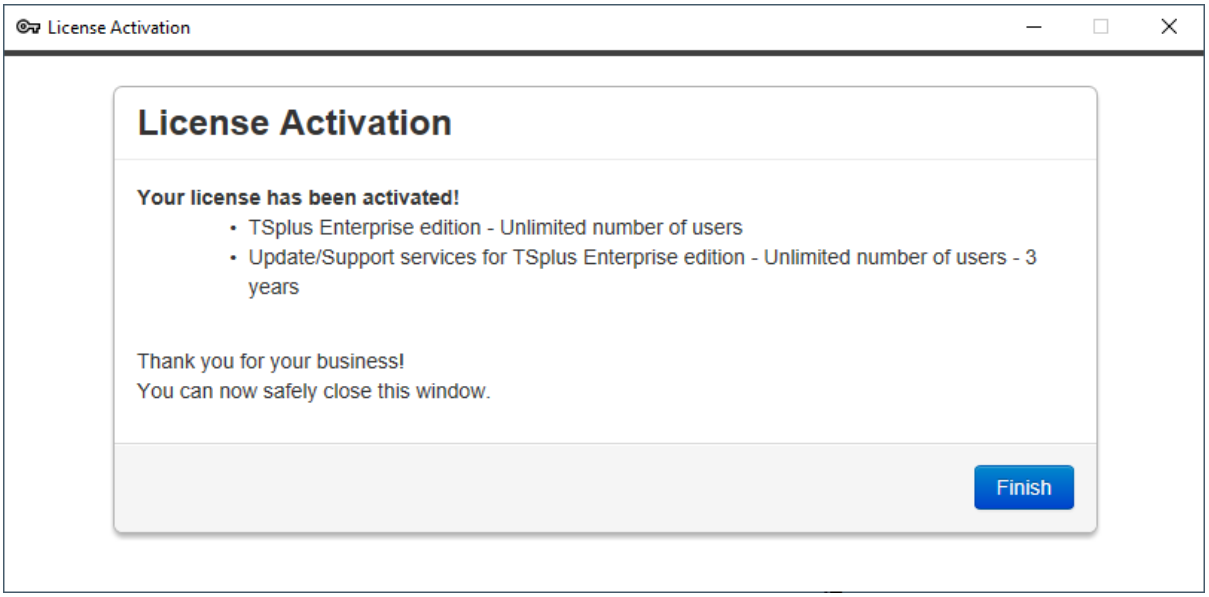
Cliquez sur la tuile « Activer votre licence » et saisissez votre clé d'activation.



Étape Trois

Puis sélectionnez « Étendre la période de support » :



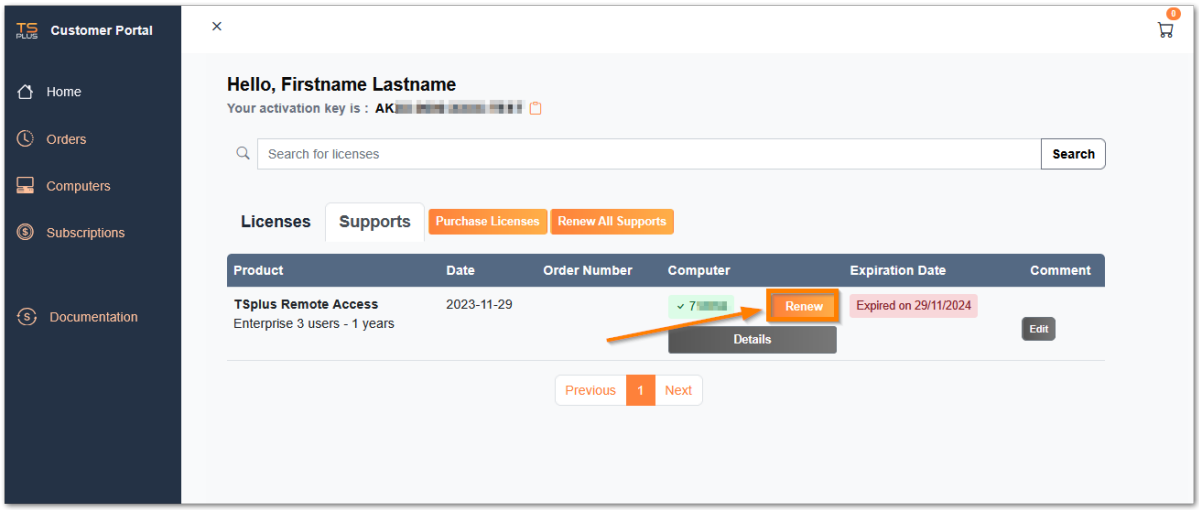


Étendre un abonnement de mise à jour/soutien

Accédez à votre portail de licence : https://license.tsplus.net/login
ID : « Adresse e-mail d'achat »
Mot de passe : « Numéro de commande de votre choix »

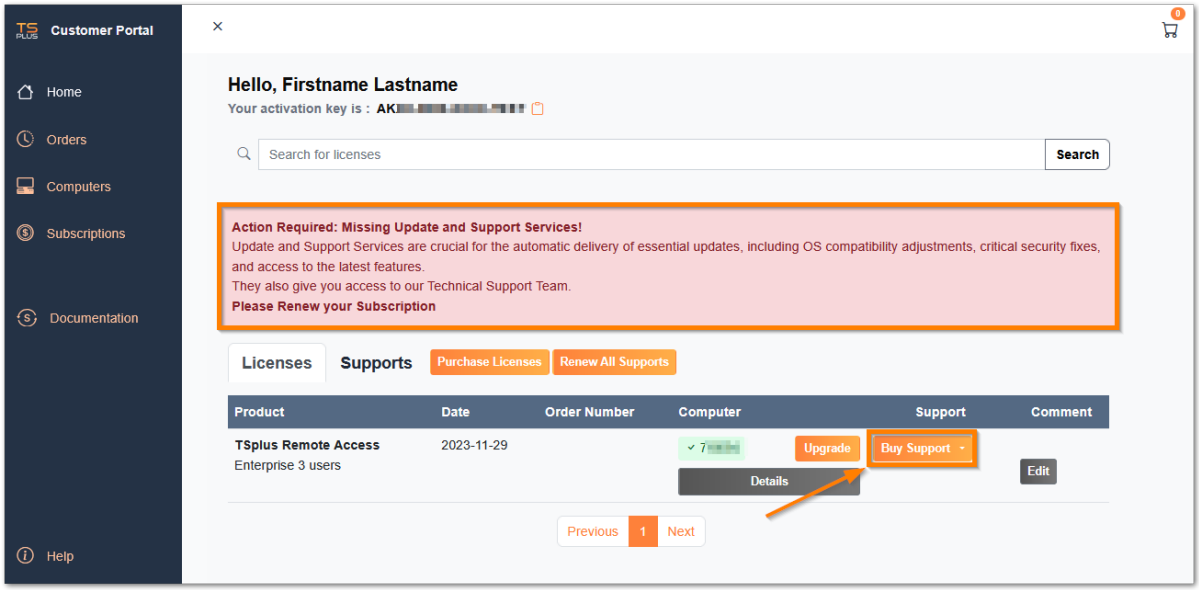
Ensuite, allez dans l'onglet Support et saisissez votre identifiant d'ordinateur (visible dans l'onglet Licence de l'AdminTool).

Puis cliquez sur le bouton « Renouveler » pour choisir la durée de support de 1, 2 ou 3 ans.



Si vous n'avez pas d'abonnement de support pour une licence, un message apparaîtra sur l'onglet de la licence indiquant
Action requise : mise à jour et services de support manquants !

Vous pouvez acheter votre abonnement de support directement en cliquant sur le bouton « ACHETER LE SUPPORT ».



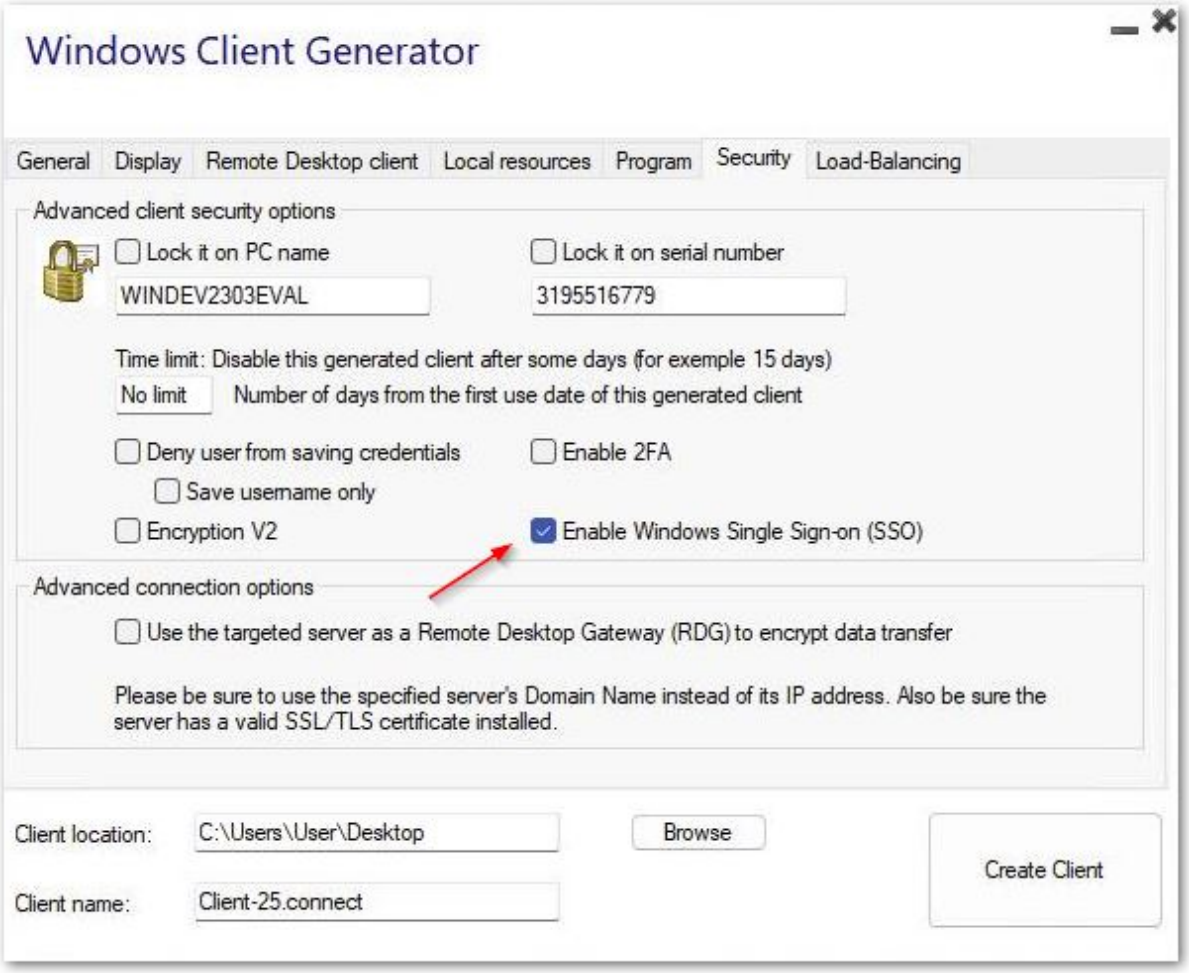
Active Directory Authentification unique

Pour activer l'authentification SSO Windows pour les clients générés :

Mettez à jour TSplus Remote Access vers la dernière version sur un serveur joint au domaine.

Générez un client à partir du Générateur de clients, en cochant la case « Activer l'authentification unique (SSO) » dans l'onglet « Sécurité ».

Connectez-vous depuis une machine jointe au domaine en utilisant le client généré.



Configurer la stratégie de groupe pour l'authentification unique (SSO) Windows via le client de bureau à distance

Depuis le contrôleur de domaine :

1. Ouvrez la console de gestion des stratégies de groupe.

2. Cliquez avec le bouton droit sur l'Unité Organisationnelle (OU) où l'Objet de Stratégie de Groupe (GPO) doit être appliqué et sélectionnez « Créer un GPO dans ce domaine et le lier ici… ».

3. Nommez le GPO (par exemple, SSO_RDS_MON_SERVEUR) et cliquez sur « OK ».

4. Cliquez avec le bouton droit sur la politique créée et sélectionnez « Modifier ».

5. Naviguez vers l'emplacement suivant : « Configuration de l'ordinateur / Stratégies / Modèles administratifs / Système / Délégation des informations d'identification. »

6. Double-cliquez sur « Autoriser la délégation des informations d'identification par défaut » pour ouvrir les paramètres.

7. Activez le paramètre et cliquez sur « Afficher… »

8. Dans le champ Valeur, entrez le(s) serveur(s) au format TERMSRV/ nom_de_domaine_fully_qualified et cliquez sur « OK ».

9. Cliquez sur « Appliquer » et « OK » pour fermer la fenêtre. Depuis la machine cliente :

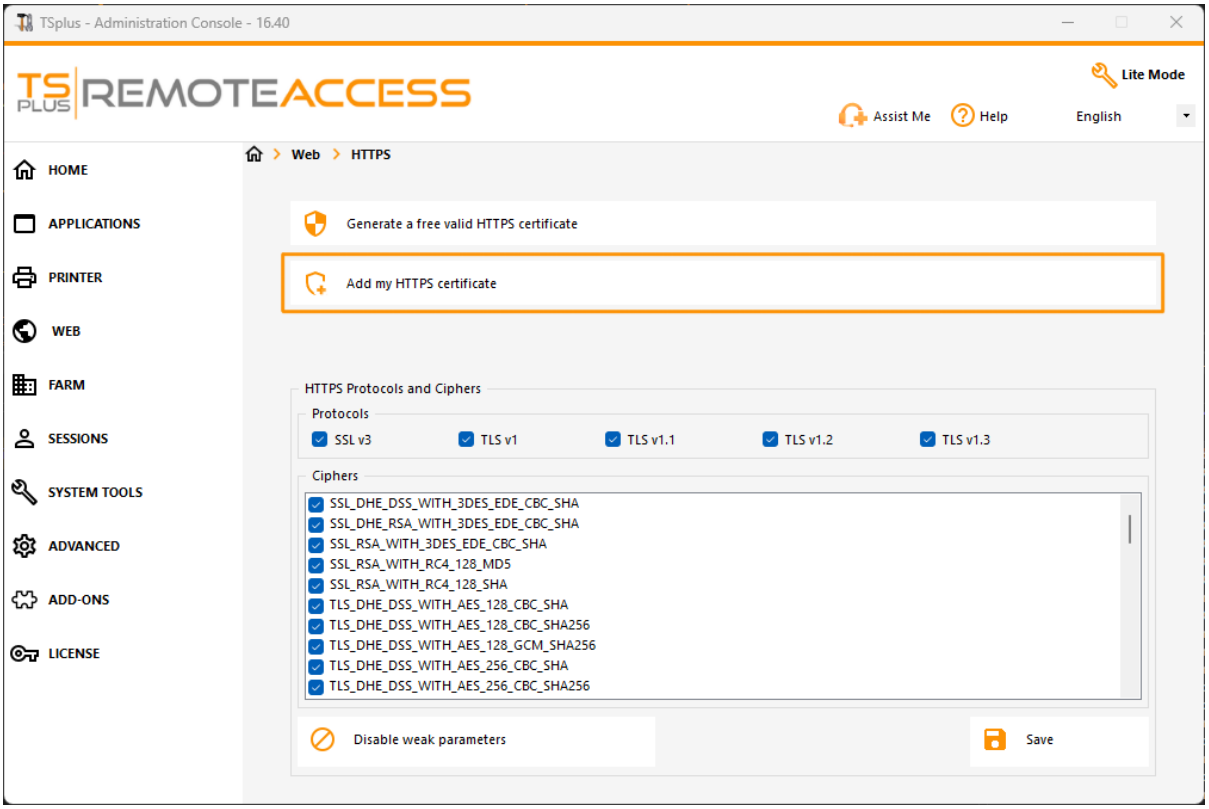
10. Mettez à jour les stratégies de groupe en exécutant la commande suivante en tant qu'administrateur : gpupdate /force.

HTTPS et certificats SSL de tiers

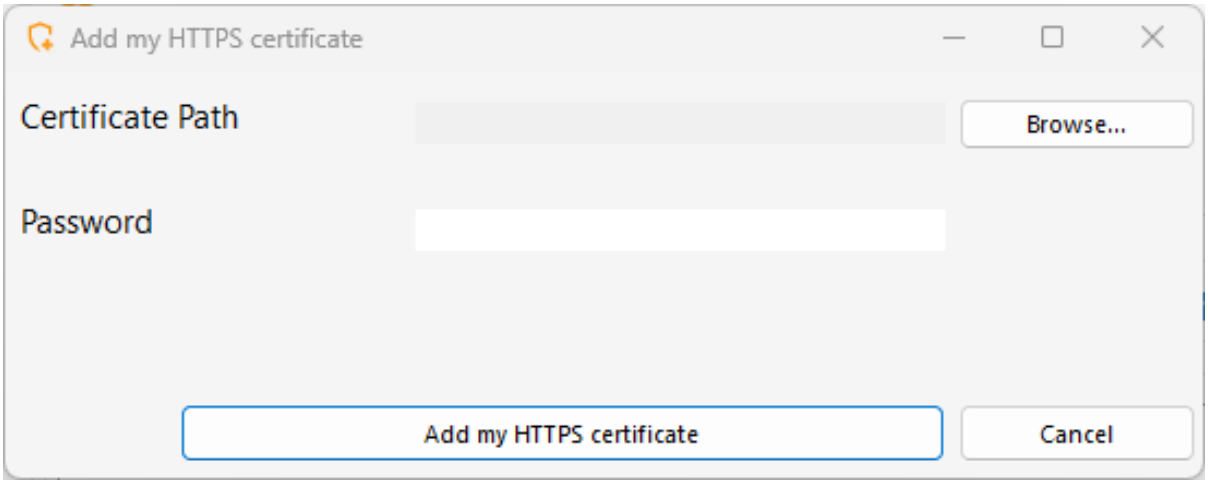
Ajoutez votre propre certificat

Si vous avez déjà un certificat HTTPS valide, vous pouvez l'ajouter à votre serveur web.

Ouvrez TSPlus AdminTool, cliquez sur l'onglet « Web », allez dans le menu « HTTPS » puis cliquez sur « Ajouter mon certificat HTTPS » comme indiqué dans la capture d'écran ci-dessous :



Une fenêtre s'ouvrira où vous pourrez sélectionner votre certificat :



Votre fichier de certificat doit utiliser le format “.pfx”.

Si votre certificat est protégé par un mot de passe, vous pouvez le saisir dans le champ correspondant.

Cliquez sur le bouton « Ajouter mon certificat » pour ajouter votre certificat.

Veuillez noter que vous devrez renouveler votre certificat manuellement.

Liens supplémentaires

Fournisseurs de certificats SSL de confiance :

- GoDaddy
- DigiCert

Vous pouvez convertir votre .pem en format pfx avec des outils ou des sites en ligne. Par exemple, sur ce site : https://www.sslshopper.com/ssl-converter.html

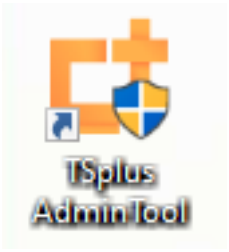
Vous pouvez utiliser ceci Outil de test de serveur SSL afin de valider la bonne qualité d'un portail web en HTTPS.

Aperçu de l'outil d'administration TSplus

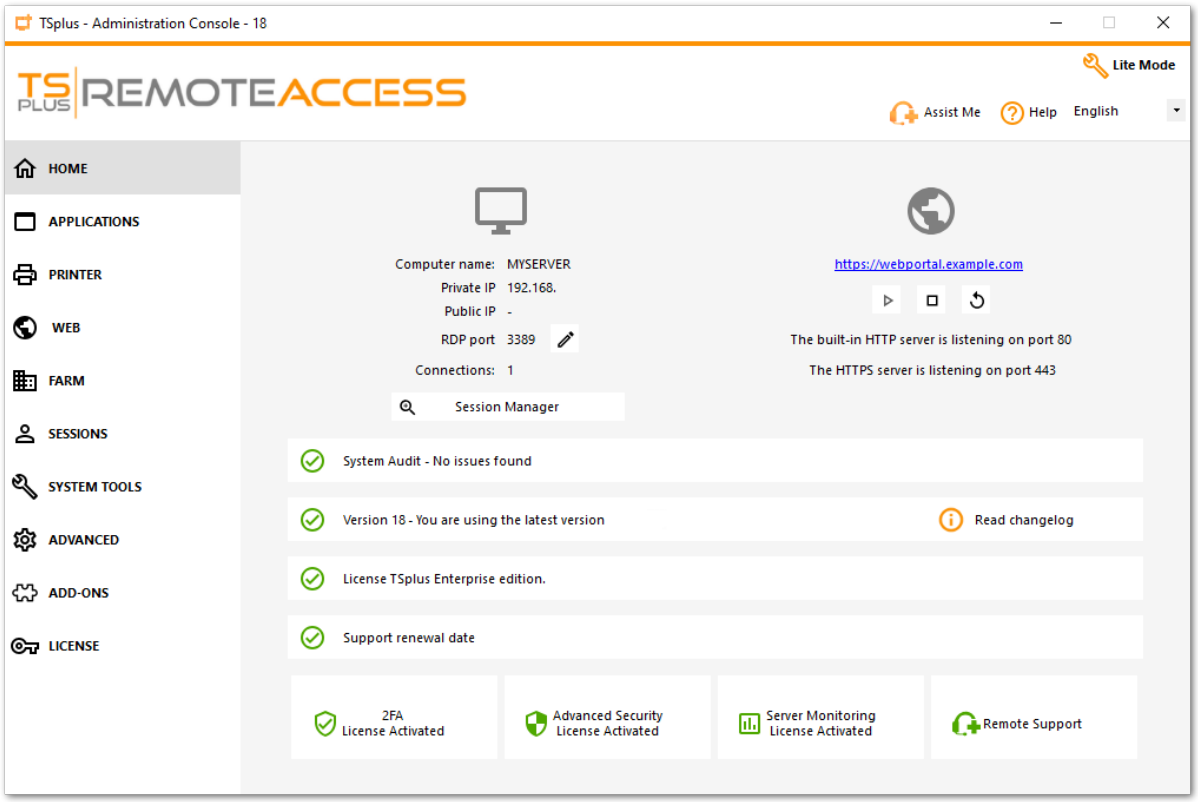
Après installer TSplus votre serveur est immédiatement prêt à fonctionner.

Cependant, vous pouvez **personnaliser tous les paramètres du système** avec un puissant outil d'administration.

Pour ce faire, cliquez sur l'icône suivante créée sur votre Bureau :



L'outil Administrateur sera alors affiché :

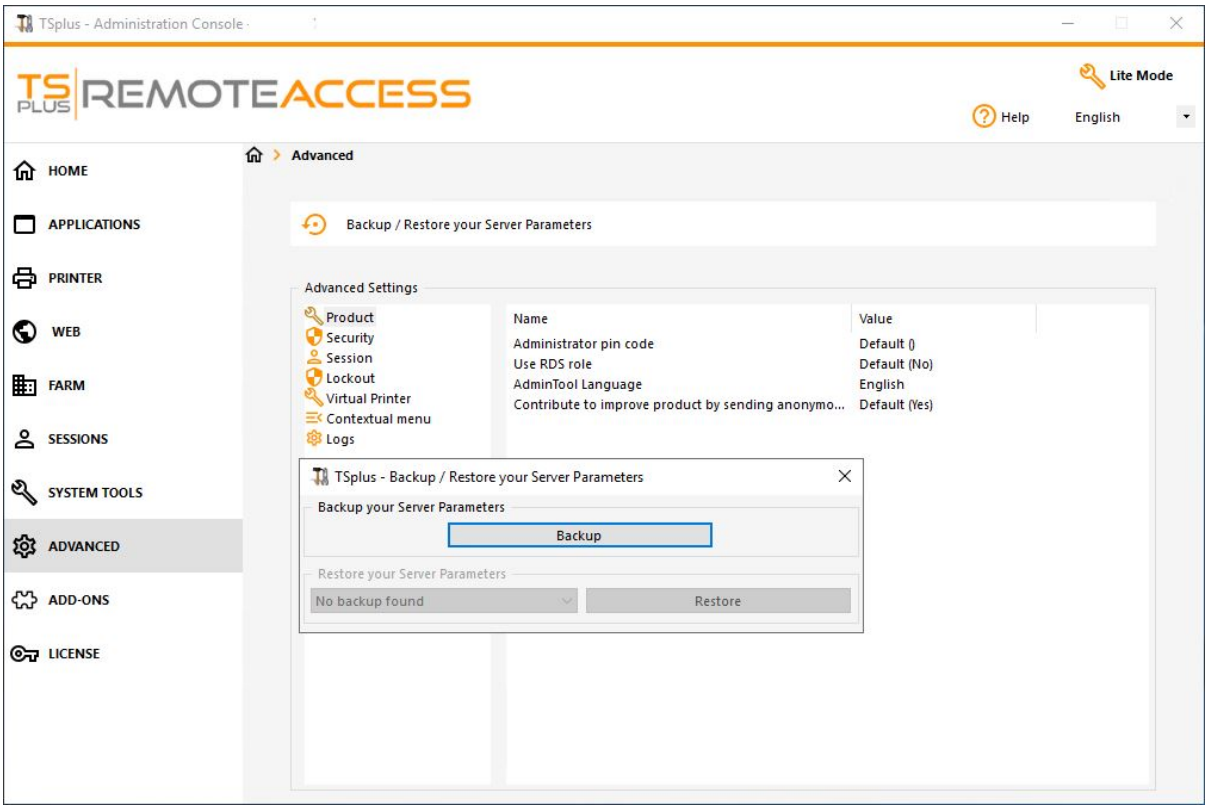


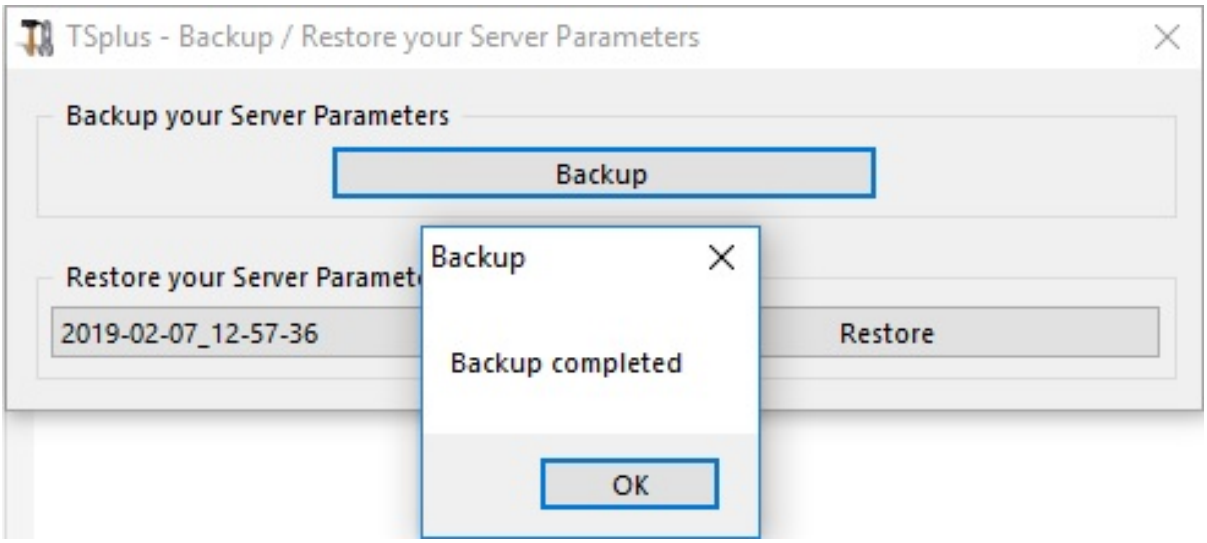
Voulez-vous obtenir de l'aide rapidement sur une fonctionnalité de TSplus Admin Tool ? Juste **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !

Sauvegarde et restauration

Depuis la version 14 dans le **Avancé** onglet, vous pouvez configurer les paramètres TSplus.

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





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

- **Sauvegarde** :

admintool.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 sécurité de TSplus. Cependant, la sauvegarde peut être enregistrée dans un dossier spécifié. Des chemins relatifs et absolus sont autorisés.

- **Restaurer** :

admintool.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.

si vous aimez utiliser des lignes de commande et vous vous demandez quelles autres lignes de commande sont disponibles, veuillez vous rendre à ceci documentation spécifique)

Veuillez suivre les étapes ci-dessous pour migrer TSplus 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 dossier C:\Backupparam.

2. Copiez le nouveau dossier de sauvegarde créé (par exemple nommé backup-2021-01-29_15-01-29), 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.

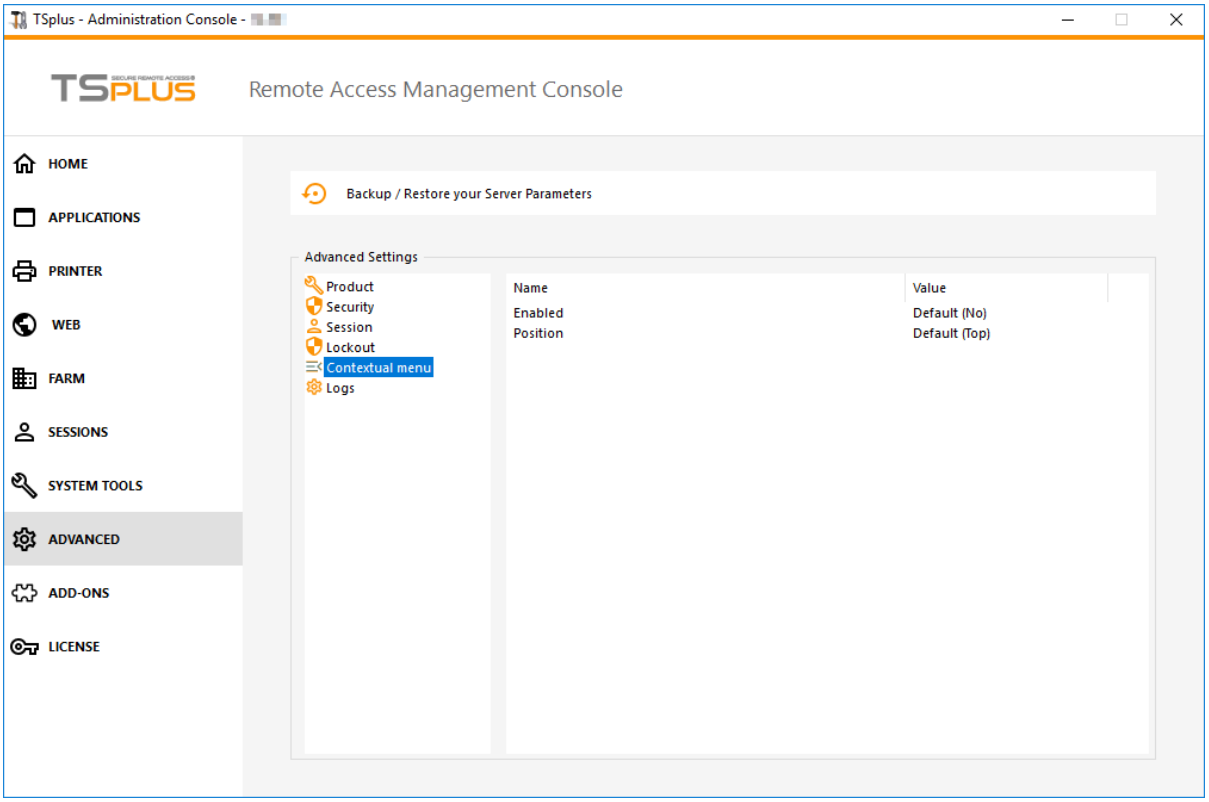
4. Ensuite, cliquez sur Restaurer uniquement les paramètres pour restaurer les paramètres. Alternativement, il est possible de cliquer sur Restaurer pour restaurer toutes les données et paramètres, ce qui n'est pas recommandé pour une migration mais utile pour restaurer TSplus sur l'ordinateur A.

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

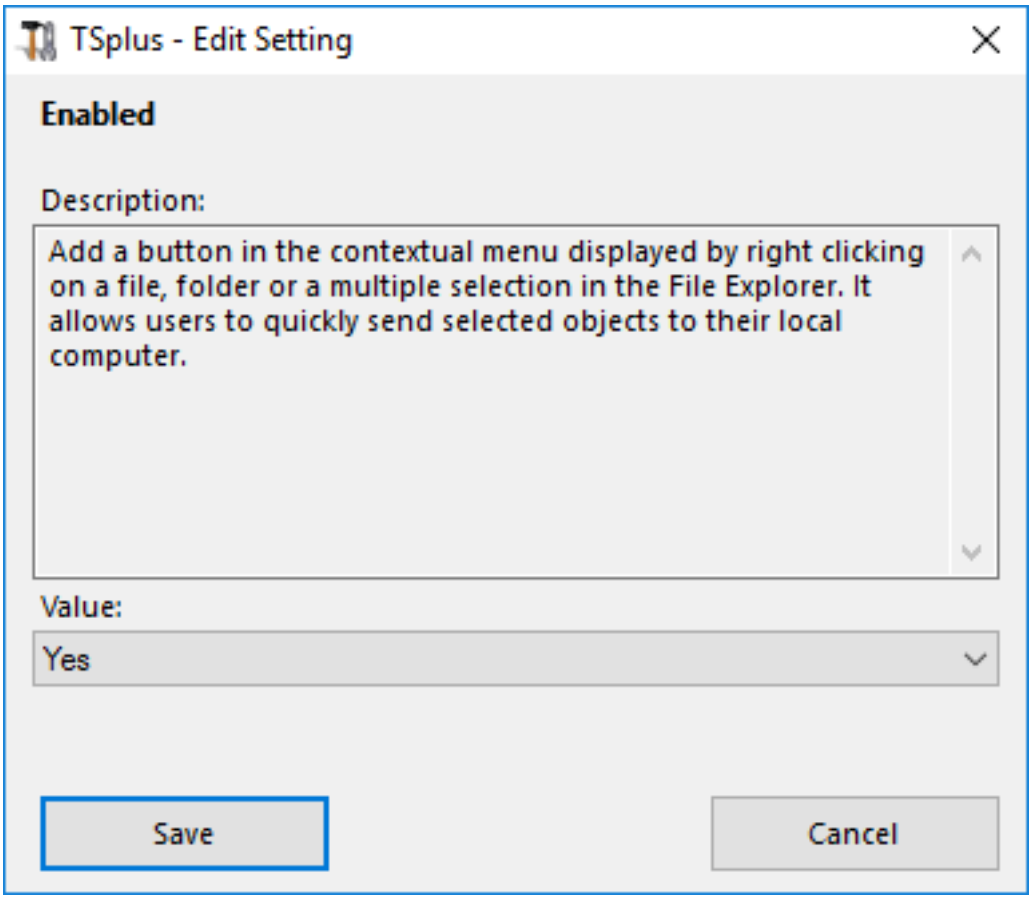
Fonctionnalités avancées - Menu contextuel

Aperçu

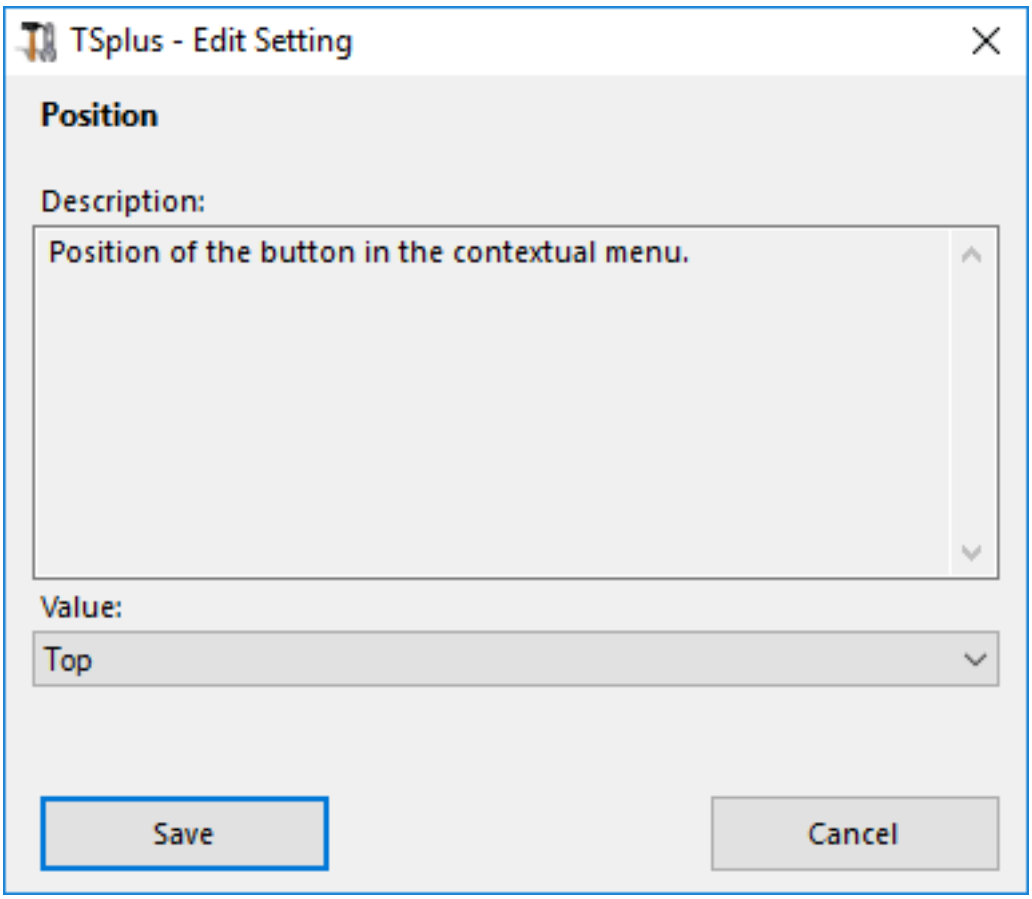
Depuis la version 12.50 de TSplus, un nouveau **Menu "Envoyer au client"** peut être activé sous l'onglet Avancé > Menu contextuel pour envoyer facilement des fichiers à la station de travail du client. Cette fonctionnalité fonctionne avec tous les modes de connexion.



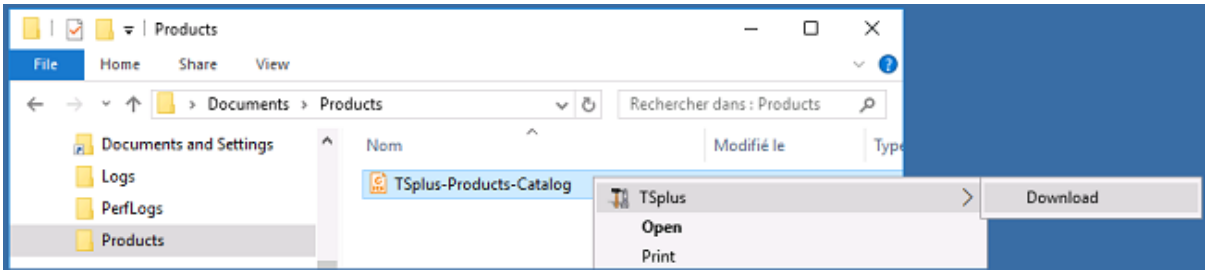
Par défaut, cette fonctionnalité est désactivée. Sélectionnez la valeur « Oui », puis cliquez sur « Enregistrer » pour l'activer :



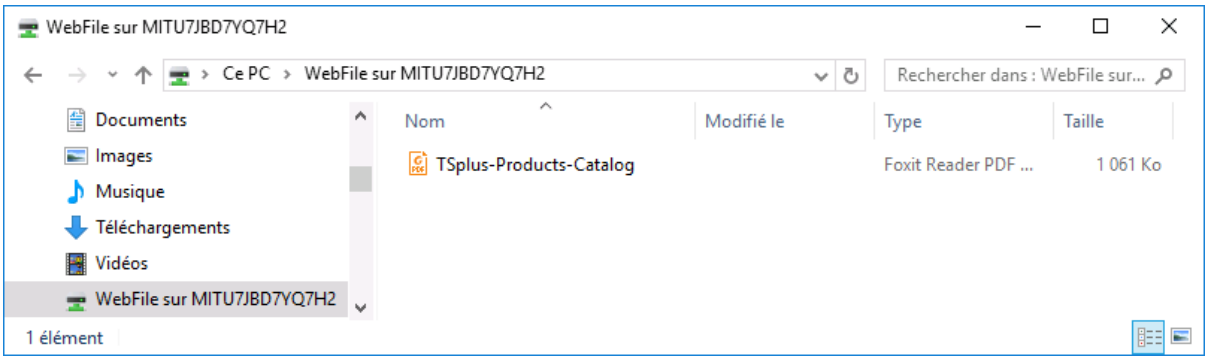
Vous pouvez également changer sa position. Par défaut, il s'affichera en haut :



Ceci est un menu contextuel accessible par un clic droit. Il suffit de sélectionner le dossier ou les fichiers souhaités, de faire un clic droit dessus, de sélectionner l'onglet “TSplus” et de cliquer simplement sur “Télécharger”.



Vous trouverez votre téléchargement dans le dossier Webfile et dans le dossier « Téléchargements » de votre navigateur web :

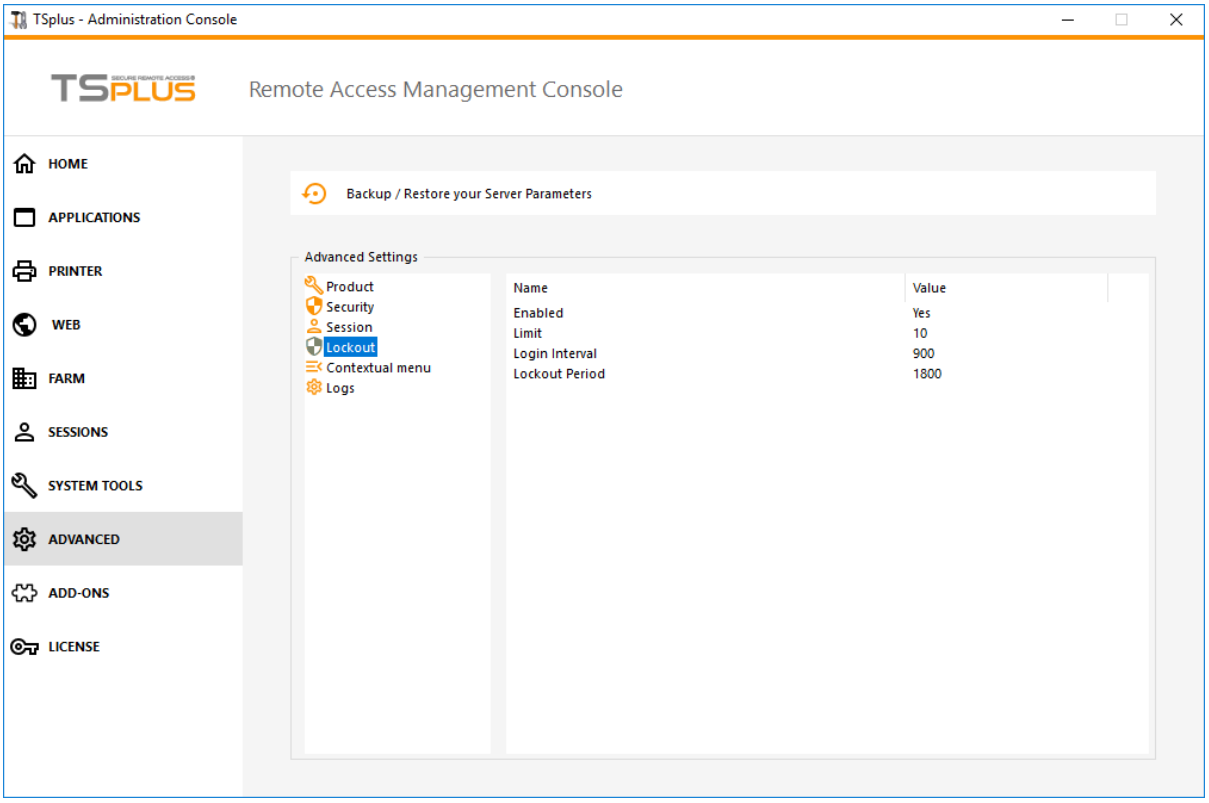


Chaque dossier téléchargé est automatiquement compressé en un fichier zip.

Fonctionnalités avancées - Verrouillage

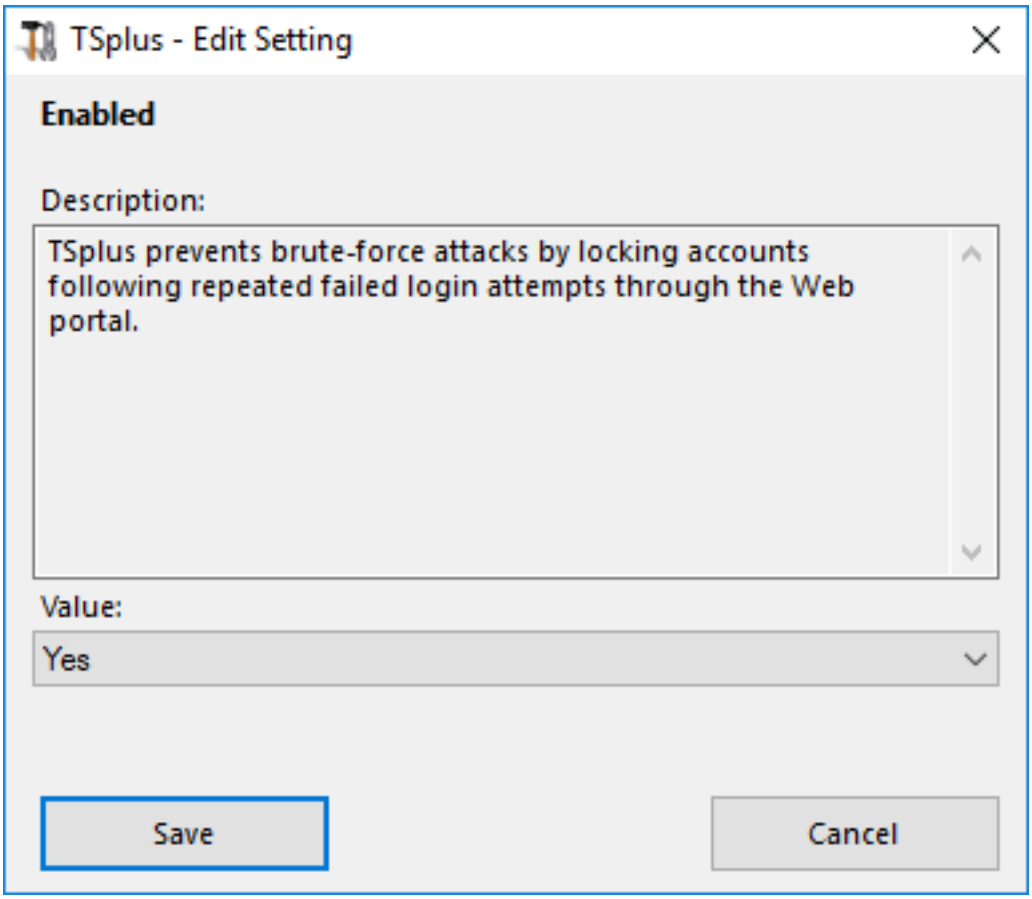
Aperçu

Sur cet onglet, vous pouvez activer/désactiver et configurer TSplus Lockout paramètres.



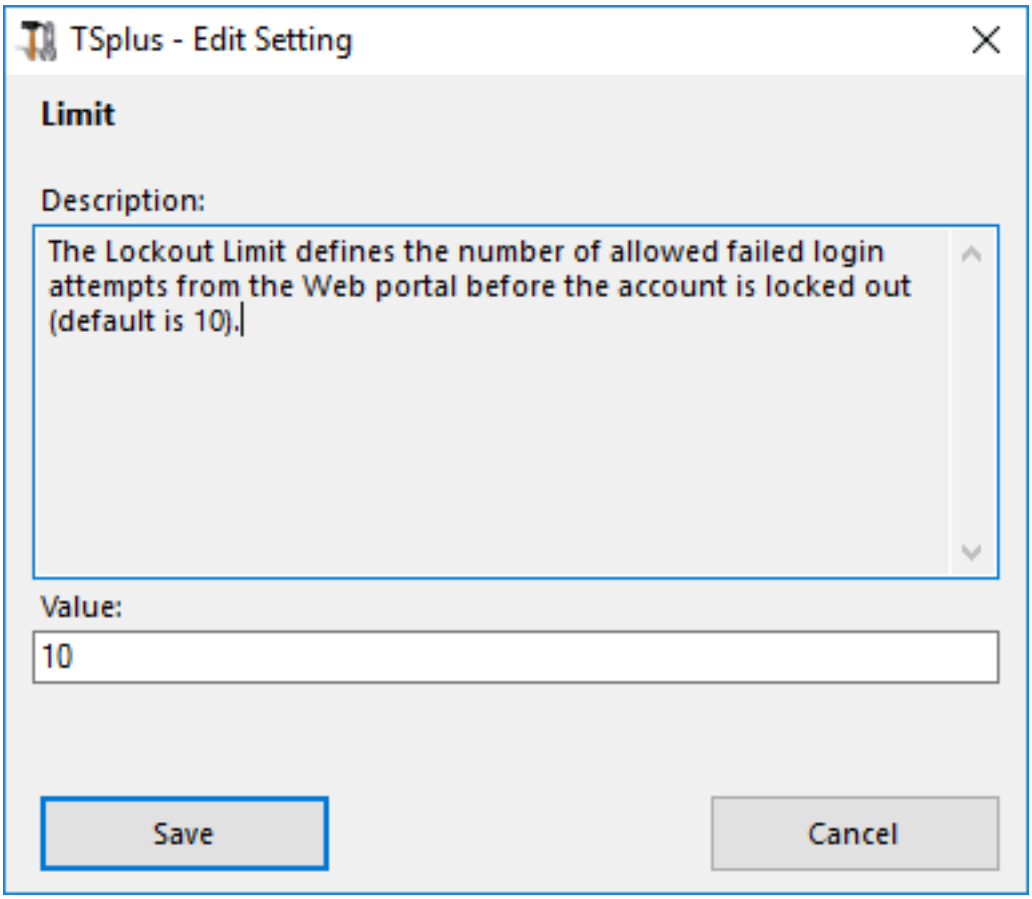
Activer/Désactiver la fonction de verrouillage

La fonction de verrouillage est activée par défaut. Vous pouvez la désactiver en changeant la valeur de « Oui » à « Non » dans cette fenêtre, puis cliquez sur enregistrer.



Limite

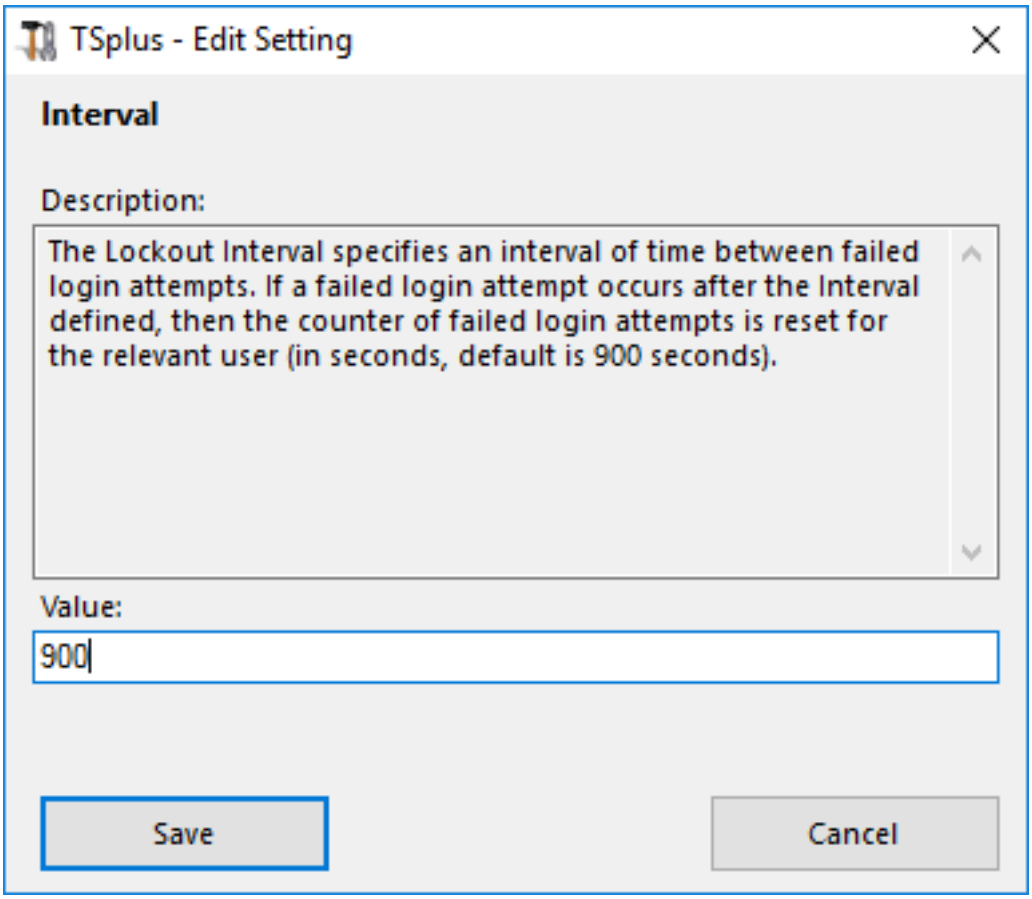
La limite de verrouillage définit le nombre de tentatives de connexion échouées autorisées depuis le portail Web avant que le compte ne soit verrouillé (la valeur par défaut est 10). Vous pouvez modifier cette valeur en saisissant la valeur souhaitée dans le champ correspondant et en cliquant sur enregistrer.



Interval

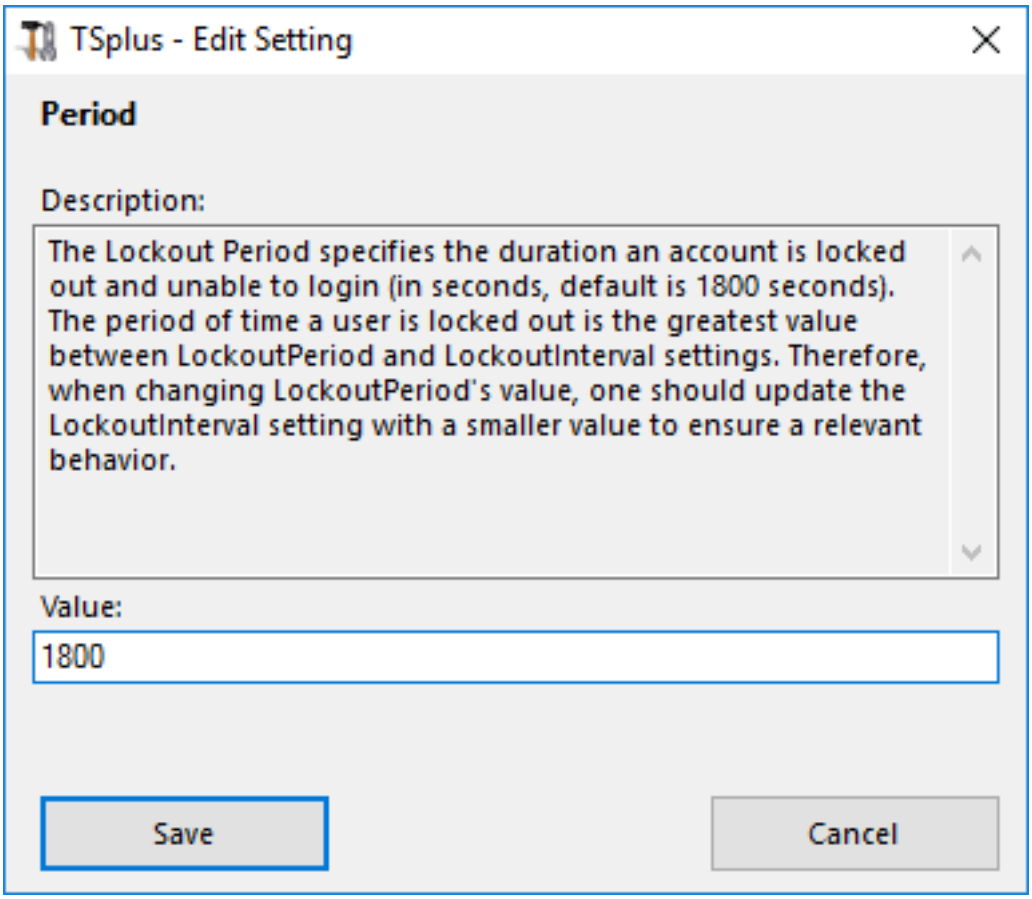
L'intervalle de verrouillage spécifie un intervalle de temps entre les tentatives de connexion échouées.

Si une tentative de connexion échouée se produit après l'intervalle défini, alors le compteur des tentatives de connexion échouées est réinitialisé pour l'utilisateur concerné (en secondes, la valeur par défaut est de 900 secondes). Vous pouvez modifier cette valeur en saisissant la valeur souhaitée dans le champ correspondant et en cliquant sur enregistrer.



Période

La période de verrouillage spécifie la durée pendant laquelle un compte est verrouillé et incapable de se connecter (en secondes, la valeur par défaut est de 1800 secondes). La période pendant laquelle un utilisateur est verrouillé est la plus grande valeur entre les paramètres LockoutPeriod et LockoutInterval. Par conséquent, lors de la modification de la valeur de LockoutPeriod, il convient de mettre à jour le paramètre LockoutInterval avec une valeur plus petite pour garantir un comportement pertinent. Vous pouvez modifier cette valeur en saisissant la valeur souhaitée dans le champ correspondant et en cliquant sur enregistrer.


TSplus - Edit Setting
Period
Description:
The Lockout Period specifies the duration an account is locked out and unable to login (in seconds, default is 1800 seconds). The period of time a user is locked out is the greatest value between LockoutPeriod and LockoutInterval settings. Therefore, when changing LockoutPeriod's value, one should update the LockoutInterval setting with a smaller value to ensure a relevant behavior.
Value:
1800
Save
Cancel

Fonctionnalités avancées - Journaux

Aperçu

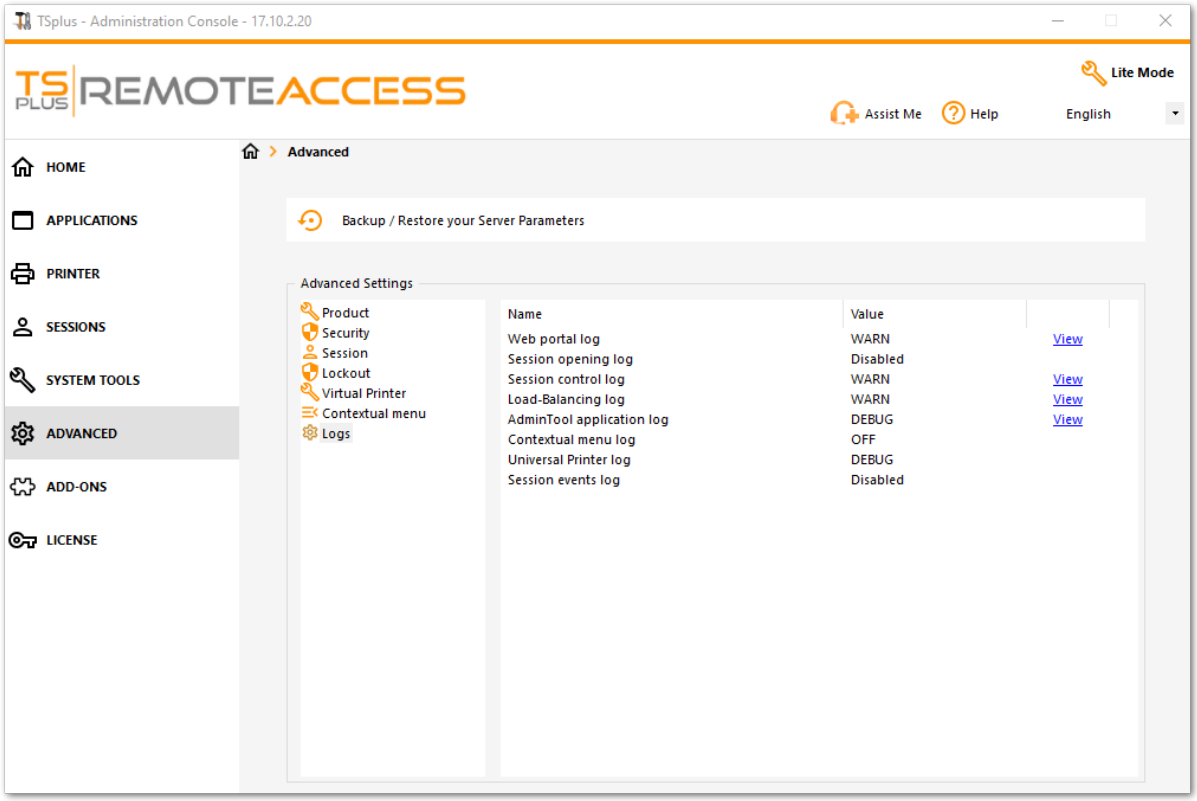
Sur cet onglet, vous pouvez configurer les paramètres des journaux TSplus.

Par défaut, TSplus ne crée pas de journaux, afin d'éviter des problèmes de performance.

Des journaux existent pour trouver plus facilement l'origine des erreurs rencontrées sur TSplus et vous pouvez les activer en procédant comme suit :

- aller à C:\wsession
- créez le dossier 'Trace'. Les journaux y seront automatiquement créés, par utilisateur.

Vous devrez activer la génération de journaux dans l'AdminTool > Avancé > Journaux.



Il existe 5 types de journaux :

- Le journal du portail Web,
- Le journal d'ouverture de session,
- Le journal de contrôle de session,
- Le journal de répartition de charge et
- L'application AdminTool (interface) journal.

Les niveaux de journalisation correspondent à différents composants, notre équipe de support vous indiquera quelle valeur mettre en fonction du problème rencontré.

Voici les différents noms et emplacements des fichiers journaux :

- Web Portal log : “C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\hb.log”

- Journal d'ouverture de session : “C:\wsession\trace”
- Journal de contrôle de session : “C:\Program Files (x86)\TSplus\UserDesktop\files\APSC.log”
- Journal de répartition de charge : “C:\Program Files (x86)\TSplus\UserDesktop\files\svcenterprise.log”
- AdminTool application log : “C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.log”
- RDS-Knight / TSplus Advanced Security : “C:\Program Files (x86)\TSplus-Security\logs”

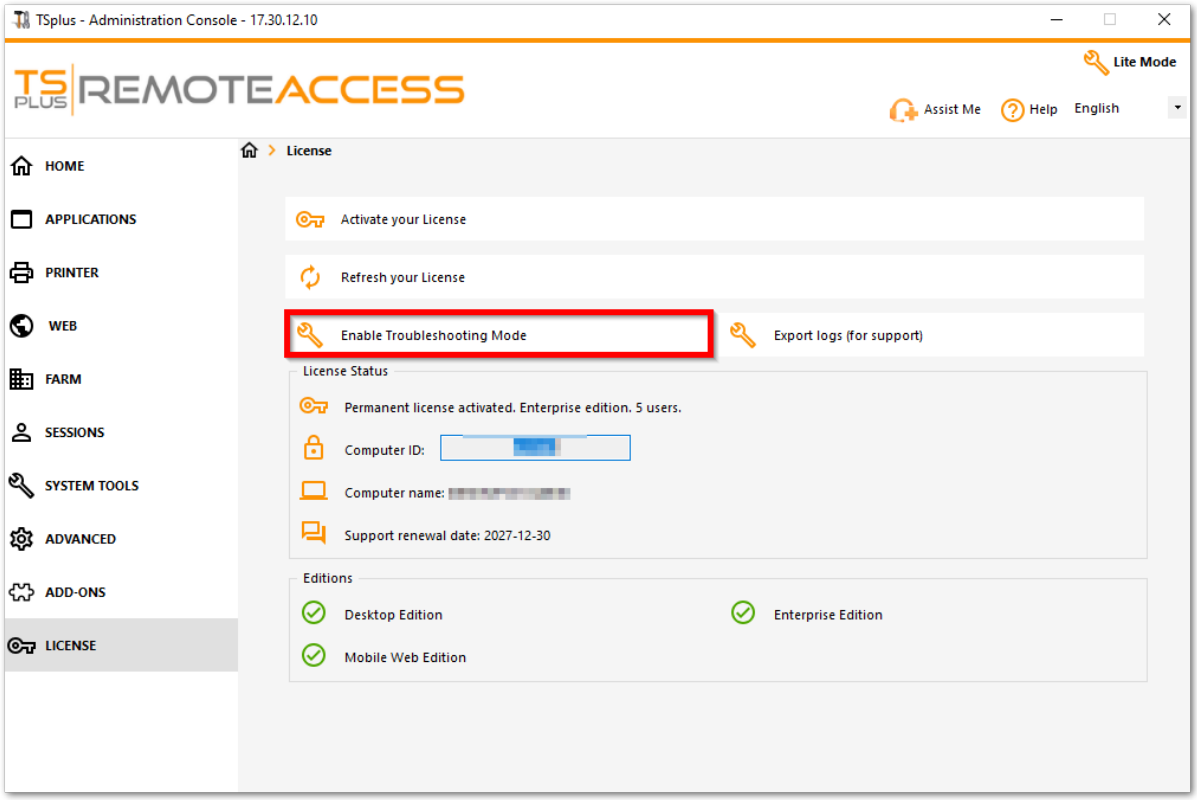
Vous pouvez activer les journaux pour le Client de Connexion du côté client en ajoutant la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\ConnectionClient “Debug”=“true”

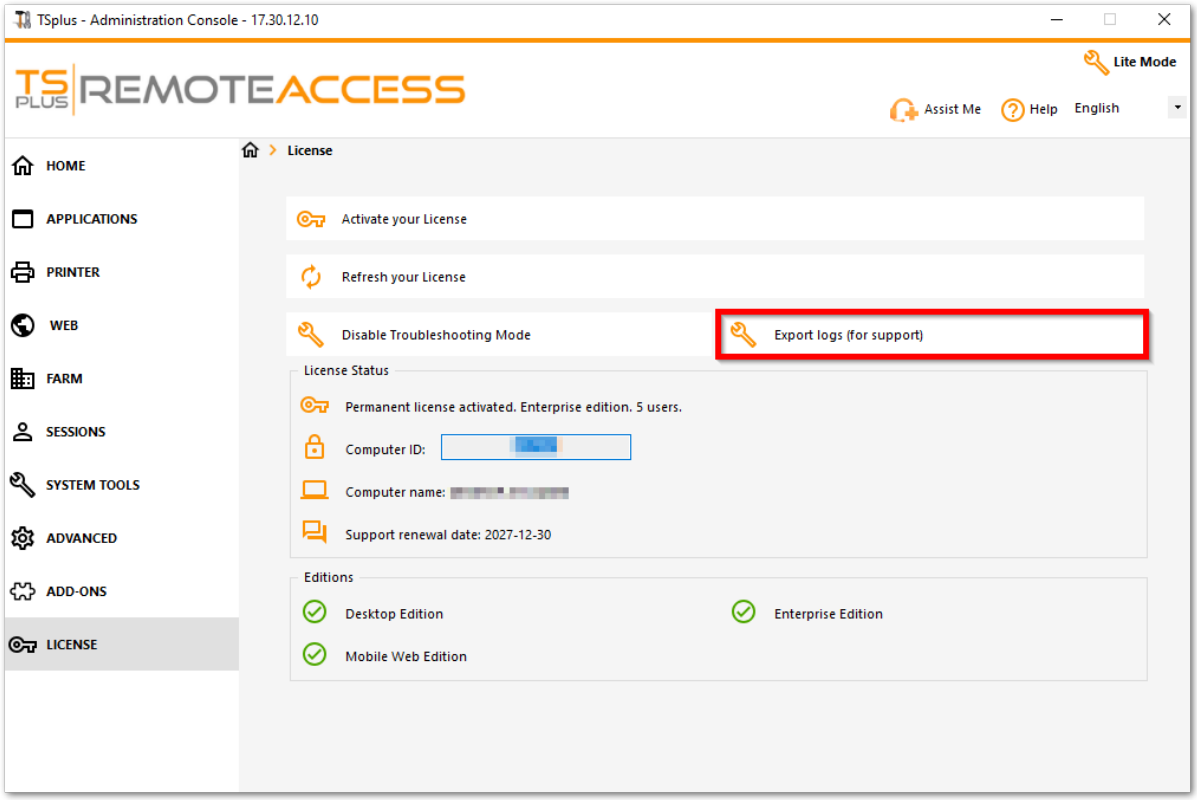
Les journaux sont situés dans C:\Users Répertoire RDP6\logs si l'installation est par utilisateur ou dans C:\Program Files (x86)\Connection Client\RDP6\logs si l'installation est pour tous les utilisateurs.

Activer le mode de dépannage

Allez à l'onglet « Licence » Cliquez sur le **Activer le mode de dépannage** bouton.



Reproduisez votre problème, puis cliquez sur le **Exporter des journaux (pour le support)** bouton pour envoyer les journaux à l'équipe de support par e-mail.



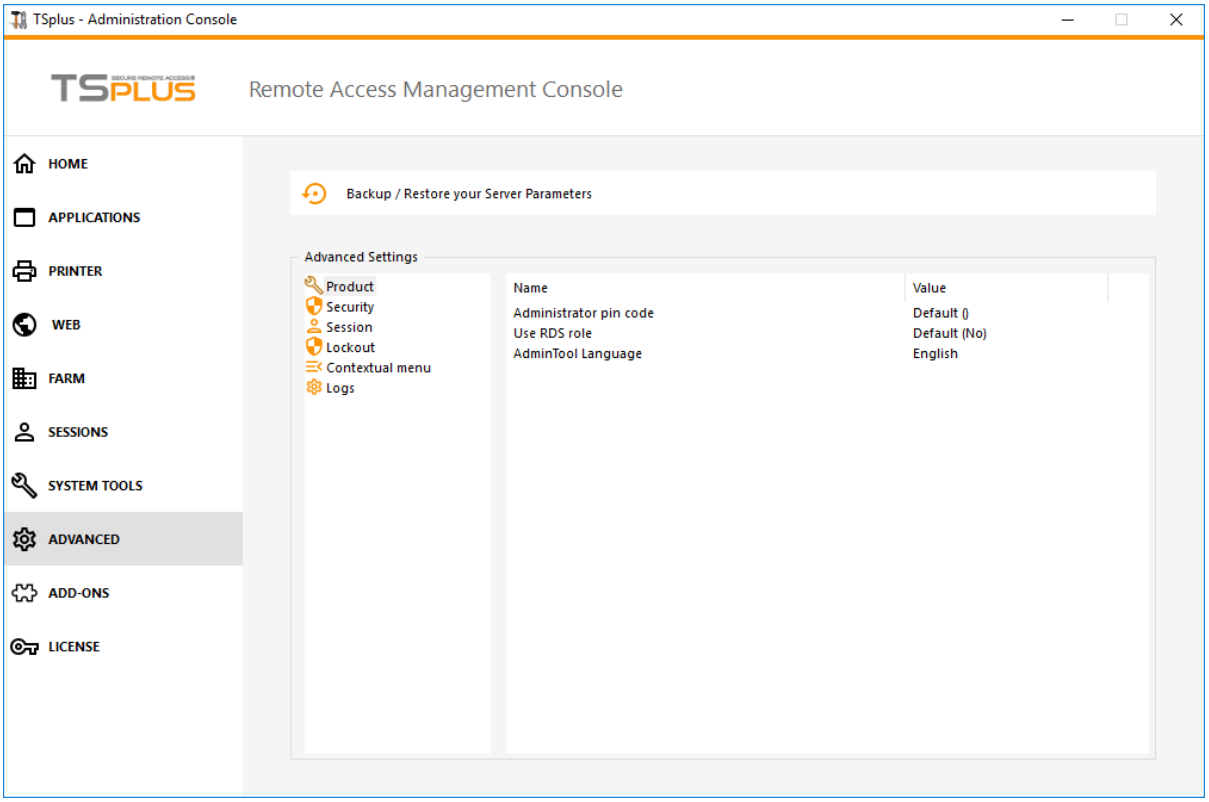


Le format du fichier à envoyer est **.zip.logs** fichiers et est protégé par le mot de passe **mot de passe** .

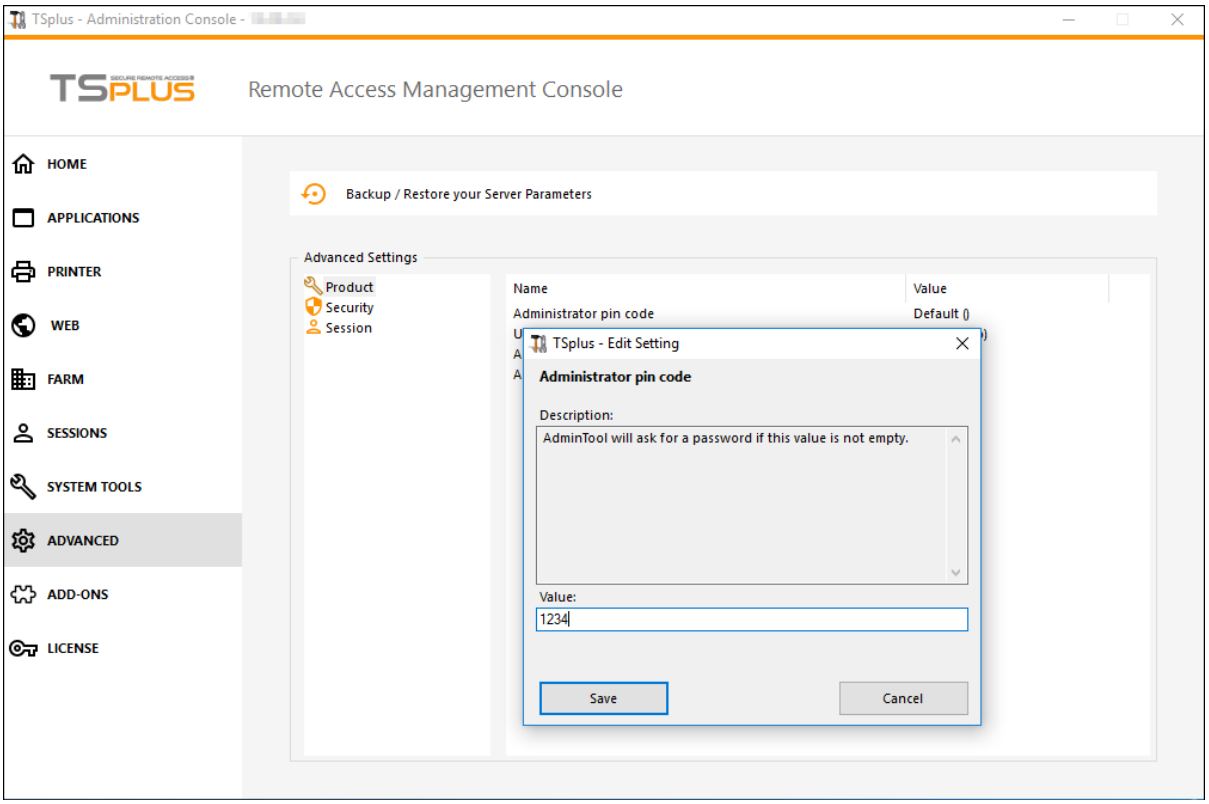
Fonctionnalités Avancées - Produit

Aperçu

Sur cet onglet, vous pouvez modifier les paramètres de TSplus en ajoutant un code PIN AdminTool, en utilisant le rôle RDS de Windows et en personnalisant la couleur de fond et la langue de l'AdminTool.



L'administrateur peut sécuriser l'accès à l'outil d'administration en définissant un code PIN qui sera demandé à chaque démarrage, dans l'onglet Avancé de l'AdminTool, sous les paramètres du produit :

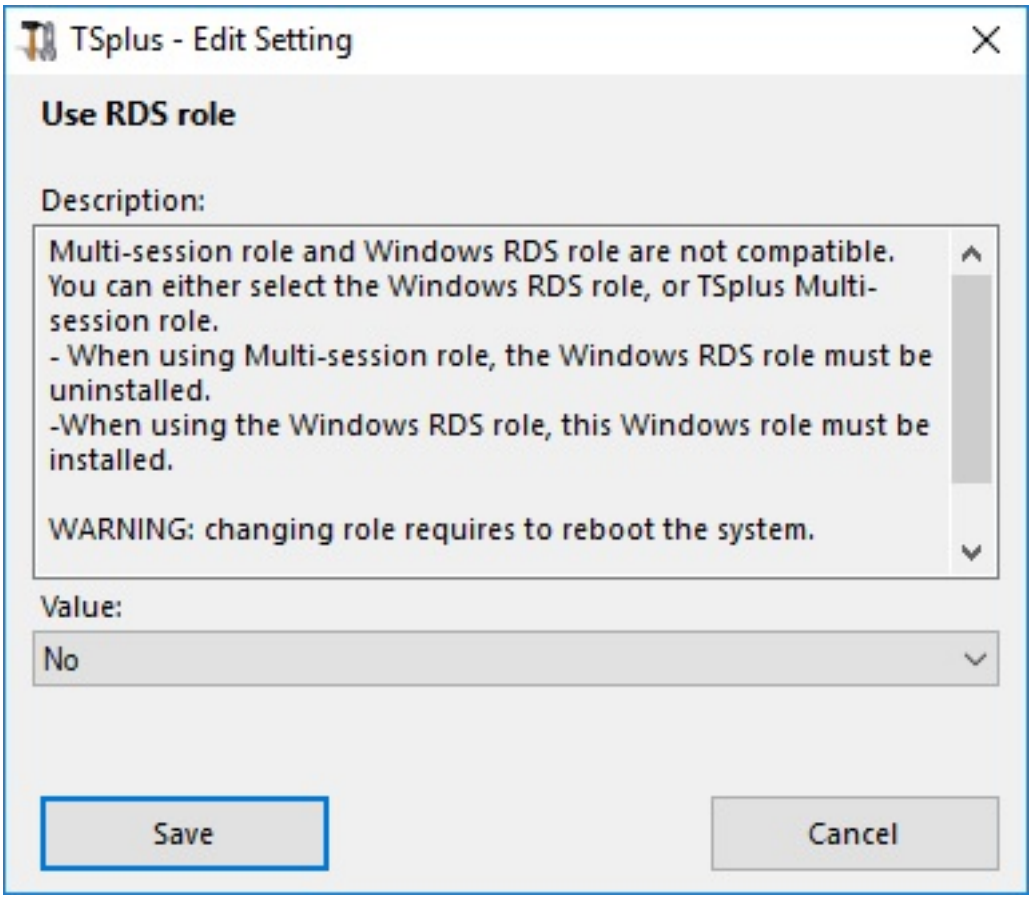


Utiliser le rôle RDS

Le rôle multi-session et le rôle Windows RDS ne sont pas compatibles. Vous pouvez soit sélectionner le rôle Windows RDS, soit le rôle multi-session TSplus.

- Lors de l'utilisation du rôle Multi-session, le rôle RDS de Windows doit être désinstallé.
- Lors de l'utilisation du rôle RDS de Windows, ce rôle Windows doit être installé.

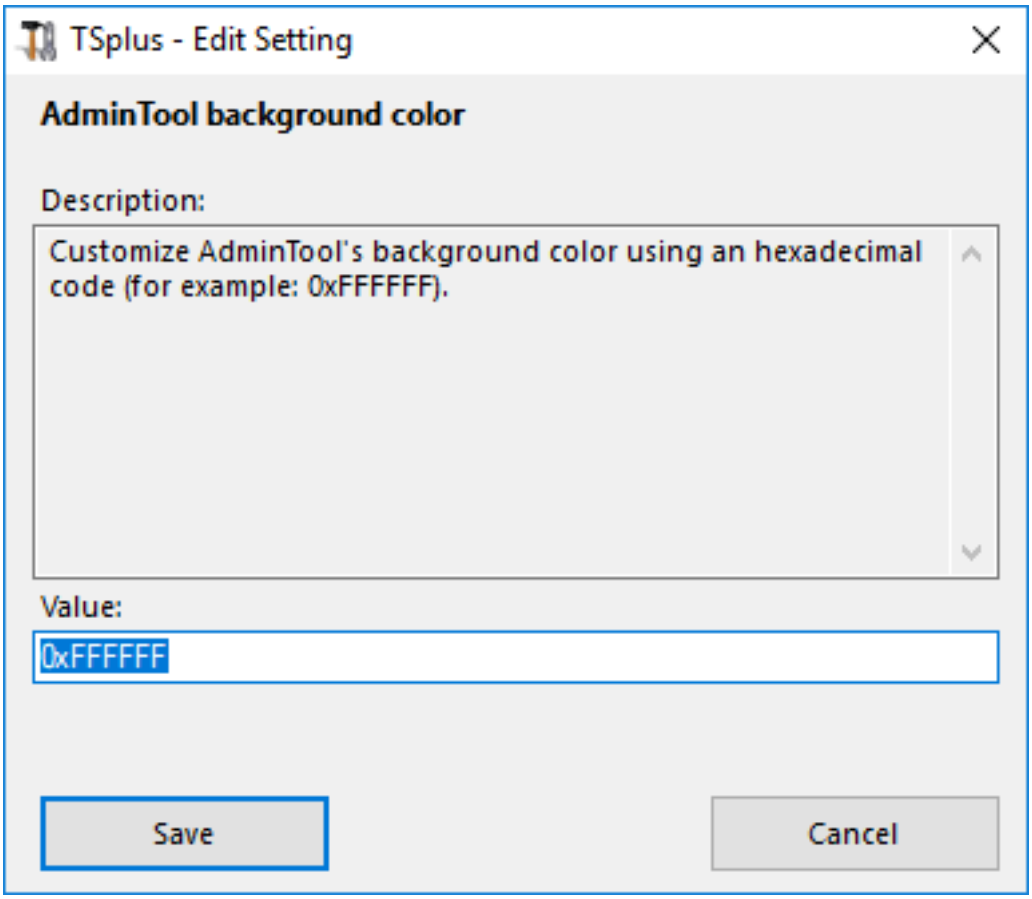
AVERTISSEMENT Changer de rôle nécessite de redémarrer le système. Lors de la sélection de Windows Remote Desktop, un seul utilisateur à la fois sera autorisé sur un système de poste de travail.



Pour utiliser le rôle RDS de Windows, sélectionnez la valeur « Oui » et enregistrez.

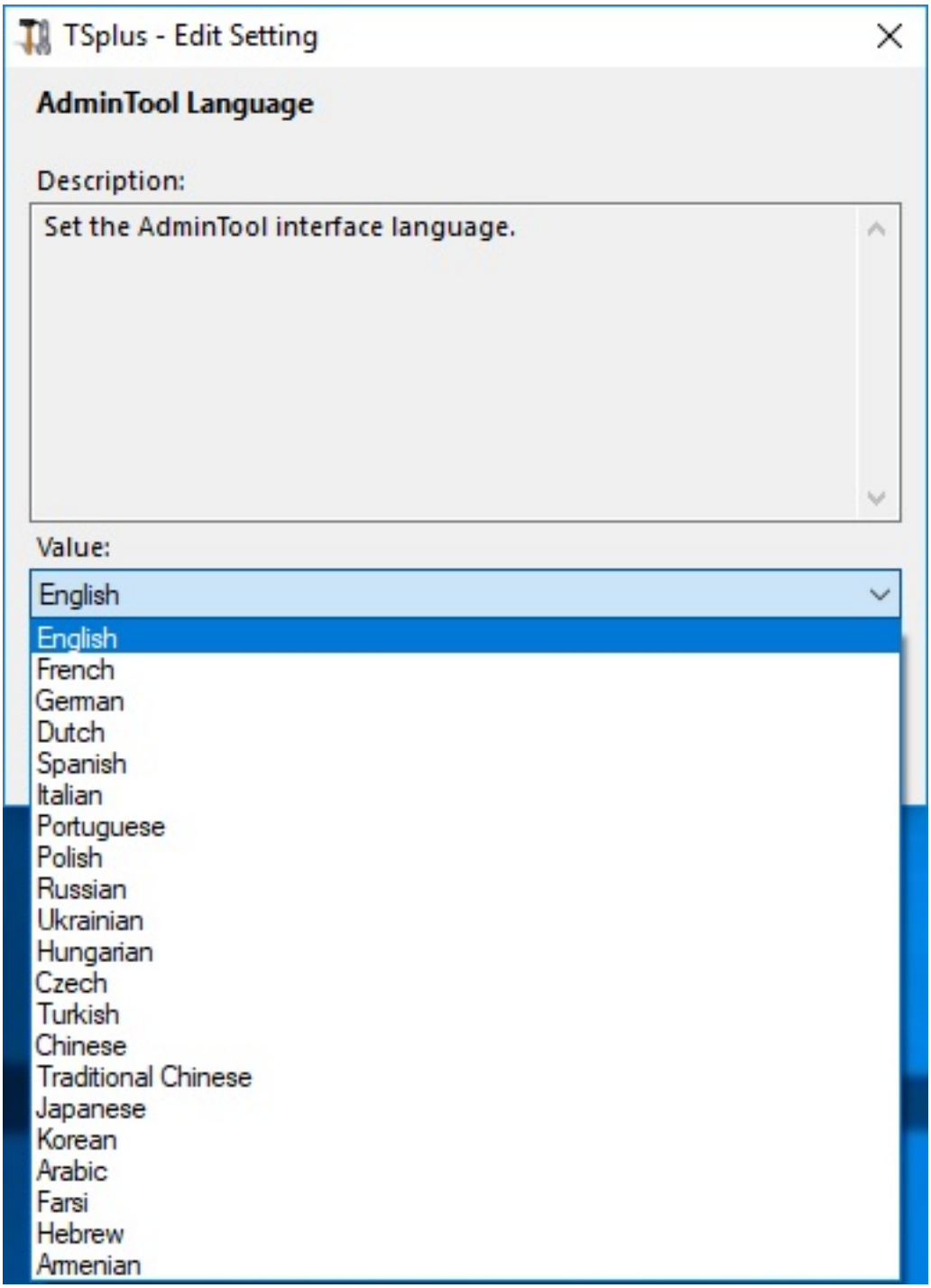
Modifier la couleur de fond de l'AdminTool

Personnalisez la couleur de fond de l'AdminTool en utilisant un code hexadécimal (par exemple : 0xFFFFFF).



Modifier la langue de l'AdminTool

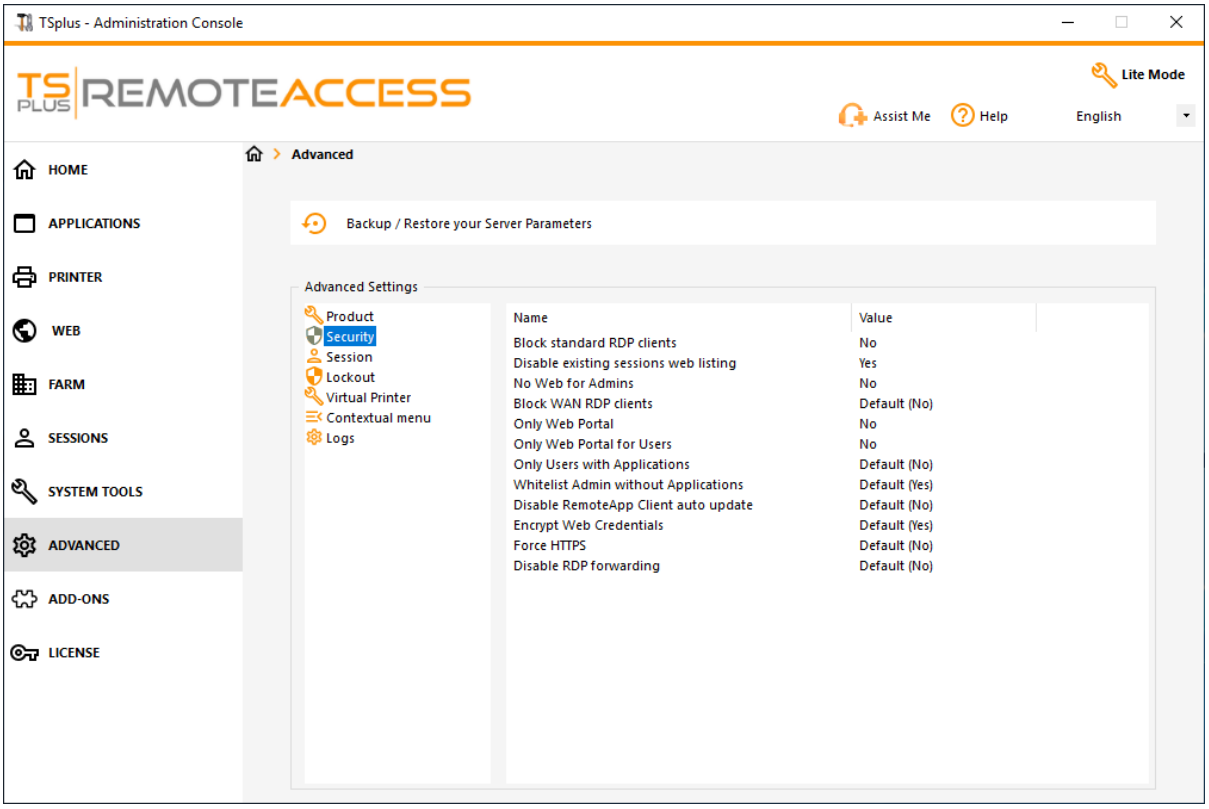
Sélectionnez votre langue préférée pour l'AdminTool parmi les 21 disponibles.


TSplus - Edit Setting
AdminTool Language
Description:
Set the AdminTool interface language.
Value:
English
English
French
German
Dutch
Spanish
Italian
Portuguese
Polish
Russian
Ukrainian
Hungarian
Czech
Turkish
Chinese
Traditional Chinese
Japanese
Korean
Arabic
Farsi
Hebrew
Armenian

Fonctionnalités avancées - Sécurité

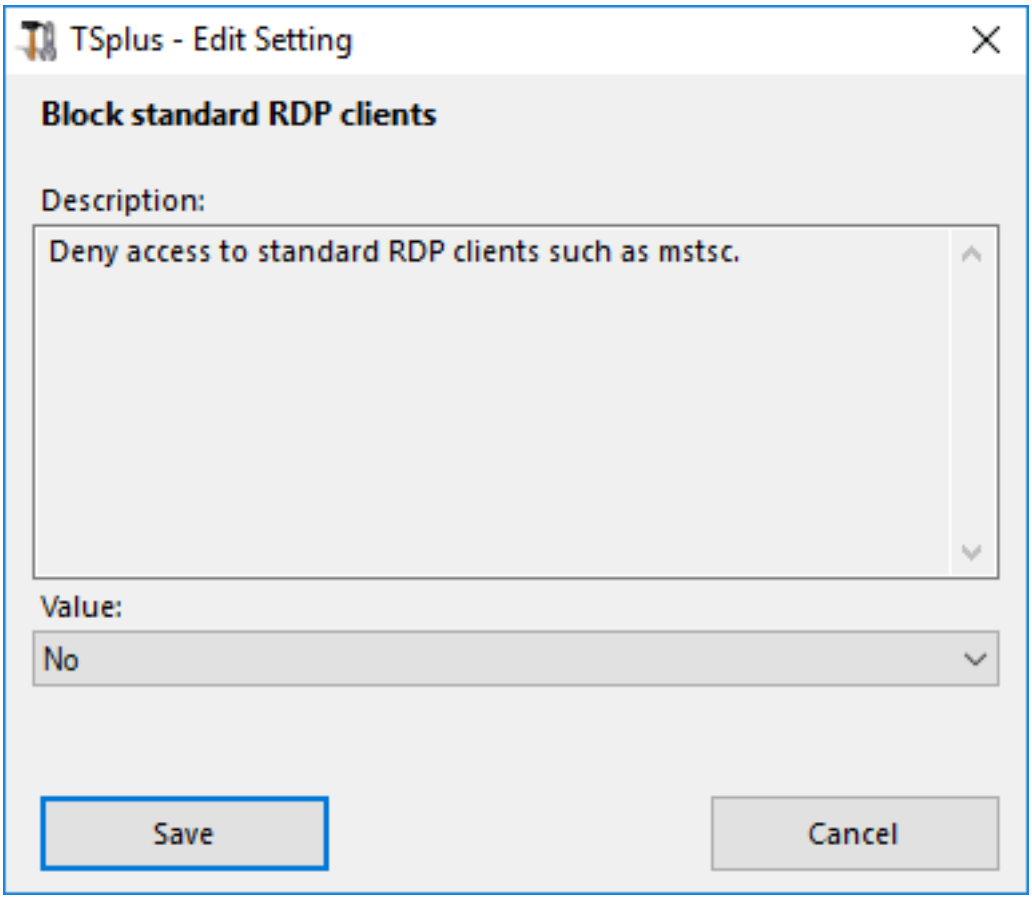
Aperçu

Dans la section Sécurité des fonctionnalités avancées, vous pouvez bloquer, désactiver ou personnaliser les types de connexion pour les utilisateurs.



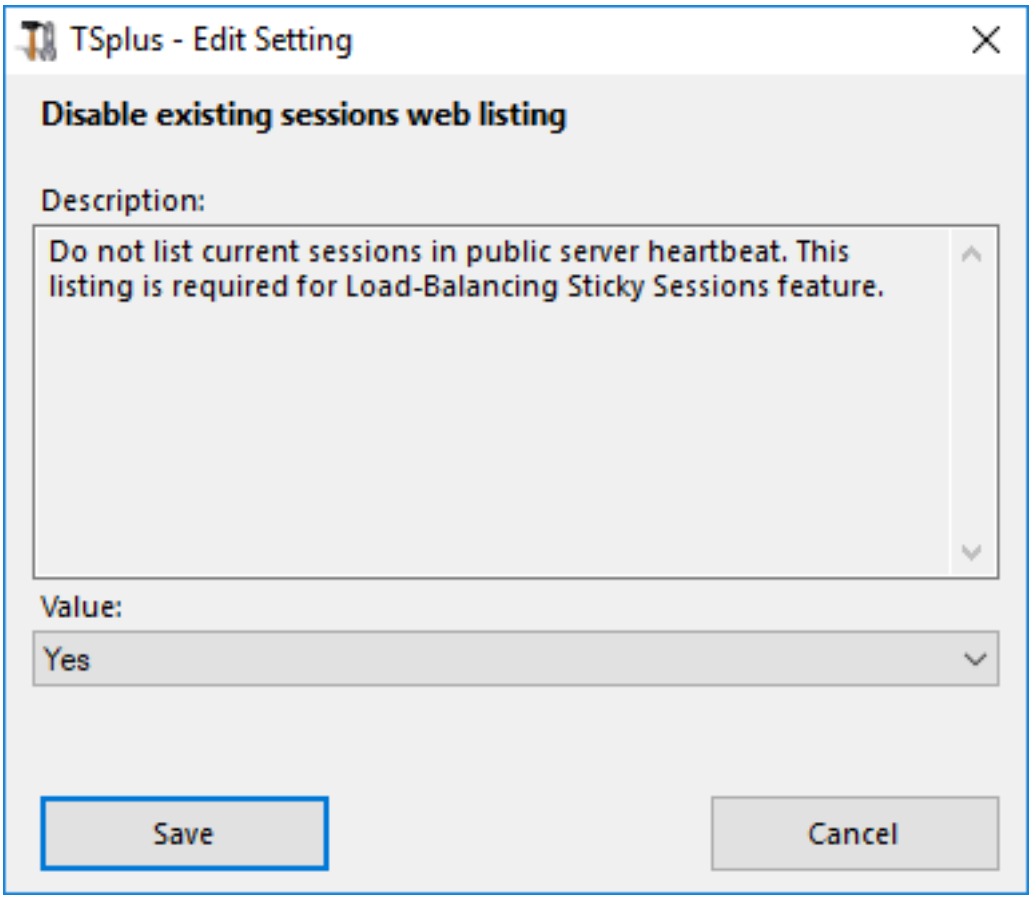
Bloquer les clients RDP standard

Sélectionnez la valeur « Oui » si vous souhaitez refuser l'accès aux clients RDP standard tels que mstsc pour vos utilisateurs.



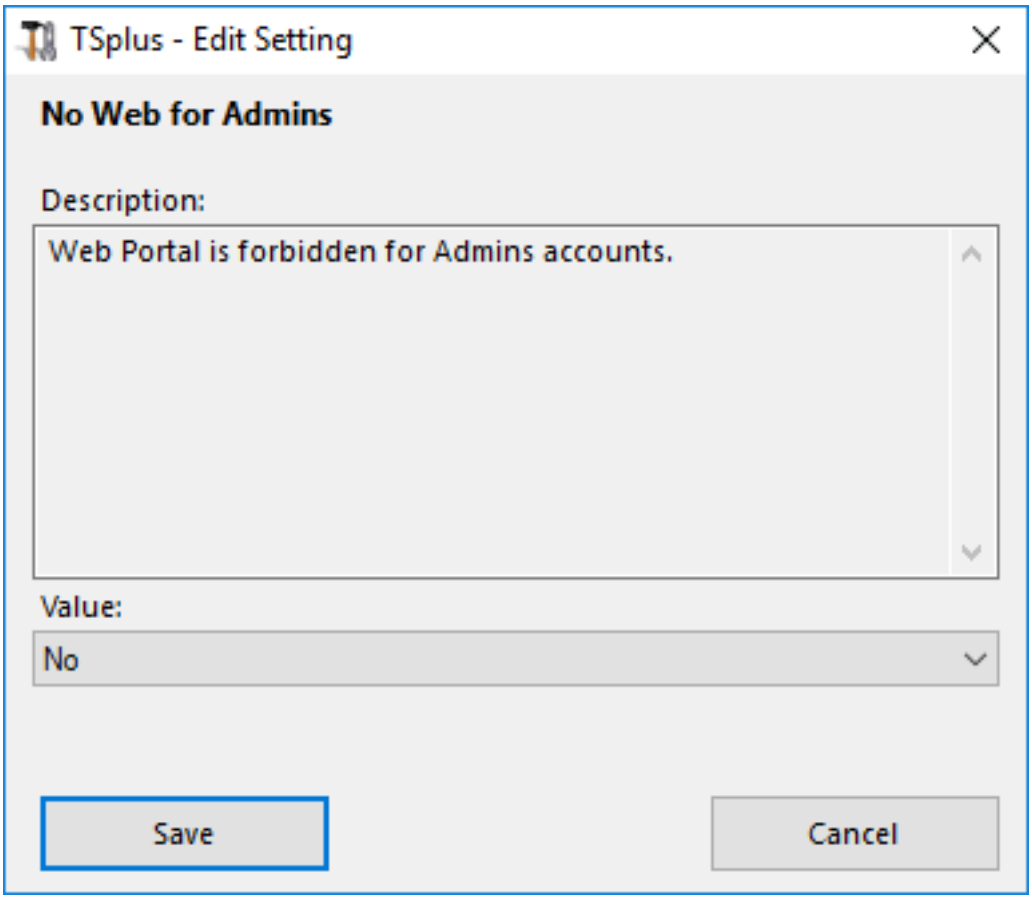
Désactiver la liste des sessions existantes sur le web

Cette liste est requise pour la fonctionnalité de sessions collantes de répartition de charge et est activée par défaut. Si vous souhaitez la désactiver, sélectionnez la valeur « Non » dans cette fenêtre, puis cliquez sur enregistrer :



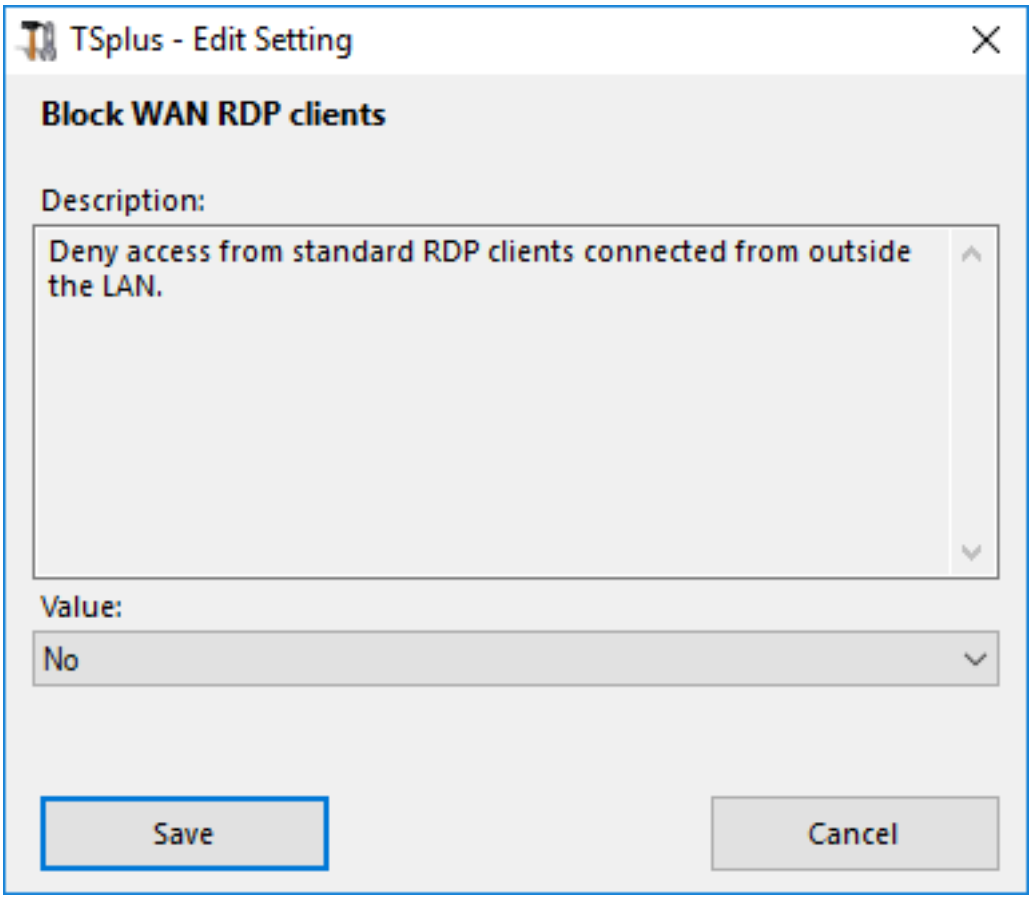
Pas de Web pour les administrateurs

Désactiver le portail Web pour les administrateurs en sélectionnant la valeur « Oui » :



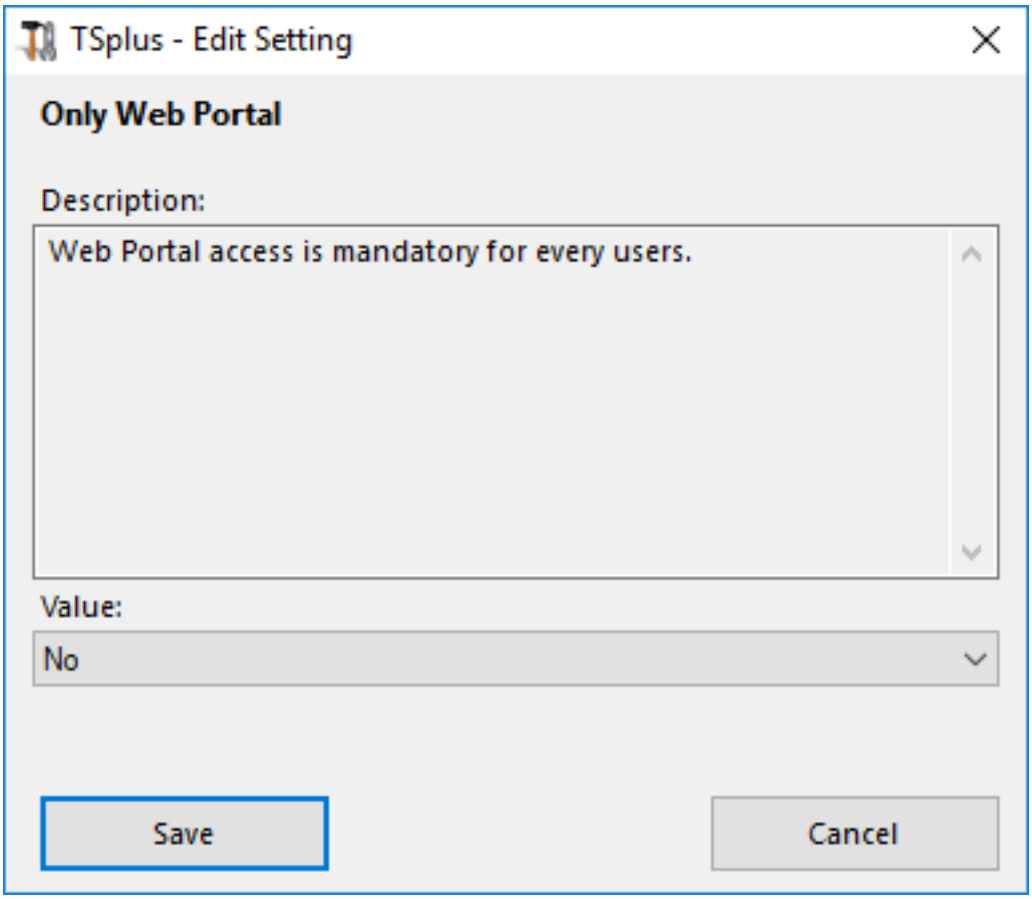
Bloquer les clients RDP WAN

Refuser l'accès aux clients RDP standard connectés depuis l'extérieur du LAN en sélectionnant la valeur « Oui ».



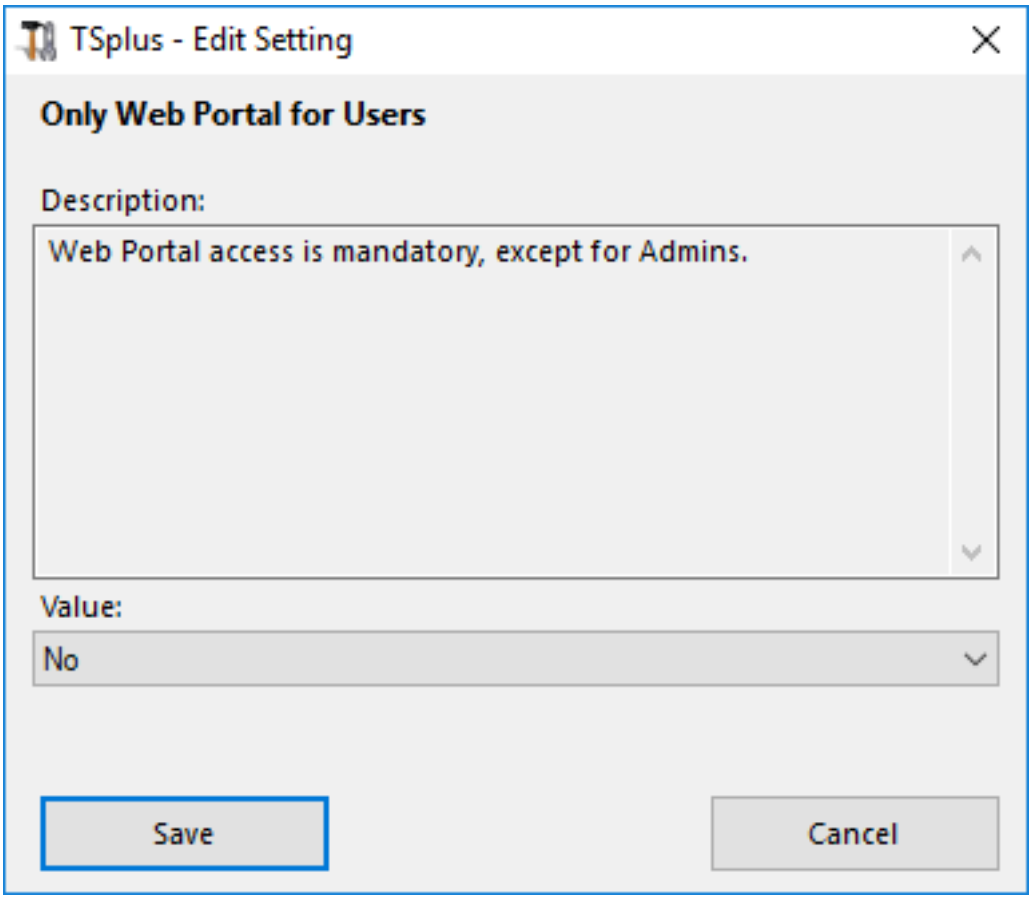
Seulement portail Web

Rendre l'accès au portail Web obligatoire pour chaque utilisateur en sélectionnant la valeur « oui ».



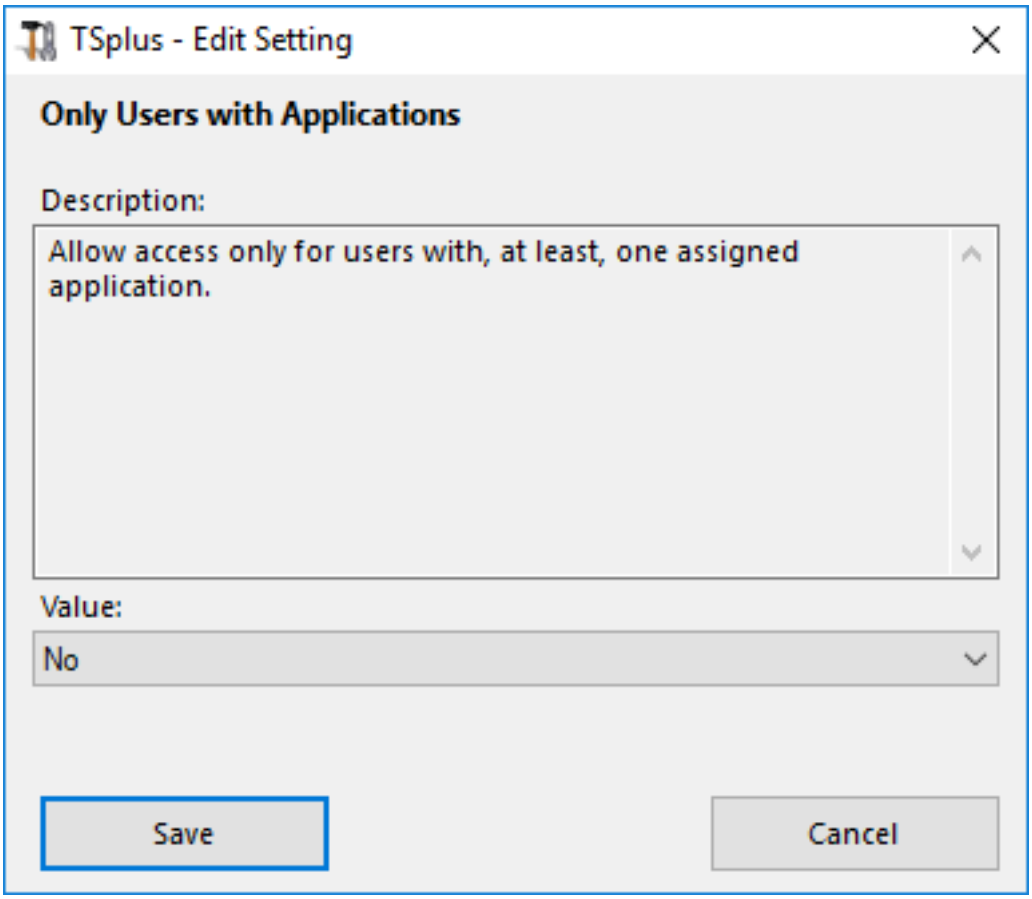
Seulement le portail Web pour les utilisateurs

Rendre l'accès au portail Web obligatoire pour chaque utilisateur, sauf les administrateurs, en sélectionnant la valeur « oui ».



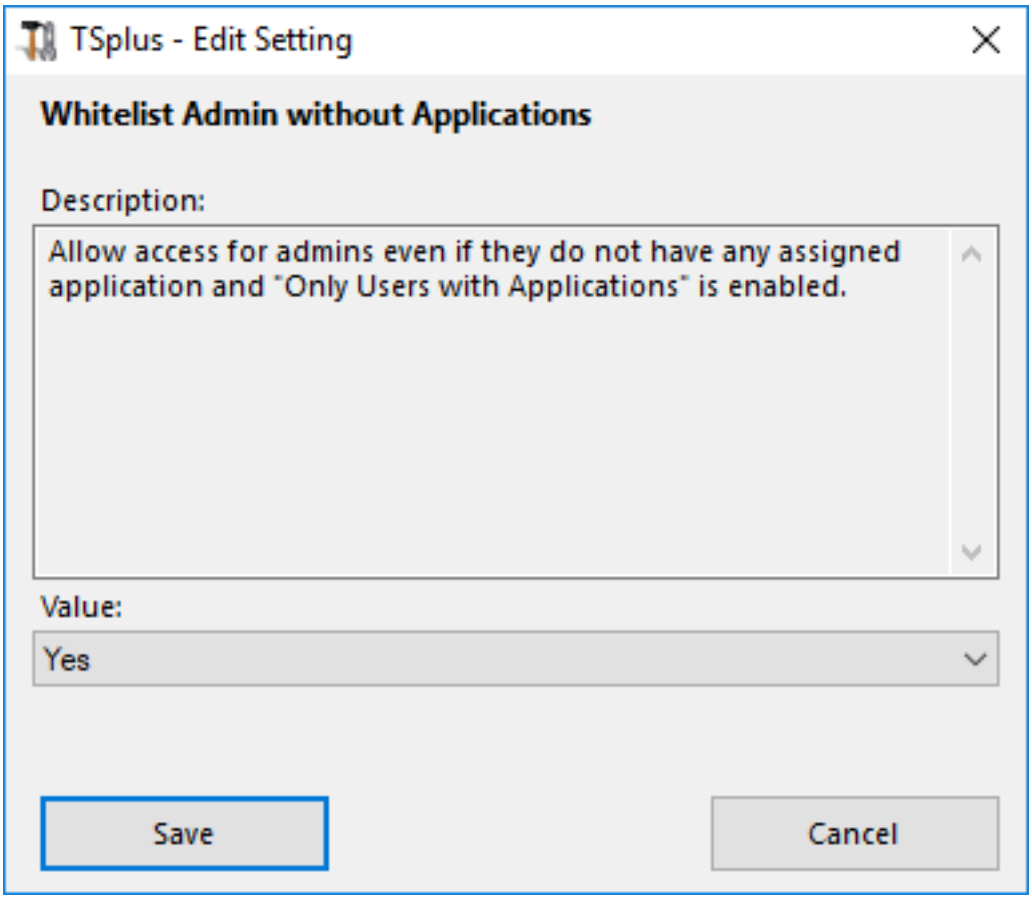
Seulement les utilisateurs avec des applications

Autoriser l'accès uniquement aux utilisateurs ayant au moins une application assignée en sélectionnant la valeur « oui ».



Administrateurs de liste blanche sans applications

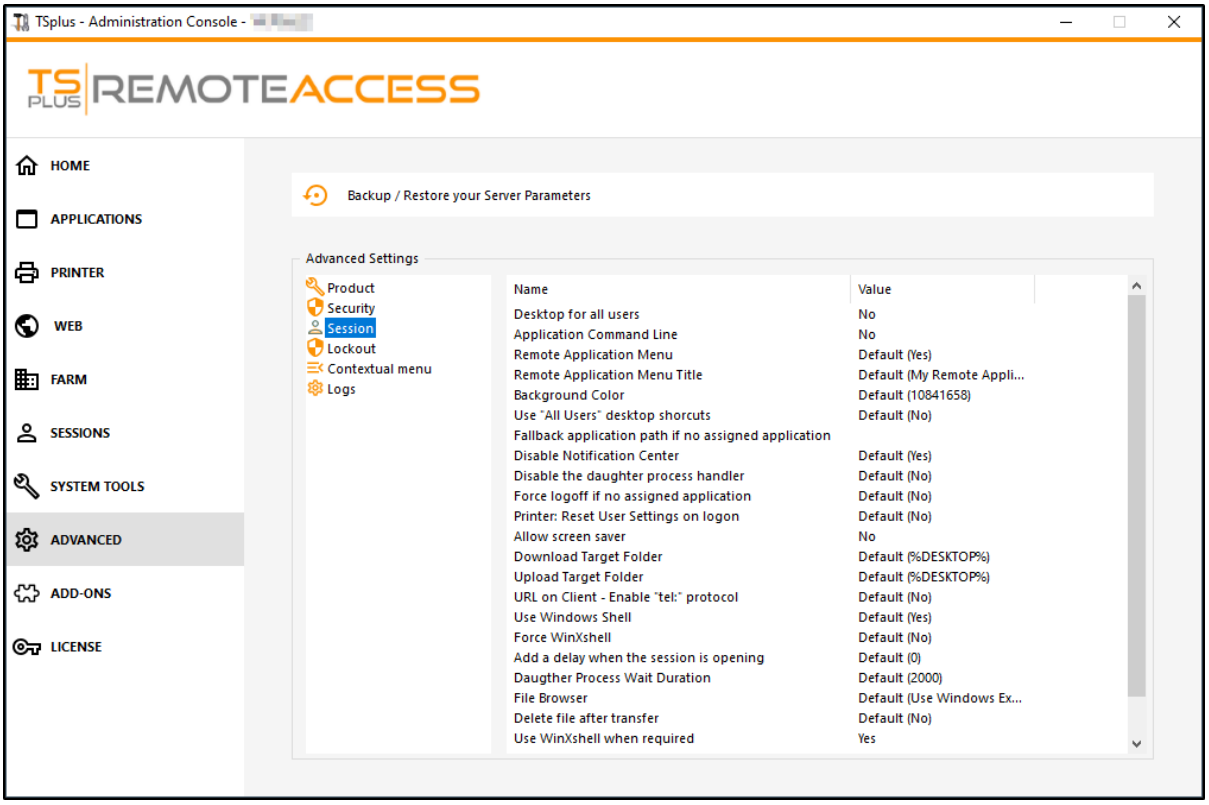
Autoriser l'accès aux administrateurs même s'ils n'ont aucune application assignée et que "Seules les utilisateurs avec des applications" est activé. Cette fonctionnalité est activée par défaut. Si vous souhaitez la désactiver, sélectionnez la valeur "Non" dans cette fenêtre, puis cliquez sur enregistrer :


TSplus - Edit Setting
Whitelist Admin without Applications
Description:
Allow access for admins even if they do not have any assigned application and "Only Users with Applications" is enabled.
Value:
Yes
Save
Cancel

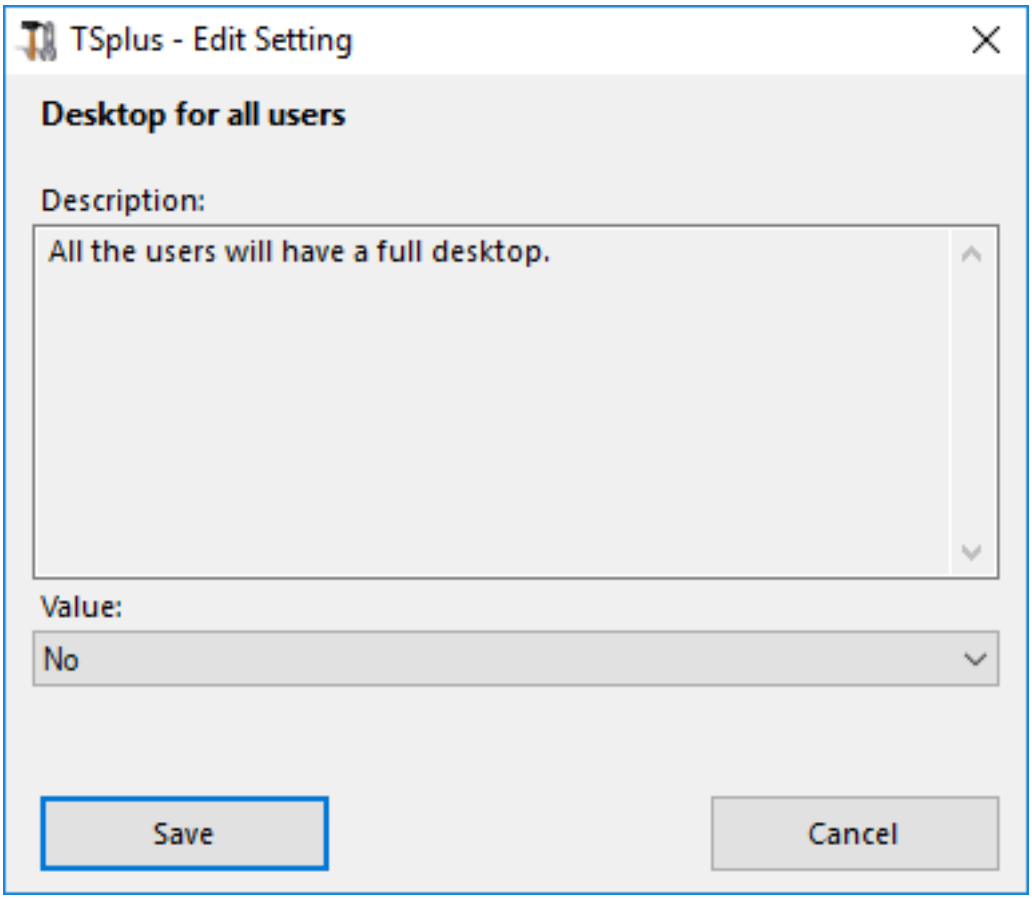
Fonctionnalités avancées - Session

Aperçu

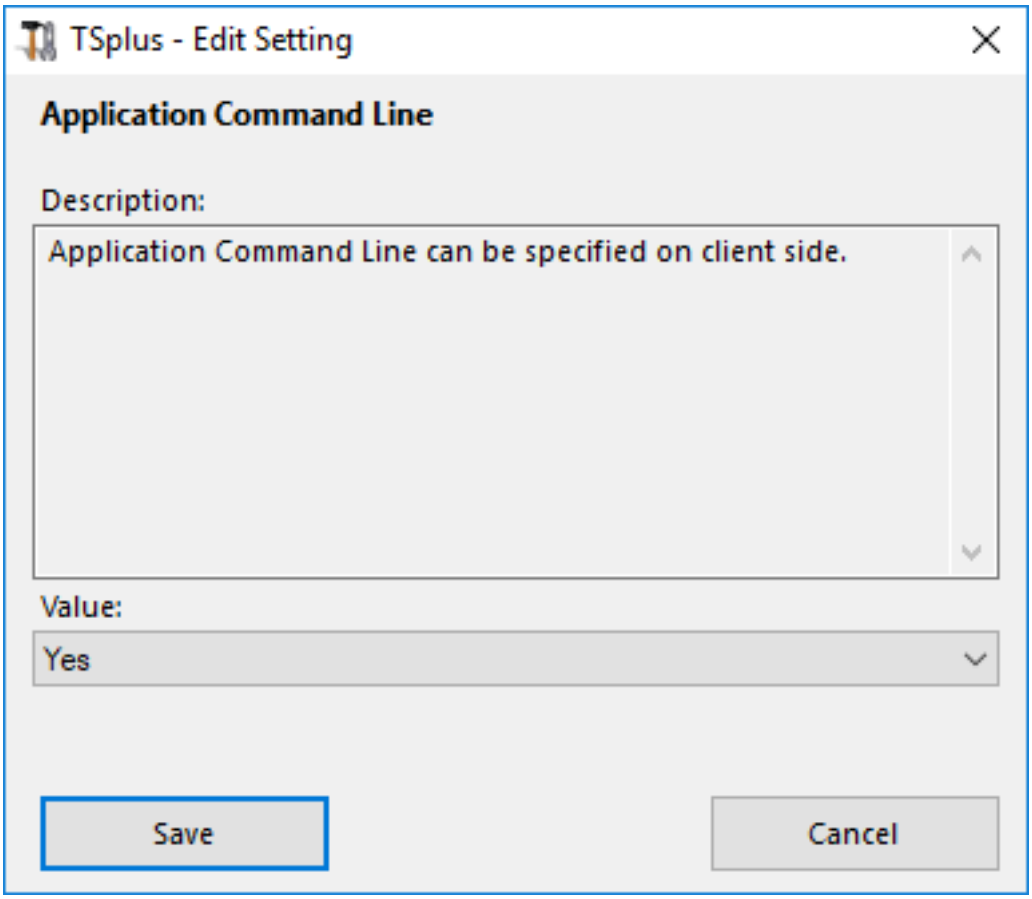
Cette section de l'onglet Avancé vous permet de configurer les droits des utilisateurs et les aspects de leurs sessions.



Activez un bureau complet pour tous les utilisateurs en sélectionnant la valeur « Oui » dans cette fenêtre, puis cliquez sur enregistrer :

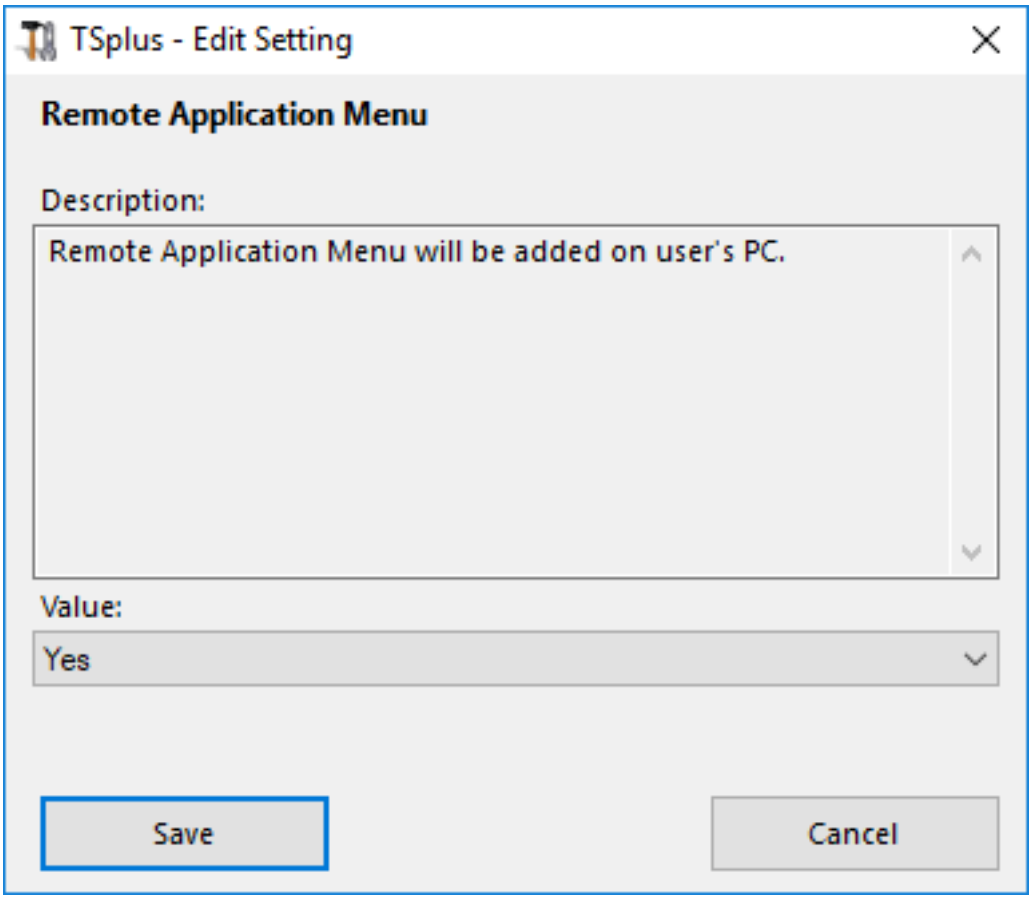


La ligne de commande de l'application peut être spécifiée du côté client. Cette fonctionnalité est activée par défaut. Si vous souhaitez la désactiver, sélectionnez la valeur « Non » dans cette fenêtre, puis cliquez sur enregistrer :



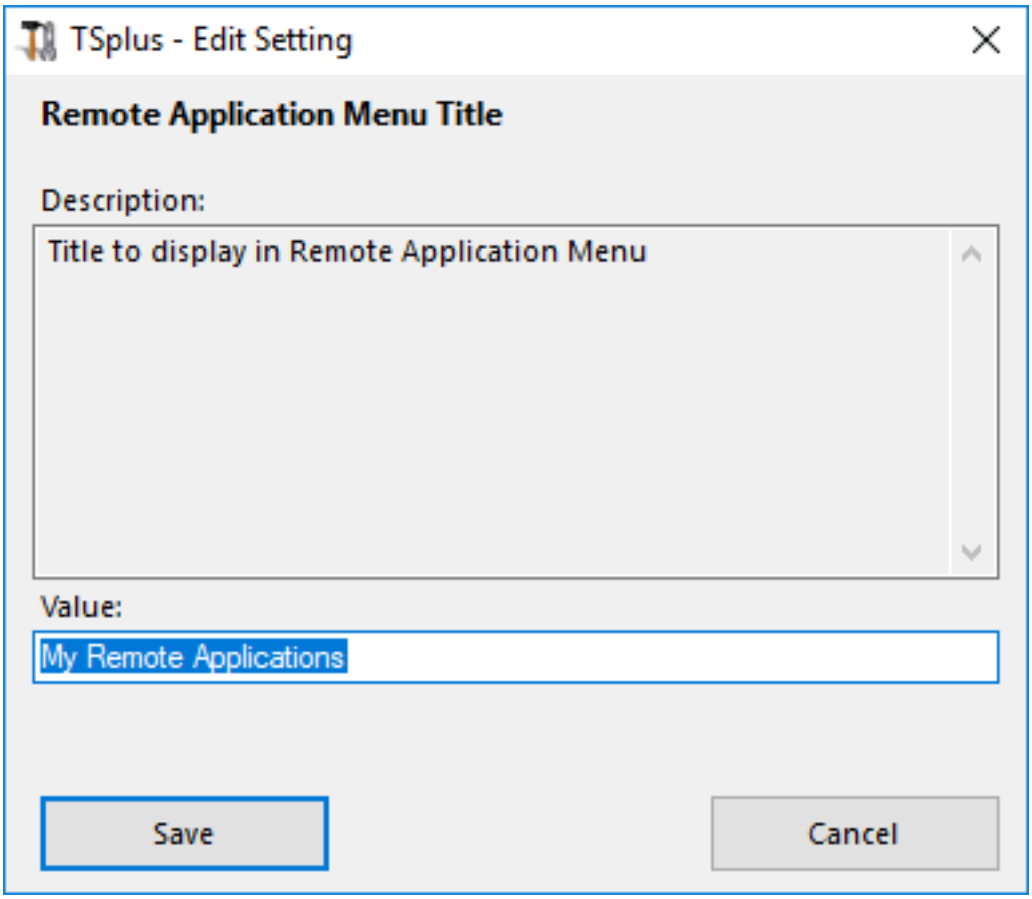
Menu d'application à distance

Le menu d'application distante sera ajouté sur le PC de l'utilisateur. Cette fonctionnalité est activée par défaut. Si vous souhaitez la désactiver, sélectionnez la valeur "Non" dans cette fenêtre, puis cliquez sur enregistrer.



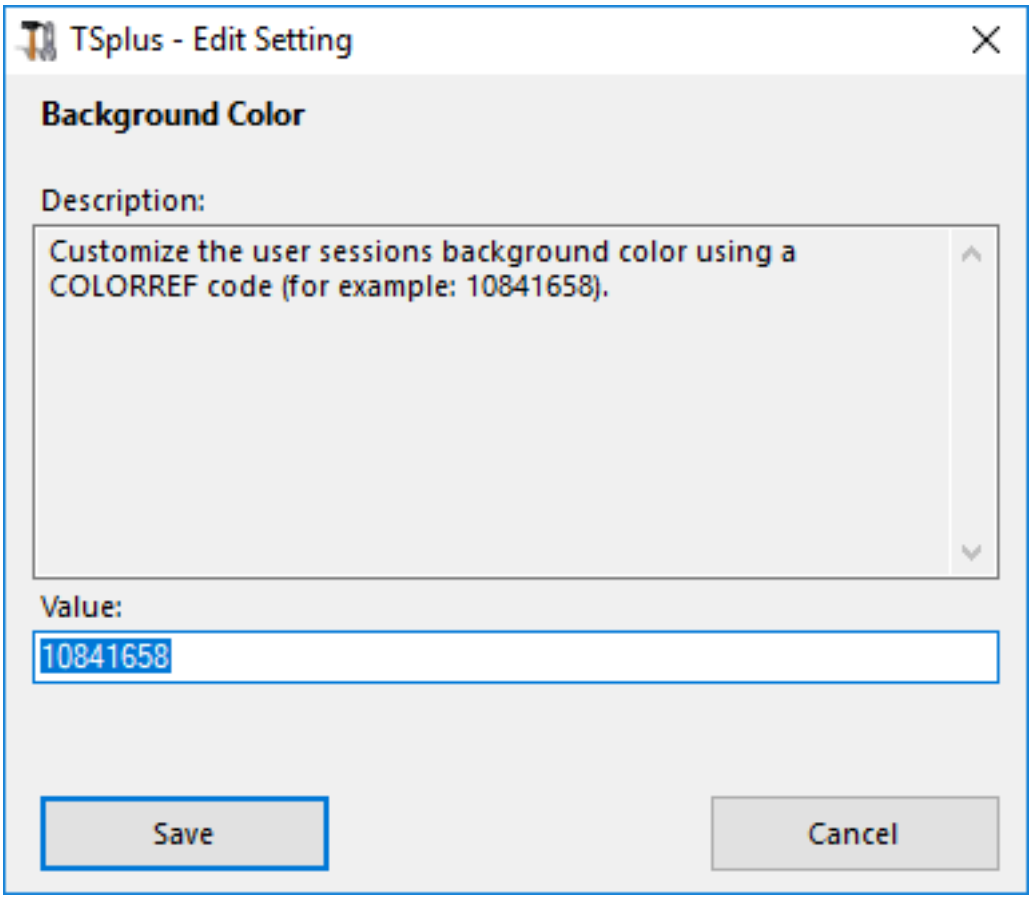
Titre du menu d'application à distance

Vous pouvez modifier le titre du menu d'application à distance. Le titre par défaut est « Mes applications à distance ». Si vous souhaitez le modifier, entrez le titre souhaité, puis cliquez sur enregistrer :



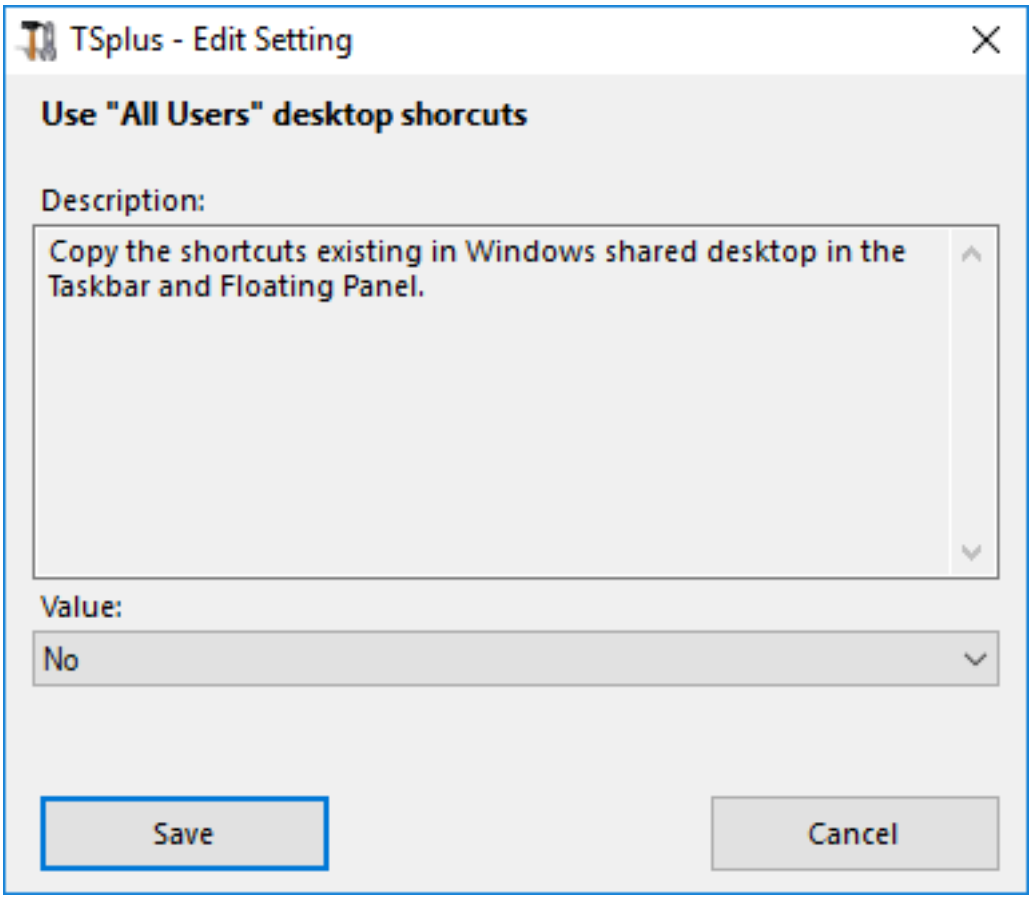
Couleur de fond

Personnalisez la couleur de fond des sessions utilisateur en utilisant un code COLORREF (par exemple, le code par défaut est : 10841658).



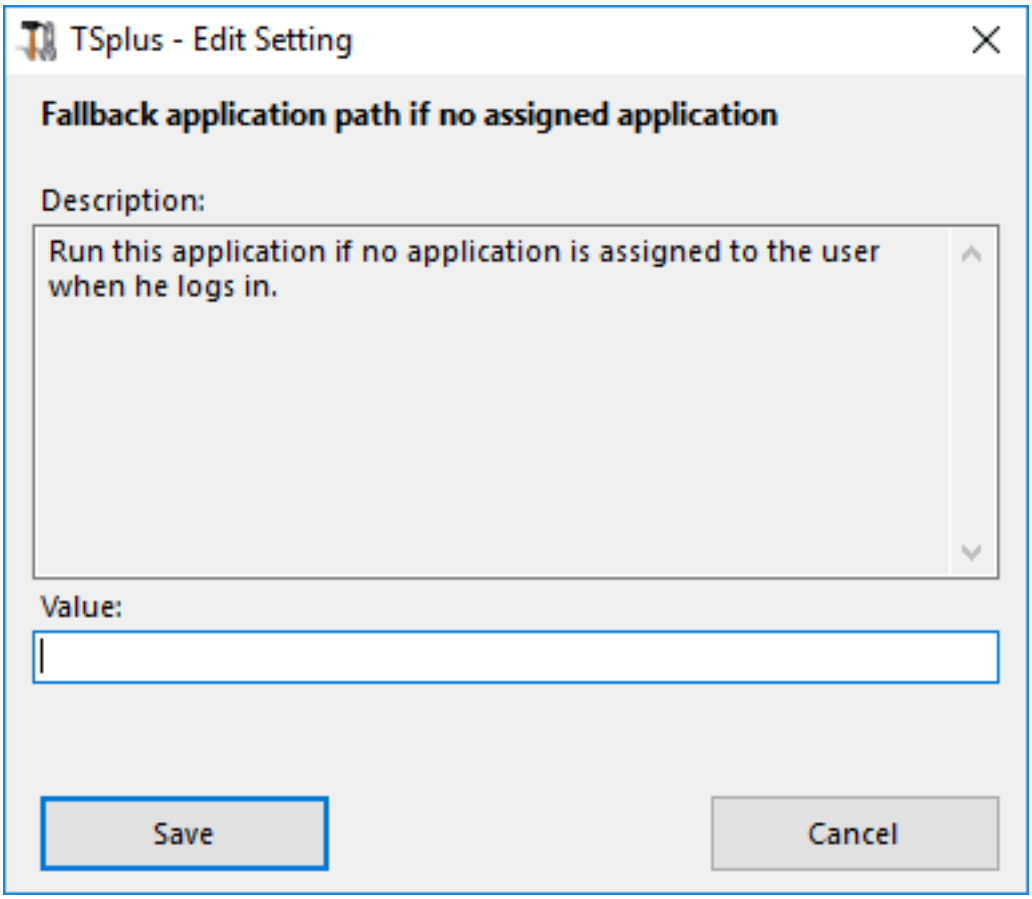
Utilisez les raccourcis de bureau "Tous les utilisateurs"

Copiez les raccourcis existants dans le bureau partagé de Windows dans la barre des tâches et le panneau flottant. Activez cette fonctionnalité en sélectionnant la valeur « Oui » dans cette fenêtre, puis cliquez sur enregistrer :



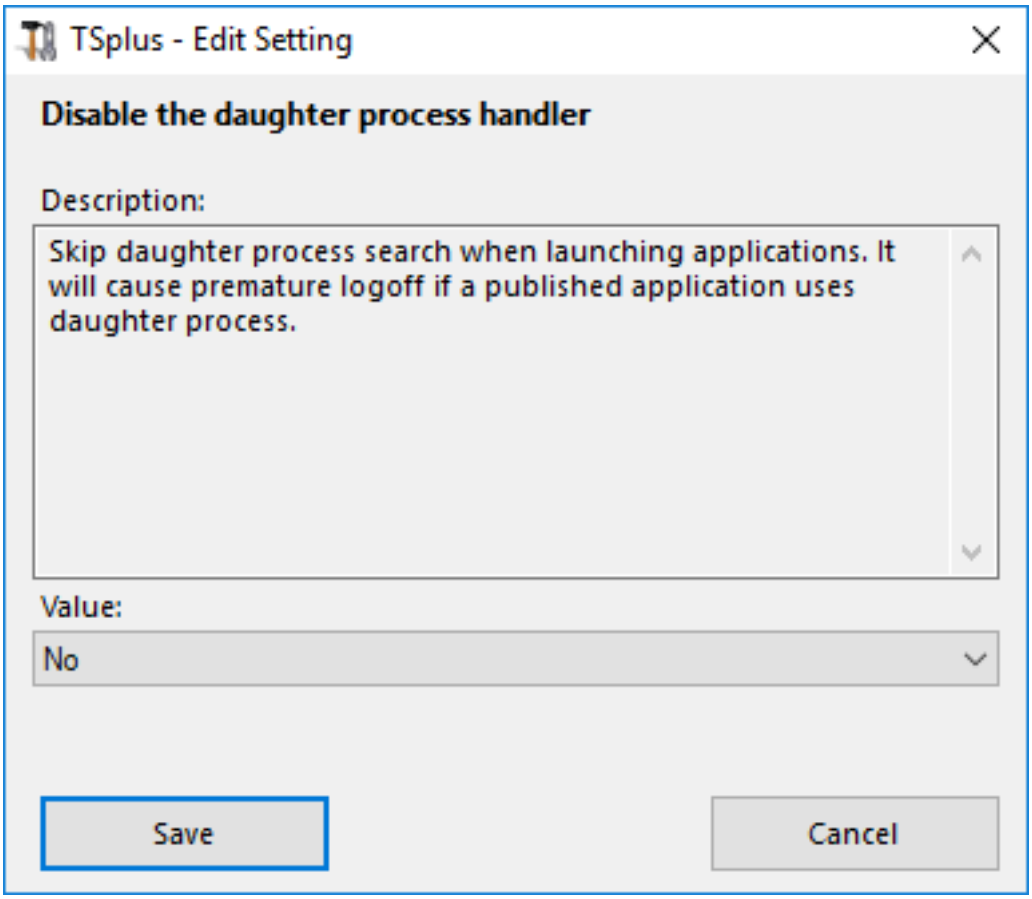
Chemin d'application de secours si aucune application assignée

Exécutez cette application si aucune application n'est assignée à l'utilisateur lorsqu'il se connecte. Il n'y a pas de valeur par défaut. Activez cette fonctionnalité en saisissant une valeur "Oui" dans cette fenêtre, puis cliquez sur enregistrer.



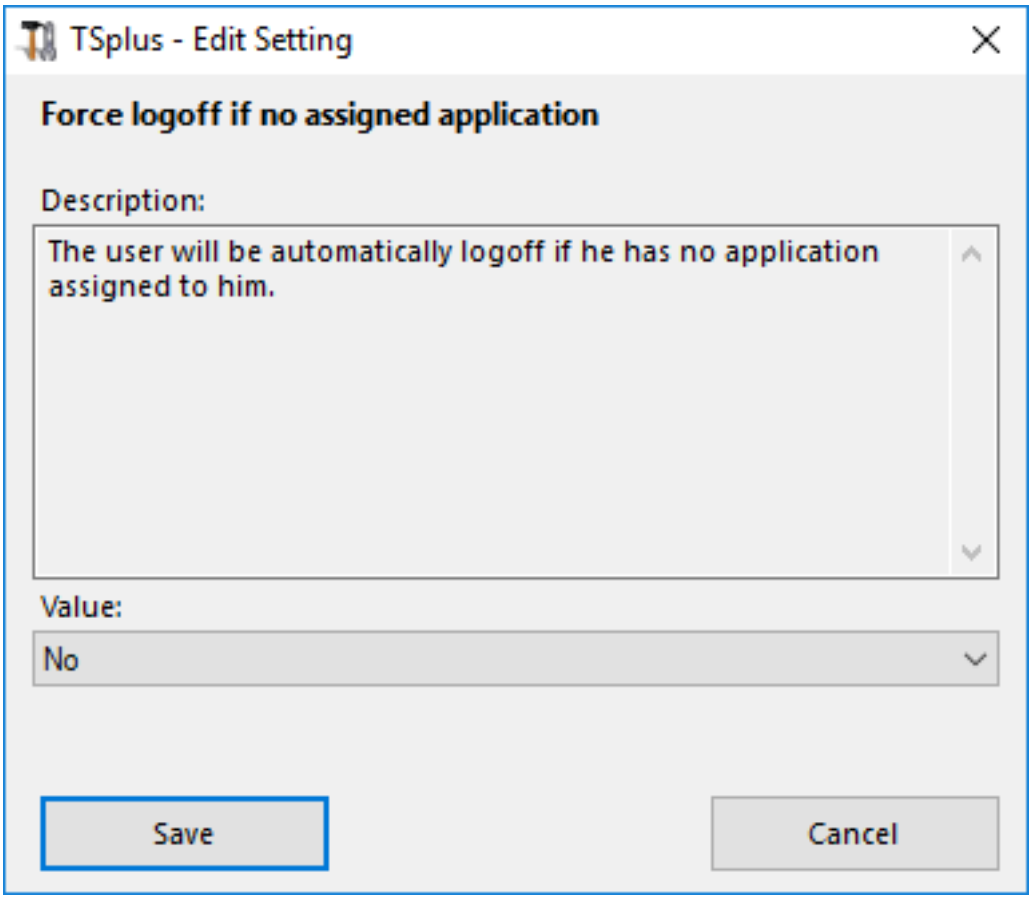
Désactiver le gestionnaire de processus fils

Sauter la recherche de processus fils lors du lancement d'applications. Cela entraînera une déconnexion prématurée si une application publiée utilise un processus fils. Cette fonctionnalité est désactivée par défaut. Activez cette fonctionnalité en sélectionnant la valeur « Oui » dans cette fenêtre, puis cliquez sur enregistrer :



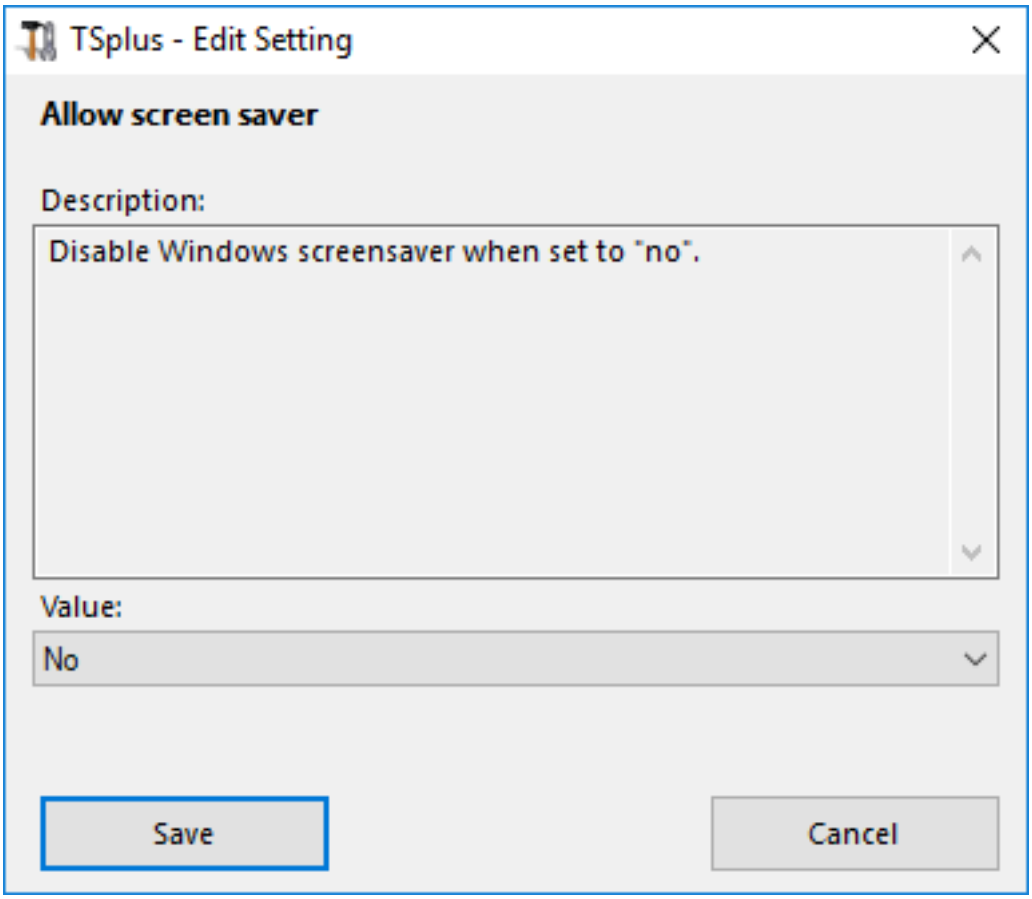
Forcer la déconnexion si aucune application assignée

L'utilisateur sera automatiquement déconnecté s'il n'a aucune application qui lui est assignée. Cette fonctionnalité est désactivée par défaut. Activez cette fonctionnalité en sélectionnant la valeur « Oui » dans cette fenêtre, puis cliquez sur enregistrer :



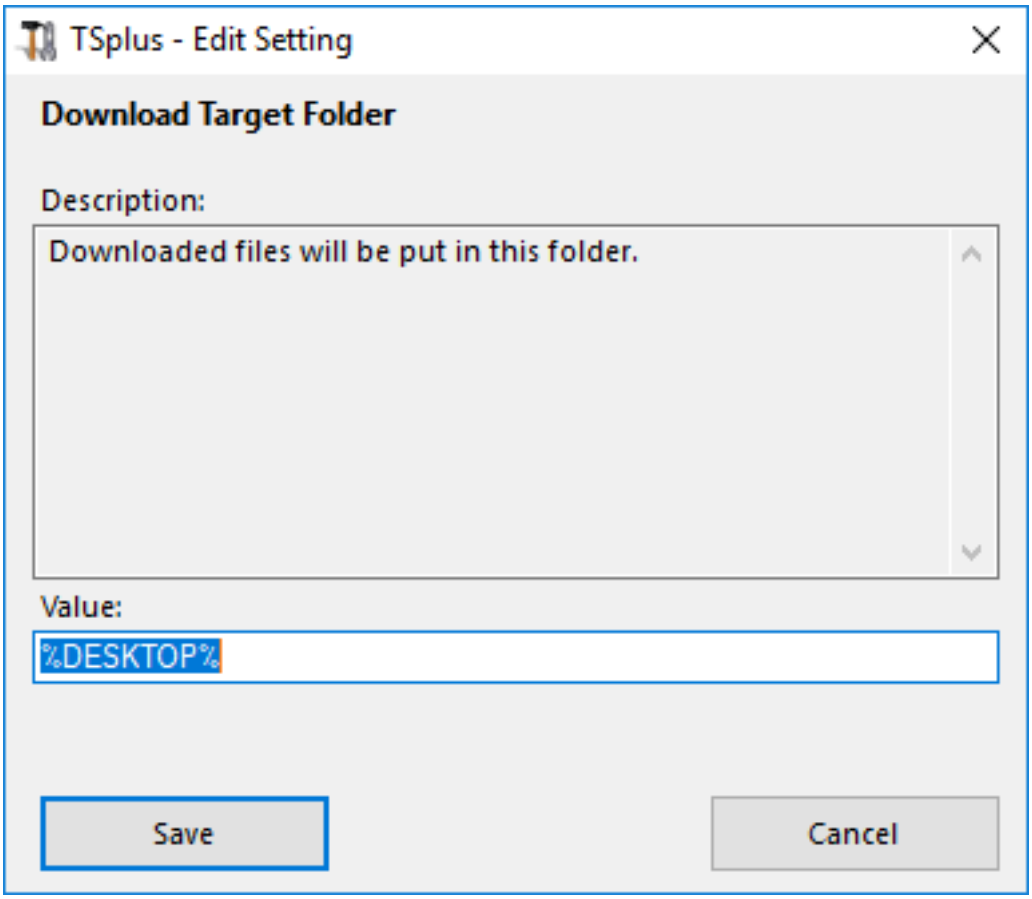
Autoriser l'économiseur d'écran

Cette fonctionnalité est désactivée par défaut. Activez l'économiseur d'écran Windows en sélectionnant la valeur « Oui » dans cette fenêtre, puis cliquez sur enregistrer :



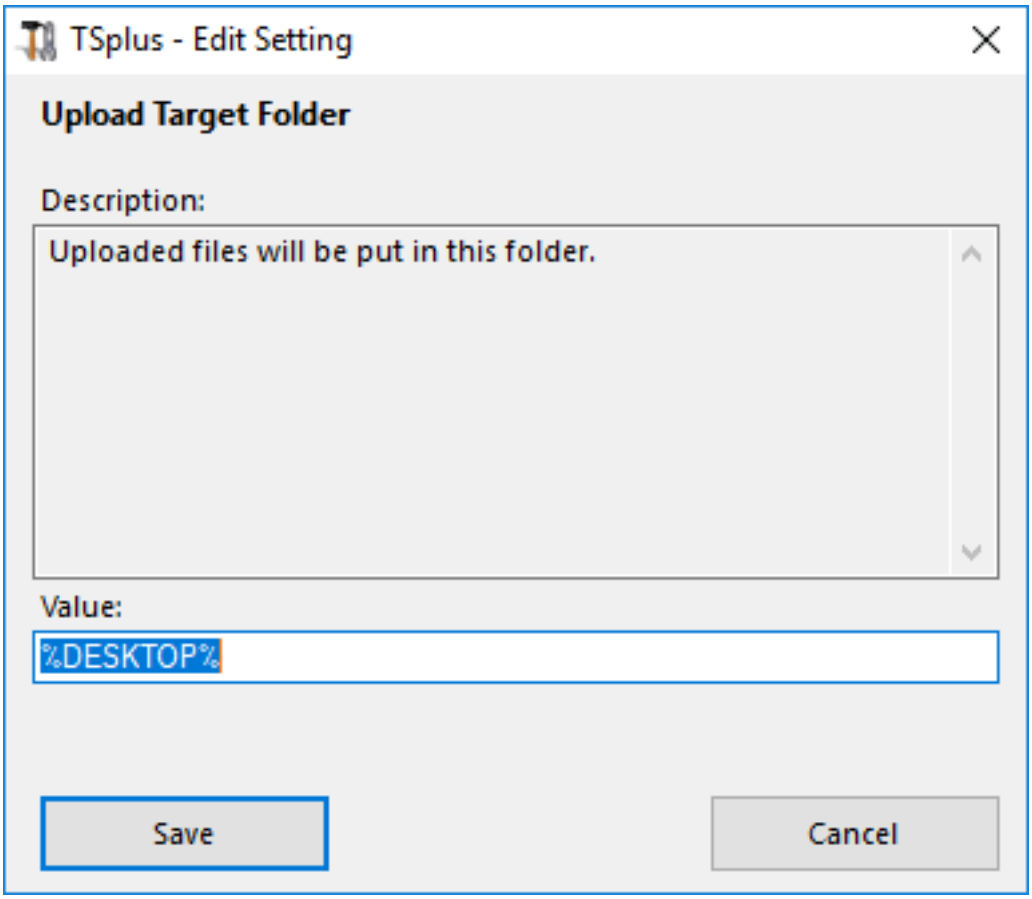
Télécharger le dossier cible

Les fichiers téléchargés seront placés sur le Bureau par défaut. Si vous souhaitez le modifier, entrez le chemin du dossier de téléchargement souhaité, puis cliquez sur enregistrer :



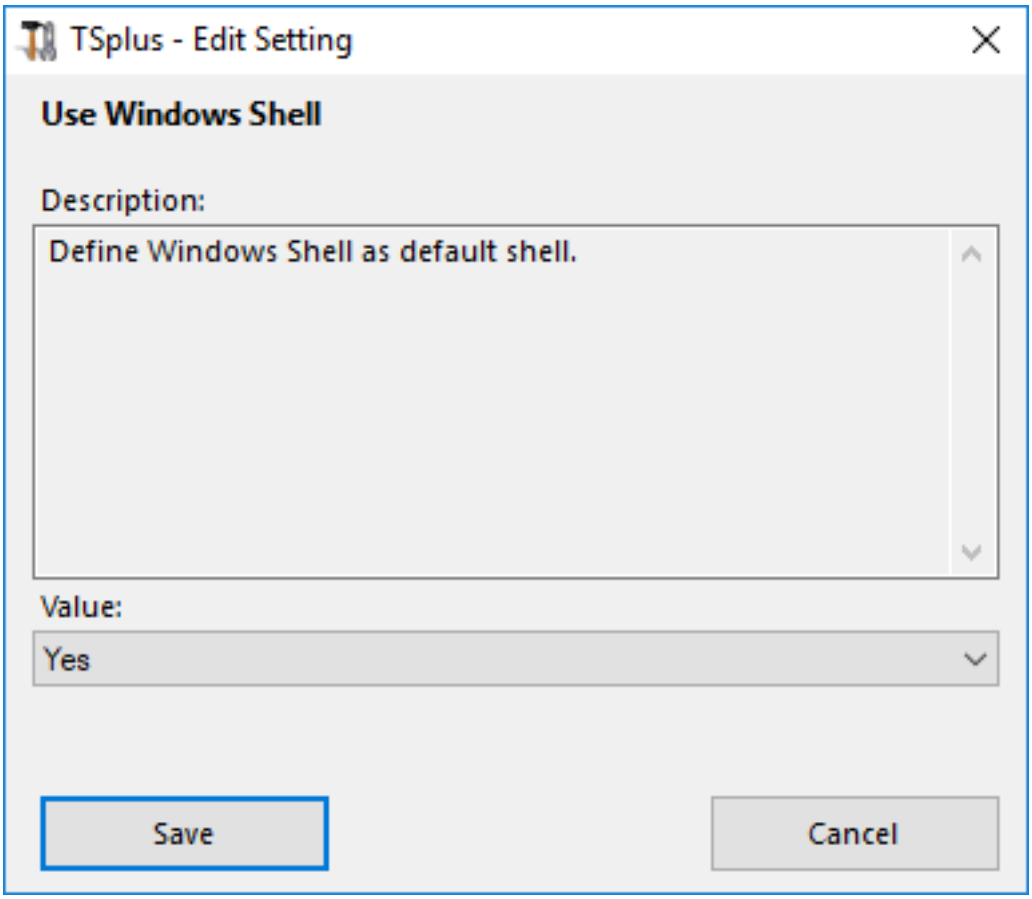
Télécharger le dossier cible

Les fichiers téléchargés seront placés dans ce dossier. Si vous souhaitez le modifier, entrez le chemin du dossier de téléchargement souhaité, puis cliquez sur enregistrer :



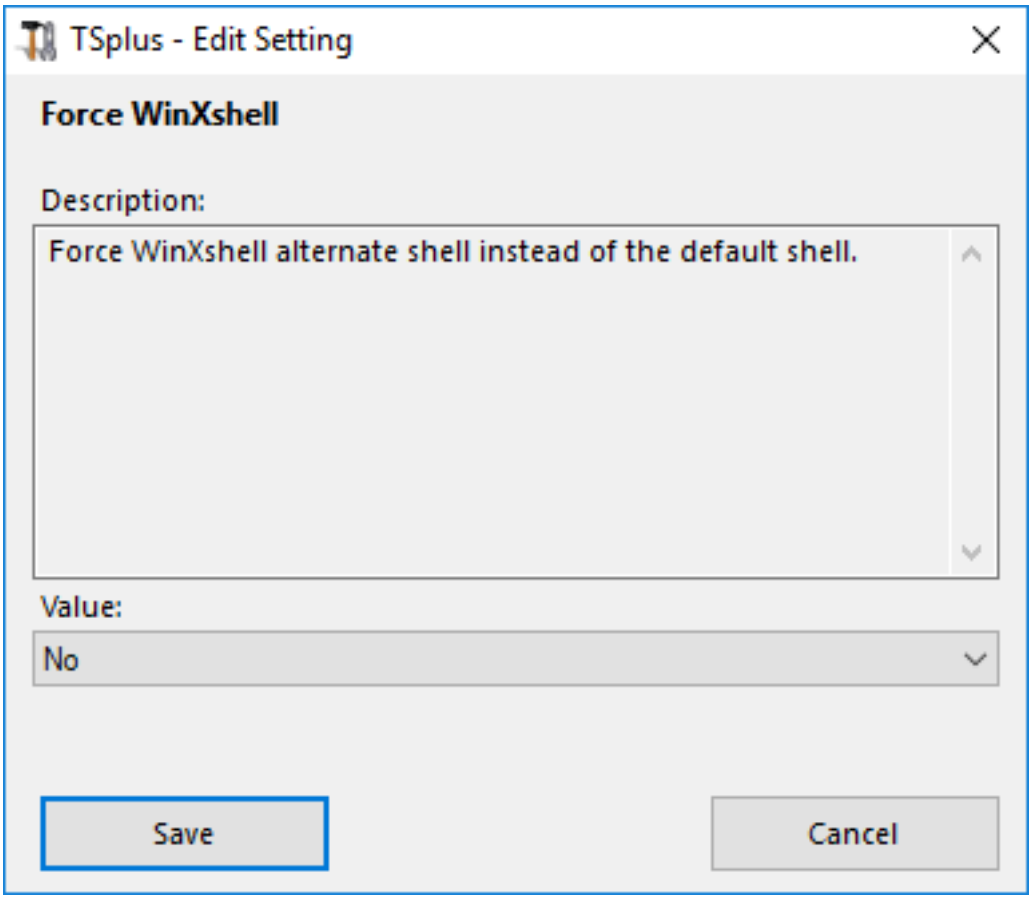
Utiliser Windows Shell

Définir Windows Shell comme shell par défaut. Cette fonctionnalité est activée par défaut. Si vous souhaitez la désactiver, sélectionnez la valeur « Non » dans cette fenêtre, puis cliquez sur enregistrer :



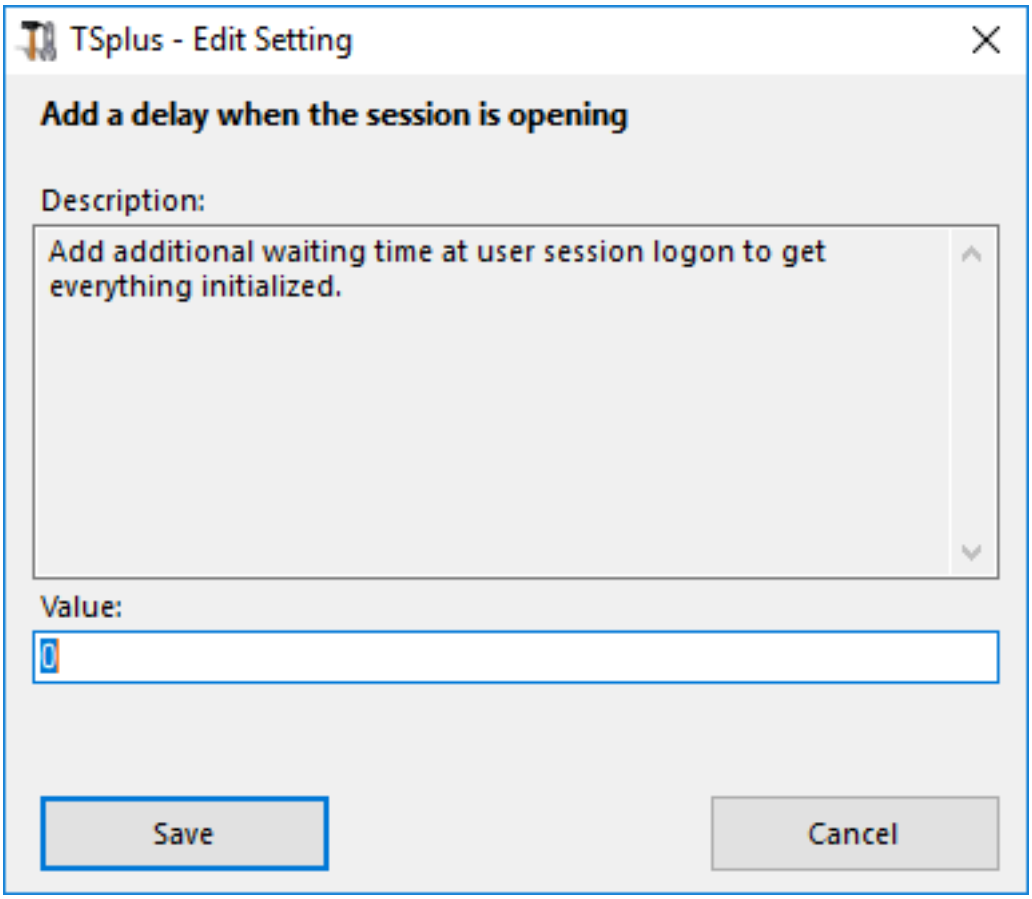
Force WinXshell

Cette fonctionnalité est désactivée par défaut. Forcez WinXshell comme shell alternatif au lieu du shell par défaut en sélectionnant la valeur « Oui » dans cette fenêtre, puis cliquez sur enregistrer :



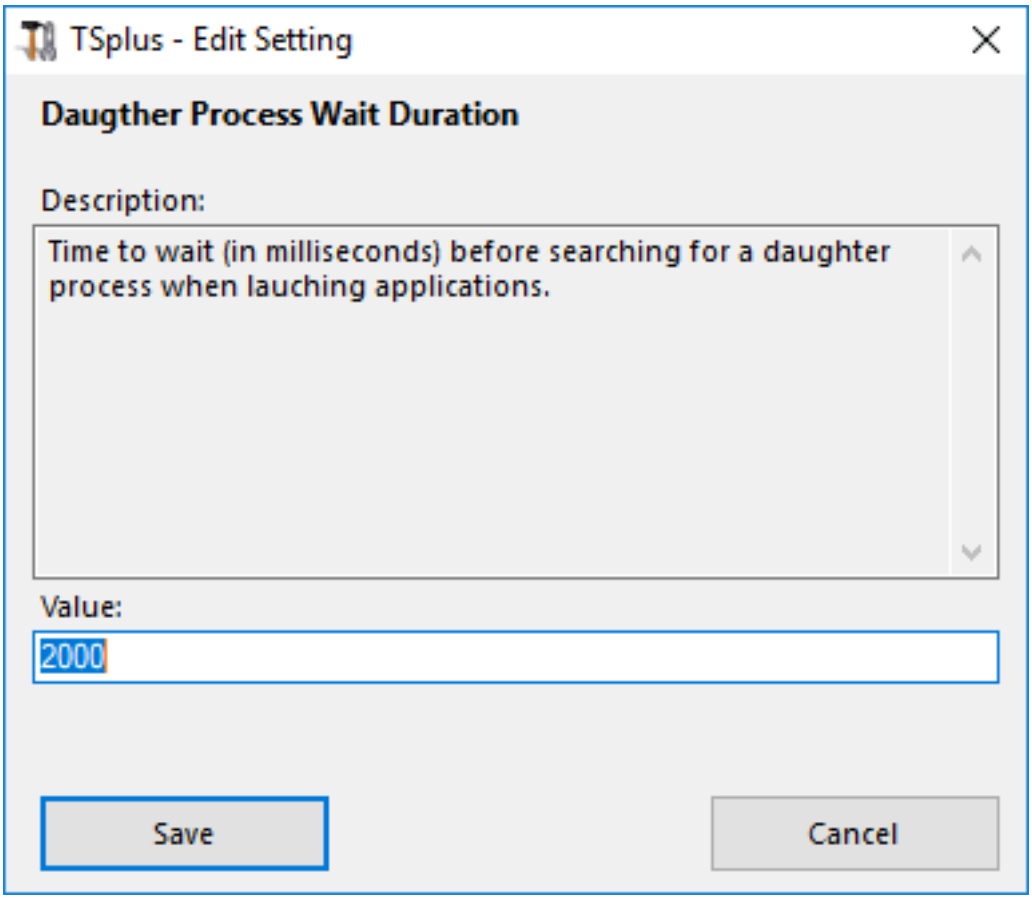
Ajoutez un délai lors de l'ouverture de la session

Ajoutez un temps d'attente supplémentaire lors de la connexion de l'utilisateur pour que tout soit initialisé. La valeur par défaut est 0. Si vous souhaitez la modifier, entrez la valeur souhaitée (en secondes), puis cliquez sur enregistrer :



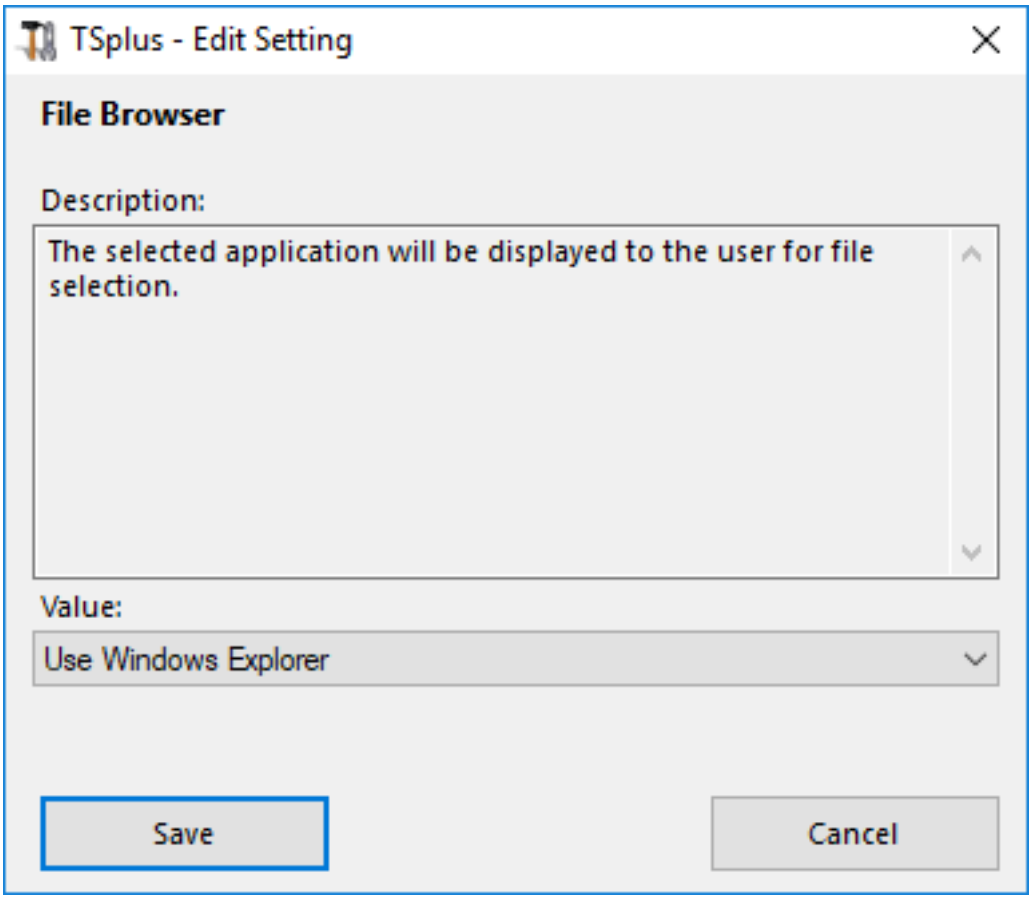
Durée d'attente du processus fils

Temps d'attente (en millisecondes) avant de rechercher un processus fils lors du lancement d'applications.



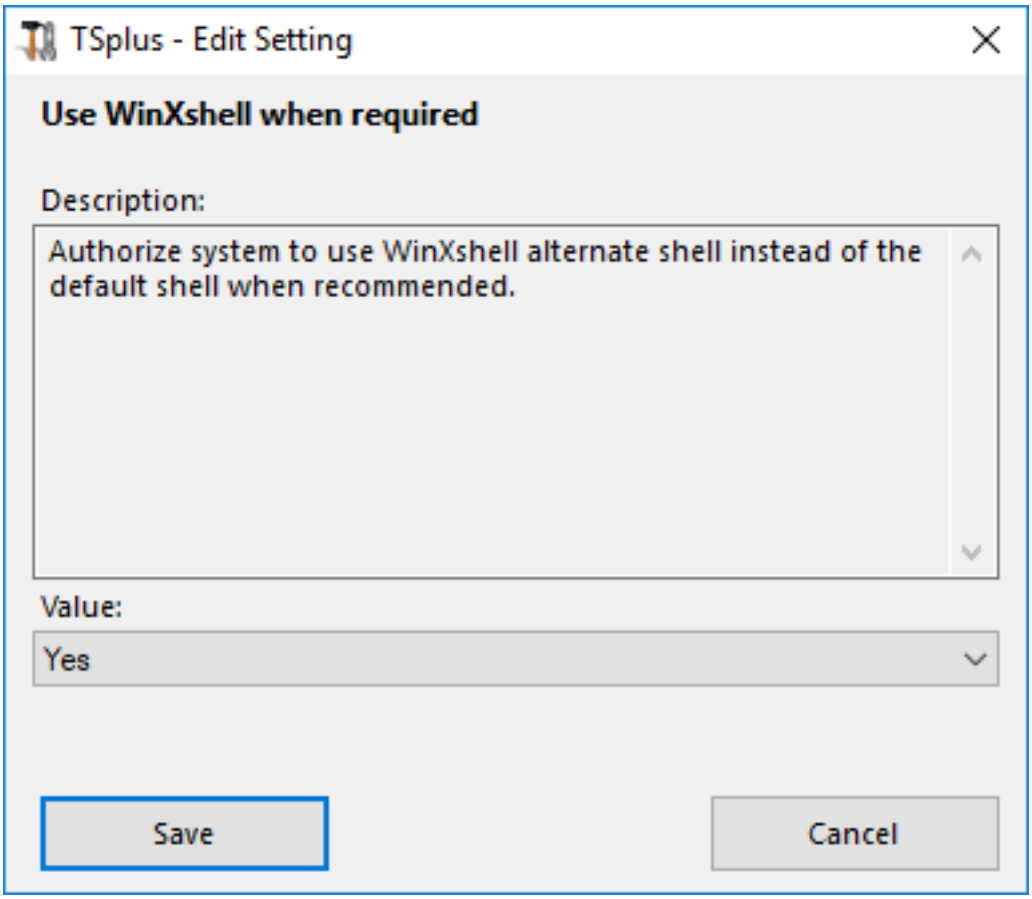
Explorateur de fichiers

L'application sélectionnée sera affichée à l'utilisateur pour la sélection de fichiers. Le navigateur par défaut est l'Explorateur Windows. Vous pouvez utiliser le navigateur de fichiers TSplus en le sélectionnant, puis cliquez sur enregistrer :



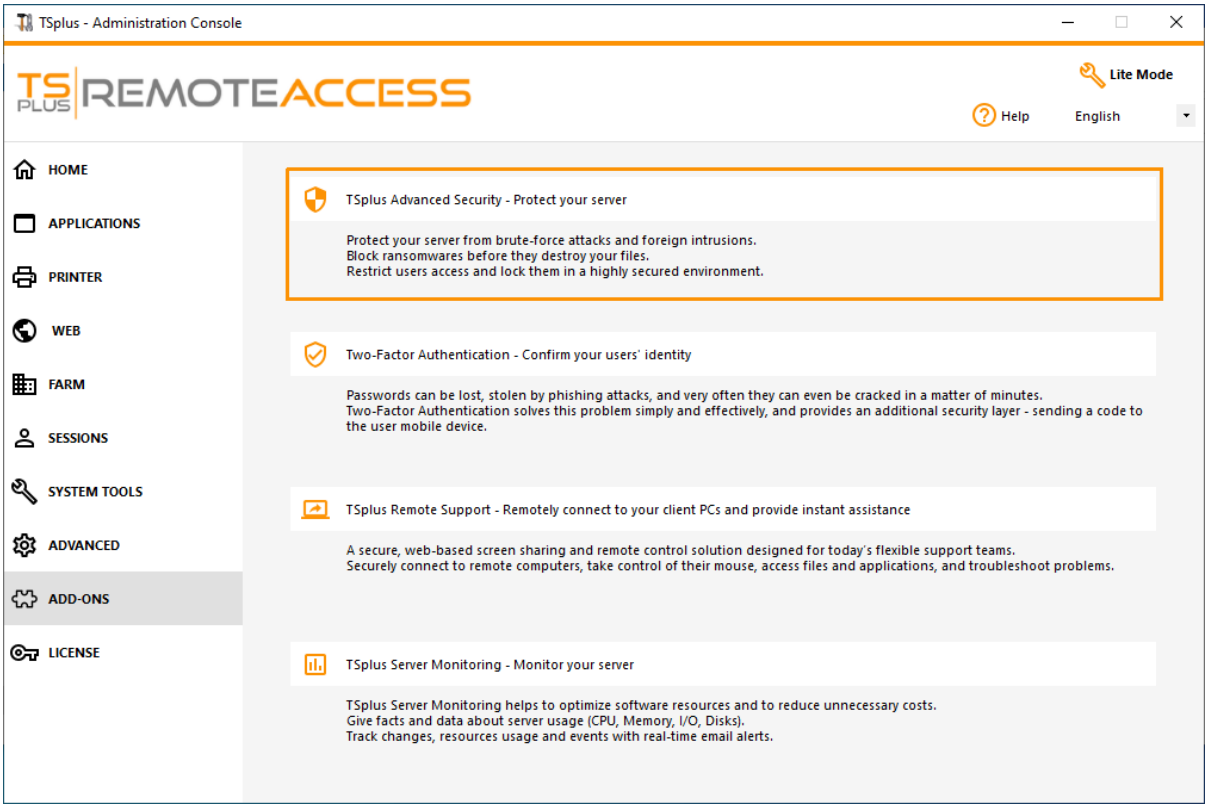
Utilisez WinXshell si nécessaire

Autoriser le système à utiliser WinXshell comme shell alternatif au lieu du shell par défaut lorsque cela est recommandé. Cette fonctionnalité est activée par défaut. Si vous souhaitez la désactiver, sélectionnez la valeur « Non » dans cette fenêtre, puis cliquez sur enregistrer :


TSplus - Edit Setting
Use WinXshell when required
Description:
Authorize system to use WinXshell alternate shell instead of the default shell when recommended.
Value:
Yes
Save
Cancel

TSplus Advanced Security

TSplus Advanced Security est disponible en tant qu'Add-On depuis TSplus AdminTool et est disponible dans l'onglet Add-Ons :

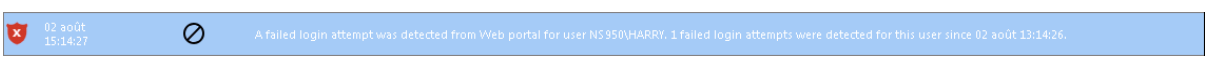


Vous pouvez trouver sa documentation complète sur cette page .

Événement de verrouillage

TSplus Lockout surveille les tentatives de connexion Web échouées sur votre serveur TSplus.

TSplus Advanced Security affichera un événement de verrouillage, après toute tentative échouée du portail Web comme dans l'exemple ci-dessous :



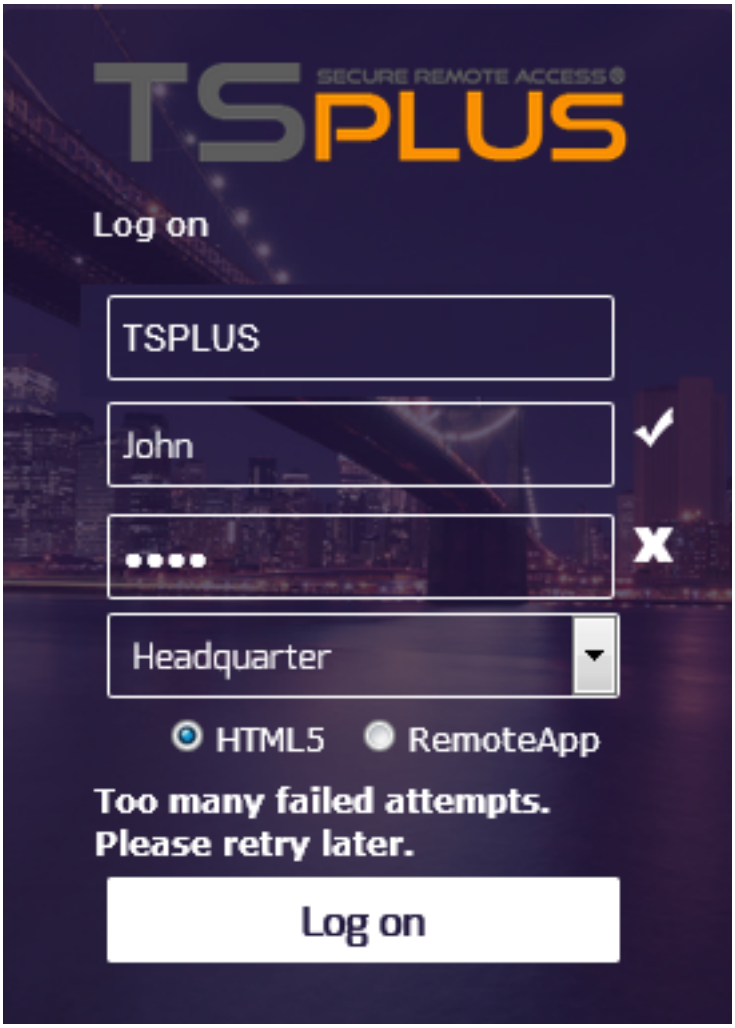
Une tentative de connexion échouée a été détectée depuis le portail Web pour l'utilisateur … 1 tentative de connexion échouée a été détectée pour cet utilisateur depuis…

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 essaieront automatiquement de se connecter à votre serveur des centaines à des milliers de fois chaque minute. En savoir plus sur cette fonctionnalité sur cette page .

Sur le portail Web

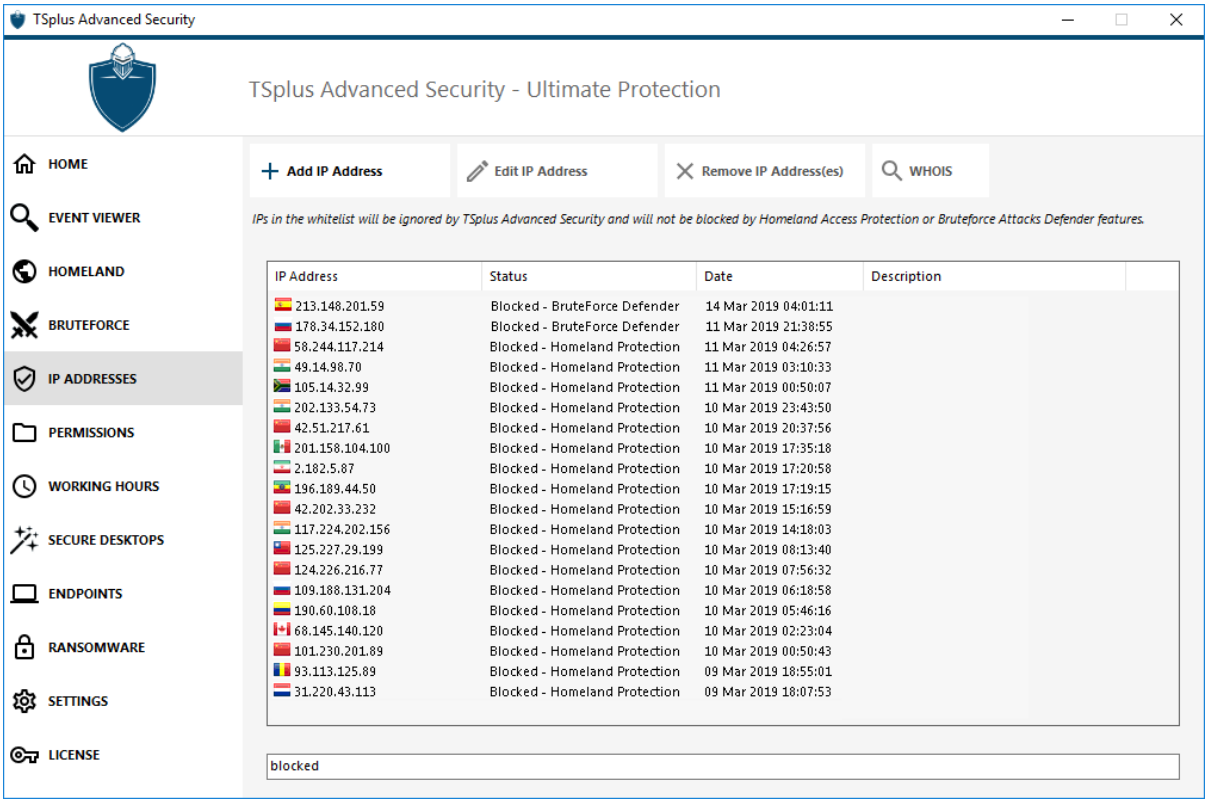
Les attaques par force brute sur le portail Web sont bloquées lorsque les utilisateurs saisissent de mauvaises informations d'identification.

Après 10 tentatives pendant une période de 10 minutes, le portail Web interdira à l'utilisateur de se connecter pendant 20 minutes.



Ce sont les paramètres par défaut qui sont personnalisables sur le Onglet de protection contre les attaques par force brute de TSplus Advanced Security AdminTool.

Vous pouvez vérifier toutes les connexions bloquées et les journaux sur le panneau des adresses IP de TSplus Advanced Security Ultimate Protection :



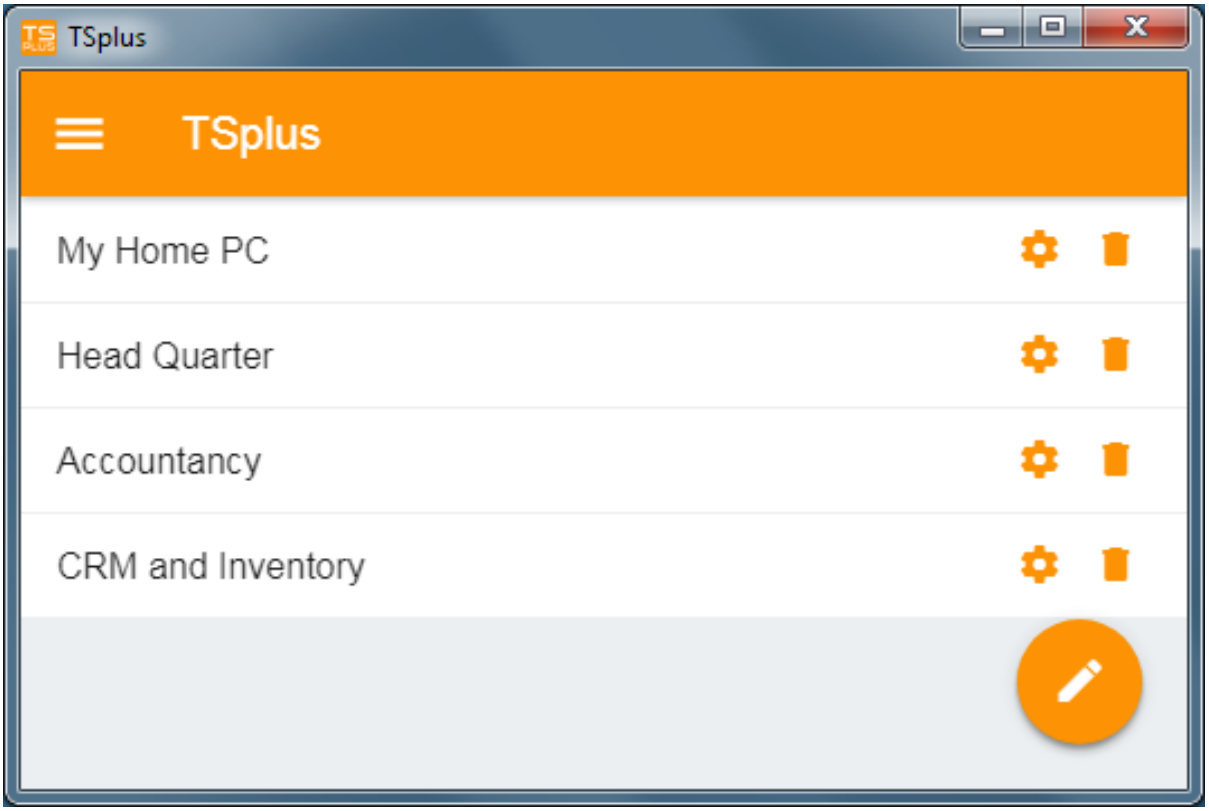
Cette fonctionnalité est visible et active après la première connexion au Web Portal.

La documentation complète de TSplus Advanced Security est disponible sur cette page .

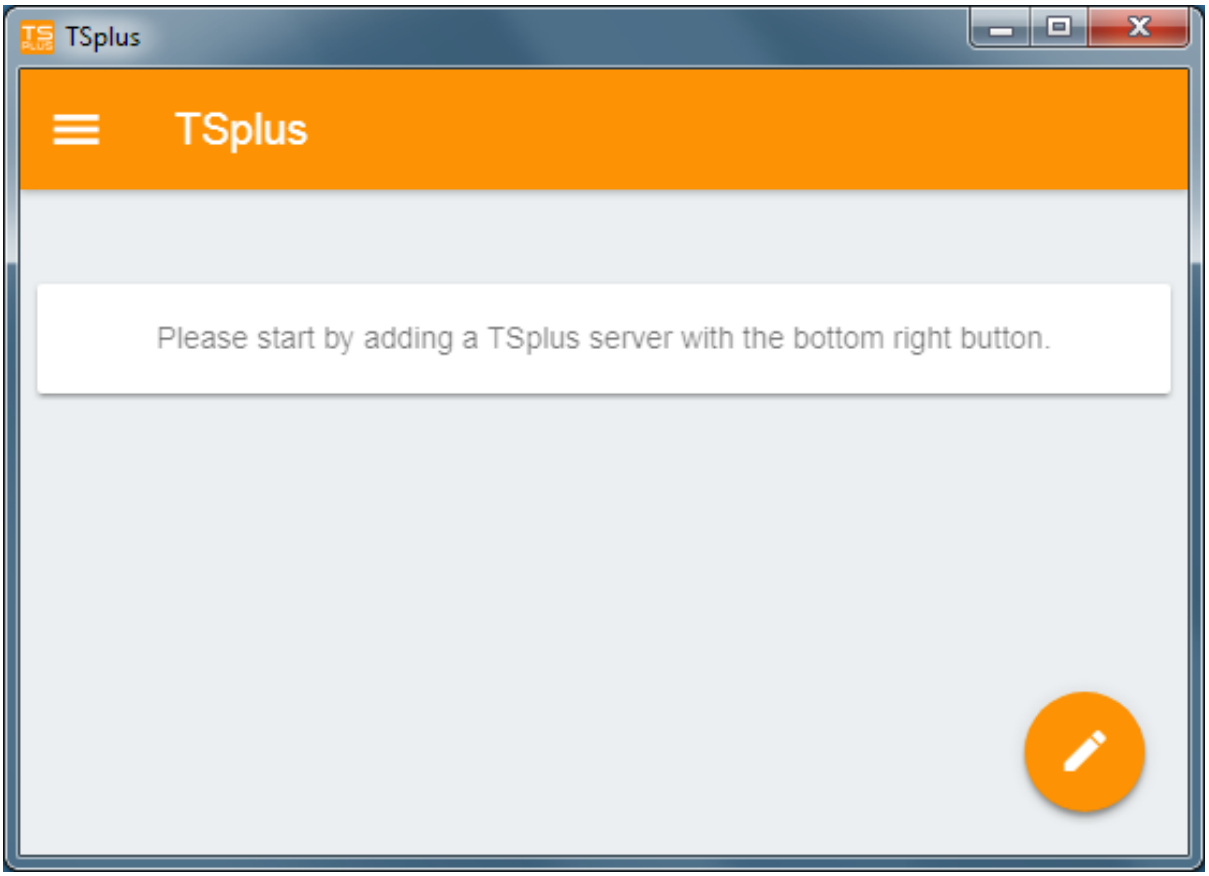
Configuration de l'application TSplus

Gérez vos serveurs

L'interface utilisateur et la configuration sont simples et intuitives.



Tout d'abord, ajoutez un serveur TSplus en cliquant sur le bouton en bas à droite :

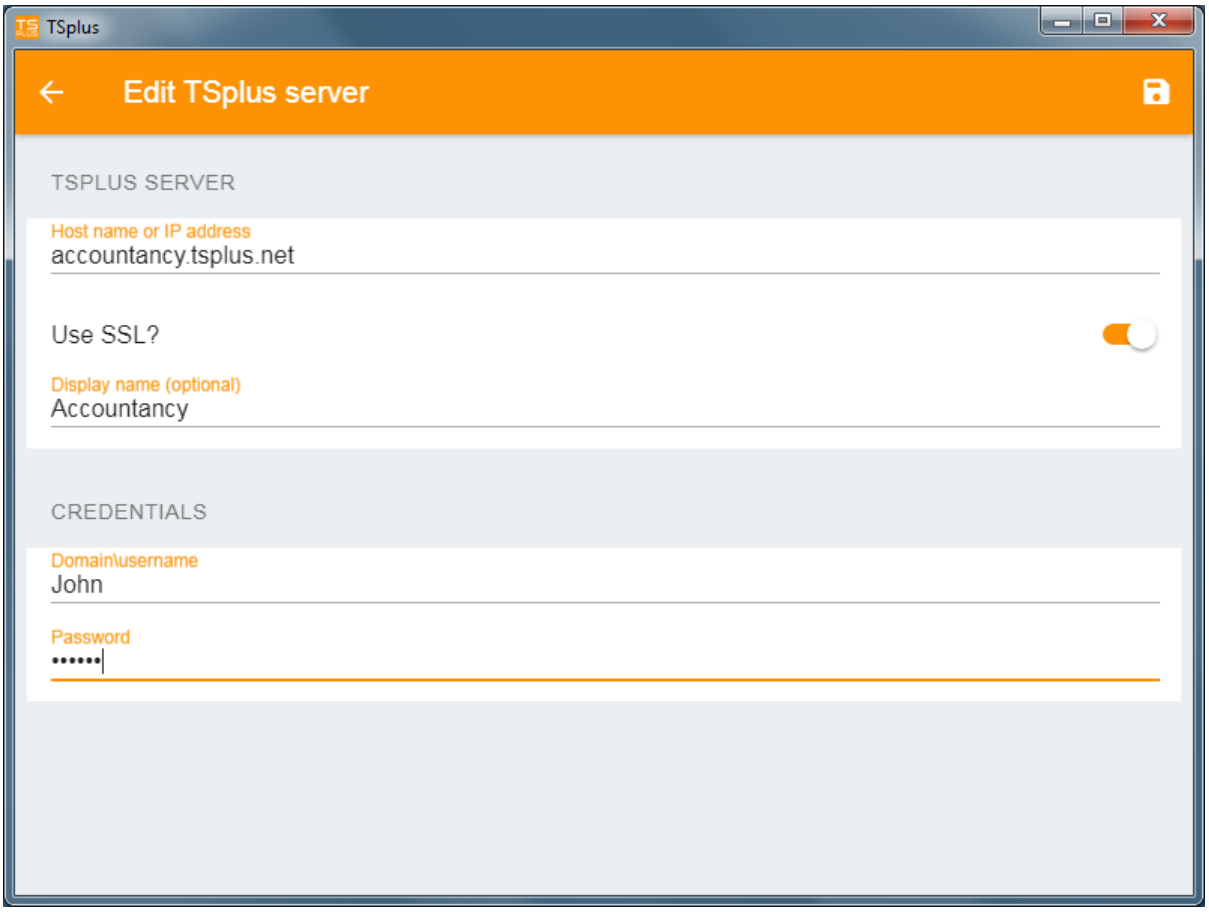


Ensuite, ajoutez les informations de votre serveur et configurez-le :

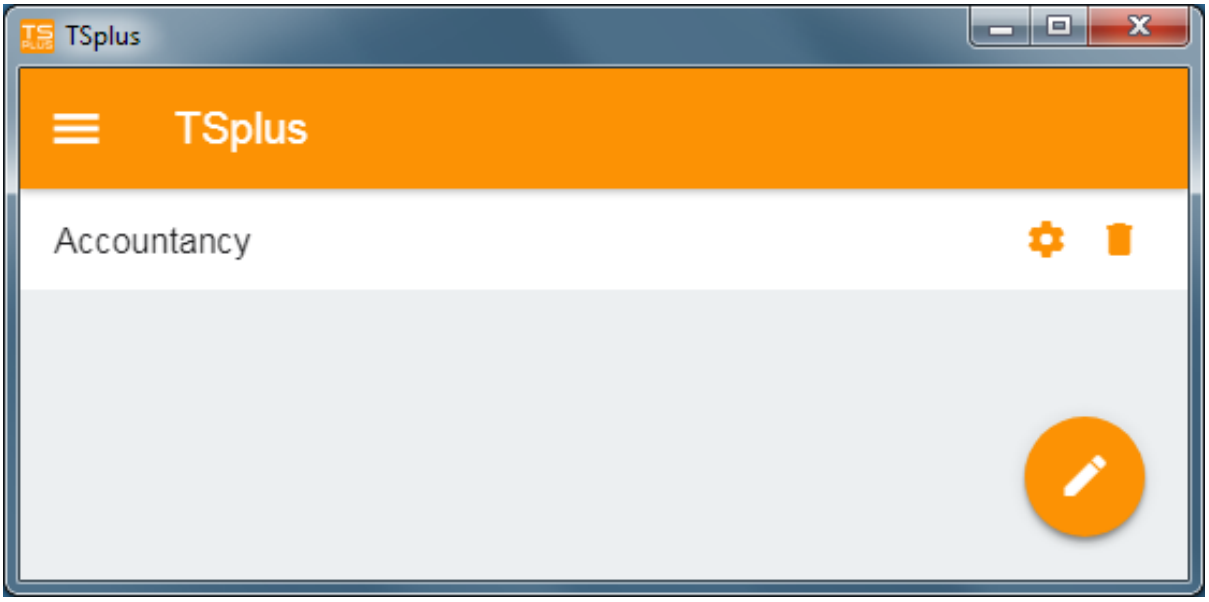
- Entrez son nom d'hôte ou son adresse IP.
- SSL est désactivé par défaut, mais vous pouvez choisir de l'activer.

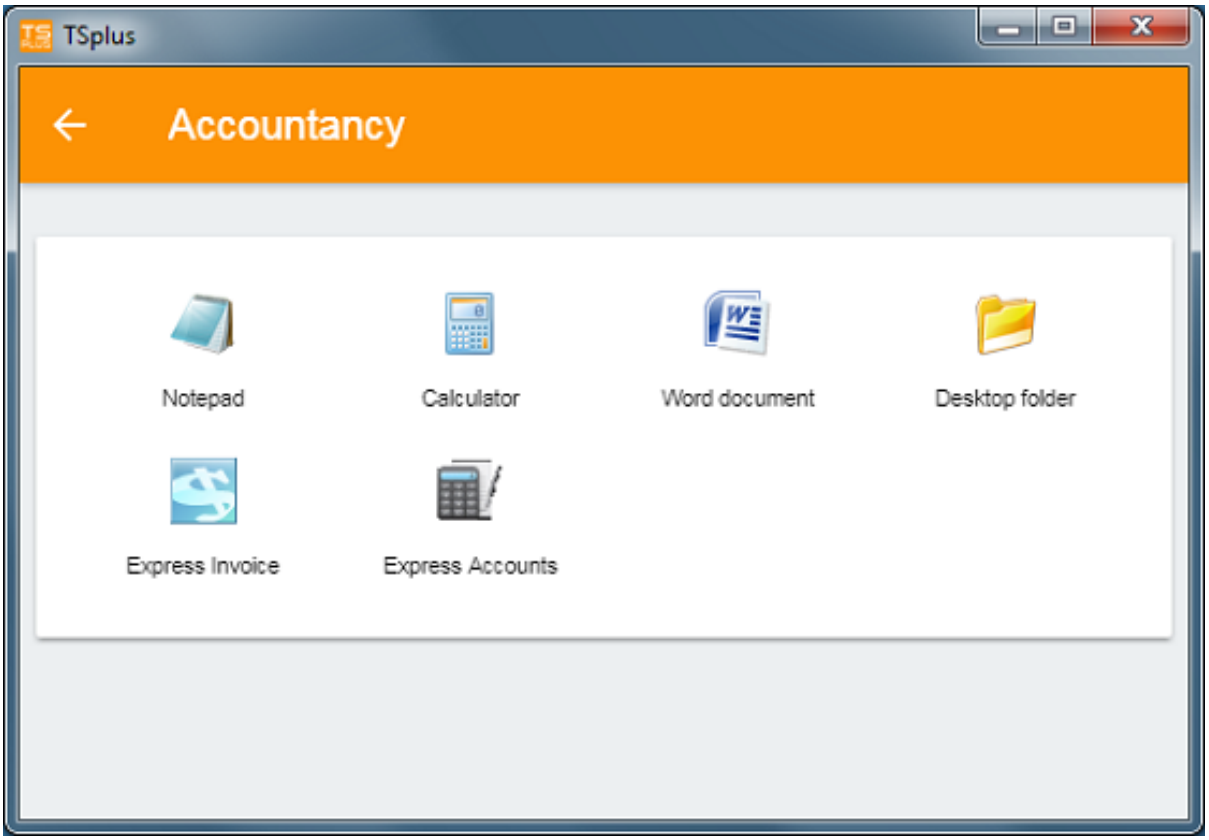
Avertissement : L'activation SSL ne fonctionne que si vous avez installé un certificat SSL valide sur votre serveur TSplus. Voir cette documentation pour plus d'informations.

- Entrez son nom d'affichage, qui est facultatif.
- Entrez les identifiants de votre utilisateur avec le domaine ou le nom d'utilisateur et son mot de passe.
- Si vous utilisez le protocole HTTPS, vous devez entrer le port dans l'adresse configurée. appportal.mydomain.com:443



Ensuite, cliquez sur le bouton en haut à droite pour enregistrer. Vous pouvez maintenant cliquer sur votre serveur pour accéder à vos applications :





Impression

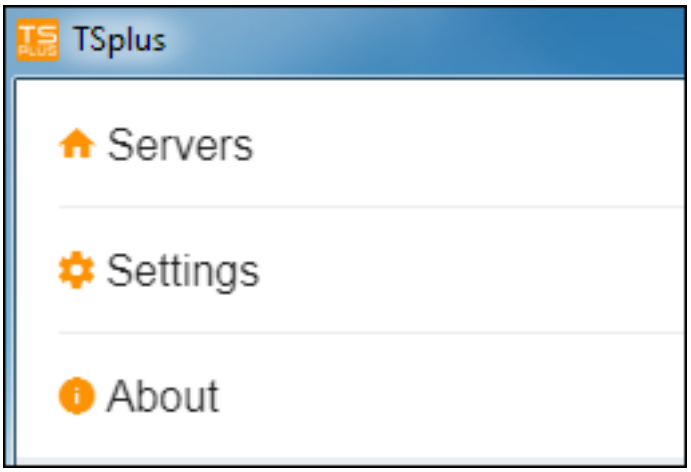
Imprimez facilement sur votre imprimante locale en utilisant le Imprimante universelle .

Depuis la version 11.40 de l'application TSplus, les documents imprimés s'ouvrent avec l'application de lecteur PDF par défaut.

Paramètres et version

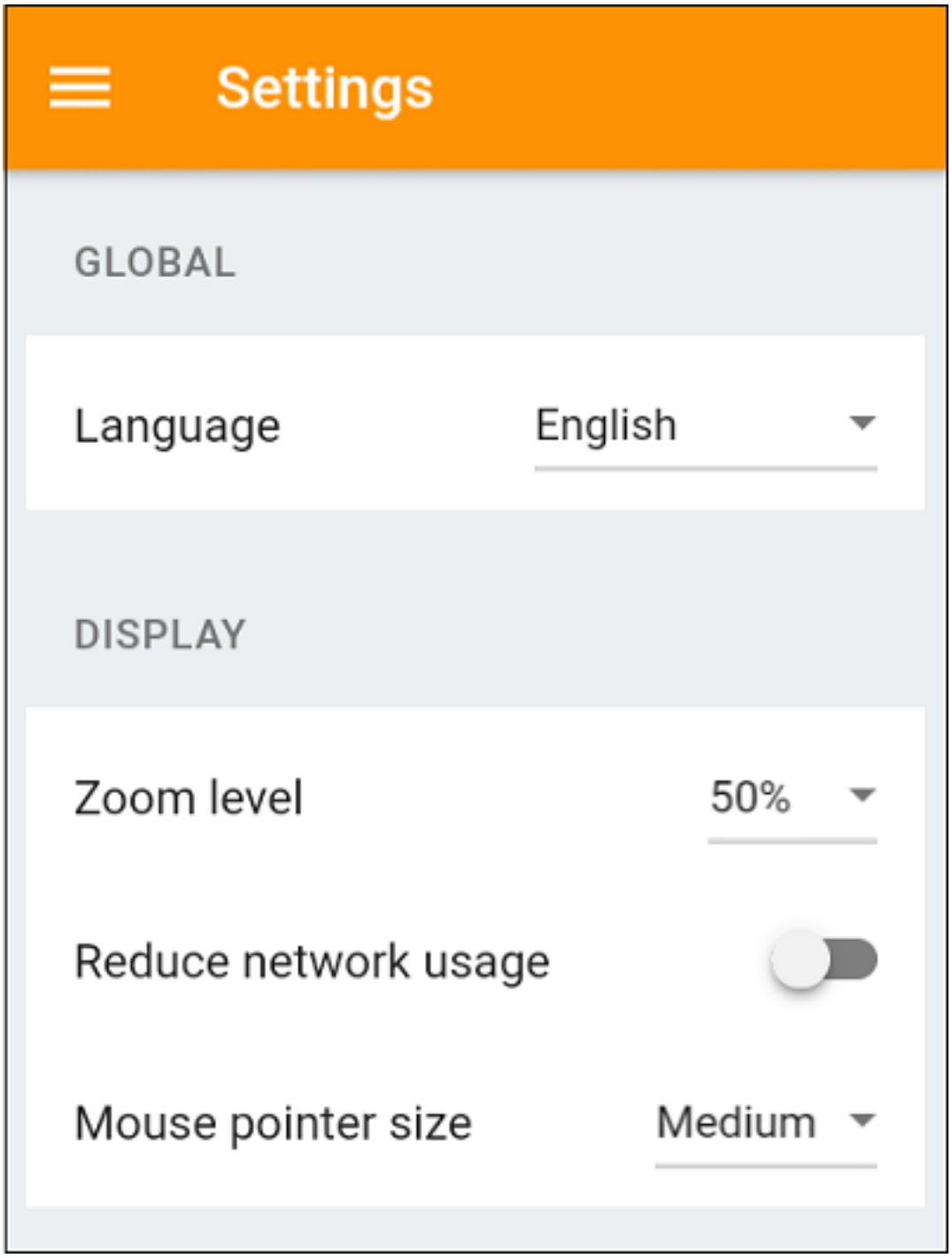
Sous le menu en haut à gauche, vous pouvez :

- Gérez vos serveurs
- Gérez vos paramètres
- Voir les informations légales dans la section À propos, et votre version de l'application TSplus.



Paramètres

Différentes options sont disponibles dans la fenêtre des paramètres :



- Vous pouvez changer la langue.
- Modifiez les paramètres d'affichage en changeant le niveau de zoom à votre convenance, réduisez l'utilisation du réseau ou choisissez entre 3 tailles de pointeur de souris : petit, moyen ou grand.

Authentification 2FA

L'application Android est compatible avec 2FA.

L'application demande le code 2FA si le compte utilisateur a été configuré pour utiliser 2FA.

L'activation ne peut pas être effectuée depuis l'application mobile, vous devez d'abord configurer 2FA depuis le portail web.

Version

Sur l'onglet À propos, vous pouvez voir les informations légales ainsi que votre version actuelle de l'application TSplus :



TSplus App

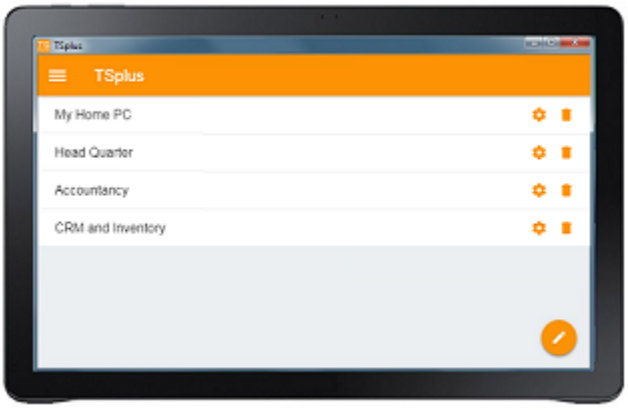
L'application TSplus vous permet de vous connecter à votre serveur TSplus depuis n'importe quel appareil, n'importe où !

Tout comme TSplus, il fournit des connexions à distance rapides et stables depuis des tablettes et des smartphones vers des bureaux Windows et des applications professionnelles.

Accédez à vos applications et données professionnelles en temps réel et imprimez facilement tout document et photo dont vous avez besoin sur l'imprimante locale la plus proche.

L'application TSplus est compatible avec 2FA.





Pour plus d'informations et des liens de téléchargement, rendez-vous sur la page de l'application de notre site web.

Exigences matérielles et systèmes d'exploitation

L'application TSplus est disponible sur mobiles et tablettes avec les systèmes d'exploitation suivants : iOS, Android à partir de la version 4.4 et Linux.

version Android

version iOS

Pré-requis

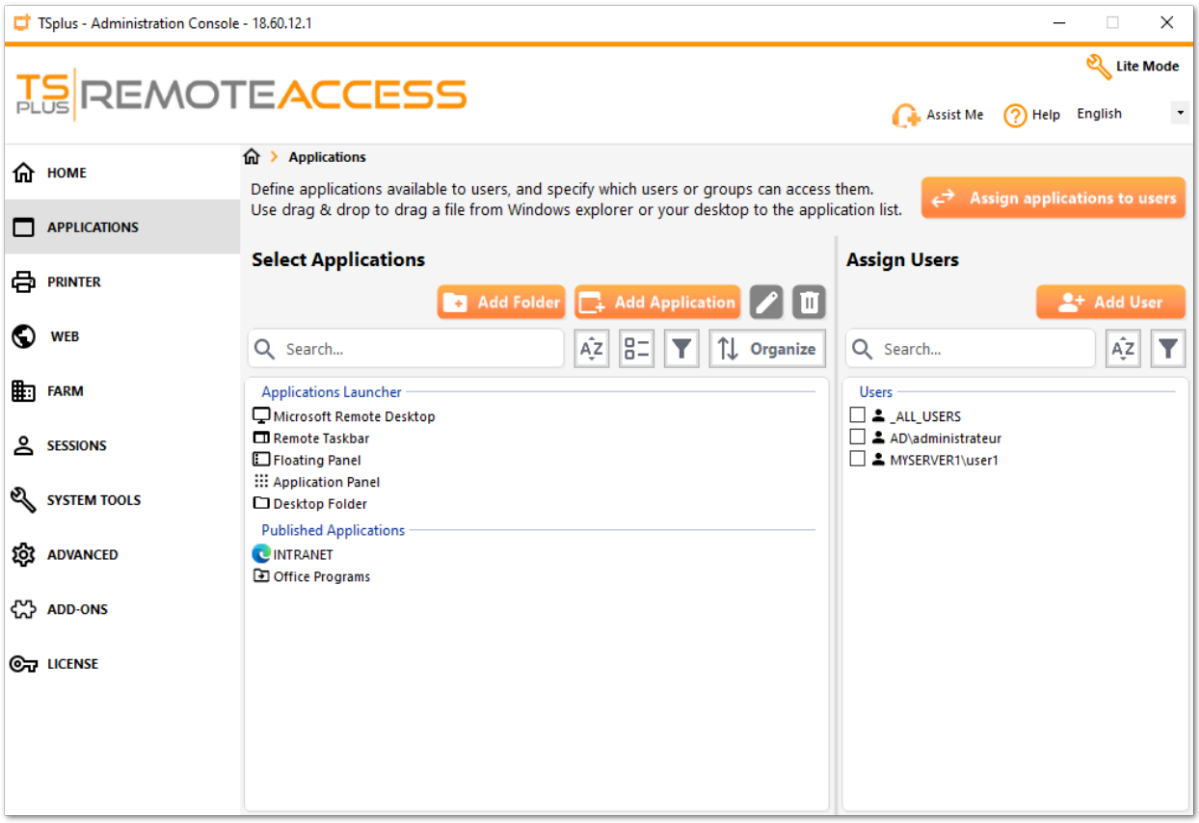
- Le site hôte doit être un système TSplus Mobile Web ou Enterprise.
- La version 11.30 (et supérieure) doit être installée sur cet hôte.

Affectation d'applications aux utilisateurs ou groupes

Une fois que vous avez publié certaines applications vous pouvez les attribuer à un ou plusieurs utilisateurs et/ou groupes.

Affecter des utilisateurs ou des groupes à des applications

Chaque affectation doit être effectuée dans le panneau de droite de la section « Applications » de l'AdminTool. Ce panneau de droite affiche tous les utilisateurs et groupes ayant actuellement des applications assignées.

