User role "Revision"

The role of auditor/data protection officer was introduced in the course of the organisational separation of technical and content control. While technical control is carried out by system administrator roles, they do not have access to user data. Content control of user data can only be carried out by the role ** *revision*** .

Legal requirements, including data protection regulations in particular, set strict limits. The auditor or data protection officer in particular is required to decide responsibly and under consideration of all circumstances whether and how control of user data is necessary. The role ** *revision*** is tailored to the needs and tasks of data protection officers and auditors.

revision is a user, i.e. access is not via the console, but via the TightGate viewer. However, the revision account is not a user account in the conventional sense; rather, the use of this account serves exclusively to exercise control rights within the framework of the tasks of a data protection officer or auditor. This account does not replace the normal user account for employees entrusted with data protection or auditing tasks. In particular, there is no possibility to use e-mail, Internet or other network services.

Hinweis

If you operate TightGate-Pro in an environment where users log on to TightGate-Pro via single sign-on, it may be necessary to create an additional desktop shortcut of the TightGate viewer with password login. This is necessary because logging in as a revision user can only be done with a user name and password. Instructions on how to create the shortcut can be found in the following FAQ: TightGate Viewer: How do I create a desktop shortcut of a TightGate viewer with password login?

Control options and limits of the Revisor role

Control possibilities

- It is possible to copy a copy of a user account into the area of the revision account and to control it there with the settings of the user concerned.
- The copied data of a user is only kept for 7 days and then deleted again. If the data is to be kept for longer than 7 days, it must be copied manually to another location (e.g. the transfer directory of ** *revision***).
- For control purposes, the programmes can be started and viewed with the user's settings.

Restrictions

- The ** *revision*** user has read-only access rights to the user data in order to make a (backup) copy for analysis. Thus, no modified data can be written back to user accounts by the user ** *revision*** .
- The same applies to all settings in the user account. Any settings changed by the administrator ** *revision*** cannot be transferred to the user account.
- The user ** *revision*** cannot send any e-mails from the copied user account, neither in his own name nor in the name of the user, even though all user settings have been transferred.

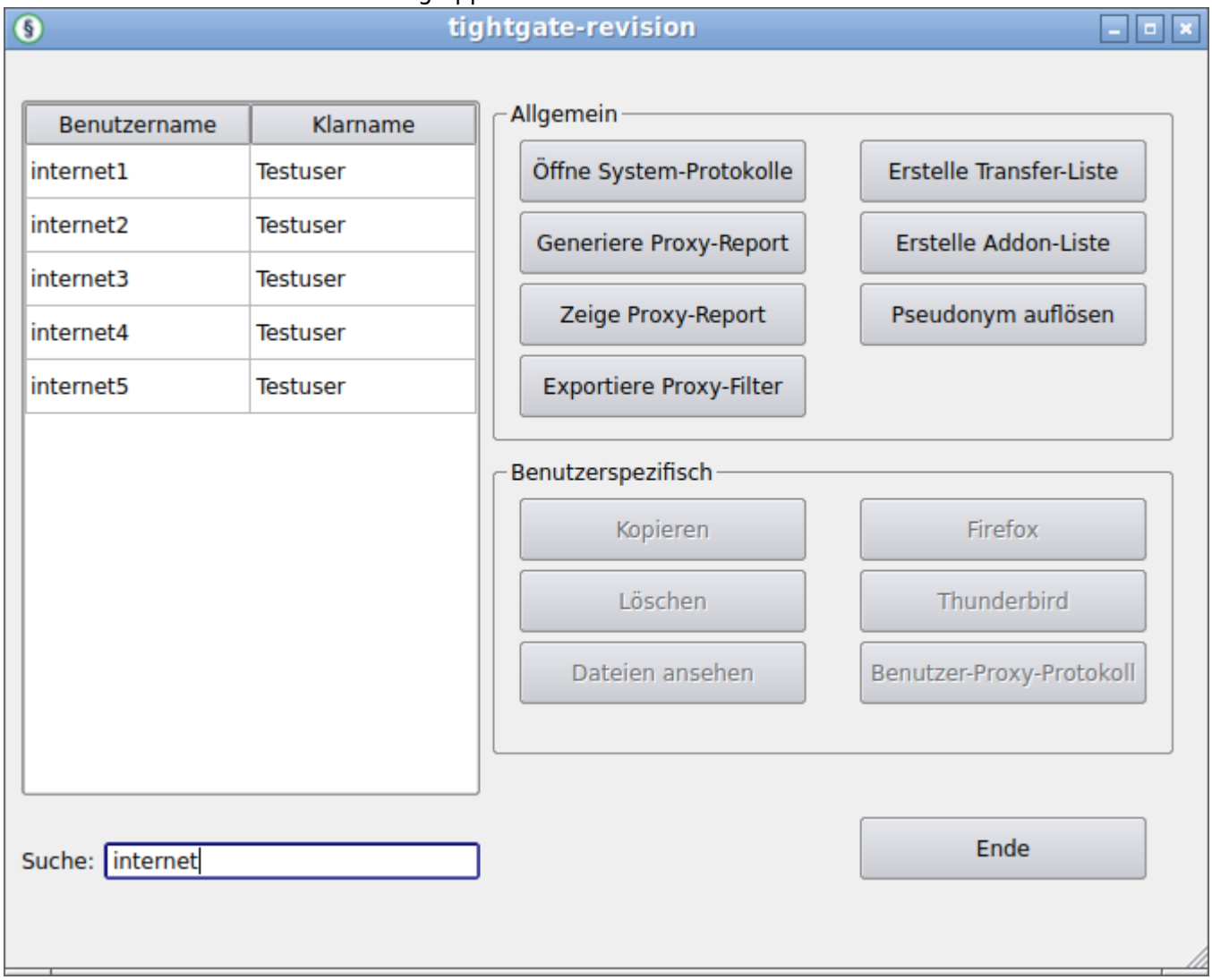
- IMAP mail accounts cannot be controlled on TightGate-Pro. These are mailboxes on a remote mail server. Control of these mailboxes is only possible there.
- If a user has not used a programme before, there may not be a corresponding configuration and error messages may be displayed.

