HOME

User Manual

DELMIA Process Engineer®

Security Guidelines

DELMIA

Foreword

This manual provides an introduction to the basic operations and functions of the Security Guidelines.

While developing these functions we have made every effort to create a clearly organized, easy-to-understand program structure.

A user-friendly interface as well as a clear menu guide will enable you to quickly learn how to operate the program and to get familiar with its functions so that you can carry out your planning tasks in a quick and reliable way.

No Liability or Guarantee

Our programs and manuals have been compiled with great care and to the best of our knowledge. They have also been tested in a production setting. However, we assume no liability and provide no guarantee that the software and related descriptions are free of error or are suitable for special purposes.

DELMIA assumes no liability for any damage that may arise from the use of this software. By using this software, the user acknowledges this exclusion from liability and shall hold DELMIA exempt from all claims.

Copyright

Modifications

Moreover, DELMIA retains the right to make modifications and improvements to the product described in this manual at any time without prior notification.

fails to meet the United States government's needs or is inconsistent in any respect with United States Federal law, the United States government agrees to return this software, unused, to DASSAULT SYSTÈMES. The following additional statement applies only to acquisitions governed by DFARS Subpart 227.4 (October 1988): "Restricted Rights – use, duplication, and disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(l)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252-227-7013 (Oct. 1988)."

Table of Contents

1. Introduction

This manual explains how to use the Process Engineer Security Guidelines for your planning purposes. It basically shows how to apply security guidelines to projects.

1.1 How to Use this Manual

This manual enables you to get familiar with the operation and functions of the Security Guidelines. This manual briefly describes:

- How to create and edit security guidelines.
- What you need to know about security guidelines.
- Creating the data objects in the system library.
- How data objects are used for the economical and efficient use of security guidelines.
- Sample cases about the basic application of security guidelines.

Note

When handling the Security Guidelines functions, please also refer to the general introduction to Process Engineer in the General Introduction Manual.

Click General Introduction to access the manual.

1.2 Documentation Conventions and Symbols

The symbols used in this manual are intended to provide you with keys to the contents in an immediately understandable manner.

This symbol is used to introduce key concepts that are covered in the sections immediately following this symbol. As a result, this symbol most frequently appears at the beginning of chapters or sections.

Note

This symbol is used to mark notes, which provide you with additional information you need to have for further work. You will either find the Note sign at the beginning of a chapter or in a particular text passage in the chapter. Texts bearing this sign are additionally marked with ***Note****. The text is always in italics.*

Caution

This symbol indicates that the text that follows describes particular circumstances that you must avoid to avoid potential errors with the operation of the

*program or harm to data. You will either find the Caution sign at the beginning of a chapter or near a particular text passage in the chapter. Texts that are introduced by this sign are additionally marked with **Caution**. The text is always in italics.*

Example This symbol marks examples which serve to illustrate a certain situation.

1 This symbol marks the individual operational steps involved in a particular operating instruction. Operating instructions describe operational steps, for example, how to open a menu or execute a function.

▪ This symbol marks listed subjects. The symbol for listed subjects can be either used to structure a continuous text or to list main subject keywords.

➢ This symbol marks list inside a bulleted or numbered list.

 This symbol marks cross reference information that is available in another manual.

1.3 New Functions in Security Guidelines

No new functionality has been added for this release.

2. Overview

The present rights concept is as of version PE R16 supplemented by new security guidelines that can be used in addition to the existing rights concept.

The security guidelines are used to regulate the propriety of objects, the confidentiality of information, and the access to data as they must be fulfilled in accordance with the legal export stipulations of the countries in question.

These security guidelines may refer to companies, countries, and users.

You can do the following to ensure that PPR components in projects are accessed in accordance with the security guidelines:

- Continue to assign rights to objects and plantypes to individual users or groups.
- Set additional security standards for companies by defining security levels and regulating external access to company-specific data by contract.
- Additionally regulate legal stipulations by determining which data are subject to export stipulations, for which countries export licenses are required, and which companies are to be granted export licenses.

Security levels defined for an object or its children can be displayed in the PPR-Navigator and can be used for print-outs.

For further information, *please refer to the* Settings Manual.

Objects subject to these security settings are filtered out internally via the server. In this way the access to PPR components is regulated for users and groups of users. After the filtering, access to objects is either permitted or not permitted to the user.

Users and groups of users are created in the user management, and they must be provided with the appropriate function permissions and access rights to PPR components.

2.1 Data Objects

Before you can assign the security settings to the PPR components, the following data objects must be created in the system library:

Company, contracts/agreements, countries, export restrictions, and export authorizations.

The permissible security levels are assigned individually for every company.

With the specific access rights to a PPR component you can set which company owns this object and to which security level this object is assigned.

Users have access to these PPR components only if they have a corresponding security level and are either employees of the respective company or are authorized by contract to access objects of this company.

PPR components of which the information is subject to legal export stipulations can be marked as such, and export restrictions can be assigned to them. Access to data to which export restrictions have been assigned is granted to a user only if the user's company has a corresponding export authorization in compliance with the export restrictions.

The linked objects between export restrictions, export authorizations, countries, and companies as well as between contracts and users or groups of users are set in the system library by the administrator or an employee with similar rights.

In order for the defined security settings to take effect on PPR components, you must create the linked objects to contracts or export restrictions individually for every PPR component.

The security settings can be used for all three planning views of the PPR-Navigator:

- Product view
- Process view
- Resource view

2.2 Displaying Data Objects

Data objects are directories that must exist in the system library in order for the security measures to be applied. You must make the following settings in order to work with the security guidelines. You can not apply the security guidelines without these settings.

- You must use the **Configuration tool** to display the data objects for the security guidelines in the system library.
- You must also set a value in the **Registry editor** that permits the application of the security guidelines.

Note

These settings should generally be executed only by an administrator or an employee with comparable rights.

2.2.1 Displaying Data Objects via Configuration Tool

You can use data objects, such as contracts, licenses, or countries to administer the security guidelines and set the corresponding relations between these data objects. *Please refer to the* Figure 3.

1) Open the context menu.
2) Select **Tools/Database Tools/Configuration Tool.**

Figure 1: Open the Configuration Tool

3) Select **Find** in the context menu. You must select **archivroot** for a different type of sorting from that shown in the image.

4) Under securitydatafolder:…/ select ergoexplorer-libray.

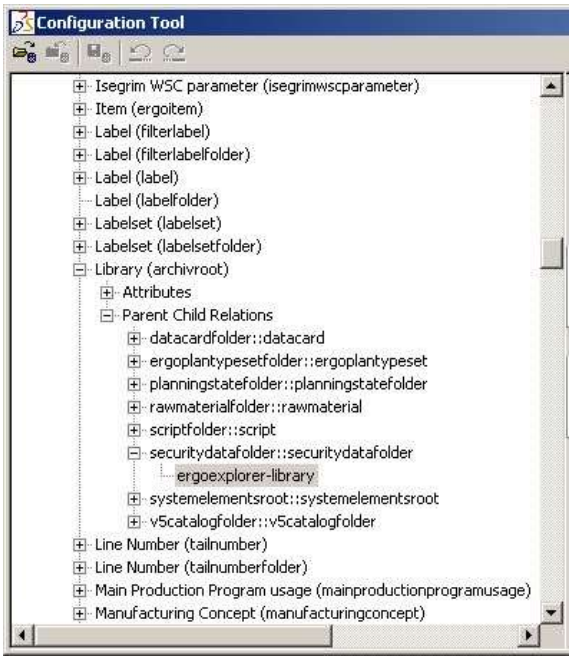


Figure 2: Open the Library in the Configuration Tool

5) Select **ergoexplorer-libray** and switch to the properties in the window.

6) In order to display the data objects in the system library, set **Yes** for the tree view. *Please refer to the* Figure 4.

Figure 3: Data Objects of the Security Guidelines Displayed in the System Library

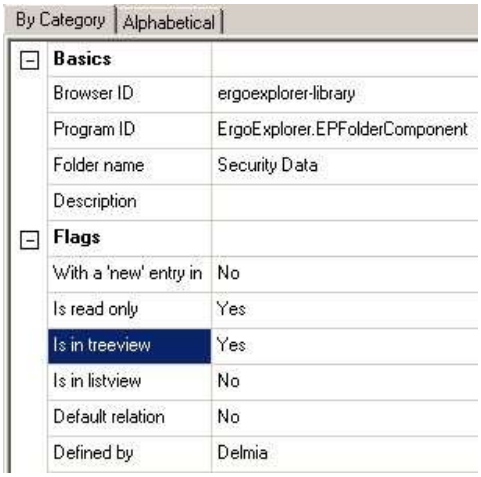


Figure 4: Displaying Data Objects

2.2.2 Displaying Data Objects via Registry

You must set the value for **FilterEnabled** to **one** in the registry editor so that the security guidelines can be applied. The value is set to **zero** in the standard configuration.

1) In the registry editor select **HKEY_LOCAL_MACHINE/SOFTWARE/DELMIA/IPDSERVER/SECURITY**.
2) Select **Filter**.
3) Select **FilterEnabled** in the list view.
4) In order to change the value: Open the context menu and select **Modify**.

Figure 5: Open the Context Menu on FilterEnabled

5) Enter the value 1 in the dialog **Edit String Value**. Confirm the selection with **OK**.

Figure 6: Set the Value to 1

The security guidelines take effect after the value has been set to one. The new value is displayed in the listview at **FilterEnabled**.

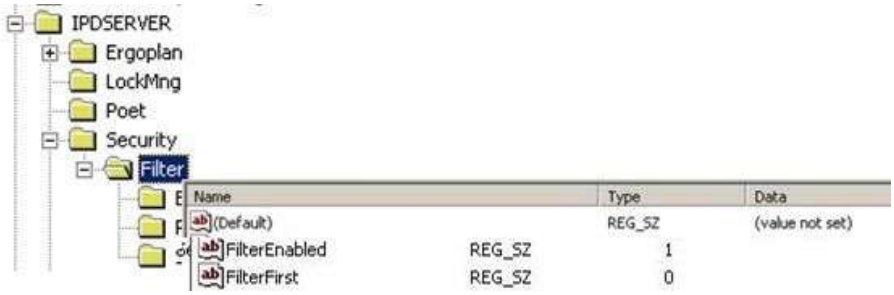


Figure 7: The value FilterEnabled is set to 1

2.2.3 Creating Users in the User Management

Additional entries on citizenship, residence, and company affiliation must be made for users who are to be granted access to your data. This is necessary for the **complete application of the** security guidelines that are described below.

Users and groups of users are set in the user management. The existing rights concept has also been extended for this case. Additional information on the user management and rights can be found in the Administration Manual.

2.2.3.1 Creating Users

The user has **superuser rights** in the example. An administrator with superuser rights is not subject to any restrictions. You must assign rights as usual on PPR components for users who do not have superuser rights (which is generally the case); these rights include, for example, the changing, reading, and writing of data. *Please refer to the* Using Countries and Using Companies.

The following additional information is required for users:

- Citizenship, location, and company. This additional information must be entered fully.
- The user management is opened via **Tools/Database Tools/User Management**.

Figure 8: Creating Users

Citizenship

Enter the citizenship of the respective user here. The citizenship of a user plays an important role in accessing data that are subject to an export restriction. The citizenship influences the assignment of export licenses.

Location

Enter the residence of a user here. The residence and the citizenship do not need to be identical. The residence of a user also plays an important role in accessing data that are subject to an export restriction. The residence influences the assignment of export licenses.

Company

Enter the company for which the user works here. If you do not enter the company for which the user works and this user is not assigned to a group that is identifiable by company, this user will not be able to access PPR components despite having been granted the right to do so by contract with the user's company. This also applies to groups of users of a company.

Note

For those without superuser rights. In order to link the user to contracts or to set security levels for the user, the function permission "useradm/edit user and groups" must be granted.

2.2.3.2 Creating Groups

When creating groups, additional information on the company must be supplied - in the example, a group for the company **Engine** is shown. You generally form a group of users whenever you combine several users to a group belonging to a company that has been granted access to your data.

