



## Benutzer Handbuch

# DELMIA Process Engineer<sup>®</sup>

## Sicherheitsrichtlinien



# Inhaltsverzeichnis

<b>Sicherheitsrichtlinien</b>	<b>1</b>
<b>Inhaltsverzeichnis</b>	<b>2</b>
<b>Einleitung</b>	<b>3</b>
Wie Sie das Handbuch einsetzen	3
Wie Sie Zeichen und Symbole lesen	4
Was Sie zu Sicherheitsrichtlinien wissen sollten	5
Datenobjekte der Sicherheitsrichtlinien	6
Funktionsweise von Gruppenfiltern	7
Datenobjekte für Sicherheitsrichtlinien einblenden	8
Datenobjekte einblenden	8
Sicherheitsrichtlinien im Registrierungs-Editor aktivieren	11
Zugriffe und Änderung auf sicherheitsrelevante Daten protokollieren	13
Anwender in der Benutzerverwaltung anlegen	17
Aufenthaltort bei der Anmeldung einblenden	20
<b>Sicherheitsrichtlinien festlegen</b>	<b>22</b>
Übersicht Exportlizenzen verwenden	23
Rechte für Anwender auf sicherheitsrelevante Datenobjekte vergeben	25
Rechte für Anwender festlegen	26
Länder verwenden	30
Firmen verwenden	36
Verträge – und Abkommen verwenden	44
Export control classification (ECC) verwenden	47
Export Lizenzen verwenden	51
Zugriffsrechte auf PPR-Komponenten anwenden	55
Zugriffsrechte bearbeiten	56
PPR-Komponenten mit anderen Datenobjekten verknüpfen	59
Entscheidungstabelle für Exportlizenzen – wichtige Fälle	61
Fallbeispiele für Sicherheitsrichtlinien	65
Ausgangssituation Exportlizenz für Staatsbürger	66
Verknüpfungen vornehmen – Beispiel 1	68
Verknüpfungen vornehmen – Beispiel 2	76
Verknüpfungen vornehmen Beispiel 3	83
<b>Abbildungsverzeichnis</b>	<b>88</b>
<b>Index</b>	<b>91</b>

# Einleitung

Die Bedienung, Funktionsweise und Menüführung, die in diesem Benutzer Handbuch für die *Sicherheitsrichtlinien* beschrieben ist, wird Ihnen in diesem Handbuch auf einfache und verständliche Weise erklärt. Es zeigt kurz gesagt auf, wie Sie Sicherheitsrichtlinien für Projekte anwenden.

## Wie Sie das Handbuch einsetzen

Wie setzen Sie nun dieses Handbuch ein?

Dieses Handbuch ist bewusst knapp gehalten, damit Sie schnell die Bedienung und Funktionsweise kennen lernen. Kurz und knapp wird Ihnen gezeigt:

- Wie Sie Sicherheitsrichtlinien anlegen und bearbeiten.

Lesen Sie deshalb das Benutzer Handbuch für die Sicherheitsrichtlinien besonders gründlich durch. Lassen Sie sich führen: Verwenden Sie dazu das Inhaltsverzeichnis, die Überschriften und die Kopfzeile und folgen auch den Querverweisen, die Ihnen weitere Informationen liefern.

In diesem Benutzer Handbuch wird Ihnen gezeigt, wie Sie unter ökonomischen Aspekten Sicherheitsrichtlinien für den Zugriff von Fremdfirmen auf Ihre Daten regeln:

- Was Sie über Sicherheitsrichtlinien wissen müssen.
- Anlegen der Datenobjekte in der Systembibliothek.
- Wie Datenobjekte für den ökonomischen und effizienten Einsatz der Sicherheitsrichtlinien verwendet werden.
- Fallbeispiele für die grundlegende Anwendung der Sicherheitsrichtlinien.

Nutzen Sie das Wissen, das Sie aus diesem Handbuch ziehen, für alle weiteren Schritte im Process Engineer.



Sie müssen jetzt nur mit Lesen anfangen.



### Hinweis:

*Denken Sie daran, zu den in diesem Handbuch beschriebenen Funktionen für die Sicherheitsrichtlinien sollten Sie das Wissen aus dem Basis Handbuch hinzuziehen, in dem die allgemeine Einführung in den Process Engineer beschrieben wird.*



Hier rufen Sie das Benutzer Handbuch [Allgemeine Einführung](#) auf.

## Wie Sie Zeichen und Symbole lesen

Die Zeichen und Symbole, die in diesem und in allen weiteren Handbüchern verwendet werden, dienen nicht nur zur allgemeinen Verschönerung eines Handbuchs, obwohl das auch eine der Aufgaben ist, sie dienen vor allem der Benutzerführung, um Ihnen den Inhalt auf leicht verständliche Weise zu erklären. Kapitel und Kapitelabschnitte werden durch Überschriften eingeleitet. Die Überschriften haben entsprechend der Verwendung unterschiedliche Schriftgrößen.

Nachfolgend wird Ihnen die Bedeutung der Symbole erklärt:



Mit diesem Zeichen werden Textstellen bezeichnet, die den Funktionsumfang beschreiben, den Sie in einem Kapitel kennen lernen werden. Es steht daher in der Regel am Anfang eines Kapitels oder Abschnitts. Zudem werden wichtige Textstellen mit diesem Zeichen hervorgehoben.



### Hinweis

Mit diesem Symbol werden Hinweise gekennzeichnet, die zu einem Thema noch zusätzliche Informationen liefern, die für das Weiterarbeiten sehr wichtig sind. Das Hinweis-Zeichen kann sowohl an einem Kapitelanfang als auch bei einer bestimmten Textstelle im Kapitel stehen. Die Texte, die mit diesem Zeichen eingeleitet werden, sind zusätzlich mit dem Wort **Hinweis** gekennzeichnet. Der Text selbst ist immer kursiv geschrieben.



### Achtung

Mit diesem Symbol werden Sie auf Sachverhalte aufmerksam gemacht, die zu möglichen Fehlern bei der Bedienung des Programms führen könnten und die Sie daher beachten sollten. Das Achtung-Zeichen kann sowohl an einem Kapitelanfang als auch bei einer bestimmten Textstelle im Kapitel stehen. Die Texte, die mit diesem Zeichen eingeleitet werden, sind zusätzlich mit dem Wort **Achtung** gekennzeichnet. Der Text selbst ist immer kursiv geschrieben.

### Beispiel

Mit diesem Symbol werden Sie auf Beispiele aufmerksam gemacht, die einen Sachverhalt verdeutlichen.



Mit diesem Symbol werden die einzelnen Bedienschritte einer Handlungsanweisung gekennzeichnet. Mit Handlungsanweisungen werden Bedienschritte beschrieben, um beispielsweise ein Menü zu öffnen oder eine Funktion auszuführen.



Mit diesem Symbol werden Aufzählungen gekennzeichnet. Das Aufzählungssymbol kann sowohl für eine Gliederung eines Fließtextes verwendet werden als auch stichpunktartig Themenschwerpunkte aufzulisten.



Mit diesem Symbol werden Sie darauf aufmerksam gemacht, dass es zu diesem Thema noch weitere Informationen in einem anderen Handbuch gibt.

## Was Sie zu Sicherheitsrichtlinien wissen sollten

Das bestehende Rechtekonzept wird ab der Version PE R16 um neue Sicherheitsrichtlinien ergänzt, die zusätzlich zu dem bestehenden Rechtekonzept angewandt werden können.

Die Sicherheitsrichtlinien werden dazu verwendet, um das Eigentum an Objekten, die Vertraulichkeit von Informationen und den Zugriff auf Daten zu regeln, die entsprechend den länderspezifischen Ausführbestimmungen nach den geltenden gesetzlichen Bestimmungen erfüllt sein müssen.

Diese Sicherheitsrichtlinien können sich dabei auf Unternehmen, Länder und Benutzer beziehen.

Um den Zugriff auf PPR-Komponenten in Projekten entsprechend den Sicherheitsrichtlinien zu gewährleisten können Sie

- wie bisher Rechte an Objekten und Planungstypen für einzelne Anwender oder Gruppen vergeben,
- zusätzlich Sicherheitsstandards für Firmen festlegen, indem Sie Vertraulichkeitsstufen definieren und Fremdzugriffe auf firmenspezifische Daten mittels Verträge regeln,
- zusätzlich länderspezifisch geltenden gesetzlichen Bestimmungen regeln, indem Sie festlegen welche Daten Exportbestimmungen unterliegen, für welche Länder Exportlizenzen benötigt werden und welche Firmen Exportlizenzen erhalten.

Vertraulichkeitsstufen, welche bei einem Objekt oder seinen Kindern definiert sind, können im PPR-Navigator angezeigt und für Ausdrücke verwendet werden.



Siehe auch Benutzer Handbuch [Einstellungen](#).

Objekte, die diesen Sicherheitseinstellungen unterliegen, werden intern über den Server ausgefiltert. Mit Hilfe dieser Regelung wird der Zugriff auf PPR-Komponenten für Benutzer und Gruppen von Benutzern geregelt. Nach dem Filtern ist dem Anwender der Zugriff auf Objekte entweder erlaubt oder auch nicht.

Anwender und Gruppen von Anwendern werden wie bisher in der Benutzerverwaltung angelegt und müssen mit entsprechenden Funktionsrechten und Zugriffsrechten auf PPR-Komponenten versehen sein.

## Datenobjekte der Sicherheitsrichtlinien

Bevor Sie die Sicherheitseinstellungen den PPR-Komponenten zuweisen können, müssen folgende Datenobjekte in der Systembibliothek angelegt werden:

- Unternehmen,
- Verträge / Abkommen,
- Länder,
- Exportbeschränkungen und
- Exportgenehmigungen.

Für jedes Unternehmen werden die zulässigen Vertraulichkeitsstufen einzeln festgelegt.

Mit Hilfe der spezifischen Zugriffsrechte an einer PPR-Komponente legen Sie fest, welches Unternehmen der Eigentümer dieses Objektes ist und welcher Vertraulichkeitsstufe dieses Objekt zugeordnet ist.

Einen Zugriff auf diese PPR-Komponenten haben Anwender nur, wenn Sie eine entsprechende Vertraulichkeitsstufe besitzen und entweder Mitarbeiter des entsprechenden Unternehmens sind oder vertraglich dazu berechtigt sind, auf Objekte dieses Unternehmens zuzugreifen.

PPR-Komponenten, deren Informationen gesetzlichen Exportbestimmungen unterliegen, können als solche gekennzeichnet und mit Exportbeschränkungen versehen werden. Einen Zugriff auf solche mit Exportbeschränkungen versehenen Daten erhält ein Anwender, wenn sein Unternehmen über eine entsprechende Exportgenehmigung verfügt, die die festgelegten Exportbeschränkungen erfüllen.

Die Verknüpfungen zwischen Exportbeschränkungen, Exportgenehmigungen, Ländern und Unternehmen sowie zwischen Verträgen und Benutzern oder Gruppen von Benutzern werden in der Systembibliothek vom Administrator oder einem gleichberechtigten Mitarbeiter festgelegt.

Damit sich die definierten Sicherheitseinstellungen auf PPR-Komponenten auswirken, müssen Sie die Verknüpfungen zu Verträgen oder Exportbeschränkungen einzeln für jede PPR-Komponente erstellen.

Die Sicherheitseinstellungen können auf alle drei Planungssichten des PPR-Navigators angewandt werden:

- Produktsicht,
- Prozesssicht,
- Ressourcensicht.

## Funktionsweise von Gruppenfiltern

Der Zugriff auf PPR-Komponenten wird durch so genannte Gruppenfilter überprüft.

Bei den Gruppenfiltern sind drei Arten zu unterscheiden:

- Vertragsfilter (Predefined)
- Vertraulichkeitsstufenfilter (Securitylevel)
- Exportlizenzfiter (Exportlicence)

Jeder dieser Filter überprüft autonom, ob der Zugriff auf eine PPR-Komponente erlaubt ist. Nur wenn das Filterkriterium erfüllt ist, wird auch der Zugriff auf eine PPR-Komponente gewährleistet.

Da die Unternehmen den Zugriff auf PPR-Komponenten unterschiedlich regeln, erlaubt es die Konfiguration des Process Engineer jeden einzelnen Gruppenfilter unabhängig zu verwenden – beispielsweise, wenn Sie den Zugriff nur über Exportlizenzen regeln, können die anderen zwei Gruppenfilter in der Konfiguration deaktiviert werden.

Oder ein anderes Beispiel: Der Zugriff soll nur über Verträge und Vertraulichkeitsstufen geregelt werden, so reicht es aus, nur diese beiden Gruppenfilter zu aktivieren.

### Gruppenfilter - Vertragsfilter

Beim Vertragsfilter wird überprüft, ob für den Zugriff auf eine PPR-Komponente ein Vertrag erforderlich ist.

### Gruppenfilter - Vertraulichkeitsstufenfilter

Beim Vertraulichkeitsstufenfilter wird überprüft, ob die erforderliche Vertraulichkeitsstufe den Zugriff auf eine PPR-Komponente erlaubt.

### Gruppenfilter - Exportlizenzfiter

Beim Exportlizenzfiter wird überprüft, ob eine Exportlizenz für den Zugriff auf eine PPR-Komponente erforderlich ist. Exportlizenzen können für Staatsbürgerschaft und Aufenthaltsort in einem Land und für den Firmensitz in einem Land erforderlich sein.

## Datenobjekte für Sicherheitsrichtlinien einblenden

Unter Datenobjekte sind die Ordner zu verstehen, die in der Systembibliothek vorhanden sein müssen, um die Sicherheitsrichtlinien anzuwenden. Für die Arbeit mit den Sicherheitsrichtlinien müssen Sie nachfolgende Einstellungen vornehmen. Ohne diese Einstellungen können Sie die Sicherheitsrichtlinien nicht anwenden.

- Zum einen müssen Sie mit Hilfe des *Konfigurationswerkzeuges* die Datenobjekte für die Sicherheitsrichtlinien in der Systembibliothek einblenden.
- Und zum anderen müssen Sie im *Registrierungs-Editor* einen Wert einstellen, der es erlaubt die Sicherheitsrichtlinien anzuwenden.



### Hinweis

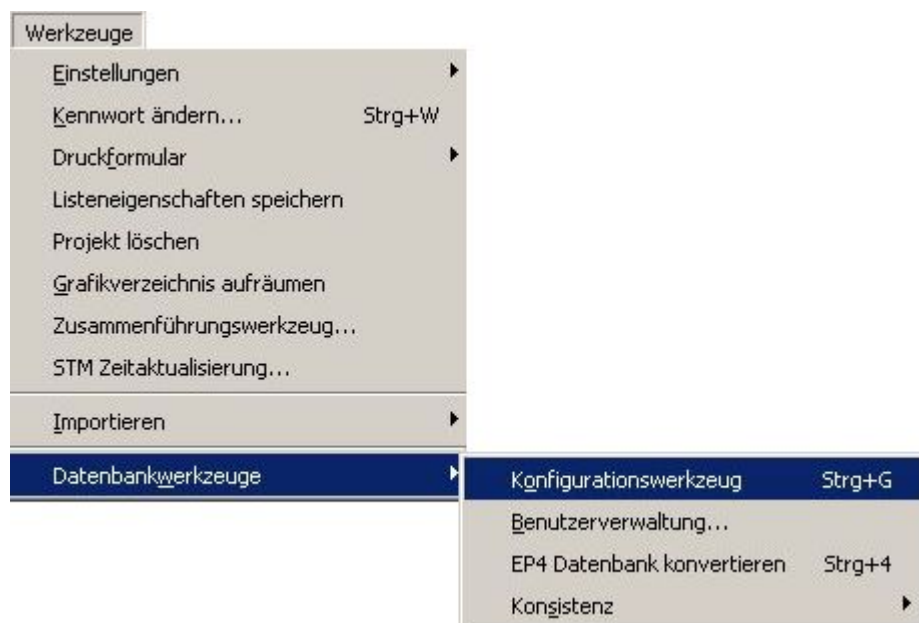
*Diese Einstellungen sollten grundsätzlich nur von einem Administrator oder einem gleichberechtigten Mitarbeiter ausgeführt werden.*

## Datenobjekte einblenden

Mit Hilfe der Datenobjekte, wie etwa Verträge, Lizenzen oder Länder, verwalten Sie die Sicherheitsrichtlinien und stellen die entsprechenden Beziehungen zwischen diesen Datenobjekten her.

Siehe auch: [Abbildung 3](#).

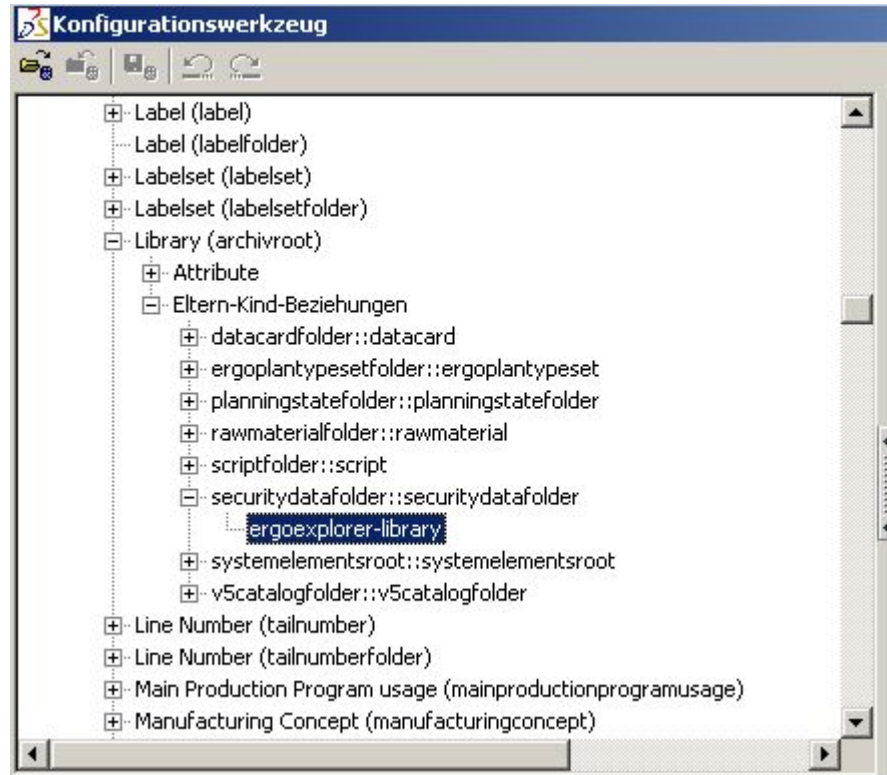
- Öffnen Sie das Konfigurationswerkzeug.
- Wählen Sie *Werkzeuge/Datenbankwerkzeuge/Konfigurationswerkzeug*.



**Abbildung 1:** Konfigurationswerkzeug öffnen



- Wählen Sie im Konfigurationswerkzeug *Library* aus. Bei einer anderen Sortierung als die im Bild gezeigte, müssten Sie *archivroot* wählen.
- Wählen Sie unter *securitydatafolder:.../ ergoexplorer-library* aus.



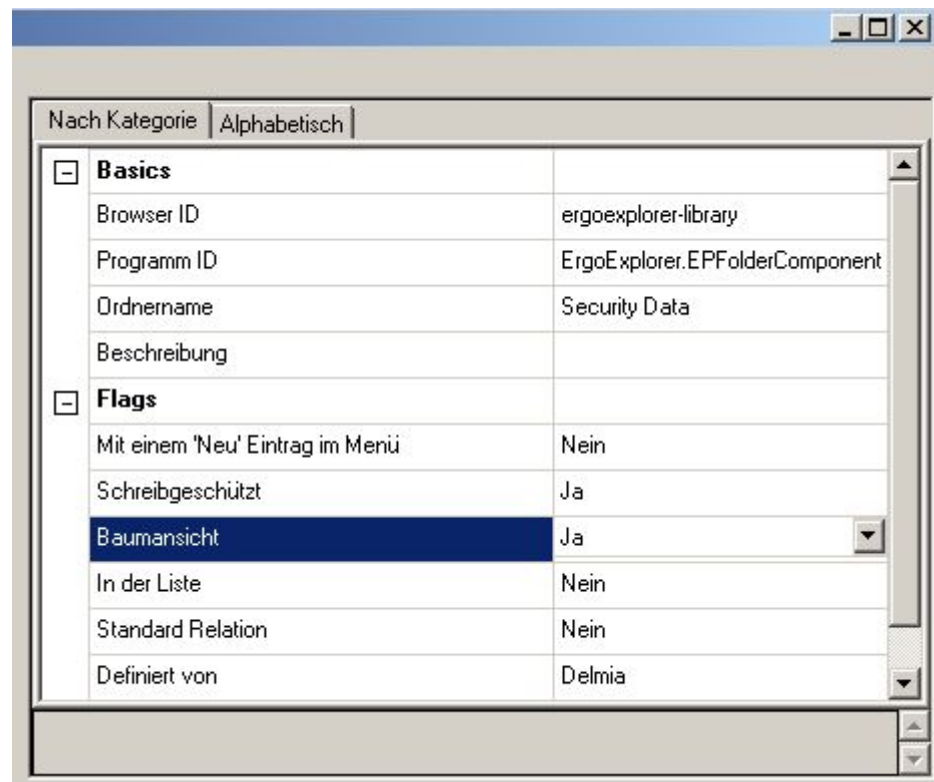
**Abbildung 2:** Library im Konfigurationswerkzeug öffnen

- Selektieren Sie *ergoexplorer-libray* und wechseln im Fenster zu den Eigenschaften.
- Um die Datenobjekte in der Systembibliothek einzublenden, stellen Sie bei Baumsicht *Ja* ein.

Siehe auch: [Abbildung 4](#).



**Abbildung 3:** Datenobjekte der Sicherheitsrichtlinien in der Systembibliothek eingebliendet

**Datenobjekt für Sicherheitsrichtlinien einblenden****Abbildung 4:** Datenobjekte einblenden

## Sicherheitsrichtlinien im Registrierungs-Editor aktivieren

Im Registrierungs-Editor müssen Sie den Wert bei *FilterEnabled* auf **eins** stellen, damit die Sicherheitsrichtlinien angewendet werden können. Standardmäßig ist der Wert auf **null** eingestellt.

- ➔ Wählen Sie im Registrierungs-Editor HKEY\_LOCAL\_MACHINE/SOFTWARE/DELMIA/IPDSERVER/SECURITY aus.
- ➔ Selektieren Sie nach dieser Auswahl *Filter*.
- ➔ Selektieren Sie in der Listview *FilterEnabled*.
- ➔ Um den Wert zu ändern. Öffnen Sie das Kontextmenü und wählen *Ändern*.



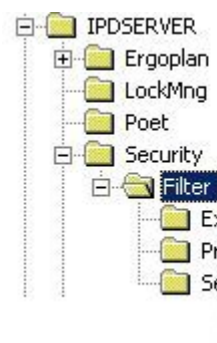
Abbildung 5: Kontextmenü auf *FilterEnabled* öffnen

- ➔ Tippen Sie im Dialog *Zeichenfolge bearbeiten* den Wert 1 ein. Bestätigen Sie die Eingabe mit *OK*.



