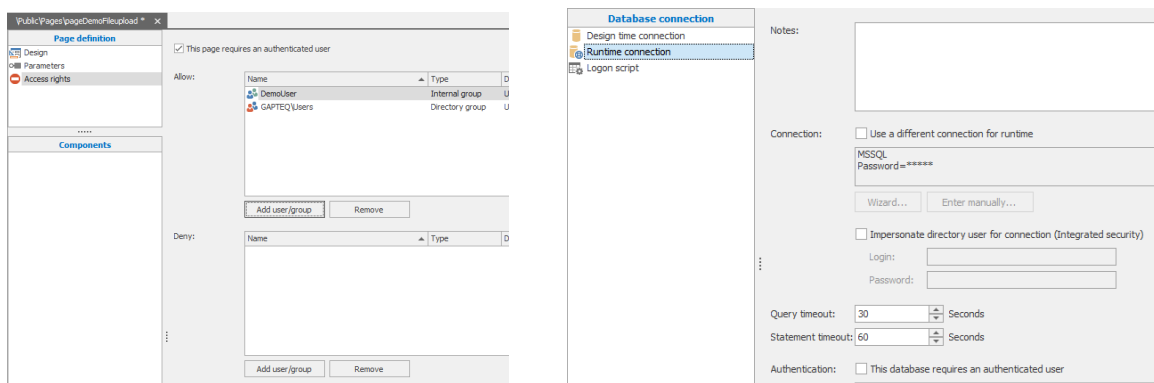


GAPTEQ-FEATURES KURZ ERKLÄRT

Zugangsberechtigungen zielgerichtet über Access Rights steuern

GAPTEQ-Applikationen können öffentlich zugänglich oder nur mit User-Login erreichbar sein. Die Zugriffsbeschränkungen können flexibel pro Seite oder global für alle Seiten einer Applikation gesetzt werden. Beim Erstellen einer Seite ist die Standardeinstellung auf öffentlich gesetzt.



Verschiedene Wege zum Setzen von Zugangsberechtigungen in GAPTEQ.

IHRE VORTEILE

- Verschiedene Zugangsberechtigungen innerhalb einer Applikation.
- Flexibles Arbeiten pro Repository Server.
- Smarter Übergang aus einem öffentlichen zu einem Login-gebundenen Bereich.

DAS FEATURE

Access Rights

Über Access Rights steuern Sie je Seite, ob diese öffentlich erreichbar ist oder ob für den Zugang ein User-Login benötigt wird. Neben dem Arbeiten auf Seiten-Ebene können Zugriffsrechte auch für alle Seiten global eingestellt werden oder an die Datenbank-Abfrage gekoppelt sein.