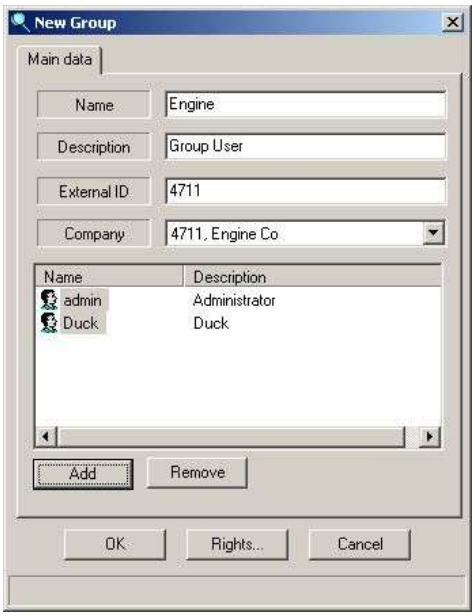


Figure 9: Groups of Users

Note

In order to link the user to contracts, the function permission "useradm/edit user and groups" must granted.

2.2.4 Display Location during Registration

When registering the Process Engineer you can open the dialog **Select User Location**. The dialog shows all of the countries stored in the system library. When creating a user, the location of residence is specified, and this location is automatically selected when opening the dialog.

This dialog is always available to users with superuser rights. A change of residence location does not affect the export stipulations for these users.

In the dialog you can assign another location to the user by selecting another country. A change of location is implemented directly in the properties dialog of the user in the user management.

If you change the location of a user in the registration, this takes effect on the export stipulations and export licenses.

1) In order to display the dialog, open the user management and activate the function permission **change location** for the user.

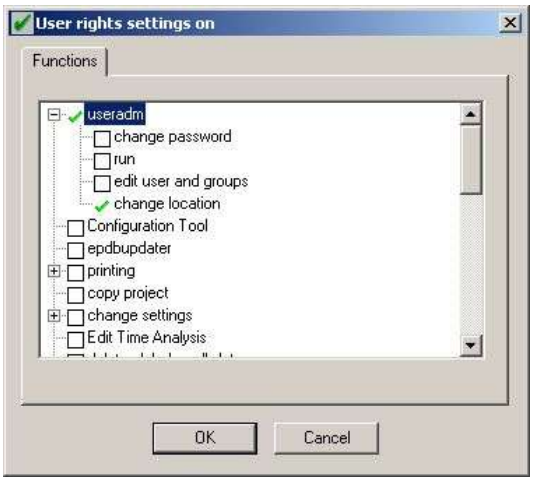


Figure 10: Activate Change Location

2) Every country that has been created is displayed in the dialog. You can change the location by selecting a country.

Figure 11: Select User Location Dialog

3. Setting Security Guidelines

Access to your PPR components in projects by external companies is regulated by use of the security guidelines. The decision as to which security guidelines are to be valid for PPR components is made on the basis of the following operational definitions of the security guidelines. These security guideline settings can be made in the system library. How to display the directory *Security Data* can be read about in Displaying Data Objects.

Note

These settings should generally be executed only by an administrator or an employee with comparable rights.You can assign an additional functional permission to employees whoc do not have these rights.

- In the following, the additional right one must have to edit the data objects described in the following are listed for every single data object.

In the chapter you will learn the basics about editing data objects:

- Countries: *Please refer to the* Using Countries.
- Companies: *Please refer to the* Using Companies.
- Contracts/agreements: *Please refer to the* Contracts – using Agreements.
- Export control classification (ECC): *Please refer to the* Use Export Control Classification.
- Export licenses: *Please refer to the* Using Export Licenses.
- Access rights to PPR components: Using Access Rights to PPR Components.
- *Please refer to the*: Sample Cases for Security Guidelines.

Note

Assign function permissions to users via the user management.

3.1 Overview of Export Licenses

Scenario – citizen of a country could require an export license.

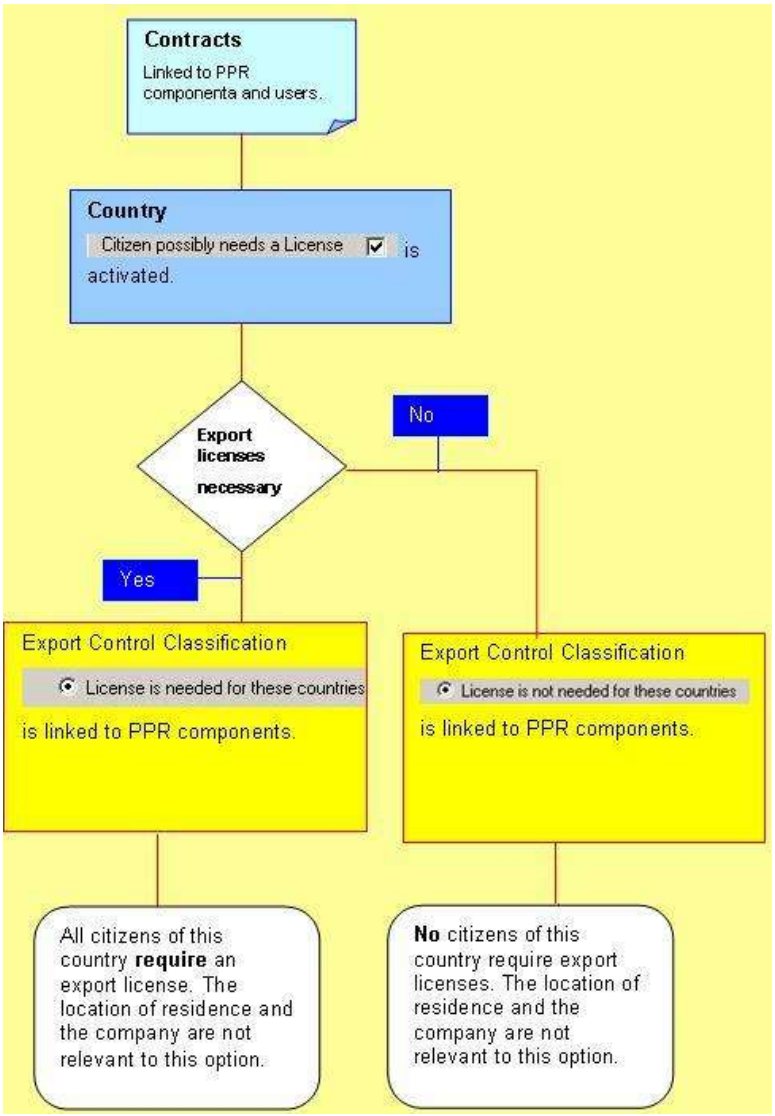


Figure 12: Scenario – Citizens could Require Licenses

Scenario – for the residence location in a country an export license could be required.

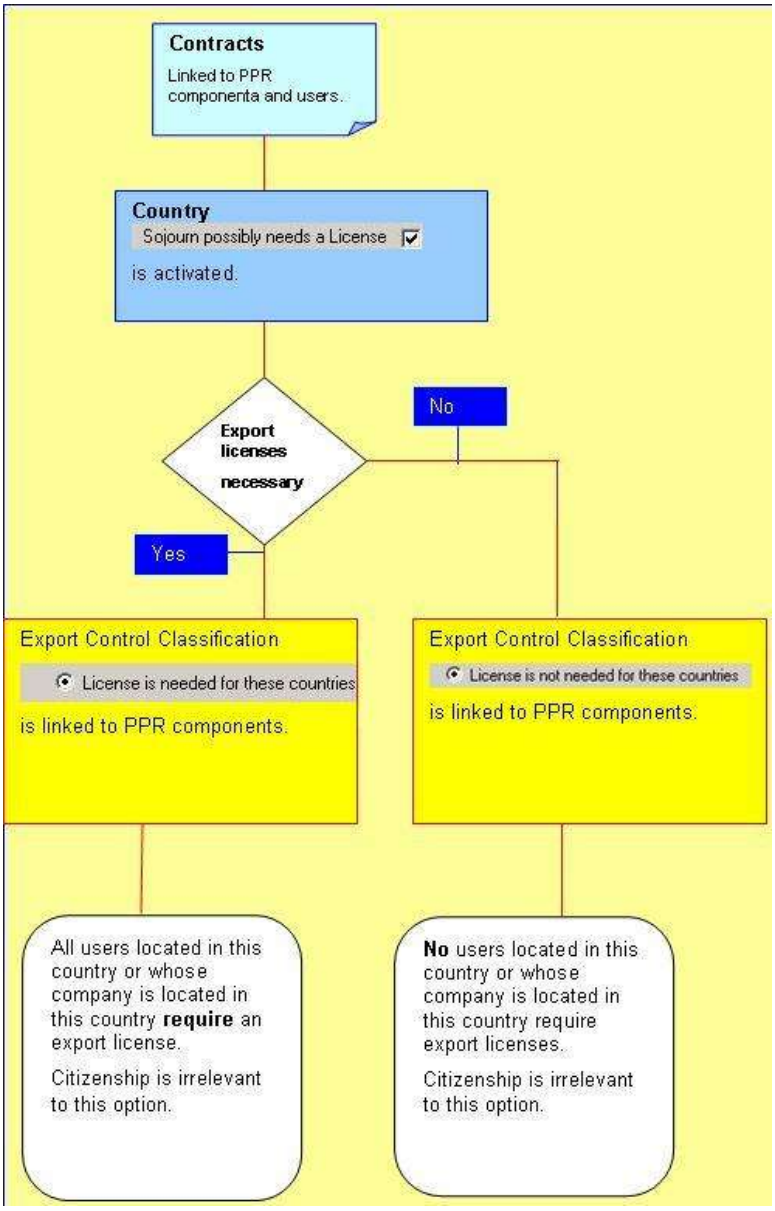


Figure 13: Scenario – Licenses could be Required for the Residence Location

3.2 Using Countries

Here you can create countries subject to export restrictions and for which valid export licenses must exist as data objects. The permission for a country is regulated in part by valid export licenses. It is also determined by export restrictions that you set for every country in the Export Control Classification (ECC).

- Users who have no superuser rights and who may create a country must also be granted the function permission **create objects/country**. In order to be able to edit the object you need the object right "Change". In order to be able to assign the object, the object right "read" must be granted.

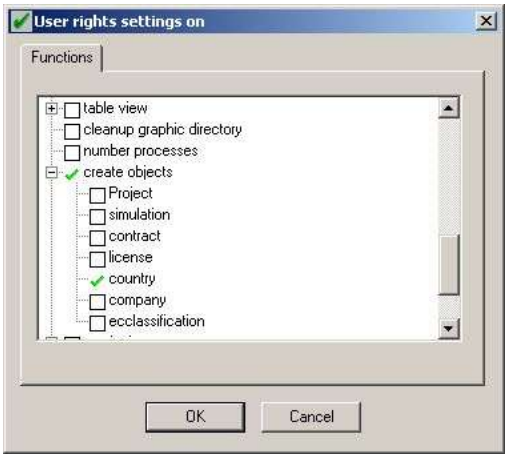


Figure 14: Assign the Function Permission to the countrY

3.2.1 Create Country

1) Open **Security Data** in the system library.
2) Open the context menu for **Countries**.
3) Select **New/Page.**

Figure 15: Open the Country on the Plantype Set

You can set export restrictions for every land that you create:

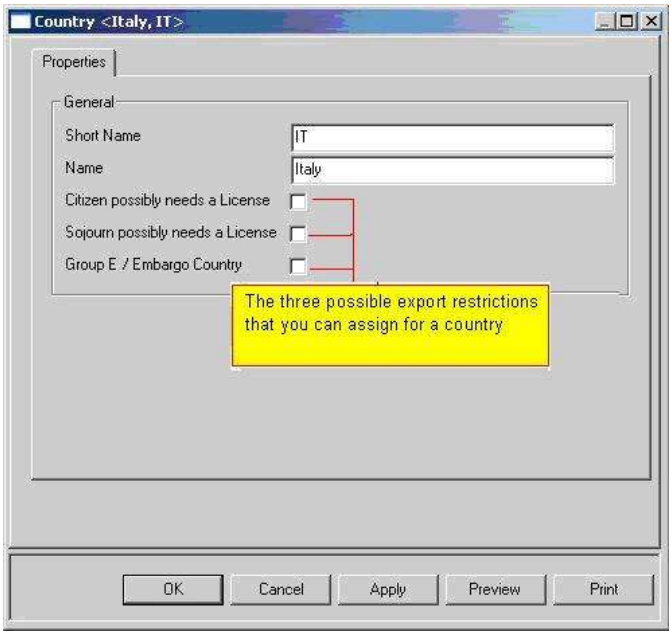


Figure 16: Properties Dialog for a Country

3.2.1.1 Setting Export Restrictions for a Country

You can define different export restrictions for every country.

