



# LECTRA FASHION PLM USERS ACCESS RIGHTS CONFIGURATION

## Configuration Guide

---

---

**Date of last update:** June, 2015

## Contents

<b>1. Product Development Profiling - How to initialize user access rights to Product development functionalities and how to manage supplier access ? .....</b>	<b>3</b>
<b>2. Product Development Profiling - How to maintain my rules to access to Product Development functionalities ? .....</b>	<b>9</b>



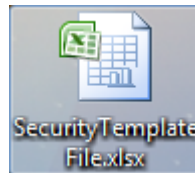
For more information on Security Management, you can also refer to the **Lectra\_Fashion\_PLM\_Security Management** document which is located in the documentation package.



Modifications made to the document since its last publication are highlighted in [blue](#).

## 1. PRODUCT DEVELOPMENT PROFILING - HOW TO INITIALIZE USER ACCESS RIGHTS TO PRODUCT DEVELOPMENT FUNCTIONALITIES AND HOW TO MANAGE SUPPLIER ACCESS ?

- Access to the Security initialization file :
  1. Open the **PLM Manager**.
  2. Click on the **Menu Security > Create Excel Security Template File...** : a file chooser window is opening.
  3. Choose a name and a directory for the security initialisation file.
  4. Click on **Save**.



- Edit the Security initialization file :
  5. Open the Security Initialization file with **Excel**.



## Security Initialization File description

**Sheet 1 - Configuration** : This sheet is generated with the Platform Configuration and contains all categories, envitemns, specification packages ... defined : useful for access key definition.

**Sheet 2 – Users & Groups** : This sheet aims at creating users. Each user should be linked to groups that are used for Product Development access rights. This Security Initialization file is filled with example data to modify.

**Sheet 3 – Profiles** : This sheet aims at creating Product Development or and Calendar Management features access rights for each group defined in the sheet 2.

**Sheet 4 – Reports** : This sheet lists all reports installed on your Lectra Fashion PLM Platform in order to define access on report generation.

**Sheet 5 – Licenses** : For more details, please contact implementation teams.

**Sheet 6 – Documentation** : This sheet explains how to fill the Excel Initialisation File.

**Sheet 7 – Lists** : Lists of values used for user creation :

- Language, Locale, Timezone codes

- Define Users and Groups :
  6. Go to the **Users & Groups** sheet.
  7. Add users by adding new lines :
    - **Login** : login for Product Development connection
    - **Password** : password for Product Development connection
    - Email : user email address
    - Firstname : user firstname
    - Surname : user surname
    - Locale : user locale
    - Language : user language
    - Timezone : user timezone



Fields in bold are mandatory.



Go to the sheet **Lists** to have all available values for column **locale**, **language** and **timezone**.

8. Add groups by adding new columns after Orange Headers (After Group timezone).
- 9.



Think about all different types of Product Development access rights and define a name for each access type.

10. Affect each user to a group by typing **1** in the intersection row of the user line and the group column.

<b>timezone</b>	full_admin	business_admin	merchandiser	designer	colorist	grading_specialist	technical_designer
Europe/London	1						
Europe/Brussels		1					
Europe/Brussels			1				
Europe/London				1			
Asia/Tokyo					1		
Europe/London						1	

11. If a group has been defined for a supplier access, type **1** in the row above the group name (**line 2 - Group Supplier ?**)

	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
		1	2	3	4	5	6	7	8	9	10	11	12	13	14
<b>timezone</b>	nin	is_admin	ndiser	ir			specialist	al_designer	maker	specialist	ocialist	manager	ar_Planner	ar_Process_N	

12. Remove example lines and columns.

- Define Product Development functionalities access rights :

13. Go to the **Profiles** sheet.

14. Add Product Development functionalities on which rights should be defined by adding new lines :

- **Level 1** : Customization first level (category name , envitem name...)
- Level 2 : Customization second level : specification package name (only if the first level is a category name)
- Level 3 : Customization third level : spec table name (only if the second level is a specification package name)



Fields in bold are mandatory.



Fields in bold are mandatory.



Go to the sheet **Configuration** to have all available configuration installed on your platform.

15. Add group names defined in **step 8** in the orange header.
16. For each Product Development functionalities and each groups, define the available actions (like create, update, delete...).
17. Remove example lines and columns.



Example of privilege keys :

- **R,P** : Read and Print report actions are available
- **\*** : all rights are available
- **C,R,U,D** : create, read, update and delete actions are available



Go to the sheet **Documentation** to know the key corresponding to each action (D = delete ...).



