Zugriffsberechtigungen

Die Invoice-Lösung enthält diverse Zugriffsbeschränkungen welche verhindern, dass ein Anwender Zugriff auf Belege oder Konfigurationen erhält, welche er nicht sehen darf.

Mappenrechte

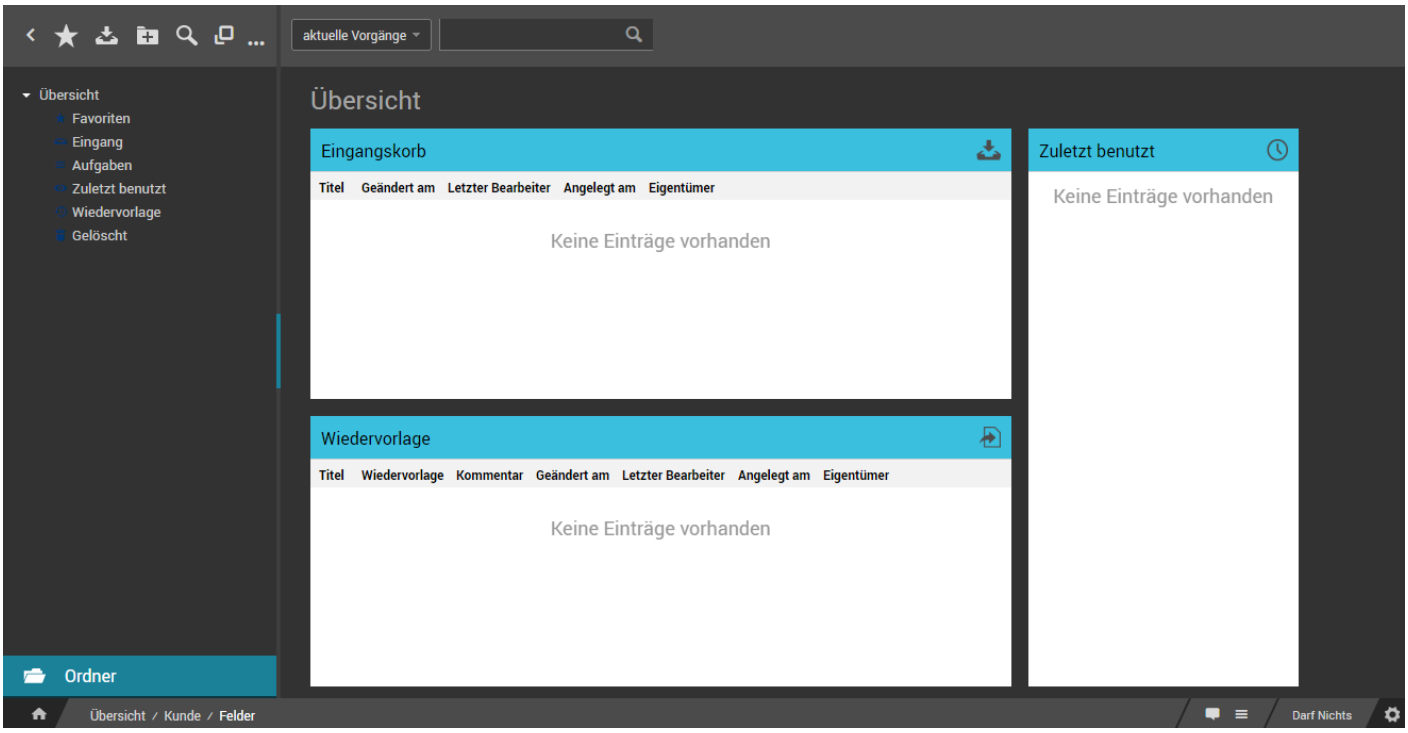
Am Mappentypen "**Invoice**" sind Mappenrechte hinterlegt. Über die Mappenrechte werden grundsätzliche Berechtigungen wie "**Lesen**" oder "**Schreiben**" oder "**Löschen**" vergeben. Die Mappenrechte legen fest, was ein User an den Vorgängen grundsätzlich machen, sehen und ausführen dürfte, wenn es keine weiteren Einschränkungen geben würde. Die Mappenrechte legen nicht fest, auf welche Vorgänge ein Anwender Zugriff hat!
Die Lese-Berechtigung wird zum Beispiel über die sogenannte GACL-Berechtigung pro Vorgang eingeschränkt. Die Schreib-Berechtigung wird zusätzlich über den Workflow pro Vorgang eingeschränkt, denn nur aktuell sperrende Benutzer können im Workflow einen Vorgang bearbeiten!

