Fine-Tune the Level of

Remote Desktop & Cloud Server Security

with

TSspeedbooster Security Add-on

When it comes to exposing Remote Desktop Protocol to direct connections, you need a solid secure server to protect your systems against remote attackers. Due to the innovative techniques available for modern cyber-criminals and a use-after-free vulnerability in the Microsoft solution, **hackers from all across the globe can easily access login credentials anywhere at all, carry out ransomware attacks and run arbitrary code on the targeted systems.**

Meanwhile, our team of qualified experts has worked hard to secure your remote desktop access. Born from the clear understanding of the problem, **TSspeedbooster Security Add-on** offers advanced functionality and makes the use of remote access in your daily routine as safe as possible. Now, with **TSspeedbooster Security Add-on** you can easily manage the entire fleet of workstations even if you are a thousand miles away.

Keep your Server Secure

If you want to log into your personal computer from another location, **TSspeedbooster Security Add-on** is your sword and shield for protecting your server environment against unauthenticated attackers. **Our product is designed to secure remote desktop, monitor login failures, block prohibited or suspicious IPs and prevent unauthorized actions.** Checking your computer's remote access options, **TSspeedbooster Security Add-on** provides you with excellent control over the connected users with granted access.

Access your Workstation Safely

Using the RDP Defender service, you can create a whitelist with dedicated IPs you need to achieve the server, and set the essential number of incorrect password attempts. Typically, setting the maximum failed login attempts from a single IP is an effective countermeasure for avoiding brute-force attacks.

If you want to secure server login and allow connections only from specific countries, be assured that our product will protect your system against any foreign attackers. On top of that, our cyber crime fighter offers endpoint protection and device control for regular checking of the device names approved for any incoming session.

Remember, **HACKERS AND MALICIOUS BOTS NEVER SLEEP.** With **TSspeedbooster Security Add-on**, you can hook into your workstation anytime, anywhere without the fear of external attacks. **Contact us today, add this outstanding tool to your arsenal, and use remote access to its full potential.**

TSspeedbooster Security Add-on exists in Two Editions:

- **TSspeedbooster Security Add-on (Essentials) is the best package to keep your Remote Desktop connection safe, with great protection features.** It is the low-cost security solution you can even apply to all W7/W10 Pro RDP accesses.

- **TSspeedbooster Security Add-on (Ultimate) is the security tool every Windows Server administrator "Must Have":** it provides all that you need to effectively protect your users' environments and prohibit malicious actions.

Included features are detailed below.

The 360 Degree Approach to Security

TSspeedbooster Security Add-on (Essentials) provides three major protections:

- Homeland Protection: prevents foreign attackers to open a session.
- Prevents Brute-Force Attacks: blacklists the offending IP addresses.
- Working Hours Restriction: prohibits users to connect at night (for all Users).

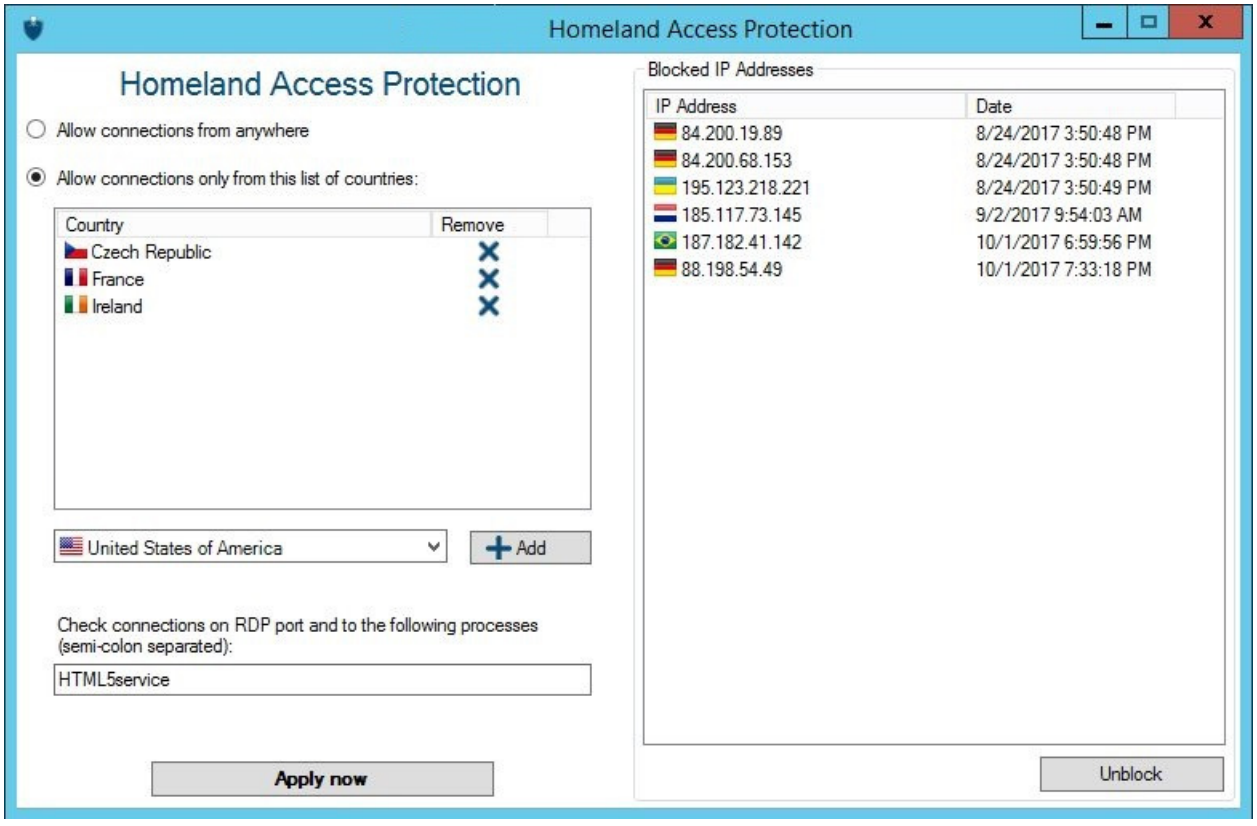
TSspeedbooster Security Add-on (Ultimate) provides all protections you need:

