Proxy

TightGate-Pro can work with multiple proxies. The following overview explains the configuration.

Settings for Uplink Proxies

Menu item	Description
HTTP Proxy (external)*	IPv4 address(es) of the HTTP proxy server(s) through which all HTTP accesses to the Internet are routed. The port used must be the same for all registered HTTP proxy servers and is specified in a separate menu option. If several servers are entered, they are addressed automatically either by the Round Robin procedure or in a certain order. The accesses are weighted according to access speed, unavailable servers are automatically skipped. **Caution:** In most cases there are only servers in the network which have to be entered here with an explicit IPv4 address. In the exceptional case in which DNS names that can be resolved here are referenced, the network concerned must be specified exactly in the HTTP proxy network menu item. Furthermore, a DNS server must be entered which can resolve the proxy name. Otherwise a correct connection to the respective proxy servers is not possible.
HTTP Proxy Order (external)*	If several proxy servers have been entered, this option can be used to specify the selection procedure. The Round-Robin procedure and the address in a certain order are available. **Hint:** If only one proxy server is entered, this menu option is not displayed.
HTTP Proxy Port (external)*	Specifies the port to be used for contact with the HTTP proxy servers entered. The setting must be the same for all referenced HTTP proxy servers.
HTTP Proxy Network (external)*	If a resolvable DNS name is entered as proxy server, the system absolutely needs the information about the IPv4 addresses behind it. The IPv4 address must be specified in the form [IP address/Valid Bits].
HTTP Proxy SSL/https (ext)*	Select whether the proxies are addressed via HTTPS or HTTP.
HTTP Proxy Login (ext)	If the proxy logon requires a user authentication with user name and password, the user name can be stored here.
HTTP Proxy Password (ext)*	If the proxy logon requires a user authentication with user name and password, the password can be stored here.
Enable HTTP Pipelining*	HTTP Pipelining is a technique in which multiple HTTP requests are passed to a single socket without waiting for a response. Especially for connections with high latency, this can mean a significant reduction in page load times. Disabling can help if loading HTTPS pages repeatedly hangs over the uplink proxy.

Proxy exceptions

Via the menu item ***Proxy > Proxy exceptions*** you can set IPv4 addresses or URLs of websites that should not be routed via the external proxy. The exceptions are set in the browser settings of the TightGate-Pro users each time they log in.

Attention: All proxy exceptions entered here must also be entered in the menu under ***Network > HTTP Server***.

Proxy Filter (Web Filter)

In addition to the display of content from the Internet, TightGate-Pro also offers the possibility of content control and restriction of Internet use. The web filter of TightGate-Pro works as a forced proxy and filters the data retrieved from the Internet according to definable criteria. The following categories are taken into account:

- Predefined blacklists for URLs and domains
- Manually defined blacklists and whitelists for URLs and domains

General information about the web filter

The functionality of the web filter is similar to that of a malware filter. There are predefined lists of unwanted content (blacklists) that are assigned to different categories. If the web filter is active and categories are selected as unwanted content, TightGate-Pro forwards each request for a website to the internal web filter for checking. This checks whether the page is on a list (blacklist) with unwanted content. If this is the case, the web filter will indicate that access to the corresponding page has been blocked instead of the content of the page. In principle, the check for admissibility of a page is based on the principle "whitelist before blacklist". If a domain or URL is noted on the whitelist in the system, access is always permitted.

Boundaries of the web filter: A content filter is only as accurate as its lists. These have a limited scope and require regular maintenance. m-privacy GmbH offers two different lists which are maintained by third parties. The m-privacy GmbH therefore assumes no liability for the completeness and content of the lists.

Exkurs on the web filtering of HTTPS-encrypted pages
In the course of web filtering, HTTPS connections to TightGate-Pro can be broken. This is the only way to ensure URL-accurate filtering of the retrieved Web content even for HTTPS accesses. If the proxy filter integrated in TightGate-Pro does not want HTTPS connections to be broken, only domain-based filtering of encrypted Web content retrieved is possible. **Attention:** We recommend that you consult the relevant data protection officer or IT security officer before activating the feature.