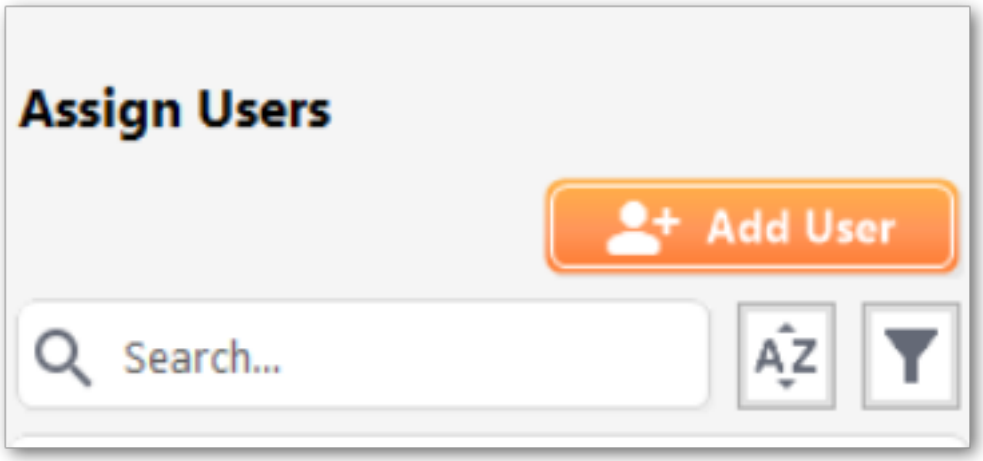


Pour attribuer des utilisateurs ou des groupes, vous devrez d'abord ajouter les utilisateurs/

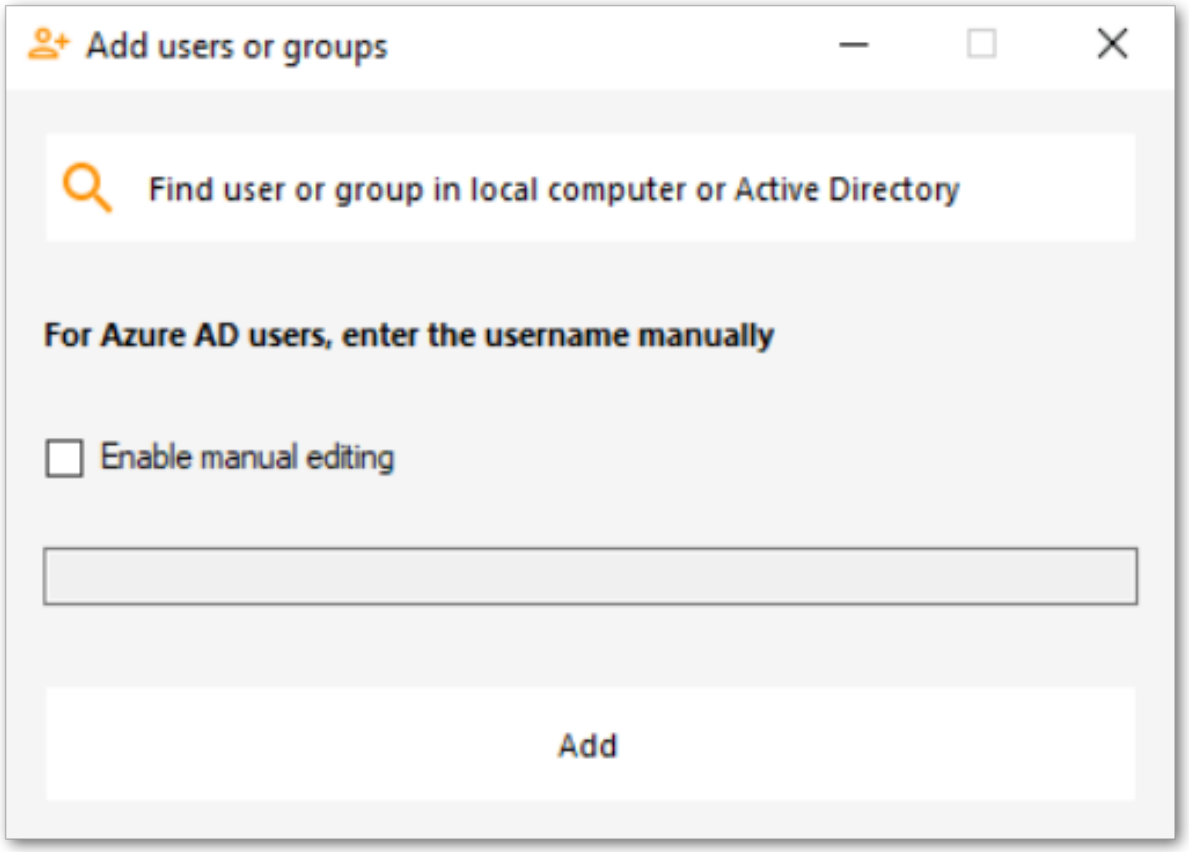
groupes pour lesquels vous souhaitez attribuer l'application.

Ajouter des utilisateurs ou des groupes

Pour ajouter des utilisateurs ou des groupes, cliquez sur les icônes de bouton « Ajouter un utilisateur ».



Vous serez accueilli avec cette interface, vous permettant soit de trouver un utilisateur ou un groupe via le sélecteur d'utilisateur/groupe, soit d'écrire directement le nom de l'utilisateur/groupe que vous souhaitez ajouter.
Les utilisateurs locaux ou Active Directory doivent être sélectionnés à l'aide du bouton Trouver des utilisateurs ou groupes locaux ou Active Directory.
Seuls les utilisateurs externes peuvent être saisis directement dans la zone de texte.



Le nom d'utilisateur spécial _ALL_USERS

Dans la liste des utilisateurs, vous trouverez toujours l'utilisateur “_ALL_USERS” disponible. Cet utilisateur n'est pas un utilisateur Windows, mais un utilisateur virtuel. Si vous sélectionnez une application et cochez le nom d'utilisateur “_ALL_USERS”, alors l'application sera disponible pour tous les utilisateurs.

Affecter des utilisateurs ou des groupes à des applications

Une fois que les utilisateurs ont été ajoutés, assignez-leur des applications en :

1. sélectionner dans le panneau de gauche les applications que vous souhaitez attribuer à votre utilisateur
2. vérifier dans le panneau de droite la case à cocher à côté de son nom d'utilisateur pour attribuer les applications sélectionnées à cet utilisateur

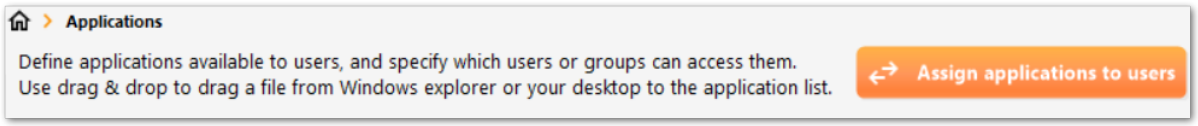
Ex : si je veux attribuer le bloc-notes à l'utilisateur "benjamin", il suffit de sélectionner l'application "bloc-notes" à gauche et de cocher la case à côté du nom d'utilisateur "benjamin" à droite.

Pour désaffecter des utilisateurs, il suffit de décocher la case à côté du nom de l'utilisateur.

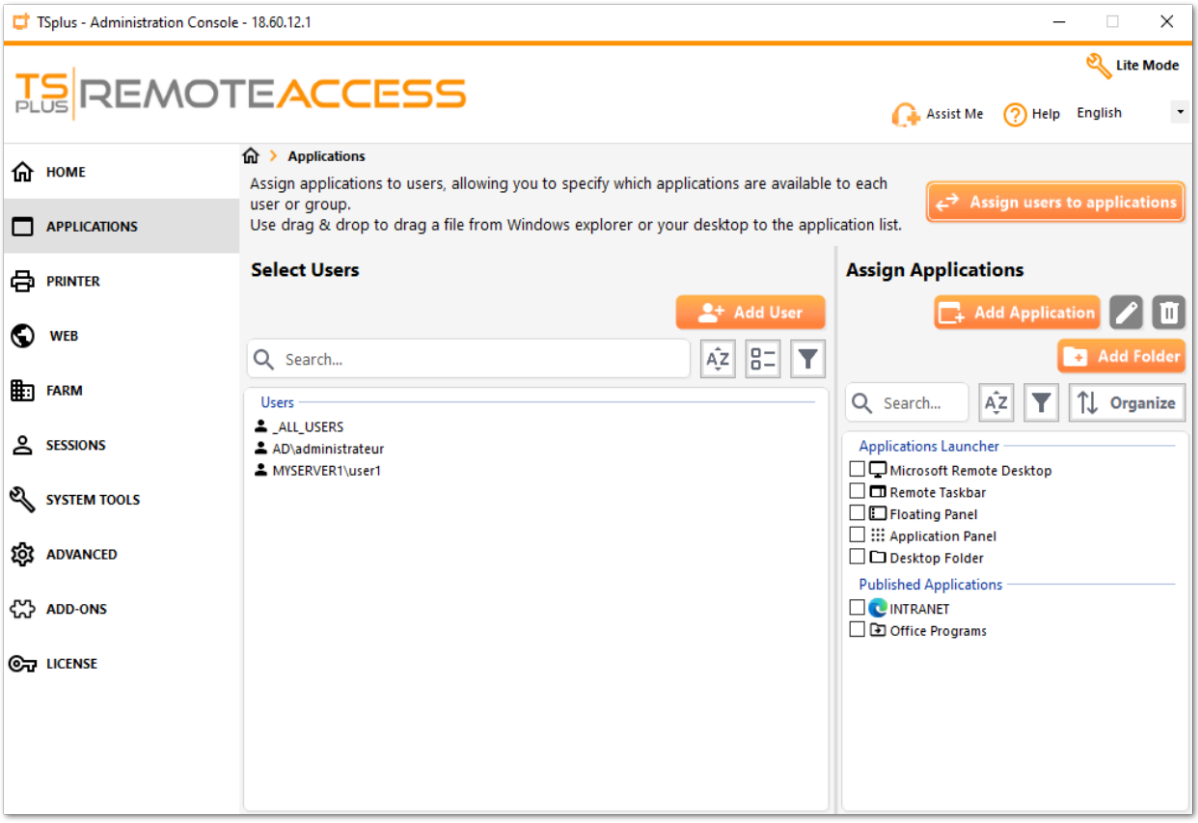
Cette action prend en charge la sélection multiple
Cela signifie que vous pouvez sélectionner plusieurs applications et que vous n'avez pas à attribuer les applications une par une.

Attribuer des applications à des utilisateurs ou des groupes

Si vous préférez sélectionner des utilisateurs ou des groupes et leur attribuer des applications, vous pouvez le faire en cliquant sur « Attribuer des applications aux utilisateurs ».



Cela fera pivoter le panneau latéral gauche et droit.



Après avoir cliqué sur le bouton, afin d'assigner des applications aux utilisateurs :

1. sélectionner dans le panneau de gauche les utilisateurs ou groupes que vous souhaitez attribuer à votre application
2. vérifiez dans le panneau de droite la case à cocher à côté du nom de votre application pour

attribuer les utilisateurs ou groupes sélectionnés à cette application

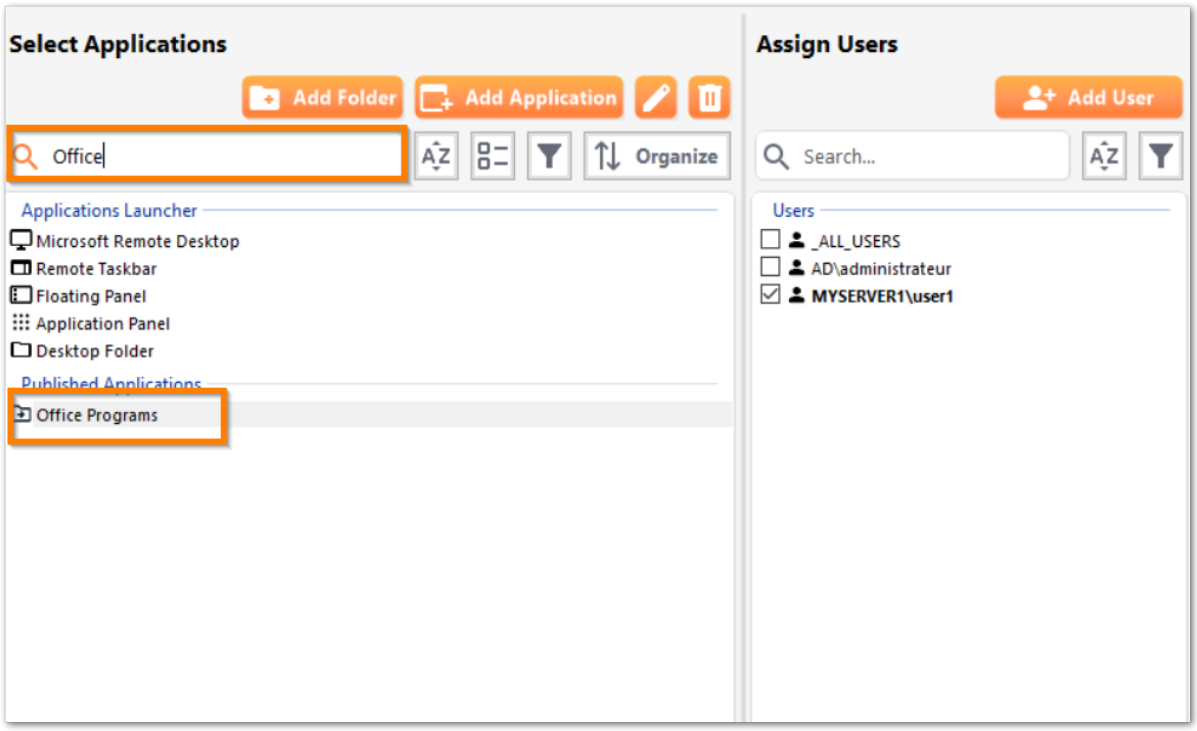
Ex : si je veux attribuer le bloc-notes à l'utilisateur "benjamin", il suffit de sélectionner l'utilisateur "benjamin" à gauche et de cocher la case à côté du nom de l'application "bloc-notes" à droite.

Pour désaffecter des applications, il suffit de décocher la case à côté du nom de l'application.

Cette action prend en charge la sélection multiple
Cela signifie que vous pouvez sélectionner plusieurs utilisateurs et que vous n'avez pas à attribuer les utilisateurs un par un.

Rechercher et filtrer

Pour faciliter la gestion de l'attribution des utilisateurs, une barre de recherche est disponible ainsi qu'un bouton de filtrage, vous permettant d'afficher uniquement les utilisateurs ou uniquement les groupes.

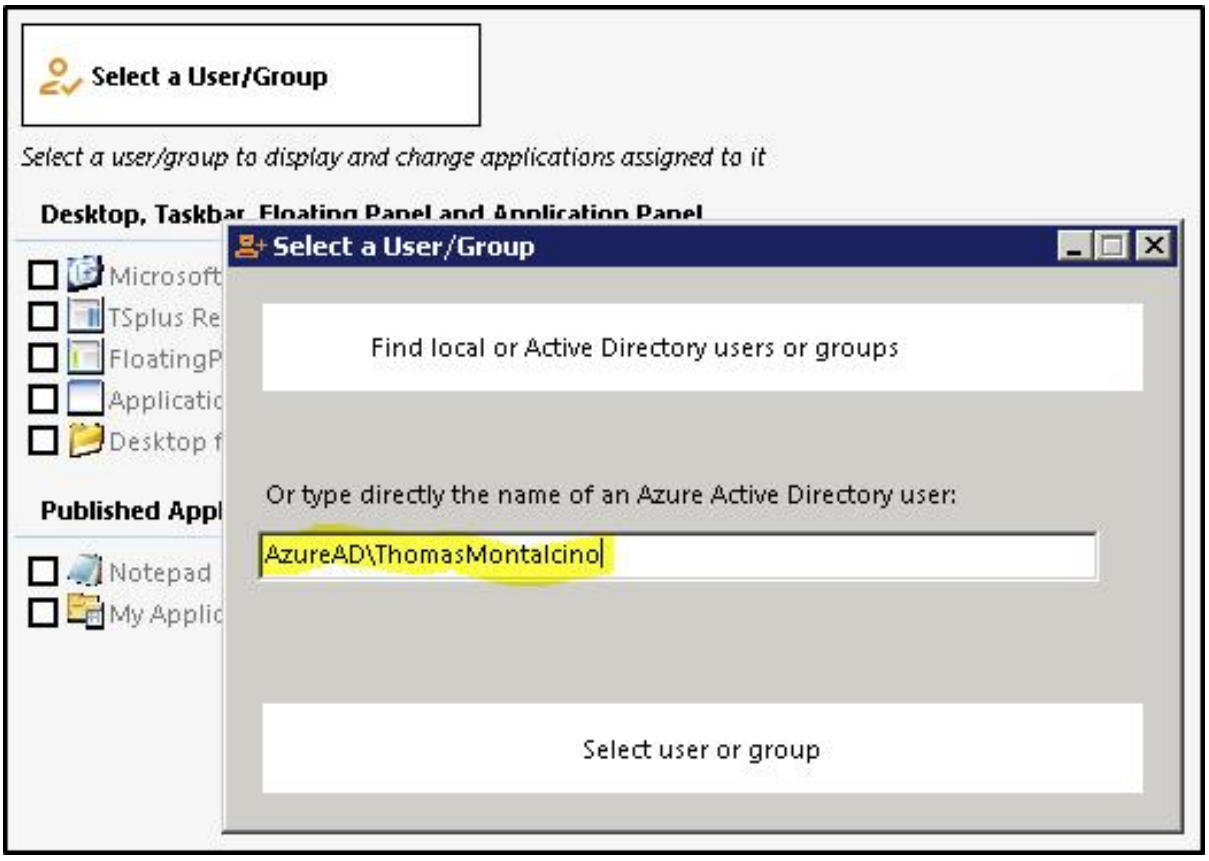


Vous pouvez également utiliser le bouton de filtre afin que seules les applications (ou les utilisateurs) assignés/non assignés soient affichés.
Cela vous aidera à gérer vos affectations au cas où vous auriez soit de nombreux utilisateurs ayant des applications assignées, soit simplement de nombreuses applications publiées.

Affectation d'applications aux utilisateurs avec Azure Active Directory

Aperçu

Pour attribuer un utilisateur Azure Active Directory à une application depuis AdminTool > Applications > Utilisateurs :



Les utilisateurs locaux ou Active Directory doivent être sélectionnés en utilisant le bouton Trouver des utilisateurs ou groupes locaux ou Active Directory. Seuls les utilisateurs externes peuvent être saisis directement dans la zone de texte.

Gestion du serveur Web intégré

Votre serveur de bureau à distance doit être disponible, facile d'accès et sûr. C'est pourquoi TSplus utilise un serveur Web intégré qui vous aide à gérer facilement son statut et ses opérations.

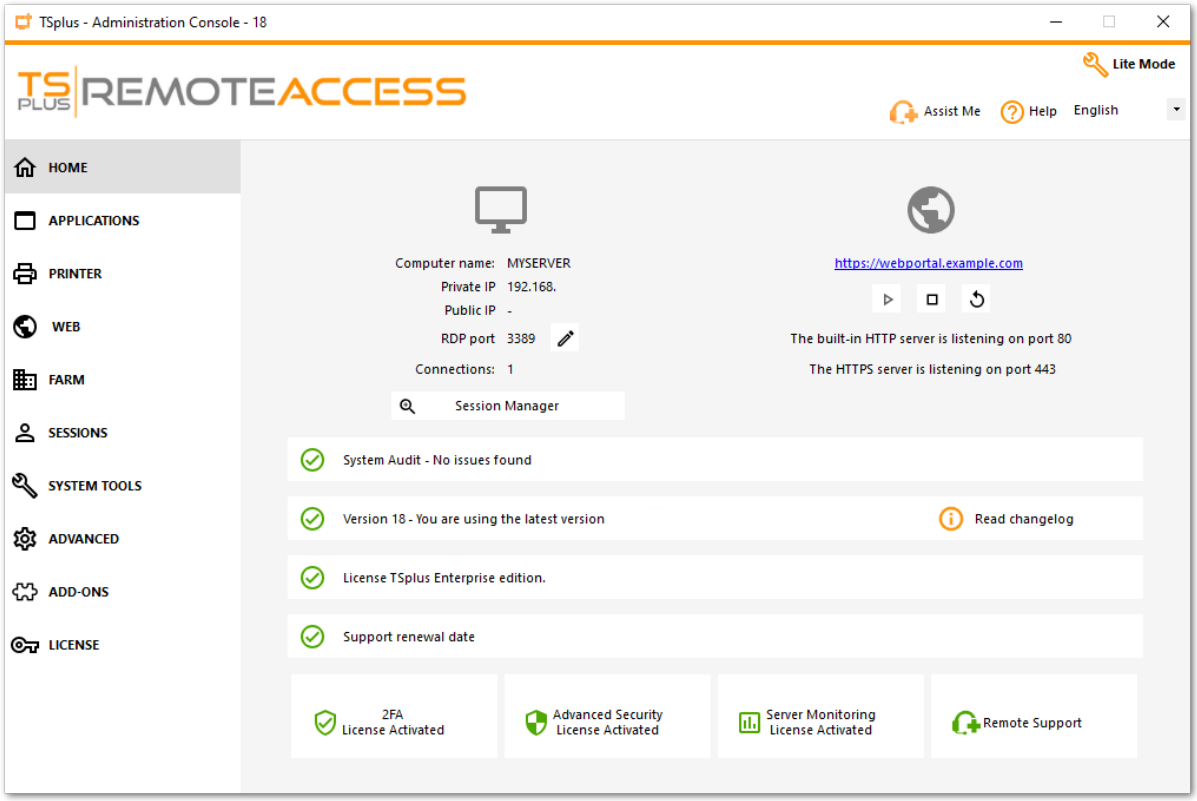
Une console de gestion est disponible dans l'outil Administrateur. Cette console de gestion vous permet de visualiser et de configurer l'état du serveur Web intégré de Terminal Service Plus.

Lorsque vous installer TSplus Les serveurs web écoutent sur les ports 80 et 443 par défaut. Assurez-vous que les ports définis sont disponibles et que Java est installé sur le serveur.

Voir la vidéo à propos des fonctionnalités Web.

État des composants du serveur Web

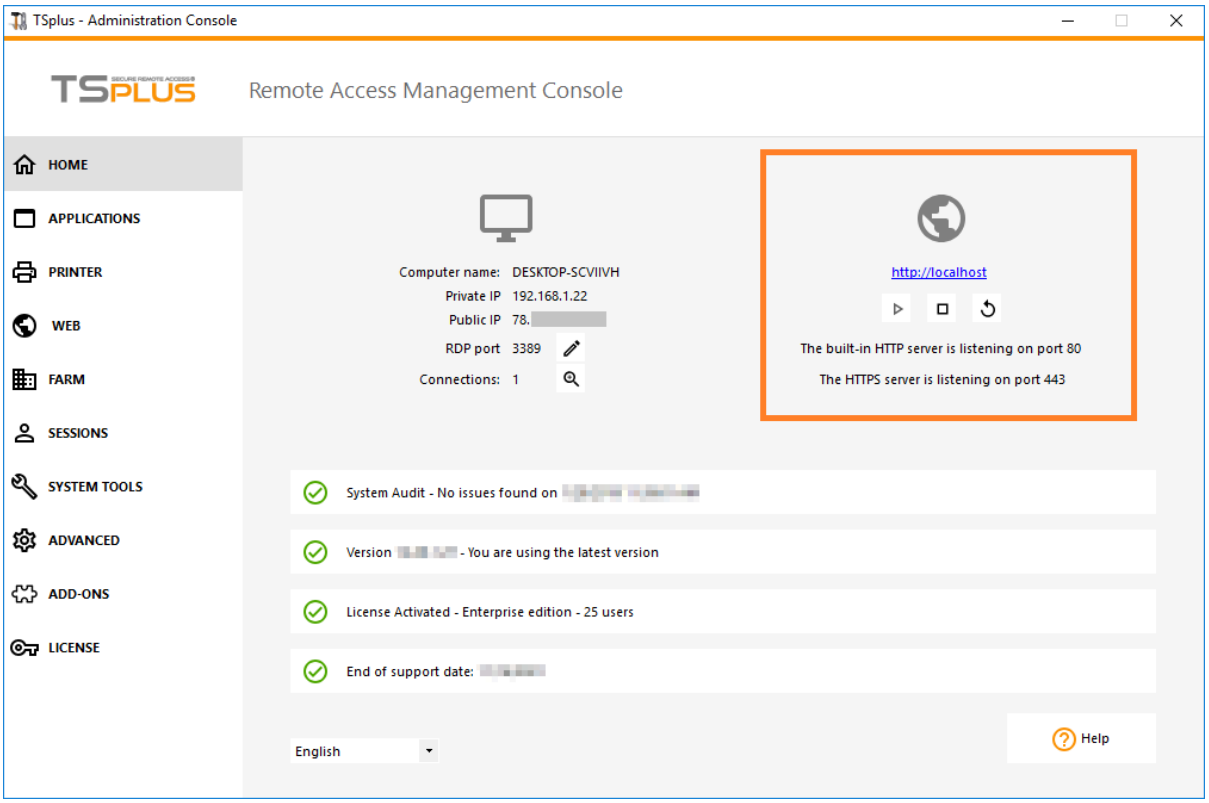
L'état des principaux composants du serveur Web est affiché sur le tableau de bord d'accueil de l'AdminTool.



Considérations sur les ports (machine locale et pare-feu / routeur)

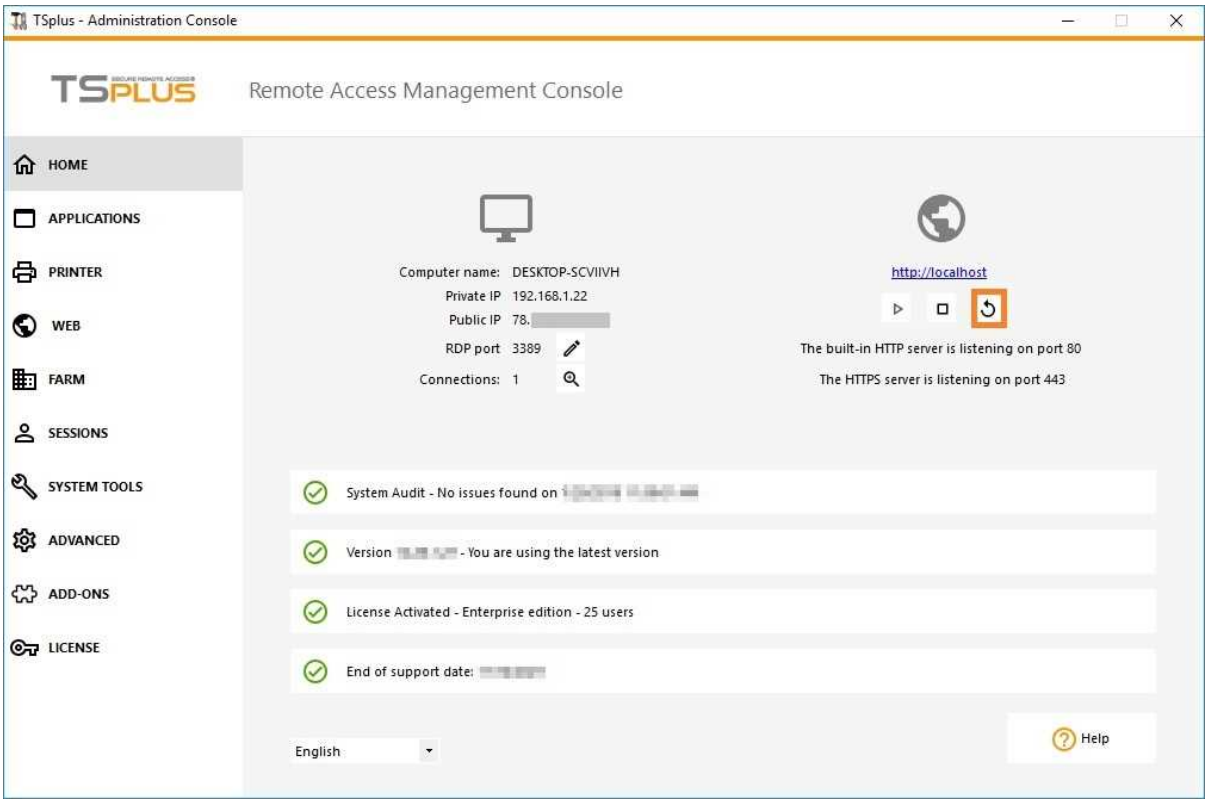
Terminal Service Plus nécessite uniquement l'ouverture du Port 80 ou du Port 443.

Le port 3389 peut rester fermé.

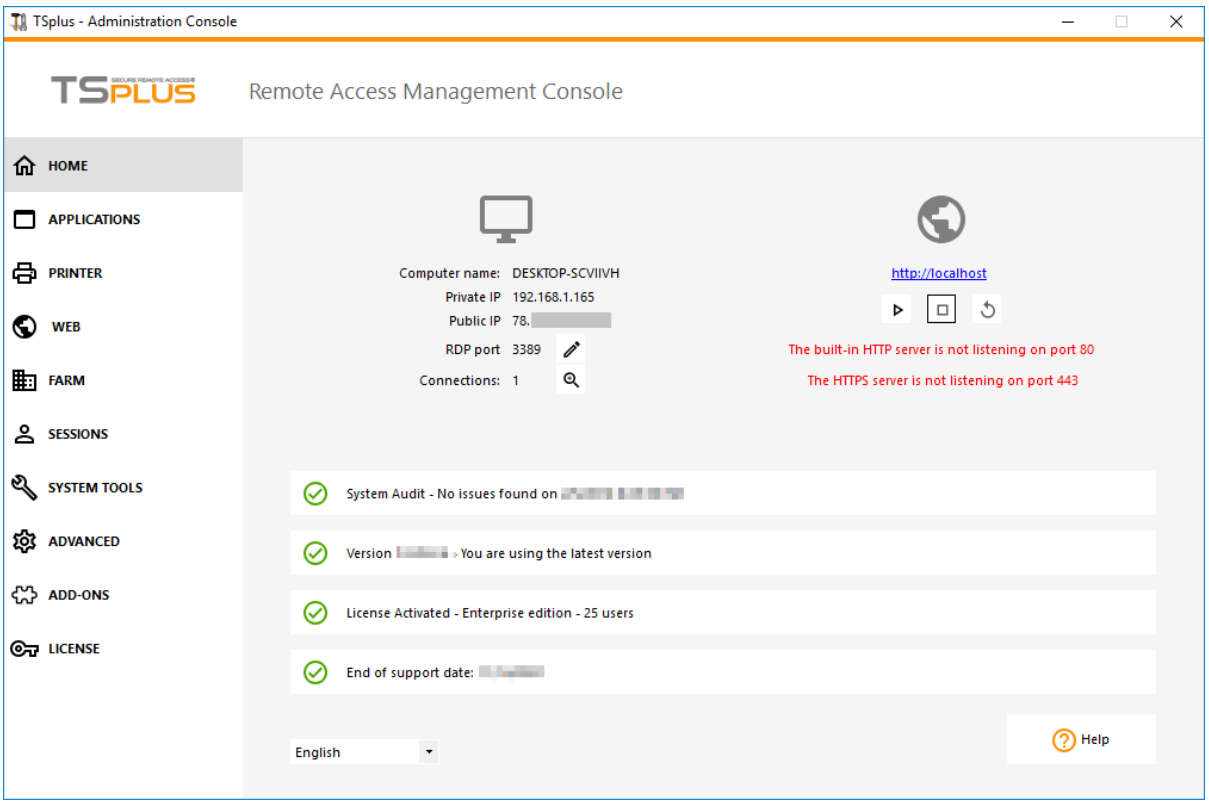


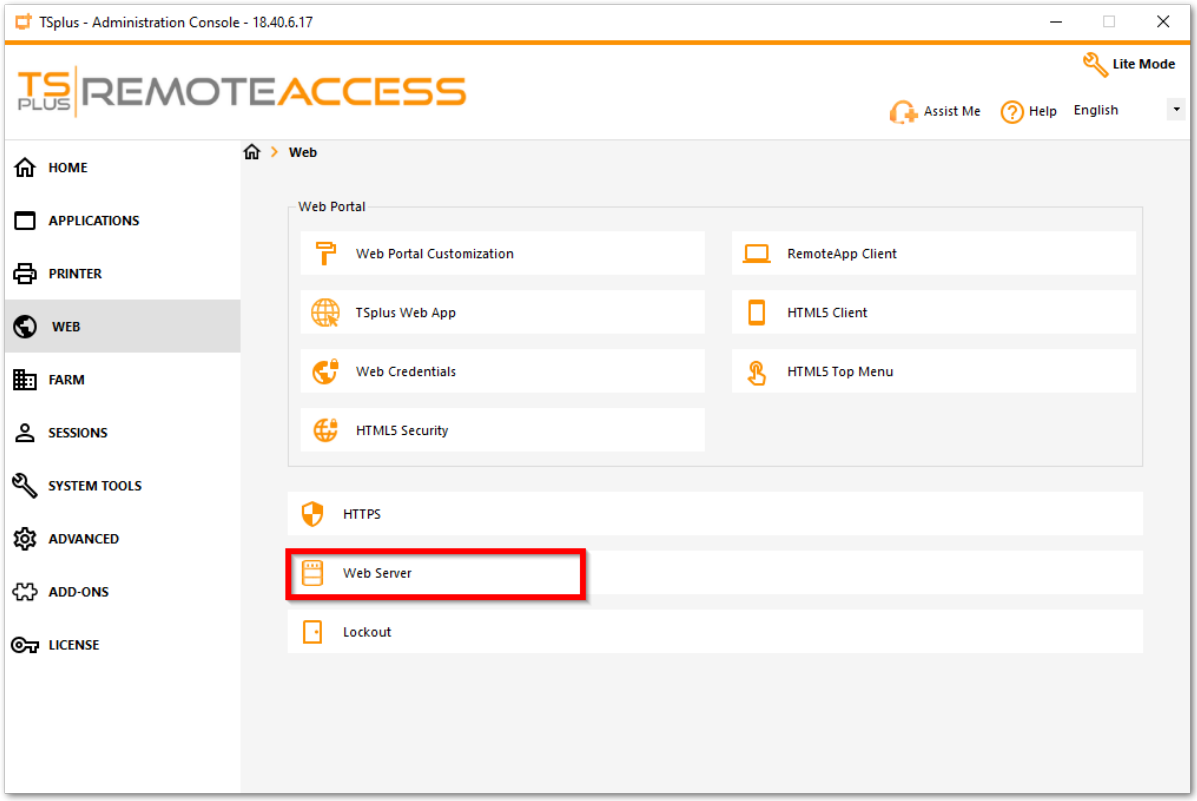
Redémarrer / Arrêter le service Web Server

Si vous constatez qu'un service ne fonctionne pas, vous devrez peut-être redémarrer les serveurs Web en cliquant sur le bouton « Redémarrer les serveurs Web » qui est représenté par une flèche à droite, les serveurs Web seront redémarrés et le service devrait fonctionner à nouveau.



Si vous cliquez sur le bouton « Arrêter les serveurs Web », situé au milieu, les serveurs Web seront arrêtés. L'état du serveur HTTP et HTTPS s'affichera maintenant en rouge, indiquant que les services HTTP / HTTPS sont arrêtés.





Vous pouvez changer les ports pendant l'installation ou à tout moment en cliquant sur l'onglet Web - Serveur Web. Sur cet onglet, vous pouvez choisir d'utiliser un serveur web HTTP différent, modifier le chemin racine du serveur Web et les numéros de port HTTP/HTTPS. Assurez-vous que ces ports sont disponibles avant de les changer : si un conflit se produit, le serveur web TSplus ne fonctionnera pas. Ici est une liste non exhaustive de ports TCP qui pourraient être utilisés par une application sur votre serveur. Une fois ces modifications effectuées, cliquez sur enregistrer et l'AdminTool redémarrera.

###Désactiver uniquement http ou http sur https

Voir cette documentation pour plus d'informations sur ce sujet.

Pour des informations plus approfondies sur **personnalisation des serveurs** et **préférences** voir ces pages :

Personnalisation du portail Web , Portail des applications Web , Identifiants Web .

Choisir vos suites de chiffrement pour améliorer la sécurité

Aperçu

TLS/SSL, la sécurité derrière HTTPS, peut utiliser plusieurs algorithmes différents pour sécuriser, chiffrer et authentifier une connexion.

Le choix de l'algorithme à utiliser est décidé par un accord entre le serveur et le client, en fonction des algorithmes disponibles de chaque côté.

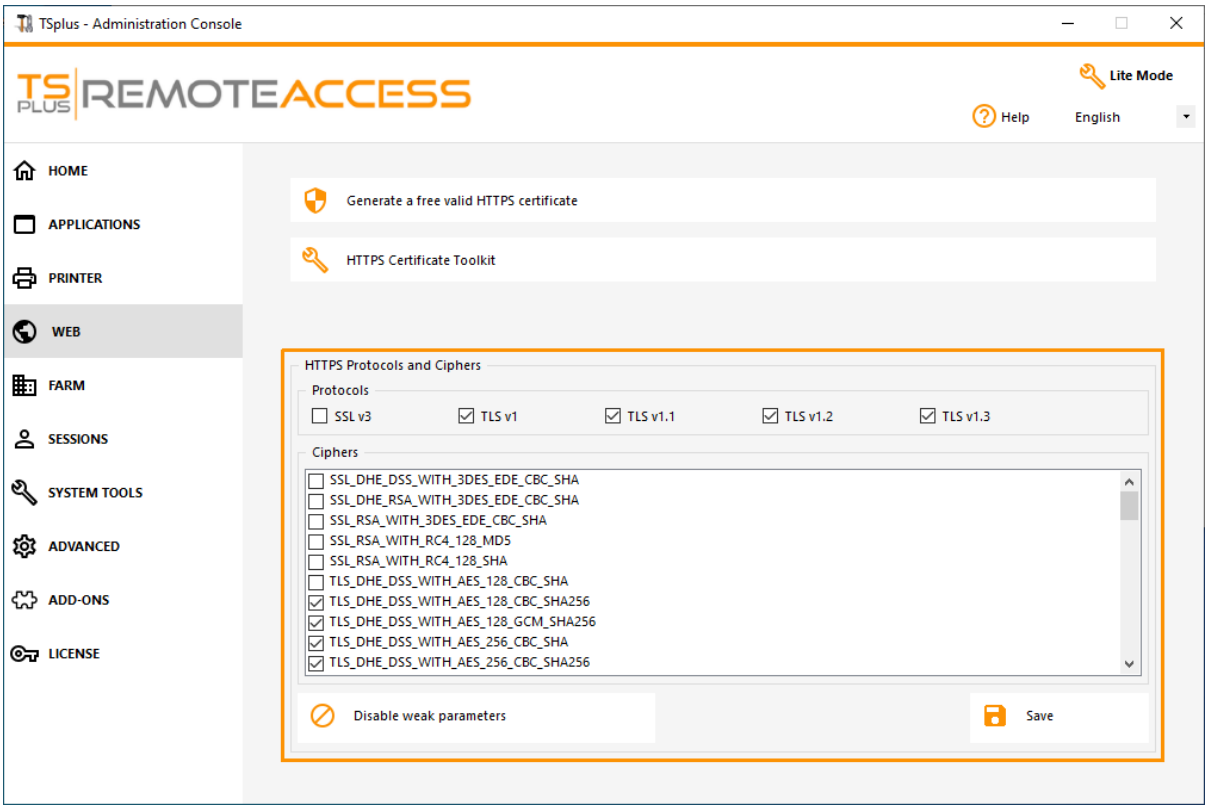
Un ensemble de chiffrement est une combinaison nommée d'algorithmes d'authentification, de chiffrement, d'authentification de message et d'échange de clés.

Le serveur Terminal Service Plus peut gérer de nombreuses suites de chiffrement différentes. Certaines d'entre elles sont plus sécurisées que d'autres, mais certains anciens navigateurs peuvent nécessiter des algorithmes relativement faibles pour se connecter.

C'est la raison pour laquelle Terminal Service Plus vous permet de choisir les suites de chiffrement que vous souhaitez activer. Bien sûr, Terminal Service Plus dispose également d'un paramètre facile pour désactiver les algorithmes les plus faibles, renforçant ainsi la sécurité de vos connexions.

Sélection des protocoles et des chiffres HTTPS

Pour voir la sélection des ciphers de Terminal Service Plus, ouvrez l'outil d'administration de Terminal Service Plus, cliquez sur l'onglet « Web - HTTPS », où vous verrez les protocoles et ciphers HTTPS :



Activer/Désactiver une suite de chiffrement

Vous pouvez facilement activer un ensemble de chiffrement en cochant sa case et désactiver un ensemble de chiffrement en la décochant.

Lorsque votre sélection est terminée, cliquez sur « Enregistrer ».

Cela enregistrera votre sélection et rechargera la nouvelle configuration dans le serveur web intégré de Terminal Service Plus. Votre nouvelle sélection de suites de chiffrement est immédiatement appliquée à chaque nouvelle connexion à votre serveur.

Sélection des suites de chiffrement recommandées

Nous recommandons à la plupart des administrateurs d'utiliser notre sélection de suites de chiffrement recommandées, en cliquant simplement sur le bouton « Désactiver les paramètres faibles » puis sur le bouton « Enregistrer ».

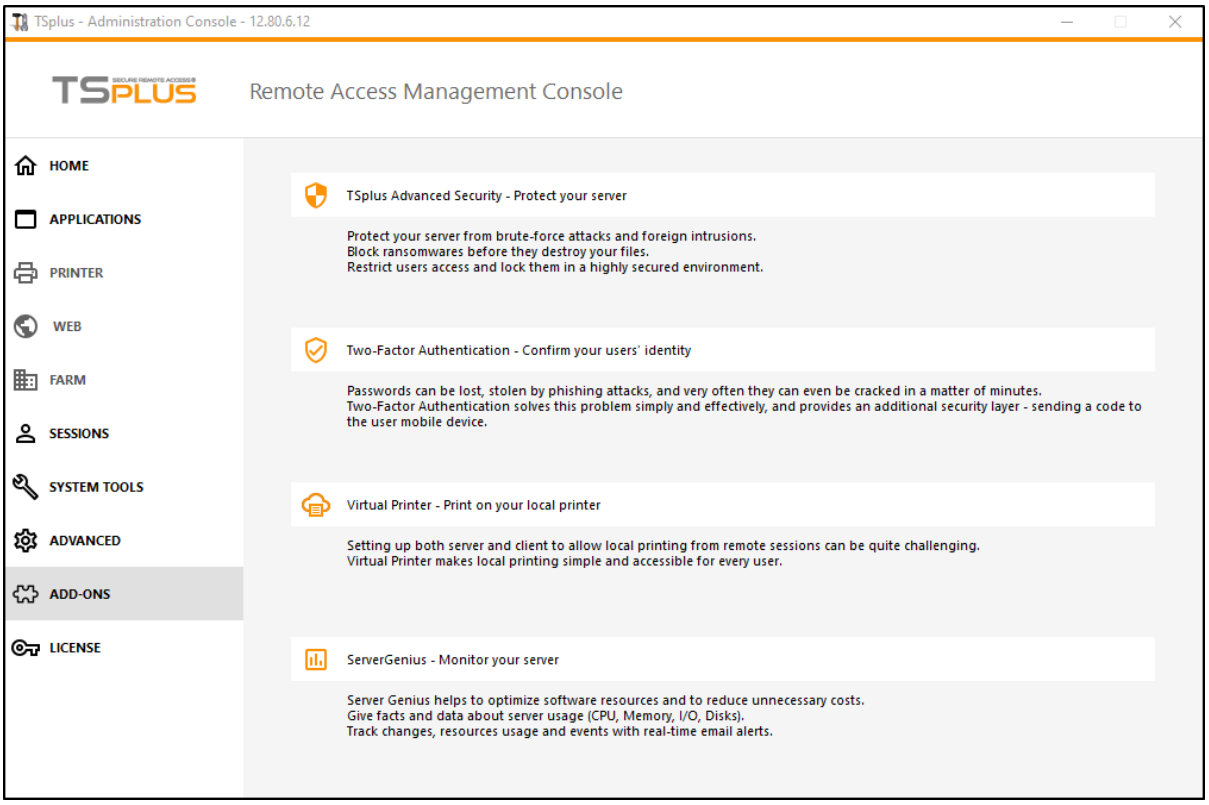
Cette action désactivera tous les ensembles de chiffrement qui sont actuellement connus pour être faibles.

Vous pouvez vérifier avec Outil de test en ligne SSL Labs sans ces suites de chiffrement faibles, vous devriez obtenir la note maximale : A !

Cliquez pour aider - Outil d'administration - Modules complémentaires

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

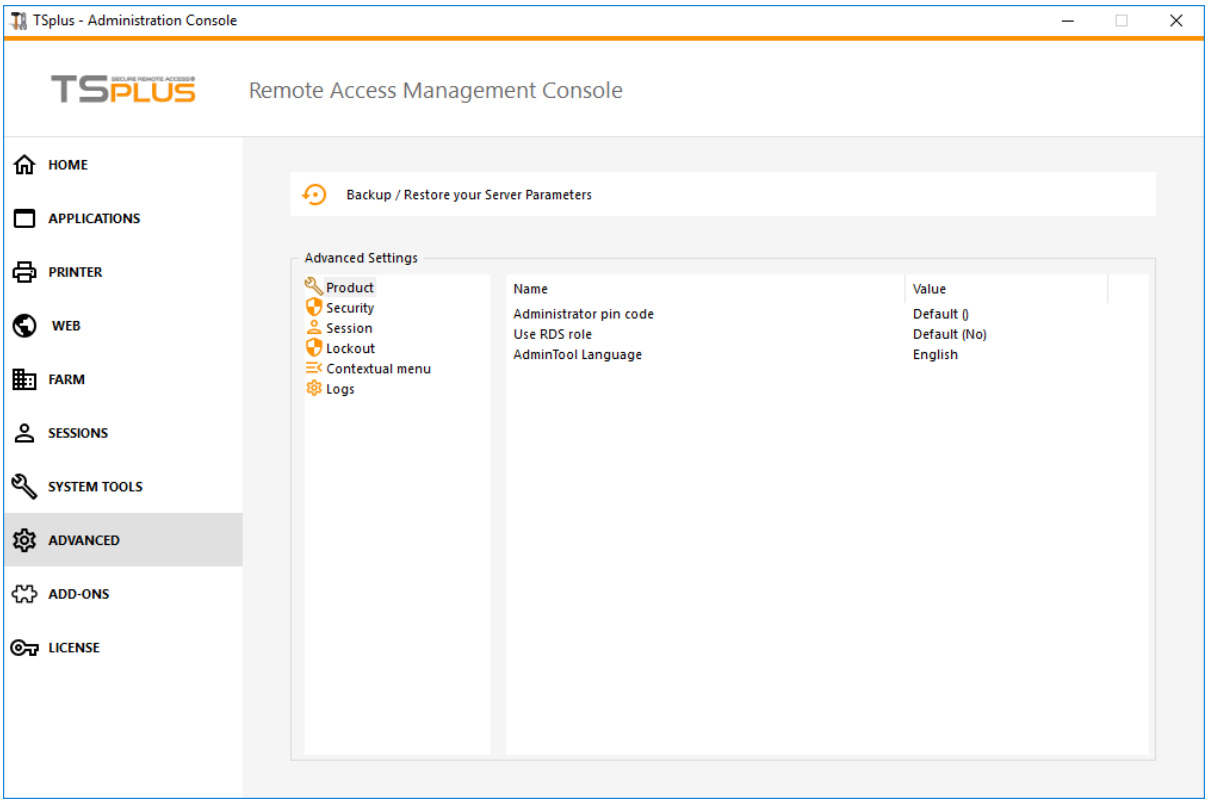
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Avancé

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

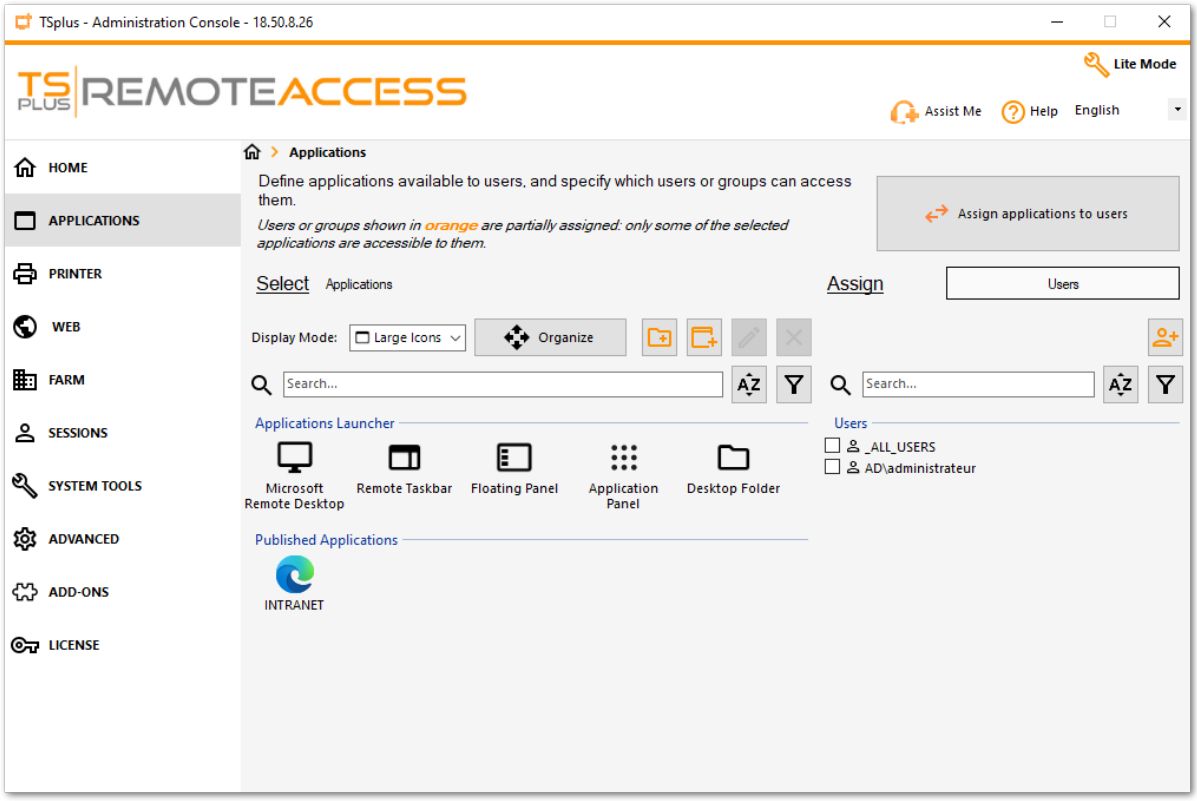
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Applications

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

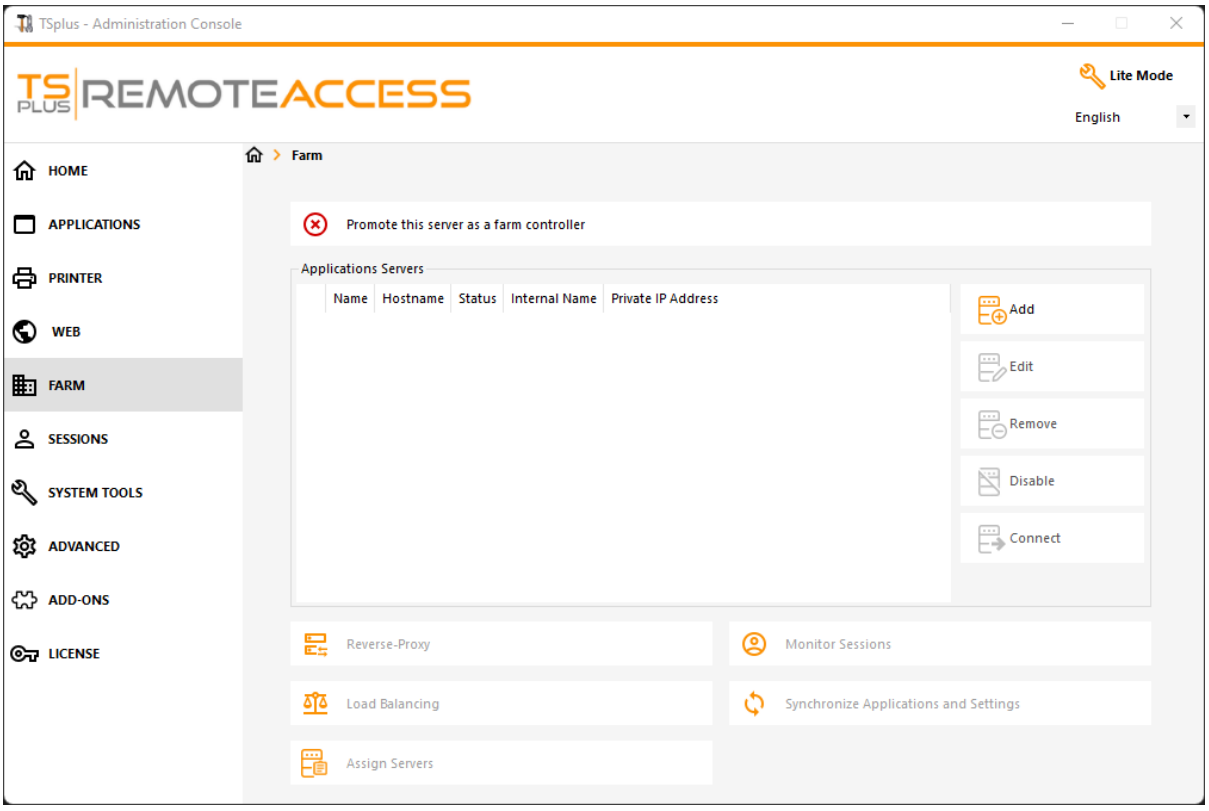
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Ferme

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

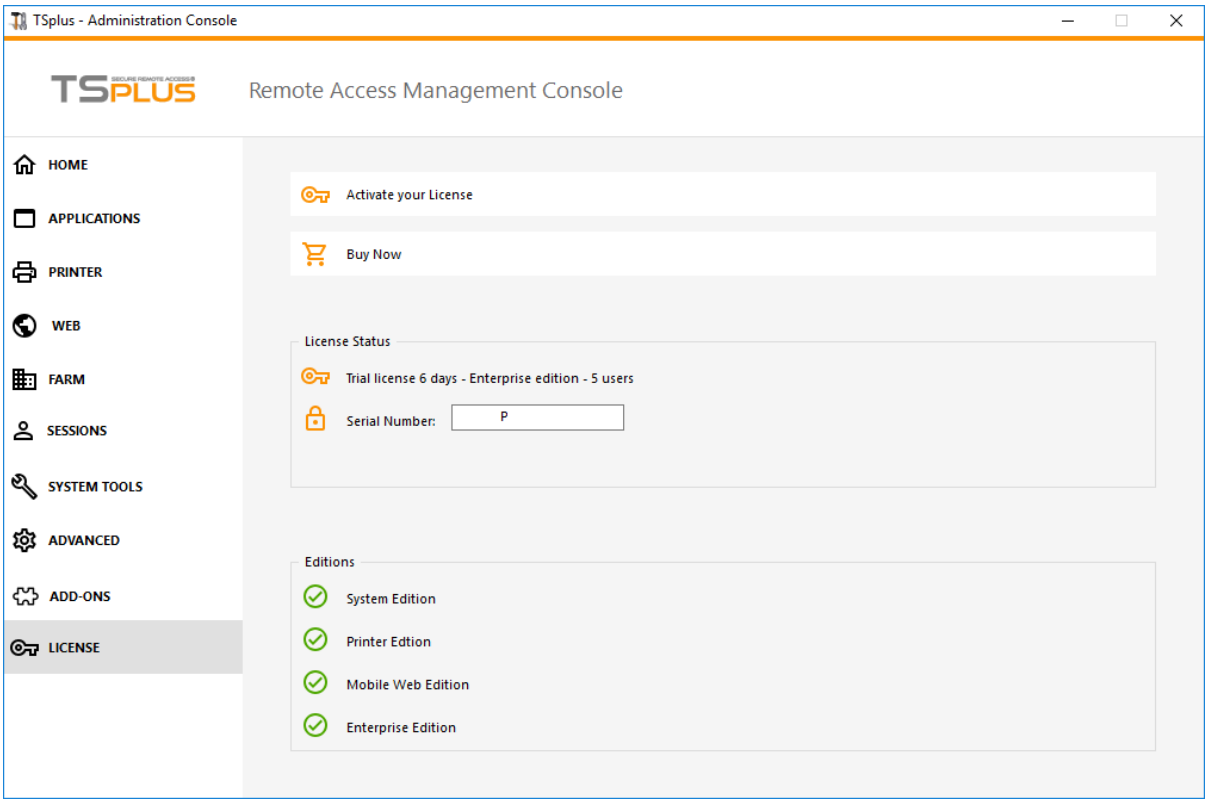
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Licence

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

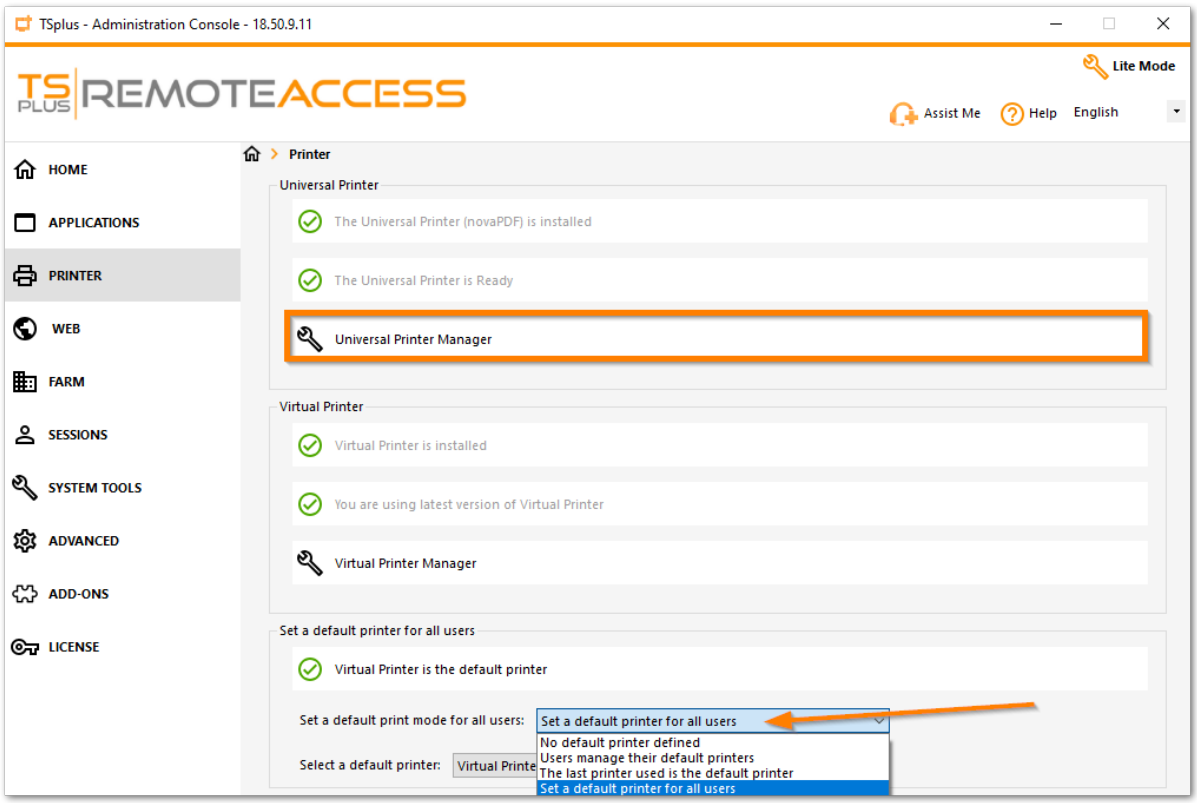
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Imprimante

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Sécurité

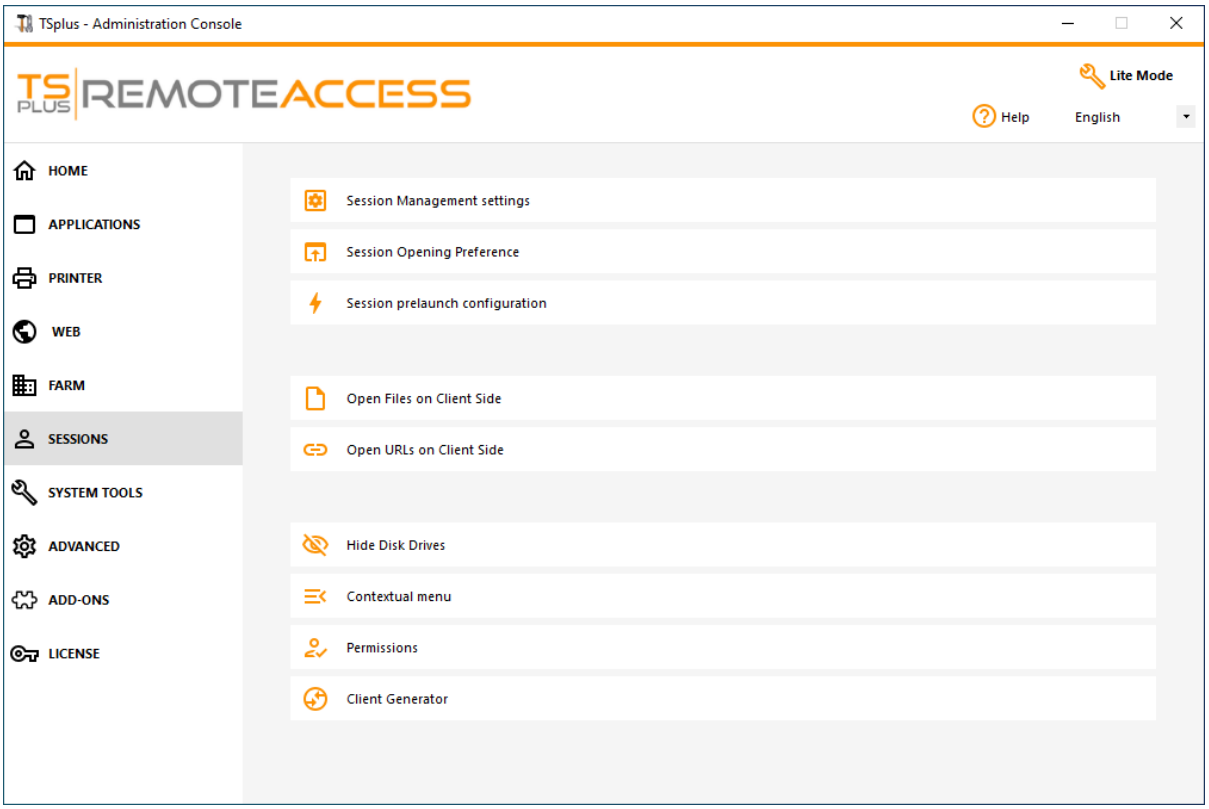
Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !

Cliquez pour aider - Outil d'administration - Sessions

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

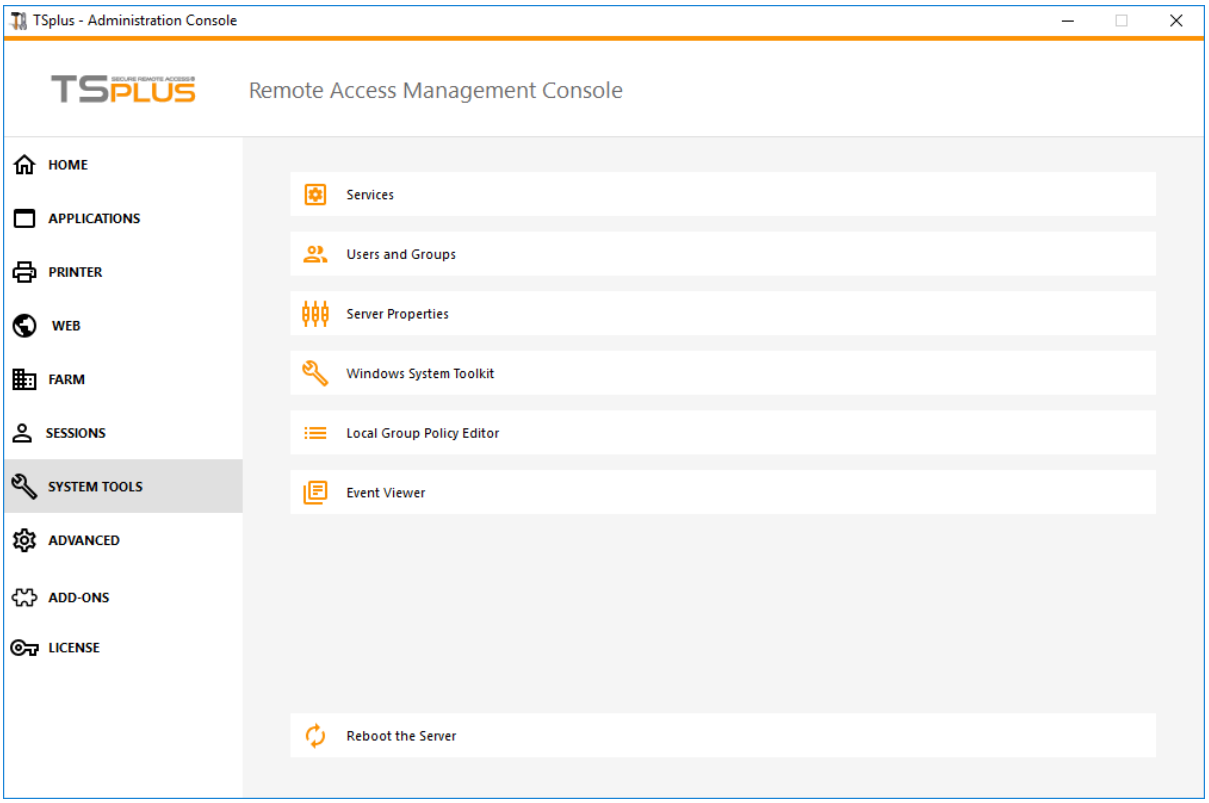
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Système

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

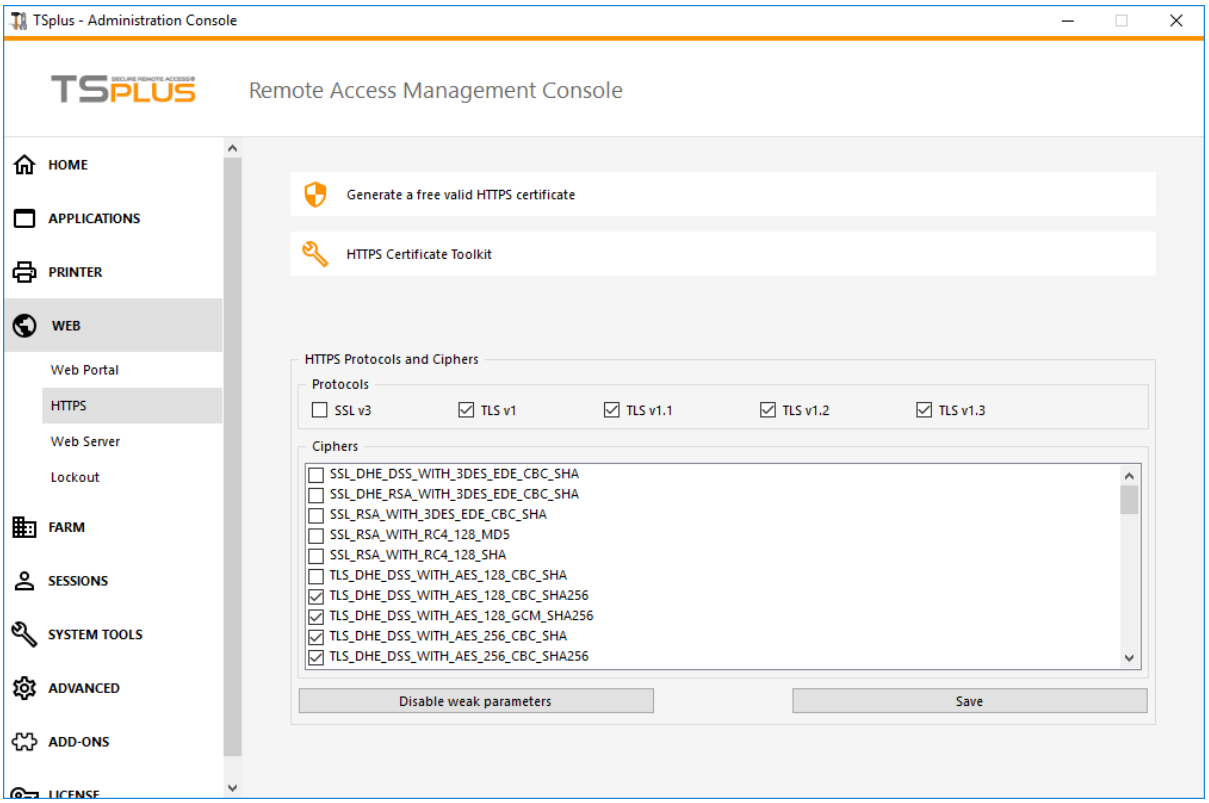
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Web

Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

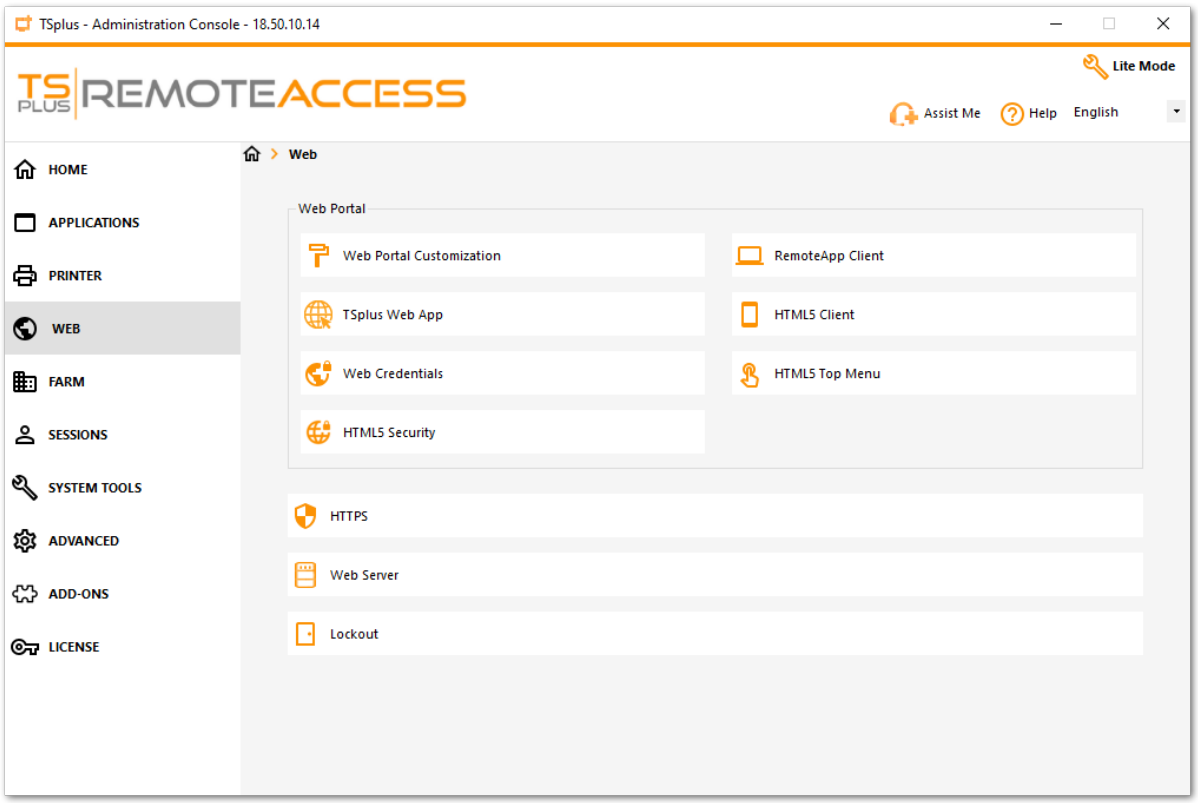
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !



Cliquez pour aider - Outil d'administration - Web

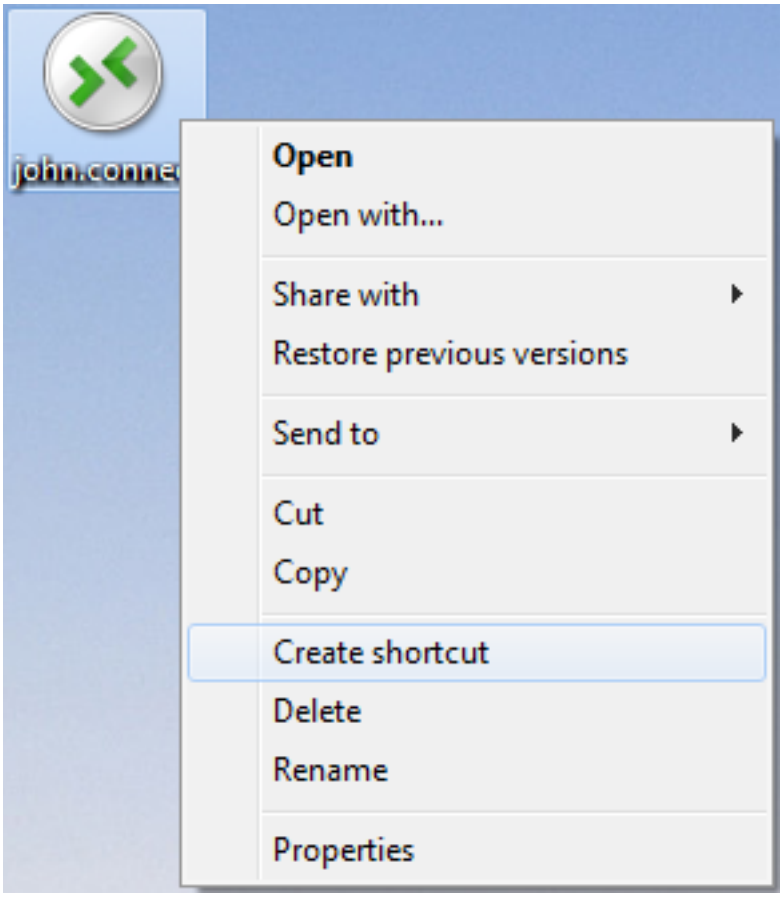
Voulez-vous obtenir rapidement de l'aide sur une fonctionnalité de l'outil d'administration Terminal Service Plus ?

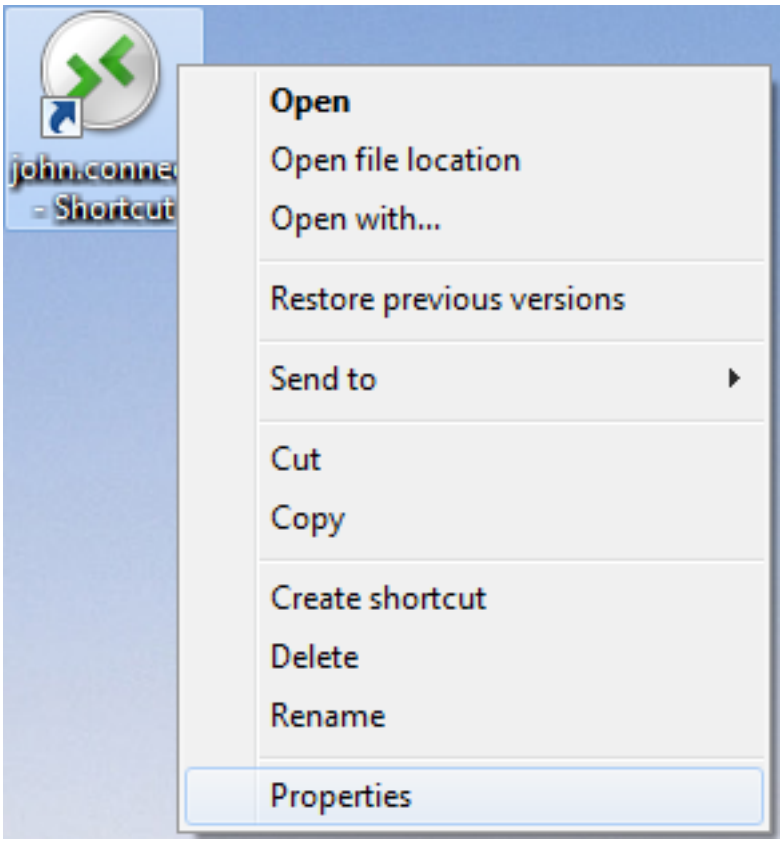
Just **cliquez sur une tuile ou sur un onglet** aller à l'aide correspondante !

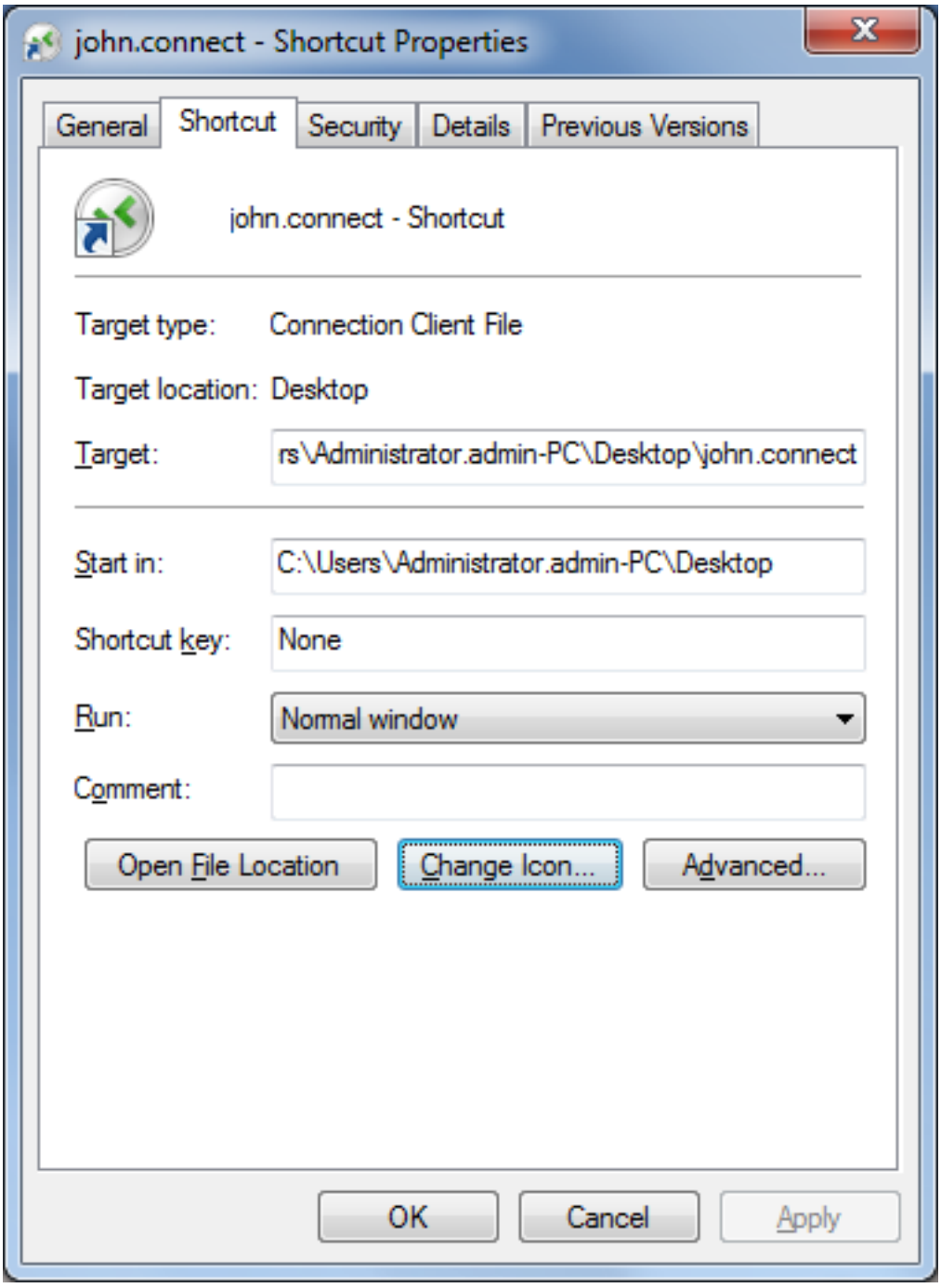


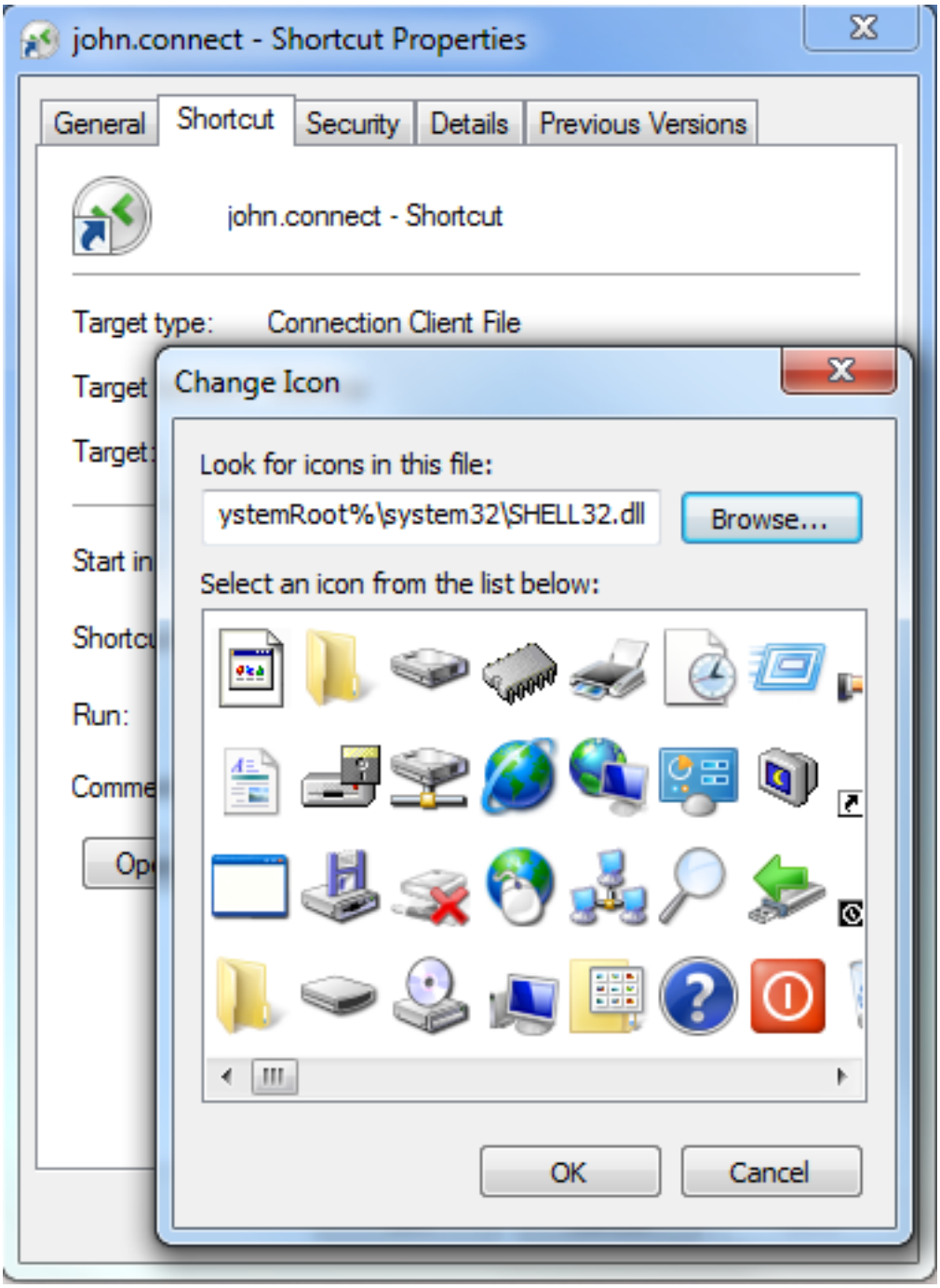
Comment modifier l'icône du client TSplus

Pour changer l'icône du client généré, il suffit de créer un raccourci du client et d'aller dans les propriétés du raccourci :




john.connec
- Shortcut
Open
Open file location
Open with...
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties


john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type: Connection Client File
Target location: Desktop
Target: rs\Administrator.admin-PC\Desktop\john.connect
Start in: C:\Users\Administrator.admin-PC\Desktop
Shortcut key: None
Run: Normal window
Comment:
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply

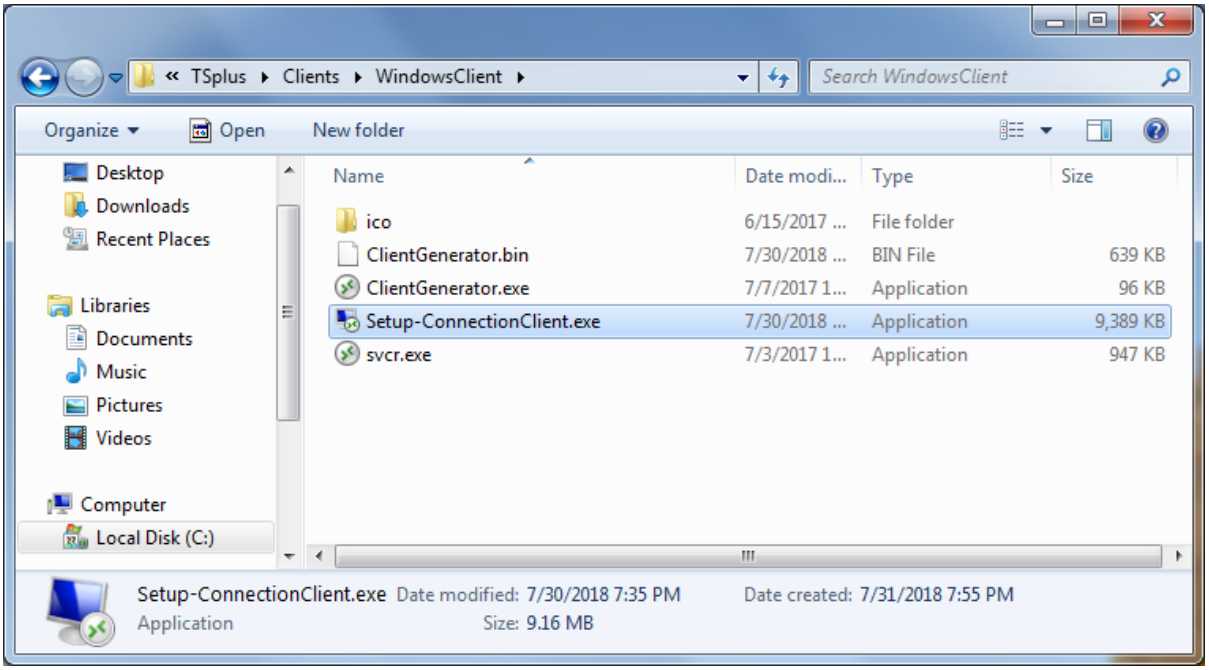

john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type:
Connection Client File
Target
Target:
Start in
Shortcu
Run:
Comme
Op
Change Icon
Look for icons in this file:
ystemRoot%\system32\SHELL32.dll
Browse...
Select an icon from the list below:
OK
Cancel

Programme d'installation du client TSplus

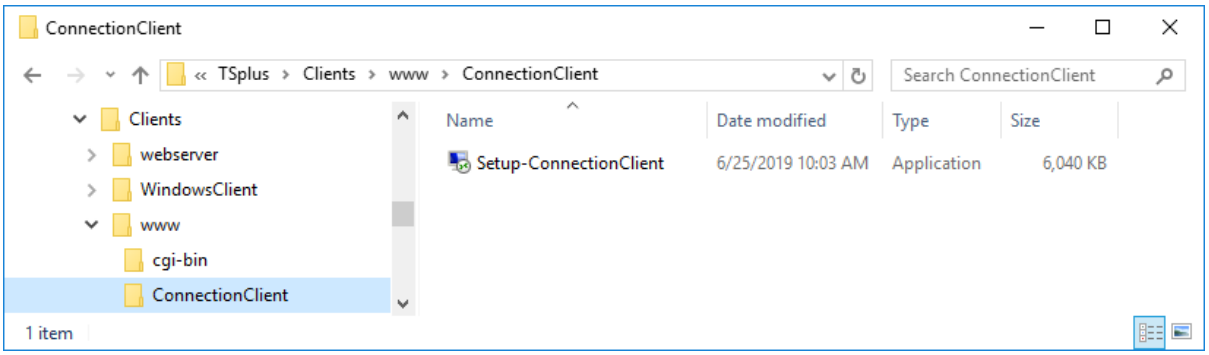
Installer

Sur le côté client, **chaque utilisateur devra exécuter un programme signé nommé “Setup-ConnectionClient.exe” en tant que pré-requis** .

Ce programme est disponible sur votre serveur, dans le dossier du programme TSplus : C:\Program Files (x86)\TSplus\Clients\WindowsClient :



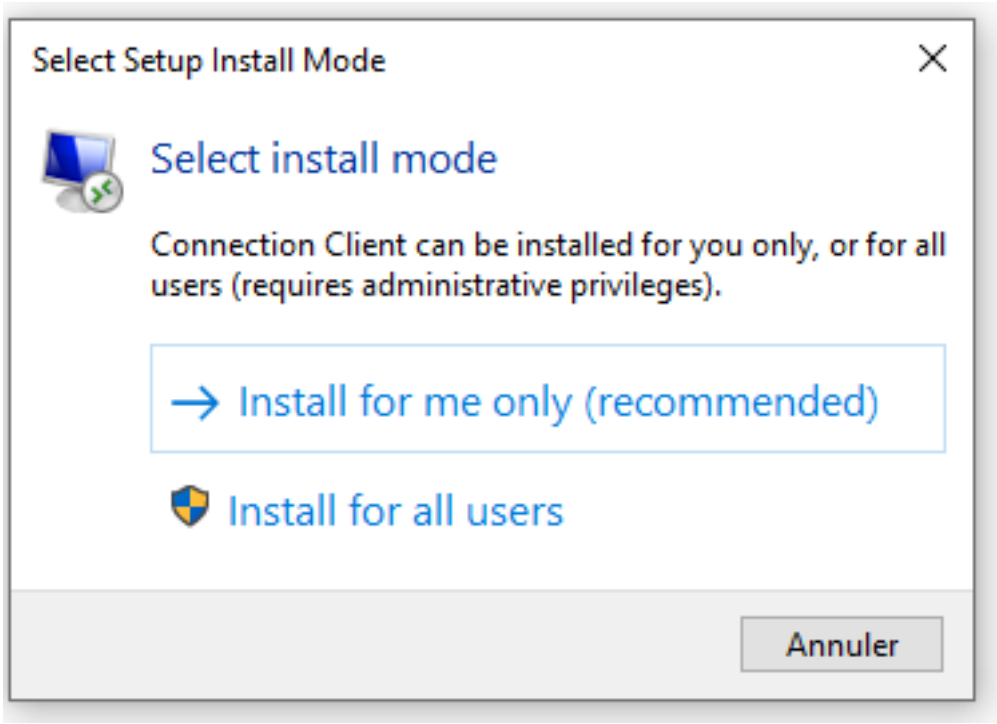
Il est également disponible dans C:\Program Files (x86)\TSplus\Clients\www\ConnectionClient, donc vos utilisateurs peuvent simplement exécuter le programme une fois sur l'adresse de votre serveur web : http://xxxxxxxxxx/ConnectionClient/Setup-ConnectionClient.exe



ou par téléchargement .

Installer pour tous les utilisateurs

Vous pouvez maintenant installer le Client de Connexion pour tous les utilisateurs. Cela signifie qu'une fois installé, tout utilisateur sur l'ordinateur en bénéficiera et pourra se connecter en mode remoteApp depuis le Portail Web, ainsi qu'avec un fichier client .connect généré.



Remarque : Pour que cette fenêtre contextuelle apparaisse, vous devez ne pas avoir déjà installé le Client de connexion. Vous pouvez également, lors d'une installation utilisant la ligne de commande, spécifier quel mode vous souhaitez utiliser avec l'argument /ALLUSERS ou / CURRENTUSER pour installer respectivement pour tous les utilisateurs ou pour l'utilisateur actuel.

Remarque Depuis TSplus 12.40, le programme de configuration du client et le Configuration du client RemoteApp ont été fusionnés et peuvent être déployés avec une seule configuration -

donc si vous téléchargez le programme d'installation du client de connexion, il ne sera pas nécessaire de télécharger celui du client RemoteApp.

Identifiant matériel et serveur cloné

1- Changement d'identifiant matériel.

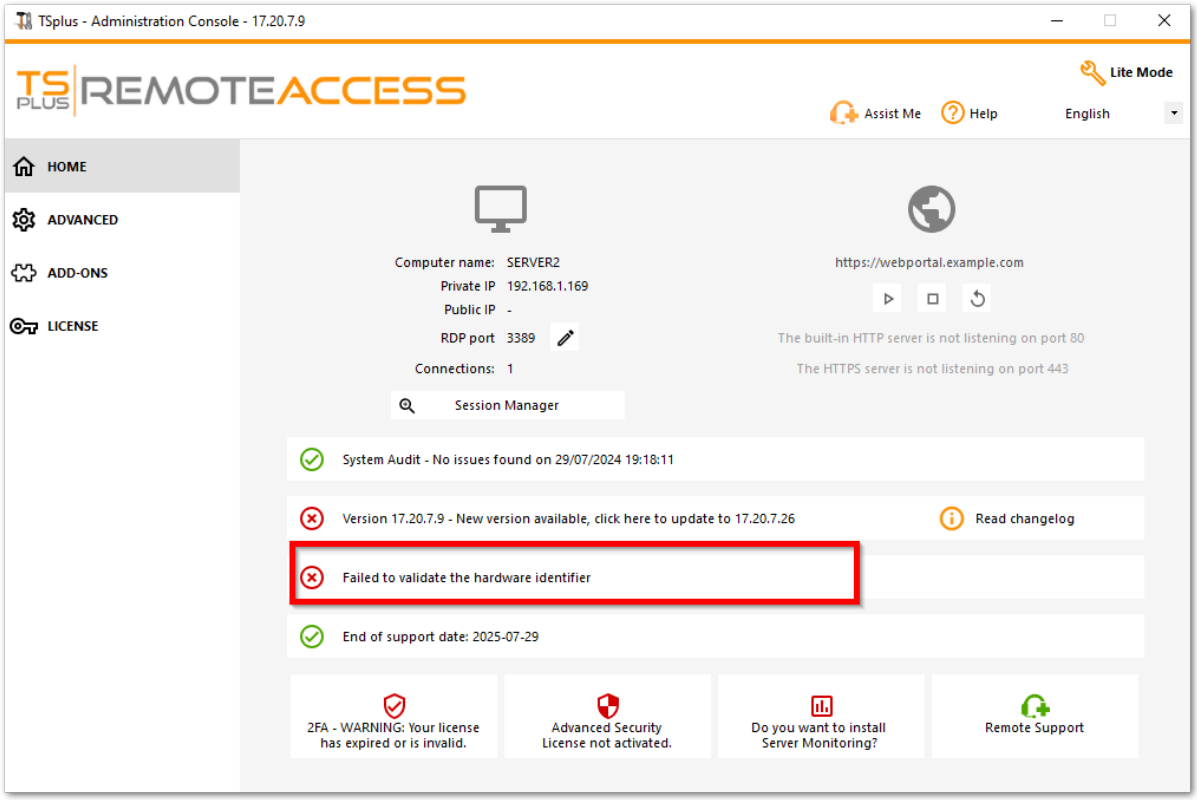
Réparation de l'identifiant matériel suite à un clonage ou une mise à jour.

Avertissement : Échec de la validation de l'identifiant matériel

Après avoir migré un serveur physique vers une machine virtuelle ou après une mise à jour du noyau Microsoft, l'état de la licence change en Échec de validation de l'identifiant matériel sur le nouveau matériel.

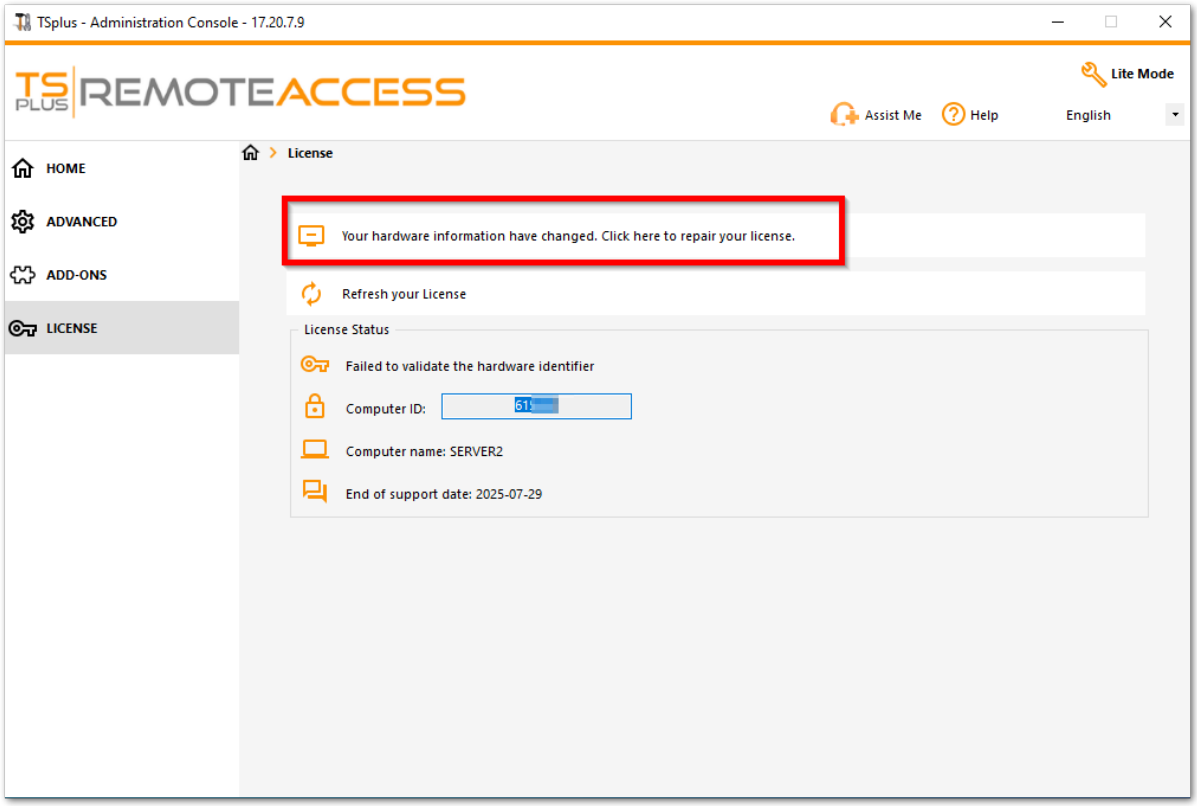
Ce message apparaît car TSplus a détecté un conflit de licence copié d'un serveur à un autre avec le même ID d'ordinateur et le même nom.
Nous vous recommandons déjà de renommer votre nouveau serveur (Exemple : SERVEUR1 > SERVEUR2)

- Redémarrez votre serveur



Cliquez sur la fenêtre pour accéder à la page de licence.

Puis cliquez sur l'onglet « Votre information matérielle a changé. Cliquez ici pour réparer votre licence.



Une fenêtre contextuelle de "réhébergement de licence" s'ouvrira pour vous permettre de restaurer votre licence.

Cas 1 : Vous n'avez pas de support !
Le rehosting ne sera donc pas possible, vous devrez souscrire à un abonnement de support sur le serveur d'origine et recommencer l'action de migration.
En cas de problèmes, Contactez le support et indiquez votre identifiant d'ordinateur et votre clé d'activation.

Cas 2 : Vous avez déjà rehosté pendant 6 mois !
Le message : Vous avez déjà réhébergé cet ordinateur au cours des 6 derniers mois. Veuillez contacter le support si vous avez besoin d'aide pour réhéberger votre licence.

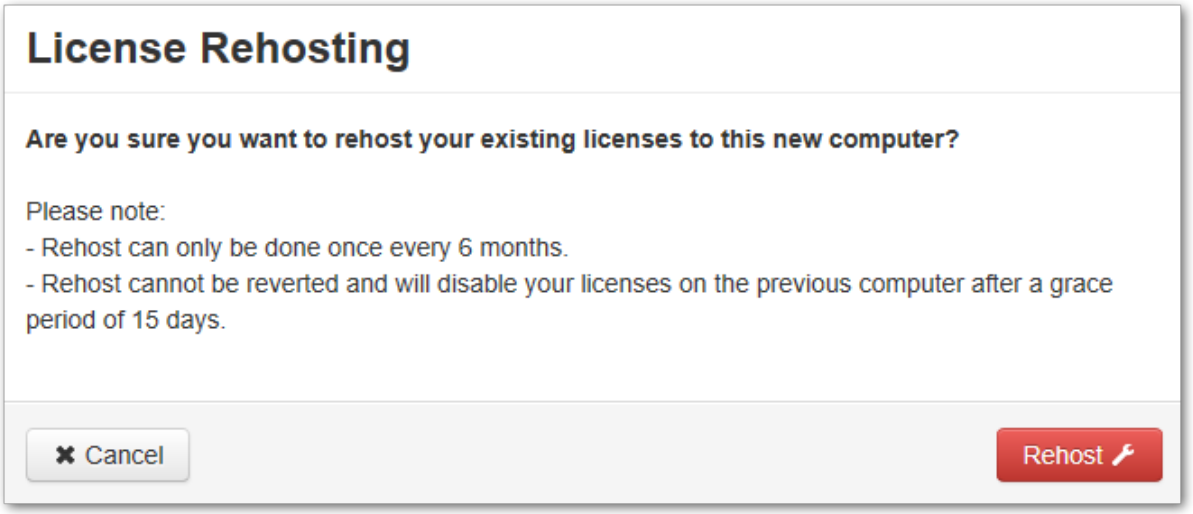
Le rehosting ne sera donc pas possible, Contactez le support et indiquez votre ID d'ordinateur et votre clé d'activation.

Cas 3 : Vous avez du support !
Le message suivant apparaît : Êtes-vous sûr de vouloir réhéberger vos licences existantes sur cet nouvel ordinateur ?

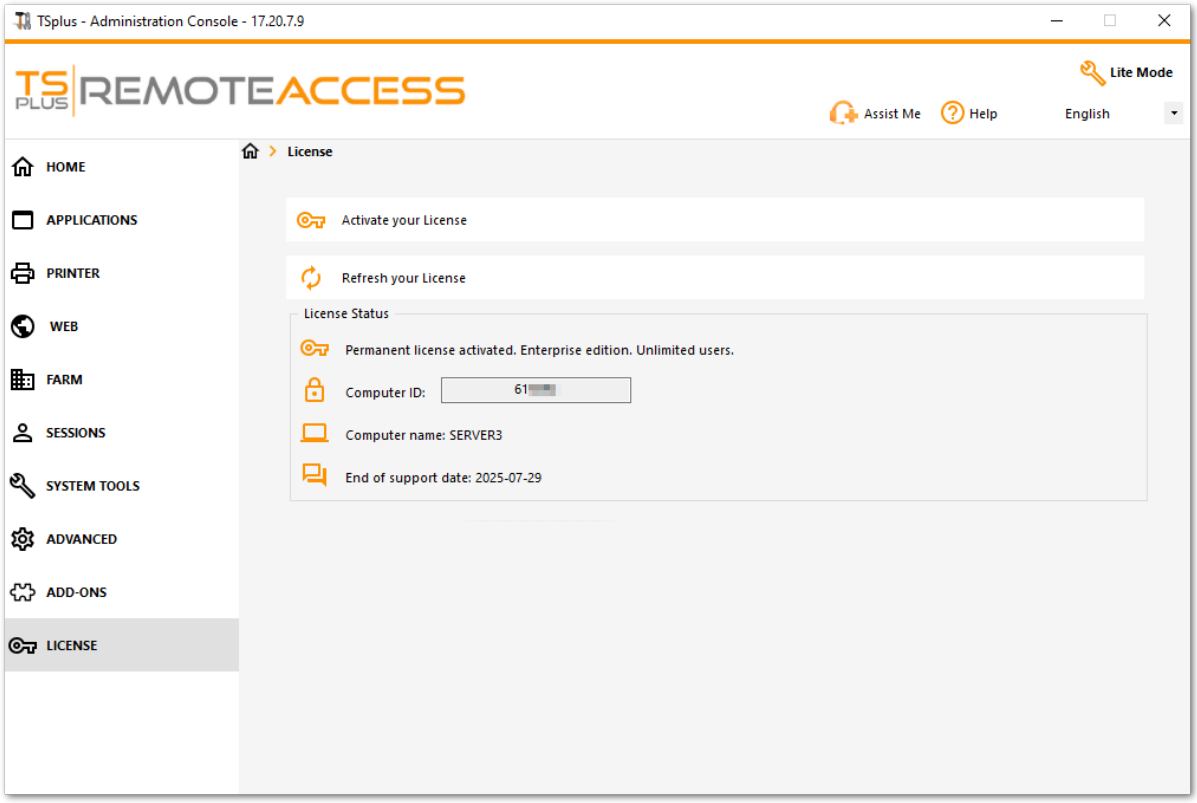
Veuillez noter :

- Le rehosting ne peut être effectué qu'une fois tous les 6 mois.
- Le rehosting ne peut pas être annulé et désactivera vos licences sur l'ordinateur précédent après une période de grâce de 15 jours.

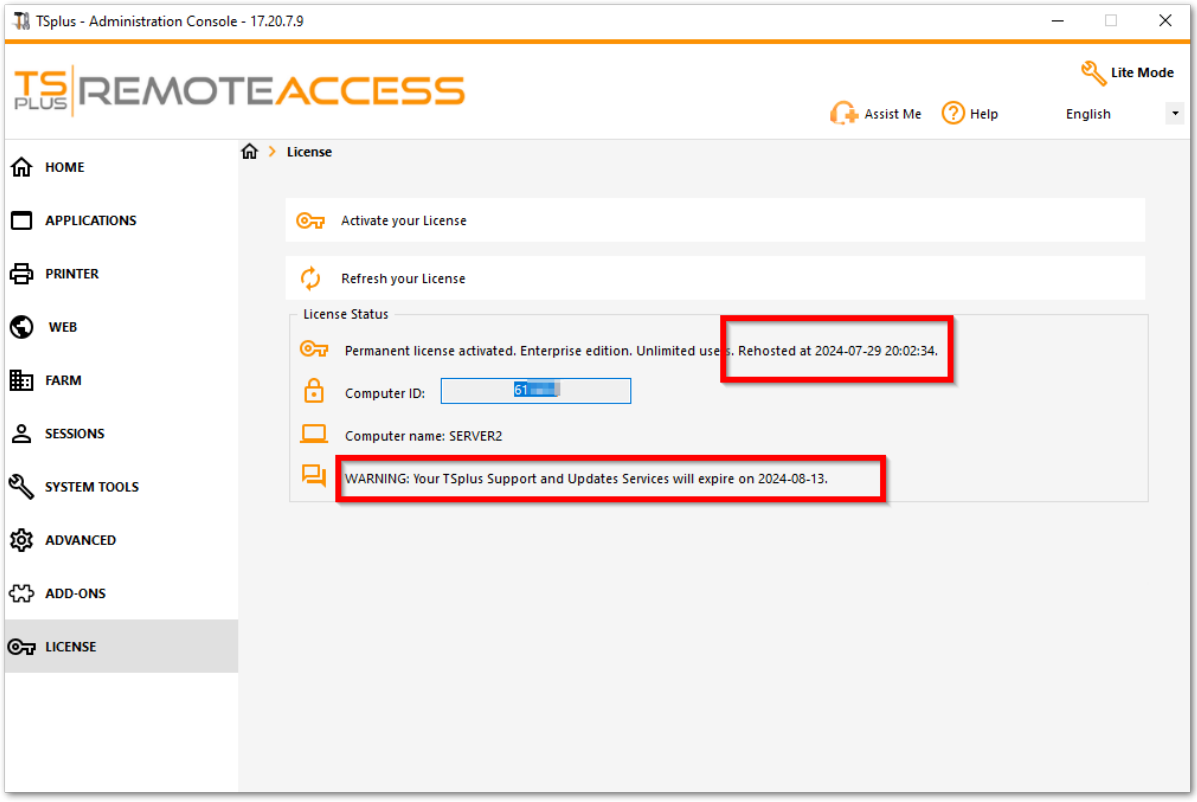
Cliquez sur le **REHOST** bouton



Votre licence est réhébergée !



Note : Un message apparaîtra sur l'ancien serveur avec la date de réhébergement ainsi que la date de fin de la période d'utilisation de l'ancien serveur (15 jours).



Échec de la mise à jour :

Exécutez la mise à jour et vérifiez si cela a résolu votre problème après avoir redémarré votre serveur.

- Télécharger le Mise à jour de la version

2- Cloner un serveur tout en conservant le serveur existant et en activant une nouvelle licence.

Exigences

Lors de l'utilisation de machines virtuelles clonées, il est important de modifier le nom de l'ordinateur et l'ID du volume disque pour garantir une installation unique de TSplus Remote Access et éviter les problèmes de licence.

Considérations sur le nom de l'ordinateur

Le nom de l'ordinateur est stocké dans le registre Windows à l'intérieur de l'image elle-même. S'il est modifié avant d'appliquer l'image, il sera écrasé par Sysprep lorsque Windows démarrera. Cependant, vous pouvez prédéfinir un nom dans un Unattended.xml Fichier de réponse. Voir Documentation Microsoft pour plus de détails.

Pour définir le nom de l'ordinateur, ajoutez la section suivante à l'intérieur Microsoft-Windows-Shell-Setup :

```
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <ComputerName>%COMPUTERNAME%ComputerName>
component>
```

Considérations sur l'ID de volume

L'ID de volume est associé à la partition de disque, pas à l'image du système d'exploitation. Il peut être modifié avant d'appliquer l'image, et il persistera. Utilisez `volumeid.exe` de Sysinternals, disponible à Microsoft Sysinternals avant que Windows ne démarre.

Étapes de déploiement

Lors du déploiement d'une nouvelle machine virtuelle à partir d'une image syspreppée, Windows entrera dans l'expérience Out-Of-Box (OOBE) au premier démarrage, demandant des paramètres de configuration.

Étapes recommandées pour le déploiement :

1. **Démarrer sur WinPE** – Préparez le système sans démarrer sous Windows.
2. **Définir l'ID de volume** – Modifiez-le avant d'appliquer l'image afin qu'il persiste.
3. **Déployer l'image syspreppée** – Utilisez DISM pour appliquer l'image à `C:\`.
4. **Définir le nom de l'ordinateur hors ligne** – Modifier le registre à l'intérieur de l'image montée.
5. **Copier un `Unattended.xml` fichier** – Automatisez la configuration OOBE. Ce fichier peut être modifié dynamiquement avant le déploiement à l'aide d'un script.
6. **Créer un script de premier démarrage** – Assurez-vous des configurations finales avec un seul redémarrage.
7. **Redémarrer sous Windows** – Windows se finalise en utilisant les configurations spécifiées.
8. **Réinitialiser la licence d'accès à distance** – Exécutez la commande suivante :

Fenêtre de terminal

```
AdminTool.exe /license /reset
```

Cela réinitialise la licence et applique une nouvelle licence.

Script de déploiement

Veuillez trouver ci-dessous le script de déploiement WinPE associé.

Fenêtre de terminal

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"    # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive

<# 3. Load Registry Offline to Set Computer Name #>
Write-Host "Modifying Registry to Set Computer Name..."
reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
reg unload HKLM\TempSys

<# 4. Ensure Unattended Setup is Used #>
Write-Host "Copying Unattended File..."
Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

<# 5. Set the First Boot Script for Final Configurations #>
Write-Host "Creating First Boot Script..."
$FirstBootScript = @"
Write-Host "Finalizing Configuration..."
Rename-Computer -NewName "$ComputerName" -Force
```

```
    Restart-Computer -Force
    "@
    Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

    Write-Host "Deployment Complete! Rebooting into Windows..."
    Write-Host "================================================"
    Write-Host "  Computer Name: $ComputerName"
    Write-Host "  Volume ID: $VolumeID"
    Write-Host "  Image Applied to: $ApplyDrive"
    Write-Host "================================================"

    <# Reboot into Windows #>
    wpeutil reboot
```

Activation de la licence

Après le déploiement, l'activation d'une licence générera un nouvel ID d'ordinateur pour la machine virtuelle. Cet ID d'ordinateur est créé par le portail de licence lorsqu'une machine demande une activation d'essai ou de licence. Pour les machines virtuelles clonées, l'activation de la licence est obligatoire. Utilisez soit une clé d'activation, soit une clé de licence en volume. **Les configurations hors ligne ne sont pas autorisées** en raison de préoccupations en matière de sécurité. Pour des étapes d'activation détaillées, reportez-vous à Liste des commandes TSplus .

Conclusion

Ce guide décrit les considérations clés pour déployer des machines virtuelles clonées avec TSplus Remote Access. Il fournit des étapes essentielles pour configurer et licencier le système correctement et doit être adapté à vos besoins et exigences.

Clonage de serveurs à l'aide de sysprep

Exigences

Lors de l'utilisation de machines virtuelles clonées, il est important de modifier le nom de l'ordinateur et l'ID du volume disque pour garantir une installation unique de TSplus Remote Access et éviter les problèmes de licence.

Considérations sur le nom de l'ordinateur

Le nom de l'ordinateur est stocké dans le registre Windows à l'intérieur de l'image elle-même. S'il est modifié avant d'appliquer l'image, il sera écrasé par Sysprep lorsque Windows démarrera. Cependant, vous pouvez prédéfinir un nom dans un Unattended.xml Fichier de réponse. Voir Documentation Microsoft pour plus de détails.

Pour définir le nom de l'ordinateur, ajoutez la section suivante à l'intérieur Microsoft-Windows-Shell-Setup :

```
    <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
        <ComputerName>%COMPUTERNAME%ComputerName>
    component>
```

Considérations sur l'ID de volume

L'ID de volume est associé à la partition de disque, pas à l'image du système d'exploitation. Il peut être modifié avant d'appliquer l'image, et il persistera. Utilisez `volumeid.exe` de Sysinternals, disponible à Microsoft Sysinternals avant que Windows ne démarre.

Étapes de déploiement

Lors du déploiement d'une nouvelle machine virtuelle à partir d'une image syspreppée, Windows entrera dans l'expérience Out-Of-Box (OOBE) au premier démarrage, demandant des paramètres de configuration.

Étapes recommandées pour le déploiement :

1. **Démarrer sur WinPE** – Préparez le système sans démarrer sous Windows.
2. **Définir l'ID de volume** – Modifiez-le avant d'appliquer l'image afin qu'il persiste.
3. **Déployer l'image syspreppée** – Utilisez DISM pour appliquer l'image à `C:` .
4. **Définir le nom de l'ordinateur hors ligne** – Modifier le registre à l'intérieur de l'image montée.
5. **Copier un `Unattended.xml` fichier** – Automatisez la configuration OOBE. Ce fichier peut être modifié dynamiquement avant le déploiement à l'aide d'un script.
6. **Créer un script de premier démarrage** – Assurez-vous des configurations finales avec un seul redémarrage.
7. **Redémarrer sous Windows** – Windows se finalise en utilisant les configurations spécifiées.
8. **Réinitialiser la licence d'accès à distance** – Exécutez la commande suivante :

Fenêtre de terminal

```
AdminTool.exe /license /reset
```

Cela réinitialise la licence et applique une nouvelle licence.

Script de déploiement

Veuillez trouver ci-dessous le script de déploiement WinPE associé.

Fenêtre de terminal

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"    # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive

<# 3. Load Registry Offline to Set Computer Name #>
Write-Host "Modifying Registry to Set Computer Name..."
reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
reg unload HKLM\TempSys

<# 4. Ensure Unattended Setup is Used #>
Write-Host "Copying Unattended File..."
Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

<# 5. Set the First Boot Script for Final Configurations #>
Write-Host "Creating First Boot Script..."
$FirstBootScript = @"
Write-Host "Finalizing Configuration..."
Rename-Computer -NewName "$ComputerName" -Force
```

```
    Restart-Computer -Force
    "@
    Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

    Write-Host "Deployment Complete! Rebooting into Windows..."
    Write-Host "================================================"
    Write-Host "  Computer Name: $ComputerName"
    Write-Host "  Volume ID: $VolumeID"
    Write-Host "  Image Applied to: $ApplyDrive"
    Write-Host "================================================"

    <# Reboot into Windows #>
    wpeutil reboot
```

Activation de la licence

Après le déploiement, l'activation d'une licence générera un nouvel ID d'ordinateur pour la machine virtuelle. Cet ID d'ordinateur est créé par le portail de licence lorsqu'une machine demande une activation d'essai ou de licence. Pour les machines virtuelles clonées, l'activation de la licence est obligatoire. Utilisez soit une clé d'activation, soit une clé de licence en volume. **Les configurations hors ligne ne sont pas autorisées** en raison de préoccupations en matière de sécurité. Pour des étapes d'activation détaillées, reportez-vous à Liste des commandes TSplus .

Conclusion

Ce guide décrit les considérations clés pour déployer des machines virtuelles clonées avec TSplus Remote Access. Il fournit des étapes essentielles pour configurer et licencier le système correctement et doit être adapté à vos besoins et exigences.

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, AdminTool.exe et TwoFactor.Admin.exe (module complémentaire 2FA) doivent être situés ici : **C:\Program Files (x86)\TSplus\UserDesktop\files**

Sauvegarder les données et les paramètres : sauvegarde

Syntax :

AdminTool.exe /backup [cheminOptionnel] [paramètres]

Description :

Commande sauvegarde est utilisé pour sauvegarder les données et les paramètres de TSplus.

Par défaut, la sauvegarde sera créée dans le répertoire des archives (C:\Backupparam)

Paramètres :

- cheminOptionnel pour sauvegarder dans un autre répertoire que celui par défaut. Les chemins relatifs et absolus sont autorisés.
- /silencieux si ce paramètre est mentionné, la sauvegarde est effectuée silencieusement

Exemples :

AdminTool.exe /backup AdminTool.exe /backup “c:/TSplus/CustomBackupFolder” /silent

Pour plus d'informations, veuillez vous rendre sur TSplus - Paramètres de sauvegarde

---

Restaurer les données et les paramètres : /restaurer

Syntax :

AdminTool.exe /restore [cheminDeSauvegarde] [paramètres]

Description :

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

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

Paramètres :

- cheminDeSauvegarde le chemin où se trouve le dossier de sauvegarde à restaurer.
- /silencieux si ce paramètre est mentionné, la restauration se fait silencieusement

Exemples :

AdminTool.exe /restore “C:/Backupparam” /silent AdminTool.exe /restore “C:/TSplus/CustomBackupFolder” /silent

Pour plus d'informations, veuillez vous rendre sur TSplus - Paramètres de sauvegarde

---

Serveur Web : /webstop , /webstart et /

webrestart

Syntax :

AdminTool.exe /webstop

AdminTool.exe /webstart

AdminTool.exe /webrestart

Description :

Commande /webstop est utilisé pour arrêter le serveur Web.

Commande /webstart est utilisé pour démarrer le serveur Web.

Commande /webrestart est utilisé pour redémarrer le serveur Web.

Paramètres :

Aucun

Mise à jour : /mettre à jour

Syntax :

AdminTool.exe /update [options]

Description :

Commande mise à jour est utilisé pour mettre à jour TSplus Remote Access et potentiellement Advanced Security.

Paramètres :

-

options
:

- /addons si cette option est utilisée, Advanced Security est également mis à jour, si une nouvelle version est disponible.

Exemple :

AdminTool.exe /update /addons

Appliquer les mises à jour de compatibilité Windows : /mettreàjourlekernel

Syntax :

svcac.exe /updatekernel [/silent]

svcac.exe doit être situé ici : **C:\Program Files (x86)\TSplus**

Description :

Commande /mettreàjourlekernel est utilisé pour appliquer des mises à jour de compatibilité Windows.

Ces mises à jour automatiques garantissent que TSplus Remote Access reste compatible avec les nouvelles mises à jour de Windows et évitent la nécessité de télécharger et de réinstaller une version plus récente de TSplus Remote Access.

Les mises à jour de compatibilité Windows peuvent se produire quotidiennement. TSplus Remote Access permet une mise à jour forcée. Cela est utile lorsque la compatibilité semble rompue et que vous devez récupérer le dernier correctif de TSplus Remote Access en dehors du calendrier de mise à jour régulier.

Veuillez noter qu'une licence valide est requise pour récupérer les mises à jour de compatibilité. Si votre licence d'essai a expiré ou si votre licence est invalide, un message d'erreur s'affichera. Veuillez contacter notre équipe de support avec une capture d'écran de ce message d'erreur si le problème est inattendu.

Paramètres :

- /silencieux Mettez à jour silencieusement en fournissant ce paramètre. Aucune boîte de message ne sera affichée.

Installer l'imprimante universelle : Installer l'imprimante universelle

Syntax :

installateuruniversalprinter.exe /InstallerImprimanteUniverselle

universalprintermanagement.exe est situé ici : **C:\Program Files (x86)\TSplus\UserDesktop\files**

Description :

Commande Installer l'imprimante universelle est utilisé pour installer Universal Printer.

Ceci est une installation propre car elle supprime l'imprimante universelle existante si elle a été installée précédemment.

Paramètres :

Aucun

Vous pouvez également effectuer cette action manuellement, veuillez consulter Imprimante universelle

---

Supprimer UniversalPrinter : Supprimer l'imprimante universelle

Syntax :

universalprintermanagement.exe /RemoveUniversalPrinter

universalprintermanagement.exe est situé ici : **C:\Program Files (x86)\TSplus\UserDesktop\files**

Description :

Commande Supprimer l'imprimante universelle est utilisé pour désinstaller Universal Printer.

Paramètres :

Aucun

Vous pouvez également effectuer cette action manuellement, veuillez consulter Imprimante universelle

---

Configurer le serveur proxy : /proxy /set

Syntax :

AdminTool.exe /proxy /set [paramètres]

Description :

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

Paramètres :

- /serveur 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.
- /nom_utilisateur le nom d'utilisateur pour se connecter au serveur proxy. Ce paramètre est facultatif
- / mot de passe 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 :

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

AdminTool.exe /proxy /set /host ie

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

Ouvrir le formulaire d'identifiants Web : /webcredentials

Syntax :

AdminTool.exe /webcredentials

Description :

Commande /webcredentials lance dans une seule fenêtre l'interface Web Credentials (comme vous le feriez dans AdminTool > Web > Web Credentials).

Paramètres :

Aucun

Créer des identifiants Web : /webcredentials-ajouter

Syntax :

AdminTool.exe /webcredentials-add [webLogin] [webPassword] [windowsLogin] [windowsPassword] [maximumConcurrentSessions]

Description :

Commande /webcredentials-ajouter est utilisé pour créer des identifiants Web (comme vous le feriez dans AdminTool > Web > Identifiants Web).

Paramètres :

- webLogin le login web que vous souhaitez créer.
- motdepasseWeb le mot de passe web associé. Il peut s'agir d'un identifiant vide. Pour cela, utilisez des guillemets doubles "" pour indiquer un mot de passe vide.
- connexionWindows le login Windows de l'utilisateur correspondant.
- mot de passe Windows le mot de passe Windows.
- sessionsConcurrentesMaximales (optionnel) : le nombre maximum de sessions simultanées pour cet utilisateur.

Exemple :

AdminTool.exe /webcredentials-add johndoe passwordABCD johnWinuser johnWinpassword 4

Pour plus d'informations, veuillez vous rendre sur Identifiants Web

---

Supprimer les identifiants Web : /webcredentials-remove

Syntax :

AdminTool.exe /webcredentials-remove [webLogin]

Description :

Commande /webcredentials-remove est utilisé pour supprimer un identifiant Web existant (comme vous le feriez dans AdminTool > Web > Identifiants Web).

Paramètres :

- webLogin le login web que vous souhaitez supprimer.

Exemple :

AdminTool.exe /webcredentials-remove johndoe

Pour plus d'informations, veuillez vous rendre sur Identifiants Web

---

Gestionnaire de session ouverte : /sessionmanager

Syntax :

AdminTool.exe /gestiondesessions

Description :

Commande /sessionmanager lance dans une seule fenêtre de taille importante le gestionnaire de session (comme vous le feriez dans AdminTool > Accueil > Gestionnaire de session).

Paramètres :

Aucun

Moniteur des sessions ouvertes : /monitorer-sessions-ferme

Syntax :

AdminTool.exe /surveiller-sessions-ferme

Description :

Commande /monitorer-sessions-ferme lance dans une seule fenêtre de taille importante le

moniteur de session du gestionnaire de ferme (comme vous le feriez dans AdminTool > Ferme > Surveiller les sessions).

Paramètres :

Aucun

Ouvrir le gestionnaire d'équilibrage de charge : / ferme-équilibrage-de-charge

Syntax :

AdminTool.exe /répartition-de-charge-farm

Description :

Commande /ferme-équilibrage-de-charge lance dans une seule fenêtre de taille importante le gestionnaire d'équilibrage de charge du gestionnaire de ferme (comme vous le feriez dans AdminTool > Ferme > Équilibrage de charge).

Paramètres :

Aucun

Exécuter l'audit du système : / systèmeaudit

Syntax :

AdminTool.exe /systemaudit

Description :

Commande / systèmeaudit exécute un audit système (comme vous le feriez manuellement

dans AdminTool > Accueil > Audit système > Exécuter l'audit système).

Paramètres :

Aucun

Activation de la licence : /activer

Syntax :

AdminTool.exe /activer [licensePath]

Description :

Commande activer est utilisé pour activer la licence Remote Access, en utilisant un fichier de licence.

Paramètres :

- cheminDeLicence le chemin du fichier de licence

Exemple :

AdminTool.exe /activate “C:\Program Files (x86)\TSplus\license.lic”

Réinitialisation de la licence suite au clonage d'une machine virtuelle : /réinitialiser

Syntax :

AdminTool.exe /license /reset

Description :

Lors de la clonage d'un serveur, l'onglet 'Licence' dans AdminTool peut ne pas afficher un ID d'ordinateur ou peut afficher le message d'erreur : "Identifiant matériel invalide." La commande / réinitialiser vise à initialiser la licence sur le serveur clone afin que de nouvelles licences puissent être attribuées pour les produits TSplus installés.

Remarques importantes :

1. Une nouvelle licence TSplus doit être activée à l'aide d'une nouvelle clé d'activation.
2. Ne pas utiliser la commande /license /reset sur une machine non clonée, car cela empêche définitivement l'attribution de la licence. Toujours confirmer l'état de la machine avant de procéder.

Étapes pour réinitialiser la licence sur un serveur cloné :

1. Ouvrez une session Administrateur sur le serveur cloné.

2. Changer le numéro de série du volume HDD.

- Exécutez le vol commande pour afficher le numéro de série du volume actuel (VSN). Le résultat devrait ressembler à : 74F8-9C08 .

- Téléchargez et installez l'utilitaire VolumeID, disponible ici .

- Exécutez la commande : volumeid C: 84F8-9C08 en tant qu'administrateur pour changer le VSN du lecteur. Dans cet exemple, nous avons changé le VSN du disque C: et j'ai changé seulement un caractère (le premier) de l'ancien VSN pour spécifier le nouveau.

- Note : cette étape est cruciale car certaines versions de Windows Server ne génèrent pas un nouveau numéro de série de volume lors du clonage, même en utilisant SysPrep.

3. Renommez le serveur cloné et redémarrez-le.

4.
Réinitialiser la licence dans AdminTool :

- Ouvrez une invite de commandes avec des privilèges d'administrateur.
- Naviguez vers le répertoire contenant l'exécutable AdminTool en utilisant cette commande : cd "C:\Program Files (x86)\TSplus\UserDesktop\files"
- Exécutez la commande suivante : AdminTool.exe /license /reset

5. Vérifiez la réinitialisation.

- Après avoir exécuté la commande, l'onglet 'Licence' devrait afficher l'erreur suivante : Échec de la lecture du fichier de licence (format de fichier inattendu).

6. Activez la nouvelle licence.

- Dans l'onglet « Licence », cliquez sur « Activer votre licence » et saisissez la nouvelle clé d'activation pour activer les licences et les supports requis.

Exemple :

AdminTool.exe /license /reset TSplus-Security.exe /license /reset ServerMonitoring.exe /license /reset

---

Activation de la licence en volume : /vl /activer

Syntax :

AdminTool.exe /vl /activer [licensekey] [parameters]

Commande vl /activer est utilisé pour activer une licence en volume.

Paramètres :

- clé de licence clé de licence pour activer, dans ce format : AAAA-BBBB-CCCC-DDDD
- / utilisateurs : tout nombre de 1 à 50, ou "illimité"
- /édition “Bureau”, “Web Mobile” ou “Entreprise”
- /supportyears Tout nombre de 0 à 3.
- /Commentaires Spécifie les commentaires à joindre à la licence sur le portail de licence

Exemple :

AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users illimité /edition Entreprise / supportyears 3 /comments “Ceci est un commentaire”

Pour plus d'informations, veuillez vous rendre sur Documentation de licence en volume

---

Activer et désactiver la licence en volume : /vl / activer et /vl /désactiver

Syntax :

AdminTool.exe /vl /enable [licensekey]

AdminTool.exe /vl /disable [licensekey]

Description :

Commande vl /enable est utilisé pour activer une licence en volume.

Commande vl /désactiver est utilisé pour désactiver une licence en volume.

Paramètres :

- clé de licence clé de licence pour activer/désactiver, dans ce format : AAAA-BBBB-CCCC-DDDD

Exemples :

AdminTool.exe /vl /enable VOLU-MELI-CENS-EKEY

AdminTool.exe /vl /disable VOLU-MELI-CENS-EKEY

Pour plus d'informations, veuillez vous rendre sur Comment activer/désactiver une licence depuis le serveur ?

Mise à jour de la licence en volume : /vl /mise à jour

Syntax :

AdminTool.exe /vl /update [licensekey] [parameters]

Description :

Commande vl /mise à jour est utilisé pour mettre à jour les utilisateurs d'une licence en volume.

Paramètres :

- clé de licence clé de licence pour mettre à jour, dans ce format : AAAA-BBBB-CCCC-DDDD
- / utilisateurs : tout nombre de 1 à 50, ou "illimité"

Exemples :

AdminTool.exe /vl /update /users 2 AdminTool.exe /vl /update /users illimité

Pour plus d'informations, veuillez vous rendre sur Comment mettre à jour les utilisateurs d'une licence en volume depuis le serveur ?

Afficher les crédits de licence restants pour une clé de licence en volume : /vl /crédits-licence

Syntax :

AdminTool.exe /vl /credits-license [licensekey] [parameters]

Description :

Commande vl /crédits-licence est utilisé pour afficher les crédits de licence restants associés à une clé de licence en volume.

Paramètres :

- clé de licence Clé de licence en volume, dans ce format : AAAA-BBBB-CCCC-DDDD
- /login fournir l'identifiant du partenaire associé à la clé de licence en volume
- /édition fournir le paramètre d'édition optionnel pour les produits Advanced Security et Server Monitoring
- /silencieux : exécute la commande silencieusement

La sortie sera stockée dans la variable d'environnement au niveau utilisateur nommée CRÉDITS DE LICENCE VOLUME Il peut être nécessaire de lire la valeur de CRÉDITS DE LICENCE VOLUME d'un processus différent, en utilisant la commande echo %VOLUME_LICENSE_CREDITS% .

Exemples :

AdminTool.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE TSplus-Security.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE /edition Essentials /silent

Pour plus d'informations, veuillez vous rendre sur Comment afficher les crédits de licence restants pour une clé de licence en volume ?

Afficher les crédits de support restants pour une clé de licence en volume : /credits-support

Syntax :

AdminTool.exe /vl /credits-support [licensekey] [parameters]

Description :

Commande vl /crédits-support est utilisé pour afficher les crédits de support restants associés à une clé de licence en volume.

Paramètres :

- clé de licence Clé de licence en volume, dans ce format : AAAA-BBBB-CCCC-DDDD
- /login fournir l'identifiant du partenaire associé à la clé de licence en volume
- /édition fournir le paramètre d'édition optionnel pour les produits Advanced Security et Server Monitoring
- /silencieux : exécute la commande silencieusement

La sortie sera stockée dans la variable d'environnement au niveau utilisateur nommée CRÉDITS DE LICENCE VOLUME Il peut être nécessaire de lire la valeur de CRÉDITS DE LICENCE VOLUME d'un processus différent, en utilisant la commande echo %VOLUME_LICENSE_CREDITS% .

Exemples :

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE TSplus-Security.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE /edition Essentials

Pour plus d'informations, veuillez vous rendre sur Comment afficher les crédits de support restants pour une clé de licence en volume ?

2FA - réinitialiser : /réinitialiser utilisateur

Syntax :

TwoFactor..Admin.exe /resetuser [user1] [user2] … [userN]

Description :

Commande /réinitialiser utilisateur est utilisé pour réinitialiser les utilisateurs 2FA, au lieu de le faire via l'interface utilisateur (cela peut être fait ici dans l'interface : TwoFactor.Admin > Gérer les utilisateurs > Réinitialiser)

Paramètres :

- user1 user2 ... userN les noms de domaine des utilisateurs que vous souhaitez réinitialiser (séparés par un espace simple)

Exemples :

TwoFactor.Admin.exe /resetuser johndoe jackrussell chuckbartowski

Pour plus d'informations, veuillez vous rendre sur Réinitialiser la configuration pour les utilisateurs

---

2FA - ajouter des utilisateurs : /addusers

Syntax :

TwoFactor.Admin.exe /addusers [userInfos1] [userInfos2] … [userInfosN]

Description :

Commande /addusers est utilisé pour ajouter plusieurs utilisateurs 2FA, au lieu de le faire via l'interface utilisateur, utilisateur par utilisateur (cela peut être fait ici dans l'interface : TwoFactor.Admin > Gérer les utilisateurs > Ajouter un utilisateur)

Paramètres :

- userInfos1 userInfos2 ... userInfosN
  les informations utilisateur des utilisateurs que vous souhaitez ajouter. Ces informations se composent des champs suivants, séparés par un point-virgule.
  - nomDeDomaine (mandatory): le nom de domaine de l'utilisateur à ajouter
  - méthode reçue méthode pour recevoir des codes de confirmation. Doit être l'une de ces valeurs : SMS, App, Email ou LaisserLUtilisateurChoisir. App est la valeur par défaut.
  - téléphone mobile (optionnel) : le téléphone de l'utilisateur à ajouter
  - email (email de l'utilisateur à ajouter)

Exemples :

TwoFactor.Admin.exe /addusers johndoe jackrussell;LaissezL'utilisateurChoisir

chuckbartowski;Téléphone;+33101010101; abcd@efgh.com samanthacarter;Email;;

Pour plus d'informations, veuillez vous rendre sur Ajouter des utilisateurs et des groupes

---

2FA - ajouter des groupes : /addgroups

Syntax :

TwoFactor.Admin.exe /addgroups [groupe1] [groupe2] … [groupeN]

Description :

Commande /addgroups est utilisé pour ajouter plusieurs groupes 2FA, au lieu de le faire via l'interface utilisateur, groupe par groupe (cela peut être fait ici dans l'interface : TwoFactor.Admin > Gérer les utilisateurs > Ajouter un groupe)

Paramètres :

- groupe1 groupe2 ... groupeN les noms des groupes que vous souhaitez ajouter.

Exemples :

TwoFactor.Admin.exe /addgroups groupe1 groupe2 groupe3

Pour plus d'informations, veuillez vous rendre sur Ajouter des utilisateurs et des groupes

---

2FA - lister les utilisateurs : /getusers

Syntax :

TwoFactor.Admin.exe /getusers

Description :

Commande /getusers est utilisé pour obtenir une liste de tous les utilisateurs/groupes configurés dans la console d'administration 2FA. Une représentation json de cette liste d'utilisateurs/groupes est renvoyée et peut être utilisée par exemple dans un script Powershell.

Cette liste peut être vue ici dans l'interface : TwoFactor.Admin > Gérer les utilisateurs.

Paramètres :

Aucun

2FA - ajouter des groupes : / supprimerutilisateur

Syntax :

TwoFactor.Admin.exe /deleteuser [domainName] [userType]

Description :

Commande /supprimerutilisateur est utilisé pour retirer un utilisateur de la configuration 2FA (cela peut être fait ici dans l'interface : TwoFactor.Admin > Gérer les utilisateurs > Retirer)

Paramètres :

- nomDeDomaine le nom de l'utilisateur ou du groupe à supprimer.
- type d'utilisateur le type d'objet à supprimer. Sa valeur doit être "utilisateur" ou "groupe"

Exemples :

TwoFactor.Admin.exe /deleteuser “Ceci est un nom de groupe” groupe TwoFactor.Admin.exe /deleteuser administrateur utilisateur

Pour plus d'informations, veuillez vous rendre sur Supprimer les utilisateurs et les groupes

---

Ajouter ou mettre à jour des identifiants dans le Gestionnaire d'identifiants Windows : / windowscredential-ajouteroumettre

Syntax :

AdminTool.exe /windowscredential-addorupdate

ou

AdminTool.exe /windowscredential-addorupdate csvFilePath

Description :

Commande /windowscredential-ajouteroumettre est utilisé pour ajouter de nouvelles

informations d'identification Windows au Gestionnaire d'informations d'identification Windows, ou mettre à jour celles existantes. Vous pouvez fournir des informations d'identification individuellement en spécifiant le domaine, le nom d'utilisateur et le mot de passe, ou traiter plusieurs entrées en masse à partir d'un fichier CSV.

Cette commande est utile pour configurer l'authentification externe via SAML pour le portail Web avec SSO.

Paramètres :

- **Mode d'authentification unique**

  - domaine (mandatoire) : le nom de domaine de l'utilisateur s'il fait partie d'un Active Directory, ou le nom de la machine si l'utilisateur est un utilisateur local
  - nom d'utilisateur (mandatoire) : le nom d'utilisateur du compte Windows
  - mot de passe (mandatoire) : le mot de passe du compte Windows

- **Mode en masse (fichier CSV)**

  - csvFilePath (mandatoire) : le chemin vers un fichier CSV contenant un ou plusieurs identifiants à ajouter ou à mettre à jour

Exemples

Pour un utilisateur d'Active Directory :

AdminTool.exe /windowscredential-addorupdate COMPANY johndoe SecurePassword123

Pour un utilisateur local :

AdminTool.exe /windowscredential-addorupdate MACHINE-NAME janedoe SecurePassword123

Pour ajouter ou mettre à jour en masse des identifiants à partir d'un fichier CSV :

AdminTool.exe /windowscredential-addorupdate C:\\credentials\\users.csv

---

Supprimer les identifiants du Gestionnaire d'identifiants Windows : /windowscredential-remove

Syntax :

AdminTool.exe /windowscredential-remove nom d'utilisateur

ou

AdminTool.exe /windowscredential-remove cheminFichierCsv

Description :

Commande /windowscredential-remove est utilisé pour supprimer les identifiants Windows. Vous pouvez supprimer un seul identifiant en spécifiant la cible, ou supprimer plusieurs identifiants en masse en utilisant un fichier CSV.

Paramètres :

- **Mode d'authentification unique :**
- cible (mandatoire) : le nom cible pour l'identifiant, généralement un nom de domaine ou de serveur
- **Mode en masse (fichier CSV) :**
  - csvFilePath (mandatoire) : le chemin vers un fichier CSV contenant les noms d'utilisateur à supprimer. Le fichier doit exister

Exemples :

AdminTool.exe /windowscredential-remove ENTREPRISE

AdminTool.exe /windowscredential-remove C:\credentials\remove_users.csv

Comment personnaliser complètement la page d'accès Web au-delà des capacités du portail Web ?

Aperçu

En utilisant le Portail Web vous pouvez personnaliser les pages d'accès Web de Terminal Service Plus de manière extensive.

Cependant, dans certains cas, cela n'est pas suffisant. Dans ces cas, vous pouvez personnaliser complètement la page d'accès Web, au-delà des capacités du portail Web, en modifiant vous-même la page d'accès Web générée par l'outil Webmaster.

Avertissement, cette documentation est destinée uniquement aux développeurs Web expérimentés.

Génération des paramètres obligatoires

Pour inclure les paramètres obligatoires dans votre page d'accès Web, nous vous recommandons de commencer par générer votre page d'accès Web en utilisant le Portail Web .

Emplacement des fichiers

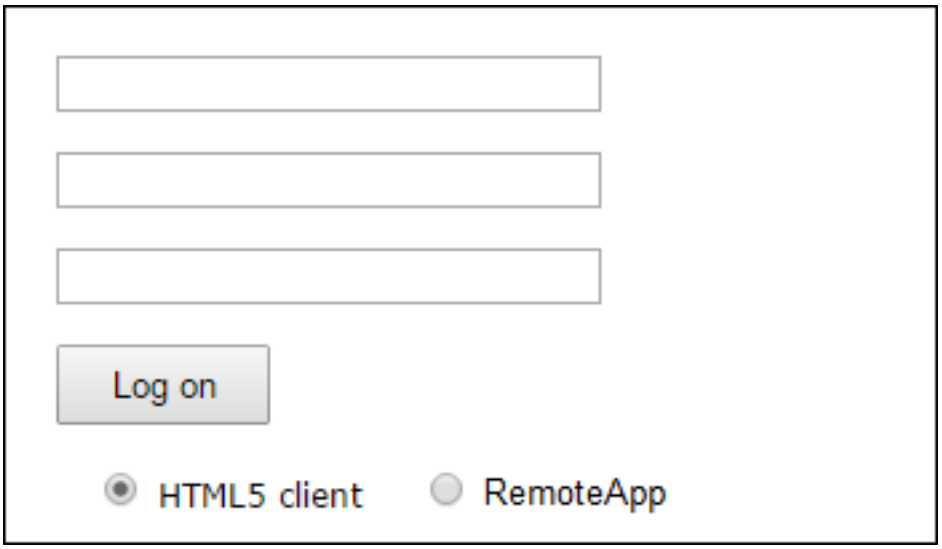
La page d'accès Web sera générée dans le dossier “C:\Program Files (x86)\TSplus\Clients\www”. Par exemple, si vous choisissez “index” comme nom de page, il s'agira du fichier nommé “index.html” dans ce dossier. C'est un fichier HTML standard, donc vous pouvez utiliser toutes vos connaissances des langages de programmation HTML, JavaScript et CSS pour développer votre page personnalisée.

Tous les fichiers d'inclusion sont écrits relativement au dossier “C:\Program Files (x86)\TSplus\Clients\www”. Par exemple, le fichier principal des styles CSS est situé à “C:\Program Files (x86)\TSplus\Clients\www\software\common.css”, il est donc inclus dans le fichier de la page d'accès Web HTML par la ligne suivante :

Page d'accès Web minimale

À partir d'un fichier HTML généré par les Préférences du Portail Web, nous allons le réduire à une page d'accès Web minimale. Nous vous conseillons d'utiliser un éditeur de texte tel que Notepad ou Notepad++. non utiliser Word).

Après notre travail, cela ressemblera à la capture d'écran ci-dessous :



Tout d'abord, vous devez conserver tout ce qui se trouve entre les
et balises HTML :

- meta tags pour forcer les navigateurs à vider leur cache
- inclusions de fichiers .js
- Déclarations des paramètres JavaScript

Ensuite, vous pouvez réduire le contenu entre les balises HTML 'body' et '/body' à ces quelques lignes :

client HTML5 RemoteApp

Rafraîchissez la page web dans votre navigateur, et vous devriez obtenir la page minimale de la

capture d'écran ci-dessus.

Nous vous recommandons de vider le cache de votre navigateur après avoir enregistré tout fichier modifié.

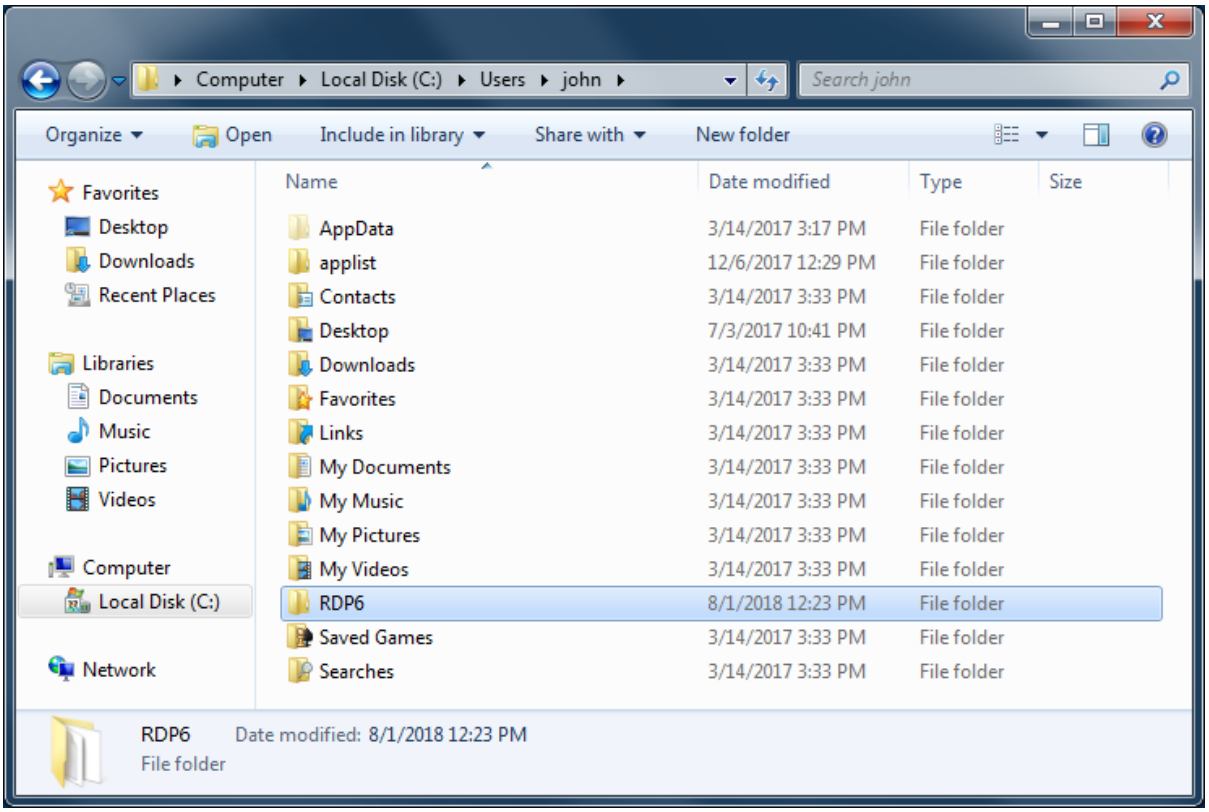
Enfin, c'est maintenant à vous de jouer !

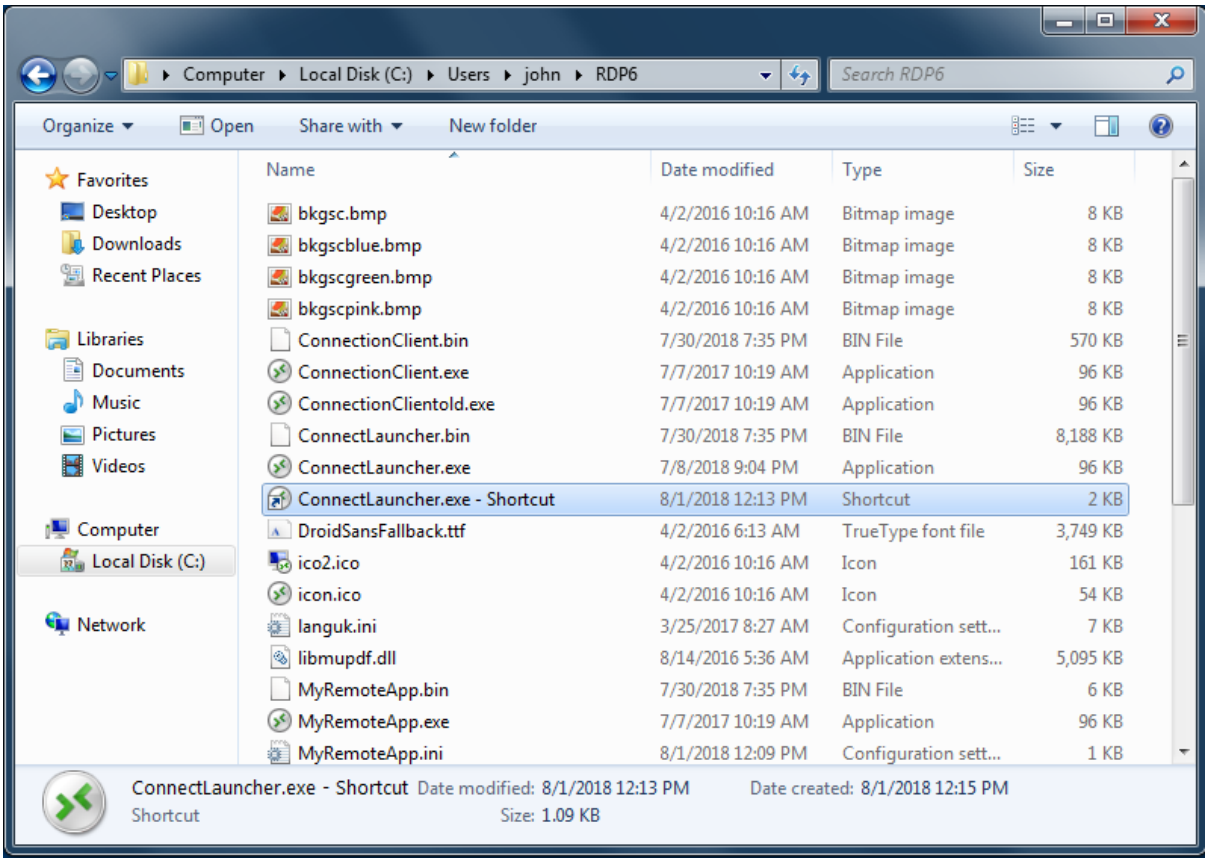
Tant que vous conservez les appels aux fonctions JavaScript sur des événements spécifiques et les identifiants donnés (id="..."), votre page d'accès Web entièrement personnalisée fonctionnera correctement !

Modifier ou supprimer les paramètres d'un client généré

Il y a de nombreuses raisons pour lesquelles vous voudriez modifier les paramètres de votre client de connexion : l'adresse IP de votre serveur TSplus a changé, vous devez ajouter la redirection d'imprimante, changer les paramètres de l'imprimante universelle, etc.

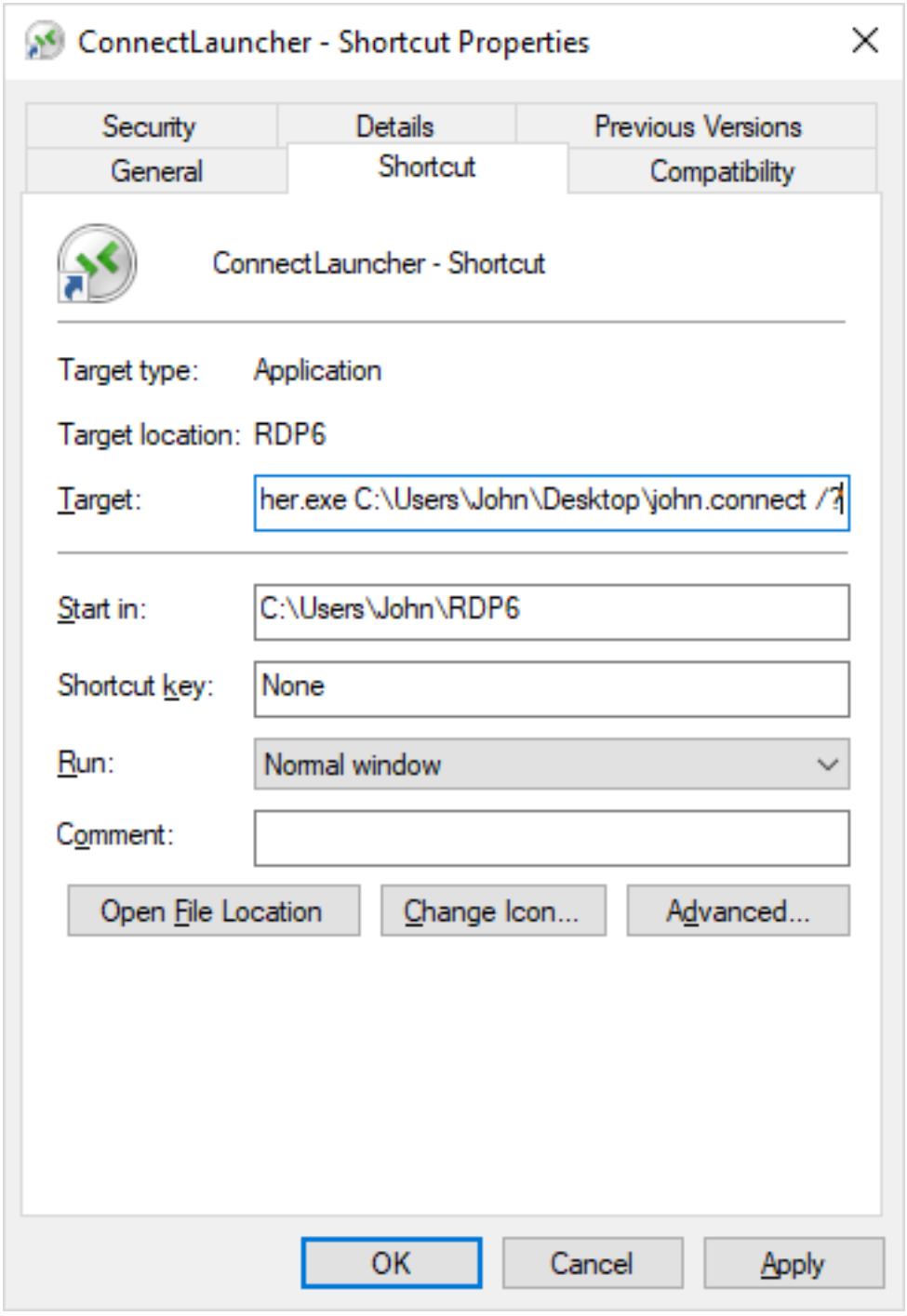
- Vous devez d'abord créer un raccourci du fichier ConnectLauncher.exe, situé dans le dossier RDP6 du profil de l'utilisateur :



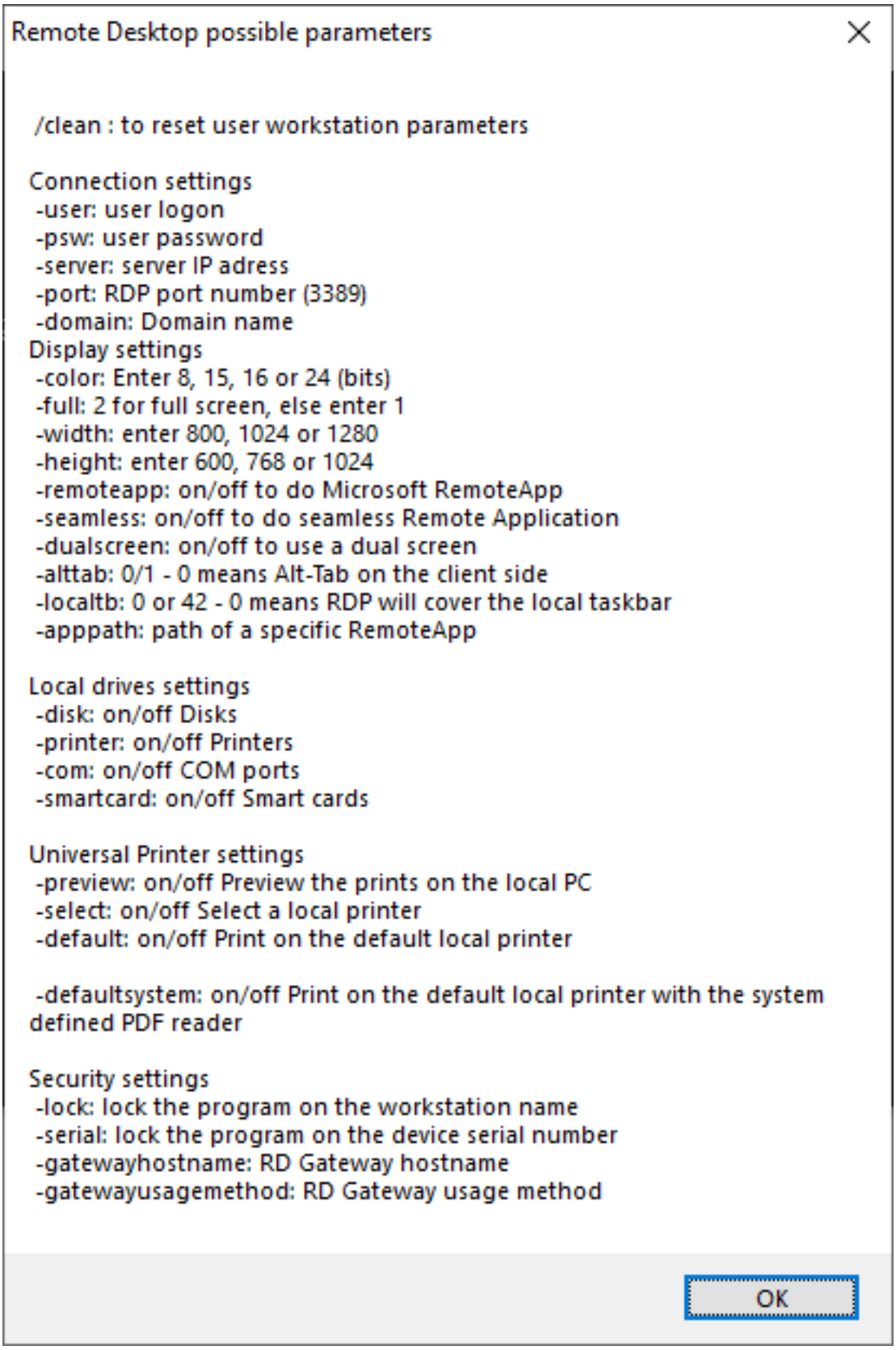


.

- Ensuite, faites un clic droit dessus et sélectionnez propriétés. Placez votre souris à la fin du champ "cible" et tapez le chemin du client suivi de "/?", par exemple : C: \Users\John\Desktop\clientname.connect /?":

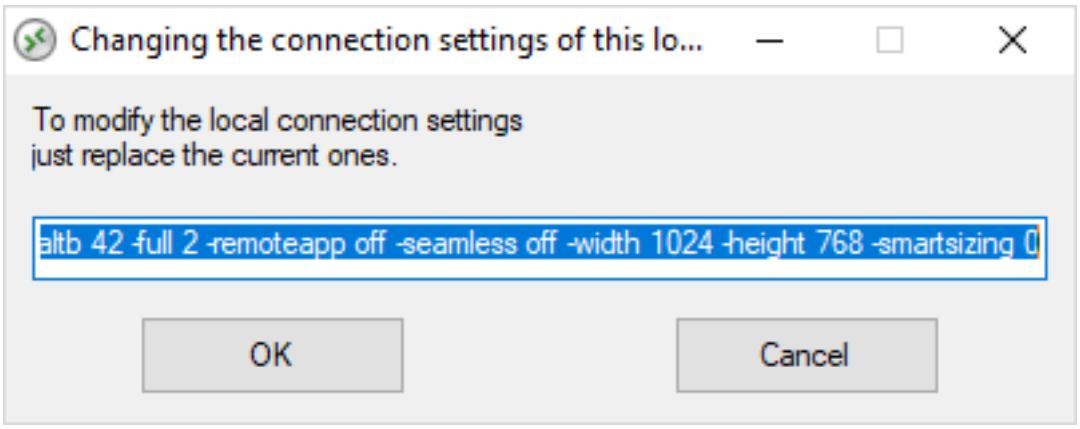


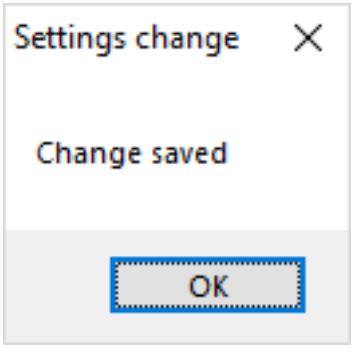
Maintenant, cliquez sur OK et double-cliquez sur le raccourci. Une liste de commutateurs apparaît :



Cliquez sur OK, la liste de tous les paramètres apparaît dans une petite fenêtre.

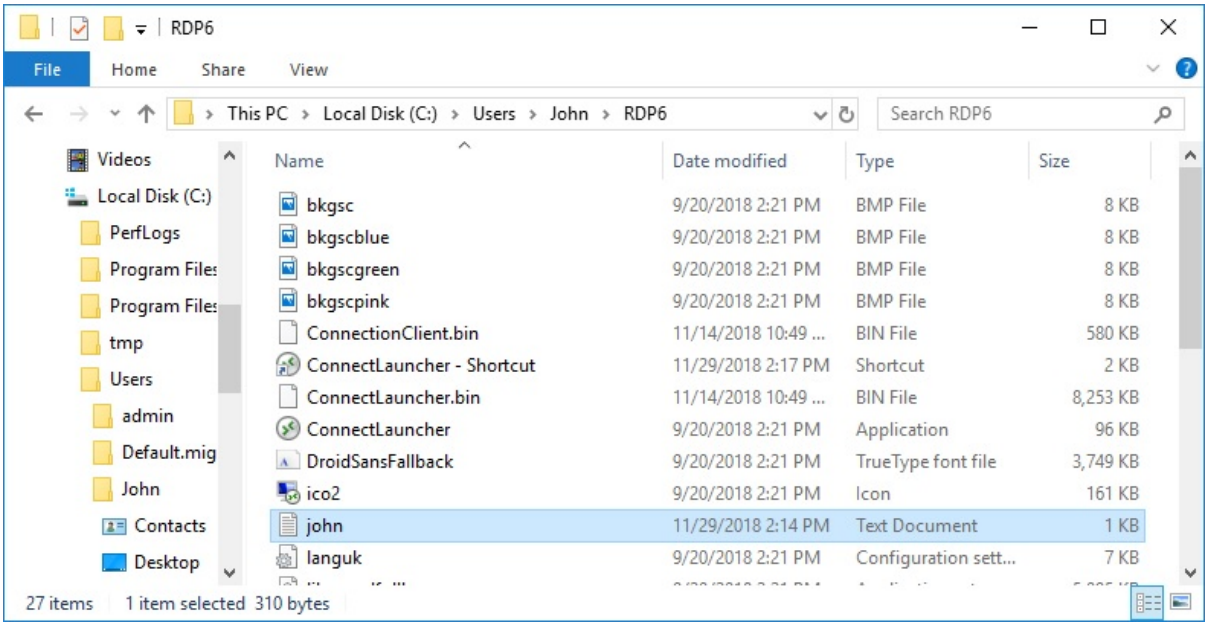
Vous pouvez maintenant les modifier pour correspondre à vos préférences, vous devrez vous déconnecter et vous reconnecter pour appliquer les modifications.





Nettoyez les paramètres d'un client généré

Après avoir lancé le client au moins une fois, vous pouvez nettoyer les paramètres en supprimant le fichier client.txt situé dans le dossier RDP6 :



Activer l'authentification intégrée de Windows sur un domaine Active Directory

Ce guide est fourni pour configurer l'authentification intégrée Windows (Kerberos/NTLM) avec un compte de service géré par groupe (gMSA) sur le portail Web.

En raison de la nature unique du réseau et de l'architecture de chaque entreprise, nous ne pouvons pas fournir de support pour les problèmes découlant du suivi de cette documentation. Cela répond aux exigences techniques pour le portail Web avec authentification intégrée Windows, mais la mise en œuvre est de votre propre responsabilité.

Configuration de domaine

L'environnement Active Directory doit prendre en charge l'authentification Kerberos ou NTLM.

Configurer un compte de service géré (gMSA)

Installez le service Web Portal et exécutez-le avec un **compte de service géré de domaine** au lieu d'un compte administrateur de domaine.

Prérequis

- Niveau de schéma Active Directory : **Windows Server 2012** ou plus tard (nécessaire pour gMSA)
- Au moins un contrôleur de domaine en cours d'exécution **Windows Server 2012** ou plus tard
- Clé racine KDS créée (configuration unique)
- Adhésion à **Administrateurs de domaine** ou **Opérateurs de compte** pour créer le compte

Créer la clé racine KDS (si elle n'est pas déjà créée)

Exécutez sur un contrôleur de domaine dans une session PowerShell élevée :

Fenêtre de terminal

```
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
```

Cela rend la clé racine immédiatement disponible.

Créer le gMSA

Utiliser New-ADServiceAccount :

Fenêtre de terminal

```
New-ADServiceAccount `
  -Name "WebPortalSvc" `
  -DNSHostName "WebPortalSvc.domain.local" `
  -PrincipalsAllowedToRetrieveManagedPassword "YourServerGroup" `
  -Enabled $true
```

- Nom nom de compte gMSA
- Nom d'hôte DNS FQDN pour le compte
- Principaux autorisés à récupérer le mot de passe géré ordinateurs/groupe autorisé à utiliser ce gMSA

Accorder des droits administratifs (optionnel / selon les

besoins)

Par défaut, un gMSA n'a aucun privilège spécial.

Pour accorder un accès au niveau du domaine (optionnel) :

Fenêtre de terminal

```
Add-ADGroupMember -Identity "Domain Admins" -Members "WebPortalSvc$"
```

Pour accorder des droits d'administrateur local/capacité de connexion (si nécessaire) :

Fenêtre de terminal

```
Add-ADGroupMember -Identity "Administrateurs" -Members "WebPortalSvc$"
```

Important : le traînant $ est requis pour les références de compte gMSA dans AD.

Exigence de redémarrage

Un redémarrage est nécessaire avant de continuer et d'installer/utiliser le compte de service. Veuillez également actualiser les politiques.

Installer le gMSA sur les serveurs cibles

Exécutez sur chaque serveur qui utilisera le gMSA :

Fenêtre de terminal

```
Install-ADServiceAccount -Identity "WebPortalSvc"
```

Installation de test :

Fenêtre de terminal

```
Test-ADServiceAccount -Identity "WebPortalSvc"
```

Configurer les services pour utiliser le gMSA

1. Accorder **Se connecter en tant que service** au compte :

- Ouvrir l'éditeur de stratégie de groupe
- Allez à : Configuration de l'ordinateur > Paramètres Windows > Paramètres de sécurité > Politiques locales > Attribution des droits d'utilisateur
- Ouvrir Se connecter en tant que service
- Ajouter DOMAIN\WebPortalSvc$

2. Assurez-vous des autorisations NTFS sur les fichiers/dossiers du portail Web :

   - Clic droit sur le dossier/application exécutable > Propriétés > Sécurité
   - Ajouter DOMAIN\WebPortalSvc$
   - Accorder au moins **Lire et exécuter** ou **Contrôle total** si nécessaire pour votre déploiement

3. Configurer l'identité du service :

   - Compte : DOMAIN\WebPortalSvc$
   - Mot de passe : **laisser vide**

Configurer le nom principal de service (SPN)

Le service web doit être enregistré dans Kerberos.

Exécuter sur un contrôleur de domaine :

Fenêtre de terminal

```
setspn -A HTTP/webserver.domain.com DOMAIN\WebPortalSvc
```

Remplacez par votre FQDN de serveur et votre compte.

Si le serveur d'hébergement du portail Web utilise HTTP.sys, enregistrez SPN contre le compte machine :

Fenêtre de terminal

```
setspn -S HTTP/portal.hiyoko.com:8008 WIN-HLBO0AGABB7
setspn -S HTTP/portal.hiyoko.com:8009 WIN-HLBO0AGABB7
```

Configurer le réseau sur la machine cliente

Pour placer un client joint au domaine dans le sous-réseau correct :

1. Identifier l'interface réseau correcte
2. Supprimer l'IP statique existante (si incorrecte)
3. Attribuer une adresse IP statique, un masque de sous-réseau et une passerelle par défaut correspondant au sous-réseau DNS/DC
4. Définir les adresses du serveur DNS

Important : attribuez des adresses IP statiques au contrôleur de domaine et aux clients. La synchronisation de la politique de sécurité nécessite que les machines soient dans le même sous-réseau dans ce contexte.

Autoriser la connectivité client requise

UDP/TCP 53 peut être bloqué, ce qui empêche les requêtes DNS.

Étapes de dépannage

Vérifier l'état du serveur DNS

Sur le contrôleur de domaine :

Fenêtre de terminal

net start DNS

Vérifiez que le service DNS est en cours d'exécution.

Vérifier l'IP du serveur DNS

Sur le client :

Fenêtre de terminal

```
ipconfig /all
```

Confirmez que l'adresse IP du serveur DNS correspond à l'adresse IP du contrôleur de domaine.

Tester la connectivité de base

Sur le client :

Fenêtre de terminal

```
ping <DC_IP_Address>
```

Si le ping échoue, dépannez le routage réseau/firewall.

Vérifiez les règles du pare-feu

Assurez-vous que le UDP/TCP 53 entrant/sortant est autorisé sur le client et le serveur.

Test avec nslookup

Fenêtre de terminal

nslookup domain.com <DC_IP_Address>

Si cela fonctionne, le serveur DNS par défaut peut être mal configuré ou inaccessible.

Vérifier le Visualiseur d'événements

Sur le contrôleur de domaine, vérifiez les erreurs liées au DNS.

Configurer Mozilla Firefox pour l'authentification intégrée de Windows

Firefox n'utilise pas WIA par défaut.

Étape 1 : négocier des URI de confiance

1. Ouvrir Firefox
2. Aller à à propos:config
3. Accepter l'avertissement
4. Définir
   network.negotiate-auth.trusted-uris
   à vos domaines, par exemple :

- intranet.domaine.com, domaine.com

Étape 2 : URIs NTLM de confiance

Définir network.automatic-ntlm-auth.uris-de-confiance à la même liste de domaines.

Étape 3 : URIs de délégation Kerberos (si nécessaire)

Définir network.negotiate-auth.delegation-uris D'accord, je suis prêt à traduire le texte que vous fournirez. Veuillez me donner le texte à traduire.

- domain.com

Étape 4 : redémarrer le navigateur

Redémarrez Firefox pour appliquer les modifications.

Configurer Google Chrome pour l'authentification intégrée de Windows

Chrome utilise les paramètres d'authentification Windows/system.

Via la stratégie de groupe (recommandé)

1. Télécharger les modèles ADMX de Chrome :
   - https://chromeenterprise.google/policies/

2. Copier
   chrome.admx
   et
   chrome.adml
   à :
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\fr-FR

3. Ouvrir gpedit.msc
4. Allez à :
   - Configuration de l'ordinateur > Modèles d'administration > Google > Google Chrome

5. Activer l'authentification intégrée pour les sites intranet et configurer les sites de confiance :
   - intranet.domaine.com, domaine.com

6. Appliquer la politique :

Fenêtre de terminal

```
gpupdate /force
```

Autres méthodes

D'autres méthodes (commutateurs et drapeaux de ligne de commande Chrome) n'ont pas réussi dans ce contexte.

Configurer Microsoft Edge pour l'authentification intégrée de Windows

Edge utilise les politiques de Microsoft Edge et les paramètres de zone de sécurité de Windows.

Activer la connexion automatique dans la zone intranet

1. Ouvrir les options Internet
2. Sécurité onglet > Intranet local > Niveau personnalisé
3. Sous
   Authentification de l'utilisateur
   , ensemble :
   - Connexion automatique uniquement dans la zone Intranet

Configurer les politiques Edge via GPO

Étape 1 : installer les modèles ADMX Edge

1. Télécharger :

- https://www.microsoft.com/fr-fr/edge/business/download

2. Copier
   msedge.admx
   et
   msedge.adml
   à :
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\fr-FR

Étape 2 : modifier les paramètres de la politique

1. Ouvrir gpedit.msc
2. Allez à :
   - Configuration de l'ordinateur > Modèles d'administration > Microsoft Edge

3. Activer :
   - Configurer la liste des serveurs auxquels Microsoft Edge peut déléguer des identifiants.

4. Configurer les serveurs de confiance :
   - intranet.domaine.com, domaine.com

Étape 3 : appliquer les politiques

Fenêtre de terminal

```
gpupdate /force
```

Autres méthodes

D'autres méthodes (commutateurs et indicateurs de ligne de commande Edge) n'ont pas réussi dans ce contexte.

Dépannage de l'authentification intégrée

Vérifier les tickets Kerberos

Sur le client Windows :

Fenêtre de terminal

klist

Vous devriez voir un ticket pour HTTP/webserver.domain.com .

Effacer les identifiants/tickets mis en cache

Fenêtre de terminal

klist purge

Vérifier l'enregistrement SPN

Sur le contrôleur de domaine :

Fenêtre de terminal

```
setspn -L serviceaccount
```

Assurez-vous HTTP/webserver.domain.com est répertorié.

Déboguer Kerberos dans Firefox

Démarrer Firefox avec journalisation :

Fenêtre de terminal

```
set NSPR_LOG_MODULES=negotiateauth:5
set NSPR_LOG_FILE=%USERPROFILE%\Desktop\firefox.log
start firefox.exe
```

Examen firefox.log pour les erreurs d'authentification.

Vérifiez les politiques de Chrome

Dans Chrome, ouvrez :

chrome://policy

Assurez-vous AuthServerWhitelist et AuthNegotiateDelegateWhitelist sont appliquées.

Vérifier les politiques Edge

Dans Edge, ouvrez :

edge://policy

Assurez-vous AuthServerWhitelist et AuthNegotiateDelegateWhitelist sont appliquées.

Fin de vie version 1-12

Remote Access v12 (et toutes les versions antérieures) cesseront de fonctionner sur tous les ordinateurs Windows.
Les interruptions de service commenceront en janvier 2026 et s'étendront progressivement jusqu'à l'arrêt complet en avril.

La mise à jour vers une version LTS ou la dernière version nécessite un **abonnement de support actif** pour votre licence. Si ce n'est pas le cas, nous vous invitons à souscrire à un abonnement de support depuis votre portail de licence et à mettre à jour votre licence depuis votre Admintool avec votre fichier .LIC pour bénéficier de la mise à jour.

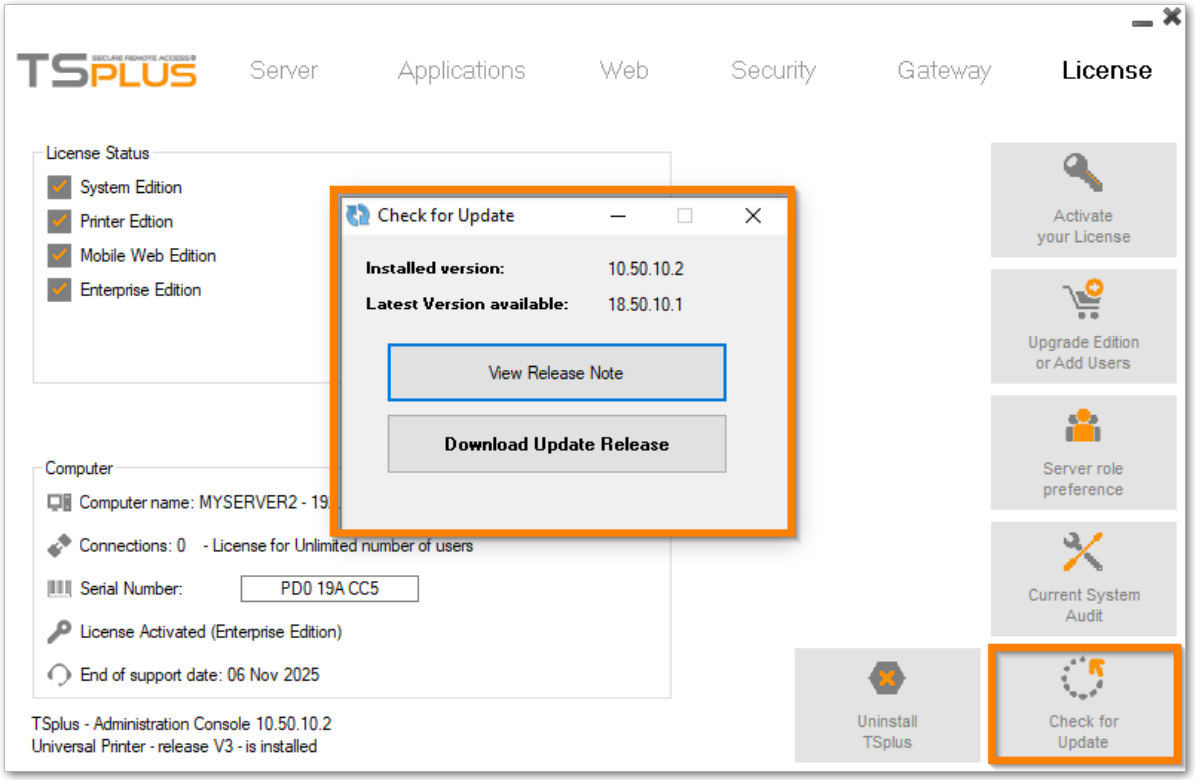
Si vous ne parvenez pas à ajouter un abonnement de support ou si vous recevez un message d'erreur,
contactez-nous en utilisant notre Contactez le support , fournissant :

- Votre numéro de licence au format PXX XXX XXX Visible dans l'onglet de licence de l'Admintool
- Votre facture d'achat de licence
- Votre facture d'abonnement de support

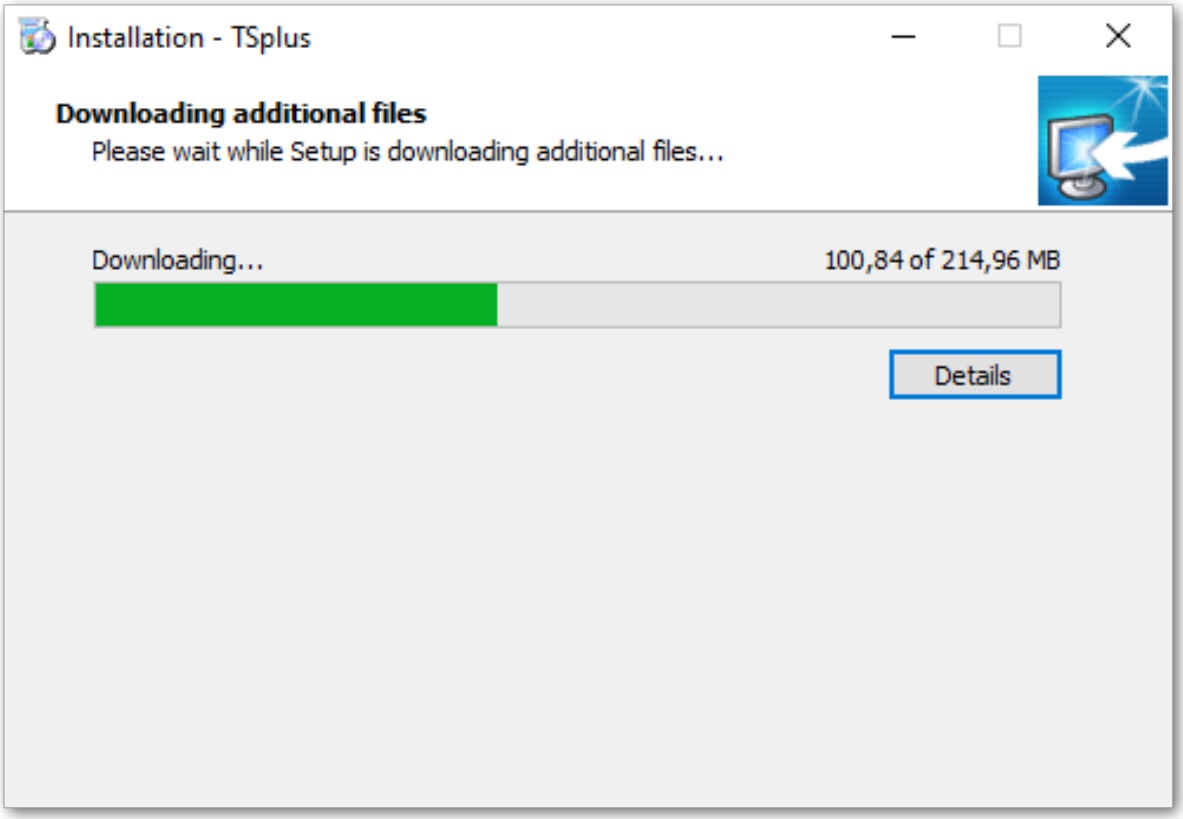
Mise à jour de votre version v10

Si vous souhaitez installer une LTS au lieu de la dernière version, allez à la page LTS)

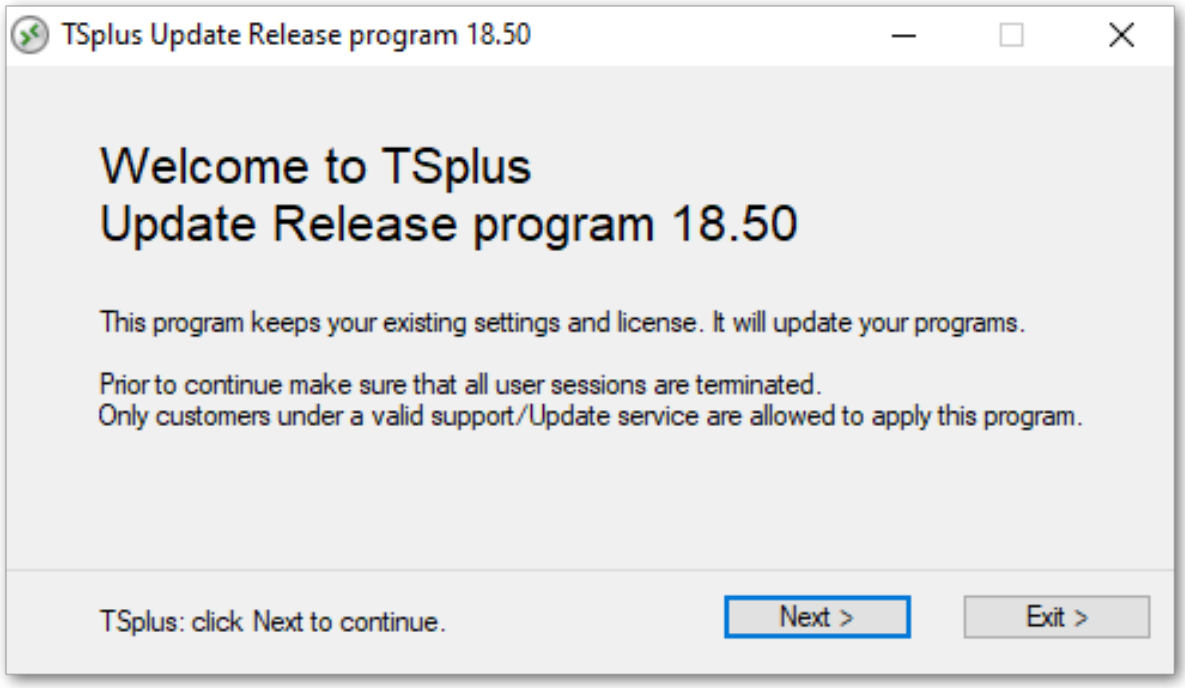
Depuis votre version en ligne 10, cliquez sur le champ suivant pour télécharger le **UpdateRelease.exe**
Vous pouvez également télécharger le UpdateRelease.exe pour commencer la procédure de mise à jour.



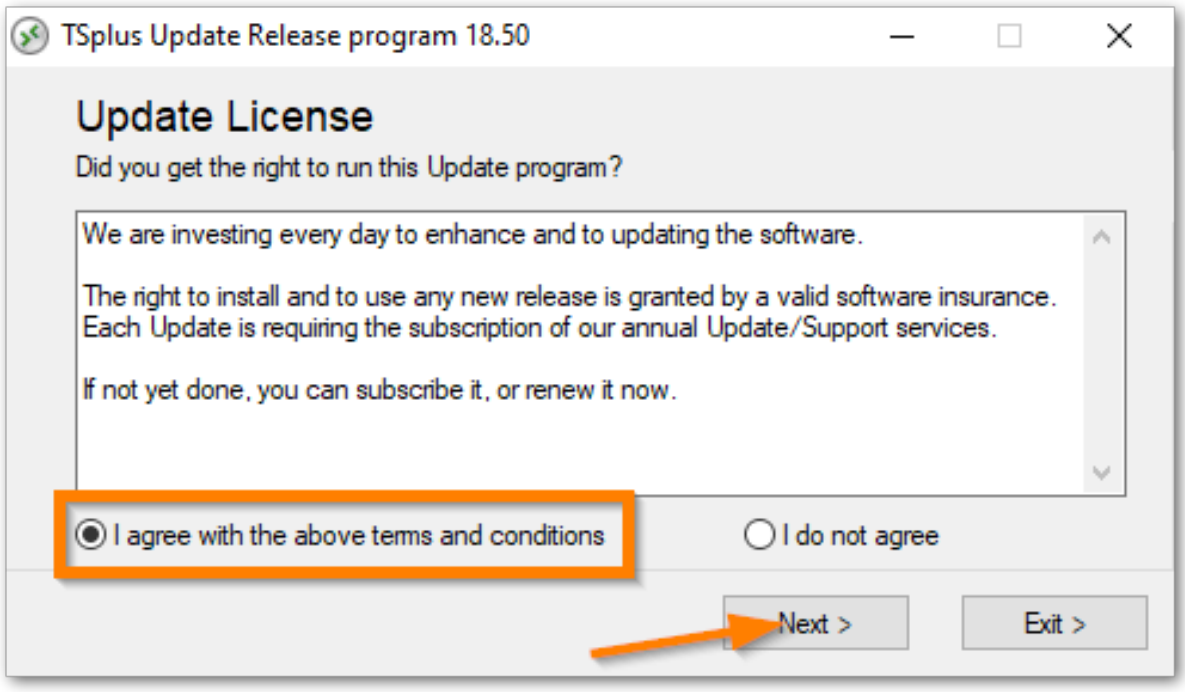
Téléchargez le updaterelease.exe et exécutez l'exécutable.



Le programme de mise à jour apparaîtra.



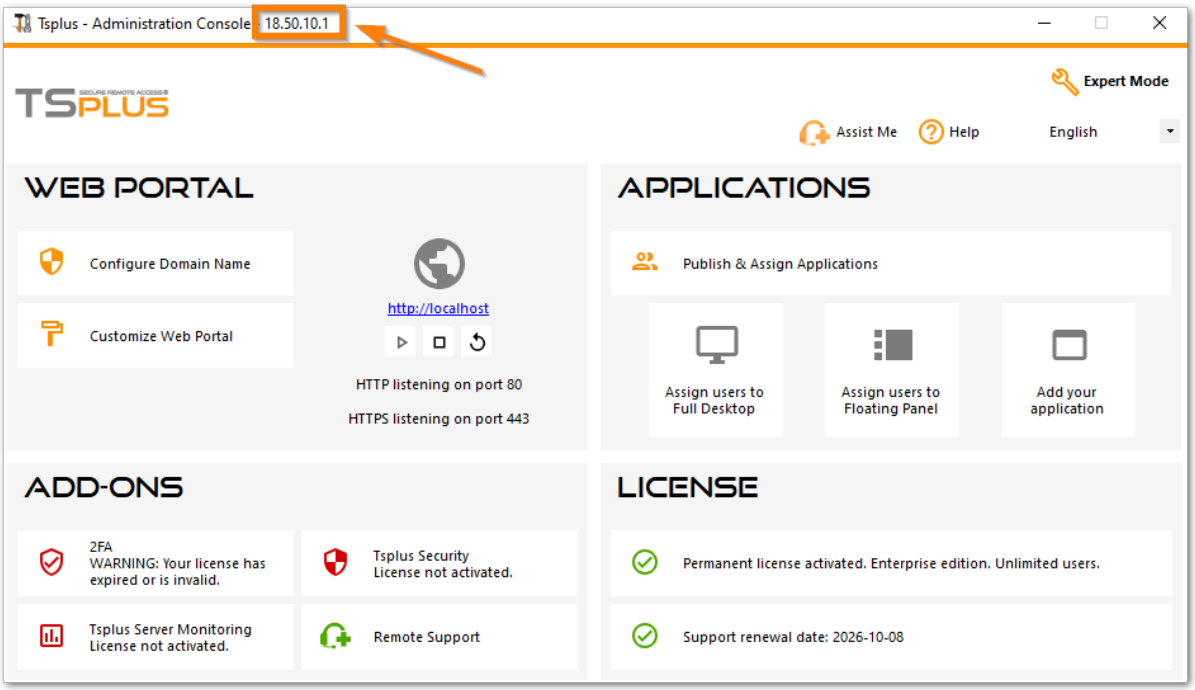
Acceptez les conditions et cliquez
SUIVANT



Suivez toutes les étapes et redémarrez ensuite votre serveur à la fin de la migration.

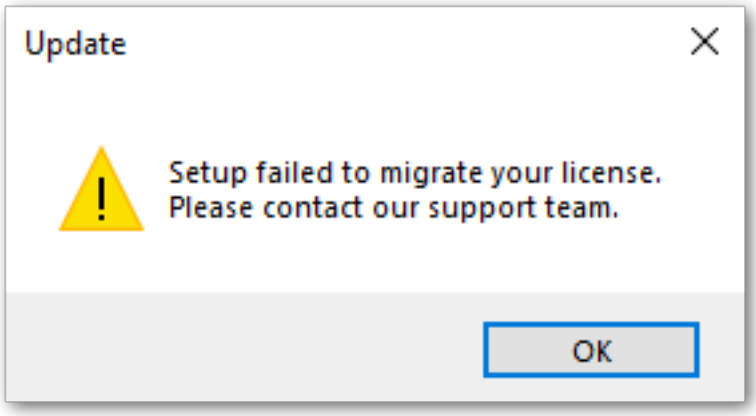
- Lorsque vous avez terminé, **Redémarrez votre serveur** pour compléter la mise à jour.

Lancez l'AdminTool. Félicitations, vous êtes maintenant à la version 19.



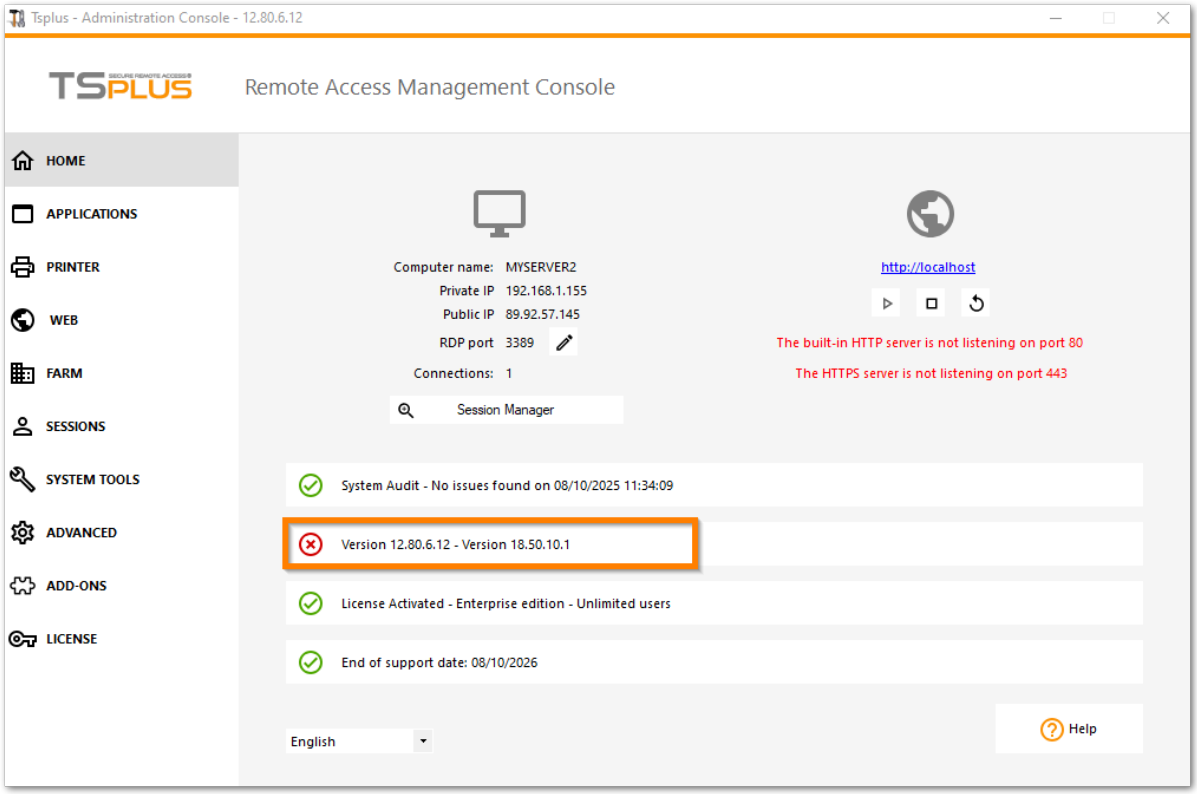
Message d'erreur v10

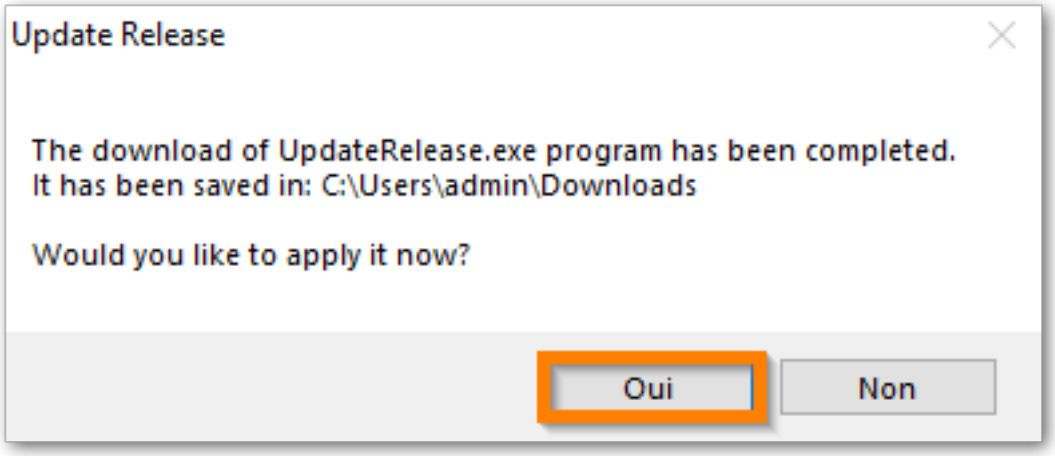
Si vous recevez ce message d'erreur,
Contactez le support
pour désinstaller Remote Access. Veuillez fournir le numéro de licence au format PXX XXX XXX ainsi qu'une preuve de la facture d'achat du support.

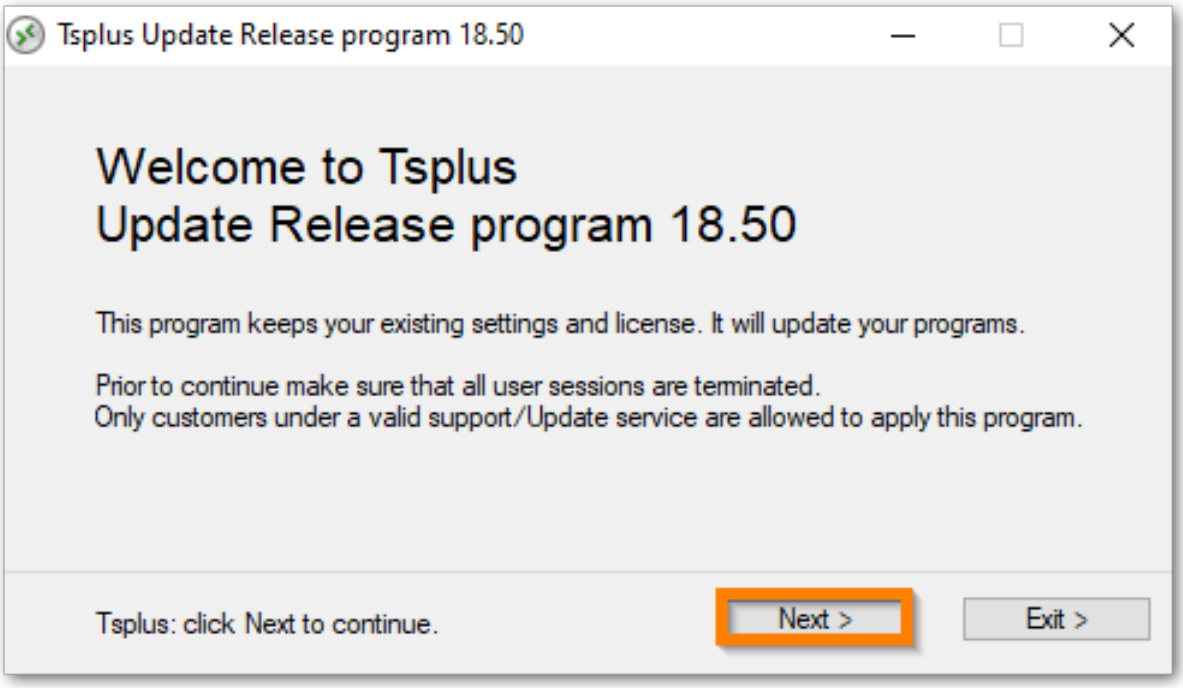


Mise à jour de votre version v12

Depuis votre version en ligne 12, cliquez sur le champ suivant pour télécharger le **UpdateRelease.exe**
Vous pouvez également télécharger le UpdateRelease.exe pour commencer la procédure de mise à jour.

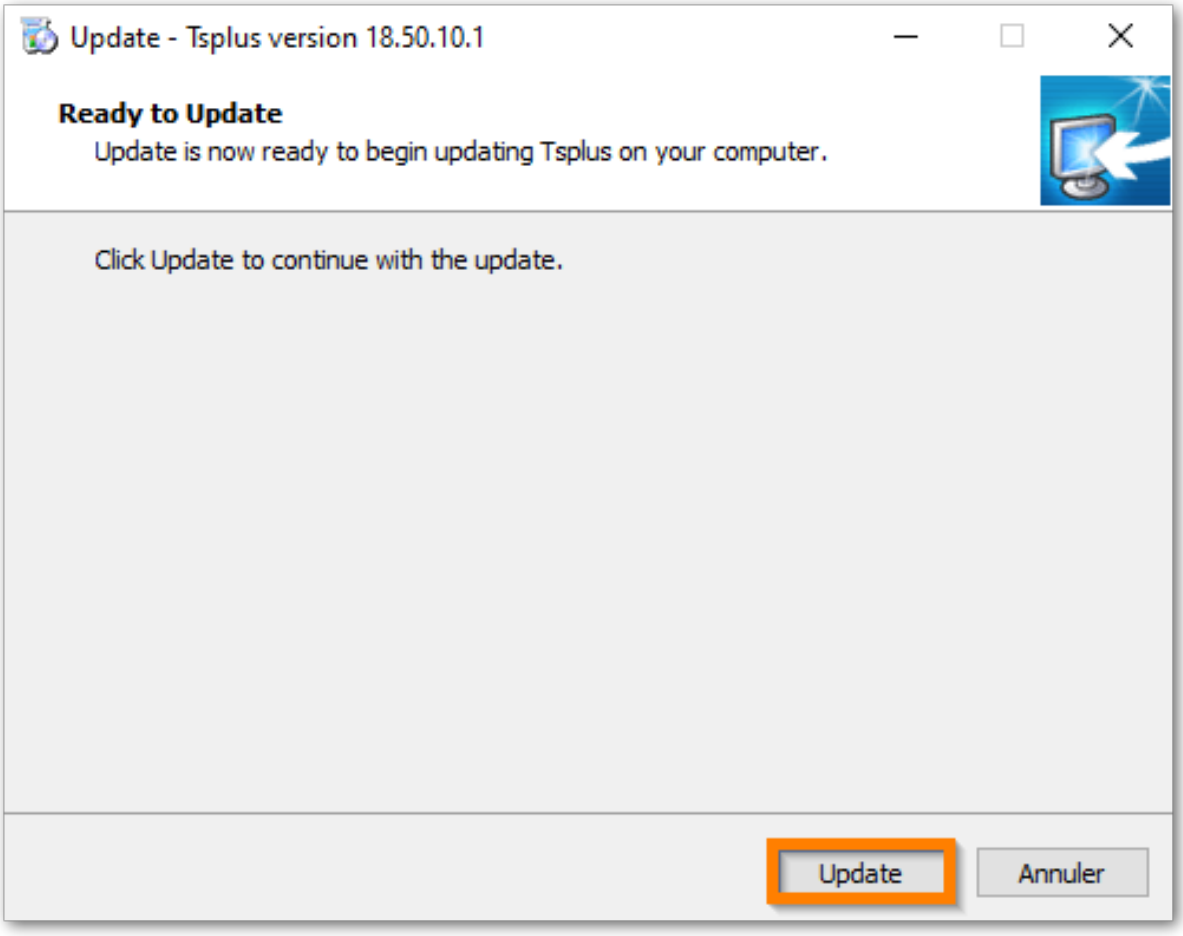

Tsplus - Administration Console - 12.80.6.12
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Computer name: MYSERVER2
Private IP 192.168.1.155
Public IP 89.92.57.145
RDP port 3389
Connections: 1
Session Manager
http://localhost
The built-in HTTP server is not listening on port 80
The HTTPS server is not listening on port 443
System Audit - No issues found on 08/10/2025 11:34:09
Version 12.80.6.12 - Version 18.50.10.1
License Activated - Enterprise edition - Unlimited users
End of support date: 08/10/2026
English
Help

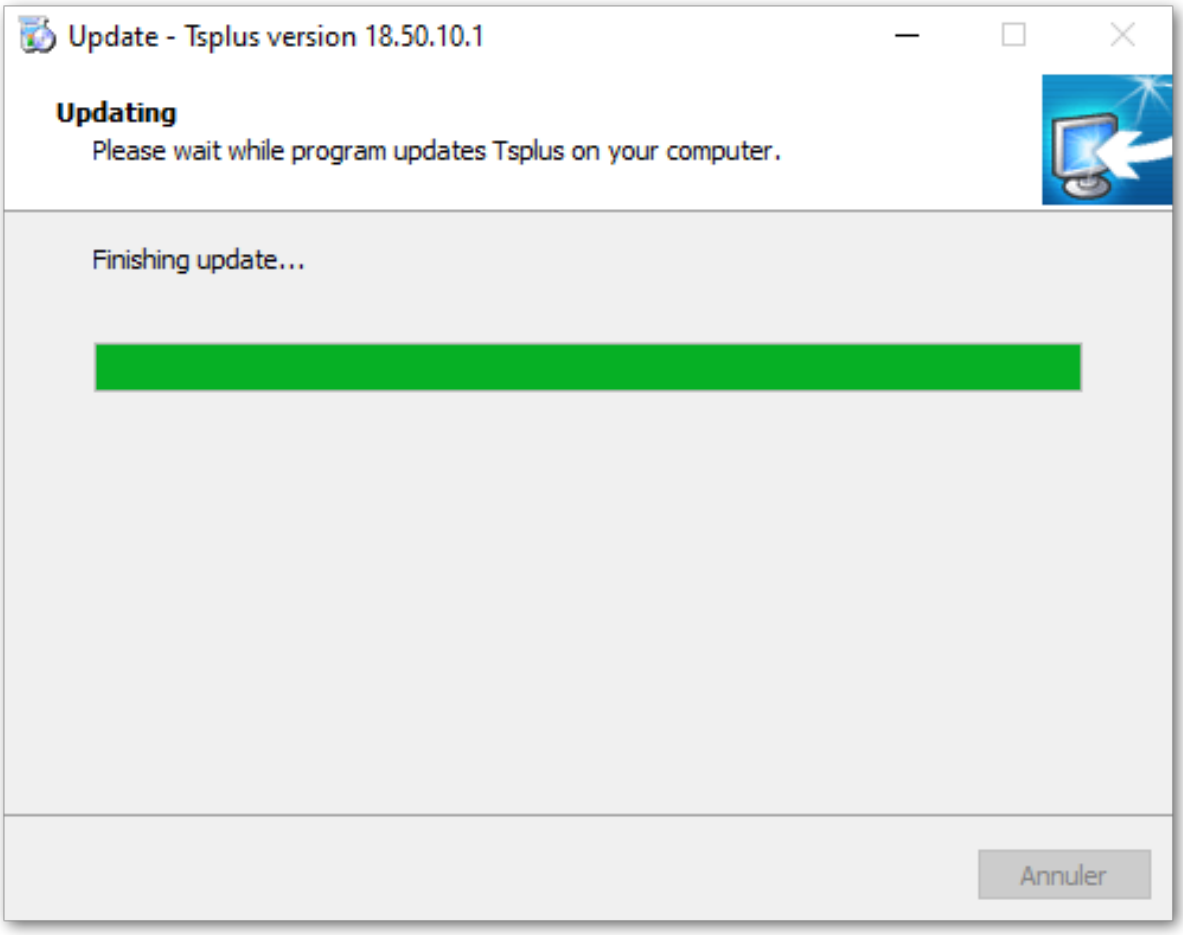

Update Release
The download of UpdateRelease.exe program has been completed.
It has been saved in: C:\Users\admin\Downloads
Would you like to apply it now?
Oui
Non



- Acceptez les conditions et cliquez sur SUIVANT

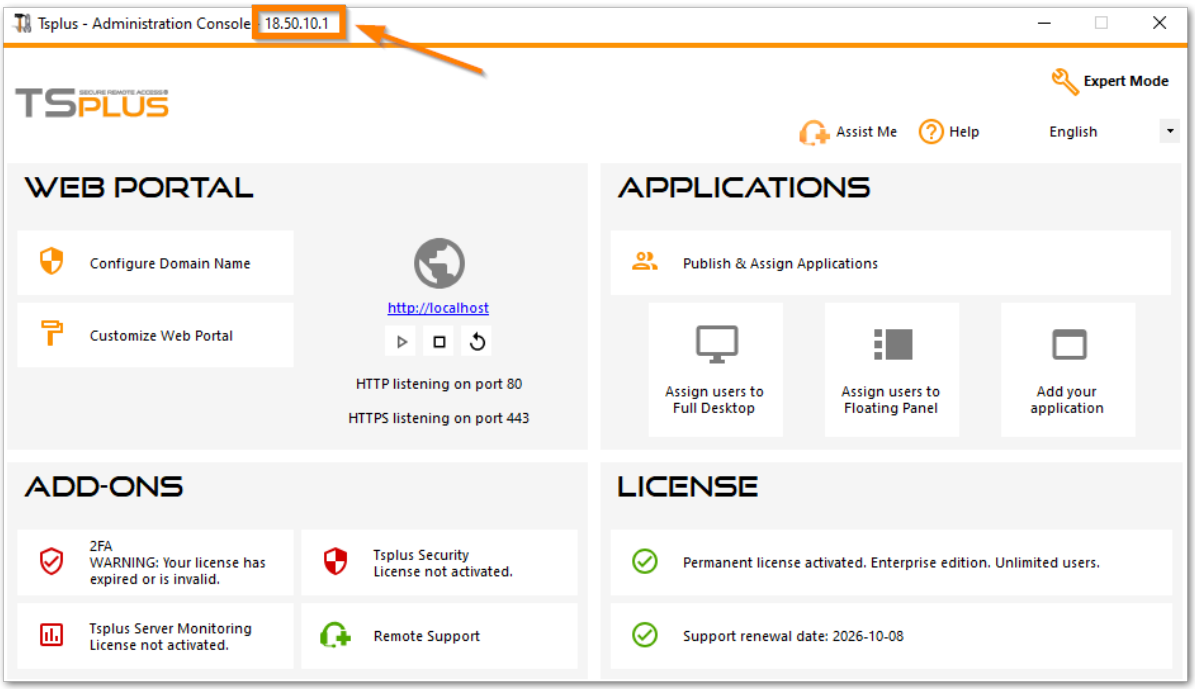
Une fois téléchargé, cliquez
Mise à jour
pour commencer le processus.





- Lorsque vous avez terminé, **Redémarrez votre serveur** pour compléter la mise à jour.

Lancez l'AdminTool. Félicitations, vous êtes maintenant à la version 19.



Message d'erreur v12

Si vous recevez ce message d'erreur, Contactez le support pour désinstaller Remote Access. Veuillez fournir le numéro de licence au format PXX XXX XXX et également une preuve de la facture d'achat du support.

Appliquer le protocole HTTPS

Cas standard

À partir de la version 9.20 de Terminal Service Plus, vous pouvez rediriger chaque requête web utilisant HTTP vers le protocole sécurisé HTTPS.

Pour activer cette fonctionnalité sur un serveur, modifiez (ou créez) le fichier “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” et ajoutez la ligne suivante :

disable_http_only=true

Enregistrez le fichier et redémarrez les serveurs web de Terminal Service Plus (AdminTool > Web > Redémarrer les serveurs web ou relisez la configuration en accédant http://127.0.0.1/w0j3?settings.bin).

Une fois cette fonctionnalité activée, vous pouvez essayer d'accéder à la page web non sécurisée à l'adresse :

http://votre-serveur

et il redirigera automatiquement votre demande vers la page sécurisée du portail Web à :

https://your-server

Cas spécial : Ports Web personnalisés

Si vous utilisez un port spécifique pour servir HTTPS, modifiez le fichier “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” et utilisez la ligne suivante à la place de la ligne décrite ci-dessus :

disable_http_only="domain.com:4431"

où domain.com est le nom de votre propre serveur hôte et 4431 est votre port HTTPS personnalisé.

Enregistrez le fichier et redémarrez les serveurs web de Terminal Service Plus (AdminTool >

Web > Redémarrer les serveurs web).

Une fois cette fonctionnalité activée, vous pouvez essayer d'accéder à la page web non sécurisée à l'adresse :

http://domain.com

et il redirigera automatiquement votre demande vers la page sécurisée du portail Web à :

https://domain.com:4431

Comment : Même si ce n'est pas sécurisé, mais que vous souhaitez désactiver ssl/https sur le port http, modifiez le fichier settings.bin et ajoutez : disable_ssl_on_http=true, enregistrez et redémarrez les serveurs.

Désactiver http sur https

Par défaut, l'accès est autorisé https://my-domain.com , https://my-domain.com:80 , http://my-domain.com:443 Donc, cela permet http sur le port 443 ou autorise https sur le port 80, cela n'a pas d'impact sur la sécurité et facilite le retour à une connexion xhr dégradée lorsque le support des websockets n'est pas possible. Mais si vous souhaitez le désactiver, modifiez le fichier settings.bin et ajoutez la ligne suivante :

disable_http_on_https=true

Puis redémarrez les serveurs web de Terminal Service Plus (AdminTool > Web > Redémarrer les serveurs web ou relire la configuration) http://127.0.0.1/w0j3?settings.bin)

Application de HTTPS et validation gratuite du certificat SSL

Veuillez noter que cette fonctionnalité d'application HTTPS est entièrement compatible avec notre Certificat SSL gratuit fonctionnalité.

Imposer l'utilisation du portail web pour se connecter au serveur

À partir de la version 6.60 de Terminal Service Plus, vous pouvez bloquer/désactiver toute tentative de connexion utilisant mstsc.exe (ou tout client RDP) sur le port ouvert/redirigé (80 ou 443).

Cette fonctionnalité permet uniquement les accès depuis le portail Web de Terminal Service Plus et désactive toute autre connexion RDP sur le port 80/443.

Pour activer cette fonctionnalité sur un serveur, modifiez le fichier C:\Program Files (x86)\TSplus\UserDesktop\files\AppControl.ini et ajoutez/modifiez la variable suivante :

Sécurité Block_rdp_splitter=oui

Équilibrage de charge

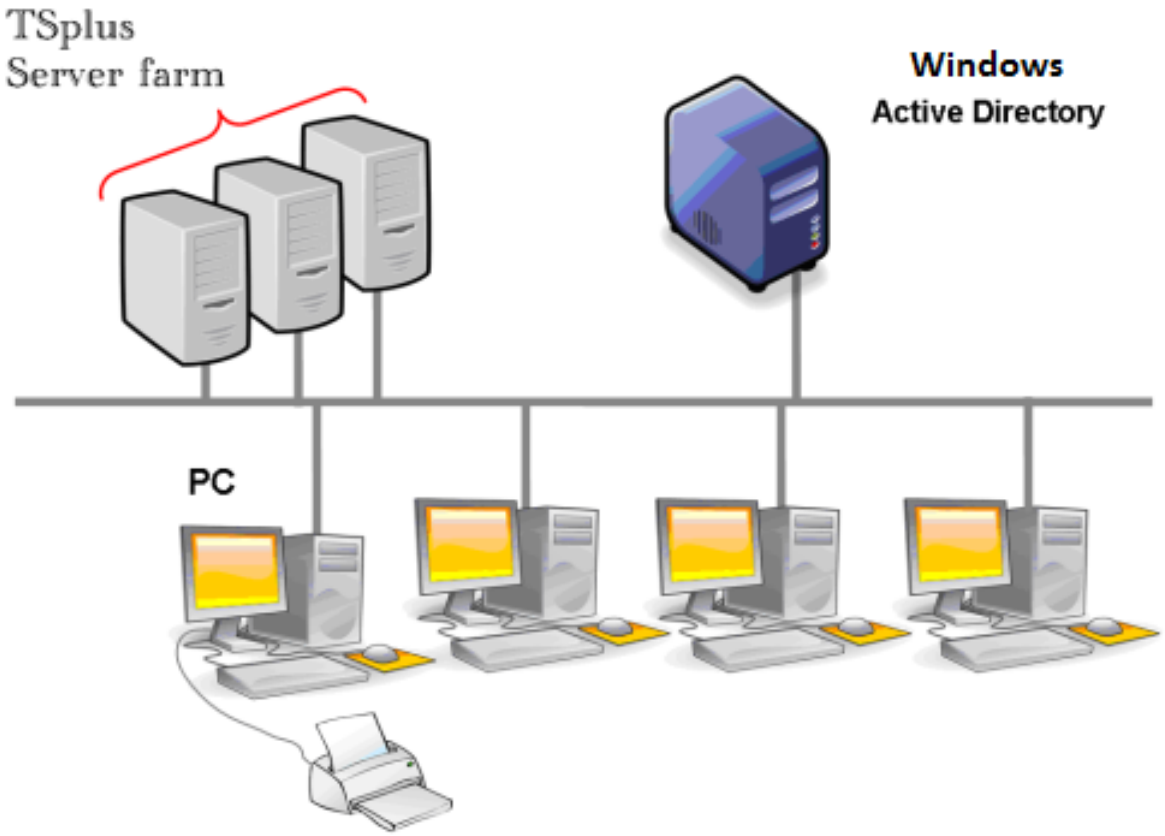
Pré-requis

En utilisant cette fonctionnalité, vous pourrez gérer un environnement équilibré en charge.

