Securing a TSplus server

Overview

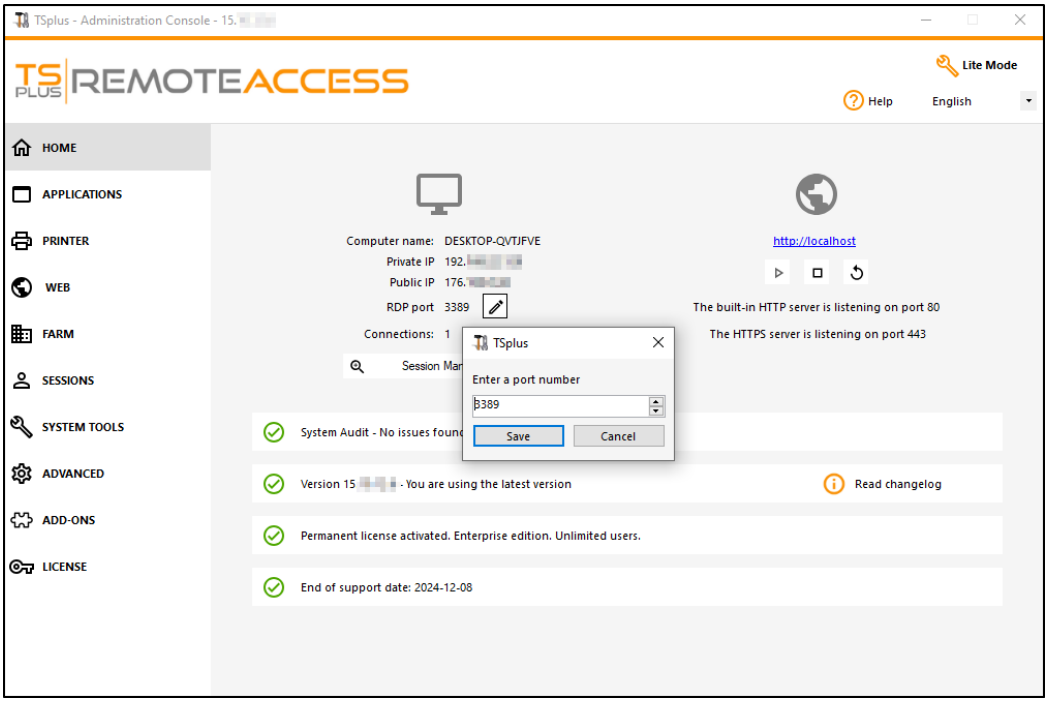
Securing any server is a never-ending story where every expert could add another chapter.
TSplus benefits from and is compatible with existing security infrastructure in a company (Active Directory, GPOs, HTTPS servers, SSL or SSL telecommunication systems, VPN, access control with or without ID cards, 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.

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. 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.