Abbildung 6: Wert auf 1 stellen

Nachdem der Wert auf eins gesetzt wurde, wirken sich die Sicherheitsrichtlinien aus. Der neue Wert wird in der Listview bei *FilterEnabled* angezeigt.



Name	Typ	Wert
(Standard)	REG_SZ	(Wert nicht gesetzt)
FilterEnabled	REG_SZ	1
FilterFirst	REG_SZ	0

**Abbildung 7:** Wert *FilterEnabled* auf 1 gesetzt

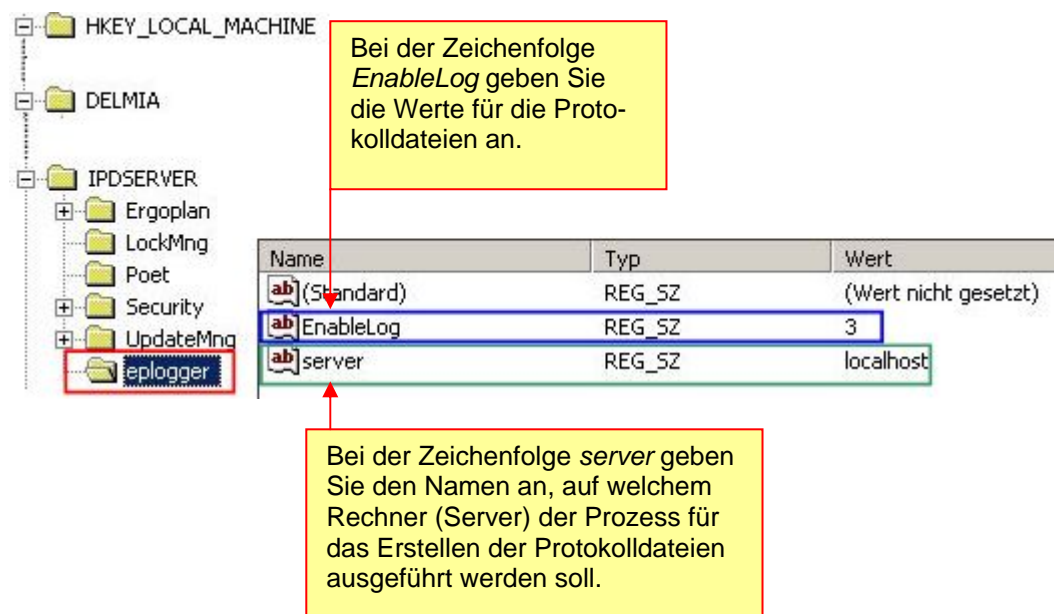
## Zugriffe und Änderung auf sicherheitsrelevante Daten protokollieren

Mit der Hilfe von Registrierungseinträgen können Sie Vorgänge protokollieren, die sicherheitsrelevanten Daten betreffen – wie etwa Anlegen neuer Anwender, Lizenzen, Verträge, Länder oder Export Control Classification zuweisen.

Die Registrierungseinträge nehmen Sie im Registrierungs-Editor im Verzeichnis **IPDServer\EPLLogger** vor:

- Wählen Sie im Registrierungs-Editor **HKEY\_LOCAL\_MACHINE\SOFTWARE\DELMIA\IPDServer\EPLLogger\EnableLog** bzw. **server**.

Standardmäßig sind Werte für diese beiden Schlüssel nicht aktiviert. Wie Sie die Registrierungseinträge anlegen und Werte angeben und ändern können, erfahren Sie im Kapitel [Schlüssel und Zeichenfolge für eplogger anlegen](#).



**Abbildung 8:** Registrierungseinträge für eplogger



### Hinweis

Wenn die Serverinstallation auf einem lokalen Rechner installiert ist, können Sie bei der **Zeichenfolge server** anstelle des Servernamens auch **localhost** angeben.

## Werte für Registrierungseinträge EnableLog und Server angeben

Mit Hilfe der Protokolldateien erhalten Sie einen Überblick, welche Anwender auf sicherheitsrelevante Daten zugegriffen haben.

Die Werte für die Registrierungseinträge des eploggers - *Enablelog* und *server*, müssen auf dem Rechner vorhanden sein, auf dem die Serverinstallation (PPRServer) installiert ist – diese Registrierungseinträge können auf Master- und Slaveserver angelegt werden.

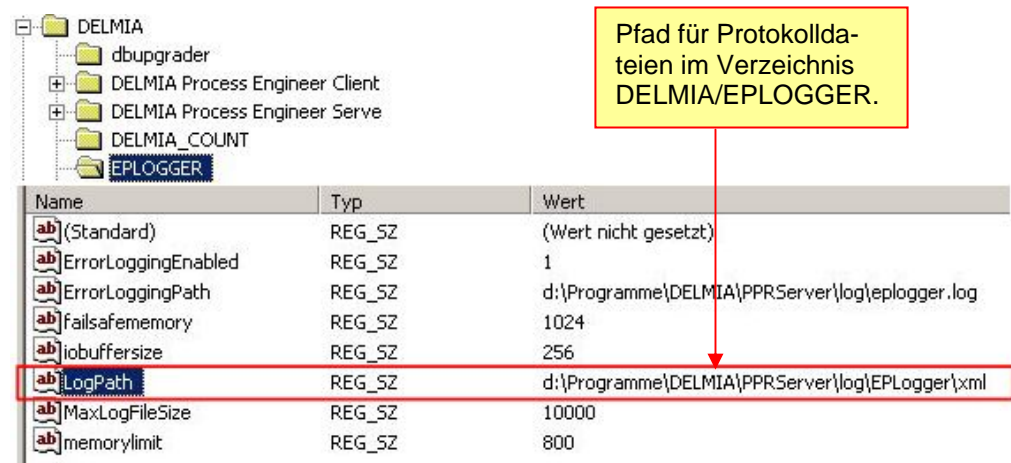
Für den Registrierungseintrag **EnableLog** können Sie vier Werte angeben:

- **Wert 0:** Der Wert null entspricht der Default-Einstellung. Bei diesem Wert werden keine Protokolldateien erstellt.
- **Wert 1:** Wenn Sie den Wert auf **1** setzen, werden Protokolldateien für Vorgänge erstellt wie Anlegen, Ändern, Verknüpfen oder Löschen von sicherheitsrelevanten Datenobjekten – wie beispielsweise das Anlegen eines neuen Anwenders oder das Verknüpfen von Verträgen mit einem Anwender oder Gruppen von Anwendern.
- **Wert 2:** Wenn Sie den Wert auf **2** setzen, werden Protokolldateien erstellt, für Vorgänge auf PPR-Komponenten, die Exportbeschränkungen (Ausfuhrkontrolle) unterliegen, wie etwa das Öffnen und Schließen einer PPR-Komponente für die die Exportbeschränkung gilt.
  - ⇒ Eine PPR-Komponente unterliegt bereits Exportbeschränkungen, wenn die PPR-Komponente mit einer *Export control classification* verknüpft ist oder das Feld Ausfuhrkontrolle selektiert ist.
- **Wert 3:** Wenn Sie den Wert auf **3** setzen, werden für alle sicherheitsrelevanten Vorgänge, wie sie bei den Werten eins und zwei beschrieben sind, Protokolldateien erstellt.

Beim **Registriereintrag server** tragen Sie den Namen des Servers ein, auf dem der Prozess für den *eplogger* ausgeführt werden soll – im Beispiel ist es der Server *localhost*. Sie können jeden Server für das Ausführen des Prozesses angeben, auf dem die Serverinstallation installiert ist.

Siehe auch: [Abbildung 8](#).

**Mit Hilfe der des eplogger-Prozess werden Protokolldateien erstellt:**



**Abbildung 9:** Pfad für Anlegen der Logdateien

- ⇒ Der Pfad für die Protokolldateien wird im Verzeichnis *DELMIA/EPLOGGER* angegeben. Der Pfad muss immer auf dem Server angegeben werden, auf dem der eplogger-Prozess ausgeführt werden soll, wie er beim Registriereintrag *server* angegeben wurde.
- ⇒ Die Protokolldateien werden im Verzeichnis > *DELMIA\PPRServer\log\EPLogger\XML* angelegt. Dieses Verzeichnis muss auf jeden Fall angelegt sein, damit Protokolldateien angelegt werden können.
- Protokolldateien werden nur erstellt, wenn Sie die Option *Beim Öffnen eines Dokuments immer aktiv* selektiert haben.
- Um die Option zu aktivieren, wählen Sie *Werkzeuge > Einstellungen > Sicherheitsdialog*.

☒ Beim Öffnen eines Dokumentes immer aktiv

**Abbildung 10:** Option im Sicherheitsdialog selektieren

## Schlüssel und Zeichenfolge für *eplogger* anlegen

- Den Schlüssel *eplogger* legen Sie über das Kontextmenü des Verzeichnis *IPDSERVER* an.



**Abbildung 11:** Schlüssel *eplogger* anlegen

- Wählen Sie *Neu > Schlüssel*, der neue Schlüssel wird im Verzeichnis *IPDSERVER* angezeigt. Geben Sie im Namensfeld *eplogger* an.
- Um die beiden Registrierungseinträge anzulegen, selektieren Sie den Schlüssel *eplogger* und öffnen Sie in der listview das Kontextmenü.
- Für jeden Eintrag müssen Sie eine Zeichenfolge erstellen. Wählen Sie *Neu > Zeichenfolge*, die neue Zeichenfolge wird in der listview angezeigt.
- Legen Sie nach dem Anlegen, die beiden Namen für die Zeichenfolgen fest: *EnableLog* und *server*. Siehe auch: [Abbildung 8](#).
- Über den Menüeintrag *Ändern* können Sie die Werte für die Zeichenfolge festlegen. Siehe auch: [Abbildung 6](#).



**Abbildung 12:** Registrierungseinträge für *eplogger* anlegen



## Anwender in der Benutzerverwaltung anlegen

Für Anwender die einen Zugriff auf Ihre Daten erhalten sollen, müssen zusätzliche Angaben zur Staatsbürgerschaft, Aufenthaltsort und Firmenzugehörigkeit gemacht werden, um die Sicherheitsrichtlinien **vollständig anwenden zu können**, die nachfolgend beschrieben werden.



In der Benutzerverwaltung werden Anwender und Gruppen von Anwender festgelegt. Das bestehende Rechtekonzept ist auch für diesen Fall erweitert worden. Weitere Informationen zur Benutzerverwaltung wie auch zu den Rechten erhalten Sie im Benutzerhandbuch [Administration](#) im Kapitel über die Benutzerverwaltung.

### Anwender anlegen

Im Beispiel hat der Anwender **Superuser Rechte**. Ein Administrator mit Superuser Rechten unterliegt keinen Beschränkungen. Für Anwender, was die Regel ist, die keine Superuser Rechte haben, müssen Sie die Rechte auf PPR-Komponenten wie bisher vergeben - wie etwa die Rechte Ändern, Lesen oder Schreiben von Daten.

Siehe auch: [Land anlegen und Firmen anlegen](#)

Für einen Anwender sind folgende zusätzliche Angaben erforderlich:

- Staatsbürgerschaft (Citizenship), Ort und Firma. Diese zusätzlichen Angaben müssen vollständig angegeben werden.
- Die Benutzerverwaltung öffnen Sie über *Werkzeuge/Datenbankwerkzeuge/Benutzerverwaltung*.

The screenshot shows a Windows-style dialog box titled 'Eigenschaften - Benutzer'. It has two tabs: 'Berechtigungseigenschaften' (selected) and 'Gruppenzugehörigkeit'. Under 'Berechtigungseigenschaften', there are several input fields: 'Anmeldename' with 'admin', 'Beschreibung' with 'Administrator', 'Externe ID' with 'admin', 'Kennwort' and 'Bestätigung' both masked with asterisks. Below these is a checked checkbox labeled 'Benutzer hat Superuser rechte'. At the bottom are three dropdown menus: 'Nationalität' (USA, US), 'Ort' (USA, US), and 'Unternehmen' (4711, Engine Co). At the very bottom are three buttons: 'OK', 'Rechte...', and 'Abbrechen'.

Abbildung 13: Anwender anlegen

**Staatsbürgerschaft (Nationalität)**

Hier geben Sie die Staatsangehörigkeit für den jeweiligen Anwender ein. Die Staatsbürgerschaft eines Anwenders spielt eine maßgebliche Rolle beim Zugriff auf Daten, die einer Exportbeschränkung unterliegen. Die Staatsbürgerschaft wirkt sich auf die Zuteilung von Exportlizenzen aus.

**Ort**

Hier geben Sie den Aufenthaltsort eines Anwenders ein. Der Aufenthaltsort und die Staatsbürgerschaft müssen nicht identisch sein. Der Aufenthaltsort eines Anwenders spielt ebenso eine maßgebliche Rolle beim Zugriff auf Daten, die einer Exportbeschränkung unterliegen. Der Aufenthaltsort wirkt sich auf die Zuteilung von Exportlizenzen aus.

**Firma (Unternehmen)**

Hier geben Sie die Firma an, für die der Anwender arbeitet. Wenn Sie bei einem Anwender zur Firma keine Angabe machen und dieser Anwender auch keiner Gruppe zugeordnet ist, welche eine Firmenzuordnung besitzt, so kann dieser Anwender auch nicht auf PPR-Komponenten zugreifen, zu denen er per Vertrag seiner Firma dazu das Recht hätte. Das gilt ebenso für Gruppen von Anwender einer Firma.

**Hinweis:** Fall „nicht Superuser“

*Um den Anwender mit Verträgen zu verknüpfen oder Security Levels für den Anwender festzulegen, muss zusätzlich das Funktionsrecht „useradm/edit user and groups“ gewährt sein.*

---

## Gruppen anlegen

Beim Anlegen einer Gruppe müssen zusätzlich Angaben zur Firma gemacht werden- im Beispiel wird eine Gruppe für die Firma **Engine** angezeigt. Eine Gruppe von Anwendern bilden Sie in der Regel, wenn Sie mehrere Anwender einer Firma zusammenfassen, die einen Zugriff auf Ihre Daten haben sollen.

Abbildung 14: Gruppen von Anwender



### Hinweis:

Um den Anwender mit Verträgen zu verknüpfen muss zusätzlich das Funktionsrecht „useradm/edit user and groups“ gewährt sein.

## Aufenthaltort bei der Anmeldung einblenden

Bei der Anmeldung des Process Engineer können Sie für Anwender den Dialog *Select User Location* einblenden. Im Dialog werden alle in der Systembibliothek angelegten Länder angezeigt. Beim Anlegen eines Anwenders wird der Aufenthaltort angegeben, dieser Aufenthaltort ist automatisch beim Öffnen des Dialogs selektiert.



Für Anwender mit Superuser Rechten steht dieser Dialog immer zur Verfügung, ein Wechsel des Aufenthaltorts wirkt sich für diese Anwender nicht auf die Exportbestimmungen aus.

Im Dialog können Sie dem Anwender einen anderen Aufenthaltort zuweisen, indem Sie ein anderes Land selektieren. Eine Änderung des Aufenthaltorts wird direkt im Eigenschaftsdialog des Anwenders in der Benutzerverwaltung nachvollzogen.

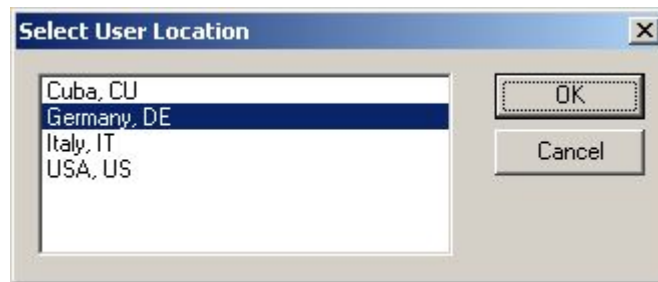
Ändern Sie den Aufenthaltort eines Anwenders bei der Anmeldung, hat das Auswirkungen auf die Exportbestimmungen und auf Exportlizenzen.

- ➔ Um den Dialog einzublenden, öffnen Sie die Benutzerverwaltung und aktivieren direkt beim Anwender das Funktionsrecht *Ort ändern*.



**Abbildung 15:** Ort ändern aktivieren

- Im Dialog werden alle angelegten Länder eingeblendet. Per Selektion eines Landes können Sie den Aufenthaltsort ändern.



**Abbildung 16:** Dialog Select User Location

## Sicherheitsrichtlinien festlegen

Mit Hilfe der Sicherheitsrichtlinien wird der Zugriff auf Ihre PPR-Komponenten in Projekten von Fremdfirmen geregelt. Die Entscheidung welche Sicherheitsrichtlinien für PPR-Komponenten gelten sollen, treffen Sie auf der Basis der nachfolgend beschriebenen allgemeingültigen Definitionen der Sicherheitsrichtlinien. Die Einstellungen der Sicherheitsrichtlinien nehmen Sie in der Systembibliothek vor.

- Wie Sie den Ordner *Security Data* einblenden erfahren Sie im Kapitel *Datenobjekte für Sicherheitsrichtlinien einblenden*.



### **Hinweis**

*Diese Einstellungen sollten grundsätzlich nur von einem Administrator oder einem gleichberechtigten Mitarbeiter ausgeführt werden. Für Mitarbeiter, die diese Rechte nicht haben, können Sie zusätzlich ein entsprechendes Recht im Verzeichnis *Global Regular Types* in der Systembibliothek vergeben.*

---

Nachfolgend wird bei jedem einzelnen Datenobjekt gezeigt, welches Recht Sie zusätzlich haben müssen, um eines der nachfolgenden beschriebenen Datenobjekte zu bearbeiten.

In diesem Kapitel lernen Sie die grundsätzliche Bearbeitung der Datenobjekte kennen:

- Länder: siehe [Länder verwenden](#).
- Firmen: siehe [Firmen verwenden](#).
- Verträge / Abkommen: siehe [Verträge – und Abkommen verwenden](#).
- Export control classification: siehe [Export control classification anlegen](#).
- Zugriffsrechte auf PPR-Komponenten: [Zugriffsrechte auf PPR-Komponenten anwenden](#).
- Siehe auch: [Fallbeispiele für Sicherheitsrichtlinien](#)

## Übersicht Exportlizenzen verwenden

Schema – der Staatsbürger eines Landes könnte eine Exportlizenz benötigen.

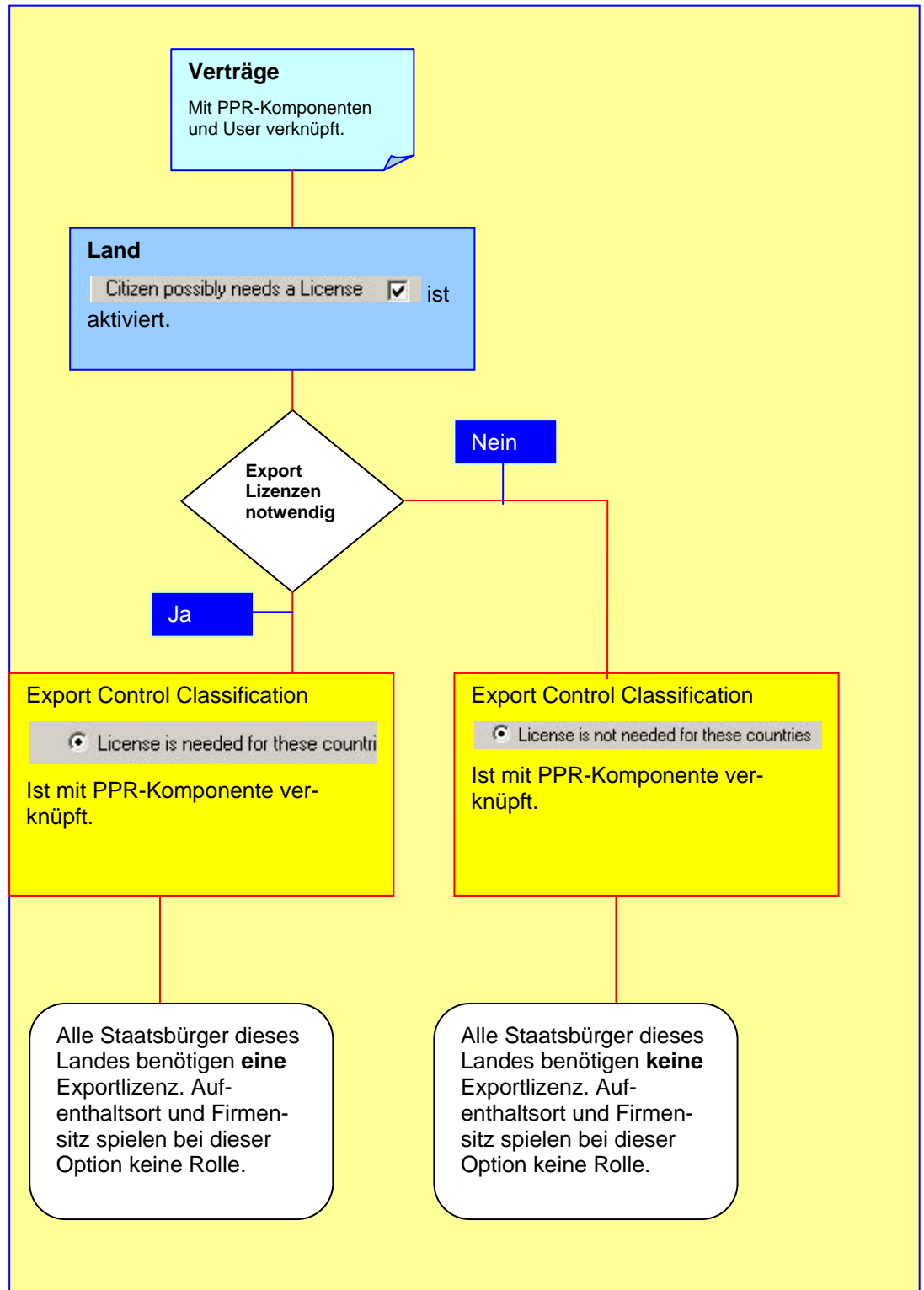


Abbildung 17: Schema – Staatsbürger können Lizenzen benötigen

Schema – für den Aufenthaltsort in einem Land könnte eine Exportlizenz benötigt werden.