Jeder Anwender, der am Rechnungseingangs-Workflow teilnehmen soll, muss zumindest der Gruppe "**Invoice**" zugeordnet werden. Hierdurch erhalten die User grundsätzlich Lese- und Schreib-Berechtigungen auf Mappen vom Typen "**Invoice**".
Bestimmte Gruppen wie "**Administration**", "**WorkflowError**", "**WorkflowRulesError**" und "**TechAccessProfile**" sowie der Benutzer "**import**" erhalten gesonderte Berechtigungen.
Projektspezifisch können weitere Mappenrechte definiert werden. Zum Beispiel könnte eine Gruppe "**InvoiceRead**" eingerichtet werden, die den Usern nur Leserechte auf Vorgänge gibt.



Gruppe	Benutzer	lesen	schreib...	löschen	versend...	archivier...	als E-Mail verse...	kopier...	verschieb...	anleg...	Mappentyp ä...	PDF erstellen (dru...	Versendung st...	Status anzei...	Monitor anz...	abbrec...
Administration		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
WorkflowError		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
WorkflowRulesError		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
TechAccessProfile		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	import (Import ...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Invoice		✓	✓			✓	✓	✓				✓		✓	✓	

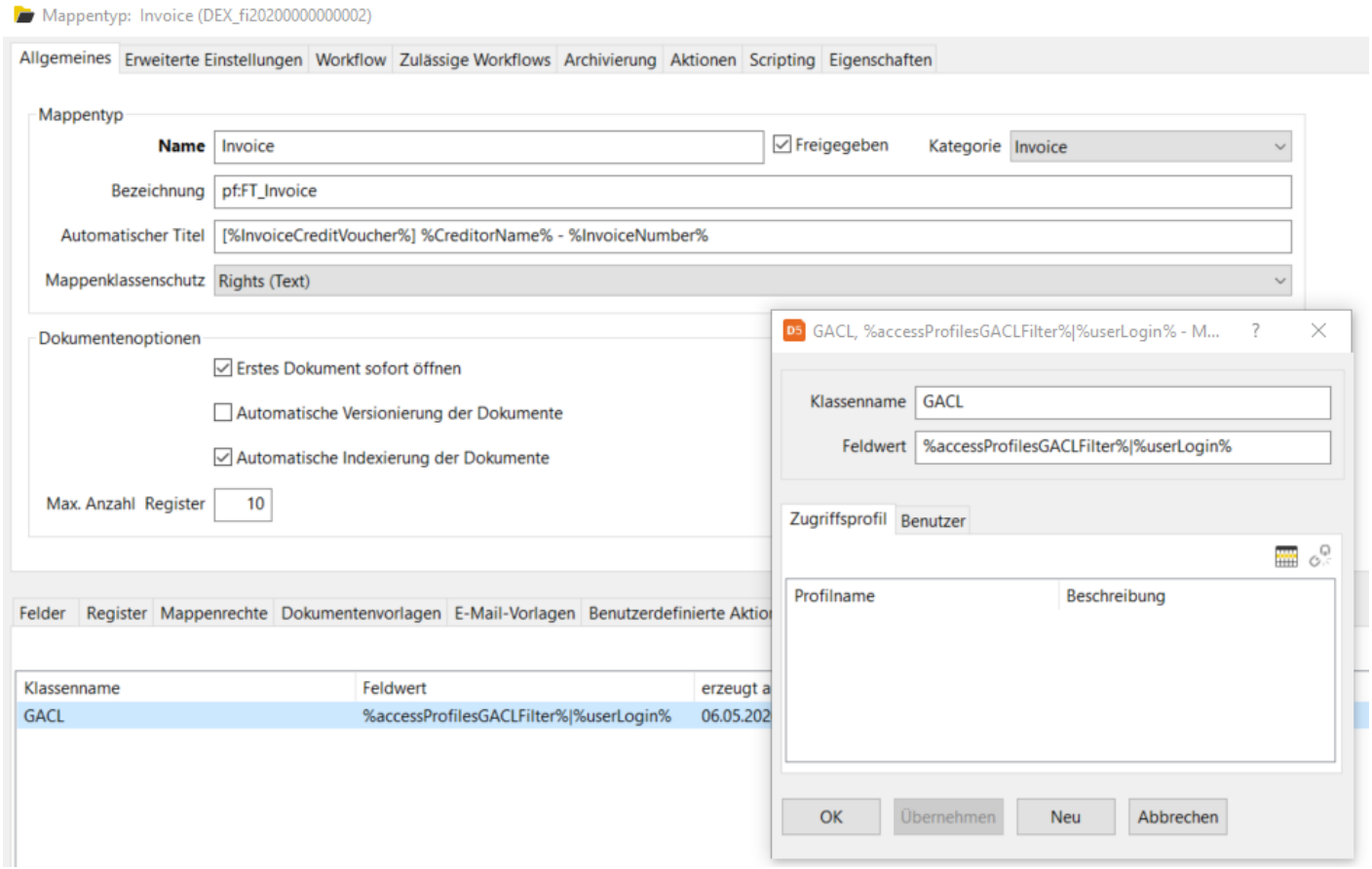
Ein Benutzer, welcher keiner der oben genannten Gruppen zugeordnet wurde, erhält keinen Zugriff auf die Outbar für die Rechnungseingänge und schon gar nicht zur Administrations-Outbar. Der Anwender kann nicht einmal nach Rechnungen suchen.



