Benutzerrolle "Revision"

Die Rolle des Revisors/Datenschutzbeauftragten wurde im Zuge der organisatorischen Trennung von technischer und inhaltlicher Kontrolle eingeführt. Während die technische Kontrolle von Systemadministrator-Rollen durchgeführt wird, haben diese keinen Zugriff auf Benutzerdaten. Die inhaltliche Kontrolle der Benutzerdaten kann nur durch die Rolle ***revision*** erfolgen.

Gesetzliche Vorgaben, darunter insbesondere Datenschutzvorschriften, setzen enge Grenzen. Besonders der Revisor bzw. Datenschutzbeauftragte ist angehalten, verantwortungsvoll und unter Abwägung aller Umstände zu entscheiden, ob und wie eine Kontrolle der Benutzerdaten erforderlich ist. Die Rolle ***revision*** ist auf die Bedürfnisse und Aufgabenstellungen der Datenschutzbeauftragten und Revisoren zugeschnitten.

revision ist ein Benutzer, d. h. der Zugang erfolgt nicht über die Konsole, sondern über den TightGate-Viewer. Der Revisionsaccount ist jedoch kein Benutzerkonto im herkömmlichen Sinne, vielmehr dient die Verwendung dieses Accounts ausschließlich der Wahrnehmung von Kontrollrechten im Rahmen der Aufgaben eines Datenschutzbeauftragten bzw. Revisors. Dieser Zugang ersetzt nicht das normale Benutzerkonto für mit Datenschutz- bzw. Revisionsaufgaben betraute Mitarbeiter. Es besteht insbesondere keine Möglichkeit, E-Mail-, Internet- oder andere Netzwerk-Dienste zu nutzen.

Hinweis

Sofern Sie TightGate-Pro in einer Umgebung betreiben, bei der sich die Benutzer per Single-Sign-On-Anmeldung am TightGate-Pro anmelden, kann es notwendig sein, sich eine zusätzliche Desktop-Verknüpfung des TightGate-Viewers mit Passwort-Anmeldung anzulegen. Dies ist notwendig, da sich eine Anmeldung als Revisionsbenutzer nur mit Benutzername und Passwort durchführen lässt. Eine Anleitung zum Anlegen der Verknüpfung finden Sie in folgendem FAQ: TightGate-Viewer: Wie erstelle ich eine Desktop-Verknüpfung eines TightGate-Viewers mit Passwort-Anmeldung?

Kontrollmöglichkeiten und Grenzen der Revisor-Rolle

Kontrollmöglichkeiten

- Es besteht die Möglichkeit eine Kopie eines Benutzerkontos in den Bereich des Revisions-Accounts zu kopieren und dort mit den Einstellungen des betreffenden Benutzers zu kontrollieren.
- Die kopierten Daten eines Benutzers werden nur 7 Tage vorgehalten und anschließend wieder gelöscht. Sollen die Daten länger als 7 Tage aufbewahrt werden, so müssen diese manuell an einen anderen Ort (z. B. das Transfer-Verzeichnis von ***revision***) kopiert werden.
- Zur Kontrolle können die Programme mit den Einstellungen des Benutzers gestartet und angesehen werden.

Beschränkungen

- Der ***revision***-Zugang hat ein ausschließlich lesendes Zugriffsrecht auf die Benutzerdaten, um eine (Sicherungs-)Kopie zur Analyse zu erstellen. Somit können durch den Benutzer ***revision*** keine veränderten Daten in Benutzerkonten zurückgeschrieben werden.