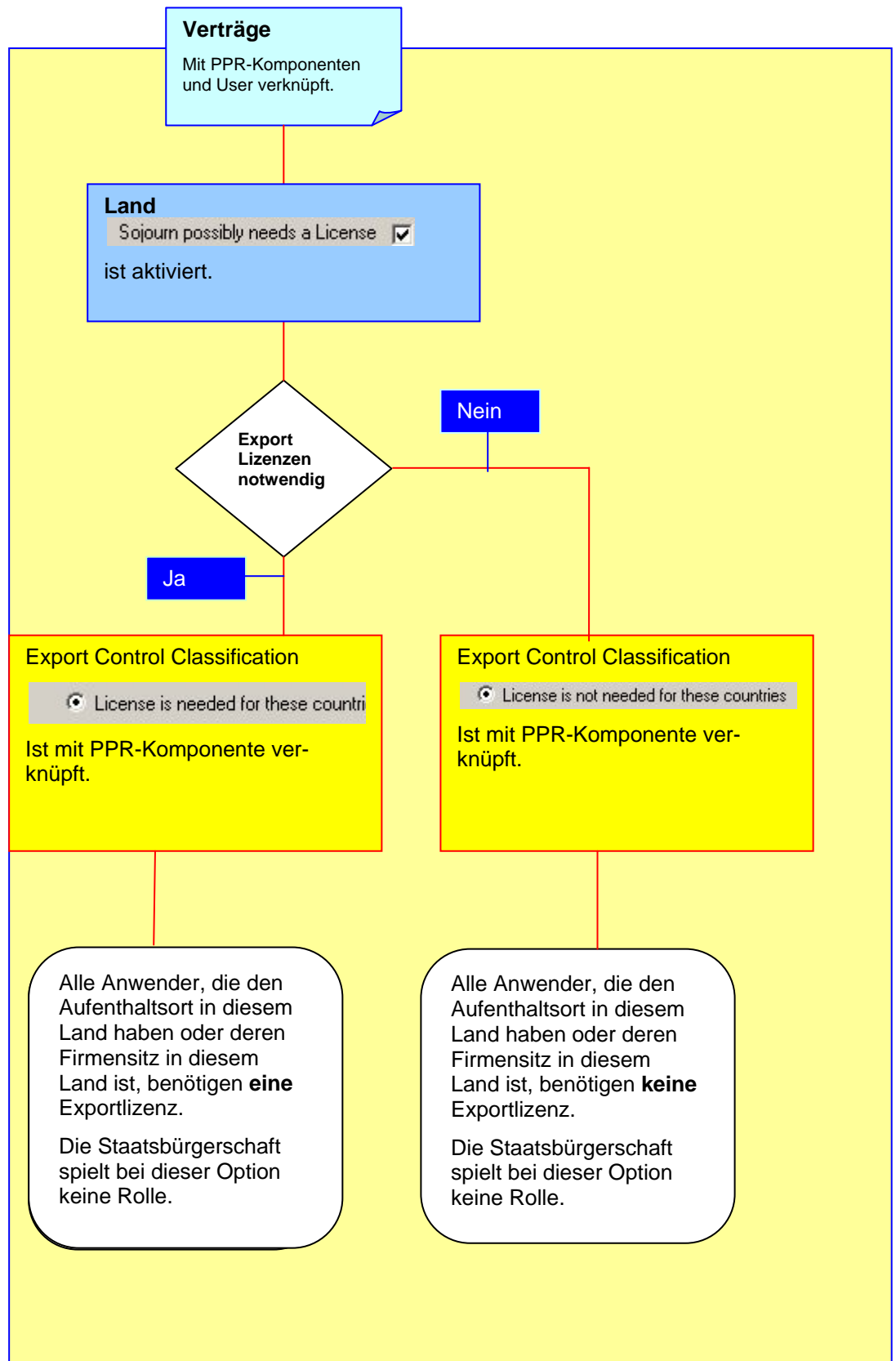
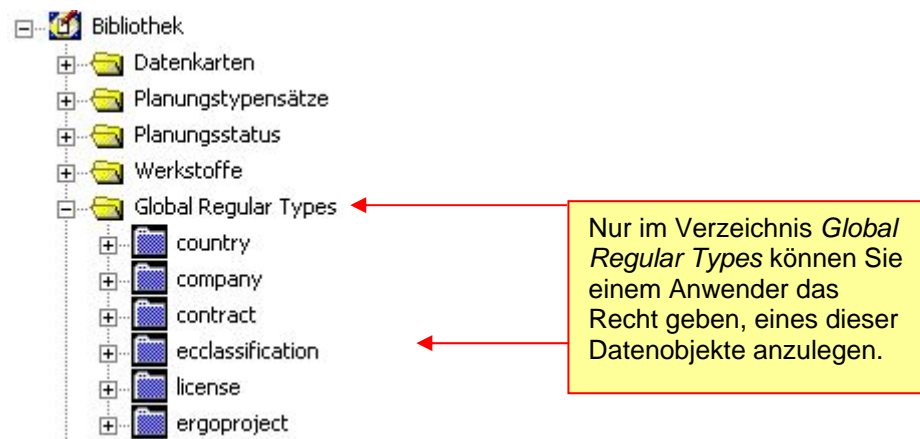


Abbildung 18: Schema – für Aufenthaltsort könnten Lizenzen benötigt werden



## Rechte für Anwender auf sicherheitsrelevante Datenobjekte vergeben

Im Verzeichnis *Global Regular Types* in der Systembibliothek können Sie für Anwender, die keine Superuser Rechte besitzen, das Recht vergeben sicherheitsrelevante Datenobjekte anzulegen wie etwa Firmen, Länder oder Verträge.



**Abbildung 19:** Global Regular Types

Diese Rechte können Sie für Anwender und Gruppen von Anwendern vergeben.



### Hinweis

Achten Sie darauf, dass das reine Recht ein Datenobjekt anzulegen noch nicht dazu berechtigt diese Datenobjekte sinnvoll einzusetzen. Um diese Datenobjekte sinnvoll einzusetzen, sollten Sie diesem Anwender noch zusätzliche Rechte zugestehen, wie etwa die im Dialog Zugriffsrechte aufgeführten Grundrechte für das Recht Schreiben.

Siehe auch: [Rechte für Anwender festlegen](#).

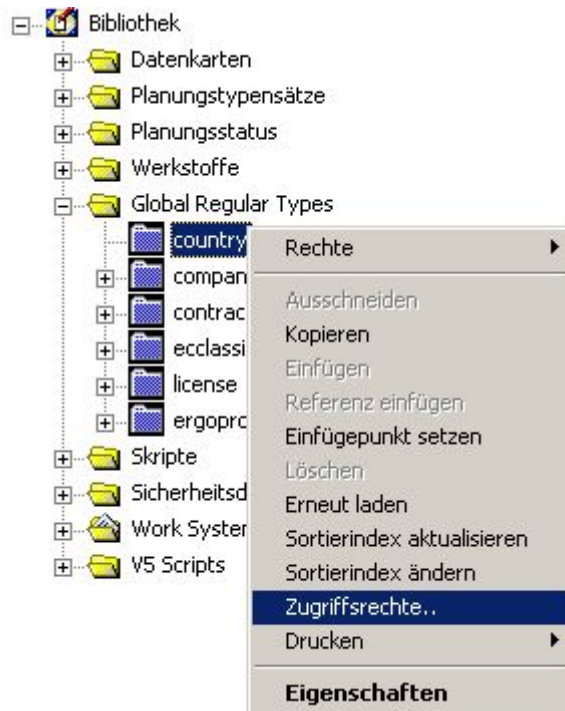
Tabelle Global Regular Types	
Regular Type – country	Recht, das Datenobjekt <b>Land</b> im Verzeichnis Sicherheitsdaten anzulegen.
Regular Type – company	Recht, das Datenobjekt <b>Firma</b> im Verzeichnis Sicherheitsdaten anzulegen.
Regular Type – contract	Recht, das Datenobjekt <b>Vertrag</b> im Verzeichnis Sicherheitsdaten anzulegen.
Regular Type – ecclassification	Recht, das Datenobjekt <b>ecclassification</b> im Verzeichnis Sicherheitsdaten anzulegen.
Regular Type – licence	Recht, das Datenobjekt <b>licence</b> im Verzeichnis Sicherheitsdaten anzulegen.
Regular Type ergoproject	Mit Hilfe des Regular Types <b>ergoproject</b> legen Sie den Zugriff für einen Anwender auf ein Projekt fest.

**Tabelle 1:** Global Regular Types

## Rechte für Anwender festlegen

Die Vorgehensweise ist für alle Datenobjekte gleich, um Rechte für Anwender oder Gruppen von Anwendern zu vergeben.

- Selektieren Sie in der Systembibliothek im Verzeichnis *Global Regular Types* ein Datenobjekt.
- Öffnen Sie auf diesem Datenobjekt das Kontextmenü und wählen Sie den Menüeintrag *Zugriffsrechte*.



**Abbildung 20:** Kontextmenü für Zugriffsrecht öffnen

Hinzufügen

Rechte ändern

- Fügen Sie im Dialog *Rechte – Datenobjekt* die Anwender bzw. Gruppen von Anwender hinzu, die das Recht haben sollen ein Datenobjekt anzulegen. Gruppen und Anwender müssen naturgemäß zuvor angelegt sein.
- Selektieren Sie einen Anwender und klicken auf den Button *Rechte ändern*.

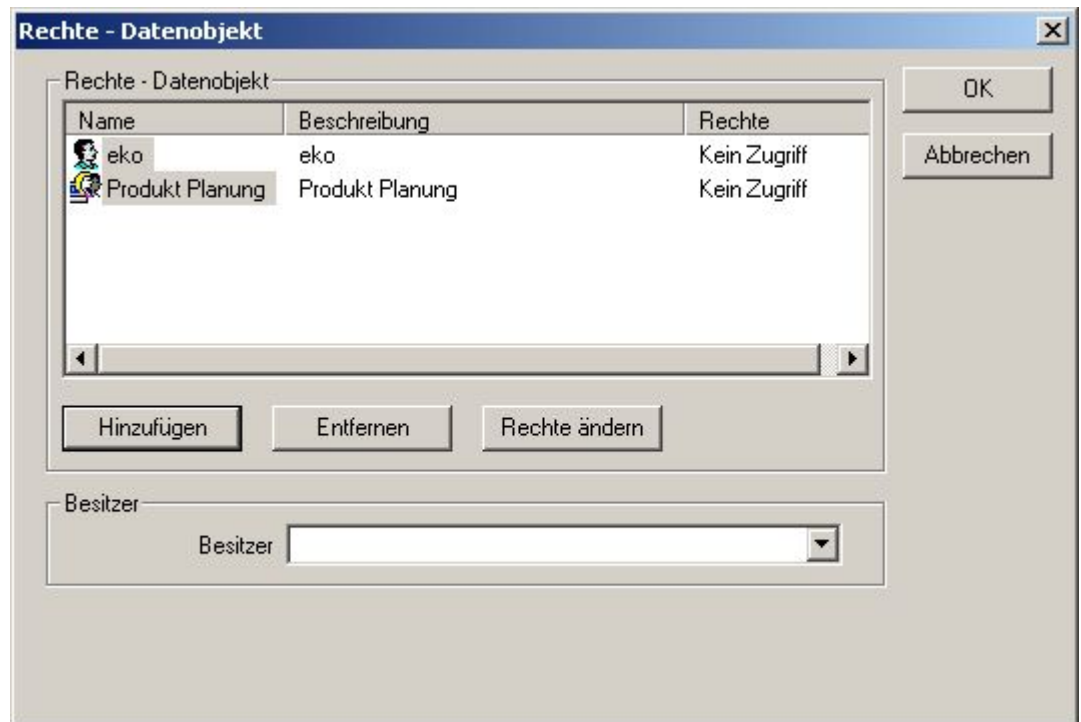


Abbildung 21: Anwender hinzufügen

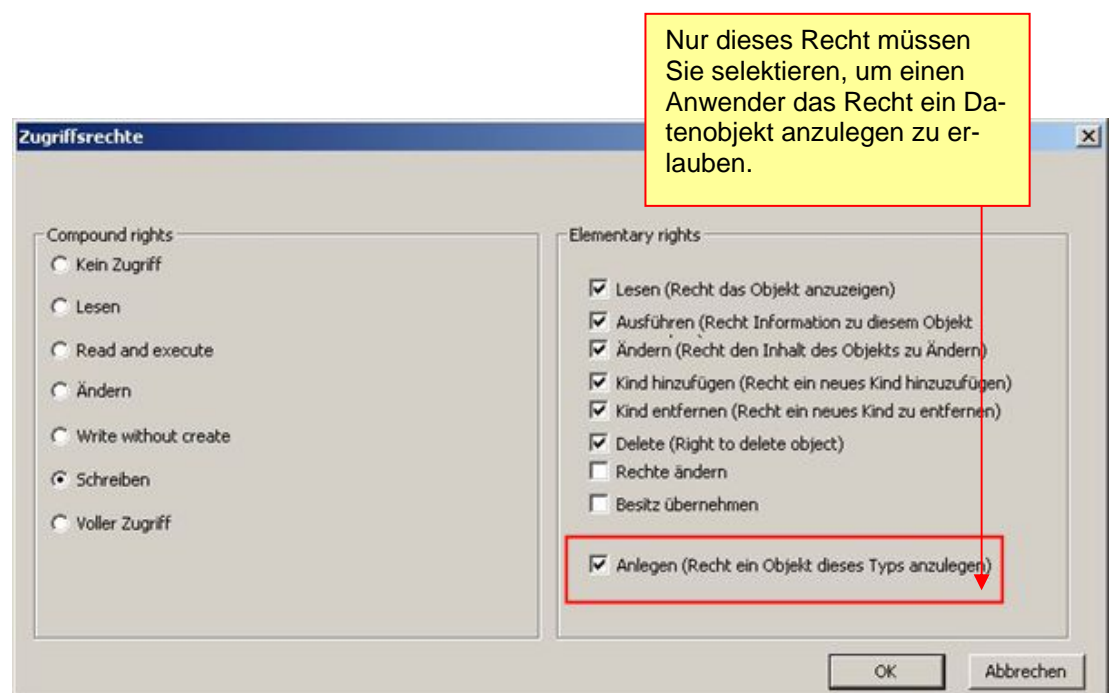


In der Benutzerverwaltung werden Anwender und Gruppen von Anwender festgelegt. Das bestehende Rechtekonzept ist auch für diesen Fall erweitert worden. Weitere Informationen zur Benutzerverwaltung wie auch zu den Rechten erhalten Sie im Benutzerhandbuch [Administration](#) im Kapitel über die Benutzerverwaltung.

Für das Anlegen eines Datenobjekts reicht es vollkommen aus, wenn Sie dem Anwender nur das Recht *Anlegen* (*Recht ein Objekt dieses Typs anzulegen*) geben.

Um im Verzeichnis Sicherheitsdaten angelegte Datenobjekte weiterzubearbeiten, können Sie neben dem Recht, ein sicherheitsrelevantes Datenobjekt anzulegen, hinzugefügten Anwendern noch zusätzlich weitere Rechte geben. Für jeden hinzugefügten Anwender können diese zusätzlichen Rechte verschieden vergeben werden.

- ⇒ Es empfiehlt sich für Anwender beispielsweise noch die im Bild gezeigten Rechte für das *Schreiben* zu geben.
- ➔ Um das Anlegen eines Datenobjekts zu erlauben, selektieren Sie in der rechten Seite des Dialogs das Recht *Anlegen* (*Recht ein Objekt dieses Typs anzulegen*).



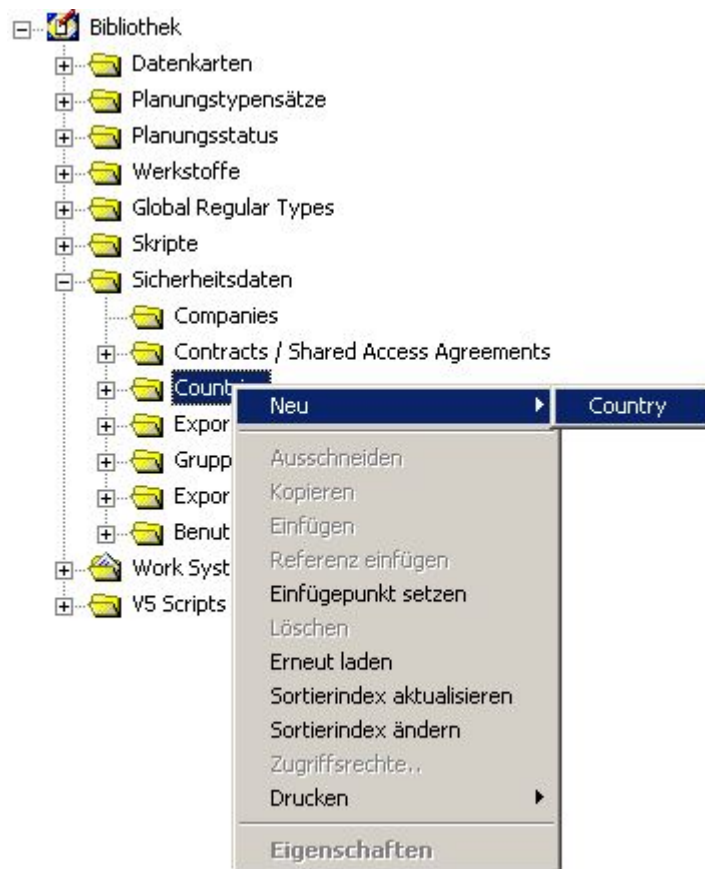
**Abbildung 22:** Recht für Anlegen eines Datenobjekts vergeben

Wenn Sie einem Anwender das Recht gegeben haben, ein bestimmtes Datenobjekt anzulegen, kann er dieses Datenobjekt im Verzeichnis *Sicherheitsdaten* der Systembibliothek anlegen – im Beispiel hat der Anwender das Recht Länder (Country) anzulegen.



### Hinweis

Mit Hilfe des Menüeintrags *Zugriffsrechte*, können Sie bei einem angelegten Datenobjekt Rechte für Anwender vergeben – entweder bestehende Rechte erweitern oder einschränken. Diese Rechte beziehen sich dann ausschließlich auf dieses angelegte Datenobjekt.



**Abbildung 23:** Anwender hat das Recht Datenobjekt anzulegen – Beispiel Land

## Länder verwenden

Länder, die Exportbeschränkungen unterliegen und deshalb gültige Exportlizenzen benötigen, legen Sie hier als Datenobjekt an. Die Zulassung für ein Land wird zum einen über gültige Exportlizenzen geregelt. Und zum anderen durch Exportbeschränkungen, die Sie für jedes Land in der Export Control Classification (ECC) festlegen.

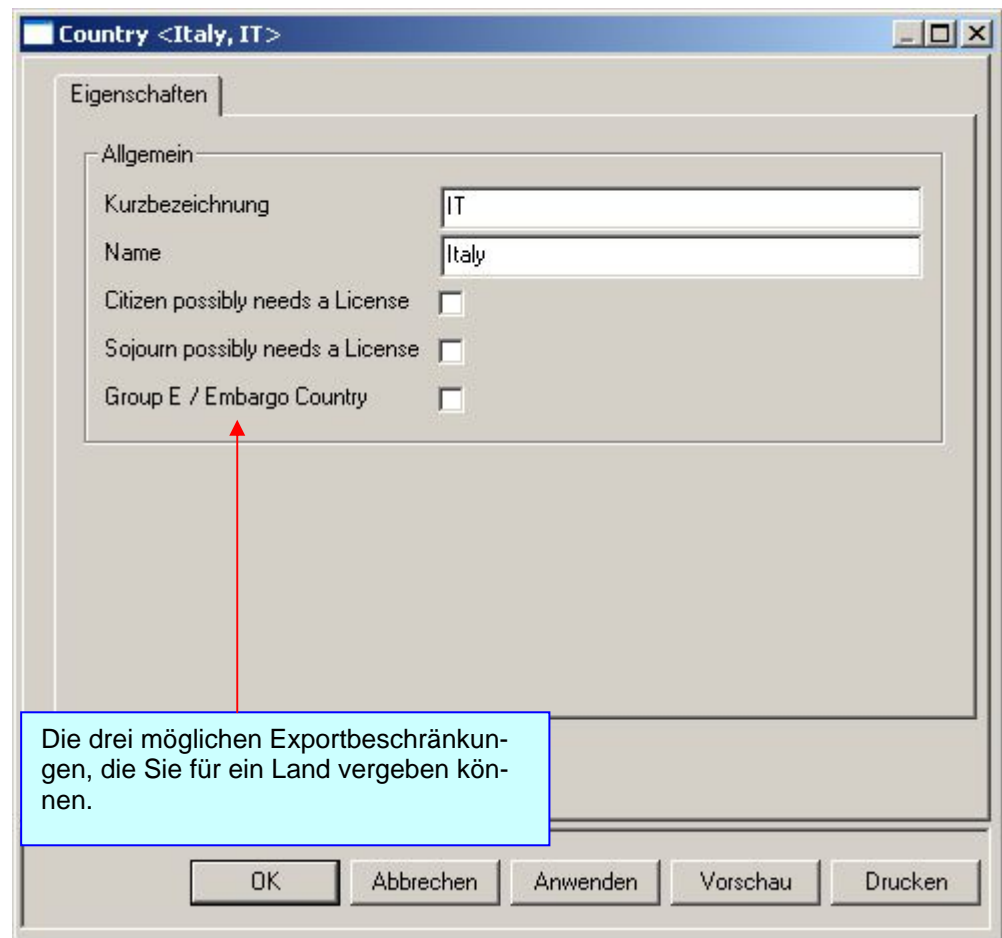
### Land anlegen

- Öffnen Sie in der Systembibliothek *Security Data*.
- Öffnen Sie das Kontextmenü bei *Countries*.
- Wählen Sie *Neu / Country*.



**Abbildung 24:** Kontextmenü auf Land öffnen

Für jedes Land das Sie anlegen, können Sie Exportbeschränkungen festlegen:



**Abbildung 25:** Eigenschaftsdialog für ein Land

## Exportbeschränkungen für ein Land festlegen

Exportbeschränkungen können Sie für jedes Land anders definieren.

Grundsätzlich wird der Zugriff auf Daten, welche Exportbeschränkungen unterliegen, nur dann mittels der ECC geregelt, wenn beim zugehörigen Land die entsprechende Option aktiviert ist.

Wenn die entsprechende Option bei diesem Land **nicht** aktiviert ist, haben Anwender von Fremdfirmen bereits einen Zugriff auf Ihre PPR-Komponenten, wenn sowohl der Anwender als auch die PPR – Komponenten mit einem Vertrag verknüpft werden, unabhängig davon ob die PPR – Komponenten Exportbeschränkungen unterliegen oder nicht.

Nur wenn Sie diese Optionen verwenden, benötigen Sie für Ihre Daten Export Control Classifications (ECC) und eine Exportlizenzen.

Die Entscheidung darüber, ob für die einzelnen Länder Exportlizenzen notwendig werden, treffen Sie also beim Land. Für welche Länder im Einzelfall wirklich Exportlizenzen benötigt werden, ist in der ECC festgelegt. Diese Optionen sind notwendig, um den Zugriff auf Ihre Daten einzugrenzen.


- Länder die als Embargo Land gekennzeichnet sind, haben grundsätzlich keinen Zugriff auf Ihre Daten, benötigen also auch keine Exportlizenz.

Die Exportbeschränkungen können Sie auch kombinieren. Wenn Sie beide Exportbeschränkungen aktivieren - *Citizen possibly needs a License* und *Sojourn possibly needs a License* – gelten auch beide Bedingungen für mögliche Exportlizenzen.

Wenn Sie diese beiden Optionen verwenden, wird technisch gesehen, die mit der PPR-Komponente verknüpfte ECC überprüft, und entsprechend der Festlegung in der ECC, kann dann eine Exportlizenz benötigt werden oder auch nicht.