Configuration of the central web filter

To turn on and configure the web filter, follow these steps:

How to do it:

- Login as administrator ***config***.
- Select the menu item **Proxy > Proxy Filter** and switch on the web filter via the selection **Yes**. This activates the web filter and further menu items are available.
- Check whether the HTTPS connections should be broken so that the web filtering does not only include domains but also URLs. If this is the case, select the menu item Break **HTTPS connections** and confirm with **Yes**.
  Note: Please note the above information on breaking HTTPS connections and discuss this

function in advance with your internal data protection or security officer.
Caution: Web filtering of HTTPS-encrypted pages can currently only be performed if no upstream HTTP proxy is used.

- If the web filter is active and a web page with an invalid certificate is called, the web filter denies access. If this page or domain should still be accessible, it can be entered in the menu item **Domains without certificate check.**. Afterwards the web filter ignores the wrong certificate.
- Via the menu item **Access Denied Text** an individual text can be stored which is displayed to users if access is denied.
  Hint: An administrative contact should be displayed here, e.g. the telephone number of the local helpdesk. In this way, users can report pages that have been blocked by mistake and have them activated if necessary.
- Via the menu item **Number of filter groups**, you can define how many different groups there should be for the web filter. Each group is assigned its own category.
- In the last step the respective web filter groups are to be provided with categories. There are two options to choose from:
  a) Prohibit everything and only allow the contents of the whitelist (created as ***maint*** under **Web page filter > Activate domains** and **Web page filter > Activate URLs**; menu item **Only whitelists**)
  b) Allow everything and only prohibit unwanted content per category (menu item **Categories (Block List)**).
- The settings in the main menu **Save** and **Apply Gently**.
- Login as administrator ***maint*** and assign a filter group to users or groups via the menu item **User Administration > Filtered Web**.

Configuration of the individual web filter

In addition to using the central white and black lists, TightGate-Pro can be extended with individual settings. This makes it possible to add individual domains and URLs to your own blacklists and whitelists.

This is required: → Activated proxy filter (web filter) → Assignment of users to the filtered Web

How to do it:

- Log in as administrator ***maint.***
- Selection of the menu item **Web page filter**. The following configuration options are available:
  Lock domains: Enter the domains to be blocked by the content filter. The domain can also be specified using wildcards (*). Example: The domain of EBAY can be completely forbidden for all countries with www.ebay.*.
  Block URLs: Enter the URL which should be blocked.
  Please note: Only the exact pages that will be blocked will be blocked. This option is not suitable for blocking complete domains.
- **Unlock domains** and **Unlock URLs**: These settings work analogously to the setting for domain blocking and define the whitelist for TightGate-Pro.
- The settings must be activated via the menu item **Soft Apply**.

Bypass content filter for individual users

TightGate-Pro provides the ability to bypass content control for individual users. The bypass of the content filter for individual users or groups is configured by the administrator ***maint*** under the menu item **User Administration > Filtered Web**.

Hint: If a user has unfiltered access to the Web, no content control is performed for this user. When a user switches from filtered to unfiltered web (or vice versa), he or she must log on to TightGate-Pro again for the setting to become active. A restart of the browser is not sufficient.

Recording of the web access

TightGate-Pro provides the ability to log web access from users. To protect data privacy, anonymization and pseudonymisation functions are already implemented during logging.

How to do it:

- Logon as administrator ***config.***
- If the logging should not be anonymized, it is to be determined under the menu option **System Preferences > Pseudomyization** whether the logging contains the clear name of the user or whether pseudonyms are used instead.
- The next step is to activate logging under the menu item **Proxy > Logging** and to determine whether an anonymous proxy protocol or one with identifiers (clear name or pseudonym) should be created.
- Furthermore, it is absolutely necessary to define a lifetime for the proxy protocol, otherwise the logging will not work. The protocol lifetime is defined via the menu item **Proxy > Protocol lifetime** and is specified in days. After the storage period has expired, the log files are deleted and cannot be reconstructed. If a 0 is entered, no logging takes place.
  Note: If proxy logging is switched off, this menu option is not displayed.
- The main menu settings **Save** and **Soft Apply**.