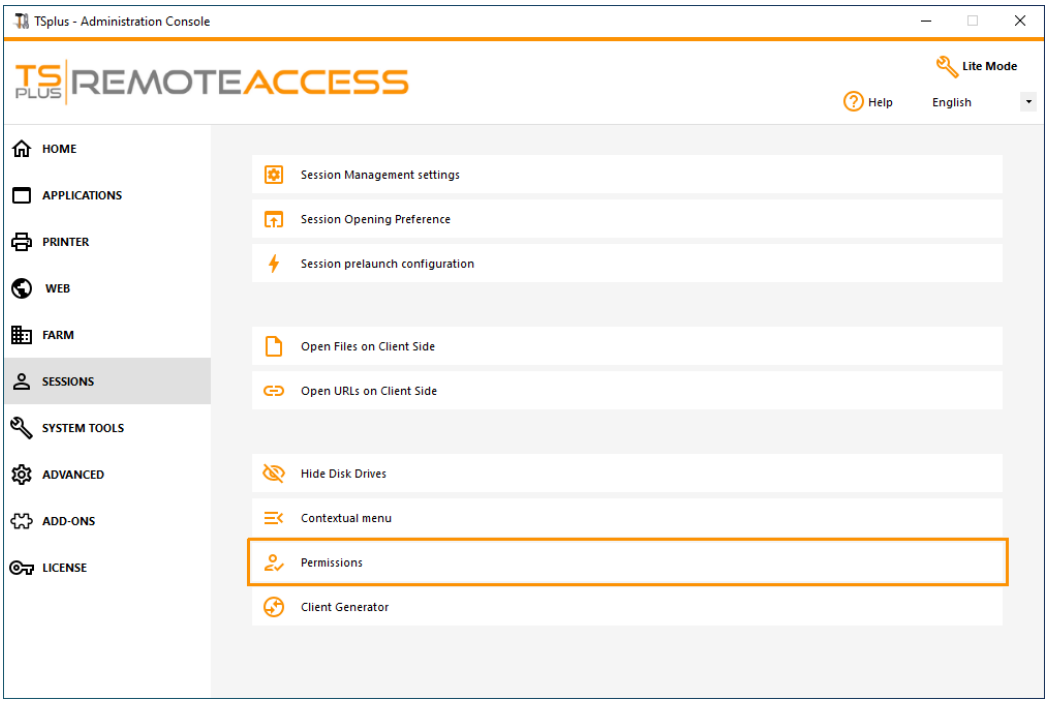
The administrator can decide that a password is mandatory to open a session.

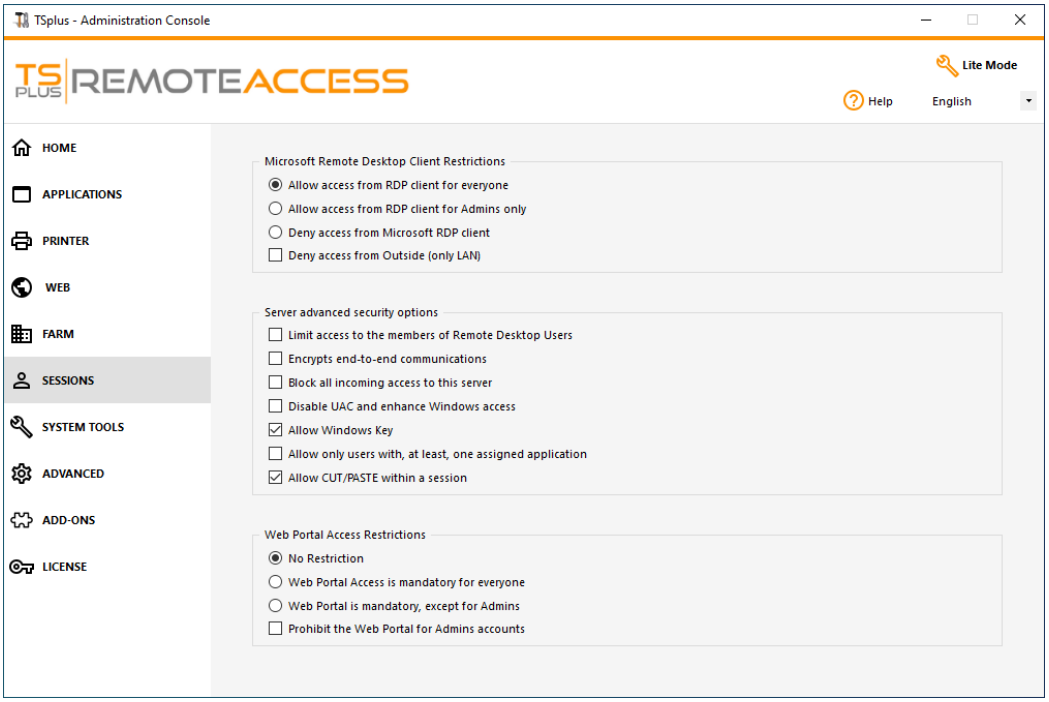
Through setting the applicable local Group Policy, the administrator can specify whether to enforce an encryption level for all data sent between the client and the remote computer during a Terminal Services session.
If the status is set to Enabled, encryption for all connections to the server is set 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.