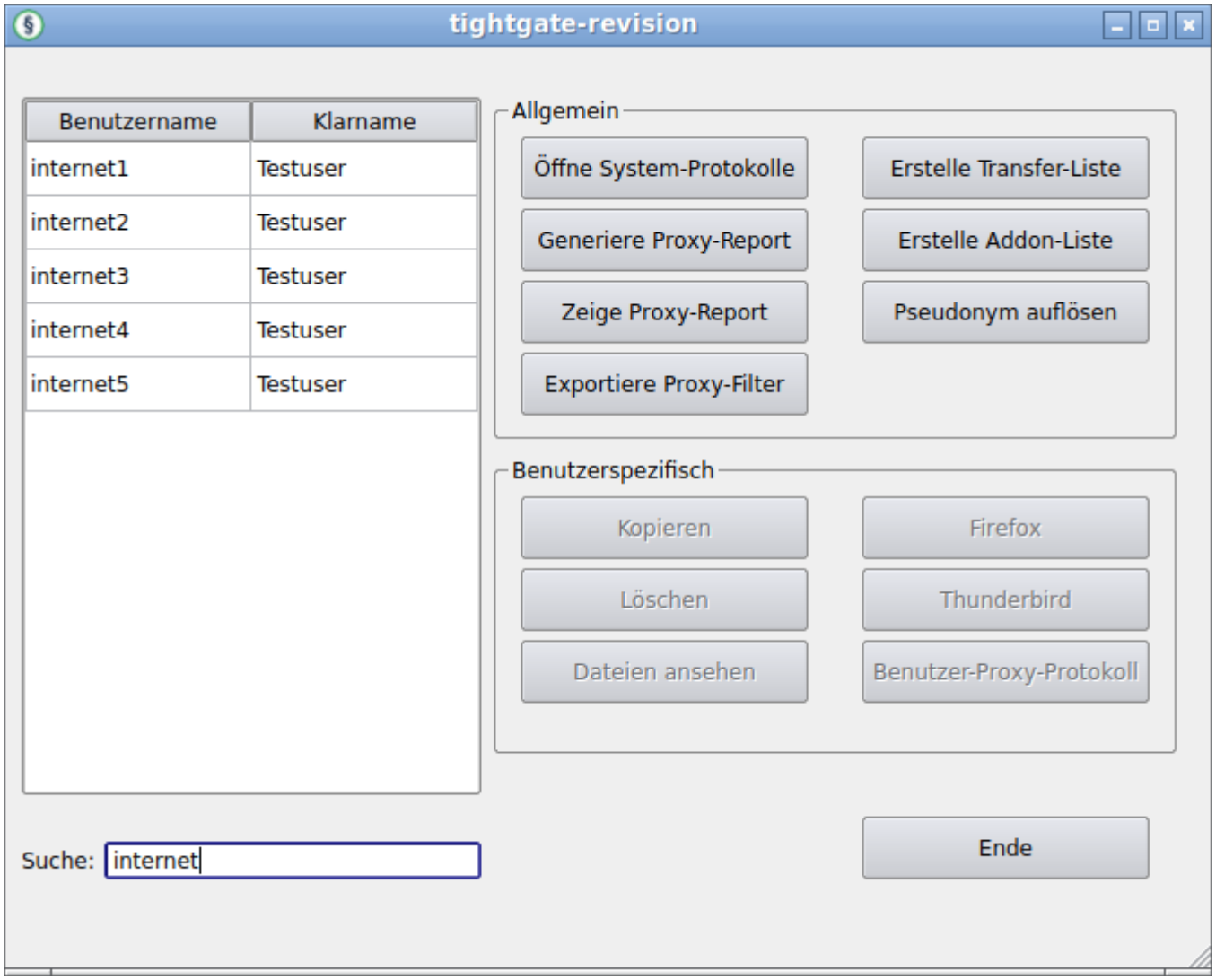
- Gleiches gilt für alle Einstellungen im Benutzeraccount. Eventuell durch den Administrator ***revision*** veränderte Einstellungen können nicht auf den Benutzeraccount übertragen werden.
- Der Benutzer ***revision*** kann, trotz Übernahme sämtlicher Benutzereinstellungen, keine E-Mails aus dem kopierten Benutzer-Account verschicken; weder im eigenen Namen, noch im Namen des Benutzers.
- IMAP-Mailkonten können auf TightGate-Pro nicht kontrolliert werden. Es handelt sich dabei um Postfächer auf einem entfernten Mailserver. Eine Kontrolle dieser Postfächer ist nur dort möglich.
- Hat ein Benutzer ein Programm bisher nicht verwendet, liegt u. U. keine entsprechende Konfiguration vor und es werden möglicherweise Fehlermeldungen angezeigt.