- Homeland Protection: prevents foreign attackers to open a session.
- Prevents Brute-Force Attacks: blacklists the offending IP addresses.
- Working Hours Restriction: prohibits users to connect at night (per Users or per Groups).
- One Click to Secure Desktop: provides highly secured user's environment (per Users or per Groups).
- End-Point Device Protection: restricts access per device (per Users).

Geo-Restriction for RDP

Your users are located in USA, UK and Canada offices. **Why anyone should be able to open a session** from China, India, Iran, or Germany?

In a snap, you protect your RDS servers from any attackers trying to open a session from foreign countries. This is extremely simple and so powerful. Just do it!

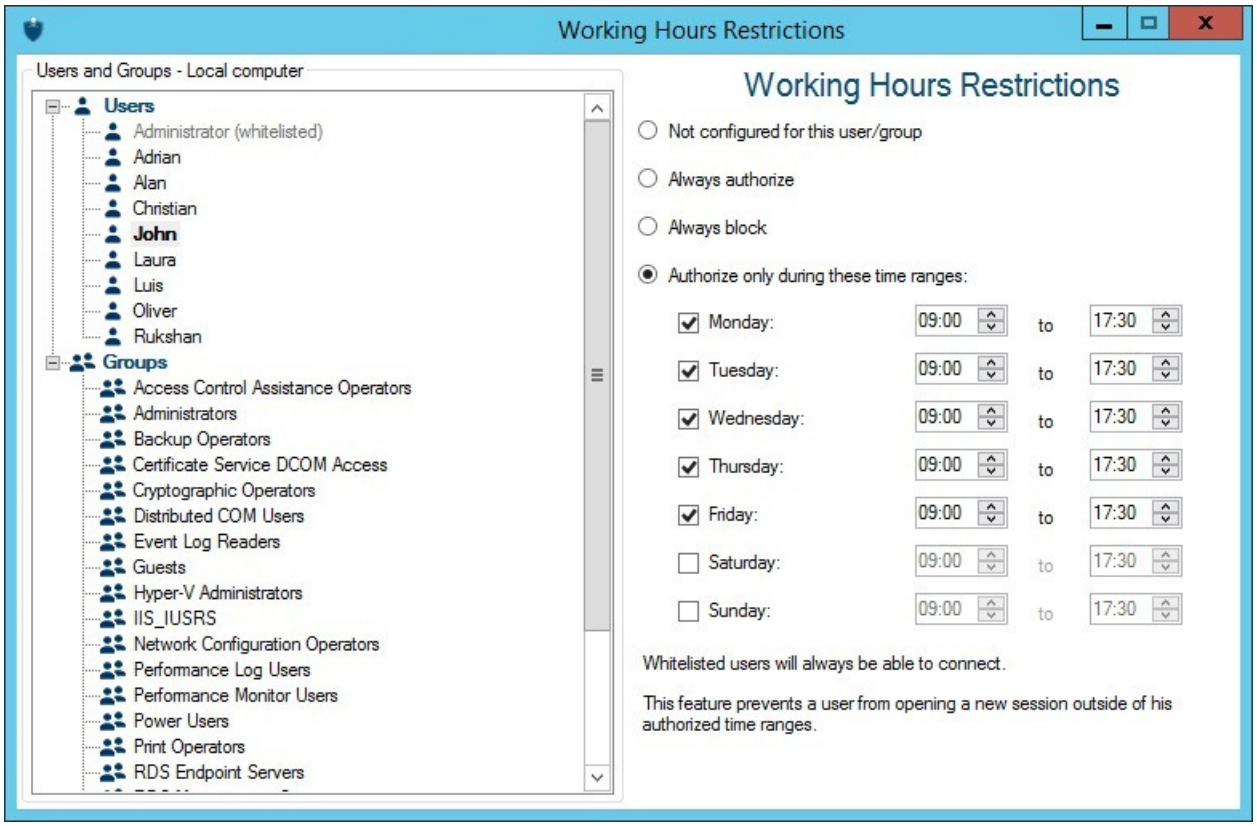


Protect your Servers at Night