Sessions Permissions

You can find multiple advanced security options if you click on the Sessions - Permissions tab:





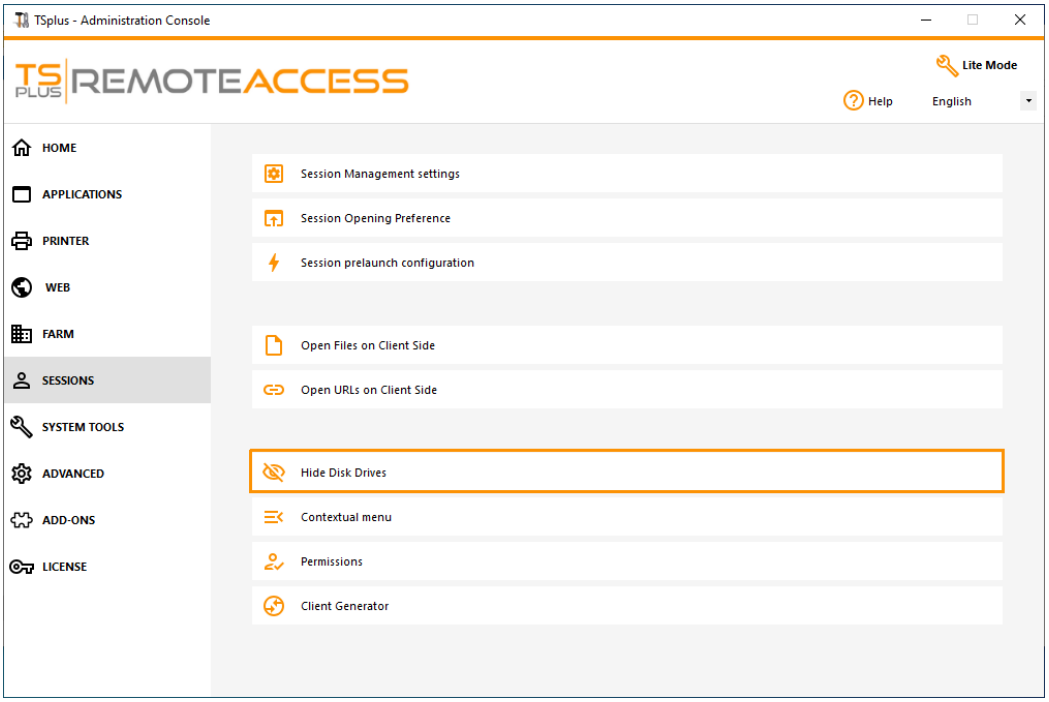
- **Allow access from Microsoft RDP client for everyone:** Allows every user to connect using mstsc.exe.
- **Allow access from Microsoft RDP client for Admins only:** Allows only Admins to connect using mstsc.exe.
- **Deny access from Microsoft RDP client:** Prevent anyone to be able to connect using 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

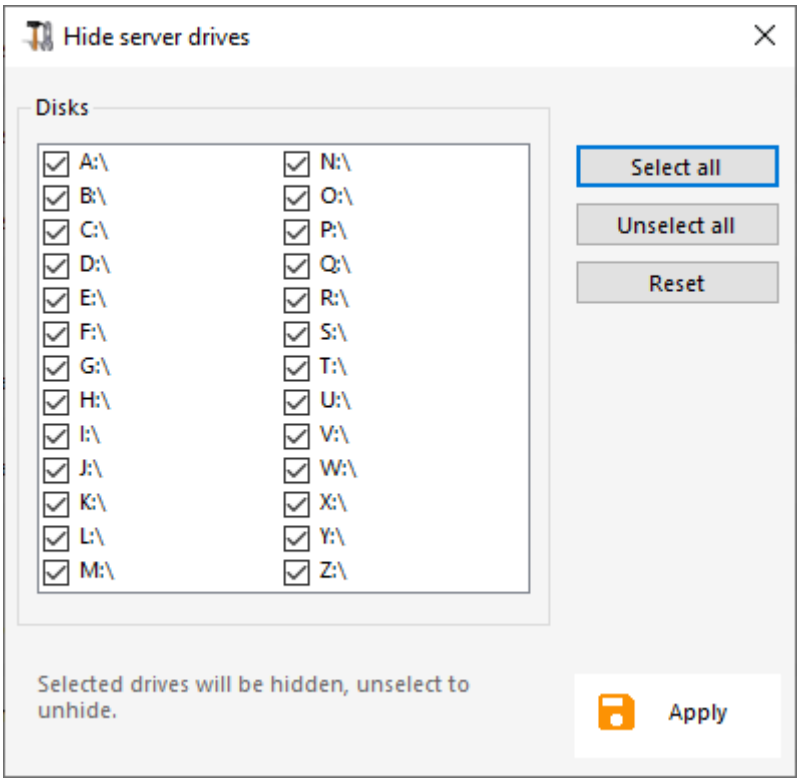
- No Restriction
- Web Portal is mandatory for everyone: users can only connect via the Web Portal.
- Web Portal is mandatory, except for Admins: users can only connect via the Web Portal, except Administrators.
- Prohibit the Web Portal for Admins accounts: Administrators cannot connect via the Web Portal.