User control by the revisor

The user ** *revision*** is a role created specifically for the Supervisor. To obtain the status of revisor, logging in with the user name ** *revision*** and the associated password is required. The password for the user ** *revision*** is assigned by the administrator ** *security*** . The login is analogous to the login of other users via the TightGate viewer.

When starting, the **revision menu** is automatically started. Alternatively, it can also be started via the menu bar using the symbol  . As a warning that the revision account is being used, the screen background is red.

The revision menu has the following appearance:



The menu is divided into two sections, the section **General**, where evaluations can be made that apply to the entire system, and the section **User-specific**, which allows control options for individual users. The menu items of the revision menu are explained below:

__ Section General__

Menu item	Description
Open System Logs	Opens a programme to display the system logs.
Generate Proxy Report	Creates a summary evaluation of the saved proxy logs, see also the section Logging web access in the configuration settings as administrator ** *config*** . Each generated proxy report is stored as a copy in the transfer directory of the revision user. Only protocol data up to the previous day is available.
Show proxy report	Shows the evaluation of the proxy logs. Before a proxy report can be displayed, it must be created via the menu item **Generate proxy report**.
Generate Transfer List	Creates a list of all uploads and downloads of files that were exchanged with the internal network via the file lock. The list is copied to the transfer folder as a CSV file with the date in the name. The CSV file is separated by semicolons.
Create Addon List	Creates a list of all installed add-ons for each user. The list is copied to the transfer folder as a CSV file with the date in the name. See the section Overview of Installed Browser Add-ons The CSV file is separated by semicolons.
Resolve pseudonym	After entering a pseudonym to be resolved, the respective user ID is displayed in plain text. See the section Resolving Pseudonyms in Log Files.
Export Proxy Filter	Creates a list of all entries in the proxy filter of TightGate-Pro. The list is copied to the transfer folder as a CSV file with the date in the name. The CSV file is separated by semicolons.

