

Intranet

How To

Einrichten von zugangsbeschränkten Bereichen im myTUM-Portal

Version 1.0
preliminary

TUM WWW & Online Services
Richard-Wagner-Strasse 18
D-80333 München

E-Mail: info@ze.tum.de

Alle in dieser Dokumentation enthaltenen Informationen, Kenntnisse und Darstellungen sind alleiniges Eigentum von Syslab.com und von WWW & Online Services der Technischen Universität München.

Die Dokumentation bzw. die darin enthaltenen Informationen, Kenntnisse und Darstellungen dürfen ohne vorherige schriftliche Zustimmung von WWW & Online Services oder Syslab.com weder vollständig noch auszugsweise, direkt oder indirekt Dritten zugänglich gemacht, veröffentlicht oder anderweitig verbreitet werden.

Das Portalsystem ElevateIT ist eine gemeinsame Entwicklung der Syslab.com, München und der Arbeitsgruppe WWW & Online Service der Technischen Universität München. ElevateIT ist Open Source. Unabhängig davon bleiben die im Rahmen von ElevateIT von Syslab.com und dem Entwicklerteam entwickelten Technologien geistiges Eigentum der Beteiligten.

Die Geltendmachung aller diesbezüglichen Rechte, insbesondere für den Fall der Erteilung von Patenten, bleiben der Syslab.com, der Technischen Universität München und dem Entwicklerteam von WWW & Online Services vorbehalten.

Die Übergabe dieser Dokumentation begründet keinerlei Anspruch auf eine Lizenz oder Benutzung.

Entwicklerteam der Technischen Universität München:

Dr. rer.-nat. Thomas Wagner (Wissenschaftliche Leitung)

Dipl.-Ing. Thomas Mehlhart

Gerhard Schmidt

Christian Hamm

© 2008

Technische Universität München,
WWW & Online Services

Inhaltsverzeichnis

1	Allgemeines	1
2	Voraussetzungen und Limitationen	1
3	Vorgehensweise	2
3.1	Zugriffsbeschränkung auf angemeldete Benutzer, Studierende, Mitarbeiter oder Alumni	2
3.2	Zugriffsbeschränkung auf explizite Benutzer oder die Mitglieder einer MetaGroup	6
3.3	Zugriffsbeschränkung aufheben	7
4	Trouble Shooting	8

1 Allgemeines

Dieses HowTo beschreibt die Einrichtung von zugangsbeschränkten Bereichen im myTUM-Portal für bestimmte Rollen. Der Zugang zu einzelnen Bereichen (Unterverzeichnissen) kann so eingeschränkt werden, dass nur angemeldete Benutzer oder nur Benutzer mit einer speziellen Rolle die in diesem Bereich enthaltenen Daten und Informationen abrufen können. Es werden zwei Fälle unterschieden:

1. Beschränkung auf eine oder mehrere der folgenden Personengruppen: Angemeldete Benutzer, Mitarbeiter, Studenten, Alumni 2. Beschränkung auf Explizite Personen oder die Mitglieder einer Metagruppe

Soll der Zugriff auf Angehörige einer (oder mehrerer) der Personengruppen 'Authenticated' (angemeldete Benutzer), 'Studenten', 'Mitarbeiter' oder 'Alumni' beschränkt werden, kann die Einstellung direkt im jeweiligen Bereich vorgenommen werden. Darüberhinaus sind keine weiteren Maßnahmen notwendig.

Soll der Zugriff auf einen bestimmten, nicht durch die oben genannten Gruppen abgegrenzten, Personenbereich (explizite Benutzer oder MetaGroups) beschränkt werden, ist ein zusätzlicher Schritt notwendig indem diesen Personen und/oder Gruppen zunächst die lokale Rolle 'Participant' zugewiesen wird und dann die Zugriffsberechtigung auf diese Rolle eingeschränkt wird.

2 Voraussetzungen und Limitationen

Um die Zugangsbeschränkung einzustellen müssen Sie über eine Portalkennung verfügen und für den zu beschränkenden Bereich SubsiteManager-Rechte haben. Sie können die Rechte ausserdem nur dann einschränken, wenn Sie mindestens über eine Ihrer Rollen in diesem Bereich auch nach der Einschränkung noch explizit zugriffsberechtigt sind.