Hiding the server disk drives:

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.

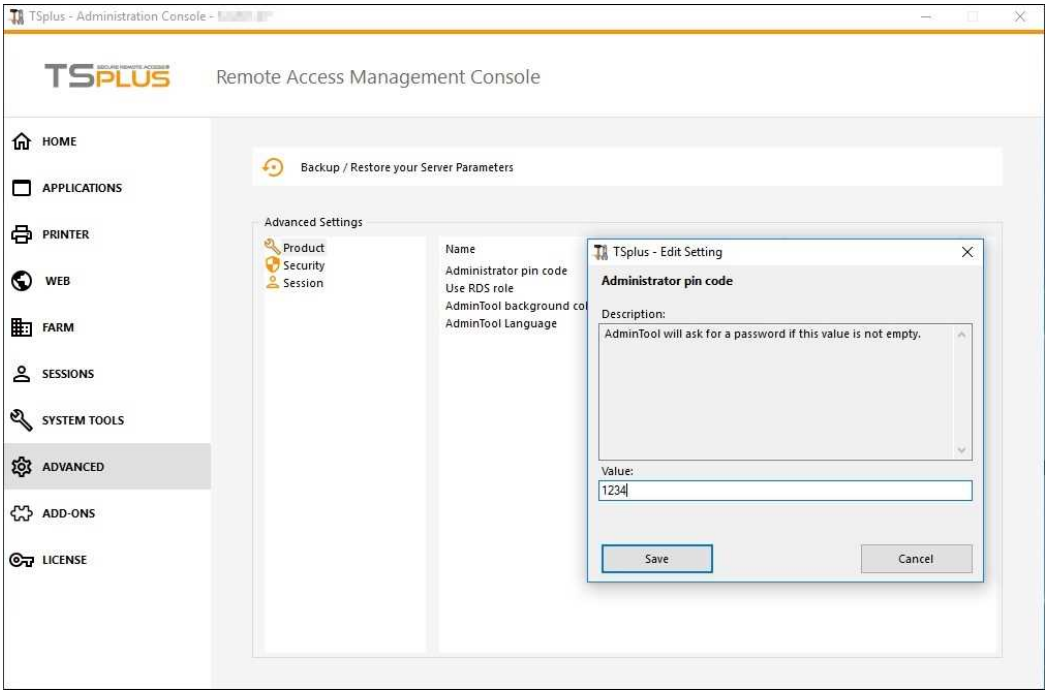
The tool flags the disks drives as hidden, but it also adds the HIDDEN property to the entire root folders and users list in Document and Settings.

If the administrator wants to see these files he must:

1. Type the disk drive letter. For example: **D:** which will take you to the D: drive.
2. Turn on **SHOW HIDDEN FILES AND FOLDERS** in the folder view properties.