Benutzerkontrolle durch den Revisor

Der Benutzer ***revision*** ist eine speziell für den Datenschutzbeauftragten geschaffene Rolle. Um den Status des Revisors zu erlangen, ist die Anmeldung mit dem Benutzernamen ***revision*** und dem zugehörigen Passwort erforderlich. Das Passwort für den Benutzer ***revision*** wird vom Administrator ***security*** vergeben. Die Anmeldung erfolgt analog zur Anmeldung anderer Benutzer über den TightGate-Viewer.

Beim Start wird automatisch das **Revisionsmenü** gestartet. Es kann alternativ auch über die Menüleiste über das Symbol  gestartet werden. Zur Warnung, dass mit dem Revisions-Account gearbeitet wird, ist der Bildschirmhintergrund rot.

Das Revisionsmenü hat Folgendes aussehen:



Das Menü unterteilt sich in zwei Abschnitte, den Abschnitt **Allgemein**, in dem Auswertungen erfolgen könne, die für das gesamte System gelten, sowie den Abschnitt **Benutzerspezifisch**, der Kontrollmöglichkeiten für einzelne Benutzer erlaubt. Nachfolgend werden die Menüpunkte des Revisionsmenüs erläutert:

__ Abschnitt Allgemein__

Menüpunkt	**Beschreibung**
Öffne System-Protokolle	Öffnet ein Programm zur Darstellung der System-Protokolle.
Generiere Proxy-Report	Erstellt eine zusammenfassende Auswertung der gespeicherten Proxy-Protokolle, siehe dazu auch den Abschnitt Protokollierung des Webzugriffs in den Konfigurationseinstellungen als Administrator ***config***. Jeder generierte Proxy-Report wird als Kopie im Transfer-Verzeichnis des Revisions-Benutzers abgelegt. Es stehen immer nur Protokoll-Daten bis zum Vortag bereit.
Zeige Proxy-Report	Zeigt die Auswertung der Proxy-Protokolle. Bevor ein Proxy-Report angezeigt werden kann ist dieser über den Menüpunkt **Generiere Proxy-Report** zu erstellen.
Erstelle Transfer-Liste	Erstellt eine Liste aller Up- und Downloads von Dateien, die über die Dateischleuse mit dem internen Netzwerk ausgetauscht wurden. Die Liste wird als CSV-Datei mit Datum im Namen in den Transfer-Ordner kopiert. Die Trennung in der CSV-Datei erfolgt durch Semikolon.

Menüpunkt	Beschreibung
Erstelle Addon-Liste	Erstellt eine Liste aller Installierten Add-ons je Benutzer. Die Liste wird als CSV-Datei mit Datum im Namen in den Transfer-Ordner kopiert. Siehe dazu den Abschnitt Übersicht installierten Browser Add-ons Die Trennung in der CSV-Datei erfolgt durch Semikolon.
Pseudonym auflösen	Nach Eingabe eines aufzulösenden Pseudonyms wird die jeweilige Benutzerkennung im Klartext angezeigt. Sie das den Abschnitt Pseudonyme in Log-Dateien auflösen.
Exportiere Proxy-Filter	Erstellt eine Liste aller Einträge im Proxy-Filter von TightGate-Pro. Die Liste wird als CSV-Datei mit Datum im Namen in den Transfer-Ordner kopiert. Die Trennung in der CSV-Datei erfolgt durch Semikolon.