In principle the access of the data, which export restrictions are subject, is regulated only with ECC if at the associated country the appropriate option is activated.

If the appropriate option at this country is **not** activated, users from external companies will have access to your PPR components if both the user as well as the PPR components is linked to a contract, regardless of whether the PPR components are subject to export restrictions. In this example, neither export licenses nor Export Control Classifications are required for these countries.

Only if you use these options do you require Export Control Classifications and export licenses for your data.

The decision as to whether export licenses are required is thus made individually for the countries. The individual countries for which export licenses are actually required is set in the ECC. These options are necessary in order to limit access to your data.

- Countries marked as embargo countries have no access to your data, and they therefore do not require export licenses.

The export restrictions can also be combined. If you activate both export restrictions - *Citizen possibly needs a license* and *Sojourn possibly needs a license* – then both conditions apply to any possible export licenses.

If you use both of the options, the ECC linked to the PPR components is in a technical sense checked, and an export license could be required or not required, depending on the ECC settings.

3.2.1.2 Citizenship of a Country

If you activate **Citizen possibly needs a License,** all users that are citizens of this country may need an export license. Whether an export license is required is set in the ECC, which must be linked to a PPR component.

Figure 17: License for Citizenship

Example

If, for example, it is set in the ECC that no export license is required for a given country and **Citizen possibly needs a License** is activated, users that are **citizens** of this country **do not** require an export license.

- **Borderline case:** If the location of the company or the user is in another country and *Sojourn possibly needs a License is* activated for this country, the user requires an export license for this country.

The corollary of this means, If, for example, it is set in the ECC that an export license is required for a given country and *Citizen possibly needs a License* is activated, users that are **citizens** of this country **require** an export license.

- **Borderline Case:** If the location of the company or the location of the user is in another country and *Sojourn possibly needs a License is* activated for this country, the user requires an export license for this country.

3.2.1.3 Location for a Country

If you activate *Sojourn possibly needs a License,* all users whose location is in this country may possibly require an export license. Whether an export license is required is set in the ECC, which must be linked to a PPR component.

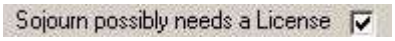


Figure 18: License for Location

Example

If, for example, it was set in the ECC that no export license is required for this country and *Sojourn possibly needs a License* is activated, users whose **residence location or company location** is in this country **do not** require an export license, since it was set in the ECC that no export license is required for this case.

The corollary of this means, If, for example, it is set in the ECC that an export license is required for a given country and *Sojourn possibly needs a License* is activated, users that whose **residence location or company location** is in this country **require** an export license.

Exclusion of a country

If you activate *Group E/Embargo Country*, all users who are citizens of this country or whose residence location is in this country have no access to your confidential data – i.e. to the PPR components already subject to an export restriction. This exclusion can be trumped by an export license.

Figure 19: Embargo Country

Example

If you activate this option for a country you need not activate the other two export restrictions.

The decision as to which countries are marked as embargo countries could be determined, for example, by political decisions. From the perspective of the USA these would include such countries as Iraq, Cuba, and North Korea.

3.2.1.4 Links to other Data Objects

A country can be linked to any number of export licenses and Export Control Classifications.

The possible links to other data objects of the system library are displayed in the list view:

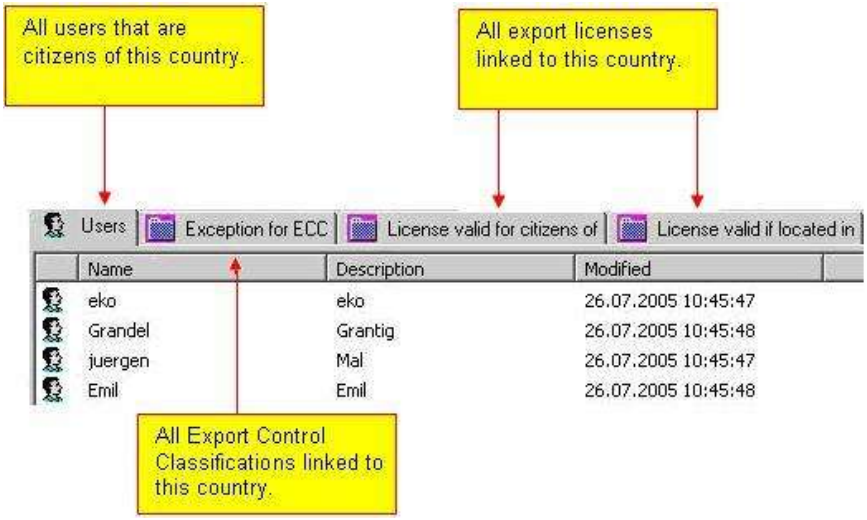


Figure 20: Display of Links in the List View - Countries

3.3 Using Companies

External companies with which you have signed contracts and who are to receive export licenses are created as data objects here.

You can set security levels for every individual company (external company and your own company). You need security levels for external companies only if these can create new PPR components in your projects or own there. The new PPR components are properties of the company allocated to the user who created the new PPR components. In addition, corresponding security levels may apply.

In order to permit user and group access to your data, they are linked to your company – this means that you must create a data object for your company in System library.

After linking the external company to your company – in a technical sense the link is made between the user of the external company to your company – you transfer to this user the security level (security level) that permits access to your PPR components.

- Users who have no superuser rights and who may create a company must also be granted the function permission *create objects/company*. In order to be able to edit the object you need the object right "Change". In order to be able to assign the object, the object right "read" must be granted.

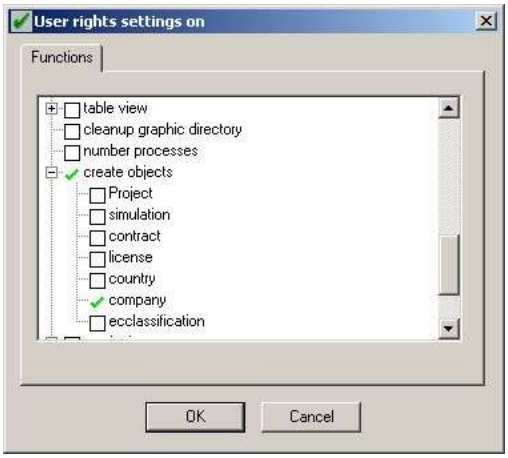


Figure 21: Function Permission "Assign Company"

3.3.1 Create Company

1) Open **Security Data** in the system library.
2) Open the context menu for **Companies**.
3) Select **New/Company**.

Figure 22: Company Context Menu

In the following examples, the company referred to as *Engine Co* is meant to represent your company.

All of the fields can be written to free of restrictions. The important point is that you assign the country in which the company is based to the company. If no country is specified for the company, access to the data of yours that is subject to export restrictions is denied. The company could be located in a country that is marked as an embargo country, to which access to such data is generally prohibited.

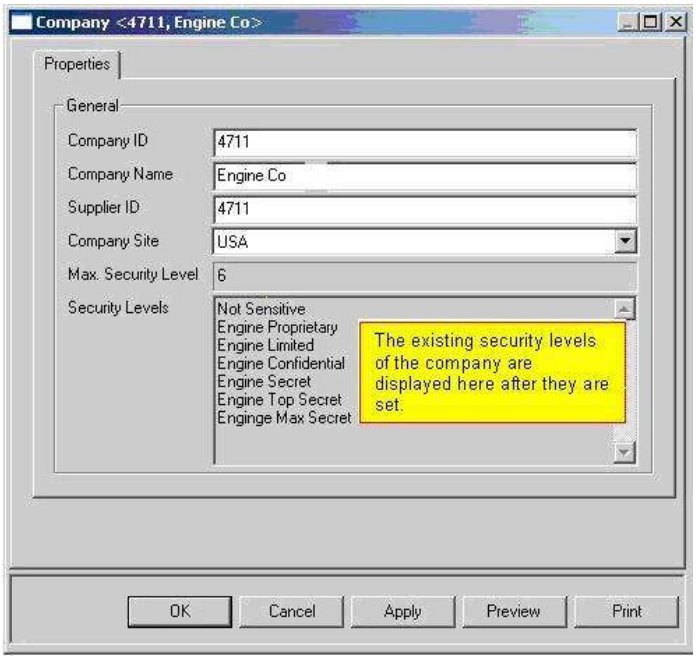


Figure 23: Company Properties Dialog

3.3.1.1 Set security Levels for the Company

You can create a maximum of nine security levels for a company.

1) Open the context menu for company in the system library. In the example, the company representing your company is *Engine Co*.

- The procedure for setting a security level as described here is identical for all companies. Since the access to data takes places via your defined security level, the procedure is explained in the example featuring the company Engine Co.

Figure 24: Open the Context Menu for Company

2) Set the security levels, of which a maximum of nine are possible. Set the valid value in the field Maximal Security Level – for the company Engine there should be a maximum of six possible security levels.

- These defined security levels are available for your PPR components, which can be assigned individually for every PPR component. In the standard configuration every PPR component has a security level of zero.

- In the example, all of the PPR components could have a maximum value of six. Each PPR component can receive a different value. *Please refer to the* Creating links – Example 2.

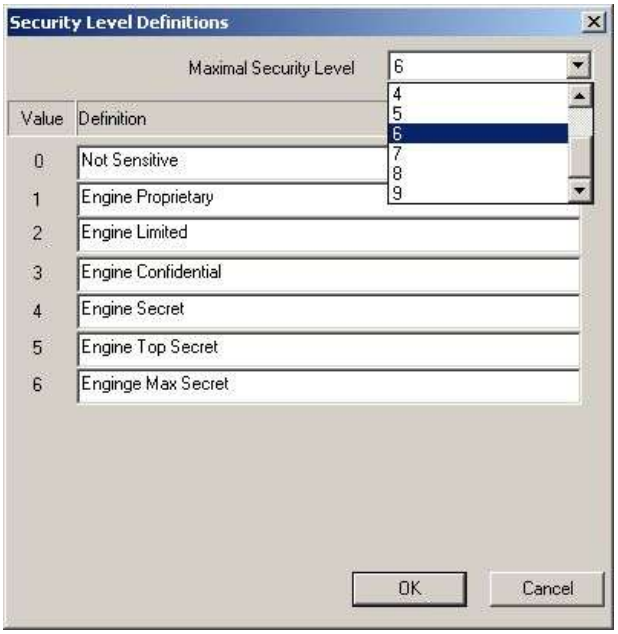


Figure 25: Set Security Levels

Note

Only the security levels up to the maximum security level are avaialble for selection. Only these security levels are displayed.

Changing Security Level

Security levels can be changed. Whenever you lower the maximum security level and the security levels for your PPR components have already been assigned, ensure that the new maximum security level is identical or higher than that assigned to a PPR component.

- If security levels of a higher value are available for PPR components, they must be changed for every PPR component.
- The same applies to users assigned to this company as well as those who have a higher security level.

This message refers to this fact:

Figure 26: Message that a Higher Security Level is Available

3.3.1.2 Set security Levels for Users

You can transfer one of the security levels you previously set to every user. All of the defined security levels are available for selection. Access should be permitted up to the assigned security level. If a user can not access certain PPR components, you can limit the security level of the user to this value.

1) Link users to your company per drag and drop.

Note

In addition you also need the function permission "useradm/edit user and groups".

- All linked users are displayed in the listview of the selected company under the tab Security Levels. In the standard configuration the assignment of security levels for the user is set to zero – this means that the user has no access to security-relevant data.

2) Select the user and open the context menu.

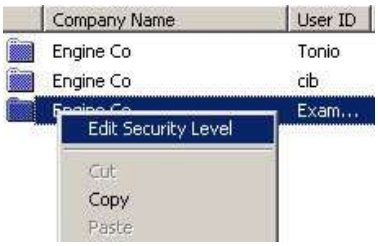


Figure 27: Edit Security Level Context Menu

3) Set the security level for the user here. All security levels defined for the company are available for selection – i.e. in order to remain consistent with the example, the security levels of your company, Firma Engine Co.

- If users of your own company who do not have superuser rights should have access to the data of your company, you can define the security levels for these users here as well. These users must also be linked to your company like users of an external company.