You can remove a right by prefixing the action with – (exemple \*-D : all rights are available except the delete action)



In a row, actions are separated with a coma.



By **default** (ie. If there is no value), **all rights are available**.

- Define Product Development Reports generation access rights :
  18. Go to the **Reports** sheet.
  19. Add group names defined in step 9 in the header.
  20. For each report and each group, set the value **1** if this group can generate this report. Otherwise, leave the column empty.



Setting **\*** in the first blue line allows the group to print all templates.

- Apply the Security Excel File
  21. Go back to the PLM Manager.
  22. Click on the **Menu Security > Load Excel Security File...** : a file chooser window is opening.

23. Select your Security Excel File.

24. Click on **Open**.

25. A progress window is opening. At the end of the process, a status window displays the import state.

- Verify the Security Initialization

**Check the users creation :**

26. Click on the Menu **Security > Users** :

- All user names are displayed on the Left Window part.

27. Check that all your users are in the list.

28. Click on each user to check that all user informations are correctly filled.

29. Check in the **Group** tab that the user is correctly affected to groups defined in the Excel Initialisation File.

**Check the groups creation :**

30. Click on the Menu **Security > Groups** :

- All group names are displayed on the Left Window part.

31. Check that all your groups are in the list.

32. Click on each group and click on the **Profile** tab to check that a profil is linked with the same name as the group.

**Check the rights creation :**

33. Click on the Menu **Security > Profiles** :

- All your security profiles are displayed



Security profiles are generated from the Security Initialization files. Their names are generated and correspond to the concatenation of the string **ProductDevelopment** (it defines that it is a Product Development profile) and the name of groups.

34. Check that we have a Product Development profile for each group in the Excel Initialization File.

35. Click on each profile to visualize privileges.



Privileges are generated from the sheet **Profiles** of the Excel Initialization File.

The Product Development Profile detail view contains the following column :

- **Type** : correspond to the level 1 of the sheet Profiles
- **Spec Package** : correspond to the level 2 of the sheet Profiles
- **SpecTable** : correspond to the level 3 of the sheet Profiles

This 3 first columns defines a Product Development functionality.

- **Action** : corresponds to the actions set into the row between the Product Development functionality and the group. Refers to the sheet Documentation to know the mapping between the action code and the action name.
- **Tag** : For more details, please contact implementation teams.
- **Value** : true if the action is available. false if the action is not available.



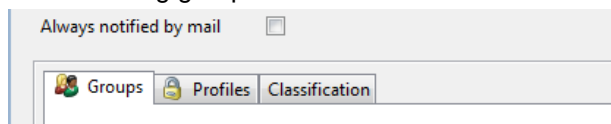
## 2. PRODUCT DEVELOPMENT PROFILING - HOW TO MAINTAIN MY RULES TO ACCESS TO PRODUCT DEVELOPMENT FUNCTIONALITIES ?


- Add a user
  1. Open the PLM Manager
  2. Click on the Menu **Security > Users**
  3. Click on the button **Add**
  4. Fill the fields :
    - **Login** : login for Product Development connection
    - Name : user surname
    - Firstname : user firstname
    - **Password** : password for Product Development connection
    - **Confirm password** : type again the password to check it
    - Email : user email address
    - Language : user language
    - Enabled : enable user.
    - Always notified by mail : User will always receive a mail for every notification



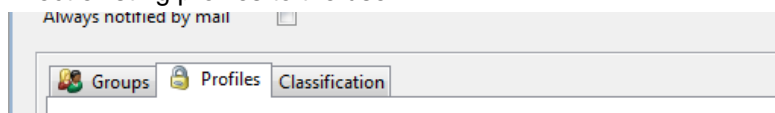
Fields in bold are mandatory.


5. Affect existing groups to the user :



- a. Click on the sheet **Groups**
- b. Affect a group by clicking on its name in the Available Groups and click on the button 

6. Affect existing profiles to the user :



- a. Click on the sheet **Profiles**
- b. Affect a profile by clicking on its name in the Available Profiles and click on the button 

7. Click on the button **Save**.

- Edit a user
  8. Open the PLM Manager

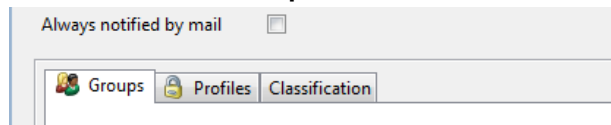
9. Click on the Menu **Security > Users**
10. Click on the user to modify
11. Fill the fields to modify :
  - **Login** : login for Product Development connection
  - Name : user surname
  - Firstname : user firstname
  - **Password** : password for Product Development connection
  - **Confirm password** : type again the password to check it
  - Email : user email address
  - Language : user language
  - Enabled : enable user.