Cela signifie que la charge de tous vos utilisateurs sera répartie entre vos serveurs. La charge de travail sera partagée entre tous les serveurs de votre ferme.

L'équilibrage de charge permet d'utiliser un nombre illimité de serveurs avec équilibrage de charge et est disponible avec l'édition Entreprise (une licence valide par serveur). Cette capacité très puissante et avancée doit être utilisée lorsqu'un grand nombre d'utilisateurs/serveurs doit être déployé.

Important : Activer simplement l'équilibrage de charge redirigera les utilisateurs vers le serveur le moins chargé de la ferme, indépendamment des serveurs assignés configurés pour les utilisateurs. Si vous avez l'intention d'utiliser l'équilibrage de charge ET l'assignation de serveur, assurez-vous de cocher la case « Équilibrer la charge sur les serveurs assignés ».



Nous recommandons généralement d'utiliser un serveur pour 50 utilisateurs simultanés.
Vous pouvez dépasser +50 utilisateurs en fonction de la puissance de votre serveur et de la consommation des ressources des applications des utilisateurs.

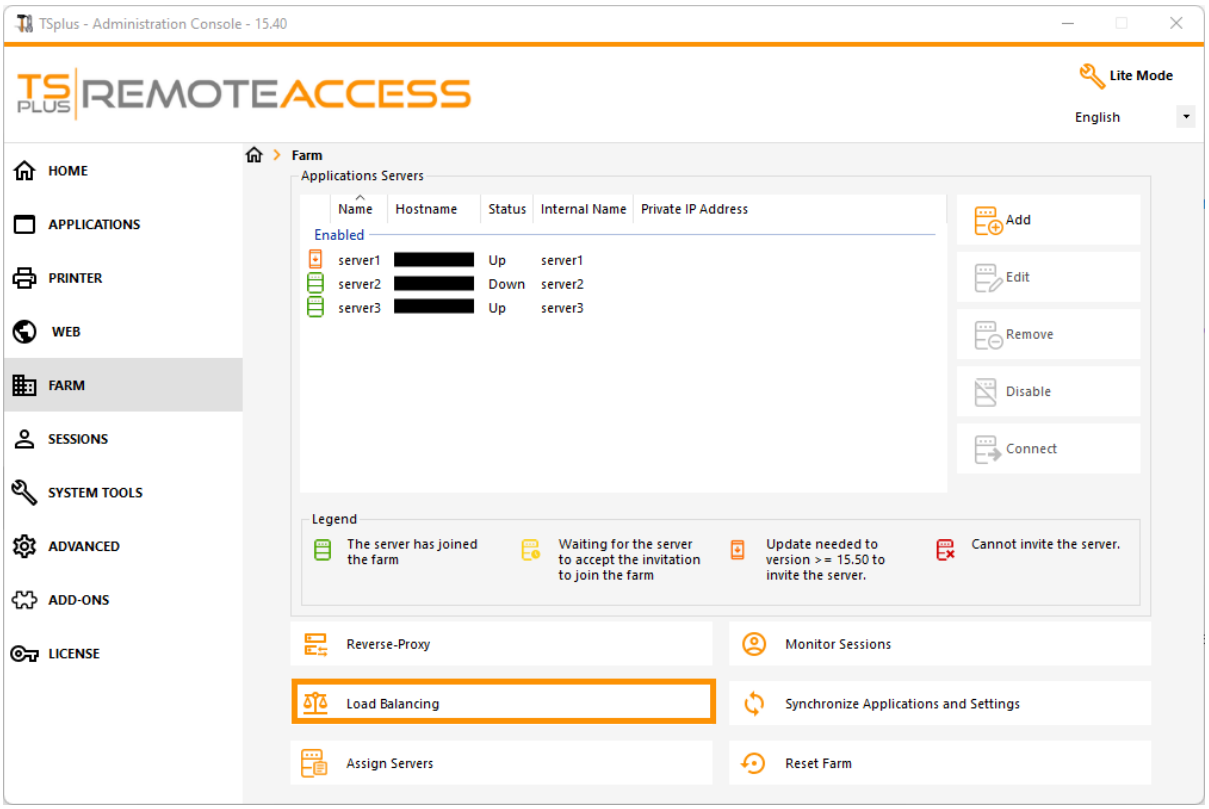
Clients générés et accès Web

Il existe trois façons de se connecter à un cluster équilibré en charge :

- Utiliser un **Client généré** programme exécutable, créé par le Générateur de client portable)
- Utiliser un **Accès au portail Web** en l'activant dans la fenêtre Préférences du Portail Web.
- Avec le TSplus App depuis votre appareil mobile.

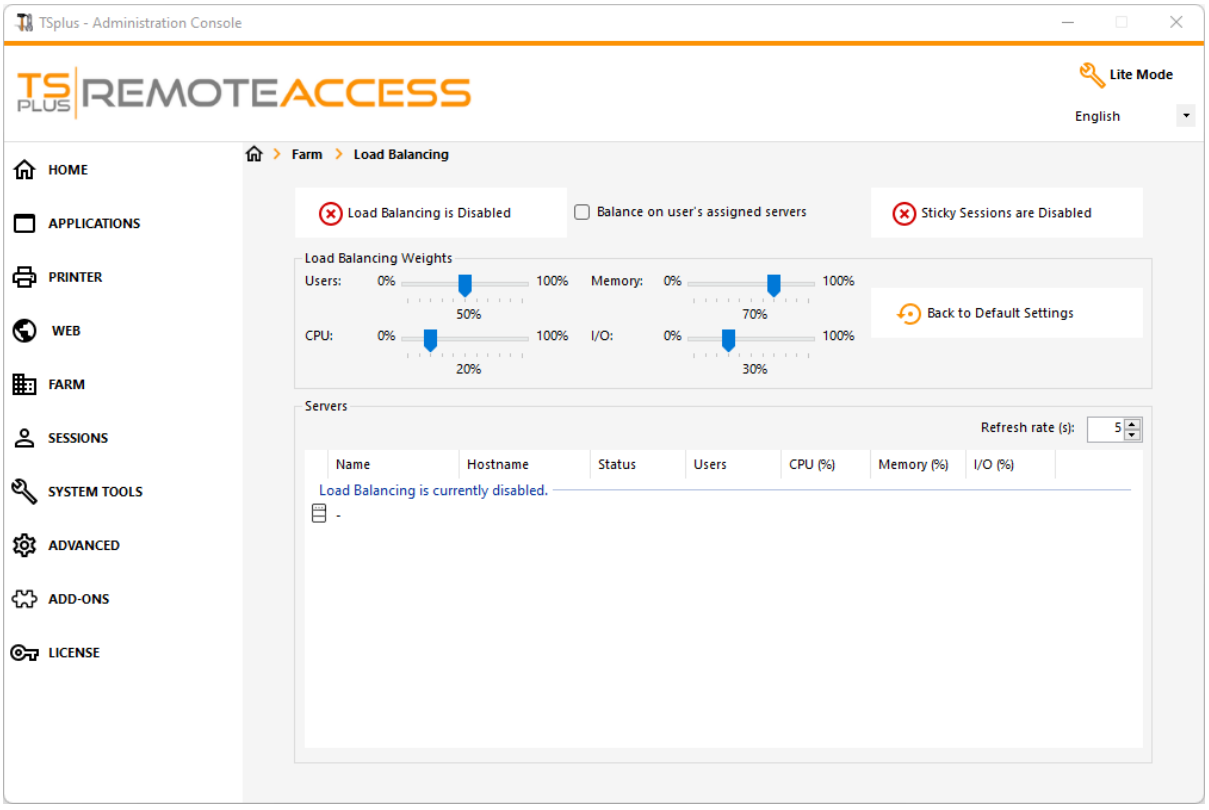
Fenêtre principale de répartition de charge

Le gestionnaire d'équilibrage de charge se trouve sous l'onglet Ferme de l'AdminTool :



Cette fenêtre vous permet de configurer l'équilibrage de charge. Elle répertorie tous les serveurs de votre ferme de serveurs équilibrés et vous permet d'activer, de désactiver et de configurer l'équilibrage de charge (plus d'informations ci-dessous).

Cliquez sur les boutons de l'image ci-dessous pour accéder aux informations correspondantes :



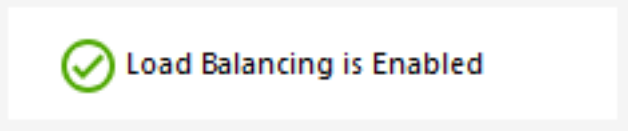
En haut de la fenêtre de répartition de charge, vous verrez un grand bouton :

- Ce bouton affiche l'état actuel de l'équilibrage de charge.
- Si vous cliquez dessus, cela activera ou désactivera l'équilibrage de charge en fonction de son état actuel.

Voici le bouton lorsque l'équilibrage de charge est **Désactivé** Un clic dessus l'activera.



Voici le bouton lorsque l'équilibrage de charge est **Activé** Un clic dessus le désactivera.



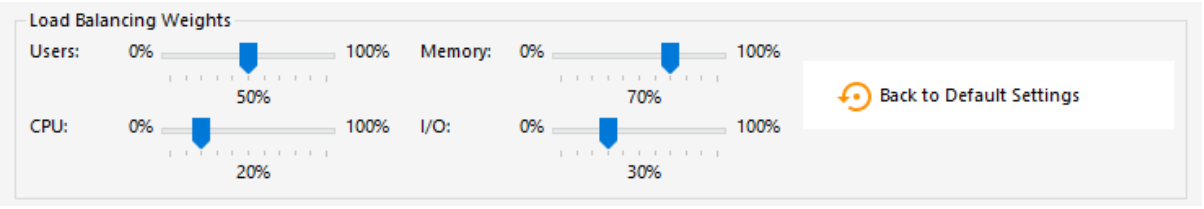
Comment le répartition de charge choisit-il un serveur ?

Lorsque l'équilibrage de charge est activé, l'utilisateur sera dirigé vers le serveur le moins chargé au moment de sa connexion.

Pour déterminer quel est le serveur le moins chargé, la charge de chaque serveur est calculée en utilisant une moyenne pondérée entre plusieurs indicateurs de performance :

- nombre d'utilisateurs connectés
- utilisation du processeur
- utilisation de la mémoire
- utilisation du disque

Vous pouvez modifier le poids (importance) de ces indicateurs en utilisant les curseurs suivants :



En utilisant ces curseurs, vous pourrez affiner l'équilibrage de charge et l'optimiser selon vos propres besoins. Par exemple, si vos utilisateurs lancent une application professionnelle avec de grandes exigences en mémoire, il pourrait être judicieux d'augmenter l'impact de la RAM dans le calcul de charge en utilisant le curseur "Mémoire".

Vous pouvez également réinitialiser ces valeurs en cliquant sur le bouton « Retour aux paramètres par défaut ».

Comment est calculée la charge du serveur ?

La charge de chaque serveur est calculée au besoin afin de décider sur quel serveur l'utilisateur doit être envoyé.

Pour ce calcul, nous utilisons un **moyenne pondérée** entre 4 métriques matérielles.

Les 4 curseurs vous permettent d'attribuer plus (ou moins) de poids à chacun de ces indicateurs, qui sont :

- Utilisateurs : nombre d'utilisateurs connectés
- CPU : pourcentage de temps processeur non inactif
- Mémoire : pourcentage de mémoire utilisée
- I/O : pourcentage de temps disque non inactif

Par exemple, si vous placez le curseur "Mémoire" sur son côté droit et tous les autres curseurs sur leur côté gauche, la charge de chaque serveur sera calculée en utilisant presque uniquement le pourcentage de mémoire utilisée - et vos utilisateurs seront envoyés vers le serveur ayant le plus de mémoire disponible.

- Lorsque le curseur est complètement à gauche, le poids utilisé dans le calcul de la charge sera de 1.
- Lorsque le curseur est complètement à gauche, le poids utilisé dans le calcul de la charge sera de 100.

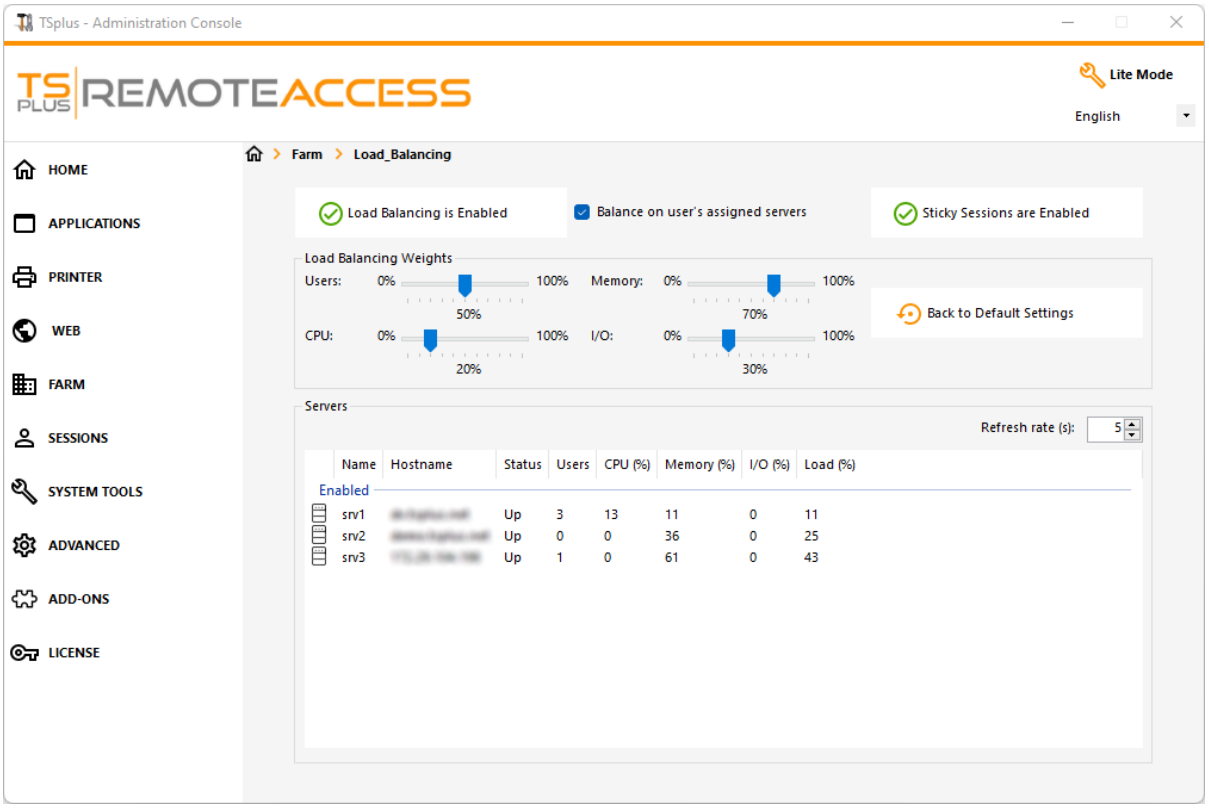
De plus, la charge d'un serveur donné dépend du ratio [ressources utilisées / ressources totales] ; donc si un serveur A est deux fois plus puissant qu'un serveur B, deux fois plus d'utilisateurs devraient être envoyés au serveur A qu'au serveur B (toutes choses étant égales par ailleurs).

Vous pouvez voir la liste des serveurs équilibrés en charge et les détails sur les indicateurs de performance de chaque serveur.

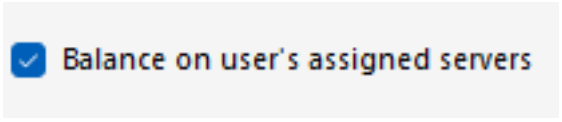
Les serveurs sont triés du moins chargé au plus chargé selon votre configuration.

La liste des statuts des serveurs équilibrés en charge est automatiquement actualisée. Cette

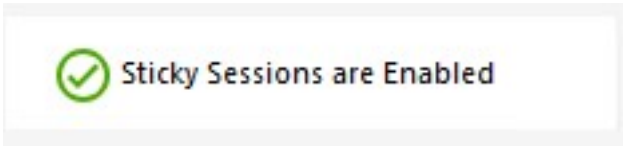
actualisation automatique s'arrête si la connexion devient indisponible. Vous pouvez changer le taux d'actualisation dans le coin supérieur droit de la boîte "Serveur".



L'équilibrage de charge peut également être effectué directement sur le serveur assigné à l'utilisateur en utilisant le **case à cocher "Équilibrer sur les serveurs assignés à l'utilisateur"** .
En conséquence, vous pourrez effectuer un équilibrage de charge sur les serveurs du département comptable uniquement pour les utilisateurs comptables, une fois que ces serveurs spécifiques auront été attribués aux utilisateurs comptables.



Vous pouvez activer la fonction de session persistante en cliquant sur le bouton droit de la fenêtre de répartition de charge :



Activation **liste des sessions existantes sur le web** est requis pour la fonctionnalité de sessions collantes de répartition de charge.

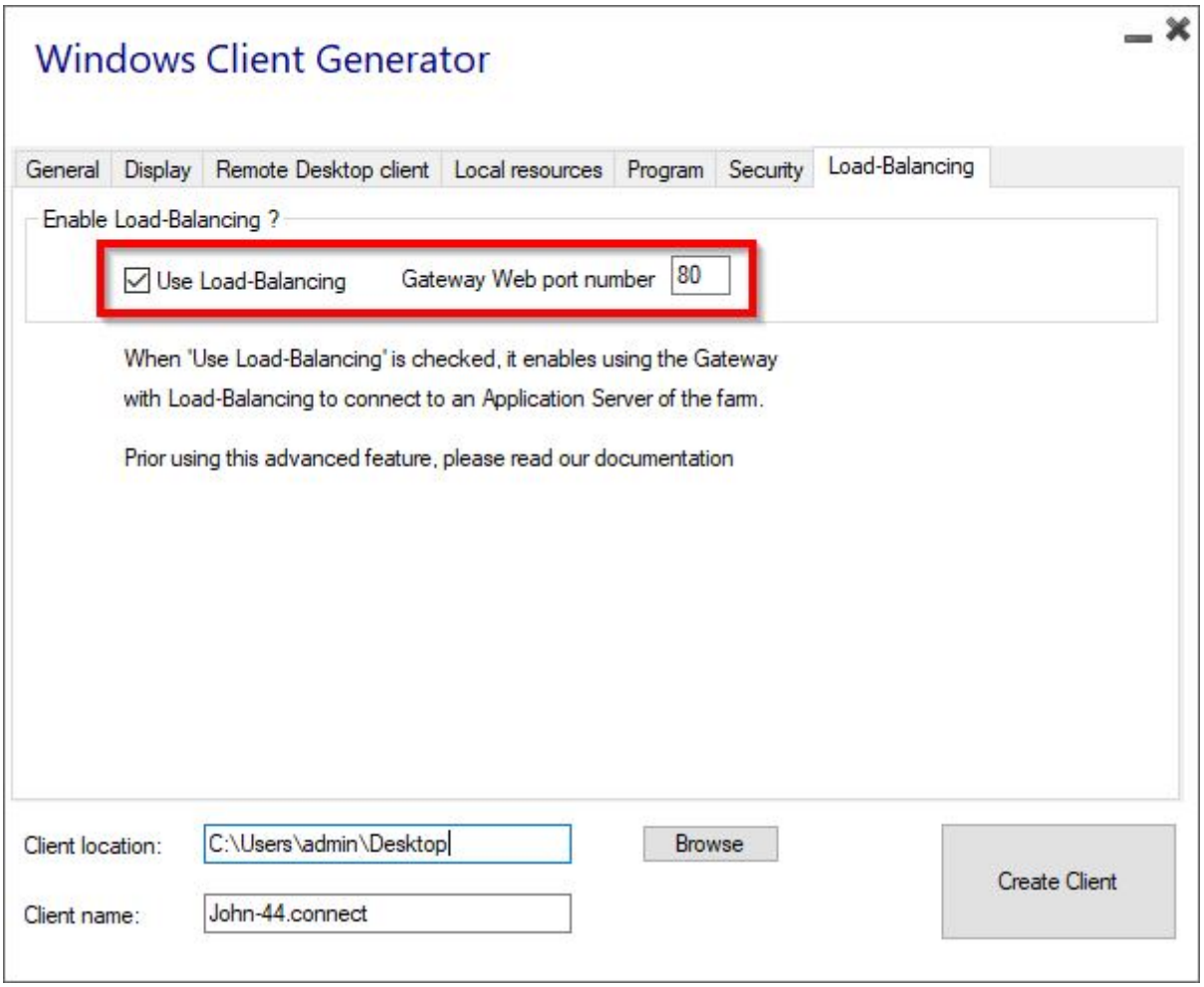
Cela vous permettra de vous reconnecter à une session déconnectée au lieu d'ouvrir une nouvelle session sur un autre serveur.

Pour activer **liste des sessions existantes sur le web** , définissez les éléments suivants paramètre à "non".

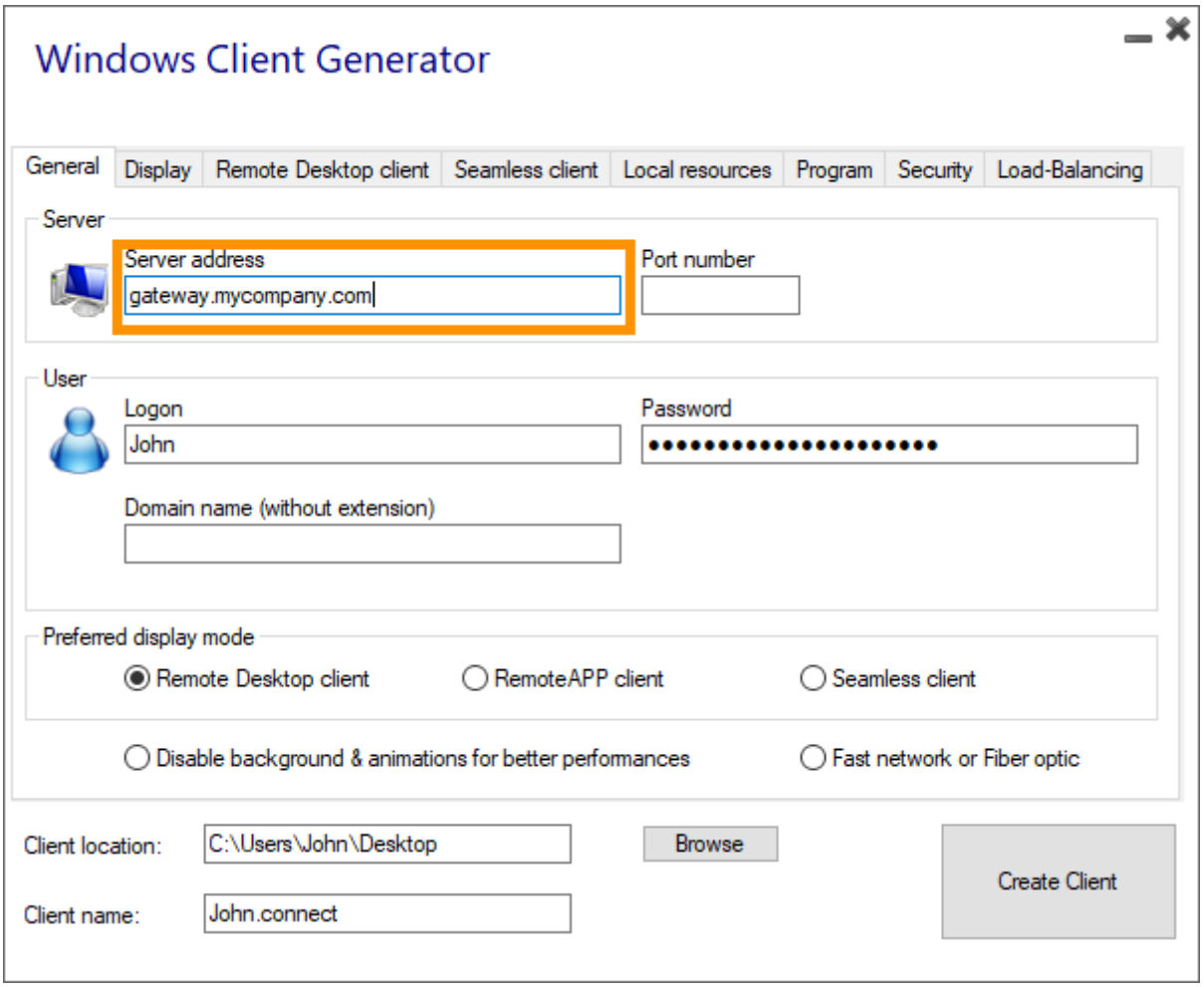
Équilibrage de charge à l'aide d'un client de connexion

Si vous souhaitez générer un Client de connexion pour qu'un utilisateur se connecte au serveur le moins chargé vous aurez besoin de Générateur de clients dans le " Équilibrage de charge " onglet vers :

- Cochez la case « Utiliser l'équilibrage de charge »
- Remplissez le champ "Numéro de port Web de la passerelle" avec le port HTTP ou HTTPS utilisé par votre serveur de passerelle.



- Utilisez l'adresse IP publique ou le nom d'hôte de votre serveur Gateway directement dans le champ « Serveur ».



Gestionnaire de ferme API

Nous sommes ravis de vous offrir une API puissante conçue pour fournir des capacités de gestion complètes pour vos fermes de serveurs.

Cette API vous permet d'intégrer sans effort notre logiciel à votre infrastructure existante, vous permettant de gérer et d'automatiser les opérations des serveurs avec vos propres scripts personnalisés.

Découvrez tout le potentiel de notre logiciel avec l'API robuste et polyvalente que nous proposons.

Exigences

Pour interroger l'API du gestionnaire de ferme, votre serveur devra :

- avoir un certificat SSL/TLS valide
- être ouvert sur le port 19956
- soyez joignable en utilisant le domaine couvert par votre certificat.

Exemples d'utilisation

Par exemple, les administrateurs peuvent utiliser le **Ferme > Obtenir la liste des serveurs** fonction pour récupérer une liste complète de tous les serveurs au sein de leur ferme, rationalisant la gestion des stocks. Le **Ferme > Initialiser la ferme** la fonction permet la configuration rapide d'une nouvelle ferme de serveurs, garantissant un processus de déploiement fluide. Pour la gestion des serveurs spécifique à l'utilisateur, le **Ferme > Liste des serveurs assignés à un utilisateur** La fonction aide à suivre et à gérer les affectations de serveur.

Dans les scénarios d'équilibrage de charge, le **Équilibrage de charge > choisir le serveur** et **Équilibrage de charge > Recharger** les fonctions permettent la sélection dynamique des serveurs et le rechargement des configurations de l'équilibreur de charge, optimisant la distribution des ressources et les performances. Le **ReverseProxy > Recharger** la fonction garantit que les modifications des paramètres de proxy sont appliquées sans temps d'arrêt. De plus, le **Serveur > Ajouter** et **Serveur > Modifier** les fonctions facilitent l'ajout et la

modification sans faille des serveurs dans la ferme.

Les administrateurs peuvent améliorer davantage leurs opérations en utilisant le **Paramètres > lister les paramètres** et **Paramètres > Appliquer les paramètres** fonctions pour récupérer et appliquer les paramètres de configuration sur l'ensemble de la ferme de serveurs.

Pour la gestion des sessions, le **Session > Déconnexion** et **Session > Déconnexion** les fonctions permettent la terminaison contrôlée des sessions utilisateur, tandis que le **Session > Liste des sessions des utilisateurs** fournit une vue détaillée des sessions actives à des fins de surveillance.

En tirant parti de ces puissantes fonctions API, vous pouvez atteindre une plus grande automatisation, efficacité et contrôle sur vos processus de gestion de serveur, garantissant des performances optimales et la fiabilité de votre infrastructure.

Documentation

La documentation complète de cette API peut être trouvée ici : Documentation de l'API

Aperçu

Aperçu et Nommage

L'objectif des fonctionnalités de TSplus Farm est de permettre à l'administrateur de gérer tous ses serveurs TSPlus à partir d'un seul serveur. Ce serveur peut être désigné comme le **Contrôleur de ferme** .

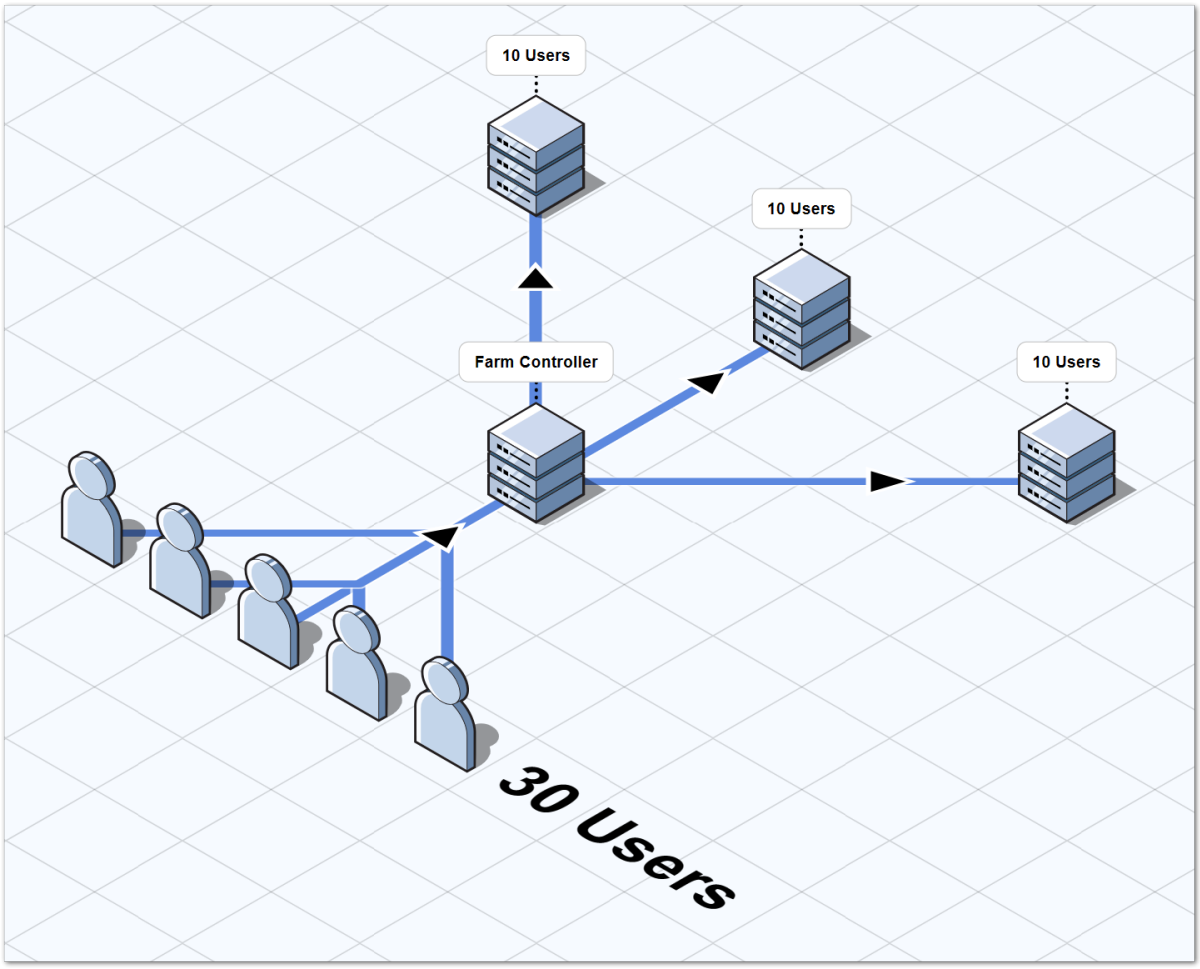
Les serveurs TSplus dans la ferme sont nommés le **Serveurs d'applications** , ou juste Serveurs.

Ce contrôleur de ferme, une fois sa ferme peuplée de serveurs d'applications, deviendra également un **Serveur de passerelle** une fois que vous avez activé l'une des fonctionnalités de la ferme telles que :

- Load balancing
- Proxy inverse
- Affecter des serveurs

Ce serveur de passerelle deviendra essentiellement le point d'entrée principal de tous vos utilisateurs lorsque "L'équilibrage de charge" ou "Affecter des serveurs" est activé.

Enfin, ce Contrôleur de Ferme vous permettra également de surveiller tous les serveurs d'applications et de transférer facilement les paramètres liés à TSplus, tels que les applications et les paramètres avancés, de votre Contrôleur de Ferme vers vos serveurs d'applications.



Architecture de la ferme de serveurs TSplus

Il existe 2 options pour déployer des fermes de serveurs TSplus :

Option 1 Tous vos serveurs ont des adresses IP publiques et peuvent être atteints depuis Internet.

OU

Option 2 Seul le portail Gateway peut être atteint depuis Internet. Le serveur Gateway fournit un « rôle de proxy inverse ».

Dans les deux options :

- Chaque serveur a la même configuration TSplus.
- Chaque serveur a les mêmes ports HTTP/HTTPS.
- Pour publier une nouvelle application, il suffit de l'ajouter à vos utilisateurs/groupes d'utilisateurs dans l'AdminTool.

Bien sûr, assurez-vous que cette application est installée sur les serveurs d'application ciblés.

Tous les types d'accès Web sont disponibles sans configuration spécifique : RemoteApp et clients HTML5.

Option 1 - Tous les serveurs ont leur propre adresse IP publique et peuvent être atteints depuis Internet.

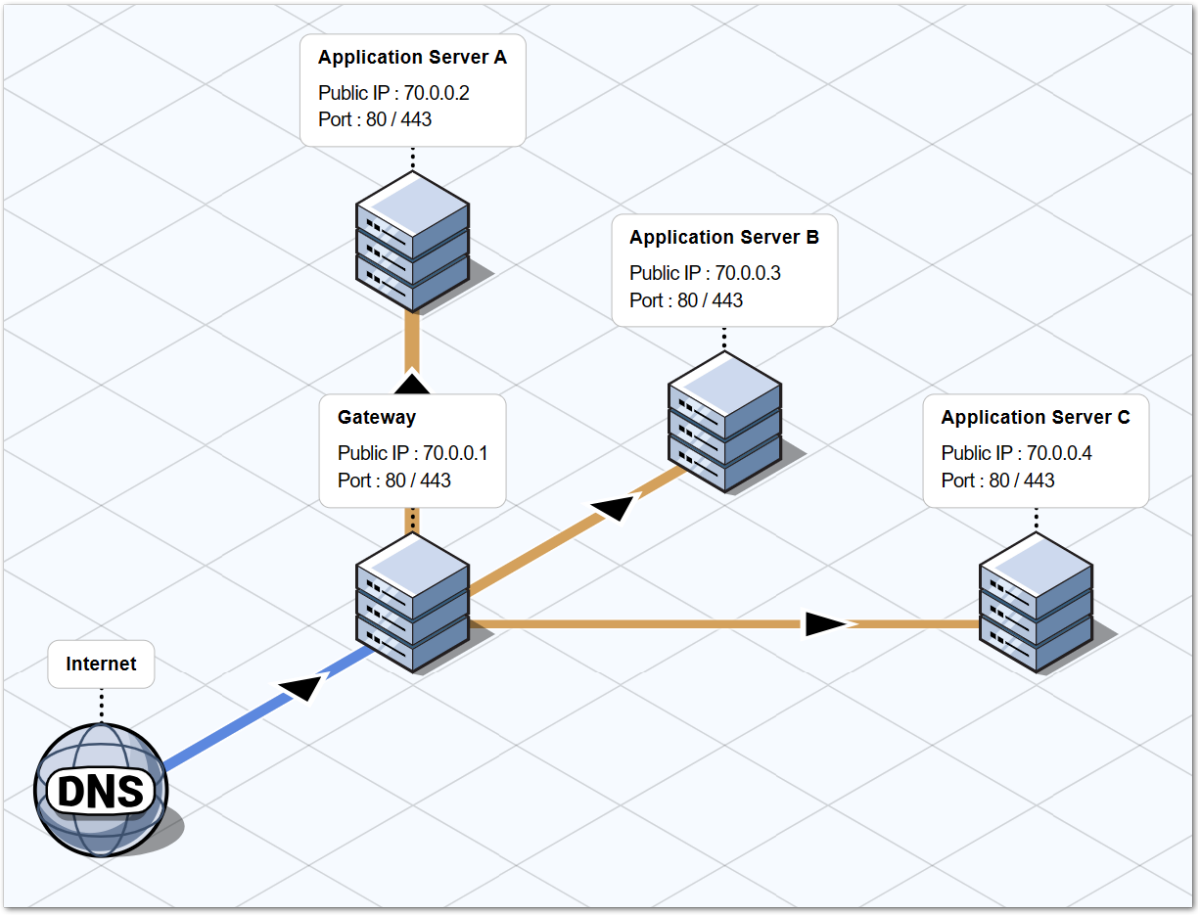
Ceci est l'architecture recommandée pour utiliser TSplus Gateway.

Cette architecture suit les meilleures pratiques et permet à l'administrateur informatique d'industrialiser son environnement :

- Chaque serveur a la même configuration de Terminal Service Plus.
- Chaque serveur a les mêmes ports HTTP/HTTPS
- Déployer un nouveau serveur d'application ne prend que quelques minutes (il suffit d'ajouter le serveur à la ferme dans l'AdminTool sur le serveur Gateway).

Avec cette architecture, tous les types d'accès sont disponibles sans configuration spécifique : Remoteapp et clients HTML5.

Cette architecture est décrite dans le diagramme ci-dessous :



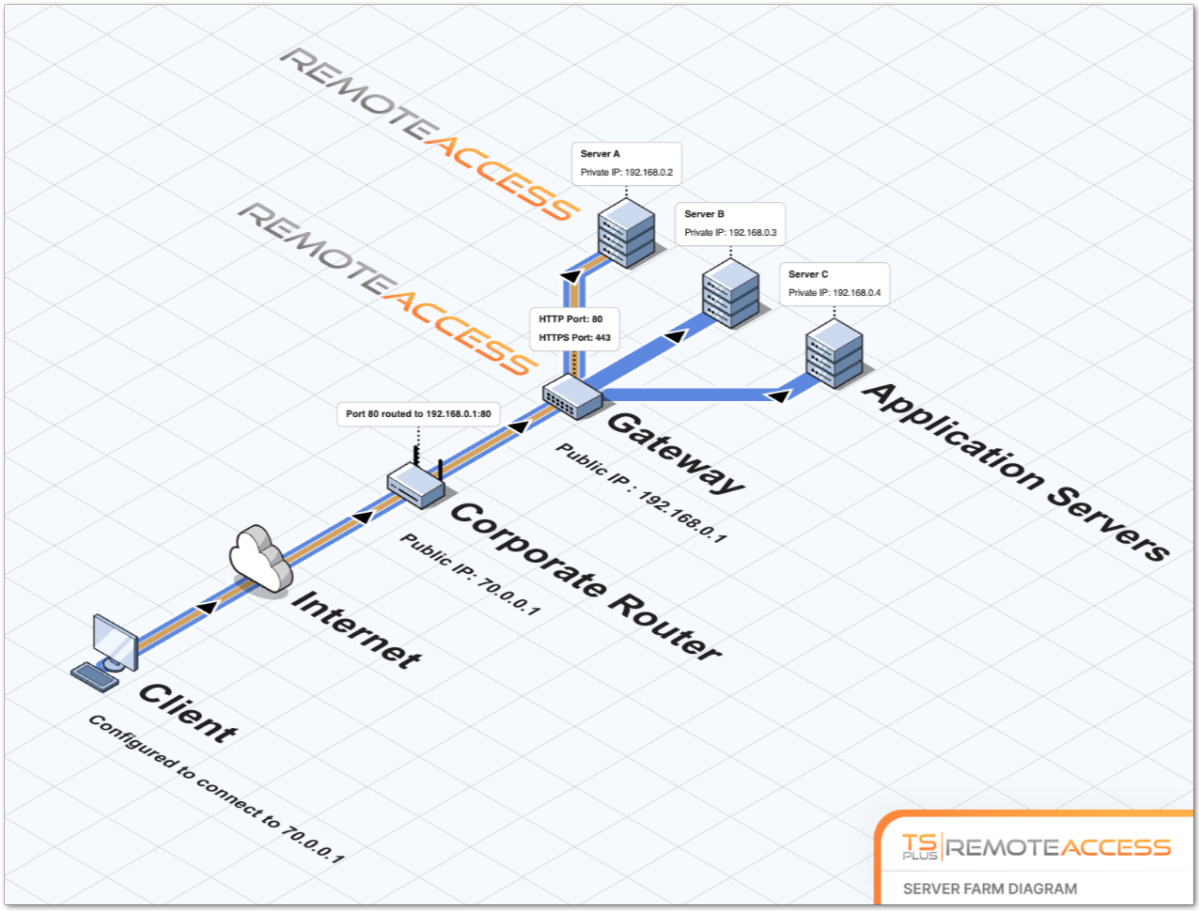
-
-
  -

Option 2 : Seul le portail Gateway peut être atteint depuis Internet et inclut un « rôle de proxy inverse ».

Le portail Terminal Service Plus peut également être configuré avec seulement 1 adresse IP publique.

La passerelle redirige toute demande de connexion externe vers tout serveur disponible. Si vous n'utilisez pas la fonction d'équilibrage de charge, les utilisateurs se connecteront à leur(s) serveur(s) assigné(s).

Cette architecture est décrite dans le diagramme ci-dessous :



Pour plus d'informations sur le rôle de proxy inverse, consultez le Documentation de la fonctionnalité Reverse Proxy .

Historique des versions

- API 1.5 (publié avec TSplus 15.50)
  - Configuration intégrée de reverse-proxy, d'équilibrage de charge et d'attribution de serveur d'application
  - Ajout de la synchronisation entre les applications/réglages du contrôleur de ferme et chaque serveur d'application.

- API 1.4 (publié avec TSplus 10.10)
  - Surveillance centralisée de l'équilibrage de charge
  - Activer/Désactiver un serveur dans le gestionnaire de répartition de charge TSplus
  - Traductions en plusieurs langues (la langue TSplus sera utilisée)
  - Plusieurs paramètres ajoutés + bugs d'affichage corrigés

- API 1.3 (publié avec TSplus 9.70)
  - Paramètres de surveillance et de gestion centralisés (Paramètres globaux / Panneau flottant / Client RemoteApp / Client HTML5)

- API 1.2 (publié avec TSplus 9.60)
  - Gestionnaire de ferme
  - Gestion centralisée des serveurs (ajouter/retirer)
  - Surveillance et gestion centralisées des sessions (messages/déconnexion/déconnexion)

- API 1.1 (publié avec TSplus 9.30)
  - Internes de répartition de charge
  - Équilibrage de charge avec sessions persistantes

Prérequis

Exigences matérielles

Le contrôleur de ferme et les serveurs d'applications ont le standard Exigences de Terminal Service Plus pour le matériel.

Exigences du système d'exploitation

Le contrôleur de ferme et les serveurs d'applications doivent utiliser l'un des systèmes d'exploitation suivants :

- 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 réseau

Chaque serveur d'application doit être accessible depuis le contrôleur de ferme.

Plus précisément, le Farm Controller émettra des demandes à chaque Application Server sur son port API (19955 par défaut) et ce port doit être ouvert sur tout pare-feu se trouvant entre le Farm Controller et les Application Servers.

La latence du réseau doit être faible entre le contrôleur de ferme et les serveurs d'application. Une latence inférieure à 200 ms est recommandée, une latence inférieure à 2 000 ms est requise.

Exigences logicielles

.NET 2.0 ou une version supérieure est requise - cela ne devrait pas poser de problème car une version .NET compatible est activée par défaut sur chaque système d'exploitation pris en charge pour Terminal Service Plus Farm.

Licence et exigences de version de Terminal Service Plus

Terminal Service Plus doit être dans l'édition « Enterprise » sur le contrôleur de ferme et sur tous les serveurs d'application.

Tous les serveurs doivent également exécuter la même version de Terminal Service Plus.

Exigences de configuration

Le contrôleur de ferme et les serveurs d'application doivent avoir la même date/heure configurée. Il est fortement recommandé de synchroniser l'horloge Windows de tous les serveurs avec un serveur de temps Internet si cela n'a pas déjà été fait.

Exigences des utilisateurs

Un Active Directory est **non** nécessaire, cependant si vous avez un Active Directory, alors vos Administrateurs de Domaine doivent également être Administrateurs Locaux du Contrôleur de Ferme pour pouvoir utiliser Terminal Service Plus Farm Manager.

Proxy inverse

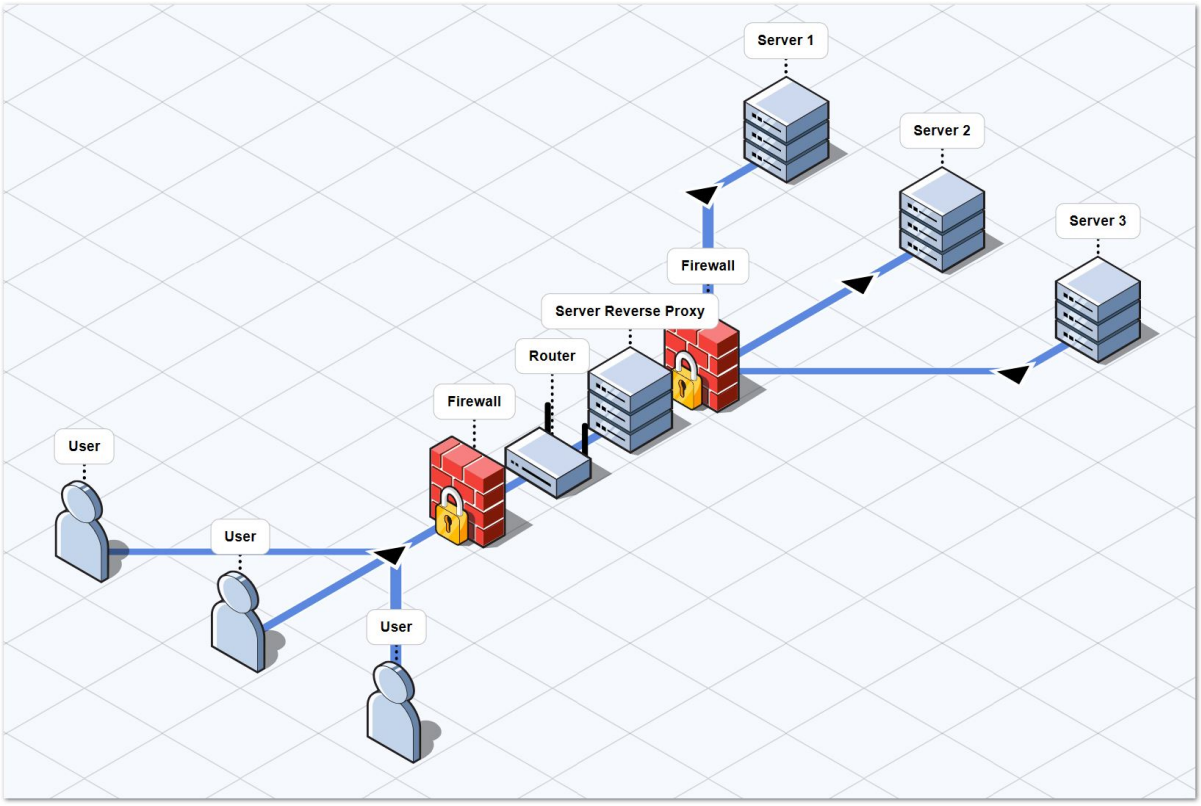
Aperçu

Cette fonctionnalité est disponible dans l'Enterprise Edition de TSplus.

Le système de Reverse Proxy agit comme un intermédiaire pour que ses serveurs associés puissent être contactés par n'importe quel client.

L'avantage d'utiliser un reverse-proxy est simple : vous n'aurez plus besoin de créer autant de règles de redirection de port que le nombre de vos serveurs TSplus.

Que vous utilisiez ou non la fonction de répartition de charge, vous devez l'activer pour vous connecter en utilisant le proxy inverse. Dans TSplus, cela fournit un point d'accès unique à un ensemble de serveurs TSplus équilibrés en charge.

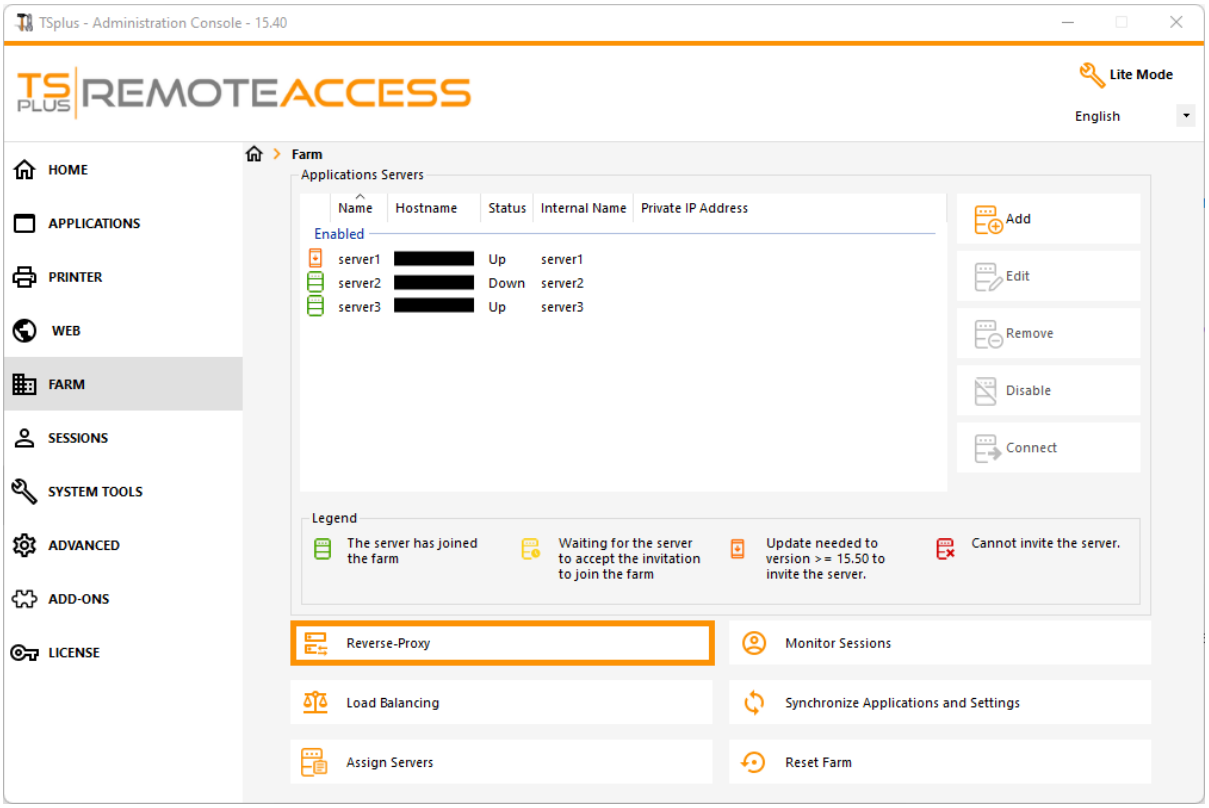


Ce point d'accès unique sera votre serveur de passerelle TSplus Web Portal.

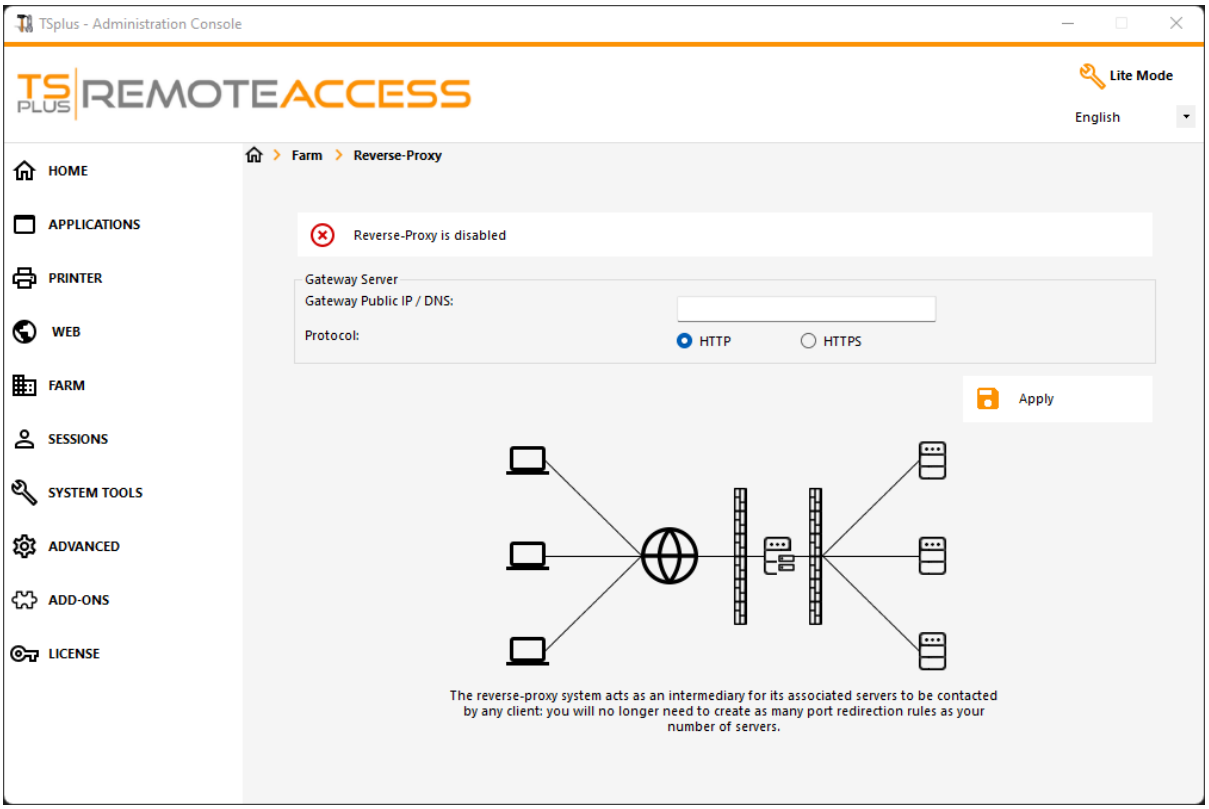
Puisque ce serveur va être accessible à distance, vous devrez configurer une règle de redirection de port sur votre routeur, y compris les ports http ou https selon votre préférence (80 étant le port par défaut pour http et 443 pour https).

Configuration

Vous pouvez accéder à l'interface de configuration du Reverse Proxy via l'onglet FARM :



Cliquez sur le bouton Reverse-Proxy.



- Cliquez sur le bouton « Reverse-Proxy est désactivé » pour l'activer.
- L'adresse IP publique de la passerelle doit être définie avec une adresse IP fixe valide ou un nom de domaine.
- Sélectionnez HTTP ou HTTPS pour votre méthode de connexion préférée, les serveurs de votre ferme doivent être capables de communiquer entre eux sur le port 80 ou 443, selon la méthode de connexion que vous utilisez. Il est également important que votre pare-feu Windows ne bloque pas ces ports.

Une fois que vous avez terminé votre configuration, cliquez sur « Appliquer » pour enregistrer ces paramètres de Reverse Proxy.

Accès aux serveurs d'applications via le serveur Gateway

Une fois activée et opérationnelle, la fonctionnalité Reverse Proxy vous permet d'accéder au serveur d'application en utilisant une URL spéciale formatée comme suit :
(1) :// **2** : **3** /~~ **4**
avec :

- (1): le protocole Reverse Proxy configuré
- l'adresse IP publique ou le nom de domaine du serveur Gateway
- le port web du serveur Gateway associé au protocole de proxy inverse configuré
- le nom interne du serveur d'application utilisé par le Reverse Proxy

Par exemple, en supposant que :

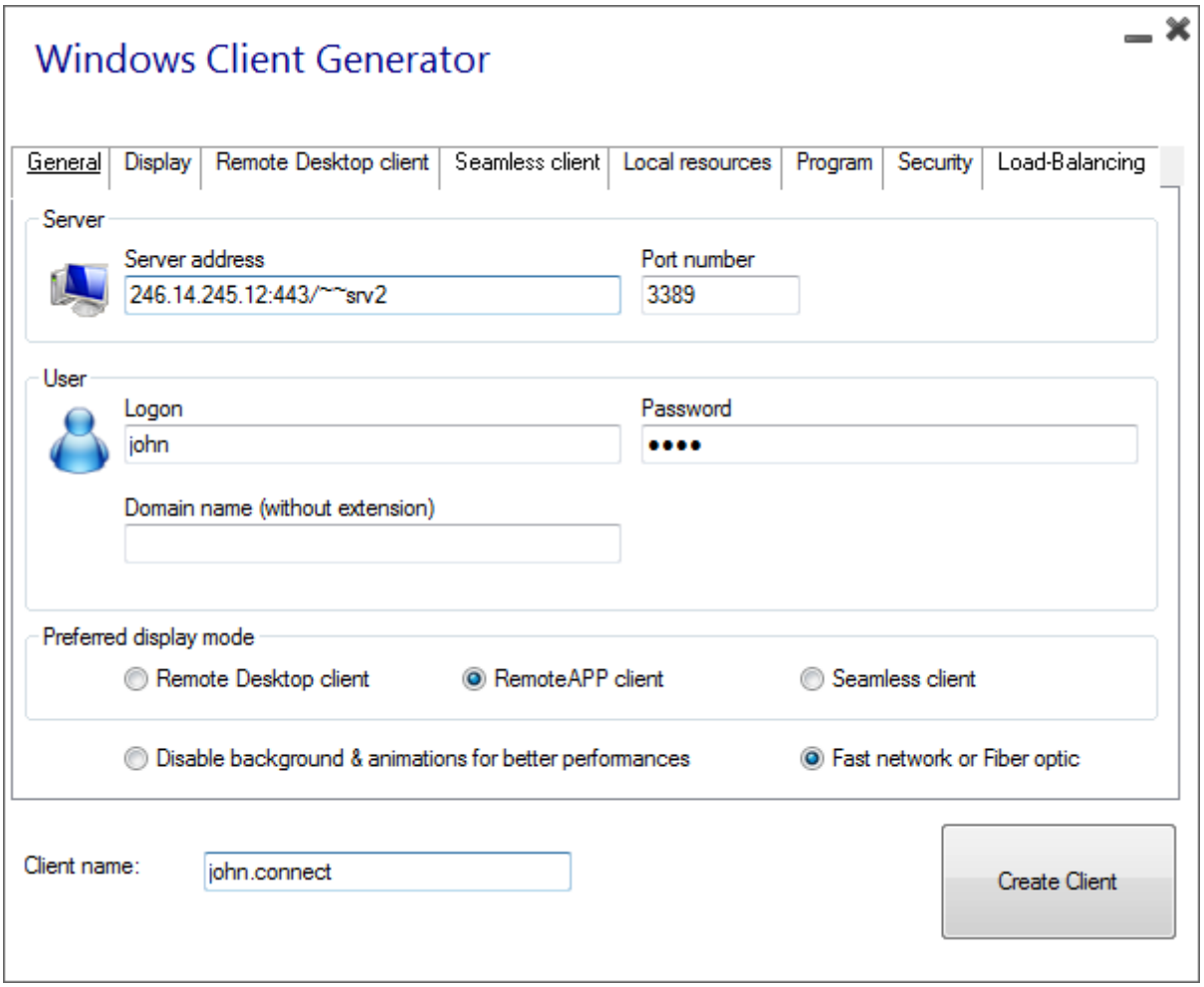
- le protocole de proxy inverse configuré est HTTPS
- votre serveur Gateway a l'IP publique 1.1.1.1
- votre serveur Gateway utilise le port HTTPS 443
- le serveur d'application ciblé auquel vous souhaitez vous connecter utilise le nom interne « srv2 »

L'URL spécial à utiliser pour atteindre le serveur d'application ciblé sera 1.1.1.1:443/~~srv2

En conséquence, vous pouvez accéder au portail web de ce serveur d'application en utilisant cette URL spéciale.

Vous pouvez également générer un Client de Connexion qui se connectera à ce serveur d'application spécifique via le serveur de passerelle en utilisant cette même méthode. Il suffit d'utiliser l'URL spéciale dans le champ d'adresse du serveur du Générateur de Client de Connexion.

Par exemple :


Windows Client Generator
General
Display
Remote Desktop client
Seamless client
Local resources
Program
Security
Load-Balancing
Server
Server address
246.14.245.12:443/~~srv2
Port number
3389
User
Logon
john
Password
Domain name (without extension)
Preferred display mode
Remote Desktop client
RemoteAPP client
Seamless client
Disable background & animations for better performances
Fast network or Fiber optic
Client name:
john.connect
Create Client

Affectation de serveur

Aperçu

Le contrôleur de ferme peut agir en tant que serveur de passerelle, redirigeant les utilisateurs lors de la connexion vers des serveurs d'application spécifiques de votre ferme. Vous pourrez attribuer un ou plusieurs serveurs à un utilisateur / un groupe local / un groupe Active Directory.

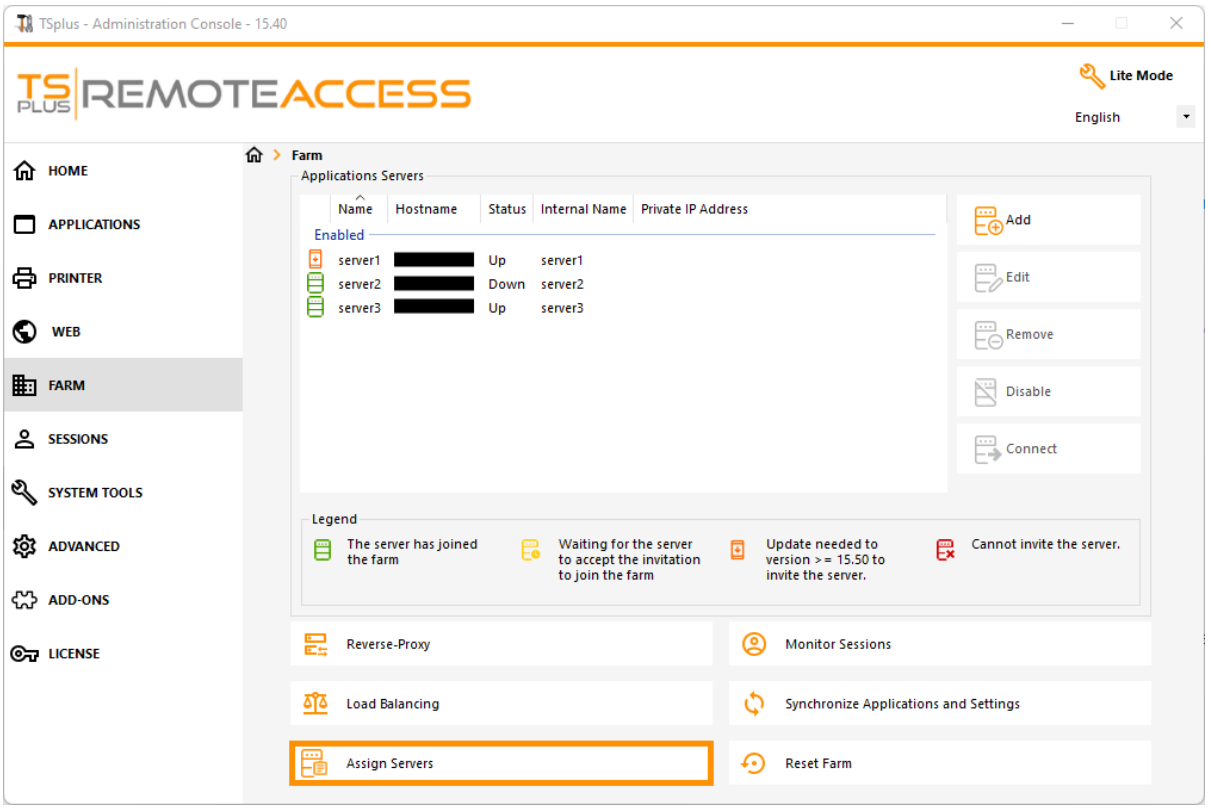
Important : L'attribution des serveurs ne fonctionne que depuis le TSplus Web Portal, et non avec les clients de connexion.

Si l'utilisateur a plus d'un serveur assigné, il pourra choisir quel serveur il souhaite accéder dans la liste des serveurs qui lui sont assignés.

Si la ferme est dans un domaine, le portail utilisera ses identifiants AD et l'utilisateur se connectera avec l'authentification unique (SSO).

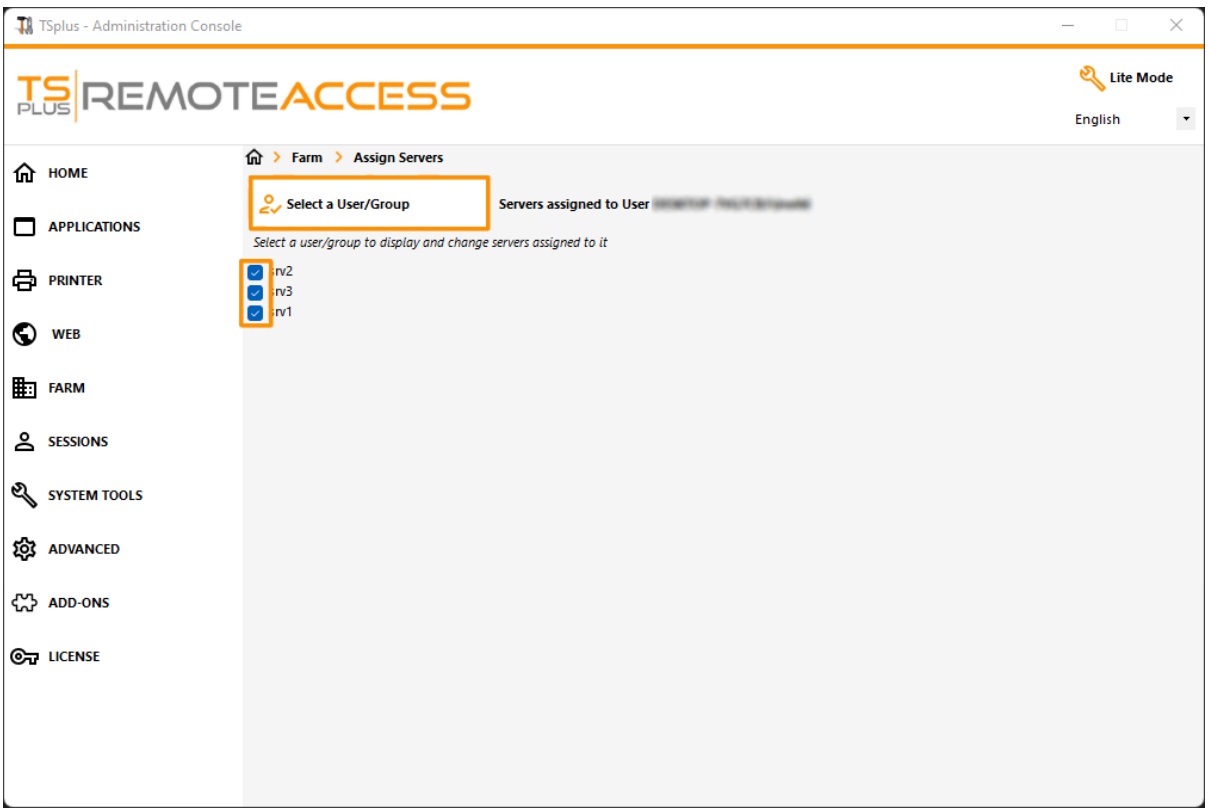
Sinon, il doit avoir les mêmes identifiants locaux sur chaque serveur.

Pour attribuer des serveurs, veuillez cliquer sur le bouton « Attribuer des serveurs » :



Pour attribuer un serveur à un utilisateur, il suffit de le sélectionner avec le bouton « Sélectionner un utilisateur/groupe » puis de cocher la case du serveur dans la liste « Serveurs ».

Pour supprimer un serveur attribué à un utilisateur, il suffit de décocher la case du serveur dans la liste "Serveurs".

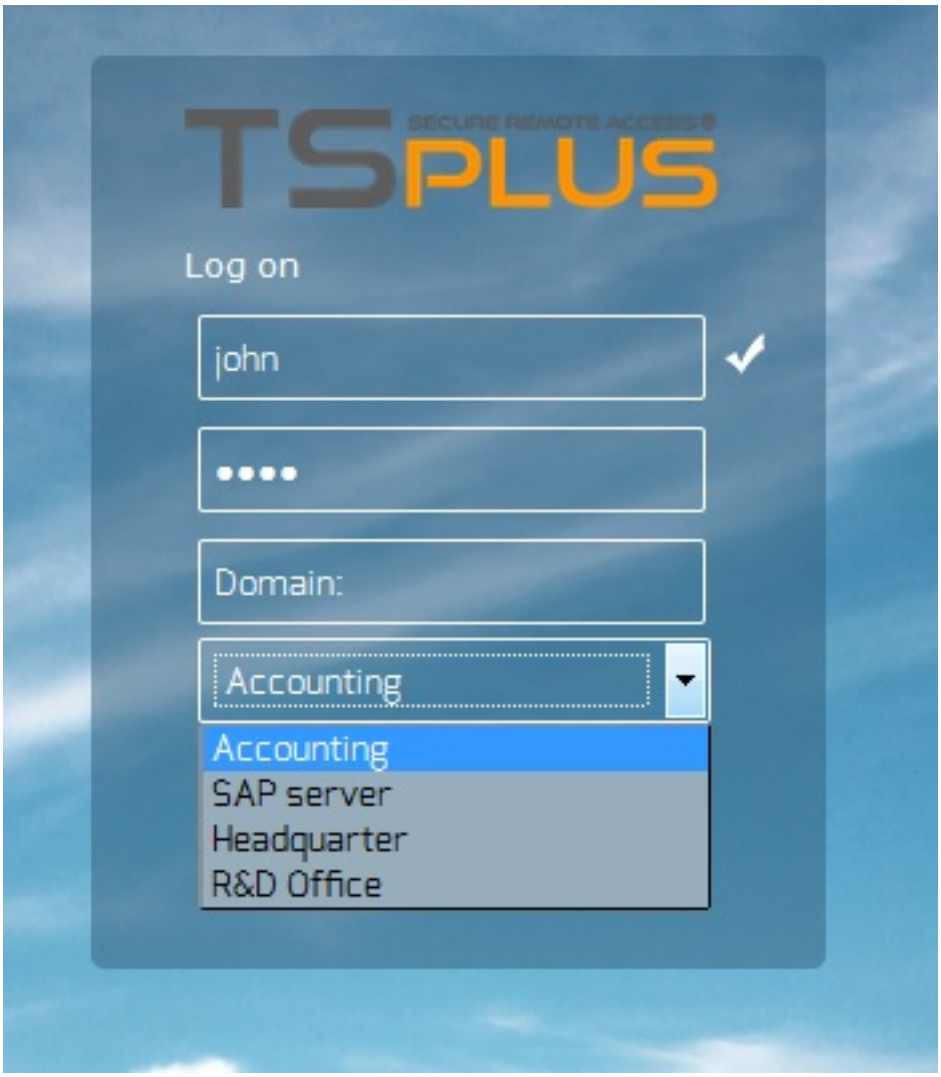


Notes importantes

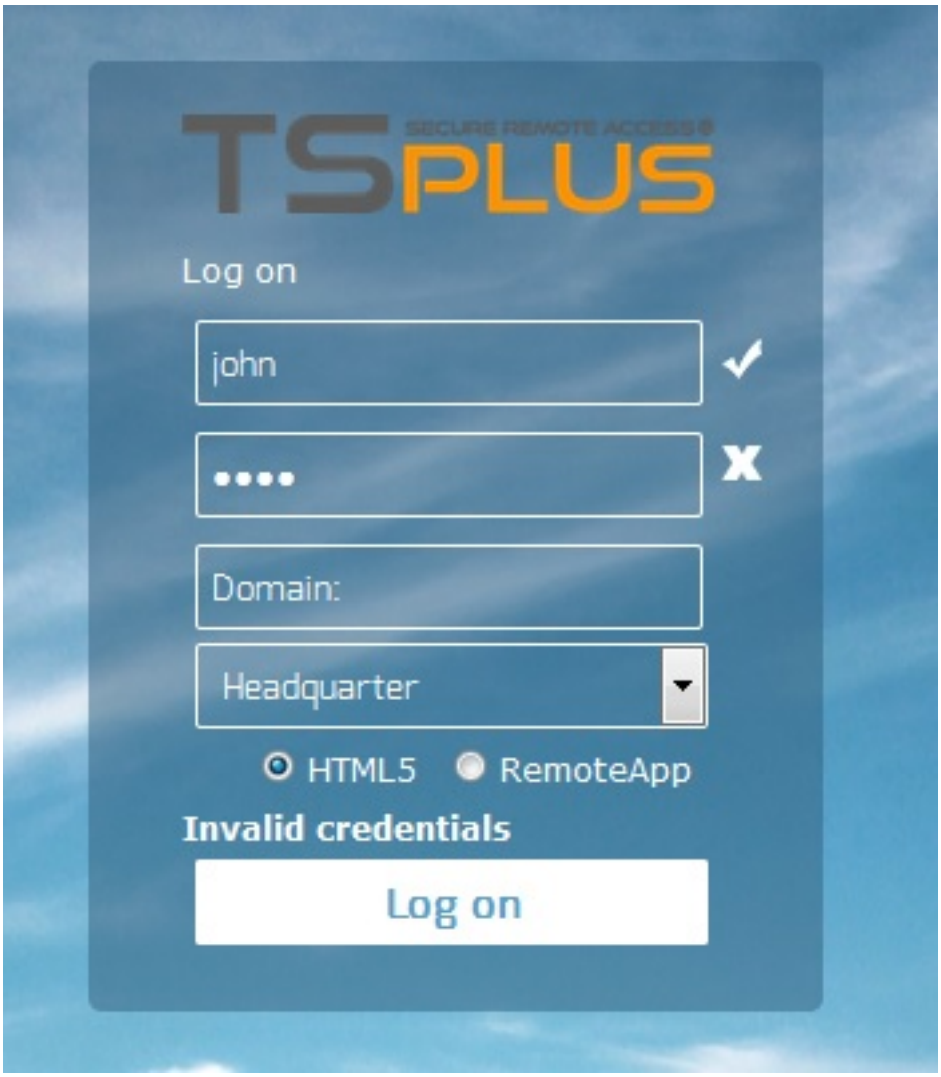
- L'exemple ci-dessus concerne un domaine ou un groupe de travail.
- Si vous utilisez un groupe de travail, les identifiants des utilisateurs doivent être les mêmes sur chaque serveur d'application que vous assignez.
- Cette fonctionnalité d'assignation de serveur peut être configurée et utilisée simultanément avec la fonctionnalité de répartition de charge, permettant au contrôleur de ferme de répartir la charge sur les serveurs assignés. Pour ce faire, activez la répartition de charge et cochez l'option « Répartir la charge sur les serveurs assignés ».
- Si la fonction d'assignation de serveur et l'équilibrage de charge sont tous deux activés, à moins que l'option « Équilibrer la charge sur les serveurs assignés » dans la configuration de l'équilibrage de charge ne soit activée, le serveur de passerelle redirigera les utilisateurs vers le serveur le moins chargé, indépendamment de leurs serveurs assignés.

Exemple de ce que vous obtiendrez lorsque les utilisateurs se connecteront au portail Gateway

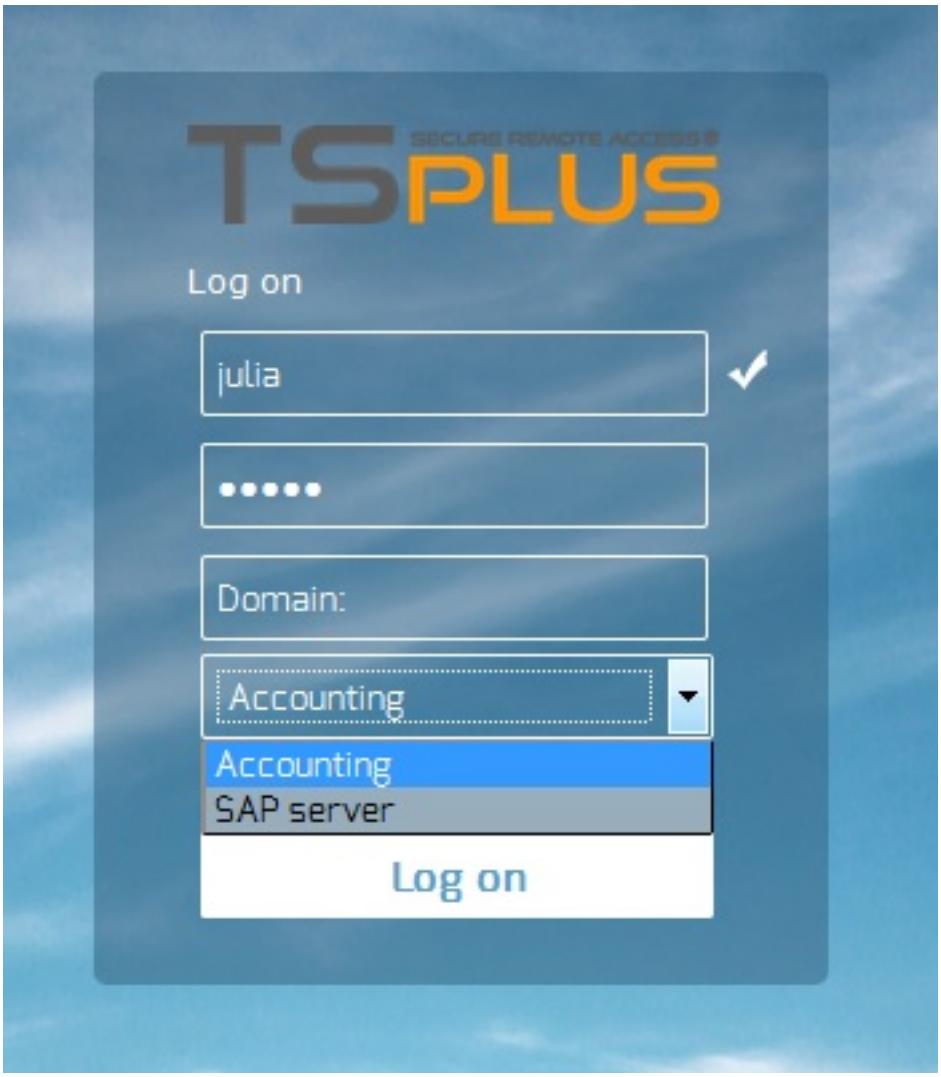
John peut sélectionner le serveur. Il le souhaite et il obtiendra une connexion automatique à ce serveur :



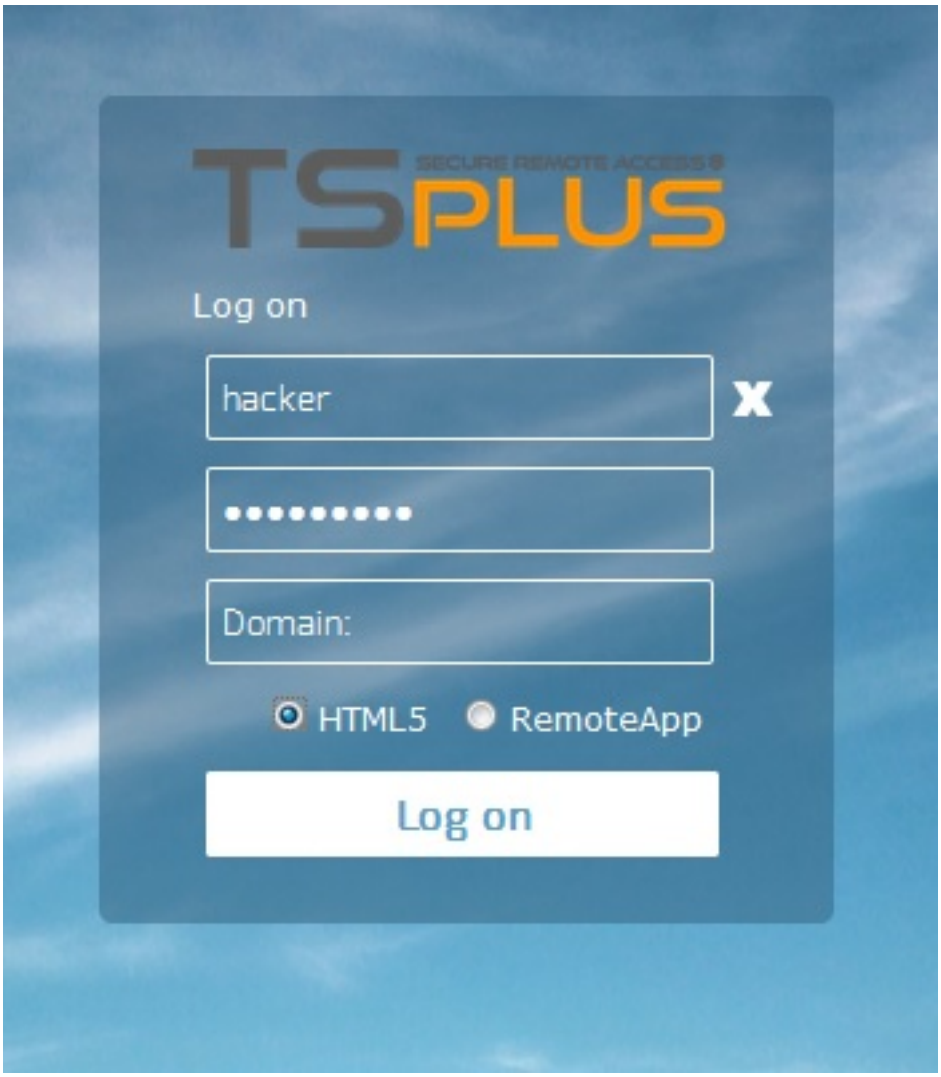
S'il tape un mot de passe incorrect, John devra retaper son mot de passe :



Julia a une liste différente de serveurs possibles :



Quelqu'un essaie de pirater le Gateway. Il ne voit aucun serveur et le Gateway bloque son accès web.

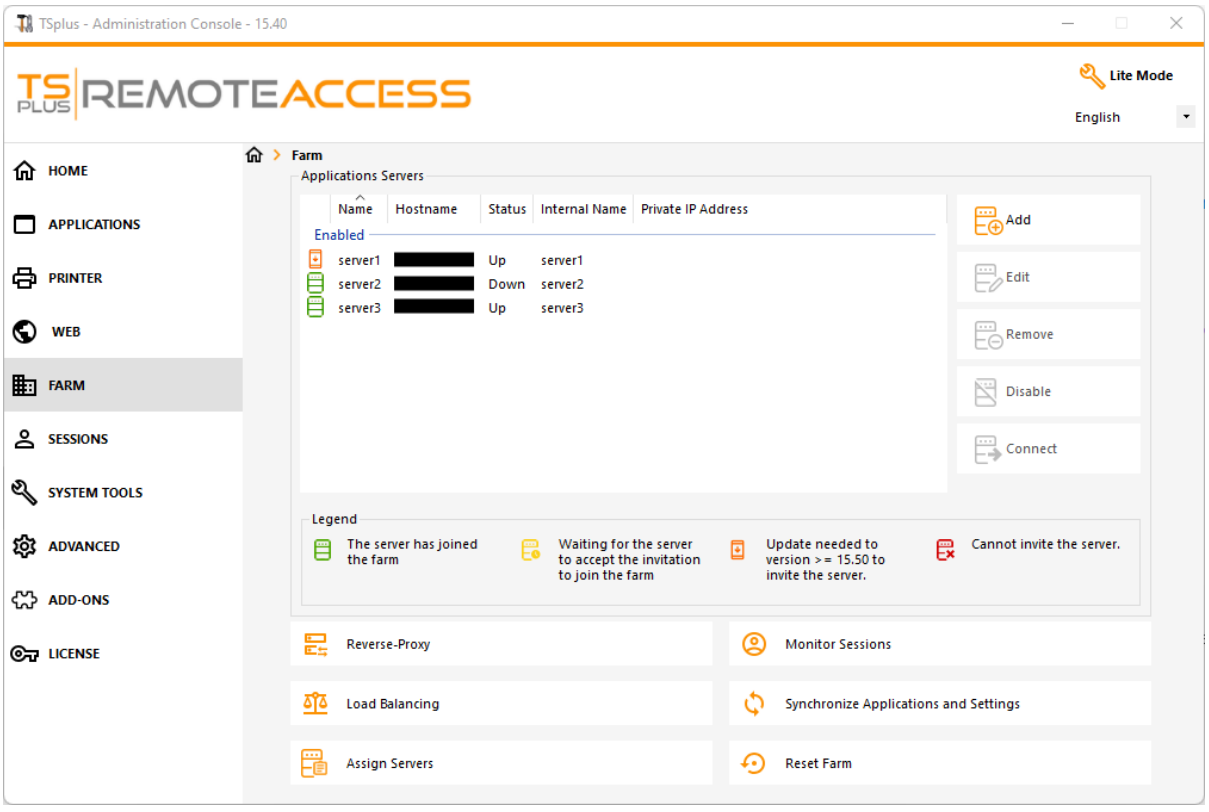

TSPLUS
SECURE REMOTE ACCESS
Log on
hacker
Domain:
HTML5
RemoteApp
Log on

Configuration de la ferme

Aperçu

Pour créer une ferme, vous devez simplement ajouter des serveurs d'application depuis le TSplus AdminTool.

Vous pourrez gérer les serveurs d'applications dans la section « Ferme » de l'AdminTool.



Depuis cette fenêtre, vous pourrez effectuer plusieurs actions :

- “ Ajouter : ajouter un nouveau serveur d'application
- “ Modifier : modifier le serveur sélectionné.
- “ Supprimer : supprimer définitivement le serveur sélectionné de la ferme (vous pouvez toujours l'ajouter à nouveau plus tard avec le bouton « Ajouter »).
- “ Désactiver/Activer : désactiver ou activer temporairement le serveur sélectionné (les

utilisateurs ne pourront pas se connecter à ce serveur).
- “ Connect : ouvrez le client RDP par défaut et connectez-vous automatiquement au serveur sélectionné. Si vos identifiants sont enregistrés dans MSTSC, ils seront utilisés, sinon vous devrez entrer vos identifiants.

Vous pouvez également accéder à ces actions depuis le menu contextuel affiché par un clic droit sur un serveur.

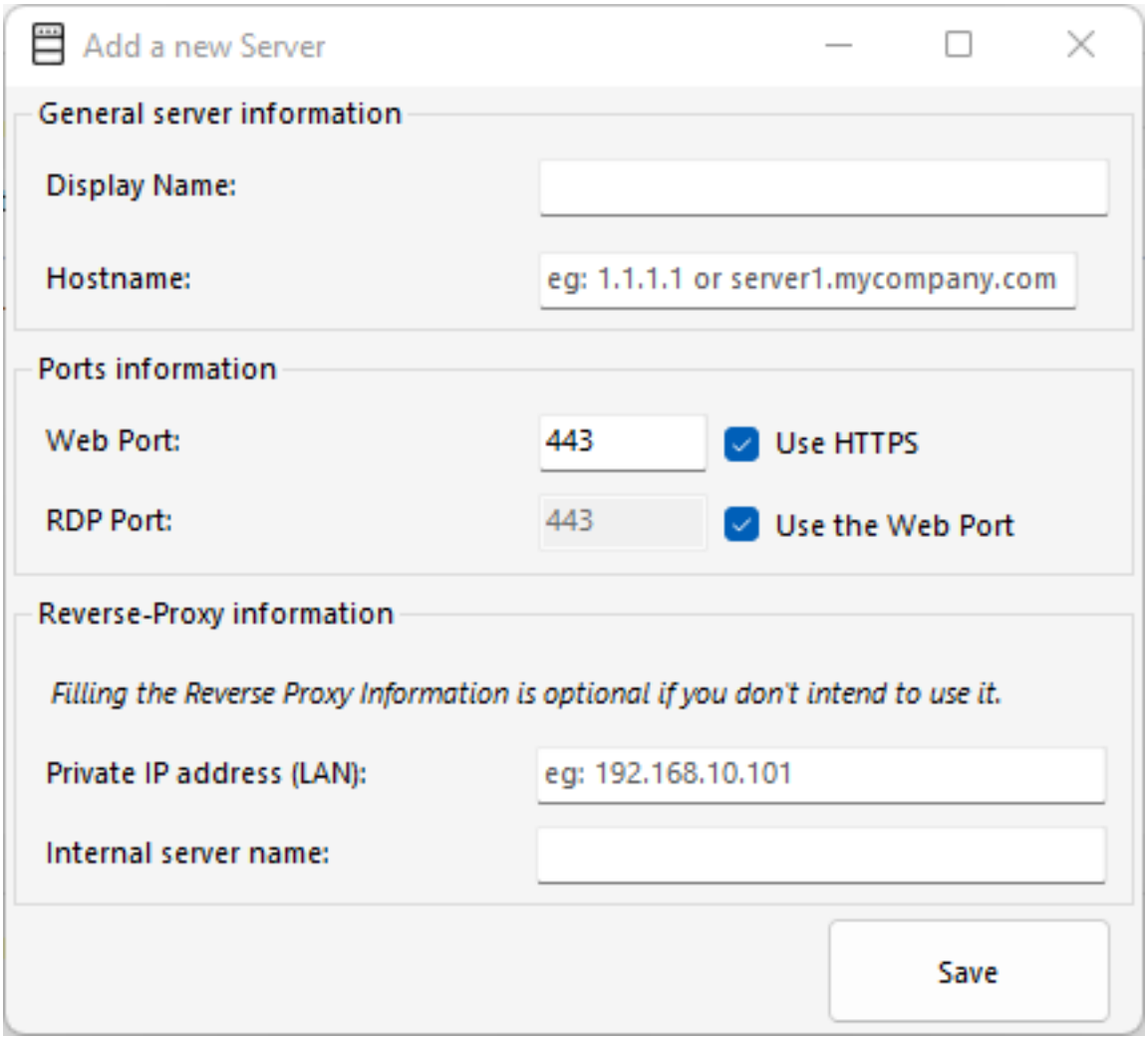
Sur le panneau inférieur, vous trouverez un accès rapide aux principales fonctionnalités de la ferme disponibles une fois que les serveurs d'application ont été ajoutés :

- “Équilibrage de charge”: vous permet de rediriger les utilisateurs se connectant depuis le serveur de passerelle vers le serveur le moins chargé de la ferme
- “Reverse Proxy” : vous permet d'exposer uniquement le serveur de passerelle et rend les serveurs d'application accessibles en utilisant des URL telles que https://gateway-server-domain-or-ip-address/~~nom-interne-du-serveur-dapplication
- “Assign Servers” : permet de restreindre les serveurs d'application disponibles pour les utilisateurs et les groupes lors de la connexion depuis le serveur passerelle, leur permettant de choisir le serveur auquel ils souhaitent se connecter si plusieurs serveurs sont assignés.
- Surveiller les sessions * permet de surveiller la session en cours et d'effectuer rapidement des actions telles que déconnexion, fermeture de session, envoi de message, affichage de la session ou contrôle de la session.
- Synchroniser les applications et les paramètres * permet de pousser tous les paramètres avancés et les applications publiées vers les serveurs d'applications sélectionnés
- “Réinitialiser la ferme” : vous permet de réinitialiser la ferme, ce qui supprimera tous les serveurs et réinitialisera toutes les configurations des fonctionnalités de la ferme, par exemple les configurations de “Proxy inverse”, de “Répartition de charge” et de “Attribution des serveurs”.

* Ces fonctionnalités ne sont accessibles que pour les serveurs d'applications qui ont complètement rejoint la ferme pour des raisons de sécurité, ce qui signifie que vous devrez d'abord accepter l'invitation envoyée par votre contrôleur de ferme, du côté du serveur d'applications.

Ajouter un serveur d'applications à la ferme

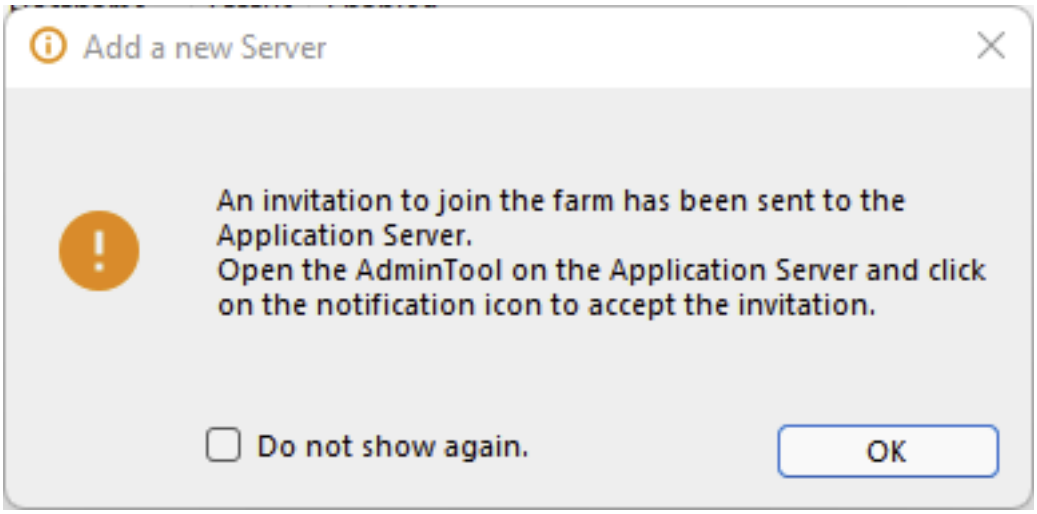
Pour ajouter un serveur d'application, cliquez sur le bouton « Ajouter ». La fenêtre suivante s'affichera :



Vous devrez spécifier son nom d'affichage et son nom d'hôte (vous pouvez saisir une adresse IP ou un nom de domaine, sans numéro de port).
Remplir les champs d'information du Proxy Inverse est facultatif uniquement si vous n'utilisez pas actuellement la fonctionnalité Proxy Inverse.
Le nom interne sera automatiquement rempli avec un nom d'affichage disponible s'il est vide pour faciliter la configuration générale du serveur.

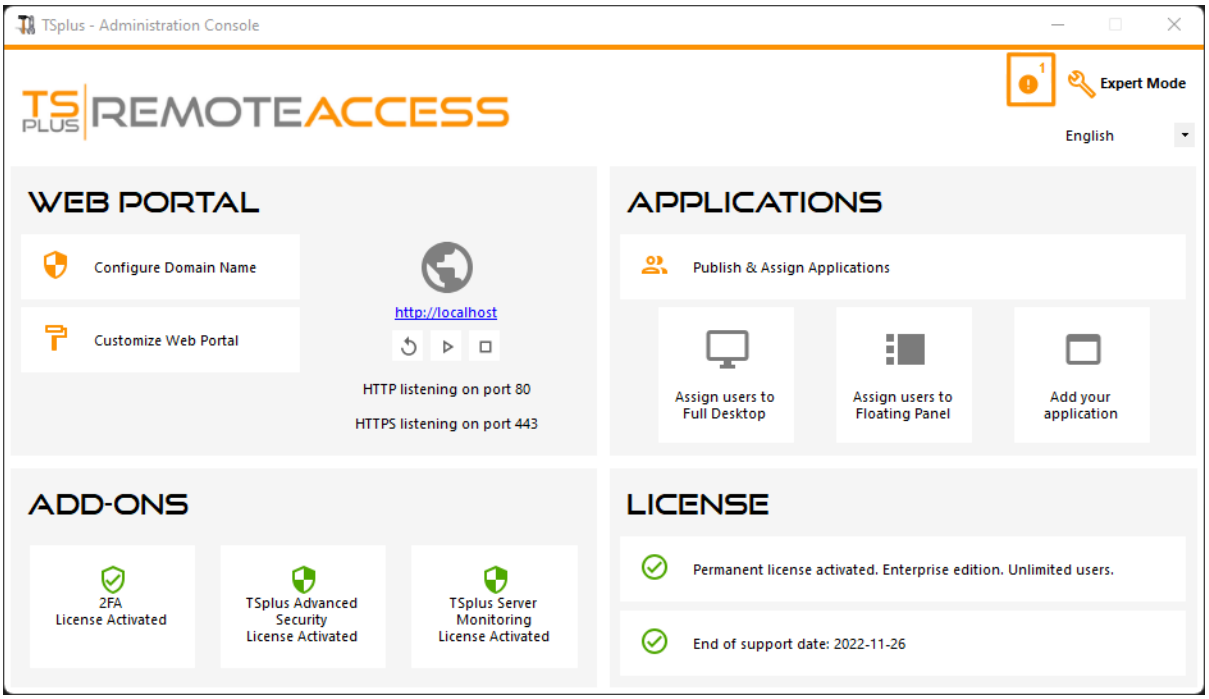
IMPORTANT : l'option de port RDP « Utiliser le port web » spécifie que vous souhaitez tirer parti de la fonctionnalité de transfert de port RDP (activée par défaut) offerte par le serveur web de l'application.
En conséquence, si vous souhaitez utiliser l'option « Utiliser le port web », veuillez vous assurer que sur le serveur d'application ajouté, l'option « Désactiver le transfert RDP » dans AdminTool > Avancé > Sécurité est réglée sur « Non ».

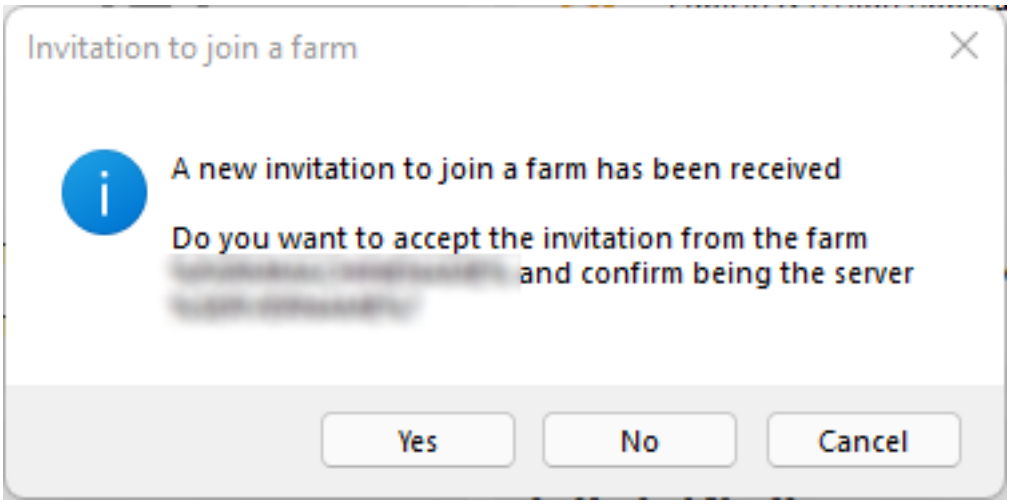
Entrez les détails du serveur d'application, puis cliquez sur le bouton « Enregistrer ». Une invitation à rejoindre la ferme sera envoyée au serveur d'application ajouté.



Accepter cette invitation du côté du serveur d'application est nécessaire si vous souhaitez pouvoir utiliser les “Sessions de surveillance” et “Synchroniser les applications et les paramètres” pour des raisons de sécurité.
Il n'est cependant pas nécessaire si vous avez seulement besoin d'utiliser les fonctionnalités « Reverse Proxy », « Loadbalancing » et « Assign Servers ».

Pour accepter l'invitation, ouvrez une session Administrateur. **sur le serveur d'application** vous avez ajouté à la Ferme. Cliquez sur le bouton d'alerte en haut à droite de l'outil d'administration TSplus, puis cliquez sur « Oui » :





Sur le côté du contrôleur de ferme, vous pouvez voir la liste des serveurs d'application dans la ferme. Ils peuvent avoir trois états représentés par des icônes colorées :

- 

  Rejoint Le serveur d'application a pleinement rejoint la ferme en acceptant l'invitation.

-

  En attente Le serveur d'application a partiellement rejoint la ferme, en attendant que le serveur d'application accepte l'invitation.

- 

  Mise à jour nécessaire Le serveur d'application a partiellement rejoint la ferme, mais l'invitation ne peut pas être envoyée car le serveur utilise une version de TSplus Remote Access < 15.50.

- 

  Inaccessible Le serveur d'application a partiellement rejoint la ferme, mais l'invitation ne peut pas être envoyée car le serveur est inaccessible.

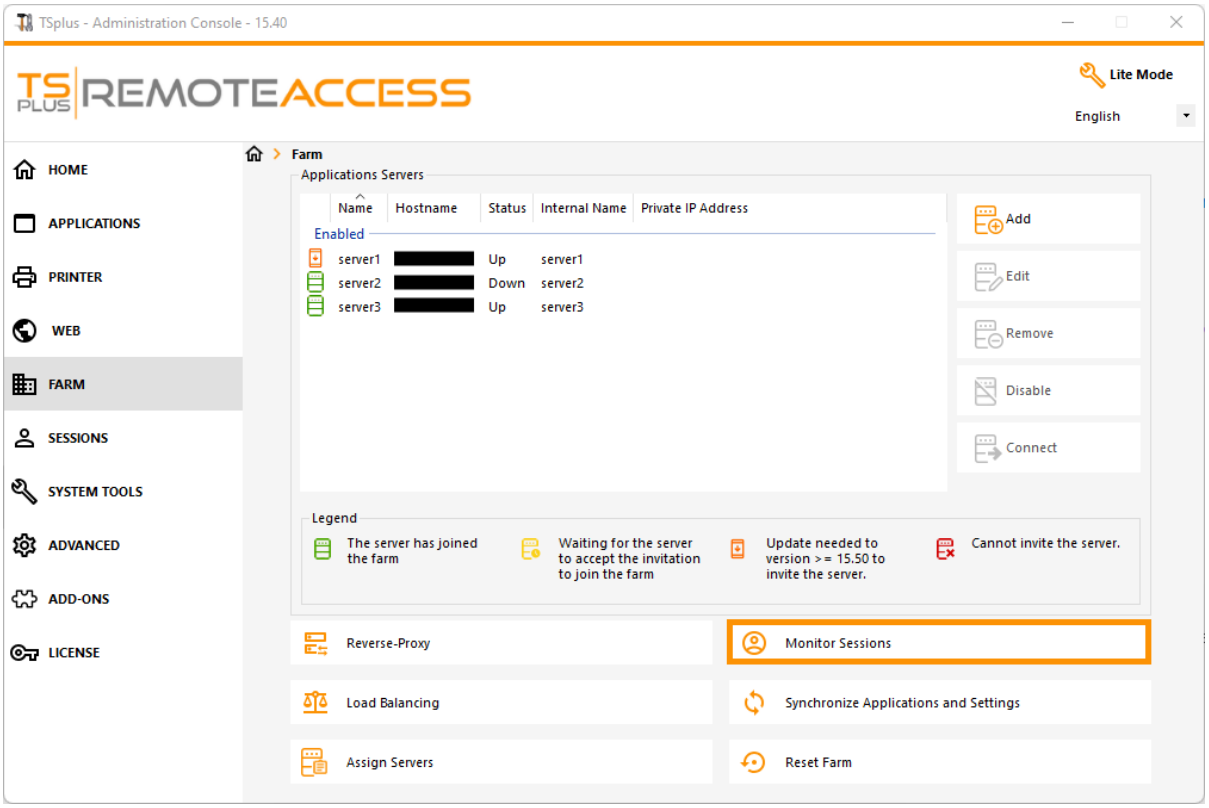
Applications Servers

	Name	Hostname	Status	Internal Name	Private IP Address
Enabled					
	srv1	Up			
	srv2	Up			
	srv3	Down			

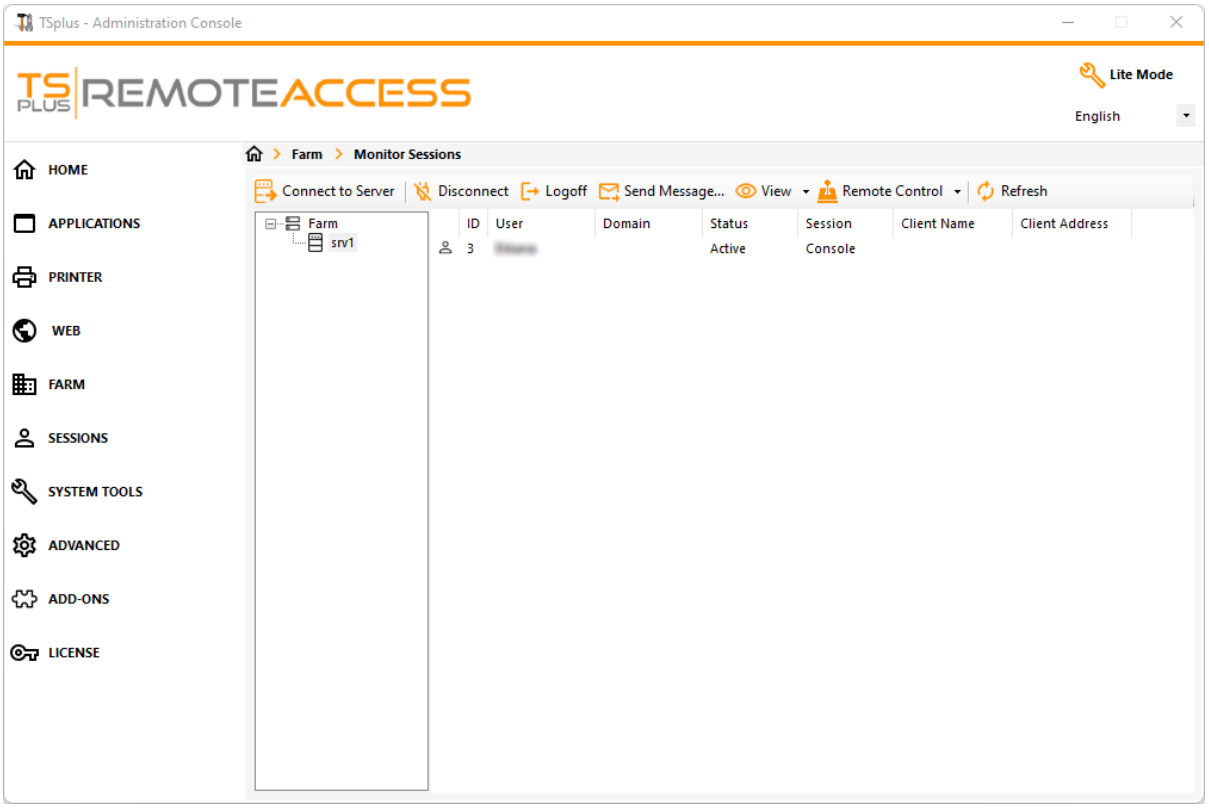
Surveiller les sessions

Aperçu

Vous pouvez accéder à l'interface de session de surveillance via l'onglet FARM :



Cliquez sur le bouton « Monitor Sessions » pour afficher l'onglet suivant :



Dans cet onglet, vous pouvez voir la liste des sessions utilisateur sur n'importe quel serveur d'application de la ferme.
Cliquez sur un serveur d'application dans le panneau de gauche pour le sélectionner et afficher ses sessions utilisateur actives actuelles. Une fois affichées, vous pouvez sélectionner une ou plusieurs sessions et effectuer plusieurs actions en cliquant sur l'un des boutons suivants :

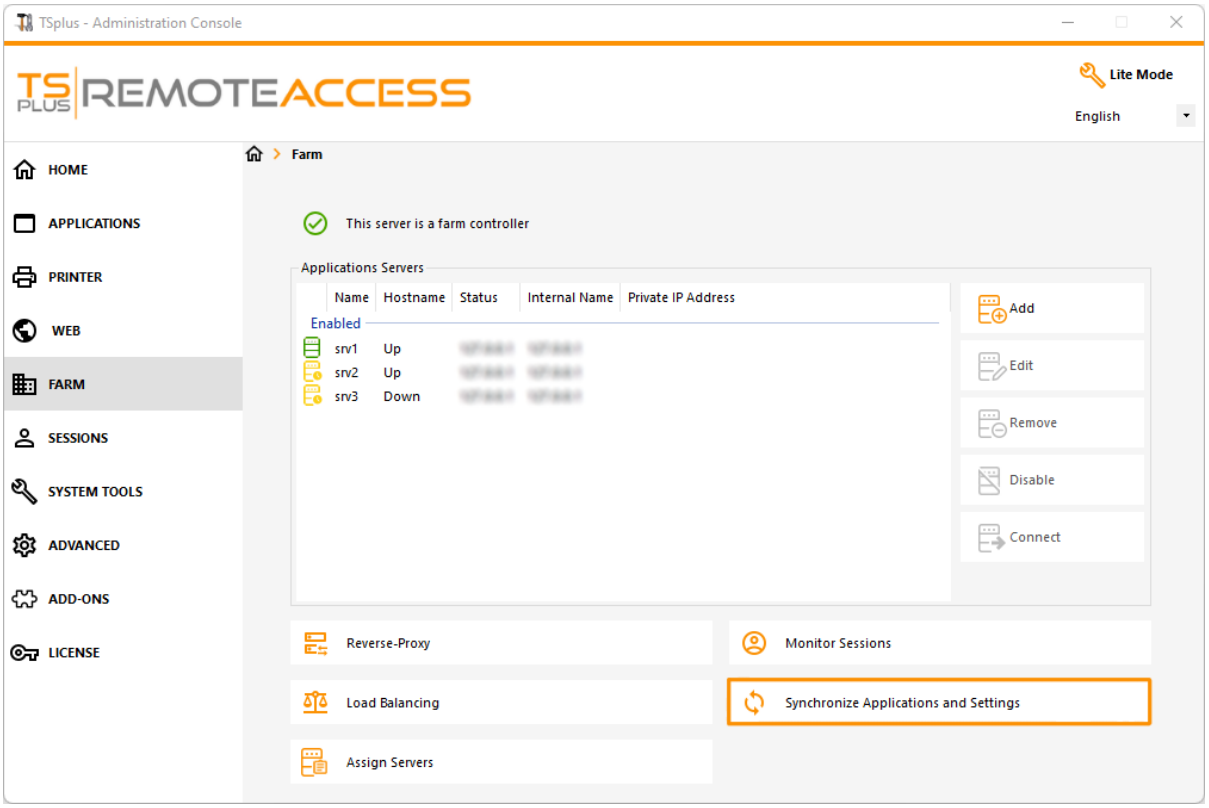
- “Déconnecter” : déconnecter la ou les sessions utilisateur sélectionnées (l'utilisateur pourra toujours se reconnecter à sa session).
- “Logoff”: déconnecter la ou les sessions utilisateur sélectionnées (toute modification non enregistrée sera perdue, les applications seront fermées brutalement).
- Envoyer un message : afficher une fenêtre pour entrer un titre et un texte, puis envoyer ce message à la ou les sessions utilisateur sélectionnées.
- Afficher une session utilisateur sélectionnée avec/sans***** autorisations.
- “Contrôle à distance” : Contrôlez à distance une session utilisateur sélectionnée avec/sans ***** autorisations.
- “Rafraîchir” : effectuer un rafraîchissement complet de la liste des sessions utilisateur pour le(s) serveur(s) sélectionné(s).

* Pour afficher ou contrôler une session **sans autorisations** vous devrez **changez le GPO suivant sur le serveur d'application que vous souhaitez visualiser et/ou contrôler les sessions de** .
Emplacement GPO : Configuration de l'ordinateur > Modèles d'administration > Composants Windows > Services de bureau à distance > Hôte de session de bureau à distance > Connexions .
Clé GPO : Définir des règles pour le contrôle à distance des sessions utilisateur des services de bureau à distance

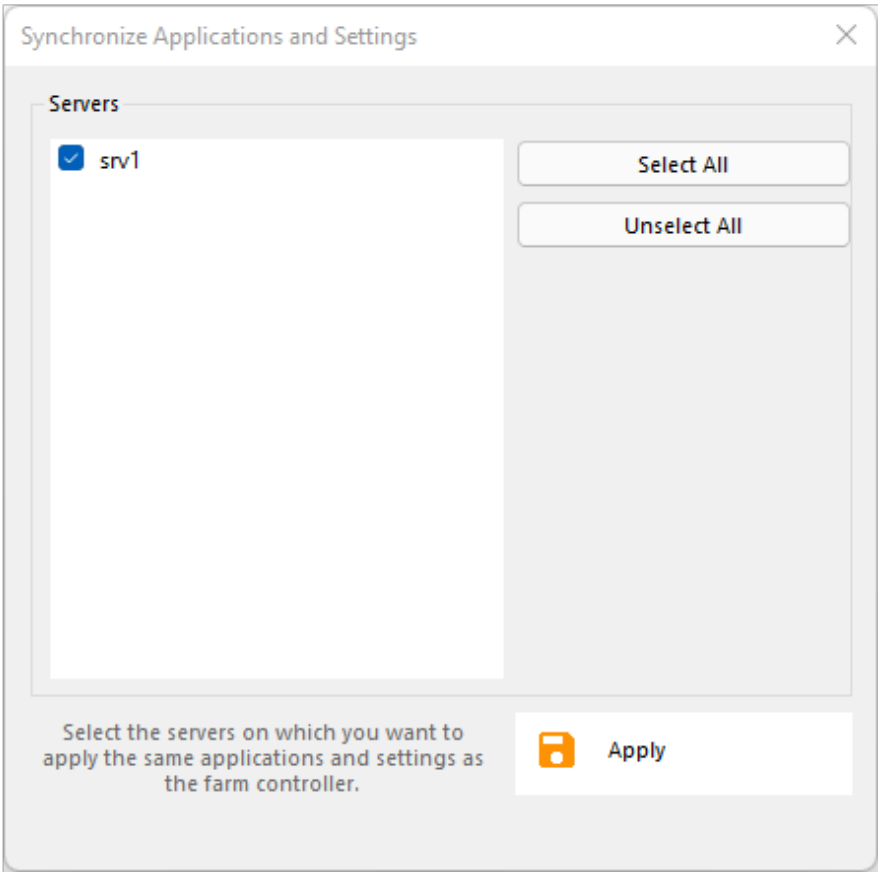
La liste des sessions utilisateur est automatiquement actualisée toutes les 5 secondes. Ce rafraîchissement automatique s'arrête si le serveur sélectionné devient indisponible. Un clic sur le bouton "Actualiser" relancera le rafraîchissement automatique.

Synchronisation des applications et des paramètres

Aperçu

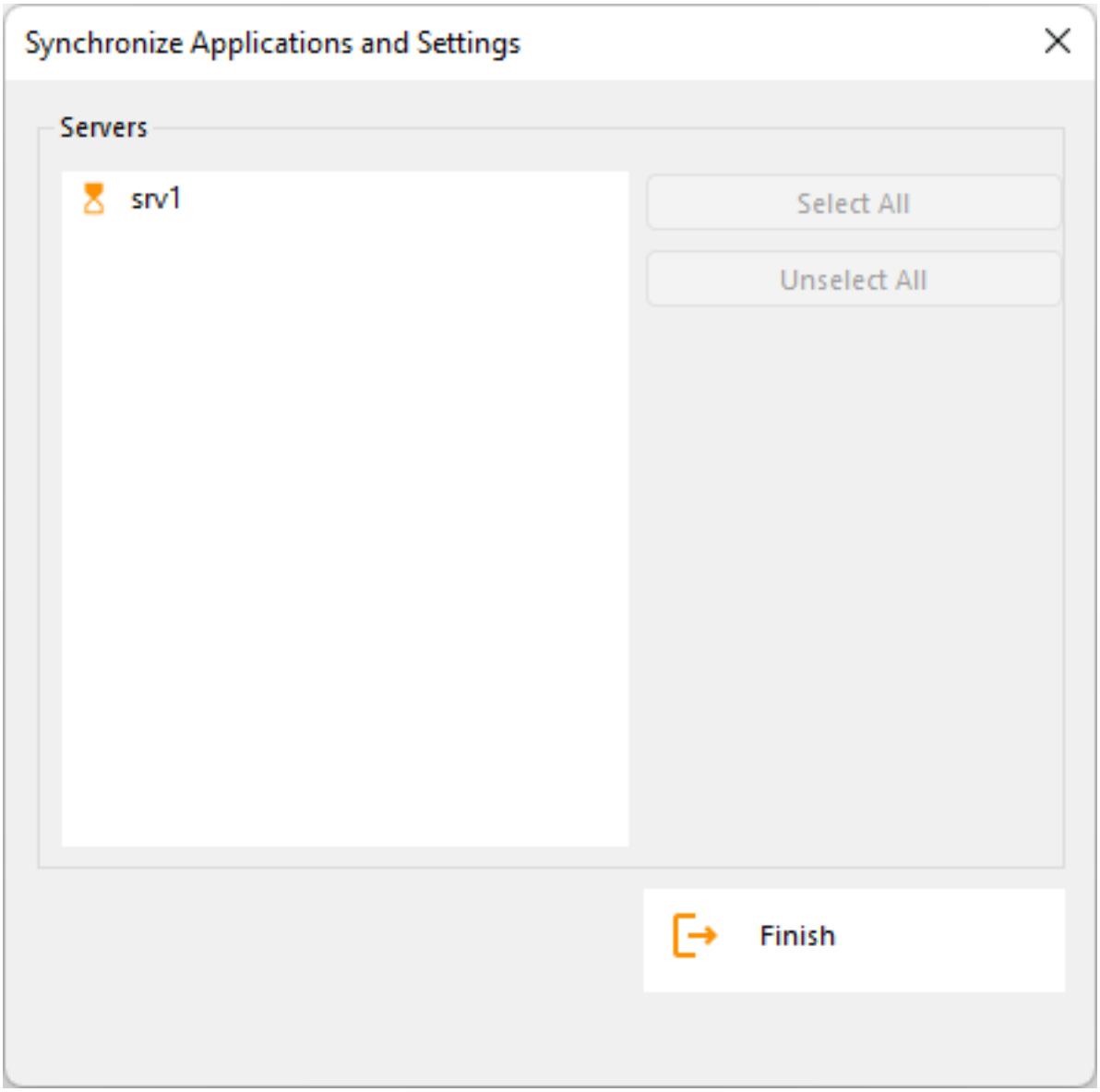


Cliquez sur le bouton « Synchroniser les applications et les paramètres » pour afficher la fenêtre suivante :



Vérifiez tous les serveurs sur lesquels vous souhaitez appliquer les mêmes paramètres et publier les mêmes applications que celles du Contrôleur de Ferme, puis cliquez sur « Appliquer ».

La fenêtre suivante sera affichée, vous permettant de surveiller l'avancement de la tâche :


Synchronize Applications and Settings
Servers
srv1
Select All
Unselect All
Finish

Transfert de fichiers rapide et facile entre l'utilisateur et le serveur

Aperçu

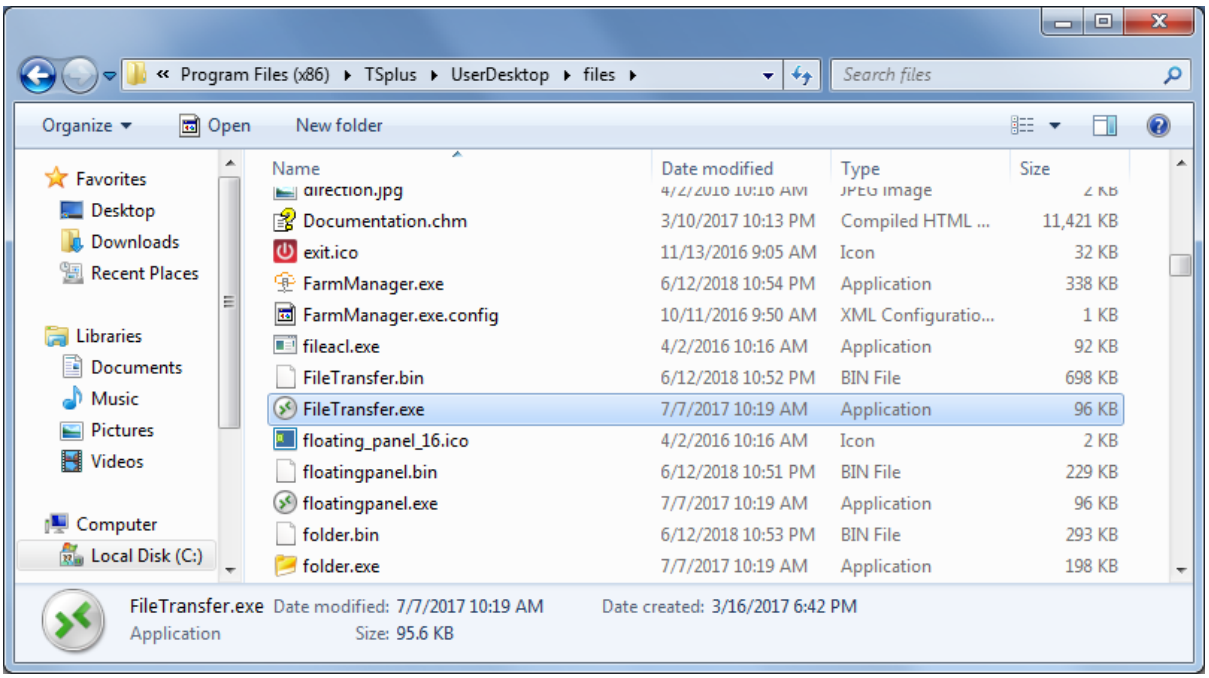
TSplus inclut une méthode unique de transfert de fichiers :

- de la station de travail utilisateur locale => vers le Bureau à distance de l'utilisateur
- du serveur TSplus vers le bureau de l'utilisateur local

Parce que les transferts de fichiers sont basés sur un canal virtuel, c'est beaucoup plus rapide qu'une copie de fichier, et cela peut être fait. **même lorsque les disques durs locaux de l'utilisateur ne sont pas mappés** .

Programme de transfert de fichiers et clients générés

Le programme de transfert de fichiers se trouve dans votre dossier de programme TSplus, sous le nom "FileTransfer.exe" dans le chemin suivant : "UserDesktop\files"



Transfert de fichiers

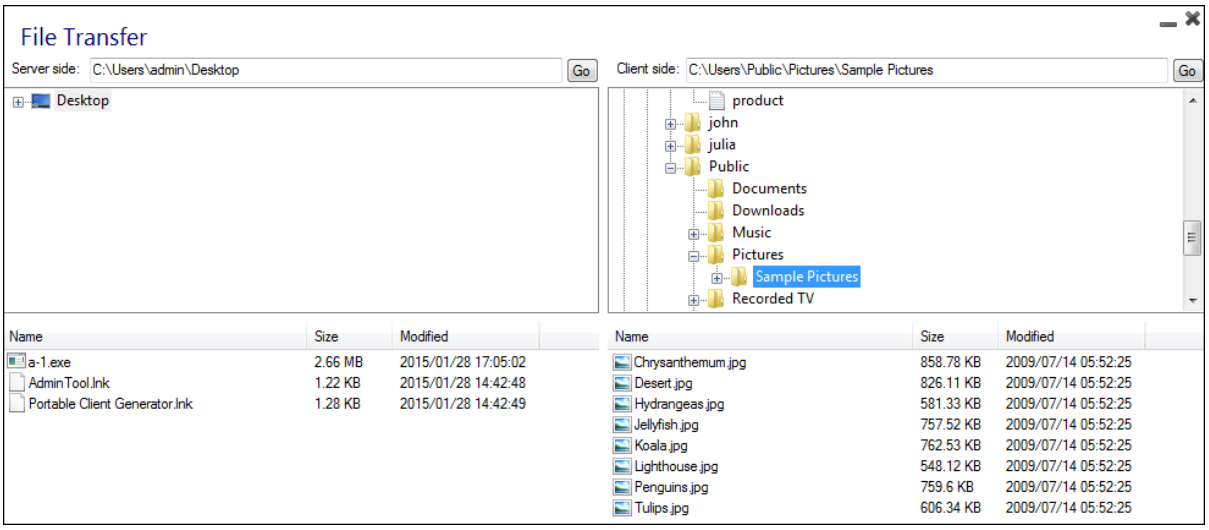
Transférer des fichiers est très facile.

Tout d'abord, lancez le transfert de fichiers (par exemple en utilisant le panneau flottant TSplus) :

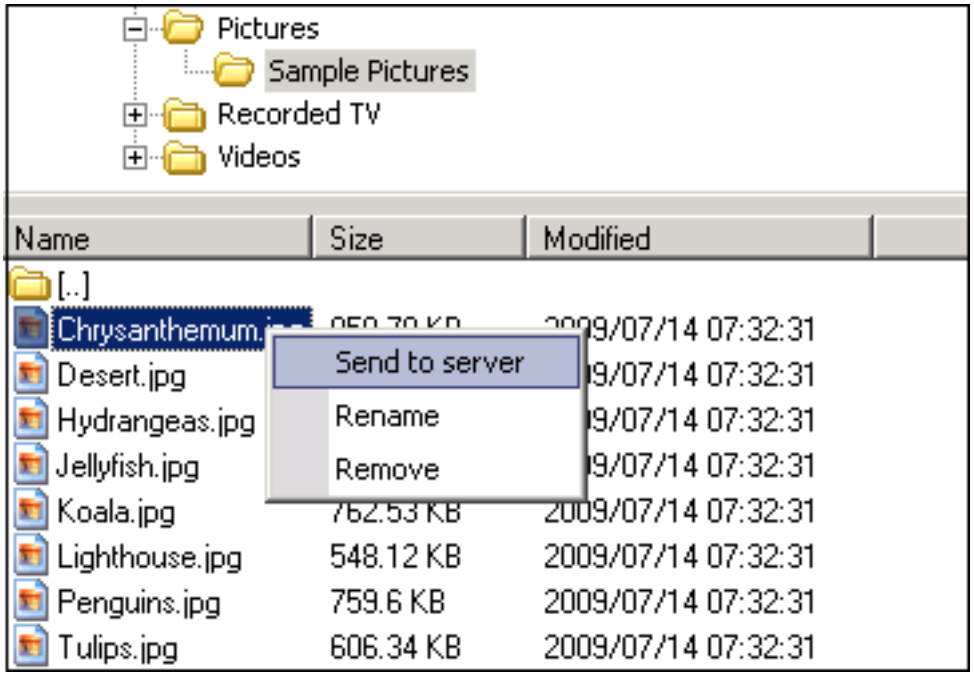


Ensuite, naviguez vers votre fichier en utilisant l'arborescence des dossiers :

- les dossiers et fichiers du serveur sont sur le **partie gauche de la fenêtre (côté serveur)**
- les dossiers et fichiers de la station de travail locale sont sur le **partie droite de la fenêtre (côté client)**



Enfin, faites un clic droit sur le fichier que vous souhaitez transférer de l'autre côté, puis cliquez sur « Envoyer au serveur » (ou « Envoyer au client ») :



Le transfert de fichiers fonctionne de la station de travail locale vers le serveur, ainsi que dans l'autre sens (du serveur vers la station de travail locale).

Remarque Lorsque vous utilisez l'utilitaire de transfert de fichiers depuis une session HTML5, vous pourrez transférer vos fichiers du serveur au client uniquement. Veuillez préférer le Méthode de menu supérieur HTML5 où vous pouvez télécharger des fichiers sur le serveur, télécharger sur le client et gérer votre liste de transferts de fichiers.

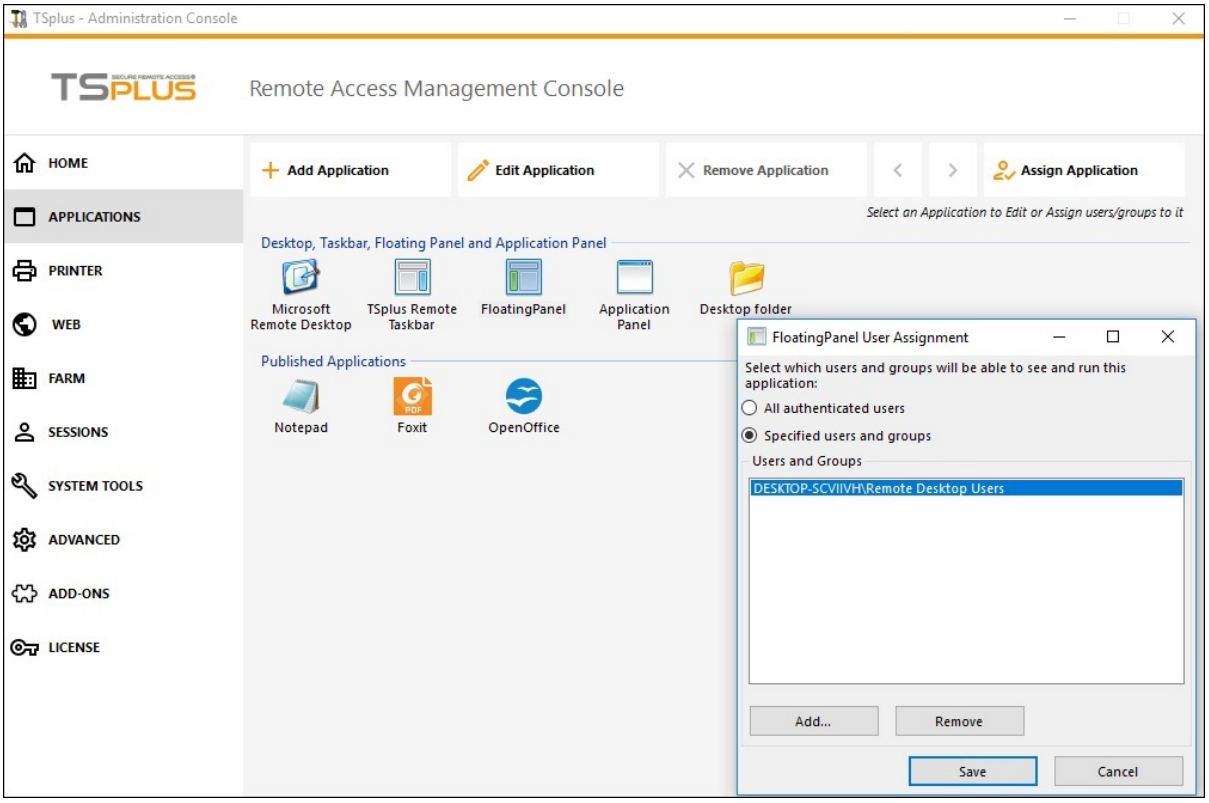
Panneau flottant et panneau d'application

Vous pouvez choisir d'activer le panneau flottant ou le panneau d'application pour vos utilisateurs ou groupes.

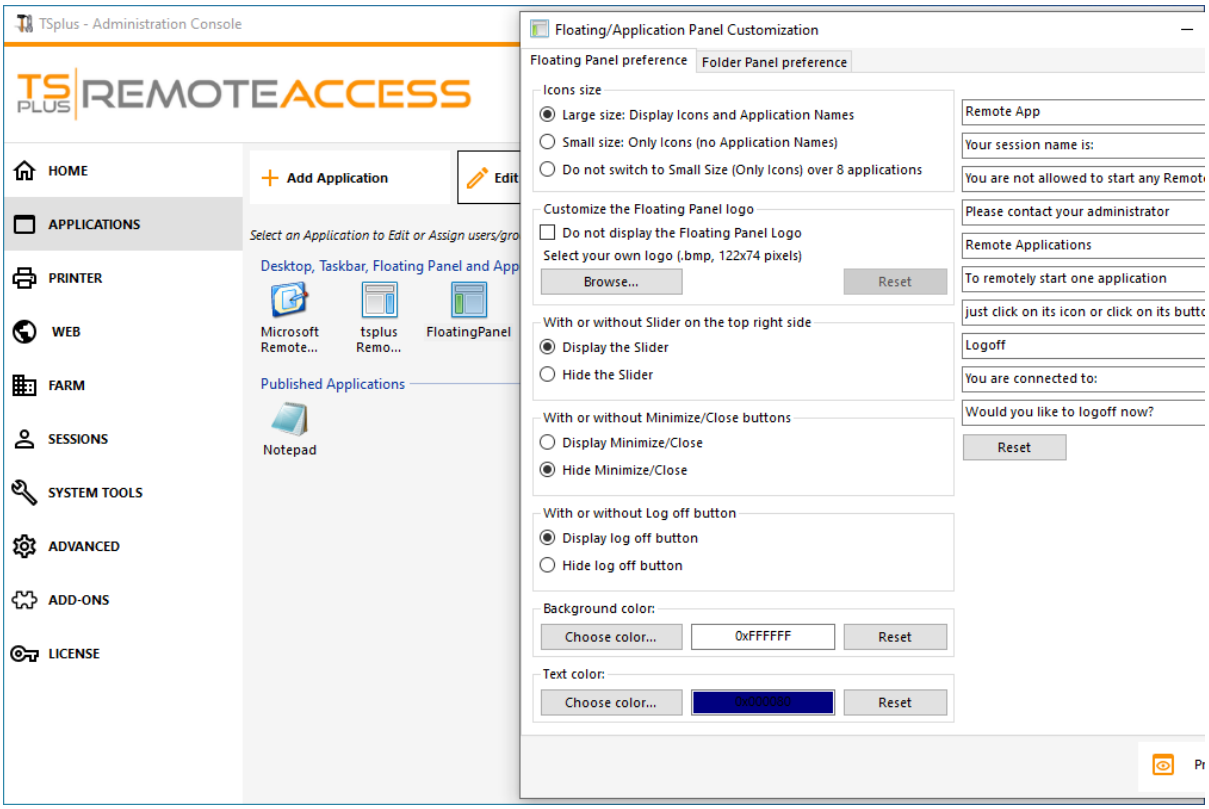
Ces deux méthodes de publication d'applications sont disponibles pour tout mode de connexion.

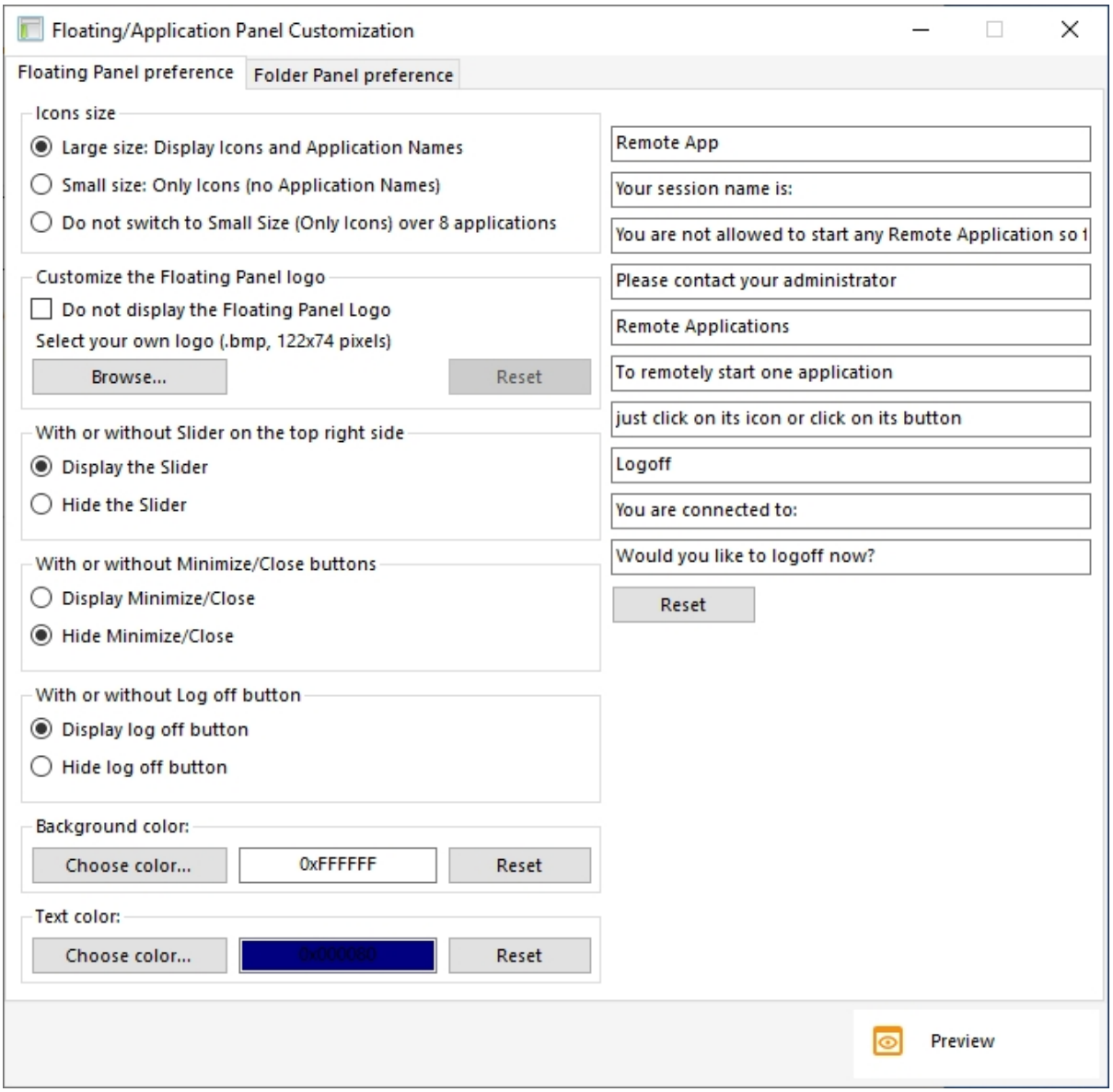
Si activé avec les applications assignées, vous pouvez voir sur le milieu-gauche de l'écran de l'utilisateur la mini liste déroulante des applications ou le panneau flottant (très apprécié par les utilisateurs de TSplus) :

Assignez-le en tant qu'application :



Sélectionnez le panneau flottant, puis cliquez sur la tuile « Modifier l'application » pour personnaliser le panneau flottant à votre convenance :


TSplus - Administration Console
TS PLUS REMOTEACCESS
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Add Application
Edit
Select an Application to Edit or Assign users/gro
Desktop, Taskbar, Floating Panel and App
Microsoft Remote...
tsplus Remo...
FloatingPanel
Published Applications
Notepad
Floating/Application Panel Customization
Floating Panel preference
Folder Panel preference
Icons size
Large size: Display Icons and Application Names
Small size: Only Icons (no Application Names)
Do not switch to Small Size (Only Icons) over 8 applications
Customize the Floating Panel logo
Do not display the Floating Panel Logo
Select your own logo (.bmp, 122x74 pixels)
Browse...
Reset
With or without Slider on the top right side
Display the Slider
Hide the Slider
With or without Minimize/Close buttons
Display Minimize/Close
Hide Minimize/Close
With or without Log off button
Display log off button
Hide log off button
Background color:
Choose color...
0xFFFFFF
Reset
Text color:
Choose color...
Reset
Remote App
Your session name is:
You are not allowed to start any Remot
Please contact your administrator
Remote Applications
To remotely start one application
just click on its icon or click on its butt
Logoff
You are connected to:
Would you like to logoff now?
Reset



Ces différentes options peuvent vous permettre de personnaliser l'expérience de l'utilisateur final.

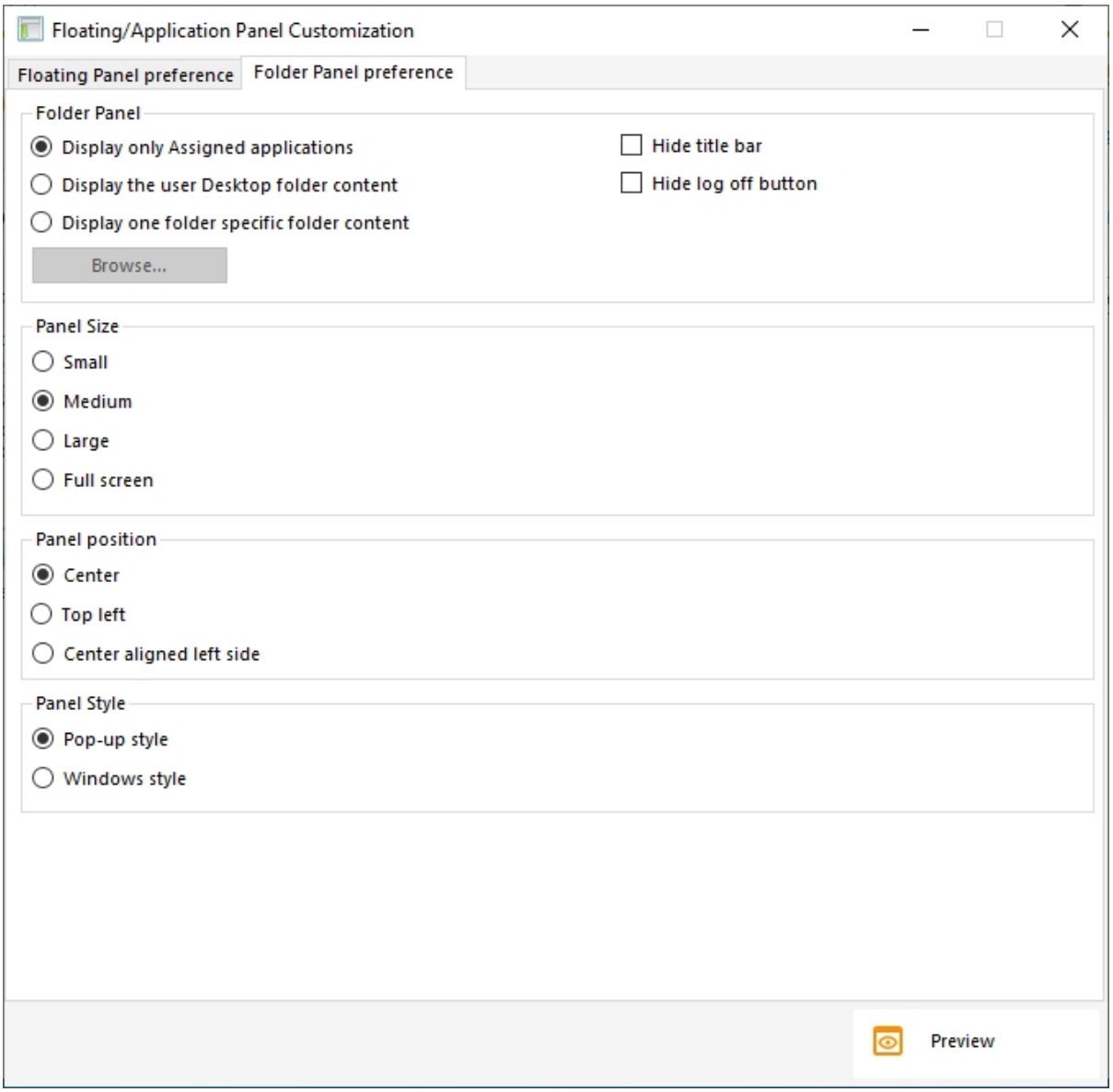
Voici les différentes options d'affichage du panneau flottant, où vous pouvez définir,

- Modifier le texte affiché,
- Choisissez votre taille préférée, entre grande et petite, où vous pouvez afficher uniquement des icônes,
- Ajoutez votre propre logo,
- Personnalisez la couleur de l'arrière-plan et du texte,
- Afficher le curseur ou non,
- Afficher les boutons Réduire/Fermer ou non,
- Afficher l'icône de déconnexion ou non…

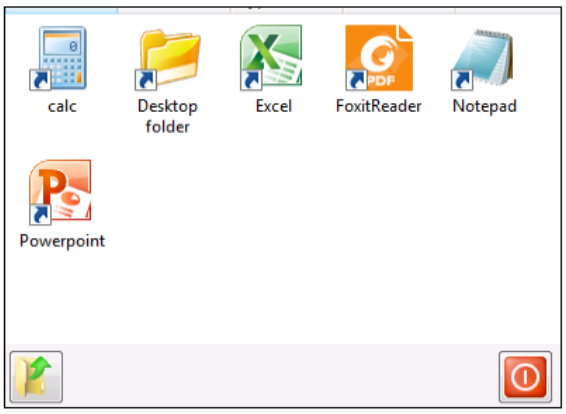


Veuillez noter que plus de 8 applications, le Panneau Flottant passe automatiquement à une taille réduite. Si vous souhaitez toujours afficher les noms des Applications, sélectionnez « Ne pas passer à la taille réduite (uniquement des icônes) pour plus de 8 applications.

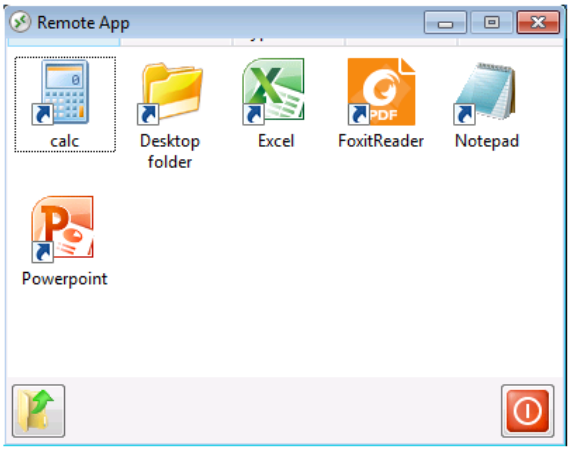
Le **Panneau de Dossiers** est personnalisable et permet d'afficher les applications assignées, le dossier Bureau de l'utilisateur ou le contenu d'un dossier spécifique dans votre session avec de nombreuses options d'affichage :



Vous pouvez changer la taille, la position et le style du panneau de dossiers (Pop-up ou Windows) à votre convenance :

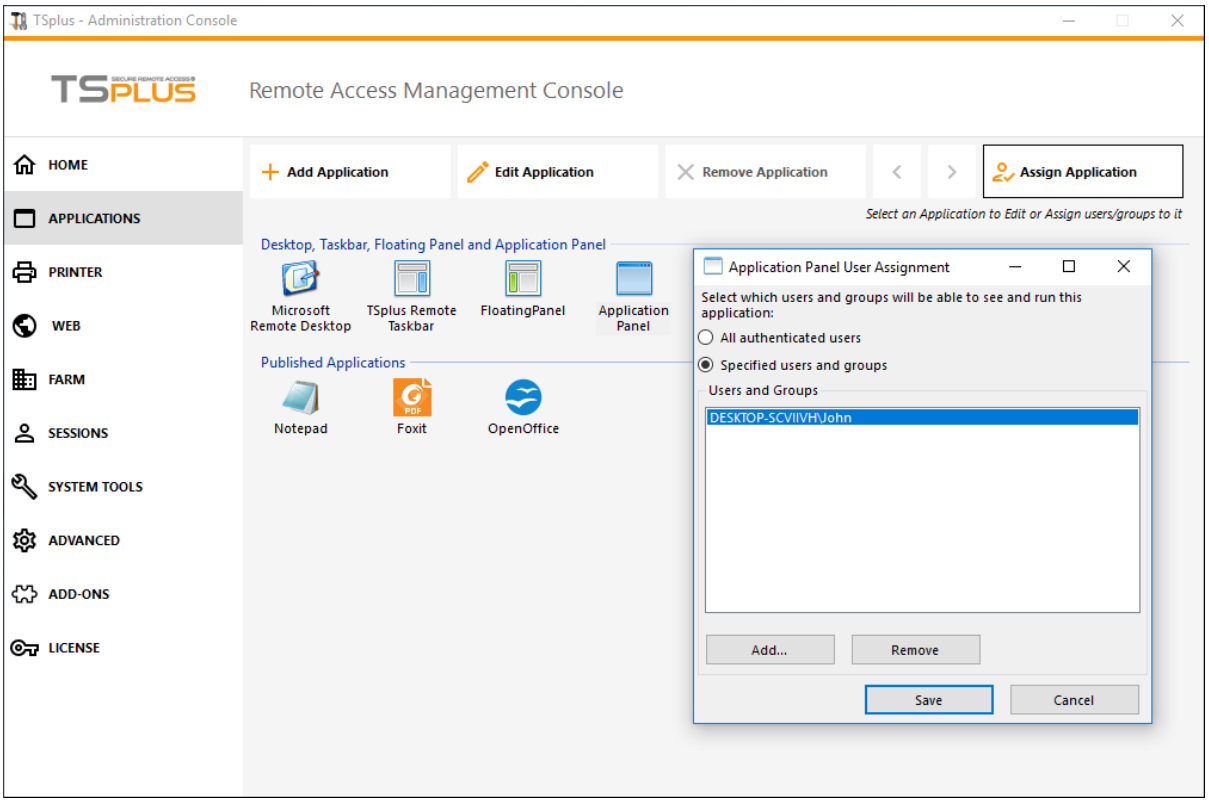


Pop-up style

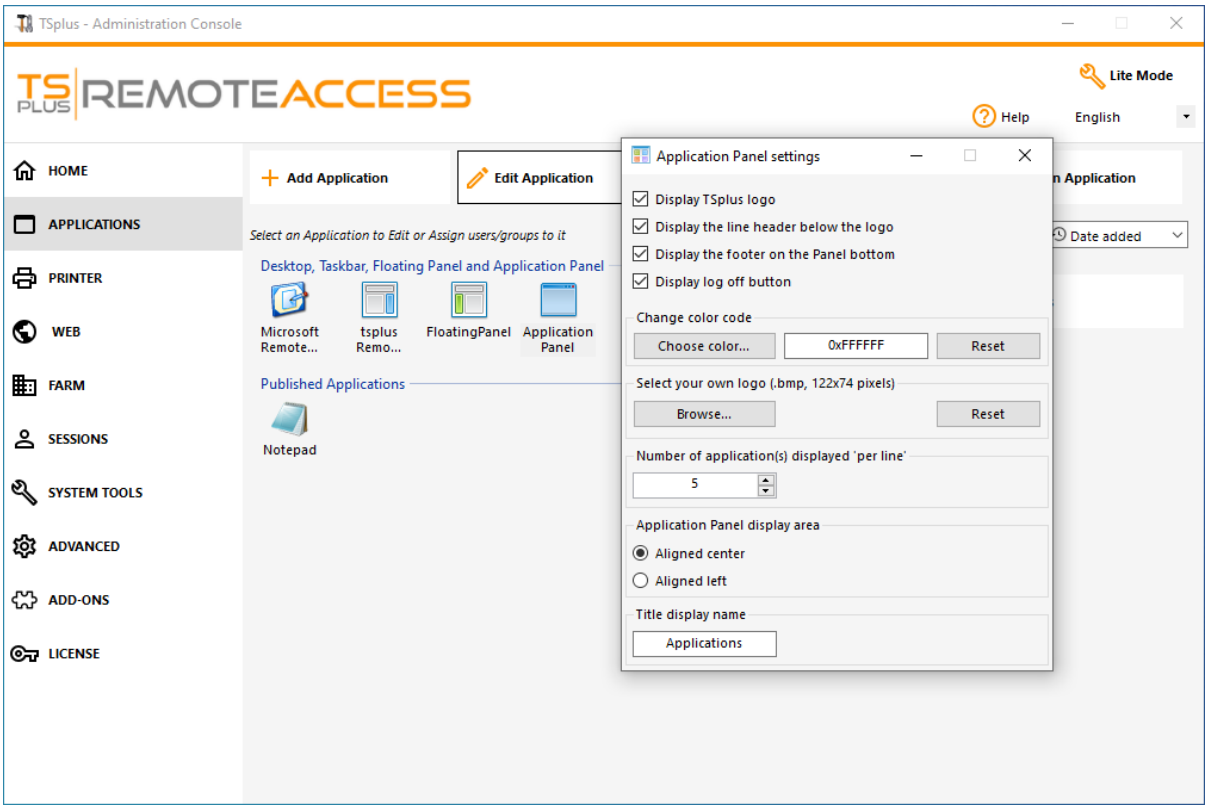


Windows style

Le Panneau d'Application vous donne la possibilité d'organiser les applications affichées, exactement comme sur le Portail d'Application Web, mais en l'assignant simplement à un utilisateur ou à un groupe.



L'administrateur peut le personnaliser en choisissant d'afficher le logo TSplus ou son propre logo, d'afficher l'en-tête de ligne sous le logo et le pied de page, de changer la couleur ou de choisir de ne rien afficher du tout en désélectionnant les cases correspondantes. Il peut également ajuster le nombre d'applications affichées par lignes et colonnes en entrant le nombre d'applications affichées par ligne, ainsi que l'alignement et le nom du panneau d'application.



Par exemple, afficher six applications dans une colonne, sans logo ; ou affichées sur 2 colonnes et 3 lignes, avec le logo TSplus :


Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

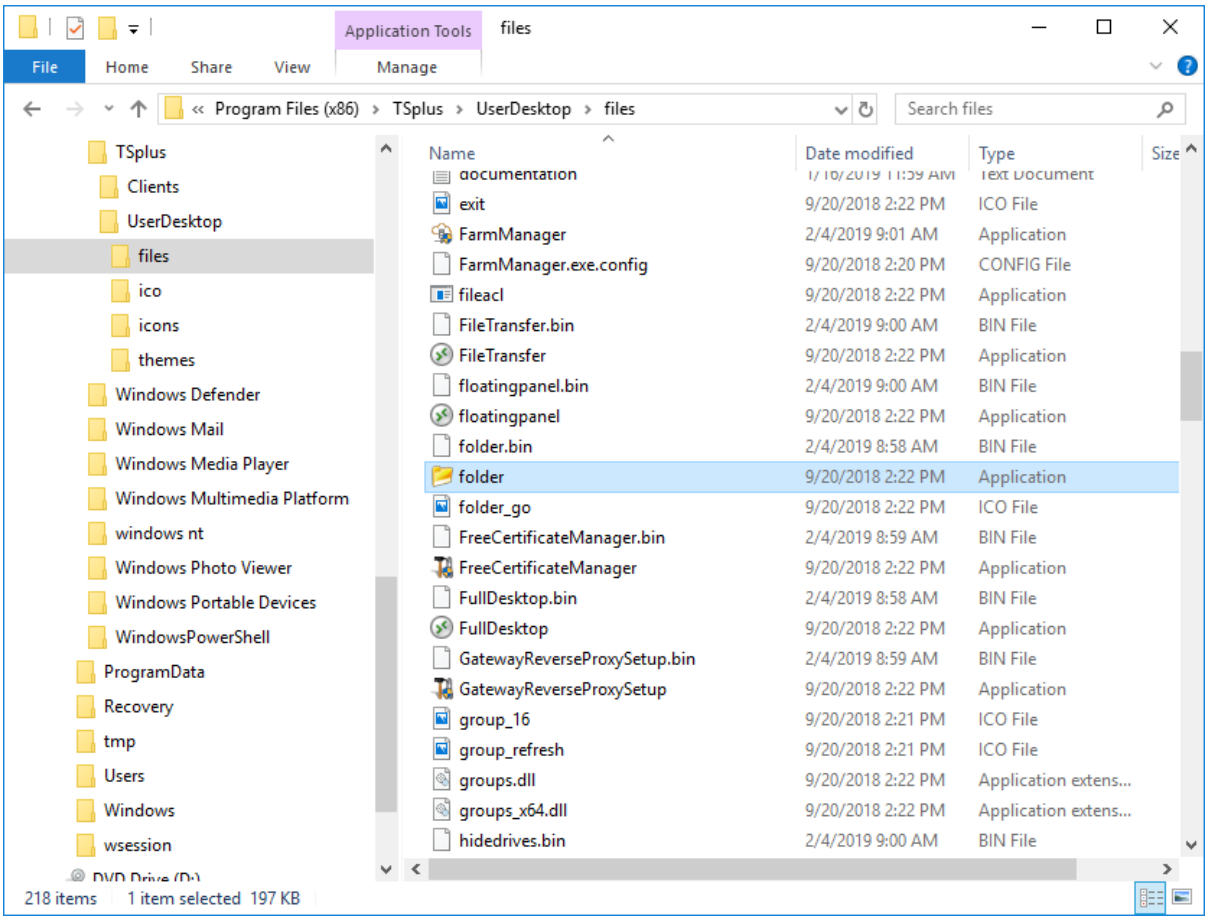

TSPLUS
Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

Partage de dossier sécurisé - Folder.exe

L'application Folder affichera en toute sécurité le contenu d'un dossier que vous rendrez disponible pour vos utilisateurs.

Tout d'abord, créez un dossier sur votre serveur avec des applications ou des documents que vous souhaitez partager.

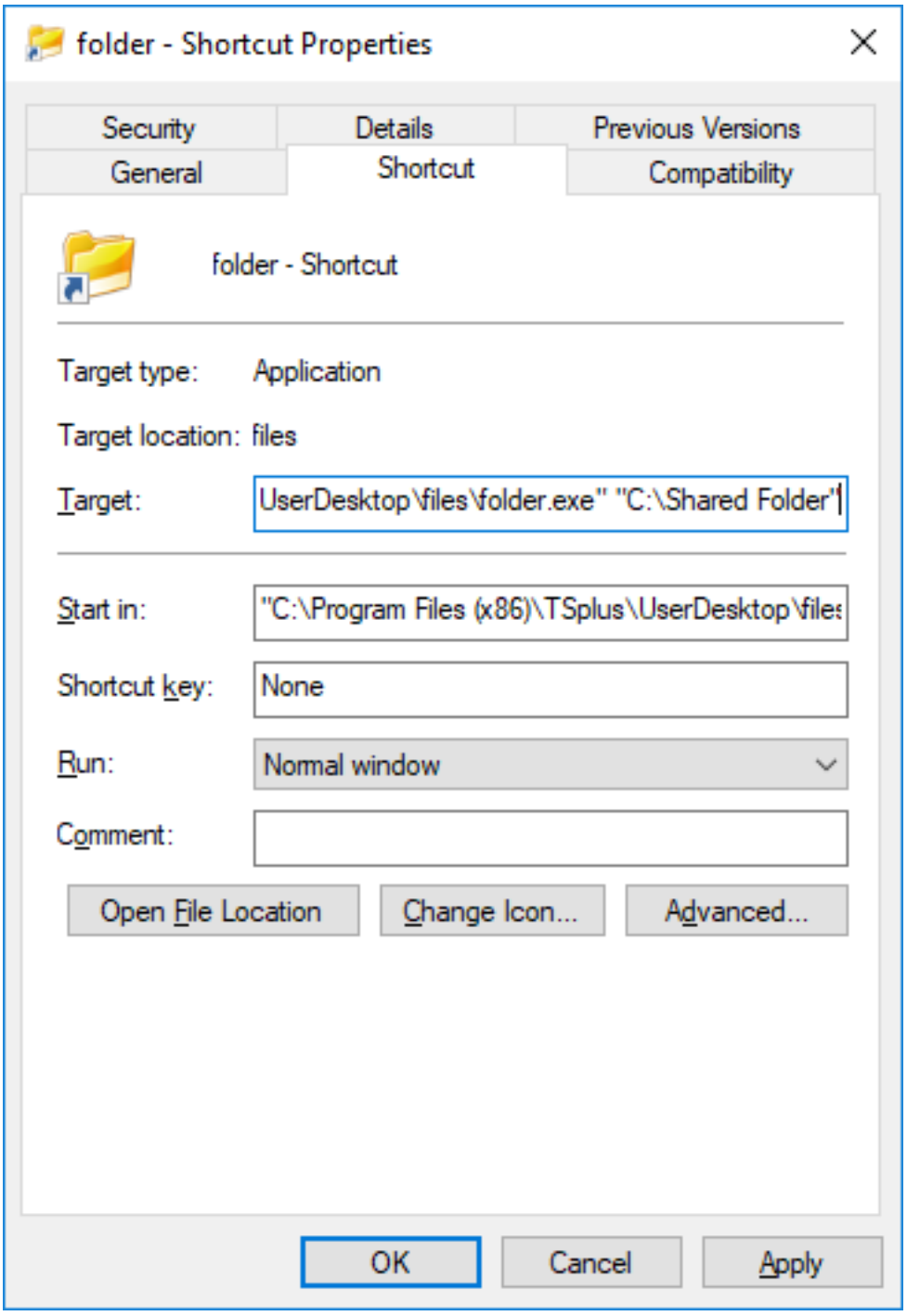
Ouvrez un explorer.exe et localisez l'application folder.exe dans C:\Program Files\tsplus\UserDesktop\files:



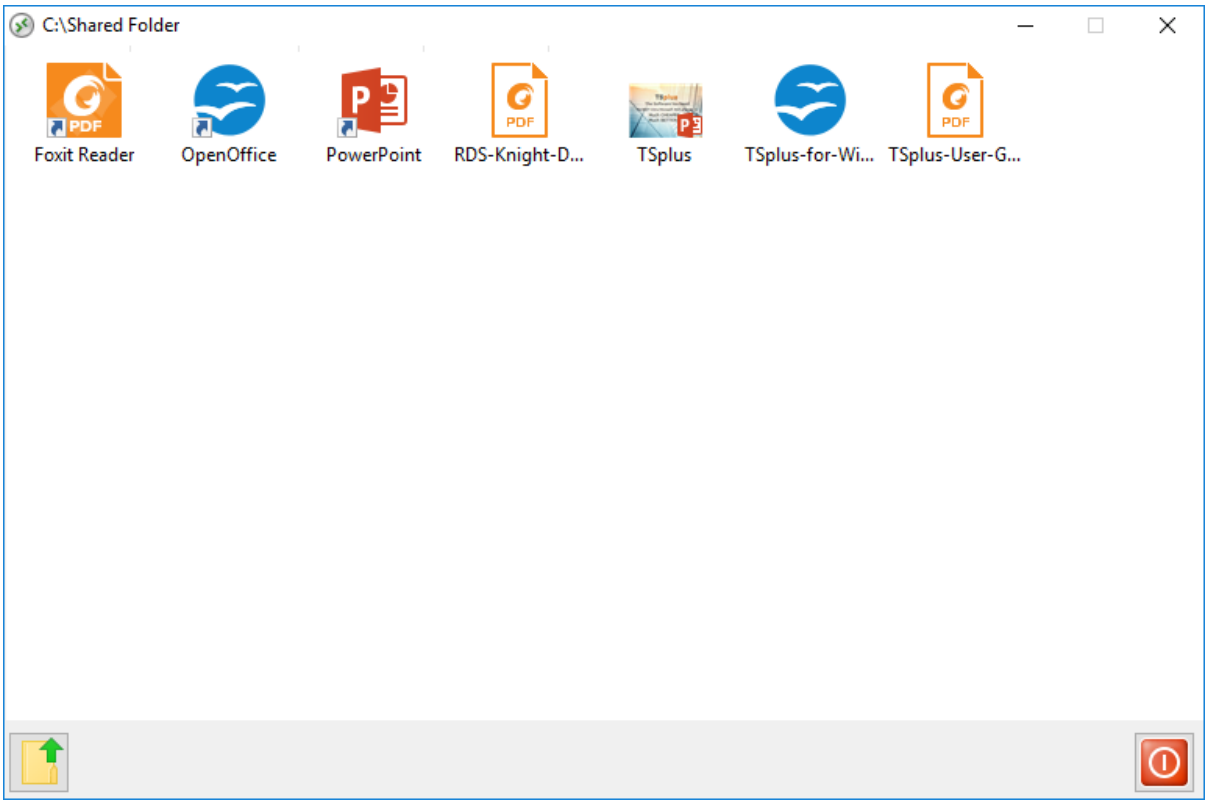
Créez un raccourci de ce fichier. Modifiez les propriétés de ce raccourci en cliquant dessus avec le bouton droit.

Ensuite, modifiez le chemin cible du raccourci en saisissant le chemin de votre dossier d'applications dans la ligne "Cible", après le chemin cible original, par exemple :

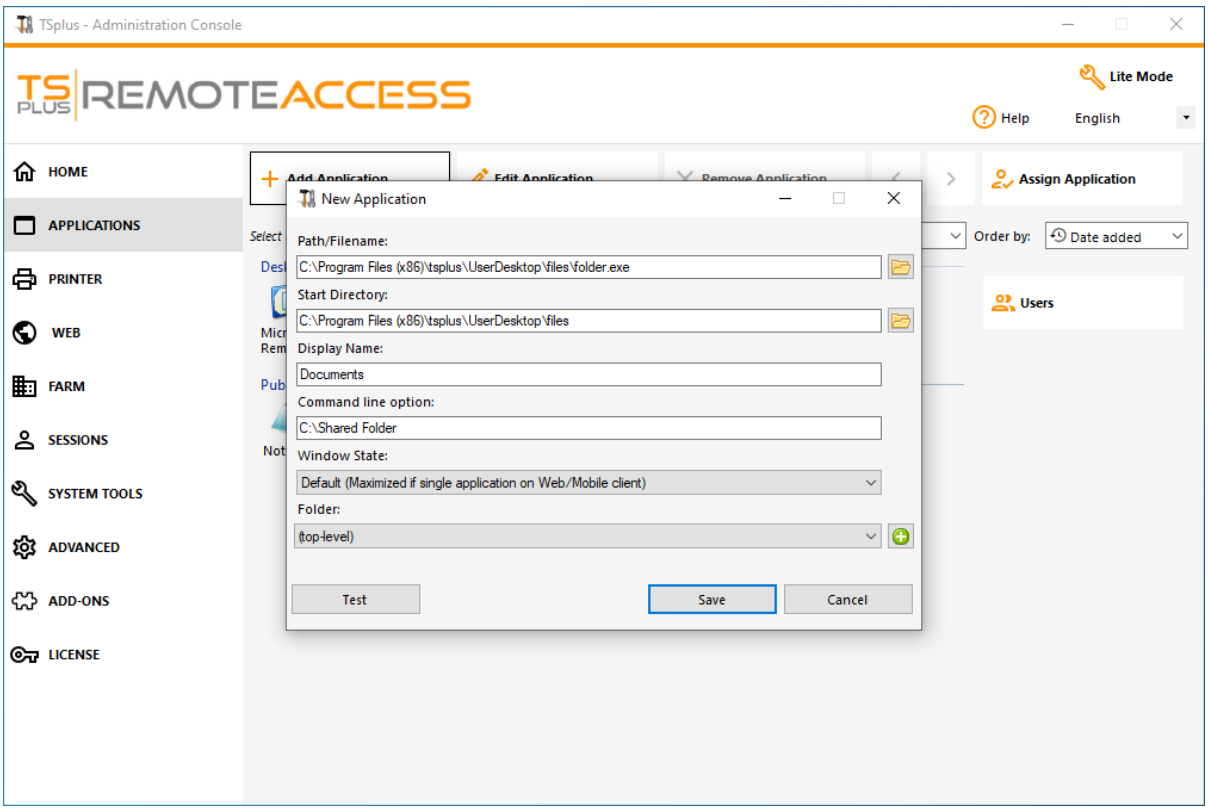
“C:\Program Files\tsplus\UserDesktop\files\folder.exe” “C:\Dossier partagé”



Lorsque vous ouvrez le raccourci folder.exe, cela devrait ressembler à ceci (avec vos propres documents et applications) :



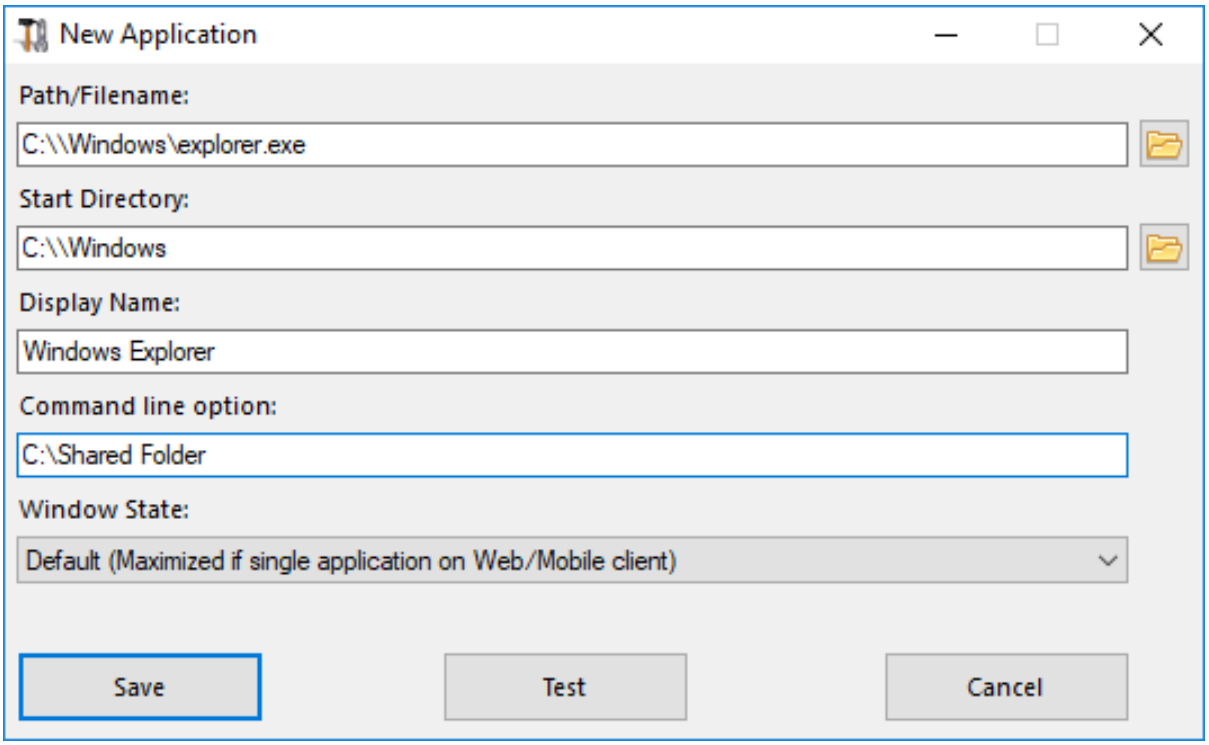
Ce raccourci peut être copié dans le dossier de bureau du profil d'un utilisateur ou vous pouvez publier le dossier.exe pour un utilisateur en tant qu'application. Si vous faites cela, vous devrez indiquer le chemin de votre dossier dans la section des options de ligne de commande.



Il existe une autre façon de partager un dossier de documents.

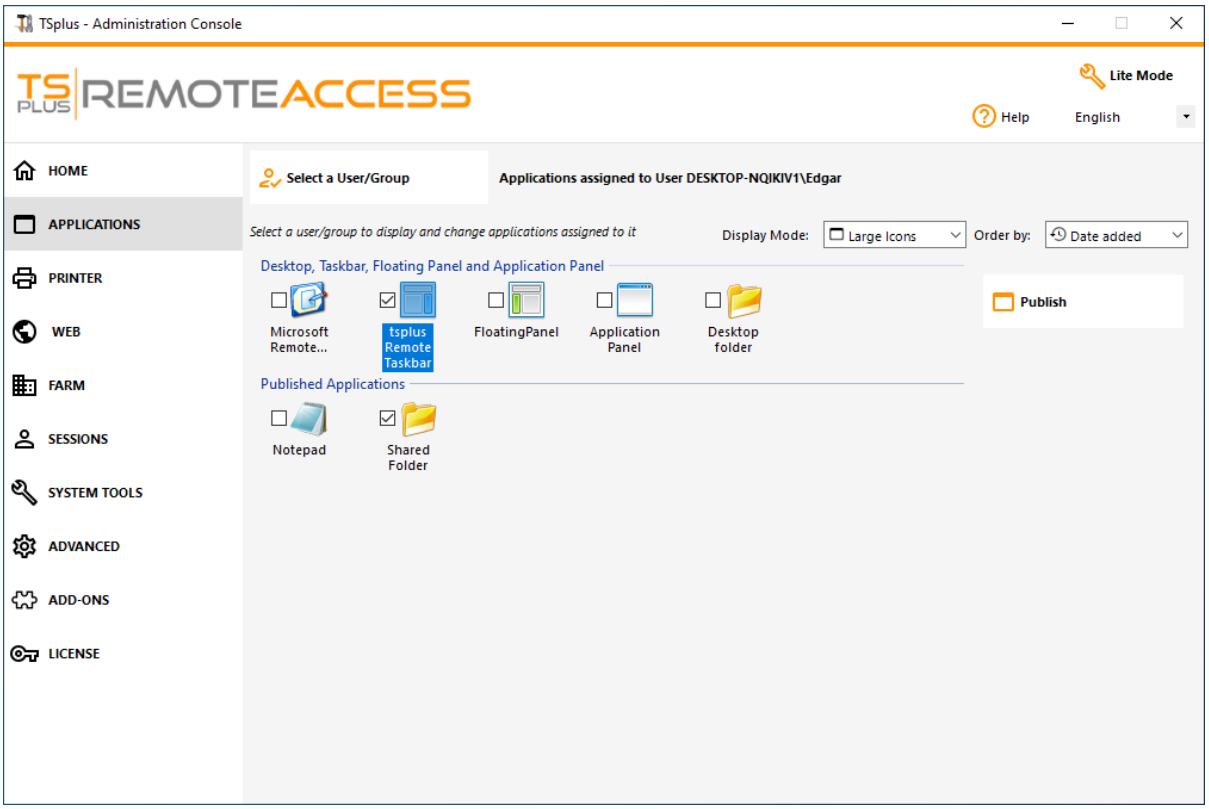
Publier un dossier partagé en tant qu'application unique :

Ajoutez une nouvelle application. Dans le champ de nom d'affichage, saisissez le nom du dossier partagé ou tout autre nom que vous souhaitez. Cliquez sur le bouton de navigation situé à droite du champ "Chemin/Nom de fichier" et localisez C:\Windows\explorer.exe. Le répertoire de démarrage sera automatiquement rempli avec le chemin de explorer.exe. Dans le champ d'option de ligne de commande, saisissez le chemin du dossier partagé, cela peut être un dossier local ou un dossier partagé sur le réseau en utilisant un chemin UNC (exemple : \data\dossier partagé). Remplissez le champ ci-dessous avec les informations de votre dossier partagé.

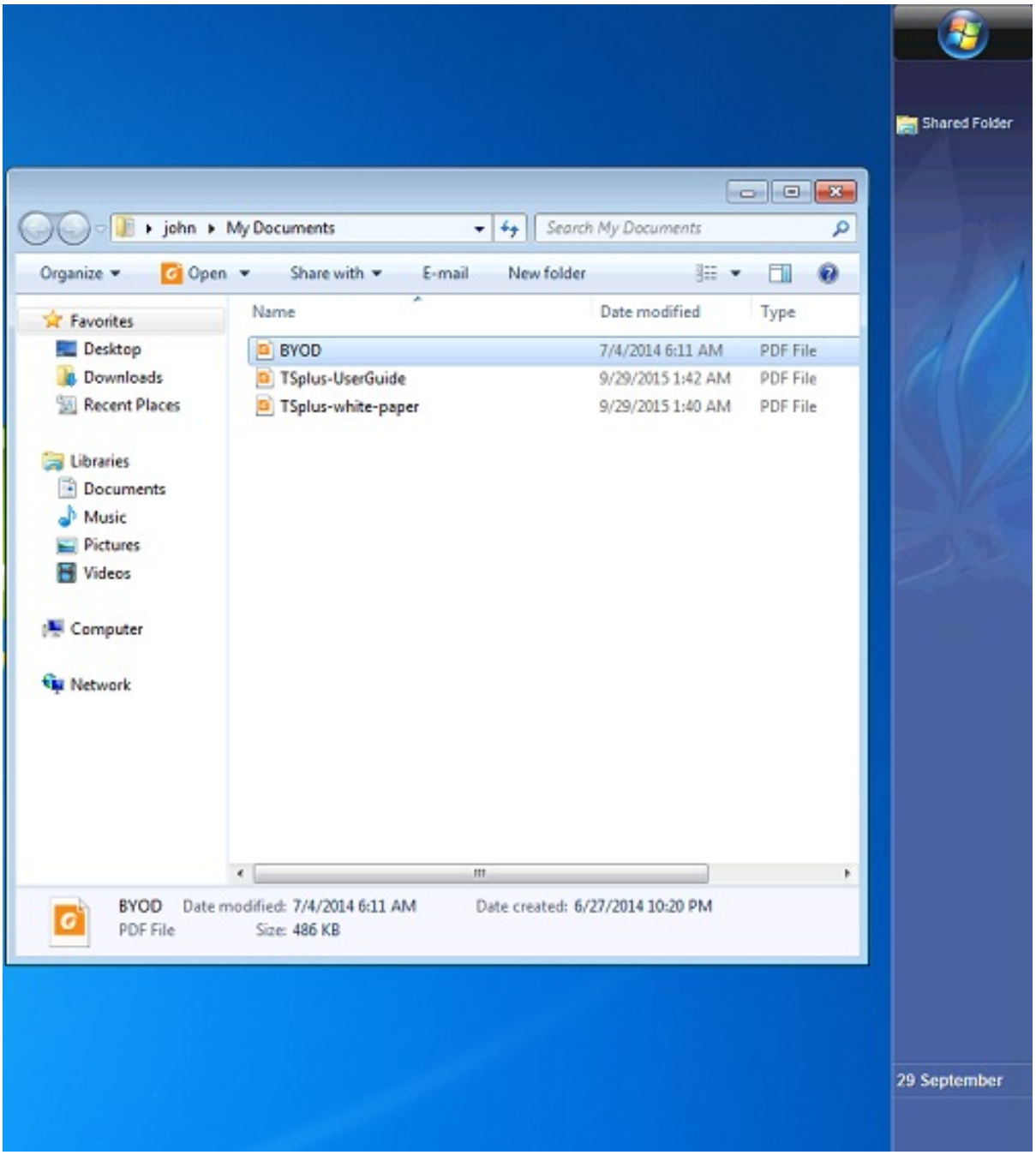


Puis cliquez sur « Enregistrer ».

Cliquez sur l'onglet « Utilisateurs ». Sélectionnez votre utilisateur et cochez les cases TSplus Remote Taskbar et Shared Folder :

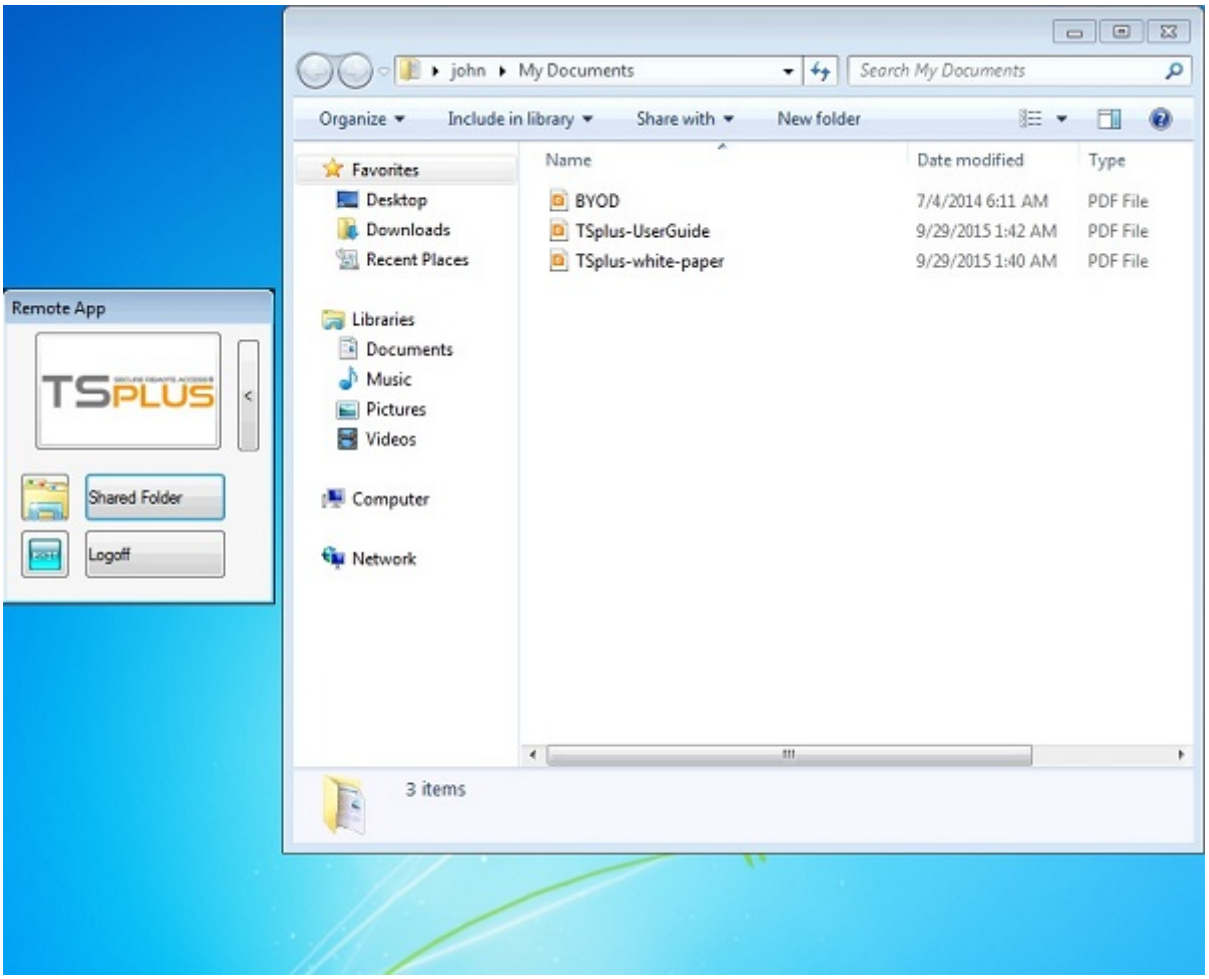


Voici le résultat, lorsque vous ouvrez une session avec un client RDP, vous verrez la barre des tâches TSplus avec l'application de dossier partagé :



Vous pouvez également faire cela avec le panneau flottant. Ouvrez un outil d'administration et cliquez sur l'onglet « Assigner une application ». Cochez les cases Panneau flottant et Dossier partagé.

Voici le résultat :


Remote App
TSPLUS
Shared Folder
Logoff
john ▸ My Documents
Search My Documents
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
BYOD
7/4/2014 6:11 AM
PDF File
TSplus-UserGuide
9/29/2015 1:42 AM
PDF File
TSplus-white-paper
9/29/2015 1:40 AM
PDF File
3 items

Certificat HTTPS gratuit et facile à installer

Aperçu

À partir de la version 9.20, TSplus propose une fonctionnalité facile à utiliser pour générer un certificat HTTPS gratuit et valide.

En 3 clics de souris, vous obtiendrez un certificat valide sécurisé, renouvelé automatiquement et configuré automatiquement dans le serveur web intégré de TSplus.

Cette fonctionnalité utilise Let's Encrypt fournir un certificat HTTPS gratuit et sécurisé pour vos connexions HTTPS.

Prérequis

Veuillez vous assurer que votre serveur TSplus répond à ces exigences avant d'utiliser le Gestionnaire de certificats gratuit :

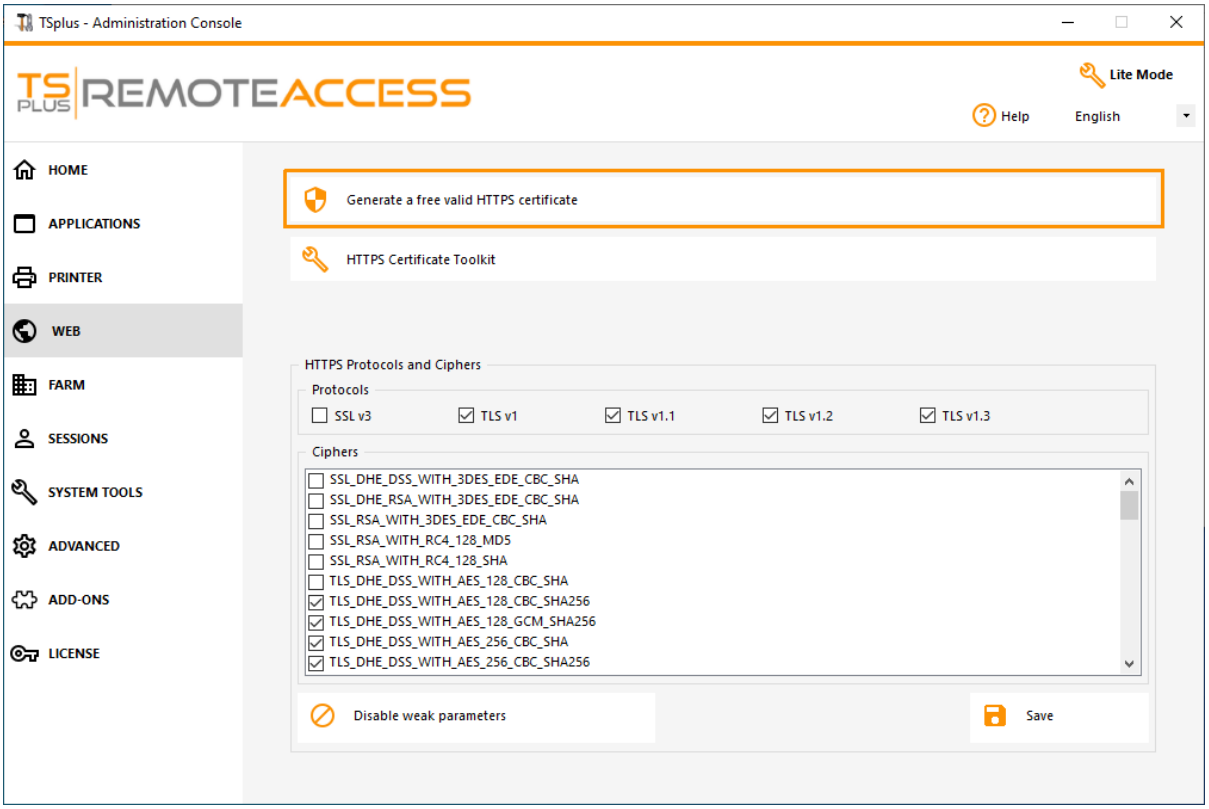
- Vous devez **utiliser le serveur web intégré de TSplus écoutant sur le port 80 pour HTTP** Ceci est requis par le processus de validation de propriété de domaine de Let's Encrypt.
- Votre **le nom de domaine du serveur doit être accessible** de l'Internet public. Cela est également nécessaire pour valider que vous êtes le véritable propriétaire du domaine.
- Vous devez **exécutez ce programme sur le serveur Gateway ou un serveur autonome, pas un serveur d'application** (sauf si votre serveur d'application est accessible depuis Internet public et a un nom de domaine public).

Il n'est pas possible d'obtenir un certificat pour une adresse IP, qu'elle soit publique ou privée.

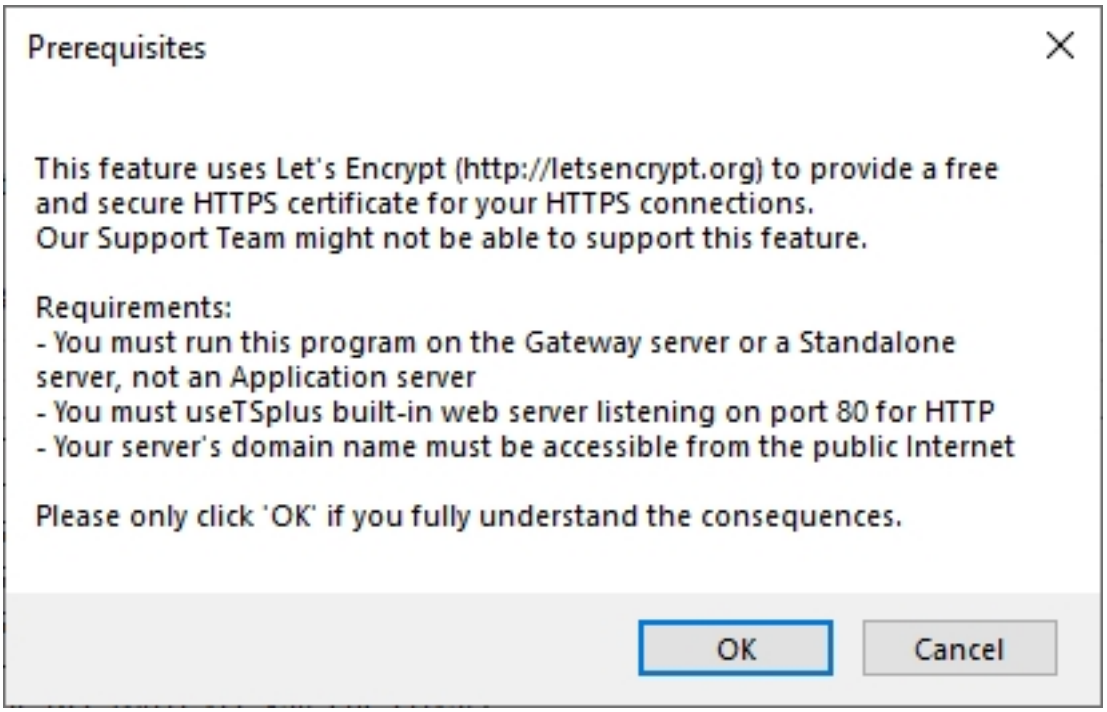
Il n'est pas possible d'obtenir un certificat pour un nom de domaine interne (c'est-à-dire un domaine qui ne se résout qu'à l'intérieur de votre réseau privé).

Gestionnaire de certificats gratuit GUI

Pour ouvrir l'interface graphique du gestionnaire de certificats gratuits TSplus, ouvrez TSplus AdminTool, cliquez sur l'onglet « Web - HTTPS », puis cliquez sur « Générer un certificat HTTPS valide gratuit » comme indiqué dans la capture d'écran ci-dessous :



Le gestionnaire de certificats gratuit GUI s'ouvrira et vous rappellera les prérequis, comme indiqué dans la capture d'écran ci-dessous :



Veuillez lire attentivement et vérifier que votre serveur répond à toutes les exigences, puis cliquez sur le bouton « Ok ».

Étape 1 : Entrez votre e-mail

Cet e-mail ne sera pas utilisé pour vous spammer. En fait, il ne sera même pas envoyé à TSplus ou à un tiers, sauf à l'émetteur du certificat : Let’s Encrypt.

Ils ne vous contacteront que si nécessaire, conformément à leurs Conditions de Service.

Étape 2 : Entrez le nom de domaine du serveur

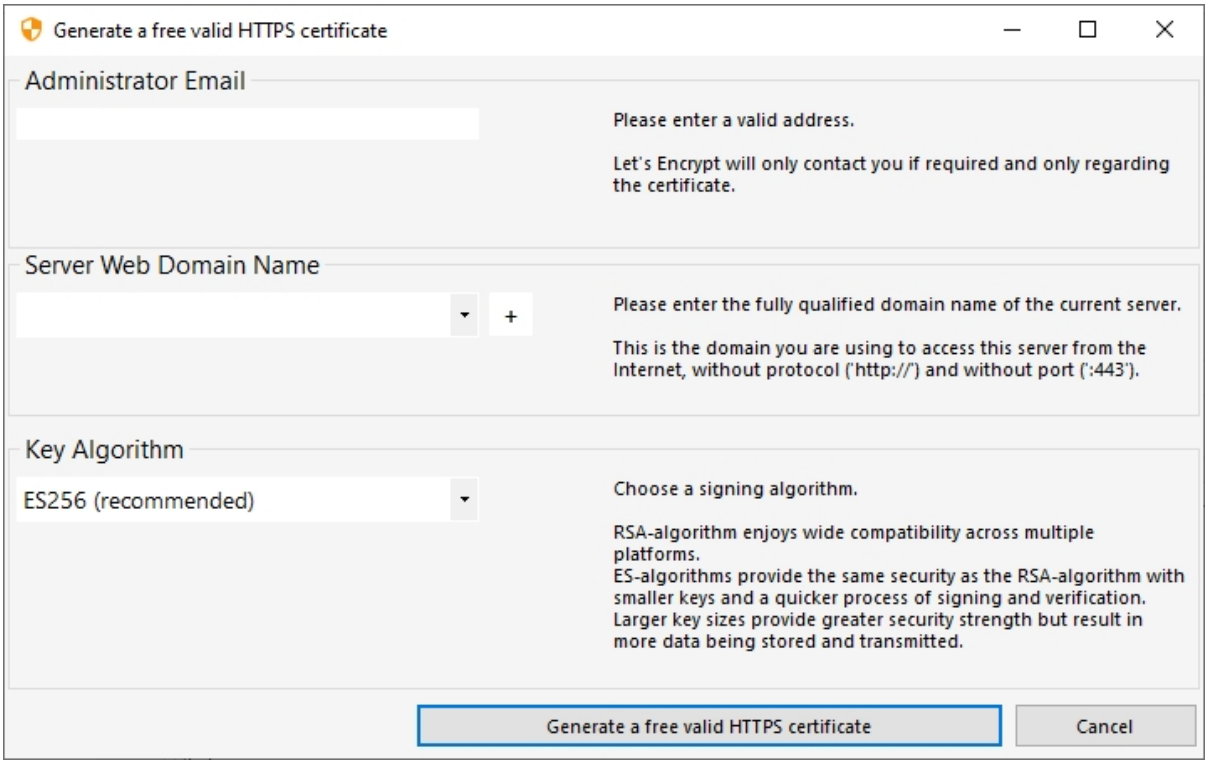
Ceci est le nom de domaine accessible au public sur Internet, quelque chose comme gateway.votre-entreprise.com. Vous pouvez également ajouter un autre nom de domaine ou un nom de sous-domaine après avoir cliqué sur le bouton ”+”.

Comme expliqué dans l'interface graphique, n'ajoutez pas de préfixe de protocole et/ou de suffixe de port, entrez simplement le(s) nom(s) de domaine propre(s).

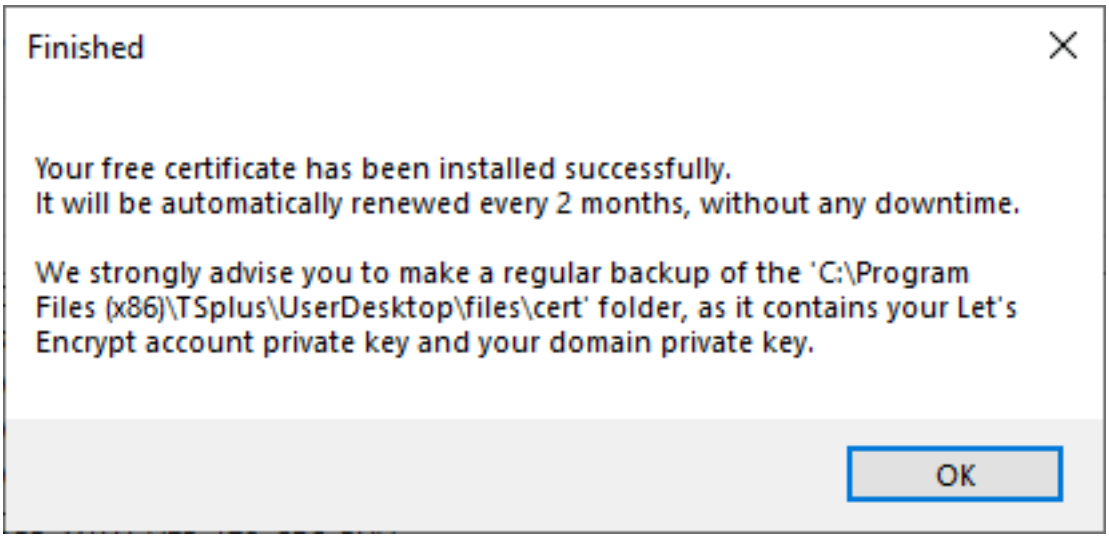
Le certificat sera généré pour ce nom de domaine, et il ne sera valide que sur une page web hébergée à ce nom de domaine. Si vos utilisateurs se connectent à votre Web Portal en utilisant https://server1.example.com:1234 alors, vous devez entrer "server1.example.com".

Étape 3 : Choisissez un algorithme de clé

Il sera utilisé pour créer des paires de clés et effectuer des opérations de signature numérique.



Profitez de votre certificat !



TSplus Free Certificate Manager utilisera désormais toutes les données pour se connecter à Let’s Encrypt, valider que vous possédez réellement le nom de domaine que vous avez saisi et obtenir le certificat valide correspondant.

Une fois que le programme reçoit le certificat, il gérera automatiquement toutes les conversions de format de fichier requises et rechargera doucement le serveur web intégré de TSplus afin d'appliquer le nouveau certificat à chaque nouvelle connexion. Le serveur web est **non**

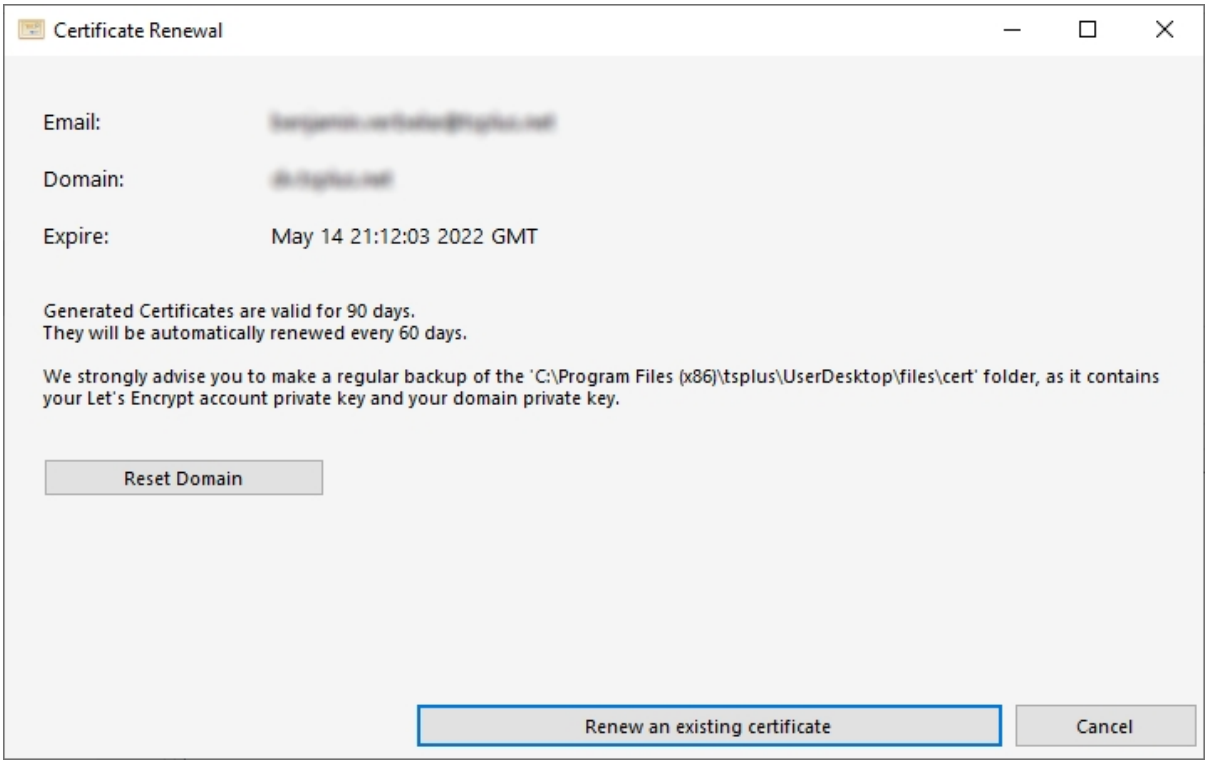
redémarré et aucune connexion n'est arrêtée.

Renouvellement de certificat

Les certificats Let's Encrypt sont valides pendant 90 jours. La période de validité sera réduite de moitié à 45 jours d'ici 2028, tout comme le reste de l'industrie.

TSplus renouvellera automatiquement le certificat tous les 15 jours pour des raisons de sécurité. Un contrôle est effectué à chaque redémarrage du serveur Windows, puis toutes les 24 heures.

Vous pouvez renouveler manuellement votre certificat en ouvrant l'outil Gestionnaire de certificats gratuit. Il affichera le nom de domaine du certificat et sa date d'expiration, comme indiqué dans la capture d'écran ci-dessous.



Pour renouveler manuellement votre certificat, il vous suffit de cliquer sur le bouton « Suivant ».

Le bouton « Réinitialiser le domaine » sur cette fenêtre supprime le certificat SSL et reconfigure le serveur Web à son état d'origine avant d'utiliser le gestionnaire de certificats.

Meilleures pratiques

Si aucune erreur ne se produit, TSplus renouvellera automatiquement le certificat tous les 15 jours. Nous vous recommandons de **vérifiez tous les 45 jours** que votre certificat a été renouvelé automatiquement. Let's Encrypt délivre actuellement des certificats valables 90 jours,

qui seront réduits de moitié à 45 jours d'ici 2028.

Nous vous recommandons également de **sauvegarder au moins une fois par mois** le dossier suivant et ses sous-dossiers :

C:\Program Files (x86)\TSplus\UserDesktop\files.lego

Ceci est un dossier interne, contenant votre clé privée de compte Let’s Encrypt, ainsi que la paire de clés de votre certificat.

Dépannage

En cas d'erreur veuillez contacter le support et leur envoyer le fichier journal suivant :

C:\Program Files (x86)\TSplus\UserDesktop\files.lego\logs\cli.log

Ce fichier journal (et peut-être les autres fichiers journaux dans le même dossier) devrait aider notre équipe de support à enquêter et à mieux comprendre le problème.

Si vous souhaitez restaurer un certificat utilisé précédemment allez dans le dossier :

C:\Program Files (x86)\TSplus\Clients\webserver

Il contiendra tous les fichiers “cert.jks” utilisés. Ce sont les fichiers “key store” et nous ne les supprimons jamais, nous les renommons uniquement avec la date et l'heure de leur désactivation.

Codes d'erreur

- Erreur 801 : le gestionnaire de certificats gratuit n'a pas pu enregistrer votre compte Let's Encrypt. Vérifiez votre connexion Internet. Vérifiez que votre adresse e-mail n'est pas déjà enregistrée chez Let's Encrypt. Réessayez avec une autre adresse e-mail.

- Erreur 802 et Erreur 803 : le Gestionnaire de certificats gratuit n'a pas pu récupérer l'adresse URL des Conditions de service de Let's Encrypt. Il s'agit d'une erreur non bloquante : vous pouvez continuer et accepter les Conditions de service de Let's Encrypt - assurez-vous de les lire d'abord dans votre navigateur, bien sûr.

- Erreur 804 : le gestionnaire de certificats gratuit n'a pas pu valider votre accord avec les conditions de service de Let's Encrypt auprès des serveurs de Let's Encrypt. Vérifiez votre connexion Internet. Réessayez.

- Erreur 805 et Erreur 806 : le Gestionnaire de certificats gratuit n'a pas pu valider que vous possédez le domaine que vous avez saisi lors de la création du certificat (Erreur 805) ou du renouvellement du certificat (Erreur 806). Vérifiez à nouveau tous les prérequis. Vérifiez votre connexion Internet. Vérifiez que votre serveur web écoute sur le port 80. Vérifiez que vous n'utilisez pas un serveur web tiers tel qu'IIS ou Apache. Vérifiez que votre nom de domaine est accessible depuis Internet.

Commande de certificat HTTPS

Préparation du fichier de configuration du certificat

À l'intérieur du dossier “C:\Program Files (x86)\TSplus\UserDesktop\files\cert”, créez un fichier nommé “FreeCertificateManager.ini” s'il n'existe pas déjà. Assurez-vous que votre éditeur de texte et/ou l'explorateur de fichiers Windows n'ajoute pas d'extension “.txt” à la fin.

Modifiez le fichier et écrivez ou mettez-le à jour afin qu'il ait le format suivant, puis enregistrez-le :

paramètres

email = your.email@company.com

domaine = votre-serveur-nom-de-domaine.entreprise.com

Créer le certificat

En tant qu'administrateur de serveur, exécutez la commande suivante :

C:\Program Files (x86)\TSplus\UserDesktop\files\cert\CertificateManager.exe /create

Pour que cette commande soit réussie :

- Le fichier “FreeCertificateManager.ini” doit exister et utiliser le format attendu
- Votre serveur TSplus Remote Access doit être opérationnel.
- Votre portail Web TSplus Remote Access doit être disponible avec le protocole

HTTP sur le port 80 du réseau public Internet, car le fournisseur de certificat HTTPS de TSplus l'utilisera pour valider le nom de domaine du serveur.

Renouveler le certificat

Une fois le certificat configuré et créé, TSplus Remote Access le renouvellera automatiquement tous les deux mois pour s'assurer qu'il n'expire jamais.

Ajouter un certificat tiers

À l'intérieur du dossier “C:\Program Files (x86)\TSplus\UserDesktop\files\cert”, créez un fichier nommé “certpassword.txt” contenant uniquement le mot de passe du certificat. En tant qu'administrateur du serveur, exécutez la commande suivante :

C:\Program Files (x86)\TSplus\UserDesktop\files\cert\CertificateManager.exe /add "your-certificate-path"

Si vous utilisez TSplus Advanced Security, vous devrez peut-être désactiver temporairement la fonction de protection géographique pour qu'elle fonctionne. Vous pouvez supprimer votre fichier de mot de passe après avoir exécuté la commande.

Prévenir l'accès RDP et autoriser HTTP sur le serveur Gateway

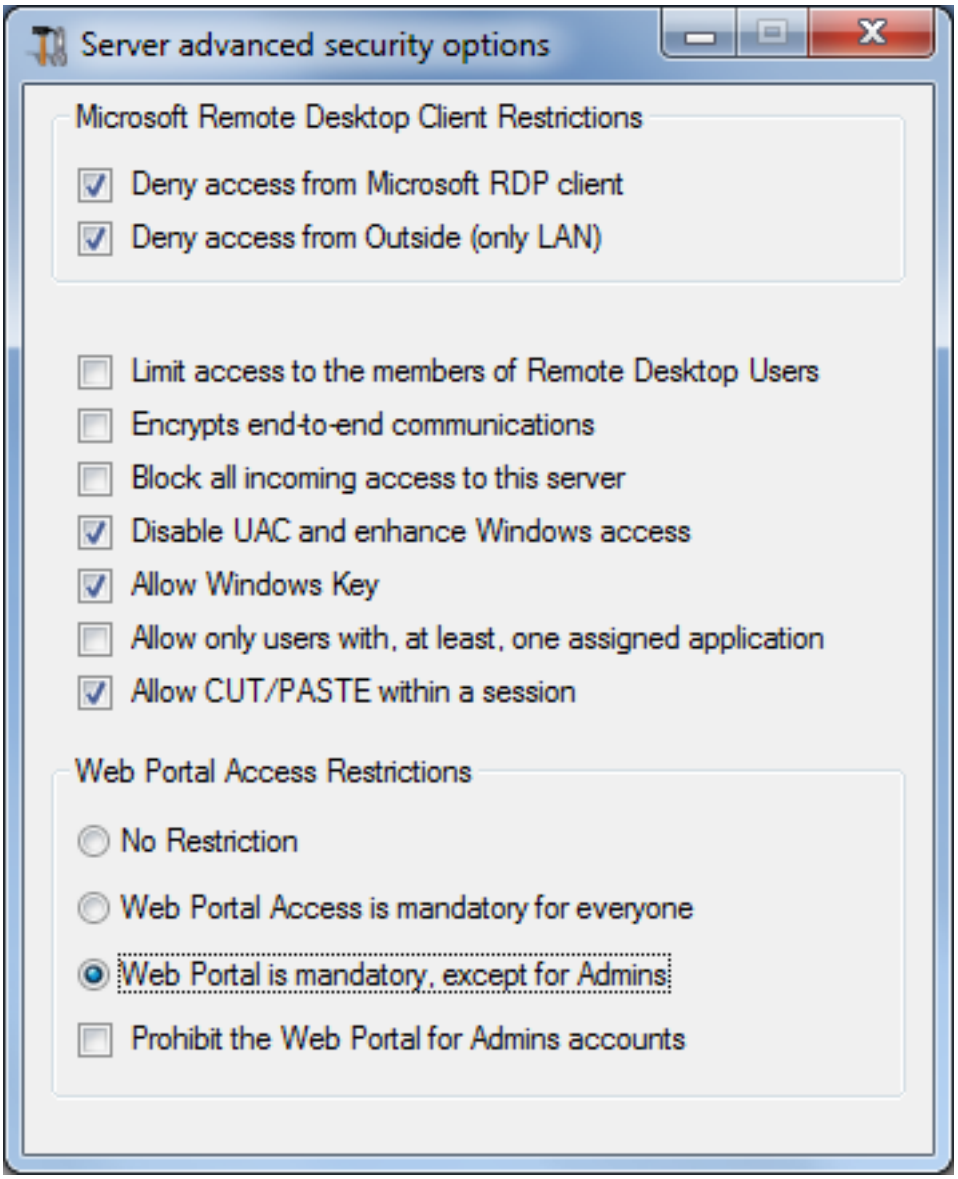
Il existe 2 façons d'accéder au serveur Gateway :

- HTML5 / HTML
- Session RDP (via l'IP/DNS de la passerelle – numéro de port)

Comment VERROUILLER HTML/HTML5

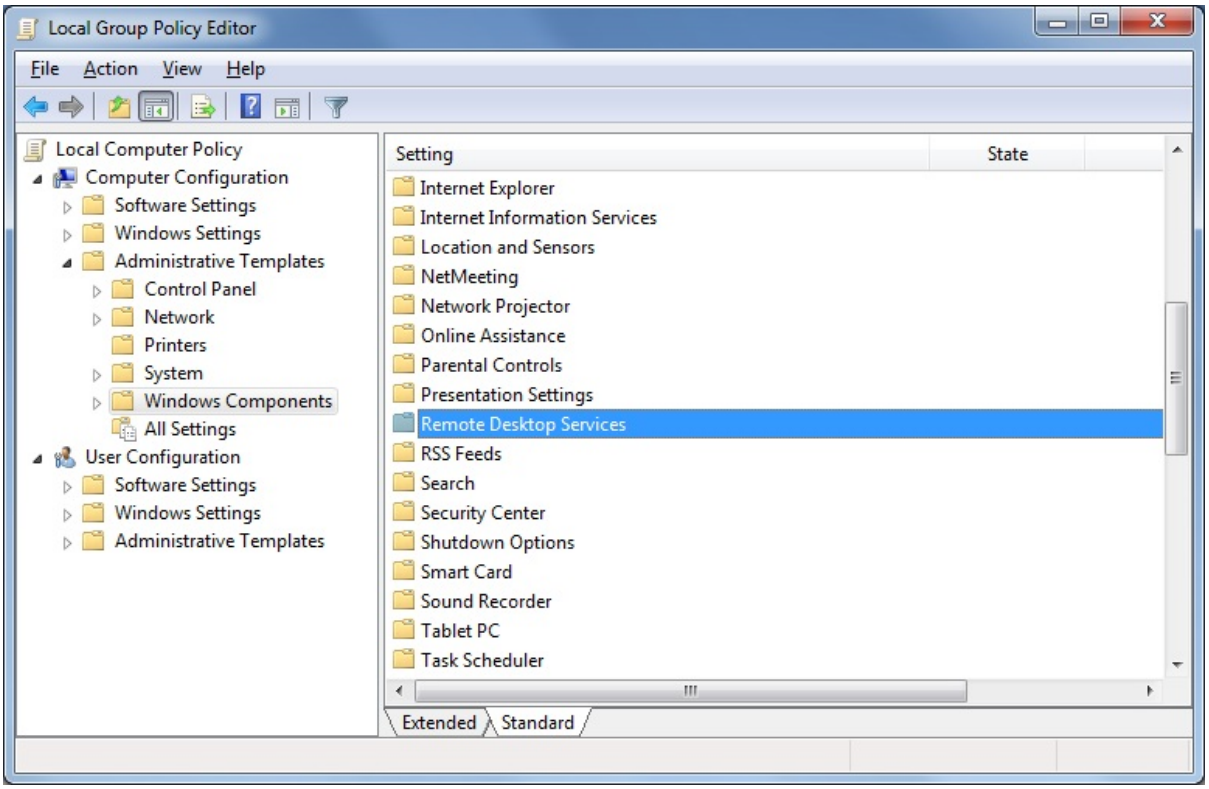
Nous pouvons utiliser mstsc avec un numéro de PORT et RDP dans un serveur d'application / passerelle TSplus.

