

# System Preferences

The System Preferences should always be configured during installation. Basic settings are made here, which also affect authentication, backup and other services.

## General system-wide defaults

The system-wide specifications have extensive implications. The following overview describes the services:

Menu item	Description
Use pseudonyms*	Determines whether the user name should be logged in plain text or as a pseudonym. For data protection reasons it is recommended to log under pseudonym.
Bookmark archive*	Activates the automatic archiving of bookmarks. If a user ID is deleted and created later under the same ID again, the archived bookmarks are automatically placed in his profile. <b>Note:</b> If bookmarks in user profiles become unusable, the user account can be reset by the administrator <b><i>maint</i></b> . Then the user can manually restore his bookmarks from the backup. If the internal bookmark database is unusable, the bookmark archive is automatically used first when the user logs on and then the profile settings.
Bookmark archive TTL*	When bookmarks are archived, a backup is written every day. With this option you specify for how many days the bookmark archive should be kept in the backup. It is recommended not to set more than 30 days. This menu item is only available if the bookmark archive is enabled.
User fullname archive*	Writes the clear names of the users to an archive. If the user is deleted and recreated with the same ID, the corresponding clear name is automatically assigned to the identifier.
User fulname archive TTL*	When archiving clear names, a backup is written every day. With this option you define for how many days the clear name archive should be kept in the backup. It is recommended not to set more than 30 days. This menu item is only available if the clear name archive is enabled.
Multiple transfer users*	If this option is enabled, <b><i>maint</i></b> can set passwords for up to 99 independent <b><i>transfer</i></b> users. <b>Caution:</b> The <b><i>transfer</i></b> users are only displayed in the administrator's menu <b><i>maint</i></b> after the administrator's administration menu has been restarted.
Allowed user IDs range*	Selects between multiple ranges where TightGate-Pro assigns UIDs for logged in users. Names of user accounts that consist of digits only cannot be in the selected range. This setting is only relevant in special cases.
Pulseaudio extra ports*	Selects a port range that should be used in addition to port 4713. The port finally used is determined by the TightGate-Viewer. Without selection, only the default port 4713 is used. <b>Hint:</b> This setting option is only used to pass audio signals to the TightGate-Viewer on terminal servers (e.g. CITRIX).
Firefox multi threading*	Enables or disables multi-threading for Firefox. If the Firefox browser in the TightGate-Pro crashes more frequently, multi-threading should be switched off.
VNC idle timeout*	Time in seconds after inactive TightGate-Viewers are automatically disconnected. The default setting is 36000s = 10 hours.

Menu item	Description
VNC session lifetime*	Time in seconds after TightGate-Viewers are disconnected in any case. An immediate reconnection is possible, the user then receives a corresponding message about the reason for the disconnection. The default setting is 86400s = 24 hours.
Max concurrent users	Defines how many concurrent user sessions are allowed on this server. The number should be in relation to the hardware used.
Max system load	Determine the maximum load of this server. The setting is not a cluster-wide setting and should only be changed in consultation with m-privacy GmbH customer service.
Password expiration time*	Defines the expiration time for user passwords. <b>Note:</b> The initial passwords assigned by the administrator <b><i>maint</i></b> are not affected by this setting. Initially assigned passwords must be changed by the user during the first login.

## System-wide defaults for users

The system-wide defaults for users can be used to configure which services are started on TightGate-Pro so that they are available for users. If services are deactivated at this point, all further settings by ***maint*** or under the menu item **User Preferences** have no effect.