Wenn bereits in einem übergeordneten Bereich eine Einschränkung existiert, können Sie diese zwar weiter einschränken, nicht jedoch erweitern, d.h. wenn in einem übergeordneten Bereich der Zugriff auf die Gruppen 'Mitarbeiter' und 'Studierende' beschränkt ist, können Sie zwar für Ihren Bereich nur 'Mitarbeiter' zulassen, nicht aber 'Alumni', da diese bereits im übergeordneten Bereich ausgeschlossen sind.

Grundsätzlich kann die Beschränkung nur auf Benutzer mit einer gültigen myTUM-Kennung erfolgen, Zugriffsbeschränkungen mit Passwort oder Bereiche für einen eingeschränkten Benutzerkreis ohne myTUM-Kennung sind nicht möglich.

3 Vorgehensweise

3.1 Zugriffsbeschränkung auf angemeldete Benutzer, Studierende, Mitarbeiter oder Alumni

Rufen Sie dazu den Bereich auf, für welchen Sie die Zugriffsbeschränkung einstellen wollen. Schalten Sie dort auf die Inhaltssicht um und wählen Sie die Aktion 'Manage Access' aus. Ist diese Aktion nicht eingeblendet, haben Sie keine Berechtigung die Zugriffseinstellungen zu ändern.

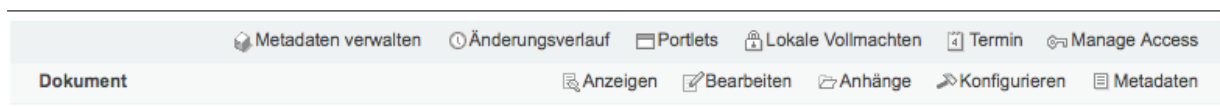


Abbildung 1: Aktionsleiste mit Schaltfläche 'Manage Access'

Es erscheint das Formular zur Acquisitionseinstellung mit einer Übersicht über die Zugriffs- und Acquisitions-Einstellungen für den Pfad des aufgerufenen Bereichs. Der von Ihnen gewünschte Bereich entspricht dabei dem untersten Eintrag. Für Bereiche, deren Einstellung Sie nicht ändern können, sind die Formularelemente disabled, d.h. grau dargestellt und nicht anwählbar.

Die Anzeige der übergeordneten Bereiche ist notwendig, da auch dort bereits der Zugriff eingeschränkt sein kann. Alle Beschränkungen sind durch einen orangenen Text hervorgehoben. Für jede Einschränkung ist ausserdem angegeben, welche Rollen explizit berechtigt sind.

**ACQUISITION STATE FOR CONTEXT:
/STUDIUM/FOLDER_LISTING**

Diese Übersicht zeigt den Acquisitionsstatus des aktuellen Contexts und seiner Parents

[TUM_Portal](#), Eigentümer: [unknown](#)

Allgemeine Acquisition

eingeschaltet

Rollen Acquisition

eingeschaltet

Acquisition Berechtigungen

Inhalte einsehen (View)

explicit: Alumnus

Alumnus
Anonymous
Archivemanager
Authenticated

Inhalte bearbeiten (Modify portal content)

explicit: Anonymous, Archivemanager

Alumnus
Anonymous
Archivemanager
Authenticated

[studium](#), Eigentümer: [Thomas Wagner](#)

Allgemeine Acquisition

eingeschaltet

Rollen Acquisition

eingeschaltet

Acquisition Berechtigungen

Inhalte einsehen (View)

explicit: Archivemanager

Alumnus
Anonymous
Archivemanager
Authenticated

Inhalte bearbeiten (Modify portal content)

explicit:

Alumnus
Anonymous
Archivemanager
Authenticated

Abbildung 2: Acquisitionseinstellungen im Context

Wenn die Acquisitionseinstellungen weitere Berechtigungen eingeschränkt sind wird dies zusätzlich angegeben. Eine Änderung ist nur durch den Manager möglich.