SO GEHT'S – SCHRITT FÜR SCHRITT

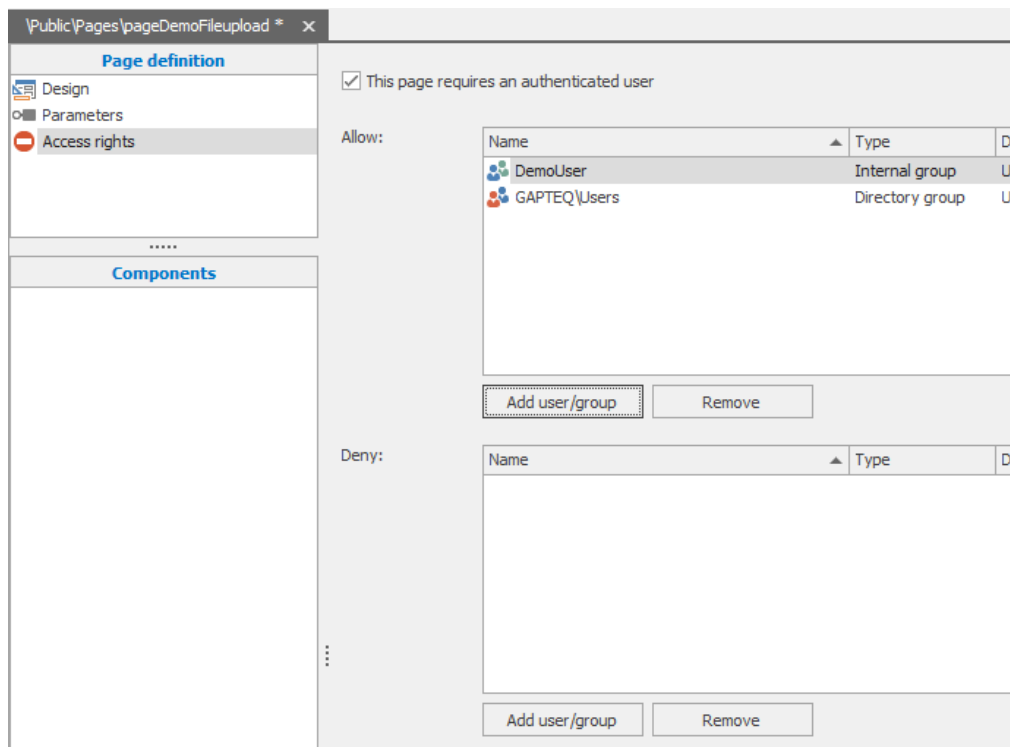
1. Access Rights auf Page-Ebene
2. Globale Einstellungen auf Repository-Ebene
3. User-Login für alle Seiten mit Datenbank-Abfrage

1. Access Rights auf Page-Ebene

Um die Zugriffsberechtigungen auf Seitenebene zu definieren, wechseln Sie im GAPTEQ-Designer im Bereich Page Definition auf Access Rights und haken die Checkbox **"This page requires an authenticated user "** an.

Soll die Seite nur für bestimmte User oder User-Gruppen erreichbar sein, schränken Sie den Zugriff durch Auswahl bei **"Allow: Add User/Group"** weiter ein.

Möchten Sie eine User-Gruppe oder einzelne User gänzlich ausschließen, wählen Sie **„Deny: Add User/Group“** und wählen anschließend die entsprechenden User oder User-Gruppe aus der Liste.



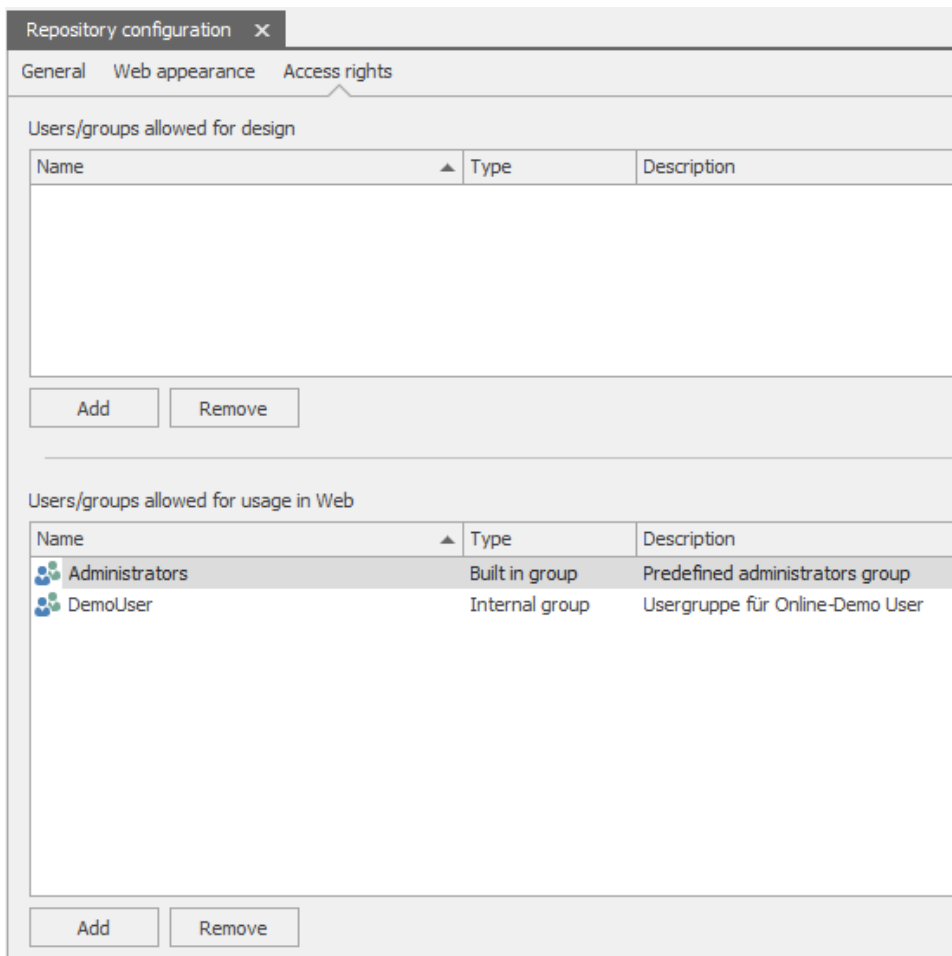
2. Globale Einstellungen auf Repository-Ebene