## Staatsbürgerschaft für ein Land

Wenn Sie *Citizen possibly needs a License* aktivieren, könnten alle Anwender die Staatsbürger dieses Landes sind, eine Exportlizenz benötigen. Ob eine Exportlizenz benötigt wird, wird in der ECC festgelegt, die mit einer PPR-Komponente verknüpft sein muss.



Citizen possibly needs a License ☒

**Abbildung 26:** Lizenz für Staatsbürgerschaft

### Beispiel

Wenn in der ECC beispielsweise festgelegt wurde, dass für dieses Land keine Exportlizenz benötigt wird und *Citizen possibly needs a License* aktiviert ist, benötigen Anwender die **Staatsbürger** dieses Landes sind, trotzdem **keine** Exportlizenz.

- ⇒ **Grenzfall:** Wenn der Aufenthaltsort der Firma oder der Aufenthaltsort des Anwenders in einem anderen Land ist, und für dieses Land *Sojourn possibly needs a License* aktiviert ist, benötigt der Anwender dann auch für dieses Land, in welchem er sich aufhält und seine Firma ihren Sitz hat, eine Exportlizenz.



**Im Umkehrschluss bedeutet dies:**

Wenn in der ECC beispielsweise festgelegt wurde, dass für dieses Land eine Exportlizenz benötigt wird und *Citizen possibly needs a License* aktiviert ist, benötigen Anwender die **Staatsbürger** dieses Landes sind, auch **eine** Exportlizenz.

⇒ **Grenzfall:** Wenn der Aufenthaltsort der Firma oder der Aufenthaltsort des Anwenders in einem anderen Land ist, und für dieses Land *Sojourn possibly needs a License* aktiviert ist, benötigt der Anwender dann auch für dieses Land eine Exportlizenz.

**Aufenthaltsort für ein Land**

Wenn Sie *Sojourn possibly needs a License* aktivieren, könnten alle Anwender deren Aufenthaltsort dieses Land ist, eine Exportlizenz benötigen. Ob eine Exportlizenz benötigt wird, wird in der ECC festgelegt, die mit einer PPR-Komponente verknüpft sein muss.

Sojourn possibly needs a License ☒

**Abbildung 27:** Lizenz für Aufenthaltsort

**Beispiel**

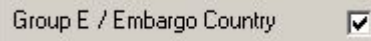
Wenn in der ECC beispielsweise festgelegt wurde, dass für dieses Land keine Exportlizenz benötigt wird und *Sojourn possibly needs a License* aktiviert ist, benötigen Anwender deren **Aufenthaltsort oder deren Firmensitz** dieses Land ist, trotzdem **keine** Exportlizenz, weil eben in ECC festgelegt wurde, dass für diesen Fall keine Exportlizenz notwendig ist.

**Im Umkehrschluss bedeutet dies:**

Wenn in der ECC beispielsweise festgelegt wurde, dass für dieses Land eine Exportlizenz benötigt wird und *Sojourn possibly needs a License* aktiviert ist, benötigen Anwender deren **Aufenthaltsort oder der Firmensitz** dieses Land ist, auch **eine** Exportlizenz.

**Ausschluss für ein Land**

Wenn Sie *Group E / Embargo Country* aktivieren, haben alle Anwender die Staatsbürger dieses Landes sind, oder deren Aufenthaltsort in diesem Land ist oder deren Firmensitz in diesem Land liegt, keinen Zugriff auf Ihre vertraulichen Daten – also für die PPR-Komponenten die bereits einer Exportbeschränkung unterliegen. Dieser Ausschluss kann durch keine Exportlizenz aufgehoben werden.



**Abbildung 28:** Embargo Land

**Beispiel**

Wenn Sie diese Option bei einem Land aktivieren, müssen Sie die beiden anderen Exportbeschränkungen nicht aktivieren.

Der Entscheidung welches Land als Embargo Land gekennzeichnet wird, dafür könnten beispielsweise politische Entscheidungen zu Grunde gelegt werden. Aus dem Blickpunkt der USA gesehen, wären das heute etwa die Länder Irak, Cuba oder Nordkorea.

## Verknüpfungen zu anderen Datenobjekte

Ein Land können Sie mit beliebig vielen Exportlizenzen und Export Control Classifications verknüpfen.

Die möglichen Verknüpfungen zu anderen Datenobjekten der Systembibliothek werden in der Listview angezeigt:

Alle Benutzer, die die Staatsbürgerschaft dieses Landes haben.

Alle Exportlizenzen, die mit diesem Land verknüpft sind.

Name	Beschreibung	Geändert
Maier	Maier	11.07.2005 13:34:06
Tonio	Tonio	19.07.2005 12:39:07
Land	Mal	13.07.2005 16:13:48
Franz	Behr	14.07.2005 08:06:37

Alle Export Control Classifications, die mit dem Land verknüpft sind.

**Abbildung 29:** Anzeige von Verknüpfungen in der Listview - Länder

## Firmen verwenden

Für die Fremdfirmen mit denen Sie Verträge abgeschlossen haben und die Exportlizenzen erhalten sollen, legen Sie hier als Datenobjekt an.

Für jede einzelne Firma (Fremdfirma und Ihre eigene Firma) können Sie Vertraulichkeitsstufen festlegen. Für Fremdfirmen benötigen Sie Vertraulichkeitsstufen nur, wenn diese neuen PPR-Komponenten in Ihren Projekten besitzen und anlegen können. Die neuen PPR-Komponenten sind Eigentum der Firma, der der Anwender, der die neue PPR – Komponente erzeugt hat, zugeordnet ist. Zusätzlich können entsprechende Vertraulichkeitsstufen gelten.

Um einen Zugriff der Anwender und Gruppen von Anwender der Fremdfirmen auf Ihre Daten zu erlauben, werden diese mit Ihrer Firma verknüpft – das bedeutet, dass Sie in der Systembibliothek ein Datenobjekt Ihrer Firma anlegen müssen.

Nach dem Verknüpfen der Fremdfirma mit Ihrer Firma – technisch gesehen verknüpfen Sie die Anwender der Fremdfirma mit Ihrer Firma – übertragen Sie auf diese Anwender, die Vertraulichkeitsstufe (Sicherheitslevel), die einen Zugriff auf Ihre PPR-Komponenten erlaubt.

### Firmen anlegen

- Öffnen Sie in der Systembibliothek *Security Data*.
- Öffnen Sie das Kontextmenü bei *Companies*.
- Wählen Sie *Neu / Firma*.



Abbildung 30: Kontextmenü Firma

Stellvertretend für Ihre Firma, verwenden wir in allen nachfolgend beschriebenen Beispielen die Firma *Engine Co.*

Alle Felder sind frei beschreibbar. Wichtig ist, dass Sie der Firma das Land für den Unternehmenssitz zuweisen. Wenn kein Land für den Unternehmenssitz angegeben wird, wird der Zugriff auf Daten, die Exportbeschränkungen unterliegen, verweigert. Die Firma könnte ja den Sitz in einem Land haben, das als Embargo Land gekennzeichnet ist, für die ein Zugriff auf solche Daten generell verboten ist.

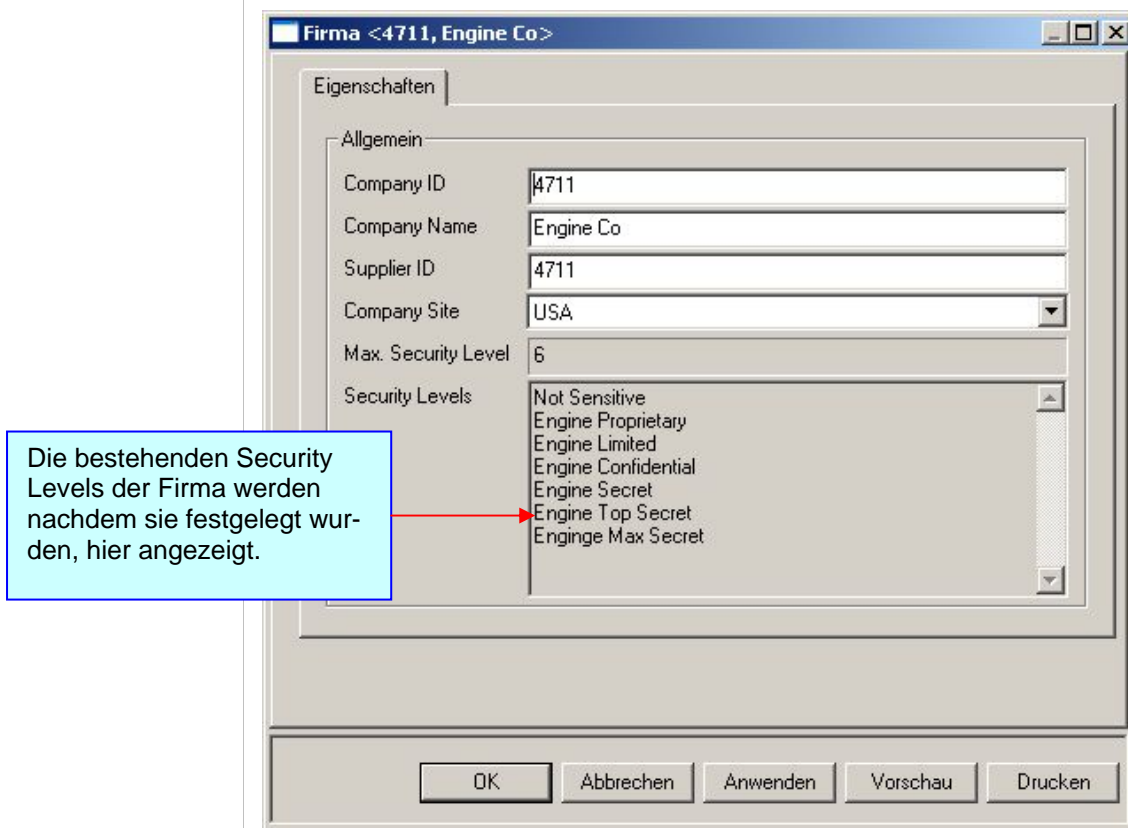


Abbildung 31: Eigenschaftsdialog Firma

## Vertraulichkeitsstufen für Firma festlegen

Maximal können Sie für eine Firma neun Vertraulichkeitsstufen (Security Levels) festlegen.

- ➔ Öffnen Sie in der Systembibliothek das Kontextmenü auf der Firma. Im Beispiel ist es Ihre stellvertretende Firma *Engine Co*.
- ⇒ Für die Festlegung eines Security Levels ist die Vorgehensweise, wie sie hier gezeigt wird, für alle Firmen gleich. Da der Zugriff auf Daten über Ihren definierten Security Level erfolgt, wird die Vorgehensweise an Hand der Firma Engine Co erklärt.

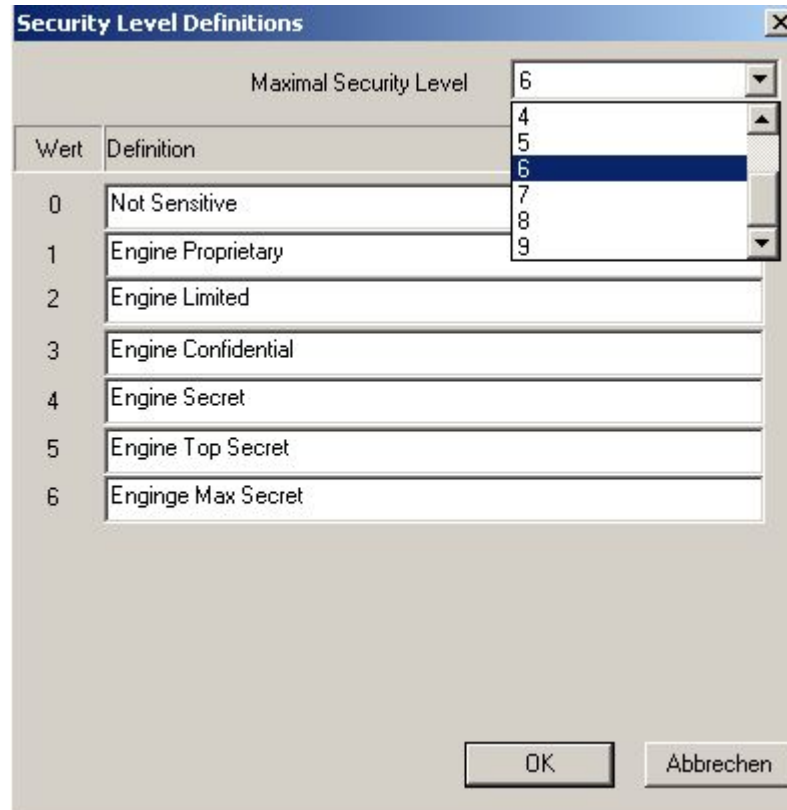


**Abbildung 32:** Kontextmenü auf Firma öffnen

- ➔ Legen Sie die Vertraulichkeitsstufen fest, maximal sind neun möglich. Im Feld Maximal Security Level stellen Sie den gültigen Wert ein – für die Firma Engine sollen maximal sechs Vertraulichkeitsstufen möglich sein.
- ⇒ Für Ihre PPR-Komponenten stehen diese definierten Vertraulichkeitsstufen zur Verfügung, die einzeln für jede PPR-Komponente zugewiesen werden können. Standardmäßig hat jede PPR-Komponente die Vertraulichkeitsstufe null.

- ⇒ Im Beispiel könnte jede PPR-Komponente den maximalen Wert sechs erhalten. Jede PPR-Komponente kann einen anderen Wert zugewiesen bekommen.

Siehe auch: [Verknüpfungen vornehmen – Beispiel 2.](#)



**Abbildung 33:** Vertraulichkeitsstufen festlegen



#### **Hinweis**

*Zur Auswahl stehen immer nur die Vertraulichkeitsstufen bis zum festgelegten maximalen Security Level zur Verfügung. Nur diese werden auch angezeigt.*

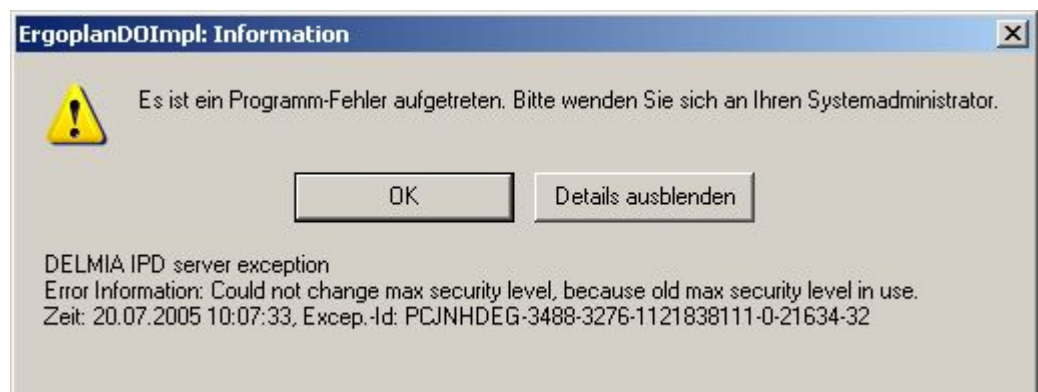
**Vertraulichkeitsstufen ändern**

Vertraulichkeitsstufen können geändert werden.

Achten Sie darauf, wenn Sie den maximalen Security Level herunterstufen, und bereits Security Levels für Ihre PPR-Komponenten zugewiesen worden sind, dass der neue maximale Security Level gleich oder höher liegt, als der einer PPR-Komponente zugewiesene.

- Falls höherwertige Security Levels an PPR-Komponenten vorhanden sind, müssen sie einzeln bei jeder PPR-Komponente geändert werden
- Das Gleiche gilt für Anwender die dieser Firma zugewiesen sind, und die einen höheren Security Level haben.

Mit dieser Meldung wird auf diesen Sachverhalt hingewiesen:



**Abbildung 34:** Meldung höherer Security Level vorhanden



## Vertraulichkeitsstufen für Anwender festlegen

Für jeden Anwender können Sie einen der von Ihnen zuvor festgelegten Vertraulichkeitsstufen übertragen. Zur Auswahl stehen alle definierten Vertraulichkeitsstufen. Bis zur zugewiesenen Vertraulichkeitsstufe sollte ein Zugriff erlaubt sein. Sollte ein Anwender auf bestimmte PPR-Komponenten nicht zugreifen können, so können Sie die Vertraulichkeitsstufe für den Anwender auf diesen Wert begrenzen.

- Anwender verknüpfen Sie per Drag & Drop mit Ihrer Firma.



### Hinweis:

*Zusätzlich benötigen Sie noch das Funktionsrecht „useradm/edit user and groups“.*

- ⇒ Alle verknüpften Anwender werden in der Listview der selektierten Firma unter dem Reiter Security Levels angezeigt. Standardmäßig ist vor dem Zuweisen der Security Level für den Anwender auf null gesetzt - das bedeutet, dass der Anwender keinen Zugriff auf sicherheitsrelevante Daten erhält.

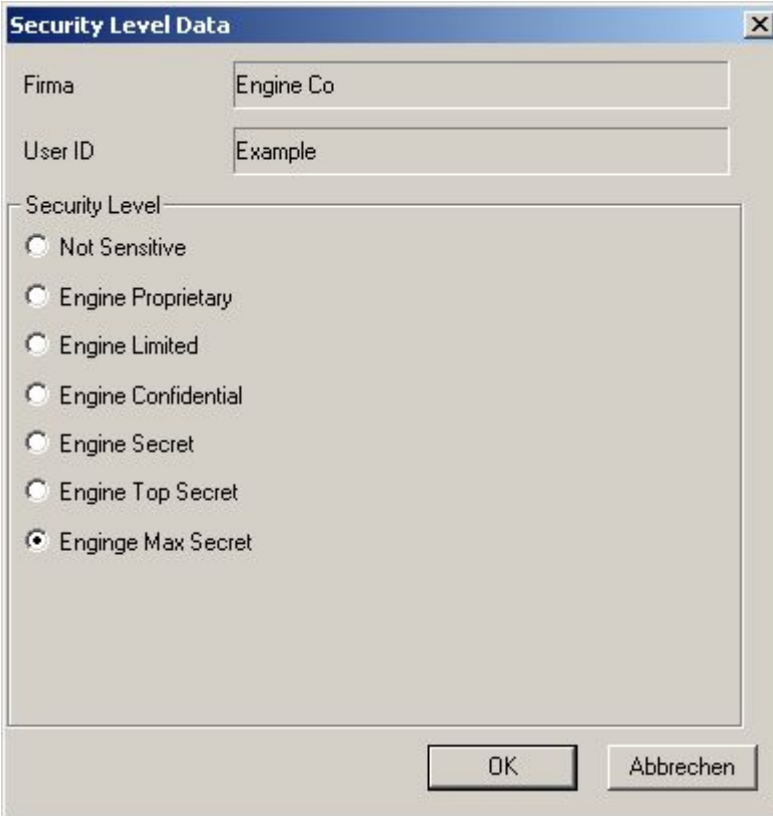
- Selektieren Sie den Anwender öffnen das Kontextmenü.



**Abbildung 35:** Kontextmenü Vertraulichkeitsstufe bearbeiten

- Legen Sie hier den Security Level für den Anwender fest. Zur Auswahl stehen alle Security Levels, die zuvor für die Firma definiert wurden – also um im Beispiel zu bleiben, die Security Levels Ihrer Firma Engine Co.

- ⇒ Sollten Anwender Ihrer eigenen Firma, die keine Superuser Rechte haben, einen Zugriff auf Daten Ihrer Firma erhalten, definieren Sie hier ebenso den Security Level für diese Anwender. Diese Anwender müssen ebenso mit Ihrer Firma verknüpft werden wie ein Anwender einer Fremdfirma.



The screenshot shows a Windows-style dialog box titled "Security Level Data". It features two text input fields at the top: "Firma" containing "Engine Co" and "User ID" containing "Example". Below these is a section titled "Security Level" which contains a list of seven radio button options: "Not Sensitive", "Engine Proprietary", "Engine Limited", "Engine Confidential", "Engine Secret", "Engine Top Secret", and "Engine Max Secret". The "Engine Max Secret" option is selected. At the bottom right of the dialog are two buttons: "OK" and "Abbrechen".

**Abbildung 36:** Security Level für Anwender festlegen

## Verknüpfungen zu anderen Datenobjekte

Eine Firma können Sie mit beliebig vielen Anwendern und Exportlizenzen verknüpfen.

Name der Firma für die der Security Level des Anwenders gilt

Name der Anwender.

Wert des zugewiesenen Security Levels

Company Name	User ID	Wert	Security Level Definition
Engine Co	Gans	6	Enginge Max Secret
Engine Co	Example	6	Enginge Max Secret
Engine Co	Tonio	5	Engine Top Secret
Engine Co	Peter	6	Enginge Max Secret
Engine Co	Castro	6	Enginge Max Secret

Abbildung 37: Listview mit verknüpften Anwendern

## Verträge – und Abkommen verwenden

Ein Vertrag wird zwischen Ihnen und Fremdfirmen abgeschlossen, um den Zugriff auf Ihre Daten zu regeln.

Mit einem Vertrag wird die Basis gelegt auf dem alle weiteren Schritte erfolgen. Ohne einen bestehenden Vertrag hat eine Fremdfirma keinen Zugriff auf Ihre Daten.

In den Verträgen wird festgehalten welche Firmen überhaupt Rechte erhalten sollen, auf vertrauliche Daten Ihres Unternehmens zugreifen zu können.

### Wirksamkeit von Verträgen

- Ein Vertrag wird nur wirksam, wenn Sie den Vertrag den Anwendern der Firmen zuweisen, für die ein Vertrag abgeschlossen wurde. Technisch gesehen bedeutet das nichts anderes, als dass Sie Verträge entsprechend in der Systembibliothek mit Anwendern oder Gruppen von Anwendern einer Firma verknüpfen.
- Weiterhin wirkt sich ein Vertrag auf Ihre vertrauliche Daten erst aus, wenn Sie den Vertrag mit PPR-Komponenten im Projekt, beim Objekt und seinen Kindern, verknüpfen.
- Ein Vertrag muss einzelnen mit jeder PPR-Komponente verknüpft werden, damit überhaupt eine grundsätzliche Erlaubnis vorhanden ist, um auf Ihre Daten zugreifen zu können.

### Verträge anlegen

- Öffnen Sie in der Systembibliothek *Security Data*.
- Öffnen Sie das Kontextmenü bei *Contracts / Shared Access Agreements*.
- Wählen Sie *Neu / Contract / Shared Access*.



Abbildung 38: Kontextmenü für Verträge

- Im Eigenschaftsdialog legen Sie den Vertragsgegenstand fest. Alle Felder des Eigenschaftsdialogs sind frei beschreibbar.