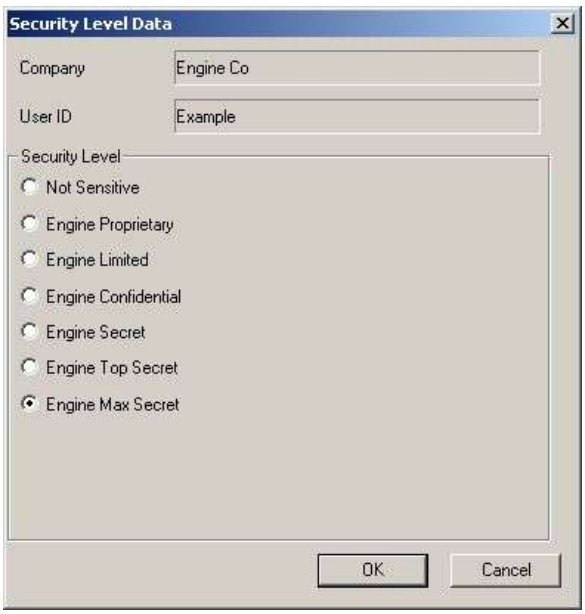


Figure 28: Set Security Level for Users

3.3.1.3 Links to other Data Objects

You can link a company to an unlimited number of users and export licenses.

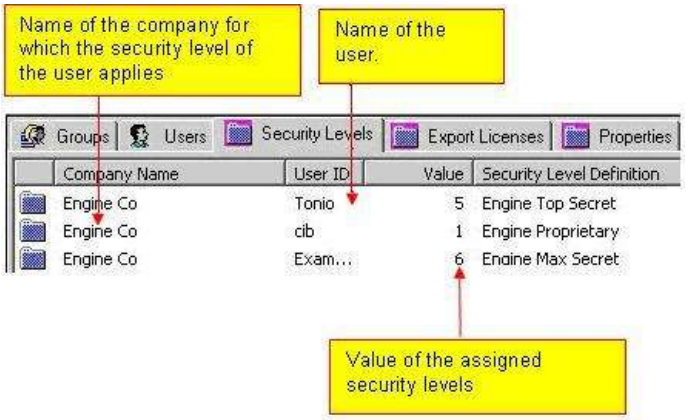


Figure 29: Listview with Linked Users

3.4 Contracts – using Agreements

A contract between your company and external companies is signed so that access to your data can be regulated.

The basis on which further steps are based is set in the contract. A company has no access to your data without a valid contract.

The contracts establish which companies are to be granted rights to access the confidential data of your company.

Effectiveness of Contracts

- A contract is effective only if you have assigned the contract to the users of the company for which a contract has been signed. Technically speaking this means nothing more than that you have linked contracts with users or groups of users of a company accordingly in the system library.
- Furthermore, a contract takes effect on your confidential data only after you have linked the contract to PPR components in the project, for the object, and its children.
- A contract must be linked individually to every PPR component so that a basic permission to access your data is available at all.

➢ Users who have no superuser rights and who may create contracts must also be granted the function permission create objects/contract. In order to be able to edit the object you need the object right "Change". In order to be able to assign the object, the object right "read" must be granted.

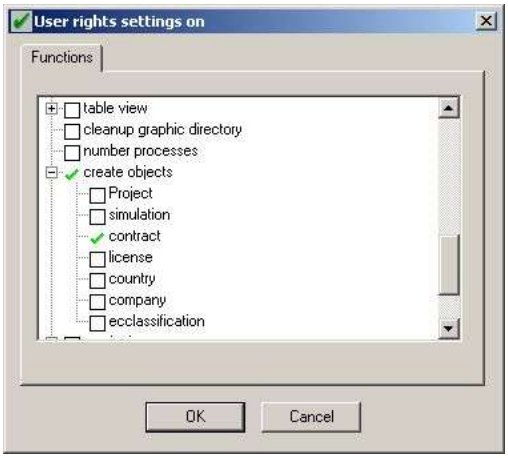


Figure 30: Assign Contract Function Permission

3.4.1 Creating Contracts

1) Open **Security Data** in the system library.
2) Open the context menu for **Contracts/Shared Access Agreements**.
3) Select **New/Contract/Shared Access**.

Figure 31: Context Menu for Contracts

4) Set the subject of the contract in the properties dialog. All field of the properties dialog can be written to free of restrictions.

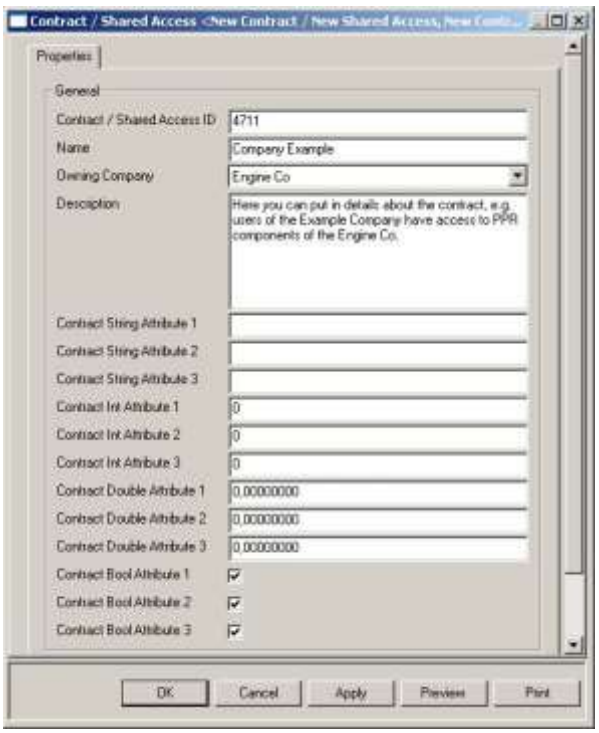


Figure 32: Contract Properties Dialog

Links to other Data Objects

- You can link a contract to an unlimited number of users, groups of users, and PPR components.
- Link contracts to users or groups of users from external companies who are to be granted access to your data.
- These users and groups are linked to your company; the contract is technically valid as of this point.
- After the linking of the user to your company, the security level that permits access to your data can be transfered to this user.

The possible links to other data objects of the system library are displayed in the list view:

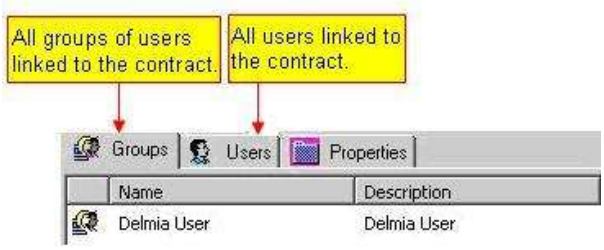


Figure 33: Display in the Listview of Linked Data Objects - Contracts

3.5 Use Export Control Classification

With the Export Control Classification you can define which countries require export licenses and for which countries **no** export licenses are required.

The use of export licenses is furthermore dependent on which form of regulation was decided upon for the country itself. If regulations overlap, the regulation concerning export licenses for a country is considered decisive in a legal sense. In this case, the form of regulating export licenses as set for the country applies. *Please refer to the* Using Countries and Sample Cases for Security Guidelines.

In the *Export control classification* you can set whether the confidential data of the marked PPR components are subject to either the stipulations of the ***International Traffic in Arms Regulations (ITAR)*** or the ***Export Administration Regulations (EAR)***. One of the two fields is always active.

- Users who have no superuser rights and who may create, edit, and assign an export control classification must be additionally granted the function permission *create objects/ecclassification*. In order to be able to edit the object you need the object right "Change". In order to be allowed to assign the object, the object right "read" (assignment to export license and PPR components) or the object rights "Change" and "Add Child" (allocation to countries) must be granted, depending on the assignment operation.

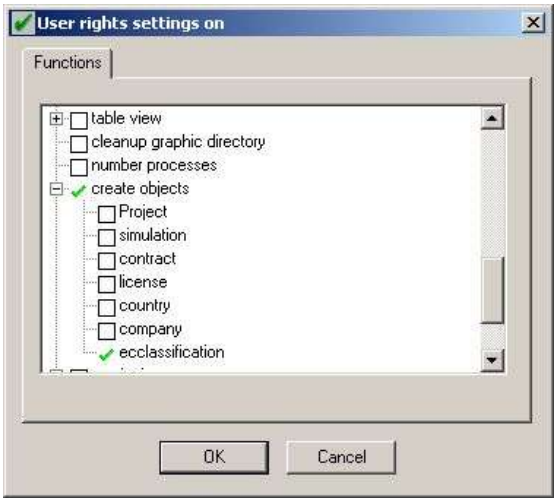


Figure 34: Function Permission assign Ecclassification

3.5.1 Creating Export Control Classification

1) Open **Security Data** in the system library.
2) Open the context menu for **Export Control Classifications**.
3) Select **New/Export Control Classification**.

Figure 1: Context Menu for Export Control Classification

Set the data in the properties dialog, *Please refer to the* Meaning of the Fields for Export Control Classification

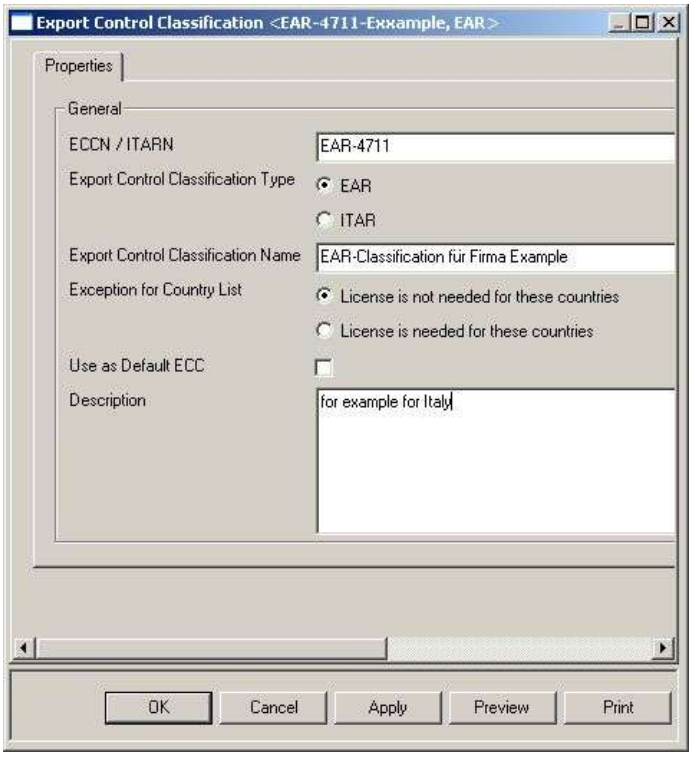


Figure 35: Export Control Classification Properties Dialog

3.5.1.1 Meaning of the Fields for Export Control Classification

ECCN/ITARN

This field is generally free for writing to – for example, you can clearly identify the export classification with the help of the classifications type and a unique number assignment – such as in example EAR 4711.

Export Control Classification Type

With the help of EAR or ITAR you can set the stipulations that apply to the Export Control Classification. You should take this setting into account when linking to export licenses.

Export Control Classification Name

This field is generally free for writing to. Here you can enter the name.

Exception for Country List

One of the two fields is always active.

- If **License is not needed for these countries** is active, the following conditions apply: all countries that have been assigned this ECC require **no** license. The corollary of this is that all countries not linked to this ECC require an export license.
- If **License is needed for these countries** is active, the following conditions apply: all countries that have been assigned this ECC **require** a license. The corollary of this is that countries that are not linked to this ECC do not require an export license.

➢ License stipulations set for a country, such as licenses for citizenship or residence location, could nullify the ECC regulations for certain users.

Use as Default ECC

If you are certain that the Export Control Classification should be valid for all PPR – components, activate the field *Use as Default ECC.*

If *Use as Default ECC is active* all newly created PPR components are automatically linked to this Export Control Classification.

Description
This field is free to be written to and it is of a purely informative character. However, it is sensible to use this field so you can enter which countries require export licenses.

3.5.1.2 Links to other Data Objects

An Export Control Classification can be linked to an unlimited number of countries, licenses, and PPR components.

