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":

👪 TSplus - Administration Console	e - 15.	- 🗆 X
	EACCESS	💐 Lite Mode 🕜 Help English 💌
М номе		
	Computer name: DESKTOP-QVTJFVE Private IP 192.	http://localhost
S web	Public IP 176.	The built-in HTTP server is listening on port 80
FARM	Connections: 1 TSplus X	The HTTPS server is listening on port 443
SESSIONS	Q Session Mar Enter a port number β389 ♣	
SYSTEM TOOLS	System Audit - No issues found Save Cancel	
ស៊្លា advanced	Version 15	(i) Read changelog
었 add-ons	Permanent license activated. Enterprise edition. Unlimited users.	
ତିନ୍ଦ୍ର LICENSE	End of support date: 2024-12-08	

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:

TSplus - Administration Console			- 🗆	×	
	ACCESS		Ҳ Lite Mode		
		Help	English	•	
М НОМЕ					
	Session Management settings				
	Session Opening Preference				
	Session prelaunch configuration				
S WEB					
FARM	Open Files on Client Side				
	C=> Open URLs on Client Side				
SYSTEM TOOLS					
ស៊្វែ ADVANCED	X Hide Disk Drives				
Հ子 ADD-ONS					
ତିଙ୍ଗ LICENSE	2 Permissions				
	Client Generator				

			🔍 Lite N	lode
	REMOTEACCESS		English	•
	Microsoft Remote Desktop Client Restrictions			
	Allow access from RDP client for everyone Allow access from RDP client for Admins only			
	Deny access from Microsoft RDP client Deny access from Outside (only LAN)			
S web	Server advanced servicity options			
FARM	Limit access to the members of Remote Desktop Users Encruits end-to-end communications			
	Block all incoming access to this server Dirable LICC and enhanced Windows access			
SYSTEM TOOLS	Allow Windows Key Allow Windows Key			
ADVANCED	Allow CUT/PASTE within a session			
값 ADD-ONS	Web Portal Access Restrictions			
ତିନ୍ଦୁ License	No Restriction Web Portal Access is mandatory for everyone Web Portal is mandatory, except for Admins Prohibit the Web Portal for Admins accounts			

- 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" :

🐺 TSplus - Administration Console		- 🗆 X
	ACCESS () HEID	✓ Lite Mode English ▼
	Session Management settings	
	Session Opening Preference	
FARM	Open Files on Client Side	
SYSTEM TOOLS	C Open URLs on Client Side	
段 advanced	X Hide Disk Drives	
값 ADD-ONS	Contextual menu 2 Permissions	
	Client Generator	

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:

<table-of-contents> Hide server drives</table-of-contents>	5	×
Hide server drives Disks A:\ A:\ B:\ C:\ C:\ C:\ C:\ C:\ C:\ C:\ C:\ C:\ C	s N:\ O:\ O:\ P:\ Q:\ R:\ S:\ T:\ U:\ U:\	× Select all Unselect all Reset
 ✓ I:\ ✓ J:\ ✓ K:\ ✓ L:\ ✓ M:\ Selected drives will to unhide. 	V:\ W:\ X:\ Y:\ Z:\ De hidden, unselect to	- Apply

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:

С НОМЕ	0				
	Backup / Restor	e your Server Parameters			
A	Advanced Settings				
	Product	Name	1 TSplus - Edit Setting	×	
WEB WEB	Security Session	Administrator pin code Use RDS role AdminTool background co	Administrator pin code		
FARM		AdminTool Language	AdminTool will ask for a password if this value is not	empty. 🗠	
SESSIONS					
SYSTEM TOOLS					
ADVANCED			Value:	*	
17. 227			1234		
ADD-ONS					
THE LICENSE			Save	Cancel	

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:

TSplus - Administration Console	- 0	×
	ACCESS $\ensuremath{\mathfrak{S}}\$ Lite Mo $\ensuremath{\mathfrak{S}}\$ Help English	ode •
П НОМЕ		1
	Protect your server from brute-force attacks and foreign intrusions. Block ransomwares before they destroy your files. Restrict users access and lock them in a highly secured environment.	
S web	V Two-Factor Authentication - Confirm your users' identity	
FARM	Passwords can be lost, stolen by phishing attacks, and very often they can even be cracked in a matter of minutes. Two-Factor Authentication solves this problem simply and effectively, and provides an additional security layer - sending a code to the user mobile device.	
SYSTEM TOOLS	TSplus Remote Support - Remotely connect to your client PCs and provide instant assistance	
ADVANCED	A secure, web-based screen sharing and remote control solution designed for today's flexible support teams. Securely connect to remote computers, take control of their mouse, access files and applications, and troubleshoot problems.	
C LICENSE		
ULCHOSE	TSplus Server Monitoring - Monitor your server TSplus Server Monitoring helps to optimize software resources and to reduce unnecessary costs. Give facts and data about server usage (CPU, Memory, I/O, Disks). Track changes, resources usage and events with real-time email alerts.	

Which brings powerful features, documented on this page.

👻 TSplus Advanced Security	X
	TSplus Advanced Security - Ultimate Protection
	Keep threats away from your Windows system.
	Prevent, protect and fight cyber attacks.
	21 Oct 16:52:53 🔇 A logon request has been granted for user WIN-A1L00CN0E56\Laura because WIN-A1L00CN0E56\Laura is whitelisted
	21 Oct 16:52:53 A connection has been authorized for user WIN-A1L00CN0E56\Laura from computer because this feature is not enabled for this user
	21 Oct 16:52:53 X No session configuration was applied to user's session WIN-A1L00CN0E56\Laura because the feature is not enabled for WIN-A1L00CN0E56\Laura
	21 Oct 16:52:53 🏃 No session configuration was applied to user's session WIN-A1LOOCNOE56(Laura because the user is whitelisted
	1 21 Oct 16:52:36 Protection against Ransomware is up and running
WORKING HOURS	
SECURE DESKTOPS	System audit - No issue found on 10/21/2019 5:09:36 PM
	Version 4.3.10.16 - You are using the latest version
	This I Licence 10 days. I Wilmshe Deshadilan edition
ស្ត្រ settings	
Or License	English •

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.

Protect your account with 2-step verification	x
Click to configure your authentication app	
Open the authenticator app on your mobile phone.Scan the QR code displayed below:	
Secret key: IMPCKUPCDGJWZOHISPHS32S456W4ERIA	
Validate your verification code obtained by SMS, e-mail or via your 2FA app	
Validate	

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.

Windows	s Client Genera	tor					_ ×
General Display	Remote Desktop client	Local resources	Program	Security	Load-Balancing	1	
Advanced clien	t security options						
	k it on PC name TOP-204950	Loci 196133	k it on seria 31728	l number			
Time lii No lim	nit: Disable this generated of Number of days from	client after some da the first use date o	ays (for exe f this gener	mple 15 da rated client	ays)		
Der	ny user from saving credent] Save username only cryption V2	iials 🗹 Enal	ble 2FA				
Advanced conr	nection options e the targeted server as a F be sure to use the specifie has a valid SSL/TLS certifi	Remote Desktop Ga d server's Domain cate installed.	ateway (RE Name inste)G) to encr ad of its IF	ypt data transfer 9 address. Also be	e sure the	
Client location: Client name:	C:\Users\admin\Desktop John-44.connect	þ	Brov	vse		Create Client	:

For more security feature informations, check TSplus Portable Client Generator documentation and our FAQ.