The screenshot shows a Windows-style dialog box titled "Contract / Shared Access <4711, Firma EXAMPLE>". It has a tab labeled "Eigenschaften". Inside, there is a section "Allgemein" with the following fields:

- Contract / Shared Access ID: 4711
- Name: Firma EXAMPLE
- Ownning Company: Engine Co (dropdown menu)
- Beschreibung: Hier können Sie Angaben zum Vertragsgegenstand machen, wie etwa Anwender der Firma EXAMPLE haben unter bestimmten Voraussetzungen einen Zugriff auf PPR-Komponenten der Firma Engine.
- Contract String Attribute 1, 2, 3: (empty text boxes)
- Contract Int Attribute 1, 2, 3: 0
- Contract Double Attribute 1, 2, 3: 0,00000000
- Contract Bool Attribute 1, 2, 3: ☒

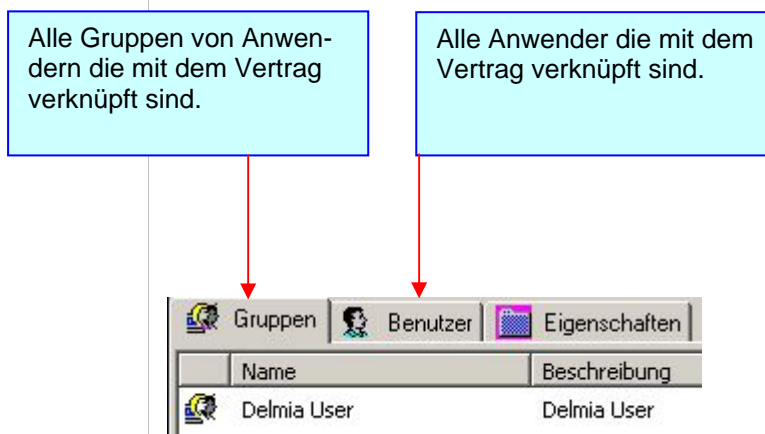
At the bottom, there are buttons: OK, Abbrechen, Anwenden, Vorschau, and Drucken.

**Abbildung 39:** Eigenschaftsdialog Vertrag

**Verknüpfungen zu anderen Datenobjekten**

- Einen Vertrag können Sie mit beliebig vielen Anwendern, Gruppen von Anwendern und PPR-Komponenten verknüpfen.
- Einen Vertrag verknüpfen Sie mit den Anwender oder Gruppen von Anwendern von Fremdfirmen, die einen Zugriff auf Ihre Daten erhalten sollen.
- Diese Anwender und Gruppen verknüpfen Sie mit Ihrer Firma, dadurch ist ein Vertrag technisch gesehen gültig.
- Nach der Verknüpfung des Anwenders mit Ihrer Firma kann die Vertraulichkeitsstufe auf diesen Anwender übertragen werden, die einen Zugriff auf Ihre Daten erlauben.

Die möglichen Verknüpfungen zu anderen Datenobjekten der Systembibliothek werden in der Listview angezeigt:



**Abbildung 40:** Anzeige in der Listview für verknüpfte Datenobjekte - Verträge

## Export control classification (ECC) verwenden

Mit Hilfe der Export control classification (ECC) können Sie definieren welche Länder Exportlizenzen benötigen und für welche Länder **keine** Exportlizenzen benötigt werden.

Die Verwendung von Exportlizenzen ist weiterhin abhängig davon, welche Regelung für Exportlizenzen beim Land selbst getroffen wurde. Überschneidet sich eine getroffene Regelung, so ist die für ein Land getroffene Regelung für Exportlizenzen rechtlich höher einzustufen. In diesem Fall gilt die Regelung für Exportlizenzen, wie sie für das Land festgelegt wurden.

Siehe auch [Länder verwenden](#) und [Fallbeispiele für Sicherheitsrichtlinien](#)

Siehe auch: [Abbildung 53](#)

In der *Export control classification* legen Sie zudem fest, ob die vertraulichen Daten der gekennzeichneten PPR-Komponenten entweder den Bestimmungen der **International Traffic in Arms Regulations (ITAR)** oder den **Export Administration Regulations (EAR)** unterliegen. Eines der beiden Felder ist immer aktiv.

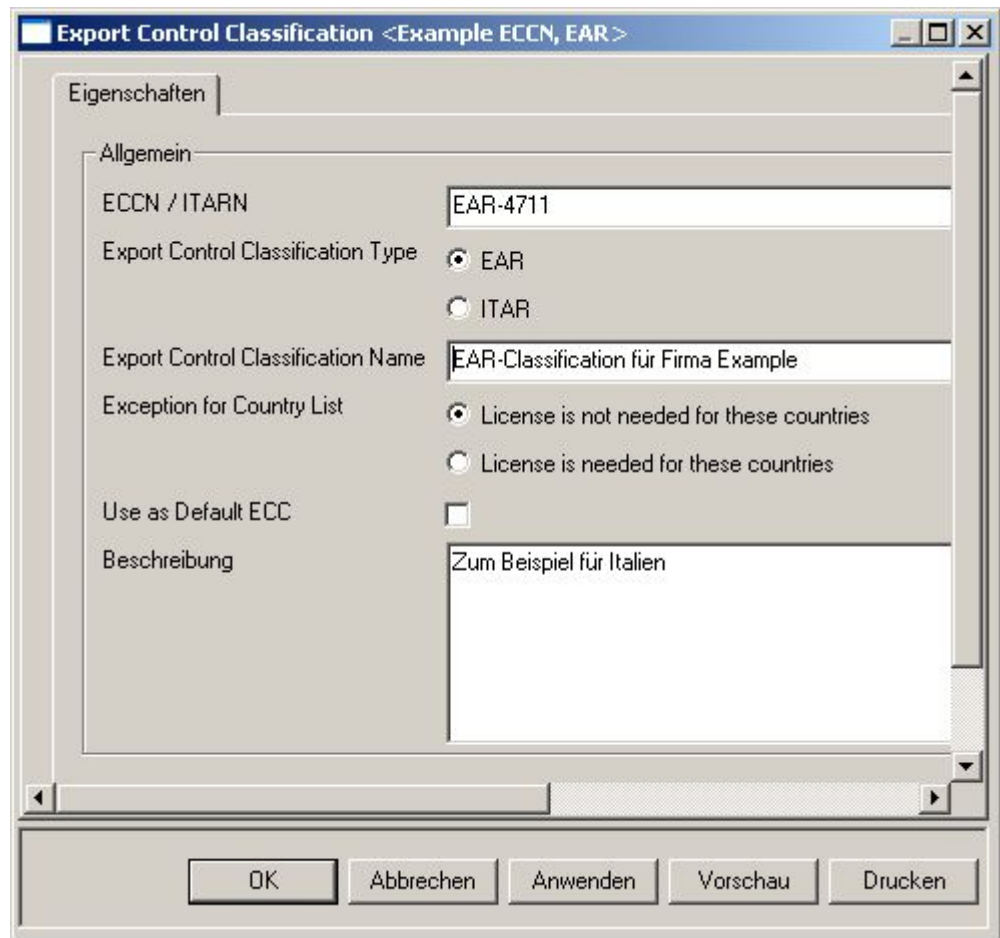
### Export control classification anlegen

- Öffnen Sie in der Systembibliothek *Security Data*.
- Öffnen Sie das Kontextmenü bei *Export Control Classifications*.
- Wählen Sie *Neu / Export Control Classification*.



**Abbildung 41** Kontextmenü für Export Control Classification

Im Eigenschaftsdialog legen Sie die Daten fest, siehe auch [Bedeutung der Felder für Export control classification \(ECC\)](#):



**Abbildung 42:** Eigenschaftsdialog Export Control Classification (ECC)



**Bedeutung der Felder für Export control classification (ECC):****ECCN / ITARN**

Grundsätzlich ist dieses Feld frei beschreibbar – beispielsweise können Sie die Export Classification mit Hilfe des Classificationstyps und einer einmalig vergebenen Nummer eindeutig identifizieren – wie im Beispiel EAR 4711.

**Export Control Classification Type**

Mit Hilfe von EAR oder ITAR Legen Sie hier fest, unter welchen Bestimmungen die Export Control Classification fällt. Die getroffene Festlegung sollten Sie beim Verknüpfen mit Exportlizenzen beachten.

**Export Control Classification Name**

Grundsätzlich ist dieses Feld frei beschreibbar. Legen Sie hier den Namen fest.

**Exception for Country List**

Eines der beiden Felder ist immer aktiviert.

- Ist **License is not needed for these countries** aktiviert gelten folgende Bedingungen: alle Länder die diese ECC zugewiesen bekommen haben, benötigen **keine** Lizenz. Im Umkehrschluss bedeutet das, alle Länder die nicht mit dieser ECC verknüpft sind, benötigen eine Exportlizenz.
  - Ist **License is needed for these countries** aktiviert gelten folgende Bedingungen: alle Länder die diese ECC zugewiesen bekommen haben, benötigen **eine** Lizenz. Im Umkehrschluss bedeutet das, alle Länder die nicht mit dieser ECC verknüpft sind, benötigen keine Exportlizenz.
- ⇒ Lizenzbestimmungen die bei einem Land festgelegt sind, wie Lizenzen für Staatsbürgerschaft oder Aufenthaltsort, könnten, die in der ECC getroffene Regelung, für bestimmte Anwender außer Kraft setzen.

Siehe auch: [Länder verwenden](#).

**Use as Default ECC**

Wenn Sie sich sicher sind, dass die Export Control Classification für alle PPR – Komponenten gelten soll, aktivieren Sie das Feld *Use as Default ECC*.

Ist *Use as Default ECC* aktiviert, werden danach alle neu erzeugten PPR-Komponenten automatisch mit dieser Export Control Classification verknüpft.

**Beschreibung**

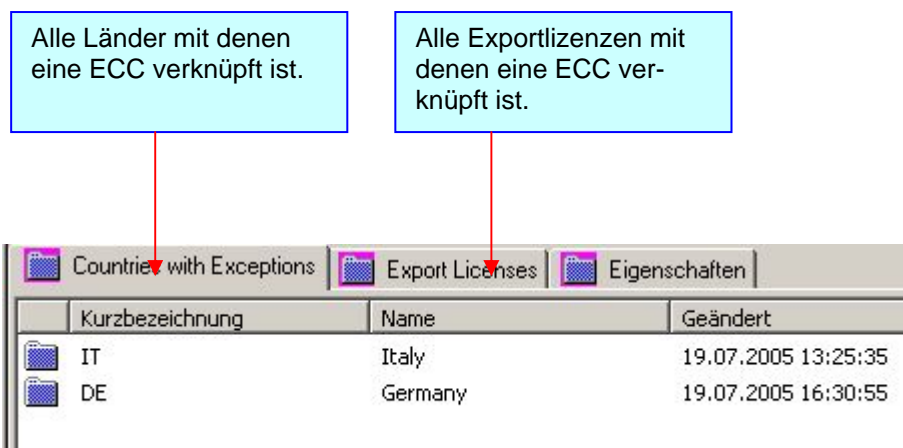
Dieses Feld ist frei beschreibbar und hat nur einen informativen Charakter. Aber es macht durchaus einen Sinn dieses Feld zu nutzen, wenn Sie hier gleich schriftlich hinterlegen, für welche Länder Exportlizenzen benötigt werden.

## Verknüpfungen zu anderen Datenobjekte

Eine Export Control Classification (ECC) können Sie mit beliebig vielen Ländern, Lizenzen und PPR-Komponenten verknüpfen.

- Eine PPR-Komponente unterliegt bereits Exportbeschränkungen, wenn die PPR-Komponente mit einer *Export control classification* verknüpft ist. Für diese PPR-Komponenten gelten die in der ECC festgelegte Definition, für welche Länder eine Exportlizenz benötigt wird.
- Eine Export Control Classification muss mit jeder PPR-Komponente einzeln verknüpft werden. Beachten Sie bei der Verknüpfung die hierarchische Baumstruktur im PPR-Navigator – hat ein Anwender zum Beispiel auf einem Vaterknoten durch Zuweisung einer ECC keinen Zugriff auf das Objekt werden auch die Kinder dieses Vaterobjekts im Baum nicht angezeigt.
- Eine Export Control Classification wird mit dem Land verknüpft, für die Exportlizenzen benötigt werden. Für welche Länder Exportlizenzen benötigt werden, ist in der verknüpften ECC definiert wurden.
- Mit der Verknüpfung der Export Control Classification (ECC) mit einer Exportlizenz legen Sie fest, welche ECC für die Exportlizenz gültig ist. Die Exportlizenzen müssen Sie dann entsprechend nach der in der ECC getroffenen Definition mit Ländern verknüpfen.

Die möglichen Verknüpfungen zu anderen Datenobjekten der Systembibliothek werden in der Listview angezeigt:



**Abbildung 43:** Anzeige für verknüpfte Datenobjekte in der Listview - ECC

## Export Lizenzen verwenden

Mit einer Export Lizenz erteilen Sie die Genehmigung dazu, welche Länder, Firmen und Anwender eine Export Lizenz erhalten sollen.

### Export Lizenz anlegen

- Öffnen Sie in der Systembibliothek *Security Data*.
- Öffnen Sie das Kontextmenü bei *Export Licenses*.
- Wählen Sie *Neu / Export License*.



**Abbildung 44:** Kontextmenü Export License

- Export Lizenzdaten, siehe auch [Bedeutung der Felder für Export Lizenz](#).

The screenshot shows a Windows-style dialog box titled "Export License <001-Example, EAR>". It has a tab labeled "Eigenschaften". Inside, there's a section titled "Allgemein" containing several input fields: "Export License Number" with the value "001-Example", "Export License Type" with radio buttons for "EAR" (selected) and "ITAR", "Applicant Control Number" with the value "002", "Validation Date" and "Expiration Date" both set to "19.07.2005", and a large empty text box for "Beschreibung". At the bottom of the dialog are five buttons: "OK", "Abbrechen", "Anwenden", "Vorschau", and "Drucken".

**Abbildung 45:** Eigenschaftsdialog Export Lizenz

### Bedeutung der Felder für Export Lizenz

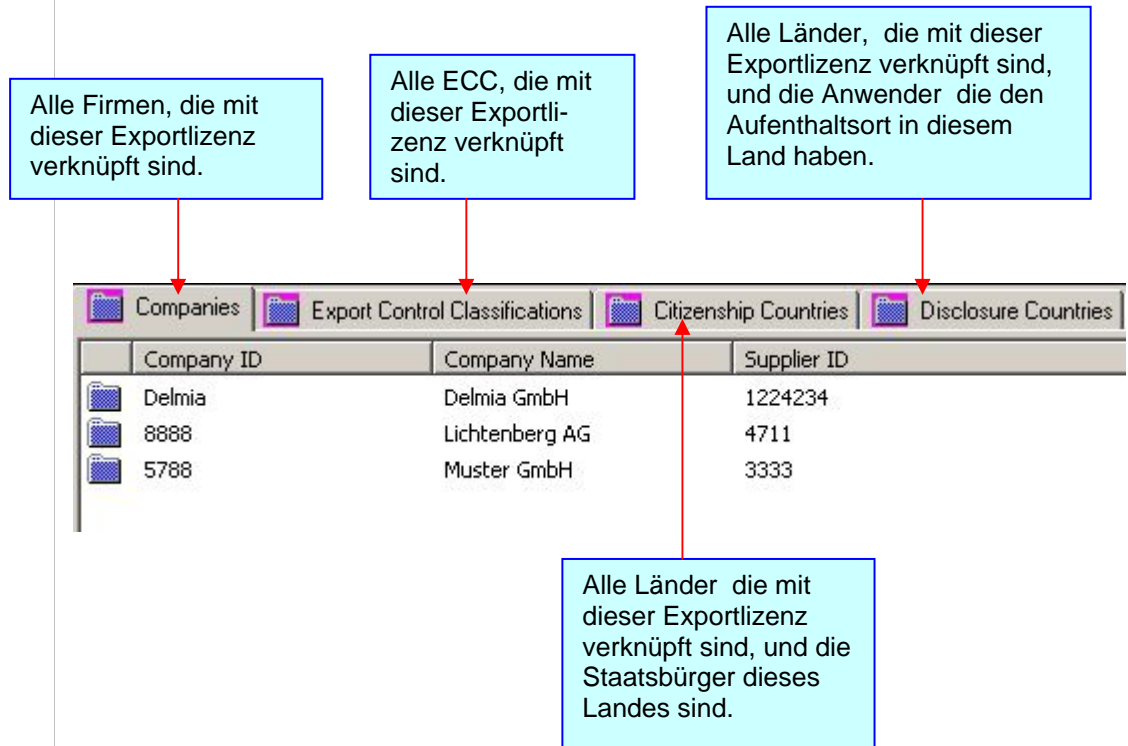
Alle Felder im Eigenschaftsdialog sind frei beschreibbar. Zu den beiden Feldern *Export License Number* und *Application Control Number* müssen Sie Angaben machen - es empfiehlt sich mit Hilfe dieser beiden Felder die Export Lizenz eindeutig zu kennzeichnen.

Mit Hilfe von EAR oder ITAR Legen Sie hier fest, unter welche Bestimmungen die Export Lizenz fällt. Die getroffene Festlegung sollten Sie beim Verknüpfen mit einer Export Control Classification beachten.

Die beiden Felder Gültigkeit und Beschreibung haben nur einen informativen Charakter. Es wäre vielleicht hilfreich bei Beschreibung die Firmen aufzuführen, für die eine Exportlizenz genehmigt werden soll.

## Verknüpfungen zu anderen Datenobjekte

Eine Export Lizenz können Sie mit beliebig vielen Ländern, Firmen und Export Control Classificationen verknüpfen.



**Abbildung 46:** Anzeige für verknüpfte Datenobjekte in der Listview - Exportlizenzen

## Exportlizenzen mit Ländern verknüpfen

Beim Verknüpfen von Exportlizenzen mit einem Land müssen Sie folgende Unterscheidung treffen,

- ob für die Anwender, die die Staatsbürgerschaft dieses Landes haben, eine Lizenz benötigt wird.
- Oder ob für die Anwender mit Aufenthaltsort in diesem Land eine Exportlizenz benötigt wird.

Diese Entscheidung wird notwendig, wenn bei einem Land eine der beiden oder beide Exportbeschränkungen aktiv geschaltet sind.

Siehe auch: [Exportbeschränkungen für ein Land festlegen](#).

- Wählen Sie *License valid for citizens of*, wenn Staatsbürger dieses Landes eine Exportlizenz benötigen.
- Wählen Sie *License valid if located in*, wenn Anwender, die einen Aufenthalt in diesem Land haben, eine Exportlizenz benötigen.
- Wenn beide Exportbeschränkungen für ein Land gelten, so müssen Sie für diese Anwender beide Lizenzberechtigungen jeweils erstellen- also die Lizenz zweimal zuweisen, eben mit der entsprechend selektierten Genehmigung.



Abbildung 47: Berechtigung für die Lizenz auswählen

## Zugriffsrechte auf PPR-Komponenten anwenden

Jede PPR-Komponente ist unter dem Aspekt der Sicherheitsrichtlinien rechtlich gesehen als eigenständiges Objekt anzusehen, das einzeln verwaltet werden muss.

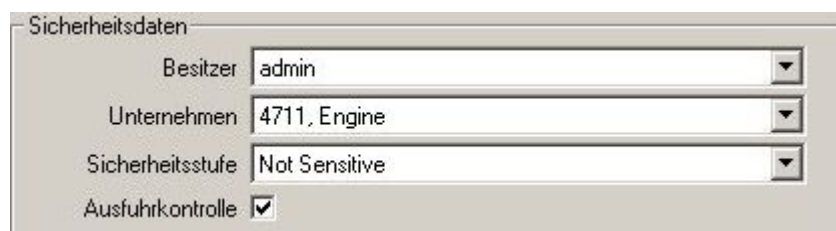
Mit Hilfe der Zugriffsrechte auf PPR-Komponenten regeln Sie

- welche Firma der Eigentümer der PPR-Komponente ist,
- welche Vertraulichkeitsstufe für die PPR-Komponente gilt,
- und ob die PPR-Komponente bereits Exportbeschränkungen unterliegt, ohne dass eine Export Control Classification dieser PPR-Komponente zugewiesen ist.

Standardmäßig ist der Wert der Vertraulichkeitsstufe mit null vorgegeben. Mit der Anwendung der Sicherheitsrichtlinien wird der Zugriff auf Ihre Daten geregelt. Nach dieser Definition sind Sie in der Regel auch Eigentümer der PPR-Komponente.

Wenn einer Fremdfirma erlaubt wird die Zugriffsrechte an Ihren Objekten zu bearbeiten, können Eigentumsrechte an PPR-Komponenten an diese Firmen übertragen werden – genauso wenn Mitarbeiter von Fremdfirmen neue PPR – Komponenten erstellen. In diesem Fall sind Sie für diese PPR-Komponenten die Fremdfirma und müssten entsprechende vertragliche Regelungen mit dieser Firma treffen, die einen Zugriff auf diese PPR-Komponenten erlauben.

Auch hier gilt: stellvertretend für Sie wird die Firma *Engine Co* verwendet.



**Abbildung 48:** Zugriffsrechte einzeln verwalten



### Hinweis

Über Zugriffsrechte können der PPR-Komponente Anwender zugewiesen werden, die entsprechenden Rechte zugeteilt bekommen können – wie etwa im Beispiel der Anwender Example einer Fremdfirma das Recht Schreiben besitzt.

Anwender von Fremdfirmen unterliegen zudem Bestimmungen der Sicherheitsrichtlinien, nur wenn diese zutreffen, kann dieser Anwender das ihm zugeteilte Zugriffsrecht ausführen.

Wie Sie Zugriffsrechte vergeben, wird nach dem bestehenden Rechtekonzept erteilt.

## Zugriffsrechte bearbeiten



Wie Sie Zugriffsrechte erteilen, erfahren Sie im Benutzer Handbuch [Administration](#) im Kapitel über die Benutzerverwaltung.

Die Zugriffsrechte müssen Sie für jede PPR-Komponente einzeln bearbeiten.

- ➔ Öffnen Sie das Kontextmenü auf einer selektierten PPR-Komponente.



Abbildung 49: Kontextmenü Zugriffsrechte öffnen



Im Dialog Rechte bearbeiten können Sie nachfolgend beschriebenen Maßnahmen treffen. Der Besitzer, im Beispiel *admin*, spielt bei der Anwendung der Sicherheitsrichtlinien keine Rolle.