GACL-Berechtigung

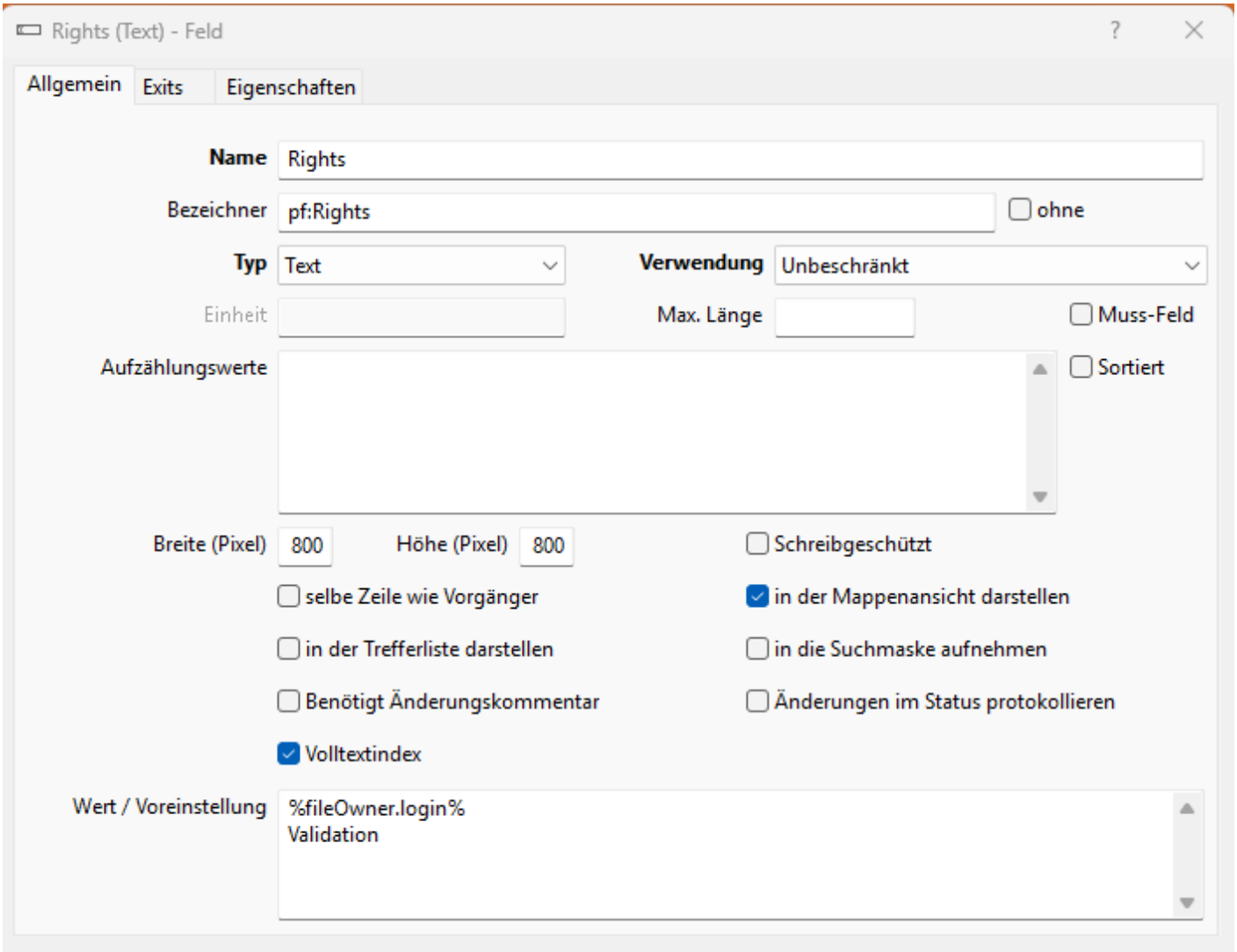
Der sogenannte Mappenklassenschutz definiert, welche User auf welche Vorgänge Zugriff haben. Der Zugriff wird über eine Liste gesteuert, in der User-Logins und technische Gruppen-Namen gelistet werden. Wenn ein User keinen Zugriff auf einen Vorgang hat, kann der User den Vorgang nicht sehen! Über die Suche erhalten die User nur Treffer auf Vorgänge, zu denen die User GACL-Berechtigungen haben!

Der Mappenklassenschutz wurde über eine **G**roup **A**ccess **C**ontrol **L**ist (**GACL**) mit dem Filter "**%accessProfilesGACLFilter%|%userLogin%**" über das Textfeld "**Rights**" umgesetzt. Die GACL berücksichtigt Access Profiles (Gruppen) und Benutzer-Logins.



Ein Benutzer erhält Zugriff zu einem Vorgang (einer sogenannten Mappe), wenn entweder sein Login in dem Textfeld enthalten ist oder wenn der Benutzer einer Gruppe angehört und der technische Name der Gruppe im Feld enthalten ist. Die einzelnen Einträge werden im Feld mit einem Zeilenumbruch getrennt ("**\r\n**").

Am Feld "**Rights**" müssen Voreinstellungen gesetzt sein. Über den Eintrag "**%fileOwner.login%**" erhält der Ersteller der Vorgänge initiale Zugriffsberechtigungen. Da der Workflow nicht direkt startet (und somit nicht automatisch weitere Berechtigungen vergeben werden), sollte zumindest eine Gruppen als Voreinstellung gesetzt werden, damit die Rechnungen für die User der Gruppe auffindbar sind. Dies ist bei der Einrichtung eines neuen Projekts zu Berücksichtigen.