- A PPR component is already subject to export restrictions if the PPR component is linked to an *Export control classification*. The definition set in the ECC as to which countries require an export license applies for this PPR component.
- An Export Control Classification must be linked individually with every PPR component. When linking pay attention to the hierarchical tree structure in the PPR-Navigator – if, for example, a user has no access to a parent node by assignment of an ECC, the children of this parent object will not be shown in the tree.
- An Export Control Classification is linked to the country for which the export licenses are required. The countries for which export licenses are required is defined in the linked ECC.
- By linking the Export Control Classification (ECC) to an export license you set which ECC is valid for the export license. You must then link the export licenses to countries in accordance with the definition in the ECC.

The possible links to other data objects of the system library are displayed in the list view:

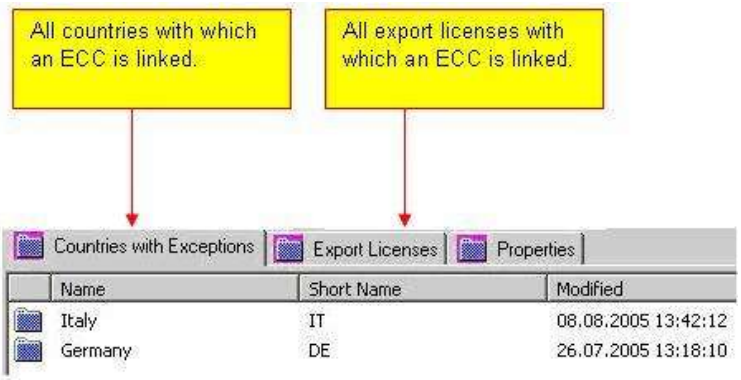


Figure 36: Display of Linked Data Objects in the Listview - ECC

3.6 Using Export Licenses

An export license is used to determine which countries, companies, and users are to be granted an export license.

Users who have no superuser rights and who may create an export license must also be granted the function permission *create objects/license*. In order to be able to edit the object you need the object right "Change". In order to be

able to assign the object, the object rights "Change" and "Add Child" must be granted.

Figure 37: Function Permission assign License

3.6.1 Creating Export License

1) Open **Security Data** in the system library.
2) Open the context menu for **Export Licenses**.
3) Select **New/Group**.

Figure 38: Context menu Export License

4) Export license data, *Please refer to the* Meaning of the Fields for Export.

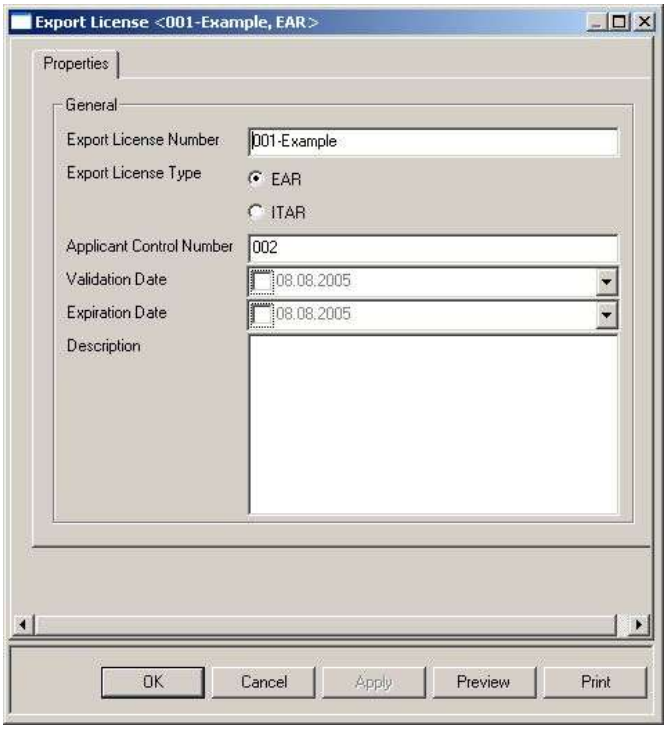


Figure 39: Export License Properties Dialog

3.6.1.1 Meaning of the Fields for Export

All of the fields in the properties dialog are free to be written to. You must make entries for the fields *Export License Number* and *Application Control Number* - it is recommended to mark the export license unambiguously by using these two fields.

With the help of EAR or ITAR you can set the stipulations that apply to the export license. The setting made should be taken into account when linking to an Export Control Classification.

The two fields effectivities and description are of an informative character only. It might be helpful to list the companies which are to receive an export license under description.

3.6.1.2 Links to other Data Objects

You can link an export license to an unlimited number of countries, companies, and Export Control Classifications.

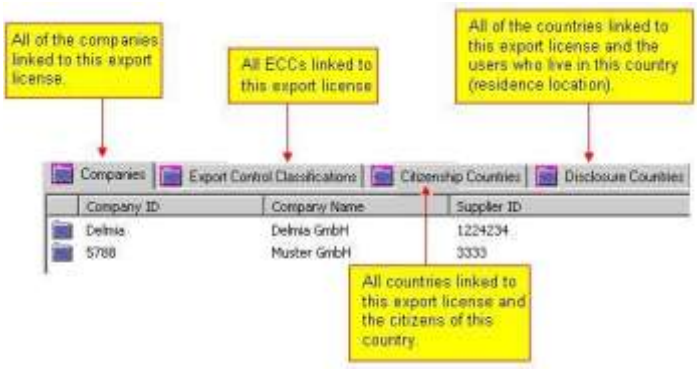


Figure 40: Display of Linked Data Objects in the Listview - Export Licenses

3.6.1.3 Linking Export Licenses with Countries

When linking export licenses with a country you must distinguish between the following:

- Whether a license is required for users who are citizens of this country.
- Or whether an export license is required for users whose residence is located in this country.

This decision is necessary if one or both of the export restrictions are active for a country. *Please refer to the* Setting Export Restrictions for a Country.

1) Select *License valid for citizens of* if citizens of this country require an export license.
2) Select *License valid if located in* if users who have a residence in this country also require an export license.
3) If both export restrictions apply to a country, you must create both license authorizations for these users - i.e. assign the license twice with the corresponding selected authorization.

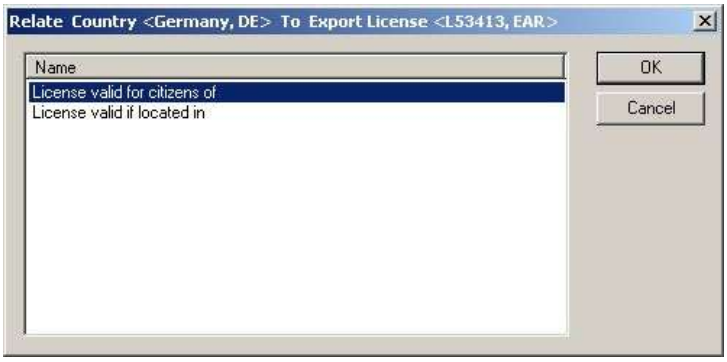


Figure 41: Select Access Right for the License

3.7 Using Access Rights to PPR Components

Every PPR component is to be seen as an independent object that must be administered individually as concerns the security guidelines in a legal sense.

By using access rights to PPR components you can regulate:

- Which company is the owner of the PPR component
- Which security level applies to the PPR component
- Whether the PPR component is subject to export restrictions without an Export Control Classification being allocated to this PPR component.

The value of the security level is set to zero in the standard configuration. Access to your data is regulated by the use of the security guidelines. According to this definition you are usually the owner of the PPR component.

If a company is allowed to edit the access rights to their objects, property rights can be transferred to this company on PPR components – this is precisely the case when employees from external companies create new PPR – components. In this case you are the external company for these PPR components and you would have to arrange contractual stipulations with this company that permit access to these PPR components.

Please note here as well: The company *Engine Co.* is meant to refer to your company.

Figure 42: Administering Access Rights Individually

Note

Users who can be granted rights can be assigned to the PPR components via corresponding access rights – such as in the example, the user Example of an external company has the right to write.

Users from external companies are subject to the stipulations of the security guidelines; only if these are fulfilled can the user make use of the granted access right.

How access rights are assigned is determined based on the present rights concept.

How to assign access rights is discussed in the Administration Manual.

3.7.1 Edit Access Rights

You must edit the access rights for every PPR component individually.

1) Open the context menu to a selected PPR component.

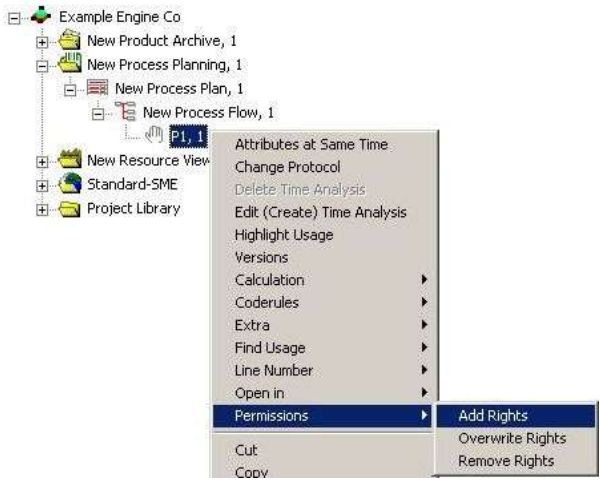


Figure 43: Open Context Menu Access Rights

In the dialog Edit Rights you can take the measures described in the following. The owner, *admin* in the example, plays no role in the application of security guidelines.

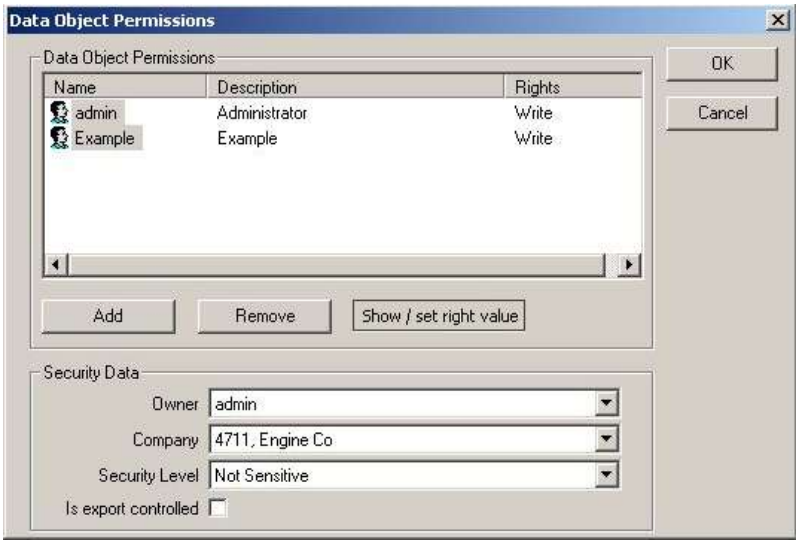


Figure 44. Data Object Permissions Dialog

The three fields **Company**, **Security Level** and **Is export controlled** are of particular importance for the application of the security guidelines.

3.7.1.1 Company

If the creator of the PPR components is assigned to a company, this company is shown automatically. As a rule this is the creator of your company, i.e. in the example the administrator or an employee of your company who has the corresponding rights.

PPR components can be assigned to another company using the combobox. All created companies are available for selection in the combobox, even your own company – in the example, Engine Co.

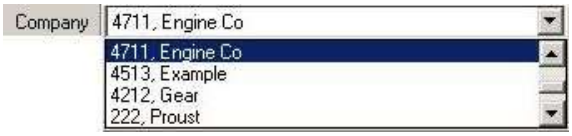


Figure 45: Select Companies

3.7.1.2 Security Level

Set the security level that is to be legally valid for your PPR components.

The security levels are available only if you have previously set them for a company. All of the security levels are then available for the corresponding company; you can make a selection among them in the combobox.

If no security level was set for the PPR components, *Not Sensitive* is always set; this corresponds to a security level of zero. Access to your PPR components is regulated on the basis of the set security level. In order to be permitted access, a user must have a security level that corresponds to or supercedes the valid regulations of the export stipulations – such as contract, ECC, or export license.

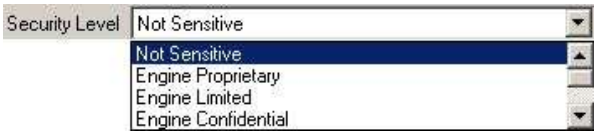


Figure 46: Security Level Selection

3.7.1.3 Is Export Controlled

Is export controlled serves to define whether the PPR component for users is already subject to an export restriction, regardless of whether the PPR component has been linked to an ECC.

