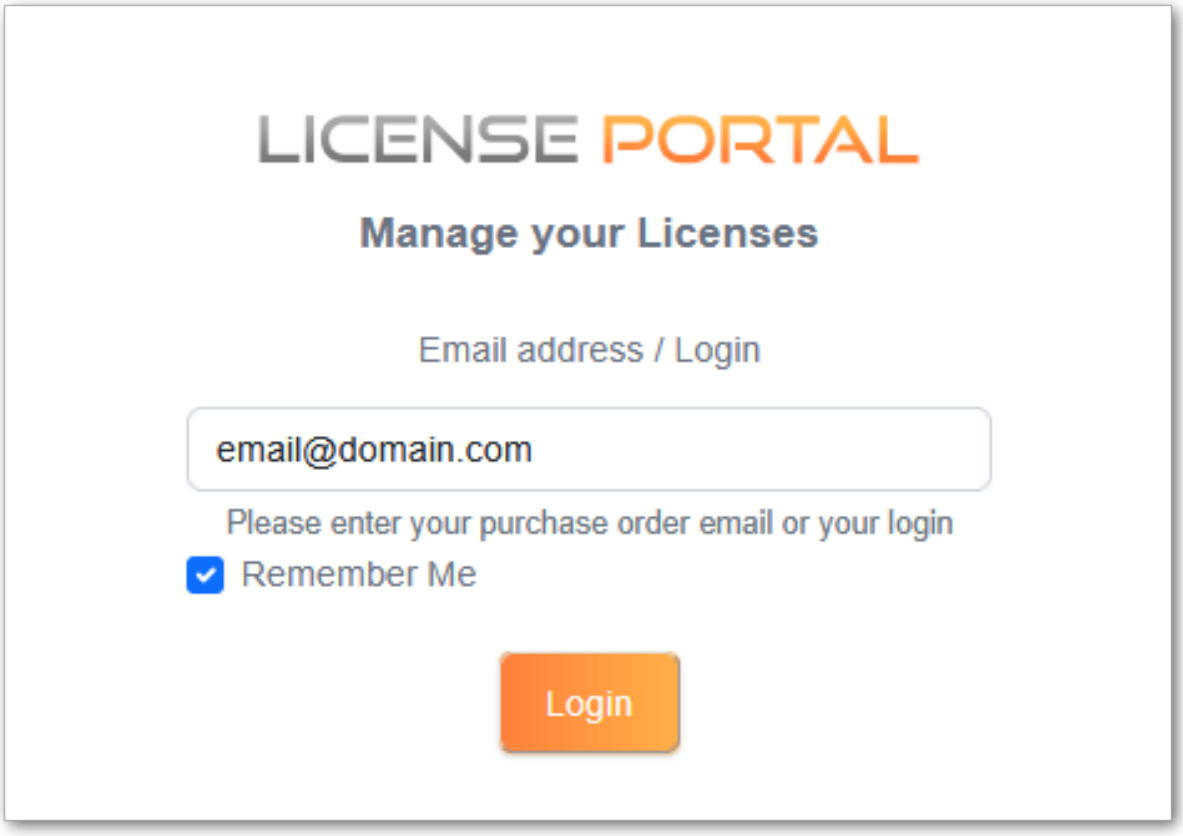
Activating Your TSplus Permanent License (Offline)

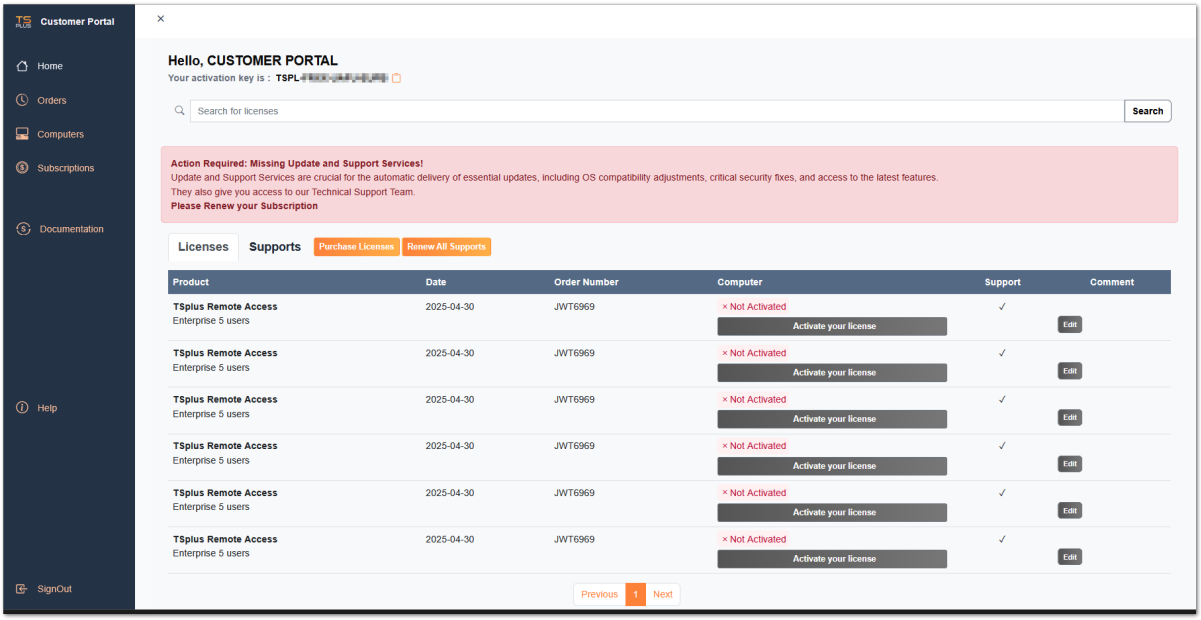
Retrieve your Activation Key

When you order a license, connect to our Licensing Portal and enter your Email Address and your Order Number.

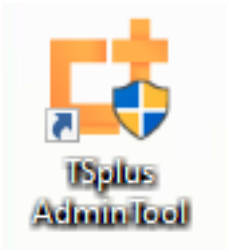


Download the Customer Portal User Guide for more information about how to use it.

Your activation key will be displayed at the top of the dashboard:



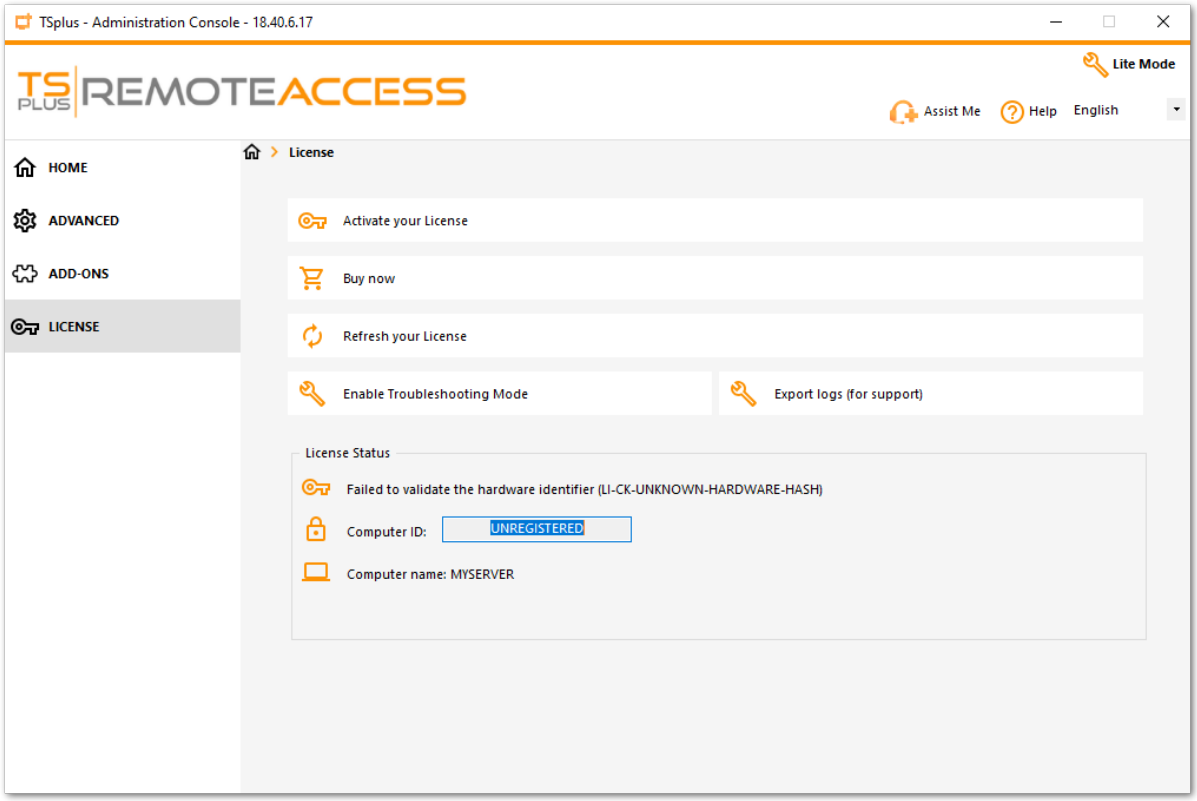
Locate the Administrator Tool on your desktop



If you cannot find the admin tool shortcut, it should be located in the desktop folder on the administrator account used to download TSplus. You can also find the TSplus folder on this path: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Double-click on it, then click on the license tab.

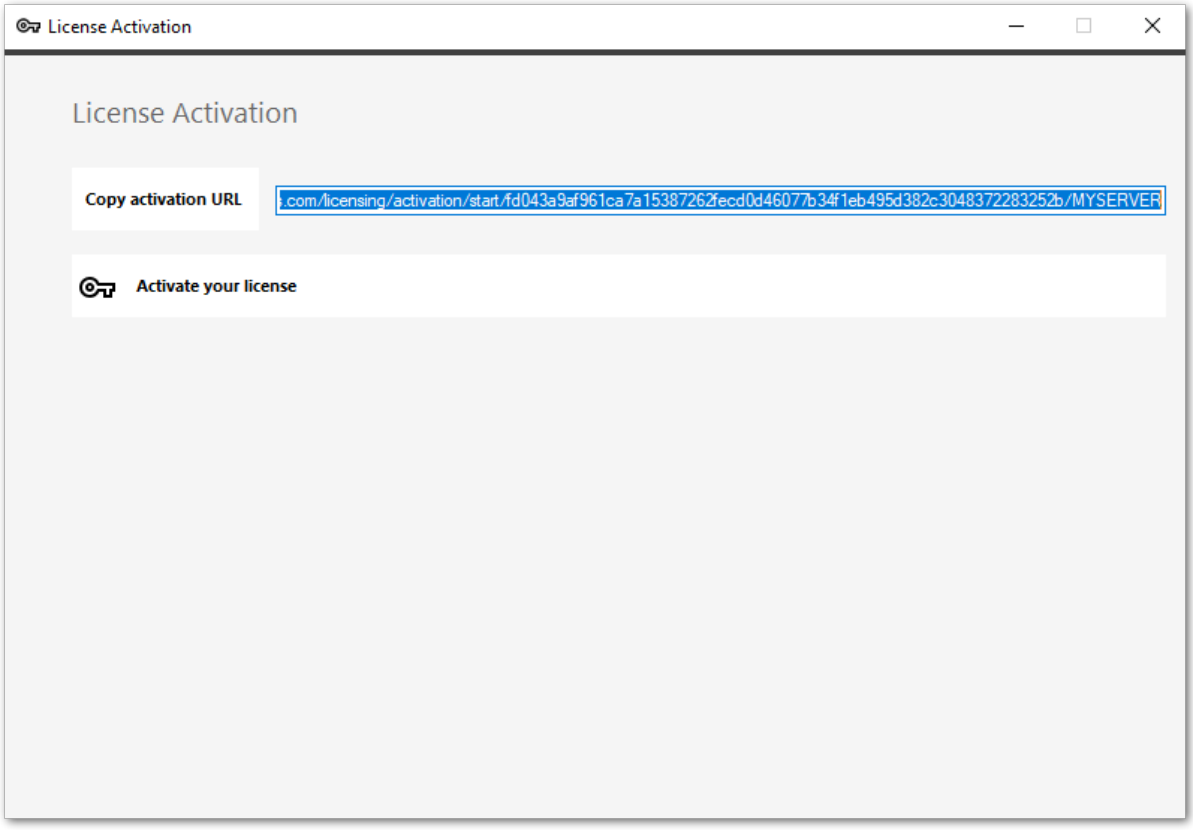
Here you can see the status of your TSplus license, as well as your Computer ID and Computer Name “UNREGISTERED”



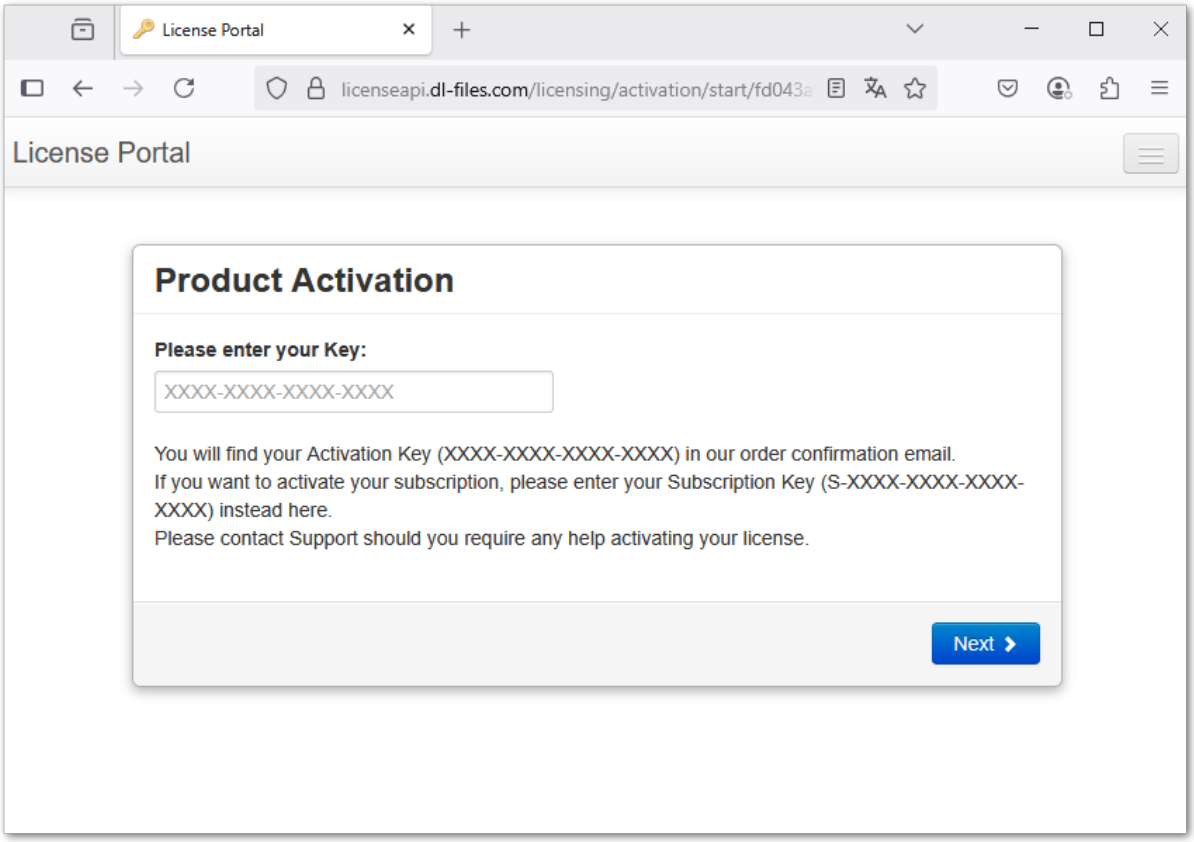
Activate your licenses on an offline TSplus server

Click on the “Activate your License” button. A popup appears and displays a quite long URL address.

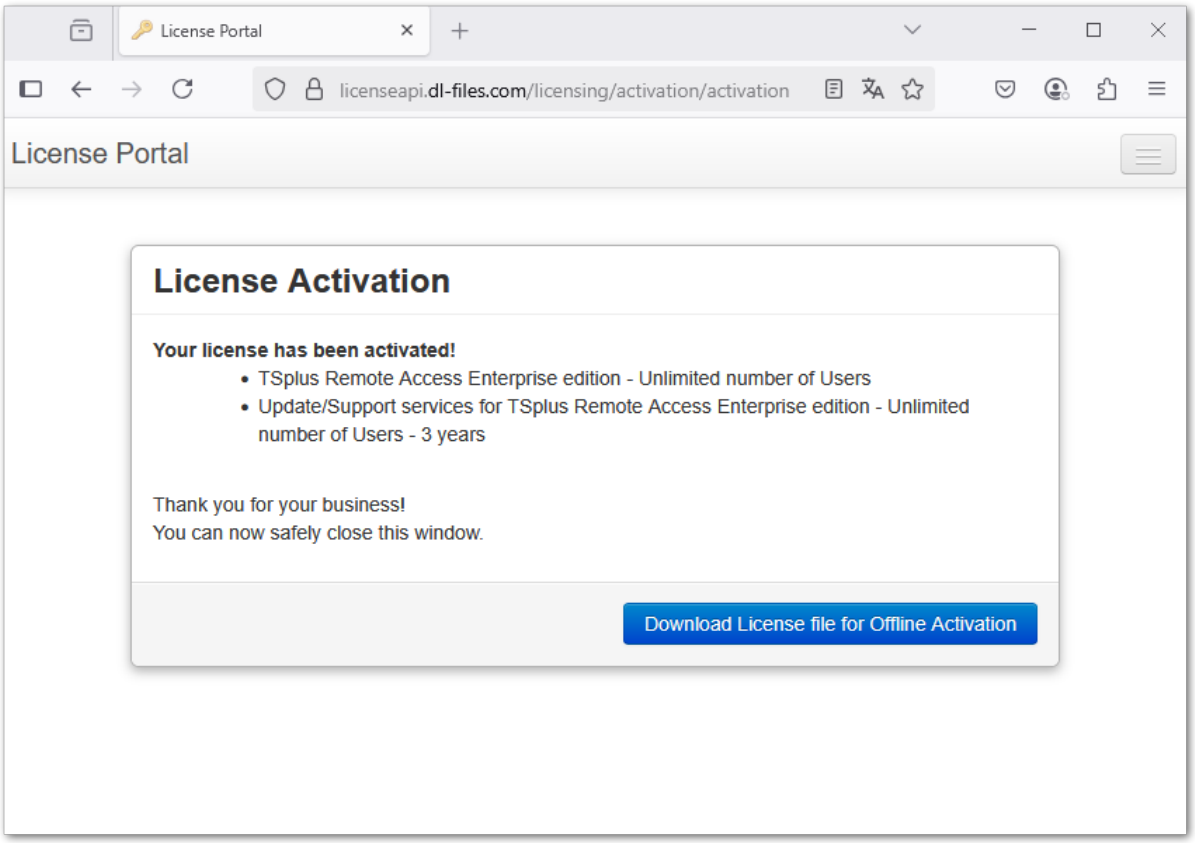
Copy this URL on an internet-connected computer browser and access it in order to retrieve a license file:



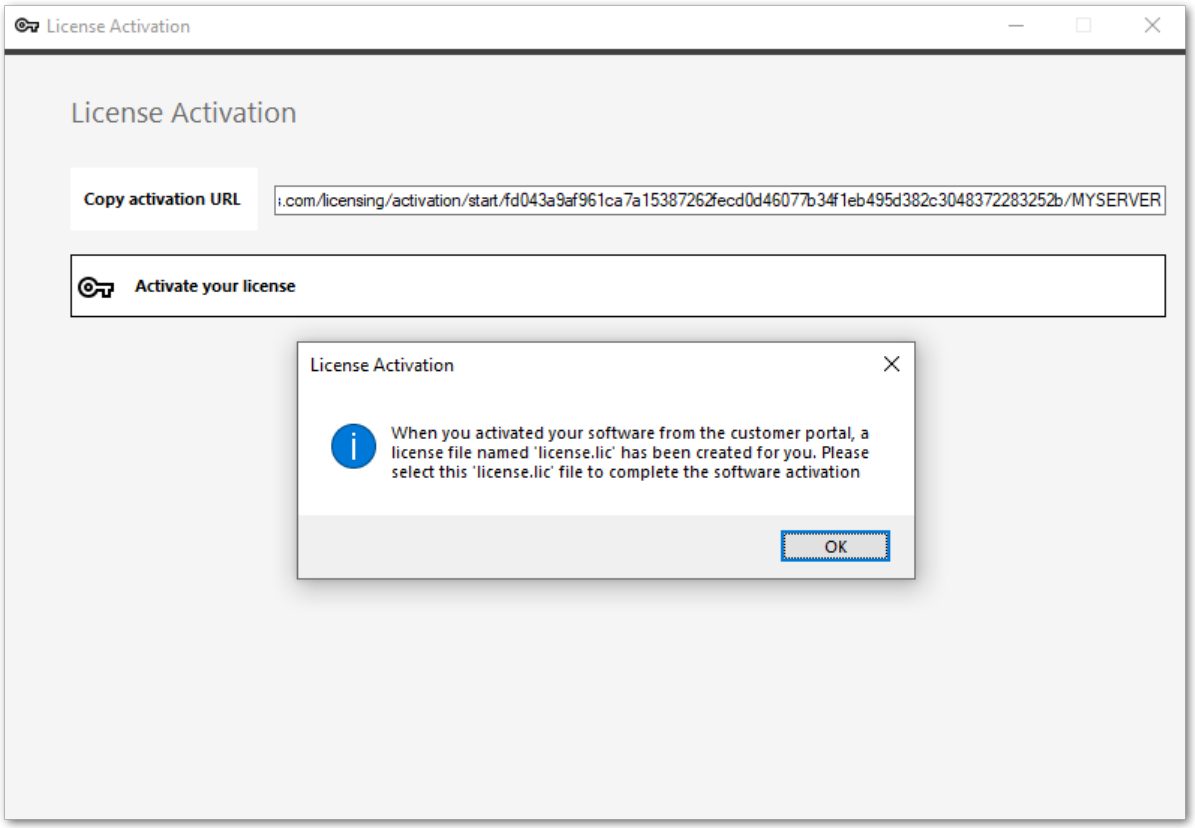
Enter your Activation Key:

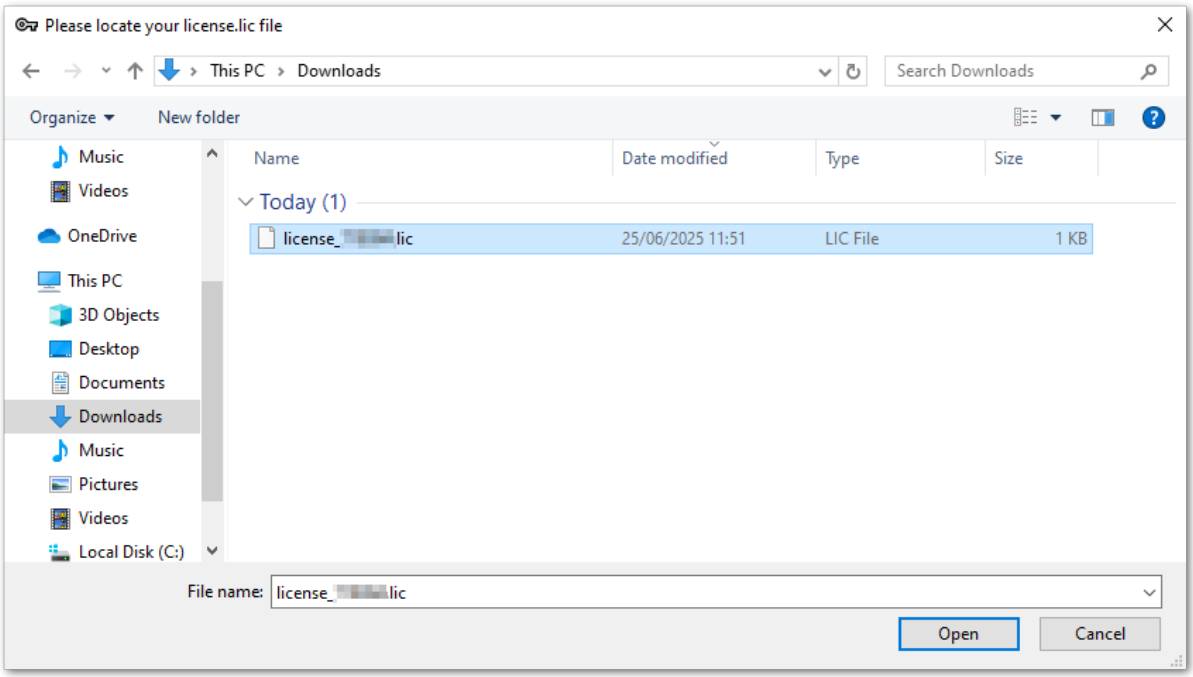


Your license is then validated. Download the license file by clicking on the corresponding button:

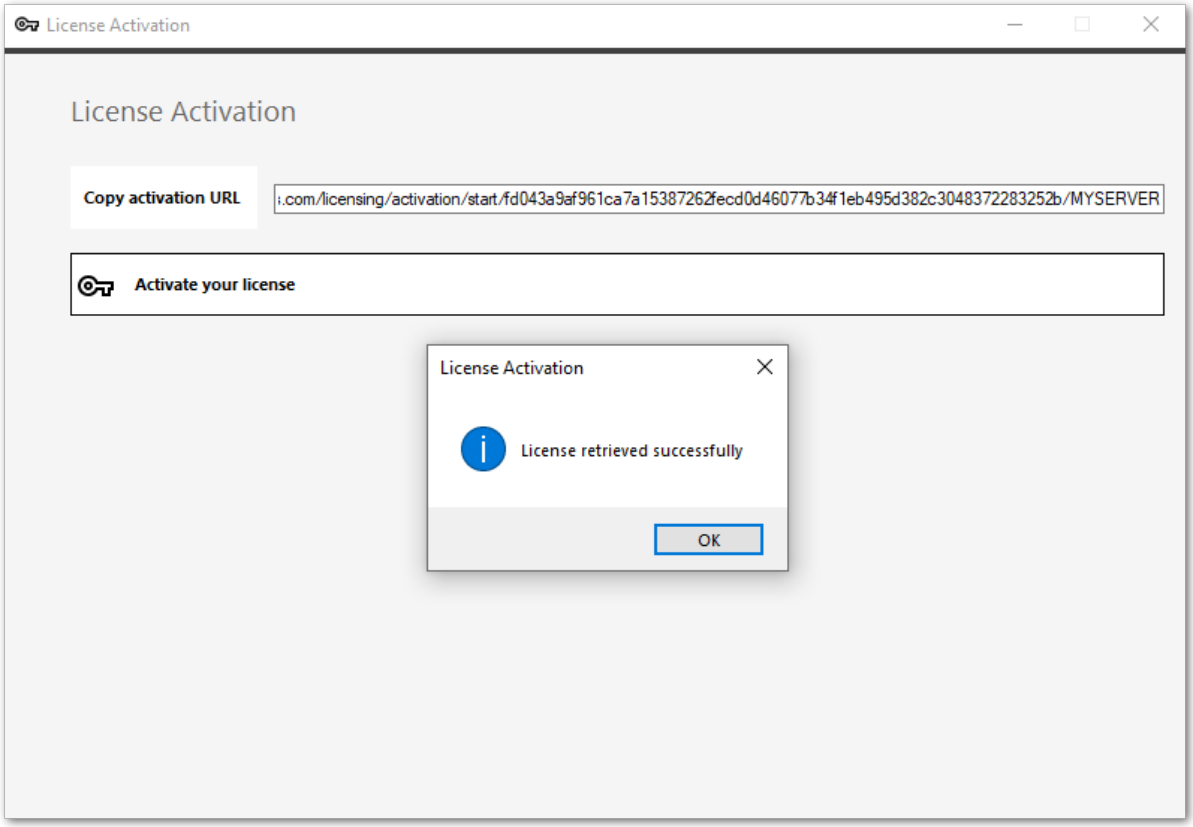


This license file must then be copied back to the server in order to finish the offline activation process:





A message will confirm that your license was retrieved succesfully :

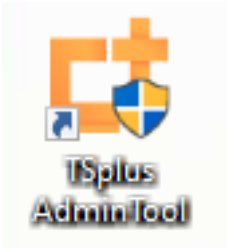


You will then have to select the corresponding licenses / support to activate and a message confirming that all your products/support are now activated.

N.B: You can still download license.lic files on the Licensing Portal for TSplus Legacy Versions. Download the Customer Portal User Guide.

Activating Your TSplus License (Online) Permanent or Subscription.

Locate the Administrator Tool on your desktop :

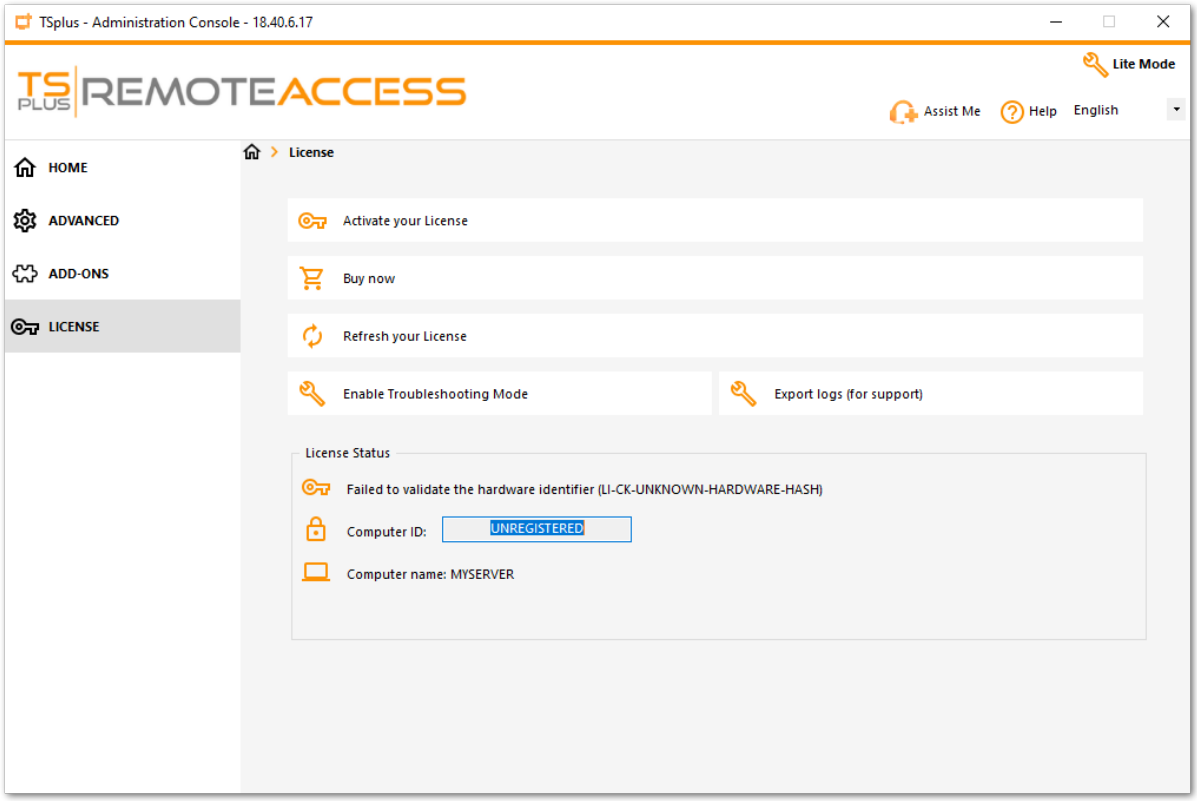


- If you cannot find the admin tool shortcut, it should be located in the desktop folder on the administrator account used to download TSplus. You can also find the TSplus folder on this path: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Double-click on it, then click on the license tab.

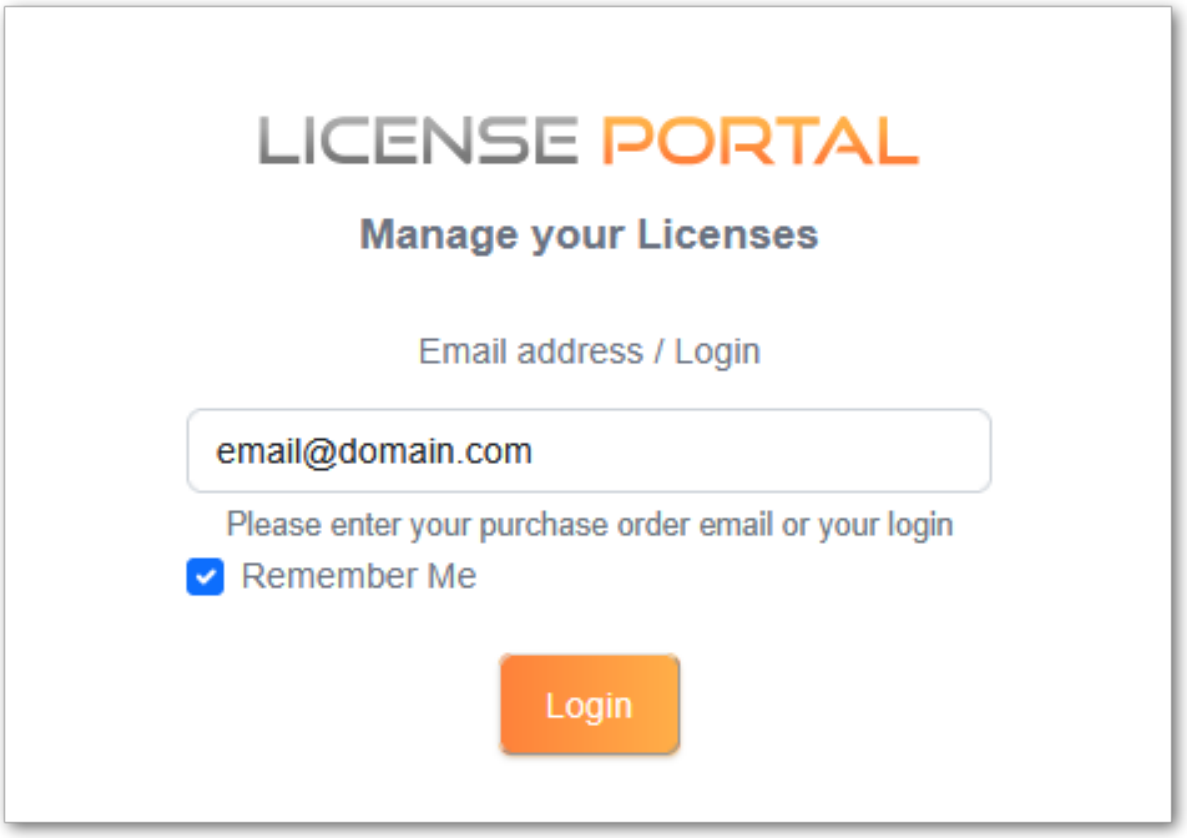
Here you can see the status of your TSplus license, as well as your Computer ID and Computer Name :

if it displays “UNREGISTERED” it means that your server is not connected to the internet and you need to check your server’s web access before continuing.



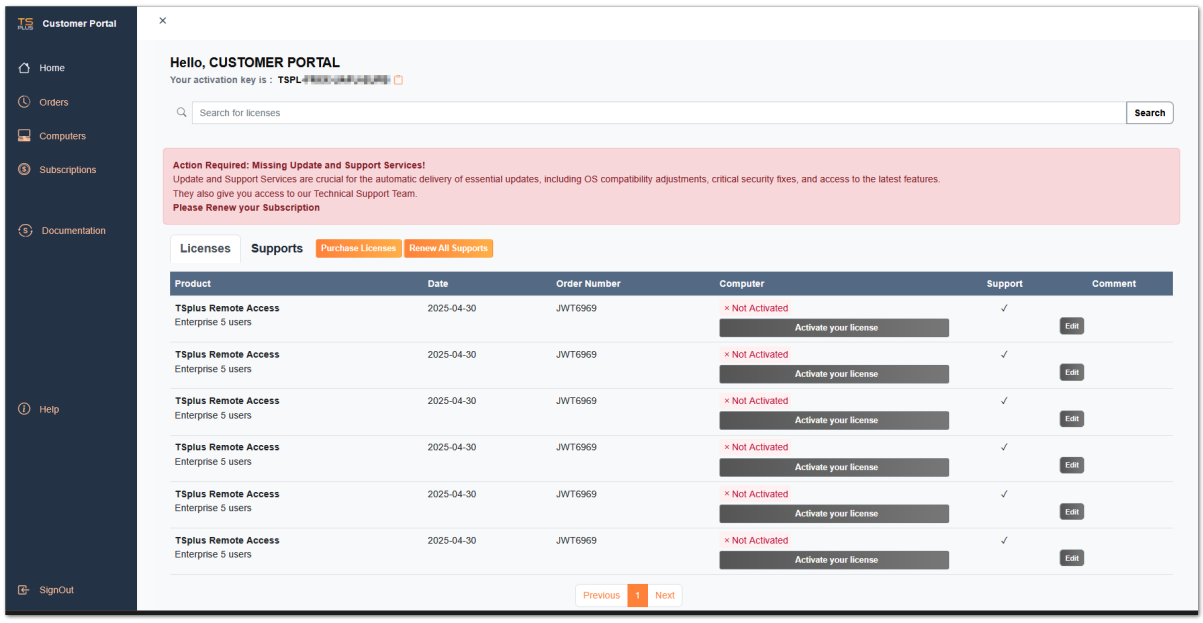
Activate your licenses on an online TSplus server

When you order a license, connect to our Licensing Portal and enter your Email Address and your Order Number:



Download the Customer Portal User Guide for more information about how to use it.

Your activation key will be displayed at the top of the dashboard:

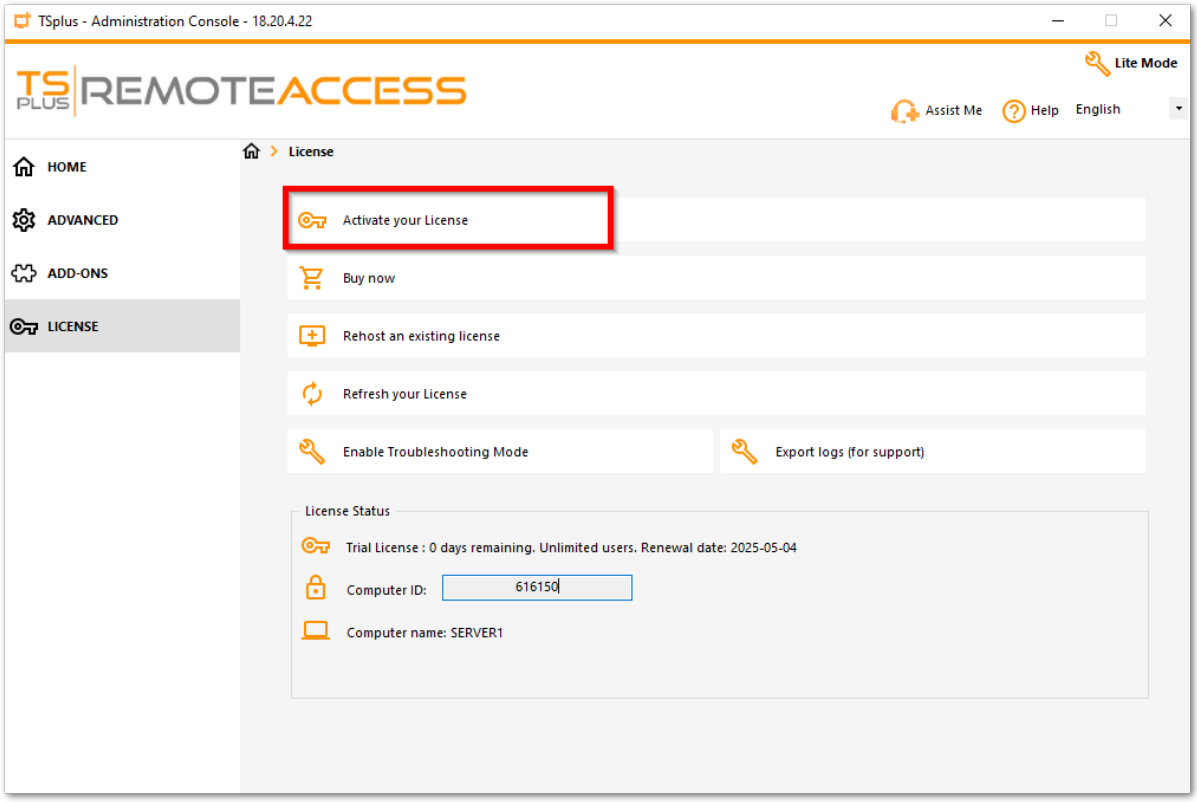


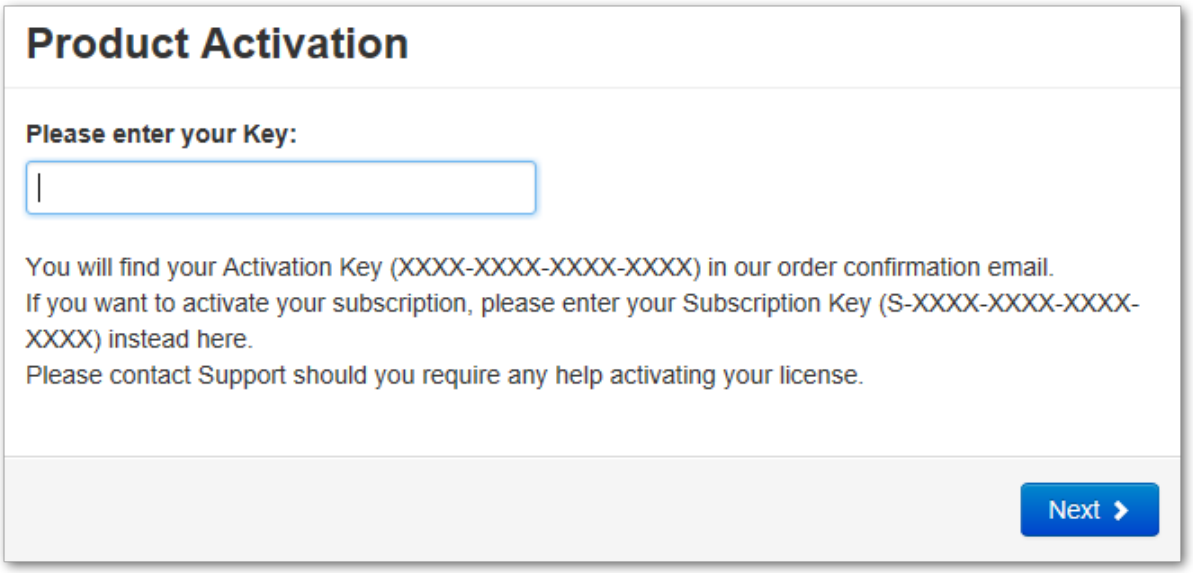
You can then go to the License Tile of the AdminTool, click on the “Activate your License” button, enter this activation key and click on “Next” .

You will find your permanent activation key **(XXXX-XXXX-XXXX-XXXX)** in our order confirmation email.

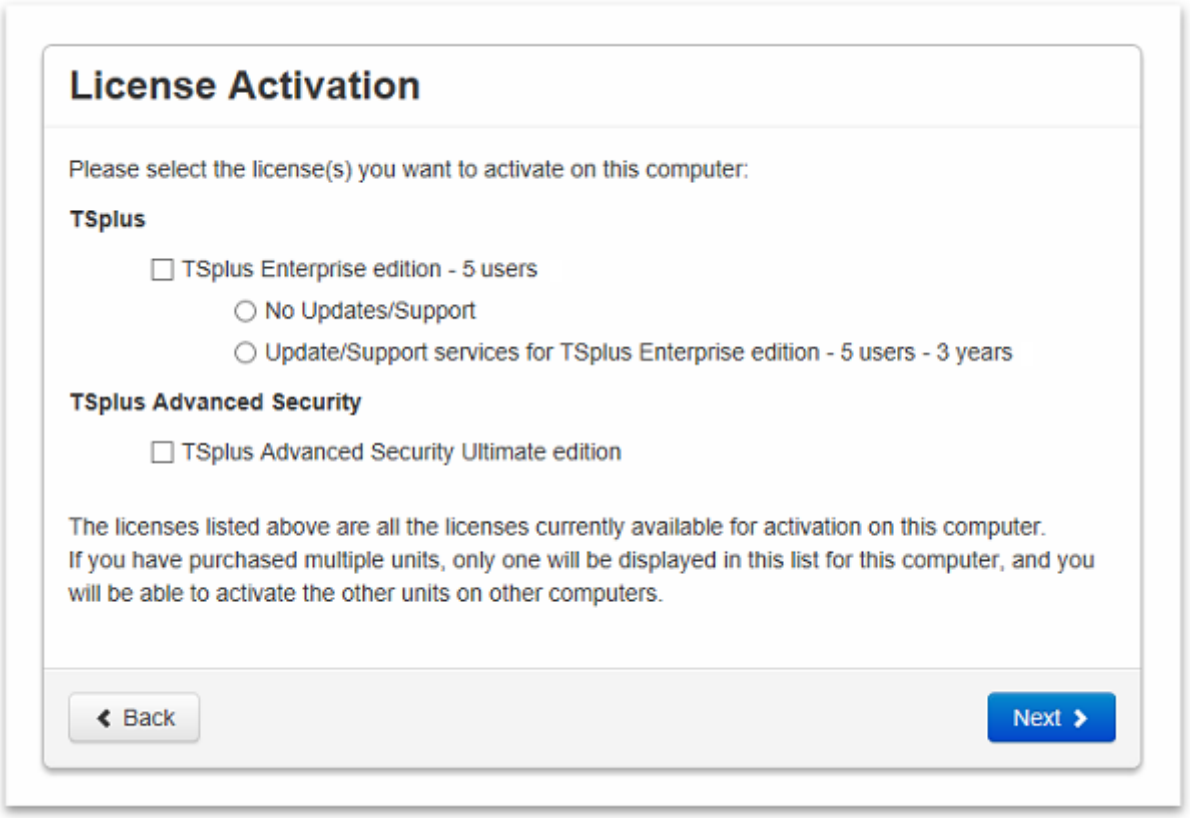
If you wish to activate your subscription, please enter your subscription key **(S-XXXX-XXXX-**

XXXX-XXXX).

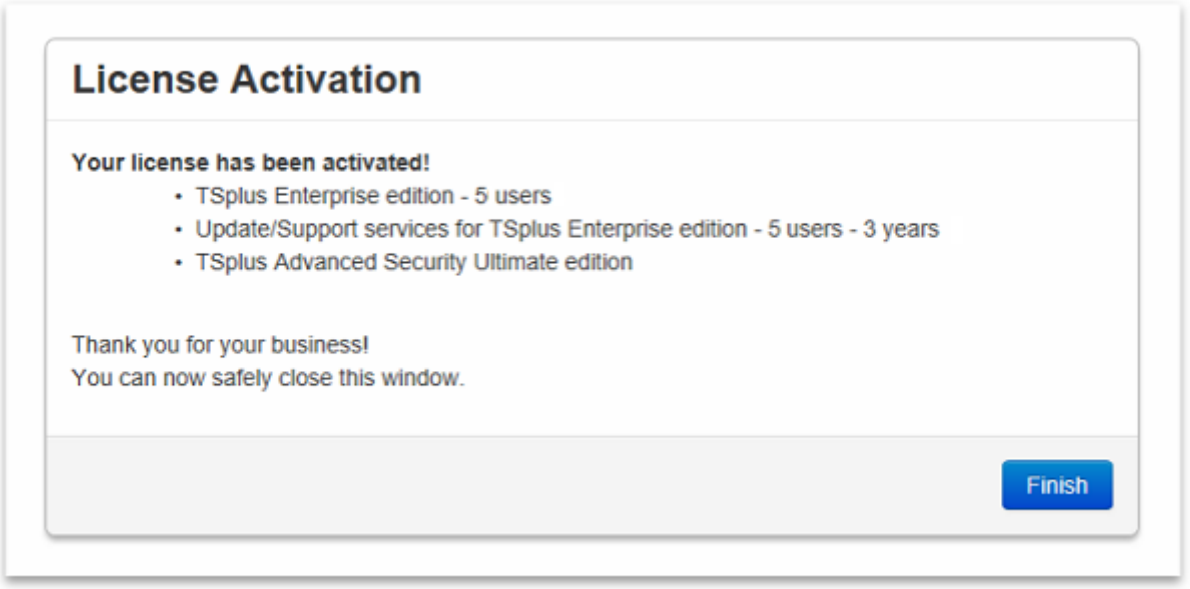




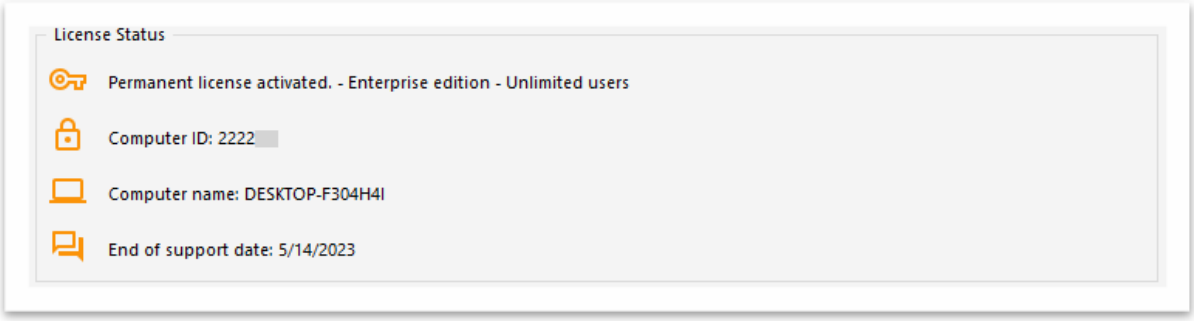
You will get a list of all the available licenses/supports assigned to this activation key, i.e. all licenses/supports not activated yet:

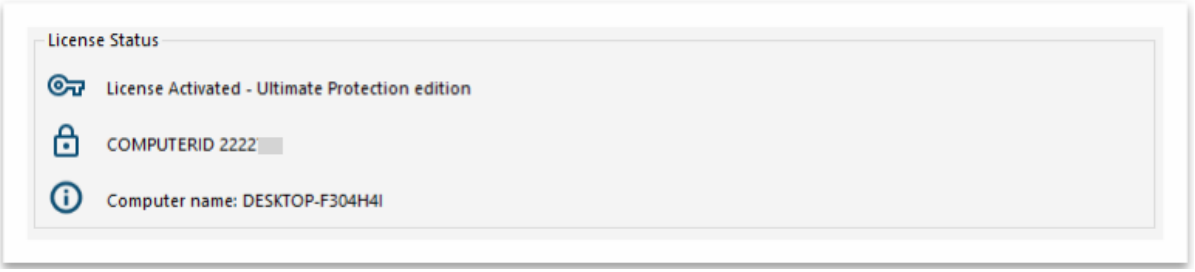


Check one or more items and click on the “Next” button. Please note that you can activate several products at the same time by checking several products/support!



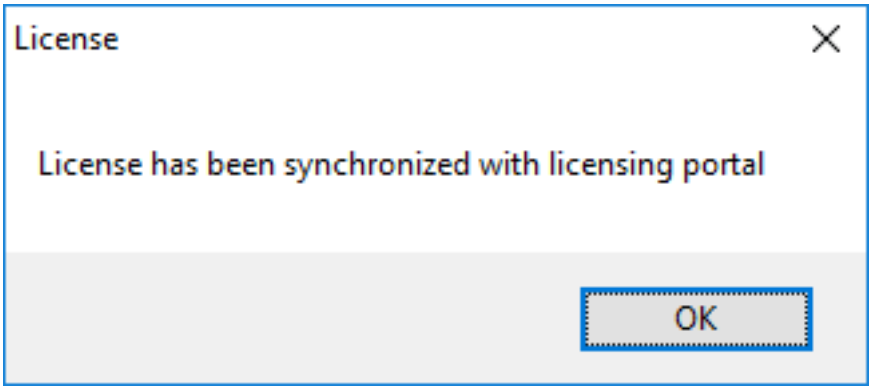
All your products/support are now activated (in this example, both TSplus with support and TSplus Advanced Security have been activated at once).





Refresh your License Data by clicking on the corresponding button at the bottom of the page, it will synchronize information with our Licensing Portal:





N.B: You can still download license.lic files on the Licensing Portal for TSplus Legacy Versions. Download the Customer Portal User Guide.

Activation problem:

Page error or the “NEXT” button is not working. Here are some solutions.

Disable your antivirus during license activation and check your firewall and antivirus settings.

Check your browser for the OK message by clicking this link:

https://licenseapi.dl-files.com/licensing/ping

If you have a problem with an antivirus program, the procedure is to exclude the following directories: C:\Program Files (x86)\TSplus and C:\wsession

URLs to allow in your antivirus and firewall for updates: setup.dl-files.com dl-files.com secure-download-file.com

License / Telemetry: 93.88.241.55 Updates: 51.254.22.117 TSplus Compatibility Updates / Check for Updates / View Changelog: 83.166.153.206

Ports to allow: (Port 3389 for RDP from WAN, Port 80 for HTTP and 443 for HTTPS)

Check your Internet security settings
Control Panel > Internet Options > Custom Level Scripts > Active Scripts > Enable

Fatal Alert Code 40 70

If you encounter fatal alert codes 40/70 TLS in the Event Viewer during each synchronization or update attempt.

Some TLS cipher suites may be disabled. You can use freeware like **IIS Crypto 4.0** to check and enable them.

Activating your support license

The 15 version of TSplus introduced a new and easy way to handle your annual support contract.

Support subscription is available for perpetual licenses only. Subscription licenses include updates.

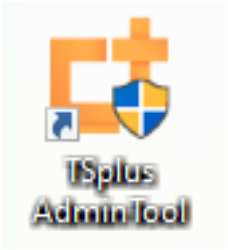
The support services include our worldwide Ticket/Email support service, Forum access, license rehosting, FAQ and tutorial support.

The Update Services include the delivery of Update codes, the right to install and to use any new release, patch and updates.

We are investing every day to enhance TSplus and to fix all known issues. So, we recommend all our customers to keep their TSplus installation updated. The annual fee is not expensive and is available on our Store Page.

Step One

Locate the Admin Tool on your desktop :



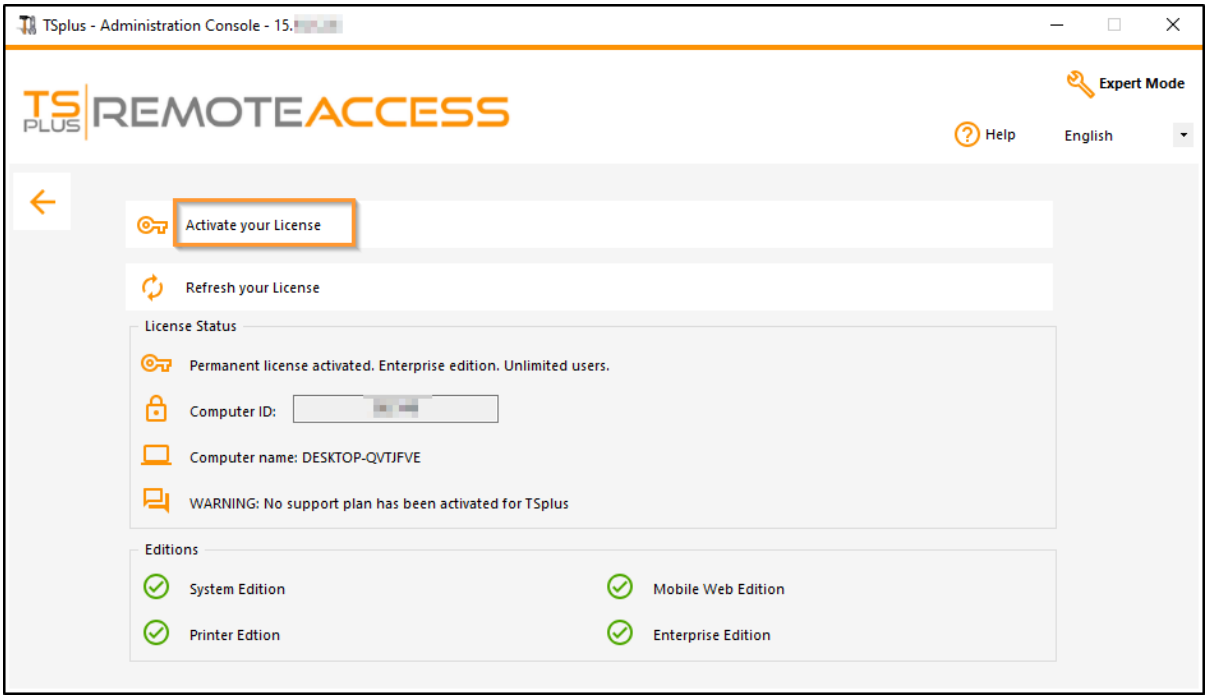
Double-click on it, then click on the license tile.

- If you cannot find the admin tool shortcut, it should be located in the desktop folder on the administrator account used to download TSplus. You can also find the TSplus folder on this path: ‘C:\Program Files (x86)\TSplus\UserDesktop\files’.

Click on the License tab You can now see the serial number:

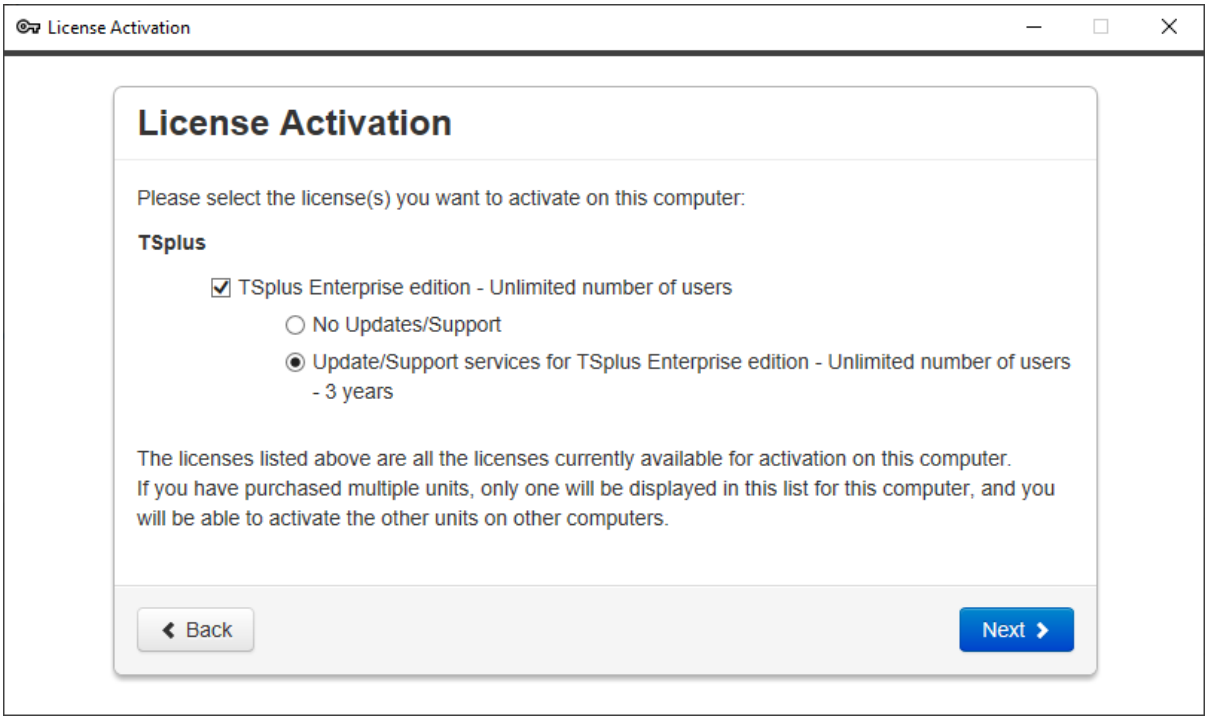
Step Two

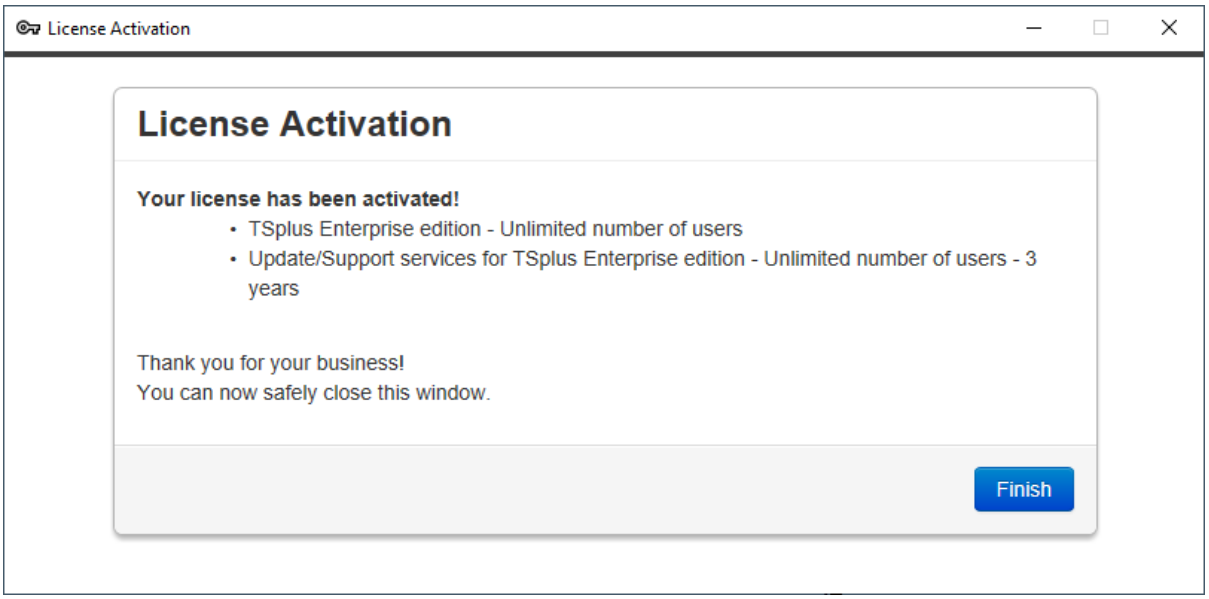
Click on the “Activate your license” tile and enter your Activation Key



Step Three

Then select “Extend Support period”:



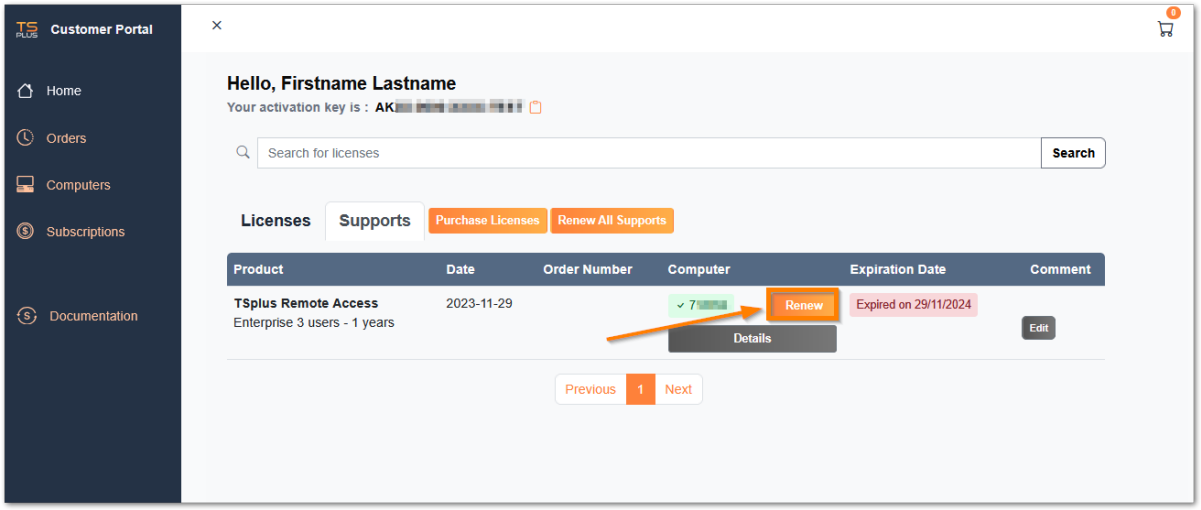


Extend an Update/Support subscription

Access your license portal: https://license.tsplus.net/login
ID: “Purchase email address”
Password: “Purchase order number of your choice”

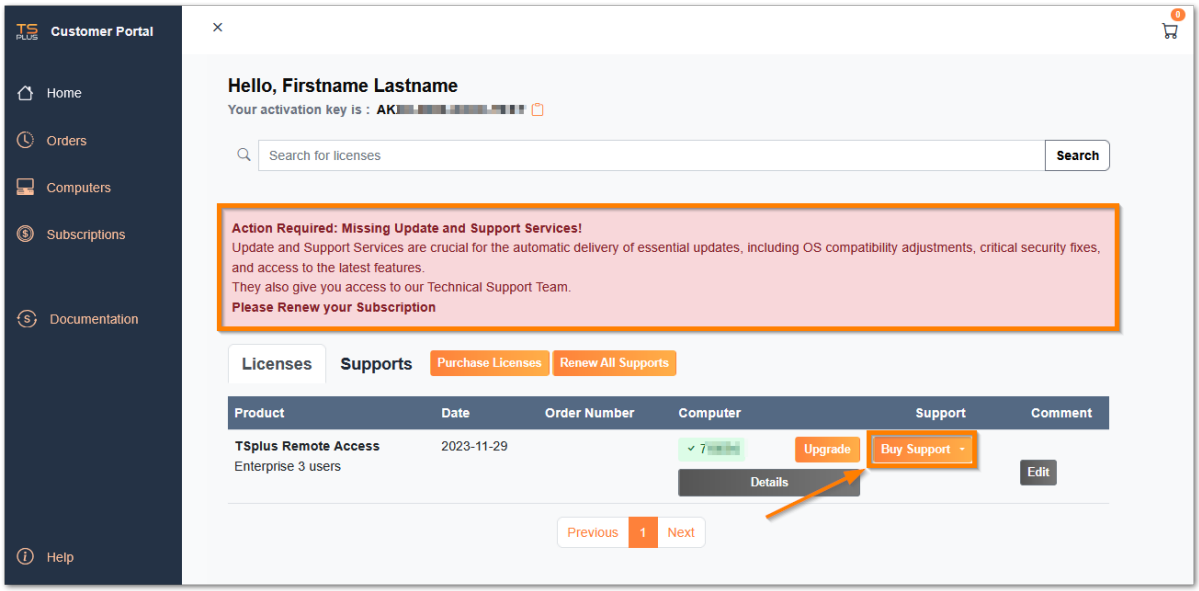
Then go to the Support tab and enter your computer ID (visible from the License tab of the AdminTool).

Then click the “Renew” button to choose the 1, 2, or 3-year support duration.



If you don’t have a support subscription for a license, A message will appear on the license tab saying
”Action Required: Missing Update and Support Services!”

You can purchase your support subscription directly by clicking the “BUY SUPPORT” button.


Customer Portal
Home
Orders
Computers
Subscriptions
Documentation
Help
Hello, Firstname Lastname
Your activation key is : AK
Search for licenses
Search
Action Required: Missing Update and Support Services!
Update and Support Services are crucial for the automatic delivery of essential updates, including OS compatibility adjustments, critical security fixes, and access to the latest features.
They also give you access to our Technical Support Team.
Please Renew your Subscription
Licenses
Supports
Purchase Licenses
Renew All Supports
Product
Date
Order Number
Computer
Support
Comment
TSplus Remote Access
Enterprise 3 users
2023-11-29
Upgrade
Buy Support
Details
Edit
Previous
1
Next

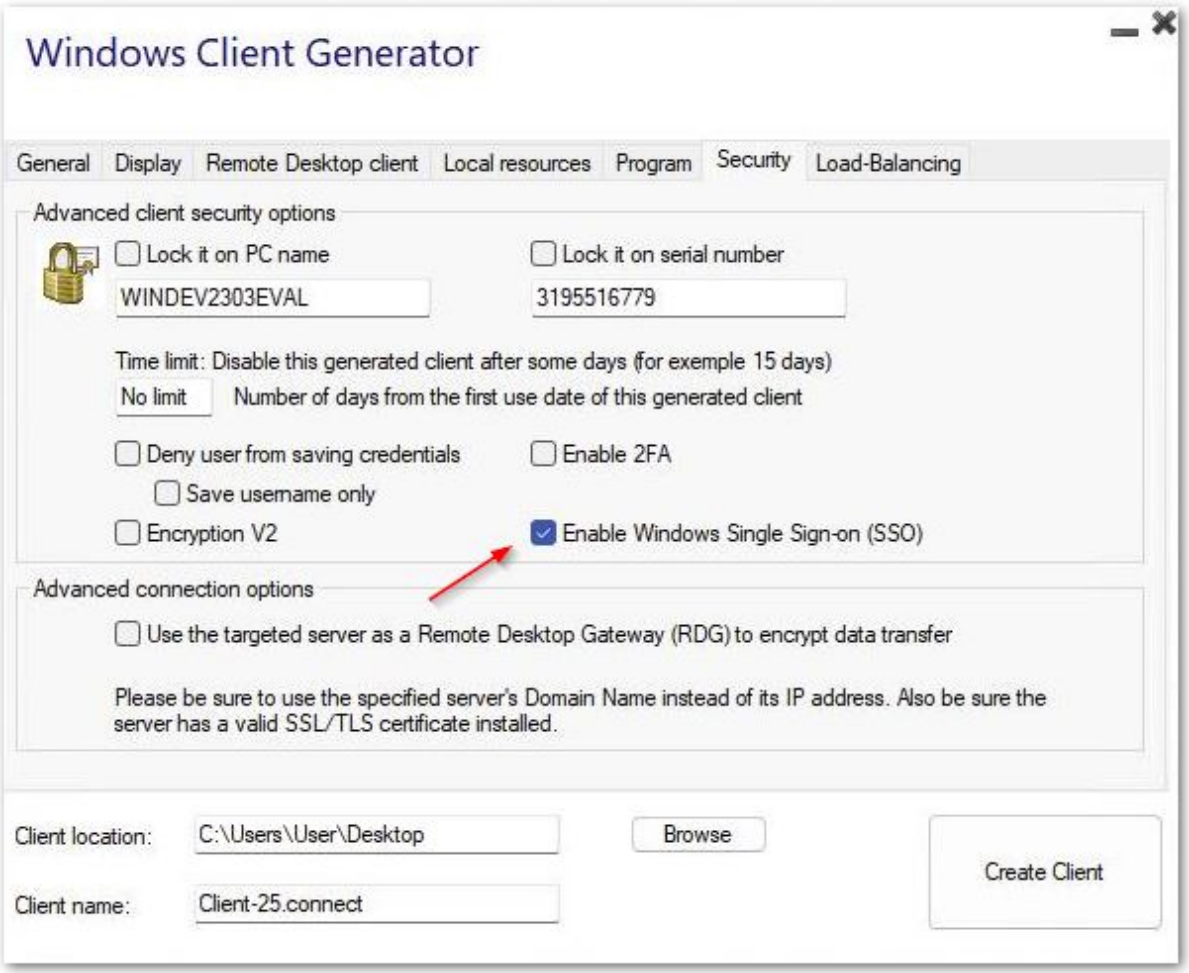
Active Directory Single Sign-On

In order to enable Windows SSO authentication for generated clients:

Update TSplus Remote Access to the latest version on a server joined to the domain.

Generate a client from the Client Generator, checking the “Enable Single Sign-On (SSO)” box in the “Security” tab.

Connect from a machine joined to the domain using the generated client.



Configuring Group Policy for Windows Single Sign-On (SSO) via Remote Desktop Client

From the domain controller:

1. Open the Group Policy Management Console.

2. Right-click on the Organizational Unit (OU) where the Group Policy Object (GPO) should be applied and select “Create a GPO in this domain, and Link it here…”.

3. Name the GPO (e.g., SSO_RDS_MY_SERVER) and click “OK”.

4. Right-click on the created policy and select “Edit”.

5. Navigate to the following location: “Computer Configuration / Policies / Administrative Templates / System / Credentials Delegation.”

6. Double-click on “Allow delegating default credentials” to open the settings.

7. Enable the setting and click “Show…”

8. In the Value field, enter the server(s) in the format TERMSRV/ server_fully_qualified_domain_name and click “OK”.

9. Click “Apply” and “OK” to close the window. From the client machine:

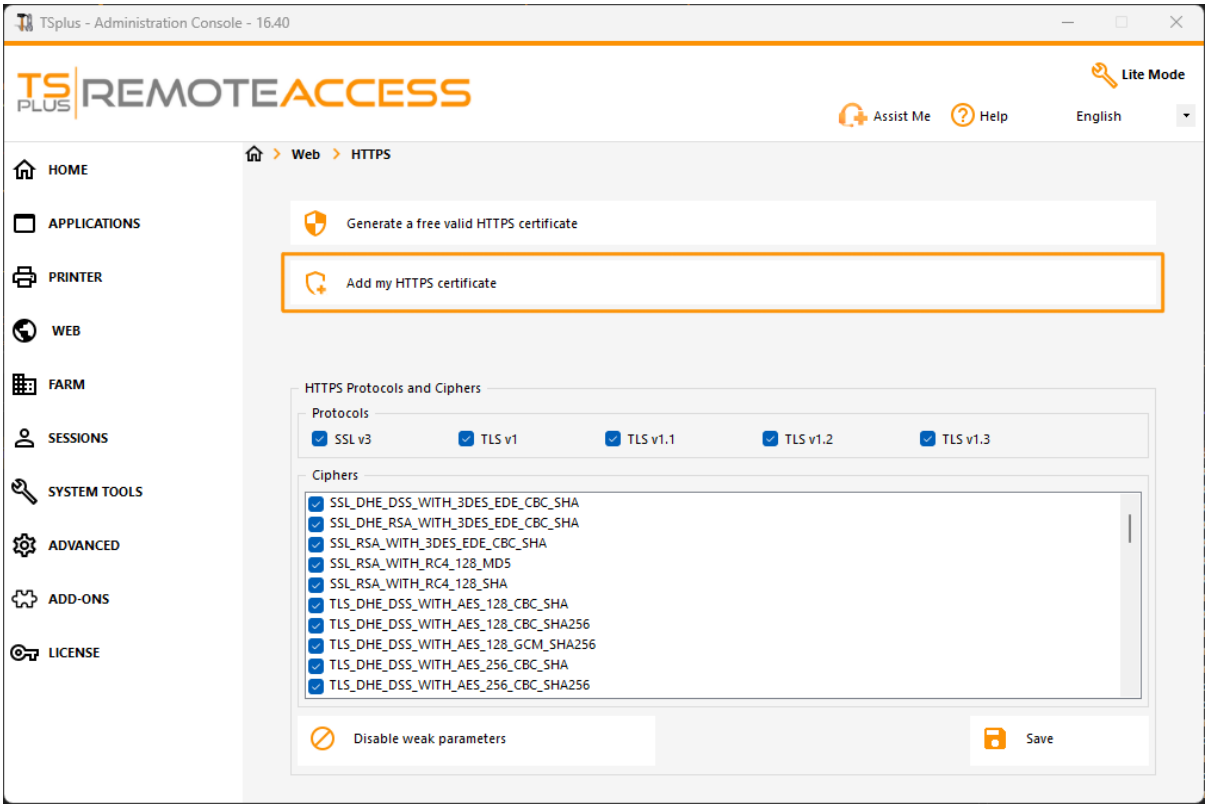
10. Update group policies by running the following command as an administrator: gpupdate / force.

HTTPS & SSL Third Party Certificates

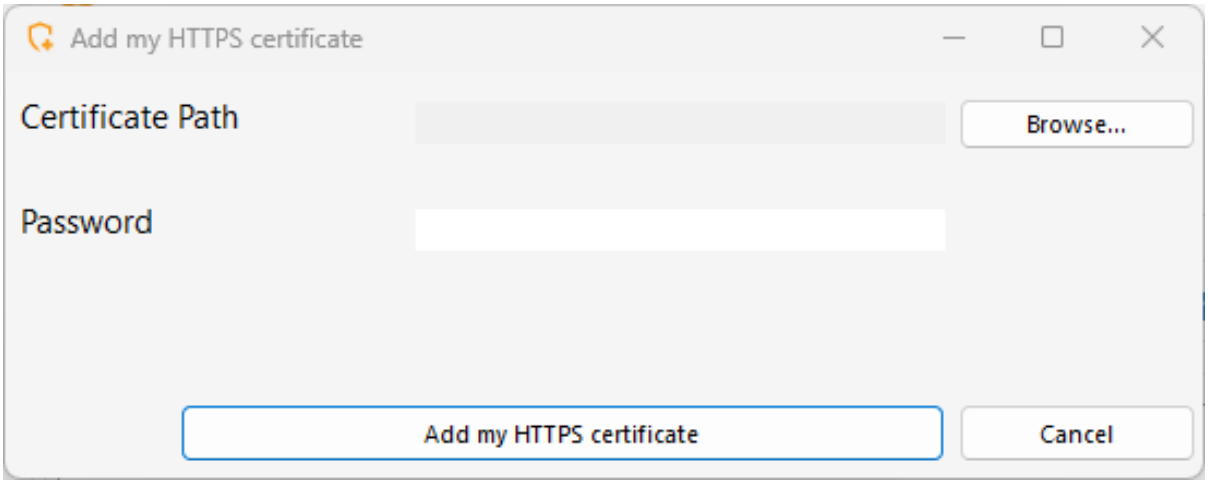
Add your own certificate

If you already have a valid HTTPS certificate you can add it to your web server.

Open TSPlus AdminTool, click on the “Web” tab, go to the “HTTPS” menu and then click on “Add my HTTPS certificate” as shown in the screenshot below:



A window will open where you can select your certificate:



Your certificate file must use the “.pfx” format.

If your certificate is protected by a password, you can enter it in the corresponding field.

Click on the “Add my certificate” button to add your certificate.

Please note that you will need to renew your certificate manually.

Additional links

Trusted SSL Certificate vendors:

- GoDaddy
- DigiCert

You can convert your .pem in pfx format with Tools or online sites. For example, on this site: https://www.sslshopper.com/ssl-converter.html

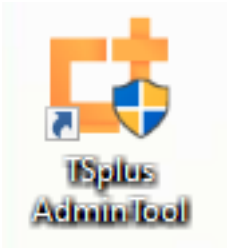
You can use this SSL Server Test tool in order to validate the good quality of a web portal in HTTPS.

TSplus Administration Tool overview

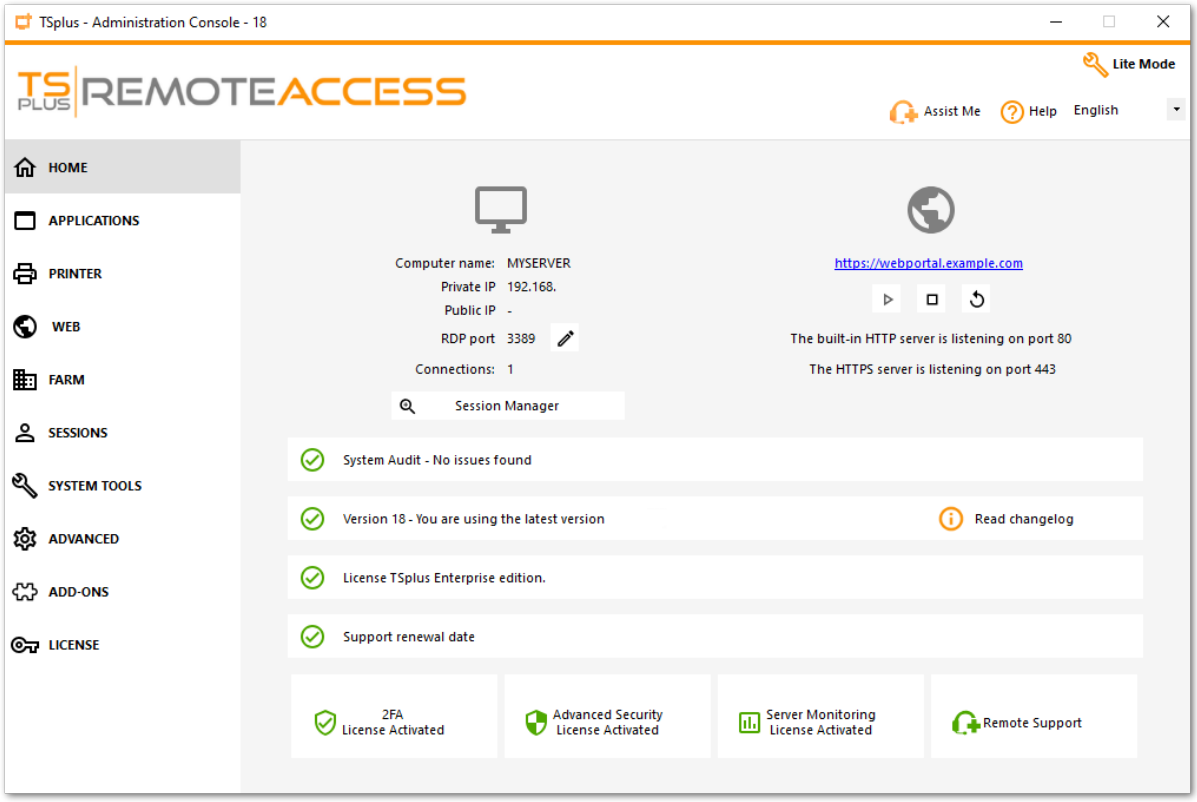
After installing TSplus, your server is immediately ready to go.

However, you can **customize all the system parameters** with a powerful Administrator Tool.

To do so, click on the following icon created on your Desktop:



The Administrator Tool will then be displayed:



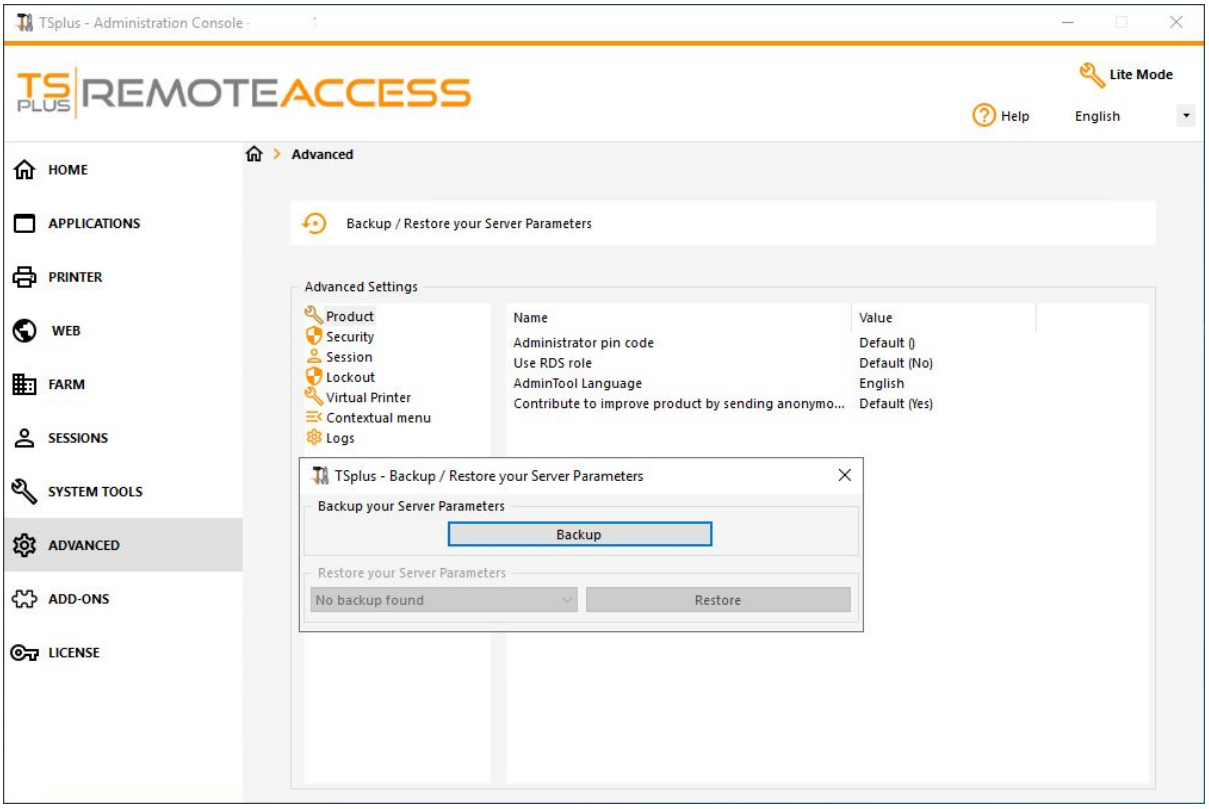
Want to get help on a feature of TSplus Admin Tool quickly? Just **click on a tile or on a tab** to

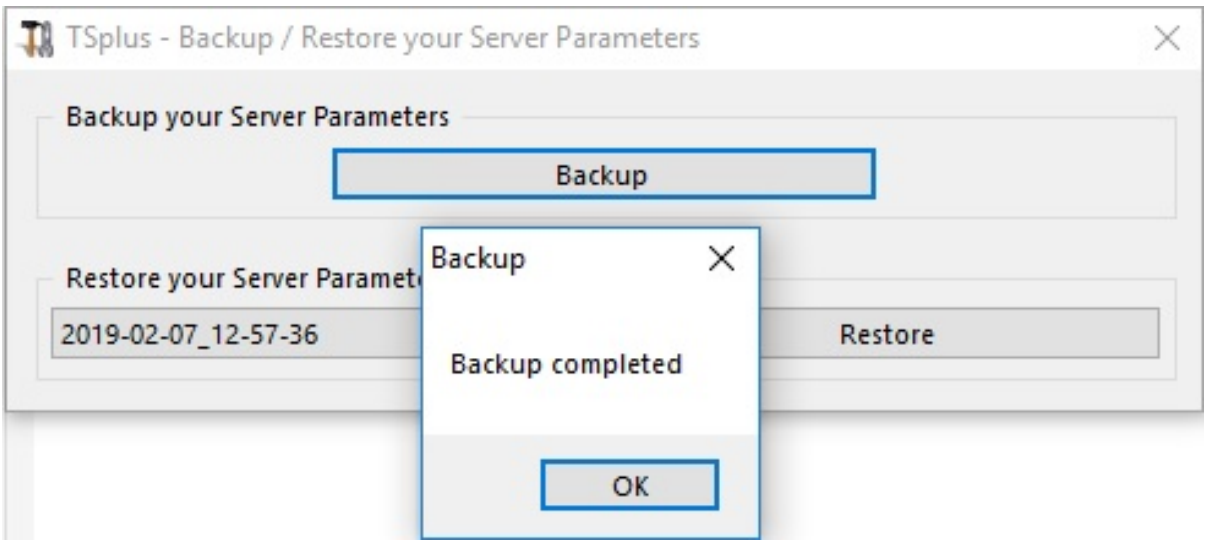
go to the matching help!

Backup and Restore

Since version 14 in the **Advanced** tab, you can configure TSplus settings.

You can Backup or Restore TSplus data and settings by clicking on the button “Backup/Restore” on the top:





The command usage is described below:

- **Backup**:

admintool.exe /backup [optional path to a directory]

By default, the backup will be created in the archives directory located in TSplus TSplus Security setup folder. However, the backup may be saved in a specified folder. Relative and absolute paths are allowed.

- **Restore**:

admintool.exe /restore [path to a backup directory]

The specified backup directory must contain a data and a settings folder, as created by the / backup command.

(if you like using command lines and are wondering what other command lines are available, please go to this specific documentation)

Please follow the steps below to migrate TSplus from computer A to computer B:

1. On computer A, please click on the Backup button to create a new backup. Settings and data will be saved in the archives directory, located on the C:\Backupparam folder.

2. Copy the newly created backup folder (e.g. named backup-2021-01-29_15-01-29), including all content, from the archives directory on computer A to the archives directory on computer B.

3. On computer B, from the Backup / Restore window, in the “Restore” section, select the relevant backup name to be restored.

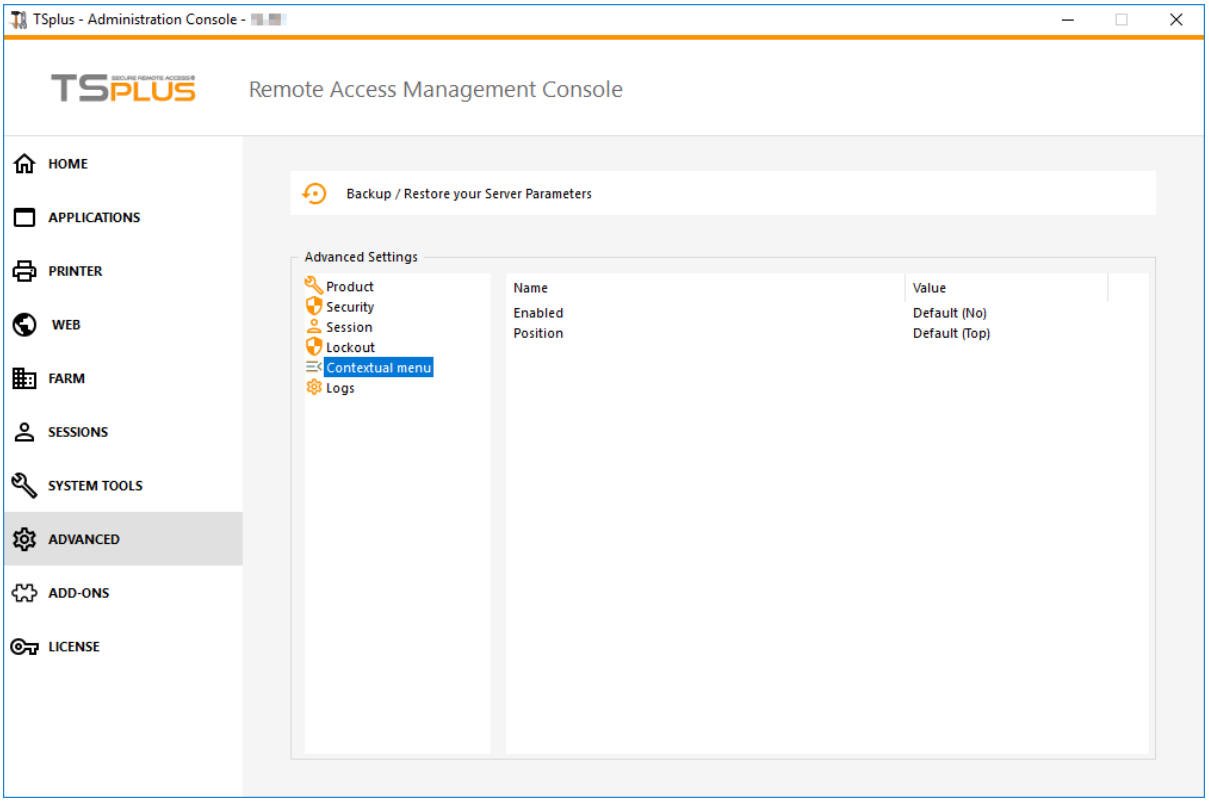
4. Then, click on Restore Settings Only to restore the settings. Alternatively, it is possible to click on Restore to restore all data and settings, which is not recommended for a migration but useful to restore TSplus on computer A.

5. Please wait at most 2 minutes for the settings to be reloaded by TSplus features.

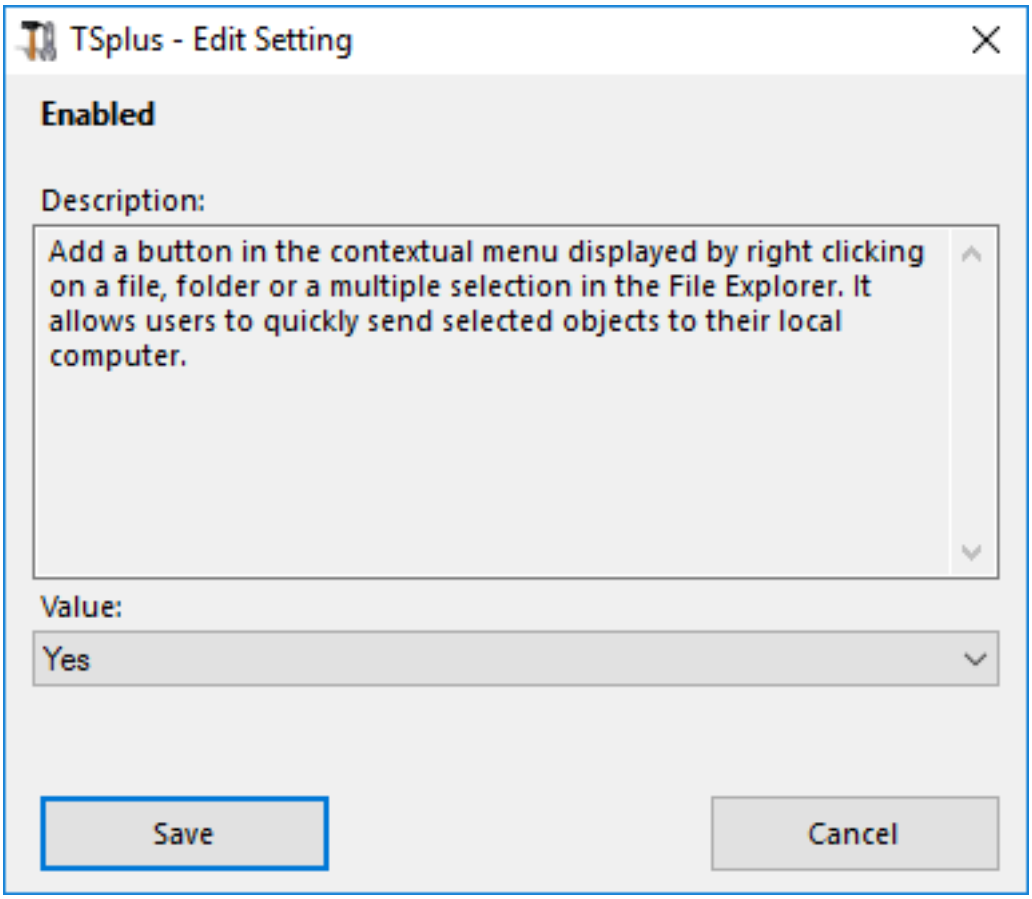
Advanced Features - Contextual Menu

Overview

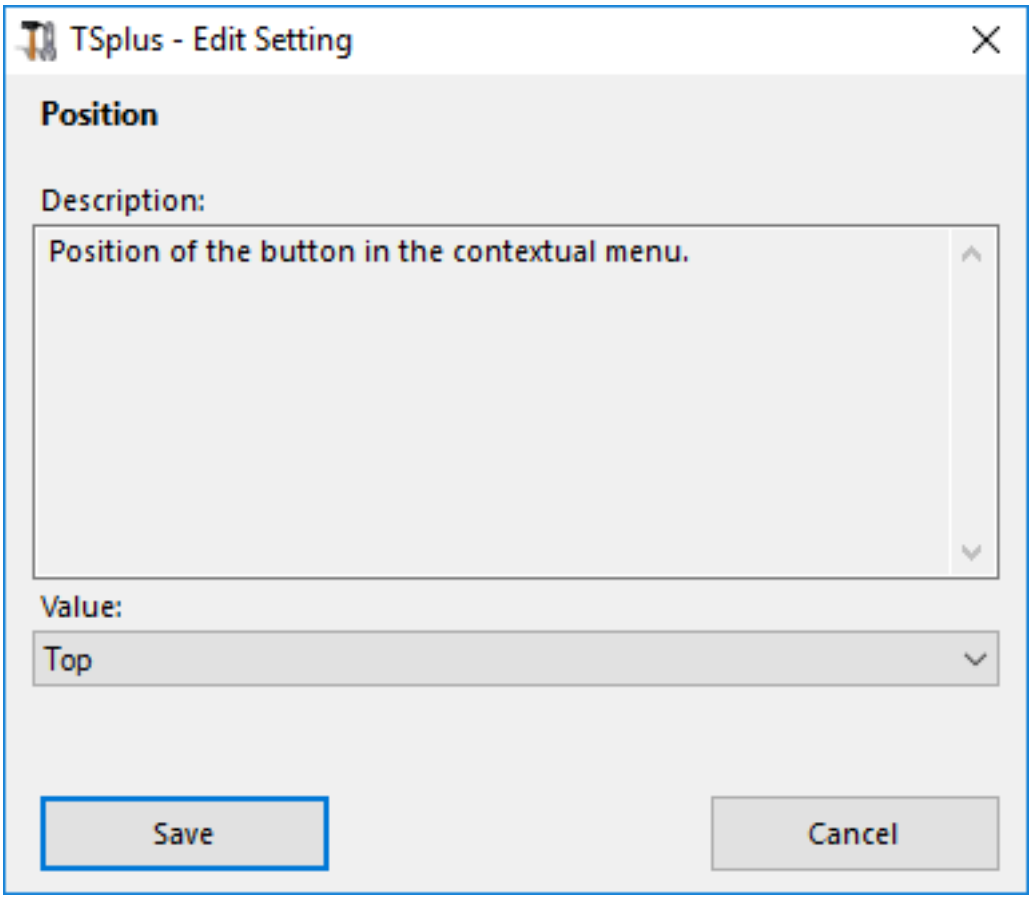
Since TSplus version 12.50, a new **“Send to Client” menu** can be enabled under the Advanced > Contextual Menu tab to easily send files to client workstation. This feature works with all connections methods.



By default, this feature is disabled. Select the “Yes” value then click on “Save”, in order to enable it :

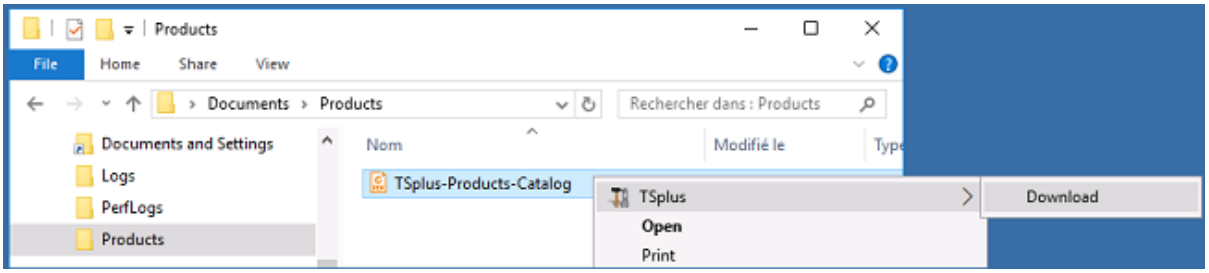


You can also change its position. By default, it will show on top:

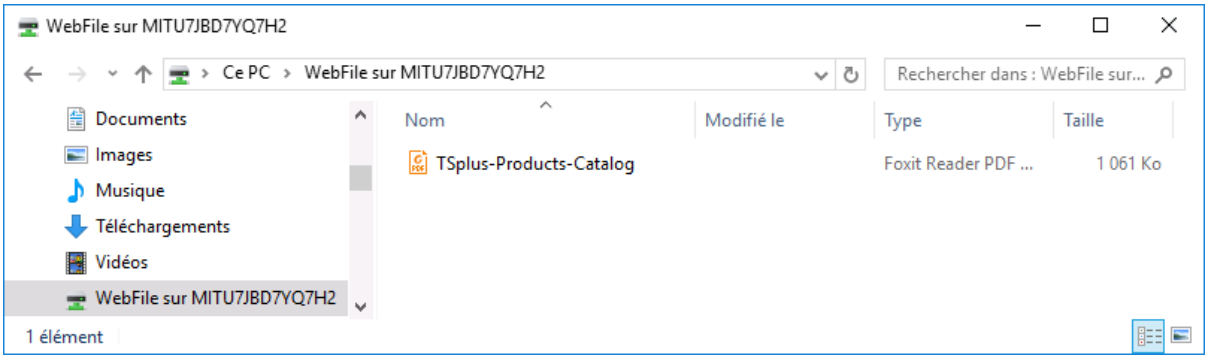


This is a right-click contextual menu. Just select the desired folder or files, right-click on it, select

the “TSplus” tab and simply click on “Download”:



You will find your download into the Webfile folder and into the “Downloads” folder of your web browser:

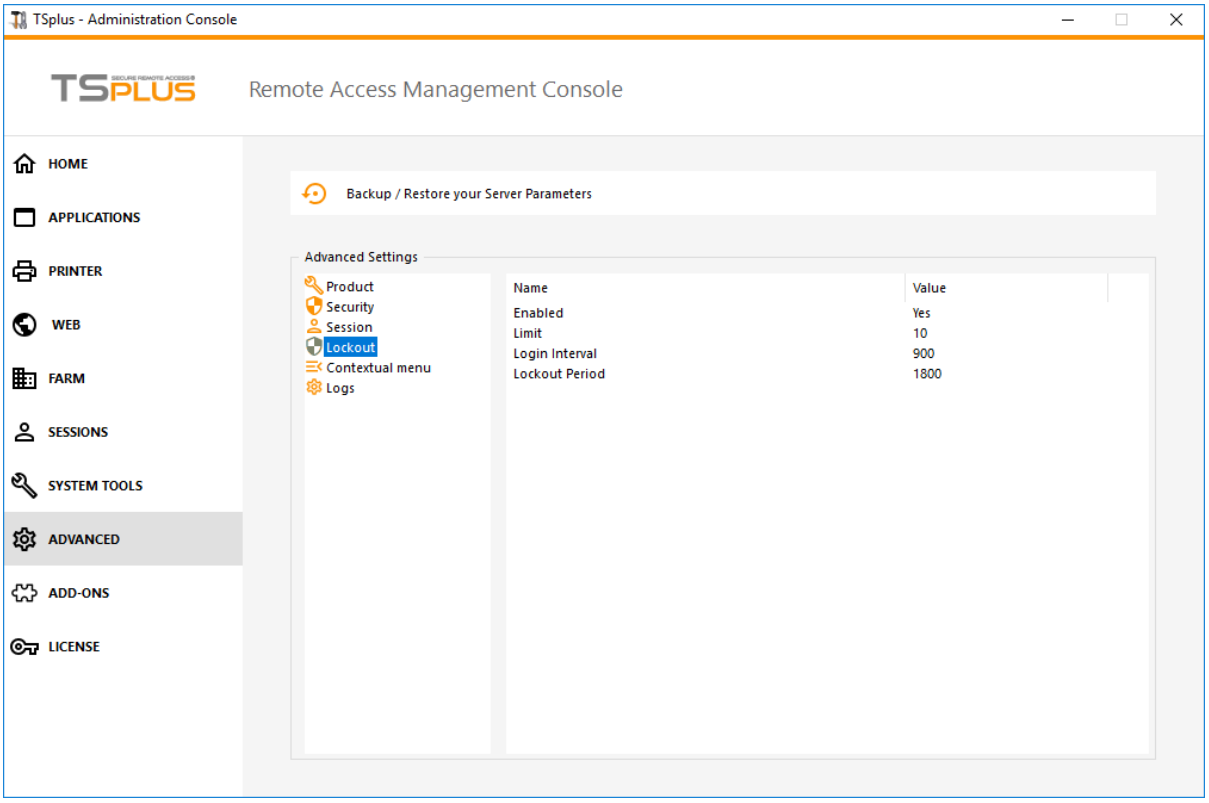


Each downloaded folder is automatically compressed into a zip file.

Advanced Features - Lockout

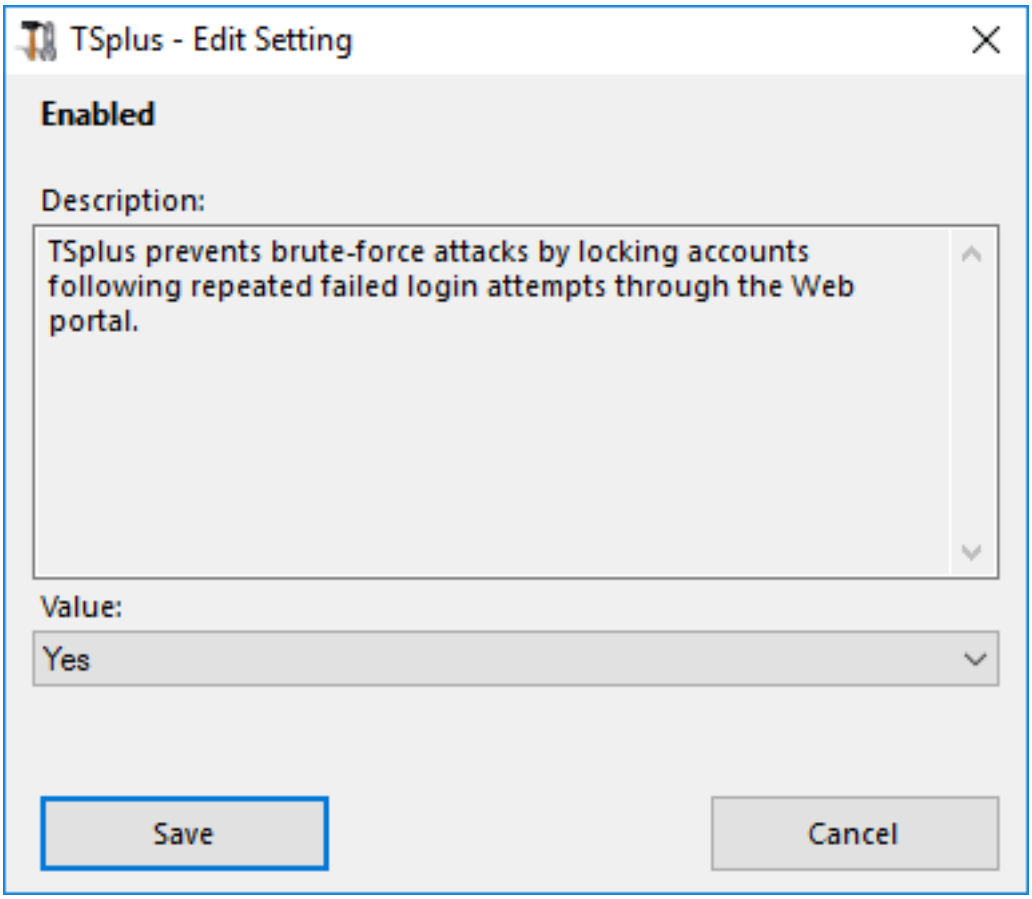
Overview

On this tab, you can enable/disable and configure TSplus Lockout settings.



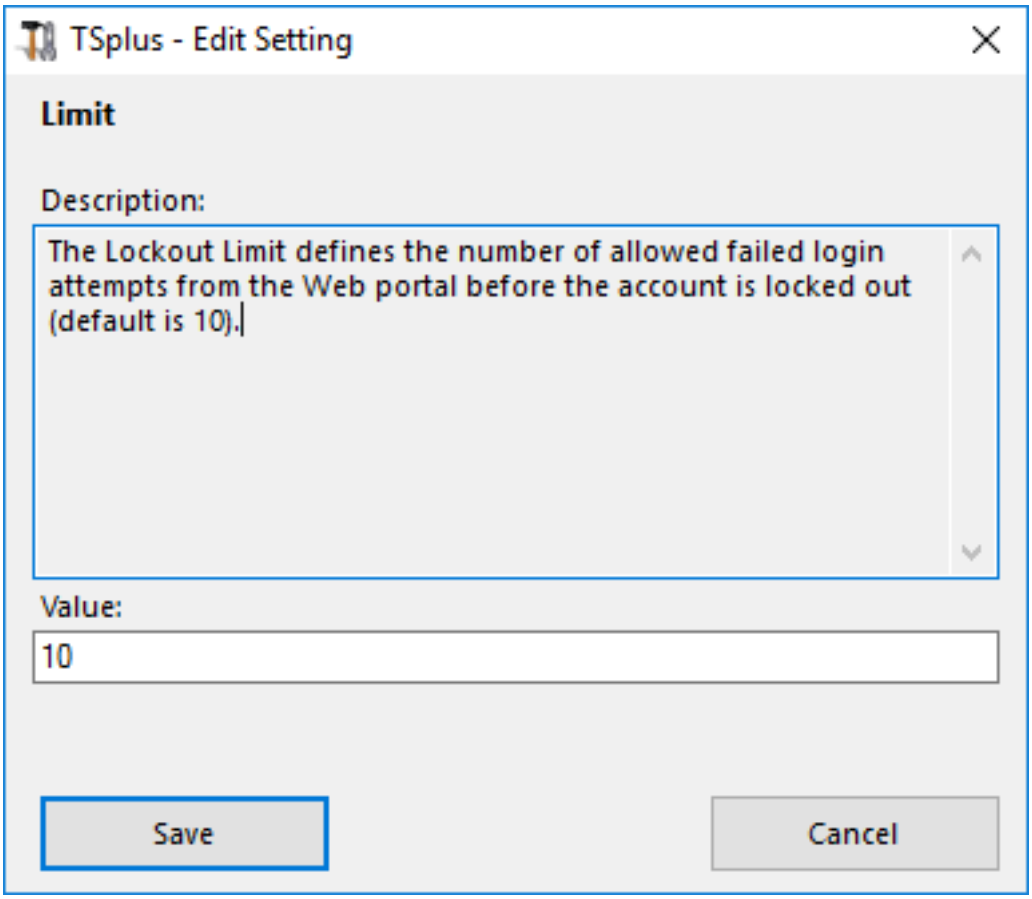
Enable/Disable Lockout Feature

The Lockout Feature is enabled by default. You can disable it by changing the value from “Yes” to “No” value on this window, then click on save.



Limit

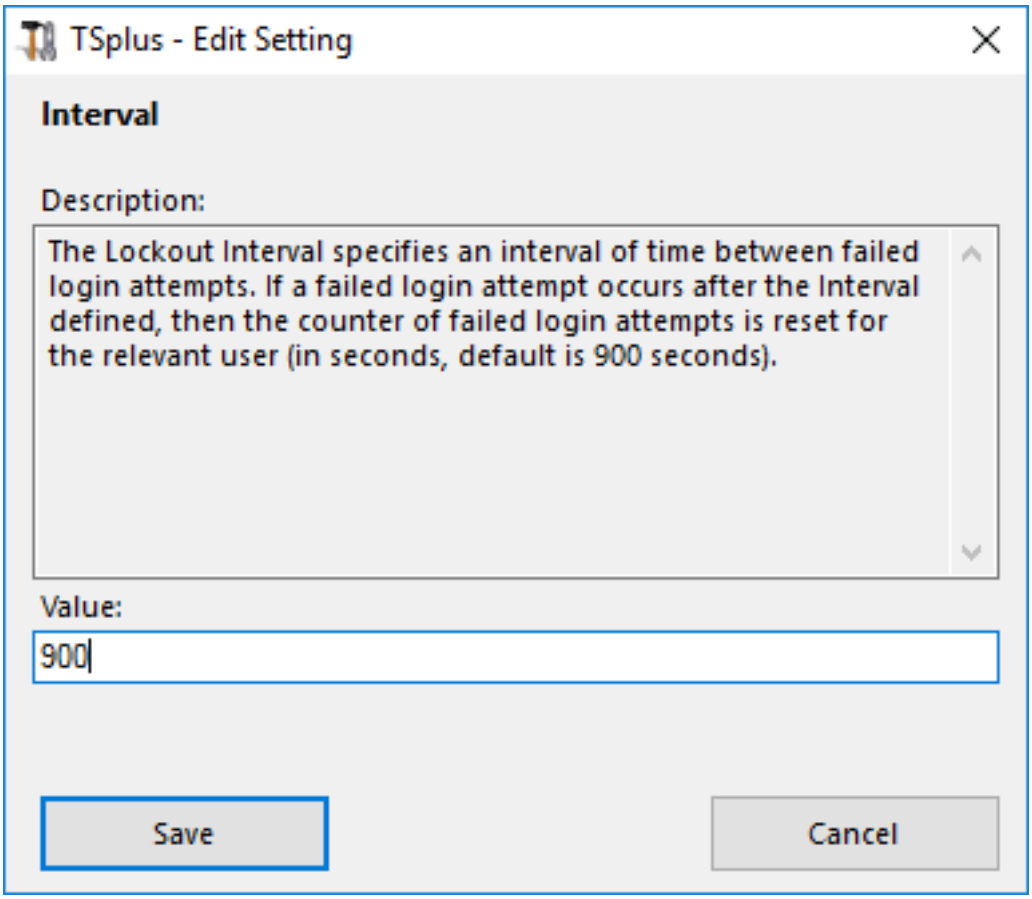
The Lockout Limit defines the number of allowed failed login attempts from the Web portal before the account is locked out (default is 10). You can modify this value by entering the desired value into the corresponding field and click on save.



Interval

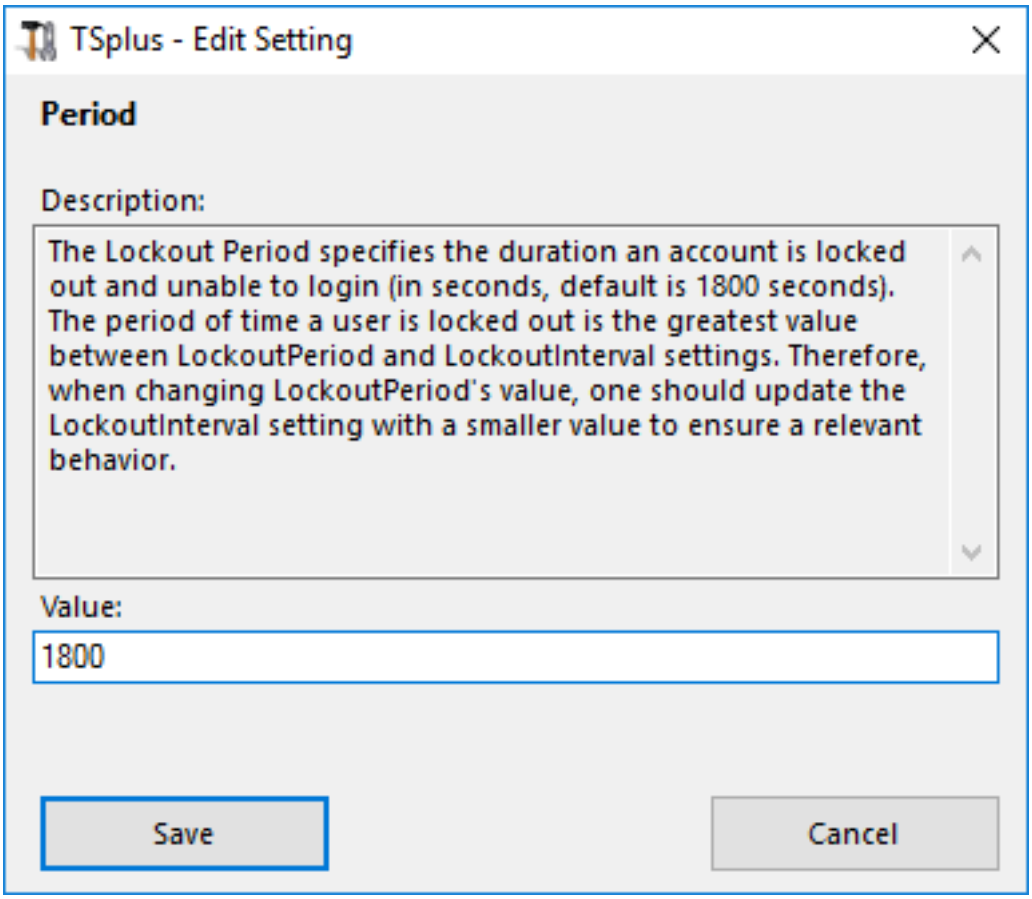
The Lockout Interval specifies an interval of time between failed login attempts.

If a failed login attempt occurs after the Interval defined, then the counter of failed login attempts is reset for the relevant user (in seconds, default is 900 seconds). You can modify this value by entering the desired value into the corresponding field and click on save.



Period

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. You can modify this value by entering the desired value into the corresponding field and click on save.


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

Advanced Features - Logs

Overview

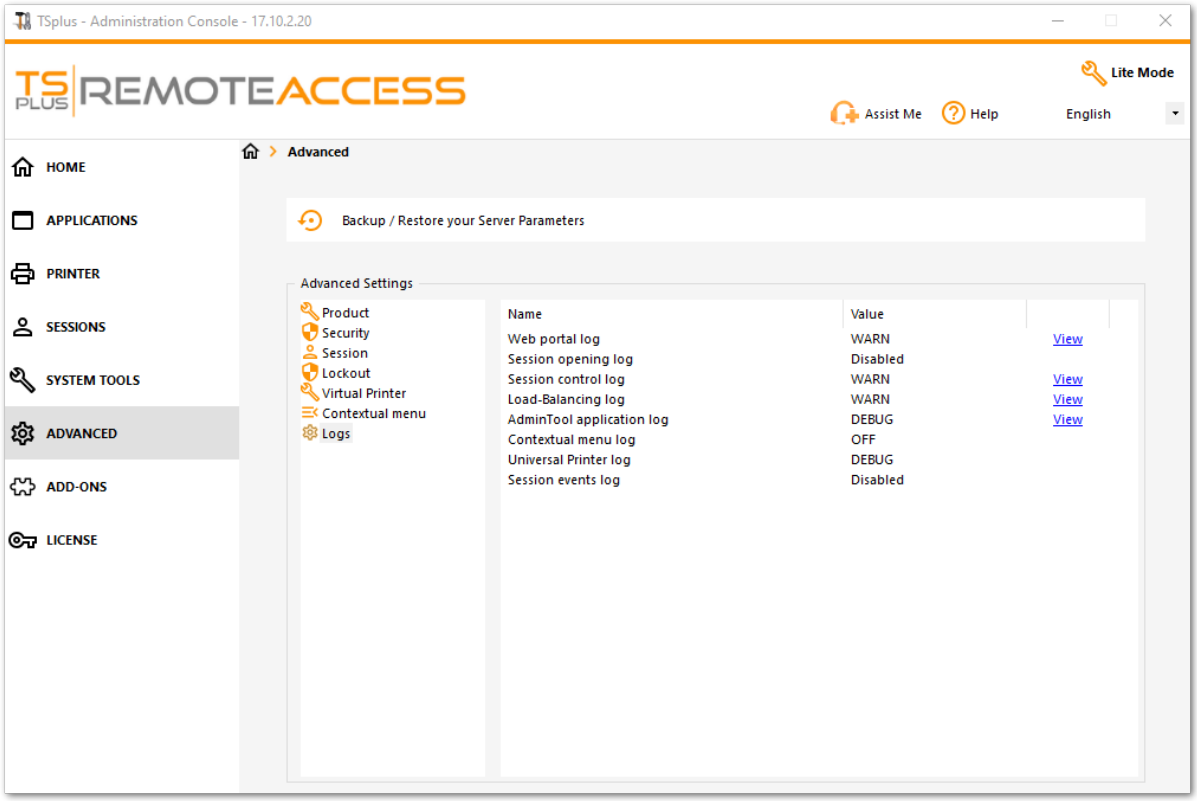
On this tab, you can configure TSplus Logs settings.

By default TSplus doesn’t create logs, to avoid performance issues.

Logs exist to find more easily the origin of the errors encountered on TSplus and you can enable them by doing so:

- go to C:\wsession
- create the folder ‘Trace’. Logs will automatically be created there, per user.

You will need to activate the log generation in the AdminTool > Advanced > Logs



There are 5 types of logs:

- The Web Portal log,
- The Session Opening log,
- The Session control log,
- The Load-Balancing log and
- The AdminTool application (interface) log.

Log levels correspond to different components, our support team will tell you what value to put according to the problem encountered.

Here are the different log file names and locations:

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

Session Opening log: “C:\wsession\trace”

- Session control log: “C:\Program Files (x86)\TSplus\UserDesktop\files\APSC.log”
- Load Balancing log: “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”

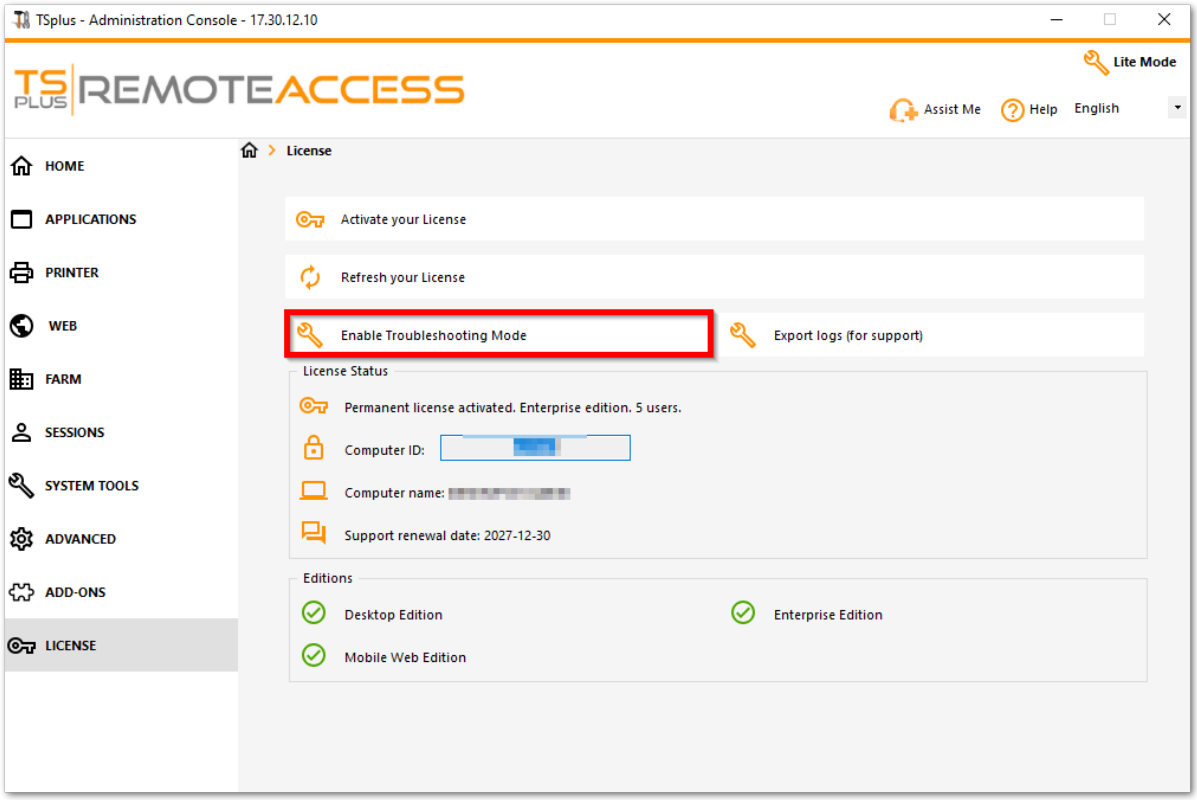
You can enable the logs for Connection Client on the client side by adding the following registry key:

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

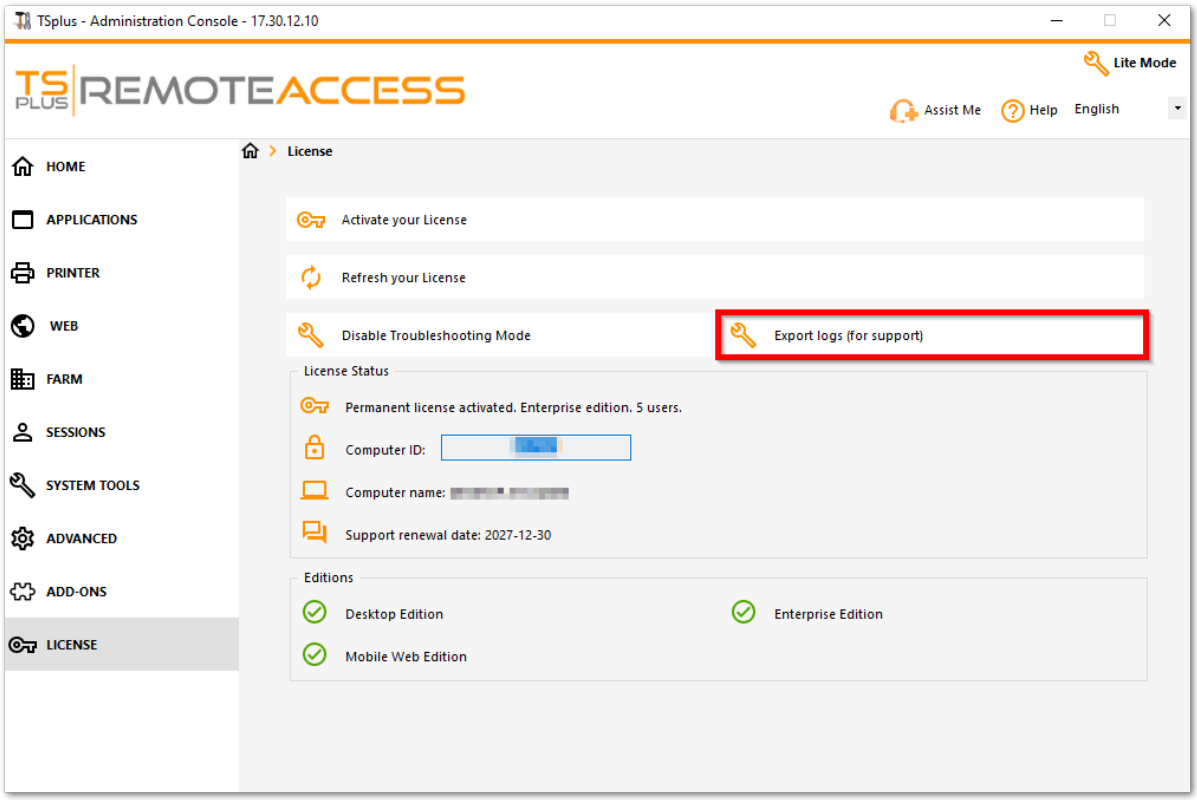
The logs are located in C:\Users<Username>\RDP6\logs directory if installation is per user or in C:\Program Files (x86)\Connection Client\RDP6\logs directory if installation is for all users.

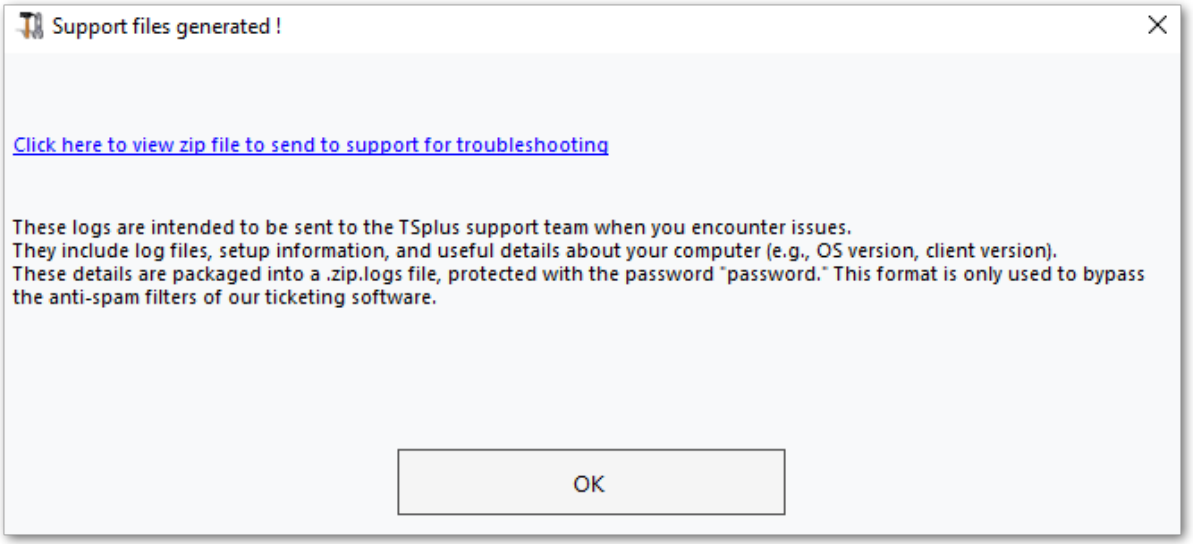
Enable Troubleshooting Mode

Go to the “License” tab Click on the **“Enable Troubleshooting Mode”** button.



Reproduce your problem, then click on the **“Export logs (for support)”** button to send the logs to the support team by email.



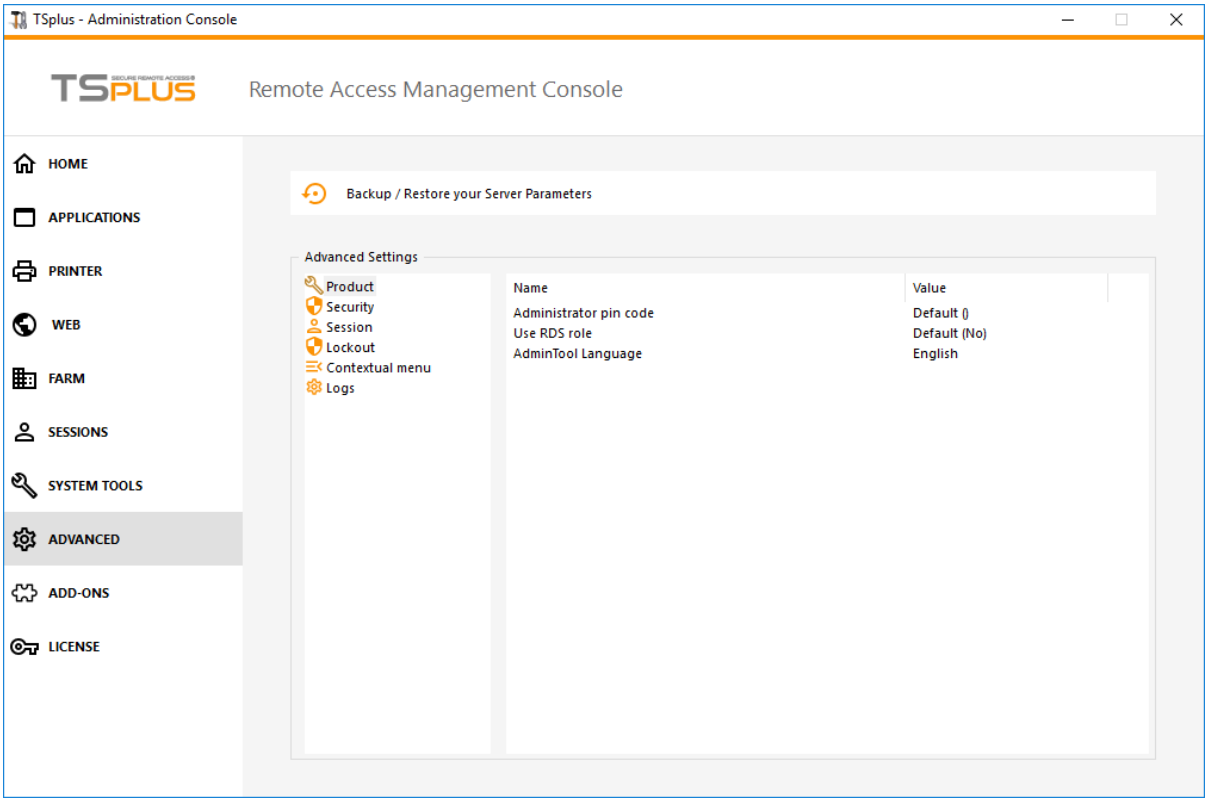


The format of the file to send is **.zip.logs** files and is protected by the password **“password”**.

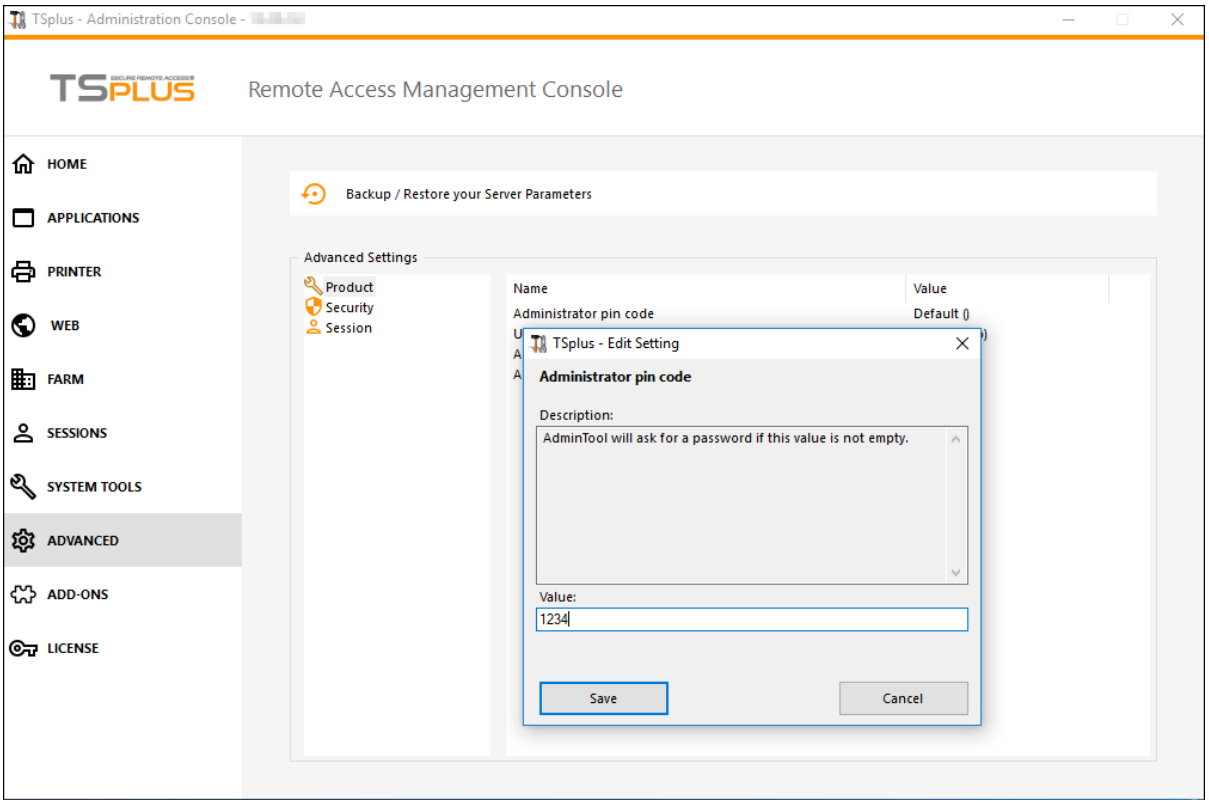
Advanced Features - Product

Overview

On this tab, you can modify TSplus settings by adding an AdminTool Pincode, use the Windows RDS role and customize the background color and language of the AdminTool.



The Administrator can secure the Administrator Tool access by setting a pin code which will be asked at every start, on the Advanced tab of the AdminTool, under the Product Settings:

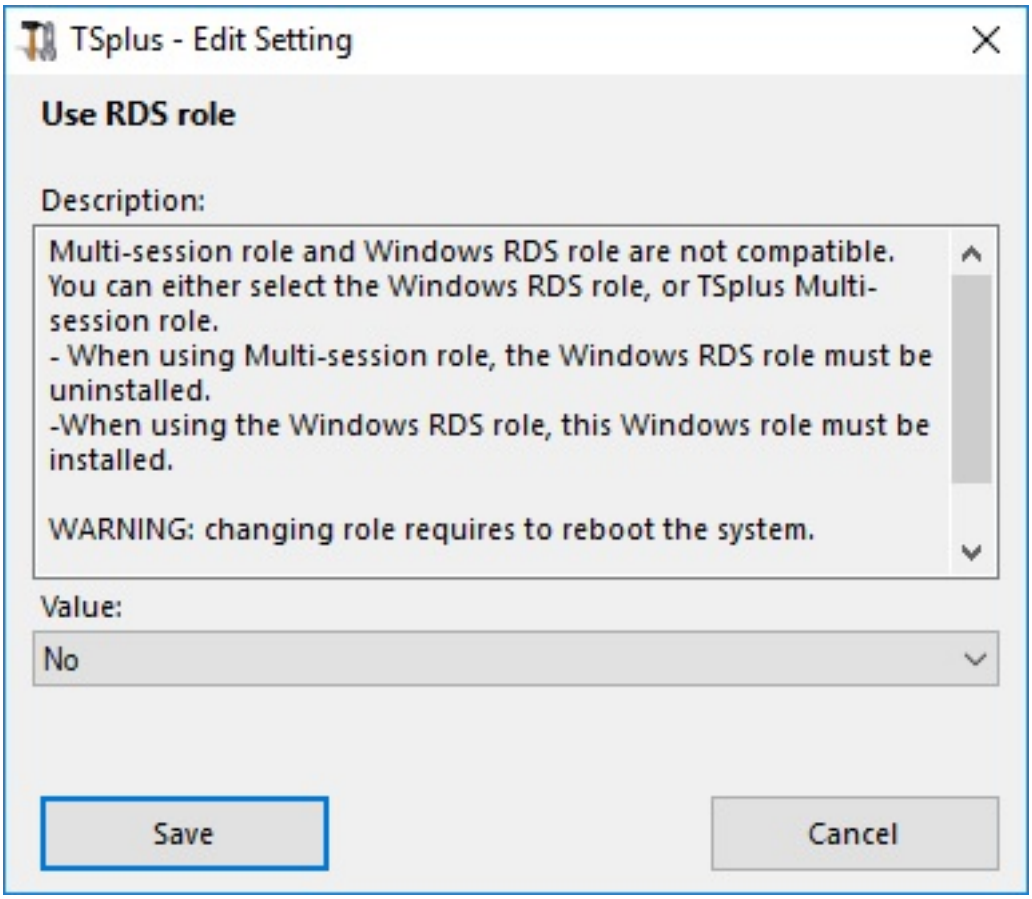


Use RDS role

Multi-session role and Windows RDS role are not compatible. You can either select the Windows RDS role, or TSplus Multi-session role.

- When using Multi-session role, the Windows RDS role must be uninstalled.
- When using the Windows RDS role, this Windows role must be installed.

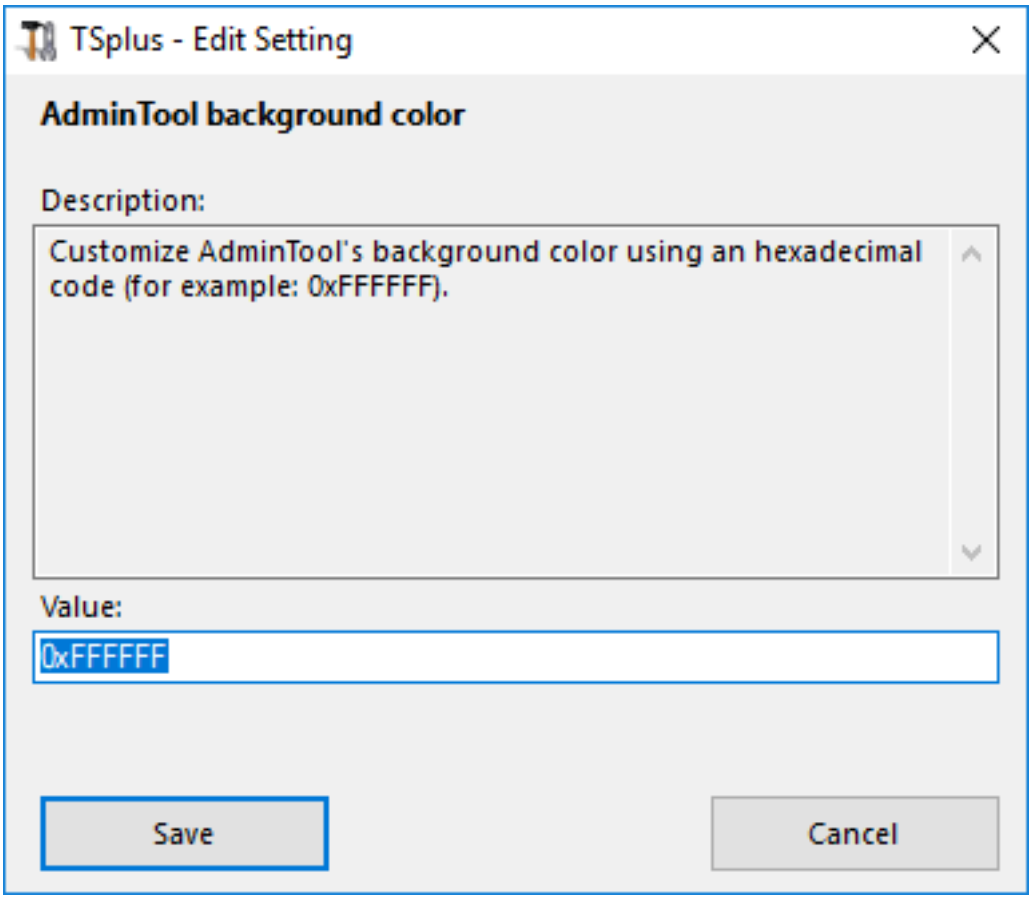
WARNING: changing role requires to reboot the system. When selecting the Windows Remote Desktop, only one user at a time will be allowed on a workstation system.



To use the Windows RDS role, select the “Yes” value and Save.

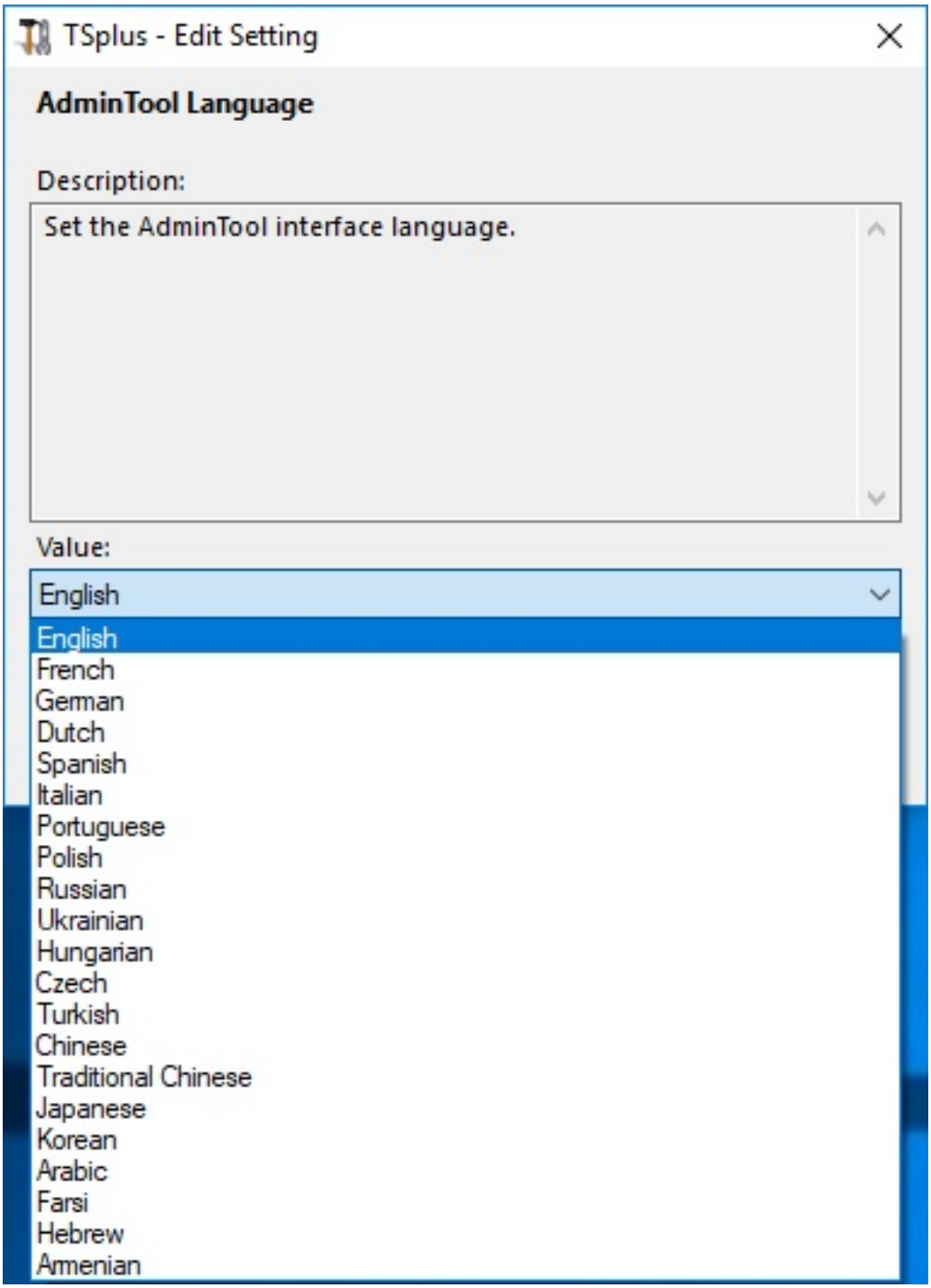
Modify the AdminTool Background color

Customize AdminTool’s background color using an hexadecimal code (for example: 0xFFFFFF).



Modify the AdminTool Language

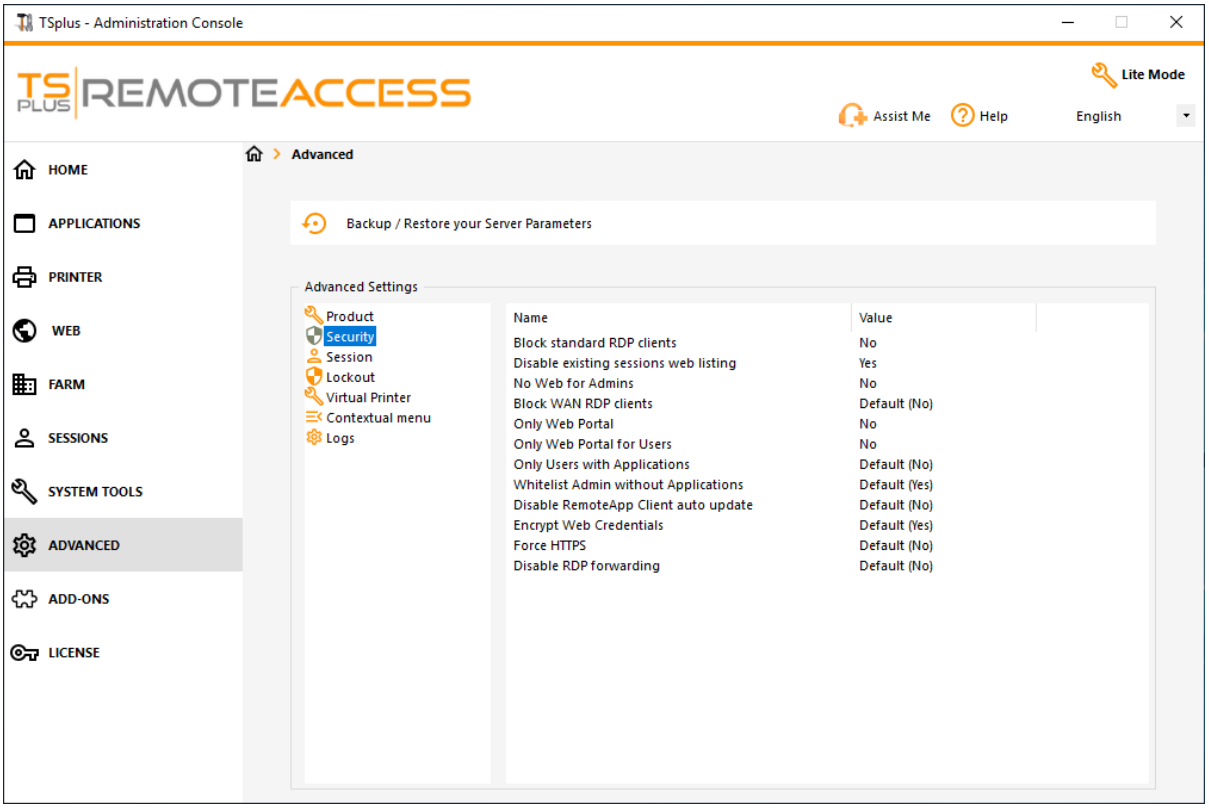
Select your preferred language for the AdminTool among the 21 available.


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

Advanced Features - Security

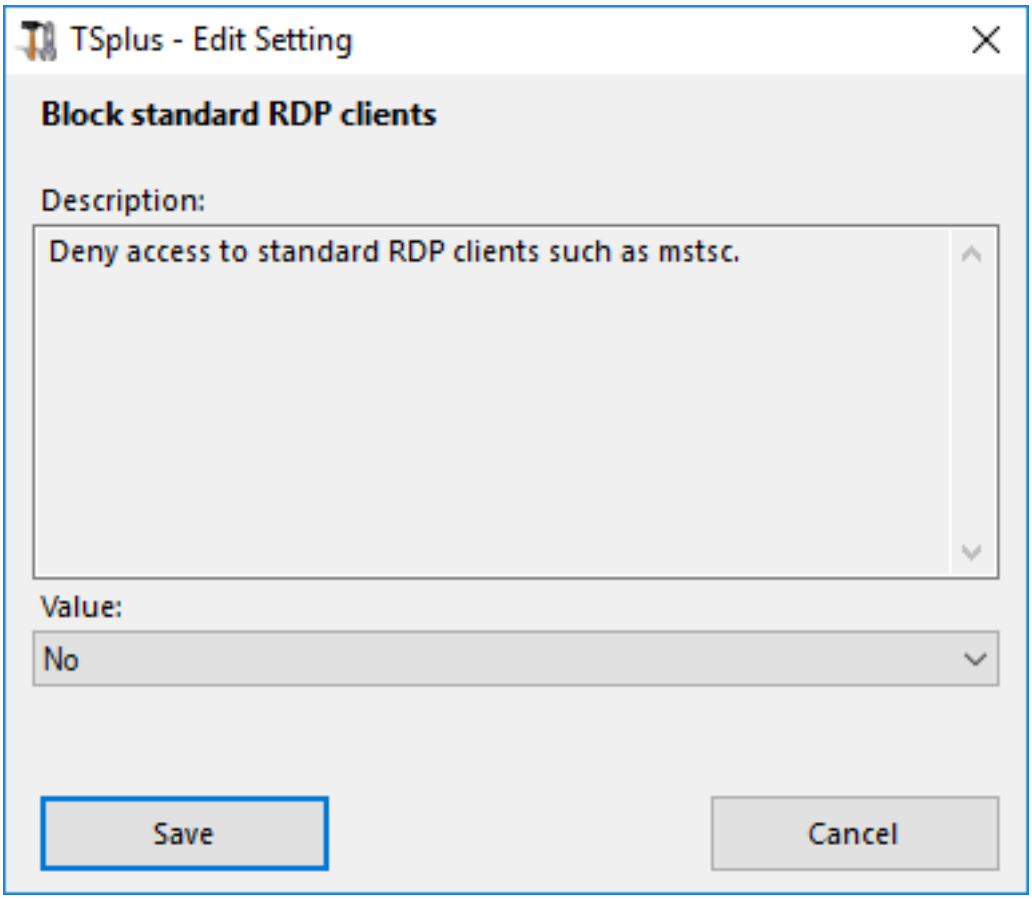
Overview

On the Security section of the Advanced features, you can block, disable or customize connection types for users.



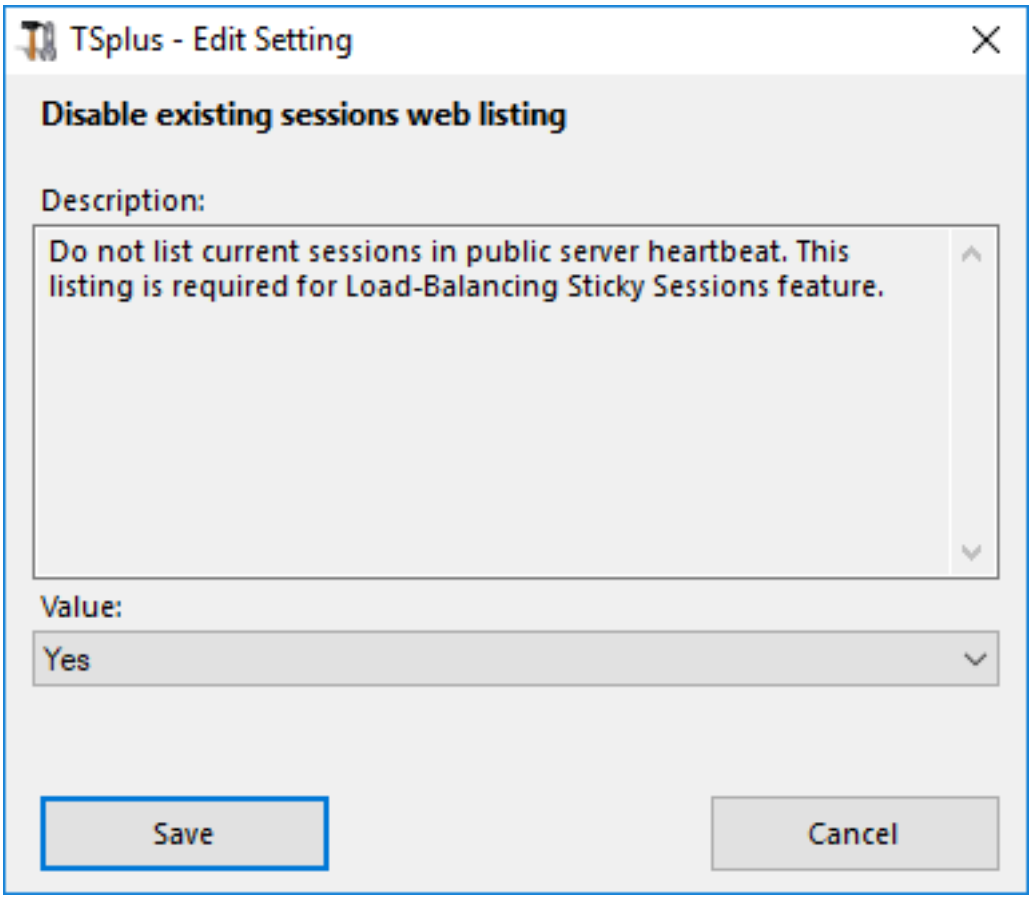
Block Standard RDP Clients

Select the “Yes” value if you wish to deny access to standard RDP clients such as mstsc to your users.



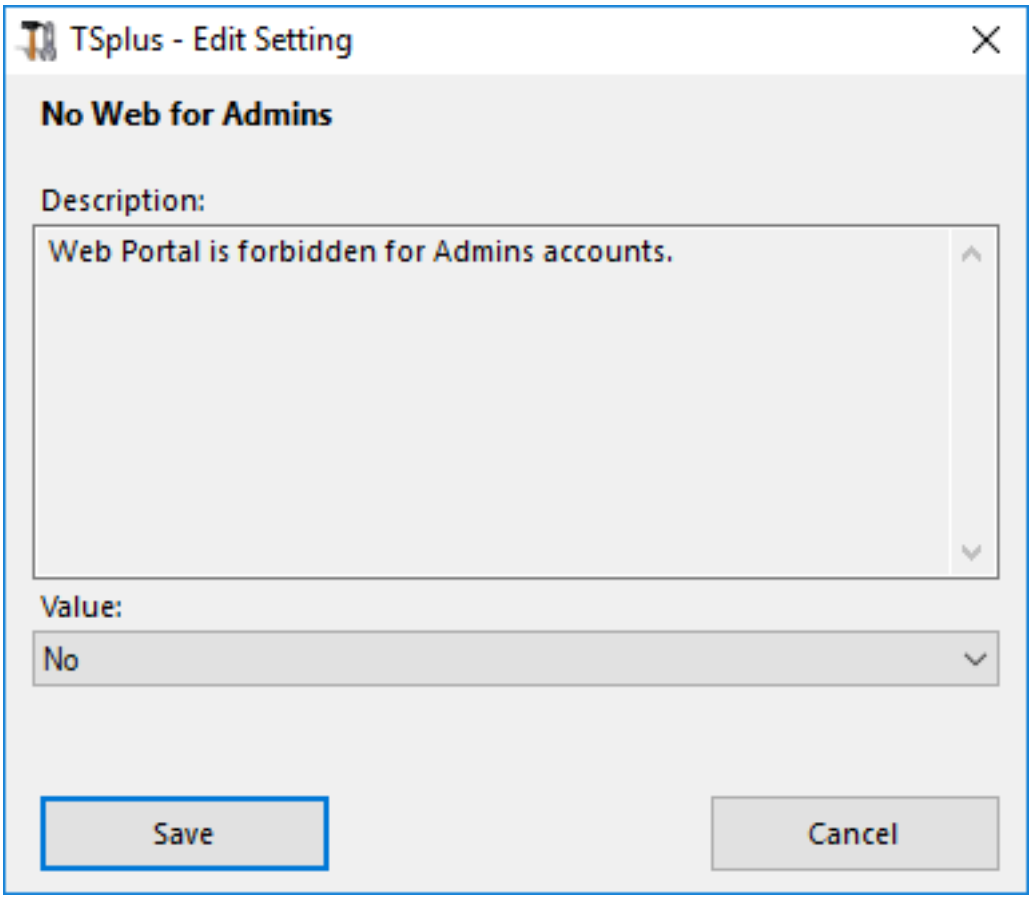
Disable existing sessions web listing

This listing is required for Load-Balancing Sticky Sessions feature and is enabled by default. If you wish to disable it, select the “No” value on this window, then click on save:



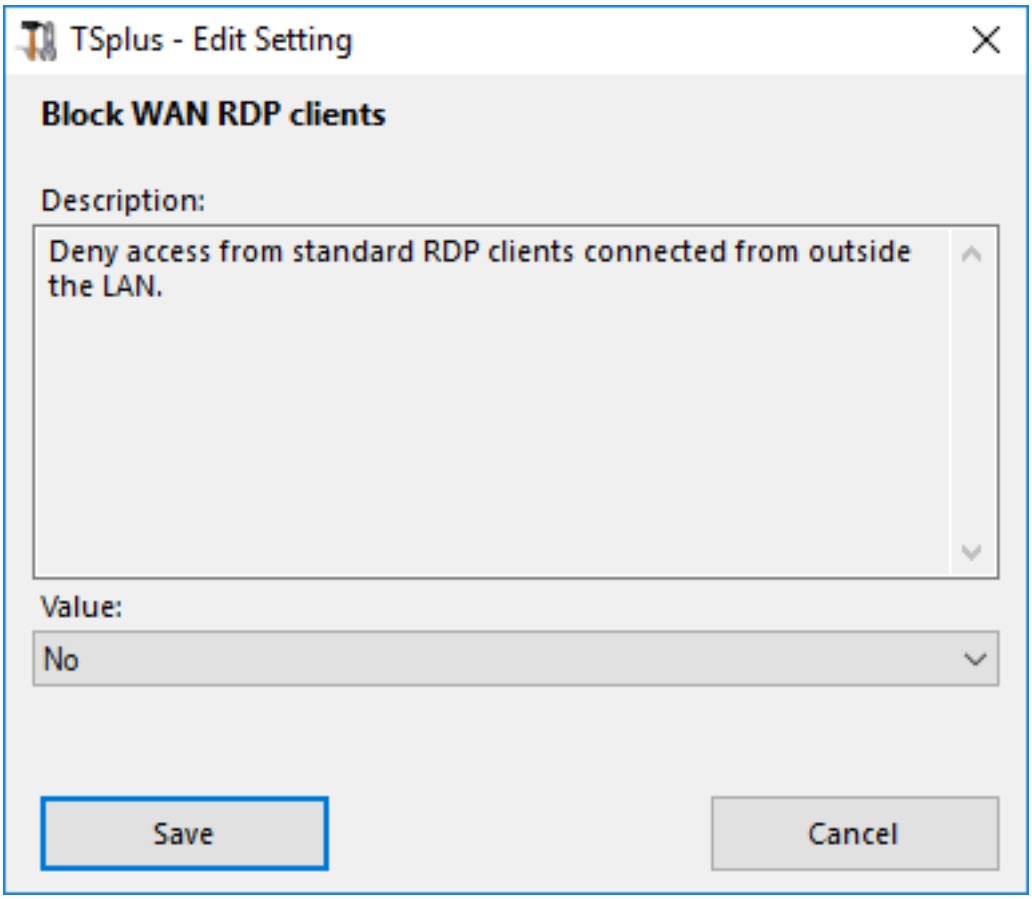
No Web for Admins

Disable the Web Portal for Administrators by selecting the “Yes” value:



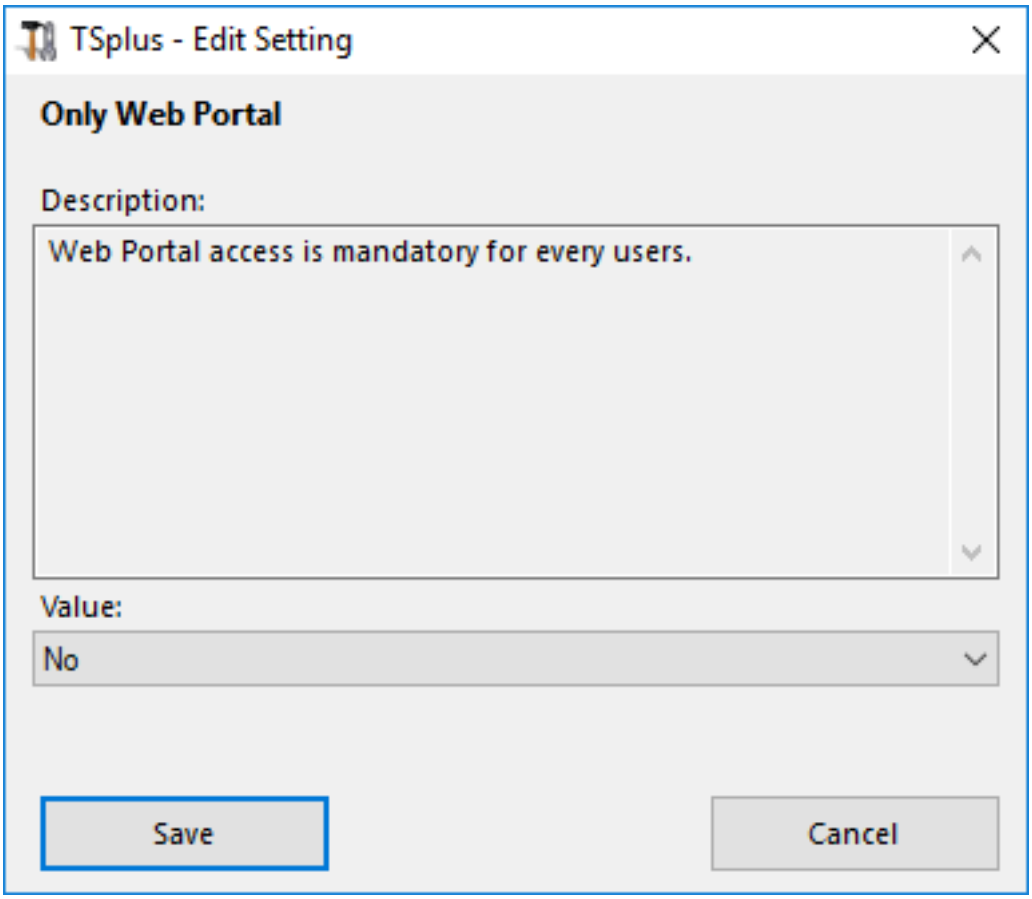
Block WAN RDP clients

Deny access from standard RDP clients connected from outside the LAN by selecting the “Yes” value.



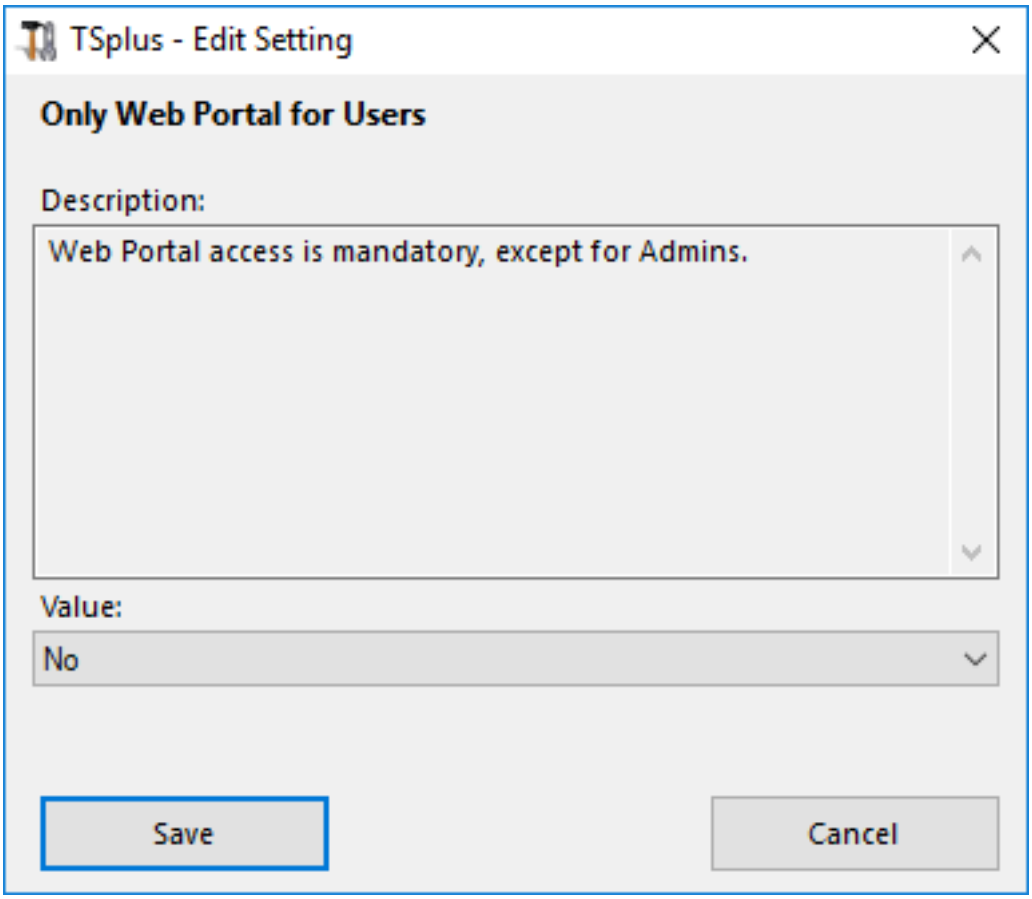
Only Web Portal

Make Web Portal access mandatory for every user by selecting the “yes” value.



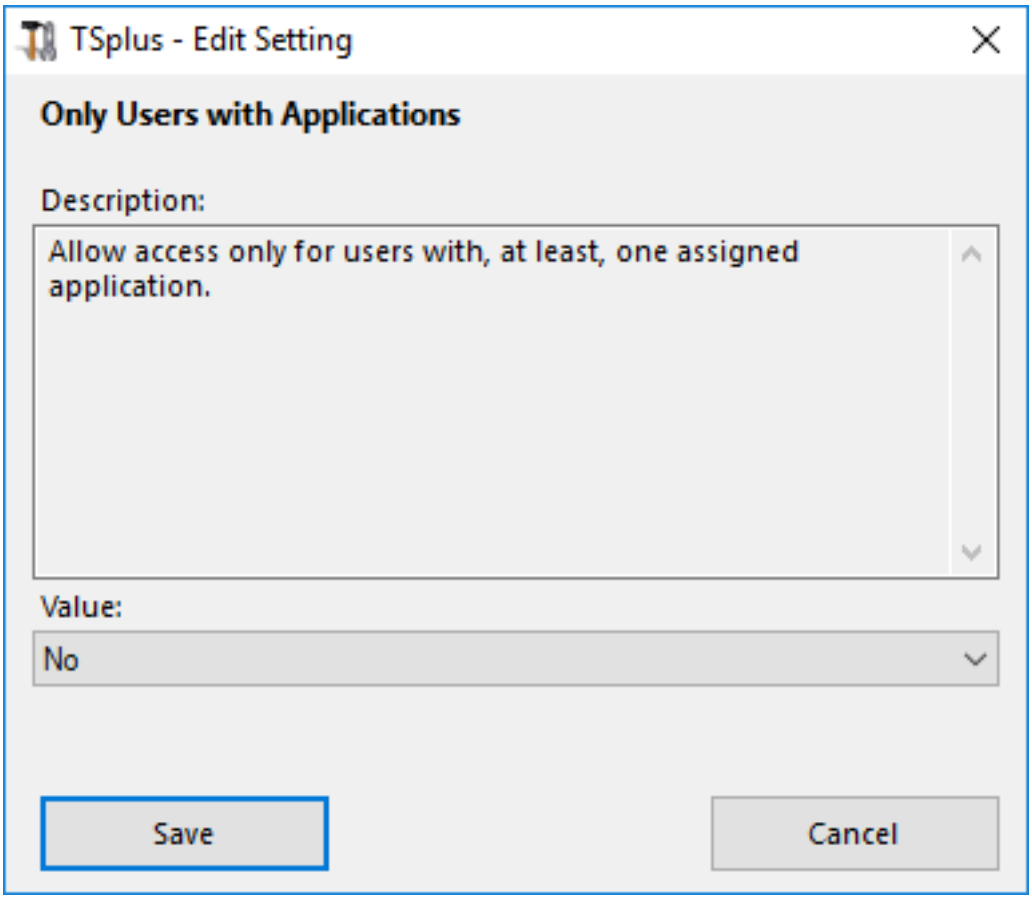
Only Web Portal for Users

Make Web Portal access mandatory for every user, except the Admins by selecting the “yes” value.



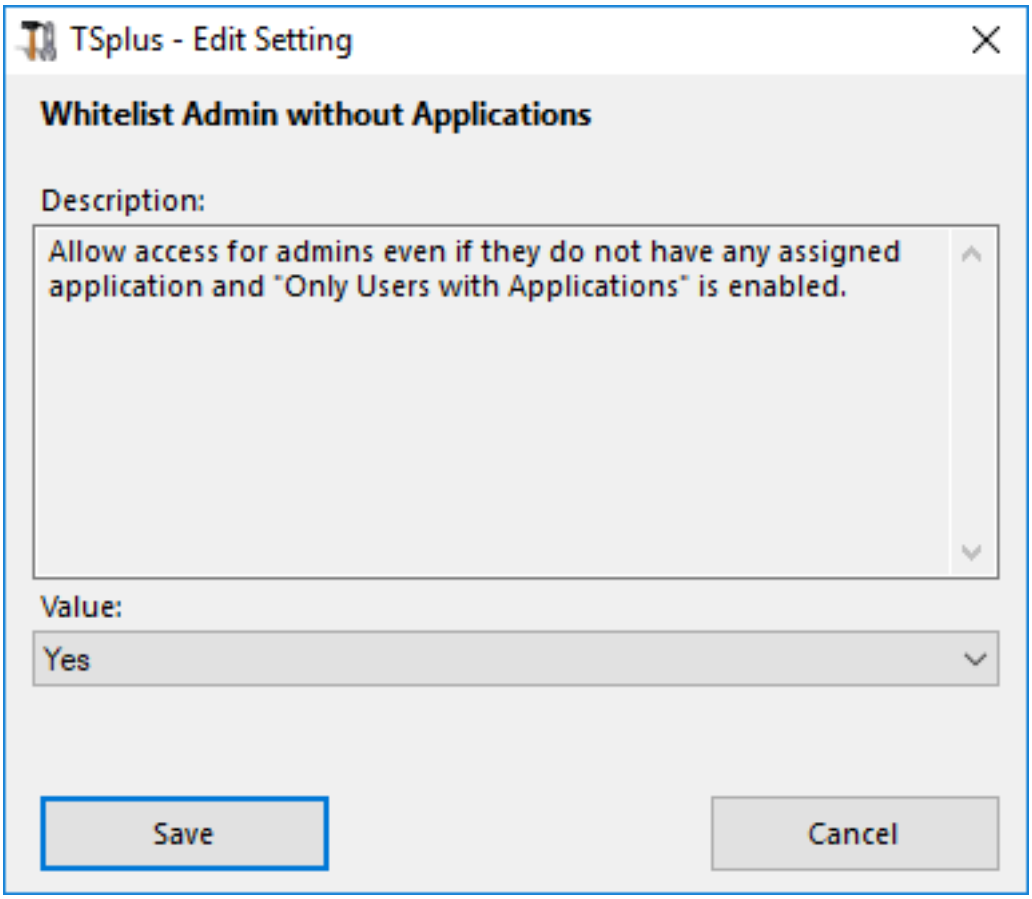
Only Users with Applications

Allow access only for users with, at least, one assigned application by selecting the “yes” value.



Whitelist Admins without Applications

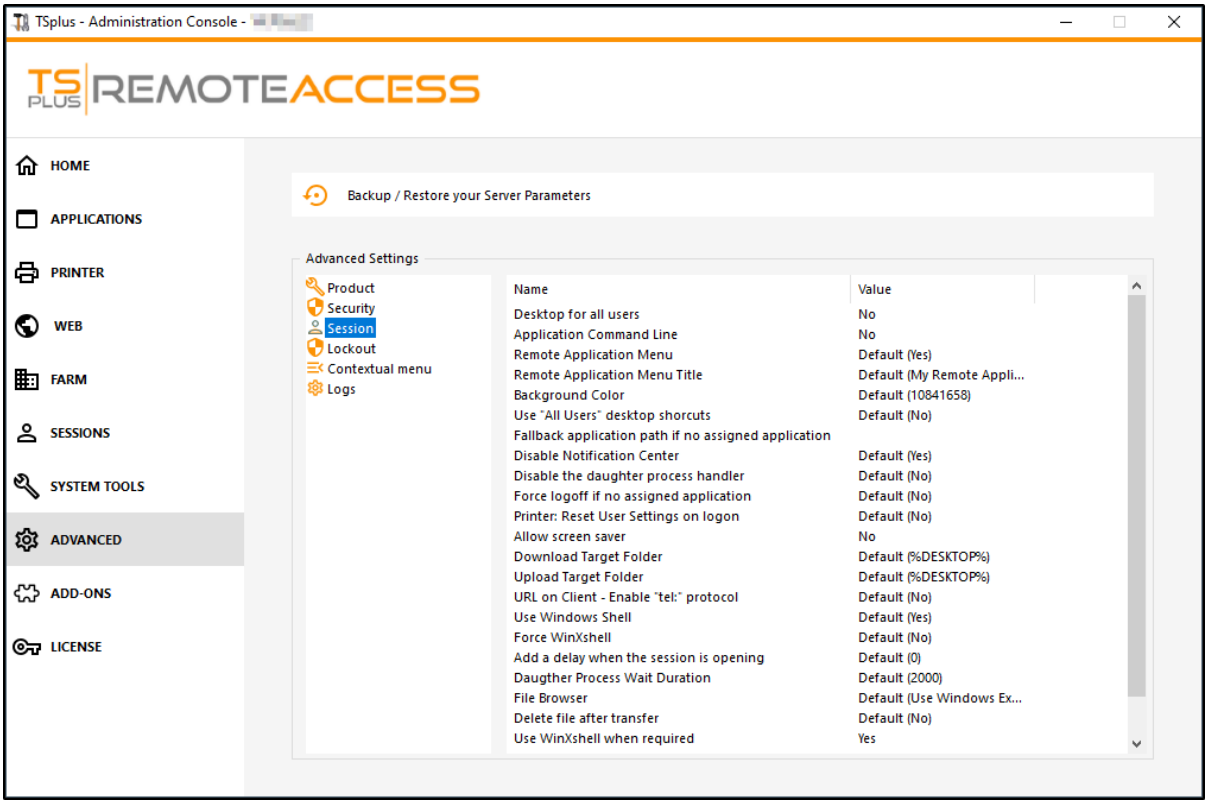
Allow access for admins even if they do not have any assigned application and “Only Users with Applications” is enabled. This feature is enabled by default. If you wish to disable it, select the “No” value on this window, then click on save:


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

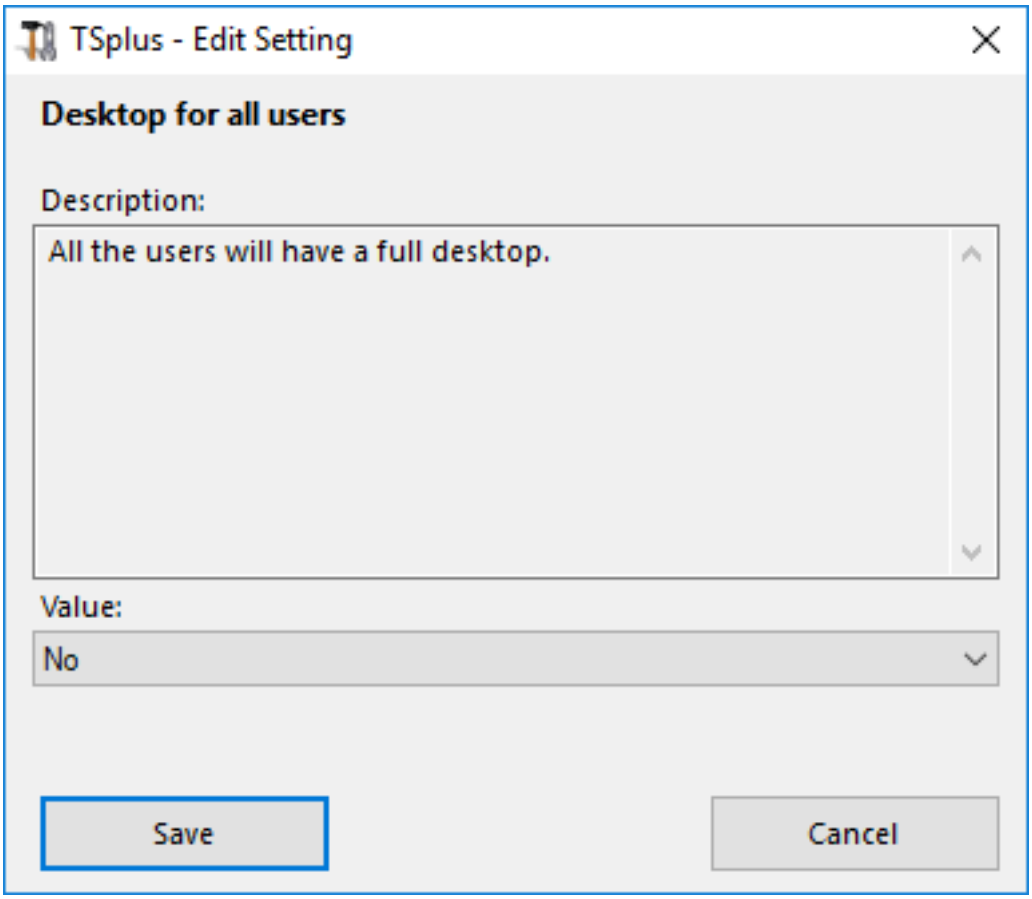
Advanced Features - Session

Overview

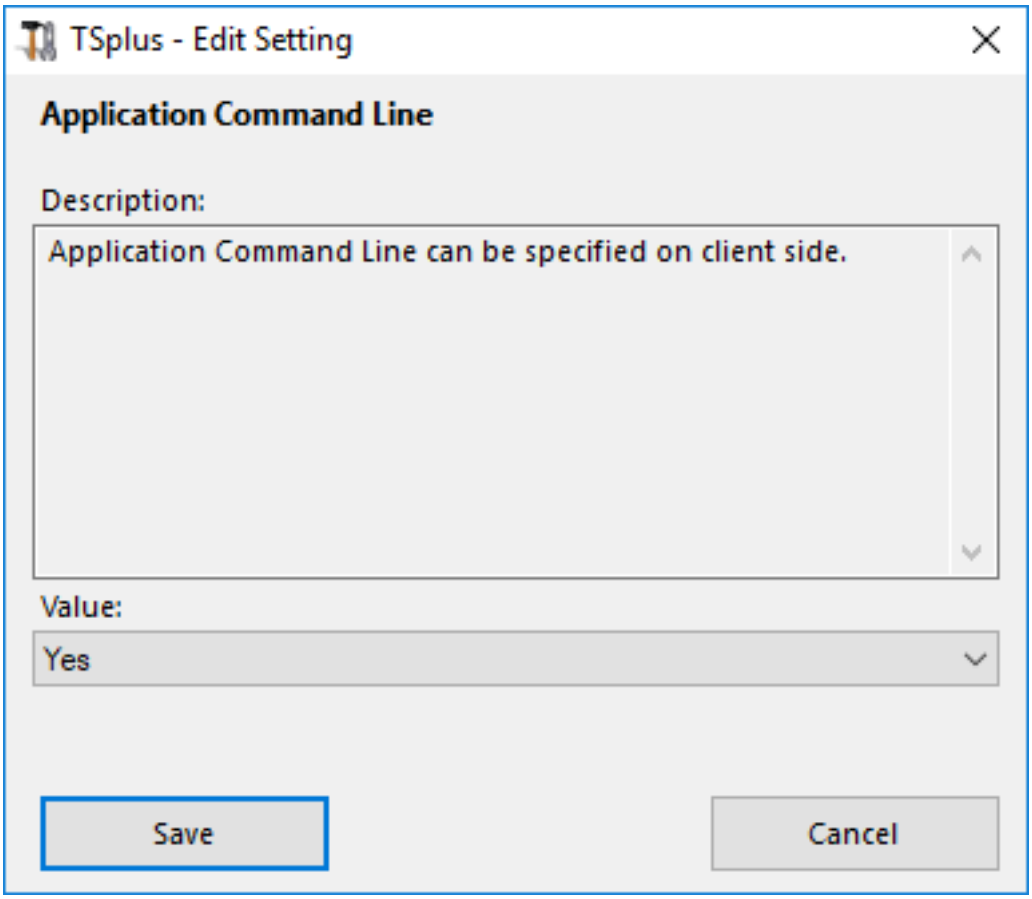
This section of the Advanced tab allows you to configure user rights and aspects on their sessions.



Enable a full Desktop for all users by selecting the “Yes” value on this window, then click on save:

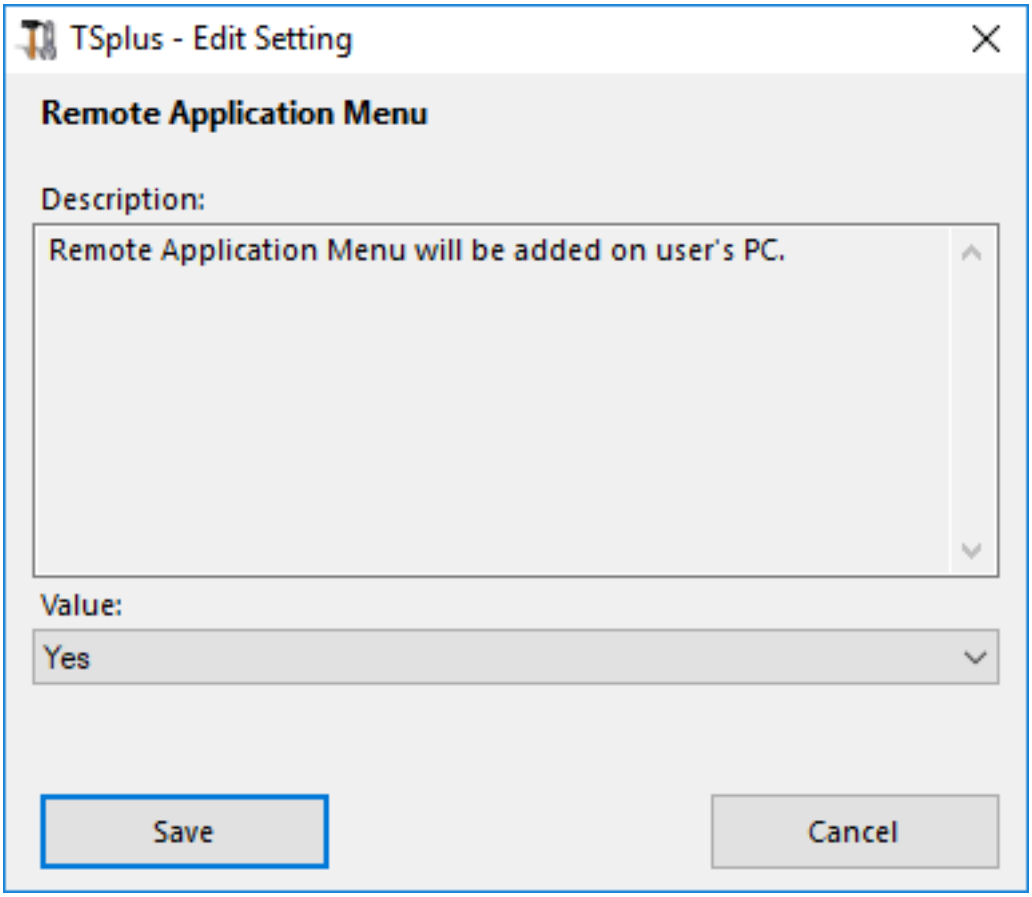


Application Command Line can be specified on client side. This feature is enabled by default. If you wish to disable it, select the “No” value on this window, then click on save:



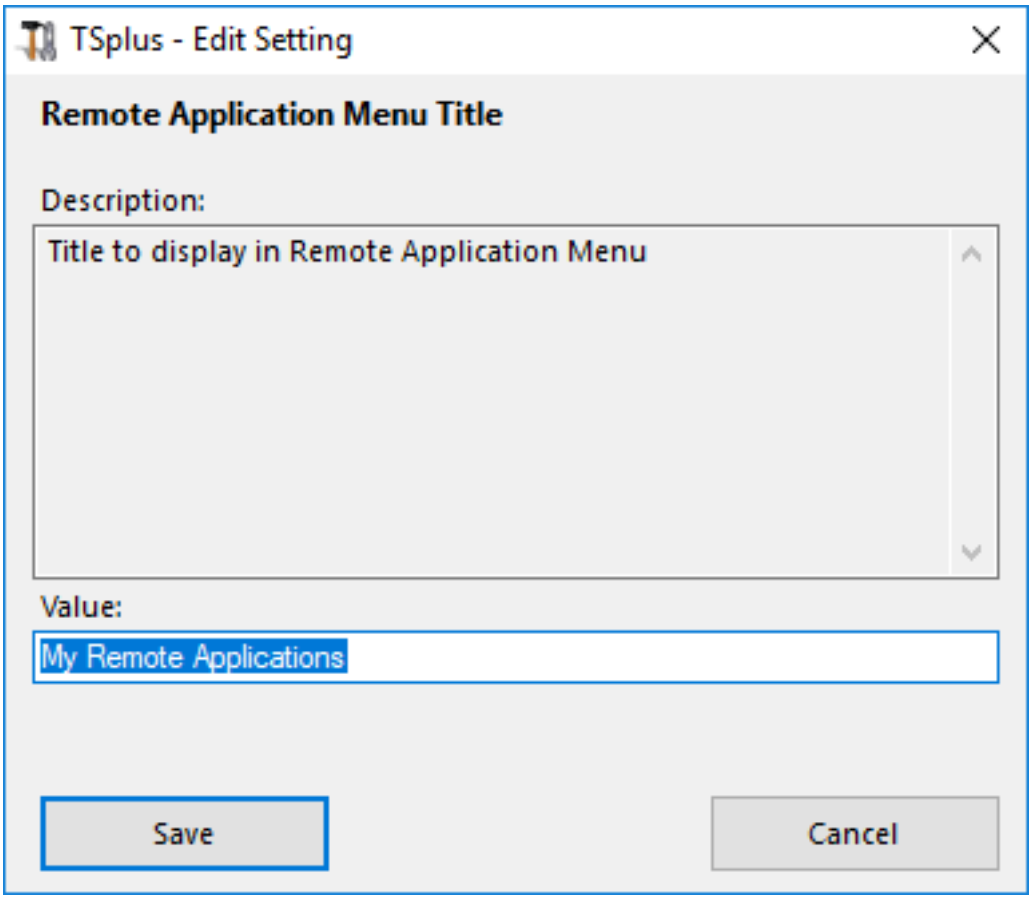
Remote Application Menu

Remote Application Menu will be added on user's PC. This feature is enabled by default. If you wish to disable it, select the "No" value on this window, then click on save:



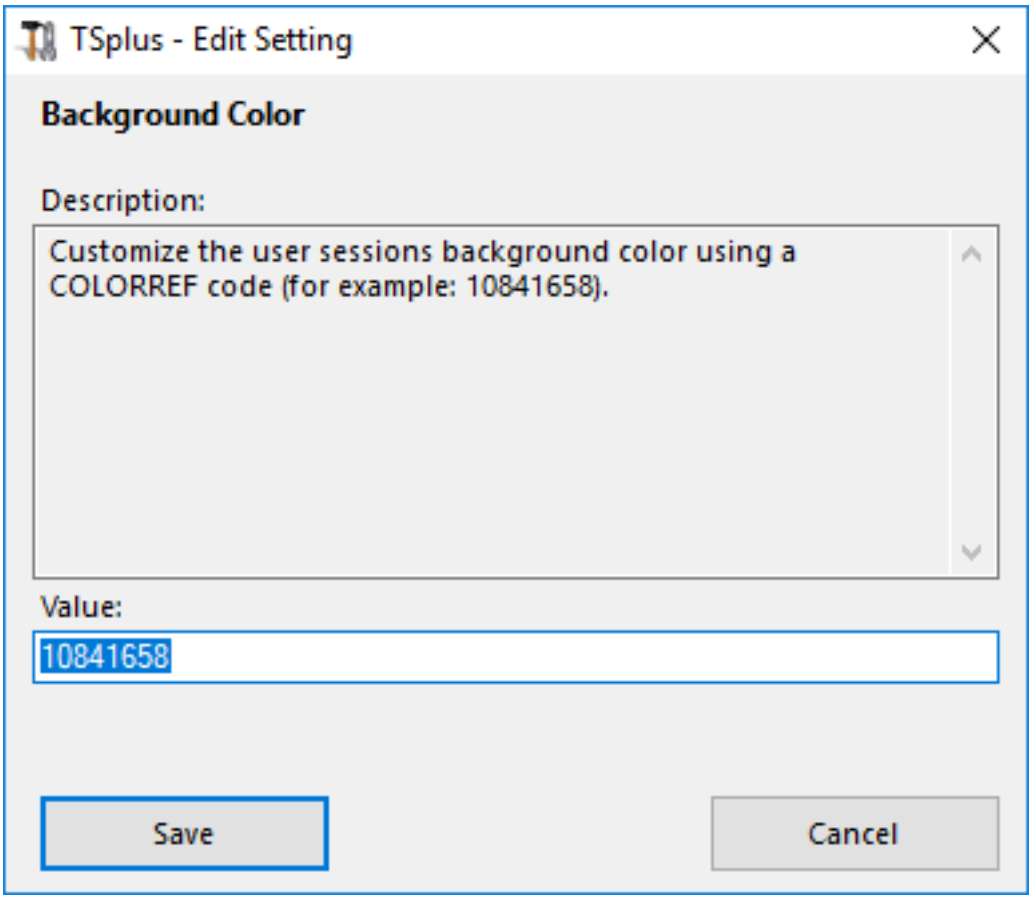
Remote Application Menu Title

You can modify the title of the Remote Application Menu. The default one is "My Remote Applications". If you wish to modify it, enter the desired title, then click on save:



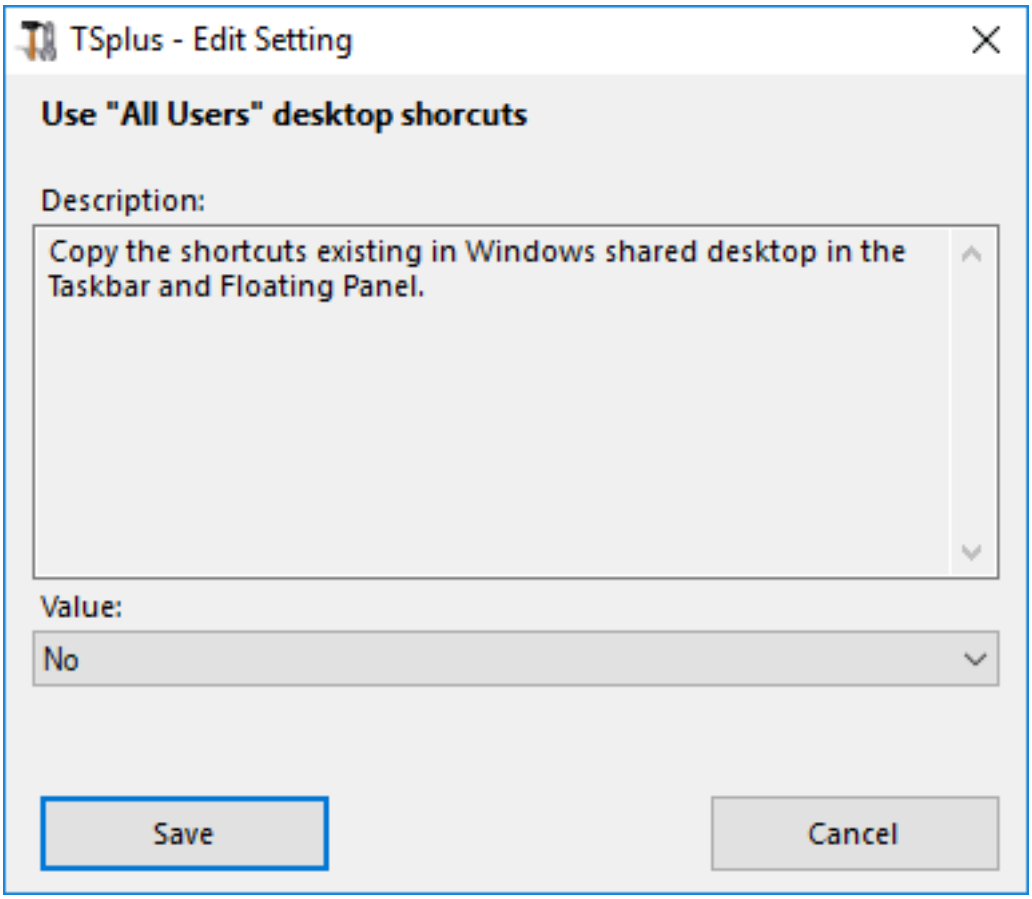
Background color

Customize the user sessions background color using a COLORREF code (for example, the default one is: 10841658).