Cependant, si nous utilisons ces outils de sécurité avancés situés dans la console d'administration TSplus sur le serveur Gateway, en allant sur le carreau/l'onglet Sécurité, puis en cliquant sur le carreau des options de sécurité avancées…

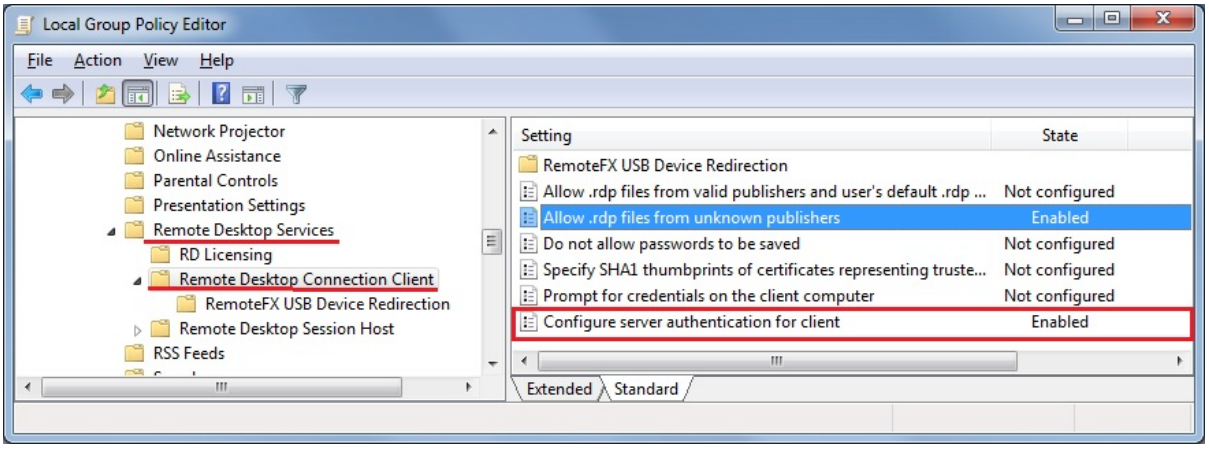


…l'accès est refusé lors de la tentative de connexion avec RDP. Pour éviter ce comportement, sur le serveur Gateway, vous devrez faire ce qui suit :

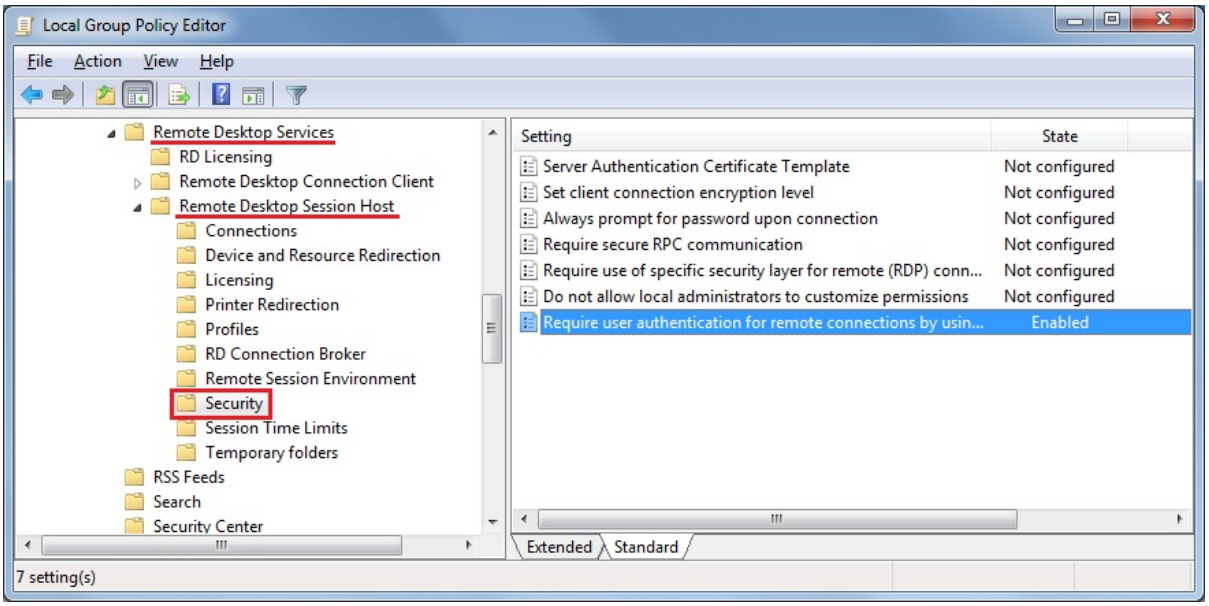
- Allez dans Gpedit.msc, puis sous Configuration de l'ordinateur, cliquez sur le dossier Modèles d'administration, sur le dossier Composants Windows et sur Services de bureau à distance :



- Ensuite, cliquez sur le dossier Client de connexion Bureau à distance, double-cliquez sur le paramètre « Autoriser les fichiers .rdp provenant d'éditeurs inconnus » et activez-le, ainsi que sur « Configurer l'authentification du serveur pour le client » :



- Sous le menu Client de Bureau à Distance, cliquez sur le dossier Hôte de Session Bureau à Distance, puis sur le dossier Sécurité. Activez le paramètre « Exiger l'authentification de l'utilisateur pour les connexions à distance en utilisant l'authentification au niveau du réseau ».

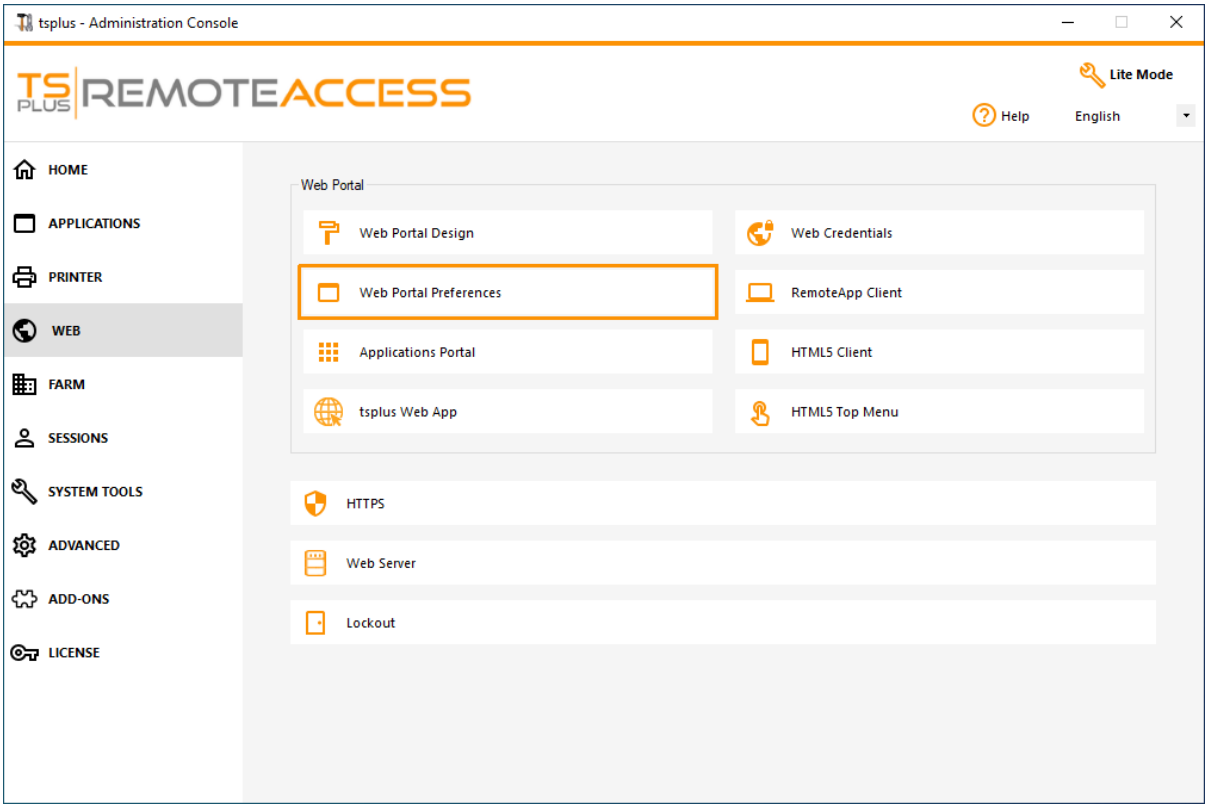

Local Group Policy Editor
File Action View Help
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment
Security
Session Time Limits
Temporary folders
RSS Feeds
Search
Security Center
Setting
State
Server Authentication Certificate Template
Not configured
Set client connection encryption level
Not configured
Always prompt for password upon connection
Not configured
Require secure RPC communication
Not configured
Require use of specific security layer for remote (RDP) conn...
Not configured
Do not allow local administrators to customize permissions
Not configured
Require user authentication for remote connections by usin...
Enabled
Extended
Standard
7 setting(s)

Activer/désactiver manuellement le serveur Gateway

Aperçu

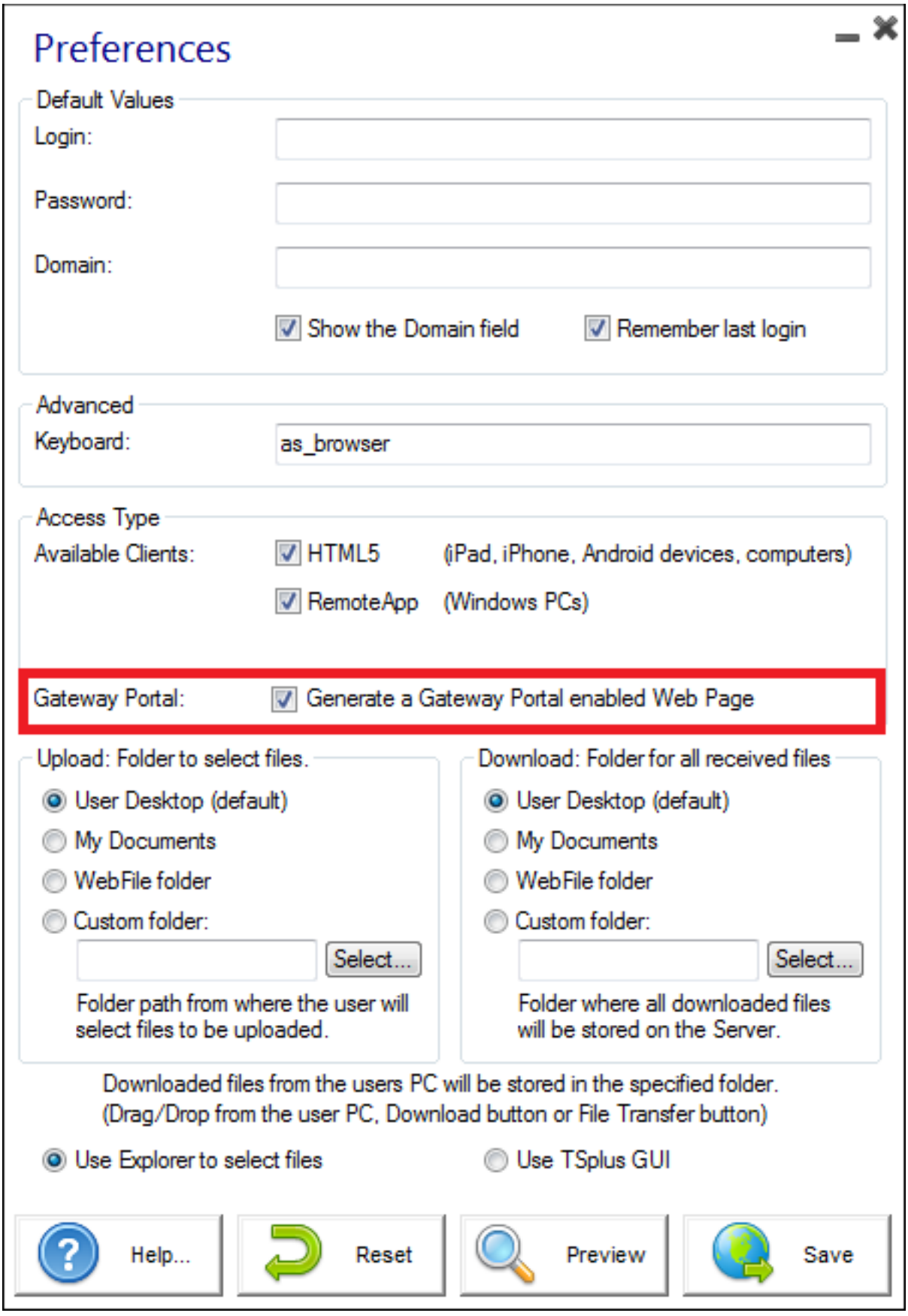
En fonction de la configuration de votre ferme, le contrôleur de ferme changera automatiquement ses propres paramètres de portail Web pour devenir un serveur passerelle. permettant aux utilisateurs de se connecter depuis le portail Web TSplus du contrôleur de ferme, de ne pas se connecter directement au contrôleur de ferme lui-même, mais à l'un des serveurs d'application de la ferme.

Cependant, si vous souhaitez modifier ce comportement manuellement, vous pouvez le faire en cliquant sur la tuile “WEB”, puis sur le bouton Préférences du portail Web.



- Cochez la case « Générer une page Web activée pour le portail Gateway » si vous souhaitez

que le portail Gateway du contrôleur de ferme (le serveur actuel que vous configurez maintenant) devienne un serveur Gateway et redirige les utilisateurs vers les serveurs d'application de la ferme.
- Décochez la case « Générer une page Web activée pour le portail Gateway » si vous souhaitez que le portail Gateway du contrôleur de ferme redirige vers le contrôleur de ferme lui-même, contournant ainsi toute configuration de ferme.



Cliquez sur « Enregistrer » pour sauvegarder ce paramètre.

Identifiant matériel et serveur cloné

1- Changement d'identifiant matériel.

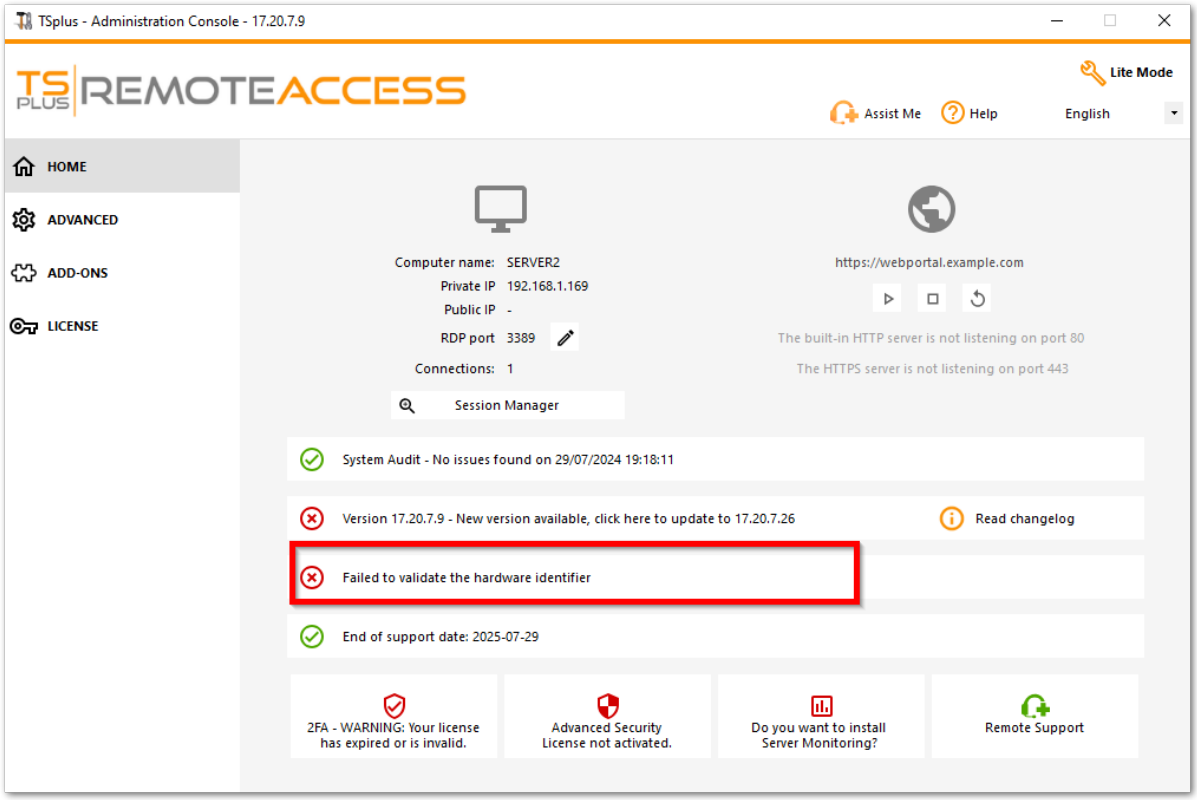
Réparation de l'identifiant matériel suite à un clonage ou une mise à jour.

Avertissement : Échec de la validation de l'identifiant matériel

Après avoir migré un serveur physique vers une machine virtuelle ou après une mise à jour du noyau Microsoft, l'état de la licence change en Échec de validation de l'identifiant matériel sur le nouveau matériel.

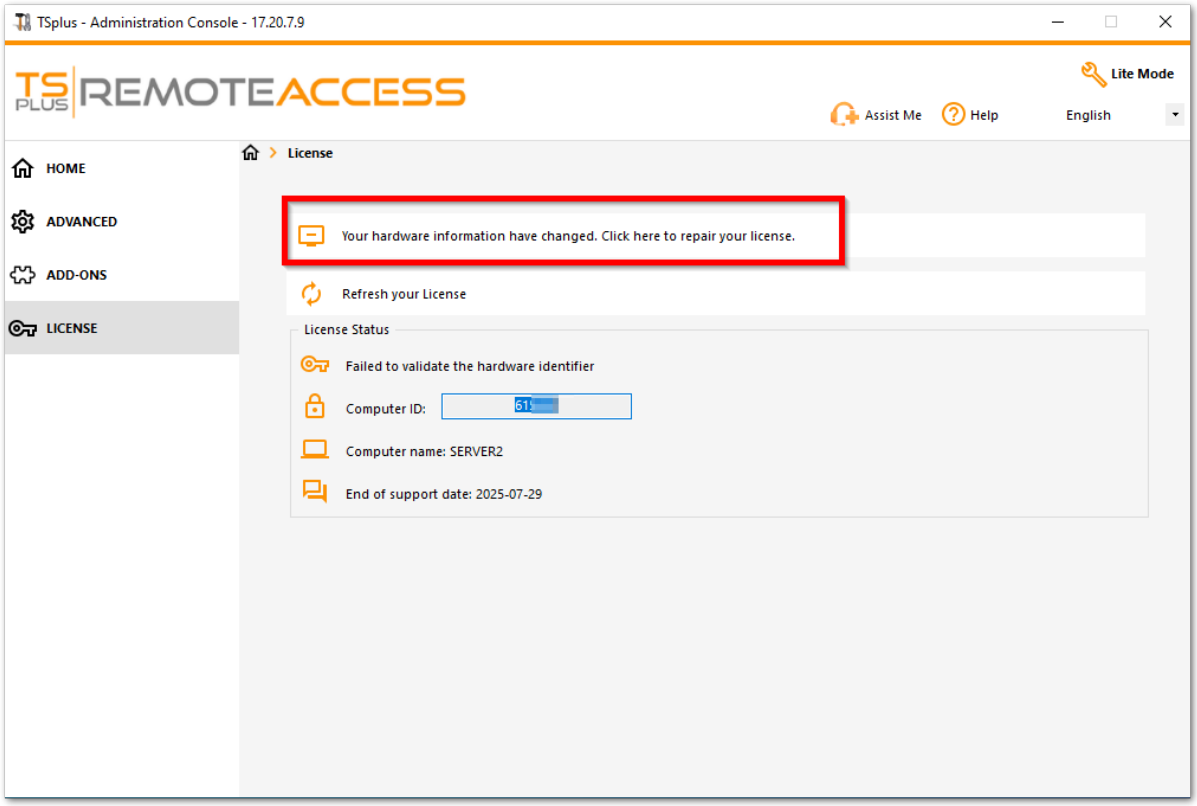
Ce message apparaît car TSplus a détecté un conflit de licence copié d'un serveur à un autre avec le même ID d'ordinateur et le même nom.
Nous vous recommandons déjà de renommer votre nouveau serveur (Exemple : SERVEUR1 > SERVEUR2)

- Redémarrez votre serveur



Cliquez sur la fenêtre pour accéder à la page de licence.

Puis cliquez sur l'onglet « Votre information matérielle a changé. Cliquez ici pour réparer votre licence.



Une fenêtre contextuelle de "réhébergement de licence" s'ouvrira pour vous permettre de restaurer votre licence.

Cas 1 : Vous n'avez pas de support !
Le rehosting ne sera donc pas possible, vous devrez souscrire à un abonnement de support sur le serveur d'origine et recommencer l'action de migration.
En cas de problèmes, Contactez le support et indiquez votre identifiant d'ordinateur et votre clé d'activation.

Cas 2 : Vous avez déjà rehosté pendant 6 mois !
Le message : Vous avez déjà réhébergé cet ordinateur au cours des 6 derniers mois. Veuillez contacter le support si vous avez besoin d'aide pour réhéberger votre licence.

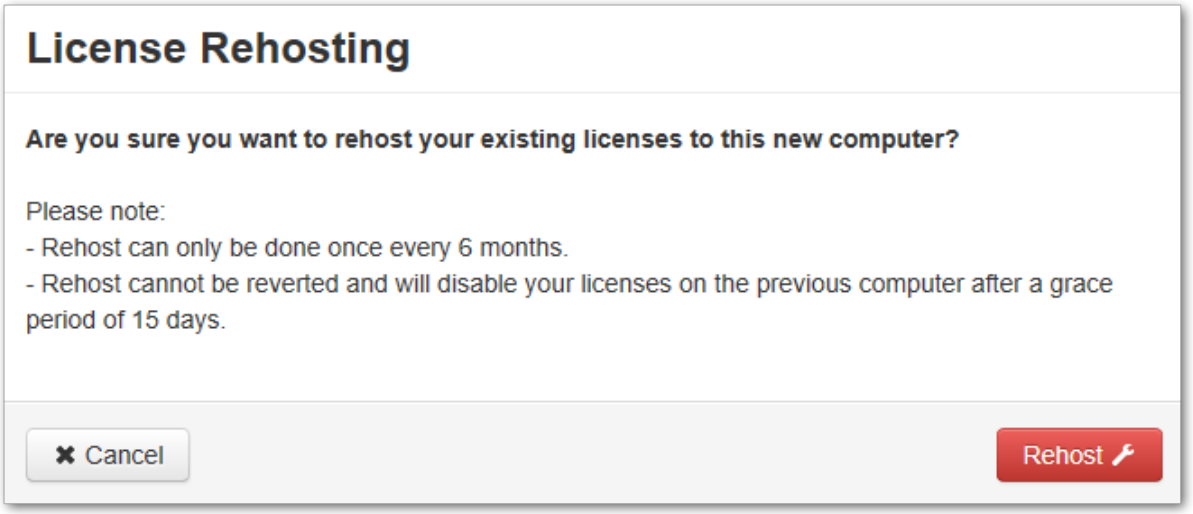
Le rehosting ne sera donc pas possible, Contactez le support et indiquez votre ID d'ordinateur et votre clé d'activation.

Cas 3 : Vous avez du support !
Le message suivant apparaît : Êtes-vous sûr de vouloir réhéberger vos licences existantes sur cet nouvel ordinateur ?

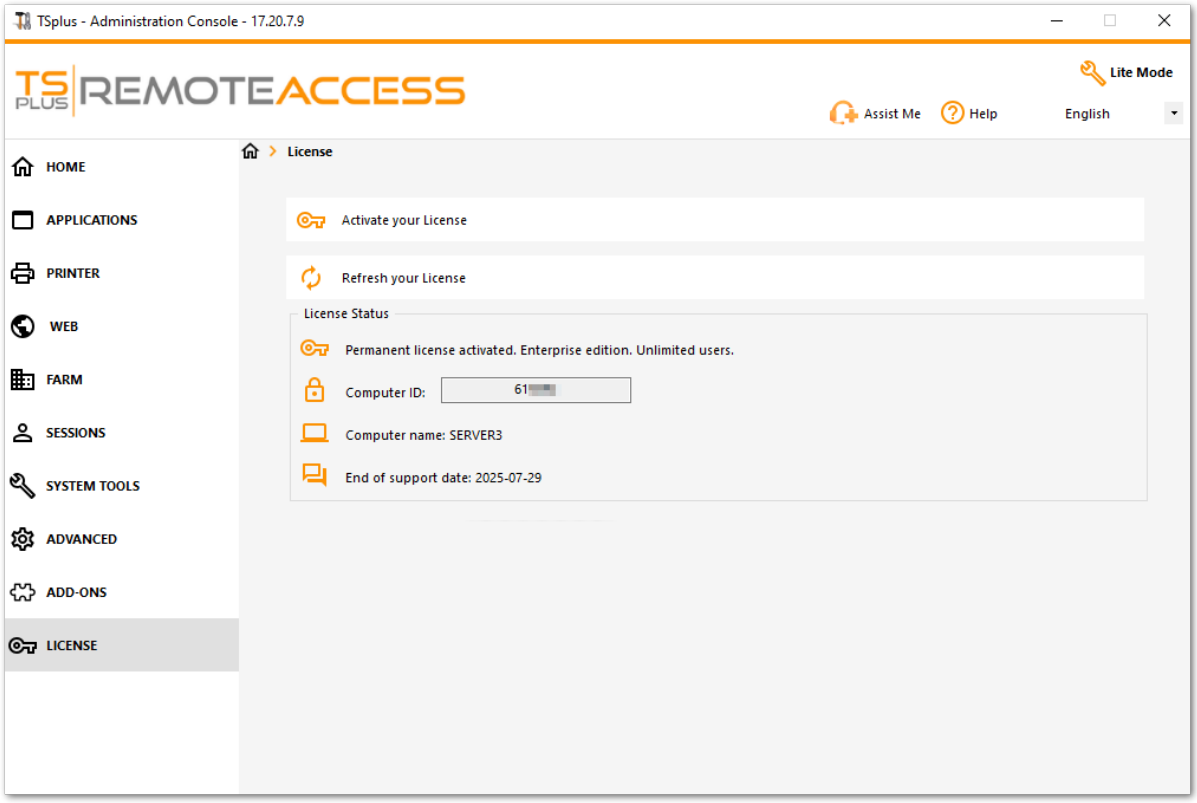
Veuillez noter :

- Le rehosting ne peut être effectué qu'une fois tous les 6 mois.
- Le rehosting ne peut pas être annulé et désactivera vos licences sur l'ordinateur précédent après une période de grâce de 15 jours.

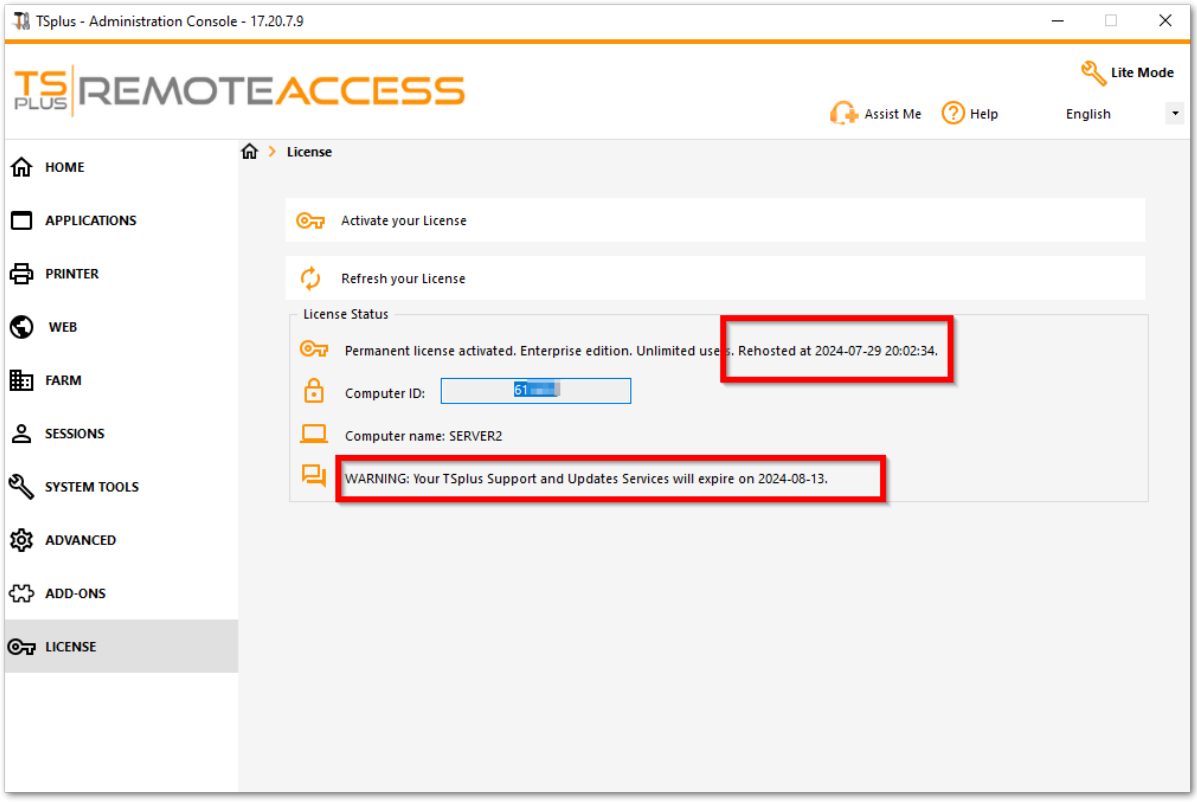
Cliquez sur le **REHOST** bouton



Votre licence est réhébergée !



Note : Un message apparaîtra sur l'ancien serveur avec la date de réhébergement ainsi que la date de fin de la période d'utilisation de l'ancien serveur (15 jours).



Échec de la mise à jour :

Exécutez la mise à jour et vérifiez si cela a résolu votre problème après avoir redémarré votre serveur.

- Télécharger le Mise à jour de la version

2- Cloner un serveur tout en conservant le serveur existant et en activant une nouvelle licence.

Exigences

Lors de l'utilisation de machines virtuelles clonées, il est important de modifier le nom de l'ordinateur et l'ID du volume disque pour garantir une installation unique de TSplus Remote Access et éviter les problèmes de licence.

Considérations sur le nom de l'ordinateur

Le nom de l'ordinateur est stocké dans le registre Windows à l'intérieur de l'image elle-même. S'il est modifié avant d'appliquer l'image, il sera écrasé par Sysprep lorsque Windows démarrera. Cependant, vous pouvez prédéfinir un nom dans un Unattended.xml Fichier de réponse. Voir Documentation Microsoft pour plus de détails.

Pour définir le nom de l'ordinateur, ajoutez la section suivante à l'intérieur Microsoft-Windows-Shell-Setup :

```
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <ComputerName>%COMPUTERNAME%ComputerName>
component>
```

Considérations sur l'ID de volume

L'ID de volume est associé à la partition de disque, pas à l'image du système d'exploitation. Il peut être modifié avant d'appliquer l'image, et il persistera. Utilisez `volumeid.exe` de Sysinternals, disponible à Microsoft Sysinternals avant que Windows ne démarre.

Étapes de déploiement

Lors du déploiement d'une nouvelle machine virtuelle à partir d'une image syspreppée, Windows entrera dans l'expérience Out-Of-Box (OOBE) au premier démarrage, demandant des paramètres de configuration.

Étapes recommandées pour le déploiement :

1. **Démarrer sur WinPE** – Préparez le système sans démarrer sous Windows.
2. **Définir l'ID de volume** – Modifiez-le avant d'appliquer l'image afin qu'il persiste.
3. **Déployer l'image syspreppée** – Utilisez DISM pour appliquer l'image à `C:\`.
4. **Définir le nom de l'ordinateur hors ligne** – Modifier le registre à l'intérieur de l'image montée.
5. **Copier un `Unattended.xml` fichier** – Automatisez la configuration OOBE. Ce fichier peut être modifié dynamiquement avant le déploiement à l'aide d'un script.
6. **Créer un script de premier démarrage** – Assurez-vous des configurations finales avec un seul redémarrage.
7. **Redémarrer sous Windows** – Windows se finalise en utilisant les configurations spécifiées.
8. **Réinitialiser la licence d'accès à distance** – Exécutez la commande suivante :

Fenêtre de terminal

```
AdminTool.exe /license /reset
```

Cela réinitialise la licence et applique une nouvelle licence.

Script de déploiement

Veuillez trouver ci-dessous le script de déploiement WinPE associé.

Fenêtre de terminal

```
<# Define variables #>
$ImagePath = "D:\Images\Windows.wim"   # Path to your sysprepped image
$ApplyDrive = "C:"                     # Target drive for deployment
$ComputerName = "REMOTE ACCESS-SERVER-" + (Get-Random -Minimum 1000 -
Maximum 9999)  # Generate a random name (naive implementation)
$VolumeID = "1234-ABCD"                # Desired Volume Serial Number
$UnattendFile = "D:\Unattended.xml"    # Path to the unattended answer file

Write-Host "=== Windows Deployment Automation ==="

<# 1. Set Volume ID before applying the image #>
Write-Host "Setting Volume ID..."
Start-Process -NoNewWindow -Wait -FilePath "volumeid.exe" -ArgumentList "$ApplyDrive
$VolumeID"

<# 2. Apply the Sysprepped Windows image #>
Write-Host "Applying Windows Image..."
dism /apply-image /imagefile:$ImagePath /index:1 /applydir:$ApplyDrive

<# 3. Load Registry Offline to Set Computer Name #>
Write-Host "Modifying Registry to Set Computer Name..."
reg load HKLM\TempSys $ApplyDrive\Windows\System32\Config\SYSTEM
reg add "HKLM\TempSys\ControlSet001\Control\ComputerName\ComputerName" /v
ComputerName /t REG_SZ /d "$ComputerName" /f
reg unload HKLM\TempSys

<# 4. Ensure Unattended Setup is Used #>
Write-Host "Copying Unattended File..."
Copy-Item -Path $UnattendFile -Destination "$ApplyDrive\Windows\Panther\Unattended.xml" -
Force

<# 5. Set the First Boot Script for Final Configurations #>
Write-Host "Creating First Boot Script..."
$FirstBootScript = @"
Write-Host "Finalizing Configuration..."
Rename-Computer -NewName "$ComputerName" -Force
```

```
    Restart-Computer -Force
    "@
    Set-Content -Path "$ApplyDrive\Windows\Setup\Scripts\SetupComplete.cmd" -Value
$FirstBootScript -Encoding ASCII

    Write-Host "Deployment Complete! Rebooting into Windows..."
    Write-Host "================================================"
    Write-Host "  Computer Name: $ComputerName"
    Write-Host "  Volume ID: $VolumeID"
    Write-Host "  Image Applied to: $ApplyDrive"
    Write-Host "================================================"

    <# Reboot into Windows #>
    wpeutil reboot
```

Activation de la licence

Après le déploiement, l'activation d'une licence générera un nouvel ID d'ordinateur pour la machine virtuelle. Cet ID d'ordinateur est créé par le portail de licence lorsqu'une machine demande une activation d'essai ou de licence. Pour les machines virtuelles clonées, l'activation de la licence est obligatoire. Utilisez soit une clé d'activation, soit une clé de licence en volume. **Les configurations hors ligne ne sont pas autorisées** en raison de préoccupations en matière de sécurité. Pour des étapes d'activation détaillées, reportez-vous à Liste des commandes TSplus .

Conclusion

Ce guide décrit les considérations clés pour déployer des machines virtuelles clonées avec TSplus Remote Access. Il fournit des étapes essentielles pour configurer et licencier le système correctement et doit être adapté à vos besoins et exigences.

Comment faire : Lier le serveur Web à plusieurs cartes réseau

Aperçu

Certains cas d'utilisation peuvent nécessiter que le serveur web Terminal Service Plus écoute sur plus d'une carte réseau, par exemple si le serveur appartient à plusieurs réseaux différents.

Cette fonctionnalité répond à ce besoin spécifique.

Liaison du serveur Web à plusieurs cartes réseau

Pour lier le serveur web Terminal Service Plus à plusieurs cartes réseau, vous devez :

- Créez le fichier “settings.bin” dans le dossier “C:\Program Files (x86)\TSplus\Clients\webserver”
- Ajoutez la ligne suivante avec toutes les adresses IP locales pour toutes les cartes réseau que vous souhaitez lier, par exemple :

  bind_nic=“127.0.0.3”,“127.0.0.4”
- Redémarrez le serveur web (AdminTool > Web > Redémarrer les serveurs web) pour appliquer les modifications

Le serveur web de Terminal Service Plus écoutera désormais toutes les requêtes provenant de toutes les cartes réseau liées (dans notre exemple, la liaison serait effectuée automatiquement sur 127.0.0.3, 127.0.0.4 et 127.0.0.1).

Comment faire : ajouter un en-tête HTTP personnalisé

Prérequis

Cette fonctionnalité est très technique et cette documentation est uniquement destinée aux experts techniques.

Vous devriez être familiarisé avec le protocole HTTP ainsi que les en-têtes HTTP.

Aperçu

Certains cas d'utilisation peuvent nécessiter que le serveur web Terminal Service Plus renvoie un ou plusieurs en-têtes HTTP personnalisés en plus des en-têtes standard.

Cette fonctionnalité répond à ce besoin spécifique.

Configurer un en-tête HTTP personnalisé

Pour ajouter votre propre en-tête HTTP personnalisé, vous devez :

- Créer le fichier “headers.bin” dans le dossier “C:\Program Files (x86)\TSplus\Clients\webserver”
- Ajoutez les en-têtes personnalisés séparés par une nouvelle ligne, par exemple : en-tête1=X-Frame-Options
- Redémarrez le serveur web (AdminTool > Web > Redémarrer les serveurs web) pour appliquer les modifications

Le serveur Terminal Service Plus répondra désormais à toutes les requêtes avec cet en-tête HTTP personnalisé en plus des en-têtes standard.

Pages HTML et personnalisation

Vous pouvez modifier les pages HTML fournies avec Notepad ou Notepad++ pour personnaliser l'interface utilisateur.

page index.html

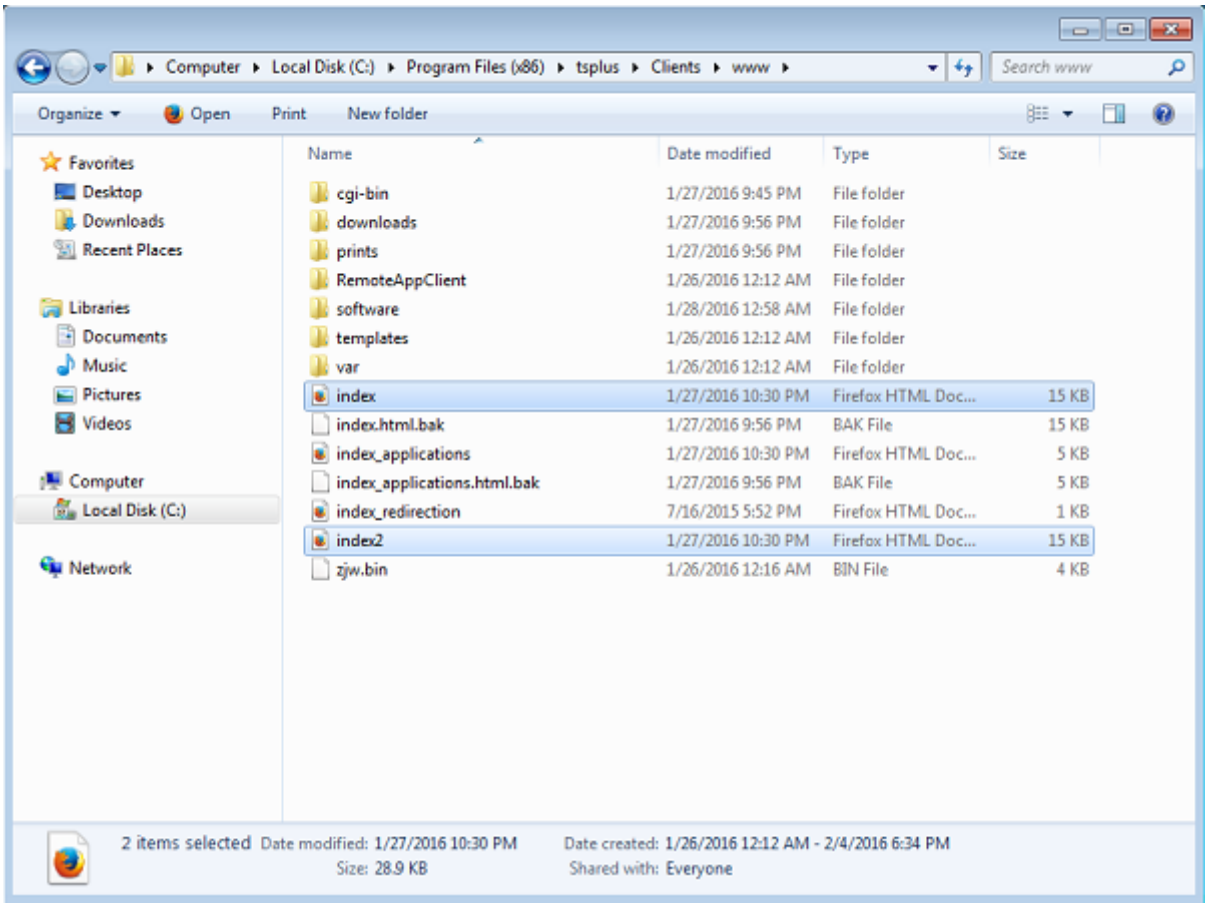
Le fichier index.html se trouve dans le chemin du dossier racine du serveur Web.

C:\Program Files (x86)\TSplus\Clients\www

La page Index.html est la page web par défaut. C'est comme une page de portail frontale avec des liens vers les pages de connexion qui se trouvent dans le dossier \www\.

Cette page web peut être copiée et renommée pour permettre plusieurs configurations et / ou informations de connexion.

Par exemple, copions et renommons index.html en index2.html, cette page sera disponible en utilisant cette URL. http://localhost/index2.html



Attention, si vous changez le nom du fichier "index.html" en "index2.html" et que vous utilisez le Portail des Applications Web, vous devez alors modifier la variable suivante dans ce fichier : "page_configuration["applications_portal"] = "index_applications.html" en "index2_applications.html", puis renommer le fichier "index_applications.html" en "index_2applications.html".

Le fichier index.html par défaut inclut toutes les options possibles :

- Accès RemoteApp aux applications, connexion en dehors du navigateur Web
- Connexion utilisant HTML5 depuis n'importe quel appareil
- Préférences d'impression locales

Vous pourrez modifier l'en-tête et le pied de page dans la fonctionnalité de conception du portail Web sur le carrelage des préférences du portail Web de l'onglet Web.

En modifiant la page web index.html, vous aurez accès à divers paramètres.

// ---------- Configuration d'accès ----------

var user = ""; // Identifiant à utiliser lors de la connexion au serveur distant (laisser "" pour utiliser l'identifiant saisi sur cette page)

var pass = ""; // Mot de passe à utiliser lors de la connexion au serveur distant (laisser "" pour utiliser le mot de passe saisi sur cette page)

var domain = ""; // Domaine à utiliser lors de la connexion au serveur distant (laisser "" pour utiliser le domaine saisi sur cette page)

var server = "127.0.0.1"; // Serveur auquel se connecter (laisser "" pour utiliser localhost et/ou le serveur choisi sur cette page)

var port = ""; // Port à utiliser pour se connecter (laisser "" pour utiliser localhost et/ou le port du serveur choisi sur cette page)

var lang = "as_browser"; // Langue à utiliser

var serverhtml5 = “127.0.0.1”; // Serveur auquel se connecter lors de l'utilisation du client HTML5

var porthtml5 = “3389”; // Port à utiliser pour se connecter lors de l'utilisation du client HTML5

var cmdline = ""; // Texte optionnel qui sera mis dans le presse-papiers du serveur une fois connecté

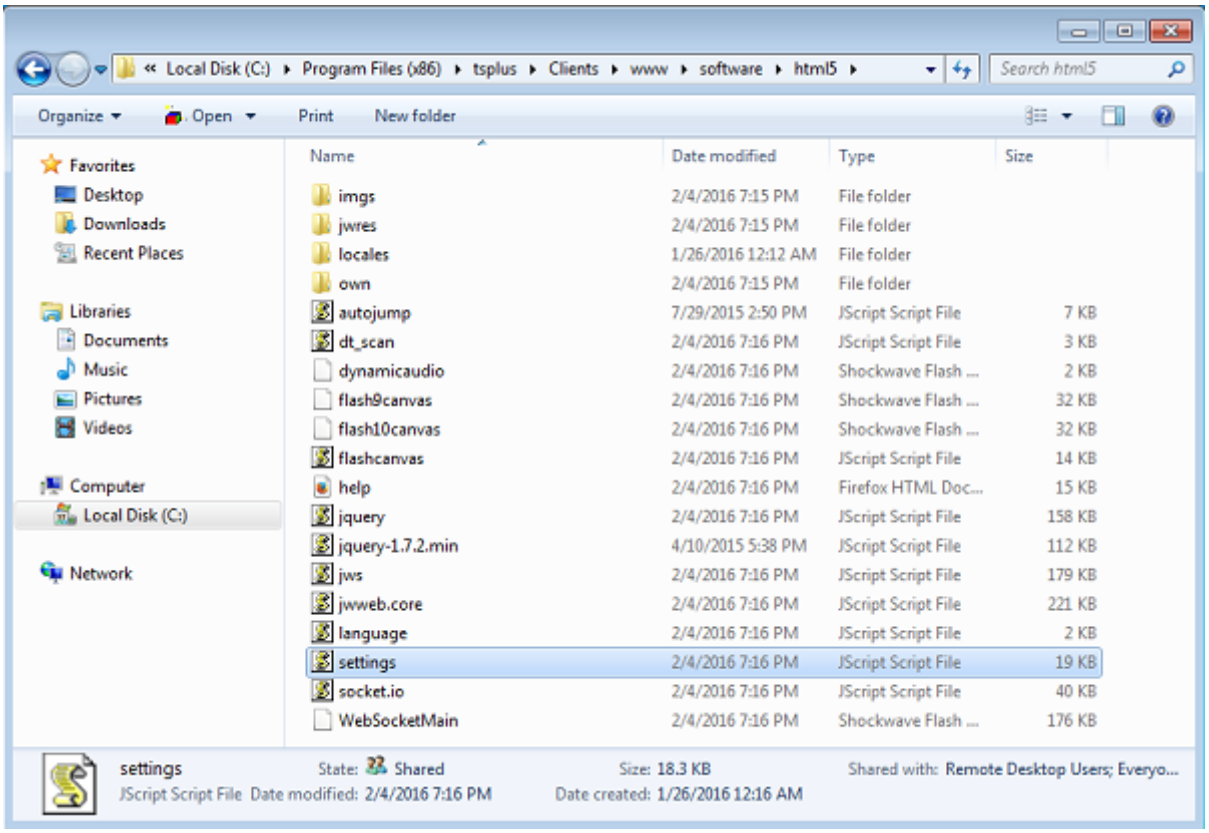
// ---------- Fin de la configuration d'accès ----------

Par exemple, je vais définir démo/Mdp comme identifiant/mot de passe en modifiant :

var user = "Démo"; var pass = "Psw";

En faisant cela, les identifiants pré-remplis sont rendus visibles à chaque visite du portail.

Un autre fichier de configuration très important est **settings.js** situé dans C:\Program Files (x86)\TSplus\Clients\www\software\html5:



Ce fichier contient divers paramètres pour le client web HTML5, tels que la désactivation du son, du presse-papiers ou l'autorisation de la reconnexion de session si l'onglet du navigateur est fermé.

- Désactivation du presse-papiers :

W.clipboard = "oui"; //ou "non"

- Désactiver le son se fait avec ce paramètre :

W.playsound = false;

- Changer la résolution par défaut pour les appareils mobiles :

W.viewportwidth = "1024" - La hauteur est calculée par le navigateur.

- Forcer HTTPS pour la connexion à distance

W.forcealways_ssl = true;

- Autoriser la reconnexion de session lorsque l'onglet du navigateur est fermé :

W.send_logoff = false;

- Ajouter une fenêtre d'avertissement pour empêcher la fermeture de l'onglet du navigateur :

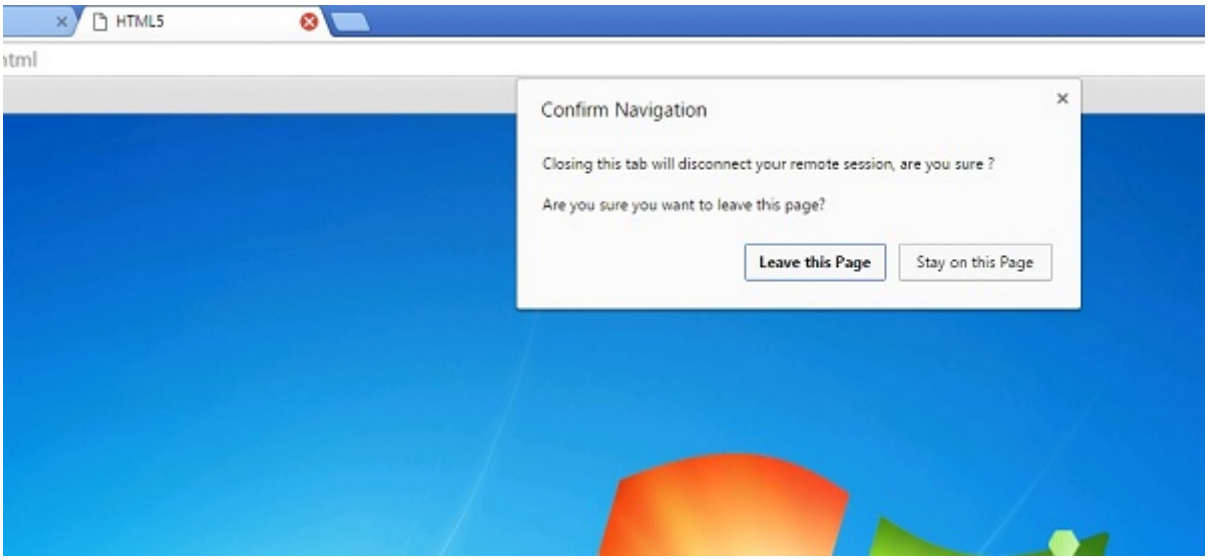
recherchez le paramètre “W.pageUnloadMessage = "" ”.

J'ai défini un exemple de message à utiliser ci-dessous :

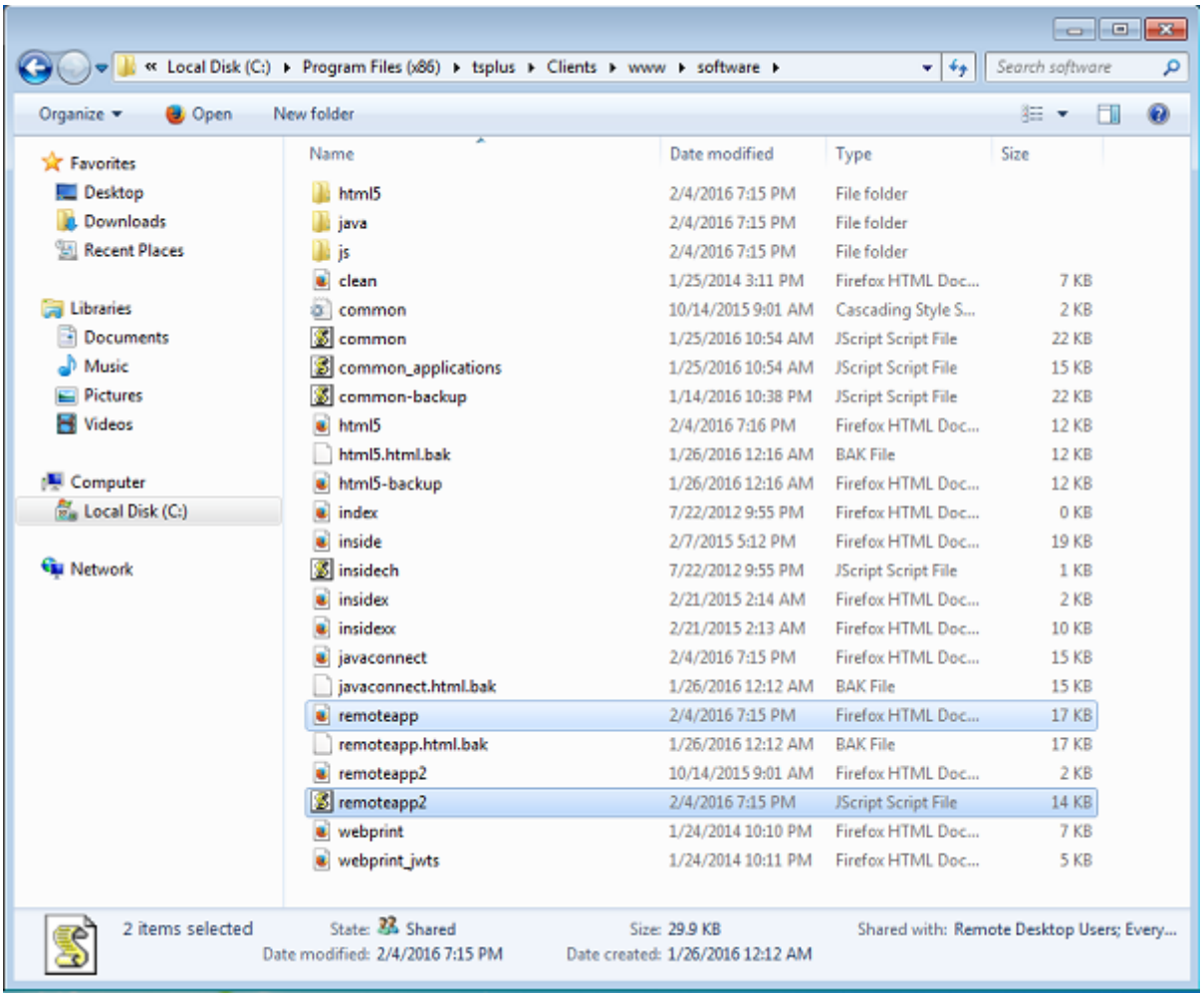
W.pageUnloadMessage = “Fermer cet onglet déconnectera votre session à distance, êtes-vous sûr ?”; //Dialog to return when page unloads.

//1. Avis important, les dialogues propres ne sont pas pris en charge dans tous les navigateurs.

//2. La norme HTML ne fait pas de distinction entre l'actualisation de la page et l'action de fermeture de la page, la boîte de dialogue apparaîtra également lors de l'actualisation de la page.



Les paramètres généraux de la page web RemoteApp sont stockés dans le dossier du logiciel, dans deux fichiers différents : **remoteapp.html** et **remoteapp2.js** .



Exemple des paramètres disponibles présents dans **remoteapp2.js** :

// Serveur de Bureau à Distance

var remoteapp2_server = ”; var remoteapp2_port = ‘443’;

// Authentification Windows

var remoteapp2_user = ”; var remoteapp2_psw = ”; var remoteapp2_domain = ”;

// Paramètres de ligne de commande optionnels

var remoteapp2_apppath = ”;

// Mode RemoteApp

var remoteapp2_wallp = 'vert'; var remoteapp2_remoteapp = 'activé';

// Écran

var remoteapp2_color = '32';

```
var remoteapp2_full = '2';

var remoteapp2_width = ”;

var remoteapp2_height = ”;

var remoteapp2_scale = '100';

var remoteapp2_smartsizing = '1';

var remoteapp2_dualscreen = 'désactivé';

var remoteapp2_span = 'désactivé';

// Mappage des disques (nécessaire pour l'impression)

var remoteapp2_disk = '1';

// Impression

var remoteapp2_printer = 'désactivé';

var remoteapp2_preview = 'off';

var remoteapp2_default = 'on';

var remoteapp2_select = 'off';

// Matériel

var remoteapp2_com = '0';

var remoteapp2_smartcard = '0';

var remoteapp2_serial = 'off';

var remoteapp2_usb = 'off';

var remoteapp2_sound = 'on';

var remoteapp2_directx = 'off';

// Divers

var remoteapp2_alttab = '0';

var remoteapp2_firewall = '1';
```

```
var remoteapp2_localtb = ‘32’;

var remoteapp2_lock = 'off';

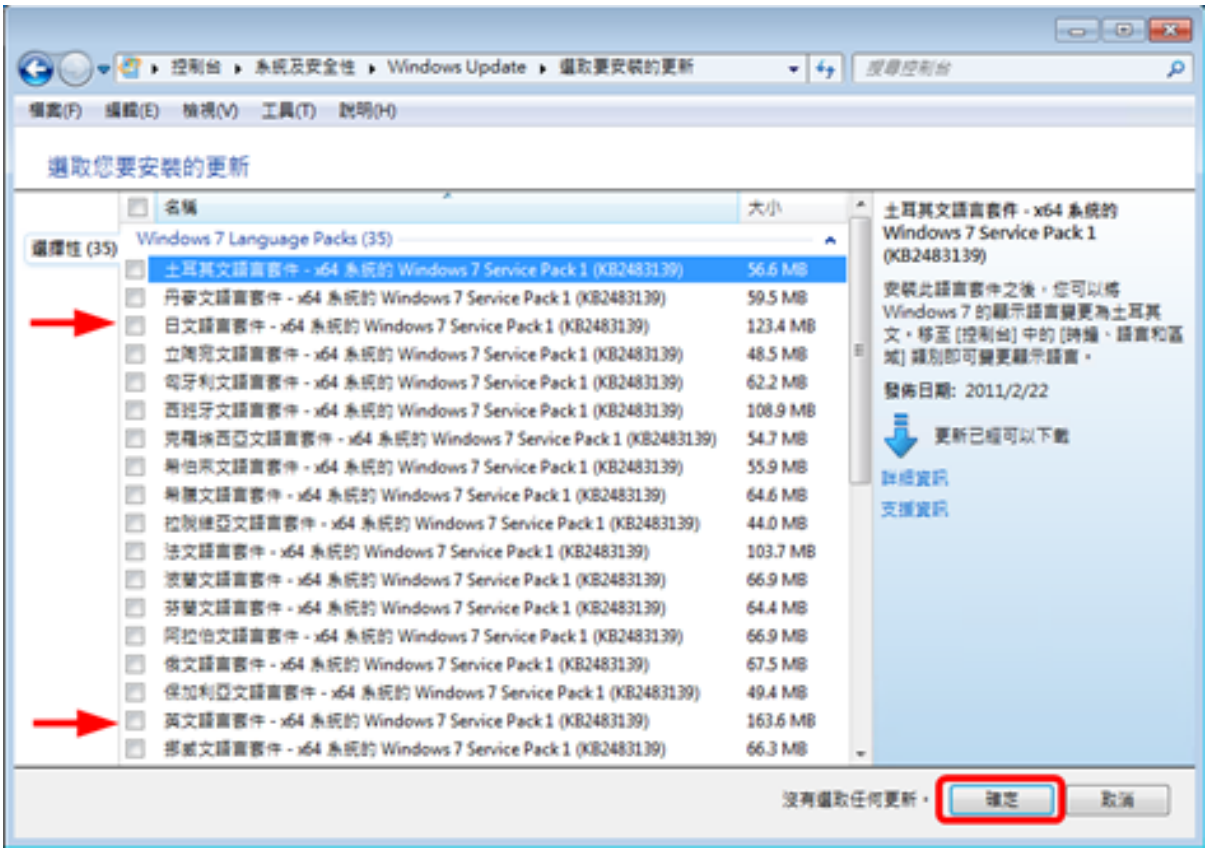
var remoteapp2_rdp5 = 'désactivé';

var remoteapp2_reset = 'off';
```

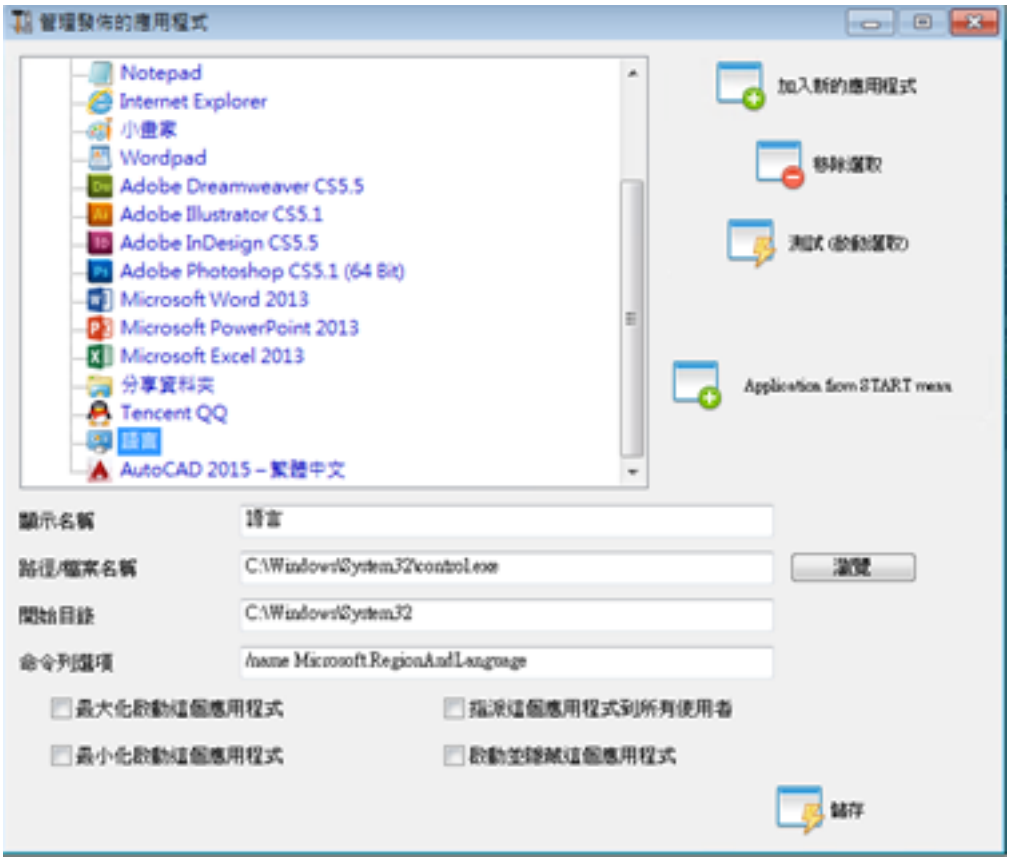
HTML5 : Changer la langue en chinois

Vous avez besoin de Windows 7 Enterprise ou Ultimate / Windows 8 Enterprise ou Professional pour utiliser plusieurs langues sur un seul système.

Vous pouvez installer toutes les langues sur le système si vous en avez besoin.



Vous pourriez publier un applet de langue pour permettre aux utilisateurs de changer leur propre langue de système d'exploitation de l'interface utilisateur et d'ajouter un IME (Éditeur de méthode d'entrée).

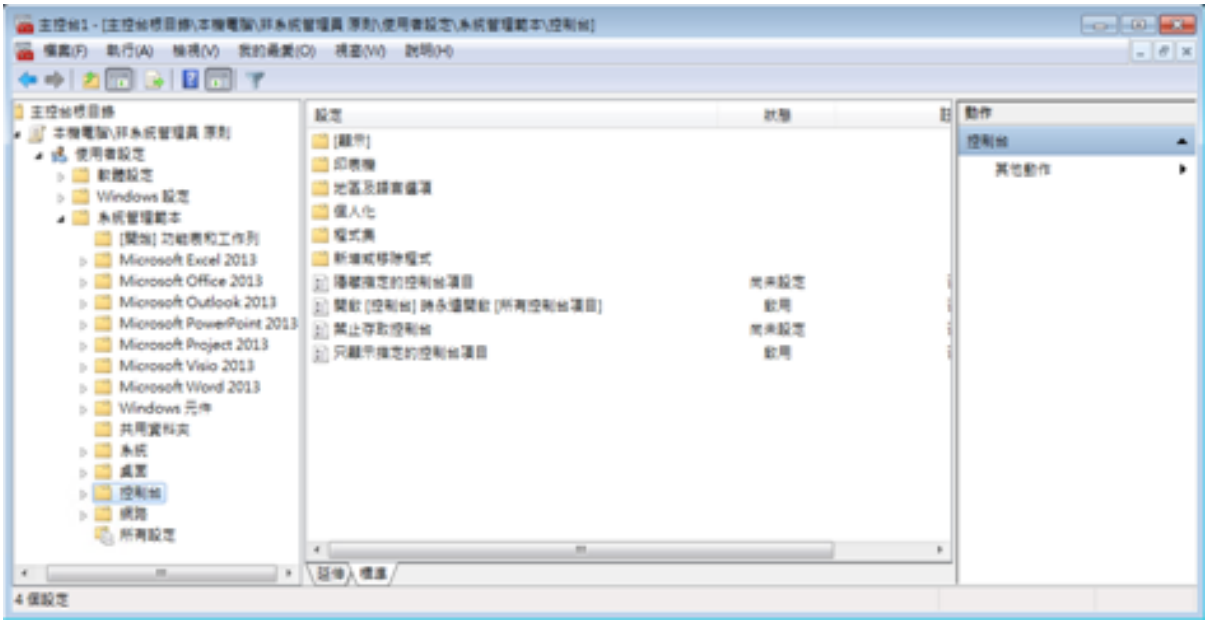


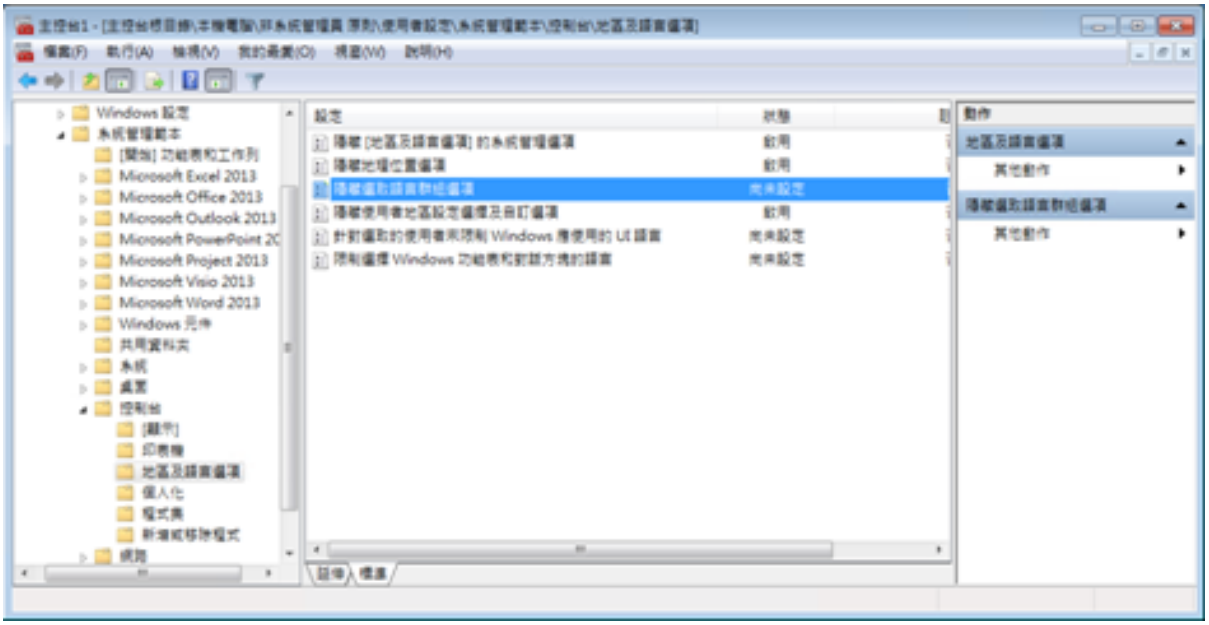
Pour Windows 7 : contrôle /nom Microsoft.RégionEtLangue

Pour Windows 8 : contrôle /nom Microsoft.Language

Liste complète : http://pcsupport.about.com/od/tipstricks/tp/control-panel-applets-list.htm

Optionnel : voici comment restreindre le comportement du Panneau de configuration pour les utilisateurs par GPO :

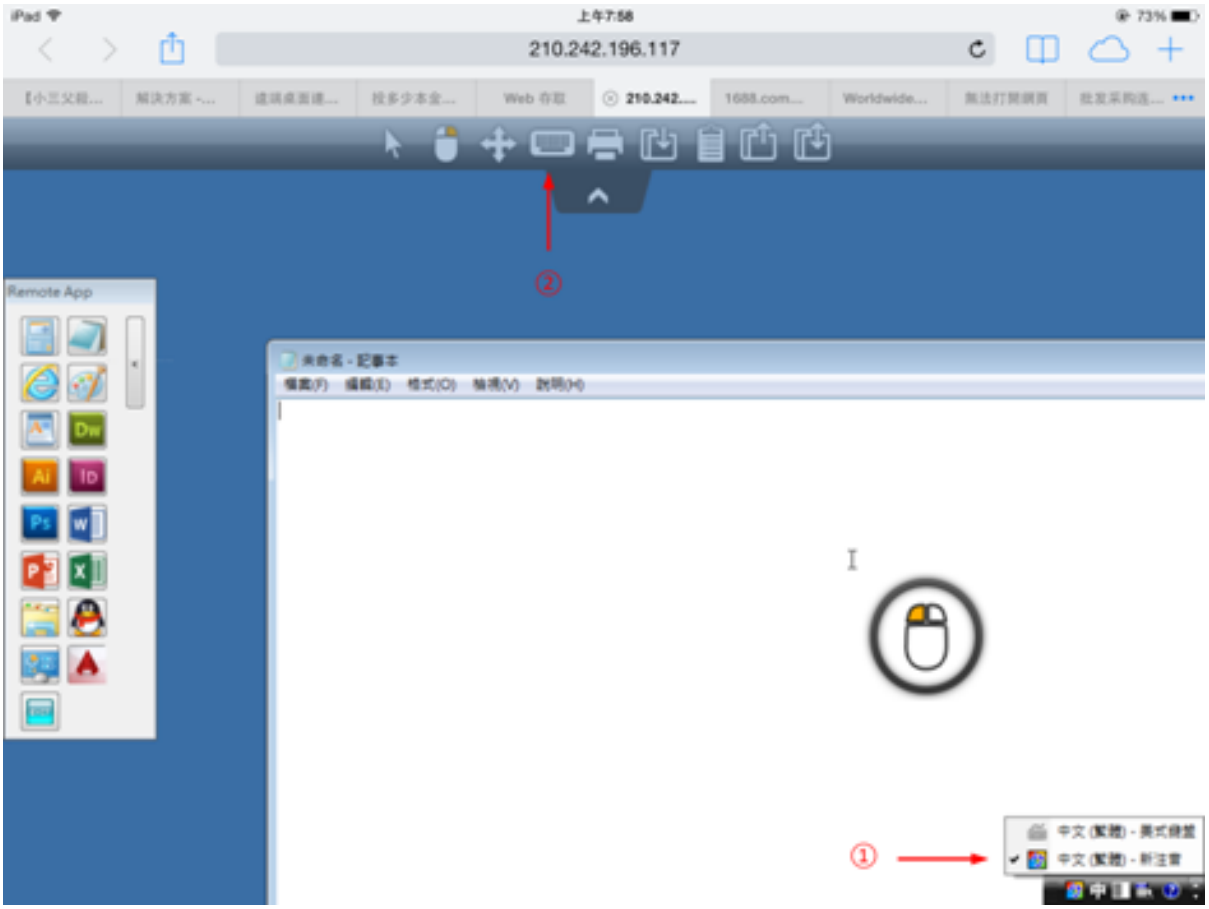




Les utilisateurs peuvent changer la langue du système d'exploitation de l'interface utilisateur après la connexion au système. (Les utilisateurs doivent se déconnecter et se reconnecter pour que ce paramètre prenne effet après l'avoir modifié.)



L'utilisateur doit d'abord sélectionner le IME chinois pour saisir des caractères chinois.


210.242.196.117
Remote App
②
①


210.242.196.117
中文中
中 中文 中國 巾 申 申請 申請人 甲 由 內 內 四 而 p 肉
.?123
上一個
確認
下一個
換行


210.242.196.117
確認
.?123
一聲
.?123

HTML5 Client : Quelle est la différence entre Websockets et XHR ?

Websockets est la connexion persistante qui peut être utilisée pour recevoir/envoyer des données sans ordre séquentiel et sans en-tête http.

Xhr-polling crée une nouvelle requête avec l'en-tête http et attend une réponse avec l'en-tête http, également dans l'ordre séquentiel.

En faisant cela, le flux de données XHR ressemble toujours à ceci :

HTTP_HEADER_ANSWER -> HTTP_HEADER_ANSWER HTTP_HEADER_ANSWER -> HTTP_HEADER_ANSWER et ainsi de suite

aussi avant que les données puissent être téléchargées, elles doivent être demandées avec HTTP_HEADER, donc son nom : xhr-polling.

Le flux de données Websockets peut ressembler à ceci :

Données_ENVOYER Données_ENVOYER Données_RECEVOIR Données_ENVOYER Données_RECEVOIR Données_RECEVOIR

Aussi, il s'agit d'un envoi/réception de données aléatoires sans ordre séquentiel spécial et sans aucune donnée d'en-tête http.

Cela rend l'utilisation avec des proxies inverses impossible en raison du manque de support des Websockets par la plupart des proxies inverses connus ; mais la moitié du transport xhr peut fonctionner avec un proxy inverse Apache.

Voir aussi : Client HTML5 : Navigateurs pris en charge

Client HTML5 : résolution de session RDP sur appareils mobiles

La résolution d'écran courante de la plupart des appareils, en particulier des téléphones mobiles, est de 320x480, mais cela n'est évidemment pas suffisant pour créer la session RDP.

Par conséquent, la résolution a été préconfigurée à 800 en largeur. La hauteur de la résolution est recalculée par la logique native des navigateurs cachés. Plus la largeur est grande, plus la hauteur est importante.

- En tant qu'exemple, la résolution standard est de 320x480, maintenant lorsque vous définissez la zone d'affichage à 800, le navigateur recalculera la valeur de la hauteur par exemple à 800x904, lorsque vous définissez la largeur à 1280, alors c'est 1280x1160, etc.

La hauteur et la largeur dépendent de l'affichage paysage/portrait de votre appareil, comme 800x904 ou 904x800, etc. Chaque navigateur peut le recalculer selon sa propre logique pour adapter l'écran RDP à la zone d'affichage de votre appareil et peut différer en fonction du navigateur, même lorsqu'il est utilisé sur le même appareil.

Si vous définissez la hauteur manuellement, vous allez alors rompre le ratio de la fenêtre de votre appareil et la session RDP finale sera hors de votre vue, et pour atteindre ces zones, vous devrez faire défiler jusqu'aux positions souhaitées.

- Il est donc recommandé de ne pas définir la hauteur manuellement, mais de laisser l'appareil choisir automatiquement la hauteur.

Si vous avez besoin de plus de hauteur, augmentez la largeur !

En testant sur des appareils de téléphonie mobile, la bonne valeur pour la largeur était de 800. Cependant, vous devez faire attention : les CPU de la plupart des téléphones mobiles sont généralement lents, donc lorsque vous augmentez la hauteur, cela augmentera la charge du CPU. Sur les appareils tablettes, les CPU sont plus rapides, il est donc recommandé de définir la largeur à une valeur plus élevée comme 1280 et de permettre à l'appareil de recalculer la valeur de la hauteur.

Parce que certains navigateurs comme FireFox mobile ne permettent pas de définir le viewport après le chargement de la page, cette valeur a été fixée dans le fichier Clients\www\software\html5.html :

Par exemple, changez-le en :

pour augmenter la largeur et en même temps la hauteur recalculée par la logique interne native des navigateurs.

En tant que deuxième exemple, le changer en :

ferait casser la zone de visualisation et la session RDP ne s'adapterait pas à l'écran.

Client HTML5 : Paramètres dans l'adresse URL

Lorsque vous utilisez le client HTML5 de Terminal Service Plus pour vous connecter à un serveur distant, vous pouvez spécifier plusieurs paramètres dans l'adresse URL pour remplacer les paramètres par défaut, tels que :

- connexion utilisateur
- mot de passe utilisateur
- programme à exécuter
- répertoire de démarrage pour le programme à exécuter
- ligne de commande pour le programme à exécuter

Exécuter une application spécifique

Voici un exemple d'une adresse URL complète pour ouvrir une session à distance pour l'utilisateur "demo" avec le mot de passe "demo" et en lançant le bloc-notes standard lors de l'ouverture de la session :

https://demo.tsplus.net/software/html5.html?user=demo&pwd=demo&program=c:\\windows\\system32\\notepad.exe&startupdir=c:\\windows\\system32¶ms=

Veuillez noter que dans l'adresse URL, tous les caractères de barre oblique doivent être répétés. **4 fois** .

Vous n'avez pas à spécifier tous ces paramètres en même temps : les paramètres non spécifiés auront leur valeur configurée par défaut.

Se connecter avec des identifiants Web

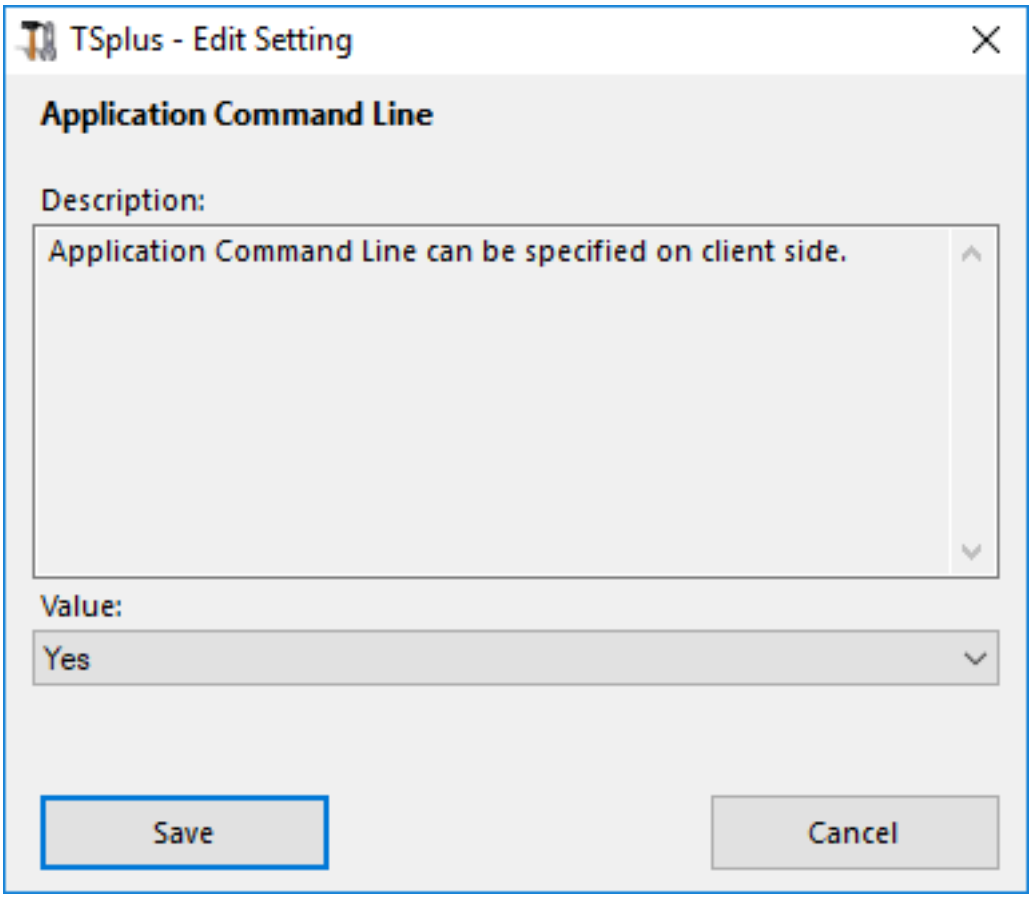
Si vous souhaitez utiliser un Web Credential Pour vous connecter, vous pouvez le passer dans une URL en ajoutant un "@" avant le Web Login.

Voici un exemple d'une adresse URL pour ouvrir une session à distance avec le Panneau d'Applications pour les Identifiants Web "1234" avec le mot de passe "demo" :

https://demo.tsplus.net/software/html5.html?user=@1234&pwd=demo

Restreindre cette utilisation aux applications par défaut des utilisateurs

Vous pouvez désactiver la ligne de commande de l'application pour les utilisateurs en allant sur le **Avancé —> Onglet de session** de l'AdminTool, en double-cliquant sur le paramètre « Ligne de commande de l'application » et en définissant la valeur sur « Non ».



Client HTML5 : Navigateurs pris en charge

Si votre navigateur affiche un avertissement rouge au démarrage en utilisant le client HTML5

Cela signifie que votre navigateur ne prend pas en charge les Websockets ou que votre navigateur ne prend pas en charge le Canvas.

Les navigateurs qui ne prennent pas en charge ces technologies sont IE6, IE7, IE8, IE9 et nécessitent FLASH pour émuler ces fonctionnalités.

Navigateurs prenant en charge Websocket et Canvas

Navigateurs	Toile	Websocket
FireFox	Complet	Version complète à partir de la version 4
Chrome	Complet	Complet dans la plupart des versions connues sur PC
Opéra	Complet	Complet dans les dernières versions
IE6	Flash	Flash (émulé et sans support de proxy)
	Flash	XHR (avec support proxy)
IE7	Flash	Flash (émulé et sans support de proxy)
	Flash	XHR (avec support proxy)
IE8	Flash	Flash (émulé et sans support de proxy)
	Flash	XHR (avec support proxy)
IE9	Flash	Flash (émulé et sans support de proxy)
	Flash	XHR (avec support proxy)
IE10	Complet	Complet
Android natif	Complet	XHR
Opera mobile	Complet	Complet dans les dernières versions
Firefox mobile	Complet	Complet
Safari mobile	Complet	Complet dans les dernières versions jusqu'à iOS4, sinon émulé via

		XHR

Voir aussi : Quelle est la différence entre les websockets et XHR ?

Si votre navigateur recharge automatiquement les pages vers l'adresse HTTPS

Cela signifie que le transport Websockets n'est pas pris en charge. C'est le cas sur plusieurs navigateurs mobiles natifs Android.

C'est dû au fait que le navigateur passe automatiquement au transport XHR.

Mais parce que ce transport se fait sur de longues distances avec le protocole HTTP, chaque requête crée une nouvelle connexion. Il est très lent et instable de créer de nouvelles connexions (jusqu'à 20 nouvelles connexions par seconde), donc pour éviter cette instabilité, le programme est conçu de manière à ce que la page se recharge automatiquement à l'adresse HTTPS pour imposer la connexion HTTPS.

Physiquement, vous bénéficiez également d'une connexion sécurisée principalement persistante et beaucoup plus stable sur de longues distances. Ainsi, la logique du navigateur réutilise la connexion SSL déjà établie au lieu de créer une nouvelle connexion comme c'est le cas avec le protocole HTTP.

Ce comportement peut être modifié par l'option suivante dans le fichier setting.js situé dans le dossier du programme TSplus sous ce chemin : Clients\www\software\html5\settings.js :

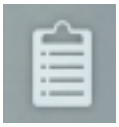
forcesslforxhr = false;

Mais il n'est absolument pas recommandé de désactiver l'utilisation de SSL en mode XHR.

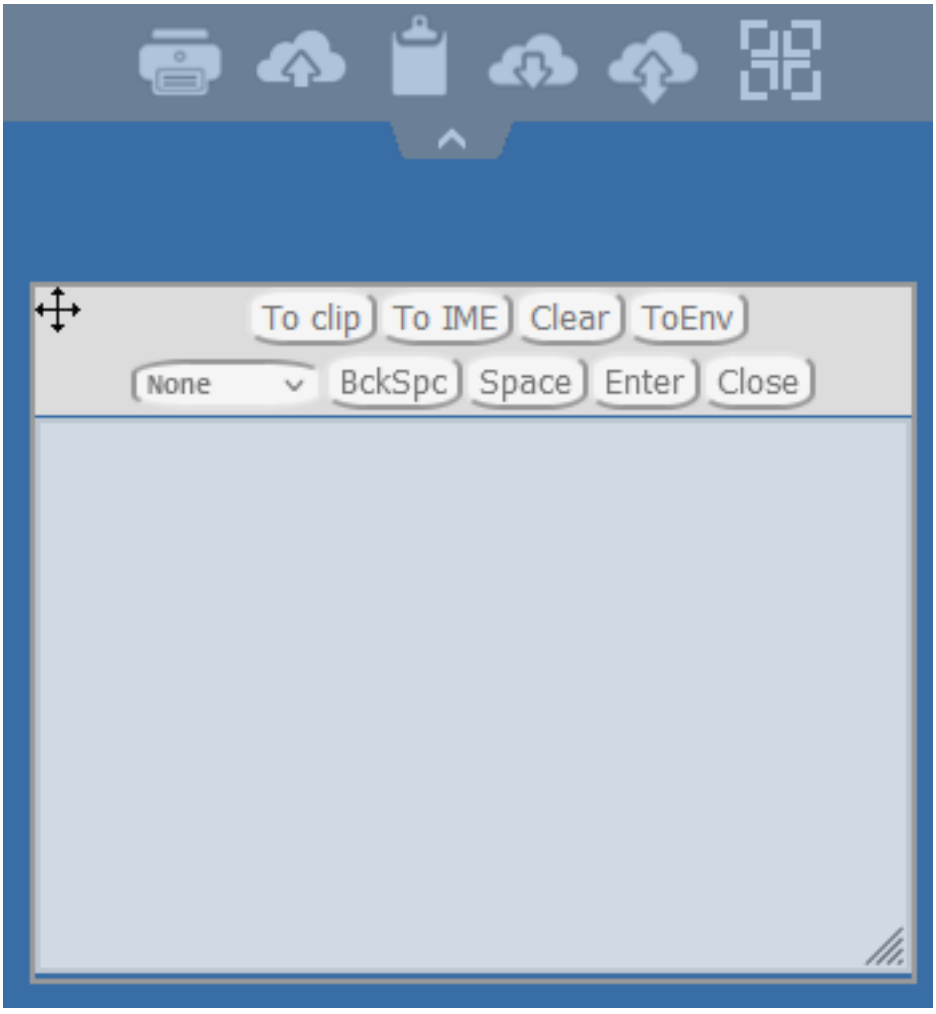
Si vous n'avez pas de fichier nommé "settings.js" dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software\html5", alors votre version de TSplus est plus ancienne et cette documentation ne s'applique pas. Veuillez d'abord mettre à jour votre système ou contacter le support.

Client HTML5 : Utilisation du Presse-papiers

Le presse-papiers se trouve dans le menu supérieur HTML5, avec cette icône :



La plupart des navigateurs, à l'exception des anciens navigateurs MSIE, ne prennent pas en charge la lecture et l'écriture directes du presse-papiers pour des raisons de sécurité.



Voici les différentes actions :

- **À couper** envoie AU SESSION RDP le contenu de la ZONE DE TEXTE et produit Ctrl+V à la fin pour mettre le texte À L'INTÉRIEUR DE LA SESSION RDP (votre PROPRE ENVIRONNEMENT n'est pas touché !!!)

- **À IME** : convertit les caractères de la ZONE DE TEXTE en frappes et les envoie comme si vous aviez utilisé le clavier. (ce bouton est nécessaire lorsque vous souhaitez placer le texte là où l'entrée de texte du presse-papiers n'est pas prise en charge dans l'application de session RDP)

- **ToEnv** ESSAIE de mettre du texte de la ZONE DE TEXTE dans votre propre PAPIER COLLANT en dehors de votre navigateur (pas dans la session RDP mais dans votre propre ENVIRONNEMENT !!!!) Parce que l'ajout de texte à votre propre presse-papiers est une action privilégiée, cela doit être exécuté par un clic.

- **À couper** Comme mentionné, gère la mise en texte dans rdp-clip+action ctrl/v sans ajouter de texte en dehors de son propre navigateur en raison de la sécurité, car il serait assez stupide de mettre du texte dans son propre presse-papiers lorsqu'on ne le souhaite pas vraiment, donc utilisez pour cela "ToEnv", ce comportement restera ainsi et ne sera pas modifié car demandé.

- **BckSpc** envoie la commande du bouton BACKSPACE à la session RDP (votre application doit être au premier plan et prendre en charge l'action du bouton Backspace)

- **Espace** envoie à la session RDP commande du bouton Espace (votre application doit être au premier plan et prendre en charge l'action du bouton Espace)

- **Entrer** : envoie la commande du bouton Entrée à la session RDP (votre application doit être au premier plan et prendre en charge l'action du bouton Entrée)

Pour copier le texte de la session dans le presse-papiers, utilisez Ctrl+C et pour insérer le texte du presse-papiers, utilisez Ctrl+V.

Mais faites attention lorsque vous copiez le texte avec Ctrl+C, attendez un certain temps avant de relâcher les touches Ctrl+C enfoncées, car si le texte demandé du presse-papiers arrive après que vous ayez relâché cette combinaison de touches, le texte ne sera pas ajouté à votre

presse-papiers d'environnement. Cette méthode utilise un support de copie du presse-papiers natif du navigateur initié par Ctrl+C.

Alternativement, vous pouvez **utilisez le menu du presse-papiers** pour copier depuis et insérer le texte dans le presse-papiers de la session RDP.

Là, vous pouvez simplement insérer le texte dans le presse-papiers de la session RDP ou l'ajouter au presse-papiers et initier automatiquement Ctrl+C sur le côté de la session RDP pour insérer le texte. Le menu du presse-papiers peut être ouvert via le menu d'action ou en appuyant sur Shift + F11.

- Lorsque vous copiez le presse-papiers avec la souris dans une session RDP, le texte est envoyé au navigateur et dès que vous sortez du focus du navigateur, le menu du presse-papiers apparaît automatiquement pour vous informer qu'il y avait un texte dans le presse-papiers et que vous ne l'avez pas ajouté à votre environnement de presse-papiers.

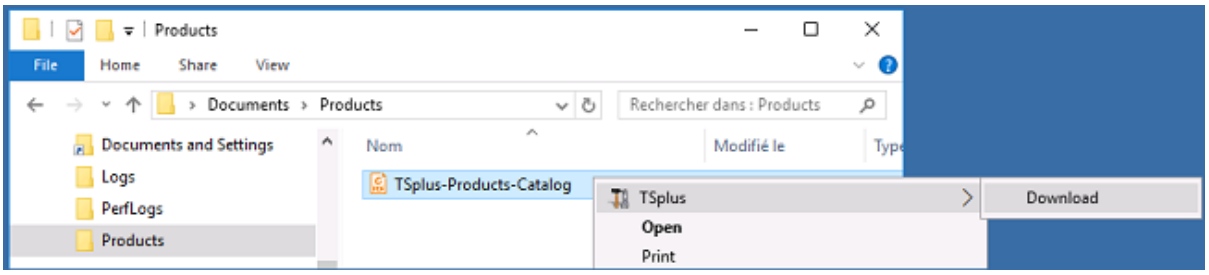
Pour éviter ce comportement, définissez la ligne suivante dans le dossier Clients, par défaut, le chemin est : C:\Program Files(x86)\tsplus\Clients\www\software\html5\settings.js :

openonclipblur = false;

Si vous n'avez pas de fichier nommé "settings.js" dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software\html5", alors votre version de TSplus est plus ancienne et cette documentation ne s'applique pas. Veuillez d'abord mettre à jour votre système ou contacter le support.

Client HTML5 : Utilisation du transfert de fichiers

Le transfert de fichiers peut se faire de plusieurs manières sur TSplus : depuis la version 12.50, **un menu contextuel est disponible pour télécharger des fichiers du serveur vers le PC local** :



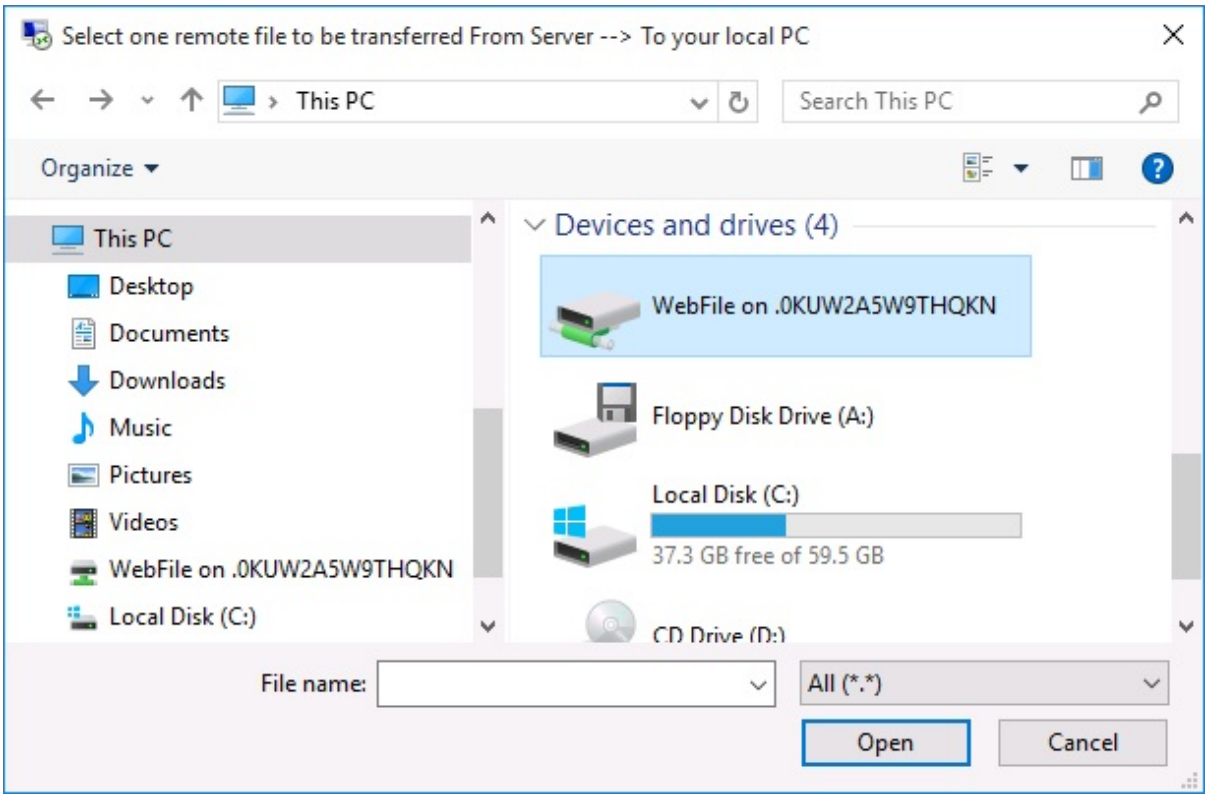
Plus d'informations peuvent être trouvées sur cette documentation .

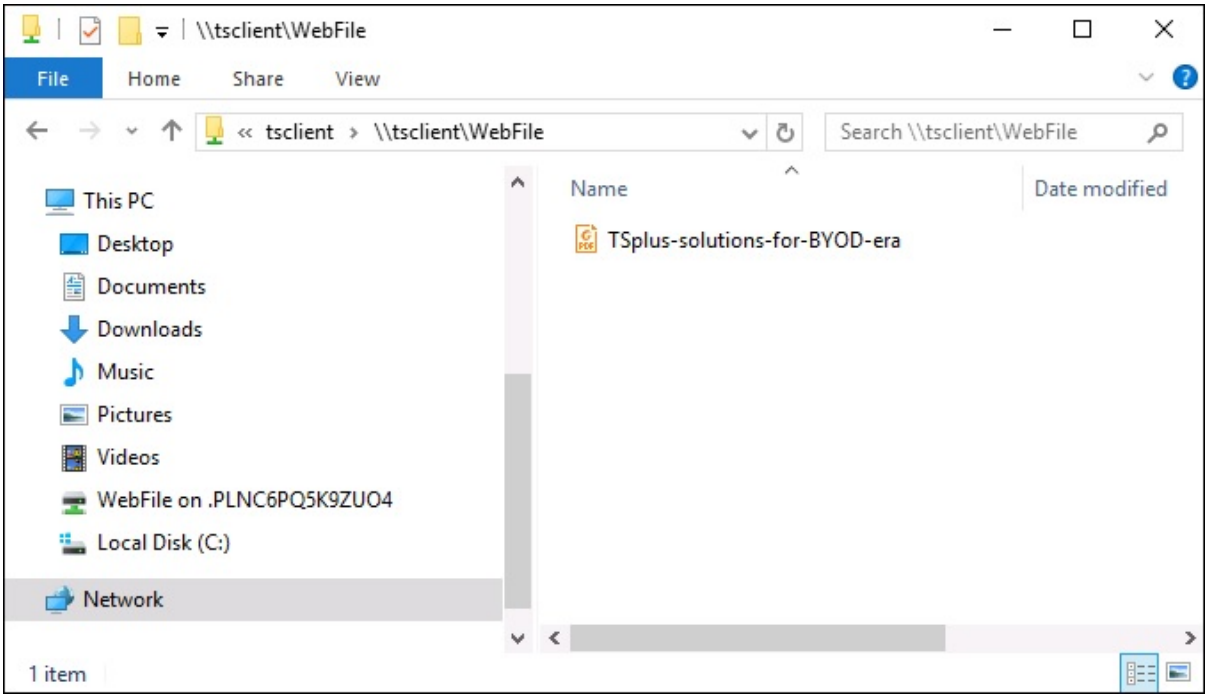
Utiliser le menu supérieur pour le transfert de fichiers :



Contrairement à une véritable session RDP, les navigateurs ne permettent pas d'accéder directement aux disques durs, le transfert de fichiers est émulé.

Le sous-dossier de la passerelle est monté en tant que périphérique WebFile dans votre session RDP. À l'intérieur de la session RDP, vous pouvez y accéder via l'Explorateur en cliquant sur "WebFile" ou appeler "\\tsclient\WebFile" directement.

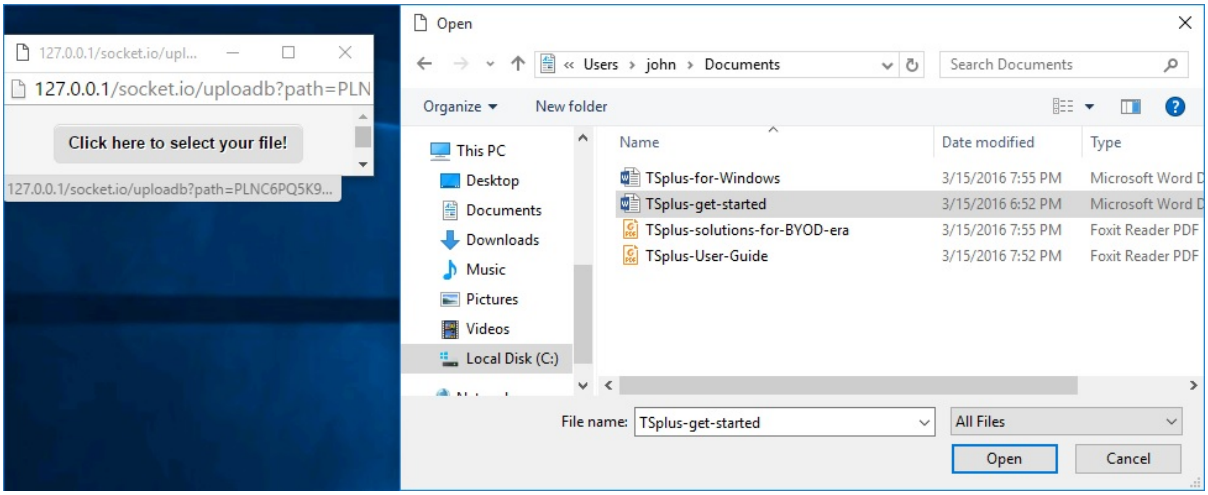




Il existe 3 possibilités différentes pour transférer un fichier :

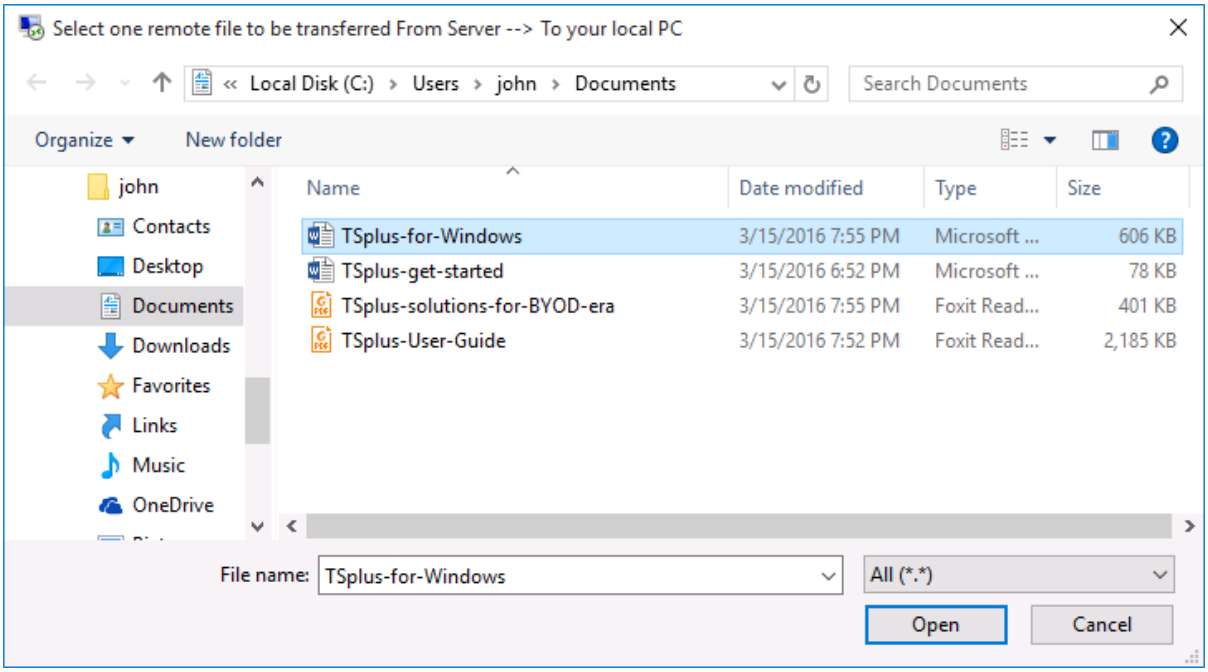
- Depuis l'ordinateur local vers le serveur :



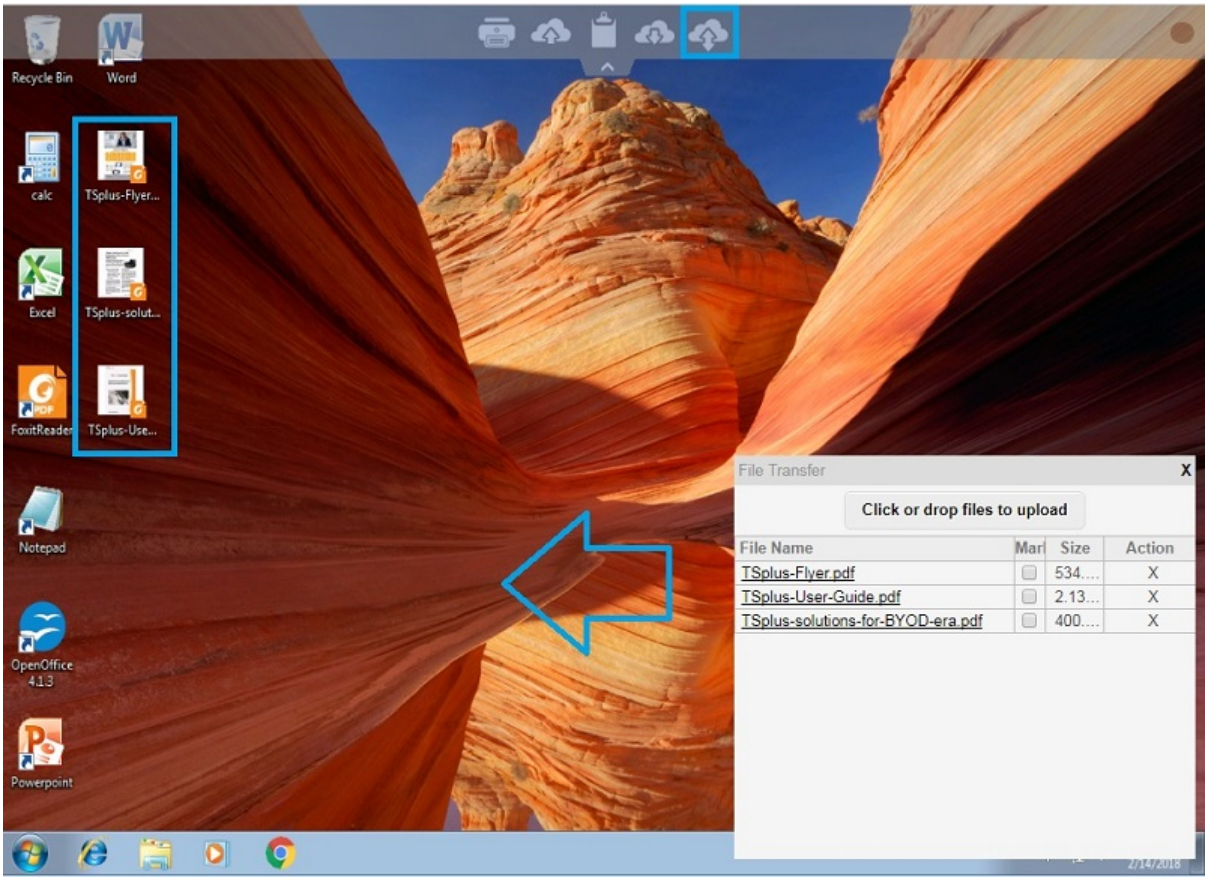


- Du serveur à l'ordinateur local :



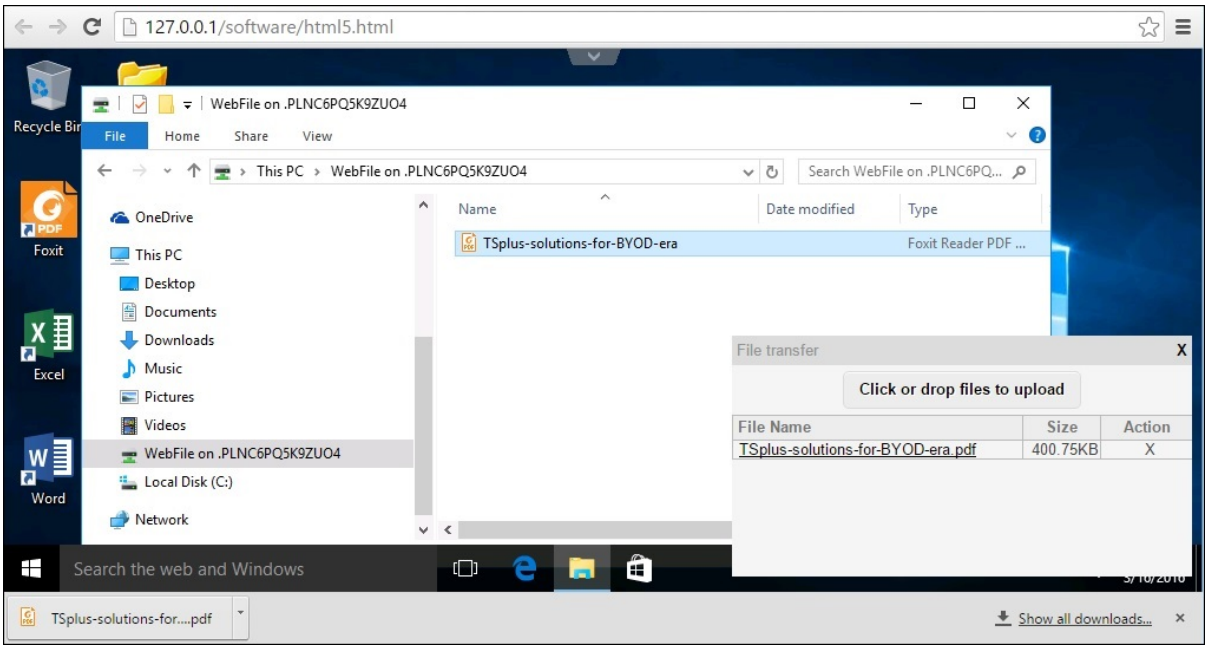


- Le gestionnaire de fichiers qui vous permet de transférer des fichiers de l'ordinateur local vers le serveur, avec un historique des fichiers transférés :

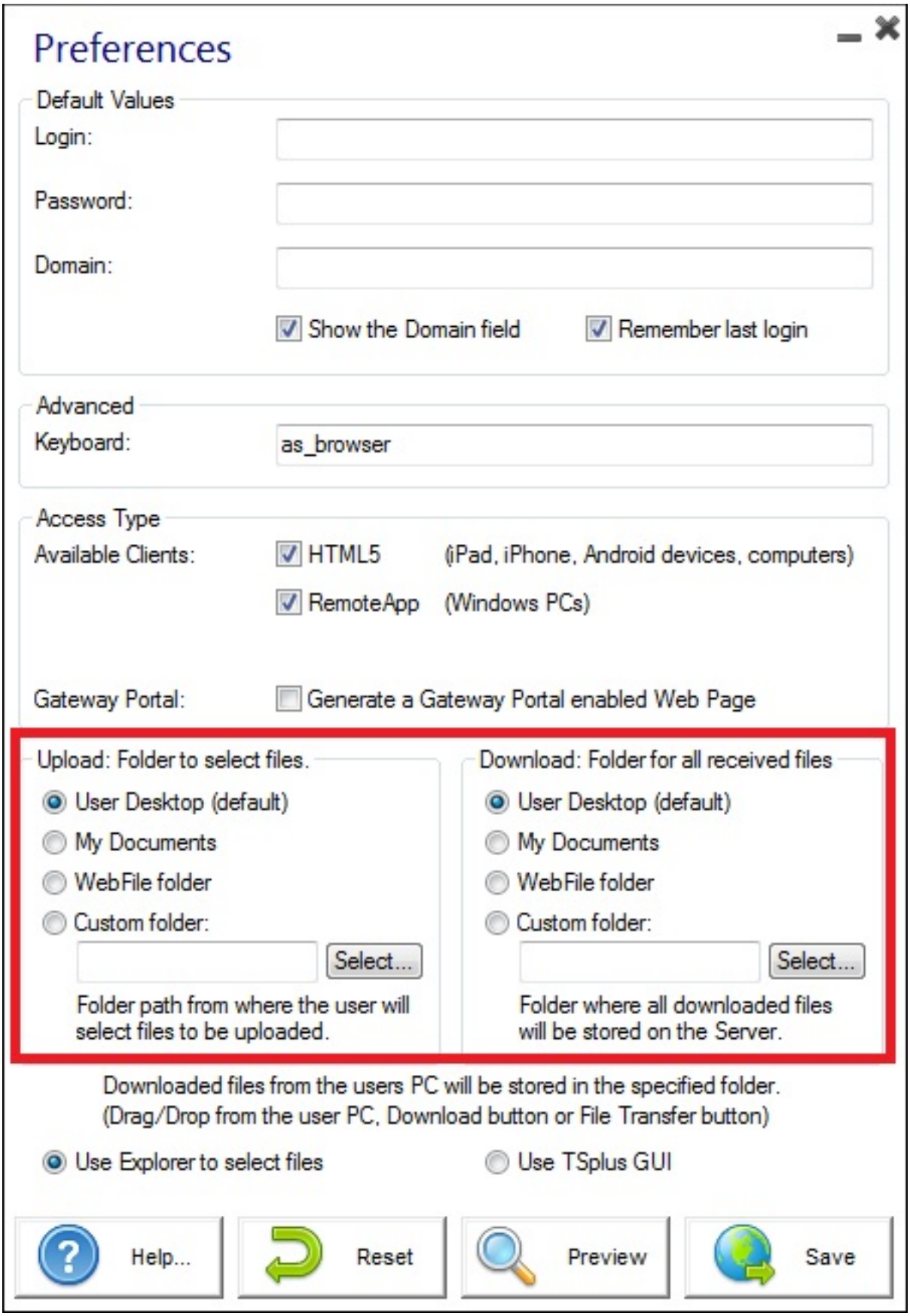


Sur le côté du navigateur, les fichiers sont affichés dans le menu de liste du navigateur. Ils peuvent être ouverts via le menu d'action ou avec Shift + F12.

- Lorsque vous copiez des fichiers avec l'Explorateur dans le dossier WebFile, cela déclenche automatiquement l'événement concernant la création d'un nouveau fichier dans le dossier WebFile et le menu du navigateur s'ouvre/rafraîchit automatiquement pour afficher le nouveau fichier.



Lorsque vous utilisez un dossier personnalisé, assurez-vous que ce dossier existe sur les côtés client et serveur. Vous pouvez définir le dossier de destination de téléchargement/téléversement dans le panneau de préférences du Portail Web sur l'onglet web de l'outil d'administration.



Si vous souhaitez éviter ce comportement, définissez la ligne suivante dans le fichier settings.js dont le chemin par défaut est : C:\Program Files (x86)\tsplus\Clients\www\software\html5\settings.js :

dropboxonnewfile = 0;

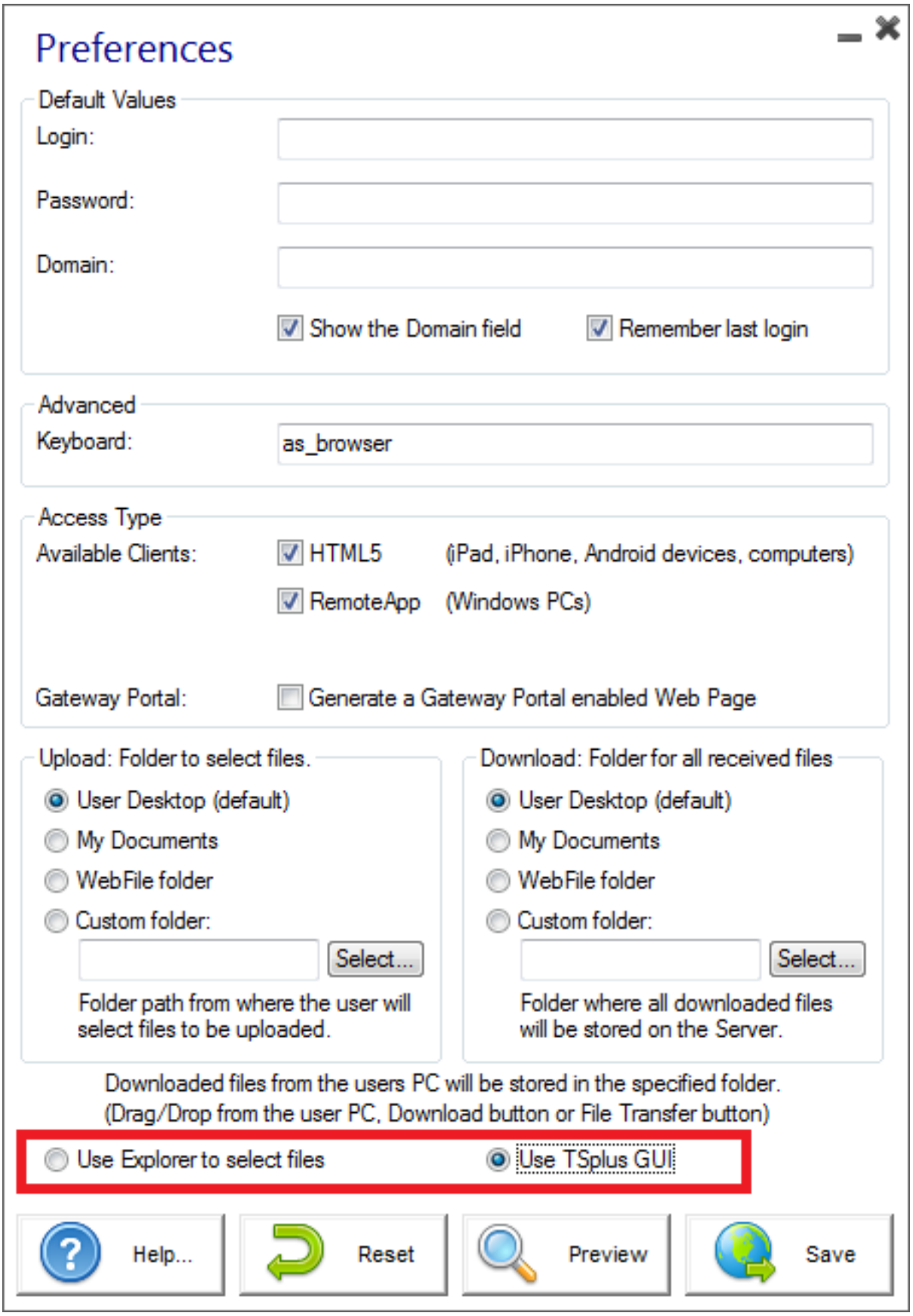
De plus, vous pouvez définir :

sharedfolder = “oui”;

pour afficher le dossier partagé et partager vos fichiers avec d'autres utilisateurs (désactivé par défaut).

Si vous n'avez pas de fichier nommé "settings.js" dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software\html5", alors votre version de TSplus est plus ancienne et cette documentation ne s'applique pas. Veuillez d'abord mettre à jour votre système ou contacter le support.

- Par défaut, l'explorateur est utilisé pour transférer des fichiers. Vous pouvez également télécharger directement vos fichiers du serveur au client en cochant "utiliser l'interface graphique TSplus", et copier des fichiers dans le dossier webfile :


Preferences
Default Values
Login:
Password:
Domain:
Show the Domain field
Remember last login
Advanced
Keyboard:
as_browser
Access Type
Available Clients:
HTML5
(iPad, iPhone, Android devices, computers)
RemoteApp
(Windows PCs)
Gateway Portal:
Generate a Gateway Portal enabled Web Page
Upload: Folder to select files.
User Desktop (default)
My Documents
WebFile folder
Custom folder:
Select...
Folder path from where the user will select files to be uploaded.
Download: Folder for all received files
User Desktop (default)
My Documents
WebFile folder
Custom folder:
Select...
Folder where all downloaded files will be stored on the Server.
Downloaded files from the users PC will be stored in the specified folder.
(Drag/Drop from the user PC, Download button or File Transfer button)
Use Explorer to select files
Use TSplus GUI
Help...
Reset
Preview
Save

Client HTML5 : Utilisation des gestes sur les appareils mobiles (tactile)

Utilisation de la zone d'écran :

1. Facile toucher sur l'écran = mouvement de la souris vers la position touchée et clic gauche de la souris
2. Double tap rapide sur l'écran = déplacement de la souris vers la position touchée et double clic gauche de la souris
3. Touchez et maintenez pendant une seconde sur l'écran = le curseur de la souris se déplace à la position touchée et effectue un clic droit.
4. Toucher et déplacer en dehors de la zone du curseur = faire défiler le cadre de session visible (comportement natif des navigateurs pour le défilement, en particulier après un zoom par pincement)
5. Touchez dans la zone du curseur et déplacez = le curseur de la souris se déplaçant uniquement
6. Double tap inside cursor area and move = left mouse down and mouse moving Utile pour déplacer la fenêtre, déplacer des éléments, redimensionner.
7. Double-tapez sur l'écran (en dehors de la zone du curseur) et déplacez votre doigt vers le bas/ vers le haut = défilement de la souris au milieu. Utile pour faire défiler des pages ou visualiser des PDF.
8. Pincer zoom avec deux doigts = zoomer le cadre de la session RDP (comportement natif des navigateurs)

Utilisation de la zone du pavé tactile - fonctions supplémentaires au point central du pavé tactile :

1. Facile toucher au milieu = clic gauche de la souris
2. Double tap au milieu = double clic gauche
3. Touchez et déplacez au milieu = mouvement de la souris et déplacement du pavé tactile
4. Appuyez et maintenez pendant une seconde = clic droit

Mode clavier activé :

1. Facilité de toucher à l'écran = perte de focus, clavier désactivé (comportement natif des navigateurs) mais cela déclenchera le mouvement de la souris et le clic gauche de la souris.
2. Double tap rapide = mouvement de la souris et clic gauche (sans désactiver le clavier) Utile pour repositionner le curseur, définir le focus sur un caractère différent et rester en mode

clavier en même temps.

3. Fonctions du pavé tactile décrites ci-dessus

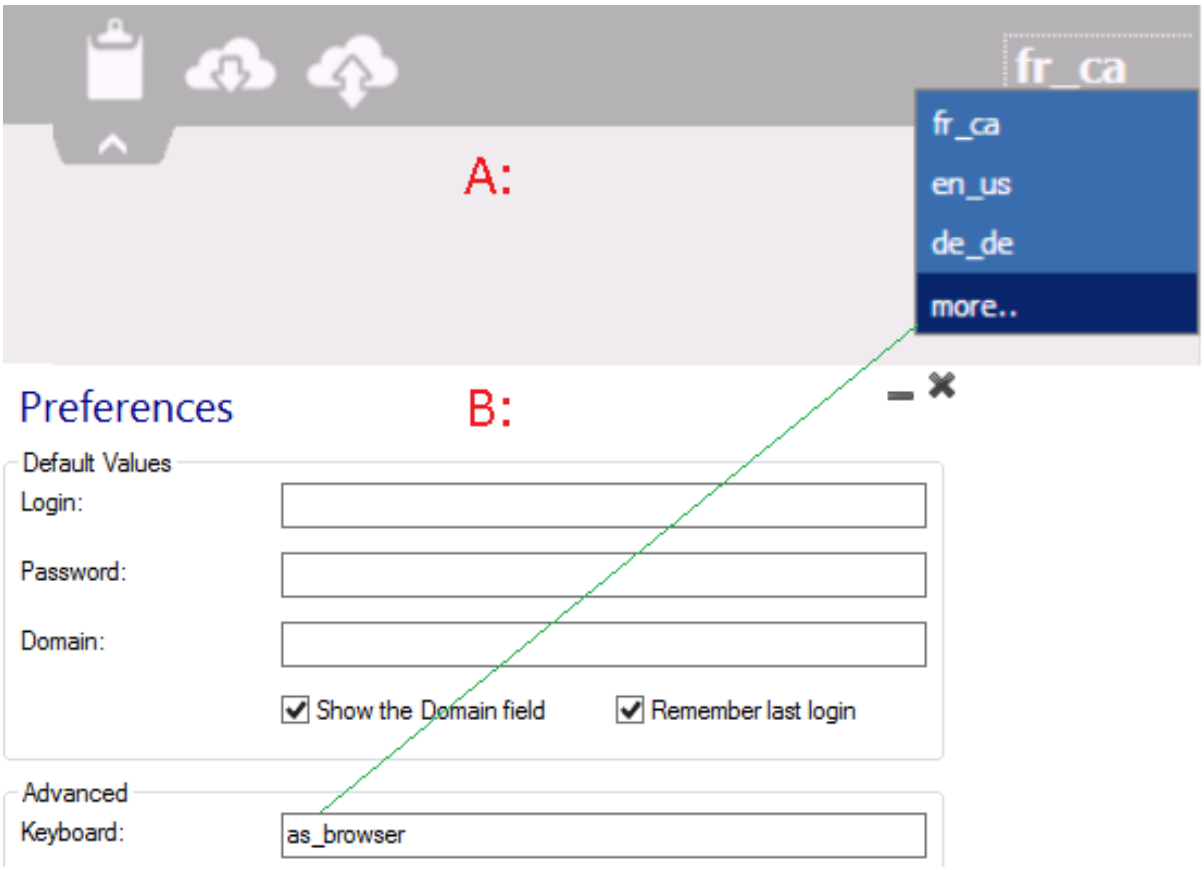
Client HTML5 : Utilisation de deux langues

Par défaut, le client HTML5 essaie de reconnaître la langue par défaut du navigateur et de l'utiliser ensuite dans la session RDP. Ce comportement est contrôlé par la balise "as_browser". Cependant, vous pouvez trouver la liste complète des balises de langue disponibles sur http:// votre_serveur /software/language.html sous "Locale"

Vous avez le choix de définir une langue fixe soit **A :** par client directement depuis le menu supérieur HTML5.

	Language	Locale	Value
○	Portal	as_portal	
○	Browser	as_browser	
○	Gateway	as_gateway	
○	Arabic	ar_ar	1025
○	Arabic (Algeria)	ar_dz	5121
○	Assamese	as_as	1101
○	Azeri (Cyrillic)	az_cy	2092
○	Azeri (Latin)	az_lt	1068
○	Belarusian	be_be	1059
○	Bulgarian	bg_bg	1026
○	Bengali	bn_bn	1093
○	Tibetan	bo_bo	1105
○	Bosnian (Cyrillic)	bs_cy	8218
○	Bosnian (Latin)	bs_lt	5146
○	Catalan	ca_ca	1027
○	Czech	cs_cs	1029
○		cs_cz	1029
○	Welsh	cy_gb	1106
○	Danish	da_da	1030
○		da_dk	1030
○	German (Swiss)	de_ch	2055
○	German	de_de	1031
○	Divehi	dv_dv	1125
○	Greek	el_el	1032
○		el_gr	1032
○	English (Canada)	en_ca	1105

B : ou depuis le portail en le configurant dans l'interface AdminTool, ce qui sera effectif pour tout le monde.



Vous devez redémarrer la session si vous définissez une autre langue comme principale.

Rappelez-vous : lors de l'utilisation **client HTML5** dans un scénario multilingue, assurez-vous que la langue utilisée dans la session Web-HTML5-RDP est synchronisée avec la langue réellement définie sur votre PC/portable/Mac, etc. Sinon, certains caractères qui sont représentés et traversent chaque carte de langue peuvent produire un mauvais caractère en envoyant le code de numérisation actuel pour une autre langue. Cela signifie également que si vous avez changé la langue de l'anglais à l'allemand dans la session Web, vous devez également la changer en allemand sur votre PC/portable/Mac.

Client HTML5 : Comment maximiser la fenêtre du navigateur

Aperçu

Le protocole RDP ne permet pas de redimensionner tout en étant connecté sans une reconnexion.

Veuillez noter que vous obtiendrez la meilleure expérience possible avec le client HTML5 de Terminal Service Plus en vous connectant avec un navigateur maximisé **.**

Cependant, si vous souhaitez forcer la fenêtre du navigateur à être aussi grande que possible, vous pouvez essayer de "forcer" la fenêtre HTML5 à s'ouvrir avec la taille maximale (mais pas en tant que fenêtre "maximisée", en raison des limitations de sécurité des navigateurs Internet).

Maximiser la fenêtre du navigateur

Vous devrez modifier le fichier “Clients\www\software\common.js” situé dans votre répertoire Terminal Service Plus. Nous vous conseillons d'utiliser un éditeur de texte tel que Notepad++. non utiliser Word).

Pour avoir une fenêtre de navigateur qui utilise tout l'écran, vous devrez modifier la ou les lignes contenant "window.open" et ajouter le texte suivant :

Fenêtre de terminal

"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(screen.availHeight-(55))

Cela permet à IE/Chrome/Firefox/Safari d'ouvrir la fenêtre avec une taille d'écran (moins la barre Windows). Malheureusement, il n'est pas possible de forcer un navigateur web à "maximiser" la fenêtre en mode "plein écran" de type Windows.

Ouvrez le fichier et recherchez "window.open("

Ensuite, ajoutez le nouveau à la fin avant des crochets, par exemple :

Fenêtre de terminal

```
window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
```

deviendra :

Fenêtre de terminal

```
window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

Et encore :

Fenêtre de terminal

```
tmpwin = window.open(p, '_blank'); //Chrome needs _blank
```

deviendra :

Fenêtre de terminal

```
tmpwin = window.open(p, '_blank',
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55))); //Chrome needs _blank
```

Et encore :

Fenêtre de terminal

```
success = window.open(p, k);
```

deviendra :

Fenêtre de terminal

```
success = window.open(p, k,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

Et enfin :

Fenêtre de terminal

```
cpwin = window.open("about:blank", n);
```

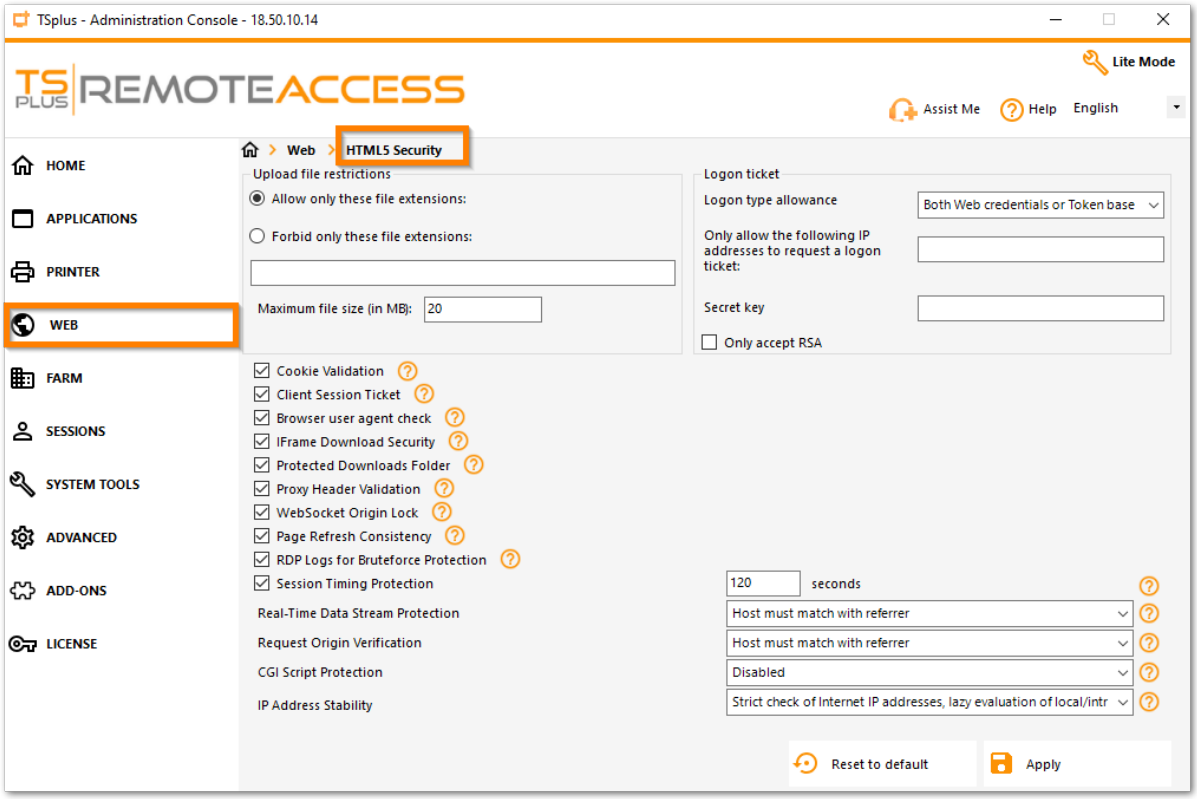
deviendra :

Fenêtre de terminal

```
cpwin = window.open("about:blank", n,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));
```

Sécurité HTML5

Dans l'onglet Sécurité HTML5, vous pouvez gérer les paramètres web.



Si vous avez besoin de sécurité supplémentaire, vous pouvez consulter et télécharger notre Advanced Security .

Utilisation de la mémoire du serveur HTML5

Le serveur Terminal Service Plus HTML5 fonctionne sur JAVA. Comprendre comment JAVA gère la mémoire aide à comprendre l'utilisation de la mémoire du serveur Terminal Service Plus HTML5.

Mémoire assignée

Lorsque Java s'exécute, il essaie d'allouer 25 % de la mémoire physique de l'ordinateur. Cette mémoire est "assignée" mais pas directement utilisée - ce n'est pas l'utilisation réelle de la mémoire que l'on peut voir dans le Gestionnaire des tâches de Windows.

plateforme JAVA : 32 bits vs 64 bits

Il y a une grande différence entre ces deux plateformes :

- JAVA 32 bits ne peut pas gérer plus de 4 Go de RAM par définition. Comme il allouera 25 % de toute la mémoire disponible, il allouera au maximum 1 Go, en supposant qu'il y ait 4 Go de mémoire physique. S'il n'y a que 2 Go de mémoire physique, il n'allouera que 500 Mo, etc.
- JAVA 64 bits peut gérer beaucoup plus de 4 Go (théoriquement jusqu'à 16 exa octets), donc la mémoire allouée dépendra uniquement de la mémoire physique.

Gestion de la mémoire JAVA

JAVA est une "machine virtuelle". Cela signifie que JAVA gère la mémoire de manière autonome. Une fois que JAVA alloue de la mémoire, même lorsqu'elle n'en a plus besoin, elle ne la rendra pas automatiquement au système. Cela est dû à des raisons de performance, car l'allocation et la désallocation de mémoire sont des tâches intensives pour le processeur.

JAVA attend généralement d'avoir un gros morceau de mémoire inutilisée avant de le rendre au système. La taille de ce gros morceau dépend directement de la taille de la mémoire physique de l'ordinateur. Plus il y a de mémoire physique sur un ordinateur, plus de mémoire est allouée par JAVA.

Utilisation de la mémoire du serveur HTML5 de Terminal

Service Plus

Tous ces détails techniques sont la raison pour laquelle on peut ouvrir le Gestionnaire des tâches Windows et penser que le serveur HTML5 de Terminal Service Plus utilise beaucoup de mémoire, ou que JAVA 32 bits utilise moins de mémoire que JAVA 64 bits.

En réalité, la mémoire réellement utilisée par le serveur HTML5 de Terminal Service Plus est directement liée au nombre de sessions HTML5 ouvertes. Plus il y a de mémoire disponible sur l'ordinateur, plus vous pouvez ouvrir de sessions HTML5.

Utilisation de la mémoire de session HTML5

La mémoire utilisée par une session HTML5 dépend des activités de l'utilisateur (applications et programmes utilisés, Word/Excel par rapport aux programmes intensifs en dessin) et de la méthode de connectivité établie entre le serveur HTML5 de Terminal Service Plus et l'ordinateur client.

Dans le cas d'utilisation général, une session HTML5 utilisera 30 Mo de mémoire (utilisation standard, connectivité websockets binaire). Dans le pire des cas, une session utilisera jusqu'à 100 Mo de mémoire (utilisation intensive, connectivité de secours "XHR" pour les anciens navigateurs).

Perte d'écoute du serveur HTTP et HTTPS

Chaque journal d'erreur Java indique une mémoire native suffisante pour le fonctionnement.

Le problème est en réalité assez simple.
Lorsque la session HTML5 démarre, il y a suffisamment de mémoire selon les valeurs rapportées.
Ensuite, dans la session RDP, il démarre un programme inconnu et vole toute la mémoire native pour lui-même.

Lorsque Java le demande à nouveau, il n'est soudainement plus disponible, ce qui entraîne cette erreur de mémoire insuffisante.

- Il n'y a pas suffisamment de mémoire pour que l'environnement d'exécution Java puisse continuer.
- Échec de l'allocation de mémoire native (mmap) pour mapper 234881024 octets. Détails de l'erreur : espace virtuel G1# Raisons possibles :
- Le système a épuisé la RAM physique ou l'espace d'échange# Ce processus s'exécute avec Compressed Oops activé, et le tas Java peut bloquer la croissance du tas natif.

Solutions possibles :

- Réduire la charge mémoire sur le système
- Augmentez la mémoire physique ou l'espace d'échange# Vérifiez si le stockage de support d'échange est plein
- Réduire la taille de la mémoire Java (-Xmx/-Xms)
- Réduire le nombre de threads Java # Réduire la taille de la pile de threads Java (-Xss)
- Définir une taille de cache de code plus grande avec -XX:ReservedCodeCacheSize=

La JVM fonctionne en mode Zero Based Compressed Oops, dans lequel le tas Java est placé dans les 32 premiers Go d'espace d'adressage. L'adresse de base du tas Java est la limite maximale pour la croissance du tas natif.
Veuillez utiliser **-XX:HeapBaseMinAddress**

Potentiellement, vous pourriez allouer plus de mémoire native à Java dès le départ et le forcer à ne plus renvoyer de mémoire au système, lui allouant ainsi à lui-même.
Cependant, dans ce cas, vous rencontrerez le problème suivant : les programmes s'exécutant dans une session RDP peuvent manquer de mémoire, et l'ensemble du système pourrait planter.

Mais vous pouvez toujours essayer.

1. Ouvrez et modifiez le fichier suivant avec Notepad : *\Clients\webserver\runwebserver.ini

2. Là, vous trouverez les paramètres de ligne de commande suivants, comme ceci :

Fenêtre de terminal

-Djdk.tls.ephemeralDHKeySize=matched -Djdk.tls.rejectClientInitiatedRenegotiation=true -Dorg.jboss.netty.epollBugWorkaround=true -XX:+UseG1GC -XX:MinHeapFreeRatio=10 -XX:MaxHeapFreeRatio=10 **********
and so on

3. Supprimez toute la ligne de runwebserver.ini et ajoutez ce qui suit à sa place :

Fenêtre de terminal

```
-server -javaagent:"%~dp0httpwebs.jar" -Djdk.tls.ephemeralDHKeySize=matched -
Djdk.tls.rejectClientInitiatedRenegotiation=true -Dorg.jboss.netty.epollBugContourn=true --add-
opens java.prefs/java.util.prefs=ALL-UNNAMED --add-opens java.base/java.lang.reflect=ALL-
UNNAMED --add-opens java.base/sun.security.ssl=ALL-UNNAMED --add-opens java.base/
java.nio=ALL-UNNAMED --add-opens java.base/jdk.internal.ref=ALL-UNNAMED --add-exports
java.prefs/java.util.prefs=ALL-UNNAMED ---add-exports java.base/java.lang.reflect=ALL-
UNNAMED --add-exports java.base/sun.security.ssl=ALL-UNNAMED --add-exports java.base/
jdk.internal.ref=ALL-UNNAMED --add-exports java.base/java.nio=ALL-UNNAMED
```

4. Redémarrez le serveur HTML5 via l'interface AdminTool pour appliquer les modifications. Mais avant de le faire, assurez-vous que le fichier web server\runwebserver.bat n'a pas d'attribut en lecture seule défini dans ses propriétés. Sinon, l'interface graphique AdminTool ne pourra pas adapter runwebserver.bat après un redémarrage.

Dans la plupart des cas, cela devrait suffire. Une fois que Java utilise de la mémoire, il l'allouera à d'autres usages au lieu de la retourner au système. Par conséquent, l'utilisation de la mémoire de html5service.exe pourrait potentiellement atteindre 70 % de la mémoire disponible du système. Dans ce cas, Java devrait potentiellement cesser de planter. Cependant, si un autre programme consomme une grande quantité de mémoire, il pourrait planter à la place. Dans ce cas, nous sommes impuissants ; vous devez vous assurer qu'il y a suffisamment de mémoire pour faire fonctionner un serveur HTML Java ainsi que d'autres programmes.

Il existe une option dans Java appelée -XX:+AggressiveHeap qui pourrait améliorer l'allocation de mémoire pour la machine virtuelle Java elle-même, et donc le contenu final de *\webserver\runwebserver.ini.

Cela pourrait ressembler à ceci :

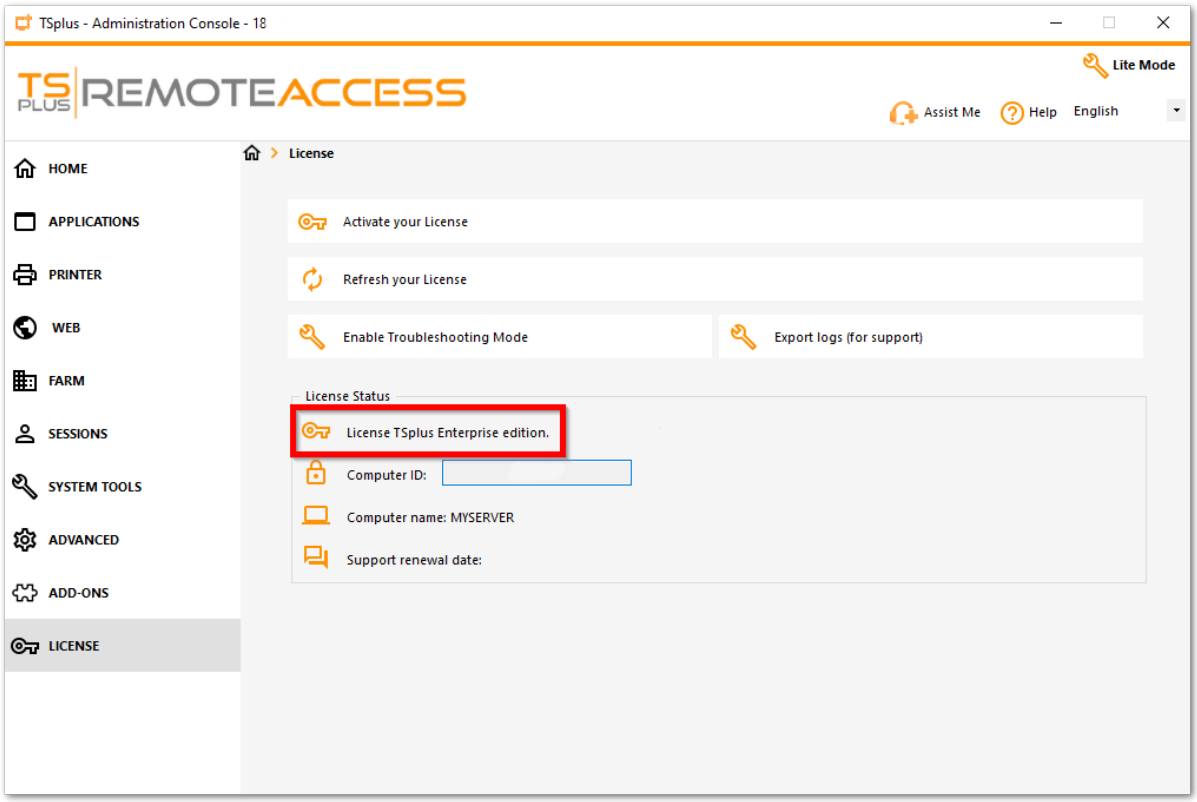
Fenêtre de terminal

```
-XX:+AggressiveHeap -server -javaagent:"%~dp0httpwebs.jar" -
Djdk.tls.ephemeralDHKeySize=matched -Djdk.tls.rejectClientInitiatedRenegotiation=true -
```

Dorg.jboss.netty.epollBugWorkaround=true --add-opens java.prefs/java.util.prefs=ALL-UNNAMED --add-opens java.base/java.lang.reflect=ALL-UNNAMED --add-opens java.base/sun.security.ssl=ALL-UNNAMED --add-opens java.base/java.nio=ALL-UNNAMED --add-opens java.base/jdk.internal.ref=ALL-UNNAMED --add-exports java.prefs/ java.util.prefs=ALL-UNNAMED --add-exports java.base/java.lang.reflect=ALL-UNNAMED --add

Comment identifier votre édition TSplus

Sur la tuile de licence sous le numéro de série, vous pouvez voir le type de licence que vous avez acheté ainsi que votre nombre d'utilisateurs à côté du nombre de connexions :



TSplus a fusionné d'anciennes licences en une seule afin d'obtenir plus de clarté. Les éditions Système et Imprimante ont migré vers **Desktop Edition** .

Desktop Edition

Fonctionnalités de base :

- TSplus Administrator Tool (AdminTool),

- Support des connexions simultanées,
- Contrôle des applications par utilisateur et/ou par groupes,
- TSplus Remote Taskbar et/ou TSplus Floating Panel,
- Accès au Bureau à distance,
- TSplus Portable Client Generator,
- Client de connexion RemoteApp,
- Entièrement conforme au protocole RDP,
- Support double écran, son bidirectionnel, RemoteFX lorsque compatible avec la version de Windows,
- Support de connexion locale et à distance,
- Support des utilisateurs de Workgroup et d'Active Directory,
- Redirection de périphérique/disque.
- Virtual Printer, vous permet d'imprimer depuis n'importe quel emplacement, sans avoir à installer de pilote spécifique et permet la redirection d'imprimante.

Édition Web Mobile

Vous permet (en plus de toutes les fonctionnalités des éditions Système et Imprimante) de :

-

Connectez-vous depuis n'importe quel navigateur web avec TSplus HTTP Web Server,

- Connexion entièrement sécurisée depuis n'importe quel navigateur web avec le serveur web HTTPS de TSplus et le serveur SSH,
- Les pages HTML incluent des clients d'accès web Windows et HTML5,
- Connectez-vous facilement depuis des appareils iPhone/iPad et Android, également avec le TSplus Mobile App ,
- Personnalisez la page de connexion web avec l'outil Webmaster facile à utiliser de TSplus,
- Avec le portail d'applications Web TSplus, les utilisateurs peuvent accéder à leur liste d'applications dans leur navigateur Web,
- Au lieu des identifiants Windows, les identifiants Web TSplus permettent aux utilisateurs de se connecter uniquement avec un e-mail ou un code PIN.
- Universal Printer vous permet d'imprimer depuis n'importe quel endroit, sans avoir à installer de pilote d'imprimante spécifique.

Enterprise Edition

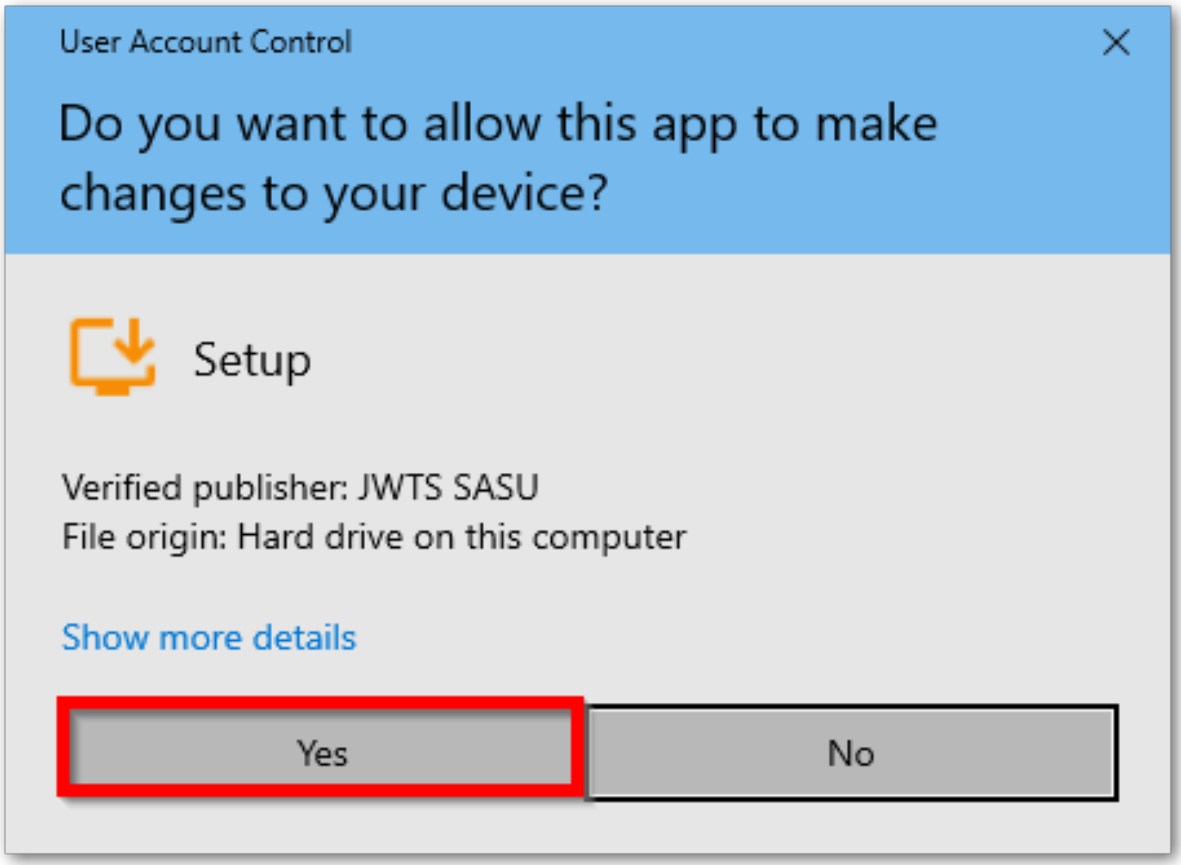
Comprend toutes les fonctionnalités précédentes plus celles-ci :

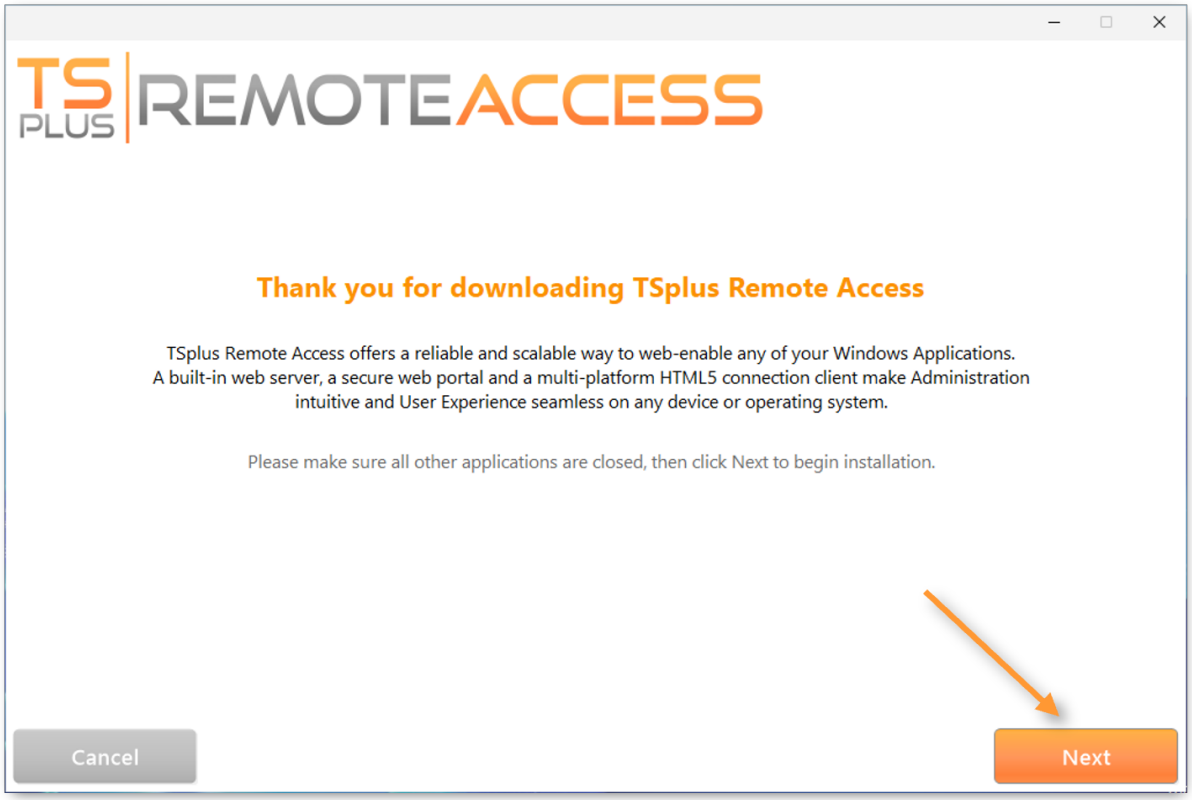
- Supportez un nombre illimité de serveurs au sein de chaque ferme TSplus (nécessite une licence par serveur),
- Des milliers d'utilisateurs travaillant simultanément sur une architecture évolutive équilibrée par charge,
- Portail unique d'entreprise pour accéder à tous vos serveurs TSplus,

- Capacité d'assigner un ou plusieurs Serveur(s) d'Application à des utilisateurs ou des groupes d'utilisateurs,
- Équilibrage de charge et support de basculement inclus.
- La possibilité d'ajouter une couche de sécurité supplémentaire avec le TSplus 2FA Add-On .

TSplus Remote Access v19 Installation

Exécuter TSplus Remote Access Setup program et ensuite **suivez les étapes d'installation** .
Votre mot de passe administrateur local est requis après le premier redémarrage de TSplus Remote Access.





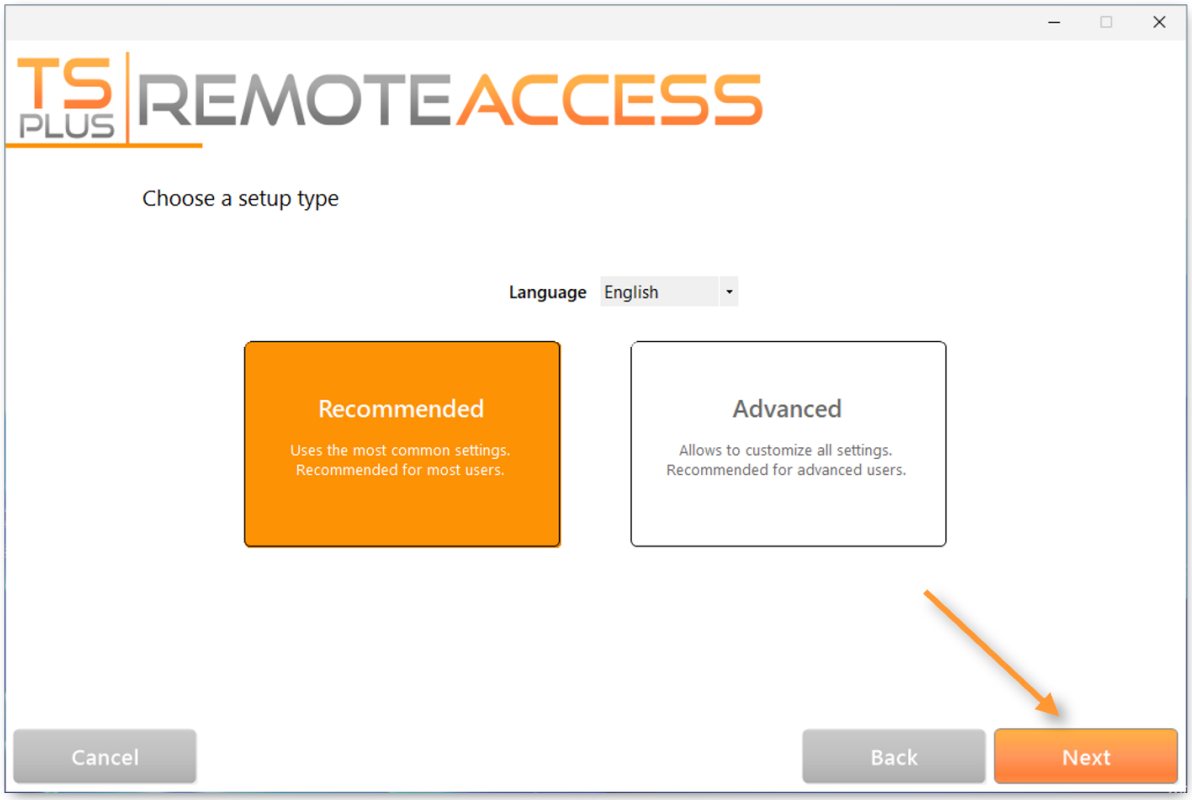
Vous pouvez ensuite sélectionner votre langue (il est possible de la changer plus tard)

Vous pouvez ensuite sélectionner deux options personnalisées en cochant les cases correspondantes : **Recommandé** ou **Avancé**

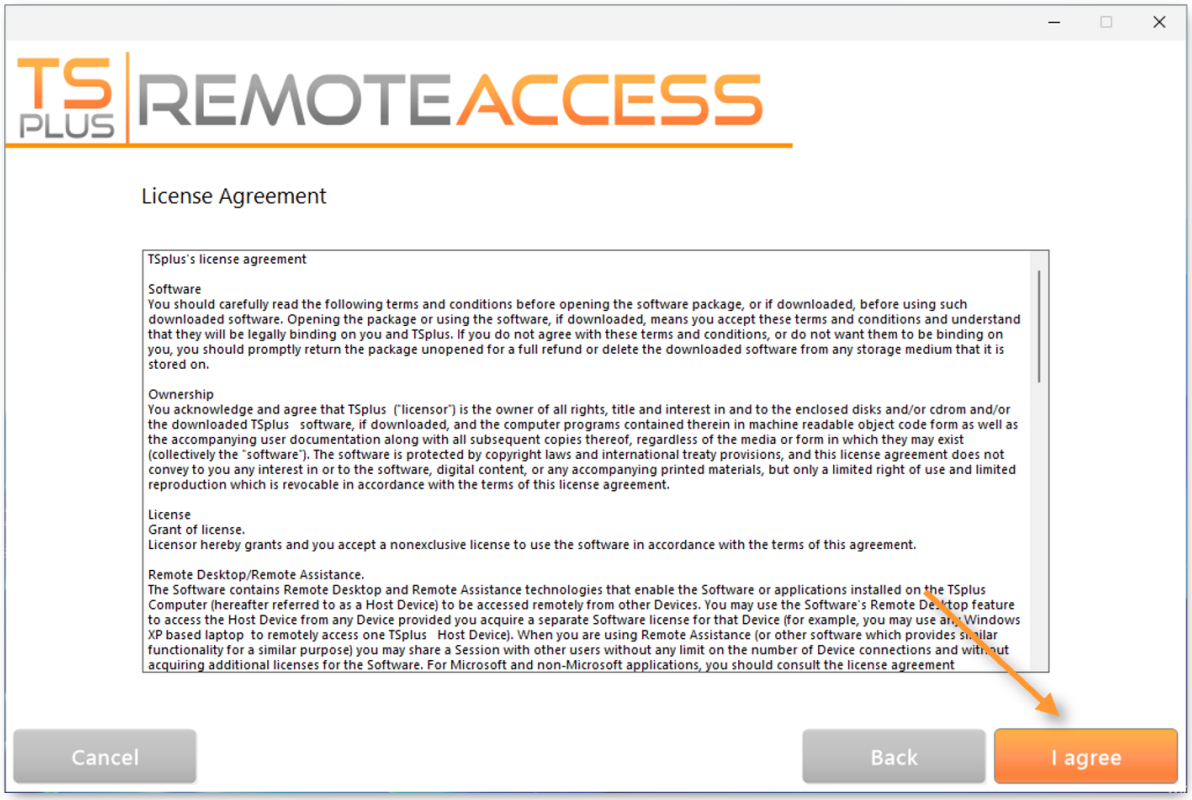
L'option Avancée vous permet de :

- Ne pas installer TSplus Advanced Security.
- Utilisez des paramètres de proxy personnalisés.
- Téléchargez uniquement le programme d'installation, qui n'installe pas TSplus.
- Changer les ports par défaut (non recommandé).

Cliquez sur Suivant.



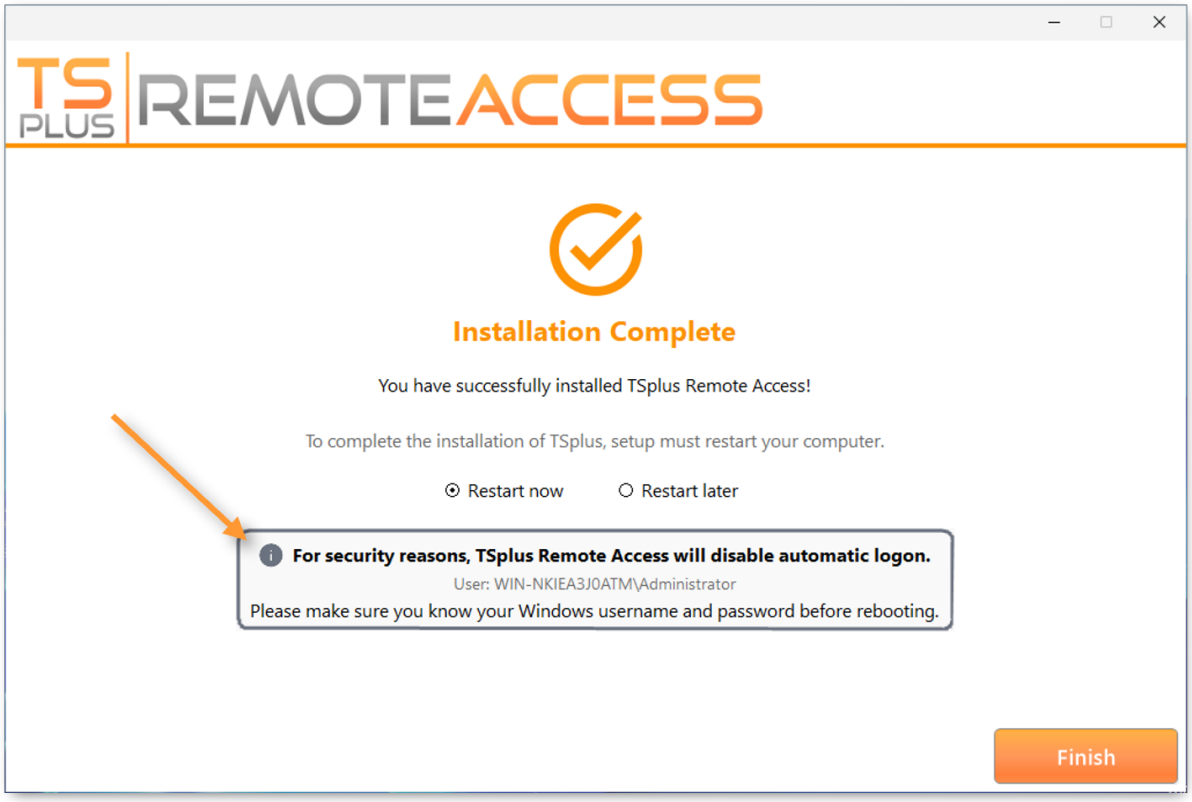
Cliquez sur J'accepte l'accord.



Veuillez patienter, téléchargement et installation du programme.



Puis le logo TSplus apparaît et une fenêtre vous informe de l'achèvement de l'installation.

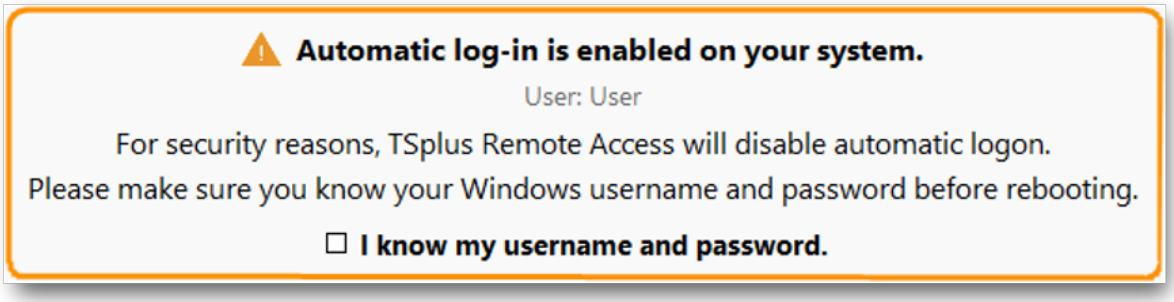


☐ **Avis important**

Pour des raisons de sécurité, **TSPlus Remote Access** vous devrez saisir manuellement votre nom d'utilisateur et votre mot de passe à chaque connexion.

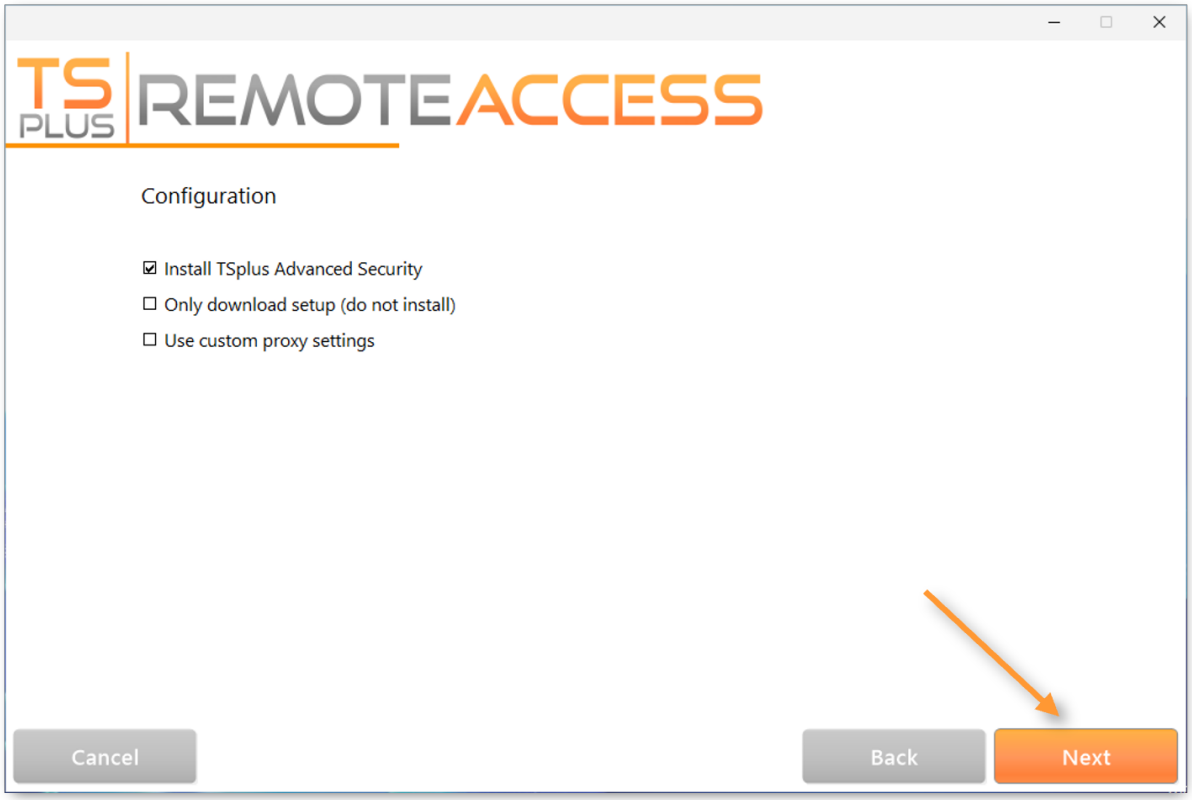
Assurez-vous de connaître vos identifiants avant de redémarrer le système pour éviter d'être verrouillé.

Si
autologon
est activé sur le système, l'installateur affichera une fenêtre d'avertissement vous demandant de confirmer que vous connaissez votre nom d'utilisateur et votre mot de passe.



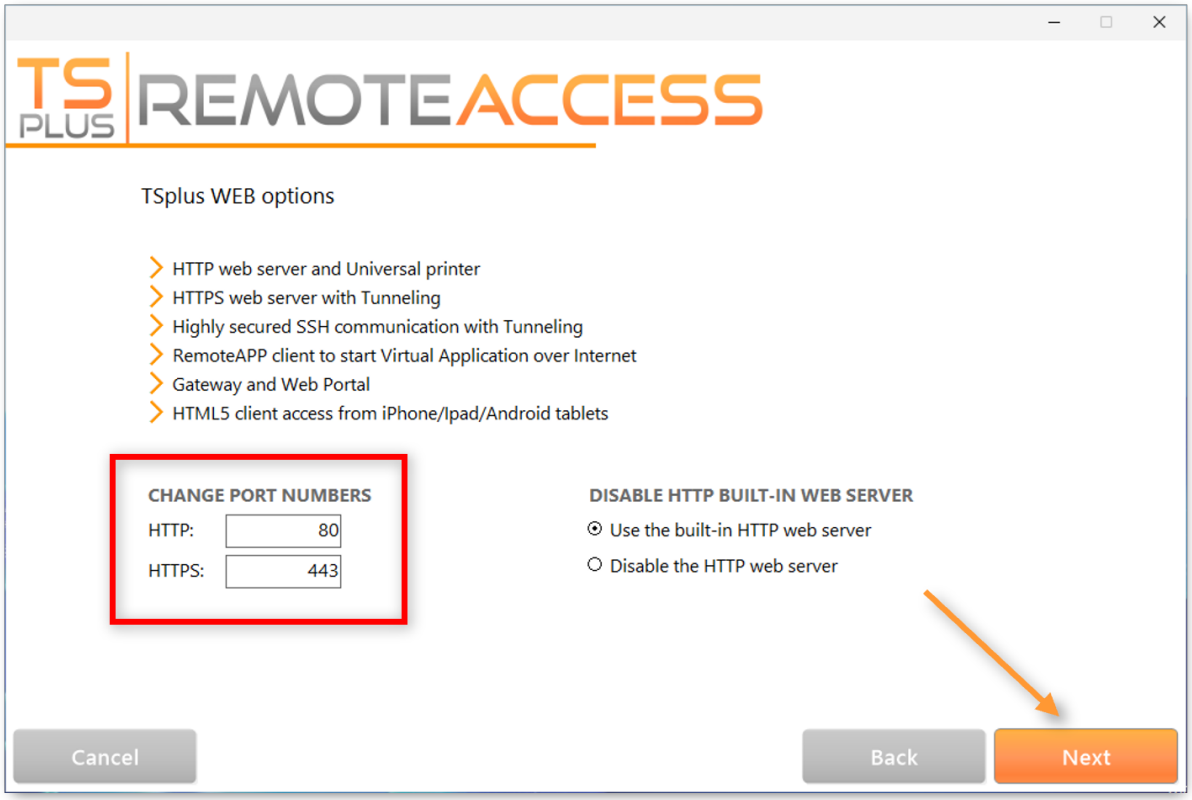
Pour utiliser TSplus, vous devez redémarrer votre système. La période d'essai offre un produit complet pendant 15 jours et 5 utilisateurs simultanés.

Les étapes ci-dessous uniquement si vous cochez installer TSplus Remote Access dans **Mode avancé** .

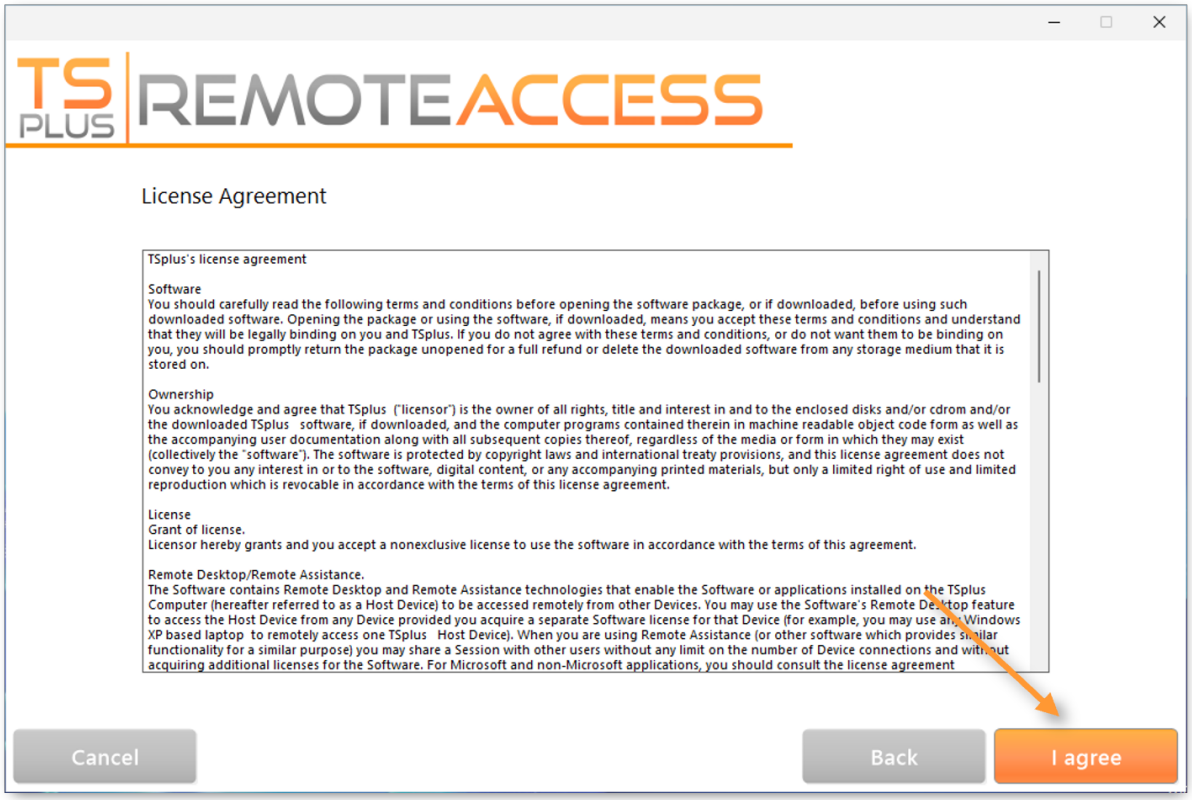


Les serveurs Web écoutent sur les ports 80 et 443 par défaut. Nous vous recommandons d'accepter nos paramètres d'installation par défaut de TSplus. Selon notre expérience, la plupart des problèmes de production sont dus aux fonctionnalités de sécurité de Windows.

Vous pouvez toujours modifier ces ports si vous le souhaitez pendant l'installation ou à tout moment sur le Gestion du serveur Web intégré de l'AdminTool Assurez-vous simplement que les ports définis sont disponibles et que Java est installé sur le serveur.



Cliquez sur J'accepte l'accord.



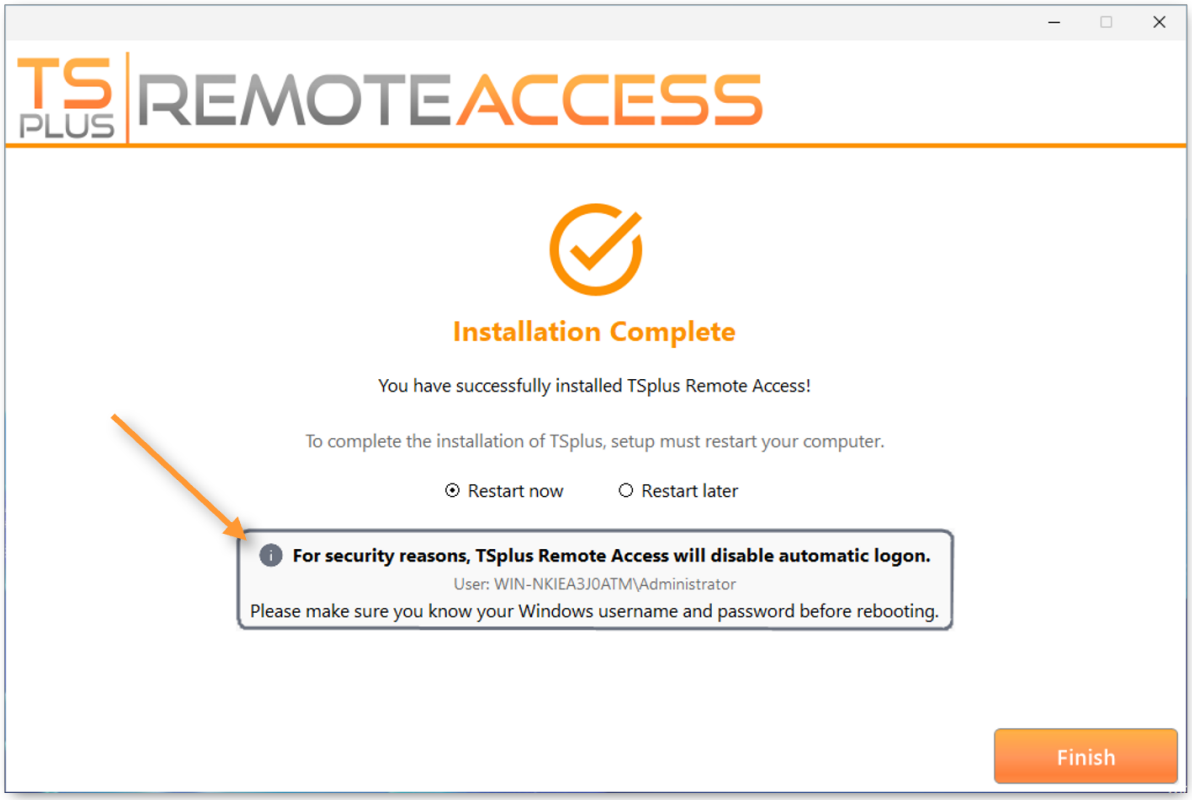
La barre de progression apparaît et vous permet de suivre l'avancement du processus :



- Depuis la version 11.40 de TSplus, vous aurez le choix d'installer TSplus Advanced Security notre puissant Add-On de Sécurité, dans sa version d'essai Ultimate (toutes les fonctionnalités de sécurité gratuites à utiliser pendant 2 semaines) pour votre système TSplus :

Pour plus d'informations sur ce produit, consultez les pages concernant TSplus Advanced Security. documentation .

Puis le logo TSplus apparaît et une fenêtre vous informe de l'achèvement de l'installation.

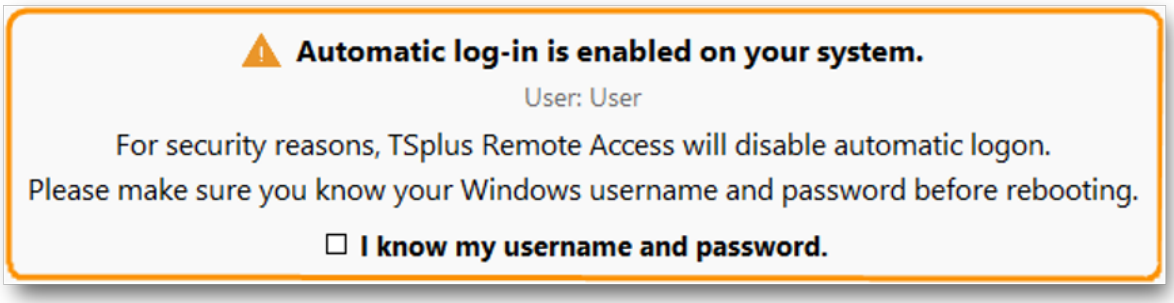


☐ **Avis important**

Pour des raisons de sécurité, **TSPlus Remote Access** vous devrez saisir manuellement votre nom d'utilisateur et votre mot de passe à chaque connexion.

Assurez-vous de connaître vos identifiants avant de redémarrer le système pour éviter d'être verrouillé.

Si
autologon
est activé sur le système, l'installateur affichera une fenêtre d'avertissement vous demandant de confirmer que vous connaissez votre nom d'utilisateur et votre mot de passe.



Pour utiliser TSplus, vous devez redémarrer votre système. La période d'essai offre un produit complet pendant 15 jours et 5 utilisateurs simultanés.

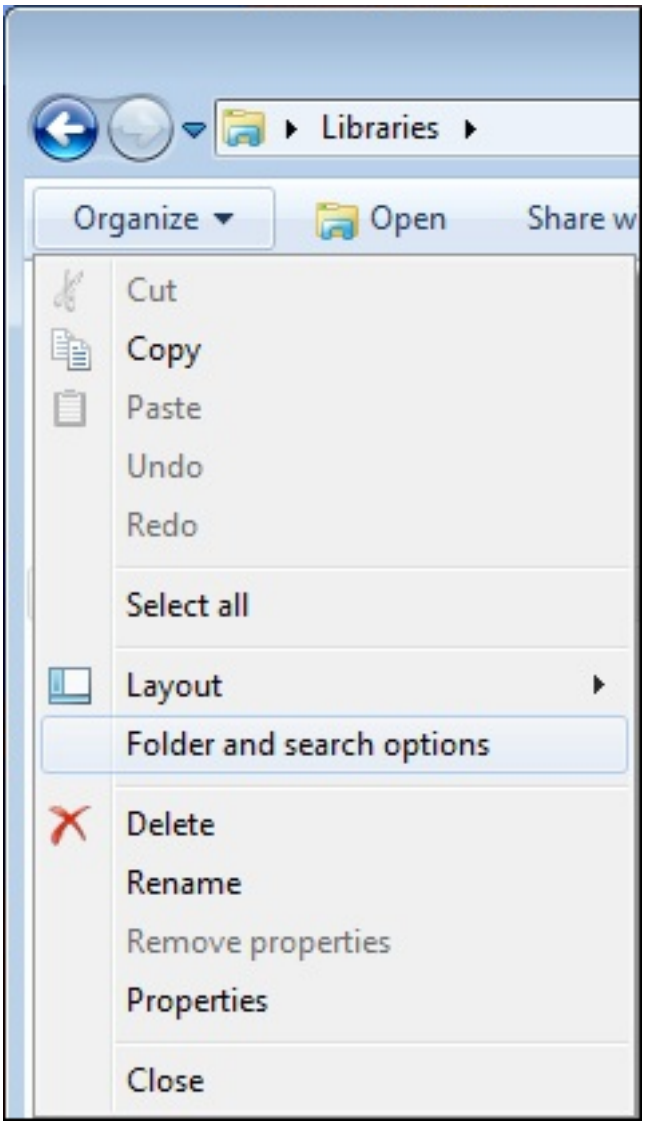
Comment monter un lecteur logique dans une session TSplus

Ce tutoriel couvrira les aspects suivants :

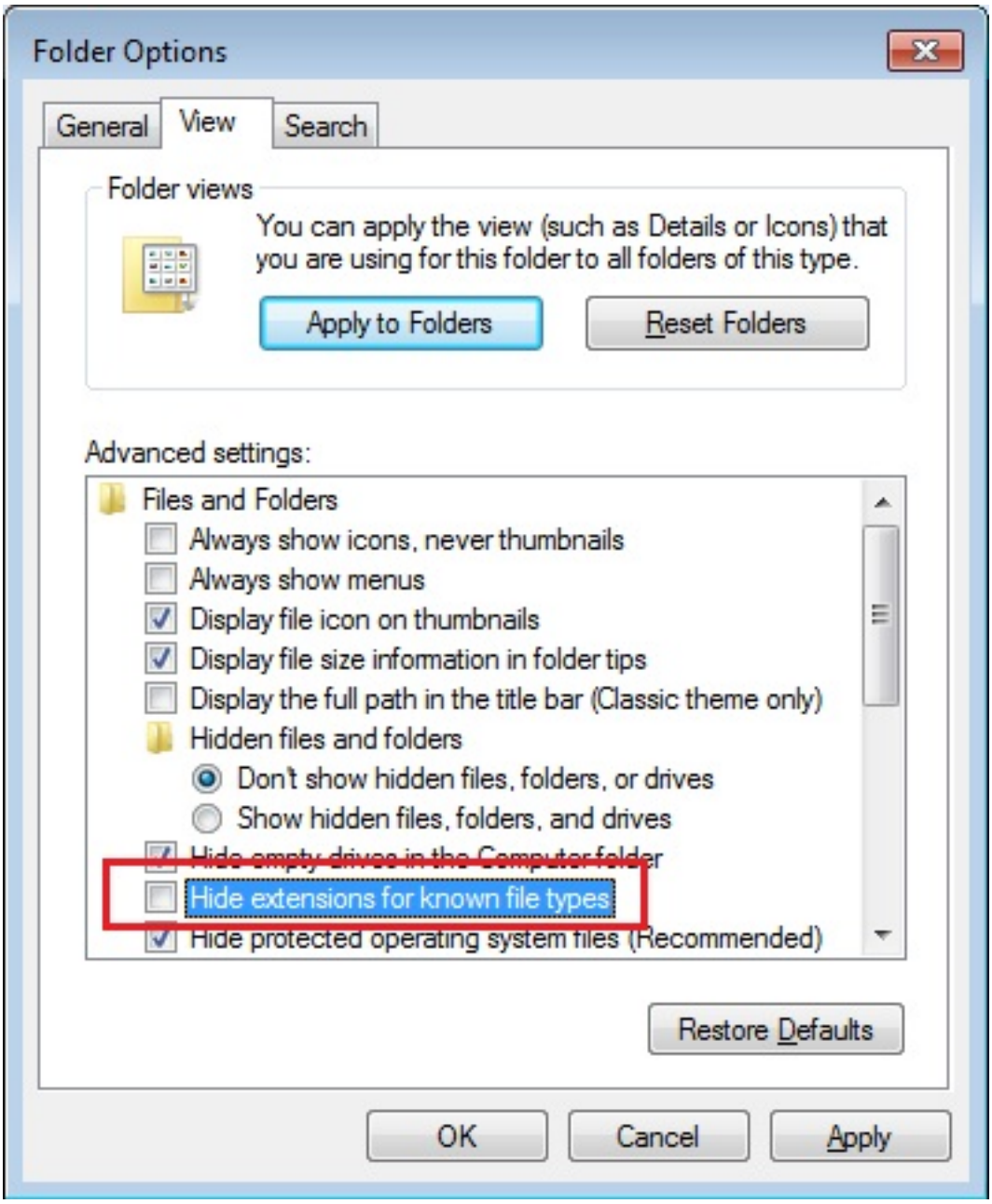
- Comment déployer un script de connexion et avoir plusieurs scénarios de scripts de connexion.
- Monter un dossier spécifique dans une session depuis le côté client ou serveur.

Si vous souhaitez publier un dossier sur un lecteur virtuel logique pour vos utilisateurs, suivez simplement cette procédure :

Avant de créer le script, ouvrez l'explorateur Windows et cliquez sur « Options des dossiers et de recherche ».



Ensuite, cliquez sur l'onglet Affichage et décochez la case "Masquer les extensions des types de fichiers connus" :

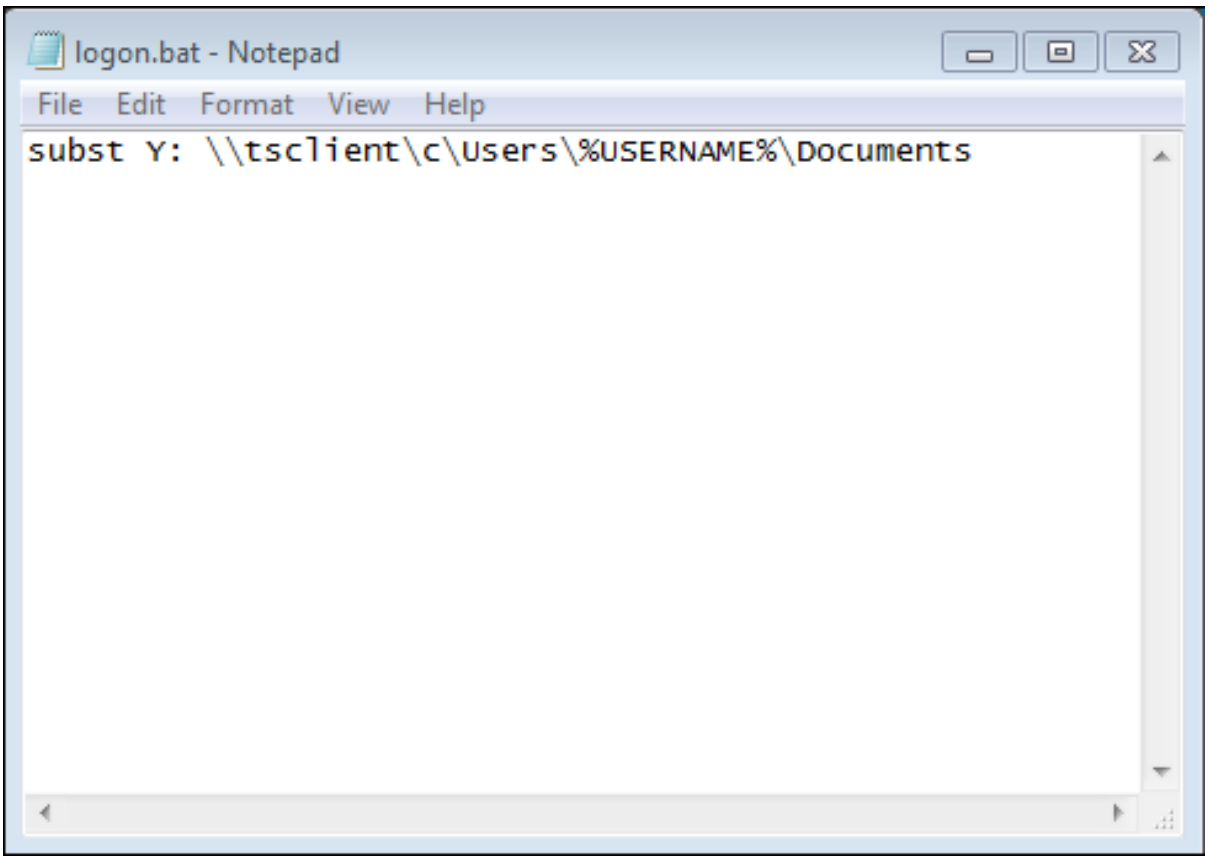


Créez un document texte et modifiez l'extension en le nommant « logon.bat » :



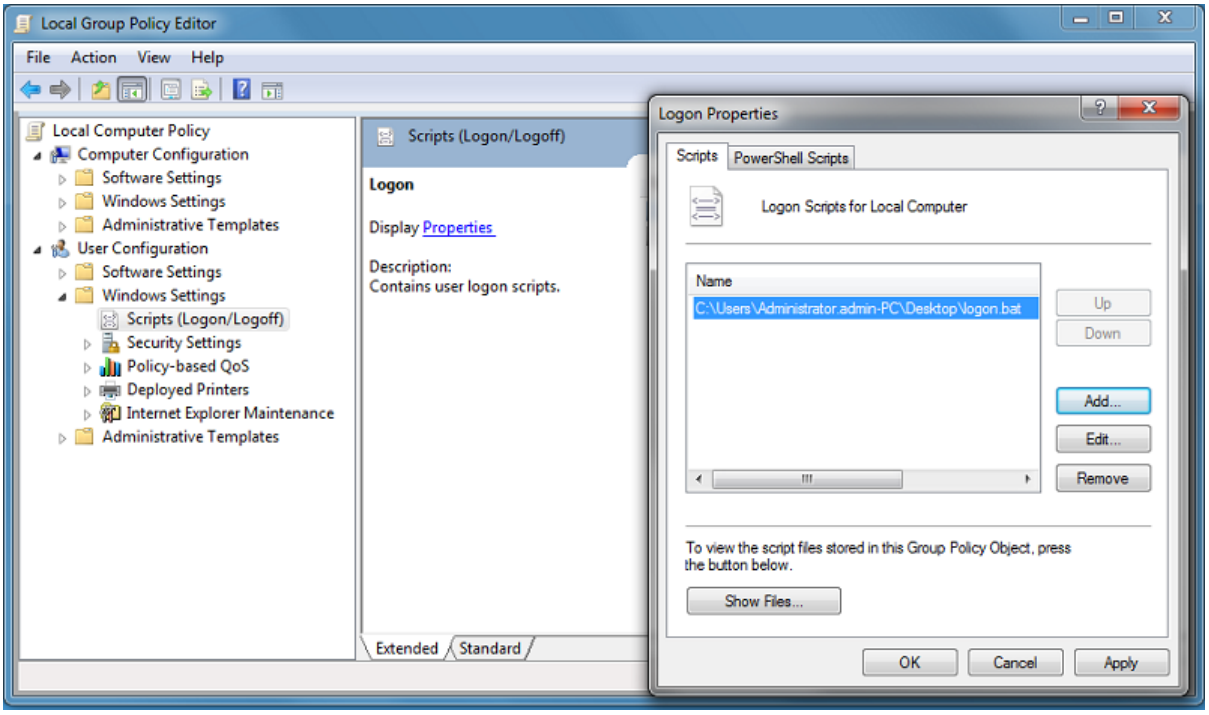
À l'intérieur du fichier, entrez par exemple cette commande pour publier le dossier Folder.exe :

subst Y: \tsclient\C\Users%USERNAME%\Documents

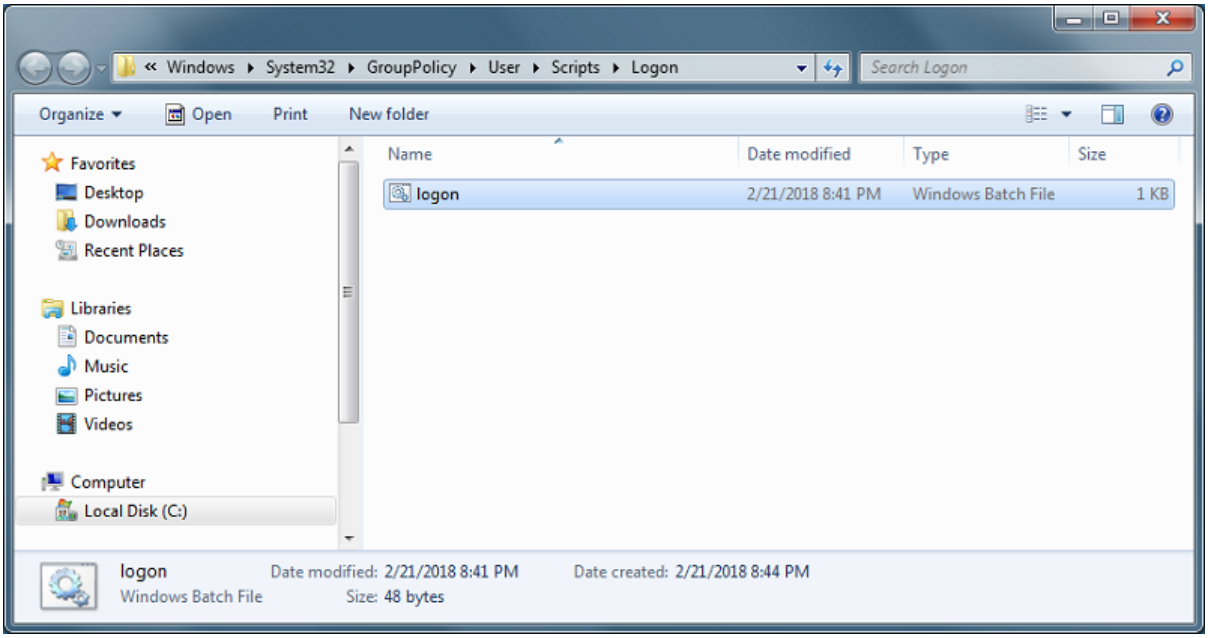


Ensuite, dans le menu de démarrage, tapez gpedit.msc dans la barre de recherche. Nous allons utiliser la stratégie locale afin que chaque utilisateur se connectant à ce serveur lance le script.

Allez dans le menu de configuration de l'utilisateur, puis dans les paramètres Windows, et enfin dans Scripts (Connexion/Déconnexion). Double-cliquez sur le script de connexion, puis cliquez sur "Ajouter", puis sur "Parcourir".

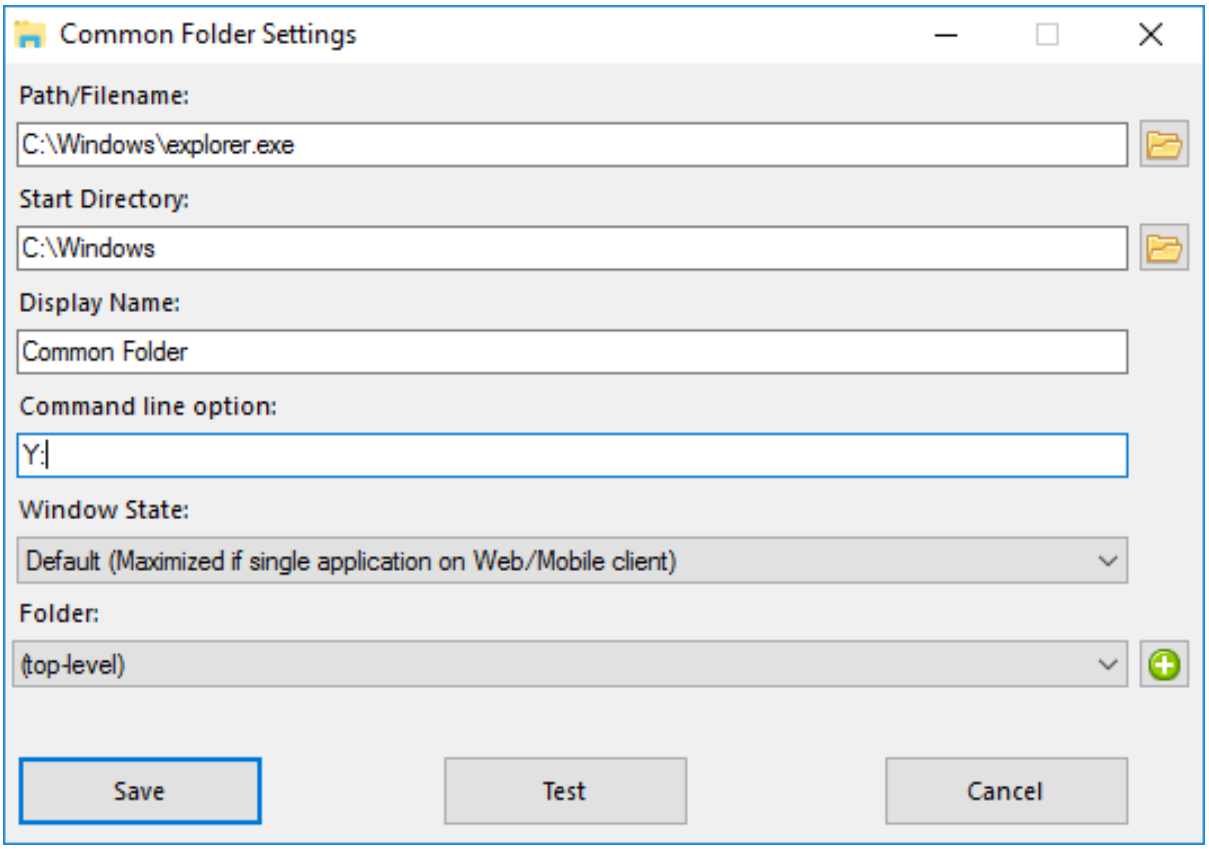


Ensuite, cliquez sur le bouton "Afficher les fichiers" dans la fenêtre des propriétés de connexion et copiez votre script logon.bat dans le chemin donné par l'éditeur de stratégie, c'est-à-dire : "C:\Windows\System32\GroupPolicy\User\Scripts\Logon"



- Vous pouvez copier ce fichier logon.bat dans C:\ProgramData si vous souhaitez que ce script soit exécuté pour tous vos utilisateurs.
- Si vous avez besoin d'un script de connexion spécifique pour chaque utilisateur, copiez le script dans C:\Users\Username\AppData\Roaming.

Maintenant, comment faire apparaître ce lecteur Y dans la session utilisateur ? Il existe plusieurs façons d'y parvenir. Vous pouvez créer une nouvelle application dans l'outil d'administration et l'assigner à vos utilisateurs, de cette façon le raccourci apparaîtra dans la session :


Common Folder Settings
Path/Filename:
C:\Windows\explorer.exe
Start Directory:
C:\Windows
Display Name:
Common Folder
Command line option:
Y:
Window State:
Default (Maximized if single application on Web/Mobile client)
Folder:
(top-level)
Save
Test
Cancel


CommonFolder

Si vous vous connectez à une session avec mstsc.exe, n'oubliez pas d'aller dans le menu des options, et dans l'onglet Ressources locales, sous Périphériques et ressources locaux, cliquez sur "Plus", puis cochez la case "Lecteurs".

Si vous souhaitez attribuer ce script uniquement aux utilisateurs non administrateurs, suivez ceci tutoriel .

Si vous souhaitez sécuriser l'accès d'un dossier, consultez notre documentation pour publier un dossier sécurisé .

Ticket de connexion et répartition de charge

Création de ticket de connexion sur le serveur Gateway

Vous pouvez créer un ticket de connexion sur le portail avec :

/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

Mais cela ne vous permettra de vous connecter que sur le serveur de passerelle lui-même.

Création de ticket de connexion sur un serveur d'application

Vous pouvez également créer un ticket de connexion sur un serveur d'application proxifié inverse avec :

/srv4/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

(en supposant que ~~srv4 est le nom interne du serveur d'application tel que configuré dans TSplus reverse-proxy)

Mais cela ne vous permettra de vous connecter qu'à ce serveur d'application spécifique.

Ticket de connexion et répartition de charge

Donc, si vous souhaitez utiliser des tickets de connexion et un équilibrage de charge, vous voudrez peut-être d'abord effectuer une requête HTTP supplémentaire :

https://your-gateway-server.com/cgi-bin/hb.exe?action=lb&l=LOGIN&d=DOMAIN&t=TIMESTAMP

Cela renverra une réponse comme celle-ci :

loadbalancing-on|SERVEUR D'APPLICATION 4|your-gateway-server.com/~~srv4|https|443|

Vous pouvez analyser cette réponse pour récupérer le serveur d'application sur lequel TSplus Load-Balancer vous recommanderait de connecter cet utilisateur spécifique.

c'est-à-dire qu'il recommandera le serveur le moins chargé de votre ferme TSplus, si les sessions persistantes sont activées sur votre portail TSplus, il prendra en compte les sessions actives existantes, etc.

Vous pouvez ensuite créer un ticket de connexion sur ce serveur d'application spécifique et vous y connecter en tant qu'utilisateur.

Ceci est précisément la requête http effectuée sur la page de connexion du portail Web TSplus.

Utiliser un ticket de connexion pour ouvrir une session utilisateur

Maintenant que vous avez un ticket de connexion valide, vous pouvez ouvrir une session utilisateur en utilisant ce ticket en ouvrant une fenêtre de navigateur à cette URL :

https://your-gateway-server.com/~~srv4/software/html5.html?user=*xxxxxxxx

où “xxxxxxxx” est le ticket de connexion.

Versions de support à long terme

Les clients qui se sont abonnés aux services de support et de mise à jour de TSplus et qui ne sont pas intéressés par les dernières fonctionnalités et améliorations de TSplus peuvent installer une version LTS (Support à long terme) de TSplus.

La version LTS (Support à Long Terme) de TSplus prolonge la période de maintenance du logiciel ; elle réduit également la fréquence des mises à jour du logiciel pour diminuer le risque, les coûts et les perturbations liées au déploiement du logiciel, tout en favorisant la fiabilité du logiciel.

De plus, TSplus LTS (Support à long terme) ne reçoit aucune nouvelle fonctionnalité.

TSplus cycle de vie

Les versions standard de TSplus sont publiées assez souvent et la dernière version est toujours la meilleure solution disponible pour nos clients : tous les bugs connus sont corrigés et de nouvelles fonctionnalités sont disponibles très souvent.

Une nouvelle version majeure de TSplus est publiée au début de chaque année.

À partir de janvier 2019, TSplus est également disponible dans une version de support à long terme, nommée « LTS ». Pour chaque nouvelle version majeure, TSplus publiera une version LTS stable de la version précédente qui sera supportée pendant 2 ans.

Avantages et limitations de TSplus LTS

TSplus LTS a plusieurs avantages :

- Aucune mise à jour sauf pour les corrections de sécurité et la compatibilité des mises à jour de Windows.
- Aucun changement de comportement et aucun changement de fonctionnalités lors de votre mise à jour.
- Moins de risques lors de la mise à jour entre deux versions mineures d'un LTS donné
- Supporté pendant au moins 2 ans

TSplus LTS a également des limitations et des contraintes :

- Le client doit acheter des services de support et de mise à jour (une licence ne peut pas être activée sans des services de support et de mise à jour actifs).
- Aucune nouvelle fonctionnalité (par rapport à la version standard de TSplus qui reçoit constamment de nombreuses mises à jour et nouvelles fonctionnalités)

Nous recommandons à nos clients d'utiliser la version standard de TSplus pour bénéficier de notre solution à la pointe de la technologie.

TSplus LTS Liens

TSplus LTS 18 pris en charge de 2026-01 à 2028-01 :

- Journal des modifications
- Configuration pour installer TSplus sur un nouveau serveur
- Mise à jour de la version pour mettre à jour une installation TSplus existante
- Documentation LTS18

TSplus LTS 17 pris en charge de 2025-01 à 2027-01 :

- Journal des modifications
- Configuration pour installer TSplus sur un nouveau serveur
- Mise à jour de la version pour mettre à jour une installation TSplus existante
- Documentation LTS17

TSplus LTS 16 (supporté de 2024-01 à 2026-01) : **Fin de support**

TSplus LTS 15 (supporté de 2023-01 à 2025-01) : **Fin de support**

TSplus LTS 14 (supporté de 2021-12 à 2023-12) : **Fin de support**

TSplus LTS 12 (supporté de 2019-12 à 2022-12) : **Fin de support**

TSplus LTS 11 (supporté de 2018-12 à 2021-12) : **Fin de support**

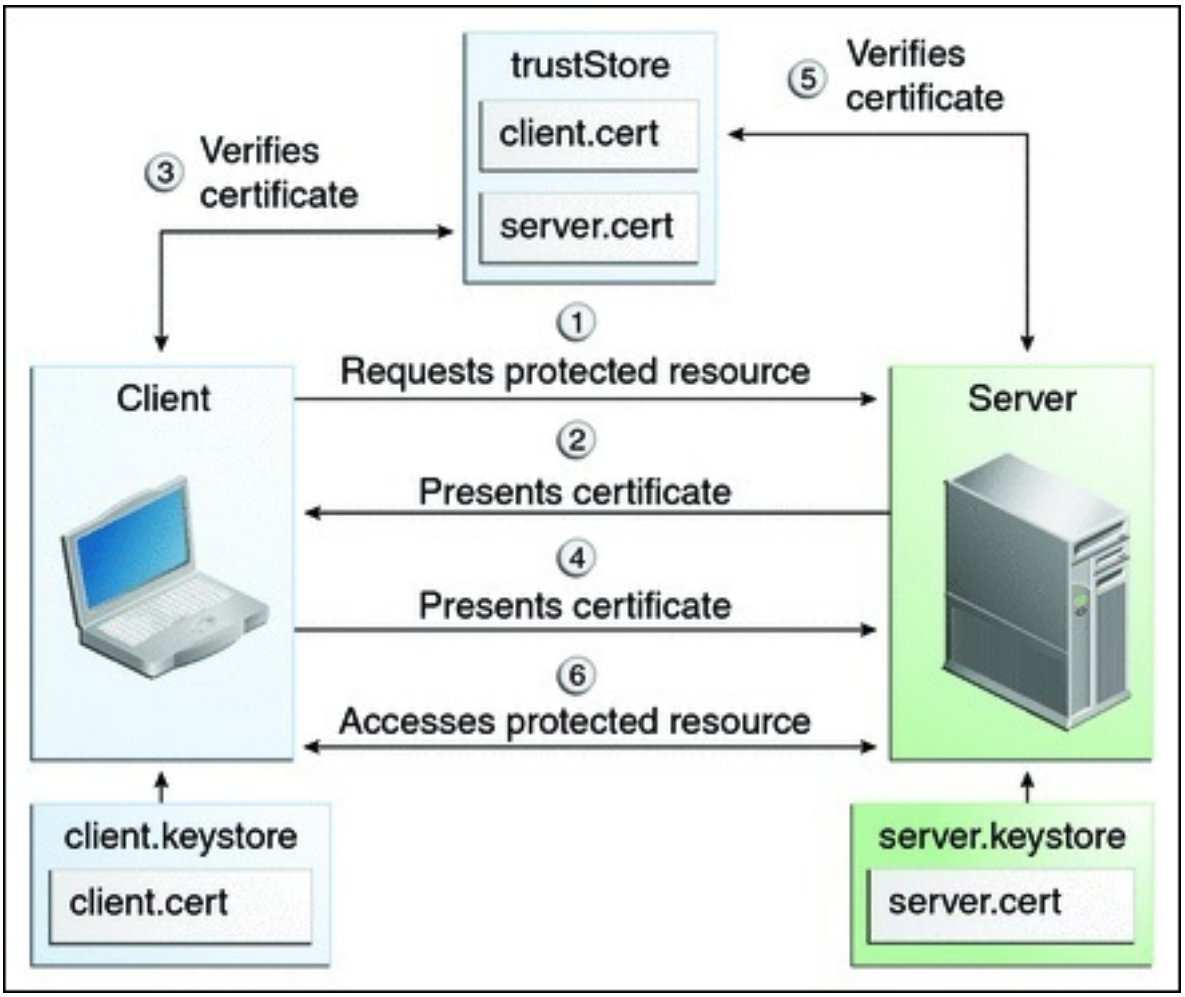
Activation de l'authentification SSL mutuelle

Qu'est-ce que l'authentification mutuelle ?

Beaucoup de gens s'attendent à une sécurité supplémentaire et l'authentification mutuelle est déjà prise en charge dans Terminal Service Plus. Elle est généralement mise en œuvre par des banques ou des organismes gouvernementaux.

Pour comprendre ce que c'est, nous pouvons le comparer à un processus SSL standard où vous ajouterez une vérification supplémentaire pour vérifier si le navigateur web de l'utilisateur autorise la connexion SSL. Vous savez ce qu'est votre certificat SSL côté serveur. Imaginez que le certificat est importé dans le navigateur web pour garantir que ce navigateur web spécifique est de confiance pour établir une connexion. Dans la première étape de communication, le navigateur web agit en tant que client et dans la deuxième étape, c'est l'inverse. À la fin, les deux parties, le navigateur web client et le serveur web, ont accepté l'autorité et la connexion peut commencer.

Une définition plus complète : L'authentification mutuelle SSL ou l'authentification mutuelle basée sur des certificats fait référence à deux parties s'authentifiant mutuellement en vérifiant le certificat numérique fourni afin que les deux parties soient assurées de l'identité de l'autre. En termes technologiques, cela fait référence à un client (navigateur web ou application cliente) s'authentifiant auprès d'un serveur (site web ou application serveur) et ce serveur s'authentifiant également auprès du client en vérifiant le certificat de clé publique/certificat numérique émis par les autorités de certification de confiance (CA). Parce que l'authentification repose sur des certificats numériques, les autorités de certification telles que Verisign ou Microsoft Certificate Server sont une partie importante du processus d'authentification mutuelle.



Activer sur TSplus

Le serveur web intégré de TSplus permet de configurer une authentification mutuelle.

Pour activer l'authentification mutuelle, suivez ce processus :

Vous devrez installer la dernière version du Kit de développement Java (JDK), disponible sur http://java.com > Téléchargements > JDK.

1. Créer et modifier avec Notepad le fichier suivant : C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin

Ajoutez ces 3 lignes :

disable_http_only=true disable_print_polling=true force_mutual_auth_on_https=true

2. Supprimer cert.jks

Dans “C:\Program Files (x86)\TSplus\Clients\webserver”, vous verrez le fichier cert.jks. Copiez-le dans “C:\Program Files (x86)\TSplus\Clients”. Supprimez “C:\Program Files (x86)\TSplus\Clients\webserver\cert.jks”.

3. Créer le fichier batch

Dans ‘C:\Program Files (x86)\TSplus\Clients’, créez un fichier batch, par exemple “createcertuser.bat” avec ces paramètres :

@rem décommentez la ligne suivante si vous souhaitez générer un nouveau certificat auto-signé cert.jks @rem keytool -genkey -v -alias jwts -keyalg RSA -validity 3650 -keystore cert.jks -storepass secret -keypass secret -dname “CN=localhost, OU=my_ou, O=my_org, L=my_city, ST=my_state, C=MY” @keytool -genkey -v -alias AliasUser1 -keyalg RSA -storetype PKCS12 -keystore forBrowserUser1.p12 -dname “CN=some_name, OU=some_ou, O=some_org, L=Paris, ST=FR, C=FR” -storepass mypassword -keypass mypassword @keytool -export -alias AliasUser1 -keystore forBrowserUser1.p12 -storetype PKCS12 -storepass mypassword -rfc -file forCertUser1.cer @keytool -alias AliasCertUser2 -import -v -file forCertUser1.cer -keystore cert.jks -storepass secret @del forCertUser1.cer

Cela importera automatiquement la paire de clés de certificat depuis le navigateur web dans "cert.jks" après avoir créé sa paire de clés de navigateur.

4. Restaurer le nouveau fichier “cert.jks” modifié

Copiez “C:\Program Files (x86)\TSplus\Clients\cert.jks” dans “C:\Program Files (x86)\TSplus\Clients\webserver” et redémarrez les serveurs Web.

5. Importation et test de certificat

Le fichier d'exemple fourni devrait avoir généré un fichier de test “BrowserUser1.p12”. Lorsque vous ouvrirez l'adresse HTTPS, vous recevrez un message de sécurité et vous ne pourrez pas accéder aux pages du serveur Web. Avec Chrome ou IE, vous pouvez cliquer sur ce fichier ‘BrowserUser1.p12’ pour importer le certificat dans le magasin de clés par défaut de Windows. Avec FireFox, vous devez aller dans les paramètres et importer ce fichier “BrowserUser1.p12” dans votre dossier de certificats.

Dès que vous l'avez correctement importé, vous pourrez accéder à l'adresse HTTPS.

L'administrateur peut créer un fichier de paire de clés séparé pour chaque utilisateur.

Par exemple :

forBrowserUser1.p12 forBrowserUser2.p12 forBrowserUser3.p12

Et il peut exporter ces certificats dans cert.jks. S'il souhaite désactiver l'accès à un utilisateur, il lui suffira de supprimer cet utilisateur de "cert.jks". Ce faisant, l'utilisateur perdra son autorisation et ne pourra plus accéder au serveur web.

Cette authentification mutuelle n'affecte que les connexions HTTPS et la connexion HTTP sera interdite avec la ligne de commande : settings.bin>disable_http_only=true

Ouvrir des fichiers sur le côté client

Aperçu

Cette fonctionnalité est puissante. Elle permet d'ouvrir des documents situés sur le serveur du côté client en fonction de son extension de fichier.

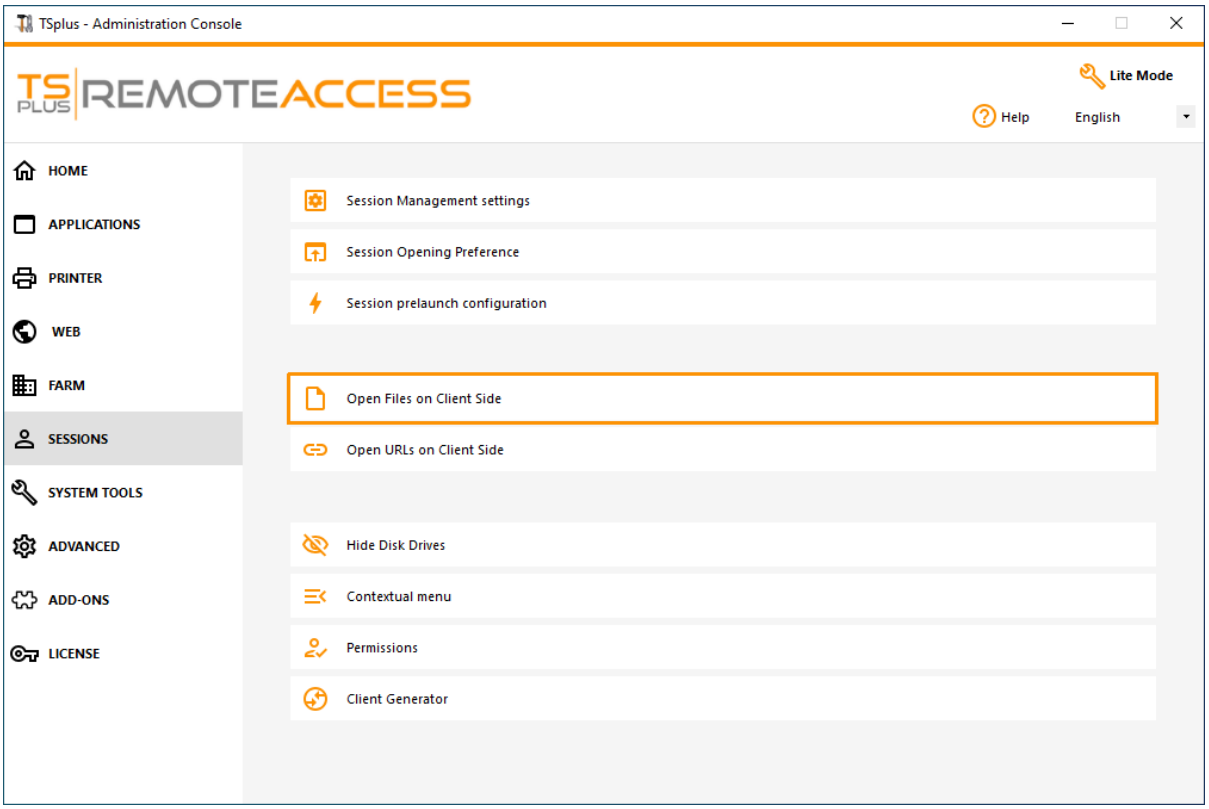
Par exemple, vous pouvez ouvrir un document Microsoft Office Word sans avoir Office installé sur votre serveur.