User-specific section

Menu item	Description
Copy	A local working copy of the relevant user data is created and kept for 7 days. The copy of the user data can also be changed or saved in a changed form. The original user data will not be touched at any time.
Delete	Deletes the working copy of a user data record from the user's workspace ** *revision*** . This function is only available if the user's data has been copied before.
View Files	Opens a file browser to view the files of the selected user. This function is only available if the user's data has been copied beforehand.
Firefox	Starts the web browser from the working copy with the user's settings. This function is only available if the user's data was previously copied. If the selected user has not yet used the web browser, error messages may be displayed.
Thunderbird	Starts the e-mail programme from the working copy with the user's settings. This function is only available if the user's data was previously copied. If the selected user has not yet used the e-mail programme, error messages may be displayed.
User proxy log	Shows all entries from all available log files for the user in question. This function is only available if the user's data was previously copied. **Attention:** If logging in the system under a pseudonym, the display of the user proxy log is empty.

Evaluate proxy log

The user ** *revision*** can view an evaluation of the web proxy. If the proxy logging is activated, a report on all available proxy logs of a TightGate-Pro single system or cluster can be generated via the button **Generate proxy report**. Once the report has been generated, it can be opened via the button **Show proxy report**. The report is opened in the web browser and offers various overviews.

__User proxy log __

The **user proxy protocol** is available for evaluating the Internet accesses of individual users. The file about user logins is output as a text file and has the following exemplary structure:

Month	Day	Time	Server name	Protocol	Authentication	User
Jan	31	12:44:53	tgpro-12	riv:	(pam_rsbac_en)	session opened for user revision by *unknown*(uid=0)
January	31	12:44:53	tgpro-12	riv (via VNC)	pam	revision

Other protocols

The button **Open system logs** can be used to view various log files. The following table lists the log files that can be viewed by the user ** *revision*** . Support in connection with the system logging functions is provided by the technical customer service of m-privacy GmbH .

Log	Description
auth.log	Logging of authorisation procedures to TightGate-Pro.
dpkg.log	Logging of operations related to package installation.
mail.log	Logging in connection with the sending and receiving of e-mails.
syslog	Logging of messages from system services.

Resolve pseudonyms

User names can be stored pseudonymised in the log files. The logs are also displayed with pseudonymised user names if this has been set. Resolving the pseudonyms is only possible manually by the user ** *revision*** .

If a pseudonym has been dissolved and it is necessary to assign a new pseudonym for a user, the user ** *security*** can assign new pseudonyms to individual users. In this case, it is recommended to contact the technical customer service of m-privacy GmbH . If new pseudonyms are to be assigned for all users, the administrator ** *config*** can do this by switching the pseudonymisation off and on again once.

If a pseudonym is changed, the list of old pseudonyms is saved in the directory **/home/revision/pseudos** and thus remains available for the evaluation of older log files.

Storage duration of log files

Regular log files: The storage duration of log files in TightGate-Pro is limited. TightGate-Pro uses a ring buffer (log rotate) for all log files by default. The rotation period is one week with four cycles. Log files are therefore stored for four weeks. When the files of the fifth week are created, the data of the first week are deleted.

Special case RSBAC log files: A shorter cycle applies to RSBAC log files. Log files are stored for seven days on a rotating basis. On the 8th day, the log file of the first day is deleted.

Overview of the log files in which RSBAC messages are stored:

Log file	Accessible via revision menu	Active (In normal operation)
kern.log	No	Yes
messages	No	Yes
syslog	Yes	Yes
debug.log	No	No

The file "debug.log" can also contain older RSBAC messages than would be expected according to the cyclic deletion.

Overview of installed browser add-ons

With the function for creating an overview of all user add-ons installed on a TightGate-Pro single system or cluster, you get a quick and comprehensive overview of version statuses and activation status (activated / deactivated).

The list also provides information on which users have the respective add-ons installed.