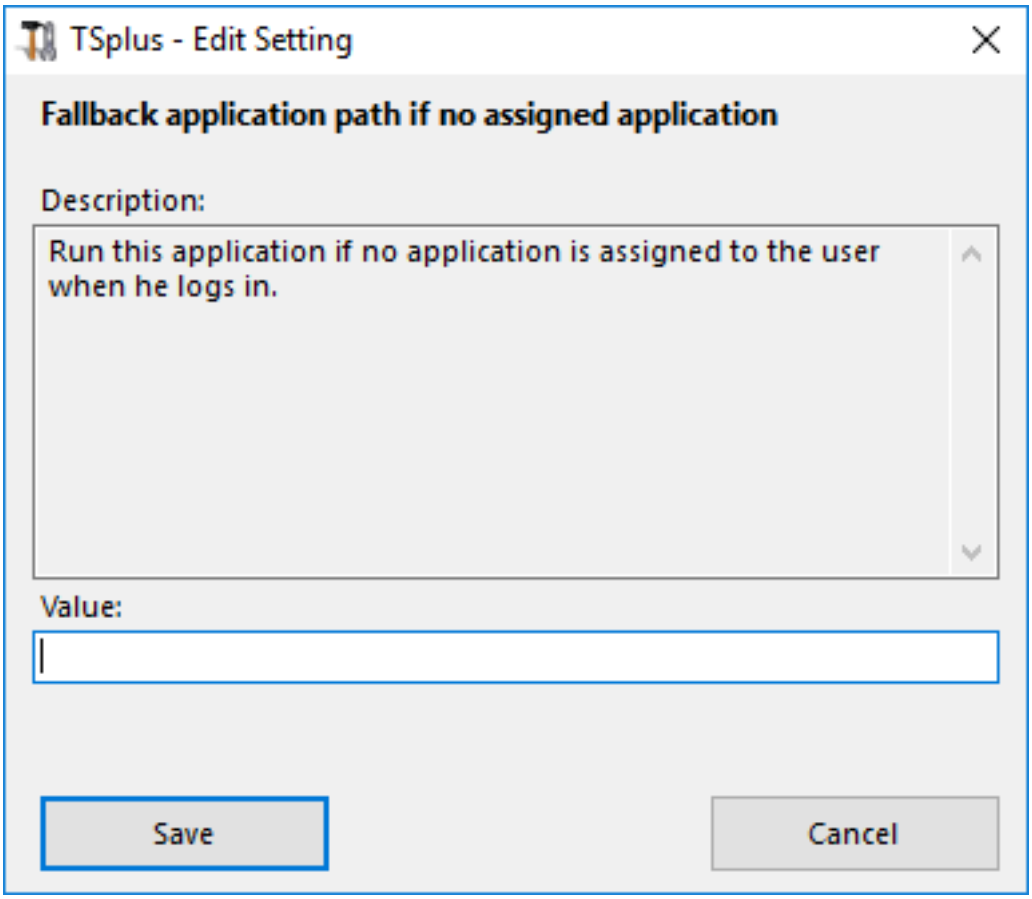
Use “All Users” desktop shortcuts

Copy the shortcuts existing in Windows shared desktop in the Taskbar and Floating Panel. Enable this feature by selecting the “Yes” value on this window, then click on save:



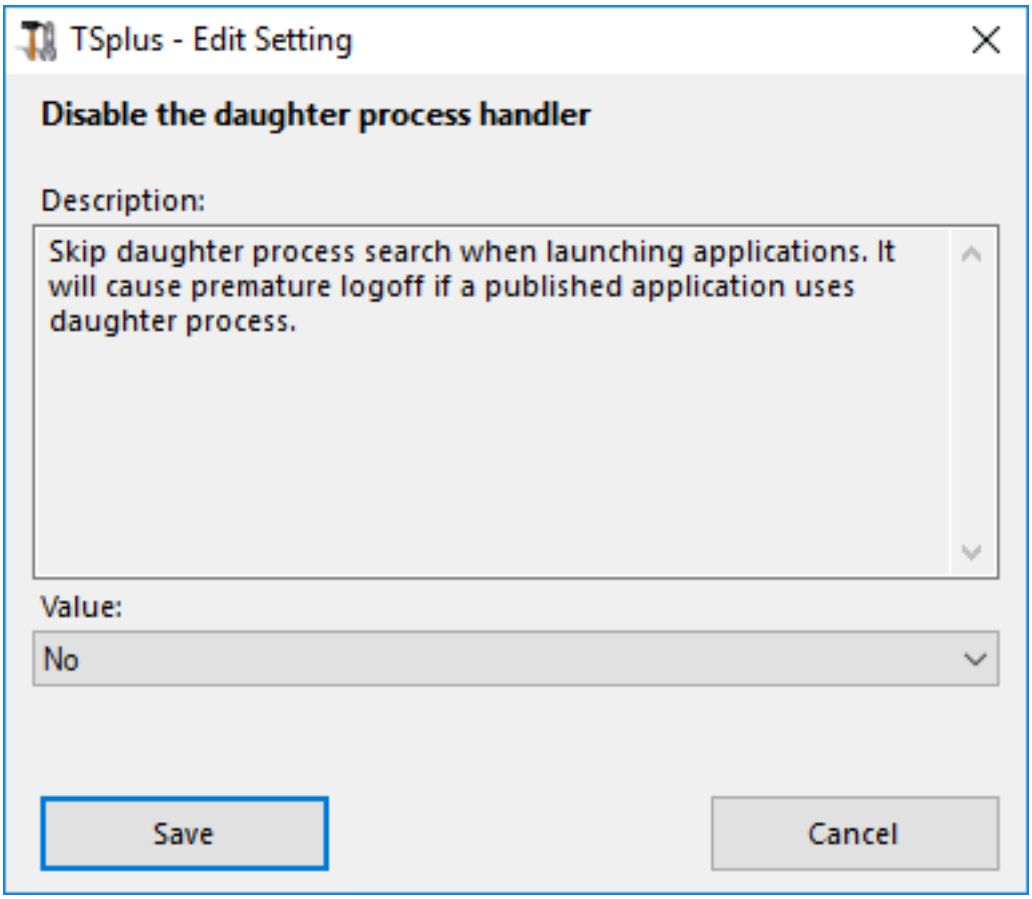
Fallback application path if no assigned application

Run this application if no application is assigned to the user when he logs in. There is no value by default. Enable this feature by entering a “Yes” value on this window, then click on save:



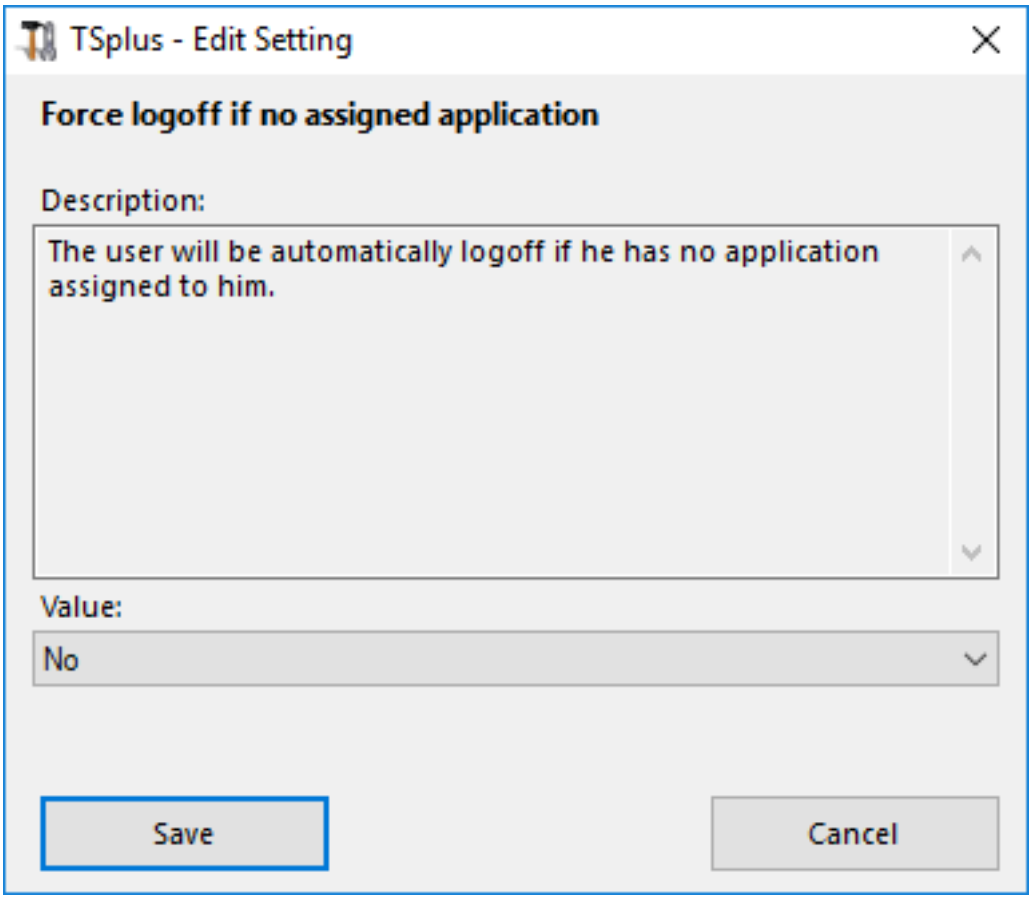
Disable the daughter process handler

Skip daughter process search when launching applications. It will cause premature logoff if a published application uses daughter process. This feature is disabled by default. Enable this feature by selecting the “Yes” value on this window, then click on save:



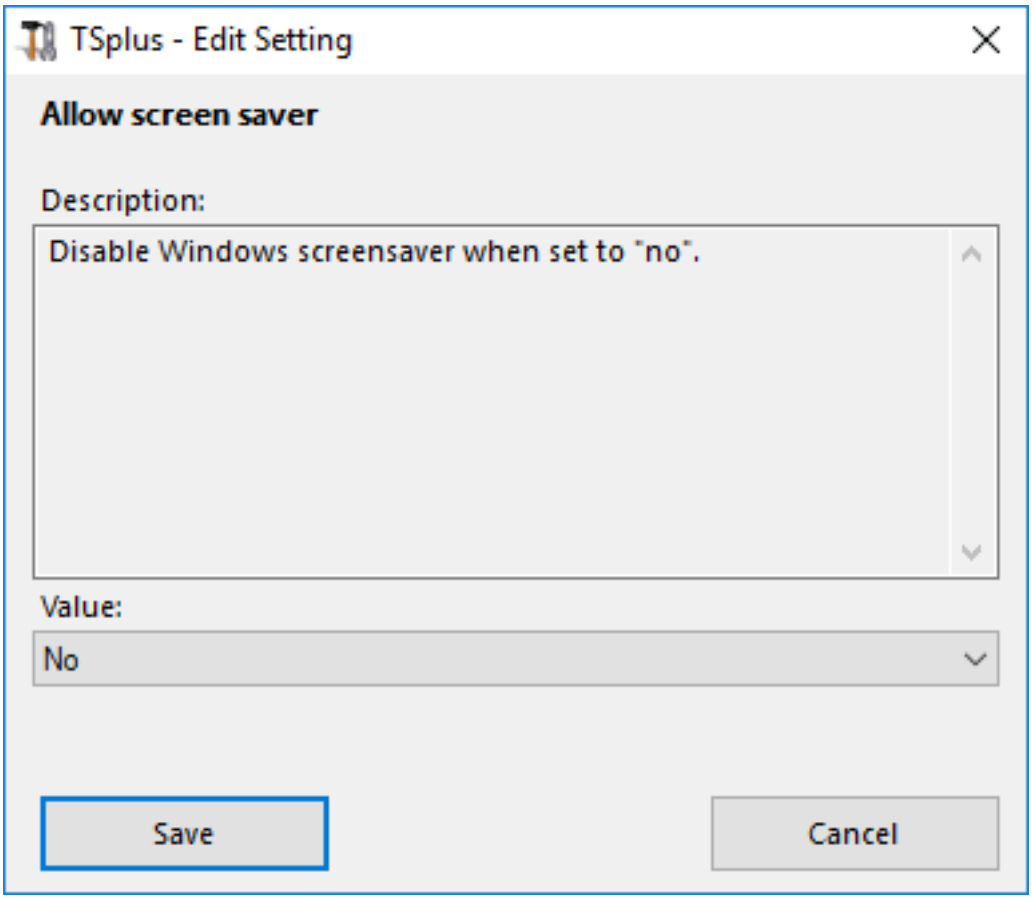
Force logoff if no assigned application

The user will be automatically logoff if he has no application assigned to him. This feature is disabled by default. Enable this feature by selecting the “Yes” value on this window, then click on save:



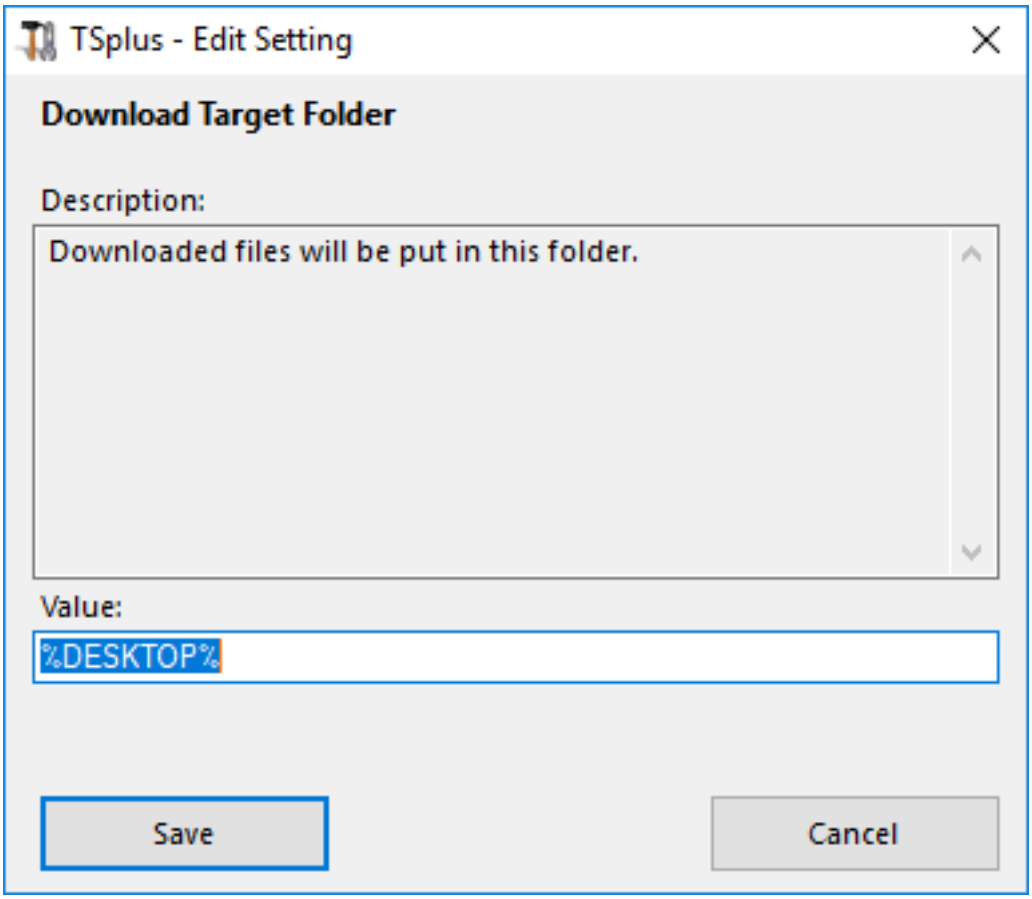
Allow screen saver

This feature is disabled by default. Enable Windows screensaver by selecting the “Yes” value on this window, then click on save:



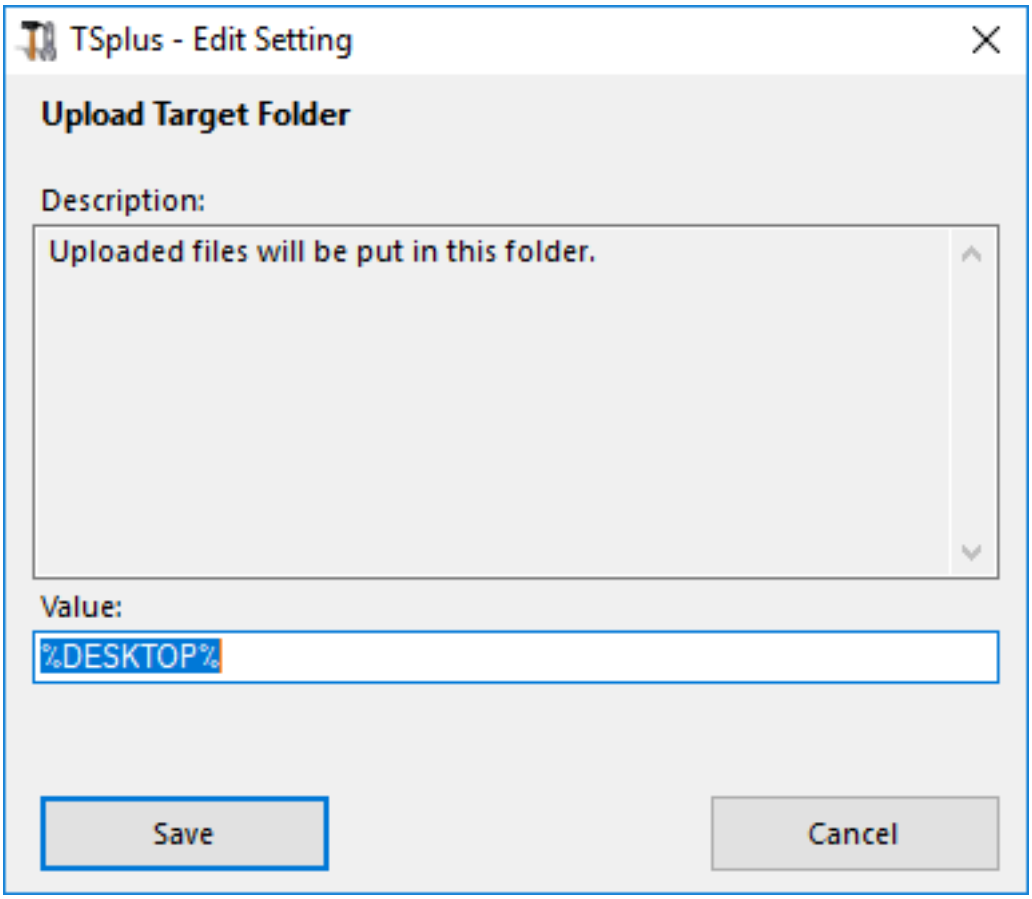
Download target folder

Downloaded files will be put on the Desktop by default. If you wish to modify it, enter the desired download folder’s path, then click on save:



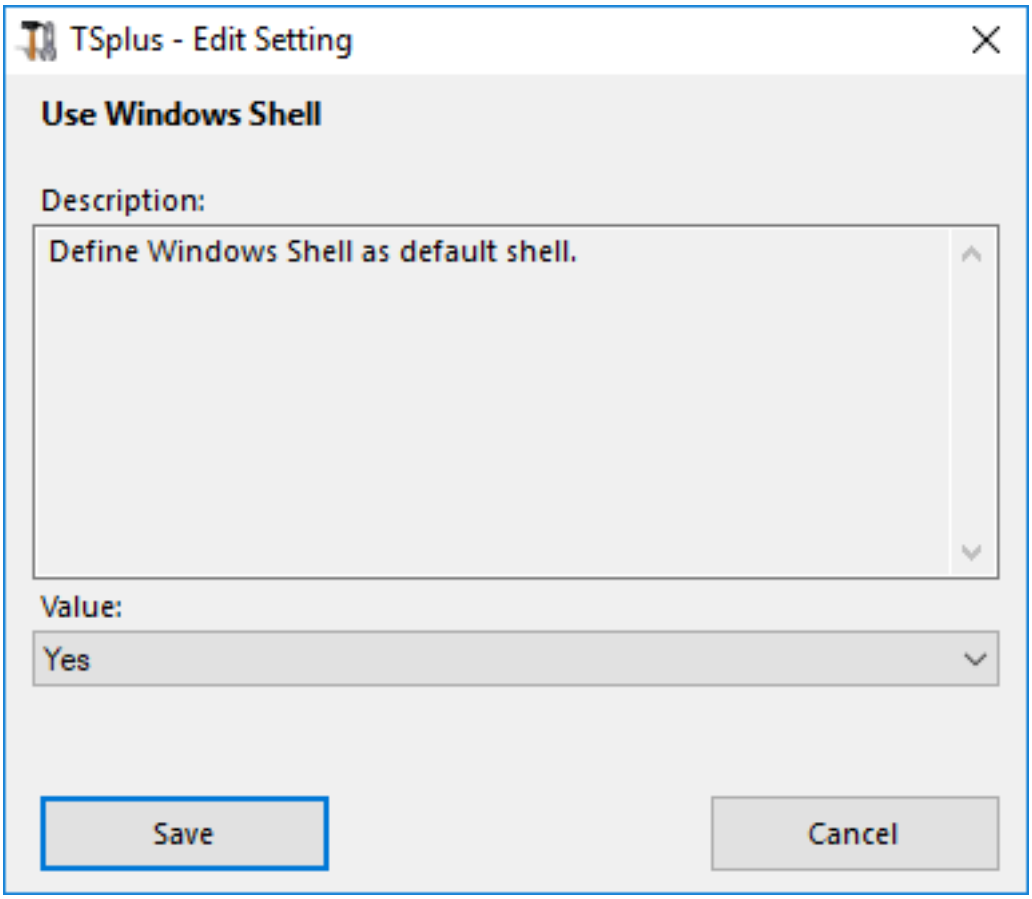
Upload target folder

Uploaded files will be put in this folder. If you wish to modify it, enter the desired upload folder’s path, then click on save:



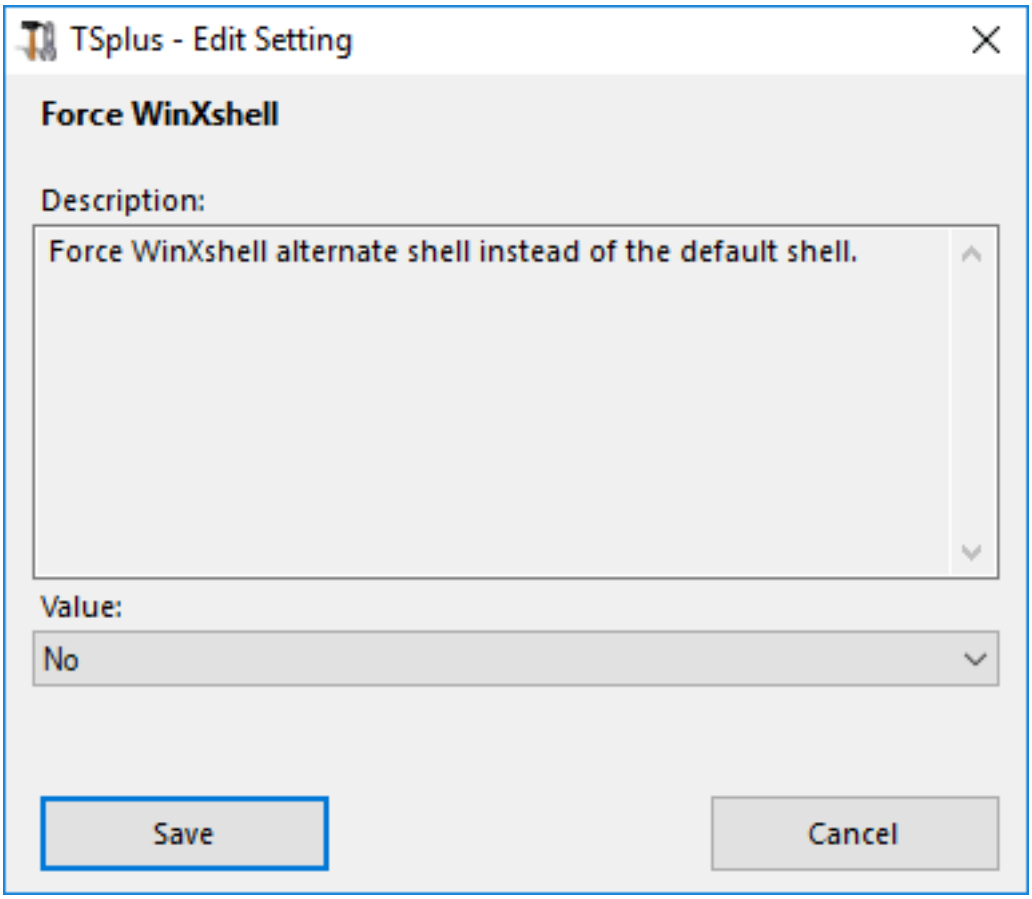
Use Windows Shell

Define Windows Shell as default shell. This feature is enabled by default. If you wish to disable it, select the “No” value on this window, then click on save:



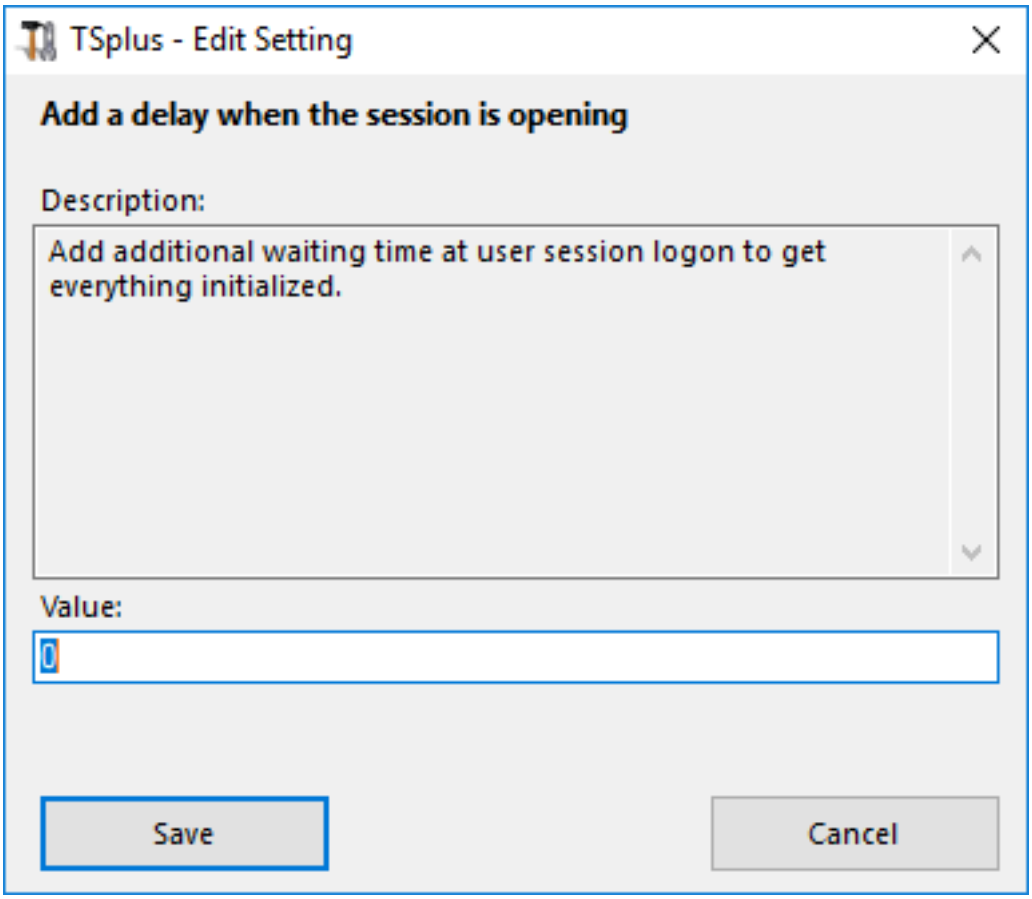
Force WinXshell

This feature is disabled by default. Force WinXshell alternate shell instead of the default shell by selecting the “Yes” value on this window, then click on save:



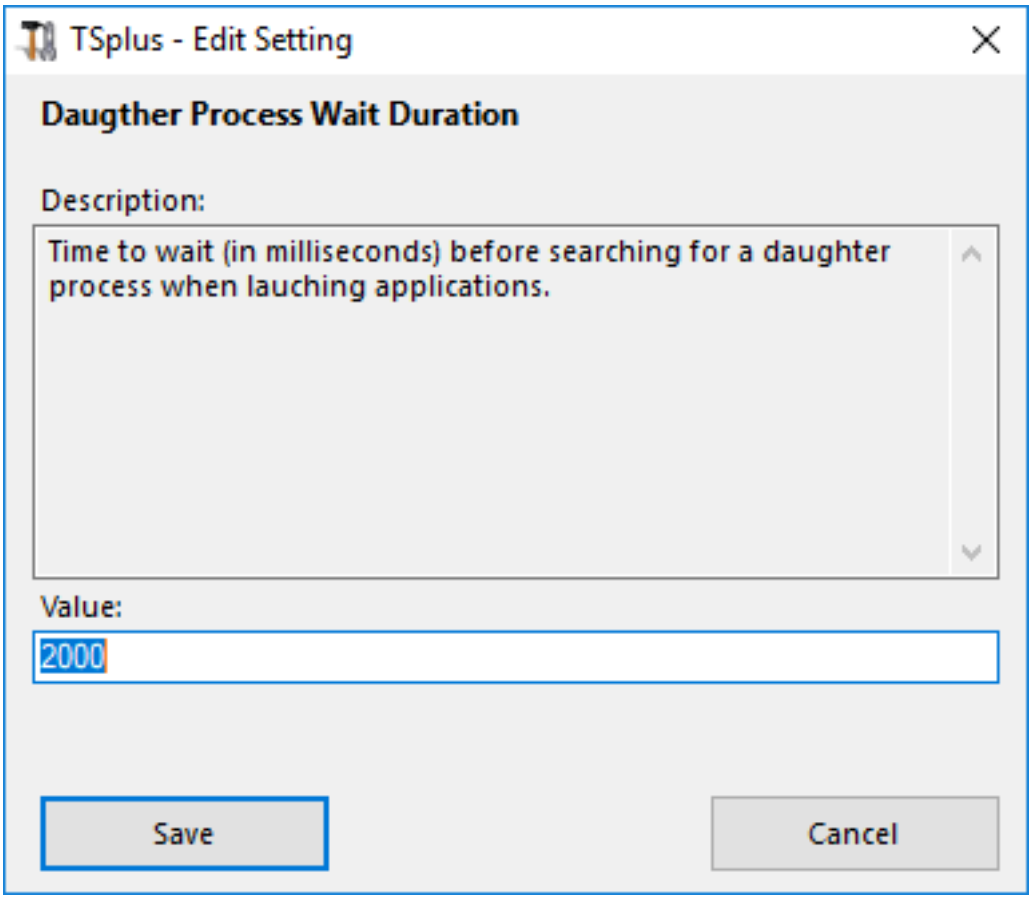
Add a delay when the session is opening

Add additional waiting time at user session logon to get everything initialized. Default value is 0. If you wish to modify it, enter the desired value (in seconds), then click on save:



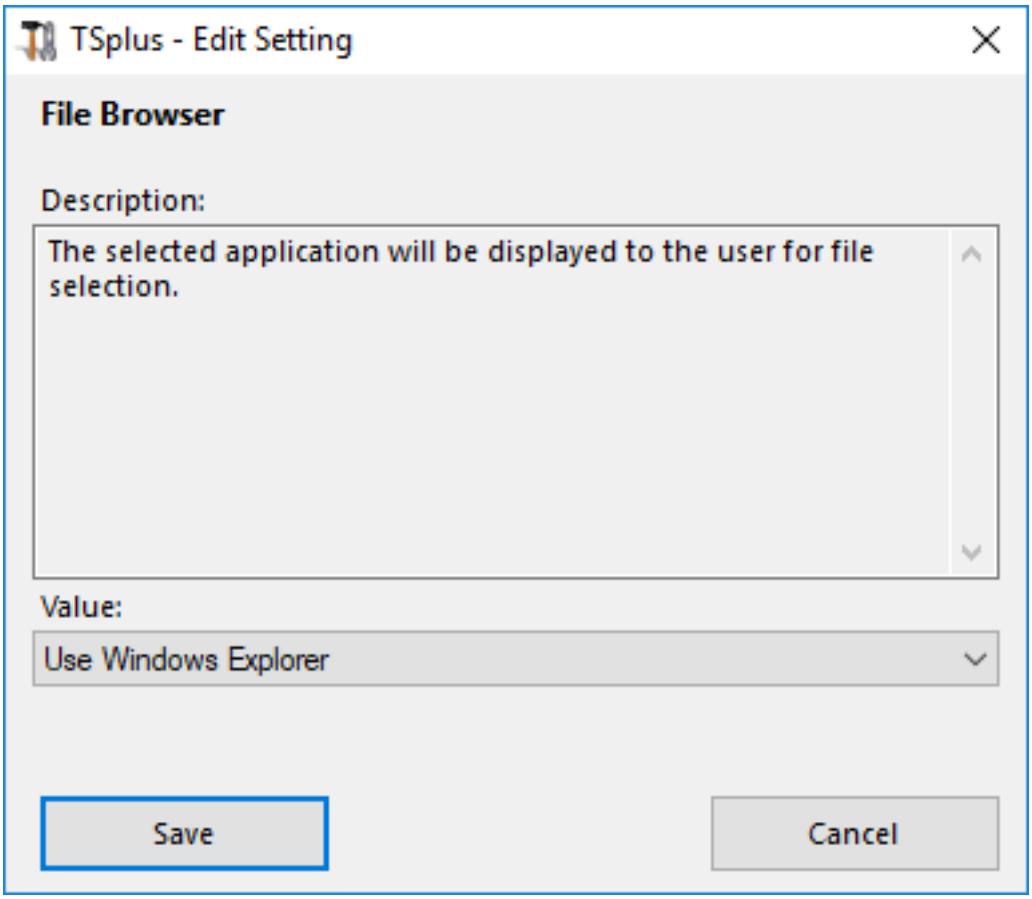
Daughter process wait duration

Time to wait (in milliseconds) before searching for a daughter process when lauching applications.



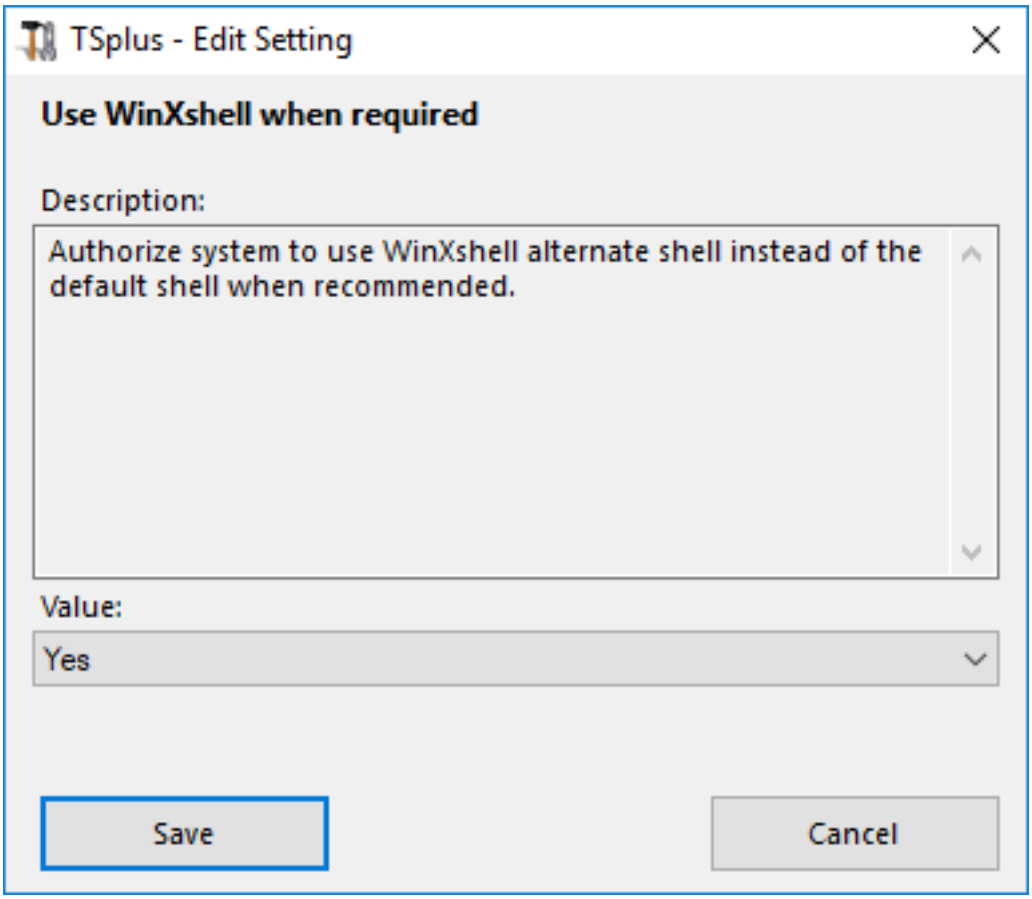
File browser

The selected application will be displayed to the user for file selection. Default browser is Windows Explorer. You can use the TSplus file browser by selecting it, then click on save:



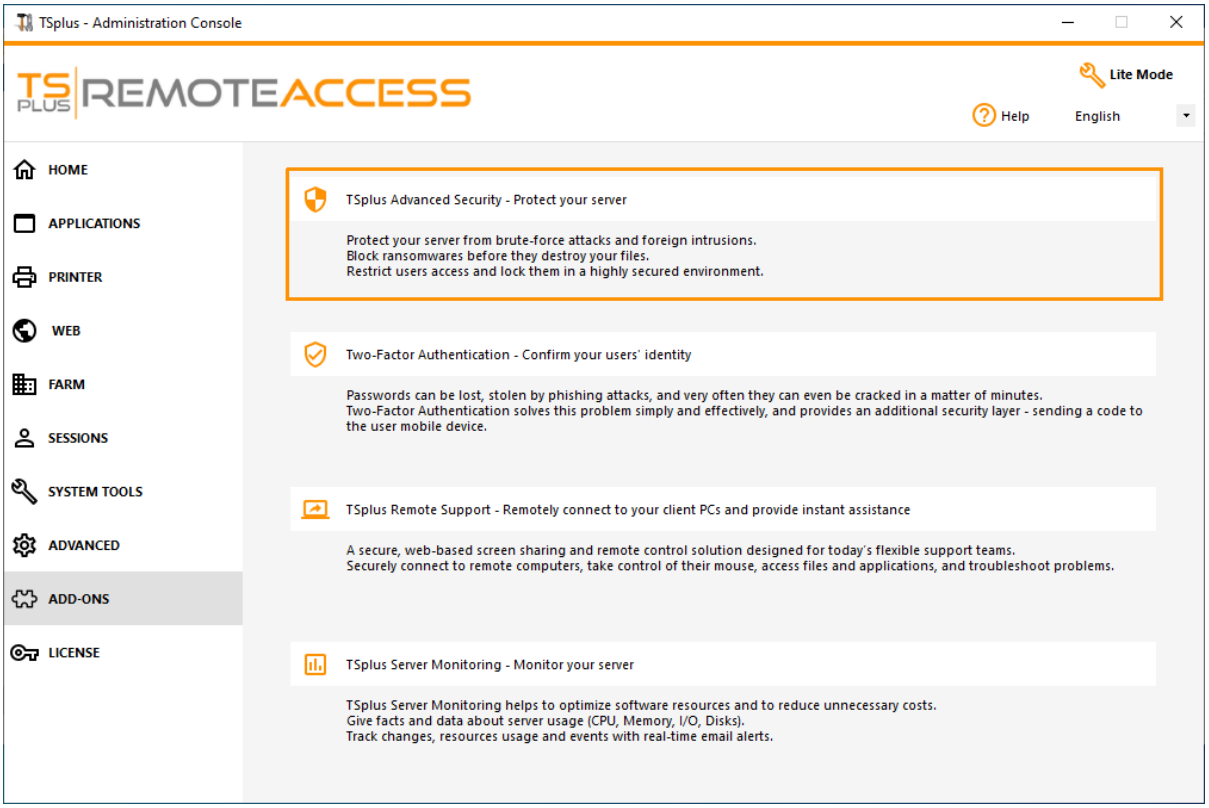
Use WinXshell when required

Authorize system to use WinXshell alternate shell instead of the default shell when recommended. This feature is enabled by default. If you wish to disable it, select the “No” value on this window, then click on save:


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 is available as an Add-On from TSplus AdminTool and is available on the Add-Ons tab:

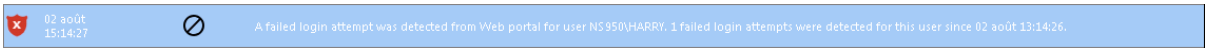


You can find its full documentation on this page.

Lockout Event

TSplus Lockout monitors failed Web Login attempts on your TSplus server.

TSplus Advanced Security will show a Lockout Event, after any Web Portal failed attempt like the example below:



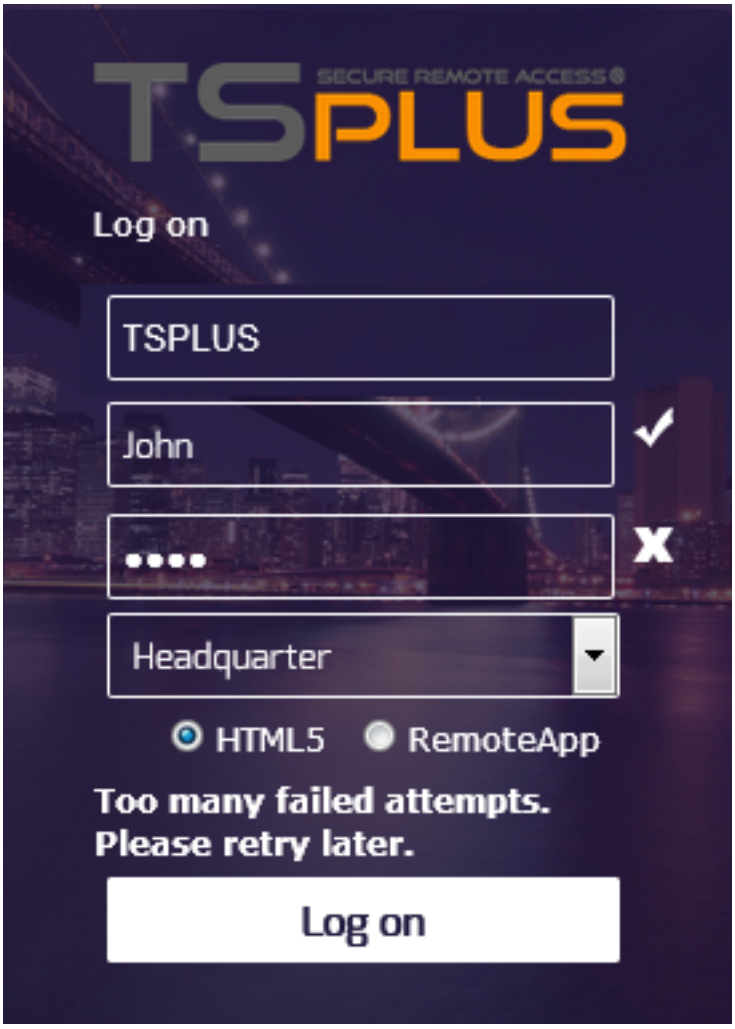
“A failed login attempt was detected from Web Portal for user … 1 Failed login attempt were detected for this user since…”

The Bruteforce Protection enables you to protect your public server from hackers, network scanners and brute-force robots that try to guess your Administrator login and password. Using current logins and password dictionaries, they will automatically try to login to your server hundreds to thousands times every minute. Learn more about this feature on this page.

On the Web Portal

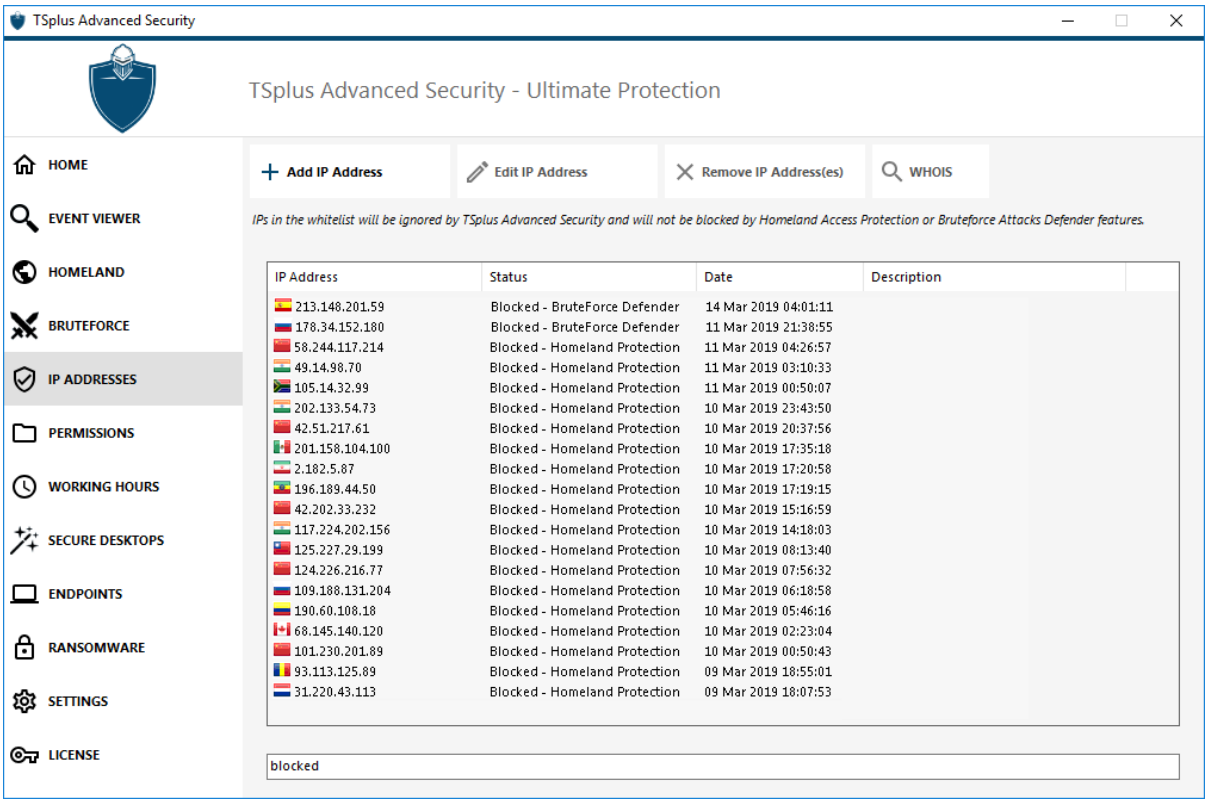
Brute-force attacks on the Web Portal are blocked when users enter wrong credentials.

After 10 attempts during a period of 10 minutes, the Web Portal will prohibit the user to logon for 20 minutes:



These are the default settings which are customizable on the BruteForce Protection tab of TSplus Advanced Security AdminTool.

You can check all blocked connections and logs on the IP Addresses tile of TSplus Advanced Security Ultimate Protection:



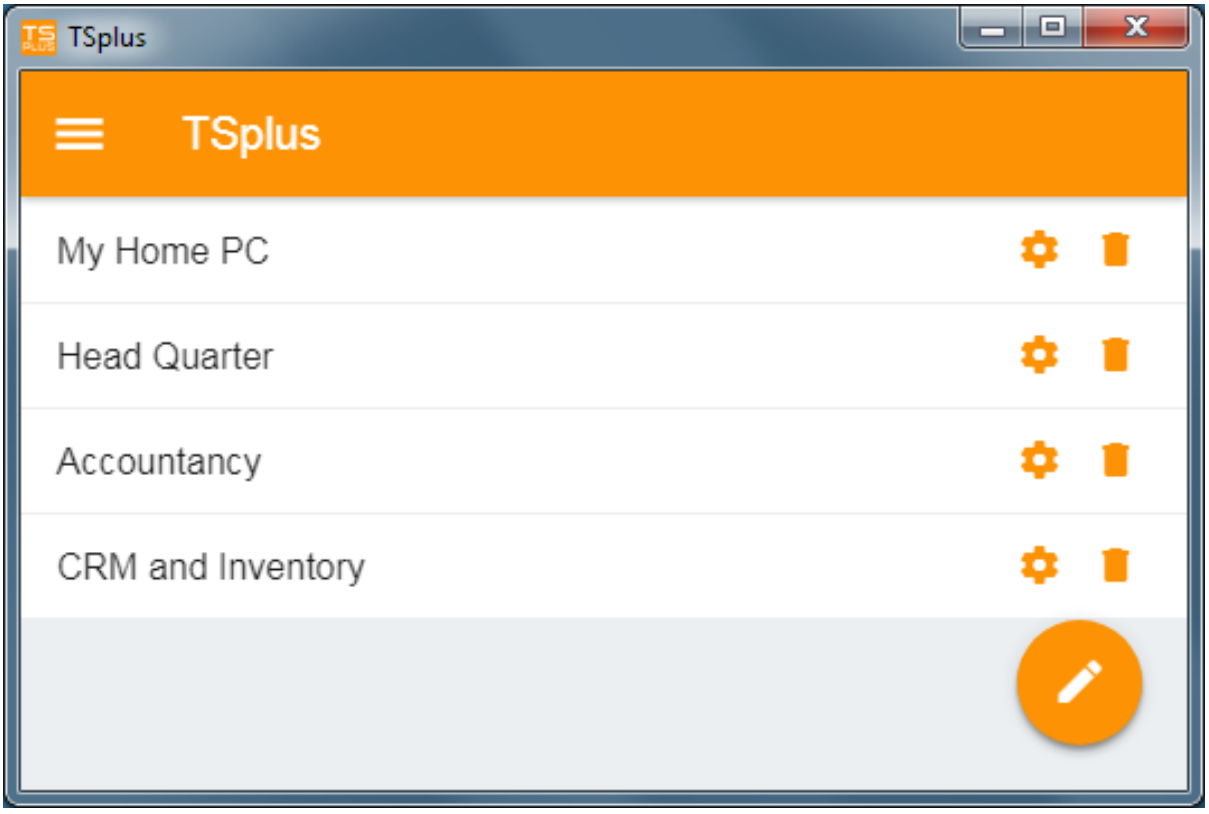
This functionality is visible and active after the first Web Portal connection.

The complete TSplus Advanced Security documentation is available on this page.

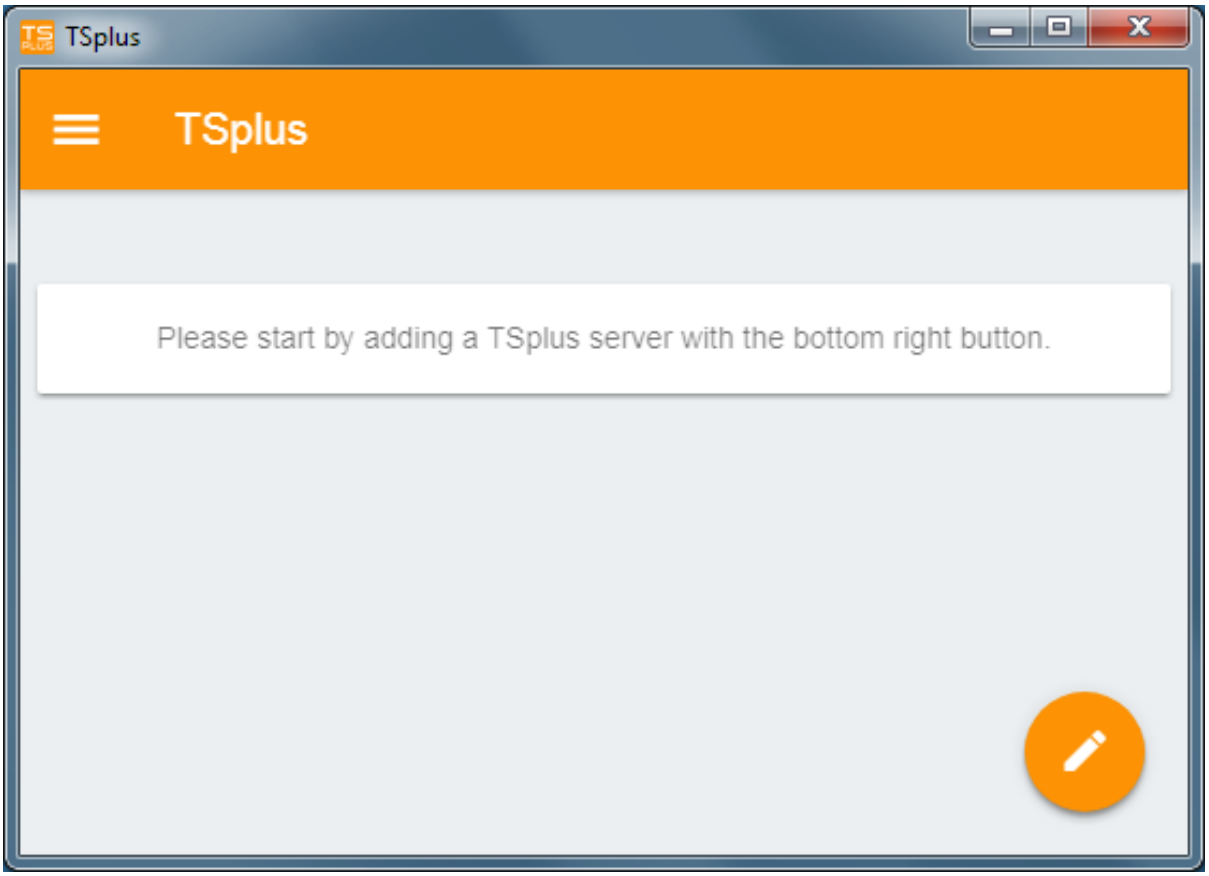
TSplus App Configuration

Manage your servers

The user interface and configuration are simple and intuitive.



First, add a TSplus server by clicking on the bottom right button:

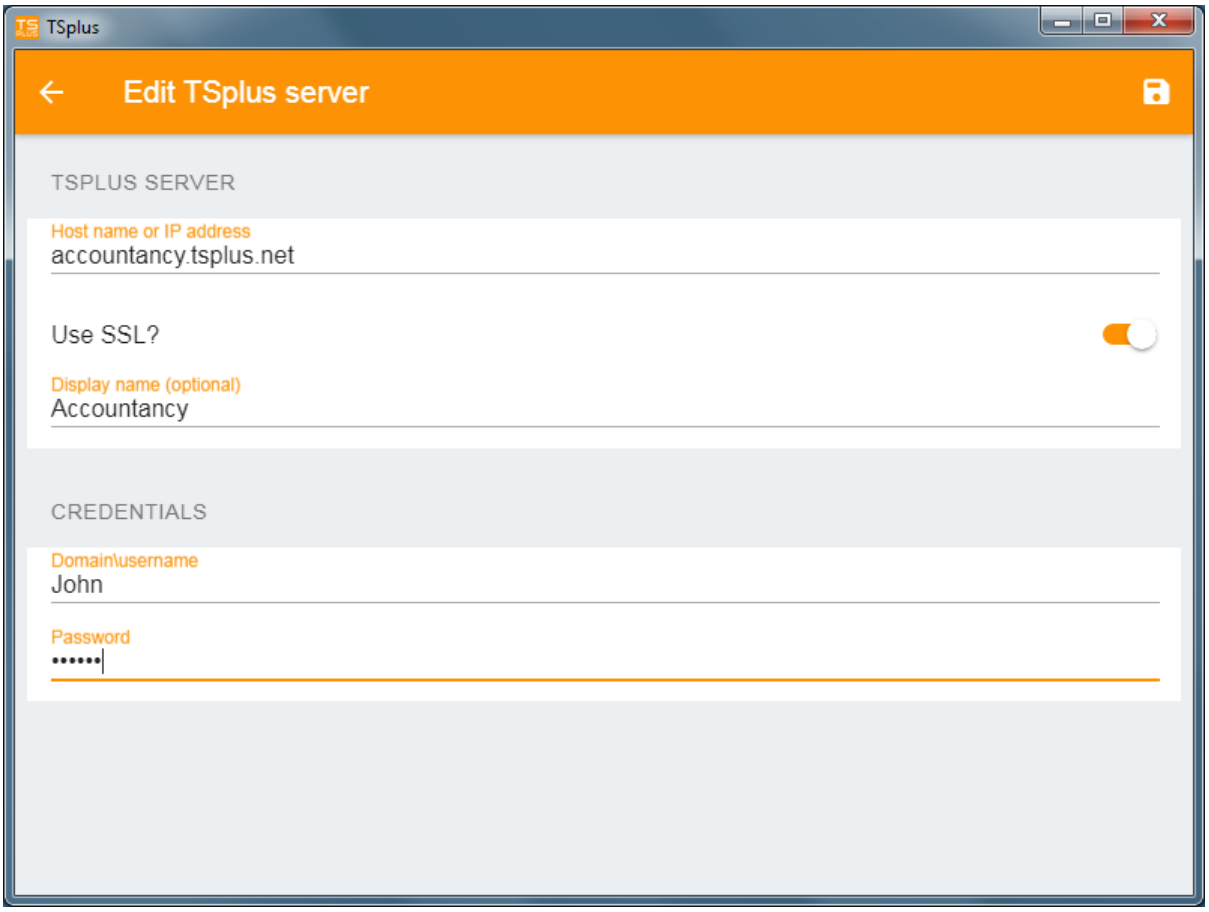


Then, add your server information and configure it:

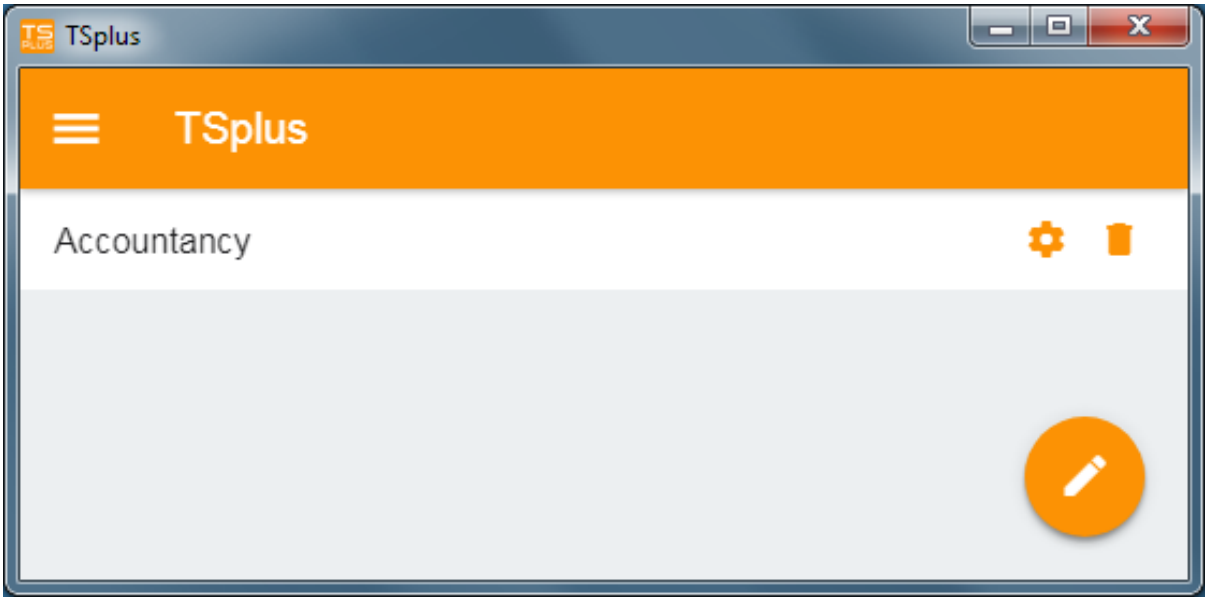
- Enter its its host name or IP address.
- SSL is disabled by default, but you can choose to enable it.

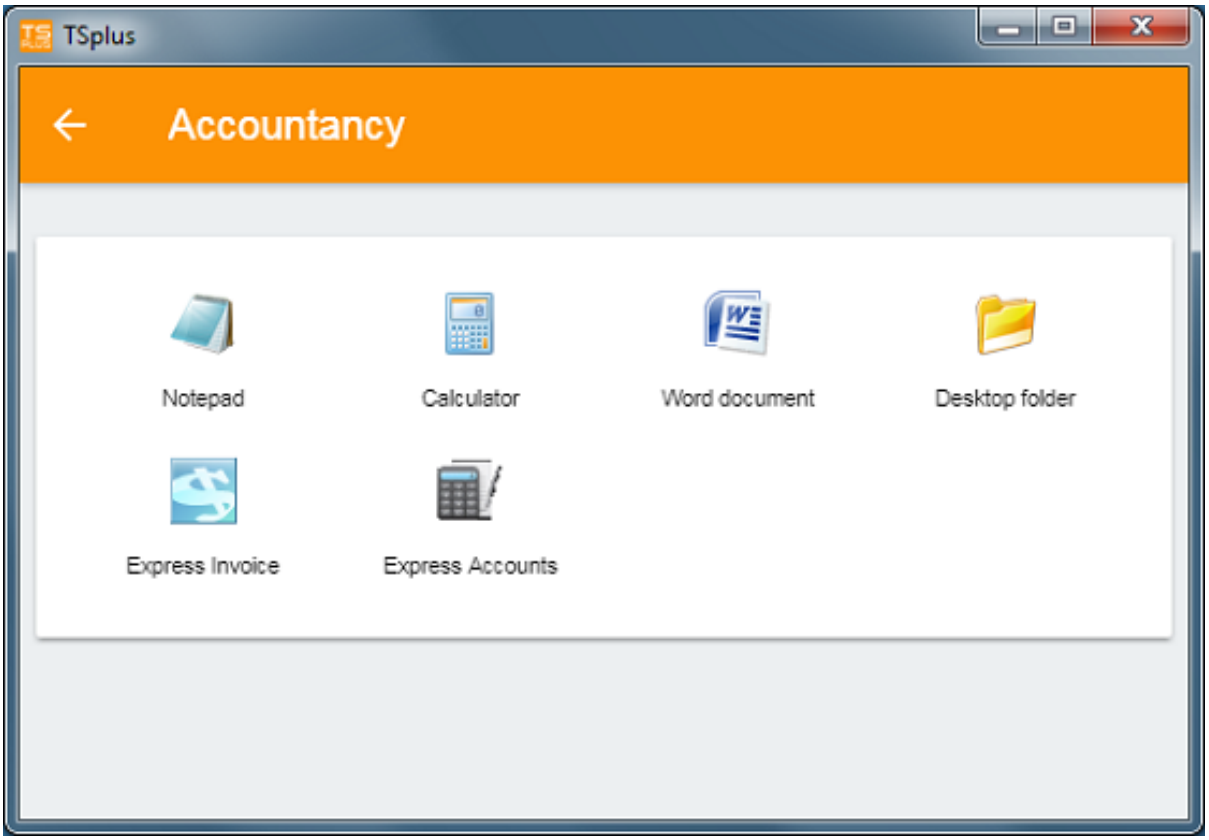
Warning: SSL Activation only works if you installed a valid SSL Certificate on your TSplus server. See this documentation for more information.

- Enter its display name, which is optional.
- Enter your user's credentials with the domain or user name and its password.
- If you are using the HTTPS protocol, you must enter the port in the configured address. For example: appportal.mydomain.com:443



Then click on the top right button to save. You can now click on your server to access your applications:





Printing

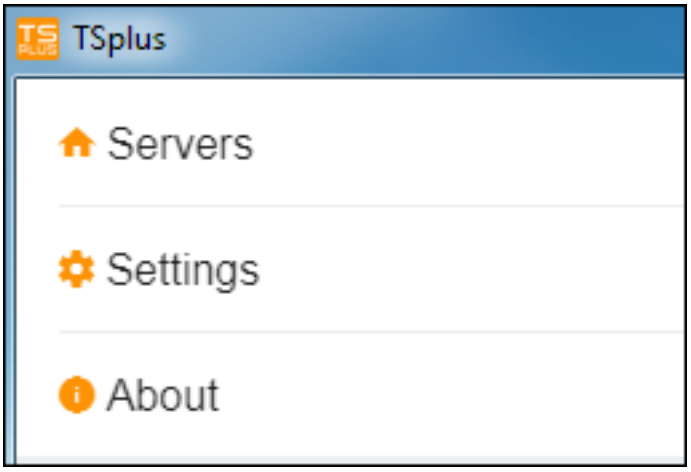
Easily print on your local printer by using the Universal Printer.

Since TSplus App 11.40 version, printed documents open with the default PDF reader app.

Settings and Version

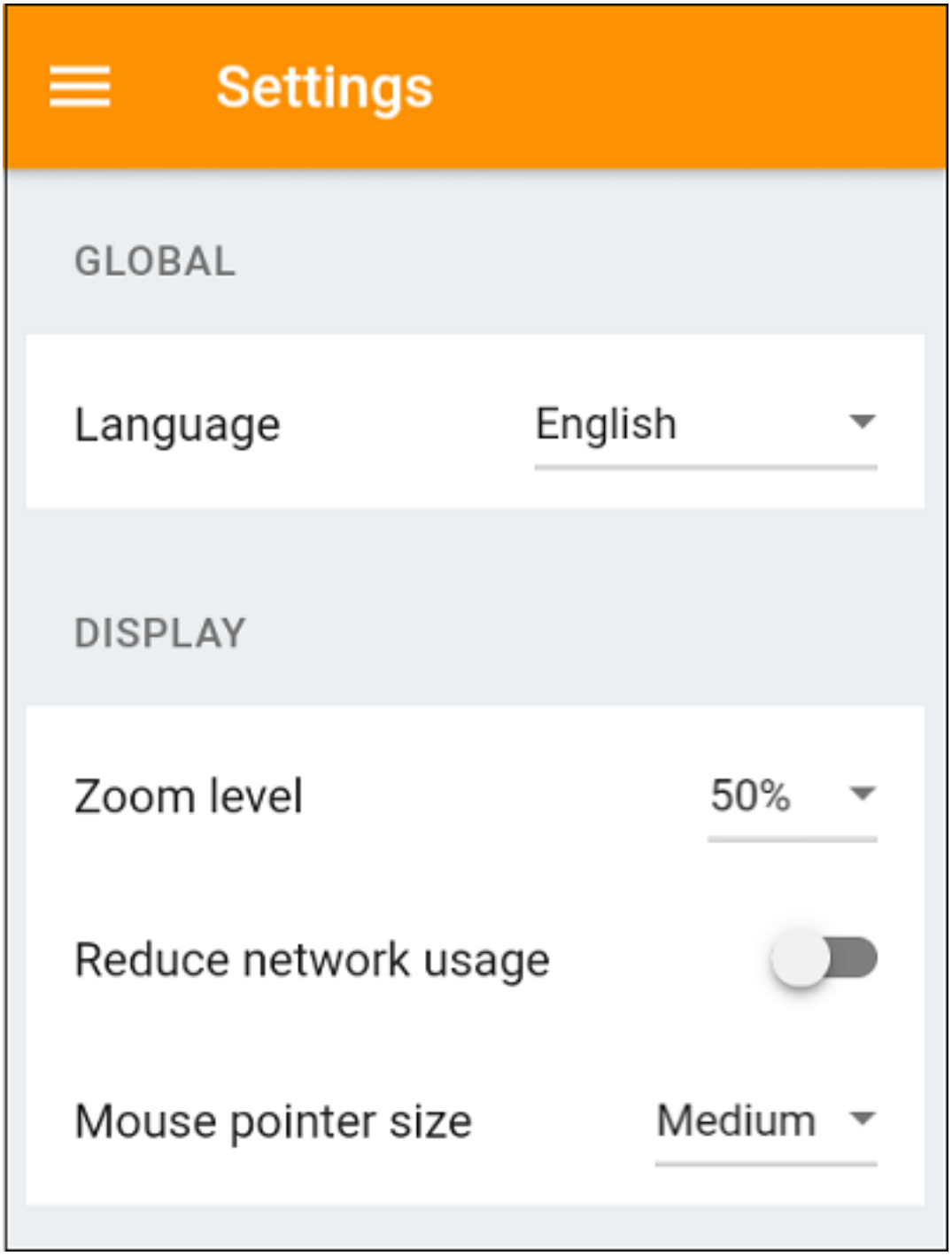
Under the top left menu, you can:

- Manage your servers
- Manage your settings
- See the legal information on the About section, and your TSplus App version.



Settings

Various settings are available on the Settings window:



- You can change the language.
- Modify the display settings by changing the zoom level at your convenience, reduce network usage or choose between 3 mouse pointer sizes: small, medium or large.

2FA Authentication

The Android app is compatible with 2FA.

The app asks for the 2FA code if the user account has been configured to use 2FA.

Activation cannot be done from the mobile app, you must first configure 2FA from the web portal first.

Version

On the About tab, you can see the legal information as well as your current TSplus App version :



TSplus App

The TSplus App allows you to connect to your TSplus server from any device, anywhere!

Just like TSplus, it provides fast and stable remote connections from tablets and smartphones to Windows desktops and business applications.

Access your applications and business data in real time and easily print any document and photo you need on the nearest local printer.

The TSplus App is compatible with 2FA.



For more information and download links, go to the App page on our website.

Hardware Requirements and Operating Systems

The TSplus App is available on mobiles and tablets with the following OSs: iOS, Android from 4.4 version and Linux.

Android version

iOS version

Pre-requisites

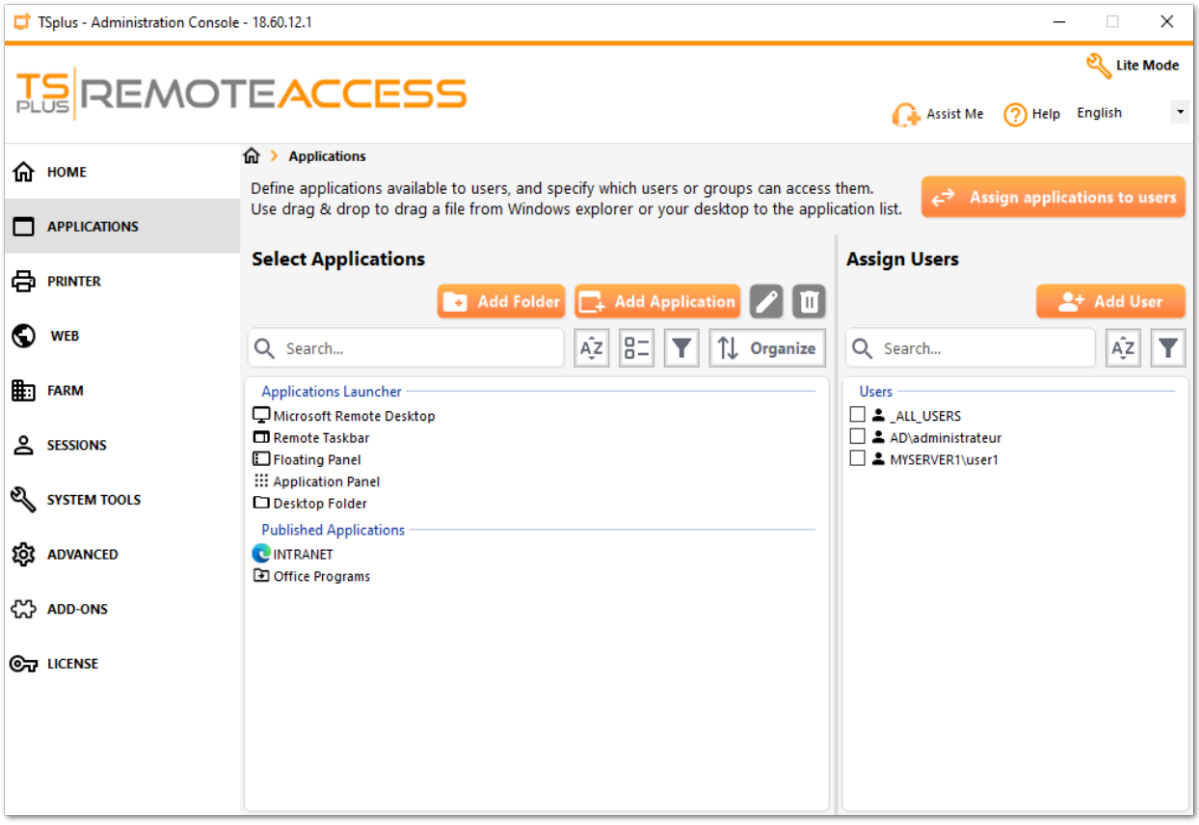
- The host site must be a TSplus Mobile Web or Enterprise system.
- The 11.30 release (and over) must be installed on this host.

Assigning Applications to Users or Groups

Once you have published some applications, you can assign them to one or more users and/or groups.

Assign users or groups to applications

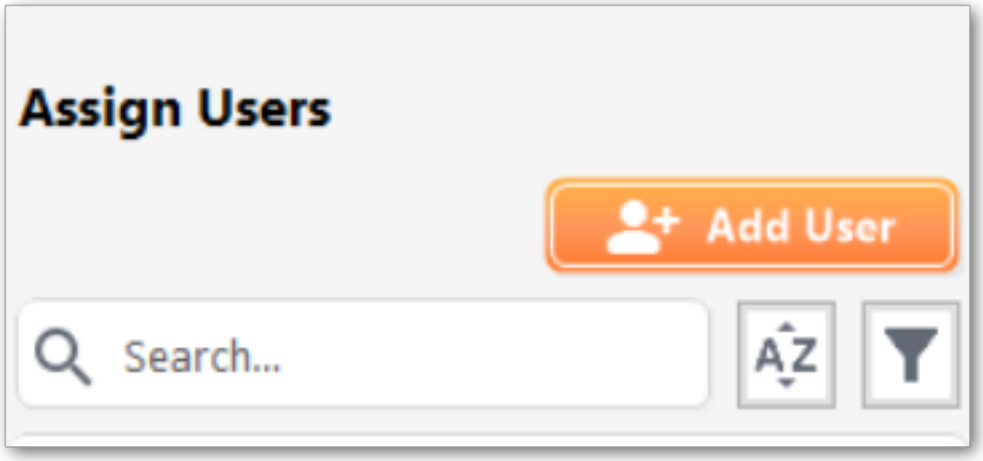
Every assignment are to be done in the right side panel of the “Applications” section of the AdminTool. This right side panel shows every users and groups currently having applications assigned.



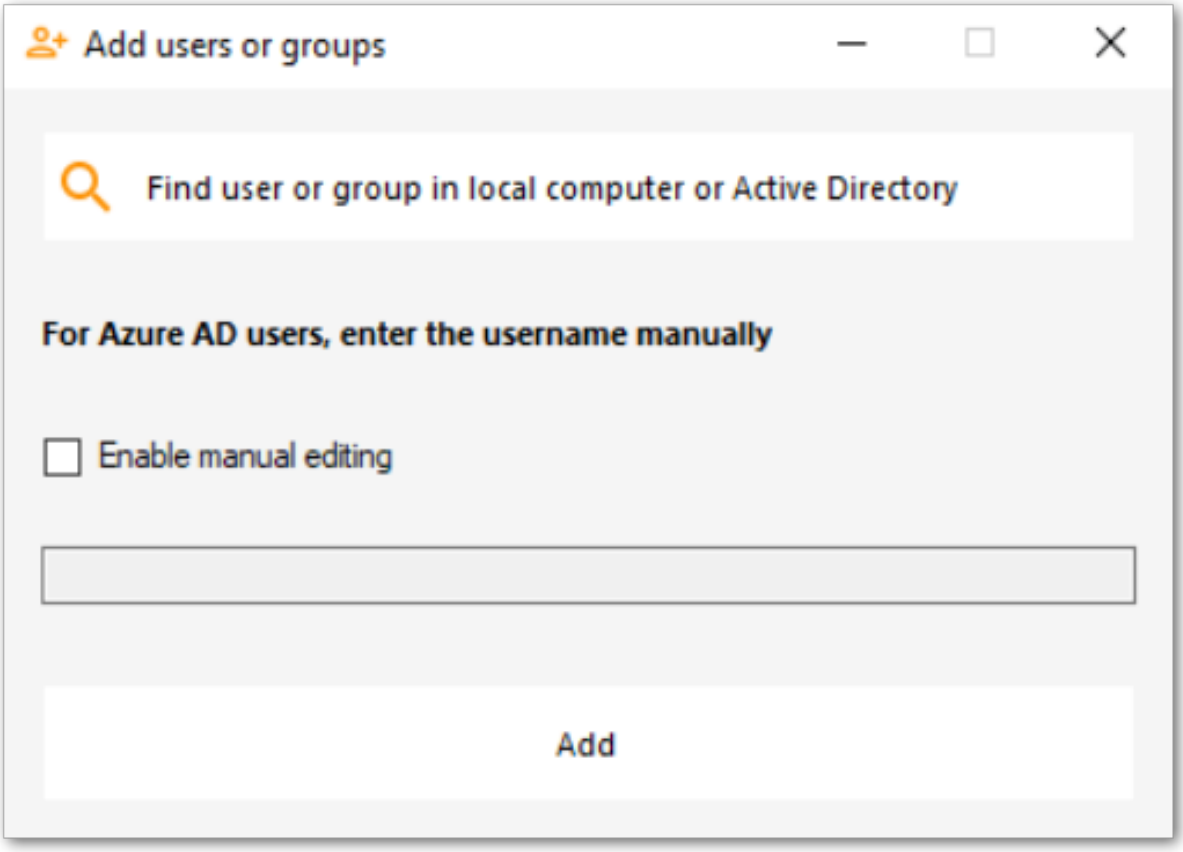
In order to assign users or groups, you will need first to add the users/groups you want to assign application for.

Add users or groups

To add users or groups, click on the “Add user” icon buttons



You will be greeted with this interface, allowing you to either find a user or group via the user/group picker, or directly write the name of the user/group you want to add.
Local or Active Directory users must be selected using the Find Local or Active Directory Users or Groups button.
Only external users can be entered directly into the text box.



The _ALL_USERS special username

In the list of users, you will always find available the “_ALL_USERS” user. This user is not a Windows user, but a virtual user. If you select an application and tick the “_ALL_USERS” username, then the application will be available to every users.

Assign users or groups to applications

Once users have been added, assign them applications by:

1. selecting on the left panel the applications you want to assign to your user
2. checking on the right panel the box next to his username to assign the selected applications to that user

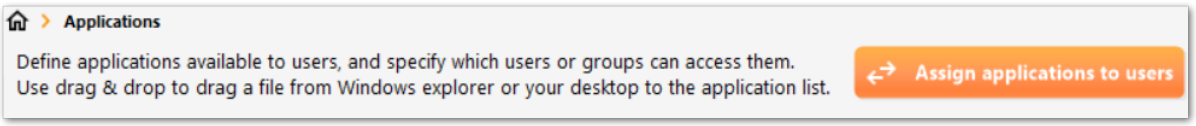
Ex: if I want to assign notepad to the user “benjamin”, simply select the “notepad” application on the left, and check the box next to the username “benjamin” on the right

To unassign users, simply uncheck the box next to the user name.

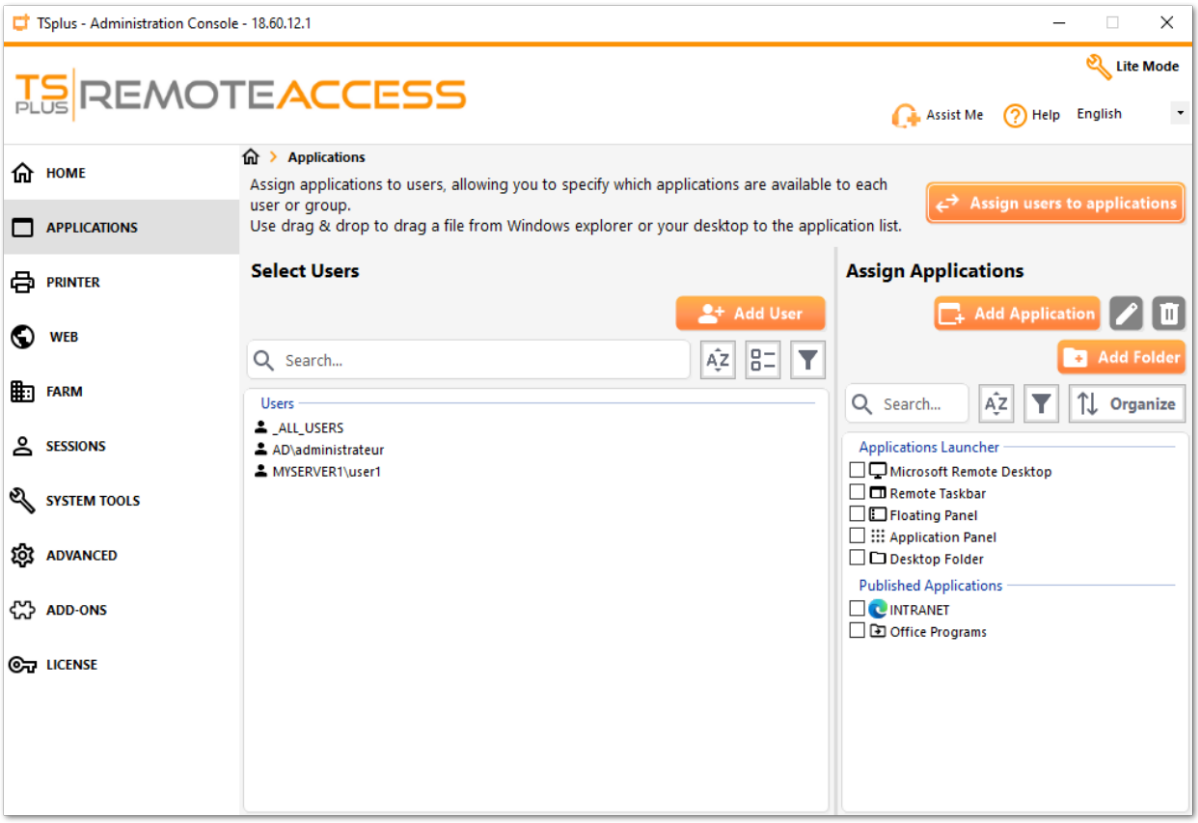
This action supports multi selection
This means you can select multiple applications, and don’t have to assign application one at a time.

Assign applications to users or groups

If you would prefer to select users or groups and assign them applications, you can do so by clicking on “Assign applications to users”.



This will flip the left and right side panel.



After clicking on the button, in order to assign applications to users:

1. selecting on the left panel the users or groups you want to assign to your application
2. checking on the right panel the box next to your application name to assign the selected users or groups to that application

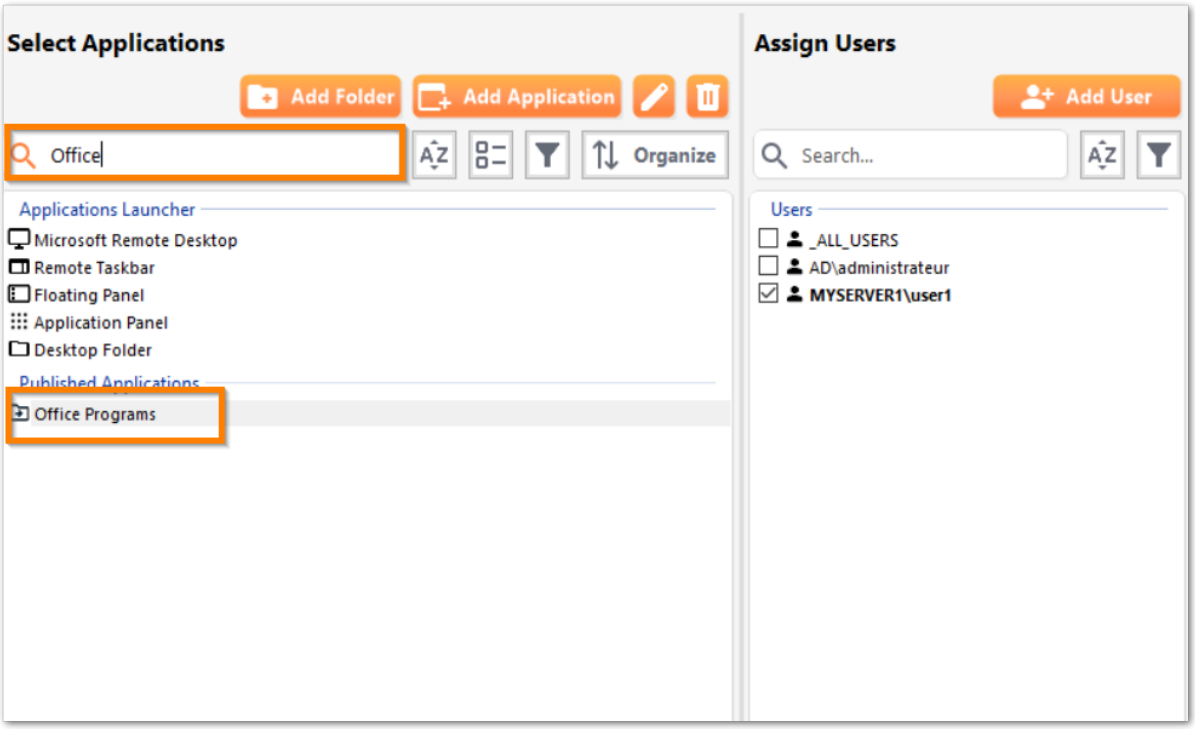
Ex: if I want to assign notepad to the user “benjamin”, simply select the user “benjamin” on the left, and check the box next to the application name “notepad” on the right

To unassign applications, simply uncheck the box next to the application name.

This action supports multi selection
This means you can select multiple users, and don’t have to assign users one at a time.

Search and filter

In order to ease users assignation management, a search bar is available as well as a filtering button, allowing you to show only users, or only groups.

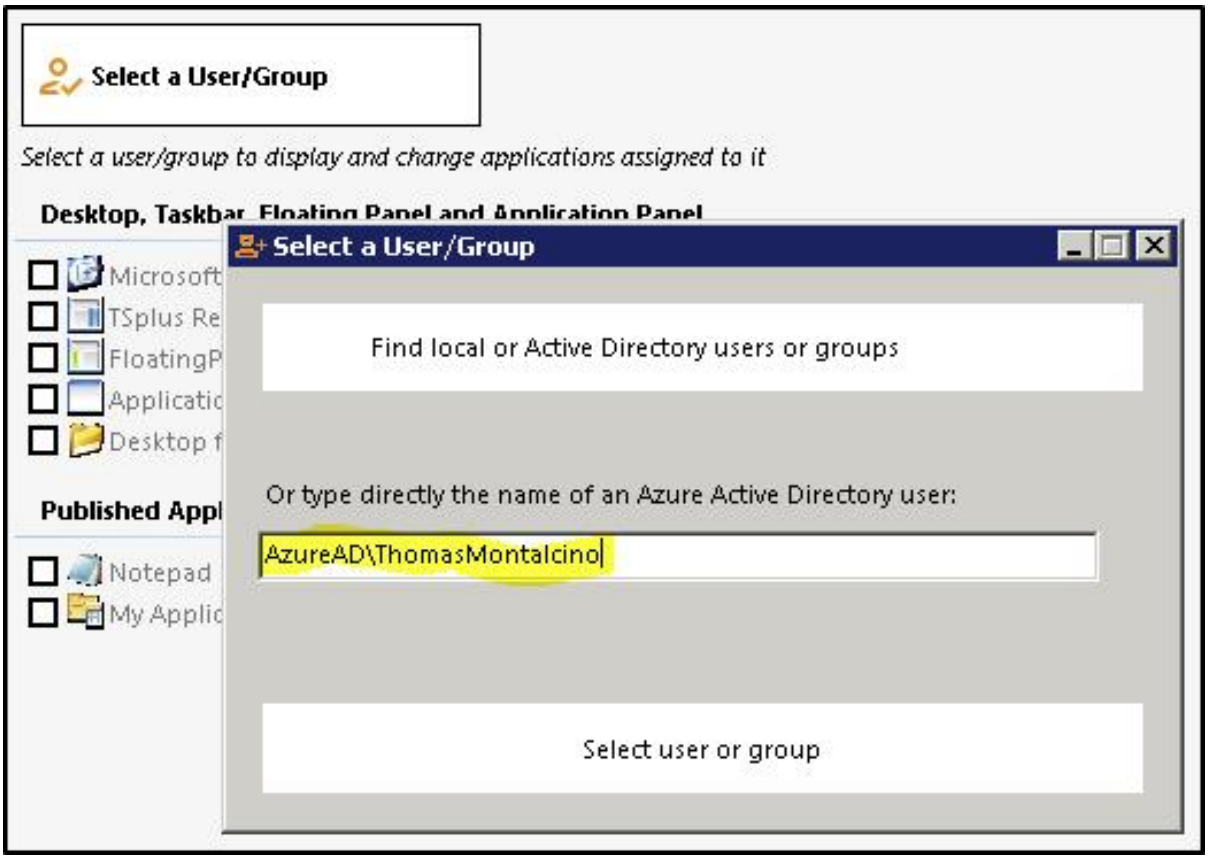


You can also use the filter button so that only assigned/unassigned applications (or assigned/unassigned users if you switch view) are shown.
This will help you manage your assignations in case you have either lots of users having applications assigned, or simply lots of published applications.

Assigning Applications to Users with Azure Active Directory

Overview

To assign an Azure Active Directory user to an application from the AdminTool > Applications > Users :



Local or Active Directory users must be selected using the Find Local or Active Directory Users or Groups button. Only external users can be entered directly into the text box.

Built-in Web Server Management

Your Remote Desktop Server must be available, easy-to-access and safe. That's why TSplus utilizes a built-in Web Server which helps you easily manage its status and operations.

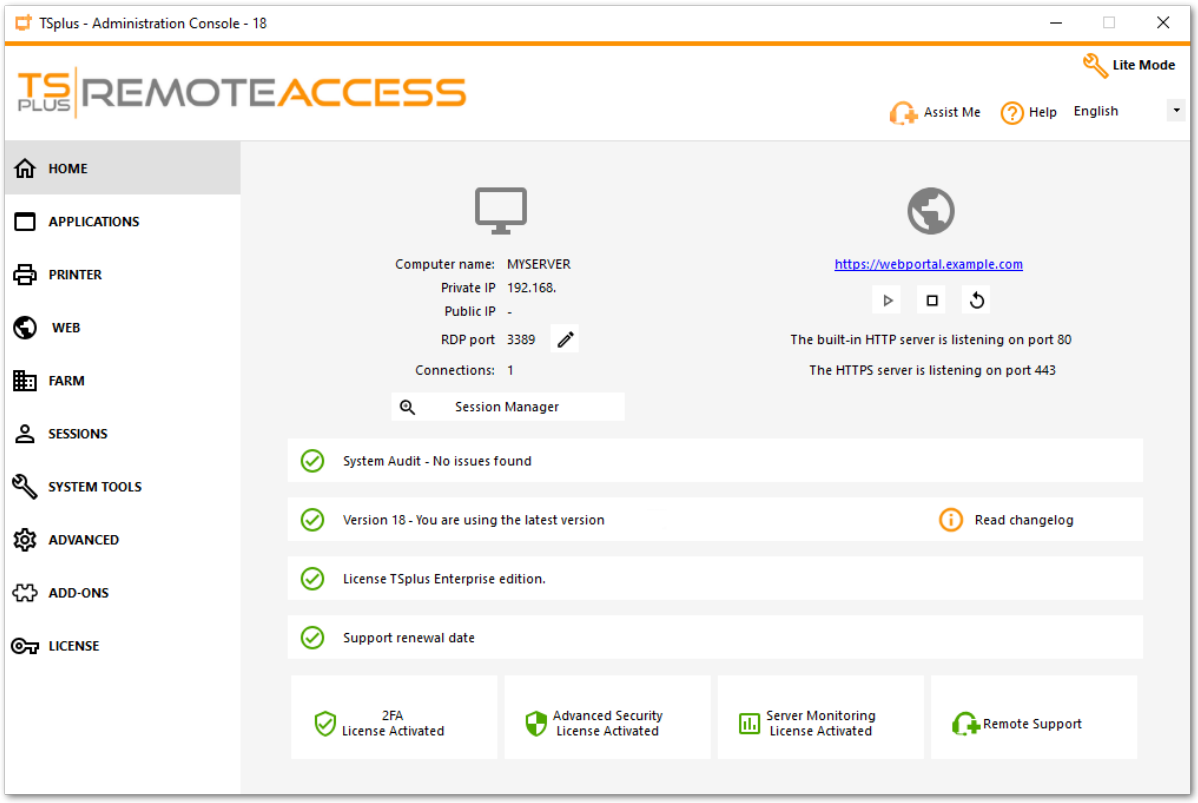
A Management Console is available in the Administrator Tool. This Management Console enables you to view and configure the status of Terminal Service Plus built-in Web Server.

When you install TSplus, web servers are listening on ports 80 and 443 by default. Make sure that the defined ports are available and that Java is installed on the server.

See the video about Web Features.

Web Server Components Status

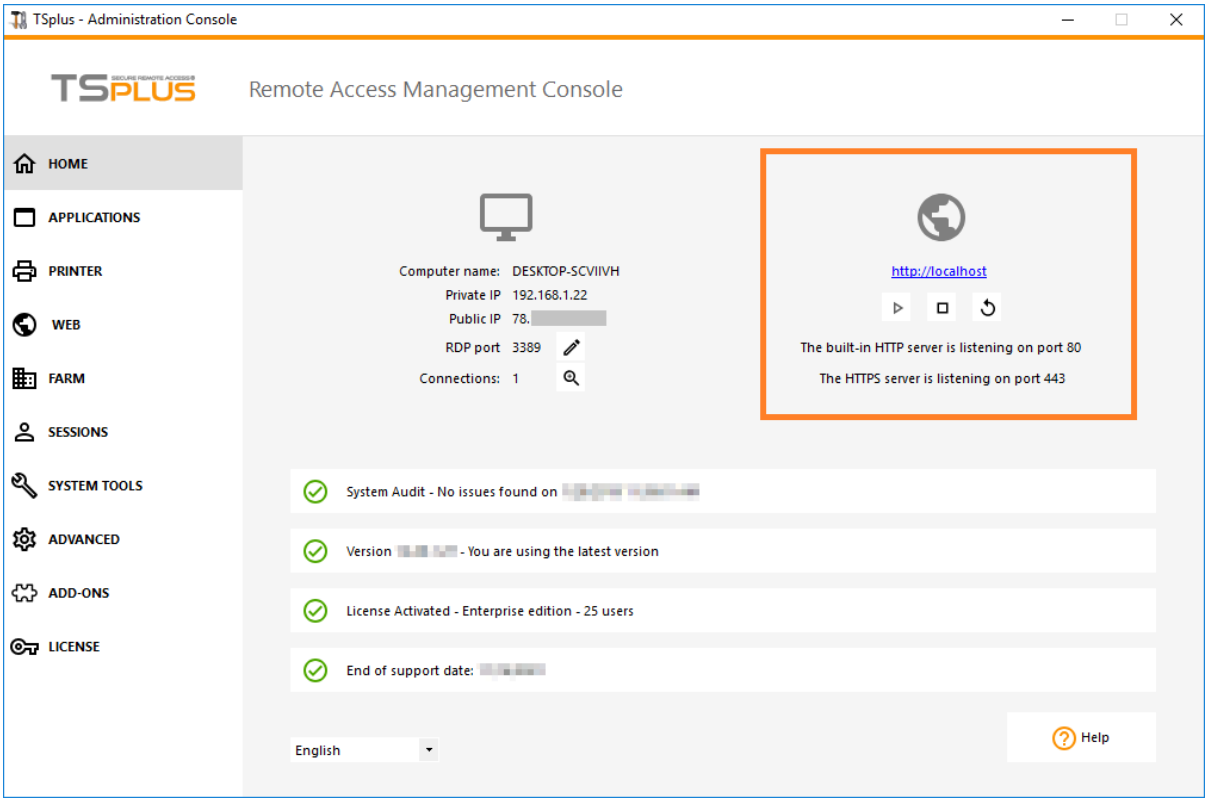
The status of the Web Server main components are displayed on the AdminTool Home dashboard.



Ports Considerations (Local Machine and Firewall / Router)

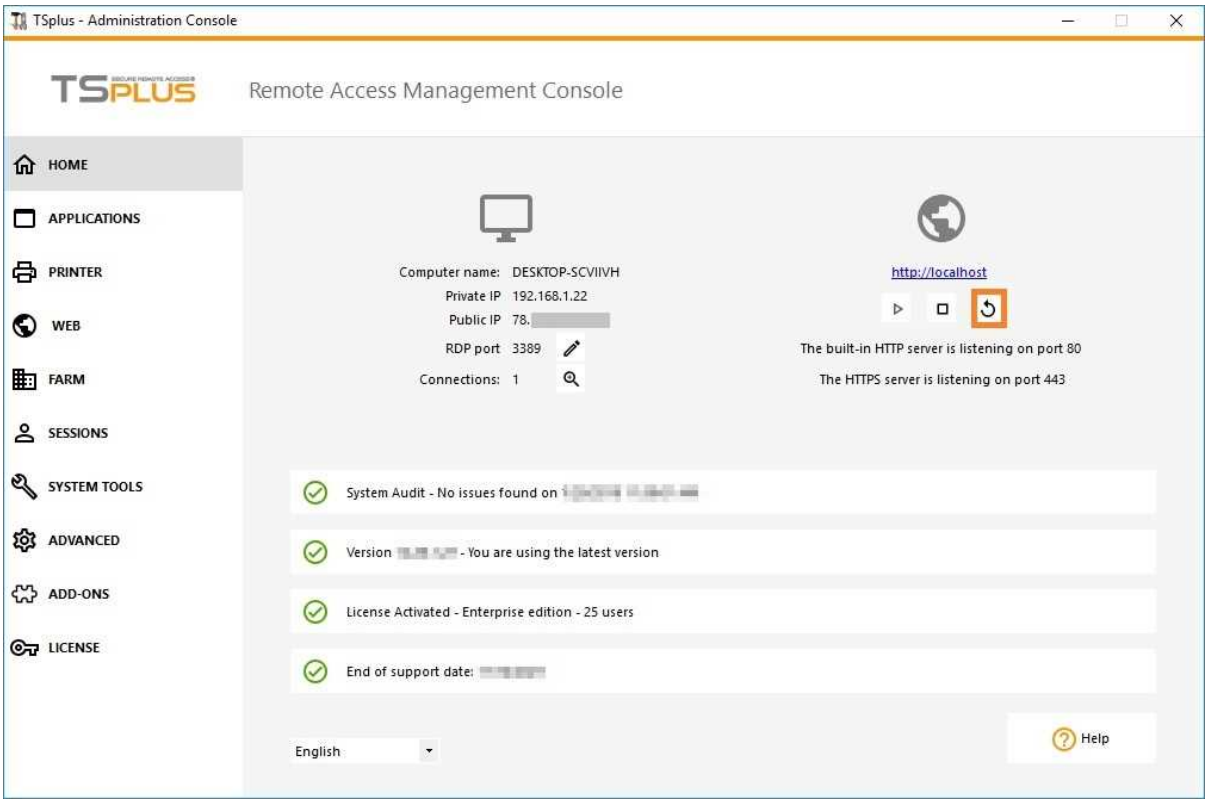
Terminal Service Plus only requires either Port 80 or Port 443 to be opened.

Port 3389 can stay closed.

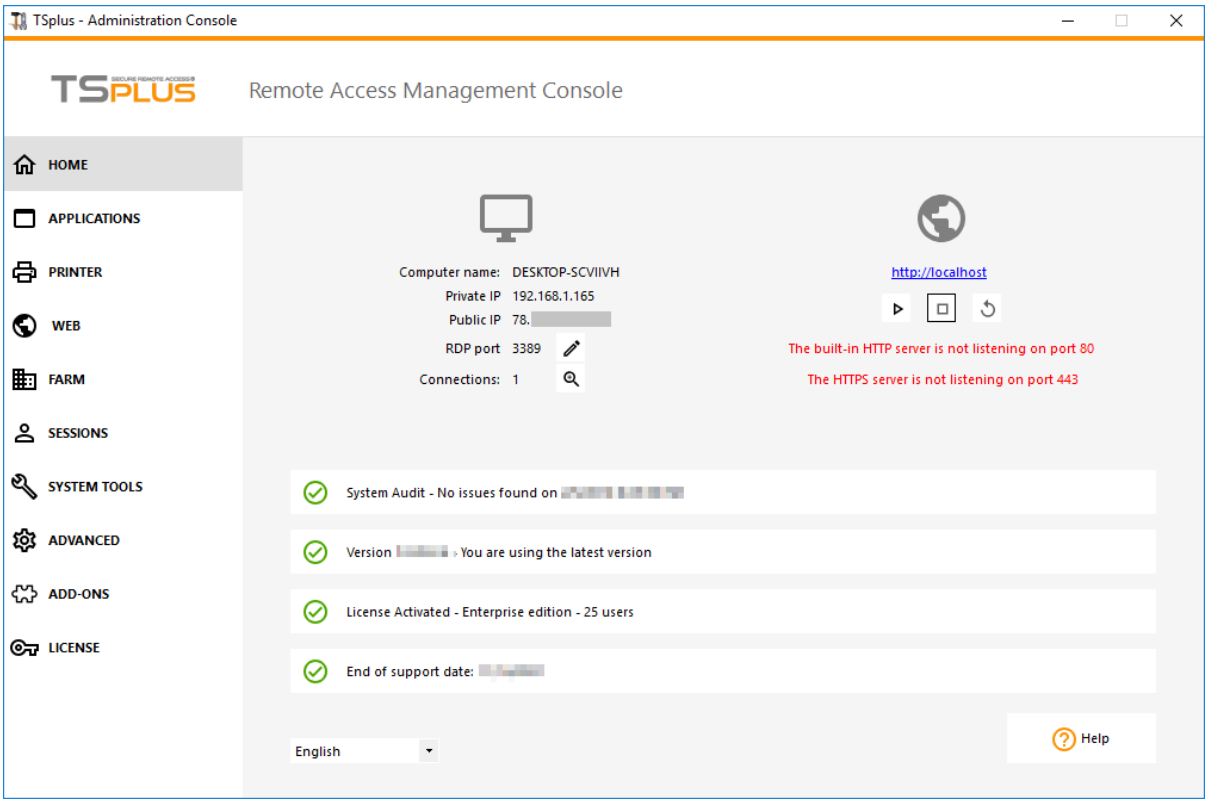


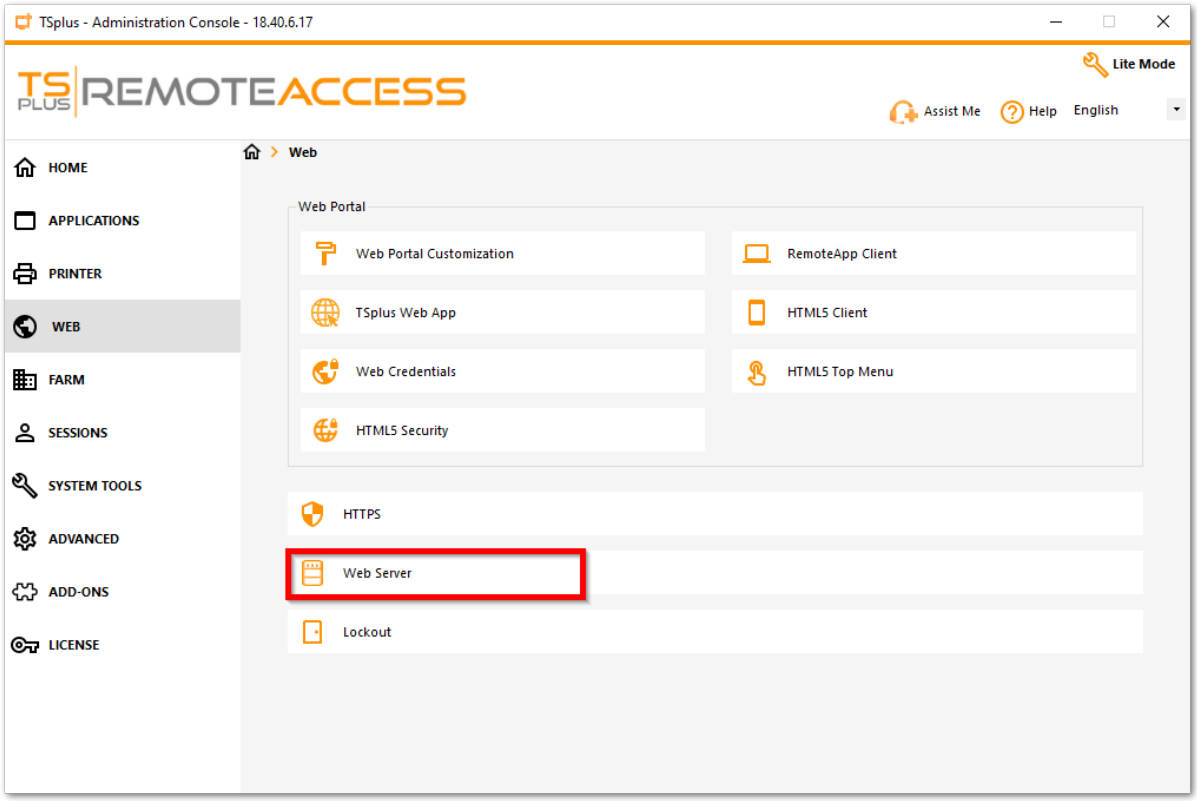
Restart / Stop the Web Server Service

If you see that a service is not running, you may need to restart the Web servers by clicking on the “Restart Web Servers button” which is represented by an arrow on the right, the Web Servers will be restarted and the service should be running again.



If you click on the “Stop Web Servers” button, placed on the middle, the Web servers will be stopped. The HTTP and HTTPS server status will now display in red indicating that the HTTP / HTTPS services are stopped:





You can change the ports during installation or at any time by clicking on the Web - Web Server tab. On this tab, you can choose to use a different HTTP web server, modify the Web Server root path and the HTTP/HTTPS port numbers. Make sure that these ports are available before changing them: if a conflict occur TSplus web server will not work. Here is a non-exhaustive list of TCP port that might be used by an application on your server. Once these modifications done, click on save and the AdminTool will restart.

###Disable http only or http on https

See this documentation for more information on this topic.

For more in-depth information about **servers customization** and **preferences**, see these pages:

Web Portal Customization, Web Applications Portal, Web Credentials.

Choosing your Ciphers Suites to enhance security

Overview

TLS/SSL, the security behind HTTPS, can use several different algorithms to secure, encrypt and authenticate a connection.

The choice of the algorithm to use is decided by an agreement between the server and the client, depending on which algorithms are available on each side.

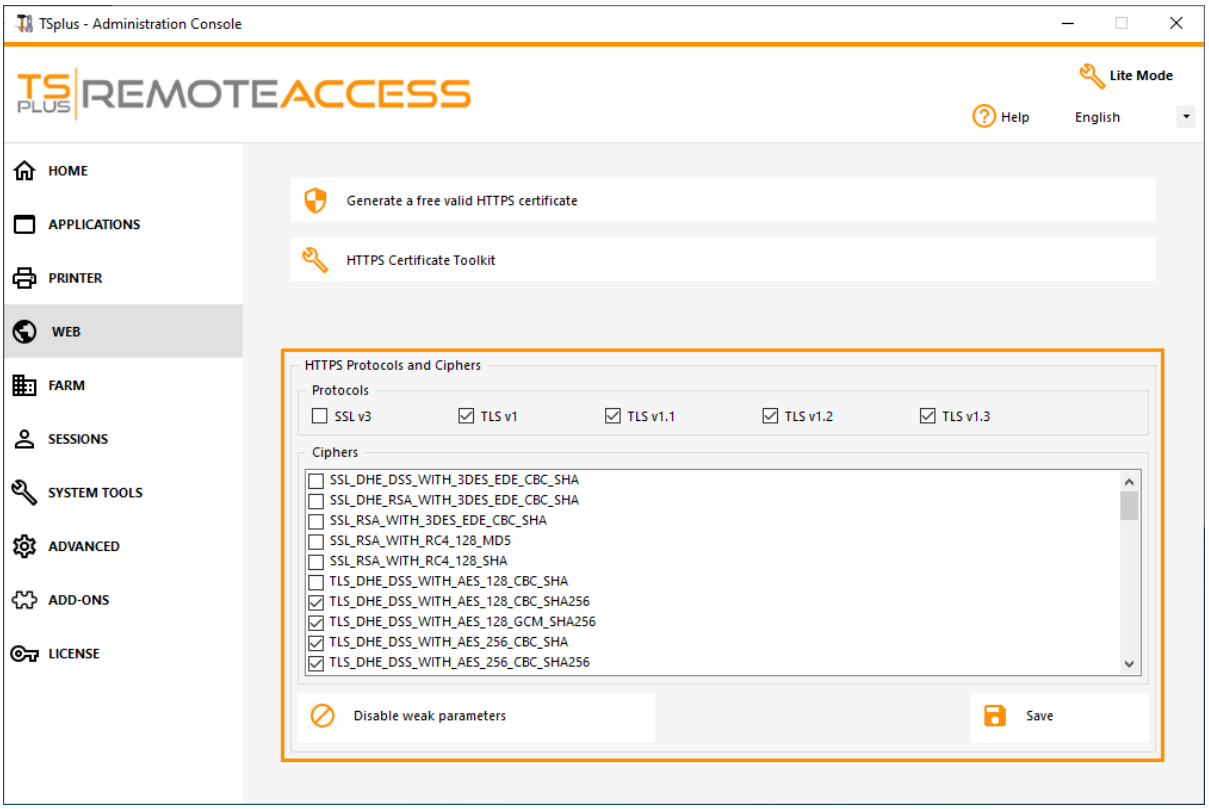
A cipher suite is a named combination of authentication, encryption, message authentication and key exchange algorithms.

Terminal Service Plus server can handle a lot of different ciphers suites. Some of them are more secure than others, but some old/legacy browsers might require relatively weak algorithms to connect.

This is the reason why Terminal Service Plus let you choose the ciphers suites you want to enable. Of course, Terminal Service Plus also has an easy setting to disable the weakest algorithms, thus enhancing your connections security.

HTTPS Protocols and Ciphers Selection

To see Terminal Service Plus Ciphers Selection, open Terminal Service Plus AdminTool, click on the “Web - HTTPS” tab, where you will see HTTPS Protocols and Ciphers:



Enabling/Disabling a Cipher Suite

You can easily enable a cipher suite by checking its checkbox and disable a cipher suite by unchecking it.

When your selection is done, click on “Save”.

This will save your selection and reload the new configuration in Terminal Service Plus built-in web server. Your new ciphers suites selection is instantly applied for every new connection to your server.

Recommended Ciphers Suites Selection

We recommend to most administrators to use our recommended ciphers suites selection, by simply clicking on the “Disable weak parameters” button and then on the “Save” button.

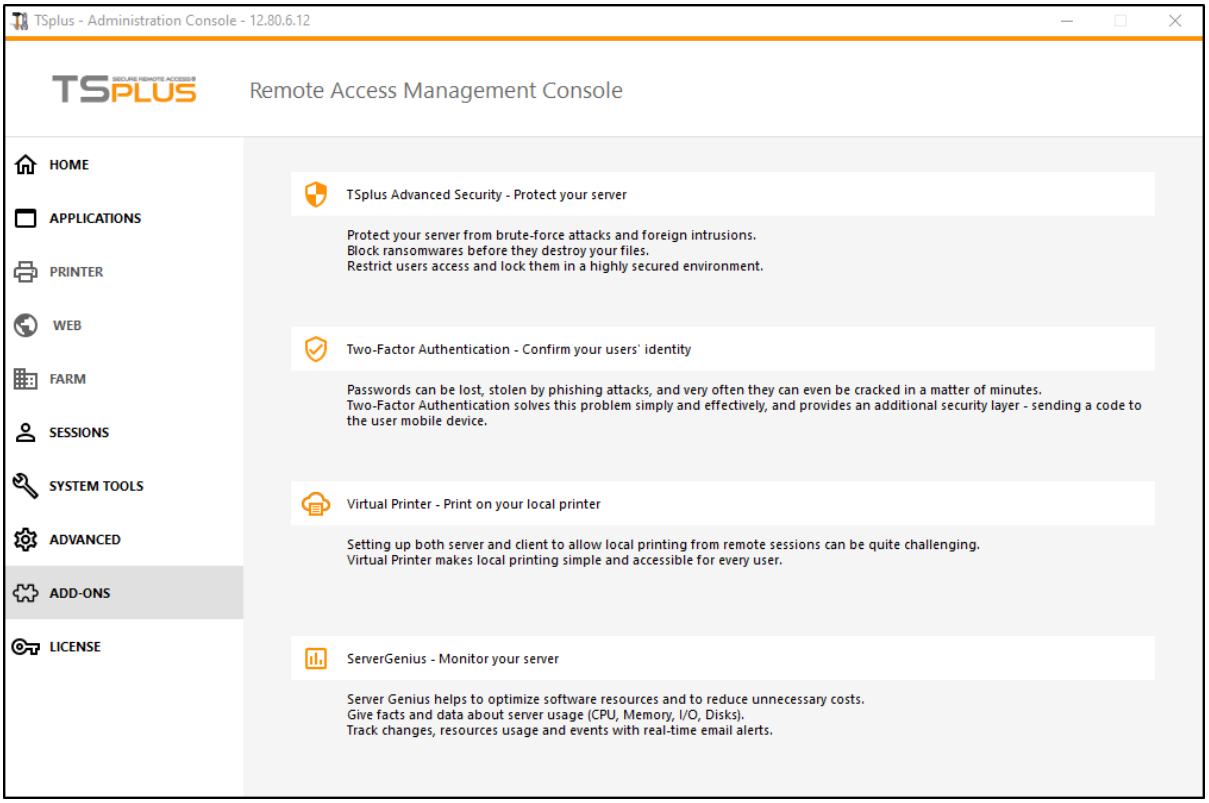
This action will disable all ciphers suites which are currently known to be weak.

You can check with SSL Labs Online Testing Tool: without those weak ciphers suites you should get the maximum grade: A!

Click-to-Help - Admin Tool - Addons

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

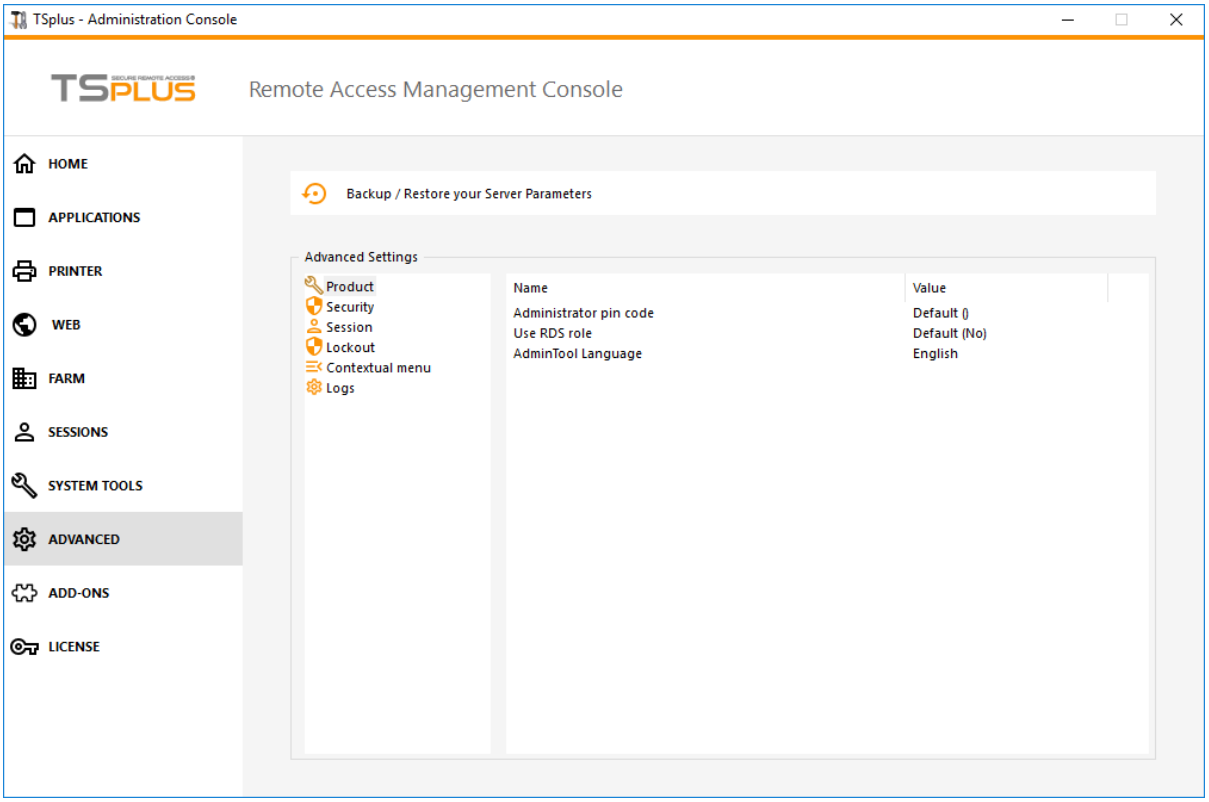
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - Advanced

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

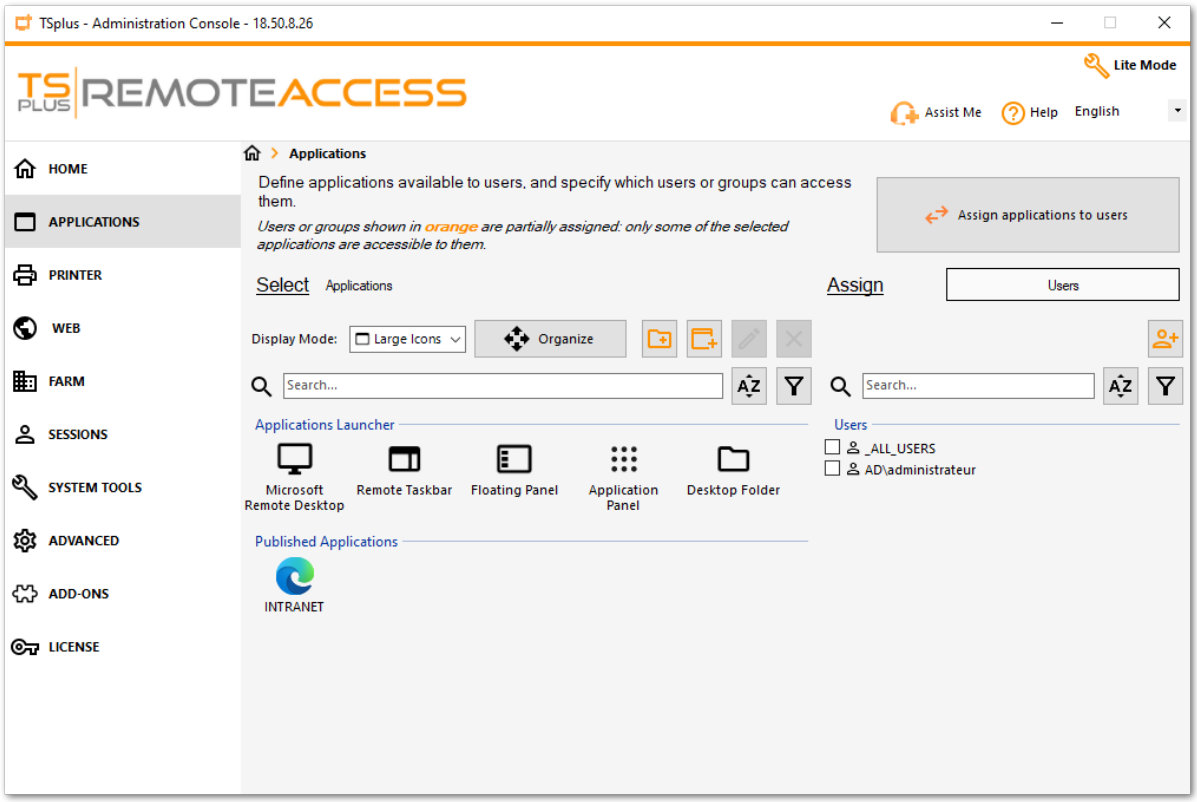
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - Applications

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

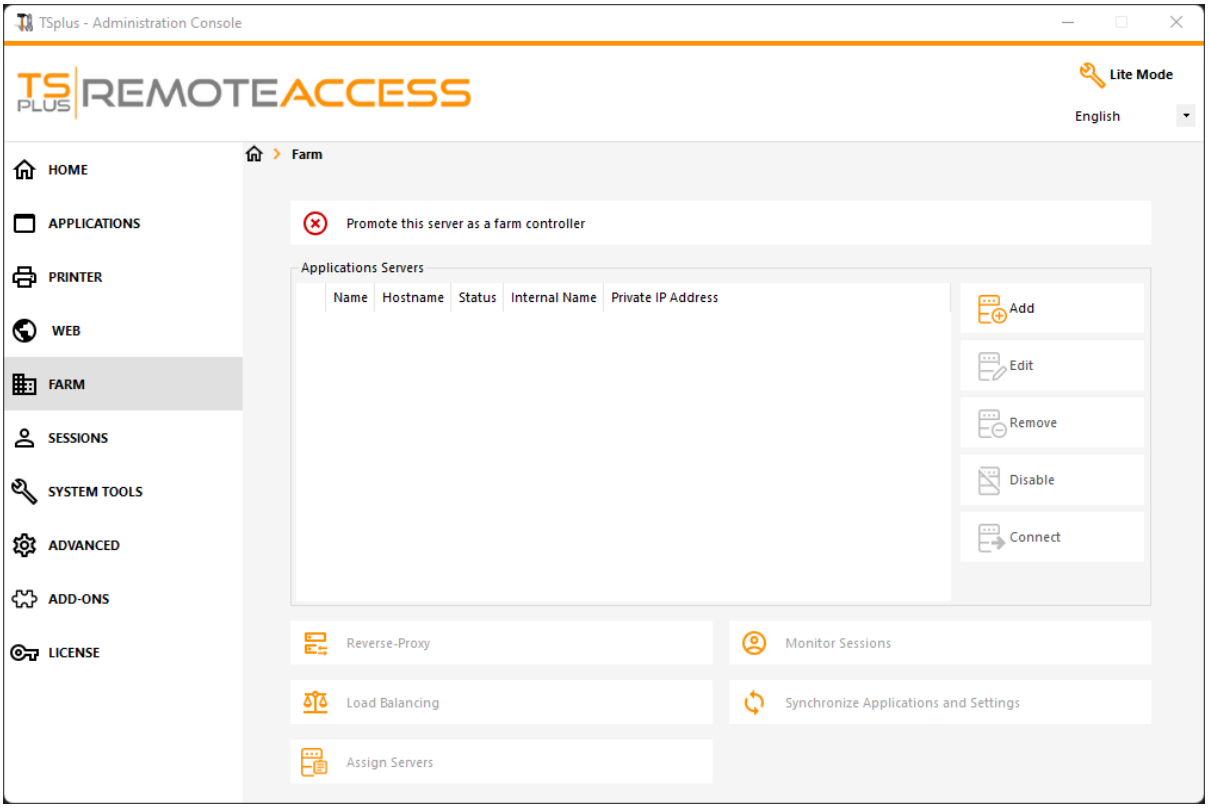
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - Farm

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

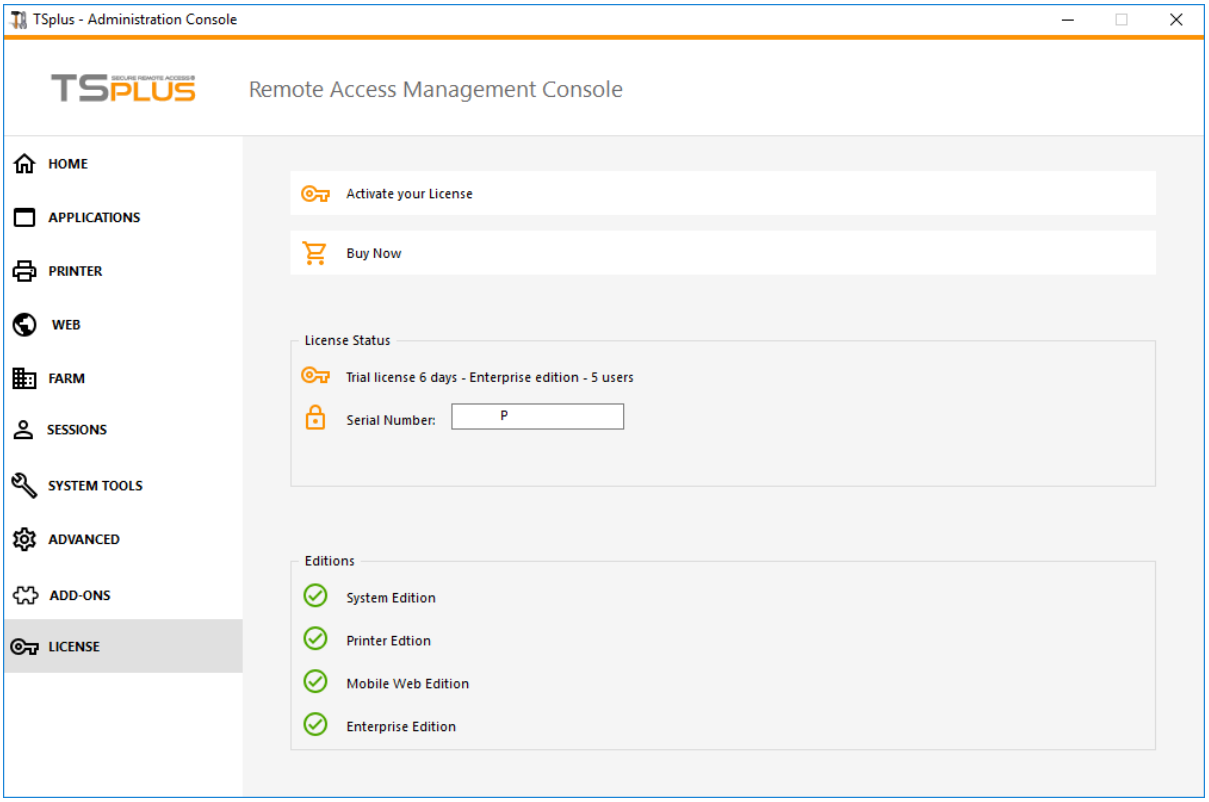
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - License

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

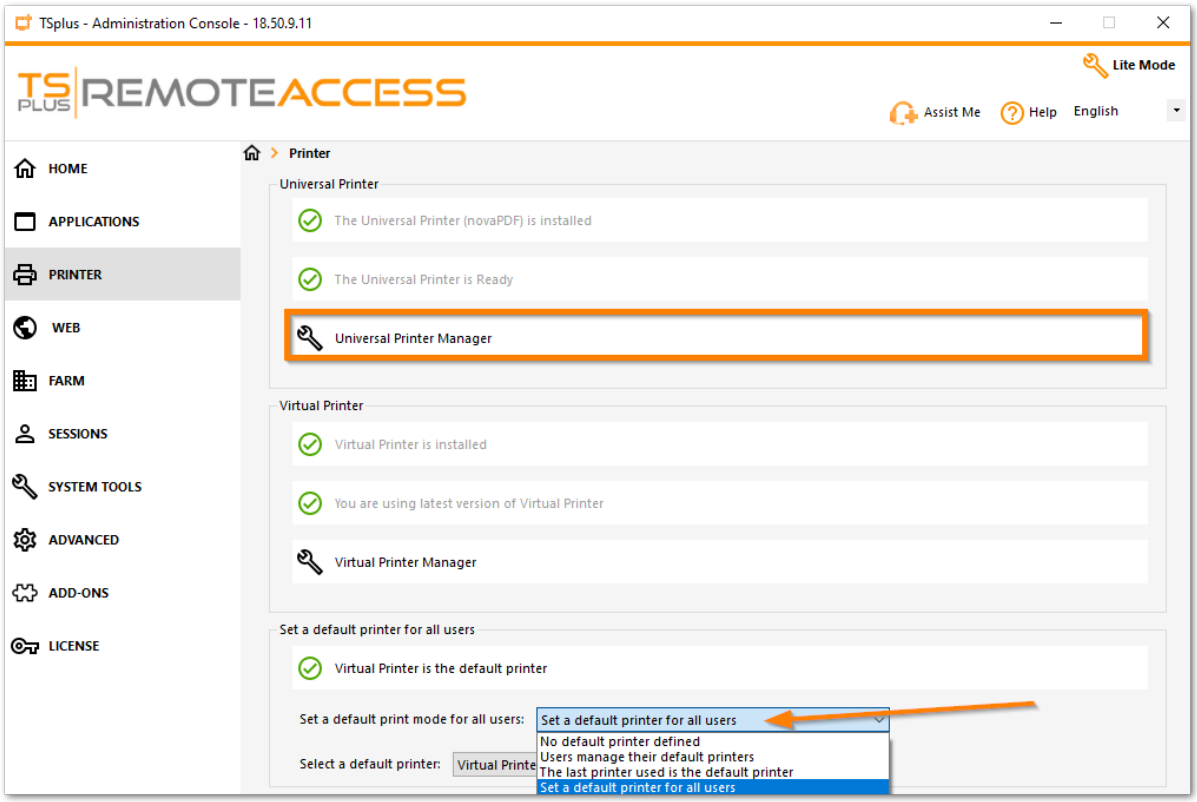
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - Printer

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - Security

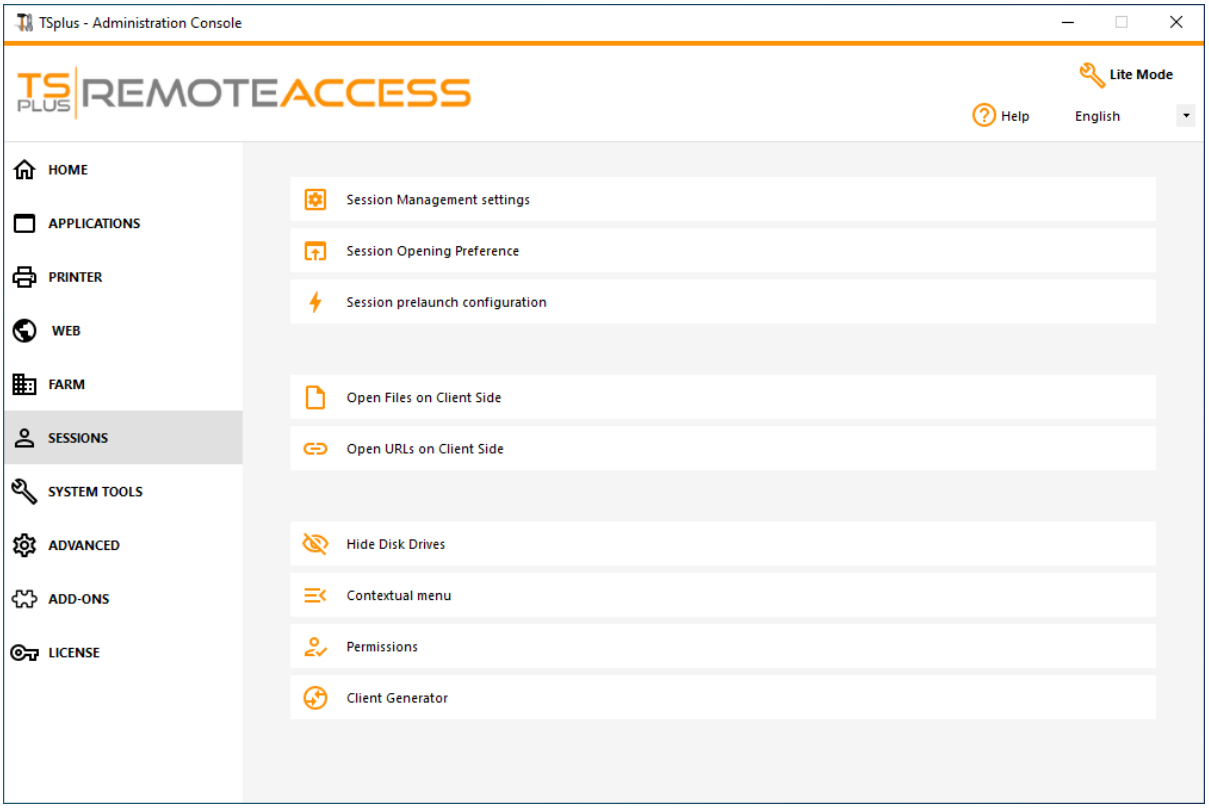
Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

Just **click on a tile or on a tab** to go to the matching help!

Click-to-Help - Admin Tool - Sessions

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

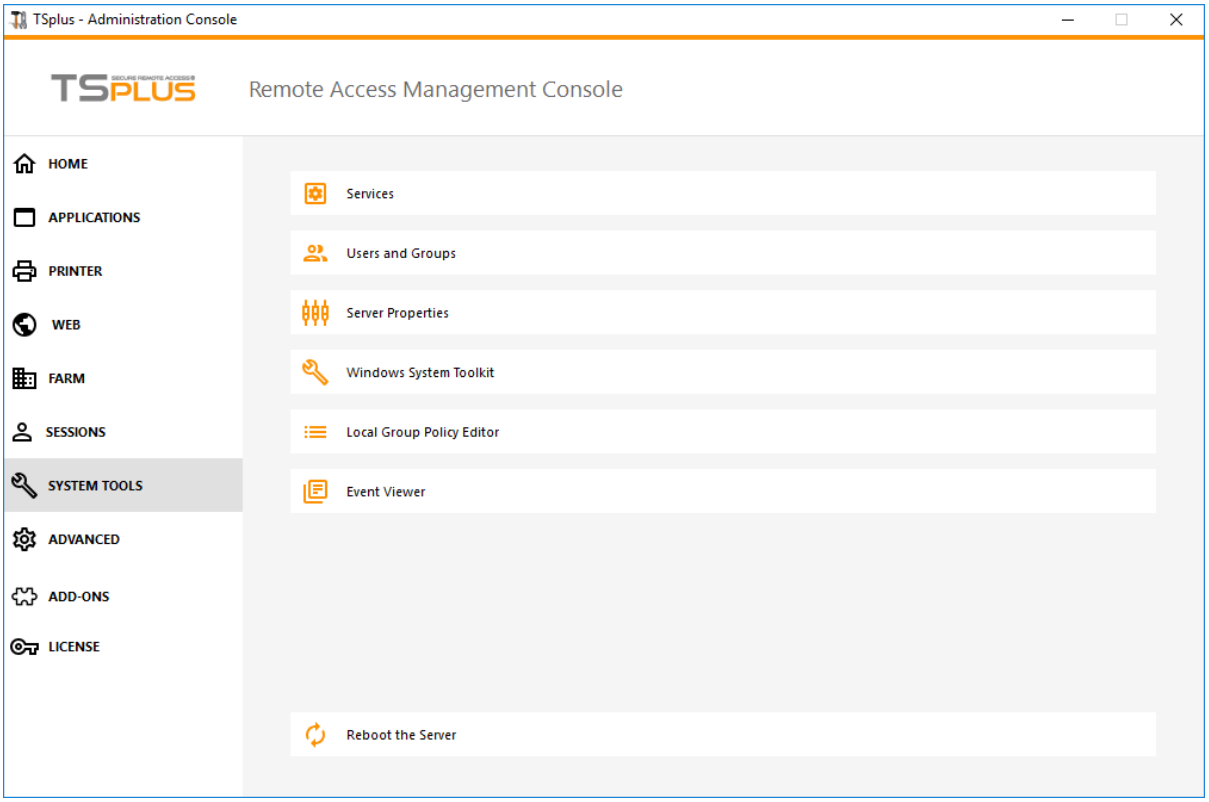
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - System

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

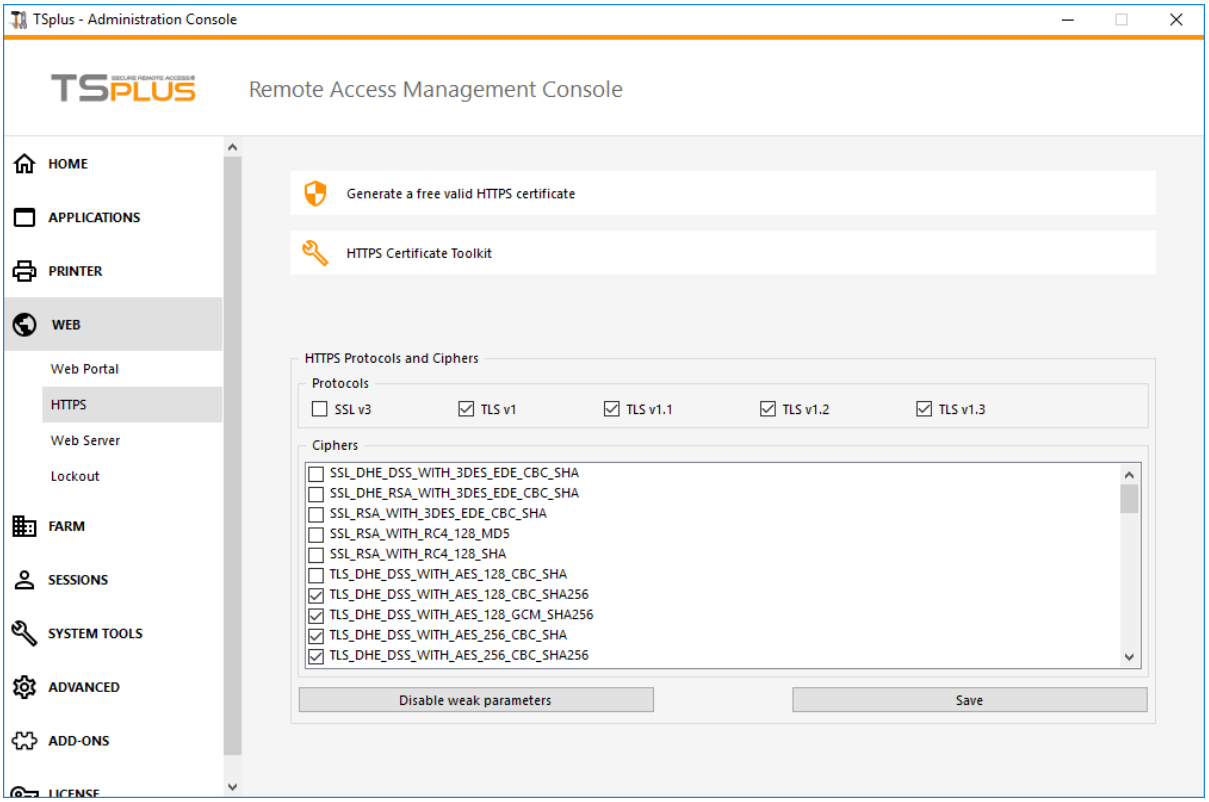
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - Web

Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

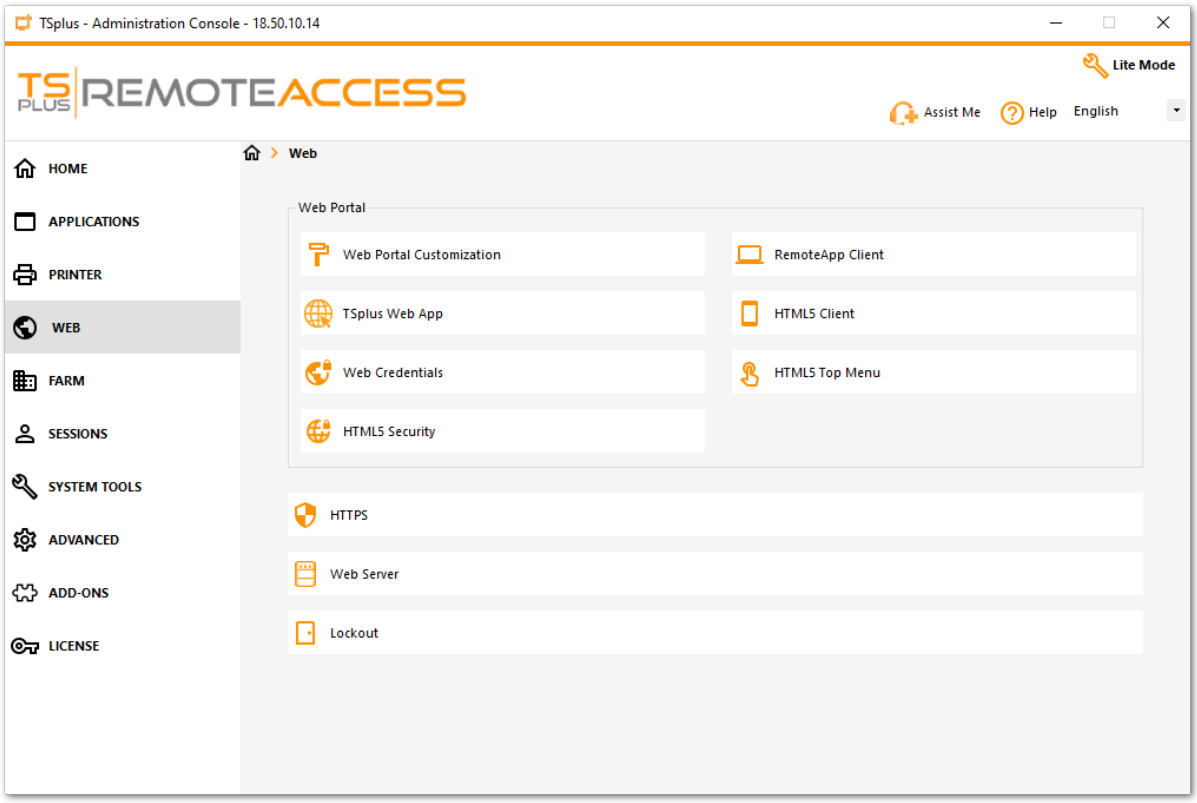
Just **click on a tile or on a tab** to go to the matching help!



Click-to-Help - Admin Tool - Web

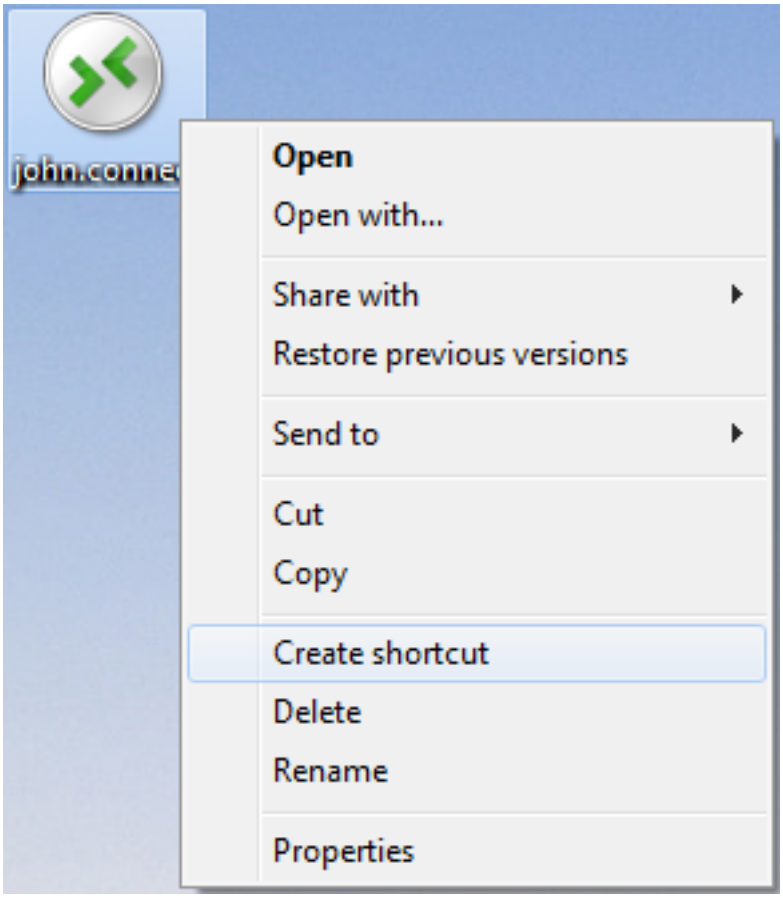
Want to get help on a feature of Terminal Service Plus Admin Tool quickly?

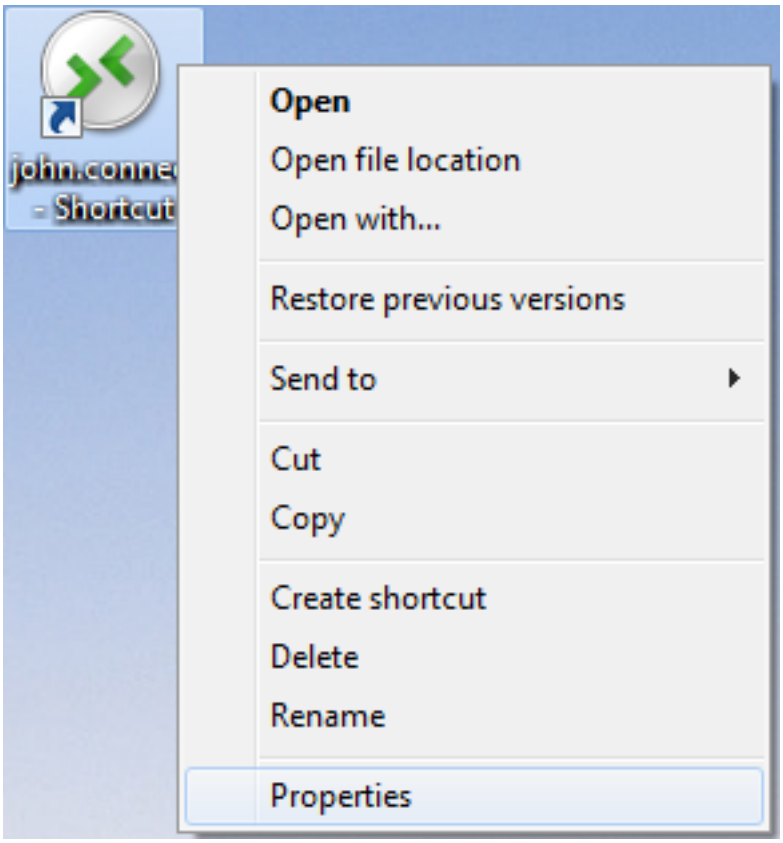
Just **click on a tile or on a tab** to go to the matching help!

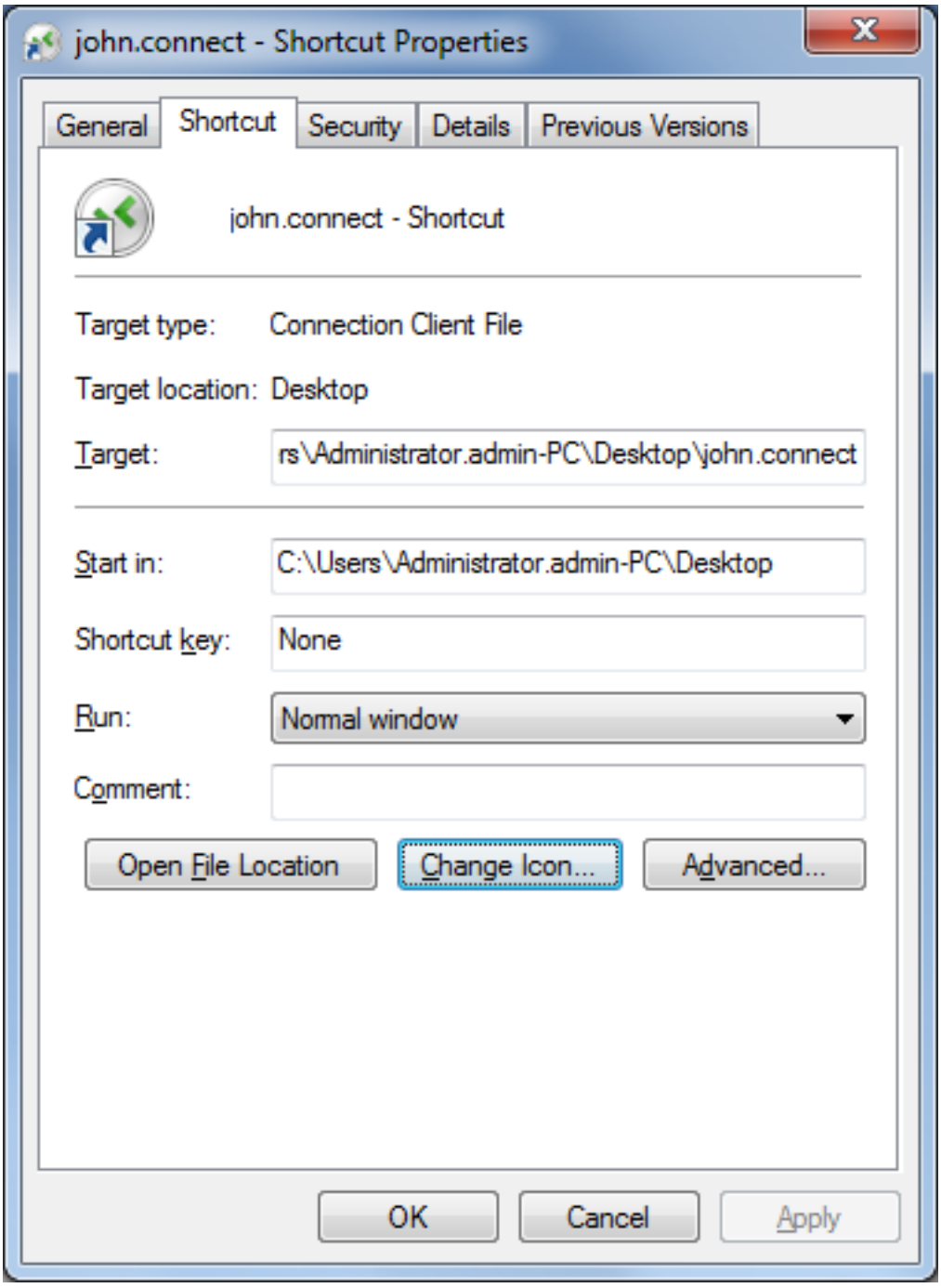


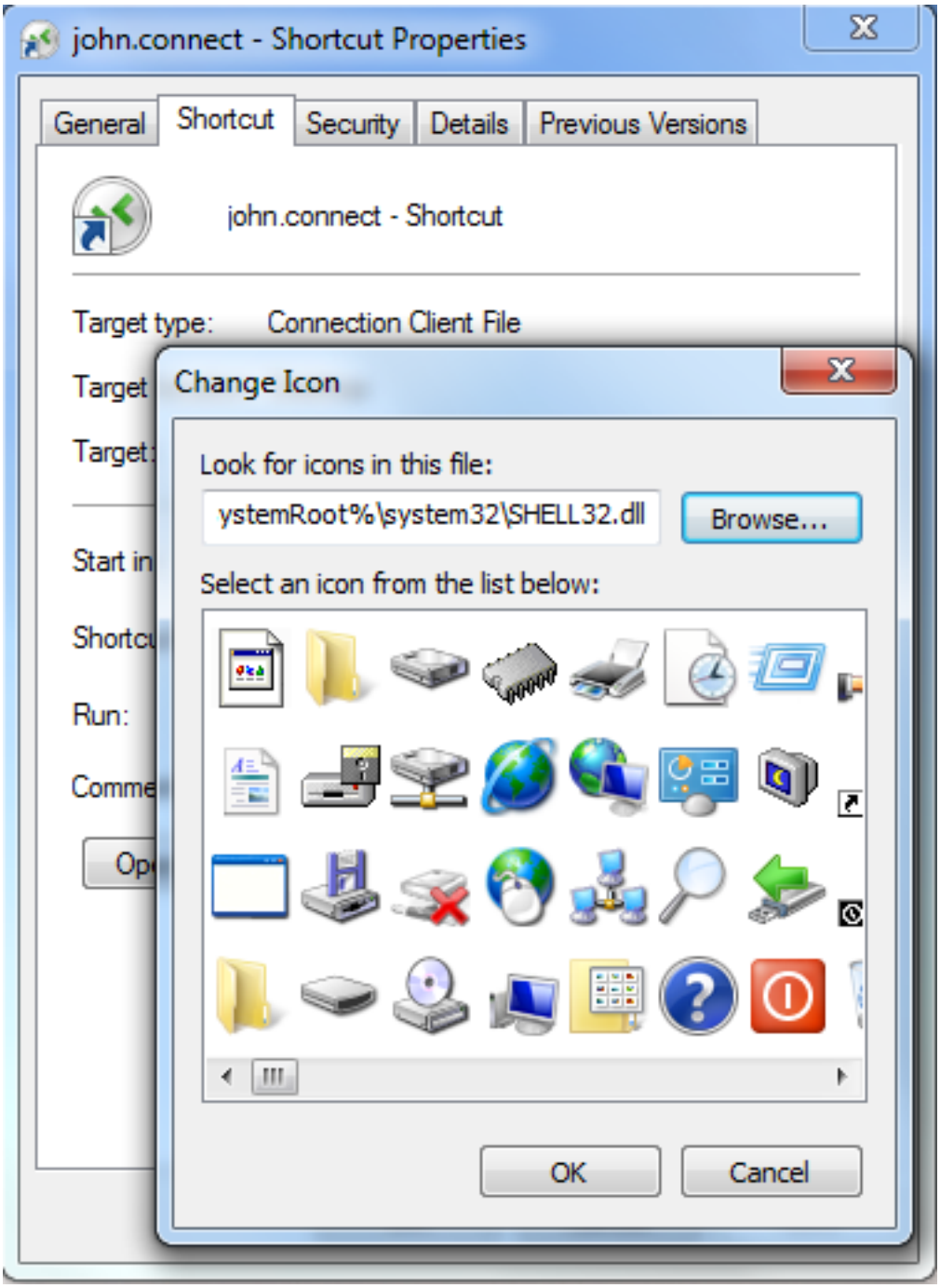
How to modify the TSplus client's icon

In order to change the generated client’s icon, just create a shortcut of the client and go to the shortcut’s properties:




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

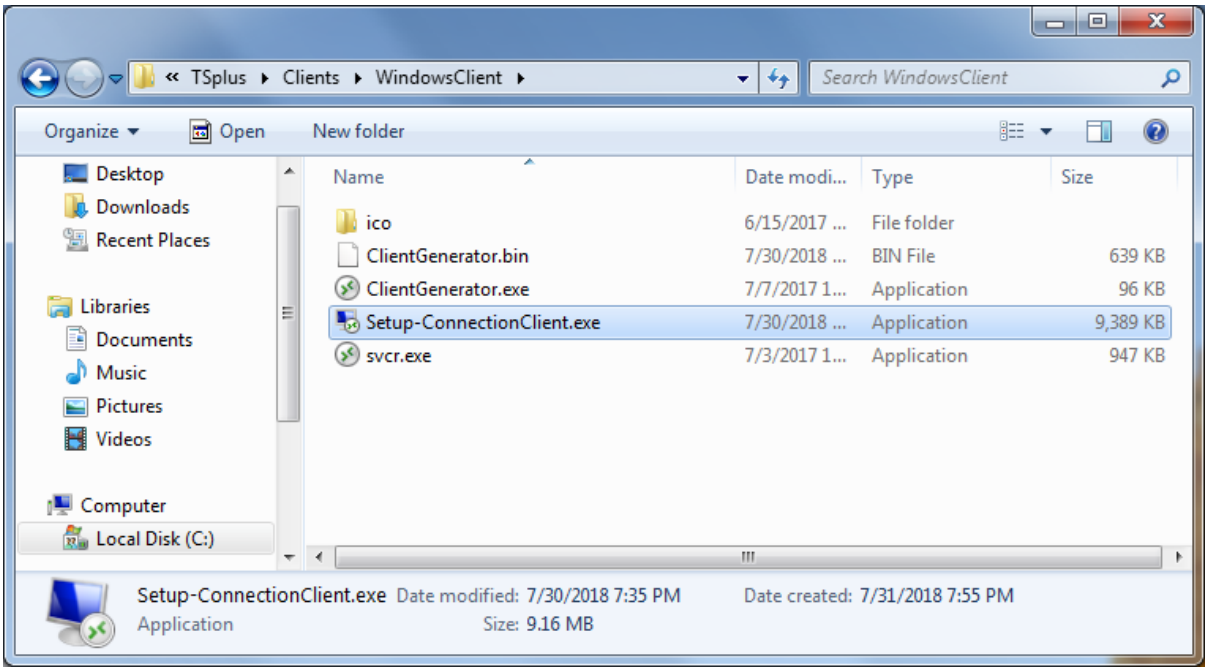

john.connect - Shortcut Properties
General
Shortcut
Security
Details
Previous Versions
john.connect - Shortcut
Target type:
Connection Client File
Target
Target:
Start in
Shortcu
Run:
Comme
Op
Change Icon
Look for icons in this file:
ystemRoot%\system32\SHELL32.dll
Browse...
Select an icon from the list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

TSplus Client Setup program

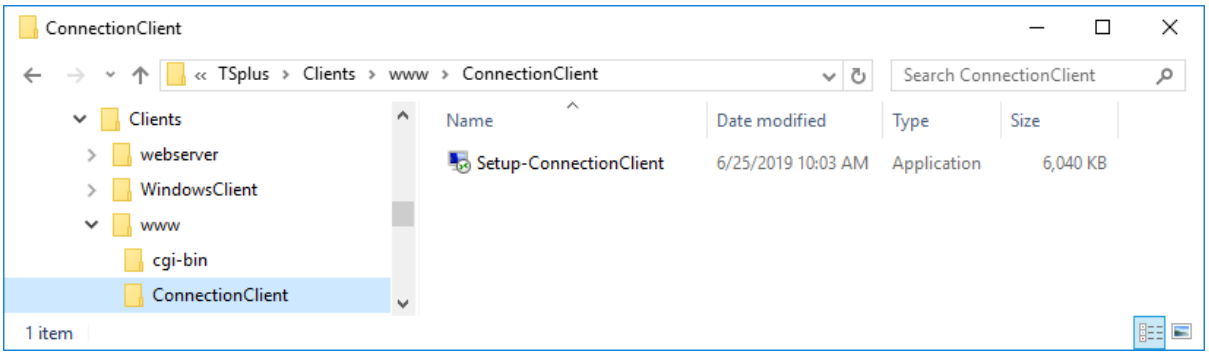
Installl

On client side, **each user will have to run a signed program named “Setup-ConnectionClient.exe” as a pre-requisite**.

This program is available on your server, in the TSplus program folder: C:\Program Files (x86)\TSplus\Clients\WindowsClient:



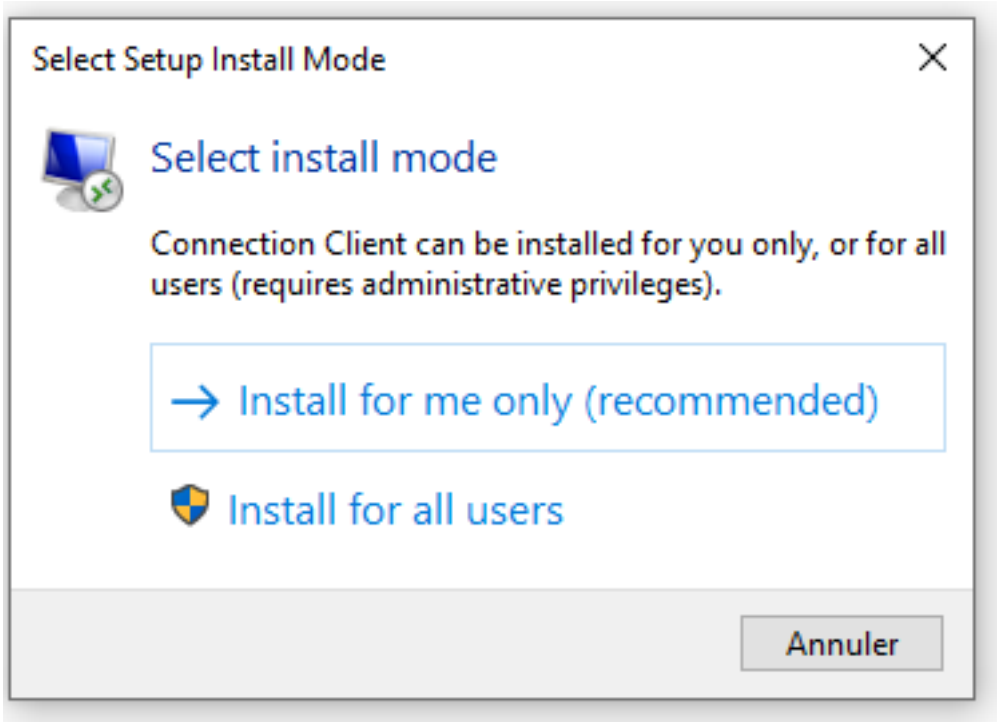
It is also available in C:\Program Files (x86)\TSplus\Clients\www\ConnectionClient, so your users can just run the program once on your web server address: http://xxxxxxxxxx/ConnectionClient/Setup-ConnectionClient.exe



or by downloading it.

Install for all users

You can now install the Connection Client for all users. This means that once installed, any user on the computer will benefit from it, and will be able to connect in remoteApp mode from the Web Portal, as well as with a generated .connect client file.



Note: For this pop-up to appear, you will need not to have the Connection Client installed already. You can also, during an installation using commandline, specify which mode you want to use with the argument /ALLUSERS or /CURRENTUSER to install respectively for all users, or for the current user.

Note: Since TSplus 12.40, The Client Setup Program and the RemoteApp client setup have been merged and can be deployed with one single setup - so if you download the Connection Client Setup, there will be no need to download the RemoteApp Client one.

Hardware Identifier & Clone Server

1- Hardware Identifier Change.

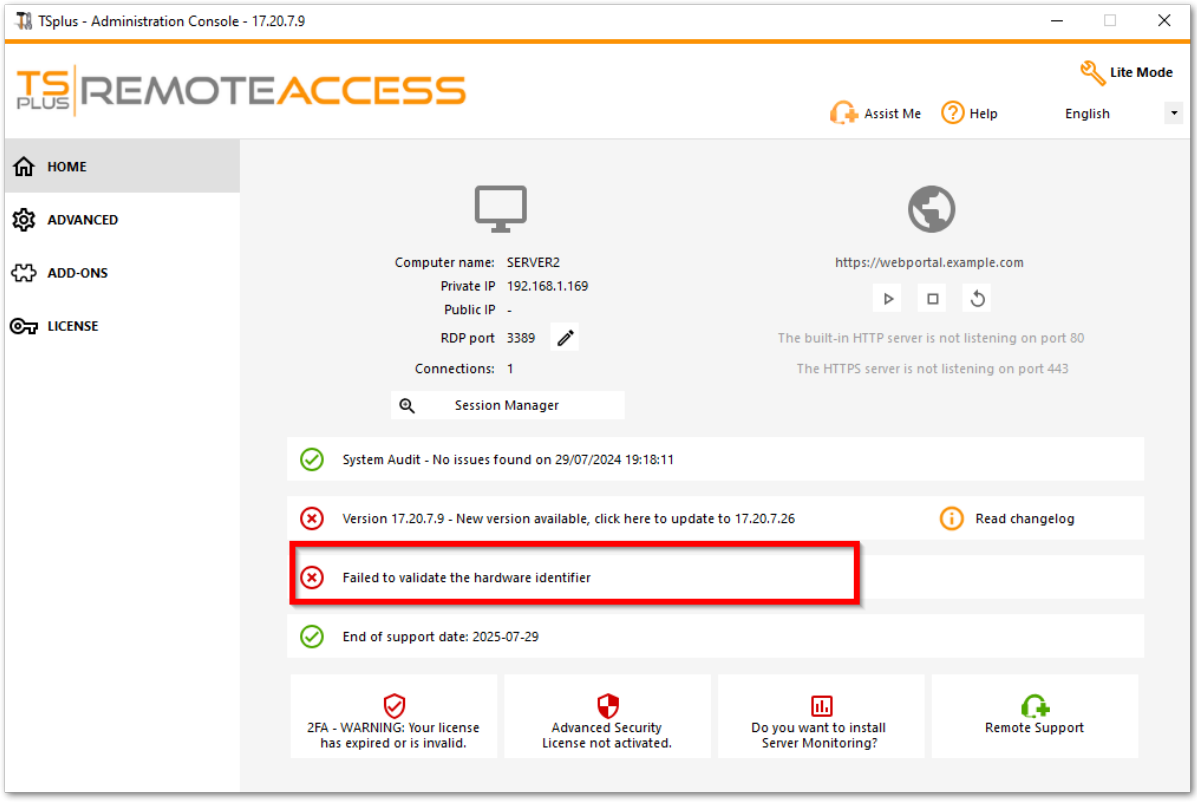
Repairing the hardware identifier following cloning or an update.

Warning : Failed to validate hardware Identifier

After migrating a physical server to a virtual machine or a Kernel Microsoft update, the license status changes to Failed to validate hardware Identifier on new hardware.

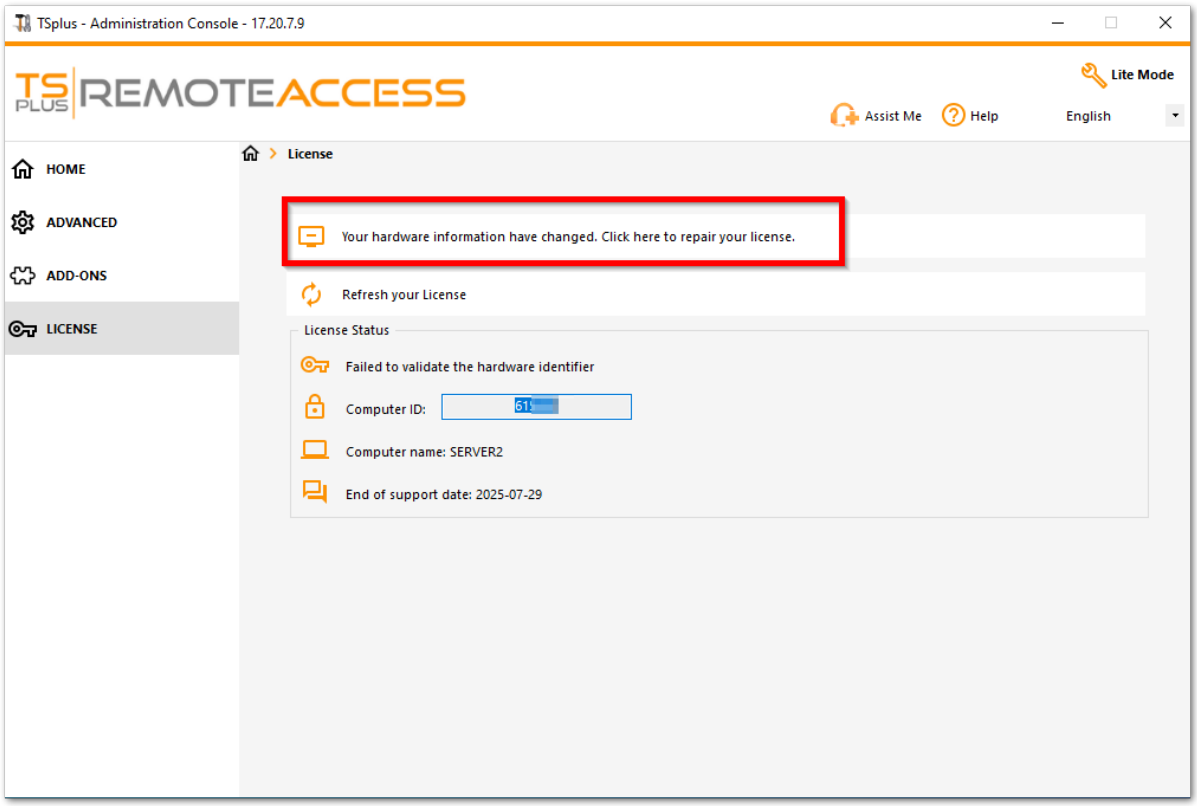
This message appears because TSplus has detected a license conflict copied from one server to another with the same Computer ID and the same name.
We already recommend renaming your new server (Example: SERVER1 > SERVER2)

- Restart your server



Click on the window to arrive on the license page.

Then click on the tab “Your hardware information has changed. Click here to repair your license.



A “license rehost” popup will open to allow you to restore your license.

Case 1: You don’t have support !
Rehosting will therefore not be possible, you will have to subscribe to a support subscription on the original server and start the migration action again.
In case of problems, Contact Support and indicate your computer ID and activation key.

Case 2: You have already rehosted for 6 months !
The Message: You have already rehosted this computer in the last 6 months. Please contact Support should you require any help rehosting your license.

The rehost will therefore not be possible, Contact Support and indicate your Computer ID and Activation Key.

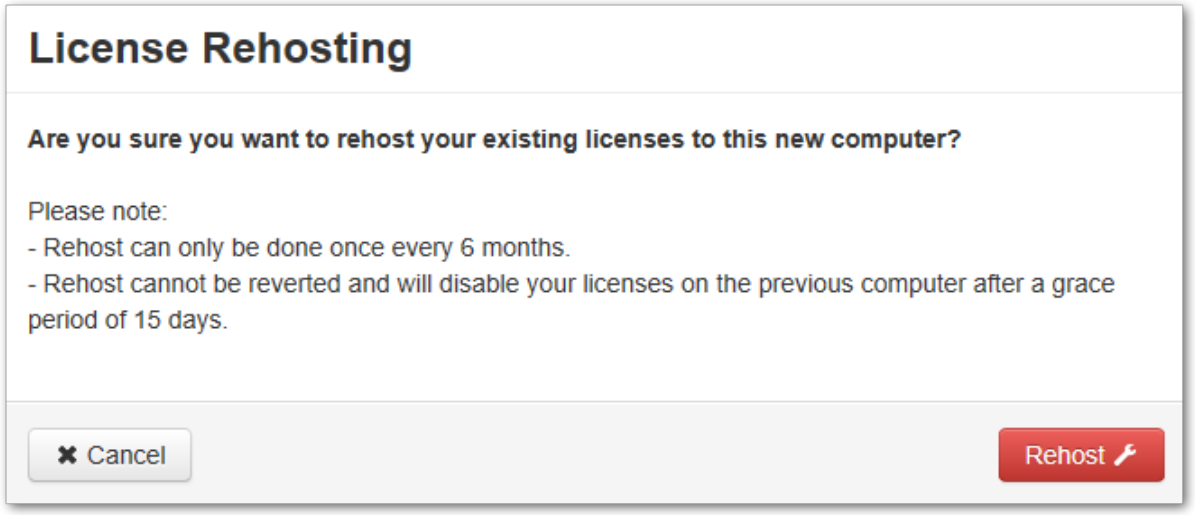
Case 3: You have support !
The following message appears: Are you sure you want to rehost your existing licenses on this new computer?

Please note:

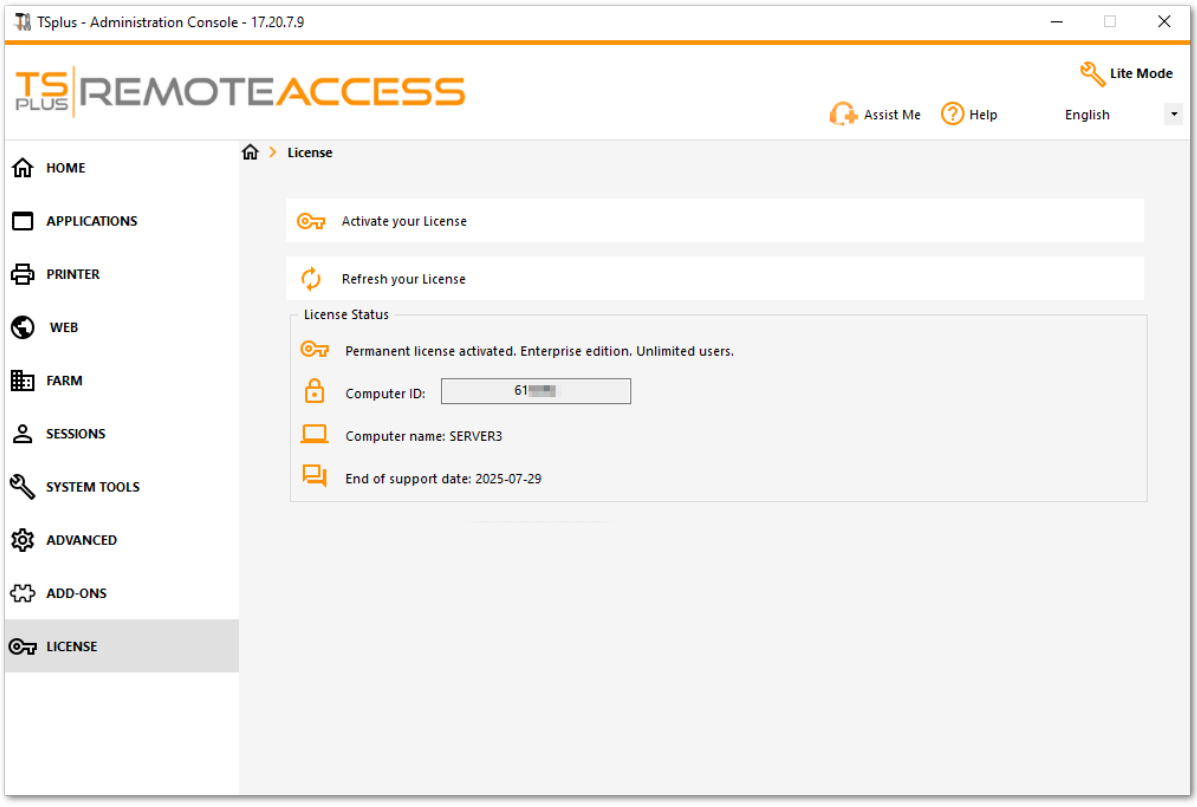
- Rehosting can only be done once every 6 months.
- Rehosting cannot be canceled and will deactivate your licenses on the previous computer

after a 15-day grace period.

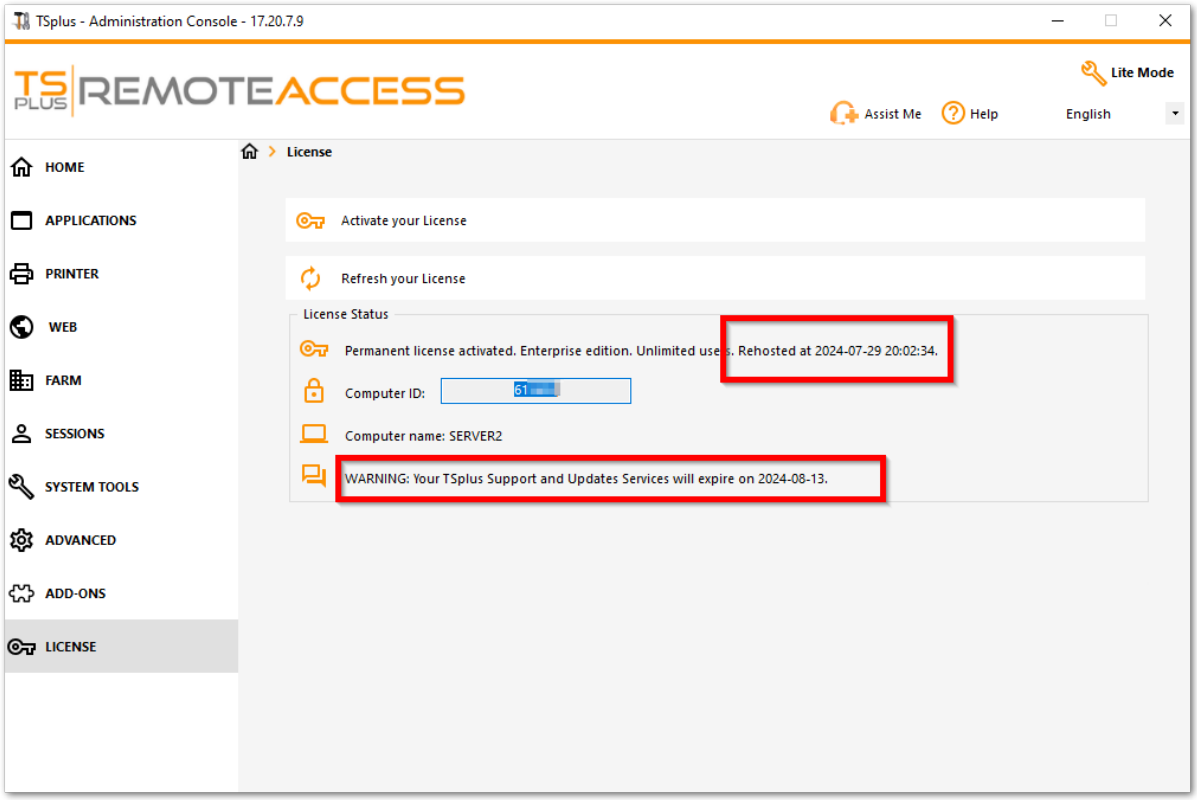
Click the **“REHOST”** button



Your license is rehosted !



Note: A message will appear on the old server with the rehost date as well as the end date of the period of use of the old server (15 days).



Update failure:
Run the Update Release and check if this has resolved your issue after restarting your server.

- Download the Update Release

2- Clone a server while keeping the existing server and activating a new license.

Requirements

When working with cloned virtual machines, it is important to modify the computer name and disk volume ID to ensure a unique TSplus Remote Access installation and avoid licensing issues.

Computer name considerations

The computer name is stored in the Windows registry inside the image itself. If modified before applying the image, it will be overwritten by Sysprep when Windows boots. However, you can predefine a name in an Unattended.xml Answer file. See Microsoft Documentation for more details.

To set the computer name, add the following section inside 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>
```

Volume ID considerations

The volume ID is associated with the disk partition, not the OS image. It can be changed before applying the image, and it will persist. Use volumeid.exe from Sysinternals, available at Microsoft Sysinternals, before Windows boots.

Deployment steps

When deploying a new virtual machine from a sysprepped image, Windows will enter the Out-Of-Box Experience (OOBE) on first boot, prompting for configuration settings.

Recommended steps for deployment:

1. **Boot to WinPE** – Prepare the system without booting into Windows.
2. **Set the Volume ID** – Change it before applying the image so it persists.
3. **Deploy the sysprepped image** – Use DISM to apply the image to C:.
4. **Set the computer name offline** – Edit the registry inside the mounted image.
5. **Copy an Unattended.xml file** – Automate OOBE configuration. This file can be dynamically modified before deployment using a script.
6. **Create a first-boot script** – Ensure final configurations with only one reboot.
7. **Reboot into Windows** – Windows finalizes itself using the specified configurations.
8. **Reset Remote Access licensing** – Run the following command:

Terminal window

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

This resets licensing and applies a new license.

Deployment script

Please find below the related WinPE deployment script.

Terminal window

```
    <# 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
```

Licensing activation

After deployment, activating a license will generate a new Computer ID for the virtual machine. This Computer ID is created by the licensing portal when a machine requests a trial or license activation. For cloned virtual machines, license activation is mandatory. Use either an activation key or a volume license key. **Offline setups are not permitted** due to security concerns. For detailed activation steps, refer to TSplus Commands List.

Conclusion

This guide outlines key considerations for deploying cloned virtual machines with TSplus Remote Access. It provides essential steps to configure and license the system correctly and must be adapted to your needs and requirements.

Cloning servers using sysprep

Requirements

When working with cloned virtual machines, it is important to modify the computer name and disk volume ID to ensure a unique TSplus Remote Access installation and avoid licensing issues.

Computer name considerations

The computer name is stored in the Windows registry inside the image itself. If modified before applying the image, it will be overwritten by Sysprep when Windows boots. However, you can predefine a name in an Unattended.xml Answer file. See Microsoft Documentation for more details.

To set the computer name, add the following section inside 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>
```

Volume ID considerations

The volume ID is associated with the disk partition, not the OS image. It can be changed before applying the image, and it will persist. Use volumeid.exe from Sysinternals, available at Microsoft Sysinternals, before Windows boots.

Deployment steps

When deploying a new virtual machine from a sysprepped image, Windows will enter the Out-Of-Box Experience (OOBE) on first boot, prompting for configuration settings.

Recommended steps for deployment:

1. **Boot to WinPE** – Prepare the system without booting into Windows.
2. **Set the Volume ID** – Change it before applying the image so it persists.
3. **Deploy the sysprepped image** – Use DISM to apply the image to C:.
4. **Set the computer name offline** – Edit the registry inside the mounted image.
5. **Copy an Unattended.xml file** – Automate OOBE configuration. This file can be dynamically modified before deployment using a script.
6. **Create a first-boot script** – Ensure final configurations with only one reboot.
7. **Reboot into Windows** – Windows finalizes itself using the specified configurations.
8. **Reset Remote Access licensing** – Run the following command:

Terminal window
```
AdminTool.exe /license /reset
```

This resets licensing and applies a new license.

Deployment script

Please find below the related WinPE deployment script.

Terminal window
```
<# 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
```

Licensing activation

After deployment, activating a license will generate a new Computer ID for the virtual machine. This Computer ID is created by the licensing portal when a machine requests a trial or license activation. For cloned virtual machines, license activation is mandatory. Use either an activation key or a volume license key. **Offline setups are not permitted** due to security concerns. For detailed activation steps, refer to TSplus Commands List.

Conclusion

This guide outlines key considerations for deploying cloned virtual machines with TSplus Remote Access. It provides essential steps to configure and license the system correctly and must be adapted to your needs and requirements.

Command lines

We are pleased to provide you with a comprehensive set of command-line tools designed to enhance the flexibility and efficiency of our software. These tools enable users to script and automate various functionalities, tailoring the software to meet their specific needs and workflows.

Explore the possibilities and optimize your experience with our command-line options.

You only have to run the following command lines as an elevated Administrator. As a reminder, AdminTool.exe and TwoFactor.Admin.exe (2FA addon) should be located here: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Backup data and settings: /backup

Syntax:

AdminTool.exe /backup [optionalPath] [parameters]

Description:

Command /backup is used to backup TSplus data and settings.

By default, the backup will be created in the archives directory (C:\Backupparam)

Parameters:

- optionalPath : to backup in another directory than the default one. Relative and absolute paths are allowed.
- /silent : if this parameter is mentioned, the backup is done silently

Examples:

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

For more information, please go to TSplus - Backup Settings

Restore data and settings: /restore

Syntax:

AdminTool.exe /restore [backupPath] [parameters]

Description:

Command /restore is used to restore TSplus data and settings.

The specified backup directory must contain a data and a settings folder, as created by the /backup command.

Parameters:

- backupPath : the path where is located the backup folder to restore.
- /silent : if this parameter is mentioned, the restore is done silently

Examples:

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

For more information, please go to TSplus - Backup Settings

Webserver: /webstop , /webstart and /webrestart

Syntax:

AdminTool.exe /webstop

AdminTool.exe /webstart

AdminTool.exe /webrestart

Description:

Command /webstop is used to stop the Web server.

Command /webstart is used to start the Web server.

Command /webrestart is used to restart the Web server.

Parameters:

None

Update: /update

Syntax:

AdminTool.exe /update [options]

Description:

Command update is used to update TSplus Remote Access and potentially Advanced Security.

Parameters:

- [options]
  :
  - /addons : if this option is used, Advanced Security is also updated, if a new version is available.

Example:

AdminTool.exe /update /addons

Apply Windows compatibility updates: /updatekernel

Syntax:

svcac.exe /updatekernel [/silent]

svcac.exe should be located here: **C:\Program Files (x86)\TSplus**

Description:

Command /updatekernel is used to apply Windows compatibility updates.

These automatic updates ensure that TSplus Remote Access remains compatible with new Windows updates and avoid the need to download and reinstall a newer version of TSplus Remote Access.

Windows compatibility updates can occur daily. TSplus Remote Access allows forced updating. This is useful when compatibility seems broken, and you need to retrieve the latest TSplus Remote Access patch outside of the regular update schedule.

Please note that a valid license is required to retrieve compatibility updates. If your trial license has expired or if your license is invalid, an error message box will be displayed. Please contact our support team with a screenshot of this error message if the issue is unexpected.

Parameters:

- [/silent] : Update silently by providing this parameter. No message box will be displayed.

Install Universal Printer: /InstallUniversalPrinter

Syntax:

universalprintermanagement.exe /InstallUniversalPrinter

universalprintermanagement.exe is located here: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Description:

Command /InstallUniversalPrinter is used to install Universal Printer.

This is a clean install as it removes existing Universal Printer if previously installed.

Parameters:

None

You can also perform this action manually, please look at Universal Printer

---

Remove UniversalPrinter: /RemoveUniversalPrinter

Syntax:

universalprintermanagement.exe /RemoveUniversalPrinter

universalprintermanagement.exe is located here: **C:\Program Files (x86)\TSplus\UserDesktop\files**

Description:

Command /RemoveUniversalPrinter is used to uninstall Universal Printer.

Parameters:

None

You can also perform this action manually, please look at Universal Printer

---

Configure proxy server: /proxy /set

Syntax:

AdminTool.exe /proxy /set [parameters]

Description:

Command /proxy /set is used to configure a proxy server for Internet access.

Parameters:

- /host : the destination host can be a predefined value (“ie” or “none”) or a user-defined value (e.g: 127.0.0.1 or proxy.company.org). This parameter is mandatory
- /port : the port number used to connect to the proxy server. Required if the hostname value is a custom user-defined value.
- /username : the username to connect to the proxy server. This setting is optional
- /password : the user’s password must be supplied if a username has been defined. However, its value can be empty

Examples:

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

AdminTool.exe /proxy /set /host ie

For more information, please go to How to configure a Proxy Server for Internet Access?

Open Web Credentials form: /webcredentials

Syntax:

AdminTool.exe /webcredentials

Description:

Command /webcredentials launches in a single window the Web Credentials interface (as you would do in AdminTool > Web > Web Credentials).

Parameters:

None

Create Web Credentials: /webcredentials-add

Syntax:

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

Description:

Command /webcredentials-add is used to create Web Credentials (as you would do in AdminTool > Web > Web Credentials).

Parameters:

- webLogin : the web login you want to create.
- webPassword : the associated web password. It can be blank credential. For that, use double quotes "" to indicate a blank password
- windowsLogin : the Windows login of the corresponding user.
- windowsPassword : the Windows password.
- maximumConcurrentSessions (optional): the maximum number of concurrent sessions for this user.

Example:

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

For more information, please go to Web Credentials

Remove Web Credentials: /webcredentials-remove

Syntax:

AdminTool.exe /webcredentials-remove [webLogin]

Description:

Command /webcredentials-remove is used to remove an existing Web Credential (as you would do in AdminTool > Web > Web Credentials).

Parameters:

- webLogin : the web login you want to remove.

Example:

AdminTool.exe /webcredentials-remove johndoe

For more information, please go to Web Credentials

Open Session Manager: /sessionmanager

Syntax:

AdminTool.exe /sessionmanager

Description:

Command /sessionmanager launches in a single sizable-window the session manager (as you would do in AdminTool > Home > Session Manager).

Parameters:

None

Open Sessions monitor: /farm-sessions-monitor

Syntax:

AdminTool.exe /farm-sessions-monitor

Description:

Command /farm-sessions-monitor launches in a single sizable-window the session monitor of the farm manager (as you would do in AdminTool > Farm > Monitor Sessions).

Parameters:

None

Open Load balancing manager: /farm-loadbalancing

Syntax:

AdminTool.exe /farm-loadbalancing

Description:

Command /farm-loadbalancing launches in a single sizable-window the load balancing manager of the farm manager (as you would do in AdminTool > Farm > Load Balancing).

Parameters:

None

Run system audit: /systemaudit

Syntax:

AdminTool.exe /systemaudit

Description:

Command /systemaudit runs a system audit (as you would do manually in AdminTool > Home > System Audit > Run System Audit).

Parameters:

None

License activation: /activate

Syntax:

AdminTool.exe /activate [licensePath]

Description:

Command activate is used to activate Remote Access license, using a license file.

Parameters:

- [licensePath] : the path of the license file

Example:

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

License reset following cloning of a virtual machine: /reset

Syntax:

AdminTool.exe /license /reset

Description:

When cloning a server, the ‘License’ tab in AdminTool may not display a Computer ID or might show the error message: “Invalid hardware identifier.” The command /reset aims to initialize licensing on the clone server so that new licenses can be assigned for the installed TSplus products.

Important Notes:

1. A new TSplus license must be activated using a new Activation Key.
2. Do not use the /license /reset command on a non-cloned machine, as it permanently prevents license assignment. Always confirm the machine’s status before proceeding.

Steps to reset license on a cloned server:

1. Open an Administrator session on the cloned server.

2. Change the HDD Volume Serial Number.

- Execute the vol command to display the current Volume Serial Number (VSN). The result should ressemble: 74F8-9C08 .

- Download and install the VolumeID utility, available here .

- Execute the command: volumeid C: 84F8-9C08 as an administrator to change the drive VSN. In this example, we changed the VSN of disk C: and I have changed only one character (the first) of the old VSN to specify the new one.

- Note: this step is critical because certain Windows Server versions do not generate a new Volume Serial Number during cloning, even when using SysPrep.

3. Rename the cloned server and restart it.

4. Reset the License in AdminTool:

- Open a Command Prompt with Administrator privileges.

- Navigate to the directory containing the AdminTool executable using this command: cd "C:\Program Files (x86)\TSplus\UserDesktop\files"

- Execute the following command: AdminTool.exe /license /reset

5. Verify the reset.

- After running the command, the ‘License’ tab should display the following error: "Failed to read license file (unexpected file format)."

6. Activate the new license.

- In the ‘License’ tab, click ‘Activate your license’ and enter the new Activation Key to activate the required licenses and supports.

Example:

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

---

Volume license activation: /vl /activate

Syntax:

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

Command vl /activate is used to activate a volume license.

Parameters:

- licensekey : license key to activate, in this format: AAAA-BBBB-CCCC-DDDD
- /users : any number from 1 to 50, or “unlimited”
- /edition : “Desktop”, “MobileWeb” or “Enterprise”
- /supportyears : Any number from 0 to 3.
- /comments : Specifies the comments to attach to the license on the License portal

Example:

AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “This is a comment”

For more information, please go to Volume license documentation

---

Enabling and disabling Volume license: /vl /enable and /vl /disable

Syntax:

AdminTool.exe /vl /enable [licensekey]

AdminTool.exe /vl /disable [licensekey]

Description:

Command vl /enable is used to enable a volume license.

Command vl /disable is used to disable a volume license.

Parameters:

- licensekey : license key to enable/disable, in this format: AAAA-BBBB-CCCC-DDDD

Examples:

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

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

For more information, please go to How to enable/disable a License from the Server?

Volume license update: /vl /update

Syntax:

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

Description:

Command vl /update is used to update the users of a volume license.

Parameters:

- licensekey : license key to update, in this format: AAAA-BBBB-CCCC-DDDD
- /users : any number from 1 to 50, or “unlimited”

Examples:

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

For more information, please go to How to Update the Users of a Volume License from the Server?

Display remaining license credits for a Volume License key: /vl /credits-license

Syntax:

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

Description:

Command vl /credits-license is used to display the remaining license credits associated with a Volume License key.

Parameters:

- licensekey : Volume License key, in this format: AAAA-BBBB-CCCC-DDDD
- /login : provide the login of the partner associated with the Volume License key
- /edition : provide the optional edition parameter for Advanced Security and Server Monitoring products
- /silent : executes the command silently

The output will be stored in the user-level environment variable named VOLUME_LICENSE_CREDITS . It may be required to read the value of VOLUME_LICENSE_CREDITS from a different process, using the command echo %VOLUME_LICENSE_CREDITS% .

Examples:

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

For more information, please go to How to display the remaining license credits for a Volume License key?

Display remaining support credits for a Volume License key: /vl /credits-support

Syntax:

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

Description:

Command vl /credits-support is used to display the remaining support credits associated with a Volume License key.

Parameters:

- licensekey : Volume License key, in this format: AAAA-BBBB-CCCC-DDDD
- /login : provide the login of the partner associated with the Volume License key
- /edition : provide the optional edition parameter for Advanced Security and Server Monitoring products
- /silent : executes the command silently

The output will be stored in the user-level environment variable named VOLUME_LICENSE_CREDITS . It may be required to read the value of VOLUME_LICENSE_CREDITS from a different process, using the command echo %VOLUME_LICENSE_CREDITS% .

Examples:

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

For more information, please go to How to display the remaining support credits for a Volume License key?

2FA - reset: /resetuser

Syntax:

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

Description:

Command /resetuser is used to reset 2FA users, instead of doing it through the user interface (this can be done here in the interface: TwoFactor.Admin > Manage Users > Reset)

Parameters:

- user1 user2 ... userN : the domain names of the users you want to reset (separated by simple space)

Examples:

TwoFactor.Admin.exe /resetuser johndoe jackrussell chuckbartowski

For more information, please go to Reset Configuration for Users

---

2FA - add users: /addusers

Syntax:

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

Description:

Command /addusers is used to add several 2FA users, instead of doing it through the user interface, user by user (this can be done here in the interface: TwoFactor.Admin > Manage Users > Add User)

Parameters:

- userInfos1 userInfos2 ... userInfosN

: the user infos of the users you want to add. These infos consist of the following fields, separated by a semi-colon:

- domainName (mandatory): the domain Name of the user to add
- receivedMethod (optional): the method to receive confirmation codes. Has to be one of these values: SMS, App, Email or LetTheUserChoose. App is the default value.
- mobilePhone (optional): the phone of the user to add
- email (optional): the email of the user to add

Examples:

TwoFactor.Admin.exe /addusers johndoe jackrussell;LetTheUserChoose chuckbartowski;Phone; +33101010101; abcd@efgh.com samanthacarter;Email;;

For more information, please go to Add Users and Groups

2FA - add groups: /addgroups

Syntax:

TwoFactor.Admin.exe /addgroups [group1] [group2] … [groupN]

Description:

Command /addgroups is used to add several 2FA groups, instead of doing it through the user interface, group by group (this can be done here in the interface: TwoFactor.Admin > Manage Users > Add Group)

Parameters:

- group1 group2 ... groupN : the names of the groups you want to add.

Examples:

TwoFactor.Admin.exe /addgroups group1 group2 group3

For more information, please go to Add Users and Groups

2FA - list users: /getusers

Syntax:

TwoFactor.Admin.exe /getusers

Description:

Command /getusers is used to get a list of all users/groups configured into 2FA administration console. A json representation of this list of users/groups is returned, and can be used for example in a Powershell script.

This list can be seen here in the interface: TwoFactor.Admin > Manage Users.

Parameters:

None

2FA - add groups: /deleteuser

Syntax:

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

Description:

Command /deleteuser is used to remove a user from 2FA configuration (this can be done here in the interface: TwoFactor.Admin > Manage Users > Remove)

Parameters:

- domainName : the name of the user or the group to remove.
- userType : the type of object to delete. Its value must be “user” or “group”

Examples:

TwoFactor.Admin.exe /deleteuser “This is a group name” group TwoFactor.Admin.exe / deleteuser administrator user

For more information, please go to Remove Users and Groups

Add or update credentials to the Windows Credentials Manager: /windowscredential-addorupdate

Syntax:

AdminTool.exe /windowscredential-addorupdate

or

AdminTool.exe /windowscredential-addorupdate csvFilePath

Description:

Command /windowscredential-addorupdate is used to add new Windows credentials to the Windows Credentials Manager, or update existing ones. You can provide credentials individually by specifying the domain, username, and password, or process multiple entries in bulk from a CSV file.

This command is useful to configure external authentication via SAML for the Web Portal with SSO.

Parameters:

- **Single credential mode**
  - domain (mandatory): the user's domain name if part of an Active Directory, or the machine name if the user is a local user
  - username (mandatory): the Windows account username
  - password (mandatory): the Windows account password
- **Bulk mode (CSV file)**
  - csvFilePath (mandatory): the path to a CSV file containing one or more credentials to add or update

Examples

For an Active Directory user:

AdminTool.exe /windowscredential-addorupdate COMPANY johndoe SecurePassword123

For a local user:

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

To bulk add or update credentials from a CSV file:

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

---

Remove credentials from Windows Credentials Manager: /windowscredential-remove

Syntax:

AdminTool.exe /windowscredential-remove username

or

AdminTool.exe /windowscredential-remove csvFilePath

Description:

Command /windowscredential-remove is used to remove Windows credentials. You can remove a single credential by specifying the target, or remove multiple credentials in bulk using a CSV file

Parameters:

- **Single credential mode:**
- target (mandatory): the target name for the credential, typically a domain or server name
- **Bulk mode (CSV file):**
  - csvFilePath (mandatory): the path to a CSV file containing usernames to remove. The file must exist

Examples:

AdminTool.exe /windowscredential-remove COMPANY

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

How to completely customize the Web Access Page beyond the Web Portal capabilities?

Overview

By using the Web Portal you can customize Terminal Service Plus Web Access Pages in an extensive way.

However, in some cases, this is not enough. In these cases, you can completely customize the Web Access Page, beyond the Web Portal capabilities, by modifying by yourself the Web Access Page generated by the Webmaster Toolkit.

Warning, this documentation is intended only for skilled Web developers.

Generating mandatory settings

In order to include the mandatory settings in your Web Access page, we recommend that you start by generating your Web Access Page by using the Web Portal.

Files location

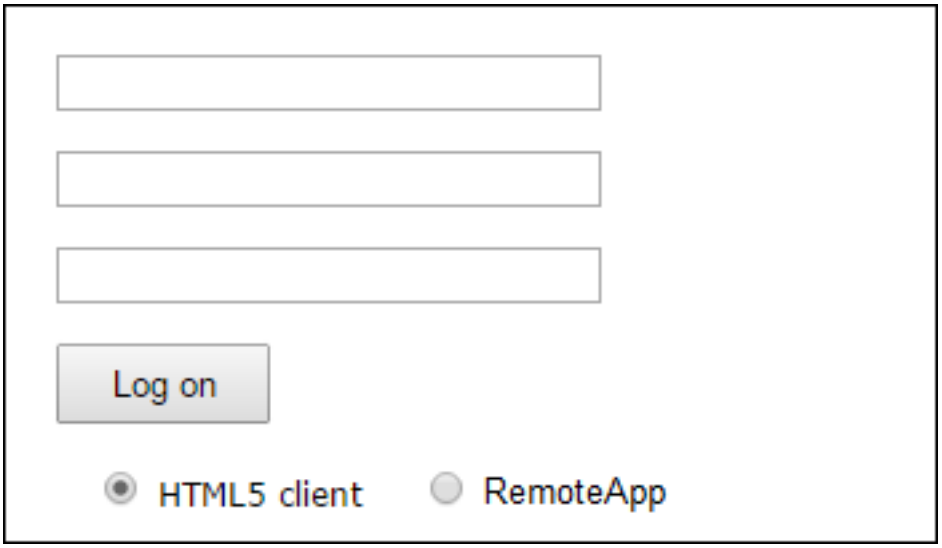
The Web Access Page will be generated in the “C:\Program Files (x86)\TSplus\Clients\www” folder, for instance if you choose “index” as the page name, it will be the file named “index.html” in this folder. It is a standard HTML file, so you can use all your knowledge of HTML, JavaScript and CSS programming languages to develop your custom page.

All the files inclusion are written relatively to the “C:\Program Files (x86)\TSplus\Clients\www” folder. For instance, the main CSS styles file is located at “C:\Program Files (x86)\TSplus\Clients\www\software\common.css”, so it is included in the HTML Web Access Page file by the following line:

Minimal Web Access Page

Starting from an HTML file generated by the Web Portal Preferences, we will reduce it down to a minimal Web Access Page. We advise you to use a text editor such as Notepad or Notepad++ (do not use Word).

After our work, it will look like the screenshot below:



First, you must keep everything that is between the and HTML tags:

- meta tags to force browsers to clear their cache
- .js files inclusions
- JavaScript settings declarations

Then, you can reduce the content between the ‘body’ and ‘/body’ HTML tags down to these few lines:

HTML5 client RemoteApp

Refresh the web page in your web browser, and you should get the minimal page of the above screenshot.

We recommend you clear your browser’s cache after saving any changed file.

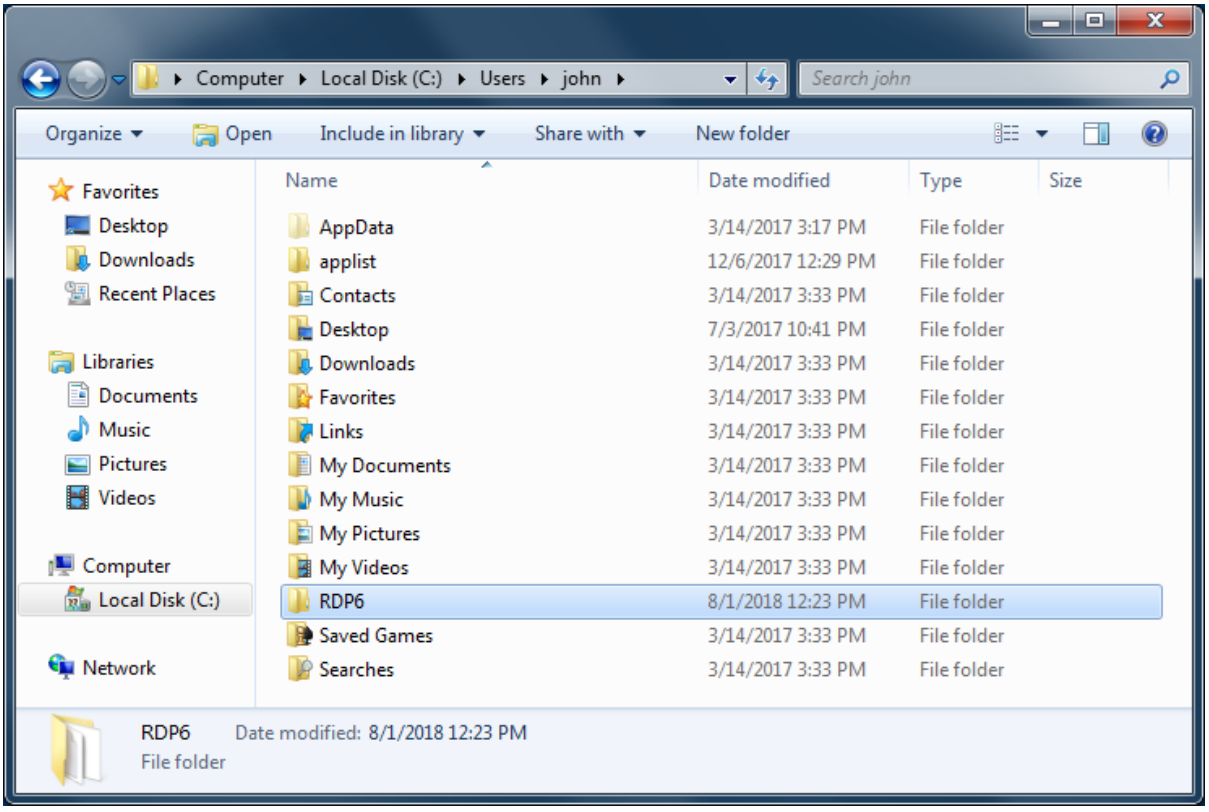
Finally, it is now up to you!

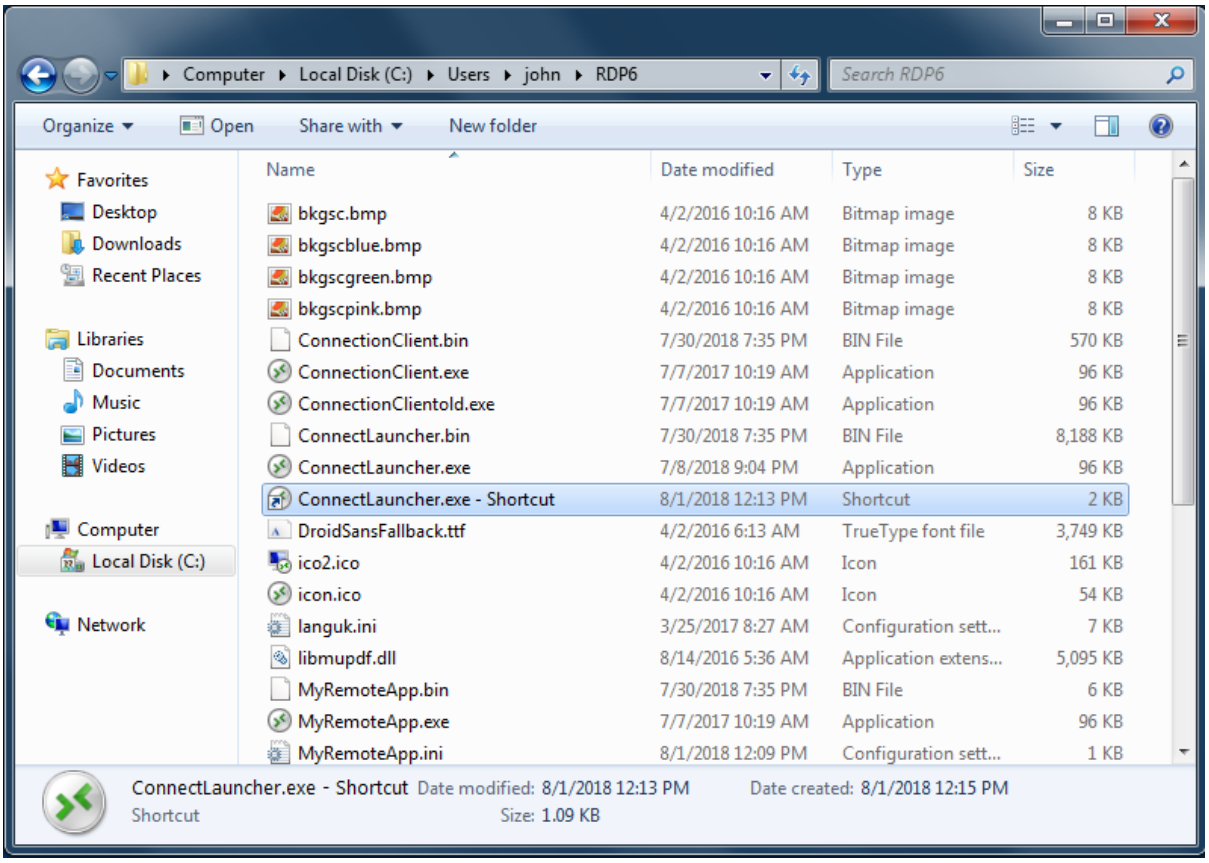
As long as you keep the calls to JavaScripts functions on specific events and the given identifiers (id=”…”), your fully customized Web Access Page will be working fine!

Edit or Delete the Parameters of a Generated Client

There are many reasons why you would want to change the parameters of your connection client: your TSplus server IP address changed, you need to add printer's redirection, to change the universal printer settings or so on…

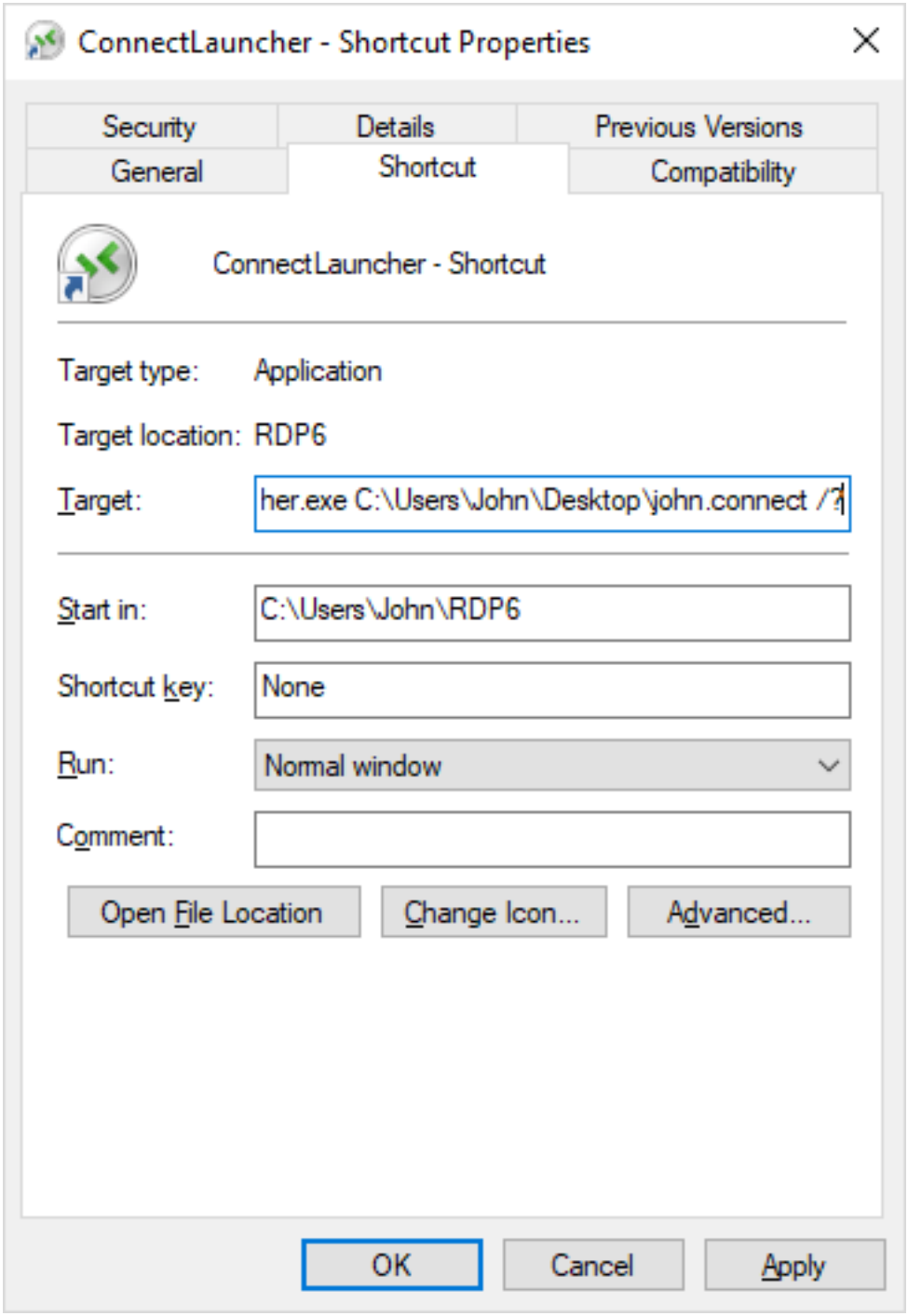
- You first need to create a shortcut of the ConnectLauncher.exe file, located on the RDP6 folder of the user's profile:



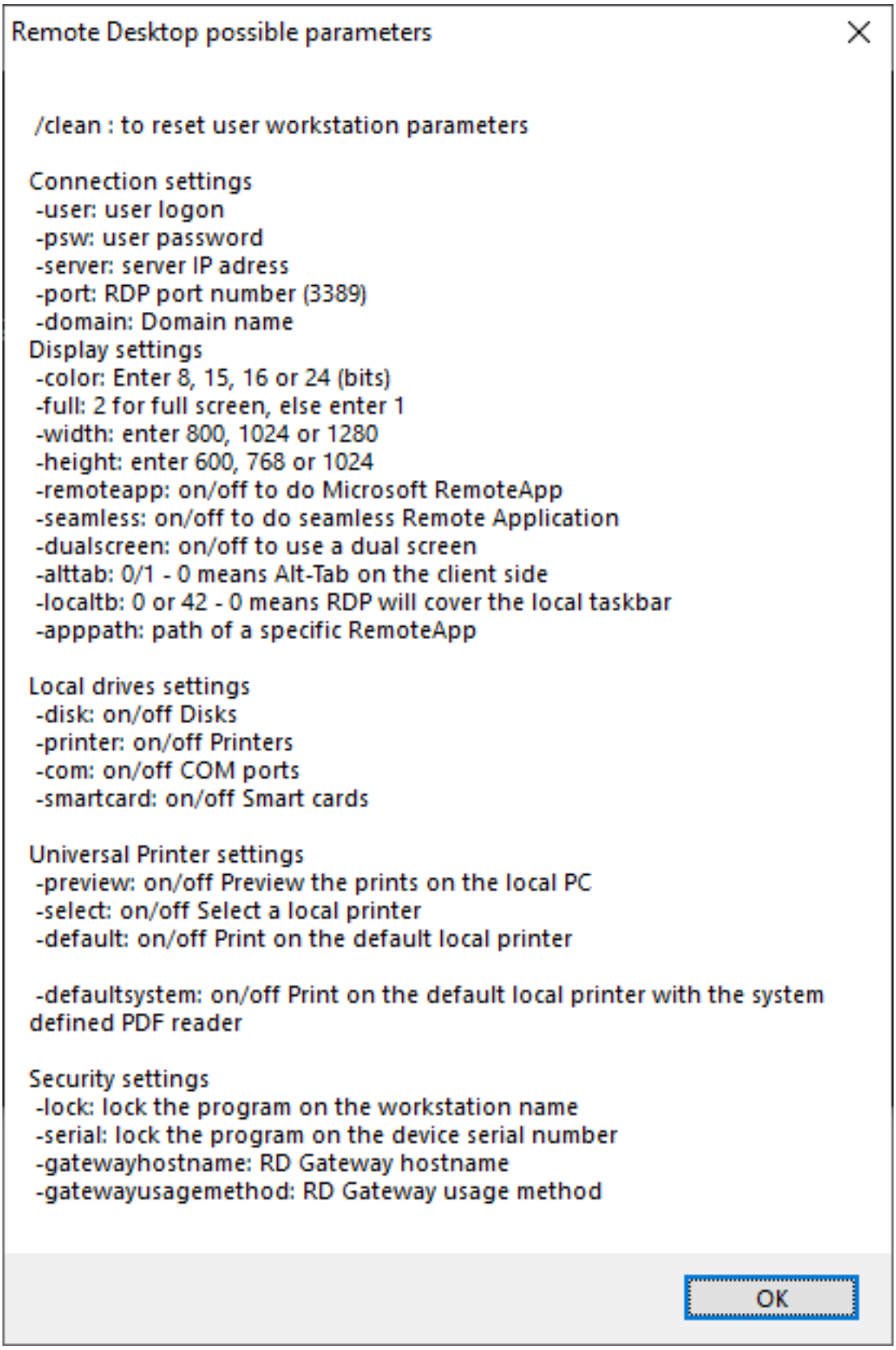


.

- Then, right click on it and hit properties. Place your mouse at the end of the “target” field and type in the client’s path followed by ”/?”, for example: “C: \Users\John\Desktop\clientname.connect /?”:

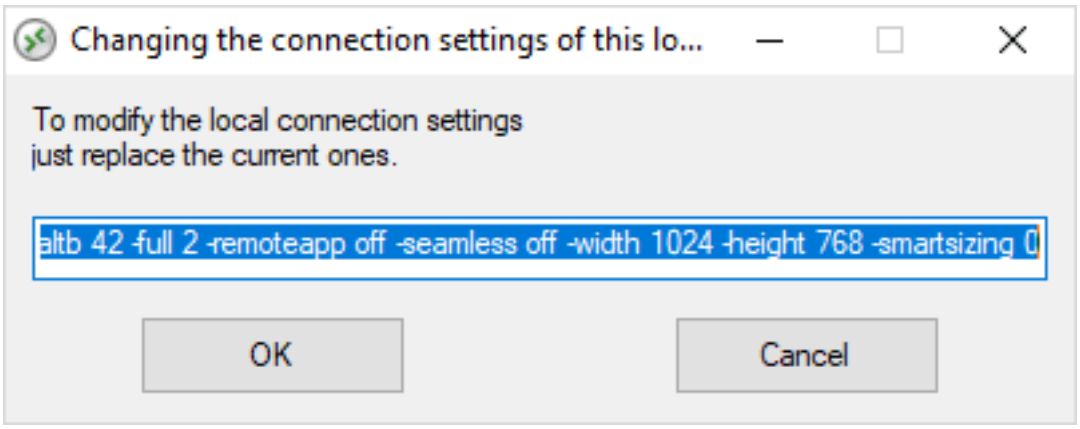


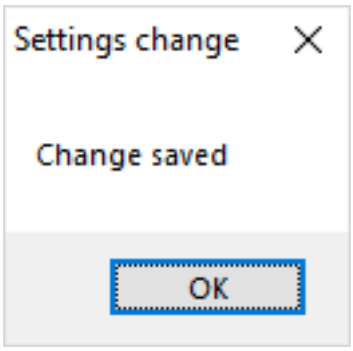
Now click OK and double click on the shortcut. A list of switch appears :



Click OK, the list of all the parameters appears in a small window.

