

Use of the TOR browser in TightGate-Pro

TOR is an overlay network for anonymising connection data. It is used for TCP connections and can be used in TightGate-Pro for anonymous surfing on the Internet. Tor protects its users from having their data traffic analysed. It is based on the idea of onion routing. **TOR** was originally an acronym for **The Onion Routing**.

At TightGate-Pro, m-privacy GmbH offers the TOR browser as an optional package. In this optional package, the TOR browser contains a TOR proxy and the version of the TOR browser preconfigured by the TOR project (Mozilla Firefox ESR). Details about the design of the TOR browser can be found on the Tor Project website at the following link:

<https://2019.www.torproject.org/projects/torbrowser/design/>

Architecture

Due to its architecture and functionality, the TOR browser has some special features that should be taken into account when preparing to use the TOR browser at TightGate-Pro. A description of how the TOR network works can be found at the TOR project under the following link:

<https://tb-manual.torproject.org/de/about/>

Preparations

The architecture of the TOR browser means that TightGate-Pro either has free access to the Internet (port 443 TCP) when using the TOR browser or an SSL/https-capable proxy must be set as an uplink proxy at TightGate-Pro.

Please make sure that:

- TightGate-Pro can either connect directly to the Internet (port 443 TCP protocol) or that an SSL-capable proxy is used for TightGate-Pro -> [Link to set the proxy settings in TightGate-Pro](#) .
If TightGate-Pro can connect freely to the Internet, a non-SSL-capable proxy can also be entered as a proxy in TightGate-Pro. The proxy is then used for all connections with Firefox and Chrome and the TOR browser connects directly to the TOR network via the free Internet access.
- The proxy must be up-to-date at TightGate-Pro.

Installation

To install the TOR browser at TightGate-Pro, please proceed as follows:

- Login as administrator **update**
- Call up the menu item **Add optional packages**
- Select the package **tor-browser**

After installation, the TOR browser is available.

How to use it

In order to use the Tor Browser, it must first be activated. The TOR browser can then be assigned to individual identifiers.

Activate TOR Browser globally

- Login as administrator **config**
- Select the menu item **System Preferences > Tor Browser Support:** and set the value to **Yes** Change
- **Save** and **Apply** the setting.

Assigning the TOR browser to identifiers

The TOR browser in TightGate-Pro can be accessed in two different ways. Firstly, the browser can be started directly via the **start menu** in the directory **Internet** directory or you can add a new icon to the menu bar for individual users or user groups to start the TOR browser.

- Login as administrator **maint**
- Select the menu item **User administration → Menu options:**
- Please select the ID or group to which you want to assign the TOR browser icon.
- In the interface menu options, select **tor** in the interface menu options. The selection is made with the **space bar**.



- Once selected, the new icon can be used and will appear on the menu bar the next time you log in via TightGate-Viewer.

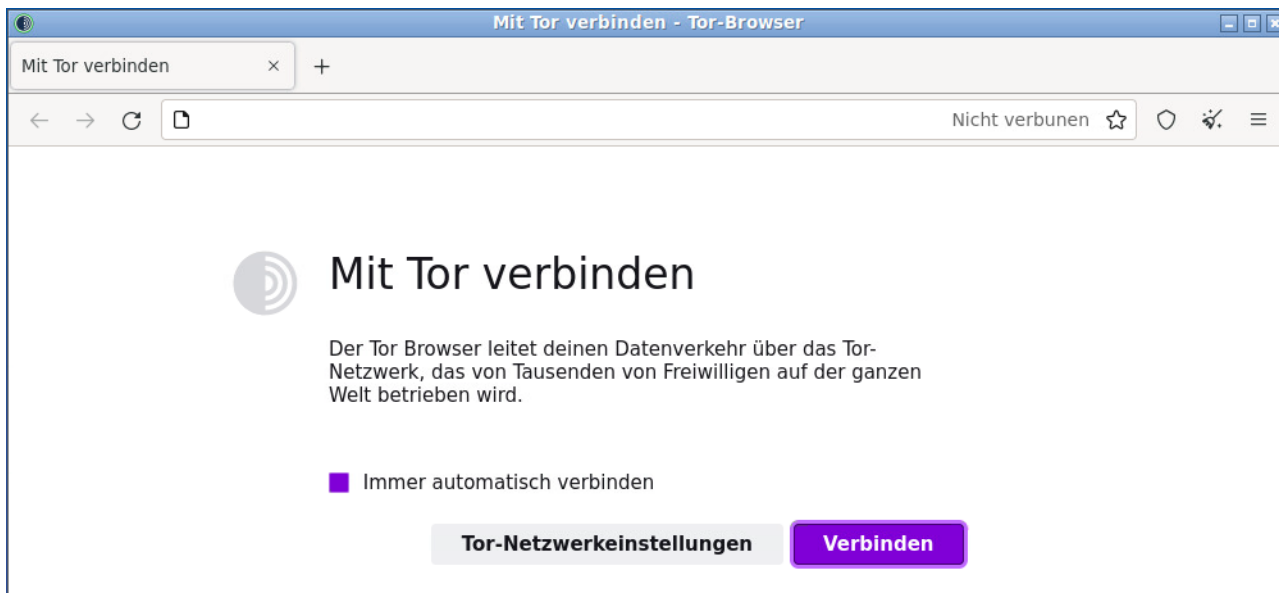
Note

If user authentication takes place via Active Directory, all user IDs that are to use the TOR browser must be added to the AD security group **TGtoricon** security group. An overview of all AD security groups can be found here: [Overview of AD security groups for TightGate-Pro](#) .

Start and first connection



- The TOR browser is started by clicking on the new icon on the menu bar.
- The TOR browser then opens with the following start screen:



- Although the start screen prompts you to connect, this is not necessary as the connection has already been established automatically in the background. It is also not necessary to configure the TOR network settings, as all settings are already preconfigured. As usual, a desired URL can be entered in the address bar of the browser.

Further instructions on using the TOR browser can be found at the TOR project under the following link: <https://support.torproject.org/de/>

Caution

No additional add-ons should be installed for the TOR browser, as this may impair some of its data protection functions.

From: <https://help.m-privacy.de/> -

Permanent link: https://help.m-privacy.de/doku.php/en:faq:tightgate_pro_tor-browser

Last update: **2024/01/28 20:12**