If this field is active for an object, all users with corresponding project rights can access the object, provided they have not been explicitly excluded.

Figure 47: Access Rights dialog

Exclusion Criteria

- The user is a citizen of a country marked as *Embargo Country*.
- The user does not have a high enough security level (*Security Level)*.
- The user is an employee of another company that has not signed a corresponding contract that would grant access to these PPR components.

3.8 Linking PPR Components to other Data Objects

You can link a PPR component to an unlimited number of different contracts and Export Control Classifications.

Note

Whenever linking PPR components, pay attention to the hierarchy of the tree structure. If, for example, you link an ECC to a parent object, this means that the children of this object are not displayed in the tree if the user does not have a valid export license. This is the case even though the children were not linked to an ECC.

By linking contracts to PPR components you set the basis for external companies accessing your data. Access to your data is prohibited without a linked contract.

- After a contract is linked to a PPR component, a user linked to this contract can under certain conditions access your data without further adjustments being made.
- The set security level must have the value of **zero**, i.e. must be set to Not Sensitive.
- The PPR components must not be subject to an export restriction. That means the field **Is export controlled** must not be activated for this PPR component, and the PPR component must not be linked to an **ECC**.

Access to PPR components subject to export restrictions is regulated with the help of a linked ECC. Only users from countries that have valid export licenses can access these PPR components according to this definition.

- The form of regulation settled on in the ECC takes immediate effect after the link to a PPR component is made. Access to your data is prohibited to users who do not have a valid export license.

- The link between PPR components and contracts and Export Control Classifications is executed via Drag & Drop. You need the "Change Rights" right for the PPR – component as well as the "Read" right for the contracts and ECCs.

3.8.1 Displaying the Linked Data Objects in the List View

The links are displayed in the listview of the selected PPR components.

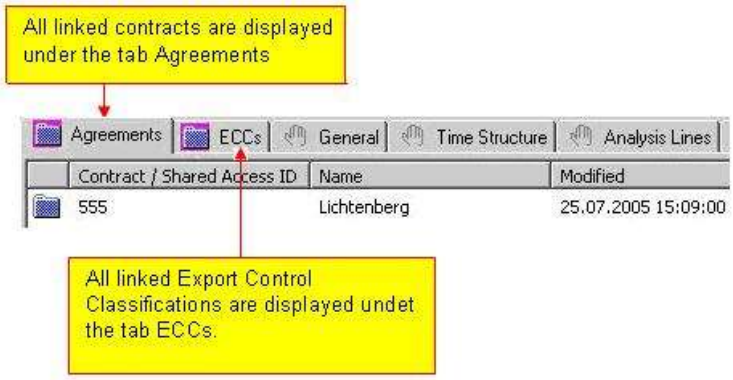


Figure 48: Display of Links in the List view – PPR Components

3.9 Decision Table for Export Licenses – Important Cases

Procedure for access to permitted PPR components is shown in the following tables. The user is in this case always a user from an external company.

Two cases are shown in this table. In the first case there is no export restriction for PPR components. In the second case, the PPR component is subject to an initial export restriction with *Is exported controlled*.

Table 1 – Decision Table for Export Licenses: Description Is Export Controlled is Active

Description of the Case	Access to PPR Components
Case 1: No export restriction for PPR components. Security level for PPR components is zero (not sensitive).	**Prerequisites:** User must be linked to the contract. The contract must be linked to PPR components. Summary: All users who have a contract also have access to the PPR- components.
Case 2: Is export controlled is activated for PPR components. Security level (security level) for PPR components is zero (not sensitive).	**Prerequisites:** User must be linked to the contract. The contract must be linked to PPR components. Summary: All users that have a contract and who are not assigned to countries marked as embargo countries have access to the PPR components. If a user's country is marked as an embargo country, it is sufficient to exclude this user if one of the three conditions is given: The user is a citizen of this country. The user resides / is located in this country. The company to which the user is assigned is based in this country.

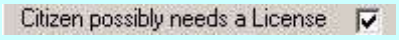
This table assumes that the security level for the PPR components is higher than zero.

Table 2 – Decision Table for Export Licenses: Description Security Level Greater than Zero

Description of the Case	Access to PPR Components
Case 3: Security level (Security Level) for PPR components is greater than zero. The PPR component has been assigned a correspondingly high security level that has been created for the company.	**Prerequisites:** User must be linked to the contract. The contract must be linked to PPR components. The user must be linked to your company. Your company will be represented in the examples by the company Engine Co. Security Levels must exist for the company. The user must have been assigned a sufficiently high enough company security level. Summary: All users who are linked to the company and have been assigned a sufficiently high security level can access the PPR components. For example, the PPR component has been assigned security level 2, and thus the user must have been assigned at least security level 2 or higher.

This table assumes that the option *Citizen possibly needs a License* is active for the country.

Table 3 – Decision Table for Export Licenses: Description Citizen possibly Needs a License

Description of the Case	Access to PPR Components
Case 4: This option is set for country.  Security level (security level) for PPR components is zero (not sensitive).	**Prerequisites**: The user must be linked to a contract and must be a citizen of this country. The contract must be linked to PPR components. The ECC must be linked to PPR components and country. ECC must be linked to export license. The export license must be linked to country and company. **Summary**: That an export license is required must be set in the ECC. The ECC must be linked to the country for which the export license is required. The export license must be linked to the country and company for which the export license is valid. The selection License valid for citizens of... must be selected in order to link the export license to the country. **Supplement to this case**: If the security level for the PPR component were greater than zero, you would also have to link the user to your company (in the example, the company Engine Co.) and assign the corresponding security level to the user.

This table assumes that the option *Sojourn possibly needs a License* is active for the country.

Table 4 – Decision Table for Export Licenses: Description Sojourn possibly needs a License

Description of the Case	Access to PPR Components
Case 5: This option is set for country. Sojourn possibly needs a License ☑ Security level (security level) for PPR components is zero (not sensitive).	**Prerequisites**: User must be linked to the contract. The user must either be located in this country or the company must be based in this country. The contract must be linked to PPR components. The ECC must be linked to PPR components and country. ECC must be linked to export license. The export license must be linked to country and company. **Summary**: That an export license is required must be set in the ECC. The ECC must be linked to the country for which the export license is required. The export license must be linked to the country and company for which the export license is valid. When linking the export license to the country, the selection License valid if located in... must be selected. **Supplement to this case**: If the security level for the PPR component were greater than zero, you would also have to link the user to your company (in the example, the company Engine Co.) and assign the corresponding security level to the user.

3.10 Sample Cases for Security Guidelines

An export license for a country and thus also for the users of companies assigned to this country is required if you have activated one of the following options for the country:

- Citizen possibly needs a license or
- Sojourn possibly needs a license.

When an export license can become necessary is determined in the Export Control Classification. An ECC is first required for PPR components if one of the two options has been activated for a country.

The procedure for doing this is explained in further detail by examples.

The following conventions apply to the following examples.

- Countries that are marked as embargo countries are not taken into further consideration since access to PPR components that are subject to export restrictions in any form is generally not granted.
- The company Engine Co. is meant to refer to your company.
- Mainly both options for a country as well as the basic cases to be taken into consideration are explained in the following examples.

Note

These links should generally be made only by an administrator or an employee with comparable rights.

3.10.1 Initial Situation: Export License for Citizens

The basis for the following examples is the initial situation described in the following; the situation will vary in this text to better reflect the additional options available.

3.10.1.1 Description of the Basic Situation

- Only *Citizen possibly needs a License* is **active** for the country. For more information on countries, *please refer to the* Using Countries.

Figure 49: Country Properties

- Your company Engine Co. is located in the USA.
- The Lichtenberg AG company is located in Italy. *Please refer to the* Using Companies for more information on companies.
- The user Tonio is a citizen of Italy, lives in Italy (residential location), and is an employee of the company Lichtenberg. For more information on users, *please refer to the* Creating Users in the User Management.

Furthermore, the following conditions apply to the project data of your company **Engine Co.**

- Export restrictions are to be available only for process data, in the example this would be process P1.
- All hierarchical levels of the process structure are to be linked to a contract.
- Process P1 is to be linked to the ECC. That an export license is required for this country – Italy in this example – is set in the ECC.
- Decision table for export licenses. The security level zero (not sensitive) is to be valid for the PPR components.
- All processes are allocated to the Engine Co.

Initial Situation of Engine Co.

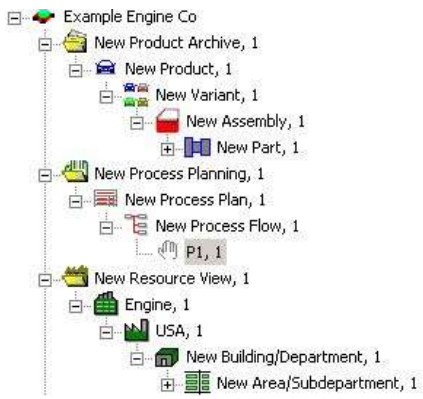


Figure 50: Example – Project Data of Engine Co.

Note

Pay attention to the tree structure when linking contracts and ECC's. Links must be created individually for every object in the tree structure; if you do not do this, children of a parent object may be excluded from the permitted access or may not be displayed at all.

Note

Do not forget to save during all of the actions that you undertake when creating links.

3.10.2 Creating Links – Example 1

In the following you will learn about the necessary steps and links that are required in order to achieve the first objective of the citizens of Italy requiring an export license for accessing your process data.

3.10.2.1 Step 1: Link the Contract with the User Tonio

There is a contract between the company Lichtenberg AG and your company. How to create and link contracts is described under Contracts – using Agreements.

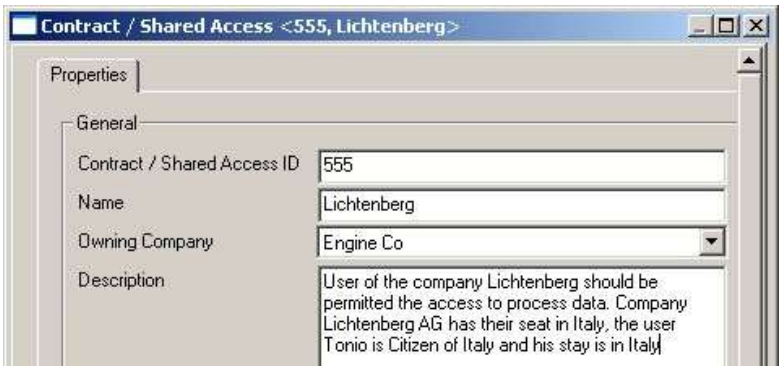


Figure 51: Create Contract

1) The link can be made in both directions. Select the user Tonio in the system library under the data object user.
2) Move the mouse pointer to the contract. Then release the mouse button. The link is created.

Figure 52: Link between Contract and User

3.10.2.2 Step 2: Link Contract to PPR Components

1) Select the contract in the system library under the data object **Contract/Shared Agreements**.

2) Move the mouse pointer to every PPR component individually. Then release the mouse button. The link is created.

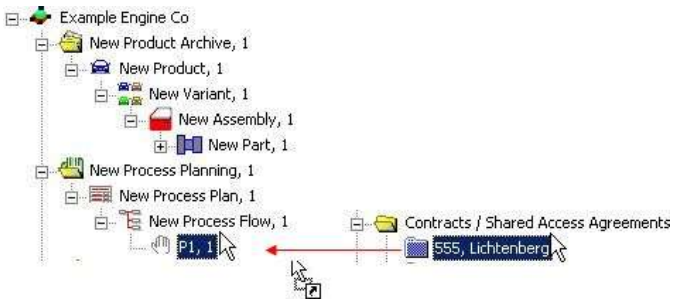


Figure 53: Create Links between Contract and PPR Components

First Intermediate Result

After the contract is linked to all of the PPR components of the process structure of Engine Co., the user Tonio of the Lichtenberg company has access only to process data since there is no contractual agreement for the product and resource data. Another reason for this is that there is not yet an export restriction for process data. *please refer to the* Figure 50.

Figure 54: Access Permitted by Link to the Contract

3.10.2.3 Step 3: Link ECC to PPR Components and Country

Assign Export Control Classifications (ECC) by following these steps:

- Create an ECC in which it is set that an export license is required for Italy.
- Link ECC to PPR components and country.