TUM Portal, Eigentümer: [unknown](#)

Allgemeine Acquisition eingeschaltet**Rollen Acquisition** eingeschaltet**Acquisition Berechtigungen** Inhalte einsehen (View)

explicit: Alumnus

 Inhalte bearbeiten (Modify portal content)

explicit: Anonymous, Archivemanager

Hinweis:

Die Acquisition weiterer Berechtigungen ist ausgeschaltet. Diese können nur von einem Benutzer der Rolle 'Manager' oder dem Eigentümer bearbeitet werden:

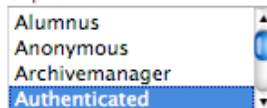
Acquisition: [manage](#)

Abbildung 3: Acquisitionseinstellungen im Context

Zur Zugriffsbeschränkung ist ausschließlich die Einstellung 'Inhalte einsehen (View)' relevant. Um den Zugriff einzuschränken, schalten Sie für Ihren Bereich unter dem Punkt 'Acquisition Berechtigungen' die Option 'Inhalte einsehen (View)' aus.

Inhalte bearbeiten (Modify portal content)

explicit:

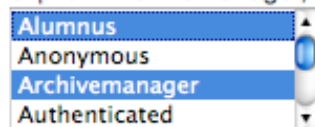


Alumnus
Anonymous
Archivemanager
Authenticated

Abbildung 4: Ausschalten der View-Rechte

Damit entziehen Sie allen Nutzern den Zugang. Nun müssen Sie noch angeben, welche Rollen zukünftig explizit Zugang zu dem Bereich haben sollen. Wählen Sie diese in der Auswahlbox aus.

explicit: Archivemanager, Manager



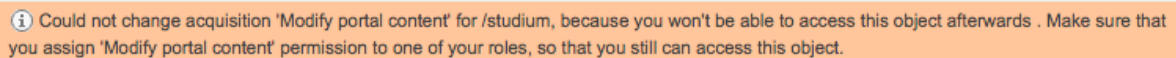
Alumnus
Anonymous
Archivemanager
Authenticated

Abbildung 5: Auswahl der Rollen, die explizite View-Rechte erhalten sollen

Dabei müssen Sie sicherstellen, dass mindestens eine Ihrer eigenen Rollen (im Zweifelsfall immer 'SubsiteManager') selektiert ist, damit Sie auch selbst weiter Zugriff auf die Daten haben.

Bitte verwenden Sie nur die Rollen 'Authenticated', 'Students', 'Mitarbeiter' oder 'Alumni' und wenn erforderlich 'SubsiteManager'. Alle Benutzer gehören immer mindestens einer dieser Gruppen an. Die übrigen Rollen sind funktionale Rollen und im Hinblick auf Benutzer und Berechtigungen unterschiedlich belegt. Ihr Einsatz für Zugriffsbeschränkung ist (abgesehen von 'SubsiteManager') nicht sinnvoll und führt gegebenenfalls nur dazu, dass der Überblick über die Berechtigungen verloren geht.

Mit Save speichern Sie die Einstellungen ab. Achten Sie dabei auf die Statusmeldung: Wenn die Einstellungen Ihren eigenen Zugriff beschränken, Sie also keine weiteren Einstellungen mehr vornehmen könnten, erscheint eine Fehlermeldung und die Einstellungen werden nicht vorgenommen.

An orange warning message box with a white background and a thin border. It contains an information icon (i) followed by the text: "Could not change acquisition 'Modify portal content' for /studium, because you won't be able to access this object afterwards . Make sure that you assign 'Modify portal content' permission to one of your roles, so that you still can access this object."/>


 Could not change acquisition 'Modify portal content' for /studium, because you won't be able to access this object afterwards . Make sure that you assign 'Modify portal content' permission to one of your roles, so that you still can access this object.

Abbildung 6: Warnmeldung, wenn Sie Ihre eigenen Berechtigungen einschränken würden.

3.2 Zugriffsbeschränkung auf explizite Benutzer oder die Mitglieder einer MetaGroup

Um die Zugriff auf explizite Personen oder eine oder mehrere MetaGroups zu beschränken sind etwas mehr Arbeitsschritte notwendig.

Rufen Sie zunächst den gewünschten Bereich auf, für den Sie die Zugangsbeschränkung einrichten wollen. Schalten Sie dort auf die Inhaltssicht um. Anschließend wählen Sie die Aktion 'Lokale Rollen' aus.

