The administrators 'root' and 'security'

The administrators ***root*** and ***security*** are responsible for managing the security system of TightGate-Pro. They can make changes to the security models or provide log analyses for maintenance. However, they are not required for the normal operation and configuration of TightGate-Pro.

For the administrators ***root*** and ***security*** to log on to TightGate-Pro, an additional activation by the administrator ***maint*** is necessary. There is also a time limit; after one hour, the login option via SSH is automatically deactivated and must be reactivated if necessary.

Warning: Improper changes to the security system of TightGate-Pro harbour considerable security risks for the internal network and the workstations on it. Furthermore, serious disruptions to productive operation can occur.

Warning: Customer service operations of m-privacy GmbH that are carried out against the background of improper interventions via the administrators ***root*** and ***security*** are not covered by the software maintenance contracts. This also applies in particular to any consequential damage, for example due to insufficient protection as a result of an impairment of the security mechanisms of TightGate-Pro.

The administrator 'security'

The role ***security*** role defines the possibilities of a security officer and can edit the entire RSBAC set of rules. New roles can be defined and the rights of existing roles can be changed. Due to the scope of authorisation, the role of ***security*** is only accessible from the local console by default. SSH access for the administrator ***security*** can only be granted by the administrator ***maint*** for a limited period of time. To view the status of the security models and the RSBAC rules, it is necessary to log in as administrator ***security*** on the console.

The following setting options are available:

Security	
Menu item	**Description**
End	Exit the menu and quit ***security***.
—	
Allow 5 min. root maintenance	Release the maintenance role for the administrator ***root*** for 5 minutes.
Menu audit ON/OFF	Switching menu logging on/off, i.e. all commands that the administrator ***security*** are logged in the /security/log/ directory. Activities of other administration roles are not logged.
VNC logging ON/OFF	Switches the logging of the TightGate VNC server on/off. The logs are saved in /home/tmpdir/tmp510/Xtightgatevnc-PID.log (PID means ProcessID of the TightGate VNC server process).
Expert menu ON/OFF	Switching an additional menu on/off in the administration menu of ***config*** to control individual parameters for transmission within the VNC protocol.
—	
Current user statistics	Gives an overview of the user IDs created in TightGate-Pro and the resources used by the IDs.

Security	
Menu item	**Description**
Start RSBAC menu	Transition to the RSBAC configuration menu. **Warning:** Settings only by the technical customer service of m-privacy GmbH . Improper changes to the security system of TightGate-Pro Server harbour considerable security risks for the internal network and the workstation computers in it. Furthermore, serious disruptions to productive operation can occur.
Console	Calling up the console for the administrator ***security***.
—	
RC Debug mode ON/OFF	Switches detailed debugging for the RSBAC RC module on/off. **Caution:** Switching on this menu option significantly increases the number of messages in the syslog. An "overflowing" log partition can have a negative impact on the system behaviour.
JAIL Debug mode ON/OFF	Switching the detailed debugging for the RSBAC JAIL module on/off. **Caution:** Switching on this menu option increases the number of messages in the syslog. Permanent use of this option is therefore not recommended.
Global Softmode ON/OFF	Switching the RSBAC security system on and off - only to be used in exceptional cases and outside of productive operation. **Warning:** Central security features of TightGate-Pro Server are disabled. The level of protection of the ReCoBS server and the internal network is greatly reduced. There is still a risk of malfunctions and data loss if the global soft mode is activated during productive operation!
RC Softmode ON/OFF	Switching off/on RC module of the RSBAC system - only to be used in exceptional cases and outside of productive operation. **Warning:** Central security features of TightGate-Pro Server are overridden. The level of protection of the ReCoBS server and the internal network is greatly reduced. There is still a risk of malfunctions and data loss if RC soft mode is activated during productive operation!
—	
Revision password	Changing the password for the administrator ***revision***.
Security password	Changing the password for the administrator ***security***.

The administrator 'root'

The role ***root*** role essentially corresponds to that of the classic administrator for system services. As administrator ***root*** administrator, installed system services can be started and stopped, tests can be carried out with system tools and system services can be configured. In contrast to the administrator account of a conventional Linux system with the same name and unlimited authorisation, the role of ***root*** role is subject to special restrictions. For example, the administrator ***root*** administrator cannot access user directories, assign RSBAC rights to programmes or change RSBAC rights, but can view them.

To display the status of the security models and processes and to view the current system log, it is necessary to log in as administrator ***root*** on the console is required.

root	
Menu item	**Description**
Quit	Exit the menu and end access as administrator ***root***
—	

root	
Menu item	**Description**
Console	Call up a console for the administrator ***root***.
Maintenance console	Calling up a maintenance console for the administrator ***root***. If the administrator ***security*** the administrator ***root*** has been assigned the maintenance role by the administrator security, the latter can work in the system with extended authorisations. This function is specifically intended for maintenance tasks and should be used with caution. The extended authorisations based on the maintenance role can be found in the appendix.
—	
Reboot	Restart the ReCoBS server, either immediately or as scheduled. Followed by the option to request a RECOVERY boot (default No).
Cancel reboot	Cancellation of a scheduled appointment to restart the ReCoBS server.
Halt	Shut down the ReCoBS server. Followed by the option to request a RECOVERY boot (default No).
—	
Root password	Change the password for the administrator ***root***.