The following overview describes the services:

Menu item	Description
Audio main switch*	Global activation of audio service in TightGate-Pro for users. Whether audio is available for a user is determined by <b><i>maint</i></b> . In TightGate-Pro (CC) version 1.4 Server, audio support is disabled by default.
Printing main switch*	Activates or deactivates the printing service to local desktop printers.
User shell support*	Allows users to start a command prompt (terminal).
Allow user data transfer*	The use of the File Transfer for users can be allowed or forbidden system-wide. The dedicated transfer user <b><i>transfer</i></b> always has access if he logs in from the client network or the administration network. <b>Hint:</b> If the File Transfer is deactivated at this point, menu items for the File Transfer are hidden in the <b>User Preferences</b> . The File Transfer is disabled by default in TightGate-Pro (CC) Server.
Transfer logging*	Enables or disables logging of all file transfers to and from the TightGate-Pro. Depending on the type of logging, the log is written with a clear name, pseudonym or anonymous. The evaluation of the logs is done by the special users <b><i>Revision</i></b> . <a href="#">A tutorial can be found here.</a>
Transfer logging TTL*	With this option you define for how many days the protocols for the File Transfers are kept. This menu item is only available if the transfer protocol is enabled.
Log user data transfer checksums*	Determines whether a SHA-256 checksum is created and logged for each file transfer. This menu item is only available if the transfer protocol is enabled. <b>Hint:</b> The additional calculation of the checksum can lead to delays in the system.
Allow auto-download*	Activate or Deactivate the semi-automatic File Transfer for TightGate-Pro. <a href="#">The use of the automatic File Transfer is described here.</a>

Menu item	Description
Auto-download client dir*	Sets the destination folder in which the semi-automatic File Transfer stores the downloads from TightGate-Pro. This menu item is only relevant for Windows clients. If the destination folder in the local configuration file was changed at the workstation, no value should be set here, since this overwrites the value in the local configuration file. This menu item is only available if auto-download is enabled. <b>Hint:</b> Windows environment variables such as %USERPROFILE% etc. can also be used for the target path.
Auto-dwonload Firefox Downloads*	When activated, the download directory of Firefox on TightGate-Pro will be changed to the <b>transfer/autotransfer</b> directory so that all downloads are automatically processed by the semi-automatic File Transfer. This menu item is only available if Auto-Download is enabled.
Allow to print PDF directly*	If this option is set to "Yes", PDF files are written to the spool directory of the client without further conversion and are accepted there for printing. It is not recommended to activate this option!
VNC Magic URLs*	Activates the functionality of the Link Switch. <a href="#">Instructions for the Link Switch for Windows</a> . <b>Warning:</b> For TightGate-Pro (CC) Version 1.4 Server this option must be disabled, otherwise the CC conformity will be lost.
Clipboard transfer*	Setting the permitted transmission paths when using the clipboard. <a href="#">Here you find the detailed instructions</a> .
Max user transfer TTL*	Setting a lifetime in days that files are kept in the <b>transfer</b> folder by users. After this time, the files are automatically deleted. The entry of zero leads to an unlimited retention period, i.e. no automatic deletion takes place. <b>Note:</b> If the system is used intensively by numerous users, the available hard disk space may be exceeded if the time-controlled deletion of files is deactivated or the period is too long. It is recommended to set a time period of 7 days.
Import custom CA*	Provides the possibility to import your own Certification Authority (CA). This is added to the standard Firefox browser, the alternative Google Chrome browser and the user's Thunderbird mail program. This option is required if an upstream proxy breaks SSL connections.
Remove custom CA*	Removes a CA stored for users.
Import Firefox policy*	Provides the ability to use your own Firefox Policy (policies.json) file from the administrator's transfer directory <b>config</b> . The policy is available system-wide after application and becomes effective for the users after a new login. The Firefox add-on " <a href="#">Enterprise Policy Generator</a> " has proven itself for creating a policies.json file.
Remove Firefox policy*	Removes the self imported Firefox Policy.

## Authentication methods

The following link gives an overview of the different ways to log on to TightGate-Pro.

[User administration in TightGate-Pro](#)

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

Permanent link:  
<https://help.m-privacy.de/doku.php/en:tightgate-pro:konfiguration:system-vorgaben>

Last update: **2024/03/07 09:51**