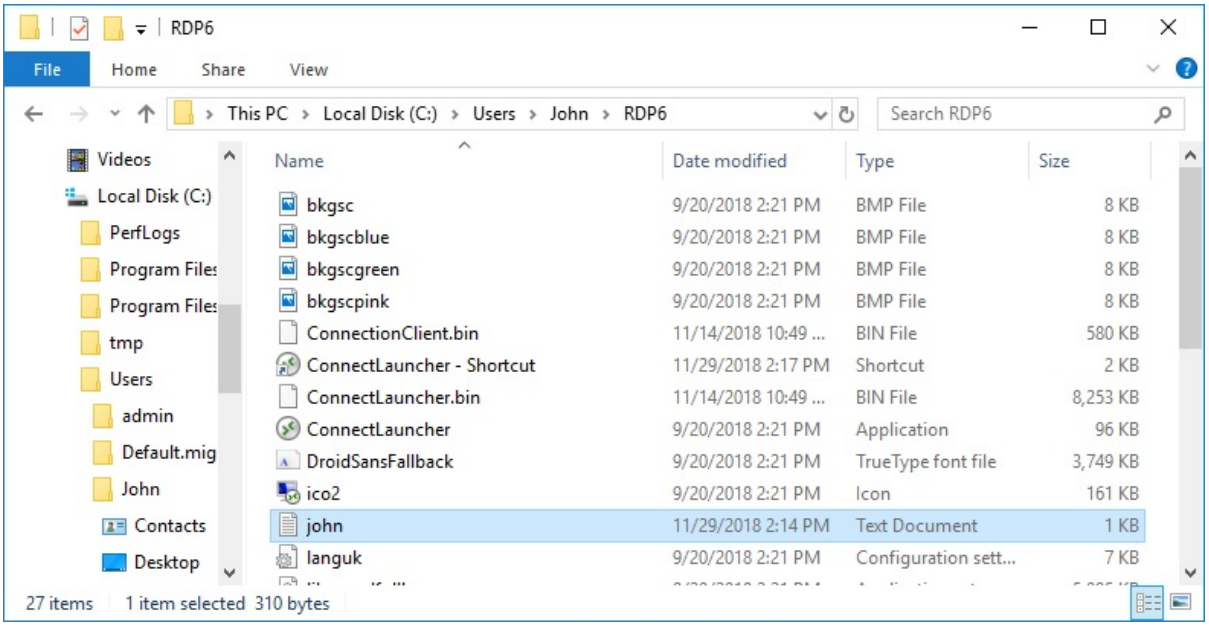
You can now edit them to match your preferences, you will need to log off and log on again to apply the changes.





Clean the Parameters of a Generated Client

After having launched the client at least once, you can clean the parameters by deleting the client.txt file located in the RDP6 folder:



Enable Windows Integrated Authentication on an Active Directory Domain

This guide is provided for configuring Windows Integrated Authentication (Kerberos/NTLM) with a Group Managed Service Account (gMSA) on the Web Portal.

Due to the unique nature of each company's network and architecture, we cannot provide support for issues arising from following this documentation. It meets the technical requirements for Web Portal with Windows Integrated Authentication, but implementation is at your own responsibility.

Domain configuration

The Active Directory environment must support Kerberos or NTLM authentication.

Set up a Managed Service Account (gMSA)

Install the Web Portal service and run it with a **domain managed service account** instead of a domain admin account.

Prerequisites

- Active Directory schema level: **Windows Server 2012** or later (required for gMSA)
- At least one domain controller running **Windows Server 2012** or later
- KDS root key created (one-time setup)
- Membership in **Domain Admins** or **Account Operators** to create the account

Create the KDS root key (if not already created)

Run on a domain controller in an elevated PowerShell session:

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

This makes the root key immediately available.

Create the gMSA

Use New-ADServiceAccount:

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

- Name: gMSA account name
- DNSHostName: FQDN for the account
- PrincipalsAllowedToRetrieveManagedPassword: computers/group allowed to use this gMSA

Grant administrative rights (optional / as needed)

By default, a gMSA has no special privileges.

To grant domain-level access (optional):

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

To grant local admin/logon capability (if needed):

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

Important: the trailing $ is required for gMSA account references in AD.

Reboot requirement

A reboot is required before continuing and installing/using the service account. Also refresh policies.

Install the gMSA on target servers

Run on each server that will use the gMSA:

Terminal window
Install-ADServiceAccount -Identity "WebPortalSvc"

Test installation:

Terminal window
Test-ADServiceAccount -Identity "WebPortalSvc"

Configure services to use the gMSA

1. Grant **Log on as a service** to the account:

   - Open Group Policy Editor
   - Go to: Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment
   - Open Log on as a service
   - Add DOMAIN\WebPortalSvc$

2. Ensure NTFS permissions on Web Portal files/folders:

   - Right-click application folder/executable > Properties > Security
   - Add DOMAIN\WebPortalSvc$
   - Grant at least **Read & Execute** (or **Full Control** if required by your deployment)

3. Configure service identity:

   - Account: DOMAIN\WebPortalSvc$
   - Password: **leave blank**

Configure Service Principal Name (SPN)

The web service must be registered in Kerberos.

Run on a domain controller:

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

Replace with your server FQDN and account.

If the Web Portal hosting server uses HTTP.sys, register SPN against the machine account:

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

Configure network on the client machine

To put a domain-joined client in the correct subnet:

1. Identify the correct network interface
2. Remove existing static IP (if incorrect)
3. Assign static IP, subnet mask, and default gateway matching DNS/DC subnet
4. Set DNS server addresses

Important: assign static IP addresses to domain controller and clients. Security policy synchronization requires machines to be in the same subnet in this context.

Allow required client connectivity

UDP/TCP 53 may be blocked, which prevents DNS queries.

Troubleshooting steps

Check DNS server status

On domain controller:

Terminal window
net start DNS

Verify DNS service is running.

Verify DNS server IP

On client:

Terminal window
ipconfig /all

Confirm DNS server IP matches the domain controller IP.

Test basic connectivity

On client:

Terminal window
ping <DC_IP_Address>

If ping fails, troubleshoot network/firewall routing.

Check firewall rules

Ensure inbound/outbound UDP/TCP 53 is allowed on client and server.

Test with nslookup

Terminal window
nslookup domain.com <DC_IP_Address>

If this works, default DNS server may be misconfigured or unreachable.

Review Event Viewer

On the domain controller, check DNS-related errors.

Configure Mozilla Firefox for Windows Integrated Authentication

Firefox does not use WIA by default.

Step 1: trusted negotiate URIs

1. Open Firefox
2. Go to about:config
3. Accept warning
4. Set
   network.negotiate-auth.trusted-uris
   to your domains, for example:
   - intranet.domain.com, domain.com

Step 2: trusted NTLM URIs

Set network.automatic-ntlm-auth.trusted-uris to the same domain list.

Step 3: Kerberos delegation URIs (if required)

Set network.negotiate-auth.delegation-uris, for example:

- domain.com

Step 4: restart browser

Restart Firefox to apply changes.

Configure Google Chrome for Windows Integrated Authentication

Chrome uses Windows/system authentication settings.

Via Group Policy (recommended)

1. Download Chrome ADMX templates:
   - https://chromeenterprise.google/policies/

2. Copy
   chrome.admx
   and
   chrome.adml
   to:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\en-US

3. Open gpedit.msc
4. Go to:
   - Computer Configuration > Administrative Templates > Google > Google Chrome

5. Enable integrated authentication for intranet sites and configure trusted sites:
   - intranet.domain.com, domain.com

6. Apply policy:

Terminal window
gpupdate /force

Other methods

Other methods (Chrome command line switches and flags) were not successful in this context.

Configure Microsoft Edge for Windows Integrated Authentication

Edge uses Microsoft Edge policies and Windows security zone settings.

Enable automatic logon in intranet zone

1. Open Internet Options
2. Security tab > Local Intranet > Custom Level
3. Under
   User Authentication
   , set:
   - Automatic logon only in Intranet zone

Configure Edge policies via GPO

Step 1: install Edge ADMX templates

1. Download:
   - https://www.microsoft.com/en-us/edge/business/download

2. Copy
   msedge.admx
   and
   msedge.adml
   to:
   - C:\Windows\PolicyDefinitions
   - C:\Windows\PolicyDefinitions\en-US

Step 2: edit policy settings

1. Open gpedit.msc
2. Go to:

- Computer Configuration > Administrative Templates > Microsoft Edge

3. Enable:
   - Configure the list of servers that Microsoft Edge can delegate credentials to

4. Configure trusted servers:
   - intranet.domain.com, domain.com

Step 3: apply policies

Terminal window
gpupdate /force

Other methods

Other methods (Edge command line switches and flags) were not successful in this context.

Troubleshooting integrated authentication

Check Kerberos tickets

On Windows client:

Terminal window
klist

You should see a ticket for HTTP/webserver.domain.com.

Clear cached credentials/tickets

Terminal window
klist purge

Verify SPN registration

On domain controller:

Terminal window
setspn -L serviceaccount

Ensure HTTP/webserver.domain.com is listed.

Debug Kerberos in Firefox

Start Firefox with logging:

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

Review firefox.log for authentication errors.

Check Chrome policies

In Chrome, open:

chrome://policy

Ensure AuthServerWhitelist and AuthNegotiateDelegateWhitelist are applied.

Check Edge policies

In Edge, open:

edge://policy

Ensure AuthServerWhitelist and AuthNegotiateDelegateWhitelist are applied.

End of Life Version 1-12

Remote Access v12 (and all older versions) will stop functioning on all Windows computers. Service interruptions will begin in January 2026 and gradually extend until complete shutdown in April.

Updating to an LTS version or the latest version requires an **active support subscription** for your license. If this is not the case, we invite you to subscribe to a support subscription from your license portal and update your license from your Admintool with your .LIC file to benefit from the update.

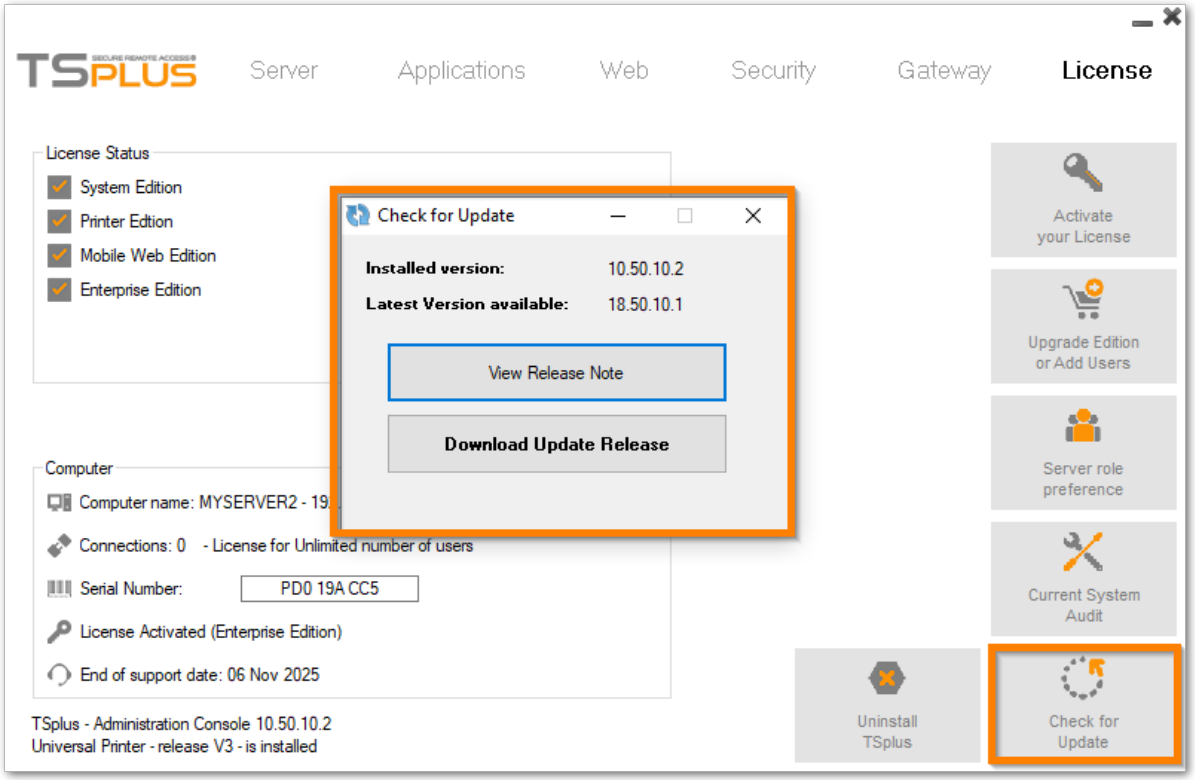
If you are unable to add a support subscription or receive an error message,
contact us using our Contact Support, providing:

- Your license number in the format PXX XXX XXX (Visible in the license tab of the Admintool)
- Your license purchase invoice
- Your support subscription invoice

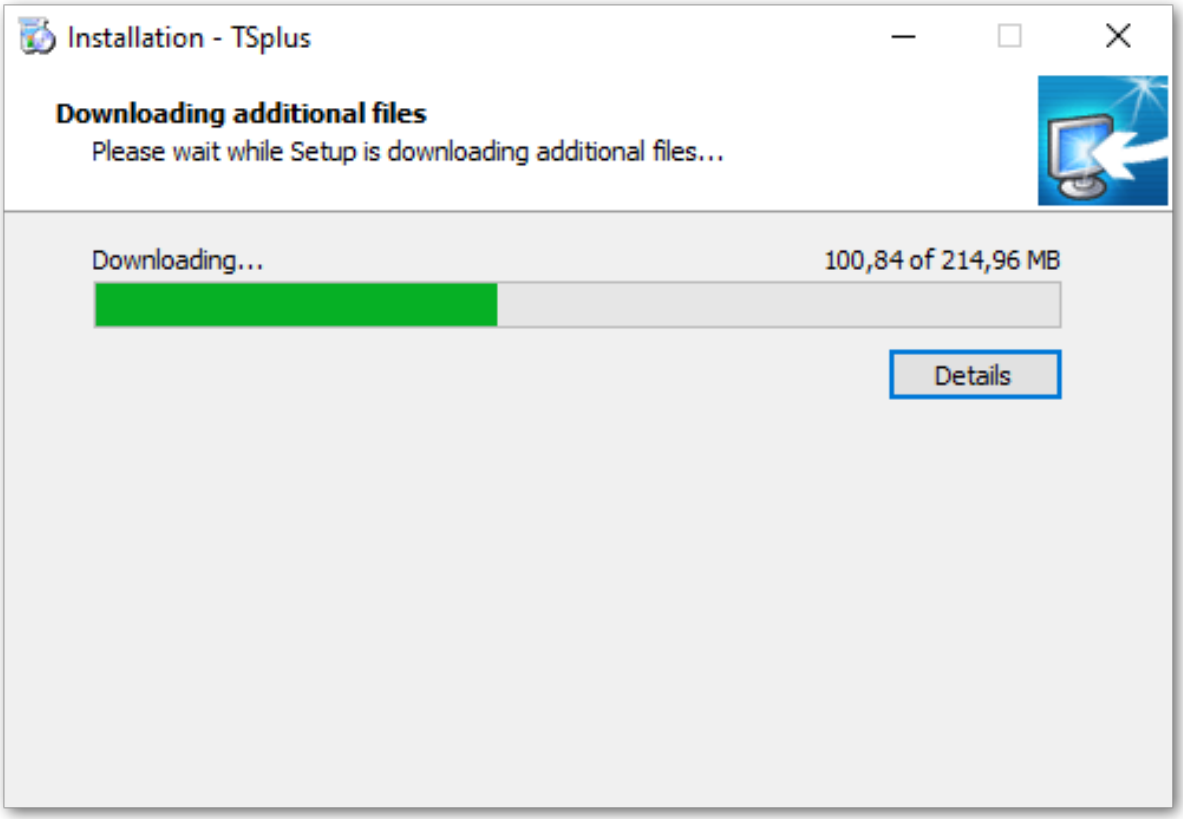
Updating Your Version v10

(If you want to install an LTS instead of the latest version, go to the page LTS)

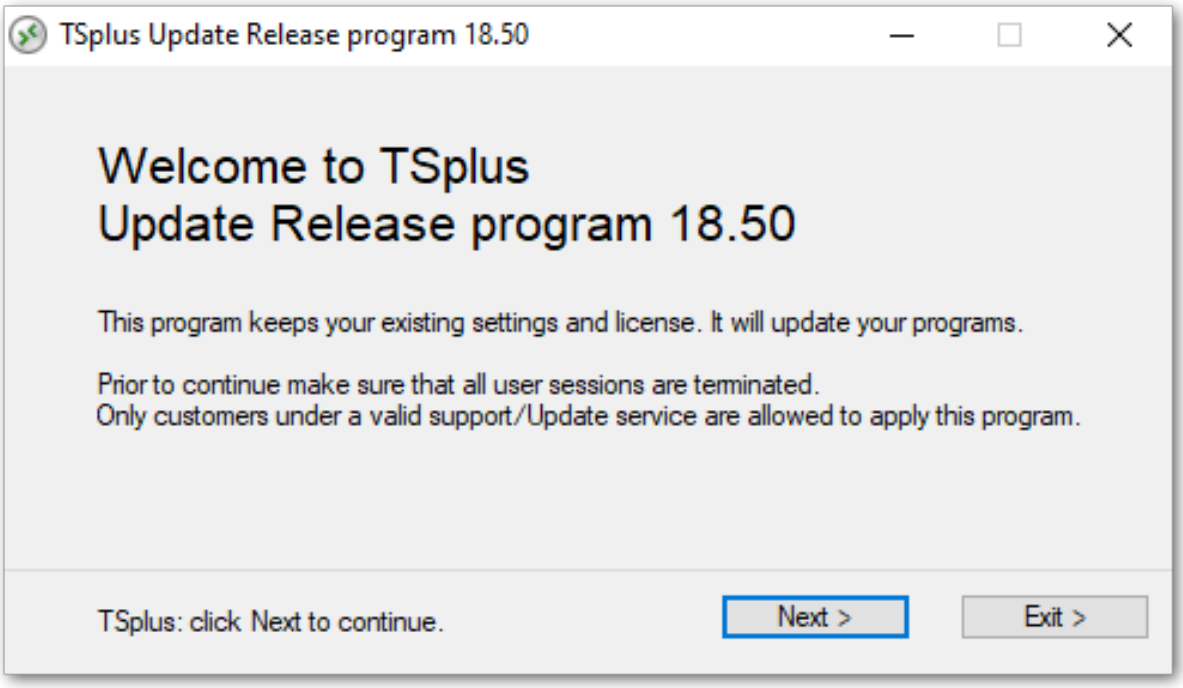
From your online version 10, click on the following field to download the **UpdateRelease.exe**
You can also download the UpdateRelease.exe to start the update procedure.



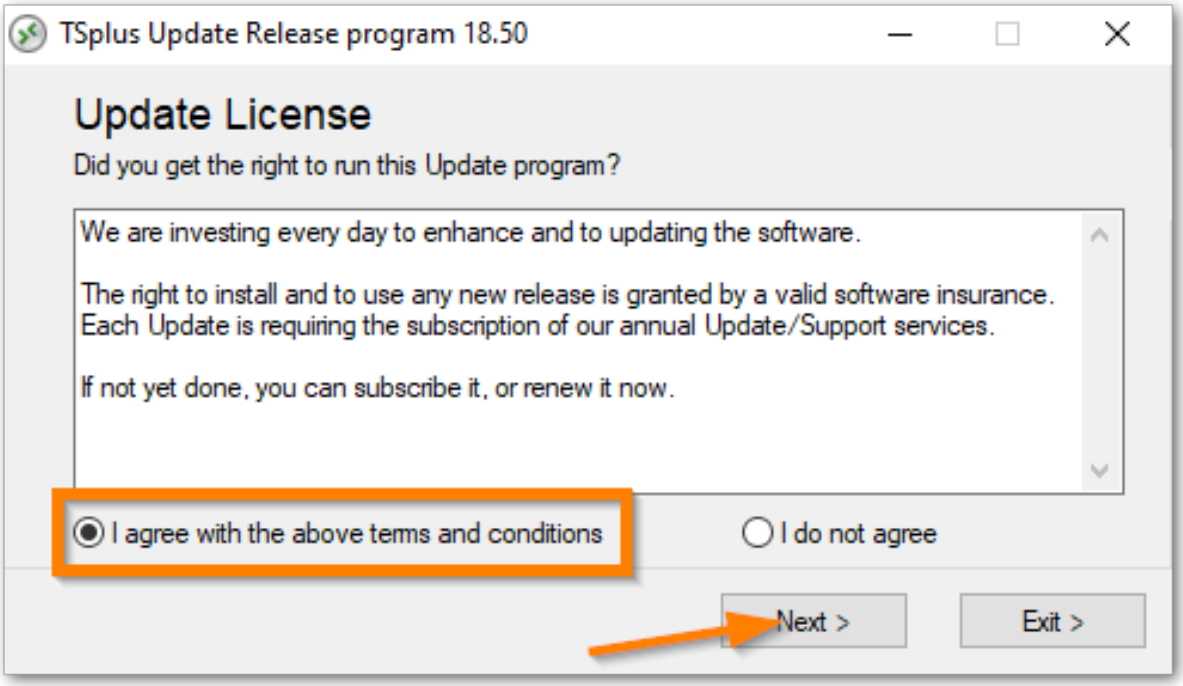
Download the updaterelease.exe and run the executable.



The update program will appear.



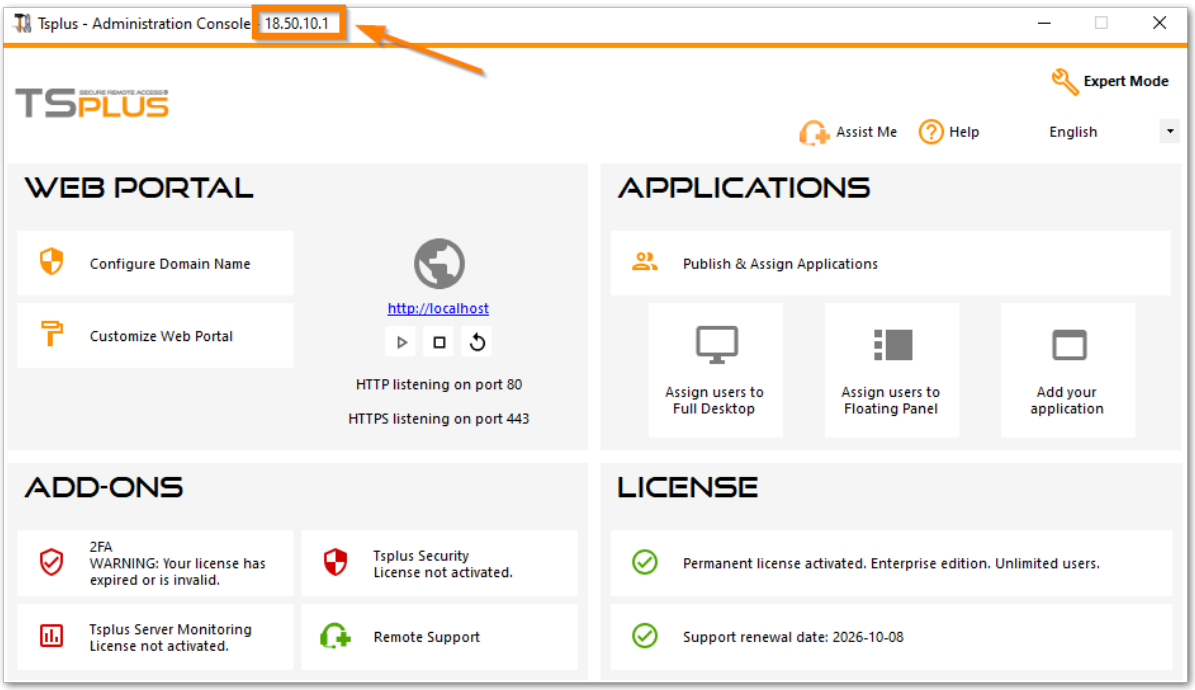
Accept the terms and click
NEXT



Follow all the steps and then restart your server at the end of the migration.

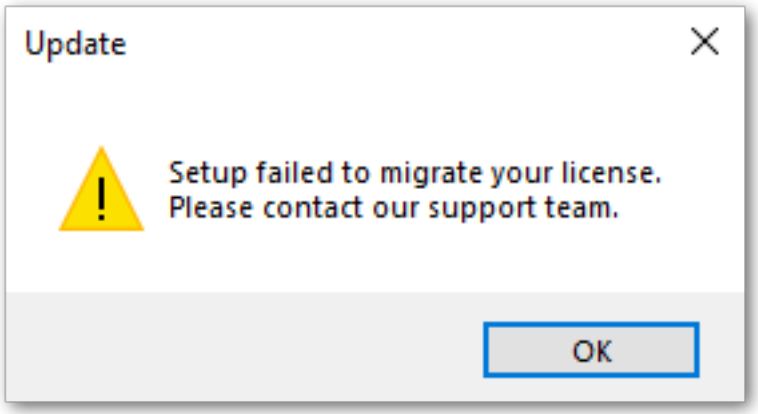
- When finished, **Restart your Server** to complete the update.

Launch the AdminTool. Congratulations, you are now on version 19.



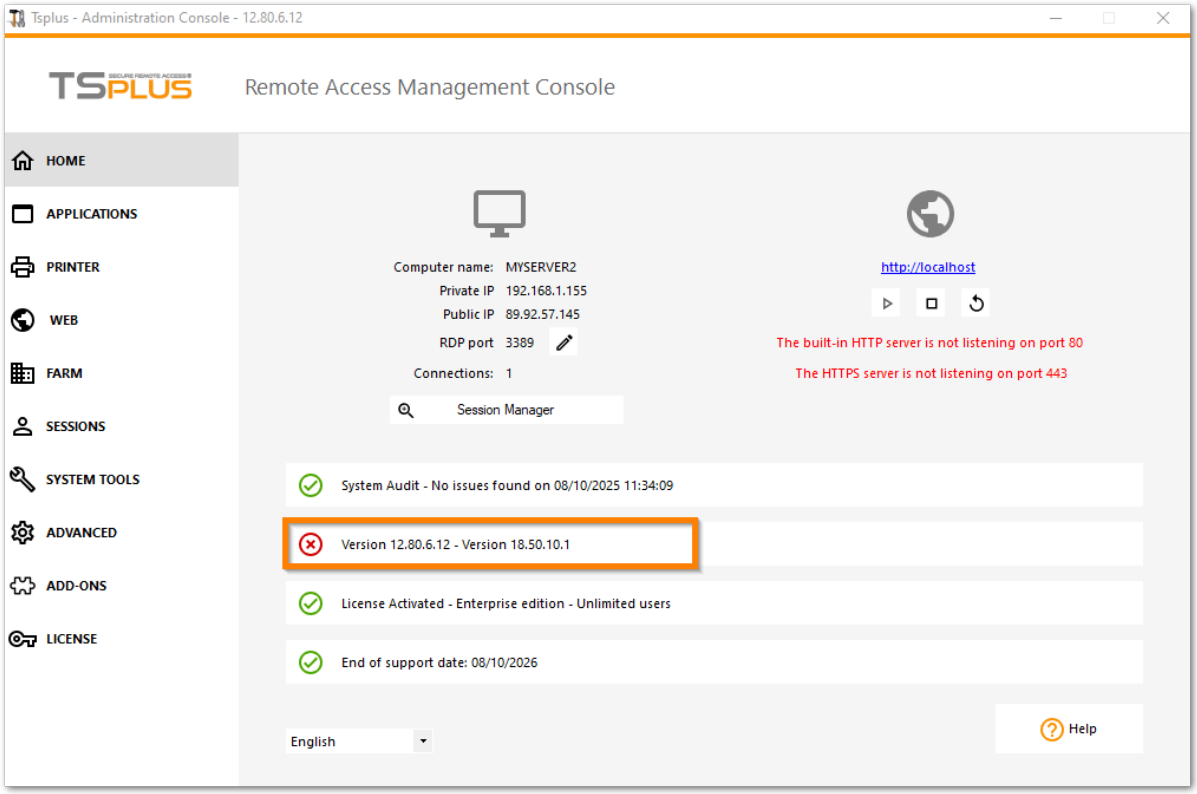
Error Message v10

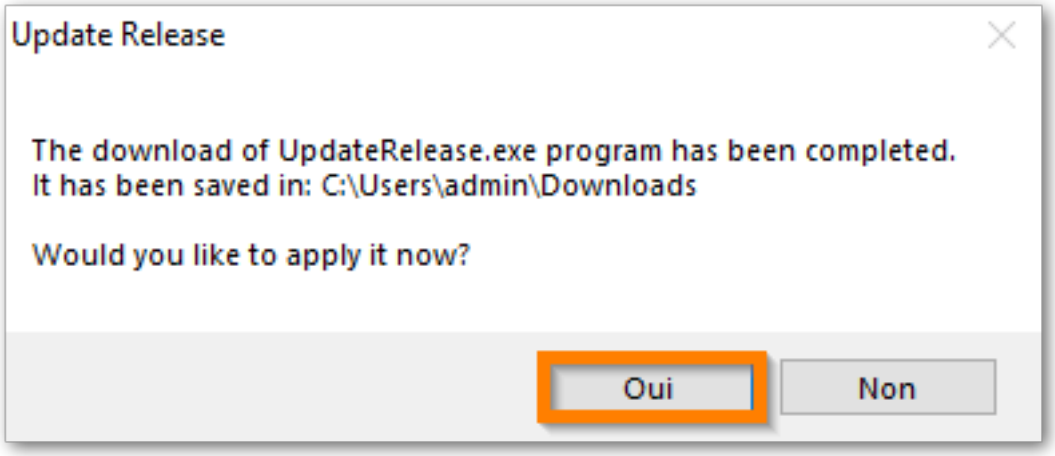
If you receive this error message,
Contact Support
to uninstall Remote Access. Please provide the license number in the format PXX XXX XXX and also proof of the support purchase invoice.

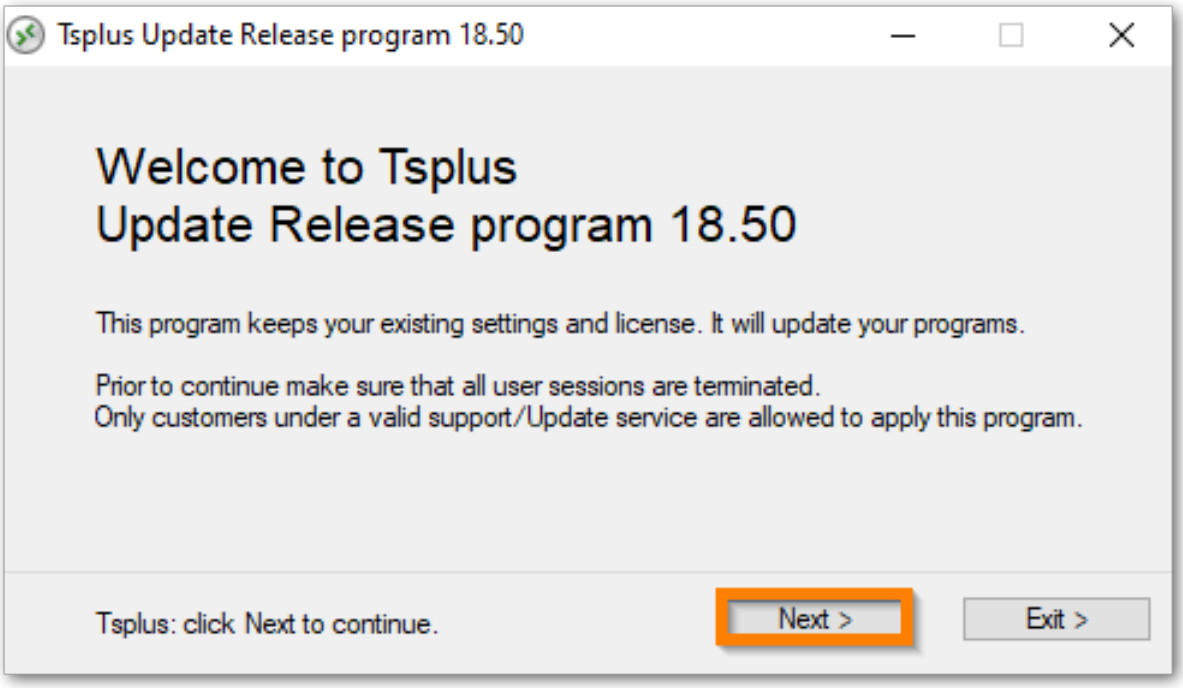


Updating Your Version v12

From your online version 12, click on the following field to download the **UpdateRelease.exe**
You can also download the UpdateRelease.exe to start the update procedure.

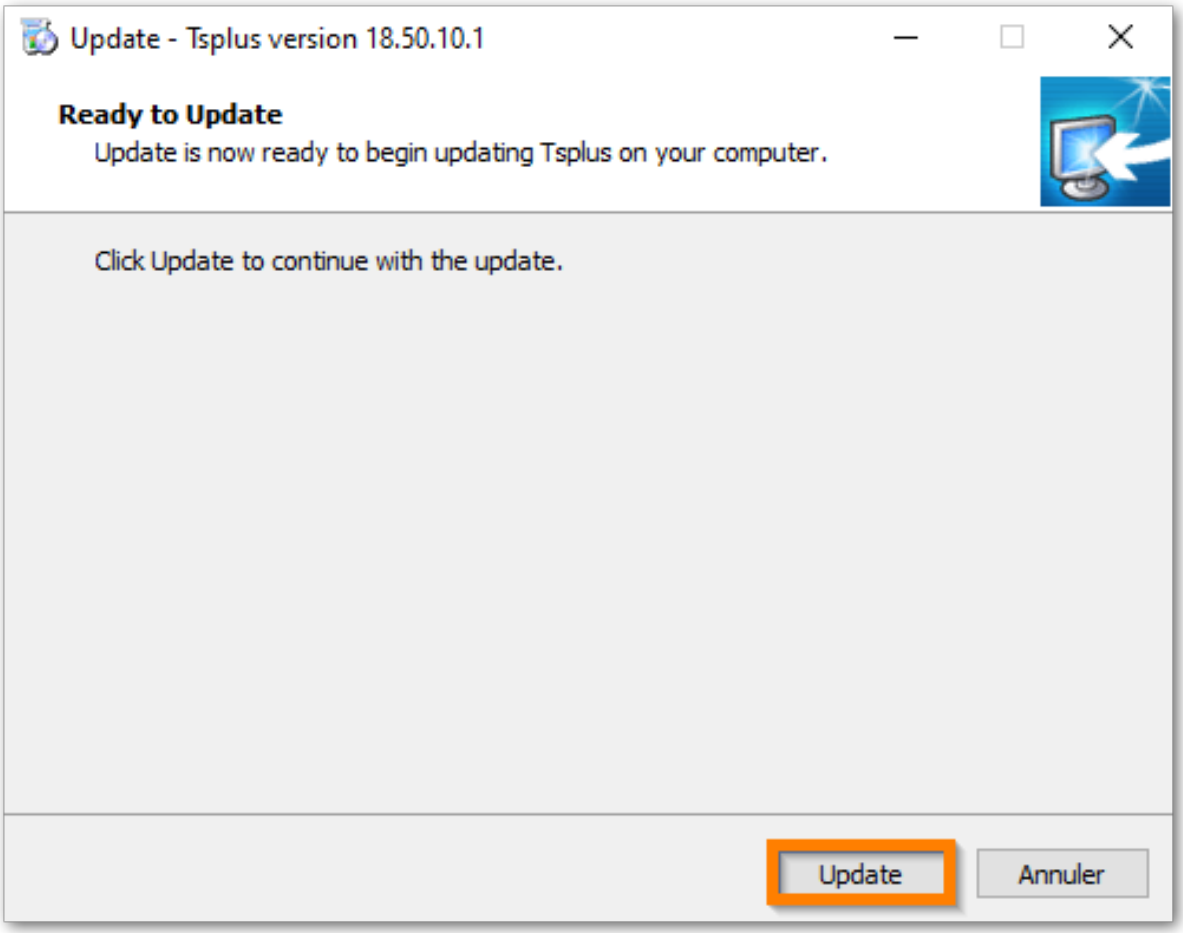

Tsplus - Administration Console - 12.80.6.12
TSPLUS
Remote Access Management Console
HOME
APPLICATIONS
PRINTER
WEB
FARM
SESSIONS
SYSTEM TOOLS
ADVANCED
ADD-ONS
LICENSE
Computer name: MYSERVER2
Private IP 192.168.1.155
Public IP 89.92.57.145
RDP port 3389
Connections: 1
Session Manager
http://localhost
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

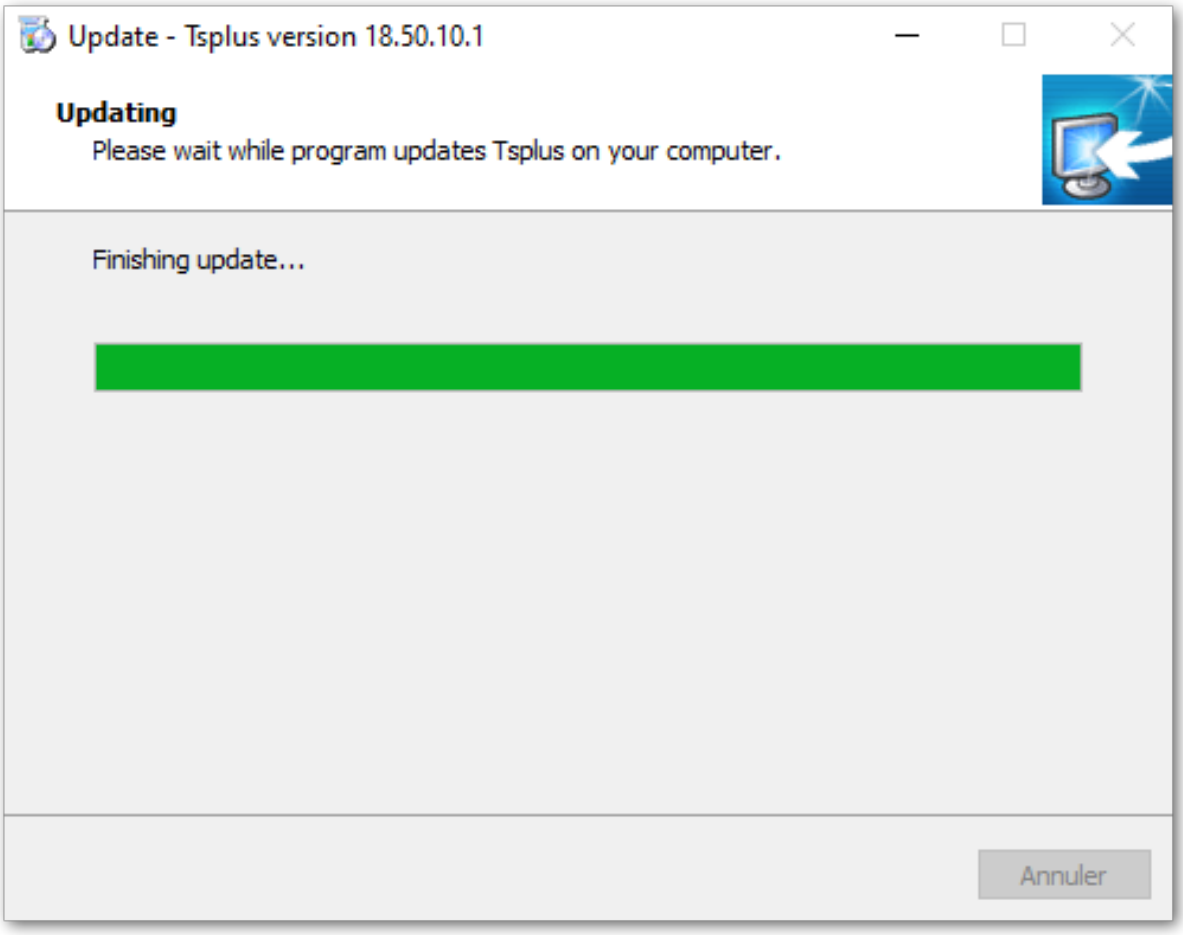

Update Release
The download of UpdateRelease.exe program has been completed.
It has been saved in: C:\Users\admin\Downloads
Would you like to apply it now?
Oui
Non



- Accept the terms and click NEXT

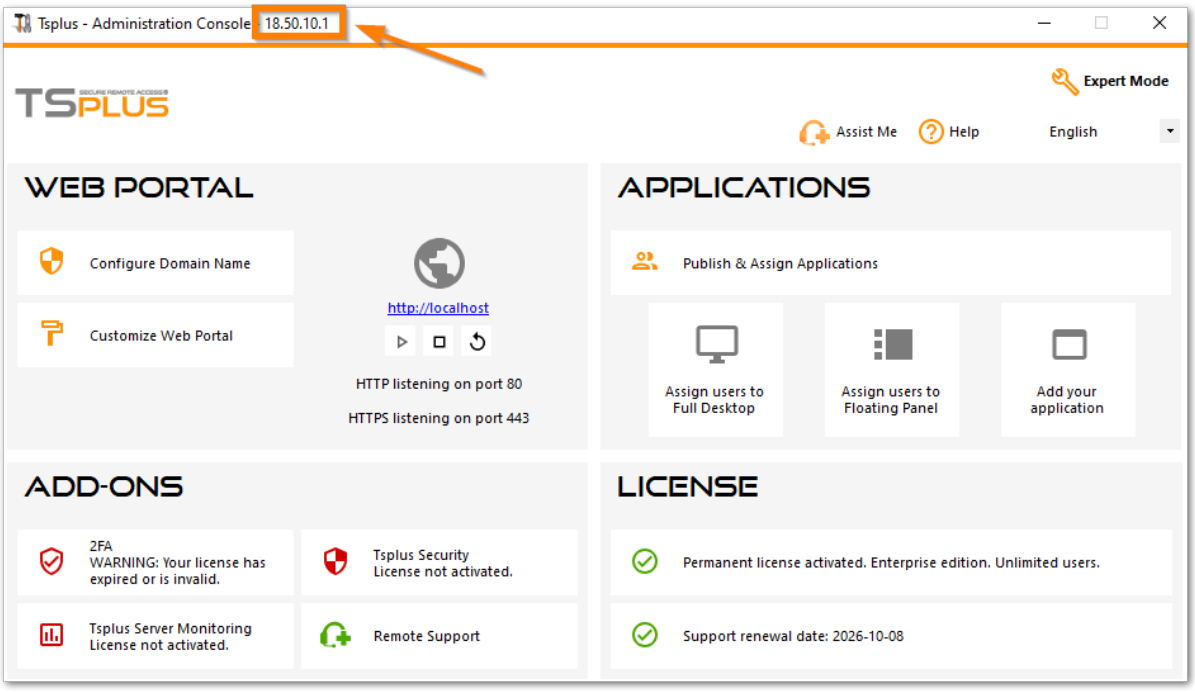
Once downloaded, click
Update
to start the process.





- When finished, **Restart your Server** to complete the update.

Launch the AdminTool. Congratulations, you are now on version 19.



Error Message v12

If you receive this error message, Contact Support to uninstall Remote Access.

Please provide the license number in the format PXX XXX XXX and also proof of the support purchase invoice.

Enforce HTTPS protocol

Standard Case

Starting from Terminal Service Plus version 9.20, you can redirect every web request which uses HTTP to the HTTPS secure protocol.

To activate this feature on a server, edit (or create) the file “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” and add the following line:

disable_http_only=true

Save the file and restart Terminal Service Plus web servers (AdminTool > Web > Restart Web Servers or reread configuration by accessing http://127.0.0.1/w0j3?settings.bin).

Once this feature is enabled, you can try to browse to the insecure web page at:

http://your-server

and it will automatically redirect your request to the secure Web Portal page at:

https://your-server

Special case: Custom Web Ports

If you are using a specific port to serve HTTPS, then edit the file “C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin” and use the following line instead of the line described above:

disable_http_only=“domain.com:4431”

where domain.com is your own server host name and 4431 is your HTTPS custom port.

Save the file and restart Terminal Service Plus web servers (AdminTool > Web > Restart Web Servers).

Once this feature is enabled, you can try to browse to the insecure web page at:

http://domain.com

and it will automatically redirect your request to the secure Web Portal page at:

https://domain.com:4431

Comment: Even if this is not secure but you wish to disable ssl/https on http port then edit the settings.bin file and add: disable_ssl_on_http=true, save and restart the servers.

Disable http on https

By default it is allowed to access https://my-domain.com, https://my-domain.com:80, http://my-domain.com:443 So it allows http on port 443 or allow https on port 80, it does not have impact on security and makes it easy to fallback to degraded xhr-connection when no websockets support is possible But if wished to disable it, edit the settings.bin file and add the following line:

disable_http_on_https=true

Then restart Terminal Service Plus web servers (AdminTool > Web > Restart Web Servers or reread configuration http://127.0.0.1/w0j3?settings.bin)

HTTPS Enforcement and Free SSL Certificate Validation

Please note that this HTTPS Enforcement feature is fully compatible with our Free SSL Certificate feature.

Enforce the use of web portal to connect to the server

Starting from Terminal Service Plus version 6.60, you can block/disable any attempt to connect using mstsc.exe (or any RDP clients) over the open/redirected port (80 or 443).

This feature only allows accesses from the Terminal Service Plus Web Portal and disables any other RDP connection on port 80/443.

To activate this feature on a server, edit the file C:\Program Files (x86)\TSplus\UserDesktop\files\AppControl.ini and add/modify the following variable:

[Security] Block_rdp_splitter=yes

Load Balancing

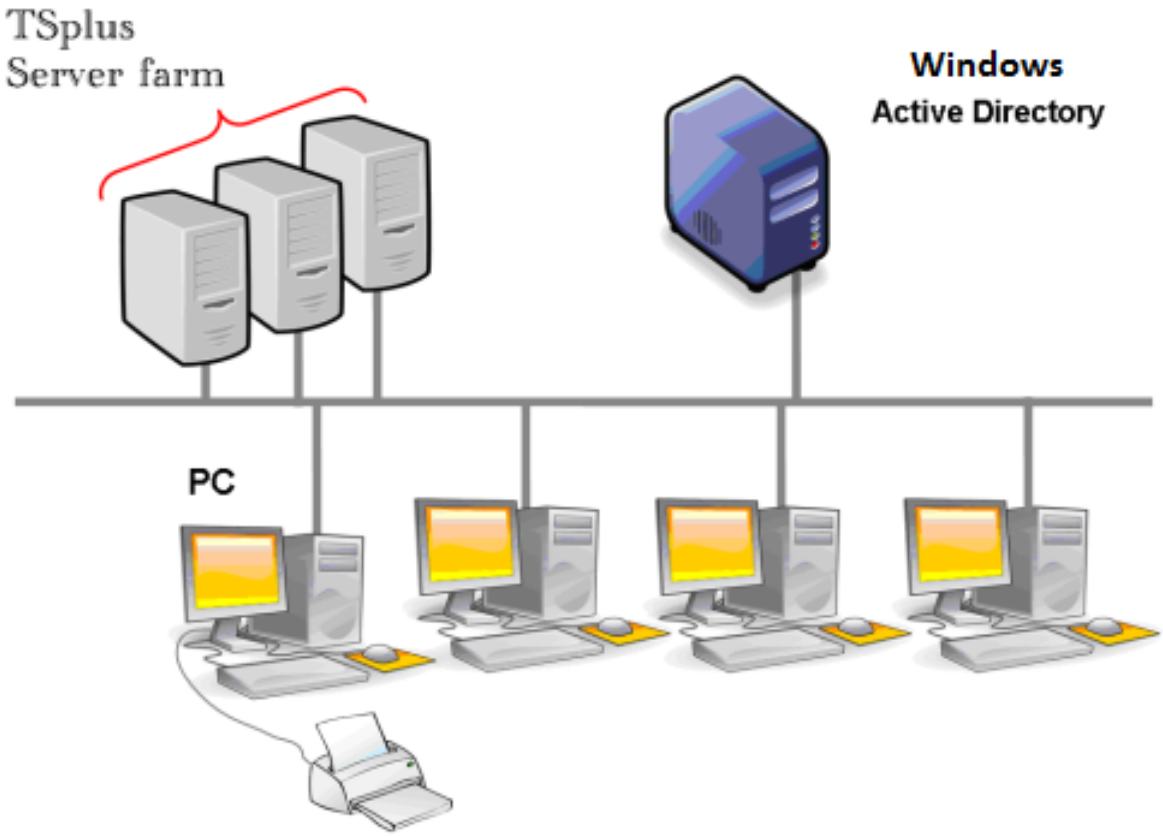
Pre-requisites

Using this feature, you will be able to manage a load balanced environment.

It means that the load of all your users will be distributed between your servers. The workload will be shared between all the servers of your farm.

Load Balancing enables to use an unlimited number of servers with load balancing, and is available with the Enterprise edition (one valid license per server). This very powerful and advanced capability is to be used when a large number of users/servers has to be deployed.

Important : Simply enabling Load Balancing will redirect users to the least loaded server of the farm regardless of any assigned servers configured for the users. If you intent to use Load Balancing AND Server Assignment, make sure to tick the checkbox “Load balance on assigned servers”



Usually we recommend using one server for 50 concurrent users.
You can exceed +50 users depending on the power of your server and the consumption of users' application resources.

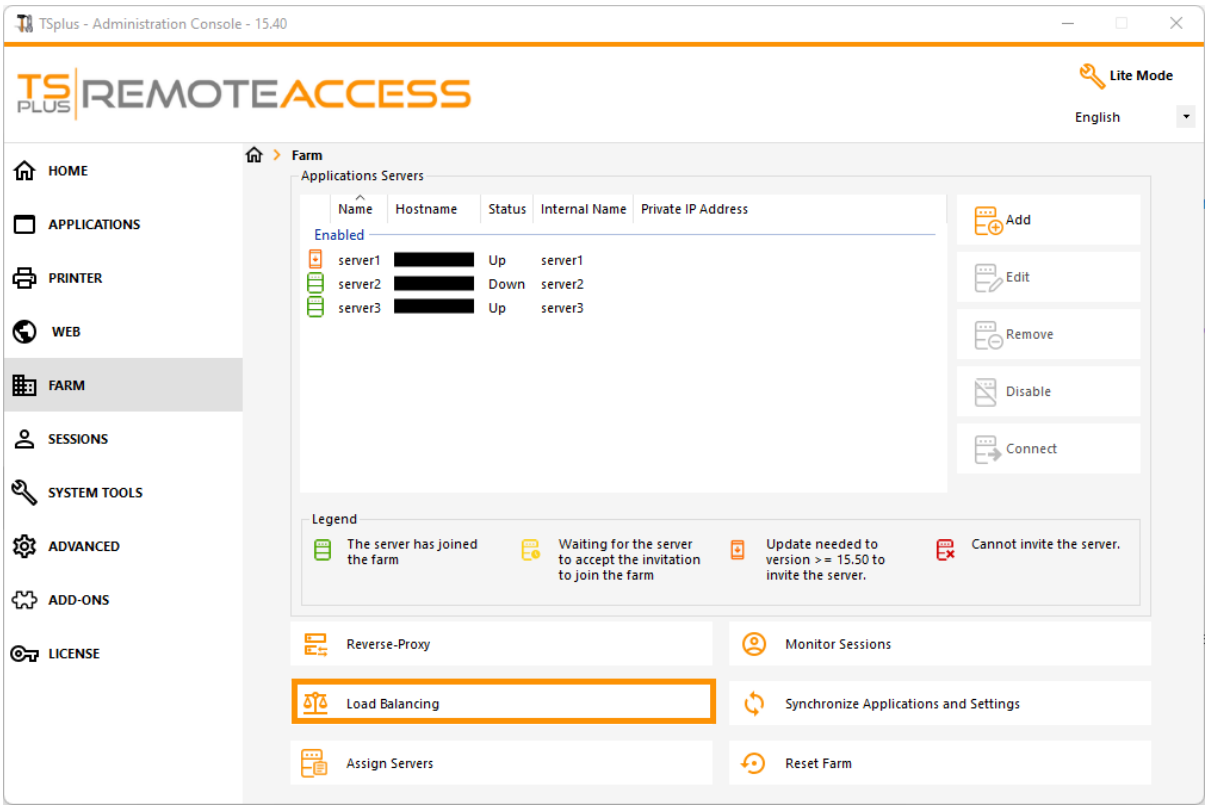
Generated Clients and Web Access

There are three ways to connect to a Load Balanced cluster:

- Using a **Generated Client** (executable program, created by the Portable Client Generator)
- Using a **Web Portal Access** by activating it on the Web Portal Preferences window.
- With the TSplus App from your mobile device.

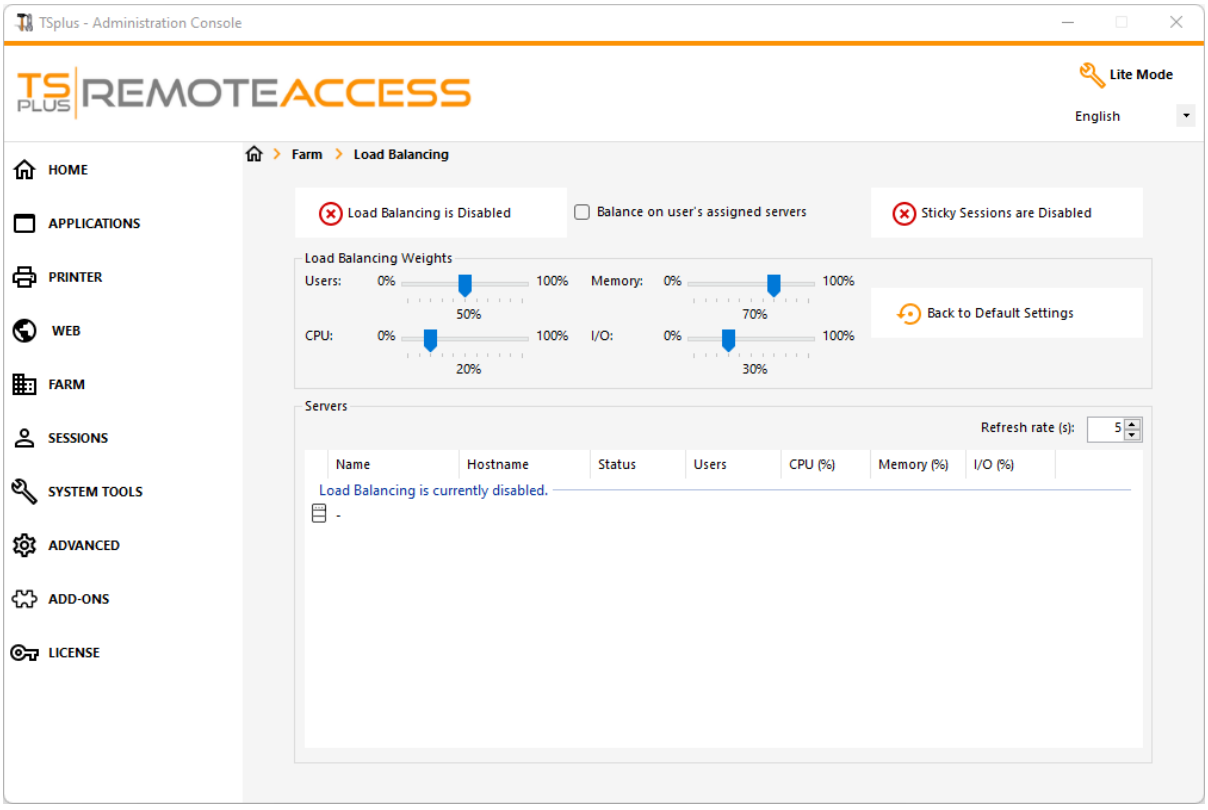
Load Balancing Main Window

The Load Balancing Manager can be found under the Farm Tab of the AdminTool:



This window allows you to configure Load Balancing. It lists all the servers in your Load Balanced server farm and allows you to enable, disable and configure the Load Balancing (more on this below).

Click on the buttons in the picture below to access the corresponding information:



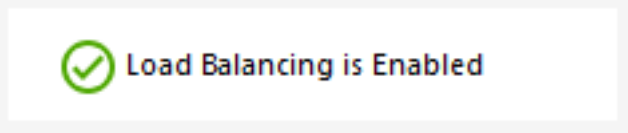
On top of the Load Balancing window, you will see a big button:

- This button displays the current state of the Load Balancing.
- If you click on it, it will enable or disable the Load Balancing depending on its current state.

Here is the button when the Load Balancing is **Disabled**. A click on it will activate it.



Here is the button when the Load Balancing is **Enabled**. A click on it will deactivate it.



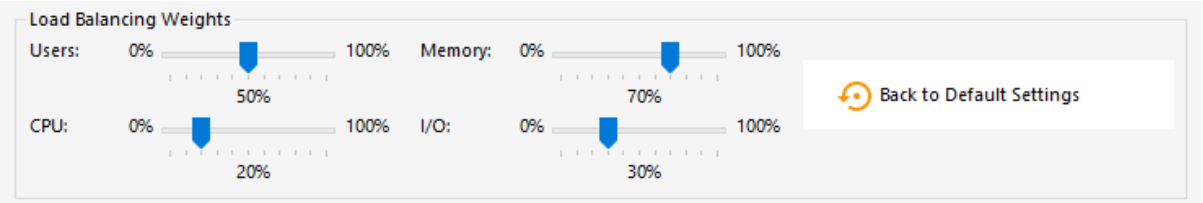
How does Load Balancing choose a server?

When Load Balancing is enabled, the user will be sent to the less loaded server at the time of his connection.

To determinate which is the less loaded server, the load of every server is computed using a weighted average between several performance indicators:

- number of connected users
- processor usage
- memory usage
- disk usage

You can modify the weight (importance) of these indicators by using the following sliders:



Using these sliders, you will be able to fine-tune the Load Balancing, and to optimize it to your own needs. For instance if your users launch a business application with big memory requirements, it might be a good idea to increase the impact of the RAM in the load computation using the “Memory” slider.

You can also reset these values by clicking on the “Back to Default Settings” button.

How is Server’s Load computed?

The load of each server is computed when needed in order to decide on which server the user must be sent.

For this computation, we use a **weighted average** between 4 hardware metrics.

The 4 sliders allow you to give more (or less) weight on each of these metrics, which are:

- Users : number of connected users
- CPU : percentage of non-idle processor time
- Memory : percentage of used memory
- I/O : percentage of non-idle disk time

For example, if you put the “Memory” slider on its right side and all the other sliders on their left side, the load of each servers will be computed using almost only the percentage of used memory - and your users will be sent to the server having the most available memory.

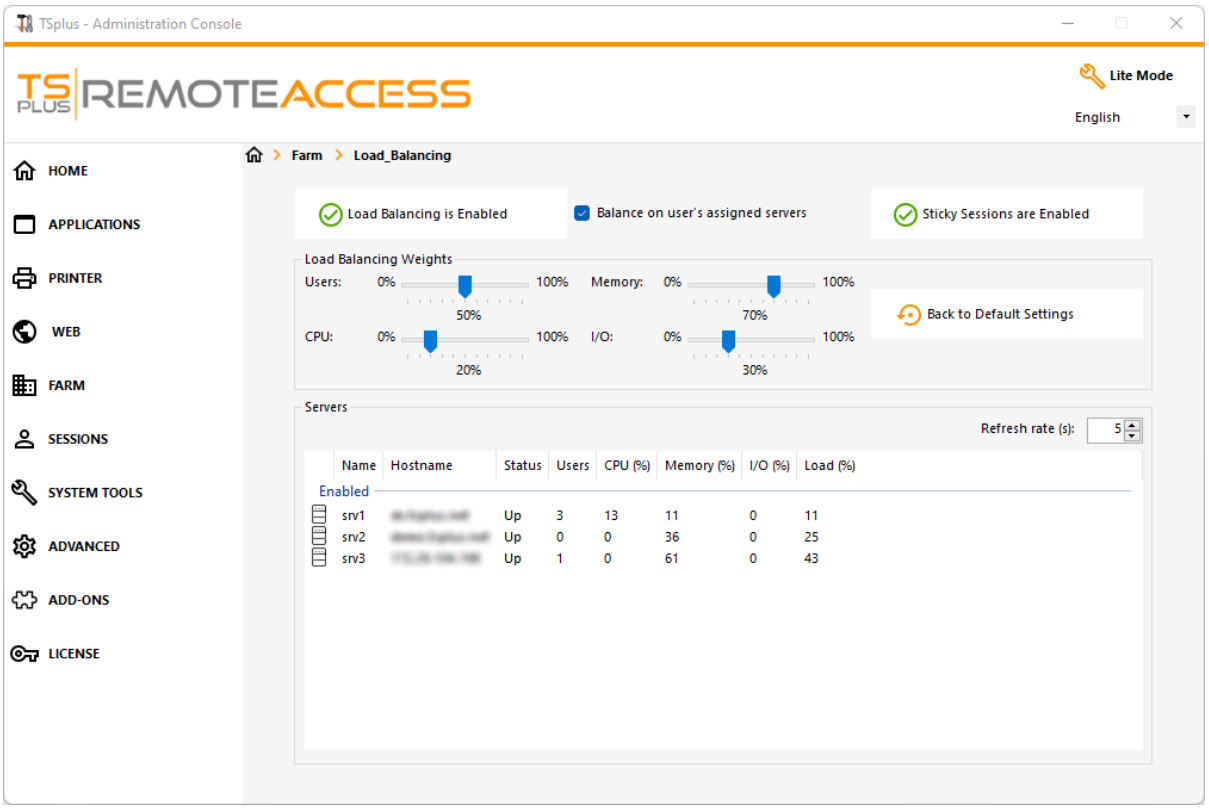
- When a slider is completely on the left, the weight used in load computation will be 1.
- When a slider is completely on the left, the weight used in load computation will be 100.

Moreover, the load of a given server depends on the ratio [used resources / total resources] ; so if a server A is twice as powerful as a server B, twice more users should be sent to server A than to server B (all other things being equals).

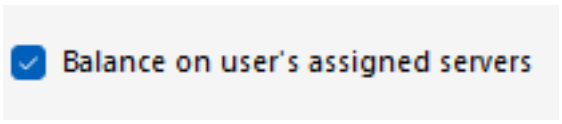
You can see the list of Load-Balanced Servers Status and details on the performances indicators of each server.

The servers are sorted from the less loaded to the most loaded according to your configuration.

The list of Load-Balanced Servers Status is automatically refreshed. This automatic refresh stops if the connection becomes unavailable. You can change the refresh rate at the top right corner of the “Server” box.



Load-balancing can also be done directly on user's assigned server using the **checkbox "Balance on user's assigned servers"**.
As a result, you will be able to load-balance on accounting department servers only for accountant users, once these specific servers have been assigned to the accountant users.



You can activate the sticky session feature by clicking on the right button of the Load balancing window:



Enabling **existing sessions web listing** is required for Load Balancing Sticky Sessions feature.

It will allow you to reconnect to a disconnected session instead of opening a new session on a different server.

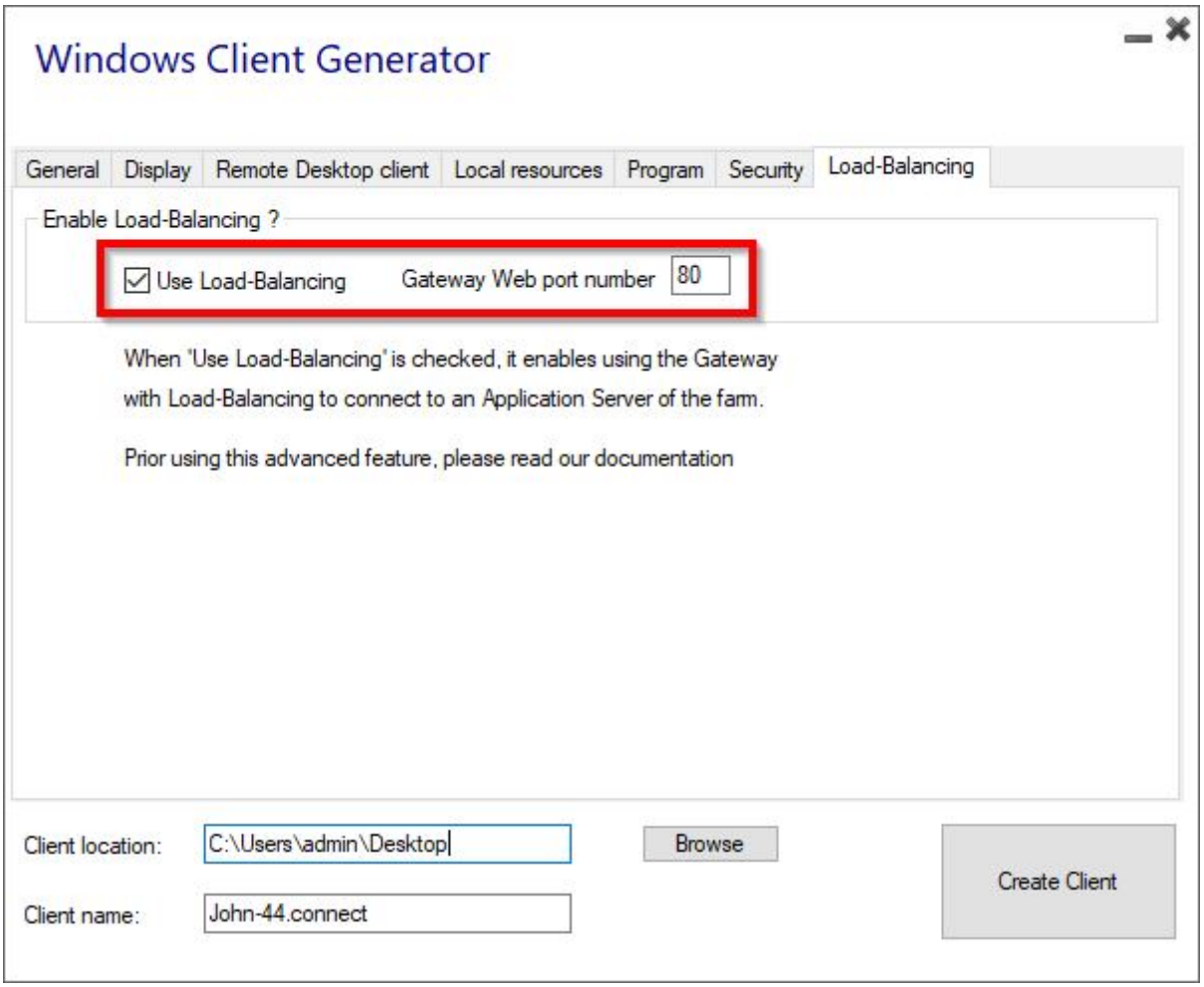
To enable **existing sessions web listing**, set the following setting to "no".

Load Balancing using a Connection Client

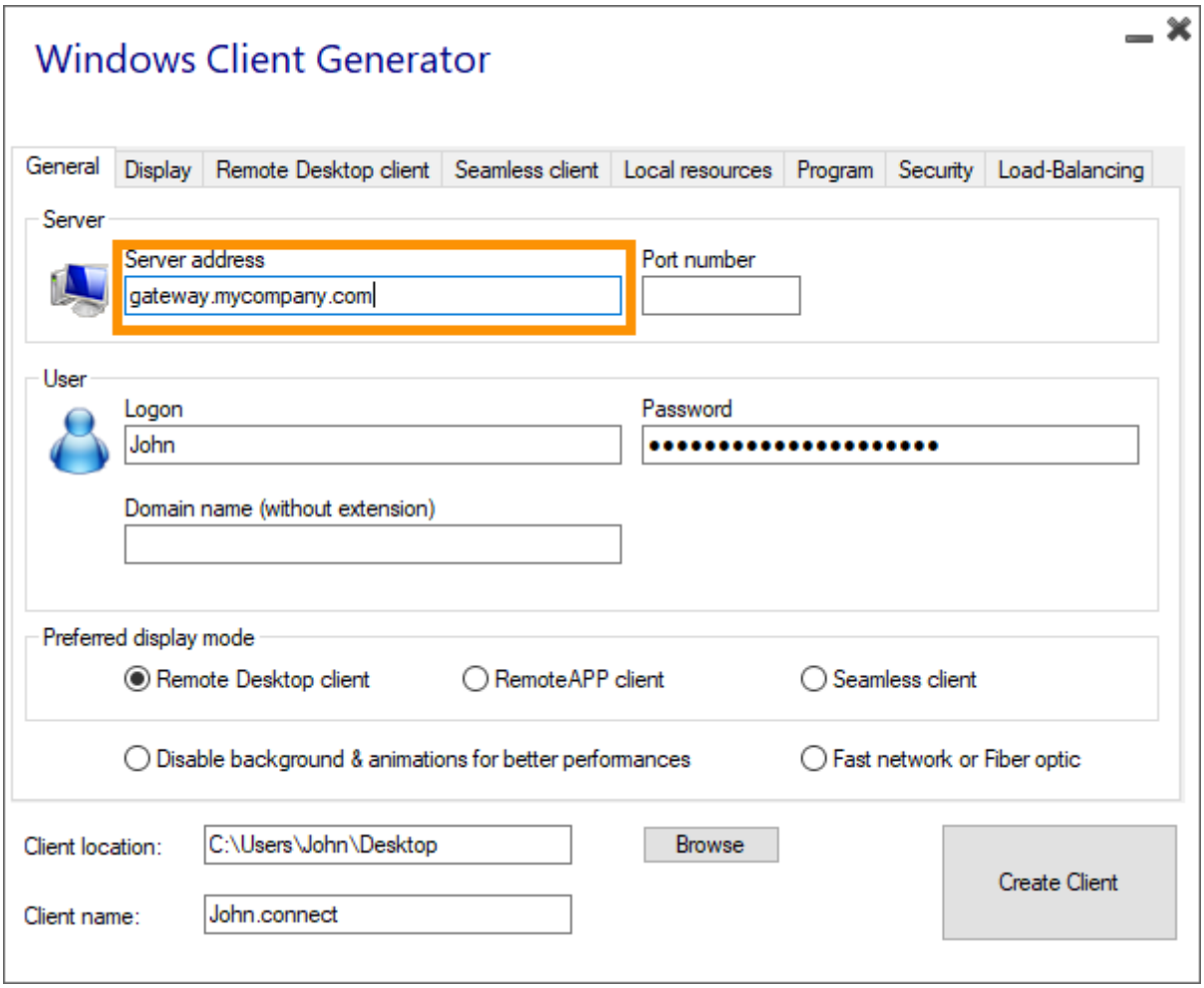
If you want to generate a Connection Client for a user to connect to the less loaded

server, you will need from the Client Generator in the “Load-Balancing” tab to:

- Check the “Use Load-Balancing” checkbox
- Fill in the “Gateway Web port number” field with the HTTP or HTTPS port used by your Gateway Server



- Use the public IP address or hostname of your Gateway Server directly in the “Server” field.


Windows Client Generator
General
Display
Remote Desktop client
Seamless client
Local resources
Program
Security
Load-Balancing
Server
Server address
gateway.mycompany.com
Port number
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 location:
C:\Users\John\Desktop
Browse
Client name:
John.connect
Create Client

Farm Manager API

We are excited to offer you a powerful API designed to provide comprehensive management capabilities for your server farms.

This API allows you to seamlessly integrate our software with your existing infrastructure, enabling you to manage and automate server operations with your own custom scripts.

Discover the full potential of our software with the robust and versatile API we provide.

Requirements

In order to query the farm manager API, your server will need to:

- have a valid SSL/TLS certificate
- be opened on port 19956
- be reachable using the domain your certificate covers.

Examples of use

For instance, administrators can use the **Farm > Get Servers list** function to retrieve a comprehensive list of all servers within their farm, streamlining inventory management. The **Farm > Initialize farm** function allows for the quick setup of a new server farm, ensuring a smooth deployment process. For user-specific server management, the **Farm > List of servers assigned to a user** function helps in tracking and managing server assignments.

In load balancing scenarios, the **Load balancing > choose server** and **Load balancing > Reload** functions enable dynamic server selection and reloading of load balancer configurations, optimizing resource distribution and performance. The **ReverseProxy > Reload** function ensures that changes to proxy settings are applied without downtime. Additionally, the **Server > Add** and **Server > Edit** functions facilitate the seamless addition and modification of servers in the farm.

Administrators can further enhance their operations by utilizing the **Setting > list settings** and **Setting > Apply settings** functions to retrieve and apply configuration settings across the server farm.

For session management, the **Session > Disconnect** and **Session > Logoff** functions allow for the controlled termination of user sessions, while the **Session > List users sessions** provides a detailed view of active sessions for monitoring purposes.

By leveraging these powerful API functions, you can achieve greater automation, efficiency, and control over your server management processes, ensuring optimal performance and reliability of your infrastructure.

Documentation

Complete documentation of this API can be found here : API Documentation

Overview

Overview and Naming

The goal of TSplus Farm features is to allow the Administrator to manage all his TSPlus servers from a single server. This server can be referred as the **Farm Controller**.

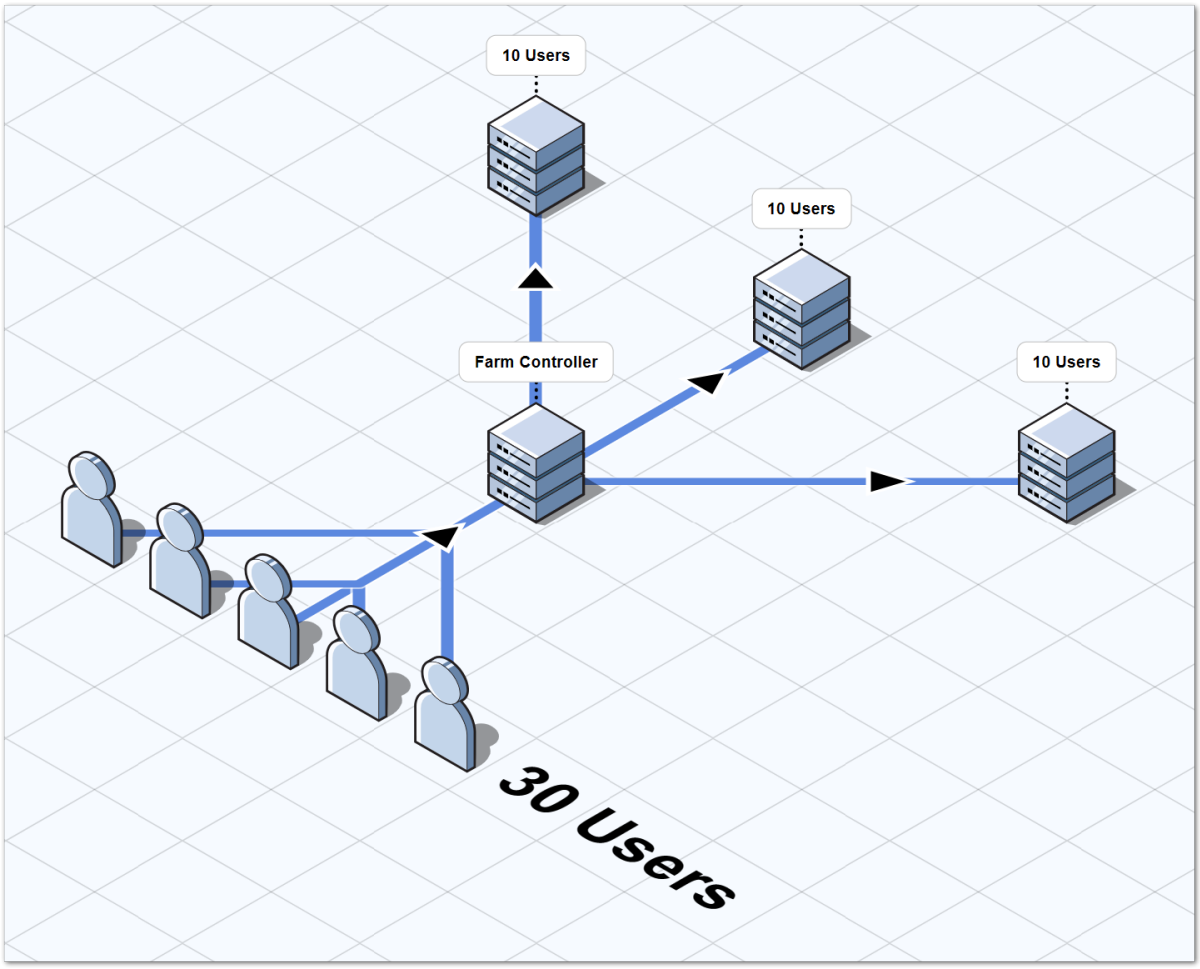
The TSplus servers in the Farm are named the **Application Servers**, or just Servers.

This Farm Controller, once having its farm populated with Application Servers, will also become a **Gateway Server** once you enabled any of the Farm features such as:

- Load balancing
- Reverse Proxy
- Assign Servers

This Gateway Server will basically become the main entry point of all your users when either “Load Balancing” or “Assign Servers” is enabled.

Finally, this Farm Controller will also allow you to monitor any Applications Servers, and easily push TSplus related settings such as Applications and Advanced settings from your Farm Controller to your Application Servers.



TSplus Farm of Servers Architecture

There are 2 options to deploy a TSplus farms of servers:

Option 1: All your servers have public IP addresses and can be reached from the Internet.

OR

Option 2: Only the Gateway Portal can be reached from the Internet. The Gateway Server is providing a “Reverse Proxy Role”.

In both options:

- Every server has the same TSplus configuration.
- Every server has the same HTTP/HTTPS ports.
- To publish a new Application just add it to your users/groups of users on the AdminTool.

Of course, make sure that this application is installed on the targeted Application Servers.

All Web Access types are available without any specific configuration: RemoteApp and HTML5 clients.

Option 1 - All Servers have their own Public IP Address and can be reached from the Internet.

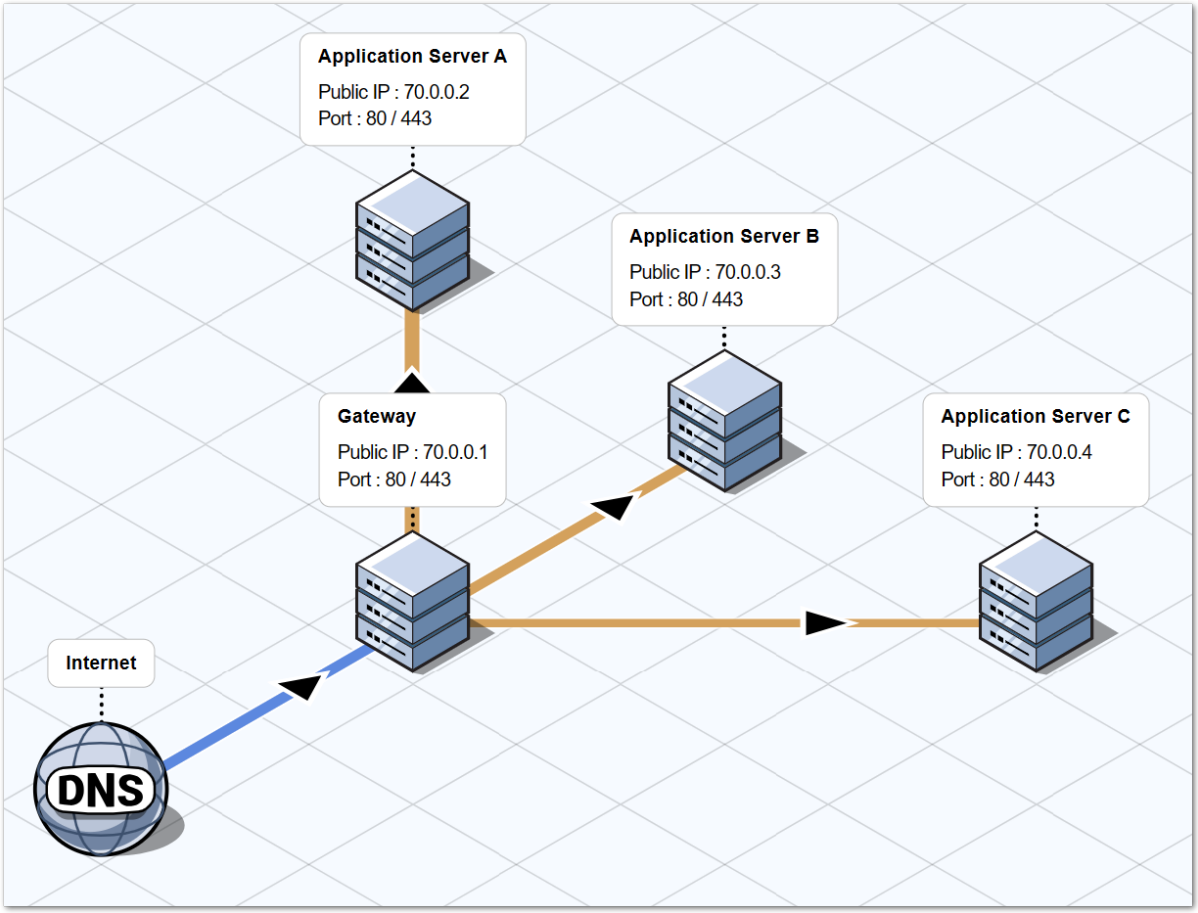
This is the recommended architecture to use Terminal Service Plus Gateway.

This architecture follows best practices and allows the IT Administrator to industrialize its environment:

- Every server has the same Terminal Service Plus configuration
- Every server has the same HTTP/HTTPS ports
- Deploying a new Application server is only a matter of minutes (just add the server to the farm in the AdminTool on the Gateway server)

With this architecture, all access types are available without any specific configuration: Remoteapp and HTML5 clients.

This architecture is described in the diagram below:



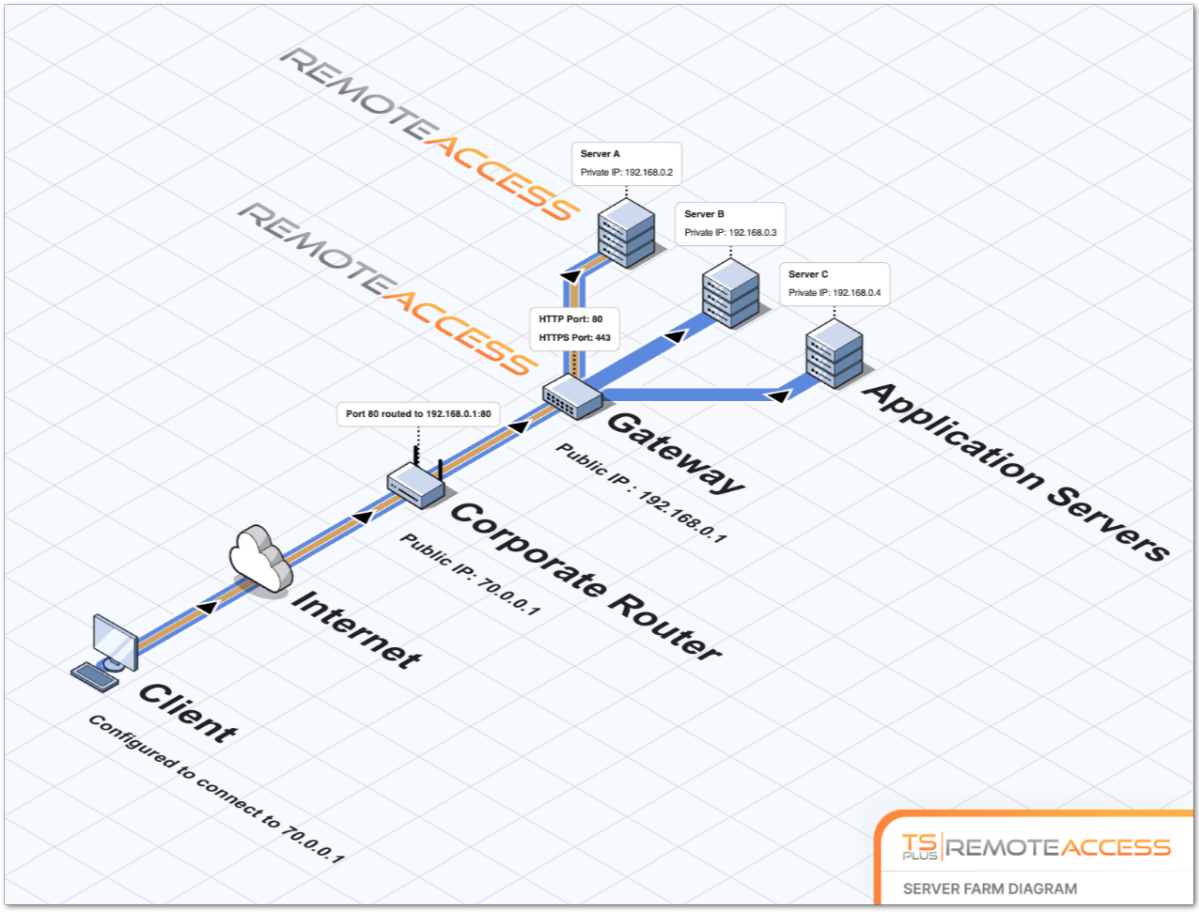
Option 2: Only the Gateway Portal can be reached

from the Internet and includes a “Reverse Proxy Role”.

Terminal Service Plus Gateway can also be set up with only 1 Public IP Address.

The Gateway redirects any external connection request to any available server. If you do not use the load balancing feature, users will connect to their assigned server(s).

This architecture is described in the diagram below:



For more information about the Reverse Proxy Role, see the Reverse Proxy Feature documentation.

Releases History

- API 1.5 (released with TSplus 15.50)
  - Integrated Reverse-Proxy, Load-balancing and application server assignment configuration
  - Added synchronisation between applications/settings of the farm controller and every application servers

- API 1.4 (released with TSplus 10.10)
  - Load-Balancing centralized monitoring

    - Enable/Disable a Server in TSplus Load-Balancing Manager
    - Translations in multiple languages (TSplus language will be used)
    - Several settings added + display bugs fixed

- API 1.3 (released with TSplus 9.70)
    - Settings centralized monitoring and management (Global settings / Floating Panel / RemoteApp Client / HTML5 Client)

- API 1.2 (released with TSplus 9.60)
    - Farm Manager
    - Servers centralized management (add/remove)
    - Sessions centralized monitoring and management (messages/disconnect/logoff)

- API 1.1 (released with TSplus 9.30)
    - Load-Balancing internals
    - Load-Balancing Sticky-Sessions

Prerequisites

Hardware Requirements

Farm Controller and Application Servers have the standard Terminal Service Plus requirements for hardware.

Operating System Requirements

Farm Controller and Application Servers must use one of the following Operating System:

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

Both 32 and 64 bits architectures are supported.

Network Requirements

Every Application Server must be accessible from the Farm Controller.

More specifically, the Farm Controller will issue requests to every Application Server on its API port (19955 by default) and this port must be opened on any firewall standing between the Farm Controller and Application Servers.

The network latency must be low between the Farm Controller and Application Servers. A latency under 200 ms is recommended, a latency under 2 000 ms is required.

Software Requirements

.NET 2.0 or higher is required - this should not be a problem as a compatible .NET version is enabled by default on every Operating System supported for Terminal Service Plus Farm.

Terminal Service Plus License and Version Requirements

Terminal Service Plus must be in “Enterprise” edition on the Farm Controller and on all the Application Servers.

All the servers must also run the same version of Terminal Service Plus.

Configuration Requirements

Farm Controller and Application Servers must have the same date/time configured. It is highly recommended to synchronize the Windows clock of all servers with an Internet Time Server if not already done.

Users Requirements

An Active Directory is **not** required, however if you do have an Active Directory, then your Domain Administrators must also be Local Administrators of the Farm Controller to be able to use Terminal Service Plus Farm Manager.

Reverse Proxy

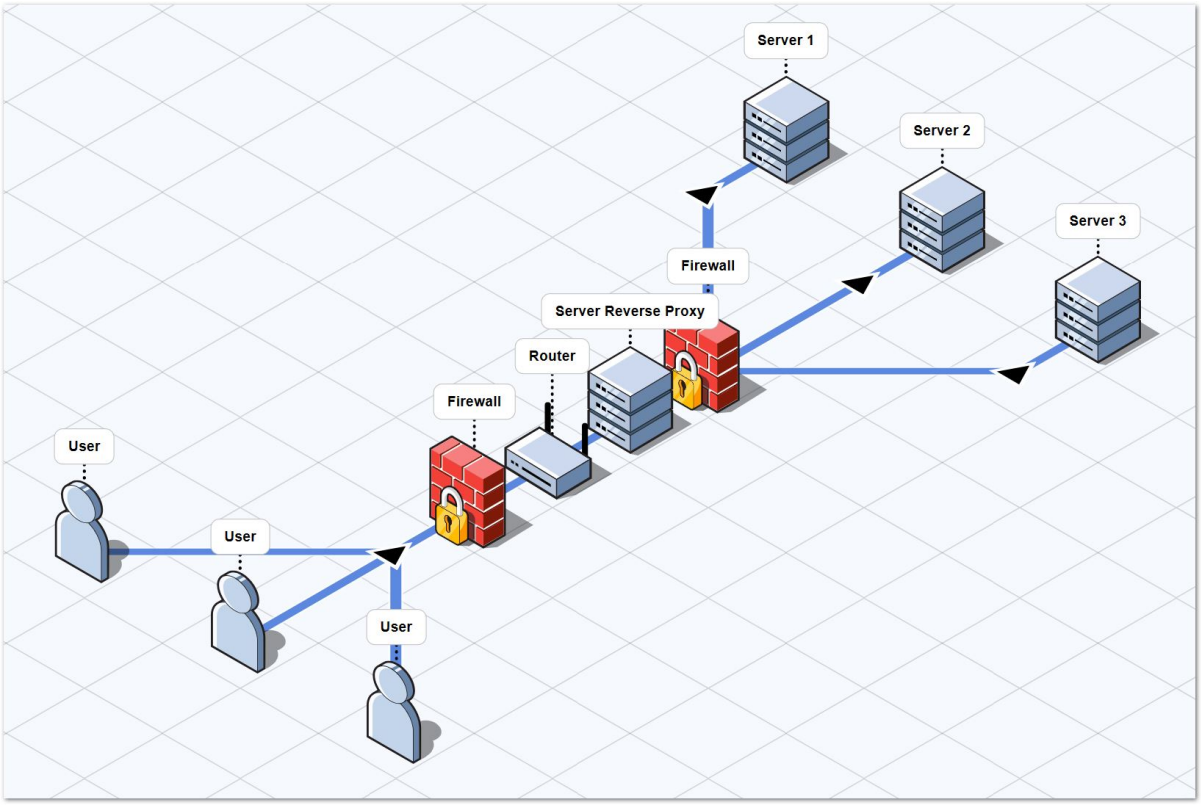
Overview

This feature is available in the TSplus Enterprise Edition.

The Reverse Proxy system acts as an intermediary for its associated servers to be contacted by any client.

The advantage of using a reverse-proxy is simple: you will no longer need to create as many port redirection rules as your number of TSplus servers.

Whether or not you are using the load balancing feature, you need to activate it in order to connect using the reverse proxy. In TSplus, it provides a unique access point to a farm of load-balanced TSplus servers:

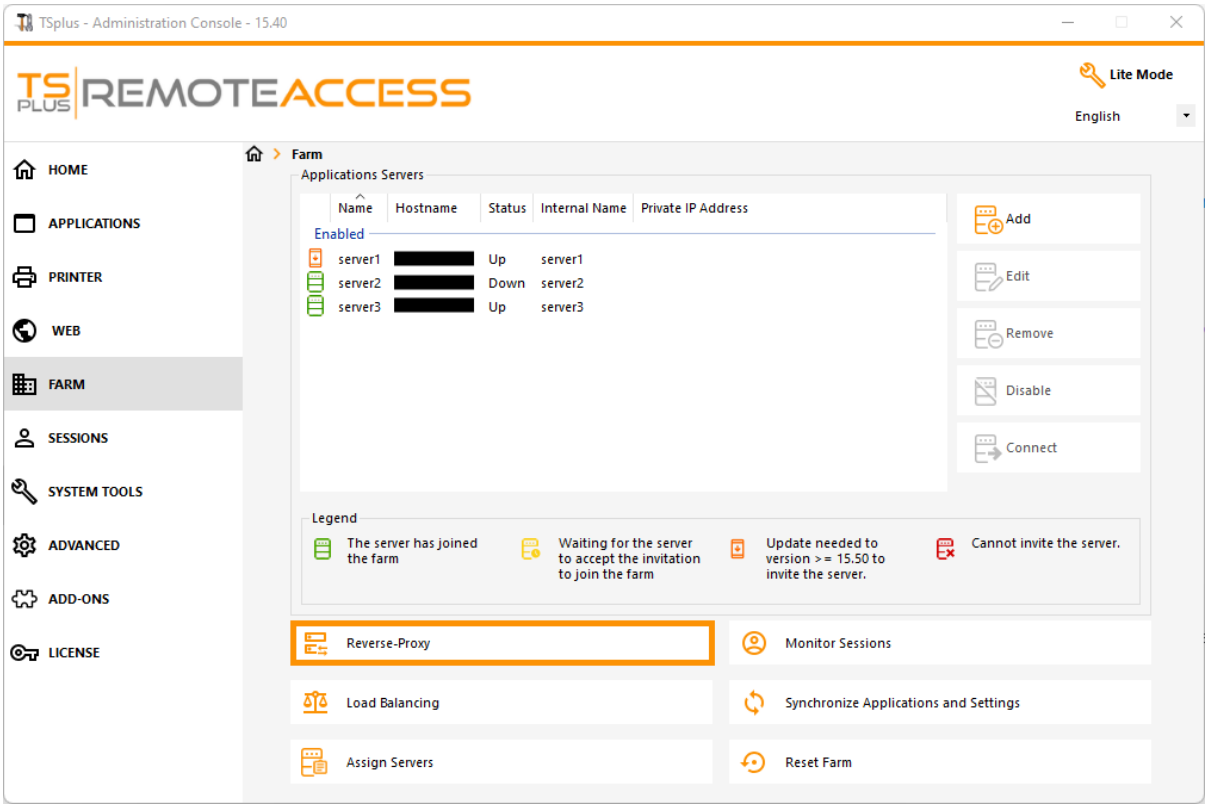


This unique access point will be your Gateway Server TSplus Web Portal.

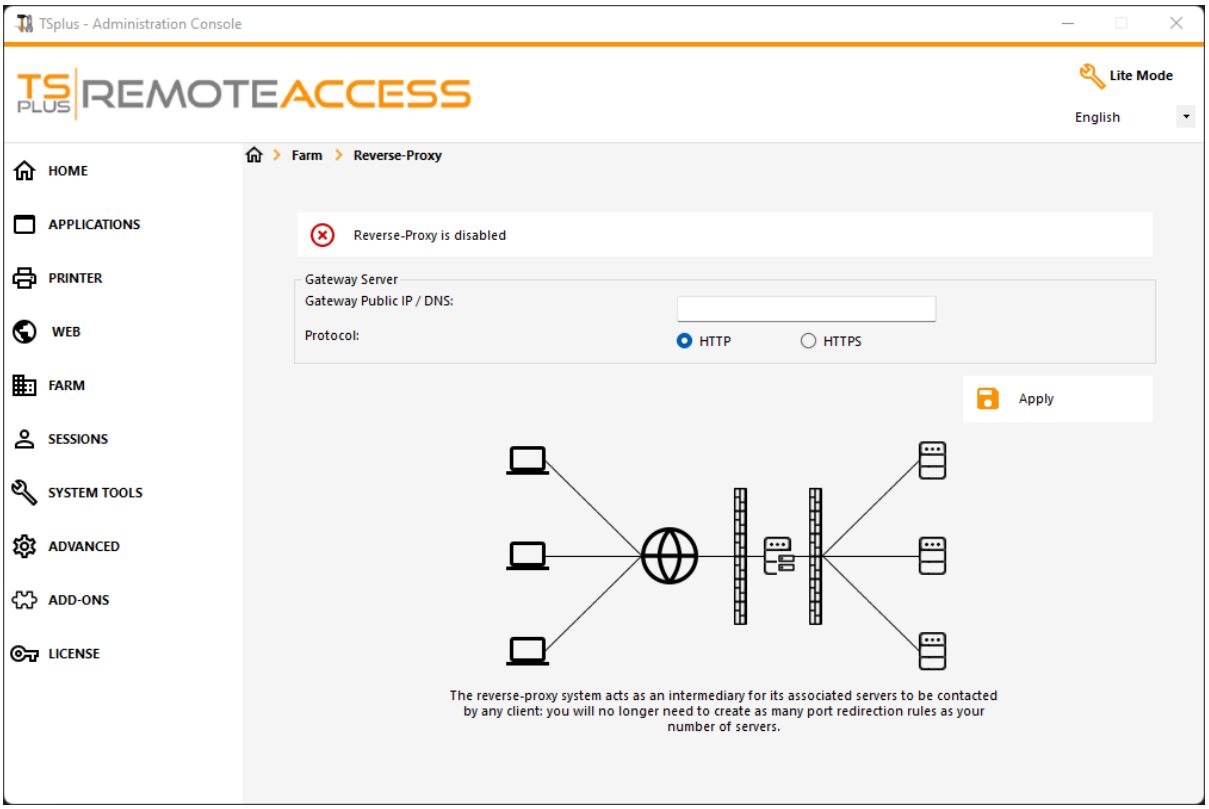
Since this server is going to be accessed remotely, you will need to set up one port redirection rule on your router, including the http or https ports depending on your preference (80 being the default port for http and 443 for https).

Configuration

You can access the Reverse Proxy configuration interface through the FARM tab:



Click on the Reverse-Proxy button.



- Click on the “Reverse-Proxy is disabled” button to activate it.
- The Gateway Public IP must be set with a fixed valid IP address or domain name.
- Select HTTP or HTTPS for your preferred connection method, the servers of your farm must be able to communicate with eachother on either port 80 or 443, depending on which connection method you use. It is also important that your windows firewall don’t block these ports.

Once you completed your configuration, click on “Apply” to save these Reverse Proxy settings.

Access to application servers through Gateway Server

Once enabled and operational, the Reverse Proxy feature allows you to access to the application server using a special URL formatted as follow:
(1)://**(2)**:**(3)**/~~**(4)**
with:

- (1): the Reverse Proxy protocol configured
- (2): the Gateway Server public IP address or domain name
- (3): the Gateway Server web port associated to the configured Reverse Proxy protocol

- (4): the application server's internal name used by Reverse Proxy

For example, assuming that:

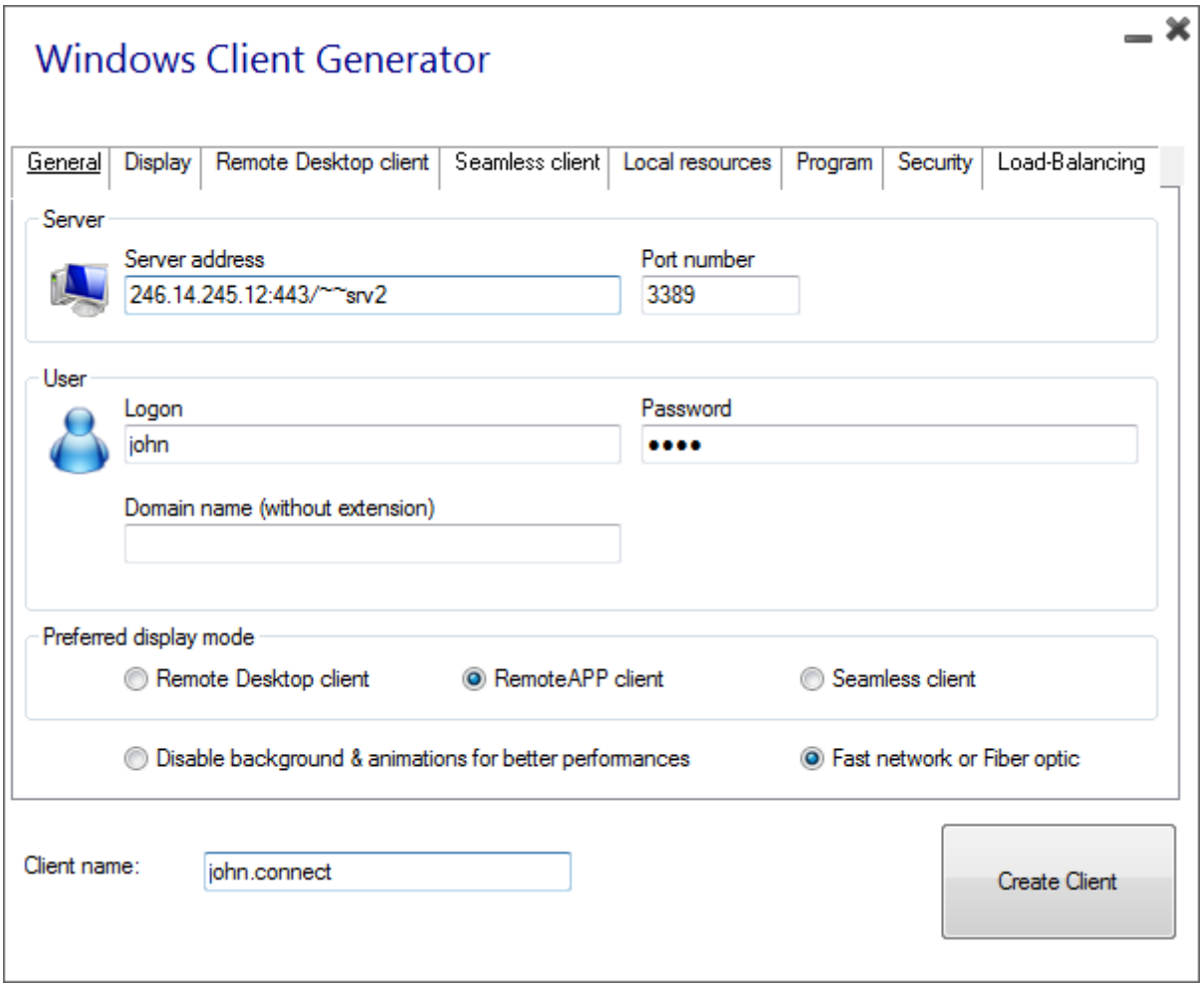
- the reverse proxy protocol configured is HTTPS
- your Gateway Server has public IP 1.1.1.1
- your Gateway Server is using the HTTPS port 443
- the targeted application server you want to connect uses the internal name "srv2"

The special URL to use in order to reach the targeted application server will be 1.1.1.1:443/~~srv2

As a result, you can access the web portal of this application server using this special URL.

You can also generate a Connection Client which will connect to this specific Application Server through the Gateway Server using this same method Simply use the special URL in the server address field of the Connection Client Generator.

For example:



Server Assignation

Overview

The farm controller can act as a Gateway Server, redirecting users upon connection to specific application servers of your farm. You will be able to assign one or several servers to a user / a local group / an Active Directory group.

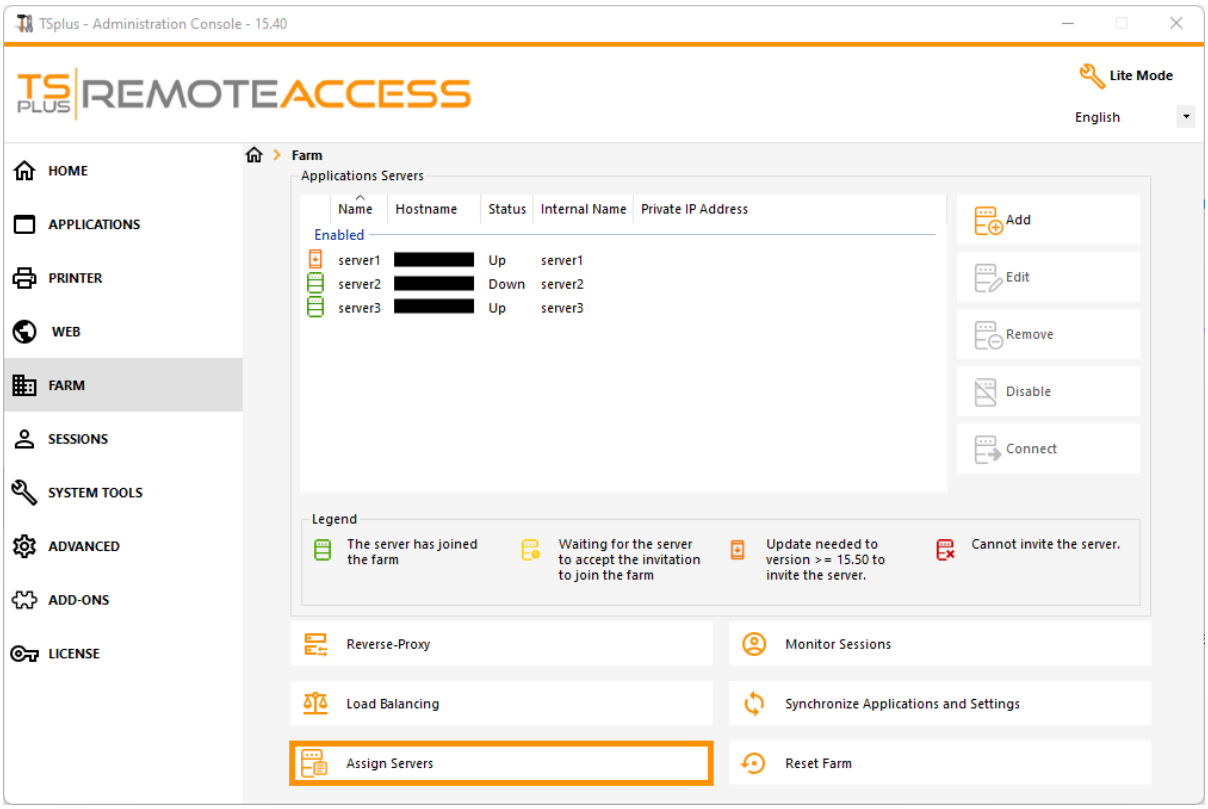
Important: Assigning servers only works from the TSplus Web Portal, and not with connection clients.

If the user has more than one server assigned, he will be able to choose which server he wants to access in the list of servers assigned to him.

If the farm is within a Domain, the Gateway will use his AD credentials and the user will connect with Single Sign-On (SSO).

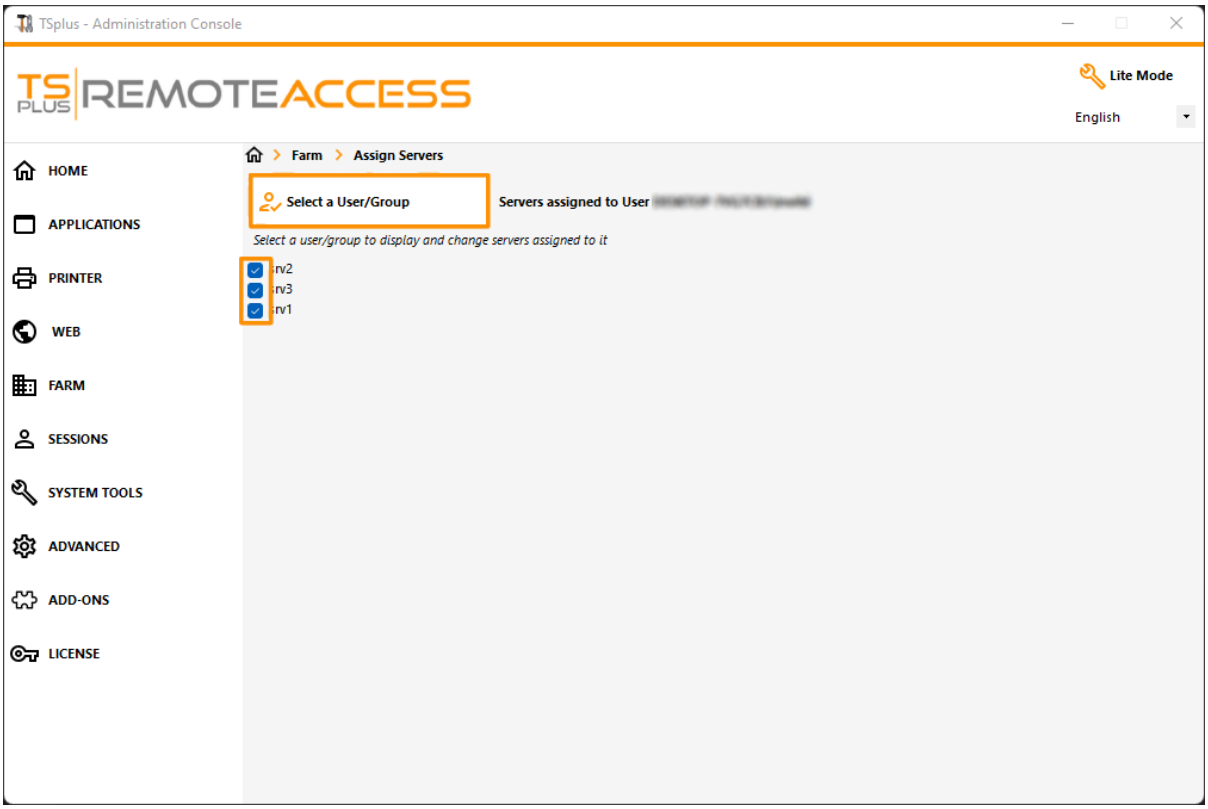
Otherwise, he must have the same local credentials on each server.

To assign servers, please click on the “Assign Servers” button:



To assign a server to a user, simply select it with the “Select a User/Group” button and then check the server’s checkbox in the “Servers” list.

To remove a server assigned to a user, simply uncheck the server’s checkbox in the “Servers” list.

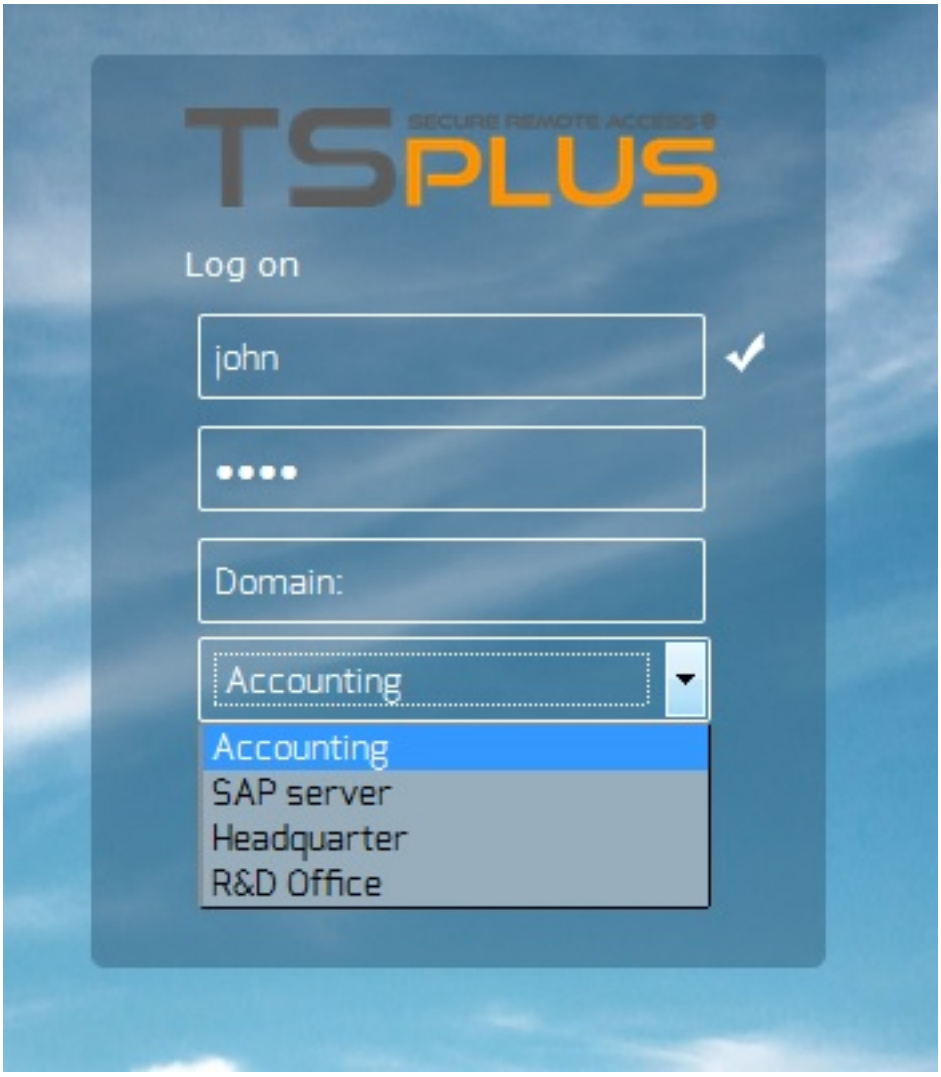


Important Notes

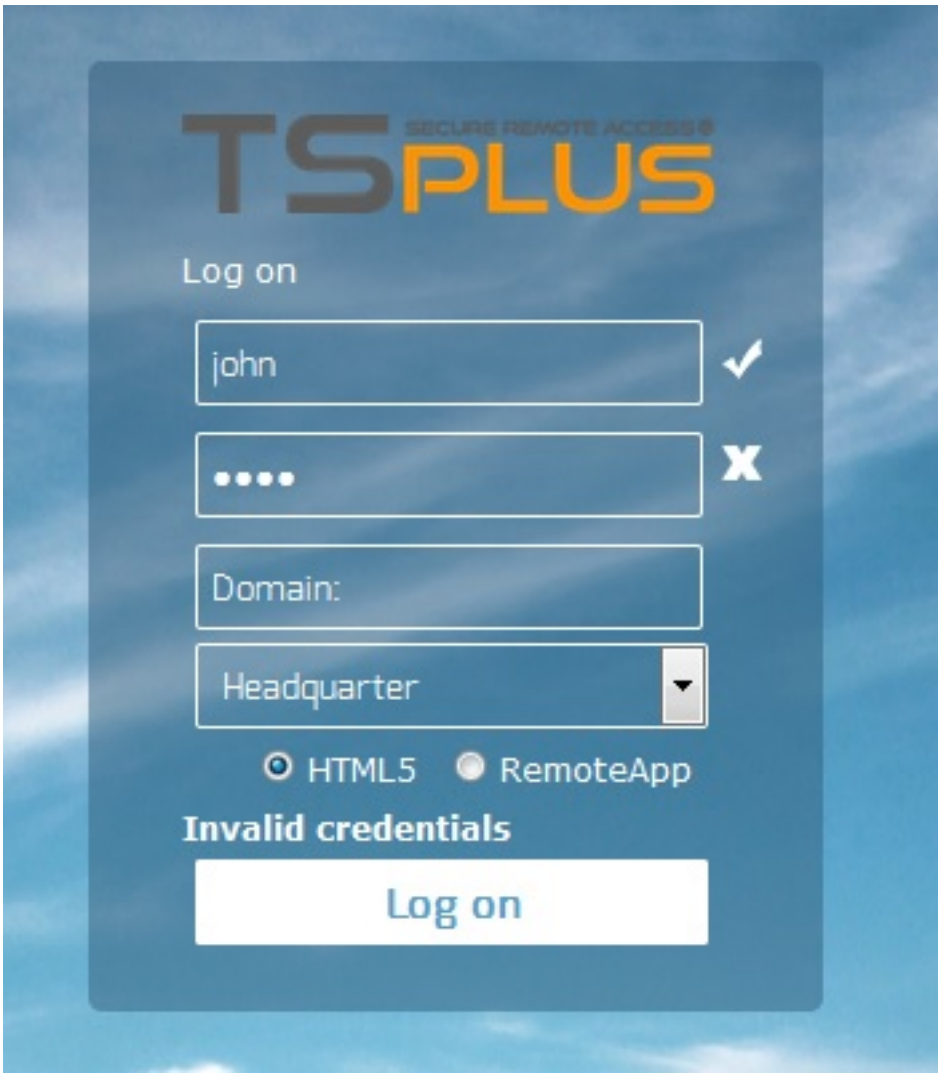
- The example above is for a Domain or a Workgroup.
- If you use a workgroup the users logins must be the same on each application server that you assign.
- This Server Assignation feature can be configured and used simultaneously with the Load Balancing feature, allowing the farm controller to load balance on assigned servers. To do so enable the Load Balancing and check the option “Load balance on assigned servers”.
- If the Server Assignation feature and the Load Balancing are both enabled, unless the option “Load balance on assigned servers” in the Load Balancing configuration is enabled, the Gateway Server will redirect users to the least loaded server regardless of their assigned servers.

Example of what you will get when users connect to the Gateway

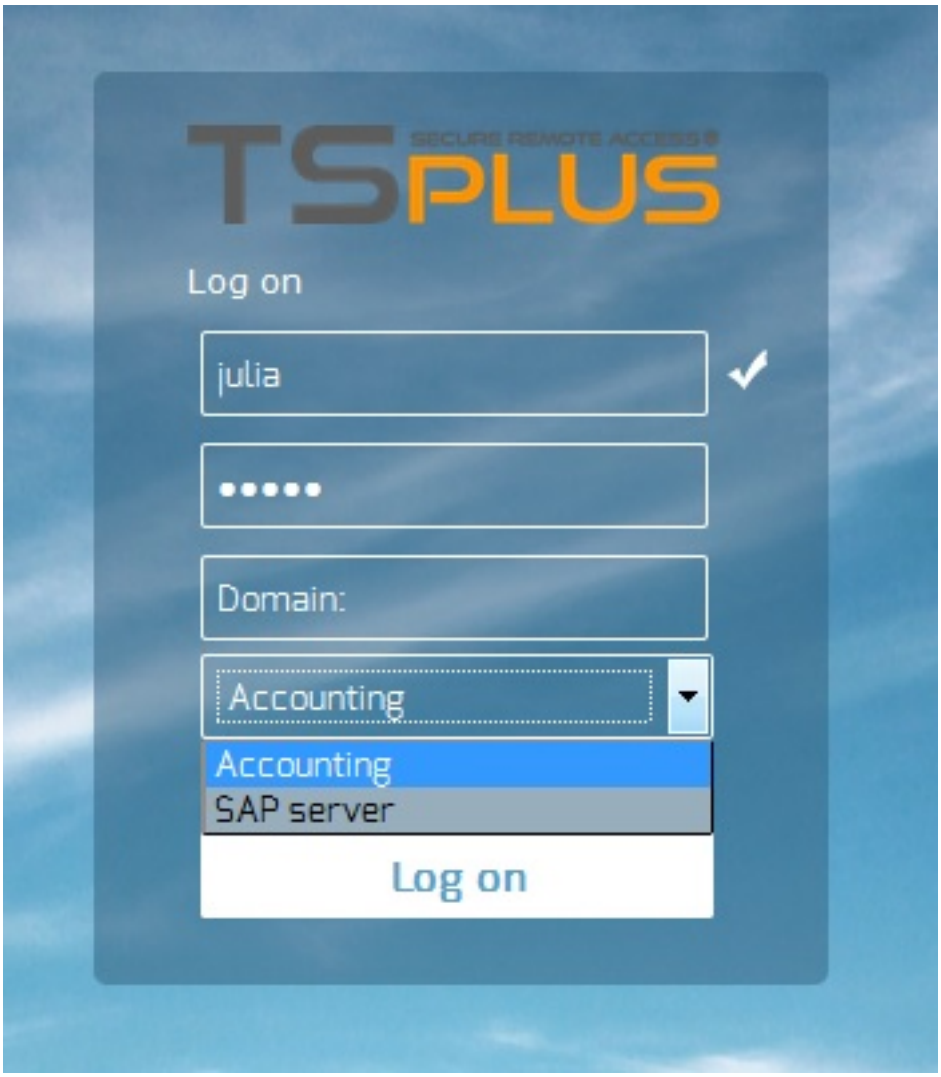
John can select the server. He wants and he will get an auto-logon to this server:



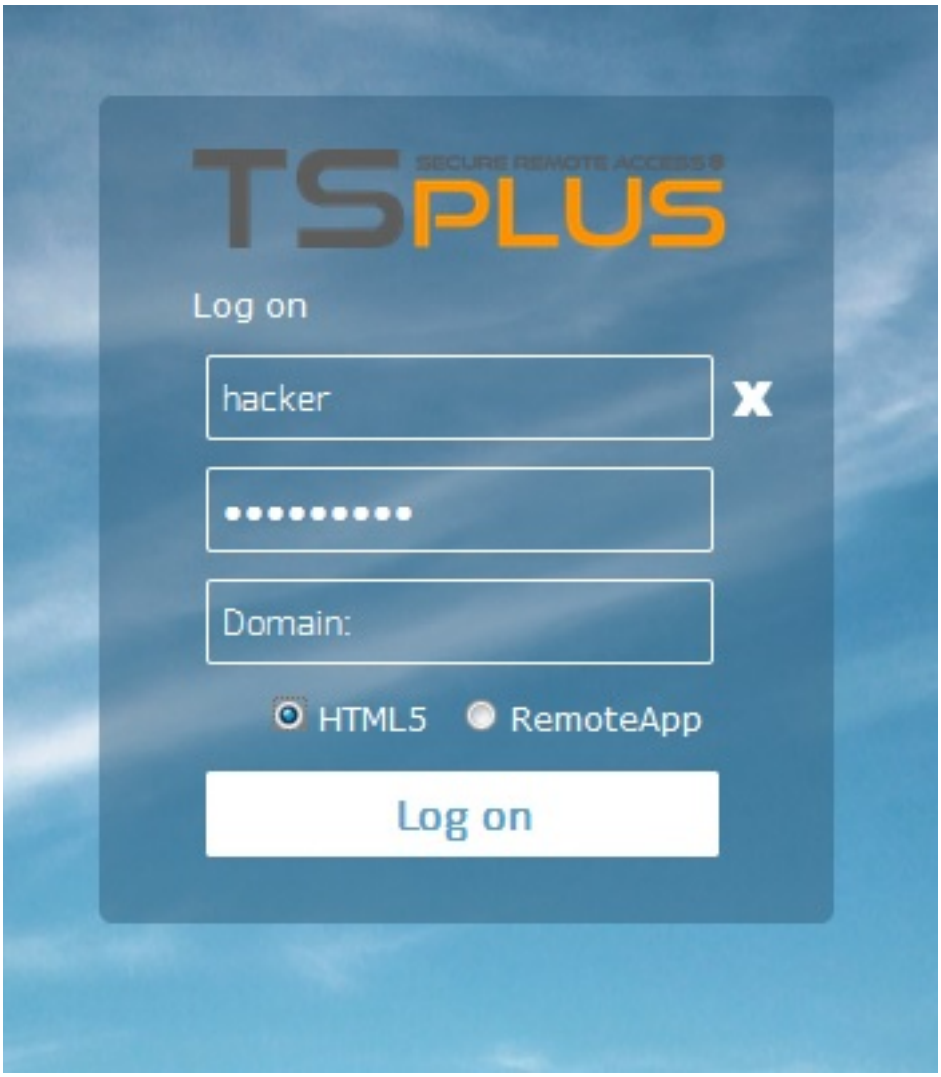
If he types a wrong password, John will have to retype his password:



Julia has a different list of possible servers:



Someone tries to hack the Gateway. He does not see any server and the Gateway blocks his web access.

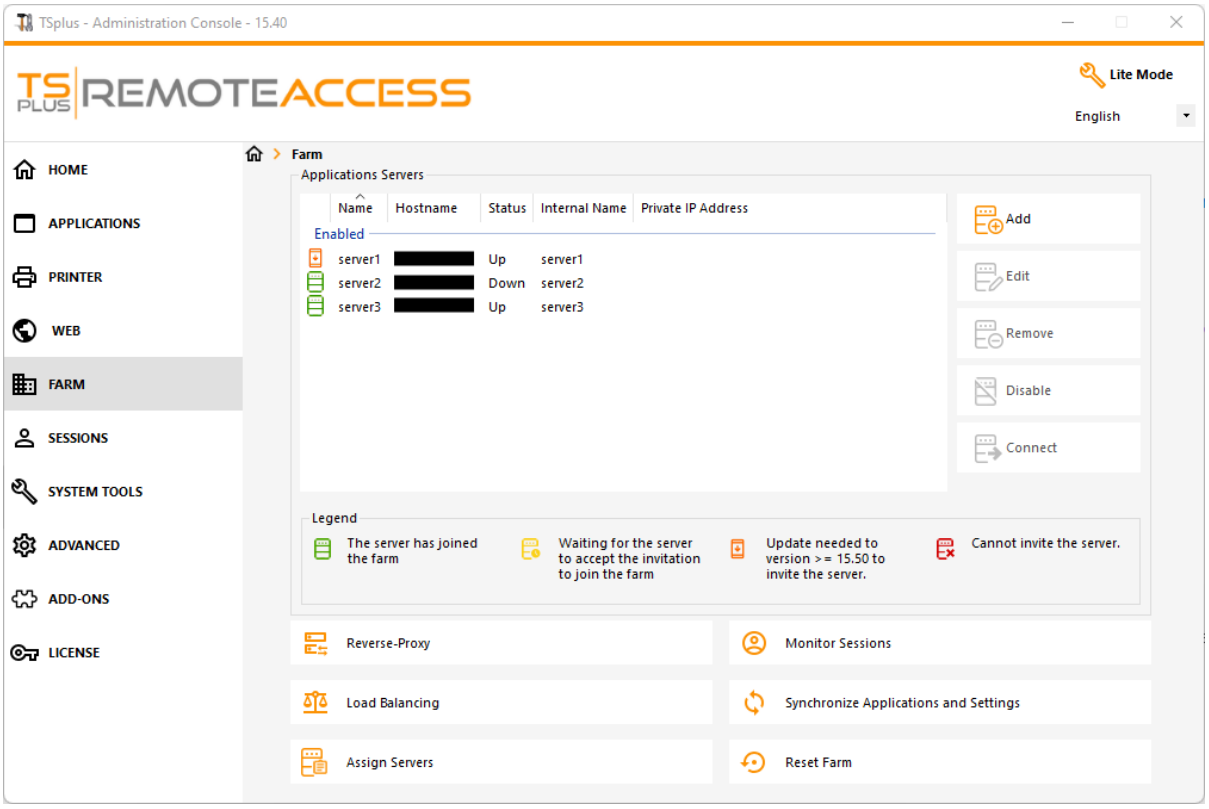

TSPLUS
SECURE REMOTE ACCESS
Log on
hacker
Domain:
HTML5
RemoteApp
Log on

Farm Setup

Overview

To create a farm, you simply need to add application servers from the TSplus AdminTool.

You will be able to manage application servers in the section “Farm” of the AdminTool.



From this window, you will be able to perform several actions:

- “Add”: add a new application server
- “Edit”: edit the selected server.
- “Remove”: permanently remove the selected server from the farm (you can still add it again later with the “Add” button).
- “Disable/Enable”: temporarily disable or enable the selected server (users will not be able to connect to this server).
- “Connect”: open the default RDP client and connect automatically to the selected server. If your credentials are saved in MSTSC they will be used, otherwise you will have to enter your

credentials.

You can also access these actions from the contextual menu displayed with a right click on a server.

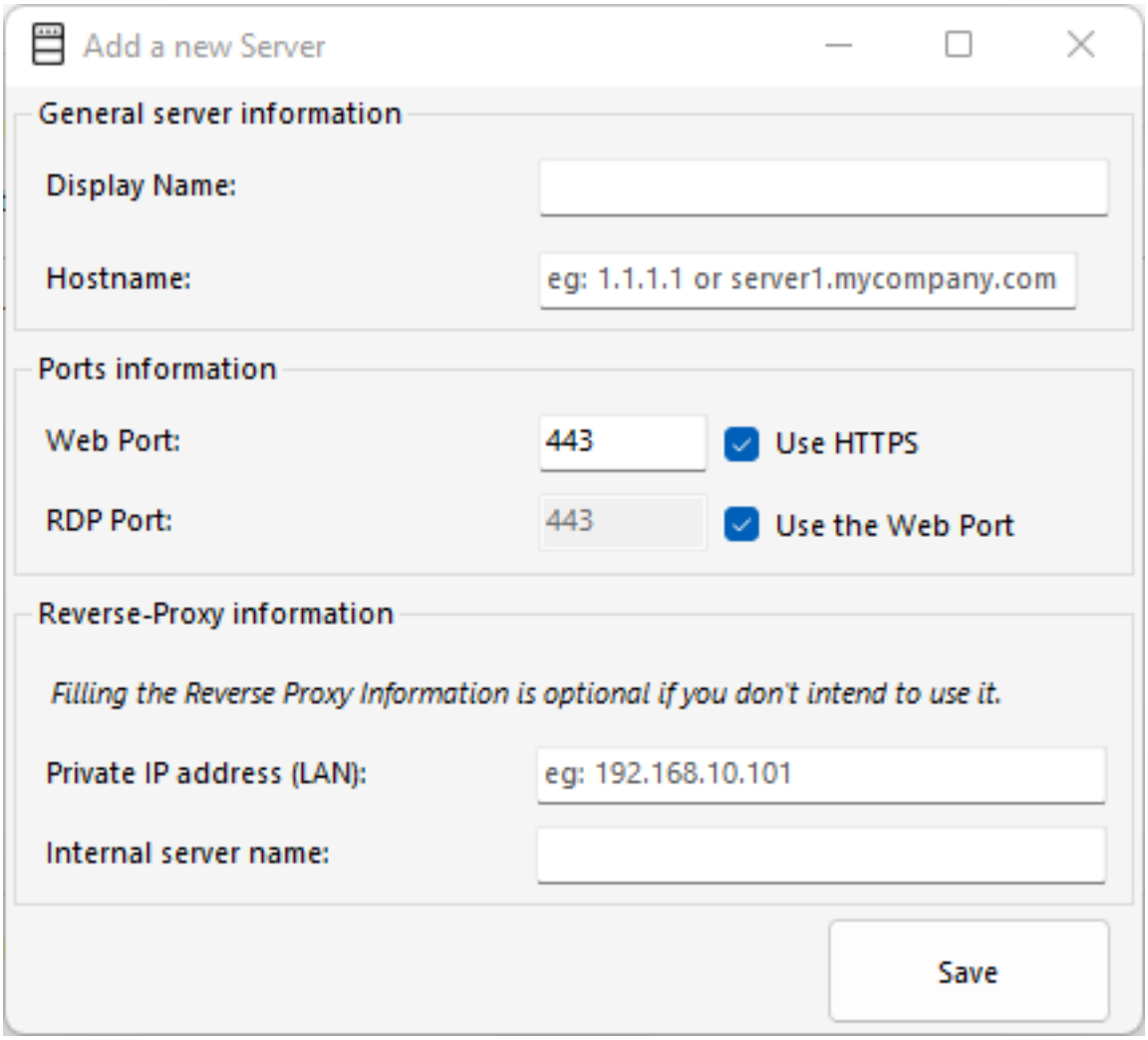
On the bottom panel you will find a quick access to the main farm features available once application servers have been added:

- “Load Balancing”: allows you to redirect users connecting from the gateway server to the least loaded server of the farm
- “Reverse Proxy”: allows you expose only the gateway server, and makes application servers accessible using URL such as https://gateway-server-domain-or-ip-address/~~application-server-internal-name
- “Assign Servers”: allows you to restrict user and groups available application servers when connecting from the gateway server, making them able to choose the server they want to connect if multiple servers are assigned.
- “Monitor Sessions”*: allows you to monitor current session and quickly perform actions such as disconnected, logoff, send message, view session or control session.
- “Synchronize Applications and Settings”*: allows you to push every advanced settings and published application to the selected application servers
- “Reset Farm”: allows you to reset the farm, which will remove every servers and reset every farm feature configurations e.g the “Reverse Proxy”, the “Load Balancing” and the “Assign Servers” configurations

*: These features are accessible only for application servers which completely joined the farm for security reasons, meaning you will need to accept first the invitation sent by your farm Controller, on the application server side.

Add an Application Server to the Farm

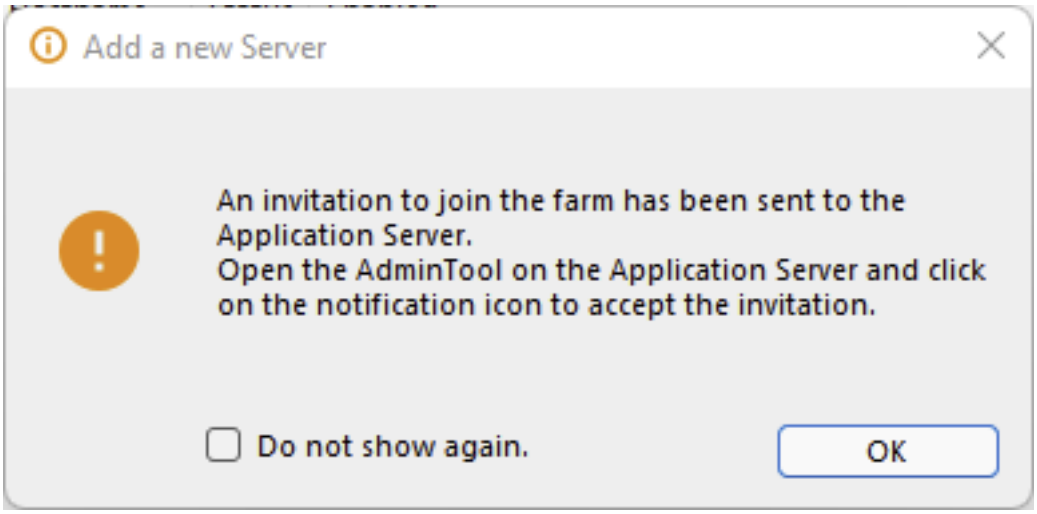
To add an application server, click on the “Add” button. The following window will be displayed:



You will need to specify its Display Name and Hostname (you can type an IP or a domain name, without a port number).
Filling the Reverse Proxy information fields is optional only if you are not currently using the Reverse Proxy feature.
The internal name will be automatically filled with an available display name if empty to ease the overall server configuration.

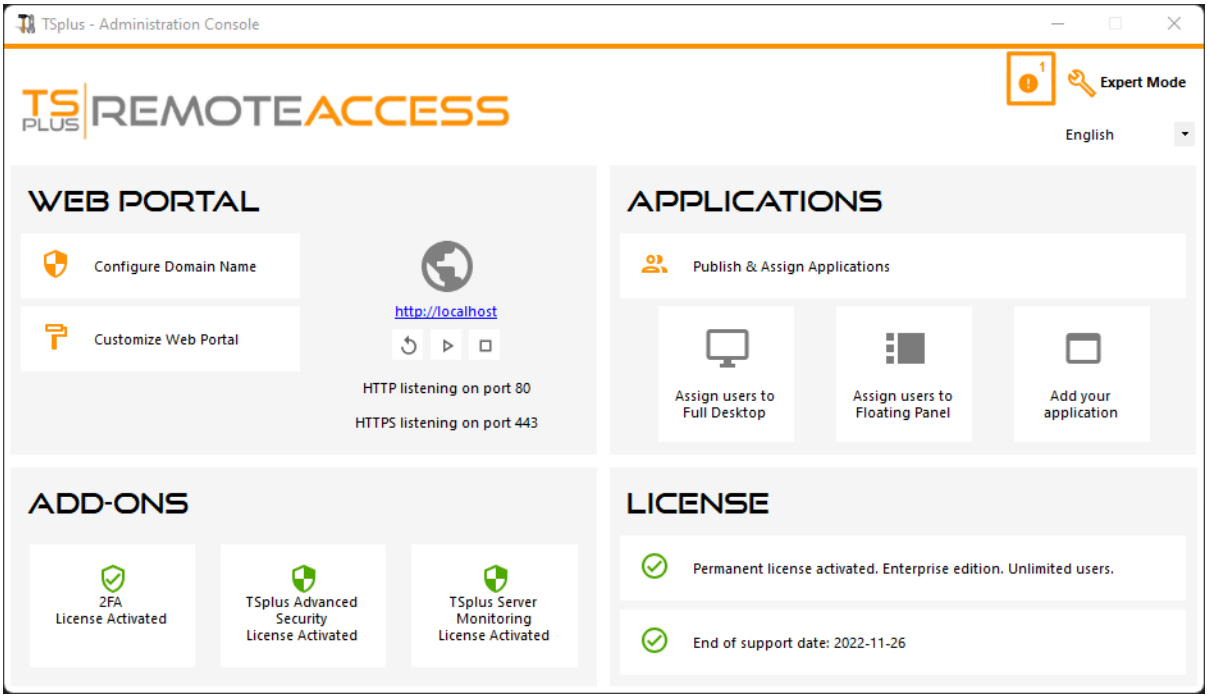
IMPORTANT: the RDP port option “Use the web port” specify that you want to leverage the RDP port forwarding feature (enabled by default) offered by the application server’s web server.
As a result, If you want to use the “Use the web port” option, please make sure that on the application server added, the “Disable RDP forwarding” option in the AdminTool > Advanced > Security is set to “No”.

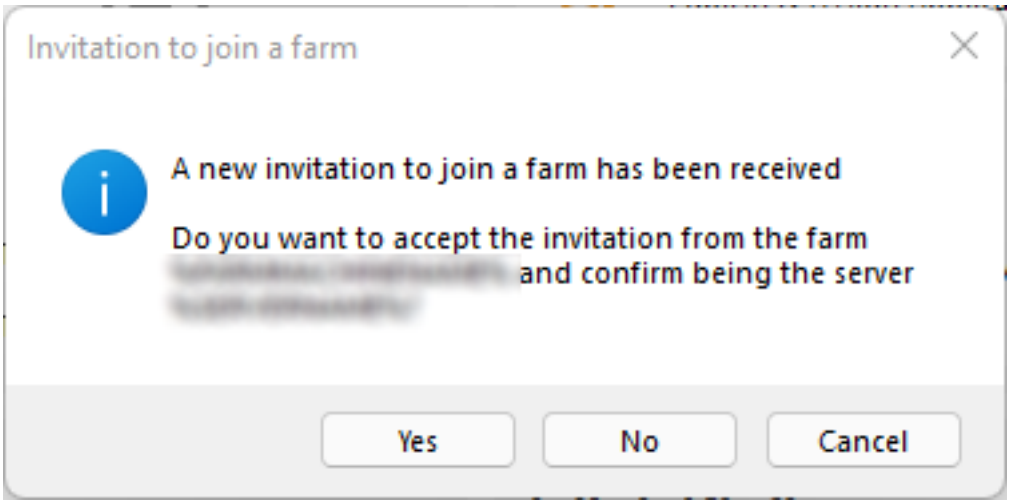
Enter the Application Server details, then click on the “Save” button. An invitation to join the Farm will be sent to the Application Server added:



Accepting this invitation on the application server side is required if you want to be able to use the “Monitor Sessions” and “Synchronize Applications and Settings” for security reasons.
It is however not required if you only need to use the “Reverse Proxy”, “Loadbalancing” and “Assign Servers” features.

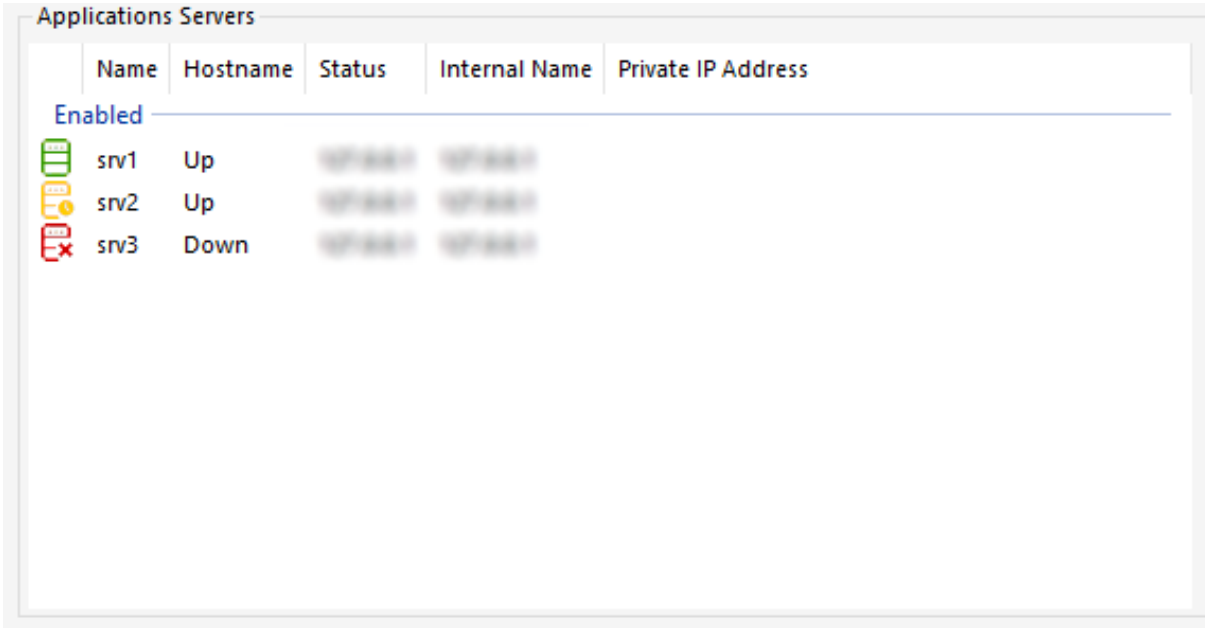
To accept the invitation, open an Administrator session **on the Application Server** you added to the Farm. Click on the alert button at the top right corner of the TSplus AdminTool, then click on “Yes”:





On the Farm Controller side, you can see the list of Application Servers in the Farm. They can have three states represented by colored icons:

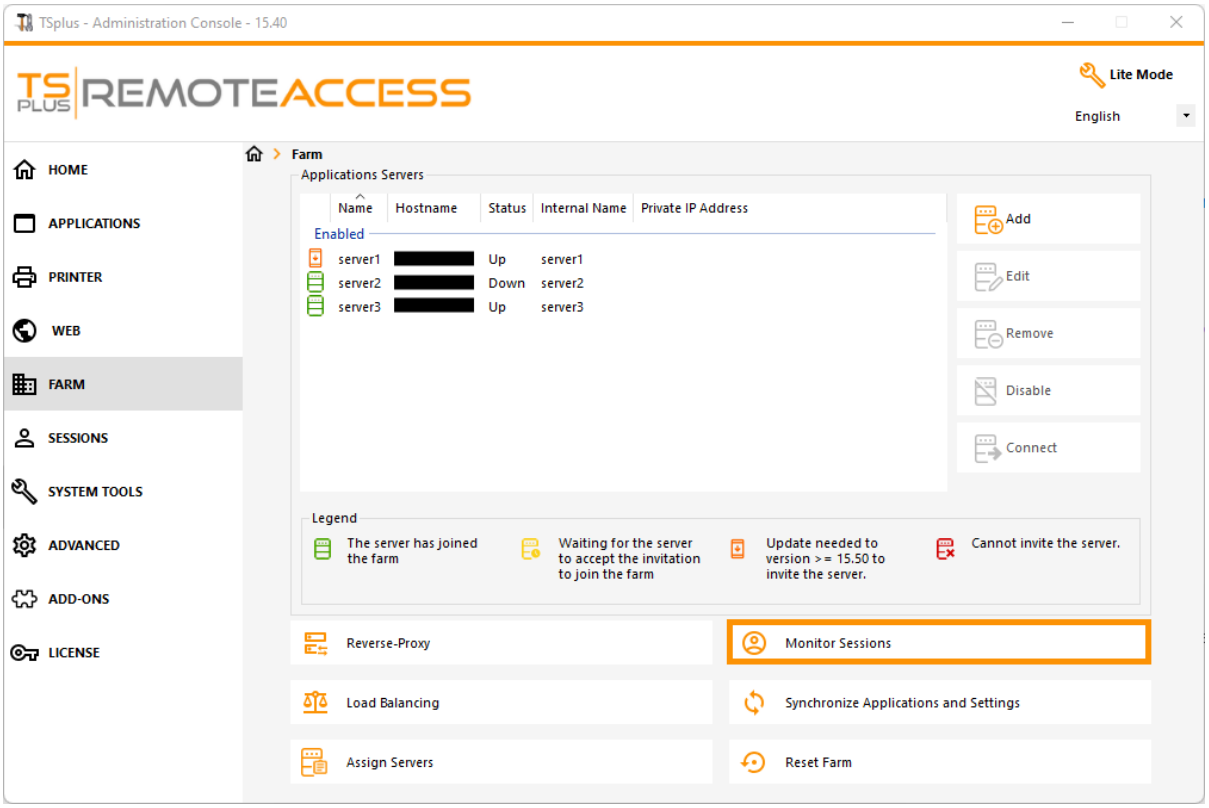
- Joined: The Application Server has fully joined the Farm by accepting the invitation
- Pending: The Application Server has partially joined the farm, waiting for the application server to accept the invitation
- Update needed: The Application Server has partially joined the farm, but the invitation cannot be sent because the server is using a TSplus Remote Access version < 15.50
- Unreachable: The Application Server has partially joined the farm, but the invitation cannot be sent because the server is unreachable



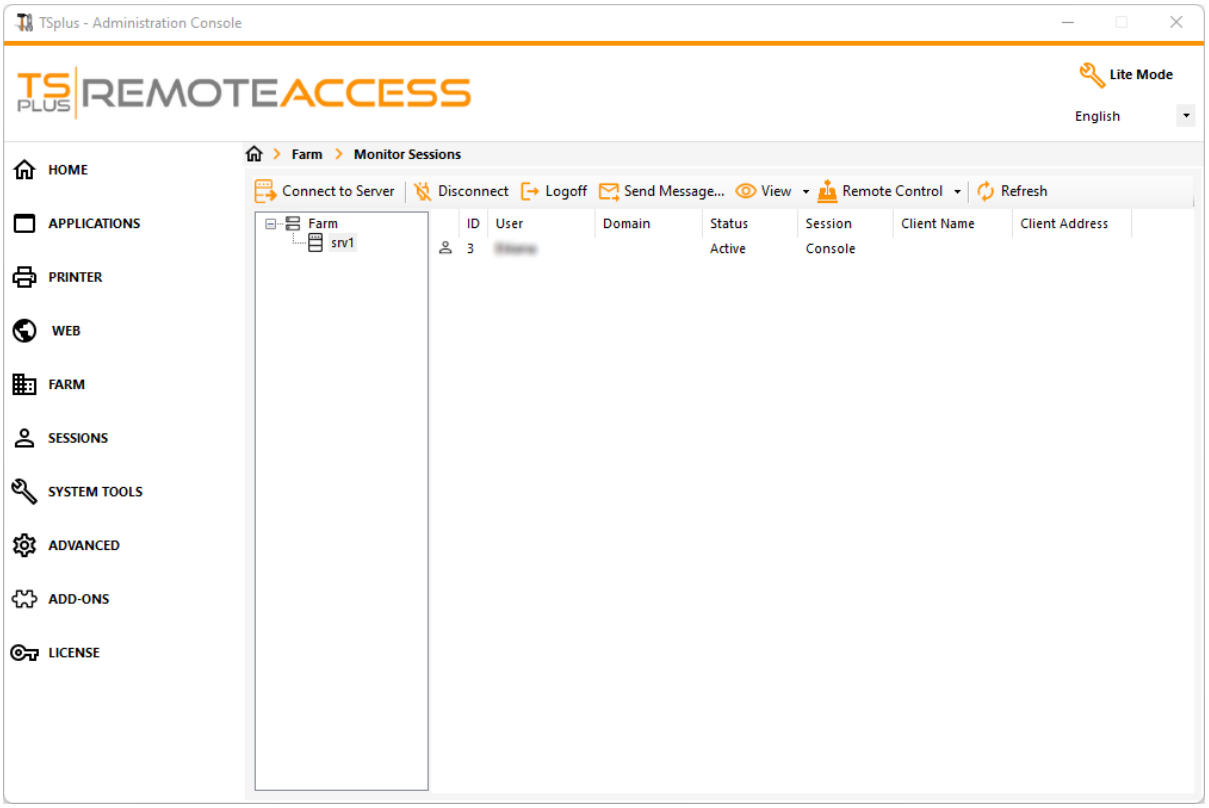
Monitor Sessions

Overview

You can access the monitoring session interface through the FARM tab:



Click on the “Monitor Sessions” button to display the following tab:



In this tab, you can see the list of User Sessions on any Application Server of the Farm.
Click on an application server on the left panel to select it and display its current active user sessions. Once displayed, you can select one or more sessions and perform several actions by clicking on one of the following buttons:

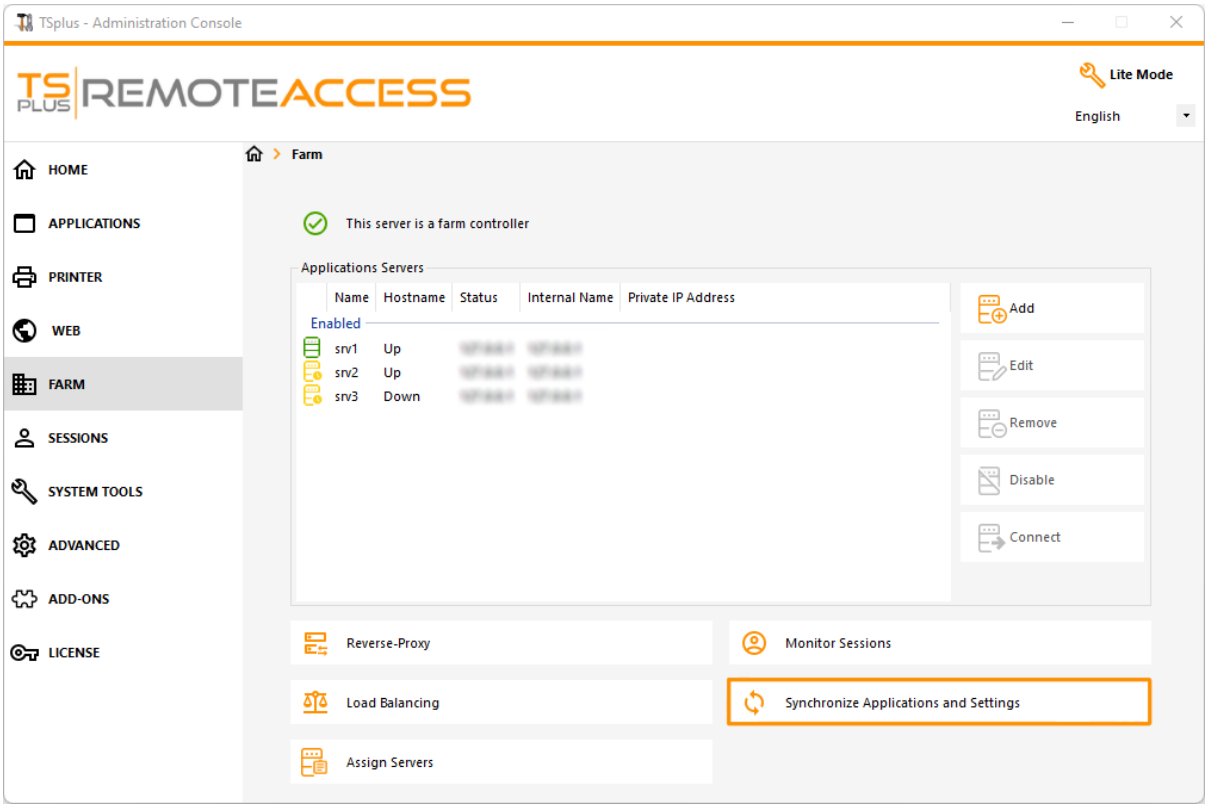
- “Disconnect”: disconnect the selected user session(s) (the user will still be able to connect back to his session).
- “Logoff”: log off the selected user session(s) (every unsaved modification will be lost, applications will be shut down abruptly).
- “Send Message”: display a window to enter a title and a text, then send this message to the selected user session(s).
- “View”: View a selected user session with/without***** permissions.
- “Remote Control”: Remotely control a selected user session with/without***** permissions.
- “Refresh”: perform a full refresh of the list of user sessions for the selected server(s).

*: To view or control a session **without permissions**, you will need to **change the following GPO on the application server you want to view and/or control the sessions of**.
GPO location: Computer Configuration> Administrative Templates> Windows Components> Remote Desktop Services> Remote Desktop Session Host > Connections.
GPO key: Set rules for remote control of Remote Desktop Services user sessions

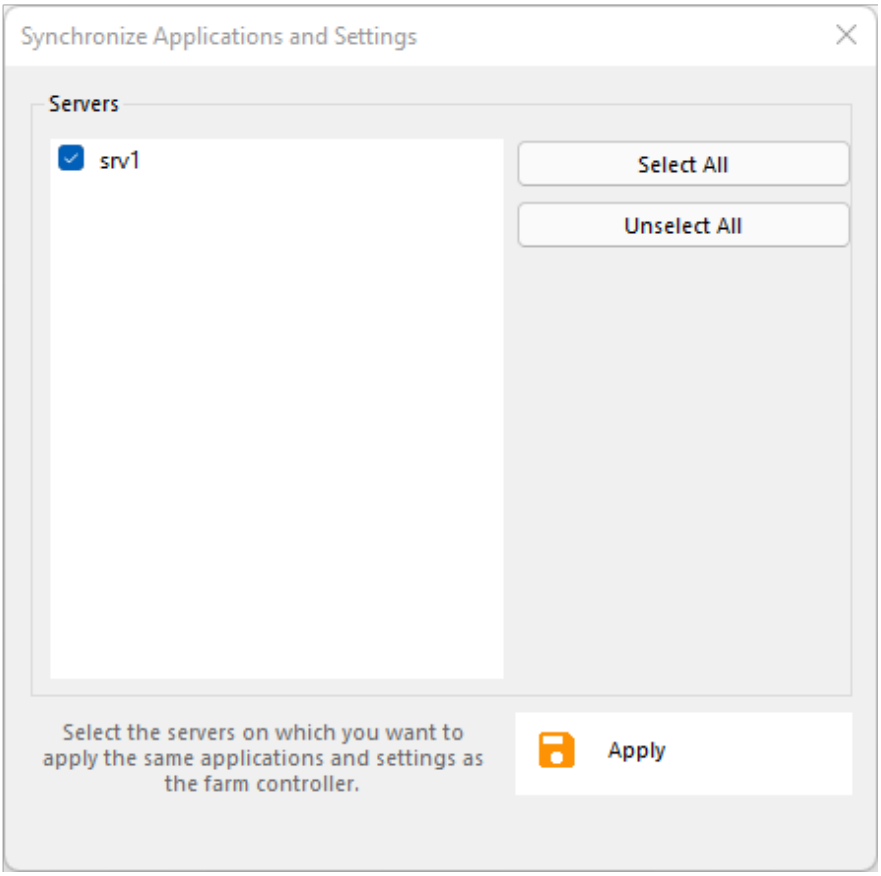
The list of User Sessions is automatically refreshed every 5 seconds. This automatic refresh stops if the selected server becomes unavailable. A click on the “Refresh” button will resume the automatic refresh.

Applications and Settings Synchronization

Overview

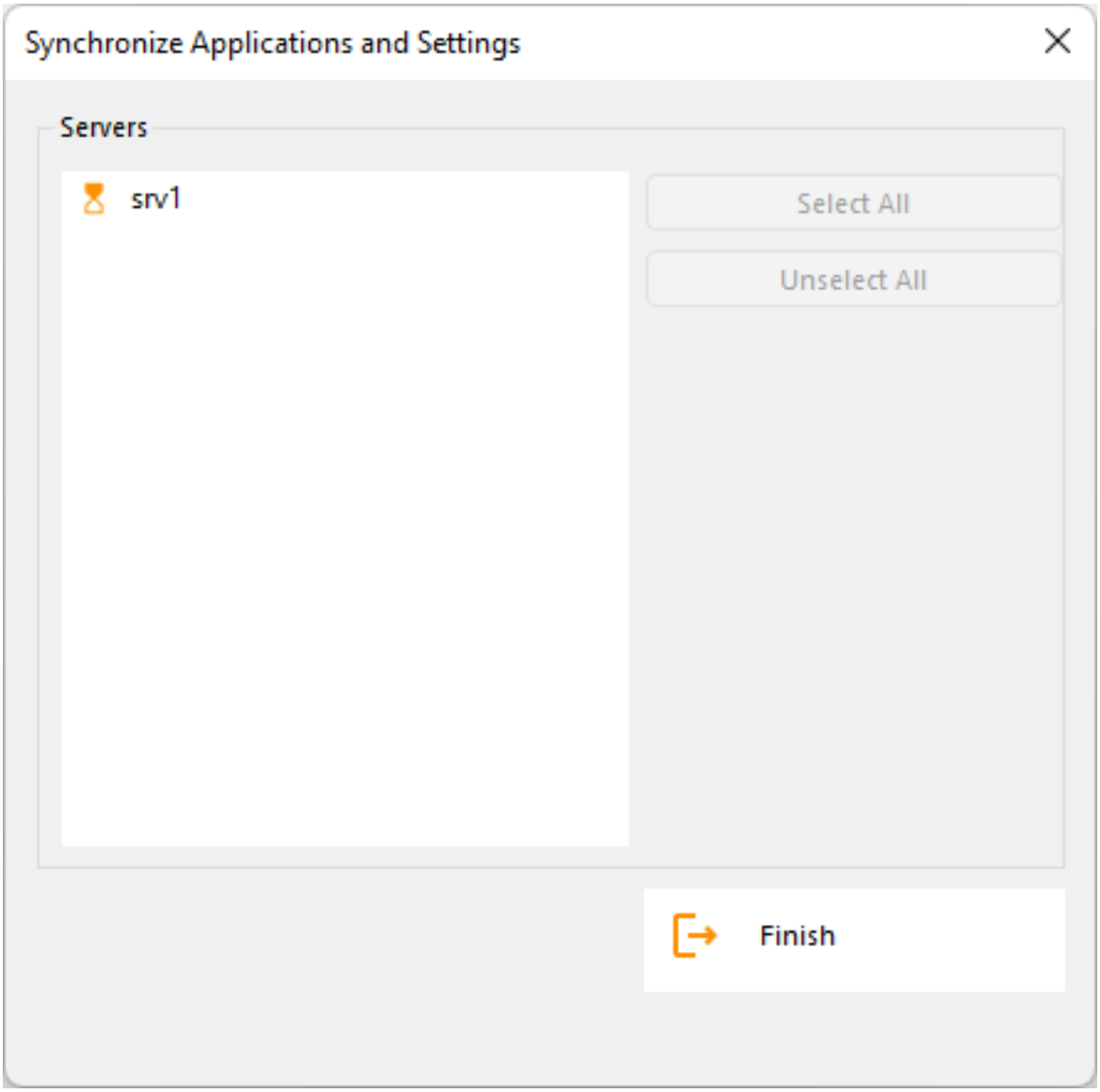


Click on the “Synchronize Applications and Settings” button to display the following window:



Check all the servers on which you want to apply the same settings and publish the same applications as the Farm Controller's, then click on "Apply".

The following window will be displayed, allowing you to monitor the task progress:


Synchronize Applications and Settings
Servers
srv1
Select All
Unselect All
Finish

Fast and easy File Transfer between the User and the Server

Overview

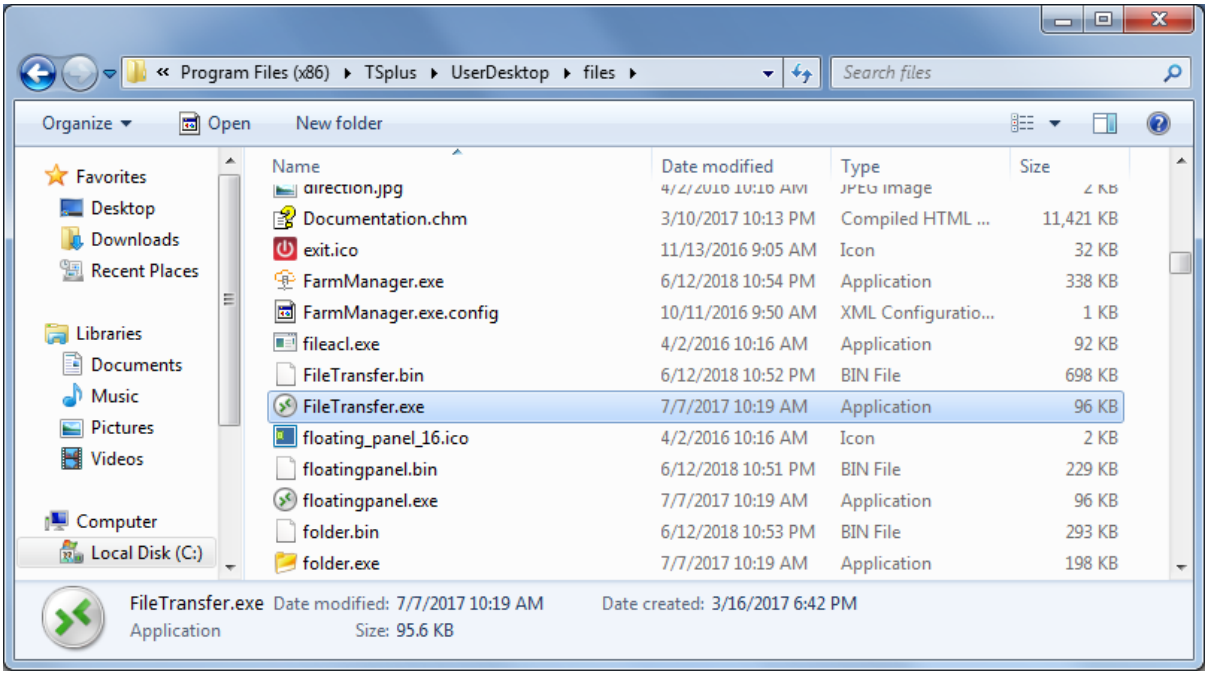
TSplus includes a unique method of transferring files:

- from the local user workstation => to the user Remote Desktop
- from the TSplus server => to the local user Desktop

Because the file transfers are based on a Virtual Channel, it is a lot faster than a file copy, and it can be done **even when the local user disk drives are not mapped**.

FileTransfer program and Generated Clients

The File Transfer program is located in your TSplus program folder, under the name “FileTransfer.exe” into the following path: “UserDesktop\files”



Transferring files

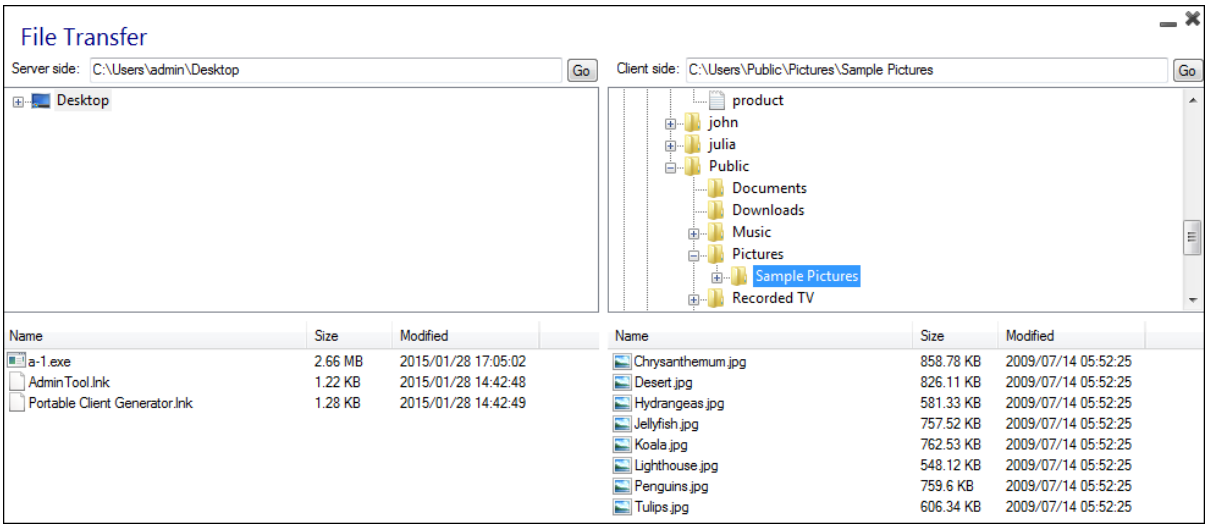
Transferring files is very easy.

First, launch the File Transfer (for instance by using TSplus Floating Panel):

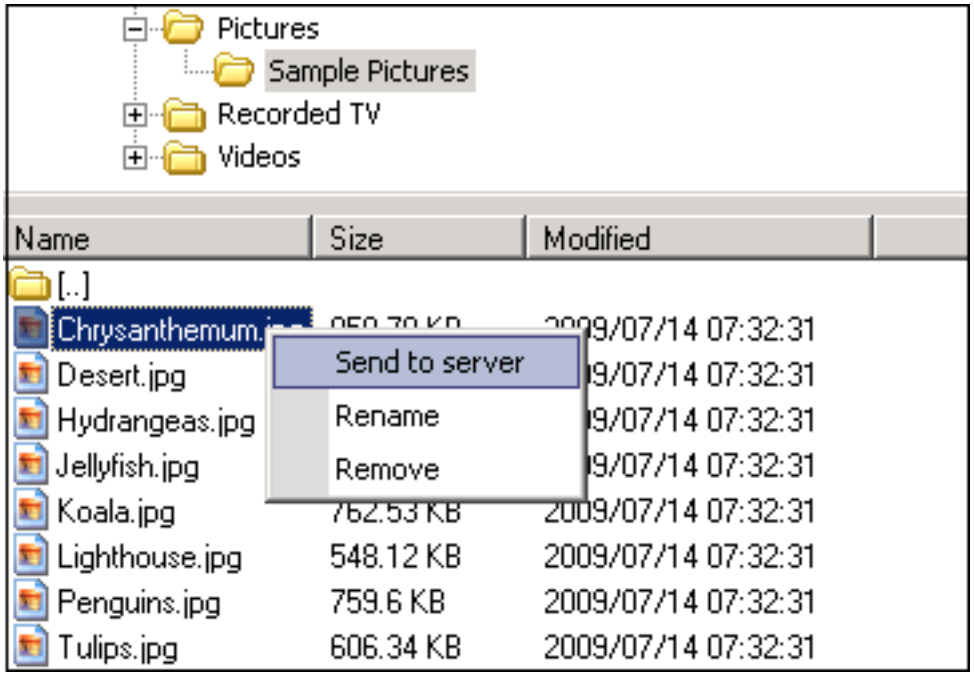


Then navigate to your file using the folders tree:

- server's folders and files are on the **left part of the window (server side)**
- local workstation's folders and files are on the **right part of the window (client side)**



Finally, right click on the file that you want to transfer to the other side, and click on “Send to server” (or “Send to client”):



File Transfer works from the local workstation to the server, as well as the other way around (from the server to the local workstation).

Note: When using the file transfer utility from an HTML5 session, you will be able to transfer your files from server to client only. Please prefer the HTML5 Top Menu method, where you can upload files to the server, download to client and manage your file transfer listing.

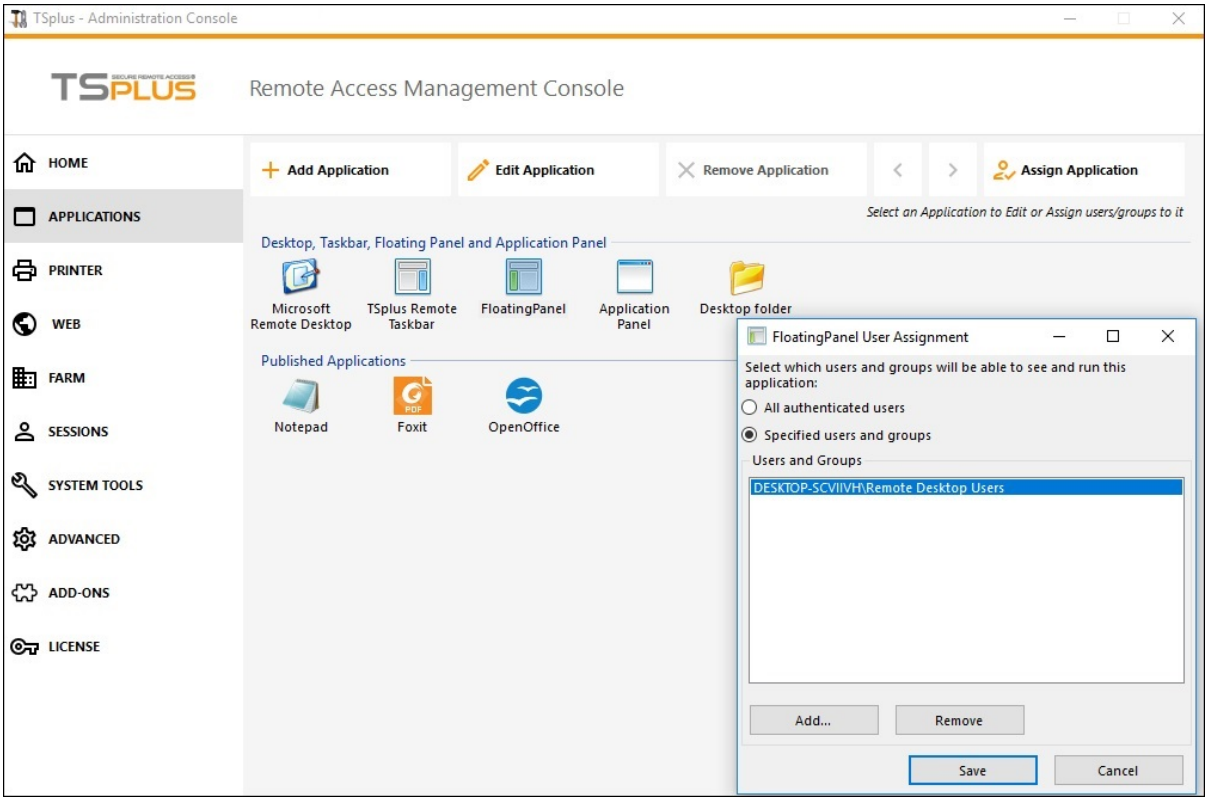
Floating Panel and Application Panel

You can choose to enable the Floating or the Application Panel for your users or groups.

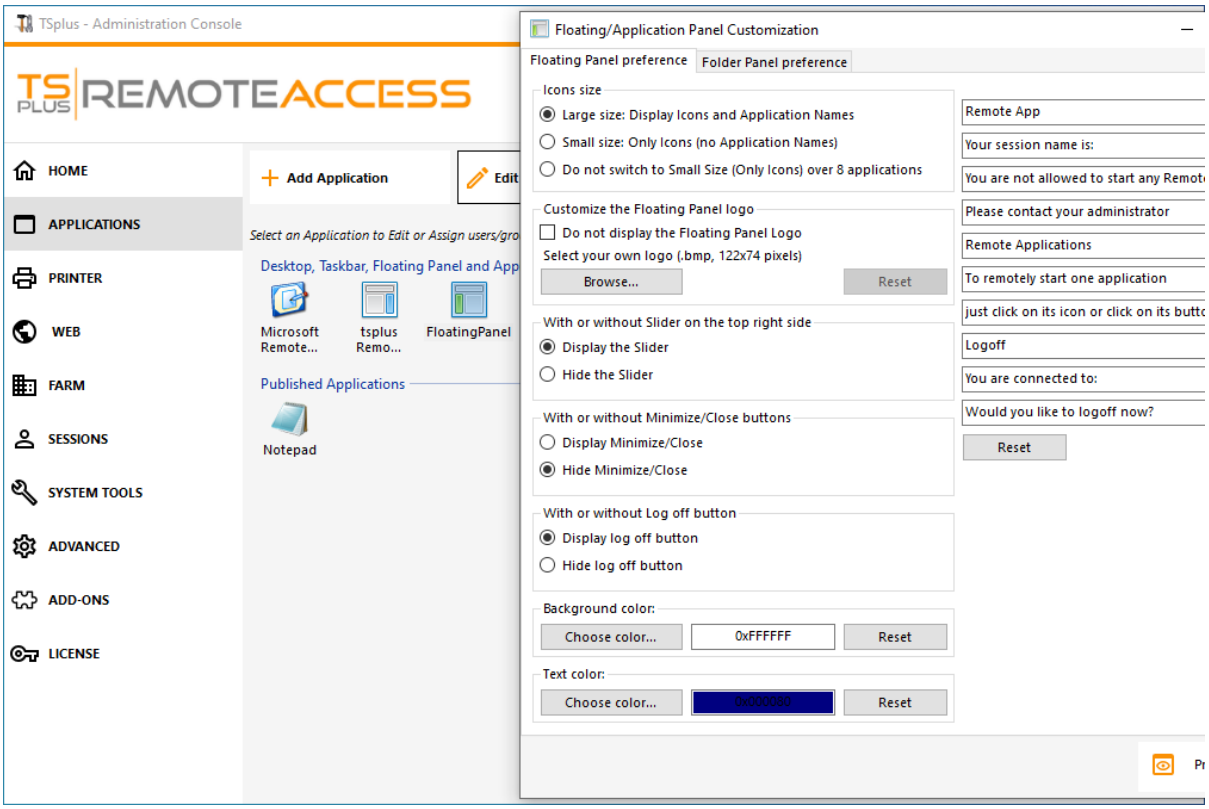
These two ways of publishing applications are available for any connection method.

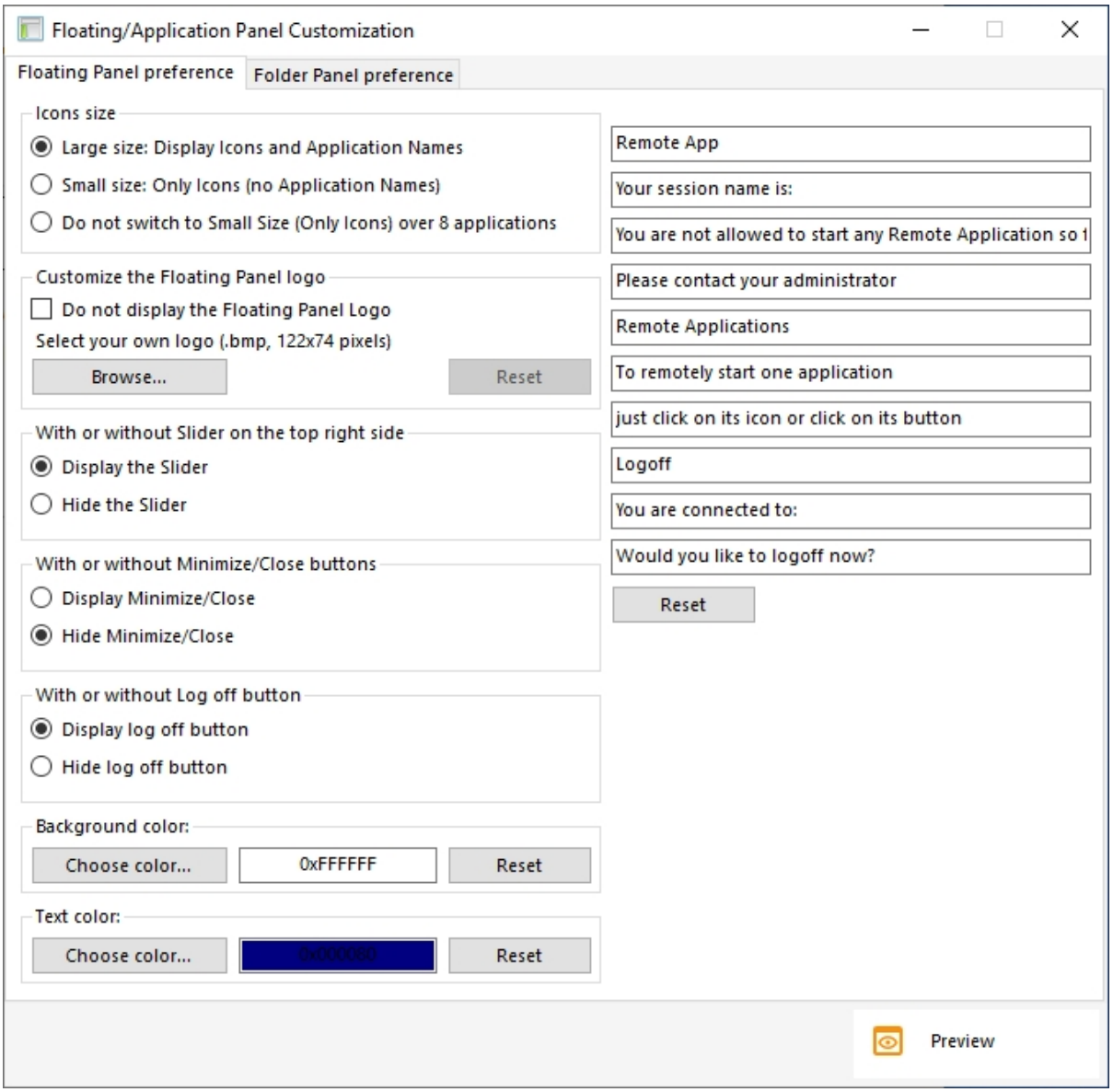
If activated with the assigned applications, you can see on the middle-left of the user screen the mini drop-down list of applications or floating panel (very much appreciated by TSplus users):

Assign it as an application:



Select the Floating Panel, then click on the “Edit Application” tile you to customize the Floating Panel at your convenience:


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


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 Remote Application so t
Please contact your administrator
Remote Applications
To remotely start one application
just click on its icon or click on its button
Logoff
You are connected to:
Would you like to logoff now?
Reset
Preview

These various options can allow you to customize the end user's experience.

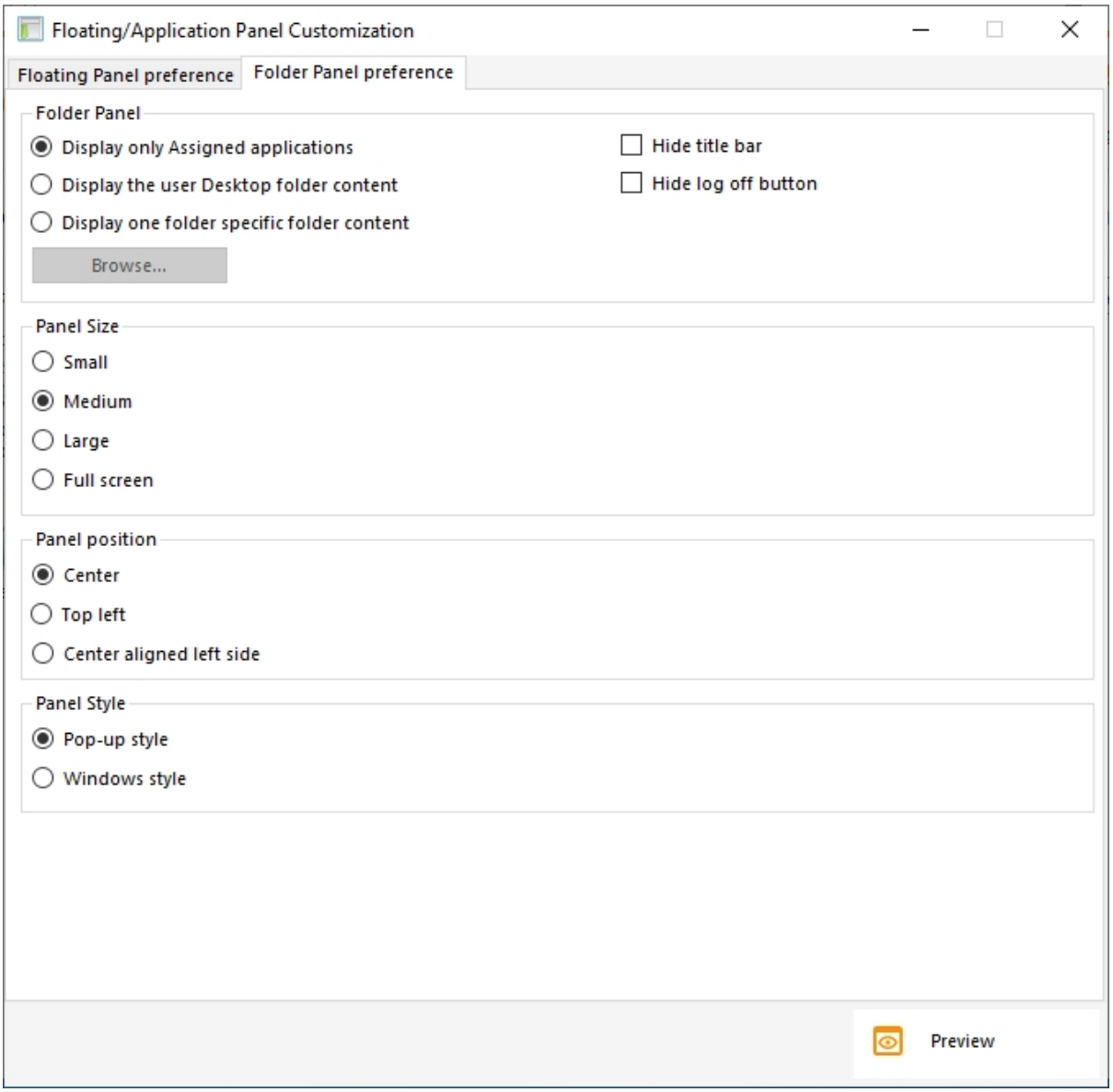
Here are the different Floating Panel display options, where you can set ,

- Modify the displayed text,
- Choose your preferred size, between Large and small, where you can display only icons,
- Add your own Logo,
- Customize color for the background and for the text,
- Display the slider or not,
- Display the Minimize/Close buttons or not,
- Display the Logoff icon or not…

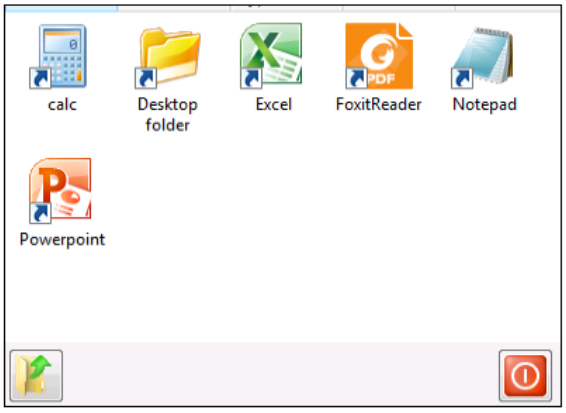


Please note that over 8 applications, the Floating Panel automatically switch to small-size. If you still want it to display the Applications names, select "Do not switch to Small Size (Only Icons) over 8 applications.

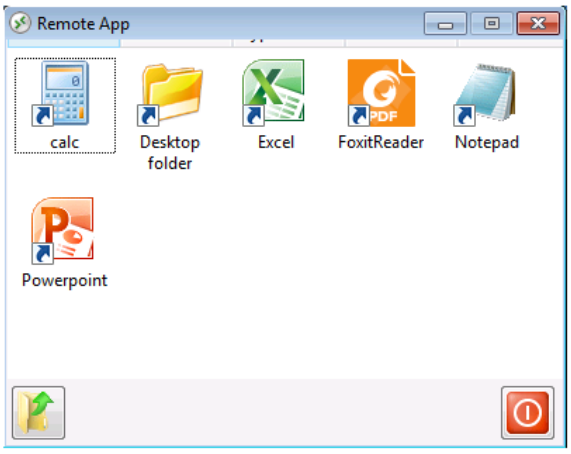
The **Folder Panel** is customizable as well and enables to display the assigned applications, the user Desktop folder or one specific folder content in your session with many display options:



You can change the Folder Panel size, position and style (Pop-up or Windows) at your convenience:

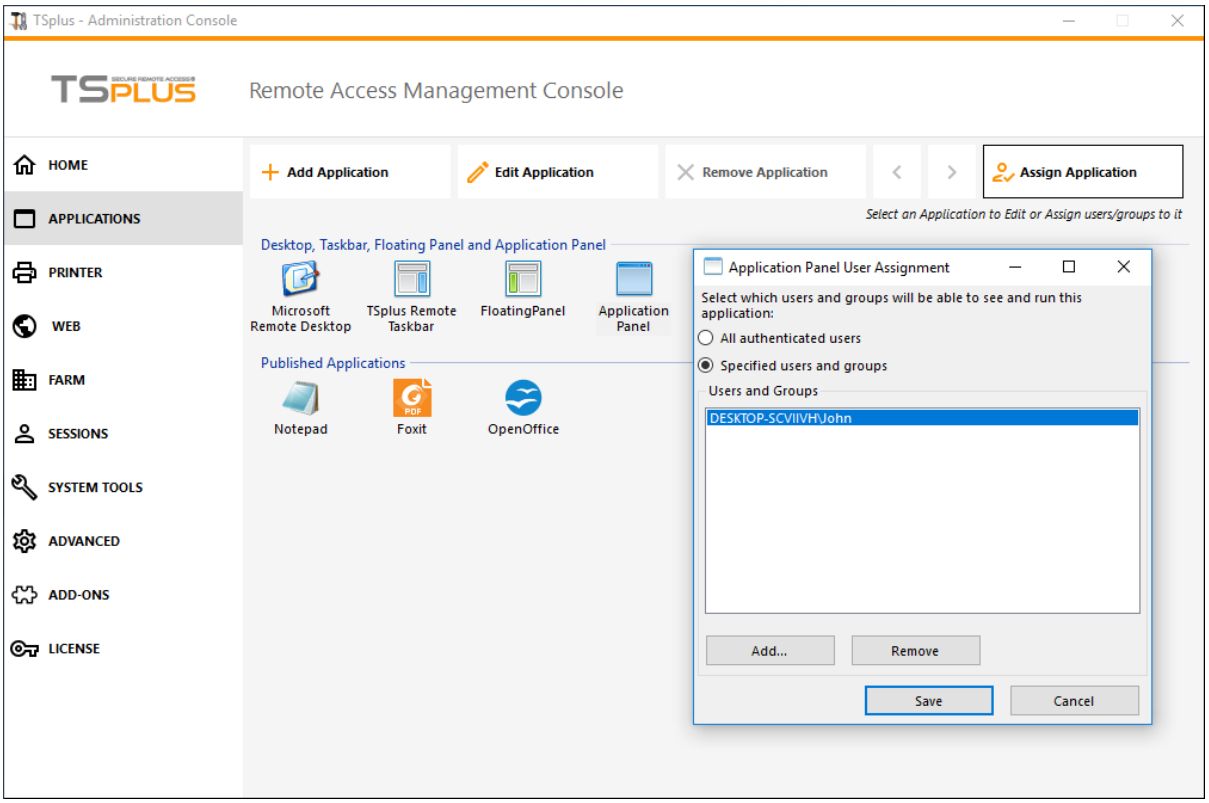


Pop-up style

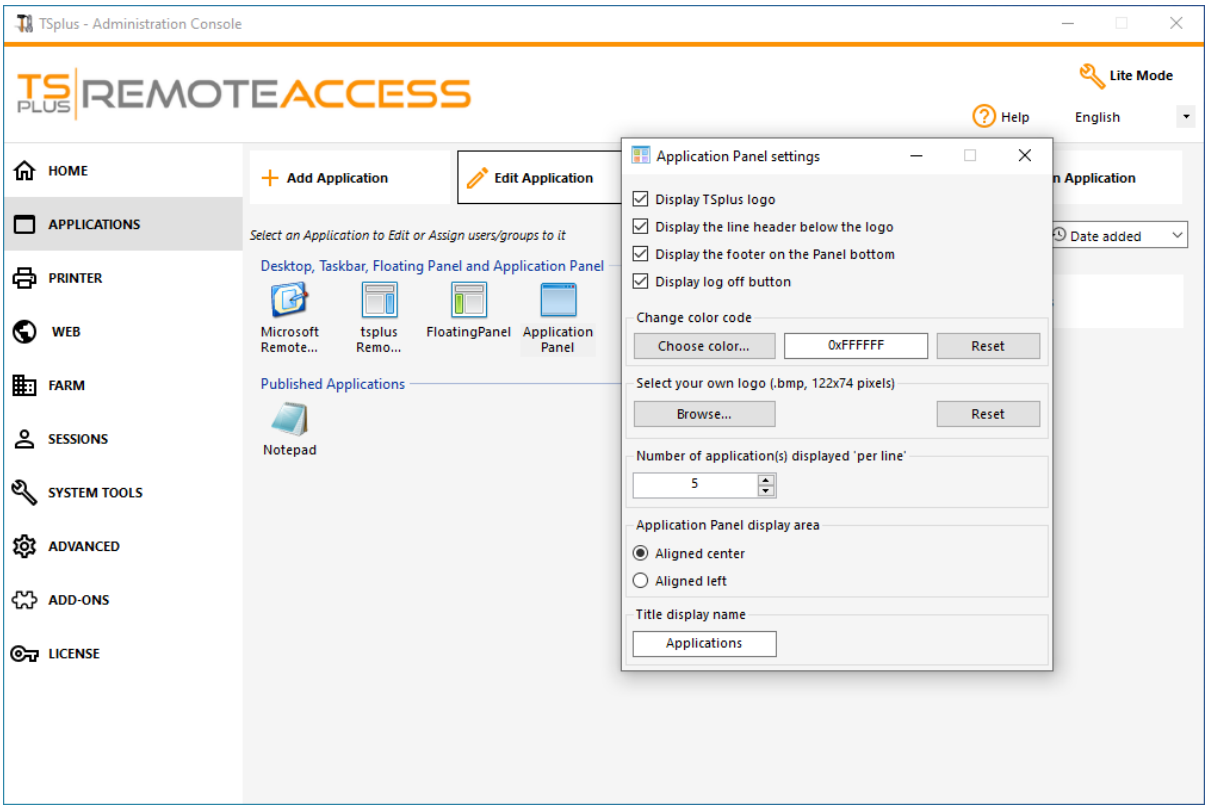


Windows style

The Application Panel gives you the possibility to organize the displayed applications, exactly like on the Web Application Portal, but by simply assigning it to one user or group:



The Administrator can customize it by choosing to display the TSplus logo or his own logo, display the line header below the logo and the footer, change the color or choose to not display any of it at all by unselecting the corresponding boxes. He can also adjust the number of displayed applications by lines and columns by entering the number of applications displayed per line, as well as the alignment and name of the Application panel.



For example, display six Apps in one column, without logo; or displayed on 2 columns and 3 lines, with the TSplus logo:


Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

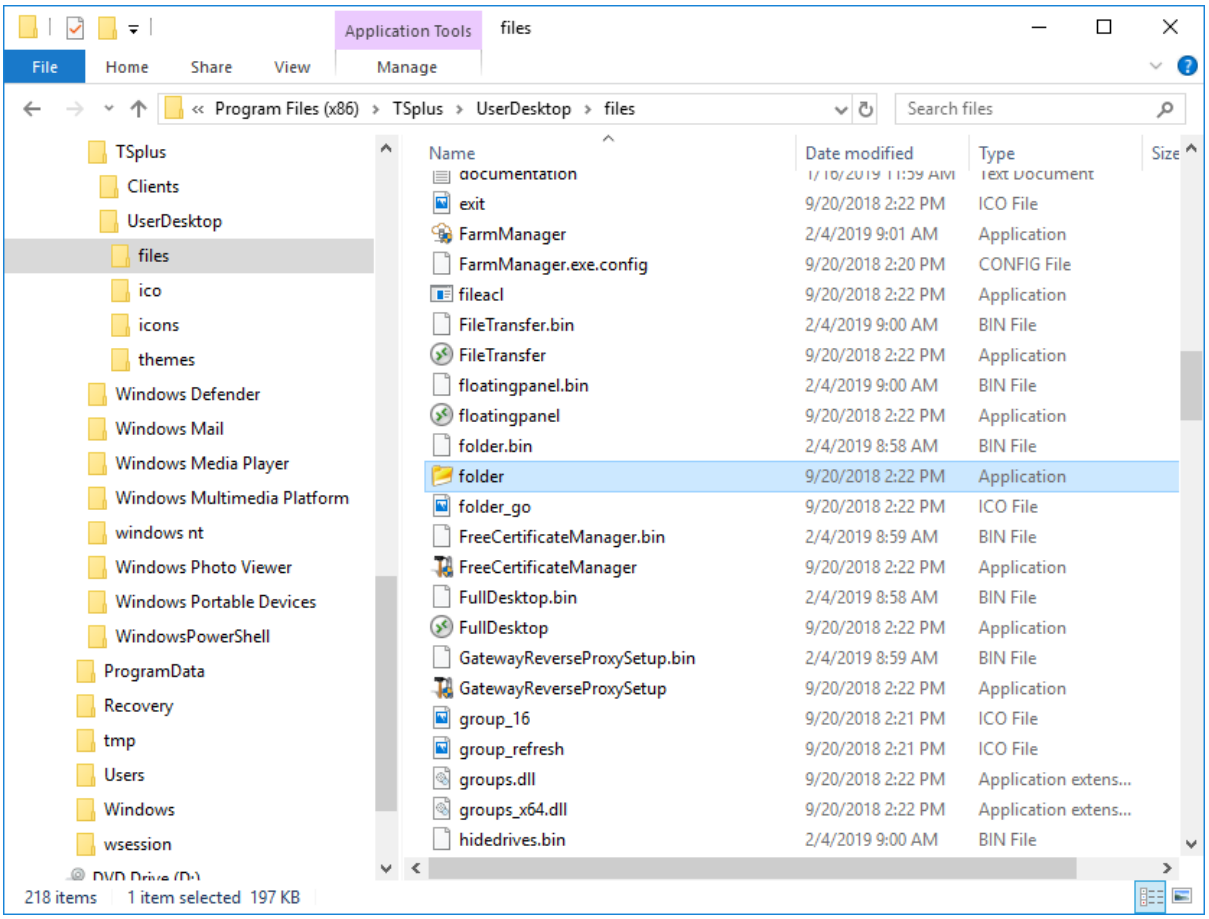

TSPLUS
Notepad
FoxitReader
Excel
Powerpoint
calc
Desktop folder

Secured Folder Sharing - Folder.exe

The Folder application will securely display the content of a folder that you will make available for your users.

First, create a folder on your server with Applications or documents that you want to share.

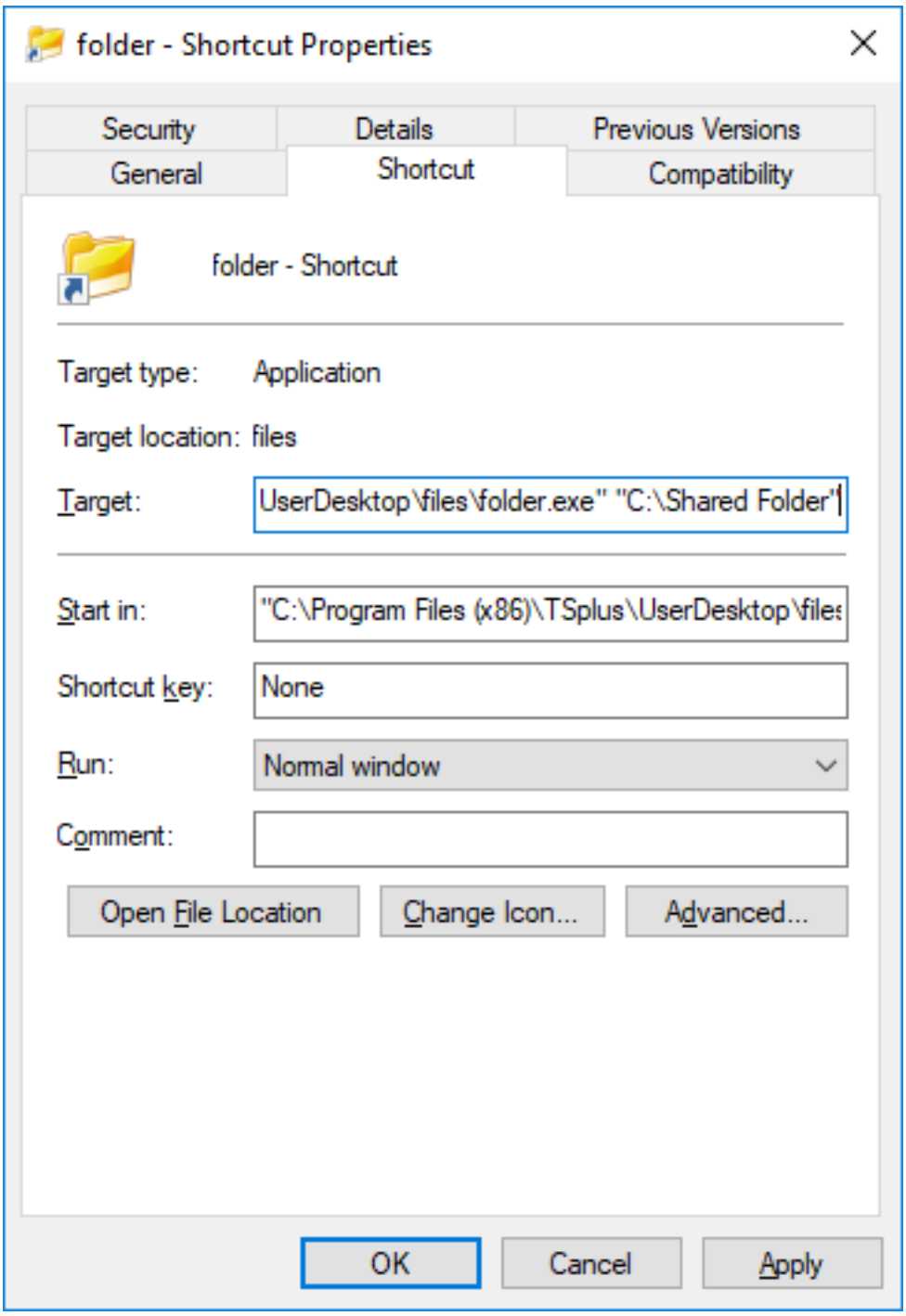
Open an explorer.exe and locate the folder.exe application in C:\Program Files\tsplus\UserDesktop\files:



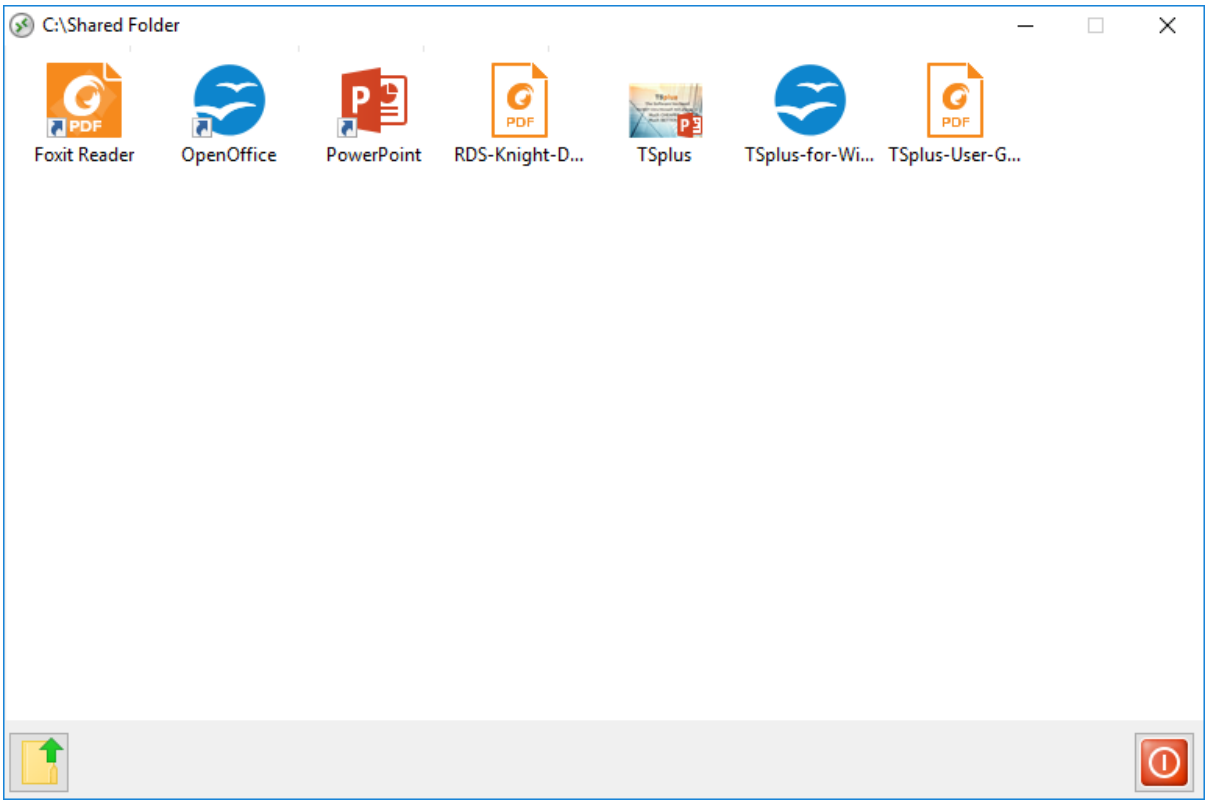
Create a shortcut of this file. Edit the properties of this shortcut by right clicking on it.

Then modify the target path of the shortcut by entering the path of your applications folder on the “Target” line, after the original target path, for example:

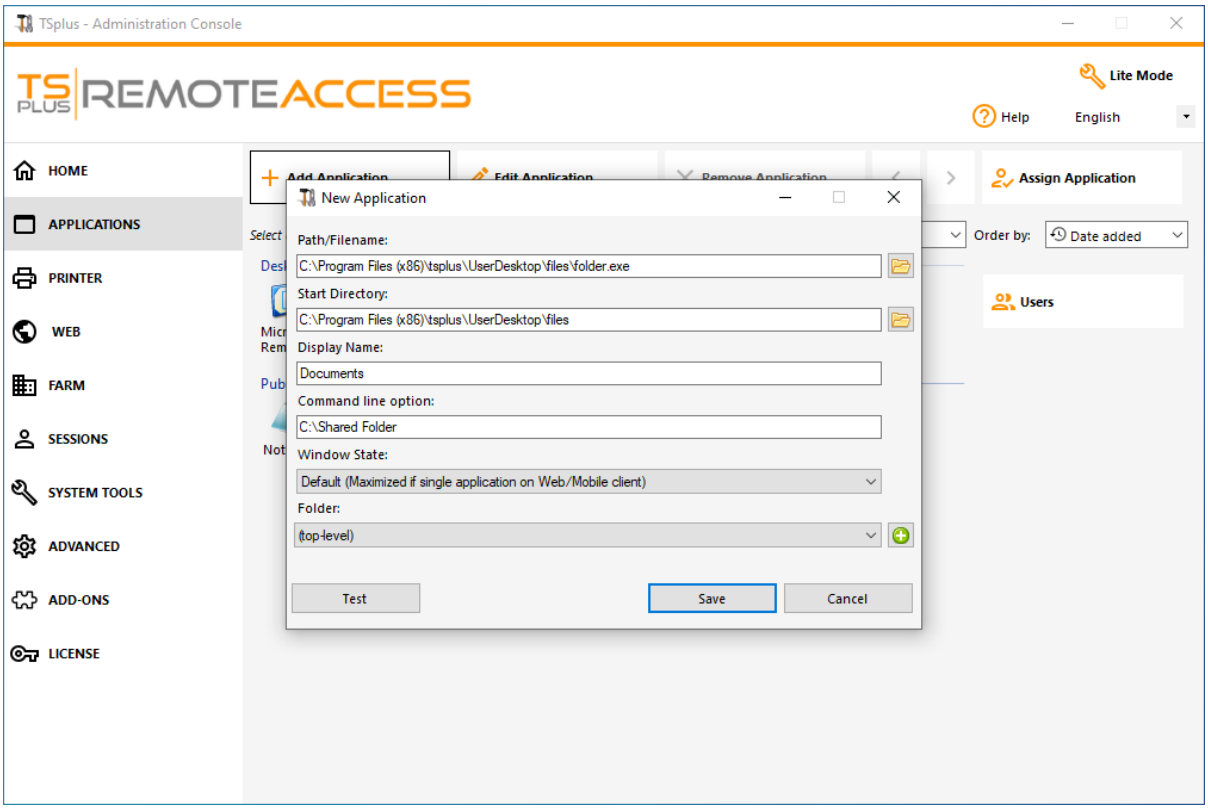
“C:\Program Files\tsplus\UserDesktop\files\folder.exe” “C:\Shared Folder”



When you open the folder.exe shortcut, it should look like this (with your own documents and applications):



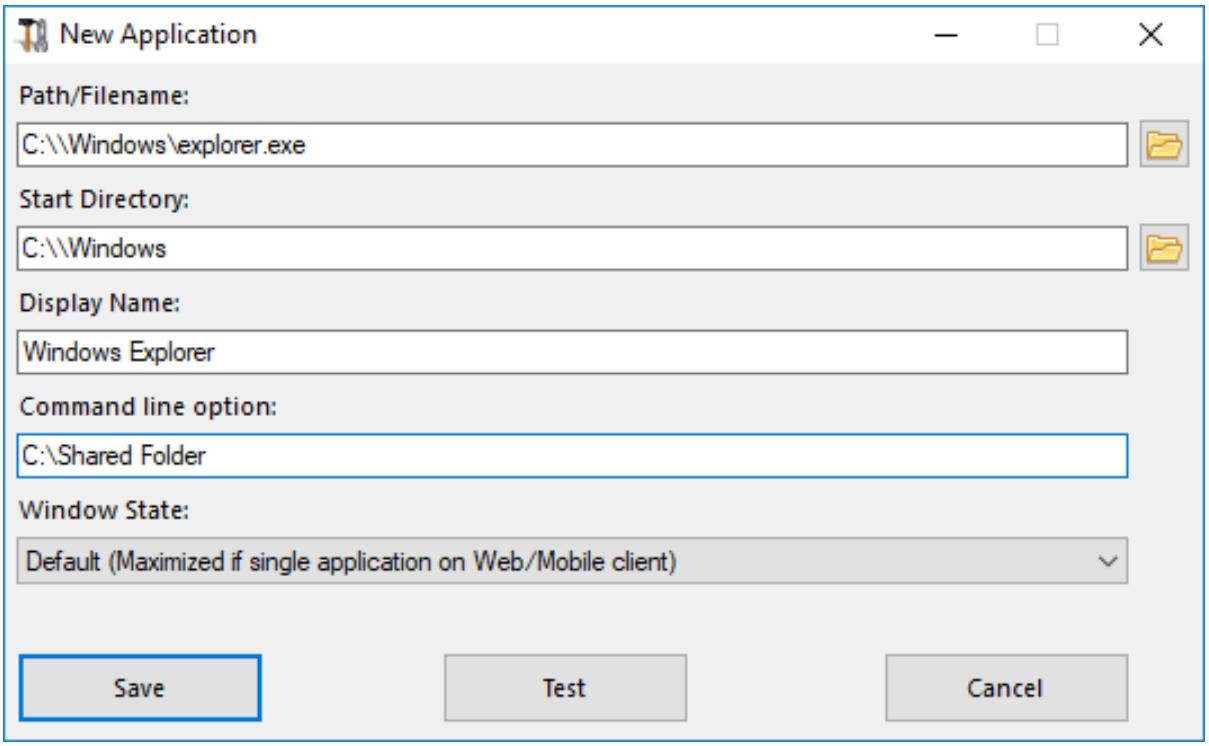
This shortcut can be copied to a user's profile desktop folder or you can publish the folder.exe for a user as an application. If you do the latest, you will have to indicate the path of your folder in the Command Line option section:



There is an alternative way of sharing a Folder of documents.