Of course, your users should be free to connect and to work when they are at their desks. However, why would they be allowed to open a session at midnight?

You can **specify the working time of the day when each of your user or group are allowed to open sessions**.

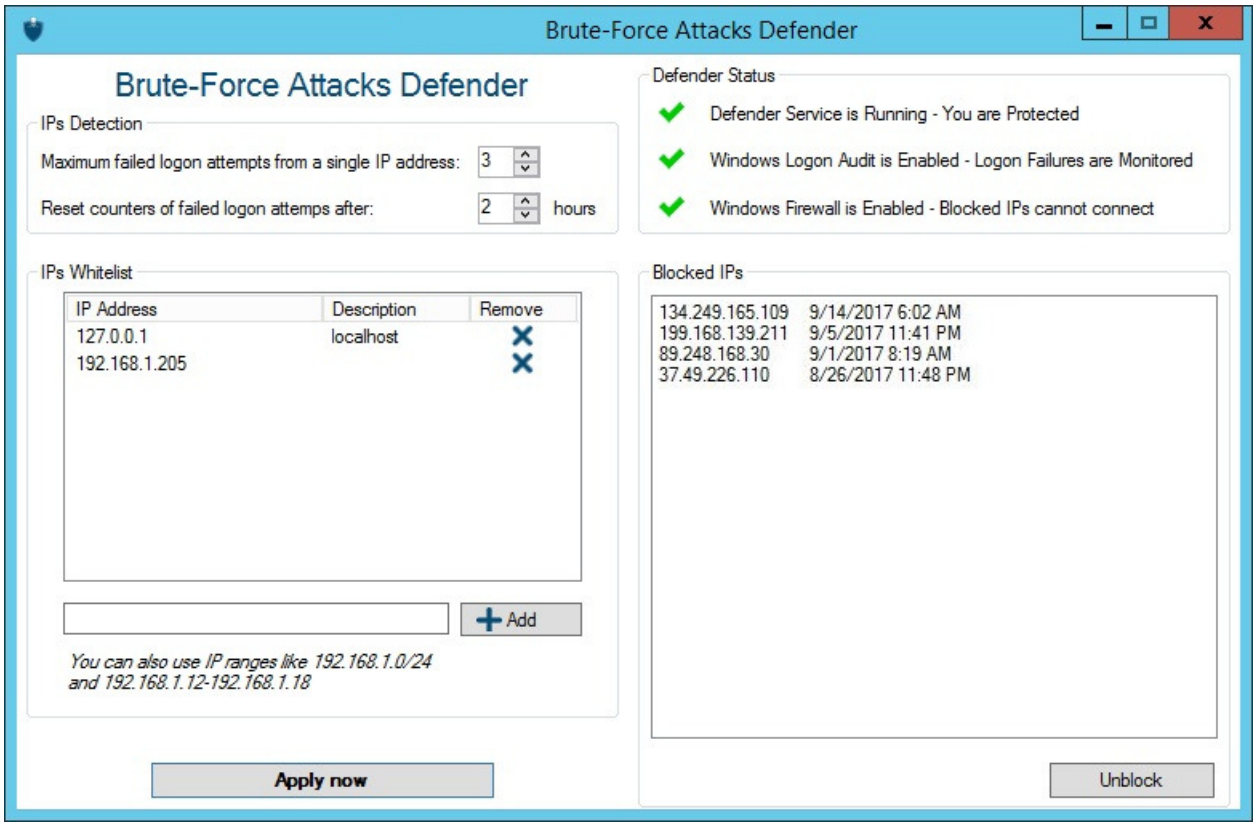
It will be so easy and amazingly nice to enhance your security policies.



Block Brute-force Attacks

If your Windows server is publicly available on Internet, then there is a 100% probability that **hackers, network scanners and brute force robots** are trying to guess your Administrator login and password – as we speak. Using current logins and password dictionaries, they will automatically try to login to your server hundreds to thousands times every minute. Not only this is **bad for your server's security**, but it can also **consume a lot of its resources** (CPU and bandwidth)!