Der Feldwert vom Feld "**Rights**" setzt sich aus 2 anderen Feldwerten zusammen. Zum einen werden über den Workflow Berechtigungen im Feld "**RightsWorkflow**" gesammelt. Zum anderen können über eine WEB-Konfiguration initiale Berechtigungen vergeben werden. Die initialen Berechtigungen werden in das Feld "**RightsInitial**" geschrieben. Die Summe der beiden Feldwerte wird in das Feld "**Rights**" geschrieben:

RightsWorkflow + RightsInitial = Rights

Workflow Berechtigungen

Jeder Benutzer bzw. jede Gruppe, welche im Laufe des Workflows den Beleg sperrt, wird zum Feld "**RightsWorkflow**" hinzugefügt. Die Berechtigungen werden zum Beispiel bei der Zuordnung über die Workflow-Regeln erweitert - aber auch bei jeder Weiterleitung oder bei einer Rückfrage. Wenn ein einzelner User zugeordnet wird und dieser User ist abwesend, dann wird automatisch auch die zuständige Vertretung des Users berechtigt.

Jedes Mal wenn die Workflow-Berechtigungen erweitert werden, werden auch die initialen Berechtigungen erneut ermittelt und gesetzt! Im Anschluss wird aus den beiden Feldwerten der

Feldwert "**Rights**" gebildet.

Initiale Berechtigungen

Über die initialen Berechtigungen können Benutzer und Gruppen Zugriff auf alle Vorgänge/Mappen erhalten bzw. können Berechtigungen abhängig von Feldwerten definiert werden. Zum Beispiel können grundsätzliche Zugriffs-Berechtigungen pro Mandant definiert werden.

Benutzer für den Support oder der Job-ausführende Benutzer müssen zum Beispiel immer Zugriff auf alle Vorgänge/Mappen haben! Diese Einstellung kann auf der Administrations-Outbar "**Invoice**" über die WEB-Konfiguration "**Initiale Berechtigungen**" vorgenommen werden.



Die Berechtigungen können allerdings auch abhängig von Feldwerten gesetzt werden und diese Feldwerte können sich im Laufe des Workflows ändern. Zum Beispiel können Gruppen oder Benutzer abhängig vom Mandanten berechtigt werden. Wenn der Mandant allerdings nicht automatisch oder gar falsch erkannt wurde, kann sich der Feldwert und somit die Zuordnung der berechtigten Gruppen im Workflow-Verlauf ändern. Anders als das "initial" vermuten lässt, werden die Gruppen nach jeder Weiterleitung erneut ermittelt und in das Feld "**RightsInitial**" wird neu geschrieben. Durch Feldwert-Anpassungen kann es passieren, dass Benutzer oder Gruppen Ihre Zugriffsberechtigung erst verzögert durch einen geänderten Feldwert erhalten und es kann auch passieren, dass Benutzer durch Feldwertänderungen Ihre Zugriffsberechtigungen wieder verlieren.

Pro Eintrag in der WEB-Konfiguration können bis zu 3 Feldwerte abgefragt werden. Es werden immer alle Einträge überprüft!

Berechtigungen im Archiv

Die Berechtigungen im Archiv richten sich nach dem angeschlossenen Archiv sind sind projektspezifisch zu klären! Bei einem schemabasierten Archiv wird die gesamte Berechtigungs-Struktur im Archiv gehalten. Hier muss eine eigenes Berechtigungs-Konzept entwickelt werden.

In der Regel werden in den Projekten schemalose Archive eingesetzt, wo die Zugriffsberechtigungen durch das angeschlossene System gesteuert werden. Bei diesen Archivien bleiben die GACL-Zugriffsberechtigungen erhalten. die Anwender finden auch im Archiv nur die Belege, auf die Sie bereits im Workflow Zugriff erhalten haben.

Revision #16
Created 2020-06-05 11:23:36 UTC by Markus Meisner
Updated 2025-07-16 09:02:45 UTC by Markus Meisner