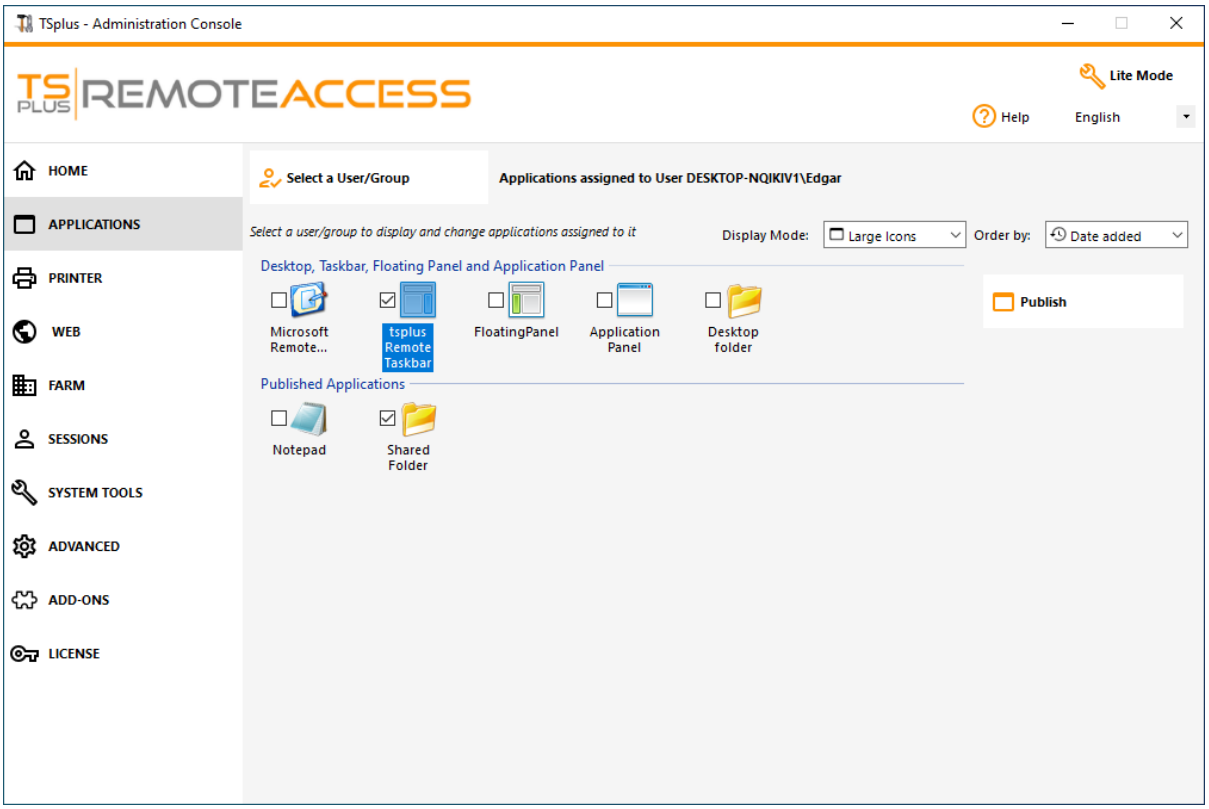
Publishing a shared folder as a unique application :

Add a new application. In the display name type in the name of the shared folder or any name you want. Click on the browse button located on the right side of the “Path/Filename” field and locate C:\Windows\explorer.exe. The start directory will be filled in automatically with the path of explorer.exe. In the Command line option field, type in the path of the shared folder, it can be a local folder or a network shared folder using a UNC path (example : \data\shared folder) Fill in the field below with your shared folder information:

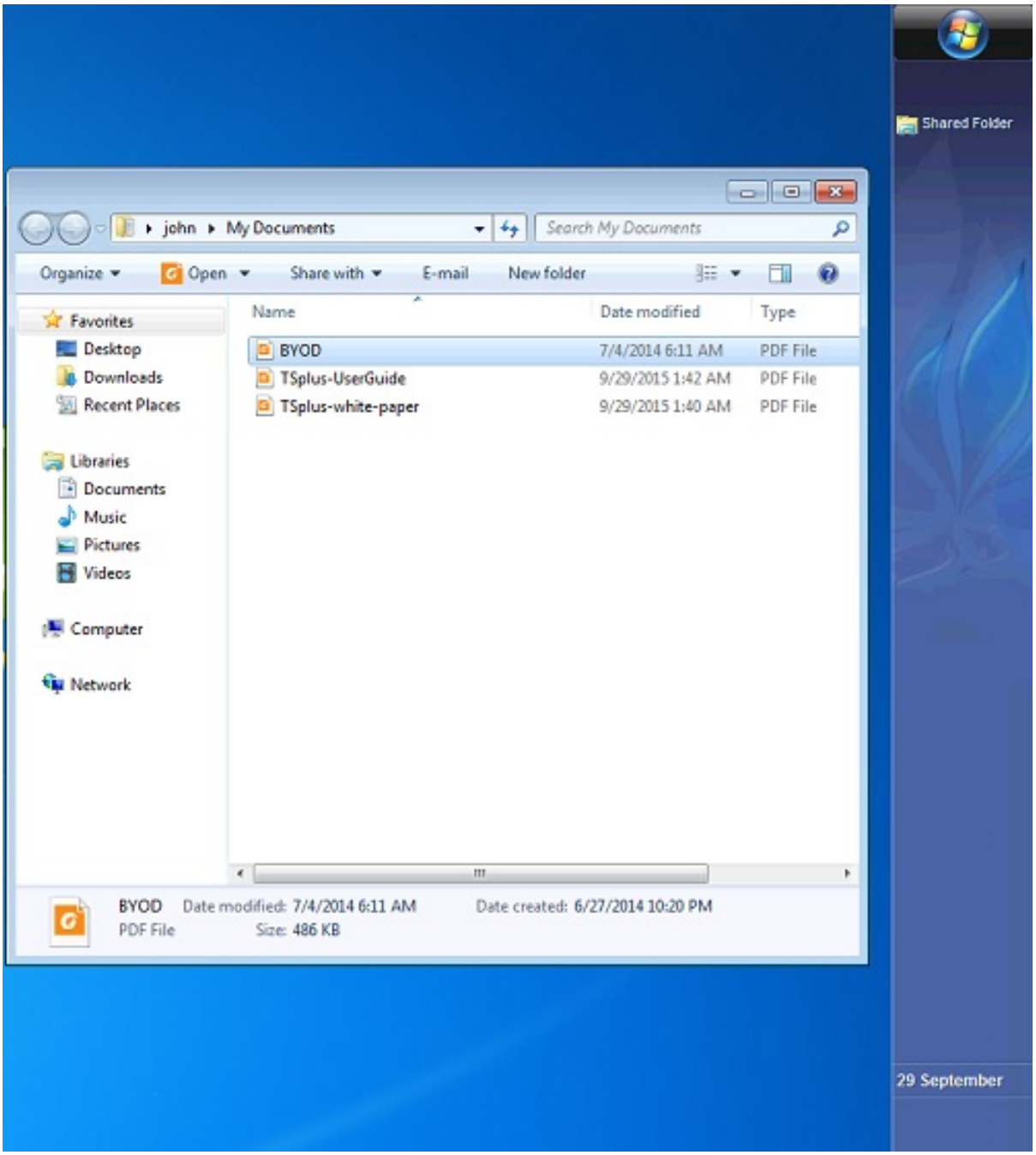


Then click on “Save”.

Click on the “Users” tab. Select your user and check the TSplus Remote Taskbar and Shared Folder boxes:

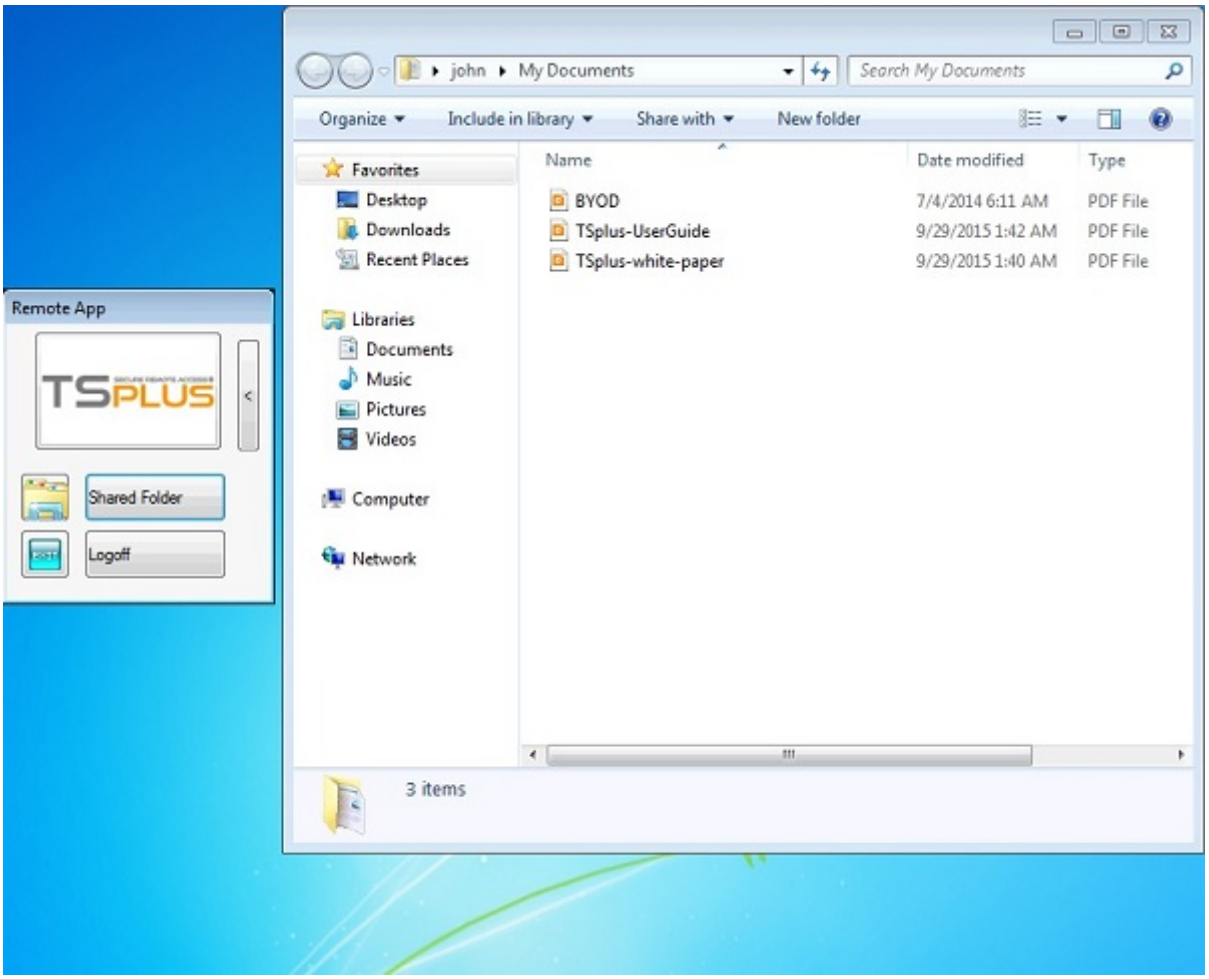


Here is the result, when you open a session with an rdp client, you will see the TSplus taskbar with the shared folder application:



You can also do this with the floating panel. Open an admin tool and click on the “Assign application” tab. Check the Floating Panel and the Shared Folder boxes.

Here is the result:


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

Free and Easy-to-install HTTPS Certificate

Overview

Starting with version 9.20, TSplus provides an easy to use feature to generate of a free and valid HTTPS certificate.

In 3 mouse clicks you will get a secured valid certificate, renewed automatically, and configured automatically into TSplus built-in web server.

This feature uses Let's Encrypt to provide a free and secure HTTPS certificate for your HTTPS connections.

Prerequisites

Please ensure that your TSplus server meet these requirements before using the Free Certificate Manager:

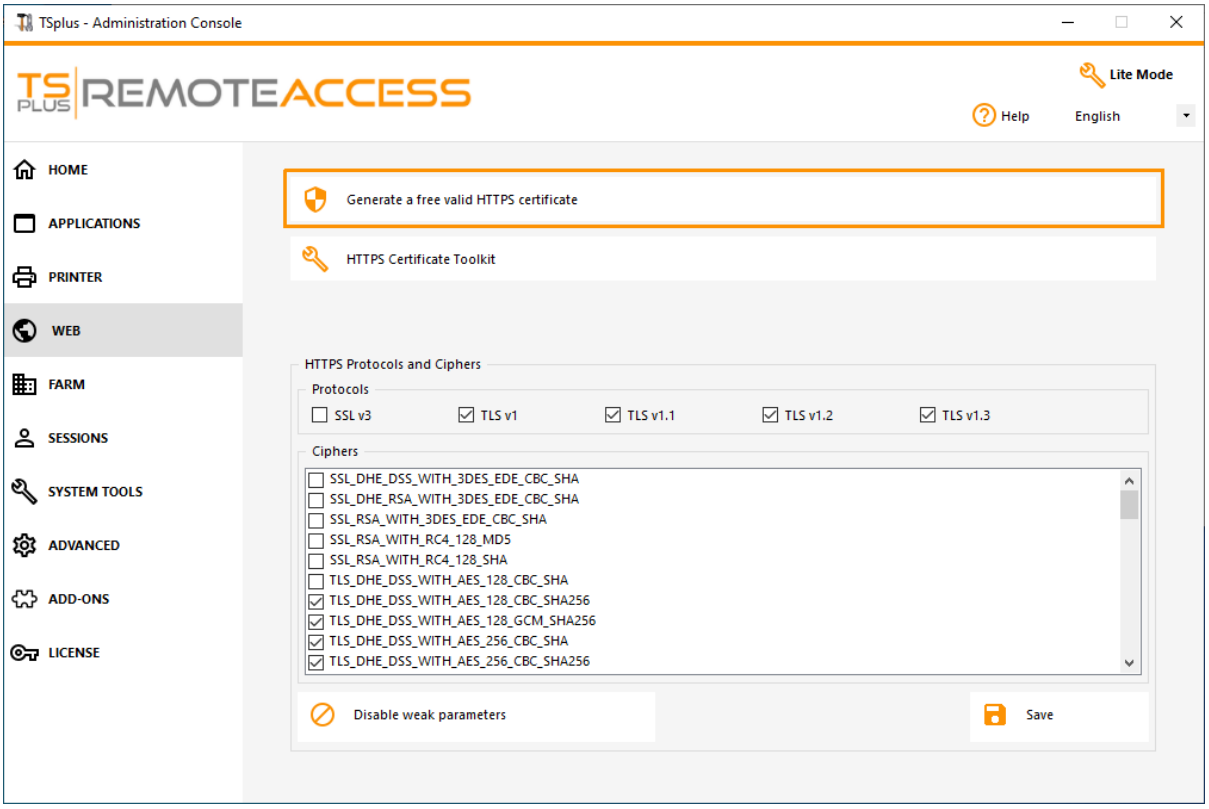
- You must **use TSplus built-in web server listening on port 80 for HTTP**. This is required by Let's Encrypt domain ownership validation process.
- Your **server's domain name must be accessible** from the public Internet. This is required as well to validate that you are the real owner of the domain.
- You must **run this program on the Gateway server or a Standalone server, not an Application server** (except if your Application Server is accessible from the public Internet and has a public domain name).

It is not possible to get a certificate for an IP address, be it public or private.

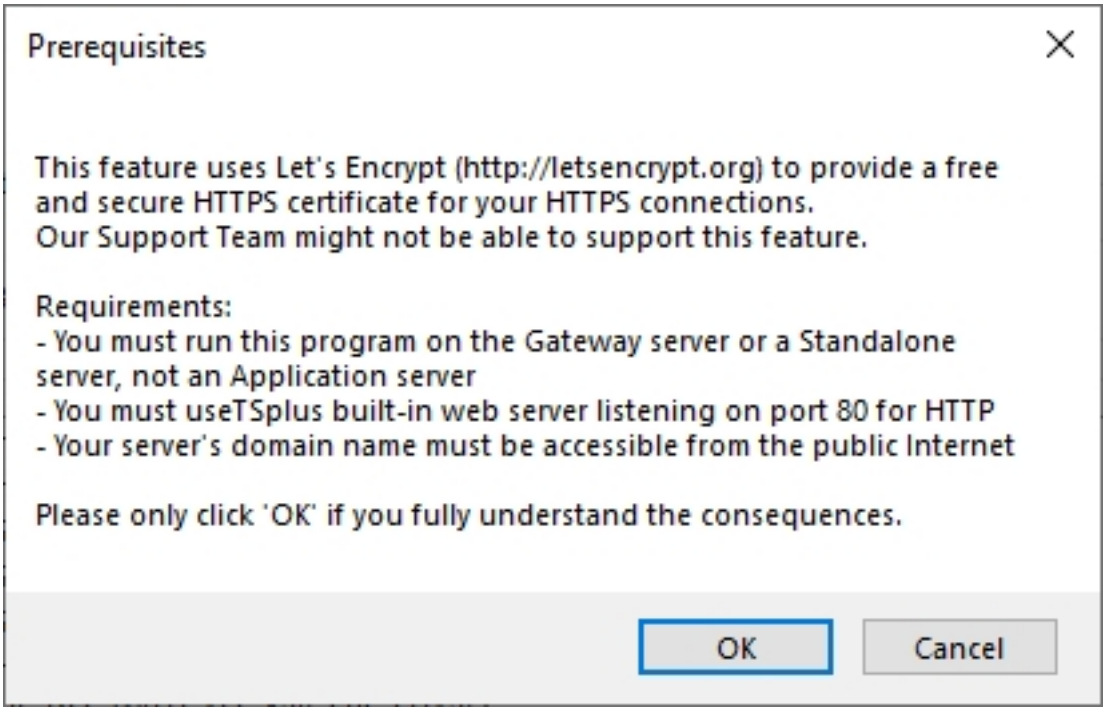
It is not possible to get a certificate for an internal domain name (i.e. a domain which only resolves inside your private network).

Free Certificate Manager GUI

To open TSplus Free Certificate Manager GUI, open TSplus AdminTool, click on the “Web - HTTPS” tab, then click on “Generate a free valid HTTPS certificate” as shown in the screenshot below:



The Free Certificate Manager GUI will open and remind you about the prerequisites, as shown in the screenshot below:



Please read carefully and check that your server meet all the requirements, then click on the “Ok” button.

Step 1: Enter your Email

This email will not be used to spam you. Actually it will not even be sent to TSplus or any third party, except the certificate issuer: Let’s Encrypt.

They will only contact you if needed, according to their Terms Of Service.

Step 2: Enter the server’s Domain Name

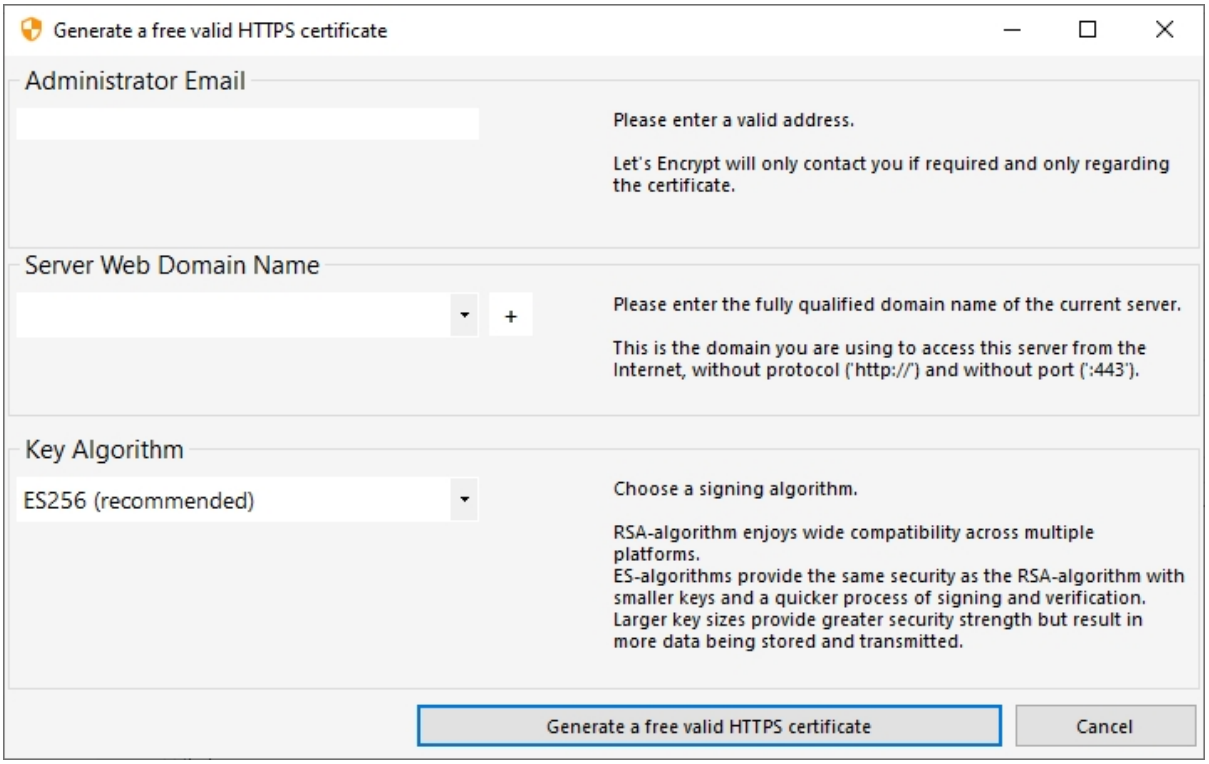
This is the public Internet accessible Domain Name, something like gateway.your-company.com. You can also add another domain name or a subdomain name after clicking on the ”+” button.

As explained in the GUI, do not add a protocol prefix and/or a port suffix, just enter the clean domain name(s).

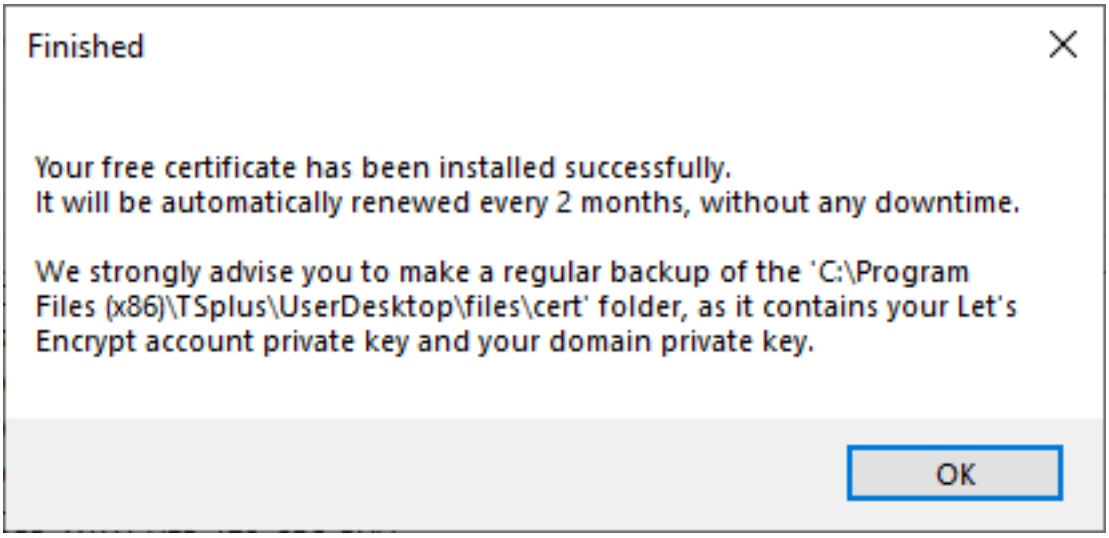
The certificate will be generated for this domain name, and it will only be valid on a web page hosted at this domain name. If your users connect to your Web Portal using https://server1.example.com:1234, then you must enter “server1.example.com”.

Step 3: Choose a Key Algorithm

It will be used to create key pairs and perform digital signature operations.



Enjoy your Certificate!



TSplus Free Certificate Manager will now use all the data to connect with Let's Encrypt, validate that you really own the domain name you typed, and get the matching valid certificate.

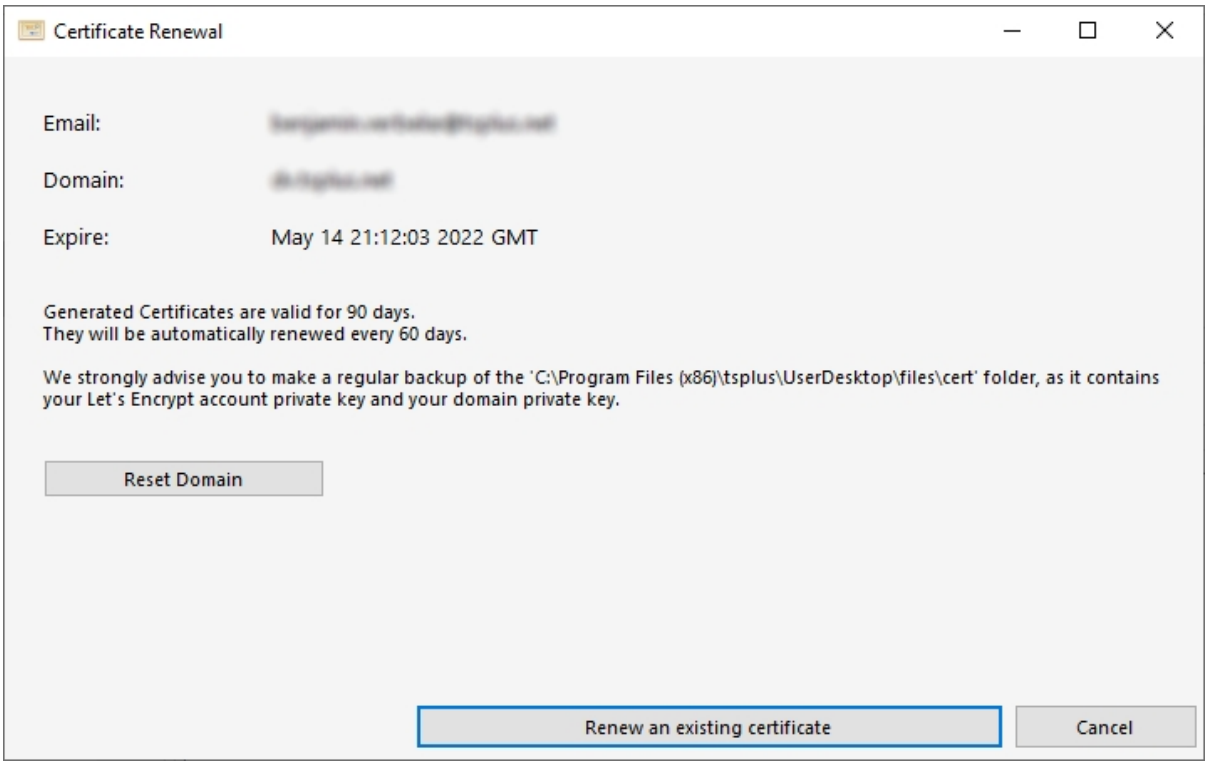
Once the program receives the certificate, it will automatically handle all the required file format conversions and softly reload TSplus built-in web server in order to apply the new certificate to every new connection. The web server is **not** restarted and no connection is stopped.

Certificate Renewal

Let's Encrypt certificates are valid for 90 days. Validity period will be cut in half to 45 days by 2028, as well as the rest of the industry.

TSplus will automatically renew the certificate every 15 days for safety. A check is done at every reboot of the Windows server, and then every 24 hours.

You can manually renew your certificate by opening the Free Certificate Manager tool. It will display the domain name of the certificate and its expiration date, as shown in the screenshot below.



To manually renew your certificate, just click on the “Next” button.

The “Reset Domain” button on this window deletes the SSL certificate and reconfigure the Web Server to its original state before using the Certificate Manager.

Best Practices

If no error occurs, TSplus will renew the certificate automatically every 15 days. We recommend that you **check every 45 days** that your certificate has been automatically renewed. Let’s Encrypt currently issues certificates valid for 90 days, which will be cut in half to 45 days by 2028.

We also recommend that you **backup at least every month** the following folder and its sub-folders:

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

This is an internal folder, containing your Let’s Encrypt account private key, as well as the key pair of your certificate.

Troubleshooting

In case of an error, please contact support and email them the following log file:

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

This log file (and maybe the other log files in the same folder) should help our support team to investigate and to better understand the issue.

If you want to restore a previously used certificate, go to the folder:

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

It will contain every “cert.jks” files used. These are the “key store” files and we never delete them, we only rename them with the date and time of their disabling.

Error Codes

- Error 801: Free Certificate Manager was not able to register your Let’s Encrypt account. Check your Internet connection. Check that your email is not already registered at Let’s Encrypt. Try again with another email.
- Error 802 & Error 803: Free Certificate Manager could not retrieve Let’s Encrypt Terms Of Service URL address. This is a non blocking error: you can still continue and accept Let’s Encrypt Terms Of Service - be sure to read them from your browser first of course.
- Error 804: Free Certificate Manager was not able to validate your agreement to Let’s Encrypt Terms Of Service with Let’s Encrypt servers. Check you Internet connection. Try again.
- Error 805 & Error 806: Free Certificate Manager was not able to validate that you own the domain you entered during certificate creation (Error 805) or certificate renewal (Error 806). Check again all the prerequisites. Check your Internet connection. Check that your web server is listening on port 80. Check that you do not use a third-party web server such as IIS or Apache. Check that your domain name is accessible from the public Internet.

HTTPS Certificate Command Line

Preparing the Certificate Configuration File

Inside the “C:\Program Files (x86)\TSplus\UserDesktop\files\cert” folder, create a file named “FreeCertificateManager.ini” if it does not already exist. Make sure your text editor and/or Windows file explorer does not add an ending “.txt” extension.

Edit the file and write or update it so it has the following format, then save it:

[settings]

email = your.email@company.com

domain = your-server- domain-name.company.com

Creating the Certificate

As a server administrator, run the following command:

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

In order for this command to be successful:

- The “FreeCertificateManager.ini” file must exist and use the expected format
- Your TSplus Remote Access server must be up and running
- Your TSplus Remote Access Web Portal must be available with protocol

HTTP on port 80 from the internet public network, as TSplus HTTPS certificate provider will use that to validate the server domain name

Renewing the Certificate

Once the certificate is configured and created, TSplus Remote Access will automatically renew it every two months to make sure it never expires.

Adding a Third Party Certificate

Inside the “C:\Program Files (x86)\TSplus\UserDesktop\files\cert” folder, create a file named “certpassword.txt” containing only the certificate password. As a server administrator, run the following command:

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

If you are using TSplus Advanced Security you might need to temporarily disable the Geographic Protection feature for it to work. You can delete your password file after running the command.

Prevent RDP access and allow HTTP on the Gateway Server

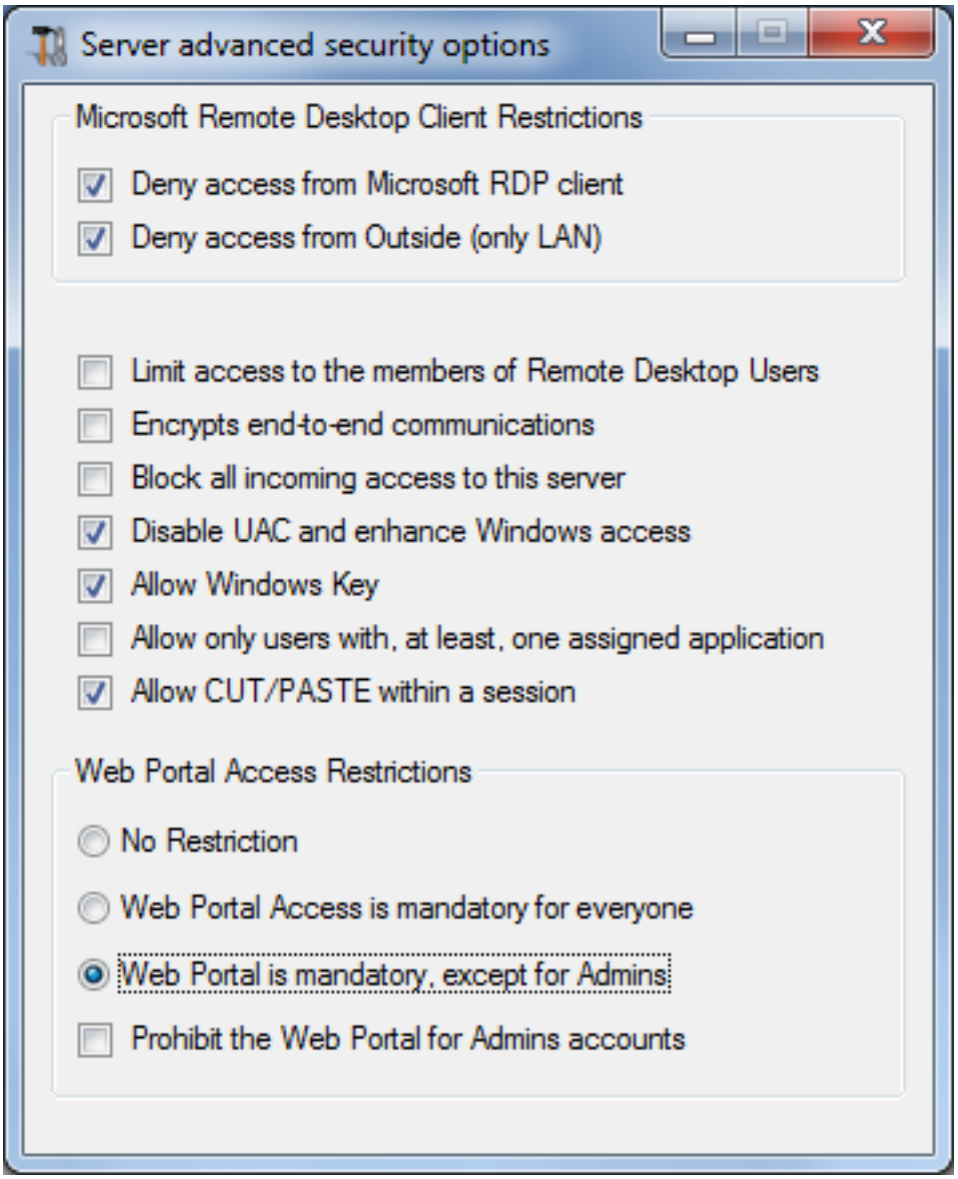
There are 2 ways to access the Gateway Server:

- HTML5 / HTML
- RDP Session (via the Gateway IP/DNS – Port number)

How to LOCK DOWN HTML/HTML5

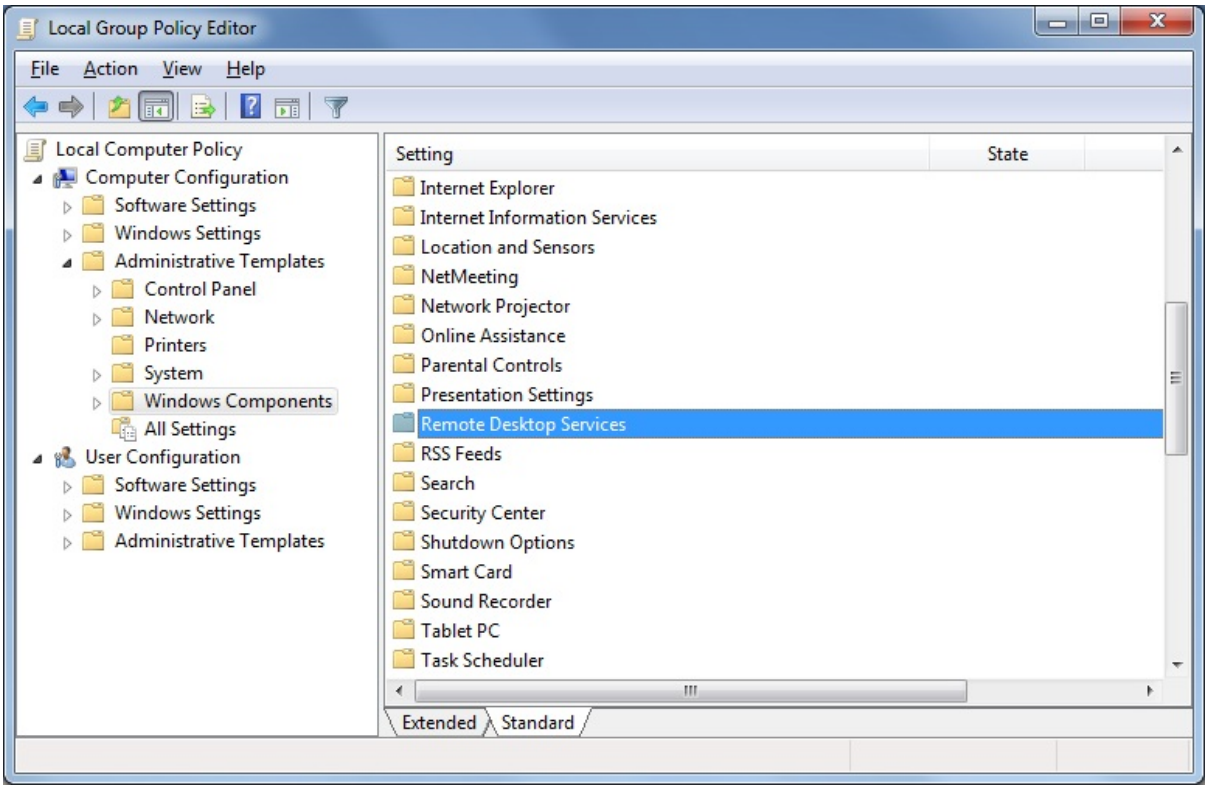
We can use mstsc with a PORT number and RDP into a TSplus Application / Gateway Server.

However, if we use these advanced Security tools located the TSplus Admin Console on the Gateway Server, by going on the Security tile/tab, then clicking on the Advanced Security options tile…:

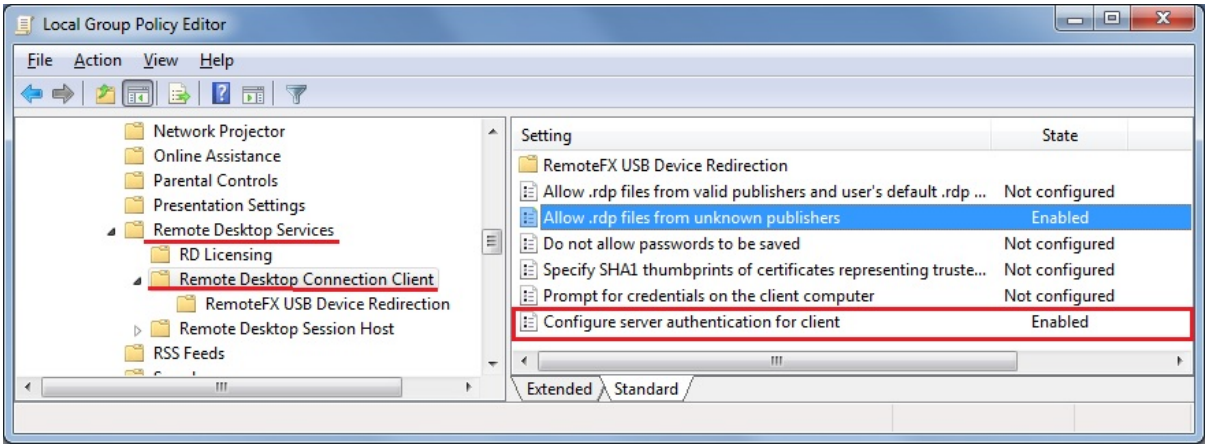


…the access is denied when trying to connect with RDP. To avoid this behavior, on the Gateway Server, you will have to do the following:

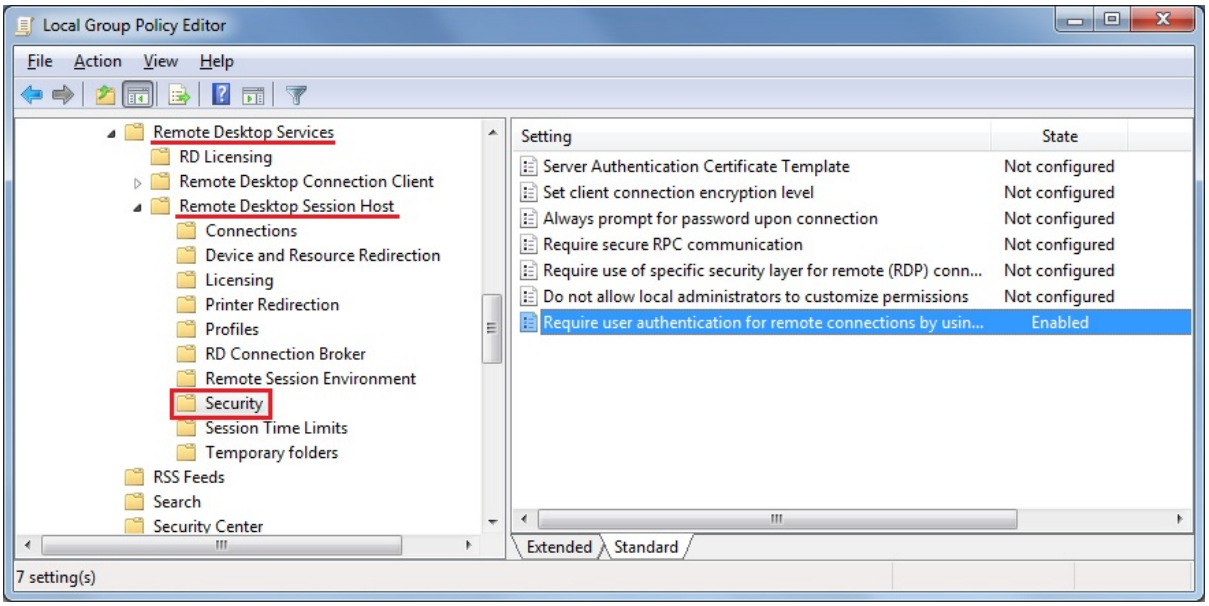
- Go to Gpedit.msc, then under Computer Configuration, click on the Administrative Templates folder, on the Windows Components folder and on Remote Desktop Services:



- Then, click on the Remote Desktop Connection Client folder, double-click on the “Allow .rdp files from unknown publishers” setting and enable it, as well as the “Configure server authentication for client”:



- Under the Remote Desktop Client menu, click on the Remote Desktop Session Host folder, then on the Security folder. Enable the “Require user authentication for remote connections by using Network Level Authentication” setting.

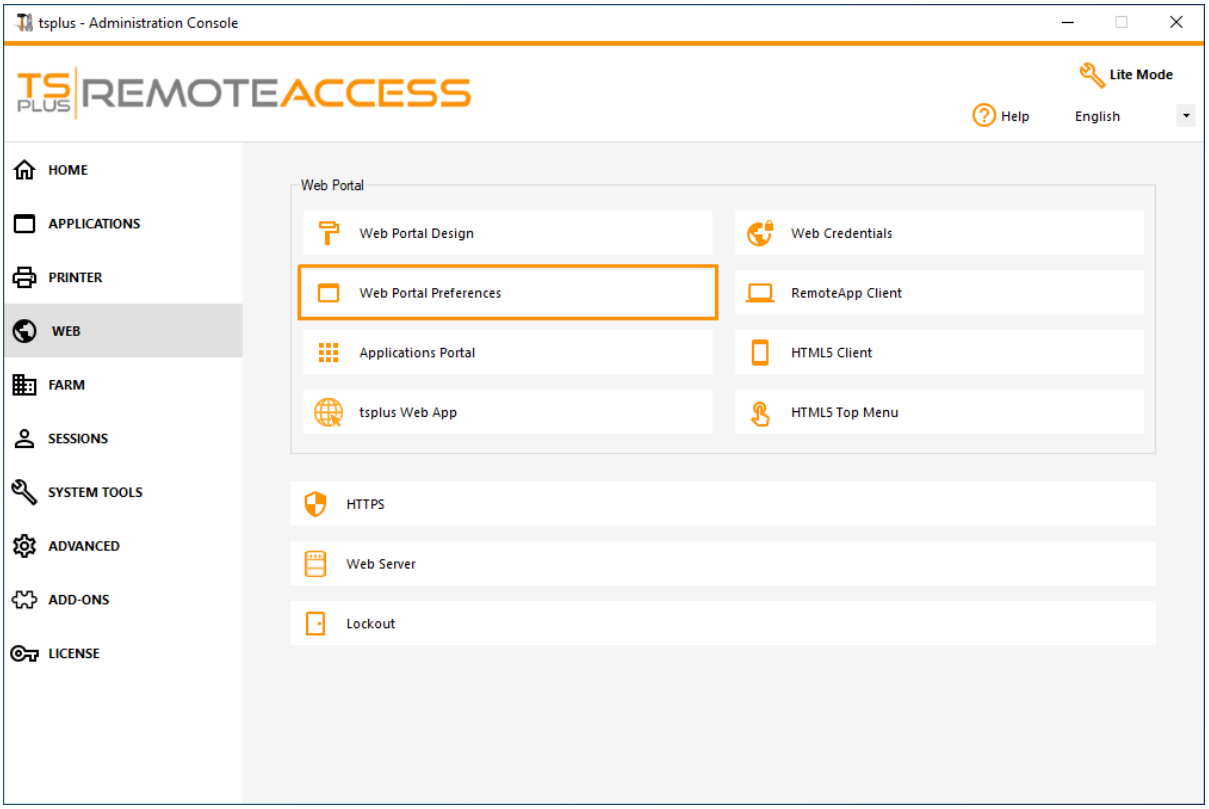

Local Group Policy Editor
File Action View Help
Remote Desktop Services
RD Licensing
Remote Desktop Connection Client
Remote Desktop Session Host
Connections
Device and Resource Redirection
Licensing
Printer Redirection
Profiles
RD Connection Broker
Remote Session Environment
Security
Session Time Limits
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)

Manually enable/disable the Gateway Server

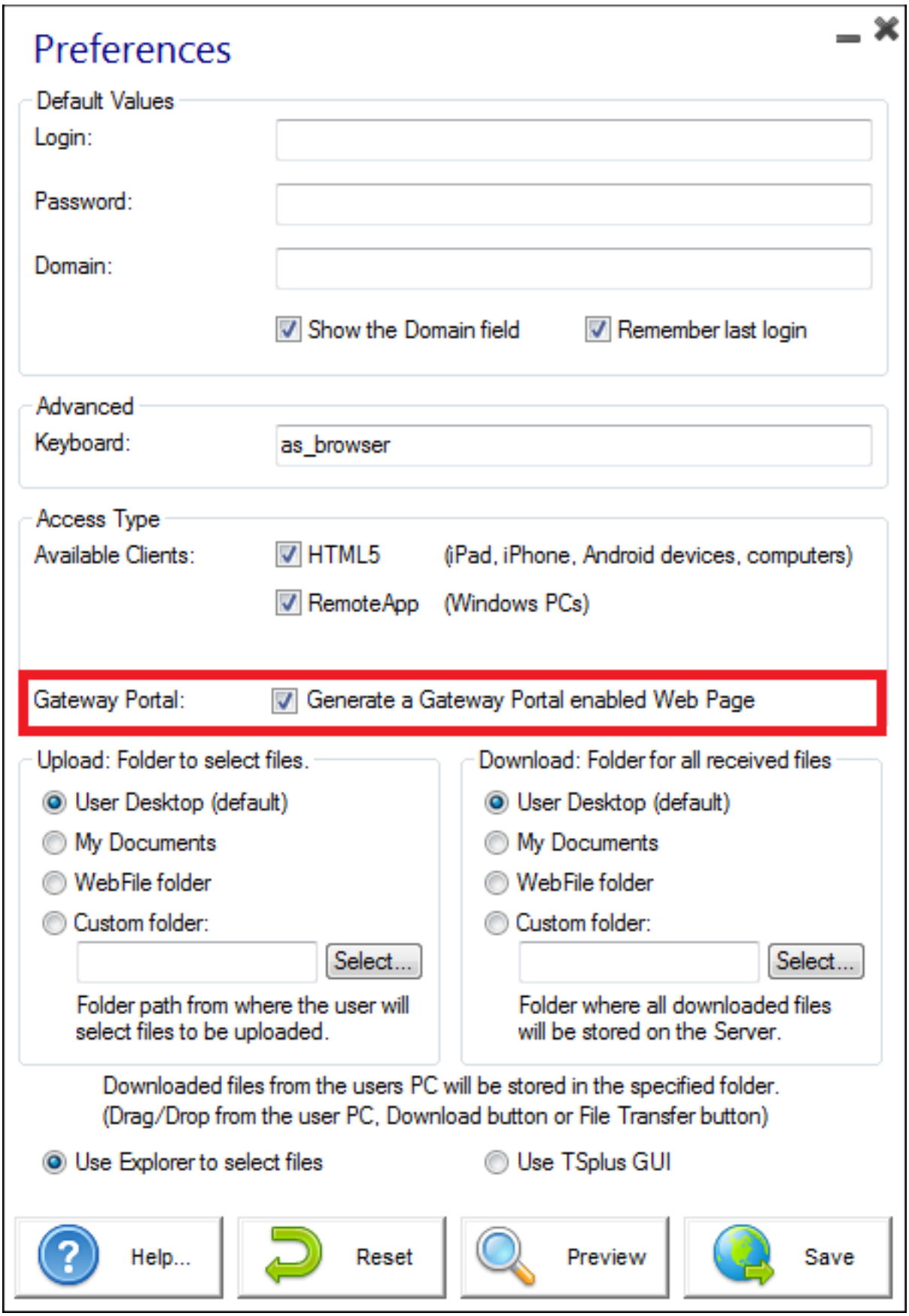
Overview

Based on your farm configuration, the Farm Controller will automatically change its own Web Portal settings to become a Gateway Server, allowing users connecting from the TSplus Web Portal of the Farm Controller, not to connect directly to the Farm Controller itself, but to one of the application server of the Farm.

However, if you want to manually change this behaviour, you can do so by clicking on the “WEB” tile, then on the Web Portal Preferences button.



- Check the “Generate a Gateway Portal enabled Web Page” box if you want the Gateway Portal of the Farm Controller (the current server you are configuring now) to become a Gateway Server and redirect users to application servers of the farm.
- Uncheck the “Generate a Gateway Portal enabled Web Page” box if you want the Gateway Portal of the Farm Controller to redirect to the Farm Controller itself, thus bypassing any farm configuration.



Click on “Save” to save this setting.

Hardware Identifier & Clone Server

1- Hardware Identifier Change.

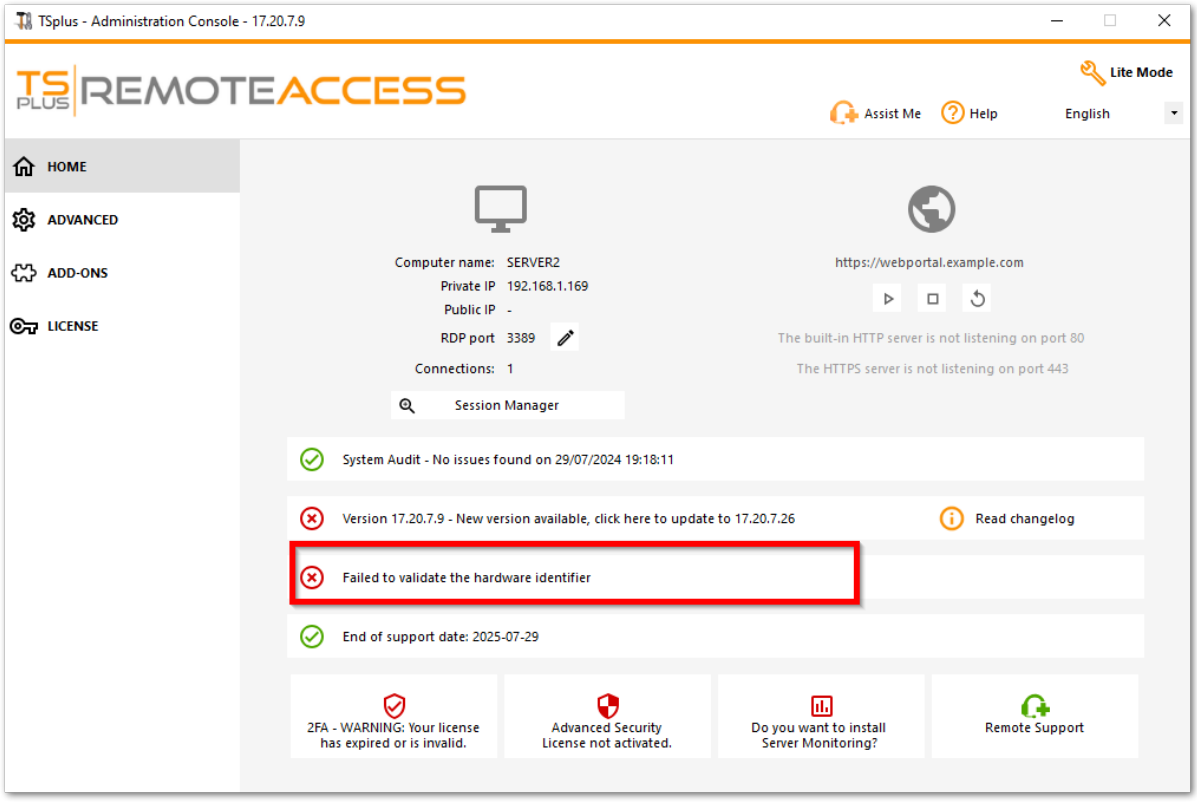
Repairing the hardware identifier following cloning or an update.

Warning : Failed to validate hardware Identifier

After migrating a physical server to a virtual machine or a Kernel Microsoft update, the license status changes to Failed to validate hardware Identifier on new hardware.

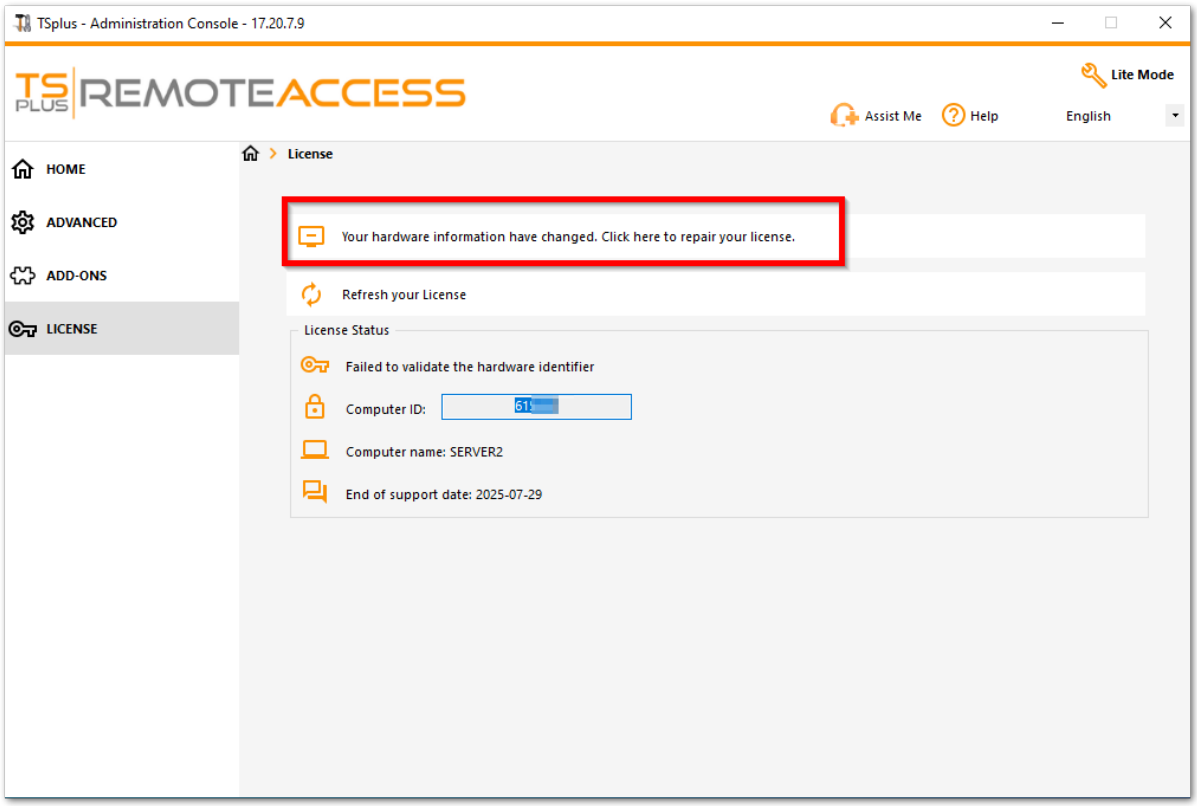
This message appears because TSplus has detected a license conflict copied from one server to another with the same Computer ID and the same name.
We already recommend renaming your new server (Example: SERVER1 > SERVER2)

- Restart your server



Click on the window to arrive on the license page.

Then click on the tab “Your hardware information has changed. Click here to repair your license.



A “license rehost” popup will open to allow you to restore your license.

Case 1: You don’t have support !
Rehosting will therefore not be possible, you will have to subscribe to a support subscription on the original server and start the migration action again.
In case of problems, Contact Support and indicate your computer ID and activation key.

Case 2: You have already rehosted for 6 months !
The Message: You have already rehosted this computer in the last 6 months. Please contact Support should you require any help rehosting your license.

The rehost will therefore not be possible, Contact Support and indicate your Computer ID and Activation Key.

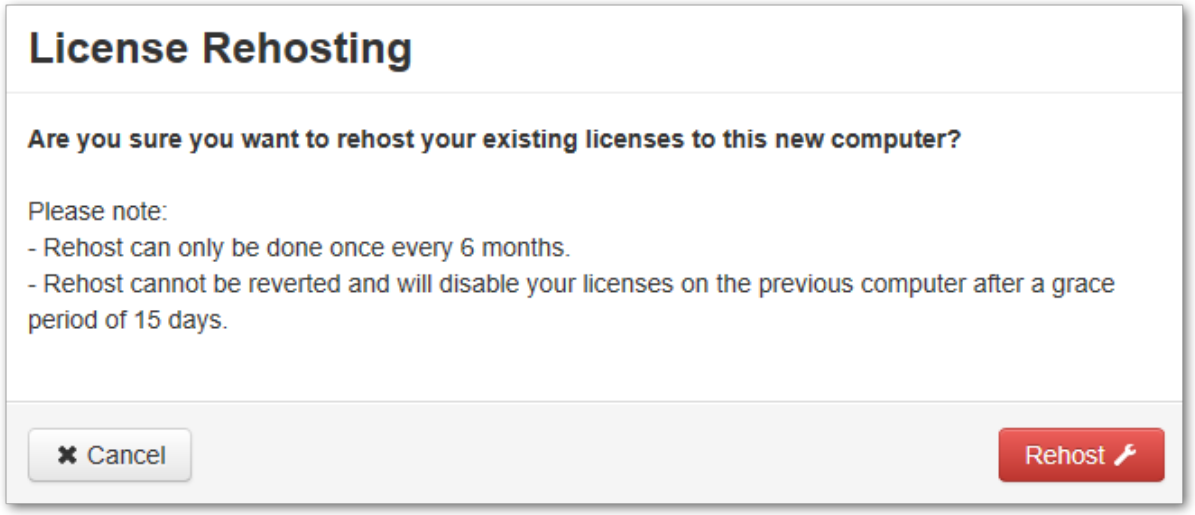
Case 3: You have support !
The following message appears: Are you sure you want to rehost your existing licenses on this new computer?

Please note:

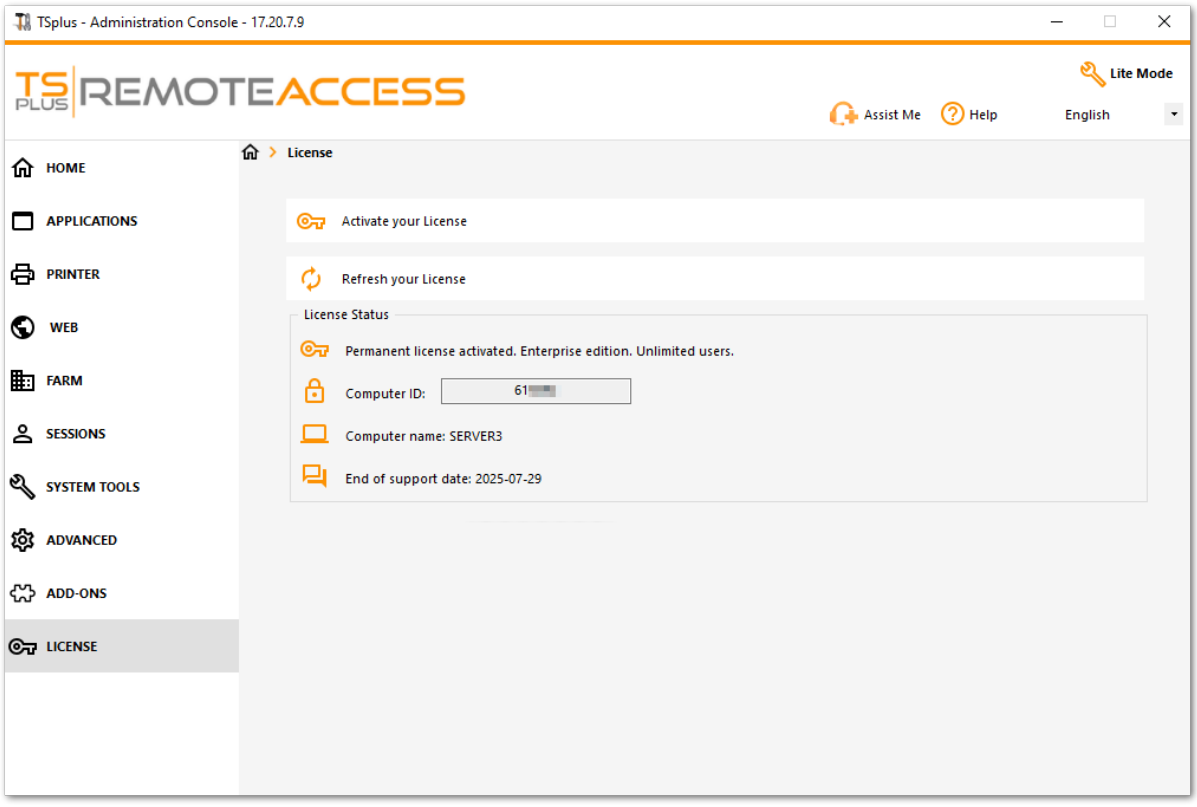
- Rehosting can only be done once every 6 months.
- Rehosting cannot be canceled and will deactivate your licenses on the previous computer

after a 15-day grace period.

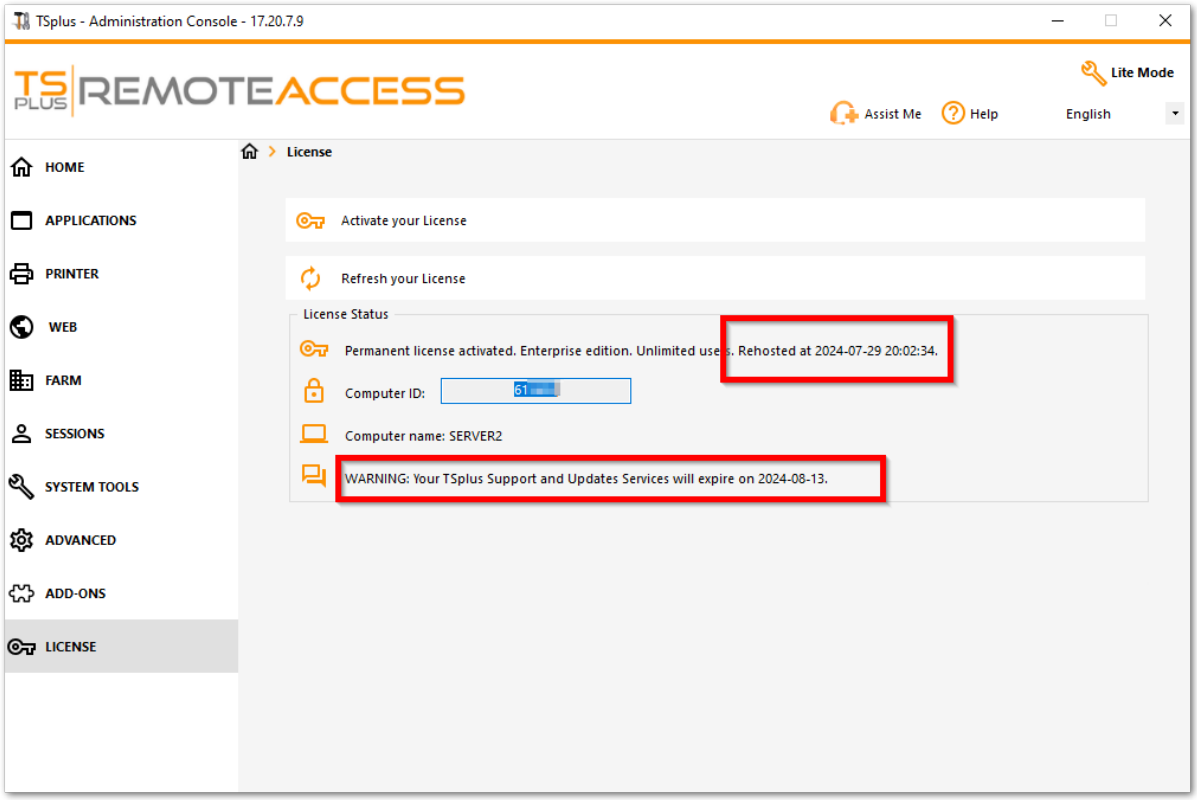
Click the **“REHOST”** button



Your license is rehosted !



Note: A message will appear on the old server with the rehost date as well as the end date of the period of use of the old server (15 days).



Update failure:
Run the Update Release and check if this has resolved your issue after restarting your server.

- Download the Update Release

2- Clone a server while keeping the existing server and activating a new license.

Requirements

When working with cloned virtual machines, it is important to modify the computer name and disk volume ID to ensure a unique TSplus Remote Access installation and avoid licensing issues.

Computer name considerations

The computer name is stored in the Windows registry inside the image itself. If modified before applying the image, it will be overwritten by Sysprep when Windows boots. However, you can predefine a name in an Unattended.xml Answer file. See Microsoft Documentation for more details.

To set the computer name, add the following section inside 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>
```

Volume ID considerations

The volume ID is associated with the disk partition, not the OS image. It can be changed before applying the image, and it will persist. Use volumeid.exe from Sysinternals, available at Microsoft Sysinternals, before Windows boots.

Deployment steps

When deploying a new virtual machine from a sysprepped image, Windows will enter the Out-Of-Box Experience (OOBE) on first boot, prompting for configuration settings.

Recommended steps for deployment:

1. **Boot to WinPE** – Prepare the system without booting into Windows.
2. **Set the Volume ID** – Change it before applying the image so it persists.
3. **Deploy the sysprepped image** – Use DISM to apply the image to C:.
4. **Set the computer name offline** – Edit the registry inside the mounted image.
5. **Copy an Unattended.xml file** – Automate OOBE configuration. This file can be dynamically modified before deployment using a script.
6. **Create a first-boot script** – Ensure final configurations with only one reboot.
7. **Reboot into Windows** – Windows finalizes itself using the specified configurations.
8. **Reset Remote Access licensing** – Run the following command:

Terminal window

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

This resets licensing and applies a new license.

Deployment script

Please find below the related WinPE deployment script.

Terminal window

```
    <# 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
```

Licensing activation

After deployment, activating a license will generate a new Computer ID for the virtual machine. This Computer ID is created by the licensing portal when a machine requests a trial or license activation. For cloned virtual machines, license activation is mandatory. Use either an activation key or a volume license key. **Offline setups are not permitted** due to security concerns. For detailed activation steps, refer to TSplus Commands List.

Conclusion

This guide outlines key considerations for deploying cloned virtual machines with TSplus Remote Access. It provides essential steps to configure and license the system correctly and must be adapted to your needs and requirements.

How To: Bind Web Server to Several Network Cards

Overview

Some use case might require that Terminal Service Plus web server listens on more than one network card, for instance if the server belongs to several different networks.

This feature answers this specific need.

Binding Web Server to Several Network Cards

To bind Terminal Service Plus web server to several network cards, you need to:

- Create the file “settings.bin” in the folder “C:\Program Files (x86)\TSplus\Clients\webserver”
- Add the following line with all the local IP addresses for all the network cards you want to bind to, for instance:

  bind_nic=“127.0.0.3”,“127.0.0.4”
- Restart webserver (AdminTool > Web > Restart Web Servers) to apply changes

Terminal Service Plus web server will now listen to all queries from all the binded network cards (in our example case the binding would be done to 127.0.0.3, 127.0.0.4 and 127.0.0.1 automatically).

How To: Add a Custom HTTP Header

Prerequisites

This feature is very technical and this documentation is only for technical experts.

You should be familiar with HTTP protocol as well as HTTP Headers.

Overview

Some use case might require that Terminal Service Plus web server returns one or more custom HTTP Headers in addition to the standard ones.

This feature answers this specific need.

Setting up a custom HTTP Header

To add your own custom HTTP Header, you need to:

- Create the file “headers.bin” in the folder “C:\Program Files (x86)\TSplus\Clients\webserver”
- Add the custom headers separated by new line, for instance case: header1=X-Frame-Options
- Restart webserver (AdminTool > Web > Restart Web Servers) to apply changes

Terminal Service Plus server will now respond to all queries with this custom HTTP Header in addition to the standard ones.

HTML Pages and Customization

You can edit the provided HTML pages with Notepad or Notepad++ to customize it user interface.

index.html page

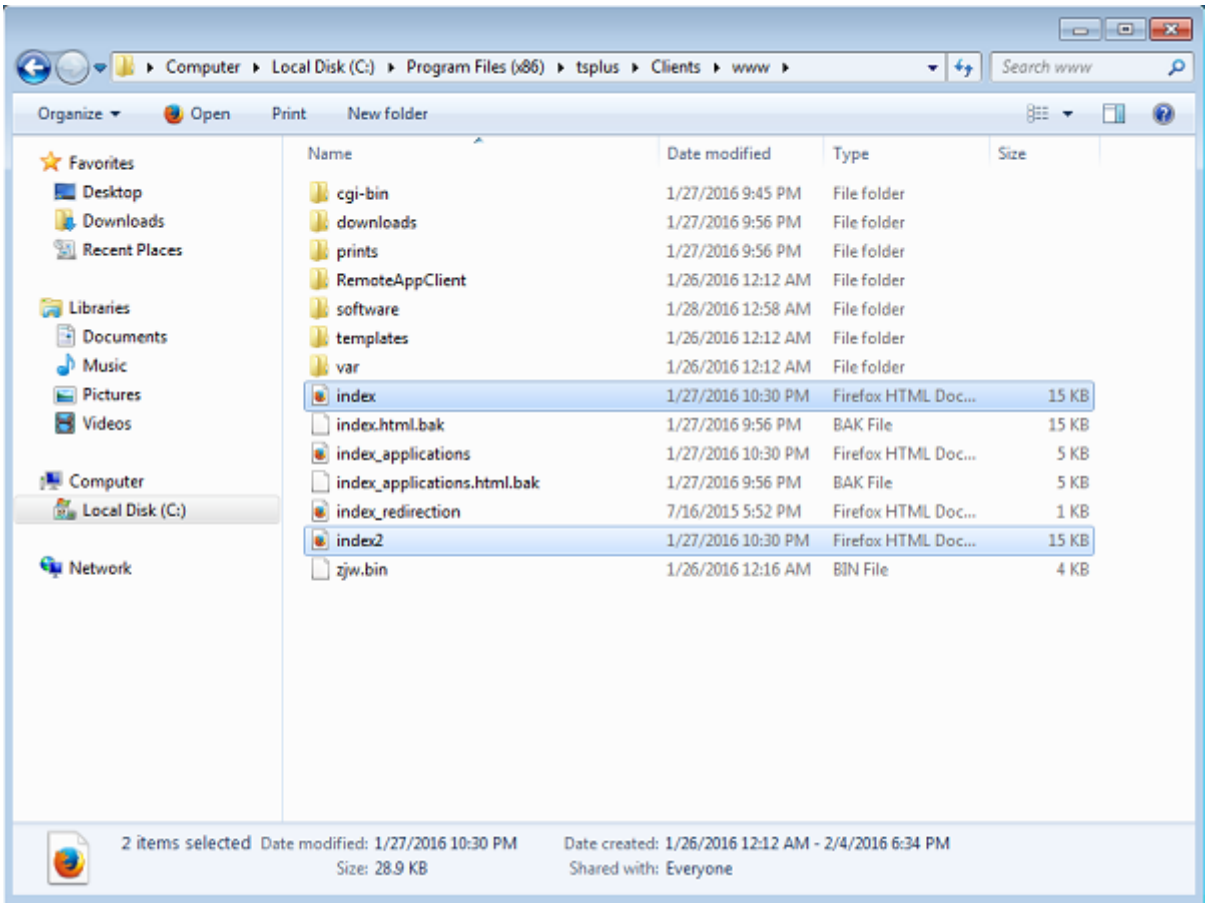
The index.html is located in Web Server root folder path.

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

Index.html page is the default web page. It's like a front-end Portal page with links to the connection pages which are located in \www\ folder.

This web page can be copied and renamed to allow multiple configuration and / or logon information.

For example let's copy and rename index.html into index2.html, this page will be available using this url http://localhost/index2.html



Beware that if you change the “index.html” file name to “index2.html” and that you are using the Web Applications Portal, then you must change the following variable on this file: “page_configuration[“applications_portal”] = “index_applications.html” to “index2_applications.html” then rename the “index_applications.html” file into “index_2applications.html”.

The default index.html includes all possible options:

- RemoteApp access to applications, connection outside the Web Browser
- Connection using HTML5 from any device
- Local printing preferences

You will be able to change header and footer in the Web portal design feature on the web portal preferences tile of the Web tab.

By editing the index.html web page, you will have access to various settings.

// ---------- Access Configuration ----------

var user = ""; // Login to use when connecting to the remote server (leave "" to use the login typed in this page)

var pass = ""; // Password to use when connecting to the remote server (leave "" to use the password typed in this page)

var domain = ""; // Domain to use when connecting to the remote server (leave "" to use the domain typed in this page)

var server = “127.0.0.1”; // Server to connect to (leave "" to use localhost and/or the server chosen in this page)

var port = ""; // Port to connect to (leave "" to use localhost and/or the port of the server chosen in this page)

var lang = “as_browser”; // Language to use

var serverhtml5 = “127.0.0.1”; // Server to connect to, when using HTML5 client

var porthtml5 = “3389”; // Port to connect to, when using HTML5 client

var cmdline = ""; // Optional text that will be put in the server’s clipboard once connected

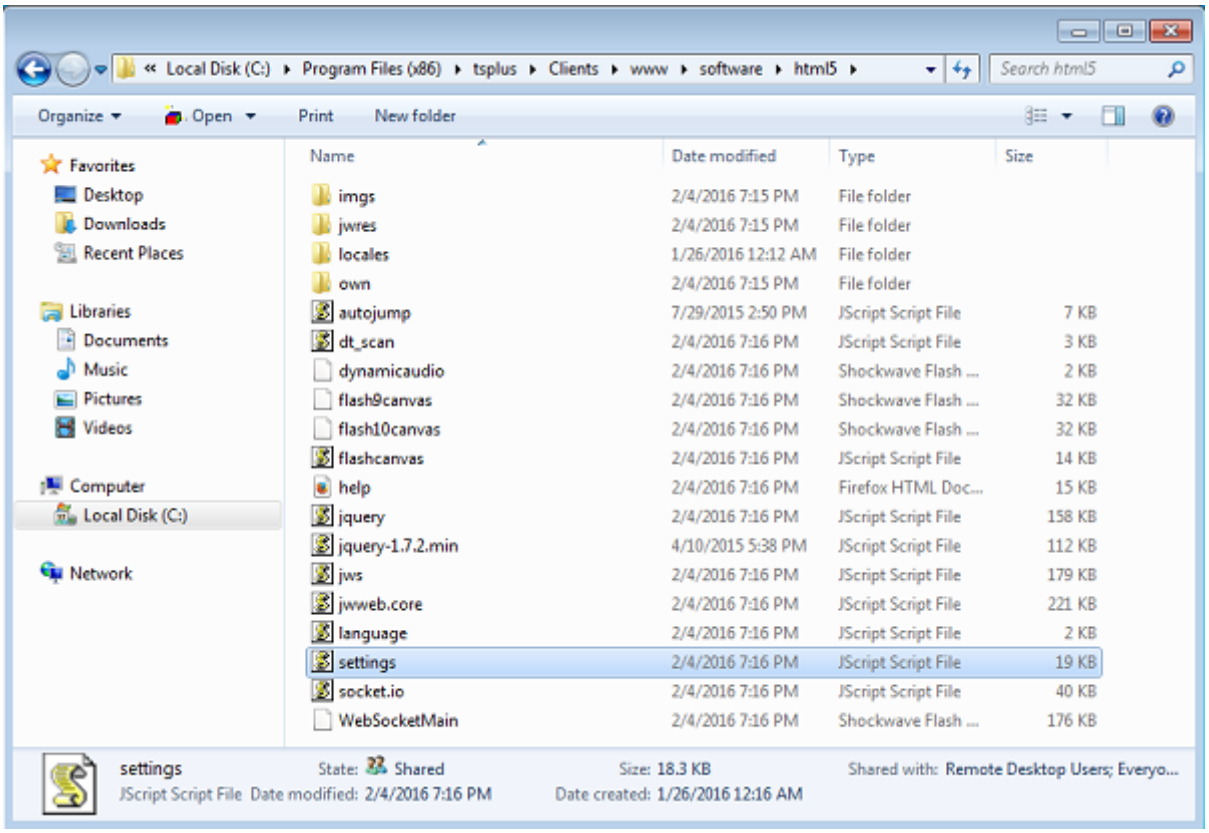
// ---------- End of Access Configuration ----------

For example I will preset demo/Psw as login/password by editing:

var user = “Demo”; var pass = “Psw”;

Doing so, pre-filled credentials are made visible at each visit of the portal.

Another very important configuration file is **settings.js**, located in C:\Program Files (x86)\TSplus\Clients\www\software\html5:



This file contains various settings for the HTML5 web client like disabling sound, clipboard or allowing session reconnection if browser tab is closed.

- Disabling clipboard:

“W.clipboard = “yes”; //or “no” ”

- Disabling sound is done with this setting:

“W.playsound = false;”

- Changing default resolution for Mobile devices:

“W.viewportwidth = “1024” ” - The height gets computed by browser.

- Forcing HTTPS for remote connection

“W.forcealways_ssl = true;”

- Allowing session reconnection when browser tab is closed:

“W.send_logoff = false;”

- Adding a warning pop up to prevent closing the browser tab:

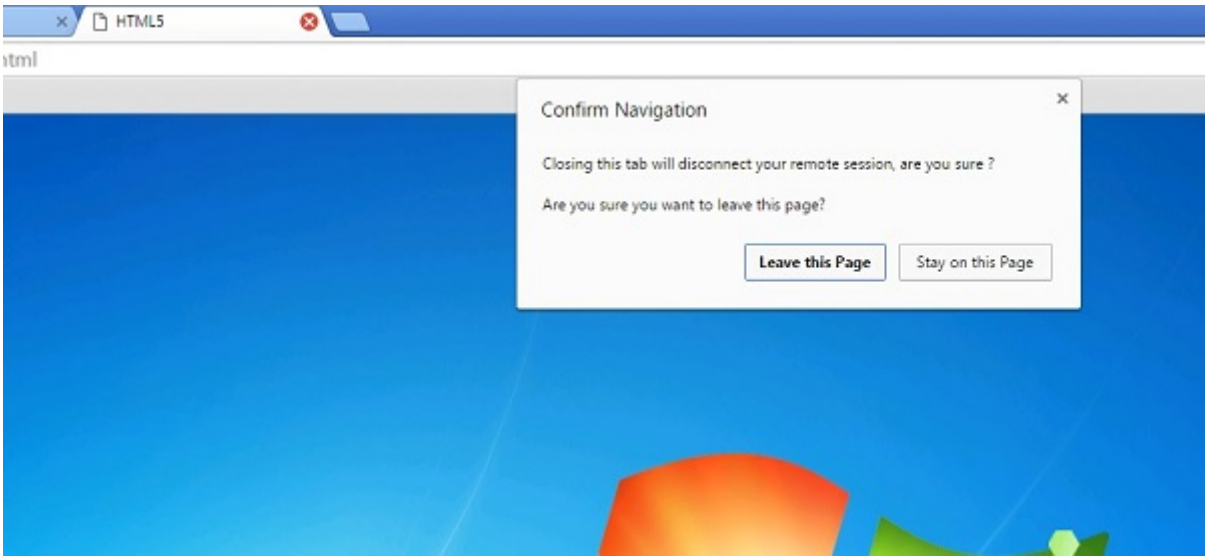
search the “W.pageUnloadMessage = "" ” parameter.

I have set an example of message to be used below :

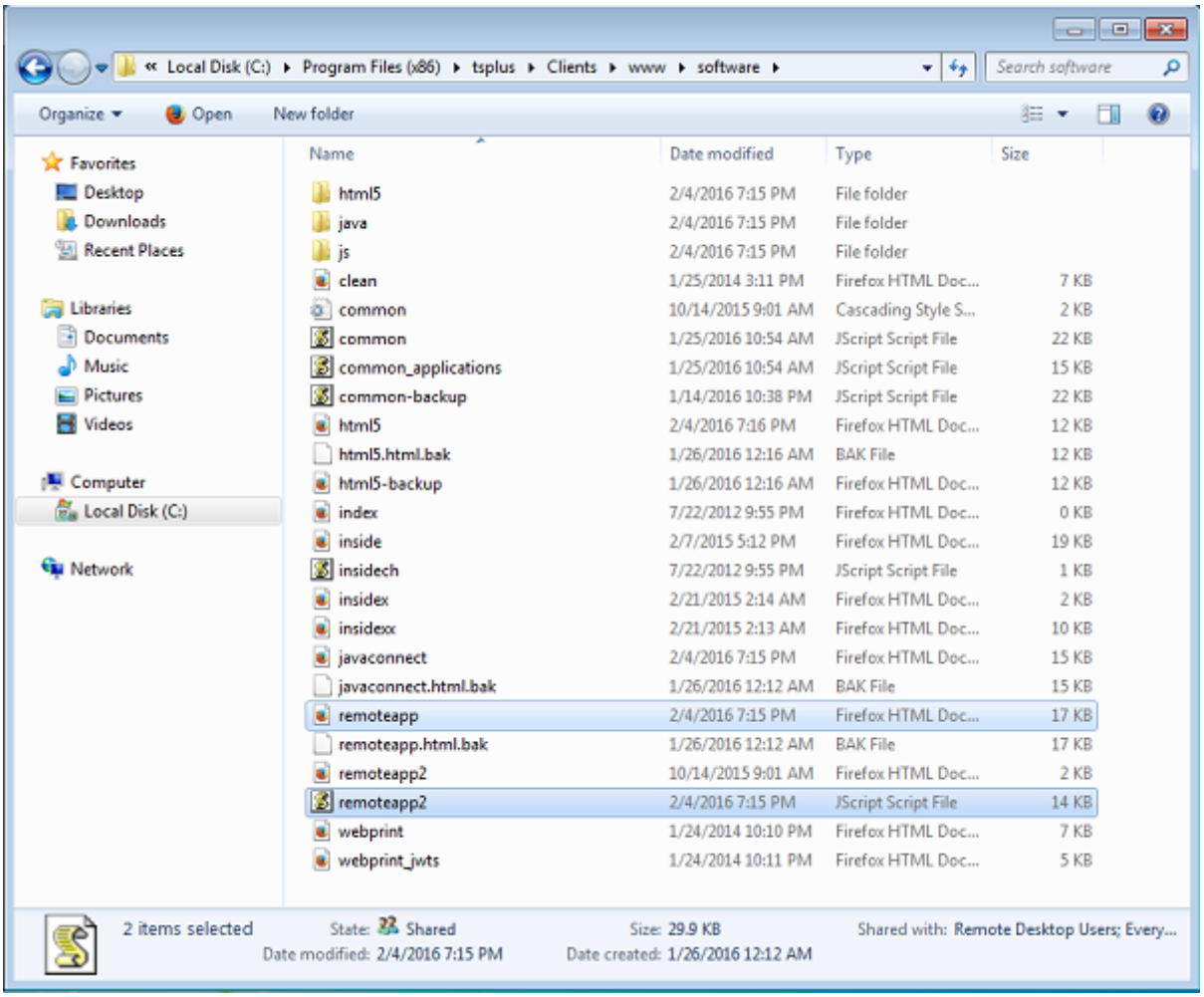
W.pageUnloadMessage = “Closing this tab will disconnect your remote session, are you sure ?”; //Dialog to return when page unloads.

//1. Important notice, own dialogs are not supported in all browsers.

//2. HTML standard does not distinguish between page refresh and page close action, the dialog will popup on page refresh too.



The general settings for the RemoteApp web page is stored on the software folder, in two different files: **remoteapp.html** and **remoteapp2.js**.



Example of available settings present in **remoteapp2.js** :

// Remote Desktop Server

var remoteapp2_server = ''; var remoteapp2_port = '443';

// Windows Authentication

var remoteapp2_user = ''; var remoteapp2_psw = ''; var remoteapp2_domain = '';

// Optional Command Line Parameters

var remoteapp2_apppath = '';

// RemoteApp mode

var remoteapp2_wallp = 'green'; var remoteapp2_remoteapp = 'on';

// Screen

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 = ‘off’;

var remoteapp2_span = ‘off’;

// Disks mapping (required for printing)

var remoteapp2_disk = ‘1’;

// Printing

var remoteapp2_printer = ‘off’;

var remoteapp2_preview = ‘off’;

var remoteapp2_default = ‘on’;

var remoteapp2_select = ‘off’;

// Hardware

var remoteapp2_com = ‘0’;

var remoteapp2_smartcard = ‘0’;

var remoteapp2_serial = ‘off’;

var remoteapp2_usb = ‘off’;

var remoteapp2_sound = ‘on’;

var remoteapp2_directx = ‘off’;

// Miscellaneous

var remoteapp2_alttab = ‘0’;

var remoteapp2_firewall = ‘1’;
```

```
var remoteapp2_localtb = ‘32’;

var remoteapp2_lock = ‘off’;

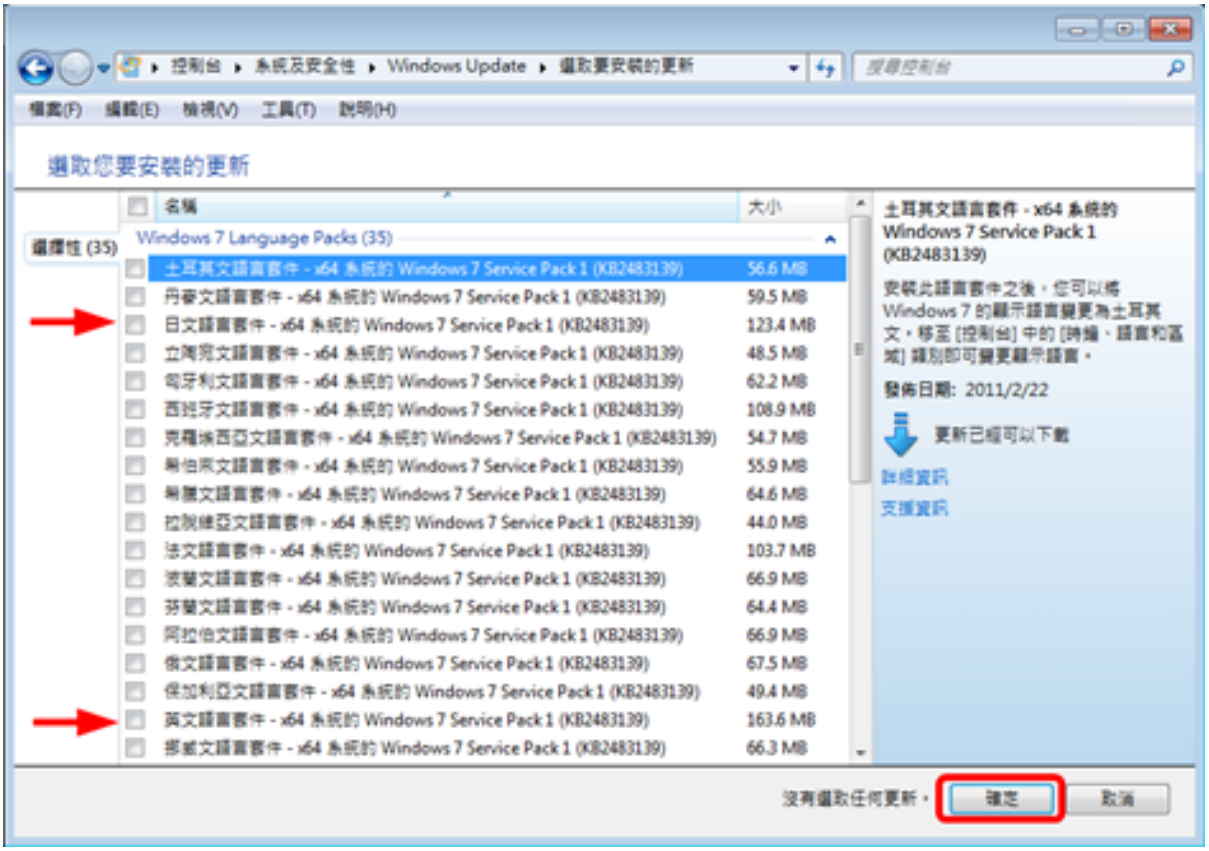
var remoteapp2_rdp5 = ‘off’;

var remoteapp2_reset = ‘off’;
```

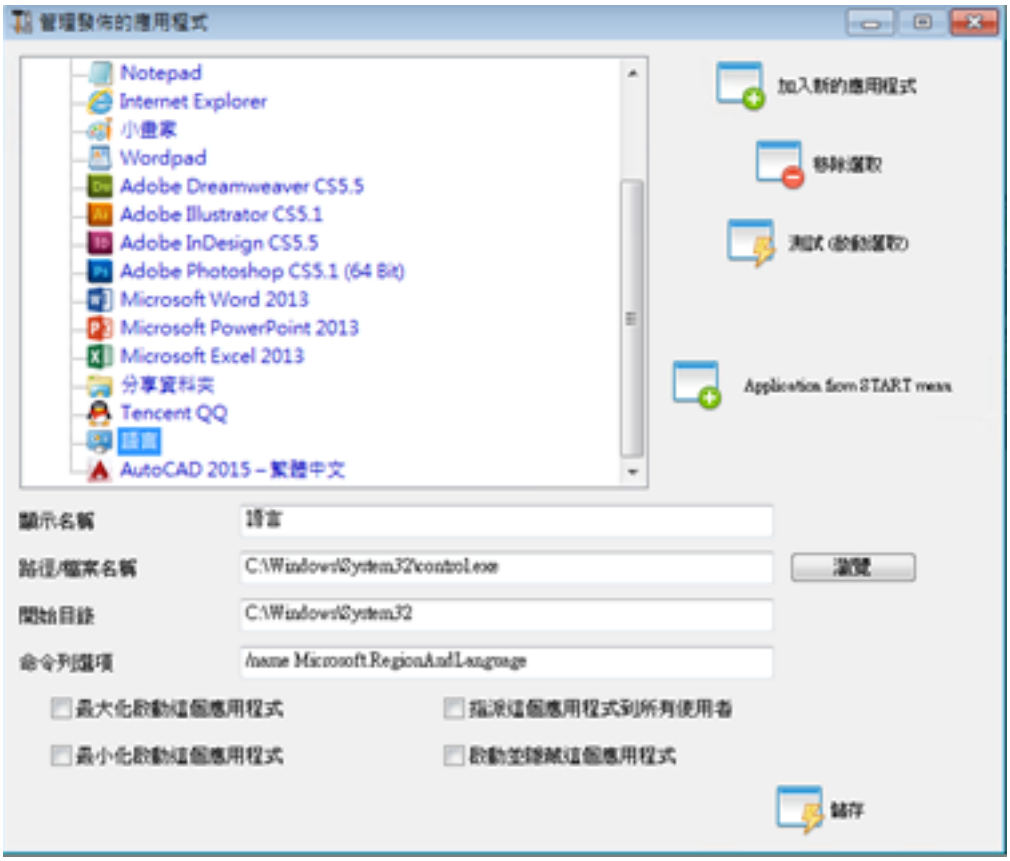
HTML5 : Changing language to Chinese

You need Windows 7 Enterprise or Ultimate / Windows 8 Enterprise or Professional to use multi-language on one system.

You can install every language on the system if you need.



You could publish a language applet for users to change their own O/S language of UI and add IME (Input Method Editor).

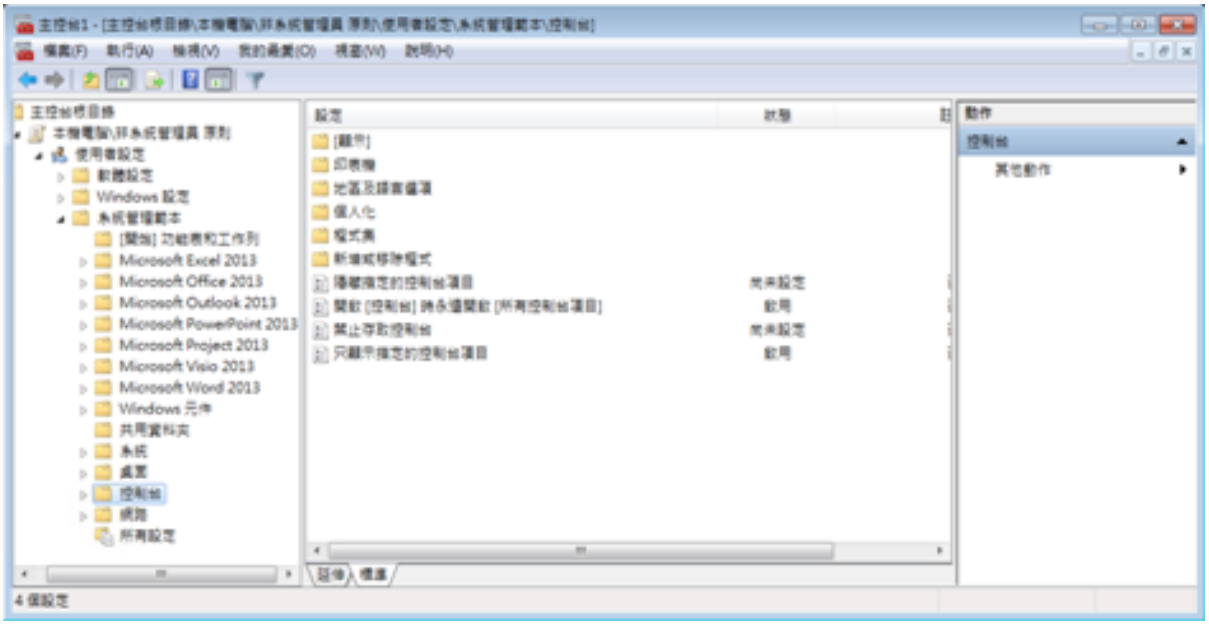


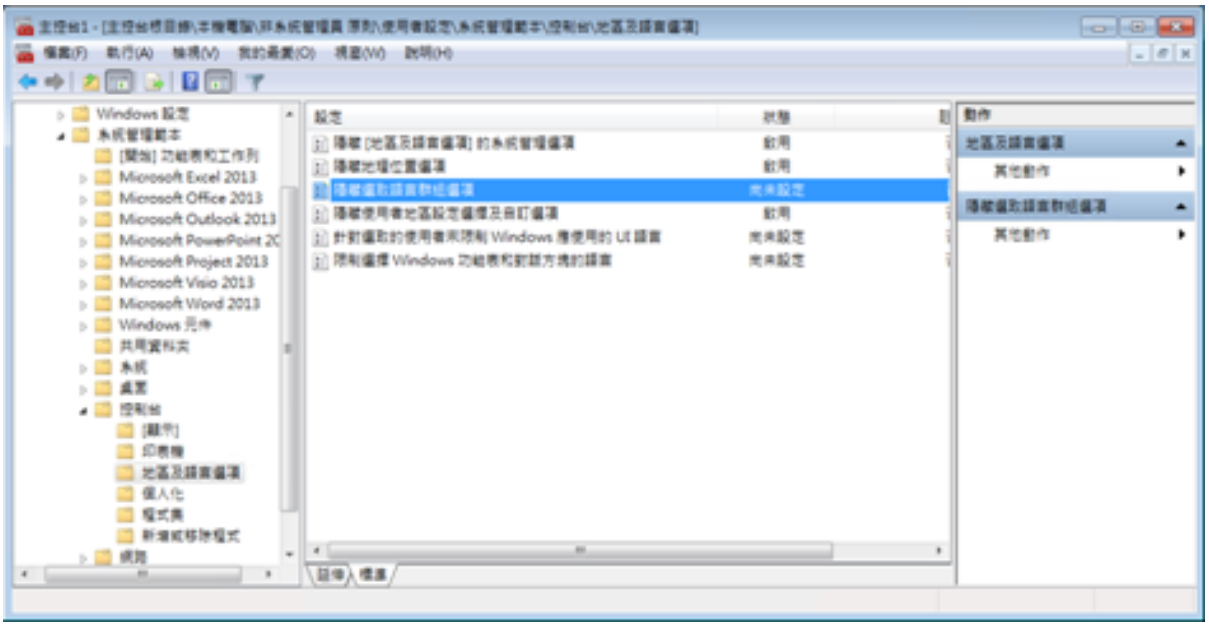
For Windows 7: control /name Microsoft.RegionAndLanguage

For Windows 8: control /name Microsoft.Language

Complete List: http://pcsupport.about.com/od/tipstricks/tp/control-panel-applets-list.htm

Optional : this is how to restrict the Control Panel behavior for users by GPO :

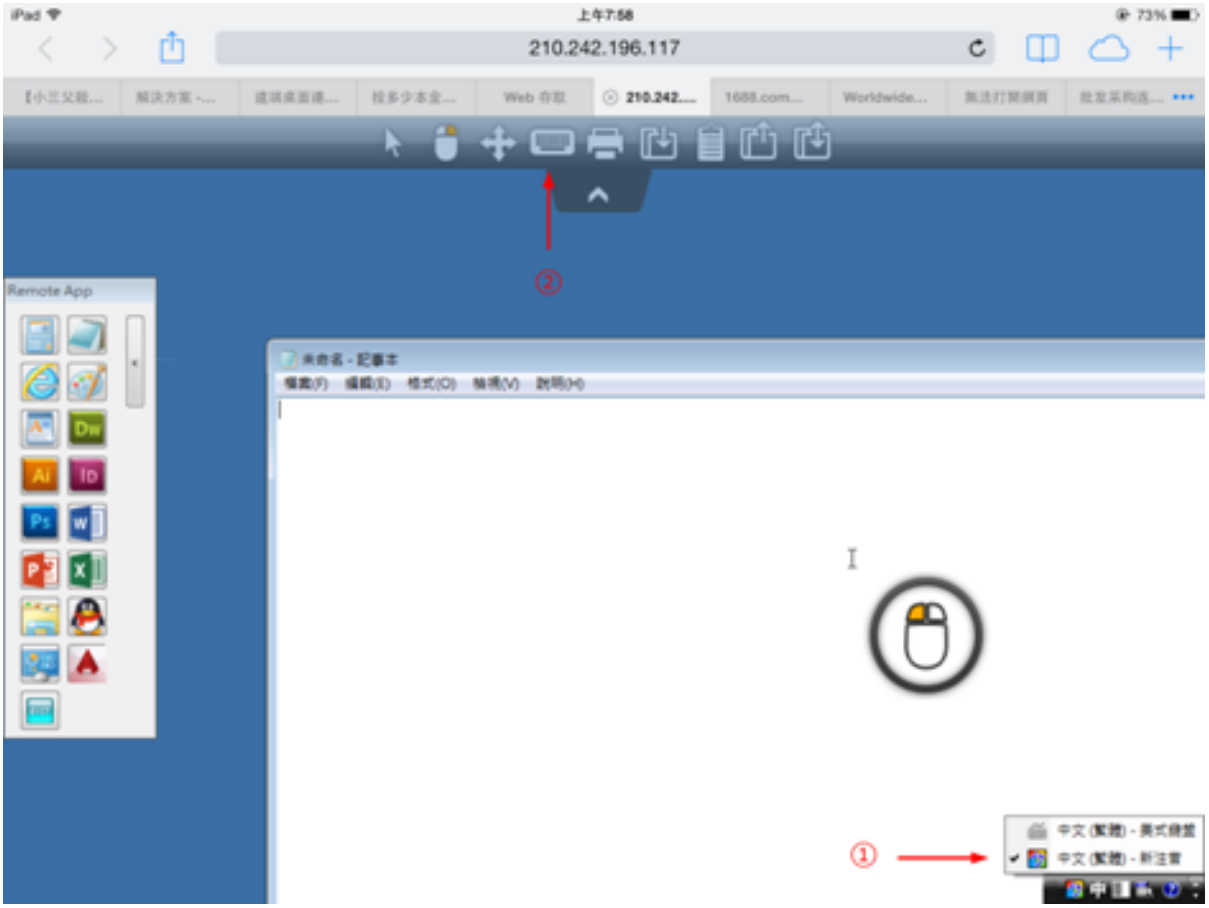




Users can change O/S language of UI after logon system. (Users have to logout and logon again to take effect after changing this setting)



The user has to select Chinese IME first to input Chinese chars.


210.242.196.117
Remote App
②
①


210.242.196.117
中文虫
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
中 種 重 鐘 終 腫 仲 蟲 冢 忠 眾 踵 鍾 衷 塚 忪 众 潼 僮 狆
確認
.?123
一聲
.?123

HTML5 Client: What is the difference between Websockets and XHR?

Websockets is the persistent connection that can be used to receive/send data without sequential order and without http header.

Xhr-polling creates new request with http header and waits for answer with http header, also sequential order.

Doing so, XHR data flow always looks like this:

HTTP_HEADER_REQUEST -> HTTP_HEADER_ANSWER HTTP_HEADER_REQUEST -> HTTP_HEADER_ANSWER and so on

also before the data can be downloaded, it must be requested with HTTP_HEADER, therefore its name: xhr-polling.

Websockets data flow may look like this:

FRAME_DATA_SEND FRAME_DATA_SEND FRAME_DATA_RECEIVE FRAME_DATA_SEND FRAME_DATA_RECEIVE FRAME_DATA_RECEIVE

Also it is random data sending/receiving without special sequential order and without any http header data.

That makes the usage with reverse proxies impossible due to the lack of Websockets support by most known reverse proxies; but half of the xhr transport may work with Apache reverse proxy.

Also see: HTML5 Client: Supported Browsers

HTML5 Client: RDP session resolution on mobile devices

The common screen resolution by most devices, especially mobile phones is 320x480, but that is obviously not sufficient to create the RDP session.

Therefore the resolution was preset to 800 in width. The height of resolution gets recomputed by hidden browsers native logic. The higher the width the bigger the height.

- As an example, standard resolution is 320x480, now when you set the viewport to 800, the browser recomputes the value for height for example to 800x904, when you set the width to 1280, then it’s 1280x1160 etc.

The height and width depend on landscape/portrait view of your device, like 800x904 or 904x800 etc. Each browser can recompute it on its own logic to fit the rdp screen into the viewport of your device and may differ depending on the browser even when used on same device.

If you set the height manually, then you will break the viewport ratio of your device and the final RDP session will be out of your port view, and to reach these areas you will have to scroll to wished positions.

- Therefore it is recommended not to set height manually, but let the device choose automatically the height.

If you need more height, increase the width!

By testing on mobile phone devices, the good value for width was 800. Though you must pay attention : the CPU’s on most mobile phones are usually slow, therefore when you increase the height, it will increase the CPU load. On tablet devices the CPU’s are faster, therefore it is recommended to set the width to higher value like 1280 and allow the device to recompute the value for height.

Because some browsers like FireFox mobile do not allow the setting of viewport after page loading, this value was set fixed into the Clients\www\software\html5.html file:

For example change it to:

to increase width and at same time height recomputed by browsers native internal logic.

As a second example, changing it to :

would break viewport area and RDP session would not fit the screen.

HTML5 Client: Parameters in URL address

When using Terminal Service Plus HTML5 client to connect to a remote server, you can specify several parameters in the URL address to override default parameters, such as:

- user login
- user password
- program to run
- startup directory for the program to run
- command line for the program to run

Run a Specific Application

Here is an example of a full URL address to open a remote session for user “demo” with password “demo” and by starting standard notepad upon session opening:

https://demo.tsplus.net/software/html5.html?user=demo&pwd=demo&program=c:\\windows\\system32\\notepad.exe&startupdir=c:\\windows\\system32&params=

Please note that in the URL address all slashes characters must be repeated **4 times**.

You do not have to specify all these parameters at the same time: the parameters not specified will have their default configured value.

Connect with Web Credentials

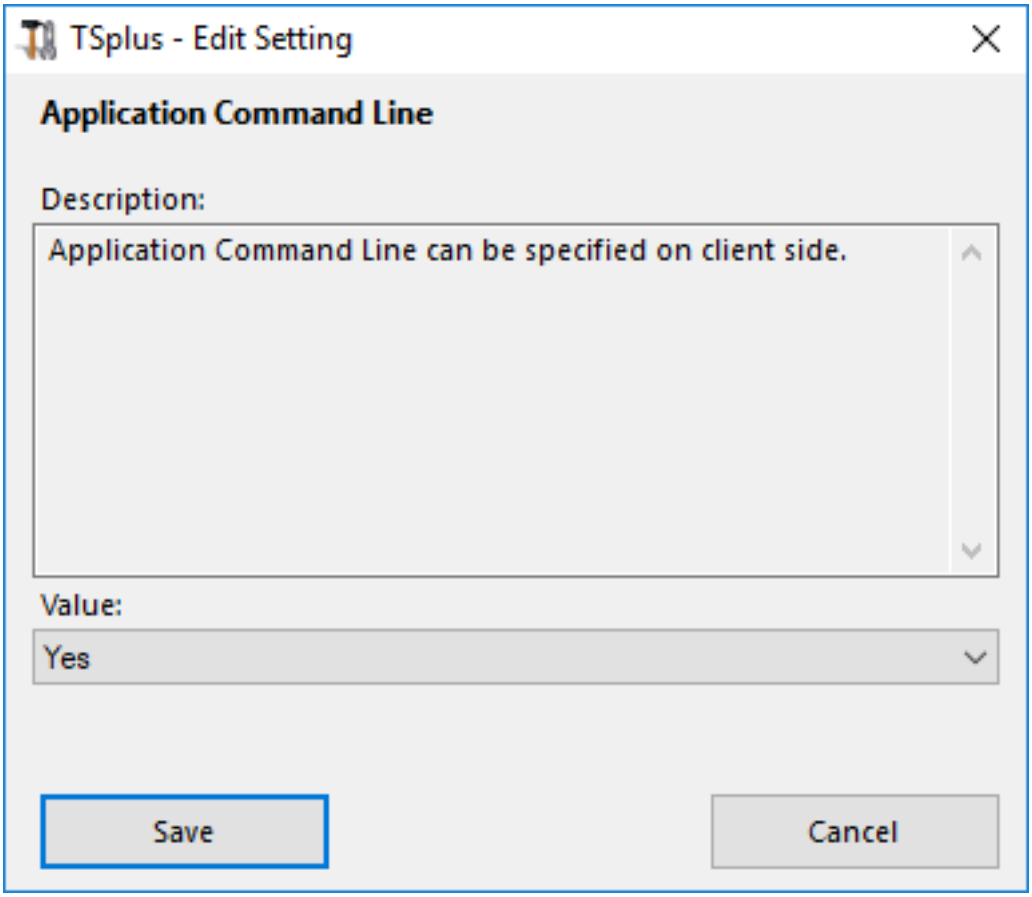
If you want to use a Web Credential to connect, you can pass it in an URL by adding an ”@” before the Web Login.

Here is an example of a URL address to open a remote session with the Applications Panel for Web Credentials “1234” with password “demo”:

https://demo.tsplus.net/software/html5.html?user=@1234&pwd=demo

Restrict this usage to Users Default Applications

You can disable the Application Command Line for users by going on the **Advanced —> Session tab** of the AdminTool, double-clicking on the “Application Command Line” setting and setting the value to “No”.



HTML5 Client: Supported Browsers

If your browser shows red warning on start by using HTML5 client

It means that your browser does not support Websockets or your browser does not support Canvas.

Such browsers that do not support these technologies are IE6, IE7, IE8, IE9 and need FLASH to emulate these features.

Browsers supporting Websocket and Canvas

Browsers	Canvas	Websocket
FireFox	Full	Full starting with version 4
Chrome	Full	Full in most known versions on PC's
Opera	Full	Full in newest versions
IE6	Flash	Flash (emulated and no proxy support)
	Flash	XHR (with proxy support)
IE7	Flash	Flash (emulated and no proxy support)
	Flash	XHR (with proxy support)
IE8	Flash	Flash (emulated and no proxy support)
	Flash	XHR (with proxy support)
IE9	Flash	Flash (emulated and no proxy support)
	Flash	XHR (with proxy support)
IE10	Full	Full
Android native	Full	XHR
Opera mobile	Full	Full in newest versions
Firefox mobile	Full	Full
Safari mobile	Full	Full in newest versions up iOS4, else emulated via XHR

Also see: What's the difference between websockets and XHR?

If your browser automatically reloads the pages to HTTPS address

It means that Websockets transport is not supported. This is the case on several Android native mobile browsers.

It is due to the fact that the browser automatically switches to XHR transport.

But because this transport layers on long distances with HTTP protocol, each request creates new connection. It is very slow and unstable to create new connections (up to 20 new connections per second), therefore to avoid this instability the program is conceived so that the page reloads automatically to HTTPS address to enforce HTTPS connection.

Physically you also get mostly persistent secured connection and much more stable on long distances. So the logic of browser reuses already established SSL connection instead of creating a new connection like by the use of HTTP protocol.

This behavior can be changed by the following option on the setting.js file located in the TSplus program folder under this path: Clients\www\software\html5\settings.js:

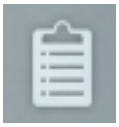
forcesslforxhr = false;

But it is absolutely not recommended to disable the use of SSL in XHR mode.

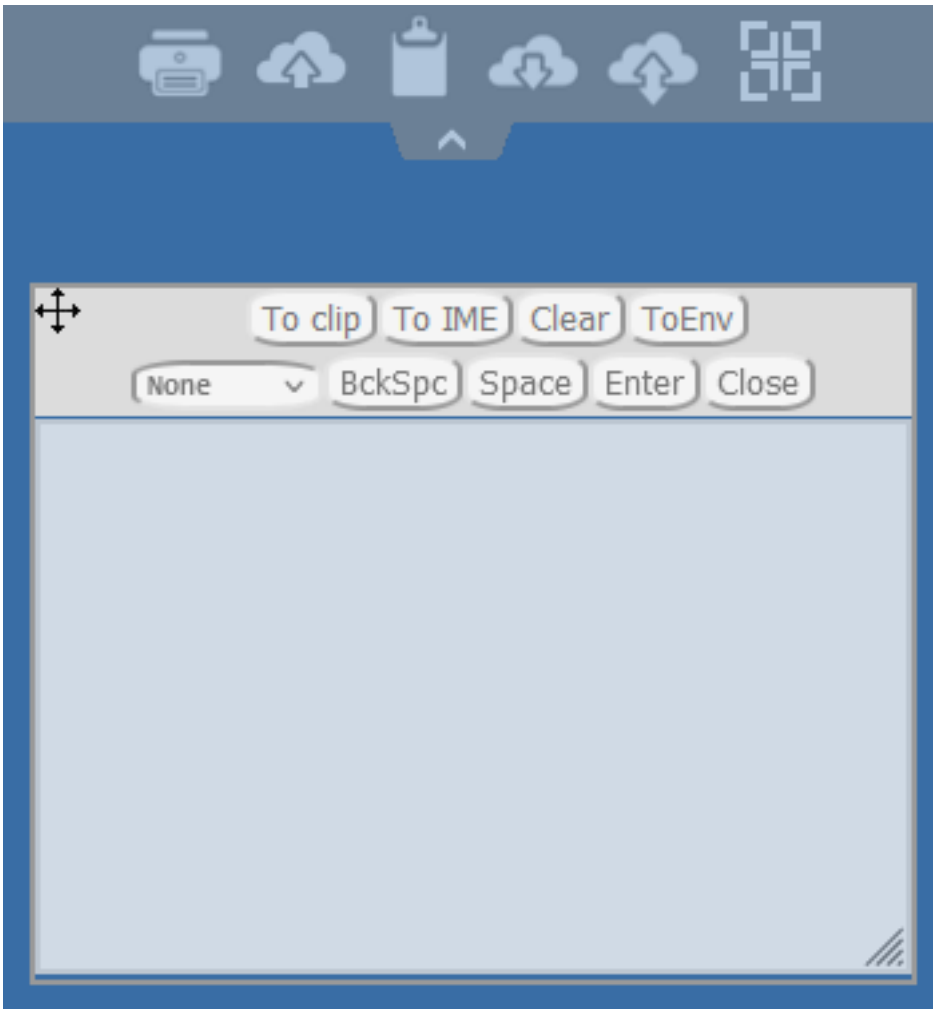
*If you do not have a file named "settings.js" in the "C:\Program Files (x86)\TSplus\Clients\www\software\html5" folder, then your TSplus version is older and this documentation does not apply. Please update your system first or contact support.

HTML5 Client: Using Clipboard

The clipboard can be found on the HTML5 Top menu, with this icon:



Most browsers except older MSIE browsers do not support the direct clipboard reading and writing due to security reasons.



Here are the different actions:

- **To Clip**: sends TO RDP SESSION the content of the TEXT AREA and produces Ctrl+V on the end to put the text INSIDE RDP SESSION (your OWN ENVIRONMENT is not touched!!!)

- **To IME**: converts chars from TEXT AREA to keystrokes and sends it so as if you have used keyboard. (this button is necessary when you want to put the text where clipboard text input is not supported inside rdp session app)

- **ToEnv**: TRIES to put text from TEXT AREA to YOUR OWN CLIPBOARD outside of your browser (not to RDP session but your own ENVIRONMENT!!!!) Because adding text to own clipboard is priviledged action it must be executed by click.

- **To Clip**: as mentioned, handles putting of text to rdp-clip+ctrl/v action without adding text outside of own browser due security since it would be pretty dumb to put text inside own clipboard when not really wished to do, so use for it “ToEnv”, this behavior will stay so and won’t be changed since requested so.

- **BckSpc**: sends to RDP session BACKSPACE button command (your app must be focused and support Backspace button action)

- **Space**: sends to RDP session Space button command (your app must be focused and support Space button action)

- **Enter**: sends to RDP session Enter button command (your app must be focused and support Enter button action)

To copy the text from session to clipboard use Ctrl+C and to insert the text from clipboard use Ctrl+V.

But pay attention when you copy the text with Ctrl+C, wait some time before releasing the pushed Ctrl+C buttons, because if the requested clipboard text arrives after you release this key combination, the text will not be added to your environment clipboard. This way uses a native browser clipboard copy support initiated by Ctrl+C.

Alternatively you can **use the clipboard menu** to copy from and to insert the text into RDP session clipboard.

There you can just insert the text into RDP session clipboard or add it to clipboard and auto-initiate Ctrl+C on RDP session side to insert text. The clipboard menu can be opened via action menu or Shift + F11.

- When you copy the clipboard with mouse inside a RDP session, the text gets sent to browser and as soon as you go out of browser focus, the clipboard menu appears automatically to inform you that there was a clipboard text and that you did not add it to your clipboard environment.

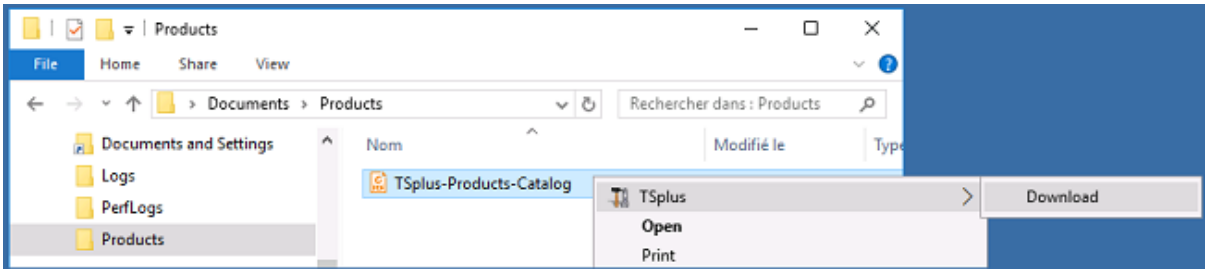
To avoid this behavior set the following line on the Clients folder, by default, the path is: C:\Program Files(x86)\tsplus\Clients\www\software\html5\settings.js :

openonclipblur = false;

*If you do not have a file named “settings.js” in the “C:\Program Files (x86)\TSplus\Clients\www\software\html5” folder, then your TSplus version is older and this documentation does not apply. Please update your system first or contact support.

HTML5 Client: Using File Transfer

File Transfer can be done in multiple ways on TSplus: since Version 12.50, **a contextual menu is available to download files from the server to the local pc**:



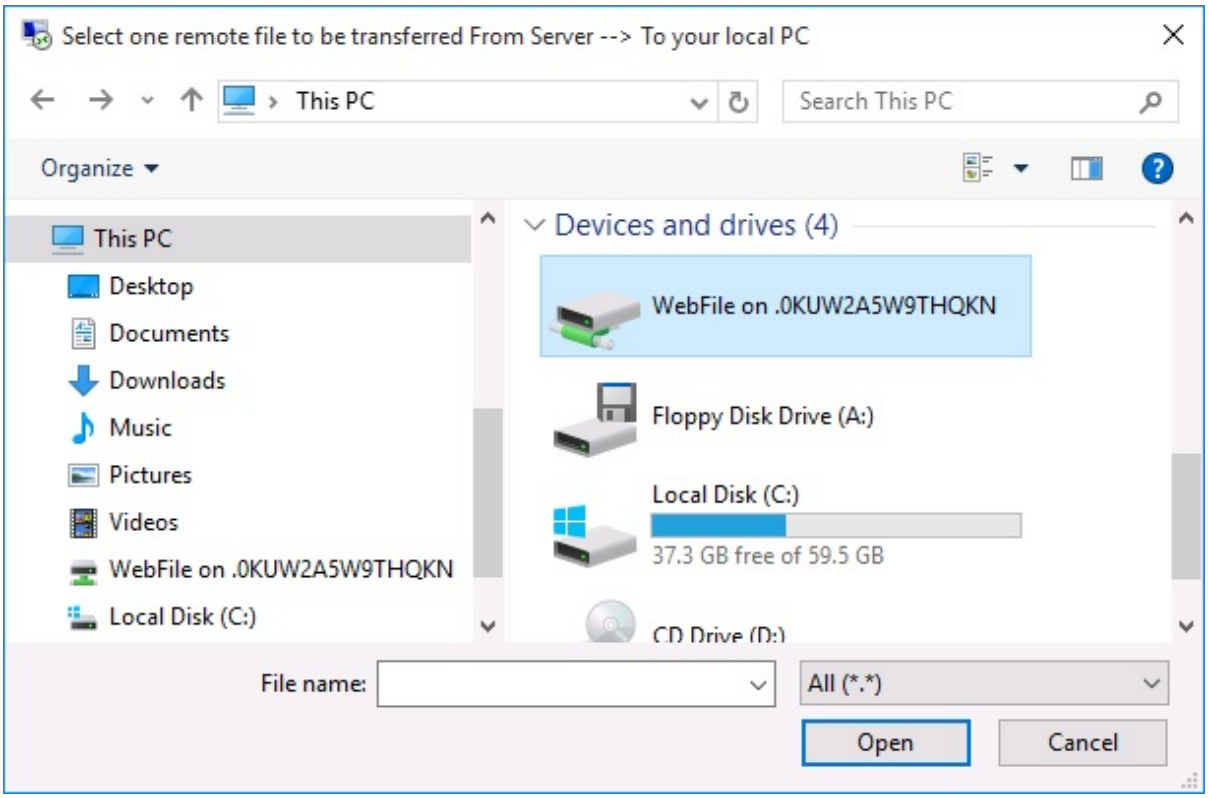
More information can be found on this documentation.

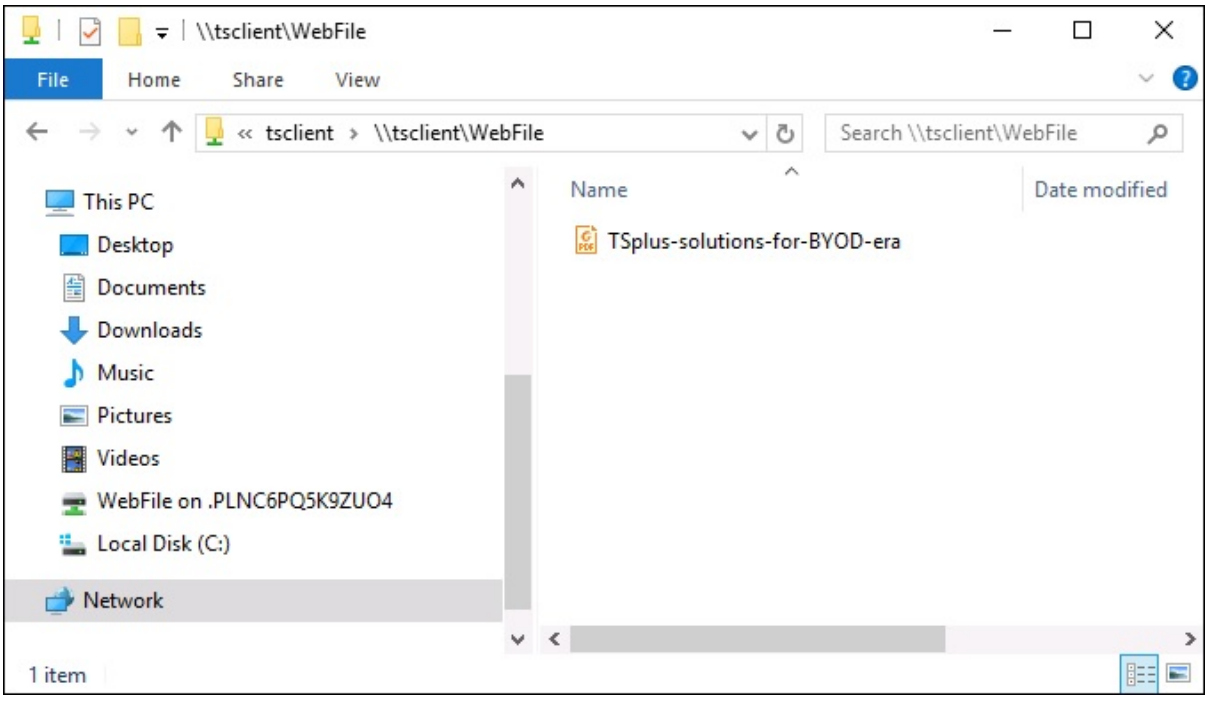
Using the top menu for file transfer:



Unlike real RDP session the browsers do not allow to access the hard drives directly, the file transfer is emulated.

The sub-folder of gateway gets mounted as a WebFile device into your RDP session. Inside the RDP session you can access it via Explorer by clicking on “WebFile” or call “\\tsclient\WebFile” directly:

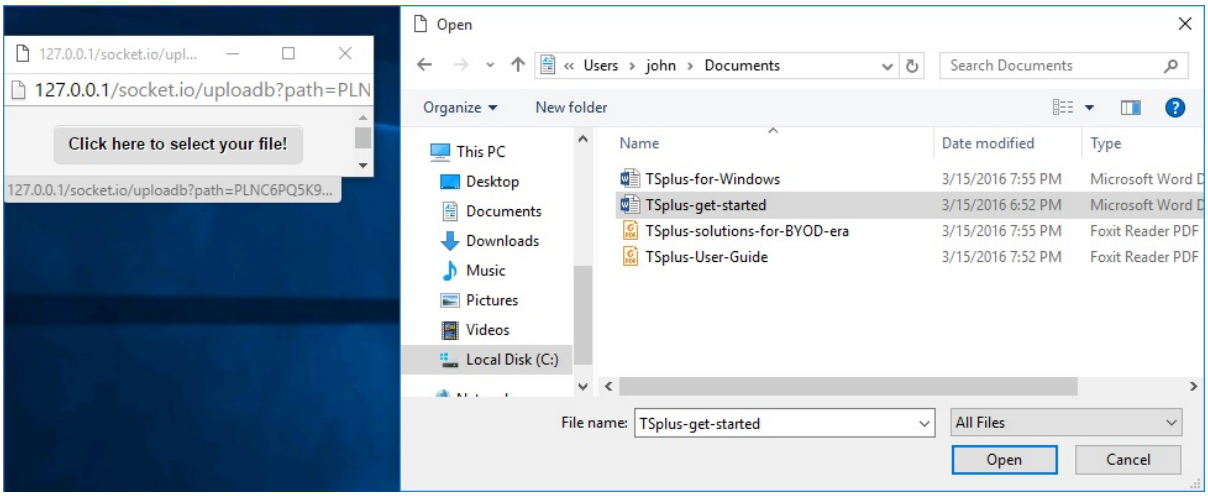




There are 3 different possibilities to transfer a file:

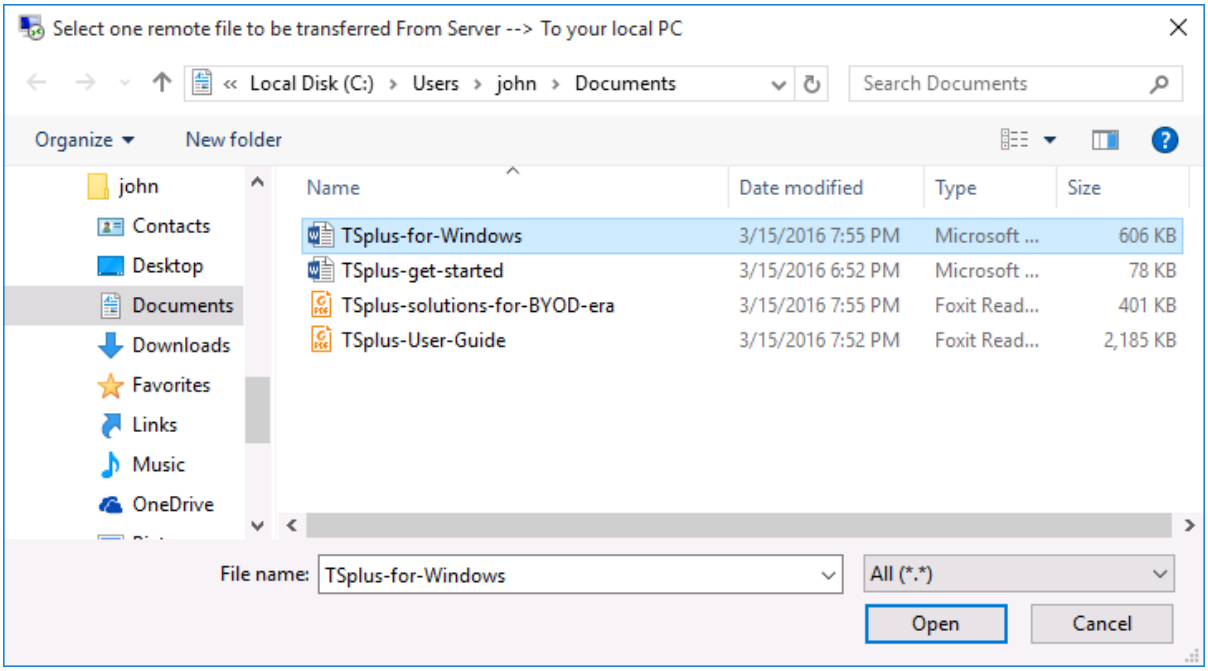
- From the local computer to the server:





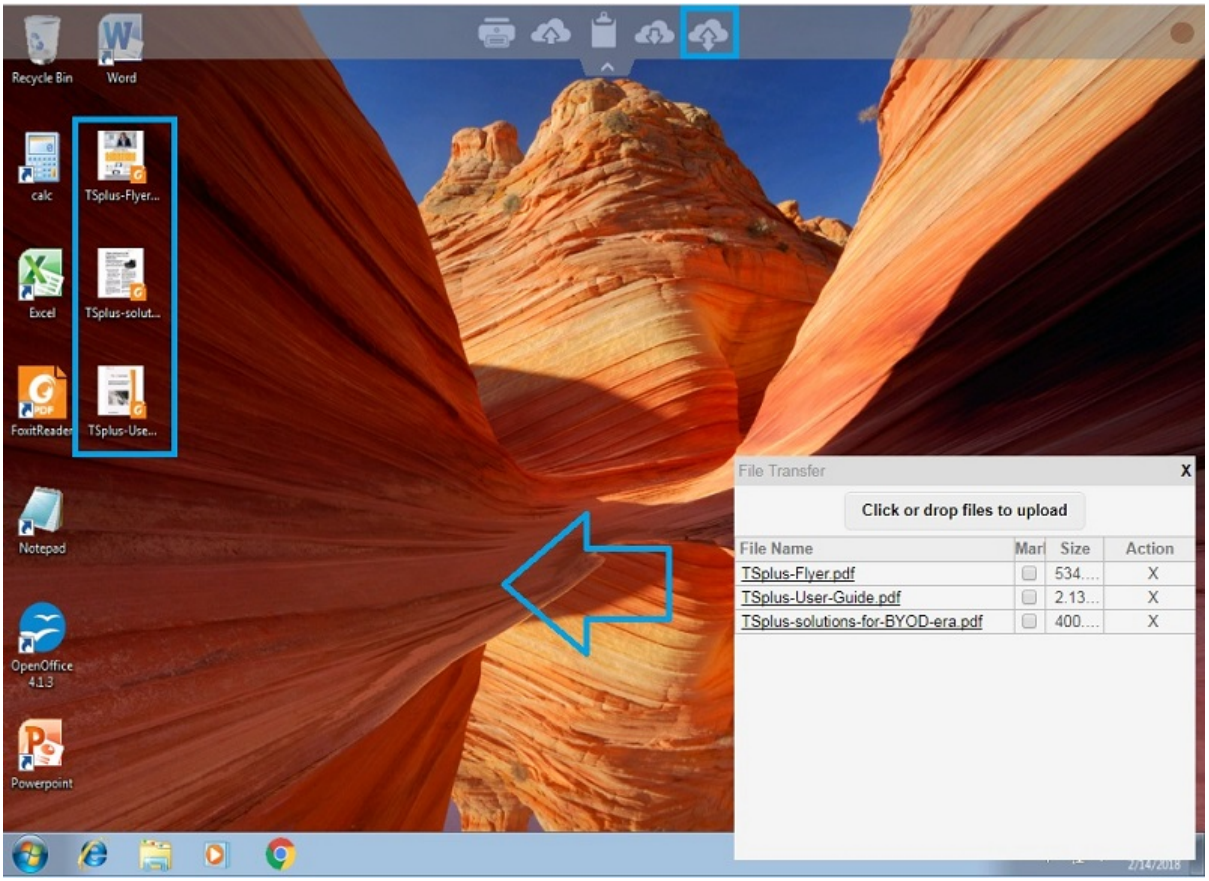
- From the server to the local computer:





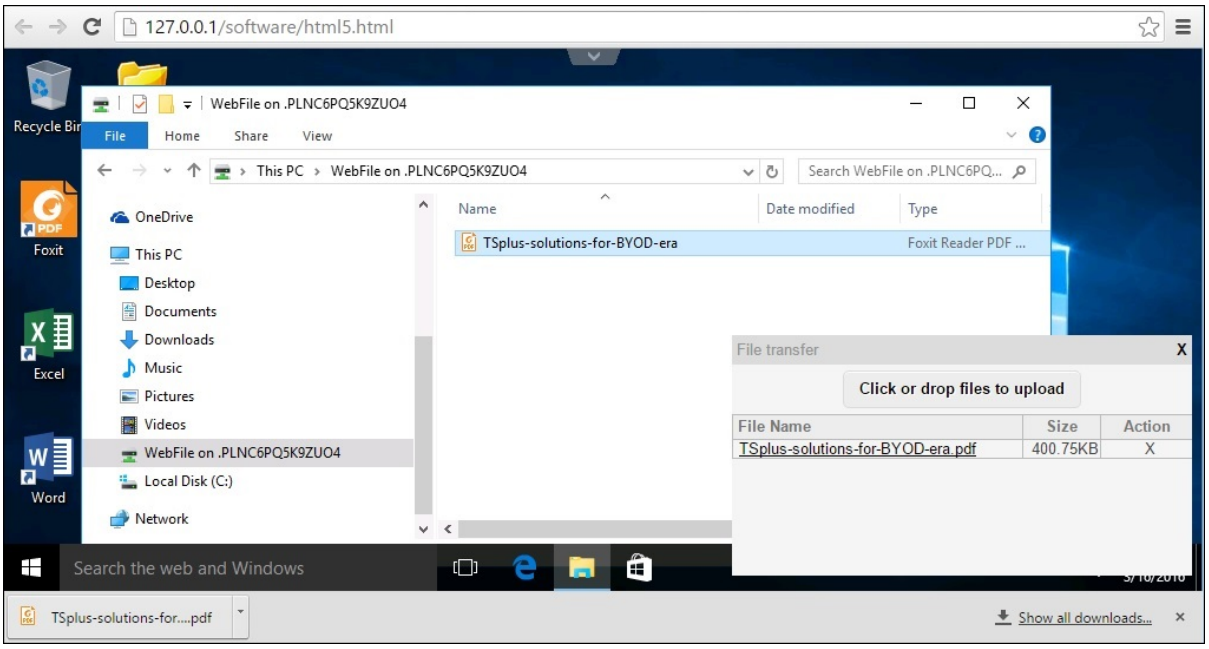
- The file manager which enables you to transfer files from the local computer to the server, with an history of the transferred files:



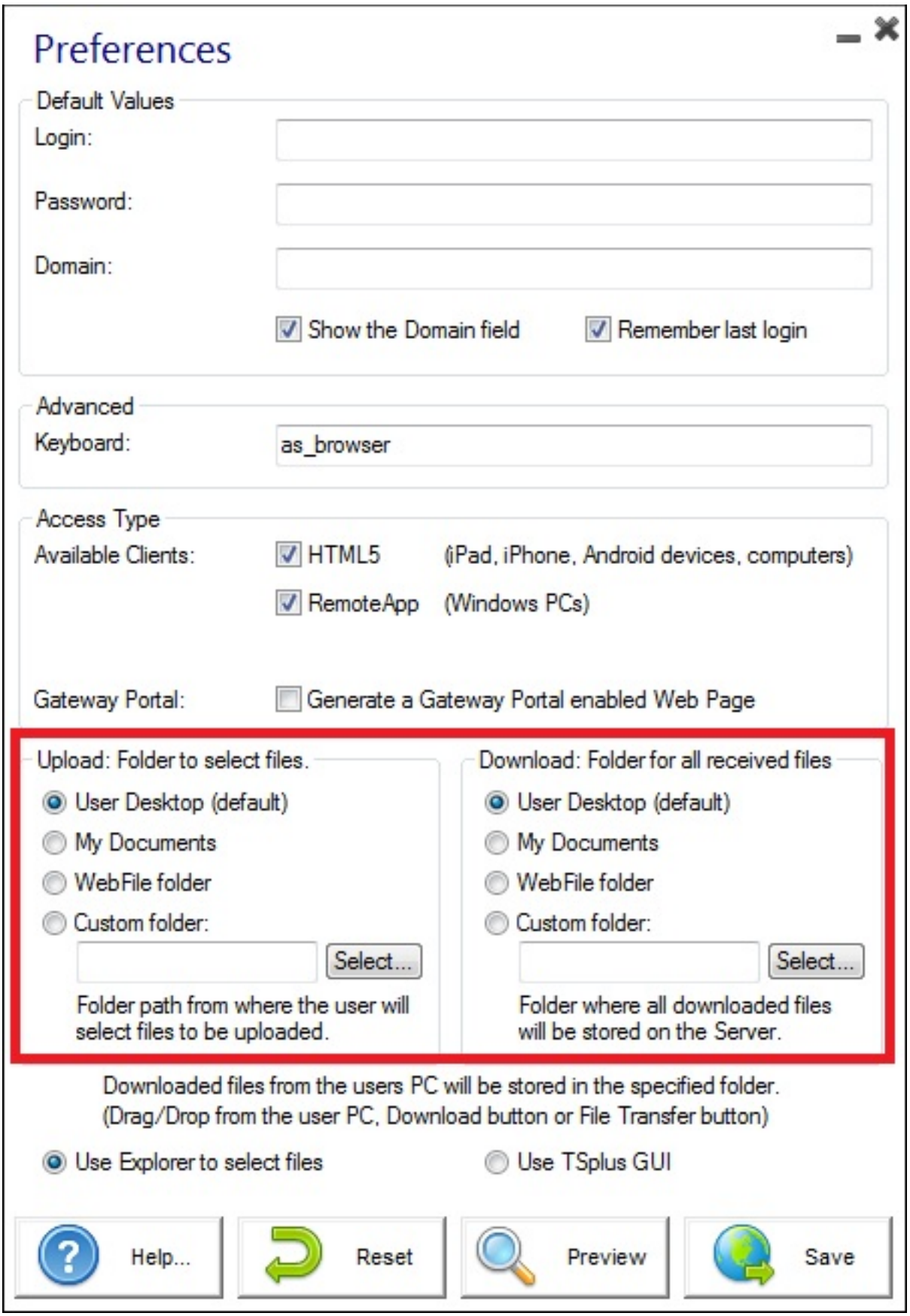


On the browser side the files are showed inside the browser's list menu. It can be opened via action menu or with Shift + F12.

- When you copy files with Explorer into the WebFile folder, this triggers automatically the event about the creation of a new file in the WebFile folder and the browser menu opens/refreshes automatically to show the new file:



When using a custom folder, make sure this folder exists on client and server sides. You can set the upload/download destination folder on the Web Portal preferences tile on the web tab of the Admin Tool:



If you want to avoid this behavior, set the following line on the setting.js file which path is by default: C:\Program Files (x86)\tsplus\Clients\www\software\html5\settings.js :

dropboxonnewfile = 0;

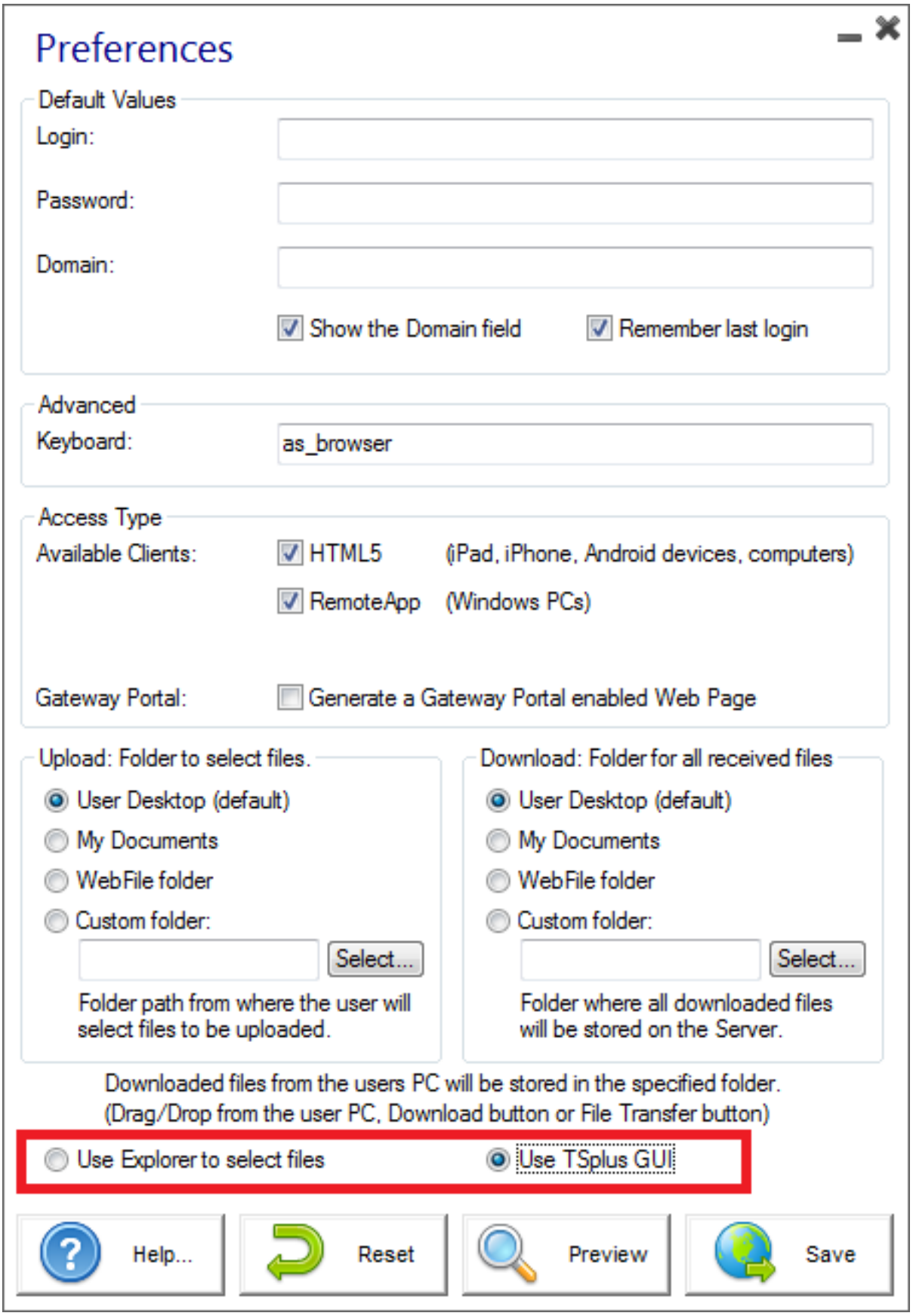
Additionally you can set:

sharedfolder = “yes”;

to show shared folder and share your files with other users (disabled by default).

If you do not have a file named “settings.js” in the “C:\Program Files (x86)\TSplus\Clients\www\software\html5” folder, then your TSplus version is older and this documentation does not apply. Please update your system first or contact support.

- By default, explorer is used to transfer files. You can also directly download your files from server to client by checking the “use TSplus GUI”, and copy any files into the webfile folder:


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

HTML5 Client: Using Gestures on mobile devices (Touch)

Using screen area:

1. Easy touch on screen = mouse move to touched position and left mouse click
2. Fast double tap on screen = mouse move to touched position and left mouse double click
3. Touch and hold for one second on screen = mouse move to touched position and right mouse click
4. Touch and move outside of cursor area = scrolling the visible session frame (this is native browsers behavior for scrolling especially after pinch-zoom)
5. Touch in cursor area and move = mouse cursor moving only
6. Double tap inside cursor area and move = left mouse down and mouse moving Useful for moving window, moving elements, resizing.
7. Double tap on screen(outside of cursor area) and move finger down/up = middle mouse scrolling Useful for scrolling pages or view pdf's.
8. Pinch zoom with two fingers = zoom the RDP session frame (this is native browsers behavior)

Using mouse pad area - additional functions in the middle point of mouse pad:

1. Easy touch in the middle = left mouse click
2. Double tap in the middle = left mouse double click
3. Touch and move in the middle = mouse move and mouse pad moving
4. Touch and hold for one second = right mouse click

Keyboard mode on:

1. Easy touch on screen = focus lose, keyboard disabled (this is native browsers behavior) but this will fire mouse move and left mouse click.
2. Fast double tap = mouse move and left mouse click (without keyboard disabling) Useful to reposition the cursor, set focus on different character and stay at the same time in keyboard mode.
3. +Functions of mouse pad described above

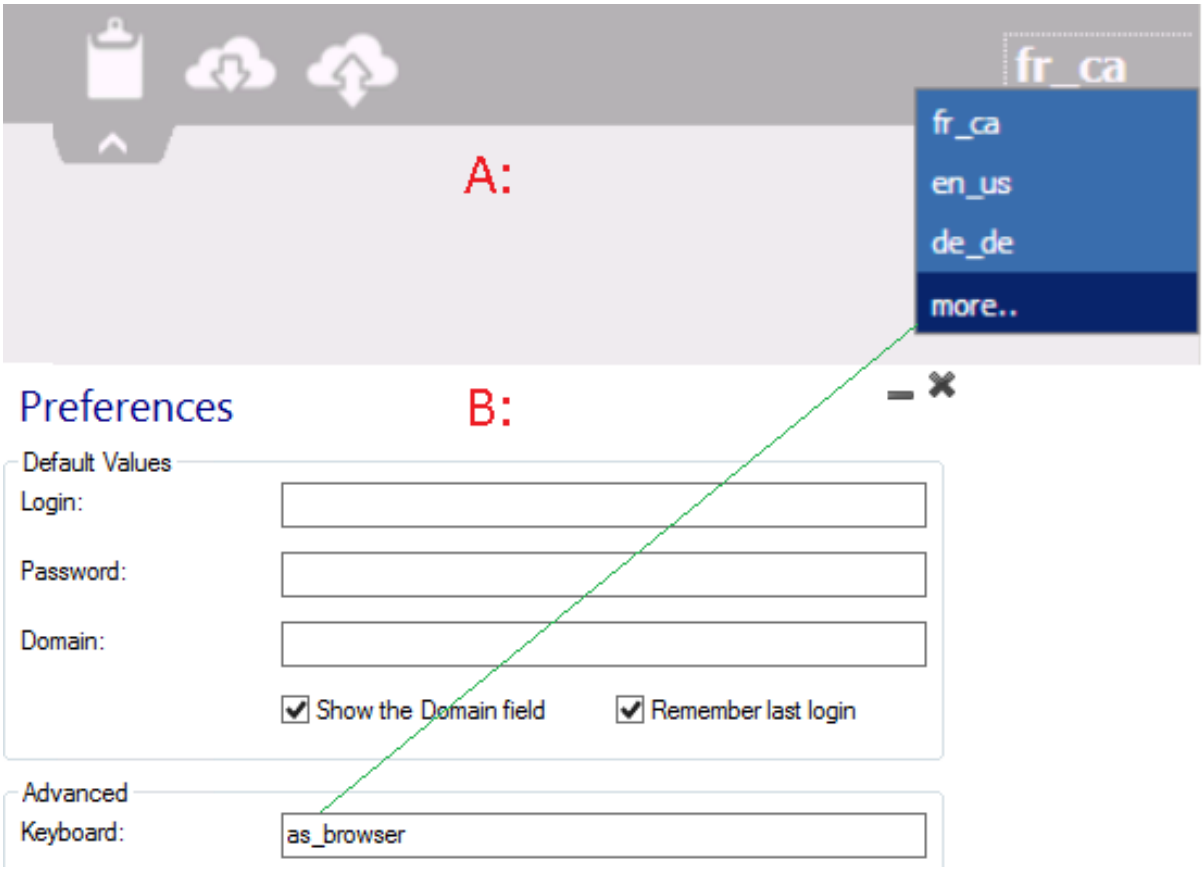
HTML5 Client: Using two languages

By default the HTML5 client tries to recognize browsers default language and then use it inside RDP session. This behavior is controlled by tag “as_browser” However you may find the full list of available language tags in http://your_server/software/language.html under “Locale”

You have the choice to set fixed language either **A:** per client directly from HTML5 top menu.

	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: or from portal by setting it in AdminTool GUI which will be effective for everyone.



You should restart session if setting another language as main.

Remember: when using **HTML5 client** in mulitple language scenario go sure that language used inside Web-HTML5-RDP session is synchronized with the language actually set on your PC/ Laptop/Mac etc. Else some chars that are represented and crossing in every language map may produce wrong char by sending scan code actual for another language. Also that means, if you changed the language from English to German inside web-session then change it to German on PC/Laptop/Mac too.

HTML5 Client: How to maximize the browser window

Overview

The RDP protocol does not allow to resize while connected without a reconnection.

Please note that you will get the best experience possible from Terminal Service Plus HTML5 client by connecting with a maximized browser**.**

However, if you want to force the browser window to be as big as possible, you can try to “force” the HTML5 window to open with the maximum size (but not as a “maximized” window, due to internet browsers security limitations).

Maximizing the browser window

You will have to modify the file “Clients\www\software\common.js” located in your Terminal Service Plus directory. We advise you to use a text editor such as Notepad++ (do not use Word).

In order to have a browser window which uses all the screen, you will have to modify the line(s) with “window.open” in it, and add the following text:

Terminal window
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(screen.availHeight-(55))

This allows IE/Chrome/Firefox/Safari to open the window with a screen size (minus Windows bar). Unfortunately it is not possible to force a web browser to “maximize” the window in a “fullscreen” Windows type.

Open the file and search “window.open(”

Then add the new at the end before the brackets, for example:

Terminal window
window.open(hostGateway + jwtsclickLinkBefore(getside(), p), window.opforfalse);

will become:

Terminal window
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)));

And again:

Terminal window
tmpwin = window.open(p, '_blank'); //Chrome needs _blank

will become:

Terminal window
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

And again:

Terminal window
success = window.open(p, k);

will become:

Terminal window
success = window.open(p, k,
"screenX=0,screenY=0,left=0,top=0,fullscreen=yes,width="+(screen.availWidth-5)+",height="+(sc
reen.availHeight-(55)));

And finally :

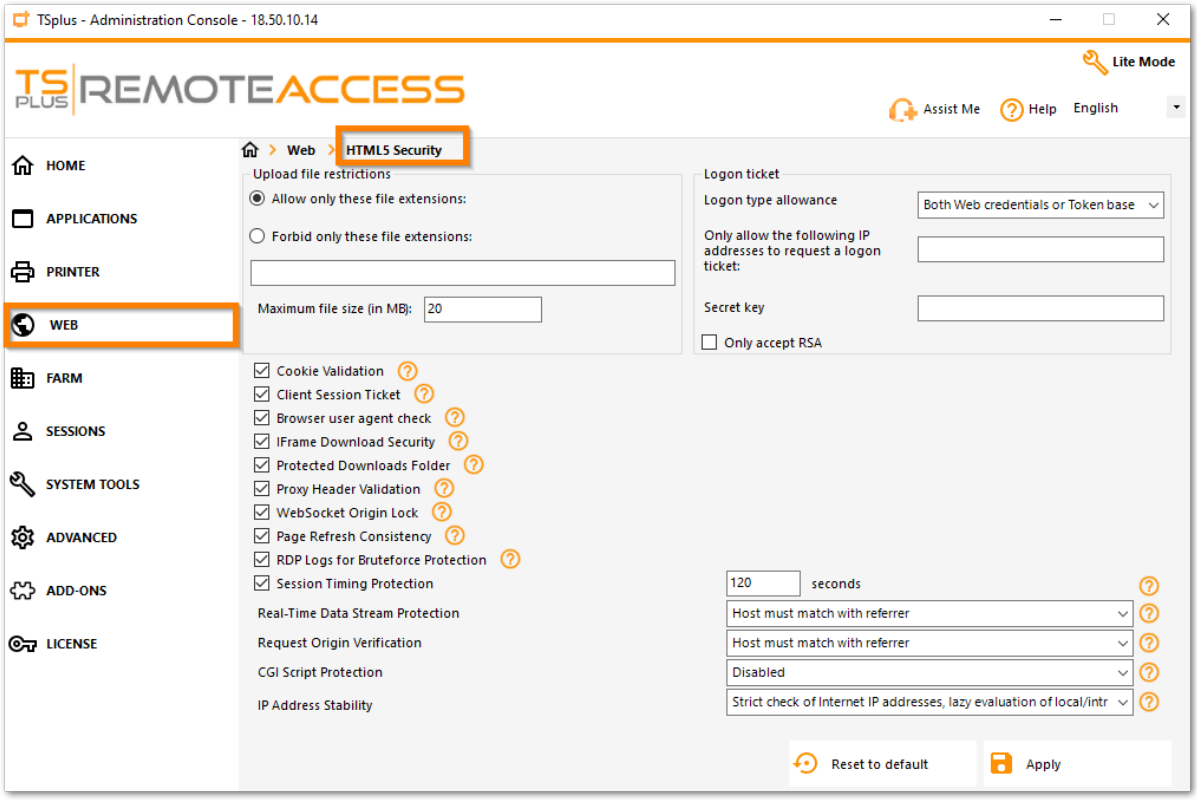
Terminal window
cpwin = window.open("about:blank", n);

will become:

Terminal window
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)));

HTML5 Security

In the HTML5 Security tab, you can manage web settings.



If you need additional security, you can view and download our Advanced Security.

HTML5 Server Memory Usage

Terminal Service Plus HTML5 Server runs on JAVA. Understanding how JAVA handles memory help to understand Terminal Service Plus HTML5 Server memory usage.

Assigned memory

When Java runs, it tries to allocate 25% of the computer physical memory. This memory is “assigned” but not directly used - it is not the real memory usage that one can see in Windows Task Manager.

JAVA platform: 32-bit vs 64-bit

There is one big difference between these two platforms:

- JAVA 32-bit cannot handle more than 4GB of RAM by definition. Since it will allocate 25% of all available memory, it will allocate at most 1GB, assuming there is 4GB physical memory. If there is only 2GB physical memory, it will only allocate 500MB, etc.
- JAVA 64-bit can handle a lot more than 4GB (theoretically up to 16 exabytes), so the allocated memory will only depend on physical memory.

JAVA Memory Management

JAVA is a “virtual machine”. It means that JAVA handles memory management on its own. Once JAVA allocates some memory, even when it does not need it anymore, it will not automatically give it back to the system. This is for performance reasons, as memory allocating and de-allocating are CPU intensive tasks.

JAVA will usually wait until it has a big chunk of unused memory before giving it back to the system. The size of this big chunk directly depends on the size of the computer physical memory. The more physical memory on a computer, the more memory is allocated by JAVA.

Terminal Service Plus HTML5 Server Memory Usage

All these technical details are the reason why one can open Windows Task Manager and think

that Terminal Service Plus HTML5 Server uses a lot of memory, or that JAVA 32 bit uses less memory than JAVA 64 bit.

Actually, the memory really used by Terminal Service Plus HTML5 Server is directly related to the number of opened HTML5 sessions. The more available memory on the computer, the more HTML5 sessions you can open.

HTML5 Session Memory Usage

The memory used by an HTML5 session depend on the user activities (applications and programs used, Word/Excel versus drawing-intensive programs) and the connectivity method established between the Terminal Service Plus HTML5 Server and the client computer.

In the general use case, an HTML5 session will use 30 MB of memory (standard use, binary websockets connectivity). In the worst case, a session will use up to 100 MB of memory (intensive use, “XHR” fallback connectivity for older browsers).

Loss of HTTP and HTTPS server listening

Each Java error log indicates sufficient native memory for operation.

The problem is actually quite simple.
When the HTML5 session starts, there is enough memory according to the reported values.
Then, within the RDP session, it starts an unknown program and steals all the native memory for itself.

When Java requests it again, it is suddenly no longer available, causing this insufficient memory error.

- There is insufficient memory for the Java runtime environment to continue.
- Native memory allocation (mmap) failed to map 234881024 bytes. Error details: virtual space G1# Possible reasons:
- The system has run out of physical RAM or swap space# This process is running with Compressed Oops enabled, and the Java heap may be blocking the growth of the native heap

Possible solutions:

- Reduce the memory load on the system
- Increase physical memory or swap space# Check if the swap support storage is full
- Decrease the Java heap size (-Xmx/-Xms)
- Decrease the number of Java threads # Decrease the Java thread stack size (-Xss)
- Set a larger code cache with -XX:ReservedCodeCacheSize=

The JVM is running in Zero Based Compressed Oops mode, in which the Java heap is placed in the first 32 GB address space. The base address of the Java heap is the maximum limit for

native heap growth.
Please use **-XX:HeapBaseMinAddress**

Potentially, you could allocate more native memory to Java from the start and force it to stop returning memory to the system, thus allocating it to itself.
However, in this case, you will encounter the following problem: programs running in an RDP session may run out of memory, and the entire system could crash.

But you can still try.

1. Open and edit the following file with Notepad: *\Clients\webserver\runwebserver.ini

2. There, you will find the following command-line settings, like this:

Terminal window
-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. Remove the entire line from runwebserver.ini and add the following in its place:

Terminal window
-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. Restart the HTML5 server via the AdminTool GUI to apply the changes.
   (But before doing so, make sure that the web server\runwebserver.bat file doesn't have a read-only attribute set in its properties. Otherwise, the AdminTool GUI won't be able to adapt runwebserver.bat after a restart.)

In most cases, this should be sufficient. Once Java uses memory, it will allocate it to other uses instead of returning it to the system. Therefore, the memory usage of html5service.exe could potentially reach 70% of the system's available memory. In this case, Java should potentially stop crashing. However, if another program is consuming a large amount of memory, it could crash instead. In that case, we are powerless; you must ensure that there is enough memory to run a Java HTML server as well as others. programs.

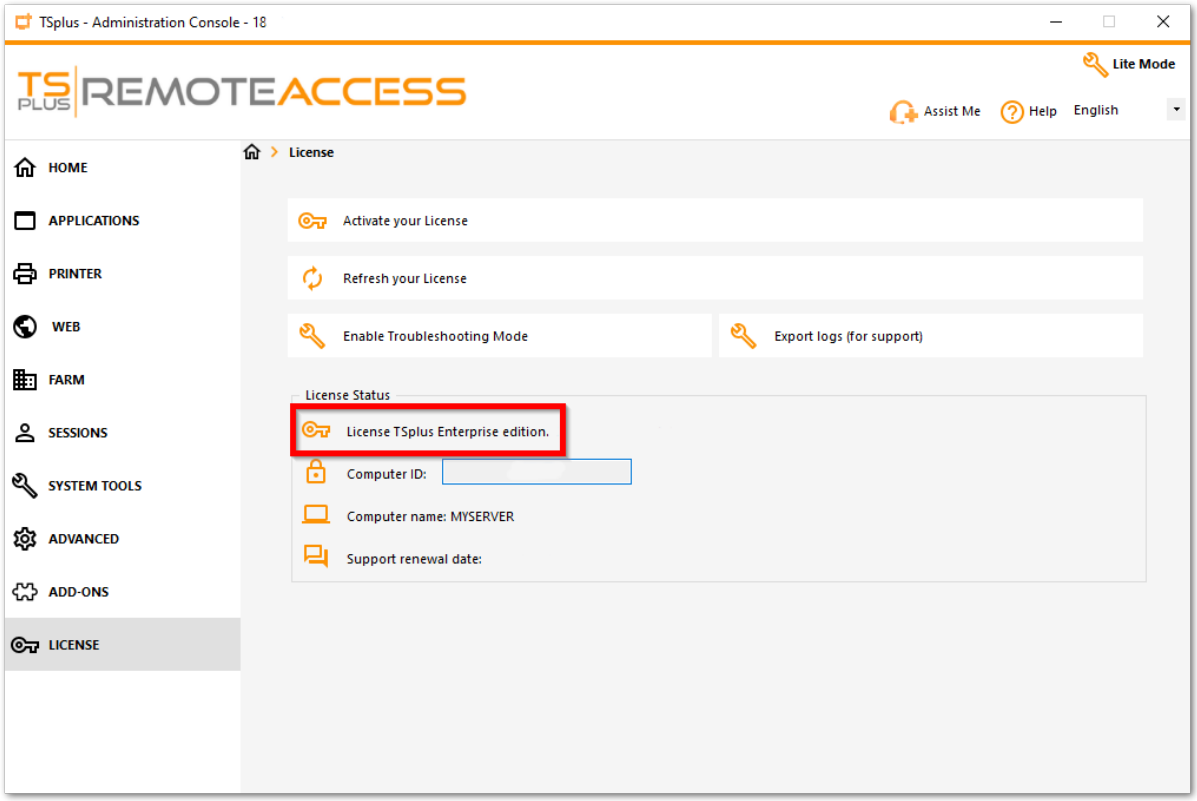
There’s an option in Java called -XX:+AggressiveHeap that could improve memory allocation for the Java Virtual Machine itself, and therefore the final content of *\webserver\runwebserver.ini.

It might look something like this:

Terminal window
-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

How to identify your TSplus Edition

On the License Tile under the Serial Number, you can see the type of License you purchased as well as your number of users next to the number of connections:



TSplus has merged old licenses into one in order to gain more clarity. System and Printer editions have migrated to **Desktop Edition**.

Desktop Edition

Basic features:

- TSplus Administrator Tool (AdminTool),
- Concurrent connections support,

- Application Control per user and/or per groups,
- TSplus Remote Taskbar and/or TSplus Floating Panel,
- Remote Desktop access,
- TSplus Portable Client Generator,
- RemoteApp connection client,
- Fully compliant with RDP protocol,
- Dual Screen support, bi-directional Sound, RemoteFX when compatible with Windows version,
- Local and Remote connection support,
- Workgroup and Active Directory users support,
- Device/Disk redirection.
- Virtual Printer, enables you to print from any location, without having to install any specific driver and allows printer redirection.

Mobile Web Edition

Enables you (in addition to all the System and Printer editions features) to:

- Connect from any web browser with TSplus HTTP Web Server,
-

Entirely secured connection from any web browser with TSplus HTTPS Web Server and SSH server,

- HTML pages includes Windows and HTML5 web access clients,
- Easily connect from iPhone/iPad and Android devices, also with the TSplus Mobile App,
- Customize logon web page with TSplus easy-to-use Webmaster Toolkit,
- With TSplus Web Applications Portal, users can access their application list inside their web browser,
- Instead of Windows Credentials, TSplus Web Credentials allows users to connect with only an e-mail or a pin-code,
- Universal Printer enables you to print from any location, without having to install any specific printer driver,

Enterprise Edition

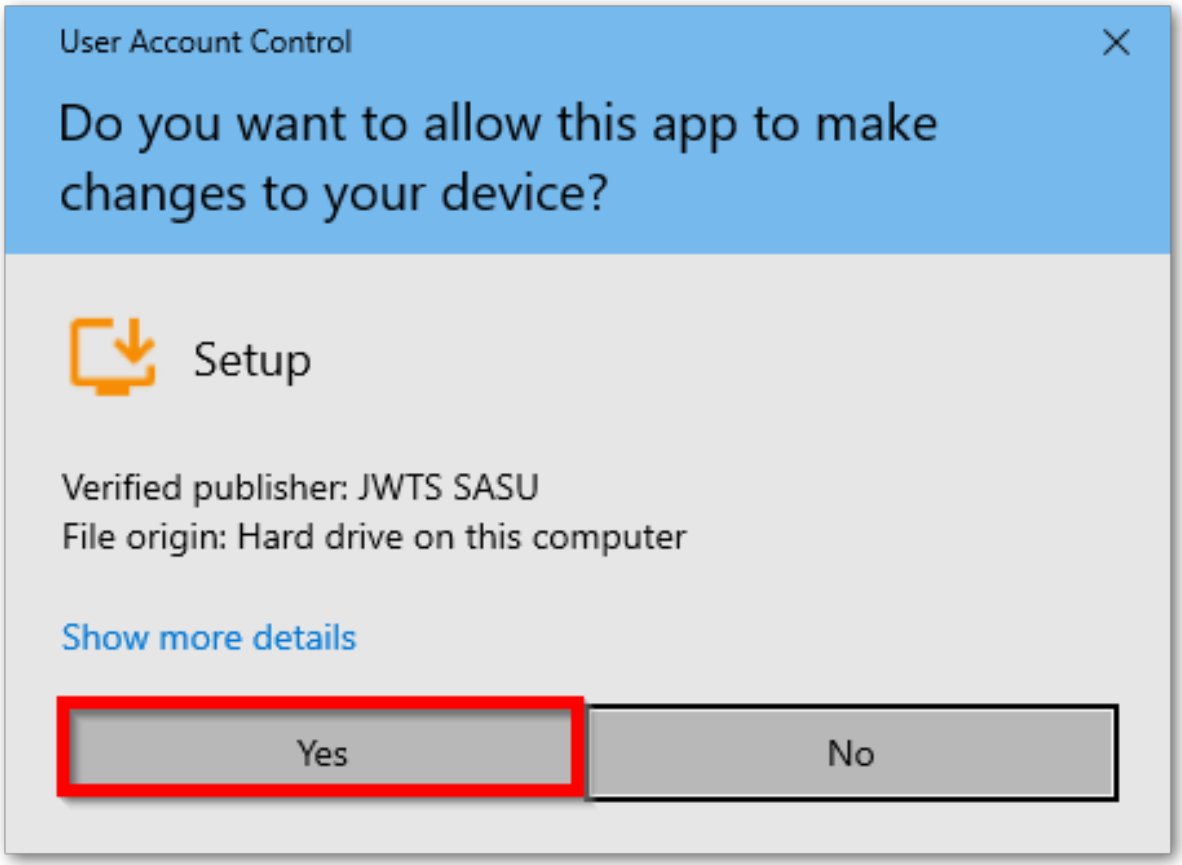
Includes all of the previous features plus these ones:

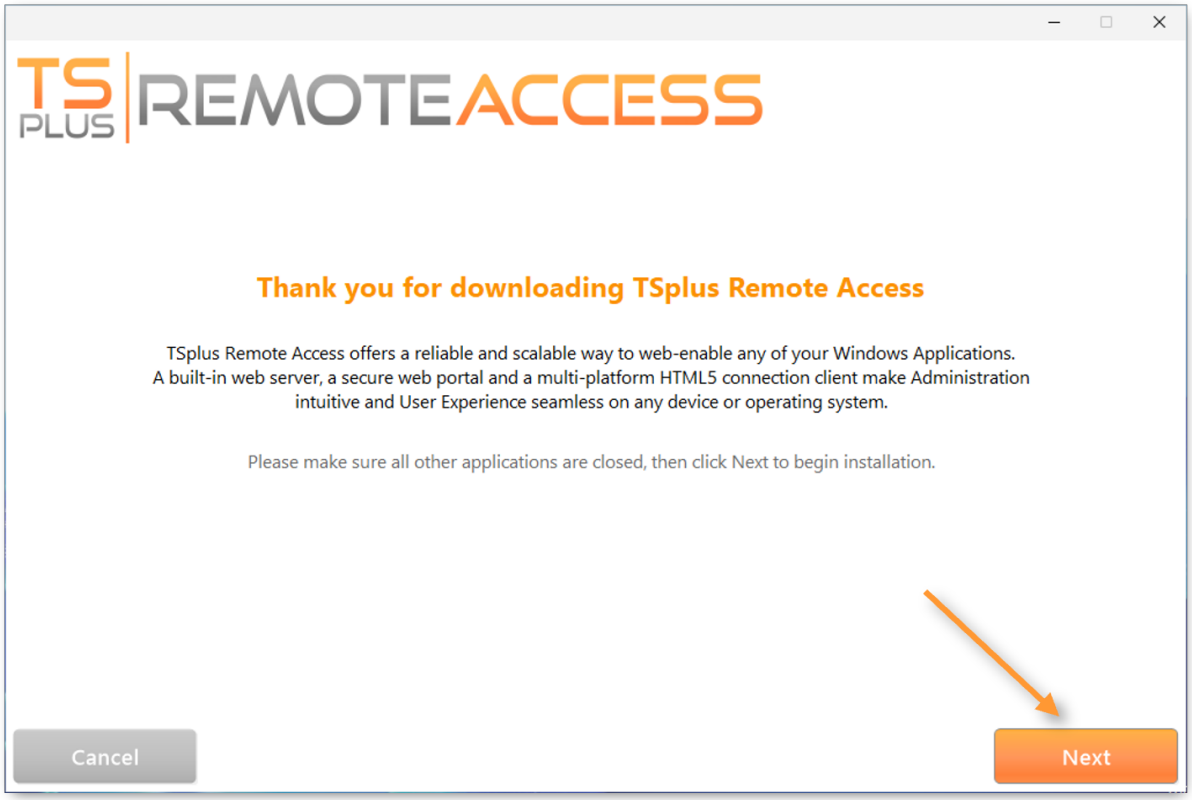
- Support an unlimited number of servers within each TSplus Farm (requires one license per server),
- Thousands of users working concurrently on a scalable Load-Balanced architecture,
- Single Enterprise Portal to access all your TSplus servers,
- Ability to assign one or several Application Server(s) to users or groups of users,
- Load Balancing and Failover support included.

- The Possibility to add an extra-layer of security with the TSplus 2FA Add-On.

TSplus Remote Access v19 Installation

Run TSplus Remote Access Setup program and then **follow the installation steps**.
Your local administrator password is required after the first restart of TSplus Remote Access.





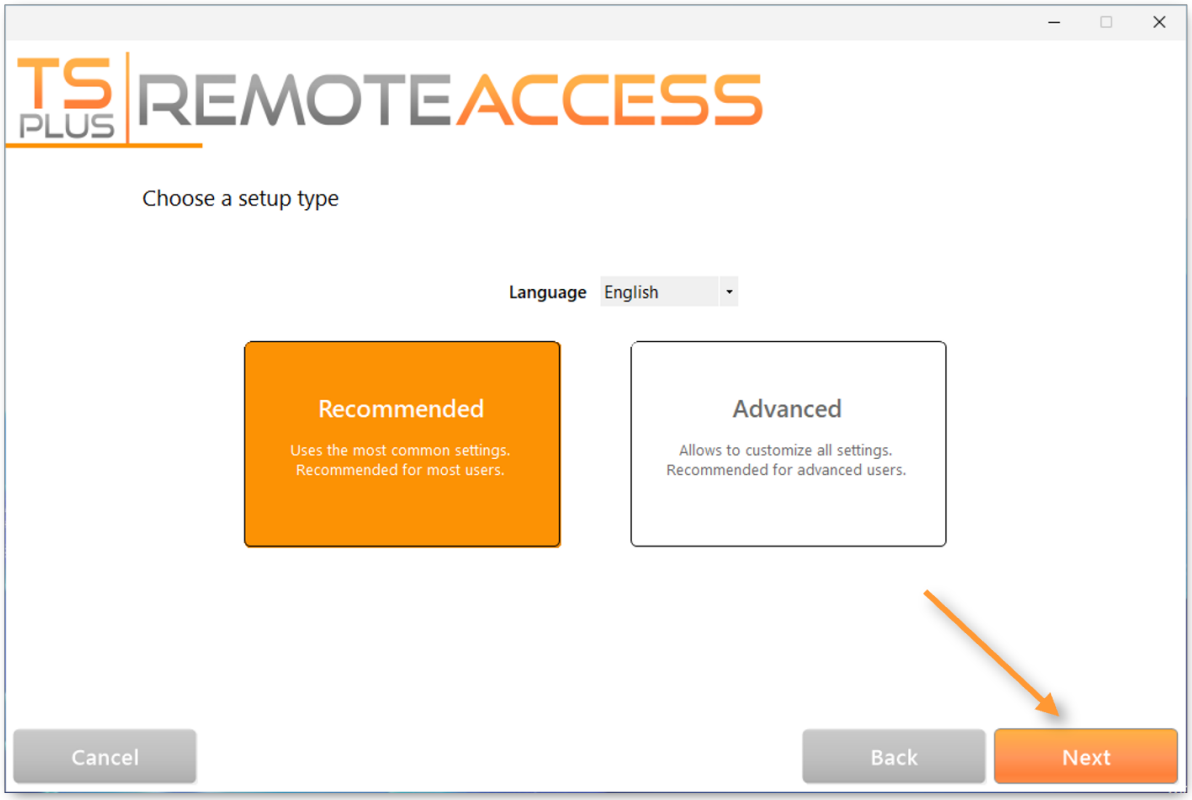
You can then select your language (possible to change it later)

You can then select two custom options by checking the corresponding boxes: **Recommended** or **Advanced**

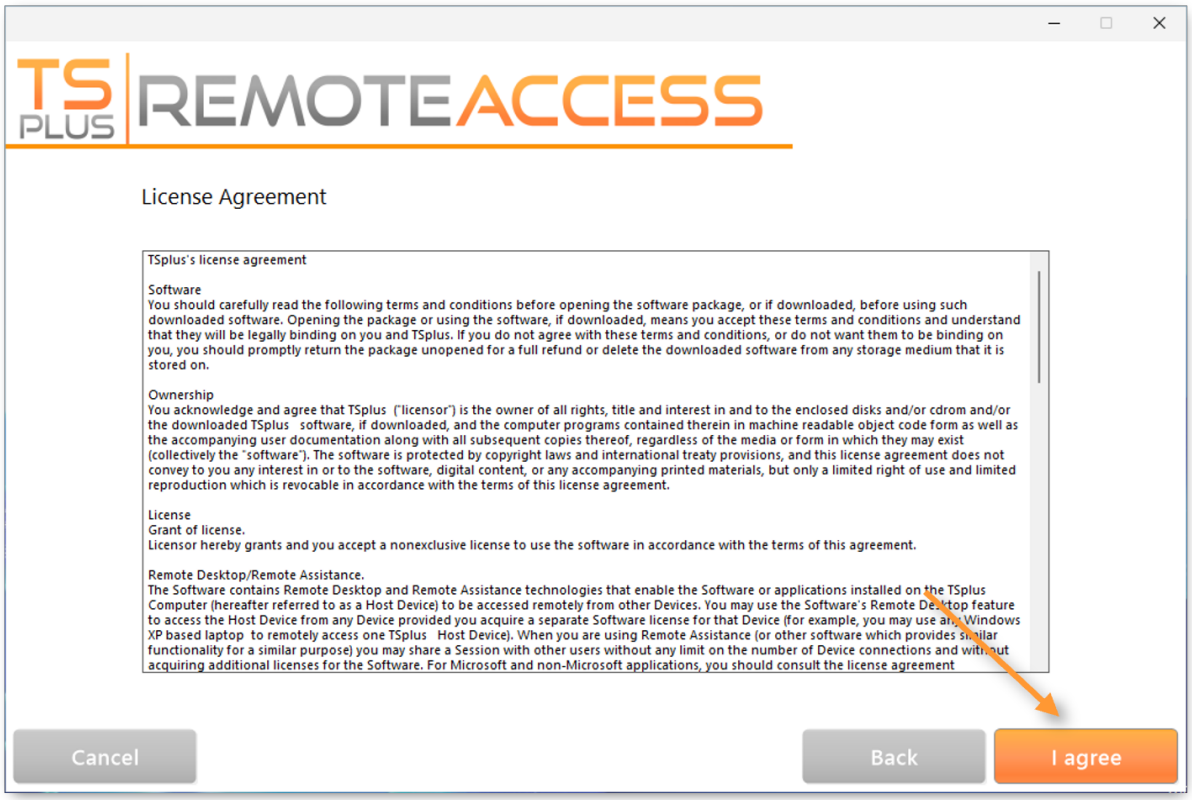
The Advanced option allows you to:

- Not install TSplus Advanced Security.
- Use custom proxy settings.
- Download only the installer, which does not install TSplus.
- Change default ports (not recommended).

Click on Next.



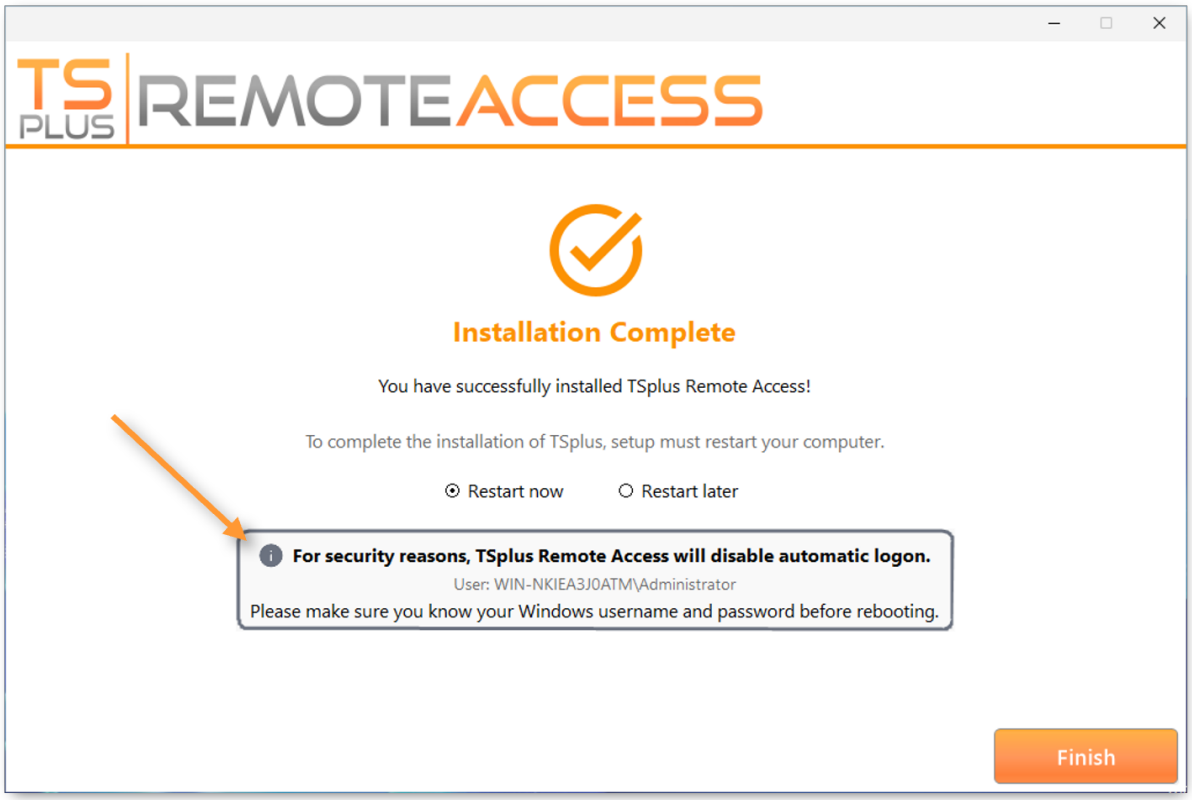
Click on “I accept the agreement”.



Please wait, downloading and installing the program



Then the TSplus logo appears and a window informs you about the completion of the installation.

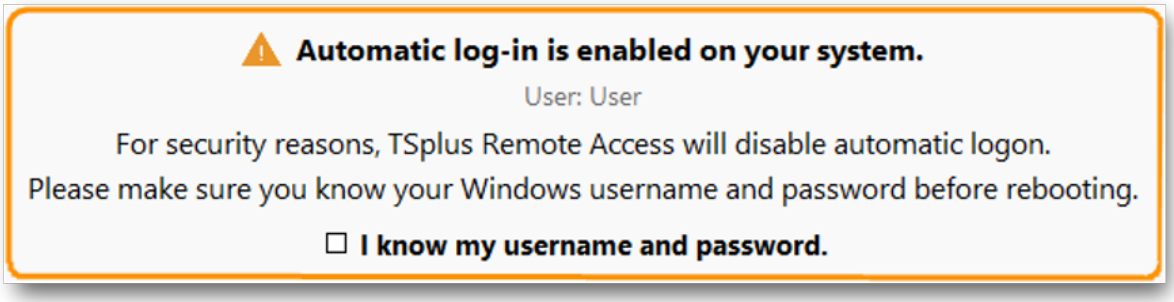


☐ Important Notice

For security reasons, **TSPlus Remote Access** will require you to manually enter your username and password at each login.

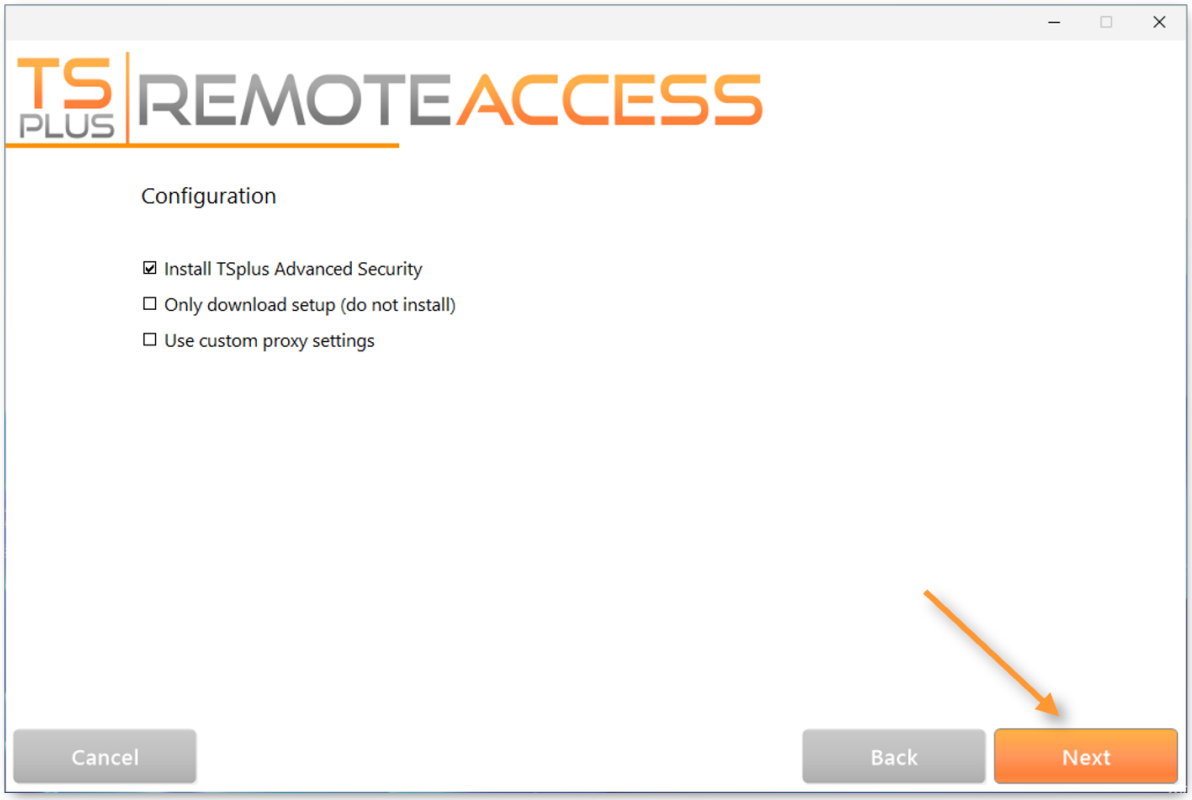
Make sure you know your credentials before restarting the system to avoid being locked out.

If
autologon
is enabled on the system, the installer will show a warning popup asking you to confirm you know your username and password.



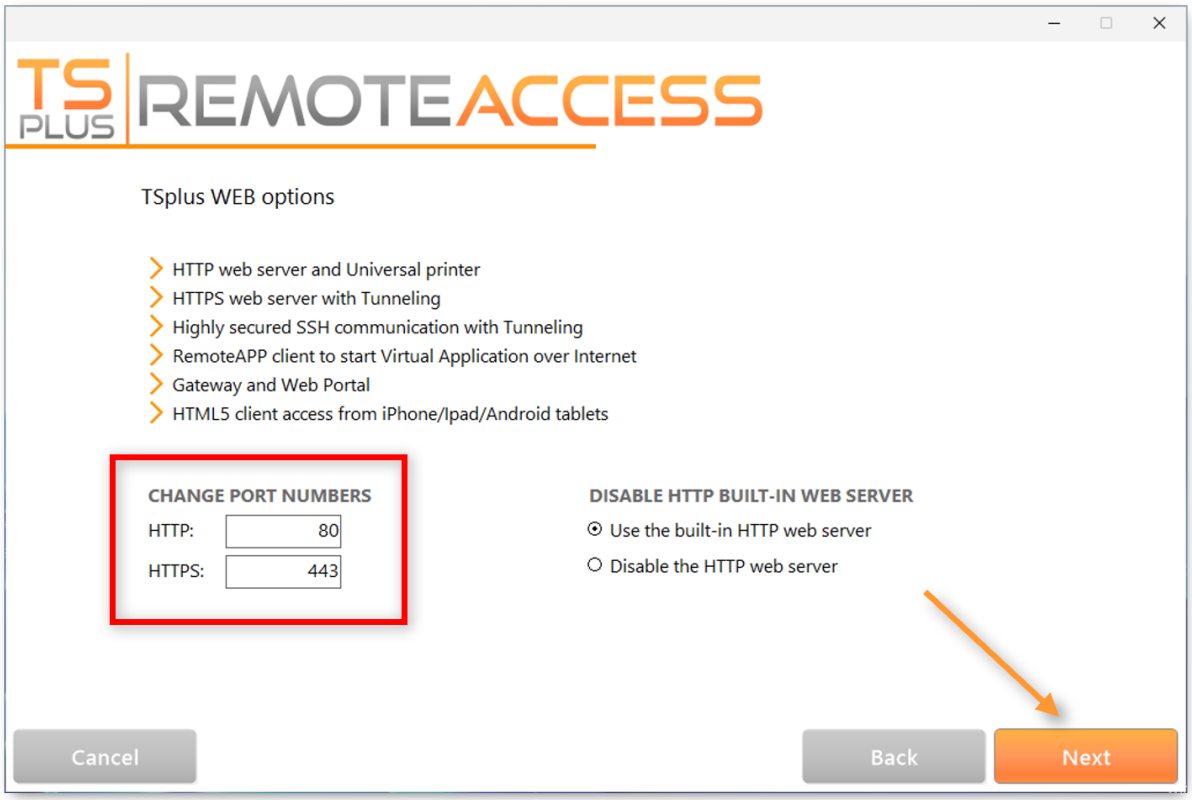
To use TSplus, you must reboot your system. The trial period delivers a full product for 15 days and 5 concurrent users.

The steps below only if you check install TSplus Remote Access in **Advanced mode**.

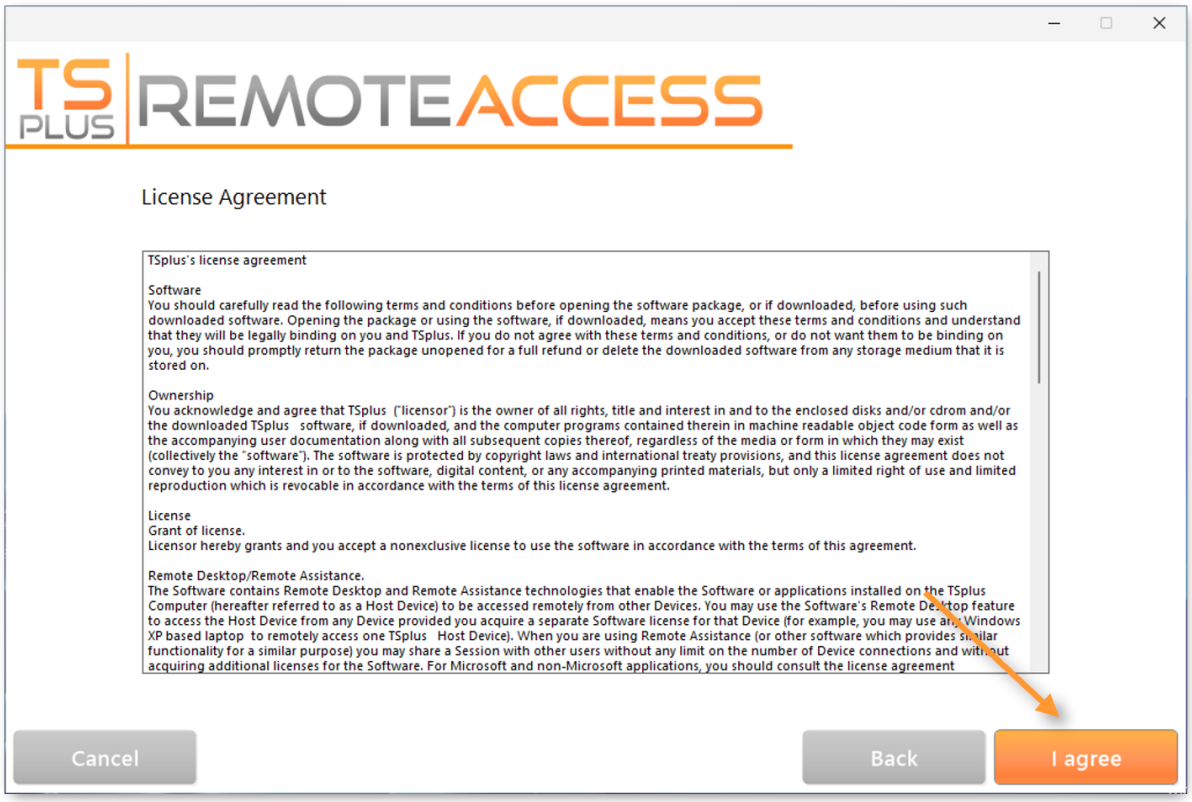


Web servers are listening on ports 80 and 443 by default. We recommend you to accept our TSplus default installation settings. According to our experience, most of the production issues are due to Windows security features.

You can still modify these ports if you wish during installation or at any time on the Built-in Web Server Management of the AdminTool. Just make sure that the defined ports are available and that Java is installed on the server.



Click on “I accept the agreement”.



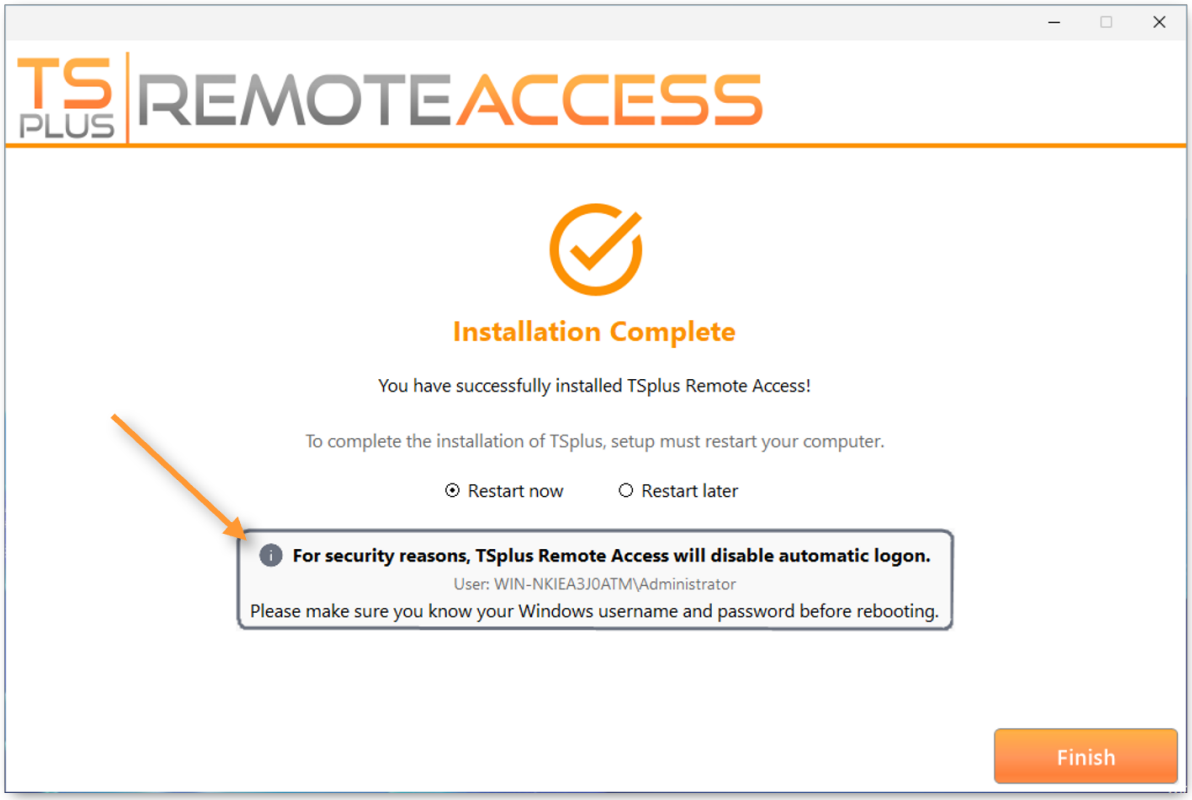
The progress bar appears and allows you to follow the progress of the process:



- Since TSplus 11.40 version, you will have the choice to install TSplus Advanced Security, our powerful Security Add-On, in its Ultimate trial version (All Security features free to use for 2 weeks) to your TSplus system:

For more information about this product, see pages about TSplus Advanced Security documentation.

Then the TSplus logo appears and a window informs you about the completion of the installation.

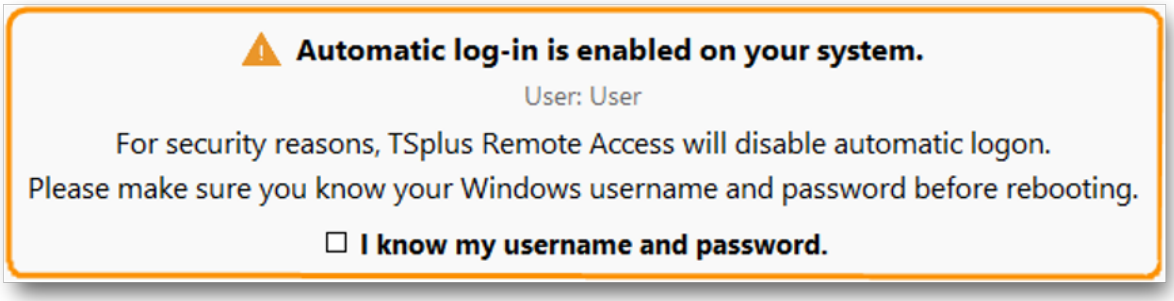


☐ **Important Notice**

For security reasons, **TSPlus Remote Access** will require you to manually enter your username and password at each login.

Make sure you know your credentials before restarting the system to avoid being locked out.

If
autologon
is enabled on the system, the installer will show a warning popup asking you to confirm you know your username and password.



To use TSplus, you must reboot your system. The trial period delivers a full product for 15 days and 5 concurrent users.

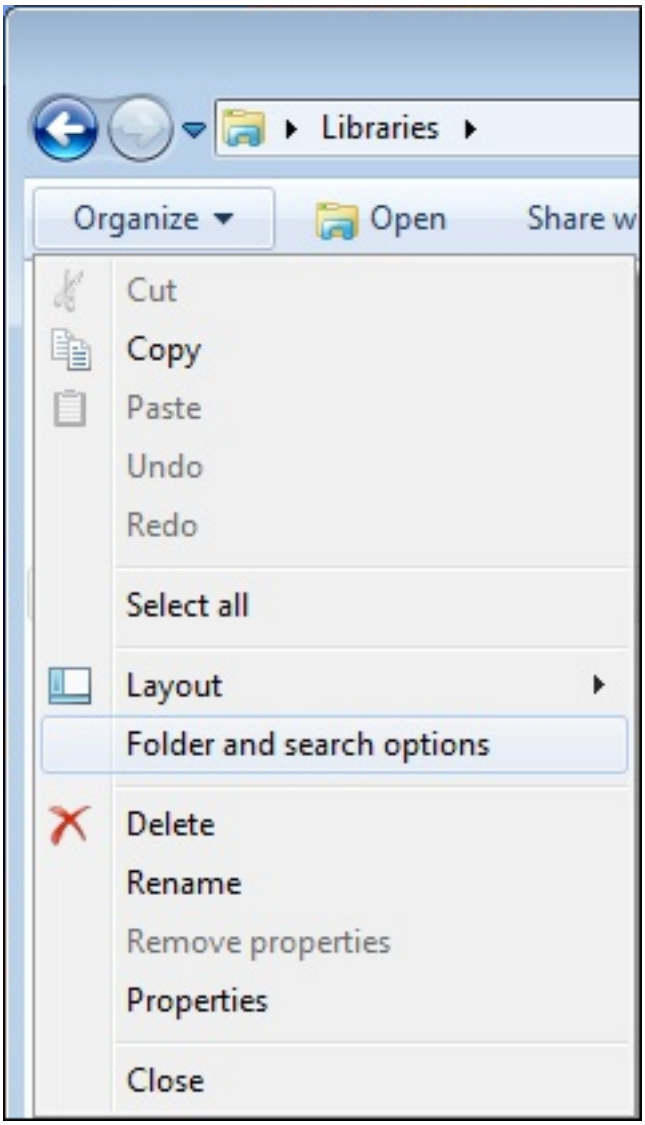
How to mount a logical drive within a TSplus session

This tutorial will cover the following aspects:

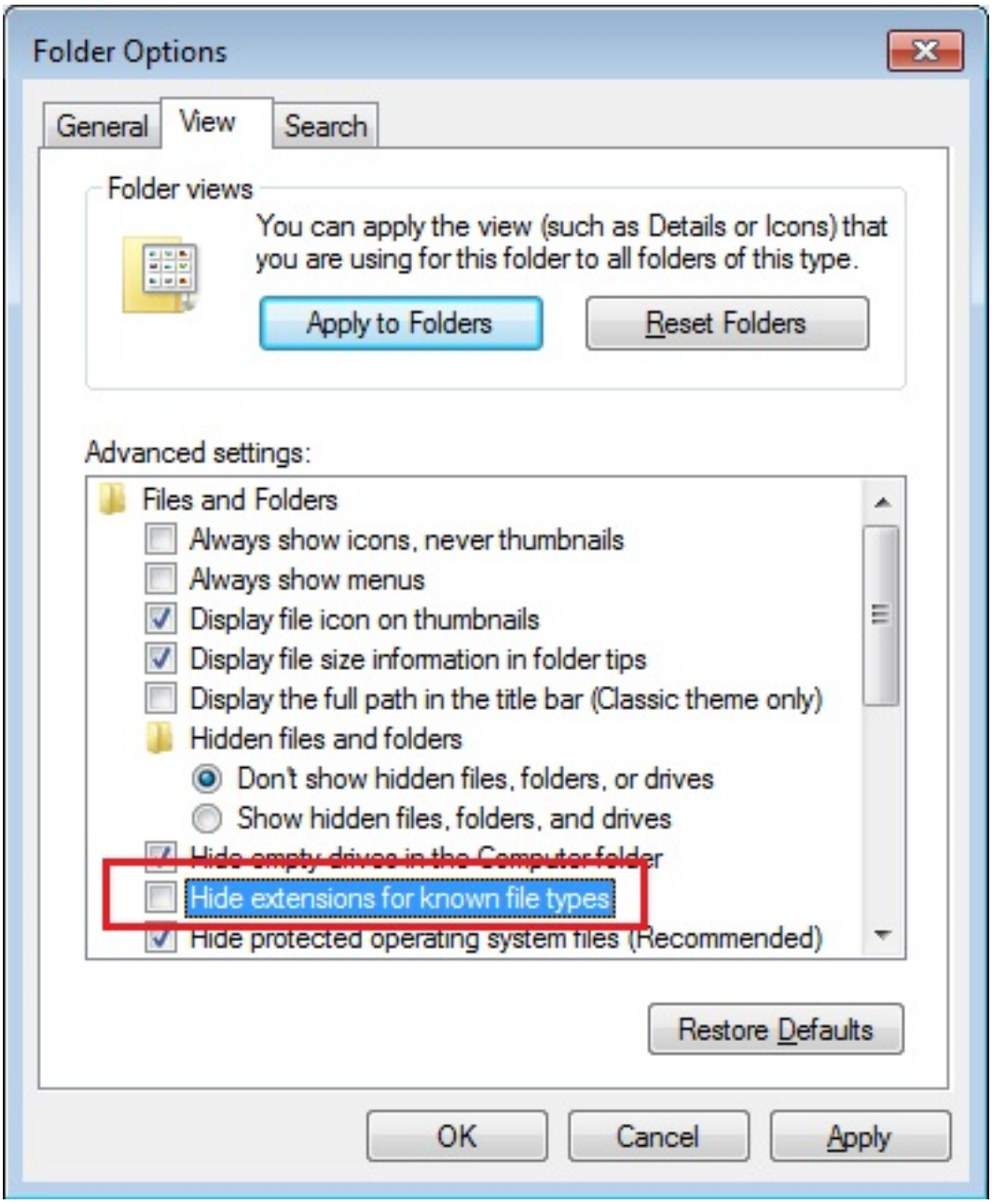
- How to deploy a logon script and have multiple logon scripts scenarii.
- Mounting a specific folder within a session from client or server side.

If you wish to publish a folder on a logical virtual drive for your users, just follow this procedure:

Prior to creating the script, open windows explorer and click on “Folder and search options”.



Then, click on the view tab and uncheck the box “Hide extensions for known types”:

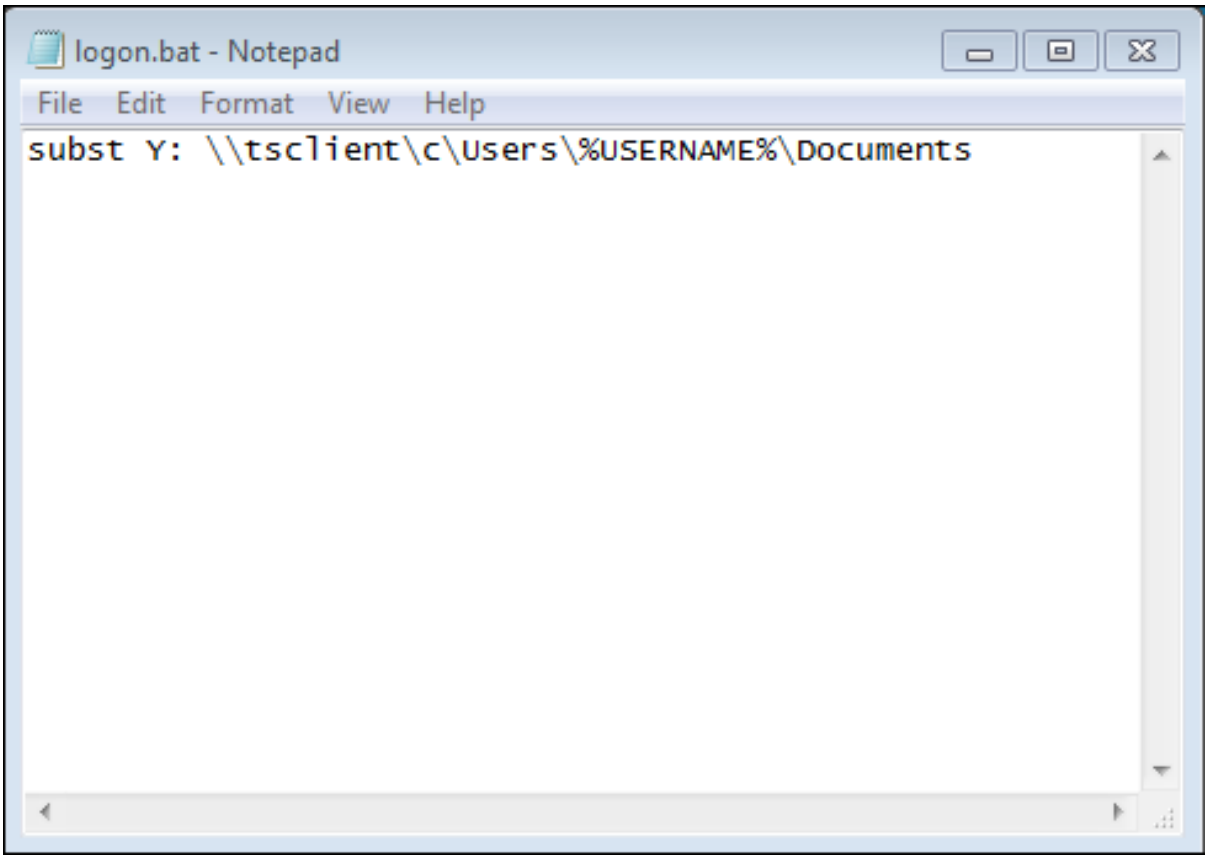


Create a text document and modify the extension by naming it “logon.bat”:



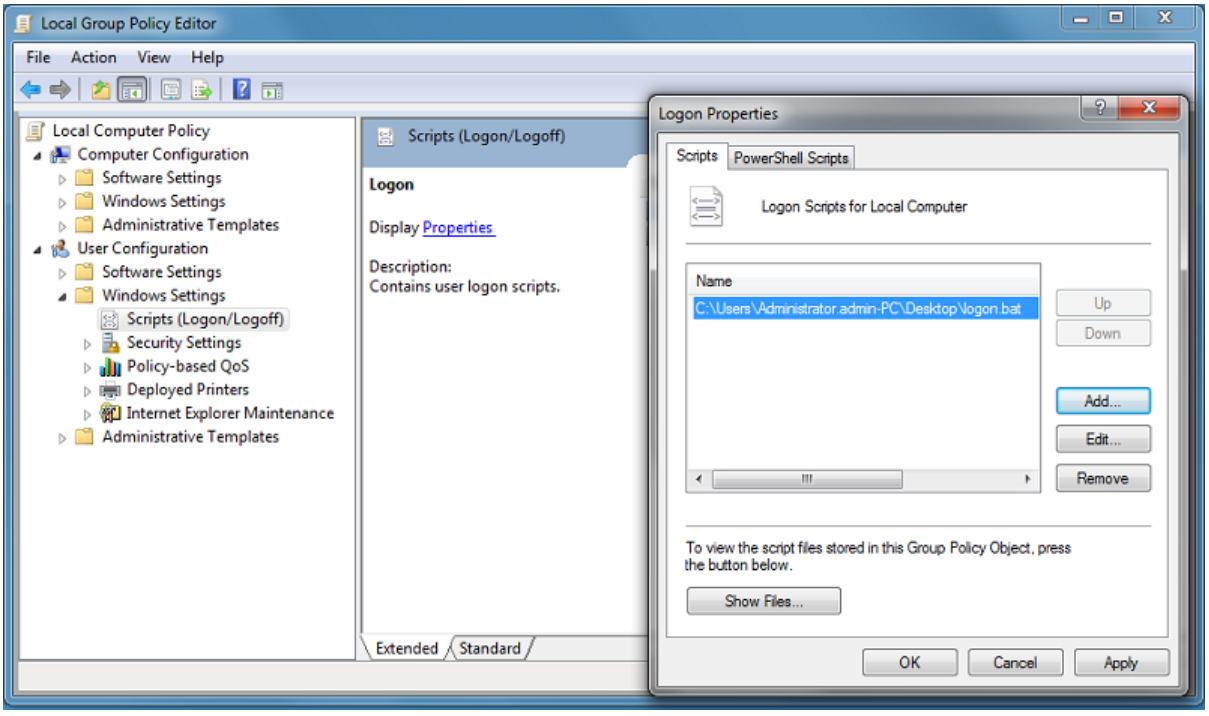
Inside the file, enter for example this command to publish the Folder.exe folder:

“subst Y: \tsclient\C\Users%USERNAME%\Documents”

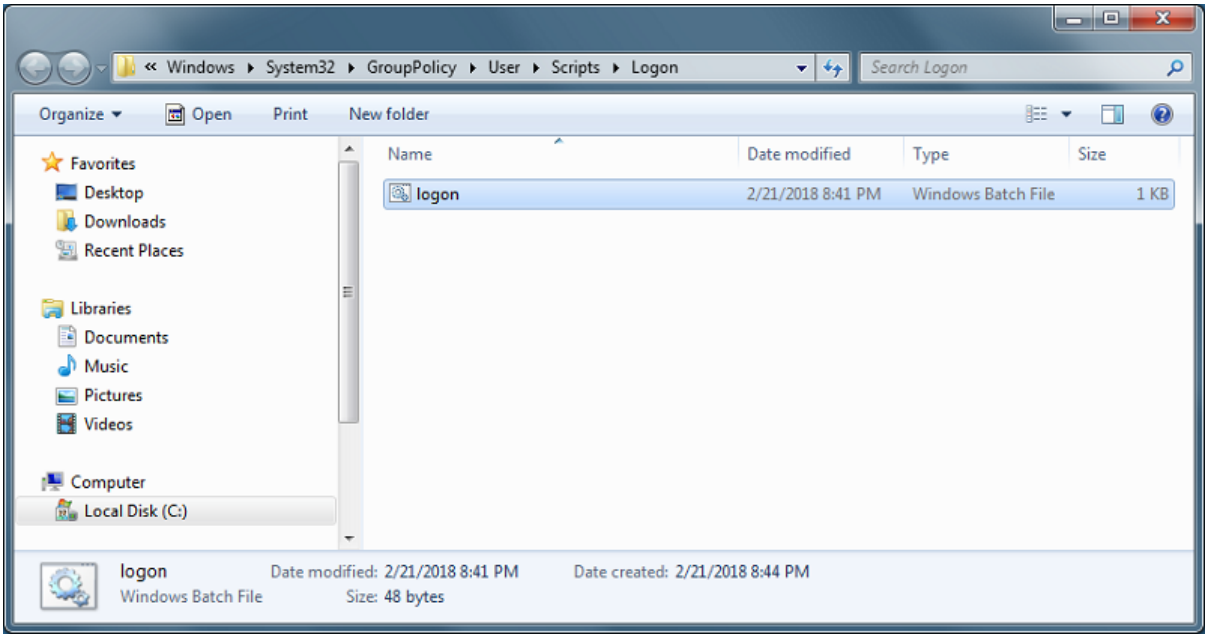


Then, on the start menu, type in gpedit.msc on the search taskbar. We are going to use local policy so that every user connecting to this server launches the script.

