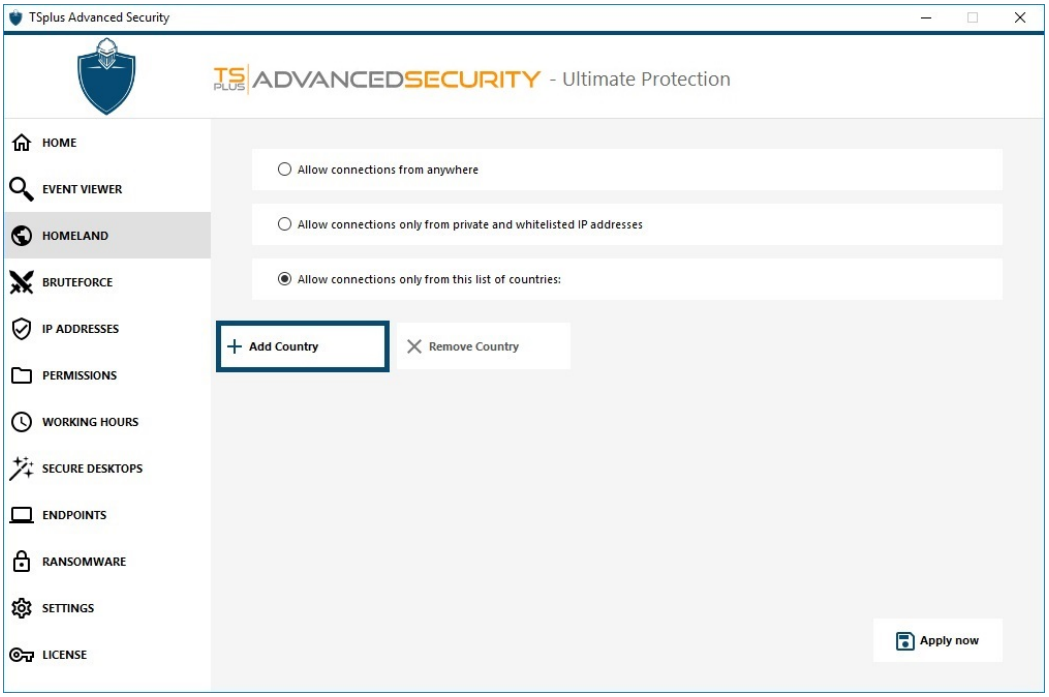
Homeland Access Protection

Restrict access from other countries

To allow remote access from only specific countries, select the "Allow connections only from this list of countries" button and then click on the "Add country" button.