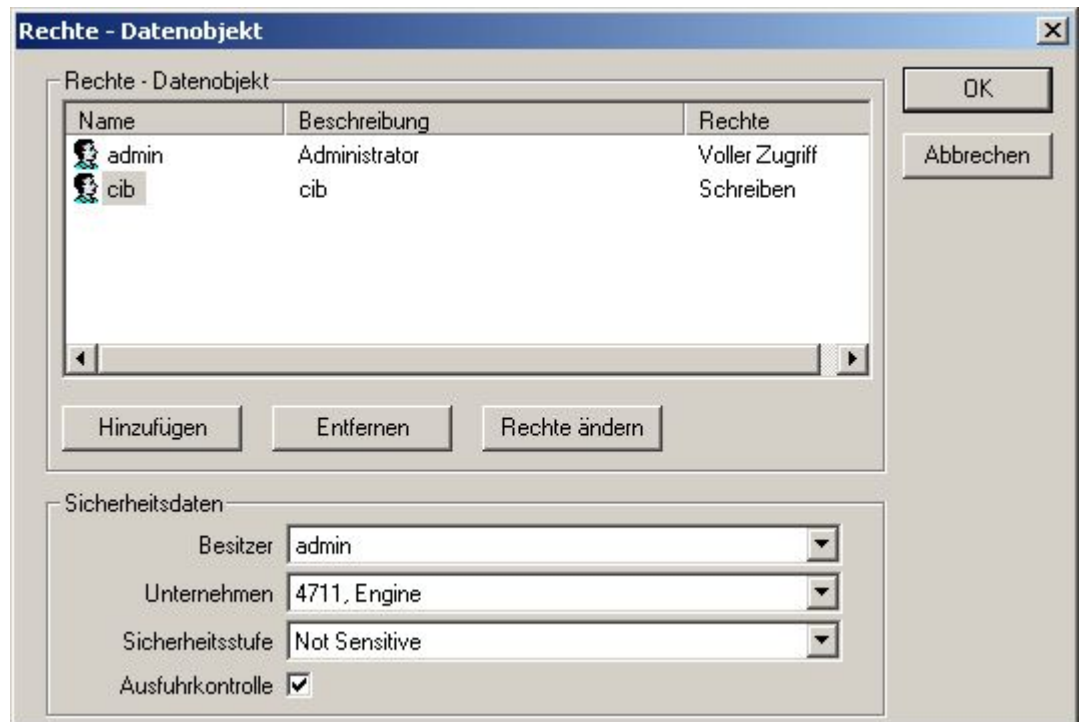


Abbildung 50. Dialog Rechte Datenobjekt

Für die Anwendung der Sicherheitsrichtlinien sind die drei Felder **Unternehmen**, **Sicherheitsstufe** und **Ausfuhrkontrolle** von besonderer Bedeutung.

## Zur Firma

Wenn der Ersteller der PPR-Komponente einer Firma zugeordnet ist, wird automatisch diese Firma angezeigt. In der Regel ist es der Ersteller Ihrer Firma, also im Beispiel Ihr Administrator, oder ein Mitarbeiter Ihrer Firma der die entsprechenden Rechte besitzt.

Über die Combobox kann die PPR-Komponente einer anderen Firma zugewiesen werden. In der Combobox stehen alle angelegten Firmen zur Auswahl zur Verfügung, auch Ihre eigene Firma – im Beispiel die Engine Co. Solange keine Verträge zugewiesen sind, haben nur Mitarbeiter der eingestellten Firma Zugriff auf diese PPR – Komponente.

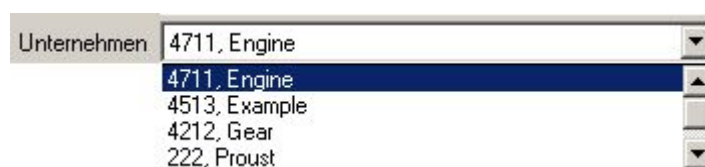


Abbildung 51: Auswahl Firmen

## Zur Sicherheitsstufe

Stellen Sie hier die Vertraulichkeitsstufe ein, die für Ihre PPR-Komponente rechtlich gelten soll.

Die Vertraulichkeitsstufen stehen nur dann zur Verfügung, wenn Sie zuvor für eine Firma festgelegt wurden. Es stehen dann immer alle für die entsprechende Firma festgelegten Vertraulichkeitsstufen zur Verfügung, aus der Sie die Auswahl aus der Combobox treffen können.

Wenn keine Vertraulichkeitsstufe für die PPR-Komponente festgelegt wurde, ist immer *Not Sensitive* eingestellt, die der Vertraulichkeitsstufe null entspricht. Mit Hilfe der eingestellten Vertraulichkeitsstufe wird der Zugriff auf Ihre PPR-Komponente geregelt. Ein Anwender muss neben den geltenden Regelungen der Exportbestimmungen – wie etwa Vertrag, ECC oder Exportlizenz – dieser oder einer höheren Vertraulichkeitsstufe entsprechen, die einen Zugriff erlaubt.

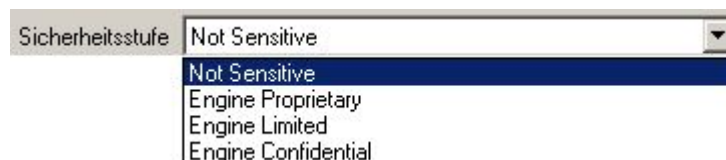


Abbildung 52: Auswahl Vertraulichkeitsstufen

## Zu Ausfuhrkontrolle

Mit Hilfe von *Ausfuhrkontrolle* wird definiert, ob die PPR-Komponente für Anwender bereits einer Exportbeschränkung unterliegt oder nicht, unabhängig davon, ob die PPR-Komponente mit einer ECC verknüpft wurde.

Wenn dieses Feld an einem Objekt aktiviert ist, haben alle Anwender mit entsprechenden Projektrechten einen Zugriff auf das Objekt, die nicht explizit ausgeschlossen sind.

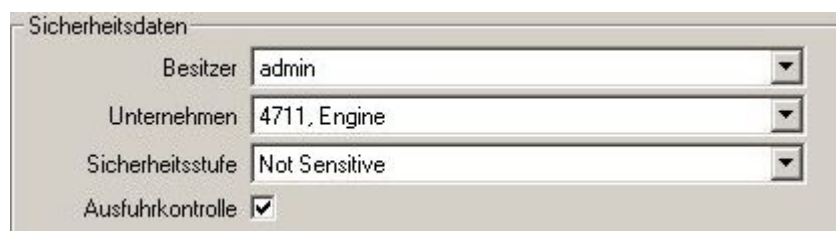


Abbildung 53: Dialog Zugriffsrechte

### Ausschlusskriterien:

- Der Anwender der Bürger eines Landes ist, das als *Embargo Country* gekennzeichnet ist.
- Der Anwender hat keine entsprechend hohe Vertraulichkeitsstufe (*Security Level*).
- Der Anwender ist Mitarbeiter eines anderen Unternehmens, das keinen entsprechenden Vertrag abgeschlossen hat, das einen Zugriff auf diese PPR-Komponenten erlaubt.

## PPR-Komponenten mit anderen Datenobjekten verknüpfen

Eine PPR-Komponente können Sie mit beliebig vielen verschiedenen Verträgen und Export Control Classifications (ECC) verknüpfen.



### Hinweis

*Achten Sie beim Verknüpfen von PPR-Komponenten auf die Hierarchie der Baumstruktur. Wenn Sie beispielsweise eine ECC mit einem Vaterobjekt verknüpfen, bedeutet dies, dass die Kinder dieses Objekts im Baum nicht angezeigt werden, wenn der Anwender über keine gültige Exportlizenz verfügt. Obwohl die Kinder mit keiner ECC verknüpft wurden.*

Mit Hilfe der Verknüpfung von Verträgen zu PPR-Komponenten legen Sie die Grundlage für den Zugriff von Fremdfirmen auf Ihre Daten. Ohne einen verknüpften Vertrag ist der Zugriff auf Ihre Daten ausgeschlossen.

- ⇒ Nachdem ein Vertrag mit einer PPR-Komponente verknüpft ist, kann ein Anwender unter bestimmten Voraussetzungen ohne weitere Anpassungen, der wiederum mit diesem Vertrag verknüpft wurde, bereits auf Ihre Daten zugreifen:
- ⇒ Die eingestellte Vertraulichkeitsstufe muss den Wert **null** haben, also auf **Not Sensitive** eingestellt sein.
- ⇒ Die PPR-Komponente darf nicht einer Exportbeschränkung unterliegen. Das bedeutet, das Feld **Ausfuhrkontrolle** darf bei dieser PPR-Komponente nicht aktiviert sein, und die PPR-Komponente darf mit keiner **ECC** verknüpft sein.

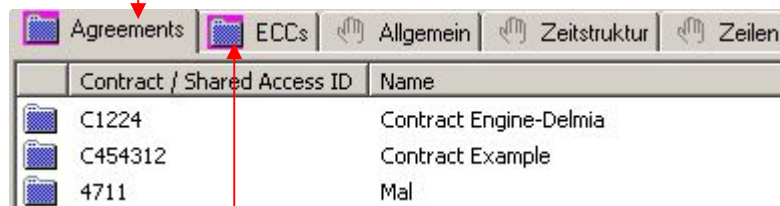
Mit Hilfe einer verknüpften ECC wird der Zugriff auf PPR-Komponenten geregelt, die Exportbeschränkungen unterliegen. Es haben nach dieser Definition nur die Anwender von Ländern auf diese PPR-Komponente einen Zugriff, die über eine gültige Exportlizenz verfügen.

- ⇒ Nach der Verknüpfung mit einer PPR-Komponente, wird die in der ECC getroffene Regelung sofort wirksam. Für Anwender, die nicht über eine gültige Export Lizenz verfügen, ist der Zugriff auf Ihre Daten verboten.
- ⇒ Die Verknüpfung zwischen PPR-Komponenten und Verträgen und Export Control Classifications führen Sie per Drag & Drop aus. Hierzu benötigen Sie das „Change Rights“ Recht an der PPR – Komponente sowie das „Read“ Recht an den Verträgen und ECCs.

## Anzeige der verknüpften Datenobjekte in der Listview

Die Verknüpfungen werden in der Listview der selektierten PPR-Komponente angezeigt.

Unter dem Reiter Agreements werden alle verknüpften Verträge angezeigt



Contract / Shared Access ID	Name
C1224	Contract Engine-Delmia
C454312	Contract Example
4711	Mal

Unter dem Reiter ECCs werden alle verknüpften Export Control Classifications angezeigt

**Abbildung 54:** Anzeige von Verknüpfungen in der Listview – PPR-Komponente

## Entscheidungstabelle für Exportlizenzen – wichtige Fälle

In den nachfolgenden Tabellen wird an mehreren beispielhaften Fällen die Vorgehensweise gezeigt, wenn ein entsprechender Zugriff auf PPR-Komponenten erlaubt ist. Der User ist dabei immer ein User einer Fremdfirma.

In dieser Tabelle werden zwei Fälle aufgezeigt: Im ersten Fall bestehen keine Exportbeschränkung für PPR-Komponenten. Im zweiten Fall unterliegt die PPR-Komponente mit Hilfe von *Is exported controlled* bereits einer ersten Exportbeschränkung.

Entscheidungstabelle für Exportlizenzen	
Fallbeschreibung	Zugriff auf PPR-Komponenten
<b>Fall1:</b> Keine Exportbeschränkung für PPR-Komponenten. Vertraulichkeitsstufe auf PPR-Komponente ist null (not sensitive).	<b>Voraussetzungen:</b> ⇒ User muss mit Vertrag verknüpft sein. ⇒ Vertrag muss mit PPR-Komponente verknüpft sein. <b>Fazit:</b> Alle User, die einen Vertrag haben, haben Zugriff auf die PPR-Komponente.
<b>Fall2:</b> Ausfuhrkontrolle ist bei PPR-Komponente aktiviert. Vertraulichkeitsstufe (Security Level) auf PPR-Komponente ist null (not sensitive).	<b>Voraussetzungen:</b> ⇒ User muss mit Vertrag verknüpft sein. ⇒ Vertrag muss mit PPR-Komponente verknüpft sein. <b>Fazit:</b> Alle User, die einen Vertrag haben, und keinem als Embargo Land gekennzeichnetem Land zugewiesen sind, haben Zugriff auf die PPR-Komponente. Für den Ausschluss eines User, das als Embargo Land gekennzeichnet ist, reicht es aus, wenn einer der drei Optionen erfüllt ist: ⇒ Der User ist Staatsbürger dieses Landes. ⇒ Der User hat den Aufenthaltsort in diesem Land. ⇒ Die Firma, der der User zugeordnet ist, hat den Firmensitz in diesem Land.

Abbildung 55: Tabelle 1 – Beschreibung Ausfuhrkontrolle aktiviert

In dieser Tabelle wird auf den Fall eingegangen, dass der Security Level an der PPR-Komponente höher null ist.

Entscheidungstabelle für Exportlizenzen	
Fallbeschreibung	Zugriff auf PPR-Komponenten
<b>Fall3:</b> Vertraulichkeitsstufe (Security Level) auf PPR-Komponente ist größer null. PPR-Komponente hat einen entsprechend hohen, bei der Firma festgelegten Security Level zugewiesen bekommen.	<b>Voraussetzungen:</b> <ul style="list-style-type: none"> <li>⇒ User muss mit Vertrag verknüpft sein.</li> <li>⇒ Vertrag muss mit PPR-Komponente verknüpft sein.</li> <li>⇒ User muss mit Ihrer Firma verknüpft sein. Stellvertretend wird für Ihre Firma in den Beispielen die Firma <b>Engine Co</b> verwendet.</li> <li>⇒ Für Firma müssen Security Levels vorhanden sein.</li> <li>⇒ User muss entsprechend hohen Security Level der Firma zugewiesen bekommen haben.</li> </ul> <b>Fazit:</b> Alle User haben einen Zugriff auf die PPR-Komponente, die mit der Firma verknüpft sind und einen entsprechend hohen Security Level zugewiesen bekommen haben: Beispiel, die PPR-Komponente hat der Security Level 2 zugewiesen bekommen, so muss der User mindestens den Security Level 2 haben oder größer.

**Abbildung 56:** Tabelle 2 – Beschreibung Security Level größer null.

In dieser Tabelle wird auf den Fall eingegangen, dass beim Land die Option *Citizen possibly needs a License* aktiviert ist.

Entscheidungstabelle für Exportlizenzen	
Fallbeschreibung	Zugriff auf PPR-Komponenten
<p><b>Fall4:</b></p> <p>Beim Land ist diese Option eingestellt.</p> <p><input checked="" type="checkbox"/> Citizen possibly needs a License</p> <p>Vertraulichkeitsstufe (Security Level) auf PPR-Komponente ist null (not sensitive).</p>	<p><b>Voraussetzungen:</b></p> <ul style="list-style-type: none"> <li>⇒ User muss mit Vertrag verknüpft sein und muss Staatsbürger dieses Landes sein.</li> <li>⇒ Vertrag muss mit PPR-Komponente verknüpft sein.</li> <li>⇒ ECC muss mit PPR-Komponente und Land verknüpft sein.</li> <li>⇒ ECC muss mit Exportlizenz verknüpft sein.</li> <li>⇒ Exportlizenz muss mit Land und Firma verknüpft sein.</li> </ul> <p><b>Fazit:</b></p> <ul style="list-style-type: none"> <li>⇒ In der ECC muss festgelegt sein, dass für dieses Land eine Exportlizenz benötigt wird.</li> <li>⇒ ECC muss mit dem Land verknüpft sein, für welches die Exportlizenz erforderlich ist.</li> <li>⇒ Exportlizenz muss mit dem Land und der Firma verknüpft werden, für die die Exportlizenz gilt.</li> <li>⇒ Bei der Verknüpfung der Exportlizenz mit dem Land, muss die Auswahl User ist Staatsbürger dieses Landes (License valid for citizens of..) selektiert werden.</li> </ul> <p><b>Ergänzung für diesen Fall:</b></p> <p>Wenn der Security Level bei der PPR-Komponente höher als null wäre, müssten Sie zudem den User mit Ihrer Firma (im Beispiel, Firma Engine Co) verknüpfen, und dem User den entsprechenden Security Level zuweisen.</p>

**Abbildung 57:** Tabelle 3 – Beschreibung *Citizen possibly needs a License*

In dieser Tabelle wird auf den Fall eingegangen, dass beim Land die Option *Sojourn possibly needs a License* aktiviert ist.

Entscheidungstabelle für Exportlizenzen	
Fallbeschreibung	Zugriff auf PPR-Komponenten
<p><b>Fall 5:</b></p> <p>Beim Land ist diese Option eingestellt.</p> <p><i>Sojourn possibly needs a License</i> <input checked="" type="checkbox"/></p> <p>Vertraulichkeitsstufe (Security Level) auf PPR-Komponente ist null (not sensitive).</p>	<p><b>Voraussetzungen:</b></p> <ul style="list-style-type: none"> <li>⇒ User muss mit Vertrag verknüpft sein. User muss entweder den Aufenthaltsort in diesem Land haben, oder der Firmensitz muss in diesem Land sein.</li> <li>⇒ Vertrag muss mit PPR-Komponente verknüpft sein.</li> <li>⇒ ECC muss mit PPR-Komponente und Land verknüpft sein.</li> <li>⇒ ECC muss mit Exportlizenz verknüpft sein.</li> <li>⇒ Exportlizenz muss mit Land und Firma verknüpft sein.</li> </ul> <p><b>Fazit:</b></p> <ul style="list-style-type: none"> <li>⇒ In der ECC muss festgelegt sein, dass für dieses Land eine Exportlizenz benötigt wird.</li> <li>⇒ ECC muss mit dem Land verknüpft sein, für welches die Exportlizenz erforderlich ist.</li> <li>⇒ Exportlizenz muss mit dem Land und der Firma verknüpft werden, für die die Exportlizenz gilt.</li> <li>⇒ Bei der Verknüpfung der Exportlizenz mit dem Land, muss die Auswahl User hat den Aufenthaltsort in diesem Land (License valid if located in..) selektiert werden.</li> </ul> <p><b>Ergänzung für diesen Fall:</b></p> <p>Wenn der Security Level bei der PPR-Komponente höher als null wäre, müssten Sie zudem den User mit Ihrer Firma (im Beispiel, Firma Engine Co) verknüpfen, und dem User den entsprechenden Security Level zuweisen.</p>

**Abbildung 58:** Tabelle 3 – Beschreibung *Sojourn possibly needs a License*



## Fallbeispiele für Sicherheitsrichtlinien

Eine Exportlizenz für ein Land, und damit auch für Anwender von Firmen, die diesem Land zugeordnet sind, wird erst dann fällig, wenn Sie bei einem Land einer dieser beiden Optionen aktiviert haben:

- *Citizen possibly needs a License* oder
- *Sojourn possibly needs a License*.

Wenn eine Exportlizenz fällig werden kann, ist das in der Export Control Classification (ECC) festgelegt. Auch eine ECC wird für PPR-Komponenten erst fällig, wenn einer der beiden Optionen bei einem Land aktiviert wurde.

Vor diesem Hintergrund wird Ihnen in diesem Kapitel die Vorgehensweise an exemplarisch ausgewählten Beispielen näher erläutert.

Folgende Konventionen sollen für die nachfolgenden Beispiele gelten:

- Länder die als Embargo Land gekennzeichnet sind, werden in diesen Beispielen nicht näher betrachtet, weil für PPR-Komponenten, die in irgendeiner Form Exportbeschränkungen unterliegen ein Zugriff generell nicht gewährt wird.
- Stellvertretend für Ihre Firma, wird die Firma **Engine Co** verwendet.
- Es wird in den folgenden Beispielen hauptsächlich auf die beiden Optionen für ein Land eingegangen und die wesentlichen Fälle, die zu berücksichtigen sind, näher erklärt.



---

### **Hinweis**

*Diese Verknüpfungen sollten grundsätzlich nur von einem Administrator oder einem gleichberechtigten Mitarbeiter ausgeführt werden.*

---

## Ausgangssituation Exportlizenz für Staatsbürger

Die Basis für die folgenden Beispiele ist die nachfolgend beschriebene Ausgangssituation, die an entsprechender Stelle variiert wird, um zusätzliche Optionen besser zu verdeutlichen.

### Beschreibung der Ausgangssituation:

- Für das Land Italien ist nur *Citizen possibly needs a License* **aktiviert**. Zu Ländern, lesen Sie bitte das Kapitel [Länder verwenden](#).



The screenshot shows a software interface for configuring a country. The title bar reads 'Country <Italy, IT>'. Below it, there's a tabbed interface with 'Eigenschaften' selected. Under 'Allgemein', there are three fields: 'Kurzbezeichnung' with the value 'IT', 'Name' with the value 'Italy', and a checkbox labeled 'Citizen possibly needs a License' which is checked.

- Ihre Firma Engine Co hat den Firmensitz in den USA.
- Firma Lichtenberg AG hat den Firmensitz in Italien. Zu Firmen, lesen Sie das Kapitel [Firmen verwenden](#).
- Anwender Tonio ist Staatsbürger von Italien, hat den Aufenthaltsort in Italien und ist Mitarbeiter der Firma Lichtenberg. Zu Anwender, lesen Sie bitte das Kapitel [Anwender in der Benutzerverwaltung anlegen](#).

Weiterhin sollen für die Projektdaten Ihrer Firma **Engine Co** folgende Bedingungen gelten:

- Exportbeschränkungen sollen nur für Prozessdaten vorhanden sein, im Beispiel Prozess P1.
- Alle Hierarchieebenen der Prozessstruktur sollen mit einem Vertrag verknüpft werden.
- Prozess P1 soll mit der ECC verknüpft werden. In der ECC soll festgelegt werden, dass für dieses Land – im Beispiel Italien – eine Exportlizenz benötigt wird.
- Für die PPR-Komponenten soll der Security Level null (not sensitive) gelten.
- Alle Prozesse sollen der Firma Engine Co zugeordnet sein.

**Ausgangssituation Firma Engine****Abbildung 59:** Beispiel – Projektdaten Firma Engine**Hinweis**

Beachten Sie beim Verknüpfen von Verträgen und ECC's die Baumstruktur. Verknüpfungen müssen einzeln für jedes Objekt in der Baumstruktur erstellt werden, wenn Sie das nicht beachten, könnte es sein, dass Kinder eines Vaterobjekts von dem erlaubten Zugriff ausgeschlossen sind oder überhaupt erst nicht angezeigt werden.

**Hinweis**

Vergessen Sie das Speichern nicht bei allen Aktionen, die Sie bei der Herstellung von Verknüpfungen durchführen.

## Verknüpfungen vornehmen – Beispiel 1

Nachfolgend lernen Sie die notwendigen Schritte und Verknüpfungen kennen, die notwendig sind, um das erste Ziel zu erfüllen, dass die Staatsbürger von Italien eine Exportlizenz für den Zugriff auf Ihre Prozessdaten benötigen.

### Schritt 1: Vertrag mit Anwender Tonio verknüpfen

Zwischen der Firma Lichtenberg AG und Ihrer Firma soll folgender Vertrag bestehen.

Zum Anlegen und Verknüpfen von Verträgen, siehe [Verträge – und Abkommen verwenden](#).