Create an ECC

License is needed for these country must be active in the ECC. Additional information on the Export Control Classification (ECC) can be found in Use Export Control Classification.

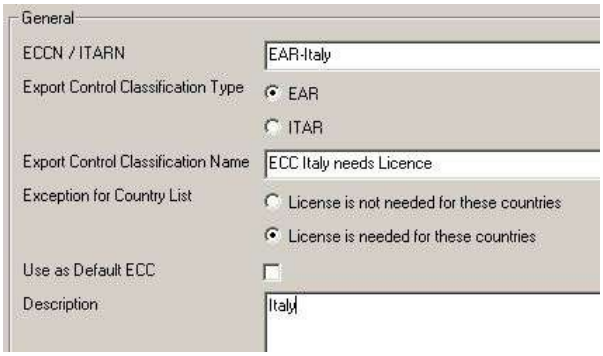


Figure 552: Create an ECC

Linking the ECC to a Country

In the example, the ECC is linked only to Italy.

1) The link can be made in both directions. Select the valid ECC in the system library under the data object *Export Control Classification*.

2) Move the mouse pointer to the country. Then release the mouse button. The link is created.

Figure 56: Linking the ECC to a Country

Linking the ECC to the PPR Components

In the example, the ECC is linked only to process P1.

1) Select the valid ECC in the system library under the data object *Export Control Classification*.

2) Move the mouse pointer to the process (P1). Then release the mouse button. The link is created.

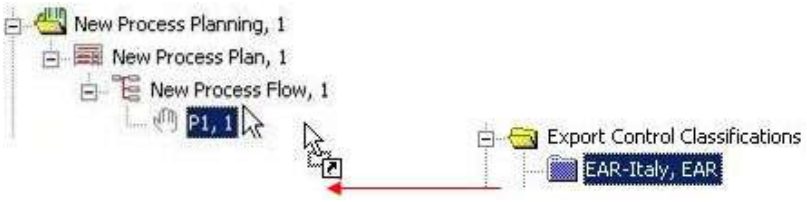


Figure 57: Linking the ECC to A process

First Intermediate Result

After the ECC is linked to the country and PPR component P1, the user Tonio can no longer access the PPR components. The export restriction that citizens from Italy require an export license is valid for these PPR components.

All other users not from Italy who would be contractually authorized to access your data would in this example be able to access these PPR components.

Figure 58: Access Denied

In order to grant access to the user Tonio, he also requires an export license. The procedure for granting a license will be shown in the next step.

3.10.2.4 Step 4: Access is Granted with the Export License

In order to grant an export license, the following steps are required:

- Create the export license
- Linking the export license to the ECC, company, and country.

Creating an Export License

The conditions to which this applies is set in the in the export license. In the example, the conditions for the company Lichtenberg AG apply.

Additional information on export licenses can be found in Using Export Licenses.

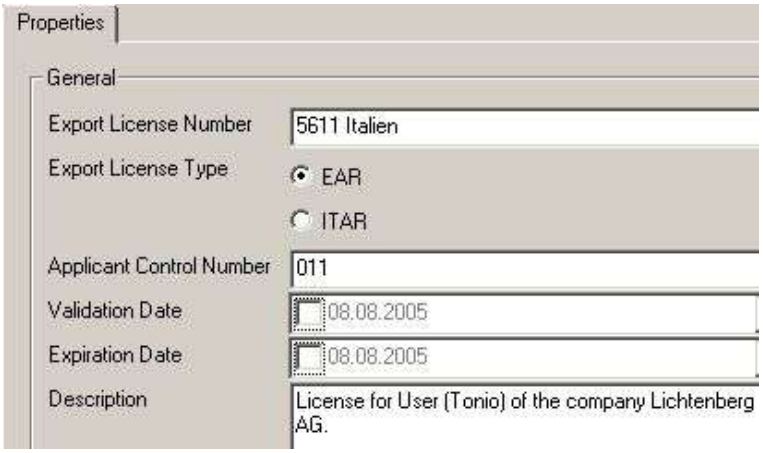


Figure 59: Creating an Export License

Linking the Export License to the valid ECC

In the example, the ECC is linked to the export license *5611 Italy*.

1) The link can be made in both directions. Select the valid ECC in the system library under the data object *Export Licenses*.

2) Move the mouse pointer to the ECC. Then release the mouse button. The link is created.

Figure 60: Linking the Export License to the ECC

Linking the Export License to a Company

The export license must be linked to the company for which this export license is to apply – in the example, the company Lichtenberg AG.

1) The link can be made in both directions. Select the valid ECC in the system library under the data object *Export Licenses*.

2) Move the mouse pointer to the ECC. Then release the mouse button. The link is created.

Figure 61: Linking the Export License to the Company

Linking the Export License to a Country

The export license must be linked to the country for which the export license is to apply – Italy in the example.

1) The link can be made in both directions. Select the valid ECC in the system library under the data object *Export Licenses*.

2) Move the mouse pointer to the country. Then release the mouse button.

Figure 62: Moving the Export License to the Country

3) For our example select the option **License valid for citizens of**.

4) Confirm the selection with **OK**. The link is created.

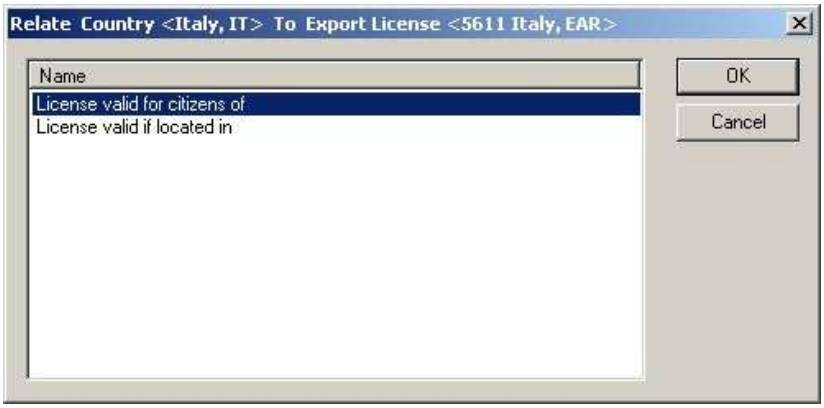


Figure 63: Select Citizenship

Result of the Link

The user Tonio can now access the PPR component P1.

Figure 64: Access with Export License Permitted

Conclusion

You have now created all of the links necessary to fulfill the conditions that the citizens of Italy require a license. The procedure described here applies to every country with the same initial conditions.

3.10.3 Creating links – Example 2

Security Levels for the Company Engine

These security levels are set for your company, Engine Co. *please refer to the* Set security Levels for the Company.

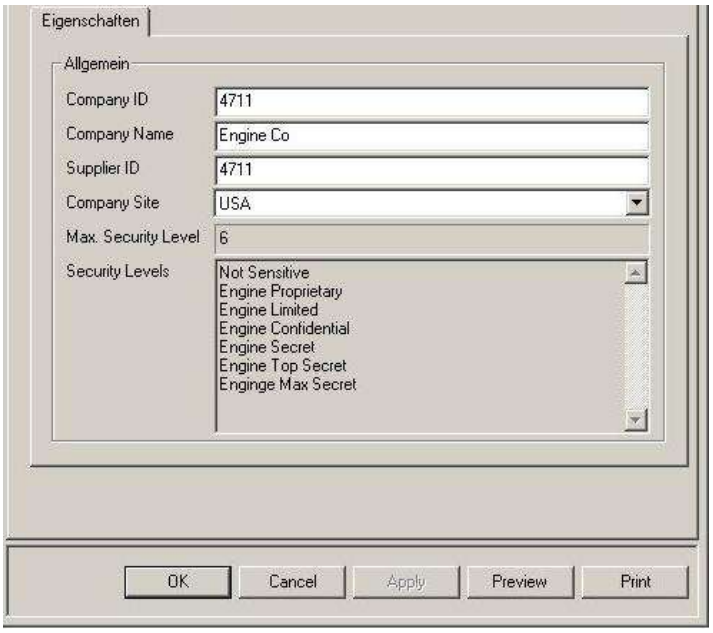


Figure 65: Set Security Levels for the Company

Access to PPR component P1 is permitted in the following steps only because the security level (security level) of **not sensitive** was set for the PPR components.

The security level for process P1 is increased by one level in the following example.

The following prerequisites must be fulfilled:

- The PPR component P1 must contain the security level 1.
- Security levels must exist for your company (*Please refer to the* Using Companies).

- In the example, the user Tonio must be linked to your company, Engine Co.
- The user Tonio must be granted the corresponding security level. This security level can be equal to or greater than the security level of the PPR component Process1.

Increasing the Security Level for Process 1 by One

1) Open the context menu to Process 1 in your project (example of Engine Co.).
2) Select the menu item Access Rights. *please refer to the* Using Access Rights to PPR Components.

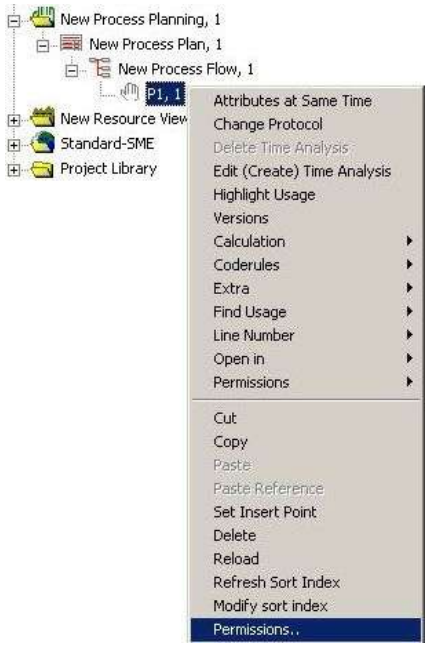


Figure 66: Open the Context Menu to Process Components

1) In the example, the security level is to be increased by one security level.

- The possible security levels are available for the PPR components only if they are also created for the company – in the example, Engine Co.

2) Select the security level in this dialog. Confirm the selection with **OK**.

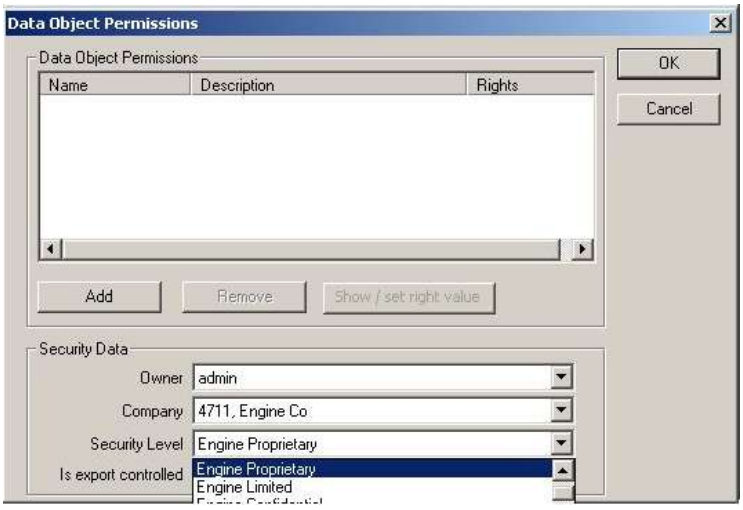


Figure 67: Increasing the Security Level by One

As long as the user Tonio does not have this increased security level, he can not access this process component.

Figure 68: The User does not have a Sufficient Security Level

Security Levels for the Company Engine

These security levels are set for your company, Engine Co. *please refer to the* Set security Levels for the Company.

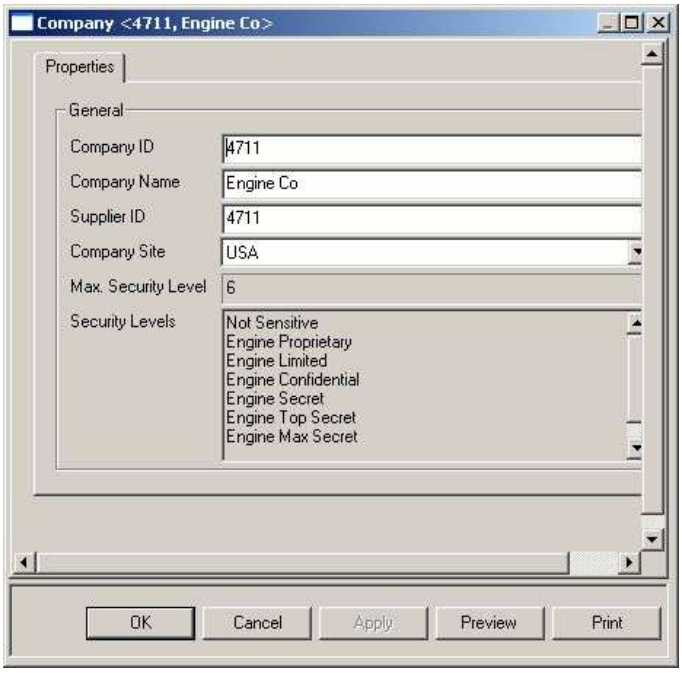


Figure 69: Set the Security Levels for a Company

Link Users to the Engine Co.