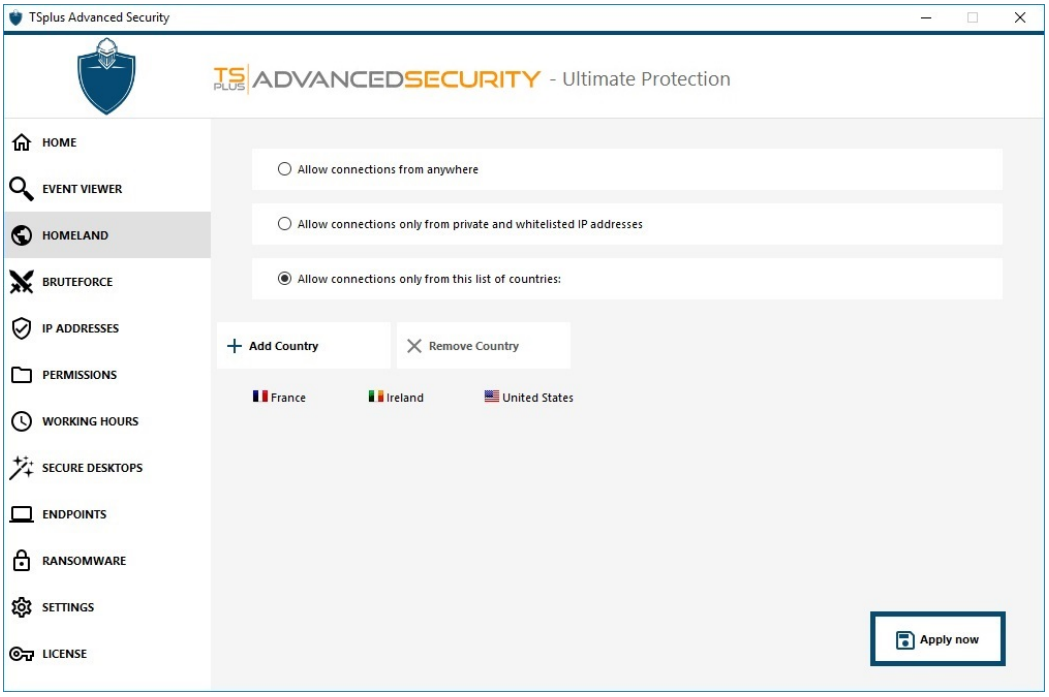


A popup offering a country list opens. Select the country you wish to add on the list.

You can choose to check the box below to unblock all previously blocked IP addresses for the selected country.

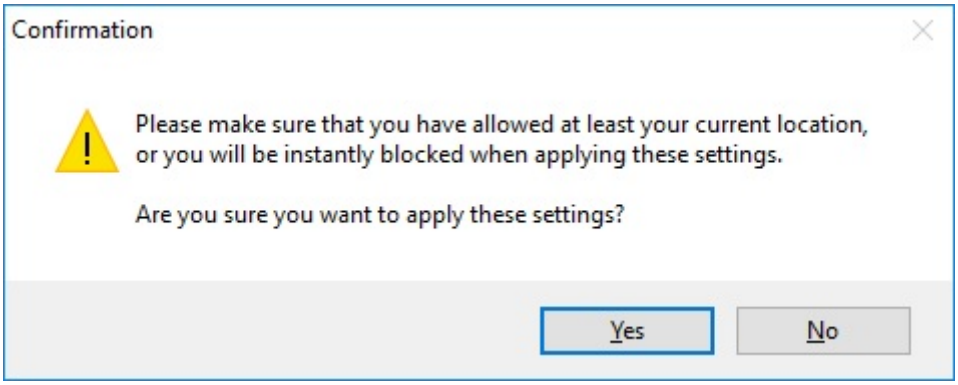
Click on the button "Add Country" to return to the feature main screen.

Important: In order to save your changes, click on the "Apply" button.



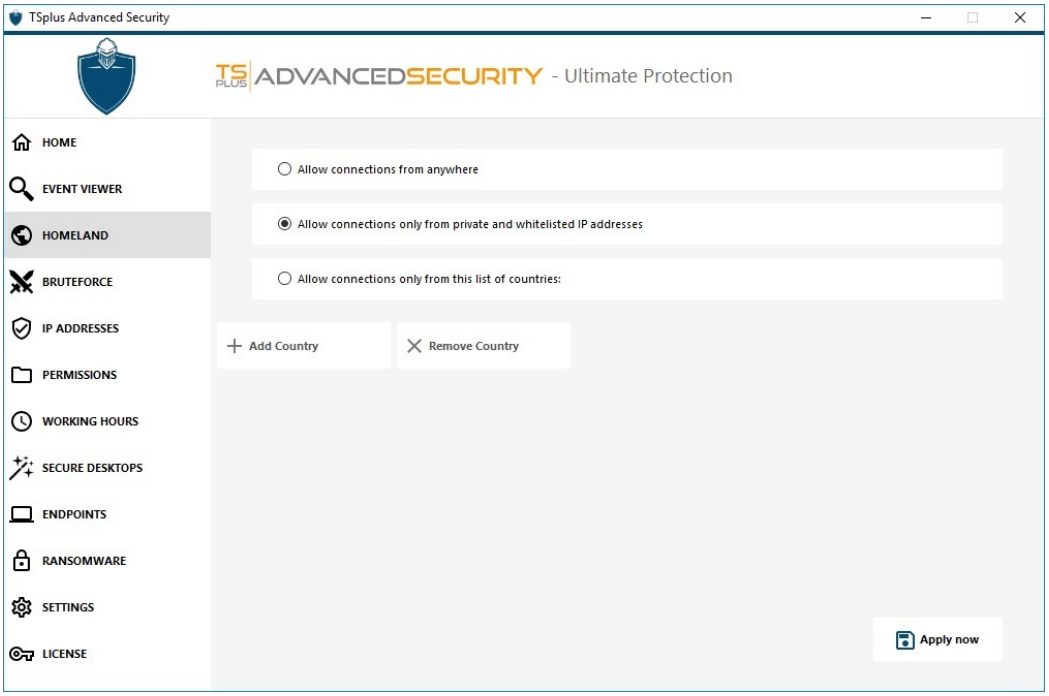
In this example, remote access is allowed for users connecting from United States, Ireland and France.