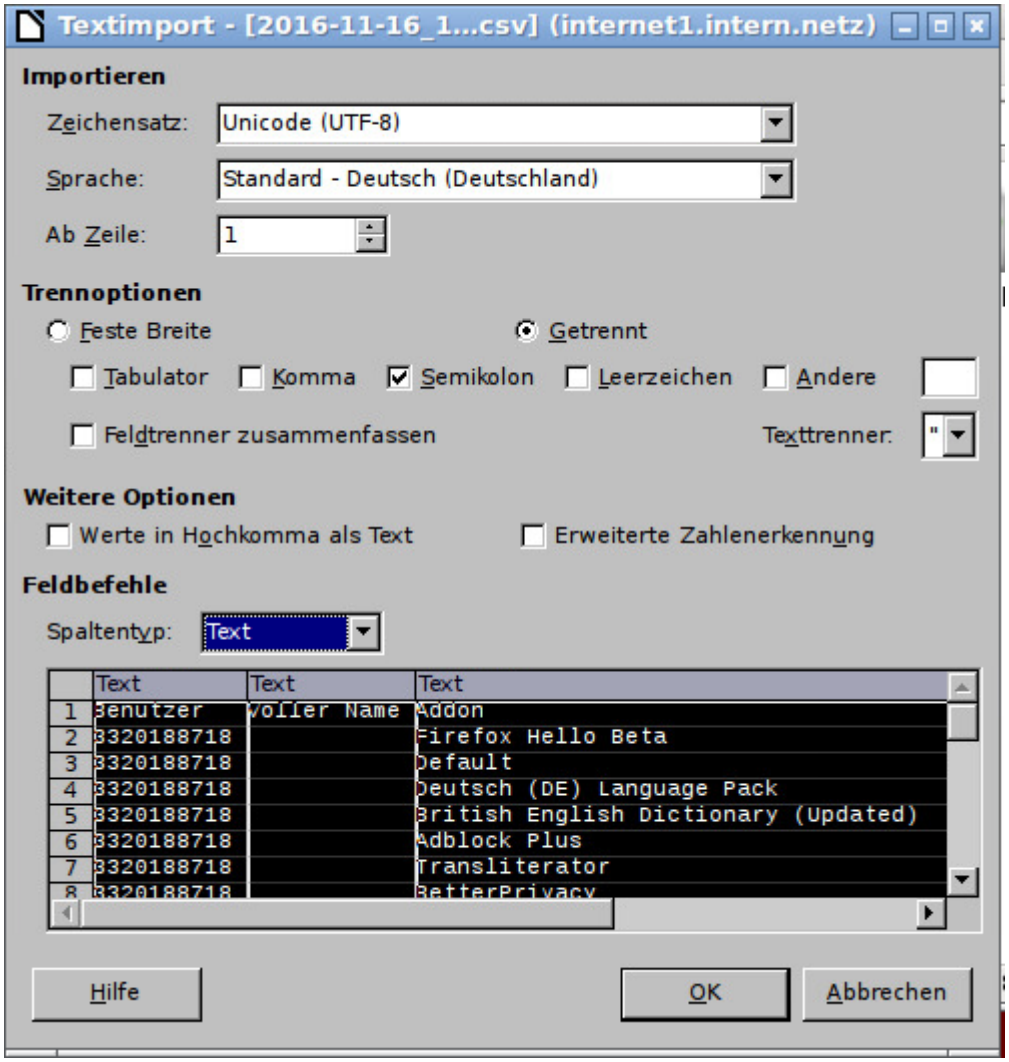
The list is generated as a standard-compliant CSV file, which can be opened and further processed on TightGate-Pro or can also be routed to external systems via the airlock functionality.

This is how it works

- Log in via TightGate-Viewer with the identification ** *revision***
- Double-click in the revision menu on the menu item **Create Addon List**

The successful creation of the list is signalled by a message window.

- The file created is located in the transfer directory of the user ** *revision*** and can be opened there by double-clicking. The following settings must be made to open the generated CSV file with the word processor at TightGate-Pro:
    - Separation option: **Semicolon**
    - Column type: **Text**



Explanations for data protection-compliant implementation

The list for the overview of installed add-ons contains data that may affect the right to informational self-determination of users. In order to take this into account and to continue the data protection-friendly concept of TightGate-Pro in this function as well, the add-on list takes into account the logging type specified in TightGate-Pro.

The following table gives an overview of the values displayed (user name + plain name) in the generated add-on overview depending on the logging type set:

Logging type	**Add-on list "User" column**	**Add-on list "Full name" column**
Anonymous	blank	blank
Pseudonym	Pseudonym	blank
User	Plain name	Plain name

Process 'Add-on list' externally

If external processing of the **add-on list** is desired, it can be ejected from TightGate-Pro via the file lock of the user ** *revision*** . The standard-compliant CSV file can be opened and processed with common spreadsheet programs.

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

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

Last update: **2022/08/22 11:39**