Go into the user's configuration menu, then into the Windows settings, and finally, into Scripts (Logon/Logoff) Double click on the Logon script, then click on "Add", then on "Browse".

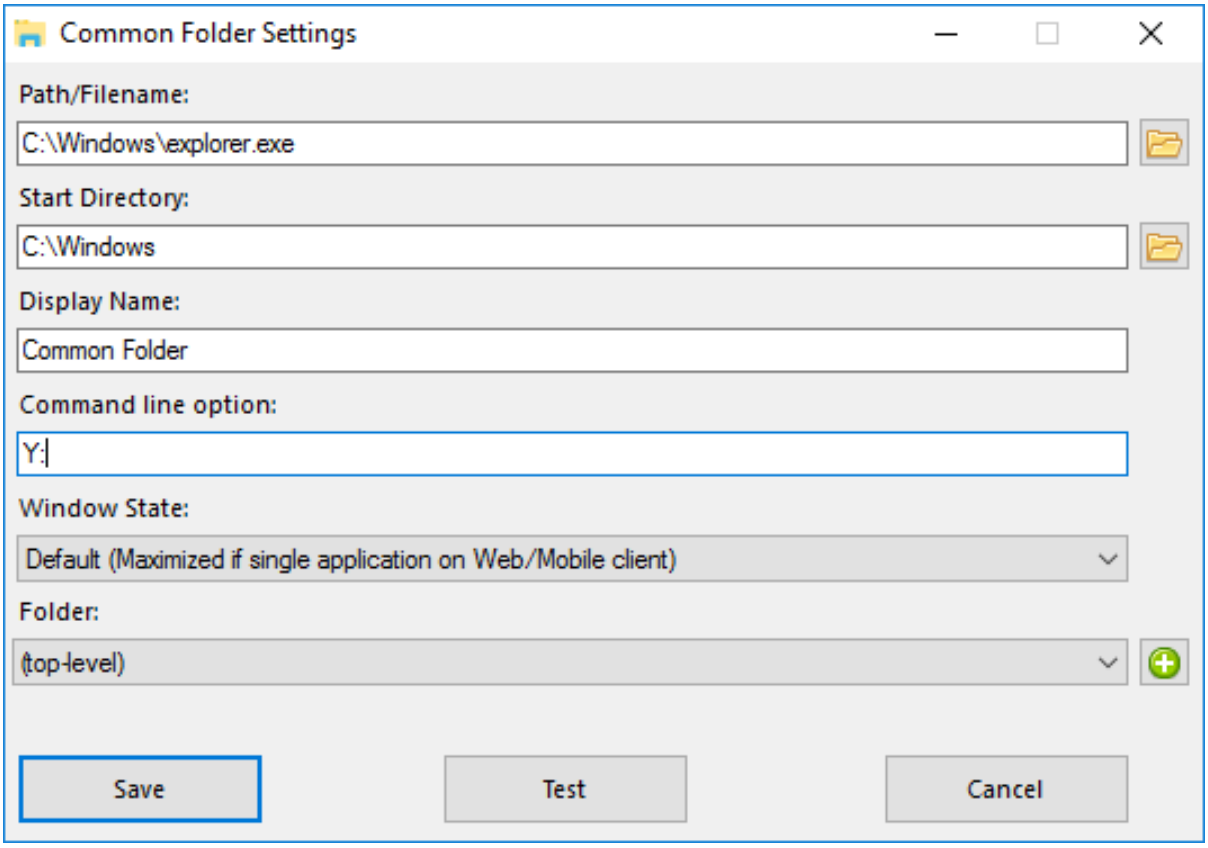


Then, click on "Show Files" button on the Logon Properties window and copy your logon.bat script into the path given by the Policy Editor, i.e.: "C:\Windows\System32\GroupPolicy\User\Scripts\Logon"



- You can copy this logon.bat file in C:\ProgramData if you want this script to be executed for all of your users.
- If you need a specific logon script for each user then copy the script in C: \Users\Username\AppData\Roaming

Now how do we make this Y drive appear in the user session? There many ways to achieve this. You can create a new application within the admin tool and assign it to your users, doing so the shortcut will appear in the session:




CommonFolder

If you connect to a session with mstsc.exe, don’t forget to go to the options menu, and on the Local Resources tab, under Local devices and resources, click on “More”, then check the box “Drives”.

If you want to assign this script only for non-admin users, follow this tutorial.

If you want to secure the access of a folder, see our documentation to publish a secured folder.

Logon Ticket and Load-Balancing

Logon Ticket creation on the Gateway Server

You can create a logon ticket on the gateway with:

/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

But it will only allow you to connect on the gateway server itself.

Logon Ticket creation on an Application Server

You can also create a logon ticket on a reverse-proxified application server with:

/~~srv4/socket.io/LPW?WinUser=DOMAIN\LOGIN&WinPassword=PASSWORD

(assuming ~~srv4 is the internal name of the application server as configured in TSplus reverse-proxy)

But it will only allow you to connect on this specific application server.

Logon Ticket and Load-Balancing

So if you want to use logon tickets and load-balancing, you might want to do an additional HTTP request first:

https://your-gateway-server.com/cgi-bin/hb.exe?action=lb&l=LOGIN&d=DOMAIN&t=TIMESTAMP

This will return an answer like this one:

loadbalancing-on|APP SERVER 4|your-gateway-server.com/~~srv4|https|443|

You can parse this answer to retrieve the application server on which TSplus Load-Balancer would recommend you to connect this specific user.

i.e. it will recommend the less-loaded server on your TSplus farm, if sticky sessions are enabled on your TSplus gateway, it will take existing active sessions into account, etc.

You can then create a logon ticket on this specific application server and connect to user to it.

This is precisely the http request done on TSplus Web Portal logon page.

Using a Logon Ticket to Open a User Session

Now that you have a valid logon ticket, you can open a user session using this ticket by opening a browser window to this URL:

https://your-gateway-server.com/~~srv4/software/html5.html?user=*xxxxxxxx

where “xxxxxxxx” is the logon ticket.

Long Term Support versions

Customers who have subscribed to TSplus Support & Update Services and are not interested in TSplus latest features and improvements can install a TSplus LTS (Long Term Support) version.

TSplus LTS (Long Term Support) version extends the period of software maintenance; it also reduce the frequency of software updates to reduce the risk, expense, and disruption of software deployment, while promoting the dependability of the software.

Moreover, TSplus LTS (Long Term Support) does not receive any new features.

TSplus lifecycle

TSplus standard versions are published quite often and the latest release is always the best solution available to our customers: all known bugs are fixed and new features are available very often.

A new major TSplus version is released at the start of every year.

Starting January 2019, TSplus is also available in a Long Term Support version, named “LTS”. Every new major version, TSplus will publish a stable LTS version of the previous version which will be supported for 2 years.

Benefits and Limitations of TSplus LTS

TSplus LTS has several benefits:

- No updates except for security fixes and Windows updates compatibility
- No changes in behavior and no changes in features when you update
- Less risk when updating between two minor versions of a given LTS
- Supported for at least 2 years

TSplus LTS also has limitations and constraints:

- Customer must purchase Support & Update Services (a license cannot be activate without active Support & Update Services)
- No new features at all (compared to TSplus standard version which constantly receives a lot of

updates and new features)

We recommend our customers to use TSplus standard version to benefit from our state-of-the-art solution.

TSplus LTS Links

TSplus LTS 18 (supported from 2026-01 to 2028-01):

- Changelog
- Setup (to install TSplus on a new server)
- UpdateRelease (to update an existing TSplus installation)
- LTS18 Documentation

TSplus LTS 17 (supported from 2025-01 to 2027-01):

- Changelog
- Setup (to install TSplus on a new server)
- UpdateRelease (to update an existing TSplus installation)
- LTS17 Documentation

TSplus LTS 16 (supported from 2024-01 to 2026-01): **End Of Support**

TSplus LTS 15 (supported from 2023-01 to 2025-01): **End Of Support**

TSplus LTS 14 (supported from 2021-12 to 2023-12): **End Of Support**

TSplus LTS 12 (supported from 2019-12 to 2022-12): **End Of Support**

TSplus LTS 11 (supported from 2018-12 to 2021-12): **End Of Support**

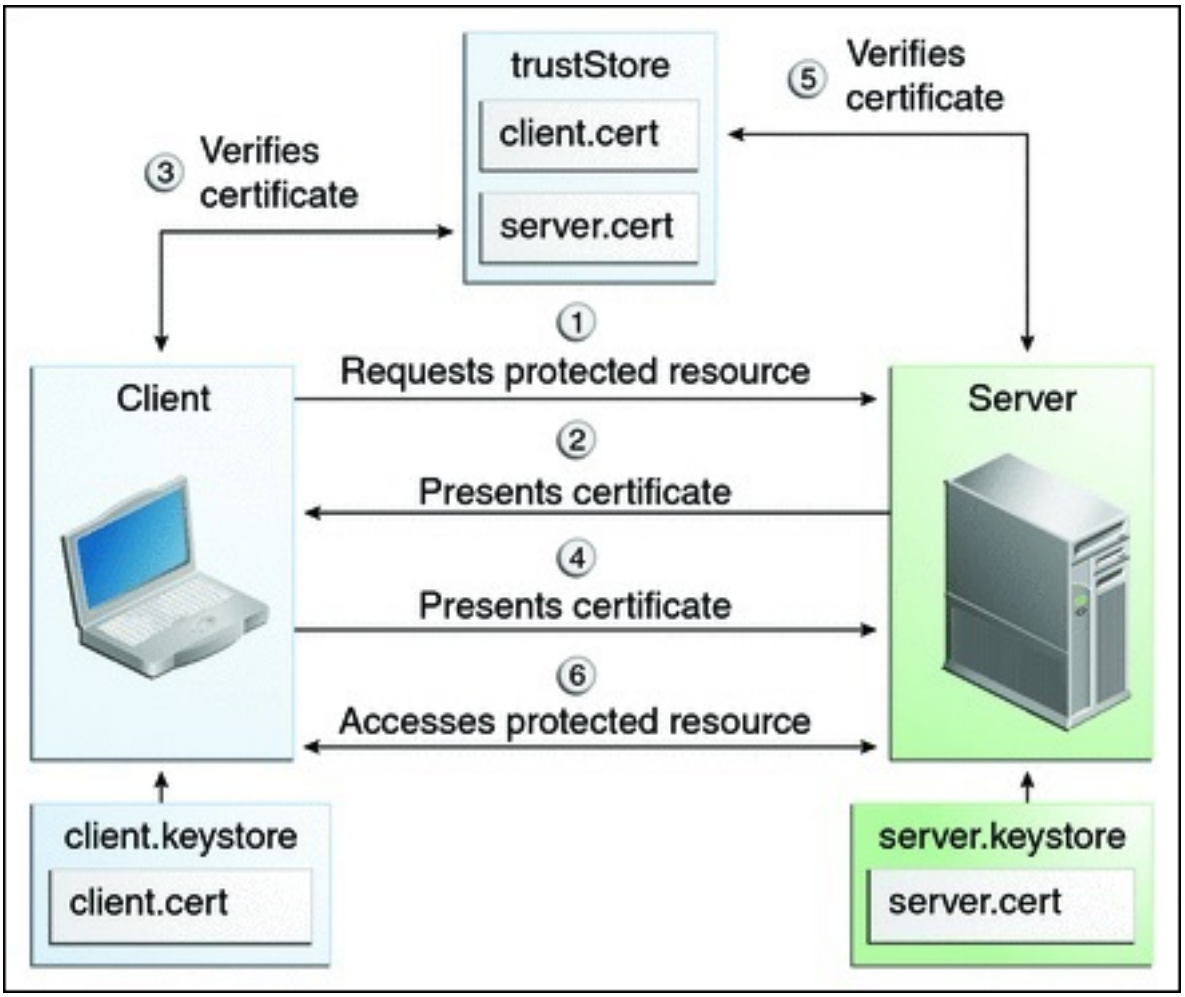
Activating Mutual SSL Authentication

What is Mutual Authentication?

Many people are expecting extra security and Mutual authentication is already supported in Terminal Service Plus. It is usually implemented by banks or government bodies.

To understand what that is, we can compare it to a standard SSL process where you will add extra check to verify if the user web browser is allowing SSL connection. You know what your server-side SSL certificate is. Imagine that the certificate is imported into the web browser to ensure that this specific web browser is trusted to create a connection. In the first step of communication, the web browser is acting as a client and in the second step, it is the reverse. At the end both side, client web browser and web server, have accepted the authority and the connection can start.

A more complete definition: Mutual SSL authentication or certificate-based mutual authentication refers to two parties authenticating each other through verifying the provided digital certificate so that both parties are assured of the others' identity. In technology terms, it refers to a client (web browser or client application) authenticating themselves to a server (website or server application) and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs). Because authentication relies on digital certificates, certification authorities such as Verisign or Microsoft Certificate Server are an important part of the mutual authentication process.



Activating it on TSplus

TSplus built-in web server enables to setup mutual authentication.

To enable the mutual authentication follow this process:

You will have to install the latest Java Development Kit (JDK), available from http://java.com > Downloads > JDK.

1. Create and edit with Notepad the following file: C:\Program Files (x86)\TSplus\Clients\webserver\settings.bin

Add these 3 lines:

disable_http_only=true disable_print_polling=true force_mutual_auth_on_https=true

2. Remove cert.jks

In “C:\Program Files (x86)\TSplus\Clients\webserver” you will see the file cert.jks Copy it in “C:\Program Files (x86)\TSplus\Clients” Remove “C:\Program Files (x86)\TSplus\Clients\webserver\cert.jks”

3. Create the batch file

In ‘C:\Program Files (x86)\TSplus\Clients’ create a batch file, for example “createcertuser.bat” with these settings:

@rem uncomment next line, if you want to generate new self signed 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

This will automatically import the cert key pair from the web browser into “cert.jks” after creating its browsers key pair.

4. Restore the new created the modified “cert.jks”

Copy “C:\Program Files (x86)\TSplus\Clients\cert.jks” into “C:\Program Files (x86)\TSplus\Clients\webserver” and restart the Web Servers.

5. Certificate import and Testing

The provided batch example should have generated a test file “BrowserUser1.p12”. When you will open the HTTPS address, you will get a security message and you will be unable to access Web Server pages. With Chrome or IE, you can click on this ‘BrowserUser1.p12’ file to import the certificate into Windows default key store. With FireFox, you have to go to Settings and to import this “BrowserUser1.p12” file under your certificate folder.

As soon as you have properly imported it, you will be able to access the HTTPS address.

The administrator can create a separate key pair file for each user.

For example:

forBrowserUser1.p12 forBrowserUser2.p12 forBrowserUser3.p12

And he can export theses certificates into cert.jks. If he wants to disable the access to one user he will just have to delete this user from “cert.jks”. Doing so, the user will lose his authorization and will not be able to access the web server anymore.

This mutual authentication only affects the HTTPS connections and HTTP connection will be prohibited with the command line: settings.bin>disable_http_only=true

Open Files on Client Side

Overview

This feature is a powerful one. It allows to open documents located on the server on the client side depending on its file extension.

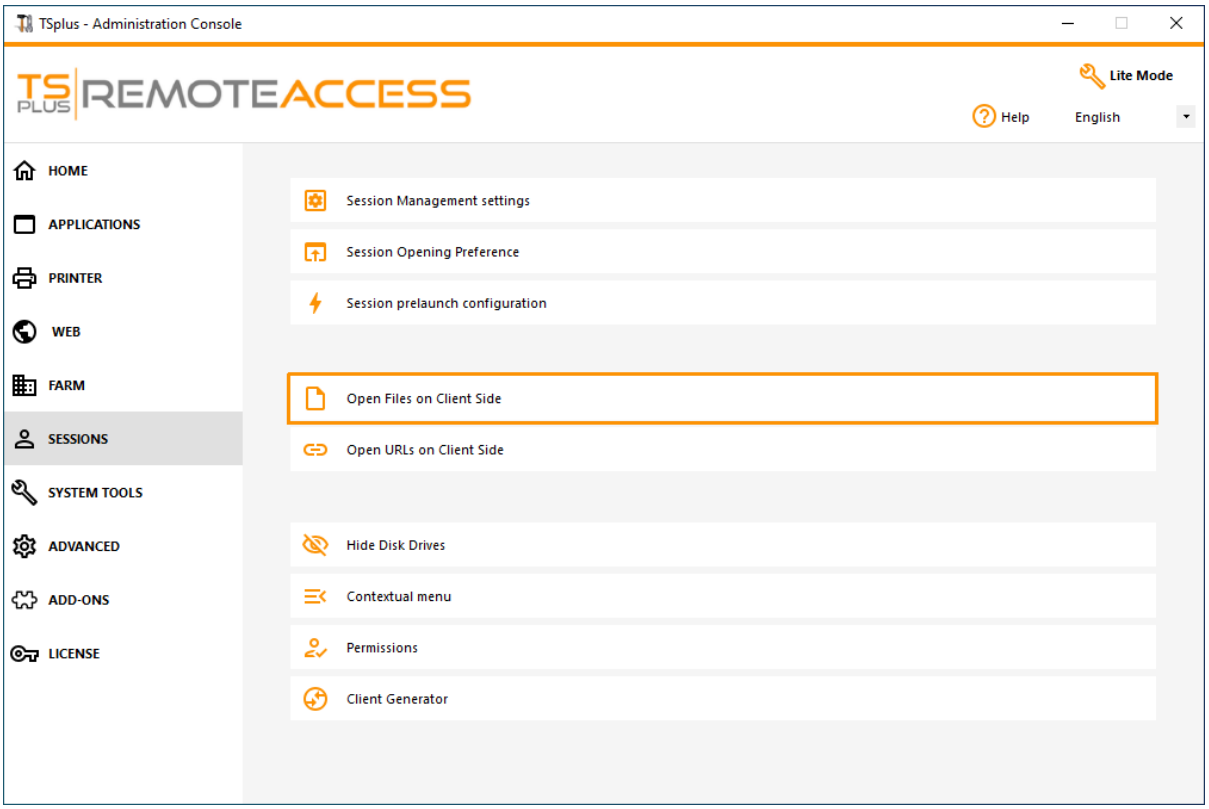
For instance, you can open a Microsoft Office Word document without having Office installed on your server.

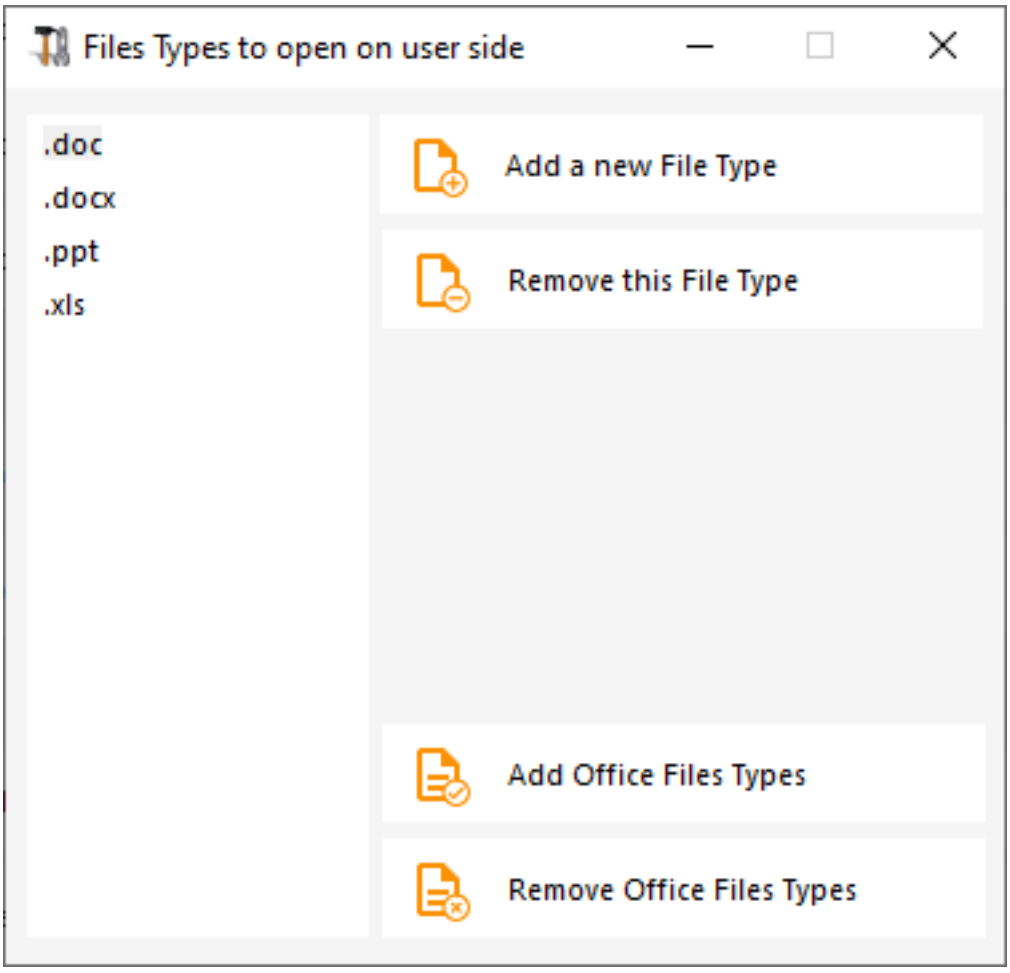
The .docx (or .xlsx) document is automatically uploaded on the user side where the local Office will be used to open it.

If you are hosting your application on a Cloud server and if your application is generating an Excel, Access or Word document, this feature prevents to care about Office licenses on the server.

Configuring a File Type to open on the client side

The tile “Open Files on Client Side” is located in the “Sessions - Settings” tab of the AdminTool. Click on it to display the configuration window:





The button “Add a new File Type” allows you to add an extension (such as “.docx” for Microsoft Office Word 2007-2010) to the list.

All the files having an extension in this list will then be opened on client side, provided that

you use one of Terminal Service Plus connection clients:

- Any generated Terminal Service Plus Client (RemoteApp or RDP)
- Any Windows connection from the Terminal Service Plus Web Portal
- Any HTML5 connection from Terminal Service Plus Web Portal

Warning: this feature is not supported for:

- Any RDP client (mstsc for example)

Troubleshooting

If you have configured a file type to open on client side, and it is not working (i.e. the file is still opened on its own computer), then we advise you to check the “Open With” list in Windows context-menu:

- right-click on the file.
- click on the “Open With” menu item.
- if there is more than one application in this list, click on “Choose default program” and select “OpenOnClient.exe”.

This Terminal Service Plus great tool applies its configuration to all users using the computer, however please keep in mind the following rules:

- Windows allows each user to change this default opening program with another program of its choice.
- Using HTML5 connection client, the file will be downloaded and managed by the local browser. Some browsers treat some file types in specific ways, so browser’s settings should also be checked twice.

These rules explain most of the issues when using the Open On Client feature, that is why we advise you to start by checking the default program:

- for the logged user on the server
- for the user on the client
- for the browser on the client (when using HTML5)

Open URLs on Client Side

Overview

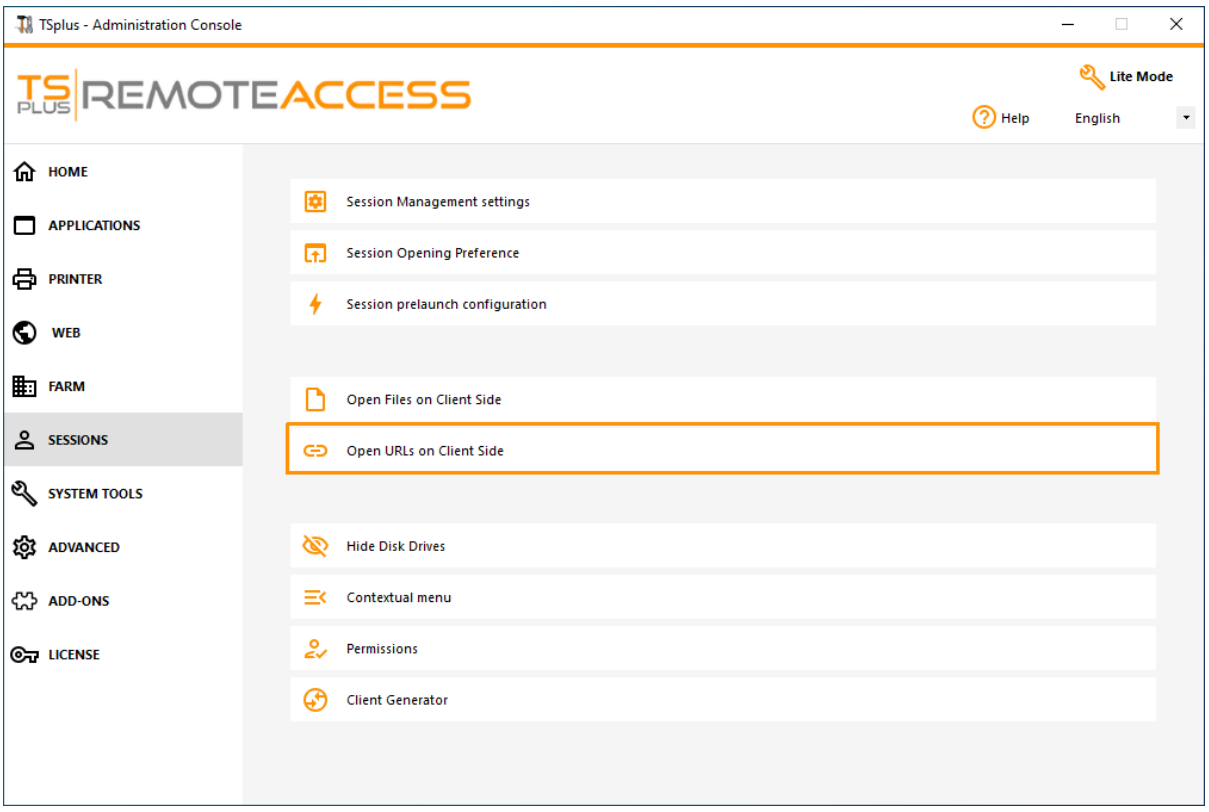
This feature is a powerful one. It allows to open on the client side every websites links and websites shortcuts located on the server.

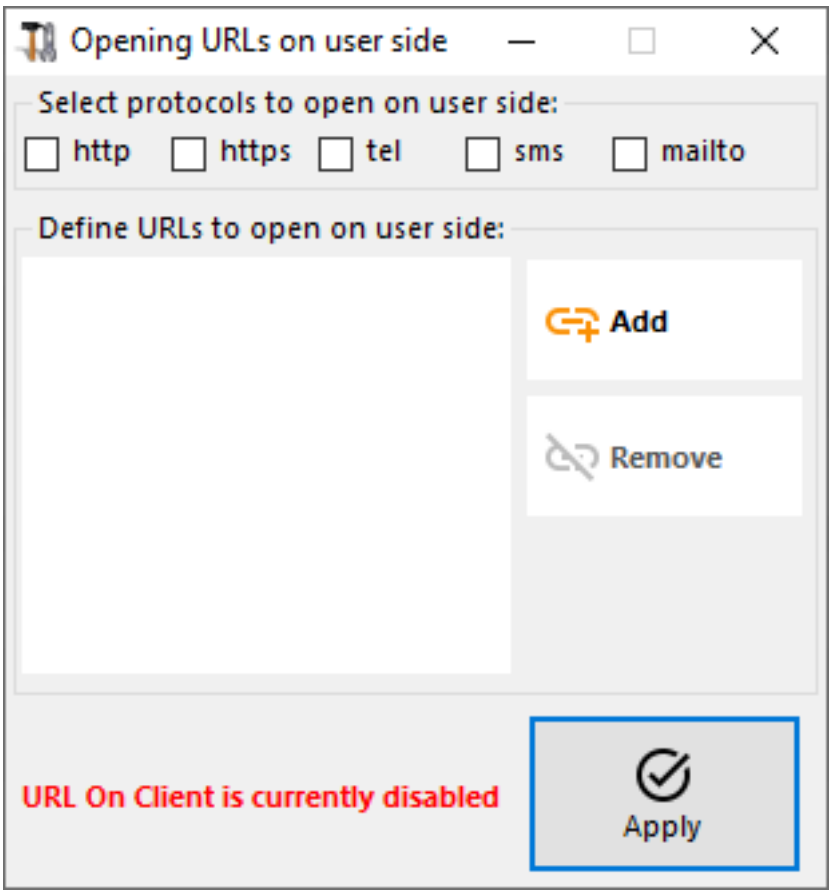
For instance, you can open YouTube videos directly on the client, thus saving lots of bandwidth and CPU power on your server.

The web address (URL) is automatically transferred on the user side where the local default browser will be used to open it.

Enabling this Feature on a server

The “Open URLs on Client Side” tile is located in the “Sessions - Settings” tab of the AdminTool. Click on it to display the configuration window:





Http and https protocols boxes are not ticked by default.
You can also activate tel, sms and mailto protocols by ticking the corresponding boxes.

Then click on the “Apply” button, which allows you to activate this feature for all users on the server.

In order to fully enable this feature, every user will have to restart its session (logoff then login) before they can use this feature.

All the web links and shortcuts will then be opened on client side, provided that you use one of Terminal Service Plus connection clients:

- Any generated Terminal Service Plus Client (RemoteApp or RDP)
- Any Windows connection from the Terminal Service Plus Web Portal
- Any HTML5 connection from Terminal Service Plus Web Portal.

Warning: this feature is not supported for:

- Any RDP client (mstsc for example).

Web Browser behaviour (Web Portal):

Some web browsers —particularly on iOS devices— do not allow links to be opened automatically from our application. In these cases, a clickable link is displayed so users can

manually access the intended destination.



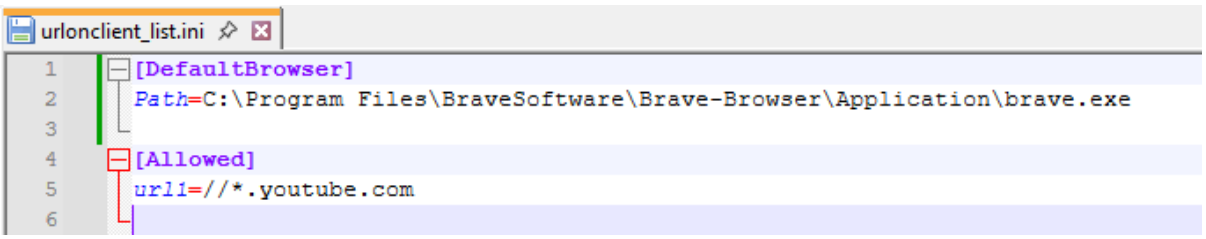
Changing the server default web browser

All URL's that are not defined to be opened on client side will continue to be opened on server side, using Microsoft Edge or Internet Explorer. If you want to change the default web browser used on the server side, you need to edit the configuration file **urlonclient_list.ini** located in the TSPlus installation folder.

The exact location (depending on your exact installation path) should be : "C:\Program Files (x86)\TSplus\UserDesktop\files\urlonclient_list.ini".

The you need to add a new section "DefaultBrowser" in the file, and an entry "Path" with value the path of the web browser you want. Like so :

[DefaultBrowser]
Path=C:\Path\To\Your\Favorite\WebBrowser.exe



Setting default browser to Brave

☐ **If you have replaced firefox.exe by c:\wsession\URLonClient.exe**

and you want Firefox to be your default web browser on server side :

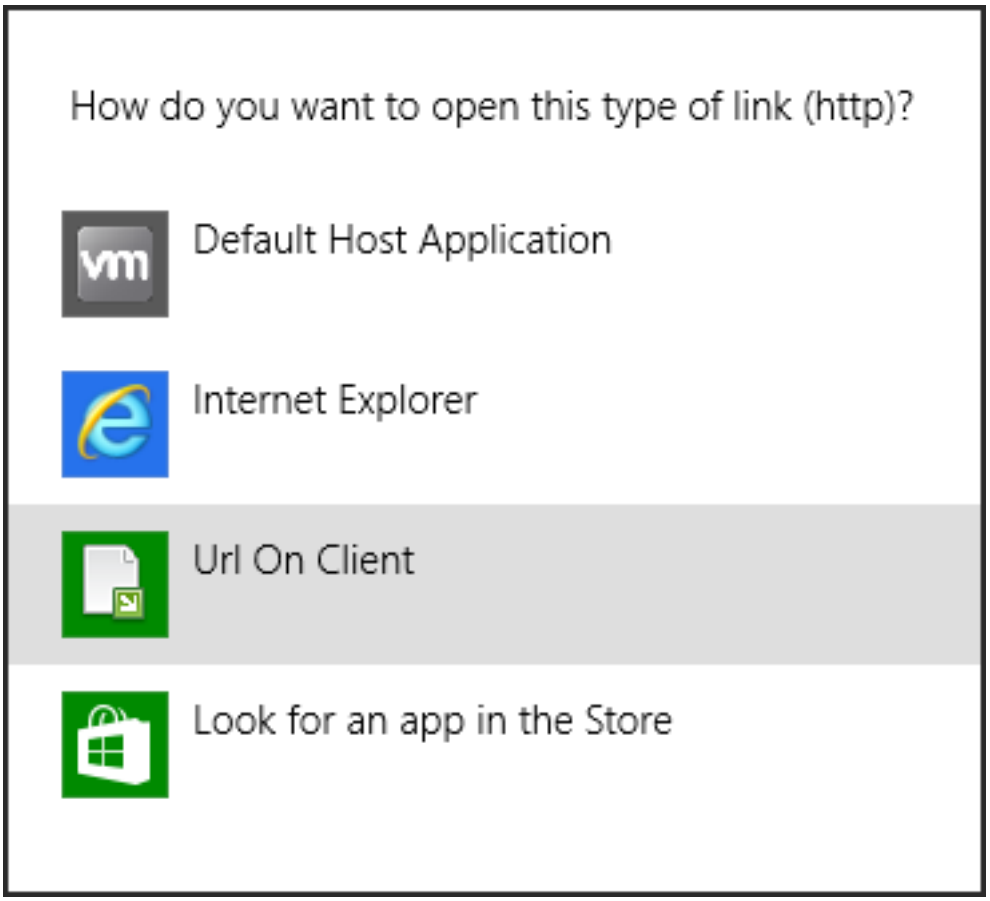
- Rename the old firefox.exe file into firefox-real.exe.
- use the new executable name in the **urlonclient_list.ini** file :

[DefaultBrowser]
Path=C:\Program Files\Mozilla Firefox\firefox-real.exe

Windows 8 and 8.1

Starting with Windows 8, Microsoft has forbidden automatic change of user's default browser.

This is why, once the feature is activated on the server, every user will have to choose 'Url On Client' when asked for a default browser.



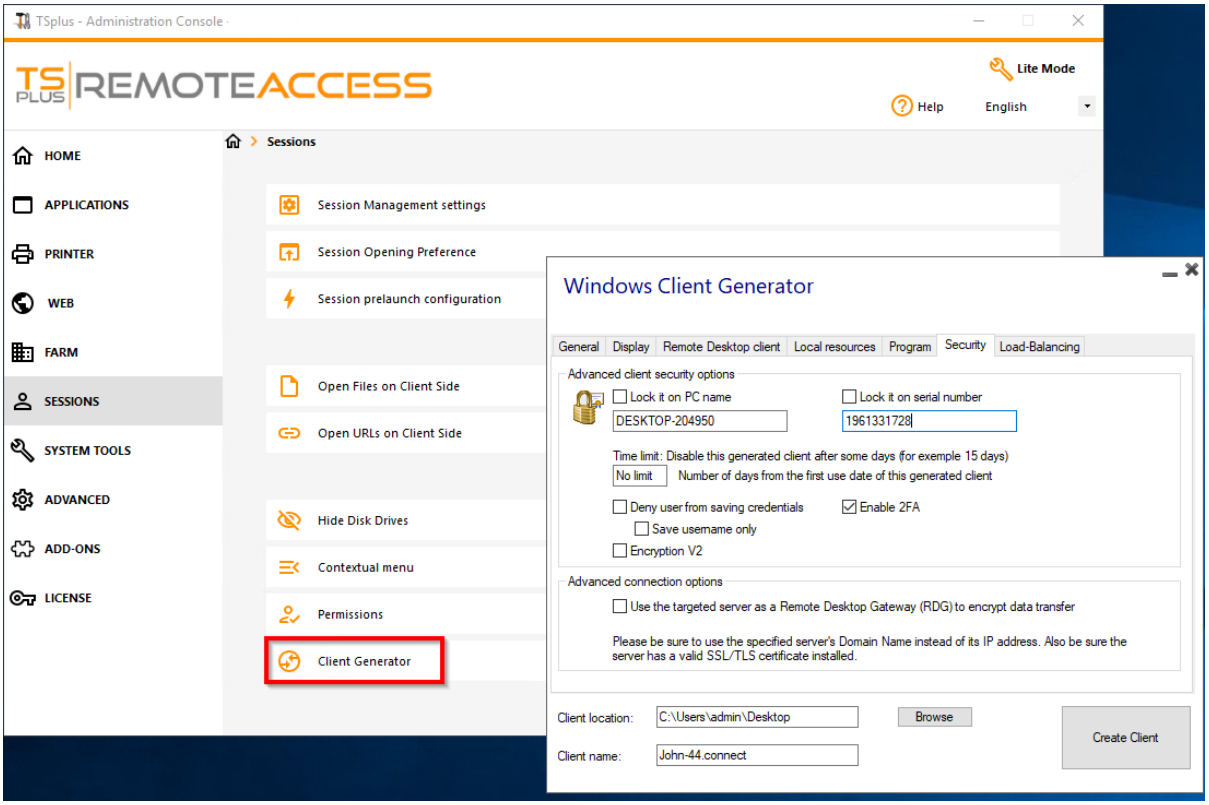
This window will only be displayed the first time a user opens a web link. Unfortunately, this is Microsoft Windows policy and we are not aware of any workaround.

Portable Client Generator

TSplus creates by default an icon for the Portable Client Generator:



It can also be accessed in the Sessions tab of the AdminTool:



It enables you to create 2 types of connection clients which can be copied to the users' Desktop or onto a USB stick for portable use.

Note: Connection Clients are not compatible with Mac computers.

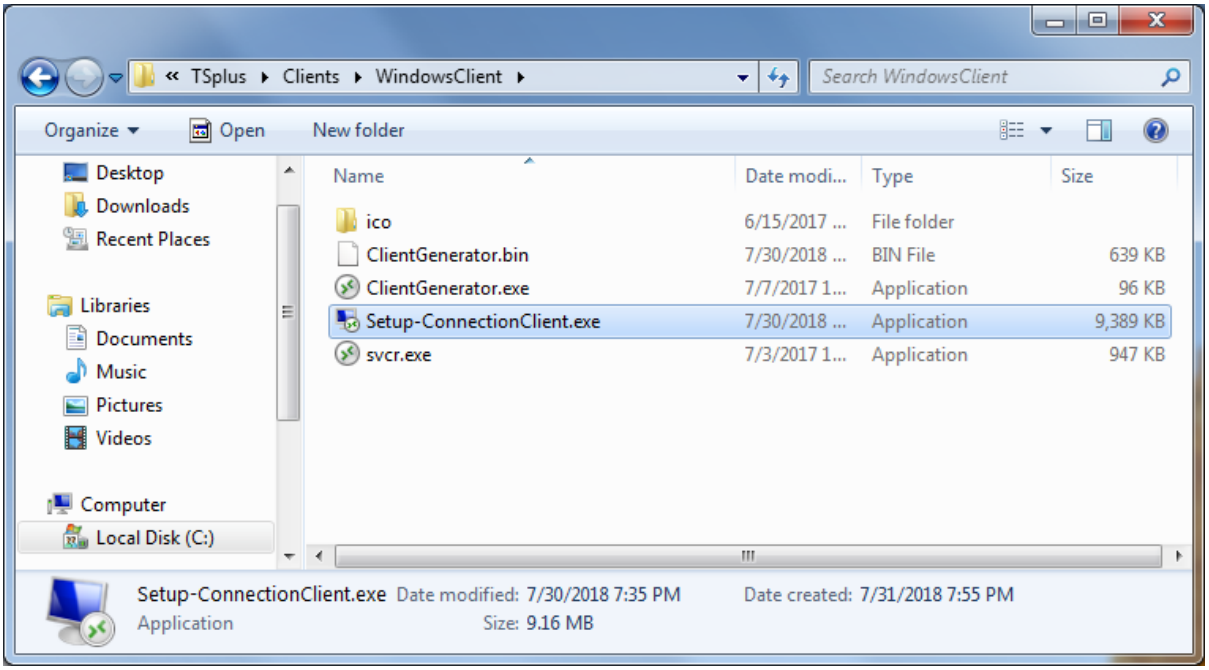
Since TSplus 11.40 release, the client generator has been redesigned to be numerically signed and to avoid false/positive antiviruses reactions.

Instead of a ".exe" program, the new Client Generator is creating a flat encrypted file with the extension ".connect":

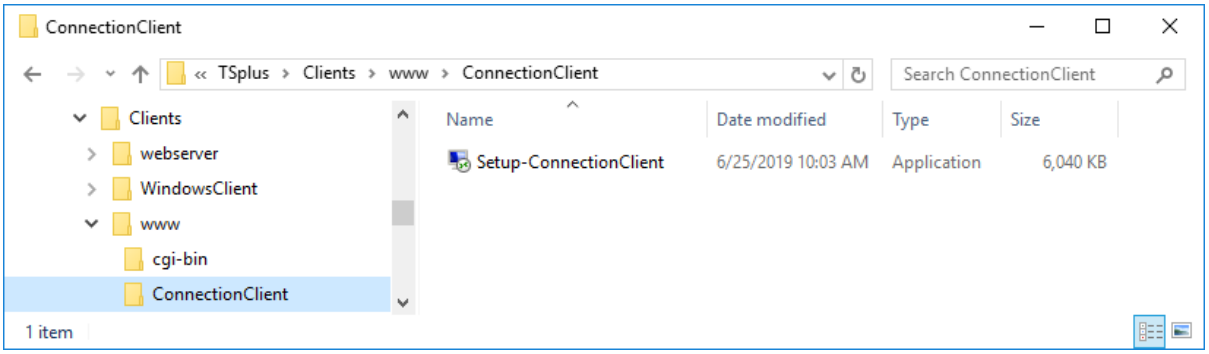


Pre-requisite on Client Side

On client side, each user will have to run a signed program named "Setup-ConnectionClient.exe" as a pre-requisite. This program is available on your server, in the TSplus program folder: TSplus\Clients\WindowsClient:



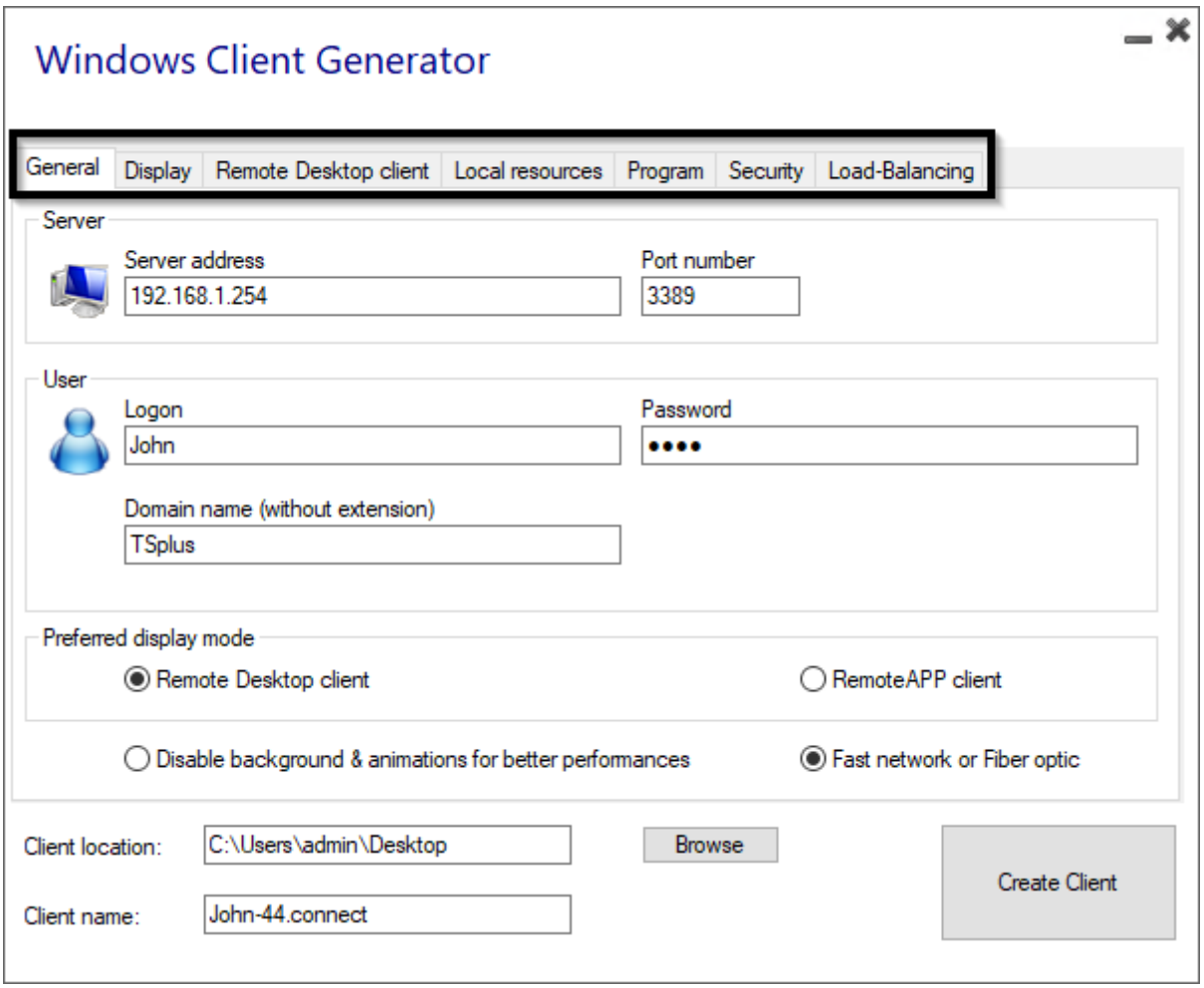
or on the TSplus\Clients\www folder:



or by downloading it.

Detailed Overview

Click on **a tab** to go to the corresponding information:



When you launch the client generator, the first tab displayed is the general tab, Here you will find all of the essential connection settings that you need to get you started.

- **Server Address:** Enter the IP address of the server you would like the client to connect to.
- **Port Number:** Enter the server port number. The default is 3389.
- **Username and Password:** If you enter a username and password, the client program will not ask the user to retype it at each session.

To reset this logon/password saving, you must create and edit a shortcut of the Remote Desktop Client and add the -reset on switch at the end of the target field.

Credentials

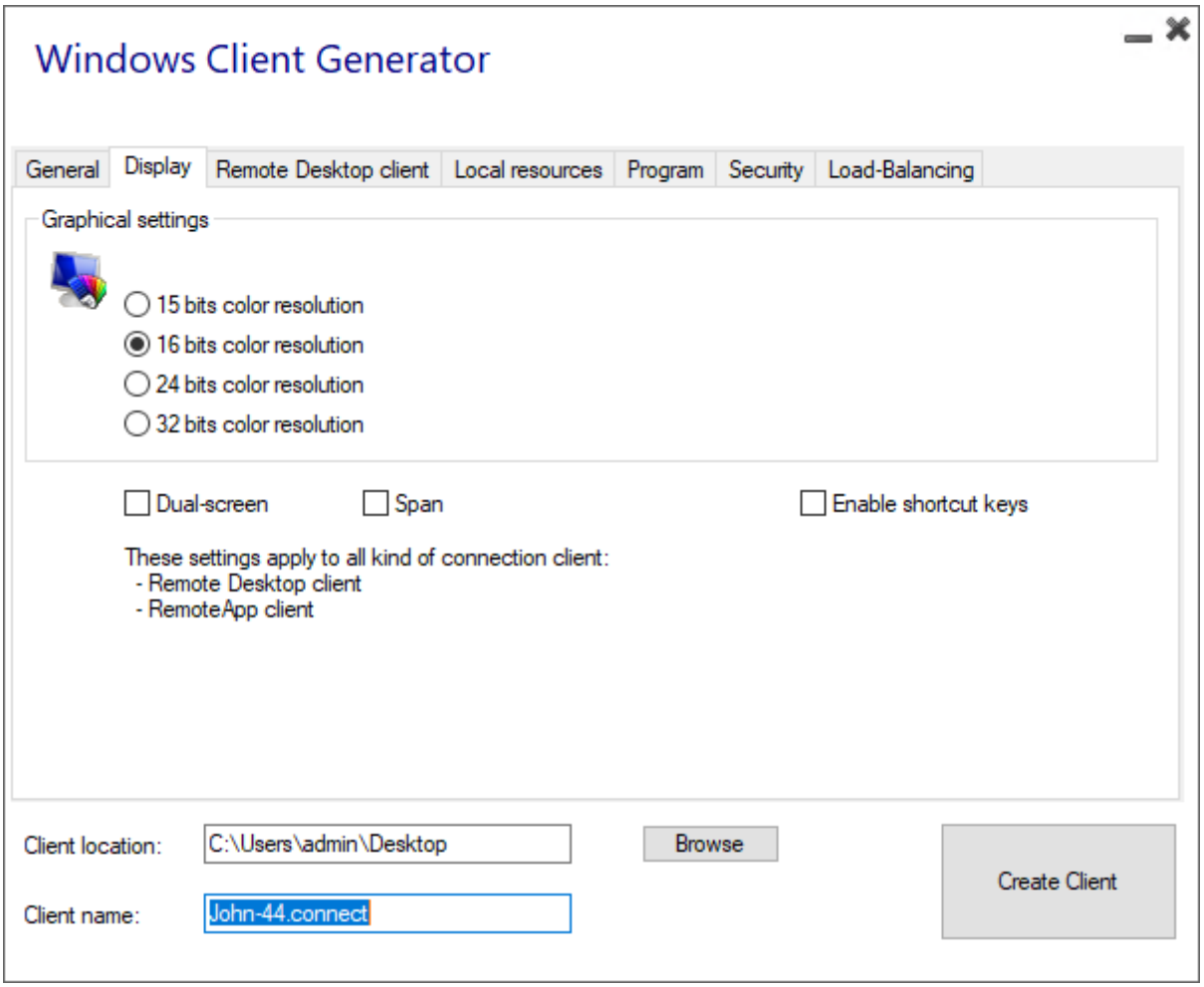
- If you don’t want to save credentials, enter “nosavecredential” in the logon field of the Portable Client Generator.
- If you don’t want to display the logon window with the user name, password and domain name, simply enter “nopassword” on the password field.
- If you want to enable autologon, enter *SSO in the username field, the client program will just ask for username and password during the very first connection. It will save this information on the user’s workstation so that the user doesn’t have to identify himself ever again.
- If you want the current local user’s name to be displayed as a logon for the session, enter **, or %USERNAME% in the logon field.

- **Domain name:** Enter a domain name if any.
- **Preferred Display Mode:** You can choose your preferred Display Mode from the following options:
  - The Classic Remote Desktop, displaying your remote session environment.
  - The Microsoft RemoteApp connection client, to display your remote applications as if they were installed locally. It has a better graphic performance over minimized applications.

- **Network speed**: You can choose between two options depending on your network speed:
  - Disable background display & graphic animations for low speed networks.
  -

Enable background display and graphic animations for fiber optic or fast network.

- **Client location:** Define the location of your generated client.
- **Client name:** You can name your client as you wish.

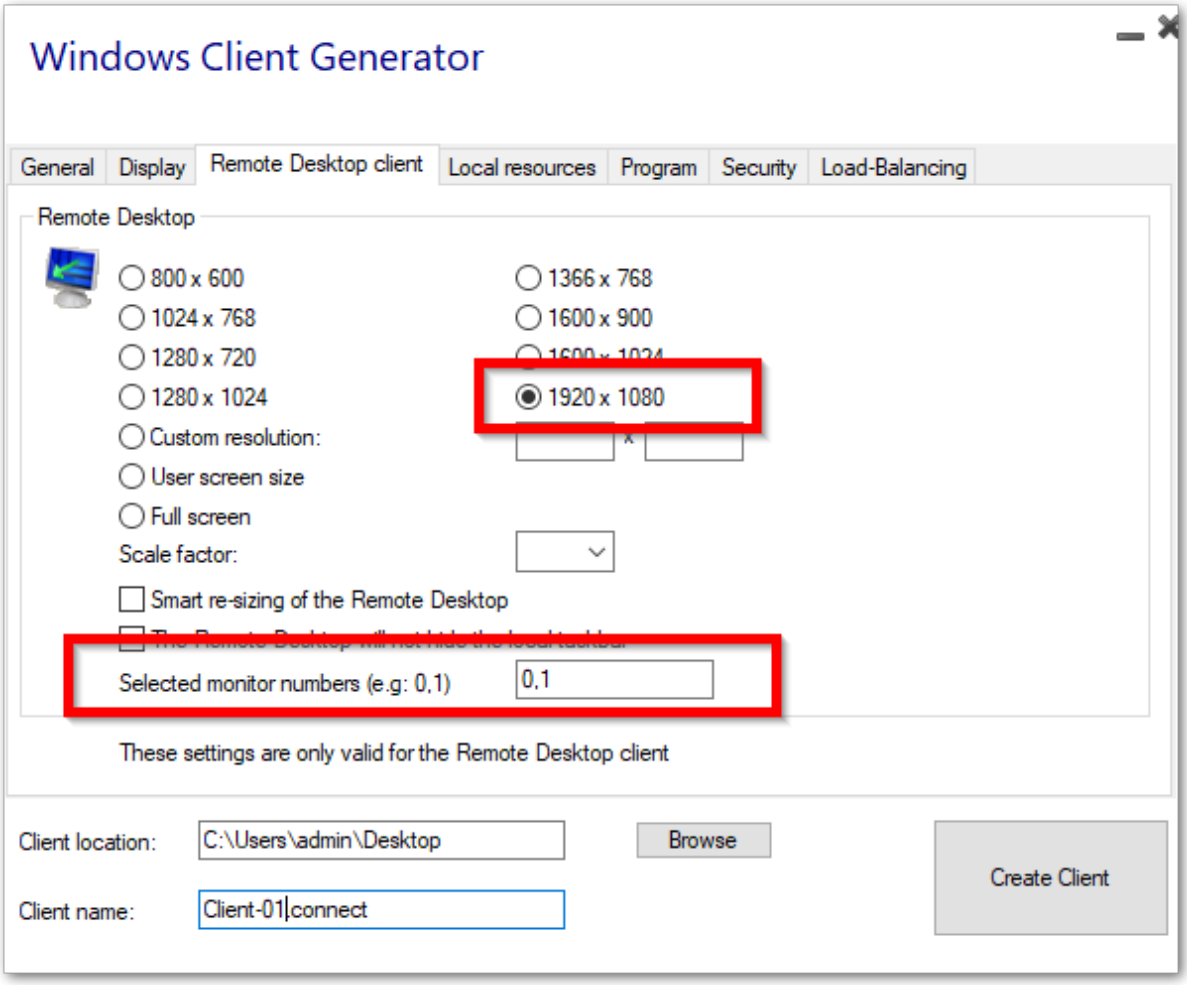


On this tab, you can change the color and the session screen resolution.

You can also adapt your session for dual-screens, with or without span. The span option allows you to stretch your session across both screens.

You can allow the use of the TAB key in the session.

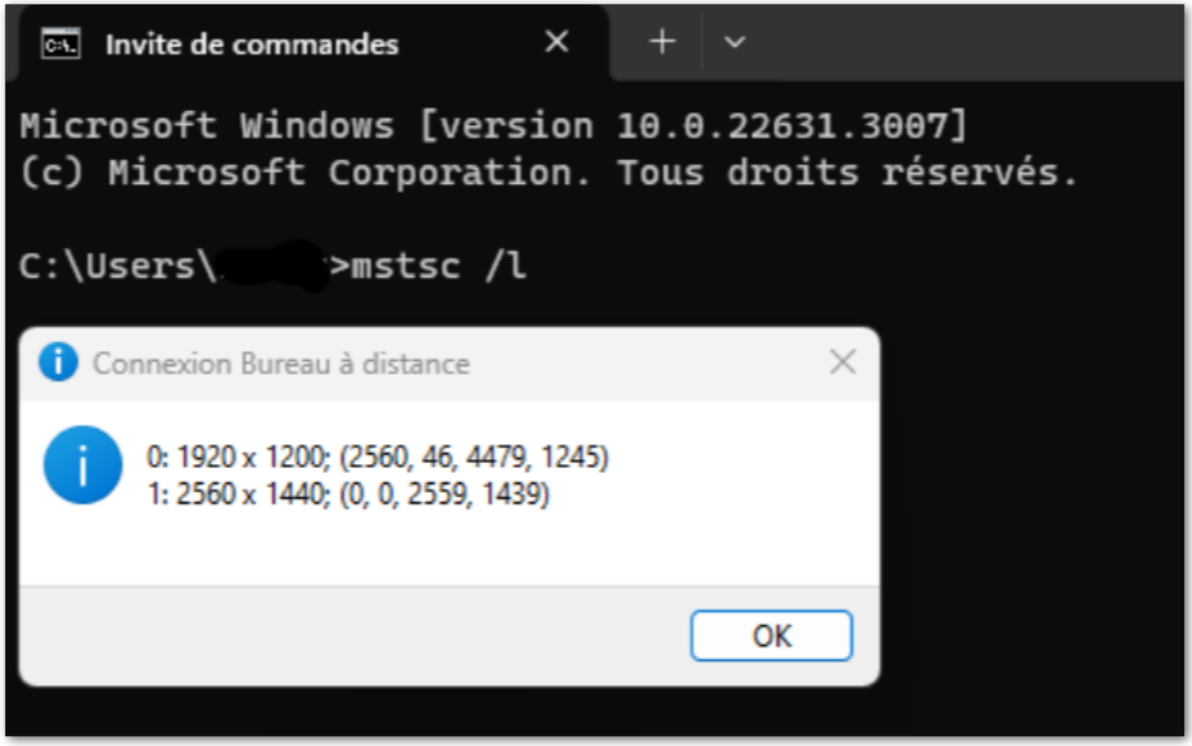
On this tab, you can choose which resolution you want to enable for the user:



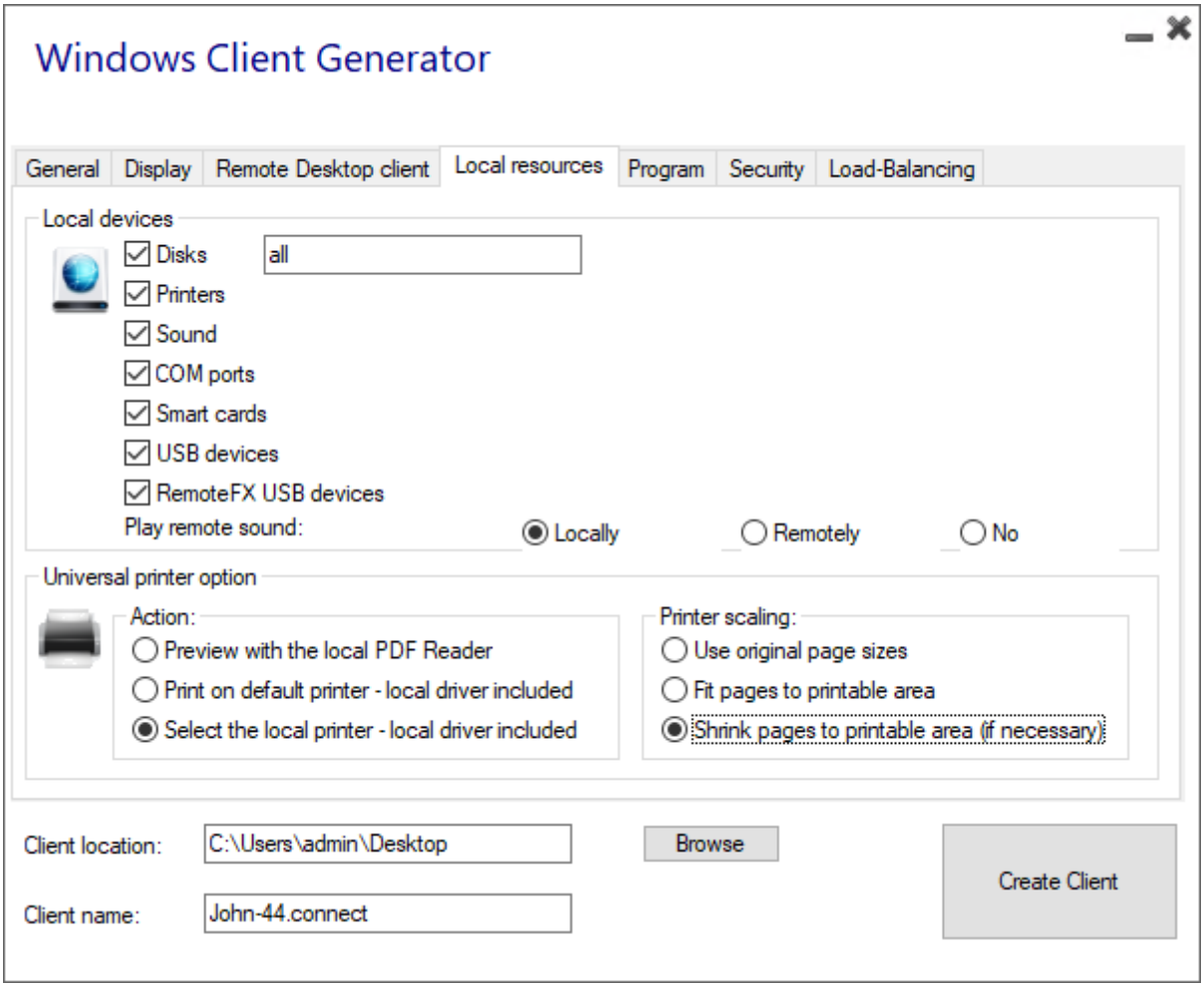
You can check the boxes to enable smart-sizing of the Remote Desktop, and if you want the Remote Desktop not to hide or overlap the local taskbar.

Screen selection option

This allows you to indicate the monitors you want to use for the RDP session. The field must be filled with the list of screen numbers to use (separated by a comma, a space or a semicolon)



To identify the screen numbers, simply run the command **“mstsc /l”**



The local resources tab gathers all the devices that you may redirect in your remote session.

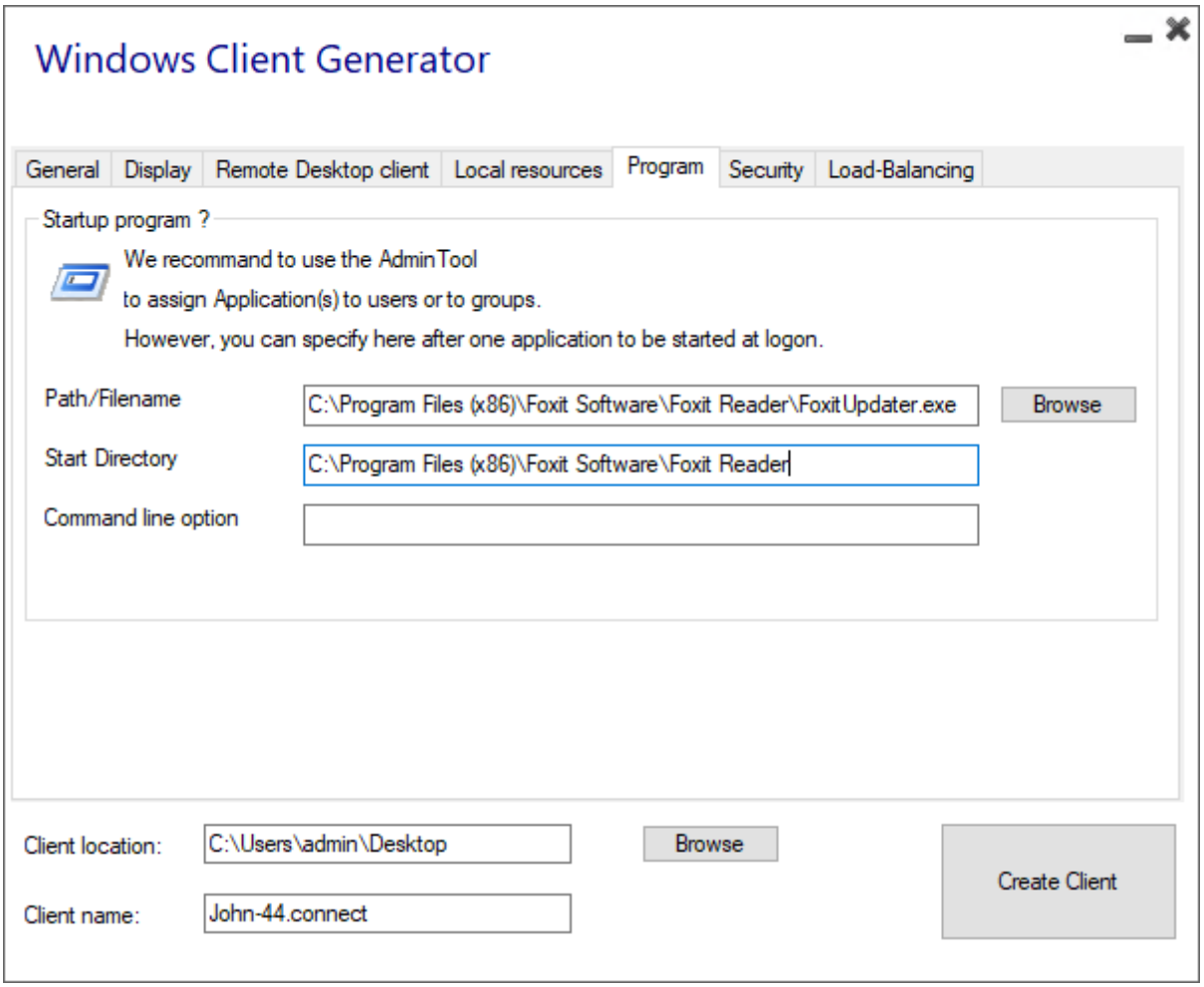
The editable field next to the **disks** box allows to specify which disks are available in the remote session. You just have to separate each letter of disk (C :, E: …) by a comma. When the disks box is ticked and no disk is specified, all the disks are included in the remote session.

Printers correspond to LPT ports, and COM Ports correspond to Serial Ports. Since TSplus 11.50 version, these local devices are selected by default.

Below, you can choose your option for printing, with the universal printer:

- **Local PDF Reader preview:** The document will be rendered as a PDF and the local Acrobat Reader will open the file. The user can print it, or save a copy on his local disk drive.
- **Print on the user's default printer:** the document will be automatically pushed to the user's default printer (the local print driver is included in the TSplus connection client).
- **Select a local printer:** The user can select one of his local printers (the local print driver is included in the TSplus connection client).

If you do not have a PDF Reader installed on your machine, we recommend the use of Foxit Reader.



You can set a startup application via the Portable Client Generator, and specify its path, directory and parameters, since the 11.30 release.

However, we recommend you to use the AdminTool to assign the desired applications.

TSplus offers two extra layers of physical security to keep your users' connections safe.

The connection can be locked to the ID of a USB key, locked to a computer name, or you can use both layers of security simultaneously.

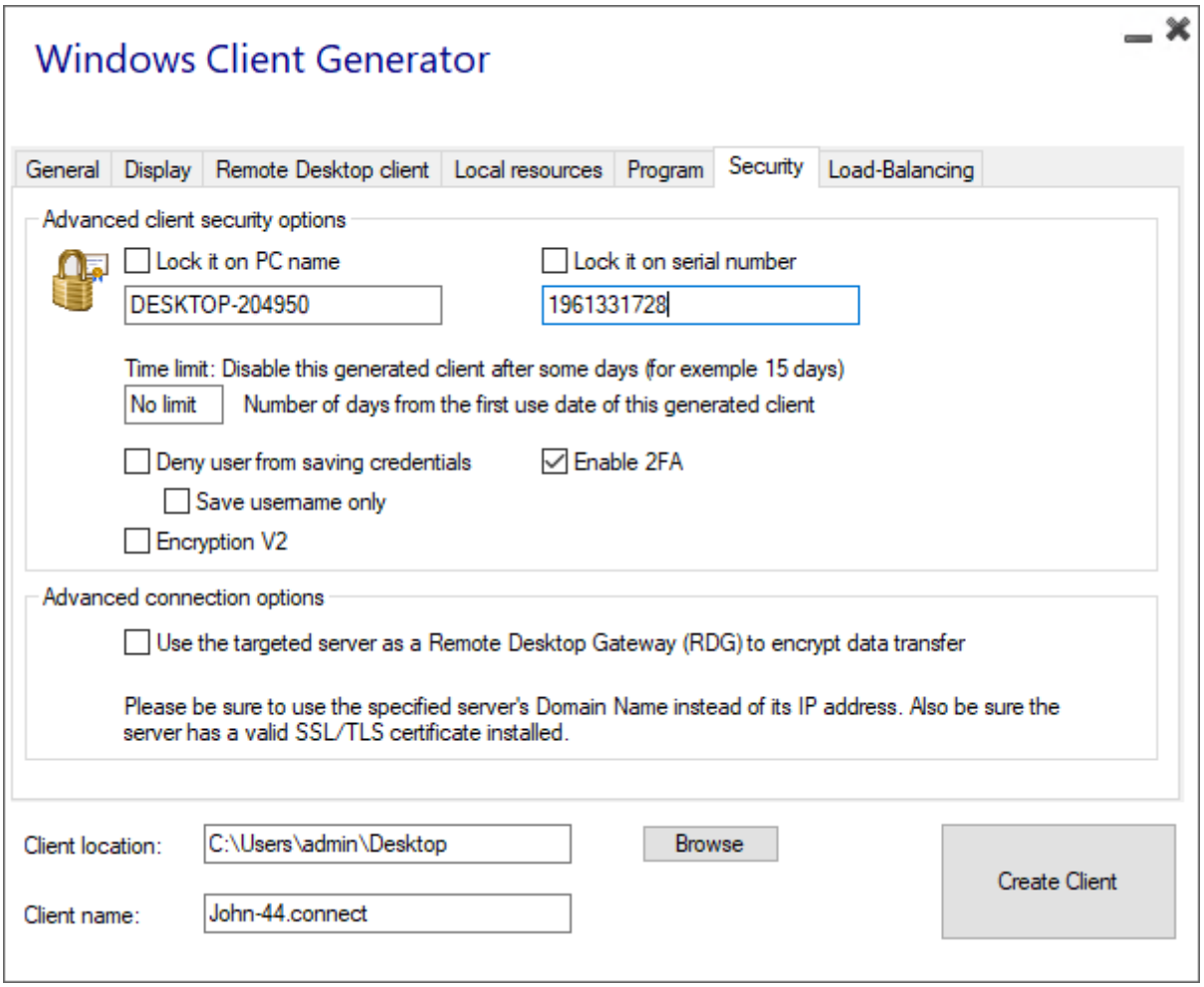
Advanced client security option

- **If locked to a USB key**, the user can initiate a connection from any qualifying windows computer by inserting the USB key and using the connection program placed there by the administrator.
- **If locked to a computer name**, the user can only successfully connect from the computer whose name has been registered with the server for that user's portable client connection. If both security options are used, the user is limited to connecting from their specific device and only if the correct pre-configured USB key is in place.

In order to lock a connection client onto a USB key you can do so by copying the client generator located in : C:\Program Files (x86)\TSplus\Clients\WindowsClient

Now double click on the client generator and check the lock on serial number box located on the security tab. Once it is done, you can delete the client generator from the USB key.

The newly generated connection client will be placed on the desktop, don't forget to copy it back to the USB key! You can delete the client generator that you copied on the USB key afterwards.



- You can define the **time limit** from the first use date of a generated client by entering the value on the time limit box. (which is by default set to “no limit”).

- Boxes below enable you to:

  - Not display the ability to save credentials for a generated client.
    - Save username only.
    - Use Encryption V2.

Support for two-factor authentication

The client generator supports **two-factor authentication** since version 15.30.3.15. Two-factor authentication support also requires a **Mobile Web edition or greater**.

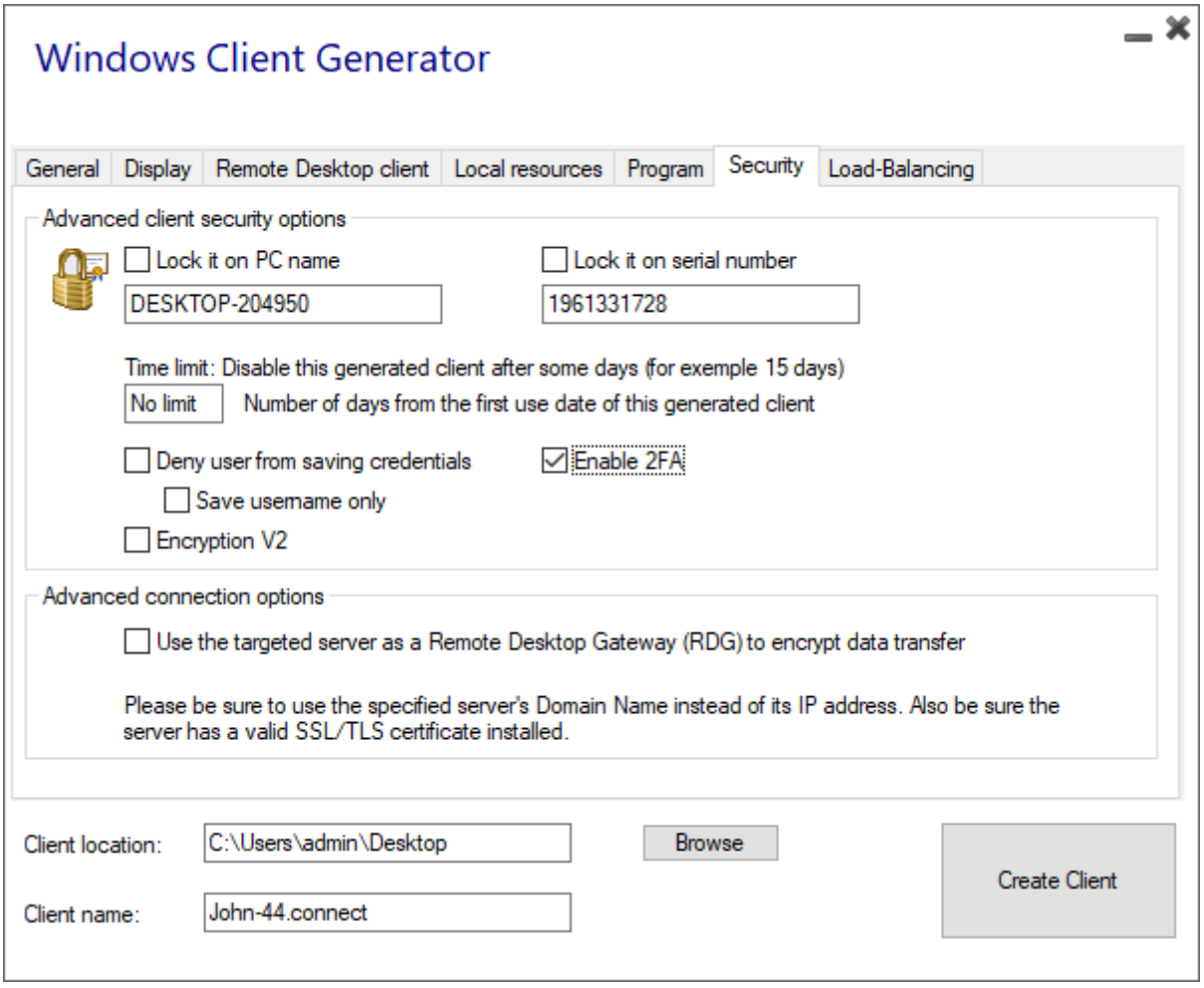
Please refer to Two-factor Authentication documentation page for more information on how to configure and enable two-factor autnentication for users and groups on your TSplus Remote Access installation.

Please note the following additional requirements to enable two-factor authentication for a generated client:

- Connection Client validates the authentication code against the Web Portal using the HTTPS port. Therefore, **Web portal must be up-and-running** and reachable through its HTTPS port from the client machine.
- If the HTTPS port of the Web portal is modified, then the generated clients enabled for two-factor authentication must be generated again. Previously generated clients will fail to validate any two-factor authentication.

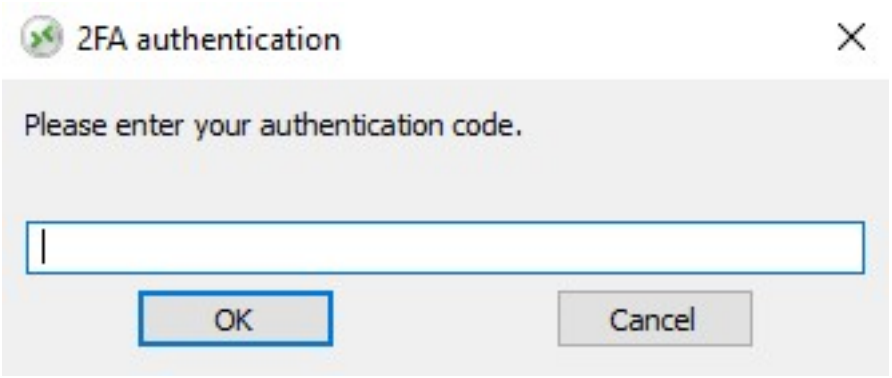
Since version 15.30.3.15, any previously generated client and any new client generated without 2FA support enabled will behave the same as before. **If a user enabled for two-factor authentication attempts to login using a client generated without explicit 2FA support, the login will be denied** as two-factor authentication is not possible and therefore will fail.

To add support for two-factor authentication, check the **Enable 2FA** checkbox before generating your client file. As a result, two-factor authentication will be validated when connecting to the Remote Access application server. If two-factor authentication is enabled on the application server and the connecting user is not configured, then the connection will be denied.



Be mindful that adding 2FA support to a generated client later is not supported. For example, adding 2FA support through command line against the generated .connect file is not supported.

Once a user has configured his account in an authenticator app, he or she will be able to connect using its password and the code provided by its authenticator app or by SMS.



Advanced connection option

If the targeted server possesses a specific and accessible domain name, as well as a valid SSL/TLS certificate installed, you can enable the “Use the targeted server as a Remote Desktop Gateway (RDG) to encrypt data transfer”.

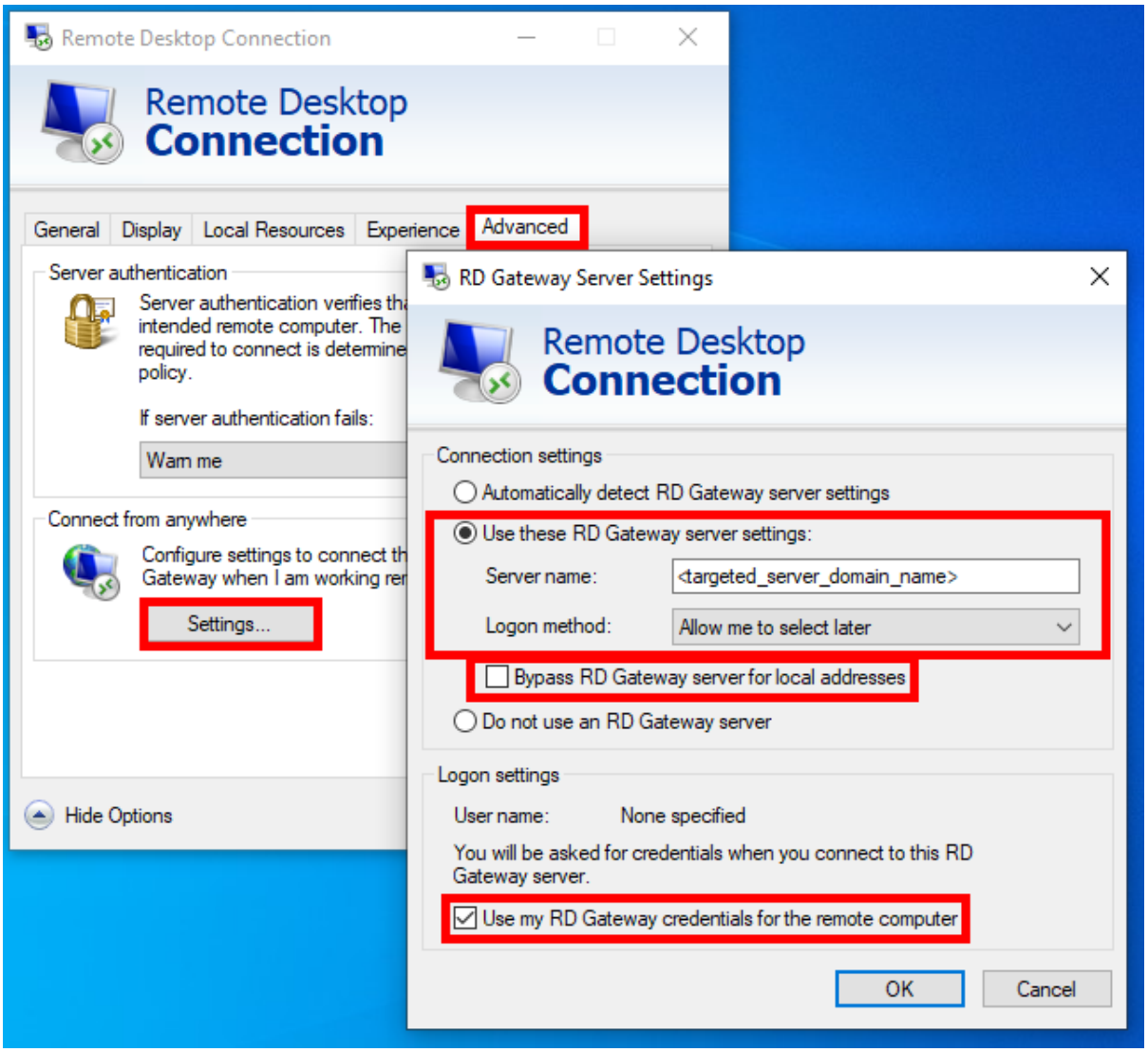
This option makes the RDP data transfer during the connection encrypted using TLS encapsulation, making it a suitable alternative to any VPN in term of data encryption.

Use mstsc instead to connect to the RD Gateway

You can also use this feature through mstsc configuration without using a generated client if the prerequisites mentionned above are met.

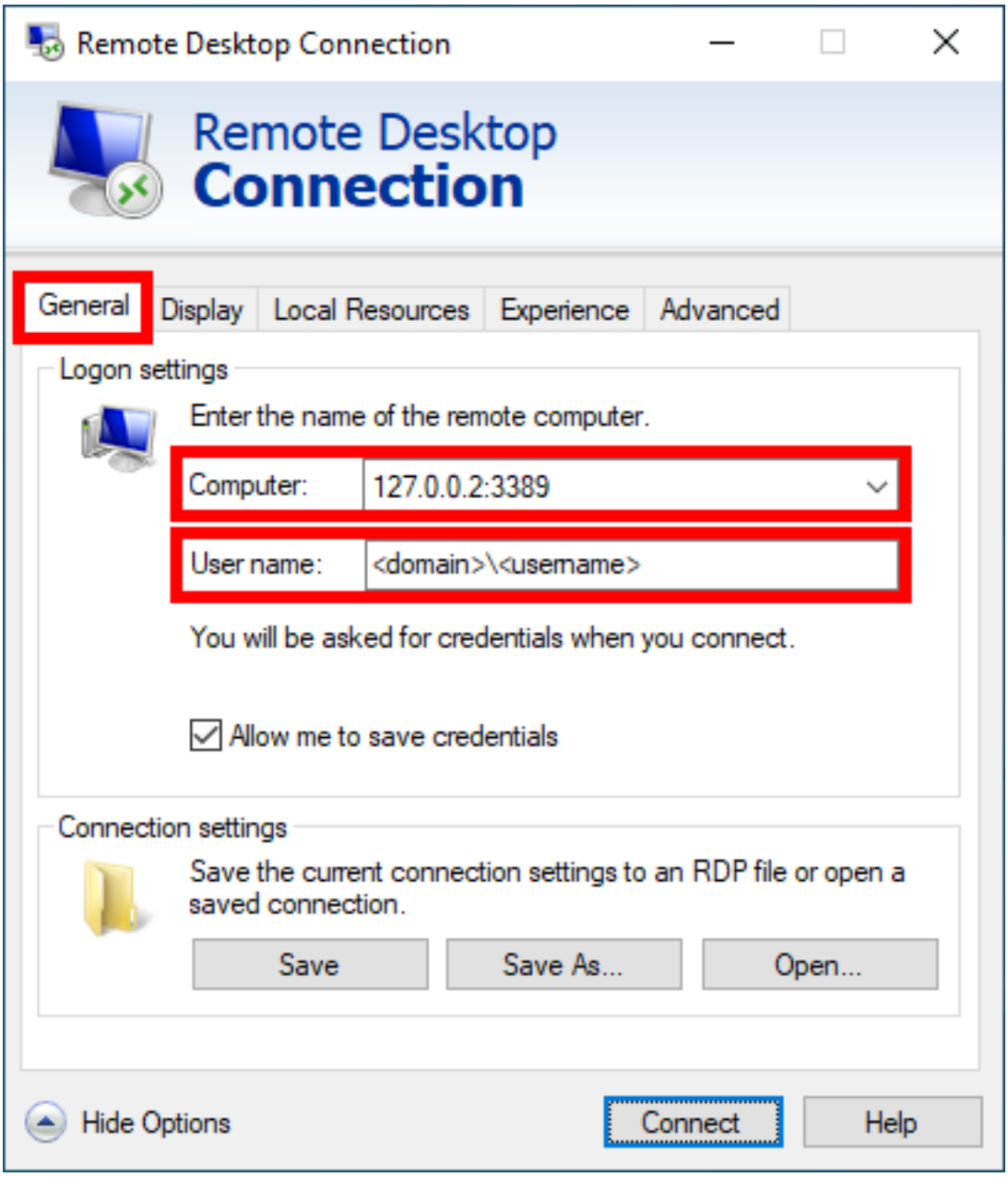
To do so, go to the advanced tab first, then on the “Connect from anywhere” section click on “Settings” and configure the Remote Desktop Gateway by :

- Ticking the “Use these RD Gateway server settings” option
- Replacing the server name with the targeted server domain name (without https://)
- Selecting the Logon method “Allow me to select later”
- Unticking the “Bypass RD Gateway server for local addresses” option
- Ticking the “Use my RD Gateway credentials for the remote computer” option
- Clicking “OK” to save these settings



Then go to the “General” tab, and :

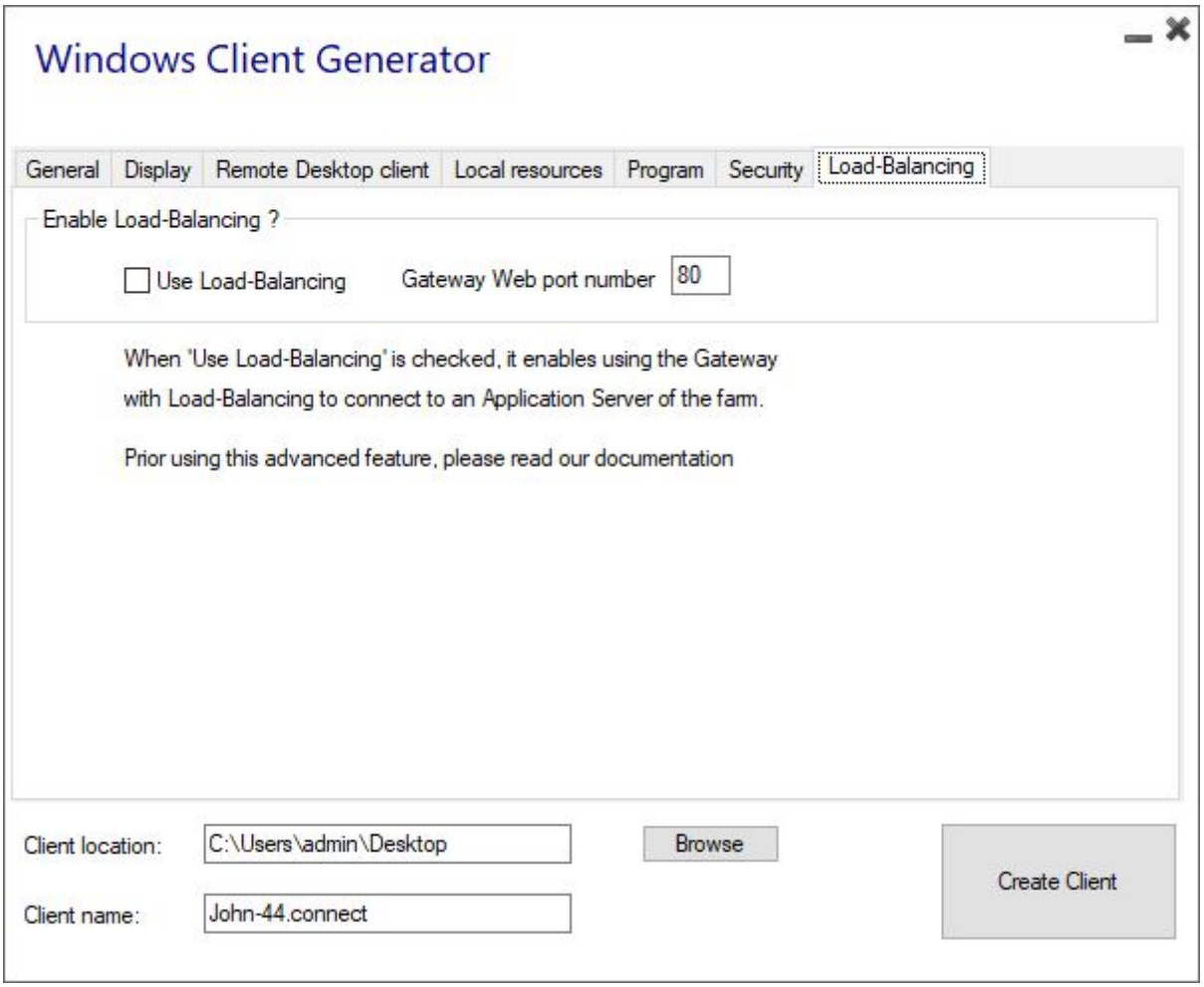
- Replace the computer name with “127.0.0.2:3389”, and change the port “3389” if you are using a different one
- Replace the username with the username you want to connect with (**important: specifying the domain is mandatory**)
- Clicke on “Connect”

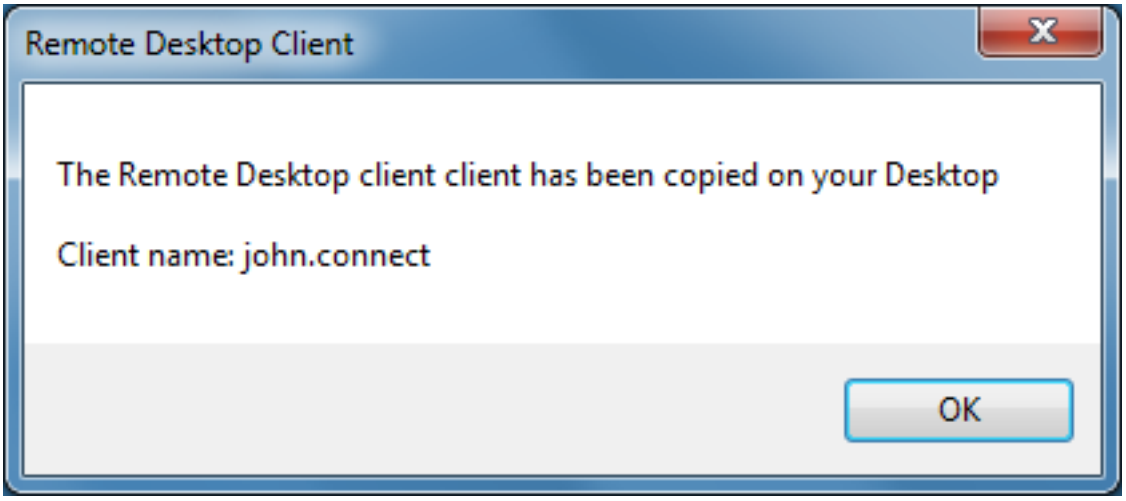


You can also enable the Load Balancing to connect to one server of your farm.

Do not check the “Use Load-Balancing” box if you did not activate the Load-Balancing feature on your server.

You will need to enter the Gateway Web port, which should be the same as the default web port used on all the servers of your farm.





Client Customization is possible. See the corresponding documentation on how to modify the client's icon and edit or delete its parameters.

You can enable the logs for Connection Client on the client side by adding the following registry key:

[HKEY_LOCAL_MACHINE\SOFTWARE\Digital River\ConnectionClient] "Debug"="true"

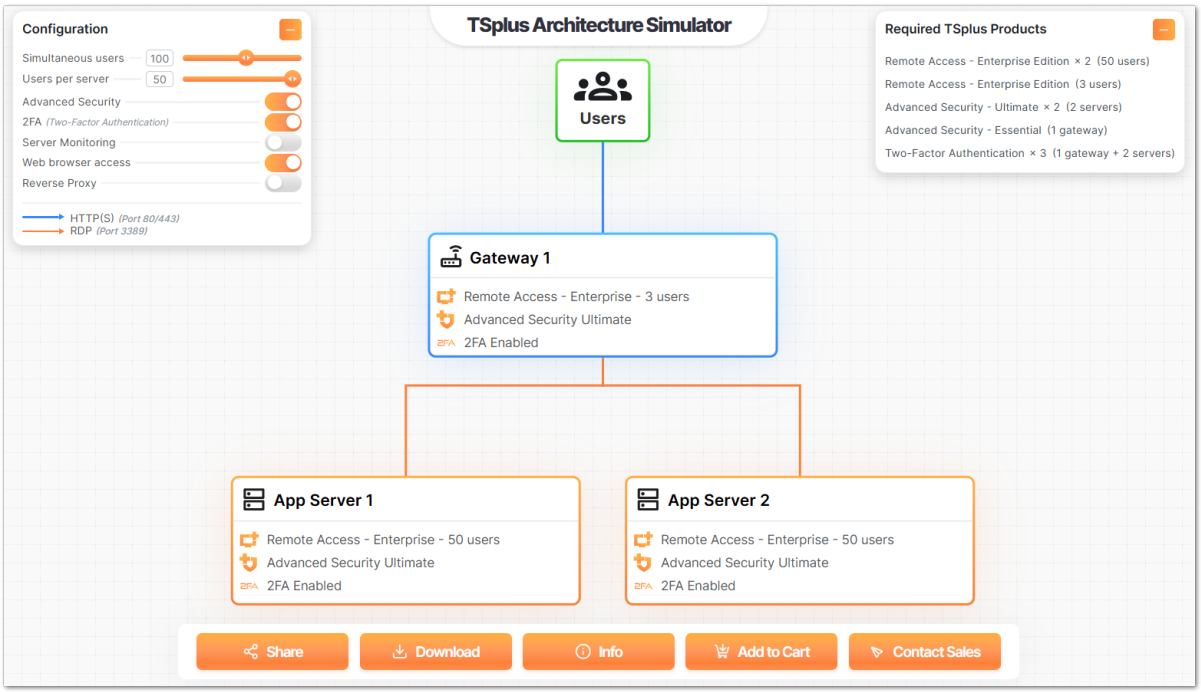
The logs are located in C:\Users<Username>\RDP6\logs directory if installation is per user or in C:\Program Files (x86)\Connection Client\RDP6\logs directory if installation is for all users.

TSplus Remote Access Prerequisites

Architecture Simulator

Configure your architecture online to help you choose our software and add-ons.

TSplus Architecture Simulator



1. Hardware

TSplus Remote Access Server minimum requirements:

Number of users	Windows 2008 to 2025 or 7 to 11 Pro
3 - 5	I5 or above One CPU 2 GHZ Minimum : 4 GB RAM Recommended : 8 GB RAM
10	I5 or above

	One CPU 2 GHZ Minimum : 8 GB RAM Recommended : 16 GB RAM
25	One CPU I7 or Xeon Minimum : 16 GB RAM Recommended : 32 GB RAM
50 and above	32 GB Dual CPU - SSD Disk dedicated to the system Minimum : 32 GB RAM Recommended : 64 GB RAM

We recommend using a CPU that is less than ten years old.

Regarding RAM usage, it will depend on the OS installed, the number of concurrent users and the applications that are assigned to them.

Each server (physical or virtual ones) can potentially handle up to 50 concurrent users. For over 50 concurrent sessions, we recommend using a farm of servers with the Load Balancing feature available in TSplus Remote Access Enterprise Edition.

Note: The exact specifications of your hardware will depend on what kind of resources (CPU/ RAM/Disk) your applications consume.

Only **x86 and x64** architectures are supported.
ARM32 and ARM64 architectures are not supported.

2. Operating system

Your hardware must use one of the operating systems below:

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

Both 32 and 64 bits architectures are supported.

The required framework is **.NET version 4.7.2** for all supported Windows versions.

Remote Access version	Minimum Windows version
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

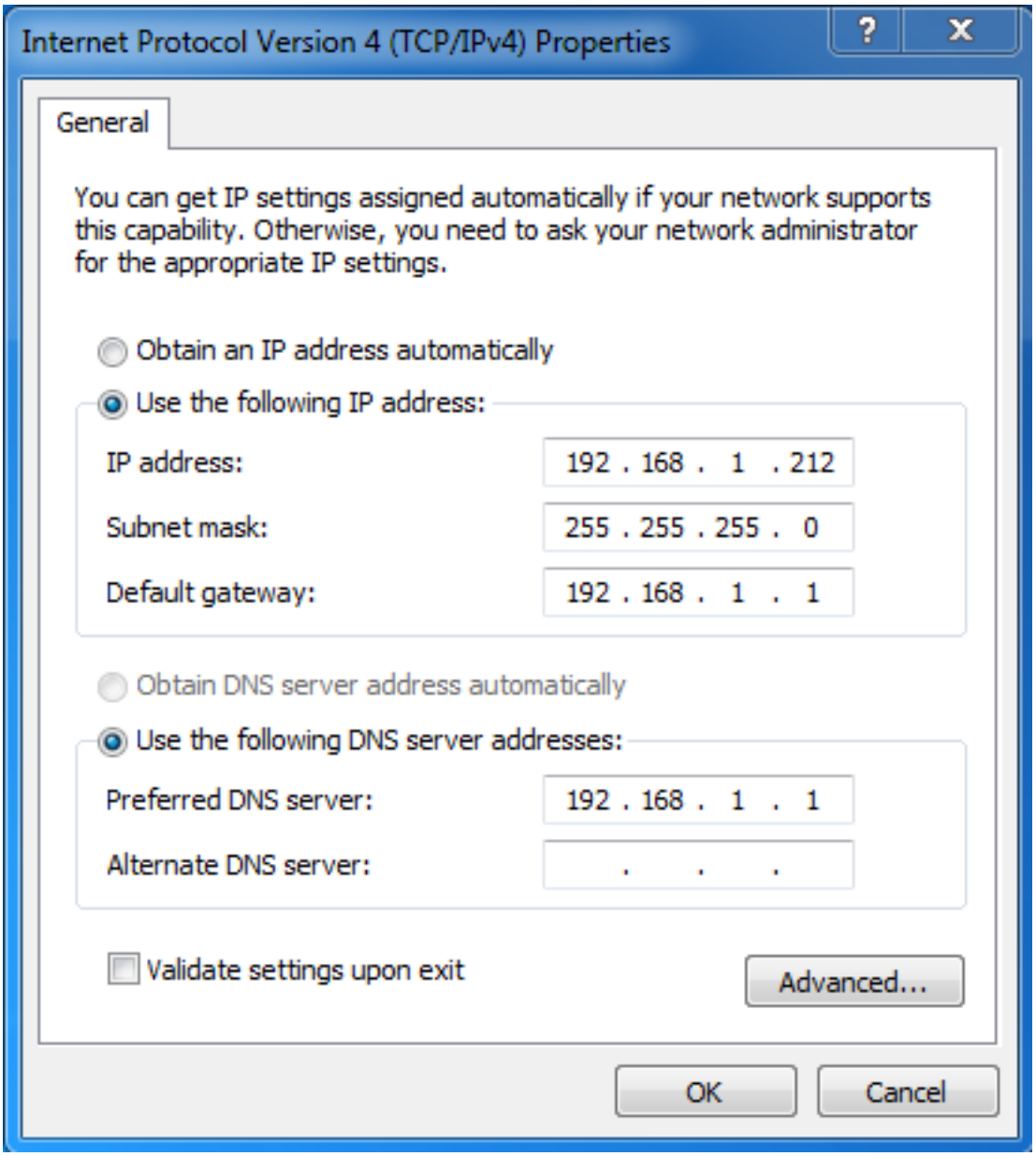
- If you install Remote Access on a Windows Server OS make sure the RDS/Terminal Services and RDS/Terminal Services Licensing roles are not installed before installing TSplus Remote Access.

If these roles are currently installed, remove them and reboot.

- Windows Home Editions are not supported.
- On Windows Server 2016, 15 sessions maximum are allowed for Remote Desktop access.
- Windows Server 2016, 2019, 2022 Essentials Edition is not supported nor recommended for using TSplus Remote Access.
- TSplus Remote Access built-in Web server requires **Java OpenJDK 17 or greater.**.

3. Network parameters

The Remote Access Server must have a static private IP address:



Remote access (from Wide Area Network - WAN)

- A broadband internet connection is recommended as well as a static public IP address. If you do not have a static IP address, consider using a dynamic DNS service like <http:// DynDNS.org>
- The TCP RDP port (by default 3389) must be opened both ways on your firewall.

3. Security

Since early 2024,
TSplus has updated its automatic SSL/TLS certificate generation mechanism to align with Let's Encrypt's change in the chain of trust: the **"DST Root CA X3"** root has been replaced by **"ISRG Root X1"**.

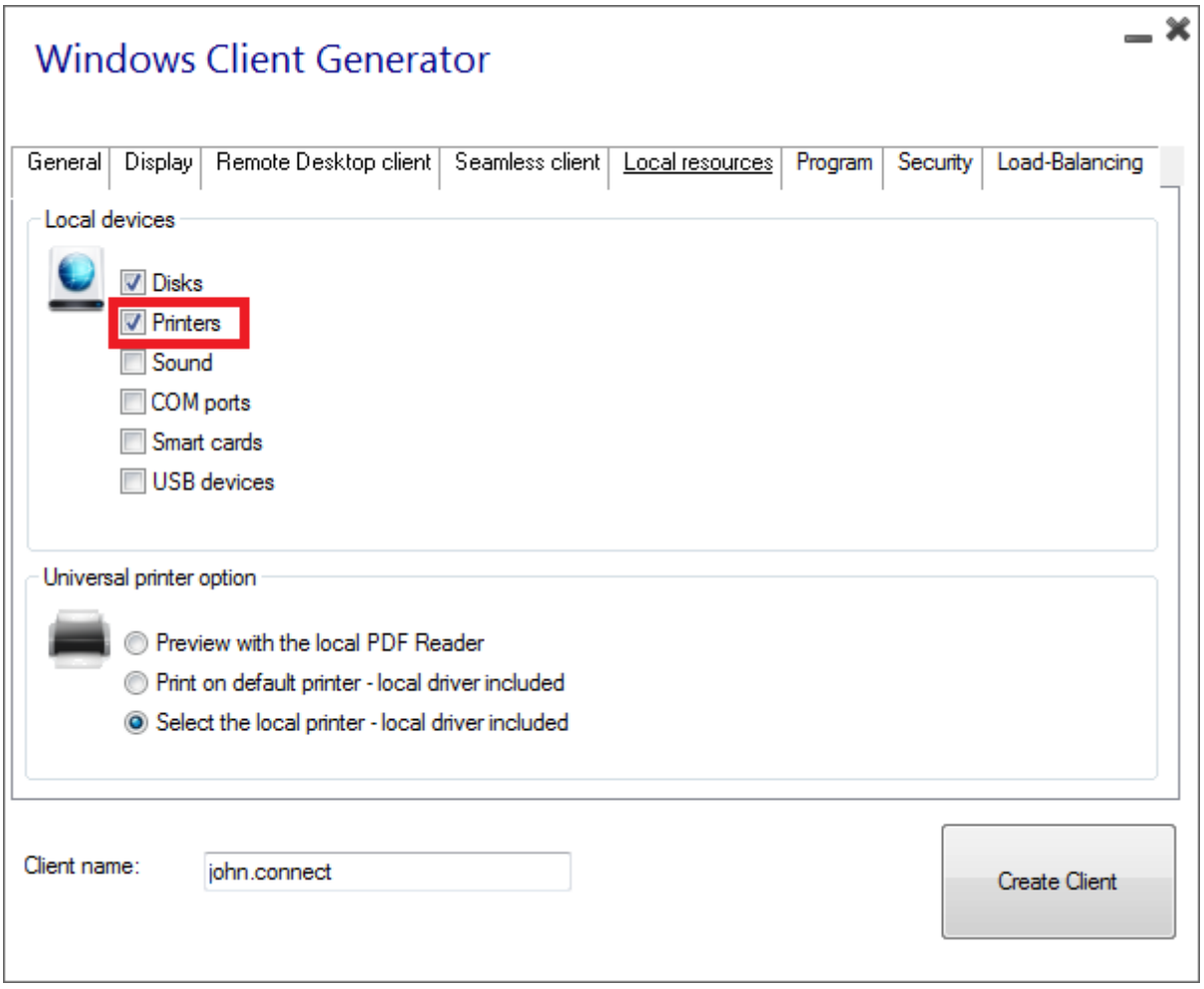
If a client or workstation does not recognize the new certificate, it may be necessary to add **"ISRG Root X1"** to the Windows trusted certificate store.

TSplus works with wildcard certificates and supports the TLS protocol for secure remote connections.

Printing with Standard RDP Printer-Mapping Feature

This is commonly used by Remote Desktop users and is equivalent to what you would have with Microsoft Terminal Services.

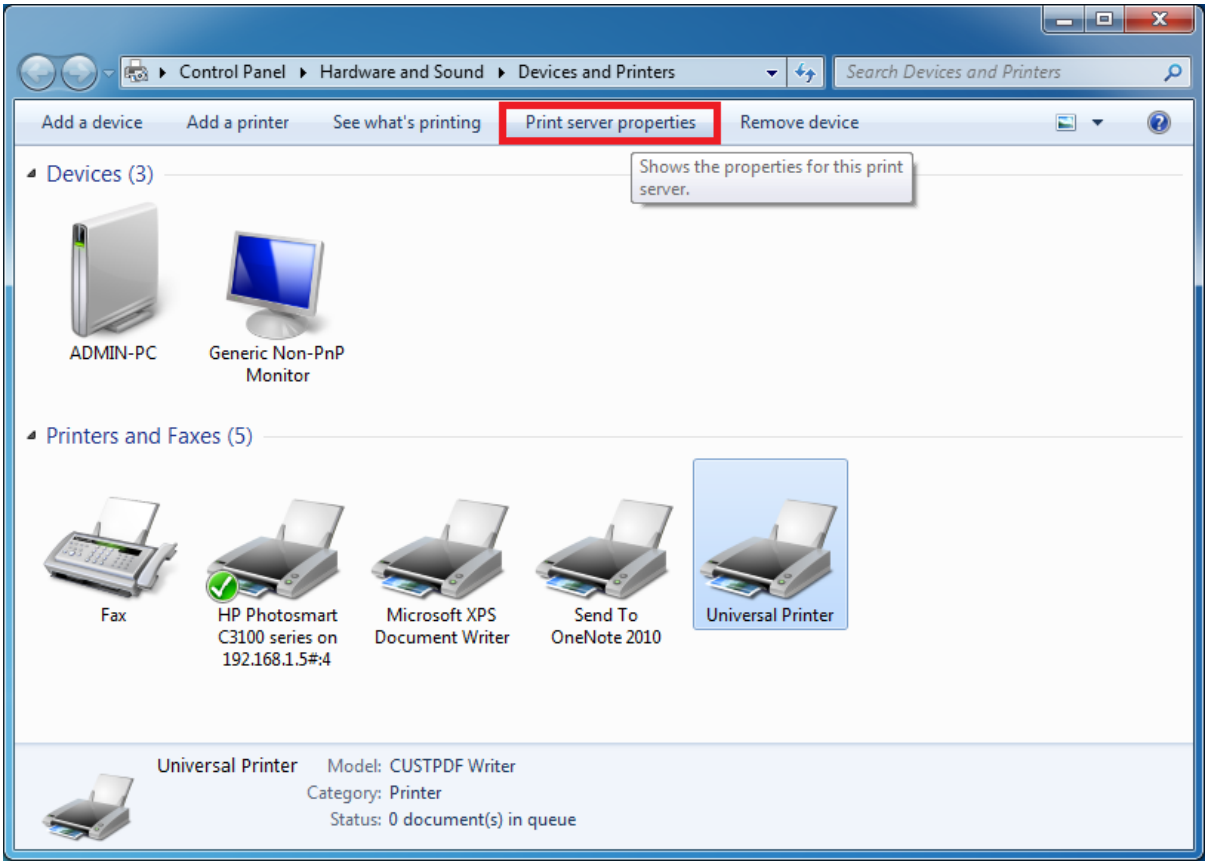
If you plan to use exotic printers, be sure to check the box for printers in the local resources tab of the client generator.



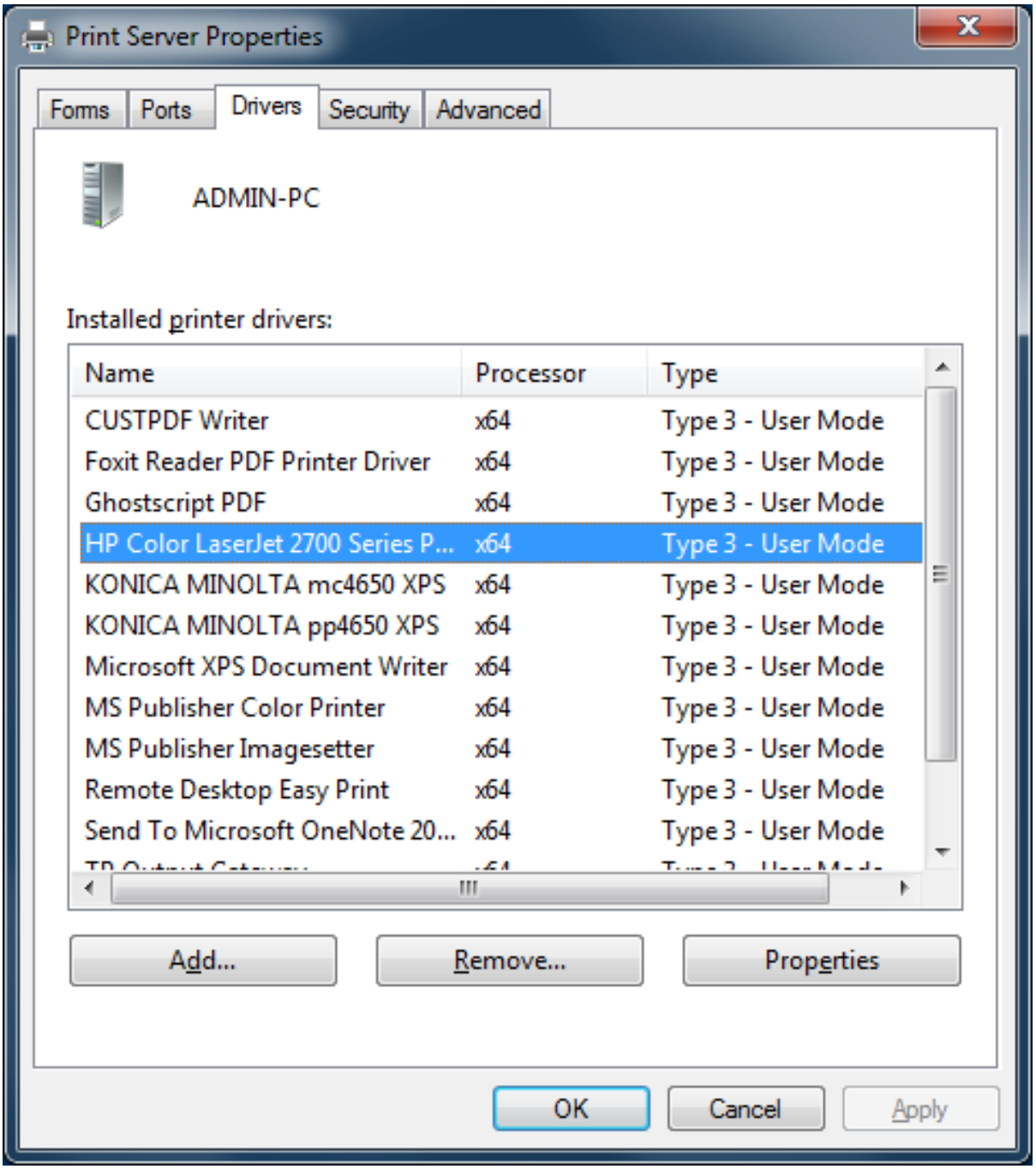
Most of the time it will require that you install the same version of the printer drivers on both the client and the server in order to work properly.

This means that if your server is Windows 2008 64 bit and your client computers are running Windows XP 32 bit, you will need to install the 32 bit XP Printer Drivers on the server.

Click on the Start Menu, then on Devices and Printers. Click on any printer to display the Print server properties button at the top of the window:



Once in the Print Server Properties, click on the Driver tab to manually add your client driver. (In this case, we are installing the Windows XP 32 bit driver)



You can also directly install your printer drivers using information and drivers from the Printer Manufacturer Website.

- It is recommended to check your hardware manual for an installation procedure in a terminal server environment.
- If you are using USB printers, make sure you updated the RDP protocol of your client computer to RDP version 6 or above to ensure maximum compatibility with redirected printers.

For the best results, it is recommended not to use USB printers. Compatibility and reliability are improved when using COM or LPT printers.

Some exotic printers, such as label or receipt printers, may not be suitable to be redirected in a TSplus session, you should always check with your hardware manufacturer for compatibility and installation procedures in an RDS or terminal server environment, which is very close to TSplus

in this case.

TSplus Remote Access v19: Quickstart Guide

Prerequisites:

On the Server:

- **OS:** Microsoft Windows Versions 7 to 11 or Windows Server 2008R2 to 2025 with at least 2GB of RAM.
- TSplus does not support installation of Remote Access on Windows Home Editions.
- The operating system **must** be on the C: drive.
- Java Runtime Environment. If Java is not already installed, Remote Access will install OpenJDK during setup.
- If you are installing Remote Access on a Windows Server operating system, make sure that the RDS/Terminal Services and RDS/Terminal Services licensing roles are **not installed** before installing TSplus Remote Access.
- Your Remote Access server must have a static private IP address.
- For External access, your server must have a static public IP address or dynamic DNS provider.
- TSplus Remote Access built-in Web server requires **Java OpenJDK 17 or greater.**.

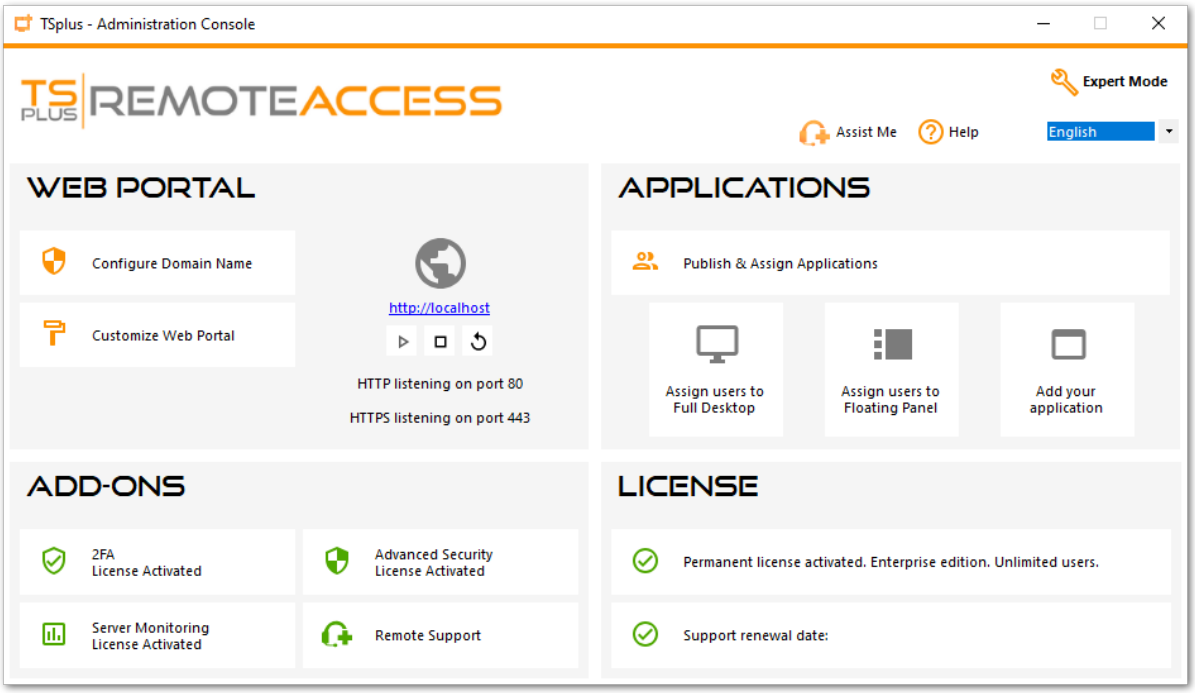
On the Client:

- **OS:** Microsoft Windows Versions 7 to 11 are fully supported.
- For MacOS you can use any Mac RDP client or the TSplus HTML5 client.
- For Linux you can use Rdesktop or the TSplus HTML5 client.
- Java Runtime Environment.
- A PDF reader (example: Foxit Reader or Acrobat DC)

For more detailed prerequisites please see the documentation

Note:

Starting with Remote Access Version 15, the Administration console has changed its look. A **Lite Mode** and an **Expert Mode** have been introduced. Administrators can toggle between the two interface styles by clicking the button in the upper-right corner of the Admin Console.



Step 1 : Installation.

Note:

The trial version of Remote Access is the fully-featured Enterprise Edition. It is licensed for up to 5 concurrent users for a period of 15 days.

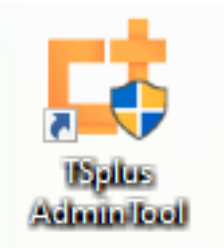
Installing TSplus Remote Access is an easy process. Just download it from our web site, run the Setup-TSplus.exe program.

Files are decompressed and copied into:

- C:\Program Files\TSplus (32-bit systems)
- C:\Program Files(x86)\TSplus (64-bit systems).

Once the installation is complete the installer will ask you to reboot.

After the reboot, you will see 2 new icons on your Desktop:



The AdminTool is what you need to use Remote Access.

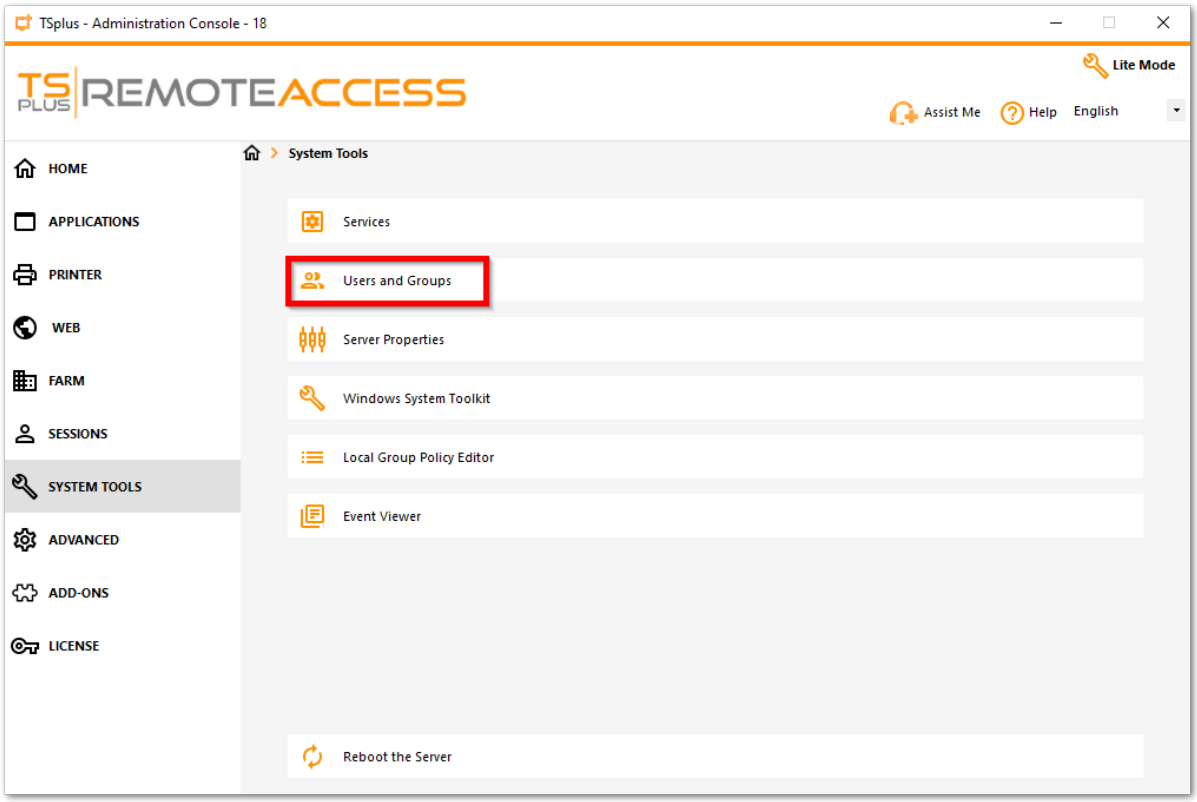


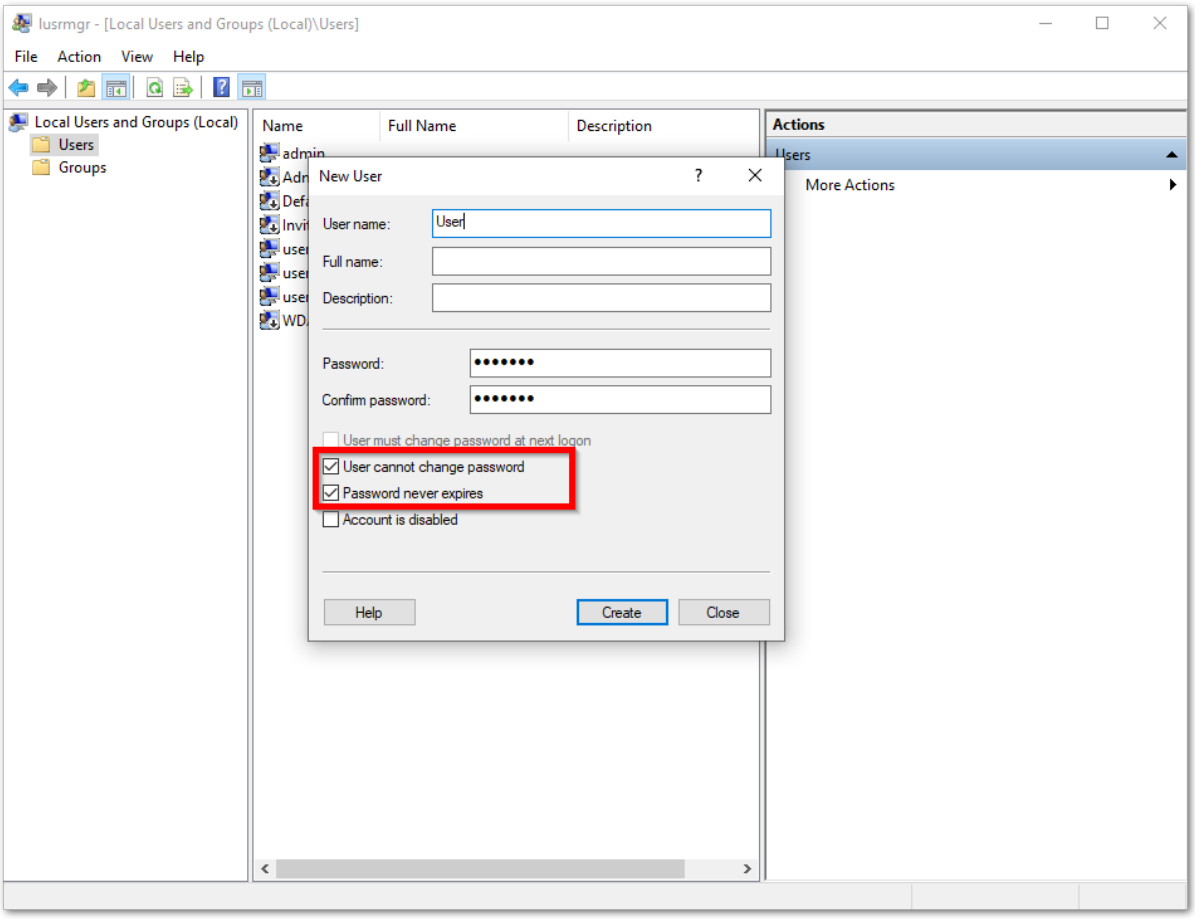
The Portable Client Generator is used to create Remote Access connection clients for your users.

See the documentation for full installation instructions.

Step 2 : Creating users.

After the reboot, the Remote Access Server is almost ready to go. Now we'll create users. Open the AdminTool to get started. Then go to the System Tools tab and click on "Users and Groups". This will take you to the Local Users and Groups window:





Each user must have a User Name AND a Password. When creating users, be aware of the box labeled “User must change password at next logon”. If you don’t want your users to change their password during the first login, uncheck this box and check the “Password never expires” or “User cannot change password”.

Step 3 : Select the most suitable client for your needs.

Remote Access is compatible with Windows Remote Desktop Protocol. Any user can connect locally or remotely with a standard Remote Desktop Connection client (mstsc.exe) or any RDP compatible client. To fully benefit from the advanced features in Remote Access (RemoteApp, Universal Printer…) you can use a generated client or the Remote Access Web Portal.

Remote Access is a very flexible solution and offers multiple ways to open a session:

- **Classic Remote Desktop Connection** (MSTSC.EXE).
- **Portable TSplus RDP client** which will display a windowed environment for your remote connection that you can minimize in the Windows taskbar.
- **MS RemoteAPP client** which will display application using the native MS RemoteApp.
- **Windows client** over the TSplus Web Portal.
- **HTML5 client** over the TSplus Web Portal.

These clients give the user the following experience:

With Remote Desktop Connection (mstsc.exe)

- **Connection**: The connection is a very standard one. The Universal Printer is not supported with this type of connection.

- **Display**: Users will see their session within a Remote Desktop window. This desktop displays the content of the user's desktop folder.

  If the administrator has assigned specific applications with the AdminTool, only these applications will be displayed (no taskbar, no Desktop).

TSplus RDP generated client.

This is a unique TSplus solution, it empowers local and remote users to connect using one single dedicated program.

It includes the connection program, the Universal Printing advanced feature, portability with high level of security while keeping it very simple for the users.

For more information about using the TSplus Client Generator, see this documentation

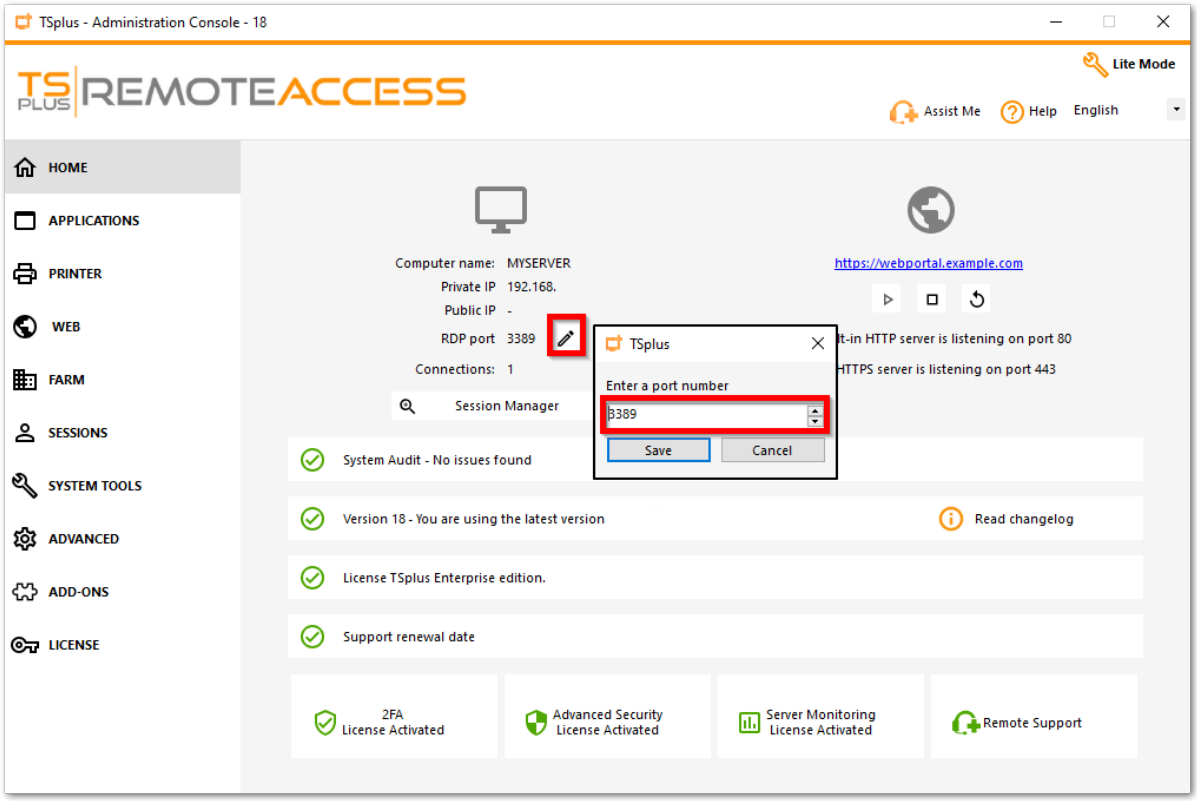
The TSplus RemoteApp generated Client.

Remote applications will look and behave like a local application. Instead of a classic Remote Desktop window, you will be free to switch between your local and remote applications without having to minimize a Remote Desktop window.

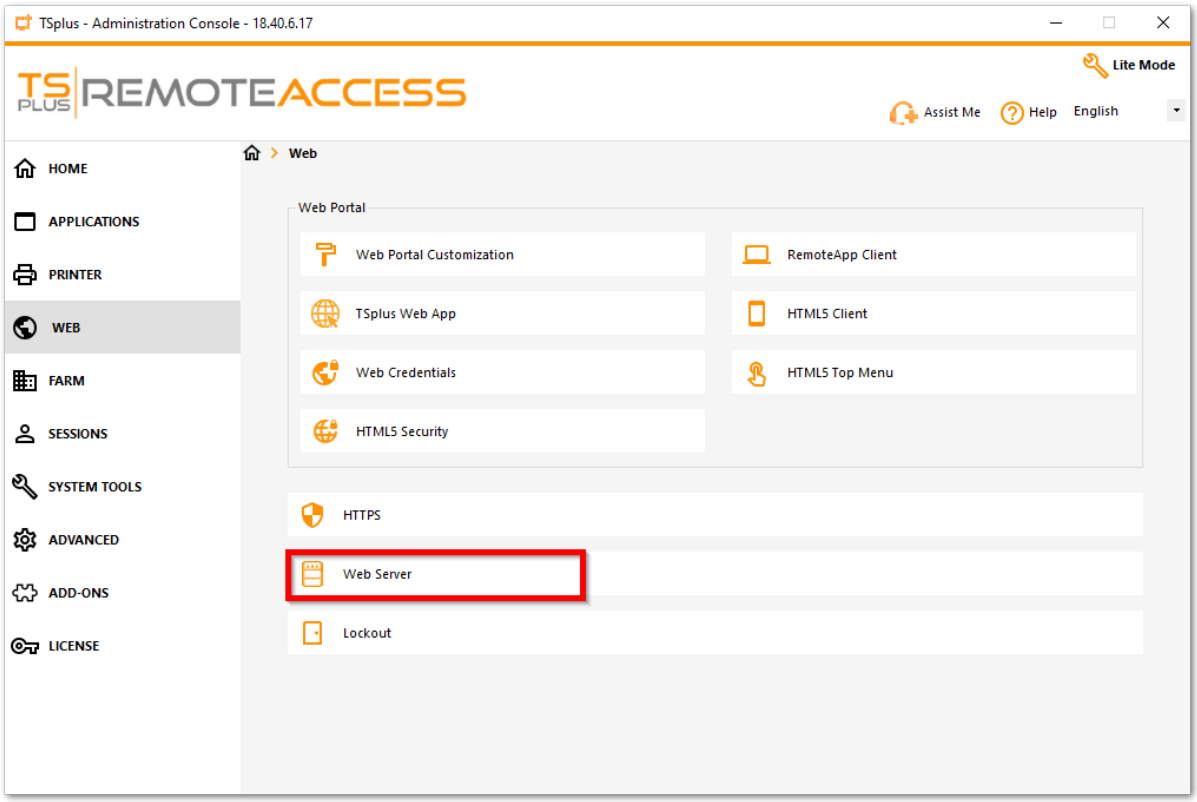
For more information about these clients, see this documentation.

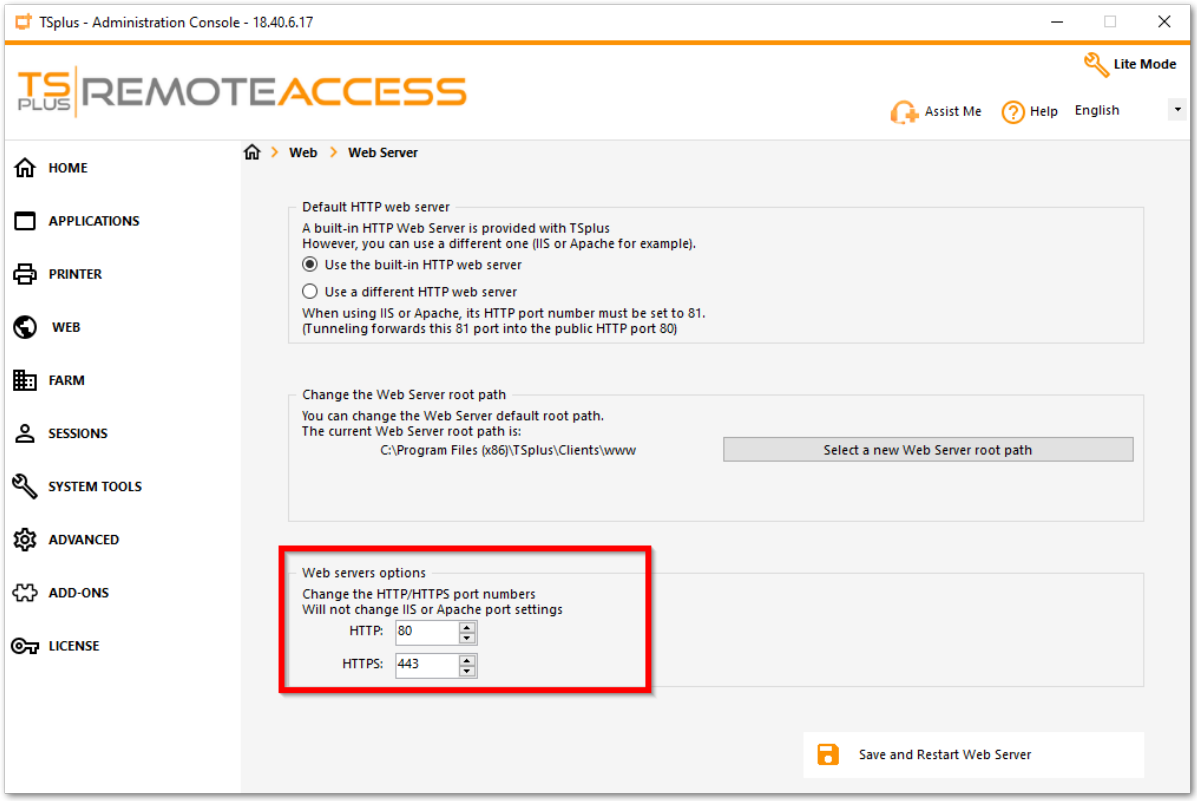
Accessing your TSplus Remote Access server from a remote location

To access your Remote Access server from outside of your local network, you will have to create a port forwarding or port redirection rule of 3389/80/443 ports depending on your preferred connection method. You can change the RDP port in the Home tab:



The 80/443 ports can be changed in the Web Server tab:



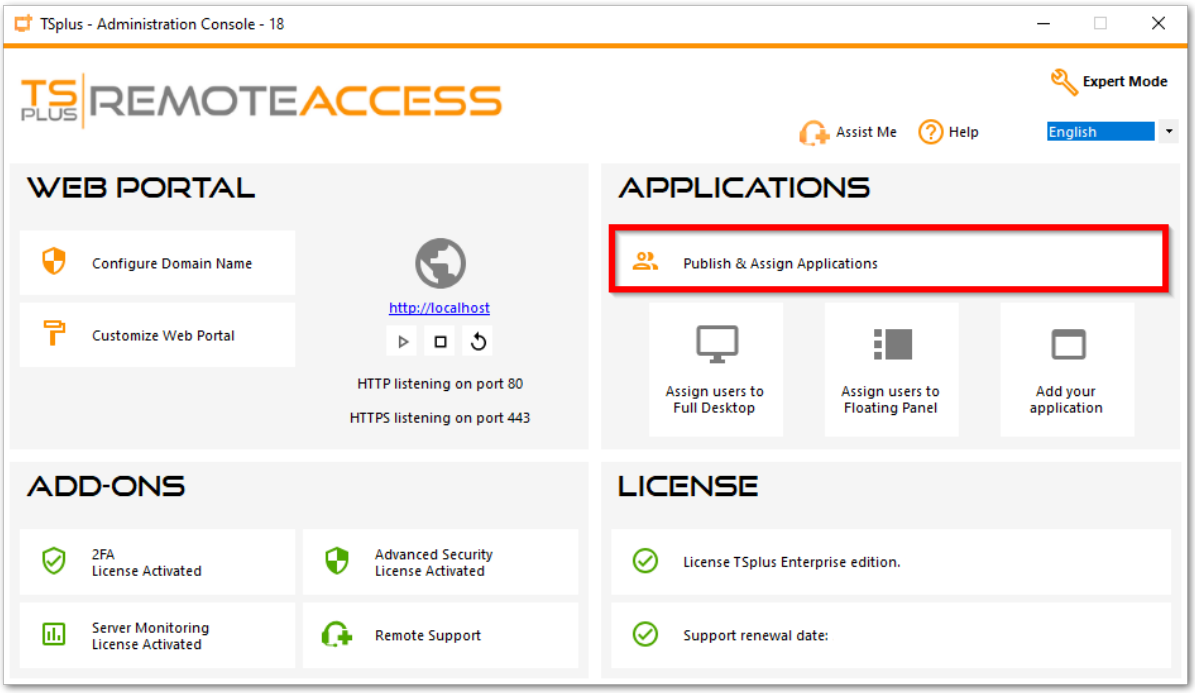


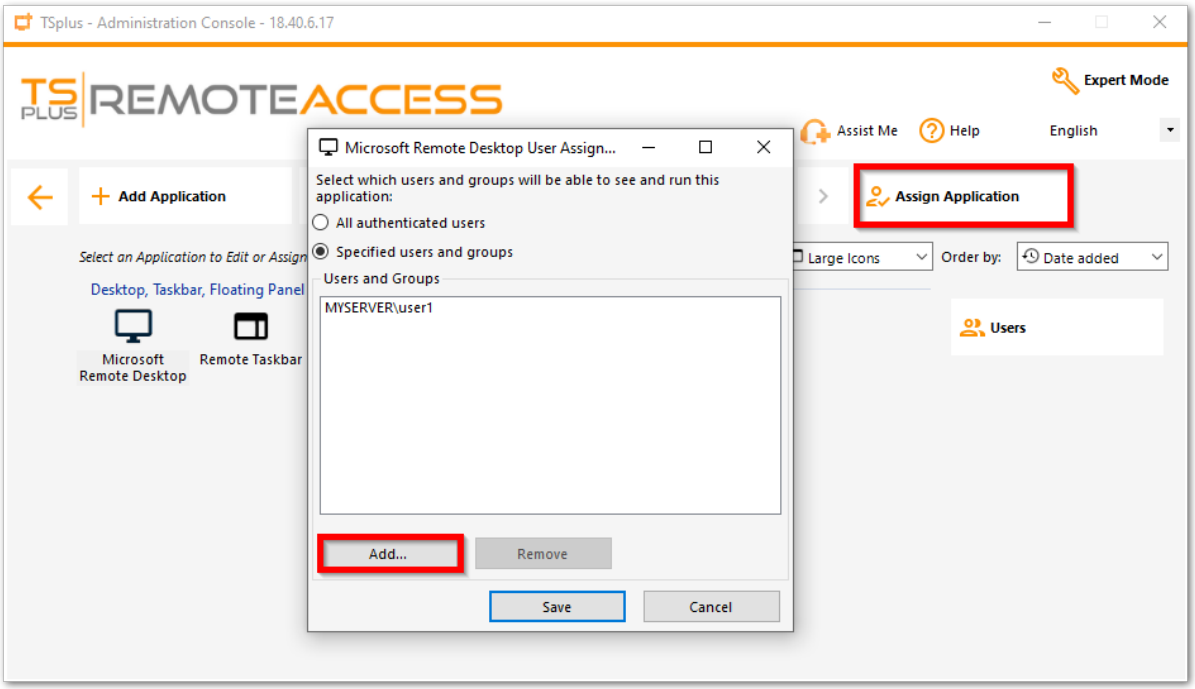
Step 4 : Application Publishing and Application Control.

In the Remote Access AdminTool you can assign application to users or groups.

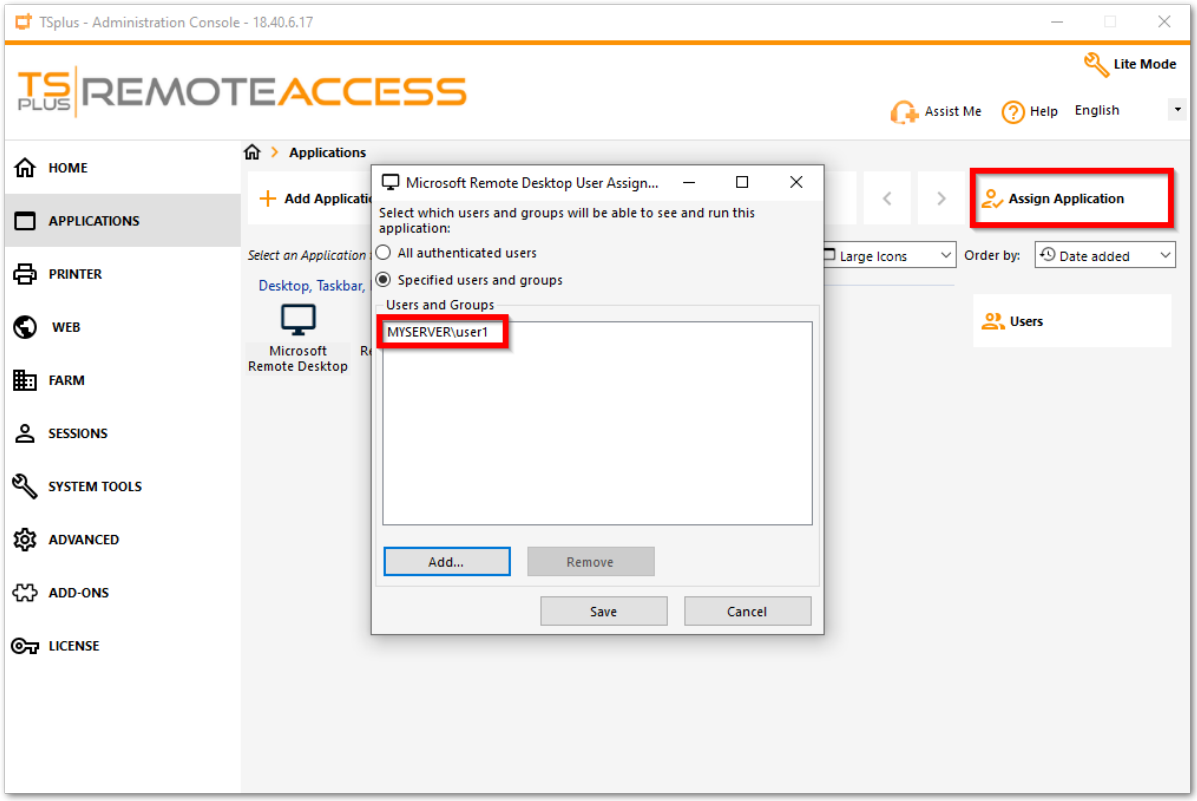
- If you assign one application to a user, they will only see this application.
- You also can assign them the TSplus Taskbar, the Floating Panel or the Application Panel to display multiple applications.
- You can also publish a full Remote Desktop.

Now available in
Lite Mode
from the home tab.





Or go to **Expert Mode >** Apps tab to add, edit, delete, and assign apps.



In this example, the administrator has decided that the user ‘John’ will get the TSplus Taskbar. See this documentation for more information.

Thank you for using TSplus Remote Access!

Rehosting Your TSplus License

Online Rehosting

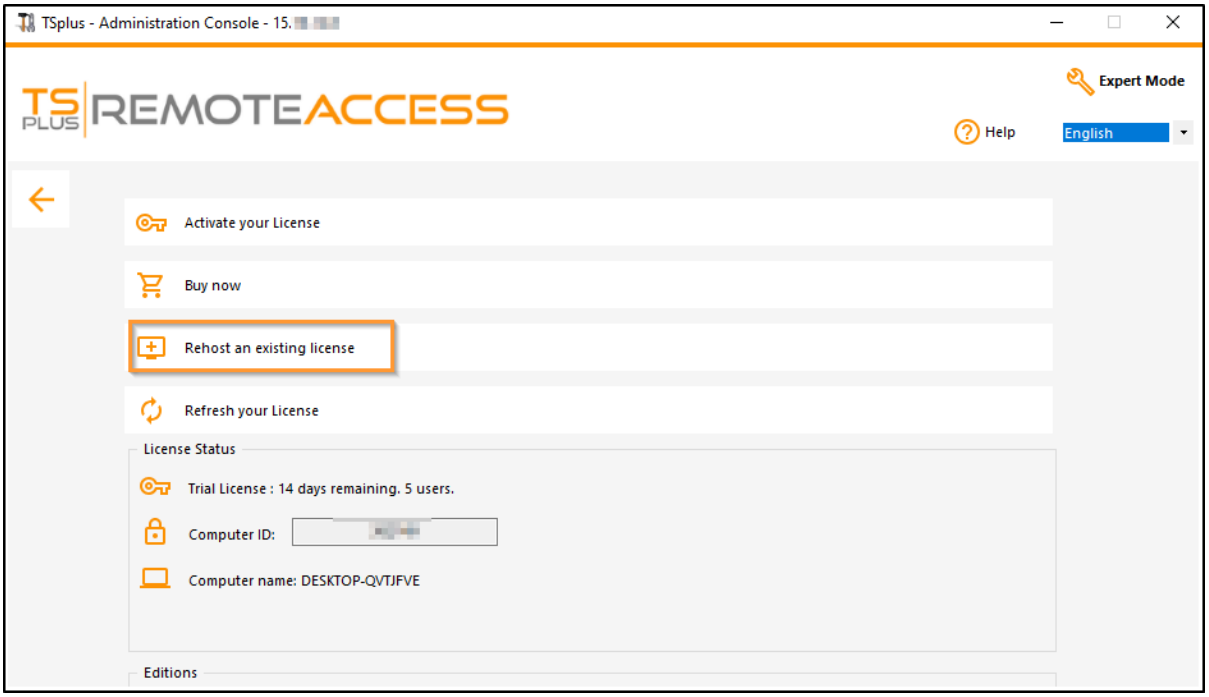
Online Activation is authorized once a month.

Prerequisites: It is necessary to have an active support subscription to rehost your license.

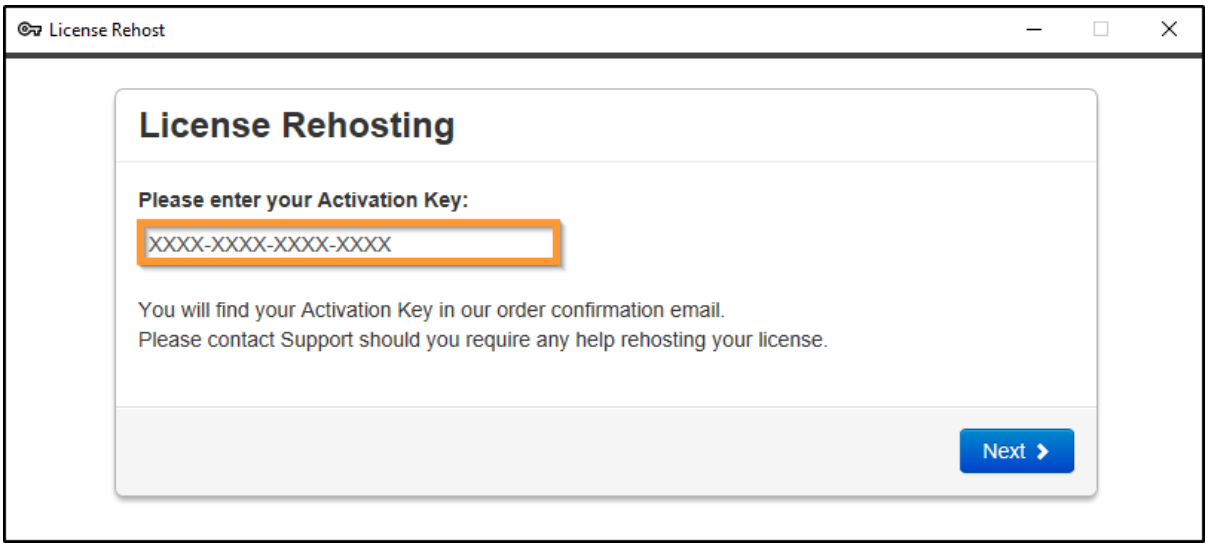
It is necessary to install a new version of non-cloned Remote Access to generate a new Computer ID.

If you have duplicated your server and cloned the Remote Access, please go to the following page: Clone your server

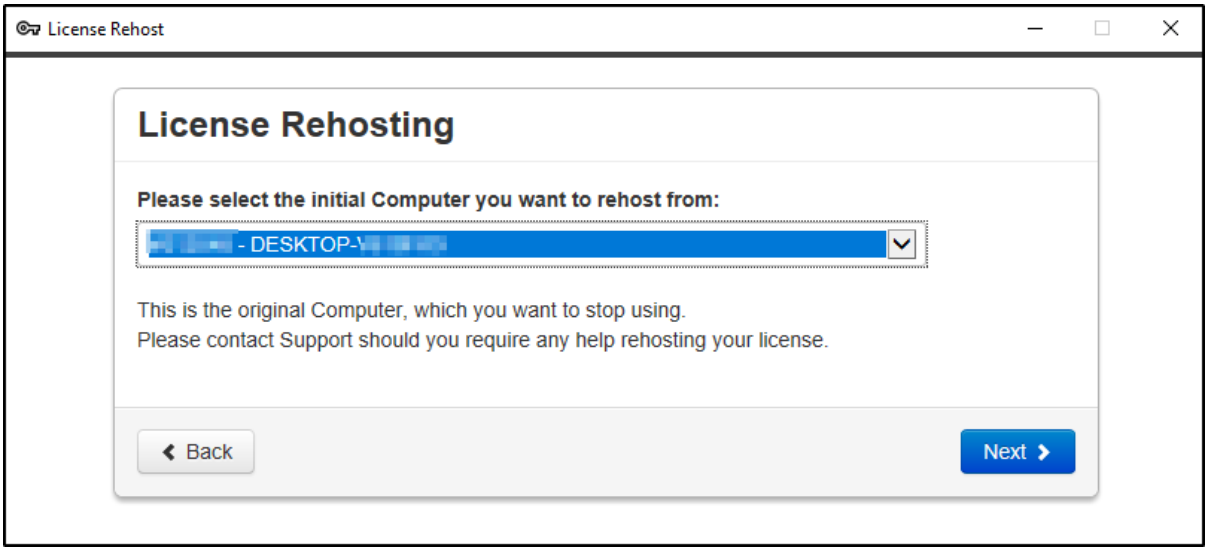
On the new server Go to the “License” tab Click on “Rehost an existing license”



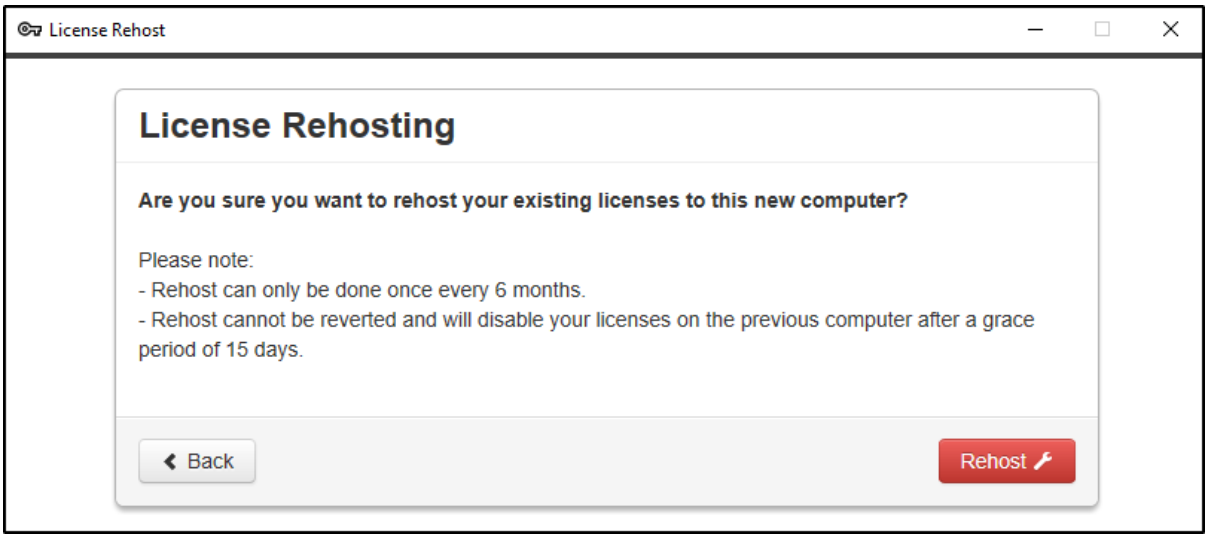
Enter your Activation Key:



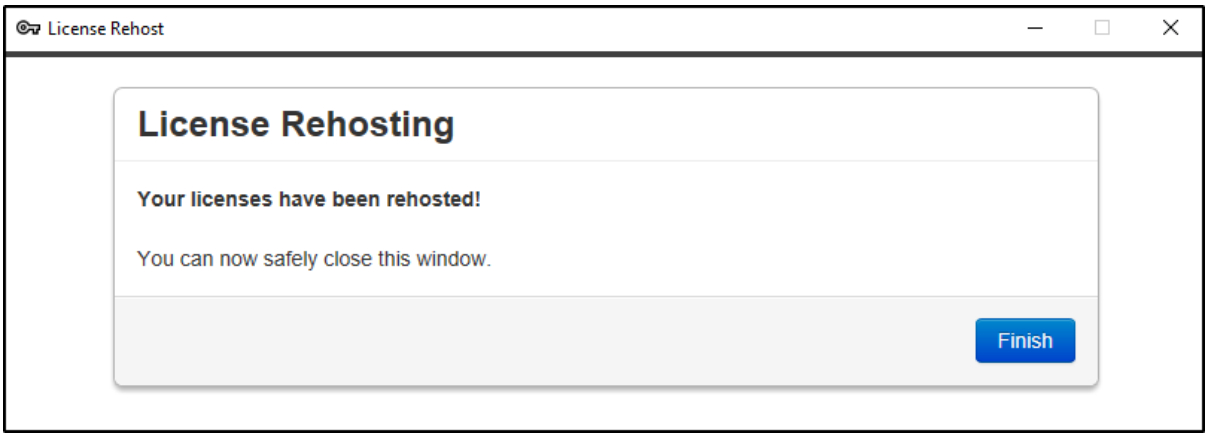
Select the initial Computer you want rehost.



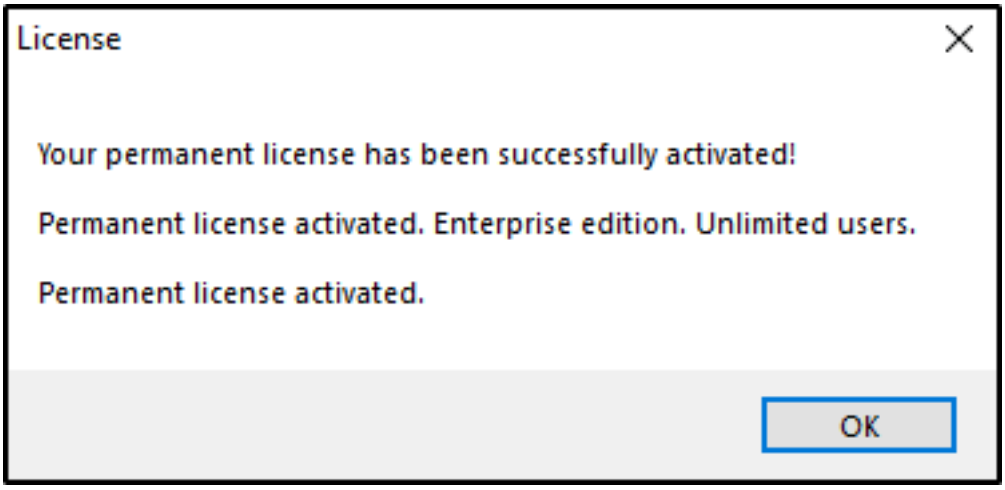
Confirm rehost



Your license rehost is finished.

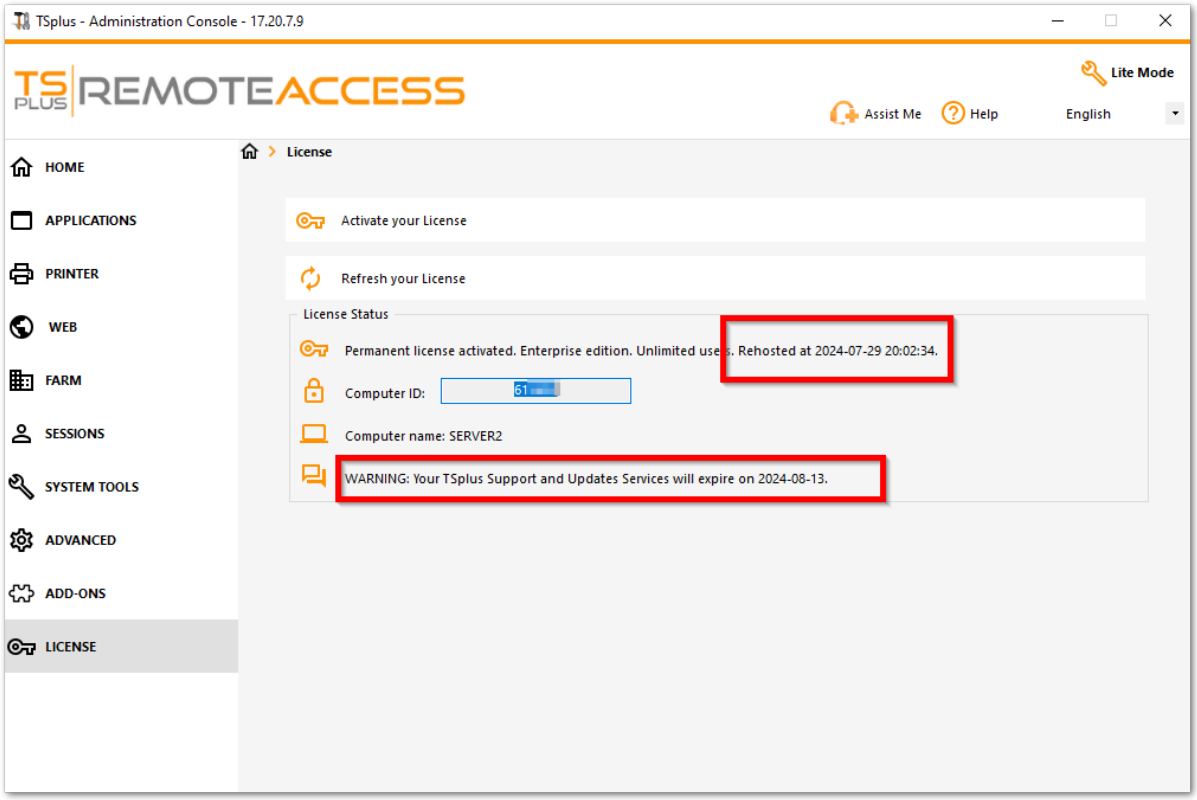


Wait a few moments for your AdminTool to synchronize until the window appears.



Congratulations on your license has been successfully activated!

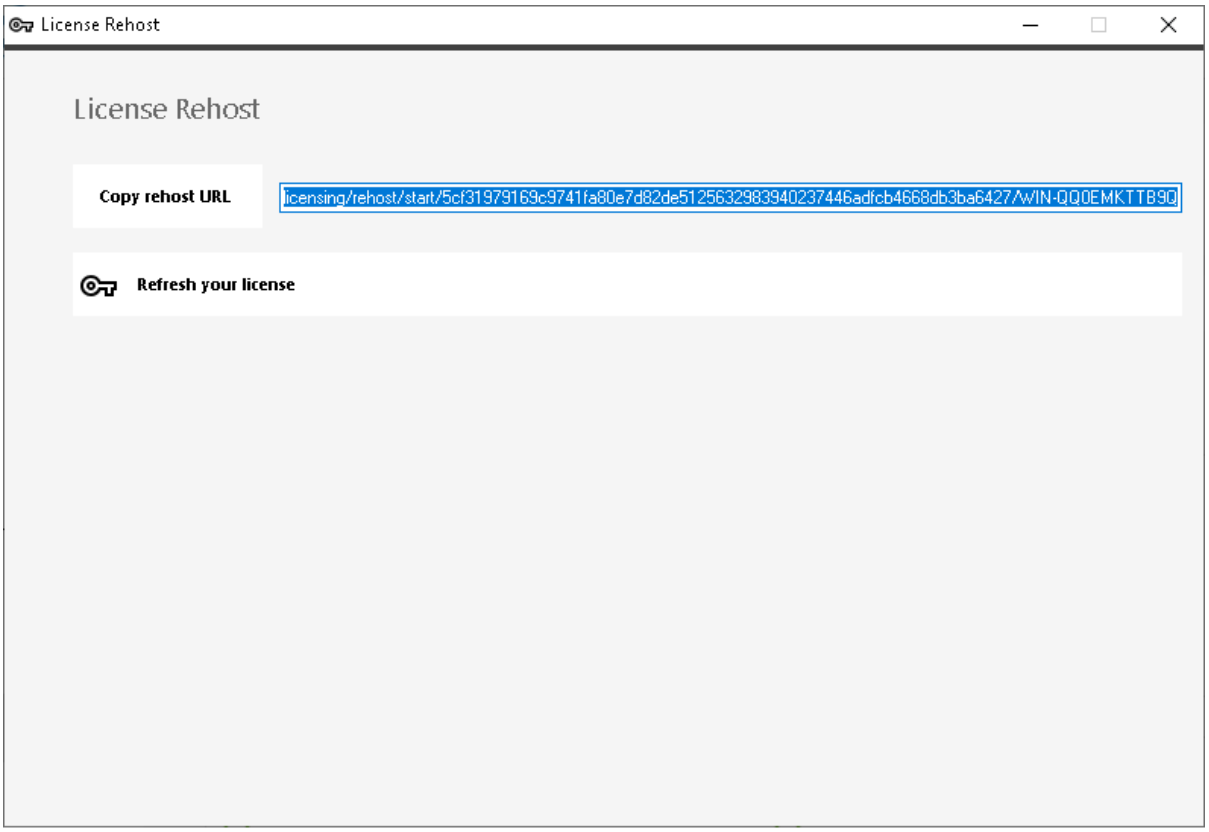
Note: A message will appear on the old server with the rehost date as well as the end of use date.
After a rehost, the old server will still work for **15 days** to help you make the transition.



Offline Rehosting

Offline Activation can also be done for rehosting licenses.

When the server does not have Internet access, the ‘rehost an existing License’ button will present the offline rehost page:



The process is the same as Offline Activation.

Remote Connection from an iPhone / iPad / Android device

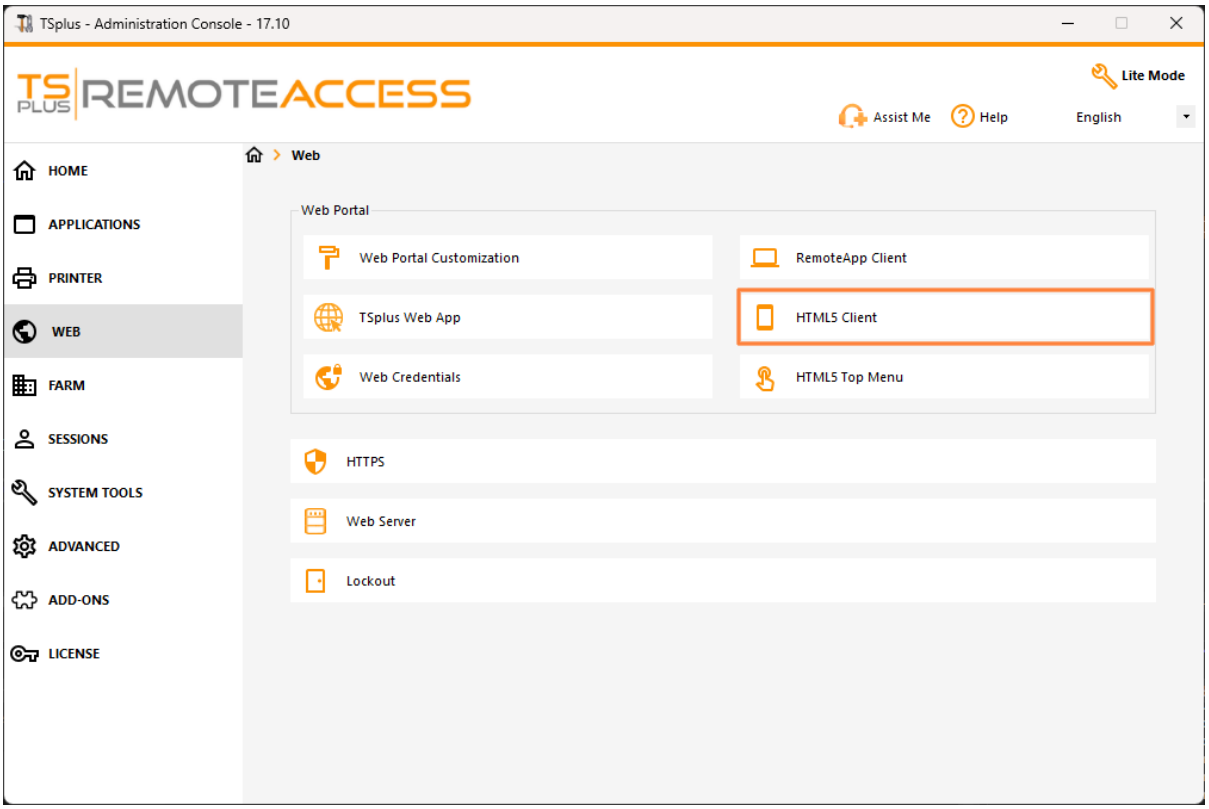
You can connect to your Terminal Service Plus server on any browser from any mobile device supporting the HTML5 technology, such as:

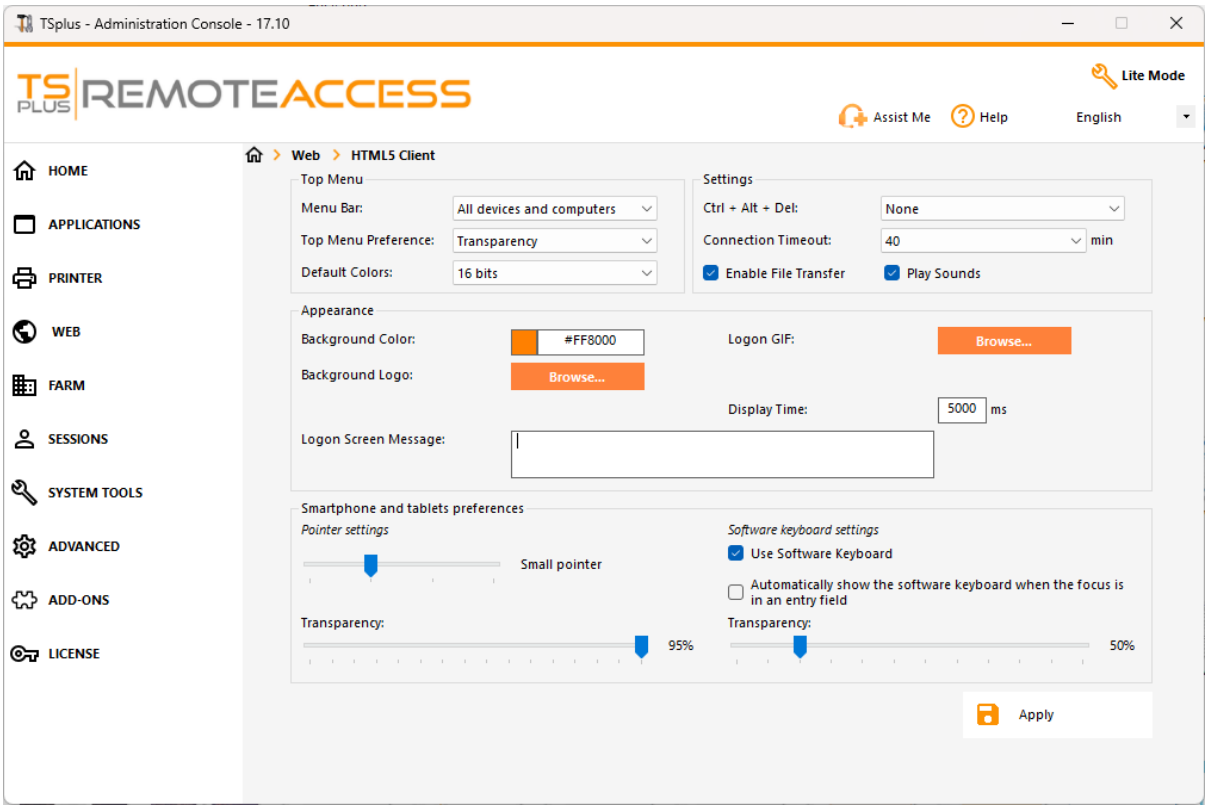
- an iPhone
- an iPad
- an Android smartphone
- an Android tablet

Edit the preferences for Mobile devices

Since the 11.20 release, the TSplus HTML5 client has been greatly enhanced to offer the best possible user experience even from Smartphones or tablets. The keyboard has been redesigned to automatically pop-up when the focus is over an entry field. The mouse pointer has been redesigned to facilitate the selection of buttons and fields even if located on the left or the bottom borders of a Smartphone.

You can set up various different HTML5 settings for mobile devices or computers on the HTML5 client tile of the Web Tab:





- Display the menu bar for all devices and computers or for mobile devices only.
- Enable or Disable File Transfer.
- Allow the Ctrl + Alt + Del shortcut on a specific type of device.
- Choose your favorite Top Menu display between transparency and solid.
- The number of graphical color bits.
- The Connection Timeout, the maximum duration (in seconds) a session remains active while waiting for a client to reconnect. 0 to disable timeout.
- Show or Hide Warning Messages.

- Enable or disable sounds.
- Choose your favorite background color.
- Add a logo to the background.
- Change the logon screen message and animated gif, as well as its display time in milliseconds.

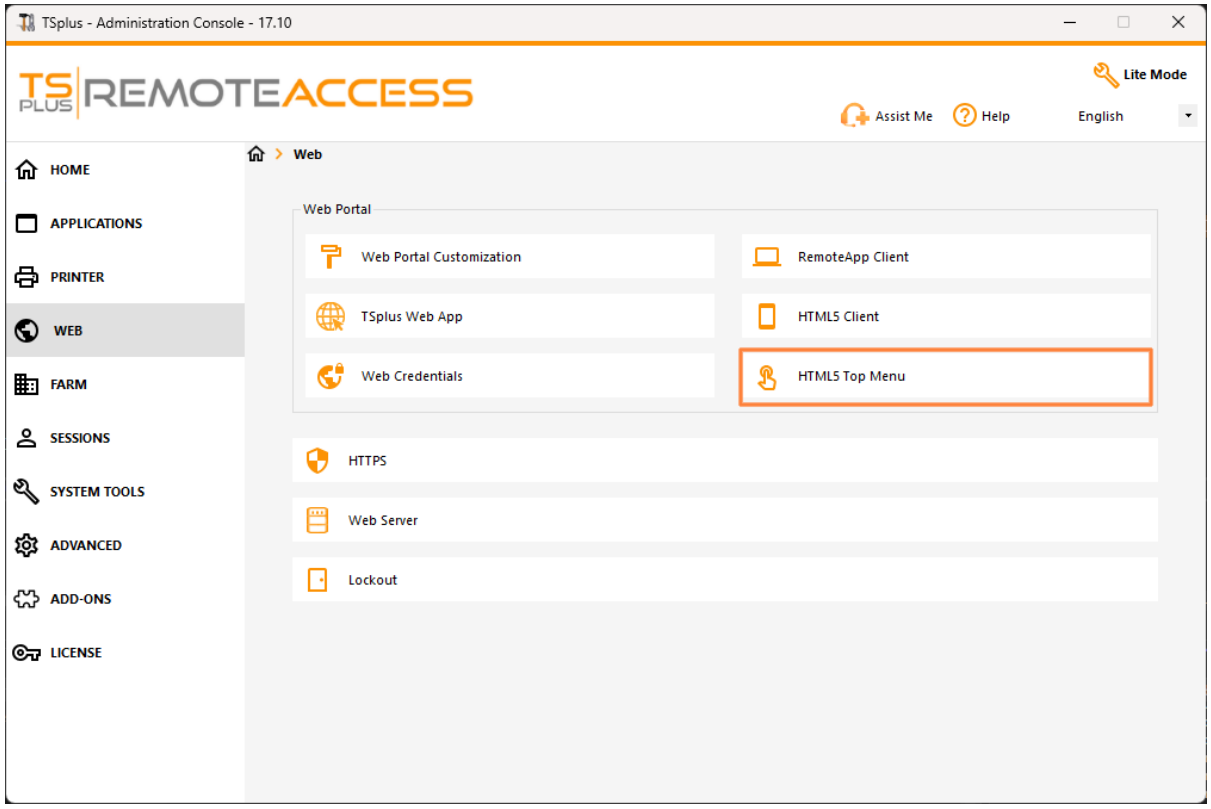
Smartphone and tablets Preferences:

- If the administrator uses the software keyboard, when it is hiding an entry field, the application is moved up and the user is still able to see what he is typing.

- The administrator can select a small, a medium or a large size for the mouse pointer or no mouse pointer at all. It makes intuitive for the user to navigate inside his application.

- He can also select the level of transparency for mouse and keyboard.

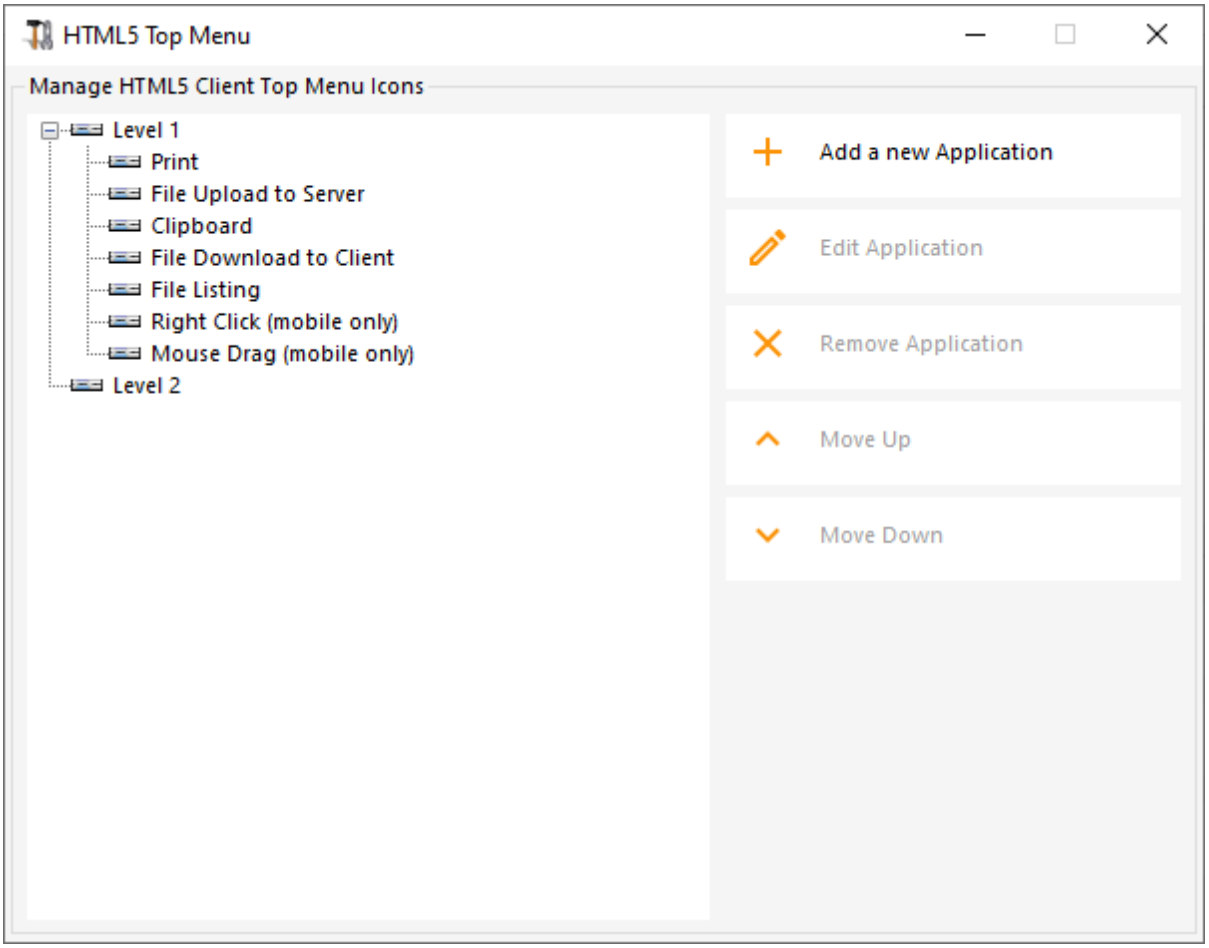
On the HTML5 Top Menu tab, you can add applications that will be displayed on the first or second level of the Top Menu in HTML5:



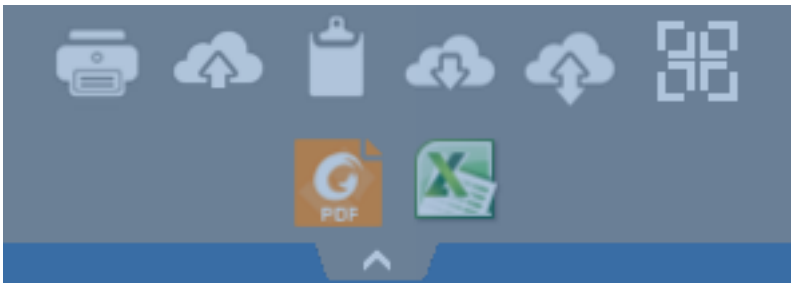
On level one, you can find the integrated HTML5 features: printing, file transfer and a clipboard. (For more information about these features, go to theses pages:

Universal Printer for HTML5, Using file transfer and Using Clipboard.)

On this example, Foxit and Excel are published on level 2:

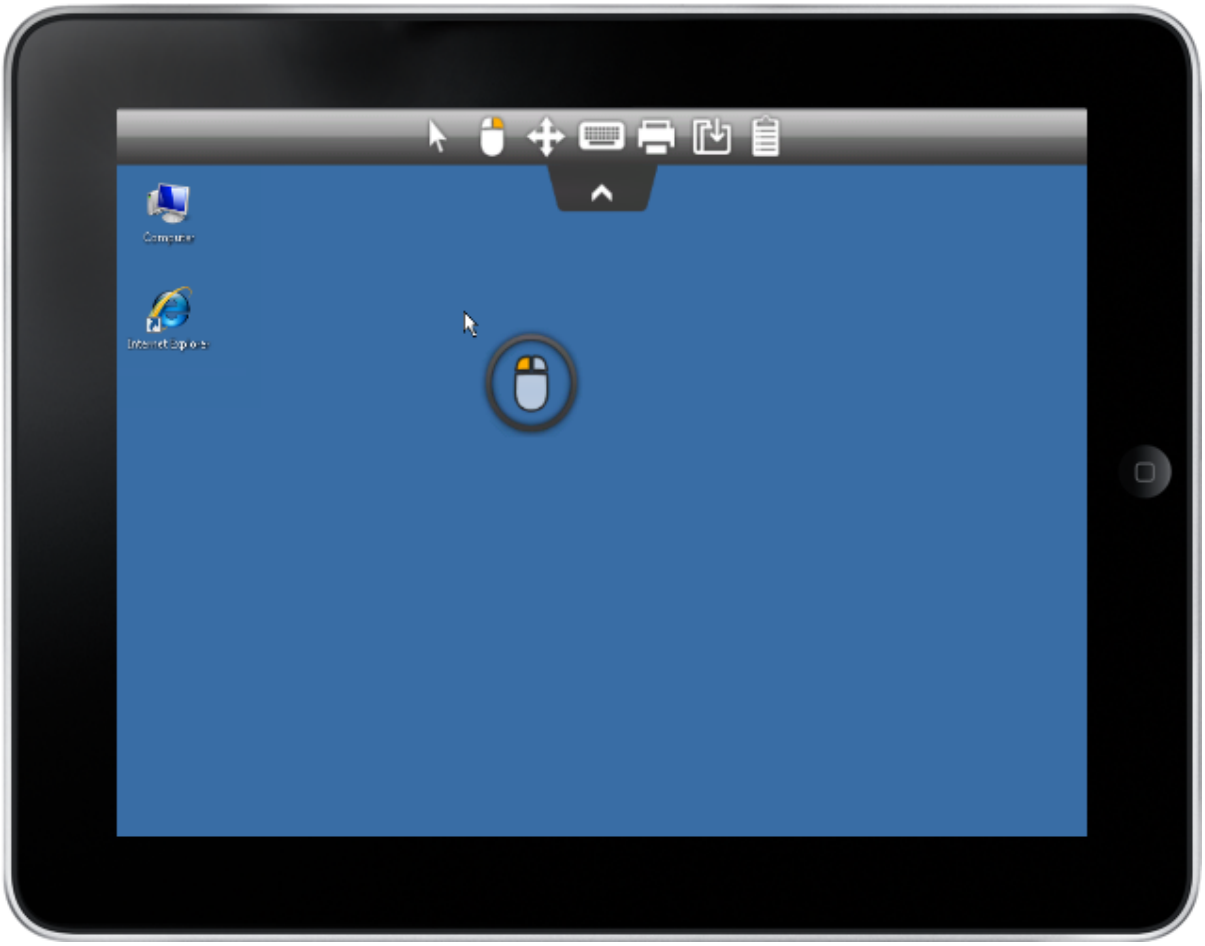


And can be found under the integrated features on the top menu into the HTML5 session:



Furthermore, the top-right icon allows you to switch your session to fullscreen.

Terminal Service Plus built-in HTML5 client provides the user a completely new menu on tablets and mobile devices. With this new menu the user gets an easy access to mobile keyboard and right click, but also to file sharing and to our unique Universal Printing feature!



Please refer to this documentation for how to use the mini mouse and keyboard.

Language selection

You can now change the language with the language button at the right of the top menu:



You can choose the language for the specific country you wish to on this menu:

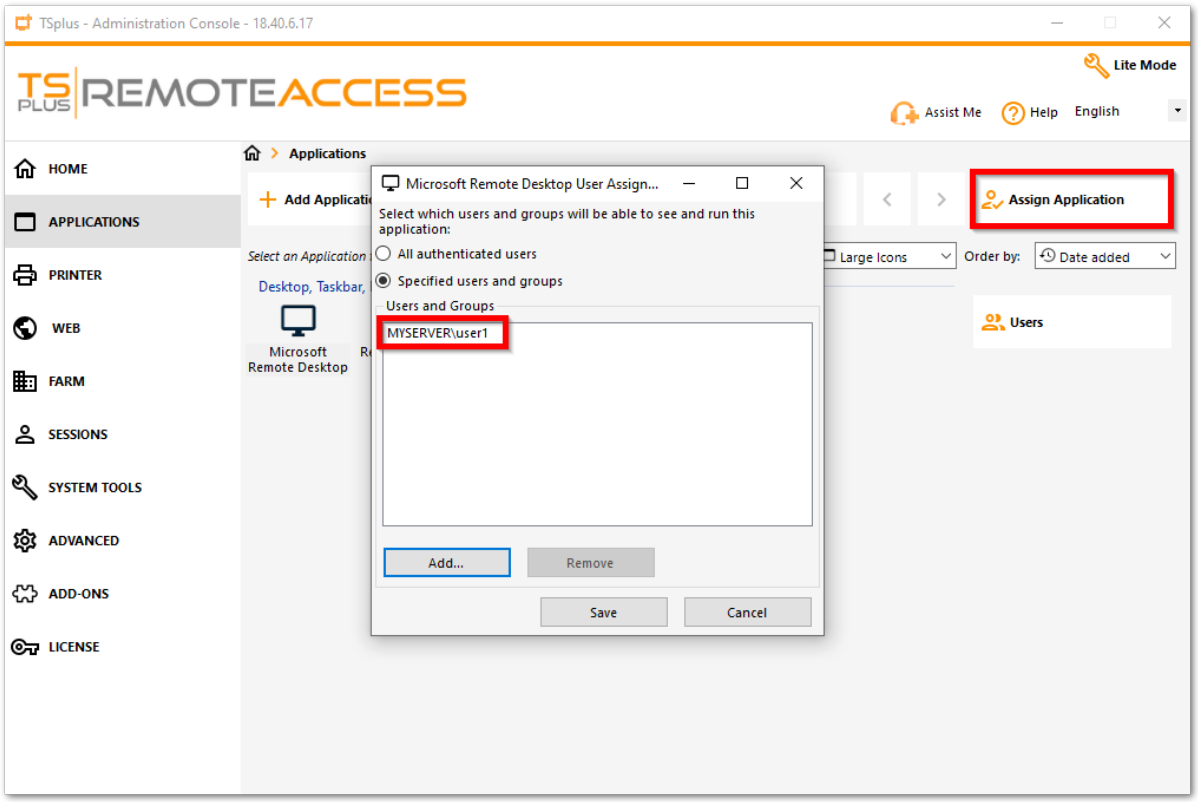
	Language	Locale	Value
◯	Portal	as_portal	
◯	Browser	as_browser	
◯	Gateway	as_gateway	
◯	Arabic	ar_ar	1025
◯	Belarusian	be_be	1059
◯	Bulgarian	bg_bg	1026
◯	Bengali	bn_bn	1093
◯	Bosnian (Cyrillic)	bs_cyrl_ba	8218
◯	Bosnian (Latin)	bs_latn_ba	5146
◯	Catalan	ca_ca	1027
◯	Czech	cs_cs	1029
◯		cs_cz	1029
◯	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

Remote Taskbar and Desktops themes

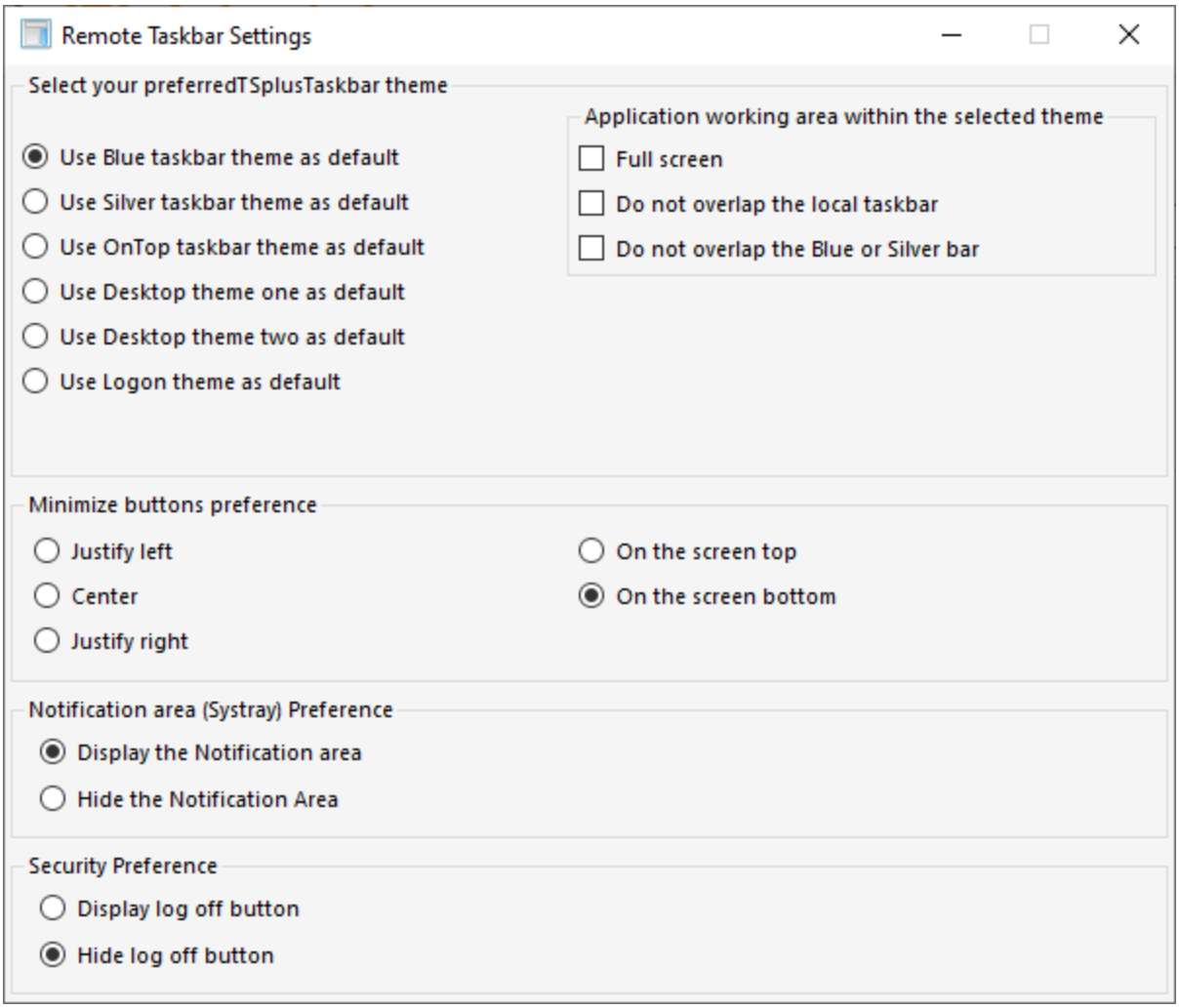
Administrator tools on the server

With the AdminTool, the Administrator can choose between 4 display modes when he assigns applications: The Microsoft Remote Desktop, The Remote Taskbar, The Floating Panel or The Application Panel. The Remote Taskbar, Floating and Application Panels are available for any connection method.

When you assign applications to an user, you can enable the TSplus remote taskbar. The user can launch remote applications with one click on the TSplus taskbar and still have the full local Desktop available. You can assign the Remote Taskbar to your users or groups by double-clicking on it or by selecting it, then clicking on the “Assign Application” tile:



The Administrator can easily decide what will be the default Remote Desktop theme the user will see when opening a session. Select the TSplus Remote Taskbar, then click on “Edit Application”:



- Only the Administrator can choose the themes for his users.

- He can choose to display the maximized applications in full-screen mode or not to overlap the TSplus taskbar as well as the Silver or Blue taskbars.

- Minimized buttons position on the taskbar can be changed (on top of the screen, on the bottom, on the right, the left side, or in the center).

  The administrator can even decide to display it on top of the user screen instead of the default bottom side.

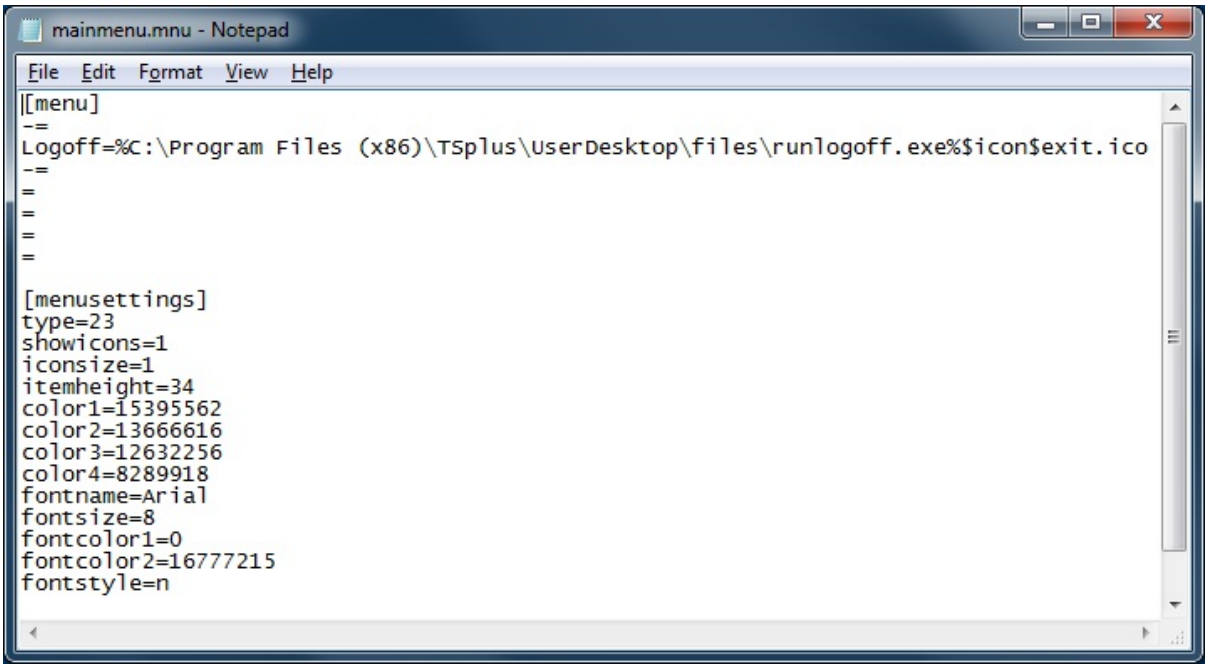
- Systray icons can be hidden by ticking the “Hide the Notification Area” circle.

- Since TSplus 12.60 version, the Logoff button can now be hidden.

By editing the users menu, the Administrator can add/suppress applications and functionalities.

Customization of the users menu is easy.

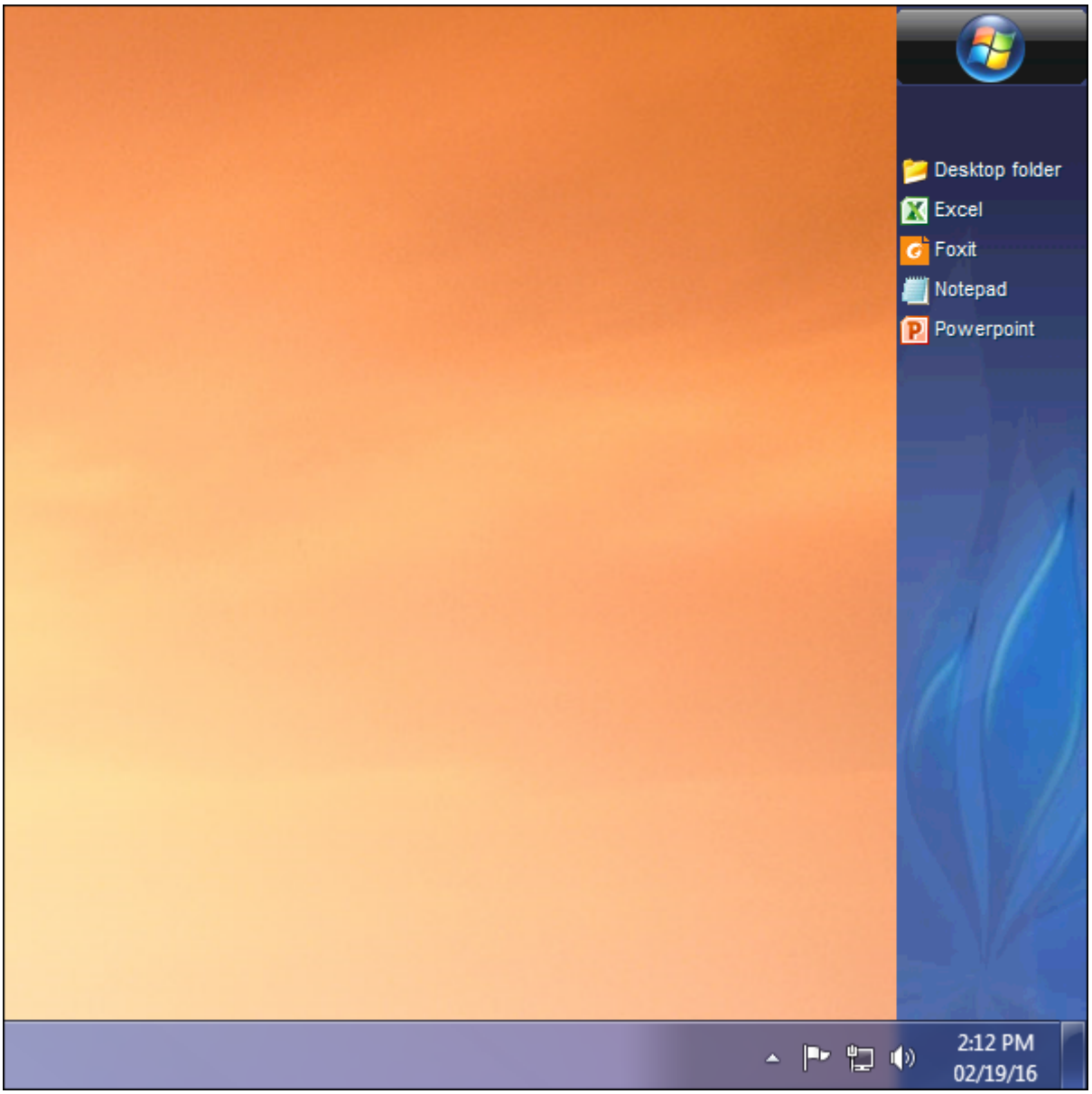
The content of the users menu (located in Program Files/TSplus/UserDesktop/mainmenu.mnu) is modifiable by the administrator using Notepad:



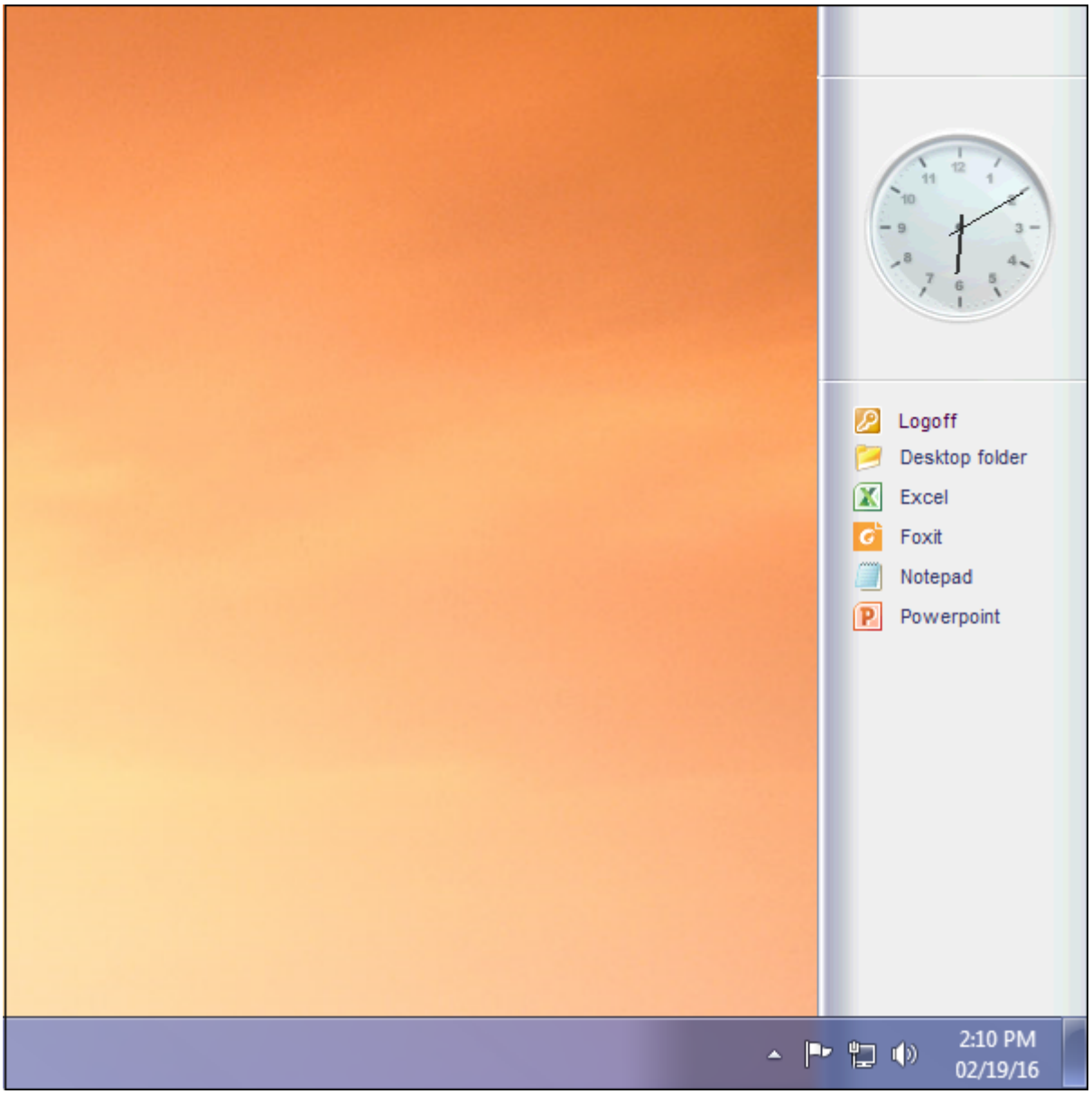
On the applications tile of the AdminTool the administrator can select 3 different styles of Remote Desktop TSplus Taskbar.