Assign local role to users and/or groups

Zuzuweisende bzw. zu entziehende Rollen

- ObjectAdmin
- ObjectUser
- Participant**
- PortalManager
- Questionnaire Author
- Redakteur
- Sszteam
- Studenten

Diese Rolle(n) sollen folgenden Usern bzw. Gruppen zugewiesen/entzogen werden:

Benutzer

`erika.mustermann@mytum.de`

Abbildung 7: Rolle 'Participant' an Benutzer vergeben

Weisen Sie den gewünschten Benutzern bzw. Gruppen die lokale Rolle 'Participants' zu und speichern Sie die Einstellung ab.

Rufen Sie anschließend über die Aktion 'Manage Access' das Formular zu den Acquisitionseinstellungen auf. Gehen Sie nun wie unter ... beschrieben vor, schalten Sie die Acquisition für 'Inhalte einsehen (View)' aus und weisen Sie die Berechtigung explizit der Rolle 'Participants' zu.

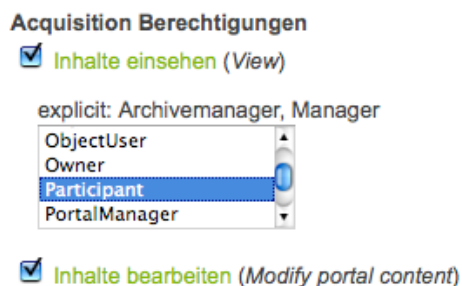


Abbildung 8: View-Berechtigung an Rolle 'Participant' explizit vergeben

Um sicherzustellen, dass Sie selbst weiterhin Zugriff auf den Bereich haben fügen Sie sicherheitshalber die Rolle 'SubsiteManager' hinzu.

Speichern Sie die Einstellungen mit 'Save' ab und achten Sie auf die Statusmeldung des Portals.

Wenn Sie eine größere Zahl von expliziten Personen berechtigen wollen, empfiehlt es sich, eine MetaGroup mit den zu berechtigenden Personen einzurichten. Dies erleichtert die Administration und erhöht die Transparenz.

Über die Pseudogruppen-Funktionalität von MetaGroups können auch komplexere Zugriffsregeln erstellt werden, z.B. für alle Studierende eines Studiengangs, die Teilnehmer an einer Veranstaltung usw. Lesen Sie dazu die entsprechende Anleitung im User Manual 'MetaGroups'.

3.3 Zugriffsbeschränkung aufheben

Um eine Zugangsbeschränkung für Ihren Bereich aufzuheben rufen Sie den Bereich zunächst auf. Wählen Sie die Inhaltssicht und klicken Sie in der Aktionsleiste auf 'Manage access'.

Setzen Sie in Ihrem Bereich die Checkbox 'Inhalte einsehen (View)' und löschen Sie in der Auswahlbox die explizit ermächtigten Rollen. Anschließend speichern Sie die Einstellungen mit 'Save' ab.

Beachten Sie jedoch, dass der Zugriff auch in einem übergeordneten Bereich beschränkt sein kann. Sie können dann zwar die Zugangsbeschränkungen für Ihren Bereich ändern, allerdings gelten für alle Benutzer dann die Beschränkungen des übergeordneten Bereichs.

[studium](#), Eigentümer: [Thomas Wagner](#)

Allgemeine Acquisition eingeschaltet**Rollen Acquisition** eingeschaltet**Acquisition Berechtigungen** Inhalte einsehen (View)

explicit: Archivemanager, Manager

Alumnus
Anonymous
Archivemanager
Authenticated

 Inhalte bearbeiten (Modify portal content)

explicit:

Alumnus
Anonymous
Archivemanager
Authenticated

[studiengaenge](#), Eigentümer: [No owner](#)

Allgemeine Acquisition eingeschaltet**Rollen Acquisition** eingeschaltet**Acquisition Berechtigungen** Inhalte einsehen (View)

explicit: Alumnus, Anonymous, Archivemanager, Authenticated

Alumnus
Anonymous
Archivemanager
Authenticated

 Inhalte bearbeiten (Modify portal content)

explicit: Alumnus, Anonymous

Alumnus
Anonymous
Archivemanager
Authenticated

Abbildung 9: Im übergeordneten Bereich ausgeschaltete Berechtigung

4 Trouble Shooting

Prüfen Sie Ihre Berechtigungen mit Hilfe entsprechender Benutzer. Kontrollieren Sie die Einstellungen über den gesamten Pfad und achten Sie auch auf explizite Berechtigungen oder zusätzliche ausgeschaltete Acquisition.