Only if a higher security level greater than one exists for your PPR components do you need to link the users of a company – in the example the user Tonio with the Engine Co.

1) The link can be made in both directions. Select the user in the system library under the data object user.
2) Move the mouse cursor to the company. Then release the mouse button. The link is created.

Figure 70: Linking the User to a Company

Assigning a Security Level for Users

After the user is linked to your company, you can either assign the security level to the user or your company. The link is displayed in the list view under the tab *Security Levels*.

1) Click on the tab Security Levels in the list view.
2) Select the linked object – in the example, Engine Co. (Tonio).
3) Open the context menu and select the menu item *Edit Security Level*.

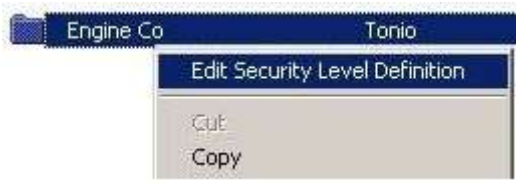


Figure 71: Open Context Menu – Select Edit Security Level

4) Click in the field next to the possible Security Levels – in the example, the security level **Engine Proprietary** is used.
5) Confirm the entry with **OK**.

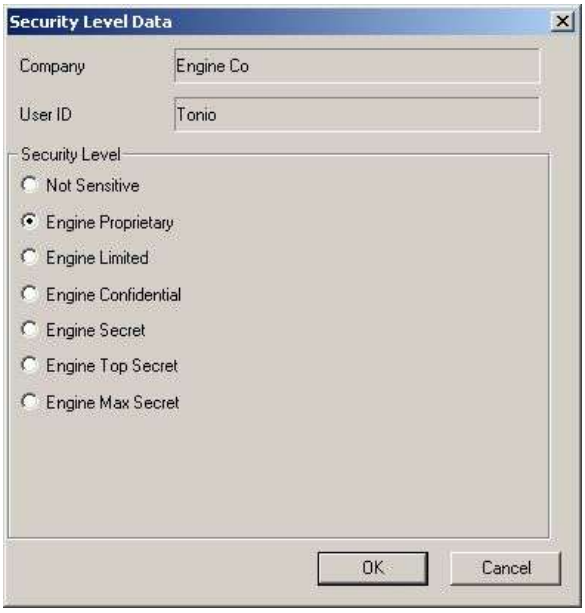


Figure 72: Assign a Security Level to a User

Result – Example 2

After all of these links have been created, the user Tonio will again have access to the process component P1.

If, as is the case in this example, the Security Overlays Properties… are activated, the set security level is displayed in the list view of Process P1.

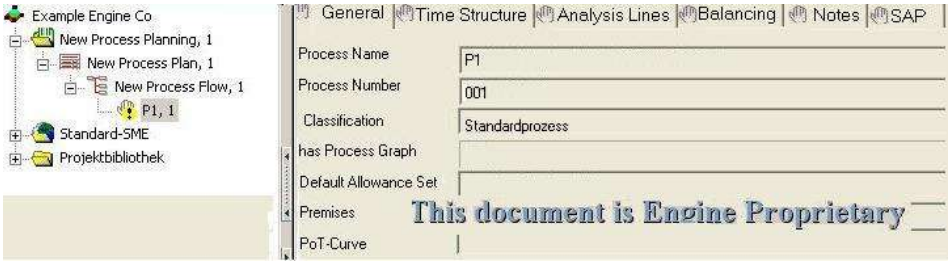


Figure 73: Access to Process P1 Permitted – Example 2

3.10.4 Creating Links - Example 3

The essential prerequisite for accessing the process component **P1** in the previous examples was that the user is a citizen of Italy.

The following prerequisites were valid in the initial situation:

- The user Tonio is a citizen of Italy.
- He lives in Italy (residence location).
- The company is located in Italy.

The residence location of the user Tonio is to be changed in this example. The residence location is to be switched to Germany. Therefore an export license is required for Germany as a residence location.

1) In the example, the user Tonio's residence location is changed in the user management under User. *Please refer to the* Creating Users in the User Management.

Figure 74: Change the Residence Location of the User in the User Management

2) In order to fulfill this prerequisite, activate the field *Sojourn possibly needs a License* for the country Germany. *Please refer to the* Location for a Country.

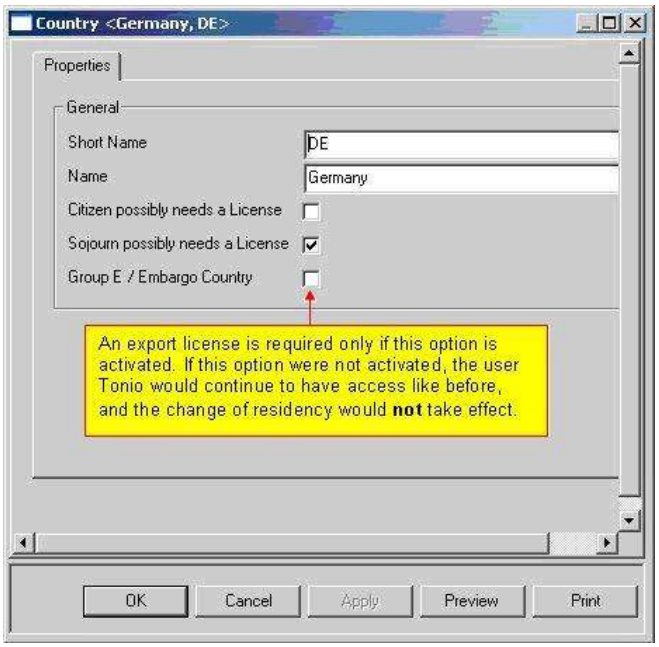


Figure 75: Activate Residence Location: Germany

Prerequisites

The previous prerequisites apply to this example as well. The ECC has been extended so that it would also apply to Germany in order to simplify the matter. You would actually set the countries for which an ECC is valid in advance.

The following conditions must be fulfilled:

- Germany must be set as the location in which the user Tonio resides.
- The option *Sojourn possibly needs a License must be* activated for the country.

- That an export license is required must be set in the ECC. In the example, the ECC is also linked to Germany.

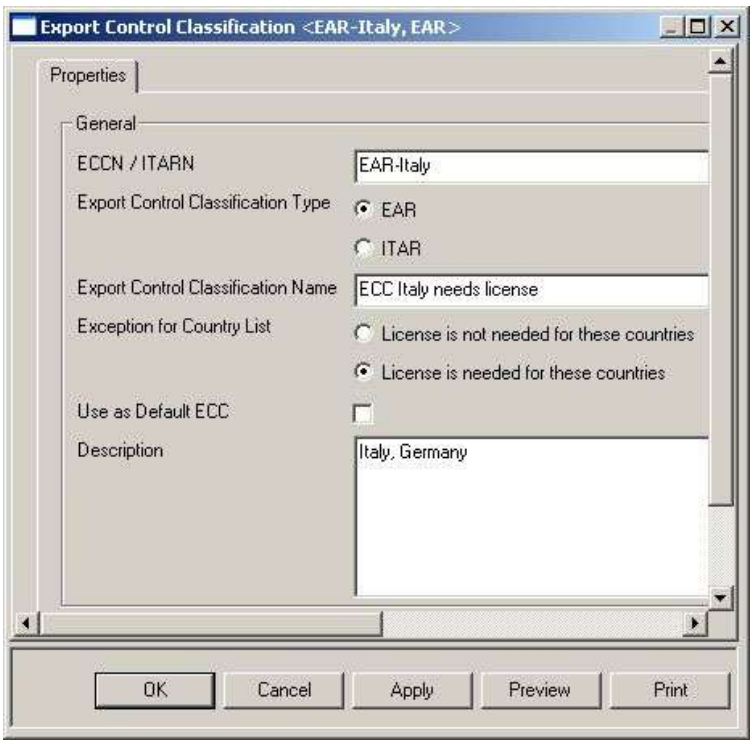


Figure 76: ECC Extended for Germany

- The export license must be linked to Germany in order for the user Tonio to be granted access to the process components.

ECC is Linked to Country

In the example, the ECC is linked to Germany. Linking the ECC to the export license is not necessary in the example because the link for the company **Lichtenberg AG** already exists. If this prerequisite were not fulfilled, you would of course have to create a link to an export license and link the license to the company.

1) The link can be made in both directions. Select the valid ECC in the system library under the data object *Export Control Classification*.

2) Move the mouse pointer to the country. Then release the mouse button. The link is created.

Figure 77: Link the ECC to Germany

Linking the Export License to a Country

In the example, the export license is linked to Germany. Linking the export license to the company is not necessary in the example because the link for the company **Lichtenberg AG** already exists.

1) The link can be made in both directions. Select the valid ECC in the system library under the data object *Export Licenses* – in the example, this would be the same export license *(5611 Italy*).

2) Move the mouse pointer to the country. Then release the mouse button. The link is created.

Figure 78: Link the Export License to Germany

3) In the dialog select License valid if located in.

4) Confirm the selection with **OK**. The link is created.

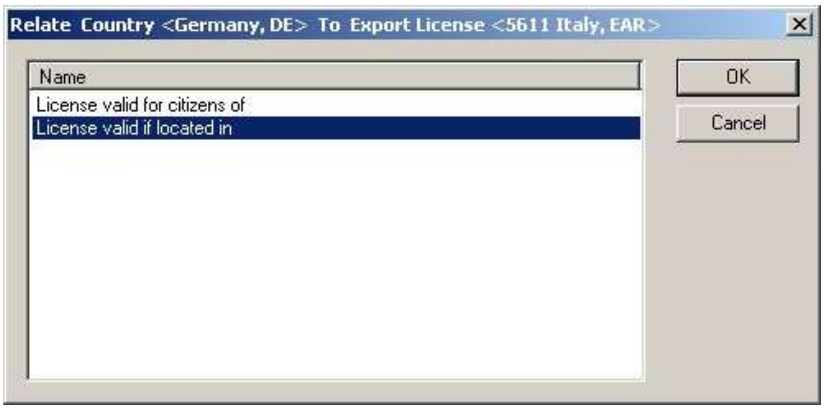


Figure 79: Select Residence Location

Result – Example 3

After these steps, the user Tonio is again granted access to the PPR component **Process P1**.

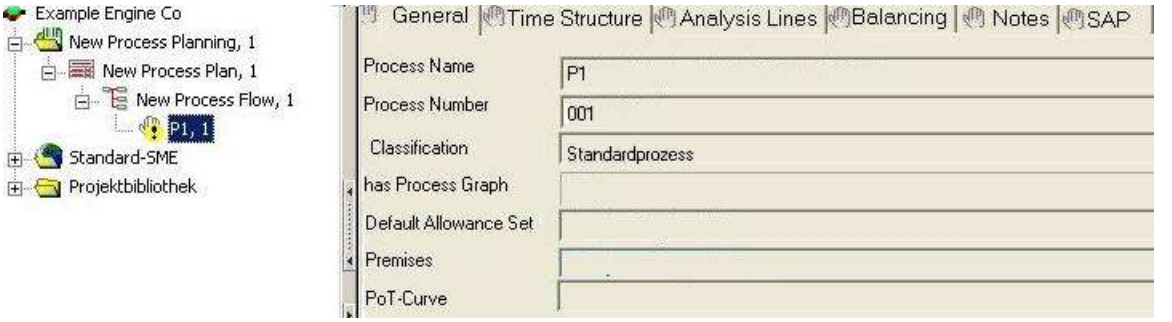


Figure 80: Access to Process Components Permitted

.

List of Figures

List of Tables

Index