The user can launch remote applications with one click on the TSplus taskbar and still have the full local Desktop available.

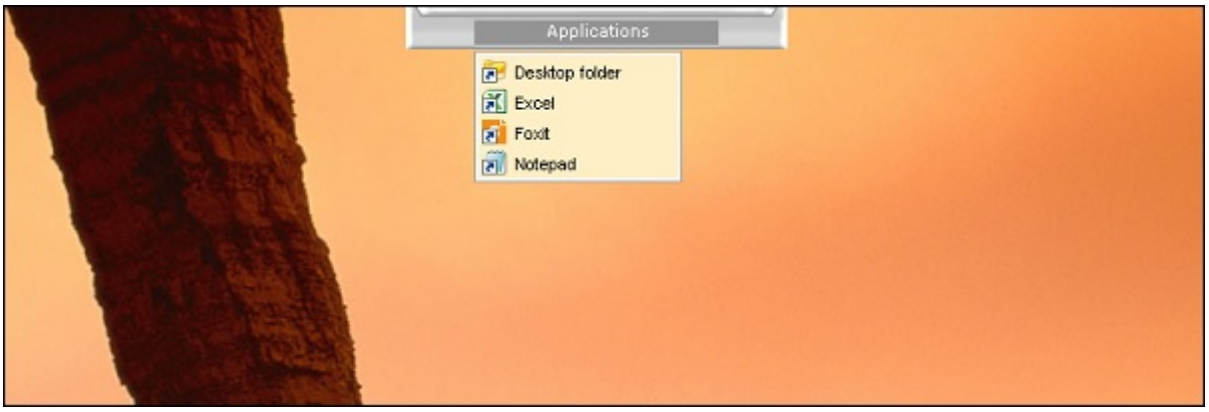
Right-side Blue theme taskbar



Right-side Silver theme taskbar



On Top taskbar



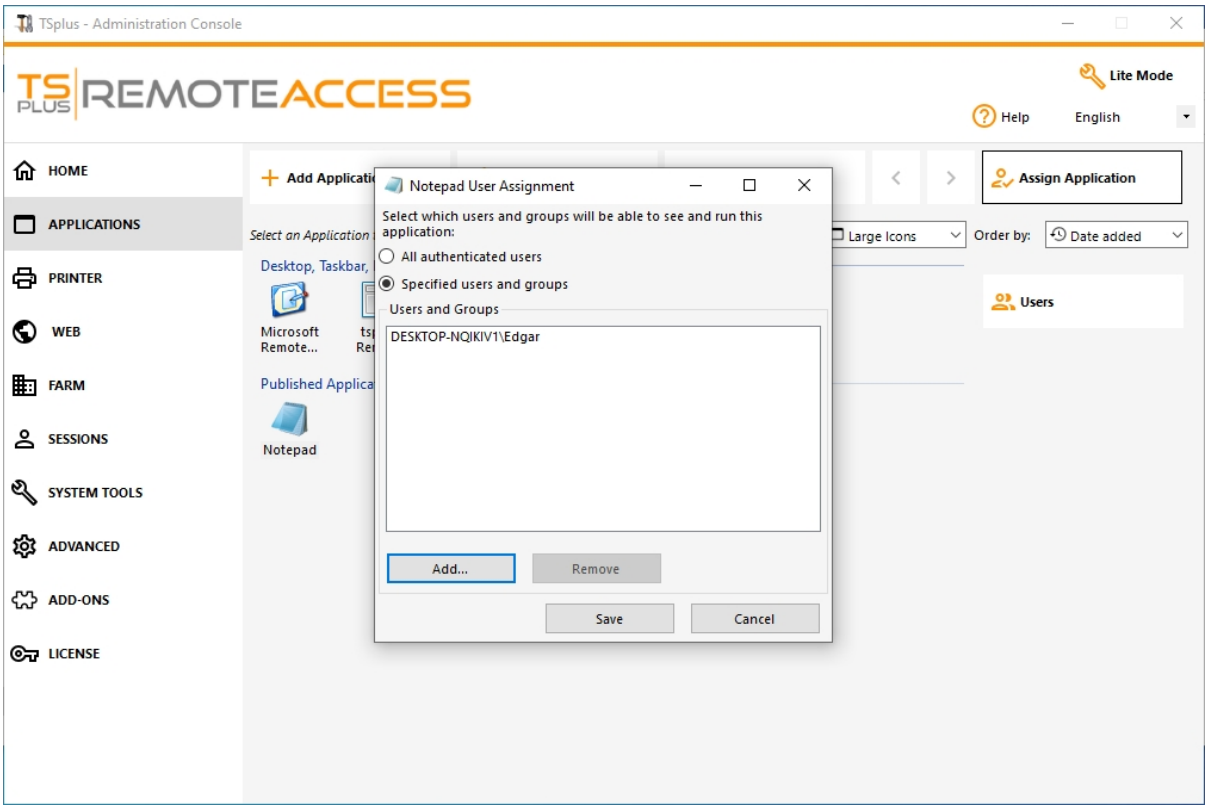
Back To Top

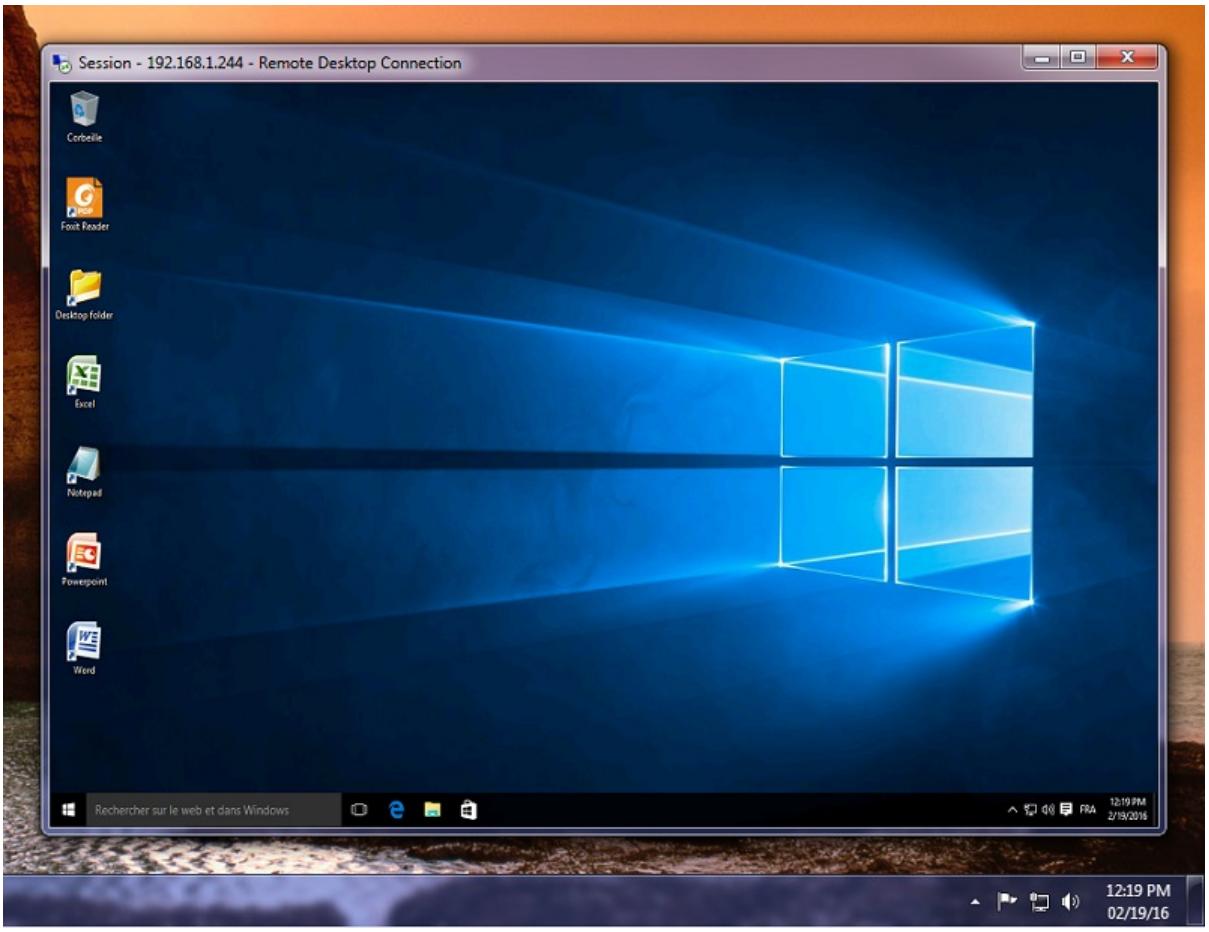
With the AdminTool, the Administrator can easily decide what will be the default Remote Desktop theme the user will see when opening a session. He has the choice between 4 different styles of full screen Remote Desktop. The standard Microsoft Remote Desktop can also be used if preferred.

Because these TSplus Desktops are full screen desktops, the user's display is entirely filled when a session is opened from dedicated thin-clients, any RDP based client, or accessed from a web page or TSplus Remote Desktop clients.

There are benefits over a standard Remote Desktop. It enhances the server security (no START button neither full control of the Desktop).

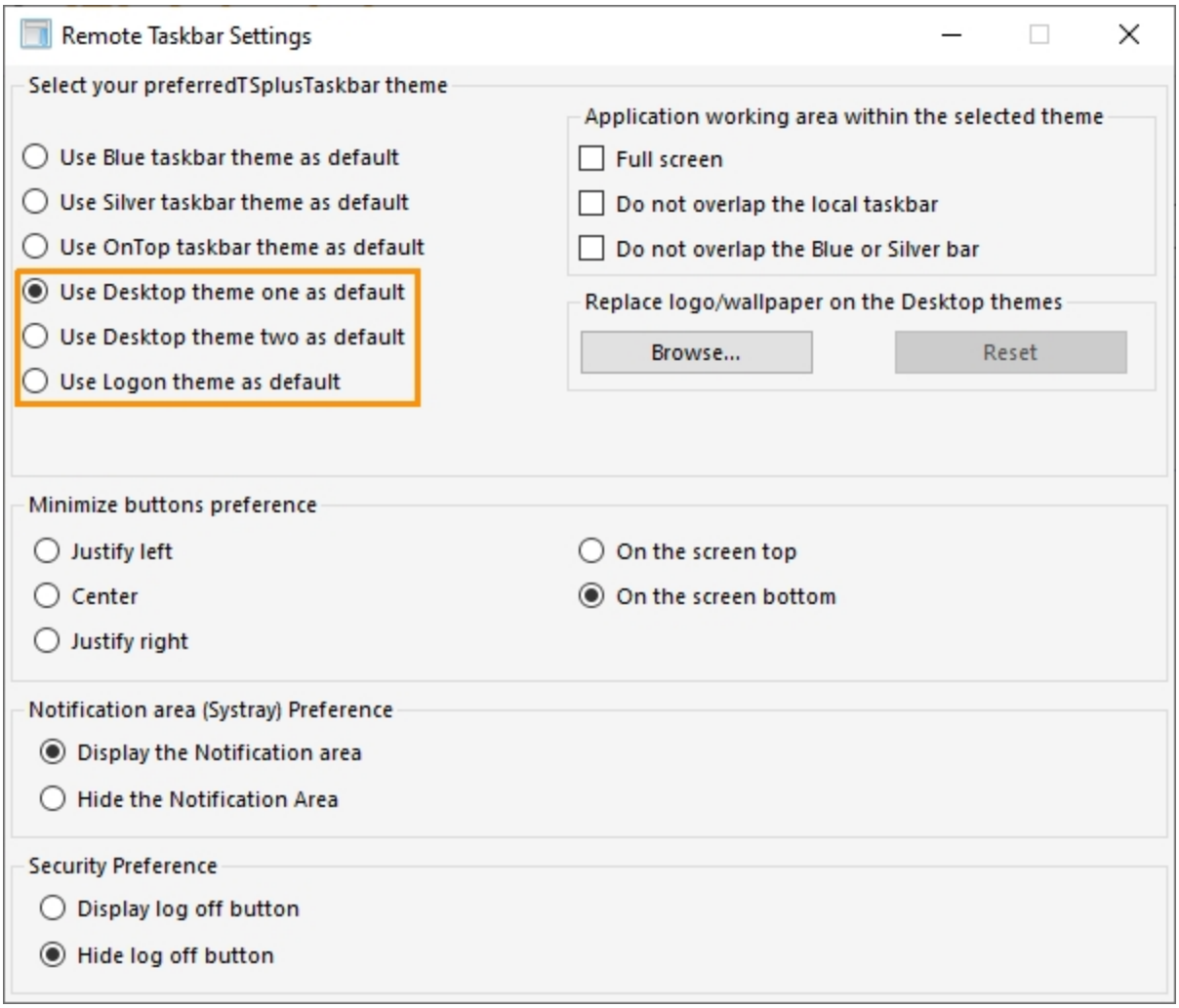
Standard Microsoft Remote Desktop





- The user has a complete desktop including Start Button and full control of the desktop
- To assign to complete desktop, just assign the Microsoft Remote Desktop application.

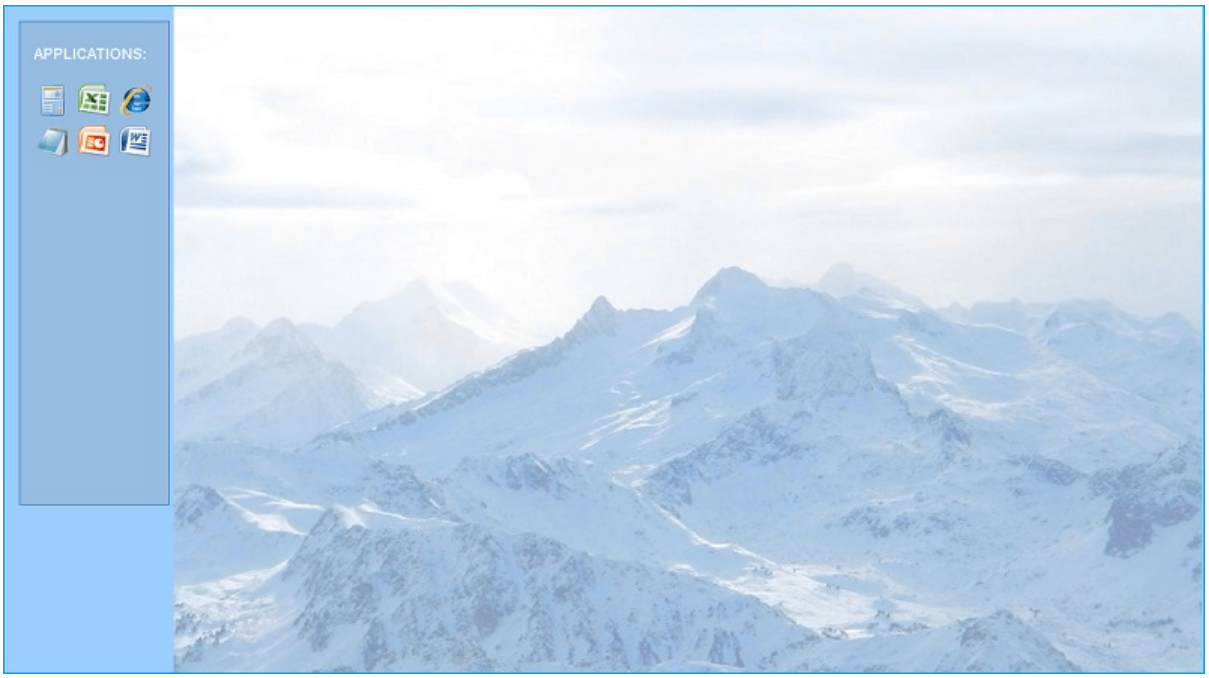
In order to change the Desktop themes, you will have to assign the TSplus Remote Taskbar and choose between the 3 suggested themes:



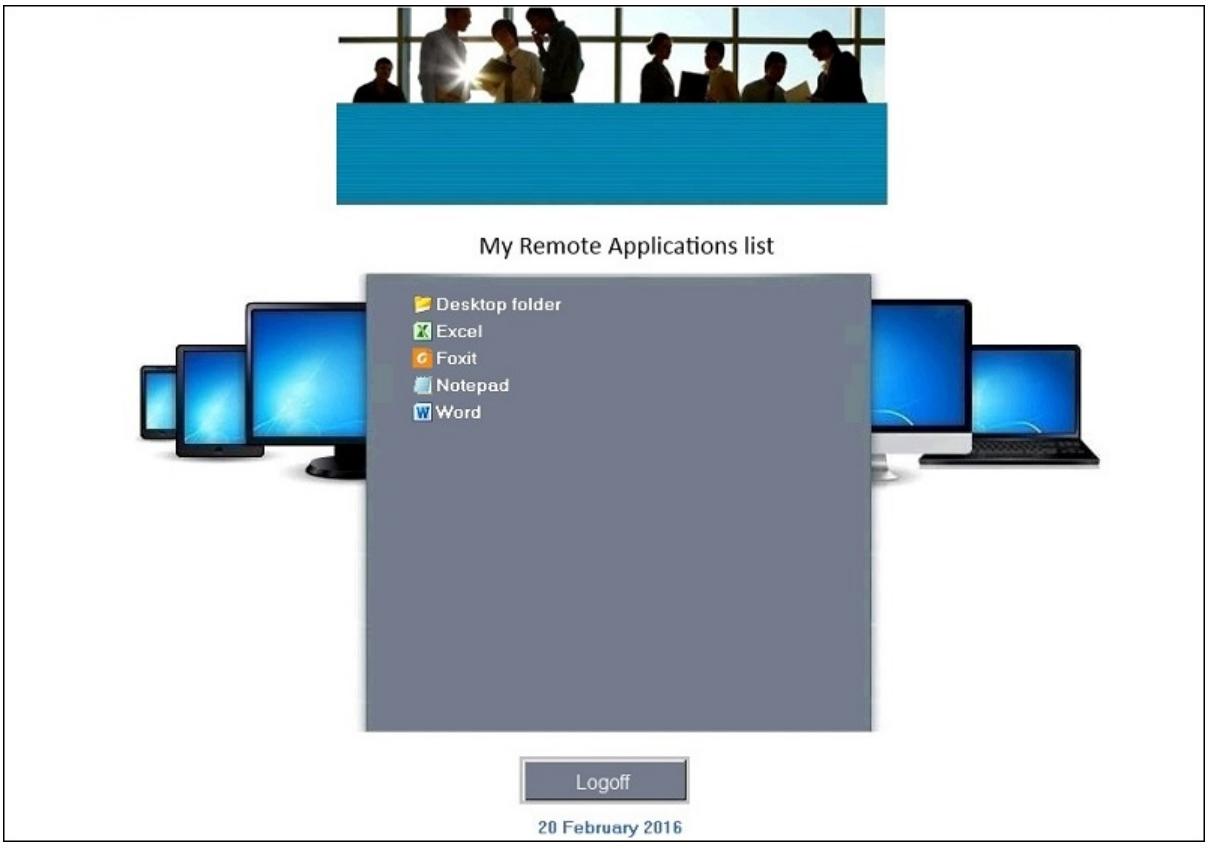
TSplus Desktop theme one



TSplus Desktop theme two

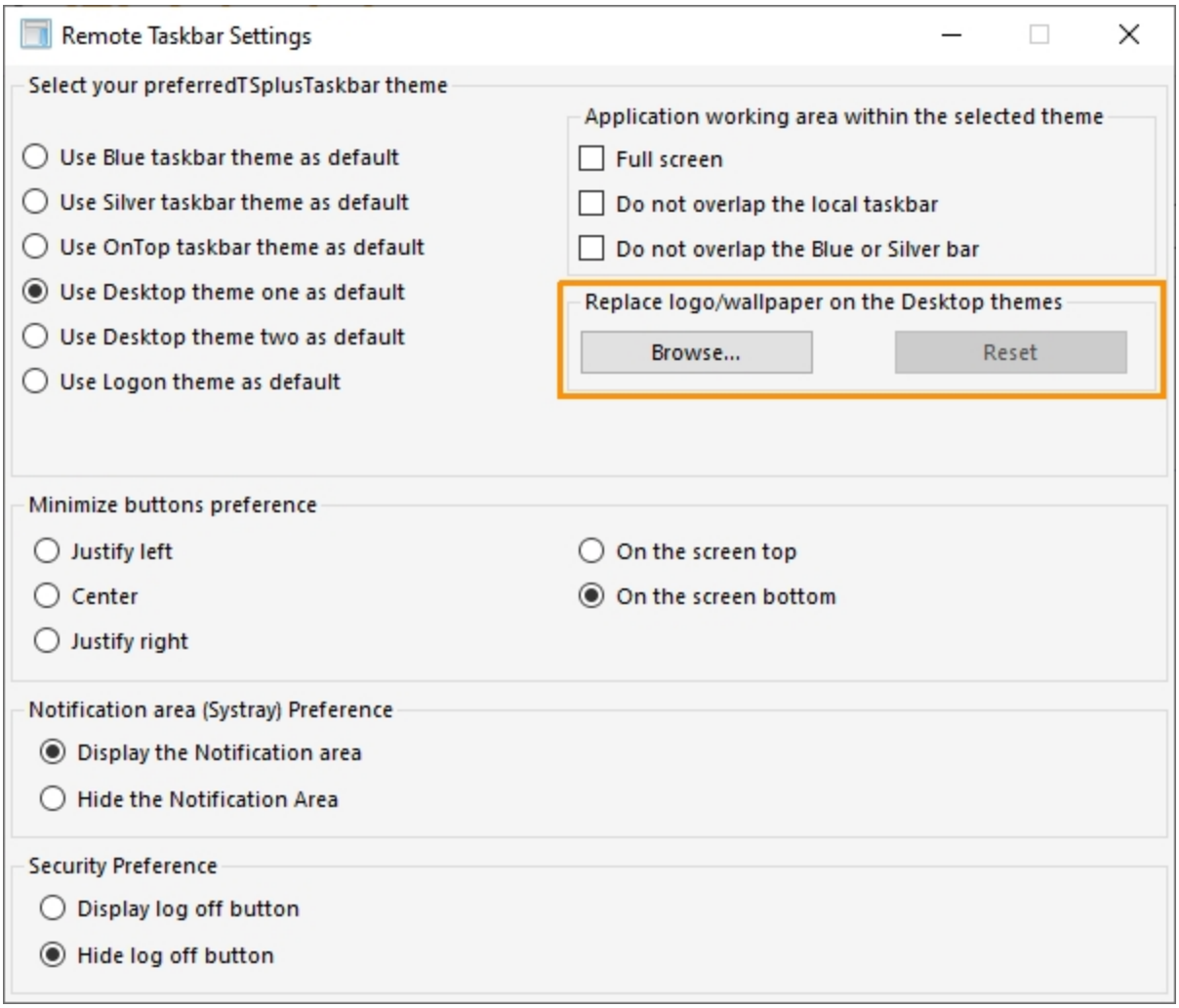


TSplus logon theme



Customized theme

For each theme, the Administrator can customize it and for example, display the Corporate logo. He can also add his own Desktop wallpaper by selecting one of the Desktop themes and by clicking on the Replace logo/wallpaper button to select your .jpg file, for example:



- You can add your own Desktop wallpaper by selecting one of the Desktop themes and by clicking on the Replace logo/wallpaper button to select your .jpg file, for example:



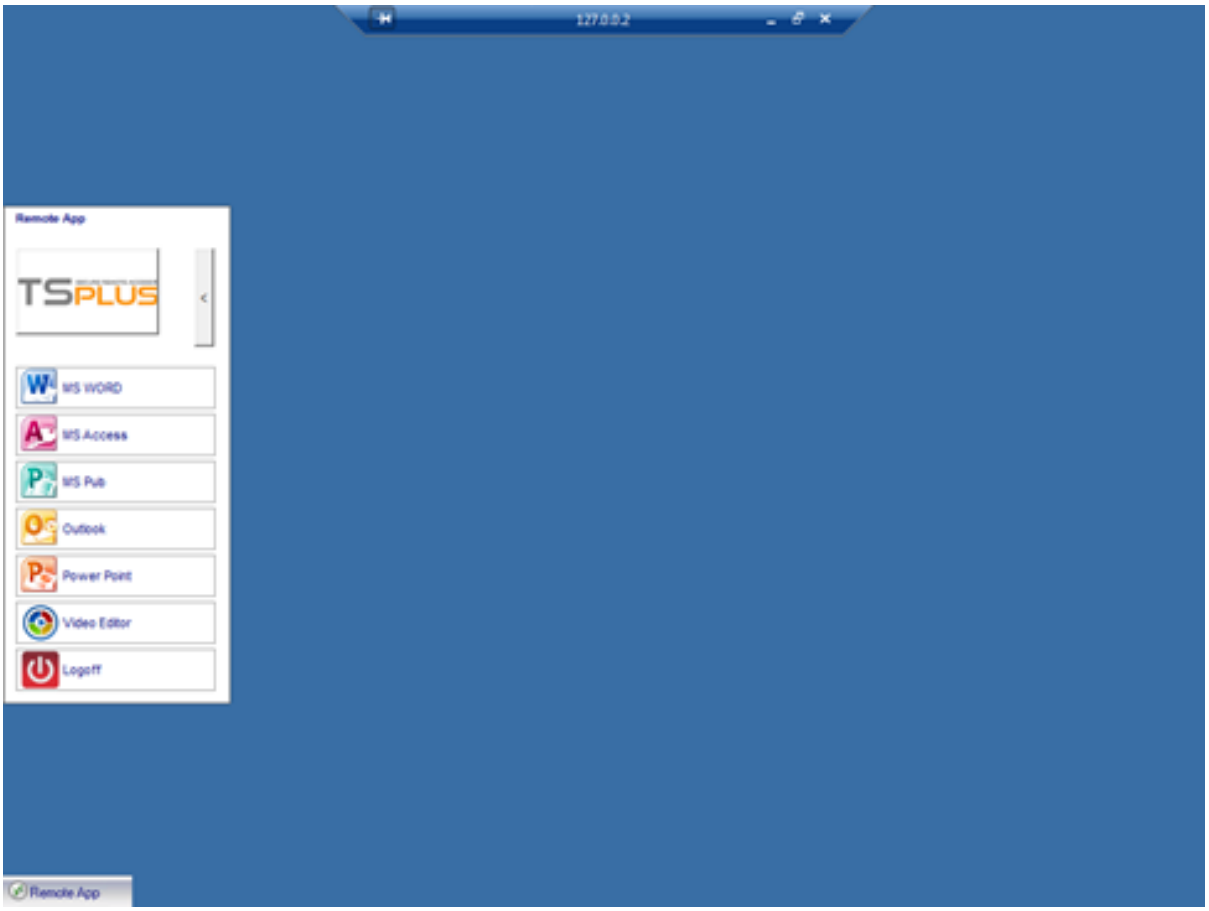
RemoteApp On Client Feature

In the past the generated TSplus Portable client was the usual method for a user to start applications. The 10.50 release introduces **an icon in the notification area** which gives to each user the list of all of his Remote Applications. Within this application list, the user can select the one he wants to start.

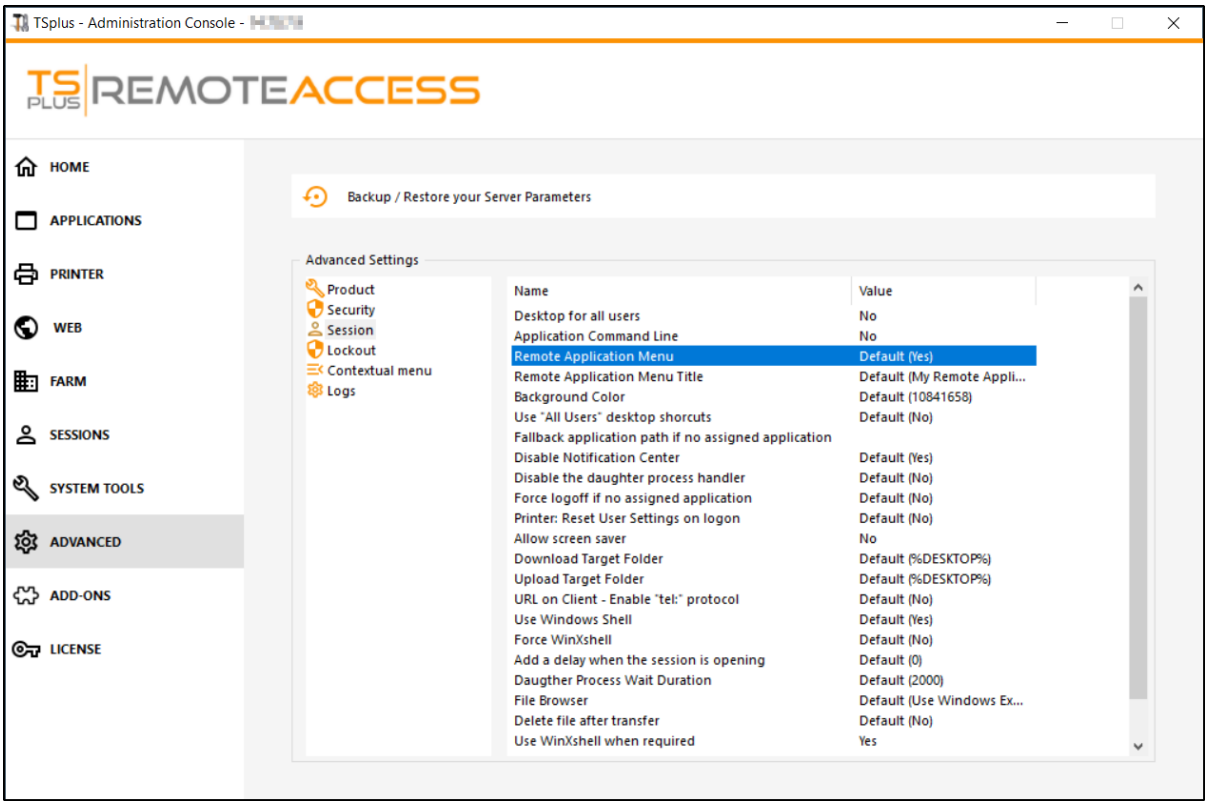
This is a new way for administrators to deliver remote applications (referred to as “RemoteApps“) to their users. Specifically, RemoteApp On Client enables a straightforward publishing process that allows applications installed directly on the server to be provided to users, allows RemoteApp programs to run side-by-side with local programs, and offers integration with a custom “launcher” application to make it simple for users to find and launch RemoteApp programs.

The user Application list will also appear in the **Start menu** under **All Programs** in a folder called **My Remote Applications**. To deploy this new amazing TSplus capability is simple: The Administrator have generated new connection clients and allowed it with the AdminTool. This guide will explain step by step what will happen when the administrator will enable this new feature and will deliver to his users a new generated connection client.

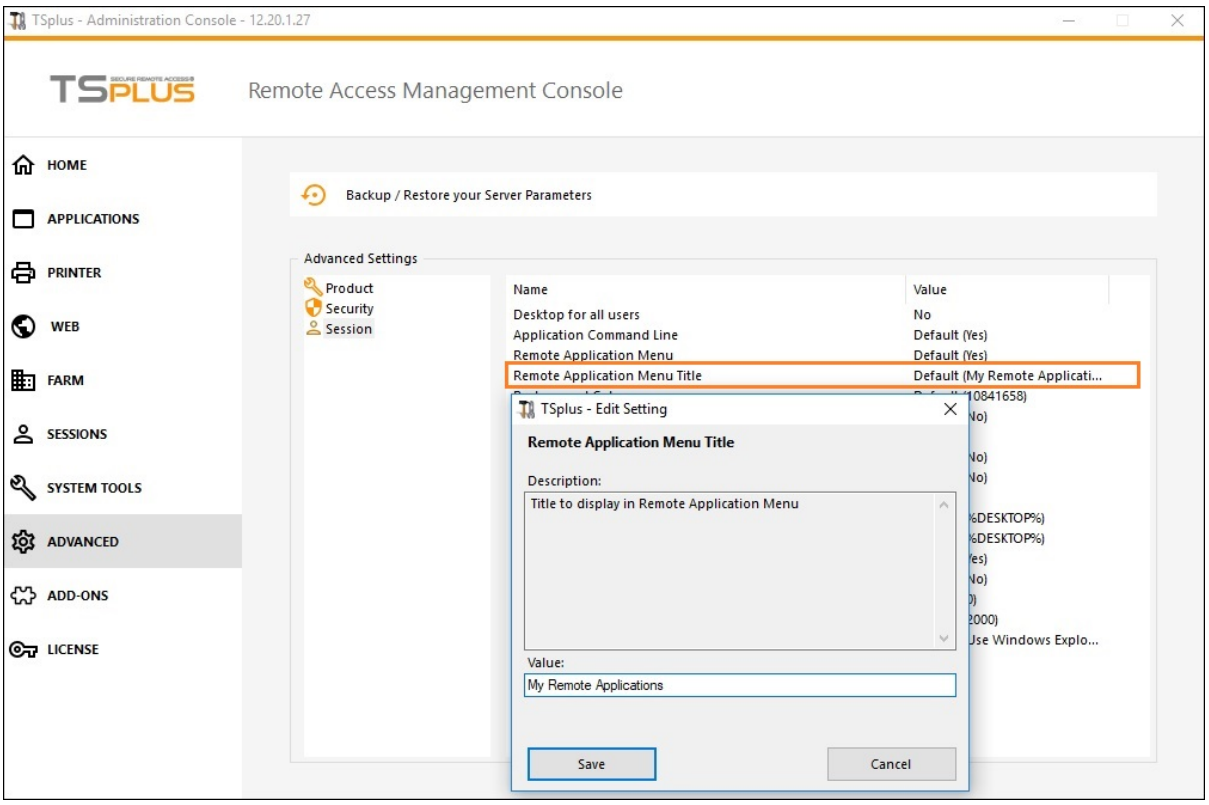
Example: The user “Laura” is using TSplus to access her remote application. To do so, she is using a generated client named **LauraPortableClient.exe**. When she runs it on her PC she gets the following result:



However, the administrator did provide her a new one, created with the TSplus 10.50 release. She will have to run it at least once to benefit from the new **RemoteApp On Client feature**. When the administrator is adding/removing application to a user, such change will be set on the server side at the next logon. It means that the current session will not reflect such modification. The Advanced tab of the AdminTool has an option to enable or to disable this RemoteApp On Client feature, by default, it is enabled:

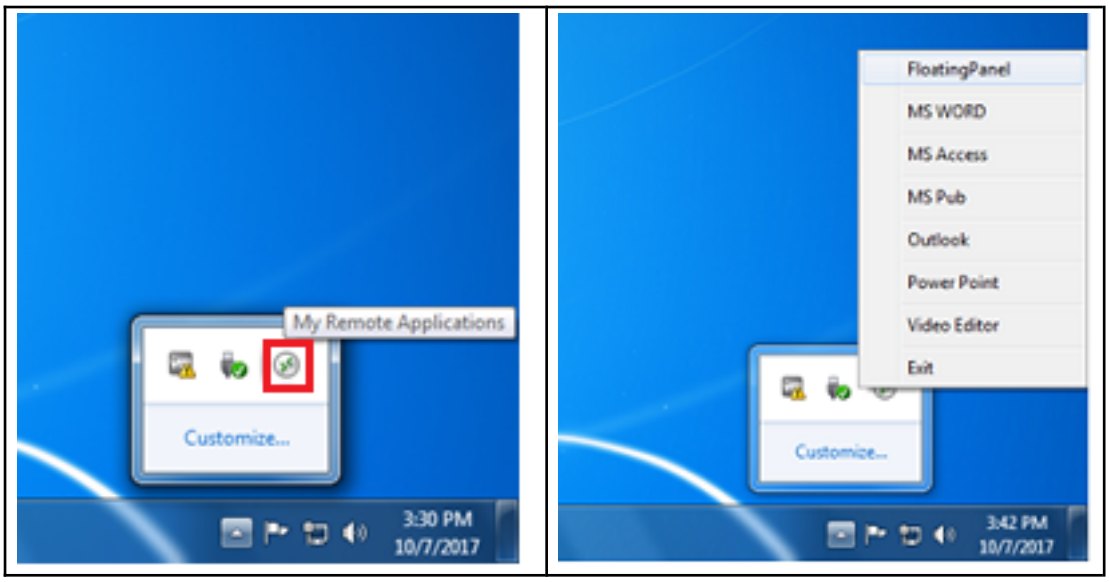


You can change the menu name as you wish, by clicking on the Remote Application Menu Title below, and adding it on the value box:

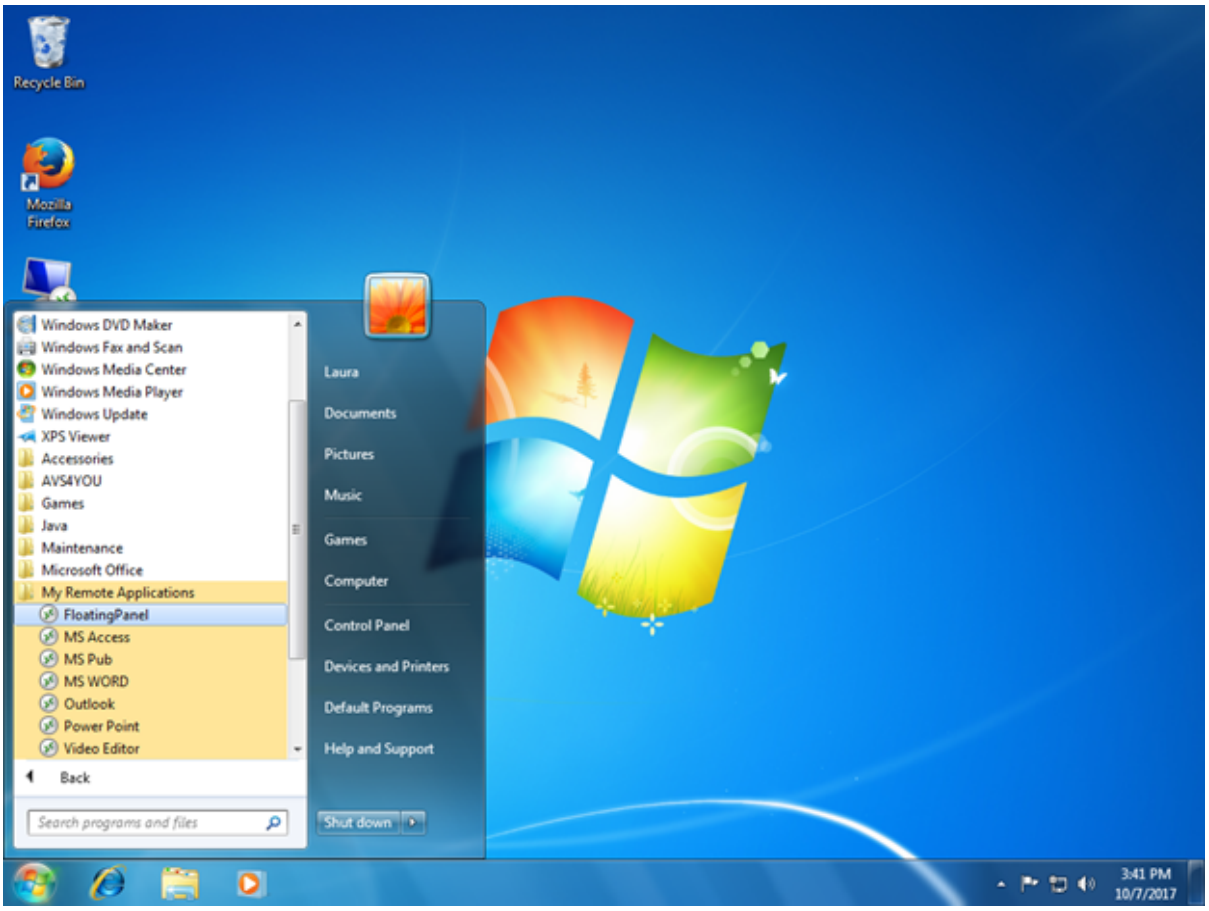


What will happen on her PC when she will run once her new generated client: She will see a new icon in the Notification Area of her local task bar.

My Remote Applications new icon	Application list menu

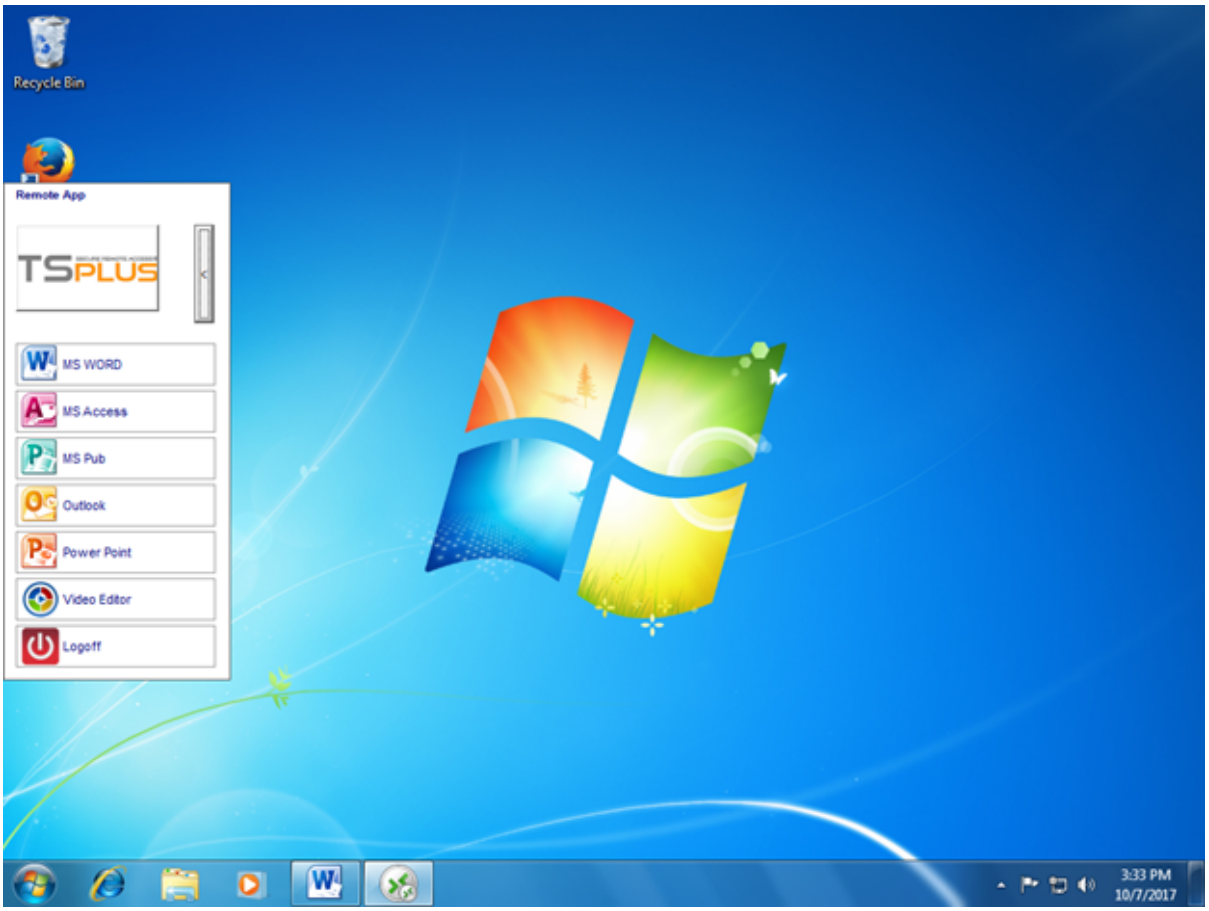


She will also see a new entry within her Start menu Program list named **“My Remote Applications”**:



She will now be able to select one of these listed applications and to start it as a RemoteApp. She will not need to use the provided LauraPortableClient.exe generated client.

For example, if she selects the Floating Panel, she will get this result:

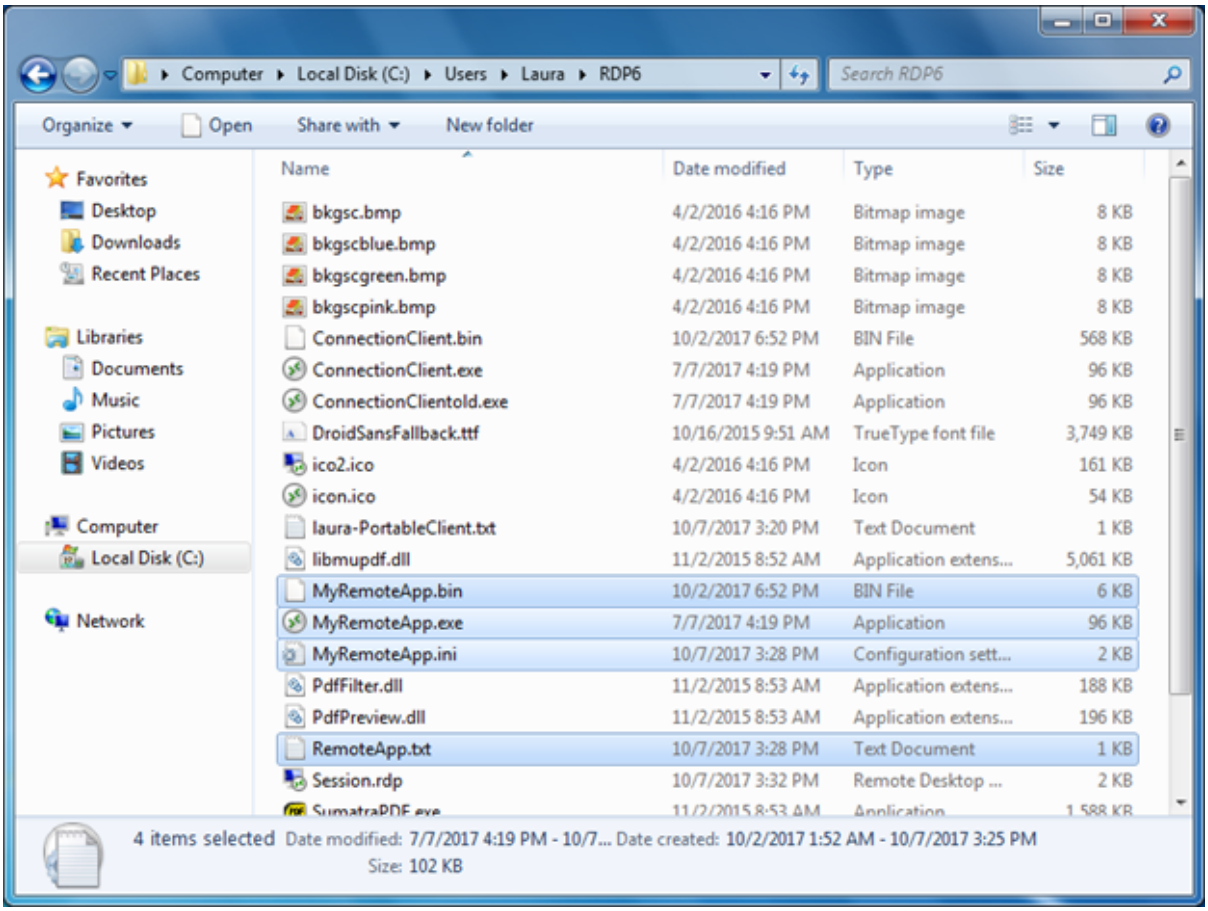


Technical background behind this new technology.

The new generated client of the 10.50 release is adding several files within C:\Users%UserName%\RDP6 folder of the local PC's user profile.

MyRemoteApp.exe and MyRemoteApp.bin are the program codes which are started to create the new icon in the notification area and the new entry in the All Programs list of the Start button.

MyRemoteApp.ini is a file received from the server. It is providing the details of each application which are assigned to this user on the server side. It is updated at each new connection to the server. Usually, it takes 30 secondes after each logon to receive this file from the server. RemoteApp.txt is providing the name of the last generated client started on this PC.



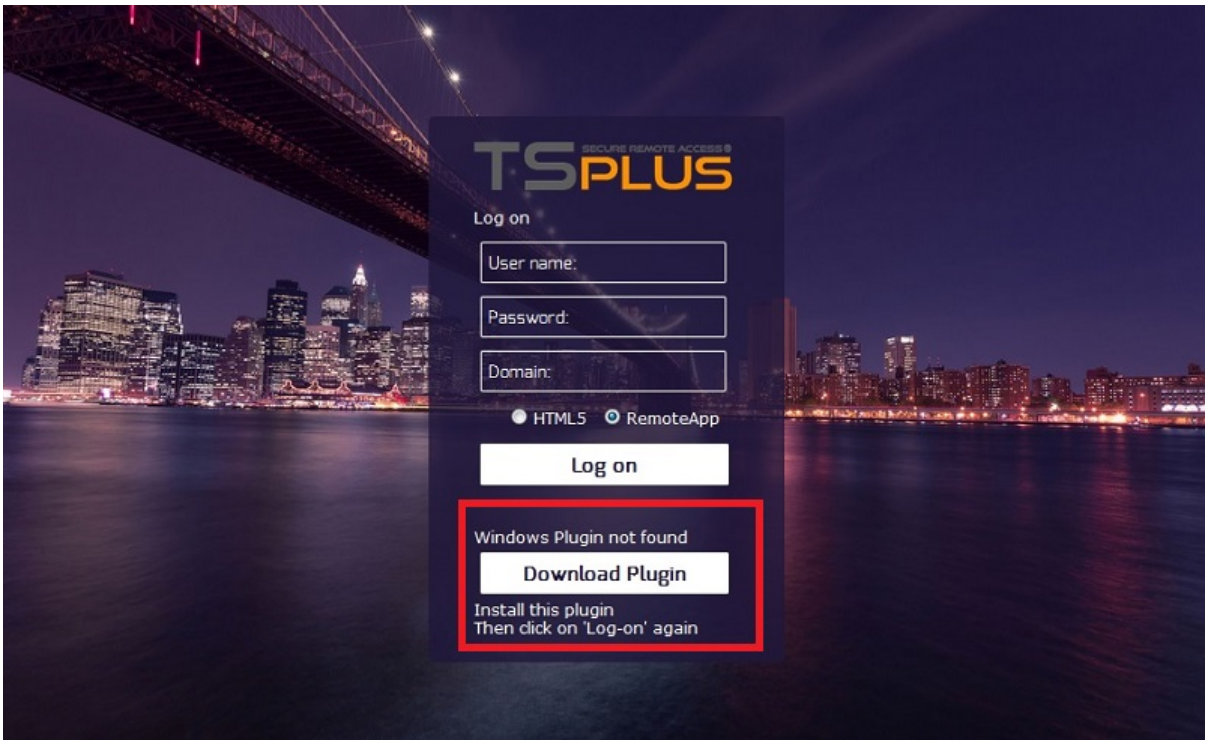
Comments:

If the user has administrator right on his own PC, **MyRemoteApp.exe** will be started automatically at each reboot and the Start button will be updated too. Else, the administrator must run once the new generated client “As Administrator” to enable the new feature. Doing so he will create the proper registry entries in HKLM. If a user is connecting to only one server, this new system is perfect. However, if he is using several connection clients to open sessions on different servers you should keep in mind that the file **MyRemoteApp.ini** will be updated with the values of the last connection. It can be confusing for the user and in such deployment case we recommend no to use this new feature.

Remote App Plugin

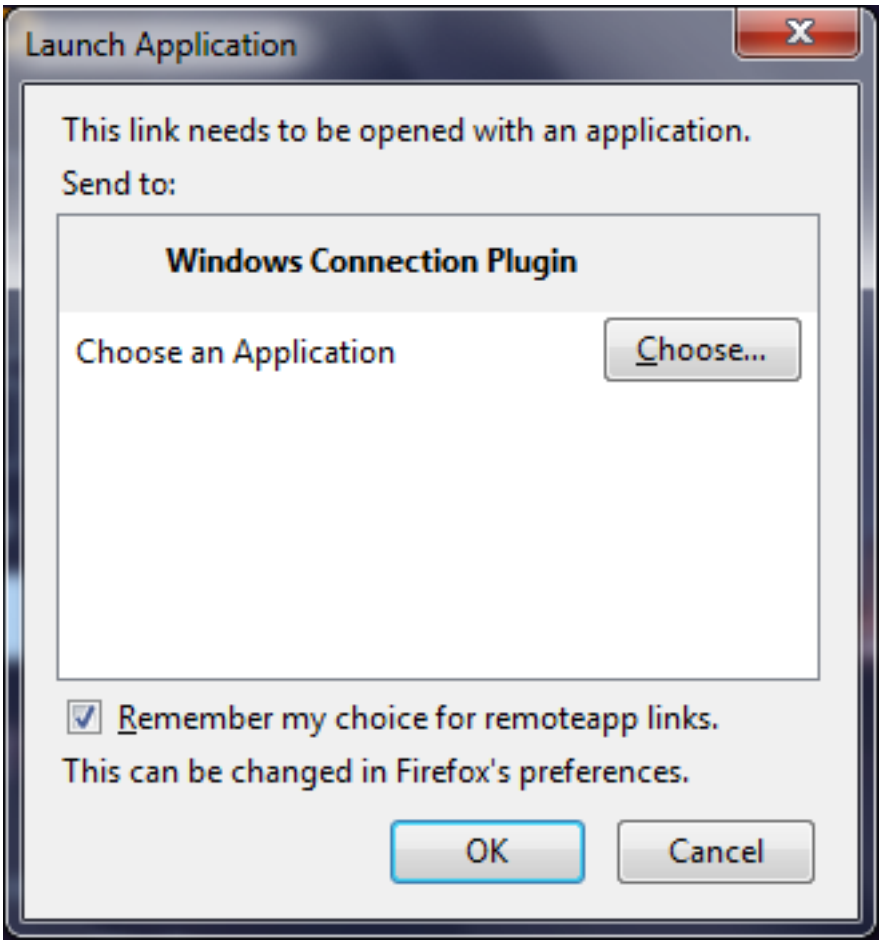
Since the new 8.40 version of TSplus, there is no need anymore for a Java plugin to be installed on the client browser.

You can now access the Windows RemoteApp client by downloading and installing a small Windows plugin via the Web Portal. This operation is fast and needed only once per client.



You can also install it on the C:\Program Files (x86)\TSplus\Clients\www\RemoteAppClient folder.

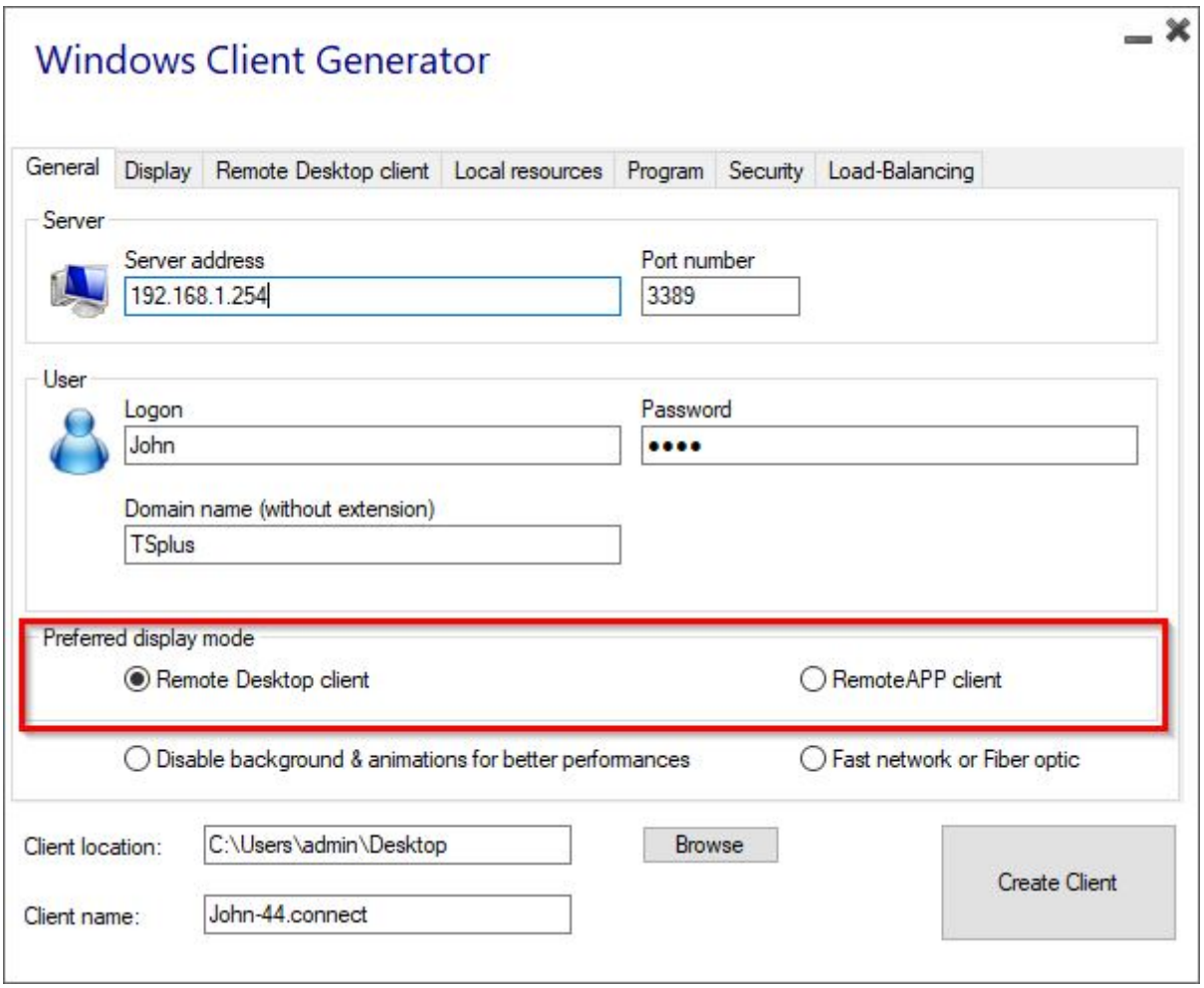
When using firefox, this message will be displayed on your first connection. If you choose the ‘’remember my choices’’ option, the notification will be disabled upon future connections



Note: Since TSplus 12.40, RemoteApp client setup and the The Client Setup Program have been merged and can be deployed with one single setup - so if you download the RemoteApp Client Setup, there will be no need to download the Connection Client one.

RemoteApp Connection Client

You can choose between 2 display modes on the general tab of the client generator:



###RemoteApp connection client

The RemoteApp connection client does not depend on the transparency color settings.

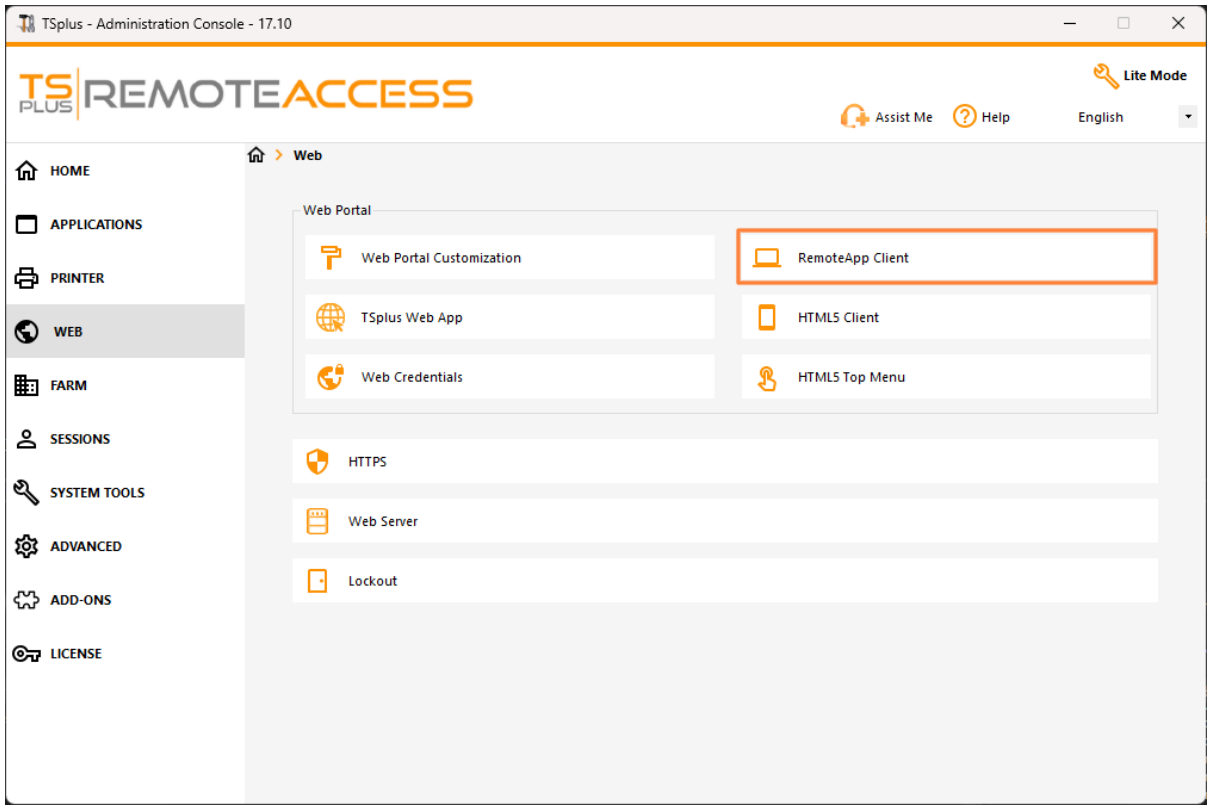
This allows for perfect application display as well as native Windows behavior.

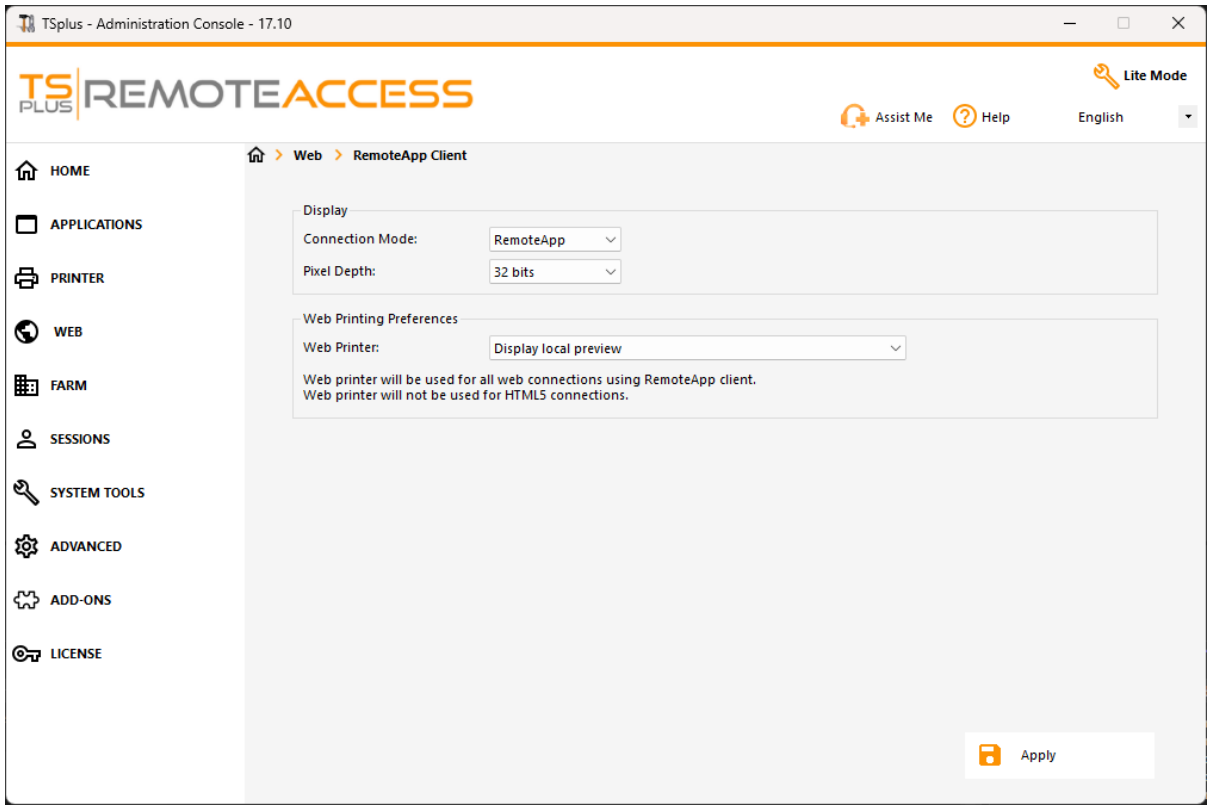
- On the Client side, the installation of RDP6 or above is required.
- On the Server side, TSplus must be installed on a machine running Windows 7 to Windows

Server 2019.

Note: RemoteApp is not supported on Windows 10 1803 et 1809 Home Windows 2019 Essentials Editions.

You can change the RemoteApp client display and Printing preferences on the Web tab of the Admintool:





Minimized applications can be found directly inside the Windows taskbar, like a local application.

In this example, Firefox and Paint are launched locally; Notepad, Word and Foxit are launched remotely.



For the Remoteapp connection client, you can choose to publish one unique application to be launched seamlessly at the user's logon. You can also publish applications with the TSplus Remote Taskbar, the Floating Panel or the Application Panel.

Run Windows client under Proxy environment

Usually the SSH package support HTTP(S) proxies and this should be sufficient to overcome most known proxies.

However, there are existing very difficult cases, where the proxy environment can not be properly recognized, is hidden from third party software or the target servers are behind reverse proxies.

For such difficult cases the software contains Non-SSH solution called “Rescue mode”.

If you can establish HTML5 connection, then you can be sure this software will help you to establish native socket connections through Websocket(FF, Chrome, Opera, IE10 etc) or XHR (IE6-IE9).

Be careful, some proxies allow Websocket/XHR traffic only via HTTPS layer, so use https address instead of http.

If proxy does not ask for proxy authentication and you can access pages via browser:

1. Open http(s)://yourserver.com__/software/html5/jwres/__
2. Wait for successful connection (and authorize Java execution if asked)
3. Click on the red text “open the link” to open the working web access page
4. Use Windows client access as usual

If proxy requests proxy authentication and you can access pages via browser:

1. Open http(s)://yourserver.com__/software/html5/jwres/__
2. If the proxy requests for authentication for java applets, press “cancel”
3. Click on “Download LocalWebserver”, and execute it after successful download, that will start local http server on port 18888
4. Click on “Force Applet loading from http://localhost:18888”, this will reload the page with loading of jars from local http server
5. Wait for successful connection
6. Click on the red text “open the link” to open the working web access page
7. Use Windows client access as usual

Securing a TSplus server

Overview

Securing any server is a never-ending story where every expert could add another chapter.

TSplus benefits from and is compatible with existing security infrastructure in a company (Active Directory, GPOs, HTTPS servers, SSL or SSL telecommunication systems, VPN, access control with or without ID cards, etc).

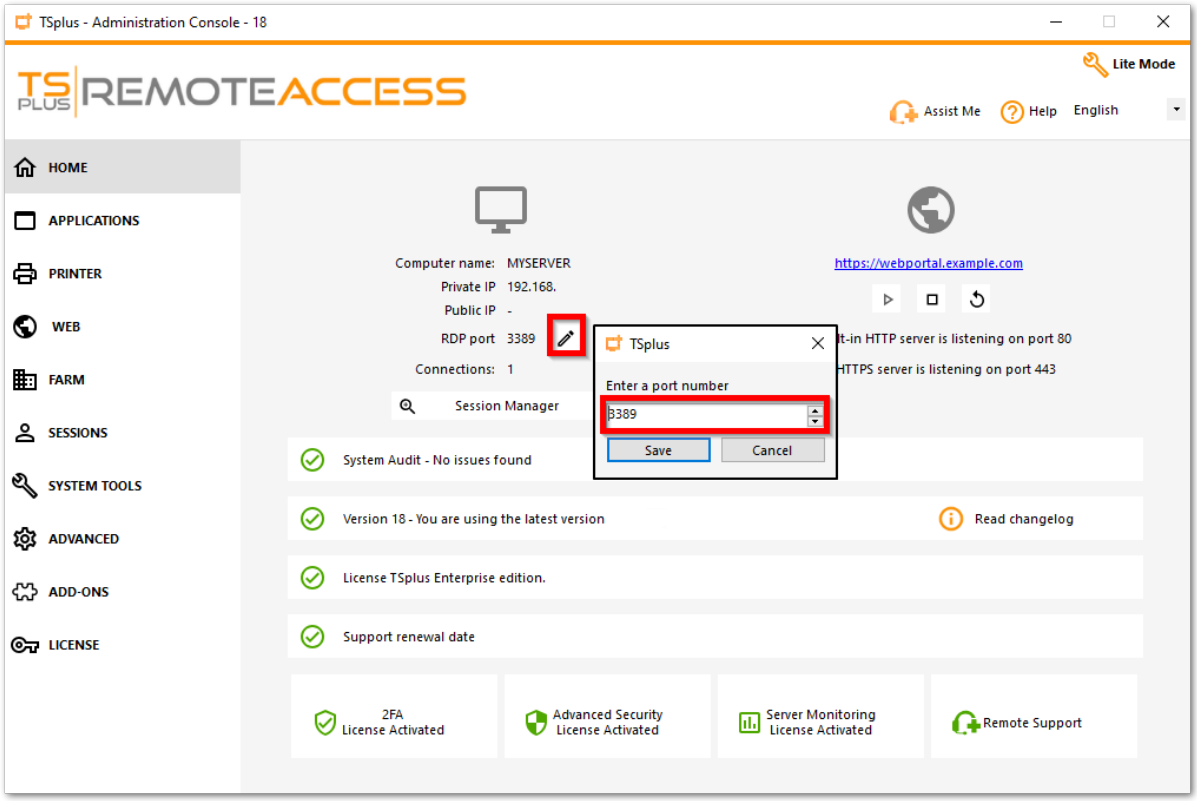
For customers who want to easily secure their servers, TSplus offers a set of simple and effective ways to enforce good levels of security.

With the AdminTool, you can select a different TCP/IP port number for the RDP service to accept connections on. The default one is 3389.

You can choose any arbitrary port, assuming that it is not already used on your network and that you set the same port number on your firewalls and on each TSplus user access programs.

TSplus includes a unique port forwarding and tunneling capability: regardless the RDP port that has been set, the RDP will also be available on the HTTP and on the HTTPS port number!

If users want to access your TSplus server outside from your network, you must ensure all incoming connections on the port chosen are forwarded to the TSplus server. On the Home tab, click on the pencil button next to the “RDP Port”:



Change the RDP port and save.

Server side security options

The AdminTool allows you to deny access to any user that is not using a TSplus connection program generated by the administrator. In this case, any user that would attempt to open a session with any Remote Desktop client other than the TSplus one (assuming he has the correct server address, the port number, a valid logon and a valid password) will be disconnected automatically.

The administrator can decide that only members of the Remote Desktop User group will be allowed to open a session.

The administrator can decide that a password is mandatory to open a session.

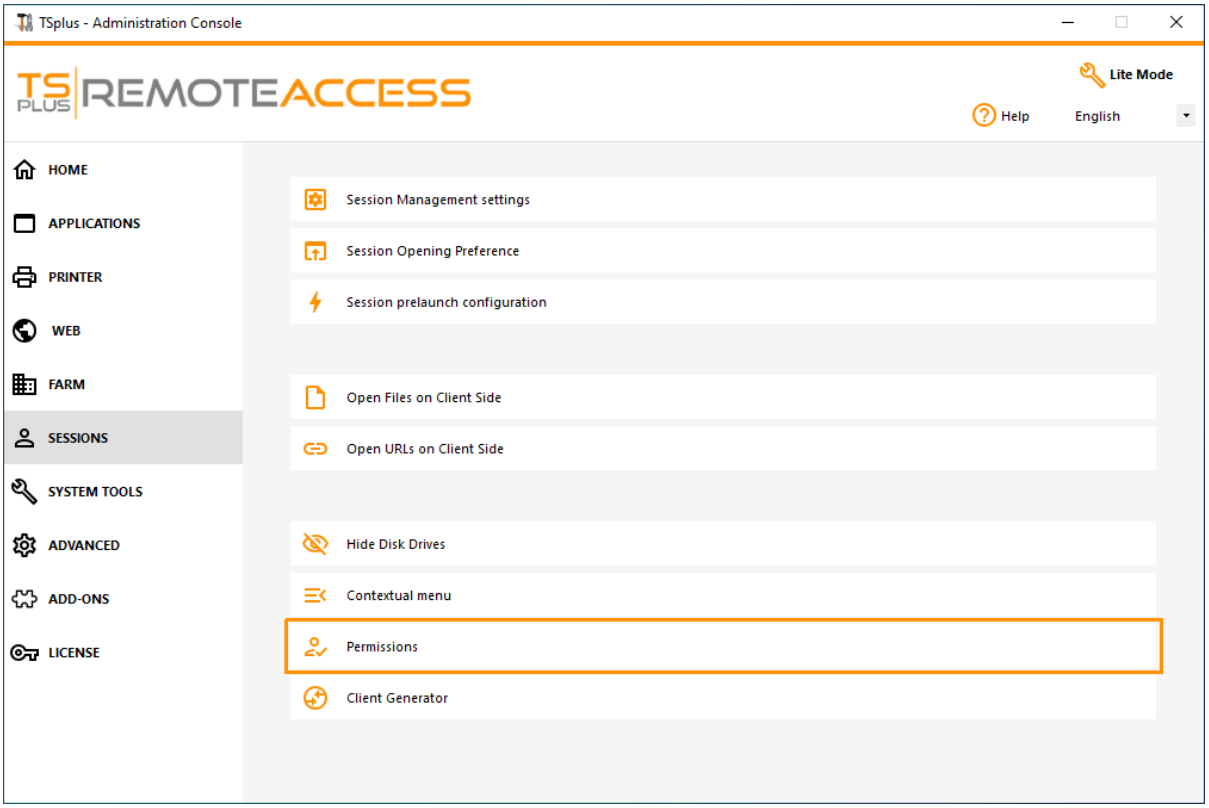
Through setting the applicable local Group Policy, the administrator can specify whether to enforce an encryption level for all data sent between the client and the remote computer during a Terminal Services session.

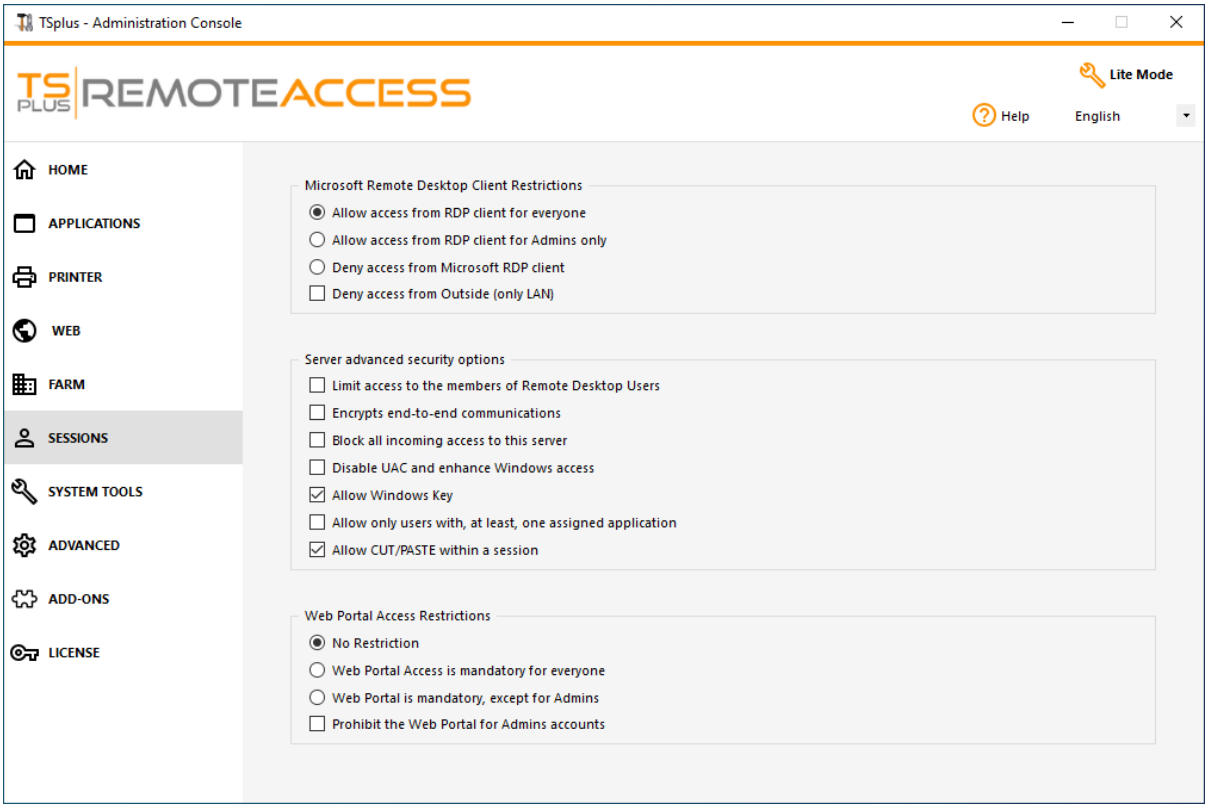
If the status is set to Enabled, encryption for all connections to the server is set to the level decided by the administrator. By default, encryption is set to High.

The administrator can also set as a rule that only users with a TSplus connection client will be able to open a session.

Any incoming access with a standard RDP or a web access will be automatically rejected.

You can find multiple advanced security options if you click on the Sessions - Permissions tab:





- **Allow access from Microsoft RDP client for everyone:** Allows every user to connect using mstsc.exe.
- **Allow access from Microsoft RDP client for Admins only:** Allows only Admins to connect using mstsc.exe.
- **Deny access from Microsoft RDP client:** Prevent anyone to be able to connect using

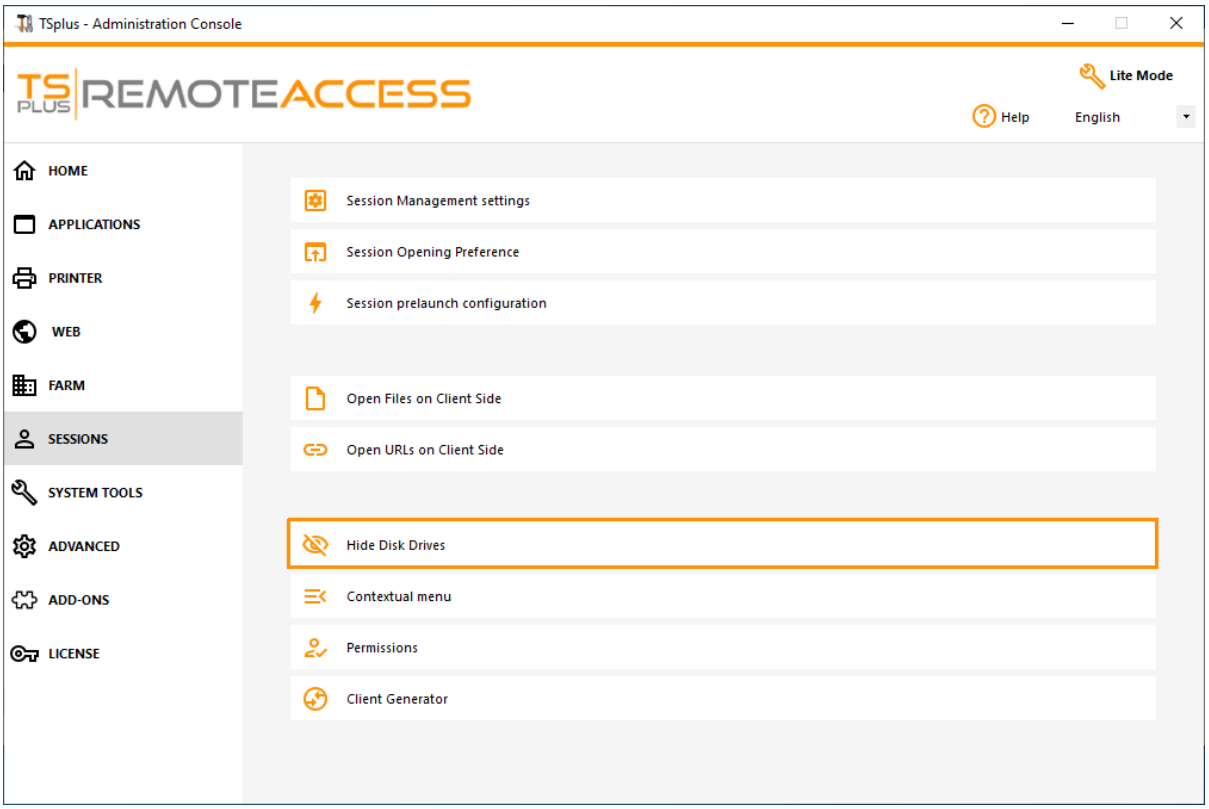
mstsc.exe.

- **Deny access from Outside:** It means that only private IPs from LAN will be able to open a session.
- **Limit access to the members of Remote Desktop users:** This limit applies only to this local group of users (which you can see by clicking on the Users and Groups tile.
- **Encrypts end-to-end communications:** High Encrypts client/server communication using 128-bit encryption. Use this level when the clients accessing the terminal server also support 128-bit encryption.
- **Block all incoming access to this server:** All alive sessions will remain active, while all incoming connections attempts will be blocked. Make sure that you can physically access the console of the server if you check this box. Do not use this option if your server is hosted on a Cloud environment.
- **Disable UAC and enhance Windows Access:** Deactivates the User Accounts Controls, remove all unwanted security pop-ups from Windows. users limitation (messages) while launching applications.
- **The "Allow Windows Key" box** allow the use of the Windows keys and combinations inside a TSplus session.
- **Allow only users with, at least, one assigned application:** User with one application and more are allowed to open a session.
- **Allow CUT/PASTE within a session:** unchecking this box will disable the CTRL C/CTRL V commands

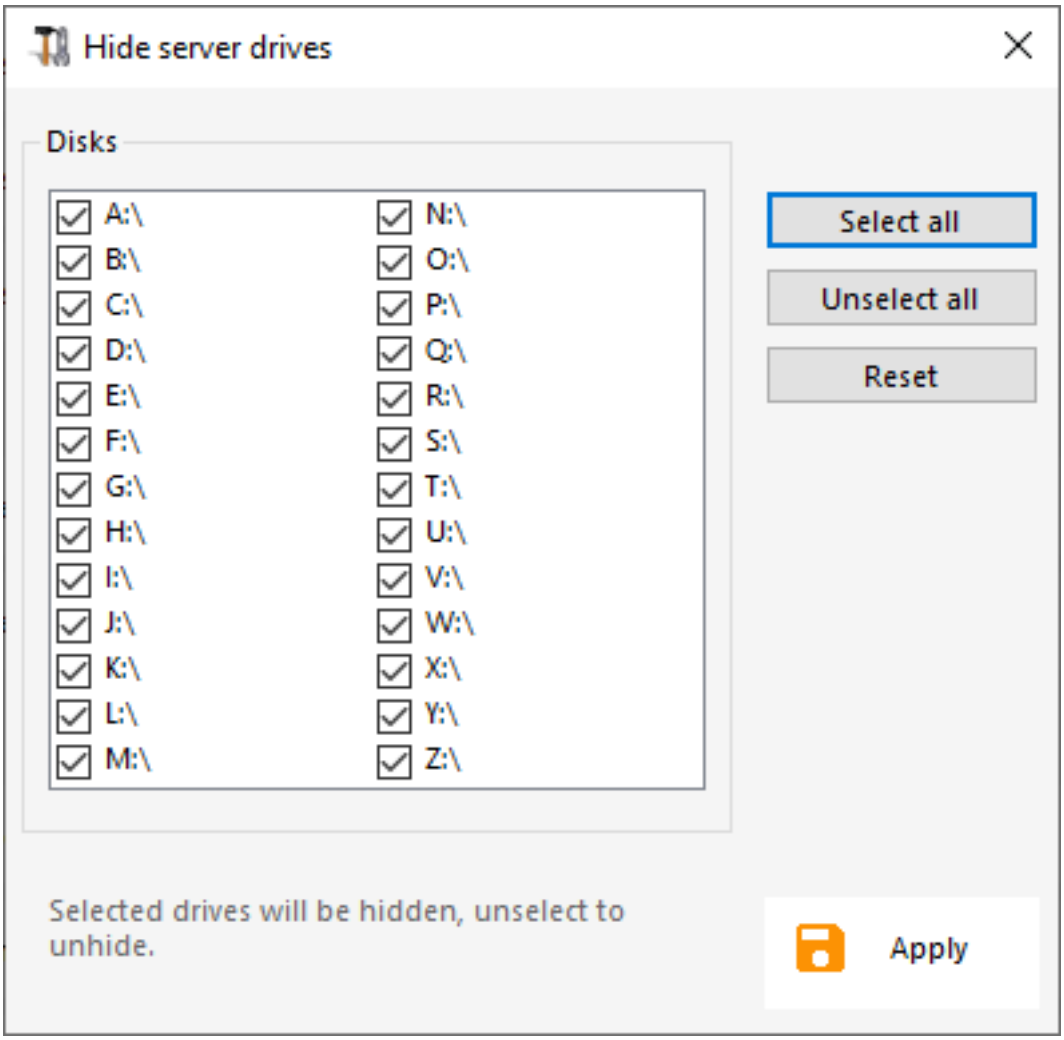
Web Portal Access Restrictions

- No Restriction
- Web Portal is mandatory for everyone: users can only connect via the Web Portal.
- Web Portal is mandatory, except for Admins: users can only connect via the Web Portal, except Administrators.
- Prohibit the Web Portal for Admins accounts: Administrators cannot connect via the Web Portal.

The AdminTool includes a tool that enables hiding the server disk drives to prevent users from accessing folders through My Computer or standard Windows dialog boxes. On the Sessions tab, click on "Hide Disk drives" :



This tool works globally. This means that even the administrator will not have a normal access to drives after the settings have been applied. On the example below, all drivers have been selected with the “select all” button, which will check all the boxes corresponding to drives that will be hidden to everybody:



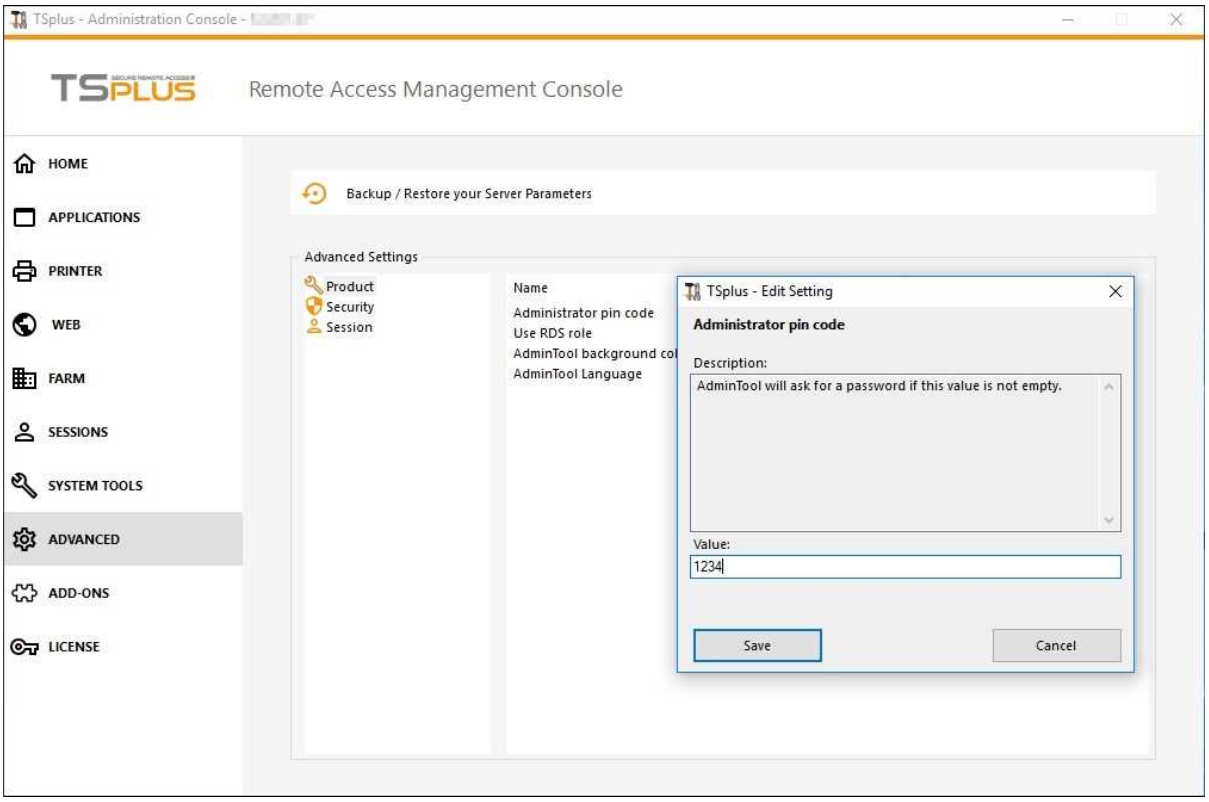
Notes: This functionality is powerful and does not disable the access to the disk drives. It just prevents the user to display it.

The tool flags the disks drives as hidden, but it also adds the HIDDEN property to the entire root folders and users list in Document and Settings.

If the administrator wants to see these files he must:

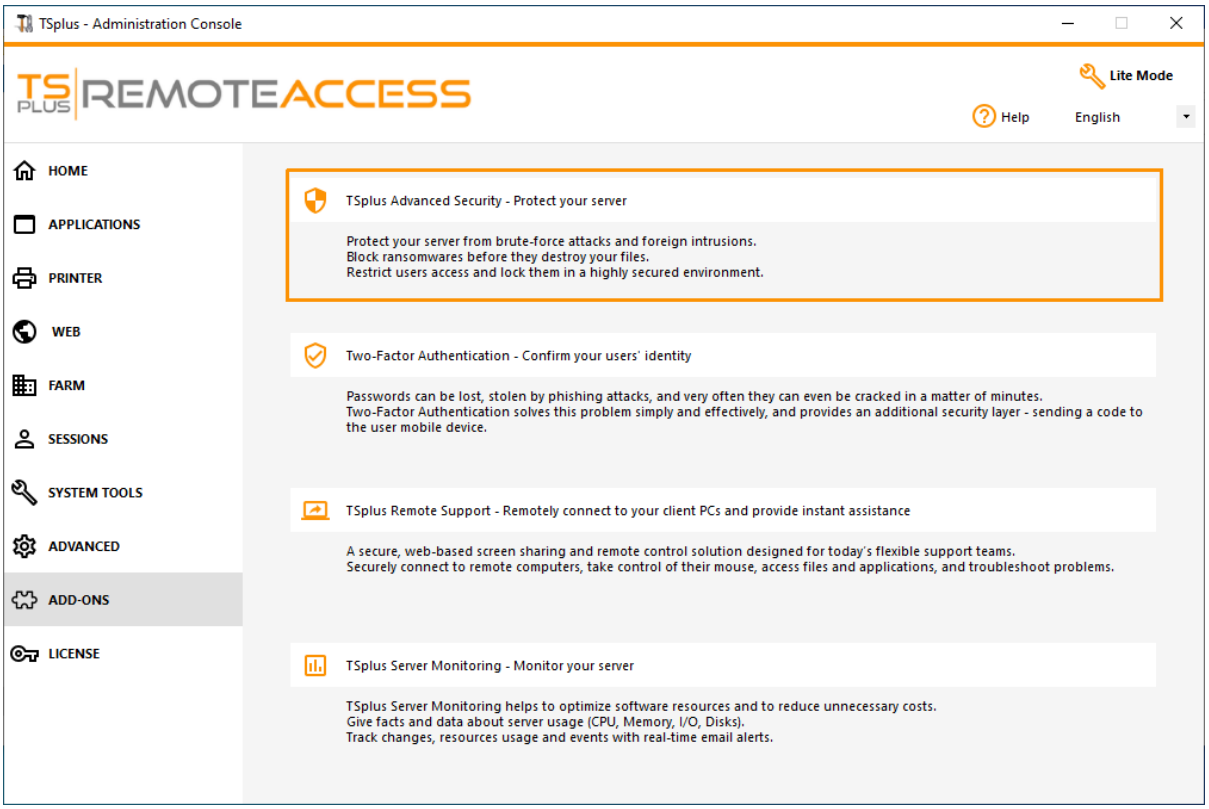
1. Type the disk drive letter. For example: **D:<ENTER>** which will take you to the D: drive.
2. Turn on **SHOW HIDDEN FILES AND FOLDERS** in the folder view properties.

The Administrator can secure the Administrator Tool access by setting a pin code which will be asked at every start, on the Advanced tab of the AdminTool, under the Product Settings:

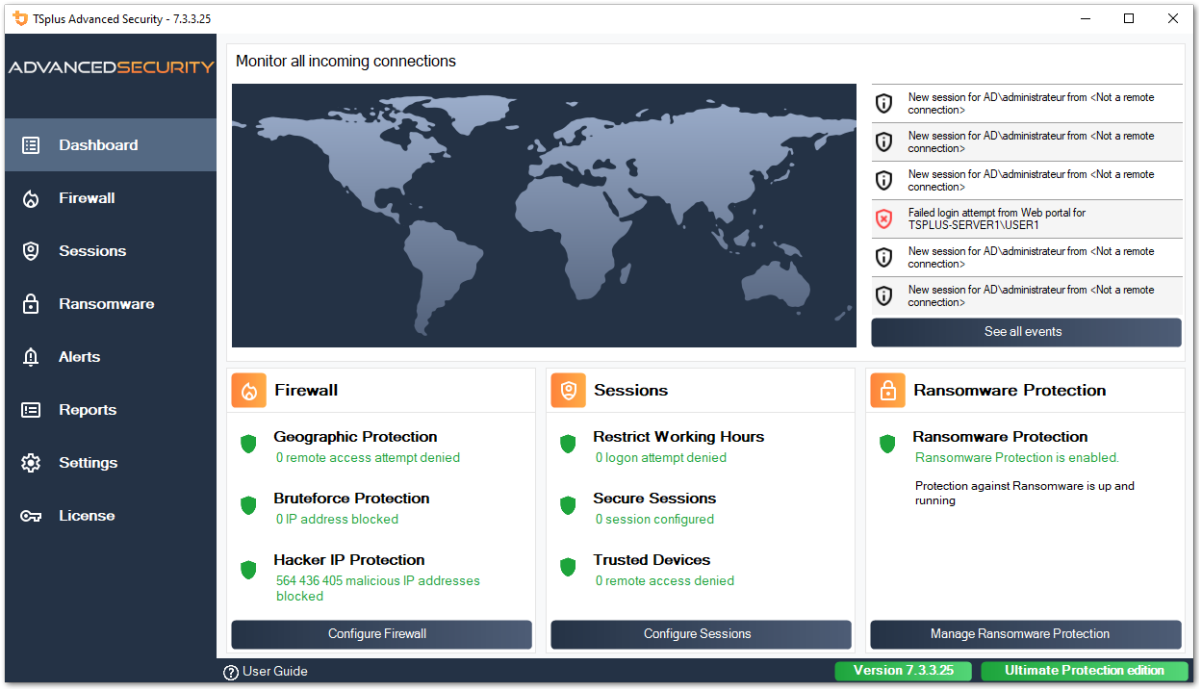


TSplus Advanced Security Ultimate

Since TSplus 11.40 version, you will find a one-of-a-kind Security Add-on Tool, which you can launch on the Add-Ons tab:



Which brings powerful features, documented on this page.



The Bruteforce Protection role on the Web Portal is described on this page.

Two Factor Authentication

Since TSplus 12 Version, you can enable two-factor authentication as an add-on for your TSplus Web Portal.



More information on this amazing new feature can be found on this page.

SSL Certificates

SSL Certificates process is detail on these pages:

- TSplus provides an easy-to-use tool to generate of a free and valid SSL certificate: Free and Easy-to-install SSL Certificate
- HTTPS & SSL Third Party Certificates.
- Choose your Ciphers Suites to enhance Security.

TSplus access program security options:

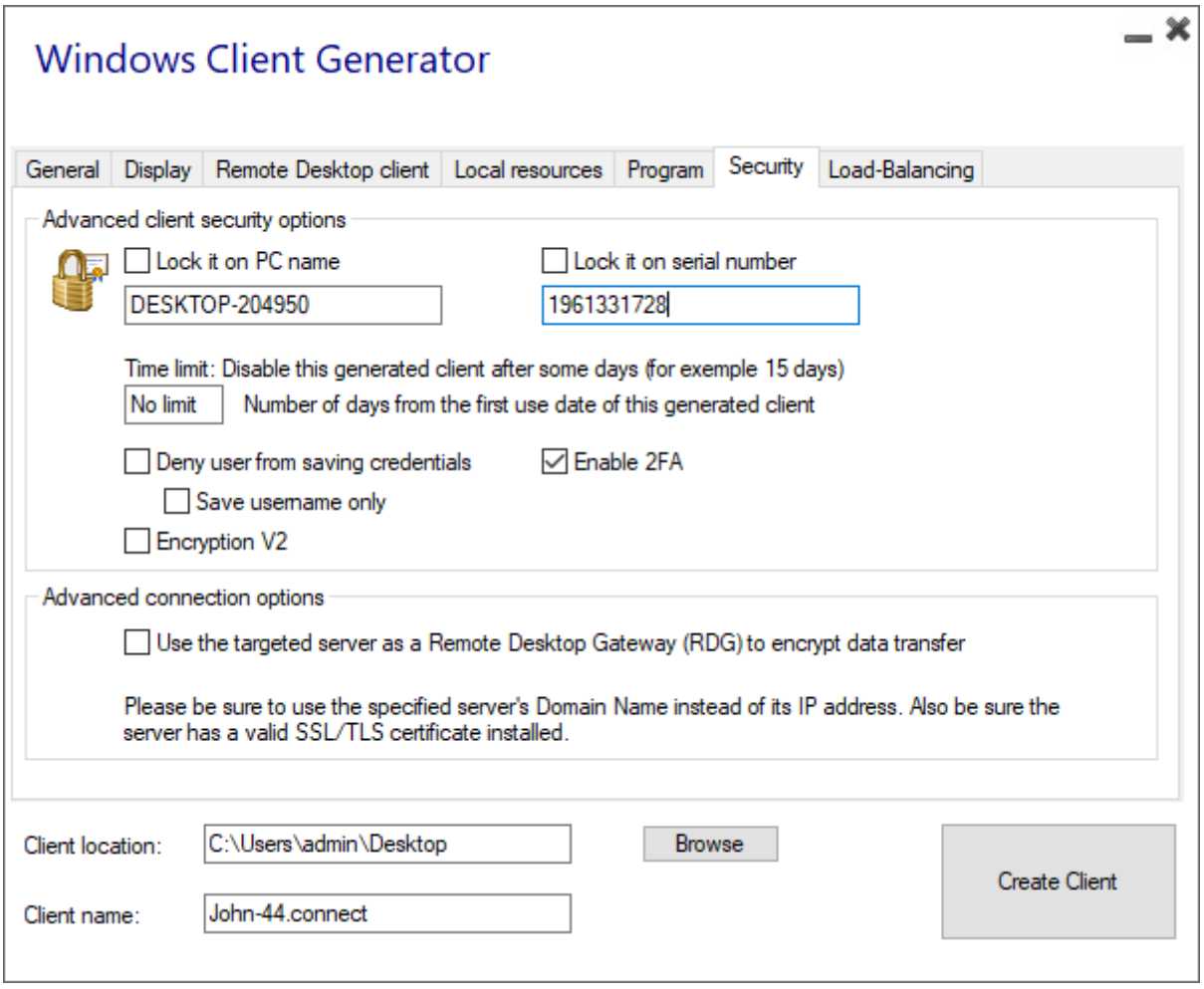
The TSplus client generator gives the capability, on its Security tab, to lock the TSplus client to:

- A specific PC name. It means this program will not be able to start from any other PC.
- A physical drive serial number (PC HDD or USB stick). This is a very easy and powerful way to set a high level of security.

  The only way to connect is with a specific client, and this specific client can only start on a specific USB stick or PC HDD.

  Some of our customers are delivering fingerprint-reading USB sticks to each of their users and each generated program is locked to the device serial number.

  This way, they can restrict access to the client's program itself, as well as ensuring it cannot be copied off the USB stick and used elsewhere.

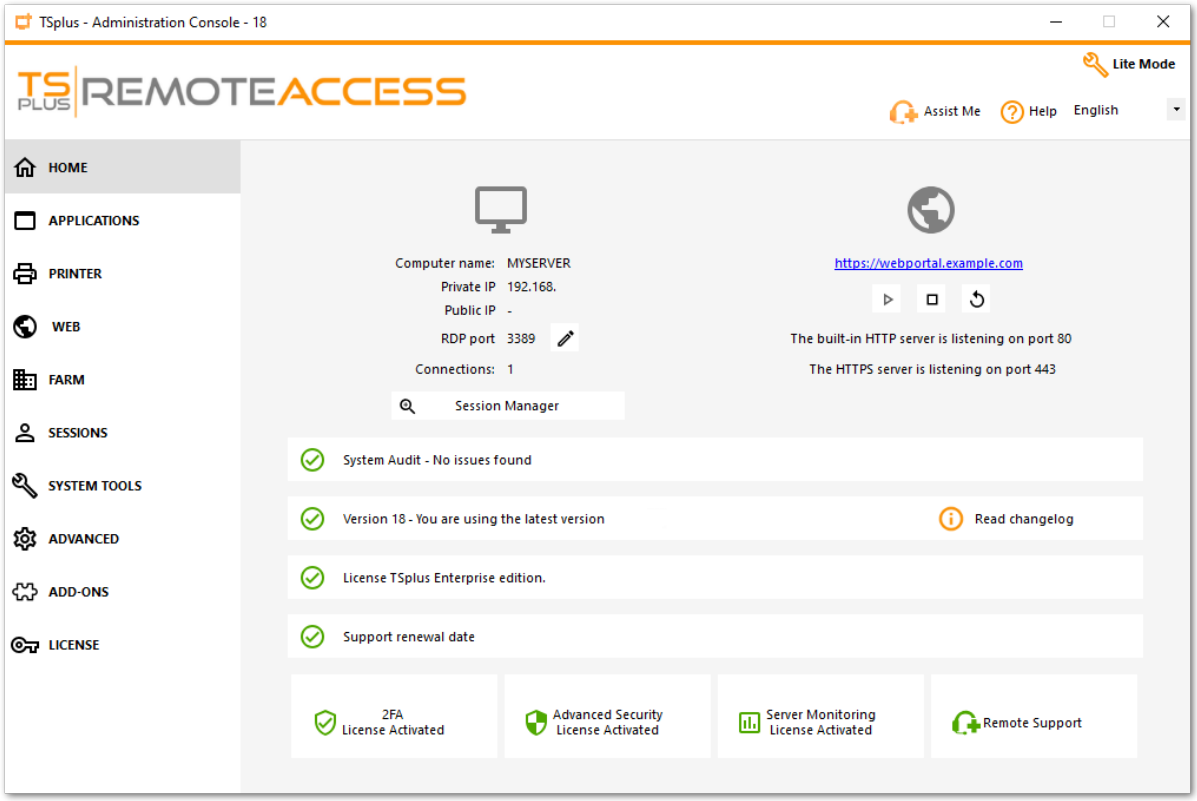


For more security feature informations, check TSplus Portable Client Generator documentation

and our FAQ.

Server Management

On the Home tab of the AdminTool, you can see all the needed information about your TSplus server:



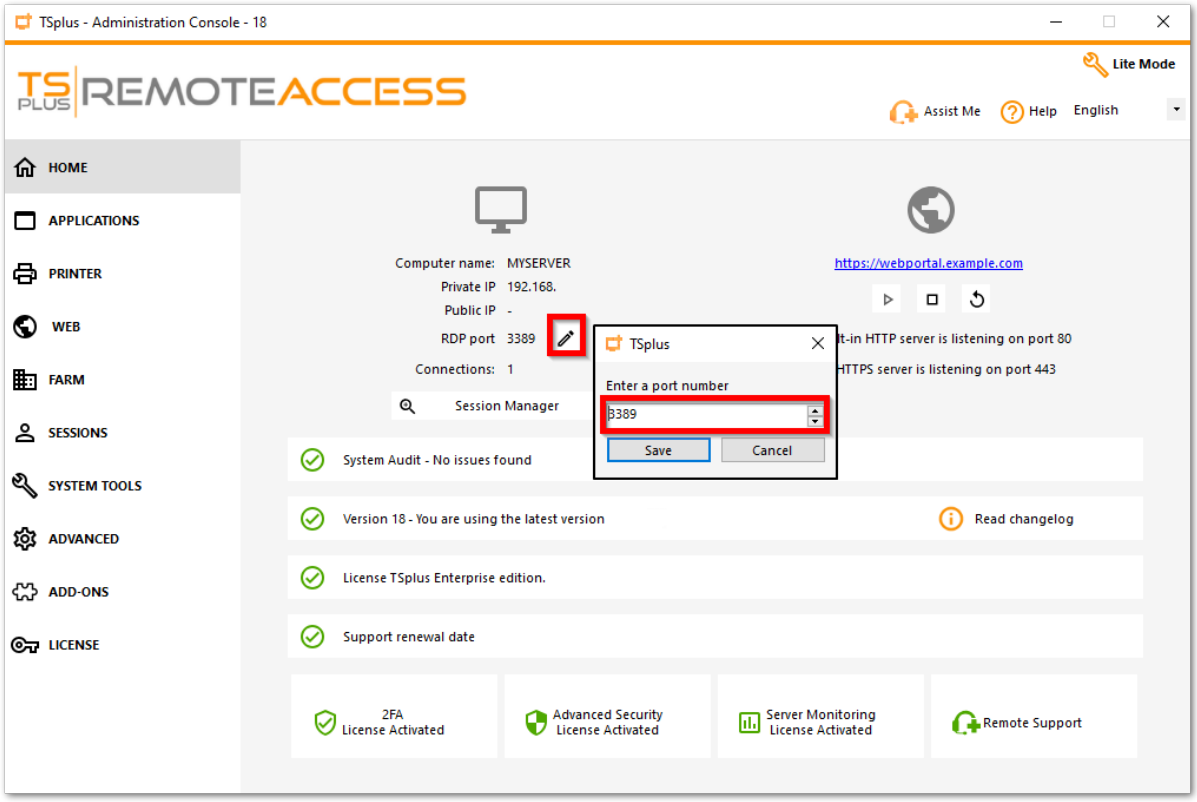
Changing the RDP port number and setting up the firewall

With the AdminTool, you can select a different TCP/IP port number for the RDP service to accept connections on. The default one is 3389. You can choose any arbitrary port, assuming that it is not already used on your network and that you set the same port number on your firewalls and on each TSplus user access programs.

TSplus includes a unique port forwarding and tunneling capability: regardless the RDP port that has been set, the RDP will also be available on the HTTP and on the HTTPS port number!

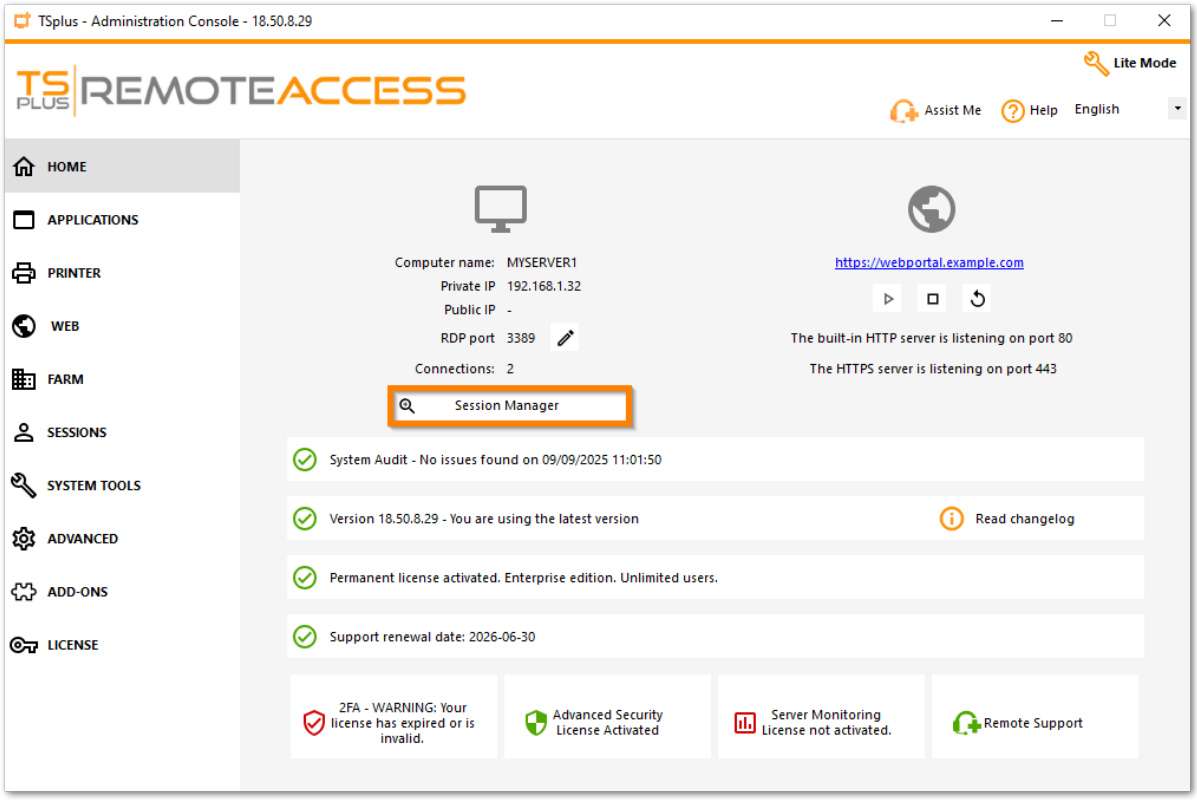
If users want to access your TSplus server outside from your network, you must ensure all

incoming connections on the port chosen are forwarded to the TSplus server.

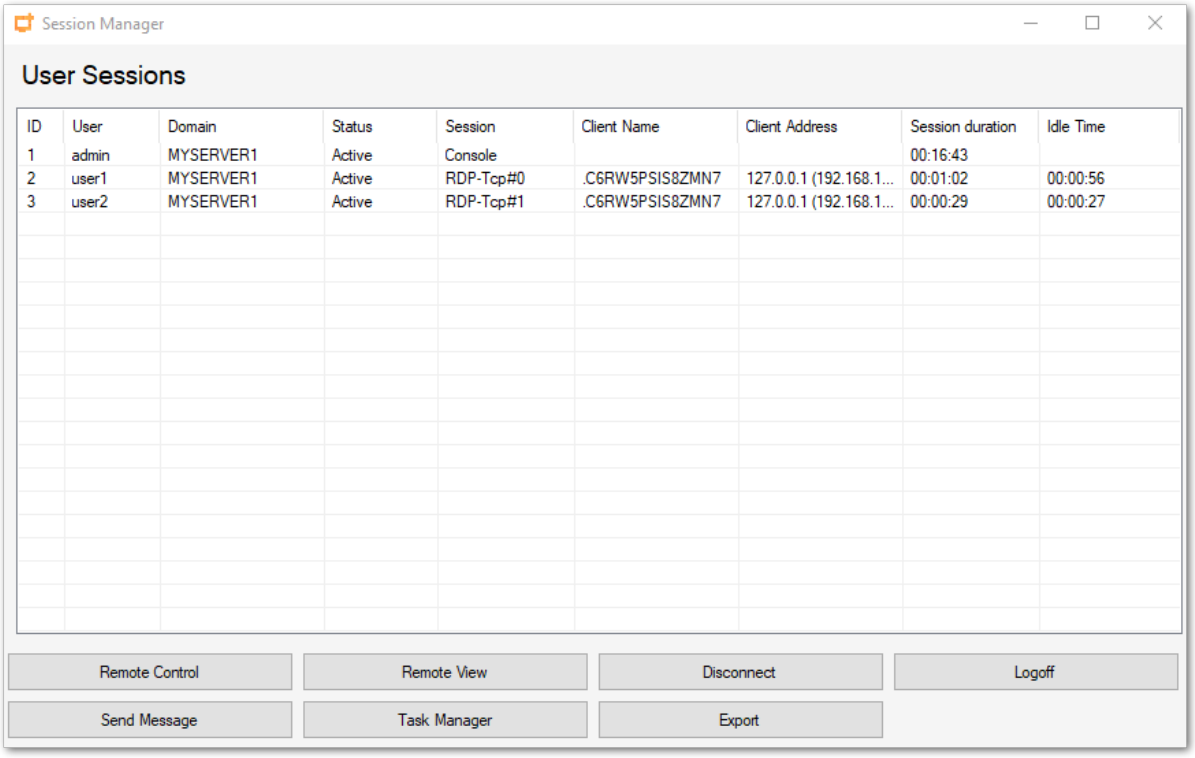


Management of users and sessions

The session manager is located right below the RDP port:



You can display your server's task manager, and you have the possibilities to active a remote control, disconnect, logoff or send a message to your users.



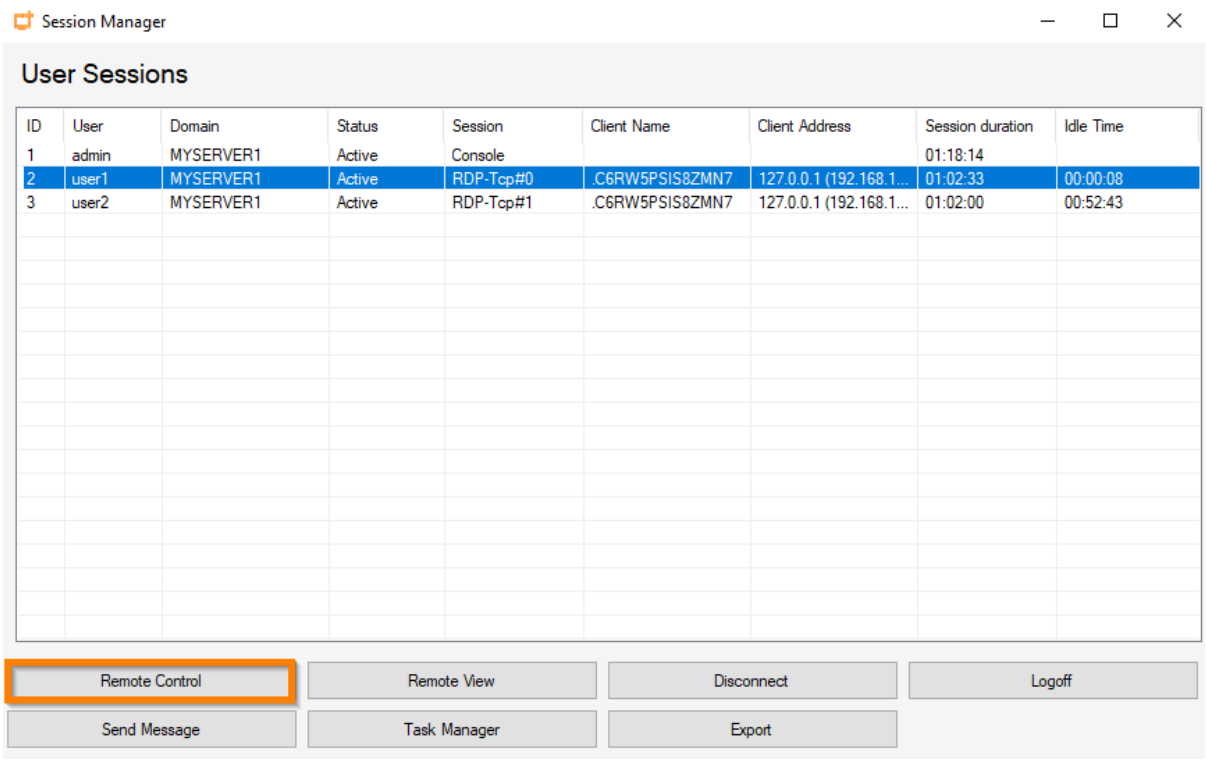
You can activate the remote control via a remote session with an admin account on the following Operating Systems:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows 7
- Windows 8.1
- Windows 10 pro and above

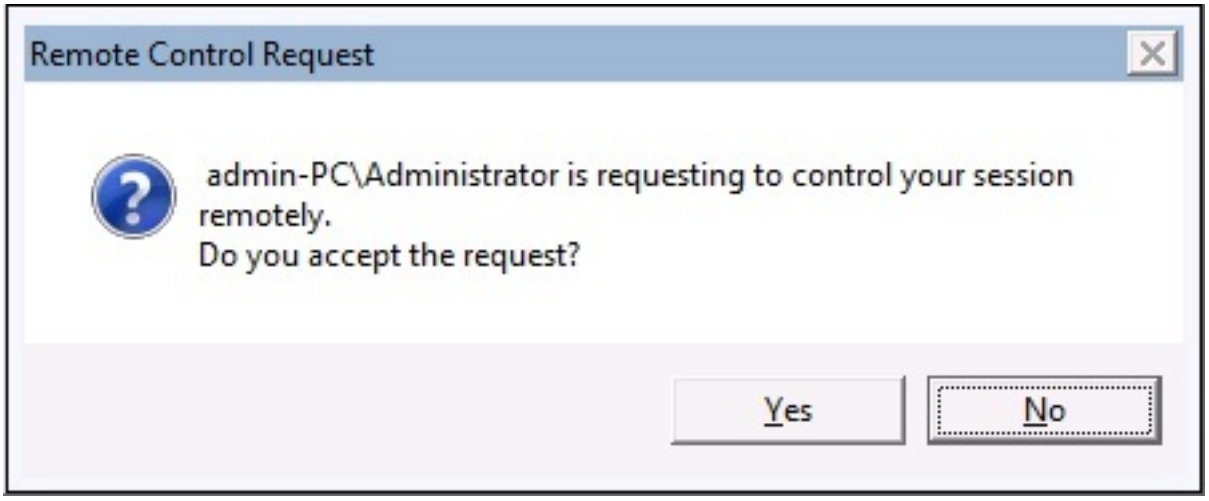
On Windows XP, 2003, Vista, and 2008 there is no remote control button.

On Windows 2012 and 8 a message appears advising you to update to 2012 R2 or 8.1.

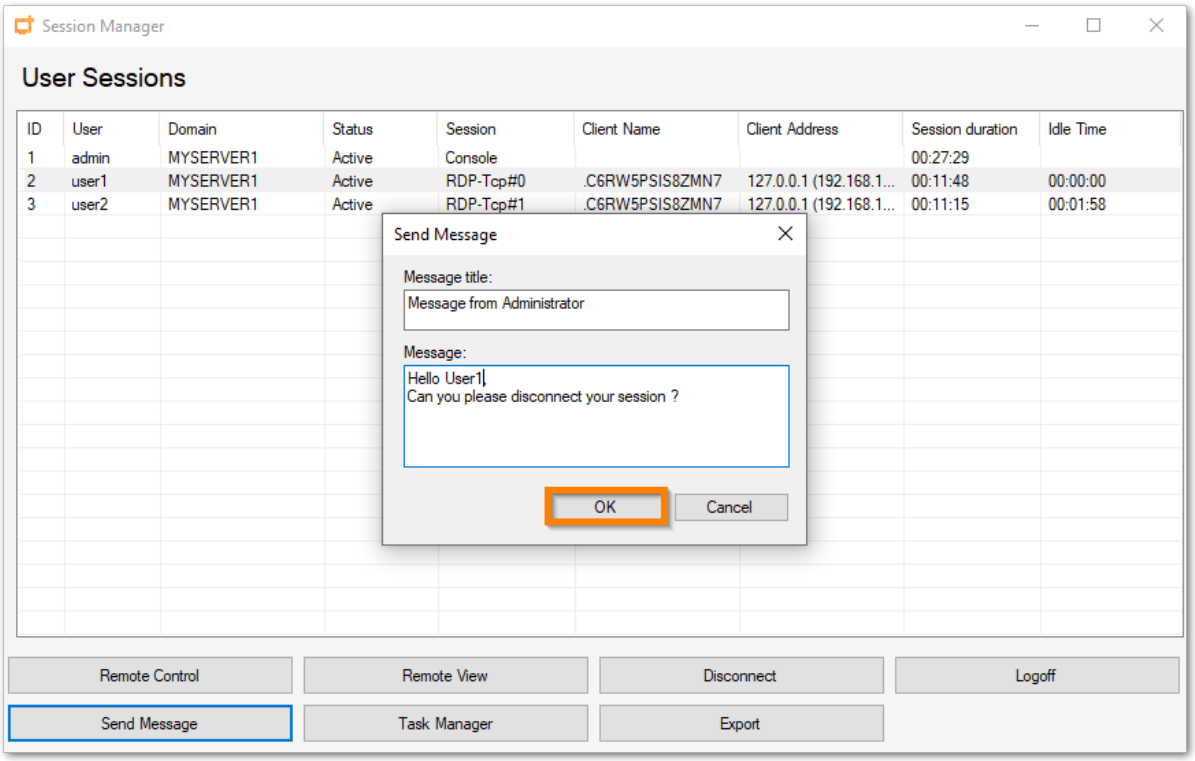
When you activate the remote control for a user's session, this message appears, indicating the keyboard shortcut to end the session:



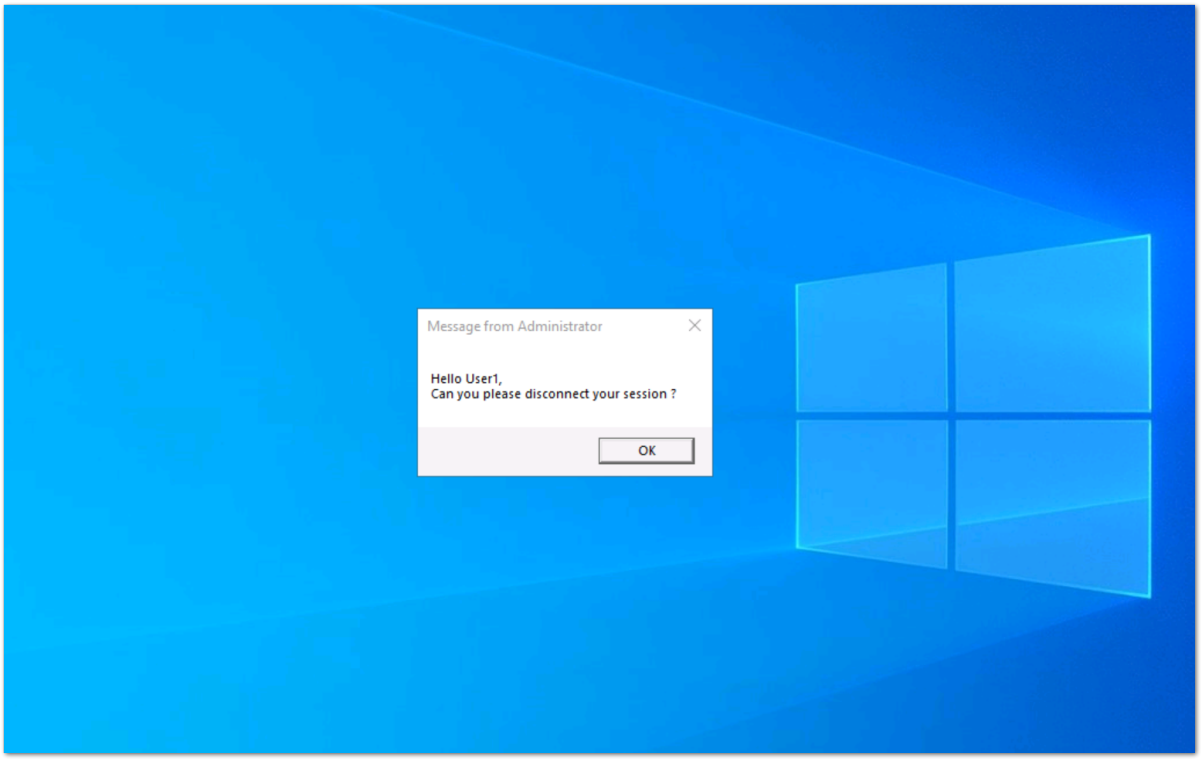
On the client side, this message appears to accept the remote control:



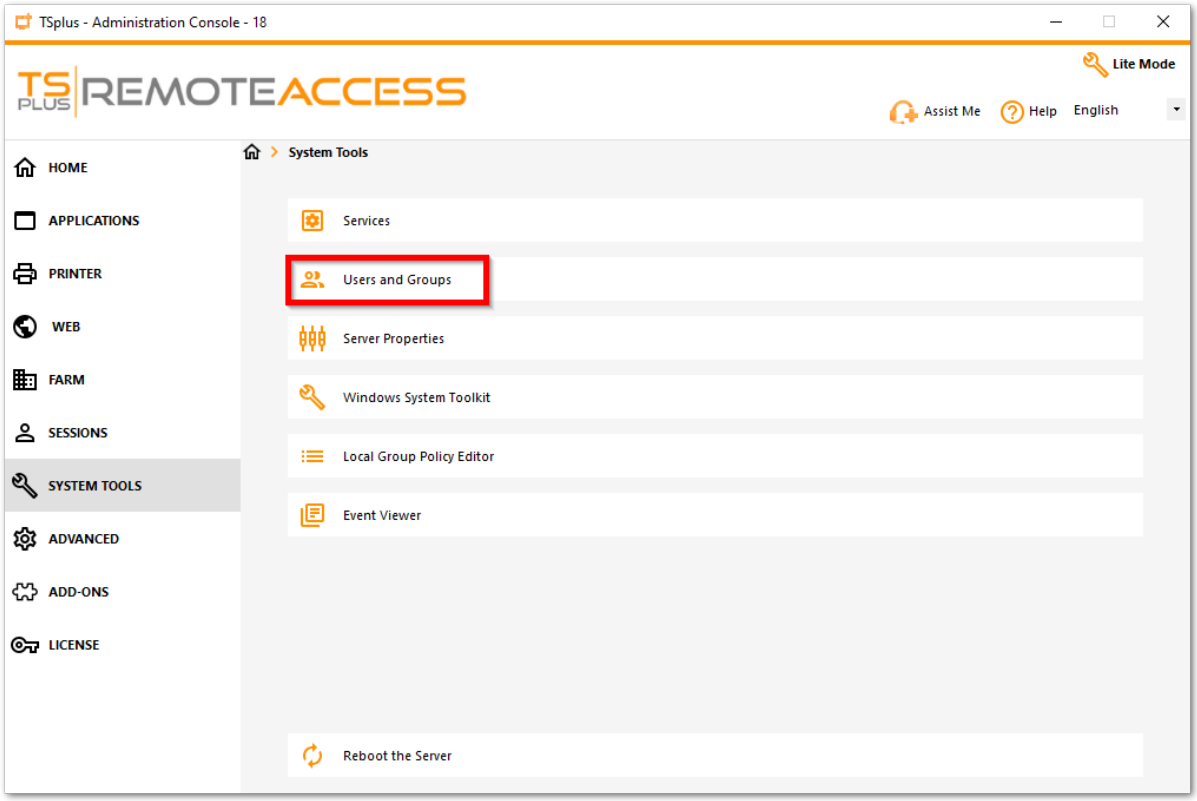
You can also send a message to your user:



Message sent on Server Side

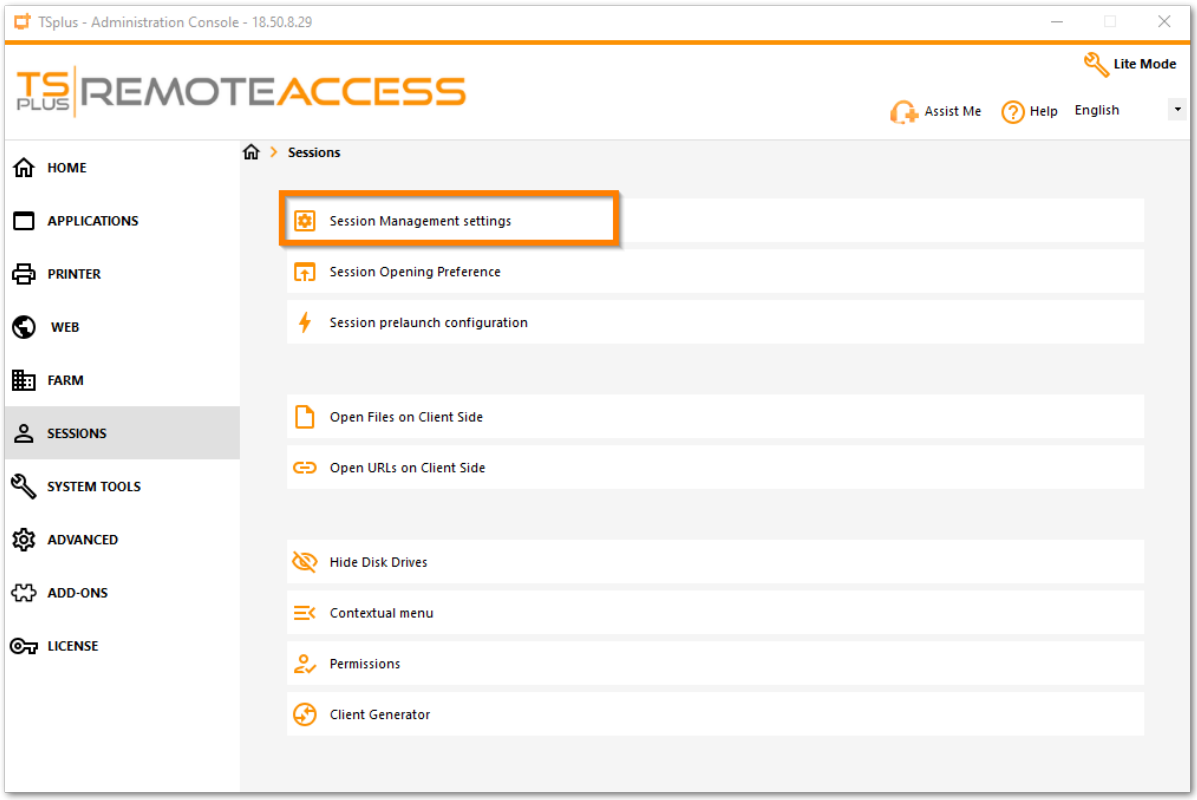


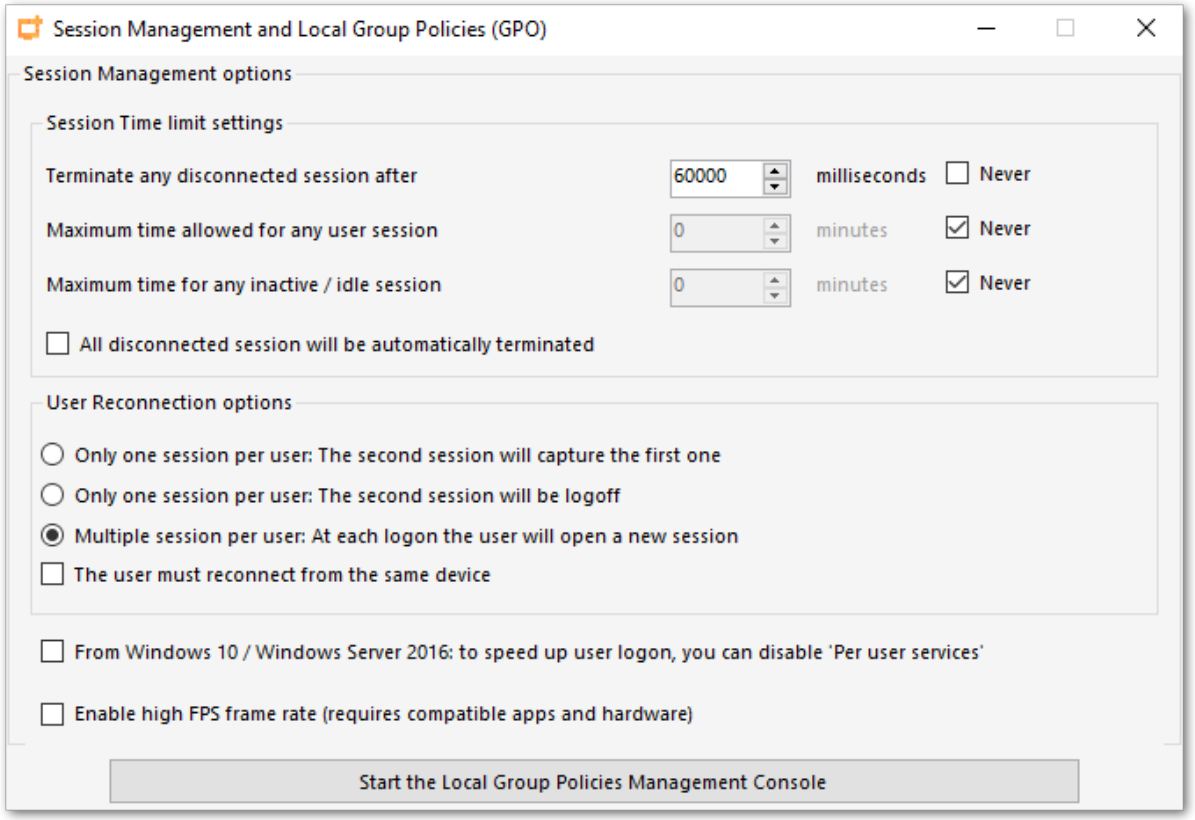
Message appearing on Client Side



See this documentation for more information.

- With the Session Management Settings (GPO) tab, you can set various connection settings for each session and user:

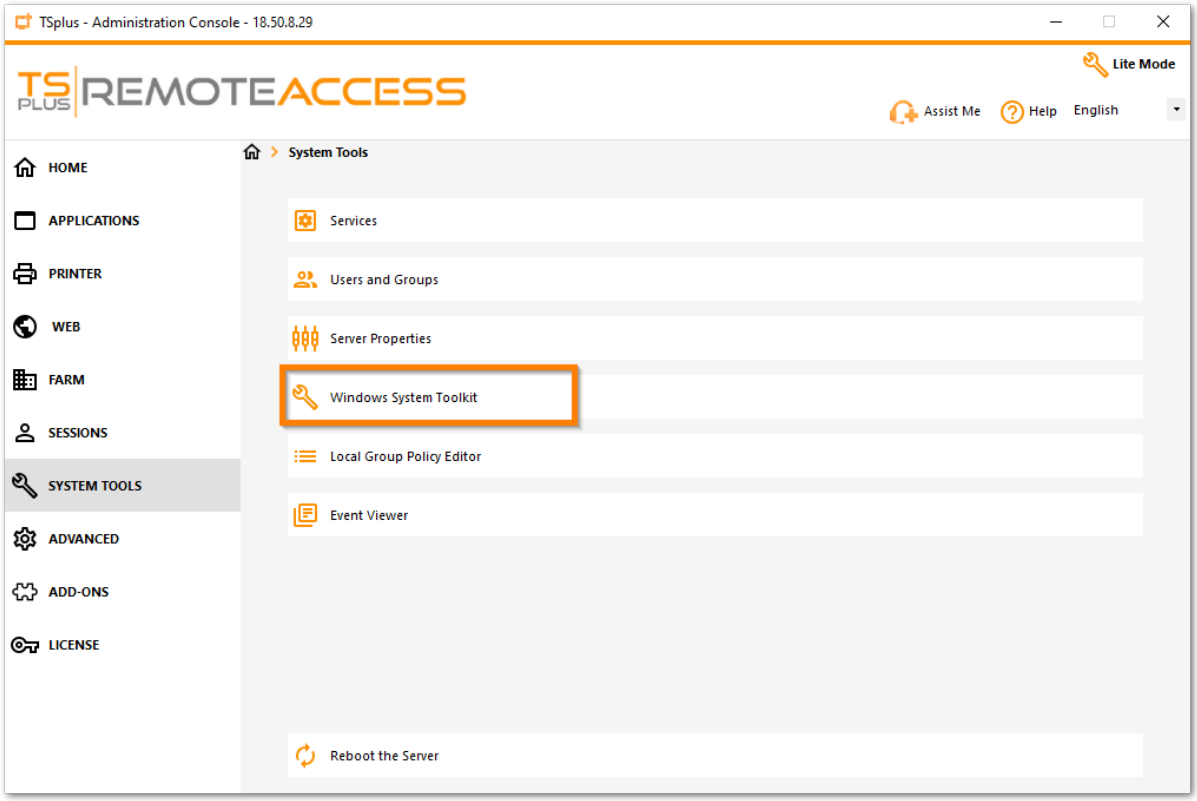


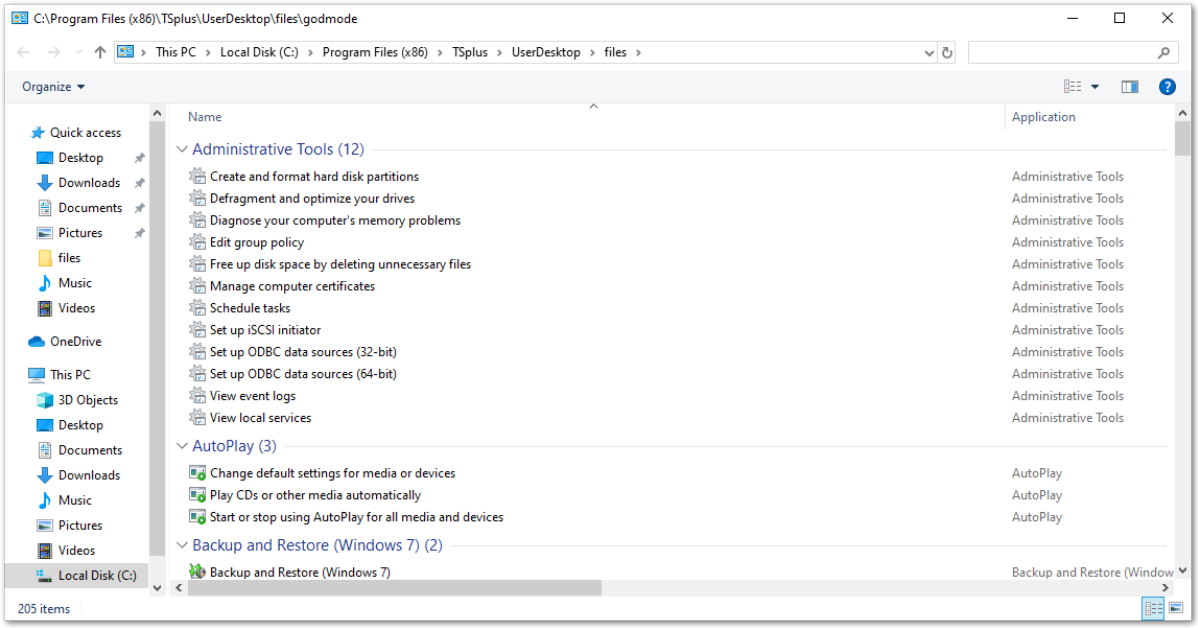


Windows Server 2016 introduced a new “Per user service”, which makes services start all processes per users, which slows the users logons time.

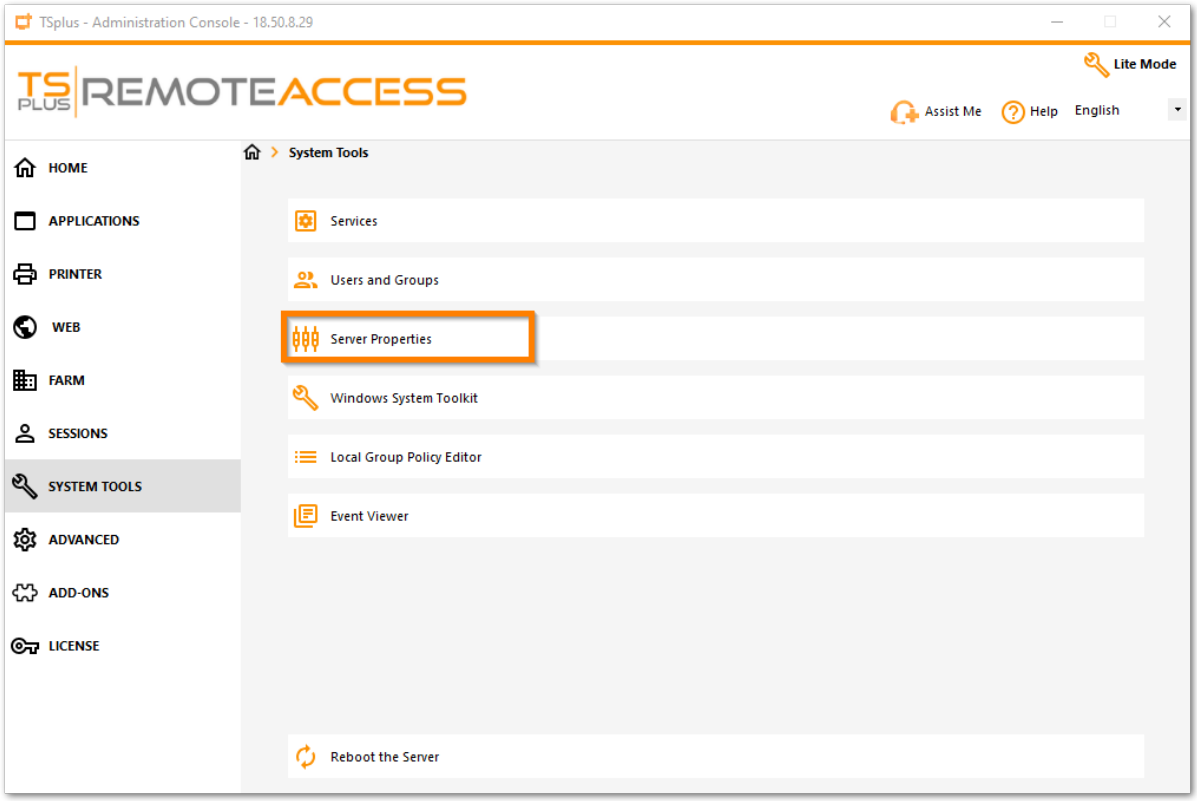
Since TSplus 11.70 release, you can **disable per user services in order to speed up users logons**.

- The Windows Toolkit is an enhanced control panel, summarizing all the Windows Administration tools.

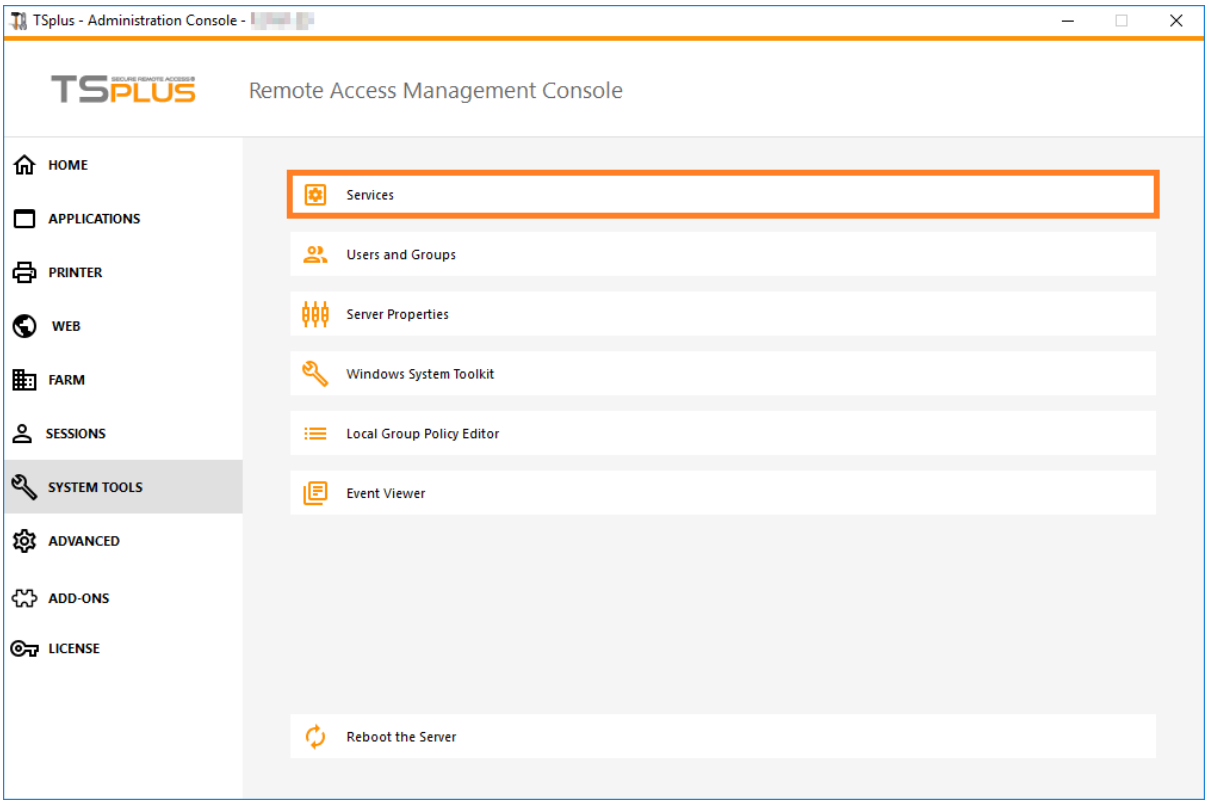




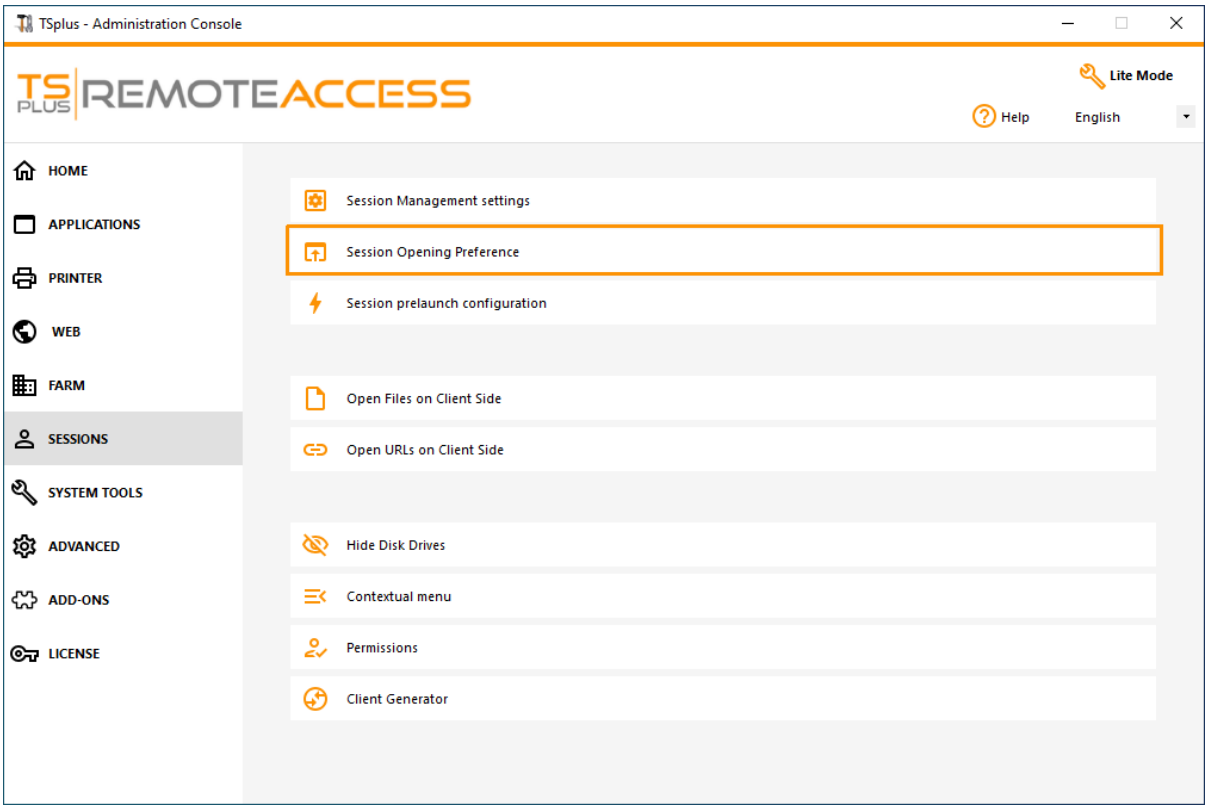
- You can also launch the “Server Properties” tab to have an overview of the control panel.



- You can see all the services on your server and their status on the Services tile.

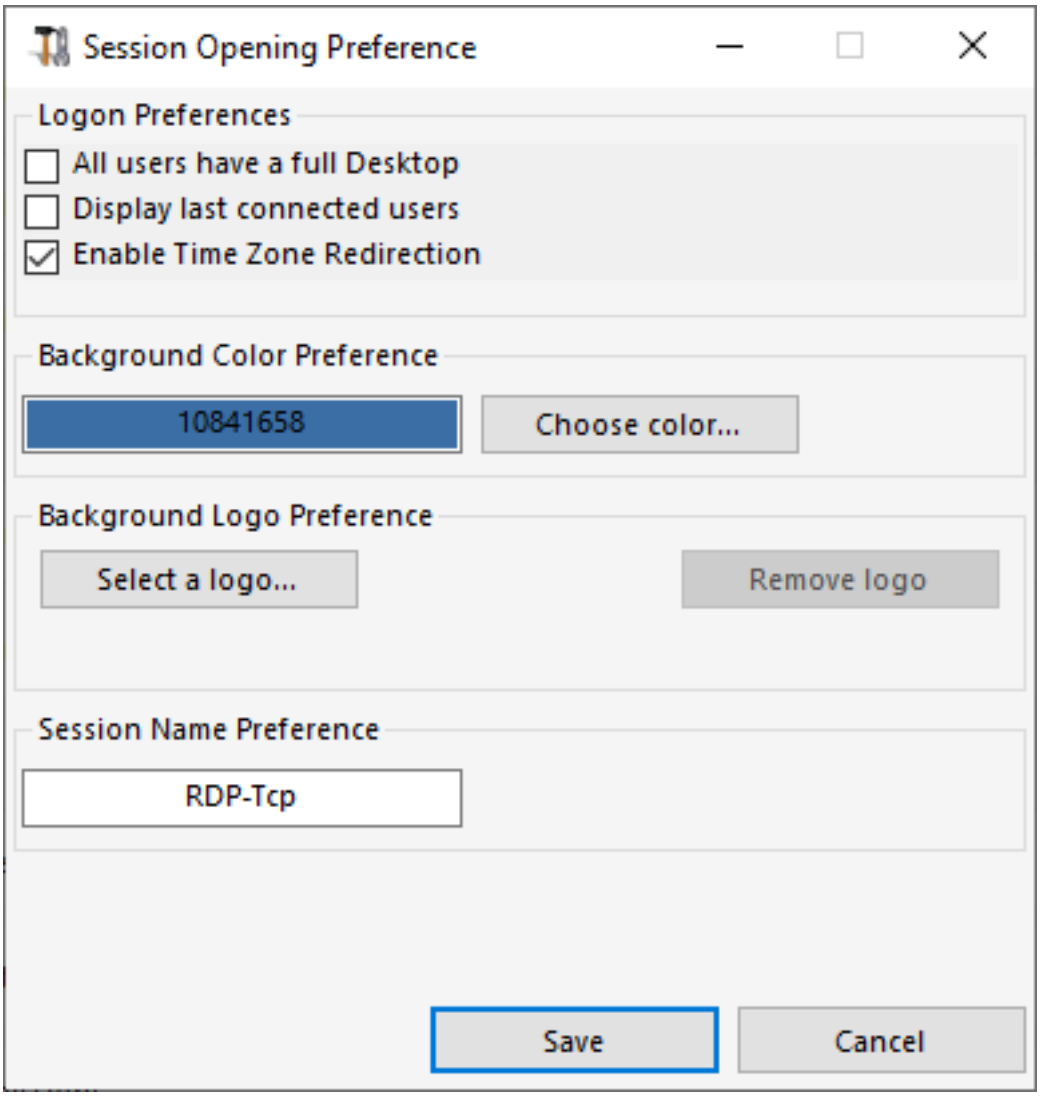


The session opening preference allows you to choose your shell session preference, your logon preferences, the background color of your sessions, add your own logo and rename it to your liking.



By default, on these logon preferences are enabled:

- The “**Display progress bar during logon**”.
- “**Enable Time Zone Redirection**” which enables the client computer to redirect its time zone settings to the Remote Desktop Services session. If you enable this policy setting, clients that are capable of time zone redirection send their time zone information to the server.



You can also **set a full Desktop** for all your users and **get a display the last connected users** by ticking the corresponding boxes. You can **customize your users sessions** by adding a new Background Color, another logo or none and use the session name of your choice.

- Since TSplus 11.70 release, you can use **TSplus WinXshell** as an alternative to the Windows shell.

Following the October 10 Windows Update, administrators allowing their users to start a Remote Desktop saw the Windows shell as an issue.

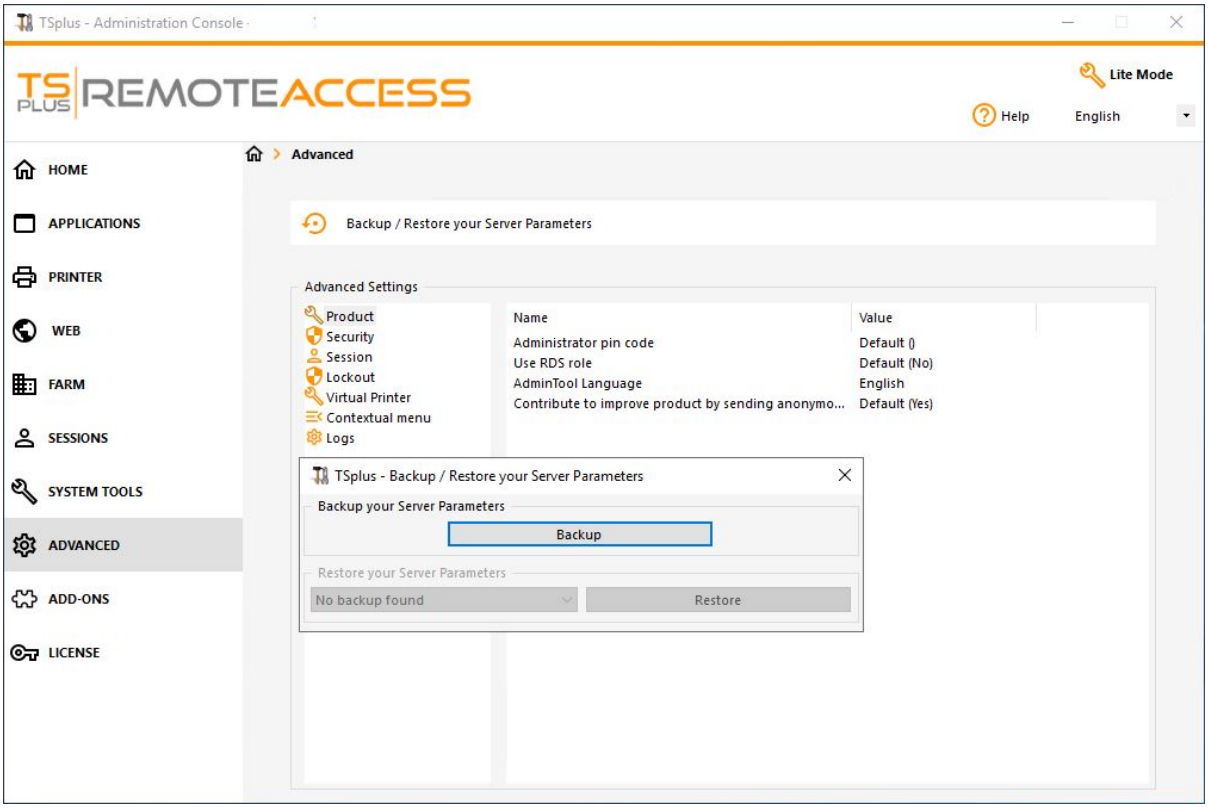
The main problem resides in the session opening/black screen issue when a complete desktop is assigned to multiple users on Windows 10 and Server 2016.

It provides features and graphical experience similar to Windows 2016 Windows shell, such as the display of the 2016 Start button and taskbar.

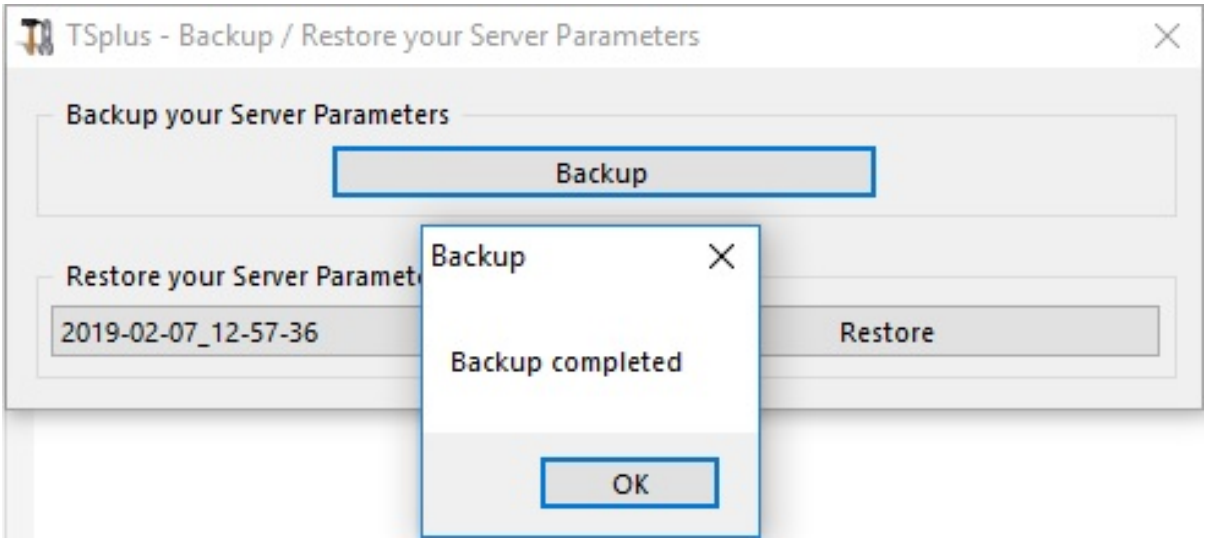
It is especially useful if you **use Windows 10 or Windows 16 Operating systems**, **manage 10 users or more** and **wish to assign them a full desktop**.

Backup Parameters

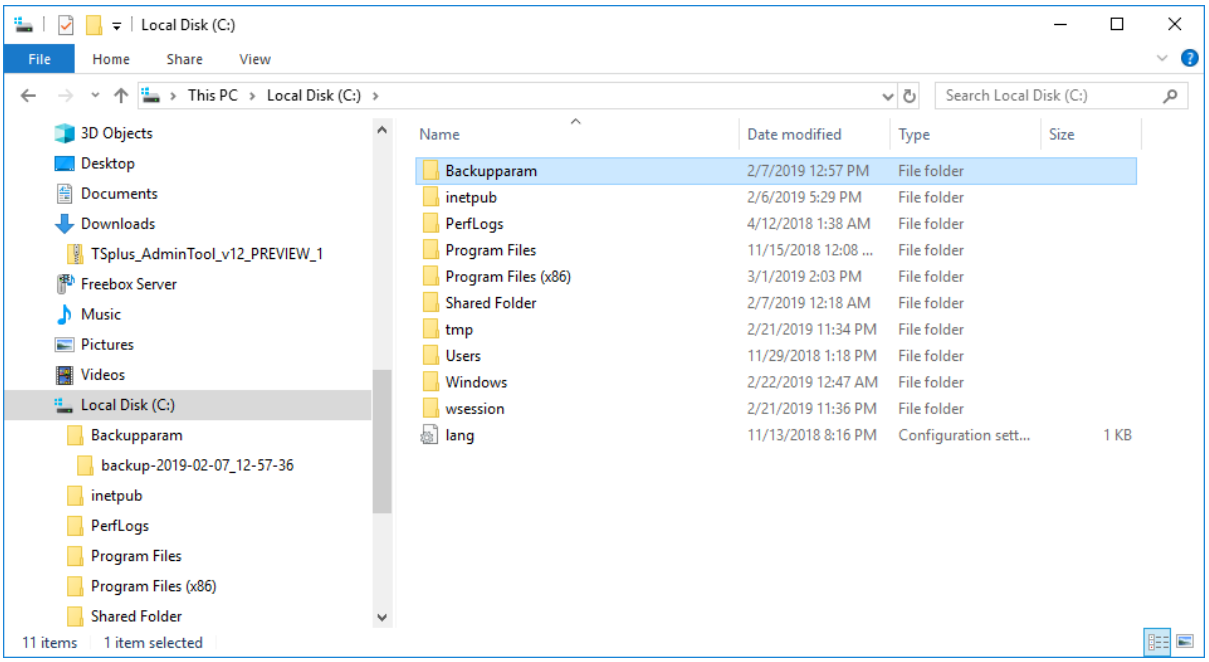
You can backup or restore your server parameters by clicking on the tile of the same name, on the Advanced tab:



Click on the Backup button to make a backup, which will be dated and added to the list of your restore points:



The backup file can be found on the C:\Backupparam folder:



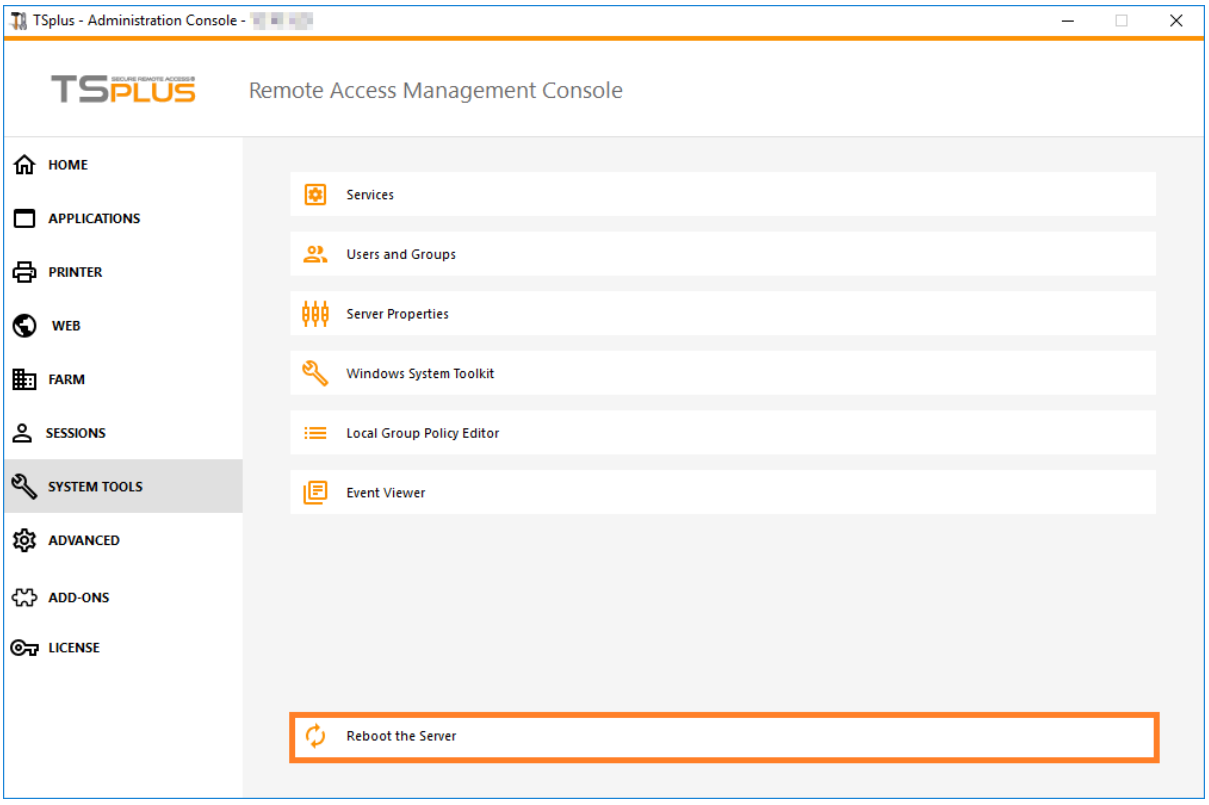
Copy the folder to the new server after installing TSplus Remote Access and restore the backup.

You can then check with the trial for 15 days that the functioning of the accounts and access is correct before migrating your license definitively.

More information on this documentation.

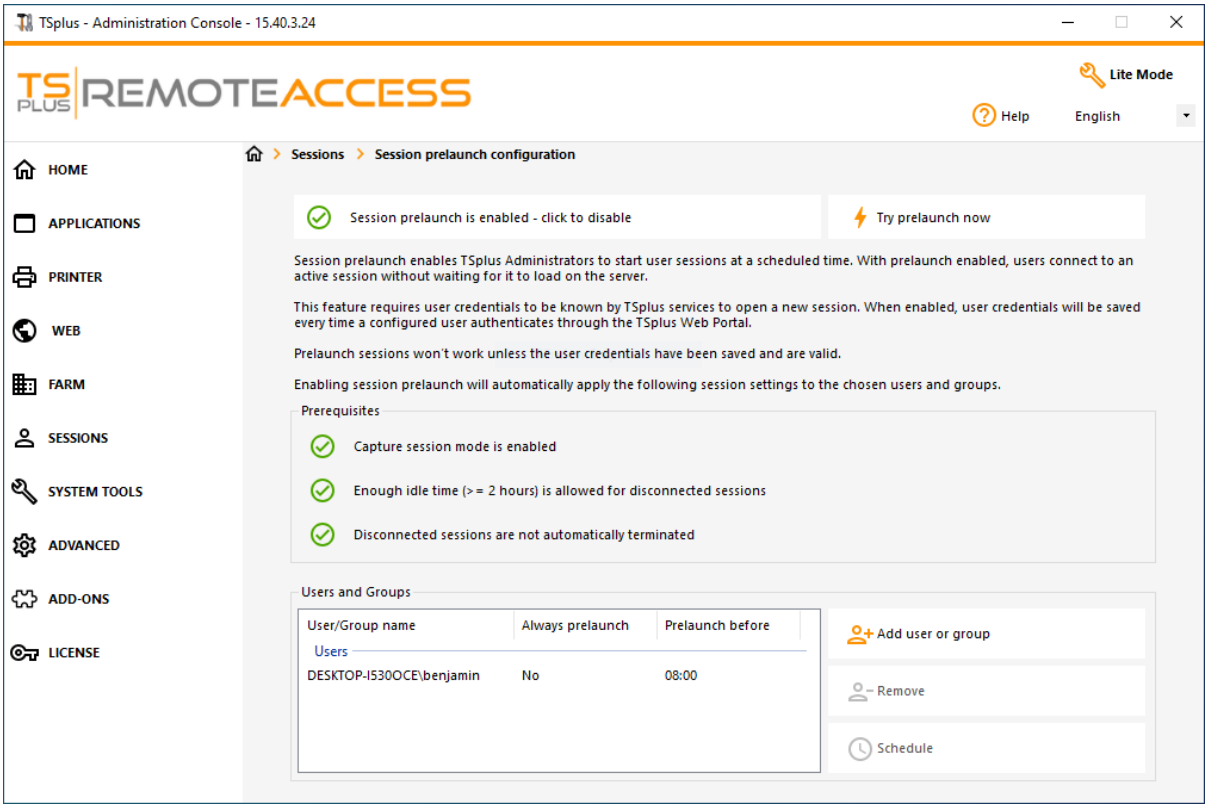
Reboot your server

The “Reboot the server tab” allows you to reboot your server.



Session Prelaunch

Access the Session Prelaunch configuration menu from the Sessions > Settings tab of the Admintool, by clicking on the “Session Prelaunch configuration” tile.

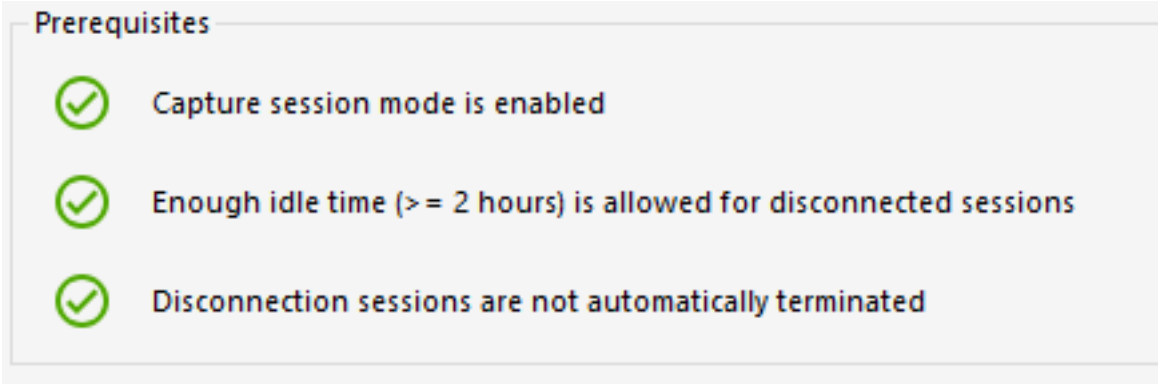


Overview

The session prelaunch feature enables Tsplus Remote Access administrators to configure user sessions to launch before a scheduled time. The idea is to prepare and load the session of every configured user ahead of time, so that once a user connects, they capture their specific session. This can cut connection wait times from minutes to seconds.

Prerequisites

Prelaunch requires multiple prerequisites to be met.



1 - In order to capture a session, **capture session mode must be enabled.** This means you won't be able to benefit from this feature if the multi-session configuration is mandatory for your users.

2 - Since the prepared session loaded ahead of time needs to be present (not logged of) when the user connect and captures it, **a minimum of 2 hours of idle time for disconnected session must be allowed.** You can of course also set the session settings so that it never logs off a disconnected session.

3 -Since the prepared session is disconnected once loaded to reduce the overall resource usage, **the session settings must be configured not to automatically log off disconnected sessions.**

Important note! Each configured user will need to authenticate at least once through the TSplus Web Portal after the session prelaunch feature is enabled to make the TSplus services able to open the configured user session.

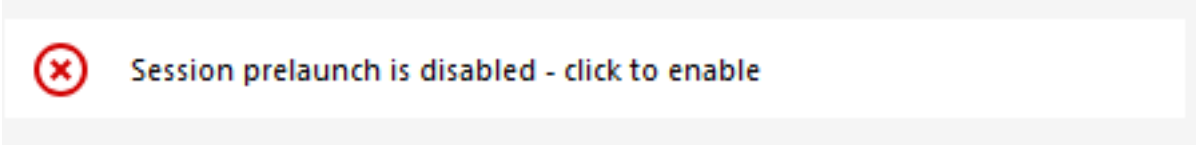
Session Prelaunch compatibilities

Session prelaunch is compatible with HTML5 sessions and generic RDP sessions opened via generated client or mstsc.

It is however not compatible with the Remote App connection or custom RDP connections made for opening a specific program.
As a result, connections coming from the TSplus Web Application Portal are not supported.

Enable the feature

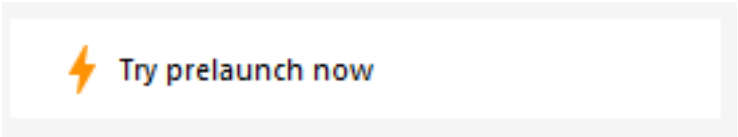
To enable the session prelaunch feature, simply click on the tile labeled "Session prelaunch is disabled - click to enable" near the top of the window.



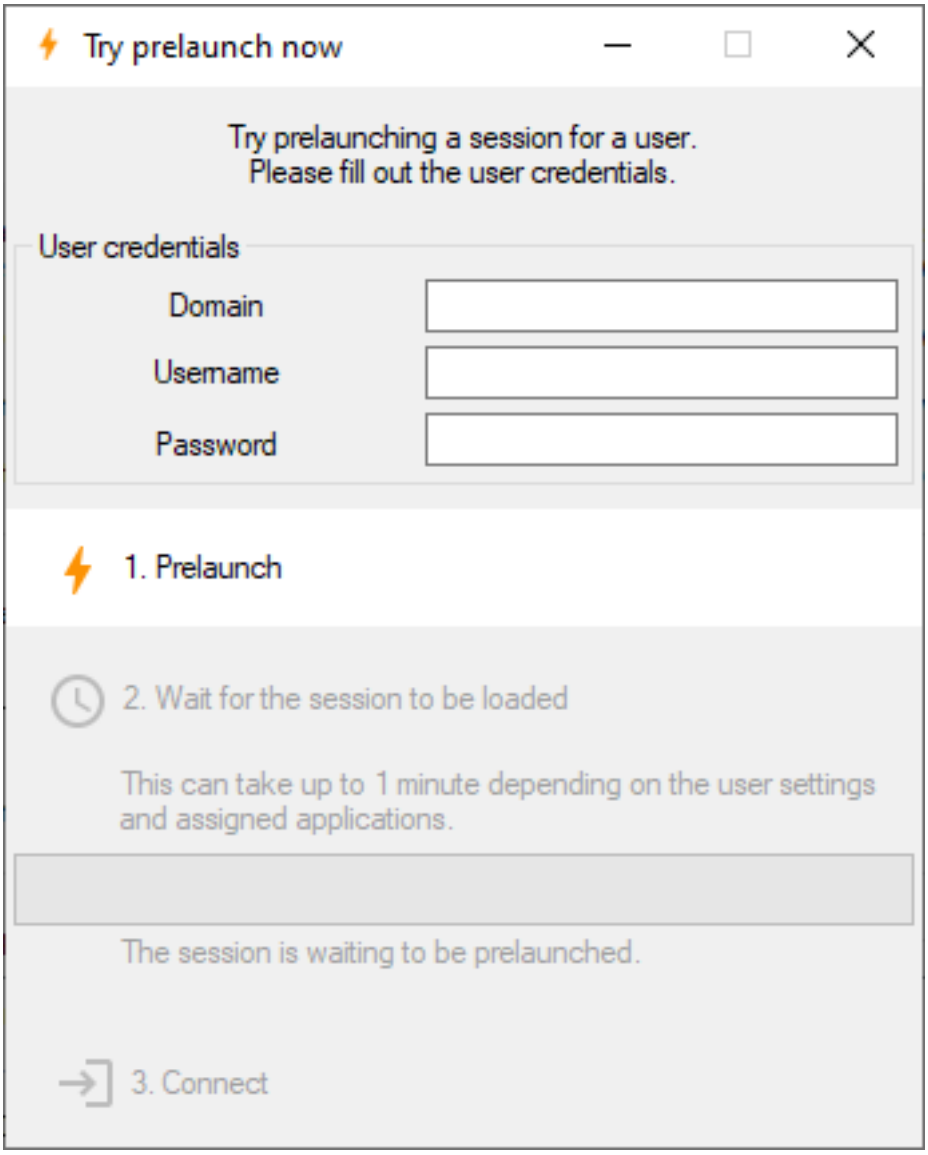
If any of the prerequisites aren't met when enabling Session Prelaunch, you will be asked if you want to automatically configure session settings to meet the prerequisites and use the feature. Note that changing session settings may require a reboot.

Test the session prelaunch

Once enabled, you will be able to quickly test the feature by clicking on the button "Try prelaunch now" at the top.



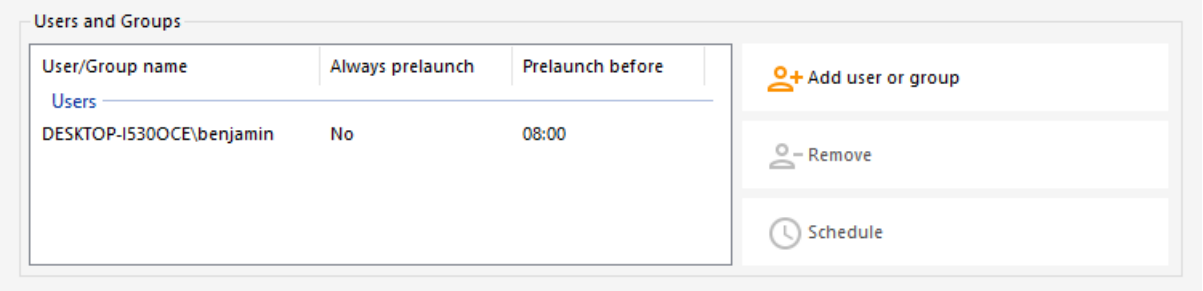
In the windows that appears, enter user credentials so that TSplus services can prelaunch the session for this specific user.



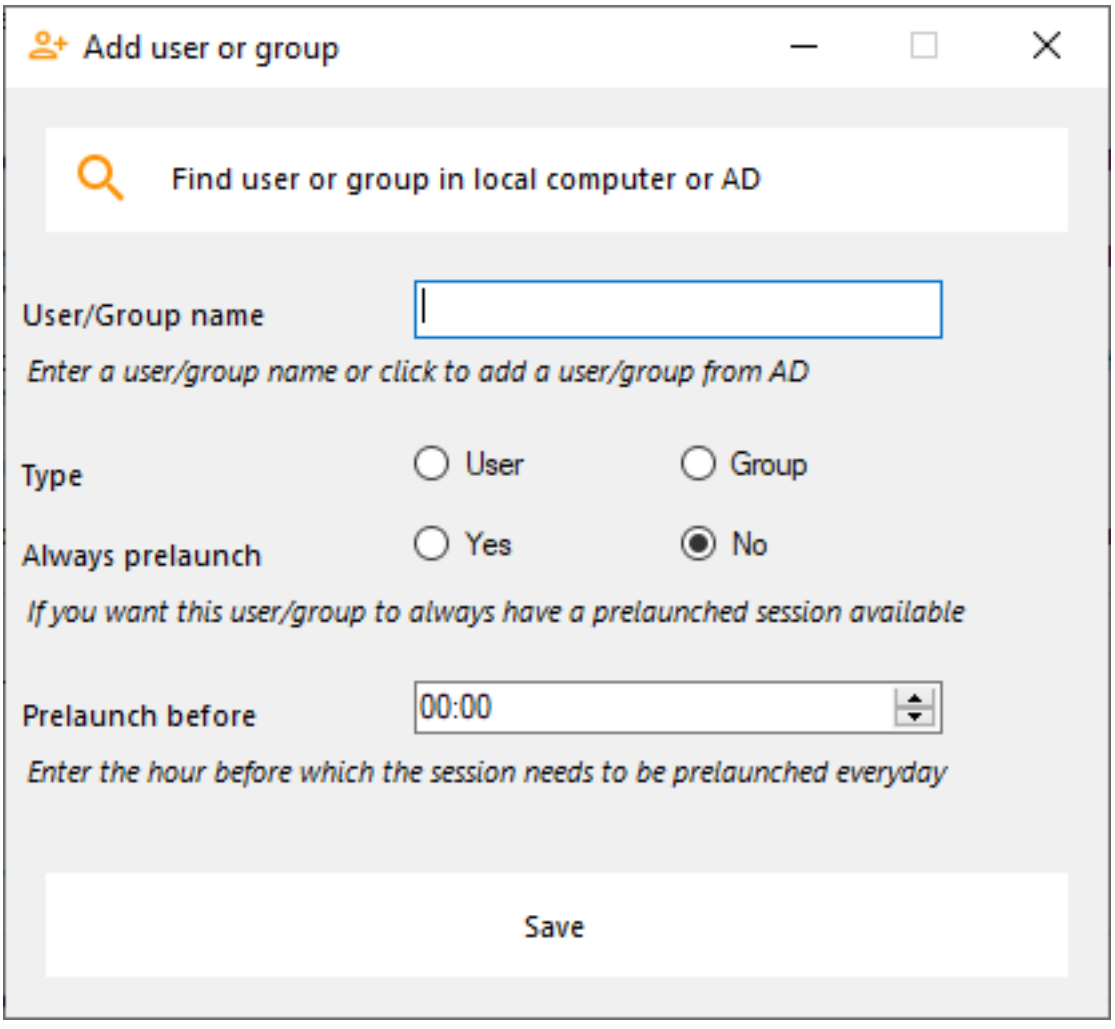
Click on "Prelaunch" to start and load a new session for this user.
Wait until it is fully loaded, and then click on "Connect" to capture the freshly loaded session.

Manage configured users and groups

To add session prelaunch users and groups, simply click on “Add user or group”.
To edit or remove a configured user, select the matching user/group in the configured user/group list, then click on “Schedule” to change the ‘prelaunch before’ time, or the “Remove” button to remove the user.



After clicking on “Add user or group”, you will be asked the user/group name to configure as well as the time before which the session needs to be loaded, called “prelaunch before” here.
You can also configure this user/group to always have a session prelaunched when connecting instead of having to schedule it by selecting “Yes” on the “Always prelaunch” option.



How to setup Apache reverse proxy support of Websockets

1. first of all change following variable to false www\software\html5\settings.js > W.xhrreverse = false; (if you don't change it to false, it will always try xhr instead websockets, what we don't want anymore)

2. install Apache with proxy_wstunnel support (older Apaches without proxy_wstunnel are unsupported!)

3. allow in Apache config (httpd.conf etc.) following modules. 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. let's assume you want to access html5 main portal via subfolder "/html5/" As example http://your_ip_or_domain.net/html5/ And Tsplus is installed in intranet on server "intranetxyz" then add to the config (httpd.conf etc.) following

   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. Restart Apache to take changes effect.

Two-factor Authentication

Two-factor authentication adds an extra layer of security and **prevents access to your users' session even if someone knows their password**.

A combination of two different factors is used to achieve a greater level of security:

1. something they know, **a password**.
2. something they have, a **device - such as a smartphone - with an authentication app installed.**.

You can use one of the following authenticator apps to proceed. These apps are available across a wide range of platforms:

- Authy
- Google Authenticator
- Microsoft Authenticator

Each time a user sign in to its remote session it will need its password and a verification code available from its mobile phone. Once configured, the authenticator app will display a verification code to allow him or her to log in any time. It works even if its device is offline.

OR you can decide to receive verification codes by **SMS**. In this case, you will have to create a free account on Twilio.

The **2FA codes generated are TOTP** (time-based one time password), and therefore are for single use.

Therefore, it is not possible to reuse a 2FA code that has already been used. This prevents the

theft and then the use of a 2FA code by observing the user while he enters his code.

Requirements

Two-factor authentication requires TSplus Remote Access **Mobile Web** or **Enterprise** Editions.

Two-factor authentication is supported by:

- TSplus Remote Access **Web portal**, for both HTML5 and Remoteapp connections
- TSplus Connection Client, for clients generated since version 15.30.3.15, with 2FA support explicitely enabled. See Portable Client Generator Support for Two-factor Authentication
- 2FA is related to Windows Users and not Web credentials

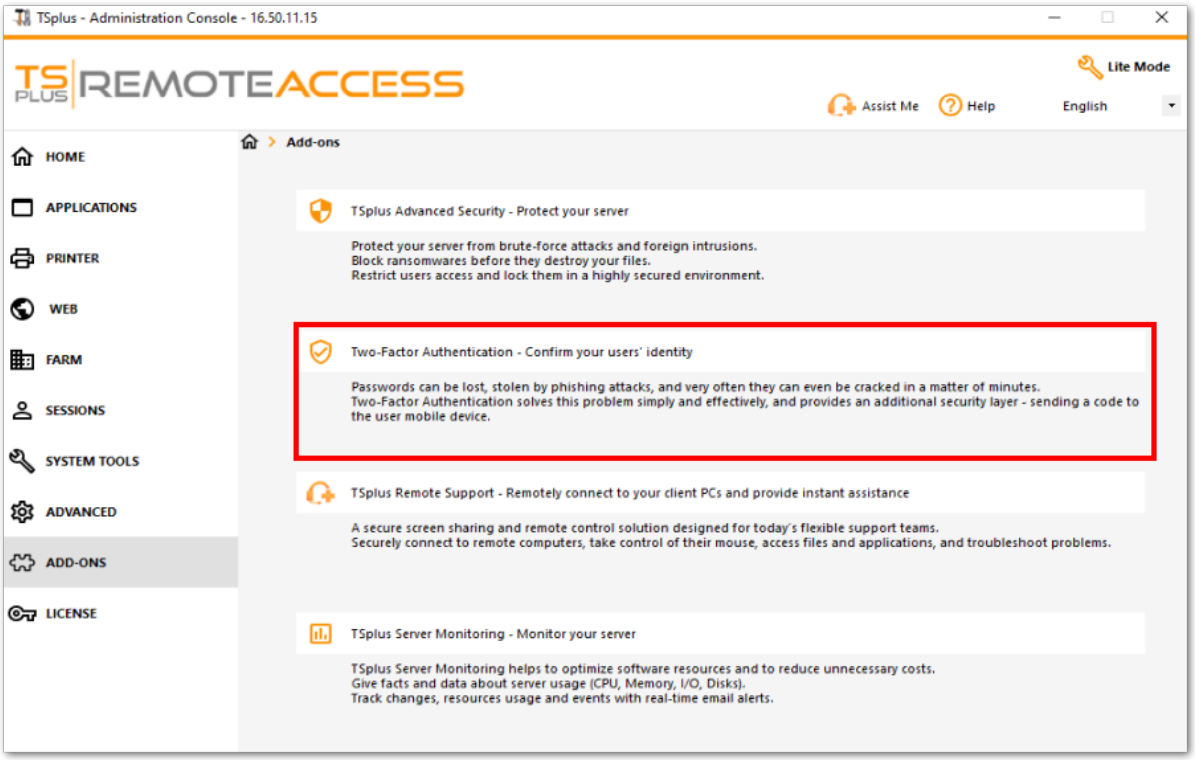
This authentication mode does not support login through standard Microsoft Remote Desktop client (mstsc.exe).

In order to provide an even safer solution, RDP connections are denied for 2FA enabled users.

As a prerequisite, TSplus server and Devices must be on time. See the Time Synchronization and Settings sections for more configuration information.

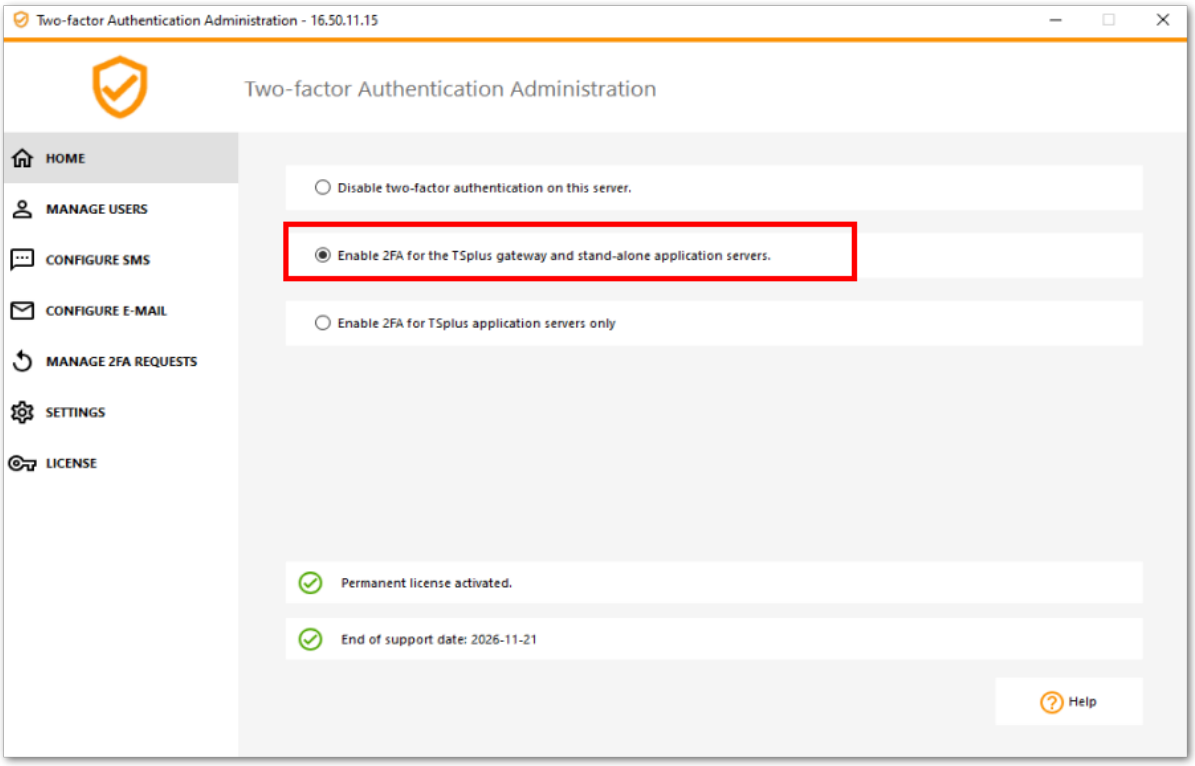
Activating Two-factor Authentication Add-On License

The Two-Factor Authentication feature can be found on the Add-On tab of the AdminTool:



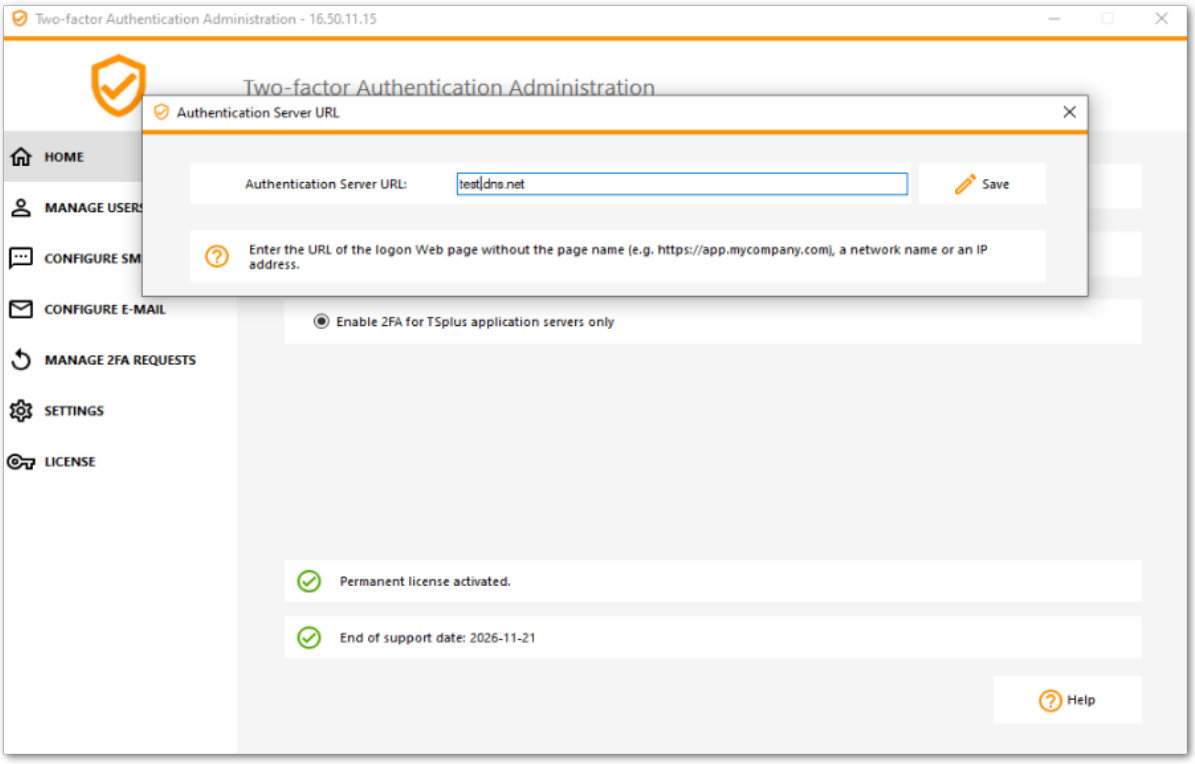
Perform the following steps to enable two-factor authentication for your TSplus server or deployment. If your TSplus deployment is configured to use multiple servers, perform this task on the TSplus server exposed as the single point of entry for users or having the reverse proxy role.

1. Open the two-factor authentication administration application. The two-factor authentication status and the license status are displayed:

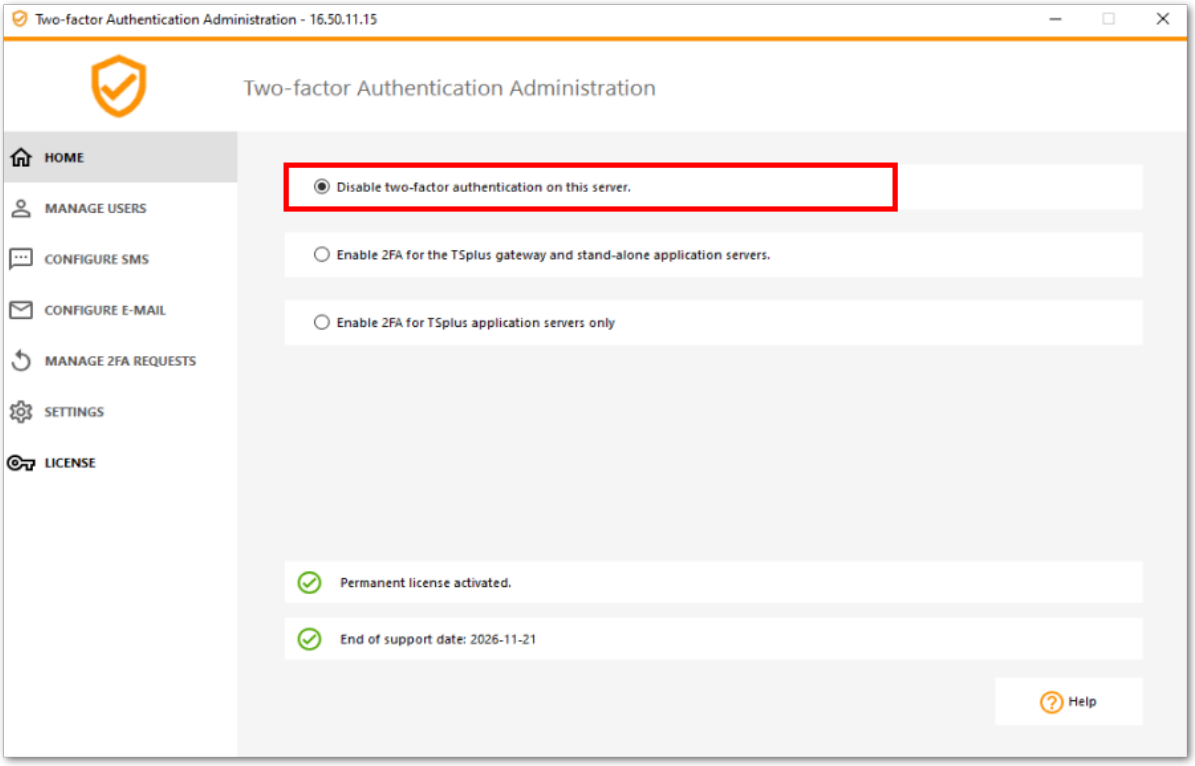


By default, 2FA is enabled for the TSplus gateway and stand-alone application servers.

You can enable it for TSplus application servers only, by entering the authentication server URL:



Or disable it:

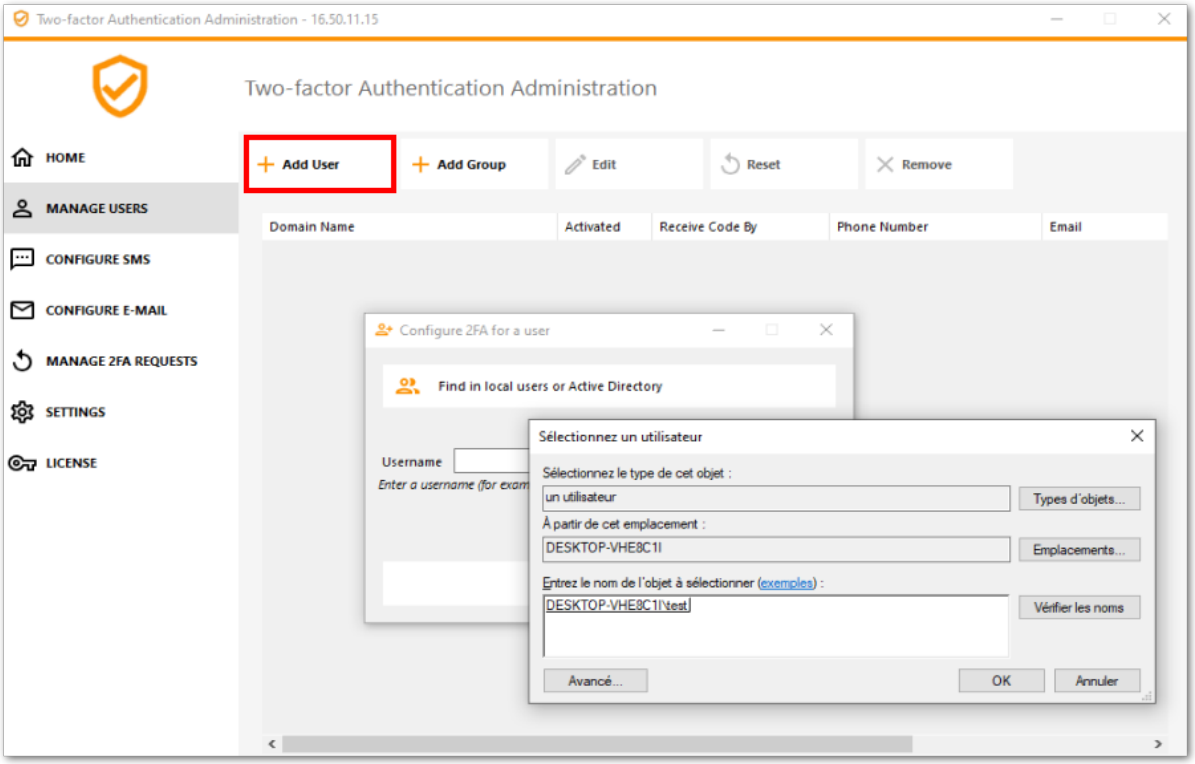


Add users and groups

Once two-factor authentication is enabled, you can configure users for two-factor authentication.

1. From the two-factor authentication administration application, click on the Manage Users tab.

2. Then, click on Add to select users and/or groups of users. The Select Users or Groups box opens.



3. Add as many users and groups as required and then click OK. The users and groups are added to the list and enabled for two-factor authentication.

Here are commands to add users/groups
3 types of possible arguments:

just the domainName
TwoFactor.Admin.exe /addusers domainName1

- adds the user with the default values (reception method = app, email and telephone fields not entered)

the domainName and the reception method
TwoFactor.Admin.exe /addusers domainName1;SMS

- adds the user with the desired receive method, but does not attempt to activate it

the domainName, the reception method, the Phone field (even if empty), the Email field (even if empty)
*TwoFactor.Admin.exe /addusers domainName1;SMS;+33606060606;username1@truc.net

domainName2;Email;;username2@truc.net domainName3;SMS;+33606060607;domainName4 *

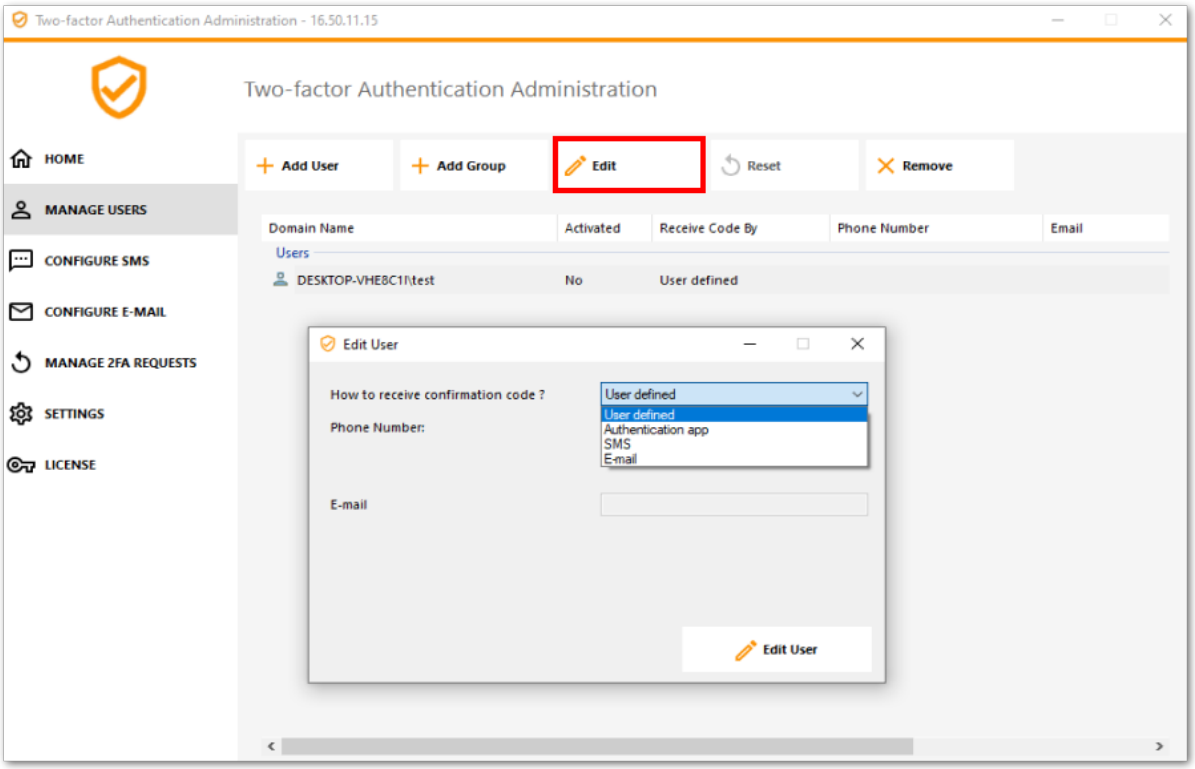
- Same behavior as in the HMI, when we add a user, then edit it with correct information: we try to activate the user

As shown in the last example, several users can be indicated (separated by a space). The different fields of a user are separated by a semicolon

For single groups:
TwoFactor.Admin.exe /addgroups group1 group2 group3

Edit users

On the same tile, you can edit the way users receive verification codes by selecting a user and clicking on the “Edit” button:

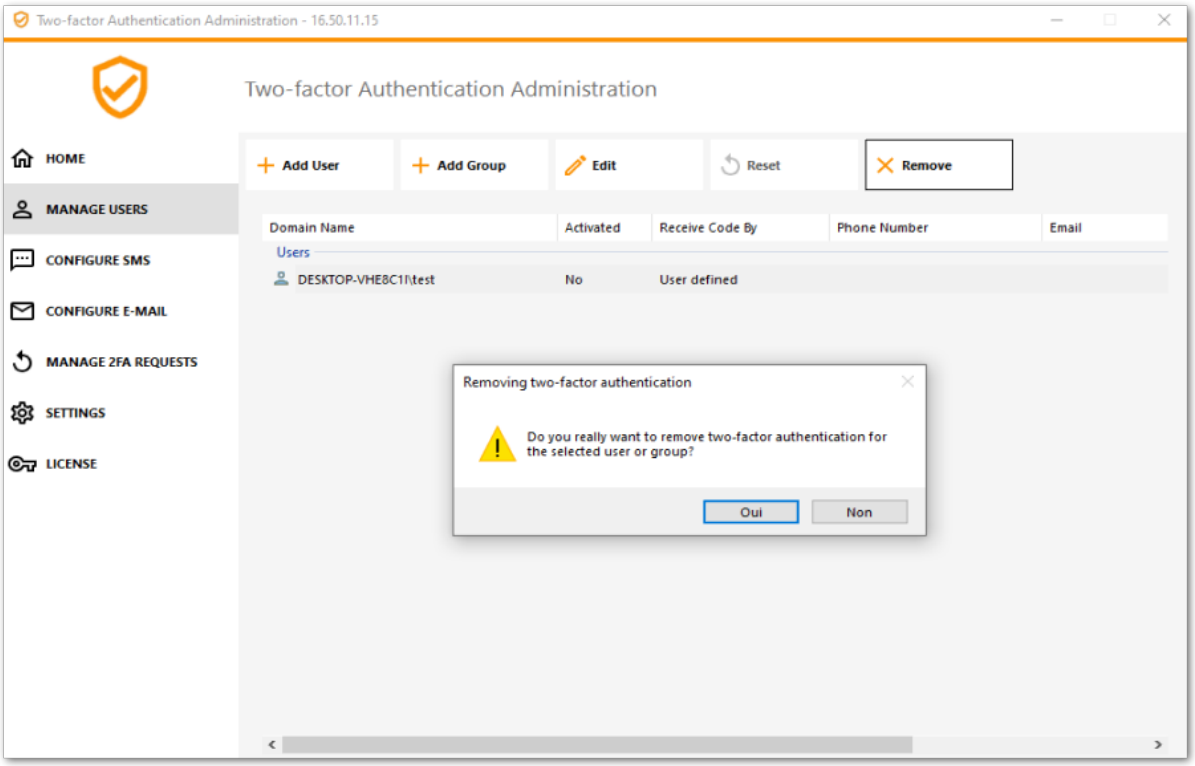


The user receives verification codes on the authentication app by default. You can choose that he/she receives it by SMS or EMAIL by selecting the option.

Selected SMS and added the user’s phone number in the field or selected EMAIL and added the user’s email.

