Network

This menu is used to configure the network interfaces and the accessible servers. Below is an overview of all the menu options:

Menu item	Description
Network interfaces	Configuration of the network interfaces available in TightGate-Pro. The settings must be configured in accordance with the operating environment.
Enable IPv6	Enables or disables IPv6 support in TightGate-Pro. Even if this option is not enabled here, IPv6 addresses can still be entered for all IP addresses in TightGate-Pro. However, these will only be used if IPv6 support has been enabled here.
—	
Name servers*	IPv4 or IPv6 addresses of name servers via which TightGate-Pro resolves DNS names. A maximum of 5 entries are permitted. The name servers are queried in the order listed in the entries should individual servers be unreachable.
Local domain name servers*	Specification of locally used domains and the associated name servers. This setting is particularly important for Active Directory connections if the AD server cannot or is not permitted to perform DNS resolution on the internet. A maximum of 10 entries are permitted. **Caution:** As a rule, reverse resolution (IPv4 address → DNS name) must also be specified in a separate entry.
Time servers*	IPv4, IPv6 address or DNS name of time servers from which TightGate-Pro obtains its system time. A maximum of 6 entries are permitted. The time servers are queried in the order in which they are listed, in the event that individual servers are unavailable. **Note:** A DNS name for a time server can only be entered if it can be resolved at the time of entry. **Warning:** The correct system time is of particular importance in a cluster environment. Time discrepancies between computers within a cluster can lead to operational disruptions!
—	
Client networks*	IPv4 or IPv6 address ranges that are permitted to connect to the TightGate-Pro. If a specific gateway is required for a client network, this must be specified directly in the format [IP address/valid bits/gateway]. A maximum of 25 client networks may be defined. **Note:** Access from TightGate-Pro to services/servers located within the client networks is strictly prohibited. **Warning:** The client network must not be defined with the address range 0.0.0.0/0, as otherwise no internet access will be possible.

Menu item	Description
Privileged clients*	IPv4 or IPv6 addresses that are to be granted privileged access to TightGate-Pro. TightGate-Pro distinguishes between two limits up to which user logins are permitted. These are defined in the licence for TightGate-Pro. The first limit refers to the number of regular users; the second limit refers to the number of privileged users. Once the limit on regular users has been reached, only privileged users will be admitted – provided that the limit for them has not yet been reached. Once the second limit has been reached, any further connection attempts by a client to TightGate-Pro will be rejected with a corresponding error message. Privileged clients are not only admitted in accordance with a separate quota, but are also allocated a larger share of RAM, storage and CPU time on TightGate-Pro. **Note:** Privileged clients can also be set up using the user ID. This is done in user management by the administrator ***maint***.
Mailserver*	IPv4 or IPv6 addresses of email servers that may be accessed directly via TightGate-Pro. The addresses must be specified in the format [IP address/valid bits]. A maximum of 25 entries are permitted. **Note:** An email client (Thunderbird) is already implemented in TightGate-Pro. **Caution:** The email servers must not be located within the defined client networks!
Administration networks*	Specification of IP addresses or IP network ranges that allow administrative access (for the roles ***config, maint, update, backuser, root*** and ***security***) to TightGate-Pro. If a network is configured here, the following menu item appears, under which the port for administrative access via SSH can be set.
Administrative SSH ports*	Selection of the alternative SSH port through which the administrative networks gain access to TightGate-Pro. The available ports are 22, 222, 2222 and 22222. **Caution:** If you set a port other than the default port 22, please ensure that the firewall rules in your network are correctly configured to allow access from the administration networks.
Nagios/SNMP networks*	Specify all IP addresses of monitoring servers that are to monitor TightGate-Pro. For monitoring, the relevant service (NRPE/SNMP) must be enabled under the dienste.
SSH servers*	IPv4 or IPv6 addresses of servers that may be accessed directly via SSH at TightGate-Pro. The addresses must be specified in the format [IP address/valid bits]. A maximum of 25 entries are permitted. **Caution:** The SSH servers must not be located within the defined client networks!
HTTP server*	IPv4 or IPv6 addresses of servers that may be accessed directly (without a proxy) via HTTP at TightGate-Pro. Each address must be specified in the format [IP address/valid bits]. A maximum of 25 entries are permitted. **Note:** If, under **Proxy > Proxy Exceptions** , these must also be explicitly entered here, as otherwise the servers may not be accessible. **Caution:** The HTTP servers must not be located within the defined client networks!
HTTP ports*	Specify which ports the **HTTP servers** . **Note:** This menu option is only available if HTTP servers have been entered.
RDP/Citrix servers*	IPv4 or IPv6 addresses of Citrix servers that may be accessed directly via TightGate-Pro. The addresses must be specified in the format [IP address/valid bits]. A maximum of 25 entries are permitted. **Note:** A corresponding client programme (remmina) is already implemented in TightGate-Pro. Its use is described in the User Manual under 'Remote Desktop Connections to CITRIX and Windows Servers'. **Caution:** The Citrix servers must not be located within the defined client networks!

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

Permanent link:
https://help.m-privacy.de/doku.php/en:tightgate-pro:konfiguration:netzwerk

Last update: **2026/07/27 07:27**