

Rechesystem

1	Einleitung.....	1
1.1	Menübaum.....	1
1.2	Entitäten-Popups	2
1.3	Entitäten-Reiter	3
1.4	Frei definierbare Policies	3
2	Supervisor-Funktion	3
3	Aufbau / Verhältnis Benutzer zu Gruppe	3

1 Einleitung

Im easyFramework werden Zugriffsrechte auf verschiedene Bereiche unterteilt, die da wären:

- Menübaum
- Entitäten-Popups
- Entitäten-Reiter
- Frei definierbare Policies

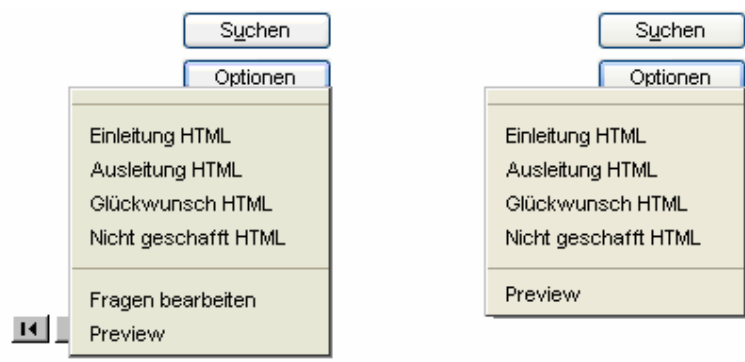
1.1 Menübaum

Mit en Zuordnungen von Benutzern und Benutzergruppen zu Menübaumeinträgen, können Sie steuern, wer Zugriff auf welche Funktionen im Menübaum. Steht eine Funktion einem Benutzer nicht zur Verfügung, so wird diese aus dem Baum ausgeblendet.

1.2 Entitäten-Popups

Mit en Zuordnungen von Benutzern und Benutzergruppen zu Entitäten-Popups, können Sie steuern, wer Zugriff auf welche Popup-Einträge zu einer gewissen Entität hat. Steht eine Funktion einem Benutzer nicht zur Verfügung, so wird diese nicht angezeigt.

Wenn Sie z.B. den Eintrag „per Mail versenden“ oder „Preview“ im Entitäten-Popup definiert haben, können Sie einstellen welche Benutzer darauf zugriff haben und welche nicht, z.B.:



(im zweiten Bild hat der Benutzer keinen Zugriff auf „Fragen bearbeiten“)

1.3 Entitäten-Reiter

Mit en Zuordnungen von Benutzern und Benutzergruppen zu Entitäten-Reitern, können Sie steuern, wer Zugriff auf welche Reiter im Entitäten-Bearbeitungsdialog hat. Steht ein Reiter einem Benutzer nicht zur Verfügung, so wird dieser nicht angezeigt, z.B.:

The first screenshot shows a dialog with three tabs: 'Daten', 'Publikation', and 'Info'. The 'Daten' tab is active, showing fields for 'Name' (test2), 'externe Web-ID', 'Status' (In Entwicklung), and 'Art'. The second screenshot shows the same dialog but with only the 'Daten' tab visible, indicating that the user does not have access to the 'Publikation' and 'Info' tabs.

(Im zweiten Bild hat der Benutzer keinen Zugriff auf „Publikationen“ und „Info“)

1.4 Frei definierbare Policies

Mit den Policies haben Sie die Möglichkeit, freie Text-Strings zu definieren, z.B. „**Benutzer darf Memos ausdrucken**“. Im Programmcode können Sie dann eine Methode aufrufen, in der Art **bHasAccess(„Benutzer darf Memos ausdrucken“)**. Wenn der Benutzer ein Zugriffsrecht hat, können Sie den entsprechenden Programmcode zum Drucken ausführen.

2 Supervisor-Funktion

In Tabelle tsUsers ist ein BIT-Feld namens „usr_supervisor“ hinterlegt. Ist dieses Feld bei einem Benutzer auf TRUE, so darf dieser Benutzer alles. Er hat immer Vollzugriff. Sinnvoll ist dieses Flag für Sysadmins, die das System prüfen und anderen Benutzern Rechte zuweisen.

3 Aufbau / Verhältnis Benutzer zu Gruppe

In den Tabellen tsUsers und tsUserGroups werden Benutzer und Benutzergruppen gehalten. Es lassen sich Zugriffe sowohl für Benutzergruppen, als auch für einzelne Benutzer festlegen. Der Gedanke ist: falls für einen Benutzer nichts festgelegt ist, so gelten die Einstellungen der Benutzergruppe.

Da ein Benutzer in mehreren Gruppen Mitglied sein kann (ähnlich wie im Windows-Rechtesystem), erhält er den maximal möglichen Zugriff aus den Gruppen. Gehört er beispielsweise zur Gruppe Gast und Administratoren, und die Gruppe Gast hat

keinen Zugriff auf Policy A, jedoch die Gruppe Administratoren, so hat der Benutzer Zugriff auf Policy A.

Man kann einzelnen Benutzer auch explizit ein Recht geben oder nicht, z.B. könnte man einem Benutzer aus den Administratoren das Recht auf die Policy A nehmen, obwohl er eben Administrator ist.

Hierzu gibt es in den Datenbanktabellen auf Benutzerebene das Feld „*_explicit_access“, ein Bit-Feld, welches angibt, ob der Benutzer, trotz irgendwelcher Gruppen, das Recht besitzt oder nicht.

Ein Beispiel sind die Tabellen **tsMenuAccessTsUsers** und **tsMenuAccessTsUserGroups**, welche den Zugriff auf die Hauptmenüeinträge regeln.

Liegt beispielsweise kein Datensatz für einen Benutzer in Tabelle tsMenuAccessTsUsers vor, so gilt allein die Gruppenrichtlinie für den Zugriff. Ist in Tabelle tsMenuAccessTsUsers explizit ein Zugriff definiert, so erhält der Benutzer den Zugriff.