Bevor Sie für einzelne Seiten Zugriffsbeschränkungen setzen, definieren Sie auf Repository Ebene User und User-Gruppen, die für den Zugriff auf das Frontend Ihrer Applikation berechtigt sind.

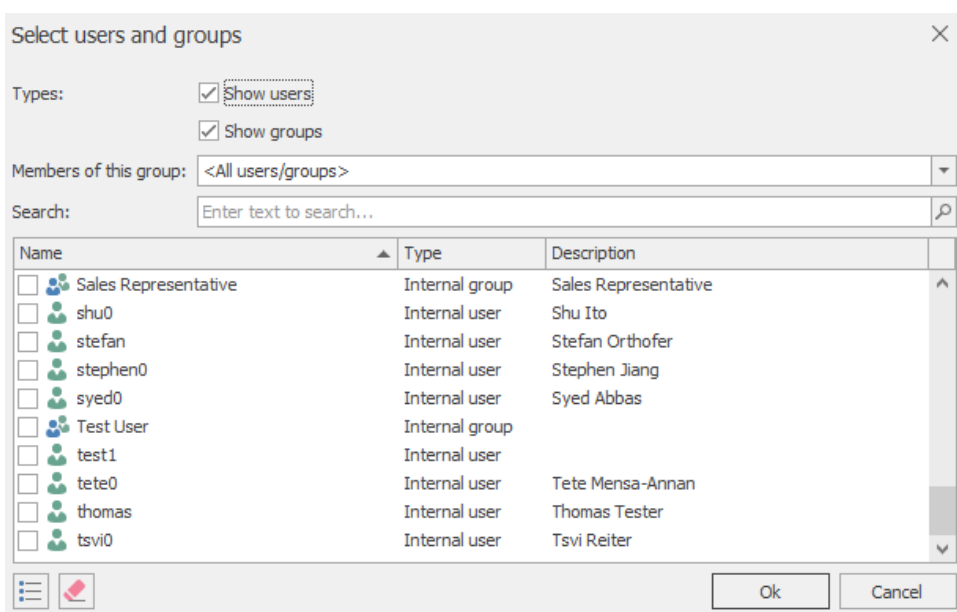
Wir empfehlen in der User-Verwaltung mindestens eine User-Gruppe für Frontend-User zu erstellen und diese bei **„Users/groups allowed for usage in Web“** zu hinterlegen.

TIPP: Sollten Sie auf Ihrem GAPTEQ-Server mit mehreren Repositories arbeiten, können Sie für jede Applikation eine User-Gruppe mit Frontend-Usern erstellen und so vorab schon definieren, welche User auf die jeweilige Applikation zugreifen dürfen.

Die Einstellungen finden Sie im GAPTEQ-Designer unter dem Menüpunkt **„Repository configuration“** im Reiter **„Access rights“**.