Remove Users and Groups

In order to remove users or groups, select the user or the group and then click on Remove. A confirmation message is displayed.



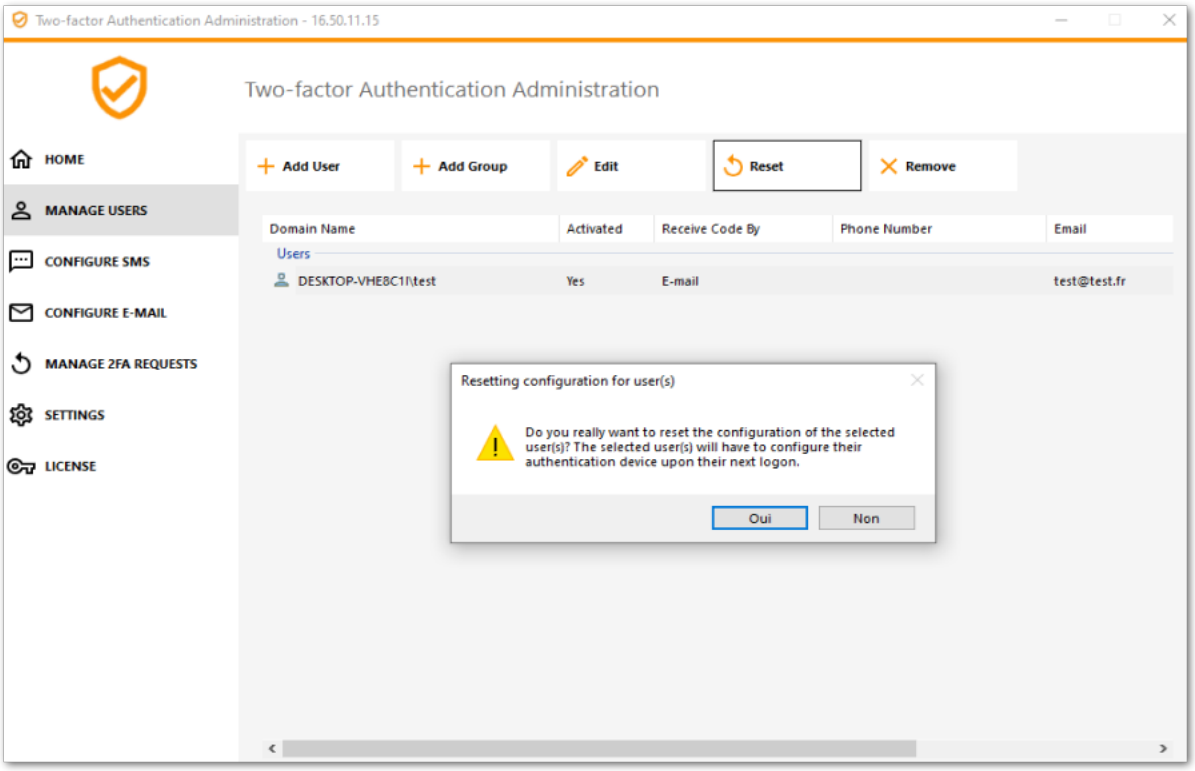
Click Yes. The user or the group is removed from its list and won't connect using two-factor authentication anymore.

Reset Configuration for Users

In the event of the loss of the authenticating device for a user, or if the user needs to display the secret QR code again, you must reset the user authentication settings.

1. From the two-factor authentication administration application, click on the Manage Users tab.

2. Select one or multiple activated users and then click on Reset. A confirmation message is displayed:



3. Click Yes. The selected users will be presented a new QR code at the next login and will have to scan it in their device's authentication app.

You can also modifiy the user's phone number, so that he can receive a verification code on his new device.

Enroll User for Two-factor Authentication

Once a user has been enabled for using two-factor authentication, an activation message will be displayed at his next successful logon from the TSplus Web portal.



In order to complete the required steps, you have two choices: either generate codes via an authenticator app, either make the user receive codes by SMS.

Receive codes with an Authenticator Application

The user must install an authenticator app on a portable device, such as his smartphone.

You can use one of the following authenticator apps to proceed. These apps are available across a wide range of platforms:

- Authy
- Google Authenticator
- Microsoft Authenticator

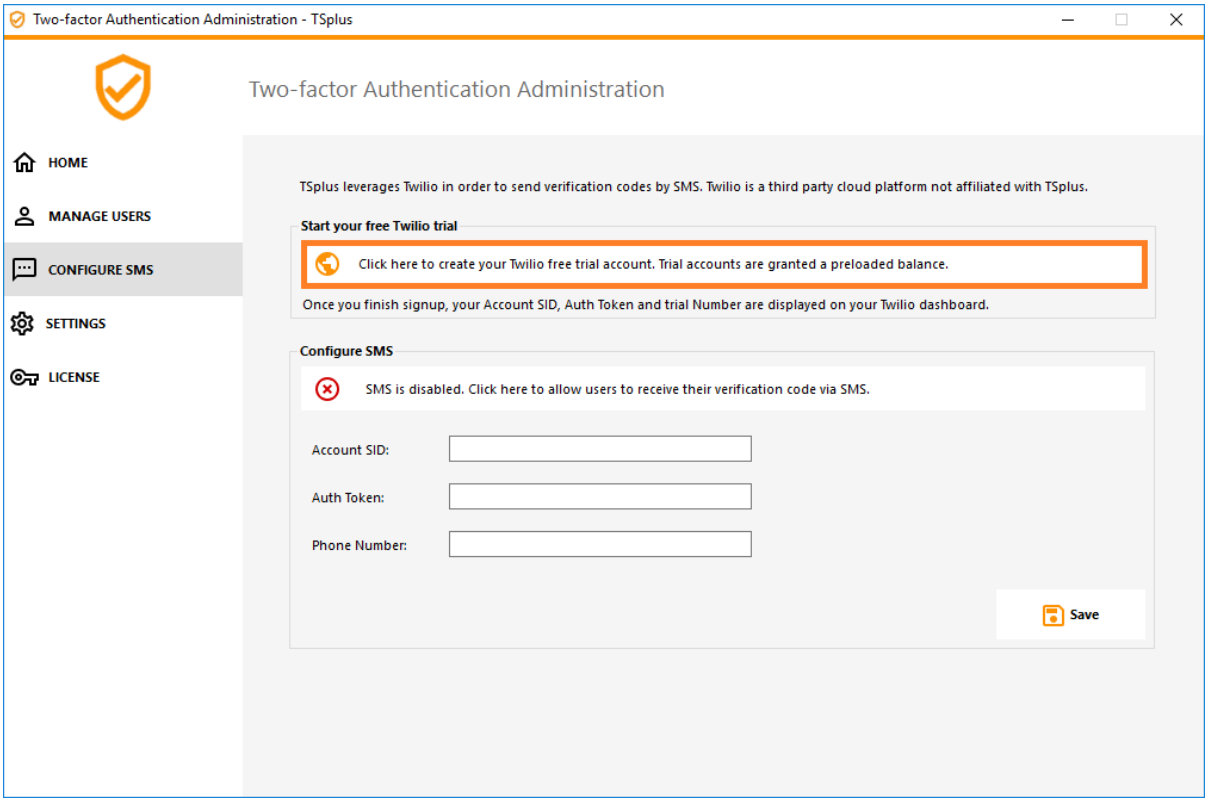
Please use each app documentation for more details on how to proceed to add your TSplus account.

Configure SMS

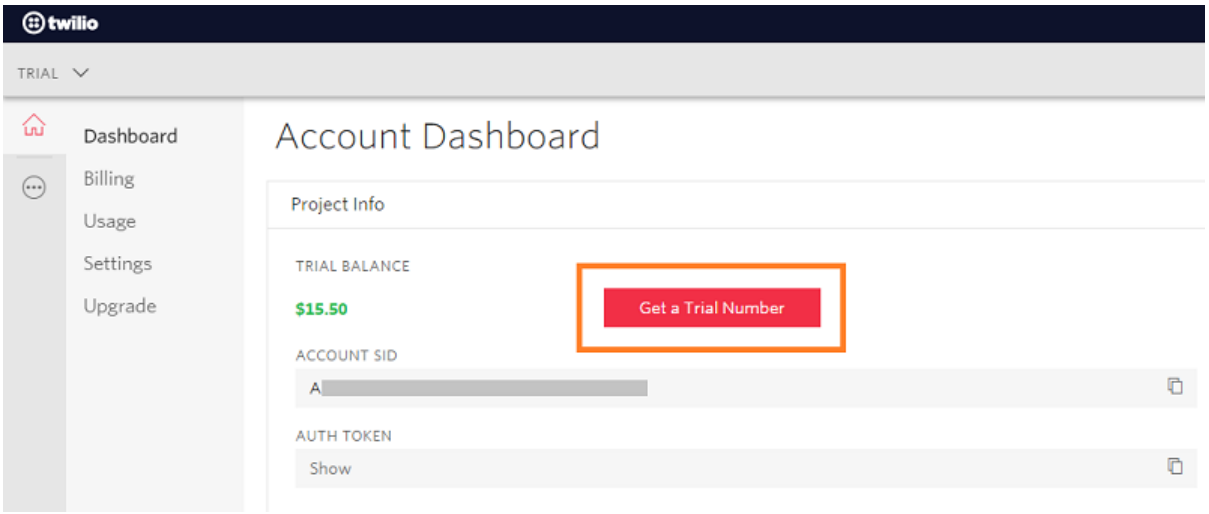
In order for the user to receive verification codes by SMS, you must first enable it. Click on the Configure SMS tab:

TSplus leverages Twilio in order to send verification codes by SMS. Twilio is a third-party cloud platform, not affiliated with TSplus.

1. Just create a free account on Twilio by clicking on the button below “Start your free trial with Twilio”:

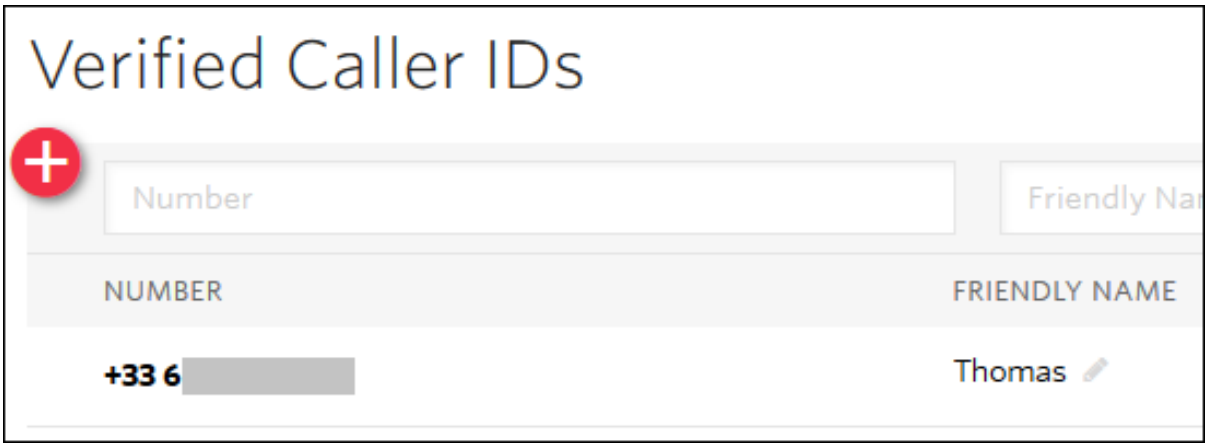


2. On your Twilio account dashboard, you will need to activate your Trial Number:

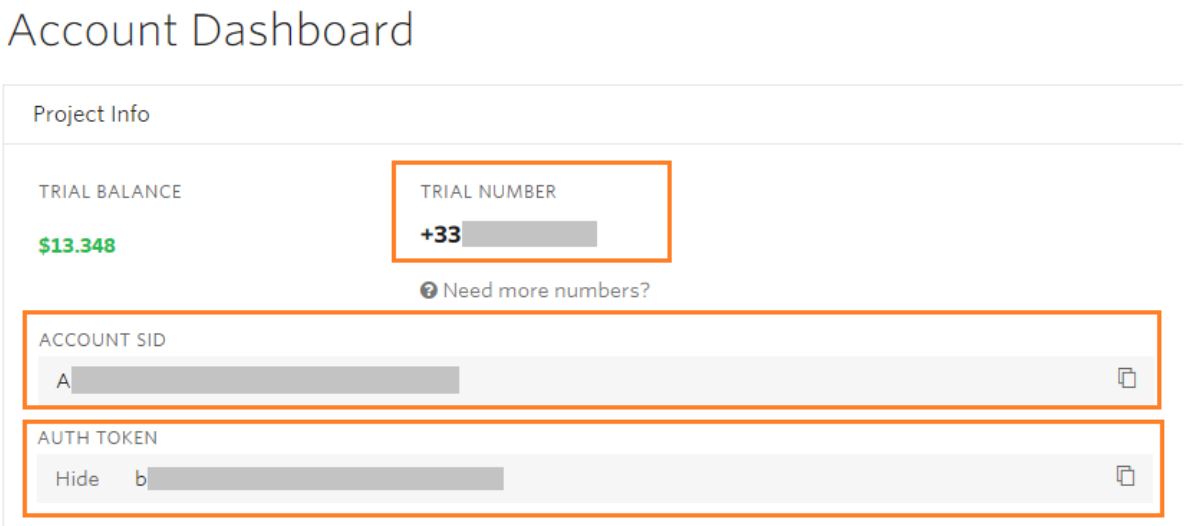


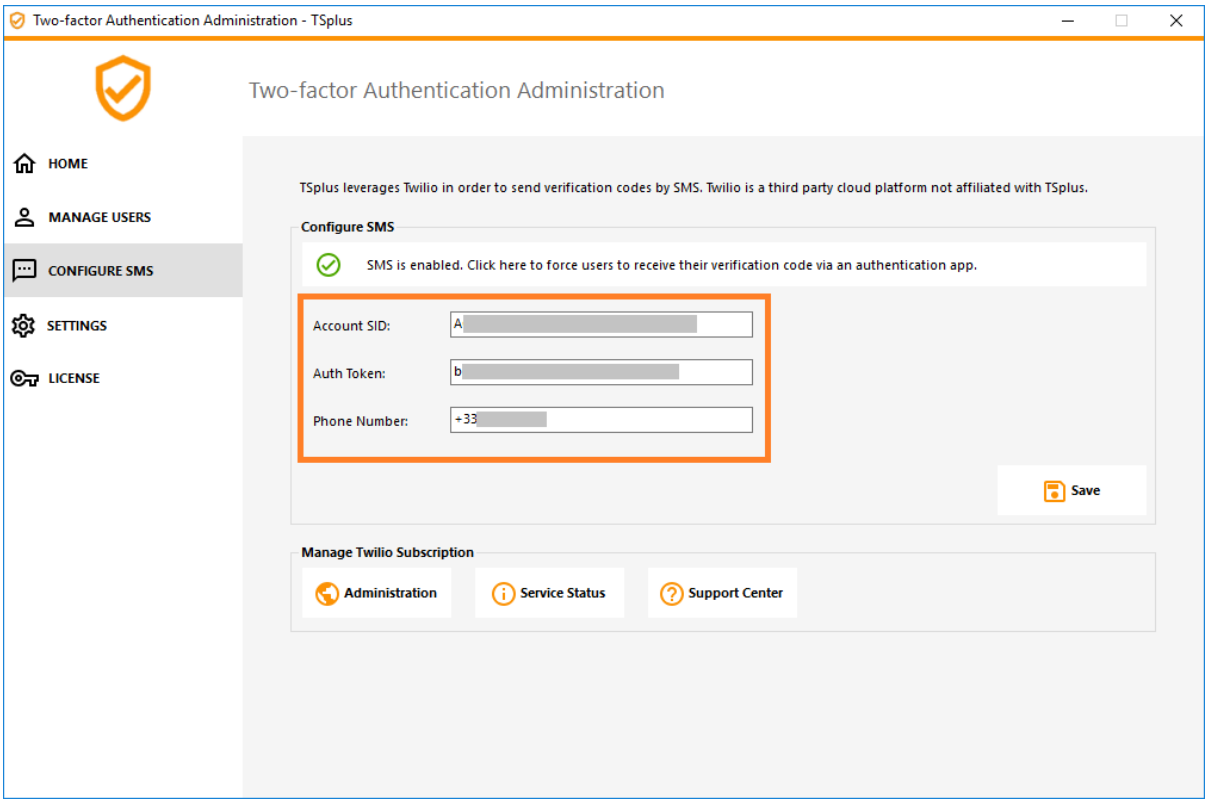
3. The next step is only necessary for Trial versions. It allows Twilio to verify the actual phone number on which SMS will be sent.

Enter this number under the [“Phone Numbers” menu - “Verified Caller IDs”](#) tab :

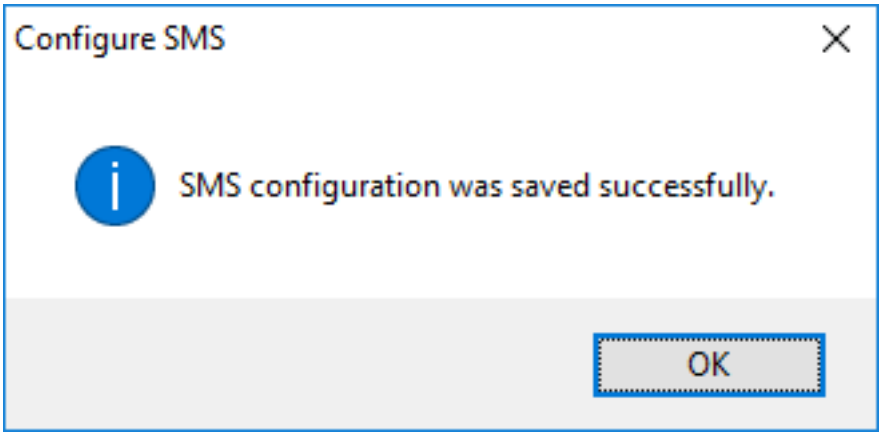


4. You will then be able to enter your account SID, Authentication Token and **Trial Number** as the Phone Number on the Configure SMS tab of TSplus:





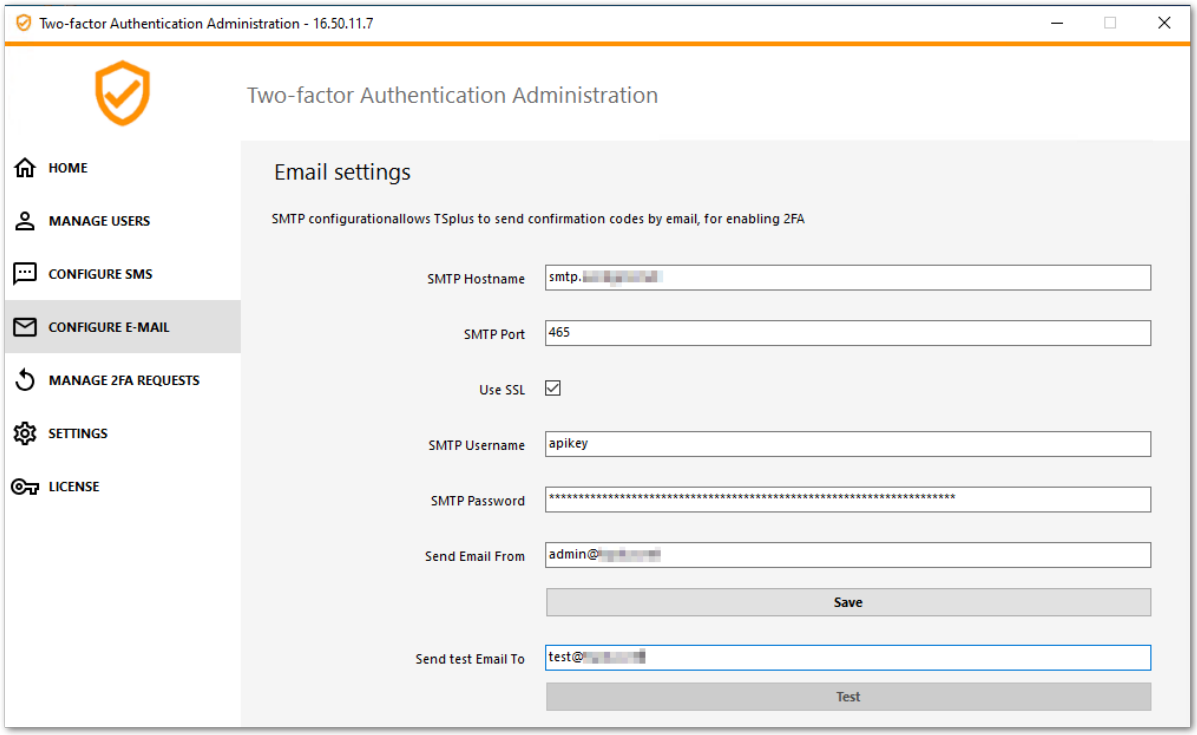
Then, click on Save. The following message will be displayed:



You can manage your Twilio subscription on the Manage Twilio subscription section, at the bottom of the Configure SMS tab. Administrate your account, see the Service Status or reach Twilio Support Center just by clicking on the corresponding buttons.

Configure EMAIL

For the user to receive verification codes by EMAIL, you must first configure your SMTP email.



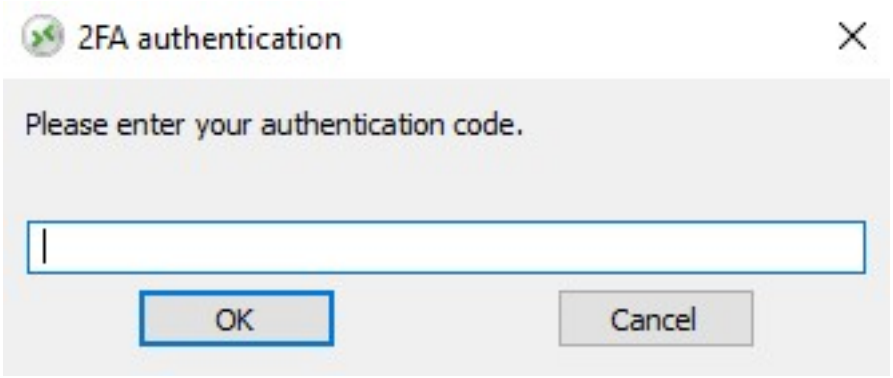
Login using Two-factor Authentication

Once a user has configured his TSplus account in his authenticator app, he or she will be able to connect using its password and the code provided by its authenticator app, by SMS or Email.

From the TSplus Remote Access Web portal:



From the TSplus generated client:



TSplus application servers and client devices must share the same time. This means that the time and date of the server must be synchronized with a time server. Client devices must also have time synchronization, regardless of the time zone on which they are configured.

If an authentication request comes from a Device whose date and time are not synchronized, or if the server's date and time are not synchronized, this request may be rejected.

The validation of information between the Device and the server relates to UTC time.

In the **Settings** section, the Discrepency parameter is used to manage the period of validity of the code, in intervals of 30 seconds.

Example of validation or valid authentication:

- the server is synchronized with a time server, the time zone is UTC + 2, it is 2:30 pm
- the Device is synchronized with a time server, the time zone is UTC + 1, it is 1:30 pm
- the Discrepency parameter is configured at 60, i.e. a code validity period of 30 minutes
- referred to UTC time, the Device time and the server time are identical.

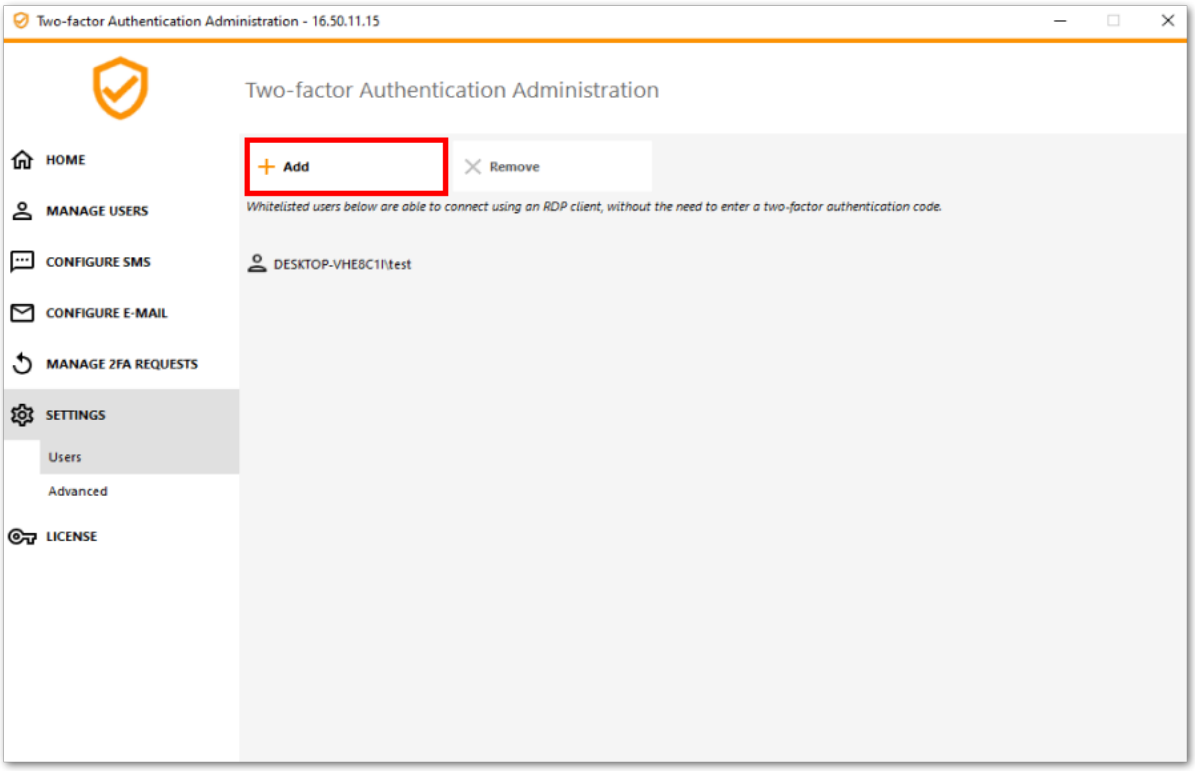
Example of validation or invalid authentication:

- the server is synchronized with a time server, the time zone is UTC + 2, it is 2:30 pm
- the Device is not synchronized with a time server, the time zone is UTC-1, the time is manually set to 1:30 pm
- the Discrepency parameter is configured at 60, i.e. a code validity period of 30 minutes
- the server time referred to UTC time is 12:30 am
- the time communicated by the Device, referred to UTC time is 2:30 pm
- the difference is 120 minutes, the validation code is therefore refused.

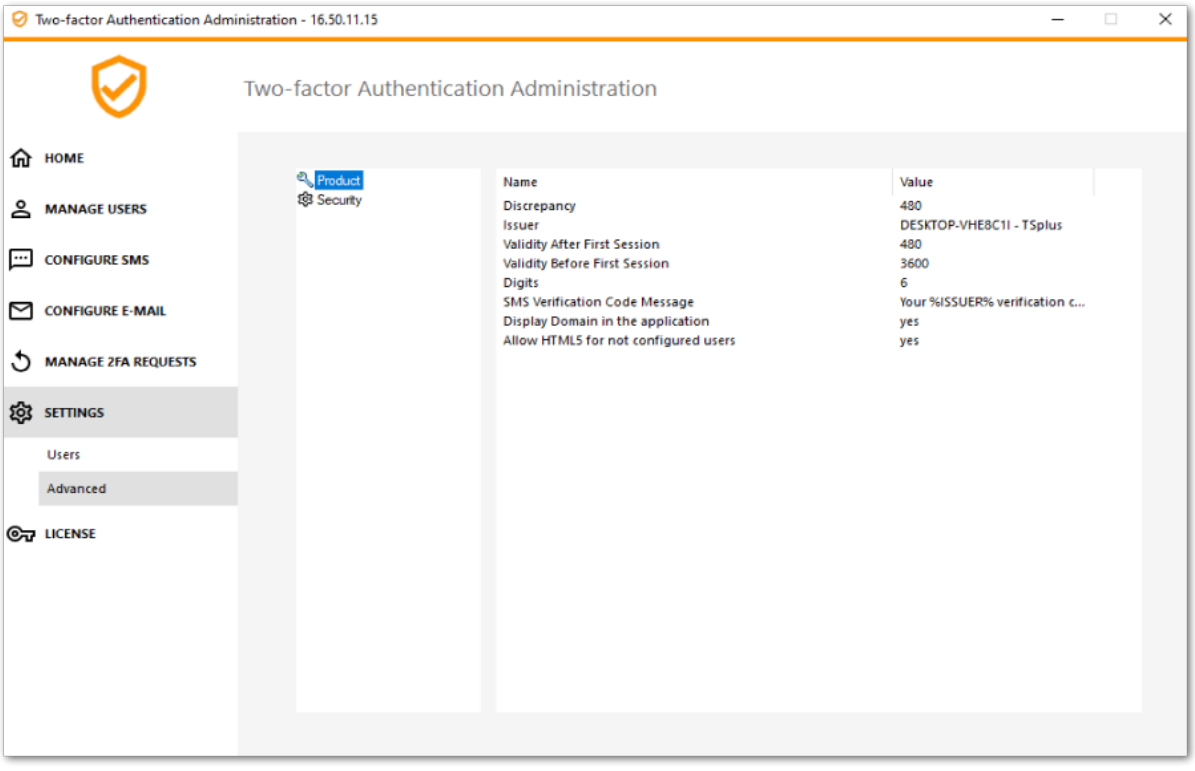
Settings

The Settings tab allows you to **whitelist users, in order for them to connect using an RDP client, without the need to enter a two-authentication code.**

Click on the "Add" button to add a user and remove a user by selecting it and clicking on the "Remove" button.



The Advanced tab allows you to configure Two-Factor Authentication in-depth settings.

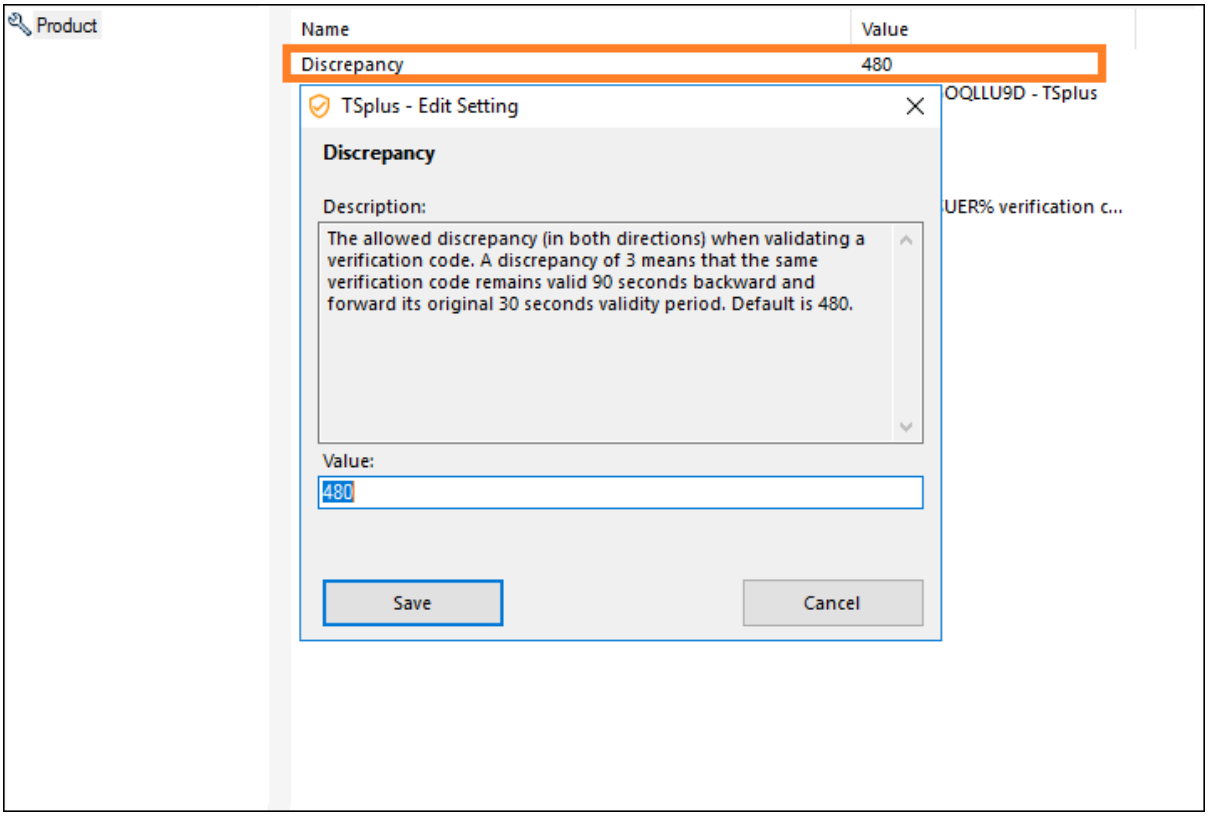


Discrepancy

You can modify the Discrepancy value, which allows you to set the validation time of a verification code.

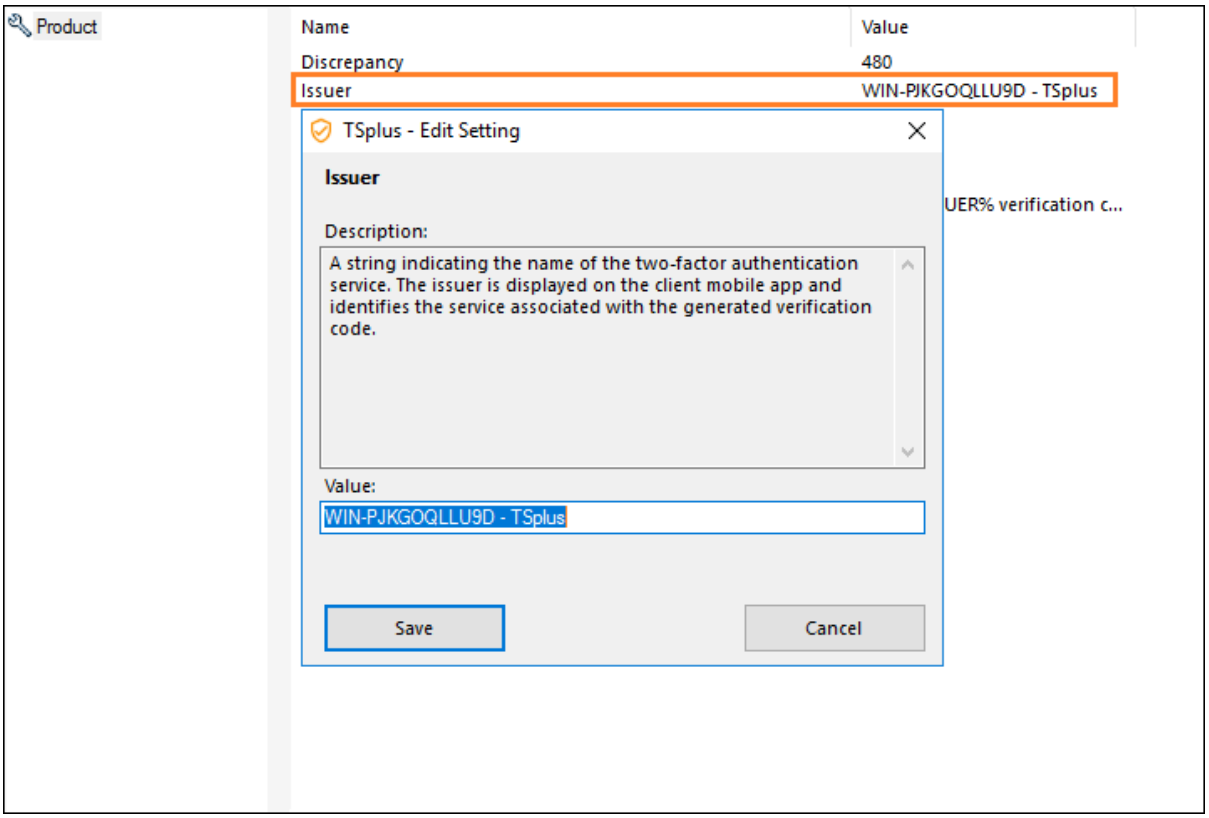
A discrepancy of 3 means that the same verification code remains valid 90 seconds backward

and forward its original 30 seconds validity period. Default is 480, which means 480 x 30 seconds= 4 hours.



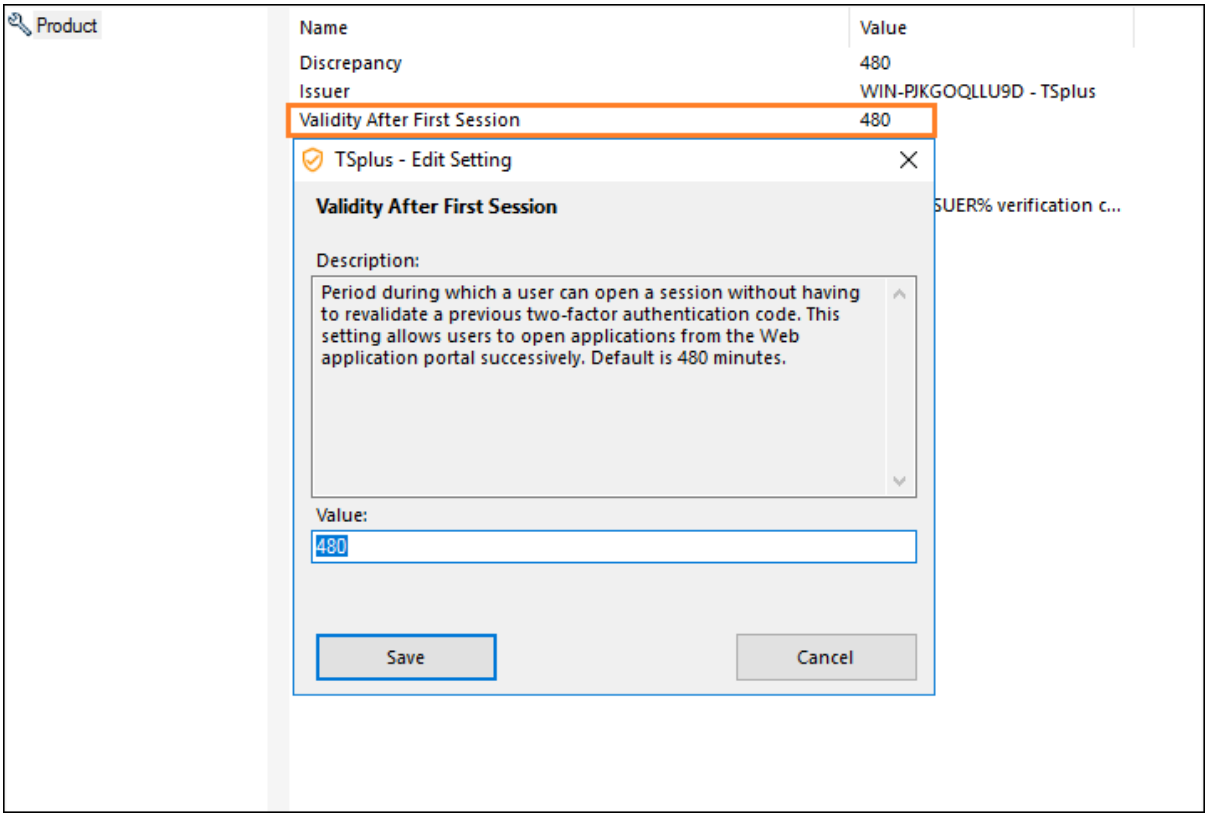
Issuer

A string indicating the name of the two-factor authentication service. The issuer is displayed on the client mobile app and identifies the service associated with the generated verification code. By default, it is composed of the server's name with TSplus.



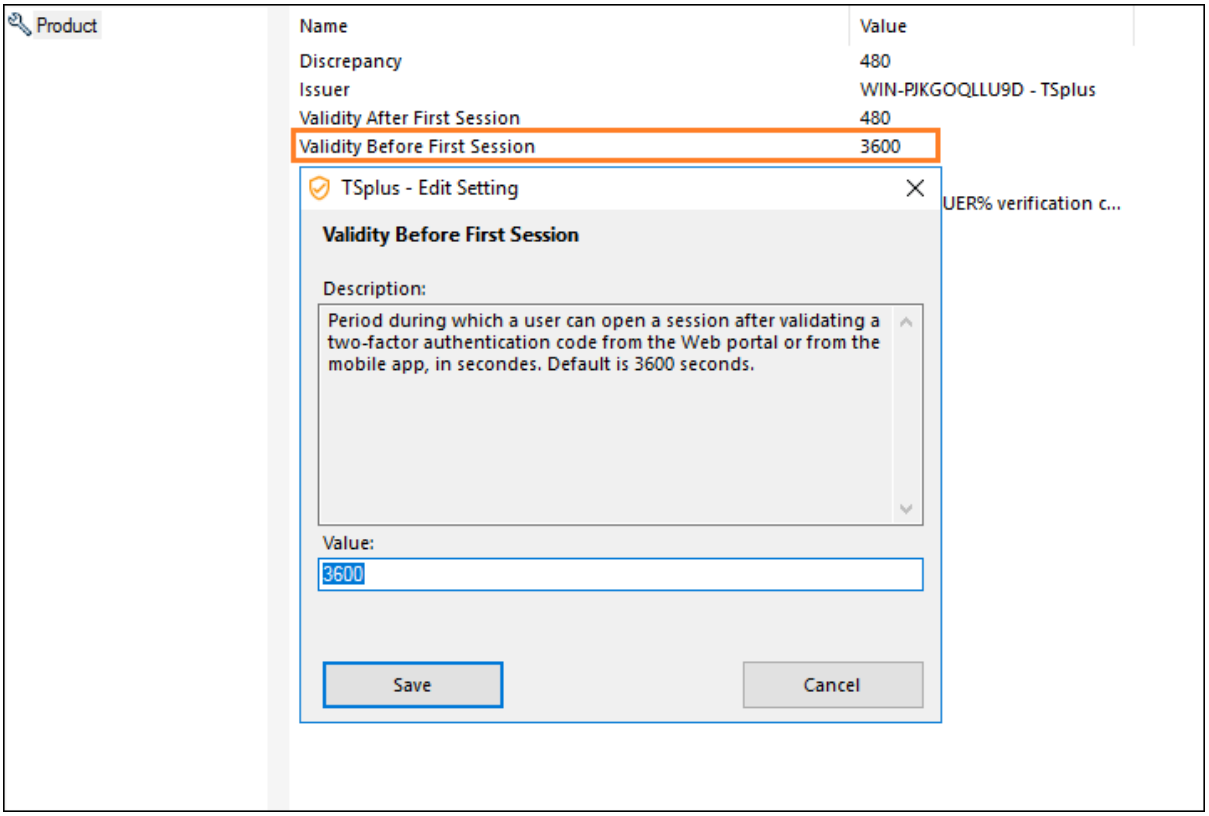
Validity After First Session

Period during which a user can open a session without having to revalidate a previous two-factor authentication code. This setting allows users to open applications from the Web application portal successively. Default is 480 minutes.



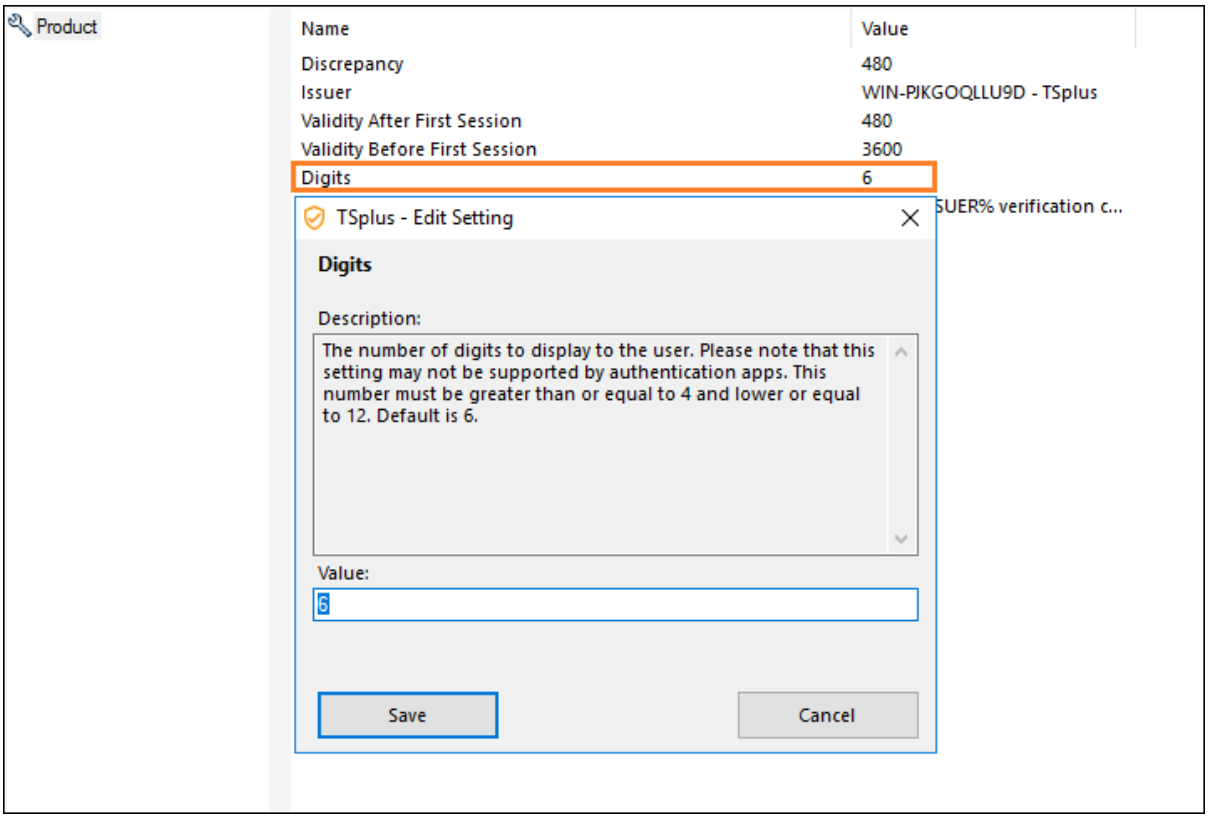
Validity Before First Session

Period during which a user can open a session after validating a two-factor authentication code from the Web portal or from the mobile app, in secondes. Default is 3600 seconds.



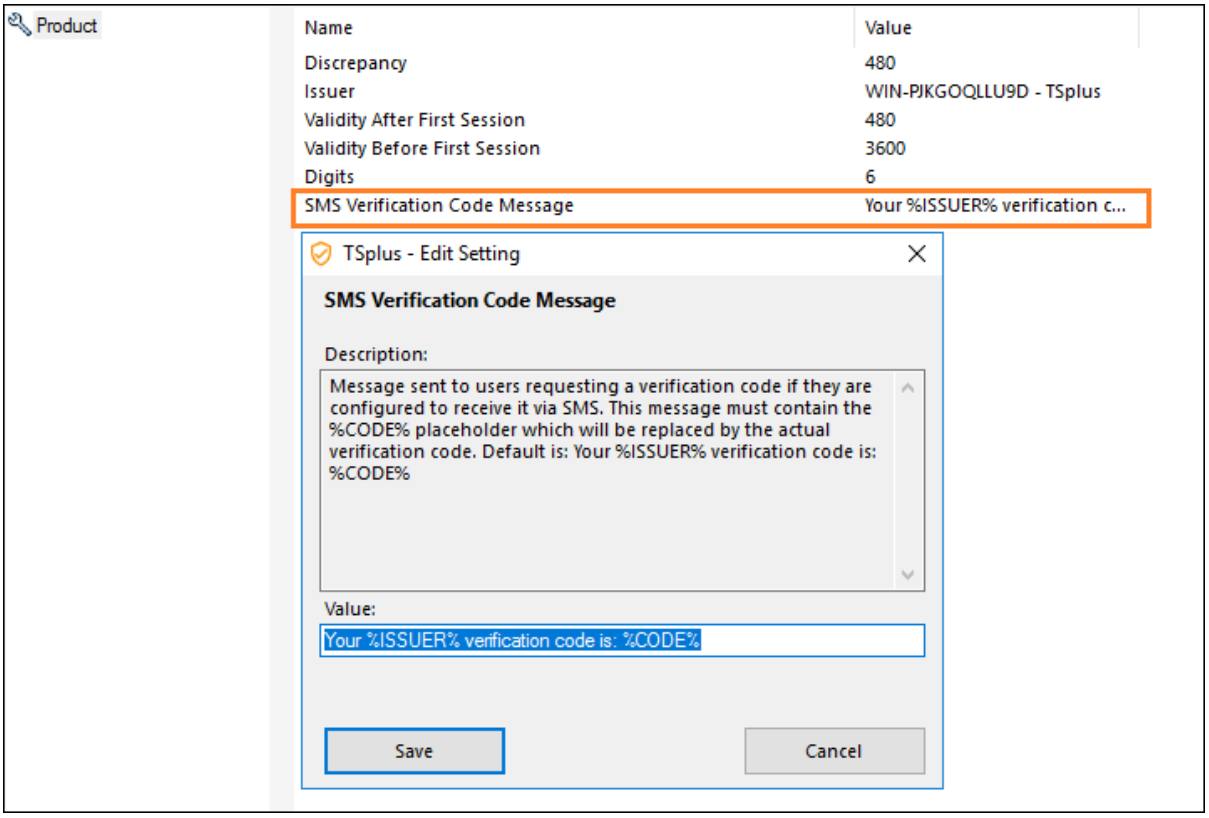
Digits

The number of digits to display to the user. Please note that this setting may not be supported by authentication apps. This number must be greater than or equal to 4 and lower or equal to 12. Default is 6.



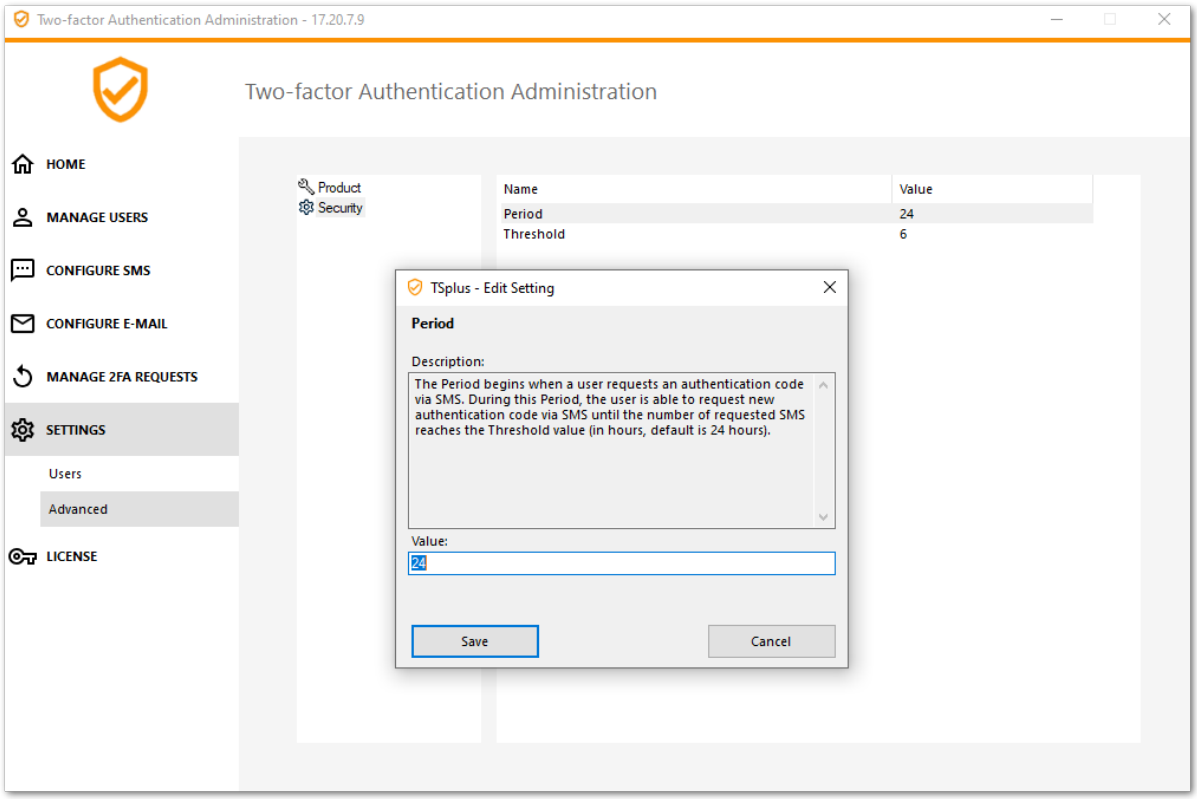
SMS Verification Code Message

Message sent to users requesting a verification code if they are configured to receive it via SMS. This message must contain the %CODE% placeholder which will be replaced by the actual verification code. Default is: Your %ISSUER% verification code is: %CODE%



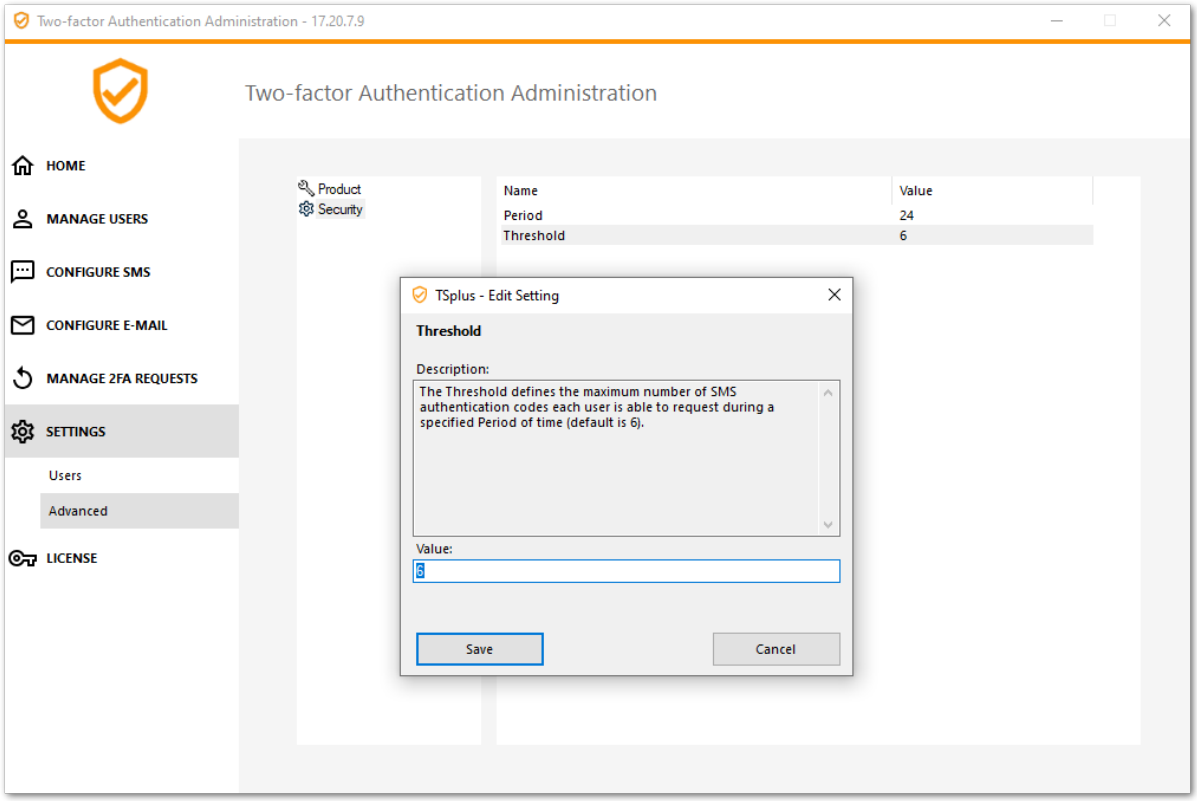
SMS Security Period

The Period begins when a user requests an authentication code via SMS. During this Period, the user is able to request new authentication code via SMS until the number of requested SMS reaches the Threshold value (in hours, default is 24 hours).



SMS Security Threshold

The Threshold defines the maximum number of SMS authentication codes each user is able to request during a specified Period of time (default is 6).


Two-factor Authentication Administration - 17.20.7.9
Two-factor Authentication Administration
HOME
MANAGE USERS
CONFIGURE SMS
CONFIGURE E-MAIL
MANAGE 2FA REQUESTS
SETTINGS
Users
Advanced
LICENSE
Product
Security
Name
Value
Period
24
Threshold
6
TSplus - Edit Setting
Threshold
Description:
The Threshold defines the maximum number of SMS authentication codes each user is able to request during a specified Period of time (default is 6).
Value:
6
Save
Cancel

Universal Printer (novaPDF)

The TSplus Universal Printer allows you to preview or print documents from any PC or mobile device supported by TSplus Remote Access. Universal Printer is relevant from an HTML5 session and when connected using a generated client. Universal Printer is not relevant when using the standard RDP client (mstsc.exe) because printers can be shared between server and client.

Starting Remote Access version 17, Universal Printer leverages novaPDF (https://www.novapdf.com/) to produce 100% industry-standard PDF (Portable Document Format) files from the remote document. The generated PDF document is then sent to the desired local printer. The Universal Printer (novaPDF) replaces Universal Printer (CustPDF) and Universal Printer (GhostScript) which are discontinued and no longer available to install on your Remote Access server.

Two printers are available for remote printing: Universal Printer and Virtual Printer. Although Virtual Printer offers better printing performance, it is not compatible with the HTML5 client and requires to install a client application. Therefore, the Universal Printer is set as the default printer following Remote Access setup. See TSplus Virtual Printer.

Requirements

NovaPDF11Service service should be in the exlcusion list of any active firewall or antivirus.

Configure the Universal Printer

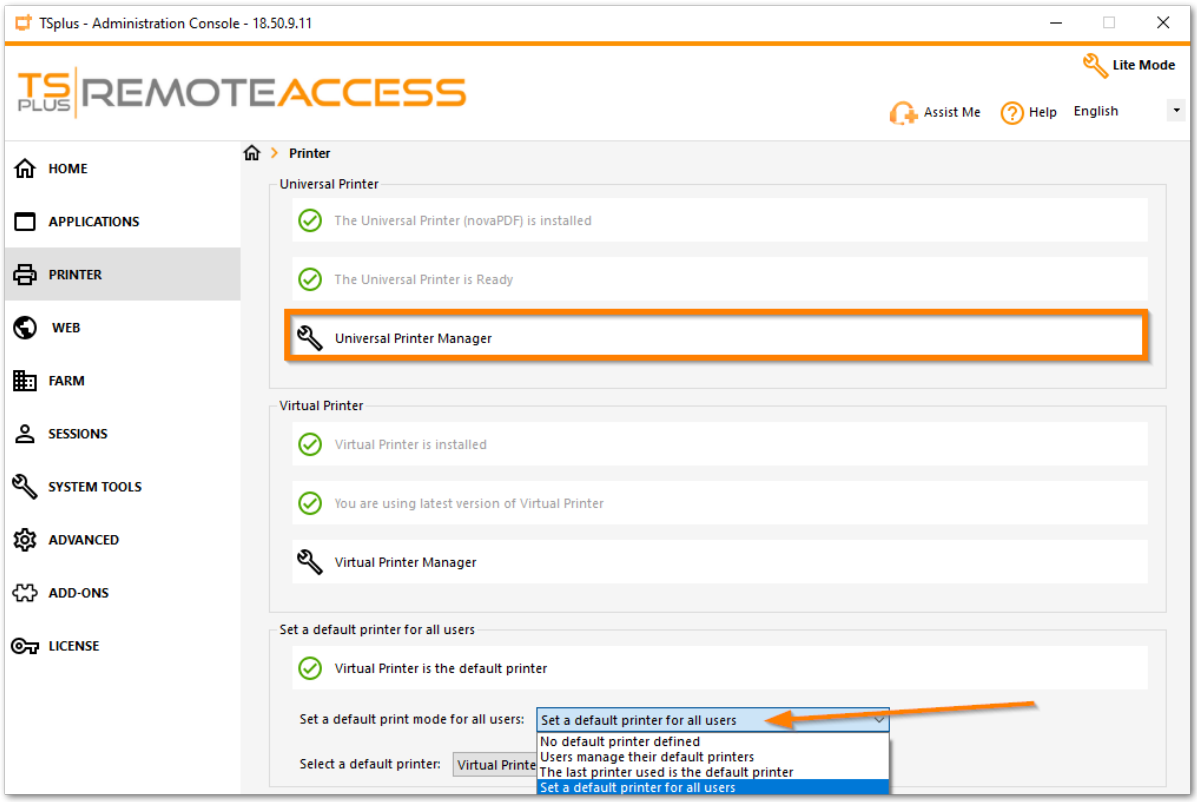
To configure your Universal Printer, open the AdminTool and click on the Printers menu.

To access to Universal Printer control panel, please navigate through the AdminTool: Printer > Universal Printer Manager

Set a default printer for all users

- No default printer defined: the user's default printer configuration is not affected.
- User manage their default printers: the "Let Windows manage my default printer" option is disabled, and it is therefore up to the user to select their default printer.

- The last printer used is the default printer: the “Let Windows manage my default printer” option is enabled.
- Set a default printer for all users: the administrator forces the user’s default printer.



The Universal Printer section displays fours tiles which enables administrators to:

- Check the Universal Printer setup status. If the Universal Printer is not installed, then clicking on the tile will install the Universal Printer.

- Check the Universal Printer printing status. If the Universal Printer is not ready to receive print jobs, the tile may display additionnal relevant information about the error.

- Check if the Universal Printer is set as the default printer. If the Universal Printer is not set as the default printer, then clicking on the tile will set it as the default printer. Please note that this behavior may be overriden by your users should they be allowed to do so.

- The tile named **Universal Printer Manager** leads to an more detailled screen which provides additonnal actions and properties, such as removing the Universal Printer.

Universal Printer Manager

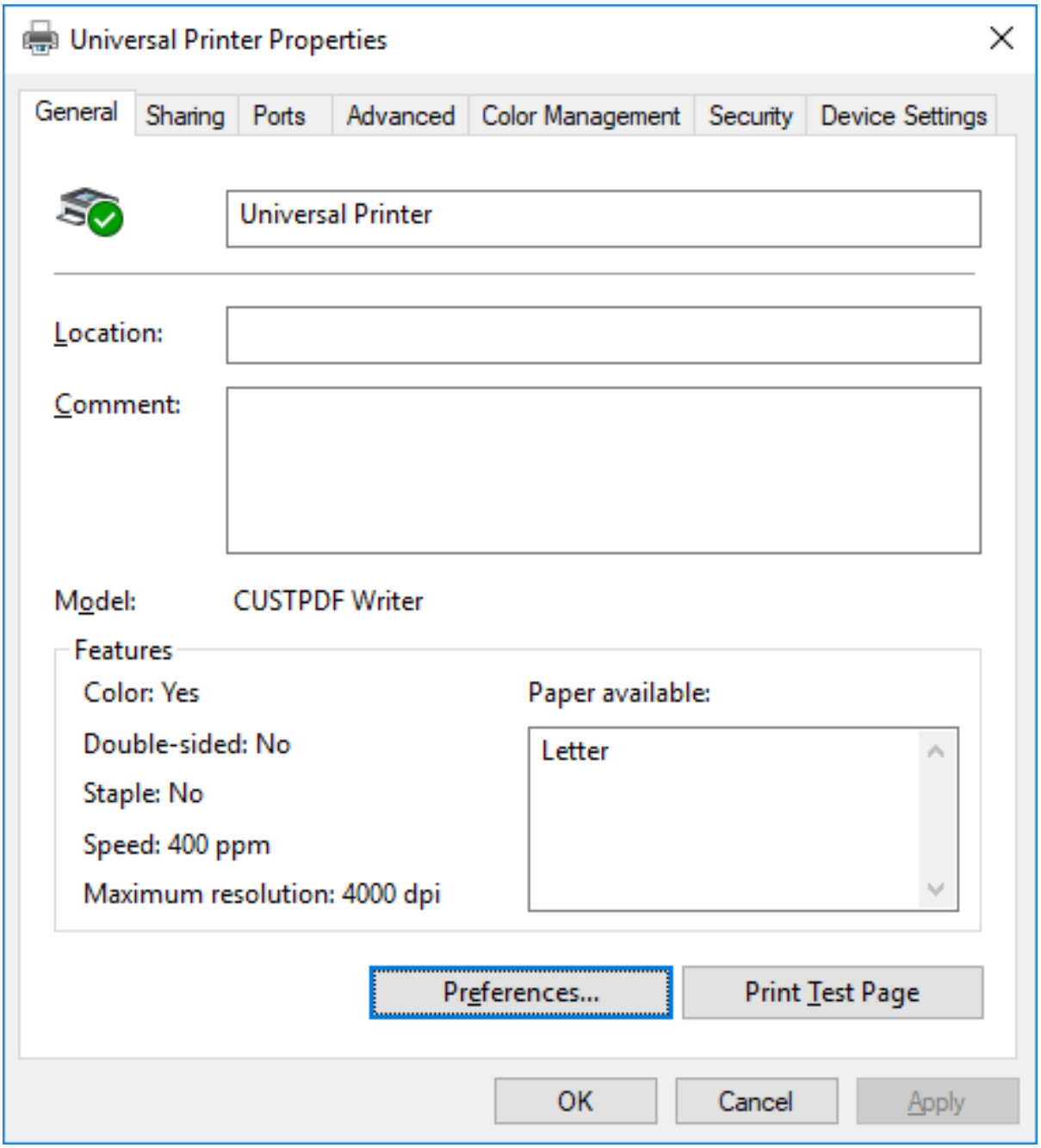
The Universal Printer Manager allows administrator to check the Universal Printer status, remove the Universal Printer, access to the printing queue and printer properties.

In particular, the button located at the bottom of the page allow administrators to:

- **Remove the Universal Printer**: Uninstall the Universal Printer. It can be reinstalled later from this screen.

- **View Printer**: Opens a window where you can see the status of your printing documents, pause, resume or cancel the print job. You can also set your printing preferences and properties.

- **Universal Printer Properties**: Opens this window, where you can see all the printing properties. After the General Tab, there are tabs for sharing, ports, advanced, color management, security and device settings. At the bottom of the popup window, the printer **properties** allows administrators to set the page size for printing from A4 to any kind of printing format. You can also choose between two printing orientations: Portrait or Landscape.

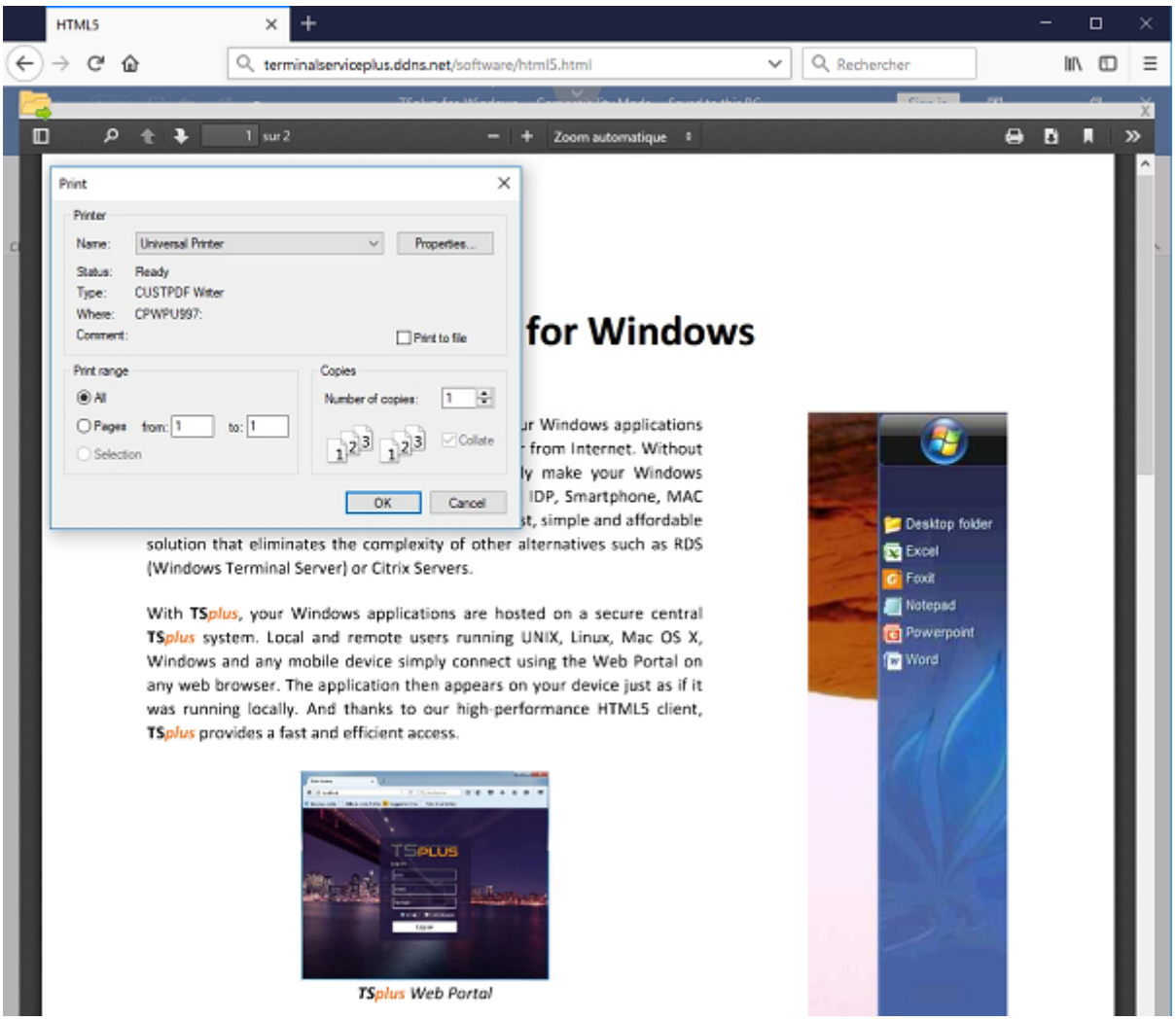


Note: The Universal Printer leverages novaPDF, which enables administrators to create profiles to define fonts, graphics, watermark, overlays and more through the **Manage profiles** button located below the Page size and Orientation sections on the printer properties popup window. Should a profile be selected by default, then the **Show Select Profiles dialog before printing** may be checked to allow user to select a profile before printing. Please refer to the novaPDF documentation for more details about profiles: Profile Manager.

Printing with the Universal Printer

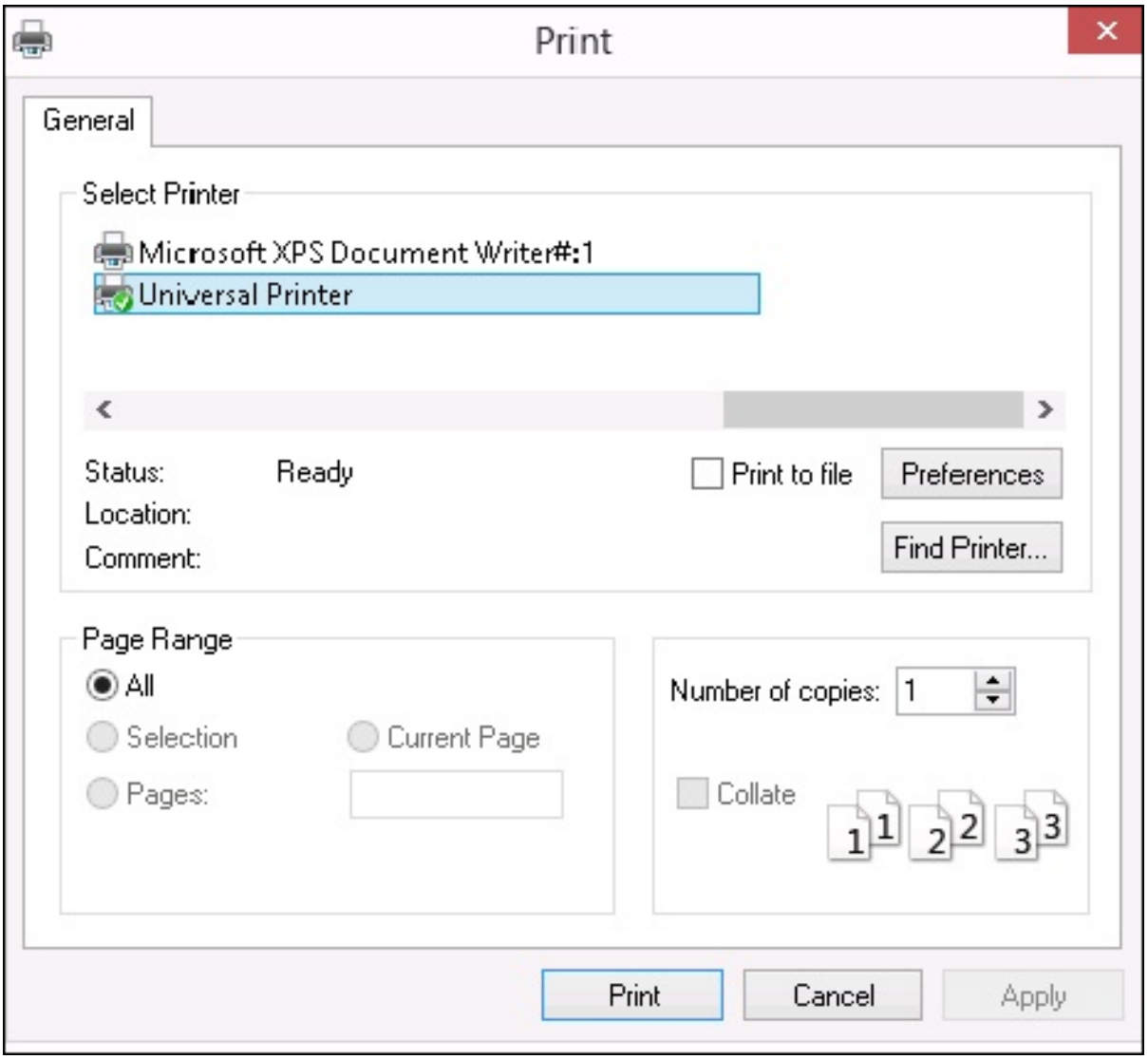
While printing using this printer, the document in the print queue is automatically converted into a PDF file by the Universal Printer (novaPDF) printer.





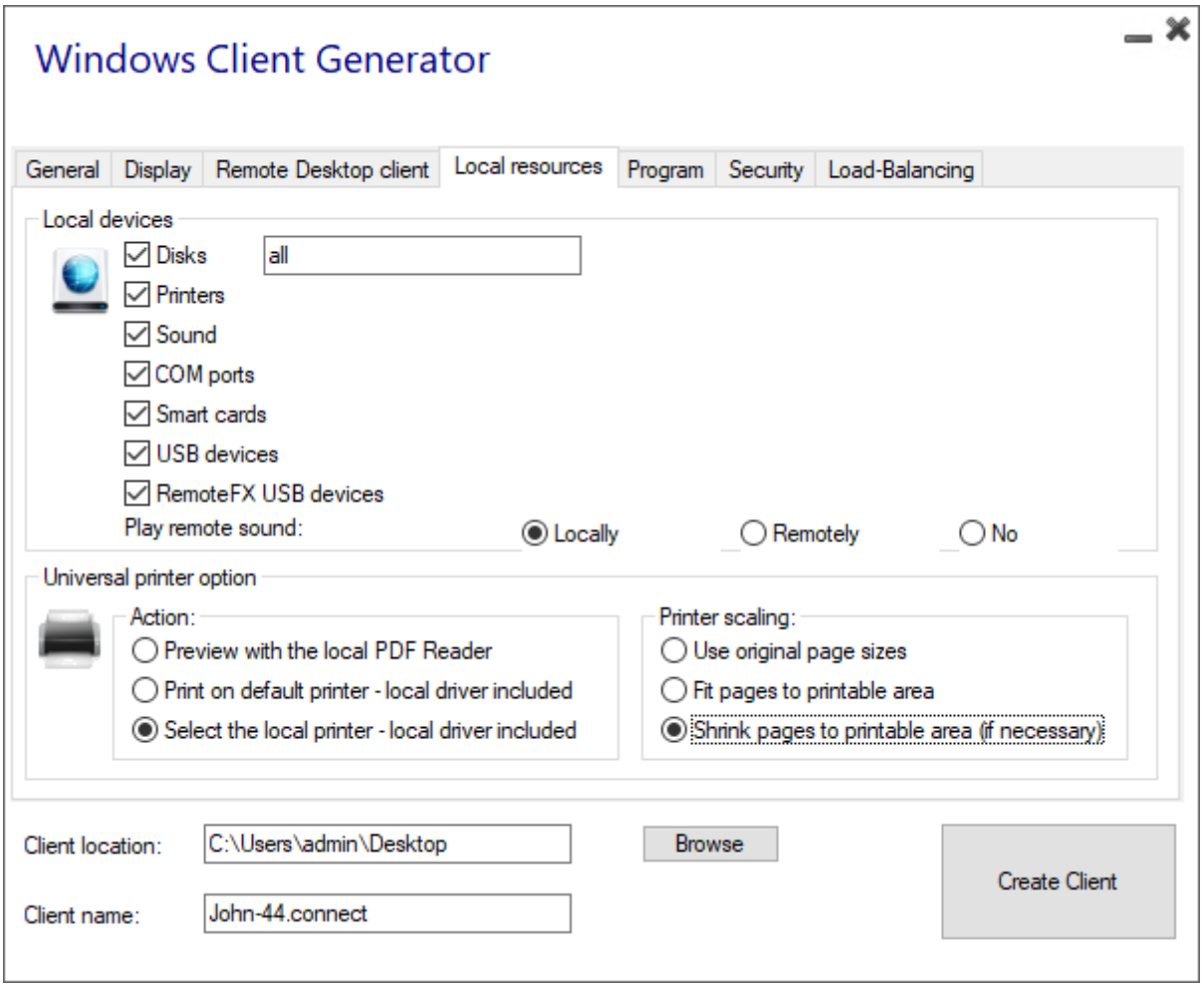
The generated PDF file is then pushed to the local PDF reader of the user's workstation.

Each print job is opened as soon as it is ready on the user's local disk. The printing process starts once the PDF file has been transferred on the client' side, which guarantees the print job to start without delay.



Configuring Printing options with the Client Generator

You can choose from 3 printing options on the Local Resources tab of the Portable Client generator
When using the TSplus connection client, you need to map at least the **C: drive or all disks**



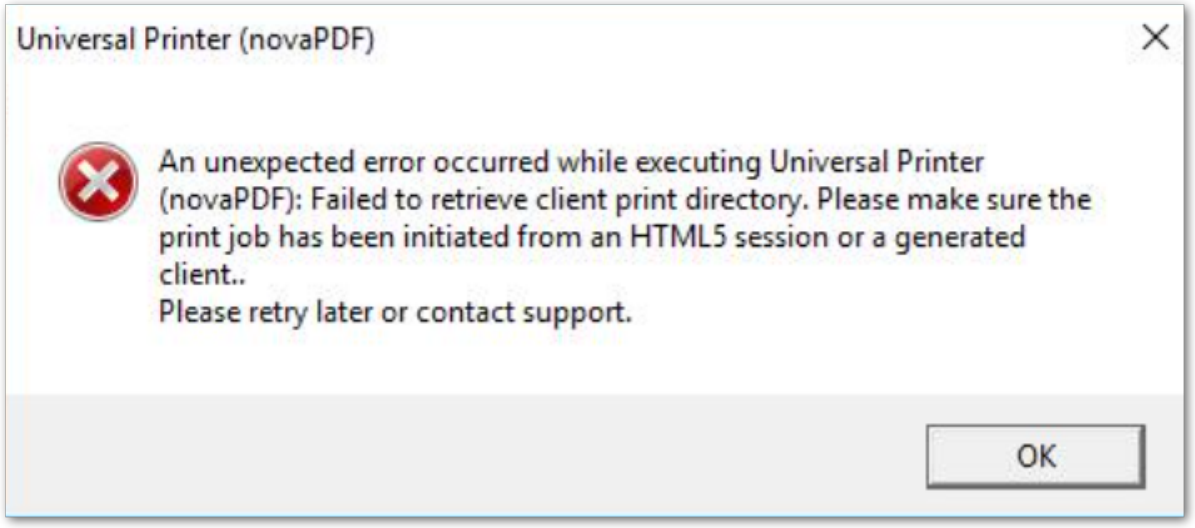
- **Local PDF Reader preview**: the document is pushed on the client's workstation and the local default PDF reader opens the received PDF file. The user can then print it, or save a copy on his local disk drive (this behaviour is expected when printing from an HTML5 session).

- **Print on the user's default printer**: the document is automatically printed by the user's default printer (this option is only available when using th TSplus connection client). This option is preferred for users who have a lot of print jobs to print during the day and use the same printer for this purpose.

- **Select a local printer**: the user can select one of his local printer (this option is only available when using th TSplus connection client).

For reading PDF files, these days many people get by without having to use an external application at all. Both Firefox and Chromium, the open source version of Google's Chrome browser, come bundled with in-browser PDF readers, so an external plugin is no longer necessary for most users.

FOR YOUR INFORMATION
: If the C: drive is not mapped, the user will receive this error message



Configure novaPDF printer

From **Printer Preferences** > **Tools** > **Password**, you can:

- Edit the default password
- Change the Profile Manager interface's language
- Monitor the progress of print jobs in real-time
- Check the printer history

Opening print job in a new tab

By default, print jobs from an HTML5 session are displayed inside a pop-up as before version 17.10.

It is possible to modify this behavior and open print jobs in a new browser's tab using the following setting: **AdminTool** > **Advanced** > **Session** > **Open Print Jobs In New Tab**

Profiles

Profiles enables to customize layouts, watermarks, compression level and much more. The Profile Manager allows you to manage profiles. Profiles consist of configurations utilized when printing using the Universal Printer. For instance, you can establish various printing profiles tailored to specific output requirements, such as distributing PDFs, high-quality printing, review purposes, or marking documents as confidential.

To open Profile Manager, open Devices and Printers, right click on Universal Printer and select Printing Preferences. Then, click on the **Manage Profiles** button. The default password is: pass@word1

Understanding the default profiles

- **Default Profile**: the default profile is intended to work for printing a single or multiple documents at a time. Suitable for most scenarios.
- **Print Opened Documents Profile**: Use this profile to automatically print a document when opened usign a PDF viewer. This profile is useful to gain a click when printing from an HTML5 session.

When opening an HTML5 session, the Print Opened Documents Profile is selected automatically for the current user. However, auto print in HTML5 session will be disabled if another session is currently opened for the same user in RDP mode. In this case, the Default Profile is applied by default.

Note: The Print Opened Documents Profile cannot be selected automatically for UWP applications such as Notepad in Windows 11 because these applications are designed to run in complete isolation with the system. However, it remains possible for the user to manually select the profile to use and to choose it by default for the next print jobs. There is no workaround at the moment. However, the redesign of the novaPDF printer scheduled for the next novaPDF major release due Q4 2024 will lift this limitation.

What profile can user choose?

By default, users can choose which profile to use among the two default profiles. Users are allowed to select one profile as active and do not show the Select Profile dialog box for the next print jobs. Administrators can define one or multiple profiles available for all users. This decision supersede any users' choices. See https://www.novapdf.com/printer-manager-profiles-help.html.

Important: It is recommended to copy the existing profiles to create more personilized profiles, as exisiting profiles embed several features required for most installation, such as embeded fonts in the generated PDF document.

Troubleshooting

Please find below troubleshooting tips to resolve Universal Printer (novaPDF) issues.

Staying up-to-date

- Updating the Connection Client may fix some issues occurring on the client side.
- Review the changelog to see if a newer version fixes your issue at https://dl-files.com/TSplus-changelog.html
- Remember that the development team can only support the latest code base.

Understanding which part of the printing process

failed

- Has the print job been created in the print queue ? What is its status ?

Collecting logs for printing errors

- **Session opening logs**, especially useful for issues like failed retrieval of client print directory, located at **C:\wsession\trace**.
- **AdminTool application logs** located at **C:\Program Files (x86)\TSplus\UserDesktop\files**.
- **Universal Printer logs**, sending the print job to the client side, located at **C:\wsession\UniversalPrinter\logs**.
- **Session events logs** for the printing user, handling reconnections, located at **%appdata%\UniversalPrinter\logs**.

Collecting logs for printer installation issues

- **Setup Log** 2024-02-XX #XX.txt available in the **%temp%** directory.
- **universalprintermanagement**_XX022024.txt located at **C:\Program Files (x86)\TSplus\UserDesktop\files**.
- All .txt files located in **C:\Program Files (x86)\TSplus\UserDesktop\files\UniversalPrinter**.

Collecting logs for client-side printing errors, when using the Connection Client

- **version.dat** file. Please always advise to update Connection Client to latest version.
- **Connection Client** and **Universal Printer Client** logs. These logs can be enabled by creating the following key value in the registry: **HKEY_LOCAL_MACHINE\Software\Digital River\ConnectionClient\Debug" = "true"**. The resulting logs are located here: **C:\Users<username>\RDP6\logs**.

Updating TSplus Remote Access

Check out our fixes and improvements by clicking on Changelog

Our development team is working on a daily-basis to ensure the stability and compatibility of TSplus with the latest versions of Microsoft Operating Systems and the latest Updates.

We are proud to provide you with new features and enhancements every week.

This is why it is recommended to keep your server up to date.

When a “2 sessions per server” issue occurs, typically after Windows updates on the second Tuesday of the month, please check your TSplus Remote Access (or TSplus LTS 18/17) version.

A new release will soon be published to restore compatibility with the latest Windows update.

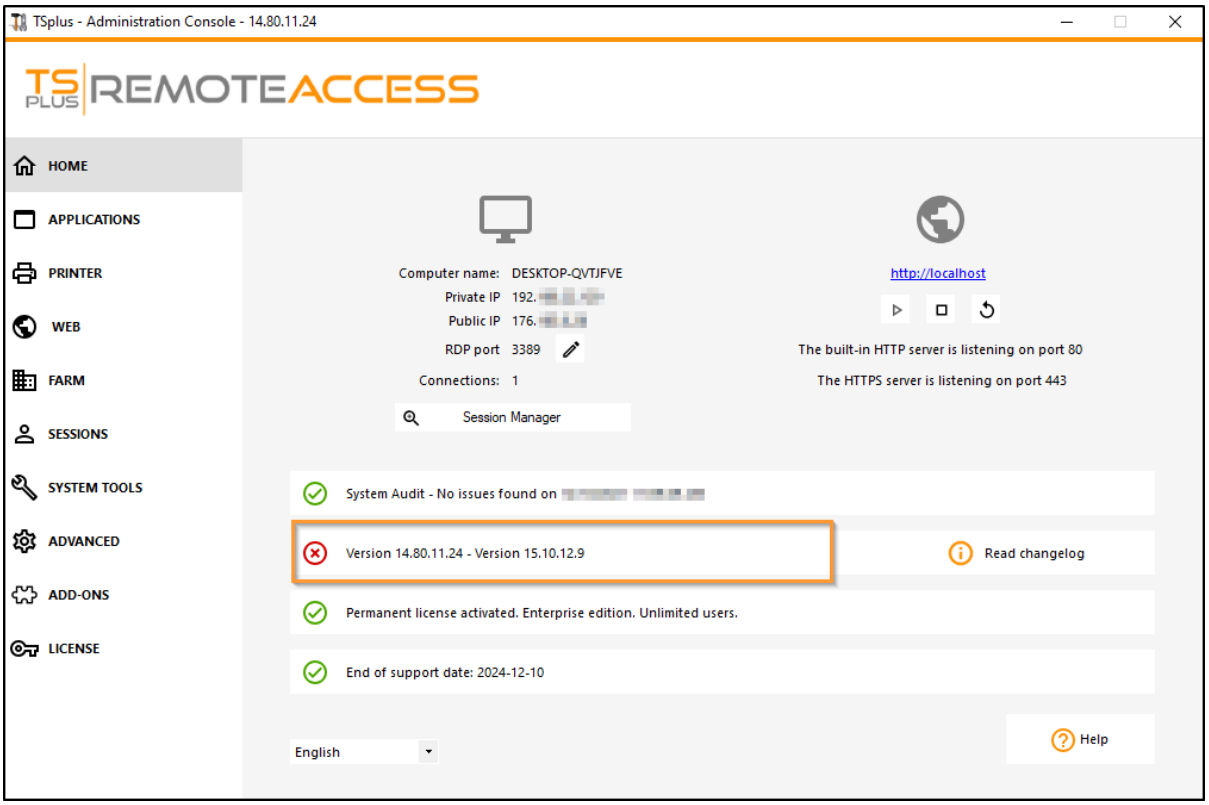
As a temporary workaround, you may uninstall the Windows update of the day and reboot.

Important: Avoid uninstalling TSplus Remote Access or restoring an older system image. These actions can trigger licensing conflicts that are far more complex to resolve. In most cases, a simple reboot is enough to apply compatibility fixes automatically.

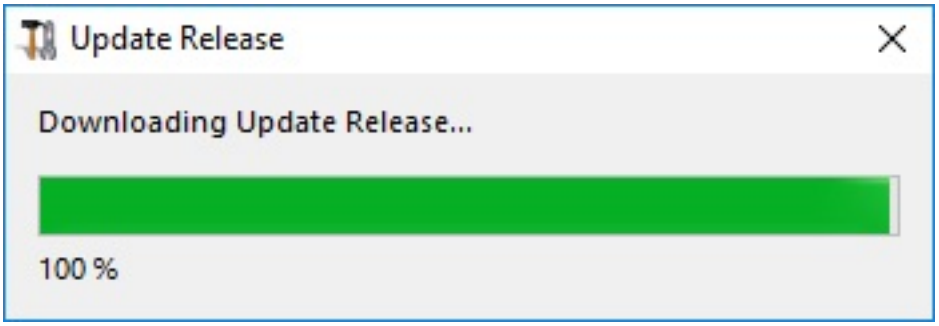
By subscribing to our annual Support and Updates Services, you will have access to the latest Updates and bug fixes.

In order to see which TSplus version you have and update it:

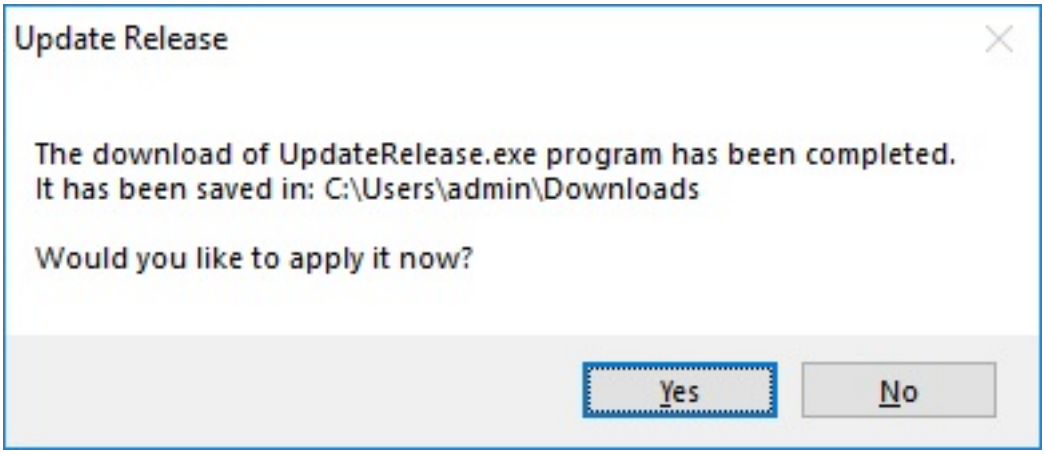
- You can check the status of your TSplus release on the Home tab of your AdminTool:



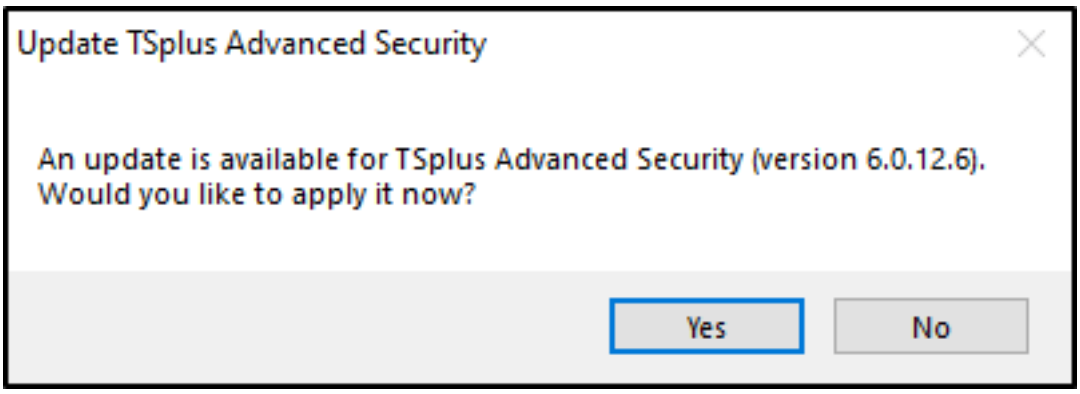
- You can then click on it. Since TSplus 11.50 version, the AdminTool automatically downloads…:



…and applies the Update Release program when requested:



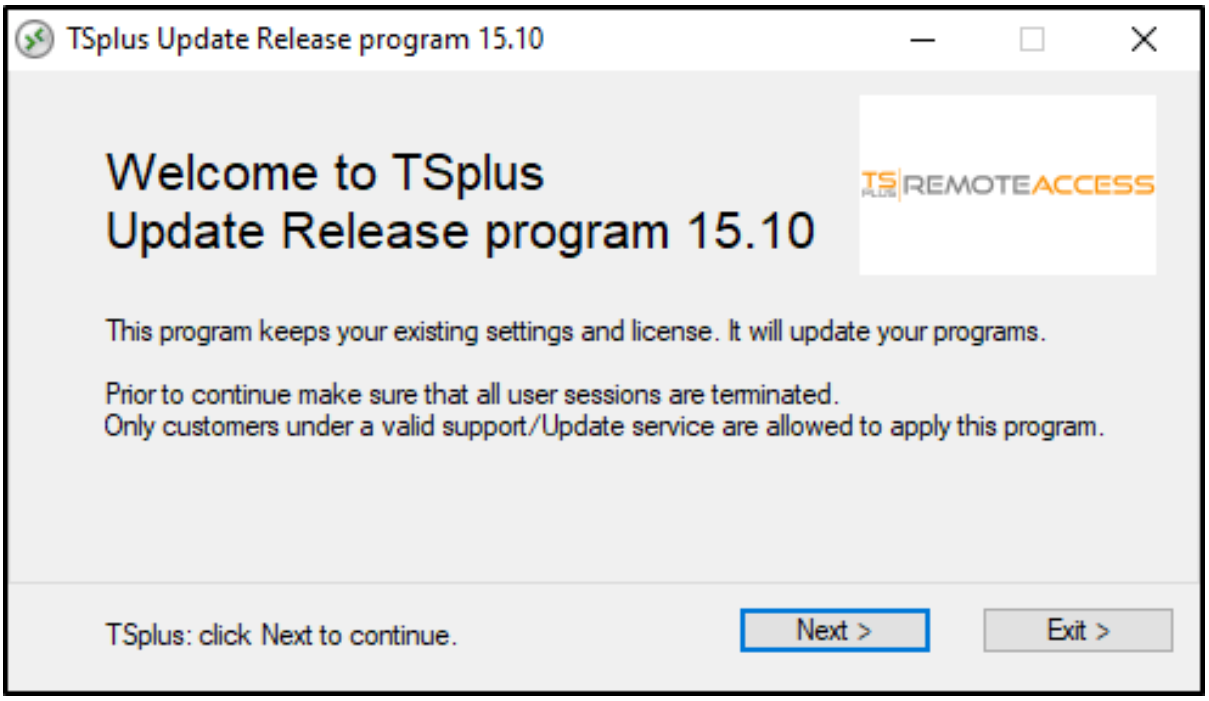
- Since TSplus 11.40 version, you will have the choice to install TSplus Advanced Security, our powerful Security Add-On, in its Ultimate trial version (All Security features free to use for 2 weeks) to your TSplus system:

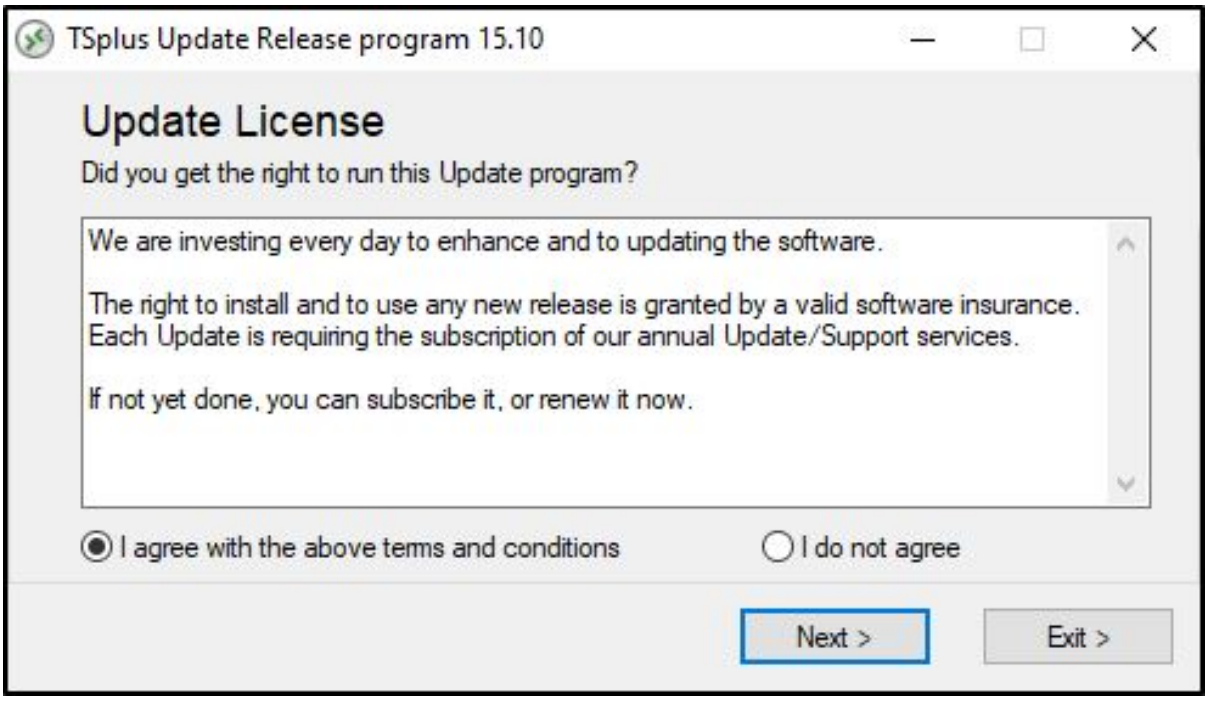


You still can download it via this link: Update Release and apply it manually.

The Update Release program is designed to keep your current TSplus settings safe.

If you have not subscribed yet for TSplus Update/Support services, or if your subscription has expired, you will not be able to run the Update Release program:

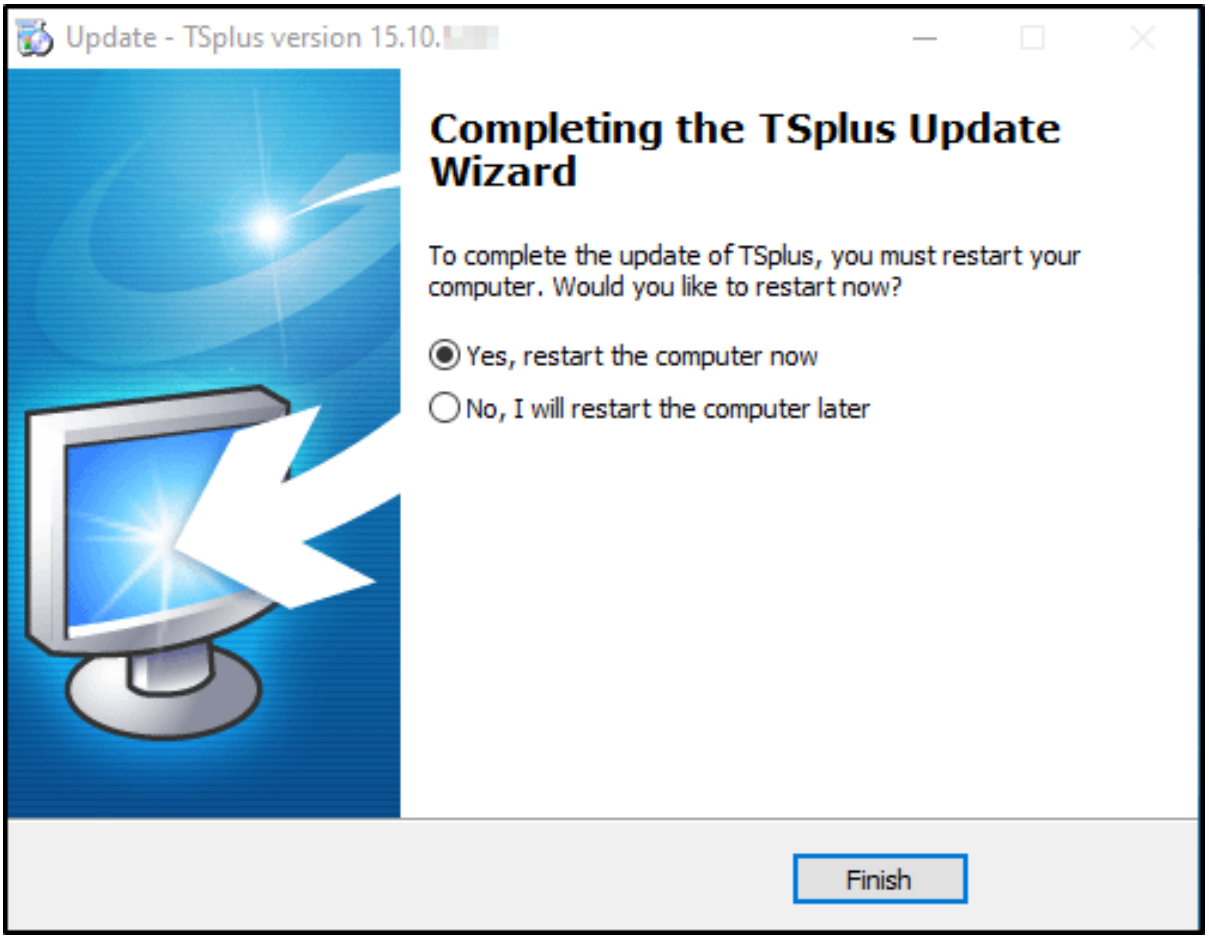




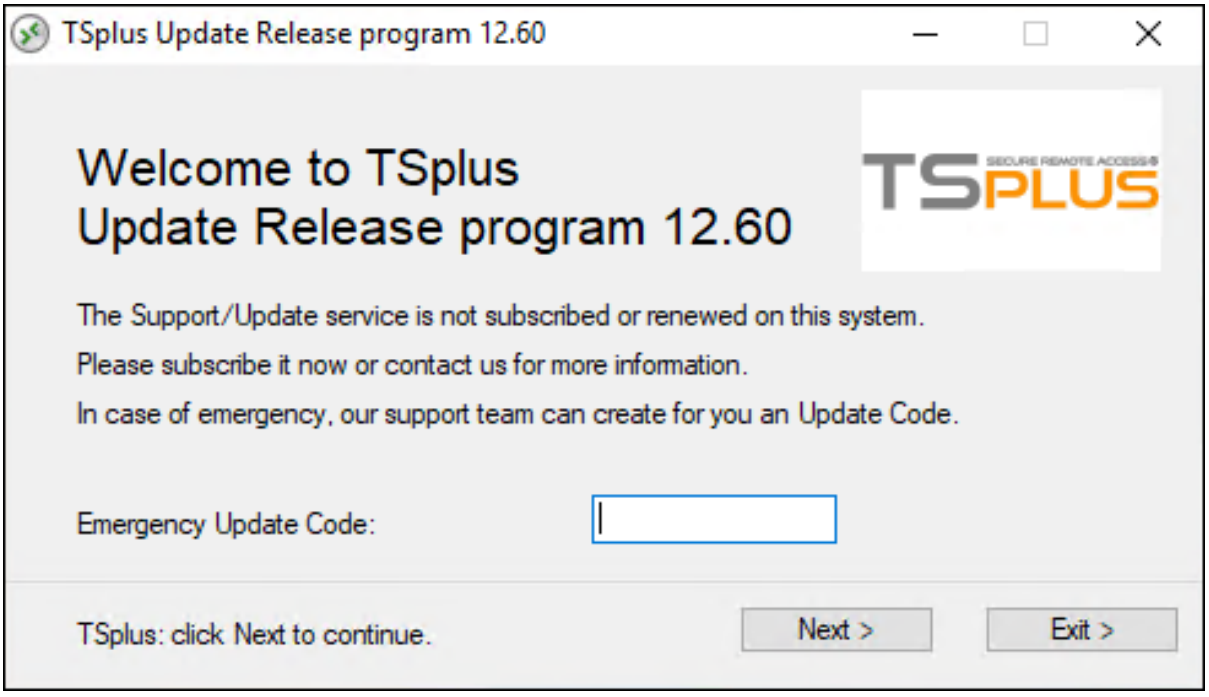
In such case, we advise you to place your order on our Store Page.

You will receive back the proper information to download your support.lic file. Activating your Update/Support services is an easy process described here.

When the update is finished, a reboot is required:



For versions previous to v14, just for specific requirements, the TSplus Support team can deliver an Emergency Update code which will unlock the Update Release program.



Update problem:

Check for the missing file

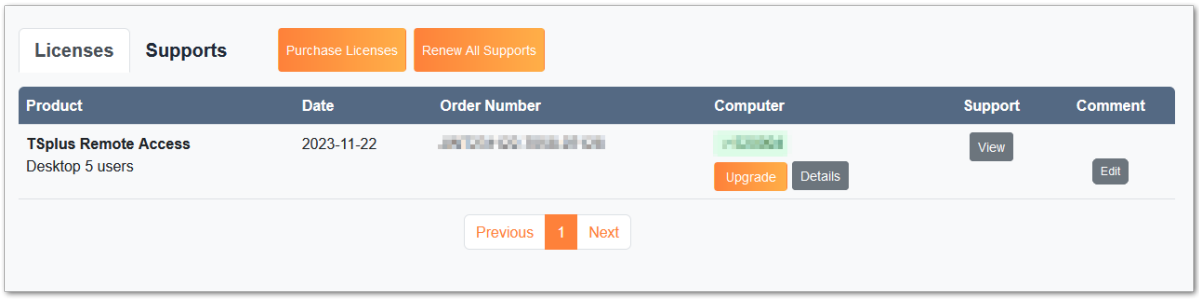
“C:\Program Files (x86)\TSplus\reboot_required.dat”

1. If this file is present, delete it.
2. Restart your server
3. Run the update again from this link by clicking here : Update Release

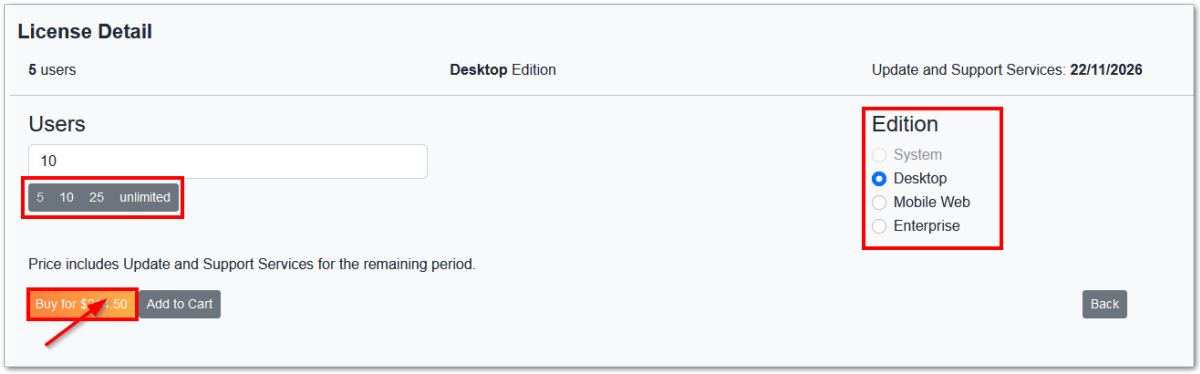
---

Upgrading your TSplus version

If you want to update your current version of TSplus, in order to add more users or more features, register in your license portal.



Select your choice of upgrade (users and version) and click on **“Buy for”** to continue on our store.



After your purchase, the update will be instant and visible on your license portal.
You must also follow the same procedure on your device so that it is linked to your license.

On your server, click on the **“Refresh your license”** button in the AdminTool > License tab.

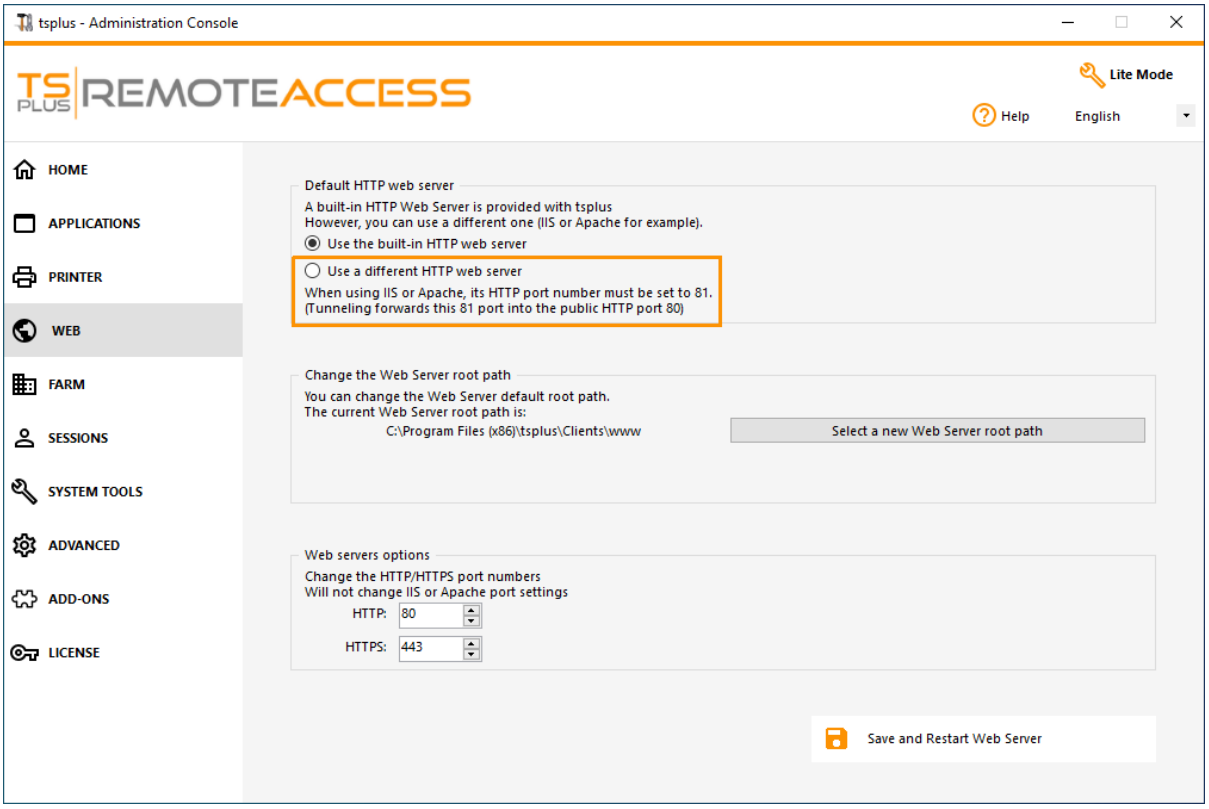
How to use Apache rather than Terminal Service Plus default Web server

Pre-requisites

It can be a good idea to Update Terminal Service Plus to be sure that you get the latest TSplus programs.

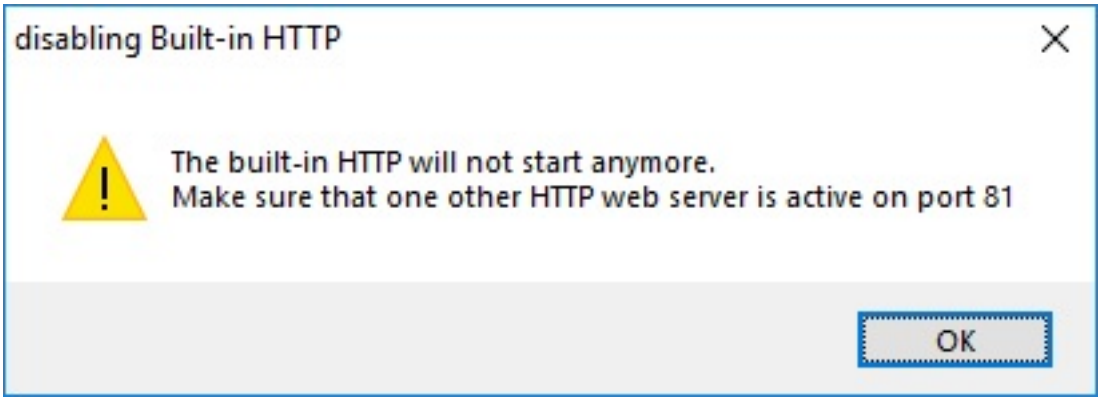
1. Start AdminTool and go to the Web Server Tab

Click On the Manage Web Servers tile, check **Use a different HTTP web server** because you want to use Apache.



Then, use the button **Select a new Web Server root path** to tell TSplus where will be the new web folder root.

TSplus will copy the requested files/folders into this new root folder and, at this point, the TSplus setting for Apache is near completion. A pop-up will recommend you to change Apache HTTP port to 81:



It’s now time to set up Apache.

2. Setting up Apache

Change the HTTP from 80 to 81.

The specific way of doing this depends on your Apache version and your current Apache settings.

We advise you to backup any Apache settings file before modifying them, so you will have a way to restore them if needed.

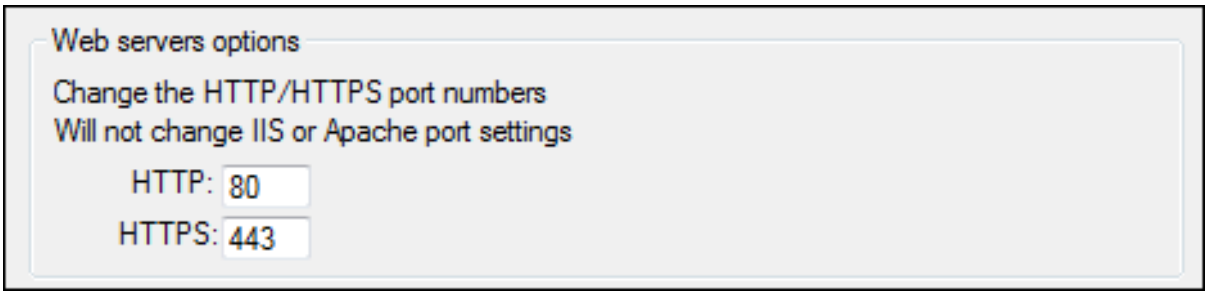
Usually you can change Apache listening port by editing the file httpd.conf found in “Apache\conf” directory:

Listen 81

Once it is done, restart the Apache service.

3. Going back to TSplus Web Servers Management tool

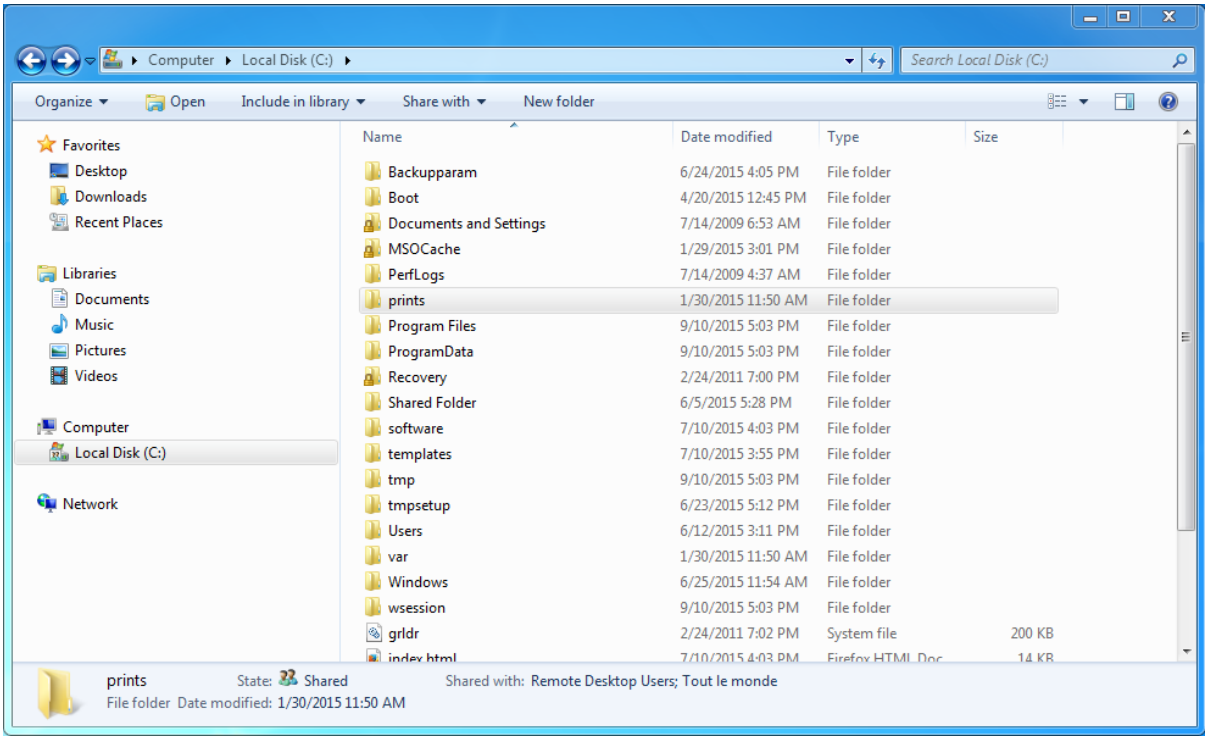
You can set the HTTP and HTTPS ports in TSplus Web Management tool. We recommend using standard ports, but this feature can be handy when trying to avoid a conflict with an other process.

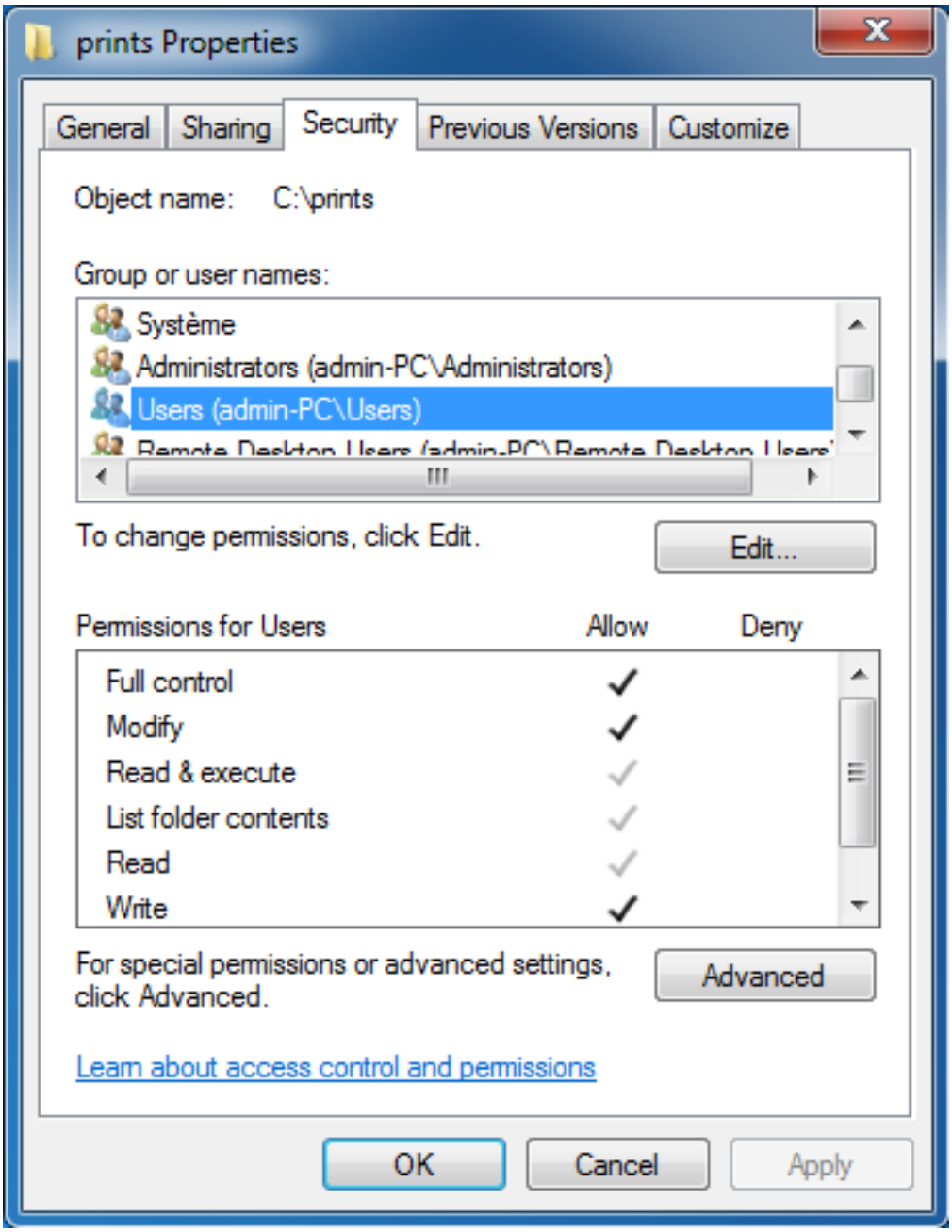


4. Last steps

For the Universal Printer, we need to be able to write in the PRINTS folder.

So, verify that Everyone/Users… have full rights on …/prints folder.





Then select the .html file you wish to use as a Web Access page in:

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

and copy it as index.html in your web root folder, typically this is the “Apache\htdocs” directory.

5. Specific Settings for TSplus Gateway Portal, Load Balancing and/or HTML5 file transfer

If you want to use this Apache based system as a TSplus Gateway Portal and/or use TSplus Gateway Portal Load Balancing feature and/or use HTML5 file transfer feature, you will need to allow the execution of TSplus GCI scripts by Apache.

First, you must have the CGI module enabled in Apache.

Edit the file httpd.conf found in “Apache\conf” directory, and search for a line looking like:

;LoadModule cgi_module modules/mod_cgi.so

Remove the ”;” to enable the CGI module:

LoadModule cgi_module modules/mod_cgi.so

Then, find a line starting by:

AddHandler cgi-script

And add the .exe extension to authorize .exe files to be handled as CGI programs by Apache:

AddHandler cgi-script .exe

Finally, you must tell Apache that the TSplus “cgi-bin” folder contains CGI programs. To do so, you must add the following line in the file httpd.conf found in “Apache\conf” directory:

ScriptAlias /cgi-bin/ “C:/Program Files (x86)/TSplus/Clients/www/cgi-bin/”

Once it is done, restart the Apache service.

If you face any issue setting up CGI on your Apache server, please refer to the Official Apache documentation

Checking your settings: To validate your settings, please open a web browser on your server and go to http://localhost/cgi-bin/hb.exe. If you get an Apache error page, you have an issue in your Apache configuration. If you get a line of text/numbers, everything is fine!

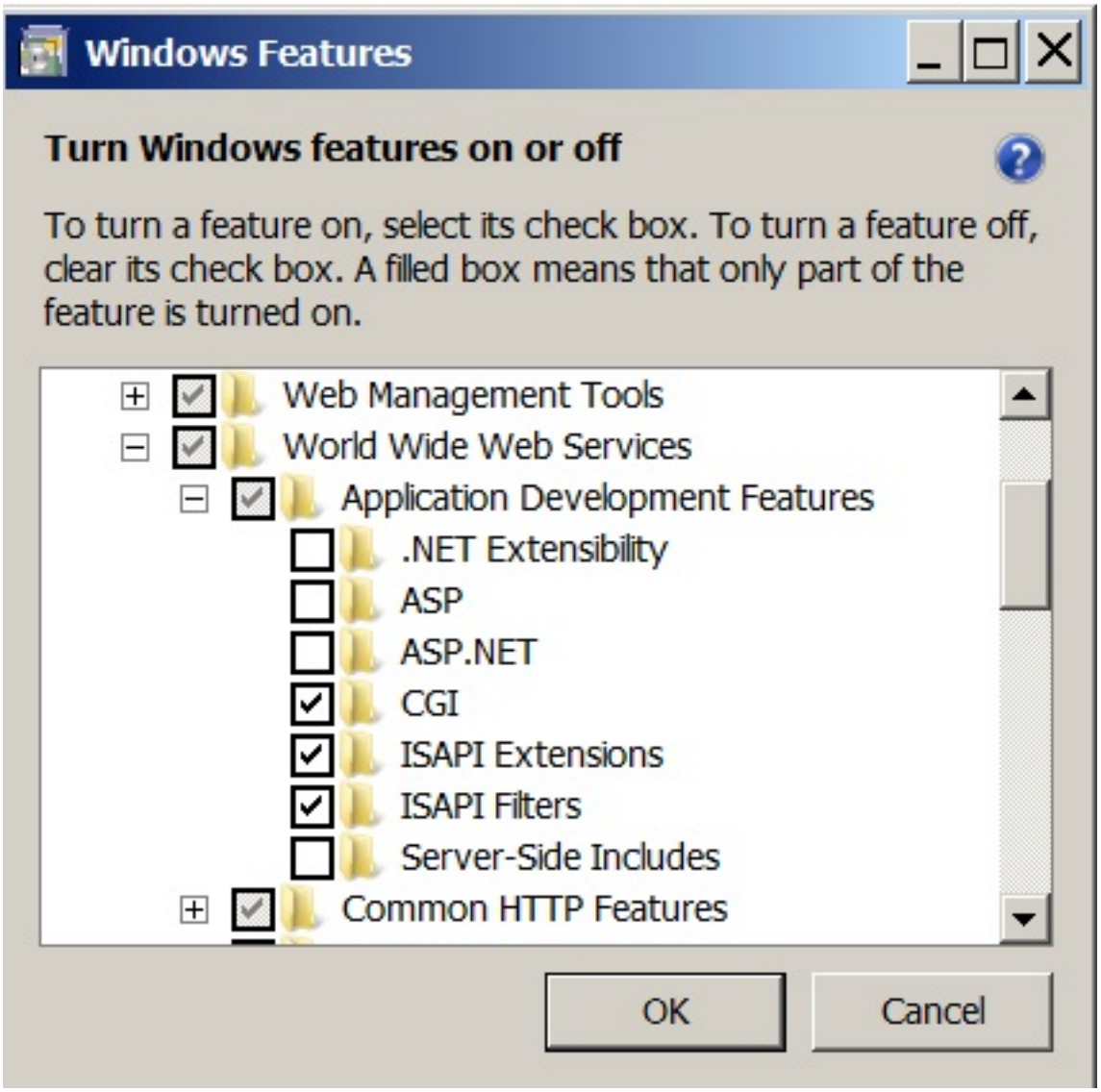
How to use IIS rather than Terminal Service Plus default Web servers

Pre-requisites

It can be a good idea to Update Terminal Service Plus to be sure that you get the latest TSplus programs.

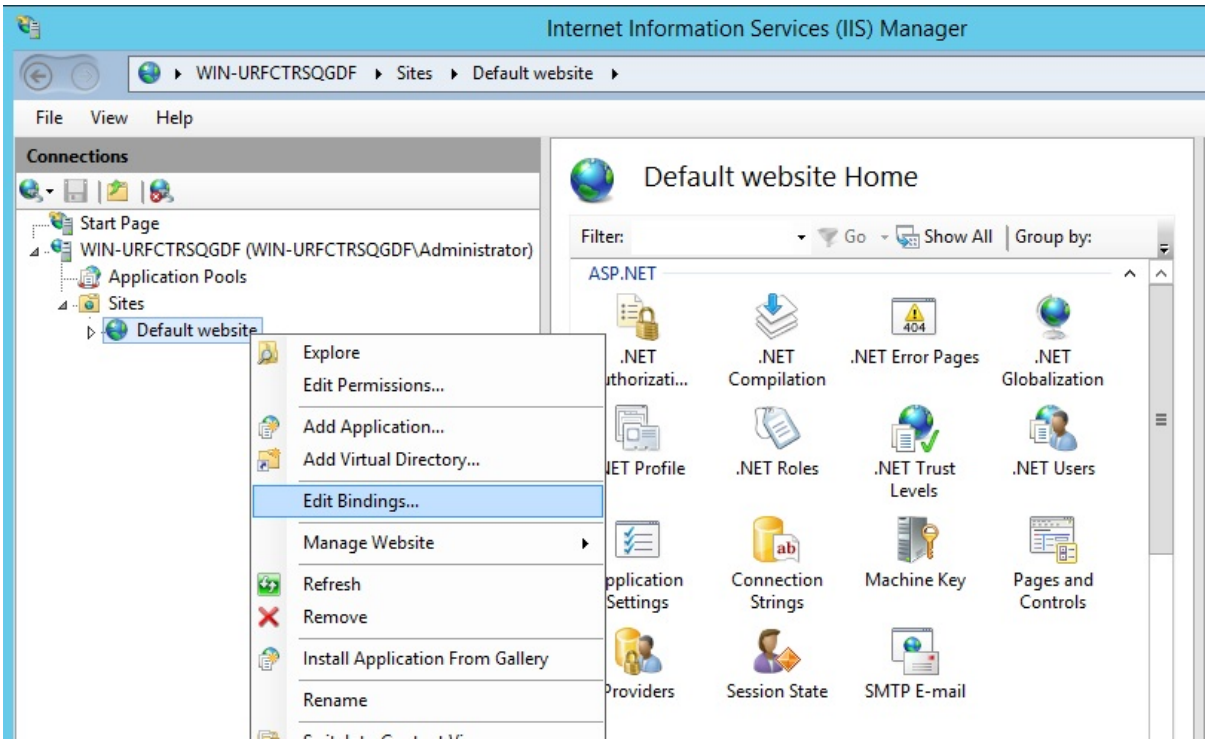
1. IIS configuration

- Install IIS with the following modules : CGI, ISAPI Extensions and ISAPI Filters.

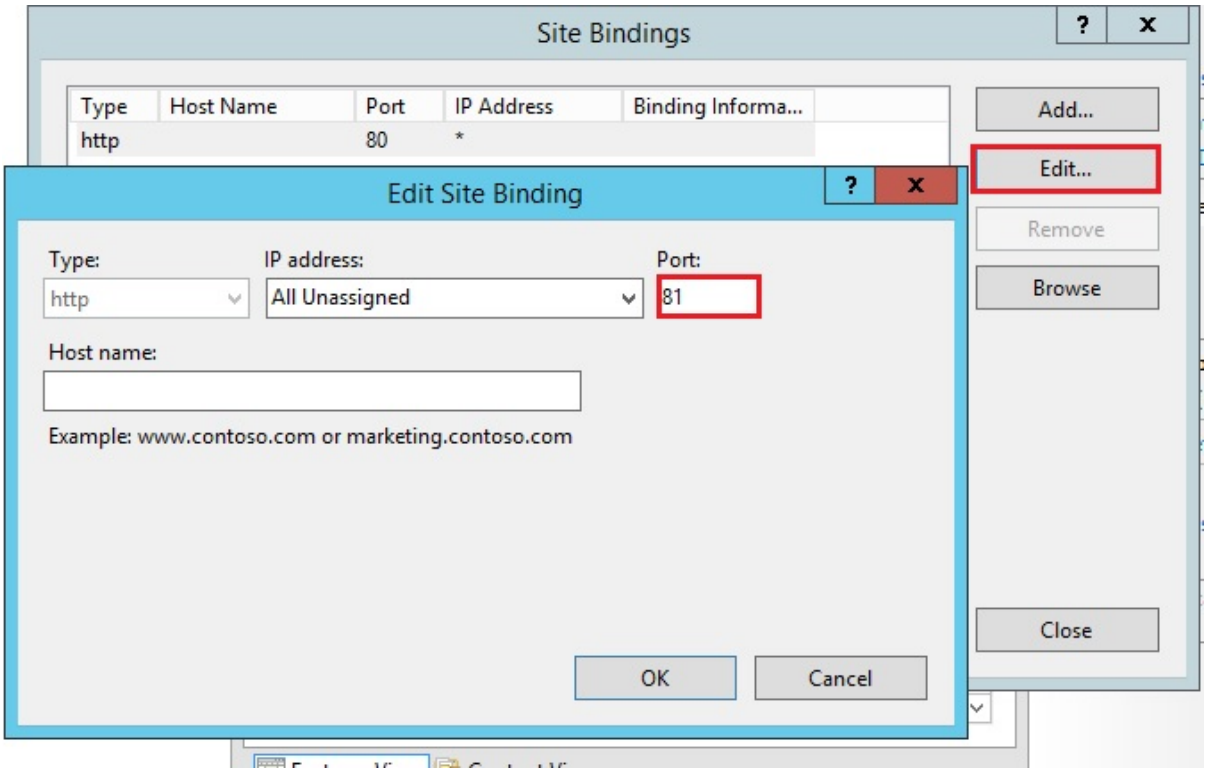


- Configuring the IIS Port:

Access the IIS management console, expand the list below your server name, then Expand the “Sites” menu and right click on “Default Web Site” and click on “Edit Bindings”:



Click on “http” and “Edit”. Change the port to 81 and click Ok, and then click Close:



Disable the 443 port or change this port for another free port.

Then, restart the IIS Manager.

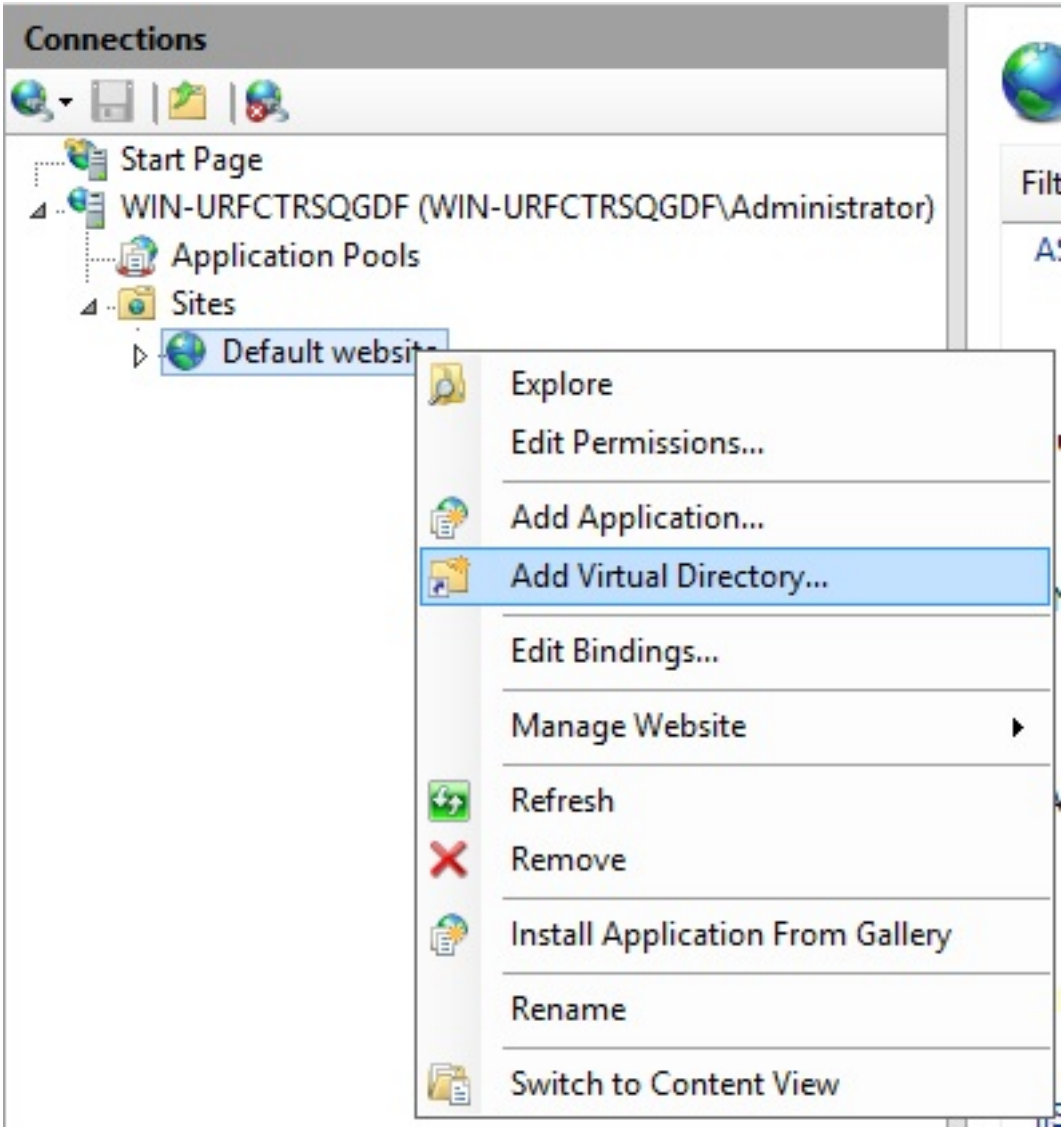
2. Create virtual directory for CGI

NB: All files from the default web root (C:\Program Files (x86)\TSplus\Clients\www) are not

copied when the web root directory is modified.

You will need to check and copy them manually when migrating to the IIS web server.

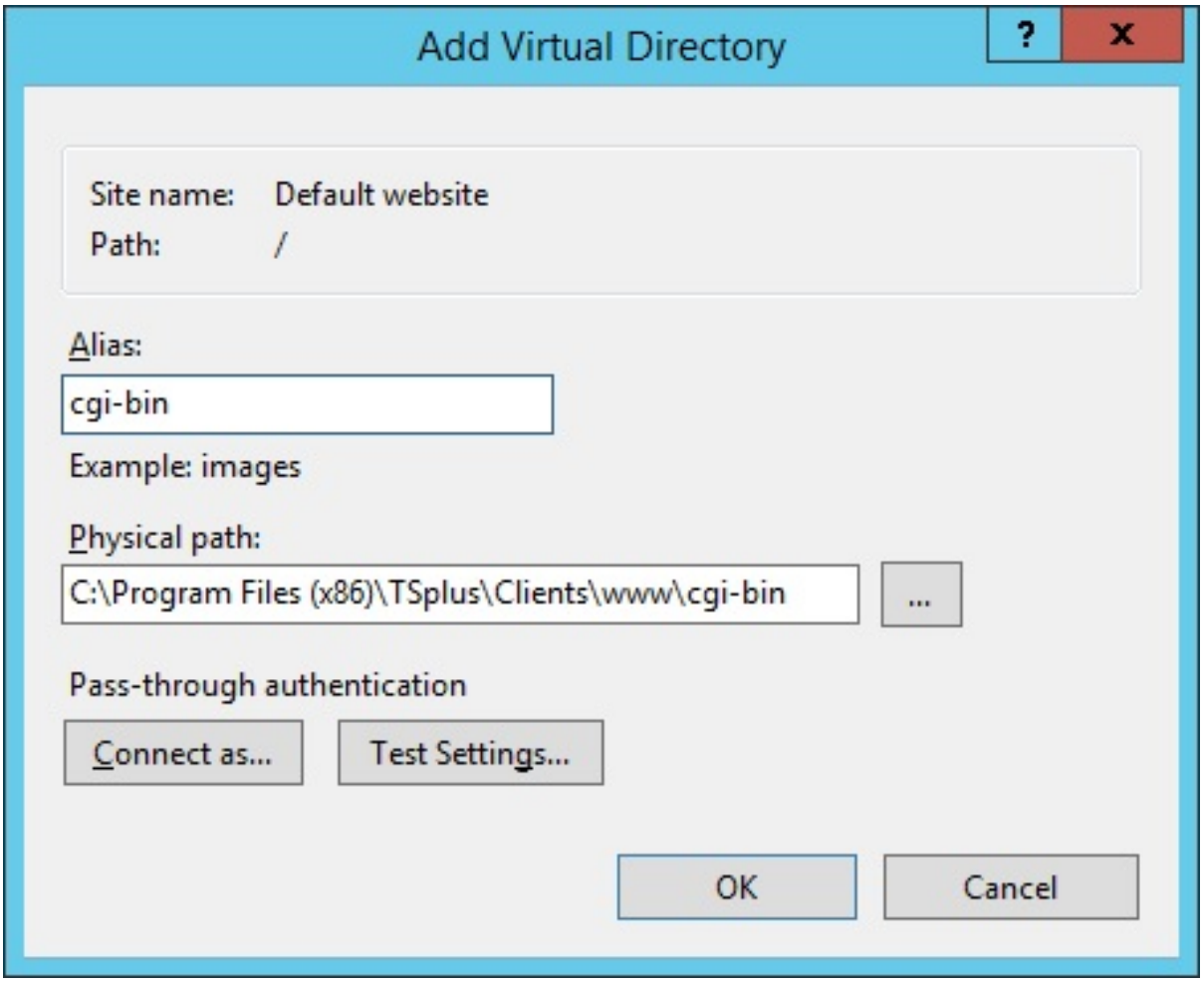
In the left panel menu, expand the menu under your server, then “Sites,” and right-click on your site to add a new “virtual directory”, as shown in the image below:



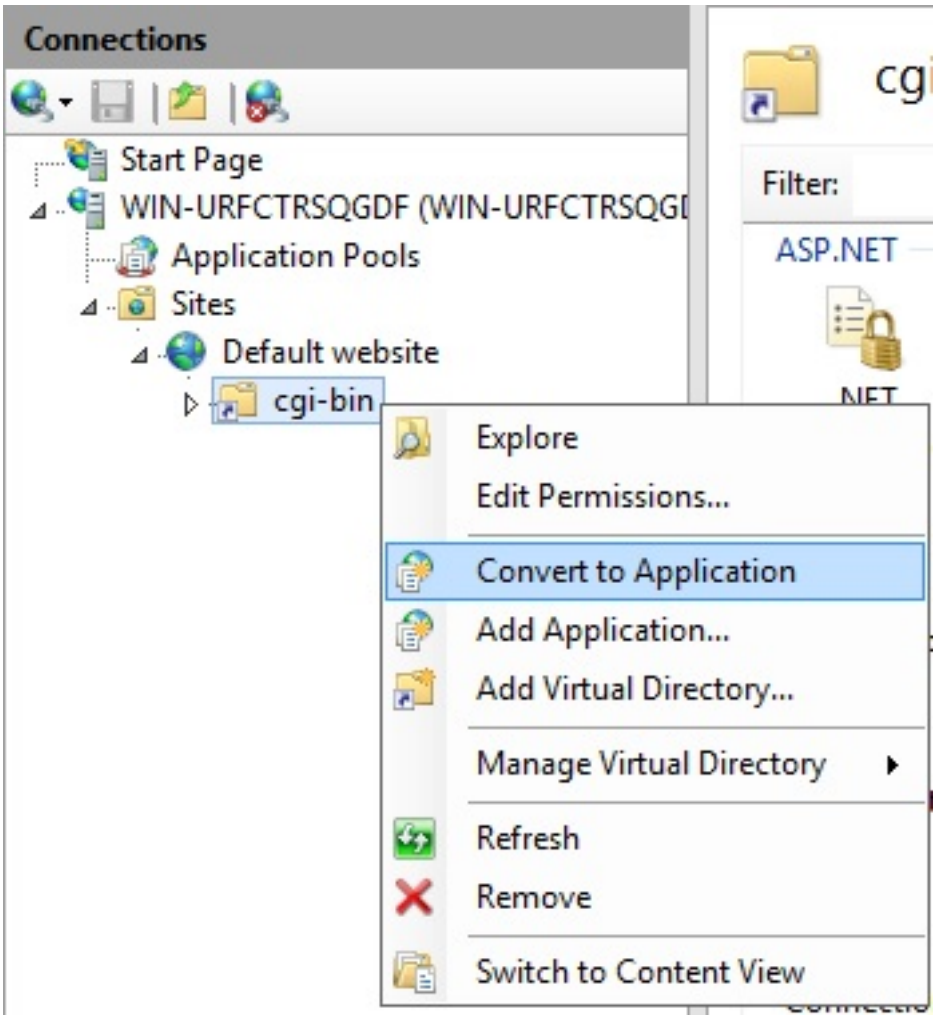
On the window that will open fill in as follows:

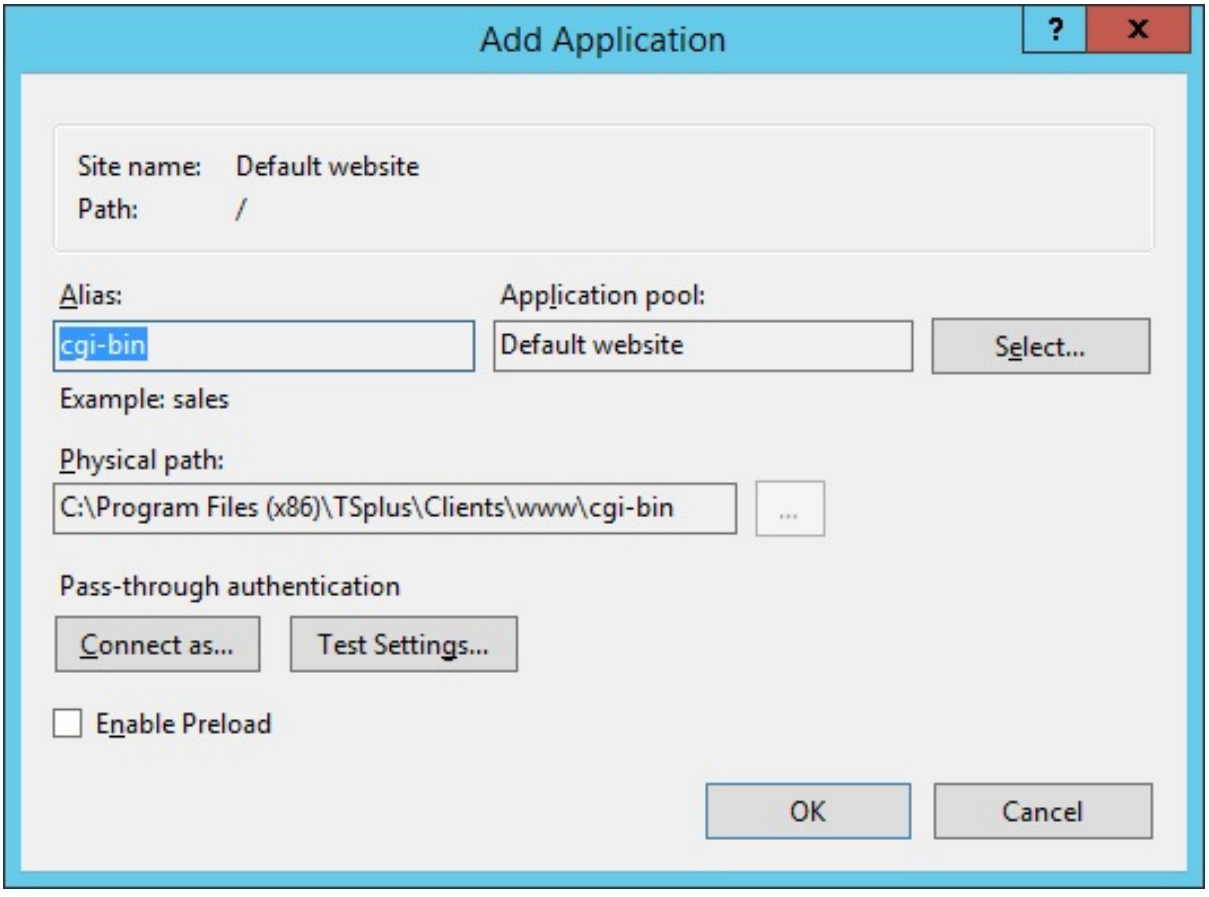
Alias: cgi-bin

Physical path: “C:\Program Files(x86)\TSplus\Clients\www\cgi-bin”

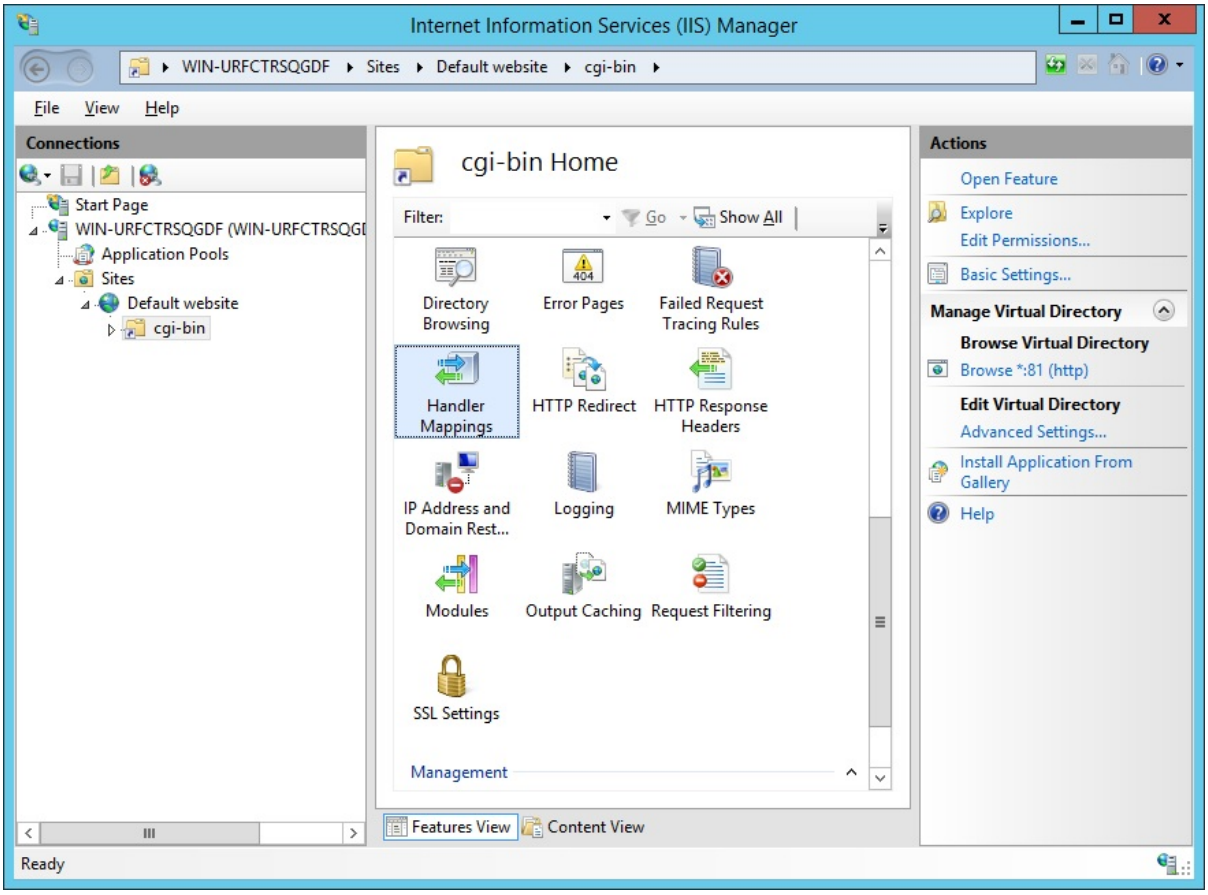


Then click “OK” and you will see that the “cgi-bin” virtual directory has been added to your IIS Web site. Now, right-click this “cgi-bin” virtual directory and click on “Convert to Application”. Click “OK” and accept the default settings.



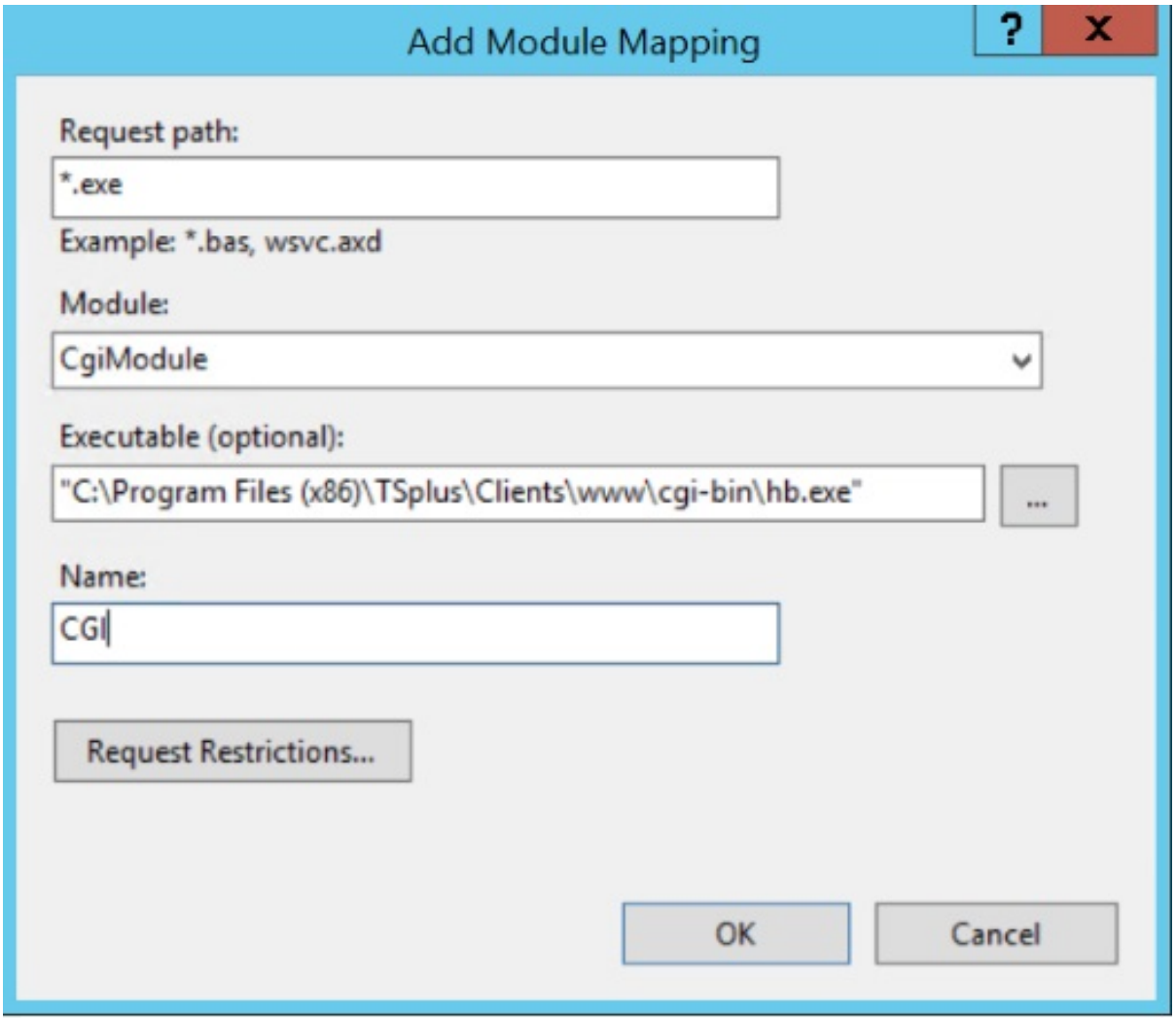


Then select the “Handler Mappings” icon for this folder on the right side of the Manager window:

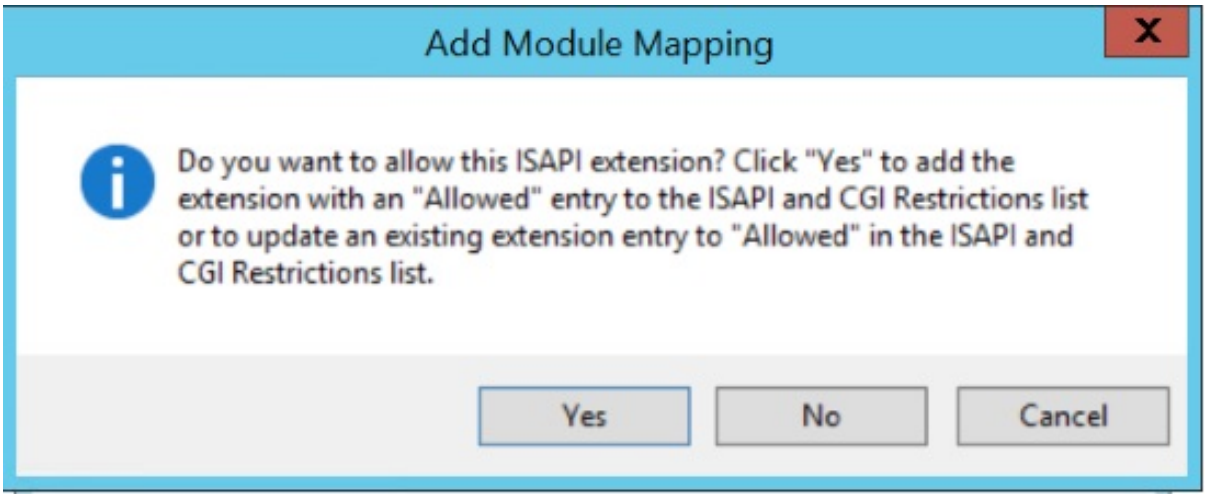


From the list of Handler Mappings, double click on “CGI-exe”.

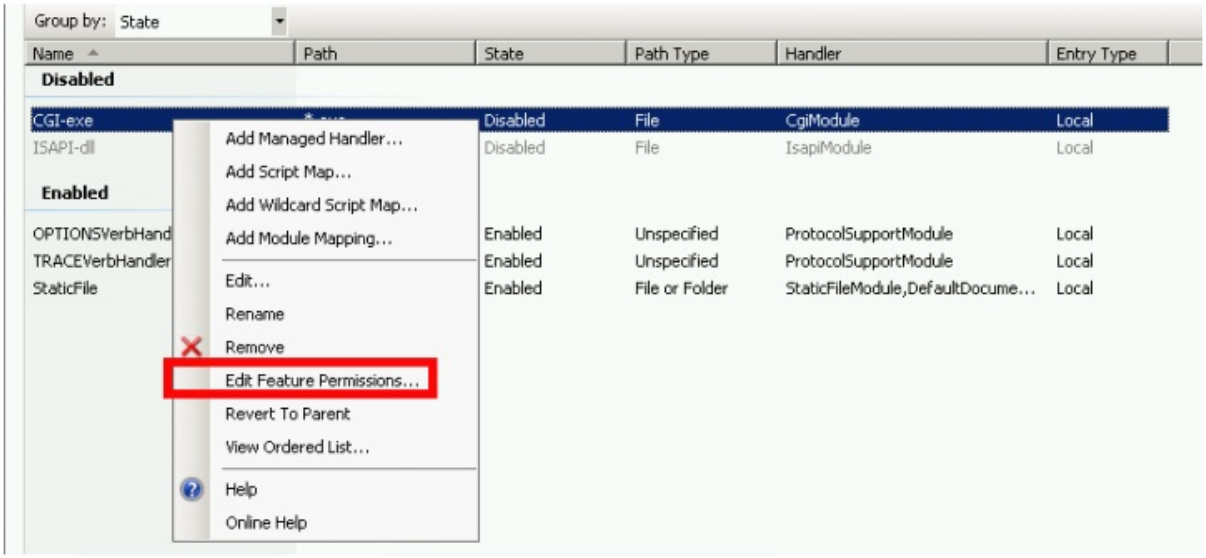
Then, search the hb.exe executable from the Executable property box and click OK.



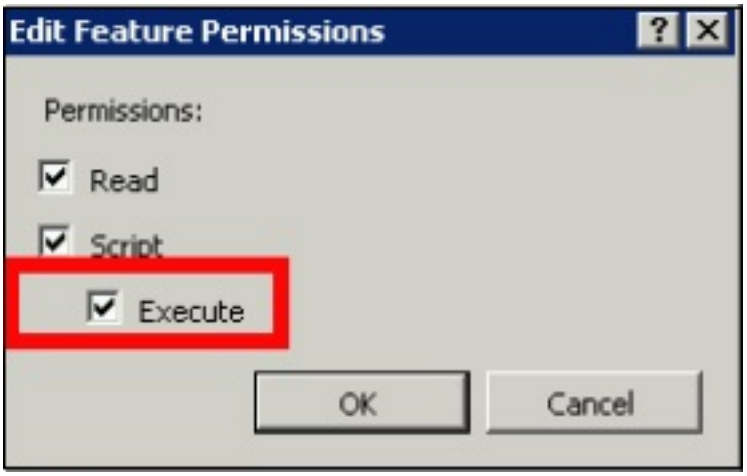
A prompt for confirmation appears. Click “OK” to allow this ISAPI extension.



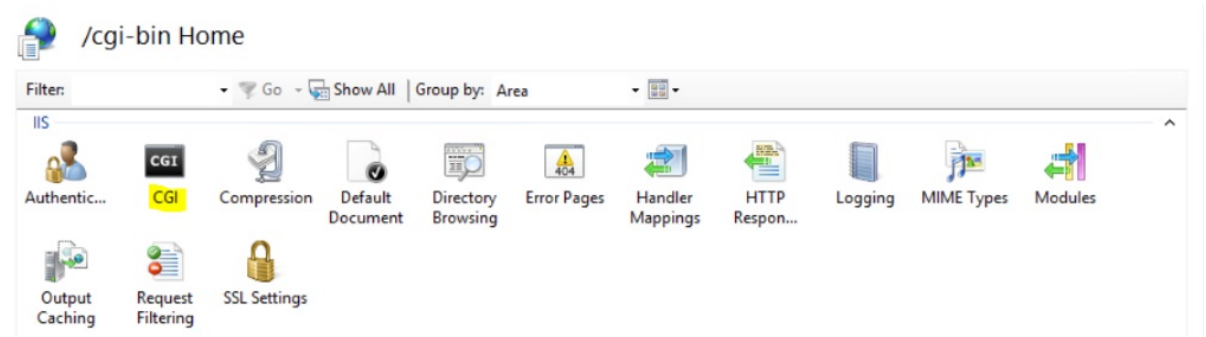
Now click on “Edit Feature Permissions”:



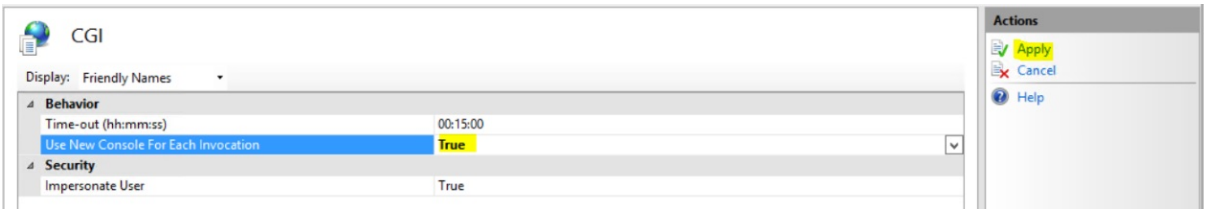
Check the “Execute” checkbox and click OK:



Back to the “CGI-bin” Home, click on “CGI” to open the CGI properties:



Change the value of “Use New Console For Each Invocation” to “True”. Then, click “Apply” to save the changes.

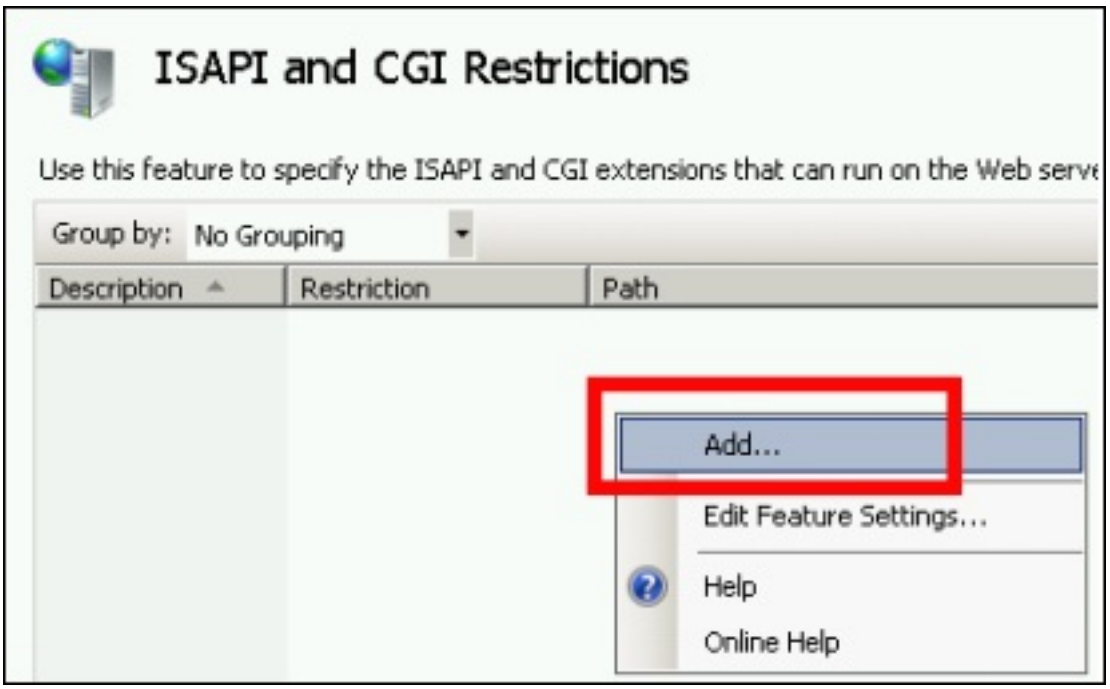


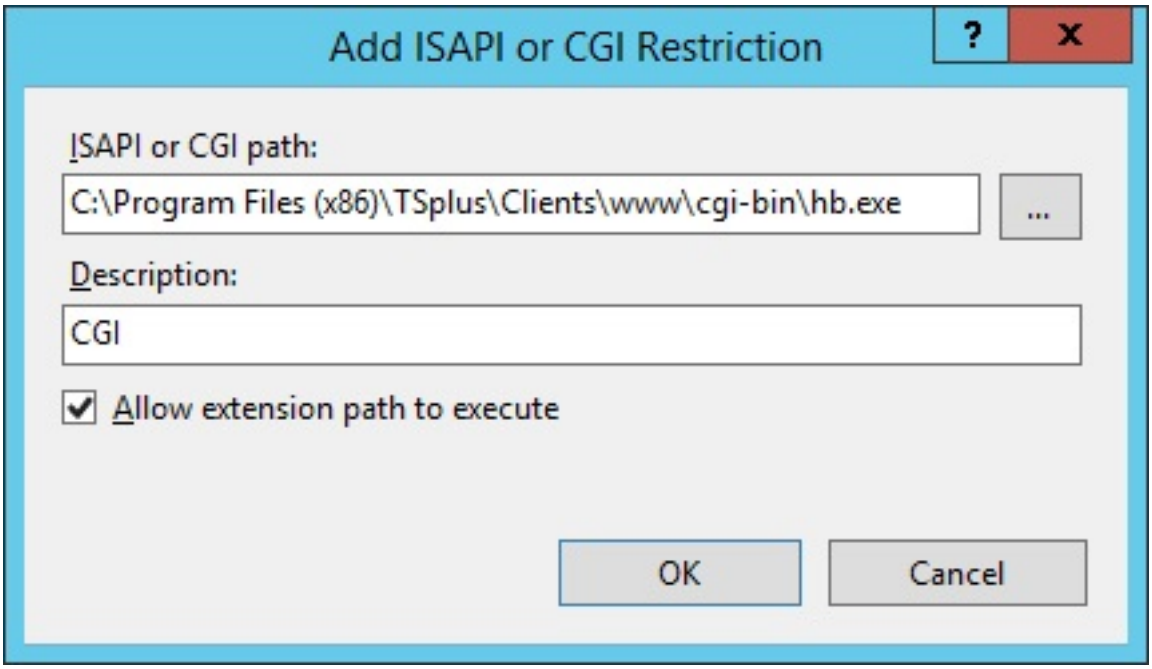
3. Configure CGI extension permission

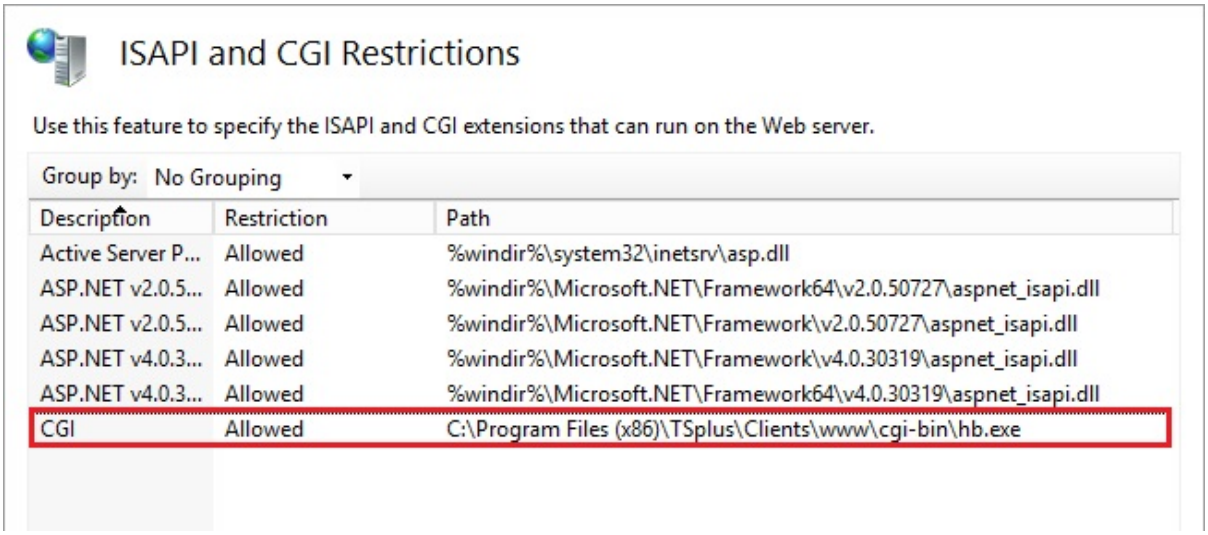
Now, the last step is to allow the CGI extension to run on the server. Click on the “ISAPI and CGI Restrictions” icon. This can be found by clicking on the machine name in the menu on the left side of the window.



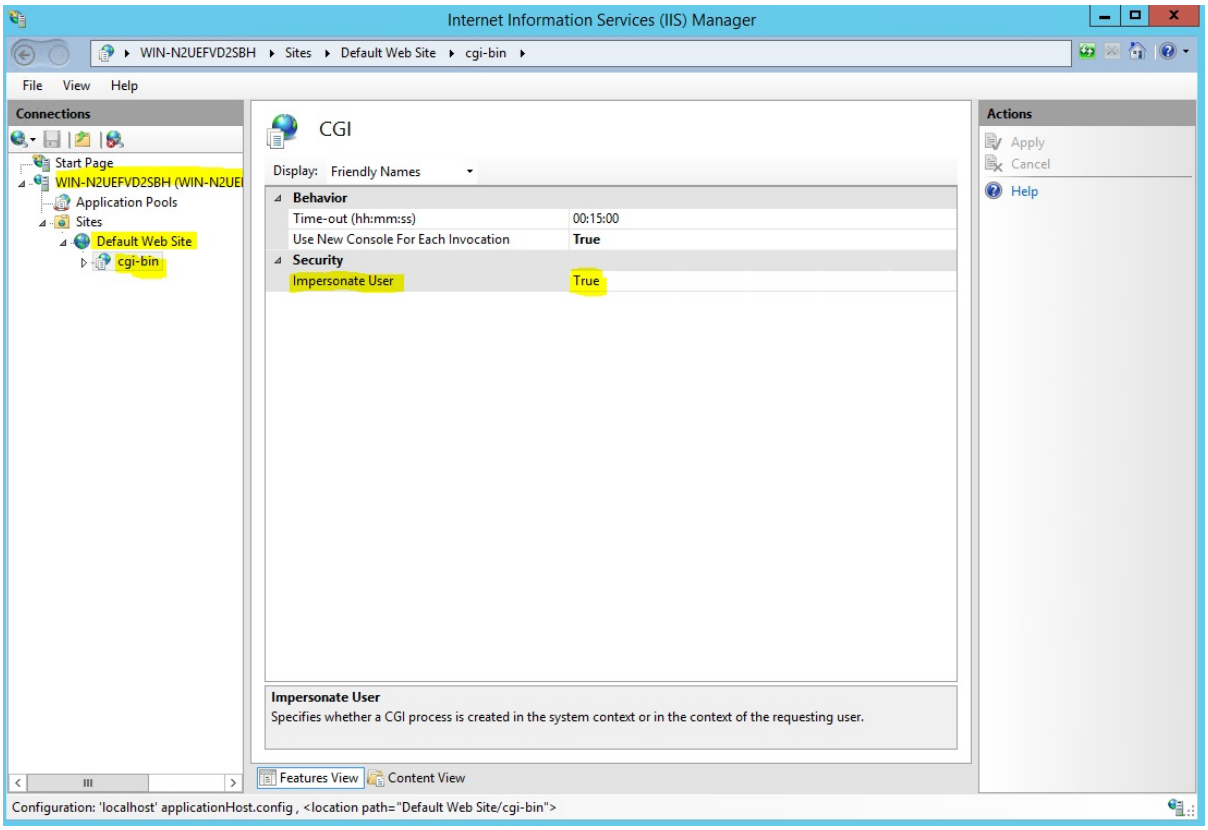
On the “ISAPI and CGI Restrictions” page, click “Add …” on the right side of the window. Now specify the full path to the “hb.exe” file hosted in the TSplus folder. Be sure to check the “Allow extension path to execute” option, as Illustrate the following images:







Make sure that in CGI section of your server, “Default Web Site” and “cgi-bin” the setting “Impersonate User” is set to “True”.



- Give full permission to user “IUSR” in the directory ”C:\Program Files (x86)\TSplus\Clients\www\cgi-bin”

- Please make sure to enable permission inheritance when the IUSR user is configured for full control over the directory.
”C:\Program Files (x86)\TSplus\Clients\www\cgi-bin”

- Give full permission to user “IUSR” in the directory ”C:\Program Files (x86)\TSplus\Clients\webserver\twofa”

4. Add Mime types in IIS

Open a command prompt as an administrator and run the following commands:

Terminal window
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent /+[fileExtension='.dat',mimeType='text/plain']

Terminal window
%SystemRoot%\system32\inetsrv\appcmd set config /section:staticContent /+[fileExtension='.',mimeType='text/plain']

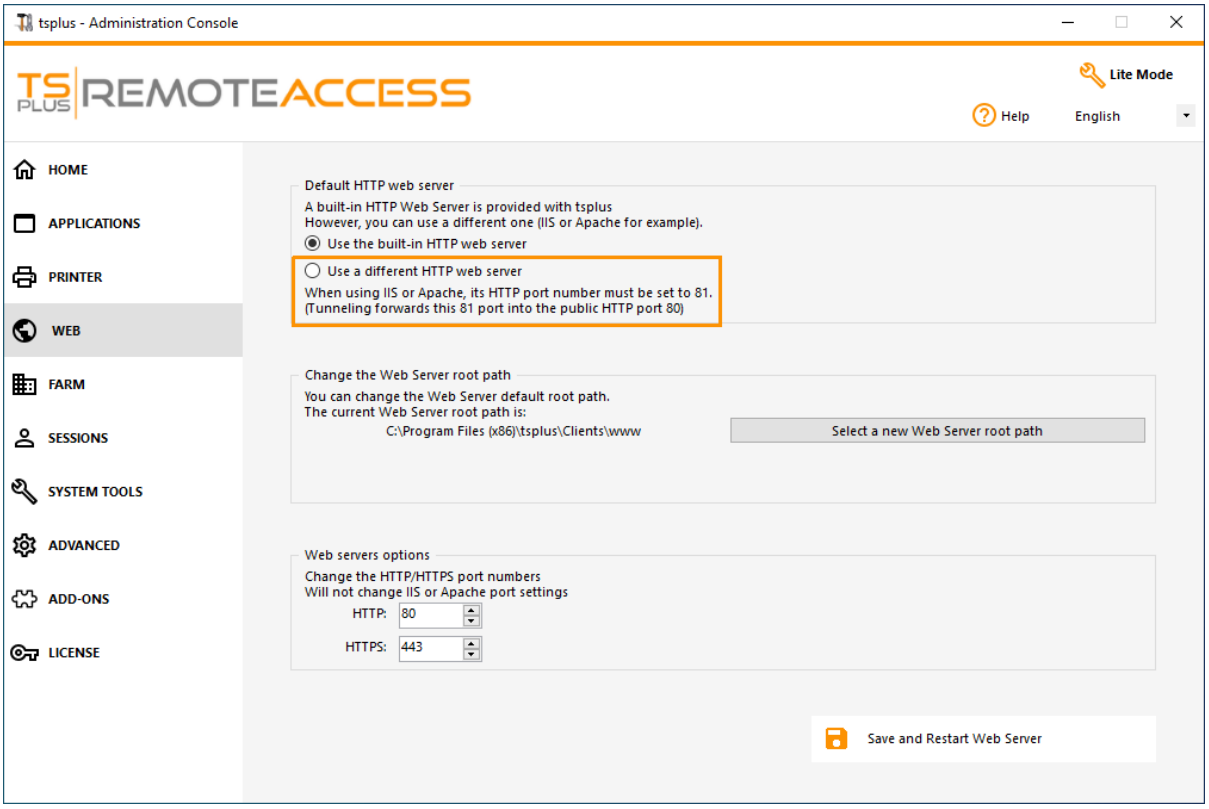
Restart IIS.

5. Configure IIS Directory Permissions

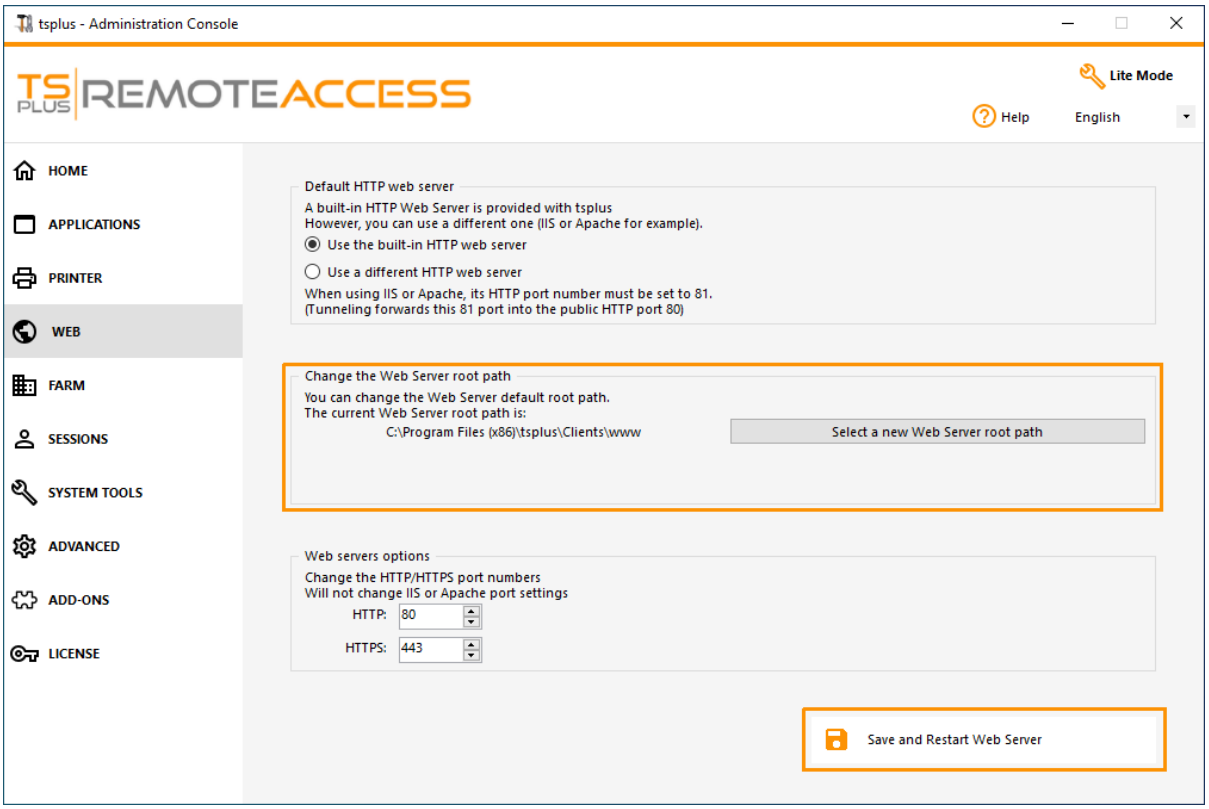
Give full permission to the group “Everyone” in the directory “C:\inetpub\wwwroot”

6. Configure TSplus

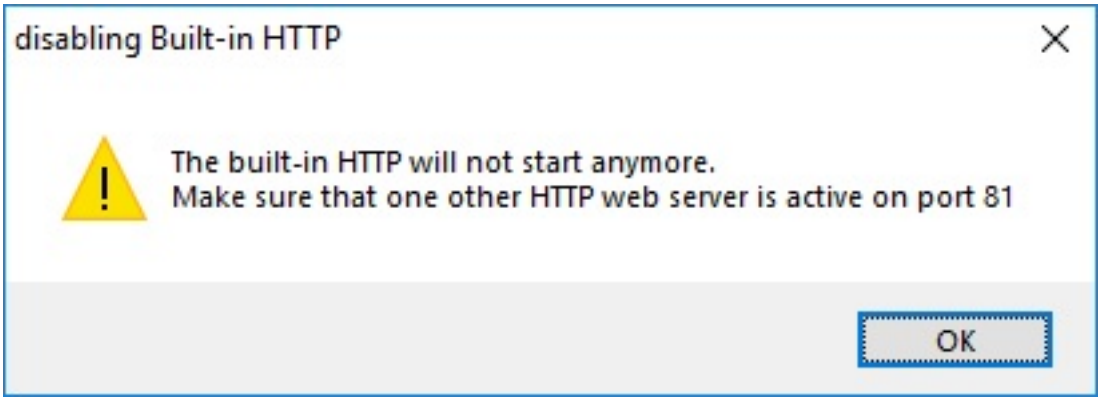
Go to the Web Server tab of the AdminTool, then choose the “Use a Different HTTP server” option:

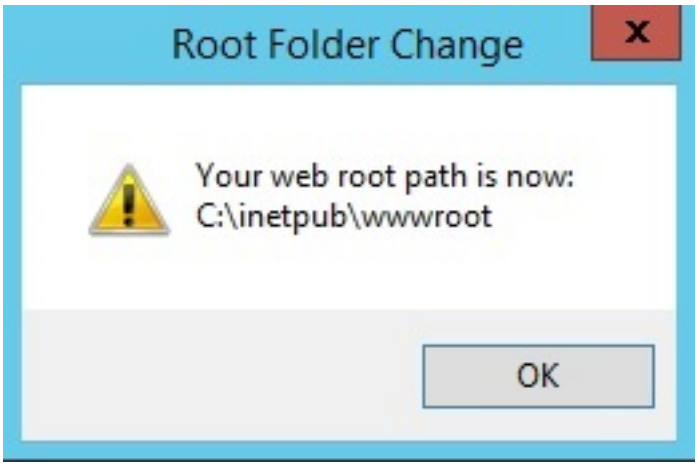


Then, in the same window, click on “Select a new Web Server root path”, and put the path of the IIS directory, which should be something like: “C: \ inetpub \ wwwroot”. Now click on “Save and Restart the AdminTool”.



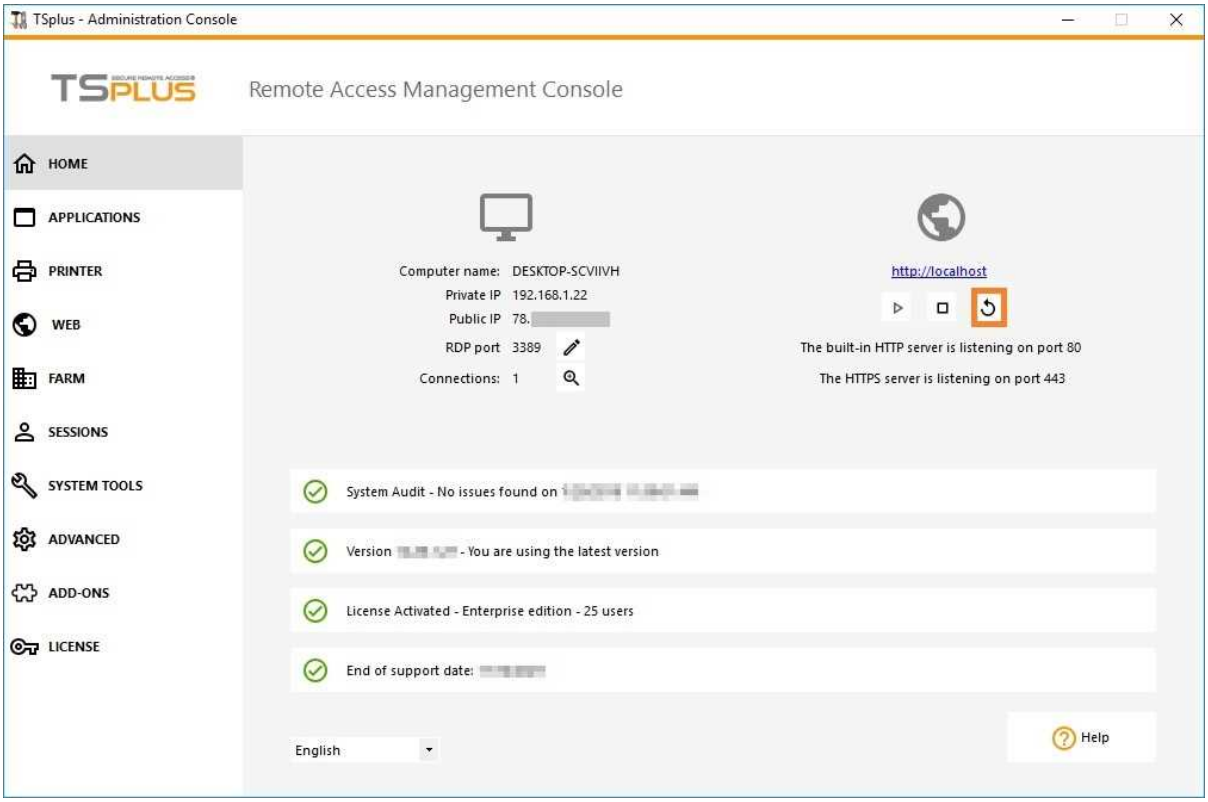
The following messages will appear:





Wait. The Admintool will be closed automatically. Then open the Admintool again and click on the Web tile.

Finally, restart the web servers:



7. Test with local host

Warning: Use a different user account.

If you try with your current user account from your own RDP session to the server, then you will be disconnected and not be able to reconnect.



Additional actions:

Configure RemoteApp

The “remoteapp” folder in the IIS web root (c:\inetpub\www\cgi-bin\remoteapp) must also have full permissions to the IUSR user, otherwise a 704 error will appear when attempting to use RemoteApp.

Configure 2FA

On a fresh install where 2FA has never been enabled, there is no folder named C:\Program Files (x86)\TSplus\Clients\webserver\twofa, or the twofactorauth.ini file.

It’s necessary :

- activate 2FA in AdminTool to create this folder and this .ini file
- then deactivate 2FA
- then apply IUSR user permissions to the newly created twofa folder.

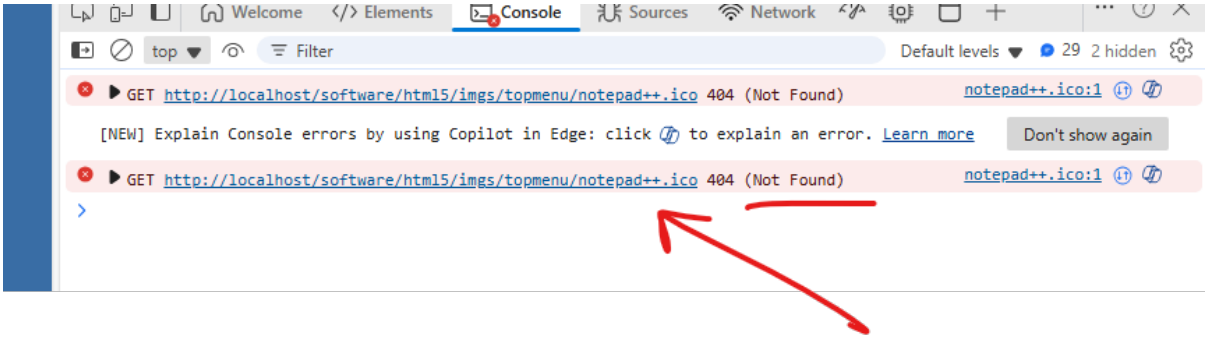
Failure to complete this step (even if you don’t intend to use 2FA) will prevent users from logging in with an error message stating that the credentials are invalid.

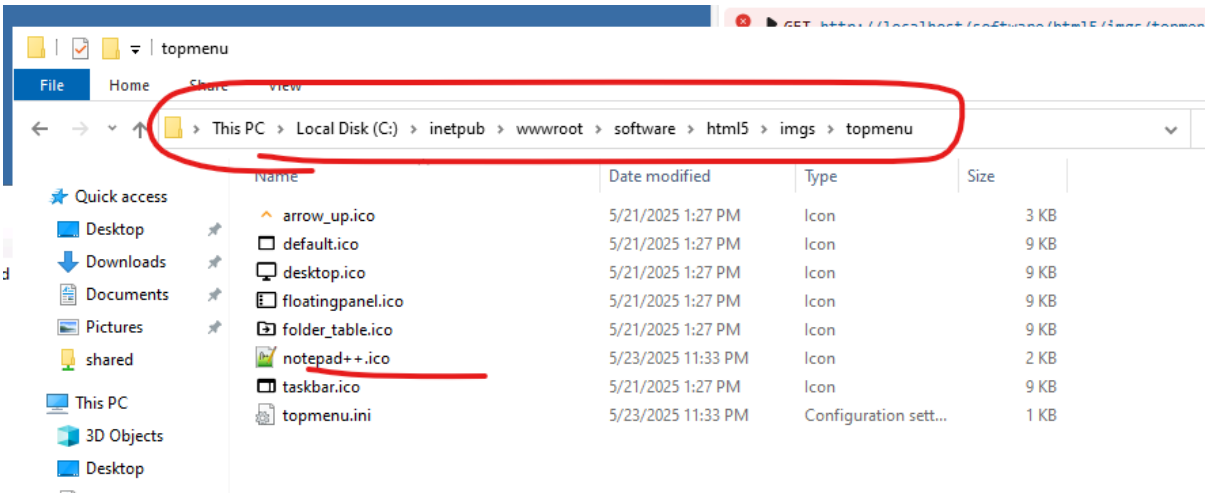
8. Allow double escaping

To allow downloads, you need to enable “Allow double escaping” in Request Filtering within IIS. This change will enable IIS to correctly handle special characters like ”+” in file names. Here’s how to enable “Allow double escaping” in IIS:

1. Open IIS Manager: Launch the Internet Information Services (IIS) Manager.

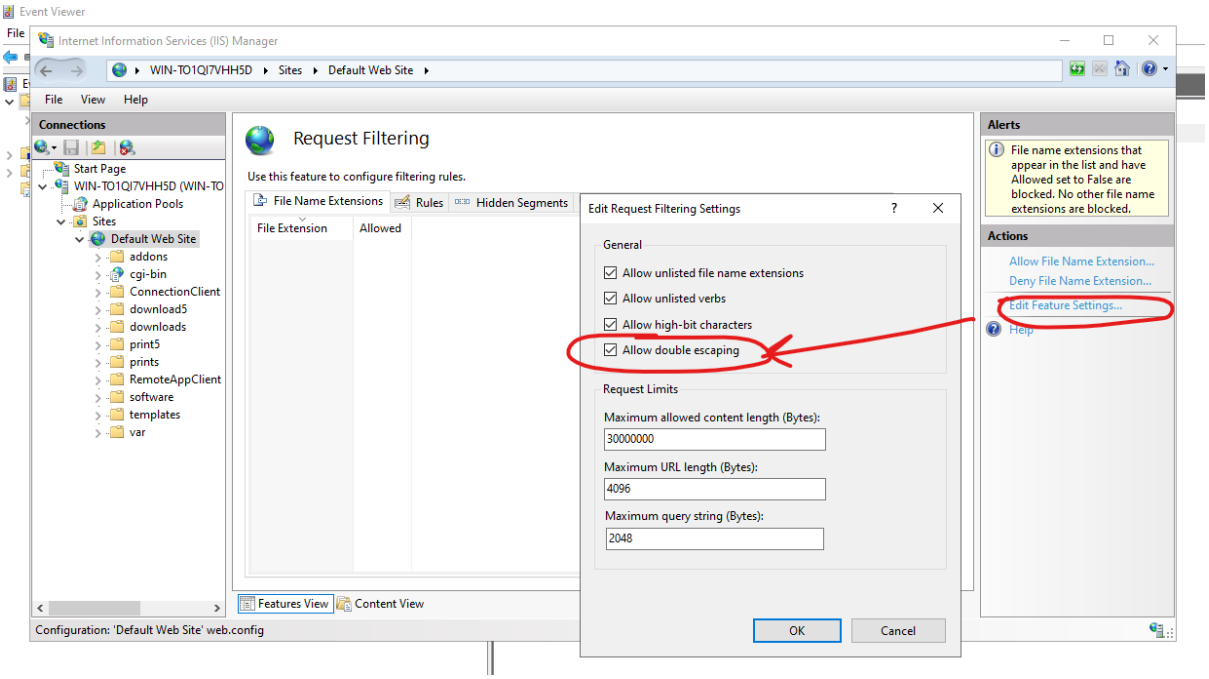
2. Navigate to Request Filtering: In IIS Manager, select the folder or website containing the file with the ”+” character. Then, double-click “Request Filtering” in the Features View.





3. Edit Feature Settings: In the Actions pane, click “Edit Feature Settings.”

4. Enable Allow double escaping: In the Edit Request Filtering Settings dialog, check the box for “Allow double escaping.”



5. Restart IIS (optional): Restarting IIS may help ensure that the changes take effect.

Using servers behind Reverse Proxy

It is possible to use servers behind reverse proxies via xhr-polling, with some limitations.

As described, Websockets are not part of HTTP protocol, even if first http request looks like http request, actually, it isn't, therefore most known reverse proxies do not support Websockets and drop many important areas of first Websocket request.

If you know that the server is behind reverse proxy, disable Websockets by setting this option in Clients\www\software\html5\settings.js :

disablewebsocket = true;

That will enforce the usage of XHR-polling and avoid time delay when connecting.

If you do not have a file named "settings.js" in the "C:\Program Files (x86)\TSplus\Clients\www\software\html5" folder, then your TSplus version is older and this documentation does not apply. Please update your system first or contact support.

Please note that the usage of XHR-polling is not as stable as Websockets due its connection nature.

The other limitation using Xhr polling via reverse proxy is the poor support on files upload. While working with XHR in direct connection, done for example via Apache reverse proxy, Apache can accidentally interrupt the file's upload.

TSplus Virtual Printer v2

A new version of Virtual Printer is now available!
This version includes an important update to the Virtual Printer component (v1.x -> v2.x).

Why: the Virtual Printer v2 is the latest Fabulatech's flagship, bringing many improvements and fixing issues reported by customers.

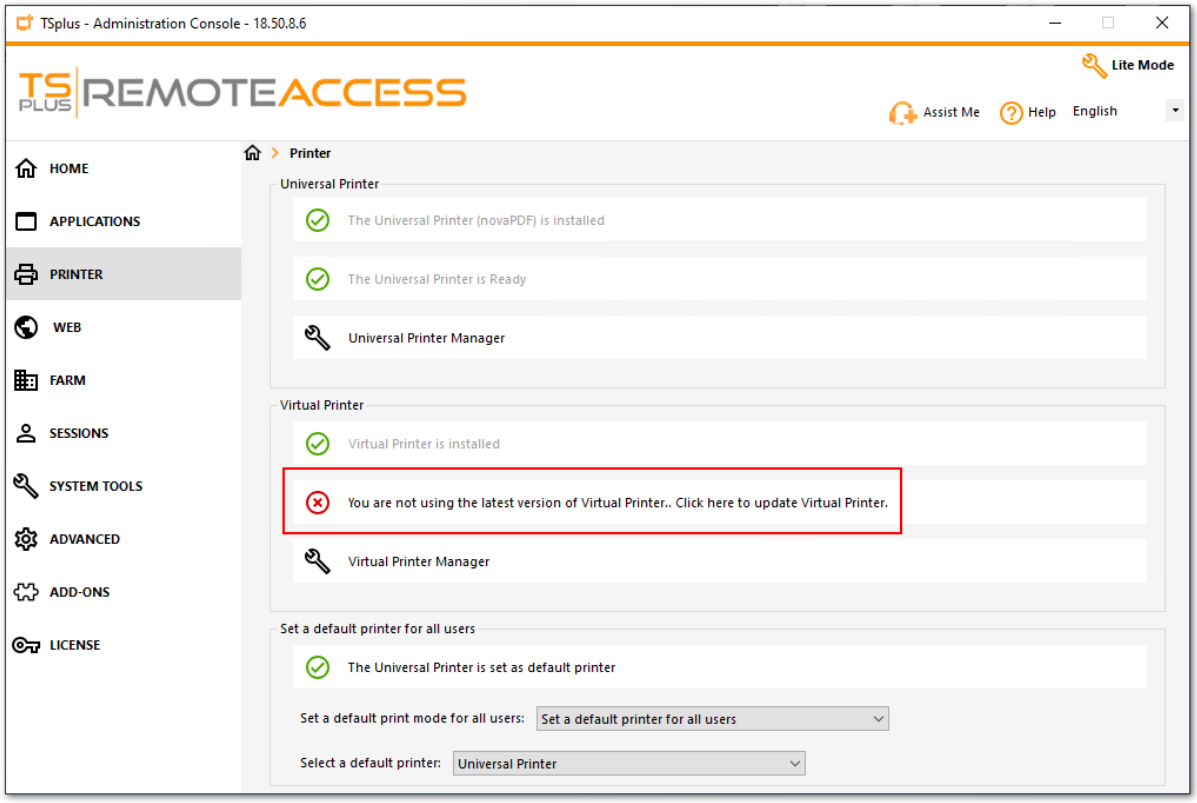
Attention: Virtual Printer v1.x and v2.x are not compatibles, you need the same major version on both client and server sides to work properly.

Don't panic: the UpdateRelease only brings the new Virtual Printer Setup programs (client and server).
They are located in "C:\Program Files (x86)\TSplus\UserDesktop\files\addons".
It's up to you to manually trigger the actual virtual printer update from AdminTools.

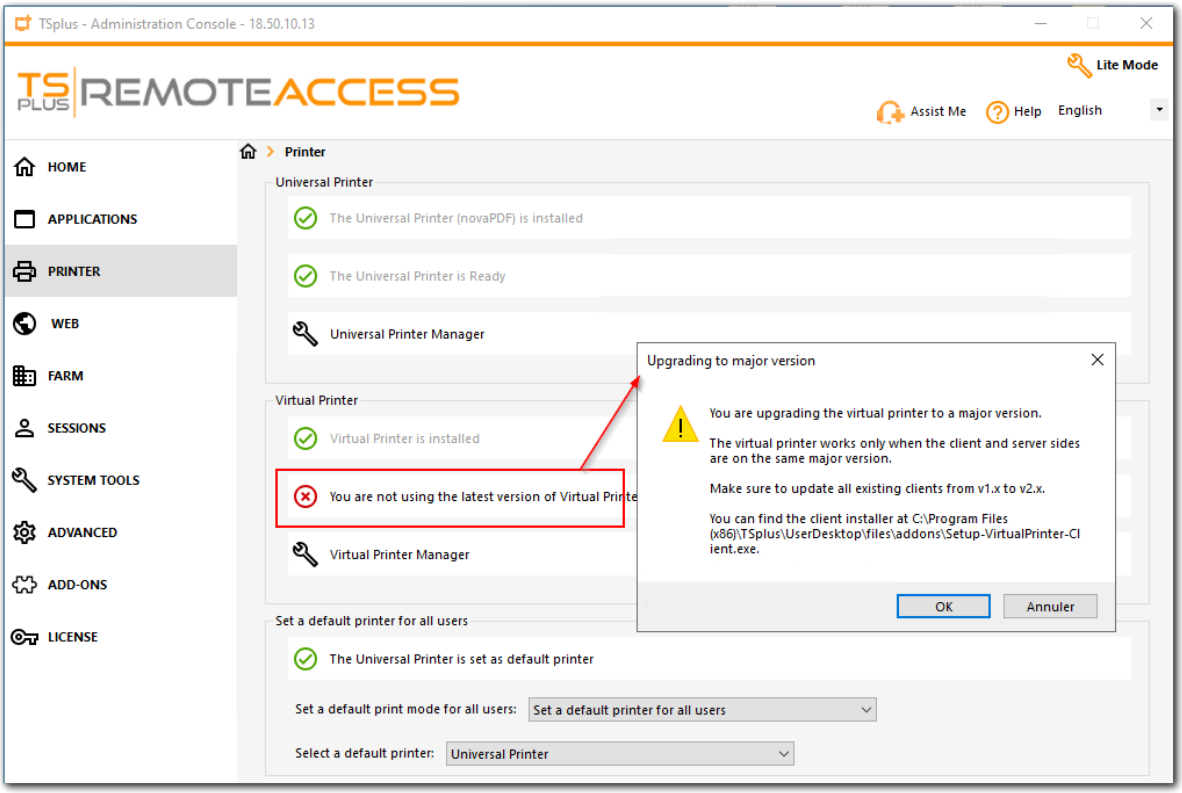
Links : TSplus Setup Full TSplus UpdateRelease Rebrand UpdateRelease

How to Update ?

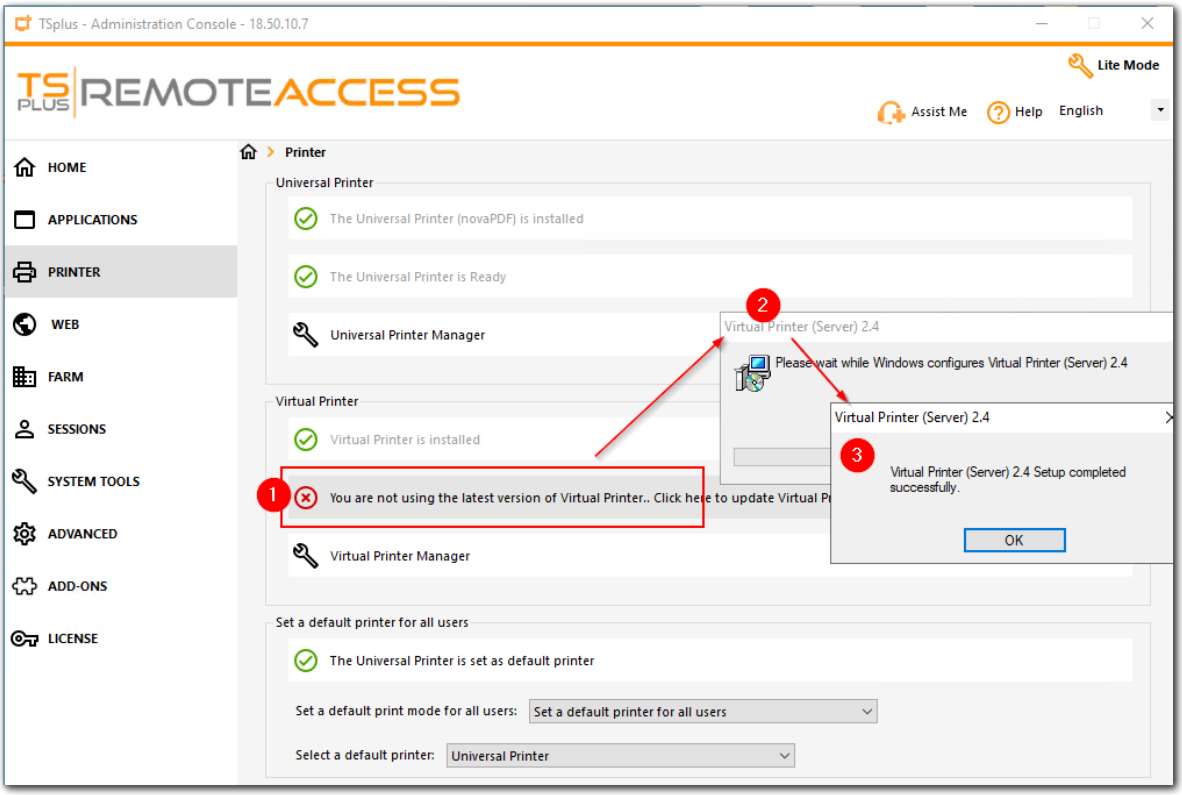
After installed the UpdateRelease, AdminTools will detect there is a new virtual printer version available.
Until you click on the "notice update" button, your currently installed virtual printer version remains unchanged, and everything will continue to work as before.