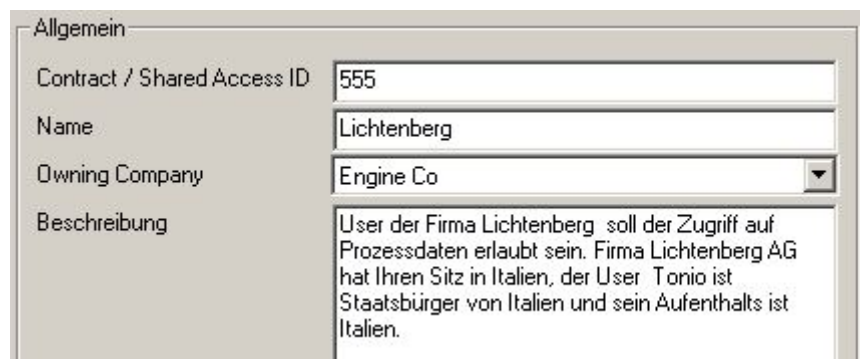


Abbildung 60: Vertrag anlegen

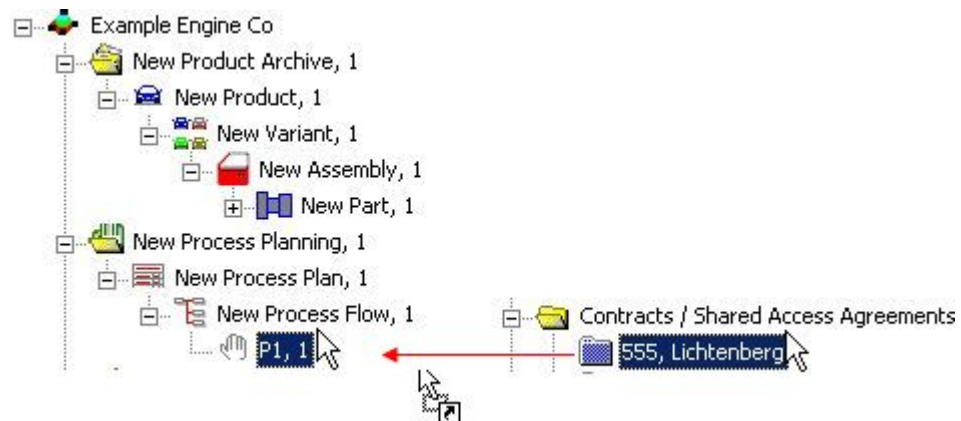
- Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt Benutzer den Anwender Tonio.
- Ziehen Sie den Mauszeiger auf den Vertrag. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.



Abbildung 61: Verknüpfung Vertrag und Anwender

## Schritt 2 : Vertrag mit PPR-Komponenten verknüpfen

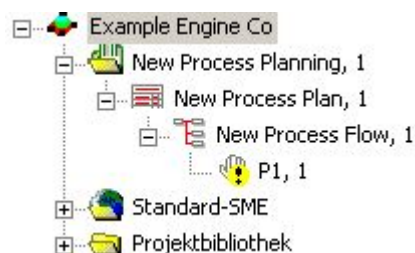
- Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Contract / Shared Agreements* den Vertrag.
- Ziehen Sie den Mauszeiger einzeln auf jede PPR-Komponente. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.



**Abbildung 62:** Verknüpfungen zwischen Vertrag und PPR-Komponenten herstellen.

### Erstes Zwischenergebnis:

Nachdem der Vertrag mit allen PPR-Komponenten der Prozessstruktur Ihrer Firma Engine Co verknüpft ist, hat der Anwender Tonio der Firma Lichtenberg zum einen nur noch auf Prozessdaten einen Zugriff, da für die Produkt- und Ressourcendaten keine vertragliche Vereinbarung besteht. Und zum anderen, weil für die Prozessdaten noch keine Exportbeschränkung gilt. Siehe auch [Abbildung 59](#).



**Abbildung 63:** Zugriff durch Verknüpfung mit Vertrag erlaubt

### Schritt 3: ECC mit PPR-Komponenten und Land verknüpfen

Export Control Classifications (ECC) zuweisen, dazu sind nachfolgende Schritte notwendig:

- Anlegen einer ECC. In der festgehalten ist, dass für Italien eine Exportlizenz benötigt wird.
- Verknüpfen der ECC mit PPR-Komponente und Land.

#### Anlegen einer ECC :

In der ECC muss *Licence is needed for these Country* aktiviert sein. Weitere Informationen zur Export Control Classification (ECC), siehe auch [Export control classification \(ECC\) verwenden](#).

Abbildung 64: Anlegen einer ECC

#### Verknüpfen der ECC mit Land:

Im Beispiel wird die ECC nur mit Italien verknüpft.

- Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Export Control Classification* die gültige ECC.
- Ziehen Sie den Mauszeiger auf das Land. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.

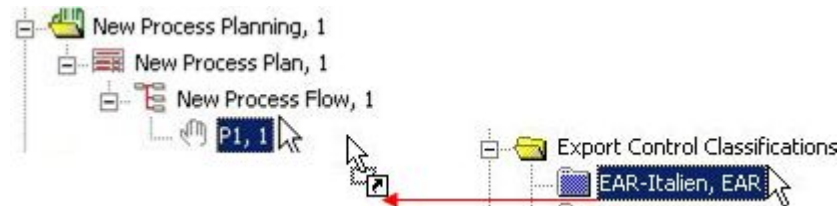


Abbildung 65: ECC mit Land verknüpfen

**Verknüpfen der ECC mit PPR-Komponente :**

Im Beispiel wird die ECC nur mit dem Prozess P1 verknüpft.

- Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Export Control Classification* die gültige ECC.
- Ziehen Sie den Mauszeiger auf den Prozess (P1). Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.

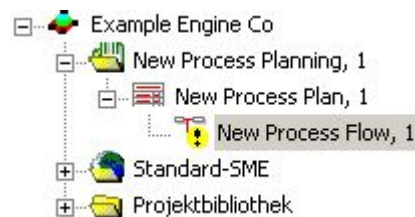


**Abbildung 66:** ECC mit Prozess verknüpfen

**Erstes Zwischenergebnis:**

Nachdem die ECC mit dem Land und der PPR-Komponente P1 verknüpft ist, kann der Anwender Tonio nicht mehr auf die PPR-Komponente zugreifen. Für diese PPR-Komponente gilt die Exportbeschränkung, dass Staatsbürger aus Italien eine Exportlizenz benötigen.

Alle anderen Anwender, die keine Staatsbürger von Italien sind, und die vertraglich berechtigt wären auf Ihre Daten zugreifen zu können, hätten in diesem Beispiel einen Zugriff auf diese PPR-Komponente.



**Abbildung 67:** Zugriff verweigert

Um einen Zugriff für den Anwender Tonio zu gewähren, benötigt dieser also eine Exportlizenz. Die Vorgehensweise zur Exportlizenz lernen Sie im nächsten Schritt kennen.

### Schritt 4: Zugriff wird mit der Exportlizenz gewährt

Um eine Exportlizenz zuzuweisen, dazu sind nachfolgende Schritte notwendig:

- Anlegen der Exportlizenz
- Verknüpfen der Exportlizenz mit der ECC, Firma und Land.

#### Anlegen einer Exportlizenz:

In der Exportlizenz werden die Bedingungen festgehalten, für die diese gilt. Im Beispiel also die Bedingungen für die Firma Lichtenberg AG.

Weitere Informationen zu Exportlizenzen, siehe auch [Export Lizenzen verwenden](#).

Abbildung 68: Anlegen einer Exportlizenz

#### Verknüpfen der Exportlizenz mit der gültigen ECC:

Im Beispiel wird die ECC mit der Exportlizenz *5611 Italien* verknüpft.

- Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Export Licenses* die gültige Exportlizenz.
- Ziehen Sie den Mauszeiger auf die ECC. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.



Abbildung 69: Exportlizenz mit ECC verknüpfen



**Verknüpfen der Exportlizenz mit Firma:**

Die Exportlizenz muss mit der Firma verknüpft werden, für die diese Exportlizenz gelten soll – im Beispiel mit der Firma Lichtenberg AG.

- ➔ Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Export Licenses* die gültige Exportlizenz.
- ➔ Ziehen Sie den Mauszeiger auf die ECC. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.



**Abbildung 70:** Exportlizenz mit Firma verknüpfen

**Verknüpfen der Exportlizenz mit Land:**

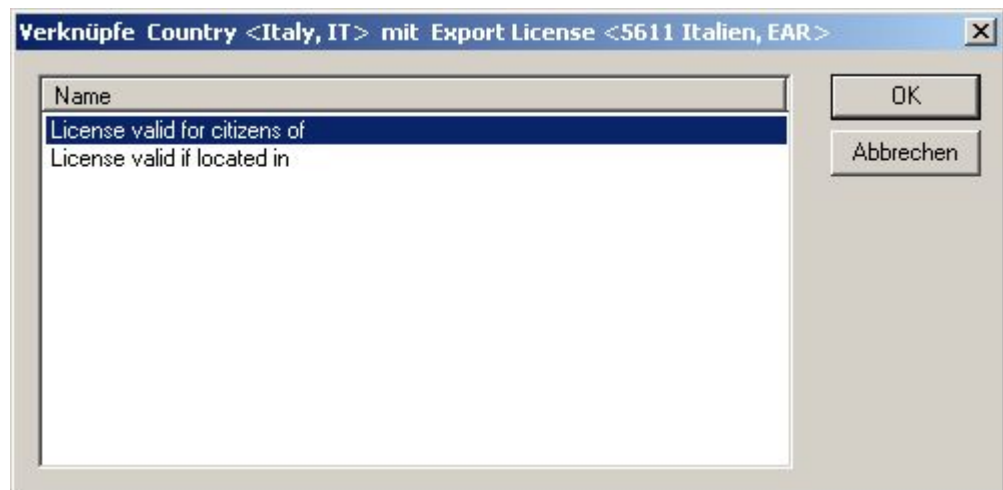
Die Exportlizenz muss mit dem Land verknüpft werden, für welches die Exportlizenz gelten soll – im Beispiel mit Italien.

- Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Export Licenses* die gültige Exportlizenz.
- Ziehen Sie den Mauszeiger auf das Land. Lassen Sie den Mauszeiger danach wieder los.



**Abbildung 71:** Exportlizenz auf das Land ziehen

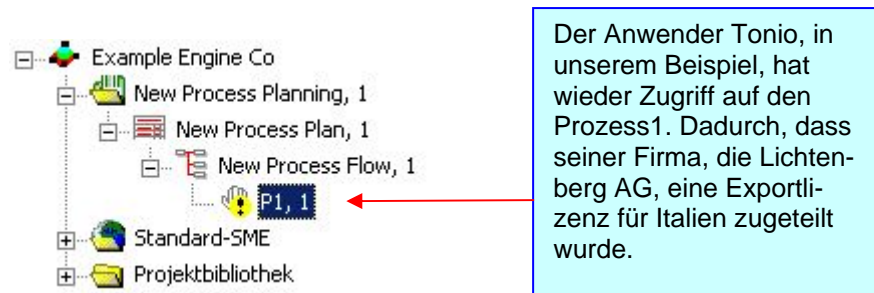
- Wählen Sie für unser Beispiel die Option *License valid for citizens of*.
- Bestätigen Sie die Auswahl mit *OK*. Die Verknüpfung ist hergestellt.



**Abbildung 72:** Staatsbürgerschaft selektieren

**Ergebnis der Verknüpfung**

Anwender Tonio hat jetzt einen Zugriff auf die PPR-Komponente P1.



**Abbildung 73:** Zugriff mit Exportlizenz erlaubt

**Fazit**

Jetzt haben Sie alle Verknüpfungen hergestellt, die notwendig sind, um die Bedingung zu erfüllen, dass die Staatsbürger von Italien eine Lizenz benötigen. Diese beschriebene Vorgehensweise gilt für jedes Land unter denselben Ausgangsbedingungen.

## Verknüpfungen vornehmen – Beispiel 2

### Vertraulichkeitsstufen für Firma Engine

Für Ihre Firma Engine sind für das Beispiel diese Vertraulichkeitsstufen (Security Levels) festgelegt worden. Siehe auch: [Vertraulichkeitsstufen für Firma festlegen](#).

The screenshot shows a Windows-style dialog box titled 'Unternehmen <4711, Engine>'. It has a tab labeled 'Eigenschaften'. Under the 'Allgemein' section, there are several input fields: 'Company ID' with the value '4711', 'Company Name' with 'Engine Co', 'Supplier ID' with '4711', 'Company Site' with a dropdown menu showing 'USA', 'Max. Security Level' with the value '6', and 'Security Levels' with a list box containing the following items: 'Not Sensitive', 'Engine Proprietary', 'Engine Limited', 'Engine Confidential', 'Engine Secret', 'Engine Top Secret', and 'Engine Max Secret'. At the bottom of the dialog, there are buttons for 'OK', 'Abbrechen', 'Anwenden', 'Vorschau', 'Drucken', 'Nächstes', and 'Prev'.

**Abbildung 74:** Vertraulichkeitsstufen für Firma festlegen

Der Zugriff auf die PPR-Komponente P1 ist unter den vorgenommenen Schritten nur erlaubt worden, weil bei den PPR-Komponenten die Vertraulichkeitsstufe (Security Level) auf **not sensitive** eingestellt war.

Für das folgende Beispiel soll der Security Level für den Prozess P1 um eine Stufe erhöht werden.

Nachfolgende Voraussetzungen müssen erfüllt sein:

- Der PPR-Komponente P1 muss den Security Level 1 erhalten.
- Für Ihre Firma müssen Vertraulichkeitsstufen vorhanden sein. Siehe auch: [Firmen verwenden](#).
- Der Anwender Tonio in unserem Beispiel muss mit Ihrer Firma Engine Co verknüpft sein.
- Der Anwender Tonio muss den entsprechenden Security Level zugewiesen bekommen. Dieser Security Level kann gleich oder größer als der Security Level der PPR-Komponente Prozess 1 sein

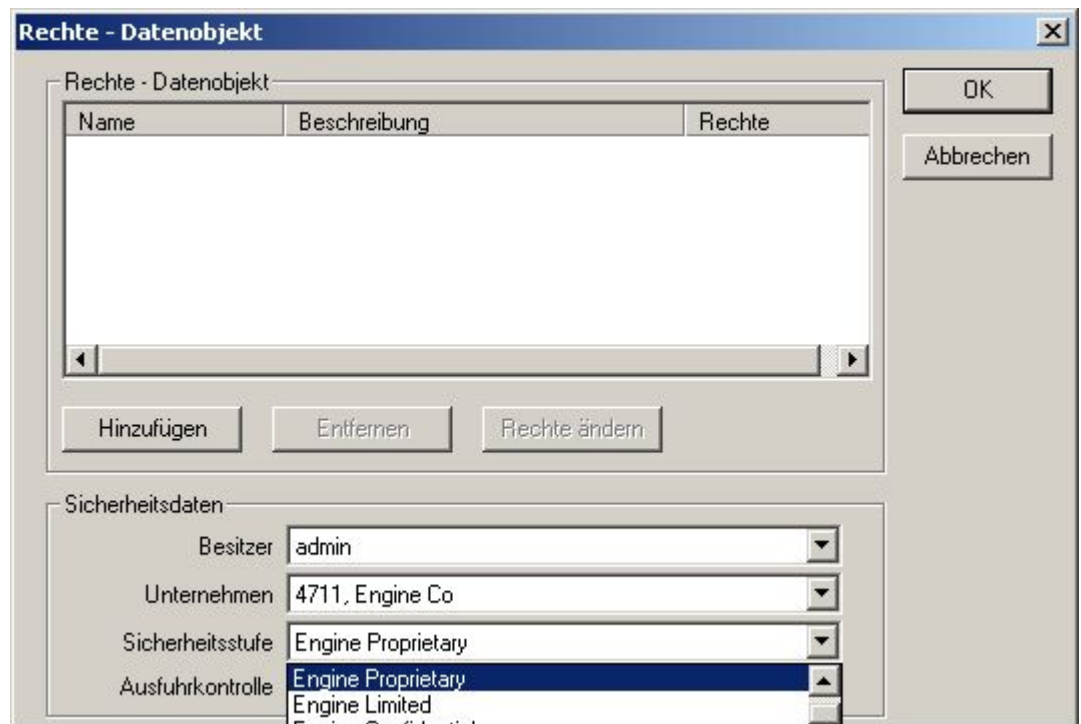
**Security Level bei Prozess 1 um eins erhöhen**

- Öffnen Sie in Ihrem Projekt (Beispiel Engine) das Kontextmenü auf dem Prozess 1.
- Wählen Sie den Menüeintrag Zugriffsrechte. Siehe auch: [Zugriffsrechte auf PPR-Komponenten anwenden](#).



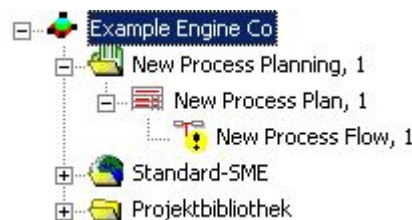
**Abbildung 75:** Kontextmenü auf Prozesskomponente öffnen

- Im Beispiel soll der Security Level um eine Vertraulichkeitsstufe erhöht werden.
- ⇒ Die möglichen Security Levels stehen an der PPR-Komponente nur zur Verfügung, wenn diese auch für die Firma erstellt wurden – im Beispiel also für Ihre Firma Engine.
- Wählen Sie den Security Level aus diesem Dialog aus. Bestätigen Sie die Auswahl mit **OK**.



**Abbildung 76:** Security Level um eins erhöhen

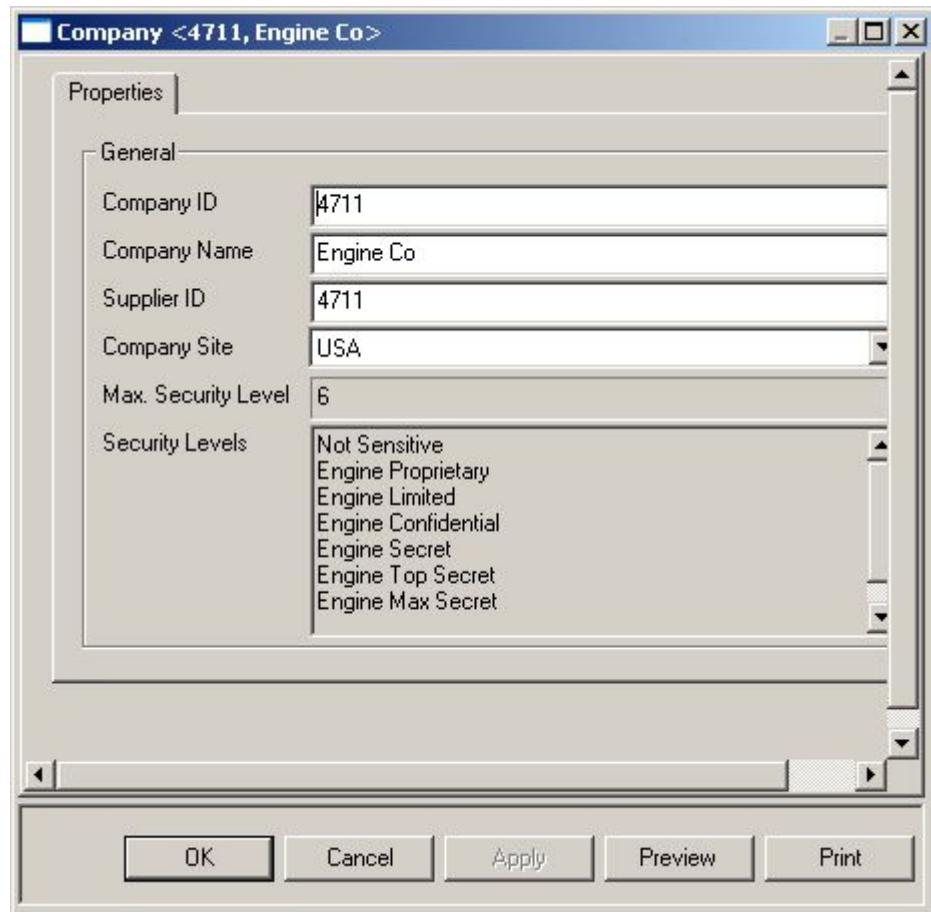
Solange der Anwender Tonio nicht diesen erhöhten Security Level hat, kann er auf diese Prozesskomponente nicht zugreifen.



**Abbildung 77:** Anwender hat keinen entsprechend hohen Security Level

**Vertraulichkeitsstufen für Firma Engine**

Für Ihre Firma Engine sind für das Beispiel diese Vertraulichkeitsstufen (Security Levels) festgelegt worden. Siehe auch: [Vertraulichkeitsstufen für Firma festlegen](#).



**Abbildung 78:** Vertraulichkeitsstufen für Firma festlegen

### Anwender mit Firma Engine verknüpfen

Nur wenn für Ihre PPR-Komponenten eine höhere Vertraulichkeitsstufe größer null vorhanden ist, müssen Sie gegebenenfalls die Anwender einer Firma verknüpfen – im Beispiel Anwender Tonio mit Firma Engine.

- Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt Benutzer den Anwender.
- Ziehen Sie den Mauszeiger auf die Firma. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.

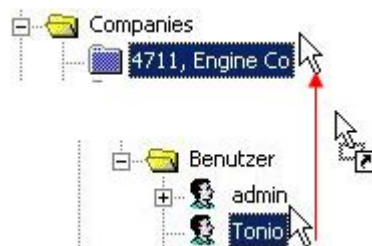


Abbildung 79: Anwender mit Firma verknüpfen

### Vertraulichkeitsstufe für Anwender zuweisen

Nachdem der Anwender mit Ihrer Firma verknüpft ist, können Sie entweder beim Anwender oder bei Ihrer Firma den Security Level zuweisen. Die Verknüpfung wird in der Listview unter dem Reiter *Security Levels* angezeigt.

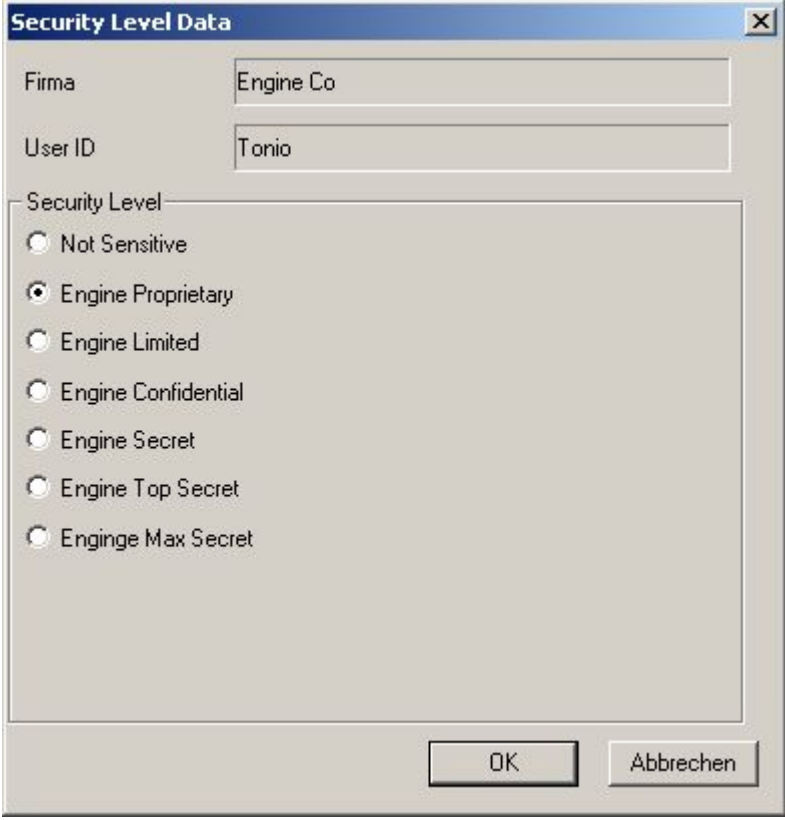
- Klicken Sie in der Listview auf den Reiter *Security Levels*.
- Selektieren Sie die Verknüpfung – im Beispiel eben Engine Co (Tonio).
- Öffnen Sie das Kontextmenü und wählen den Menüeintrag *Edit Security Level*.