A confirmation message appears to avoid blocking the connected user. Click "Yes" to confirm and apply the changes.



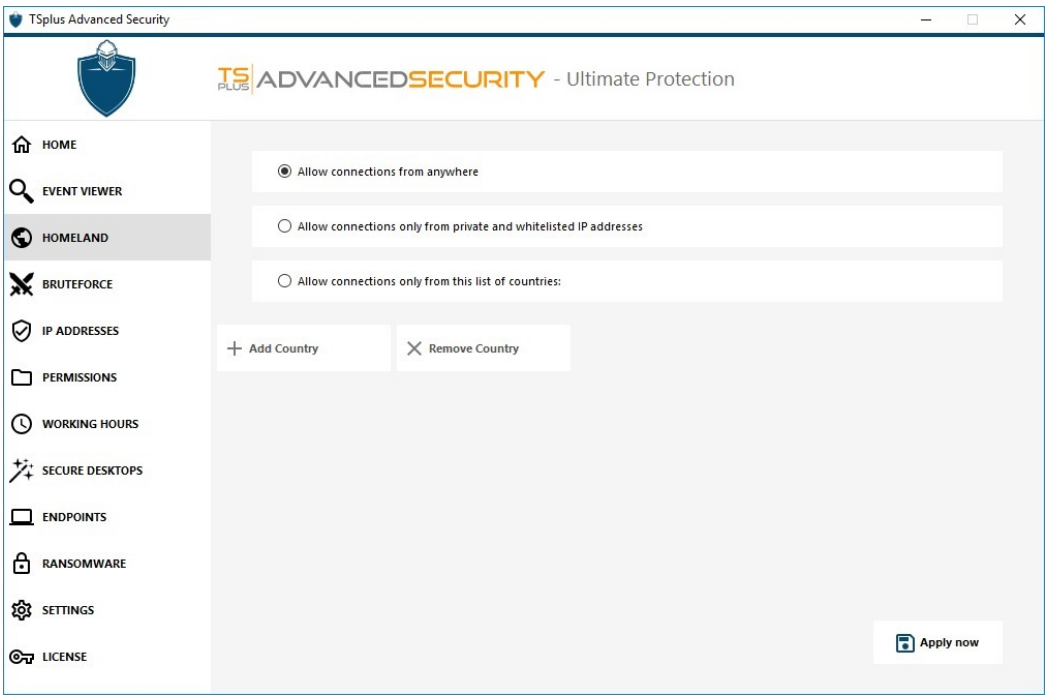
Restrict access from the internet

Homeland can be configured to restrict the access to your machine to only private and whitelisted IP addresses, as shown below:



Disable Homeland Access Protection

By default, Homeland Access Protection allows access for users connecting from all over the world:



Unblocking blocked IP addresses

When an IP address gets blocked, it appears on the IP Addresses. Blocked IP addresses can then be unblocked and eventually added to the list of allowed IP addresses.