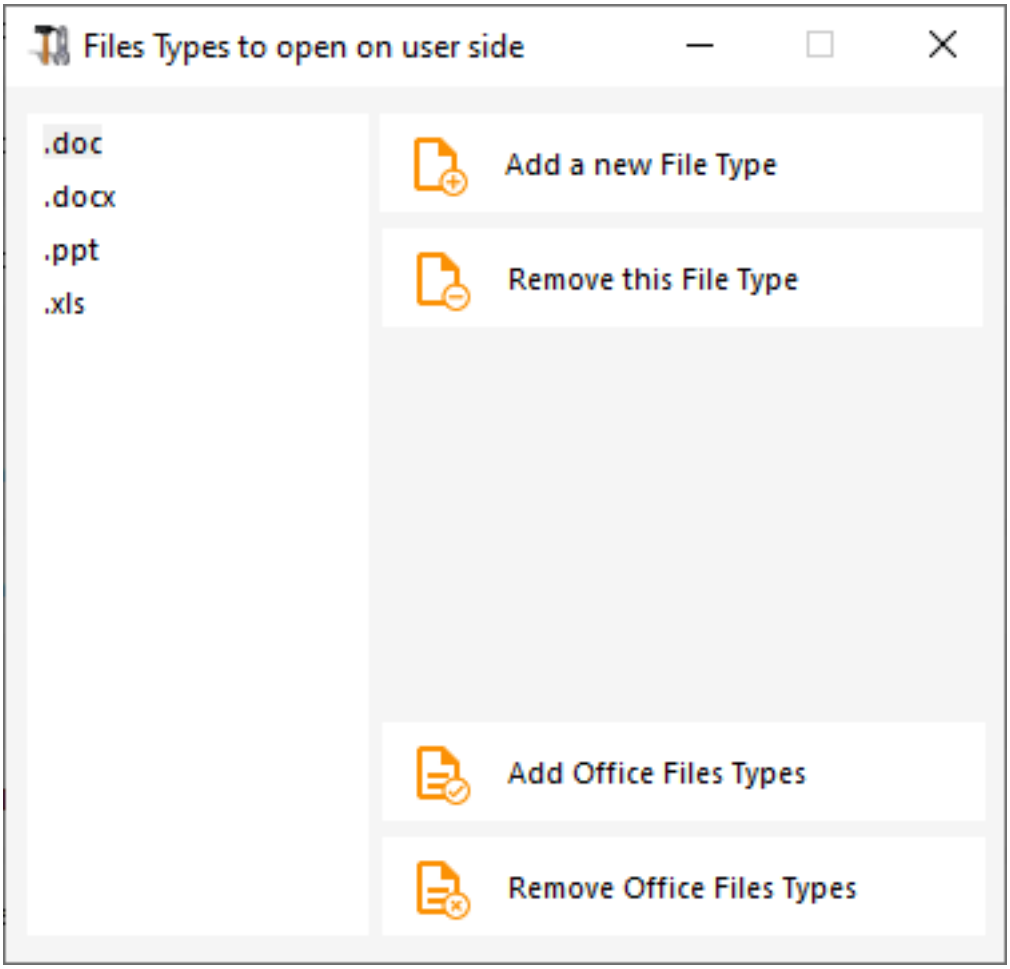
Le document .docx (ou .xlsx) est automatiquement téléchargé du côté de l'utilisateur où la version locale d'Office sera utilisée pour l'ouvrir.

Si vous hébergez votre application sur un serveur Cloud et si votre application génère un document Excel, Access ou Word, cette fonctionnalité évite de se soucier des licences Office sur le serveur.

Configurer un type de fichier à ouvrir du côté client

Le titre « Ouvrir des fichiers sur le côté client » se trouve dans l'onglet « Sessions - Paramètres » de l'AdminTool. Cliquez dessus pour afficher la fenêtre de configuration :





Le bouton « Ajouter un nouveau type de fichier » vous permet d'ajouter une extension (comme

« .docx » pour Microsoft Office Word 2007-2010) à la liste.

Tous les fichiers ayant une extension dans cette liste seront ensuite ouverts côté client. à condition d'utiliser l'un des clients de connexion de Terminal Service Plus :

- Tout client généré de Terminal Service Plus (RemoteApp ou RDP)
- Toute connexion Windows depuis le portail Web de Terminal Service Plus
- Toute connexion HTML5 depuis le portail Web de Terminal Service Plus

Avertissement : cette fonctionnalité n'est pas prise en charge pour :

- Tout client RDP (mstsc par exemple)

Dépannage

Si vous avez configuré un type de fichier pour s'ouvrir sur le côté client, et que cela ne fonctionne pas (c'est-à-dire que le fichier s'ouvre toujours sur son propre ordinateur), nous vous conseillons de vérifier la liste "Ouvrir avec" dans le menu contextuel de Windows :

- clic droit sur le fichier.
- cliquez sur l'élément de menu « Ouvrir avec ».
- si plusieurs applications figurent dans cette liste, cliquez sur « Choisir le programme par défaut » et sélectionnez « OpenOnClient.exe ».

Cet outil Terminal Service Plus applique sa configuration à tous les utilisateurs utilisant l'ordinateur, cependant veuillez garder à l'esprit les règles suivantes :

- Windows permet à chaque utilisateur de changer ce programme d'ouverture par défaut avec un autre programme de son choix.
- En utilisant le client de connexion HTML5, le fichier sera téléchargé et géré par le navigateur local. Certains navigateurs traitent certains types de fichiers de manière spécifique, il est donc également conseillé de vérifier deux fois les paramètres du navigateur.

Ces règles expliquent la plupart des problèmes lors de l'utilisation de la fonctionnalité Open On Client, c'est pourquoi nous vous conseillons de commencer par vérifier le programme par défaut :

- pour l'utilisateur connecté sur le serveur
- pour l'utilisateur sur le client
- pour le navigateur sur le client (lors de l'utilisation de HTML5)

Ouvrir des URL du côté client

Aperçu

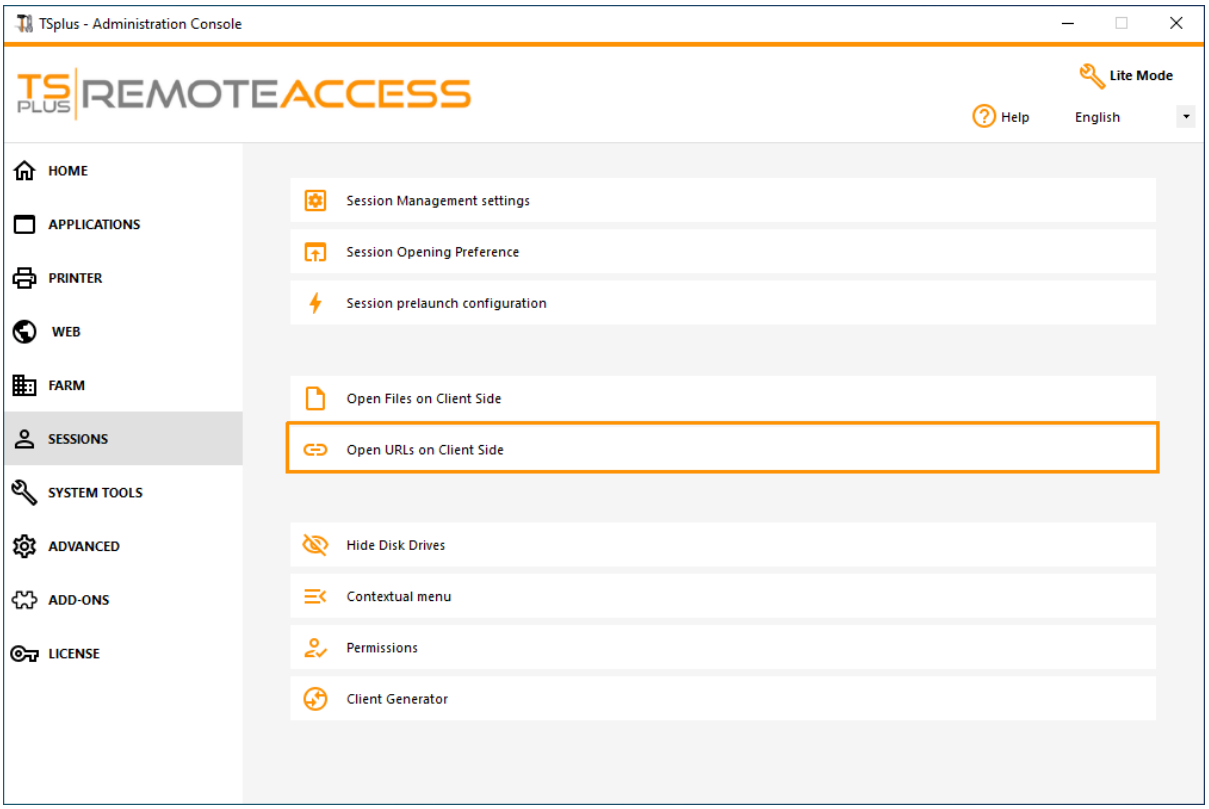
Cette fonctionnalité est puissante. Elle permet d'ouvrir du côté client tous les liens de sites web et les raccourcis de sites web situés sur le serveur.

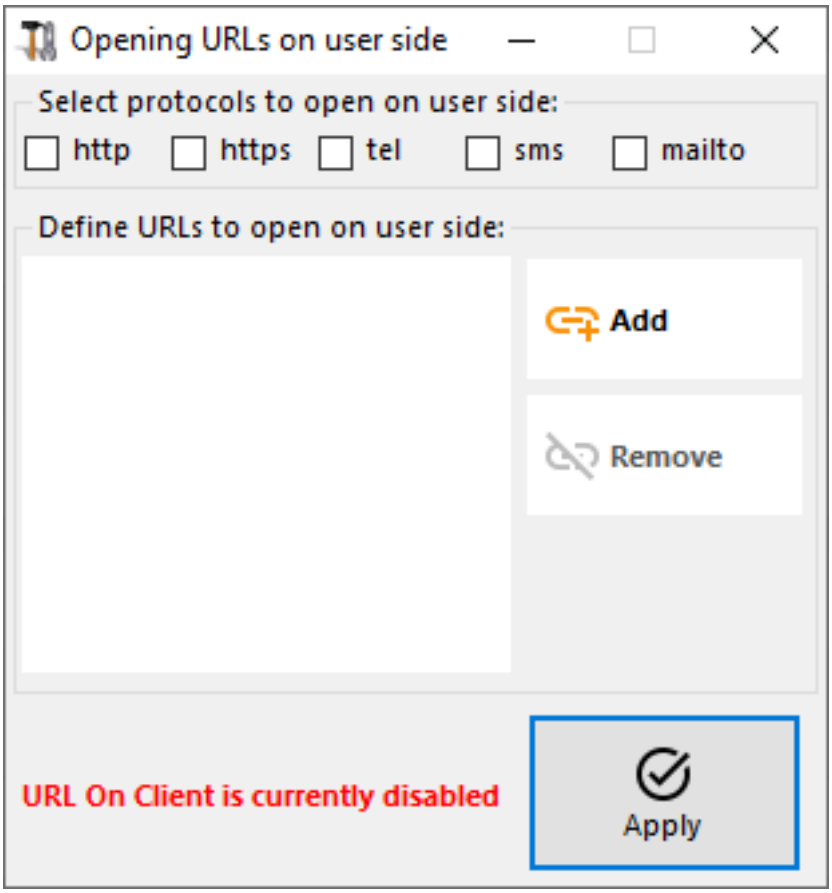
Par exemple, vous pouvez ouvrir des vidéos YouTube directement sur le client, ce qui permet d'économiser beaucoup de bande passante et de puissance CPU sur votre serveur.

L'adresse web (URL) est automatiquement transférée du côté de l'utilisateur où le navigateur par défaut local sera utilisé pour l'ouvrir.

Activer cette fonctionnalité sur un serveur

Le carrelage « Ouvrir les URL côté client » se trouve dans l'onglet « Sessions - Paramètres » de l'AdminTool. Cliquez dessus pour afficher la fenêtre de configuration :





Les cases des protocoles Http et https ne sont pas cochées par défaut.
Vous pouvez également activer les protocoles tel, sms et mailto en cochant les cases correspondantes.

Puis cliquez sur le bouton « Appliquer », qui vous permet d'activer cette fonctionnalité pour tous les utilisateurs sur le serveur.

Pour activer pleinement cette fonctionnalité, chaque utilisateur devra redémarrer sa session (déconnexion puis connexion) avant de pouvoir utiliser cette fonctionnalité.

Tous les liens web et raccourcis s'ouvriront alors du côté client. à condition d'utiliser l'un des clients de connexion de Terminal Service Plus :

- Tout client généré de Terminal Service Plus (RemoteApp ou RDP)
- Toute connexion Windows depuis le portail Web de Terminal Service Plus
- Toute connexion HTML5 depuis le portail Web de Terminal Service Plus.

Avertissement : cette fonctionnalité n'est pas prise en charge pour :

- Tout client RDP (mstsc par exemple).

Comportement du navigateur Web (Portail Web) :

Certains navigateurs web — en particulier sur les appareils iOS — ne permettent pas d'ouvrir automatiquement des liens depuis notre application. Dans ces cas, un lien cliquable est affiché afin que les utilisateurs puissent accéder manuellement à la destination souhaitée.



Changer le navigateur web par défaut du serveur

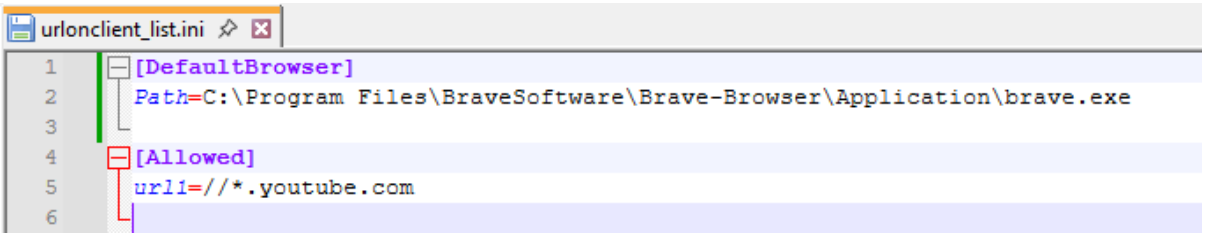
Tous les URL qui ne sont pas définis pour être ouverts du côté client continueront à être ouverts

du côté serveur, en utilisant Microsoft Edge ou Internet Explorer. Si vous souhaitez changer le navigateur web par défaut utilisé du côté serveur, vous devez modifier le fichier de configuration. **urlonclient_list.ini** situé dans le dossier d'installation de TSPlus.

L'emplacement exact (en fonction de votre chemin d'installation exact) devrait être : C:\Program Files (x86)\TSplus\UserDesktop\files\urlonclient_list.ini .

Vous devez ajouter une nouvelle section "DefaultBrowser" dans le fichier, et une entrée "Path" avec la valeur du chemin du navigateur web que vous souhaitez. Comme ceci :

[DefaultBrowser]
Path=C:\Path\To\Your\Favorite\WebBrowser.exe



Définir le navigateur par défaut sur Brave

☐ **Si vous avez remplacé firefox.exe par c:\wsession\URLonClient.exe**

et vous souhaitez que Firefox soit votre navigateur web par défaut côté serveur :

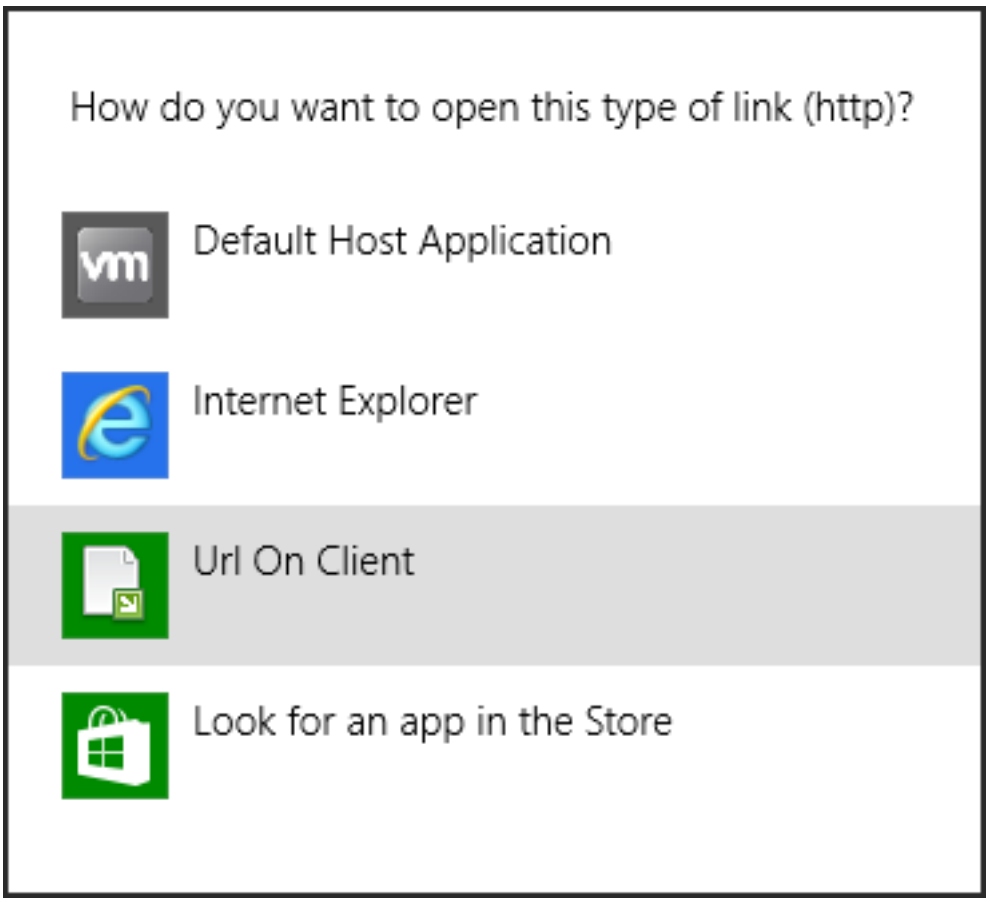
- Renommez le fichier ancien firefox.exe en firefox-real.exe.
- utilisez le nouveau nom exécutable dans le **urlonclient_list.ini** fichier :

```
[DefaultBrowser]
Path=C:\Program Files\Mozilla Firefox\firefox-real.exe
```

Windows 8 et 8.1

À partir de Windows 8, Microsoft a interdit le changement automatique du navigateur par défaut de l'utilisateur.

C'est pourquoi, une fois la fonctionnalité activée sur le serveur, chaque utilisateur devra choisir 'Url On Client' lorsqu'on lui demandera un navigateur par défaut.



Cette fenêtre ne sera affichée que la première fois qu'un utilisateur ouvre un lien web.

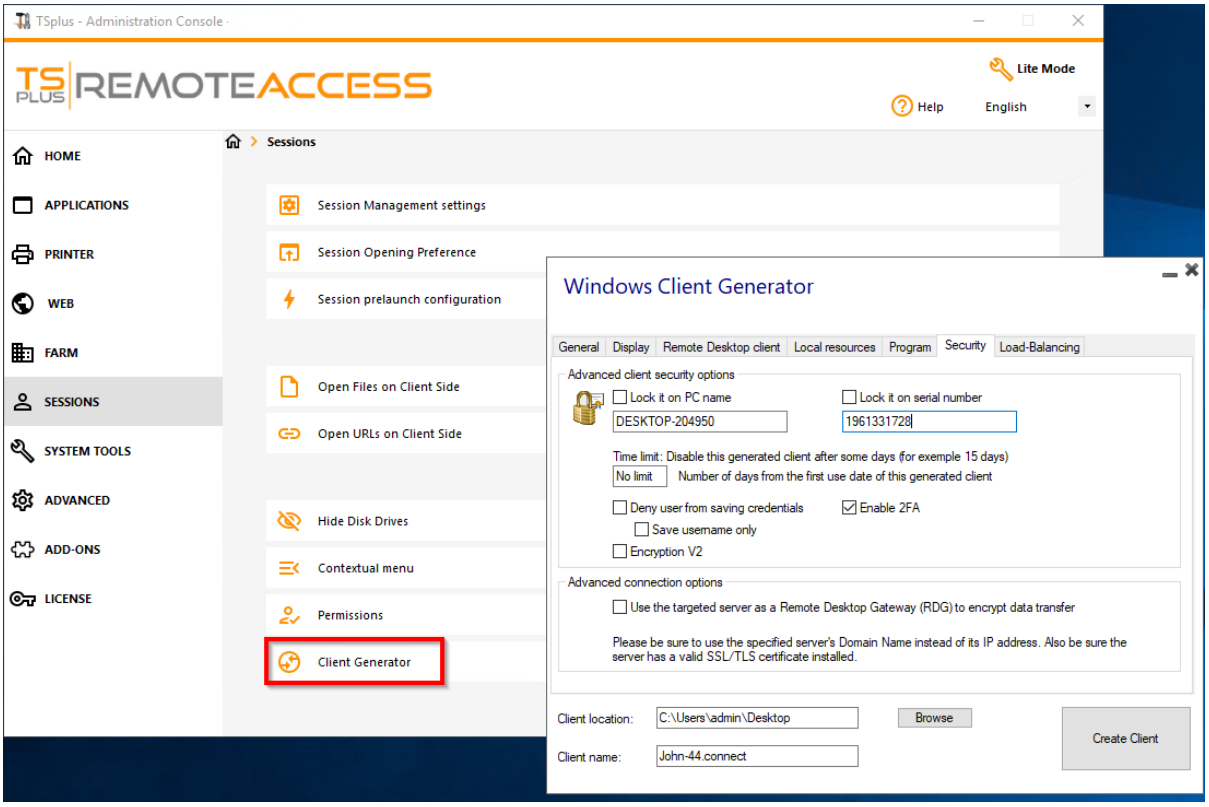
Malheureusement, c'est la politique de Microsoft Windows et nous ne sommes pas au courant d'une solution de contournement.

Générateur de client portable

TSplus crée par défaut une icône pour le Générateur de Client Portable :



Il peut également être accessible dans l'onglet Sessions de l'AdminTool :



Il vous permet de créer 2 types de clients de connexion qui peuvent être copiés sur le Bureau

des utilisateurs ou sur une clé USB pour une utilisation portable.

Remarque Les clients de connexion ne sont pas compatibles avec les ordinateurs Mac.

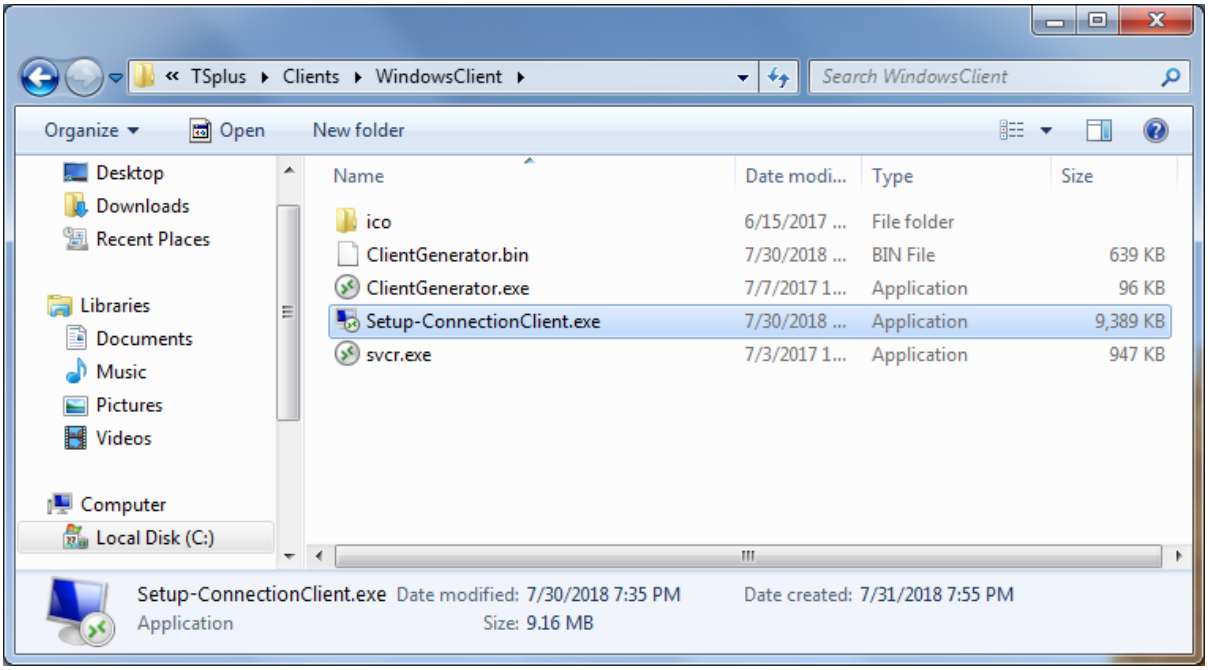
Depuis la version 11.40 de TSplus, le générateur de clients a été repensé pour être numériquement signé et éviter les réactions faussement positives des antivirus.

Au lieu d'un programme ".exe", le nouveau générateur de client crée un fichier plat chiffré avec l'extension ".connect" :

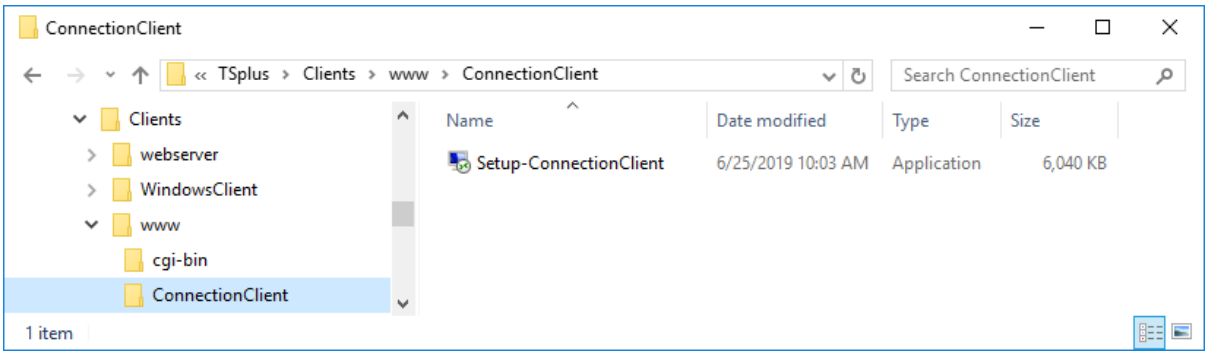


Pré-requis côté client

Sur le côté client, chaque utilisateur devra exécuter un programme signé nommé « Setup-ConnectionClient.exe » en tant que pré-requis. Ce programme est disponible sur votre serveur, dans le dossier du programme TSplus : TSplus\Clients\WindowsClient :



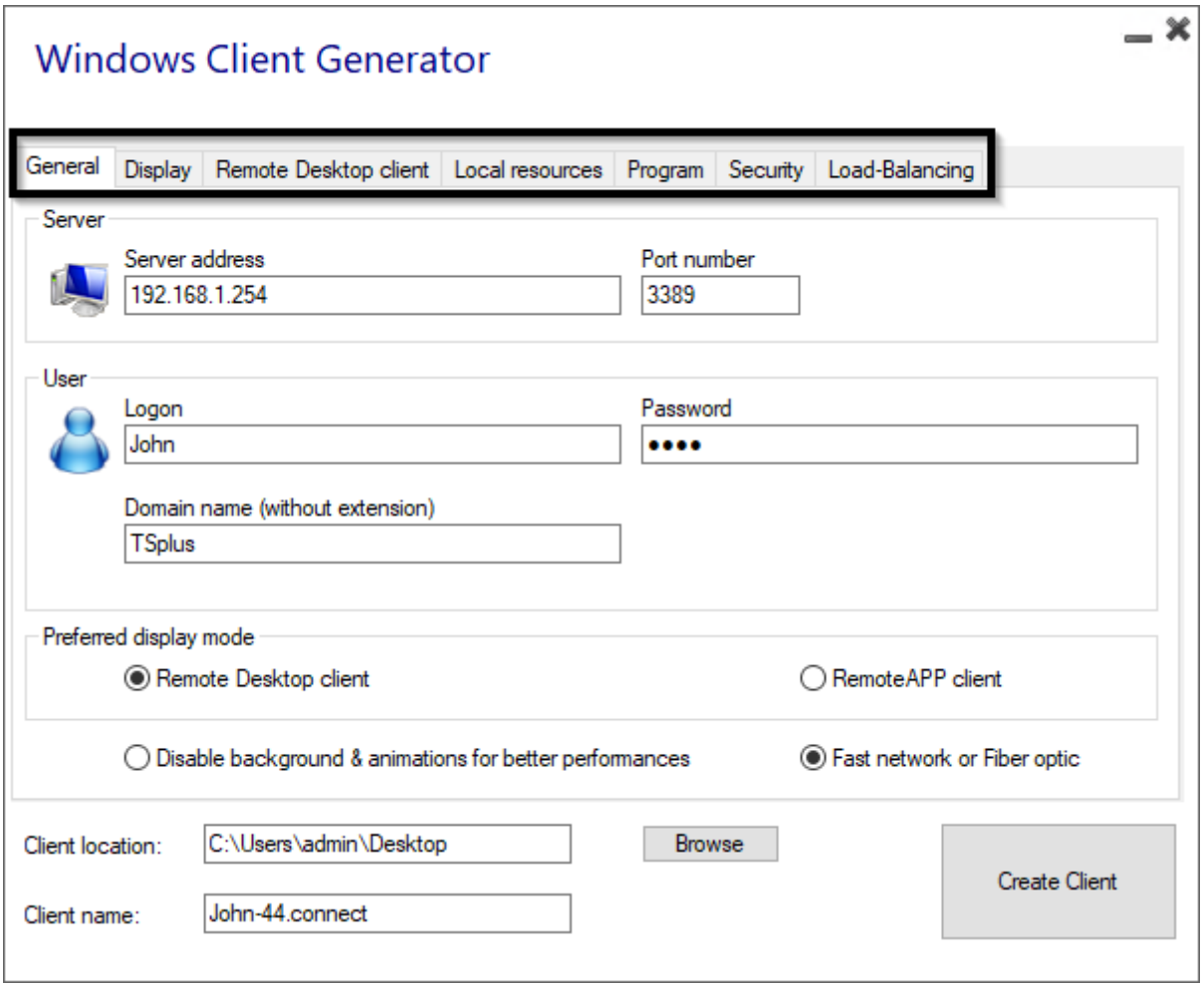
ou dans le dossier TSplus\Clients\www :



ou par téléchargement .

Aperçu détaillé

Cliquez sur **un onglet** aller à l'information correspondante :



Lorsque vous lancez le générateur de client, le premier onglet affiché est l'onglet général. Ici, vous trouverez tous les paramètres de connexion essentiels dont vous avez besoin pour

commencer.

- **Adresse du serveur :** Entrez l'adresse IP du serveur auquel vous souhaitez que le client se connecte.
- **Numéro de port :** Entrez le numéro de port du serveur. La valeur par défaut est 3389.
- **Nom d'utilisateur et mot de passe :** Si vous entrez un nom d'utilisateur et un mot de passe, le programme client ne demandera pas à l'utilisateur de le retaper à chaque session.

Pour réinitialiser cette sauvegarde de connexion/mot de passe, vous devez créer et modifier un raccourci du Client Bureau à distance et ajouter le - réinitialiser activé commutateur à la fin du champ cible.

Identifiants

- Si vous ne souhaitez pas enregistrer les identifiants, entrez "nosavecredential" dans le champ de connexion du Générateur de Client Portable.
- Si vous ne souhaitez pas afficher la fenêtre de connexion avec le nom d'utilisateur, le mot de passe et le nom de domaine, il vous suffit d'entrer "nopassword" dans le champ du mot de passe.
- Si vous souhaitez activer l'autologon, entrez *SSO dans le champ du nom d'utilisateur, le programme client demandera simplement le nom d'utilisateur et le mot de passe lors de la toute première connexion. Il enregistrera ces informations sur le poste de travail de l'utilisateur afin que celui-ci n'ait plus jamais à s'identifier.
- Si vous souhaitez que le nom de l'utilisateur local actuel soit affiché comme identifiant de connexion pour la session, entrez **, ou %USERNAME% dans le champ de connexion.

- **Nom de domaine :** Entrez un nom de domaine le cas échéant.
- **Mode d'affichage préféré :** Vous pouvez choisir votre mode d'affichage préféré parmi les options suivantes :
  - Le Classic Remote Desktop , affichant votre environnement de session à distance.

- Le Client de connexion Microsoft RemoteApp pour afficher vos applications distantes comme si elles étaient installées localement. Il offre de meilleures performances graphiques par rapport aux applications minimisées.

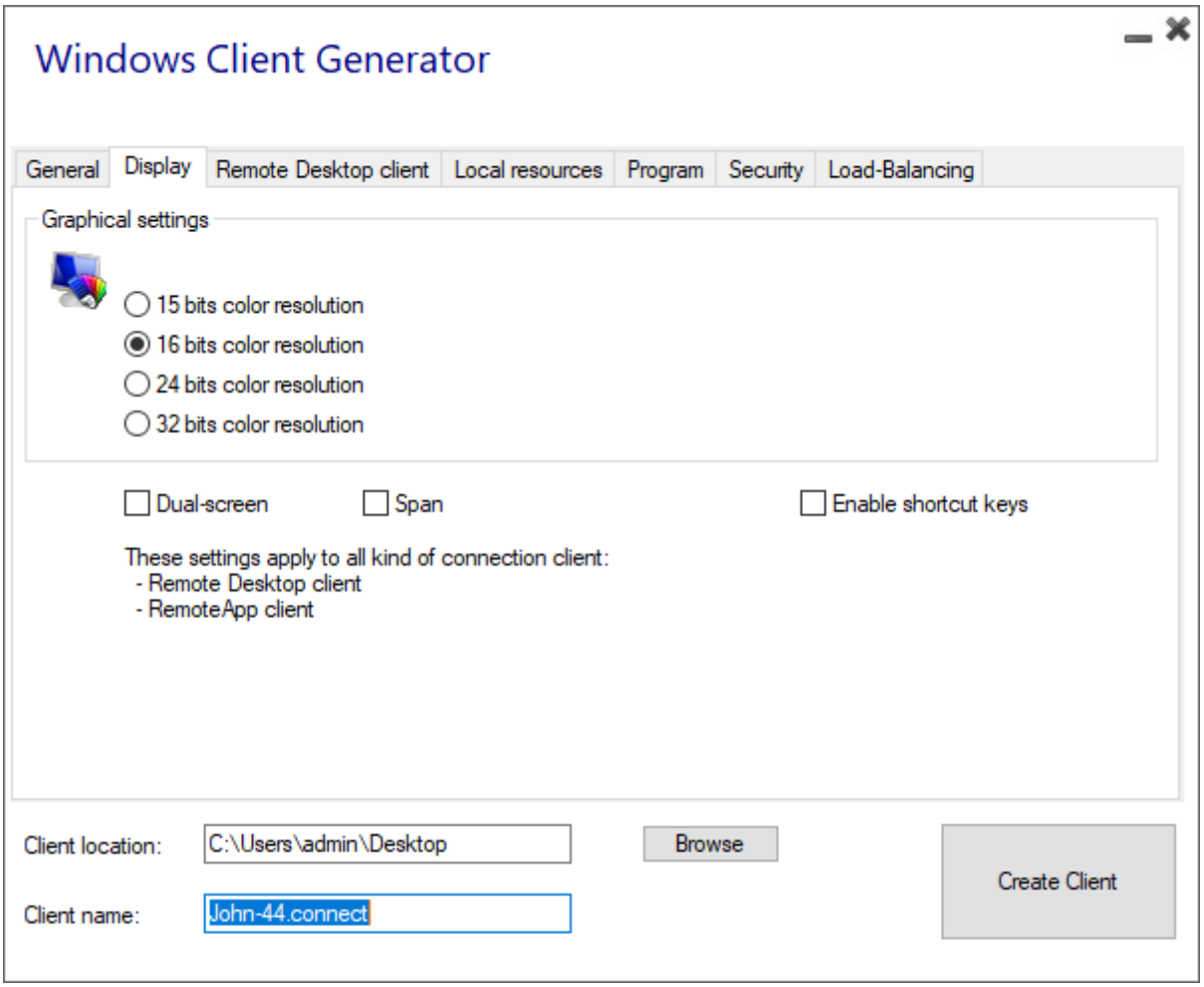
- **Vitesse du réseau** Vous pouvez choisir entre deux options en fonction de la vitesse de votre réseau :

  - Désactiver l'affichage en arrière-plan et les animations graphiques pour les réseaux à faible vitesse.

  - Activer l'affichage en arrière-plan et les animations graphiques pour la fibre optique ou un réseau rapide.

- **Emplacement du client :** Définissez l'emplacement de votre client généré.

- **Nom du client :** Vous pouvez nommer votre client comme vous le souhaitez.

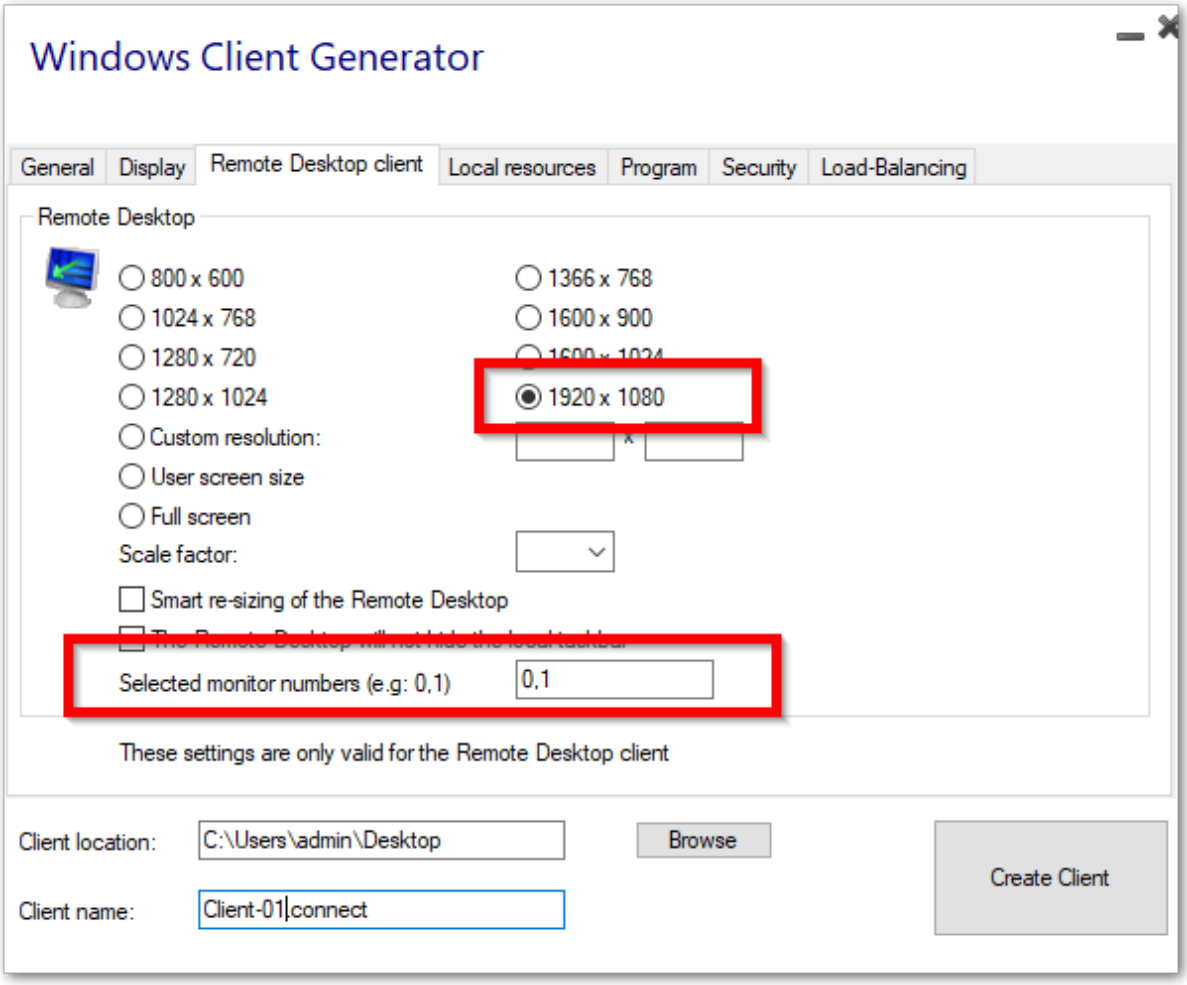


Sur cet onglet, vous pouvez changer la couleur et la résolution de l'écran de session.

Vous pouvez également adapter votre session pour des écrans doubles, avec ou sans étirement. L'option d'étirement vous permet d'étendre votre session sur les deux écrans.

Vous pouvez autoriser l'utilisation de la touche TAB dans la session.

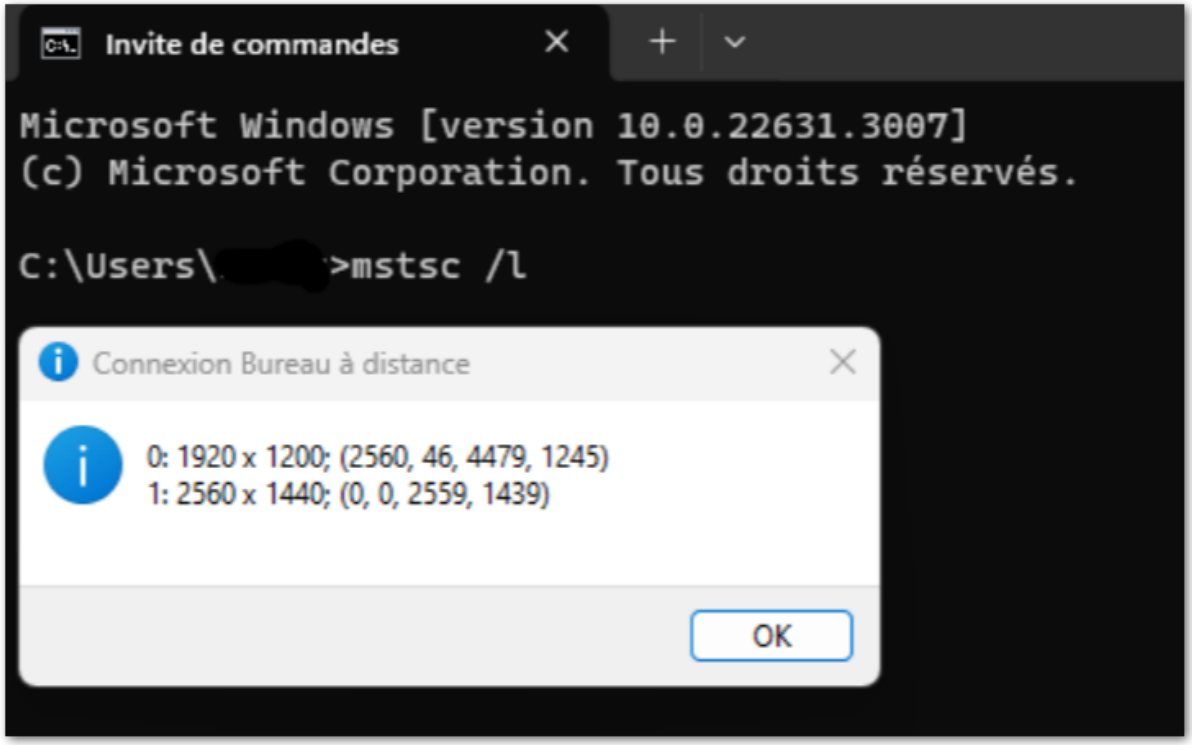
Sur cet onglet, vous pouvez choisir quelle résolution vous souhaitez activer pour l'utilisateur :



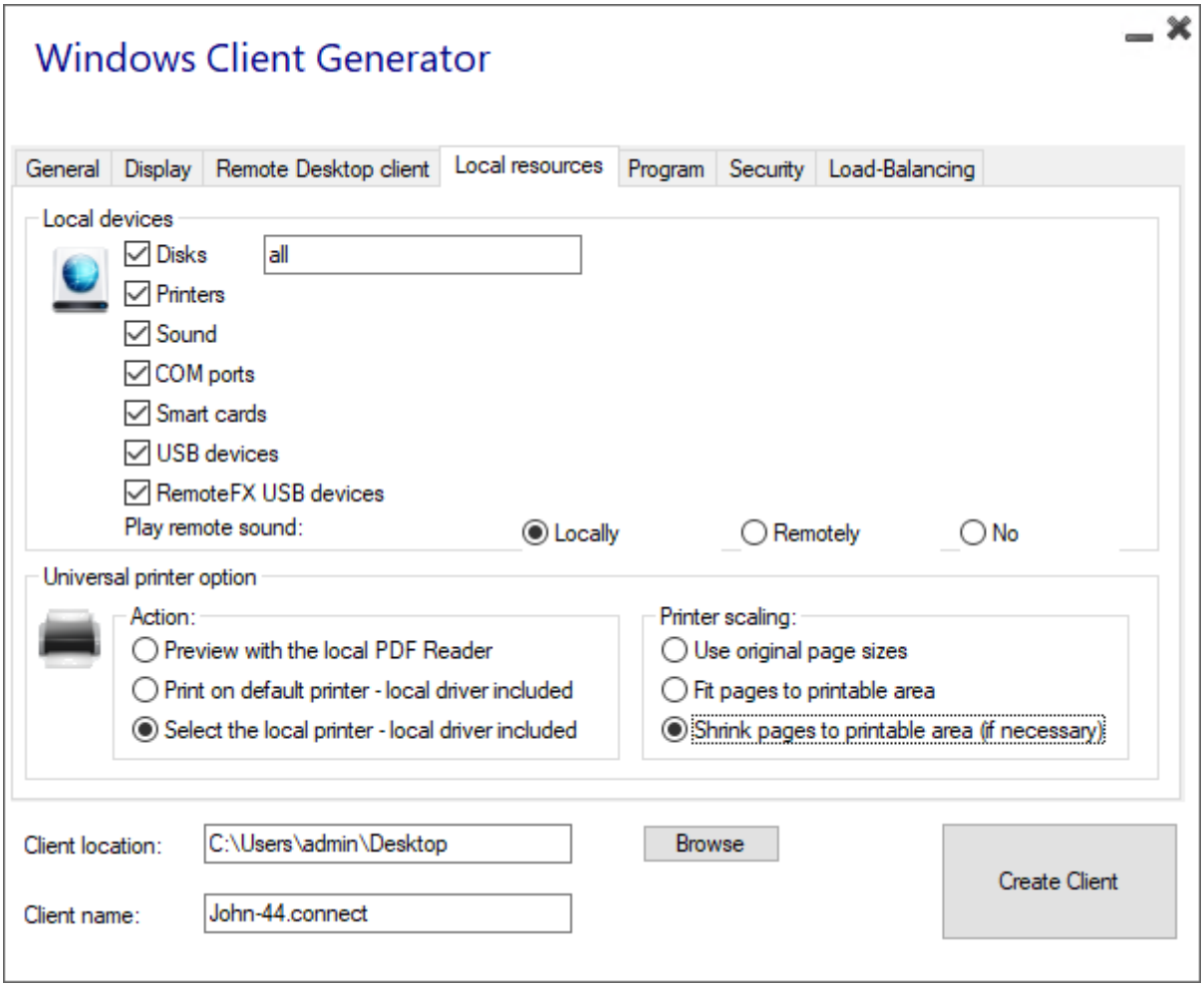
Vous pouvez cocher les cases pour activer le redimensionnement intelligent du Bureau à distance, et si vous ne souhaitez pas que le Bureau à distance cache ou chevauche la barre des tâches locale.

Option de sélection d'écran

Cela vous permet d'indiquer les moniteurs que vous souhaitez utiliser pour la session RDP. Le champ doit être rempli avec la liste des numéros d'écran à utiliser (séparés par une virgule, un espace ou un point-virgule).



Pour identifier les numéros d'écran, il suffit d'exécuter la commande. **mstsc /l**



L'onglet des ressources locales regroupe tous les appareils que vous pouvez rediriger dans votre session à distance.

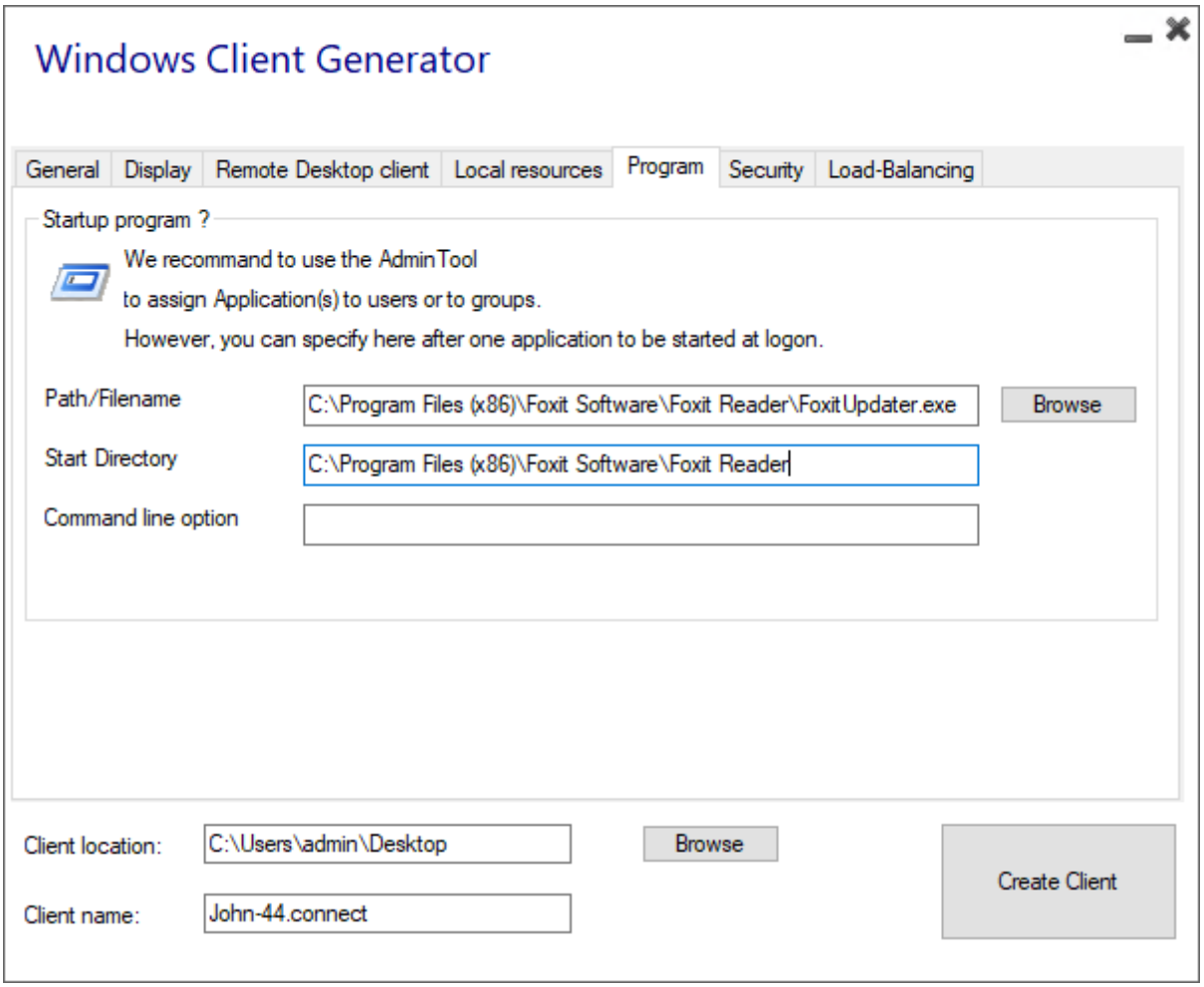
Le champ modifiable à côté de la **disques** La boîte permet de spécifier quels disques sont disponibles dans la session à distance. Il suffit de séparer chaque lettre de disque (C :, E: …) par une virgule. Lorsque la case des disques est cochée et qu'aucun disque n'est spécifié, tous les disques sont inclus dans la session à distance.

Imprimantes correspondent aux ports LPT, et les ports COM correspondent aux ports série. Depuis la version 11.50 de TSplus, ces périphériques locaux sont sélectionnés par défaut.

Ci-dessous, vous pouvez choisir votre option d'impression, avec l'imprimante universelle :

- **Aperçu du lecteur PDF local :** Le document sera rendu au format PDF et le lecteur Acrobat local ouvrira le fichier. L'utilisateur peut l'imprimer ou enregistrer une copie sur son disque dur local.
- **Imprimer sur l'imprimante par défaut de l'utilisateur :** le document sera automatiquement envoyé à l'imprimante par défaut de l'utilisateur (le pilote d'impression local est inclus dans le client de connexion TSplus).
- **Sélectionnez une imprimante locale :** L'utilisateur peut sélectionner l'une de ses imprimantes locales (le pilote d'impression local est inclus dans le client de connexion TSplus).

Si vous n'avez pas de lecteur PDF installé sur votre machine, nous vous recommandons d'utiliser Foxit Reader.



Vous pouvez définir une application de démarrage via le Générateur de Client Portable et spécifier son chemin, son répertoire et ses paramètres, depuis la version 11.30.

Cependant, nous vous recommandons d'utiliser l'AdminTool pour attribuer les applications souhaitées.

TSplus offre deux couches supplémentaires de sécurité physique pour protéger les connexions de vos utilisateurs.

La connexion peut être verrouillée sur l'ID d'une clé USB, verrouillée sur un nom d'ordinateur, ou vous pouvez utiliser les deux couches de sécurité simultanément.

Option de sécurité avancée pour les clients

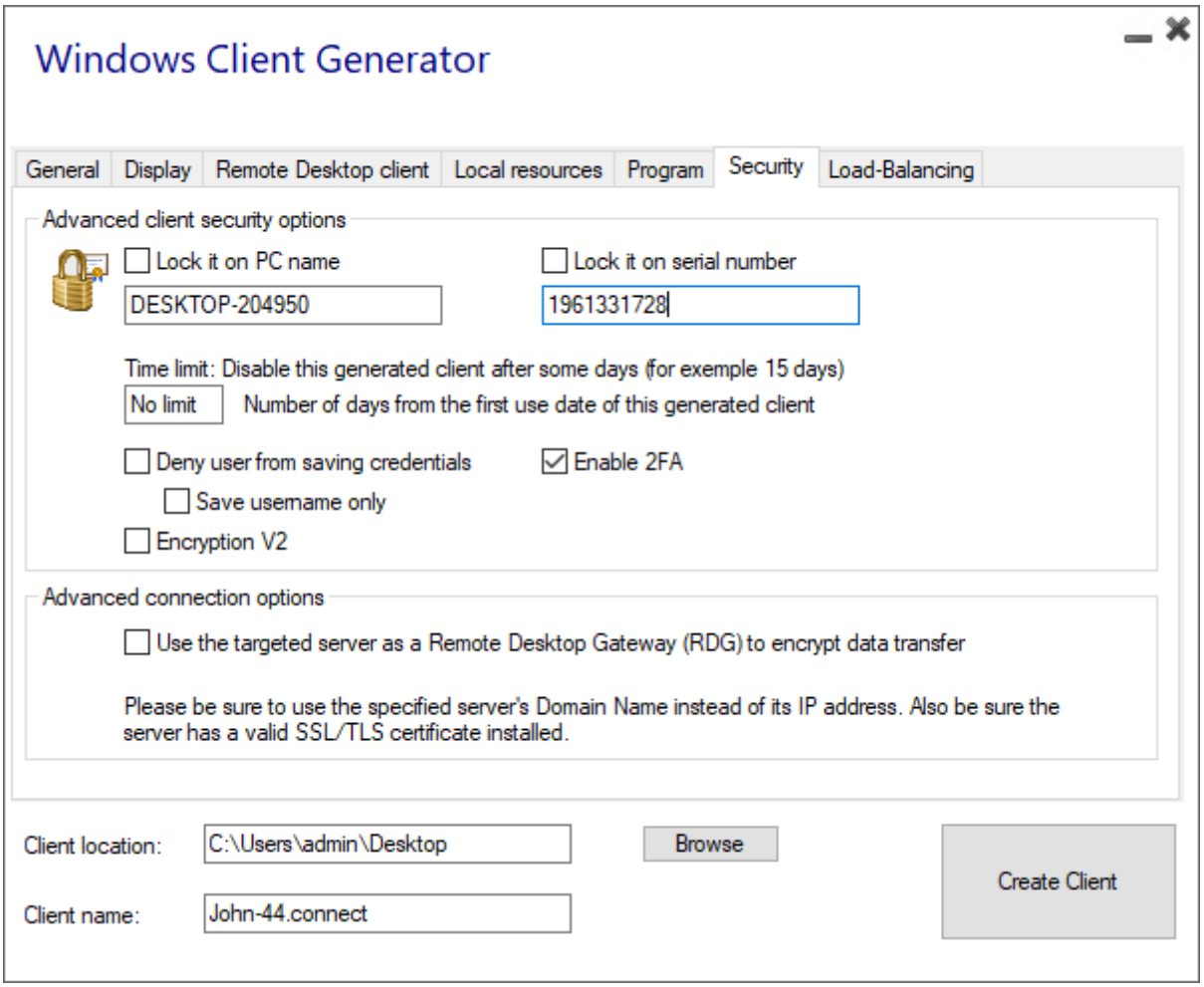
- **Si verrouillé sur une clé USB** l'utilisateur peut initier une connexion depuis n'importe quel ordinateur Windows éligible en insérant la clé USB et en utilisant le programme de connexion placé là par l'administrateur.
- **Si verrouillé à un nom d'ordinateur** l'utilisateur ne peut se connecter avec succès que depuis l'ordinateur dont le nom a été enregistré auprès du serveur pour la connexion client portable de cet utilisateur. Si les deux options de sécurité sont utilisées, l'utilisateur est limité à se connecter depuis son appareil spécifique et uniquement si la clé USB préconfigurée

correcte est en place.

Pour verrouiller une connexion client sur une clé USB, vous pouvez le faire en copiant le générateur de client situé dans : C:\Program Files (x86)\TSplus\Clients\WindowsClient

Maintenant, double-cliquez sur le générateur de client et vérifiez le verrou sur la case du numéro de série située dans l'onglet de sécurité. Une fois cela fait, vous pouvez supprimer le générateur de client de la clé USB.

Le client de connexion nouvellement généré sera placé sur le bureau, n'oubliez pas de le copier à nouveau sur la clé USB ! Vous pouvez supprimer le générateur de client que vous avez copié sur la clé USB par la suite.



- Vous pouvez définir le **limite de temps** à partir de la date de première utilisation d'un client généré en entrant la valeur dans la case de limite de temps. (qui est par défaut réglée sur "aucune limite").

- Les cases ci-dessous vous permettent de :

- Ne pas afficher la possibilité de sauvegarder les identifiants pour un client généré.
  - Enregistrer uniquement le nom d'utilisateur.
  - Utiliser le chiffrement V2.

Support pour l'authentification à deux facteurs

Le générateur de clients prend en charge **authentification à deux facteurs** depuis la version 15.30.3.15. Le support de l'authentification à deux facteurs nécessite également un **Édition Web Mobile ou supérieure** .

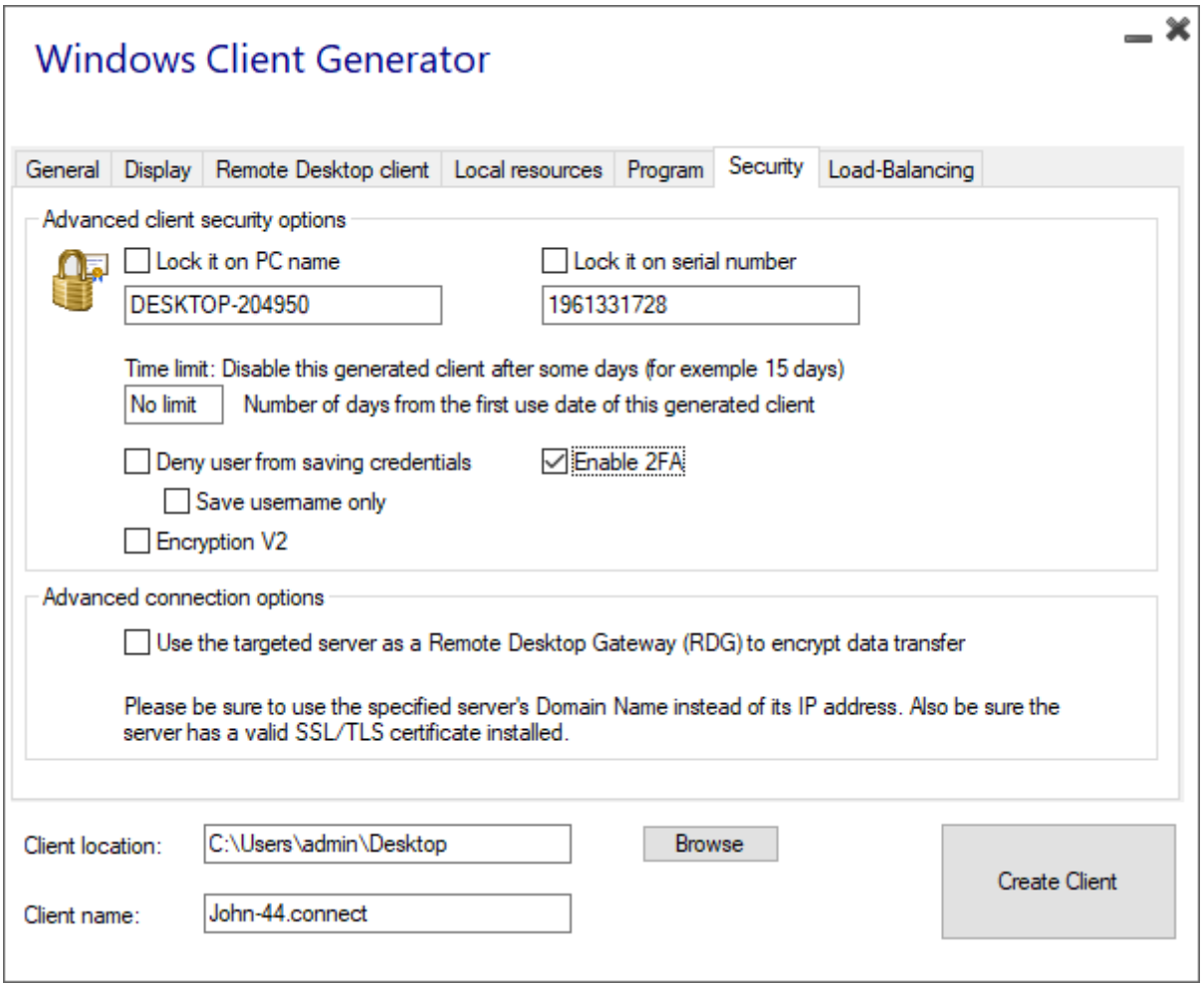
Veuillez vous référer à Page de documentation sur l'authentification à deux facteurs pour plus d'informations sur la façon de configurer et d'activer l'authentification à deux facteurs pour les utilisateurs et les groupes sur votre installation TSplus Remote Access.

Veuillez noter les exigences supplémentaires suivantes pour activer l'authentification à deux facteurs pour un client généré :

- Le client de connexion valide le code d'authentification auprès du portail Web en utilisant le port HTTPS. Par conséquent, **Le portail Web doit être opérationnel.** et accessible via son port HTTPS depuis la machine cliente.
- Si le port HTTPS du portail Web est modifié, alors les clients générés activés pour l'authentification à deux facteurs doivent être générés à nouveau. Les clients précédemment générés échoueront à valider toute authentification à deux facteurs.

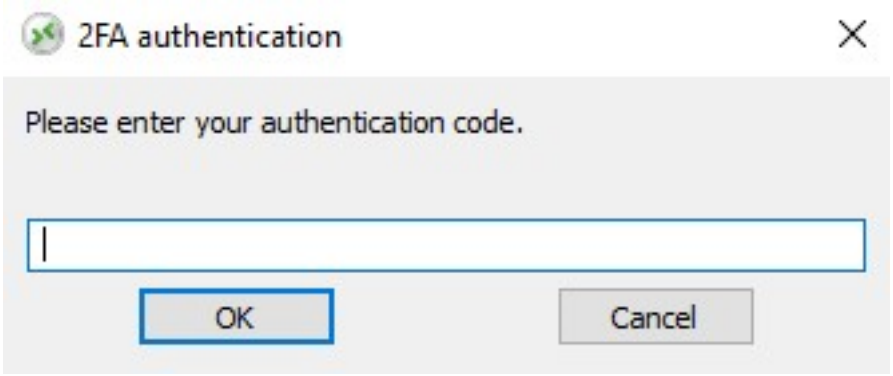
Depuis la version 15.30.3.15, tout client précédemment généré et tout nouveau client généré sans le support 2FA activé se comportera de la même manière qu'auparavant. **Si un utilisateur activé pour l'authentification à deux facteurs tente de se connecter en utilisant un client généré sans support explicite pour 2FA, la connexion sera refusée.** car l'authentification à deux facteurs n'est pas possible et échouera donc.

Pour ajouter le support de l'authentification à deux facteurs, vérifiez le **Activer 2FA** Cochez avant de générer votre fichier client. En conséquence, l'authentification à deux facteurs sera validée lors de la connexion au serveur d'application Remote Access. Si l'authentification à deux facteurs est activée sur le serveur d'application et que l'utilisateur se connectant n'est pas configuré, alors la connexion sera refusée.



Soyez conscient que l'ajout de la prise en charge de 2FA à un client généré ultérieurement n'est pas pris en charge. Par exemple, l'ajout de la prise en charge de 2FA via la ligne de commande contre le fichier .connect généré n'est pas pris en charge.

Une fois qu'un utilisateur a configuré son compte dans une application d'authentification, il ou elle pourra se connecter en utilisant son mot de passe et le code fourni par son application d'authentification ou par SMS.



Option de connexion avancée

Si le serveur ciblé possède un nom de domaine spécifique et accessible, ainsi qu'un certificat SSL/TLS valide installé, vous pouvez activer l'option « Utiliser le serveur ciblé comme passerelle de bureau à distance (RDG) pour chiffrer le transfert de données ».

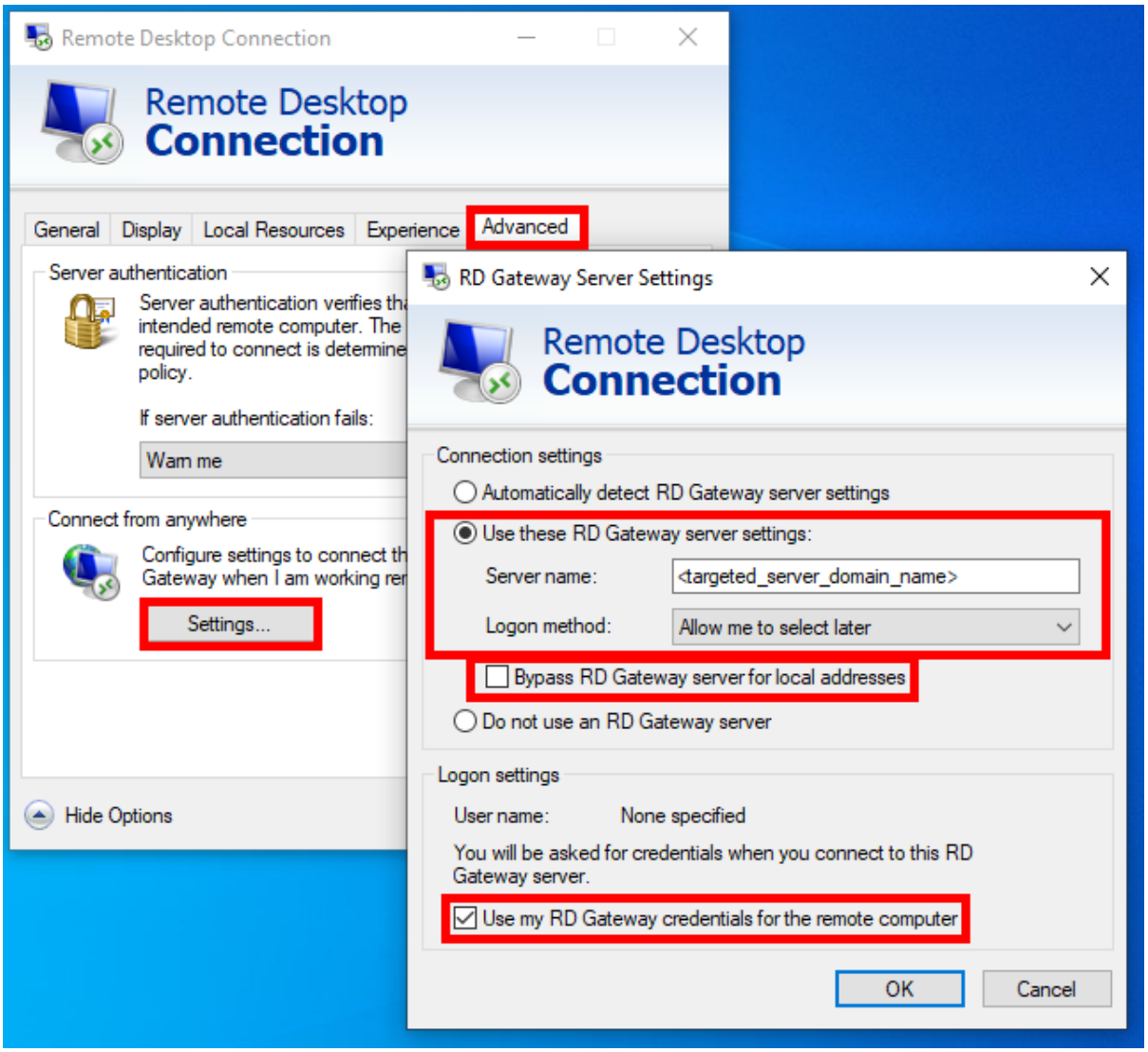
Cette option rend le transfert de données RDP pendant la connexion crypté en utilisant l'encapsulation TLS, ce qui en fait une alternative appropriée à tout VPN en termes de cryptage des données.

Utilisez mstsc à la place pour vous connecter au RD Gateway

Vous pouvez également utiliser cette fonctionnalité via la configuration mstsc sans utiliser un client généré si les prérequis mentionnés ci-dessus sont respectés.

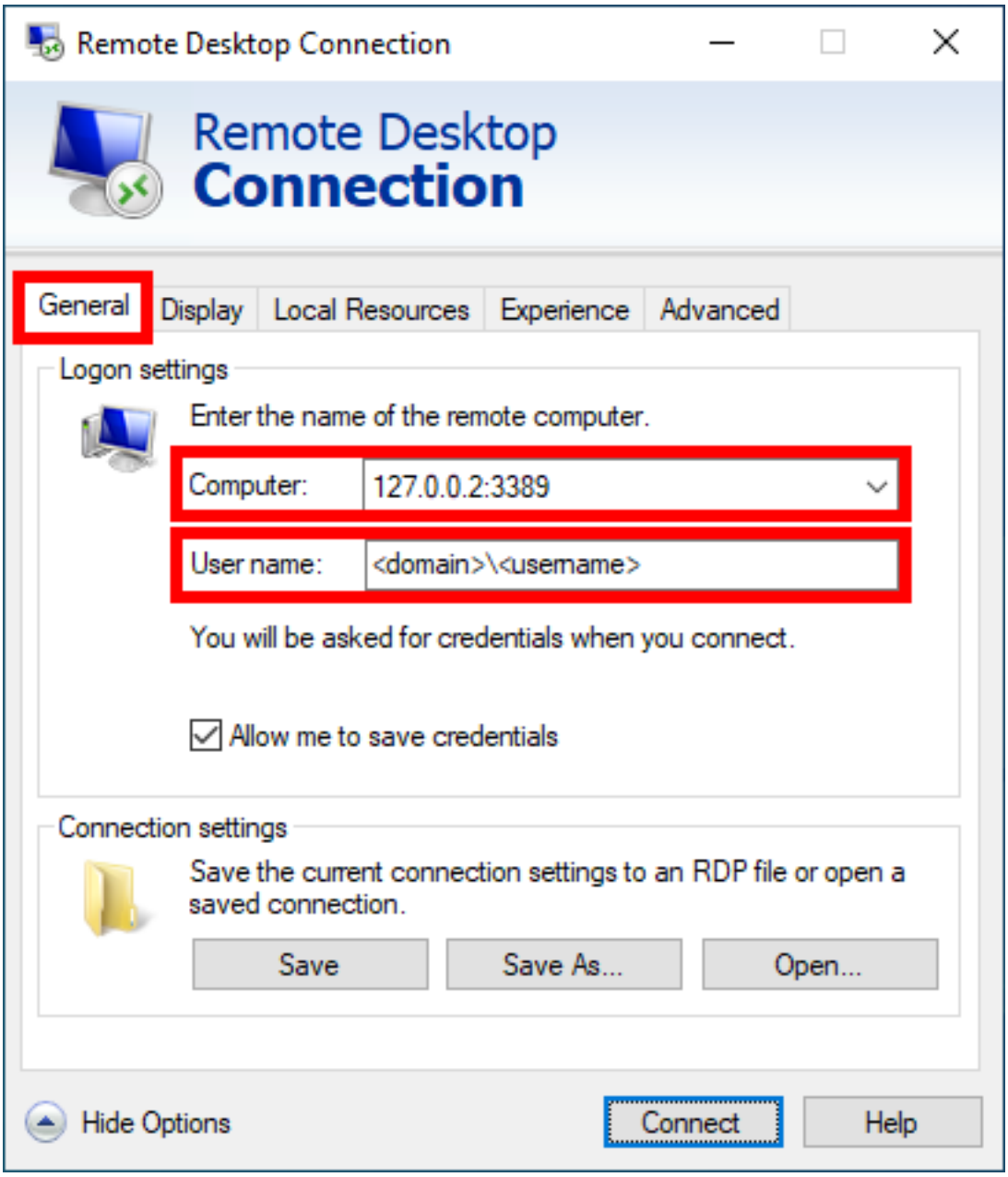
Pour ce faire, allez d'abord dans l'onglet avancé, puis dans la section « Se connecter de n'importe où », cliquez sur « Paramètres » et configurez le Gateway de Bureau à distance par :

- Cocher l'option « Utiliser ces paramètres de serveur RD Gateway »
- Remplacer le nom du serveur par le nom de domaine du serveur ciblé (sans https://)
- Sélectionner la méthode de connexion « Me permettre de sélectionner plus tard »
- Désélectionner l'option « Contourner le serveur RD Gateway pour les adresses locales »
- Cocher l'option « Utiliser mes identifiants RD Gateway pour l'ordinateur distant »
- Cliquer sur "OK" pour enregistrer ces paramètres



Ensuite, allez dans l'onglet « Général », et :

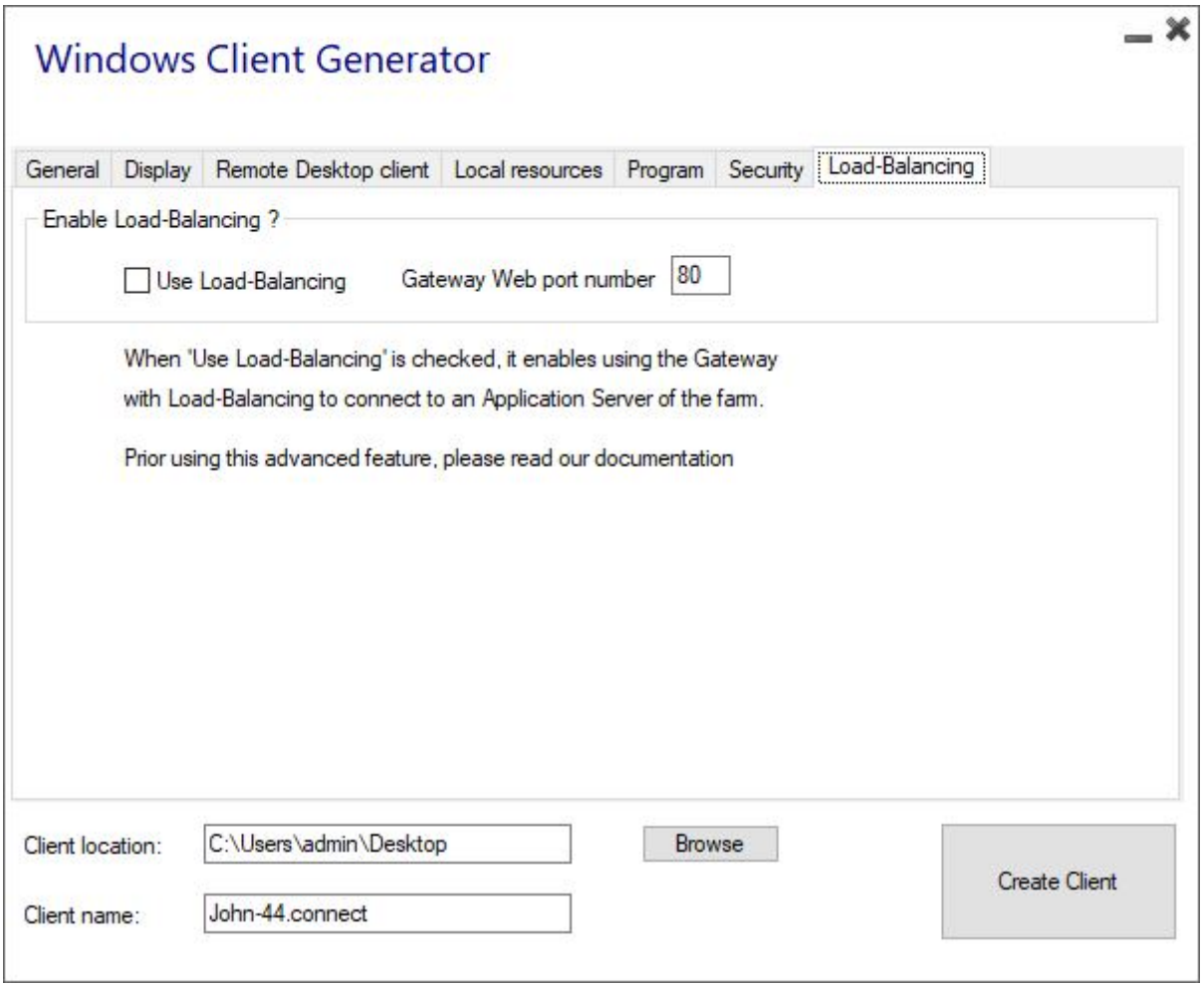
- Remplacez le nom de l'ordinateur par "127.0.0.2:3389" et changez le port "3389" si vous en utilisez un différent.
- Remplacez le nom d'utilisateur par le nom d'utilisateur avec lequel vous souhaitez vous connecter (**important : spécifier le domaine est obligatoire**)
- Cliquez sur "Connecter"

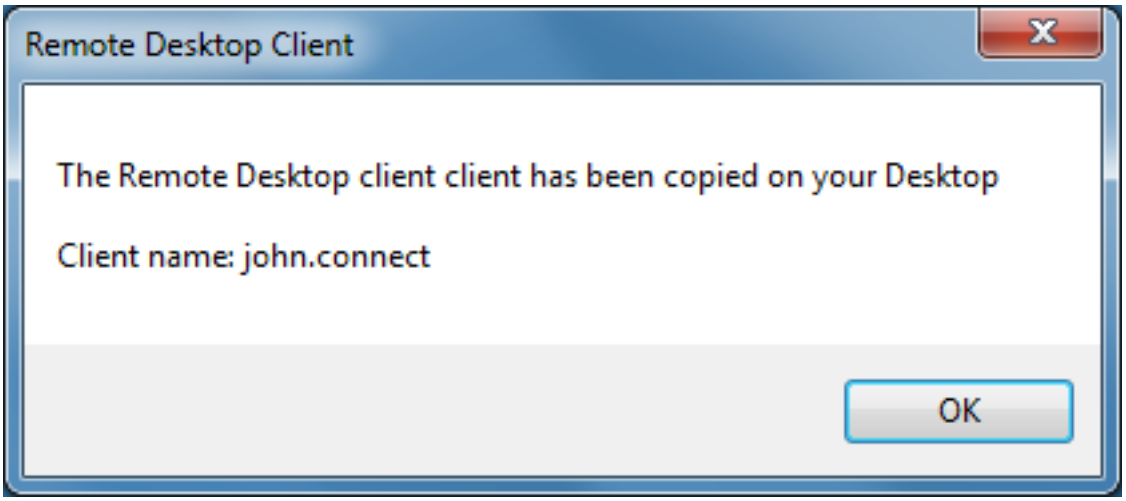


Vous pouvez également activer l'équilibrage de charge pour vous connecter à un serveur de votre ferme.

Ne cochez pas la case « Utiliser l'équilibrage de charge » si vous n'avez pas activé la fonctionnalité d'équilibrage de charge sur votre serveur.

Vous devrez entrer le port Web de la passerelle, qui devrait être le même que le port Web par défaut utilisé sur tous les serveurs de votre ferme.





La personnalisation du client est possible. Consultez la documentation correspondante sur comment modifier l'icône du client et modifier ou supprimer ses paramètres .

Vous pouvez activer les journaux pour le Client de Connexion du côté client en ajoutant la clé de registre suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\ConnectionClient “Debug”=“true”

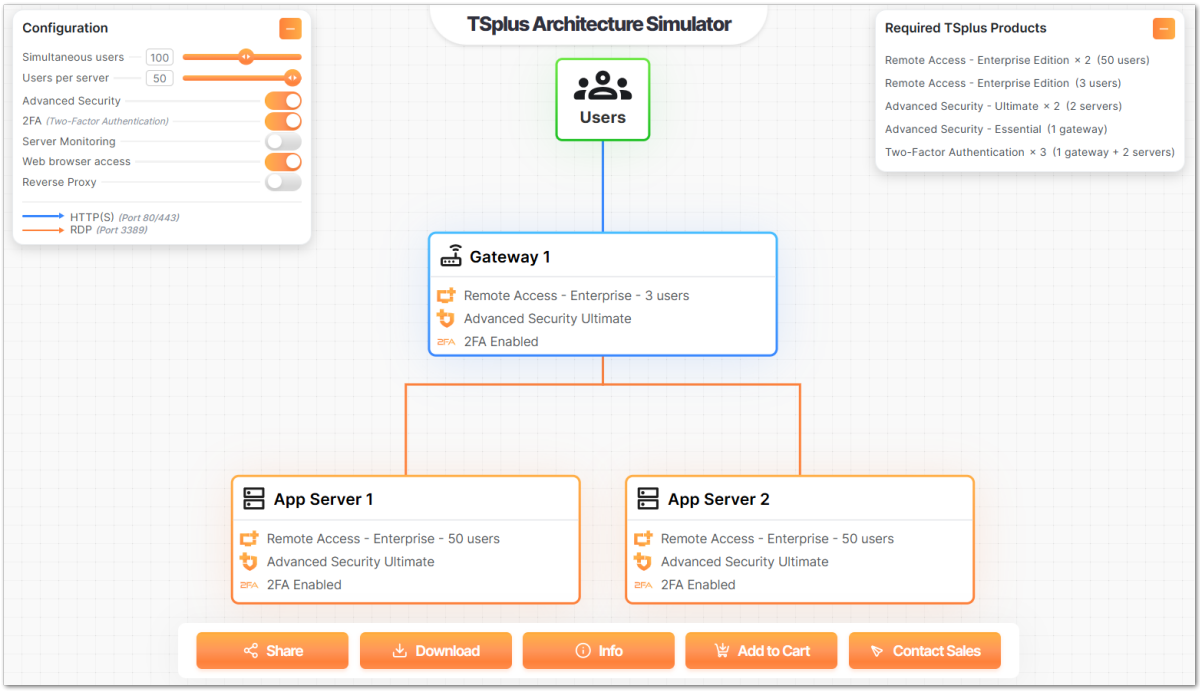
Les journaux sont situés dans C:\Users Répertoire RDP6\logs si l'installation est par utilisateur ou dans C:\Program Files (x86)\Connection Client\RDP6\logs si l'installation est pour tous les utilisateurs.

Prérequis pour TSplus Remote Access

Simulateur d'architecture

Configurez votre architecture en ligne pour vous aider à choisir nos logiciels et modules complémentaires.

TSplus Architecture Simulator



1. Matériel

Exigences minimales du serveur TSplus Remote Access :

Nombre d'utilisateurs	Windows 2008 à 2025 ou 7 à 11 Pro
3 - 5	I5 ou supérieur Un CPU 2 GHZ Minimum : 4 Go de RAM

	Recommandé : 8 Go de RAM
10	I5 ou supérieur Un CPU 2 GHZ Minimum : 8 Go de RAM Recommandé : 16 Go de RAM
25	Un CPU I7 ou Xeon Minimum : 16 Go RAM Recommandé : 32 Go de RAM
50 et plus	32 Go Dual CPU - Disque SSD dédié au système Minimum : 32 Go de RAM Recommandé : 64 Go de RAM

Nous recommandons d'utiliser un processeur de moins de dix ans.

Concernant l'utilisation de la RAM, cela dépendra du système d'exploitation installé, du nombre d'utilisateurs simultanés et des applications qui leur sont attribuées.

Chaque serveur (physique ou virtuel) peut potentiellement gérer jusqu'à 50 utilisateurs simultanés. Pour plus de 50 sessions simultanées, nous recommandons d'utiliser un parc de serveurs avec la fonctionnalité de répartition de charge disponible dans TSplus Remote Access Enterprise Edition.

Remarque : Les spécifications exactes de votre matériel dépendront du type de ressources (CPU/RAM/Disque) que vos applications consomment.

Seulement **x86 et x64** les architectures sont prises en charge.
ARM32 et ARM64 les architectures ne sont pas prises en charge.

2. 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.

Le cadre requis est **version .NET 4.7.2** pour toutes les versions Windows prises en charge.

Version d'accès à distance	Version minimale de Windows
19, LTS 18, LTS 17, LTS 16, LTS 15	Windows 7 Service Pack 1 Windows Server 2008 R2 Service Pack 1
LTS 14	Windows Vista Windows Server 2008

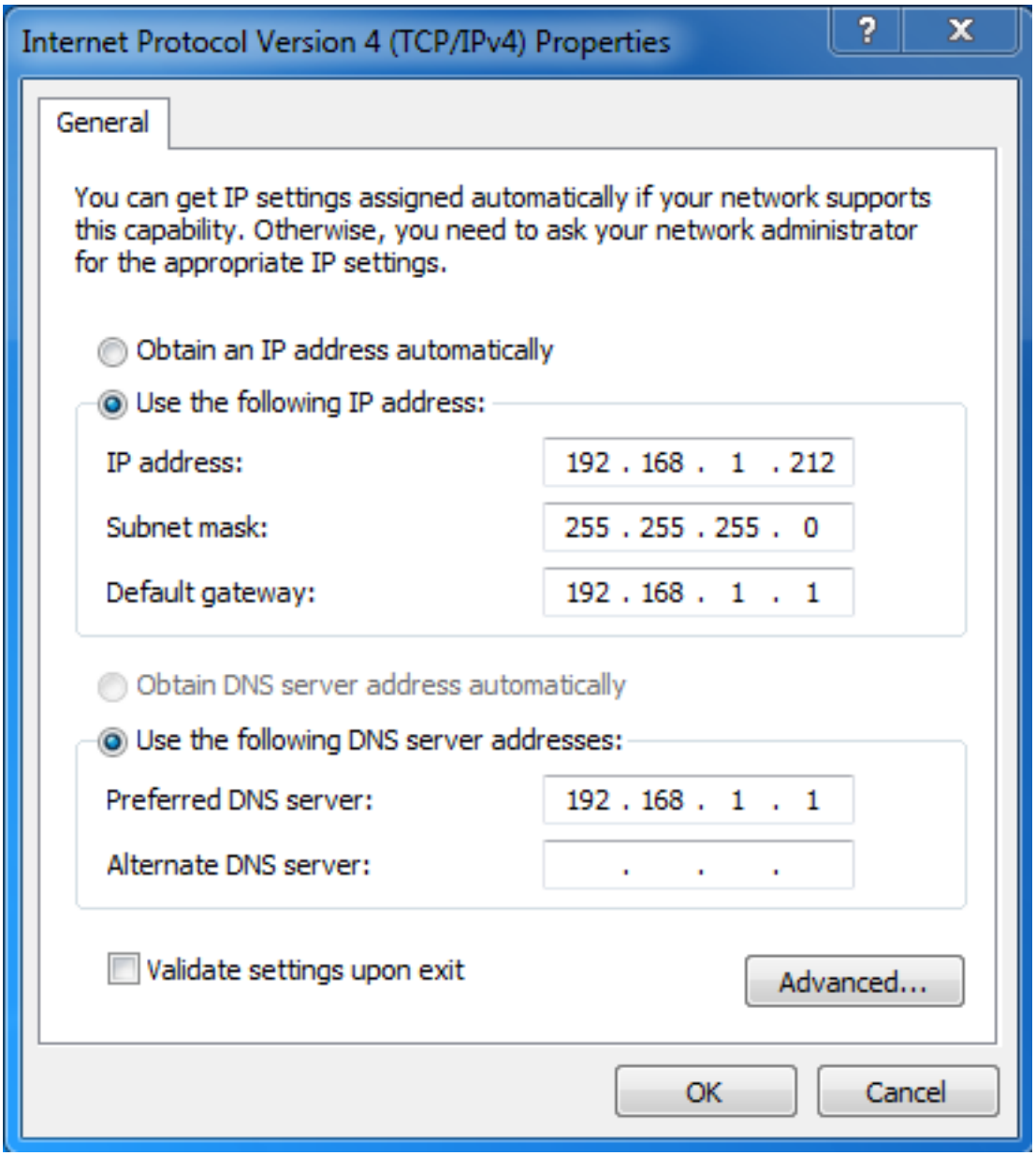
- Si vous installez Remote Access sur un système d'exploitation Windows Server, assurez-vous que les rôles RDS/Terminal Services et RDS/Terminal Services Licensing ne sont pas installés avant d'installer TSplus Remote Access.

Si ces rôles sont actuellement installés, supprimez-les et redémarrez.

- Les éditions Windows Home ne sont pas prises en charge.
- Sur Windows Server 2016, un maximum de 15 sessions est autorisé pour l'accès à distance.
- Windows Server 2016, 2019, 2022 Essentials Edition n'est pas pris en charge ni recommandé pour utiliser TSplus Remote Access.
- Le serveur Web intégré de TSplus Remote Access nécessite **Java OpenJDK 17 ou supérieur.** .

3. Paramètres réseau

Le serveur d'accès à distance doit avoir une adresse IP privée statique :



Accès à distance (depuis un réseau étendu - WAN)

- Une connexion Internet à large bande est recommandée ainsi qu'une adresse IP publique statique. Si vous n'avez pas d'adresse IP statique, envisagez d'utiliser un service DNS dynamique comme
- Le port TCP RDP (par défaut 3389) doit être ouvert dans les deux sens sur votre pare-feu.

3. Sécurité

Depuis début 2024,
TSplus a mis à jour son mécanisme de génération automatique de certificats SSL/TLS pour s'aligner sur le changement de la chaîne de confiance de Let's Encrypt : le **DST Root CA X3** la racine a été remplacée par **ISRG Root X1** .

Si un client ou un poste de travail ne reconnaît pas le nouveau certificat, il peut être nécessaire

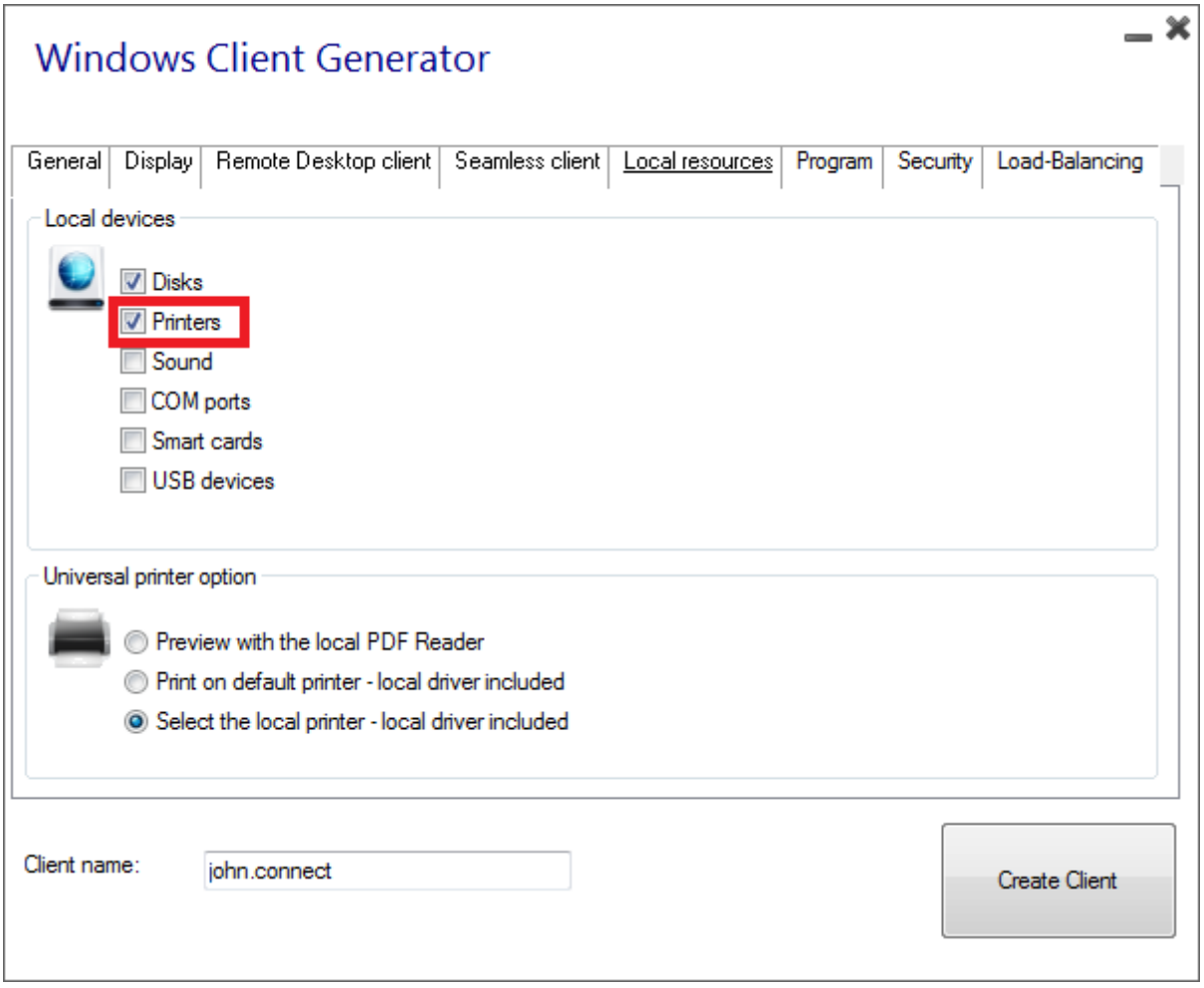
d'ajouter **ISRG Root X1** au magasin de certificats de confiance Windows.

TSplus fonctionne avec des certificats génériques et prend en charge le protocole TLS pour des connexions à distance sécurisées.

Impression avec la fonctionnalité de mappage d'imprimante RDP standard

Cela est couramment utilisé par les utilisateurs de Remote Desktop et est équivalent à ce que vous auriez avec Microsoft Terminal Services.

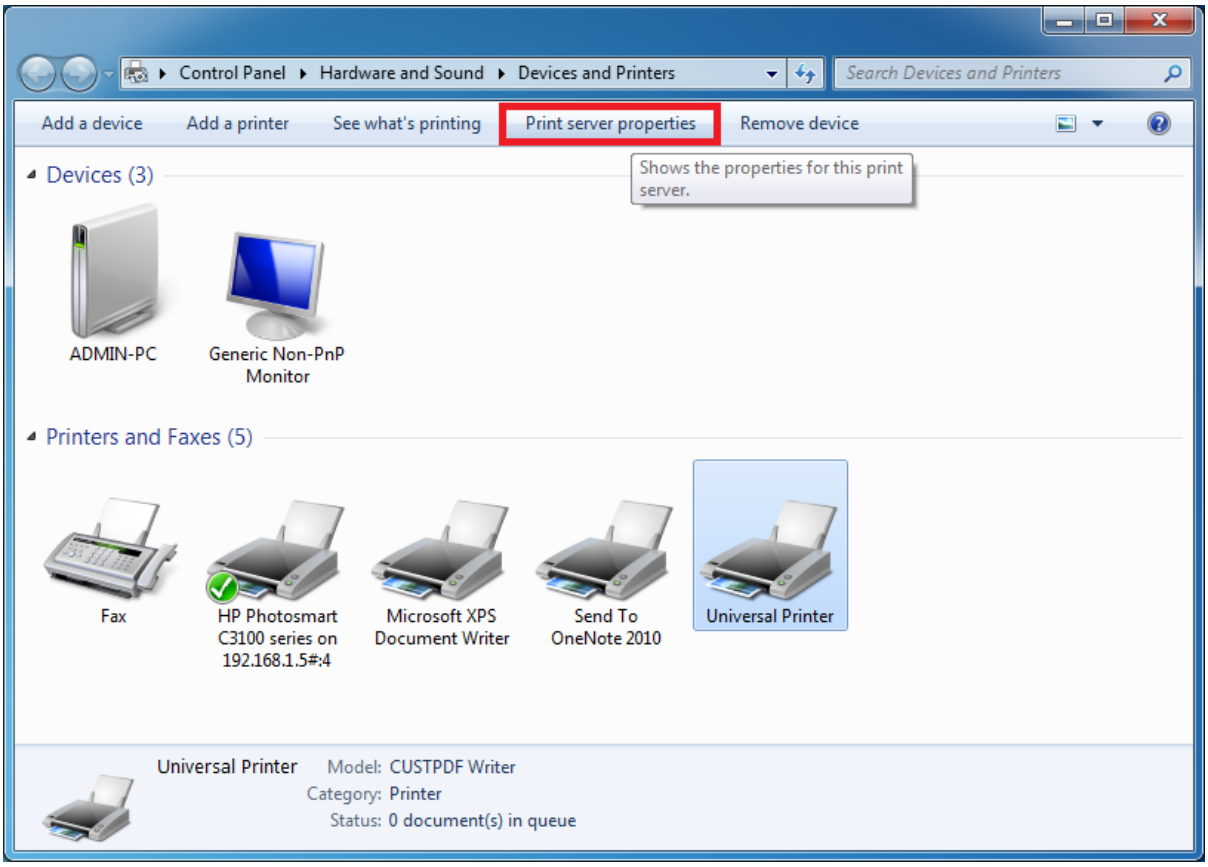
Si vous prévoyez d'utiliser des imprimantes exotiques, assurez-vous de cocher la case pour les imprimantes dans l'onglet des ressources locales du générateur de client.



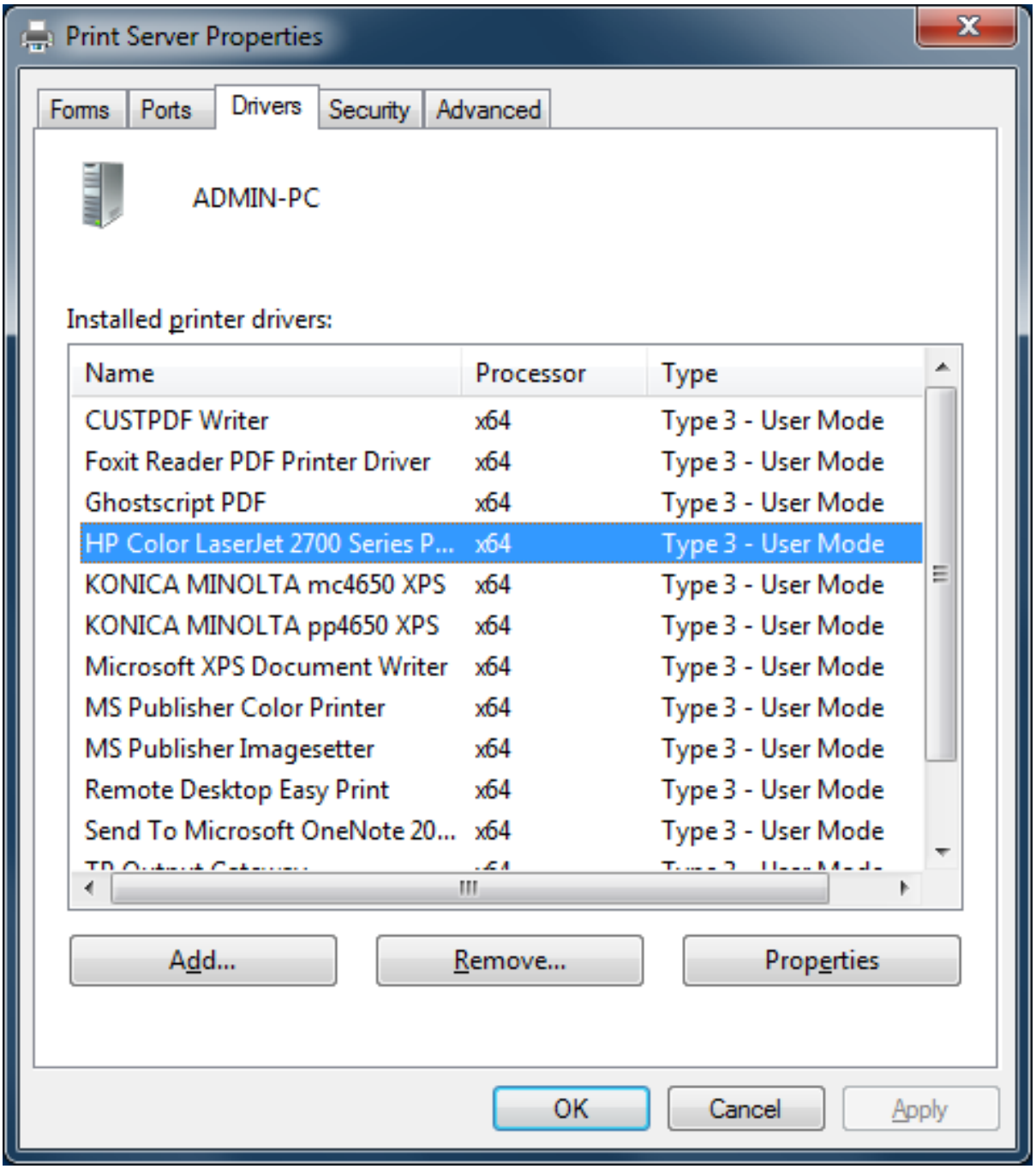
La plupart du temps, il sera nécessaire d'installer la même version des pilotes d'imprimante à la fois sur le client et sur le serveur afin de fonctionner correctement.

Cela signifie que si votre serveur est Windows 2008 64 bits et que vos ordinateurs clients fonctionnent sous Windows XP 32 bits, vous devrez installer les pilotes d'imprimante XP 32 bits sur le serveur.

Cliquez sur le menu Démarrer, puis sur Périphériques et imprimantes. Cliquez sur n'importe quelle imprimante pour afficher le bouton Propriétés du serveur d'impression en haut de la fenêtre :



Une fois dans les propriétés du serveur d'impression, cliquez sur l'onglet Pilote pour ajouter manuellement votre pilote client. (Dans ce cas, nous installons le pilote Windows XP 32 bits)



Vous pouvez également installer directement vos pilotes d'imprimante en utilisant les informations et les pilotes du site Web du fabricant de l'imprimante.

- Il est recommandé de consulter le manuel de votre matériel pour une procédure d'installation dans un environnement de serveur terminal.
- Si vous utilisez des imprimantes USB, assurez-vous d'avoir mis à jour le protocole RDP de votre ordinateur client vers la version 6 ou supérieure pour garantir une compatibilité maximale avec les imprimantes redirigées.

Pour de meilleurs résultats, il est recommandé de ne pas utiliser d'imprimantes USB. La compatibilité et la fiabilité sont améliorées lors de l'utilisation d'imprimantes COM ou LPT.

Certains imprimantes exotiques, telles que les imprimantes d'étiquettes ou de reçus, peuvent ne

pas être adaptées à la redirection dans une session TSplus, vous devez toujours vérifier auprès de votre fabricant de matériel pour la compatibilité et les procédures d'installation dans un environnement RDS ou de serveur terminal, qui est très proche de TSplus dans ce cas.

TSplus Remote Access v19 : Guide de démarrage rapide

Prérequis :

Sur le serveur :

- **OS :** Versions de Microsoft Windows 7 à 11 ou Windows Server 2008R2 à 2025 avec au moins 2 Go de RAM.
- TSplus ne prend pas en charge l'installation de Remote Access sur les éditions Windows Home.
- Le système d'exploitation **doit** soyez sur le lecteur C:.
- Java Runtime Environment. Si Java n'est pas déjà installé, Remote Access installera OpenJDK pendant la configuration.
- Si vous installez Remote Access sur un système d'exploitation Windows Server, assurez-vous que les rôles de services de bureau à distance/Terminal Services et de licences de services de bureau à distance/Terminal Services sont **non installé** avant d'installer TSplus Remote Access.
- Votre serveur Remote Access doit avoir une adresse IP privée statique.
- Pour un accès externe, votre serveur doit avoir une adresse IP publique statique ou un fournisseur DNS dynamique.
- Le serveur Web intégré de TSplus Remote Access nécessite **Java OpenJDK 17 ou supérieur.** .

Sur le client :

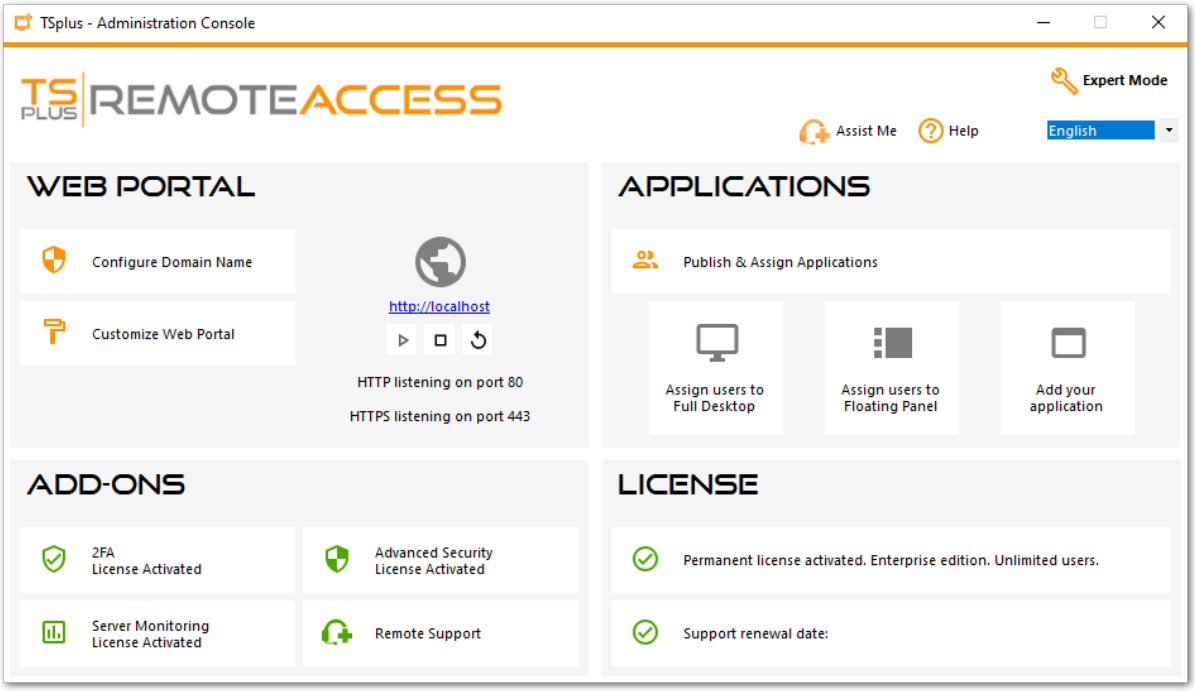
- **OS :** Les versions de Microsoft Windows 7 à 11 sont entièrement prises en charge.
- Pour MacOS, vous pouvez utiliser n'importe quel client RDP Mac ou le client HTML5 de TSplus.
- Pour Linux, vous pouvez utiliser Rdesktop ou le client HTML5 de TSplus.
- Environnement d'exécution Java.
- Un lecteur PDF (exemple : Foxit Reader ou Acrobat DC)

Pour des prérequis plus détaillés, veuillez consulter la documentation

Remarque :

À partir de la version 15 de Remote Access, la console d'administration a changé son

apparence. A **Mode Lite** et un **Mode Expert** ont été introduits. Les administrateurs peuvent basculer entre les deux styles d'interface en cliquant sur le bouton dans le coin supérieur droit de la console d'administration.



Étape 1 : Installation.

Remarque :

La version d'essai de Remote Access est l'édition Enterprise entièrement fonctionnelle. Elle est licenciée pour un maximum de 5 utilisateurs simultanés pendant une période de 15 jours.

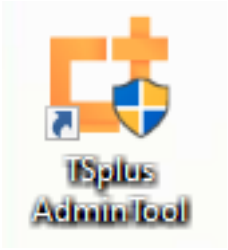
Installer TSplus Remote Access est un processus facile. Il suffit de le télécharger depuis notre site web, d'exécuter le programme Setup-TSplus.exe.

Les fichiers sont décompressés et copiés dans :

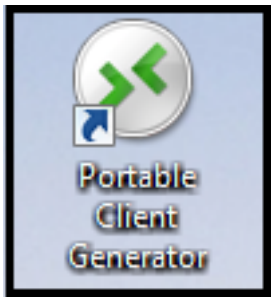
- C:\Program Files\TSplus (systèmes 32 bits)
- C:\Program Files(x86)\TSplus (64-bit systems).

Une fois l'installation terminée, l'installateur vous demandera de redémarrer.

Après le redémarrage, vous verrez 2 nouvelles icônes sur votre Bureau :



L'AdminTool est ce dont vous avez besoin pour utiliser Remote Access.

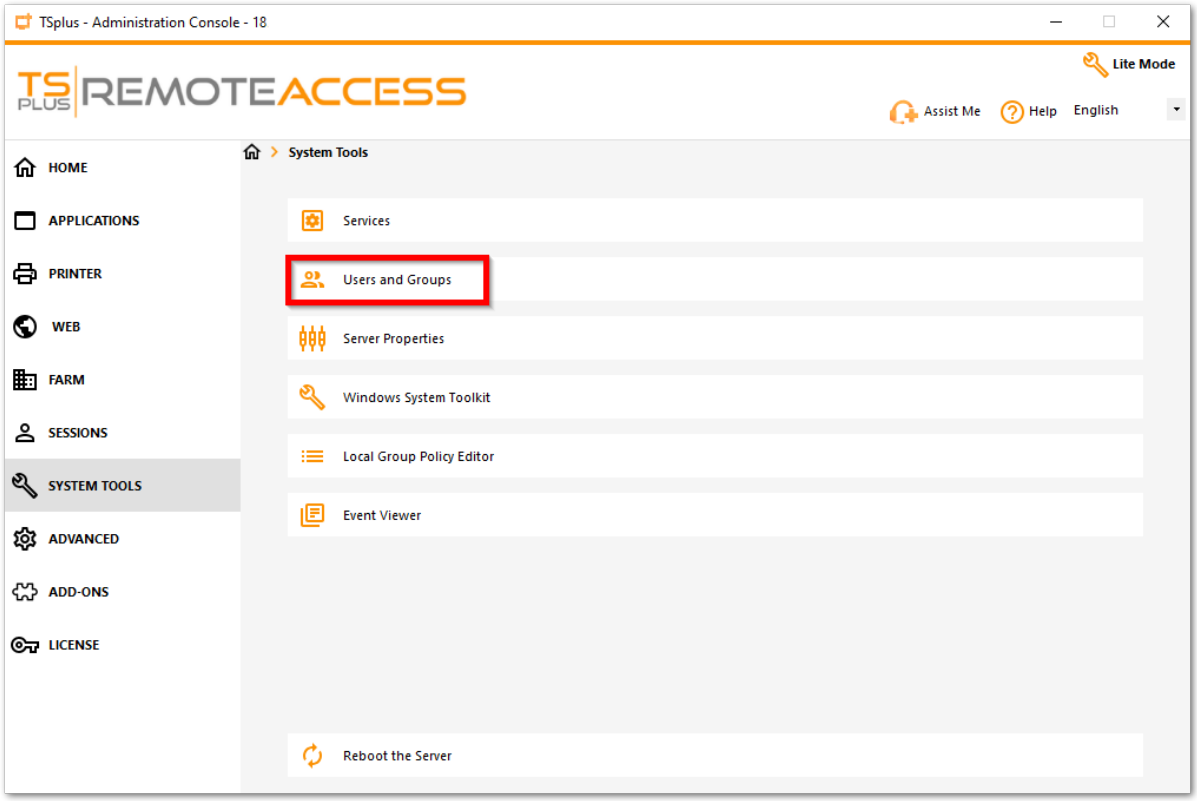


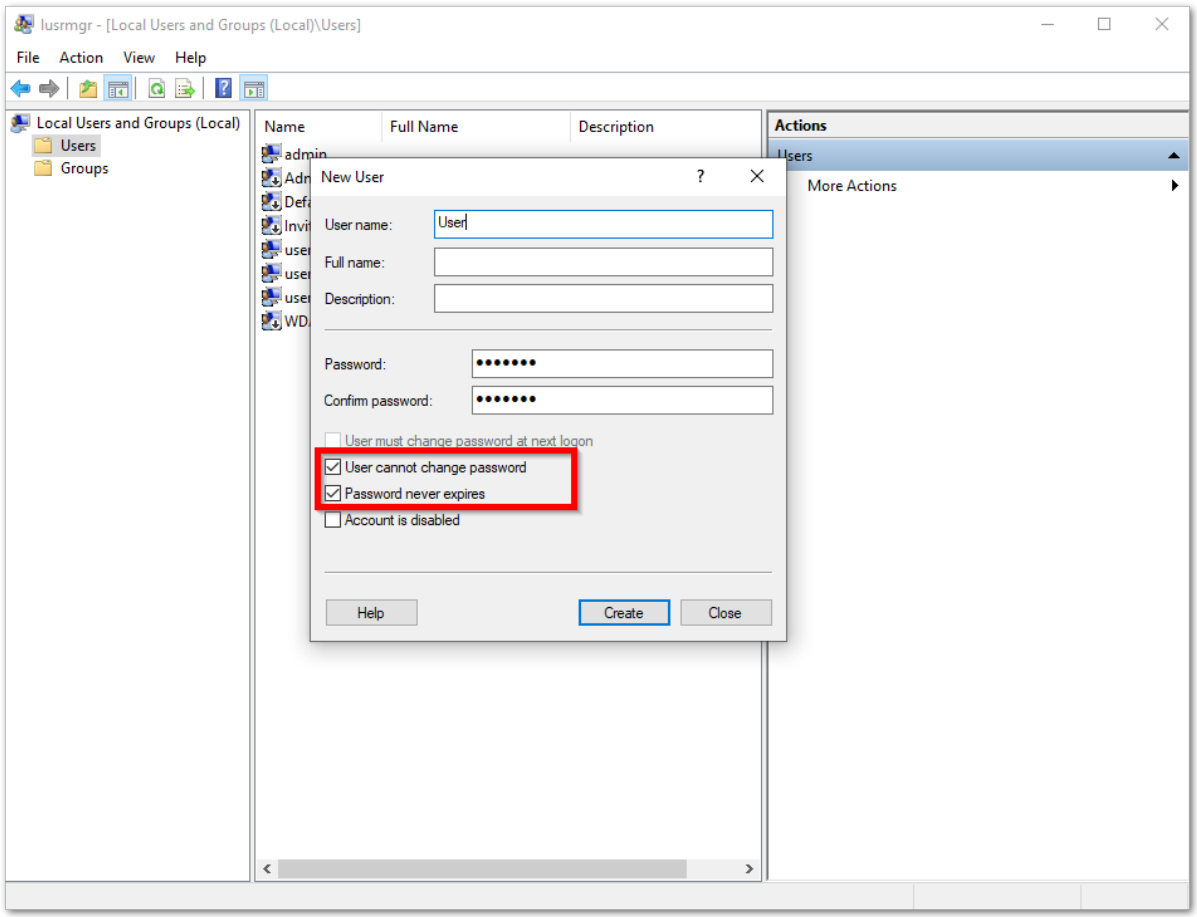
Le générateur de client portable est utilisé pour créer des clients de connexion Remote Access pour vos utilisateurs.

Voir la documentation pour des instructions d'installation complètes.

Étape 2 : Création d'utilisateurs.

Après le redémarrage, le serveur Remote Access est presque prêt à fonctionner. Maintenant, nous allons créer des utilisateurs. Ouvrez l'AdminTool pour commencer. Ensuite, allez à l'onglet Outils système et cliquez sur « Utilisateurs et groupes ». Cela vous amènera à la fenêtre Utilisateurs et groupes locaux.





Chaque utilisateur doit avoir un nom d'utilisateur ET un mot de passe. Lorsque vous créez des utilisateurs, soyez conscient de la case intitulée « L'utilisateur doit changer le mot de passe lors

de la prochaine connexion ». Si vous ne souhaitez pas que vos utilisateurs changent leur mot de passe lors de la première connexion, décochez cette case et cochez « Le mot de passe n'expire jamais » ou « L'utilisateur ne peut pas changer le mot de passe ».

Étape 3 : Sélectionnez le client le plus adapté à vos besoins.

Remote Access est compatible avec le protocole de bureau à distance Windows. Tout utilisateur peut se connecter localement ou à distance avec un client de connexion de bureau à distance standard (mstsc.exe) ou tout client compatible RDP. Pour bénéficier pleinement des fonctionnalités avancées de Remote Access (RemoteApp, Imprimante universelle…), vous pouvez utiliser un client généré ou le portail Web de Remote Access.

Remote Access est une solution très flexible et offre plusieurs façons d'ouvrir une session :

- **Connexion Bureau à Distance Classique** MSTSC.EXE.
- **Client RDP portable TSplus** qui affichera un environnement fenêtré pour votre connexion distante que vous pouvez réduire dans la barre des tâches de Windows.
- **client MS RemoteAPP** qui affichera l'application utilisant le MS RemoteApp natif.
- **client Windows** sur le portail Web TSplus.
- **client HTML5** sur le portail Web TSplus.

Ces clients offrent à l'utilisateur l'expérience suivante :

Avec la connexion Bureau à distance (mstsc.exe)

- **Connexion** La connexion est très standard. L'imprimante universelle n'est pas prise en charge avec ce type de connexion.

- **Affichage** Les utilisateurs verront leur session dans une fenêtre de Bureau à distance. Ce bureau affiche le contenu du dossier Bureau de l'utilisateur.

  Si l'administrateur a attribué des applications spécifiques avec l'AdminTool, seules ces applications seront affichées (pas de barre des tâches, pas de bureau).

TSplus client RDP généré .

Ceci est une solution unique de TSplus, elle permet aux utilisateurs locaux et distants de se connecter en utilisant un seul programme dédié.

Il comprend le programme de connexion, la fonctionnalité avancée d'impression universelle, la portabilité avec un niveau de sécurité élevé tout en restant très simple pour les utilisateurs.

Pour plus d'informations sur l'utilisation du générateur de clients TSplus, voir cette documentation

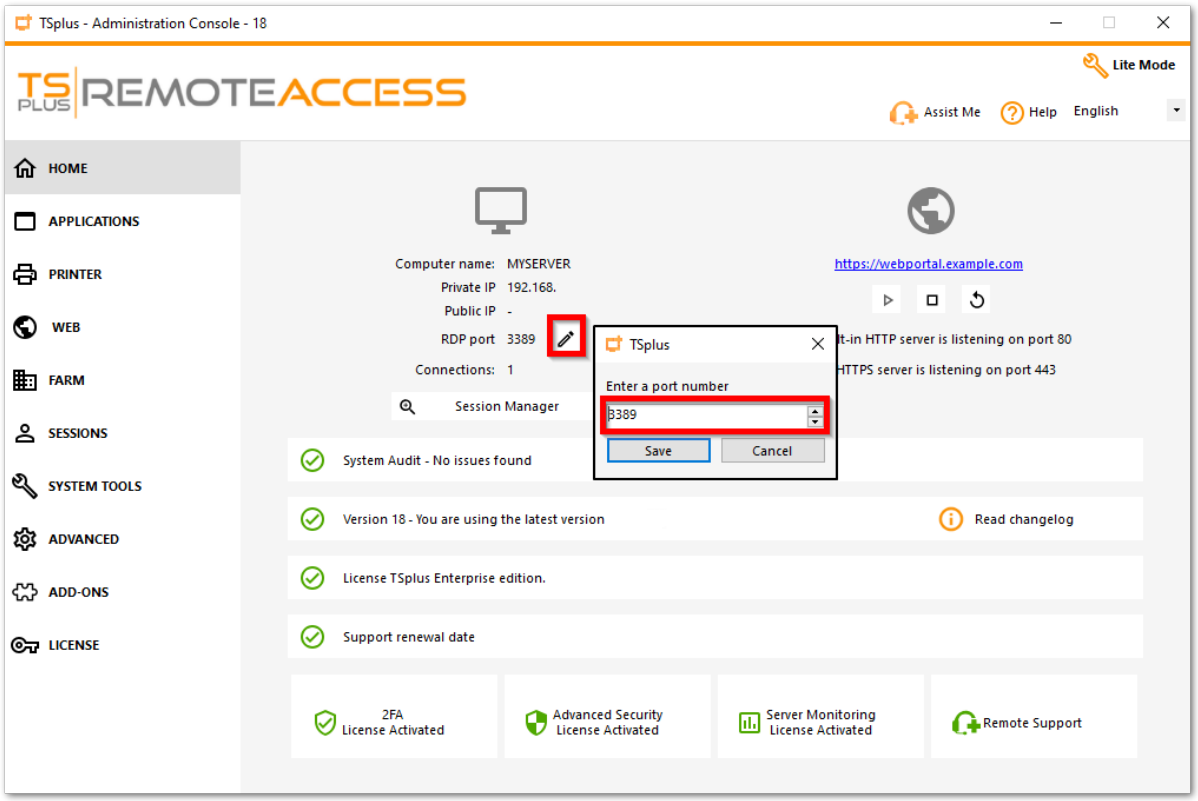
Le Client généré par TSplus RemoteApp .

Les applications distantes auront l'apparence et le comportement d'une application locale. Au lieu d'une fenêtre classique de Remote Desktop, vous pourrez passer librement entre vos applications locales et distantes sans avoir à minimiser une fenêtre de Remote Desktop.

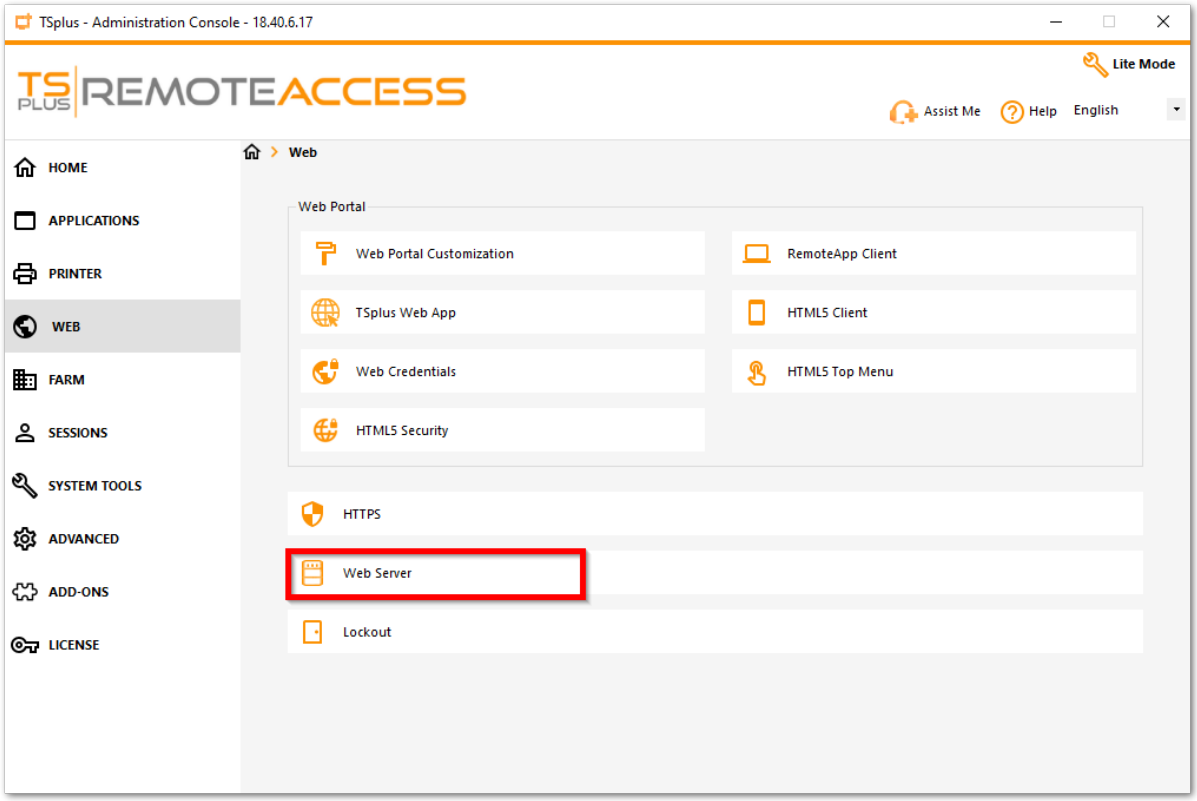
Pour plus d'informations sur ces clients, voir cette documentation .

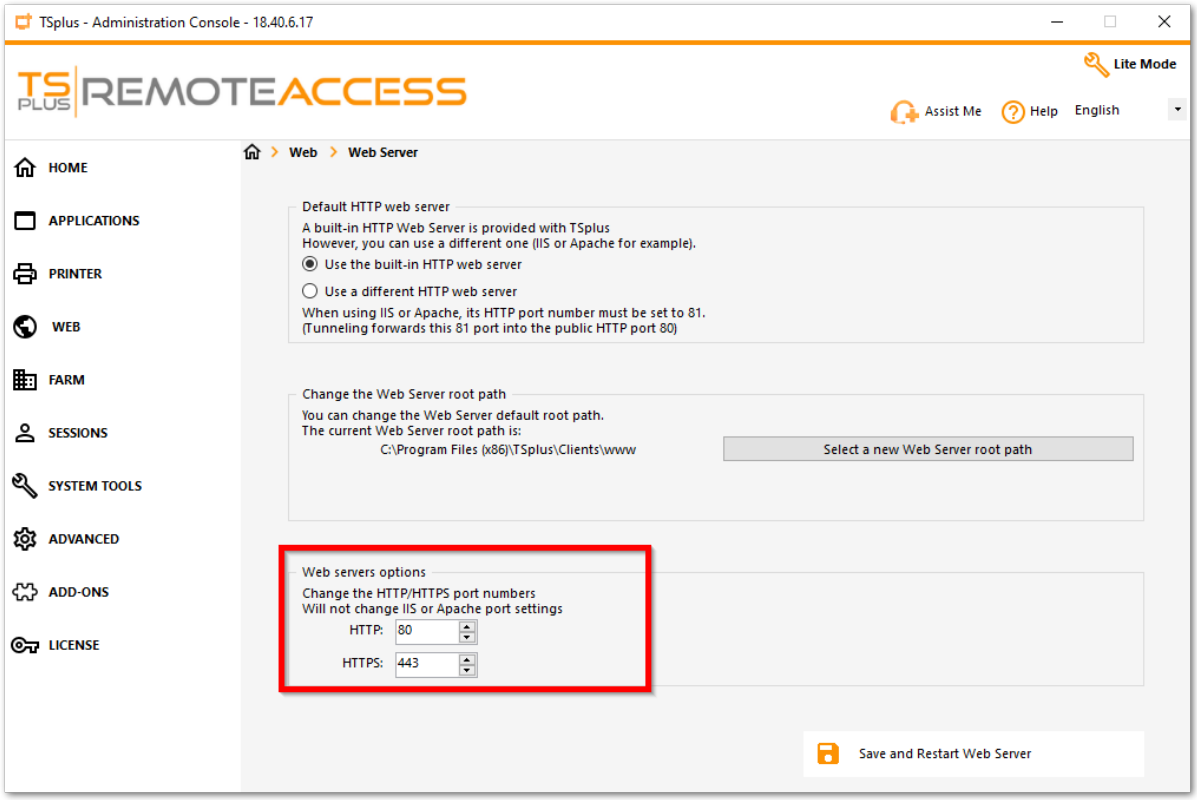
Accéder à votre serveur TSplus Remote Access depuis un emplacement distant

Pour accéder à votre serveur Remote Access depuis l'extérieur de votre réseau local, vous devrez créer une règle de redirection de port ou de transfert de port pour les ports 3389/80/443 en fonction de votre méthode de connexion préférée. Vous pouvez changer le port RDP dans l'onglet Accueil :



Les ports 80/443 peuvent être modifiés dans l'onglet Serveur Web :



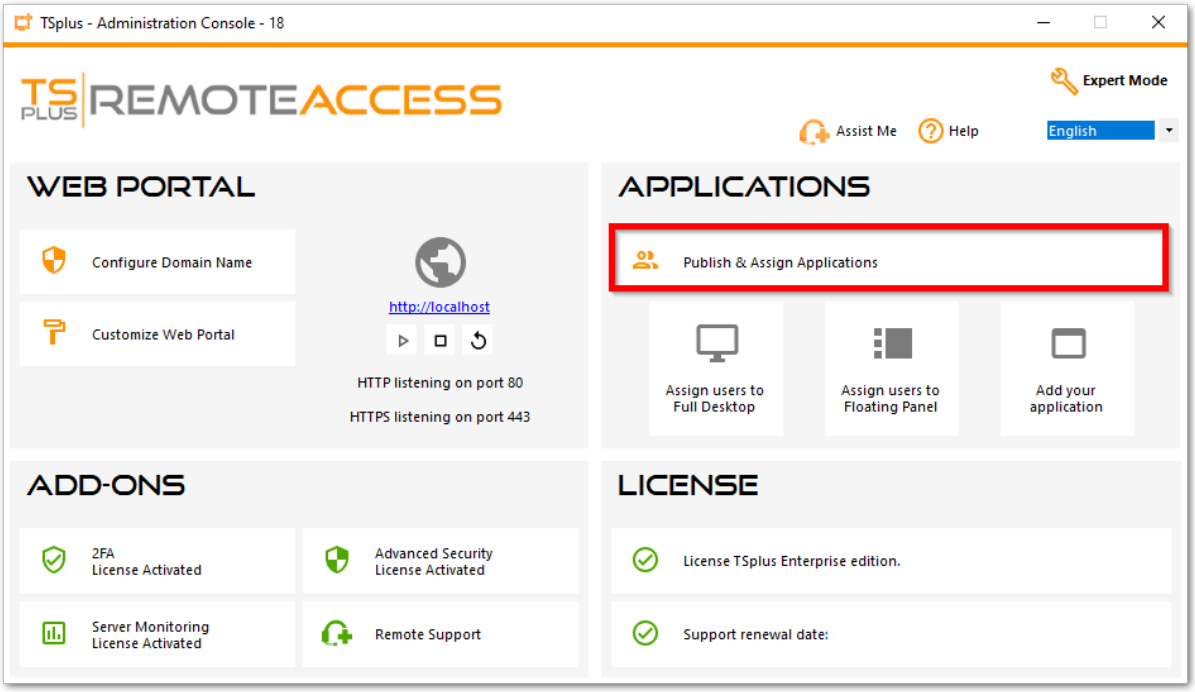


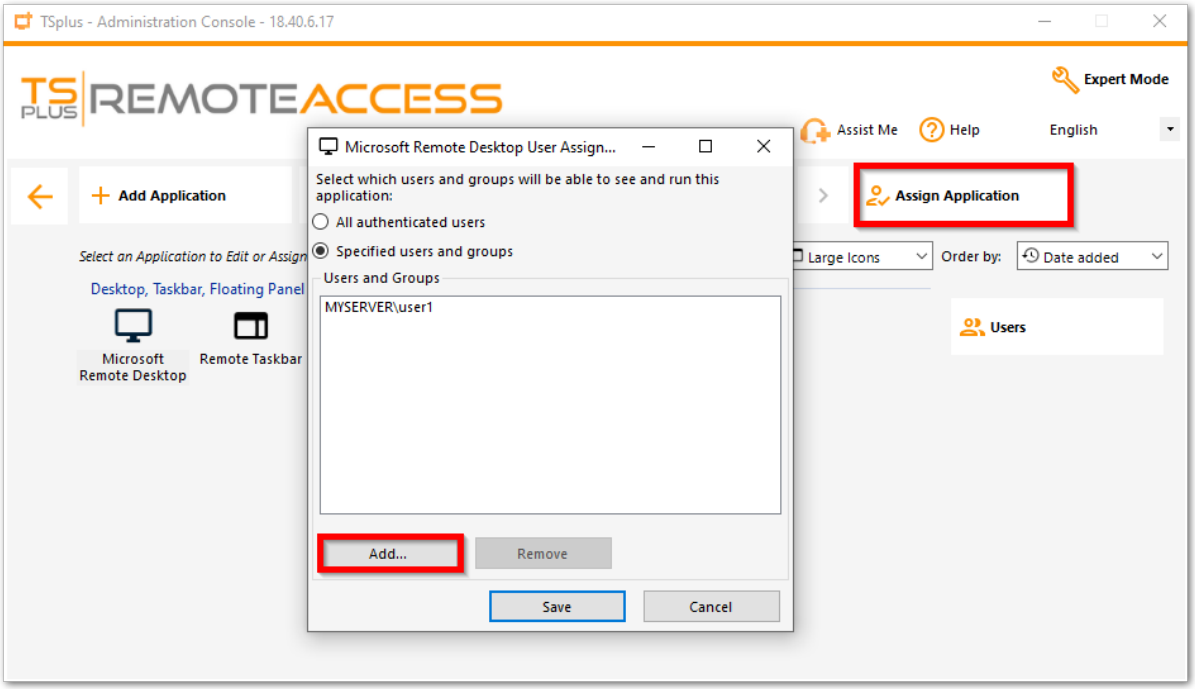
Étape 4 : Publication d'application et contrôle d'application.

Dans l'outil d'administration Remote Access, vous pouvez attribuer des applications à des utilisateurs ou à des groupes.

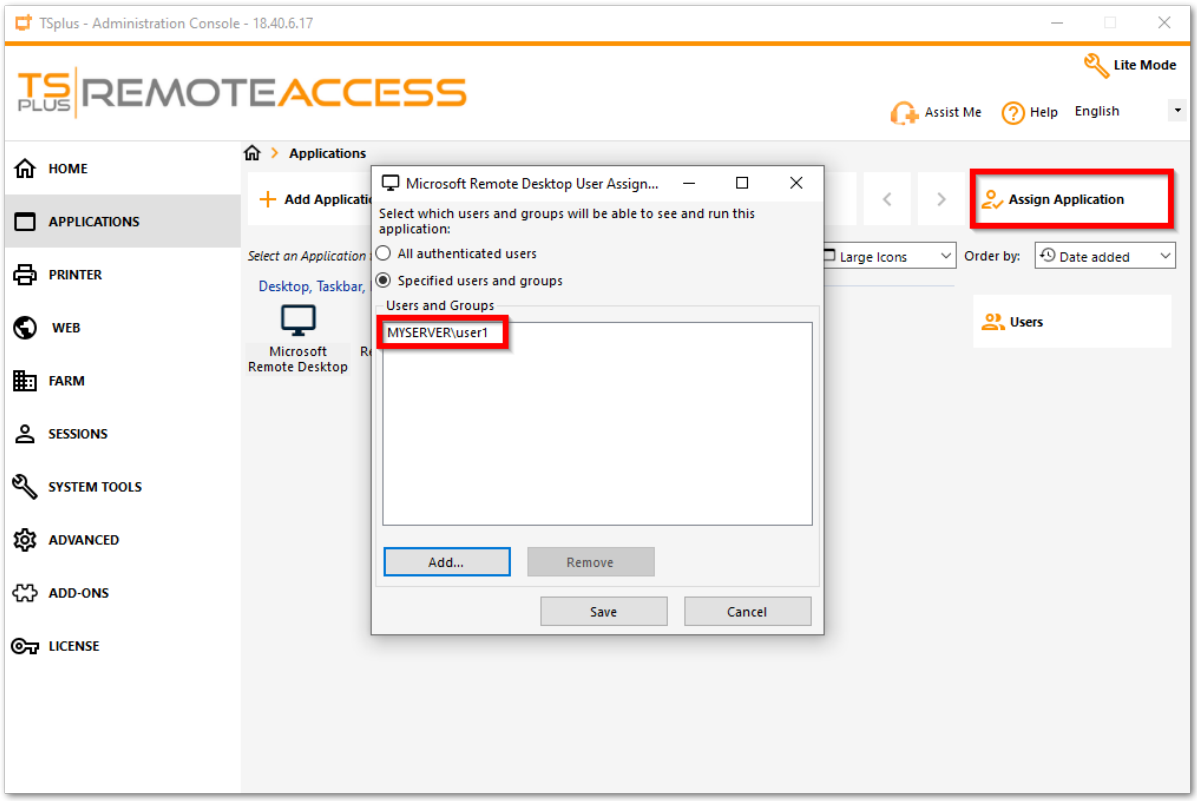
- Si vous assignez une application à un utilisateur, il ne verra que cette application.
- Vous pouvez également leur attribuer la barre des tâches TSplus, le panneau flottant ou le panneau d'application pour afficher plusieurs applications.
- Vous pouvez également publier un bureau à distance complet.

Maintenant disponible dans
Mode Lite
depuis l'onglet d'accueil.





Ou allez à **Mode Expert** > Onglet Applications pour ajouter, modifier, supprimer et attribuer des applications.



Dans cet exemple, l'administrateur a décidé que l'utilisateur 'John' obtiendra la barre des tâches TSplus. Voir cette documentation pour plus d'informations.

Merci d'utiliser TSplus Remote Access !

Rehébergement de votre licence TSplus

Hébergement en ligne

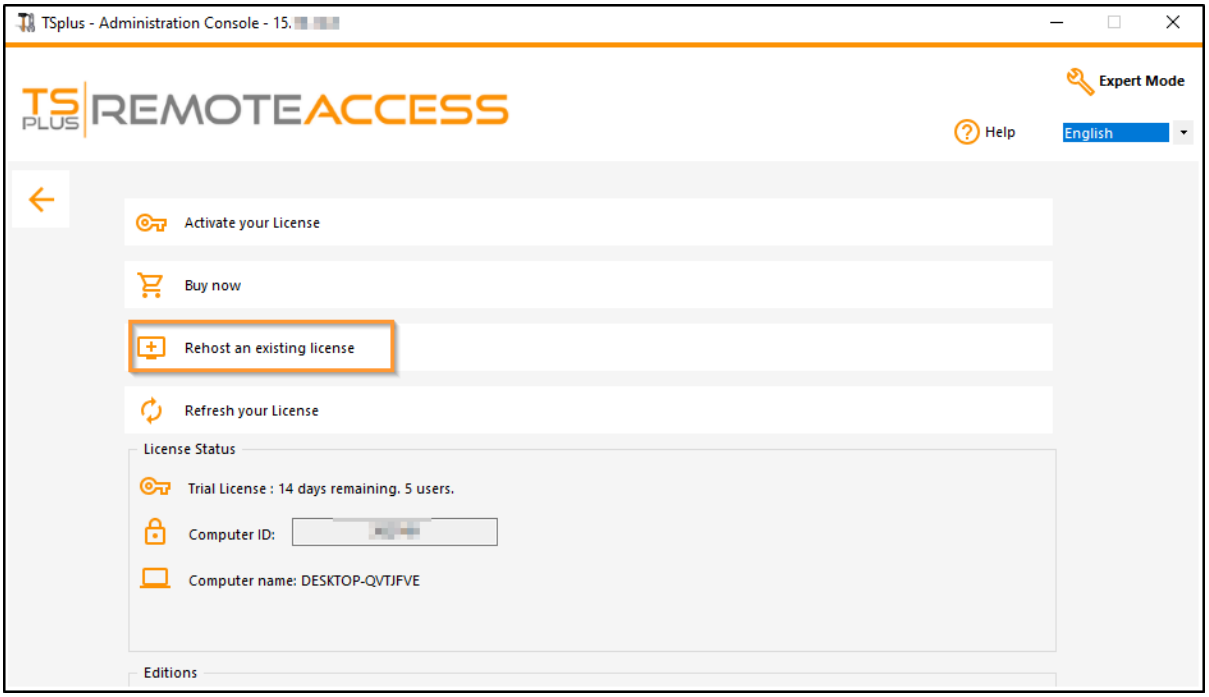
L'activation en ligne est autorisée une fois par mois.

Prérequis : Il est nécessaire d'avoir un abonnement de support actif pour réhéberger votre licence.

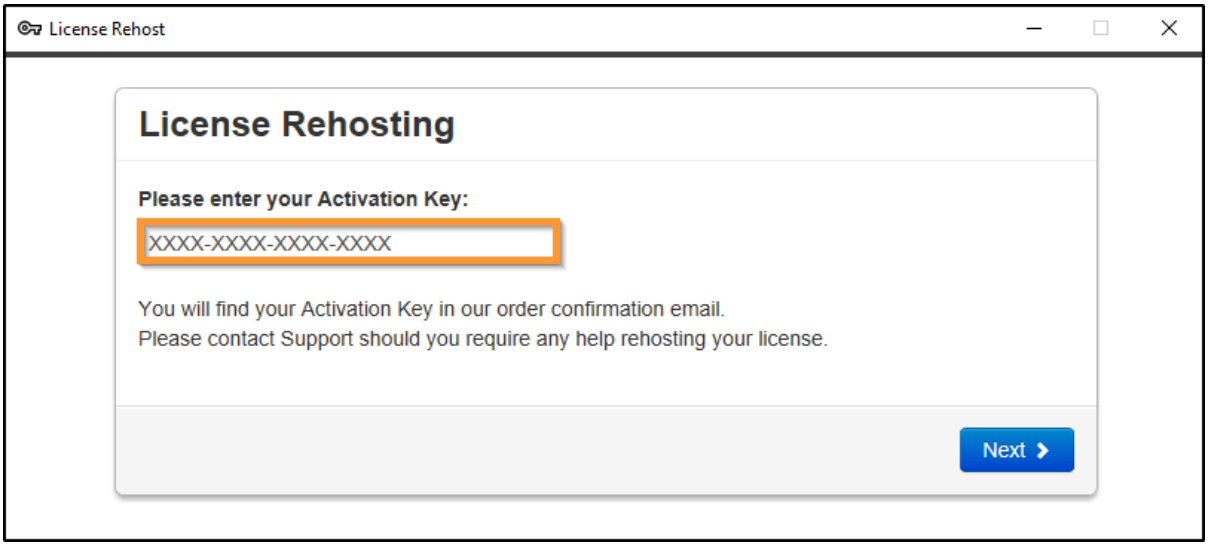
Il est nécessaire d'installer une nouvelle version de Remote Access non clonée pour générer un nouvel ID d'ordinateur.

Si vous avez dupliqué votre serveur et cloné le Remote Access, veuillez vous rendre à la page suivante : Clonez votre serveur

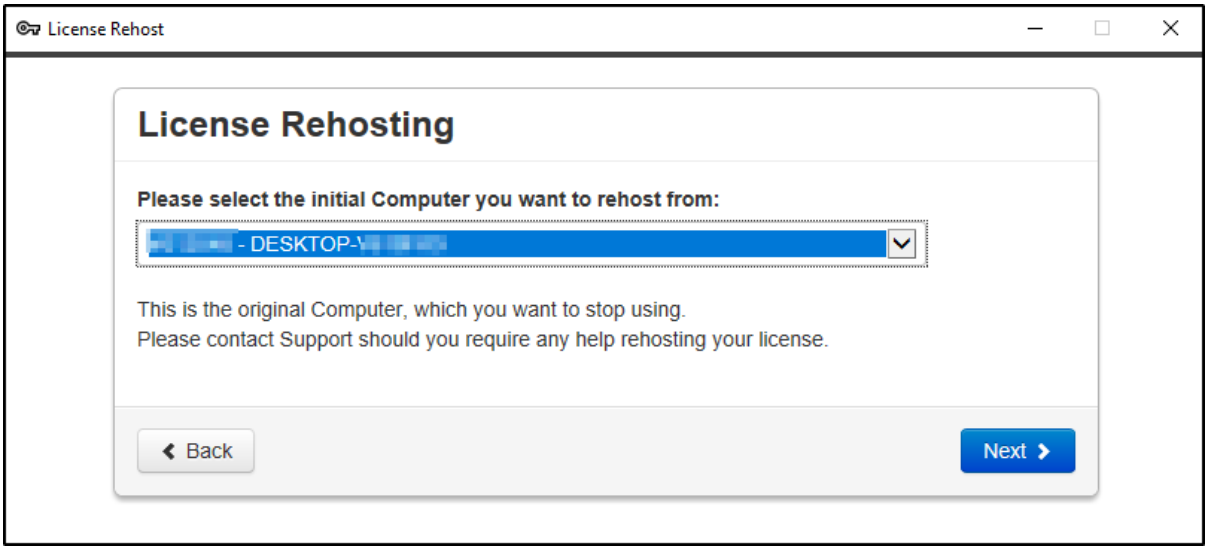
Sur le nouveau serveur Allez dans l'onglet « Licence » Cliquez sur « Réaffecter une licence existante »



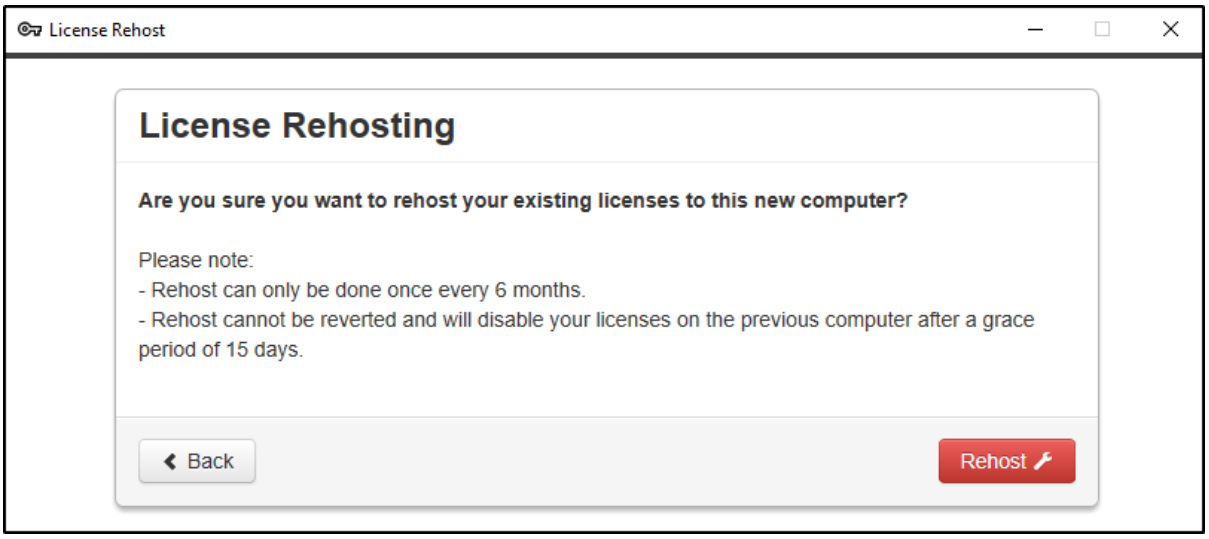
Entrez votre clé d'activation :



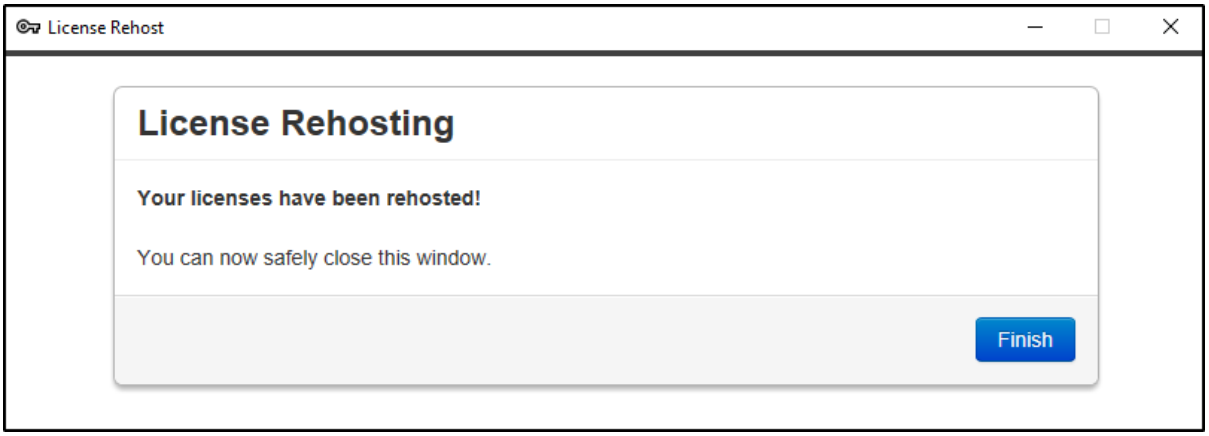
Sélectionnez l'ordinateur initial que vous souhaitez réhéberger.



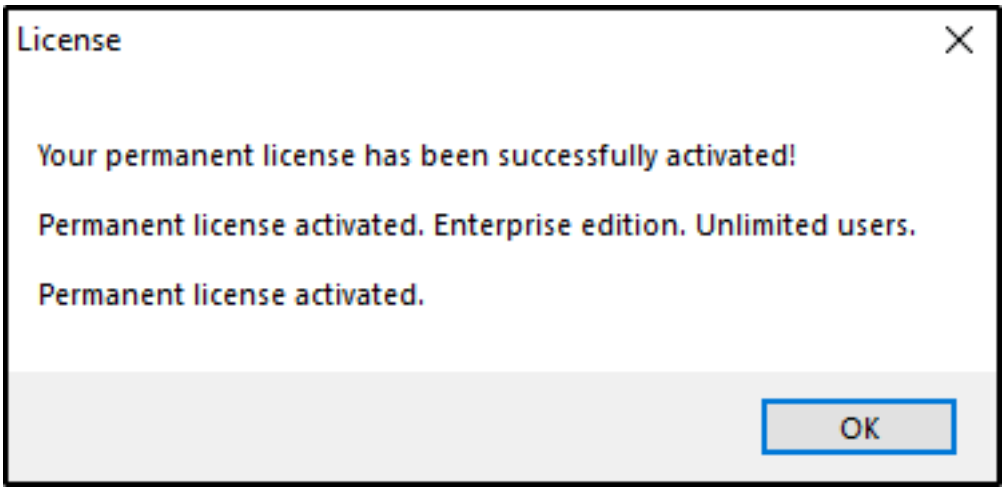
Confirmer le rehosting



Votre réhébergement de licence est terminé.

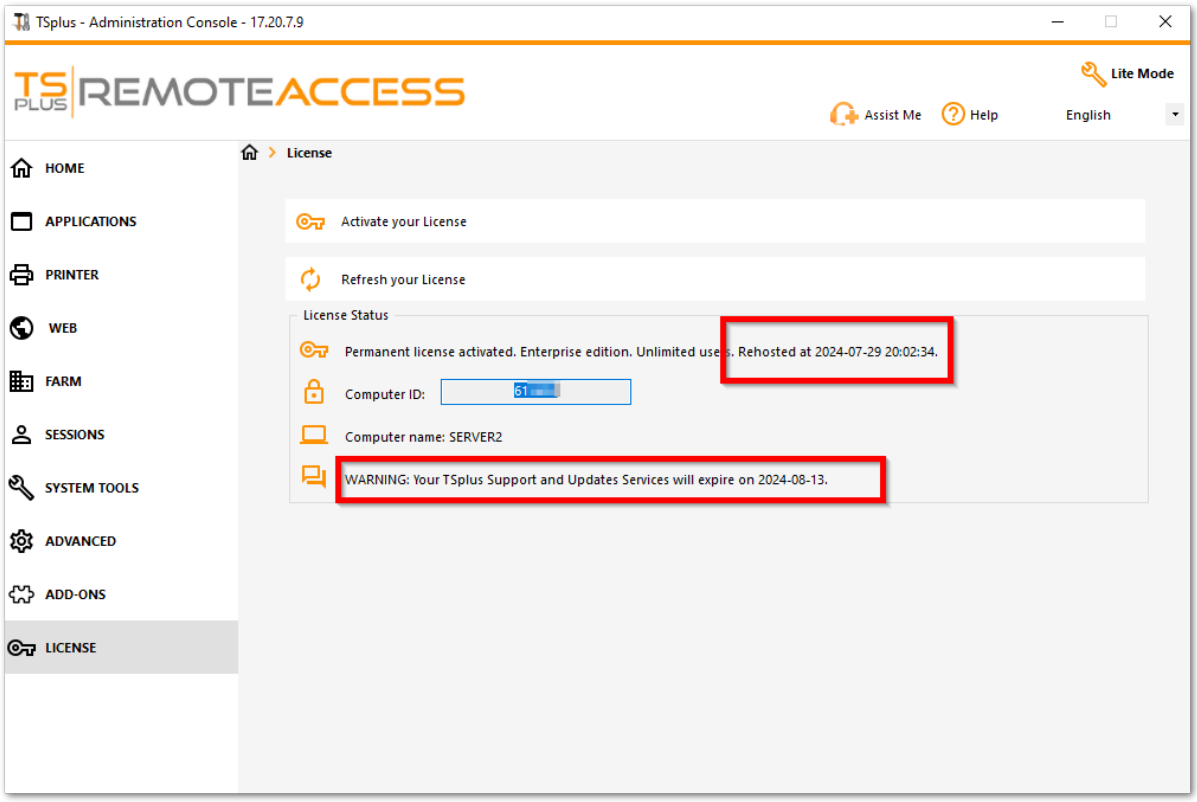


Attendez quelques instants que votre AdminTool se synchronise jusqu'à ce que la fenêtre apparaisse.



Félicitations, votre licence a été activée avec succès !

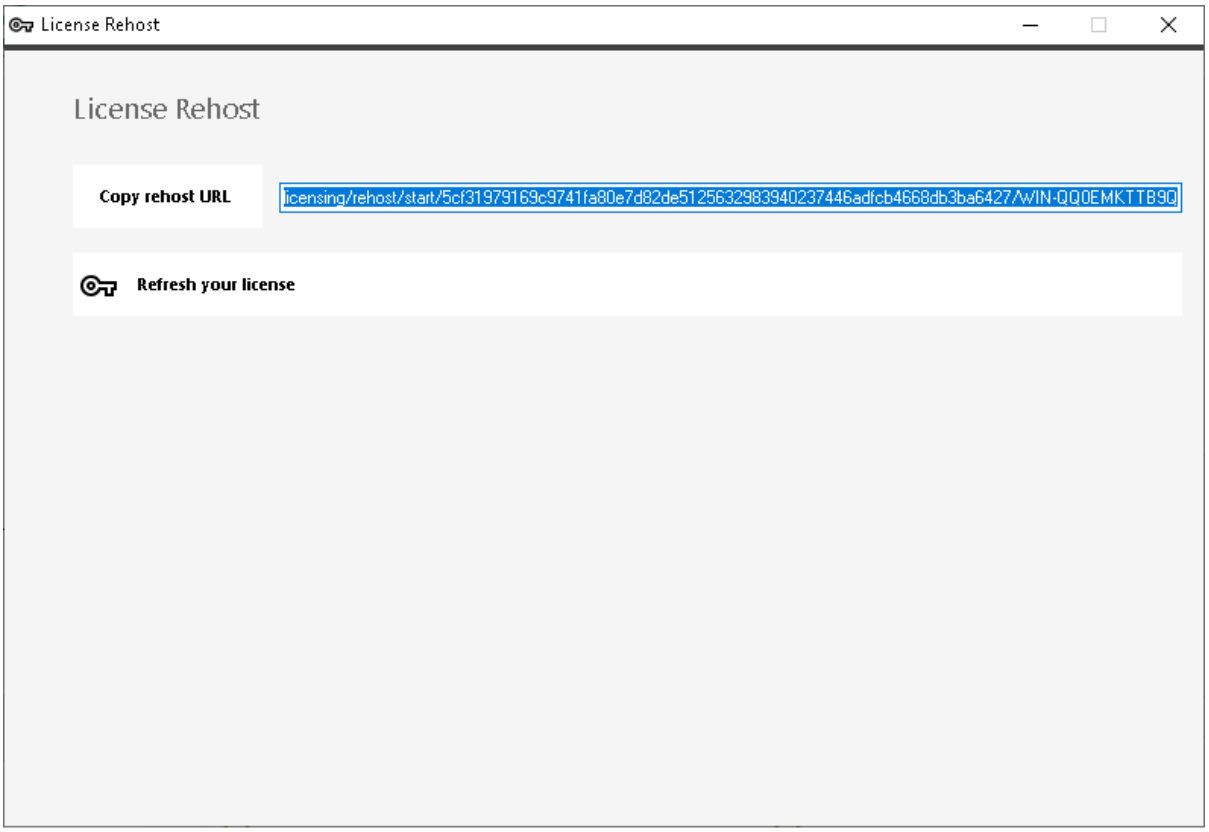
Remarque : Un message apparaîtra sur l'ancien serveur avec la date de réhébergement ainsi que la date de fin d'utilisation.
Après un rehosting, l'ancien serveur fonctionnera toujours pour **15 jours** pour vous aider à effectuer la transition.



Hébergement hors ligne

L'activation hors ligne peut également être effectuée pour les licences de rehosting.

Lorsque le serveur n'a pas accès à Internet, le bouton « réhéberger une licence existante » affichera la page de réhébergement hors ligne :



Le processus est le même que l'activation hors ligne.

Connexion à distance depuis un appareil iPhone / iPad / Android

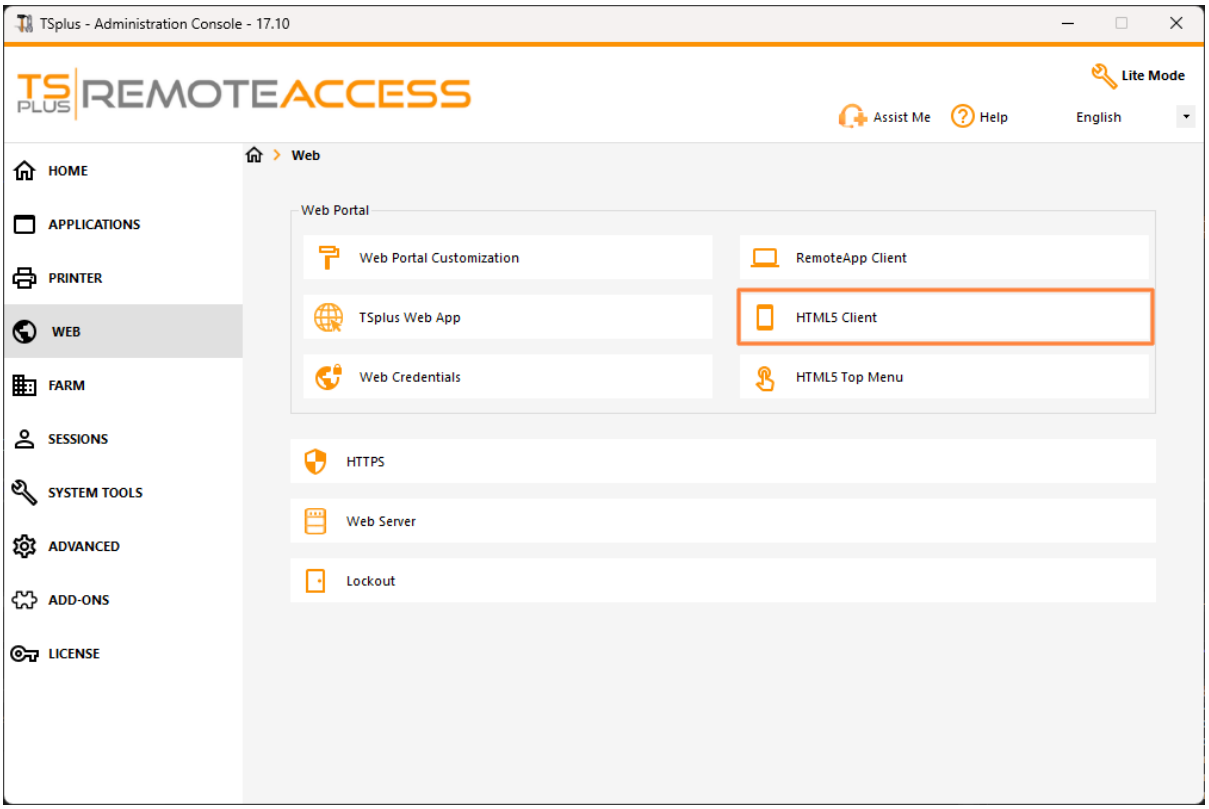
Vous pouvez vous connecter à votre serveur Terminal Service Plus sur n'importe quel navigateur depuis n'importe quel appareil mobile prenant en charge la technologie HTML5, tel que :

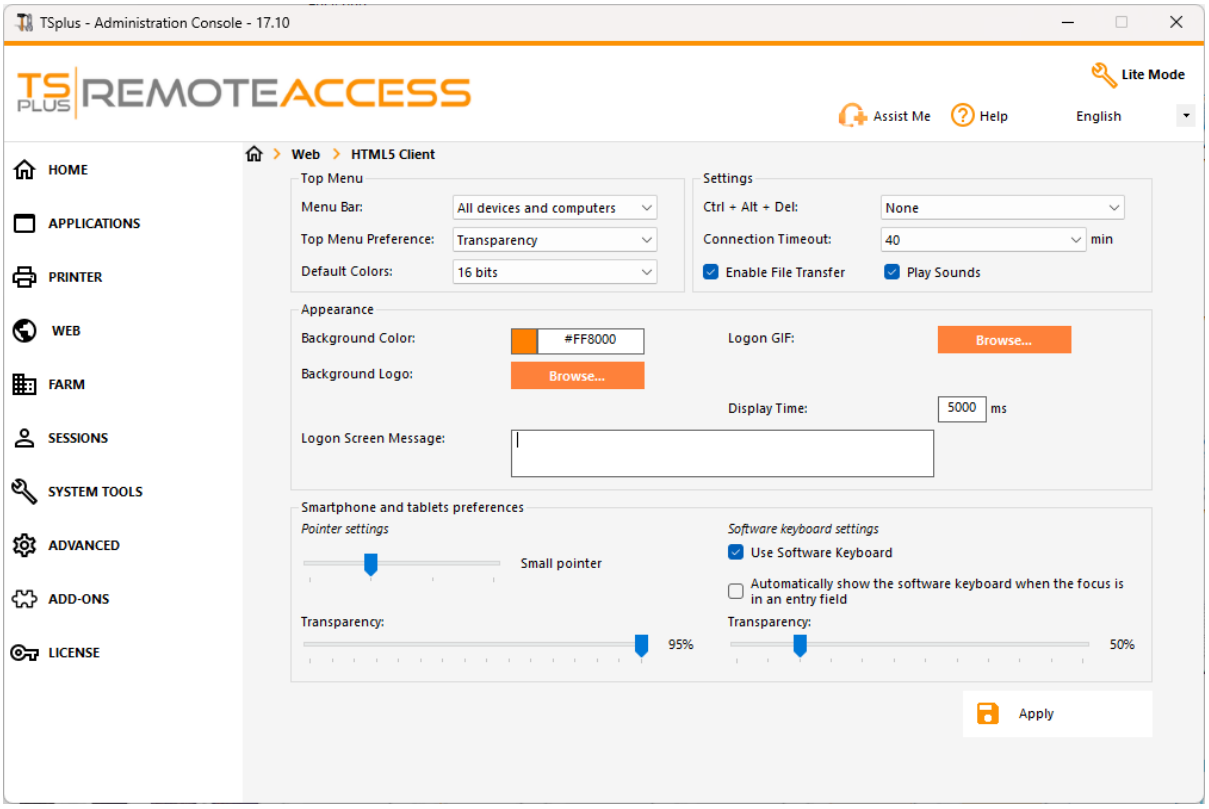
- un iPhone
- un iPad
- un smartphone Android
- une tablette Android

Modifier les préférences pour les appareils mobiles

Depuis la version 11.20, le client HTML5 de TSplus a été considérablement amélioré pour offrir la meilleure expérience utilisateur possible, même depuis des smartphones ou des tablettes. Le clavier a été repensé pour apparaître automatiquement lorsque le focus est sur un champ de saisie. Le pointeur de la souris a été redessiné pour faciliter la sélection des boutons et des champs, même s'ils sont situés sur les bords gauche ou inférieur d'un smartphone.

Vous pouvez configurer divers paramètres HTML5 différents pour les appareils mobiles ou les ordinateurs sur la tuile client HTML5 de l'onglet Web :





- Affichez la barre de menu pour tous les appareils et ordinateurs ou uniquement pour les appareils mobiles.
- Activer ou désactiver le transfert de fichiers.
- Autoriser le raccourci Ctrl + Alt + Suppr sur un type de dispositif spécifique.
- Choisissez votre affichage de menu supérieur préféré entre transparence et solide.

- Le nombre de bits de couleur graphique.
- Le délai d'attente de connexion, la durée maximale (en secondes) pendant laquelle une session reste active en attendant qu'un client se reconnecte. 0 pour désactiver le délai d'attente.
- Afficher ou masquer les messages d'avertissement.
- Activer ou désactiver les sons.
- Choisissez votre couleur de fond préférée.
- Ajoutez un logo à l'arrière-plan.
- Changez le message de l'écran de connexion et le gif animé, ainsi que son temps d'affichage en millisecondes.

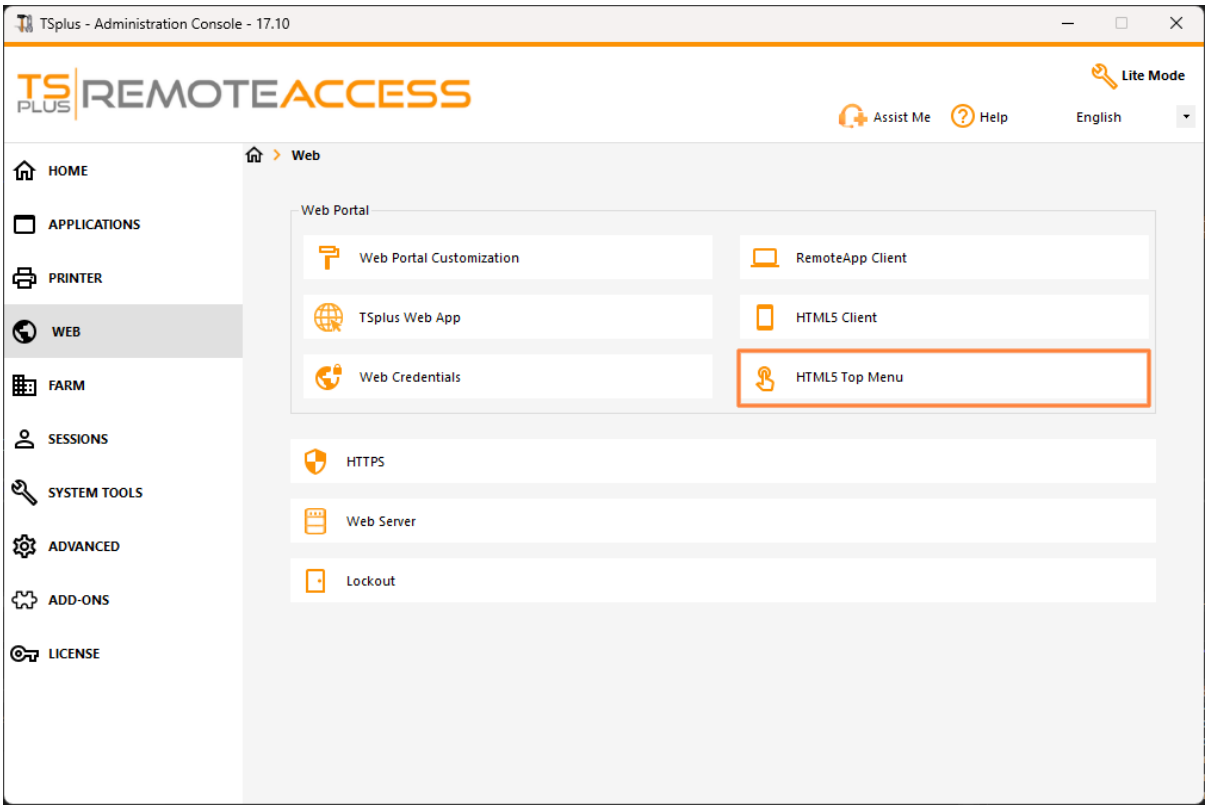
Préférences pour smartphones et tablettes :

- Si l'administrateur utilise le clavier logiciel, lorsqu'il cache un champ de saisie, l'application est déplacée vers le haut et l'utilisateur peut toujours voir ce qu'il tape.

- L'administrateur peut sélectionner une petite, une moyenne ou une grande taille pour le pointeur de la souris ou aucun pointeur de souris du tout. Cela rend la navigation dans son application intuitive pour l'utilisateur.

- Il peut également sélectionner le niveau de transparence pour la souris et le clavier.

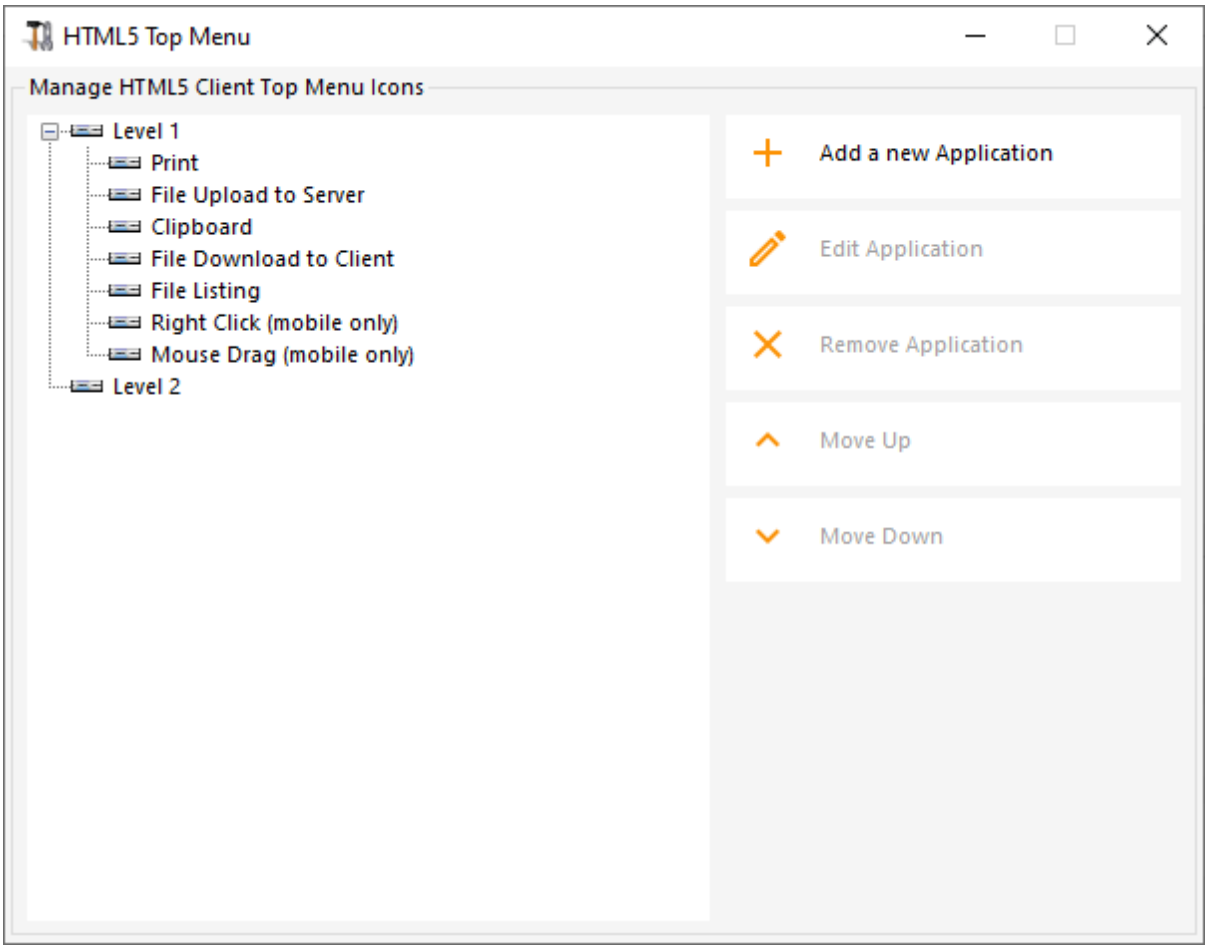
Dans l'onglet Menu supérieur HTML5, vous pouvez ajouter des applications qui seront affichées au premier ou au deuxième niveau du Menu supérieur en HTML5 :



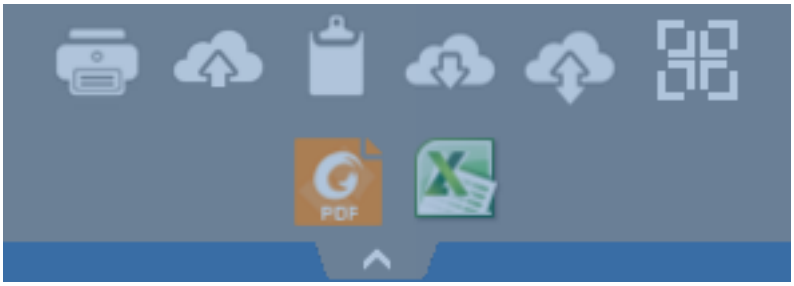
Sur le niveau un, vous pouvez trouver les fonctionnalités HTML5 intégrées : impression, transfert de fichiers et un presse-papiers. (Pour plus d'informations sur ces fonctionnalités, allez à ces pages :)

Imprimante universelle pour HTML5 , Utilisation du transfert de fichiers et Utiliser le Presse-papiers .)

Dans cet exemple, Foxit et Excel sont publiés au niveau 2 :

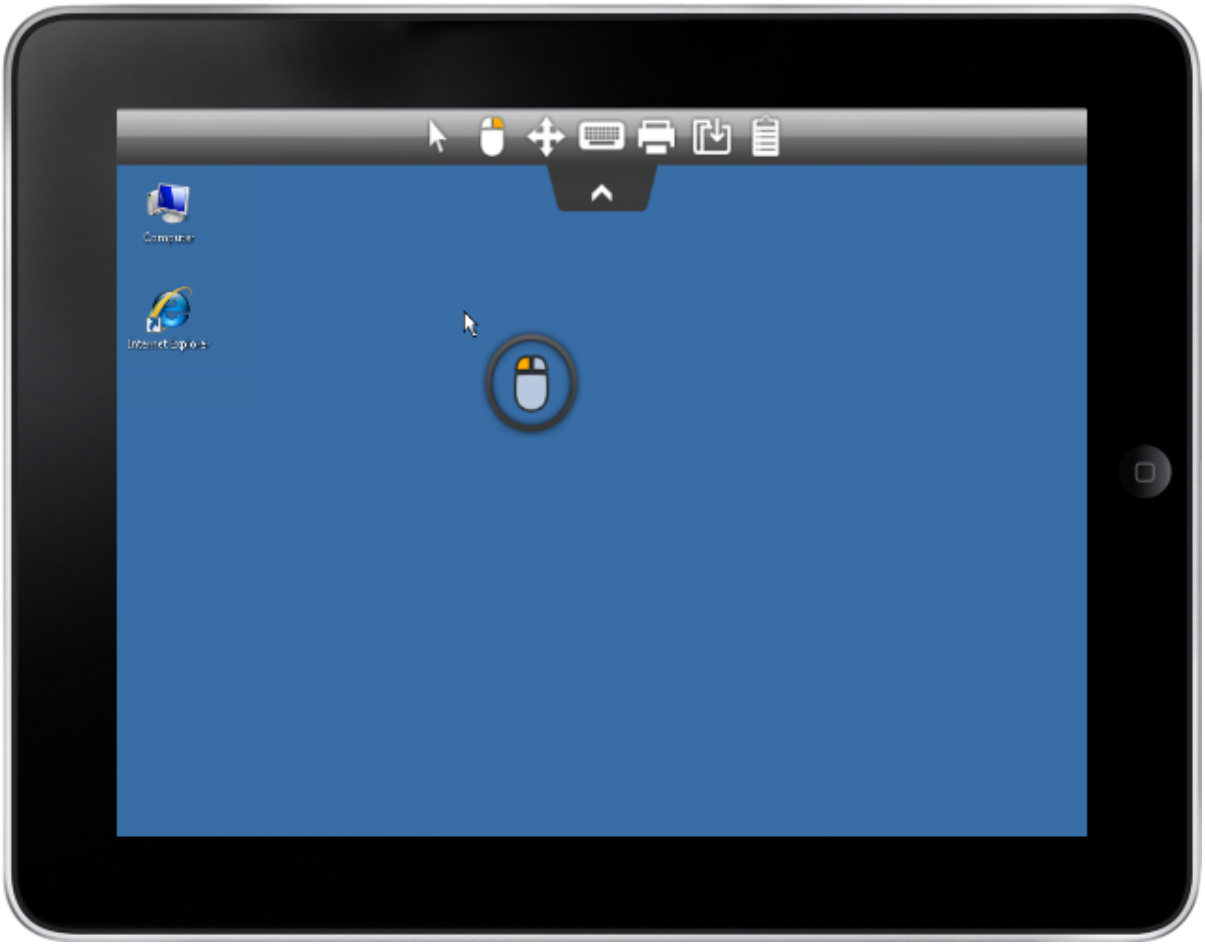


Et peut être trouvé sous les fonctionnalités intégrées dans le menu supérieur de la session HTML5 :



De plus, l'icône en haut à droite vous permet de passer votre session en mode plein écran.

Client HTML5 intégré de Terminal Service Plus fournit à l'utilisateur un tout nouveau menu sur les tablettes et les appareils mobiles. Avec ce nouveau menu, l'utilisateur bénéficie d'un accès facile au clavier mobile et au clic droit, mais aussi au partage de fichiers et à notre fonctionnalité d'impression universelle unique !



Veuillez vous référer à cette documentation pour savoir comment utiliser la mini souris et le clavier.

Sélection de la langue

Vous pouvez maintenant changer la langue avec le bouton de langue à droite du menu supérieur :



Vous pouvez choisir la langue pour le pays spécifique que vous souhaitez dans ce menu :

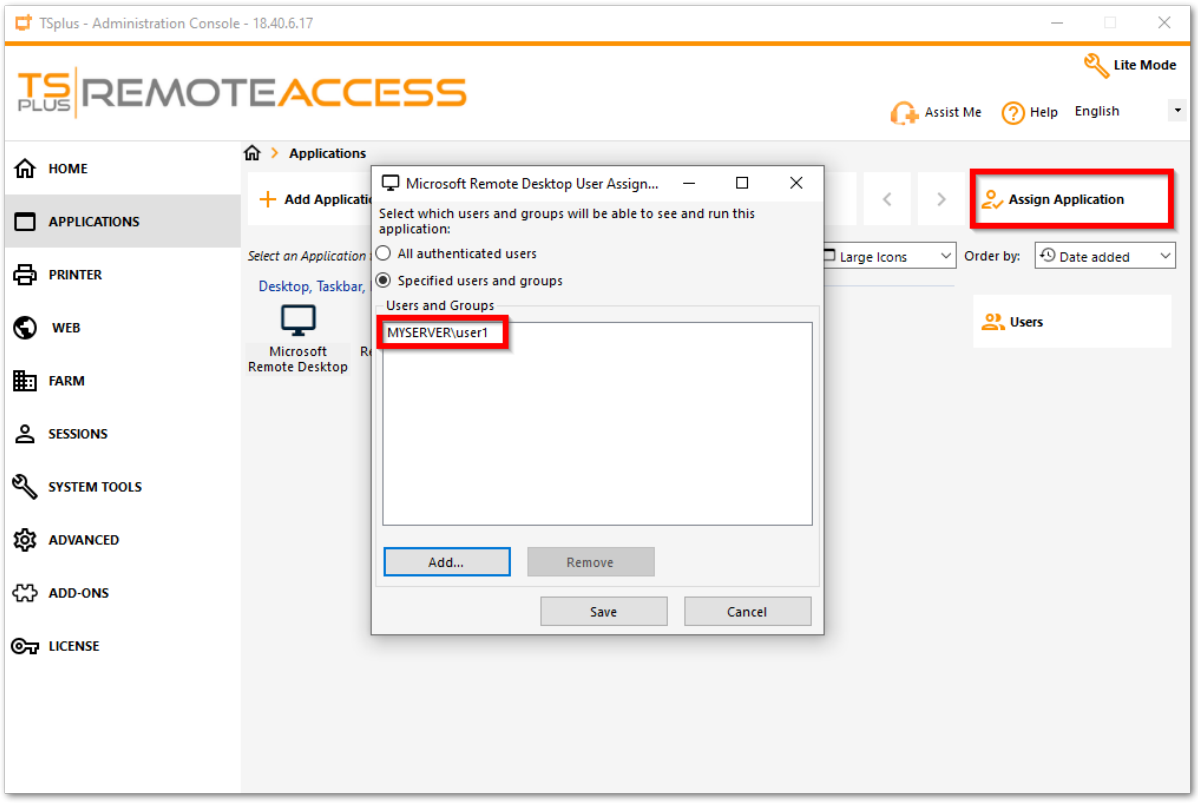
	Language	Locale	Value
◯	Portal	as_portal	
◯	Browser	as_browser	
◯	Gateway	as_gateway	
◯	Arabic	ar_ar	1025
◯	Belarusian	be_be	1059
◯	Bulgarian	bg_bg	1026
◯	Bengali	bn_bn	1093
◯	Bosnian (Cyrillic)	bs_cyrl_ba	8218
◯	Bosnian (Latin)	bs_latn_ba	5146
◯	Catalan	ca_ca	1027
◯	Czech	cs_cs	1029
◯		cs_cz	1029
◯	Welsh	cy_gb	1106
◯	Danish	da_da	1030
◯		da_dk	1030
◯	German (Swiss)	de_ch	2055
◯	German	de_de	1031
◯	Divehi	dv_dv	1125
◯	Greek	el_el	1032
◯		el_gr	1032
◯	English (Canada)	en_ca	4105

Thèmes de la barre des tâches et des bureaux à distance

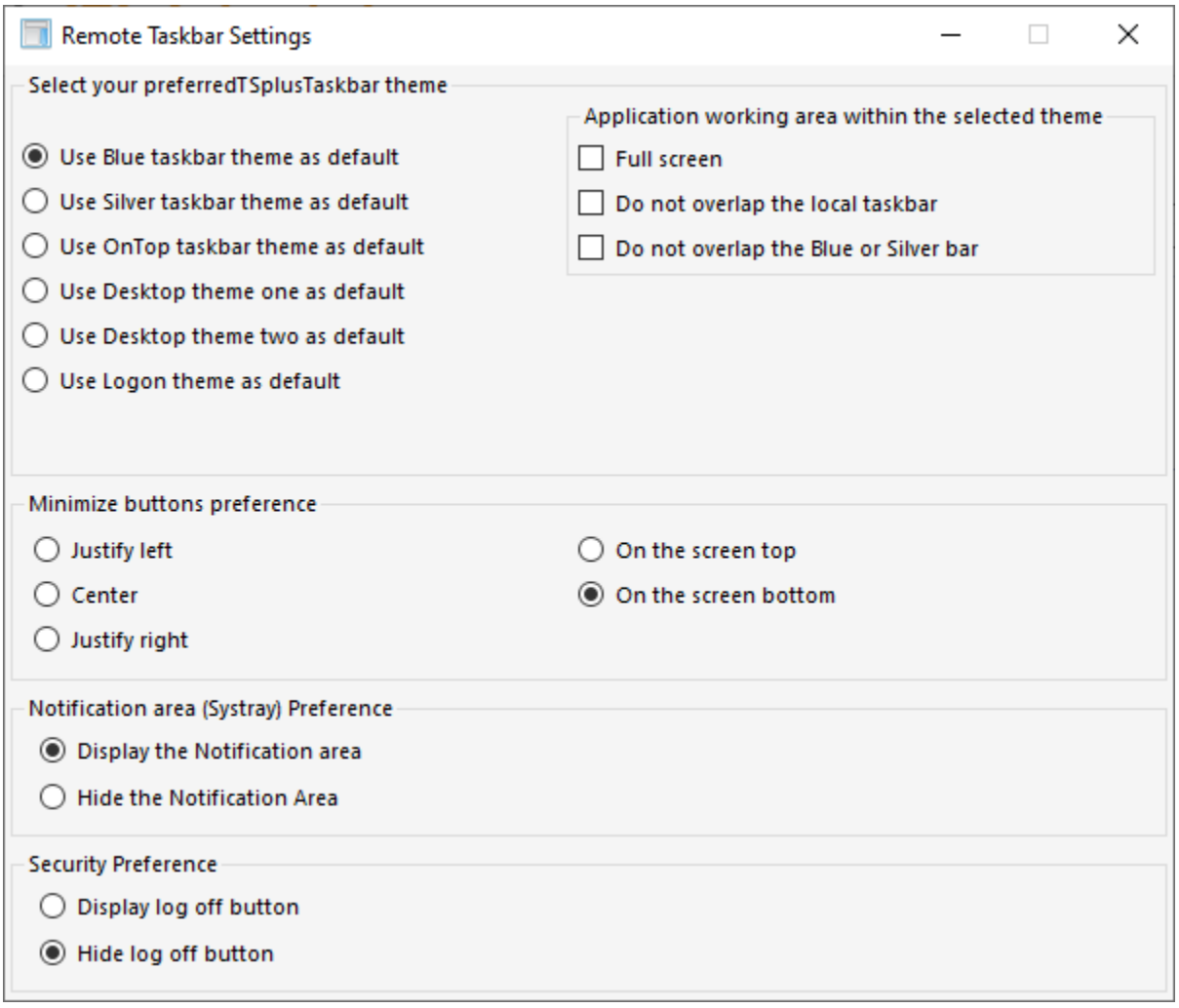
Outils d'administration sur le serveur

Avec l'AdminTool, l'administrateur peut choisir entre 4 modes d'affichage lorsqu'il assigne des applications : Le Bureau à distance Microsoft , La barre des tâches à distance , Le panneau flottant ou Le Panneau d'Application La barre des tâches distante, les panneaux flottants et d'application sont disponibles pour tout méthode de connexion.

Lorsque vous assignez des applications à un utilisateur, vous pouvez activer la barre des tâches à distance de TSplus. L'utilisateur peut lancer des applications à distance d'un simple clic sur la barre des tâches de TSplus et avoir toujours le bureau local complet à sa disposition. Vous pouvez assigner la barre des tâches à distance à vos utilisateurs ou groupes en double-cliquant dessus ou en la sélectionnant, puis en cliquant sur la tuile "Assigner une application".



L'administrateur peut facilement décider quel sera le thème par défaut du bureau à distance que l'utilisateur verra en ouvrant une session. Sélectionnez la barre des tâches TSplus Remote, puis cliquez sur « Modifier l'application » :



- Seul l'administrateur peut choisir les thèmes pour ses utilisateurs.
- Il peut choisir d'afficher les applications maximisées en mode plein écran ou de ne pas chevaucher la barre des tâches TSplus ainsi que les barres des tâches Silver ou Blue.
- La position des boutons minimisés sur la barre des tâches peut être changée (en haut de l'écran, en bas, à droite, à gauche, ou au centre).

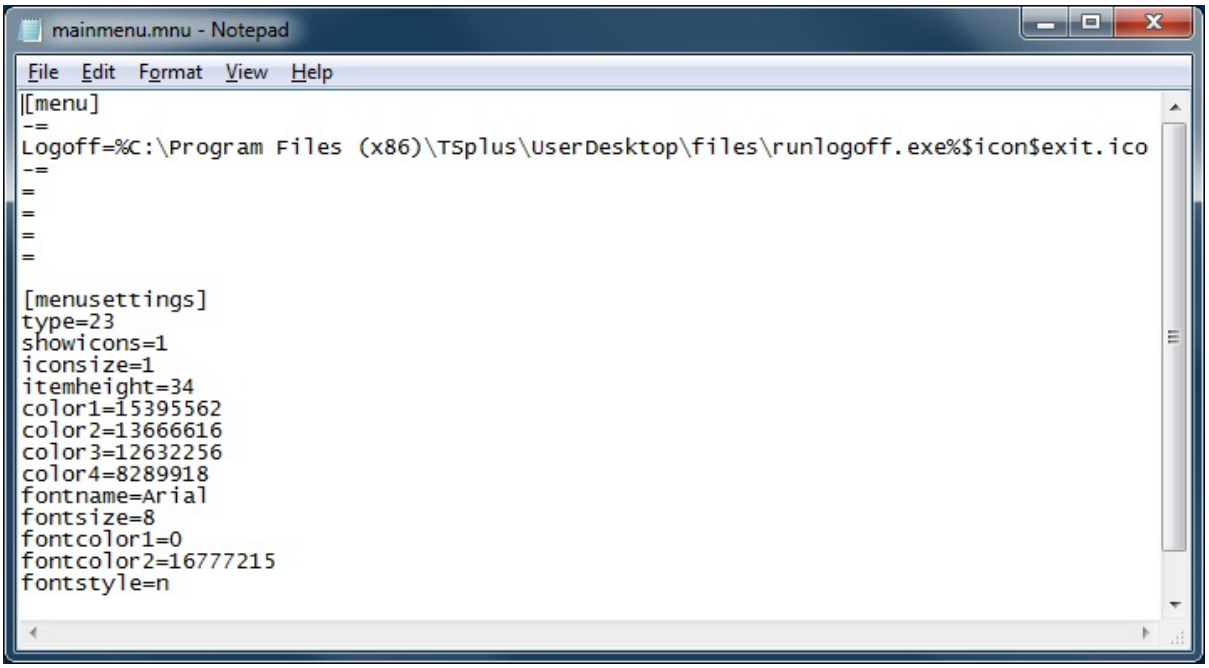
  L'administrateur peut même décider de l'afficher en haut de l'écran de l'utilisateur au lieu du bas par défaut.
-

Les icônes de la barre d'état système peuvent être masquées en cochant le cercle « Masquer la zone de notification ».

- Depuis la version 12.60 de TSplus, le bouton de déconnexion peut désormais être masqué.

En modifiant le menu des utilisateurs, l'administrateur peut ajouter/supprimer des applications et des fonctionnalités. La personnalisation du menu des utilisateurs est facile.

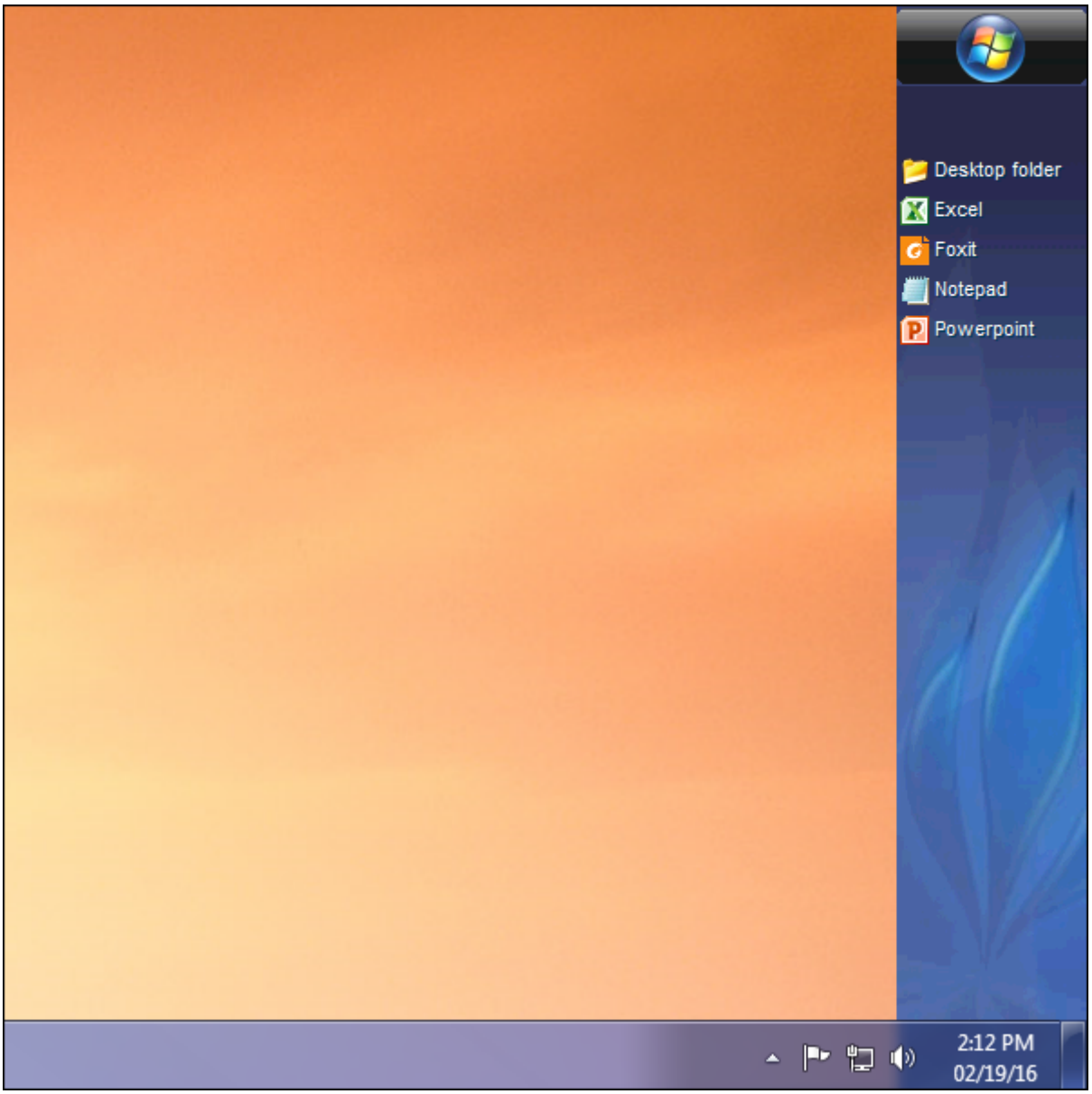
Le contenu du menu des utilisateurs (situé dans Program Files/TSplus/UserDesktop/mainmenu.mnu) est modifiable par l'administrateur à l'aide de Notepad :



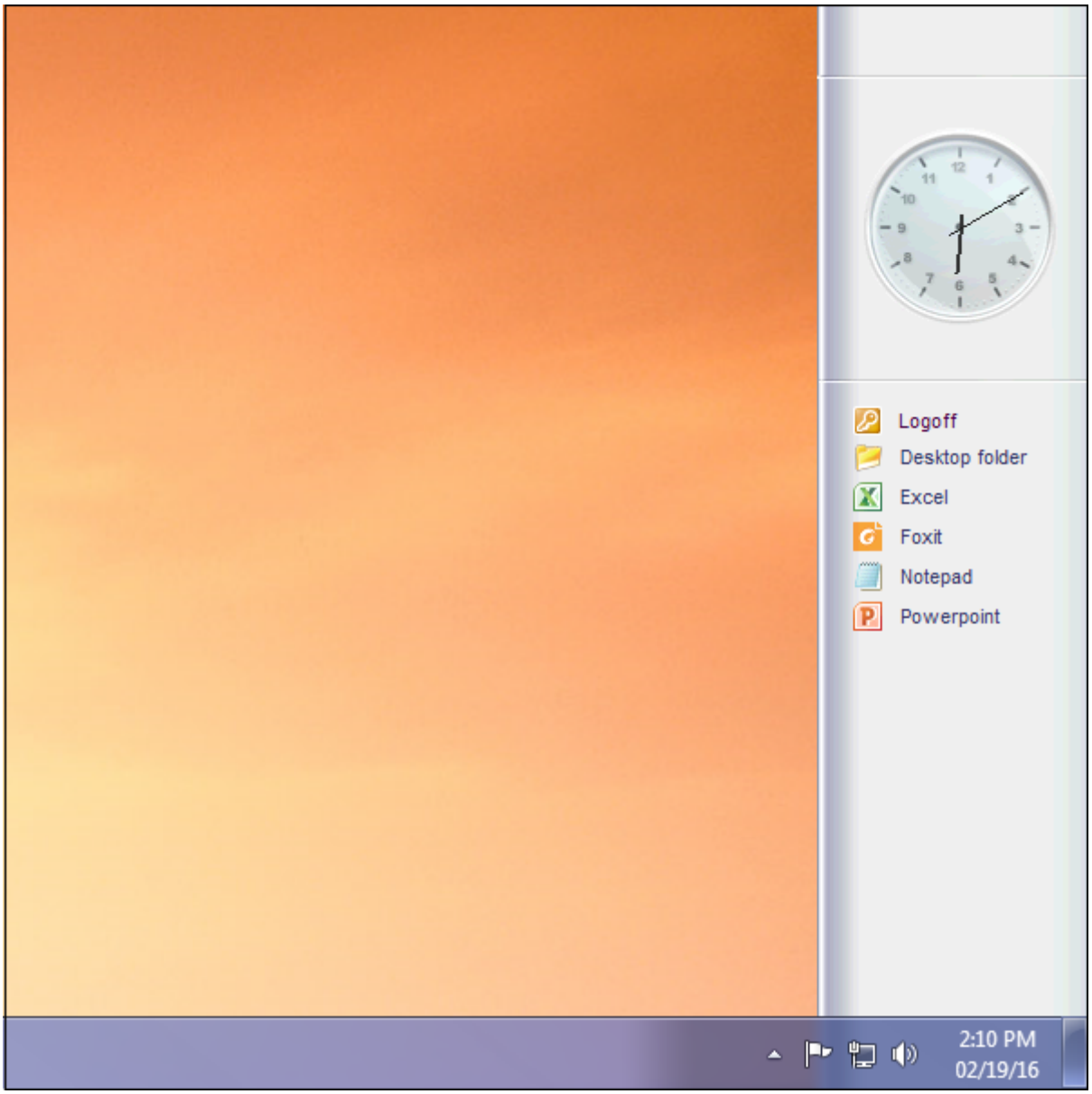
Sur le carreau des applications de l'AdminTool, l'administrateur peut sélectionner 3 styles différents de Remote Desktop TSplus Taskbar.

L'utilisateur peut lancer des applications à distance d'un simple clic sur la barre des tâches TSplus et avoir toujours le bureau local complet à disposition.

Barre des tâches bleue à droite



Barre des tâches thème argenté à droite



Sur la barre des tâches supérieure



Retour en haut

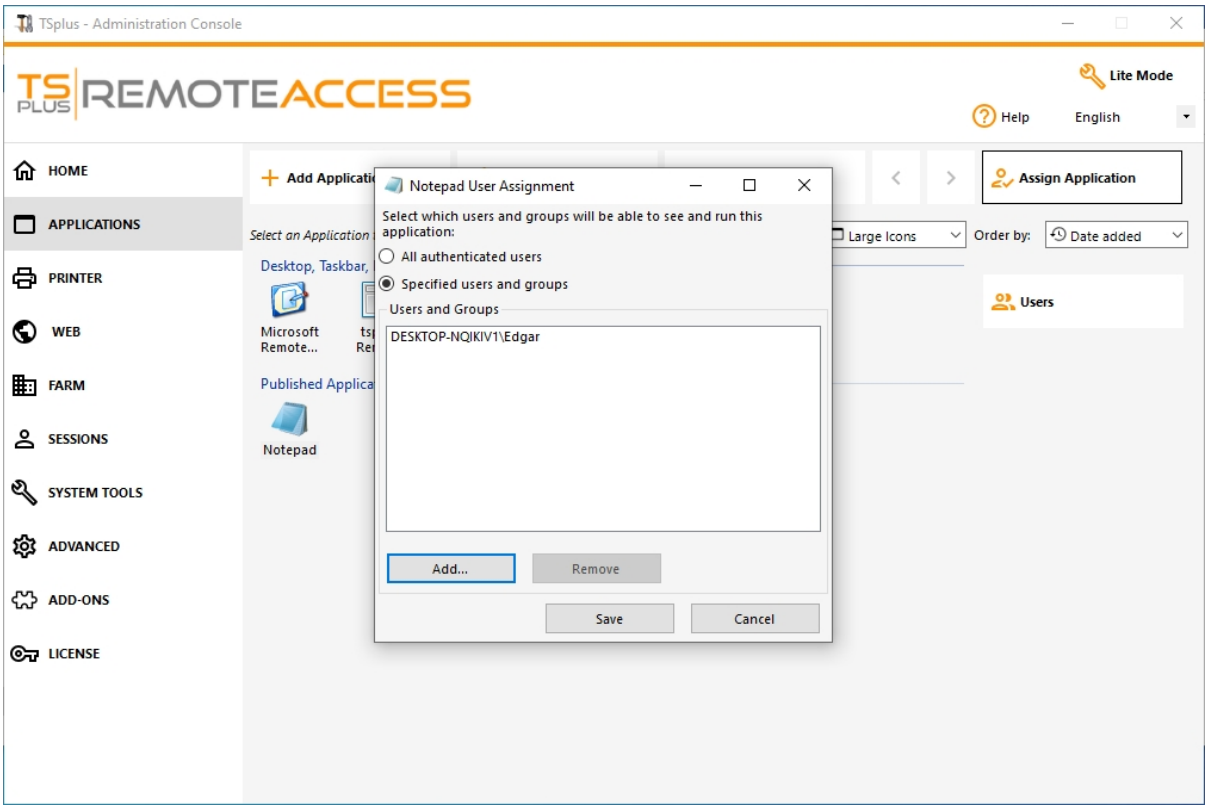
Avec l'AdminTool, l'administrateur peut facilement décider quel sera le thème par défaut du

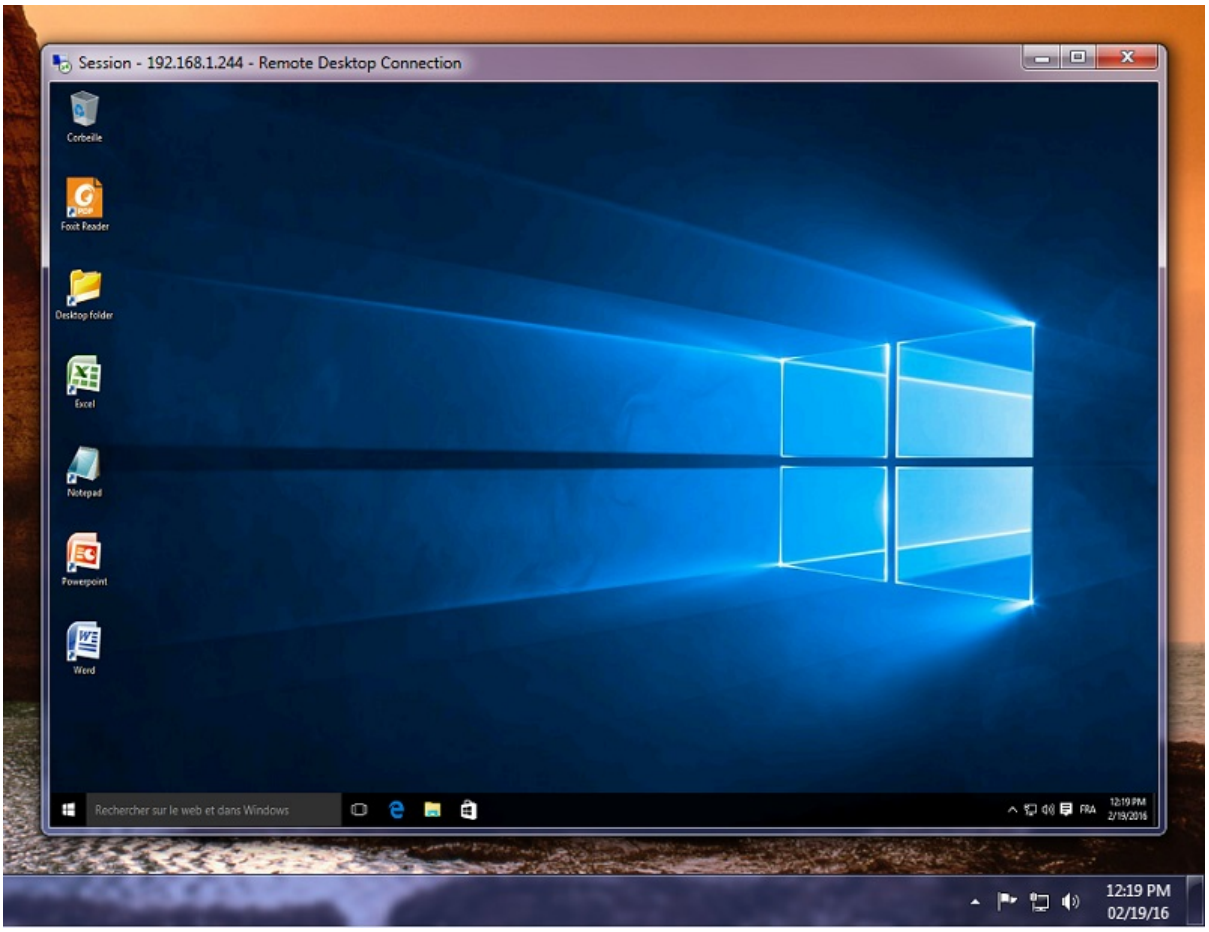
Remote Desktop que l'utilisateur verra en ouvrant une session. Il a le choix entre 4 styles différents de Remote Desktop en plein écran. Le Remote Desktop standard de Microsoft peut également être utilisé si souhaité.

Parce que ces bureaux TSplus sont des bureaux en plein écran, l'affichage de l'utilisateur est entièrement rempli lorsqu'une session est ouverte à partir de clients légers dédiés, de tout client basé sur RDP, ou accessible à partir d'une page web ou des clients TSplus Remote Desktop.

Il y a des avantages par rapport à un Bureau à distance standard. Cela améliore la sécurité du serveur (pas de bouton Démarrer ni de contrôle total du Bureau).

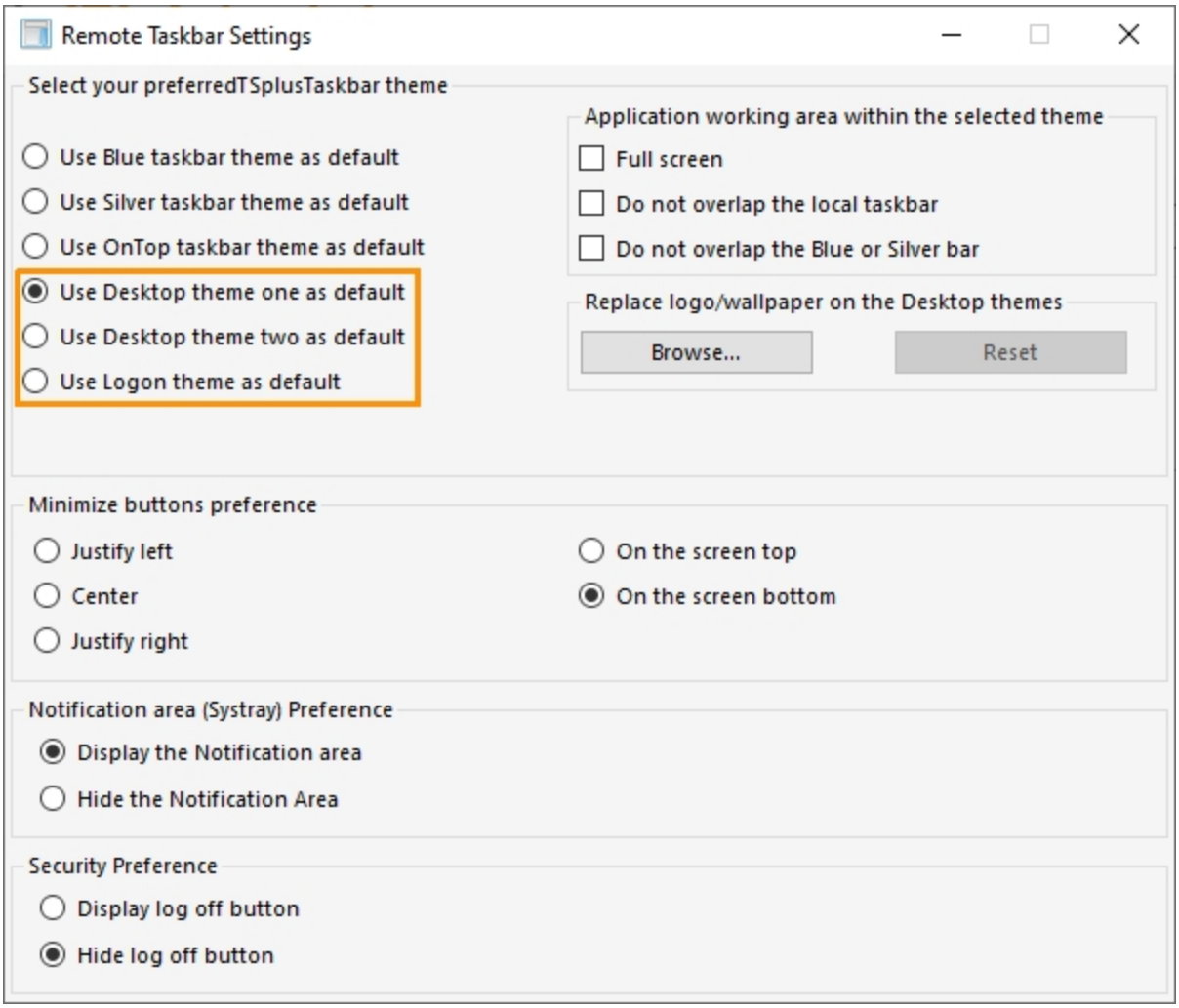
Bureau à distance Microsoft Standard





- L'utilisateur dispose d'un bureau complet comprenant le bouton Démarrer et un contrôle total du bureau.
- Pour attribuer à un bureau complet, il suffit d'attribuer l'application Microsoft Remote Desktop.