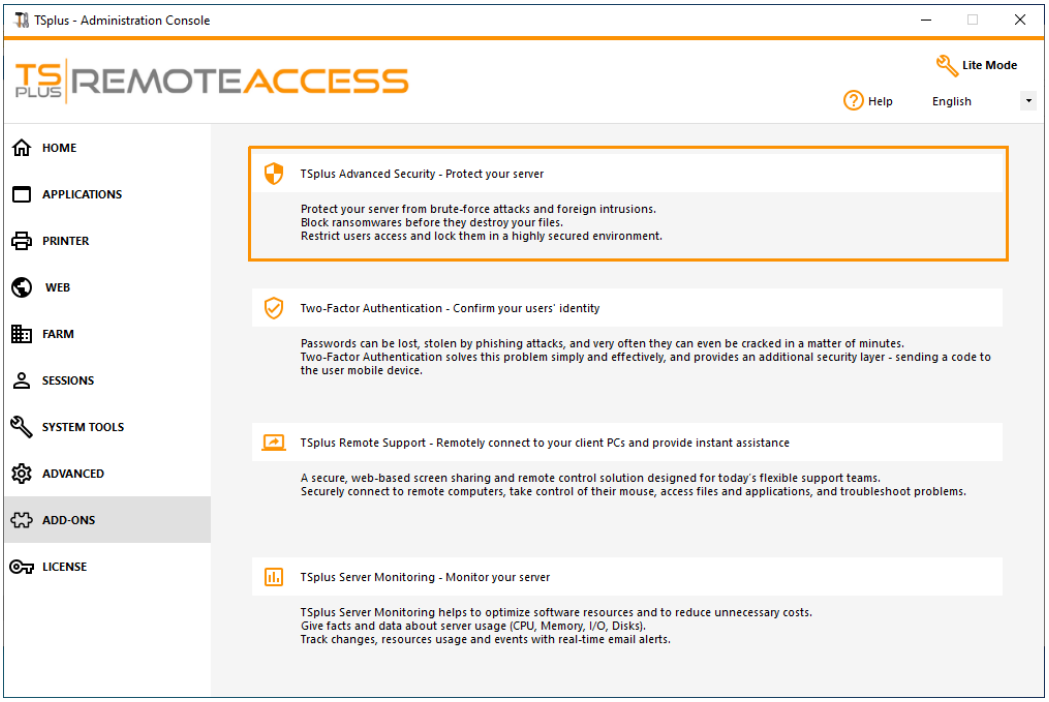
Administrator Pin Code

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:

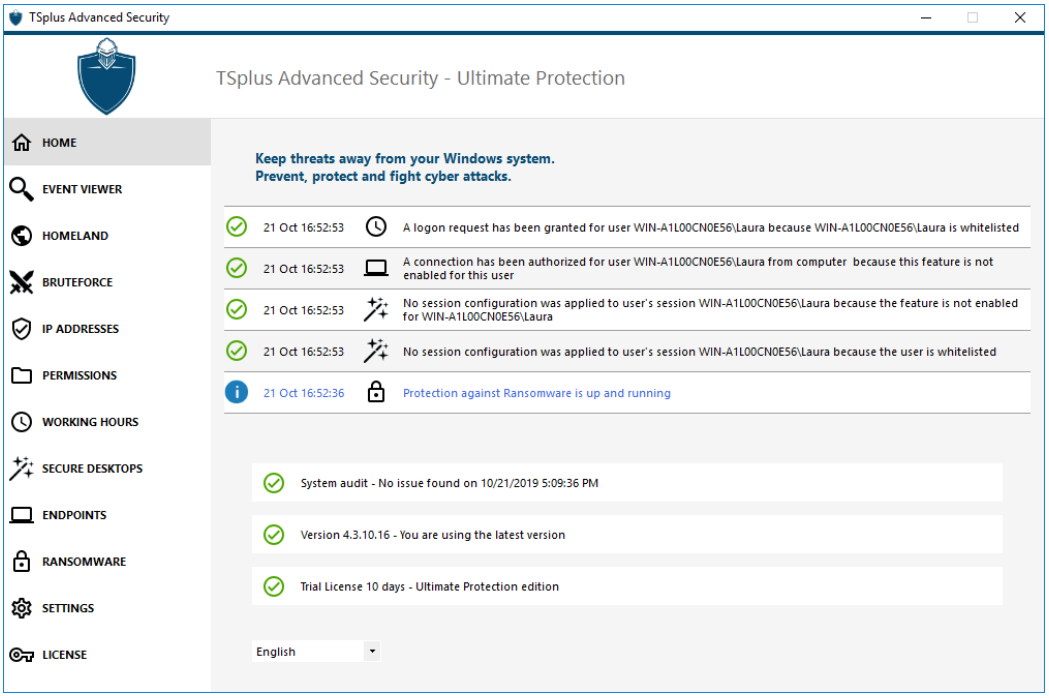


TSplus Advanced Security Ultimate

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 Brute-Force Attacks Defender 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

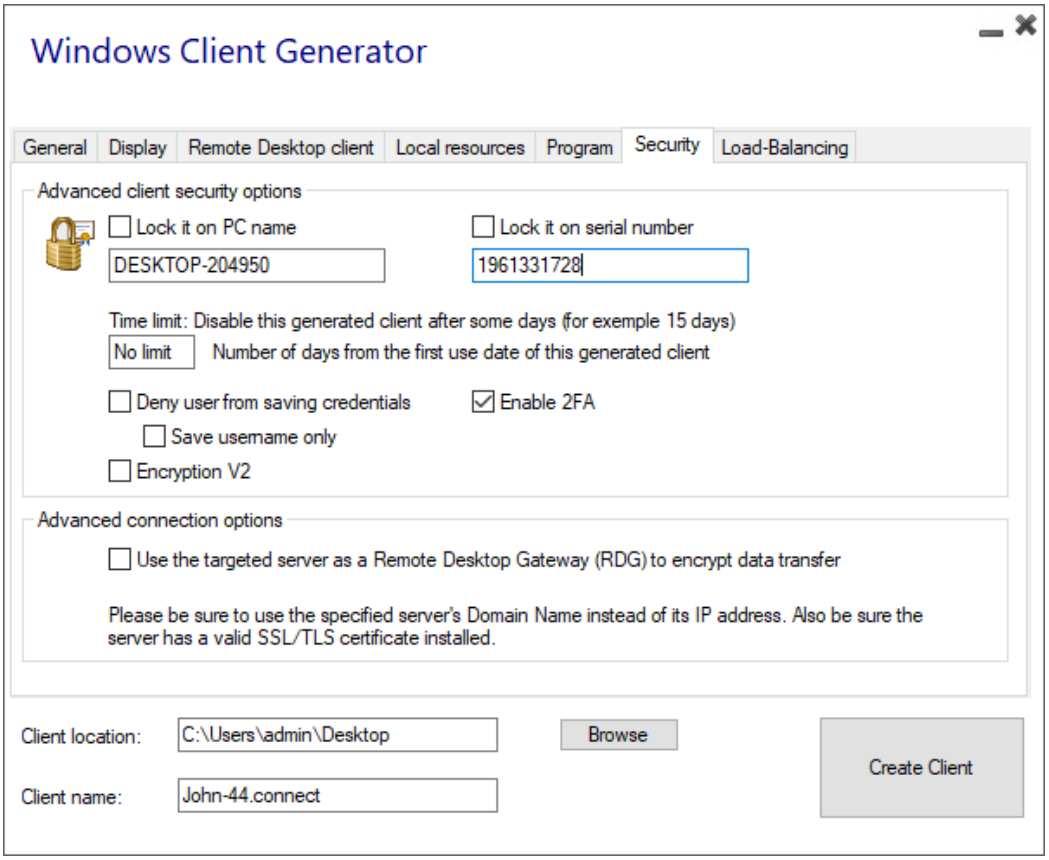
SSL Certificates process is detail on these pages:
- TSplus provides an easy-to-use tool to generate of a free and valid SSL certificate: Free and Easy-to-install SSL Certificate
- HTTPS & SSL Third Party Certificates.
- Choose your Ciphers Suites to enhance Security.

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.