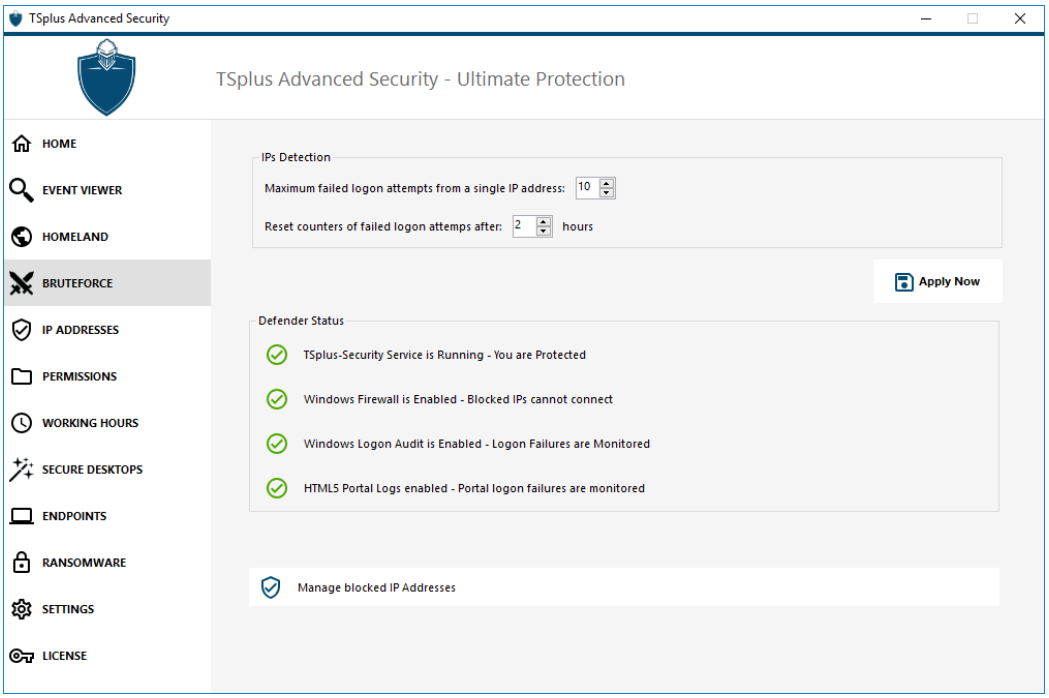
Bruteforce Attacks Defender

The Bruteforce Attacks Defender 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.

With this RDP Defender, you can monitor Windows failed login attempts and automatically blacklist the offending IP addresses after several failures.



- You can set the **maximum failed logon attempts from a single IP address inside the IPs Detection block** (by default, it is 10), as well as the time of reset for failed logon attempts counters (by default it is 2 hours).

- On the bottom of this window, you can see the **Defender status**, where you can check if the HTML5 Web Portal logon failures, the Windows Logon Failures are monitored and if the Windows Firewall and advanced-security service are enabled.
  In this case, like in our example, all the status are ticked.

- **Manage Blocked IP addresses**: You can of course configure it to match your needs, for example by adding your own workstation IP address in the IPs Whitelist, so this tool never block you. You can add as many IP addresses as you want in the whitelist. These addresses will never be blocked by the brute-force attacks defender.

- You can **ignore Local and Private IP Addresses** by changing the default setting on the Settings > Advanced > Bruteforce tab

Note: If you ever notice that the Brute-Force Attacks Defender blocked 10 IP addresses per day and that now, it is not the case anymore; and blocks one, two or even doesn't block any address, it is actually normal. Indeed, before advanced-security installation, the server having an RDP port publicly available is known by all the robots, and many robots try the current passwords and the ones coming from dictionaries. When you install advanced-security, these robots are

progressively being blocked, so that one day:

- Most of the active robots are already blocked and are not interested by the server, even the new ones.
- Also, the server does not appear anymore on the list of publicly known servers.