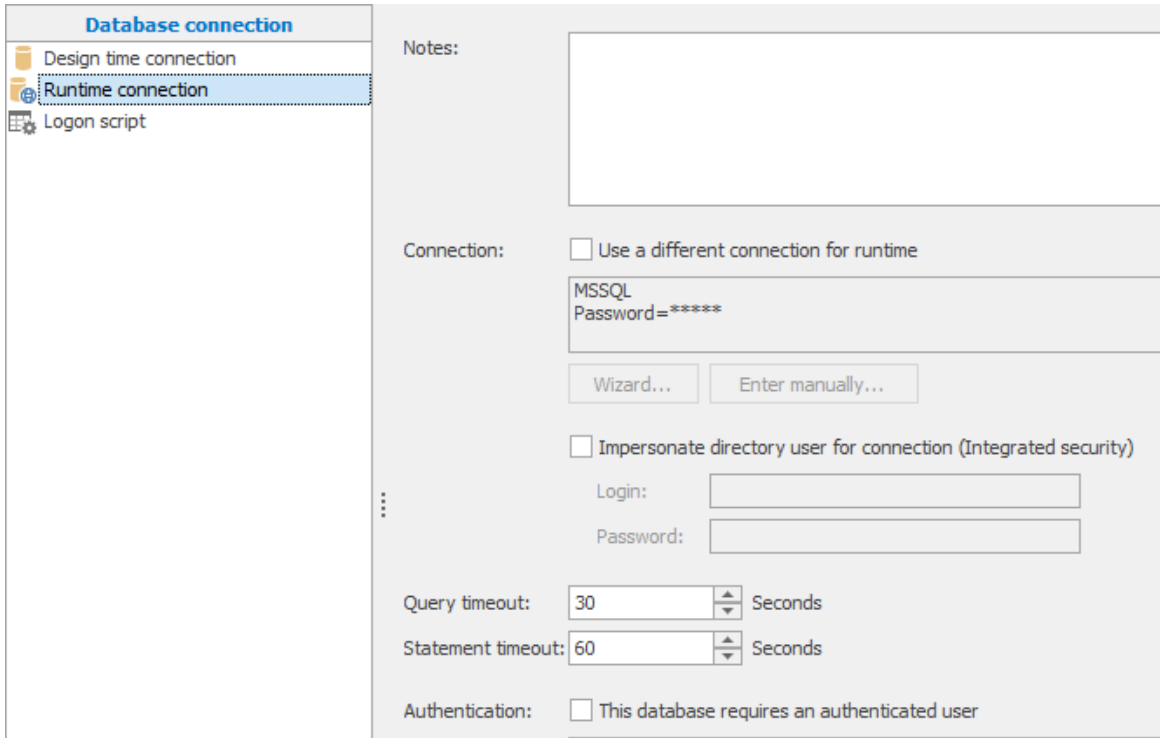


Ein Klick auf „Add“ öffnet den nachfolgenden Dialog zur Auswahl der gewünschten User und User-Gruppen.



3. User-Login für alle Seiten mit Datenbank-Abfrage

Wenn Sie in den Einstellungen der Database Connection unter Runtime Connection die Checkbox "This database requires an authenticated user" anhaken, wird für alle Seiten mit Datenbank-Zugriff ein User-Login gefordert.



The screenshot shows the 'Database connection' settings window. On the left, a tree view shows 'Design time connection', 'Runtime connection' (selected), and 'Logon script'. The main area is divided into sections: 'Notes' (empty), 'Connection' (with a checkbox 'Use a different connection for runtime' and 'MSSQL Password=*****'), 'Impersonate directory user for connection (Integrated security)' (checkbox), 'Login:' and 'Password:' (text boxes), 'Query timeout: 30 Seconds' and 'Statement timeout: 60 Seconds' (spinners), and 'Authentication:' (checkbox 'This database requires an authenticated user').

So können Sie festlegen, dass bei Datenbank-Zugriff ein User-Login zwingend notwendig ist auch wenn für einzelne Seiten keine Zugriffsbeschränkung angegeben wurde.

HINWEIS: Diese Einstellung können Sie nicht verwenden, wenn Ihre Applikation neben LogIn-gebundenen auch öffentliche Seiten umfassen soll.