If you get blocked, we recommend that you try connecting from any country you allowed on TSplus Advanced Security, for instance by connecting from another remote server or using a VPN service. You can also use a console session to connect, as this session is not a remote session and will not be blocked by TSplus Advanced Security.

Important:

- Check that you have selected the country where you are currently connected from. Otherwise, your IP address will be blocked quickly after applying the settings, thus disconnecting you without any hope of connecting back again from the same IP address.

- Consider adding your own IP address to the list of allowed IP Addresses to avoid being blocked by either Homeland Access Protection or Bruteforce Protection features.

Undestanding Homeland Access Protection

Homeland Access Protection checks incoming TCP network connexion, both IPv4 and IPV6 (except when the legacy Windows API mode is configured).

Processes: Homeland Access Protection listens to connexions sent to the TSplus Remote Access' Web server by default, if installed. The name of the corresponding process is HTML5 Service. If you wish to disable its monitoring or check connections destined to other processes, go to Settings > Advanced > Homeland.

Network ports: by default, Homeland Access Protection listens to default ports used for connecting remotely to a server. These ports include RDP (3389), Telnet (23) and VNC. Homeland supports the following VNC providers: Tight VNC, Ultra VNC, Tiger VNC and Real VNC, which are not related whatsoever with TSplus. If you wish to disable its monitoring or check connections destined to other ports, go to Settings > Advanced > Homeland.

Detection mechanisms:

Homeland detects inbound connections from unauthorized countries using three differents detection mechanisms:

- Windows API
- Event Tracing for Windows
- Built-In Firewall

On the one hand, Event Tracing for Windows is an efficient kernel-level tracing facility that capture network events in real time. Event Tracing for Windows is recommended with Windows Firewall enabled (default).

On the other hand, Windows API works great given any specific network configuration but may add a constant pressure on CPU depending on the amount of active connections. Please note that Windows API is not compatible with IPv6 yet.

Built-In Firewall enables user-mode capturing and dropping of network packets sent to the Windows network stack. When the Built-In Firewall is configured to block unwanted connections, it is recommended to use it to enforce Homeland's allowed countries.

Geolocation: Advanced Security includes geolocation data published by MaxMind, available from http://www.maxmind.com. If you find an IP address not registered in its actual country, please contact MaxMind directly to fix the issue.

Troubleshooting

If you ever notice that Homeland Access Protection does not block connections coming from a country which is actually not in the authorized countries' list, it is certainly because:

Antivirus: In order to block an IP address, Homeland Access Protection adds a blocking rule on the Windows firewall. So, firstly, the firewall must be active. You also have to check if some firewall parameters are not handled by an other program, like an antivirus. In this case, you will have to deactivate this program and restart the service "Windows Firewall". You can also contact your third-party program editor and ask them to find a way for their program to respect the rules when added to the Windows firewall. If you know any software editor's technical contact, we are ready to develop these "connectors" for the firewall. Contact us.

VPN: In case the remote client uses a VPN, Homeland Access Protection will get an IP address chosen by the VPN provider. As you know, VPN providers use relays all around the globe to allow its users to browse anonymously. Some VPN providers allow users to define the relay’s country. Thus, users with VPN providers may be relayed through an unauthorized country. For example, if a VPN provider choses an IP from Sri Lanka, this country must be authorized by Homeland Access Protection. Also, if the VPN uses an internal corporate IP address, then the protection becomes irrelevant.

Firewall / Proxy: The purpose of an hardware firewall is to filter incoming and outgoing connections for large companies. As it is only a filter, it should not modify the originating IP address and therefore should not impact Homeland Access Protection. However, a proxy would definitively change the originating IP address to use a private network address, which will always be allowed by Homeland Access Protection. The primary purpose of this feature is to block access to a server opened to the Internet. If all connections comes from the corporate network, then the protection becomes irrelevant.