Abschnitt Benutzerspezifisch

Menüpunkt	Beschreibung
Kopieren	Es wird eine lokale Arbeitskopie der betreffenden Benutzerdaten angelegt, welche für 7 Tage vorgehalten wird. Die Kopie der Benutzerdaten kann auch verändert bzw. in veränderter Form gespeichert werden. Die originären Benutzerdaten werden dabei zu keinem Zeitpunkt angetastet.
Löschen	Löscht die Arbeitskopie eines Benutzerdatensatzes aus dem Arbeitsbereich des Benutzers ***revision***. Diese Funktion steht nur zur Verfügung, sofern zuvor Daten des Benutzers kopiert wurden.
Dateien ansehen	Öffnet einen Dateibrowser zur Sichtung der Dateien des ausgewählten Benutzers. Diese Funktion steht nur zur Verfügung, sofern zuvor Daten des Benutzers kopiert wurden.
Firefox	Startet den Webbrowser aus der Arbeitskopie mit den Einstellungen des Benutzers. Diese Funktion steht nur zur Verfügung, sofern zuvor Daten des Benutzers kopiert wurden. Hat der ausgewählte Benutzer den Webbrowser noch nicht verwendet, werden möglicherweise Fehlermeldungen angezeigt.
Thunderbird	Startet das E-Mail-Programm aus der Arbeitskopie mit den Einstellungen des Benutzers. Diese Funktion steht nur zur Verfügung, sofern zuvor Daten des Benutzers kopiert wurden. Hat der ausgewählte Benutzer das E-Mail-Programm noch nicht verwendet, werden möglicherweise Fehlermeldungen angezeigt.
Benutzer-Proxy-Protokoll	Zeigt alle Einträge aus allen verfügbaren Logdateien für den betreffenden Benutzer. Diese Funktion steht nur zur Verfügung, sofern zuvor Daten des Benutzers kopiert wurden. **Achtung:** Wird im System unter Pseudonym protokolliert, so ist die Anzeige des Benutzer-Proxy-Protokolls leer.

Proxy-Protokoll auswerten

Der Benutzer ***revision*** kann sich eine Auswertung des Webproxies ansehen. Sofern die Proxy-Protokollierung aktiviert ist, kann über die Schaltfläche **Generiere Proxy-Report** ein Report über alle verfügbaren Proxy-Protokolle eines TightGate-Pro Einzelsystems oder Clusters erstellt werden. Ist der Report generiert, kann er über die Schaltfläche **Zeige Proxy-Report** geöffnet werden. Der Report wird im Webbrowser geöffnet und bietet verschiedene Übersichten an.

__Benutzer Proxy-Protokoll __

Zur Auswertung der Internetzugriffe einzelner Benutzer steht das **Benutzer-Proxy-Protokoll** zur Verfügung. Die Datei über Benutzeranmeldungen wird als Textdatei ausgegeben und hat folgenden beispielhaften Aufbau:

Monat	Tag	Zeit	Server-Name	Protokoll	Authentifikation	Benutzer
Jan	31	12:44:53	tgpro-12	riv:	(pam_rsbac_de)	session opened for user revision by *unknown*(uid=0)
Januar	31	12:44:53	tgpro-12	riv (per VNC)	pam	revision

Weitere Protokolle

Über die Schaltfläche **Öffne System-Protokolle** können unterschiedliche Logdateien gesichtet werden. Nachfolgende Tabelle führt die Logdateien auf, die durch den Benutzer ***revision*** eingesehen werden können. Unterstützung im Zusammenhang mit den Funktionen der Systemprotokollierung leistet der technische Kundendienst der m-privacy GmbH.

Protokoll	Beschreibung
auth.log	Protokollierung der Authorisierungsvorgänge an TightGate-Pro.
dpkg.log	Protokollierung zu Vorgängen im Zusammenhang mit der Paketinstallation.
mail.log	Protokollierung im Zusammenhang mit dem Versand und Empfang von E-Mails.
syslog	Protokollierung der Meldungen von Systemdiensten.

Pseudonyme auflösen

In den Logdateien können die Benutzernamen pseudonymisiert abgelegt werden. Auch die Anzeige der Logs erfolgt mit pseudonymisierten Benutzernamen, wenn dies eingestellt wurde. Die Auflösung der Pseudonyme ist nur manuell durch den Benutzer ***revision*** möglich.