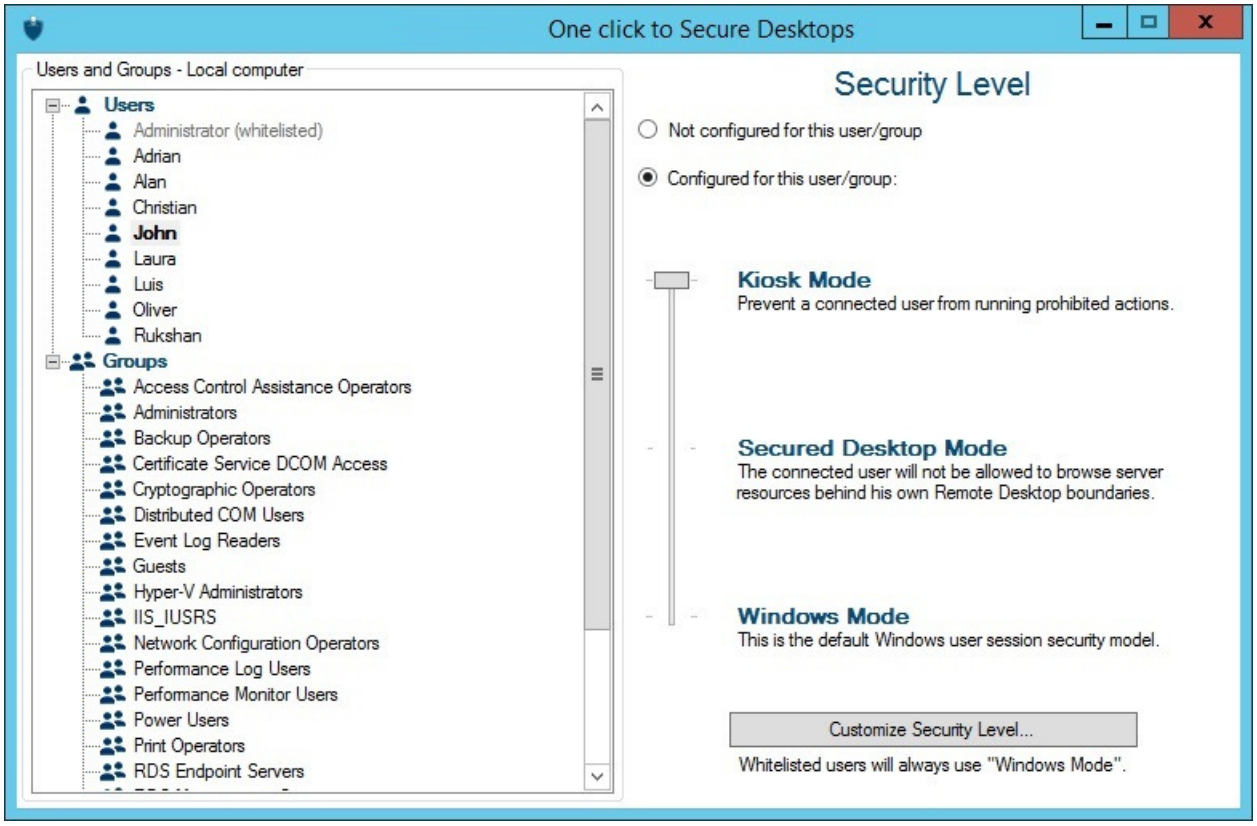
Stop the constant attacks right now with **TSspeedbooster Security Add-on** brute-force attacks defender. It **will instantly protect your server** by monitoring Windows failed login attempts and automatically blacklist the offending IP addresses after several failures. Moreover, you can of course configure it to match your needs.



One Click to Set User Rights Policies

Windows is providing many powerful GPOs but it will cost you several days to enforce the expected security rules. Most of us are not comfortable enough with such kind of system restriction policies; as a result we give up on it or we select only few of them.

In one click, TSspeedbooster Security Add-on will enforce for you the best security practice. In few minutes, you will get the best level of security that you expect to achieve for your Remote Desktop user's environment. It is as easy to do it **"user per user",** or to set it up **"per group"**. More than a time-saver to protect your server, TSspeedbooster Security Add-on is providing you more security without complexity.



Device Protection

Why should a hacker be able to use a stolen Windows credential to open a session from any device? This should be prevented. The **EndPoint Protection** is the right answer. It will bind the user's credential to the user's own device.

How does that work? **TSspeedbooster Security Add-on** will record the user's device name at his first connection. The administrator can decide to **restrict access for this logon** to that recorded device's name. Doing so, any attempt to connect from another device will be automatically detected and rejected.