Abbildung 80: Kontextmenü öffnen – *Edit Security Level* wählen



- Klicken Sie in das Feld neben den möglichen Security Levels – im Beispiel wird der Security Level **Engine Proprietary** verwendet.
- Bestätigen Sie die Eingabe mit **OK**.



The screenshot shows a Windows-style dialog box titled "Security Level Data". It contains two text input fields: "Firma" with the text "Engine Co" and "User ID" with the text "Tonio". Below these fields is a section titled "Security Level" which contains a list of radio button options. The options are: "Not Sensitive", "Engine Proprietary" (which is selected), "Engine Limited", "Engine Confidential", "Engine Secret", "Engine Top Secret", and "Enginge Max Secret". At the bottom right of the dialog are two buttons: "OK" and "Abbrechen".

**Abbildung 81:** Security Level Anwender zuweisen

### Ergebnis – Beispiel 2

Nachdem alle diese Verknüpfungen erstellt sind, hat der Anwender Tonio wieder einen Zugriff auf die Prozesskomponente P1.

Wenn, wie in diesem Beispiel, die Security Overlays Properties... aktiviert sind, wird der eingestellte Security Level in der Listview von Prozess P1 angezeigt.

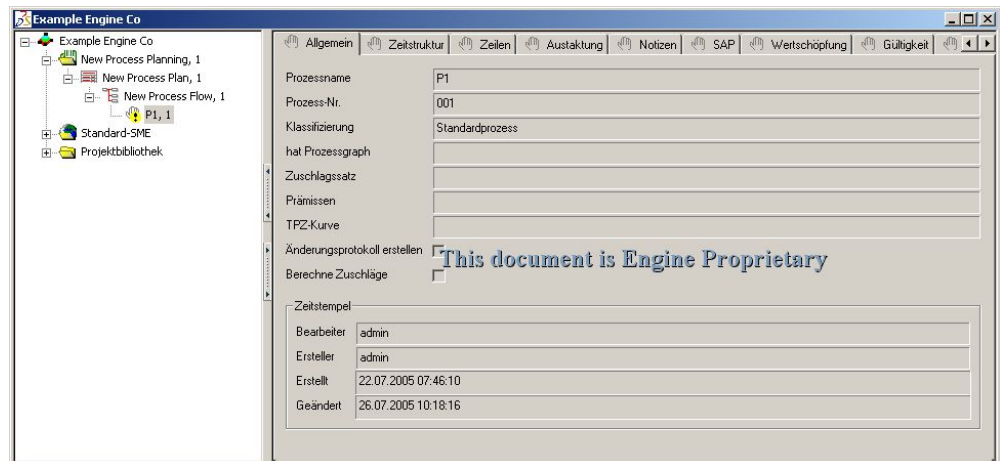


Abbildung 82: Zugriff auf Prozess P1 erlaubt – Beispiel 2

## Verknüpfungen vornehmen Beispiel 3

Für den Zugriff auf die Prozesskomponente **P1** war die wesentliche Voraussetzung in den vorhergehenden Beispielen, dass der Anwender Staatsbürger von Italien ist.

In der Ausgangssituation haben die folgenden Voraussetzungen gegolten:

- Anwender Tonio ist Staatsbürger von Italien.
- Der Aufenthaltsort ist Italien.
- Der Firmensitz ist Italien.

Im diesem Beispiel soll der Aufenthaltsort für den Anwender Tonio geändert werden. Der Aufenthaltsort soll Deutschland sein. Für den Aufenthaltsort Deutschland wird eine Exportlizenz benötigt.

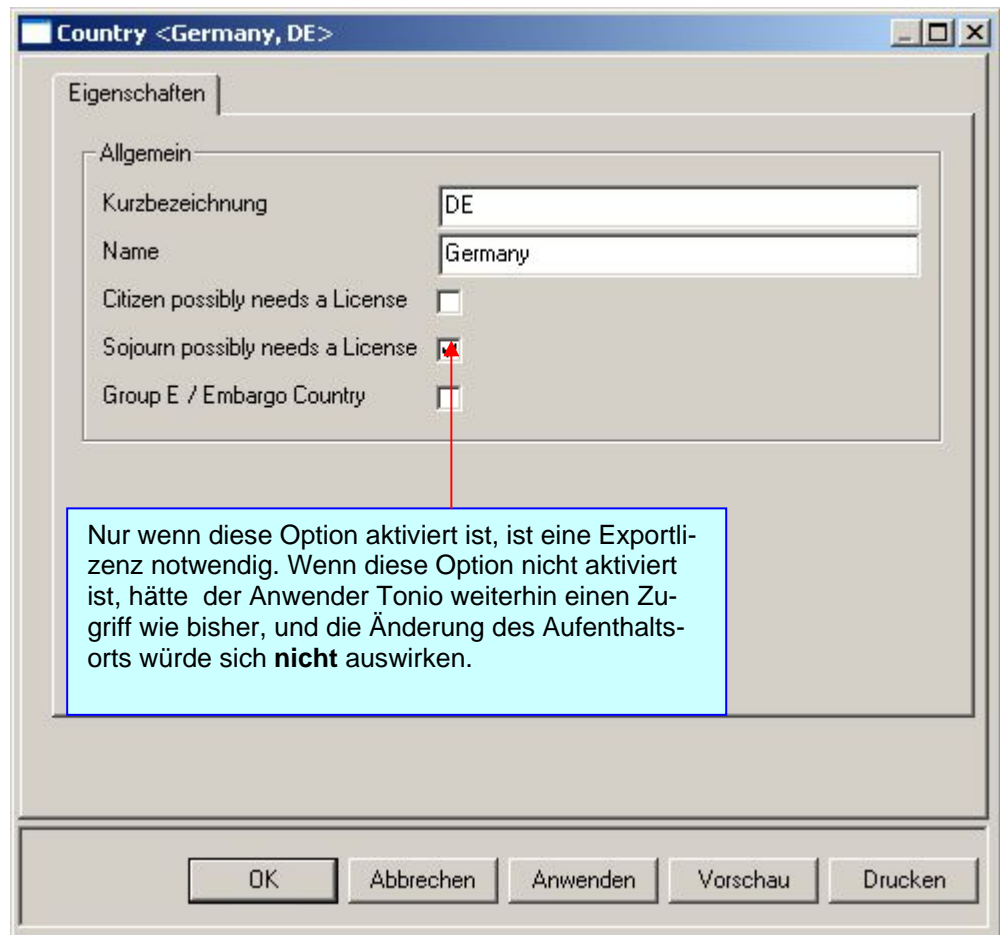
- Ändern Sie in der Benutzerverwaltung beim Anwender den Aufenthaltsort im Beispiel für den Anwender Tonio.
- Siehe auch: [Anwender in der Benutzerverwaltung anlegen](#).

The screenshot shows the 'Eigenschaften - Benutzer' (User Properties) dialog box with the 'Berechtigungseigenschaften' (Permissions) tab selected. The 'Gruppenzugehörigkeit' (Group membership) tab is also visible. The 'Anmeldename' (Username) is 'Tonio'. The 'Beschreibung' (Description) is 'Tonio'. The 'Externe ID' (External ID) is 'Tonio'. The 'Kennwort' (Password) and 'Bestätigung' (Confirmation) fields are masked with asterisks. The checkbox 'Benutzer hat Superuser rechte' (User has superuser rights) is unchecked. The 'Citizenship' dropdown is set to 'Italy, IT'. The 'Ort' (Location) dropdown is set to 'Germany, DE'. The 'Firma' (Company) dropdown is set to '8888, Lichtenberg AG'. The 'OK', 'Rechte...' (Permissions...), and 'Abbrechen' (Cancel) buttons are at the bottom.

**Abbildung 83:** Aufenthaltsort beim Anwender in der Benutzerverwaltung ändern

- Um diese Voraussetzung zu erfüllen, aktivieren Sie beim Land Deutschland das Feld *Sojourn possibly needs a License*.

Siehe auch: [Aufenthaltort für ein Land](#).



**Abbildung 84:** Aufenthaltort für Deutschland aktivieren

**Voraussetzungen:**

Für das Beispiel sollen auch die bisherigen Voraussetzungen gelten. Um die Sache zu vereinfachen ist die bestehende ECC erweitert worden, so dass Sie auch für Deutschland gelten soll. In der Praxis legen Sie in der Regel zuvor schon fest, für welche Länder eine ECC gelten soll.

Folgende Bedingungen müssen erfüllt sein:

- Beim Anwender Tonio muss für den Aufenthaltsort Deutschland eingestellt sein. Siehe [Abbildung 83](#).
- Beim Land muss die Option *Sojourn possibly needs a License* aktiviert sein. Siehe [Abbildung 84](#).
- In der ECC muss festgelegt sein, dass für dieses Land eine Exportlizenz benötigt wird. Im Beispiel wird die ECC noch mit Deutschland verknüpft.

Eigenschaften

Allgemein

ECCN / ITARN: EAR-Italien

Export Control Classification Type: ☒ EAR ☐ ITAR

Export Control Classification Name: ECC Italien benötigt Lizenz

Exception for Country List: ☐ License is not needed for these countries ☒ License is needed for these countries

Use as Default ECC: ☐

Beschreibung: Italien, Deutschland

**Abbildung 85:** ECC für Deutschland erweitert

- Damit der User Tonio einen Zugriff auf die Prozesskomponente erhält, muss die Exportlizenz noch mit Deutschland verknüpft werden.

### ECC mit Land verknüpfen

Im Beispiel wird die ECC mit Deutschland verknüpft. Eine Verknüpfung der ECC mit der Exportlizenz ist für das Beispiel nicht notwendig, da diese Verknüpfung für die Firma **Lichtenberg AG** bereits besteht. Wenn diese Voraussetzung nicht vorhanden wäre, müssten Sie naturgemäß die Verknüpfung zu einer Export Lizenz und die Lizenz mit der Firma verknüpfen.

- Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Export Control Classification* die gültige ECC.
- Ziehen Sie den Mauszeiger auf das Land. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.



Abbildung 86: ECC mit Deutschland verknüpfen

### Exportlizenz mit Land verknüpfen

Im Beispiel wird die Exportlizenz mit Deutschland verknüpft. Eine Verknüpfung der Exportlizenz mit der Firma ist für das Beispiel nicht notwendig, da diese Verknüpfung für die Firma **Lichtenberg AG** bereits besteht.

- Die Verknüpfung kann in beiden Richtungen erfolgen. Selektieren Sie in der Systembibliothek unter dem Datenobjekt *Export Licenses* die gültige ECC – für das Beispiel wiederum dieselbe Exportlizenz (*5611 Italien*).
- Ziehen Sie den Mauszeiger auf das Land. Lassen Sie den Mauszeiger danach wieder los. Die Verknüpfung ist hergestellt.



Abbildung 87: Exportlizenz mit Deutschland verknüpfen

- Selektieren Sie im Dialog *License valid if located in*.
- Bestätigen Sie die Auswahl mit OK. Die Verknüpfung ist hergestellt.

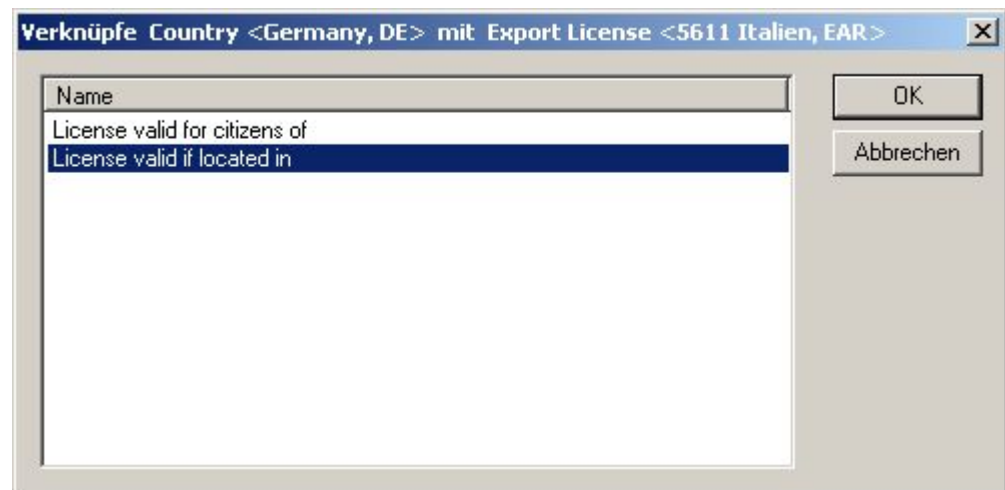


Abbildung 88: Aufenthaltsort selektieren

**Ergebnis – Beispiel 3**

Der Anwender Tonio hat nach diesen Schritten wieder Zugriff auf die PPR-Komponente **Prozess P1**.

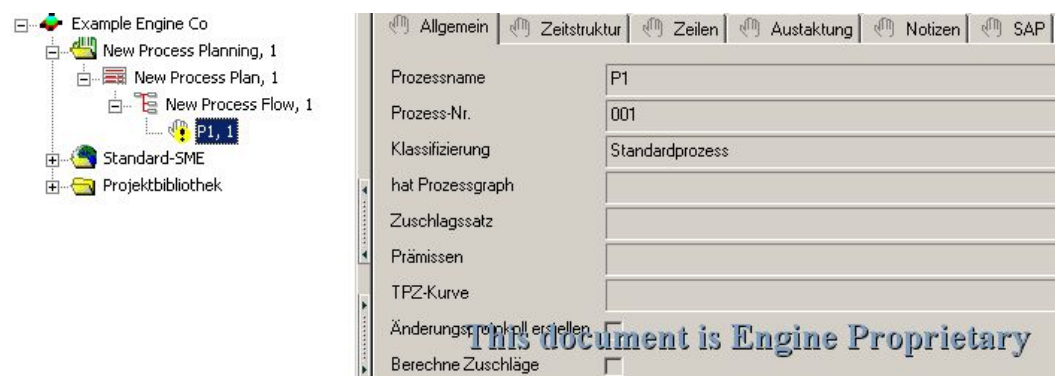


Abbildung 89: Zugriff auf Prozesskomponente erlaubt

# Abbildungsverzeichnis

Abbildung 1: Konfigurationswerkzeug öffnen .....	8
Abbildung 2: Library im Konfigurationswerkzeug öffnen .....	9
Abbildung 3: Datenobjekte der Sicherheitsrichtlinien in der Systembibliothek eingebildet.....	9
Abbildung 4: Datenobjekte einblenden .....	10
Abbildung 5: Kontextmenü auf <i>FilterEnabled</i> öffnen .....	11
Abbildung 6: Wert auf 1 stellen .....	11
Abbildung 7: Wert <i>FilterEnabled</i> auf 1 gesetzt.....	12
Abbildung 8: Registrierungseinträge für eplogger.....	13
Abbildung 9: Pfad für Anlegen der Logdateien .....	15
Abbildung 10: Option im Sicherheitsdialog selektieren .....	15
Abbildung 11: Schlüssel eplogger anlegen .....	16
Abbildung 12: Registrierungseinträge für eplogger anlegen .....	16
Abbildung 13: Anwender anlegen .....	17
Abbildung 14: Gruppen von Anwender .....	19
Abbildung 15: Ort ändern aktivieren.....	20
Abbildung 16: Dialog Select User Location .....	21
Abbildung 17: Schema – Staatsbürger können Lizenzen benötigen .....	23
Abbildung 18: Schema – für Aufenthaltsort könnten Lizenzen benötigt werden .	24
Abbildung 19: Global Regular Types .....	25
Abbildung 20: Kontextmenü für Zugriffsrecht öffnen.....	26
Abbildung 21: Anwender hinzufügen .....	27
Abbildung 22: Recht für Anlegen eines Datenobjekts vergeben .....	28
Abbildung 23: Anwender hat das Recht Datenobjekt anzulegen – Beispiel Land	29
Abbildung 24: Kontextmenü auf Land öffnen .....	30
Abbildung 25: Eigenschaftsdialog für ein Land .....	31
Abbildung 26: Lizenz für Staatsbürgerschaft .....	32
Abbildung 27: Lizenz für Aufenthaltsort .....	33
Abbildung 28: Embargo Land.....	34
Abbildung 29: Anzeige von Verknüpfungen in der Listview - Länder.....	35
Abbildung 30: Kontextmenü Firma .....	36
Abbildung 31: Eigenschaftsdialog Firma .....	37
Abbildung 32: Kontextmenü auf Firma öffnen.....	38
Abbildung 33: Vertraulichkeitsstufen festlegen .....	39
Abbildung 34: Meldung höherer Security Level vorhanden .....	40



Abbildung 35: Kontextmenü Vertraulichkeitsstufe bearbeiten.....	41
Abbildung 36: Security Level für Anwender festlegen.....	42
Abbildung 37: Listview mit verknüpften Anwendern.....	43
Abbildung 38: Kontextmenü für Verträge .....	44
Abbildung 39: Eigenschaftsdialog Vertrag .....	45
Abbildung 40: Anzeige in der Listview für verknüpfte Datenobjekte - Verträge ..	46
Abbildung 41 Kontextmenü für Export Control Classification.....	47
Abbildung 42: Eigenschaftsdialog Export Control Classification (ECC).....	48
Abbildung 43: Anzeige für verknüpfte Datenobjekte in der Listview - ECC .....	50
Abbildung 44: Kontextmenü Export License .....	51
Abbildung 45: Eigenschaftsdialog Export Lizenz .....	52
Abbildung 46: Anzeige für verknüpfte Datenobjekte in der Listview - Exportlizenzen.....	53
Abbildung 47: Berechtigung für die Lizenz auswählen .....	54
Abbildung 48: Zugriffsrechte einzeln verwalten .....	55
Abbildung 49: Kontextmenü Zugriffsrechte öffnen .....	56
Abbildung 50. Dialog Rechte Datenobjekt .....	57
Abbildung 51: Auswahl Firmen .....	57
Abbildung 52: Auswahl Vertraulichkeitsstufen .....	58
Abbildung 53: Dialog Zugriffsrechte .....	58
Abbildung 54: Anzeige von Verknüpfungen in der Listview – PPR-Komponente	60
Abbildung 55: Tabelle 1 – Beschreibung Ausfuhrkontrolle aktiviert .....	61
Abbildung 56: Tabelle 2 – Beschreibung Security Level größer null.....	62
Abbildung 57: Tabelle 3 – Beschreibung <i>Citizen possibly needs a License</i> .....	63
Abbildung 58: Tabelle 3 – Beschreibung <i>Sojourn possibly needs a License</i> .....	64
Abbildung 59: Beispiel – Projektdaten Firma Engine .....	67
Abbildung 60: Vertrag anlegen.....	68
Abbildung 61: Verknüpfung Vertrag und Anwender .....	68
Abbildung 62: Verknüpfungen zwischen Vertrag und PPR-Komponenten herstellen.....	69
Abbildung 63: Zugriff durch Verknüpfung mit Vertrag erlaubt .....	69
Abbildung 64: Anlegen einer ECC .....	70
Abbildung 65: ECC mit Land verknüpfen .....	70
Abbildung 66: ECC mit Prozess verknüpfen .....	71
Abbildung 67: Zugriff verweigert .....	71
Abbildung 68: Anlegen einer Exportlizenz .....	72
Abbildung 69: Exportlizenz mit ECC verknüpfen .....	72
Abbildung 70: Exportlizenz mit Firma verknüpfen.....	73

---

Abbildung 71: Exportlizenz auf das Land ziehen .....	74
Abbildung 72: Staatsbürgerschaft selektieren.....	74
Abbildung 73: Zugriff mit Exportlizenz erlaubt.....	75
Abbildung 74: Vertraulichkeitsstufen für Firma festlegen .....	76
Abbildung 75: Kontextmenü auf Prozesskomponente öffnen .....	77
Abbildung 76: Security Level um eins erhöhen.....	78
Abbildung 77: Anwender hat keinen entsprechend hohen Security Level .....	78
Abbildung 78: Vertraulichkeitsstufen für Firma festlegen.....	79
Abbildung 79: Anwender mit Firma verknüpfen .....	80
Abbildung 80: Kontextmenü öffnen – <i>Edit Security Level</i> wählen.....	80
Abbildung 81: Security Level Anwender zuweisen .....	81
Abbildung 82: Zugriff auf Prozess P1 erlaubt – Beispiel 2 .....	82
Abbildung 83: Aufenthaltsort beim Anwender in der Benutzerverwaltung ändern	83
Abbildung 84: Aufenthaltsort für Deutschland aktivieren .....	84
Abbildung 85: ECC für Deutschland erweitert.....	85
Abbildung 86: ECC mit Deutschland verknüpfen .....	86
Abbildung 87: Exportlizenz mit Deutschland verknüpfen .....	86
Abbildung 88: Aufenthaltsort selektieren.....	87
Abbildung 89: Zugriff auf Prozesskomponente erlaubt .....	87

# Index

## Allgemeines

Aufenthaltort einblenden .....	20
Benutzerverwaltung .....	17
Datenobjekte einblenden .....	8
Datenobjekte Sicherheitsrichtlinien .....	6
Registrierungseditor .....	11
Übersicht über das Handbuch .....	3
Übersicht über Sicherheitsrichtlinien .....	5
Zeichen und Symbole .....	4

## Bedeutung von Lizenzen

Entscheidungstabellen für Exportlizenzen .....	61
--	----

## Export control classification

Allgemeines .....	47
Definition der Bedingungen .....	49
ECC anlegen .....	47
Verknüpfung zu anderen Datenobjekten .....	50

## Export Lizenzen

Allgemeines .....	51
Bedeutung von Export Lizenzen .....	52
Export Lizenzen anlegen .....	51
Verknüpfung zu anderen Datenobjekten .....	53

## Fallbeispiele

Ausgangssituation .....	66
Beispiel 1 .....	68
Beispiel 2 .....	76
Beispiel 3 .....	83
Voraussetzungen .....	65

## Firmen

Allgemeines .....	36
Firmen anlegen .....	36
Security Level festlegen .....	38

Verknüpfung zu anderen Datenobjekten .....	43
--	----

## Funktionsweise Gruppenfilter .....7

### Global Regular Types verwenden

Allgemein .....	25
Rechte für Anwender festlegen .....	26

## Länder

Allgemeines .....	30
Aufenthaltort .....	33
Exportbeschränkungen festlegen .....	32
Länder anlegen .....	30
Staatsbürgerschaft .....	32
Verknüpfung zu anderen Datenobjekten .....	35

## PPR-Komponenten

Allgemeines .....	59
Anzeigen der Datenobjekte .....	60

## Registrierungseinträge für Protokolldateien .....13

## Sicherheitsrichtlinien festlegen

Allgemeines .....	22
Übersicht Exportlizenzen .....	23

## Verträge

Allgemeines .....	44
Verknüpfungen zu anderen Datenobjekten .....	46
Verträge anlegen .....	44
Wirksamkeit von Verträgen .....	44

## Zugriffsrechte

Allgemeines .....	55
Exportbeschränkungen .....	58
Firmen .....	57
Vertraulichkeitsstufen .....	58
Zugriffsrechte bearbeiten .....	56