Wurde ein Pseudonym aufgelöst und ist die Vergabe eines neuen Pseudonyms für einen Benutzer nötig, so kann der Benutzer ***security*** einzelnen Benutzern neue Pseudonyme vergeben. Es empfiehlt sich in diesem Fall die Kontaktaufnahme zum technischen Kundendienst der m-privacy GmbH. Sollen für alle Benutzer neue Pseudonyme vergeben werden, so kann der Administrator ***config*** dies durch einmaliges Aus- und erneutes Einschalten der Pseudonymisierung bewerkstelligen.

Wird ein Pseudonym geändert, so wird die Liste der alten Pseudonyme in das Verzeichnis **/home/revision/pseudos** gesichert und bleibt damit für die Auswertung älterer Logdateien verfügbar.

Speicherdauer von Log-Dateien

Reguläre Log-Dateien: Die Speicherdauer der Logdateien in TightGate-Pro ist begrenzt. TightGate-Pro verwendet standardmäßig einen Ringpuffer (Logrotate) für alle Logdateien. Dabei beträgt die Rotationsdauer eine Woche bei vier Zyklen. Logdateien werden also vier Wochen lang gespeichert. Bei Erstellung der Dateien der fünften Woche werden die Daten der ersten Woche gelöscht.

Sonderfall RSBAC-Log-Dateien: Für RSBAC-Logdateien gilt ein kürzerer Zyklus. Logdateien werden sieben Tage rotierend gespeichert. Am 8. Tag wird die Logdatei des ersten Tages gelöscht.

Übersicht der Logdateien, in denen RSBAC-Meldungen gespeichert sind:

Logdatei	Über Revisionsmenü erreichbar	Aktiv (Im Normalbetrieb)
kern.log	Nein	Ja
messages	Nein	Ja

Logdatei	Über Revisionsmenü erreichbar	Aktiv (Im Normalbetrieb)
syslog	Ja	Ja
debug.log	Nein	Nein

Die Datei "debug.log" kann auch ältere RSBAC-Meldungen enthalten, als gemäß der zyklischen Löschung zu erwarten wäre.

Übersicht installierten Browser Add-ons

Mit der Funktion zur Erstellung einer Übersicht sämtlicher auf einem TightGate-Pro-Einzelsystem oder -Cluster installierten Add-ons der Benutzer bekommen Sie einen schnellen und umfassenden Überblick über Versionsstände und Aktivierungsstatus (aktiviert / deaktiviert).

Die Liste gibt auch Auskunft darüber, bei welchen Benutzern die jeweiligen Add-ons installiert sind.

