Role authorisations

The roles created via RSBAC contain a series of rights that restrict or enable access to other resources (such as files, network ports and devices) for the programmes being executed. Background: In a Linux operating system with RSBAC extension, other models can be loaded in addition to the conventional access rights model and the rights can be combined with each other. Rights are also understood as restrictions. At TightGate-Pro, the Role Compatibility Model (RC model) should be mentioned in particular. The RC model allows a much finer assignment of rights than the standard access rights model under Linux.

Each role has its own set of rights, independent of all other roles. For example, if a user calls up the web browser that starts with the rights of the web browser role, the web browser has the RC rights for exactly the actions that are to be carried out with the web browser. In addition, the rights restrictions from the other security models are retained; the browser of one user cannot jeopardise the browser of another.

Note: Until now, the term "administrator" was usually used to refer to a user account created by the system with the authorisations of a specific role. In the following, roles are written in upper case, while administrator accounts are referred to in lower case. A role describes an authorisation context that a user or administrator account, but also a programme, can have. There is only one administrator account for central roles in TightGate-Pro, which is named in the same way as the role itself.

Programmes are also started in a role context. This serves to encapsulate these programmes and prevents security-relevant "attacks" on each other or on the underlying operating system.

- For the role ***OFFICE*** role, which, like ***MUA*** (Mail User Agent, role for using the e-mail application at TightGate-Pro) and ***WEBBROWSER*** is only activated when the respective programme is started, special rules apply.
- The user accounts of regular VNC users are activated in the role ***USER*** role. It is not possible to work as a logged-in user in the role context of an administrator. In the case of a direct login in an administrator role, the respective administrator account is always active, even if a regular user logs in. In contrast to conventional operating systems, it is not possible to transfer administrator rights to regular users.
- A special case of the user role is the role ***TRANSFER***. In this role context, only the so-called ***transfer***users, who are reserved for cross-system operation of the secure file transfer. ***transfer***-users are authorised to read and write to all transfer directories of all regular users.
- The role ***CONFIG*** is reserved for the special administrator account ***config***, which has the task of making the specific (network) adjustments for TightGate-Pro to the local network. The role ***MAINT*** is performed by the local administrator ***maint*** and enables the creation and deletion of users as well as the assignment of (initial) passwords.
- The role ***SECURITY*** role determines the options available to the security officer. This role 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 wide range of competences, the role ***SECURITY*** is only accessible from the local console by default. SSH remote access for ***SECURITY*** can only be granted by the administrator ***maint*** for a limited period of time.
- The role ***ROOT*** essentially corresponds to the classic system administrator for system services. As ***ROOT*** installed system services can be started and stopped, tests can be carried out with system tools and system services can be configured to a limited extent. In contrast to the universally authorised root account of a conventional Linux system, the ***ROOT*** role is subject to special restrictions. Thus ***ROOT*** cannot access user directories, cannot assign RSBAC rights to

programmes and generally cannot change RSBAC rights - but can view the RSBAC rights.

- The role ***UPDATE*** is used for the uncomplicated updating of TightGate-Pro. ***UPDATE*** combines the possibilities of network access (e.g. via SSH) and the update of programme packages using a package manager.
- The role ***REVISION*** / Data Protection Officer (DPO). The roles of auditor and data protection officer are found in practically every company and authority. Even though these roles are often performed by different people in practice, they have something in common: they have the right (and the duty) to access system and user data in a content-controlling (i.e. read-only) manner without being able to make changes.
- In the standard configuration of TightGate-Pro, the role ***REVISION*** has the control rights of a data protection officer. A help menu ("copy tool") makes it easier for the user to create copies of the user directories and work on them. The role ***REVISION*** otherwise behaves similarly to the ***USER***role, including the use of the browser, office and mail roles, but without network access.
- The role ***VNC-SERVER*** role is representative of a role assigned to a system service. The definition of the necessary RSBAC rights in the role ***VNC-SERVER ROLE*** and the assignment of this role restricts the rights of the service running under it to precisely this defined area. A possible programme error, a backdoor or an exploit targeted at the daemon can only become effective within this narrowly defined framework. Even an attempt to do something else will result in a warning message to the system administrator.
- The role ***BACKUP*** contains the authorisation context for the administrator ***backuser***, who is responsible for all matters relating to centralised data backup and restore on TightGate-Pro.
- The ***ROOT***-maintenance role is an extension of the normal ***ROOT***-role plus the authorisation to view and signal processes. As the ***ROOT***-maintenance role represents an extension of the rights for root, special precautions have been taken to protect it from misuse. The extension can only be obtained via a four-eyes principle. The role ***SECURITY*** must override the ***ROOT maintenance*** role before it can be activated by the administrator ***root*** can use it.

Function Authorisation	**Role name**									
	USER	**CONFIG**	**MAINT**	**UPDATE**	**BACKUP**	**REVISION**	**TRANSFER**	**SECURITY**	**ROOT**	**ROOT MAINTENANCE**
Changing network settings limited to menu functionality	-	+	-	-	-	-	-	-	-	-
Reboot the system	-	+	+	+	-	-	-	-	+	+
Individual modification of configuration files	-	-	-	-	-	-	-	-	-	+ restricted
Assignment of role authorisations	-	-	-	-	-	-	-	+	-	-
Shell access	+	-	-	-	-	+	-	+	+	+
Graphical user interface	+	-	-	-	-	+	-	-	-	-
User administration limited to menu functionality	-	-	+	-	-	-	-	-	-	-
Restart of individual services	-	+	+	+	-	-	-	-	+	+

Function Authorisation	**Role name**									
Time-limited authorisation of administrator logins via SSH	**-**	**-**	**+**	**-**	**-**	**-**	**-**	**+(*)**	**-**	**-**
Authorisation of logins via SSH over network from outside the intended client network	**-**	**+**	**-**	**-**	**-**	**-**	**-**	**-**	**+(*)**	**+(*)**
Open the remote maintenance access for m-privacy GmbH	**-**	**-**	**+**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Update of installed programme packages limited via menu functionality	**-**	**-**	**-**	**+**	**-**	**-**	**-**	**-**	**-**	**-**
Access to /home directories	**+ only own directory**	**-**	**-**	**-**	**-**	**+ reading only**	**-**	**+ read only**	**-**	**+**
Save and restore the RSBAC configuration	**-**	**-**	**-**	**+ Restore**	**-**	**-**	**-**	**+**	**-**	**-**
Change RSBAC configuration	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**+**	**-**	**-**
Full access via interpreter to images of selected user directories	**-**	**-**	**-**	**-**	**-**	**+**	**-**	**-**	**-**	**-**
Read-only access to system logs	**-**	**-**	**-**	**-**	**-**	**+**	**-**	**+**	**+**	**+**
Write access to system logs	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Network access	**+**	**-**	**-**	**restricted**	**restricted**	**-**	**-**	**restricted**	**restricted**	**restricted**
Read-only access to user data	**-**	**-**	**-**	**-**	**-**	**+**	**-**	**+**	**-**	**-**
Editing the configuration of unprotected system services	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**+**
Use of test tools (e.g. netstat)	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**+**	**+**
Call of "rsbac_menu"	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**+**	**+ (read only)**	**+ (read only)**

Legend:

(*) Option can only be set manually via the console, not via a menu option.