Fields in bold are mandatory.

12. Change groups in which the user is set :

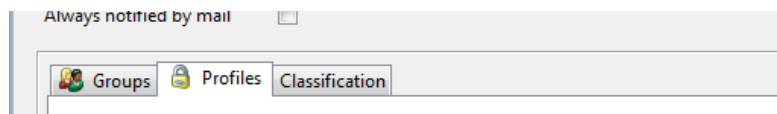
- a. Click on the sheet **Groups**





- b. Affect a group by clicking on its name in the Available Groups and click on the button 
- c. Deaffect a group by clicking on its name in the Selected Groups and click on the button 

13. Change affected profiles for the user :

- a. Click on the sheet **Profiles**









- b. Affect a profile by clicking on its name in the Available Profiles and click on the button 
- c. Deaffect a profile by clicking on its name in the Selected Profiles and click on the button 

14. Click on the button **Save**.

- Delete a user

15. Open the PLM Manager
16. Click on the Menu **Security > Users**
17. Right click on the user to delete

18. Click on the **Delete** button.
- Add a group
  19. Open the PLM Manager.
  20. Click on the Menu **Security > Groups**.
  21. Click on the button **Add**.
  22. Fill the group name.
  23. Affect existing users to the group :
    - a. Click on the sheet **Groups**
    - b. Affect a user by clicking on its name in the Available Users and click on the button 
  24. Affect the user to existing profiles :
    - a. Click on the sheet Profiles
    - b. Affect a profile by clicking on its name in the Available Profiles and click on the button 
  25. Click on the button **Save**.
- Edit a group
  26. Open the PLM Manager
  27. Click on the Menu **Security > Groups**.
  28. Click on the group to modify
  29. Change users included by the group :
    - a. Click on the sheet **Users**
    - b. Affect a user by clicking on its name in the Available Users and click on the button 
    - c. Deaffect a user by clicking on its name in the Selected Users and click on the button 
  30. Change affected profiles for the group :
    - a. Click on the sheet **Profiles**
    - b. Affect a profile by clicking on its name in the Available Profiles and click on the button 
    - c. Deaffect a profile by clicking on its name in the Selected Profiles and click on the button 
  31. Click on the button **Save**.
- Delete a group
  32. Open the PLM Manager
  33. Click on the Menu **Security > Groups**
  34. Right click on the group to delete.
  35. Click on the **Delete** button.

- Add a profile

36. Open the PLM Manager.
37. Click on the Menu **Security > Profiles**.
38. Click on the button **Add**.
39. Fill the group name.
40. Choose the Product Development namespace (for Product Development profile).
41. Add Privileges by clicking on the Add button and filling the fields :
  - **Type** : first level of configuration (category, envitem...).)
  - SpecPackage : specification package configuration name (only if the type is a category)
  - SpecTable : specification table configuration name (only if the specification package field is filled)



This 3 fields correspond to a Product Development functionality.

- Tag : For more details, please contact implementation teams.
- **Action** : action name (delete, create ...)
- **Value** : True if the action is available for the Product Development functionality.
  - False if the action is not available for the Product Development functionality.



Fields in bold are mandatory.



All possible values for privilege fields (except Tag) are provided in the list. It is not possible to set another value.

42. Click on the button **Save**.



To use this profile do not forget to affect it to the corresponding group.

- Edit a profile

43. Open the PLM Manager.
44. Click on the Menu **Security > Profiles**.
45. Click on the profile to modify.
46. Add Privileges by clicking on the **Add** button and filling fields.
47. Modify a privilege by clicking on each fields on the line and selecting the new value in the available list.

48. Delete a privilege by clicking on the line and on clicking on the **Delete** button.

- **Type** : first level of configuration (category, envitem...) )
- SpecPackage : specification package configuration name (only if the type is a category)
- SpecTable : specification table configuration name (only if the specification package field is filled)



This 3 fields correspond to a Product Development functionality.

- Tag : For more details, please contact implementation teams.
- **Action** : action name (delete, create ...)
- **Value** : True if the action is available for the Product Development functionality.
  - False if the action is not available for the Product Development functionality.



Fields in bold are mandatory.

49. Click on the button **Save**.

- Delete a profile
  - 50. Open the PLM Manager
  - 51. Click on the Menu **Security > Profiles**
  - 52. Right click on the profile to delete.
  - 53. Click on the **Delete** button.