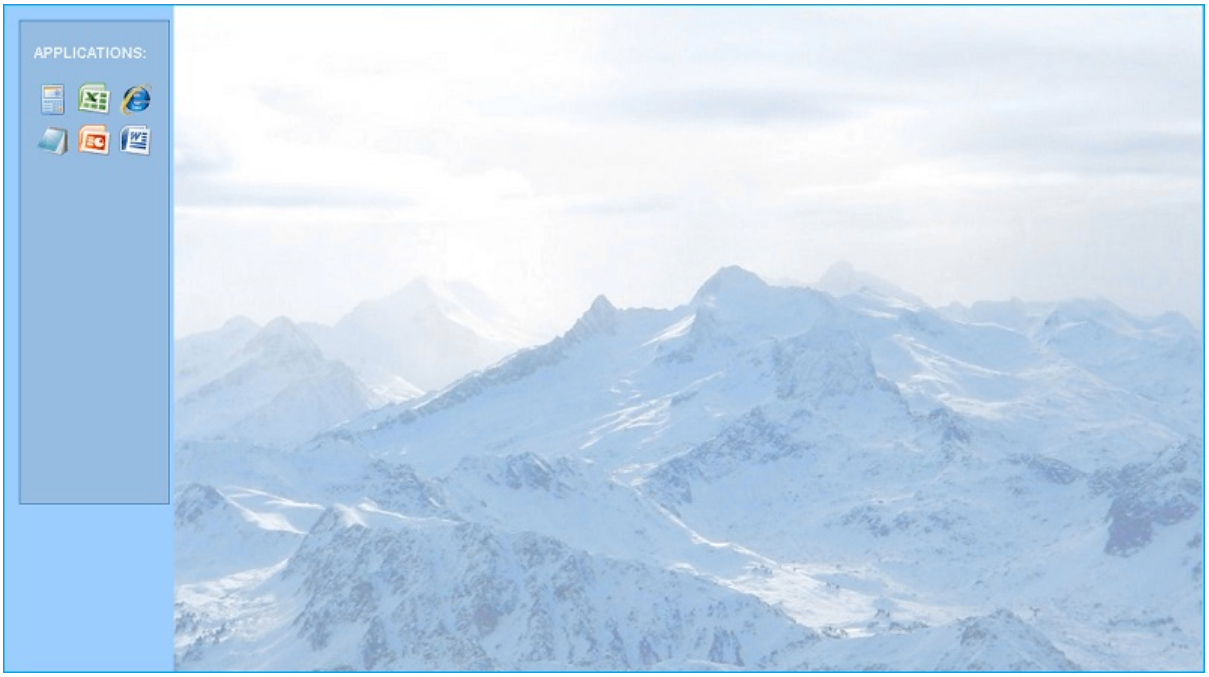
Pour changer les thèmes du Bureau, vous devrez attribuer la barre des tâches TSplus Remote et choisir entre les 3 thèmes suggérés :



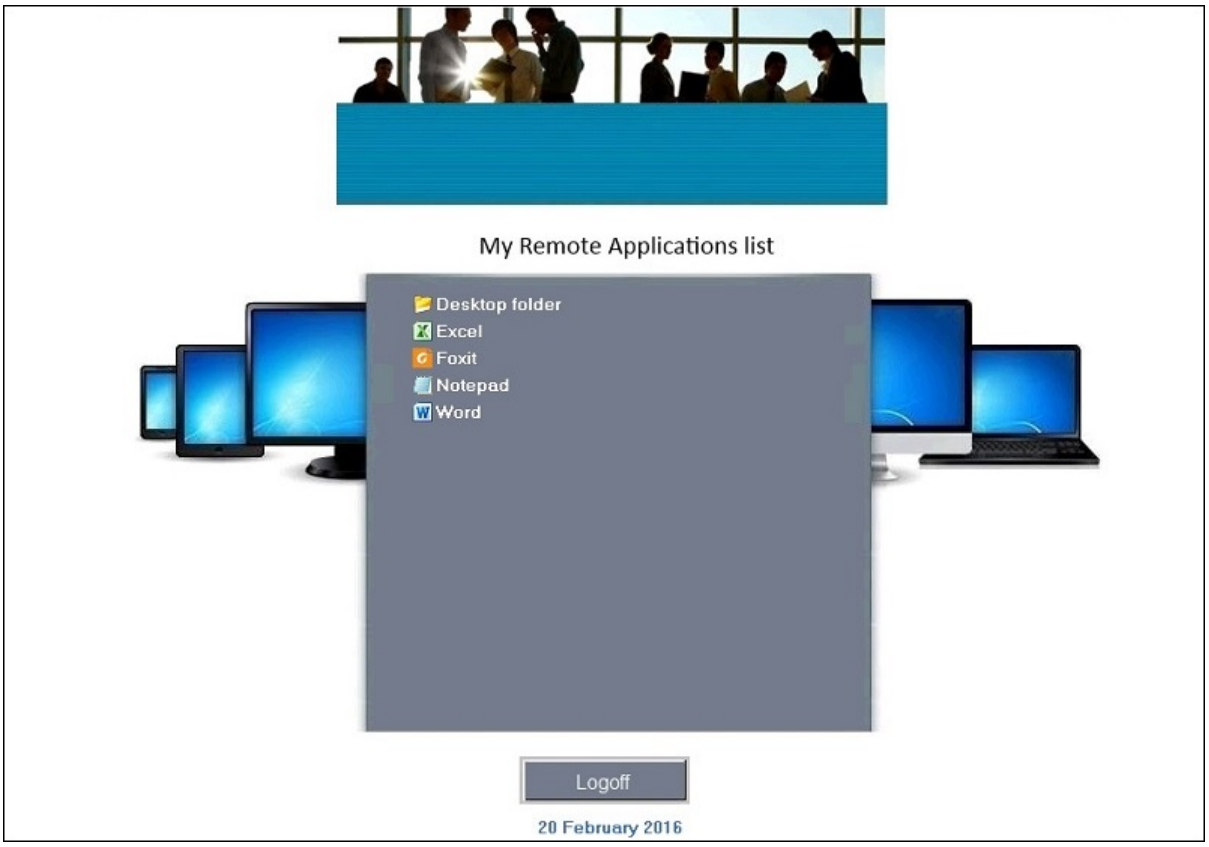
TSplus Thème de bureau un



TSplus Thème de bureau deux



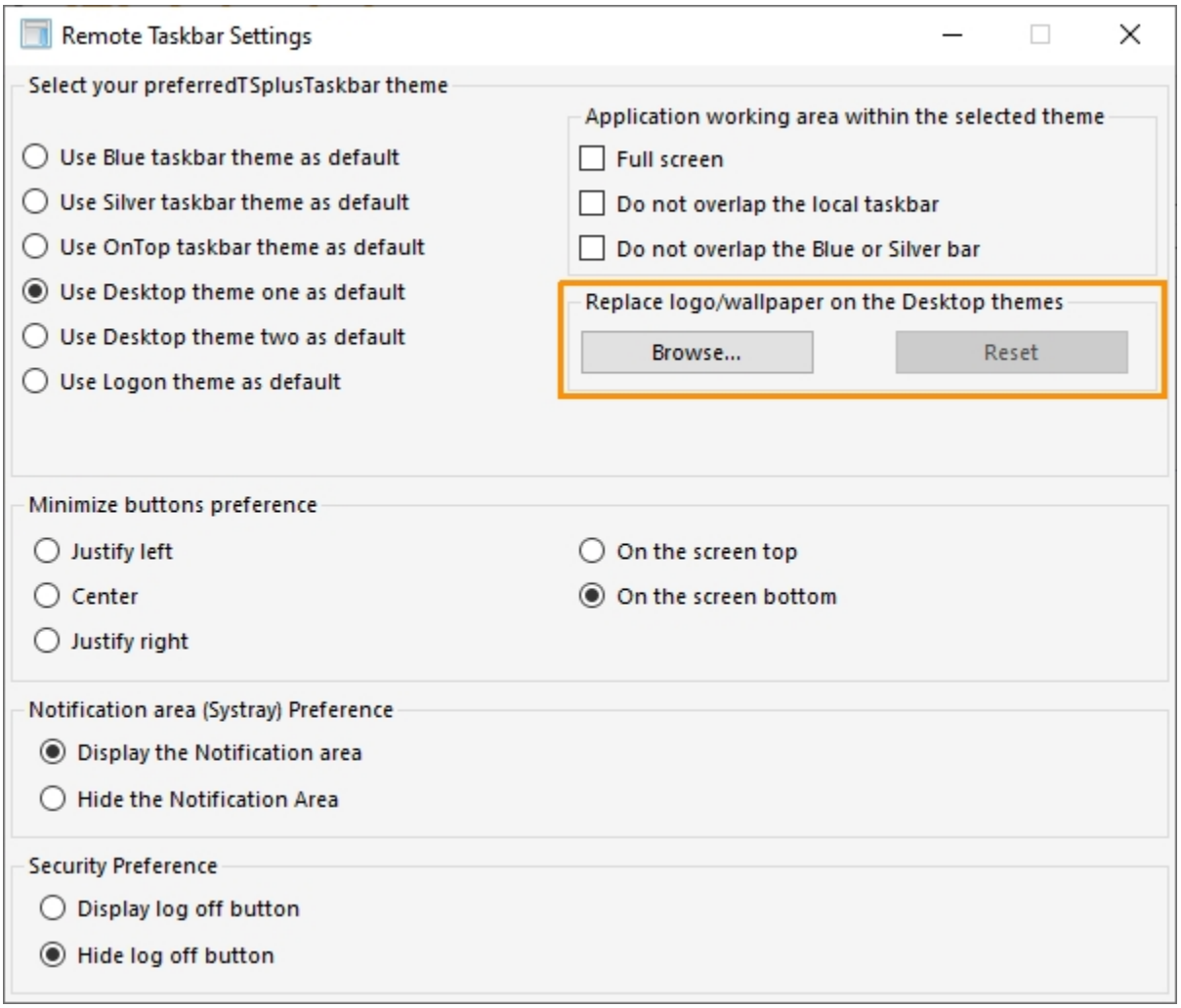
Thème de connexion TSplus



Thème personnalisé

Pour chaque thème, l'administrateur peut le personnaliser et, par exemple, afficher le logo de

l'entreprise. Il peut également ajouter son propre fond d'écran en sélectionnant l'un des thèmes de bureau et en cliquant sur le bouton Remplacer le logo/fond d'écran pour sélectionner votre fichier .jpg, par exemple.



- Vous pouvez ajouter votre propre fond d'écran de bureau en sélectionnant l'un des thèmes de bureau et en cliquant sur le bouton Remplacer le logo/fond d'écran pour sélectionner votre fichier .jpg, par exemple :


APPLICATIONS:
15 June 17

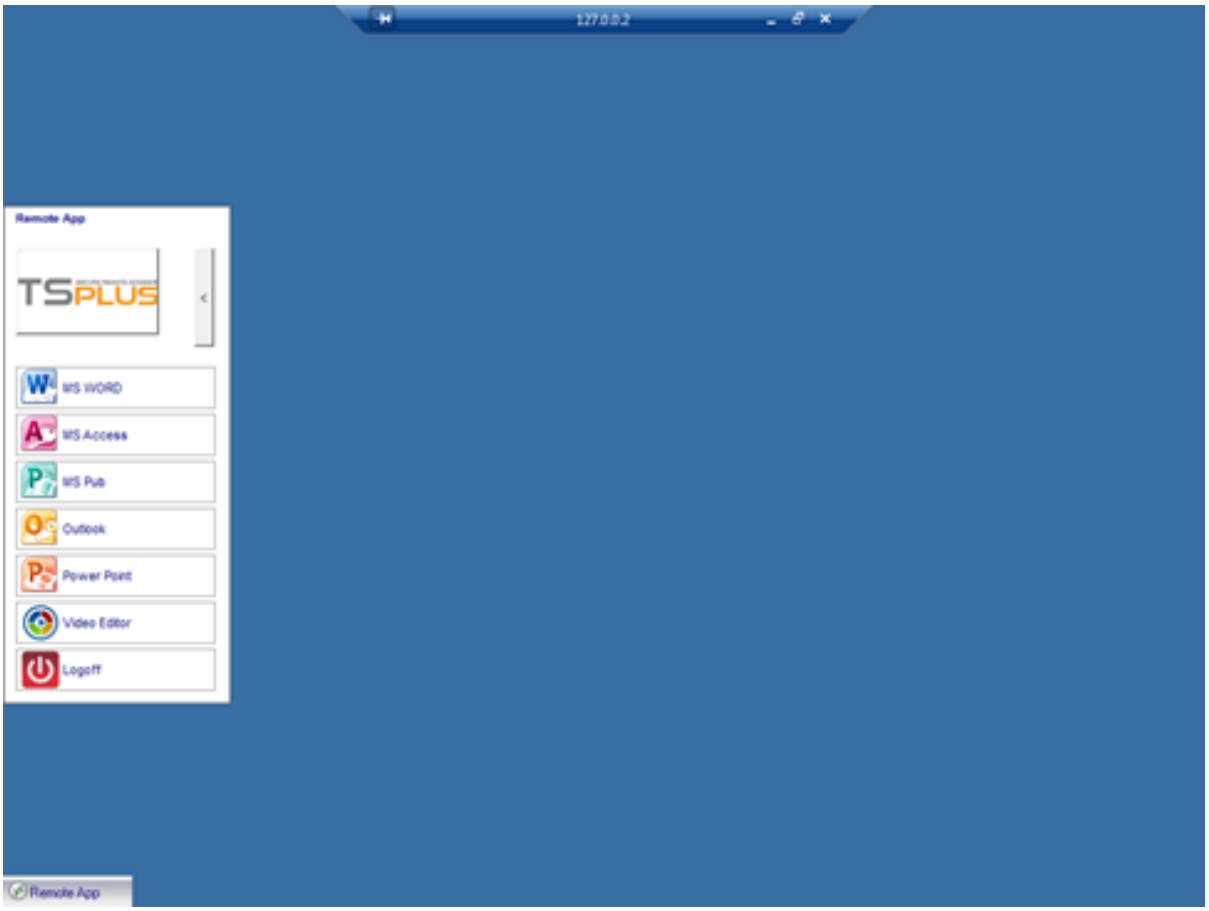
Fonctionnalité RemoteApp sur le client

Dans le passé, le client portable TSplus généré était la méthode habituelle pour un utilisateur de démarrer des applications. La version 10.50 introduit **une icône dans la zone de notification** qui donne à chaque utilisateur la liste de toutes ses applications distantes. Dans cette liste d'applications, l'utilisateur peut sélectionner celle qu'il souhaite démarrer.

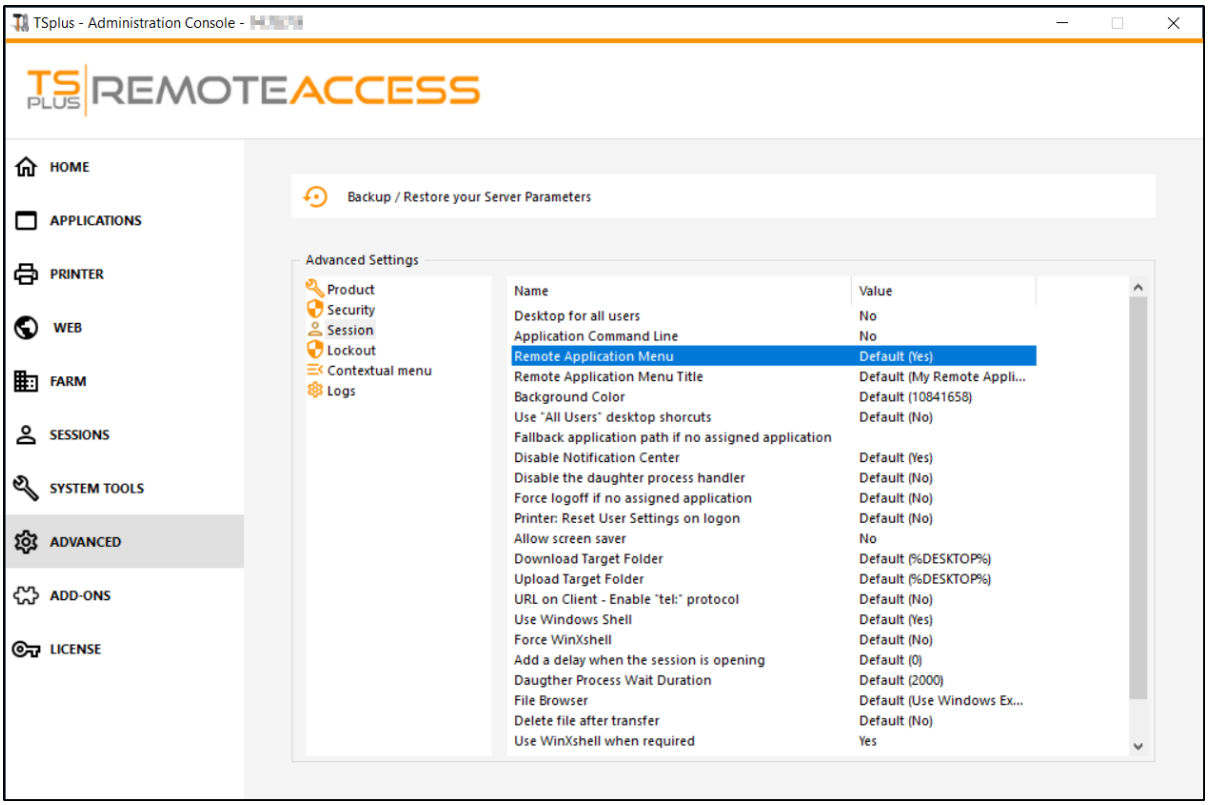
C'est une nouvelle façon pour les administrateurs de fournir des applications à distance (appelées "RemoteApps") à leurs utilisateurs. Plus précisément, RemoteApp On Client permet un processus de publication simple qui permet aux applications installées directement sur le serveur d'être fournies aux utilisateurs, permet aux programmes RemoteApp de s'exécuter côte à côte avec des programmes locaux, et offre une intégration avec une application "lanceur" personnalisée pour faciliter la recherche et le lancement des programmes RemoteApp par les utilisateurs.

La liste des applications utilisateur apparaîtra également dans le **Menu Démarrer** sous **Tous les programmes** dans un dossier appelé **Mes applications à distance** Pour déployer cette nouvelle capacité incroyable de TSplus, c'est simple : l'administrateur a généré de nouveaux clients de connexion et les a autorisés avec l'AdminTool. Ce guide expliquera étape par étape ce qui se passera lorsque l'administrateur activera cette nouvelle fonctionnalité et remettra à ses utilisateurs un nouveau client de connexion généré.

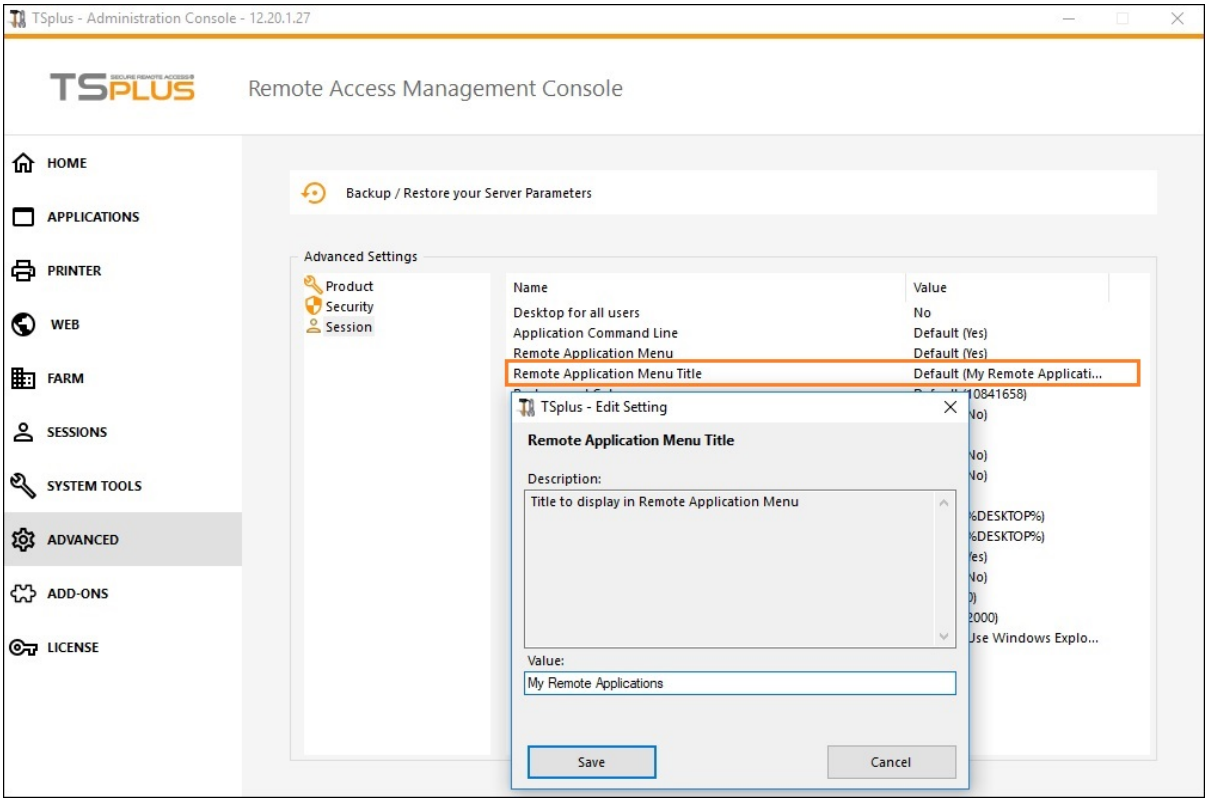
L'exemple : L'utilisateur "Laura" utilise TSplus pour accéder à son application distante. Pour ce faire, elle utilise un client généré nommé **LauraPortableClient.exe** Lorsqu'elle l'exécute sur son PC, elle obtient le résultat suivant :



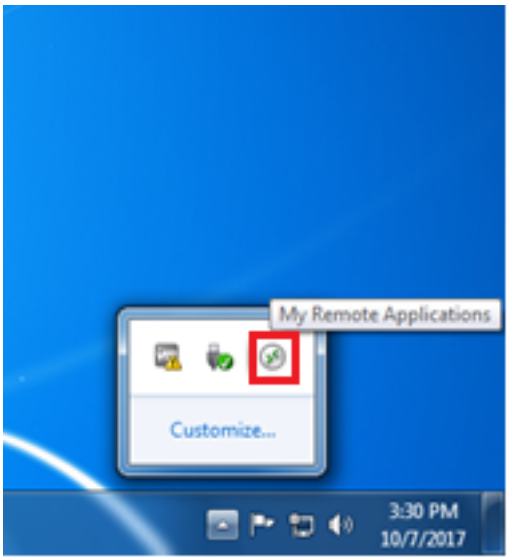
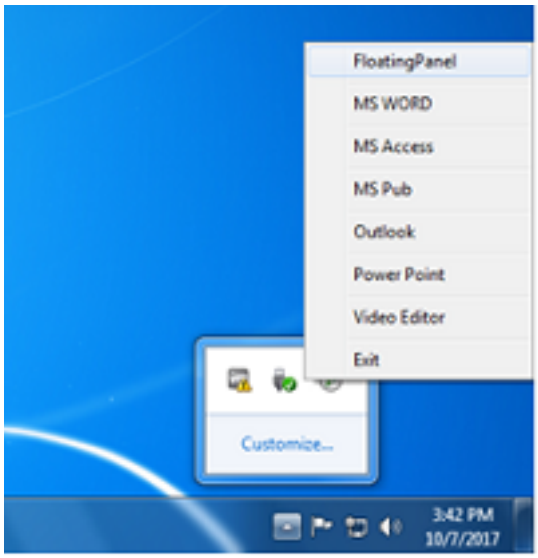
Cependant, l'administrateur lui a fourni un nouveau, créé avec la version TSplus 10.50. Elle devra l'exécuter au moins une fois pour bénéficier du nouveau. **Fonctionnalité RemoteApp sur le client** Lorsque l'administrateur ajoute ou supprime une application pour un utilisateur, ce changement sera appliqué côté serveur lors de la prochaine connexion. Cela signifie que la session actuelle ne reflétera pas cette modification. L'onglet Avancé de l'AdminTool a une option pour activer ou désactiver cette fonctionnalité RemoteApp On Client, par défaut, elle est activée.



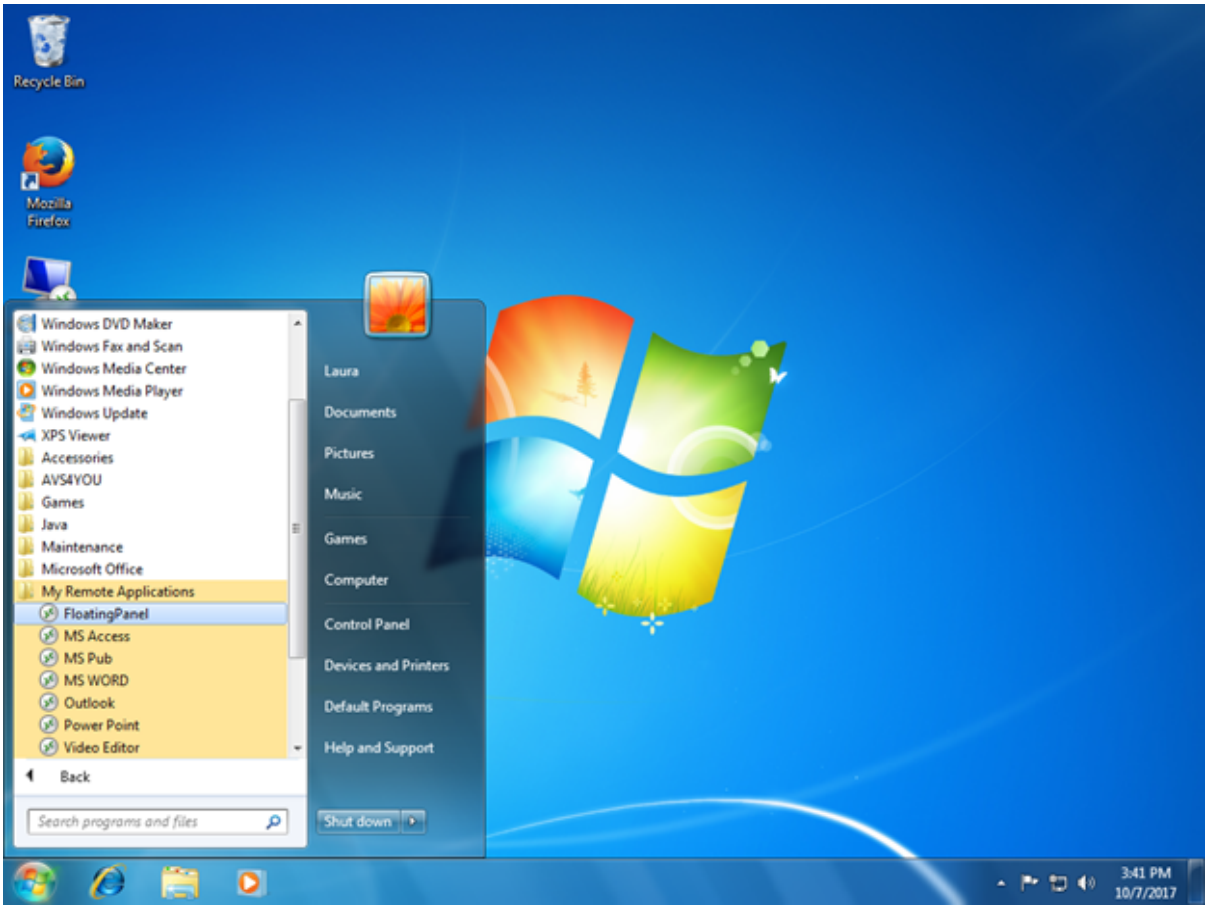
Vous pouvez changer le nom du menu comme vous le souhaitez, en cliquant sur le titre du menu d'application à distance ci-dessous, et en l'ajoutant dans la zone de valeur :



Que se passera-t-il sur son PC lorsqu'elle exécutera une fois son nouveau client généré : elle verra une nouvelle icône dans la zone de notification de sa barre des tâches locale.

Mon nouvel icône d'applications à distance	Menu de la liste des applications
	

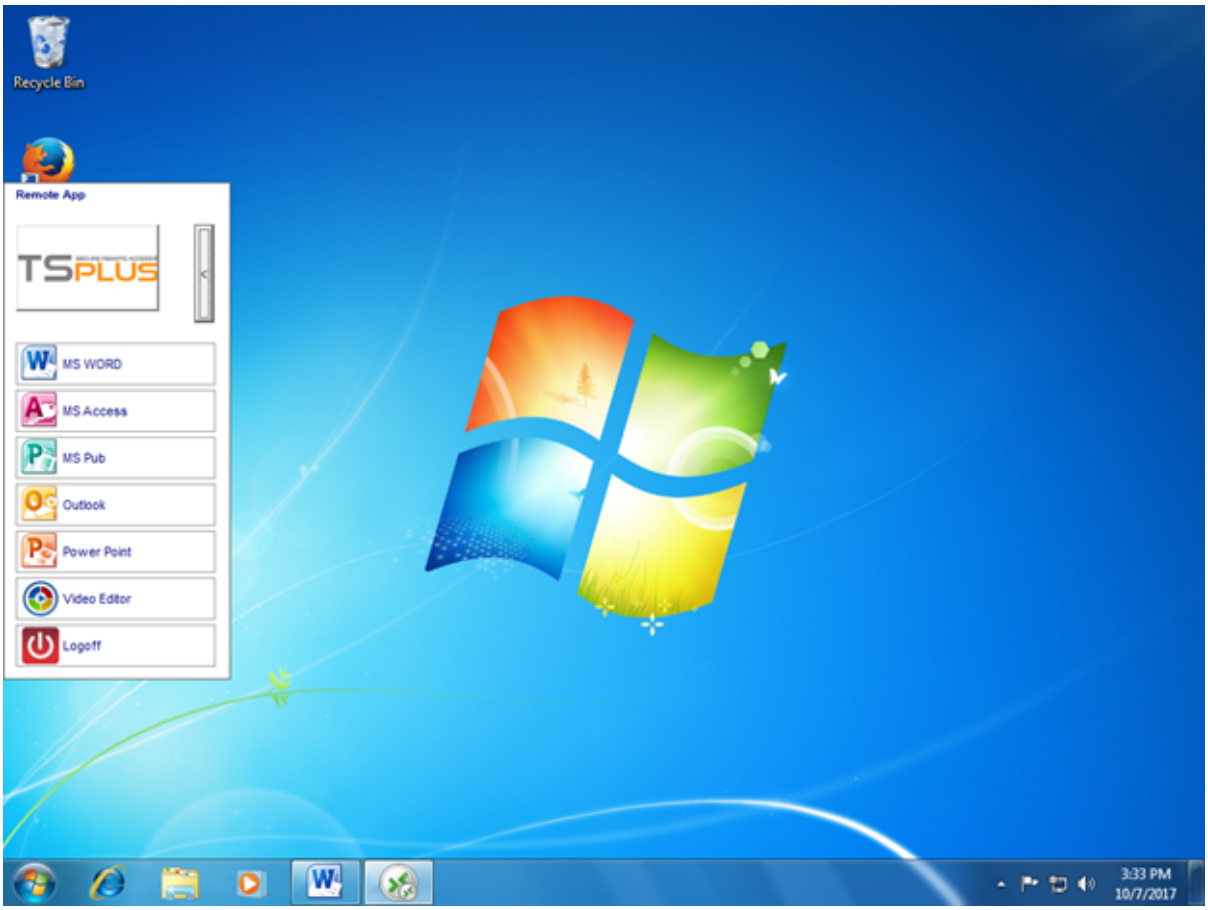
Elle verra également une nouvelle entrée dans la liste des programmes de son menu Démarrer nommée **Mes applications à distance** :



Elle pourra maintenant sélectionner l'une de ces applications listées et la démarrer en tant que

RemoteApp. Elle n'aura pas besoin d'utiliser le client généré LauraPortableClient.exe fourni.

Par exemple, si elle sélectionne le Panneau Flottant, elle obtiendra ce résultat :

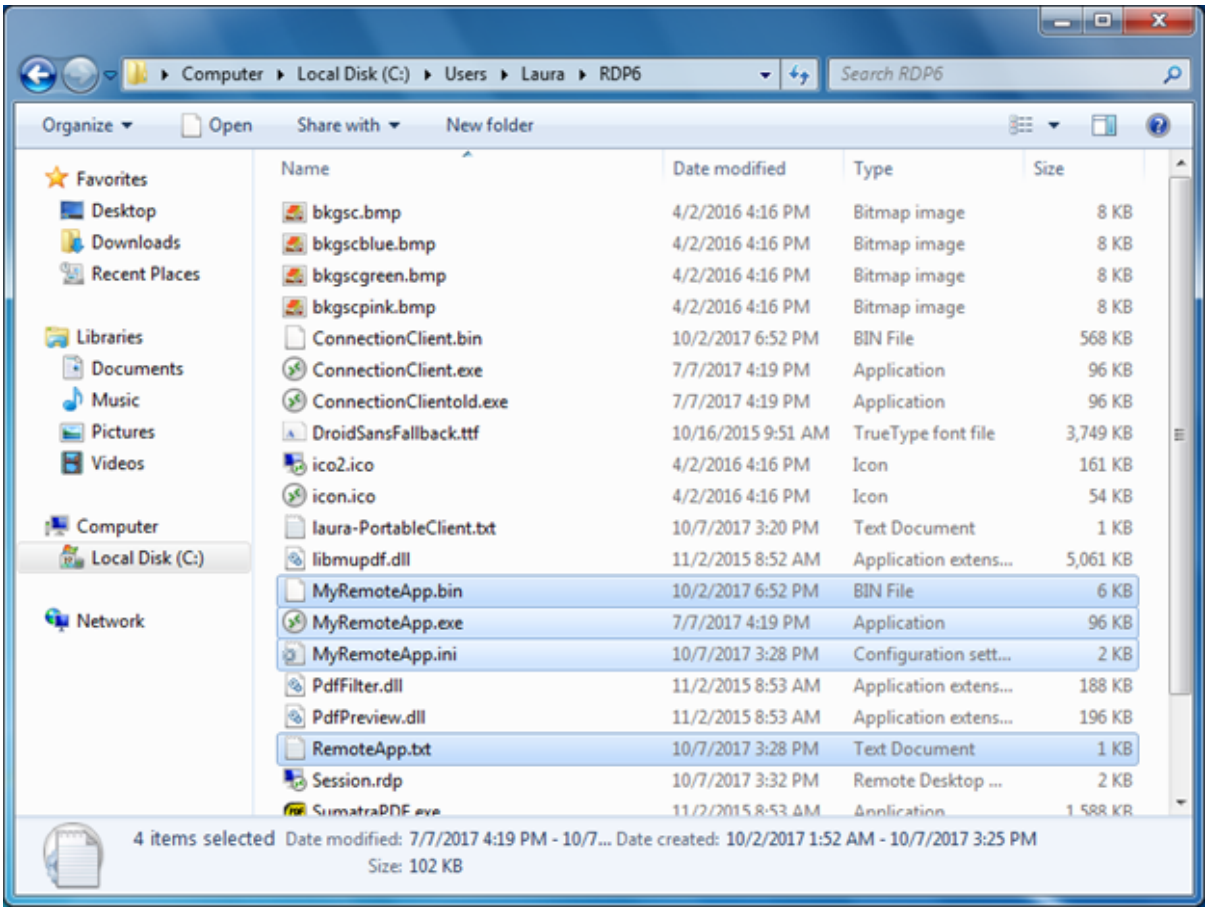


Contexte technique derrière cette nouvelle technologie.

Le nouveau client généré de la version 10.50 ajoute plusieurs fichiers dans le dossier C:\Users%UserName%\RDP6 du profil utilisateur du PC local.

MyRemoteApp.exe et MyRemoteApp.bin sont les codes de programme qui sont lancés pour créer la nouvelle icône dans la zone de notification et la nouvelle entrée dans la liste Tous les programmes du bouton Démarrer.

MyRemoteApp.ini est un fichier reçu du serveur. Il fournit les détails de chaque application qui sont assignées à cet utilisateur du côté serveur. Il est mis à jour à chaque nouvelle connexion au serveur. En général, cela prend 30 secondes après chaque connexion pour recevoir ce fichier du serveur. RemoteApp.txt fournit le nom du dernier client généré démarré sur ce PC.



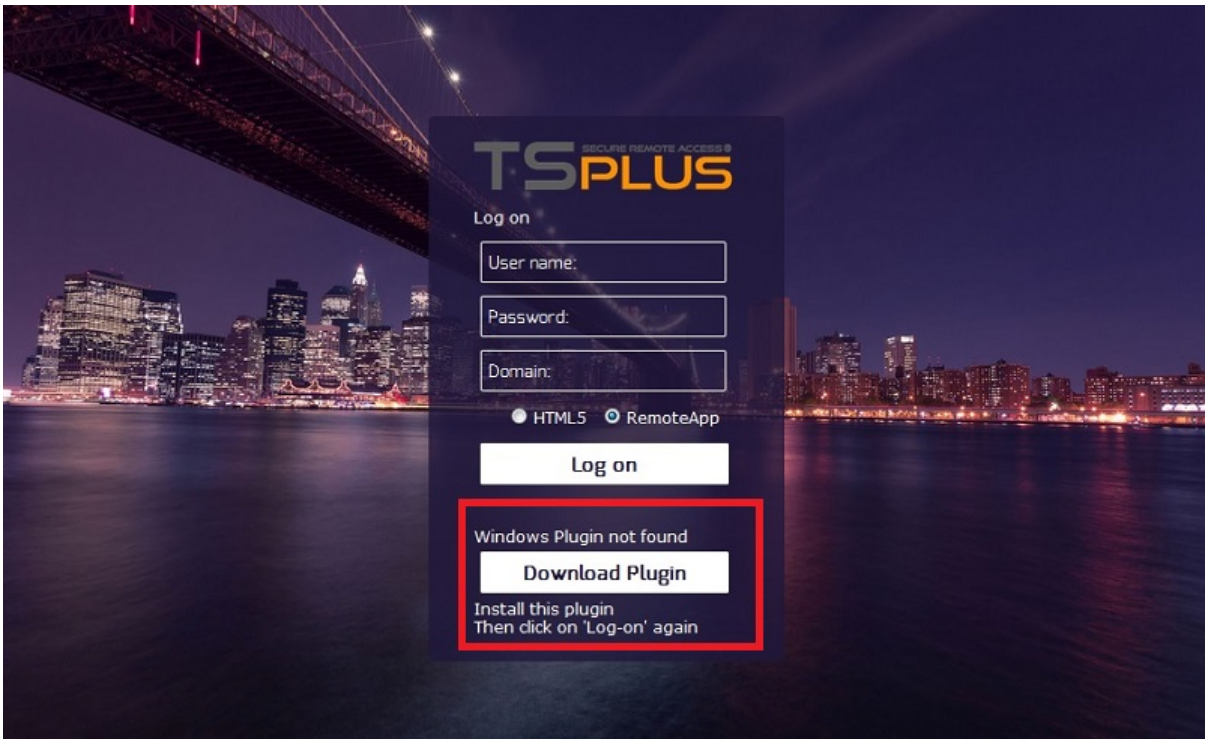
Commentaires :

Si l'utilisateur a des droits d'administrateur sur son propre PC, **MyRemoteApp.exe** sera démarré automatiquement à chaque redémarrage et le bouton Démarrer sera également mis à jour. Sinon, l'administrateur doit exécuter une fois le nouveau client généré "En tant qu'administrateur" pour activer la nouvelle fonctionnalité. Ce faisant, il créera les entrées de registre appropriées dans HKLM. Si un utilisateur se connecte à un seul serveur, ce nouveau système est parfait. Cependant, s'il utilise plusieurs clients de connexion pour ouvrir des sessions sur différents serveurs, vous devez garder à l'esprit que le fichier **MyRemoteApp.ini** sera mis à jour avec les valeurs de la dernière connexion. Cela peut être déroutant pour l'utilisateur et dans ce cas de déploiement, nous recommandons de ne pas utiliser cette nouvelle fonctionnalité.

Plugin Remote App

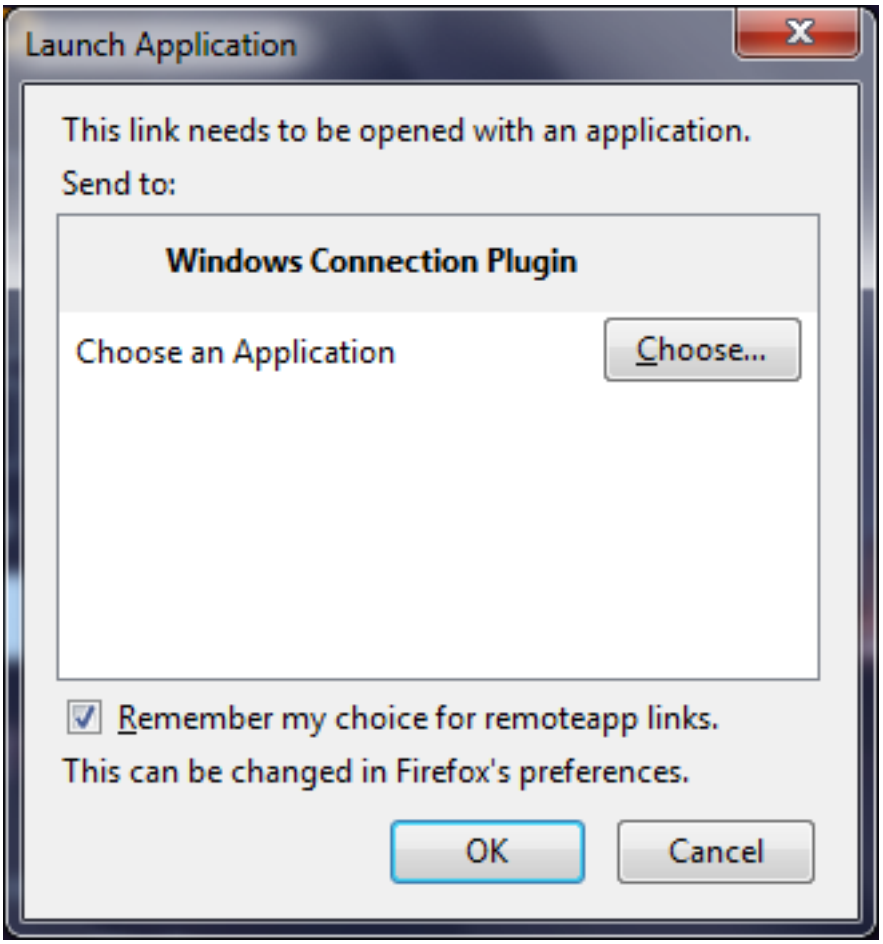
Depuis la nouvelle version 8.40 de TSplus, il n'est plus nécessaire d'installer un plugin Java sur le navigateur client.

Vous pouvez maintenant accéder au client Windows RemoteApp en téléchargeant et en installant un petit plugin Windows via le portail Web. Cette opération est rapide et nécessaire uniquement une fois par client.



Vous pouvez également l'installer dans le dossier C:\Program Files (x86)\TSplus\Clients\www\RemoteAppClient.

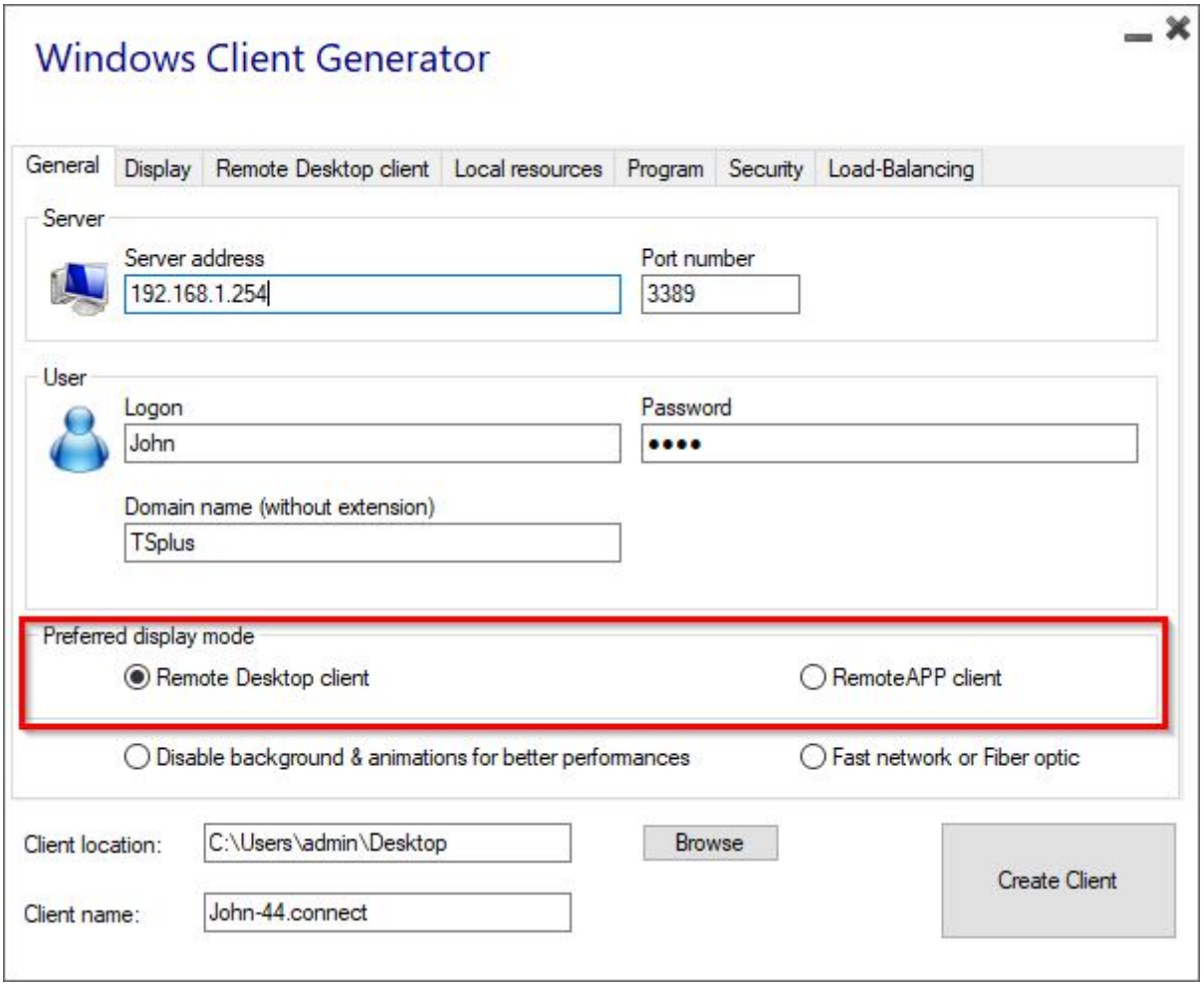
Lorsque vous utilisez Firefox, ce message s'affichera lors de votre première connexion. Si vous choisissez l'option « mémoriser mes choix », la notification sera désactivée lors des connexions futures.



Remarque Depuis TSplus 12.40, la configuration du client RemoteApp et le Le programme de configuration du client ont été fusionnés et peuvent être déployés avec une seule configuration - donc si vous téléchargez le programme d'installation du client RemoteApp, il ne sera pas nécessaire de télécharger celui du client de connexion.

Client de connexion RemoteApp

Vous pouvez choisir entre 2 modes d'affichage dans l'onglet général du générateur de client :



###Client de connexion RemoteApp

Le client de connexion RemoteApp ne dépend pas des paramètres de couleur de transparence.

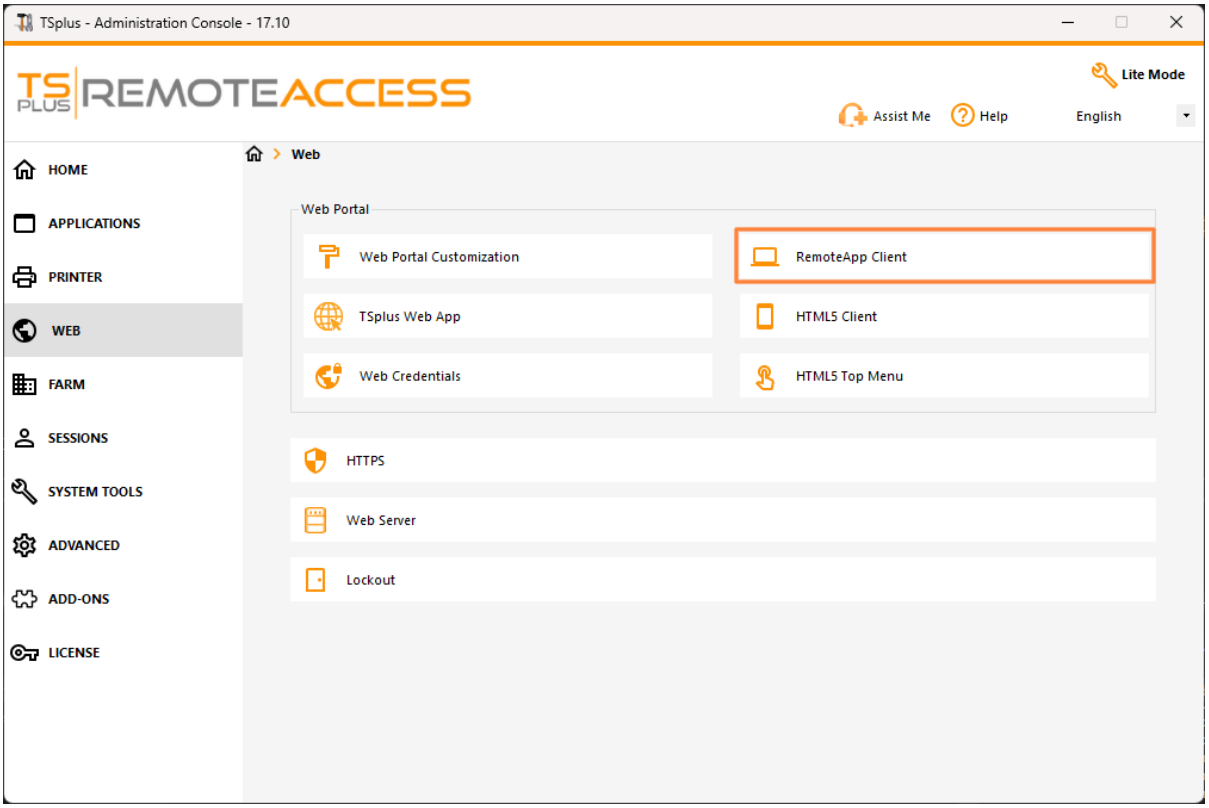
Cela permet un affichage parfait des applications ainsi qu'un comportement natif de Windows.

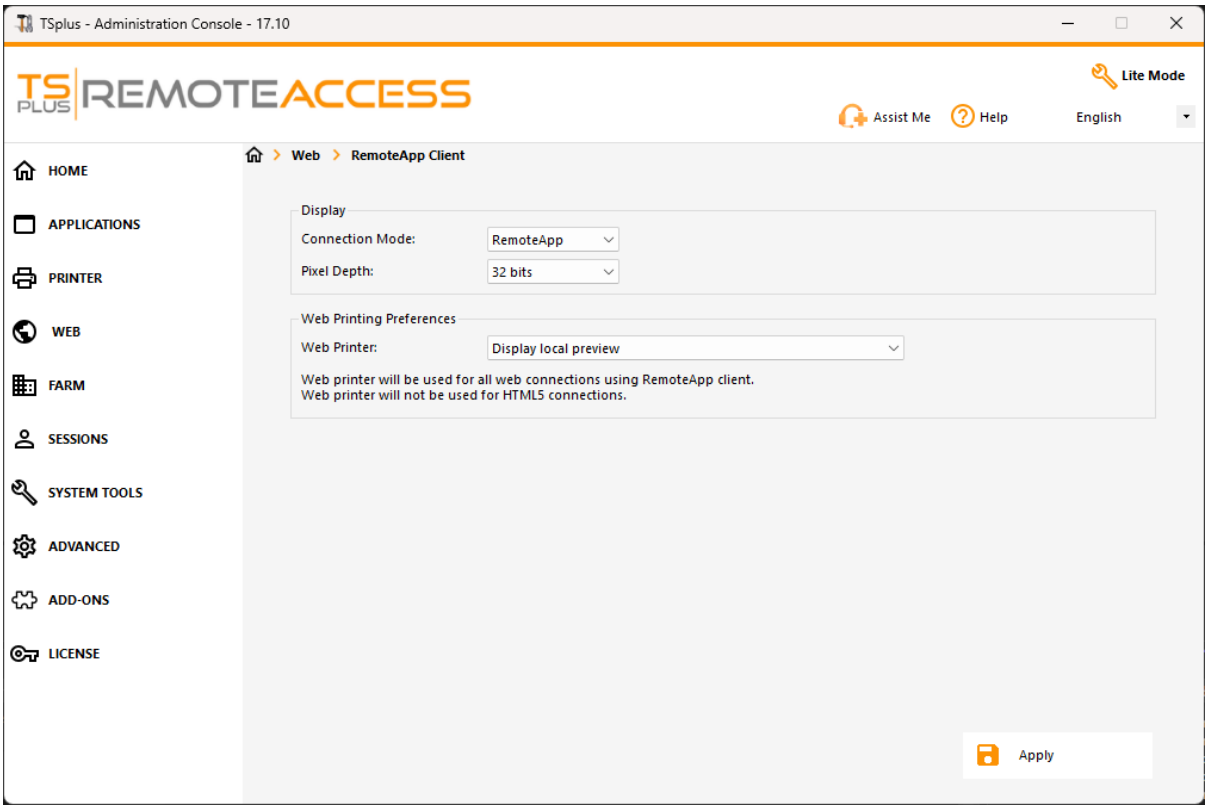
- Sur le client, l'installation de RDP6 ou d'une version supérieure est requise.

- Sur le serveur, TSplus doit être installé sur une machine exécutant Windows 7 à Windows Server 2019.

Remarque RemoteApp n'est pas pris en charge sur Windows 10 1803 et 1809 Home Windows 2019 Essentials Editions.

Vous pouvez modifier les préférences d'affichage et d'impression du client RemoteApp dans l'onglet Web de l'Admintool :





Les applications minimisées peuvent être trouvées directement dans la barre des tâches de Windows, comme une application locale.

Dans cet exemple, Firefox et Paint sont lancés localement ; Notepad, Word et Foxit sont lancés à distance.



Pour le client de connexion Remoteapp, vous pouvez choisir de publier une application unique à lancer sans interruption lors de la connexion de l'utilisateur. Vous pouvez également publier des applications avec le TSplus Remote Taskbar , le Panneau Flottant ou le Panneau d'Application .

Exécuter le client Windows dans un environnement Proxy

En général, le package SSH prend en charge les proxies HTTP(S) et cela devrait suffire à surmonter la plupart des proxies connus.

Cependant, il existe des cas très difficiles où l'environnement proxy ne peut pas être correctement reconnu, est caché des logiciels tiers ou les serveurs cibles se trouvent derrière des proxies inverses.

Pour de tels cas difficiles, le logiciel contient une solution Non-SSH appelée « mode de secours ».

Si vous pouvez établir une connexion HTML5, alors vous pouvez être sûr que ce logiciel vous aidera à établir des connexions de socket natives via Websocket (FF, Chrome, Opera, IE10, etc.) ou XHR (IE6-IE9).

Faites attention, certains proxies autorisent Websocket/XHR trafic uniquement via la couche HTTPS, donc utilisez l'adresse https au lieu de http.

Si le proxy ne demande pas d'authentification et que vous pouvez accéder aux pages via le navigateur :

1. Ouvrez http(s)://yourserver.com__/software/html5/jwres/__
2. Attendez la connexion réussie (et autorisez l'exécution de Java si demandé)
3. Cliquez sur le texte rouge « ouvrir le lien » pour accéder à la page d'accès web en cours.
4. Utilisez l'accès client Windows comme d'habitude

Si le proxy demande une authentification et que vous pouvez accéder aux pages via le navigateur :

1. Ouvrez http(s)://yourserver.com__/software/html5/jwres/__
2. Si le proxy demande une authentification pour les applets Java, appuyez sur "annuler".
3. Cliquez sur « Télécharger LocalWebserver », puis exécutez-le après le téléchargement réussi, cela démarrera le serveur http local sur le port 18888.
4. Cliquez sur « Forcer le chargement de l'applet depuis http://localhost:18888 ", cela rechargera la page avec le chargement des jars depuis le serveur http local
5. Attendre la connexion réussie

6. Cliquez sur le texte rouge « ouvrir le lien » pour accéder à la page d'accès web en cours.
7. Utilisez l'accès client Windows comme d'habitude

Sécuriser un serveur TSplus

Aperçu

Sécuriser n'importe quel serveur est une histoire sans fin où chaque expert pourrait ajouter un autre chapitre.

TSplus bénéficie de et est compatible avec l'infrastructure de sécurité existante dans une entreprise (Active Directory, GPO, serveurs HTTPS, systèmes de télécommunication SSL ou SSL, VPN, contrôle d'accès avec ou sans cartes d'identité, etc).

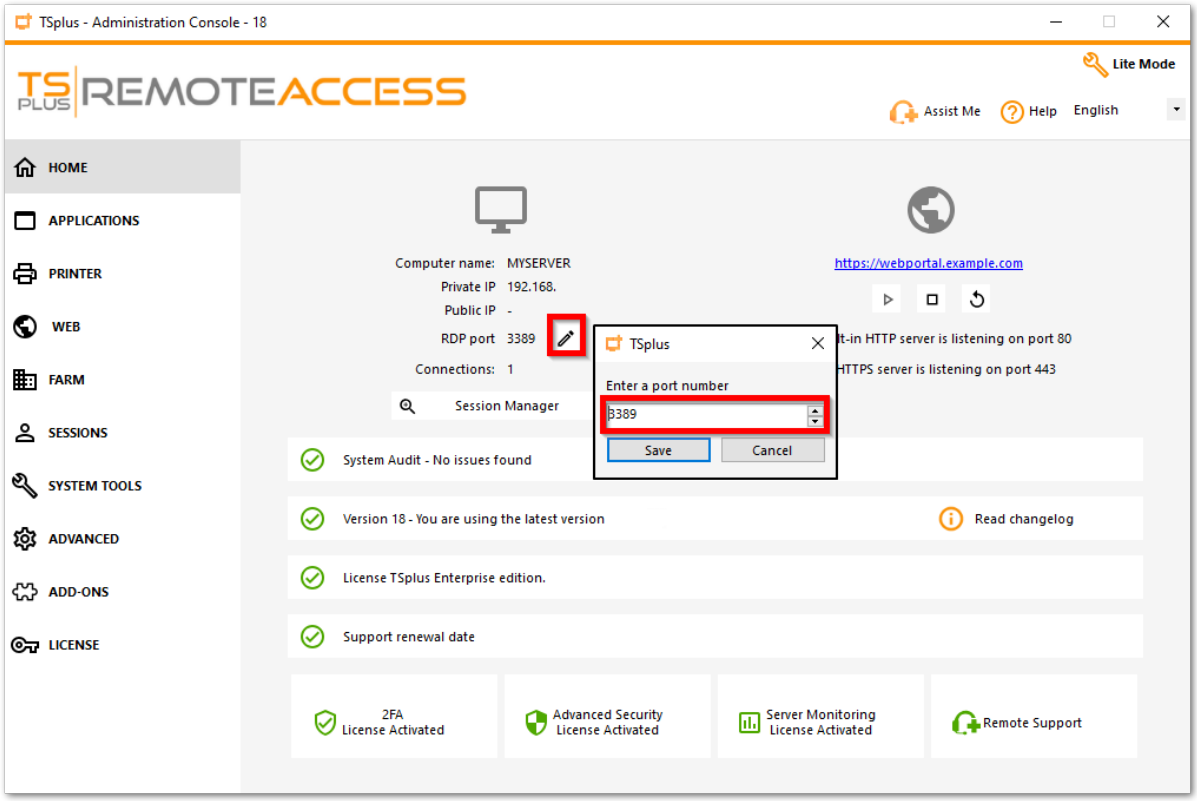
Pour les clients qui souhaitent sécuriser facilement leurs serveurs, TSplus propose un ensemble de méthodes simples et efficaces pour garantir de bons niveaux de sécurité.

Avec l'AdminTool, vous pouvez sélectionner un numéro de port TCP/IP différent pour que le service RDP accepte les connexions. Le numéro par défaut est 3389.

Vous pouvez choisir n'importe quel port arbitraire, à condition qu'il ne soit pas déjà utilisé sur votre réseau et que vous définissiez le même numéro de port sur vos pare-feu et sur chaque programme d'accès utilisateur TSplus.

TSplus inclut une capacité unique de redirection de port et de tunneling : quel que soit le port RDP qui a été défini, le RDP sera également disponible sur le numéro de port HTTP et HTTPS !

Si les utilisateurs souhaitent accéder à votre serveur TSplus en dehors de votre réseau, vous devez vous assurer que toutes les connexions entrantes sur le port choisi sont redirigées vers le serveur TSplus. Dans l'onglet Accueil, cliquez sur le bouton crayon à côté de "Port RDP" :



Changez le port RDP et enregistrez.

Options de sécurité côté serveur

L'AdminTool vous permet de refuser l'accès à tout utilisateur qui n'utilise pas un programme de connexion TSplus généré par l'administrateur. Dans ce cas, tout utilisateur qui tenterait d'ouvrir une session avec un client de Bureau à distance autre que celui de TSplus (en supposant qu'il ait la bonne adresse du serveur, le numéro de port, un identifiant valide et un mot de passe valide) sera déconnecté automatiquement.

L'administrateur peut décider que seuls les membres du groupe Utilisateur de Bureau à Distance. sera autorisé à ouvrir une session.

L'administrateur peut décider qu'un mot de passe est obligatoire pour ouvrir une session.

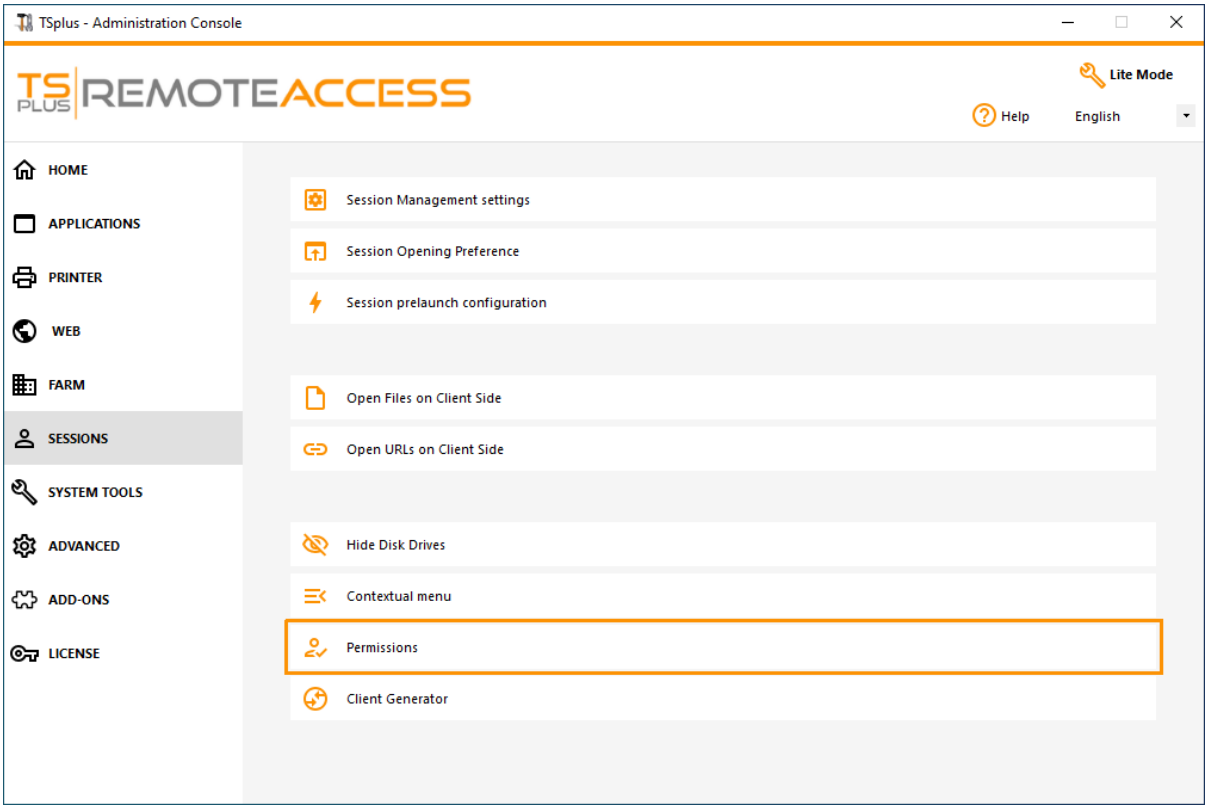
En configurant la stratégie de groupe locale applicable, l'administrateur peut spécifier s'il faut appliquer un niveau de cryptage pour toutes les données envoyées entre le client et l'ordinateur distant pendant une session de services de terminal.

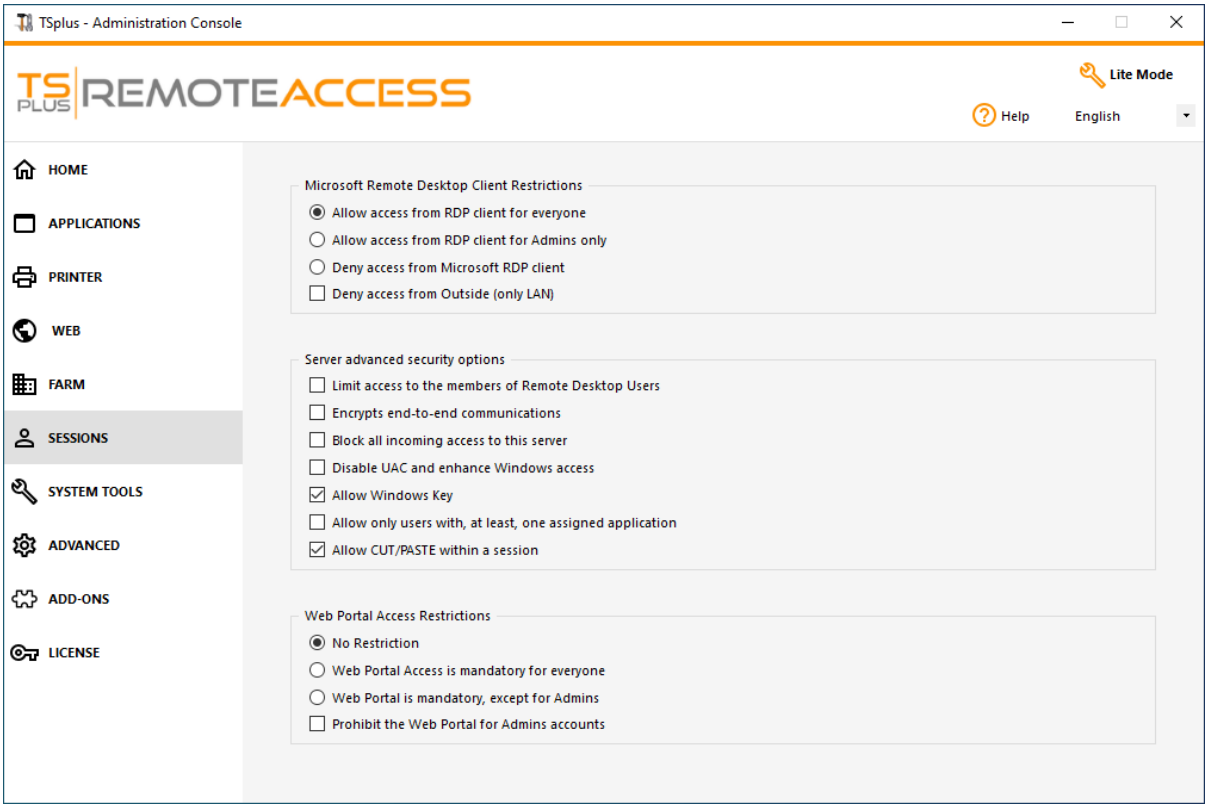
Si le statut est défini sur Activé, le chiffrement pour toutes les connexions au serveur est défini au niveau décidé par l'administrateur. Par défaut, le chiffrement est défini sur Élevé.

L'administrateur peut également définir comme règle que seuls les utilisateurs disposant d'un client de connexion TSplus pourront ouvrir une session.

Tout accès entrant avec un RDP standard ou un accès web sera automatiquement rejeté.

Vous pouvez trouver plusieurs options de sécurité avancées si vous cliquez sur l'onglet Sessions - Autorisations :



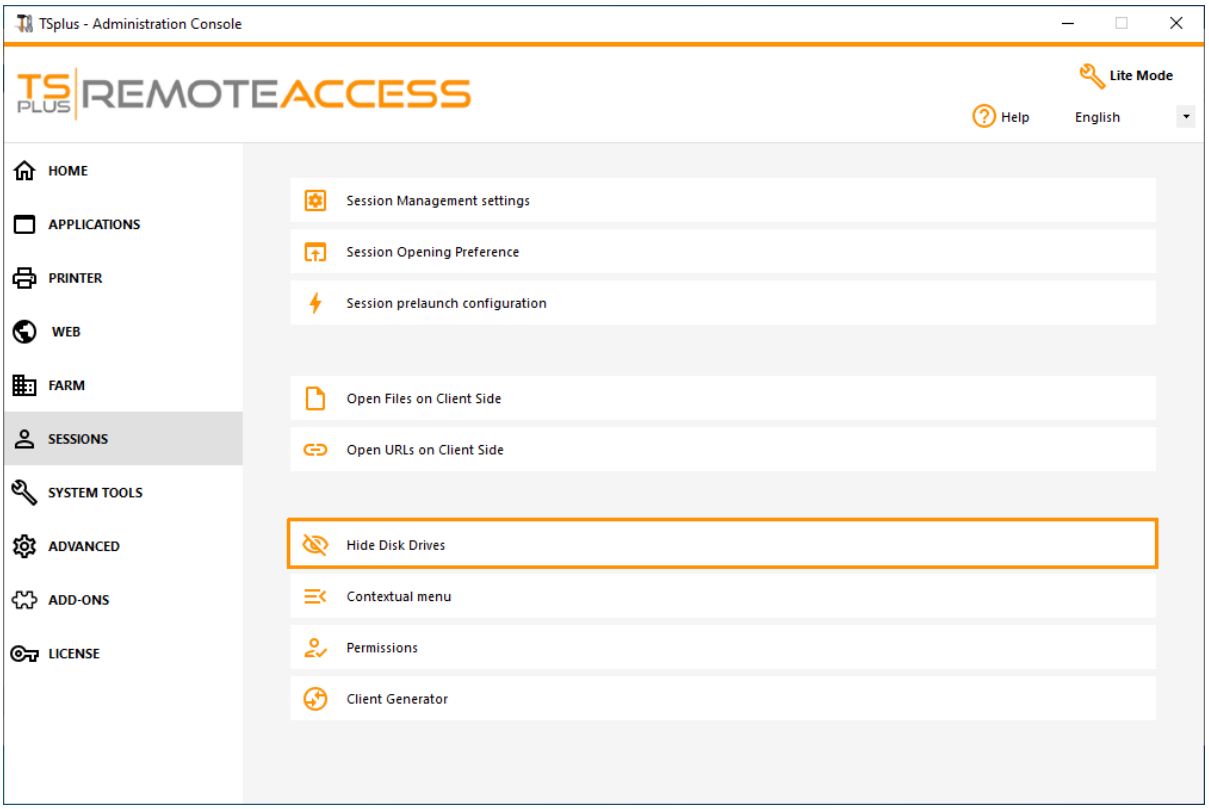


- **Autoriser l'accès depuis le client RDP de Microsoft pour tout le monde :** Permet à chaque utilisateur de se connecter en utilisant mstsc.exe.
- **Autoriser l'accès uniquement aux administrateurs depuis le client RDP de Microsoft :** Permet uniquement aux administrateurs de se connecter en utilisant mstsc.exe.
- **Refuser l'accès depuis le client RDP de Microsoft :** Empêcher quiconque de pouvoir se connecter en utilisant mstsc.exe.
- **Refuser l'accès depuis l'extérieur :** Cela signifie que seules les adresses IP privées du LAN pourront ouvrir une session.
- **Limiter l'accès aux membres des utilisateurs de Remote Desktop :** Cette limite s'applique uniquement à ce groupe local d'utilisateurs (que vous pouvez voir en cliquant sur le Utilisateurs et groupes .
- **Crypte les communications de bout en bout :** Crypte les communications client/serveur à l'aide d'un chiffrement de 128 bits. Utilisez ce niveau lorsque les clients accédant au serveur terminal prennent également en charge le chiffrement de 128 bits.
- **Bloquer tout accès entrant à ce serveur :** Toutes les sessions actives resteront actives, tandis que toutes les tentatives de connexions entrantes seront bloquées. Assurez-vous que vous pouvez accéder physiquement à la console du serveur si vous cochez cette case. N'utilisez pas cette option si votre serveur est hébergé dans un environnement Cloud.
- **Désactiver UAC et améliorer l'accès Windows :** Désactive les contrôles de compte utilisateur, supprime toutes les fenêtres contextuelles de sécurité indésirables de Windows. limitation des utilisateurs (messages) lors du lancement des applications.
- **La case "Autoriser la touche Windows"** autoriser l'utilisation des touches Windows et des combinaisons à l'intérieur d'une session TSplus.
- **Autoriser uniquement les utilisateurs ayant au moins une application assignée :** L'utilisateur avec une application et plus est autorisé à ouvrir une session.
- **Autoriser le COUPER/COLLER dans une session :** Décocher cette case désactivera les commandes CTRL C/CTRL V.

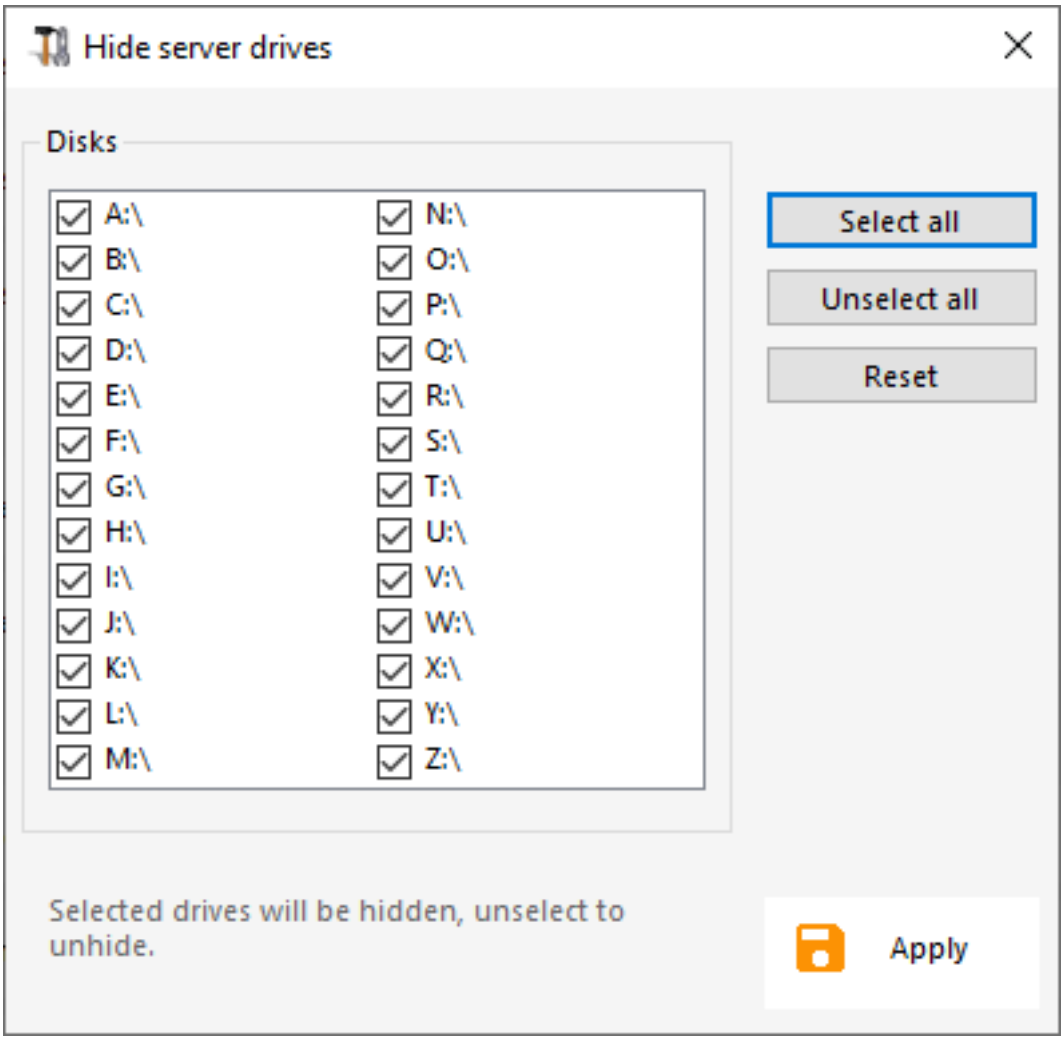
Restrictions d'accès au portail Web

- Aucune restriction
- Le portail Web est obligatoire pour tout le monde : les utilisateurs ne peuvent se connecter que via le portail Web.
- Le portail Web est obligatoire, sauf pour les administrateurs : les utilisateurs ne peuvent se connecter que via le portail Web, sauf les administrateurs.
- Interdire le portail Web pour les comptes d'administrateurs : les administrateurs ne peuvent pas se connecter via le portail Web.

L'AdminTool comprend un outil qui permet de masquer les disques durs du serveur pour empêcher les utilisateurs d'accéder aux dossiers via Mon ordinateur ou les boîtes de dialogue standard de Windows. Dans l'onglet Sessions, cliquez sur "Masquer les disques".



Cet outil fonctionne à l'échelle mondiale. Cela signifie que même l'administrateur n'aura pas un accès normal aux lecteurs après l'application des paramètres. Dans l'exemple ci-dessous, tous les pilotes ont été sélectionnés avec le bouton "tout sélectionner", qui cochera toutes les cases correspondant aux lecteurs qui seront cachés à tout le monde.



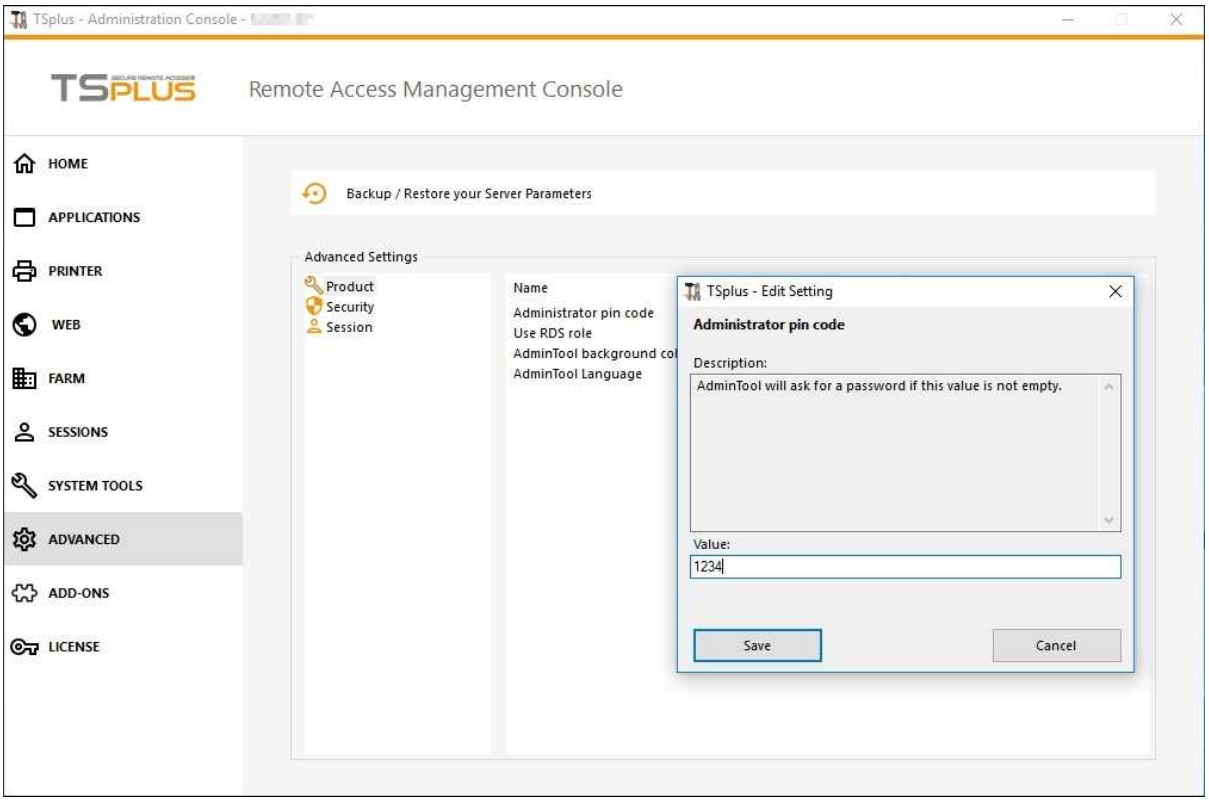
Remarques : Cette fonctionnalité est puissante et ne désactive pas l'accès aux disques. Elle empêche simplement l'utilisateur de les afficher.

L'outil marque les disques durs comme cachés, mais il ajoute également la propriété CACHÉE à l'ensemble des dossiers racines et à la liste des utilisateurs dans Documents et Paramètres.

Si l'administrateur souhaite voir ces fichiers, il doit :

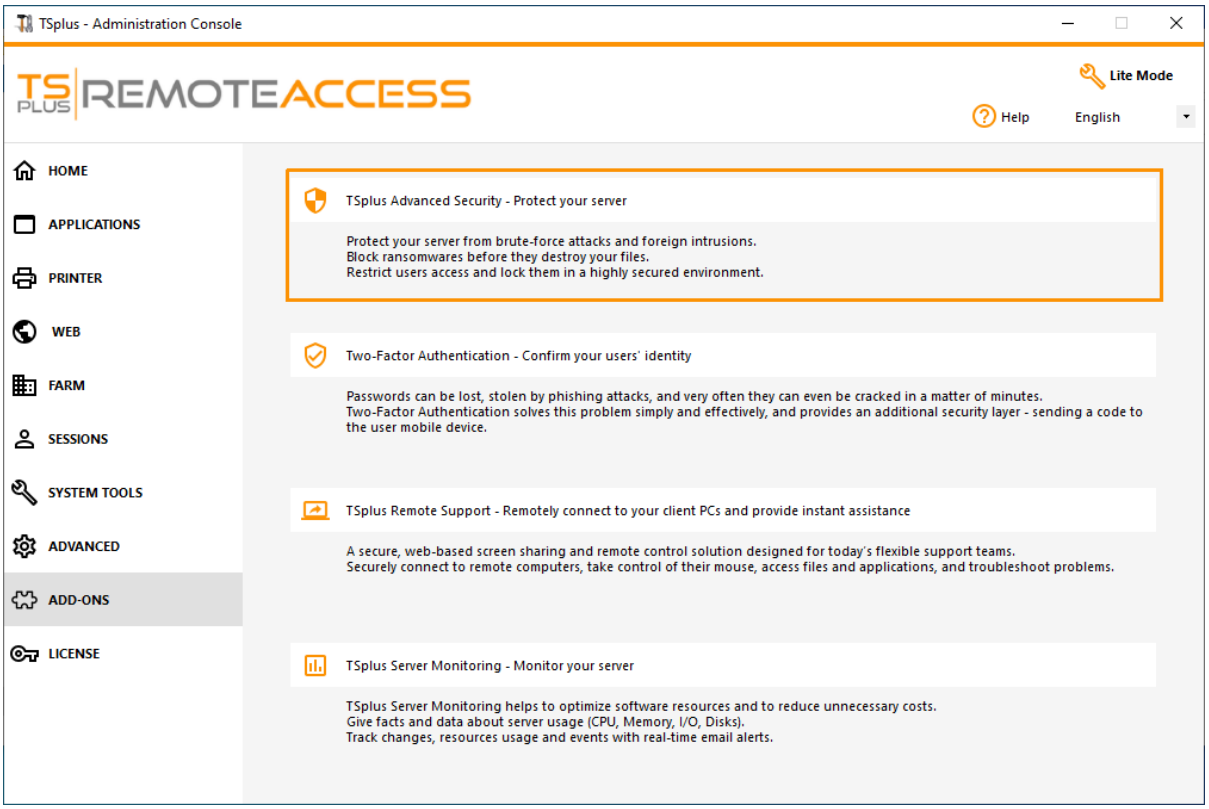
1. Tapez la lettre du lecteur de disque. Par exemple : **D:** qui vous mènera au lecteur D:.
2. Allumer **AFFICHER LES FICHIERS ET DOSSIERS CACHÉS** dans les propriétés de vue de dossier.

L'administrateur peut sécuriser l'accès à l'outil d'administration en définissant un code PIN qui sera demandé à chaque démarrage, dans l'onglet Avancé de l'AdminTool, sous les paramètres du produit :

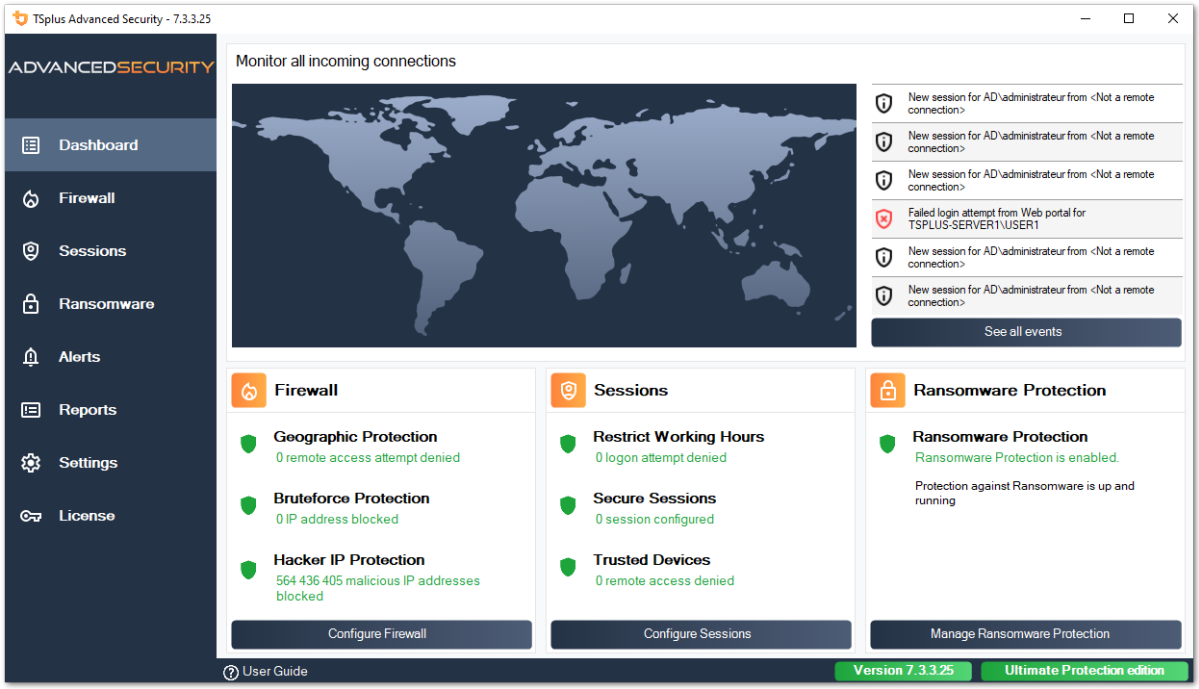


TSplus Advanced Security Ultimate

Depuis la version 11.40 de TSplus, vous trouverez un outil de sécurité unique en son genre, que vous pouvez lancer dans l'onglet Add-Ons :



Ce qui apporte des fonctionnalités puissantes, documentées sur cette page .



Le rôle de la protection contre les attaques par force brute sur le portail Web est décrit sur cette page .

Authentification à deux facteurs

Depuis la version 12 de TSplus, vous pouvez activer l'authentification à deux facteurs en tant qu'add-on pour votre portail Web TSplus.



Plus d'informations sur cette nouvelle fonctionnalité incroyable peuvent être trouvées sur cette page .

Certificats SSL

Le processus des certificats SSL est détaillé sur ces pages :

- TSplus fournit un outil facile à utiliser pour générer un certificat SSL gratuit et valide : Certificat SSL gratuit et facile à installer
-

HTTPS et certificats SSL de tiers .

- Choisissez votre Suites de chiffrement pour améliorer la sécurité .

Options de sécurité du programme d'accès TSplus :

Le générateur de client TSplus offre la possibilité, dans son onglet Sécurité, de verrouiller le client TSplus à :

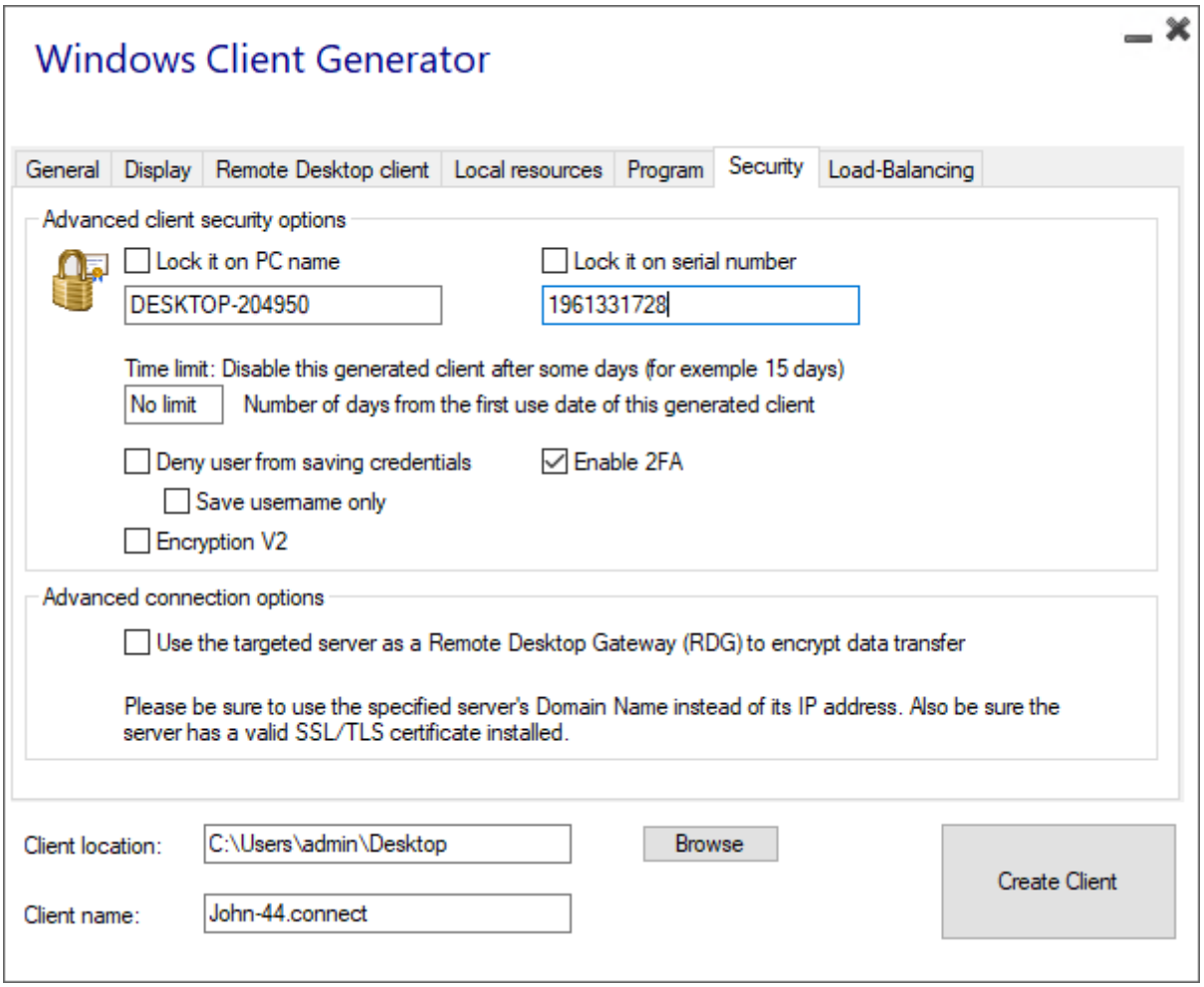
- Un nom de PC spécifique. Cela signifie que ce programme ne pourra pas démarrer depuis un autre PC.

- Un numéro de série de disque physique (disque dur PC ou clé USB). C'est un moyen très simple et puissant de définir un niveau de sécurité élevé.

  Le seul moyen de se connecter est avec un client spécifique, et ce client spécifique ne peut démarrer que sur une clé USB ou un disque dur PC spécifique.

  Certains de nos clients fournissent des clés USB à lecture d'empreintes digitales à chacun de leurs utilisateurs et chaque programme généré est verrouillé sur le numéro de série de l'appareil.

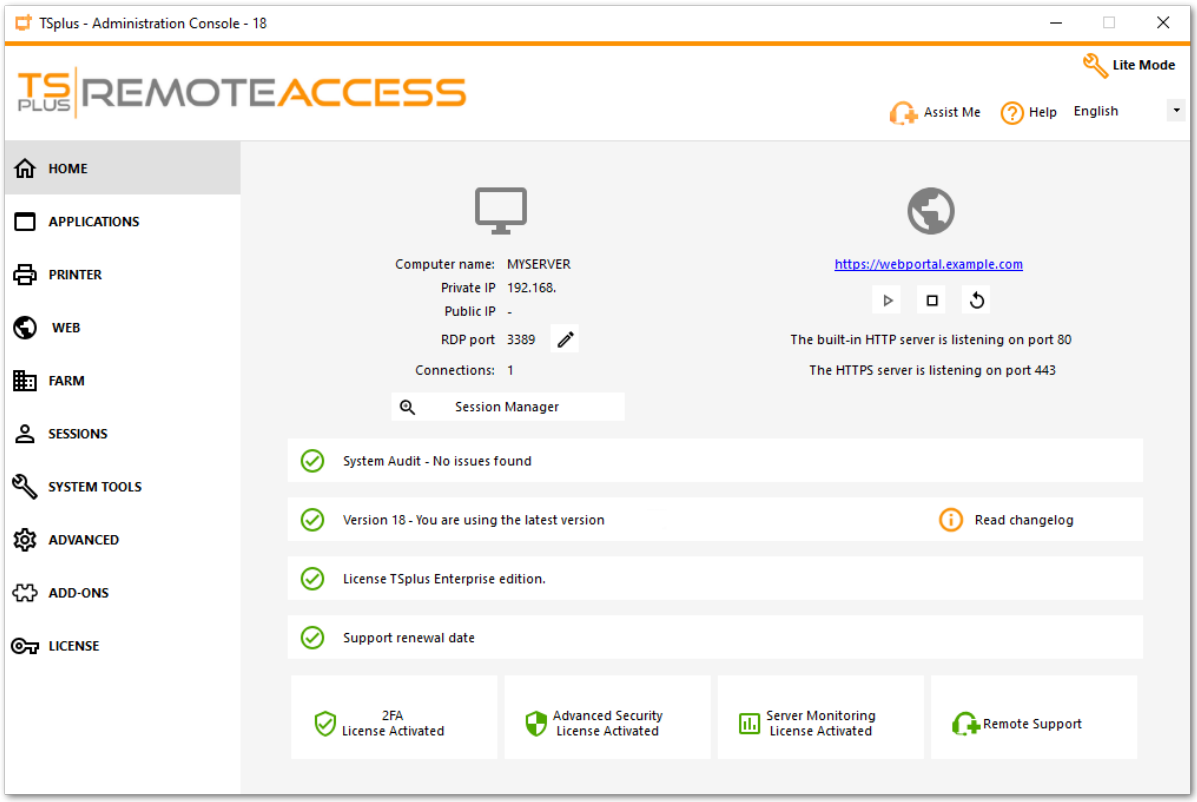
  De cette manière, ils peuvent restreindre l'accès au programme du client lui-même, tout en s'assurant qu'il ne peut pas être copié sur la clé USB et utilisé ailleurs.



Pour plus d'informations sur les fonctionnalités de sécurité, consultez Documentation du générateur de client portable TSplus et notre FAQ.

Gestion des serveurs

Sur l'onglet Accueil de l'AdminTool, vous pouvez voir toutes les informations nécessaires sur votre serveur TSplus :



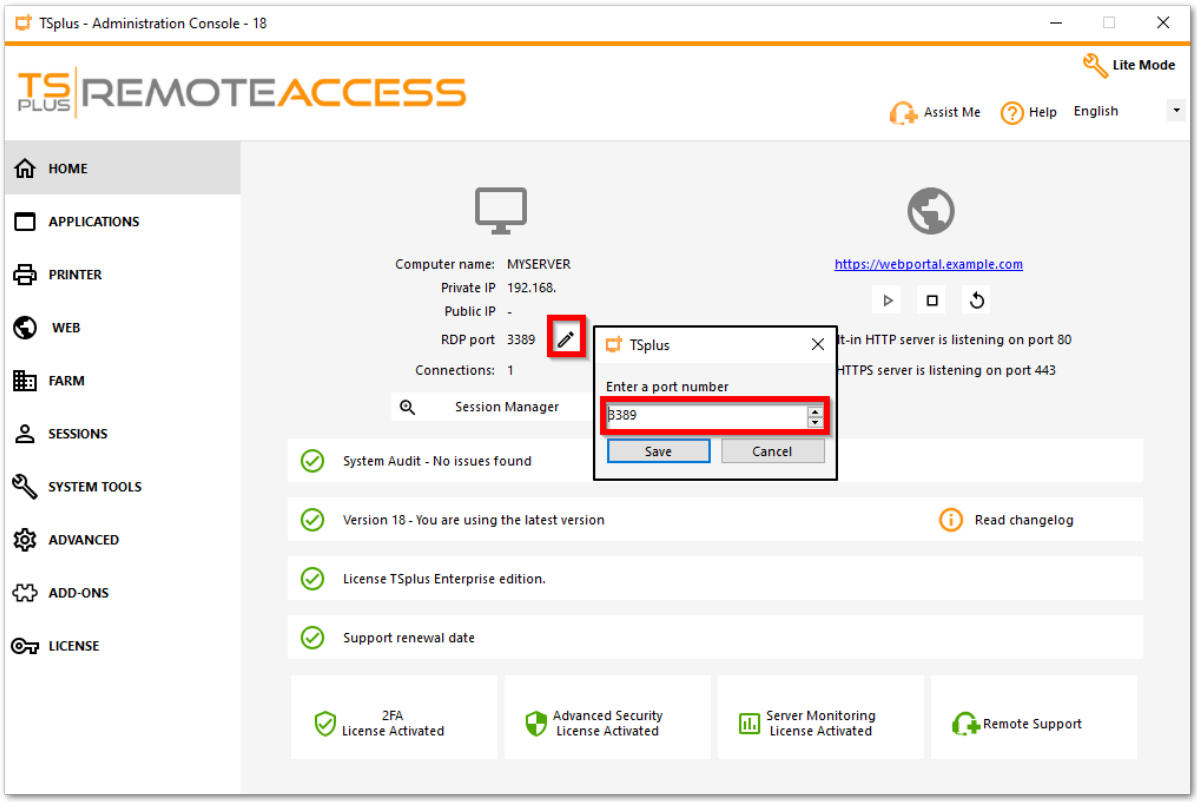
Changer le numéro de port RDP et configurer le pare-feu

Avec l'AdminTool, vous pouvez sélectionner un numéro de port TCP/IP différent pour que le service RDP accepte les connexions. Le port par défaut est 3389. Vous pouvez choisir n'importe quel port arbitraire, à condition qu'il ne soit pas déjà utilisé sur votre réseau et que vous définissiez le même numéro de port sur vos pare-feu et sur chaque programme d'accès utilisateur TSplus.

TSplus inclut une capacité unique de redirection de port et de tunneling : quel que soit le port

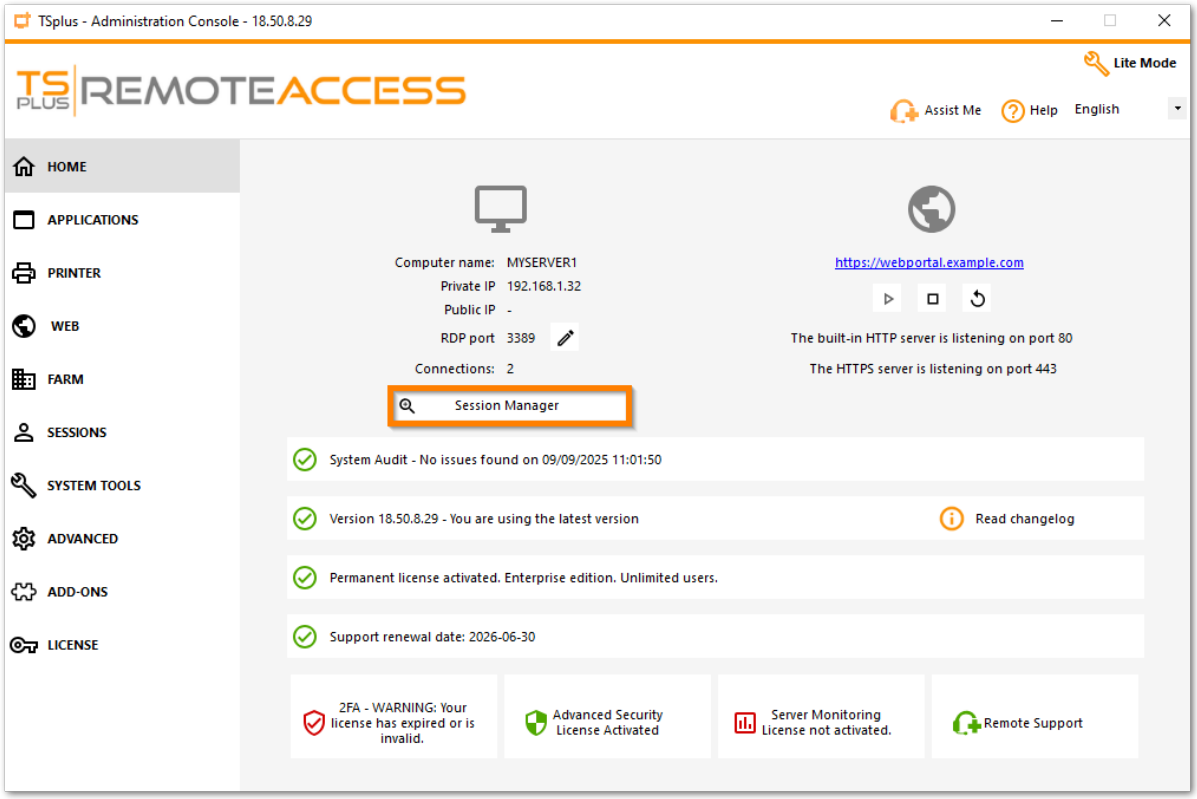
RDP qui a été défini, le RDP sera également disponible sur le numéro de port HTTP et HTTPS !

Si les utilisateurs souhaitent accéder à votre serveur TSplus en dehors de votre réseau, vous devez vous assurer que toutes les connexions entrantes sur le port choisi sont redirigées vers le serveur TSplus.

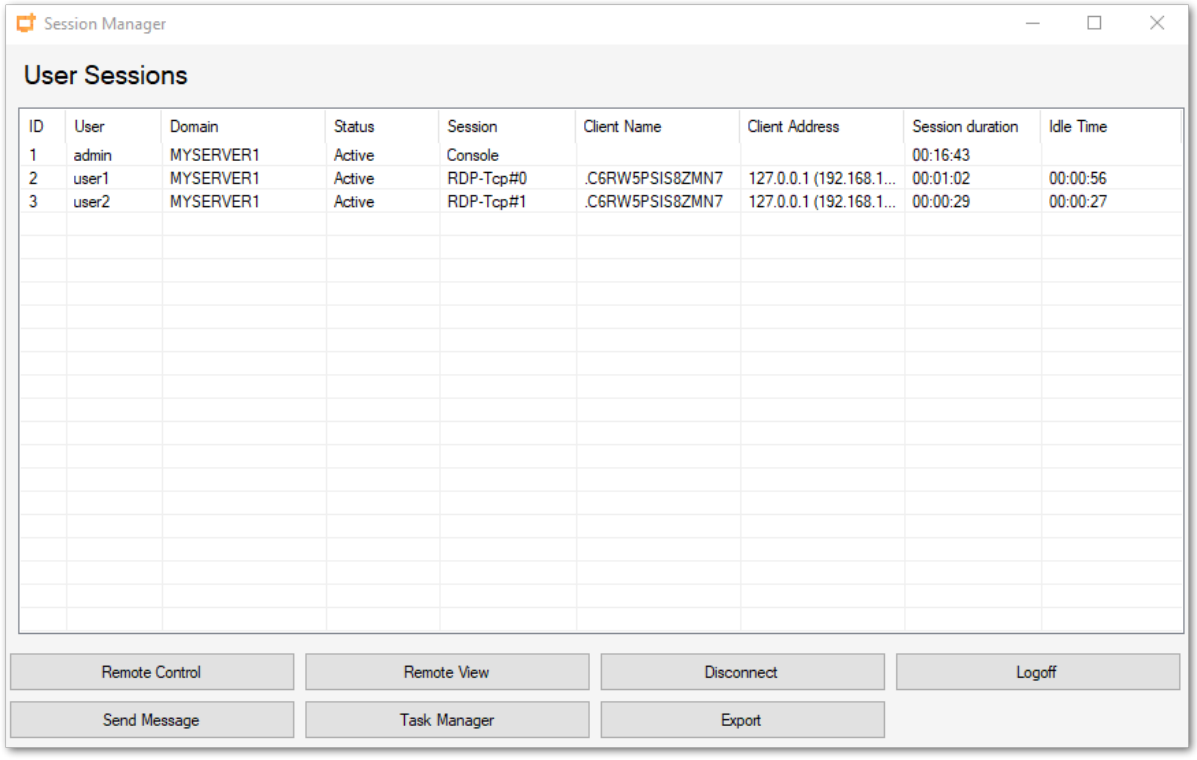


Gestion des utilisateurs et des sessions

Le gestionnaire de session est situé juste en dessous du port RDP :



Vous pouvez afficher le gestionnaire de tâches de votre serveur, et vous avez la possibilité d'activer un contrôle à distance, de déconnecter, de vous déconnecter ou d'envoyer un message à vos utilisateurs.



Vous pouvez activer le contrôle à distance via une session à distance avec un compte

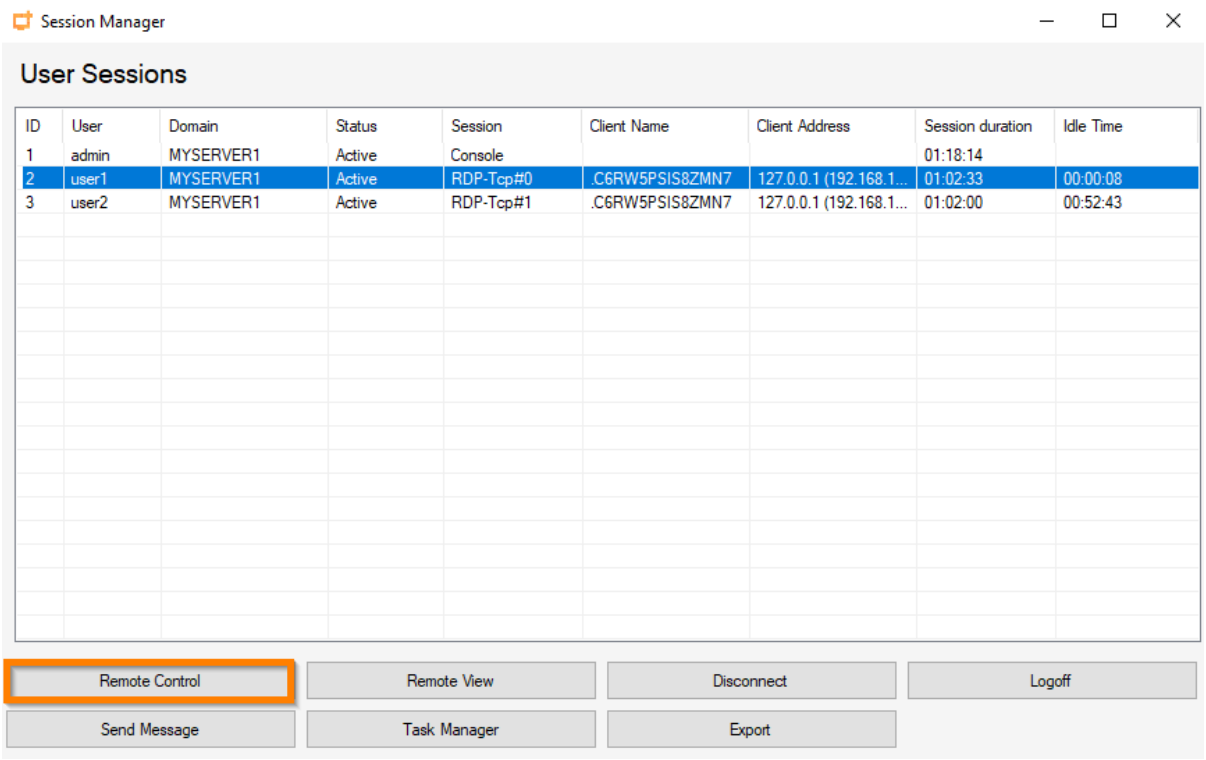
administrateur sur les systèmes d'exploitation suivants :

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7
- Windows 8.1
- Windows 10 pro et supérieur

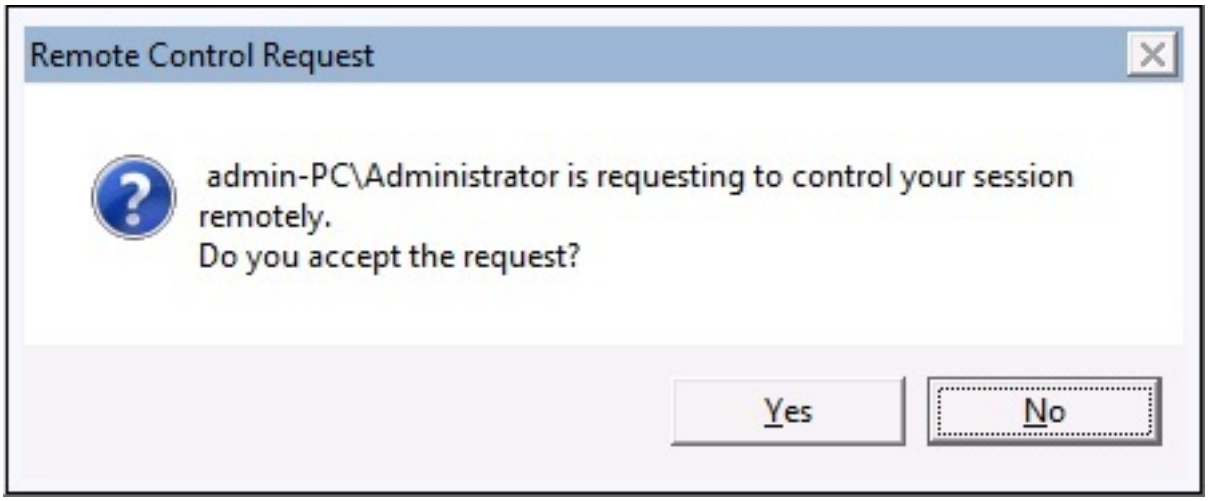
Sur Windows XP, 2003, Vista et 2008, il n'y a pas de bouton de contrôle à distance.

Sur Windows 2012 et 8, un message apparaît vous conseillant de mettre à jour vers 2012 R2 ou 8.1.

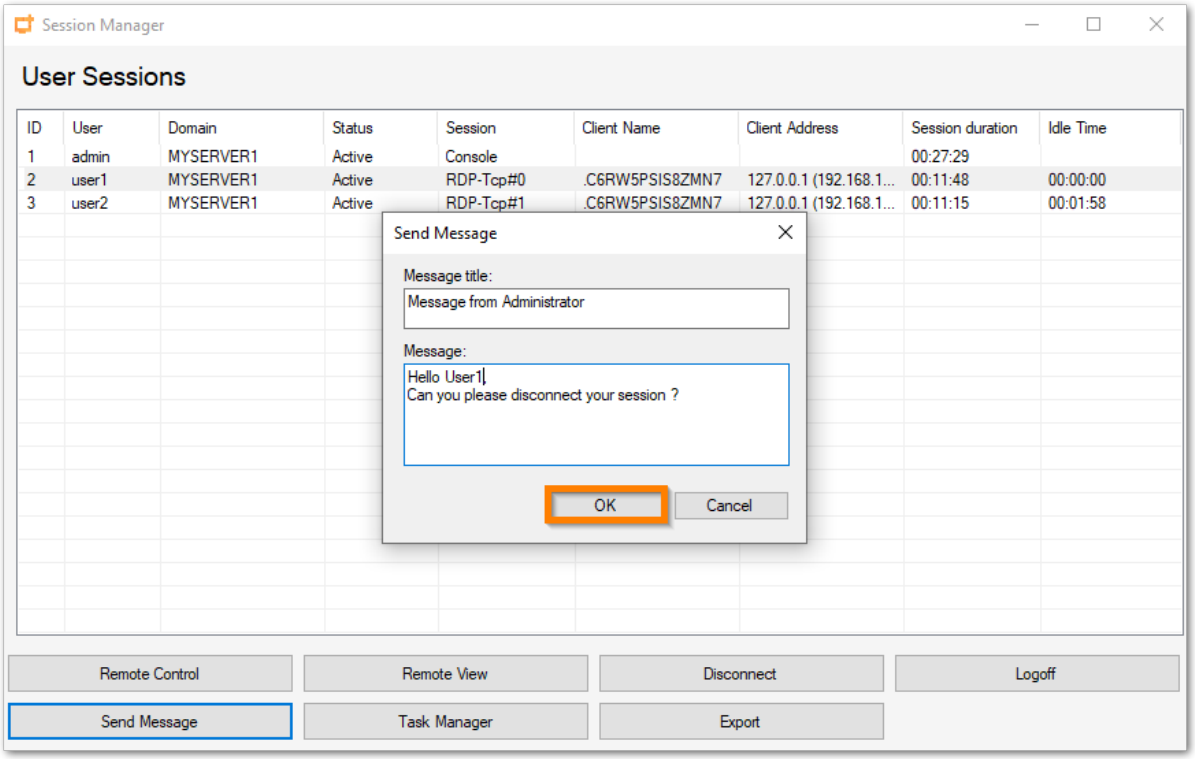
Lorsque vous activez le contrôle à distance pour la session d'un utilisateur, ce message apparaît, indiquant le raccourci clavier pour mettre fin à la session :



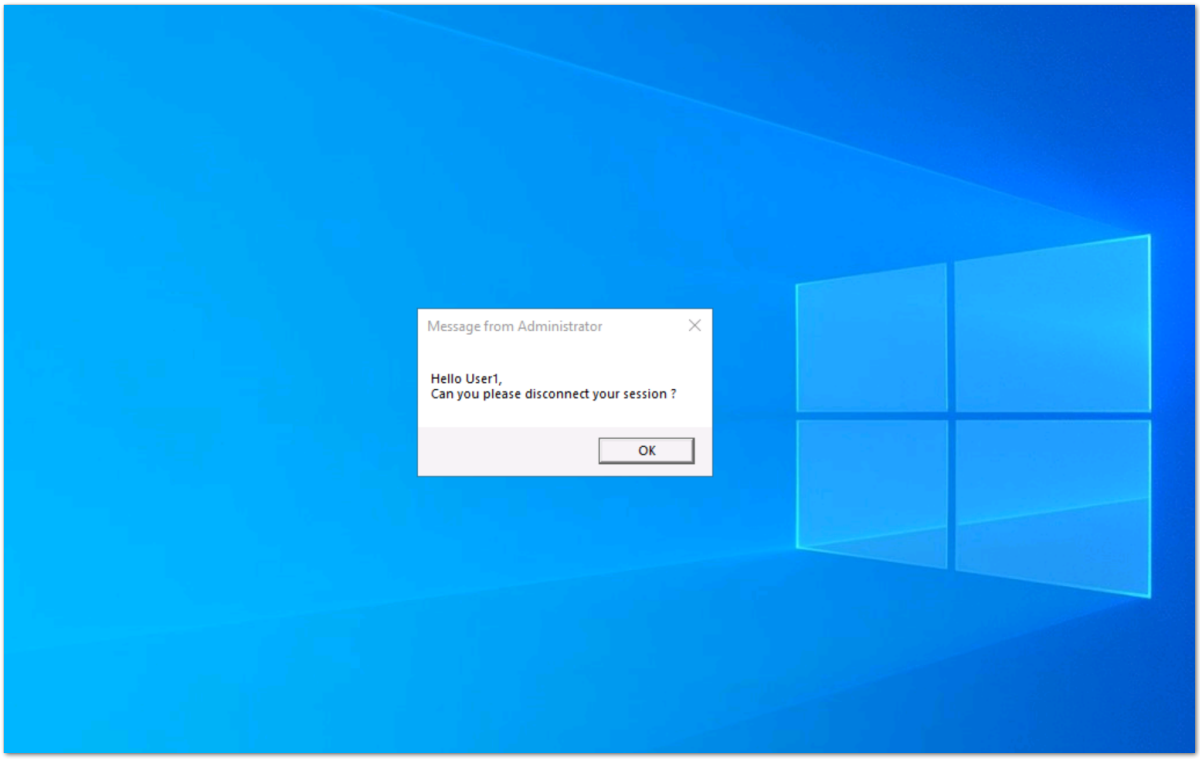
Sur le côté client, ce message apparaît pour accepter le contrôle à distance :



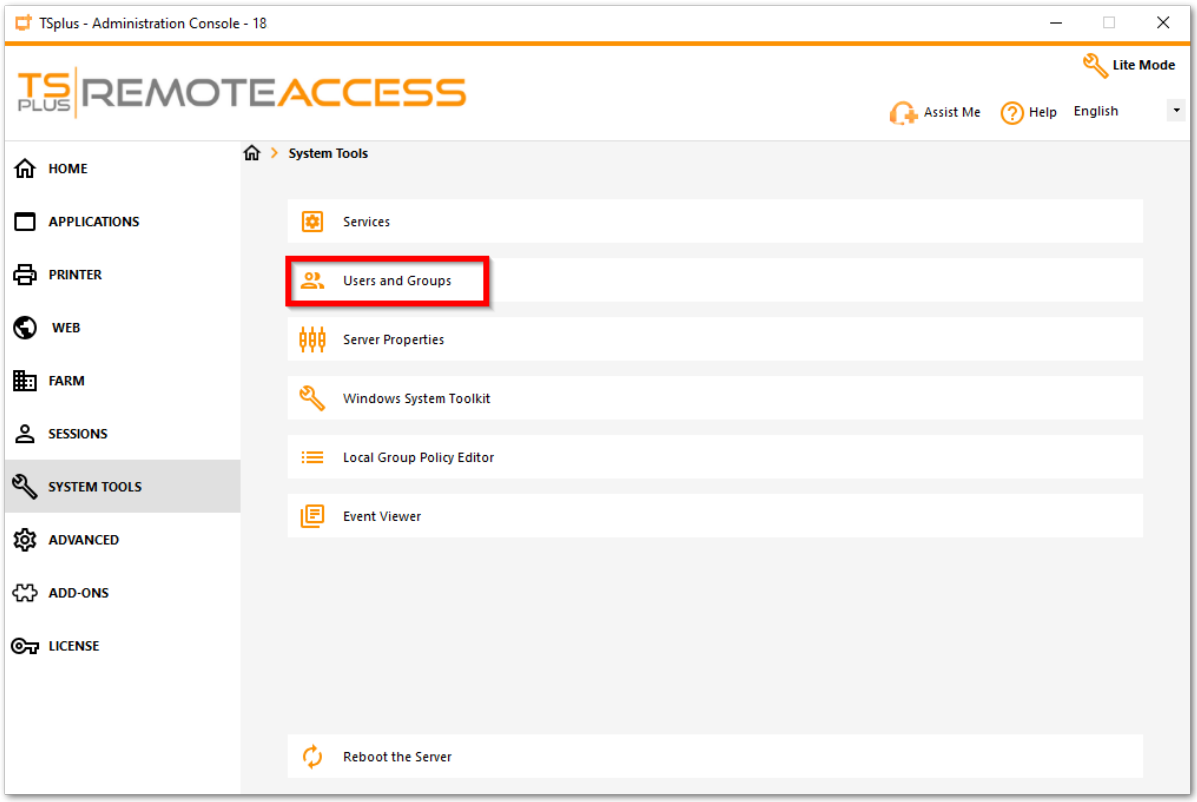
Vous pouvez également envoyer un message à votre utilisateur :



Message envoyé sur le serveur



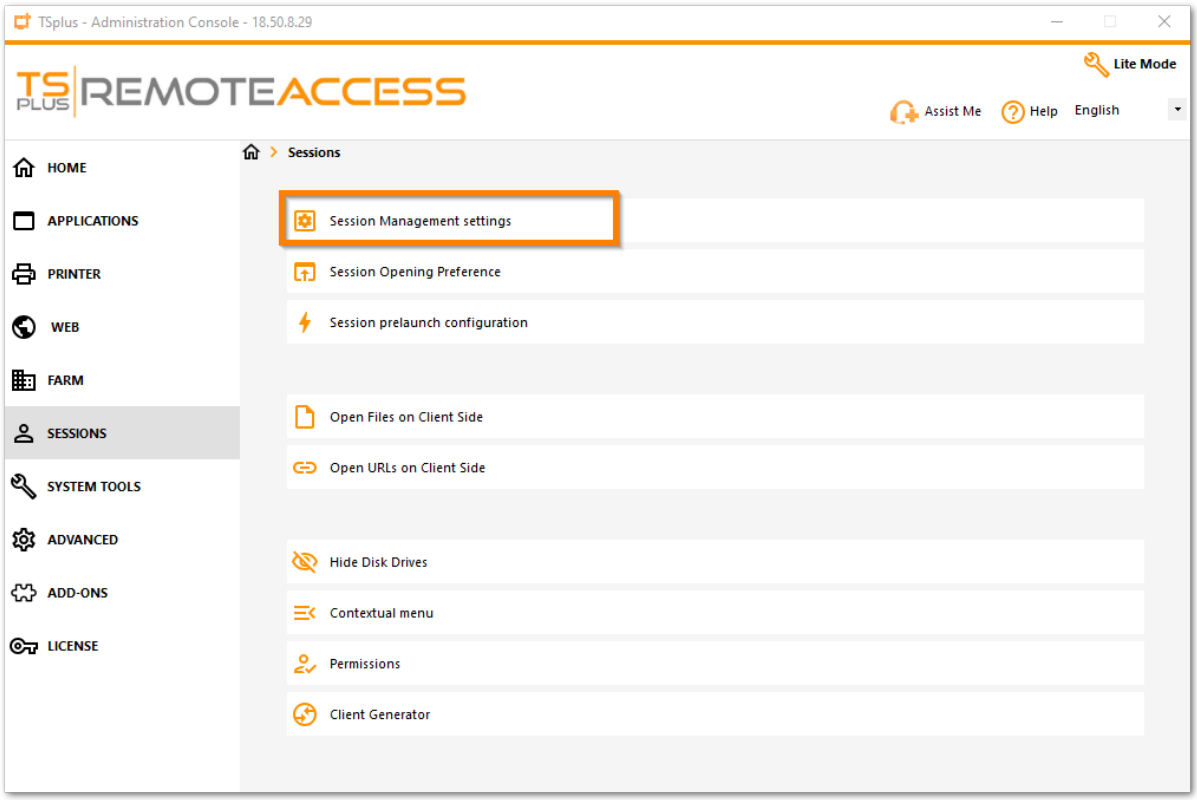
Message apparaissant du côté client

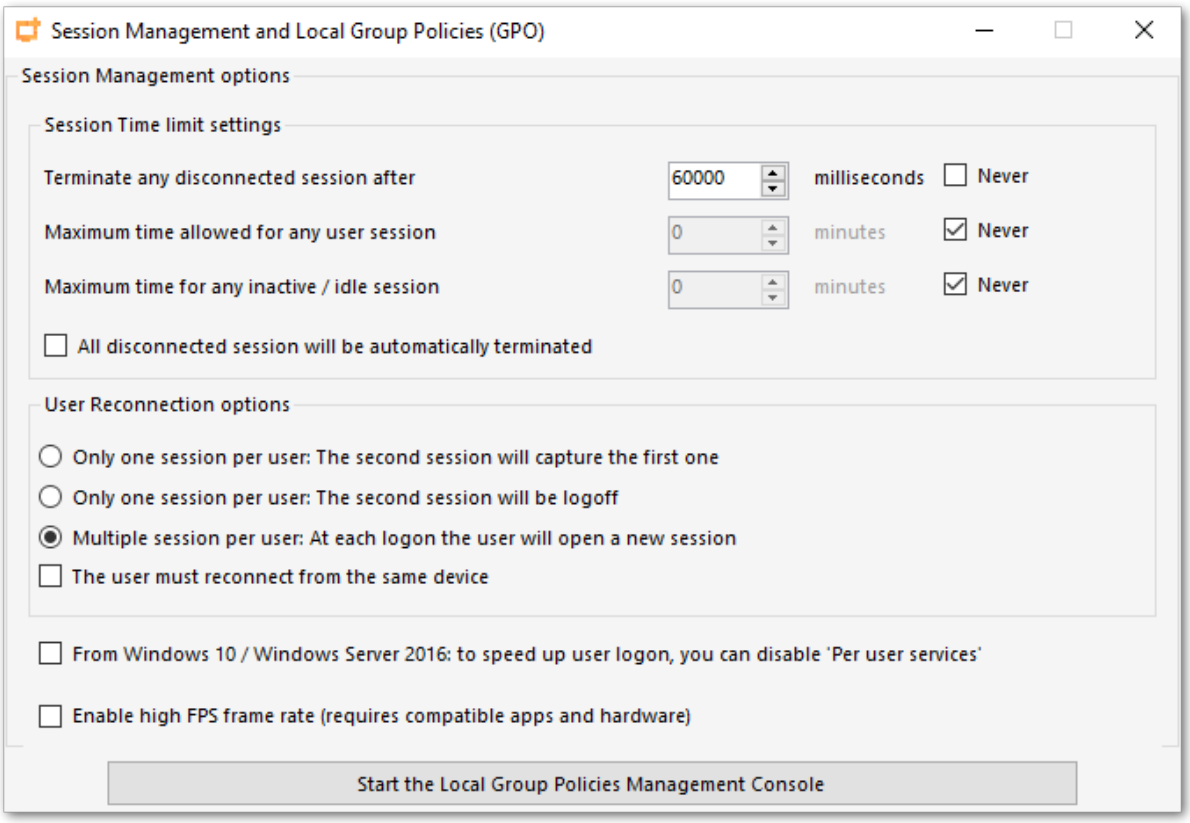


Voir cette documentation pour plus d'informations.

- Avec l'onglet Paramètres de gestion des sessions (GPO), vous pouvez définir divers

paramètres de connexion pour chaque session et utilisateur :



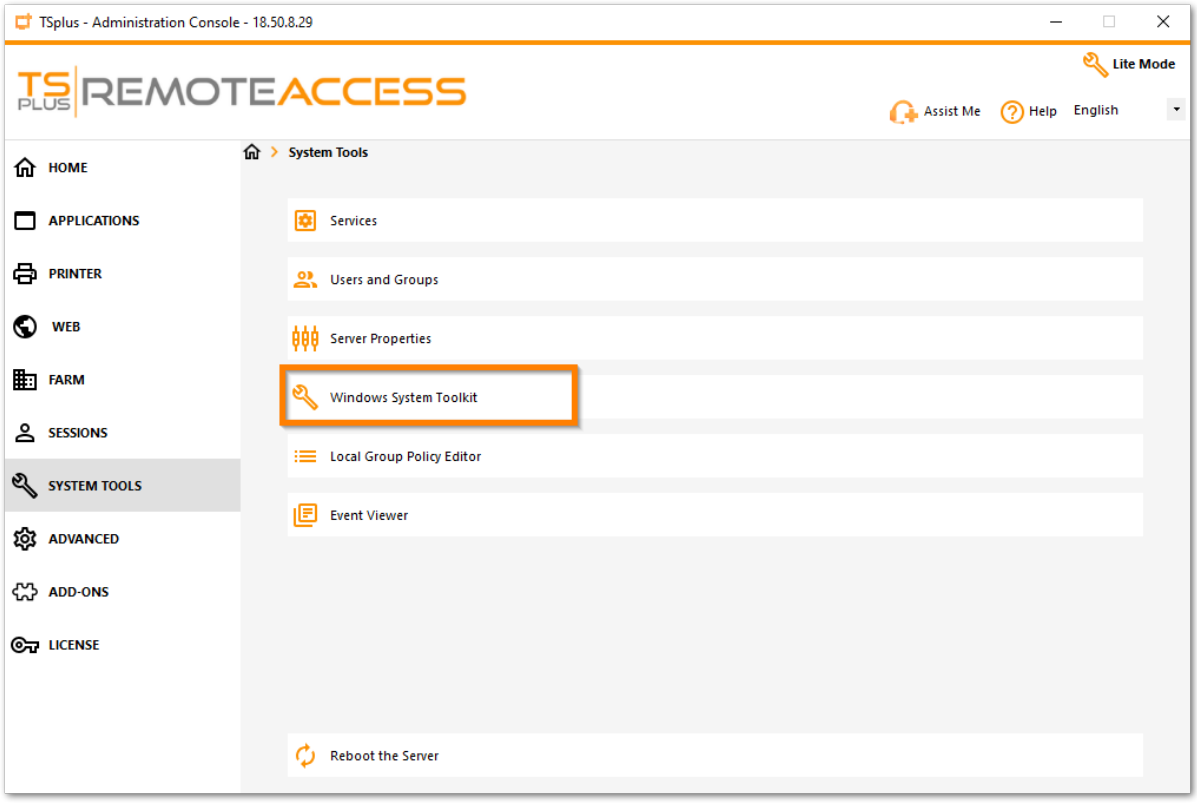


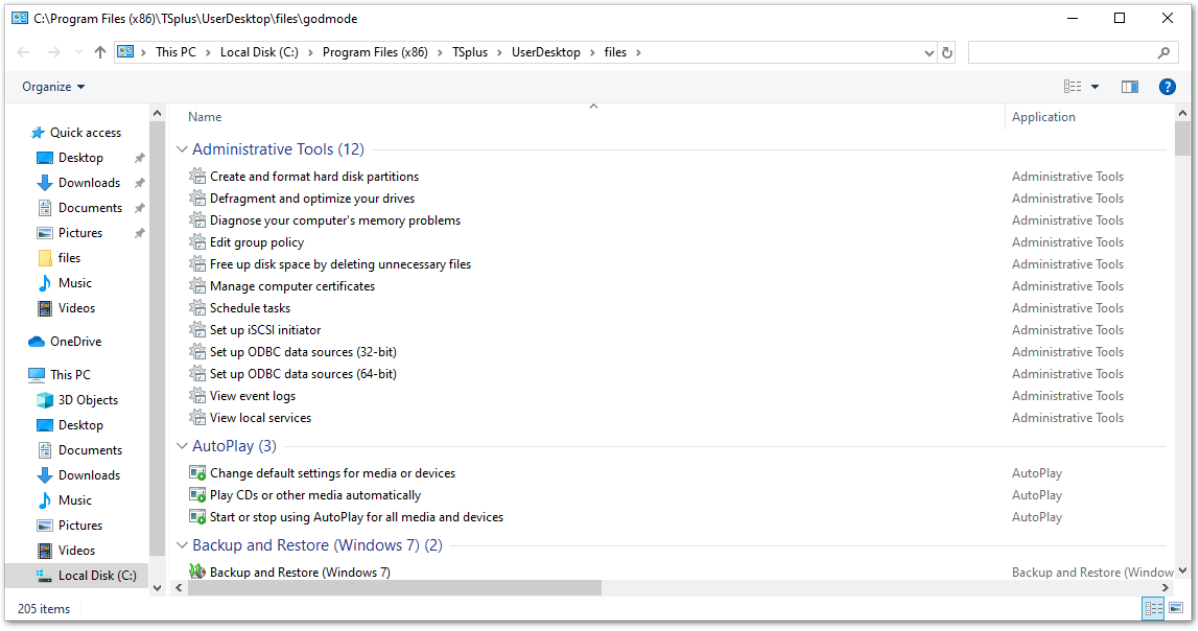
Windows Server 2016 a introduit un nouveau « service par utilisateur », qui fait démarrer tous les

processus par utilisateur, ce qui ralentit le temps de connexion des utilisateurs.

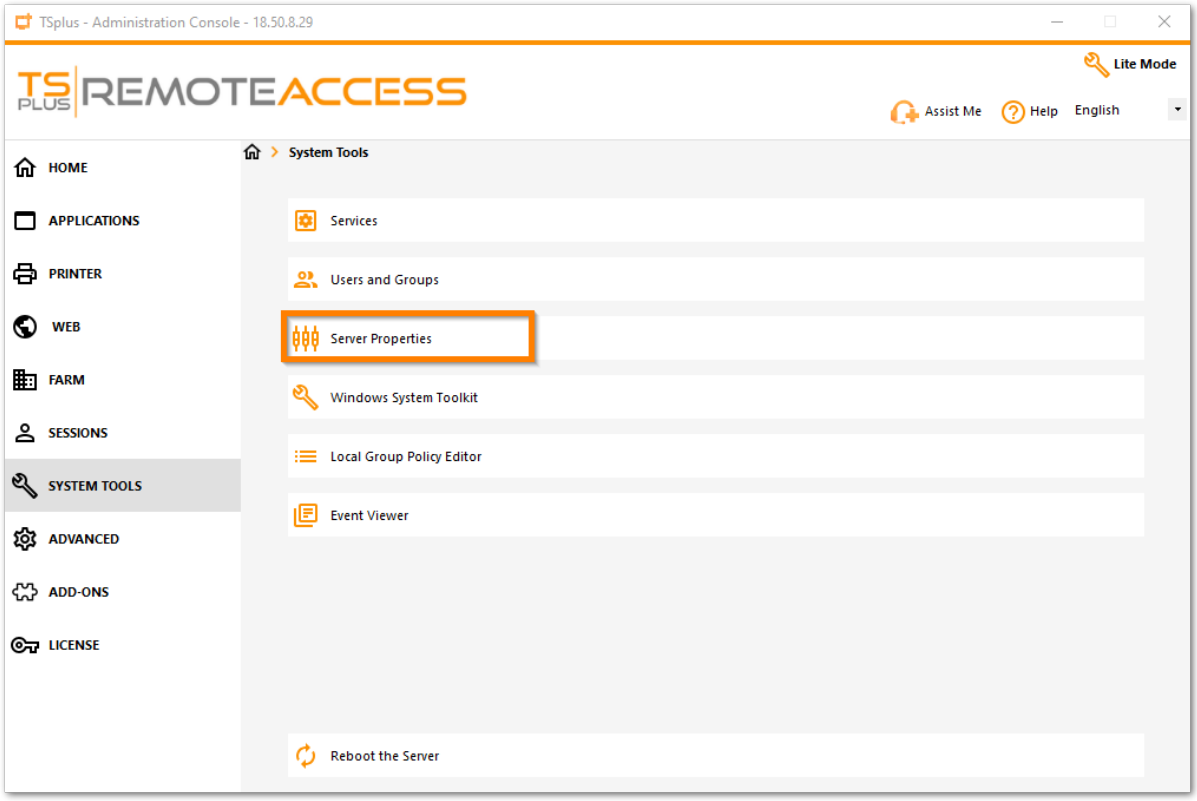
Depuis la sortie de TSplus 11.70, vous pouvez **désactiver les services par utilisateur afin d'accélérer les connexions des utilisateurs** .

- Le Kit d'outils Windows est un panneau de contrôle amélioré, résumant tous les outils d'administration Windows.

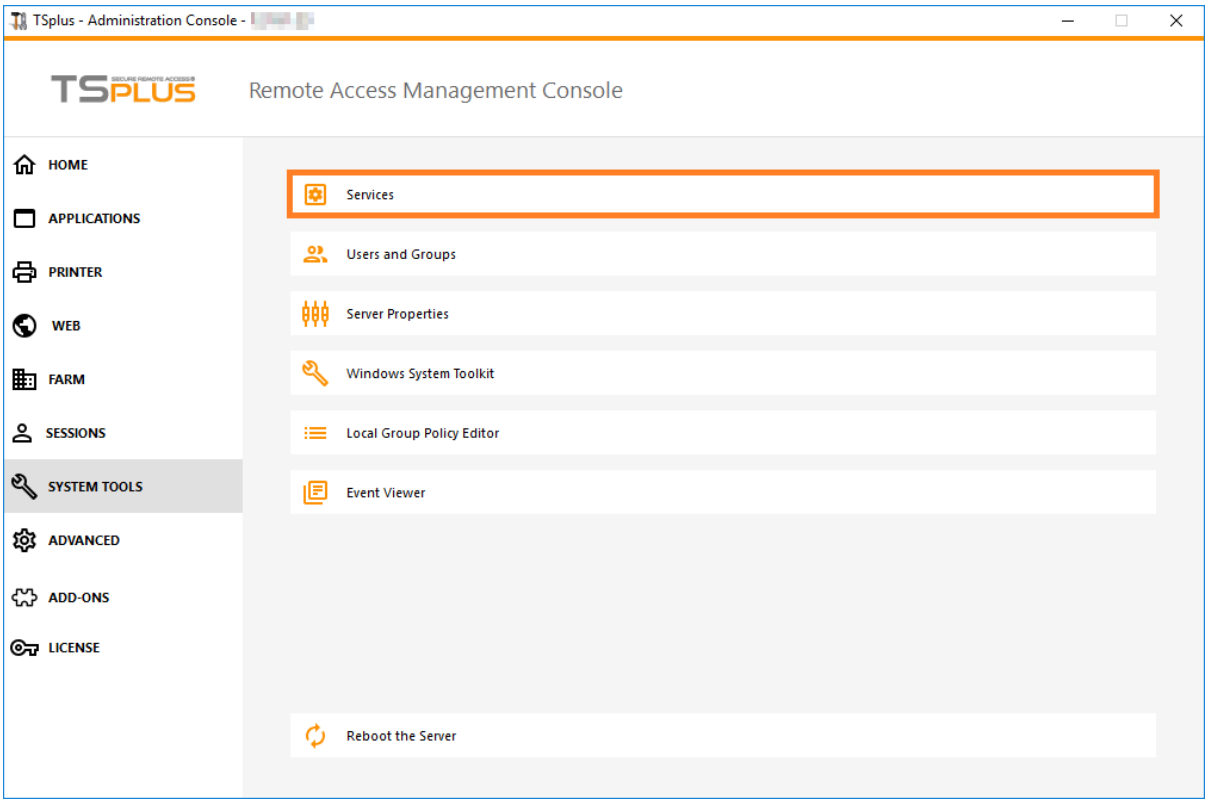




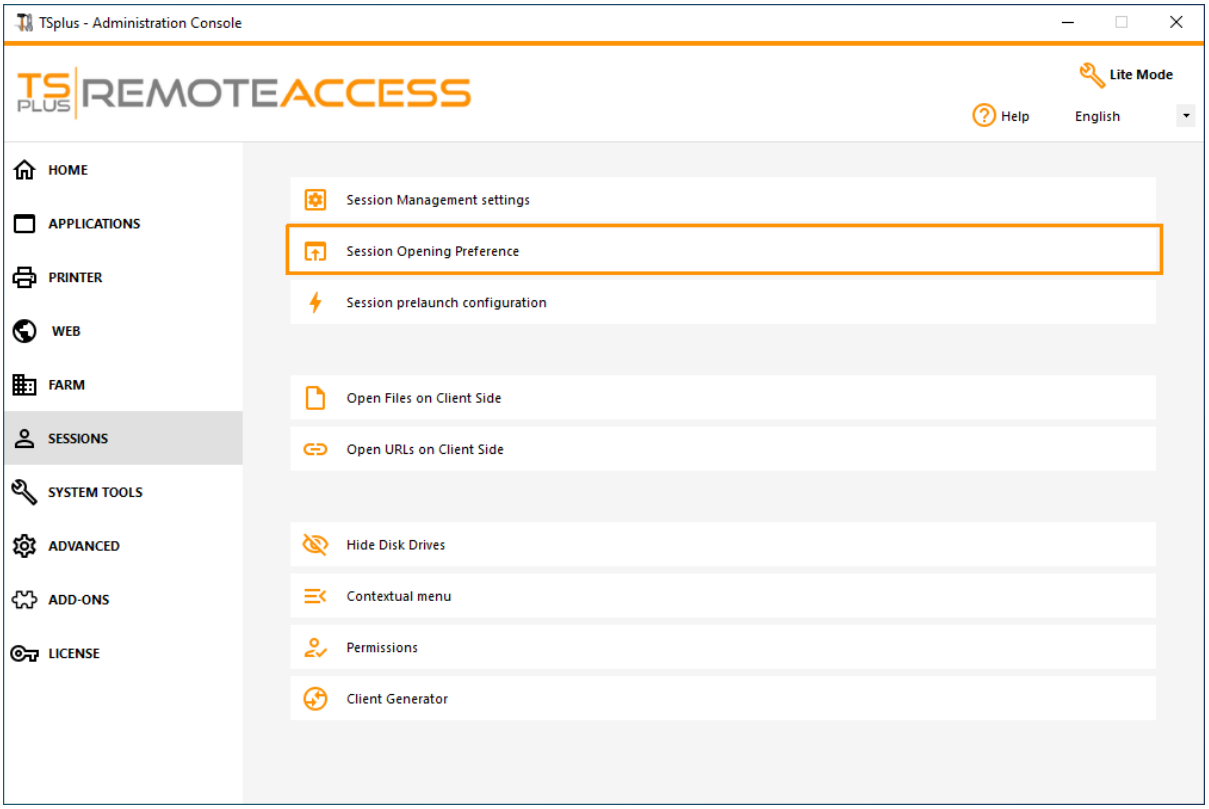
- Vous pouvez également lancer l'onglet « Propriétés du serveur » pour avoir un aperçu du panneau de contrôle.



- Vous pouvez voir tous les services sur votre serveur et leur statut sur la tuile Services.

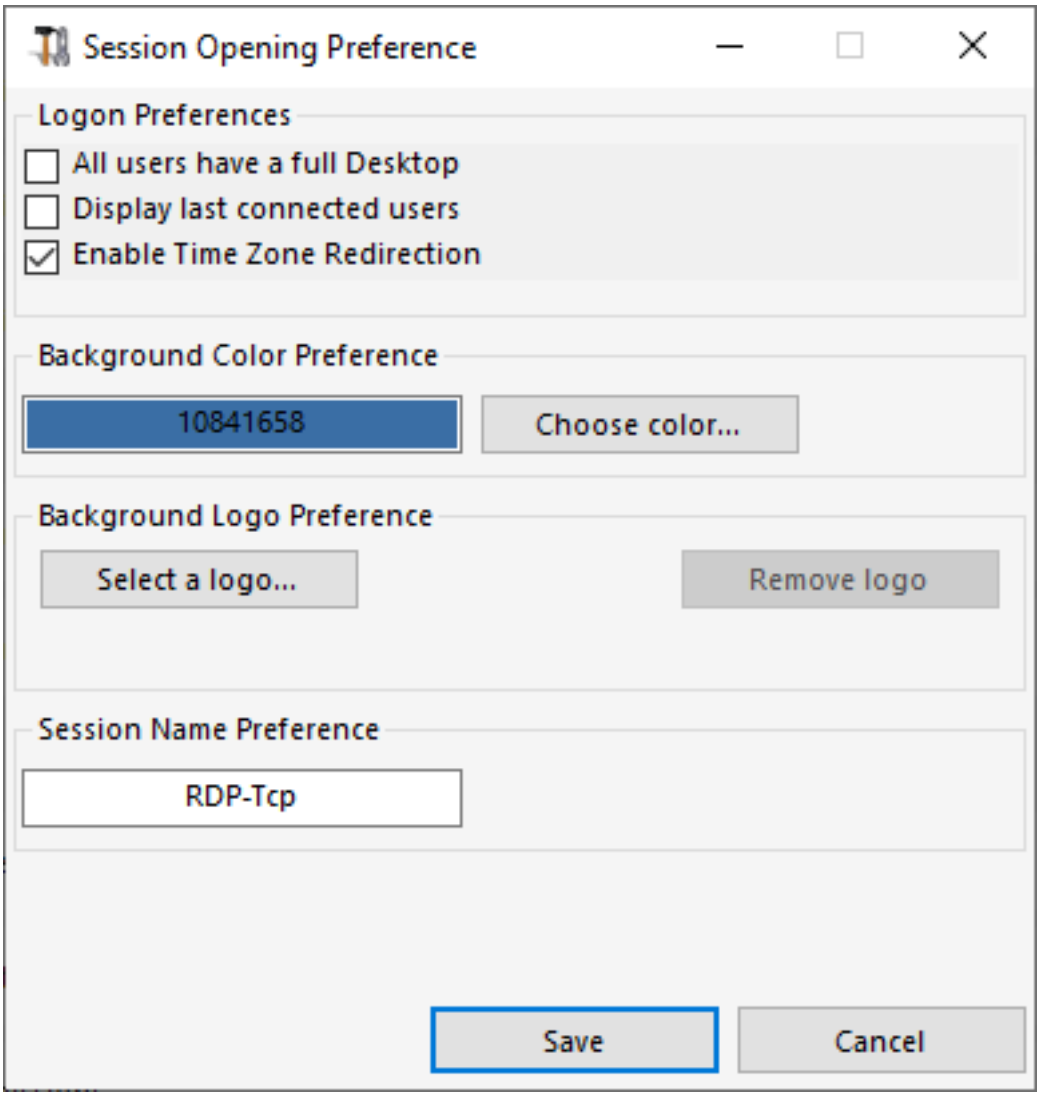


La préférence d'ouverture de session vous permet de choisir votre préférence de session shell, vos préférences de connexion, la couleur de fond de vos sessions, d'ajouter votre propre logo et de le renommer à votre convenance.



Par défaut, ces préférences de connexion sont activées :

- Le “ **Afficher la barre de progression pendant la connexion** ”.
- “ **Activer la redirection de fuseau horaire** qui permet à l'ordinateur client de rediriger ses paramètres de fuseau horaire vers la session des Services de Bureau à Distance. Si vous activez ce paramètre de stratégie, les clients capables de redirection de fuseau horaire envoient leurs informations de fuseau horaire au serveur.



Vous pouvez également **définir un bureau complet** pour tous vos utilisateurs et **obtenir un affichage des derniers utilisateurs connectés** en cochant les cases correspondantes. Vous pouvez **personnalisez les sessions de vos utilisateurs** en ajoutant une nouvelle couleur de fond, un autre logo ou aucun et en utilisant le nom de session de votre choix.

- Depuis la version 11.70 de TSplus, vous pouvez utiliser **TSplus WinXshell** comme alternative à l'interface de commande Windows.

Suite à la mise à jour de Windows du 10 octobre, les administrateurs permettant à leurs utilisateurs de démarrer un Remote Desktop ont constaté que le shell Windows posait un problème.

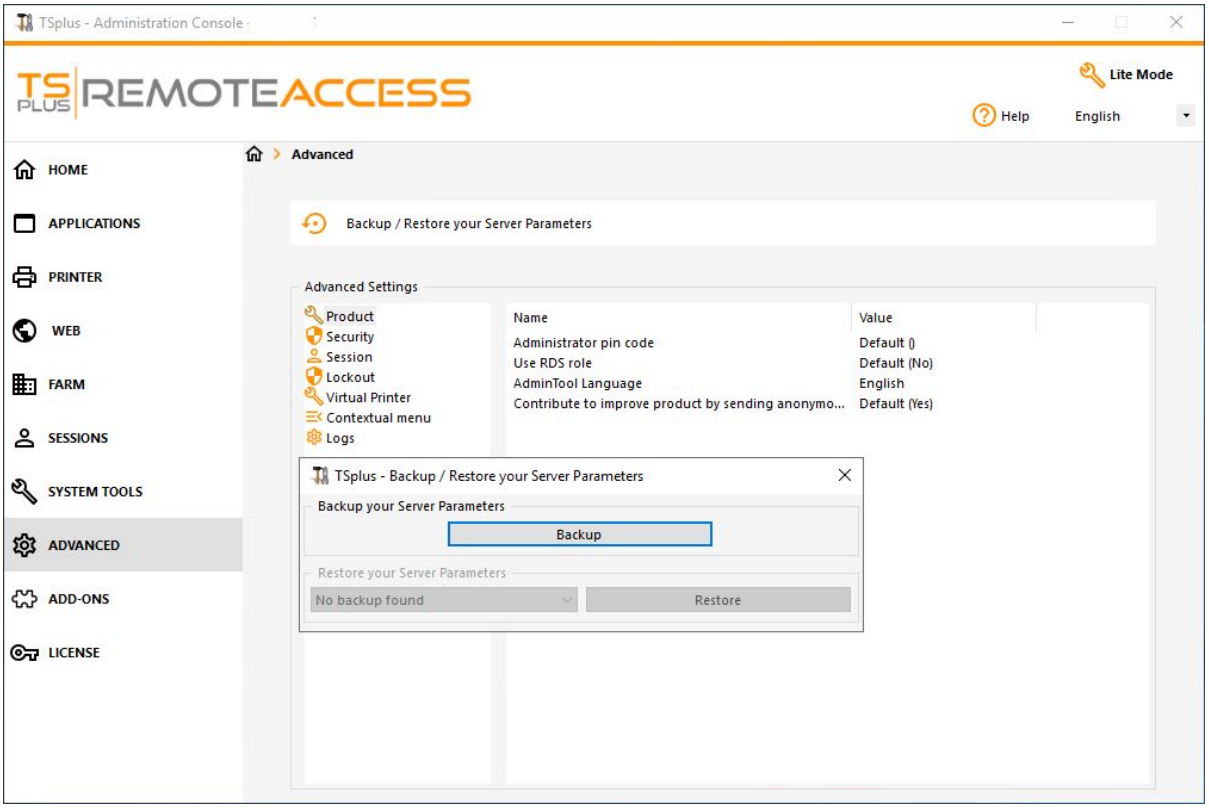
Le principal problème réside dans l'ouverture de session/problème d'écran noir lorsque un bureau complet est attribué à plusieurs utilisateurs sur Windows 10 et Server 2016.

Il offre des fonctionnalités et une expérience graphique similaires à celles de l'interface Windows 2016, telles que l'affichage du bouton Démarrer 2016 et de la barre des tâches.

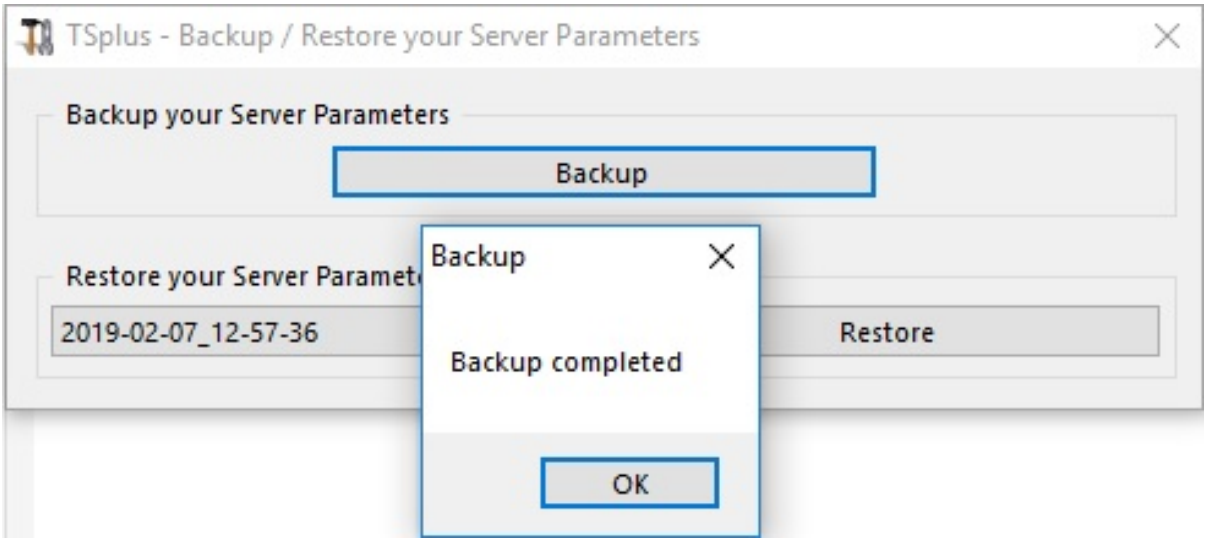
Il est particulièrement utile si vous **utiliser les systèmes d'exploitation Windows 10 ou Windows 16** , **gérer 10 utilisateurs ou plus** et **souhaite leur attribuer un bureau complet** .

Paramètres de sauvegarde

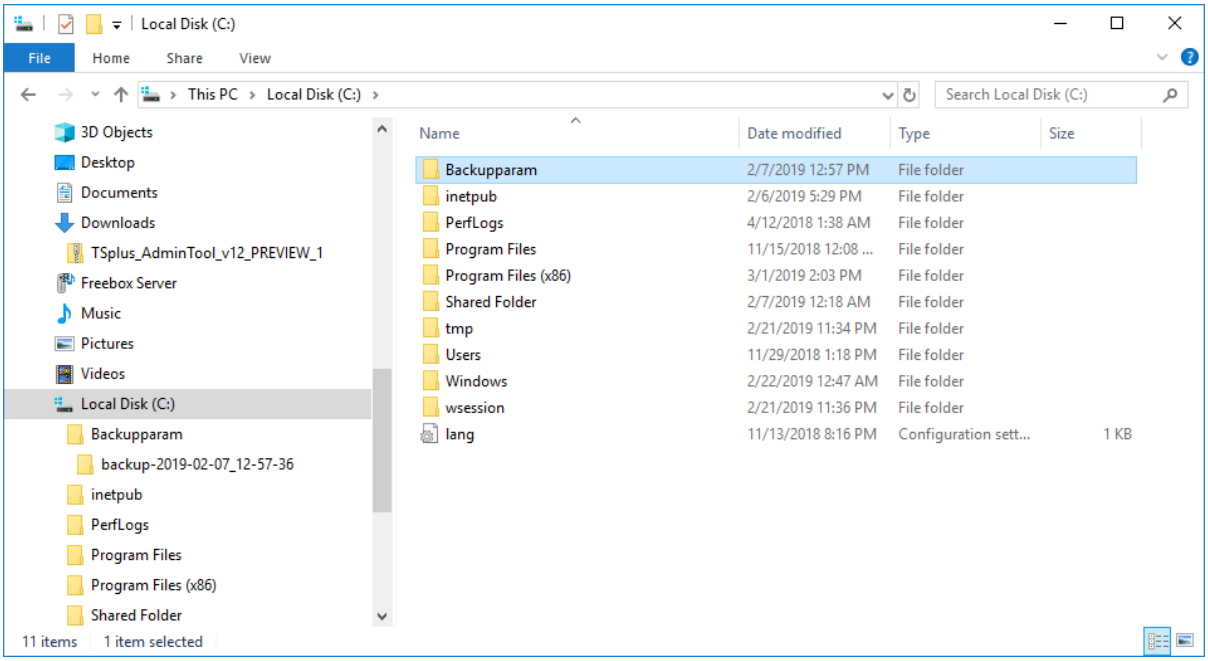
Vous pouvez sauvegarder ou restaurer les paramètres de votre serveur en cliquant sur la tuile du même nom, dans l'onglet Avancé :



Cliquez sur le bouton Sauvegarder pour effectuer une sauvegarde, qui sera datée et ajoutée à la liste de vos points de restauration :



Le fichier de sauvegarde se trouve dans le dossier C:\Backupparam :



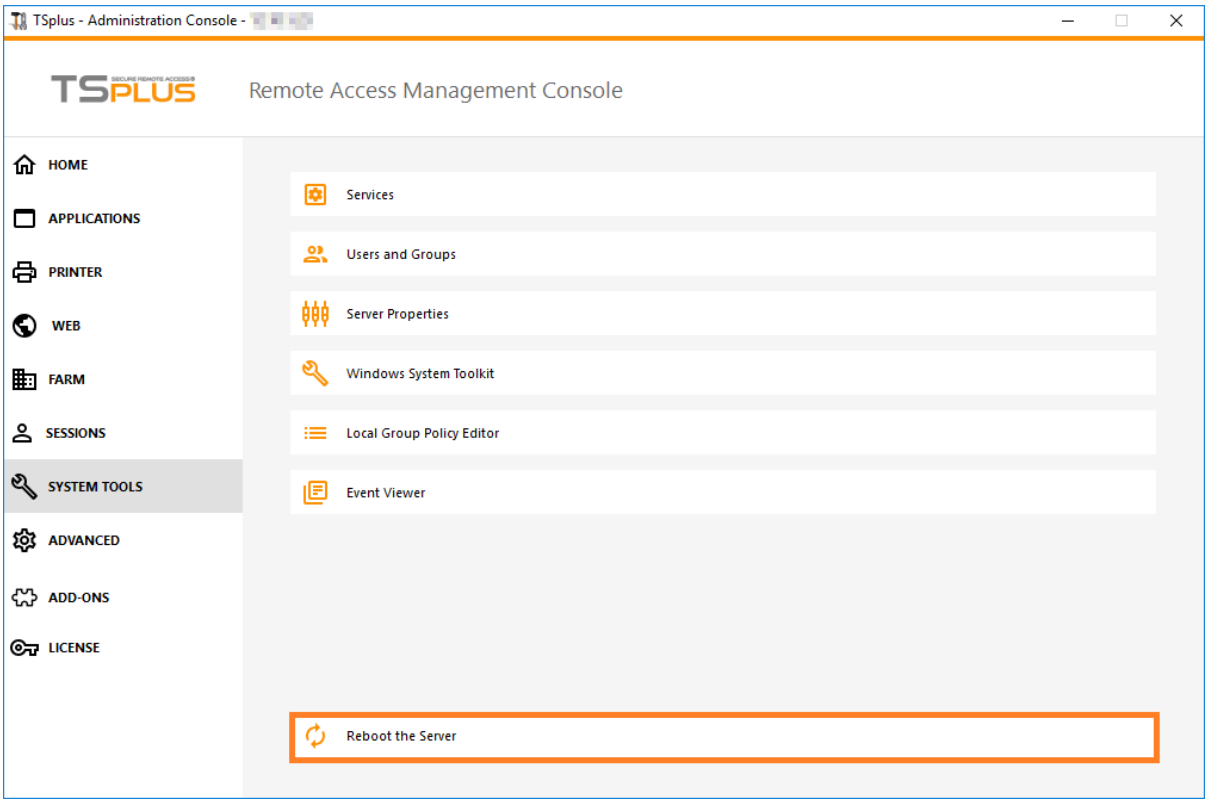
Copiez le dossier sur le nouveau serveur après avoir installé TSplus Remote Access et restaurez la sauvegarde.

Vous pouvez ensuite vérifier avec l'essai de 15 jours que le fonctionnement des comptes et des accès est correct avant de migrer votre licence définitivement.

Plus d'informations à ce sujet documentation .

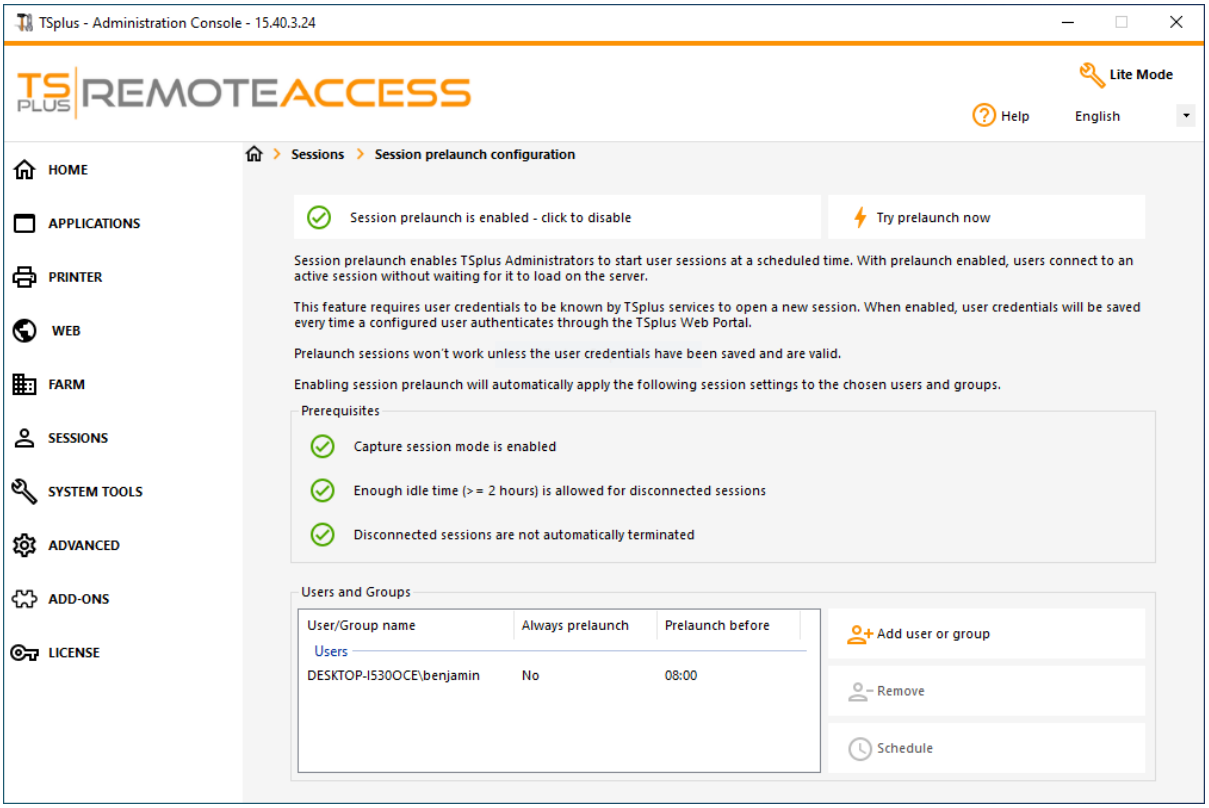
Redémarrez votre serveur

L'onglet « Redémarrer le serveur » vous permet de redémarrer votre serveur.


TSplus - Administration Console -
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Services
Users and Groups
Server Properties
Windows System Toolkit
Local Group Policy Editor
Event Viewer
Reboot the Server

Pré-lancement de session

Accédez au menu de configuration de pré-lancement de session depuis l'onglet Sessions > Paramètres de l'Admintool, en cliquant sur la tuile "Configuration de pré-lancement de session".

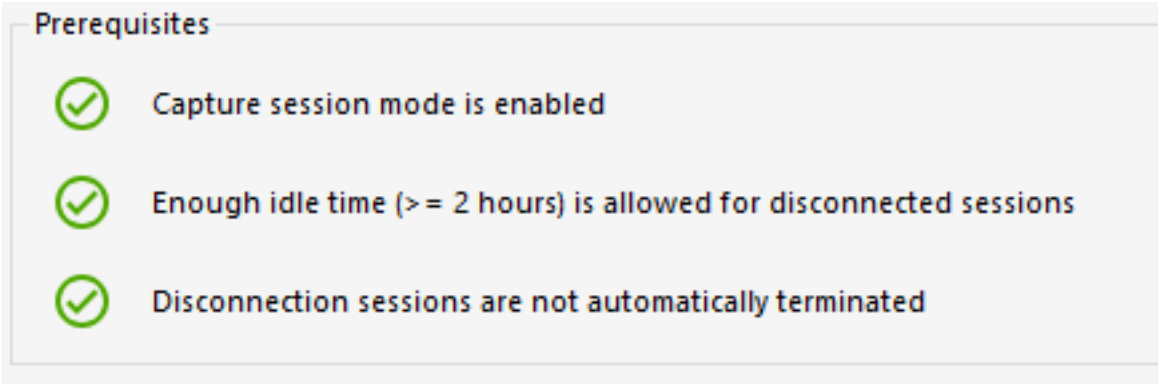


Aperçu

La fonctionnalité de pré-lancement de session permet aux administrateurs de TSplus Remote Access de configurer les sessions des utilisateurs pour qu'elles se lancent avant une heure programmée. L'idée est de préparer et de charger la session de chaque utilisateur configuré à l'avance, afin qu'une fois qu'un utilisateur se connecte, il puisse capturer sa session spécifique. Cela peut réduire les temps d'attente de connexion de plusieurs minutes à quelques secondes.

Prérequis

La pré-lancement nécessite que plusieurs prérequis soient satisfaits.



1 - Afin de capturer une session, **le mode de capture de session doit être activé.** Cela signifie que vous ne pourrez pas bénéficier de cette fonctionnalité si la configuration multi-session est obligatoire pour vos utilisateurs.

2 - Puisque la session préparée chargée à l'avance doit être présente (non déconnectée) lorsque l'utilisateur se connecte et la capture, **un minimum de 2 heures de temps d'inactivité pour une session déconnectée doit être autorisé.** Vous pouvez bien sûr également définir les paramètres de session afin qu'il ne déconnecte jamais une session déconnectée.

3 - Puisque la session préparée est déconnectée une fois chargée pour réduire l'utilisation globale des ressources, **les paramètres de session doivent être configurés pour ne pas déconnecter automatiquement les sessions déconnectées.**

Note importante ! Chaque utilisateur configuré devra s'authentifier au moins une fois via le TSplus Web Portal après l'activation de la fonction de pré-lancement de session pour que les services TSplus puissent ouvrir la session de l'utilisateur configuré.

Compatibilités de pré-lancement de session

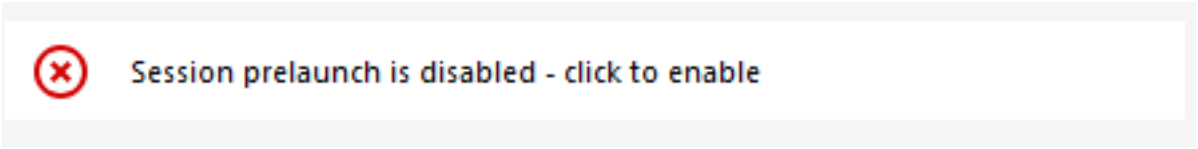
La pré-lancement de session est compatible avec les sessions HTML5 et les sessions RDP génériques ouvertes via un client généré ou mstsc.

Il n'est cependant pas compatible avec la connexion Remote App ou les connexions RDP personnalisées effectuées pour ouvrir un programme spécifique.
En conséquence, les connexions provenant du TSplus Web Application Portal ne sont pas prises en charge.

Activer la fonctionnalité

Pour activer la fonction de pré-lancement de session, il suffit de cliquer sur le carreau intitulé «

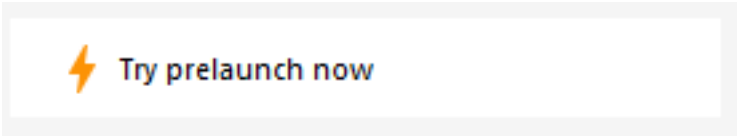
Le pré-lancement de session est désactivé - cliquez pour activer » près du haut de la fenêtre.



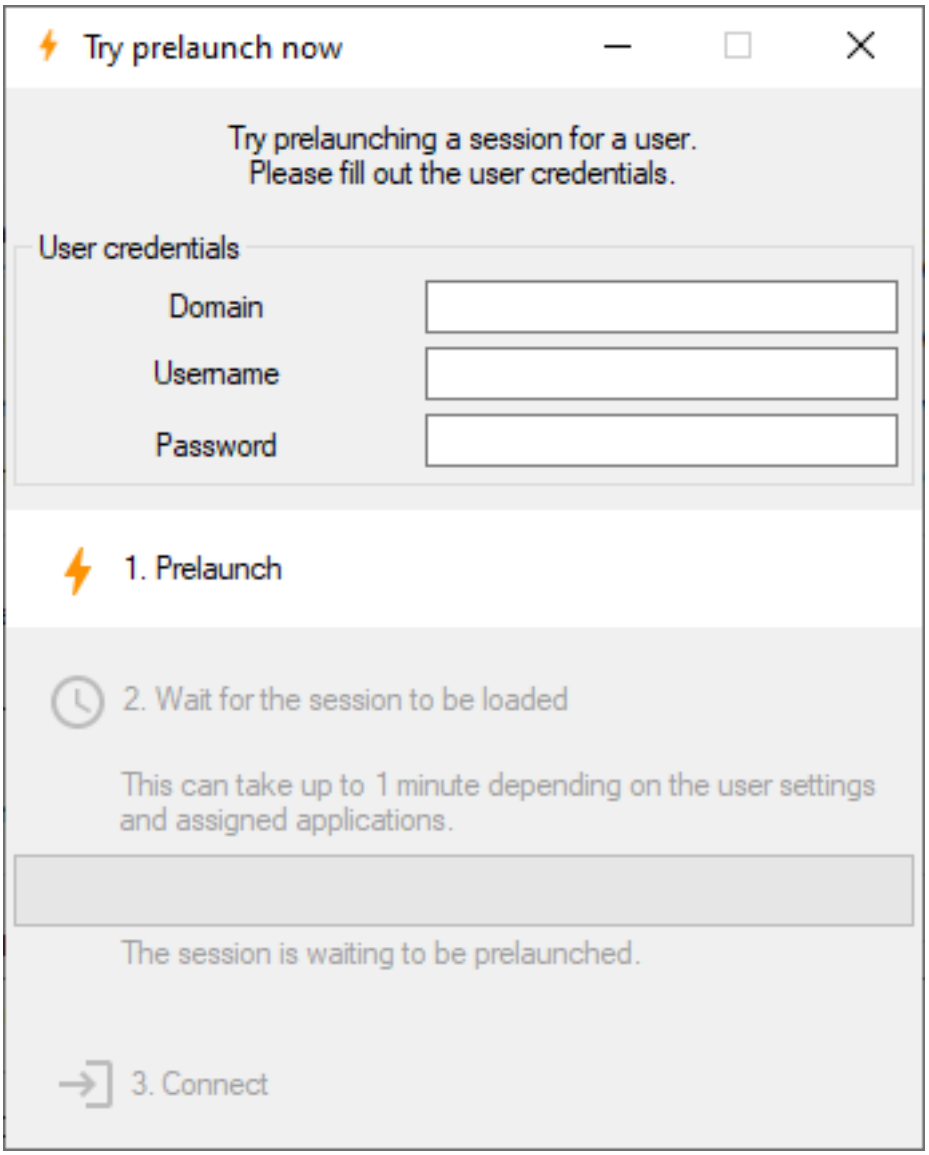
Si l'une des conditions préalables n'est pas remplie lors de l'activation de la pré-lancement de session, il vous sera demandé si vous souhaitez configurer automatiquement les paramètres de session pour répondre aux conditions préalables et utiliser la fonctionnalité. Notez que le changement des paramètres de session peut nécessiter un redémarrage.

Tester le pré-lancement de la session

Une fois activé, vous pourrez rapidement tester la fonctionnalité en cliquant sur le bouton « Essayer le pré-lancement maintenant » en haut.



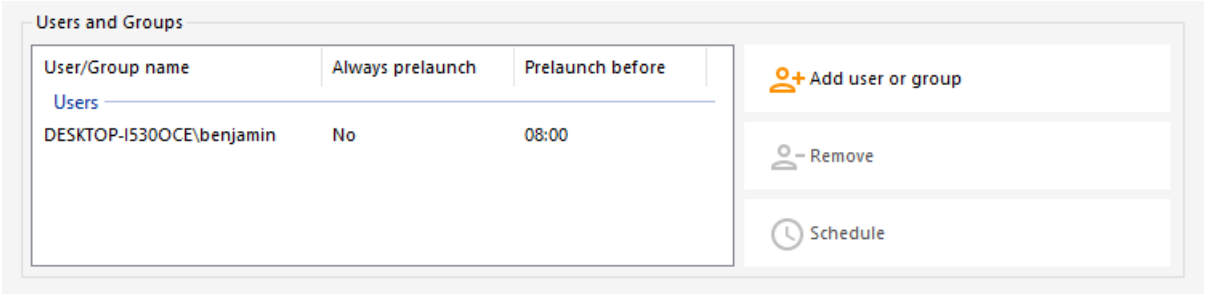
Dans la fenêtre qui apparaît, entrez les identifiants de l'utilisateur afin que les services TSplus puissent prélancer la session pour cet utilisateur spécifique.



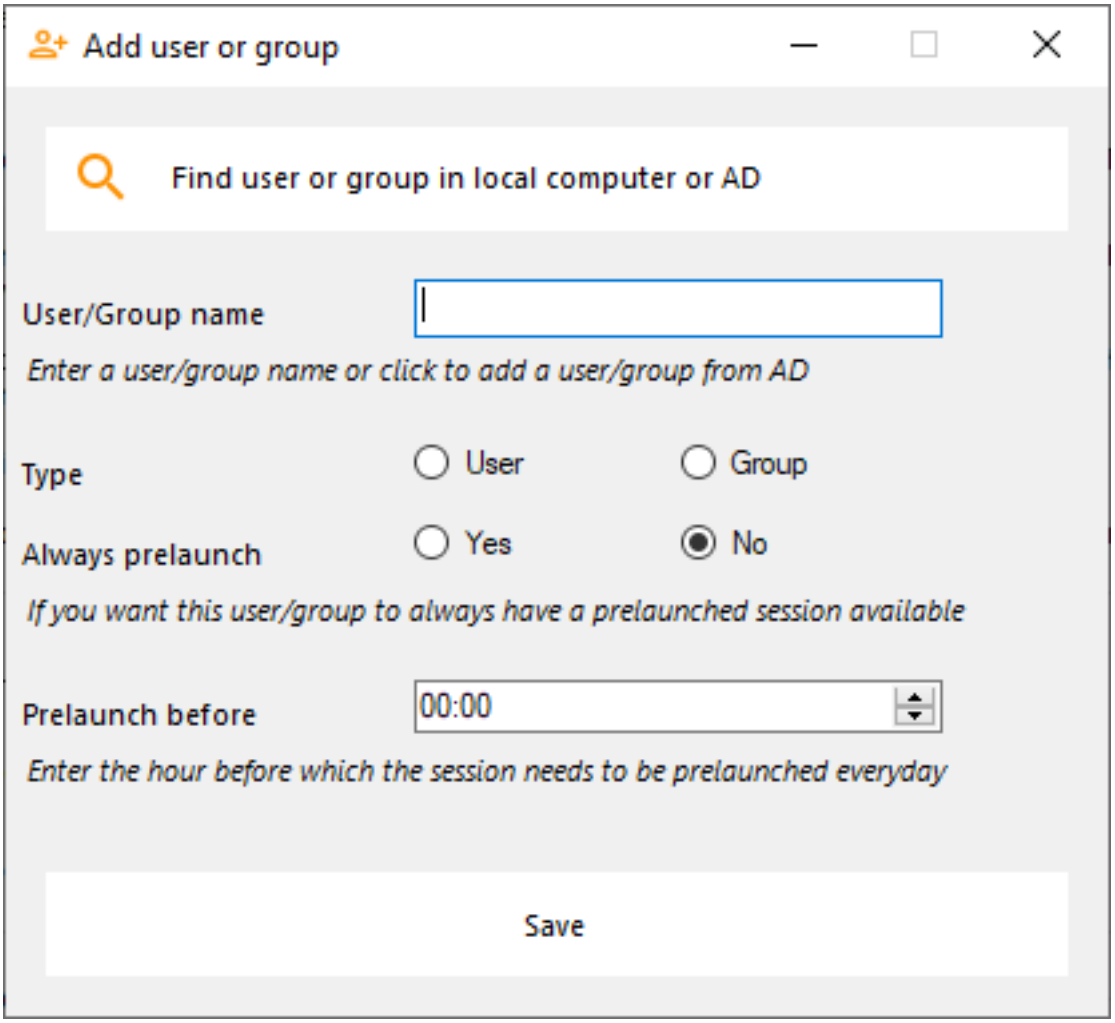
Cliquez sur « Pré-lancement » pour démarrer et charger une nouvelle session pour cet utilisateur.
Attendez qu'il soit complètement chargé, puis cliquez sur « Connecter » pour capturer la session nouvellement chargée.

Gérer les utilisateurs et groupes configurés

Pour ajouter des utilisateurs et des groupes de pré-lancement de session, il suffit de cliquer sur « Ajouter un utilisateur ou un groupe ».
Pour modifier ou supprimer un utilisateur configuré, sélectionnez l'utilisateur/groupe correspondant dans la liste des utilisateurs/groupes configurés, puis cliquez sur « Planifier » pour changer l'heure de « pré-lancement avant », ou sur le bouton « Supprimer » pour retirer l'utilisateur.



Après avoir cliqué sur « Ajouter un utilisateur ou un groupe », vous serez invité à saisir le nom de l'utilisateur/groupe à configurer ainsi que le temps avant lequel la session doit être chargée, appelé « pré-lancement avant » ici.
Vous pouvez également configurer cet utilisateur/groupe pour toujours avoir une session pré-lancée lors de la connexion au lieu de devoir la planifier en sélectionnant « Oui » dans l'option « Toujours pré-lancer ».



Comment configurer le support de proxy inverse Apache pour les Websockets

1. tout d'abord, changez la variable suivante en false www\software\html5\settings.js > W.xhrreverse = false; (si vous ne la changez pas en false, elle essaiera toujours xhr au lieu de websockets, ce que nous ne voulons plus)

2. installer Apache avec le support proxy_wstunnel (les anciennes versions d'Apache sans proxy_wstunnel ne sont pas prises en charge !)

3. autoriser dans la configuration Apache (httpd.conf etc.) les modules suivants. LoadModule proxy_module modules/mod_proxy.so LoadModule proxy_http_module modules/ mod_proxy_http.so LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so

4. supposons que vous souhaitiez accéder au portail principal html5 via le sous-dossier “/html5/” Par exemple http://your_ip_or_domain.net/html5/ Et Tsplus est installé dans l'intranet sur le serveur “intranetxyz” puis ajoutez à la configuration (httpd.conf etc.) ce qui suit

   ProxyPass /html5 http://intranetxyz:80 ProxyPassReverse /html5 http://intranetxyz:80

   ProxyPass “ws://intranetxyz:80/socket.io/websocket_https”

   ProxyPass “ws://intranetxyz:80/socket.io/websocket”

   ProxyPass “ws://intranetxyz:80/socket.io/flashsocket_https”

   ProxyPass “ws://intranetxyz:80/socket.io/flashsocket”

5. Redémarrez Apache pour que les modifications prennent effet.

Authentification à deux facteurs

L'authentification à deux facteurs ajoute une couche de sécurité supplémentaire et **empêche l'accès à la session de vos utilisateurs même si quelqu'un connaît leur mot de passe** .

Une combinaison de deux facteurs différents est utilisée pour atteindre un niveau de sécurité supérieur :

1. quelque chose qu'ils connaissent, **un mot de passe** .

2. quelque chose qu'ils ont, un **appareil - tel qu'un smartphone - avec une application d'authentification installée.** .

Vous pouvez utiliser l'une des applications d'authentification suivantes pour continuer. Ces applications sont disponibles sur une large gamme de plateformes :

- Authy
- Google Authenticator
- Microsoft Authenticator

Chaque fois qu'un utilisateur se connecte à sa session distante, il aura besoin de son mot de passe et d'un code de vérification disponible sur son téléphone mobile. Une fois configurée, l'application d'authentification affichera un code de vérification pour lui permettre de se connecter à tout moment. Cela fonctionne même si son appareil est hors ligne.

OU vous pouvez choisir de recevoir des codes de vérification par **SMS** Dans ce cas, vous devrez créer un compte gratuit sur Twilio .

Le **Les codes 2FA générés sont TOTP** (mot de passe à usage unique basé sur le temps), et donc sont à usage unique.

Par conséquent, il n'est pas possible de réutiliser un code 2FA qui a déjà été utilisé. Cela empêche le vol et ensuite l'utilisation d'un code 2FA en observant l'utilisateur pendant qu'il saisit son code.

Exigences

L'authentification à deux facteurs nécessite TSplus Remote Access **Web mobile** ou **Entreprise** Éditions.

L'authentification à deux facteurs est prise en charge par :

- TSplus Remote Access **Portail web** , pour les connexions HTML5 et Remoteapp
- TSplus Connection Client, pour les clients générés depuis la version 15.30.3.15, avec le support 2FA explicitement activé. Voir Support du générateur de client portable pour l'authentification à deux facteurs
- 2FA est lié aux utilisateurs de Windows et non aux identifiants Web.

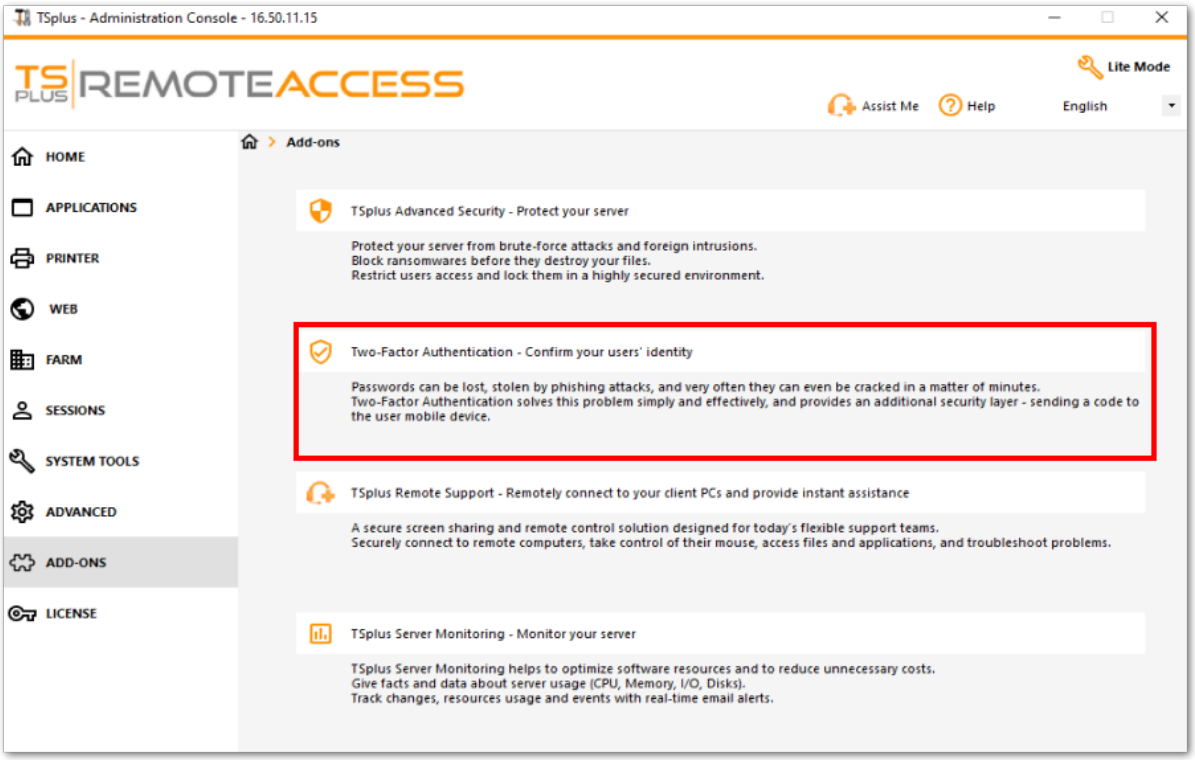
Ce mode d'authentification ne prend pas en charge la connexion via le client Microsoft Remote Desktop standard (mstsc.exe).

Afin de fournir une solution encore plus sûre, les connexions RDP sont refusées pour les utilisateurs ayant 2FA activé.

En tant que prérequis, le serveur TSplus et les appareils doivent être à l'heure. Voir le Synchronisation du temps et Paramètres sections pour plus d'informations sur la configuration.

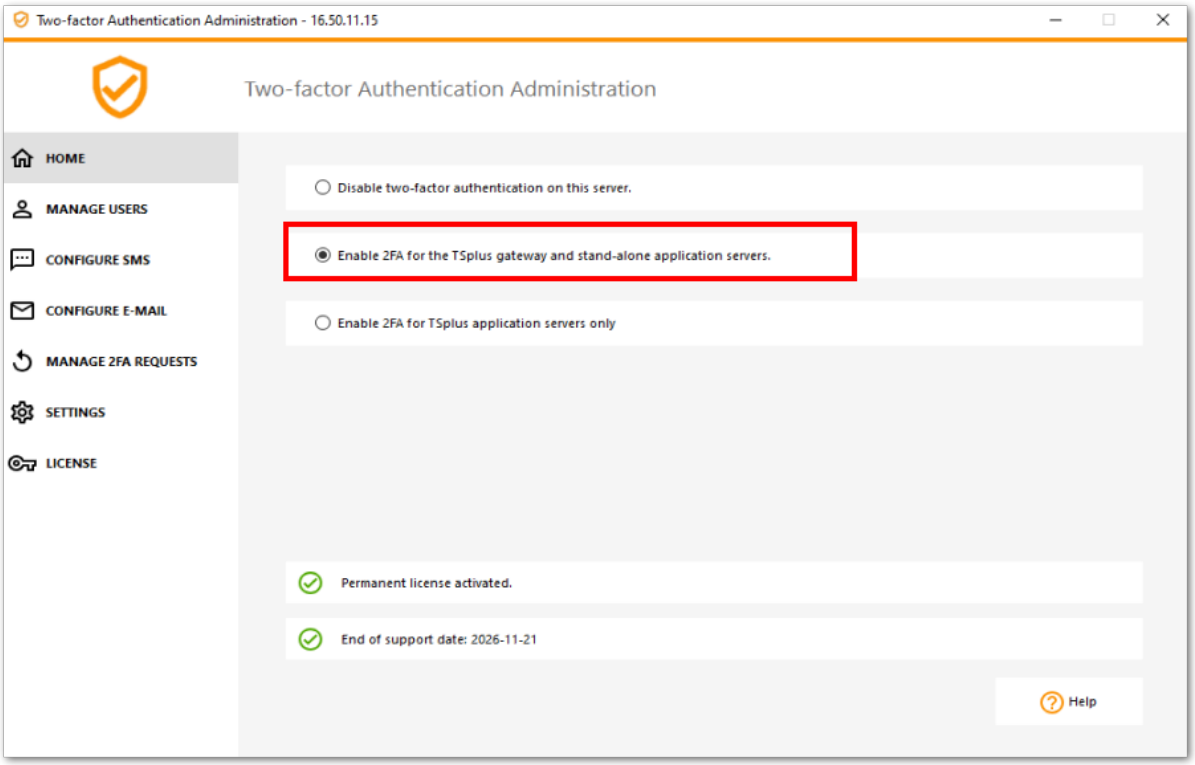
Activation de la licence de l'add-on d'authentification à deux facteurs

La fonctionnalité d'authentification à deux facteurs se trouve dans l'onglet Add-On de l'AdminTool :



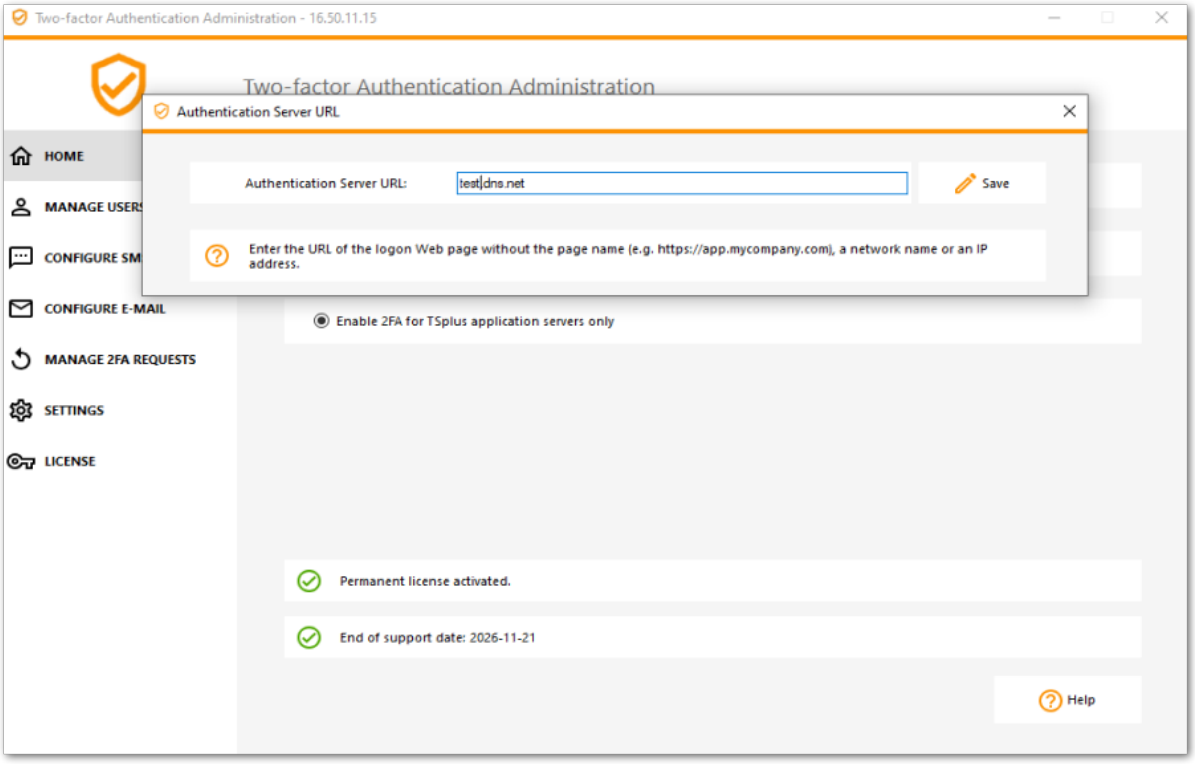
Effectuez les étapes suivantes pour activer l'authentification à deux facteurs pour votre serveur ou déploiement TSplus. Si votre déploiement TSplus est configuré pour utiliser plusieurs serveurs, effectuez cette tâche sur le serveur TSplus exposé comme le point d'entrée unique pour les utilisateurs ou ayant le rôle de proxy inverse.

1. Ouvrez l'application d'administration de l'authentification à deux facteurs. L'état de l'authentification à deux facteurs et l'état de la licence sont affichés :

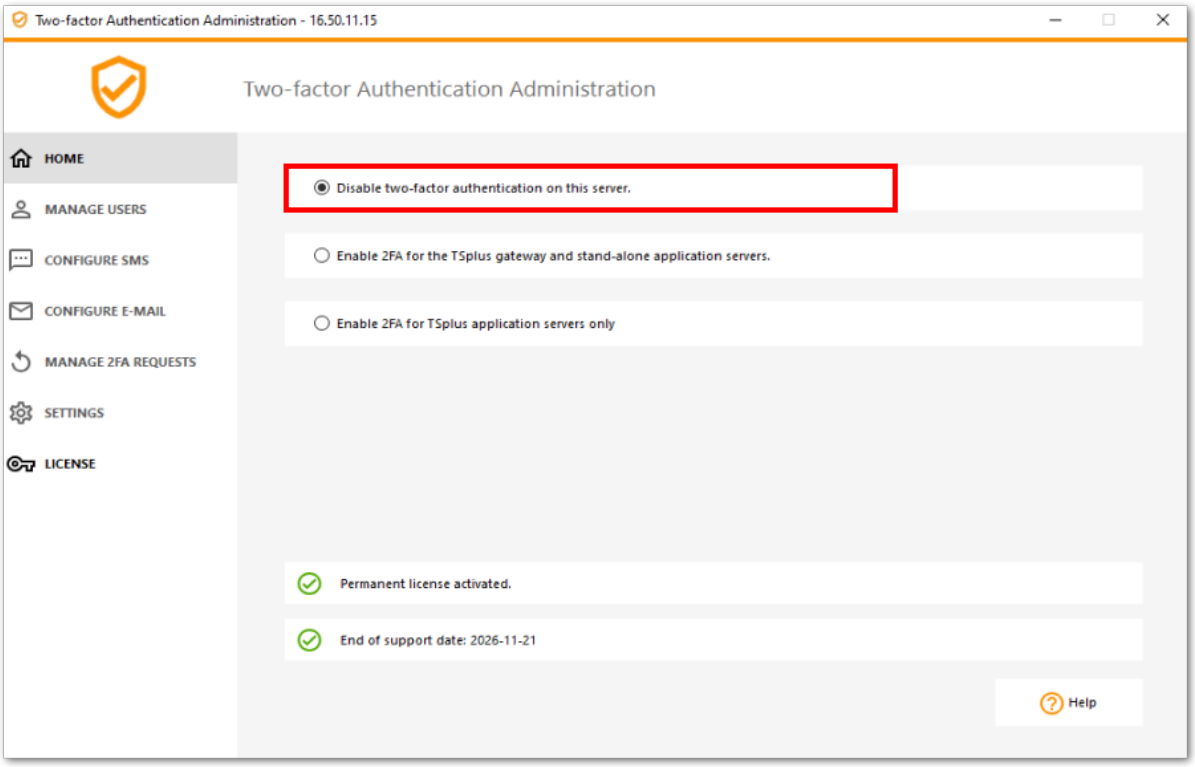


Par défaut, 2FA est activé pour le portail TSplus et les serveurs d'applications autonomes.

Vous pouvez l'activer uniquement pour les serveurs d'applications TSplus en saisissant l'URL du serveur d'authentification :



Ou désactivez-le :

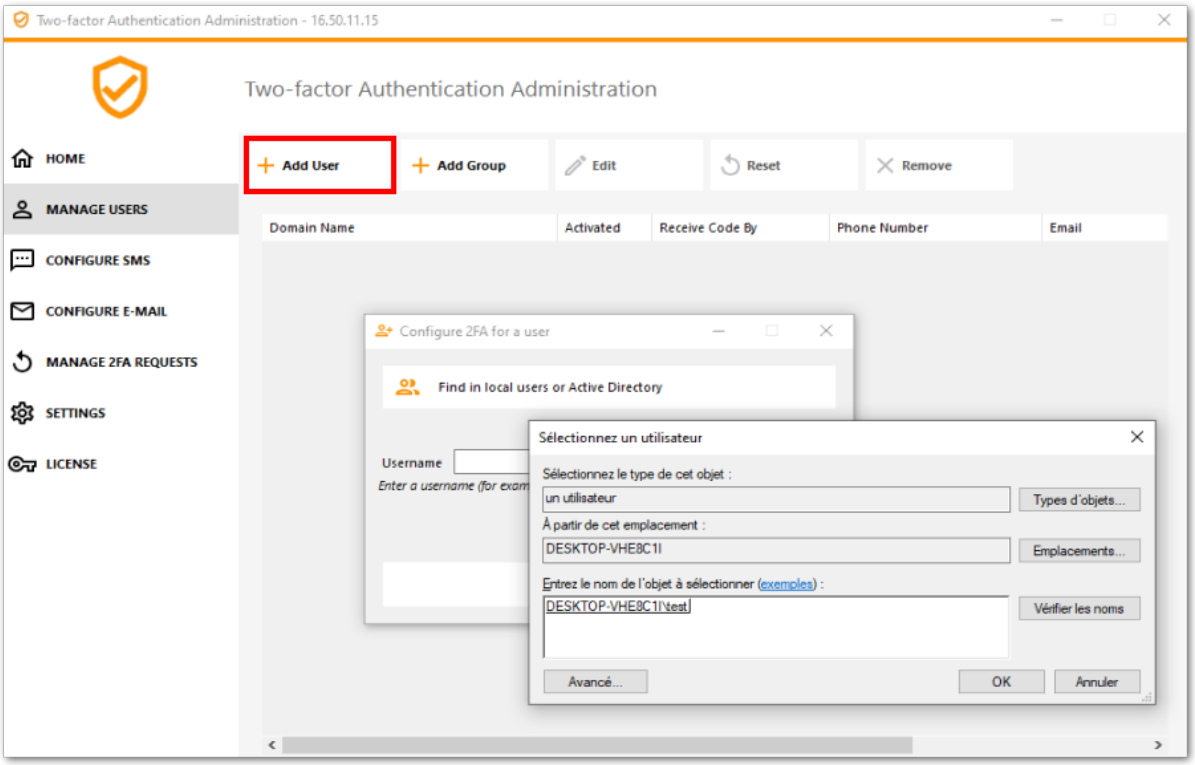


Ajouter des utilisateurs et des groupes

Une fois que l'authentification à deux facteurs est activée, vous pouvez configurer les utilisateurs pour l'authentification à deux facteurs.

1. Depuis l'application d'administration de l'authentification à deux facteurs, cliquez sur le Gérer les utilisateurs tab.

2. Ensuite, cliquez sur Ajouter pour sélectionner des utilisateurs et/ou des groupes d'utilisateurs. Le Sélectionner des utilisateurs ou des groupes la boîte s'ouvre.



3. Ajoutez autant d'utilisateurs et de groupes que nécessaire, puis cliquez. OK Les utilisateurs et les groupes sont ajoutés à la liste et activés pour l'authentification à deux facteurs.

Voici des commandes pour ajouter des utilisateurs/groupes
3 types of possible arguments :

juste le nom de domaine
TwoFactor.Admin.exe /addusers nomDeDomaine1

- ajoute l'utilisateur avec les valeurs par défaut (méthode de réception = application, champs email et téléphone non renseignés)

le nom de domaine et la méthode de réception
TwoFactor.Admin.exe /addusers domainName1;SMS

- ajoute l'utilisateur avec la méthode de réception souhaitée, mais n'essaie pas de l'activer

le nom de domaine, la méthode de réception, le champ Téléphone (même s'il est vide), le champ Email (même s'il est vide)
*TwoFactor.Admin.exe /addusers domainName1;SMS;+33606060606; username1@truc.net nomDeDomaine2;Email;; username2@truc.net domainName3;SMS; +33606060607;domainName4

- Même comportement que dans l'HMI, lorsque nous ajoutons un utilisateur, puis que nous le modifions avec les informations correctes : nous essayons d'activer l'utilisateur.

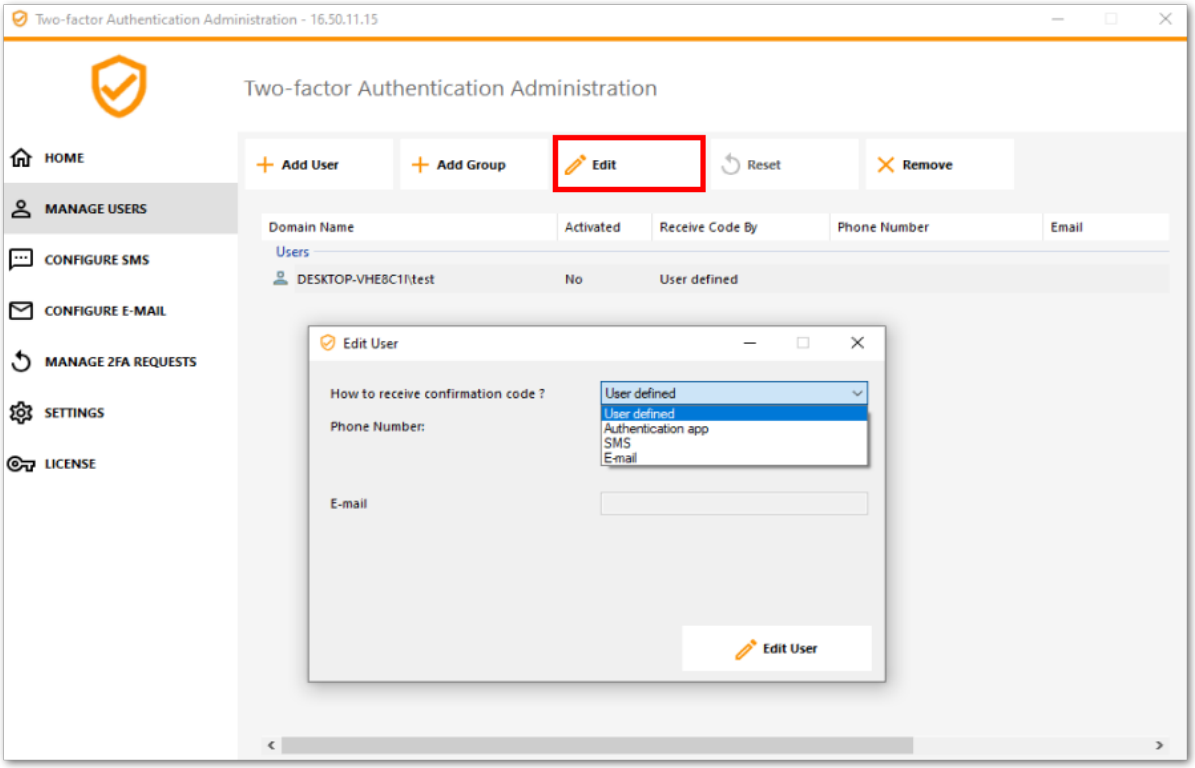
Comme indiqué dans le dernier exemple, plusieurs utilisateurs peuvent être indiqués (séparés

par un espace). Les différents champs d'un utilisateur sont séparés par un point-virgule.

Pour des groupes uniques :
TwoFactor.Admin.exe /addgroups groupe1 groupe2 groupe3

Modifier les utilisateurs

Sur le même carreau, vous pouvez modifier la façon dont les utilisateurs reçoivent les codes de vérification en sélectionnant un utilisateur et en cliquant sur le bouton « Modifier » :

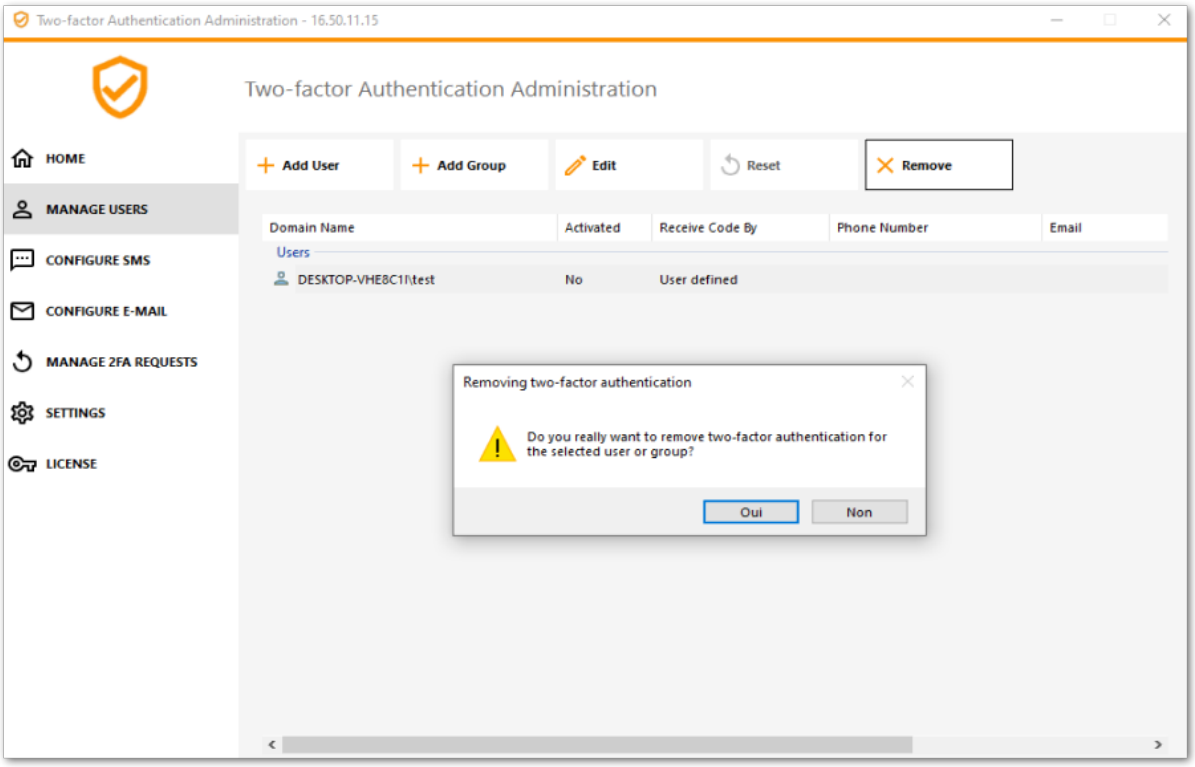


L'utilisateur reçoit des codes de vérification sur l'application d'authentification par défaut. Vous pouvez choisir qu'il/elle les reçoive par SMS ou EMAIL en sélectionnant l'option.

Sélectionné SMS et ajouté le numéro de téléphone de l'utilisateur dans le champ ou sélectionné EMAIL et ajouté l'email de l'utilisateur.

Supprimer les utilisateurs et les groupes

Pour supprimer des utilisateurs ou des groupes, sélectionnez l'utilisateur ou le groupe, puis cliquez sur Supprimer Un message de confirmation s'affiche.



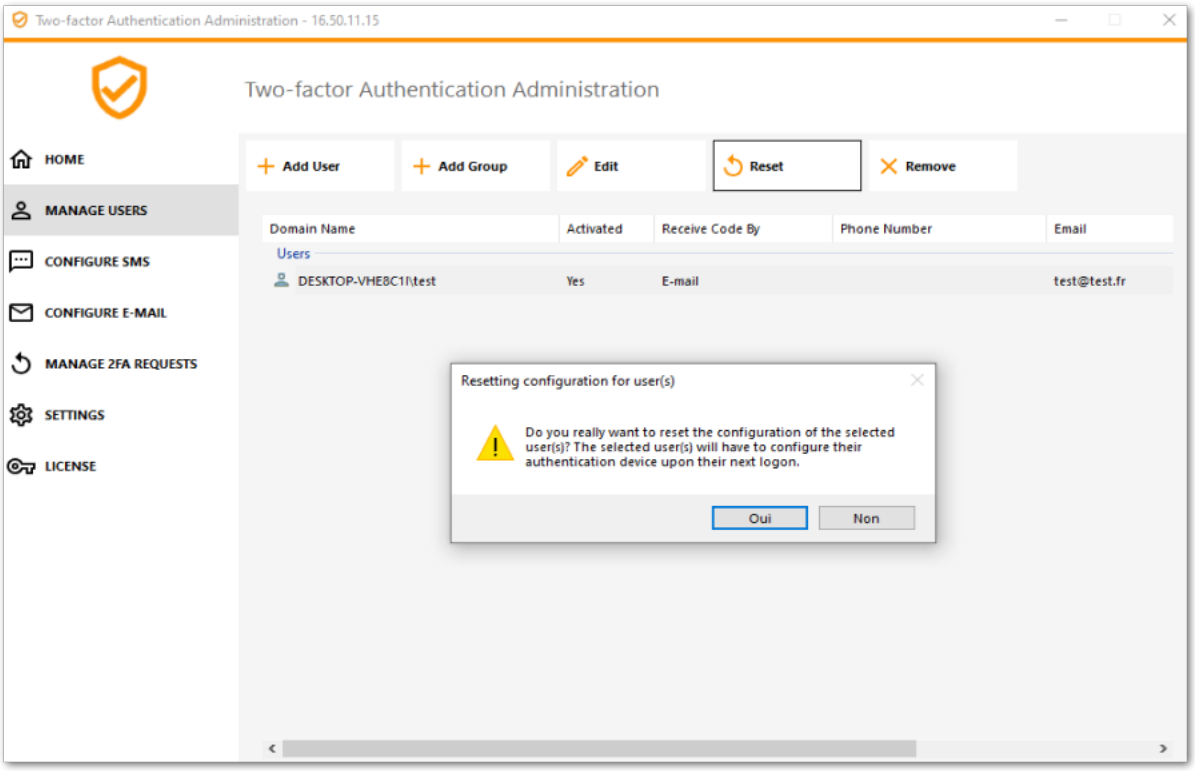
Cliquez Oui L'utilisateur ou le groupe est retiré de sa liste et ne pourra plus se connecter en utilisant l'authentification à deux facteurs.

Réinitialiser la configuration pour les utilisateurs

En cas de perte de l'appareil d'authentification d'un utilisateur, ou si l'utilisateur doit afficher à nouveau le code QR secret, vous devez réinitialiser les paramètres d'authentification de l'utilisateur.

1. Depuis l'application d'administration de l'authentification à deux facteurs, cliquez sur le Gérer les utilisateurs tab.

2. Sélectionnez un ou plusieurs utilisateurs activés, puis cliquez sur Réinitialiser Un message de confirmation s'affiche :



3. Cliquez Oui Les utilisateurs sélectionnés se verront présenter un nouveau code QR lors de la prochaine connexion et devront le scanner dans l'application d'authentification de leur appareil.

Vous pouvez également modifier le numéro de téléphone de l'utilisateur, afin qu'il puisse recevoir un code de vérification sur son nouvel appareil.

Inscrire l'utilisateur pour l'authentification à deux facteurs

Une fois qu'un utilisateur a été activé pour utiliser l'authentification à deux facteurs, un message d'activation sera affiché lors de sa prochaine connexion réussie depuis le portail Web TSplus.



Pour compléter les étapes requises, vous avez deux choix : soit générer des codes via une application d'authentification, soit faire en sorte que l'utilisateur reçoive des codes par SMS.

Recevez des codes avec une application d'authentification

L'utilisateur doit installer une application d'authentification sur un appareil portable, tel que son smartphone.

Vous pouvez utiliser l'une des applications d'authentification suivantes pour continuer. Ces applications sont disponibles sur une large gamme de plateformes :

- Authy
- Google Authenticator

- Microsoft Authenticator

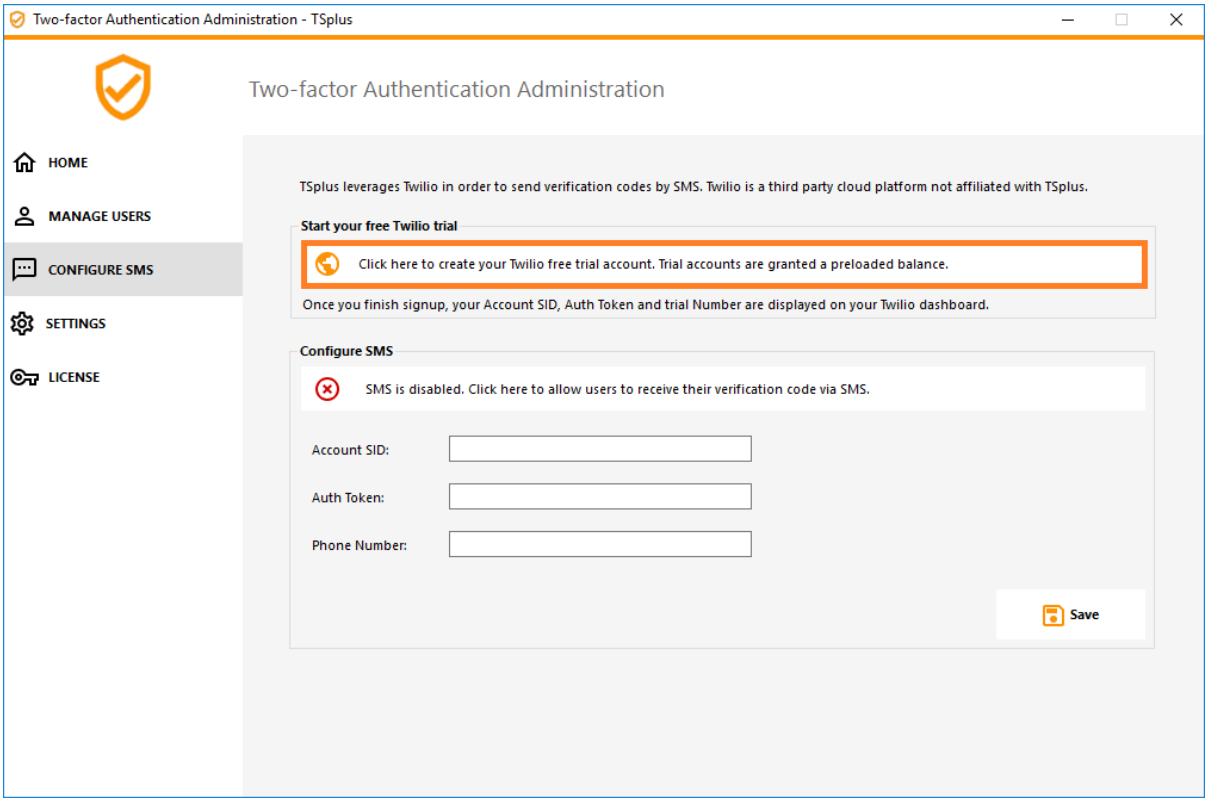
Veuillez consulter la documentation de chaque application pour plus de détails sur la façon de procéder pour ajouter votre compte TSplus.

Configurer SMS

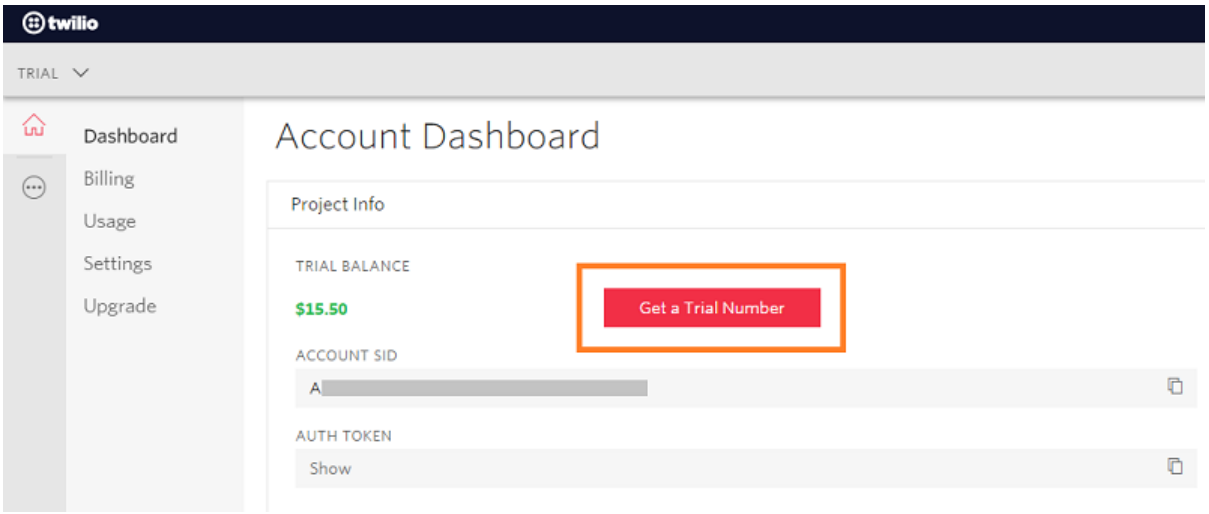
Pour que l'utilisateur reçoive des codes de vérification par SMS, vous devez d'abord l'activer. Cliquez sur le Configurer SMS onglet :

TSplus utilise Twilio pour envoyer des codes de vérification par SMS. Twilio est une plateforme cloud tierce, non affiliée à TSplus.