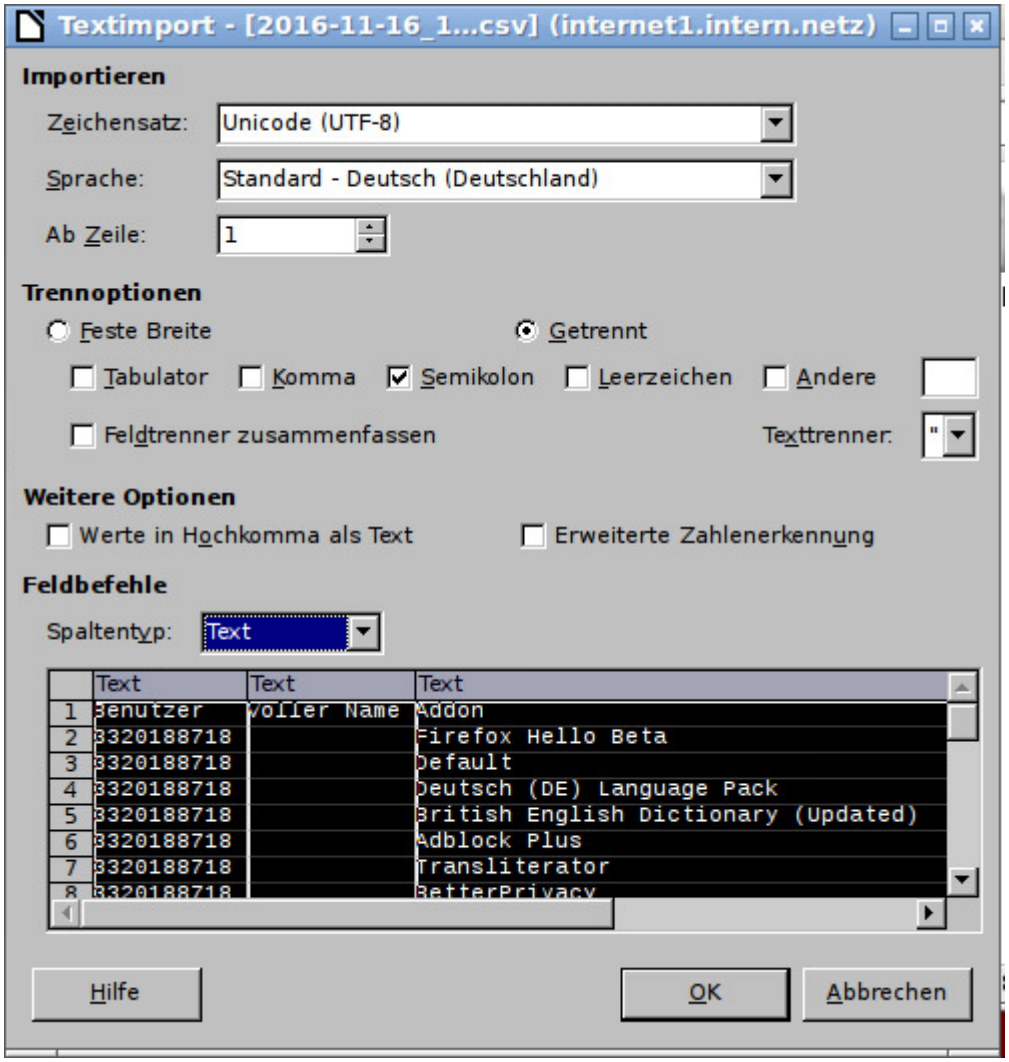
Die Liste wird als standardkonforme CSV-Datei erzeugt, welche auf TightGate-Pro geöffnet und weiter verarbeitet werden kann oder auch über die Schleusenfunktionalität auf externe Systeme geschleust werden kann.

So funktioniert‘s

- Anmelden per TightGate-Viewer mit der Kennung ***revision***
- Doppelklick im Revisions-Menü auf den Menüpunkt **Erstelle Addon-Liste**

Die erfolgreiche Erstellung der Liste wird durch ein Hinweisfenster signalisiert.

- Die erzeugte Datei befindet sich im Transfer-Verzeichnis des Benutzers ***revision*** und kann dort durch einen Doppelklick geöffnet werden. Folgende Einstellungen zum Öffnen der erzeugten CSV-Datei mit der Textverarbeitung auf TightGate-Pro sind vorzunehmen:
  - Trennoption: **Semikolon**
  - Spaltentyp: **Text**



Erläuterungen zur datenschutzkonformen Umsetzung

Die Liste zur Übersicht installierter Add-ons enthält Daten, die ggf. das Recht auf informationelle Selbstbestimmung von Benutzern berühren. Um diesem Umstand Rechnung zu tragen und das datenschutzfreundliche Konzept von TightGate-Pro auch in dieser Funktion weiterzuführen, berücksichtigt die Add-on-Liste die in TightGate-Pro vorgegebene Protokollierungsart.

Nachfolgende Tabelle gibt eine Übersicht über die angezeigten Werte (Benutzername + Klarname) in der erzeugten Add-on-Übersicht je nach eingestellter Protokollierungsart:

Protokollierungsart	Add-on-Liste Spalte "Benutzer"	Add-on-Liste Spalte "Voller Name"
Anonym	leer	leer
Pseudonym	Pseudonym	leer
Benutzer	Klarname	Klarname

‚Add-on-Liste' extern verarbeiten

Sofern eine externe Verarbeitung der **Add-On Liste** gewünscht ist, so kann diese über die Dateischleuse des Benutzers ***revision*** von TightGate-Pro ausgeschleust werden. Die standardkonforme CSV-Datei kann mit gängigen Tabellenkalkulationsprogrammen geöffnet und

verarbeitet werden.