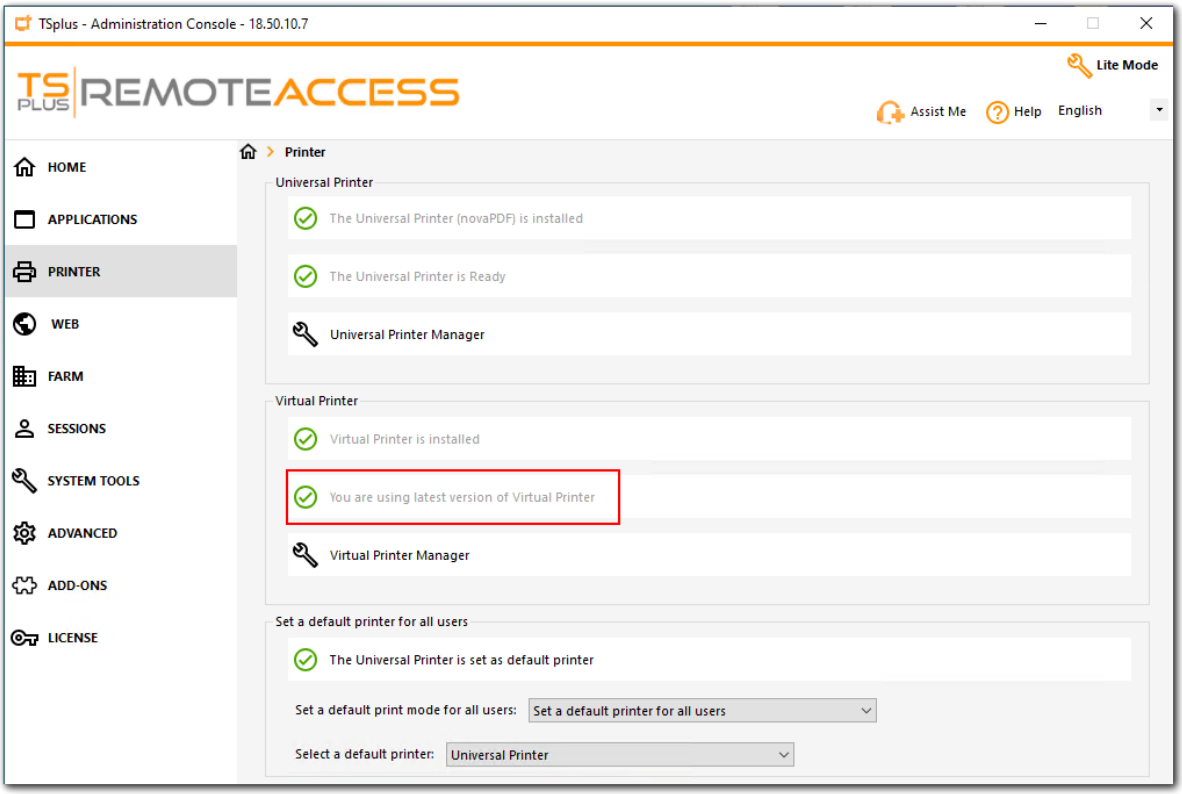
OK, but we are here to install the new VP version, so let's click on the "notice update" button.



A confirmation dialog asks if you really want to update the virtual printer the next major version. Click "OK"



Once installed, the AdminTools detects you're up to date.



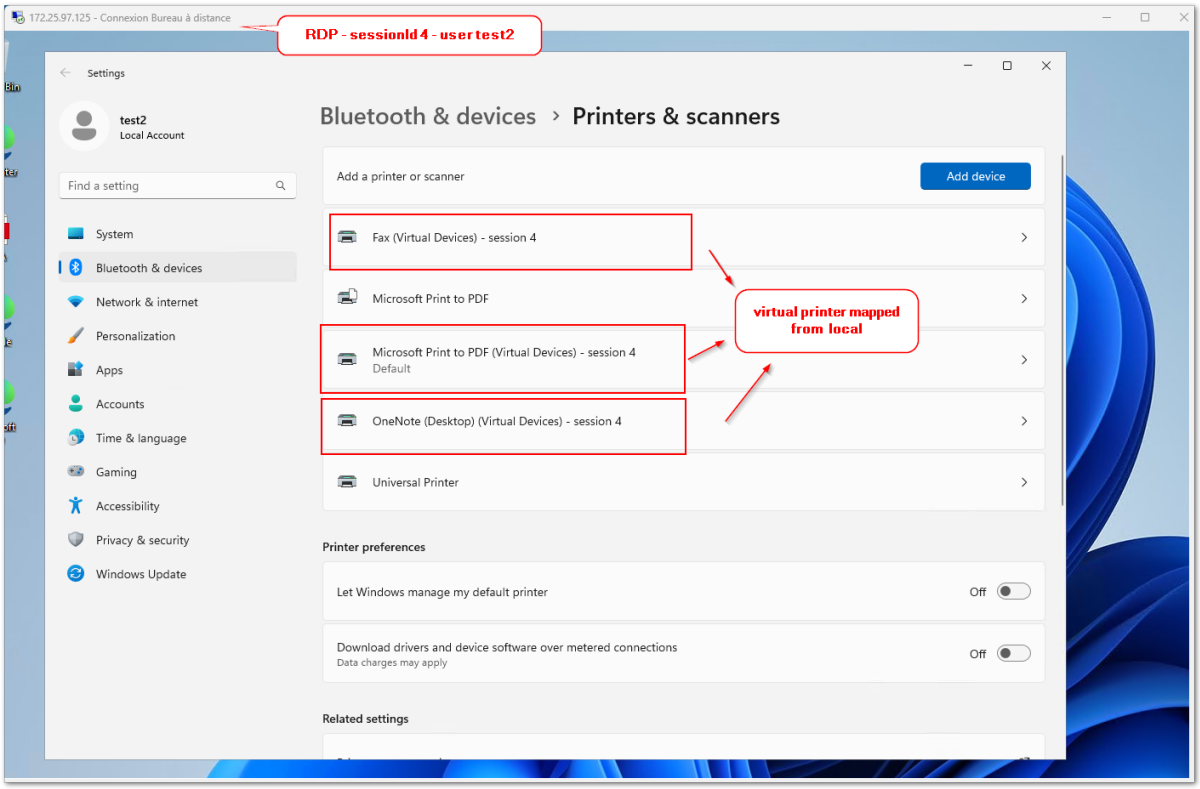
Attention: at this step, only clients running the same major version (v2.x) can print through the virtual printer on this server. Make sure to coordinate the update of both server and clients. The client installer is located in "C:\Program Files (x86)\TSplus\UserDesktop\files\addons\Setup-VirtualPrinter-Client.exe"

Breaking Change !

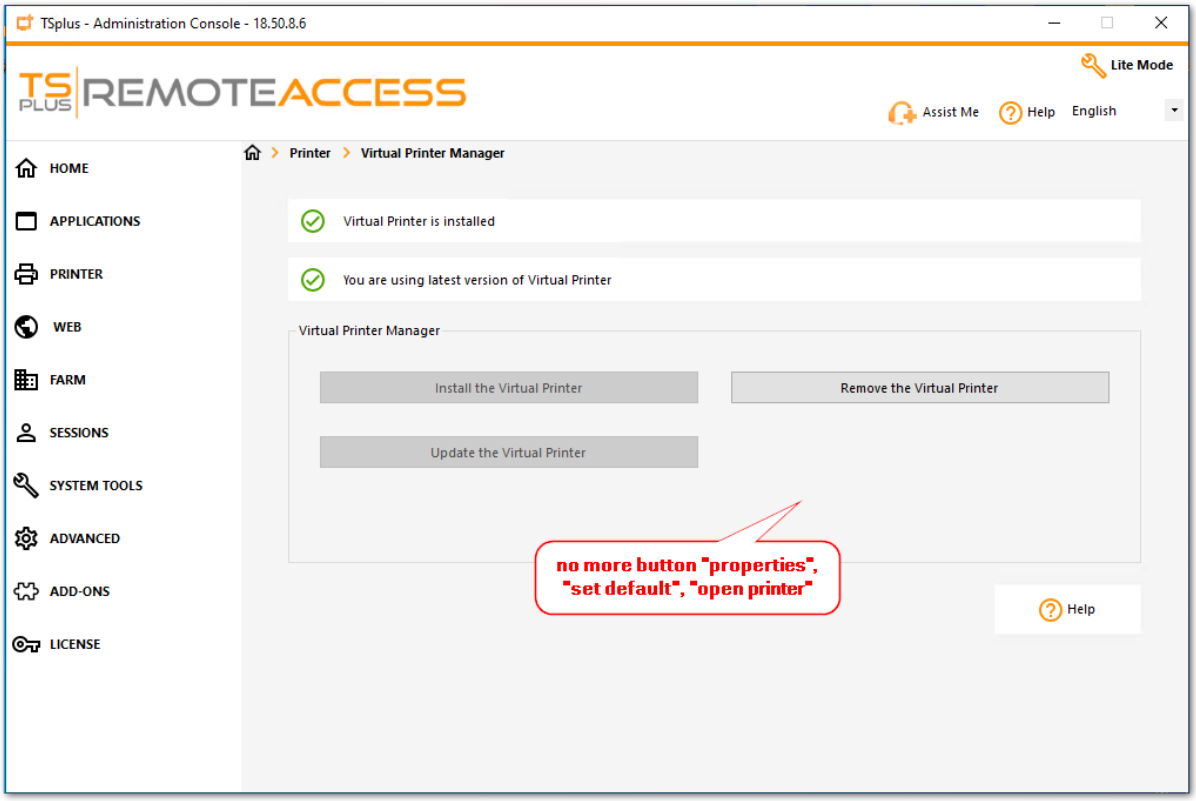
There is no longer a single “Virtual Printer” device in the printer list. Instead, each local printer is now mapped to a corresponding virtual printer in the RDP session.

In screenshot below, user “test2” is connected to RDP session #4. When opening the printers panel,
he can see and use its local printers. Each printer name follow this format : “$printerName (Virtual Devices) - session $sessionId”.

The fact that the user now sees each of their local printers individually is a major UX improvement, and that’s why Fabulatech is pushing to this new version.

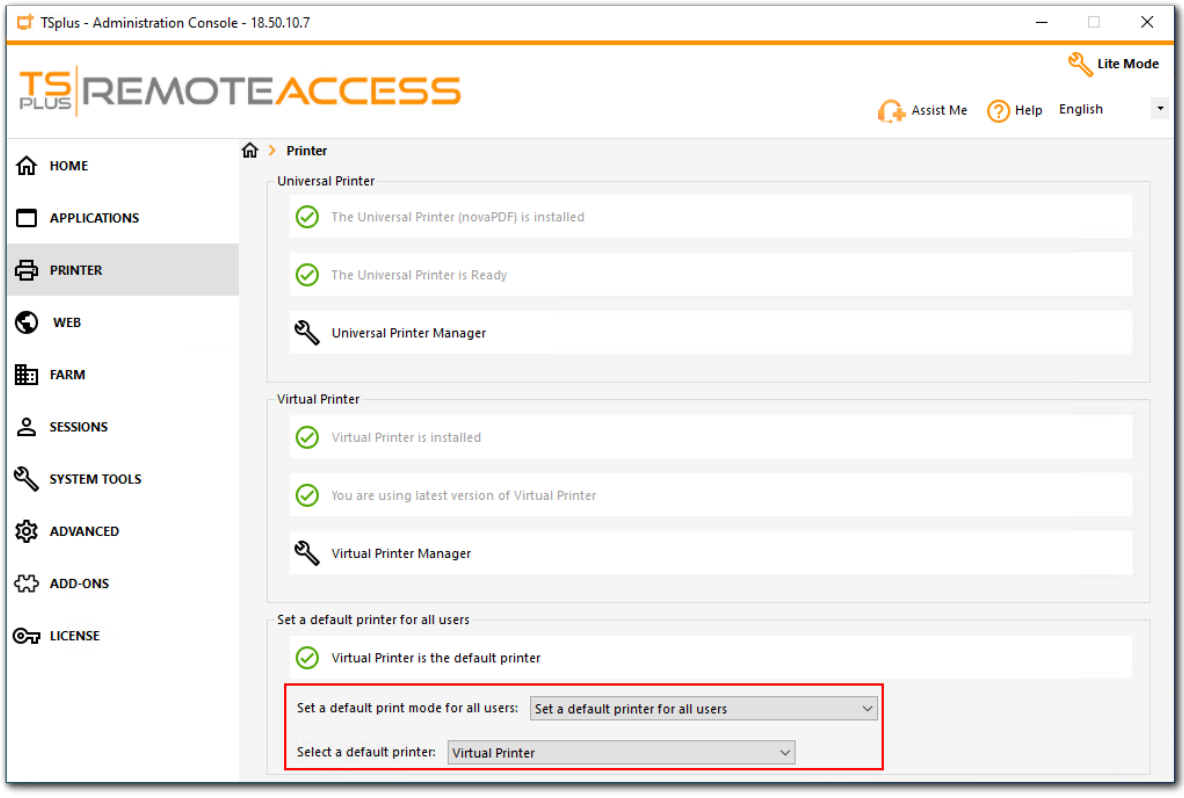


Because of this, we’ve adjusted some parts in the AdminTools UI, such as the Virtual Printer Manager : some buttons have been removed.

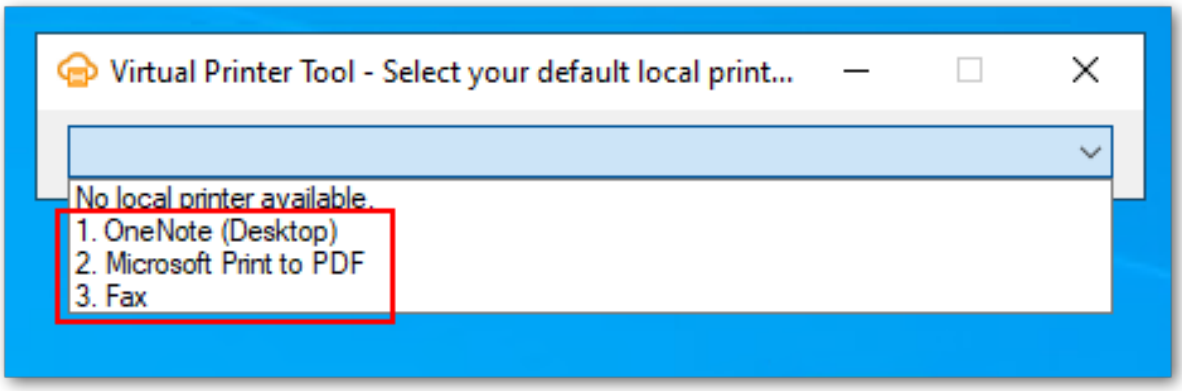


How to Configure ?

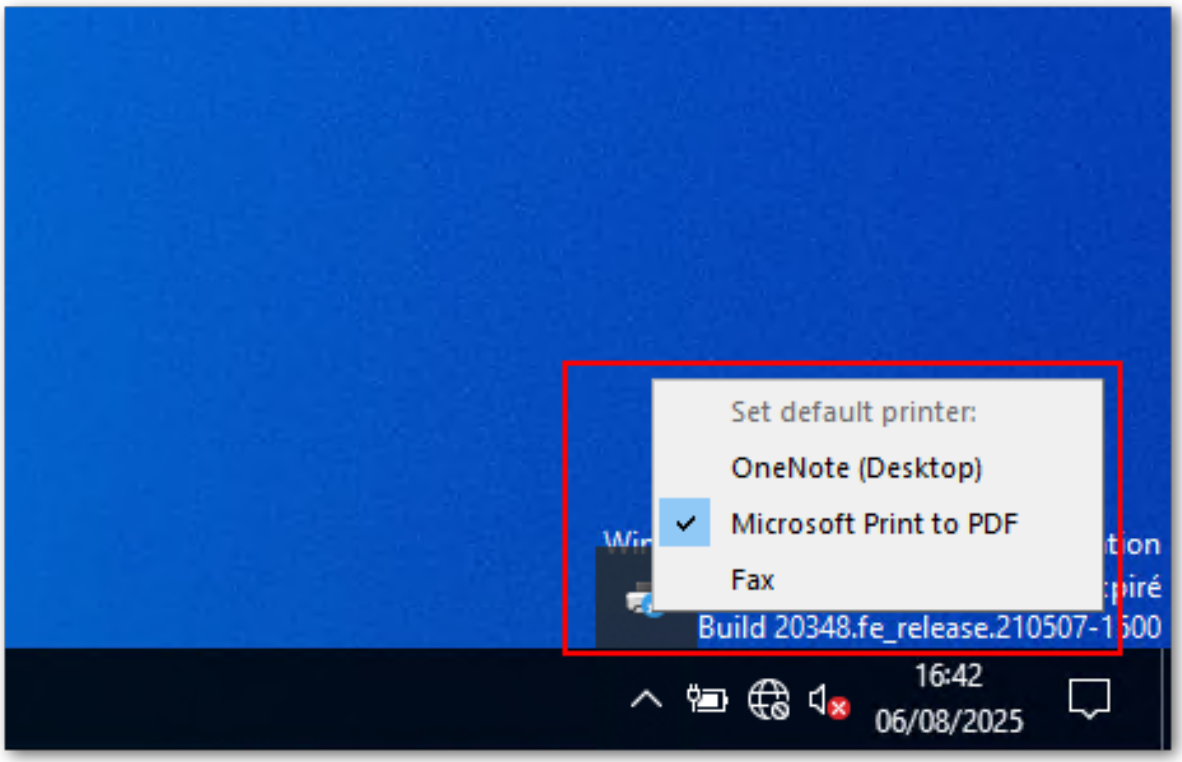
The configuration still remains the same in the AdminTools and should work as before.



If you use the Virtual Printer Tools, nothing change and it works as before.



If you use the selector in toolbar, nothing change and it works as before.



How to customize the name of the Virtual Printer mapped devices ?

On the server, execute the attached “customize-virtual-printer-name.reg”. Download

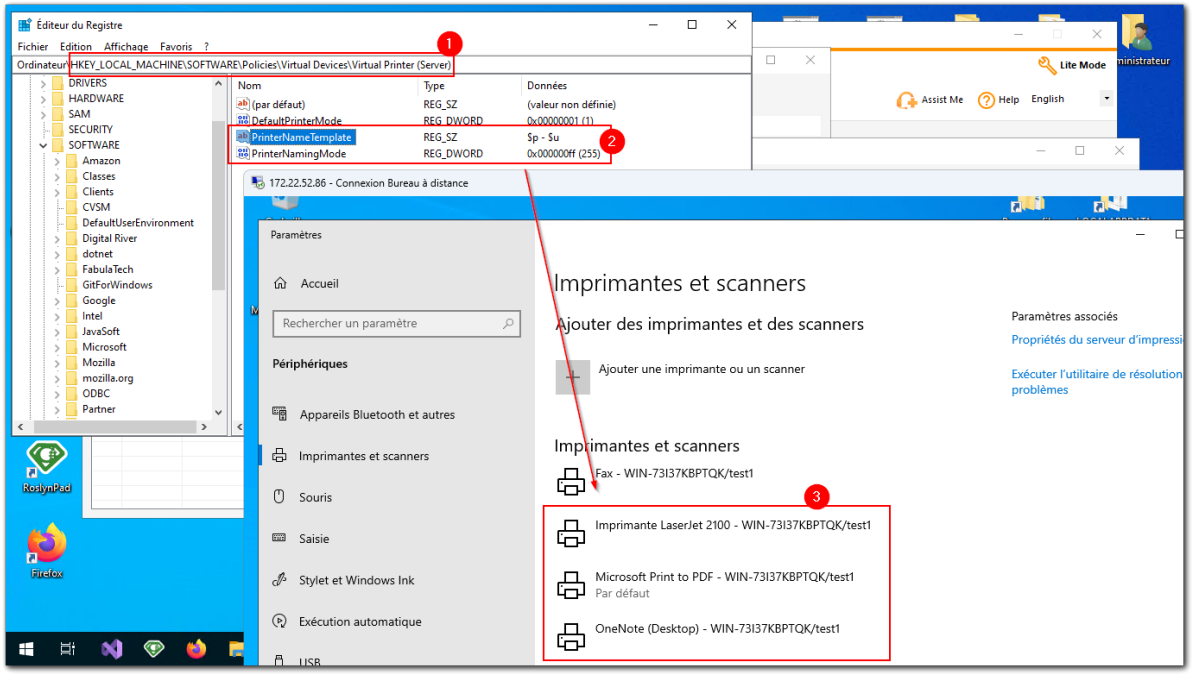
It will add 2 keys in your registry HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Virtual Devices\Virtual Printer (Server)
The PrinterNameTemplate is the template string, and there are 3 variables available :

- $p - printer name
- $u - full username (domain/user, or compname/user)
- $s - session number

Given some Fabuletch constraints : **Specifying $p and $u, or $p and $s is mandatory.**

It’s needed since the printer names should be uniques on the server for different users.

Example : PrinterNameTemplate = “$p $u”, you can see the result in the RDP session screenshot below



Advanced configuration

The advanced configuration for Virtual Printer v2 can be managed server-side via Group or Local Policy Object under Computer Configuration > Administrative Templates > Virtual Devices > Virtual Printer (Server).

The following settings are relevant for Remote Access integration:

- Default Printer Selection Mode: Defines how the default printer is assigned each time a user logs into a remote session.
- Printer Name Template: Specifies the naming format for virtual printers from user sessions.
- Limit Quality for Large Prints: Reduces print quality for pages exceeding a specified size to speed up large-format printing while preserving maximum quality for smaller pages.

For full configuration details, please refer to Virtual Printer GPO documentation at https://www.fabulatech.com/printer-for-remote-desktop-server-help/gpo.html

TSplus Virtual Printer

The TSplus virtual printer is a new alternative to classic remote desktop printing solutions, which can be unreliable, hardware dependent and difficult to manage. The virtual printer's unique compression algorithm improves the transit speed of remote print jobs by minimizing data transfer while maintaining image quality.

Note: The TSplus HTML5 client is not supported and it requires the TSplus Universal Printer.

Benefits

- Single-user and multi-user environment support.
- Zero configuration is required.
- Works with any virtual machines.
- Mixed 32 and 64-bit environment.

Pre Requisites

TSplus virtual printer OS compatibility list:

- Windows **7**
- Windows **8/8.1**
- Windows **10**
- Windows **11**
- Windows **Server 2008 R2**
- Windows **Server 2012 R2**
- Windows **Server 2016**
- Windows **Server 2019**
- Windows **Server 2022**

- Windows **Server 2025**

The TSplus Virtual Printer is compatible with:

- The TSplus generated client
- The TSplus RemoteApp client
- The TSplus RemoteApp plug-in when using the Web Portal
- The Microsoft Remote Desktop client

It is not compatible with:

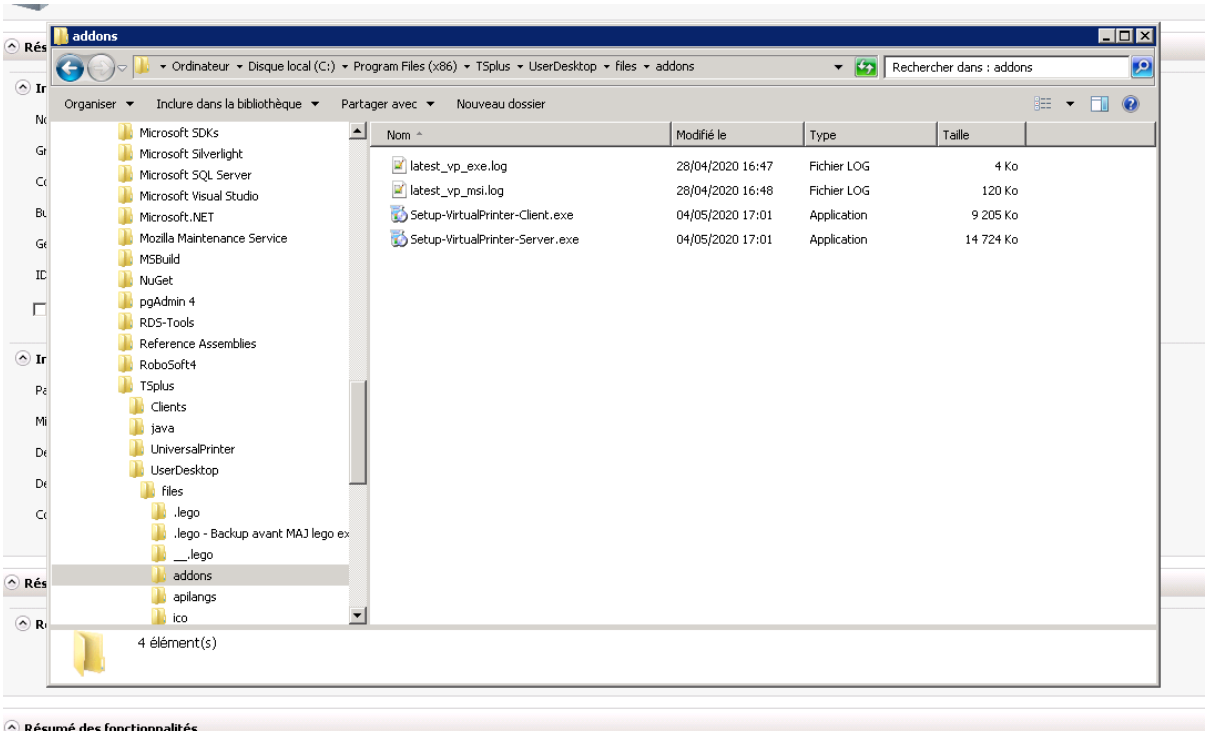
- The TSplus HTML5 client
- Hard Coded Thin-client devices where the client side setup cannot be installed.

Two Parts

The TSplus Virtual Printer is made up of two components:

- A server side component that comes installed on TSplus Remote Access.
- A Desktop component that is installed on the end-user's Windows Workstation.

Both setups are available directly in the server side in the "C:\Program Files (x86)\TSplus\UserDesktop\files\addons" folder and named "Setup-VirtualPrinter-Server.exe" and "Setup-VirtualPrinter-Client.exe":



The Client setup is also available from your TSplus web server, using the link below:

"yourtsplusserveriporpublicdomain"/addons/Setup-VirtualPrinter-Client.exe

You can also perform a silent install of the Client via a command line, by executing the setup with the following parameters:

/SUPPRESSMSGBOXES /VERYSILENT /SILENT /no_ui

Getting started

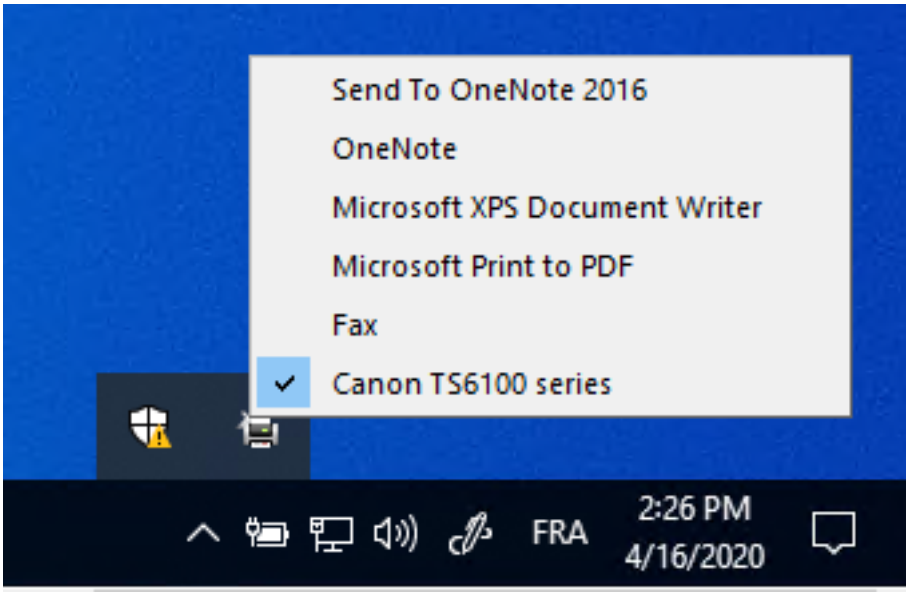
TSplus virtual printer is automatically installed during the first TSplus installation, and directly available during the trial period.

Once TSplus is installed, you will need to install the “Virtual Printer Client” on user’s computer.

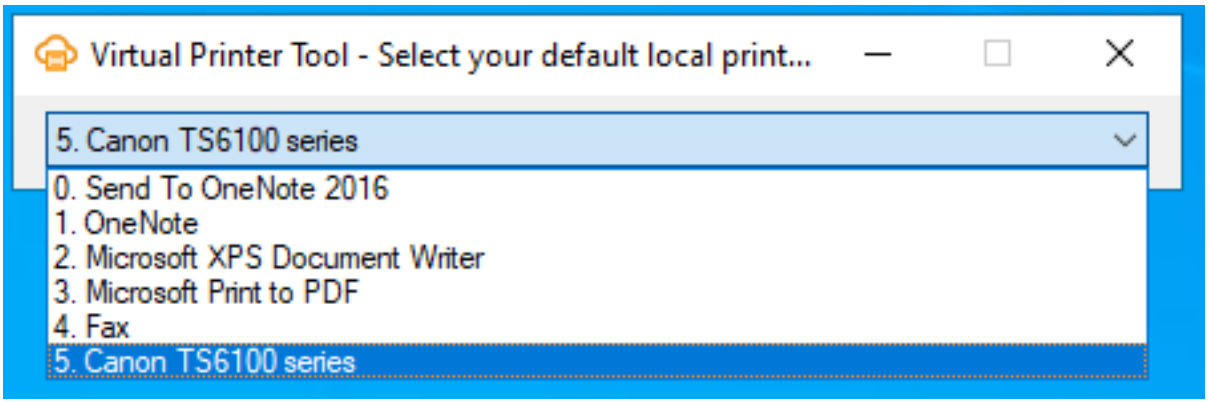
When you connect remotely to your TSPlus server using either **Microsoft RDP client** (mstsc), **TSplus generated client** or **Web Portal RemoteApp plug-in**, you will be able to print from your remote session to your local printer using the “Virtual Printer” printer. By default, the local printer selected is the local default printer.

You have 2 ways to change the local printer mapped to the “Virtual Printer” printer based on your situation:

1.If you are using the full desktop, then you can select which local printer to be used by using the virtual printer icon in the systray:



2.If you don’t have access to the full desktop, you will need to use the “Virtual Printer Tool” named “VirtualPrinterTool.exe” located in “C:\Program Files (x86)\TSplus\UserDesktop\files”. Note: you can either assign the application to the user, or make it run automatically on logon through the Virtual Printer advanced settings:

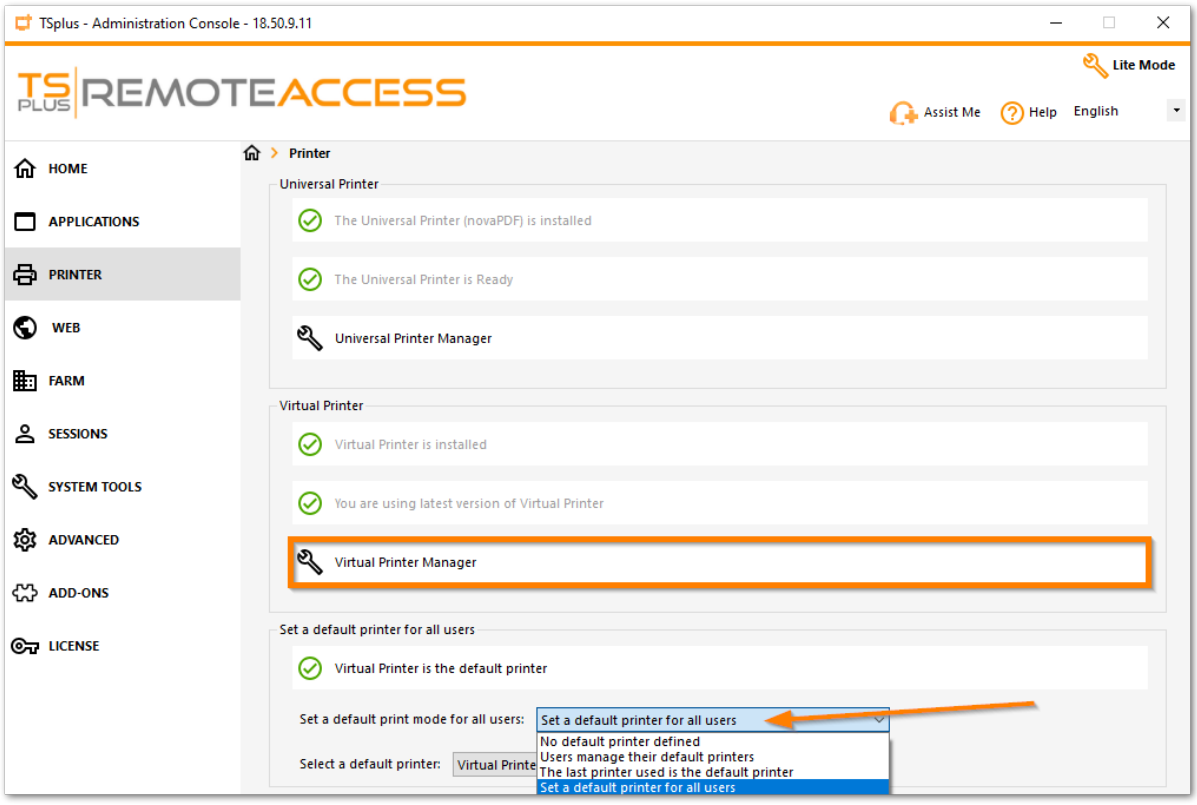


Configuration

To access to the TSplus Virtual Printer control panel, please navigate through the AdminTool: Printer > Virtual Printer Manager

Set a default printer for all users

- No default printer defined: the user's default printer configuration is not affected.
- User manage their default printers: the "Let Windows manage my default printer" option is disabled, and it is therefore up to the user to select their default printer.
- The last printer used is the default printer: the "Let Windows manage my default printer" option is enabled.
- Set a default printer for all users: the administrator forces the user's default printer.



Troubleshooting the Virtual Printer

If the Virtual Printer is not working, the most common cause is that either the client-side software “Print Application” is not running in the Task Manager of the user’s local computer, or that the Virtual Printer (server) software has been installed on the user’s local computer, rather than the Virtual Printer (workstation) version (Setup-VirtualPrinter-Client.exe). Below are the troubleshooting steps in detail for both the client and server sides.

Please note that the Virtual Printer is not compatible with our HTML5 client. If you are using the HTML5 client, please use the Universal Printer instead.

Troubleshooting Guide

How to activate a Volume License from the Server after Setup?

If you have installed your product without any command line, then it is installed as a trial version.

Activate

To activate your Volume License, run the following command line as an elevated administrator:

- **Remote Access & Two Factor Authentification**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  AdminTool.exe TwoFactor.Admin.exe
  /Users 1 (1 to 50 or unlimited)
  /edition Enterprise (Desktop, MobileWeb, Enterprise)
  /supportyears 1(1,2,3 only)

Example : C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 30 /edition Enterprise /supportyears 1

Example :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
  /edition Ultimate (Essentials or Ultimate)
  /supportyears 1(1,2,3 only)

Example :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
  /Users 1 (1 for Startup, 5 for Essential, 10 for Business)
  /supportyears 1(1 for Startup, 5 for Essential, 10 for Business)

Example :C:\Program Files (x86)\TSplus-ServerMonitoring\ServerMonitoring.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users 5 /supportyears 1

- **You can add my following additional parameters:**
  — /comments "your comments"Specify the comments to attach to the license on the license portal.
  — /verysilentExecute the setup program silently. This enables the integration of this setup program into your own initialization or automation scripts.

Example :C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate YOUR-VOLUME-LICENSE-KEY /users unlimited /edition Enterprise /supportyears 3 /comments "This is a comment"*

Parameters

This command takes the following parameters:

(if you like using command lines and are wondering what other command lines are available, please go to this specific documentation)

Update Support

To extend your update/support subscription, choose 1, 2 or 3 in operation of the extension time. Use this command:

AdminTool.exe /vl /renewsupport YOUR-VOLUME-LICENSE-KEY /supportyears 1"

Add Missing Support

This command is particularly useful if the customer forgot to activate support during installation or if they need to set a specific end date for their support period.

Run this command as an administrator, replacing the details with your own license information and the preferred end of support date:

AdminTool.exe /vl /activate-support YOUR-VOLUME-LICENSE-KEY /users [number] /edition [edition] /endofsupport [YYYY-MM-DD]

Example: To activate support for a Remote Access 5 user with the Printer edition until July 25, 2026, enter:

AdminTool.exe /vl /activate-support YOUR-VOLUME-LICENSE-KEY /users 5 /edition Printer /endofsupport 2026-07-25

This new feature makes it easier to manage support periods, so customers always know when their support period starts and ends.

How to display the remaining license credits for a Volume License key?

To display the remaining license credits for a Volume License key, run the following command line as an elevated Administrator:

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

Parameters

This command may take four parameters:

- VOLU-MELI-CENS-EKEY : use your own Volume License Key
- /login JOHNDOE : provide the login of the partner associated with the Volume License key
- /edition Essentials : provide the optional edition parameter for Advanced Security and Server Monitoring products
- /silent : executes the command silently

The output will be stored in the user-level environment variable named VOLUME_LICENSE_CREDITS. It may be required to read the value of VOLUME_LICENSE_CREDITS from a different process, using the command: echo %VOLUME_LICENSE_CREDITS%

Please find below the expected editions for Advanced Security and Server Monitoring products:

- Advanced Security: “Essentials”, “Ultimate”
- Server Monitoring: “Essentials”, “Startup”, “Business”

The following executables must be used to find the respective number of remaining credits:

- Remote Access: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- Advanced Security: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- Server Monitoring: 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
- Remote Work: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

title : “How to display the remaining support credits for a Volume License key?”

To display the remaining support credits for a Volume License key, run the following command line as an elevated Administrator:

AdminTool.exe /vl /credits-support VOLU-MELI-CENS-EKEY /login JOHNDOE [/edition Essentials] [/silent]

Parameters

This command may take four parameters:

- VOLU-MELI-CENS-EKEY : use your own Volume License Key
- /login JOHNDOE : provide the login of the partner associated with the Volume License key
- /edition Essentials : provide the optional edition parameter for Advanced Security and Server Monitoring products
- /silent : executes the command silently.

The output will be stored in the user-level environment variable named VOLUME_LICENSE_CREDITS. It may be required to read the value of VOLUME_LICENSE_CREDITS from a different process, using the command: echo %VOLUME_LICENSE_CREDITS%

Please find below the expected editions for Advanced Security and Server Monitoring products:

- Advanced Security: “Essentials”, “Ultimate”
- Server Monitoring: “Essentials”, “Startup”, “Business”

The following executables must be used to find the respective number of remaining credits:

- Remote Access: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe
- Advanced Security: C:\Program Files (x86)\TSplus-Security\TSplus-Security.exe
- Server Monitoring: 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
- Remote Work: C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe

How to Disable a License from the Server?

To disable a server which was activated with a Volume License key, run the following command line as an elevated Administrator:

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

How to Enable a License from the Server?

To enable a server which was first activated with a Volume License key and was later disabled, run the following command line as an elevated Administrator:

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

How to Disable a License from the Licensing Portal?

You must first disable the License on the Licensing portal, then make sure that the new status is applied on your server by updating its status from the administration application or the command line.

First, from both the Licenses list and the License details pages, you can click on the “Disable” button to disable the selected License.

The license will move from the “Enabled” status to the “Disabling…” status, meaning that it is currently waiting for the server to disable itself.
Then, the server will automatically disable itself following the next day if he has an internet access.

You can also do this manually by running the following command line as an elevated Administrator:

AdminTool.exe /license /refresh

Note that it is not necessary to run the refresh command line for all installed software. The refresh is supported by all products compatible with the 2020 licensing system.

The license will be accounted for in your license usage until your server has contacted the

License portal and acknowledged its disabled status.

How to install a Volume License Server in one step?

To install a Volume License server in one step, you will need to:

- Download the Product Setup program
- Use your Volume License Key
- Run the Setup program with your Volume License Key as a parameter

Your Volume License Key is the same one for any installation of any new server. If you do not remember it, connect to your account in the License portal. Your Volume License Key is displayed at the top on the home page (Licenses).

To install and activate a Volume License from a script, run the following command line as an elevated Administrator:

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments "This is a comment"

The scripted activation using Volume License 2020 is available for the following products and all their rebranded versions:

- Remote Access
- Advanced Security (aka RDS-Knight)
- Server Monitoring (formerly Server Genius)
- Two Factor Authentification

Parameters

This command takes the following parameters:

- **Remote Access & Two Factor Authentification**
  C:\Program Files (x86)\TSplus\UserDesktop\files>
  \AdminTool.exe \TwoFactor.Admin.exe
  /Users 1 (1 to 50 or unlimited)
  /edition Enterprise (Desktop, MobileWeb, Enterprise)

/supportyears 1(1,2,3 only)

- **Advanced Security**
  C:\Program Files (x86)\TSplus-Security>
  \TSplus-Security.exe
  /edition Ultimate (Essentials or Ultimate)
  /supportyears 1(1,2,3 only)

- **Server Monitoring**
  C:\Program Files (x86)\TSplus-ServerMonitoring>
  \ServerMonitoring.exe
  /Users 1 (1 for Startup, 5 for Essential, 10 for Business)
  /supportyears 1(1 for Startup, 5 for Essential, 10 for Business)

Scripting Methods

To start Setup-PRODUCT.exe with its correct command line you can use 3 methods:

1. Use your own management scripts methods

2. Create a shortcut of Setup-PRODUCT.exe and edit the properties to add the command line at the end of the path.

3. Simply open a “Command line” by pressing the Windows key and the “R” key simultaneously, then typing “cmd” and pressing the “Enter” key to confirm. This method with the keyboard shortcut is working on every existing Windows version at the time of writing of this document.

4. Once the prompt appears, change the current directory to the directory where is found your setup program (usually your Downloads folder). For instance, type:

   cd C:\Program Files (x86)\TSplus\UserDesktop\files

And finally type the full command to run the setup program with the following parameters, supplying the desired values:

C:\Program Files (x86)\TSplus\UserDesktop\files\AdminTool.exe /vl /activate VOLU-MELI-CENS-EKEY /users unlimited /edition Enterprise /supportyears 3 /comments “This is a comment”

Find the revelant Administration Program

The following programs supports Volume License commands.
The program name and location depend on the product and its setup folder:

Remote Access & Two Factor Authentification
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

The program execution is silent. This enables the integration of your license activation process into your own initialization or automatization scripts.

---

title : “Troubleshooting activate, enable, disable and update commands”

Should you want to investigate any issue and/or when prototyping your scripts, you can get success and error messages by looking at the **VolumeLicensing.log** file found at the root of the program.

---

title : “How to configure a Proxy Server for Internet Access”

Proxy settings defined during the installation are remembered and will be used to perform operations on licenses. If no proxy settings were defined, then the Volume Licensing program will use Internet Explorer proxy settings (if any is configured in the running session and/or for the windows service).

You can also configure the proxy settings manually by running the following command line as an elevated Administrator:

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

Parameters

#	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.

(if you like using command lines and are wondering what other command lines are available, please go to this specific documentation)

---

title : "How to get Support for Volume Licensing"

Volume LicensingSupport & Services team will be more than happy to help you, should you face any issue or trouble when installing and running Volume Licensing on a server.

The easiest way to contact Volume LicensingSupport & Services team is to open a ticket on our online Helpdesk at: https://support.tsplus.net

How to Update the Users of a Volume License from the Server?

To change the number of users associated with your activated Volume License, run the following command line as an elevated Administrator:

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /users 10

Parameters

This command takes two parameters:

- VOLU-MELI-CENS-EKEY : use your own Volume License Key
- /users unlimited : use any number from 1 to 50 or “unlimited”

Please note that:

- This command does not apply to Advanced Security and 2FA addon.
- Server Monitoring only accept the numbers 1, 5 and 10 corresponding to the three available editions of Server Monitoring.
- Only TSplus Remote Work accepts a count of users greater than 50.

---

title : “How to Update the Edition of a Volume License from the Server?”

To change the edition associated with your activated Volume License, run the following command line as an elevated Administrator:

AdminTool.exe /vl /update VOLU-MELI-CENS-EKEY /edition Enterprise

Parameters

This command takes two parameters:

- VOLU-MELI-CENS-EKEY : use your own Volume License Key
- /edition Enterprise : use the name of the edition

Please note that:

- This parameter does not apply to Remote Work, Remote Support, Server Monitoring, 2FA addon and Server Genius
- Possible editions are “Desktop”, “MobileWeb” or “Enterprise” for Remote Access
- Possible editions are “Essentials” or “Ultimate” for Advanced Security

(if you like using command lines and are wondering what other command lines are available, please go to this specific documentation)

Update support

To extend your update/support subscription, choose 1, 2 or 3 in operation of the extension time. Use this command: “AdminTool.exe /vl /renewsupport VOLU-MELI-CENS-EKEY /supportyears 1”

This command is only available from version 15.60.11.8

Volume Licensing

Volume Licensing is a scripting licensing solution powered by TSplus for its solutions. The following products supports activation using Volume Licensing 2020 : Remote Access, Remote Work, Advanced Security (aka RDS-Knight), Remote Support or Server Monitoring (formerly Server Genius).

When your Volume Licensing account is created on the Licensing Management portal, the Volume Licensing team will provide:

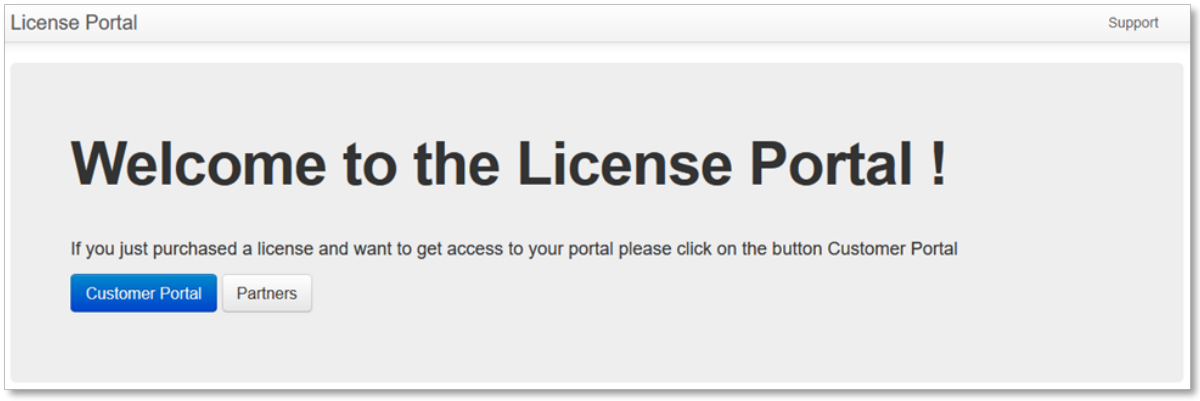
1. Your Volume License Key (please keep this information confidential)
2. Your credentials to connect to the Licensing Management portal
3. This Volume Licensing 2020 Administrator Guide

VIRTUAL PRINTER IS NO LONGER LICENSED
Please note that since 15th of March 2022 and version 15.40.3.14, Virtual Printer is no longer licensed and is included in all editions of TSplus Remote Access.

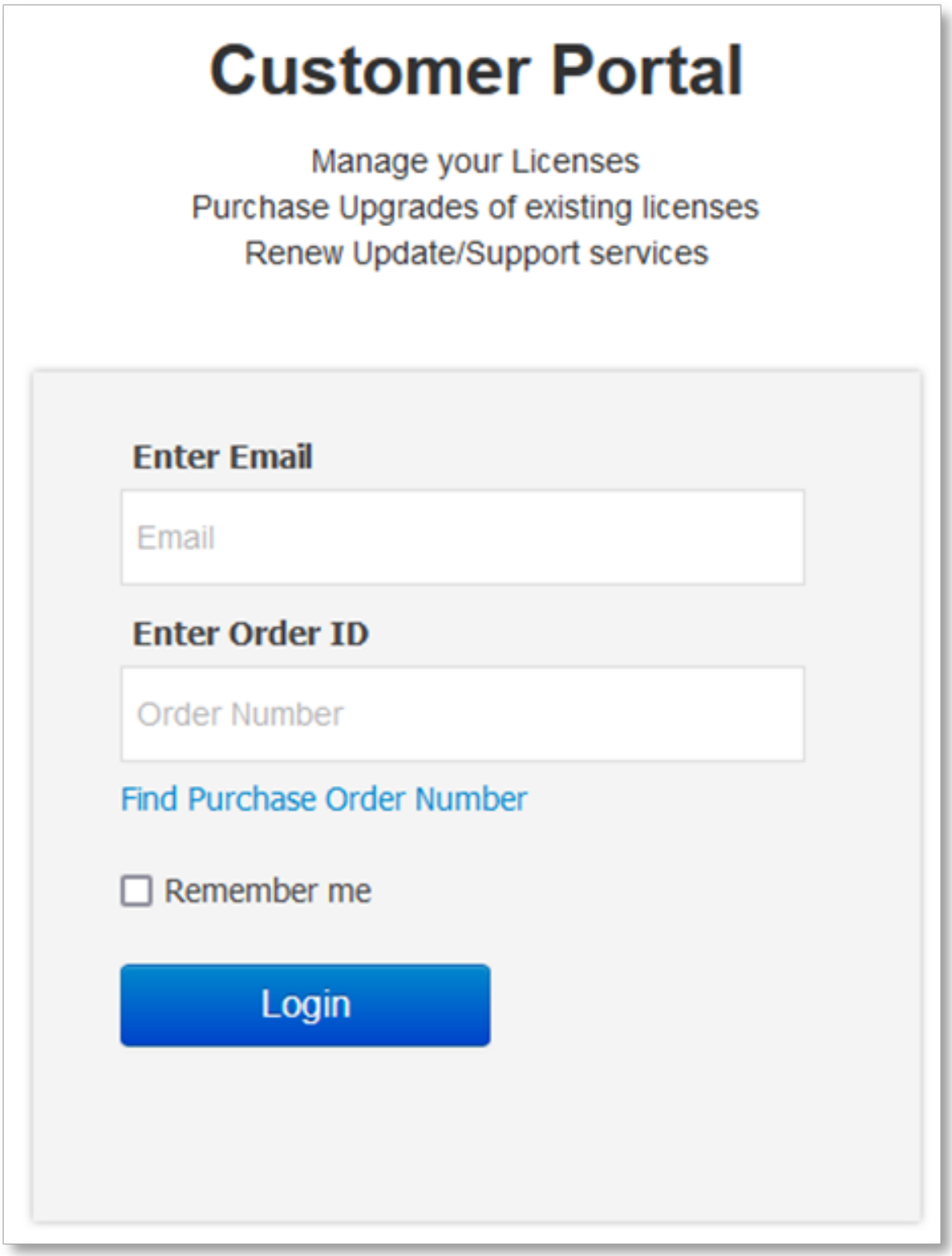
How to manage your Volume Licenses?

Your Volume Licenses and credit balance can be reviewed and managed in the TSplus License portal.
The TSplus License portal is available at the following URL: https://license.tsplus.net

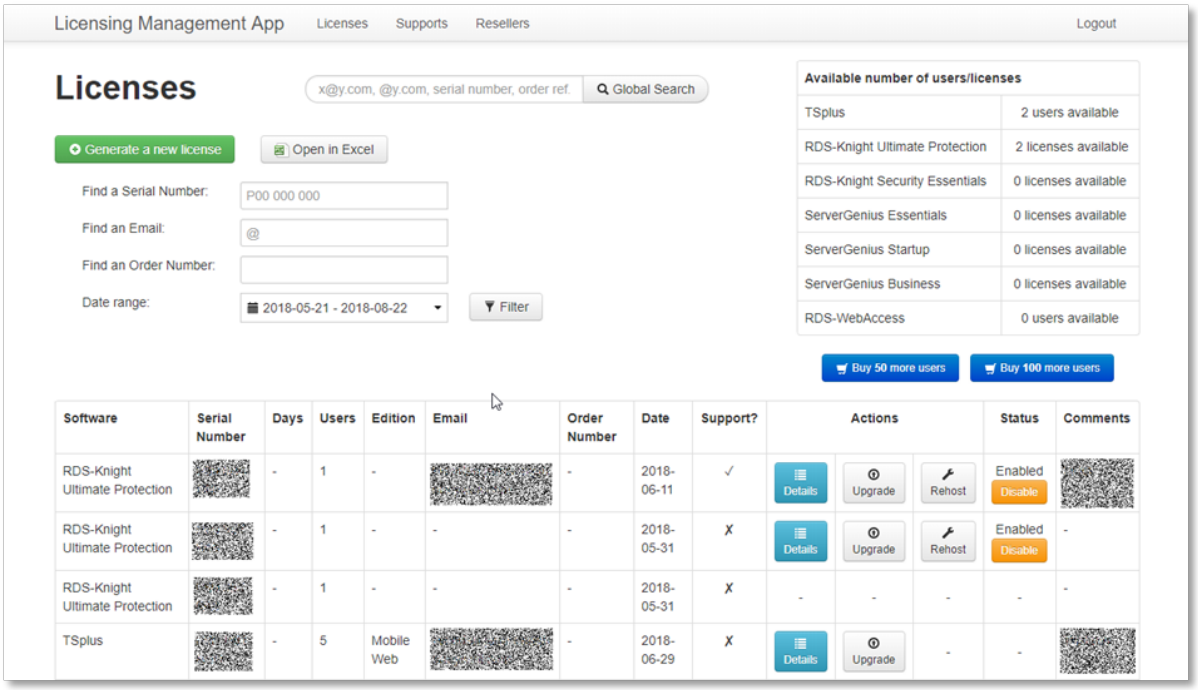
To connect and access to your account, start by clicking on Customer Portal to reach the customer's section:



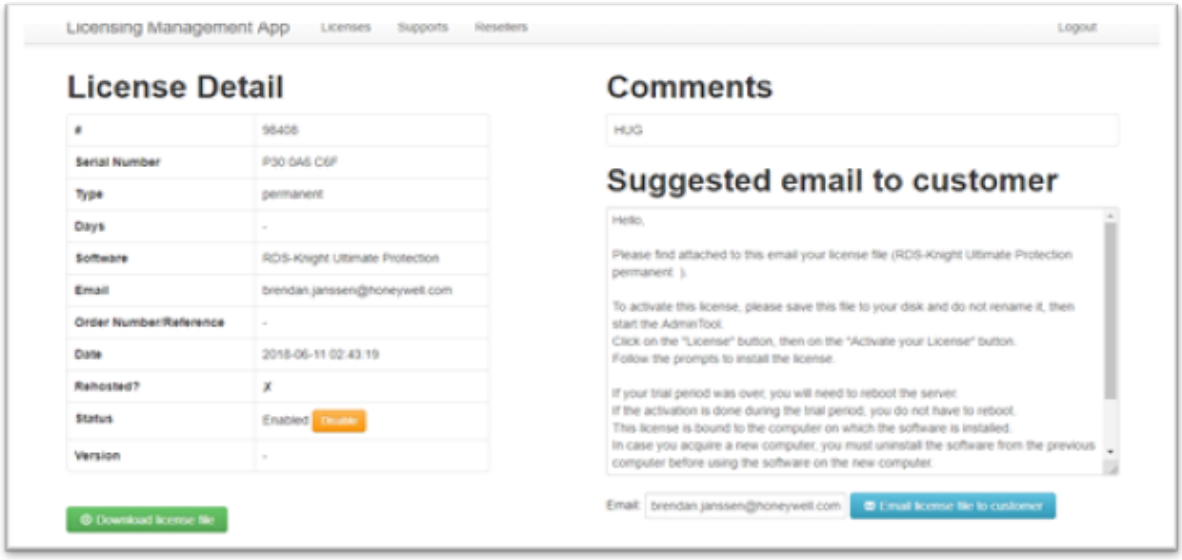
Then, type your credentials to access your account:



Once logged in, you will see the following table where all your Licenses are listed. It is the main page where you will be able to manage all your Licenses. If you have not yet activated any Volume License, this page will be empty.



To review one License history details, click on the “Details” button of the License you want to study. You will get the License details page as shown on the picture below.



TSplus Web App

TSplus Web App is a Progressive Web App (PWA) that leverages modern browser APIs to deliver a seamless remote access experience without cumbersome software installation or complicated connection clients. Designed to utilize industry standard HTML5 display and communication protocols, The TSplus Web App appears as a native connection solution, no matter what type of device you use.

Benefits

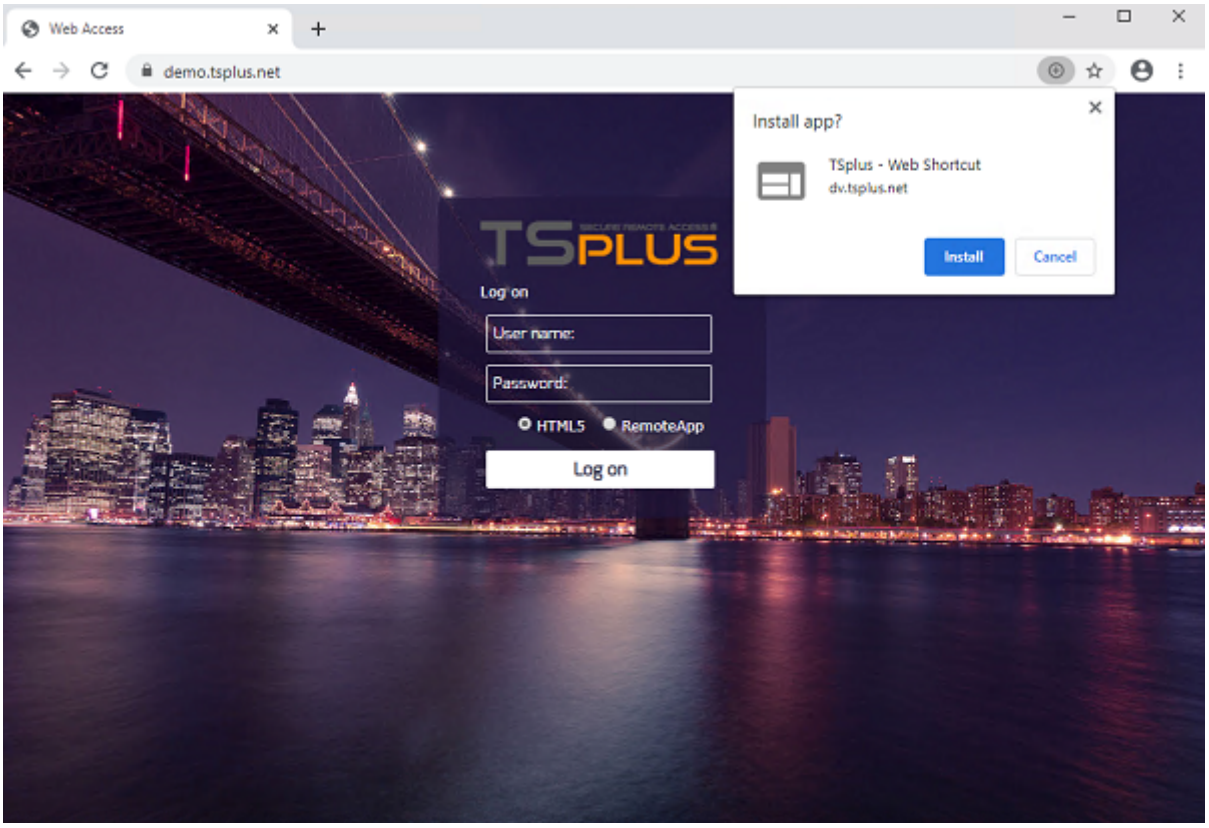
The new TSplus WebApp offers improved performance and value using the following improvements over legacy applications and connection clients:

- Faster load times due to the small software footprint.
- Lower data usage - TSplus Web App leverages common browser based traffic management to minimize data usage.
- Seamless user experience - from login display to application rendering, the TSplus WebApp offers the user the appearance of native application use.
- No more browser tabs or lost sessions due to too many open browser windows. The TSplus Web App behavior offers the same multitasking options as any other top level application.

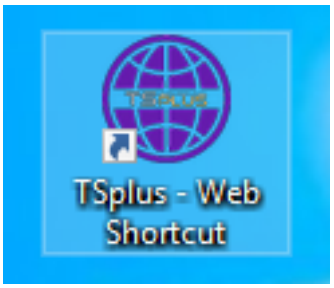
Installation - PC

Navigate to your corporate TSplus Web Portal using your preferred common web browser (HTTPS configuration required).
For use on Firefox, you will need to install the PWAS addon.

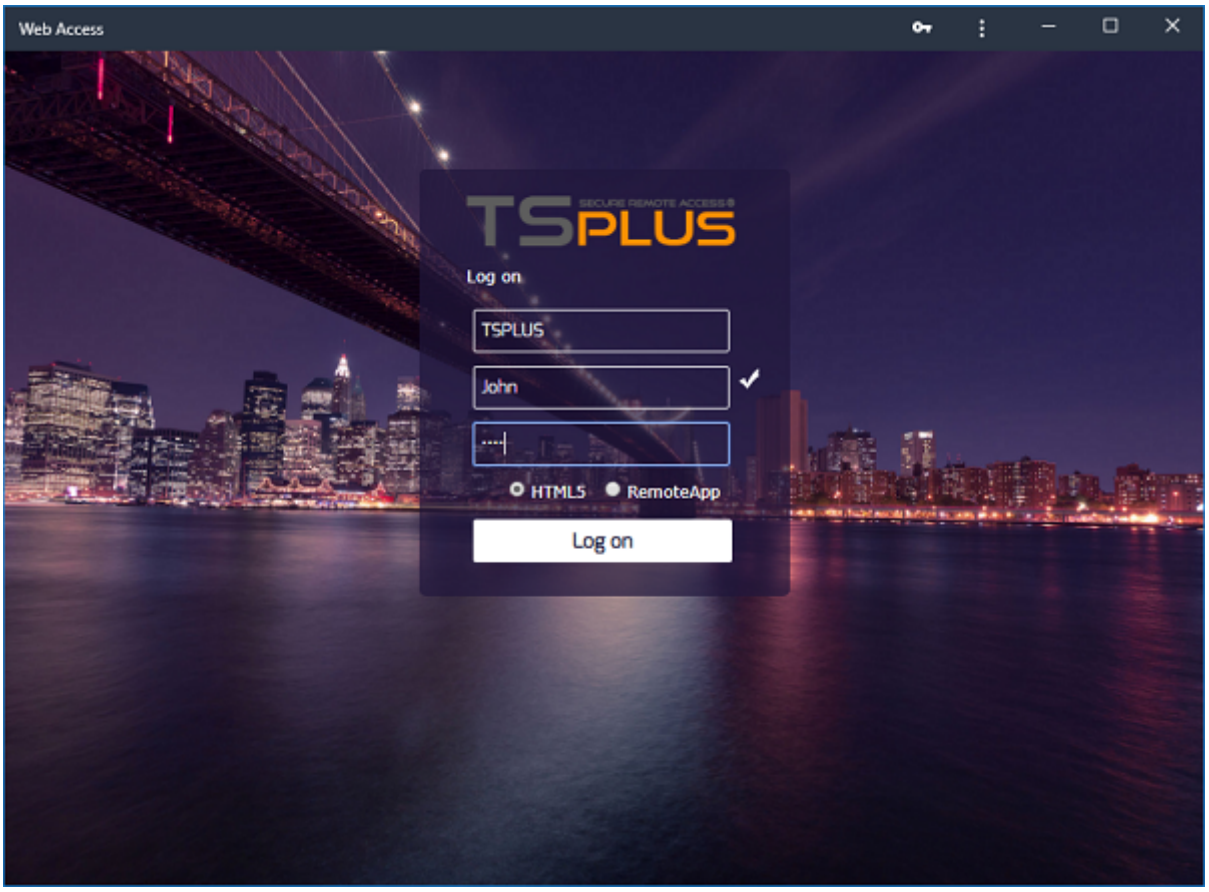
Click on the + button located on the right side of the navigation bar. When prompted, click on ‘Install’.



The installation only takes a second. It will create an icon on your desktop:



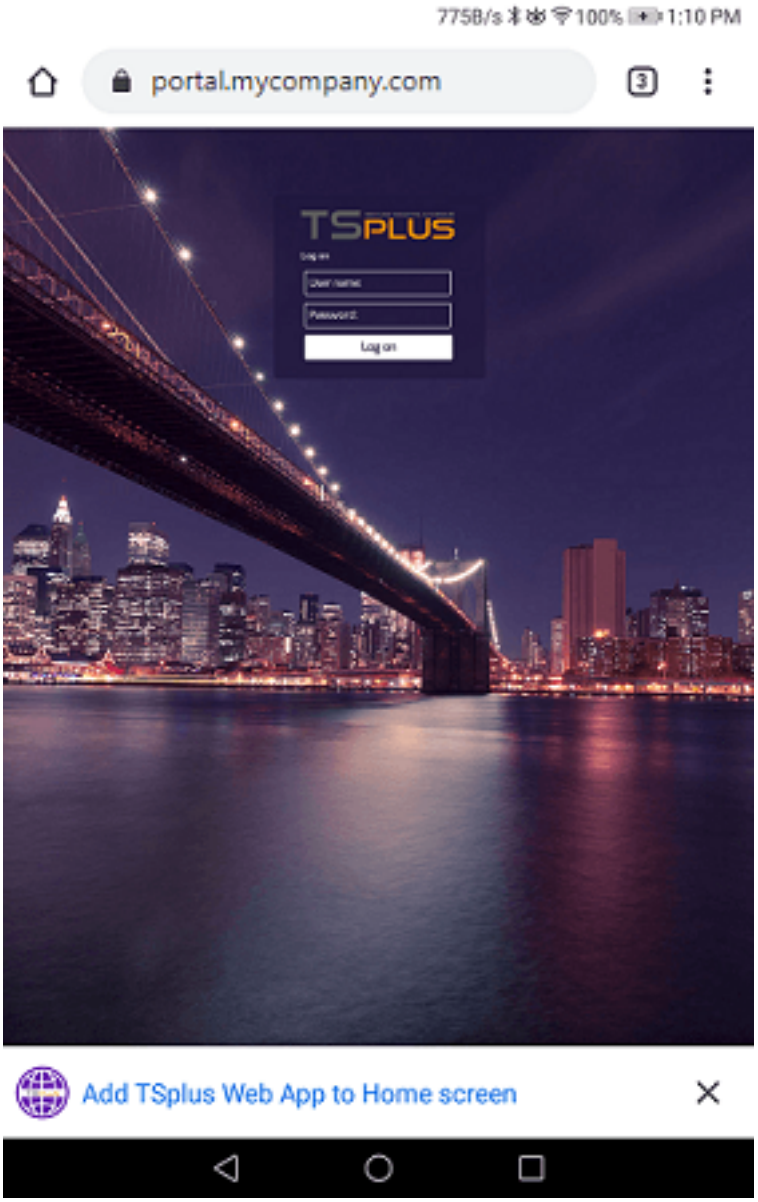
And the web app will open immediately upon completion:



Installation - Android Mobile Device

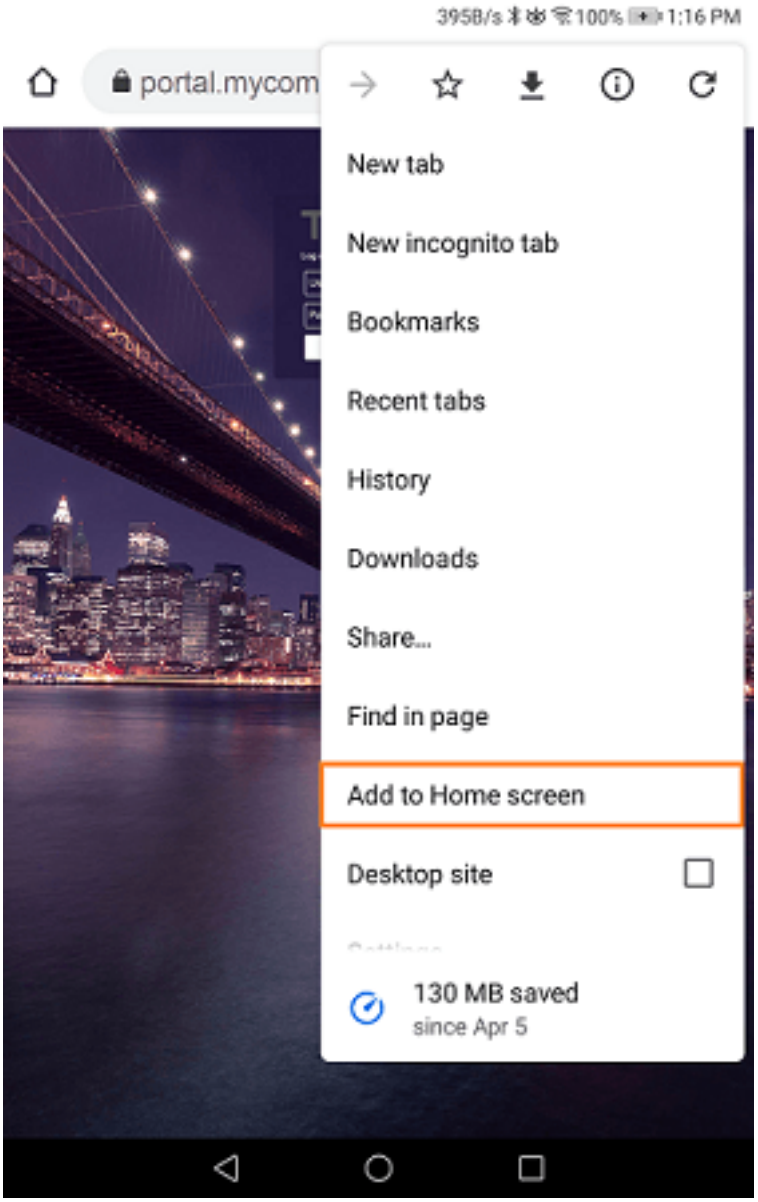
Navigate to your corporate TSplus Web Portal using your preferred common mobile web browser. **HTTPS protocol is required on the TSplus server.**

The Web Portal will offer the option to add the TSplus Web App to your home screen, by clicking on the “Add TSplus Web App to Home Screen” message at the bottom of the window:

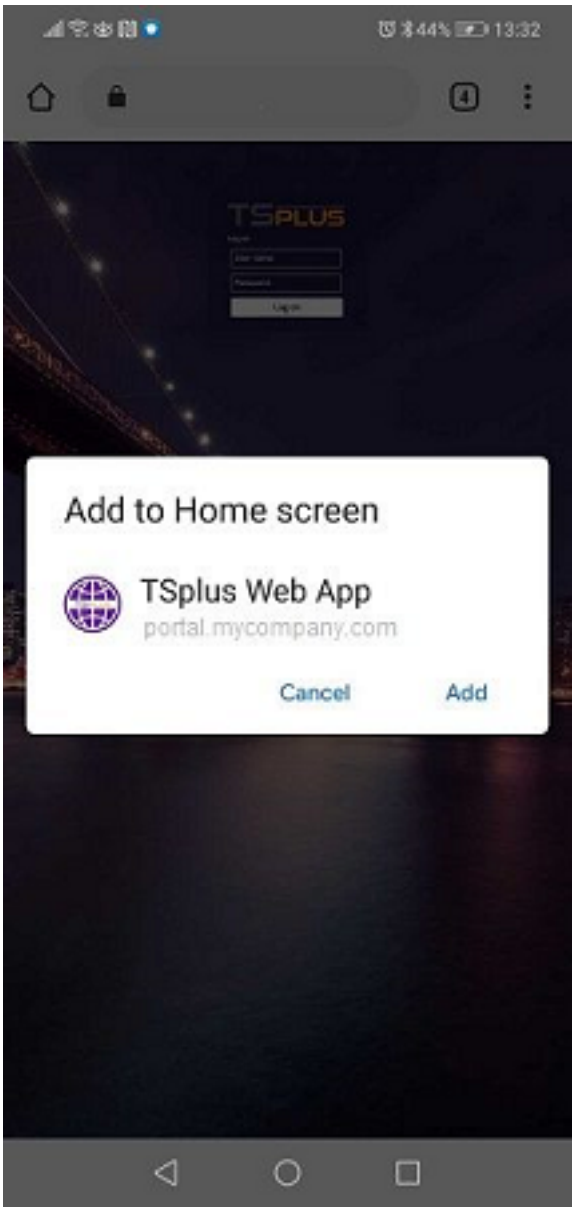


Or by clicking on the 3 dots menu on the top right of the window and clicking on “Add

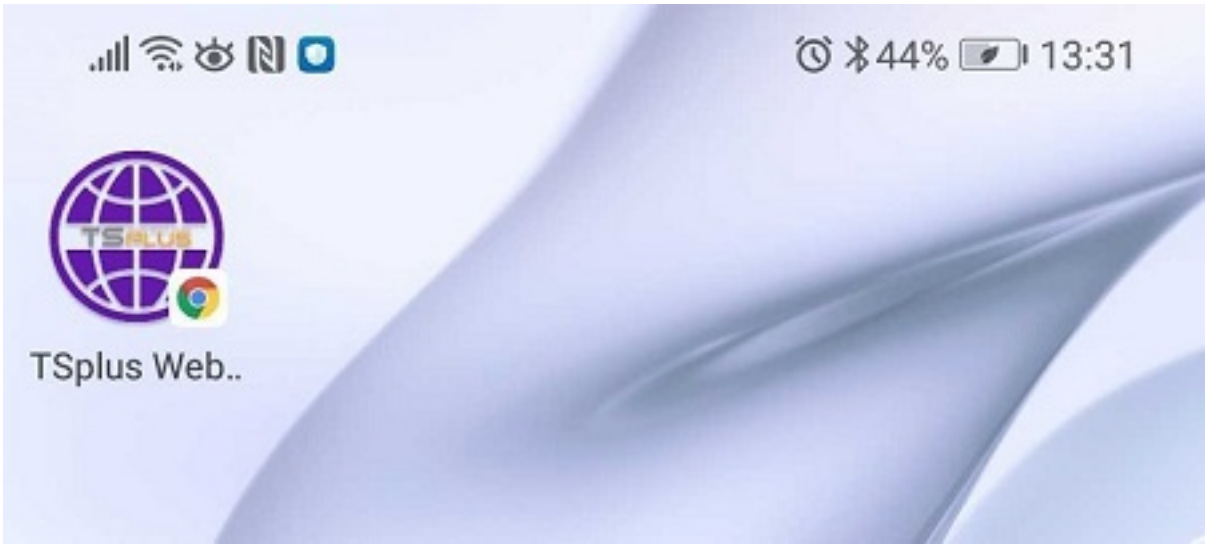
After accepting the Add to Homescreen option, the user will see the following screen:



Tap on the ‘Add’ button and the process is complete:



The TSplus Web App will now be accessible directly from the home screen of your mobile device.



Installation - Apple iOS Mobiles

The Web App installation process on iOS is similar to the Android process. Just navigate to the TSplus Web Portal using Safari Web Browser. Click on the Share button:

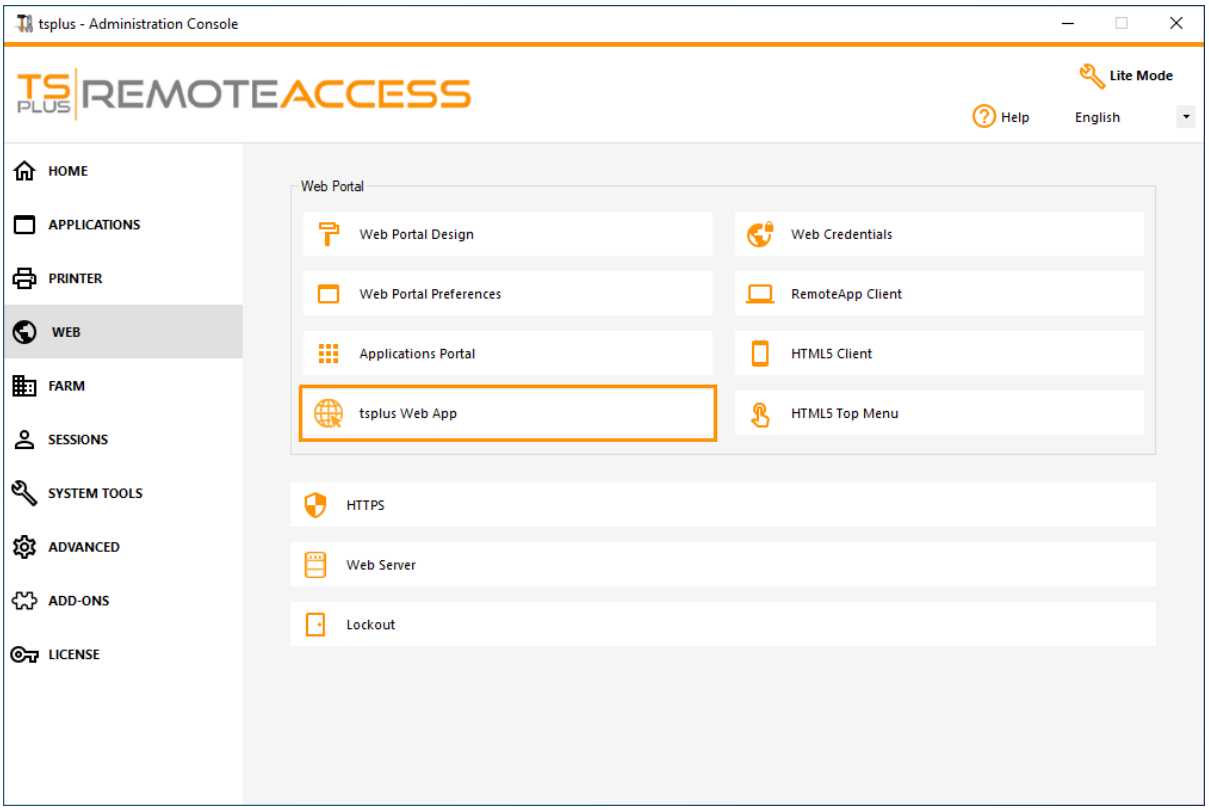


Then click on “Add to Homescreen”.

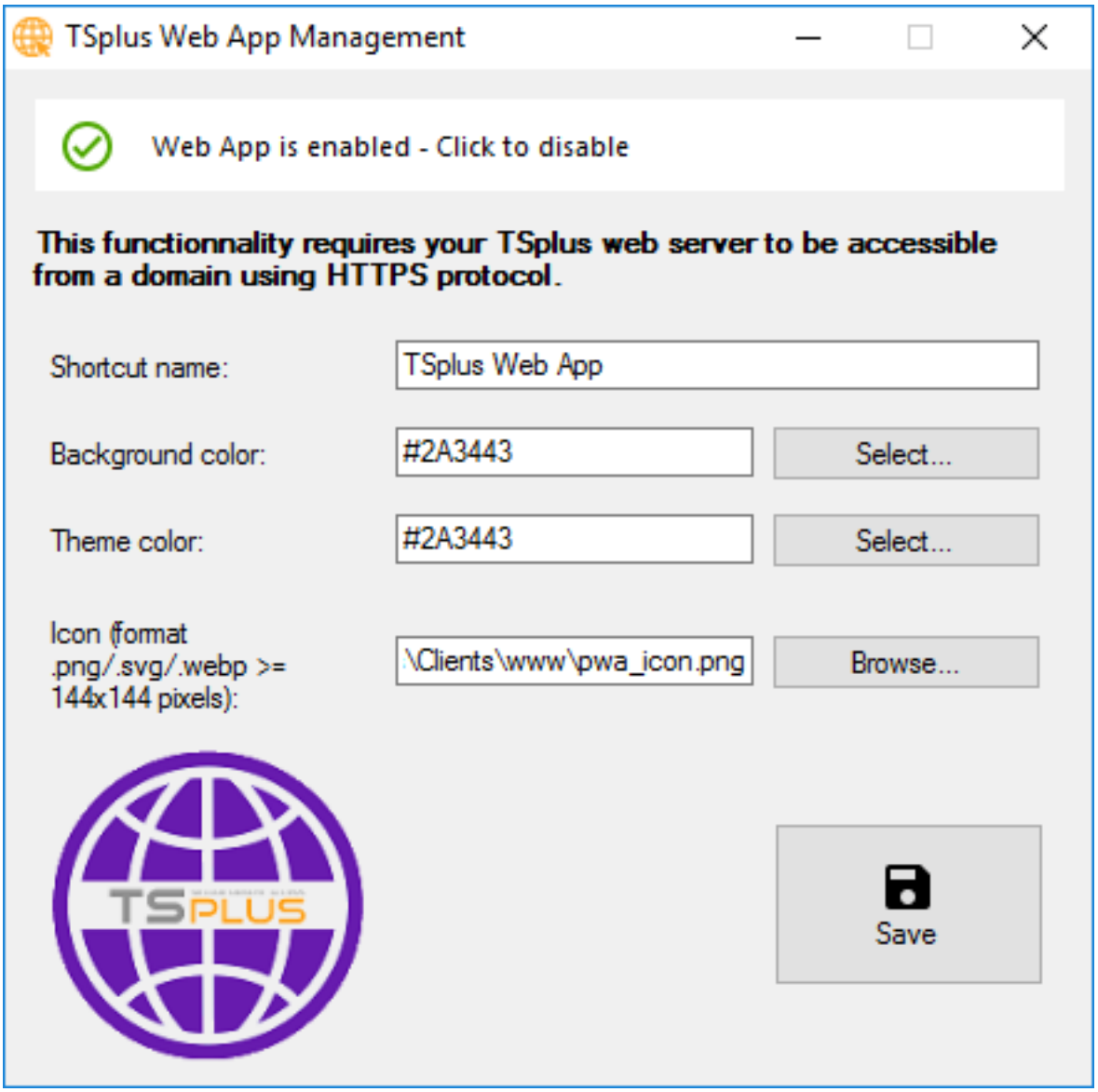
Note: Chrome browser doesn’t support the Web App feature on iOS.

Management

You can manage the Web App, by going to the TSplus Admin Tool Web - Web Portal section and clicking on TSplus Web App tile:



The Web App is enabled by default, but you can disable it. It is possible to modify the Shortcut name, background and theme colors as well as the icon of TSplus Web App:



Just click on “Save” to record your modifications.

Web Applications Portal: Parameters in URL address

If you want to bypass Terminal Service Plus standard logon Web Access page when using the Web Applications Portal and go directly to the Web Applications Portal page, you must specify several parameters in the URL address:

- user login
- user password
- user domain
- server
- port
- client type (HTML5 or Windows)

Here is an example of a full URL address for user “demo” with password “demo” on our demo server with an HTML5 client:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo&domain=&server=127.0.0.1&port=3389&type=html5

The domain, server, port and type parameters being optional, the following URL address has exactly the same behavior:

https://demo.tsplus.net/index_applications.html?user=demo&pwd=demo

To use a Windows client, use:

&type=remoteaccess

Using those parameters in the URL address, you can go directly to the Web Applications Portal page.

You do not have to specify all these parameters at the same time: the parameters not specified will have their default configured value.

If you wish to bypass Terminal Service Plus standard logon when using theconnect with the HTML5 client, check this page.

Web Applications Portal

Terminal Service Plus Web Application Portal provides a single, flexible solution that can streamline application and desktop deployment and life-cycle management to reduce IT costs. By centrally managing and web delivering on-demand applications, IT can improve the success rate of application deployment providing role-based management, application control, security and users support.

Terminal Service Plus Web Application Portal virtualizes and transforms Windows apps and desktops into a secure on-demand service.

With Web Application Portal, you will be able to publish Microsoft Windows applications (business applications, Office applications…) to the web.

As in Citrix, your users can access their applications directly from the Internet, simply by clicking on the application icon in the Portal web page, directly inside their own Internet browser.

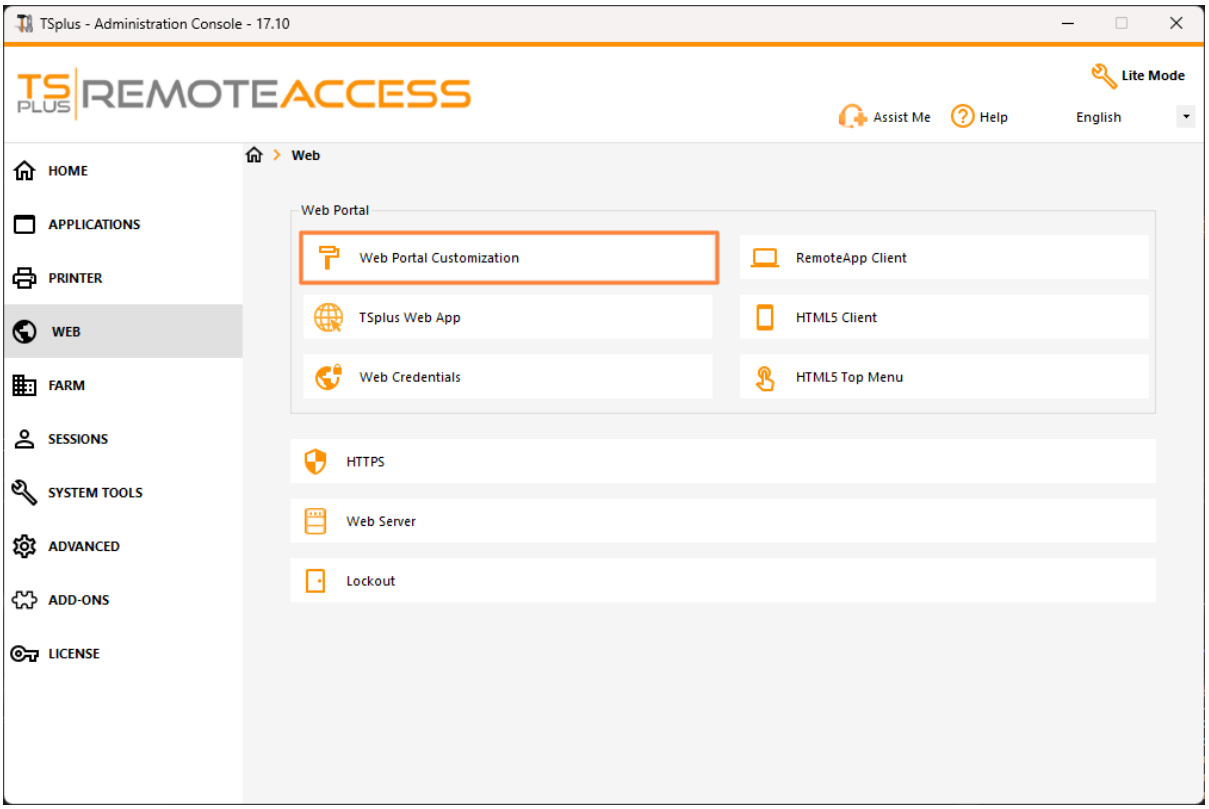
Managing your Web Applications

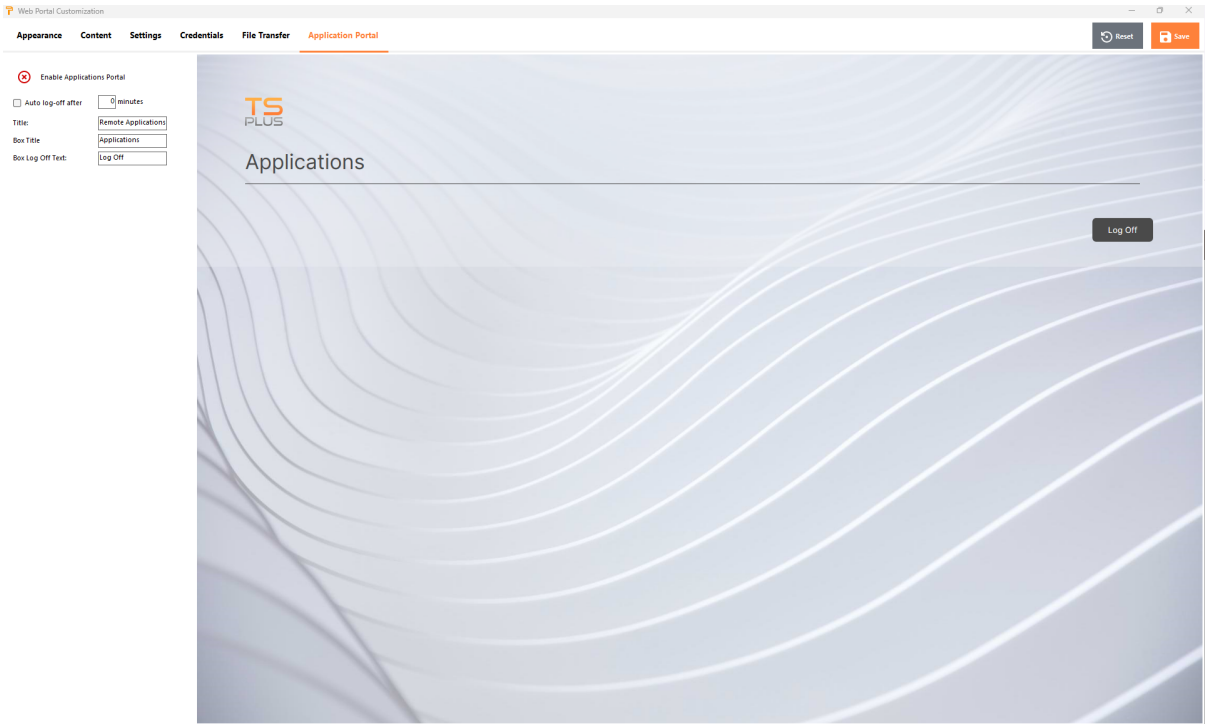
The Web Application Portal feature is **fully integrated** in Terminal Service Plus. It means that all the applications published by Terminal Service Plus Applications Publishing feature can be used in the Web Applications Portal.

If you would like to know more about this publication process, feel free to read our documentation about Application Publishing and Assigning Applications to Users or Groups.

Designing your Web Applications Portal

In the Admin Tool, open the “Web” tab and click on the “Web Portal Customization” tile and go to the “Application Portal” tile.





To generate a web access page with the Web Applications Portal feature activated, **check the “Enable Applications Portal” checkbox.** You can customize your web access page to your liking, then click on “Save” to publish this new web access page.

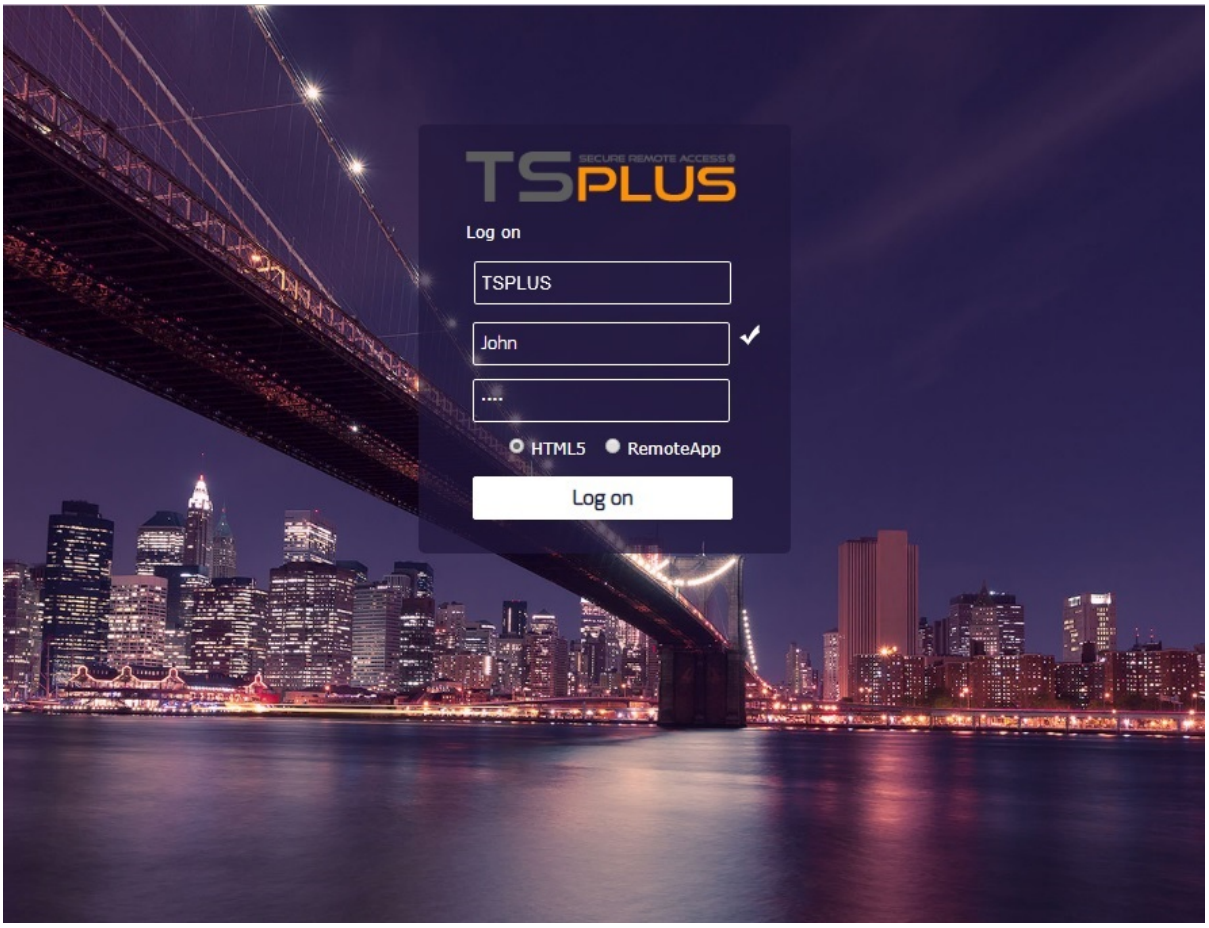
Note: You can change the box and the box border colors only for the Classic themes which can be changed on the Appearance tab.

Using the Web Applications Portal

On this example we have published the new web access page with the default name “index”.

To access it, open a web browser and go to http://your_server_name/ (in this example we use http://localhost , directly from the server itself).

The first web page displayed is the standard Terminal Service Plus web logon page:

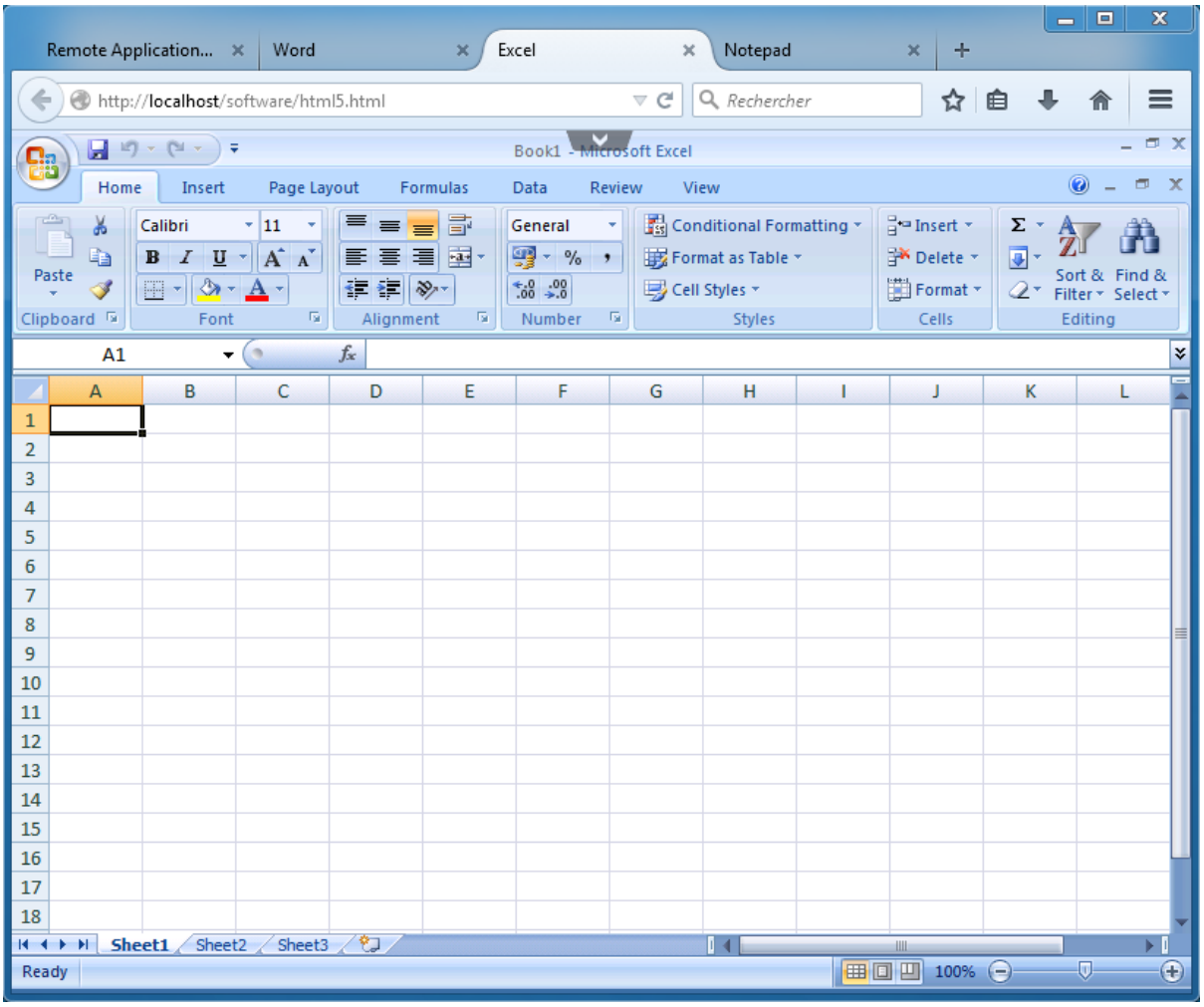


Once logged in, a new web page is displayed, this is the Web Applications Portal:

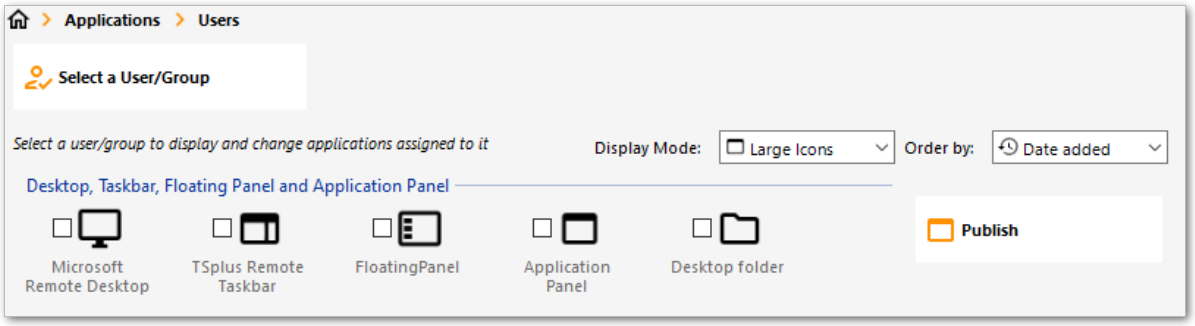


As you can see, the user gets an icon for every published application that he has access to.

The user can now click on one or more icon, in order to remotely open the matching application in a new tab:

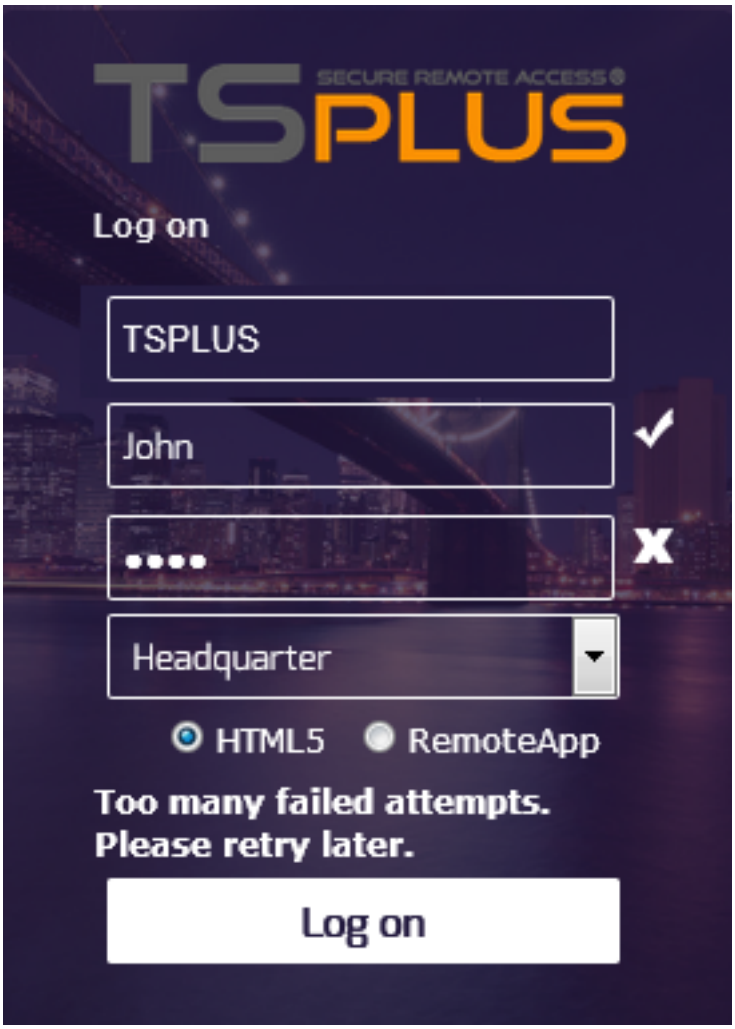


If you want to use only the application portal without opening a windows session, remote taskbar, floatingpanel,…, you must uncheck all the boxes associated with the user profile.



Since TSplus 11.40 release, brute-force attacks on the Web Portal are now blocked when users enter wrong credentials.

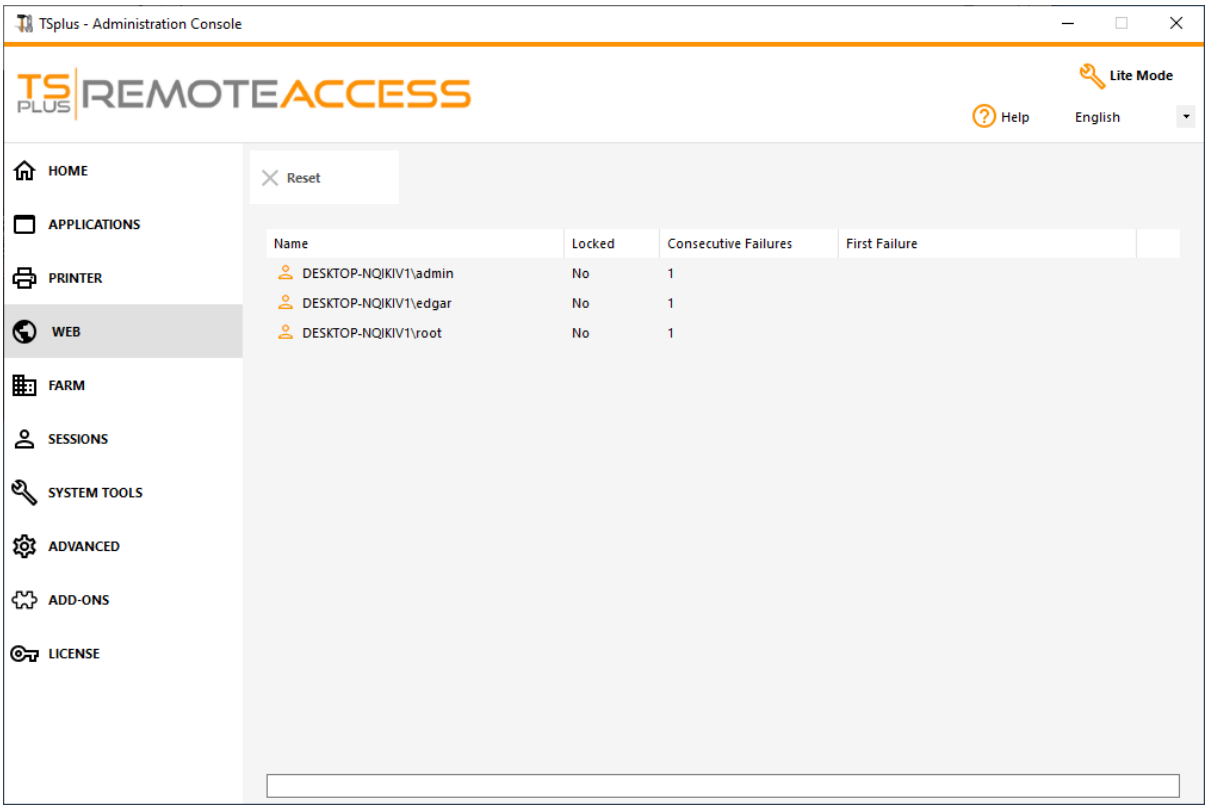
After 10 attempts during a period of 15 minutes, the Web Portal will prohibit the user to logon for 30 minutes (customizable on the Advanced - Lockout tab of the AdminTool) :



These are the default settings which are customizable on the hb.exe.config file located on the TSplus folder:

TSplus\Clients\www\cgi-bin\hb.exe.config in the “appSettings” paragraph.

You can check all blocked connections and logs by users on the Lockout feature of TSplus:



This functionality is visible and active after the first Web Portal connection.

Important Notes

- The Web Applications Portal feature is compatible with Farm / Gateway configuration and it also supports load-balancing.
- In a Farm / Gateway configuration, the Applications must be published and assigned on every server of the farm at the moment.
- In terms of Terminal Service Plus licensing, a user can open several applications at the same time without counting for more than 1 user.

Web Autologon: connect from web without portal

Overview

Terminal Service Plus Web Portal allows users to connect to their remote servers from any web browser simply by using their Windows credentials.

Sometimes however, you want to connect automatically when you launch a given URL address. This feature is called Web Autologon.

With Web Autologon, you will connect using the settings (login, password, ports, …) specified in specific Terminal Service Plus files.

Caution

When using this feature, your username and password may be exposed to anyone visiting the page.

Additionally, if all of your users share the same username, it may be possible for users to see sensitive information from other users sharing the same username.

This feature is intended for specific use cases only and is not recommended.

Web Autologon using HTML5 client

You will be able to connect directly by browsing to http://your-server/software/html5.html

You can modify the connection settings by editing the following file with Notepad or any text editor (such as Notepad++ - do not use MS Word):

C:\Program Files (x86)\TSplus\Clients\www\software\html5\settings.js

You will need to specify at least a login and a password in order to benefit from Web Autologon.

You might need to refresh the page on your web browser after modifying this file.

Web Autologon using the RemoteApp Web Client

You will be able to connect directly by browsing to http://your-server/software/remoteapp2.html

You can modify the connection settings by editing the following file with Notepad or any text editor (such as Notepad++ - do not use MS Word):

C:\Program Files (x86)\TSplus\Clients\www\software\remoteapp2.js

You will need to specify at least a login and a password in order to benefit from Web Autologon.

You might need to refresh the page on your web browser after modifying this file.

Enable multiple user sessions using the same credentials

If you want to enable multiple user sessions using the same credentials, then you can follow this procedure.

You can copy the index.html file located in:

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

as many times as your number of users. You can rename it and then access it with the url: http://nameofyourserver.com/renamedindex.html

Edit the paragraph corresponding to users credentials:

Access Configuration ---------- var user = ""; // Login to use when connecting to the remote server (leave "" to use the login typed in this page) var pass = ""; // Password to use when connecting to the remote server (leave "" to use the password typed in this page) var domain = "";

You can copy the index.html file as much time as you want, renaming it with the username will make it easier for you to provide a personal link.

Web Credentials

Overview

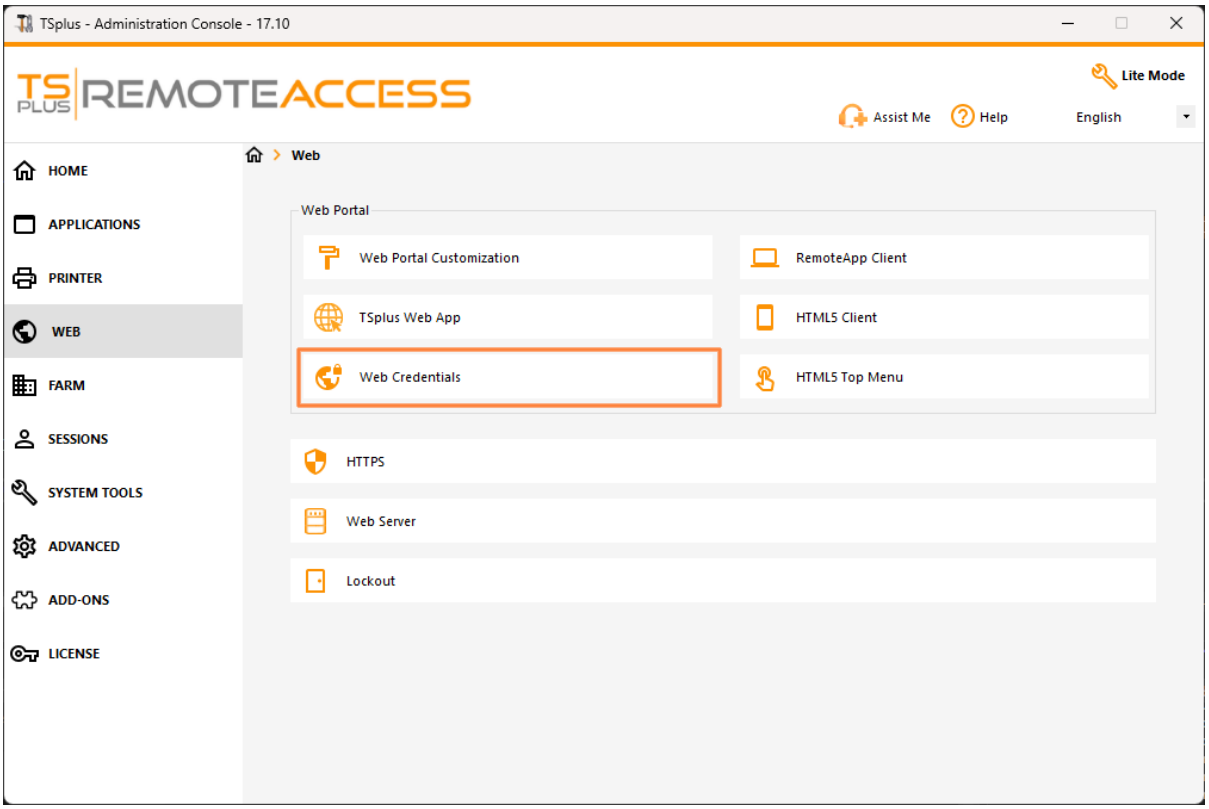
Terminal Service Plus Web Credentials is a state-of-the-art unique feature, which allows users to connect with just an e-mail address or a pin-code.

With Web Credentials, you can secure your server's access with the e-mail address of a user, or with a simple pin-code generated by your business application. One of the great benefits of this feature is that these credentials (e-mail or pin-code) are pure web credentials : the user will not know the Windows user account he is currently using, and he does not need to know a real Windows login/password to connect to his application!

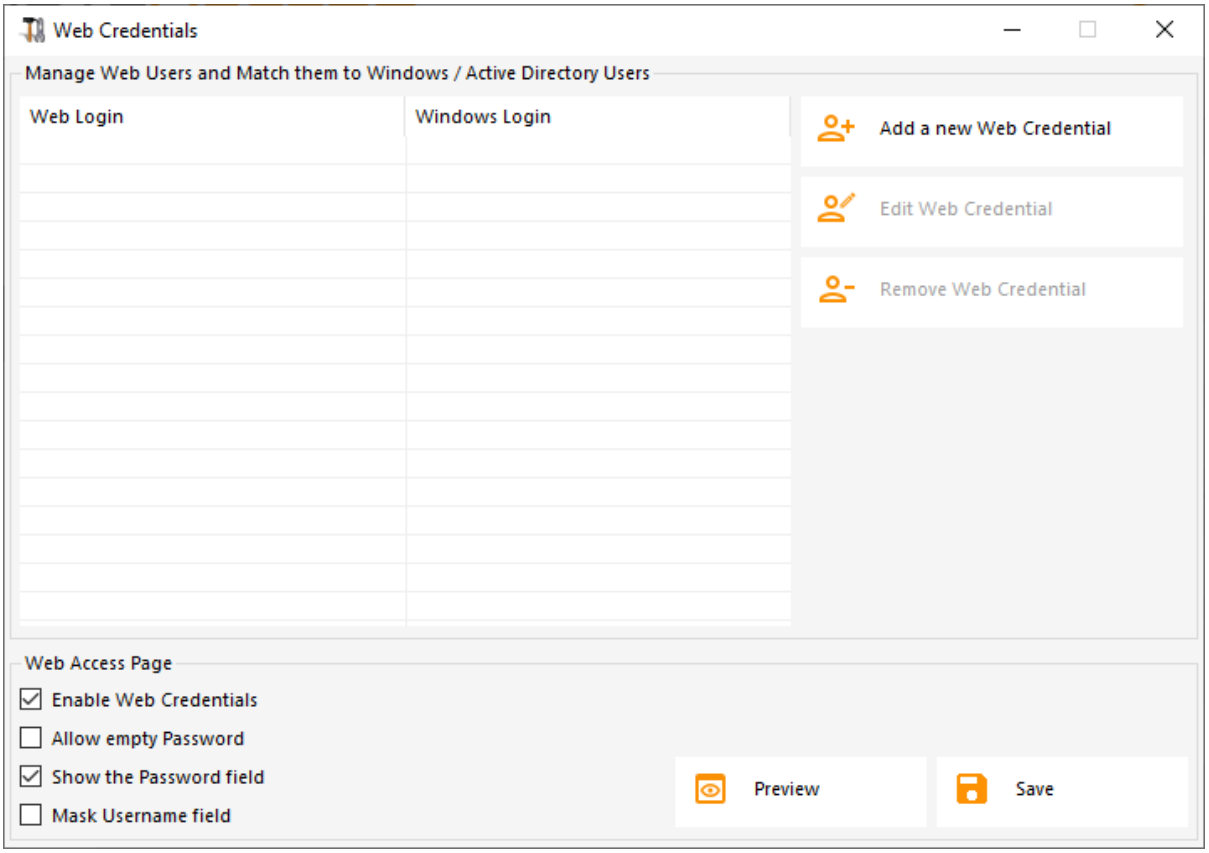
With Web Credentials, you will be able to define custom pure web credentials and match them to any existing Windows / Active Directory user account. The user will then be able to connect using these custom credentials, instead of the Windows / Active Directory ones.

Managing your Web Credentials

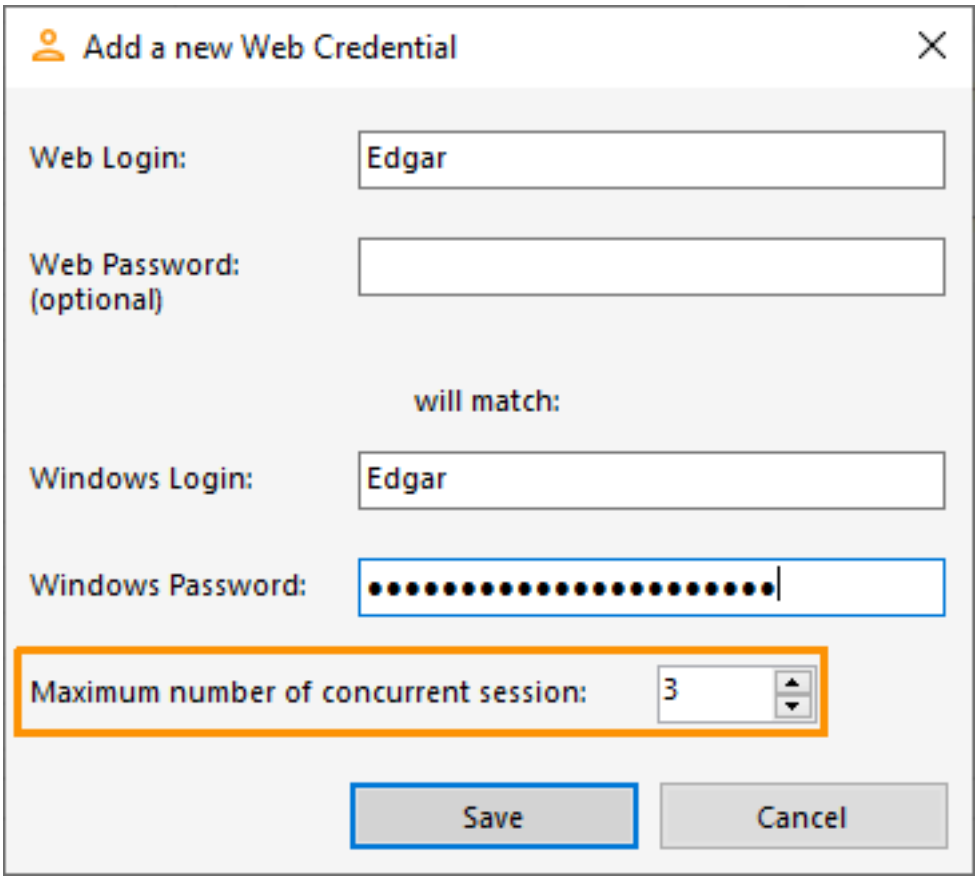
In the Admin Tool, open the "Web" tab and click on the "Web Credentials" tile.



The Web Credentials Manager will open and display this window:



You can now create a new Web Credential by matching a custom login and (optional) password with an existing Windows / Active Directory user account, as shown below:



Since TSplus 9.50 version, you can also decide the maximum number of concurrent sessions for a user.

You can also edit and remove an existing Web Credential, thus changing or disabling any custom credentials you configured.

Alternatively, you can create web credentials via a command line:

- On the Windows Start Menu, on the execute field, type in: 'cmd.exe' (or in Programs/ Accessories > 'Windows Power Shell')
- Then, in order to go to the right folder, type: cd "C:\Program Files (x86)\TSplus\UserDesktop\files", then press Enter to validate
- To add a new Web Credential, type: AdminTool.exe /webcredentials-add your_web_login your_web_password your_windows_login your_windows_password maximum_concurrent_sessions
- To add a blank credential, type two double quotes: "" to indicate a blank text.
- To delete a web credential, type: AdminTool.exe /webcredentials-remove your_web_login

(if you like using command lines and are wondering what other command lines are available, please go to this specific documentation)

Important Notes

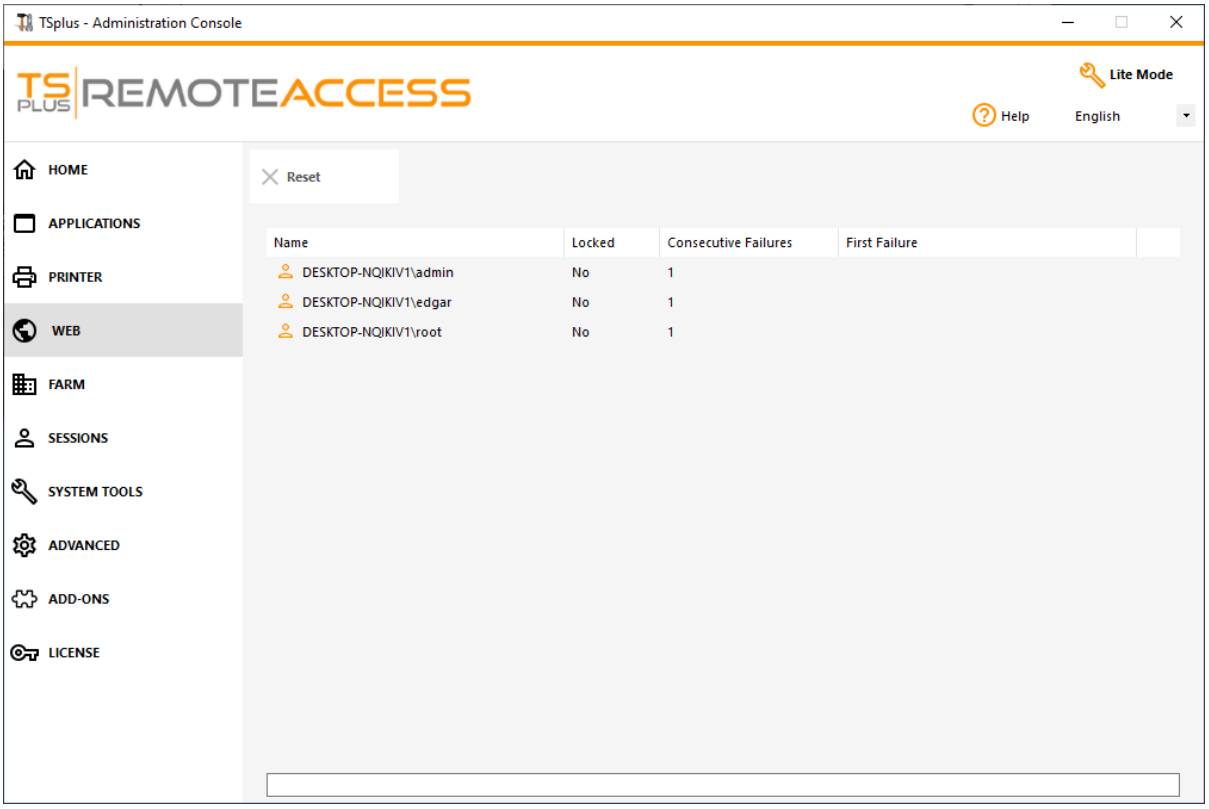
Please note the following limitations:

- ’[’, ’]’ and ’°’ characters are not supported on the password fields.
- In a Farm / Gateway configuration, Web Credentials only support the load-balancing mode (it does not work with server-assigned mode).
- In a Farm / Gateway configuration with load-balancing mode, the Web Credentials must be defined on every server of the farm at the moment.
- 2FA is not compatible with the Web Credentials feature.

Web Lockout

TSplus Web lockout, introduced with Version 12.40, is a user interface for the Web Portal Lockout feature, to unblock accounts and edit advanced settings:

FAQ: about how to configure the HTML5 Web Portal lockout feature

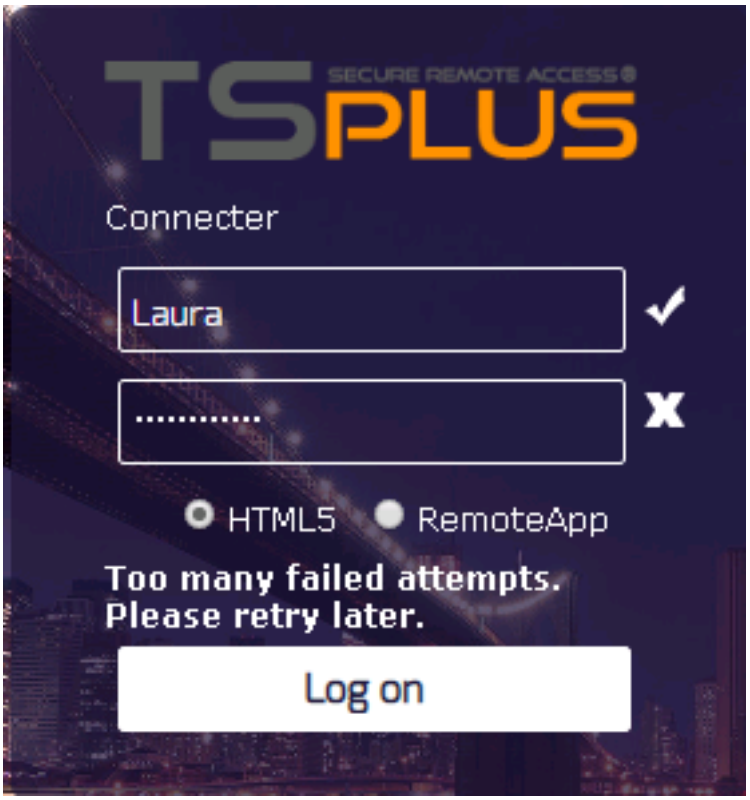


Lockout monitors failed Web Login attempts on your TSplus server. It logs attempts and automatically blocks the corresponding user after the authorized number of failed attempts has been reached.

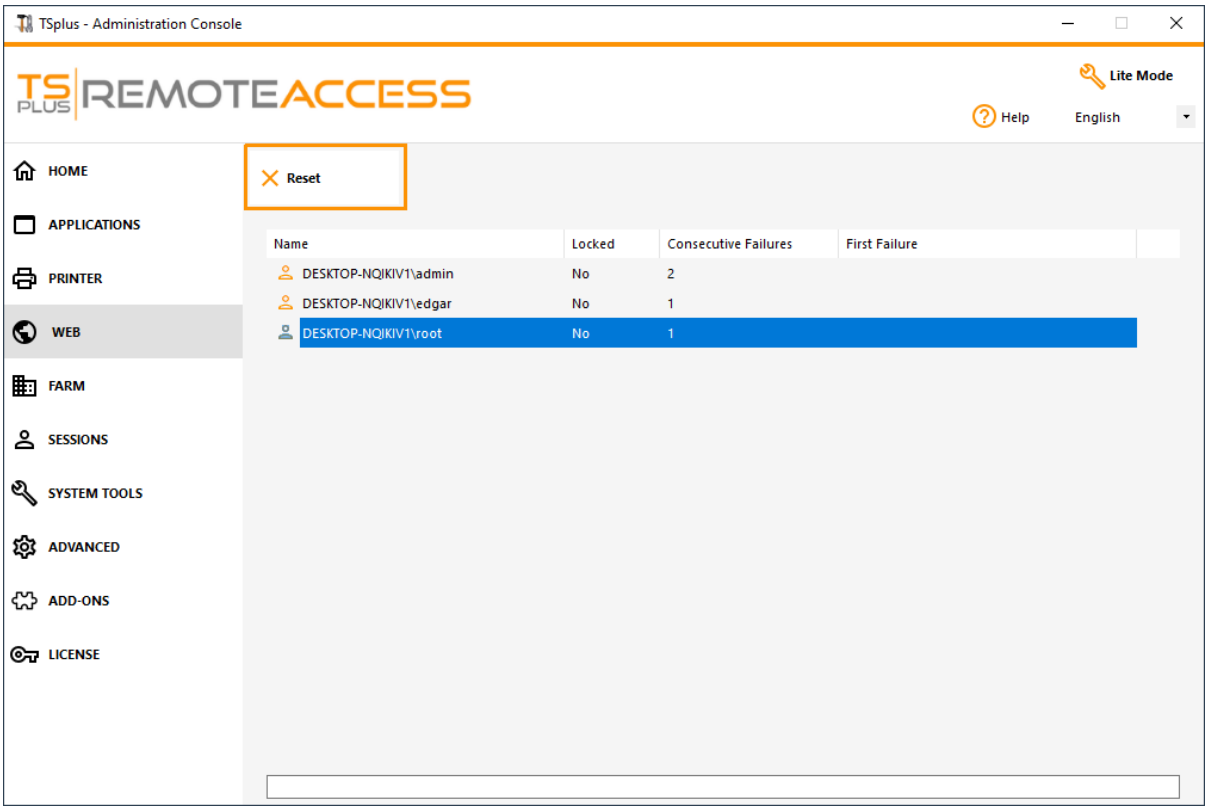
You will easily see if an Address has been locked under the “Locked” column.

The next column indicates the numbers of consecutive failures for each user.

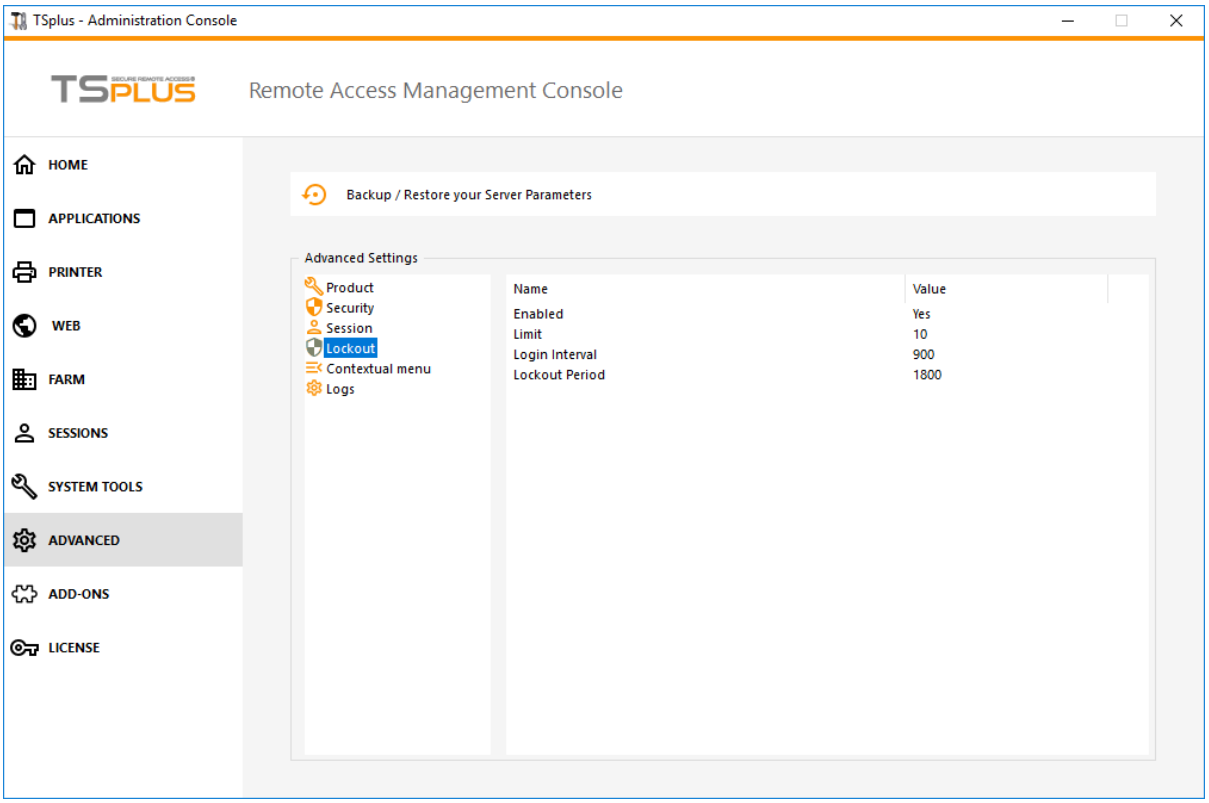
On the Web Portal, a message indicates the user that too many failed attempts were made:



Users can be quickly removed from this list, unblocked and whitelisted from the easy-to-use management console in the Web Tab of the AdminTool. Just click on the user you want to reset or unblock and then click on “Reset”.



The threshold for users blocking can be configured by the administrator, on the Advanced Settings Tab of the AdminTool:



Check the Documentation to configure Lockout Settings.

TSplus Advanced Security Integration with Lockout

If a failed login attempt has been detected on the Web Portal, TSplus Advanced Security will indicate the **“Lockout Event”, corresponding to a username on the Security Event Viewer**:



“A failed login attempt was detected from Web Portal for user … 1 Failed login attempt were detected for this user since…”

TSplus Advanced Security BruteForce Protection

TSplus Advanced Security Bruteforce Protection covers the **Client I.P. addresses aspect**. Hence, it also works for RDP connections.

Failed Brute-Force connections attempts, are also visible on TSplus Advanced Security Event Log (private IP addresses are excluded to avoid blocking proxy):



“A failed connection attempt was detected from IP address … . This IP address is not whitelisted and will be blocked following several failed attempts to connect. Provided username: Harry.”

For More information about Lockout and BruteForce Protection, check this documentation and

the Bruteforce Protection documentation

Web logon page: How to change the logon Splashscreen

Overview

When the remote connection is loading, the HTML5 client is displaying a default splashscreen such as the screenshot below:



You can customize this content by modifying a JavaScript configuration file.

HTML5 Client

Creating your customized Splashscreen content

Any content in text or HTML can be used for the Splashscreen.

Also, if you need to use simple quotes (’) or double quotes (”) you will have to write a backslash before (’ and ”) instead of just the quotes.

Finally, please note that the content must be written in only 1 line.

The following example is a valid content for the Splashscreen:

This is my customized splashscreen

Please say “hello”!

It will display a title (“This is my customized splashscreen”), a text (“Please say hello!”) and the animated ring picture as in the standard TSplus Splashscreen.

Modifying the Splashscreen data to use your own content

If you do not have a file named “settings.js” in the “C:\Program Files (x86)\TSplus\Clients\www\software\html5” folder, then your TSplus version is older and this documentation does not apply. Please update your system first or contact support.

Edit the file “settings.js” located in the “C:\Program Files (x86)\TSplus\Clients\www\software\html5” folder. We advise you to use a text editor such as Notepad or Notepad++ (do not use Word).

Search for the line starting by this:

W.splashscreencontent = ”

Replace it completely by the following line:

W.splashscreencontent = “your customized content here”;

Do not forget the ending double quotes and semi-colon (”;).

If you wish to lengthen the duration of the logon splashscreen in HTML5, you can do so by modifying the value in milliseconds:

W.splashscreentime = 5000; //splash screen play time.

We recommend you clear your browser’s cache after saving the changed html page.

Web logon page: How to close the Logon form after logon

Overview

On the Web logon page, when the user clicks on the “Log on” button, the chosen client (HTML5 or Windows) is opened in a new browser’s tab.

Sometimes, and more specifically when using the Windows client, you might want to hide the logon form to the user, for instance in order to avoid the user to click again on the “Log-on” button.

Depending on the Internet browser used, you have two choices on how to change this default behavior. Both solutions requires you to modify a JavaScript file.

Solution A: Closing the Logon tab - For Internet Explorer only

In this solution, when the user clicks on the “Log on” button, the chosen client will be opened in a new browser’s tab and the Logon tab will close itself. Depending on the Internet Explorer version, a small message window might be displayed to the user, asking him to confirm that he wants to close this tab.

Edit the file “common.js” file which is stored into the “C:\Program Files (x86)\TSplus\Clients\www\software” folder. We advise you to use a text editor such as Notepad or Notepad++ (do not use Word).

Search for these lines:

```
 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);
 }
```

And replace them by those lines:

```
 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();
```

We recommend you clear your browser's cache after saving the changed JavaScript file.

Solution B: Redirecting the Logon tab to another web page - For all browsers

In this solution, when the user clicks on the "Log on" button, the chosen client will be opened in a new browser's tab and the Logon tab will automatically navigate to another web page.

You are free to use any existing Internet address (URL) such as "http://google.com" or "http://your_intranet/your/page.html", or you can create your own web page by using "thankyou.html" as the URL and creating a file named "thankyou.html" in the "C:\Program Files (x86)\TSplus\Clients\www" folder and putting HTML content in it.

Edit the file "common.js" file which is stored into the "C:\Program Files (x86)\TSplus\Clients\www\software" folder. We advise you to use a text editor such as Notepad or Notepad++ (do not use Word).

Search for these lines:

```
 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);
 }
```

And replace them by those lines:

```
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";
```

We recommend you clear your browser’s cache after saving the changed JavaScript file.

Web logon page: How to open the HTML5 client in the same tab

Overview

On the Web logon page, when the user clicks on the “Log on” button, the HTML5 client is opened in a new browser’s tab.

You can change this behavior and have the HTML5 client to open in the same browser tab as the Web logon page by modifying a JavaScript file.

Modifying the custom.js file

Edit the file “custom.js” file which is stored into the “C:\Program Files (x86)\TSplus\Clients\www” folder. We advise you to use a text editor such as Notepad or Notepad++ (do not use Word).

Add this line:

var openinsamewindow = true;

We recommend you clear your browser’s cache after saving the changed JavaScript file.

Modifying the common_applications.js file

If you are using Terminal Service Plus Web Applications Portal feature, then you need to edit a second file. Edit the file “common_applications.js” file which is stored into the “C:\Program Files (x86)\TSplus\Clients\www\software” folder. We advise you to use a text editor such as Notepad or Notepad++ (do not use Word).

Search for these lines:

```
if (childurl != '') {
  window.name = childname;
  location.href = childurl + '#';
}
```

And replace them by those lines:

```
  if (childurl != '') {
    window.name = childname;
    location.href = childurl + '#';
  }
```

We recommend you clear your browser’s cache after saving the changed JavaScript file.

Web Portal with SSO (beta)

Key prerequisites and limitations

Web Portal 2026 with SSO is designed for the **Creative** theme and uses all customizations from AdminTool > Web > Web Portal Customization. If the selected theme is not **Creative**, the Web Portal does not display.

When enabled in a farm, all servers must run the **same Remote Access version** and be enabled for **Web Portal 2026 with SSO**

This feature is **Beta** and should **not** be deployed on production servers.

Why a new Web Portal?

Compared with the previous Web Portal, this implementation provides higher reliability and better performance under load. Plus, it allows:

- **Advanced SSO capabilities**
  - Windows Integrated Authentication (Negotiate / Kerberos / NTLM)
  - Third-party identity provider integration (currently SAML)
- **Stronger security controls**
  - Built-in anti-forgery protections
  - Endpoint rate limiting
  - Modern authentication and cookie/session controls

Its architecture will allow us to easily address any potential security audit feedback.

It is also a **more accessible product** through recommendations and improved contrast.

Web server flexibility (Kestrel by default)

The application is not tied to one front-end web server. By default, it runs on **Kestrel** (HTTP port 81). It can be fronted by **IIS** or **Apache** as a reverse proxy by changing web server configuration.

Example: Apache reverse proxy to Web Portal service

```
# Apache VirtualHost example
ProxyPreserveHost On
ProxyPass        /  http://127.0.0.1:81/
ProxyPassReverse /  http://127.0.0.1:81/

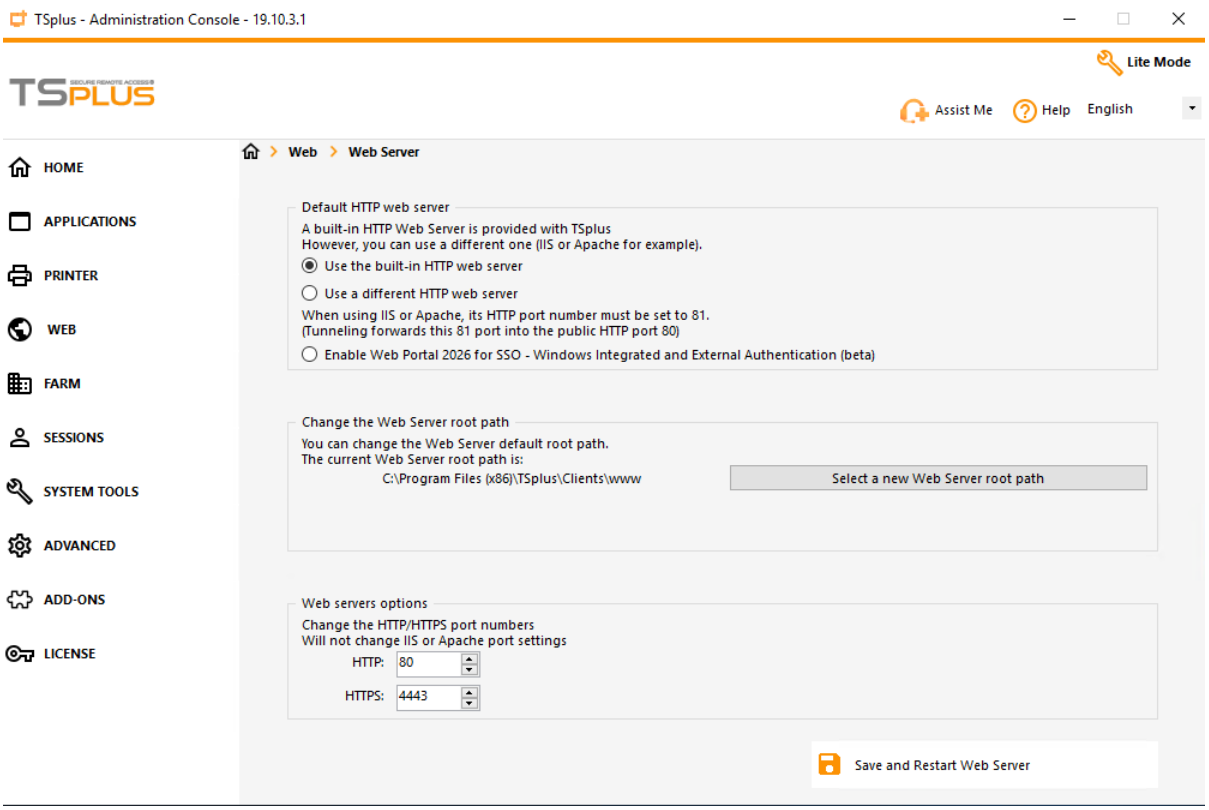
RequestHeader set X-Forwarded-Proto "https"
RequestHeader set X-Forwarded-For "%{REMOTE_ADDR}s"
```

This keeps Web Portal logic unchanged while Apache handles public HTTP/HTTPS exposure.

Please contact the development team if interested as this scenario is not yet accessible from AdminTool program and must be configured manually.

Enable Web Portal 2026 with SSO

1. Open **AdminTool**
2. Go to: Web > Web server
3. Enable: **Web portal 2026 with SSO**



Important: this option is Beta. Use only in test environments.

Supported sign-in modes

Web Portal 2026 with SSO supports:

- Traditional login form using Windows credentials
- Web credentials. See: https://docs.tsplus.net/tsplus/web-credentials/
- Windows Integrated Authentication (automatic in trusted / local scenarios)
- External identity provider via **SAML**, such as Entra ID (formerly Azure AD) or Okta

Note: Support for external authentification via **OIDC** planned later, on request

2FA behavior

2FA is applied to standard account flows, including:

- Login form using Windows credentials
- Web credentials
- Windows Integrated Authentication

External authentication providers often enforce their own MFA / 2FA. So 2FA configuration set in Remote Access 2FA addon does not apply to this scenario.

Local-network bypass is available through CustomSettings:TwoFaBypassForLocalNetwork parameter located in file: C:\Program Files (x86)\TSplus\Clients\webportal\appsettings.json, where C:\Program Files (x86)\TSplus is TSplus Remote Access setup folder. When enabled, bypass occurs only if client and gateway are in the same private subnet.

Configure Windows authentication flow

For users signing in with Windows authentication, one of the following is required:

1. Pre-register credentials with the TSplus command: AdminTool.exe /windowscredential-addorupdate. See documentation at https://docs.tsplus.net/tsplus/commands-list/#add-or-update-credentials-to-the-windows-credentials-manager-windowscredential-addorupdate
2. Or let the user sign in once through the Web Portal login form with Windows credentials.

For configuring Windows Integrated authentication, please see: Enable Windows Integrated Authentication on an Active Directory Domain. As this authentication mode is arduous to configure, customers often favor setting up an external identify provider.

Configure external authentication (SAML)

Required settings for the external application

The external application must be configured as follow:

- Single Sign-On URL must be set to the Web Portal SAML consumer service endpoint, e.g. https://mywebportal.company.com/Saml/acs
- Audience URI (SP ENtity ID) must be set to the Web Portal domain name or IP address, e.g. https://mywebportal.company.com
- Name ID format must be set to **EmailAddress**
- Application username must be set to **Email**, as the left part will identify the Windows account username

Required settings in appsettings.json

The file appsettings.json is located in C:\Program Files (x86)\TSplus\Clients\webportal, where C:\Program Files (x86)\TSplus is TSplus Remote Access setup folder.

Edit the Saml2 section:

- IdPMetadata
- Issuer
- SingleSignOnDestination (optional if metadata provides it)
- SingleLogoutDestination (optional if metadata provides it)
- Certificate-related fields

For example, using the third-party identity provider 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#"
}
```

The issuer setting sets the audience URI, as defined on the external identity provider side.

if the SignatureValidationCertificateFile setting is set to a value other than **None**, then please make sure that the certificate is considered valid on the application server. This may require to add the certificate to the list of trusted certificate machine-wide.

Windows password availability for session launch

For external SAML authentication, launching sessions still requires usable Windows credentials. Use one of:

1. Register Windows credentials with command: AdminTool.exe /windowscredential-addorupdate. See documentation at https://docs.tsplus.net/tsplus/commands-list/#add-or-update-credentials-to-the-windows-credentials-manager-windowscredential-addorupdate
2. Or forward password from IdP claim by setting CustomSettings:UseSamlPasswordClaim to the claim type containing the Windows password.

Typically, the Web Portal will take the part before the '@' of the user email address as the Windows account's username.

Please note that external authentication works with local users at the moment.

If no password is available from claim or credential store, user validation fails.

Complete appsettings.json configuration file reference

The file appsettings.json is located in C:\Program Files (x86)\TSplus\Clients\webportal, where C:\Program Files (x86)\TSplus is TSplus Remote Access setup folder.

Logging

Parameter	Purpose	Possible values	Default
Logging:LogLevel:Default	Global minimum log level.	Trace, Debug, Information, Warning, Error, Critical, None	Information
Logging:LogLevel:Microsoft.AspNetCore	ASP.NET	Same as	Warning

	Core framework log level.	above	
Logging:LogLevel:Microsoft.AspNetCore.Authentication	Authentication subsystem log level.	Same as above	Warning

Global host setting

Parameter	Purpose	Possible values	Default
AllowedHosts	Host header filtering for ASP.NET Core host protection.	* (all) or semicolon-separated host list	*

IpRateLimiting

Parameter	Purpose	Possible values	Default
IpRateLimiting:EnableEndpointRateLimiting	Enables endpoint-specific throttling rules.	true / false	true
IpRateLimiting:StackBlockedRequests	If true, blocked requests continue increasing counters.	true / false	false
IpRateLimiting:HttpStatusCode	HTTP status returned when request is blocked.	Integer HTTP code (typically 429)	429
IpRateLimiting:RealIpHeader	Header used to resolve client IP behind proxy.	Header name	X-Forwarded-For
IpRateLimiting:ClientIdHeader	Optional client-id header for custom rate limiting.	Header name	X-ClientId

IpRateLimiting:GeneralRules

Each rule object has:

Parameter	Purpose	Possible values	Default in shipped file

Endpoint	Route/method pattern to protect.	Format VERB:/path	Multiple defaults (see below)
Period	Rate window.	e.g. 1s, 1m, 5m, 1h, 1d	5m (for all default rules)
Limit	Max requests in period.	Positive integer	5 (for all default rules)

Saml2

Parameter	Purpose	Possible values	Default
Saml2:IdPMetadata	IdP metadata URL used to load SAML provider configuration.	Valid HTTPS URL	""
Saml2:Issuer	SP entity ID (this Web Portal identity).	URI string	""
Saml2:SingleSignOnDestination	IdP SSO endpoint URL (can be auto-resolved from metadata).	HTTPS URL	""
Saml2:SingleLogoutDestination	IdP SLO endpoint URL (can be auto-resolved from metadata).	HTTPS URL	""
Saml2:SignatureAlgorithm	XML signature algorithm.	URI value accepted by SAML library	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Saml2:SigningCertificateFile	Local SP signing certificate file (relative to app base path).	File name/path	""
Saml2:SigningCertificatePassword	Password for signing certificate file.	String	""
Saml2:SignatureValidationCertificateFile	IdP certificate file used to validate	File name/path	""

	signatures (optional if metadata provides certs).		
Saml2:CertificateValidationMode	Certificate chain validation mode.	None, PeerTrust, ChainTrust, PeerOrChainTrust, CustomRootTrust	ChainTrust
Saml2:RevocationMode	Certificate revocation behavior.	NoCheck, Online, Offline	Offline
Saml2:XmlCanonicalizationMethod	XML canonicalization algorithm URI.	XML-DSig canonicalization URI	http://www.w3.org/2001/10/xml-exc-c14n#

CustomSettings

In appsettings.json, these values are stored as strings ("true"/"false") and mapped to booleans by .NET configuration binding.

Parameter	Purpose	Possible values	Default
CustomSettings:UseApplicationFullPath	Controls whether application full path is used when listing/ launching assigned apps.	"true" / "false"	"false"
CustomSettings:EnableAutoWindowsAuthenticationOnLocalhost	Allows automatic Windows authentication on localhost/ loopback scenario.	"true" / "false"	"false"
CustomSettings:EnablePasswordEncryption	Encrypts domain/ username/ password in HTML5	"true" / "false"	"true"

	launch connection string using RSA parameters.		
CustomSettings:TwoFaBypassForLocalNetwork	Bypasses Web Portal 2FA when client is in same private subnet as server.	"true" / "false"	"false"
CustomSettings:UseSamlPasswordClaim	SAML claim type used as forwarded Windows password for session launch.	Claim type URI/ name or empty string	""

Troubleshooting

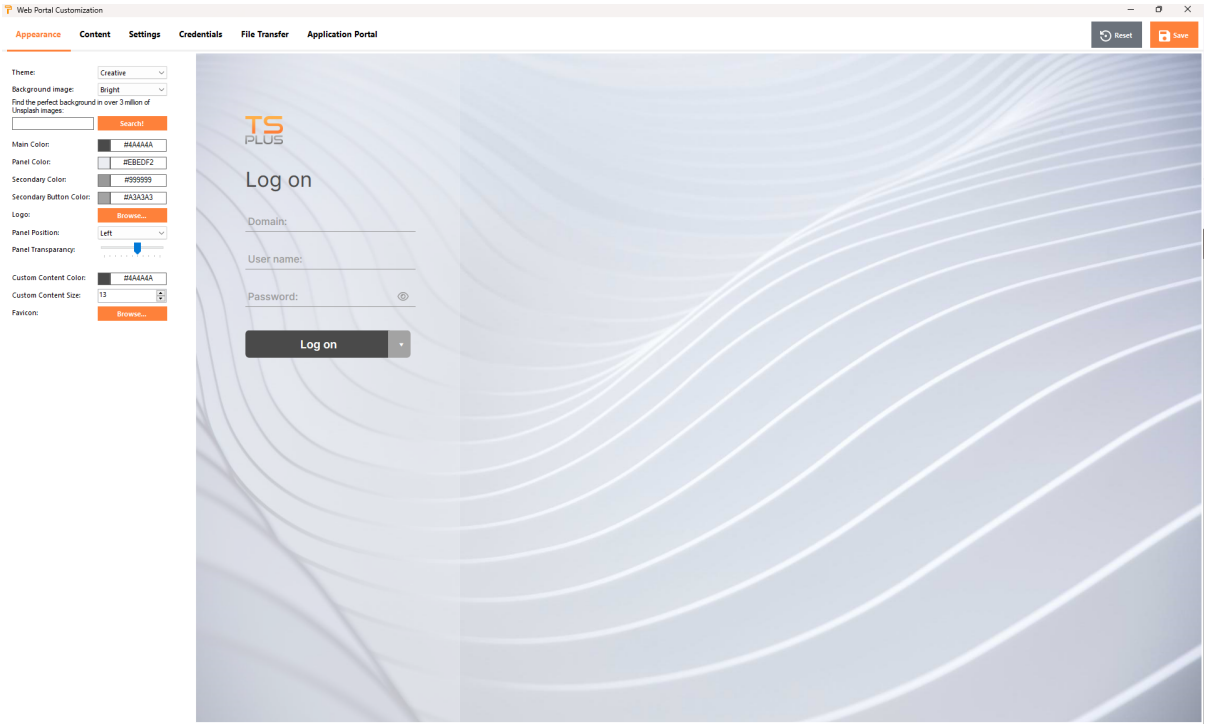
Web Portal 2026 with SSO logs can be enabled from AdminTool > Advanced > Logs > Web Portal log.

The resulting WebPortal.log log file is found in C:\Program Files (x86)\TSplus\Clients\webportal, where C:\Program Files (x86)\TSplus is TSplus Remote Access setup folder.

Creating and Customizing HTML Web Access pages using the Web Portal Customization

Using the Web Portal Customization, you will be able to create your own customized HTML Web Access pages - and there is no need to be a web developer!

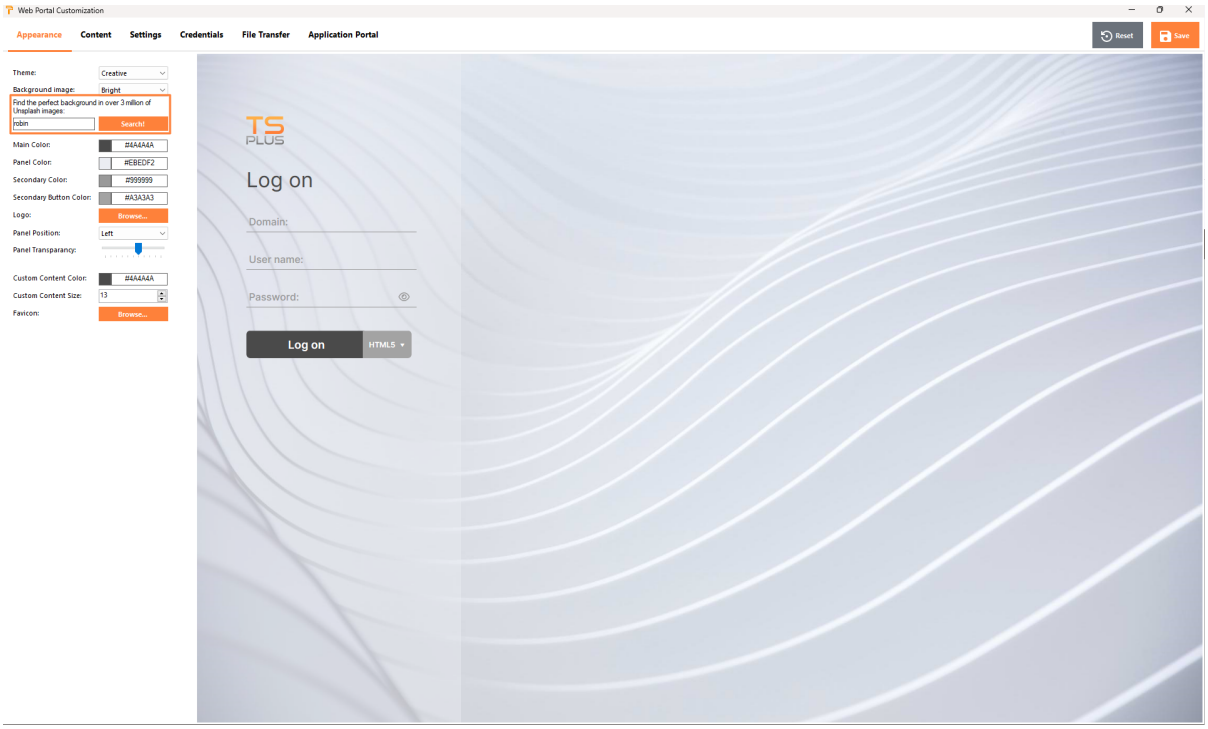
Web Portal Customization - Appearance



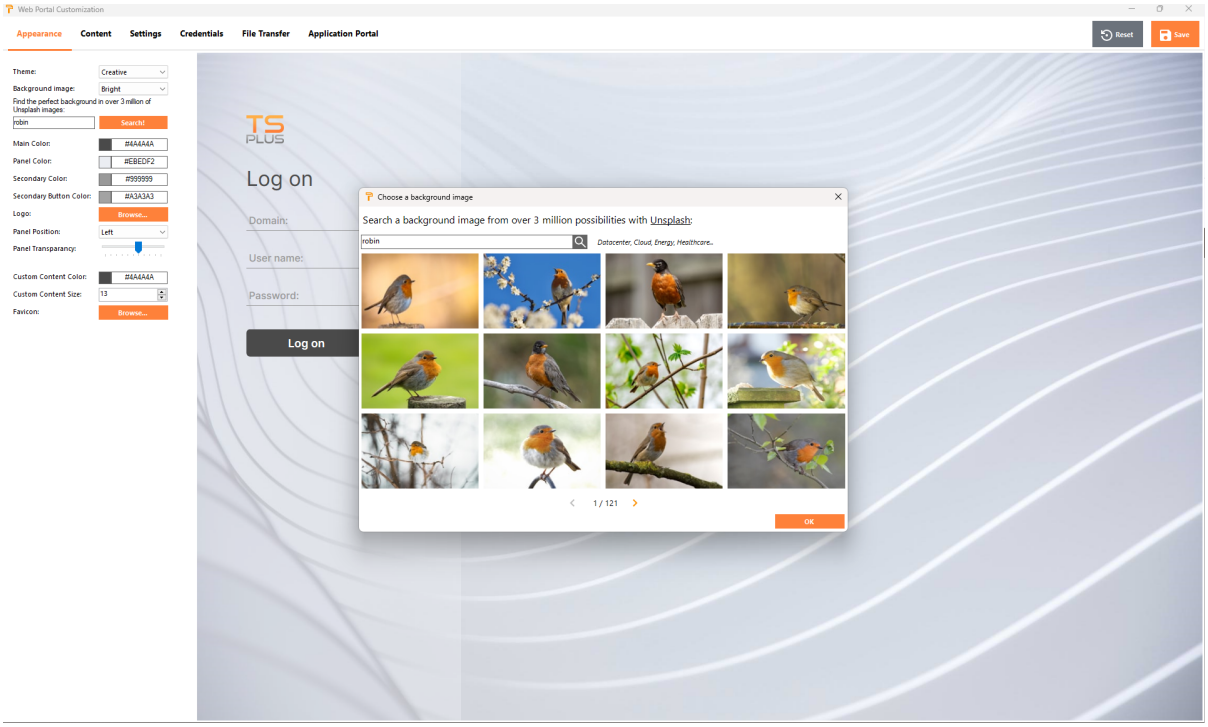
With the Appearance tab, you will be able to customize all the graphic settings, as well as add your own logo.

You have the choice between a collection of photos, or you can add your own. You can also set any color theme with the background color of your choice or you can use one of the classic themes.

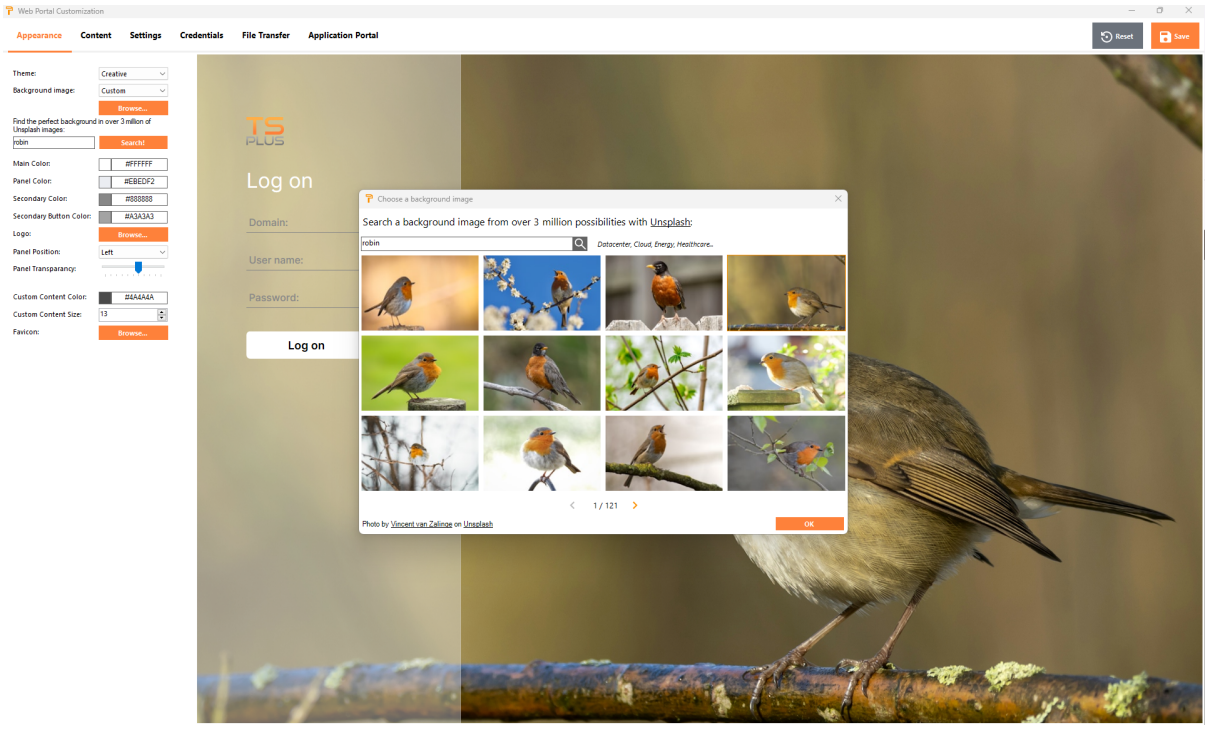
You can also type a keyword to search a background image from the Unsplash library:



I will display a collection of images to choose from.

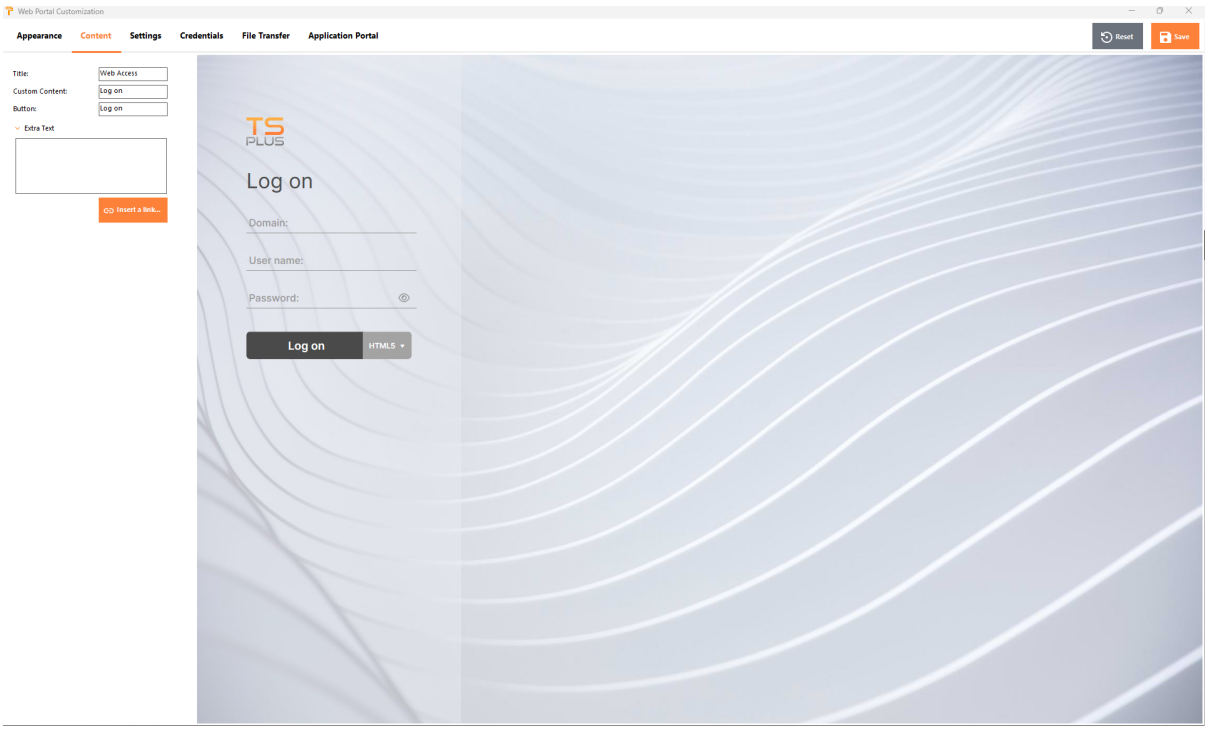


Select your favorite picture to see the result on your web portal:

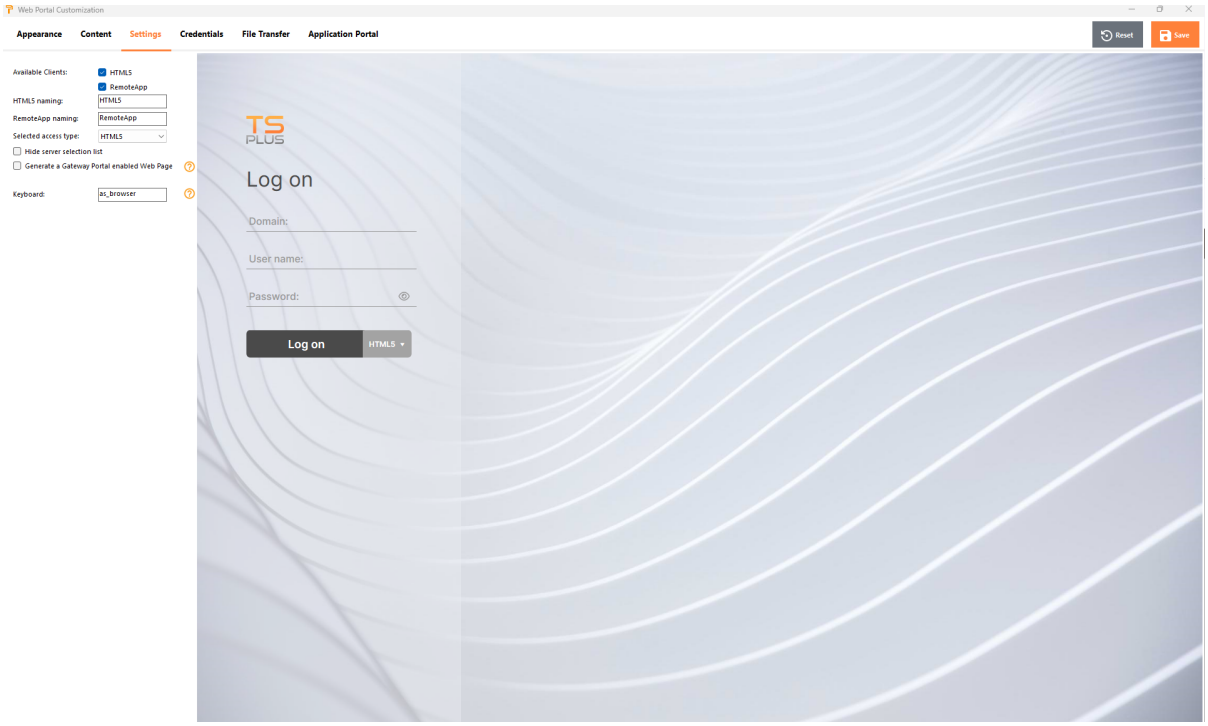


The theme colors will automatically adapt to the picture chosen once you validate your choice with the “Ok” button. Of course, you can still personalize the colors as you want.

Web Portal Customization - Content

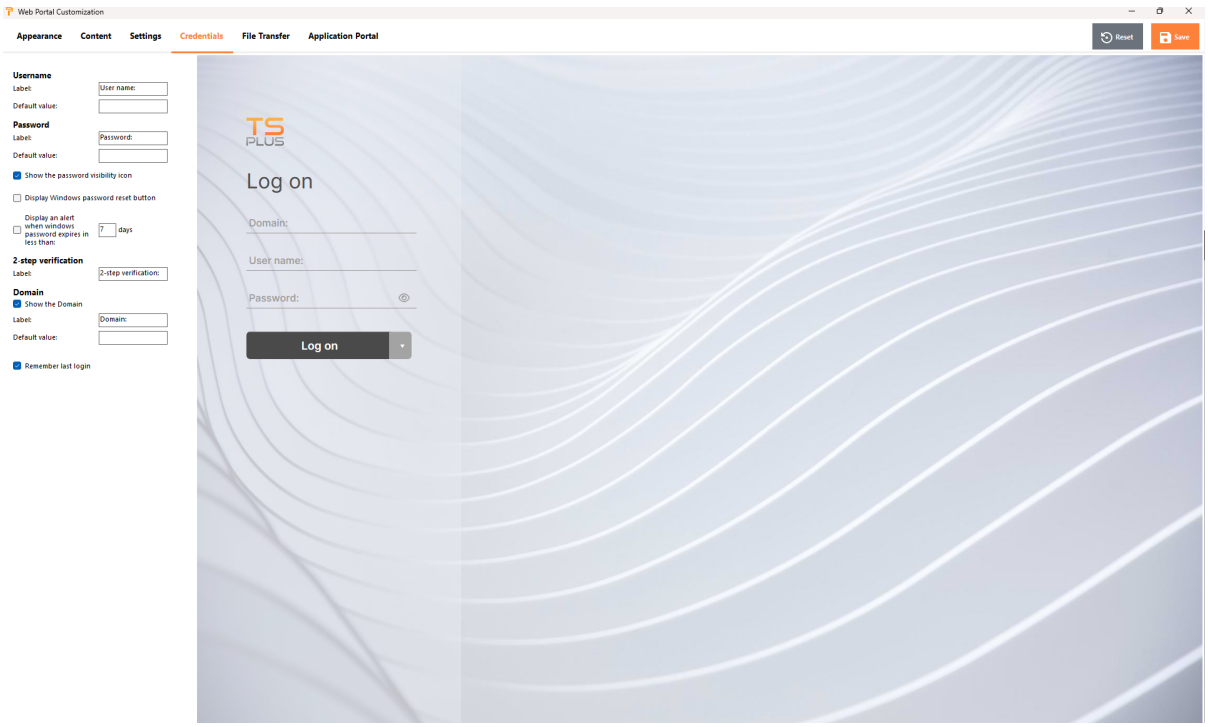


Web Portal Customization - Settings



- “**Available Clients**”: Choose between 2 types of web connection clients. If both are checked, the user will have the choice. You can change the name used for these options in your Web Portal. You can also choose which option is selected by default if both options are available.
- “**Gateway Portal**”: Check it to activate a Gateway Portal enabled page. This feature adds an extra authentication step when you assign a server to a user or group.
- “**Keyboard**”: Only for advanced administrators who have special keyboard requirements.

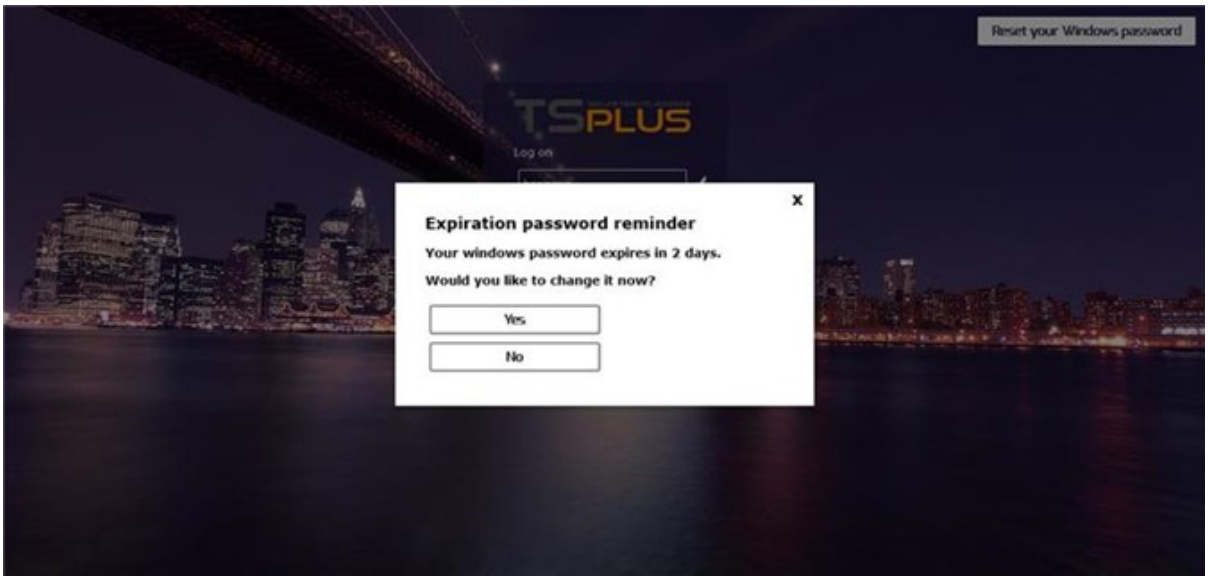
Web Portal Customization - Credentials



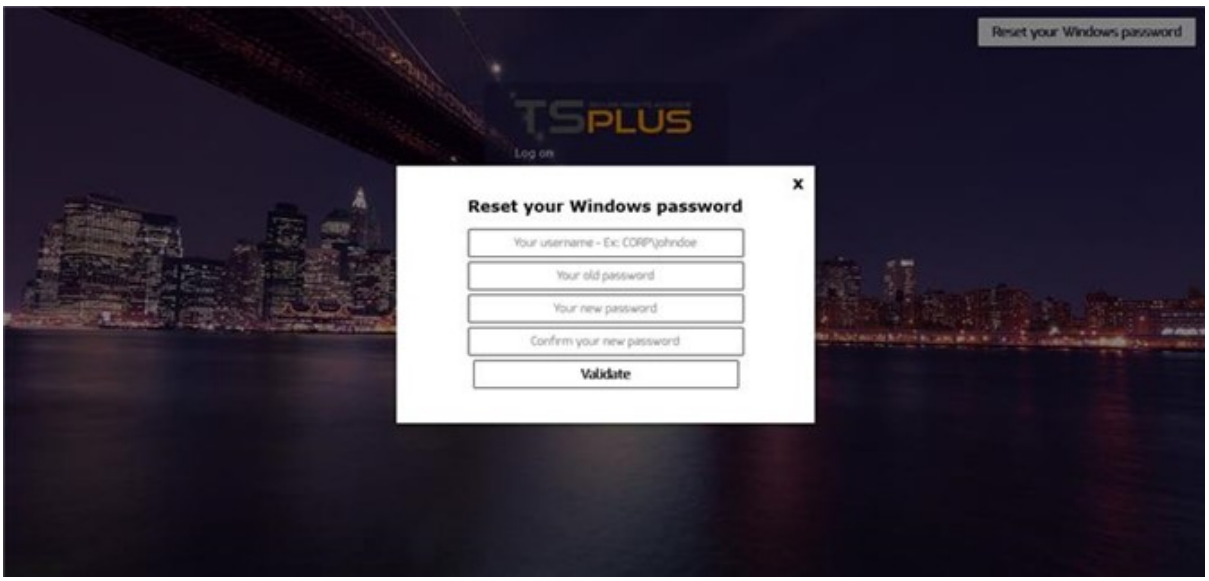
- “**Label**”: You can change the text used to designate the user name, password, …
- “**Default Values**”: You can specify a default login, password and domain that will auto-

populate the login fields. All of the settings present here are saved in the index.html file, which can be copied and renamed to your preference.

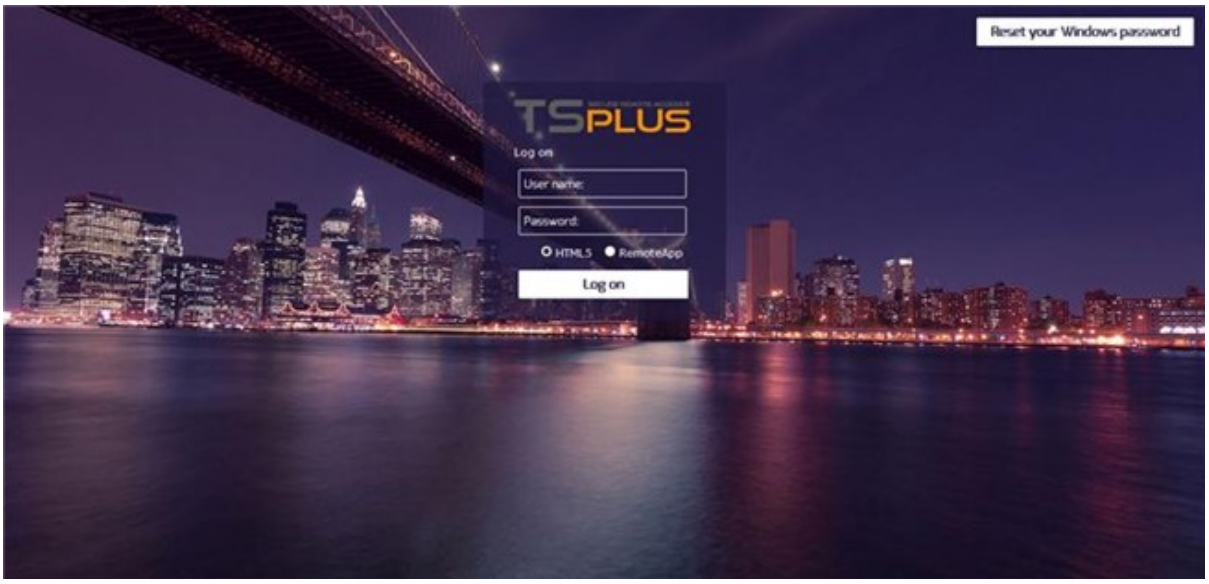
- “**Show the Domain Field**”: When checked, the Domain field is included in the login information request.
- “**Password**”: You can add an alert message showing during the connection through the web portal, to inform the user about his password expiring date. For example, the following pop-up will show if the user’s windows password expires in less than 3 days:



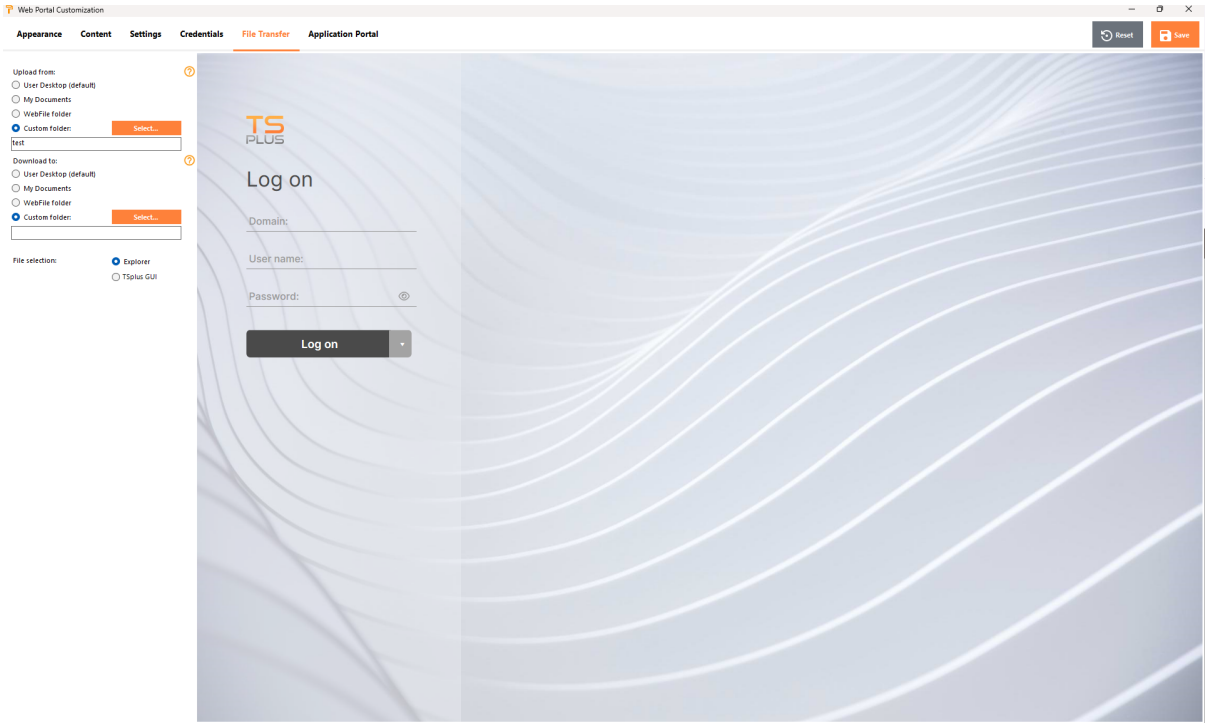
As mentioned it gives him the possibility to change it directly from the Web Portal using the pop-up displayed just below:



You can also directly make the user able to change his windows at any time, by checking the option “Display windows password reset button”.

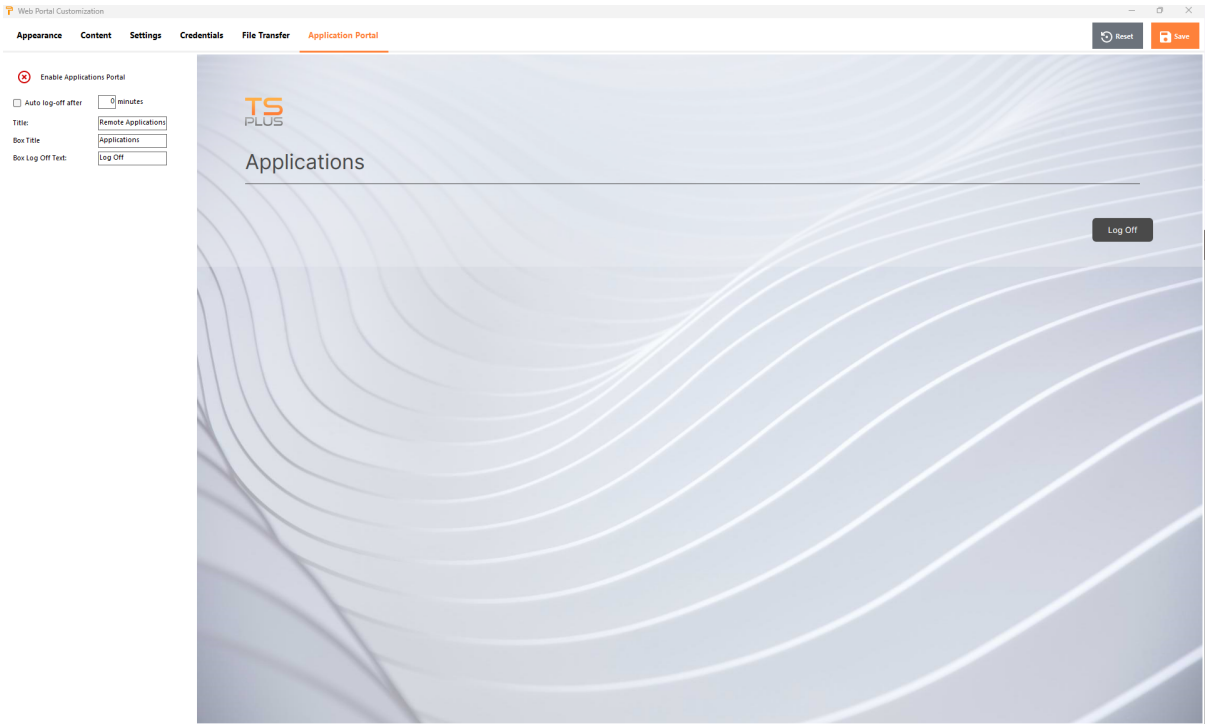


Web Portal Customization - File Transfer



- “**Upload - Download**”: choose source and destination paths for file uploads and downloads.

Web Portal Customization - Application Panel



More information on the Application Portal can be found here.

Saving typed values and Resetting to default ones

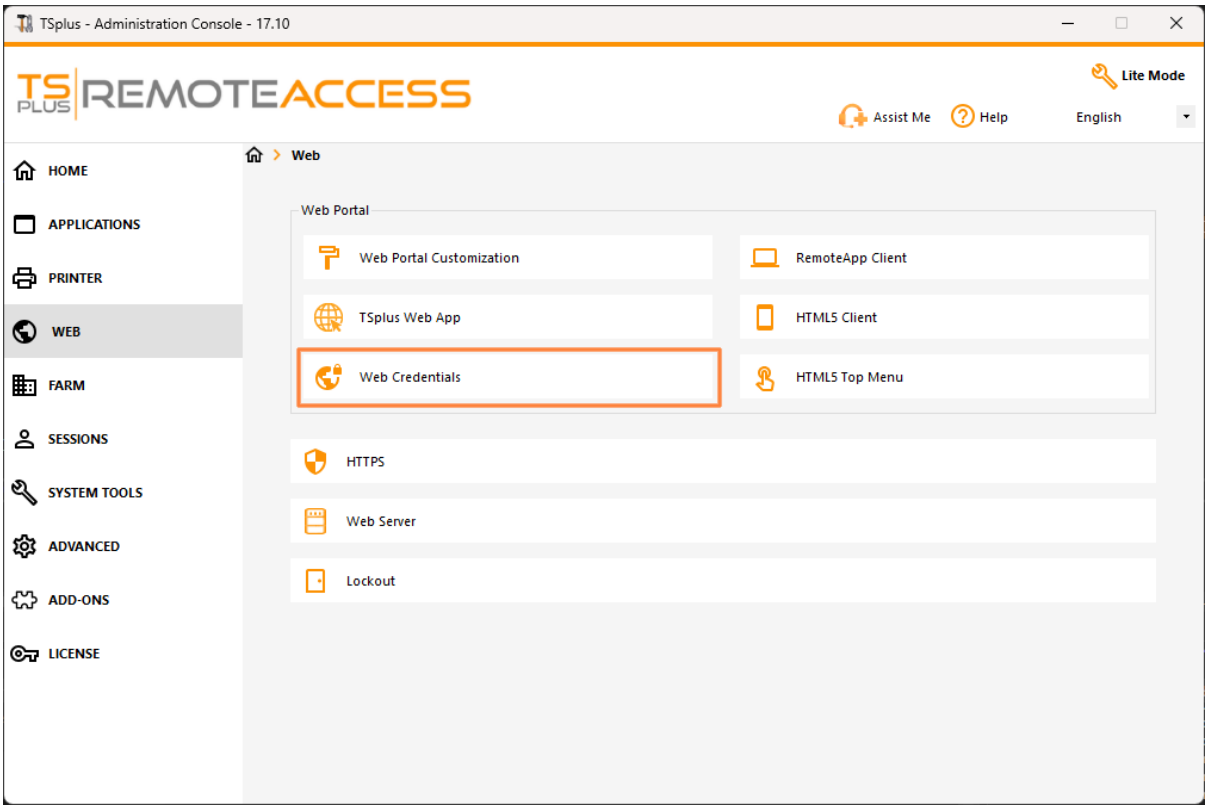
Don’t forget to click on the “Save” button to save all your modifications.

If you want to reset these values to original values, click on the “Reset” button.

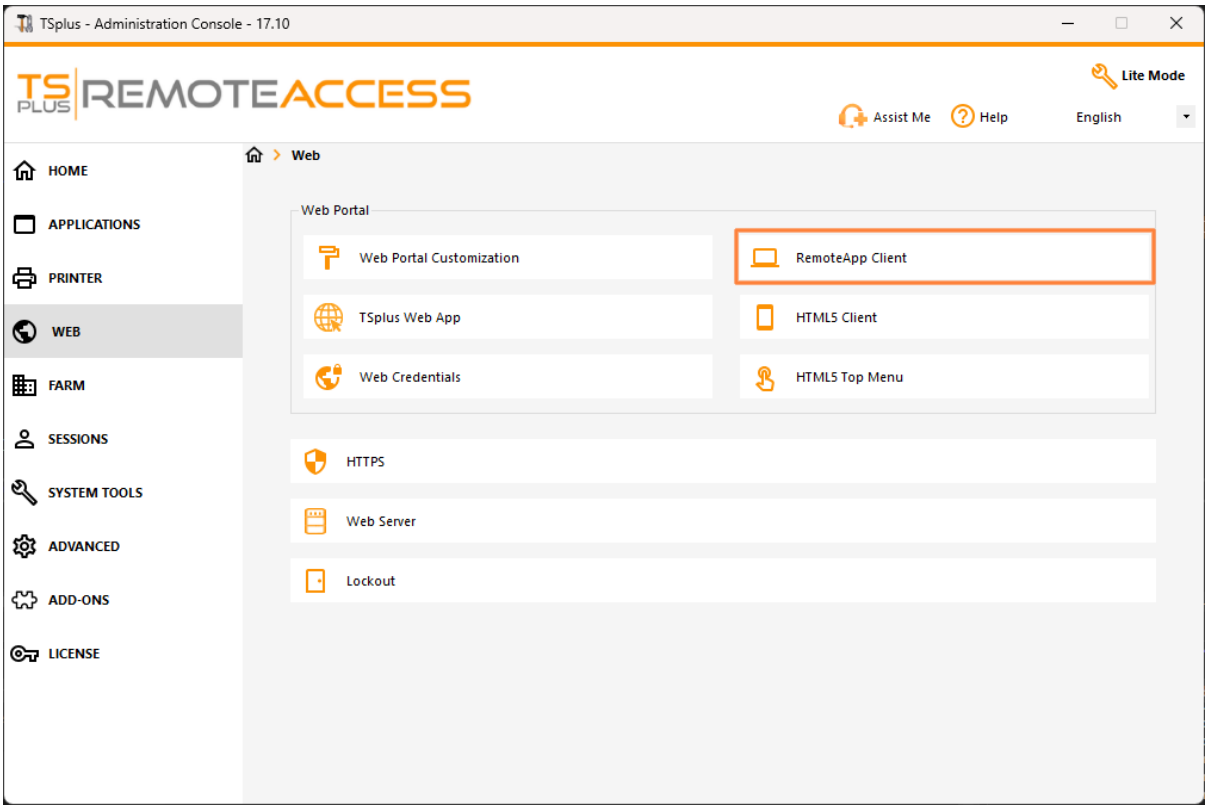
Web Credentials

The “Web Credentials” section allows you to enable (or disable) the Web Credentials feature.

When using Web Credentials, you might want to allow empty passwords. If you only have Web Credentials with empty passwords, we recommend that you uncheck the “Show Password Field” option, in order to simplify even more the web login page.

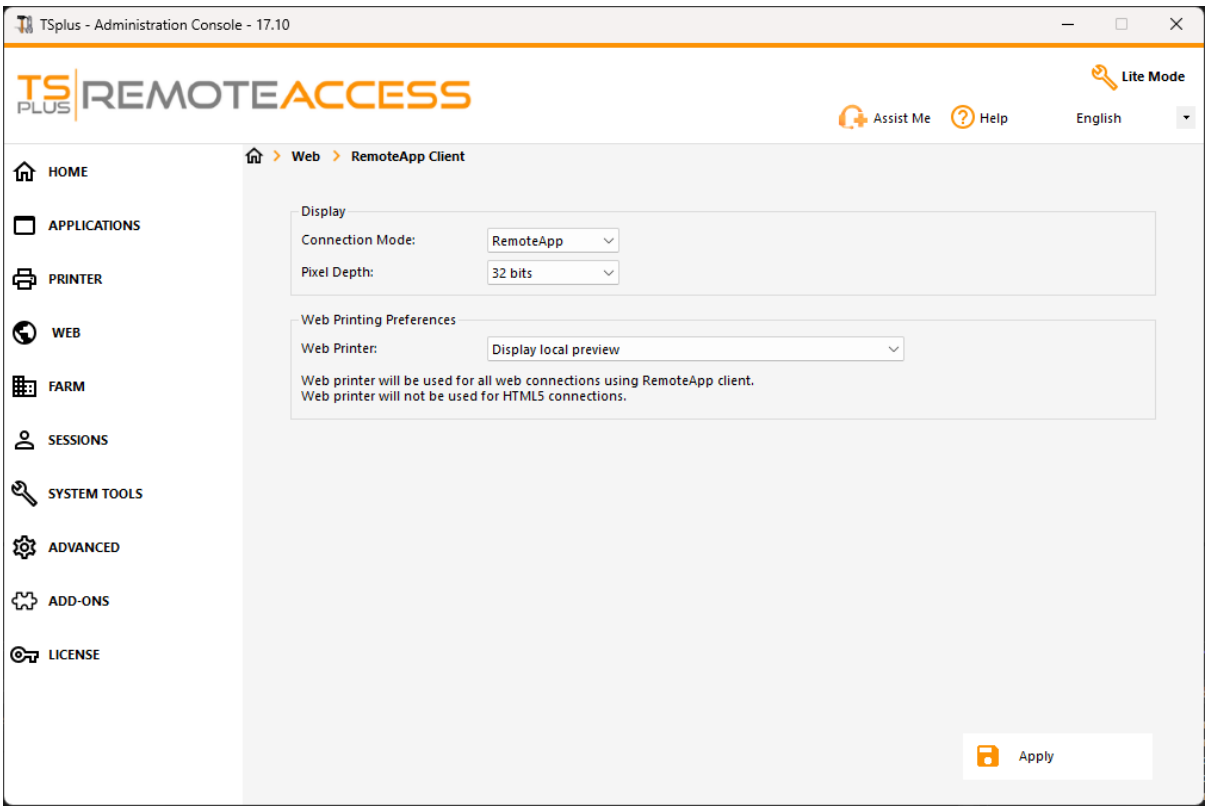


Remote App tile

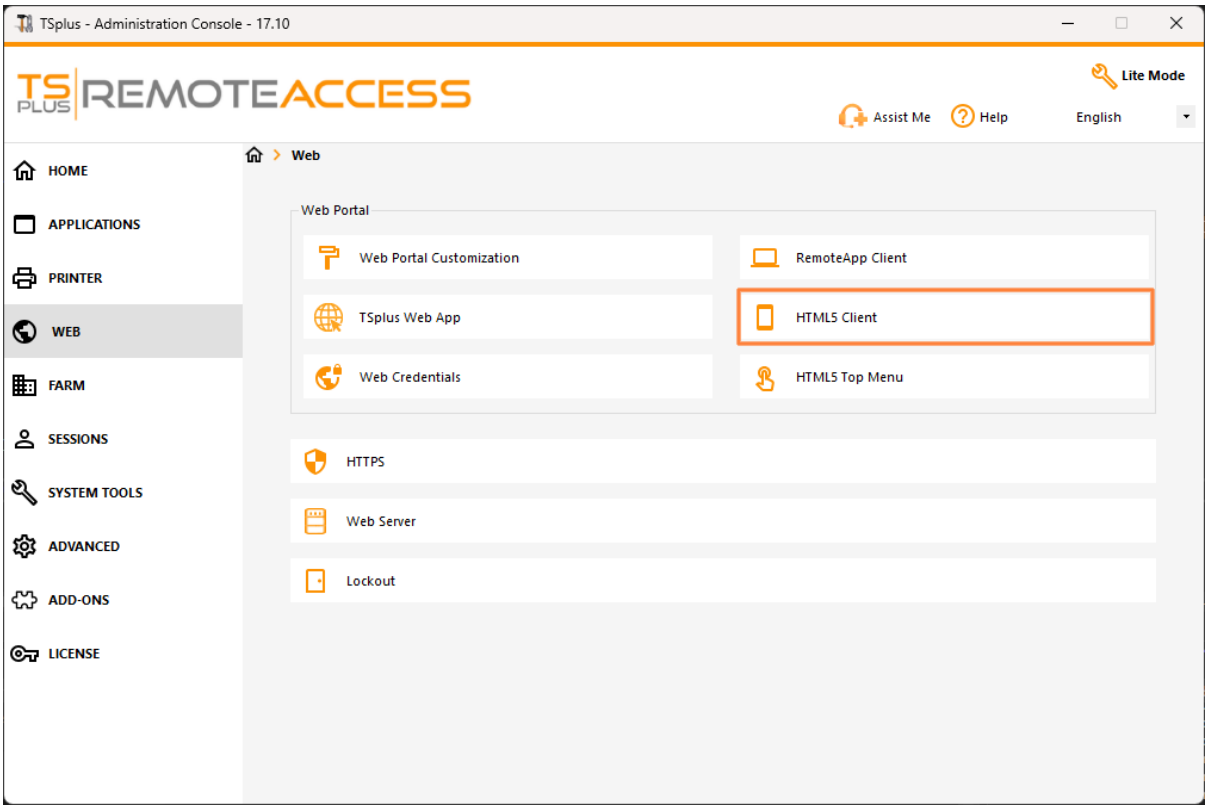


This tile is for Windows clients specific settings.

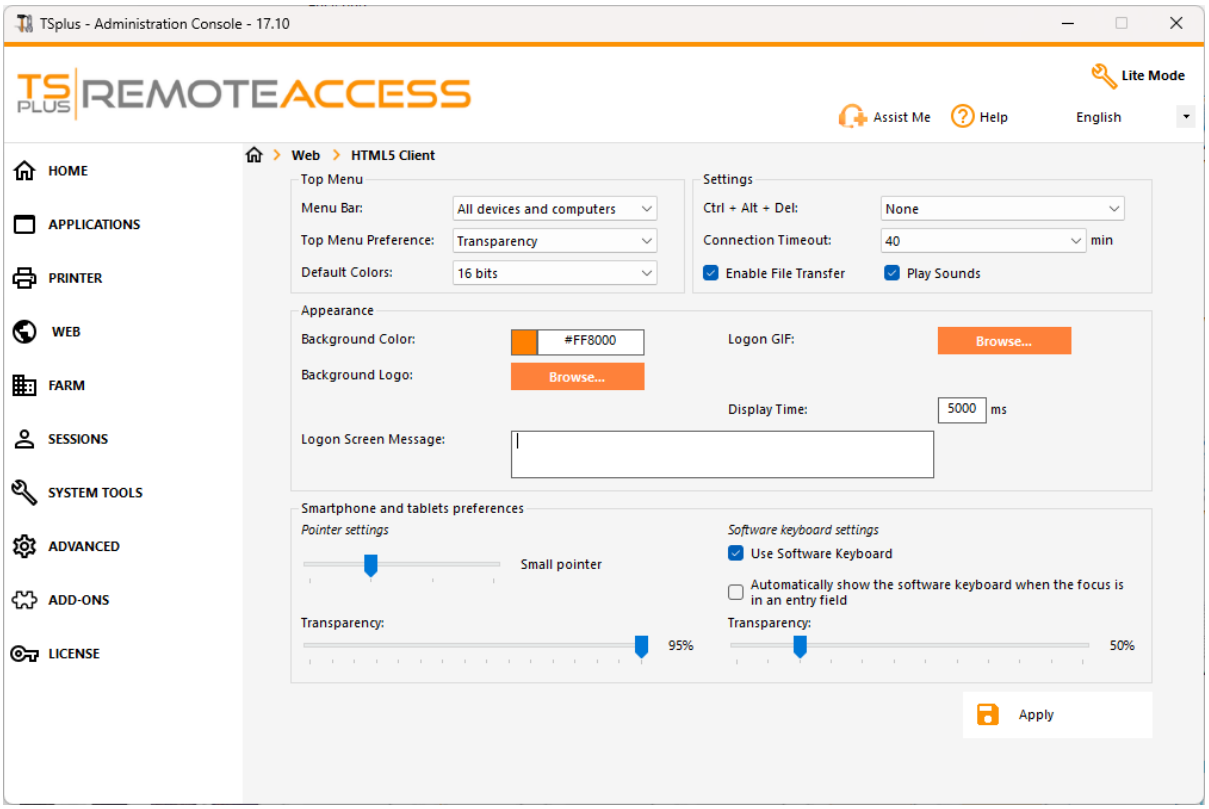
You can choose your display between RemoteApp (remote connection without the remote desktop) or Standard RDP. You can also decide if you want documents to be printed on the user default printer, display a local preview or the local printer choice.



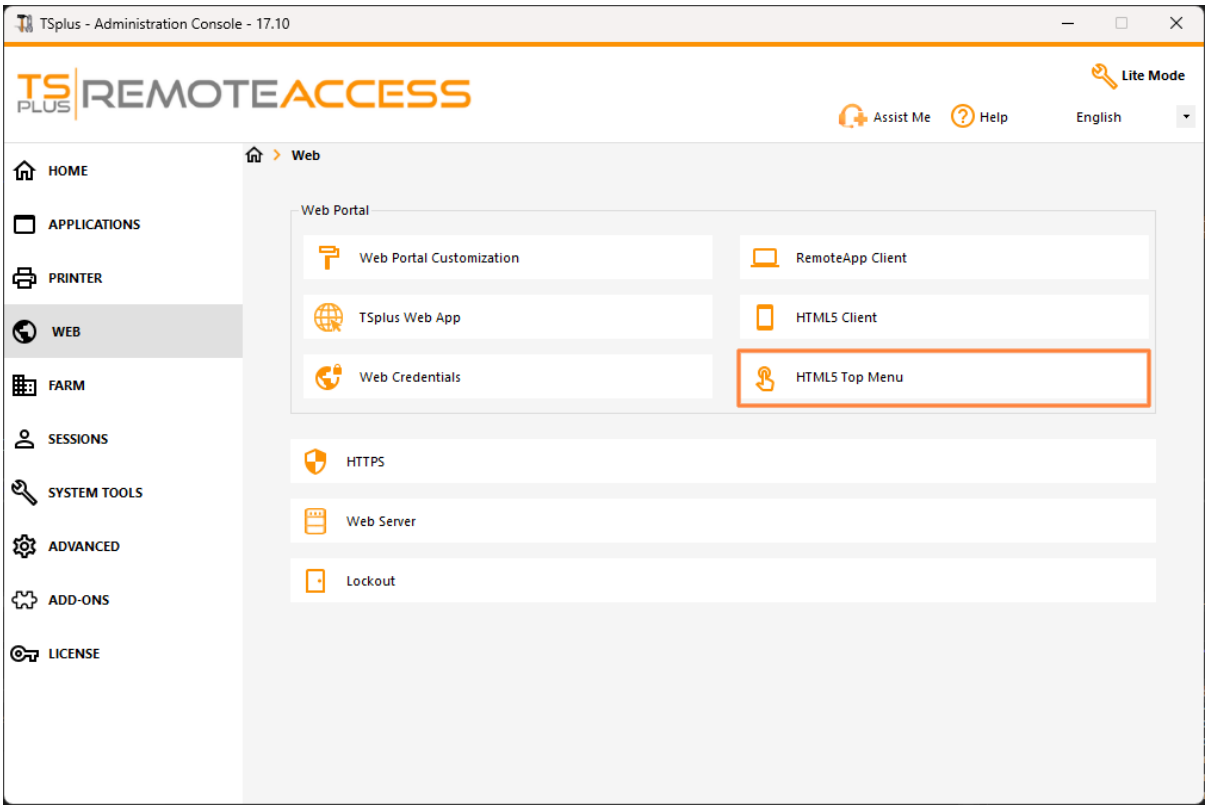
HTML5 client tile



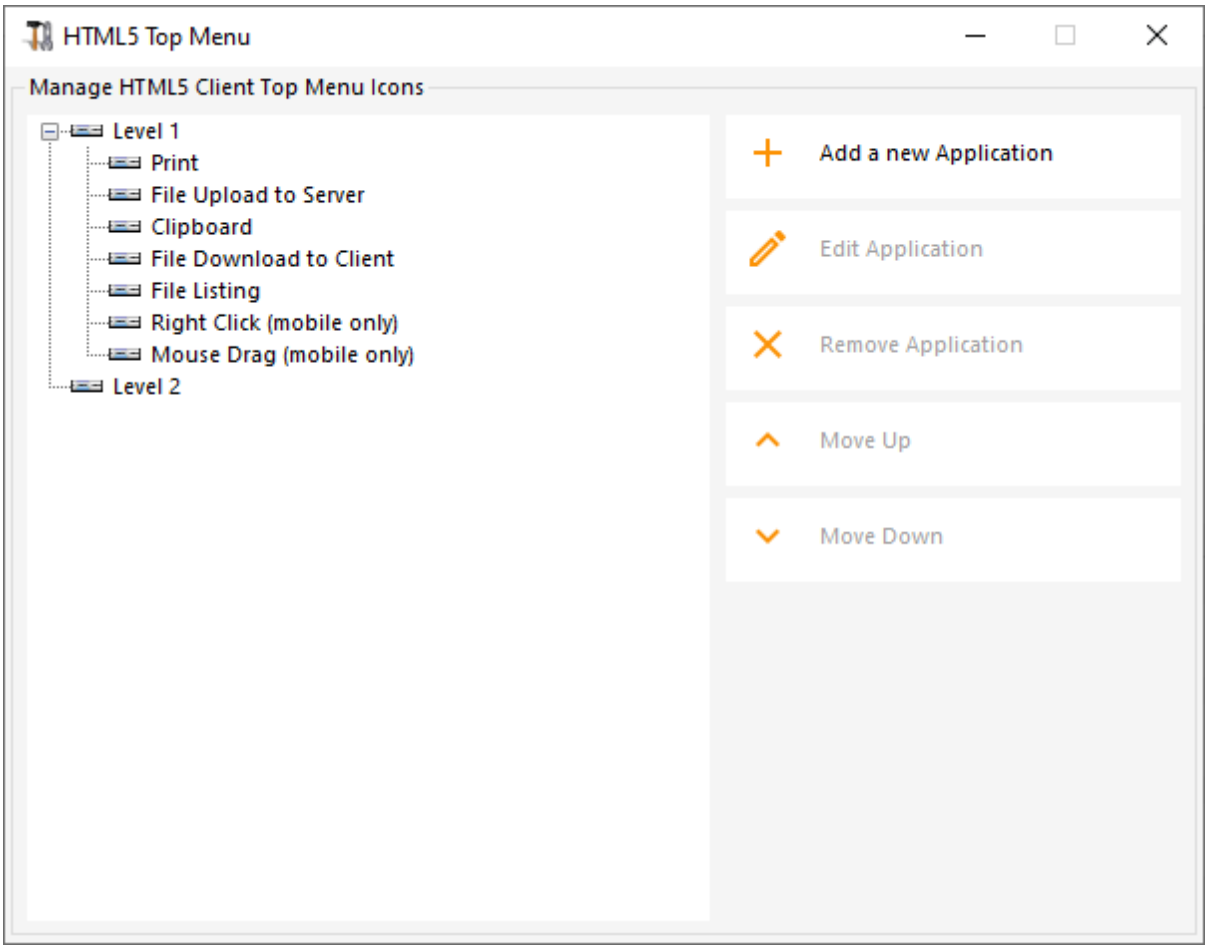
On this tile, you can edit the parameters for the HTML5 client web display. More information on this page.



HTML5 Top Menu Tile



This tile enables you to choose the applications to display on level 1 or 2 on the Top Menu of your generated remote web session. You can also edit these applications in order for them to appear on a specific client type : pc, mobile, ios… on or all of them.


HTML5 Top Menu
Manage HTML5 Client Top Menu Icons
Level 1
Print
File Upload to Server
Clipboard
File Download to Client
File Listing
Right Click (mobile only)
Mouse Drag (mobile only)
Level 2
Add a new Application
Edit Application
Remove Application
Move Up
Move Down