1. Créez simplement un compte gratuit sur Twilio en cliquant sur le bouton ci-dessous « Commencez votre essai gratuit avec Twilio » :

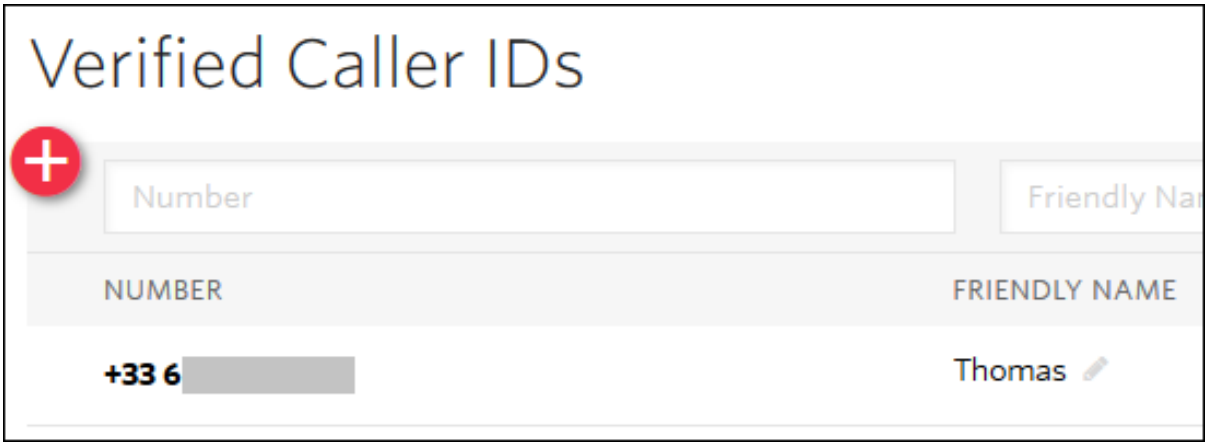


2. Sur votre Tableau de bord du compte Twilio vous devrez activer votre numéro d'essai :

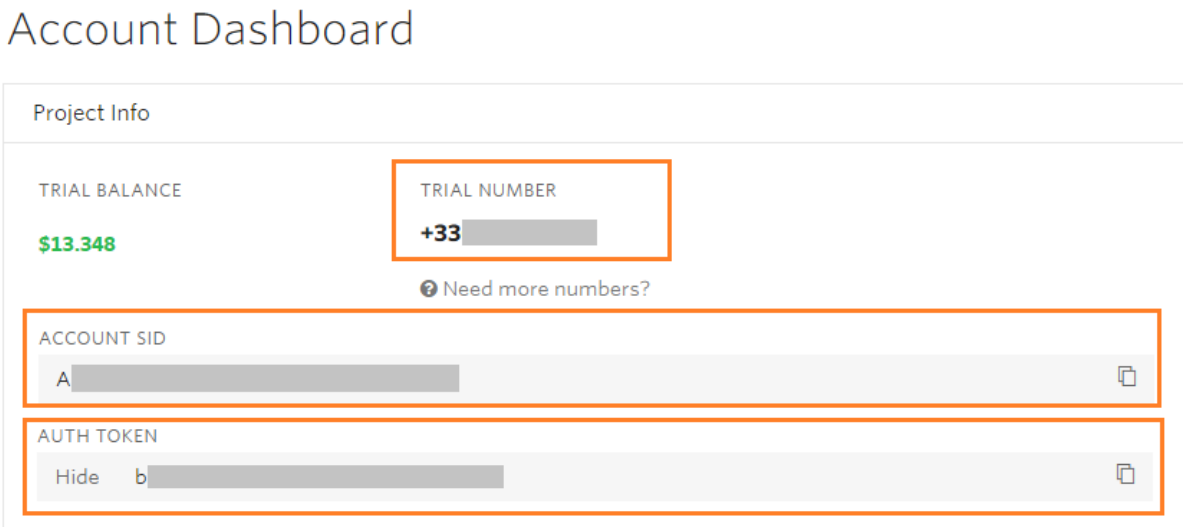


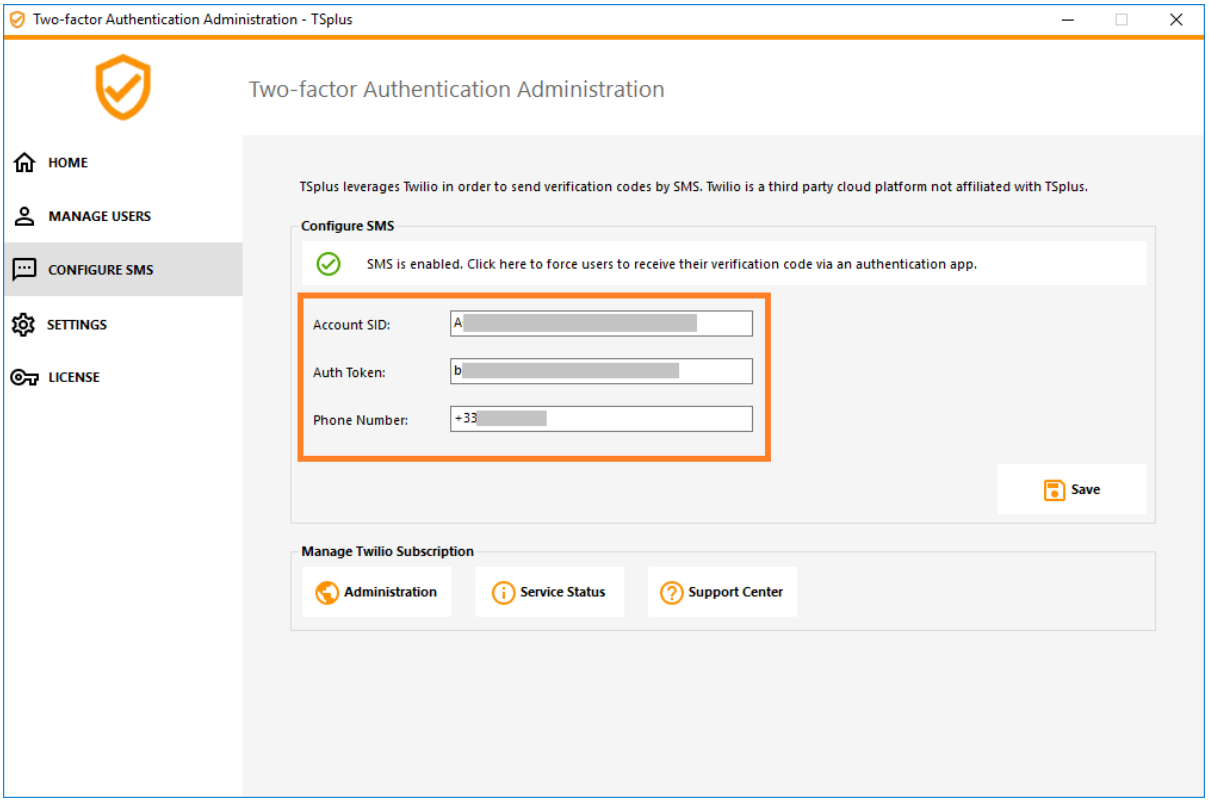
3. L'étape suivante n'est nécessaire que pour les versions d'essai. Elle permet à Twilio de vérifier le numéro de téléphone réel sur lequel les SMS seront envoyés.

Entrez ce numéro sous le menu “Numéros de téléphone” - “Identifiants d'appelants vérifiés” onglet :

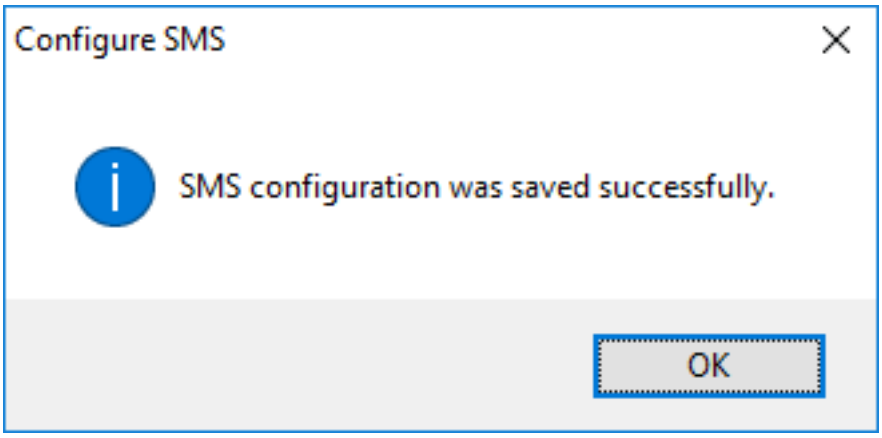


4. Vous pourrez alors entrer votre SID de compte, votre jeton d'authentification et **Numéro d'essai** comme le numéro de téléphone sur le Configurer SMS onglet de TSplus :





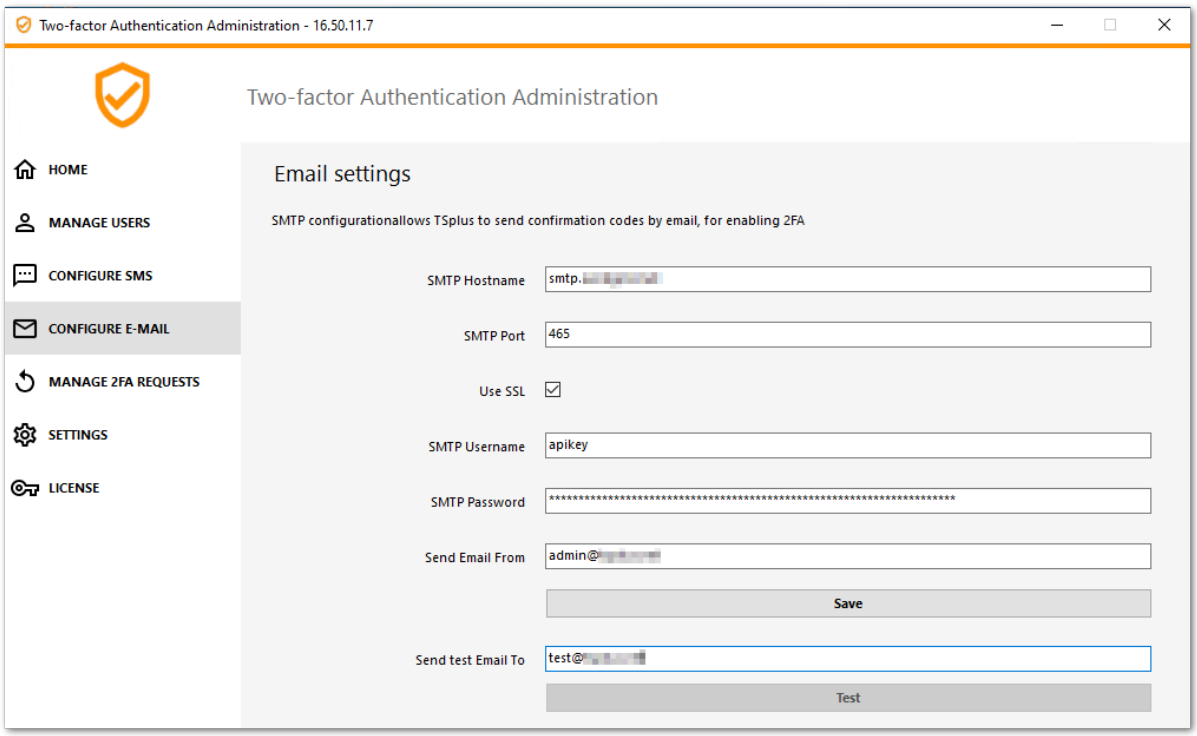
Ensuite, cliquez sur Enregistrer. Le message suivant s'affichera :



Vous pouvez gérer votre abonnement Twilio sur le Gérer l'abonnement Twilio section, en bas de la Configurer SMS Gérez votre compte, consultez l'état du service ou contactez le centre de support Twilio en cliquant simplement sur les boutons correspondants.

Configurer EMAIL

Pour que l'utilisateur reçoive des codes de vérification par EMAIL, vous devez d'abord configurer votre email SMTP.



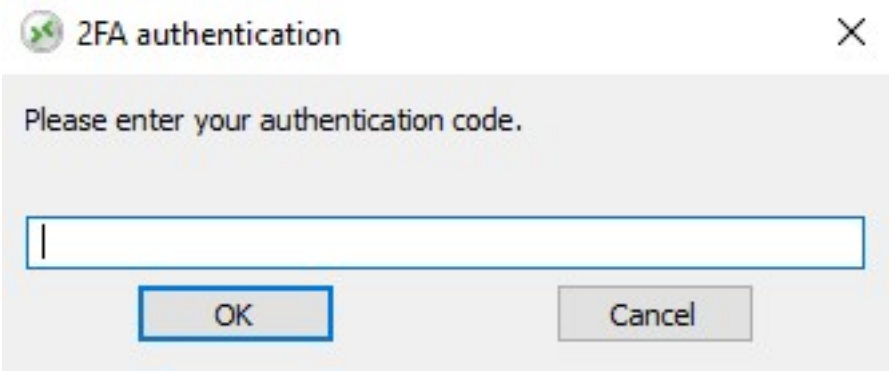
Se connecter en utilisant l'authentification à deux facteurs

Une fois qu'un utilisateur a configuré son compte TSplus dans son application d'authentification, il ou elle pourra se connecter en utilisant son mot de passe et le code fourni par son application d'authentification, par SMS ou par e-mail.

Depuis le portail Web de TSplus Remote Access :



Depuis le client généré par TSplus :



Les serveurs d'application TSplus et les dispositifs clients doivent partager le même temps. Cela signifie que l'heure et la date du serveur doivent être synchronisées avec un serveur de temps. Les dispositifs clients doivent également avoir une synchronisation horaire, quel que soit le fuseau horaire dans lequel ils sont configurés.

Si une demande d'authentification provient d'un appareil dont la date et l'heure ne sont pas synchronisées, ou si la date et l'heure du serveur ne sont pas synchronisées, cette demande peut être rejetée.

La validation des informations entre l'appareil et le serveur concerne l'heure UTC.

Dans le **Paramètres** section, le paramètre de Discrepency est utilisé pour gérer la période de validité du code, par intervalles de 30 secondes.

Exemple de validation ou d'authentification valide :

- le serveur est synchronisé avec un serveur de temps, le fuseau horaire est UTC + 2, il est 14h30
- l'appareil est synchronisé avec un serveur de temps, le fuseau horaire est UTC + 1, il est 13h30
- le paramètre de Discrepency est configuré à 60, c'est-à-dire une période de validité du code de 30 minutes
- en référence à l'heure UTC, l'heure de l'appareil et l'heure du serveur sont identiques.

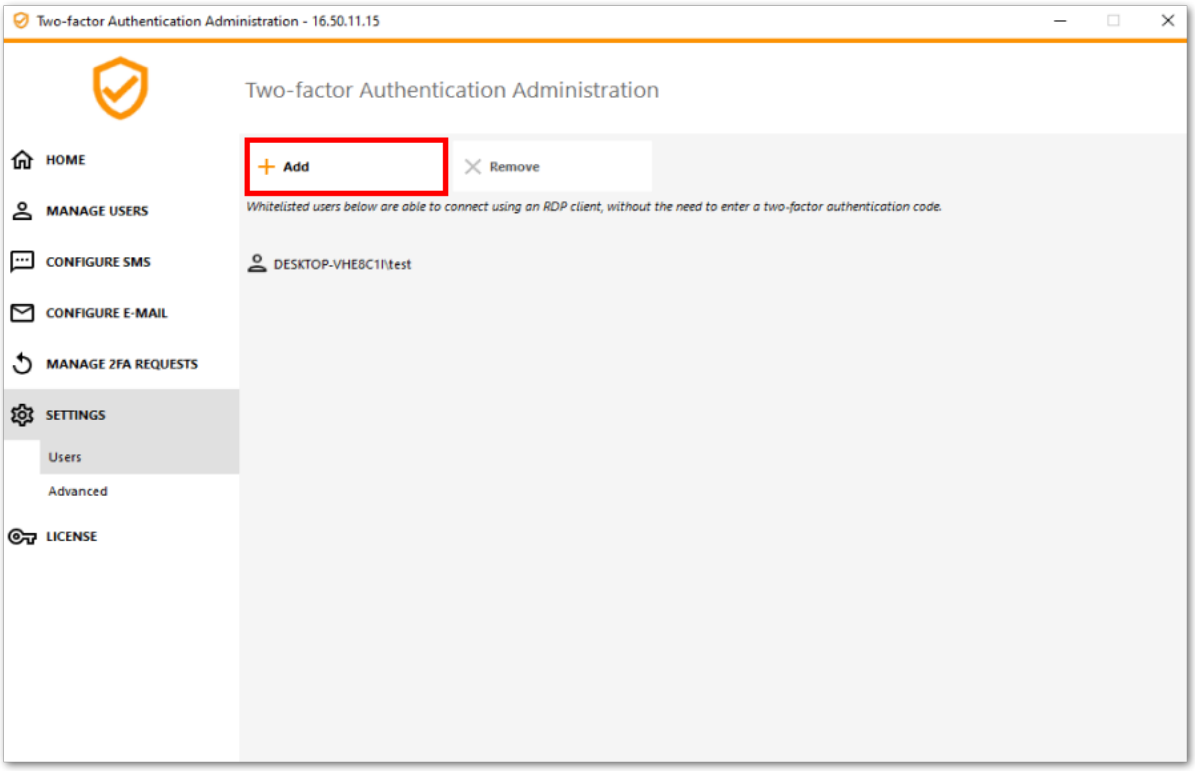
Exemple de validation ou d'authentification invalide :

- le serveur est synchronisé avec un serveur de temps, le fuseau horaire est UTC + 2, il est 14h30
- l'appareil n'est pas synchronisé avec un serveur de temps, le fuseau horaire est UTC-1, l'heure est réglée manuellement à 13h30
- le paramètre de Discrepency est configuré à 60, c'est-à-dire une période de validité du code de 30 minutes
- l'heure du serveur référencée à l'heure UTC est 00:30
- le temps communiqué par le Dispositif, appelé heure UTC, est 14h30
- la différence est de 120 minutes, le code de validation est donc refusé.

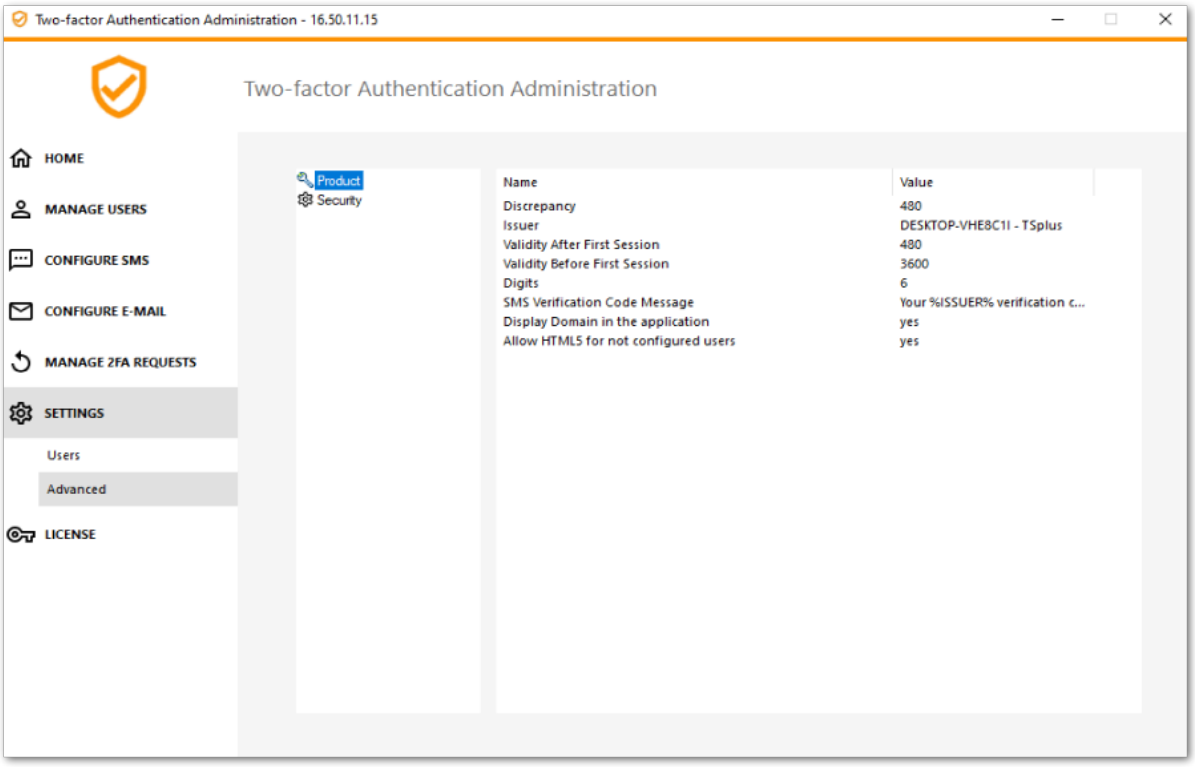
Paramètres

L'onglet Paramètres vous permet de **autoriser les utilisateurs, afin qu'ils puissent se connecter en utilisant un client RDP, sans avoir besoin de saisir un code d'authentification à deux facteurs.**

Cliquez sur le bouton « Ajouter » pour ajouter un utilisateur et supprimez un utilisateur en le sélectionnant et en cliquant sur le bouton « Supprimer ».



L'onglet Avancé vous permet de configurer les paramètres détaillés de l'authentification à deux facteurs.

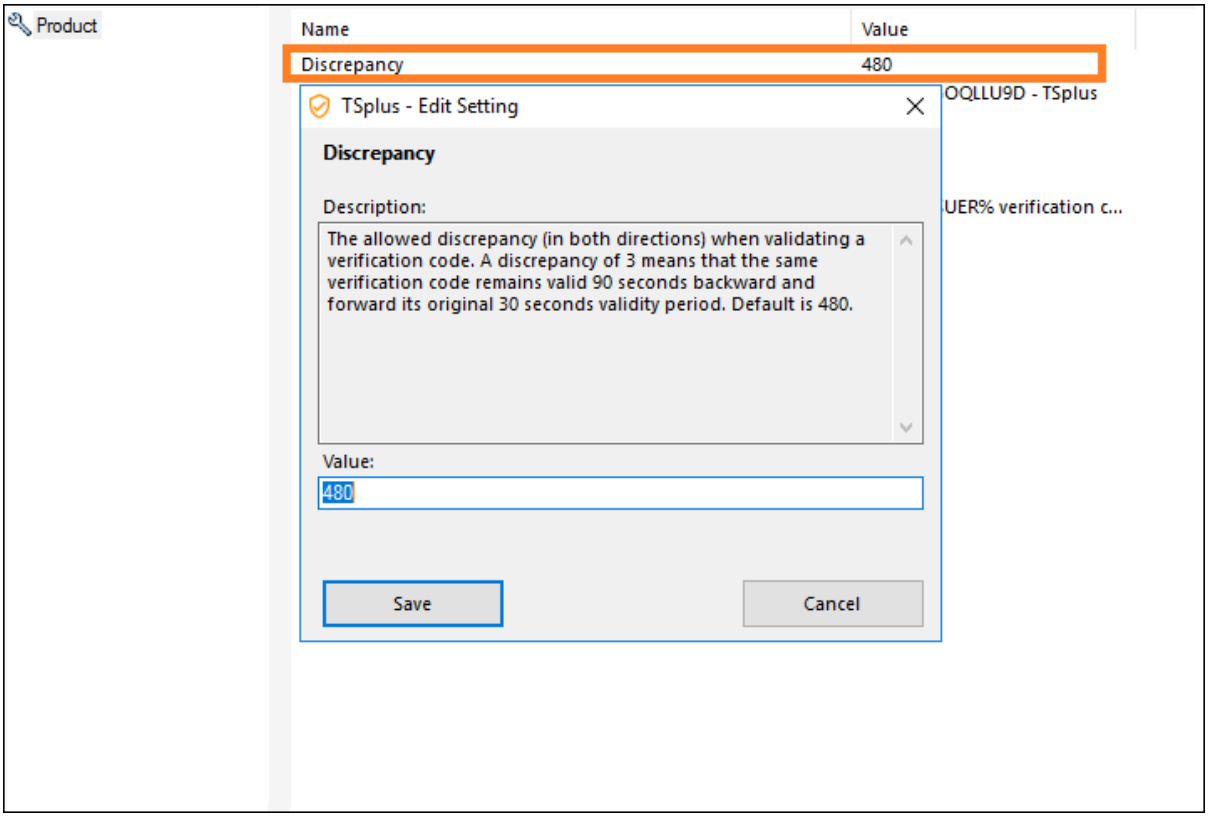


Discrepance

Vous pouvez modifier la valeur de Discrepancy, ce qui vous permet de définir le temps de

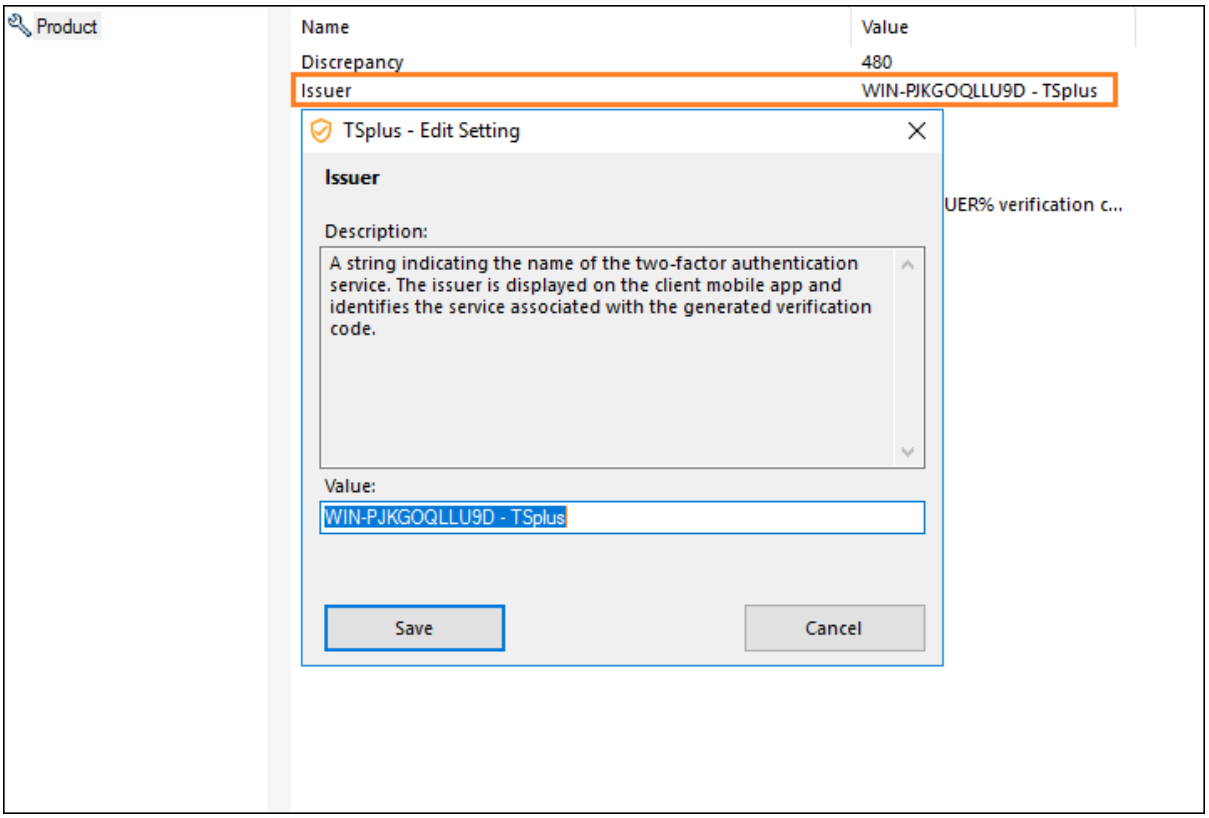
validation d'un code de vérification.

Une différence de 3 signifie que le même code de vérification reste valide 90 secondes en arrière et en avant de sa période de validité originale de 30 secondes. Par défaut, c'est 480, ce qui signifie 480 x 30 secondes = 4 heures.



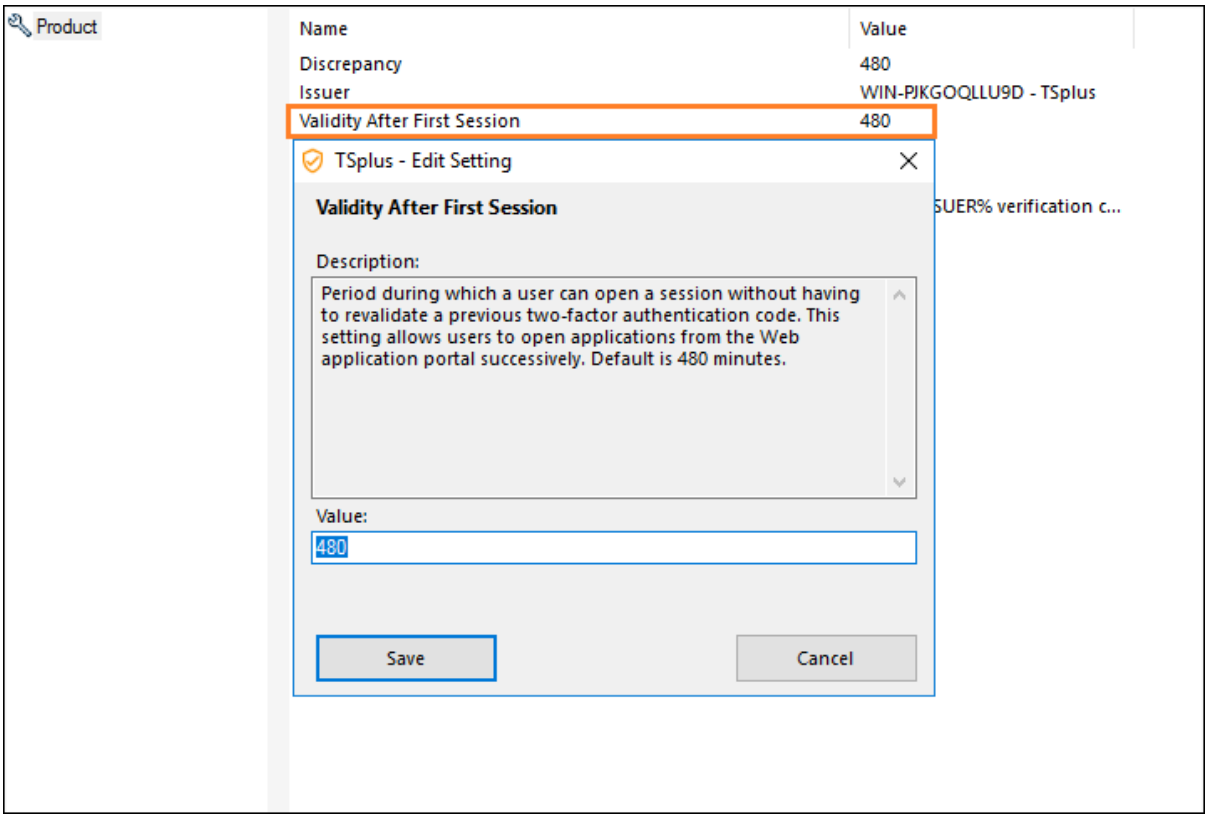
Émetteur

Une chaîne indiquant le nom du service d'authentification à deux facteurs. L'émetteur est affiché sur l'application mobile du client et identifie le service associé au code de vérification généré. Par défaut, il est composé du nom du serveur avec TSplus.



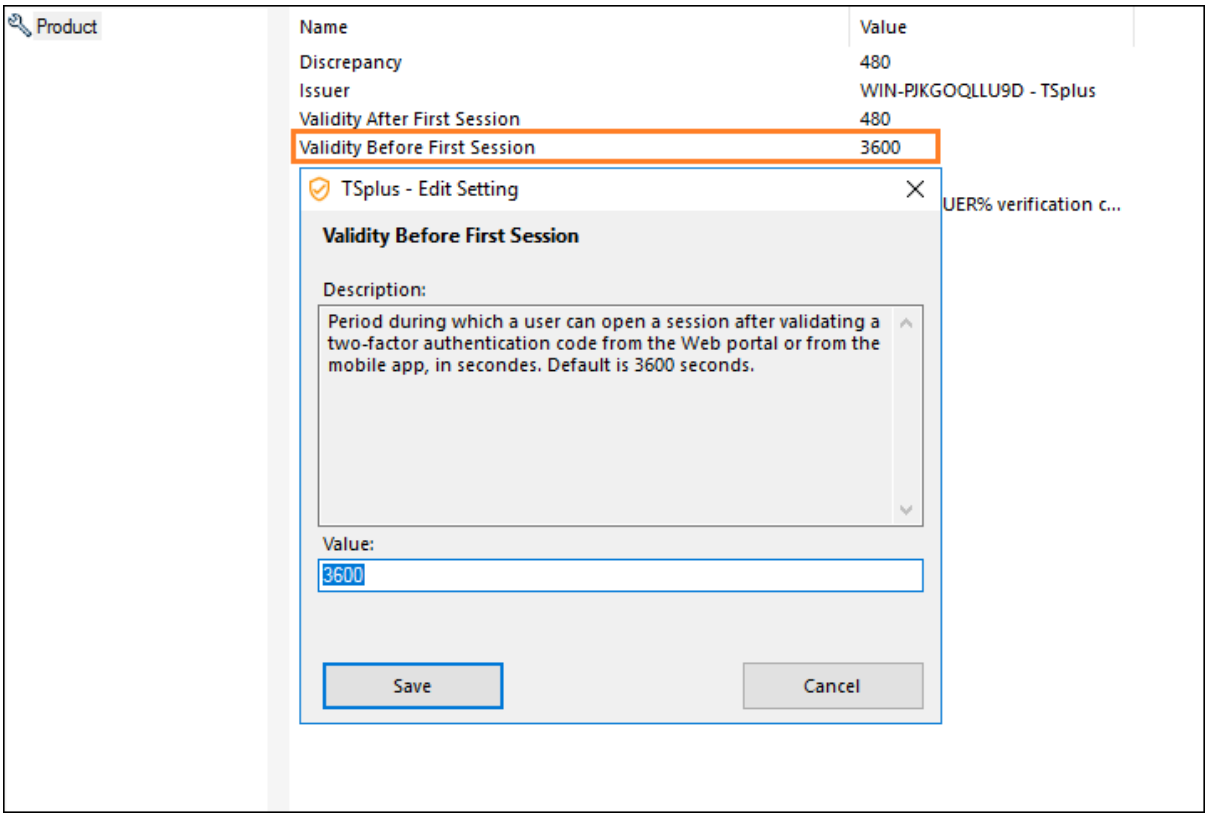
Validité après la première session

Période pendant laquelle un utilisateur peut ouvrir une session sans avoir à revalider un code d'authentification à deux facteurs précédent. Ce paramètre permet aux utilisateurs d'ouvrir des applications depuis le portail d'application Web successivement. La valeur par défaut est de 480 minutes.



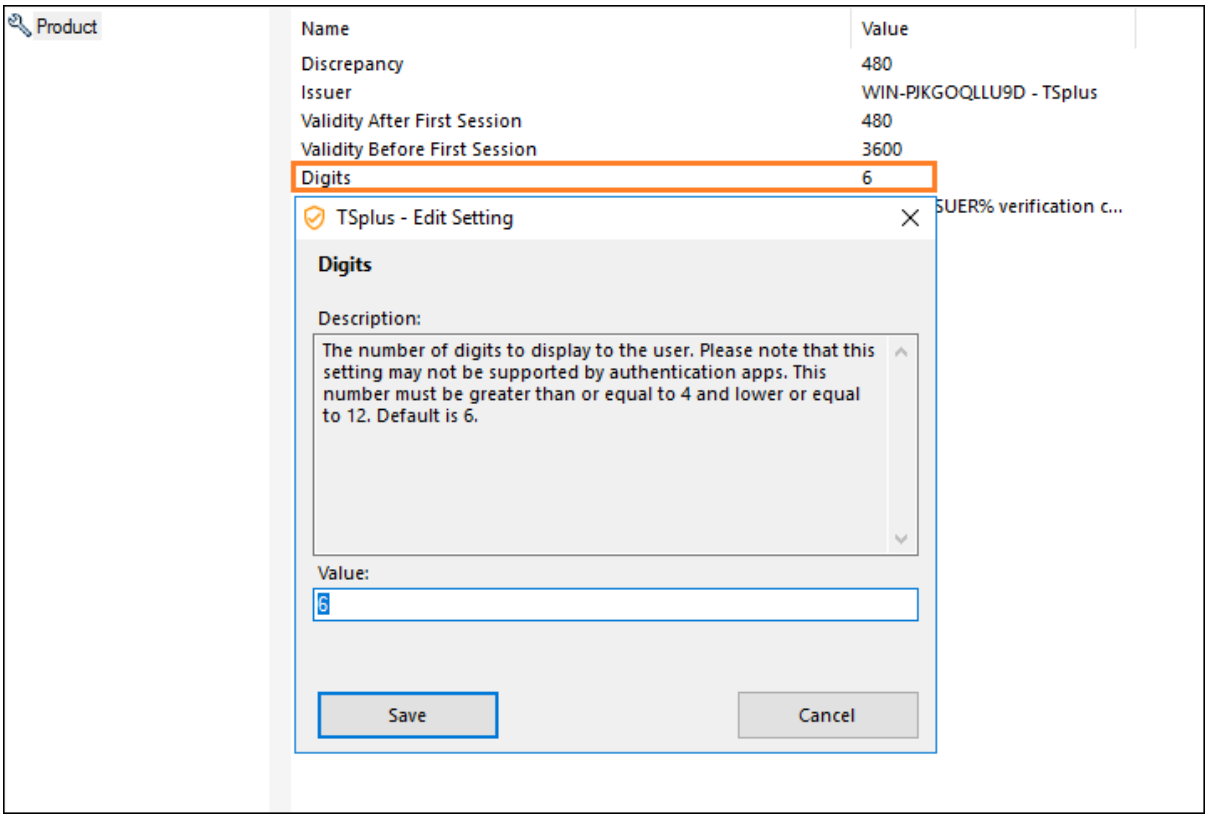
Validité avant la première session

Période pendant laquelle un utilisateur peut ouvrir une session après avoir validé un code d'authentification à deux facteurs depuis le portail Web ou depuis l'application mobile, en secondes. La valeur par défaut est de 3600 secondes.



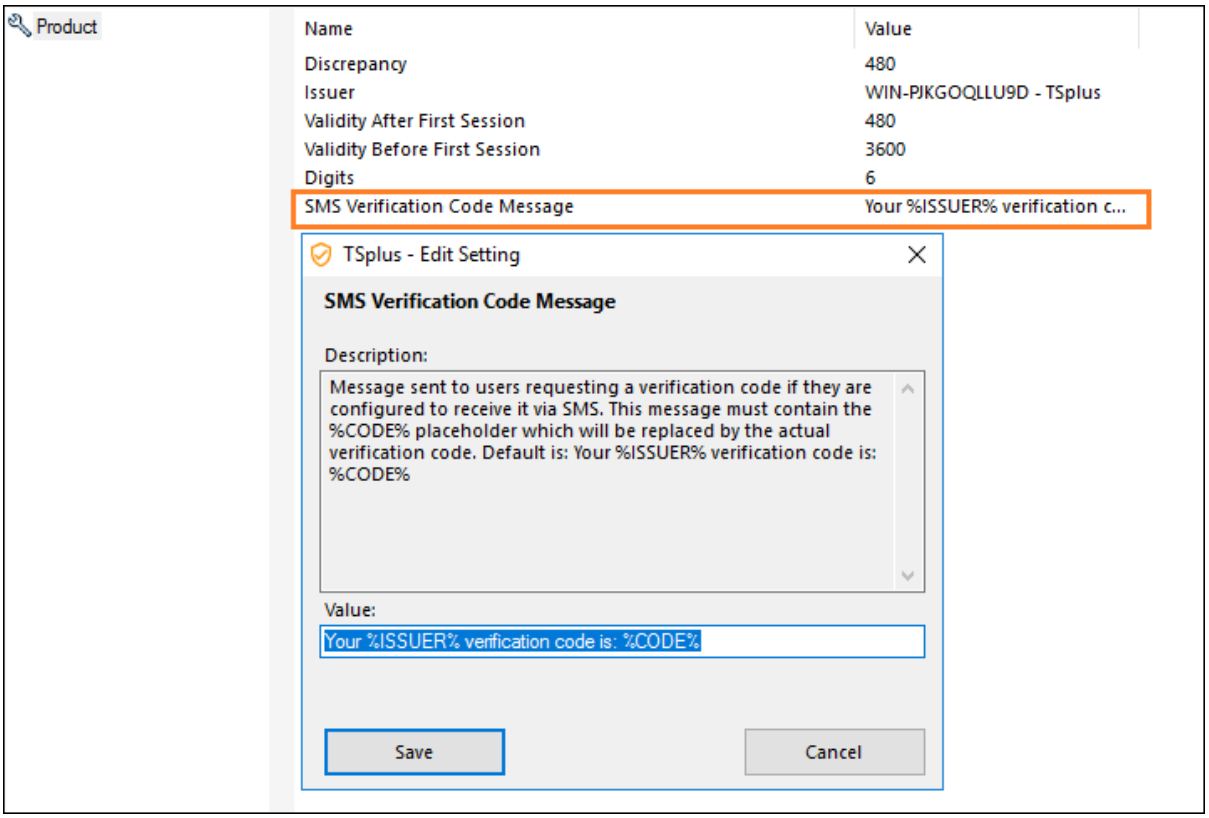
Chiffres

Le nombre de chiffres à afficher à l'utilisateur. Veuillez noter que ce paramètre peut ne pas être pris en charge par les applications d'authentification. Ce nombre doit être supérieur ou égal à 4 et inférieur ou égal à 12. La valeur par défaut est 6.



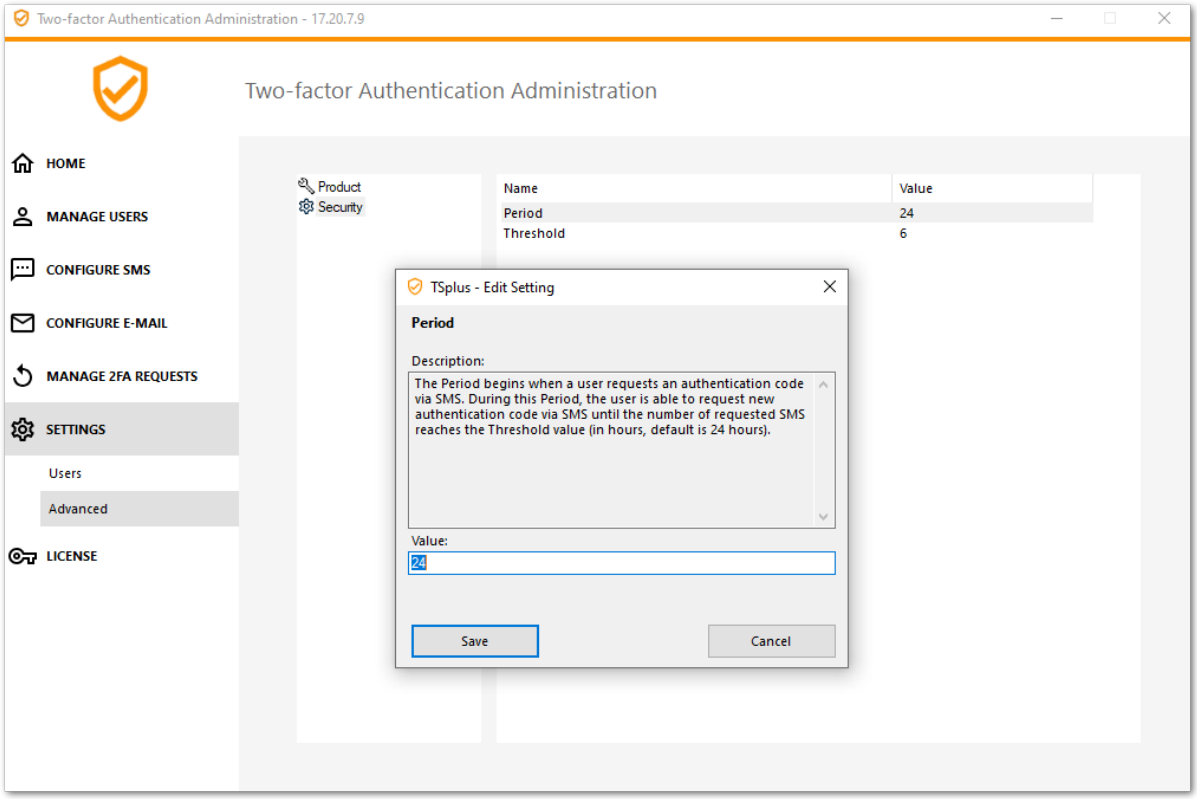
Message de code de vérification par SMS

Message envoyé aux utilisateurs demandant un code de vérification s'ils sont configurés pour le recevoir par SMS. Ce message doit contenir le placeholder %CODE% qui sera remplacé par le code de vérification réel. Par défaut : Votre code de vérification %ISSUER% est : %CODE%



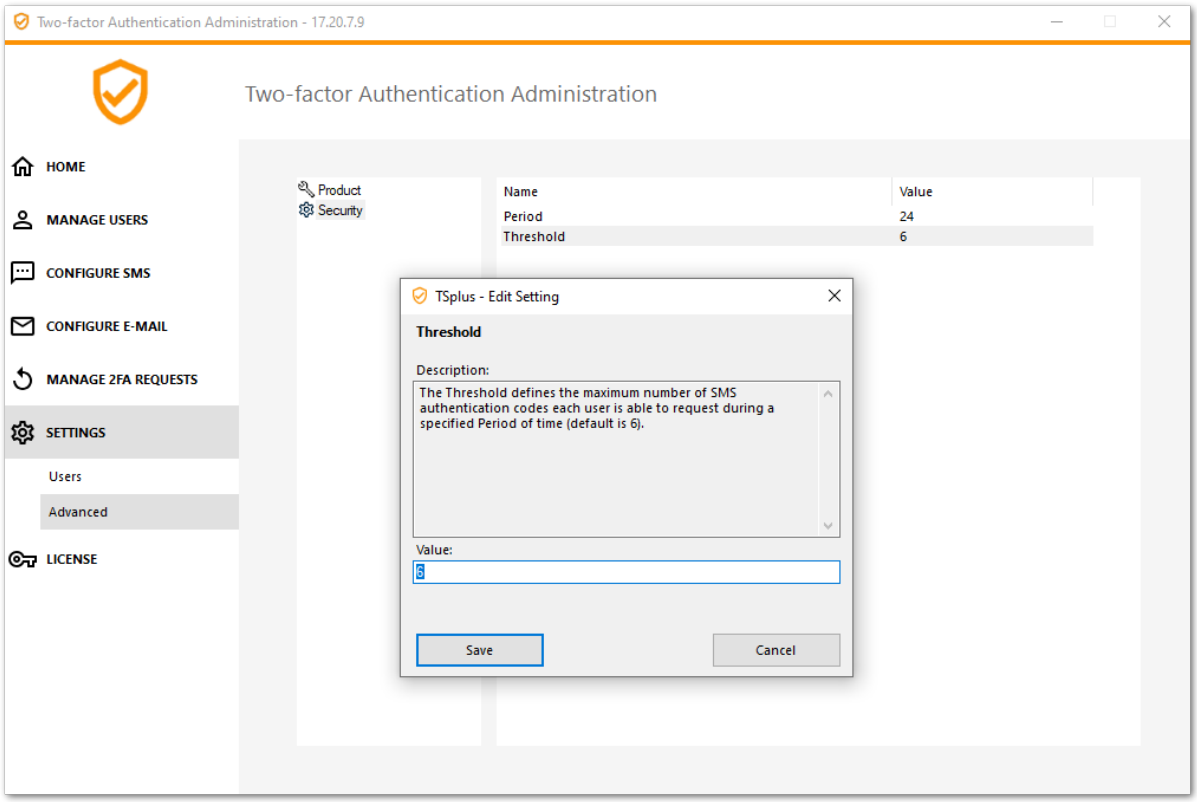
Période de sécurité SMS

La période commence lorsqu'un utilisateur demande un code d'authentification par SMS. Pendant cette période, l'utilisateur peut demander un nouveau code d'authentification par SMS jusqu'à ce que le nombre de SMS demandés atteigne la valeur seuil (en heures, par défaut 24 heures).



Seuil de sécurité SMS

Le seuil définit le nombre maximum de codes d'authentification par SMS que chaque utilisateur peut demander pendant une période de temps spécifiée (par défaut, il est de 6).



Imprimante universelle (novaPDF)

L'imprimante universelle TSplus vous permet d'apercevoir ou d'imprimer des documents depuis n'importe quel PC ou appareil mobile pris en charge par TSplus Remote Access. L'imprimante universelle est pertinente à partir d'une session HTML5 et lorsqu'elle est connectée en utilisant un client généré. L'imprimante universelle n'est pas pertinente lors de l'utilisation du client RDP standard (mstsc.exe) car les imprimantes peuvent être partagées entre le serveur et le client.

Démarrage de la version 17 de Remote Access, Universal Printer utilise novaPDF https://www.novapdf.com/) pour produire des fichiers PDF (Portable Document Format) conformes à 100 % aux normes de l'industrie à partir du document distant. Le document PDF généré est ensuite envoyé à l'imprimante locale souhaitée. L'imprimante universelle (novaPDF) remplace l'imprimante universelle (CustPDF) et l'imprimante universelle (GhostScript) qui sont abandonnées et ne sont plus disponibles pour installation sur votre serveur Remote Access.

Deux imprimantes sont disponibles pour l'impression à distance : Universal Printer et Virtual Printer. Bien que Virtual Printer offre de meilleures performances d'impression, elle n'est pas compatible avec le client HTML5 et nécessite l'installation d'une application cliente. Par conséquent, l'imprimante Universal Printer est définie comme l'imprimante par défaut après la configuration de Remote Access. Voir TSplus Virtual Printer .

Exigences

NovaPDF11Service doit être dans la liste d'exclusion de tout pare-feu ou antivirus actif.

Configurer l'imprimante universelle

Pour configurer votre imprimante universelle, ouvrez l'AdminTool et cliquez sur le Imprimantes menu.

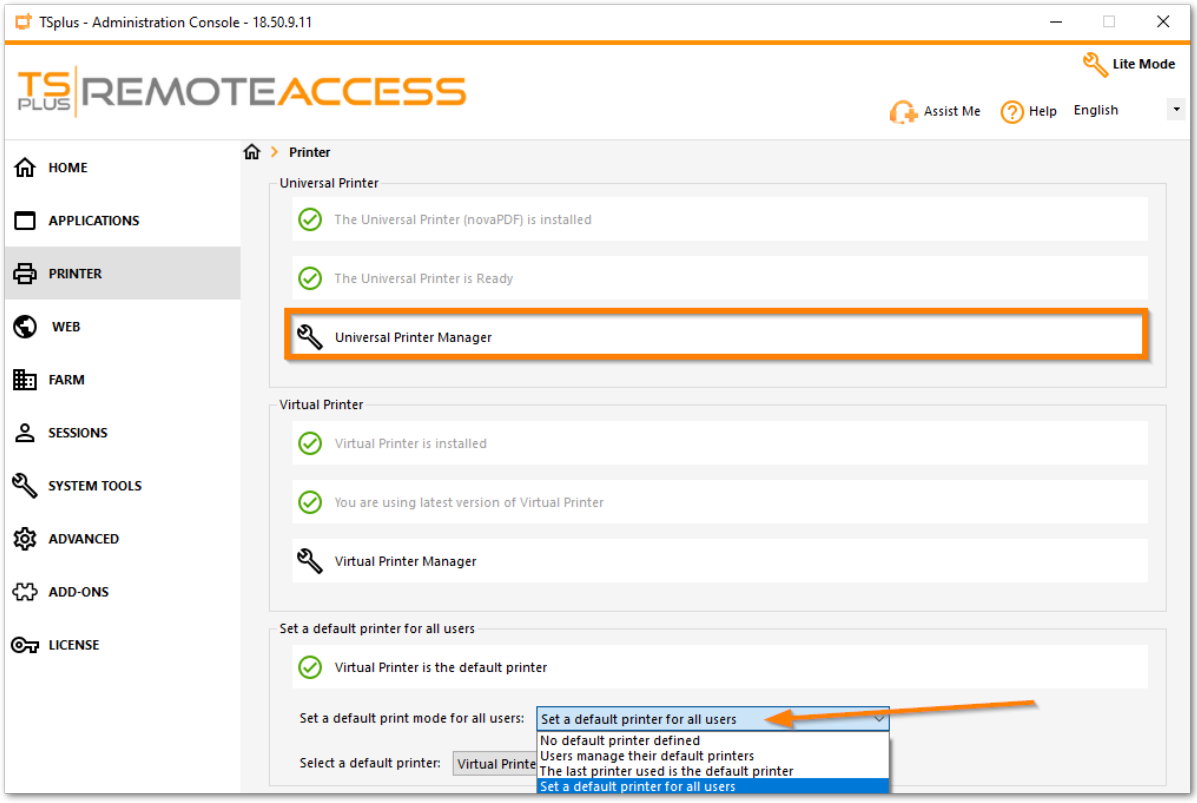
Pour accéder au panneau de contrôle de l'imprimante universelle, veuillez naviguer à travers l'AdminTool : Imprimante > Gestionnaire d'imprimante universelle.

Définir une imprimante par défaut pour tous les utilisateurs

- Aucune imprimante par défaut définie : la configuration de l'imprimante par défaut de

l'utilisateur n'est pas affectée.

- L'utilisateur gère ses imprimantes par défaut : l'option « Laisser Windows gérer mon imprimante par défaut » est désactivée, et il appartient donc à l'utilisateur de sélectionner son imprimante par défaut.
- La dernière imprimante utilisée est l'imprimante par défaut : l'option « Laisser Windows gérer mon imprimante par défaut » est activée.
- Définir une imprimante par défaut pour tous les utilisateurs : l'administrateur impose l'imprimante par défaut de l'utilisateur.



La section Imprimante Universelle affiche quatre tuiles qui permettent aux administrateurs de :

- Vérifiez l'état de configuration de l'imprimante universelle. Si l'imprimante universelle n'est pas installée, alors cliquer sur la tuile installera l'imprimante universelle.

- Vérifiez l'état d'impression de l'imprimante universelle. Si l'imprimante universelle n'est pas prête à recevoir des travaux d'impression, le carrelage peut afficher des informations supplémentaires pertinentes sur l'erreur.

- Vérifiez si l'imprimante universelle est définie comme imprimante par défaut. Si l'imprimante universelle n'est pas définie comme imprimante par défaut, alors cliquer sur le carreau la définira comme imprimante par défaut. Veuillez noter que ce comportement peut être contourné par vos utilisateurs s'ils sont autorisés à le faire.

- Le carreau nommé **Gestionnaire d'imprimante universelle** mène à un écran plus détaillé qui fournit des actions et des propriétés supplémentaires, telles que la suppression de l'imprimante universelle.

Gestionnaire d'imprimante universelle

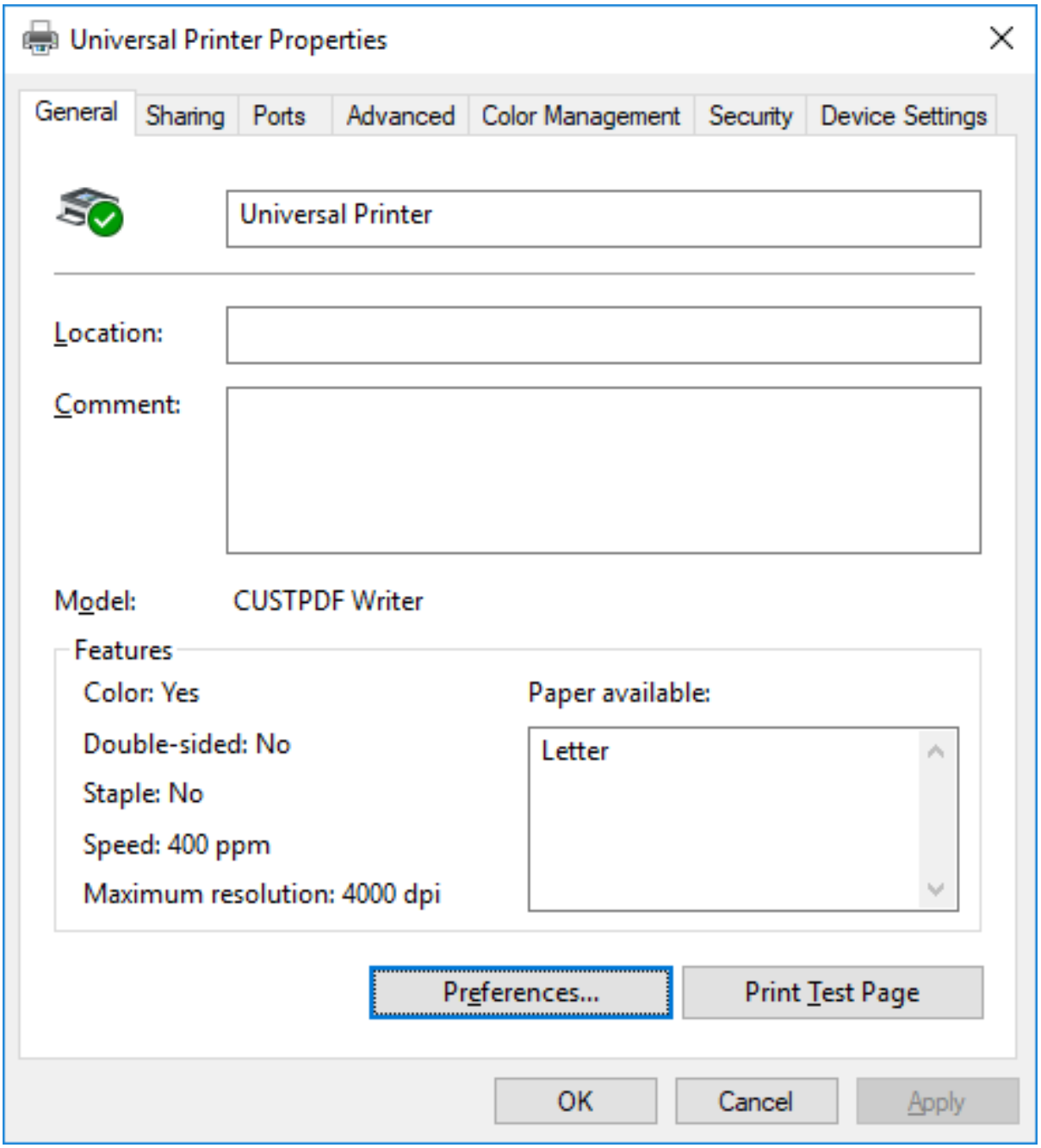
Le Gestionnaire d'Imprimante Universel permet à l'administrateur de vérifier l'état de l'Imprimante Universelle, de supprimer l'Imprimante Universelle, d'accéder à la file d'attente d'impression et aux propriétés de l'imprimante.

En particulier, le bouton situé en bas de la page permet aux administrateurs de :

- **Supprimer l'imprimante universelle** Désinstaller l'imprimante universelle. Elle peut être réinstallée plus tard depuis cet écran.

- **Voir l'imprimante** Ouvre une fenêtre où vous pouvez voir l'état de vos documents d'impression, mettre en pause, reprendre ou annuler l'impression. Vous pouvez également définir vos préférences et propriétés d'impression.

- **Propriétés de l'imprimante universelle** : Ouvre cette fenêtre, où vous pouvez voir toutes les propriétés d'impression. Après l'onglet Général, il y a des onglets pour le partage, les ports, les paramètres avancés, la gestion des couleurs, la sécurité et les paramètres de l'appareil. En bas de la fenêtre contextuelle, l'imprimante **propriétés** permet aux administrateurs de définir la taille de la page pour l'impression de A4 à tout type de format d'impression. Vous pouvez également choisir entre deux orientations d'impression : Portrait ou Paysage.

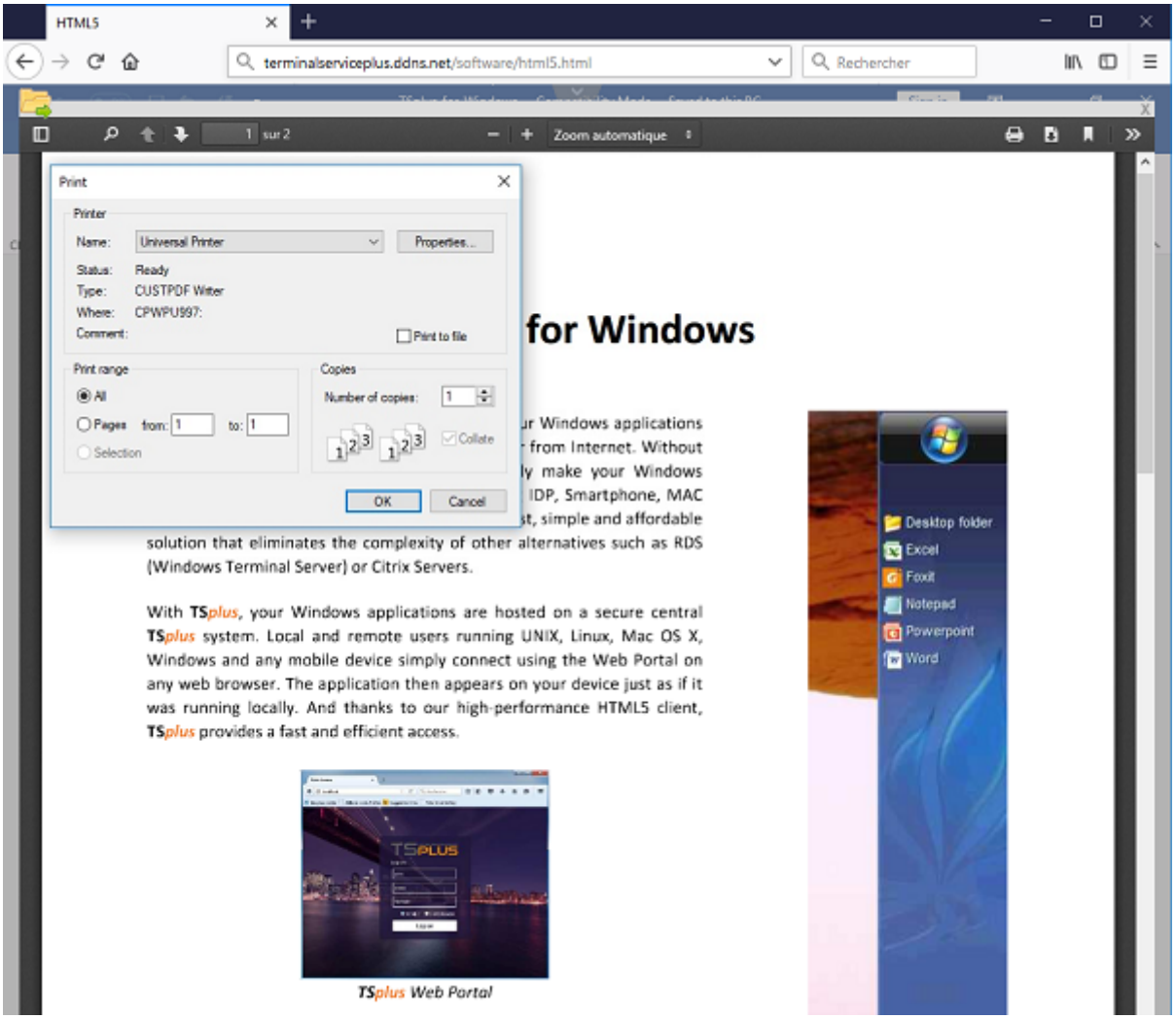


Remarque : L'imprimante universelle utilise novaPDF, qui permet aux administrateurs de créer des profils pour définir les polices, les graphiques, les filigranes, les superpositions et plus encore à travers le **Gérer les profils** bouton situé en dessous des sections Taille de page et Orientation dans la fenêtre contextuelle des propriétés de l'imprimante. Si un profil est sélectionné par défaut, alors le **Afficher la boîte de dialogue Sélectionner les profils avant d'imprimer** peut être vérifié pour permettre à l'utilisateur de sélectionner un profil avant d'imprimer. Veuillez consulter la documentation de novaPDF pour plus de détails sur les profils : Gestionnaire de profil .

Impression avec l'imprimante universelle

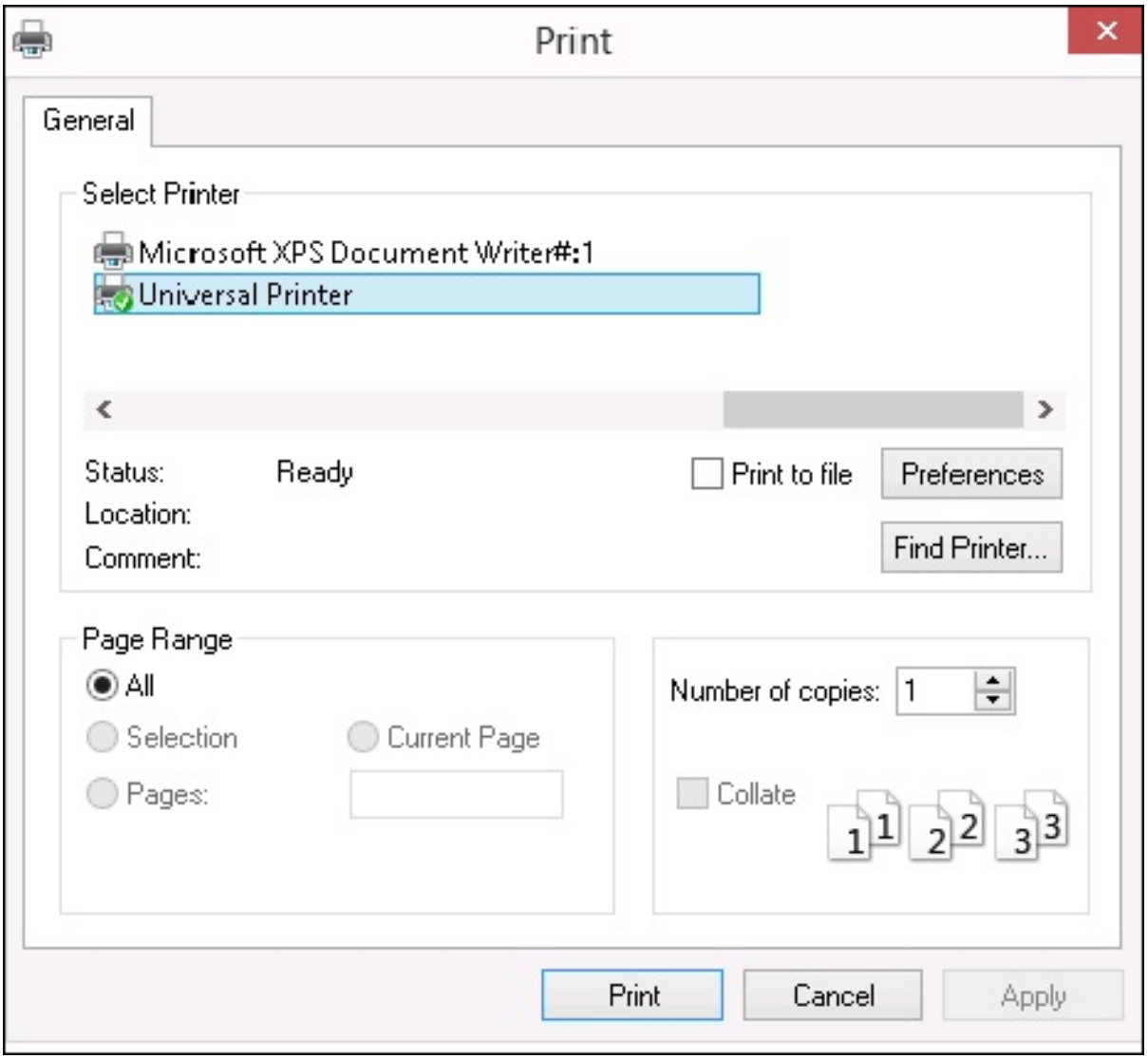
Lors de l'impression avec cette imprimante, le document dans la file d'attente d'impression est automatiquement converti en un fichier PDF par l'imprimante Universal Printer (novaPDF).





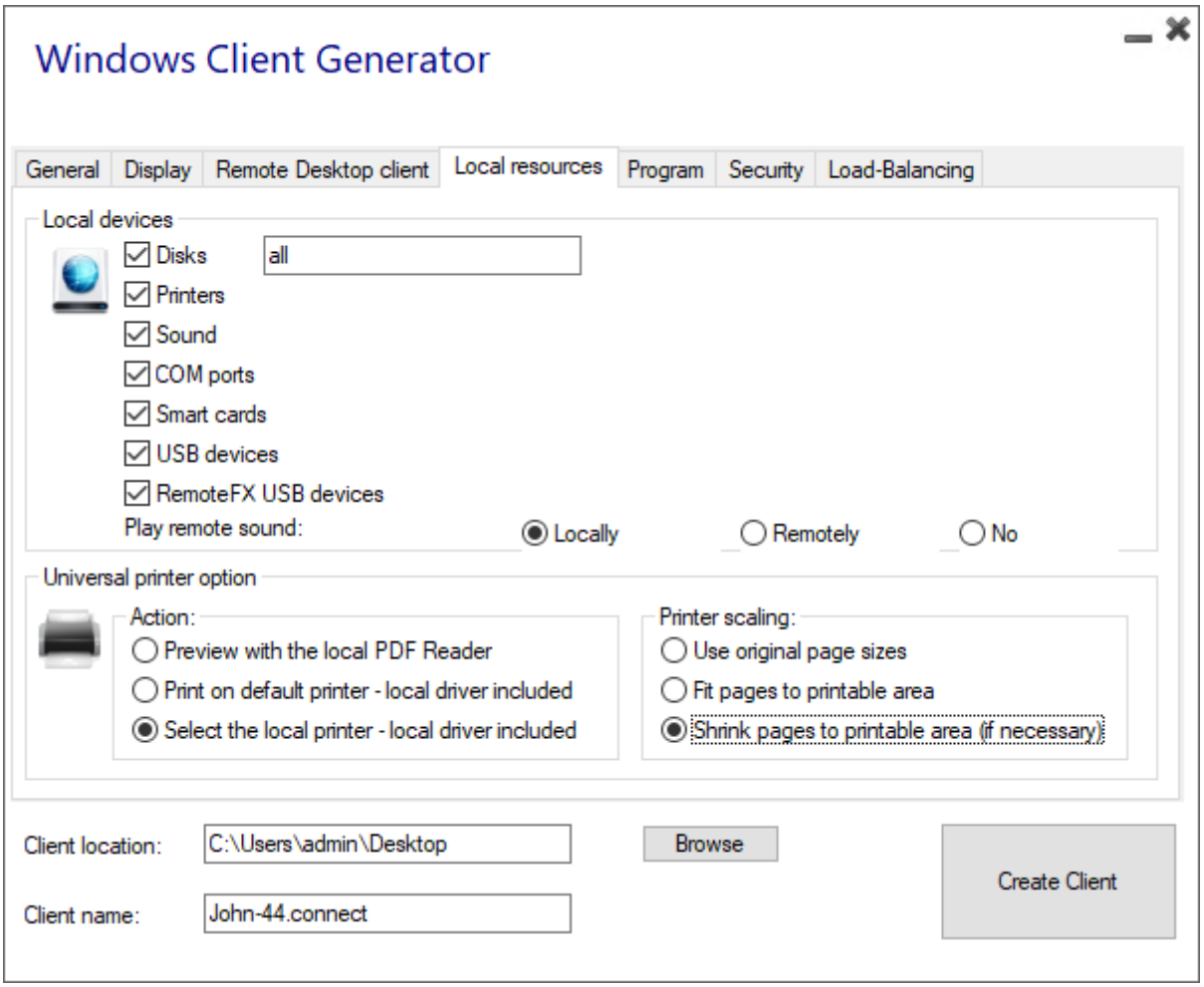
Le fichier PDF généré est ensuite envoyé au lecteur PDF local de la station de travail de l'utilisateur.

Chaque tâche d'impression est ouverte dès qu'elle est prête sur le disque local de l'utilisateur. Le processus d'impression commence une fois que le fichier PDF a été transféré du côté du client, ce qui garantit que la tâche d'impression commence sans délai.



Configurer les options d'impression avec le générateur de client

Vous pouvez choisir parmi 3 options d'impression dans l'onglet Ressources locales de la Générateur de client portable
Lorsque vous utilisez le client de connexion TSplus, vous devez mapper au moins le **C: disque ou tous les disques**



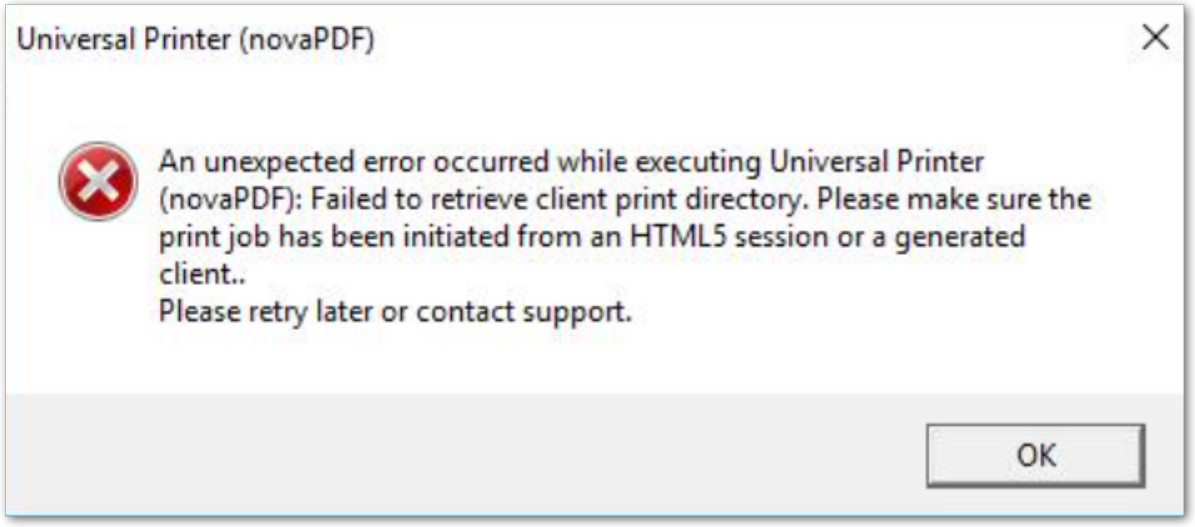
- **Aperçu du lecteur PDF local** le document est poussé sur le poste de travail du client et le lecteur PDF par défaut local ouvre le fichier PDF reçu. L'utilisateur peut alors l'imprimer ou enregistrer une copie sur son disque dur local (ce comportement est attendu lors de l'impression depuis une session HTML5).

- **Imprimer sur l'imprimante par défaut de l'utilisateur** le document est automatiquement imprimé par l'imprimante par défaut de l'utilisateur (cette option n'est disponible que lors de l'utilisation du client de connexion TSplus). Cette option est préférée pour les utilisateurs qui ont beaucoup de travaux d'impression à imprimer pendant la journée et utilisent la même imprimante à cet effet.

- **Sélectionner une imprimante locale** l'utilisateur peut sélectionner l'une de ses imprimantes locales (cette option n'est disponible que lors de l'utilisation du client de connexion TSplus).

Pour lire des fichiers PDF, de nos jours, de nombreuses personnes s'en sortent sans avoir à utiliser une application externe. Firefox et Chromium, la version open source du navigateur Chrome de Google, sont livrés avec des lecteurs PDF intégrés, donc un plugin externe n'est plus nécessaire pour la plupart des utilisateurs.

POUR VOTRE INFORMATION
Si le lecteur C: n'est pas mappé, l'utilisateur recevra ce message d'erreur.



Configurer l'imprimante novaPDF

De **Préférences d'imprimante > Outils > Mot de passe** vous pouvez :

- Modifier le mot de passe par défaut
- Changer la langue de l'interface du Gestionnaire de Profil
- Surveillez l'avancement des travaux d'impression en temps réel
- Vérifiez l'historique de l'imprimante

Ouverture de l'impression dans un nouvel onglet

Par défaut, les travaux d'impression d'une session HTML5 s'affichent dans une fenêtre contextuelle comme avant la version 17.10.

Il est possible de modifier ce comportement et d'ouvrir les travaux d'impression dans un nouvel onglet du navigateur en utilisant le paramètre suivant : **AdminTool > Avancé > Session > Ouvrir les travaux d'impression dans un nouvel onglet**

Profils

Profiles permet de personnaliser les mises en page, les filigranes, le niveau de compression et bien plus encore. Le Gestionnaire de Profils vous permet de gérer les profils. Les profils consistent en des configurations utilisées lors de l'impression avec l'Imprimante Universelle. Par exemple, vous pouvez établir divers profils d'impression adaptés à des exigences de sortie spécifiques, telles que la distribution de PDF, l'impression de haute qualité, des fins de révision

ou le marquage de documents comme confidentiels.

Pour ouvrir le Gestionnaire de profil, ouvrez Périphériques et imprimantes, faites un clic droit sur Imprimante universelle et sélectionnez Préférences d'impression. Ensuite, cliquez sur le **Gérer les profils** bouton. Le mot de passe par défaut est : pass@word1

Comprendre les profils par défaut

- **Profil par défaut** le profil par défaut est conçu pour imprimer un ou plusieurs documents à la fois. Convient à la plupart des scénarios.
- **Profil des documents ouverts à imprimer** Utilisez ce profil pour imprimer automatiquement un document lorsqu'il est ouvert avec un visualiseur PDF. Ce profil est utile pour obtenir un clic lors de l'impression depuis une session HTML5.

Lors de l'ouverture d'une session HTML5, le profil d'impression des documents ouverts est sélectionné automatiquement pour l'utilisateur actuel. Cependant, l'impression automatique dans la session HTML5 sera désactivée si une autre session est actuellement ouverte pour le même utilisateur en mode RDP. Dans ce cas, le profil par défaut est appliqué par défaut.

Remarque Le profil des documents ouverts à imprimer ne peut pas être sélectionné automatiquement pour les applications UWP telles que Notepad dans Windows 11, car ces applications sont conçues pour fonctionner en complète isolation avec le système. Cependant, il reste possible pour l'utilisateur de sélectionner manuellement le profil à utiliser et de le choisir par défaut pour les prochaines impressions. Il n'y a pas de solution de contournement pour le moment. Cependant, la refonte de l'imprimante novaPDF prévue pour la prochaine version majeure de novaPDF prévue au quatrième trimestre 2024 lèvera cette limitation.

Quel profil l'utilisateur peut-il choisir ?

Par défaut, les utilisateurs peuvent choisir quel profil utiliser parmi les deux profils par défaut. Les utilisateurs sont autorisés à sélectionner un profil comme actif et ne pas afficher la boîte de dialogue Sélectionner un profil pour les prochaines impressions. Les administrateurs peuvent définir un ou plusieurs profils disponibles pour tous les utilisateurs. Cette décision prévaut sur les choix des utilisateurs. Voir https://www.novapdf.com/printer-manager-profiles-help.html .

Important Il est recommandé de copier les profils existants pour créer des profils plus personnalisés, car les profils existants intègrent plusieurs fonctionnalités requises pour la plupart des installations, telles que les polices intégrées dans le document PDF généré.

Dépannage

Veuillez trouver ci-dessous des conseils de dépannage pour résoudre les problèmes d'Universal Printer (novaPDF).

Rester à jour

- Mettre à jour le Client de Connexion peut résoudre certains problèmes survenant du côté client.
- Consultez le journal des modifications pour voir si une version plus récente résout votre problème à https://dl-files.com/TSplus-changelog.html
- Rappelez-vous que l'équipe de développement ne peut prendre en charge que la dernière base de code.

Comprendre quelle partie du processus d'impression a échoué

- Le travail d'impression a-t-il été créé dans la file d'attente d'impression ? Quel est son statut ?

Collecte des journaux pour les erreurs d'impression

- **Journaux d'ouverture de session** surtout utile pour des problèmes tels que l'échec de la récupération du répertoire d'impression du client, situé à **C:\wsession\trace** .
- **Logs de l'application AdminTool** situé à **C:\Program Files (x86)\TSplus\UserDesktop\files** .
- **Journaux de l'imprimante universelle** l'envoi de la tâche d'impression vers le côté client, situé à **C:\wsession\UniversalPrinter\logs** .
- **Journaux des événements de session** pour l'utilisateur d'impression, gestion des reconnexions, situé à **%appdata%\UniversalPrinter\logs** .

Collecte des journaux pour les problèmes d'installation d'imprimante

- **Journal d'installation** 2024-02-XX #XX.txt disponible dans le **%temp%** répertoire.
- **gestionuniverselled'imprimantes** _XX022024.txt situé à **C:\Program Files (x86)\TSplus\UserDesktop\files** .
- Tous les fichiers .txt situés dans **C:\Program Files (x86)\TSplus\UserDesktop\files\UniversalPrinter** .

Collecte des journaux pour les erreurs d'impression côté client, lors de l'utilisation du Client de Connexion

- **version.dat** Veuillez toujours conseiller de mettre à jour le Client de Connexion vers la dernière version.
- **Client de connexion** et **Client d'imprimante universel** logs. Ces journaux peuvent être

activés en créant la valeur de clé suivante dans le registre :
HKEY_LOCAL_MACHINE\Software\Digital River\ConnectionClient\Debug" = "vrai" Les journaux résultants sont situés ici : **C:\Utilisateurs \RDP6\logs** .

Mise à jour de TSplus Remote Access

Découvrez nos corrections et améliorations en cliquant sur Journal des modifications

Notre équipe de développement travaille quotidiennement pour garantir la stabilité et la compatibilité de TSplus avec les dernières versions des systèmes d'exploitation Microsoft et les dernières mises à jour.

Nous sommes fiers de vous fournir de nouvelles fonctionnalités et améliorations chaque semaine.

C'est pourquoi il est recommandé de maintenir votre serveur à jour.

Lorsque se produit un problème de « 2 sessions par serveur », généralement après les mises à jour de Windows le deuxième mardi du mois, veuillez vérifier votre version de TSplus Remote Access (ou TSplus LTS 18/17).

Une nouvelle version sera bientôt publiée pour restaurer la compatibilité avec la dernière mise à jour de Windows.

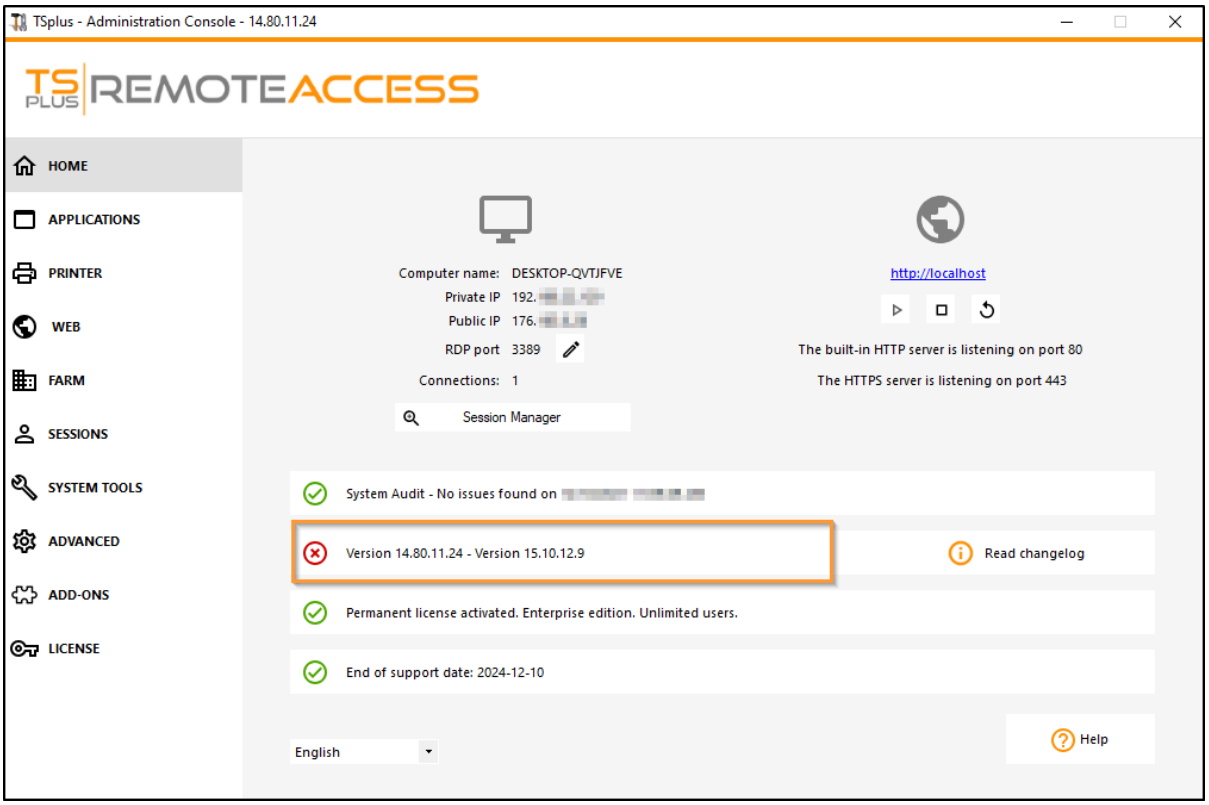
En tant que solution temporaire, vous pouvez désinstaller la mise à jour Windows du jour et redémarrer.

Important : Évitez de désinstaller TSplus Remote Access ou de restaurer une image système plus ancienne. Ces actions peuvent déclencher des conflits de licence qui sont beaucoup plus complexes à résoudre. Dans la plupart des cas, un simple redémarrage suffit pour appliquer automatiquement les correctifs de compatibilité.

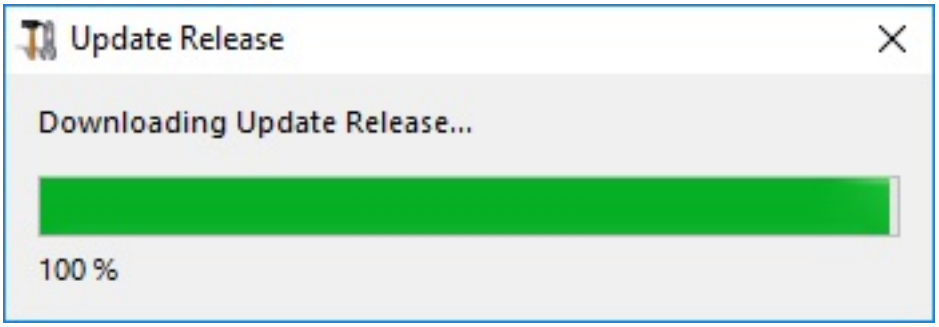
En vous abonnant à nos services de support et de mises à jour annuels, vous aurez accès aux dernières mises à jour et corrections de bogues.

Pour voir quelle version de TSplus vous avez et la mettre à jour :

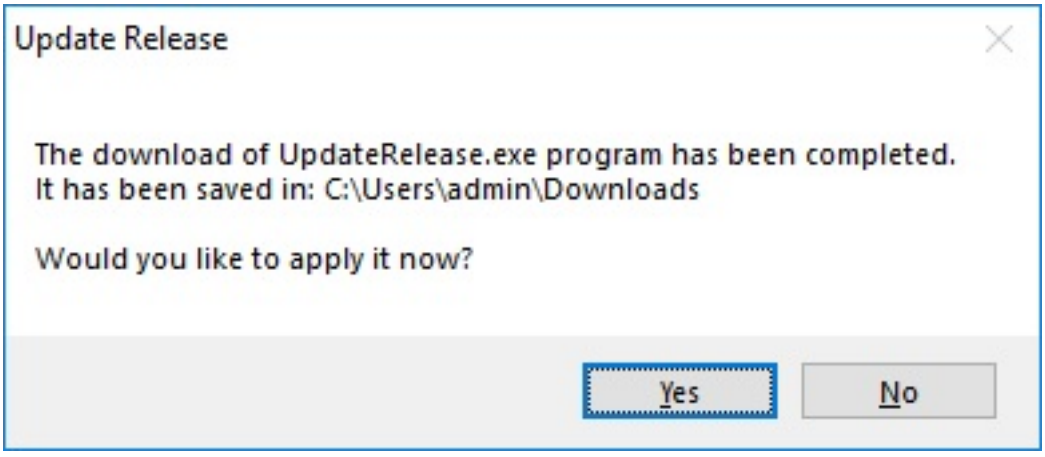
- Vous pouvez vérifier l'état de votre version TSplus dans l'onglet Accueil de votre AdminTool :



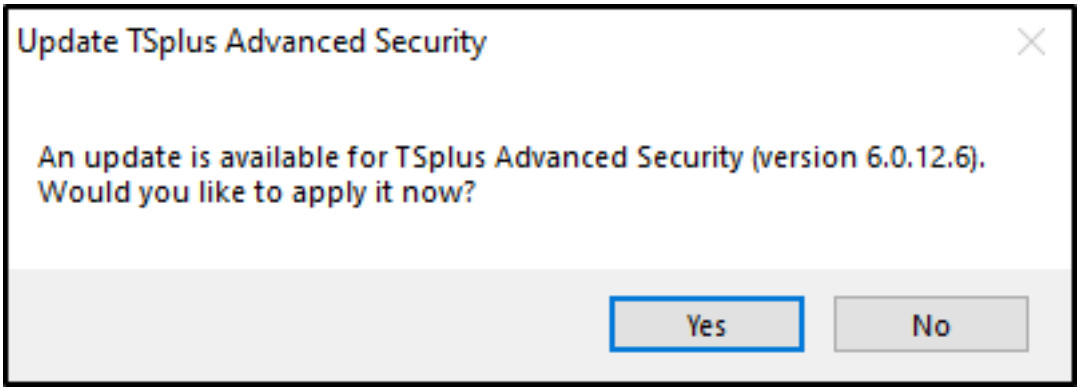
- Vous pouvez ensuite cliquer dessus. Depuis la version TSplus 11.50, l'AdminTool télécharge automatiquement…



…et applique le programme de mise à jour lorsque cela est demandé :



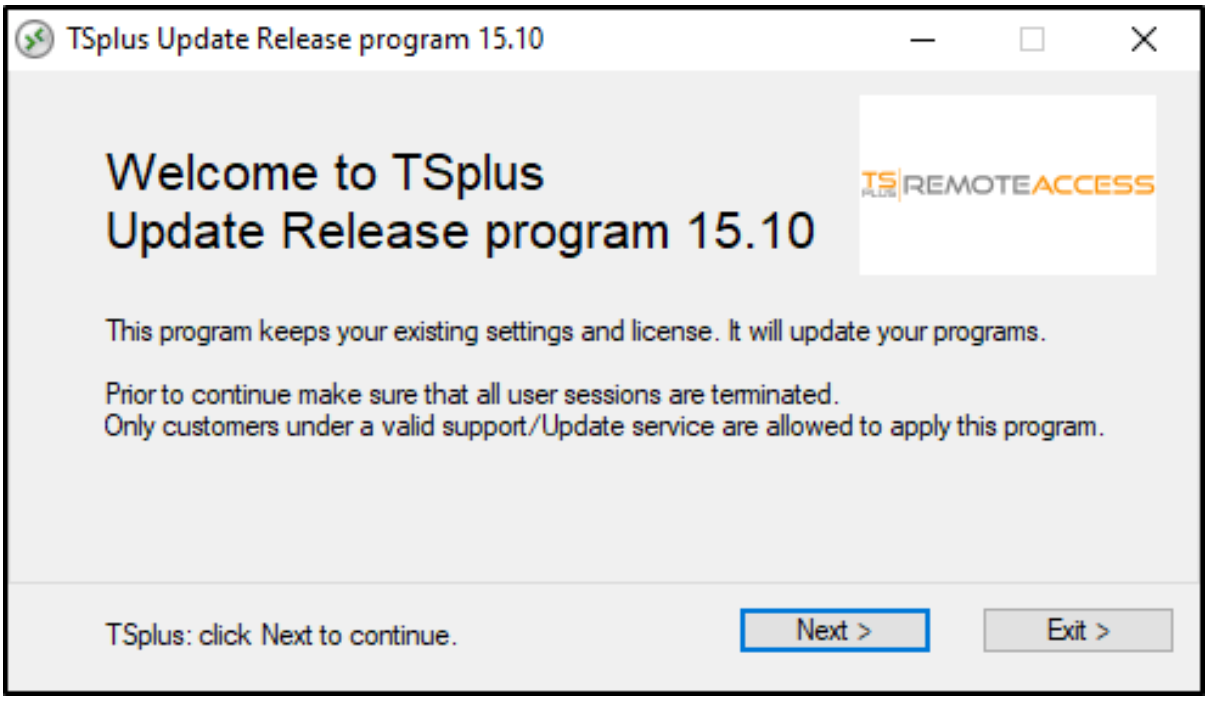
- Depuis la version 11.40 de TSplus, vous aurez le choix d'installer TSplus Advanced Security notre puissant Add-On de Sécurité, dans sa version d'essai Ultimate (toutes les fonctionnalités de sécurité gratuites à utiliser pendant 2 semaines) pour votre système TSplus :

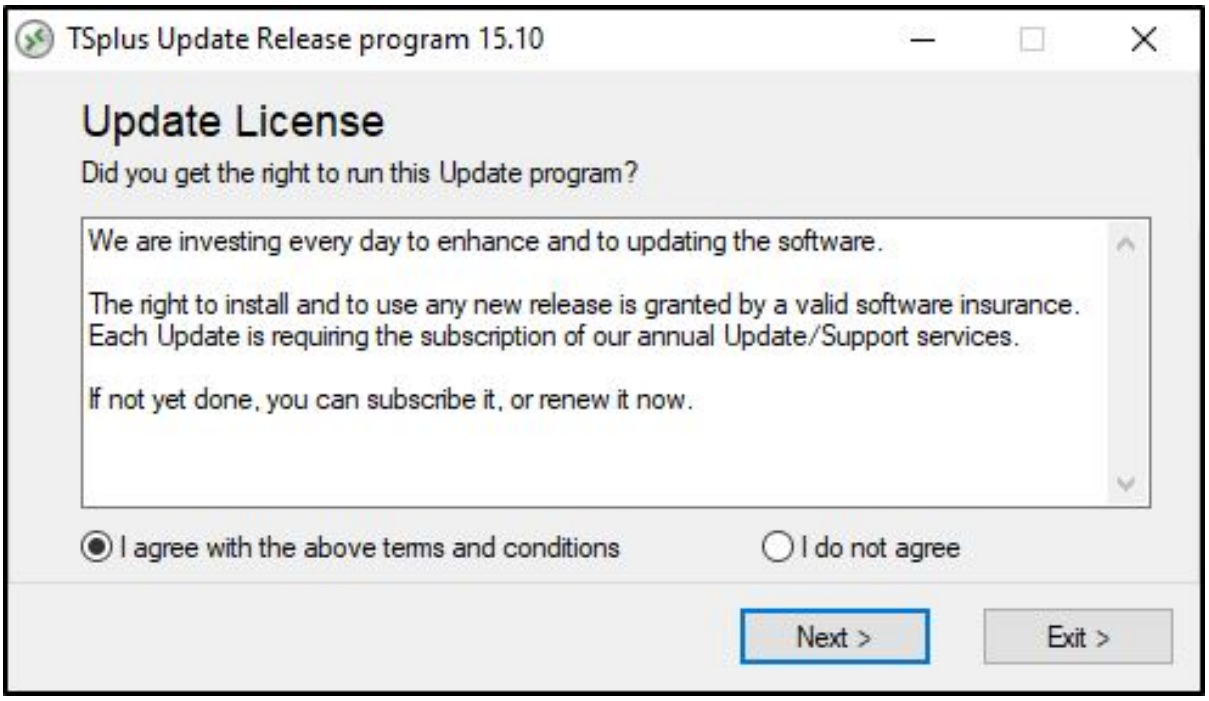


Vous pouvez toujours le télécharger via ce lien : Mise à jour de la version et appliquez-le manuellement.

Le programme de mise à jour est conçu pour garder vos paramètres TSplus actuels en sécurité.

Si vous ne vous êtes pas encore abonné aux services de mise à jour/soutien de TSplus, ou si votre abonnement a expiré, vous ne pourrez pas exécuter le programme de publication de mise à jour :

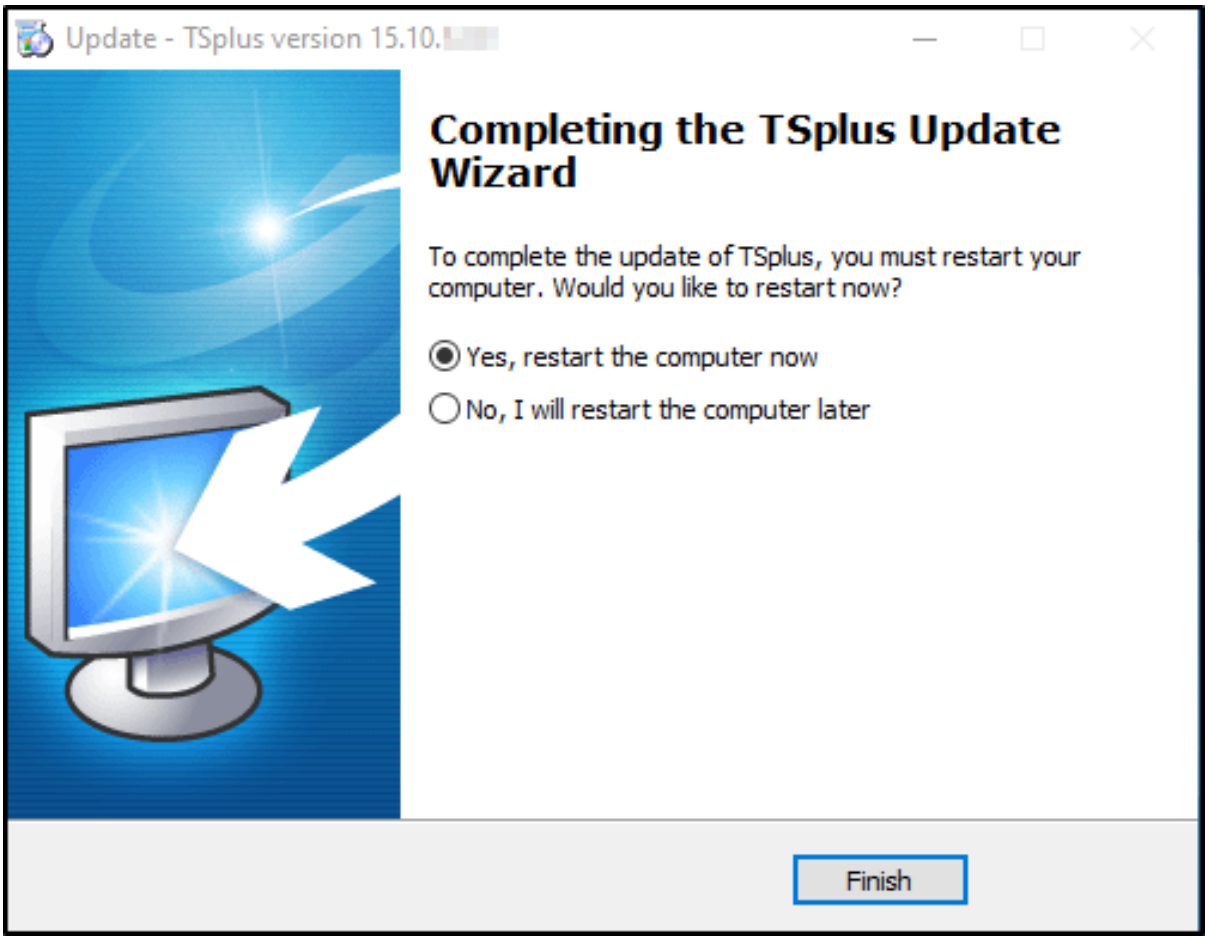




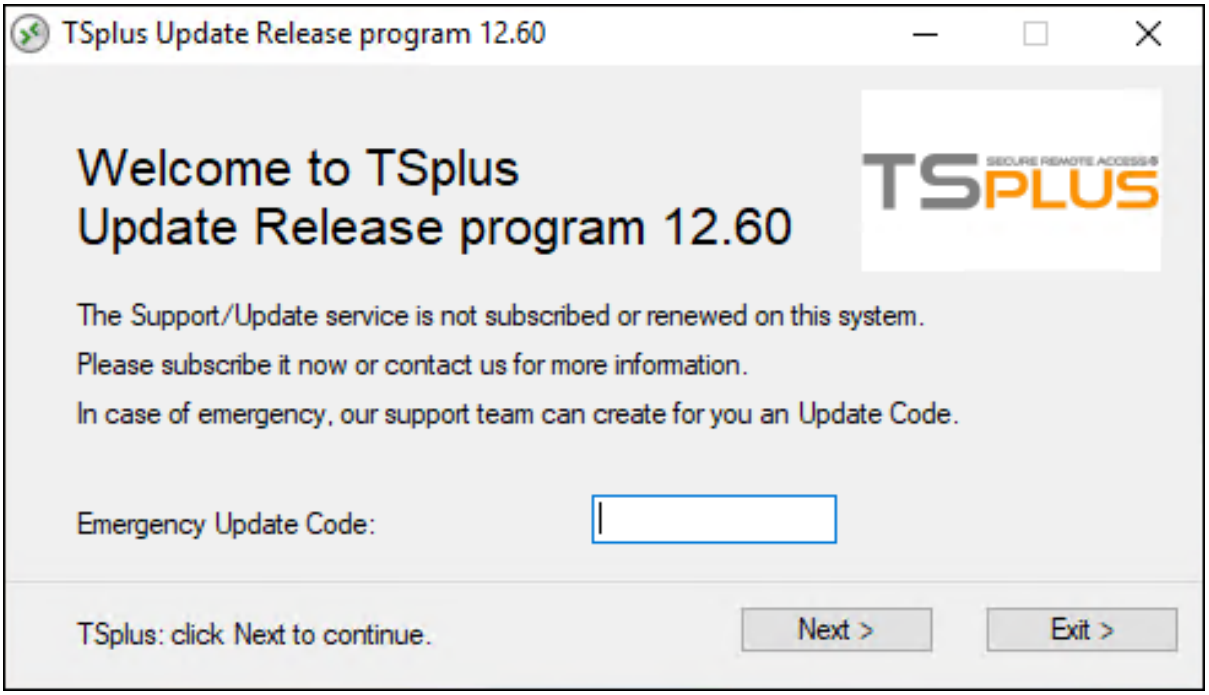
Dans ce cas, nous vous conseillons de passer votre commande sur notre page de boutique.

Vous recevrez les informations nécessaires pour télécharger votre fichier support.lic. L'activation de vos services de mise à jour/soutien est un processus simple décrit. ici .

Lorsque la mise à jour est terminée, un redémarrage est nécessaire :



Pour les versions antérieures à v14, uniquement pour des besoins spécifiques, l'équipe de support TSplus peut fournir un code de mise à jour d'urgence qui déverrouillera le programme de mise à jour.



Problème de mise à jour :

Vérifiez le fichier manquant

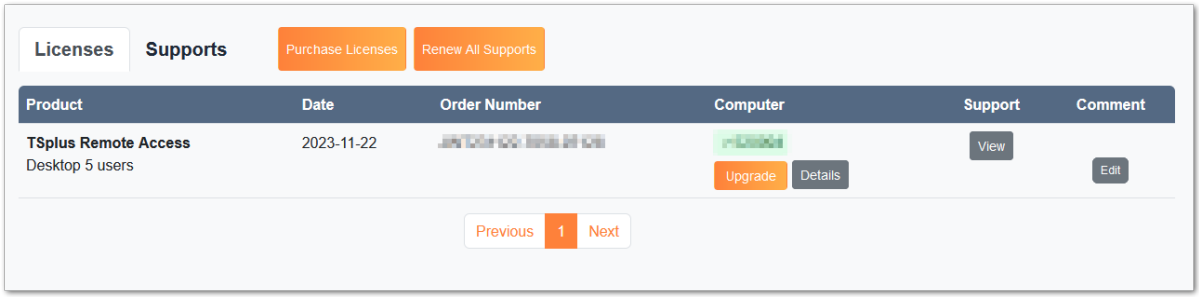
C:\Program Files (x86)\TSplus\reboot_required.dat

1. Si ce fichier est présent, supprimez-le.
2. Redémarrez votre serveur
3. Exécutez à nouveau la mise à jour à partir de ce lien en cliquant ici : Mise à jour de la version

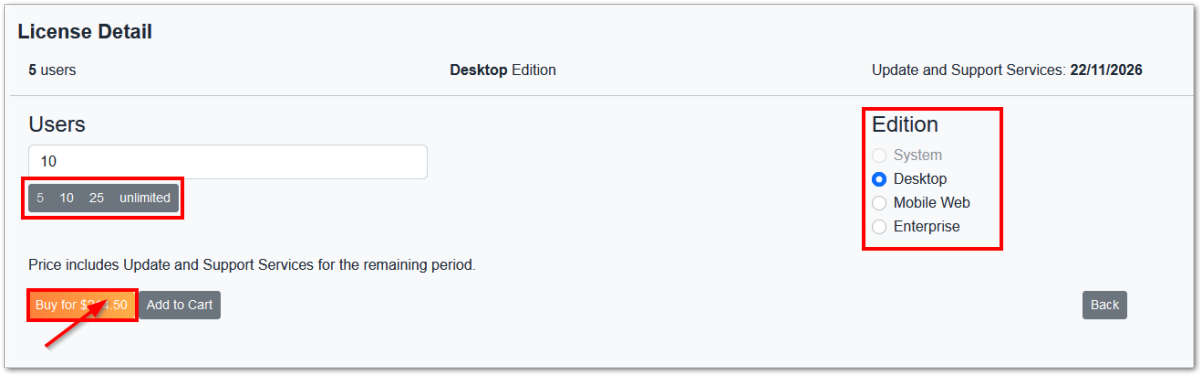
---

Mettre à niveau votre version de TSplus

Si vous souhaitez mettre à jour votre version actuelle de TSplus, afin d'ajouter plus d'utilisateurs ou plus de fonctionnalités, inscrivez-vous dans votre portail de licence.



Sélectionnez votre choix de mise à niveau (utilisateurs et version) et cliquez sur **Acheter pour** pour continuer sur notre boutique.



Après votre achat, la mise à jour sera instantanée et visible sur votre portail de licence.
Vous devez également suivre la même procédure sur votre appareil afin qu'il soit lié à votre licence.

Sur votre serveur, cliquez sur le **Rafraîchissez votre licence** bouton dans l'AdminTool > onglet Licence.

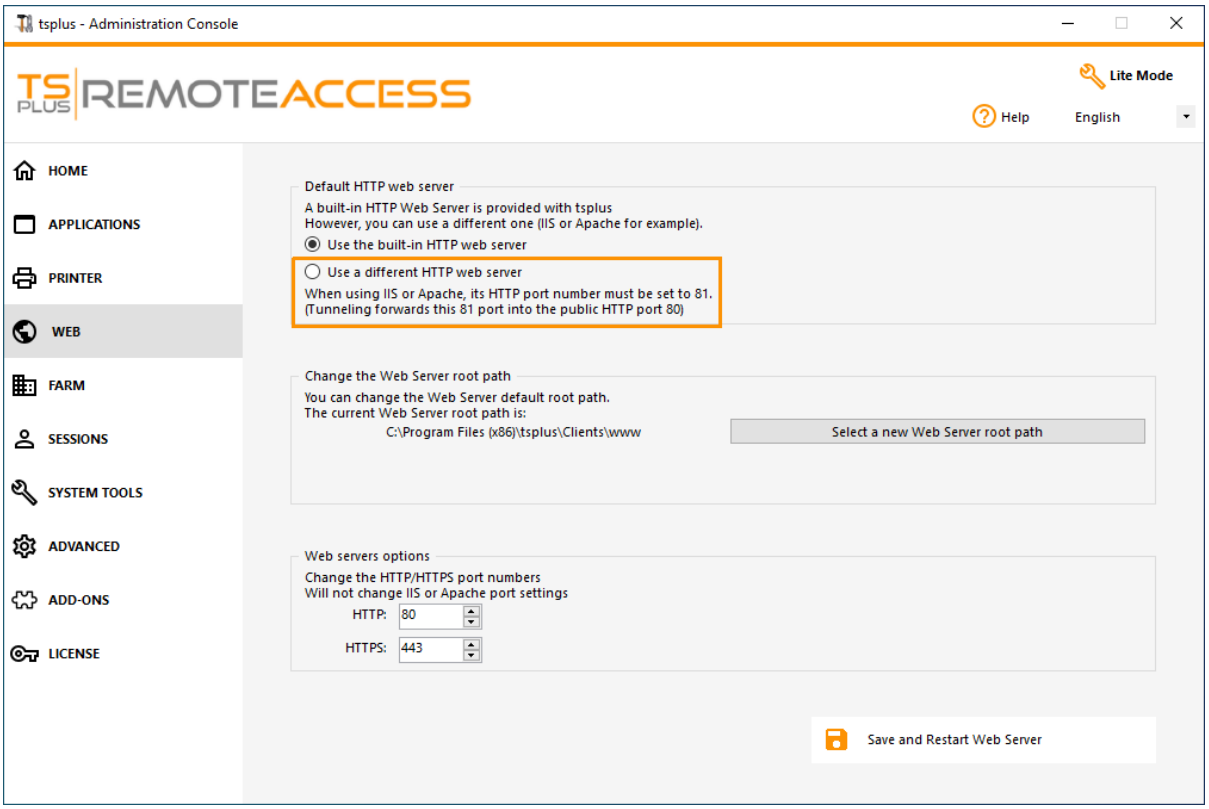
Comment utiliser Apache plutôt que le serveur Web par défaut de Terminal Service Plus

Pré-requis

Il peut être judicieux de Mettre à jour Terminal Service Plus pour être sûr d'obtenir les derniers programmes TSplus.

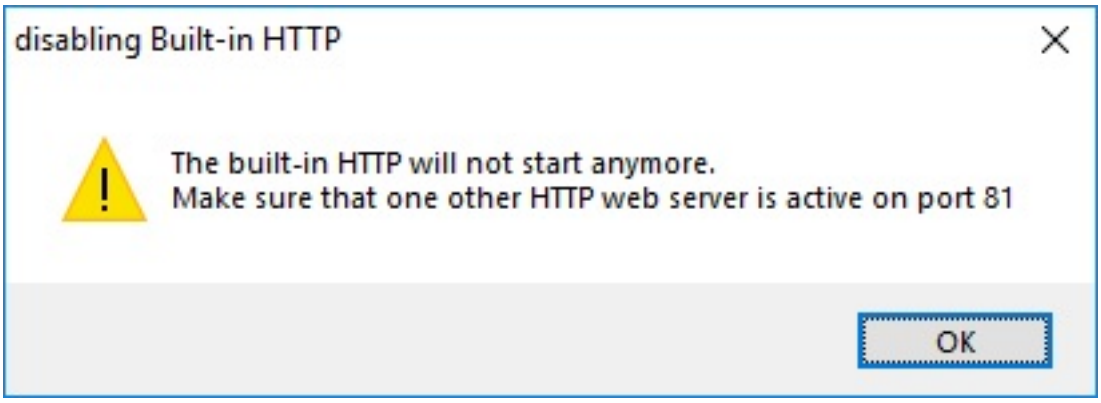
1. Démarrez AdminTool et allez à l'onglet Serveur Web

Cliquez sur la tuile Gérer les serveurs Web, vérifiez **Utilisez un serveur web HTTP différent** parce que vous voulez utiliser Apache.



Ensuite, utilisez le bouton **Sélectionnez un nouveau chemin racine de serveur Web** pour indiquer à TSplus où sera le nouveau dossier racine du web.

TSplus copiera les fichiers/dossiers demandés dans ce nouveau dossier racine et, à ce stade, le paramètre TSplus pour Apache est presque terminé. Une fenêtre contextuelle vous recommandera de changer le port HTTP d'Apache à 81.



Il est maintenant temps de configurer Apache.

2. Configuration d'Apache

Changez le HTTP de 80 à 81.

La manière spécifique de faire cela dépend de votre version d'Apache et de vos paramètres Apache actuels.

Nous vous conseillons de sauvegarder tout fichier de configuration Apache avant de les modifier, afin d'avoir un moyen de les restaurer si nécessaire.

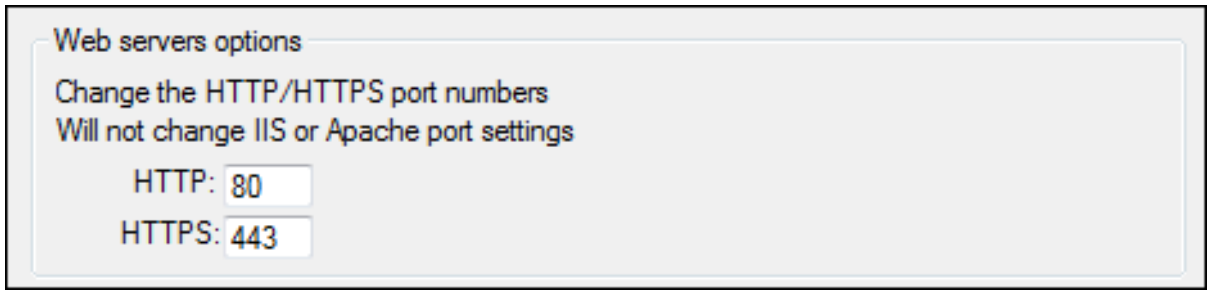
Habituellement, vous pouvez changer le port d'écoute d'Apache en modifiant le fichier httpd.conf trouvé dans le répertoire “Apache\conf”:

Écoutez 81

Une fois cela fait, redémarrez le service Apache.

3. Retour à l'outil de gestion des serveurs Web TSplus

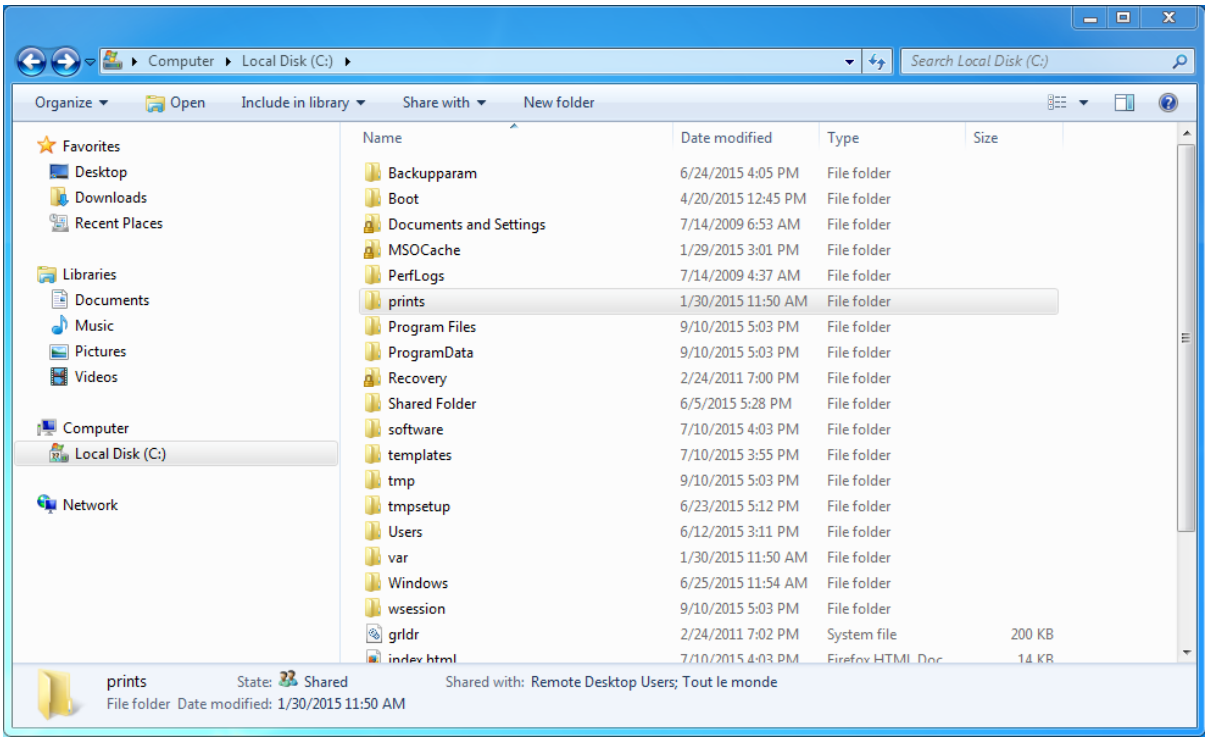
Vous pouvez définir les ports HTTP et HTTPS dans l'outil de gestion Web de TSplus. Nous recommandons d'utiliser des ports standard, mais cette fonctionnalité peut être utile pour éviter un conflit avec un autre processus.

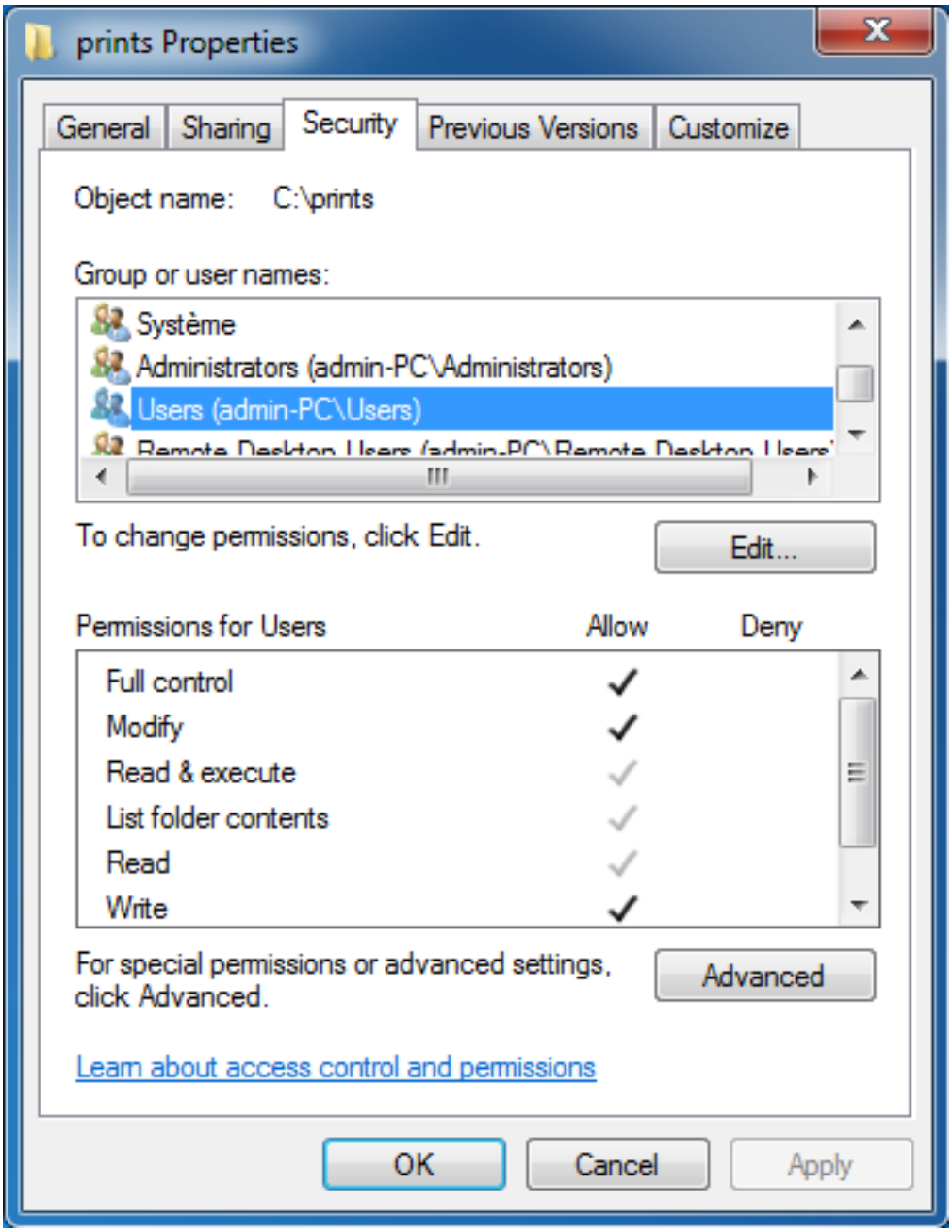


4. Dernières étapes

Pour l'imprimante universelle, nous devons pouvoir écrire dans le dossier PRINTS.

Donc, vérifiez que tout le monde/utilisateurs… a tous les droits sur le dossier …/impressions.


Computer ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Organize
Open
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Network
Name
Date modified
Type
Size
Backupparam 6/24/2015 4:05 PM File folder
Boot 4/20/2015 12:45 PM File folder
Documents and Settings 7/14/2009 6:53 AM File folder
MSOCache 1/29/2015 3:01 PM File folder
PerfLogs 7/14/2009 4:37 AM File folder
prints 1/30/2015 11:50 AM File folder
Program Files 9/10/2015 5:03 PM File folder
ProgramData 9/10/2015 5:03 PM File folder
Recovery 2/24/2011 7:00 PM File folder
Shared Folder 6/5/2015 5:28 PM File folder
software 7/10/2015 4:03 PM File folder
templates 7/10/2015 3:55 PM File folder
tmp 9/10/2015 5:03 PM File folder
tmpsetup 6/23/2015 5:12 PM File folder
Users 6/12/2015 3:11 PM File folder
var 1/30/2015 11:50 AM File folder
Windows 6/25/2015 11:54 AM File folder
wsession 9/10/2015 5:03 PM File folder
grldr 2/24/2011 7:02 PM System file 200 KB
index.html 7/10/2015 4:03 PM Firefox HTML Doc 14 KB
prints State: Shared Shared with: Remote Desktop Users; Tout le monde
File folder Date modified: 1/30/2015 11:50 AM



Ensuite, sélectionnez le fichier .html que vous souhaitez utiliser comme page d'accès Web dans :

C:\Program Files (x86)\TSplus\Clients\www

et copiez-le en tant qu'index.html dans votre dossier racine web, généralement il s'agit du répertoire "Apache\htdocs".

5. Paramètres spécifiques pour TSplus Gateway Portal, équilibrage de charge et/ou transfert de fichiers HTML5

Si vous souhaitez utiliser ce système basé sur Apache comme un TSplus Gateway Portal et/ou utiliser la fonctionnalité d'équilibrage de charge du TSplus Gateway Portal et/ou utiliser la fonctionnalité de transfert de fichiers HTML5, vous devrez autoriser l'exécution des scripts GCI de TSplus par Apache.

Tout d'abord, vous devez avoir le module CGI activé dans Apache.

Modifiez le fichier httpd.conf trouvé dans le répertoire “Apache\conf”, et recherchez une ligne ressemblant à :

;LoadModule cgi_module modules/mod_cgi.so

Retirez le ";" pour activer le module CGI :

LoadModule cgi_module modules/mod_cgi.so

Ensuite, trouvez une ligne commençant par :

AddHandler cgi-script

Et ajoutez l'extension .exe pour autoriser les fichiers .exe à être traités comme des programmes CGI par Apache :

AddHandler cgi-script .exe

Enfin, vous devez dire à Apache que le dossier “cgi-bin” de TSplus contient des programmes CGI. Pour ce faire, vous devez ajouter la ligne suivante dans le fichier httpd.conf situé dans le répertoire “Apache\conf” :

ScriptAlias /cgi-bin/ "C:/Program Files (x86)/TSplus/Clients/www/cgi-bin/"

Une fois cela fait, redémarrez le service Apache.

Si vous rencontrez des problèmes pour configurer CGI sur votre serveur Apache, veuillez vous référer à la Documentation officielle d'Apache

Vérification de vos paramètres : Pour valider vos paramètres, veuillez ouvrir un navigateur web sur votre serveur et aller à http://localhost/cgi-bin/hb.exe Si vous obtenez une page d'erreur Apache, vous avez un problème dans votre configuration Apache. Si vous obtenez une ligne de texte/nombres, tout va bien !

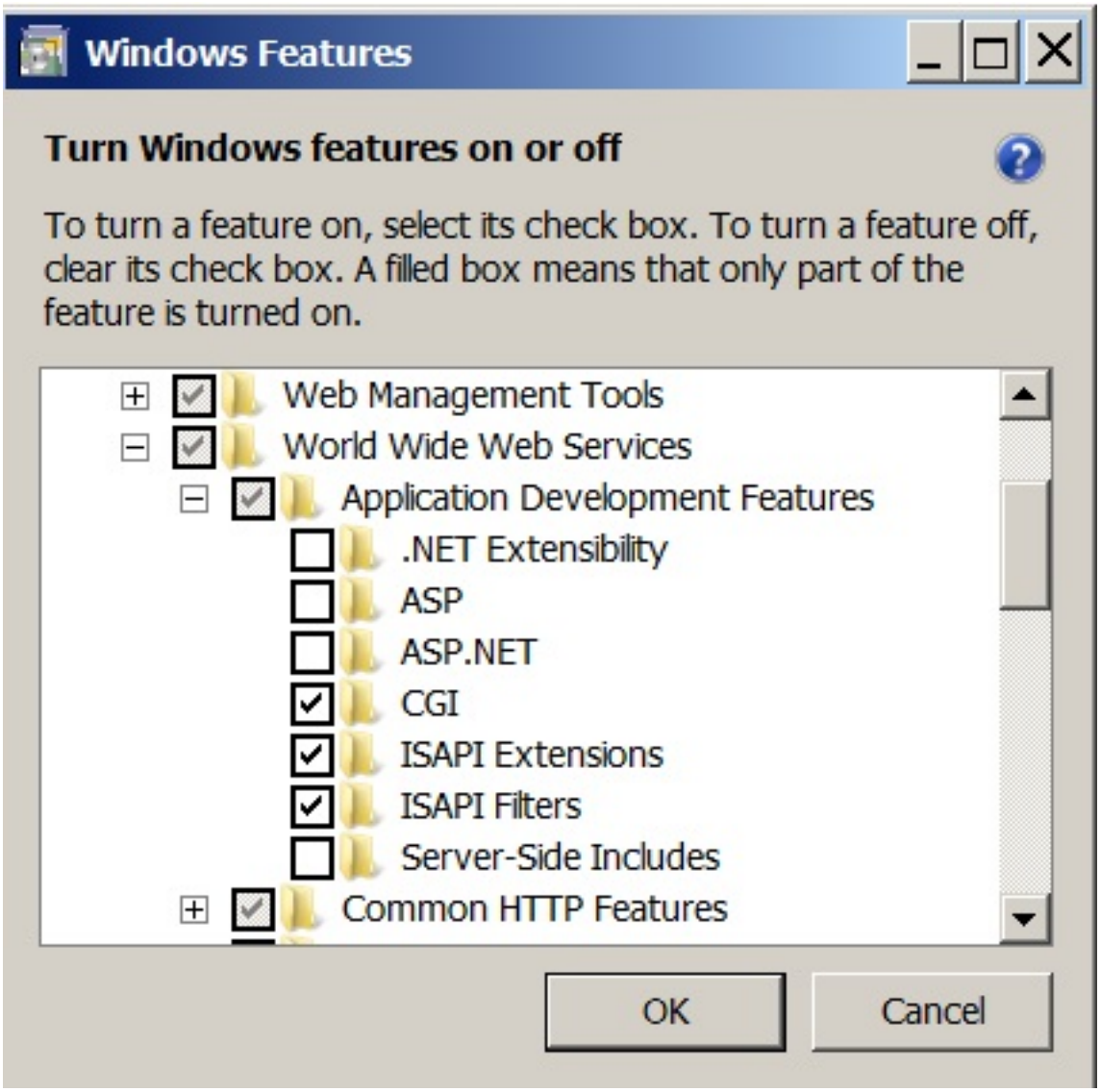
Comment utiliser IIS plutôt que les serveurs Web par défaut de Terminal Service Plus

Pré-requis

Il peut être judicieux de Mettre à jour Terminal Service Plus pour être sûr d'obtenir les derniers programmes TSplus.

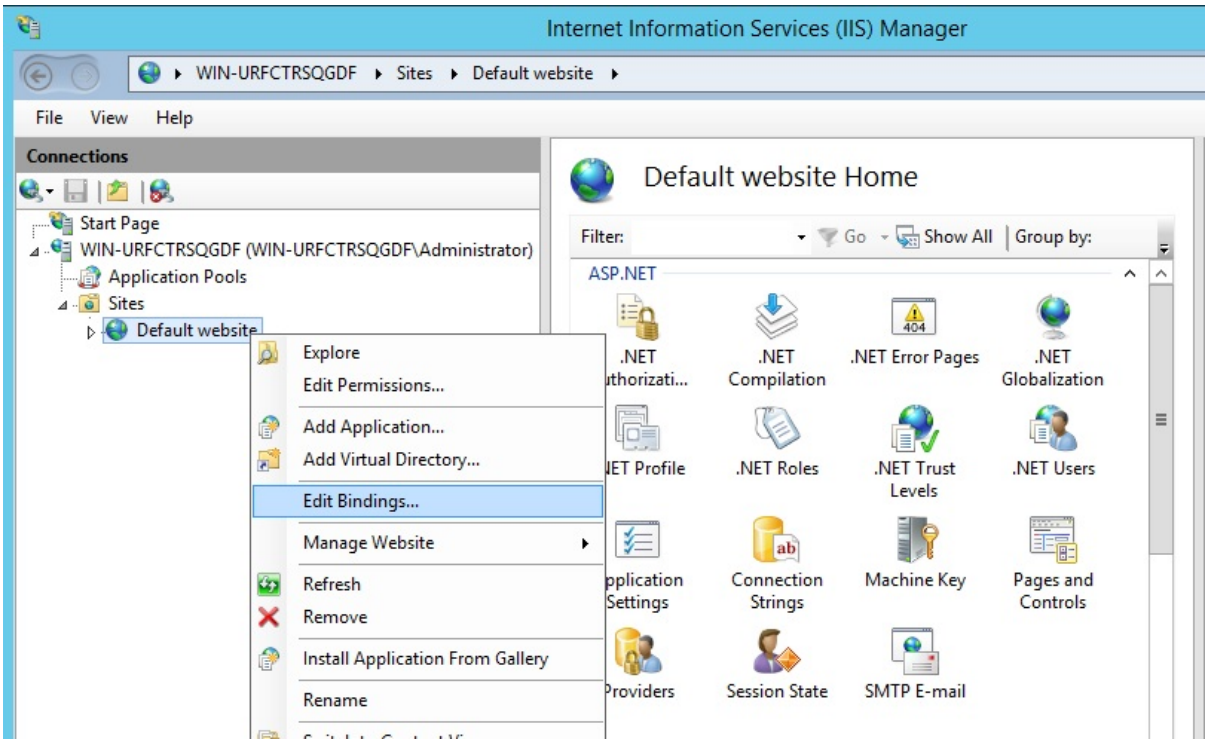
1. Configuration IIS

- Installez IIS avec les modules suivants : CGI, extensions ISAPI et filtres ISAPI.

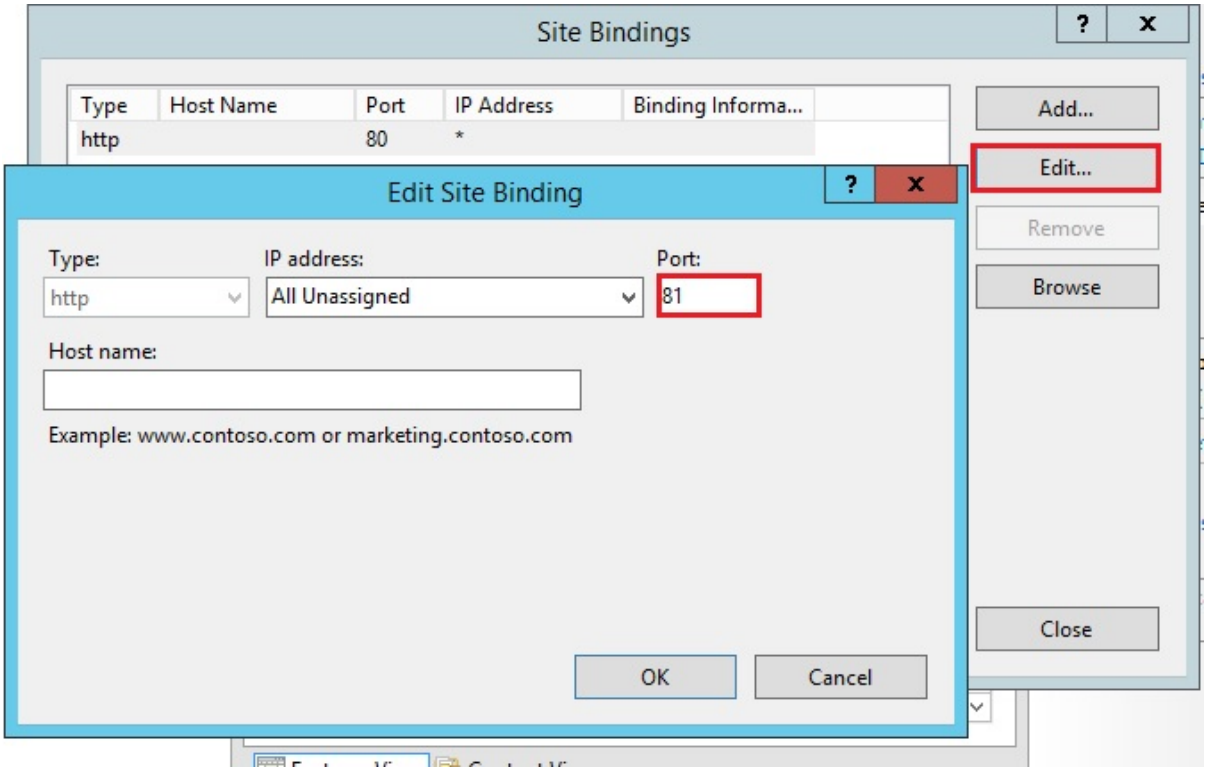


- Configurer le port IIS :

Accédez à la console de gestion IIS, développez la liste sous le nom de votre serveur, puis développez le menu "Sites", faites un clic droit sur "Default Web Site" et cliquez sur "Edit Bindings".



Cliquez sur "http" et "Modifier". Changez le port en 81 et cliquez sur Ok, puis cliquez sur Fermer :



Désactivez le port 443 ou changez ce port pour un autre port libre.

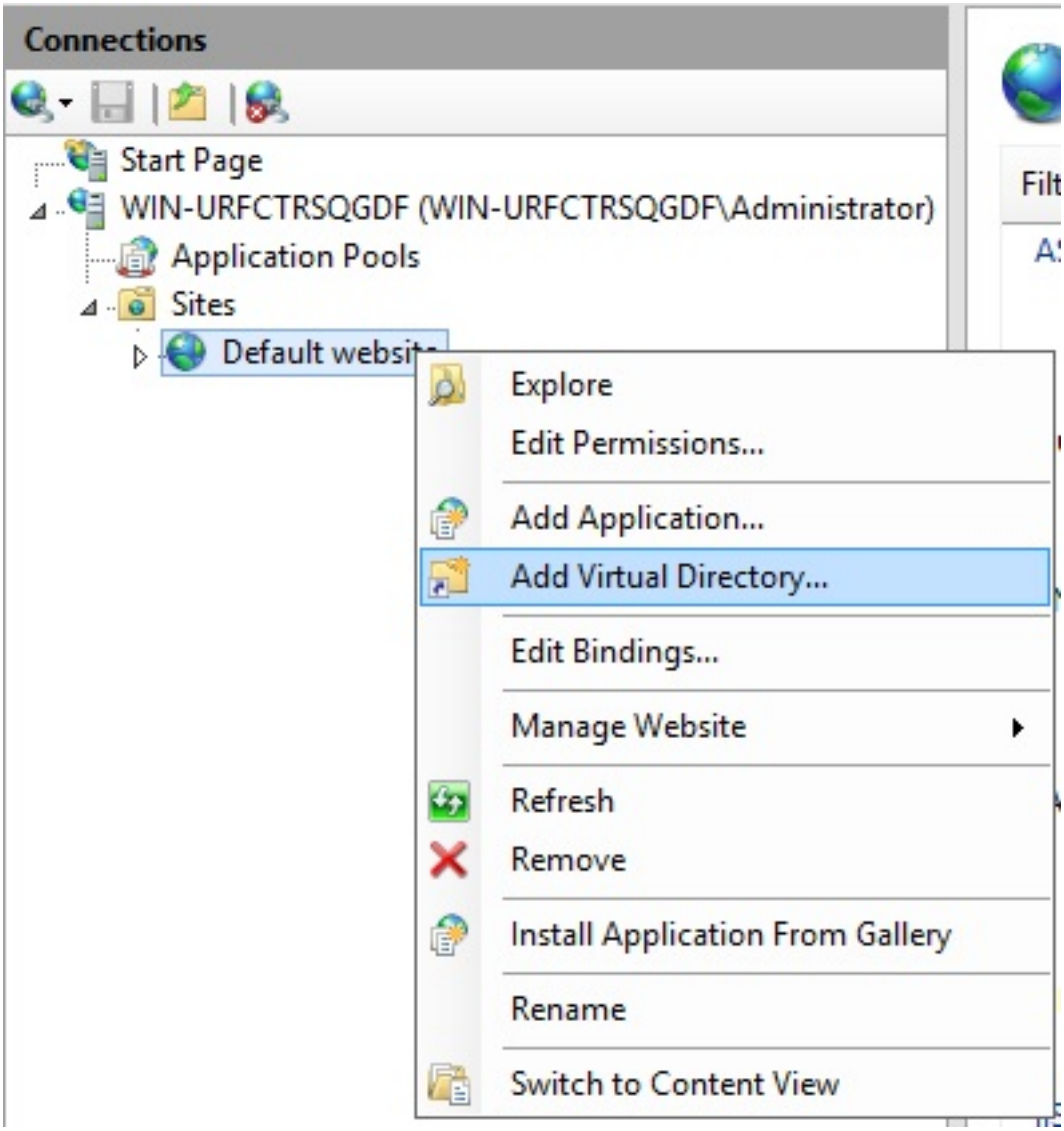
Ensuite, redémarrez le Gestionnaire IIS.

2. Créer un répertoire virtuel pour CGI

NB : Tous les fichiers du répertoire web par défaut (C:\Program Files (x86)\TSplus\Clients\www) ne sont pas copiés lorsque le répertoire racine du web est modifié.

Vous devrez les vérifier et les copier manuellement lors de la migration vers le serveur web IIS.

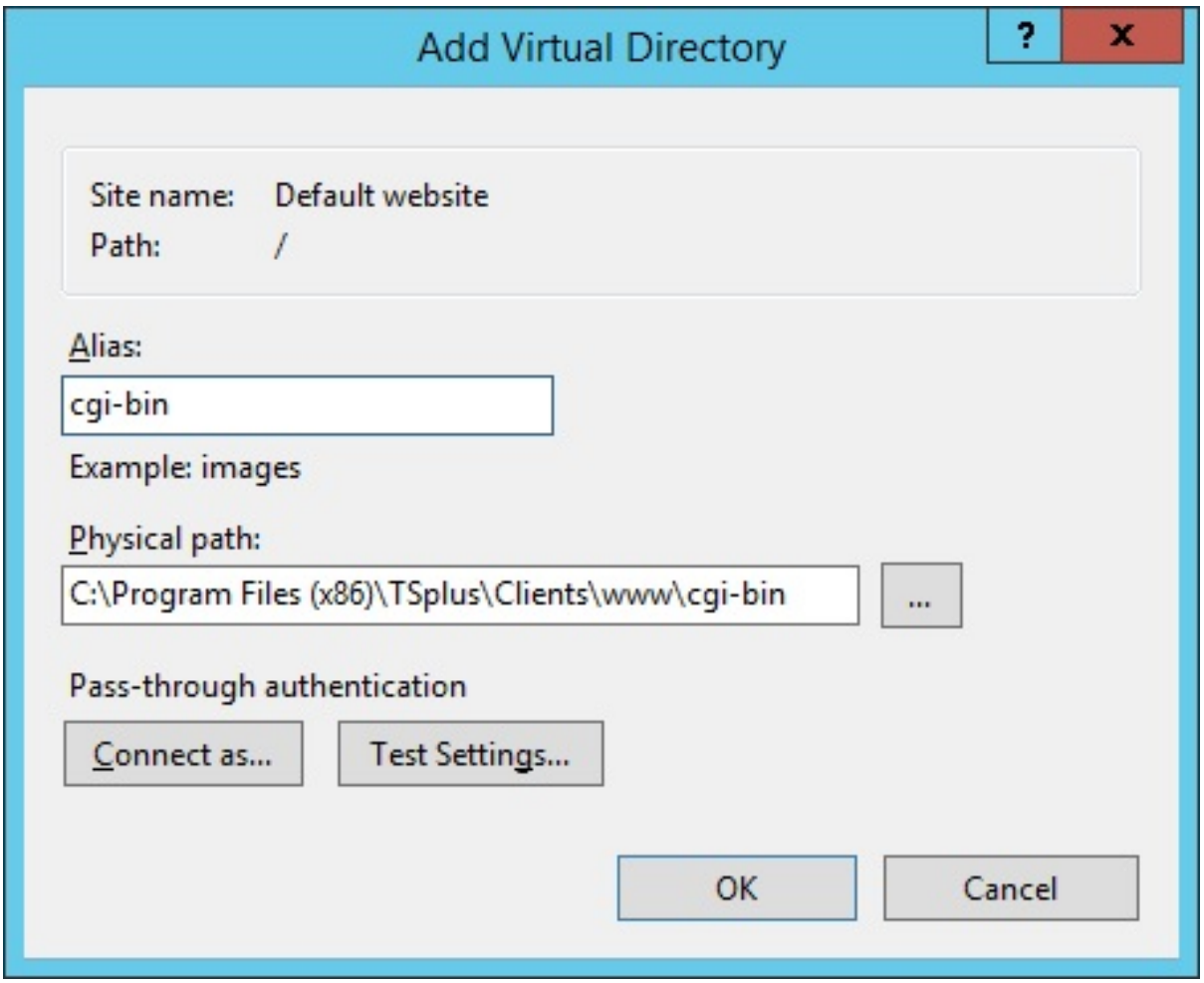
Dans le menu du panneau de gauche, développez le menu sous votre serveur, puis "Sites", et faites un clic droit sur votre site pour ajouter un nouveau "répertoire virtuel", comme indiqué dans l'image ci-dessous :



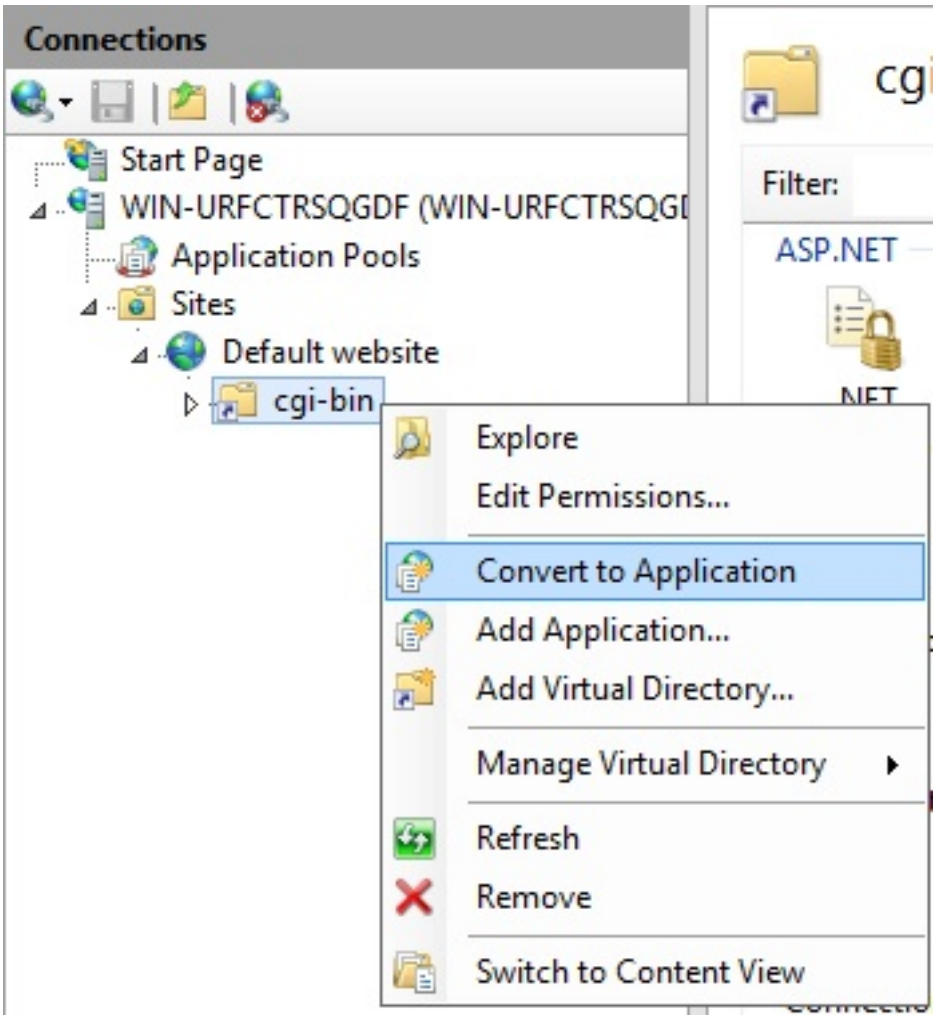
Sur la fenêtre qui s'ouvrira, remplissez comme suit :

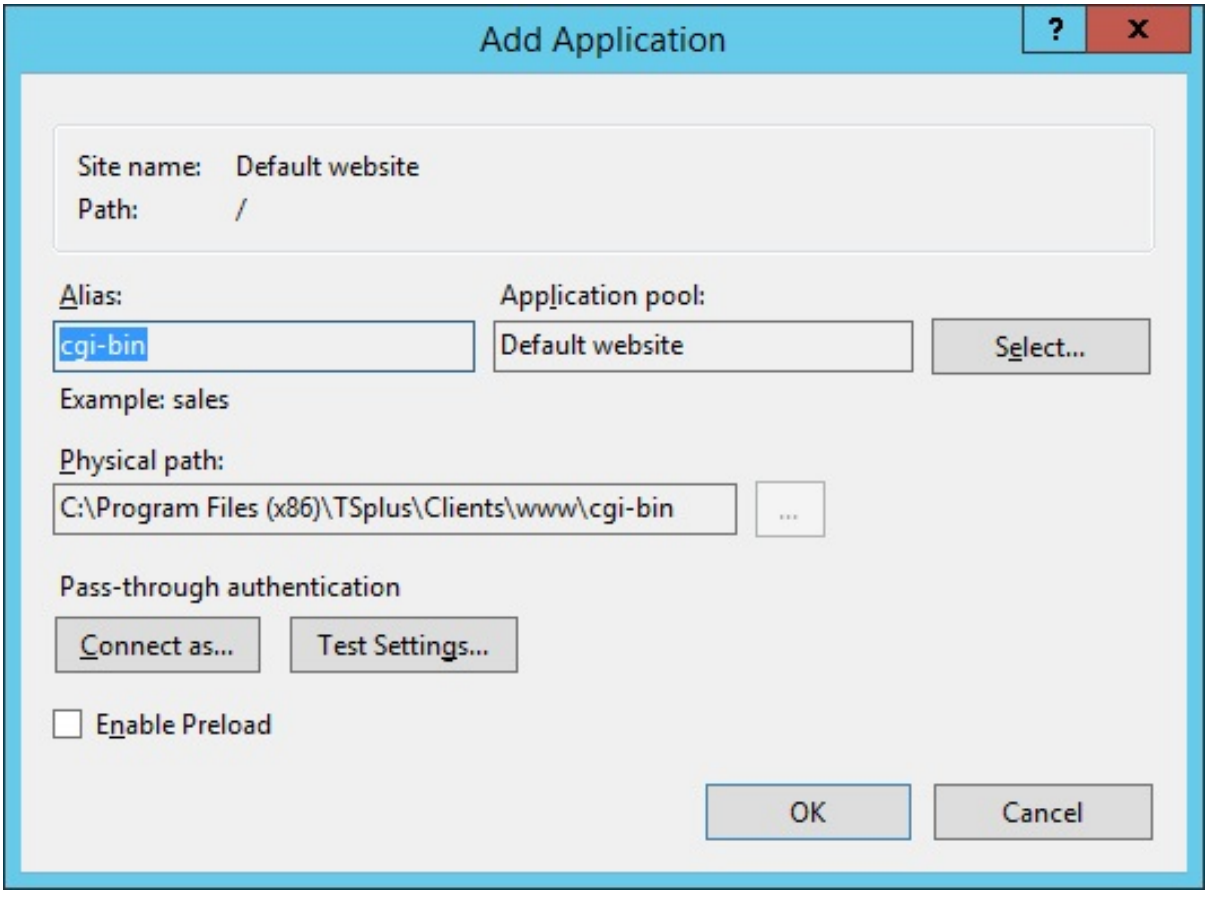
Alias : cgi-bin

Chemin physique : C:\Program Files(x86)\TSplus\Clients\www\cgi-bin

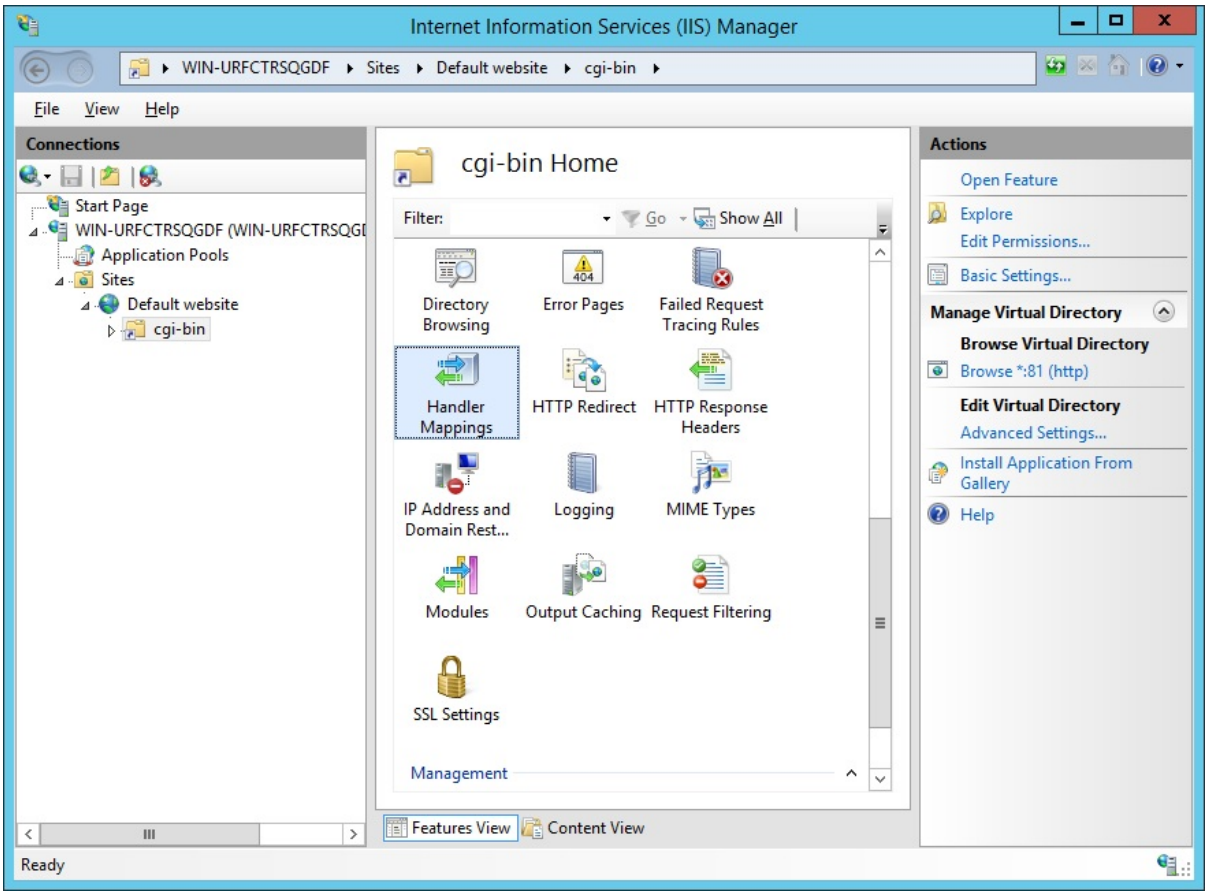


Puis cliquez sur "OK" et vous verrez que le répertoire virtuel "cgi-bin" a été ajouté à votre site Web IIS. Maintenant, faites un clic droit sur ce répertoire virtuel "cgi-bin" et cliquez sur "Convertir en application". Cliquez sur "OK" et acceptez les paramètres par défaut.


Connections
Start Page
WIN-URFCTRSQGDF (WIN-URFCTRSQGD
Application Pools
Sites
Default website
cgi-bin
Filter:
ASP.NET
Explore
Edit Permissions...
Convert to Application
Add Application...
Add Virtual Directory...
Manage Virtual Directory
Refresh
Remove
Switch to Content View

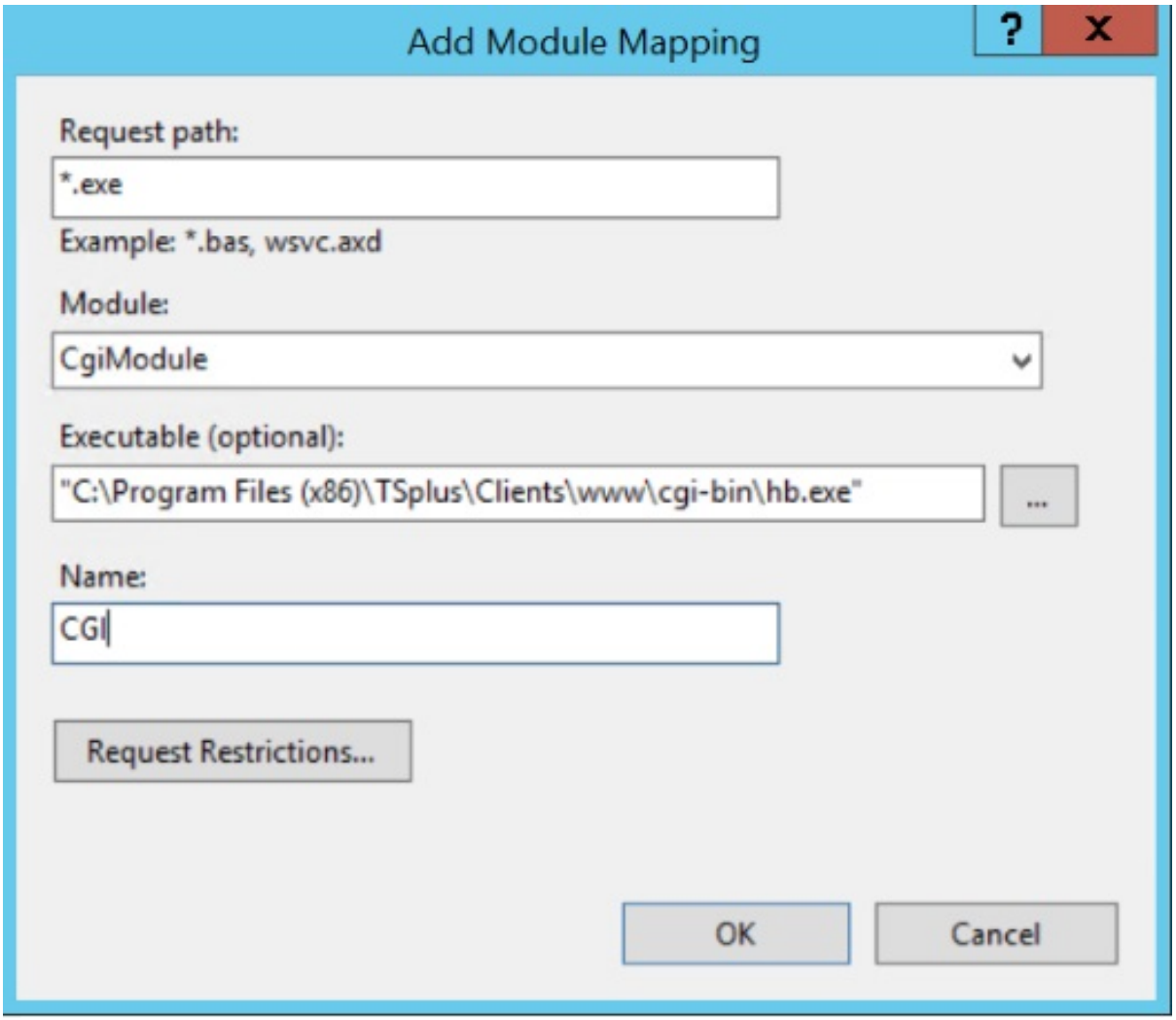

Add Application
Site name: Default website
Path: /
Alias:
cgi-bin
Example: sales
Application pool:
Default website
Select...
Physical path:
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin
...
Pass-through authentication
Connect as...
Test Settings...
Enable Preload
OK
Cancel

Ensuite, sélectionnez l'icône "Handler Mappings" pour ce dossier sur le côté droit de la fenêtre du Gestionnaire :

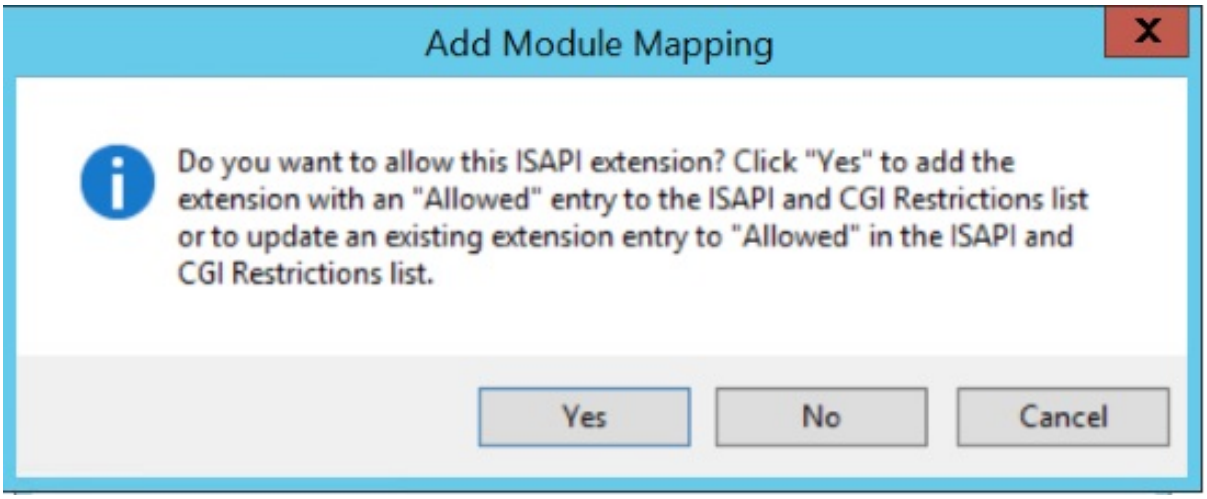


Dans la liste des mappages de gestionnaires, double-cliquez sur "CGI-exe".

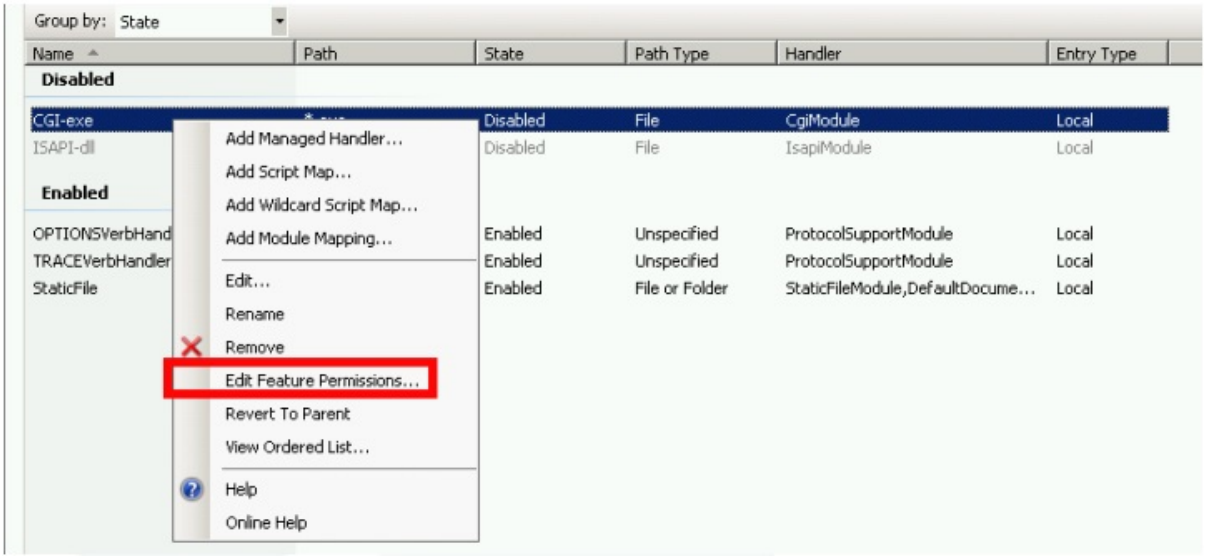
Ensuite, recherchez l'exécutable hb.exe dans la boîte de propriétés Exécutable et cliquez sur OK.



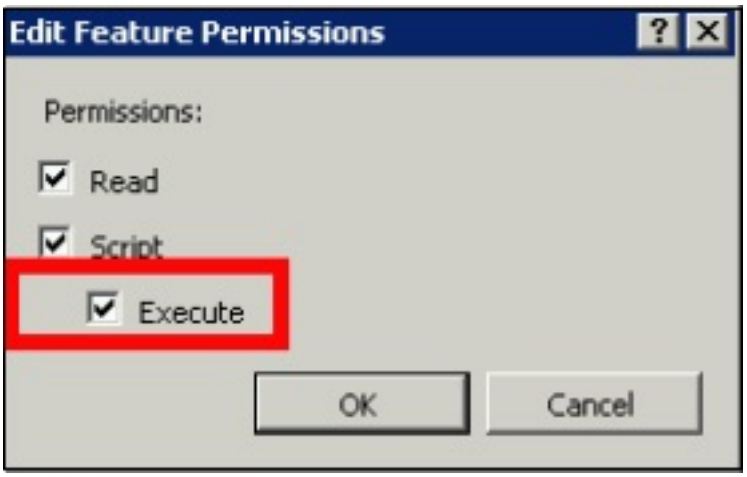
Une invite de confirmation apparaît. Cliquez sur "OK" pour autoriser cette extension ISAPI.



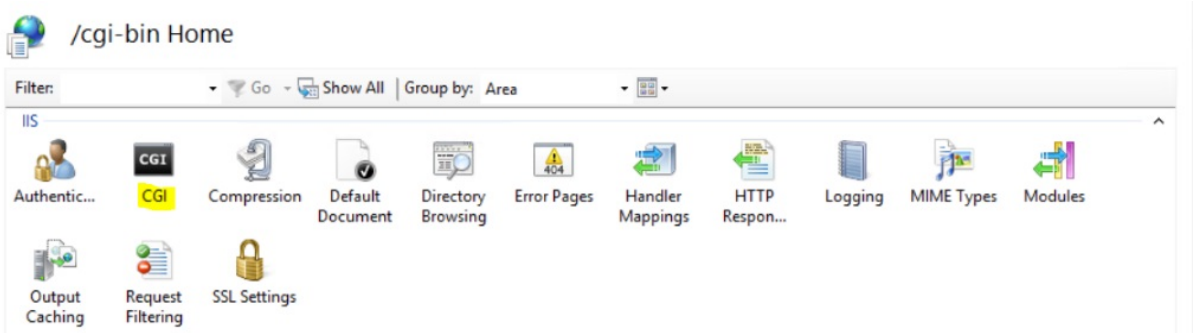
Maintenant, cliquez sur « Modifier les autorisations de fonctionnalité » :



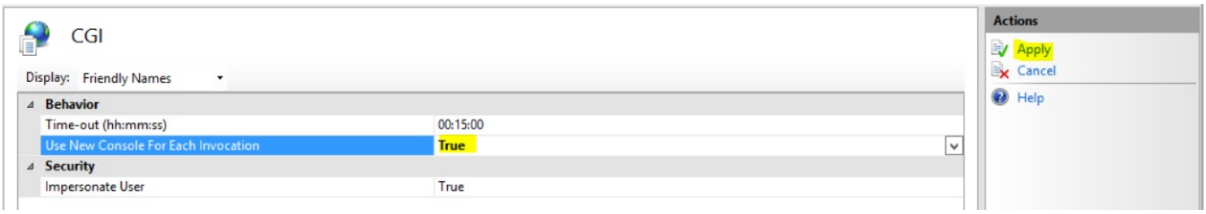
Cochez la case "Exécuter" et cliquez sur OK :



Retour à l'accueil du "CGI-bin", cliquez sur "CGI" pour ouvrir les propriétés CGI :



Changez la valeur de "Utiliser la nouvelle console pour chaque invocation" à "Vrai". Ensuite, cliquez sur "Appliquer" pour enregistrer les modifications.

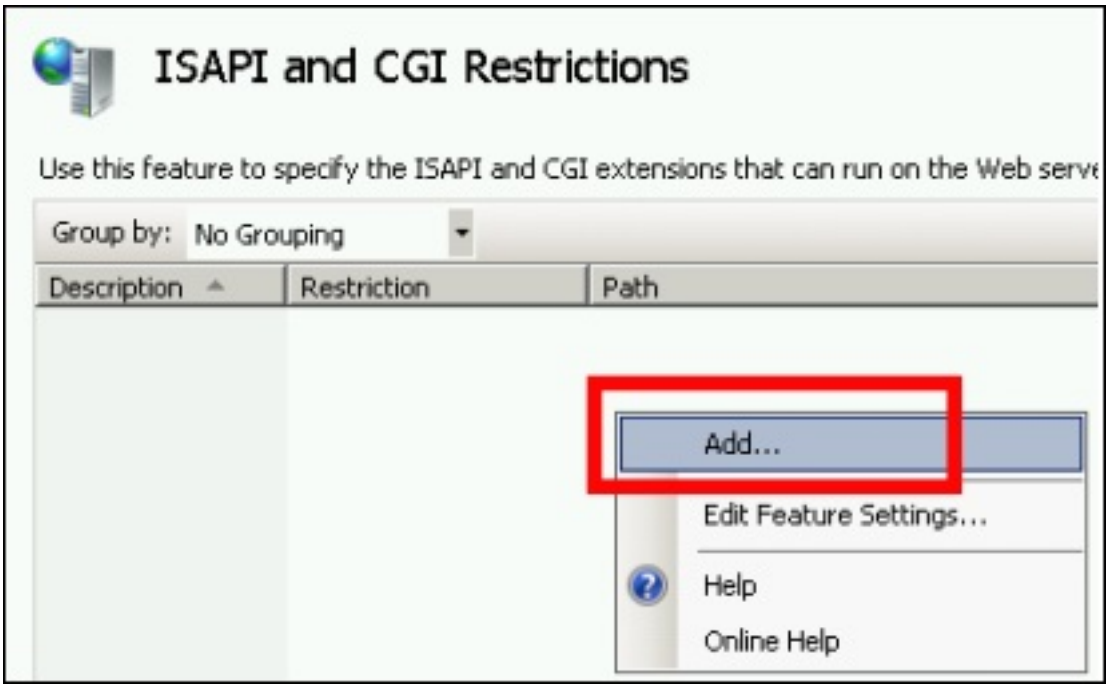


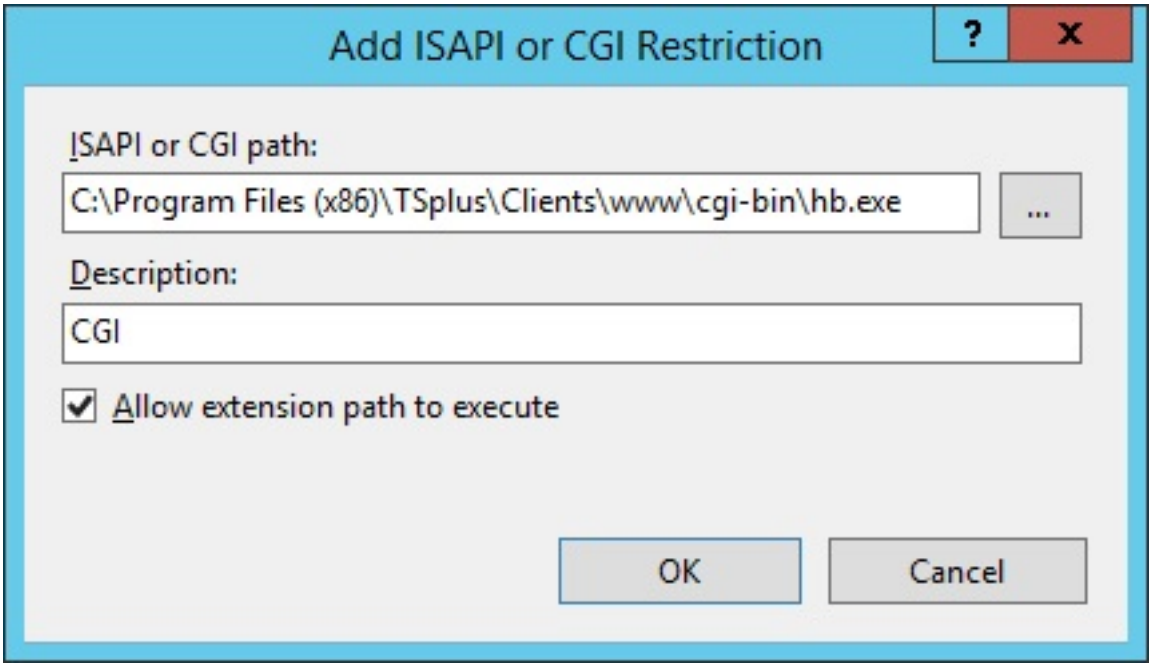
3. Configurer les autorisations d'extension CGI

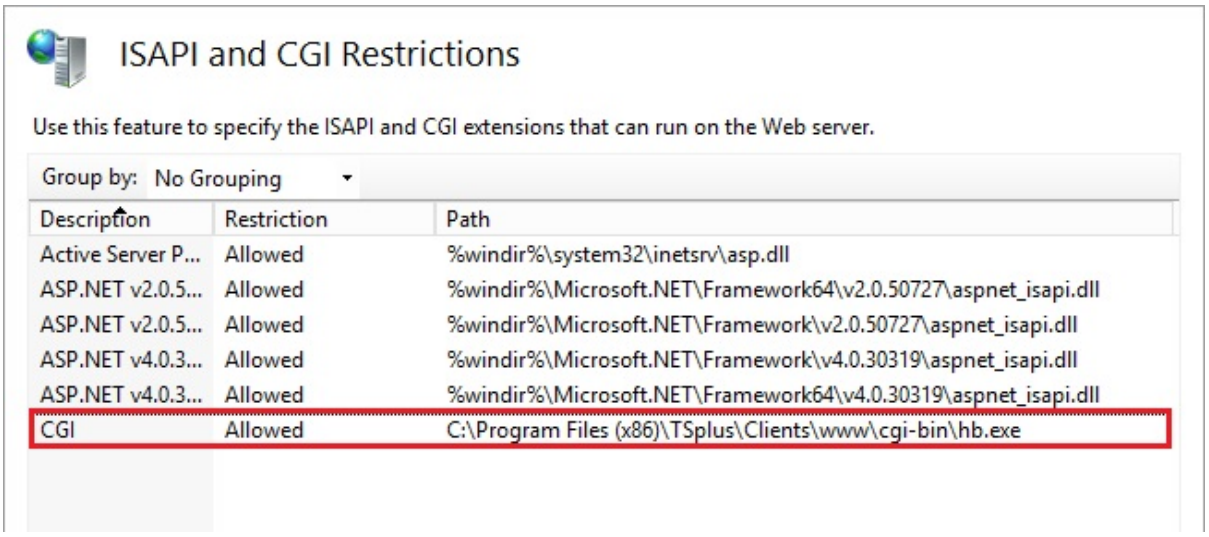
Maintenant, la dernière étape consiste à autoriser l'extension CGI à s'exécuter sur le serveur. Cliquez sur l'icône "Restrictions ISAPI et CGI". Cela peut être trouvé en cliquant sur le nom de la machine dans le menu à gauche de la fenêtre.



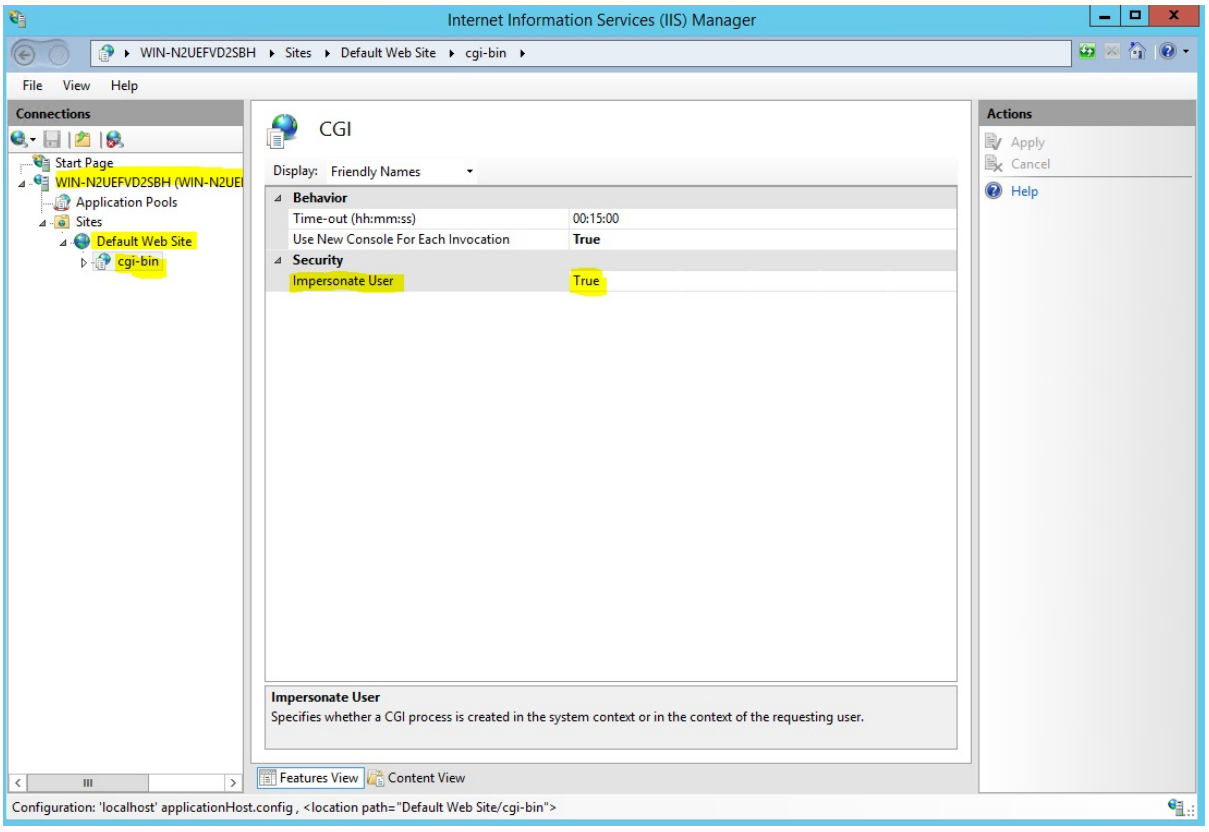
Sur la page "Restrictions ISAPI et CGI", cliquez sur "Ajouter ..." sur le côté droit de la fenêtre. Maintenant, spécifiez le chemin complet vers le fichier "hb.exe" hébergé dans le dossier TSplus. Assurez-vous de cocher l'option "Autoriser le chemin d'extension à s'exécuter", comme Illustrez les images suivantes :


ISAPI and CGI Restrictions
Use this feature to specify the ISAPI and CGI extensions that can run on the Web serve
Group by: No Grouping
Description
Restriction
Path
Add...
Edit Feature Settings...
Help
Online Help


Add ISAPI or CGI Restriction
?
X
ISAPI or CGI path:
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\hb.exe
...
Description:
CGI
Allow extension path to execute
OK
Cancel



Assurez-vous que dans la section CGI de votre serveur, "Default Web Site" et "cgi-bin", le paramètre "Impersonate User" est défini sur "True".



- Accorder tous les droits à l'utilisateur "IUSR" dans le répertoire C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- Veuillez vous assurer d'activer l'héritage des autorisations lorsque l'utilisateur IUSR est configuré pour un contrôle total sur le répertoire. C:\Program Files (x86)\TSplus\Clients\www\cgi-bin

- Accorder tous les droits à l'utilisateur "IUSR" dans le répertoire C:\Program Files (x86)\TSplus\Clients\webserver\twofa

4. Ajouter des types Mime dans IIS

Ouvrez une invite de commande en tant qu'administrateur et exécutez les commandes suivantes :

Fenêtre de terminal

```
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent
/+[fileExtension='.dat',mimeType='text/plain']
```

Fenêtre de terminal

```
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent
/+[fileExtension='.',mimeType='text/plain']
```

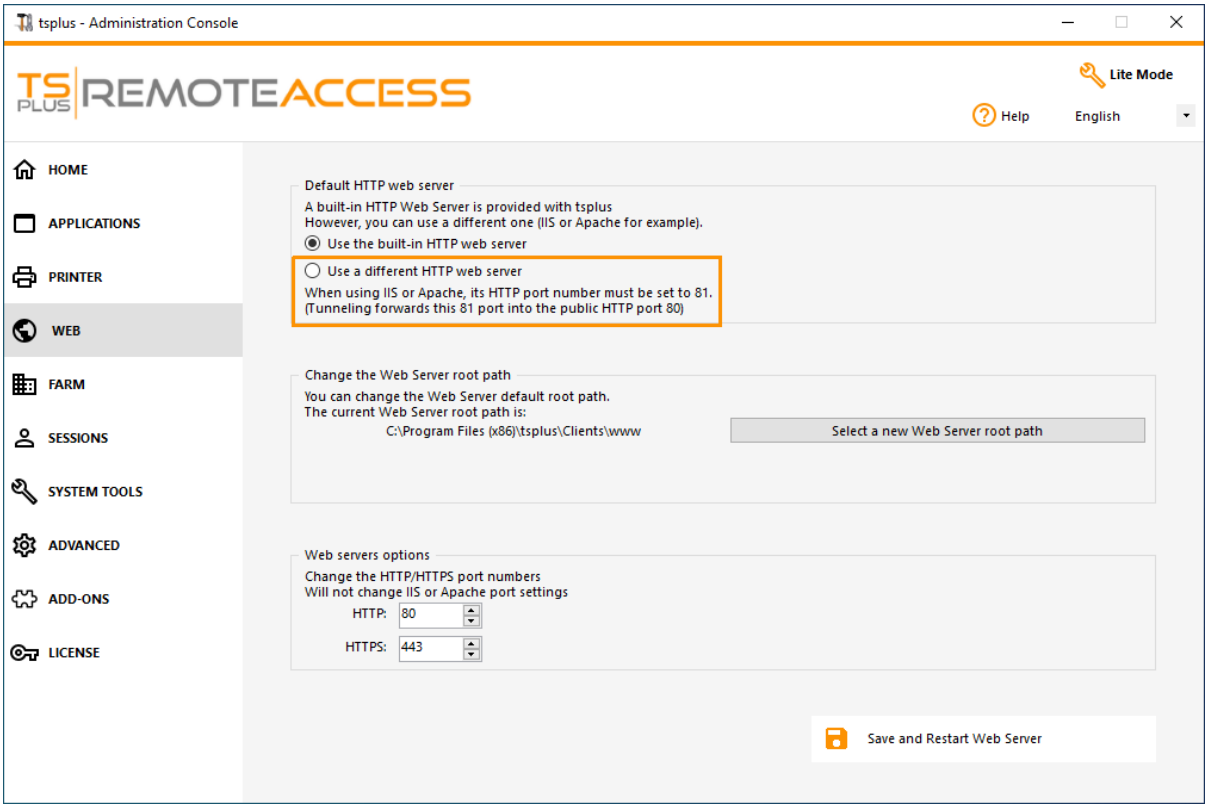
Redémarrer IIS.

5. Configurer les autorisations de répertoire IIS

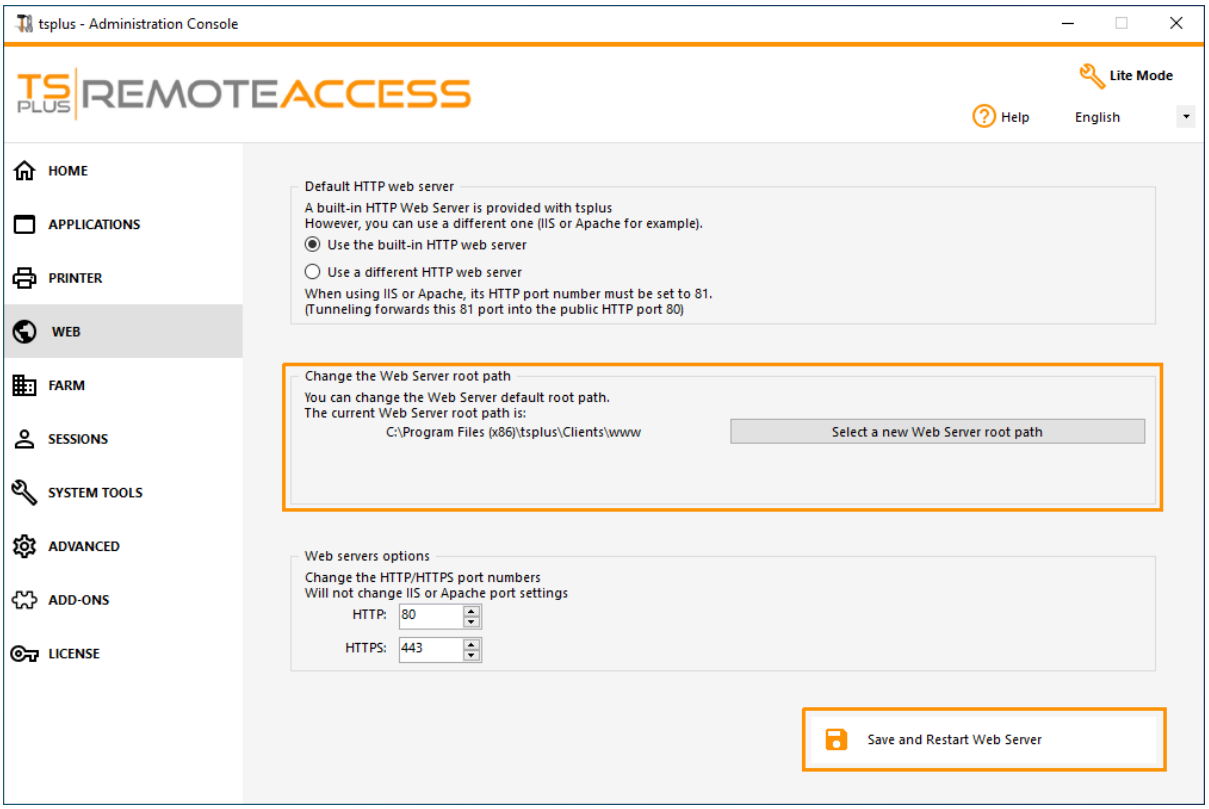
Donner toutes les autorisations au groupe « Tout le monde » dans le répertoire « C: \inetpub\wwwroot »

6. Configurer TSplus

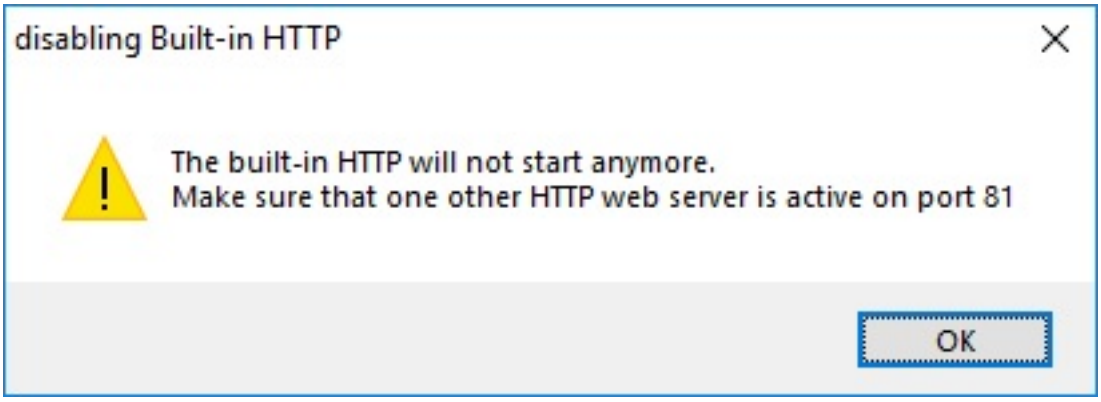
Allez dans l'onglet Serveur Web de l'AdminTool, puis choisissez l'option « Utiliser un serveur HTTP différent » :

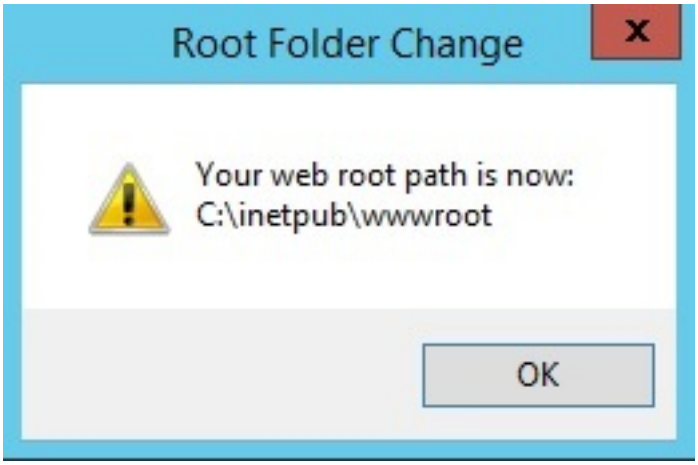


Ensuite, dans la même fenêtre, cliquez sur « Sélectionner un nouveau chemin racine de serveur Web », et mettez le chemin du répertoire IIS, qui devrait être quelque chose comme : « C: \ inetpub \ wwwroot ». Maintenant, cliquez sur « Enregistrer et redémarrer l'AdminTool ».



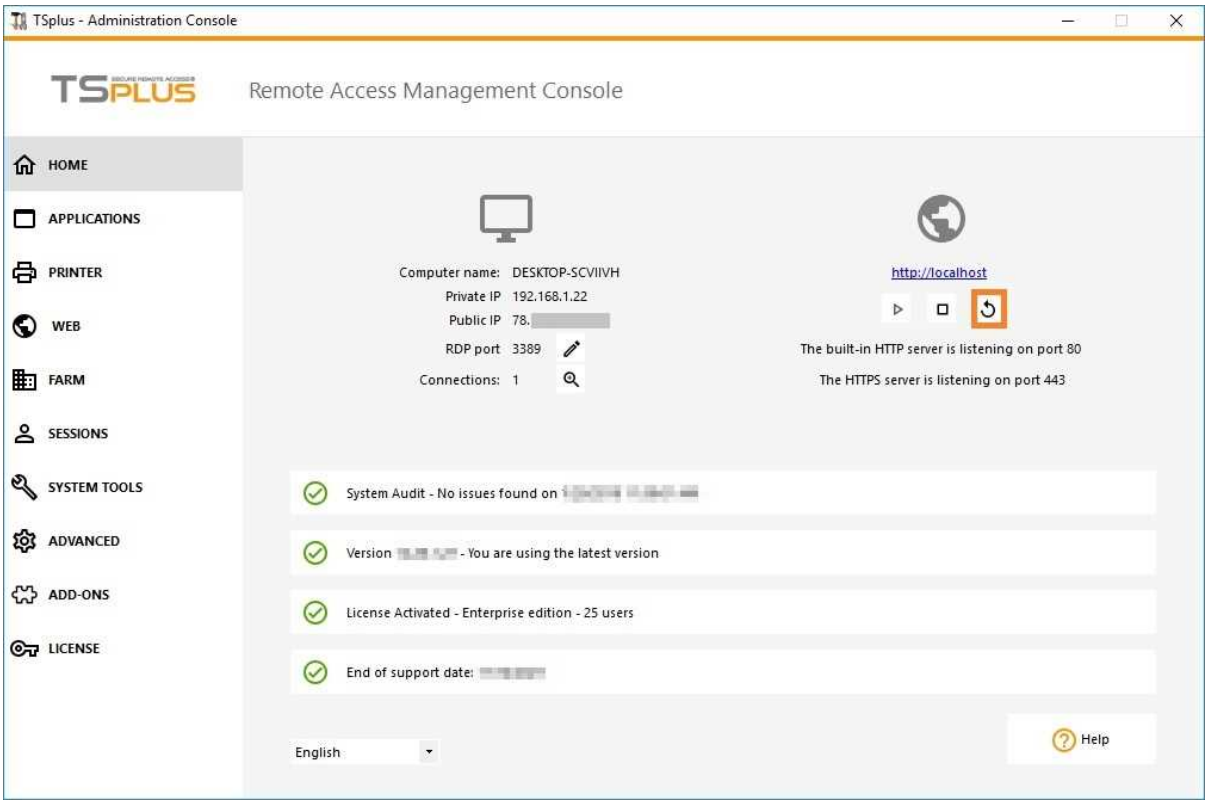
Les messages suivants apparaîtront :





Attendez. L'Admintool se fermera automatiquement. Ensuite, ouvrez à nouveau l'Admintool et cliquez sur la tuile Web.

Enfin, redémarrez les serveurs web :



7. Tester avec l'hôte local

Avertissement Utilisez un compte utilisateur différent.

Si vous essayez avec votre compte utilisateur actuel depuis votre propre session RDP vers le serveur, vous serez déconnecté et ne pourrez pas vous reconnecter.



Actions supplémentaires :

Configurer RemoteApp

Le dossier “remoteapp” dans la racine web IIS (c:\inetpub\www\cgi-bin\remoteapp) doit également avoir des autorisations complètes pour l'utilisateur IUSR, sinon une erreur 704 apparaîtra lors de la tentative d'utilisation de RemoteApp.

Configurer 2FA

Sur une installation fraîche où 2FA n'a jamais été activé, il n'y a pas de dossier nommé C:\Program Files (x86)\TSplus\Clients\webserver\twofa, ou le fichier twofactorauth.ini.

Il est nécessaire :

- activez 2FA dans AdminTool pour créer ce dossier et ce fichier .ini
- puis désactiver 2FA
- puis appliquez les autorisations d'utilisateur IUSR au nouveau dossier twofa créé.

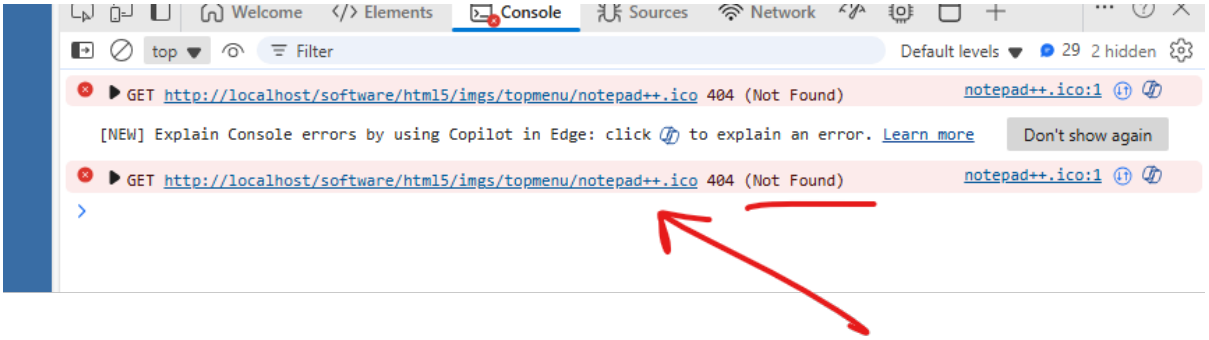
L'échec de la réalisation de cette étape (même si vous n'avez pas l'intention d'utiliser 2FA) empêchera les utilisateurs de se connecter avec un message d'erreur indiquant que les identifiants sont invalides.

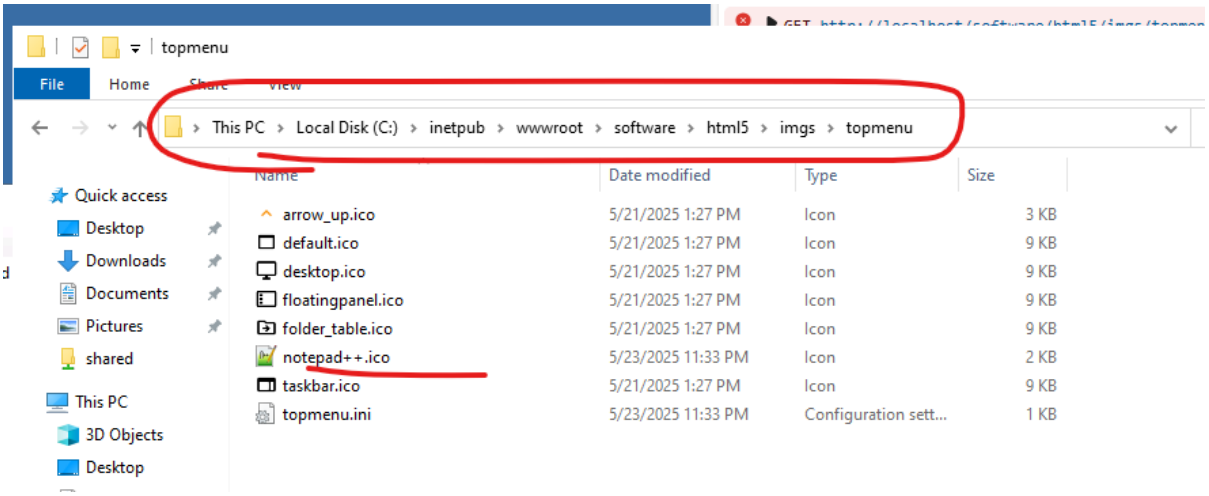
8. Autoriser l'échappement double

Pour autoriser les téléchargements, vous devez activer « Autoriser l'échappement double » dans le filtrage des requêtes au sein d'IIS. Ce changement permettra à IIS de gérer correctement les caractères spéciaux comme « + » dans les noms de fichiers. Voici comment activer « Autoriser l'échappement double » dans IIS :

1. Ouvrir le Gestionnaire IIS : Lancez le Gestionnaire des services Internet (IIS).

2. Naviguez vers le filtrage des demandes : dans le Gestionnaire IIS, sélectionnez le dossier ou le site Web contenant le fichier avec le caractère ”+”. Ensuite, double-cliquez sur “Filtrage des demandes” dans la vue des fonctionnalités.

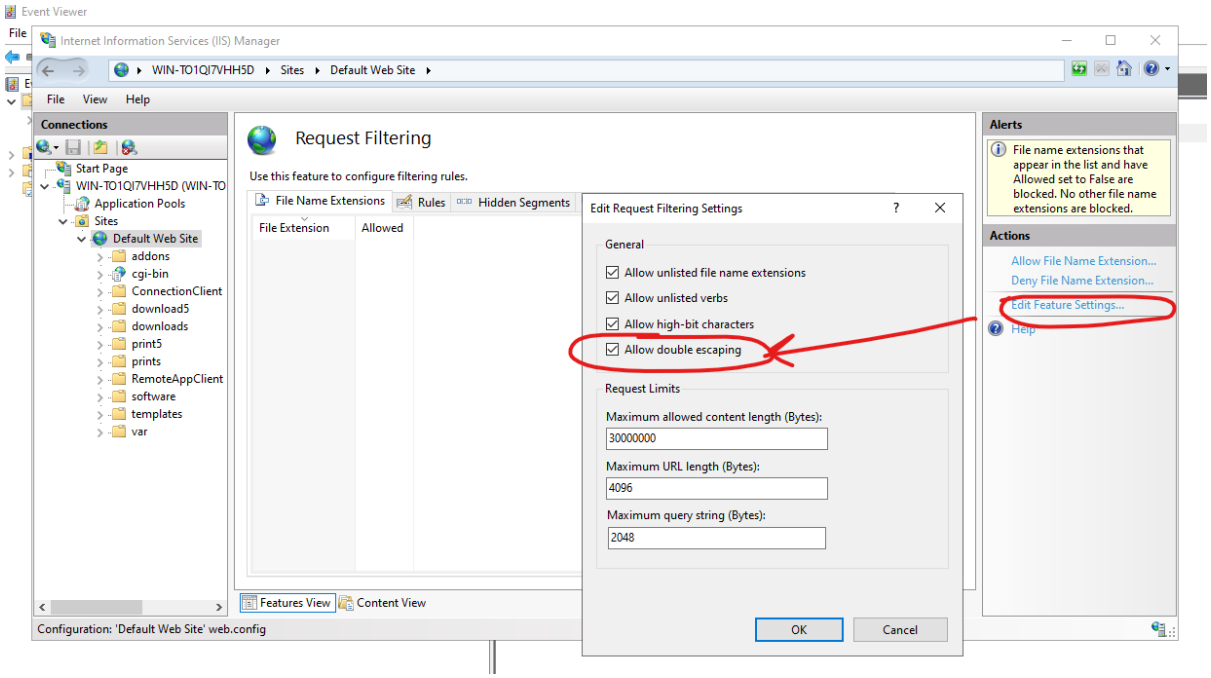




3. Modifier les paramètres de fonctionnalité : dans le volet Actions, cliquez sur « Modifier les paramètres de fonctionnalité ».

4.

Activer l'autorisation de double échappement : Dans la boîte de dialogue Modifier les paramètres de filtrage des demandes, cochez la case "Autoriser le double échappement".



5. Redémarrer IIS (optionnel) : Le redémarrage d'IIS peut aider à garantir que les modifications prennent effet.

Utiliser des serveurs derrière un proxy inverse

Il est possible d'utiliser des serveurs derrière des proxies inverses via xhr-polling, avec certaines limitations.

Comme décrit Les Websockets ne font pas partie du protocole HTTP, même si la première requête http ressemble à une requête http, en réalité, ce n'est pas le cas, par conséquent, la plupart des reverse proxies connus ne prennent pas en charge les Websockets et abandonnent de nombreux domaines importants de la première requête Websocket.

Si vous savez que le serveur est derrière un proxy inverse, désactivez les Websockets en définissant cette option dans Clients\www\software\html5\settings.js :

disablewebsocket = true;

Cela imposera l'utilisation de XHR-polling et éviter le délai lors de la connexion.

Si vous n'avez pas de fichier nommé "settings.js" dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software\html5", alors votre version de TSplus est plus ancienne et cette documentation ne s'applique pas. Veuillez d'abord mettre à jour votre système ou contacter le support.

Veuillez noter que l'utilisation du XHR-polling n'est pas aussi stable que celle des Websockets en raison de la nature de sa connexion.

La autre limitation de l'utilisation du polling Xhr via un proxy inverse est le mauvais support pour le téléchargement de fichiers. Lorsqu'on travaille avec XHR en connexion directe, effectué par exemple via un proxy inverse Apache, Apache peut accidentellement interrompre le téléchargement du fichier.

TSplus Virtual Printer v2

Une nouvelle version de Virtual Printer est maintenant disponible !
Cette version inclut une mise à jour importante du composant Virtual Printer (v1.x -> v2.x).

Pourquoi : l'imprimante virtuelle v2 est le dernier produit phare de Fabulatech, apportant de nombreuses améliorations et corrigeant des problèmes signalés par les clients.

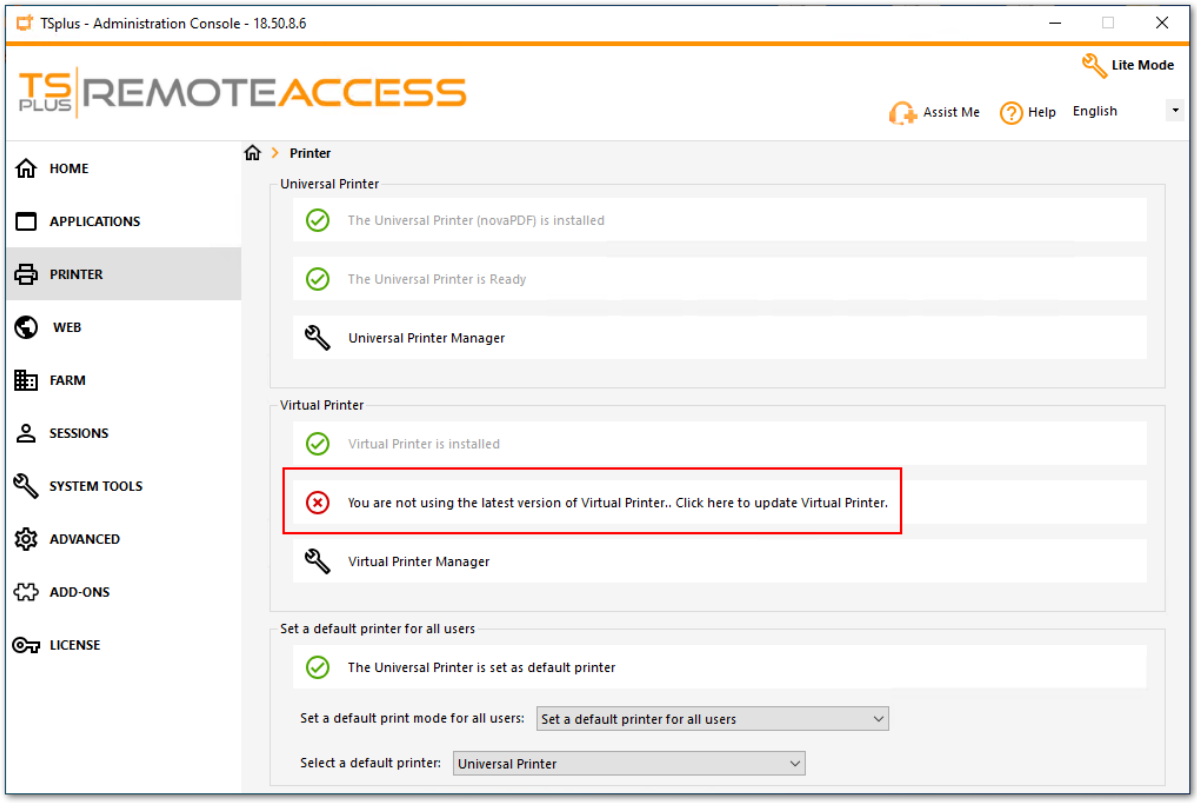
Attention : Virtual Printer v1.x et v2.x ne sont pas compatibles, vous devez avoir la même version majeure des deux côtés, client et serveur, pour fonctionner correctement.

Ne paniquez pas : la mise à jour ne contient que les nouveaux programmes de configuration de l'imprimante virtuelle (client et serveur).
Ils sont situés dans C:\Program Files (x86)\TSplus\UserDesktop\files\addons .
C'est à vous de déclencher manuellement la mise à jour réelle de l'imprimante virtuelle depuis AdminTools.

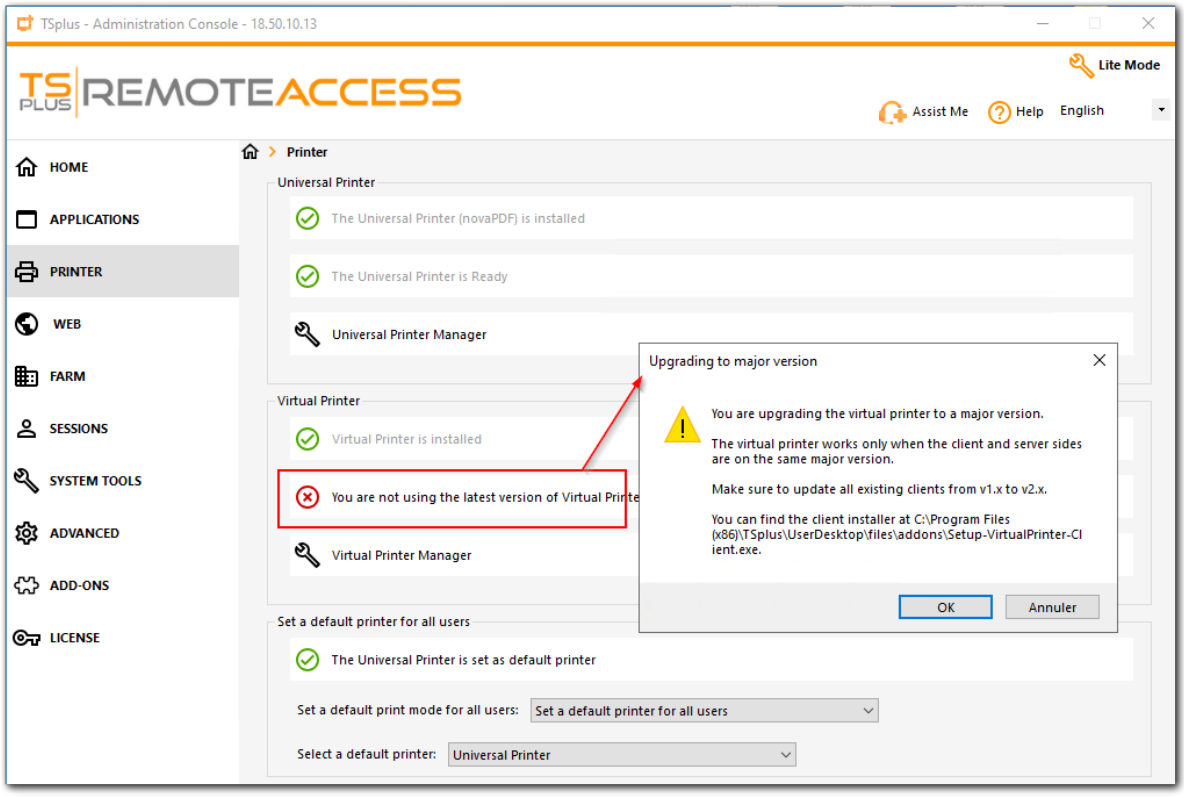
Liens : TSplus Configuration Complète Mise à jour de TSplus Mise à jour de la marque

Comment mettre à jour ?

Après avoir installé la mise à jour, AdminTools détectera qu'une nouvelle version de l'imprimante virtuelle est disponible.
Jusqu'à ce que vous cliquiez sur le bouton « mise à jour de l'avis », la version de votre imprimante virtuelle actuellement installée reste inchangée, et tout continuera de fonctionner comme avant.

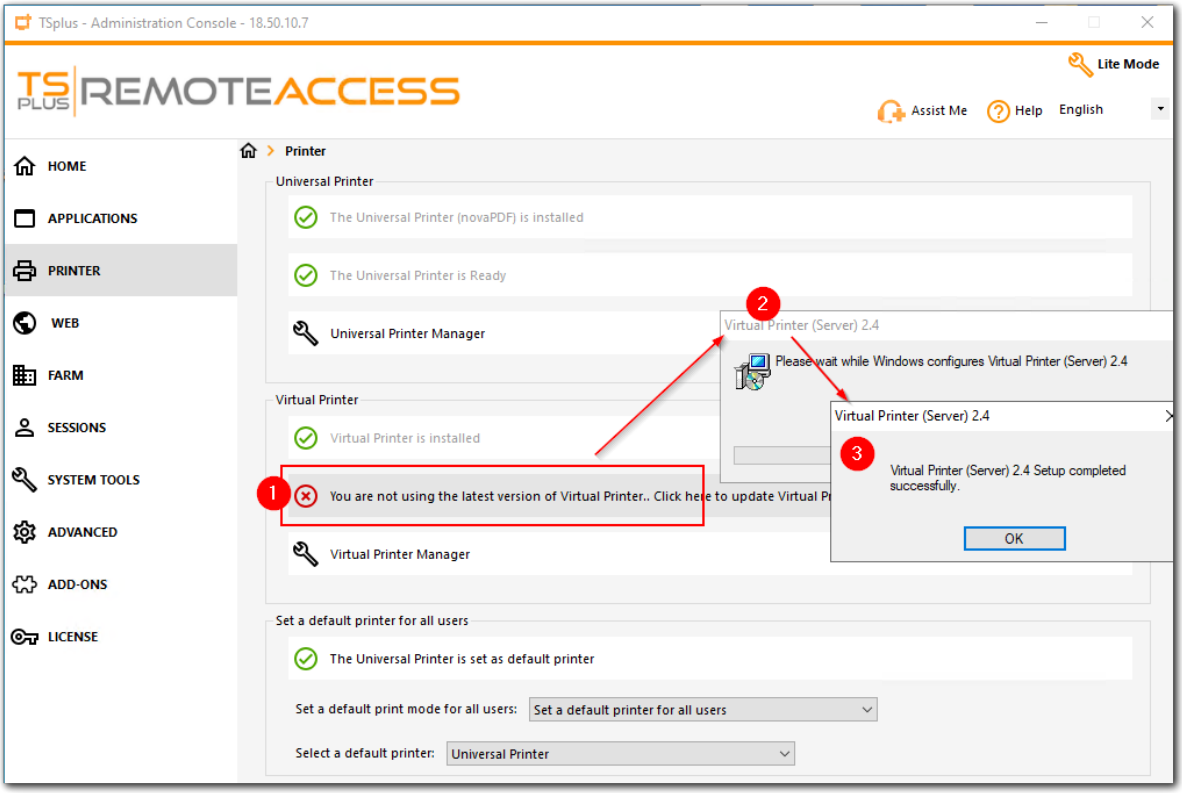


D'accord, mais nous sommes ici pour installer la nouvelle version VP, alors cliquons sur le bouton "mettre à jour l'avis".

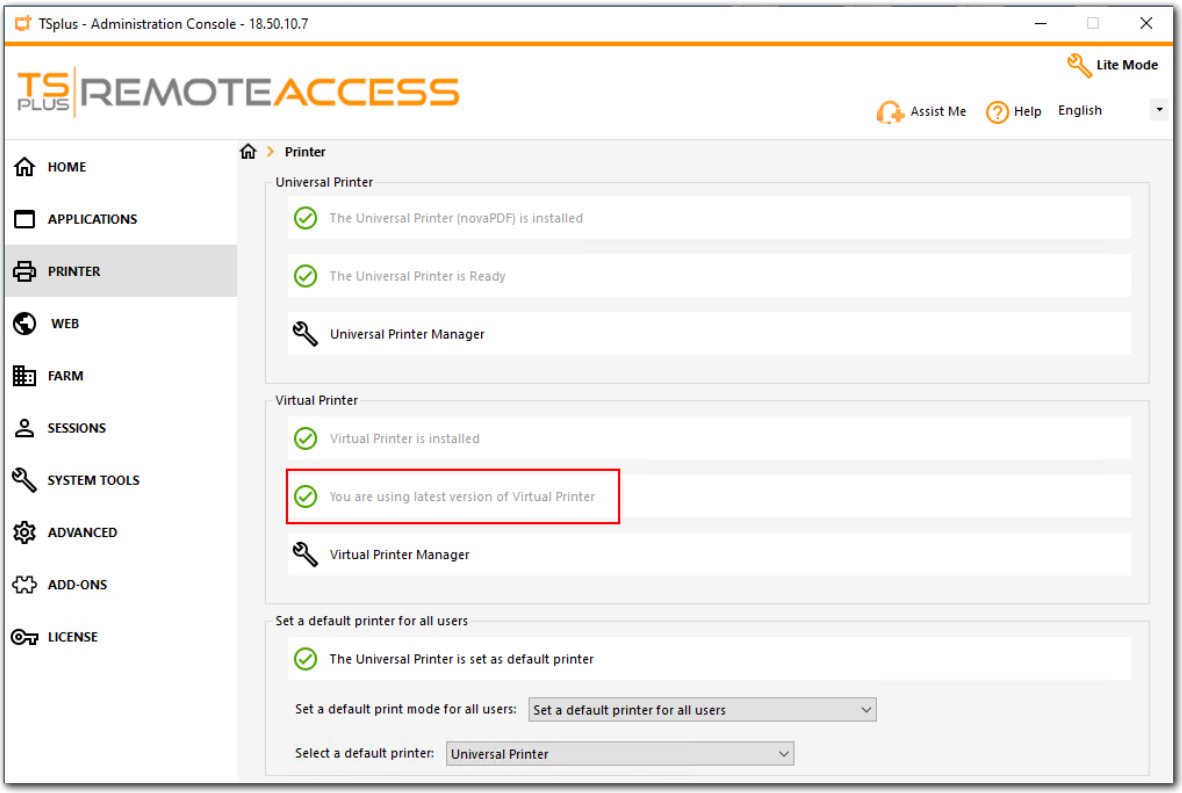


Une boîte de dialogue de confirmation demande si vous souhaitez vraiment mettre à jour

l'imprimante virtuelle vers la prochaine version majeure. Cliquez sur "OK".



Une fois installé, les AdminTools détectent que vous êtes à jour.



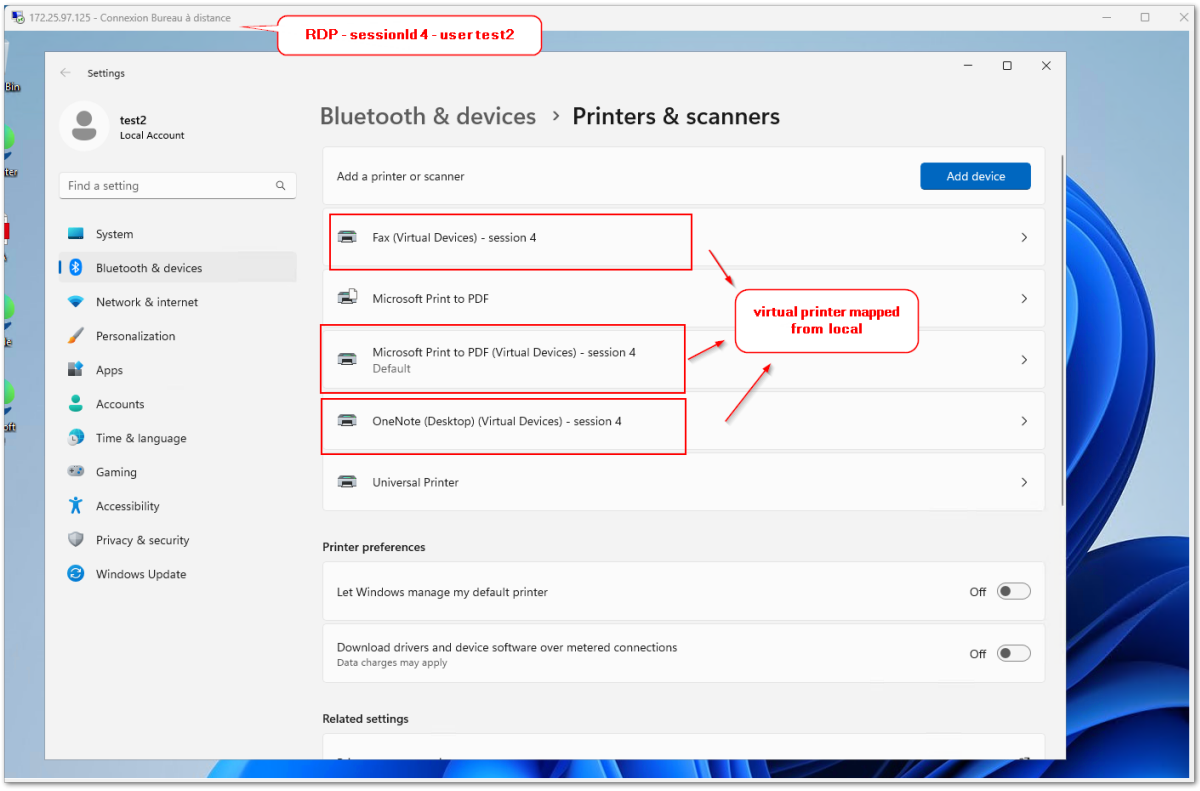
Attention : à ce stade, seuls les clients exécutant la même version majeure (v2.x) peuvent imprimer via l'imprimante virtuelle sur ce serveur. Assurez-vous de coordonner la mise à jour du serveur et des clients. L'installateur client se trouve dans “C:\Program Files (x86)\TSplus\UserDesktop\files\addons\Setup-VirtualPrinter-Client.exe”

Changement majeur !

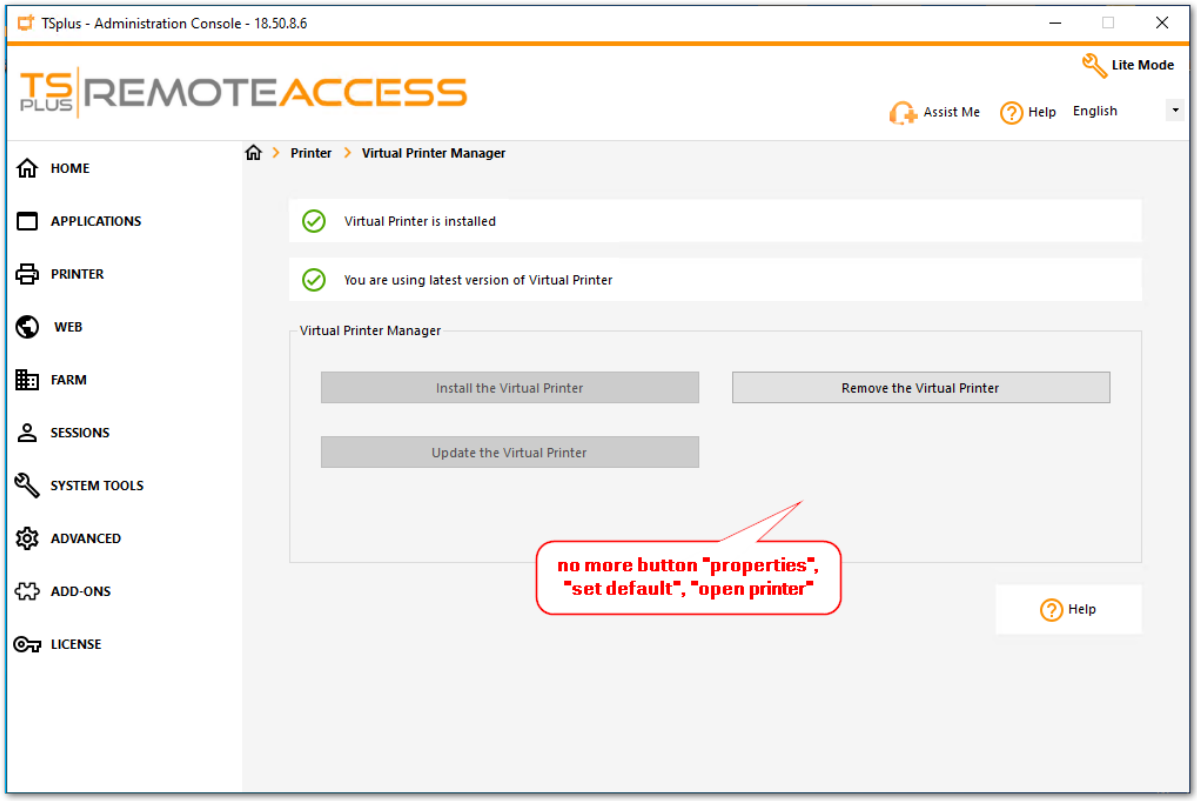
Il n'y a plus un seul appareil "Virtual Printer" dans la liste des imprimantes. Au lieu de cela, chaque imprimante locale est maintenant mappée à une imprimante virtuelle correspondante dans la session RDP.

Dans la capture d'écran ci-dessous, l'utilisateur "test2" est connecté à la session RDP n°4. Lors de l'ouverture du panneau des imprimantes,
il peut voir et utiliser ses imprimantes locales. Chaque nom d'imprimante suit ce format : $printerName (Appareils Virtuels) - session $sessionId .

Le fait que l'utilisateur voit désormais chacun de ses imprimantes locales individuellement est une amélioration majeure de l'expérience utilisateur, et c'est pourquoi Fabulatech pousse vers cette nouvelle version.

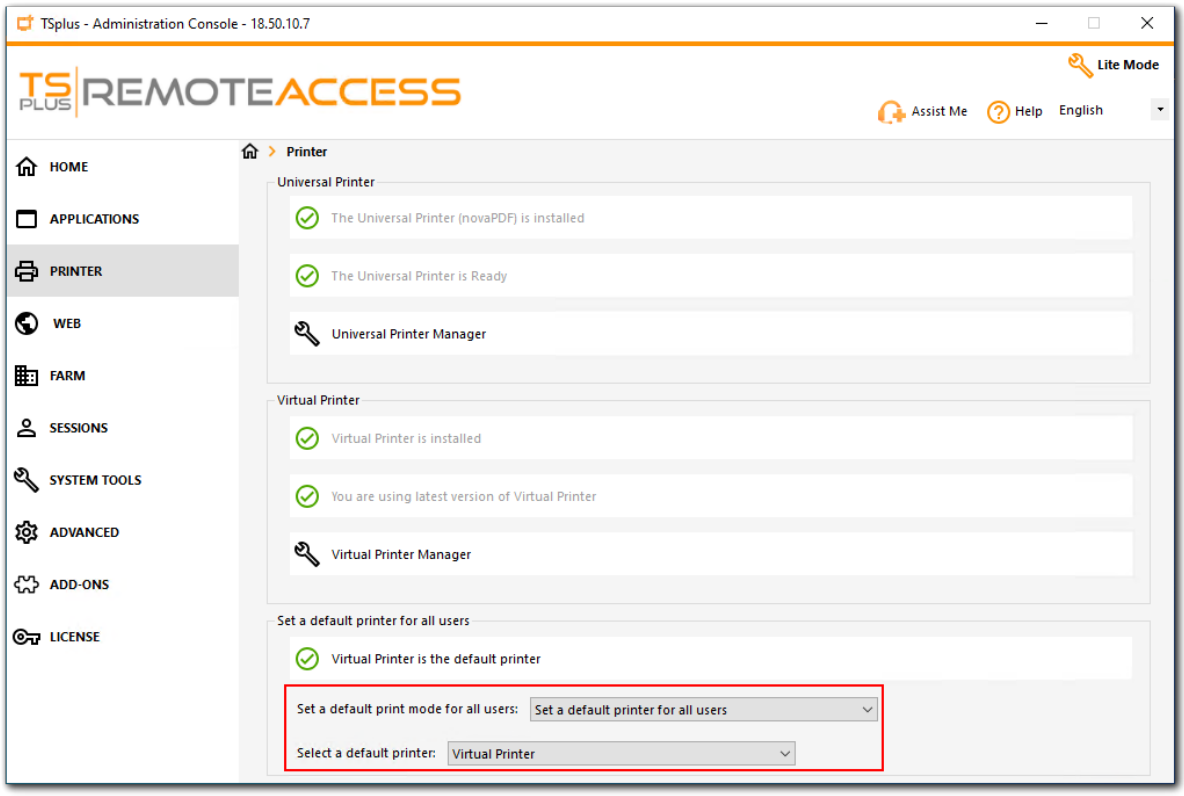


En raison de cela, nous avons ajusté certaines parties de l'interface utilisateur des AdminTools, comme le Gestionnaire d'imprimante virtuelle : certains boutons ont été supprimés.

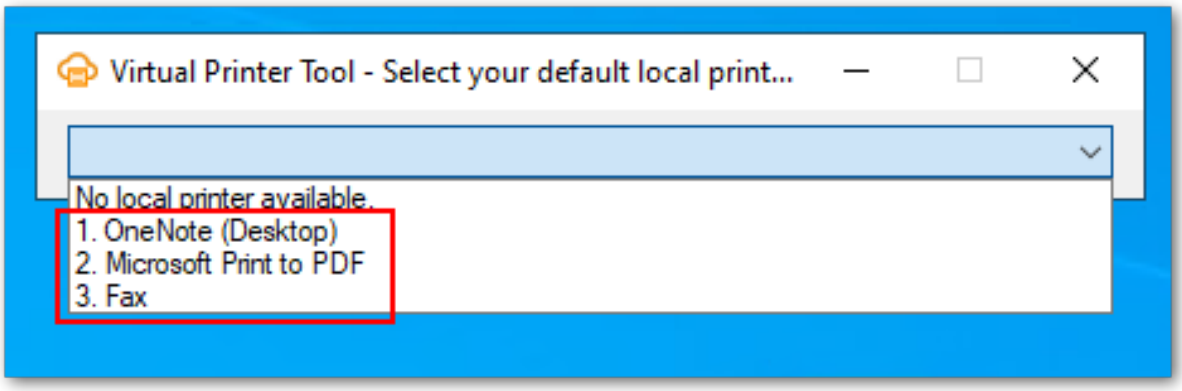


Comment configurer ?

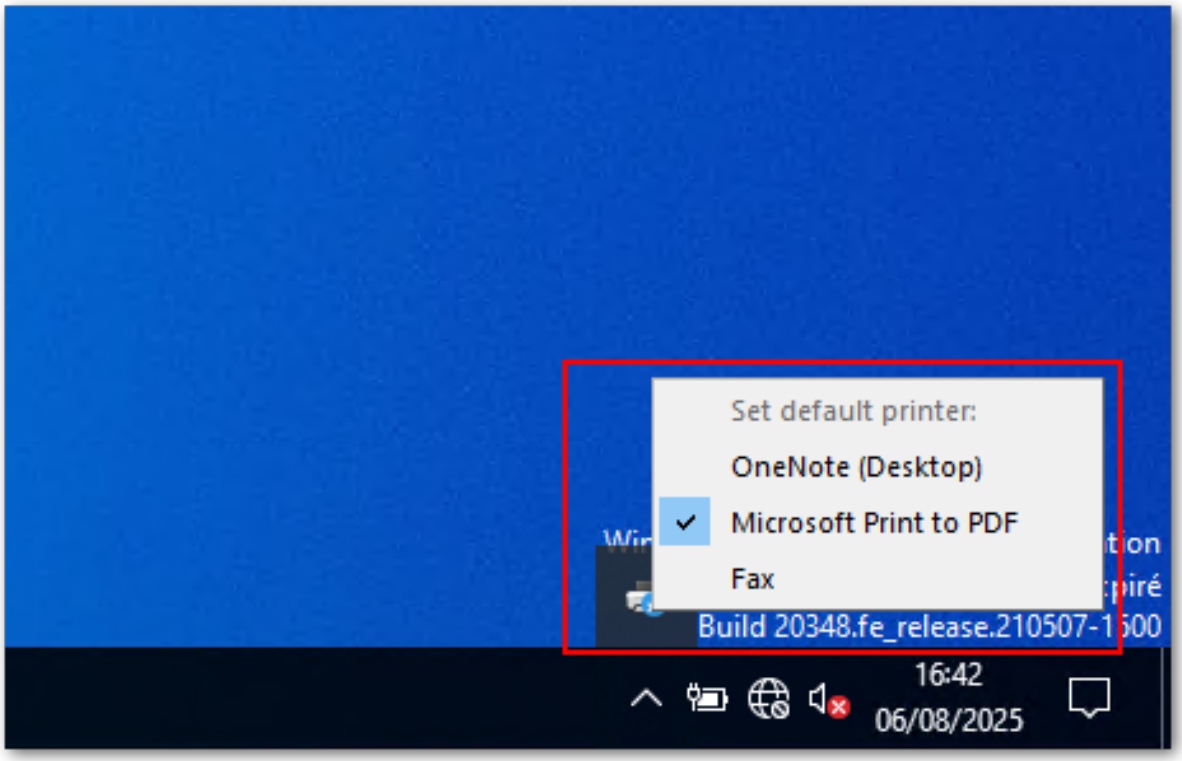
La configuration reste toujours la même dans les AdminTools et devrait fonctionner comme avant.



Si vous utilisez les outils de l'imprimante virtuelle, rien ne change et cela fonctionne comme avant.



Si vous utilisez le sélecteur dans la barre d'outils, rien ne change et cela fonctionne comme avant.



Comment personnaliser le nom des périphériques de l'imprimante virtuelle mappés ?

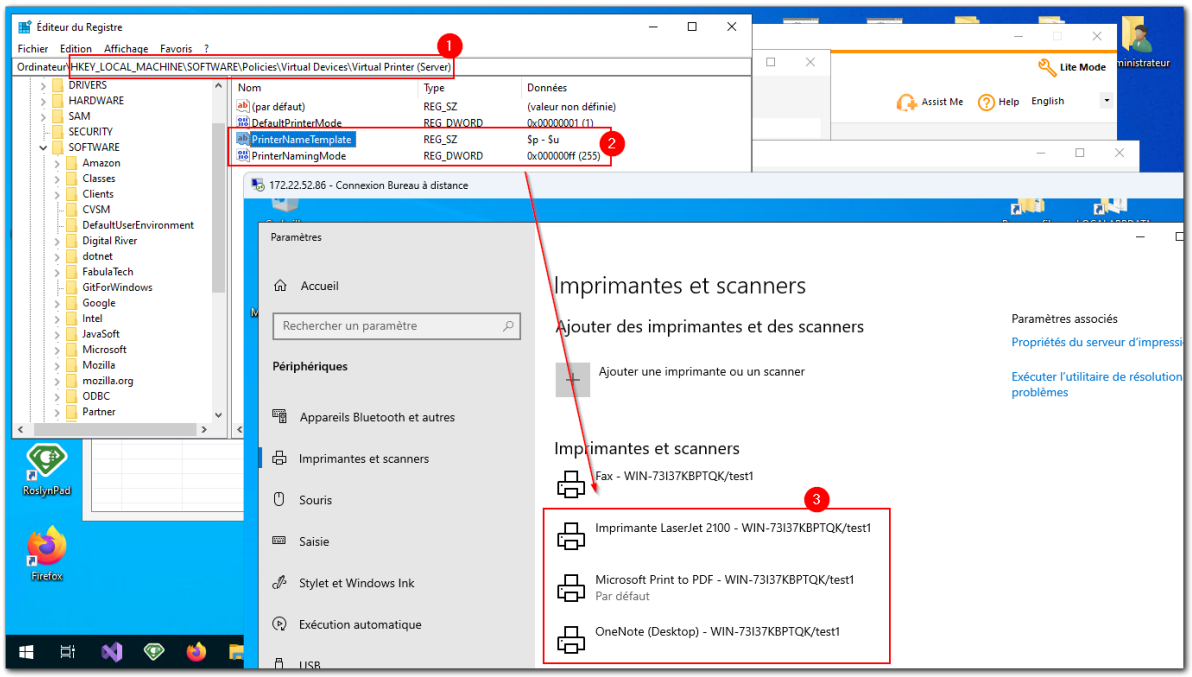
Sur le serveur, exécutez le fichier joint “customize-virtual-printer-name.reg”. Télécharger

Il ajoutera 2 clés dans votre registre HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Virtual Devices\Virtual Printer (Serveur)
Le PrinterNameTemplate est la chaîne de modèle, et il y a 3 variables disponibles :

- $p - nom de l'imprimante
- $u - nom d'utilisateur complet (domaine/utilisateur, ou nom_ordinateur/utilisateur)
- $s - numéro de session

Étant donné certaines contraintes de Fabuletch : **Il est obligatoire de spécifier $p et $u, ou $p et $s.**
Il est nécessaire que les noms des imprimantes soient uniques sur le serveur pour différents utilisateurs.

Exemple : PrinterNameTemplate = “$p $u”, vous pouvez voir le résultat dans la capture d'écran de la session RDP ci-dessous



Configuration avancée

La configuration avancée pour Virtual Printer v2 peut être gérée côté serveur via l'objet de stratégie de groupe ou de stratégie locale sous Configuration de l'ordinateur > Modèles d'administration > Périphériques virtuels > Virtual Printer (Serveur).

Les paramètres suivants sont pertinents pour l'intégration de Remote Access :

- Mode de sélection de l'imprimante par défaut : Définit comment l'imprimante par défaut est attribuée chaque fois qu'un utilisateur se connecte à une session distante.

- Modèle de nom d'imprimante : Spécifie le format de nommage pour les imprimantes virtuelles des sessions utilisateur.
- Limiter la qualité pour les grandes impressions : réduit la qualité d'impression pour les pages dépassant une taille spécifiée afin d'accélérer l'impression grand format tout en préservant une qualité maximale pour les pages plus petites.

Pour des détails complets sur la configuration, veuillez vous référer à la documentation GPO de Virtual Printer à https://www.fabulatech.com/printer-for-remote-desktop-server-help/gpo.html

TSplus Virtual Printer

L'imprimante virtuelle TSplus est une nouvelle alternative aux solutions d'impression à distance classiques, qui peuvent être peu fiables, dépendantes du matériel et difficiles à gérer. L'algorithme de compression unique de l'imprimante virtuelle améliore la vitesse de transit des travaux d'impression à distance en minimisant le transfert de données tout en maintenant la qualité de l'image.

Remarque Le client HTML5 de TSplus n'est pas pris en charge et il nécessite le TSplus Universal Printer .

Avantages

- Support pour les environnements mono-utilisateur et multi-utilisateur.
- Aucune configuration n'est requise.
- Fonctionne avec n'importe quelle machine virtuelle.
- Environnement mixte 32 et 64 bits.

Pré-requis

Liste de compatibilité des systèmes d'exploitation de l'imprimante virtuelle TSplus :

- Windows **7**
- Windows **8/8.1**
- Windows **10**
- Windows **11**
- Windows **Server 2008 R2**
- Windows **Server 2012 R2**
- Windows **Serveur 2016**

- Windows **Serveur 2019**
- Windows **Serveur 2022**
- Windows **Server 2025**

Le TSplus Virtual Printer est compatible avec :

- Le client généré par TSplus
- Le client TSplus RemoteApp
- Le plug-in TSplus RemoteApp lors de l'utilisation du portail Web
- Le client Microsoft Remote Desktop

Il n'est pas compatible avec :

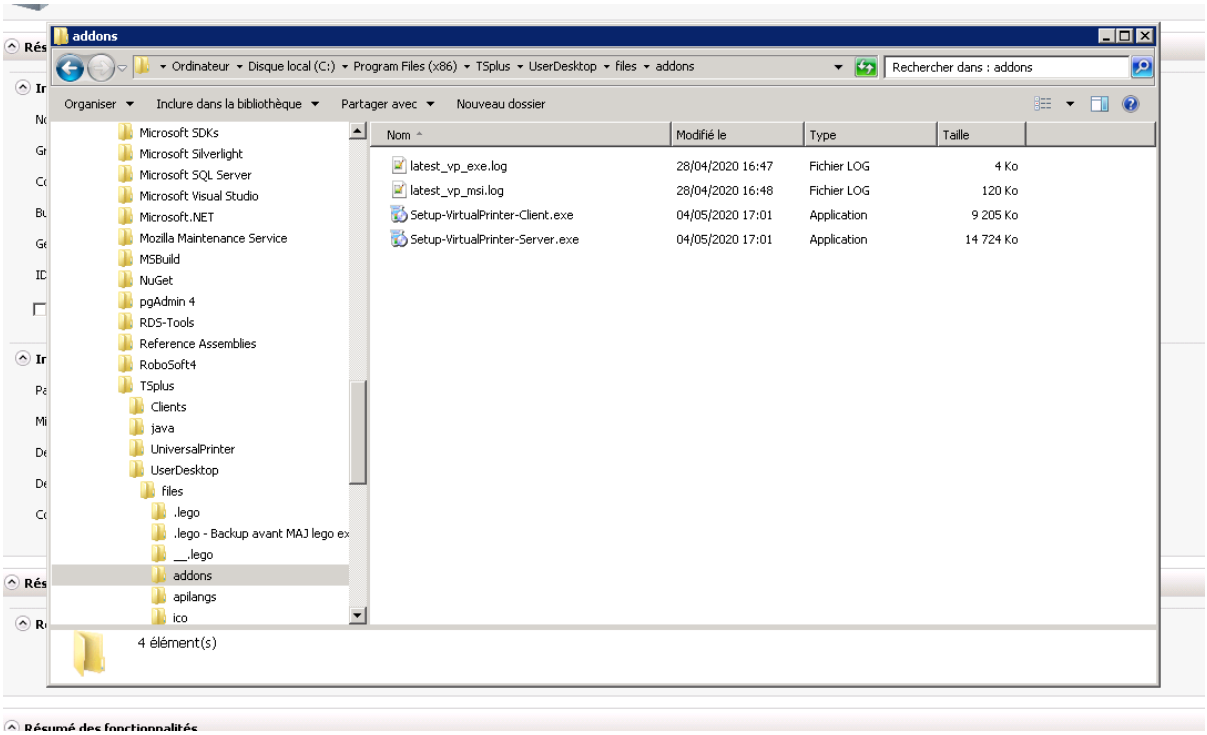
- Le client HTML5 de TSplus
- Appareils thin-client codés en dur où la configuration côté client ne peut pas être installée.

Deux parties

Le TSplus Virtual Printer est composé de deux composants :

- Un composant côté serveur qui est installé sur TSplus Remote Access.
- Un composant de bureau qui est installé sur le poste de travail Windows de l'utilisateur final.

Les deux configurations sont disponibles directement sur le serveur dans le dossier “C:\Program Files (x86)\TSplus\UserDesktop\files\addons” et sont nommées “Setup-VirtualPrinter-Server.exe” et “Setup-VirtualPrinter-Client.exe”.



La configuration du client est également disponible depuis votre serveur web TSplus, en utilisant le lien ci-dessous :

yourtsplusserveriporpublicdomain/addons/Setup-VirtualPrinter-Client.exe

Vous pouvez également effectuer une installation silencieuse du Client via une ligne de commande, en exécutant le programme d'installation avec les paramètres suivants :

/SUPPRESSMSGBOXES /VERYSILENT /SILENT /no_ui

Commencer

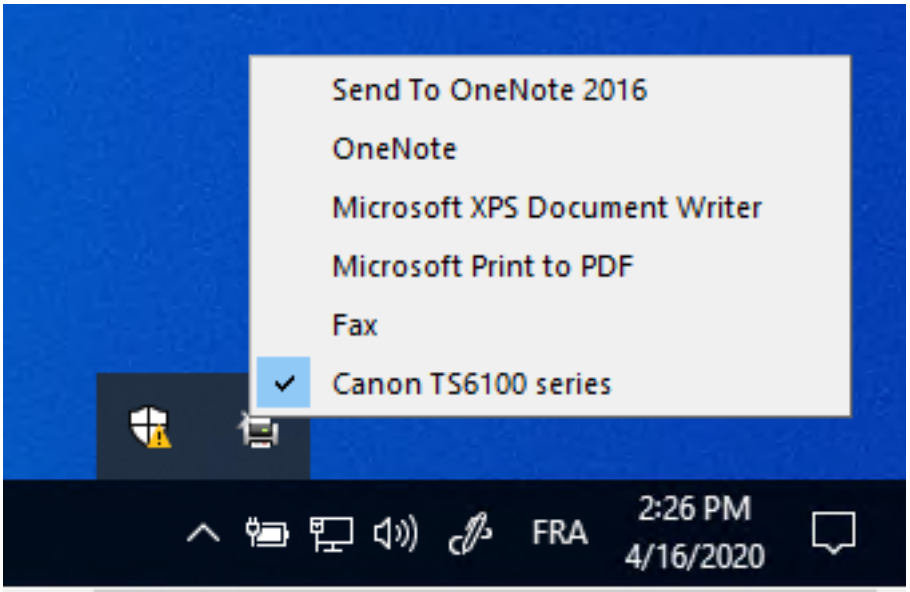
TSplus Virtual Printer est automatiquement installé lors de la première installation de TSplus et est directement disponible pendant la période d'essai.

Une fois TSplus installé, vous devrez installer le “Client d'Imprimante Virtuelle” sur l'ordinateur de l'utilisateur.

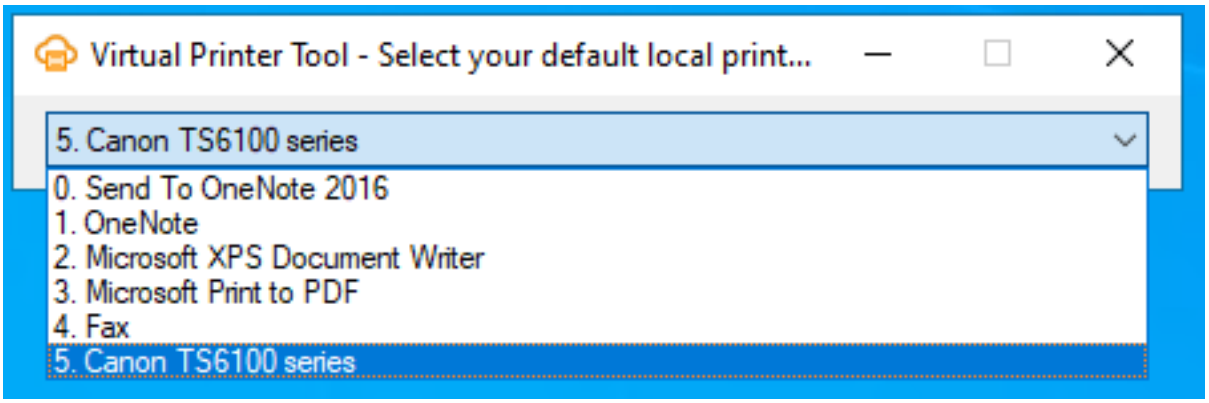
Lorsque vous vous connectez à distance à votre serveur TSPlus en utilisant soit **client RDP Microsoft** mstsc **Client généré par TSplus** ou **Plug-in RemoteApp du portail Web** vous pourrez imprimer depuis votre session distante vers votre imprimante locale en utilisant l'imprimante “Virtual Printer”. Par défaut, l'imprimante locale sélectionnée est l'imprimante par défaut locale.

Vous avez 2 façons de changer l'imprimante locale mappée à l'imprimante “Virtual Printer” en fonction de votre situation :

1. Si vous utilisez le bureau complet, vous pouvez sélectionner l'imprimante locale à utiliser en cliquant sur l'icône de l'imprimante virtuelle dans la zone de notification :



2.Si vous n'avez pas accès au bureau complet, vous devrez utiliser l'outil "Virtual Printer Tool" nommé "VirtualPrinterTool.exe" situé dans "C:\Program Files (x86)\TSplus\UserDesktop\files". Remarque : vous pouvez soit attribuer l'application à l'utilisateur, soit la faire exécuter automatiquement à la connexion via les paramètres avancés de l'imprimante virtuelle.

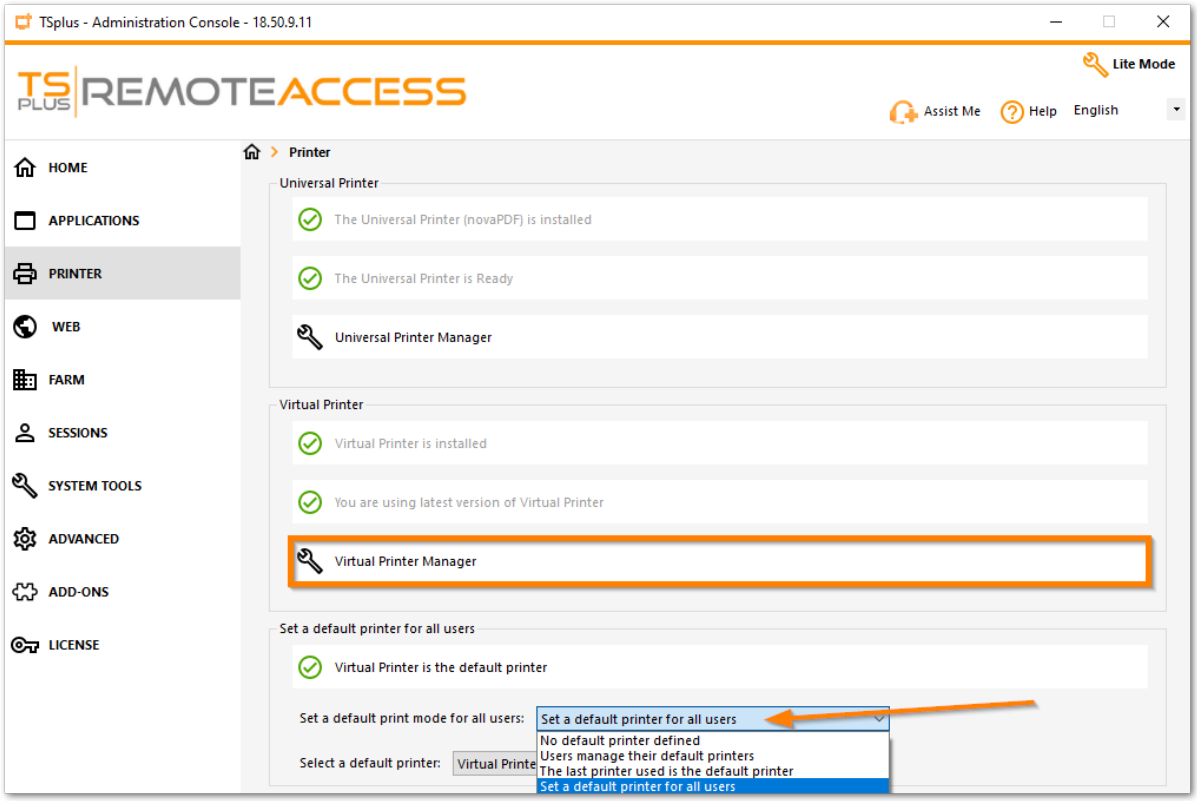


Configuration

Pour accéder au panneau de contrôle de l'imprimante virtuelle TSplus, veuillez naviguer à travers l'AdminTool : Imprimante > Gestionnaire d'imprimante virtuelle.

Définir une imprimante par défaut pour tous les utilisateurs

- Aucune imprimante par défaut définie : la configuration de l'imprimante par défaut de l'utilisateur n'est pas affectée.
- L'utilisateur gère ses imprimantes par défaut : l'option « Laisser Windows gérer mon imprimante par défaut » est désactivée, et il appartient donc à l'utilisateur de sélectionner son imprimante par défaut.
- La dernière imprimante utilisée est l'imprimante par défaut : l'option « Laisser Windows gérer mon imprimante par défaut » est activée.
- Définir une imprimante par défaut pour tous les utilisateurs : l'administrateur impose l'imprimante par défaut de l'utilisateur.



Dépannage de l'imprimante virtuelle

Si l'imprimante virtuelle ne fonctionne pas, la cause la plus courante est que soit le logiciel côté client "Print Application" ne s'exécute pas dans le Gestionnaire des tâches de l'ordinateur local de l'utilisateur, soit que le logiciel de l'imprimante virtuelle (serveur) a été installé sur l'ordinateur local de l'utilisateur, plutôt que la version de l'imprimante virtuelle (station de travail) (Setup-VirtualPrinter-Client.exe). Ci-dessous, les étapes de dépannage en détail pour les côtés client et serveur.

Veuillez noter que l'imprimante virtuelle n'est pas compatible avec notre client HTML5. Si vous utilisez le client HTML5, veuillez utiliser l'imprimante universelle à la place.

Guide de dépannage

Comment activer une licence en volume depuis le serveur après l'installation ?

Si vous avez installé votre produit sans aucune ligne de commande, alors il est installé en tant que version d'essai.

Activer

Pour activer votre licence en volume, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

- **Accès à distance et authentification à deux facteurs**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /Utilisateurs 1 (1 à 50 ou illimité)
  édition Entreprise (Desktop, MobileWeb, Entreprise)
  /supportyears 1 (1,2,3 seulement)

Exemple : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 30 /edition Enterprise /supportyears 1

Exemple : C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /supportyears 1

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  TSplus-Security.exe
  /édition Ultime Essentiels ou Ultime
  /supportyears 1 (1,2,3 seulement)

Exemple : C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /edition Ultimate /supportyears 1

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>
  ServerMonitoring.exe
  /Utilisateurs 1 (1 pour Startup, 5 pour Essentiel, 10 pour Entreprise)

/supportyears 1 (1 pour Startup, 5 pour Essentiel, 10 pour Entreprise)

Exemple : C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 5 /supportyears 1

- **Vous pouvez ajouter mes paramètres supplémentaires suivants :**
  — vos commentaires Spécifiez les commentaires à joindre à la licence sur le portail de licence.
  — /verysilent Exécutez le programme d'installation en mode silencieux. Cela permet l'intégration de ce programme d'installation dans vos propres scripts d'initialisation ou d'automatisation.

Exemple : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users unlimited /edition Enterprise /supportyears 3 /comments "Ceci est un commentaire"*

Paramètres

Cette commande prend les paramètres suivants :

si vous aimez utiliser des lignes de commande et vous vous demandez quelles autres lignes de commande sont disponibles, veuillez vous rendre à ceci documentation spécifique)

Mise à jour du support

Pour prolonger votre abonnement de mise à jour/support, choisissez 1, 2 ou 3 en fonction de la durée de l'extension.
Utilisez cette commande :

AdminTool.exe /vl /renewsupport VOTRE-CLE-DE-LICENCE-VOLUMIQUE /supportyears 1

Ajouter un support manquant

Cette commande est particulièrement utile si le client a oublié d'activer le support lors de l'installation ou s'il a besoin de définir une date de fin spécifique pour sa période de support.

Exécutez cette commande en tant qu'administrateur, en remplaçant les détails par vos propres informations de licence et la date de fin de support souhaitée :

AdminTool.exe /vl /activate-support VOTRE-CLE-DE-LICENCE-VOLUME /users [number] /edition [edition] /endofsupport [YYYY-MM-DD]

Pour activer le support pour un utilisateur de Remote Access 5 avec l'édition Printer jusqu'au 25 juillet 2026, entrez :

AdminTool.exe /vl /activate-support YOUR-VOLUME-LICENSE-KEY /users 5 /edition Printer /endofsupport 2026-07-25

Cette nouvelle fonctionnalité facilite la gestion des périodes de support, afin que les clients sachent toujours quand leur période de support commence et se termine.

Comment afficher les crédits de licence restants pour une clé de licence en volume ?

Pour afficher les crédits de licence restants pour une clé de licence en volume, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

AdminTool.exe /vl /credits-license VOLU-MELI-CENS-EKEY /login JOHNDOE [/édition Essentials] [/silent]

Paramètres

Cette commande peut prendre quatre paramètres :

- VOLU-MELI-CENS-EKEY : utilisez votre propre clé de licence en volume
- /login JOHNDOE : fournir le login du partenaire associé à la clé de licence en volume
- /édition Essentials : fournir le paramètre d'édition optionnel pour les produits Advanced Security et Server Monitoring
- /silencieux : exécute la commande silencieusement

La sortie sera stockée dans la variable d'environnement au niveau utilisateur nommée CRÉDITS DE LICENCE VOLUME Il peut être nécessaire de lire la valeur de CRÉDITS DE LICENCE VOLUME d'un processus différent, en utilisant la commande : echo %VOLUME_LICENSE_CREDITS%

Veuillez trouver ci-dessous les éditions attendues pour les produits Advanced Security et Server Monitoring :

- Sécurité Avancée : “Essentiels”, “Ultime”
- Surveillance du serveur : « Essentiels », « Démarrage », « Entreprise »

Les exécutables suivants doivent être utilisés pour trouver le nombre respectif de crédits restants :

- Accès à distance : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- Advanced Security : C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- Surveillance du serveur : C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe

- 2FA: C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe
- RPA : C:\Program Files (x86)\TSplus-RPA\AdminTool.exe
- Travail à distance : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

---

titre : “Comment afficher les crédits de support restants pour une clé de licence en volume ?”

Pour afficher les crédits de support restants pour une clé de licence en volume, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE [/édition Essentials] [/silent]

Paramètres

Cette commande peut prendre quatre paramètres :

- VOLU-MELI-CENS-EKEY : utilisez votre propre clé de licence en volume
- /login JOHNDOE : fournir le login du partenaire associé à la clé de licence en volume
- /édition Essentials : fournir le paramètre d'édition optionnel pour les produits Advanced Security et Server Monitoring
- /silencieux : exécute la commande silencieusement.

La sortie sera stockée dans la variable d'environnement au niveau utilisateur nommée CRÉDITS DE LICENCE VOLUME Il peut être nécessaire de lire la valeur de CRÉDITS DE LICENCE VOLUME d'un processus différent, en utilisant la commande : echo %VOLUME_LICENSE_CREDITS%

Veuillez trouver ci-dessous les éditions attendues pour les produits Advanced Security et Server Monitoring :

- Sécurité Avancée : “Essentiels”, “Ultime”
- Surveillance du serveur : « Essentiels », « Démarrage », « Entreprise »

Les exécutables suivants doivent être utilisés pour trouver le nombre respectif de crédits restants :

- Accès à distance : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- Advanced Security : C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- Surveillance du serveur : C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe

- 2FA: C:\Program Files (x86)\TSplus\UserDesktop\files\TwoFactor.Admin.exe
- RPA : C:\Program Files (x86)\TSplus-RPA\AdminTool.exe
- Travail à distance : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

Comment désactiver une licence depuis le serveur ?

Pour désactiver un serveur qui a été activé avec une clé de licence en volume, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

AdminTool.exe /vl /disable VOLU-MELI-CENS-EKEY

Comment activer une licence depuis le serveur ?

Pour activer un serveur qui a d'abord été activé avec une clé de licence en volume et qui a ensuite été désactivé, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

AdminTool.exe /vl /enable VOLU-MELI-CENS-EKEY

Comment désactiver une licence depuis le portail de licence ?

Vous devez d'abord désactiver la licence sur le portail de licence, puis vous assurer que le nouveau statut est appliqué sur votre serveur en mettant à jour son statut depuis l'application d'administration ou la ligne de commande.

Tout d'abord, à partir de la liste des Licences et des pages de détails de la Licence, vous pouvez cliquer sur le bouton « Désactiver » pour désactiver la Licence sélectionnée.

La licence passera du statut « Activé » au statut « Désactivation… », ce qui signifie qu'elle attend actuellement que le serveur se désactive.
Ensuite, le serveur se désactivera automatiquement le lendemain s'il a un accès à Internet.

Vous pouvez également le faire manuellement en exécutant la ligne de commande suivante en tant qu'administrateur élevé :

AdminTool.exe /license /refresh

Notez qu'il n'est pas nécessaire d'exécuter la ligne de commande de rafraîchissement pour tous

les logiciels installés. Le rafraîchissement est pris en charge par tous les produits compatibles avec le système de licence 2020.

La licence sera prise en compte dans votre utilisation de la licence jusqu'à ce que votre serveur ait contacté le portail de licence et reconnu son statut désactivé.

Comment installer un serveur de licence en volume en une étape ?

Pour installer un serveur de licence en volume en une seule étape, vous aurez besoin de :

- Téléchargez le programme d'installation du produit
- Utilisez votre clé de licence en volume
- Exécutez le programme d'installation avec votre clé de licence en volume comme paramètre.

Votre clé de licence en volume est la même pour toute installation de tout nouveau serveur. Si vous ne vous en souvenez pas, connectez-vous à votre compte dans le portail de licence. Votre clé de licence en volume est affichée en haut de la page d'accueil (Licences).

Pour installer et activer une licence en volume à partir d'un script, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users illimité /edition Enterprise /supportyears 3 /comments "Ceci est un commentaire"

L'activation scriptée utilisant la licence en volume 2020 est disponible pour les produits suivants et toutes leurs versions rebrandées :

- Remote Access
- Sécurité Avancée (alias RDS-Knight)
- Surveillance du serveur (anciennement Server Genius)
- Authentification à deux facteurs

Paramètres

Cette commande prend les paramètres suivants :

- **Accès à distance et authentification à deux facteurs**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /Utilisateurs 1 (1 à 50 ou illimité)

édition Entreprise (Desktop, MobileWeb, Entreprise)
/supportyears 1 (1,2,3 seulement)

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  TSplus-Security.exe
  /édition Ultime Essentiels ou Ultime
  /supportyears 1 (1,2,3 seulement)

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>
  ServerMonitoring.exe
  /Utilisateurs 1 (1 pour Startup, 5 pour Essentiel, 10 pour Entreprise)
  /supportyears 1 (1 pour Startup, 5 pour Essentiel, 10 pour Entreprise)

Méthodes de script

Pour démarrer Setup-PRODUCT.exe avec sa ligne de commande correcte, vous pouvez utiliser 3 méthodes :

1. Utilisez vos propres méthodes de scripts de gestion

2. Créez un raccourci de Setup-PRODUCT.exe et modifiez les propriétés pour ajouter la ligne de commande à la fin du chemin.

3. Ouvrez simplement une « Invite de commandes » en appuyant simultanément sur la touche Windows et la touche « R », puis en tapant « cmd » et en appuyant sur la touche « Entrée » pour confirmer. Cette méthode avec le raccourci clavier fonctionne sur toutes les versions de Windows existantes au moment de la rédaction de ce document.

4. Une fois l'invite apparaître, changez le répertoire actuel pour le répertoire où se trouve votre programme d'installation (généralement votre dossier Téléchargements). Par exemple, tapez :

   cd C:\Program Files (x86)\TSplus\UserDesktop\files

Et enfin, tapez la commande complète pour exécuter le programme d'installation avec les paramètres suivants, en fournissant les valeurs souhaitées :

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “Ceci est un commentaire”

Trouvez le programme d'administration pertinent

Les programmes suivants prennent en charge les commandes de licence en volume.
Le nom du programme et l'emplacement dépendent du produit et de son dossier de configuration :

Accès à distance et authentification à deux facteurs
C:\Program Files (x86)\TSplus\UserDesktop\files>
AdminTool.exe TwoFactor.Admin.exe

Advanced Security
C:\Program Files (x86)\TSplus-Security>
TSplus-Security.exe

Server Monitoring
C:\Program Files (x86)\TSplus-ServerMonitoring>
ServerMonitoring.exe

L'exécution du programme est silencieuse. Cela permet d'intégrer votre processus d'activation de licence dans vos propres scripts d'initialisation ou d'automatisation.

---

titre : “Dépannage des commandes d'activation, d'activation, de désactivation et de mise à jour”

Si vous souhaitez enquêter sur un problème et/ou lorsque vous prototypez vos scripts, vous pouvez obtenir des messages de succès et d'erreur en consultant le **VolumeLicensing.log** fichier trouvé à la racine du programme.

---

titre : “Comment configurer un serveur proxy

pour l'accès Internet”

Les paramètres de proxy définis lors de l'installation sont mémorisés et seront utilisés pour effectuer des opérations sur les licences. Si aucun paramètre de proxy n'a été défini, le programme de licence en volume utilisera les paramètres de proxy d'Internet Explorer (s'il y en a de configurés dans la session en cours et/ou pour le service Windows).

Vous pouvez également configurer manuellement les paramètres du proxy en exécutant la ligne de commande suivante en tant qu'administrateur élevé :

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

Paramètres

#	Parameter	Description
1	/set	Action to be performed on the proxy settings
2	/host (ie | none | custom)	The destination host can be a predefined value (e.g. "ie" or "none") or a user-defined value (ex. 127.0.0.1 or proxy.company.org). This parameter is mandatory.
3	/port 80	The port number used to connect to the proxy server. Required if the hostname value is a custom user-defined value.
4	/username dummy	The username to connect to the proxy server. This setting is optional.
5	/password pass@word1	The user's password must be supplied if a username has been defined. However, its value can be empty.

si vous aimez utiliser des lignes de commande et vous vous demandez quelles autres lignes de commande sont disponibles, veuillez vous rendre à ceci documentation spécifique)

---

titre : “Comment obtenir de l'assistance pour la licence en volume”

L'équipe de support et de services de Volume Licensing sera plus qu'heureuse de vous aider si vous rencontrez un problème ou une difficulté lors de l'installation et de l'exécution de Volume Licensing sur un serveur.

La façon la plus simple de contacter l'équipe Support et Services de Volume Licensing est d'ouvrir un ticket sur notre Helpdesk en ligne à : https://support.tsplus.net

Comment mettre à jour les utilisateurs d'une licence en volume depuis le serveur ?

Pour changer le nombre d'utilisateurs associés à votre licence en volume activée, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /users 10

Paramètres

Cette commande prend deux paramètres :

- VOLU-MELI-CENS-EKEY : utilisez votre propre clé de licence en volume
- /utilisateurs illimités : utilisez un nombre de 1 à 50 ou "illimité"

Veuillez noter que :

- Cette commande ne s'applique pas à Advanced Security et à l'addon 2FA.
- Server Monitoring n'accepte que les numéros 1, 5 et 10 correspondant aux trois éditions disponibles de Server Monitoring.
- Seul TSplus Remote Work accepte un nombre d'utilisateurs supérieur à 50.

---

titre : “Comment mettre à jour l'édition d'une licence en volume depuis le serveur ?”

Pour changer l'édition associée à votre licence en volume activée, exécutez la ligne de commande suivante en tant qu'administrateur élevé :

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /edition Entreprise

Paramètres

Cette commande prend deux paramètres :

- VOLU-MELI-CENS-EKEY : utilisez votre propre clé de licence en volume
- édition Entreprise : utilisez le nom de l'édition

Veuillez noter que :

- Ce paramètre ne s'applique pas au travail à distance, au support à distance, à la surveillance des serveurs, à l'addon 2FA et à Server Genius.
- Les éditions possibles sont « Bureau », « MobileWeb » ou « Entreprise » pour Remote Access.
- Les éditions possibles sont « Essentials » ou « Ultimate » pour Advanced Security.

si vous aimez utiliser des lignes de commande et vous vous demandez quelles autres lignes de commande sont disponibles, veuillez vous rendre à ceci documentation spécifique)

Mettre à jour le support

Pour prolonger votre abonnement de mise à jour/support, choisissez 1, 2 ou 3 en fonction de la durée de l'extension.
Utilisez cette commande : AdminTool.exe /vl /renewsupport VOLU-MELI-CENS-EKEY /supportyears 1

Cette commande n'est disponible qu'à partir de la version 15.60.11.8.

Licences en volume

Volume Licensing est une solution de licence par script alimentée par TSplus pour ses solutions. Les produits suivants prennent en charge l'activation utilisant Volume Licensing 2020 : Remote Access, Remote Work, Advanced Security (également connu sous le nom de RDS-Knight), Remote Support ou Server Monitoring (anciennement Server Genius).

Lorsque votre compte de licence en volume est créé sur le portail de gestion des licences, l'équipe de licence en volume fournira :

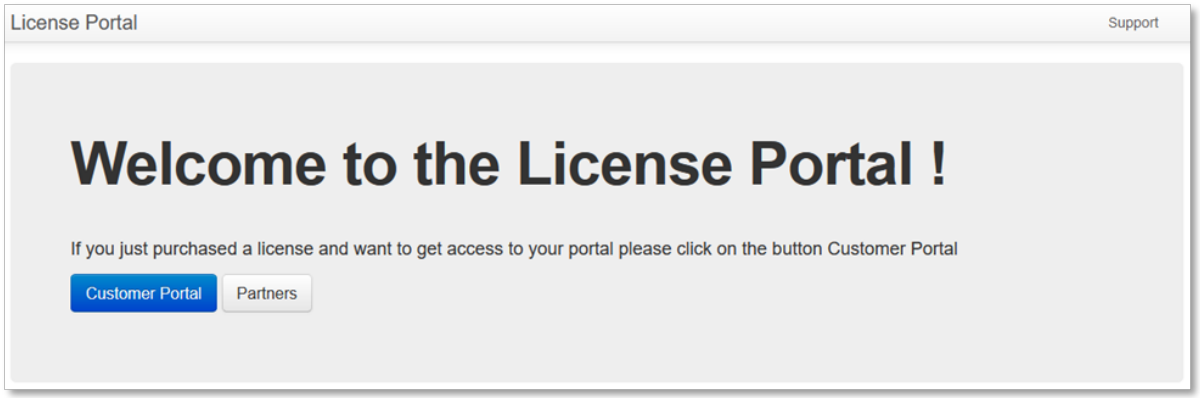
1. Votre clé de licence en volume (veuillez garder cette information confidentielle)
2. Vos identifiants pour vous connecter au portail de gestion des licences
3. Ce guide de l'administrateur sur la licence en volume 2020

L'IMPRIMANTE VIRTUELLE N'EST PLUS LICENCIÉE
Veuillez noter qu'à partir du 15 mars 2022 et de la version 15.40.3.14, Virtual Printer n'est plus sous licence et est inclus dans toutes les éditions de TSplus Remote Access.

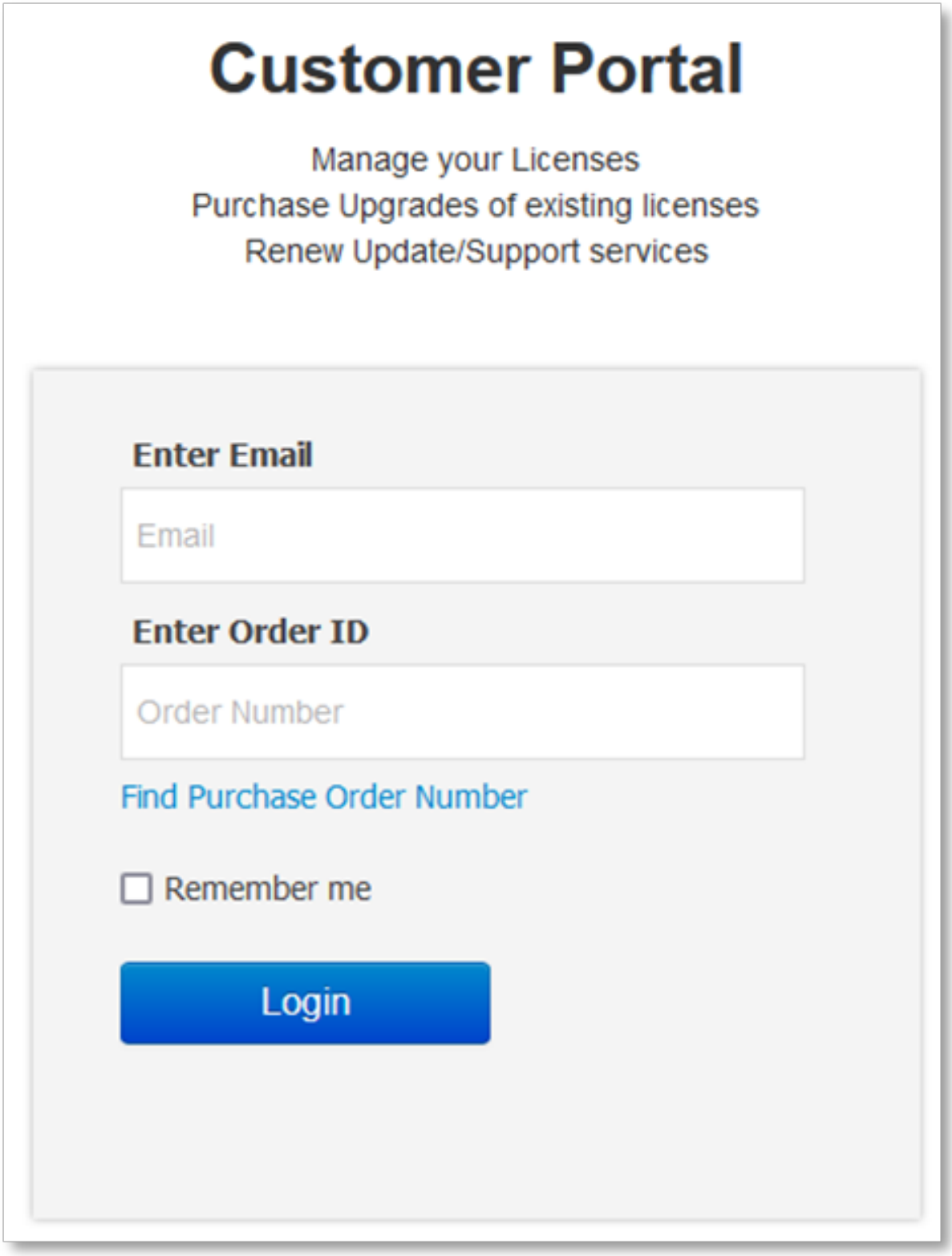
Comment gérer vos licences en volume ?

Vos licences en volume et votre solde de crédit peuvent être consultés et gérés dans le portail de licence TSplus.
Le portail de licence TSplus est disponible à l'URL suivante : https://license.tsplus.net

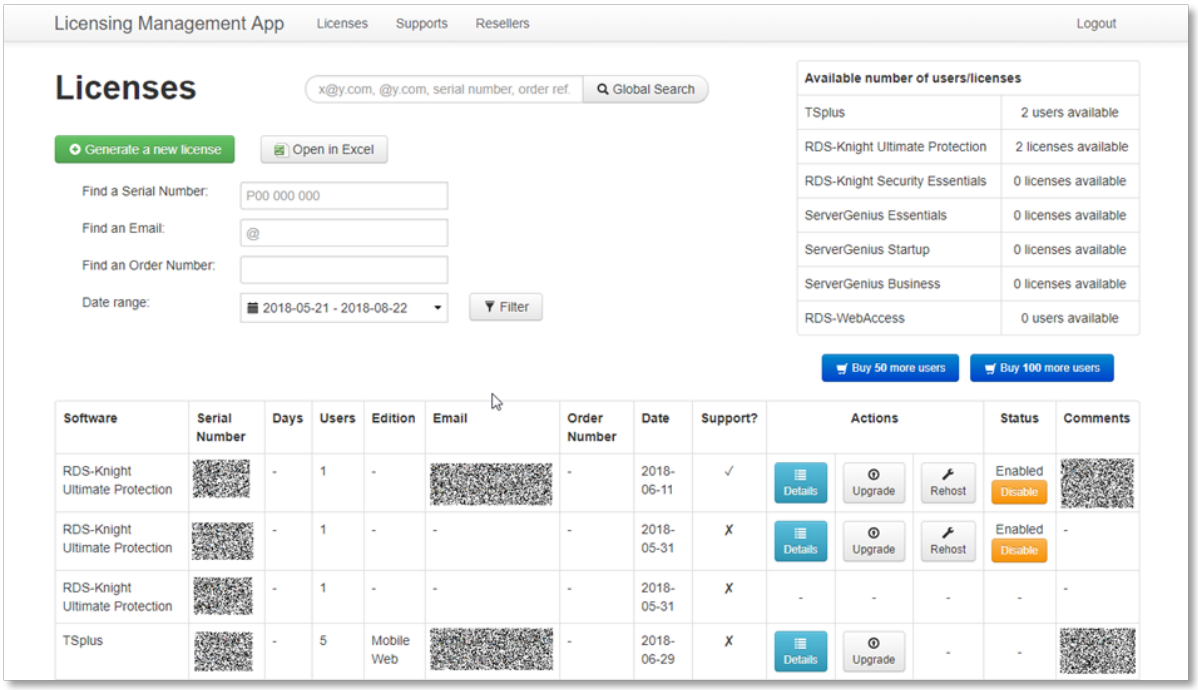
Pour vous connecter et accéder à votre compte, commencez par cliquer sur le Portail Client pour atteindre la section des clients :



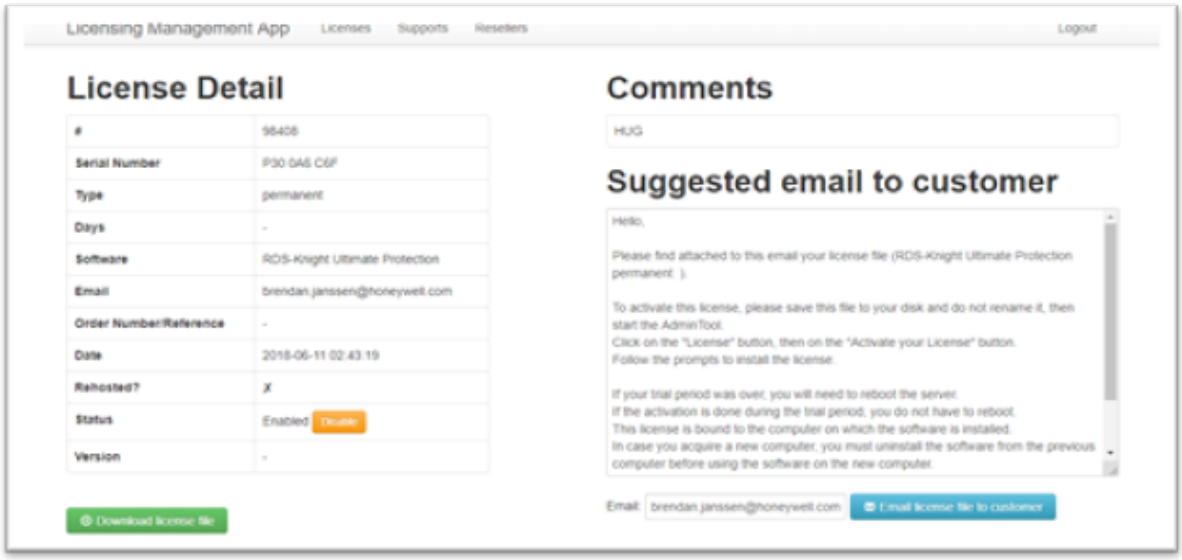
Ensuite, saisissez vos identifiants pour accéder à votre compte :



Une fois connecté, vous verrez le tableau suivant où toutes vos Licences sont listées. C'est la page principale où vous pourrez gérer toutes vos Licences. Si vous n'avez pas encore activé de Licence de Volume, cette page sera vide.



Pour consulter les détails de l'historique d'une licence, cliquez sur le bouton « Détails » de la licence que vous souhaitez étudier. Vous obtiendrez la page des détails de la licence comme indiqué sur l'image ci-dessous.



TSplus Web App

TSplus Web App est une application web progressive (PWA) qui tire parti des API modernes des navigateurs pour offrir une expérience d'accès à distance fluide sans installation de logiciel encombrante ni clients de connexion compliqués. Conçue pour utiliser des protocoles d'affichage et de communication HTML5 standard de l'industrie, l'application web TSplus apparaît comme une solution de connexion native, peu importe le type d'appareil que vous utilisez.

Avantages

Le nouveau TSplus WebApp offre des performances et une valeur améliorées grâce aux améliorations suivantes par rapport aux applications héritées et aux clients de connexion :

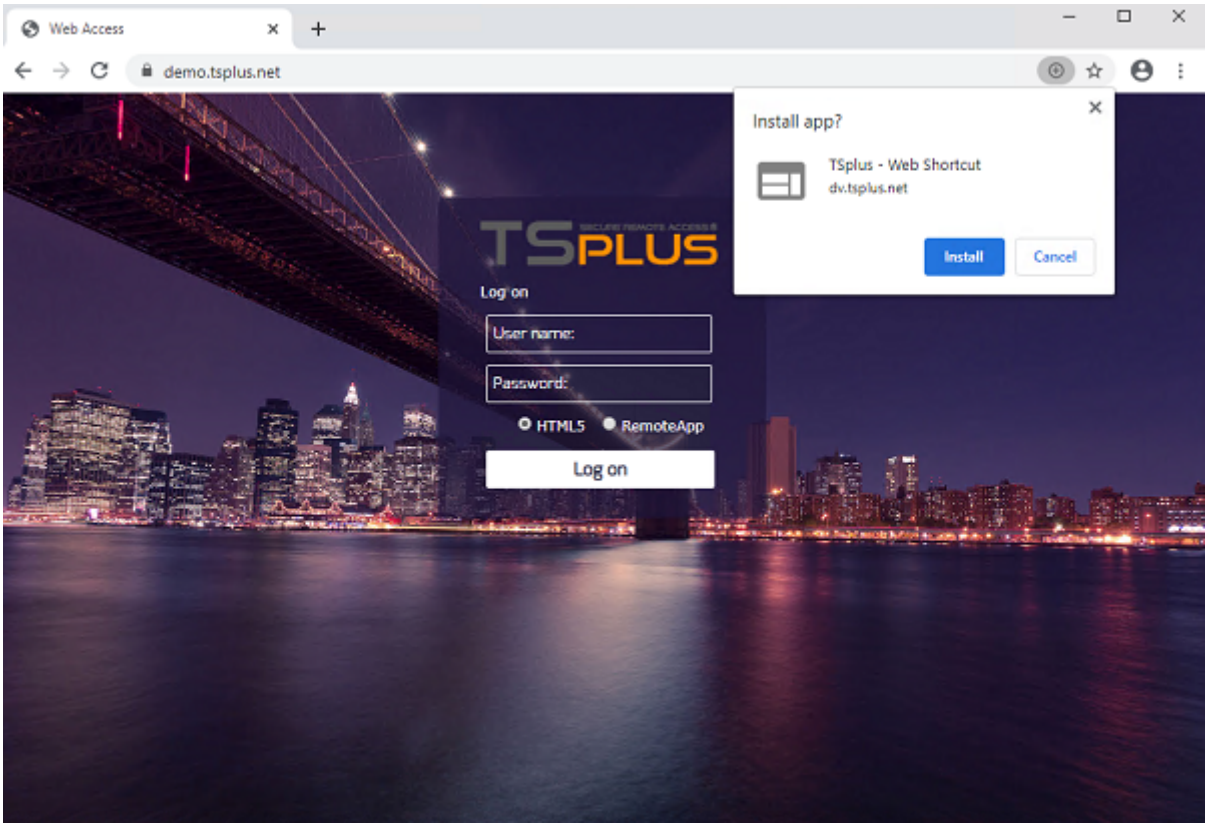
- Des temps de chargement plus rapides grâce à la petite empreinte logicielle.
- Utilisation de données inférieure - TSplus Web App utilise la gestion du trafic basée sur les navigateurs courants pour minimiser l'utilisation des données.
- Expérience utilisateur fluide - de l'affichage de connexion au rendu des applications, le TSplus WebApp offre à l'utilisateur l'apparence d'une utilisation d'application native.
- Plus de fenêtres de navigateur ou de sessions perdues en raison de trop nombreuses fenêtres de navigateur ouvertes. Le comportement de l'application Web TSplus offre les mêmes options de multitâche que toute autre application de haut niveau.

Installation - PC

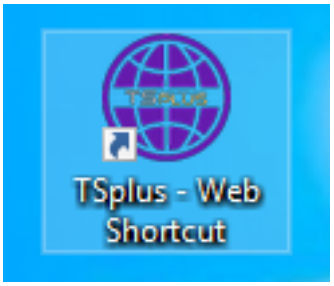
Naviguez vers votre portail Web TSplus d'entreprise en utilisant votre navigateur web commun préféré (configuration HTTPS requise).
Pour une utilisation sur Firefox, vous devrez installer le PWAS add-on.

Cliquez sur le bouton + situé sur le côté droit de la barre de navigation. Lorsque vous y êtes

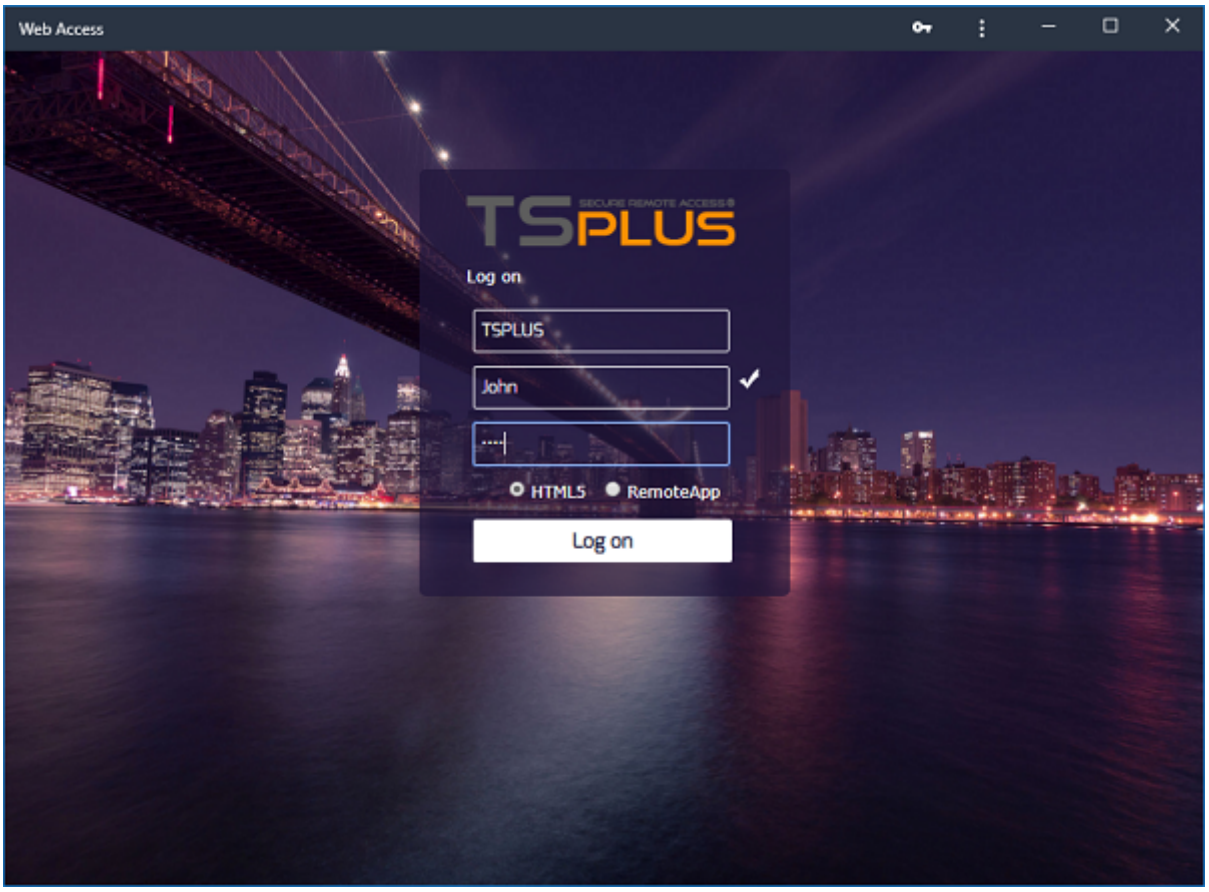
invité, cliquez sur « Installer ».



L'installation ne prend qu'une seconde. Elle créera une icône sur votre bureau :



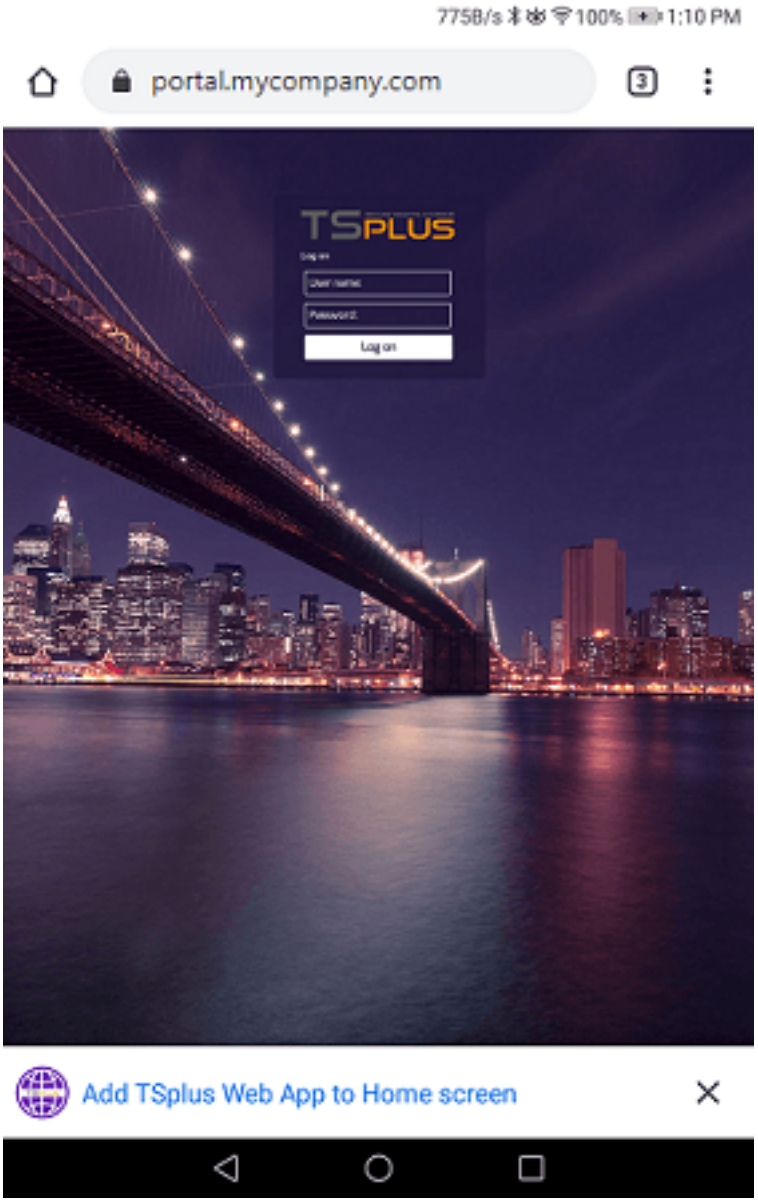
Et l'application web s'ouvrira immédiatement à la fin :



Installation - Appareil mobile Android

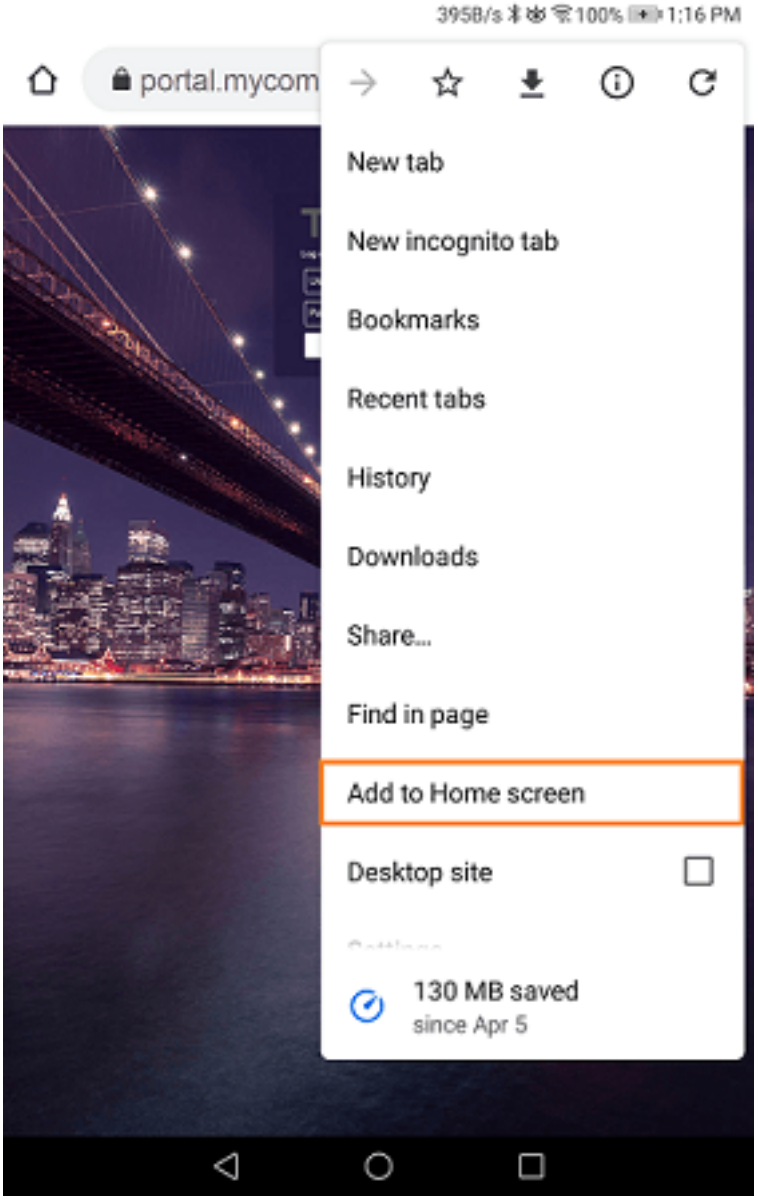
Naviguez vers votre portail Web TSplus d'entreprise en utilisant votre navigateur web mobile commun préféré. **Le protocole HTTPS est requis sur le serveur TSplus.**

Le portail Web proposera l'option d'ajouter l'application Web TSplus à votre écran d'accueil, en cliquant sur le message « Ajouter l'application Web TSplus à l'écran d'accueil » en bas de la fenêtre :

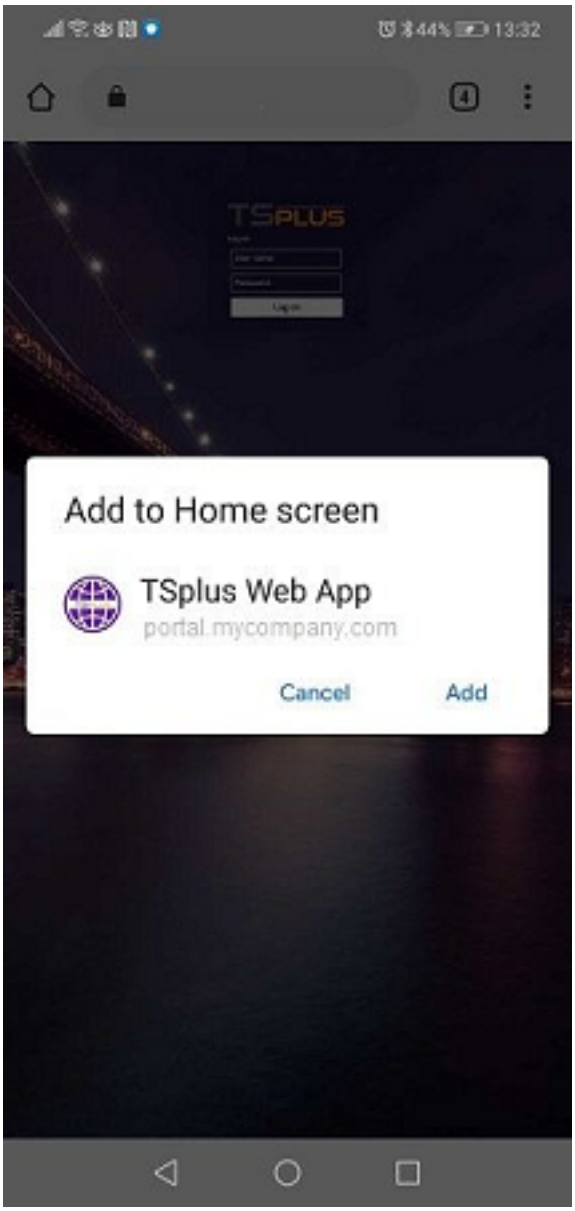


Ou en cliquant sur le menu à 3 points en haut à droite de la fenêtre et en cliquant sur « Ajouter »

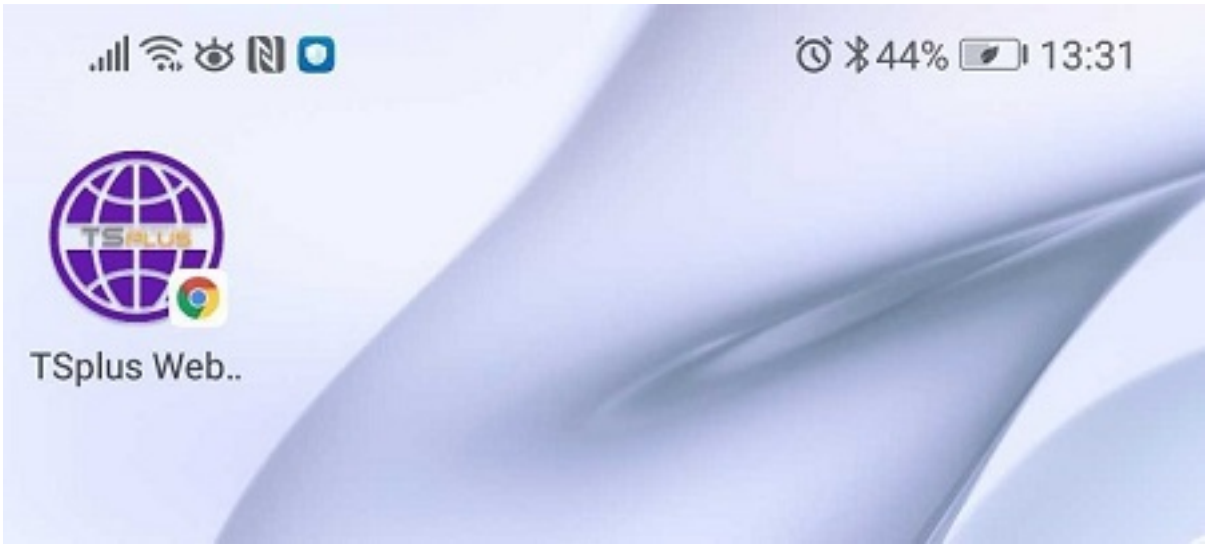
Après avoir accepté l'option Ajouter à l'écran d'accueil, l'utilisateur verra l'écran suivant :



Appuyez sur le bouton « Ajouter » et le processus est terminé :



L'application Web TSplus sera désormais accessible directement depuis l'écran d'accueil de votre appareil mobile.



Installation - Mobiles Apple iOS

Le processus d'installation de l'application Web sur iOS est similaire à celui d'Android. Il suffit de naviguer vers le TSplus Web Portal en utilisant le navigateur Safari. Cliquez sur le bouton Partager :

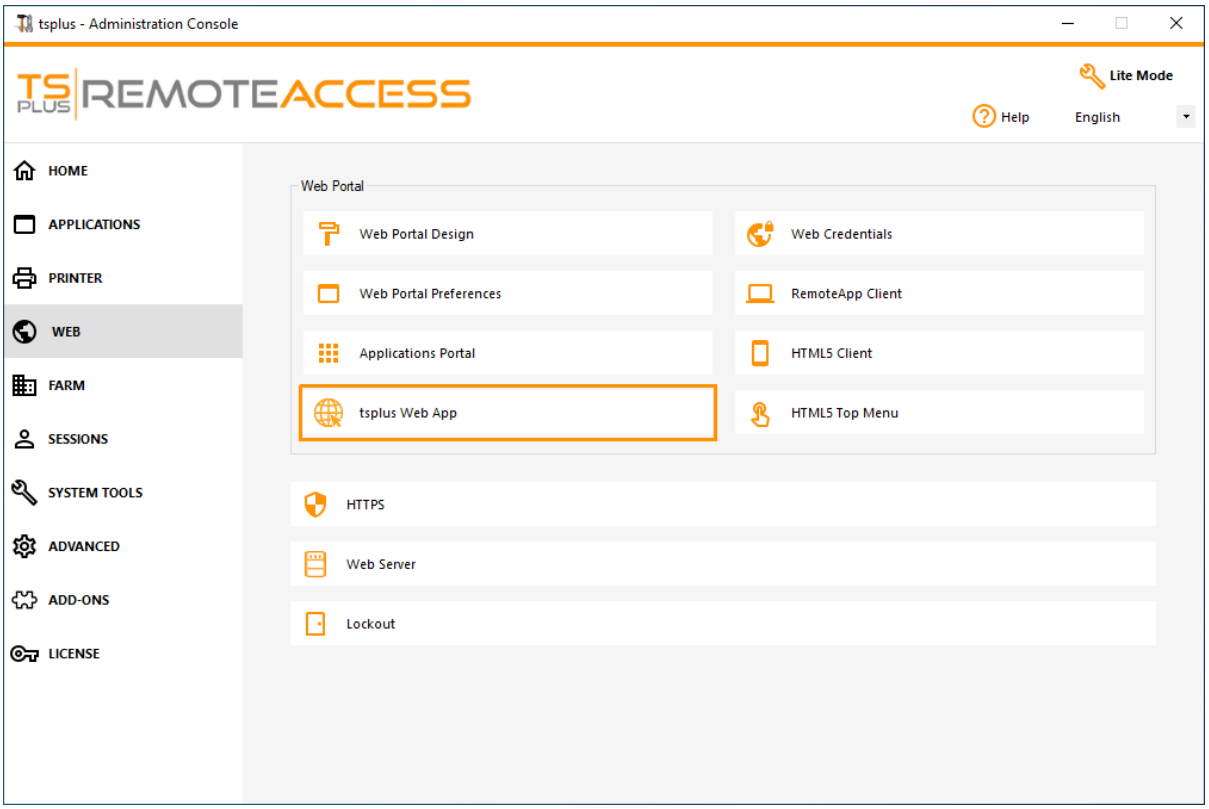


Puis cliquez sur « Ajouter à l'écran d'accueil ».

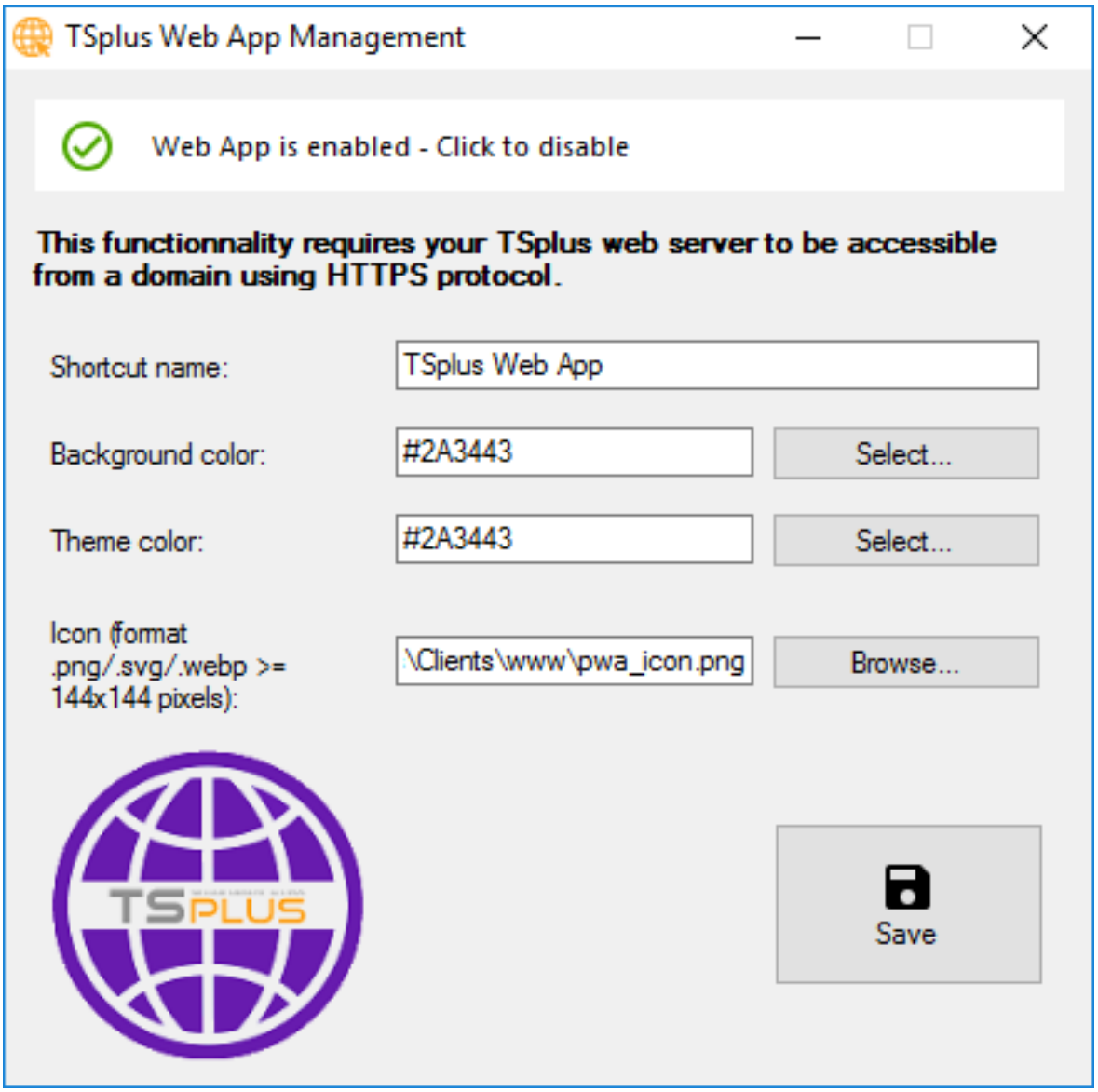
Remarque : Le navigateur Chrome ne prend pas en charge la fonctionnalité Web App sur iOS.

Gestion

Vous pouvez gérer l'application Web en allant dans la section TSplus Admin Tool Web - Portail Web et en cliquant sur le carreau de l'application Web TSplus :



L'application Web est activée par défaut, mais vous pouvez la désactiver. Il est possible de modifier le nom du raccourci, l'arrière-plan et les couleurs du thème ainsi que l'icône de TSplus Web App.



Il suffit de cliquer sur « Enregistrer » pour enregistrer vos modifications.

Portail des applications Web : paramètres dans l'adresse URL

Si vous souhaitez contourner la page de connexion standard Web Access de Terminal Service Plus lors de l'utilisation de la Portail des applications Web et allez directement à la page du portail des applications Web, vous devez spécifier plusieurs paramètres dans l'adresse URL :

- connexion utilisateur
- mot de passe utilisateur
- domaine utilisateur
- serveur
- port
- type de client (HTML5 ou Windows)

Voici un exemple d'une adresse URL complète pour l'utilisateur "demo" avec le mot de passe "demo" sur notre serveur de démonstration avec un client HTML5 :

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo&domain=&server=127.0.0.1&port=3389&type=html5

Le domaine, le serveur, le port et les paramètres de type étant optionnels, l'adresse URL suivante a exactement le même comportement :

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo

Pour utiliser un client Windows, utilisez :

&type=remoteaccess

En utilisant ces paramètres dans l'adresse URL, vous pouvez accéder directement à la page du portail des applications Web.

Vous n'avez pas à spécifier tous ces paramètres en même temps : les paramètres non spécifiés auront leur valeur configurée par défaut.

Si vous souhaitez contourner la connexion standard de Terminal Service Plus lors de l'utilisation de la connexion avec le client HTML5, cochez cette page .

Portail des applications Web

Le portail d'application Web de Terminal Service Plus offre une solution unique et flexible qui peut rationaliser le déploiement d'applications et de bureaux ainsi que la gestion du cycle de vie pour réduire les coûts informatiques. En gérant de manière centralisée et en livrant sur le web des applications à la demande, l'informatique peut améliorer le taux de réussite du déploiement des applications en fournissant une gestion basée sur les rôles, un contrôle des applications, une sécurité et un support aux utilisateurs.

Terminal Service Plus Web Application Portal virtualise et transforme les applications et bureaux Windows en un service sécurisé à la demande.

Avec le portail d'application Web, vous pourrez publier des applications Microsoft Windows (applications professionnelles, applications Office…) sur le web.

Comme dans Citrix, vos utilisateurs peuvent accéder à leurs applications directement depuis Internet, simplement en cliquant sur l'icône de l'application dans la page Web du portail, directement dans leur propre navigateur Internet.

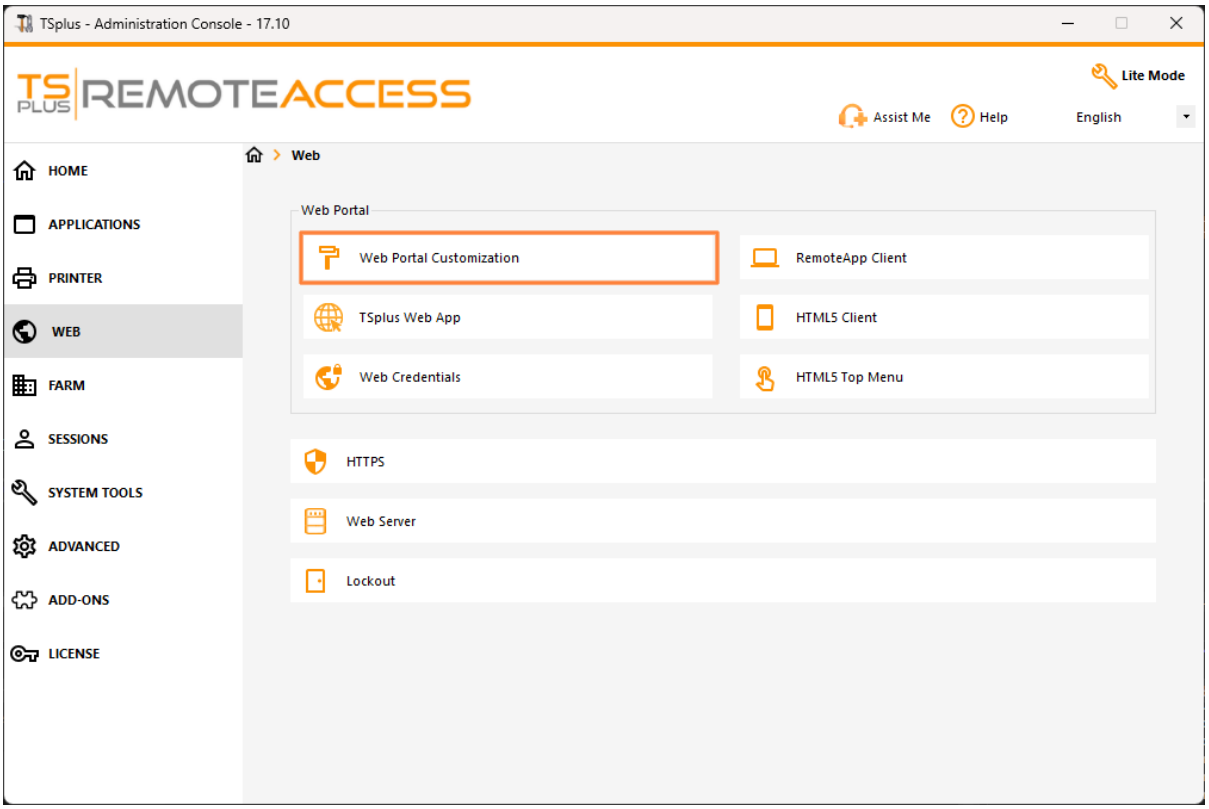
Gérer vos applications Web

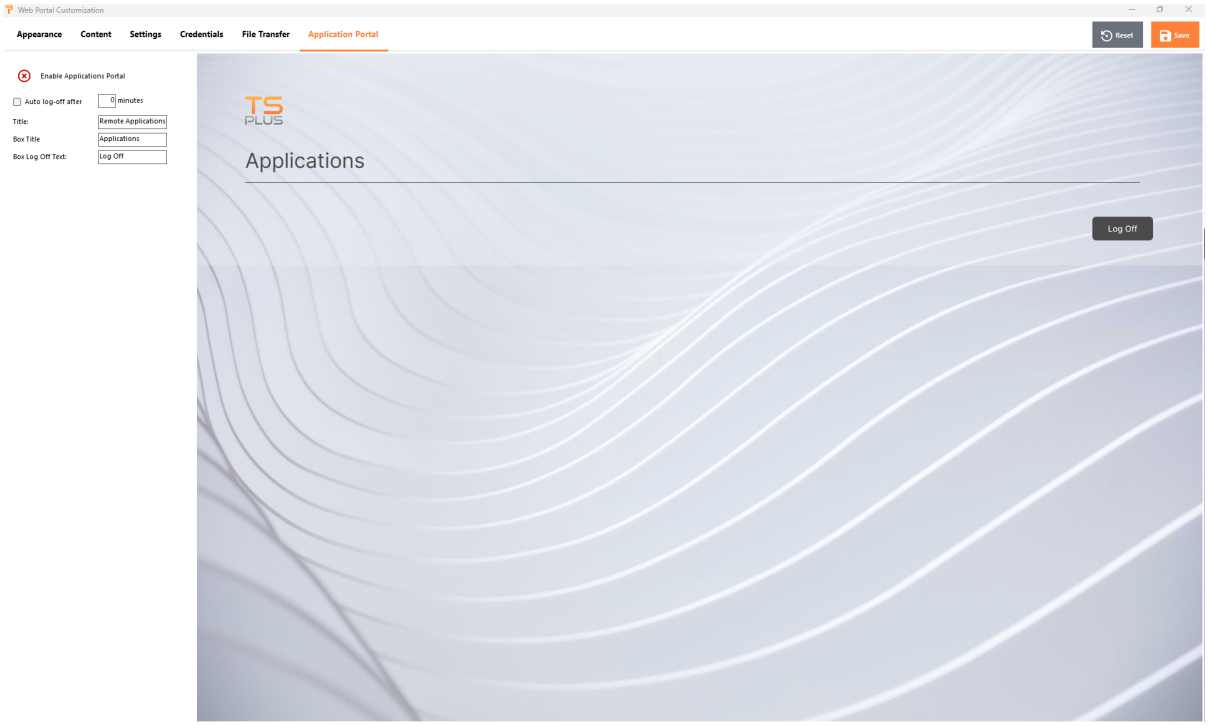
La fonctionnalité du portail d'application Web est **entièrement intégré** dans Terminal Service Plus. Cela signifie que toutes les applications publiées par la fonctionnalité de publication d'applications de Terminal Service Plus peuvent être utilisées dans le portail des applications Web.

Si vous souhaitez en savoir plus sur ce processus de publication, n'hésitez pas à consulter notre documentation sur Publication d'application et Affectation d'applications aux utilisateurs ou groupes .

Conception de votre portail d'applications Web

Dans l'outil d'administration, ouvrez l'onglet « Web » et cliquez sur la tuile « Personnalisation du portail Web », puis allez à la tuile « Portail d'application ».





Pour générer une page d'accès web avec la fonctionnalité Portail d'Applications Web activée, **cochez la case "Activer le portail des applications".** Vous pouvez personnaliser votre page d'accès web à votre goût, puis cliquez sur « Enregistrer » pour publier cette nouvelle page d'accès web.

Remarque : Vous pouvez changer les couleurs de la boîte et de la bordure de la boîte uniquement pour les thèmes classiques qui peuvent être modifiés sur le Onglet Apparence .

Utiliser le portail des applications Web

Dans cet exemple, nous avons publié la nouvelle page d'accès web avec le nom par défaut « index ».

Pour y accéder, ouvrez un navigateur web et allez à http://your_server_name/ (dans cet exemple, nous utilisons http://localhost directement depuis le serveur lui-même).

La première page web affichée est la page de connexion standard de Terminal Service Plus :

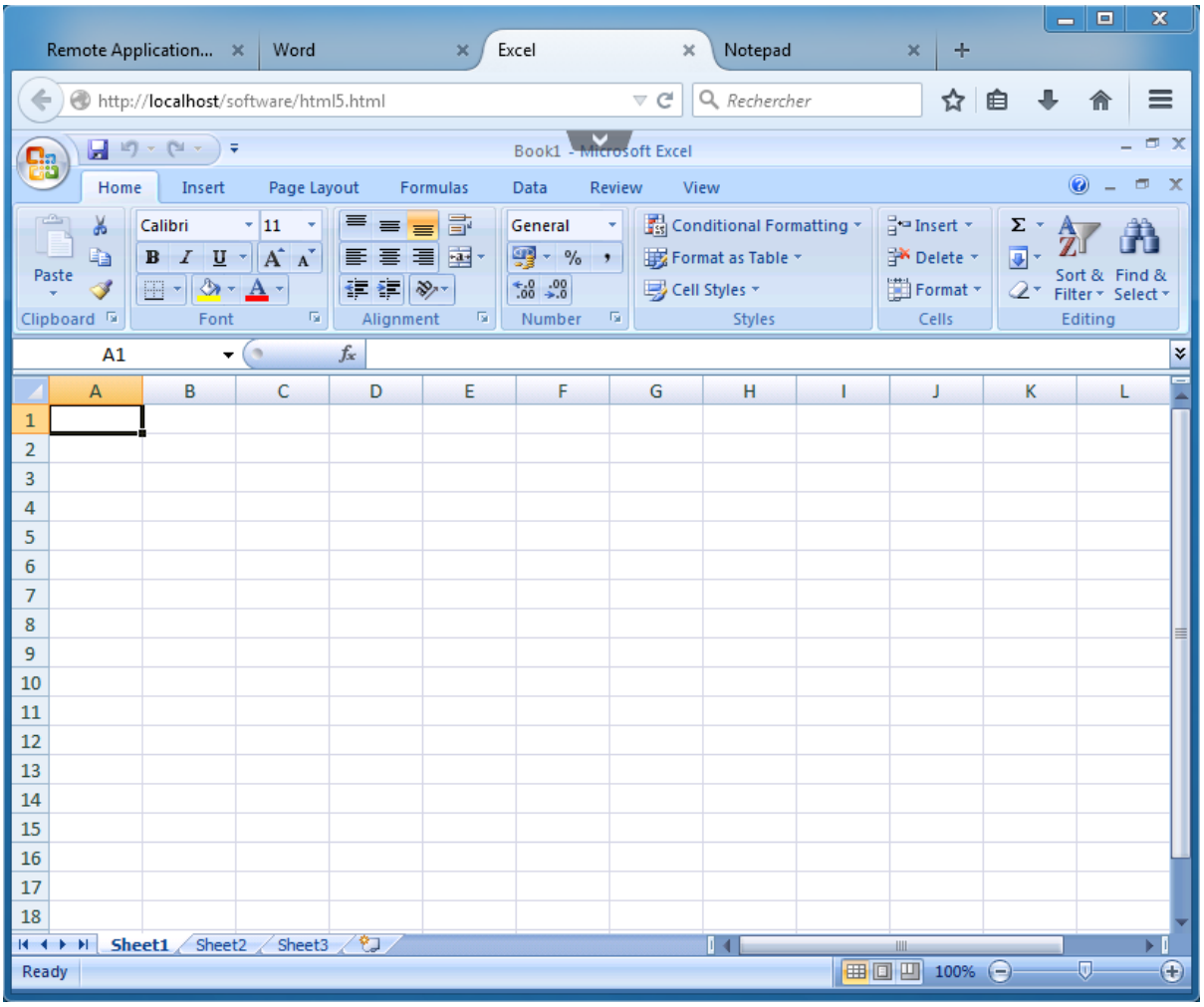


Une fois connecté, une nouvelle page web s'affiche, c'est le Portail des Applications Web :

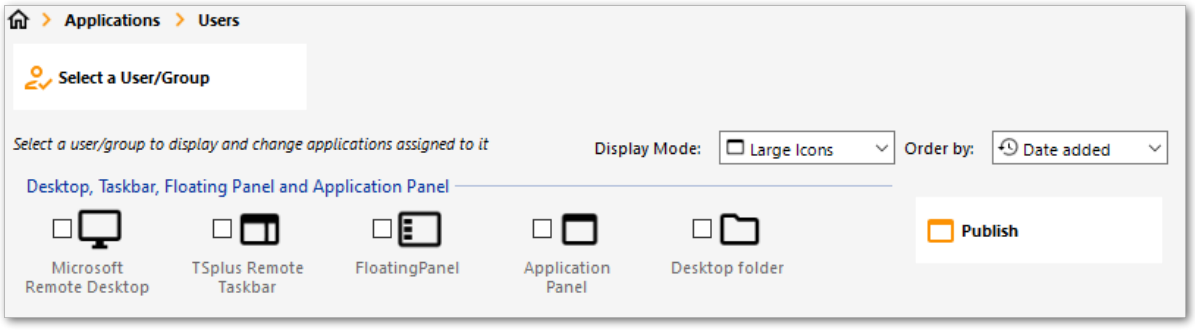


Comme vous pouvez le voir, l'utilisateur obtient une icône pour chaque application publiée à laquelle il a accès.

L'utilisateur peut maintenant cliquer sur une ou plusieurs icônes, afin d'ouvrir à distance l'application correspondante dans un nouvel onglet :

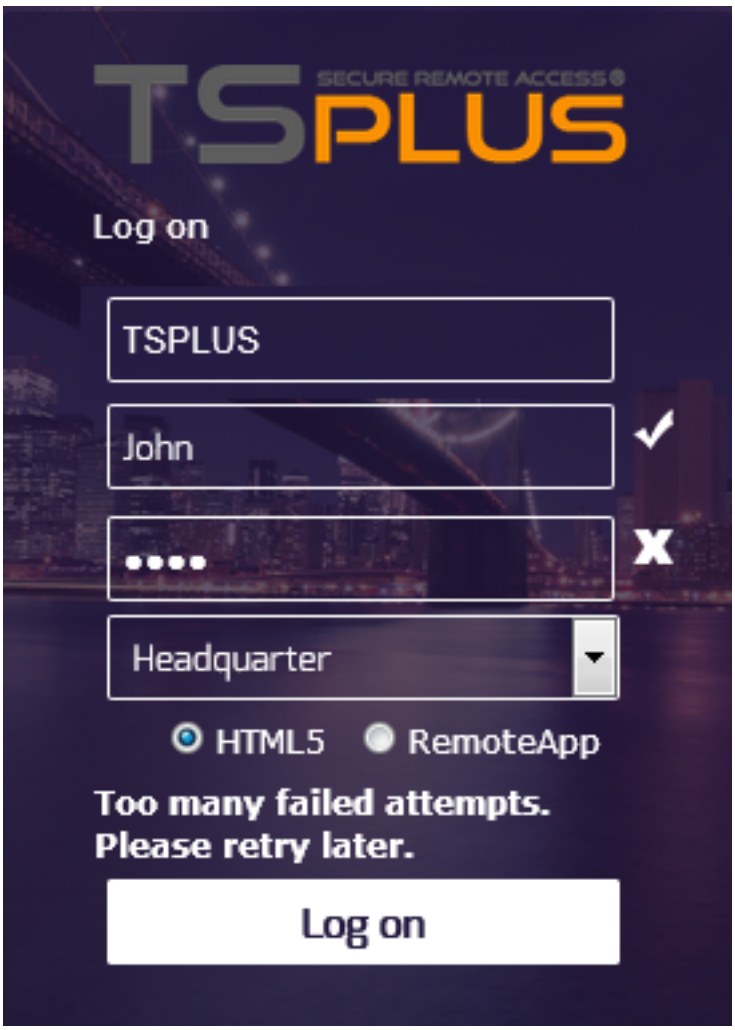


Si vous souhaitez utiliser uniquement le portail d'application sans ouvrir une session Windows, barre des tâches à distance, panneau flottant,…, vous devez décocher toutes les cases associées au profil utilisateur.



Depuis la version 11.40 de TSplus, les attaques par force brute sur le Web Portal sont désormais bloquées lorsque les utilisateurs saisissent de mauvaises informations d'identification.

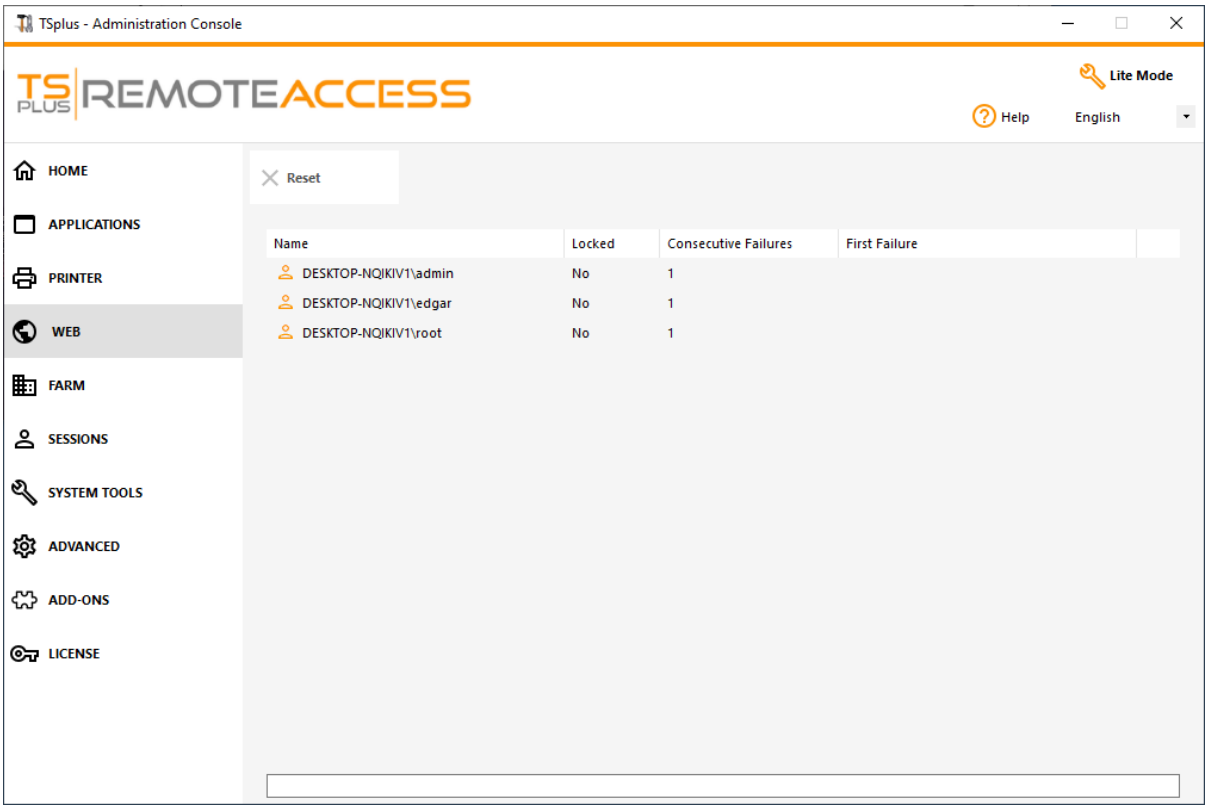
Après 10 tentatives pendant une période de 15 minutes, le Web Portal interdira à l'utilisateur de se connecter pendant 30 minutes (personnalisable sur le Advanced - Onglet de verrouillage de l'AdminTool) :]



Ce sont les paramètres par défaut qui sont personnalisables dans le fichier hb.exe.config situé dans le dossier TSplus :

TSplus\Clients\www\cgi-bin\hb.exe.config dans le paragraphe “appSettings”.

Vous pouvez vérifier toutes les connexions bloquées et les journaux par les utilisateurs dans la fonction de verrouillage de TSplus :



Cette fonctionnalité est visible et actif après la première connexion au Web Portal.

Notes importantes

- La fonctionnalité du portail des applications Web est compatible avec Configuration de la ferme / passerelle et il prend également en charge équilibrage de charge .
- Dans une configuration de ferme / passerelle, les applications doivent être publiées et assignées sur chaque serveur de la ferme à ce moment-là.
- En ce qui concerne la licence de Terminal Service Plus, un utilisateur peut ouvrir plusieurs applications en même temps sans compter pour plus d'un utilisateur.

Web Autologon : se connecter depuis le web sans portail

Aperçu

Le portail Web de Terminal Service Plus permet aux utilisateurs de se connecter à leurs serveurs distants depuis n'importe quel navigateur Web simplement en utilisant leurs identifiants Windows.

Parfois, cependant, vous souhaitez vous connecter automatiquement lorsque vous lancez une adresse URL donnée. Cette fonctionnalité s'appelle Web Autologon.

Avec Web Autologon, vous vous connecterez en utilisant les paramètres (identifiant, mot de passe, ports, …) spécifiés dans des fichiers spécifiques de Terminal Service Plus.

Avertissement

Lorsque vous utilisez cette fonctionnalité, votre nom d'utilisateur et votre mot de passe peuvent être exposés à quiconque visitant la page.

De plus, si tous vos utilisateurs partagent le même nom d'utilisateur, il se peut que des utilisateurs puissent voir des informations sensibles d'autres utilisateurs partageant le même nom d'utilisateur.

Cette fonctionnalité est destinée à des cas d'utilisation spécifiques uniquement et n'est pas recommandée.

Web Autologon utilisant le client HTML5

Vous pourrez vous connecter directement en naviguant vers http://your-server/software/html5.html

Vous pouvez modifier les paramètres de connexion en éditant le fichier suivant avec Notepad ou tout éditeur de texte (tel que Notepad++ - n'utilisez pas MS Word) :

C:\Program Files (x86)\TSplus\Clients\www\software\html5\settings.js

Vous devrez spécifier au moins un identifiant et un mot de passe afin de bénéficier de l'Autologon Web.

Vous devrez peut-être actualiser la page de votre navigateur après avoir modifié ce fichier.

Autologon Web utilisant le client Web RemoteApp

Vous pourrez vous connecter directement en naviguant vers http://your-server/software/remoteapp2.html

Vous pouvez modifier les paramètres de connexion en éditant le fichier suivant avec Notepad ou tout éditeur de texte (tel que Notepad++ - n'utilisez pas MS Word) :

C:\Program Files (x86)\TSplus\Clients\www\software\remoteapp2.js

Vous devrez spécifier au moins un identifiant et un mot de passe afin de bénéficier de l'Autologon Web.

Vous devrez peut-être actualiser la page de votre navigateur après avoir modifié ce fichier.

Activer plusieurs sessions utilisateur avec les mêmes identifiants

Si vous souhaitez activer plusieurs sessions utilisateur en utilisant les mêmes identifiants, vous pouvez suivre cette procédure.

Vous pouvez copier le fichier index.html situé dans :

C:\Program Files (x86)\TSplus\Clients\www

autant de fois que votre nombre d'utilisateurs. Vous pouvez le renommer et y accéder ensuite avec l'url : http://nameofyourserver.com/renamedindex.html

Modifier le paragraphe correspondant aux identifiants des utilisateurs :

Configuration d'accès ---------- var user = ""; // Identifiant à utiliser lors de la connexion au serveur distant (laisser "" pour utiliser l'identifiant saisi sur cette page) var pass = ""; // Mot de passe à utiliser lors de la connexion au serveur distant (laisser "" pour utiliser le mot de passe saisi sur cette page) var domain = "";

Vous pouvez copier le fichier index.html autant de fois que vous le souhaitez, le renommer avec le nom d'utilisateur facilitera la fourniture d'un lien personnel.

Identifiants Web

Aperçu

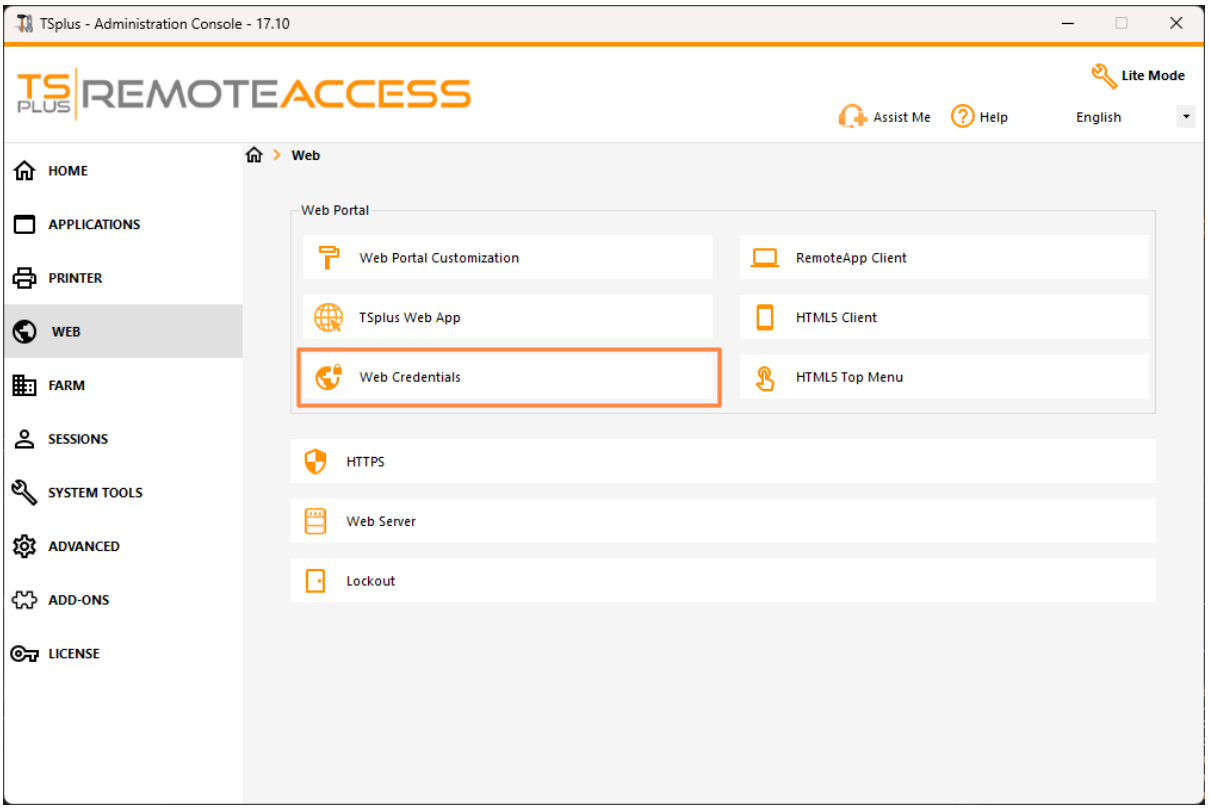
Les identifiants Web de Terminal Service Plus sont une fonctionnalité unique à la pointe de la technologie, qui permet aux utilisateurs de se connecter simplement avec une adresse e-mail ou un code PIN.

Avec les identifiants Web, vous pouvez sécuriser l'accès de votre serveur avec l'adresse e-mail d'un utilisateur ou avec un simple code PIN généré par votre application professionnelle. L'un des grands avantages de cette fonctionnalité est que ces identifiants (e-mail ou code PIN) sont de véritables identifiants Web : l'utilisateur ne saura pas quel compte utilisateur Windows il utilise actuellement et il n'a pas besoin de connaître un véritable identifiant/mot de passe Windows pour se connecter à son application !

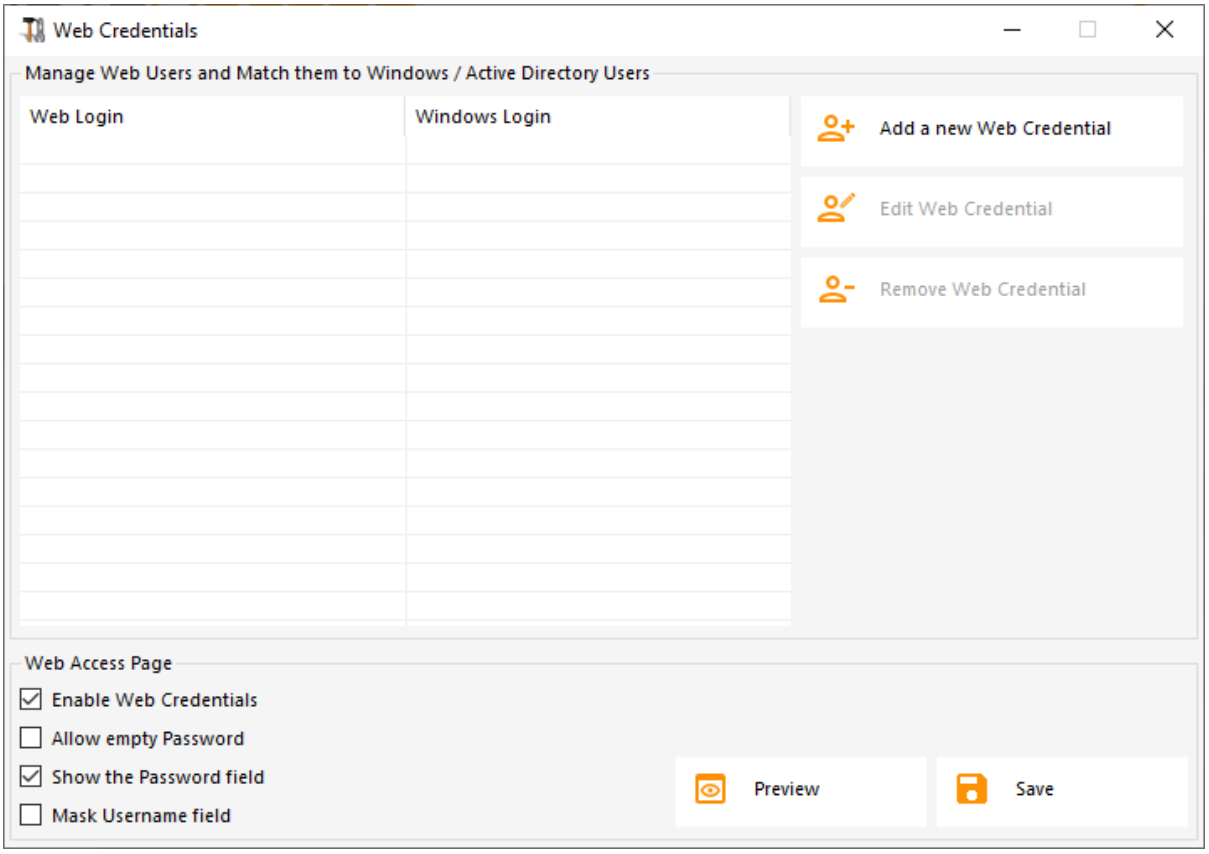
Avec les identifiants Web, vous pourrez définir des identifiants Web personnalisés et les associer à tout compte utilisateur Windows / Active Directory existant. L'utilisateur pourra alors se connecter en utilisant ces identifiants personnalisés, au lieu de ceux de Windows / Active Directory.

Gérer vos identifiants Web

Dans l'outil d'administration, ouvrez l'onglet « Web » et cliquez sur la tuile « Identifiants Web ».

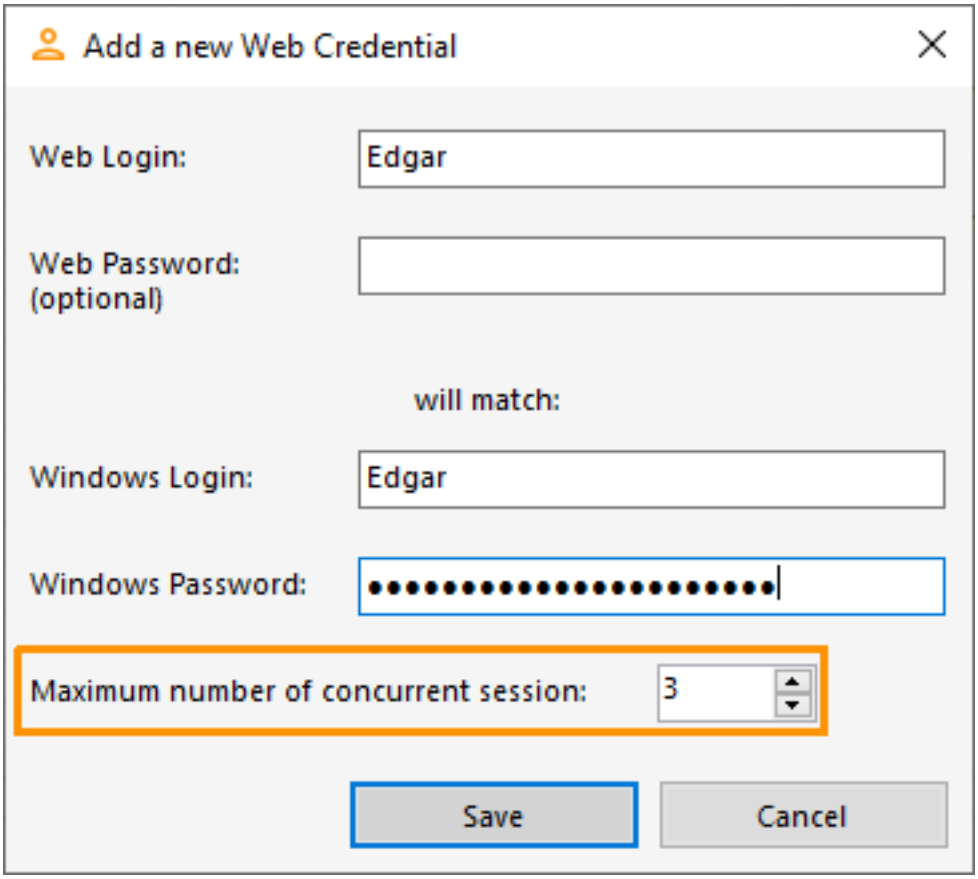


Le Gestionnaire de Crédentiels Web s'ouvrira et affichera cette fenêtre :



Vous pouvez maintenant créer une nouvelle identification Web en associant un identifiant personnalisé et un mot de passe (facultatif) à un compte utilisateur Windows / Active Directory

existant, comme indiqué ci-dessous :



Depuis la version 9.50 de TSplus, vous pouvez également décider du nombre maximum de sessions simultanées pour un utilisateur.

Vous pouvez également modifier et supprimer un identifiant Web existant, ce qui vous permet de changer ou de désactiver tout identifiant personnalisé que vous avez configuré.

Alternativement, vous pouvez créer des identifiants web via une ligne de commande :

- Dans le menu Démarrer de Windows, dans le champ d'exécution, tapez : 'cmd.exe' (ou dans Programmes/Accessoires > 'Windows Power Shell')
- Ensuite, pour accéder au bon dossier, tapez : cd “C:\Program Files (x86)\TSplus\UserDesktop\files”, puis appuyez sur Entrée pour valider.
- Pour ajouter un nouveau Web Credential, tapez : AdminTool.exe /webcredentials-add votre_identifiant_web votre_mot_de_passe_web votre_identifiant_windows votre_mot_de_passe_windows sessions_concurrentes_maximum
- Pour ajouter un identifiant vide, tapez deux guillemets doubles : "" pour indiquer un texte vide.
- Pour supprimer un identifiant web, tapez : AdminTool.exe /webcredentials-remove votre_identifiant_web

si vous aimez utiliser des lignes de commande et vous vous demandez quelles autres lignes de commande sont disponibles, veuillez vous rendre à ceci documentation spécifique)

Notes importantes

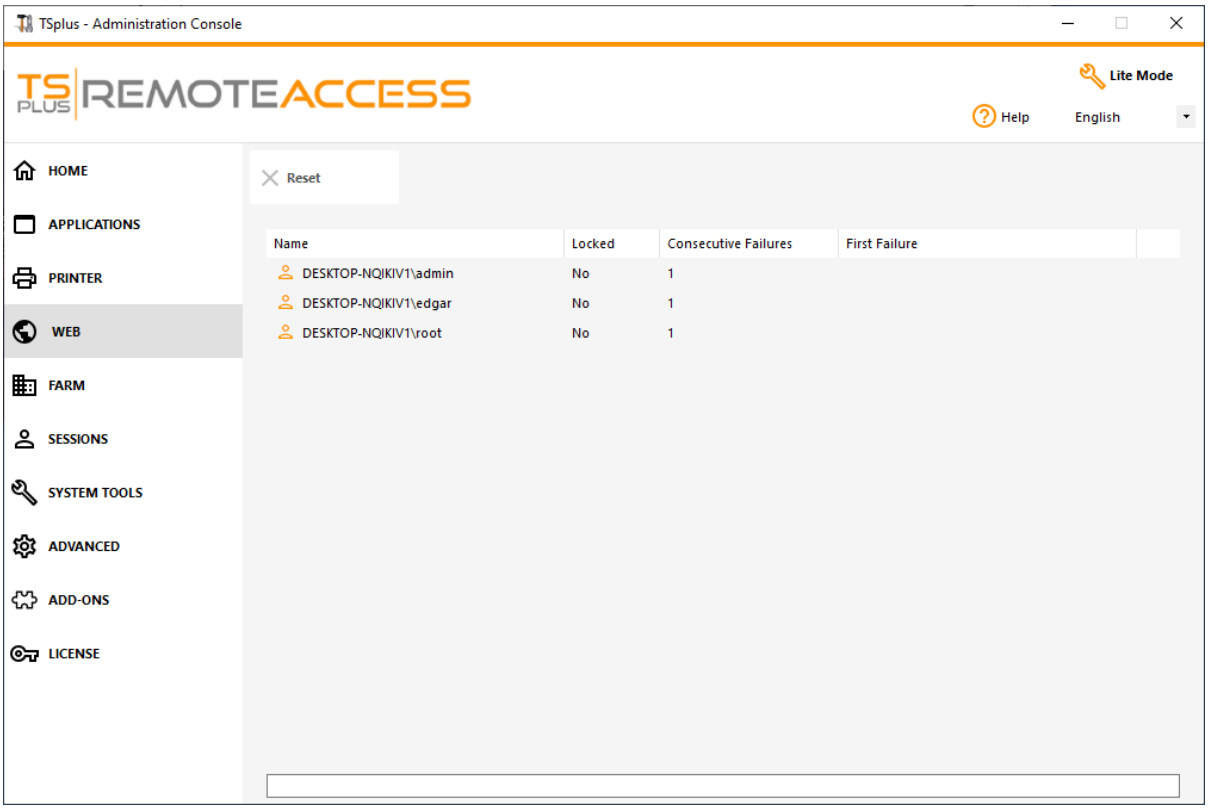
Veuillez noter les limitations suivantes :

- Les caractères '[', ']' et '°' ne sont pas pris en charge dans les champs de mot de passe.
- Dans un Configuration de la ferme / passerelle Les identifiants Web ne prennent en charge que le mode de répartition de charge (il ne fonctionne pas avec le mode assigné par le serveur).
- Dans une configuration de ferme / passerelle avec mode de répartition de charge, les identifiants Web doivent être définis sur chaque serveur de la ferme au moment.
- 2FA n'est pas compatible avec la fonctionnalité Web Credentials.

Verrouillage Web

TSplus Web lockout, introduit avec la version 12.40, est une interface utilisateur pour la fonctionnalité de verrouillage du portail Web, pour débloquer des comptes et modifier des paramètres avancés :

FAQ : sur la façon de configurer la fonction de verrouillage du portail Web HTML5



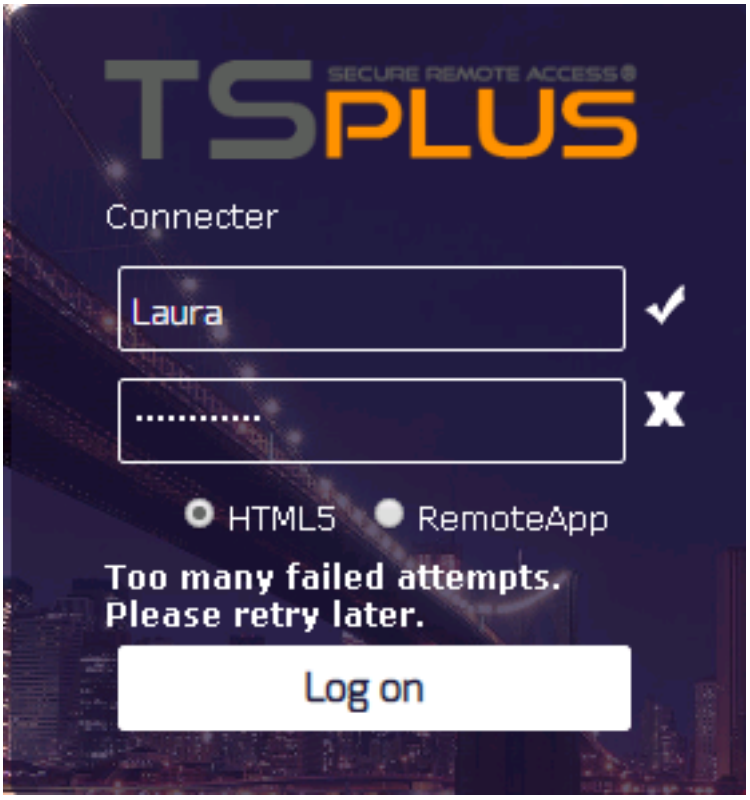
Les moniteurs de verrouillage surveillent les tentatives de connexion Web échouées sur votre serveur TSplus. Ils enregistrent les tentatives et bloquent automatiquement l'utilisateur correspondant après que le nombre autorisé de tentatives échouées a été atteint.

Vous verrez facilement si une adresse a été verrouillée sous la colonne « Verrouillé ».

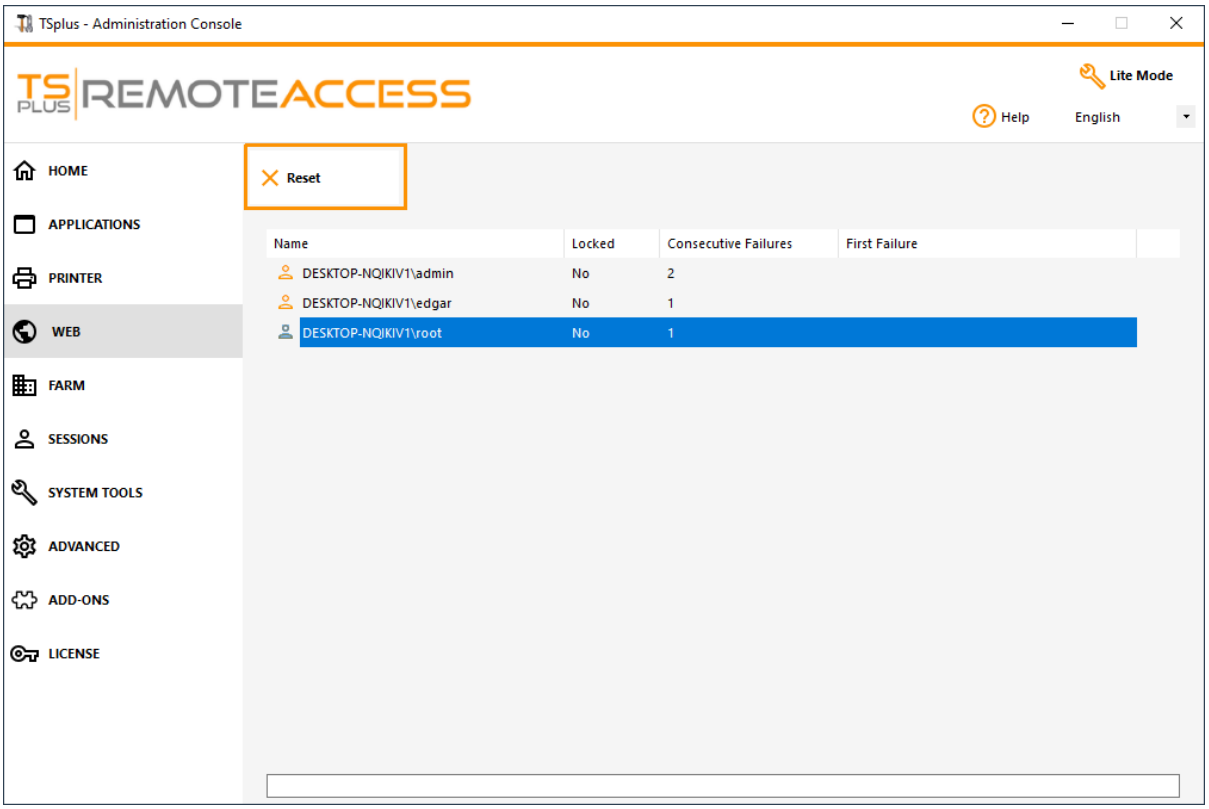
La colonne suivante indique le nombre d'échecs consécutifs pour chaque utilisateur.

Sur le portail Web, un message indique à l'utilisateur que trop de tentatives échouées ont été

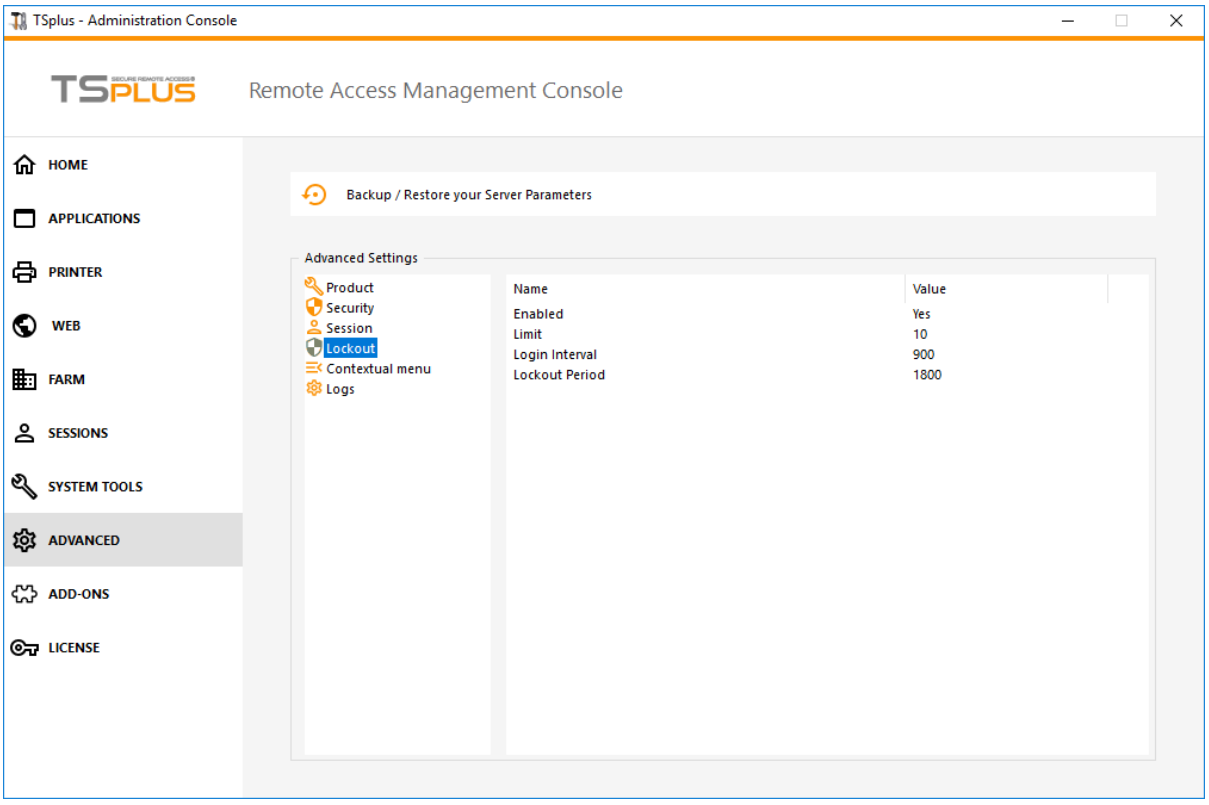
effectuées :



Les utilisateurs peuvent être rapidement supprimés de cette liste, débloqués et ajoutés à la liste blanche depuis la console de gestion facile à utiliser dans l'onglet Web de l'AdminTool. Il suffit de cliquer sur l'utilisateur que vous souhaitez réinitialiser ou débloquer, puis de cliquer sur « Réinitialiser ».



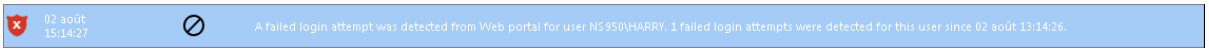
Le seuil de blocage des utilisateurs peut être configuré par l'administrateur, dans l'onglet Paramètres avancés de l'AdminTool :



Vérifiez la documentation pour configurer les paramètres de verrouillage.

Intégration de TSplus Advanced Security avec Lockout

Si une tentative de connexion échouée a été détectée sur le portail Web, TSplus Advanced Security indiquera le **Événement de verrouillage, correspondant à un nom d'utilisateur dans le Visualiseur d'événements de sécurité** :



Une tentative de connexion échouée a été détectée depuis le portail Web pour l'utilisateur … 1 tentative de connexion échouée a été détectée pour cet utilisateur depuis…

TSplus Advanced Security BruteForce Protection

TSplus Advanced Security Bruteforce Protection couvre le **Aspect des adresses I.P. des clients** Ainsi, cela fonctionne également pour les connexions RDP.

Échecs des tentatives de connexions par force brute , sont également visibles sur le journal des événements de TSplus Advanced Security (les adresses IP privées sont exclues pour éviter de bloquer le proxy) :



Une tentative de connexion échouée a été détectée depuis l'adresse IP … . Cette adresse IP n'est pas sur la liste blanche et sera bloquée après plusieurs tentatives échouées de connexion. Nom d'utilisateur fourni : Harry.

Pour plus d'informations sur la protection contre les verrouillages et les attaques par force brute, consultez cette documentation et le Documentation de la protection contre les attaques par force brute

Page de connexion Web : Comment changer l'écran de démarrage de connexion

Aperçu

Lorsque la connexion à distance se charge, le client HTML5 affiche un écran de démarrage par défaut tel que la capture d'écran ci-dessous :



Vous pouvez personnaliser ce contenu en modifiant un fichier de configuration JavaScript.

Client HTML5

Créer le contenu de votre écran de démarrage personnalisé

Tout contenu dans le texte ou HTML peut être utilisé pour l'écran de démarrage.

Aussi, si vous devez utiliser des apostrophes simples (’) ou des guillemets doubles (”), vous devrez écrire un antislash avant (’ et ”) au lieu de simplement les guillemets.

Enfin, veuillez noter que le contenu doit être rédigé en une seule ligne.

L'exemple suivant est un contenu valide pour l'écran de démarrage :

Ceci est mon écran de démarrage personnalisé

Veuillez dire "bonjour"!
Il affichera un titre (“Ceci est mon écran de démarrage personnalisé”), un texte (“Veuillez dire bonjour !”) et l'image animée de l'anneau comme dans l'écran de démarrage standard de TSplus.

Modifier les données de l'écran de démarrage pour utiliser votre propre contenu

Si vous n'avez pas de fichier nommé "settings.js" dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software\html5", alors votre version de TSplus est plus ancienne et cette documentation ne s'applique pas. Veuillez d'abord mettre à jour votre système ou contacter le support.

Modifiez le fichier “settings.js” situé dans le dossier “C:\Program Files (x86)\TSplus\Clients\www\software\html5”. Nous vous conseillons d'utiliser un éditeur de texte tel que Notepad ou Notepad++. non utiliser Word).

Recherchez la ligne commençant par ceci :

W.splashscreencontent = ”

Remplacez-le complètement par la ligne suivante :

W.splashscreencontent = “votre contenu personnalisé ici”;

N'oubliez pas les guillemets de fin et le point-virgule (”;).

Si vous souhaitez prolonger la durée de l'écran de connexion en HTML5, vous pouvez le faire en modifiant la valeur en millisecondes :

W.splashscreentime = 5000; //temps de lecture de l'écran de démarrage.

Nous vous recommandons de vider le cache de votre navigateur après avoir enregistré la page html modifiée.

Page de connexion Web : Comment fermer le formulaire de connexion après la connexion

Aperçu

Sur la page de connexion Web, lorsque l'utilisateur clique sur le bouton « Se connecter », le client choisi (HTML5 ou Windows) s'ouvre dans un nouvel onglet du navigateur.

Parfois, et plus précisément lors de l'utilisation du client Windows, vous pourriez vouloir cacher le formulaire de connexion à l'utilisateur, par exemple afin d'éviter que l'utilisateur ne clique à nouveau sur le bouton « Connexion ».

Selon le navigateur Internet utilisé, vous avez deux choix sur la façon de modifier ce comportement par défaut. Les deux solutions nécessitent de modifier un fichier JavaScript.

Solution A : Fermer l'onglet de connexion - Pour Internet Explorer uniquement

Dans cette solution, lorsque l'utilisateur clique sur le bouton « Se connecter », le client choisi s'ouvrira dans un nouvel onglet du navigateur et l'onglet de connexion se fermera automatiquement. Selon la version d'Internet Explorer, une petite fenêtre de message peut s'afficher à l'utilisateur, lui demandant de confirmer qu'il souhaite fermer cet onglet.

Modifiez le fichier "common.js" qui est stocké dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software". Nous vous conseillons d'utiliser un éditeur de texte tel que Notepad ou Notepad++. non utiliser Word).

Recherchez ces lignes :

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
```

Et remplacez-les par ces lignes :

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
window.open('','_parent','');
window.close();
```

Nous vous recommandons de vider le cache de votre navigateur après avoir enregistré le fichier JavaScript modifié.

Solution B : Rediriger l'onglet de connexion vers une autre page web - Pour tous les navigateurs

Dans cette solution, lorsque l'utilisateur clique sur le bouton « Se connecter », le client choisi s'ouvrira dans un nouvel onglet du navigateur et l'onglet de connexion naviguera automatiquement vers une autre page web.

Vous êtes libre d'utiliser n'importe quelle adresse Internet existante (URL) telle que « http://google.com ou pouvez également créer votre propre page web en utilisant "thankyou.html" comme URL et en créant un fichier nommé "thankyou.html" dans le dossier "C:\Program Files (x86)\TSplus\Clients\www" et en y mettant du contenu HTML.

Modifiez le fichier "common.js" qui est stocké dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software". Nous vous conseillons d'utiliser un éditeur de texte tel que Notepad ou Notepad++. non utiliser Word).

Recherchez ces lignes :

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
```

Et remplacez-les par ces lignes :

```
p = 'software/remoteapp.html';
window.name = " " + window.opforfalse;
if (cpwin != false) {
  cpwin.name = window.opforfalse;
  cpwin.location.replace(hostGateway + jwtsclickLinkBefore(getside(), p));
} else {
  window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);
}
window.location.href = "http://google.com";
```

Nous vous recommandons de vider le cache de votre navigateur après avoir enregistré le fichier JavaScript modifié.

Page de connexion Web : Comment ouvrir le client HTML5 dans le même onglet

Aperçu

Sur la page de connexion Web, lorsque l'utilisateur clique sur le bouton « Se connecter », le client HTML5 s'ouvre dans un nouvel onglet du navigateur.

Vous pouvez modifier ce comportement et faire en sorte que le client HTML5 s'ouvre dans le même onglet du navigateur que la page de connexion Web en modifiant un fichier JavaScript.

Modifier le fichier custom.js

Modifiez le fichier "custom.js" qui est stocké dans le dossier "C:\Program Files (x86)\TSplus\Clients\www". Nous vous conseillons d'utiliser un éditeur de texte tel que Notepad ou Notepad++. non utiliser Word).

Ajoutez cette ligne :

var openinsamewindow = true;

Nous vous recommandons de vider le cache de votre navigateur après avoir enregistré le fichier JavaScript modifié.

Modifier le fichier common_applications.js

Si vous utilisez la fonctionnalité du portail d'applications Web de Terminal Service Plus, vous devez alors modifier un deuxième fichier. Modifiez le fichier "common_applications.js" qui est stocké dans le dossier "C:\Program Files (x86)\TSplus\Clients\www\software". Nous vous conseillons d'utiliser un éditeur de texte tel que Notepad ou Notepad++. non utiliser Word).

Recherchez ces lignes :

```
if (childurl != '') {
  window.name = childname;
  location.href = childurl + '#';
}
```

Et remplacez-les par ces lignes :

```
  if (childurl != '') {
    window.name = childname;
    location.href = childurl + '#';
  }
```

Nous vous recommandons de vider le cache de votre navigateur après avoir enregistré le fichier JavaScript modifié.

Portail Web avec SSO (bêta)

Conditions préalables et limitations clés

Web Portal 2026 avec SSO est conçu pour le **Créatif** thème et utilise toutes les personnalisations de AdminTool > Web > Personnalisation du portail Web. Si le thème sélectionné n'est pas **Créatif** le portail Web ne s'affiche pas.

Lorsque activé dans une ferme, tous les serveurs doivent exécuter le **même version Remote Access** et être activé pour **Web Portal 2026 avec SSO**

Cette fonctionnalité est **Bêta** et devrait **non** être déployé sur des serveurs de production.

Pourquoi un nouveau portail Web ?

Comparé au précédent portail Web, cette mise en œuvre offre une fiabilité supérieure et de meilleures performances sous charge. De plus, elle permet :

- **Capacités SSO avancées**
  - Authentification intégrée Windows (Négocier / Kerberos / NTLM)
  - Intégration de fournisseur d'identité tiers (actuellement SAML)
- **Des contrôles de sécurité renforcés**
  - Protections anti-contrefaçon intégrées
  - Limitation de taux des points de terminaison
  - Authentification moderne et contrôles des cookies/sessions

Son architecture nous permettra de répondre facilement à tout retour d'audit de sécurité potentiel.

C'est aussi un **produit plus accessible** par des recommandations et un contraste amélioré.

Flexibilité du serveur Web (Kestrel par défaut)

L'application n'est pas liée à un seul serveur web frontal. Par défaut, elle s'exécute sur **Kestrel** (Port HTTP 81). Il peut être précédé par **IIS** ou **Apache** comme un proxy inverse en modifiant la configuration du serveur web.

Exemple : proxy inverse Apache vers le service Web Portal

```
# Apache VirtualHost example
ProxyPreserveHost On
ProxyPass        /  http://127.0.0.1:81/
ProxyPassReverse /  http://127.0.0.1:81/

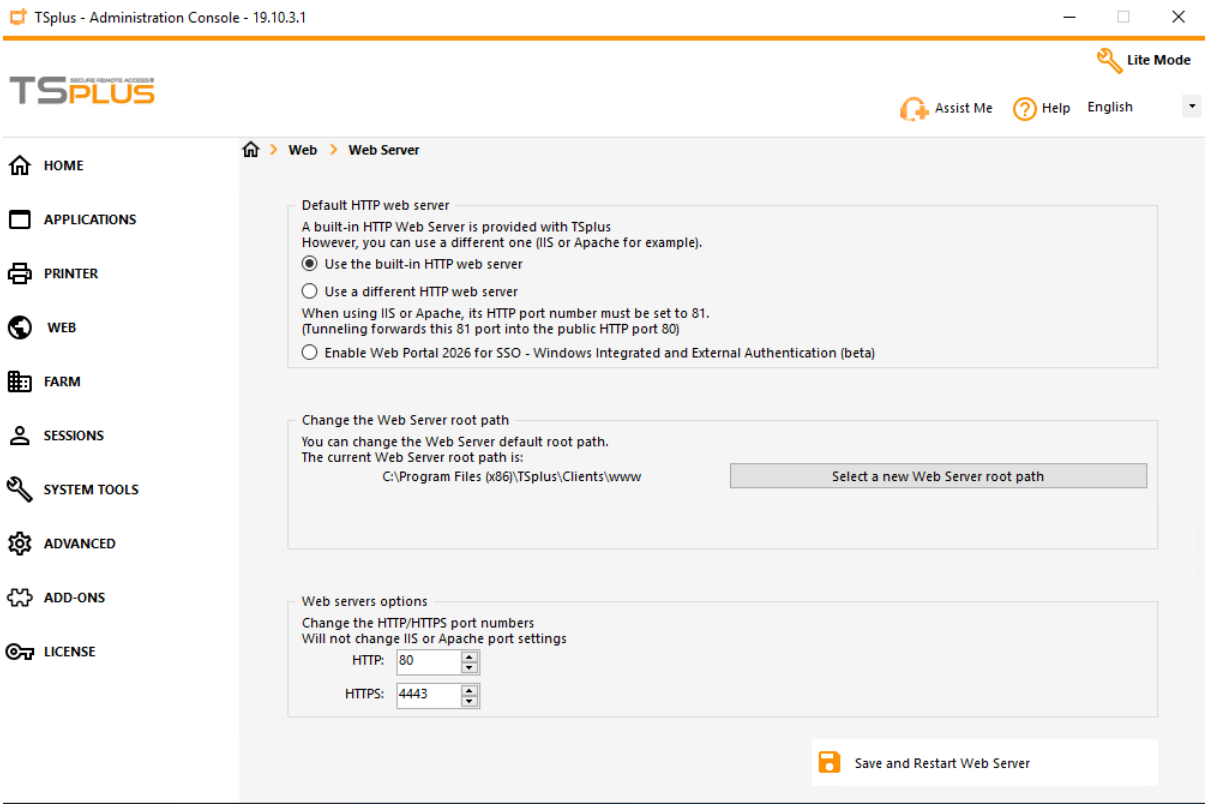
RequestHeader set X-Forwarded-Proto "https"
RequestHeader set X-Forwarded-For "%{REMOTE_ADDR}s"
```

Cela maintient la logique du portail Web inchangée tandis qu'Apache gère l'exposition publique HTTP/HTTPS.

Veuillez contacter l'équipe de développement si vous êtes intéressé, car ce scénario n'est pas encore accessible depuis le programme AdminTool et doit être configuré manuellement.

Activer le portail Web 2026 avec SSO

1. Ouvrir **AdminTool**
2. Allez à : Web **>** Serveur web
3. Activer : **Portail web 2026 avec SSO**



Important cette option est en version Beta. Utilisez-la uniquement dans des environnements de test.

Modes de connexion pris en charge

Portail Web 2026 avec SSO prend en charge :

- Formulaire de connexion traditionnel utilisant des identifiants Windows
- Identifiants Web. Voir : https://docs.tsplus.net/tsplus/web-credentials/
- Authentification intégrée Windows (automatique dans les scénarios de confiance / locaux)
- Fournisseur d'identité externe via **SAML** tel que Entra ID (anciennement Azure AD) ou Okta

Remarque : Support pour l'authentification externe via **OIDC** prévu plus tard, sur demande

comportement 2FA

2FA est appliqué aux flux de compte standard, y compris :

- Formulaire de connexion utilisant des identifiants Windows
- Identifiants Web
- Authentification intégrée Windows

Les fournisseurs d'authentification externes appliquent souvent leur propre MFA / 2FA. Ainsi, la configuration 2FA définie dans l'addon 2FA de Remote Access ne s'applique pas à ce scénario.

Le contournement du réseau local est disponible via CustomSettings:Contournement2FAPourRéseauLocal paramètre situé dans le fichier : C:\Program Files (x86)\TSplus\Clients\webportal\appsettings.json , où C:\Program Files (x86)\TSplus est le dossier de configuration de TSplus Remote Access. Lorsqu'il est activé, le contournement se produit uniquement si le client et la passerelle se trouvent dans le même sous-réseau privé.

Configurer le flux d'authentification Windows

Pour les utilisateurs se connectant avec l'authentification Windows, l'un des éléments suivants est requis :

1. Pré-enregistrer les identifiants avec la commande TSplus : AdminTool.exe / windowscredential-ajouteroumettre à jour Voir la documentation à https://docs.tsplus.net/tsplus/commands-list/#ajouter-ou-mettre-à-jour-des-identifiants-dans-le-gestionnaire-d-identifiants-windows-windowscredential-addorupdate
2. Ou laissez l'utilisateur se connecter une fois via le formulaire de connexion du portail Web avec des identifiants Windows.

Pour configurer l'authentification intégrée Windows, veuillez consulter : Activer l'authentification intégrée Windows sur un domaine Active Directory. Comme ce mode d'authentification est difficile à configurer, les clients préfèrent souvent mettre en place un fournisseur d'identité externe.

Configurer l'authentification externe (SAML)

Paramètres requis pour l'application externe

L'application externe doit être configurée comme suit :

- URL de connexion unique doit être défini sur le point de terminaison du service consommateur SAML du portail Web, par exemple https://mywebportal.company.com/Saml/acs
- URI d'audience (ID d'entité SP) doit être défini sur le nom de domaine ou l'adresse IP du portail Web, par exemple https://mywebportal.company.com
- Format d'identifiant de nom doit être défini sur **AdresseEmail**
- Nom d'utilisateur de l'application doit être défini sur **Email** , car la partie gauche identifiera le nom d'utilisateur du compte Windows

Paramètres requis dans appsettings.json

Le fichier appsettings.json est situé dans C:\Program Files (x86)\TSplus\Clients\webportal , où C:\Program Files (x86)\TSplus est le dossier de configuration de TSplus Remote Access.

Modifier le Saml2 section :

- IdPMetadata
- Émetteur
- Destination de l'authentification unique optionnel si les métadonnées le fournissent
- Destination de déconnexion unique optionnel si les métadonnées le fournissent
- Champs liés au certificat

Par exemple, en utilisant le fournisseur d'identité tiers okta :

```
"Saml2": {
  "IdPMetadata": "https://mycompany.okta.com/app/abcdfegh12345678/sso/saml/metadata",
  "Issuer": "https://portal.mycompany.com",
  "SingleSignOnDestination": "https://mycompany.okta.com/app/mycompany_portalsaml_1/
abcdfegh12345678/sso/saml",
  "SingleLogoutDestination": "https://mycompany.okta.com",
  "SignatureAlgorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256",
  "SigningCertificateFile": "",
  "SigningCertificatePassword": "",
  "SignatureValidationCertificateFile": "okta.identity.saml2.portal.cert",
  "CertificateValidationMode": "ChainTrust",
  "RevocationMode": "Offline",
  "XmlCanonicalizationMethod": "http://www.w3.org/2001/10/xml-exc-c14n#"
}
```

Le paramètre de l'émetteur définit l'URI de l'audience, tel que défini du côté du fournisseur d'identité externe.

si le Fichier de certificat de validation de signature le paramètre est défini sur une valeur autre que **Aucun** alors, veuillez vous assurer que le certificat est considéré comme valide sur le serveur d'application. Cela peut nécessiter d'ajouter le certificat à la liste des certificats de

confiance à l'échelle de la machine.

Disponibilité du mot de passe Windows pour le lancement de session

Pour l'authentification SAML externe, le lancement des sessions nécessite toujours des identifiants Windows utilisables. Utilisez l'un des :

1. Enregistrer les informations d'identification Windows avec la commande : AdminTool.exe / windowscredential-ajouteroumettre à jour Voir la documentation à https://docs.tsplus.net/tsplus/commands-list/#ajouter-ou-mettre-à-jour-des-identifiants-dans-le-gestionnaire-d-identifiants-windows-windowscredential-addorupdate
2. Ou transférer le mot de passe de la revendication IdP en configurant CustomSettings:UtiliserSamlPasswordClaim au type de réclamation contenant le mot de passe Windows.

Typiquement, le portail Web prendra la partie avant le '@' de l'adresse e-mail de l'utilisateur comme le nom d'utilisateur du compte Windows.

Veuillez noter que l'authentification externe fonctionne actuellement avec des utilisateurs locaux.

Si aucun mot de passe n'est disponible dans le magasin de revendications ou de certificats, la validation de l'utilisateur échoue.

Référence complète du fichier de configuration appsettings.json

Le fichier appsettings.json est situé dans C:\Program Files (x86)\TSplus\Clients\webportal , où C:\Program Files (x86)\TSplus est le dossier de configuration de TSplus Remote Access.

Journalisation

Paramètre	Objectif	Valeurs possibles
Journalisation:NiveauDeJournal:ParDéfaut	Niveau de journalisation minimum global.	Trace , Déboguer , Information , Avertissemer , Erreur , Critique , Aucun
Journalisation:NiveauDeJournal:Microsoft.AspNetCore	Niveau de	Même que ci-

	journalisation du framework ASP.NET Core.	dessus
Journalisation:NiveauDeJournal:Microsoft.AspNetCore.Authentication	Niveau de journal du sous-système d'authentification.	Même que ci-dessus

Paramètre d'hôte global

Paramètre	Objectif	Valeurs possibles	Par défaut
Hôtes autorisés	Filtrage de l'en-tête d'hôte pour la protection des hôtes ASP.NET Core.	* (liste d'hôtes séparés par des points-virgules)	*

Limitation de taux IP

Paramètre	Objectif	Valeurs possibles	Par d
IpRateLimiting:ActiverLaLimitationDeTauxDePointDeTerminaison	Active des règles de limitation spécifiques aux points de terminaison.	vrai / faux	vrai
IpRateLimiting:StackBlockedRequests	Si vrai , les demandes bloquées continuent d'augmenter les compteurs.	vrai / faux	faux
IpRateLimiting:HttpStatusCode	Statut HTTP renvoyé lorsque la demande est bloquée.	Code HTTP entier (typiquement 429)	429
IpRateLimiting:RealIpHeader	En-tête utilisé pour résoudre l'IP du client derrière un proxy.	Nom de l'en-tête	X-Forwa For

IpRateLimiting:ClientIdHeader	En-tête client-id optionnel pour la limitation de taux personnalisée.	Nom de l'en-tête	X-Cli

IpRateLimiting:RèglesGénérales

Chaque objet de règle a :

Paramètre	Objectif	Valeurs possibles	Par défaut dans le fichier expédié
Point de terminaison	Modèle de route/ méthode à protéger.	Format VERB:/ chemin	Plusieurs défauts (voir ci-dessous)
Période	Fenêtre de tarification.	e.g. 1s , 1m , 5m , 1h , 1j	5m (pour toutes les règles par défaut)
Limite	Max demandes dans la période.	Entier positif	5 (pour toutes les règles par défaut)

Saml2

Paramètre	Objectif	Valeurs possibles	F
Saml2:IdPMetadata	URL des métadonnées IdP utilisé pour charger la configuration du fournisseur SAML.	URL HTTPS valide	
Saml2:Émetteur	ID d'entité SP (cette identité du portail Web).	chaîne URI	
Saml2:Destination de connexion unique	URL de point de terminaison IdP SSO (peut être résolu automatiquement à partir des métadonnées).	URL HTTPS	
Saml2:SingleLogoutDestination	URL de point de	URL HTTPS	

	terminaison SLO IdP (peut être résolu automatiquement à partir des métadonnées).		
Saml2:SignatureAlgorithm	Algorithme de signature XML.	Valeur URI acceptée par la bibliothèque SAML	
Saml2:SigningCertificateFile	Fichier de certificat de signature SP local (relatif au chemin de base de l'application).	Nom de fichier/chemin	
Saml2:MotDePasseDuCertificatDeSignature	Mot de passe pour le fichier de certificat de signature.	Chaine	
Saml2:FichierDeCertificatDeValidationDeSignature	Fichier de certificat IdP utilisé pour valider les signatures (optionnel si les métadonnées fournissent des certificats).	Nom de fichier/chemin	
Saml2:ModeValidationDuCertificat	Mode de validation de la chaîne de certificats.	Aucun , PeerTrust , ChainTrust , Confiance par paire ou chaîne , ConfianceRootPersonnalisée	
Saml2:ModeDeRévocation	Comportement de révocation de certificat.	NoCheck , En ligne , Hors ligne	
Saml2:XmlCanonicalizationMethod	URI de l'algorithme de canonisation XML.	URI de canonicalisation XML-DSig	

Paramètres personnalisés

Dans appsettings.json ces valeurs sont stockées sous forme de chaînes vrai / faux) et mappé à des booléens par le binding de configuration .NET.

Paramètre	Objectif	Valeurs possibles
CustomSettings:UtiliserLeCheminCompletDeLApplication	Contrôle si le chemin complet de l'application est utilisé lors de l'affichage/ lancement des applications assignées.	vrai / fau
CustomSettings:ActiverAuthentificationWindowsAutomatiqueSurLocalhost	Permet l'authentification automatique de Windows dans un scénario localhost/ loopback.	vrai / fau
CustomSettings:ActiverLeChiffrementDuMotDePasse	Crypte le domaine/le nom d'utilisateur/le mot de passe dans la chaîne de connexion de lancement HTML5 en utilisant des paramètres RSA.	vrai / fau
CustomSettings:Contournement2FAPourRéseauLocal	Contourne le 2FA du portail Web lorsque le client se trouve dans le même sous-réseau privé que le serveur.	vrai / fau
CustomSettings:UtiliserSamlPasswordClaim	Type de revendication SAML utilisé comme mot de passe Windows transféré pour	Type de réclamatio URI/nom ou chaîne vide

	le lancement de session.	

Dépannage

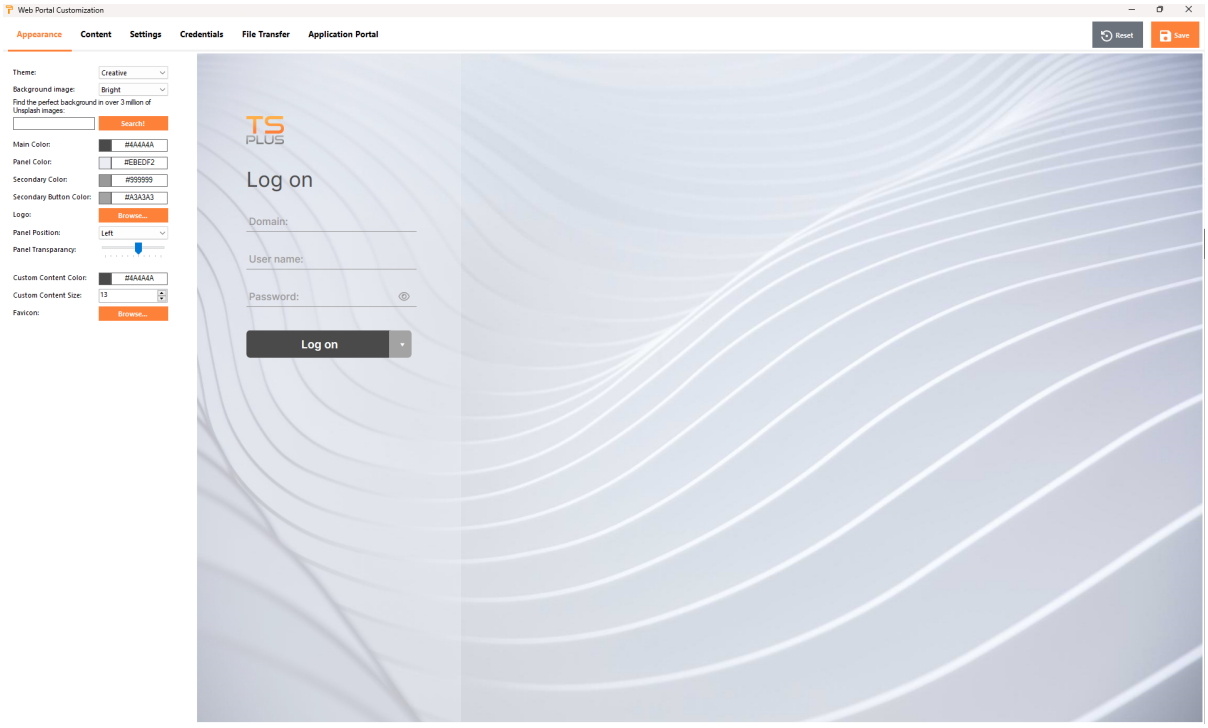
Web Portal 2026 avec les journaux SSO peut être activé depuis AdminTool > Avancé > Journaux > Journal du portail Web.

Le résultat WebPortal.log le fichier journal se trouve dans C:\Program Files (x86)\TSplus\Clients\webportal , où C:\Program Files (x86)\TSplus est le dossier de configuration de TSplus Remote Access.

Créer et personnaliser des pages d'accès Web HTML en utilisant la personnalisation du portail Web

En utilisant la personnalisation du portail Web, vous pourrez créer vos propres pages d'accès Web HTML personnalisées - et il y a pas besoin d'être un développeur web !

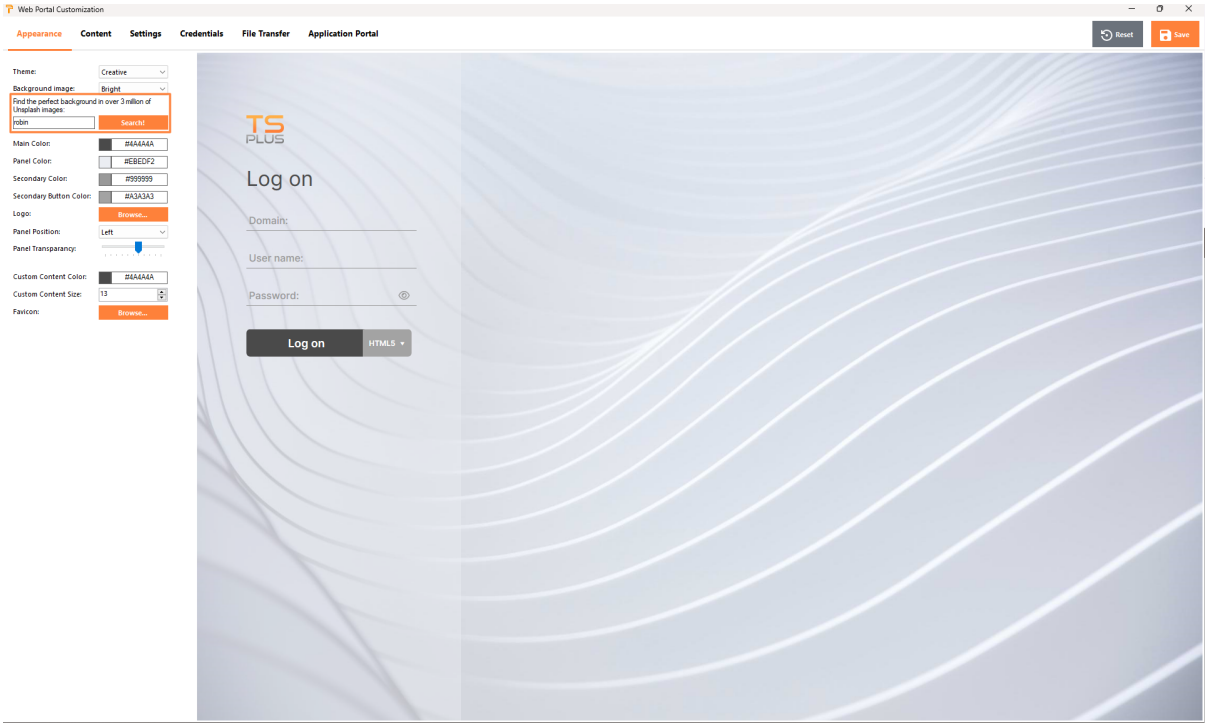
Personnalisation du portail Web - Apparence



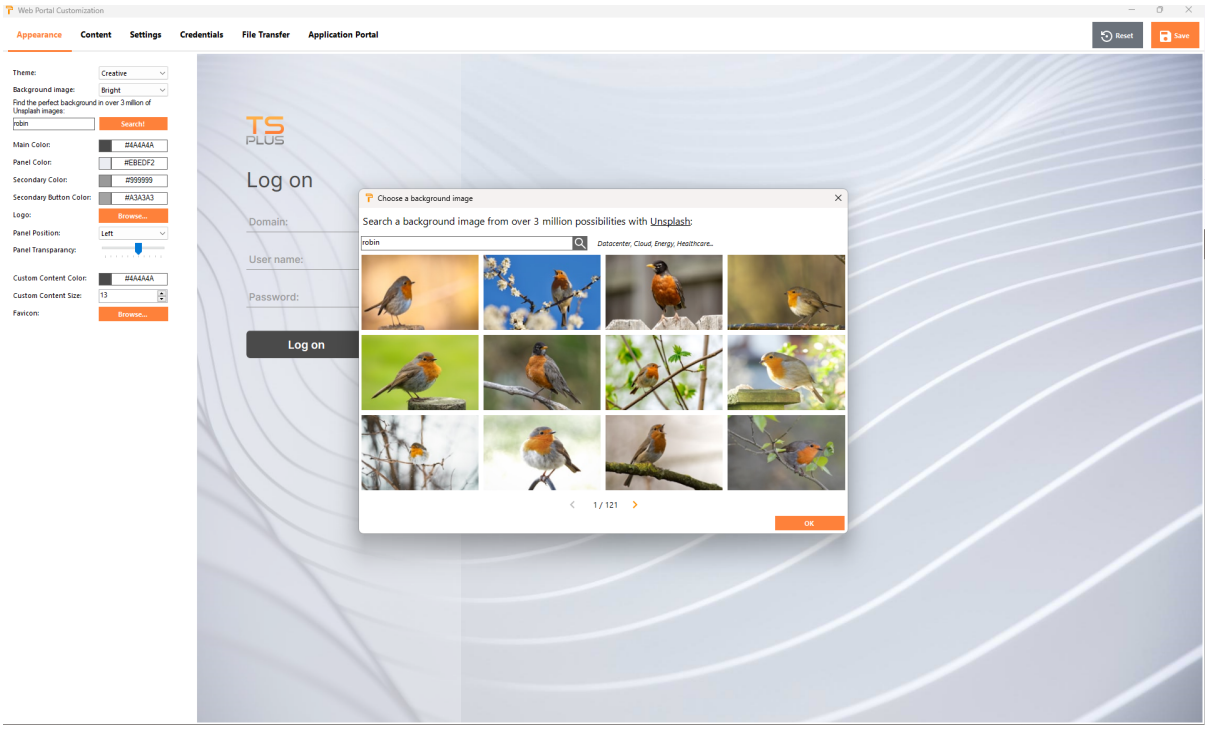
Avec l'onglet Apparence, vous pourrez personnaliser tous les paramètres graphiques, ainsi qu'ajouter votre propre logo.

Vous avez le choix entre une collection de photos, ou vous pouvez ajouter les vôtres. Vous pouvez également définir n'importe quel thème de couleur avec la couleur de fond de votre choix ou vous pouvez utiliser l'un des thèmes classiques.

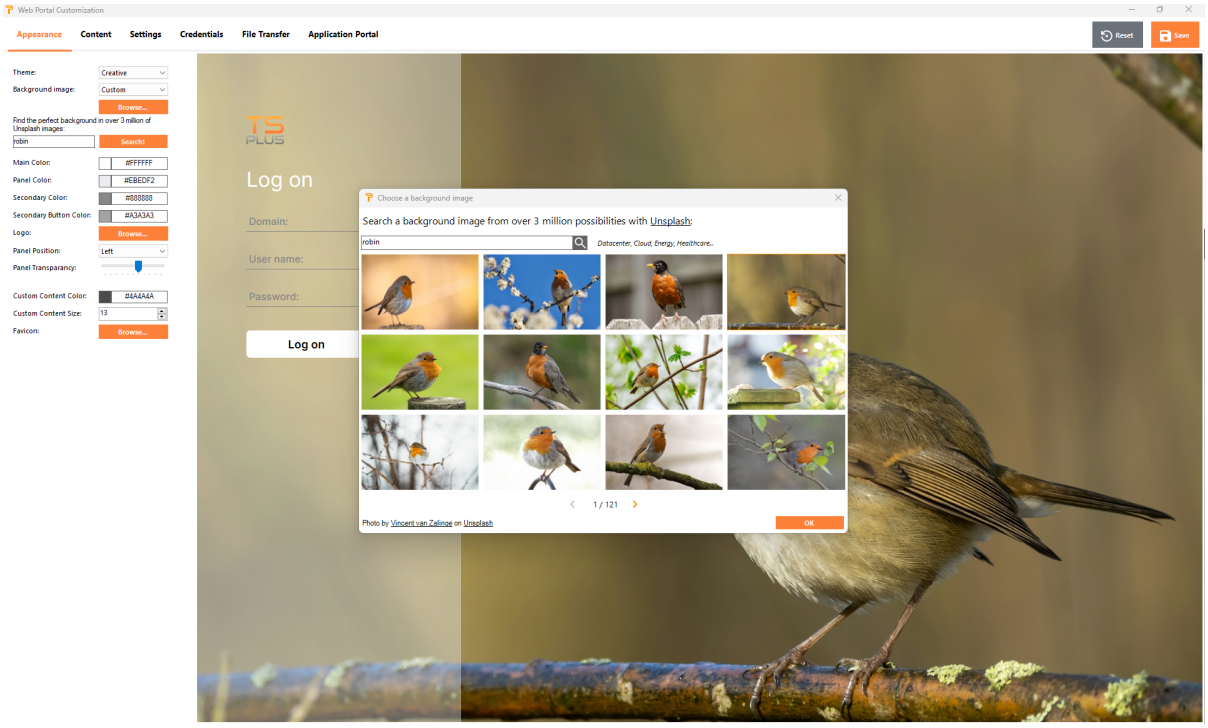
Vous pouvez également taper un mot-clé pour rechercher une image de fond dans la bibliothèque Unsplash :



Je vais afficher une collection d'images parmi lesquelles choisir.

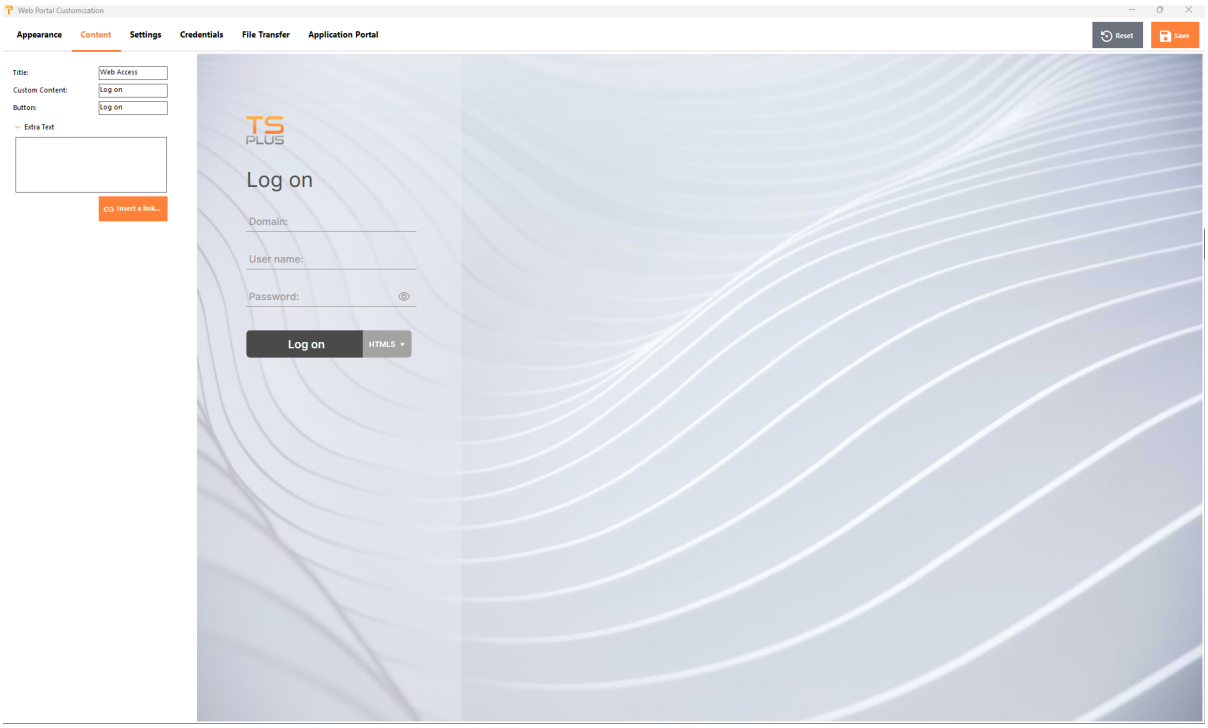


Sélectionnez votre image préférée pour voir le résultat sur votre portail web :

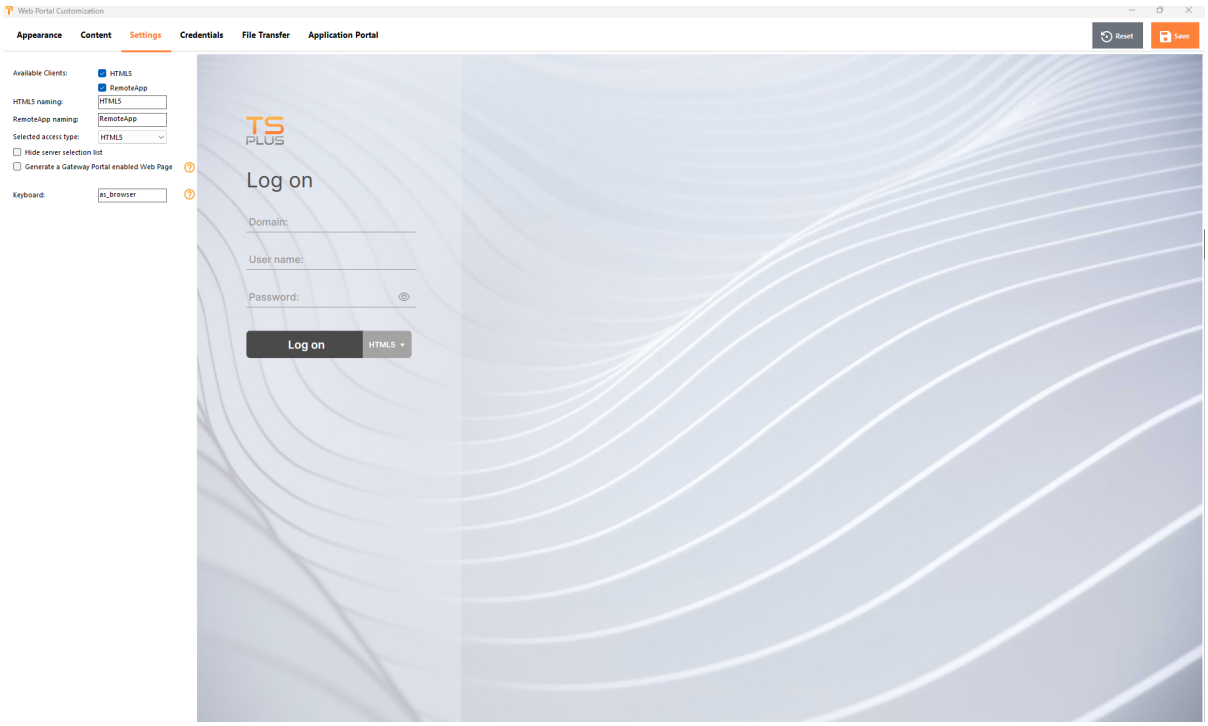


Les couleurs du thème s'adapteront automatiquement à l'image choisie une fois que vous aurez validé votre choix avec le bouton « Ok ». Bien sûr, vous pouvez toujours personnaliser les couleurs comme vous le souhaitez.

Personnalisation du portail Web - Contenu

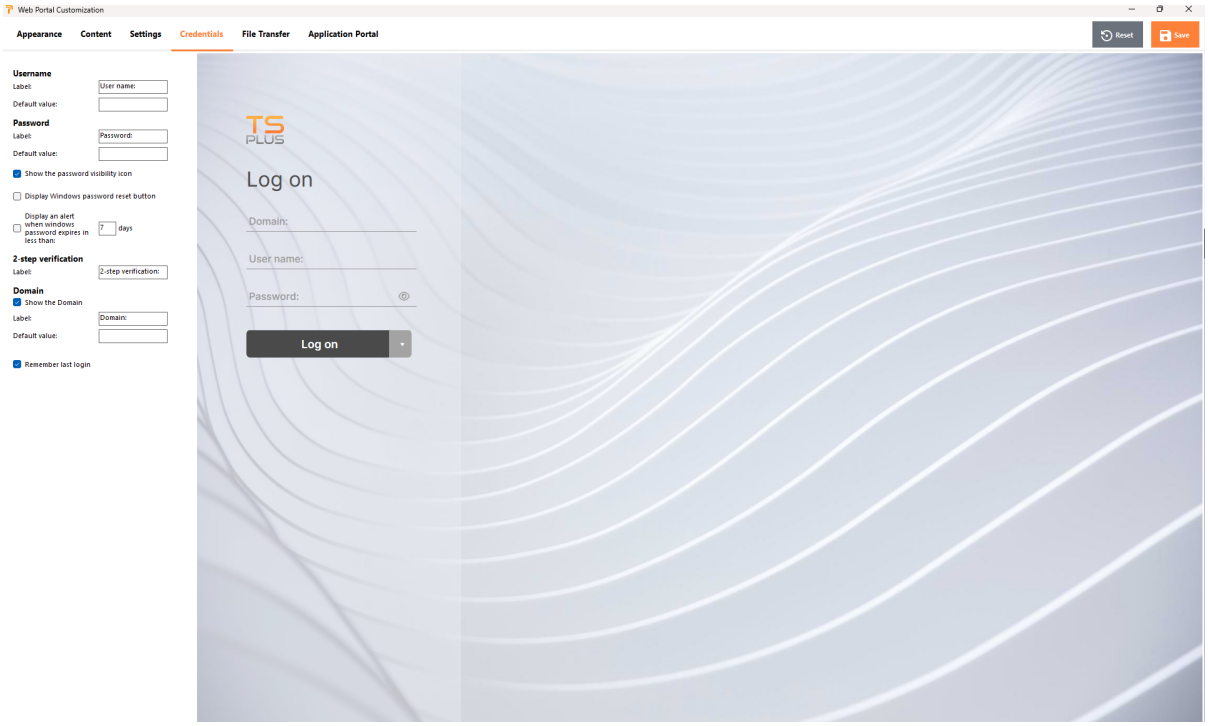


Personnalisation du portail Web - Paramètres

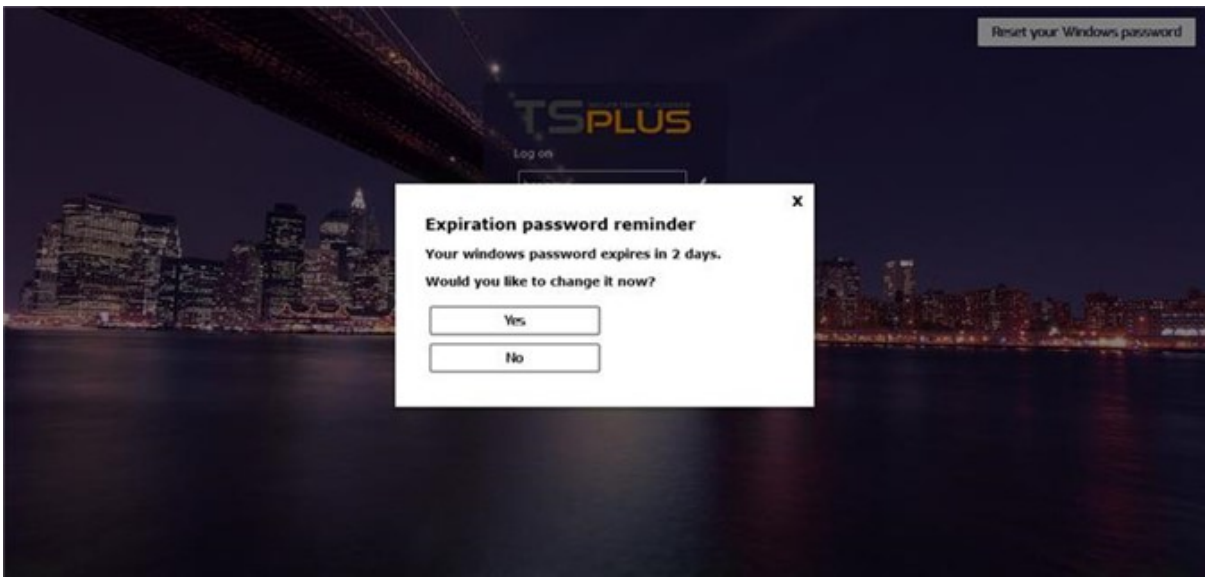


- “ **Clients disponibles** Choisissez entre 2 types de clients de connexion web. Si les deux sont cochés, l'utilisateur aura le choix. Vous pouvez changer le nom utilisé pour ces options dans votre portail web. Vous pouvez également choisir quelle option est sélectionnée par défaut si les deux options sont disponibles.
- “ **Portail de passerelle** Vérifiez-le pour activer une page avec le portail Gateway activé. Cette fonctionnalité ajoute une étape d'authentification supplémentaire lorsque vous assignez un serveur à un utilisateur ou à un groupe.
- “ **Clavier** Seulement pour les administrateurs avancés qui ont des exigences spéciales en matière de clavier.

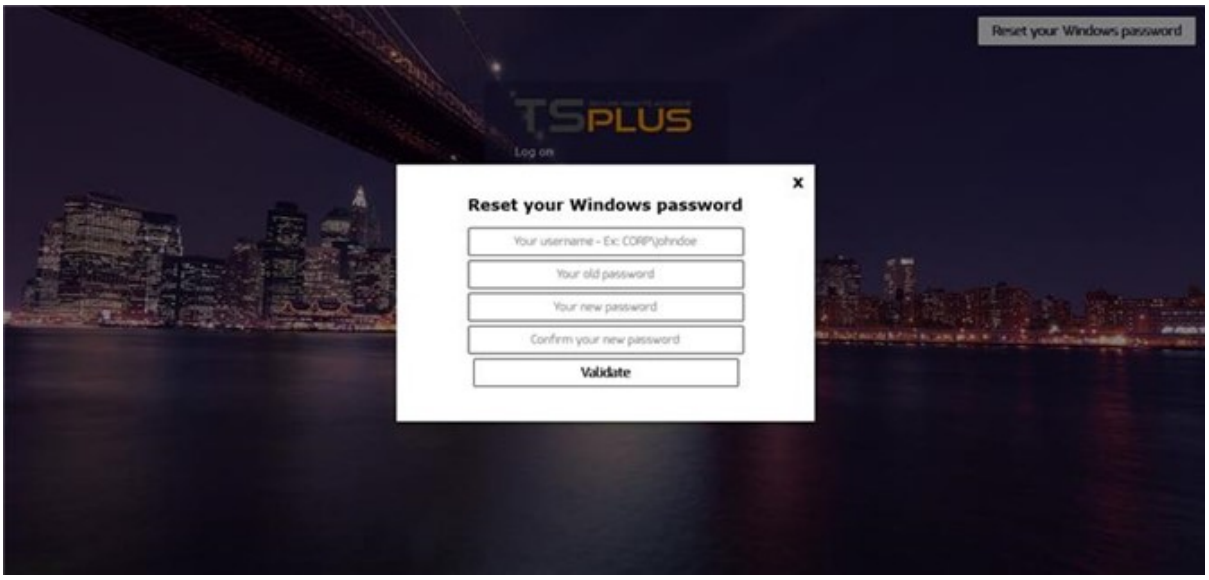
Personnalisation du portail Web - Identifiants



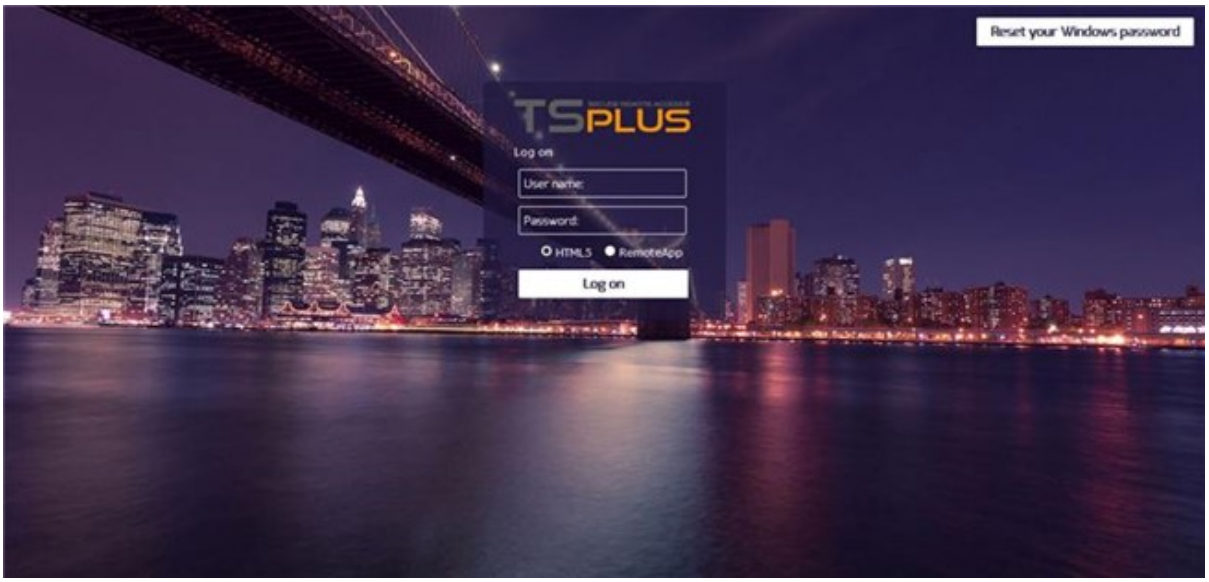
- “ **Étiquette** Vous pouvez changer le texte utilisé pour désigner le nom d'utilisateur, le mot de passe, …
- “ **Valeurs par défaut** Vous pouvez spécifier un identifiant par défaut, un mot de passe et un domaine qui rempliront automatiquement les champs de connexion. Tous les paramètres présents ici sont enregistrés dans le fichier index.html, qui peut être copié et renommé selon votre préférence.
- “ **Afficher le champ de domaine** Lorsque cette option est cochée, le champ Domaine est inclus dans la demande d'informations de connexion.
- “ **Mot de passe** Vous pouvez ajouter un message d'alerte s'affichant pendant la connexion via le portail web, pour informer l'utilisateur de la date d'expiration de son mot de passe. Par exemple, le pop-up suivant s'affichera si le mot de passe Windows de l'utilisateur expire dans moins de 3 jours :



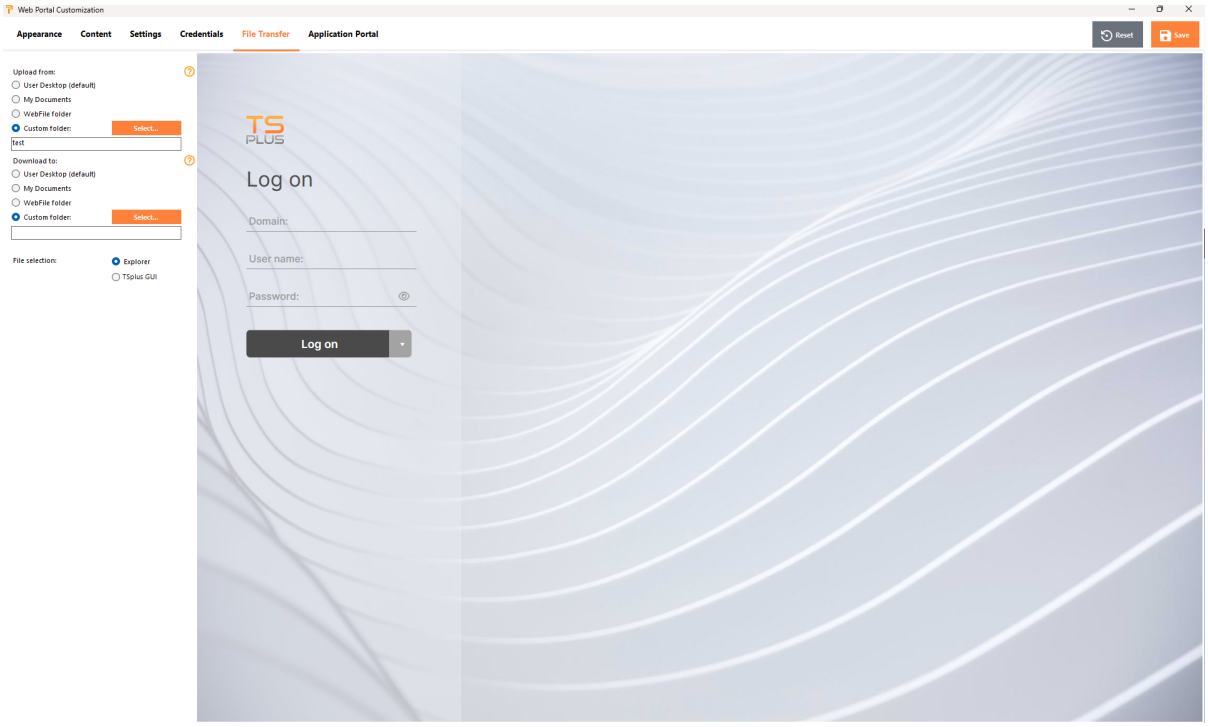
Comme mentionné, cela lui donne la possibilité de le changer directement depuis le portail Web en utilisant le pop-up affiché juste en dessous :



Vous pouvez également permettre à l'utilisateur de changer ses fenêtres à tout moment en cochant l'option « Afficher le bouton de réinitialisation du mot de passe des fenêtres ».

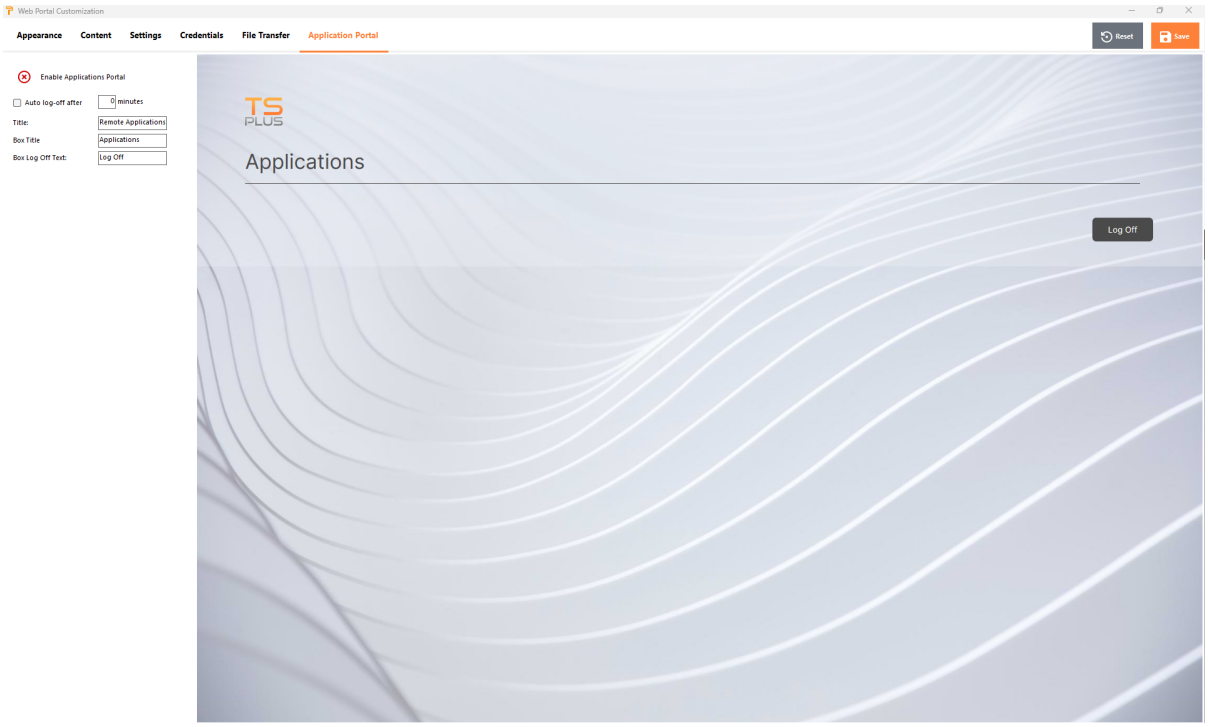


Personnalisation du portail Web - Transfert de fichiers



- “ **Télécharger - Télécharger** : choisissez les chemins source et destination pour les téléchargements et les envois de fichiers.

Personnalisation du portail Web - Panneau d'application



Plus d'informations sur le portail d'application peuvent être trouvées ici .

Sauvegarde des valeurs saisies et réinitialisation aux valeurs par défaut

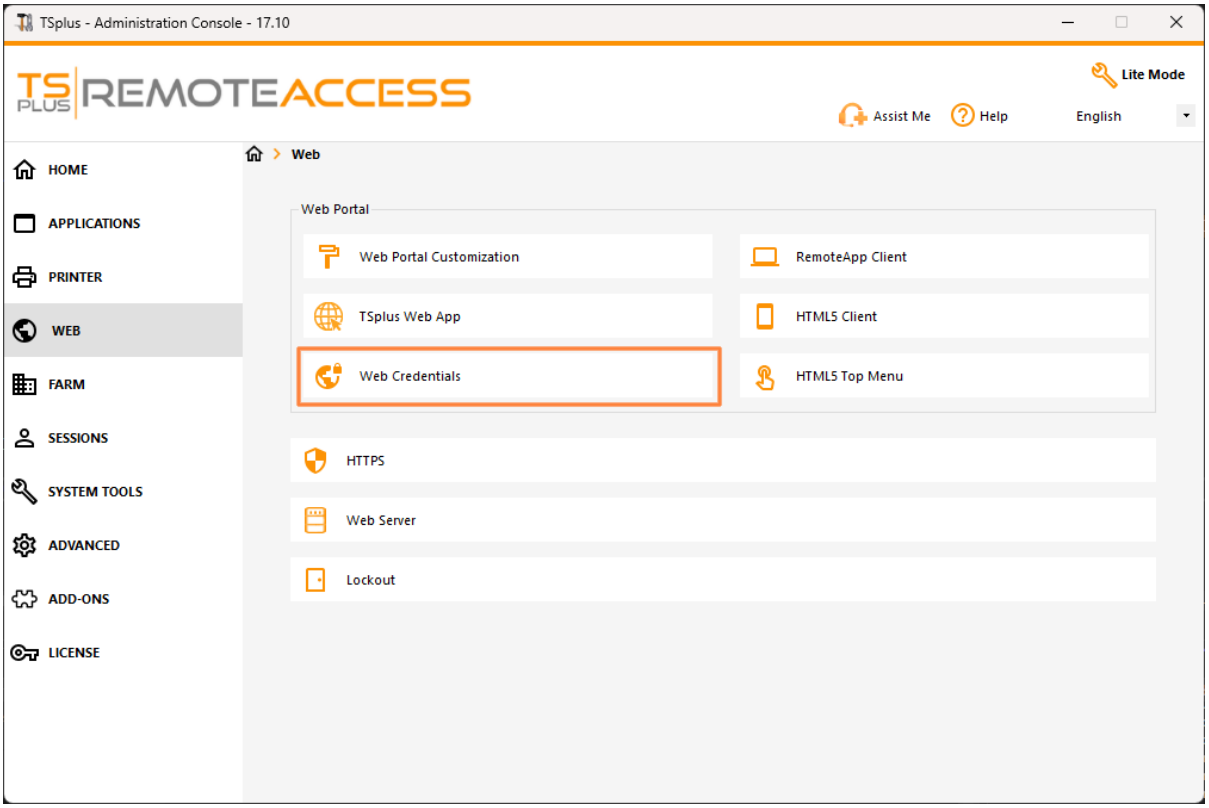
N'oubliez pas de cliquer sur le bouton "Enregistrer" pour sauvegarder toutes vos modifications.

Si vous souhaitez réinitialiser ces valeurs aux valeurs d'origine, cliquez sur le bouton « Réinitialiser ».

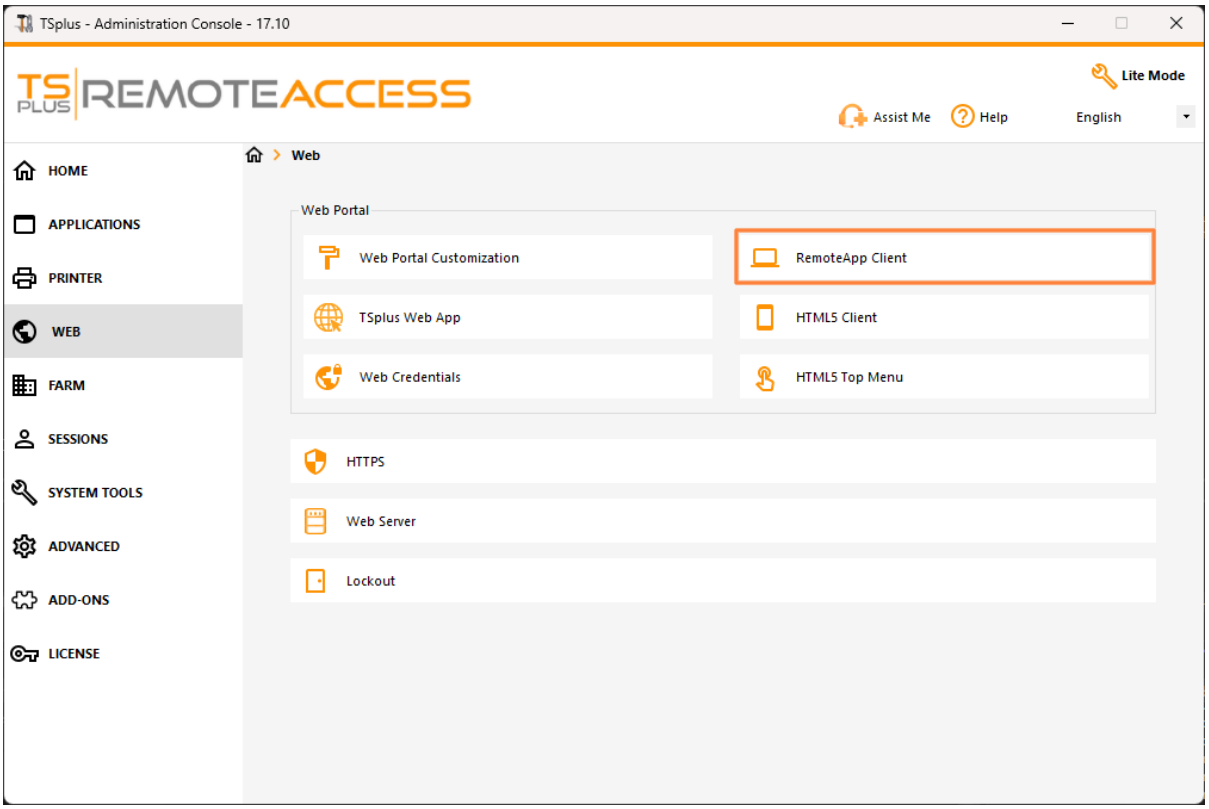
Identifiants Web

La section « Informations d'identification Web » vous permet d'activer (ou de désactiver) le Identifiants Web fonctionnalité.

Lorsque vous utilisez des identifiants Web, vous voudrez peut-être autoriser les mots de passe vides. Si vous n'avez que des identifiants Web avec des mots de passe vides, nous vous recommandons de décocher l'option « Afficher le champ de mot de passe » afin de simplifier encore plus la page de connexion web.

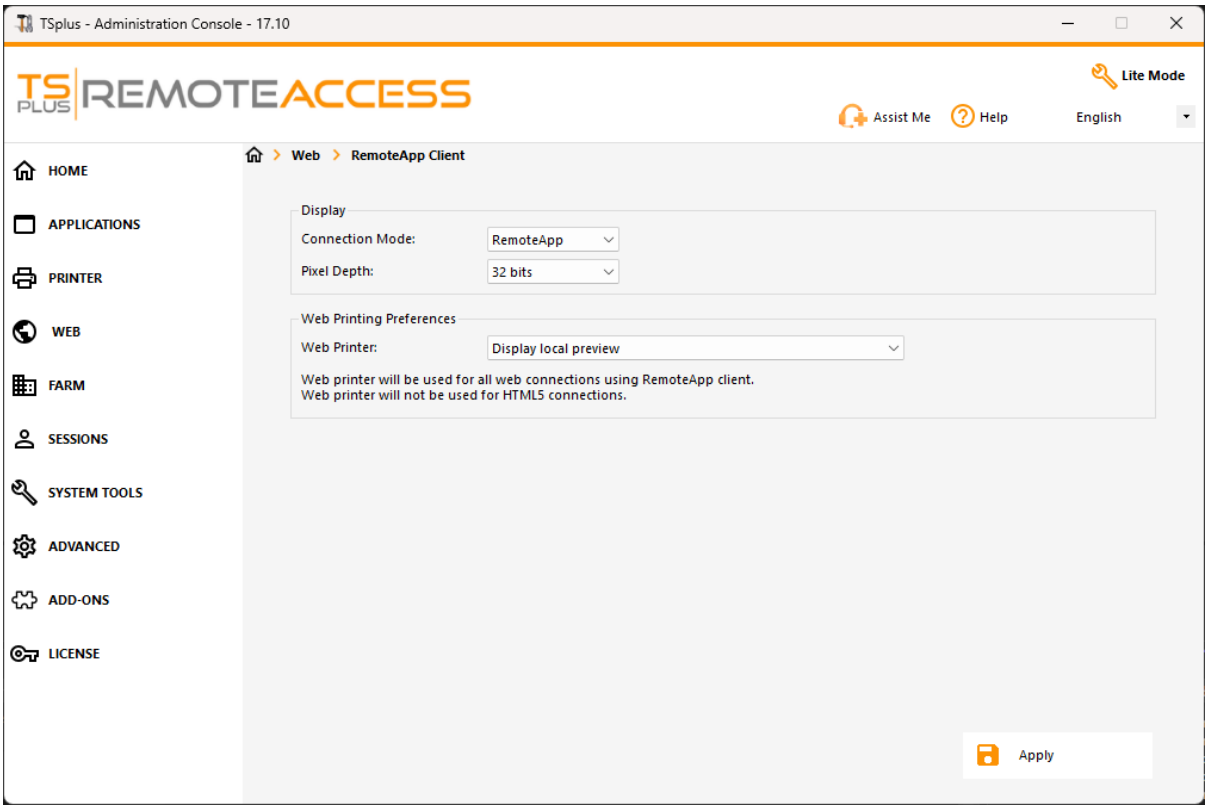


Tuile d'application distante

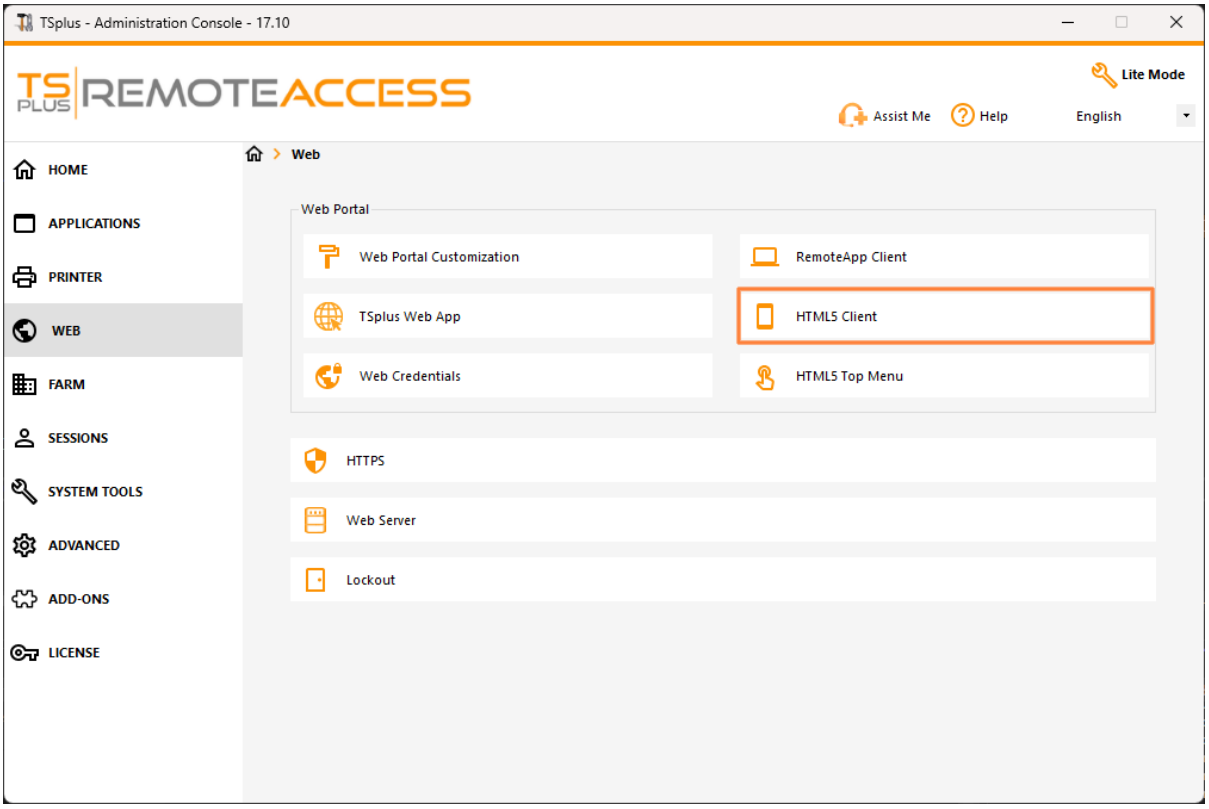


Ce panneau est destiné aux paramètres spécifiques des clients Windows.

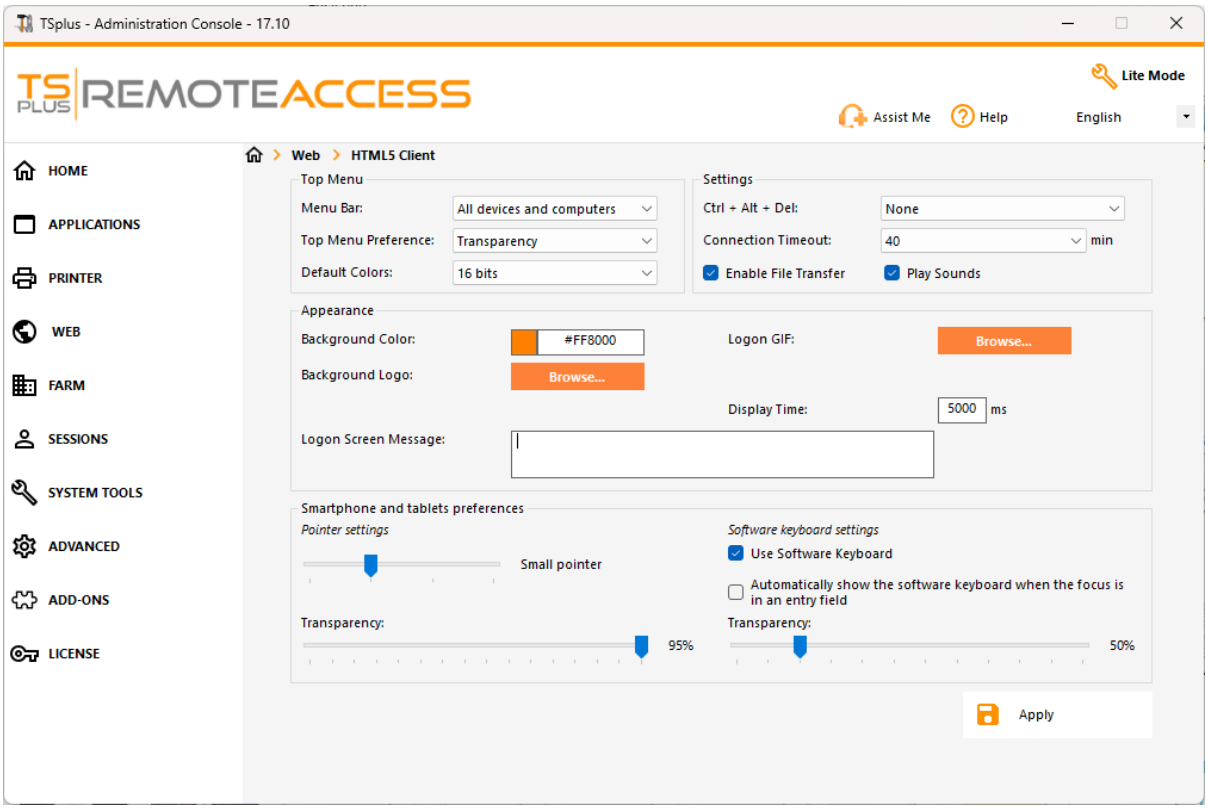
Vous pouvez choisir votre affichage entre RemoteApp (connexion à distance sans le bureau à distance) ou RDP standard. Vous pouvez également décider si vous souhaitez que les documents soient imprimés sur l'imprimante par défaut de l'utilisateur, afficher un aperçu local ou le choix de l'imprimante locale.



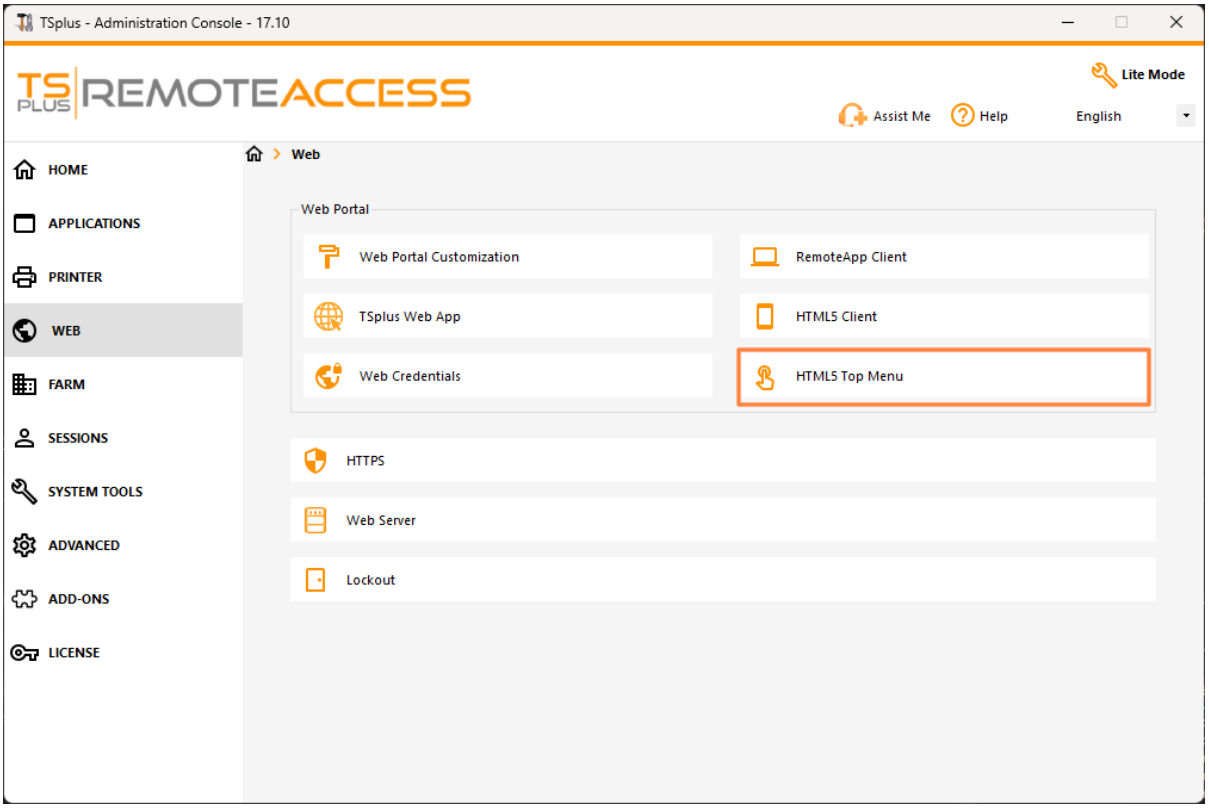
client HTML5



Sur ce carrelage, vous pouvez modifier les paramètres d'affichage web du client HTML5. Plus d'informations sur cette page .



Menu supérieur HTML5



Ce panneau vous permet de choisir les applications à afficher au niveau 1 ou 2 dans le menu supérieur de votre session web distante générée. Vous pouvez également modifier ces

applications afin qu'elles apparaissent sur un type de client spécifique : pc, mobile, ios… ou sur tous.

