Security Profiles

Administration Tool

This document is the property of SIATEL.
All rights reserved to SIATEL.

Table of contents

General - Access rights to Gargantua production objects 5
How are access rights to production objects managed in Gargantua? 5
What is a security profile? 6
Access rights cascading inheritance 7
What is the "Security profile" system attribute for? 7
Access rights and database security levels 8

Creating a new security profile 10

Security profiles management screen 11
Global structure 11
Access rights applying to all production objects 12
Access rights applying only to folders and processes 13
Access rights applying only to documents 14

Managing security profiles 18
Duplicating a security profile 18
Exporting a security profile 18
Importing a security profile 19
Deleting a security profile 19

Assigning a predefined security profile to an object in the Web Client 21
Assigning a custom profile to an object 22
Assigning a custom profile based on a predefined security profile to an object 22

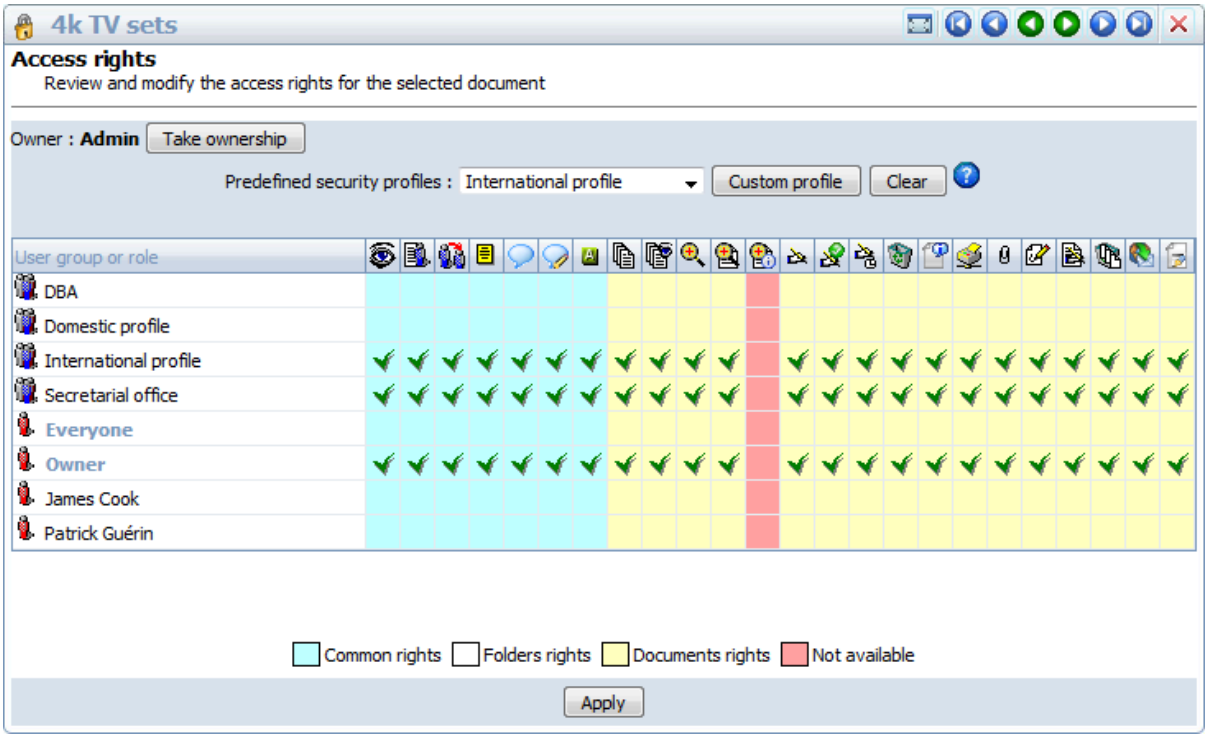
General - Access rights to Gargantua production objects

How are access rights to production objects managed in Gargantua?

With Gargantua, you can set very accurately what operations each user, group or role is allowed to perform on each production object (that is, on each object created from the Web Client: folder, document, pin, process instance...). For example, a user can be allowed or not to create, archive or delete a folder or a document, to modify its attribute, to modify its form, to annotate it...

Setting access rights on production objects is done from the Web Client, by clicking the **Access rights** icon in the toolbar.

You access a screen allowing you to apply security profiles to the current object (check detailed procedures below):

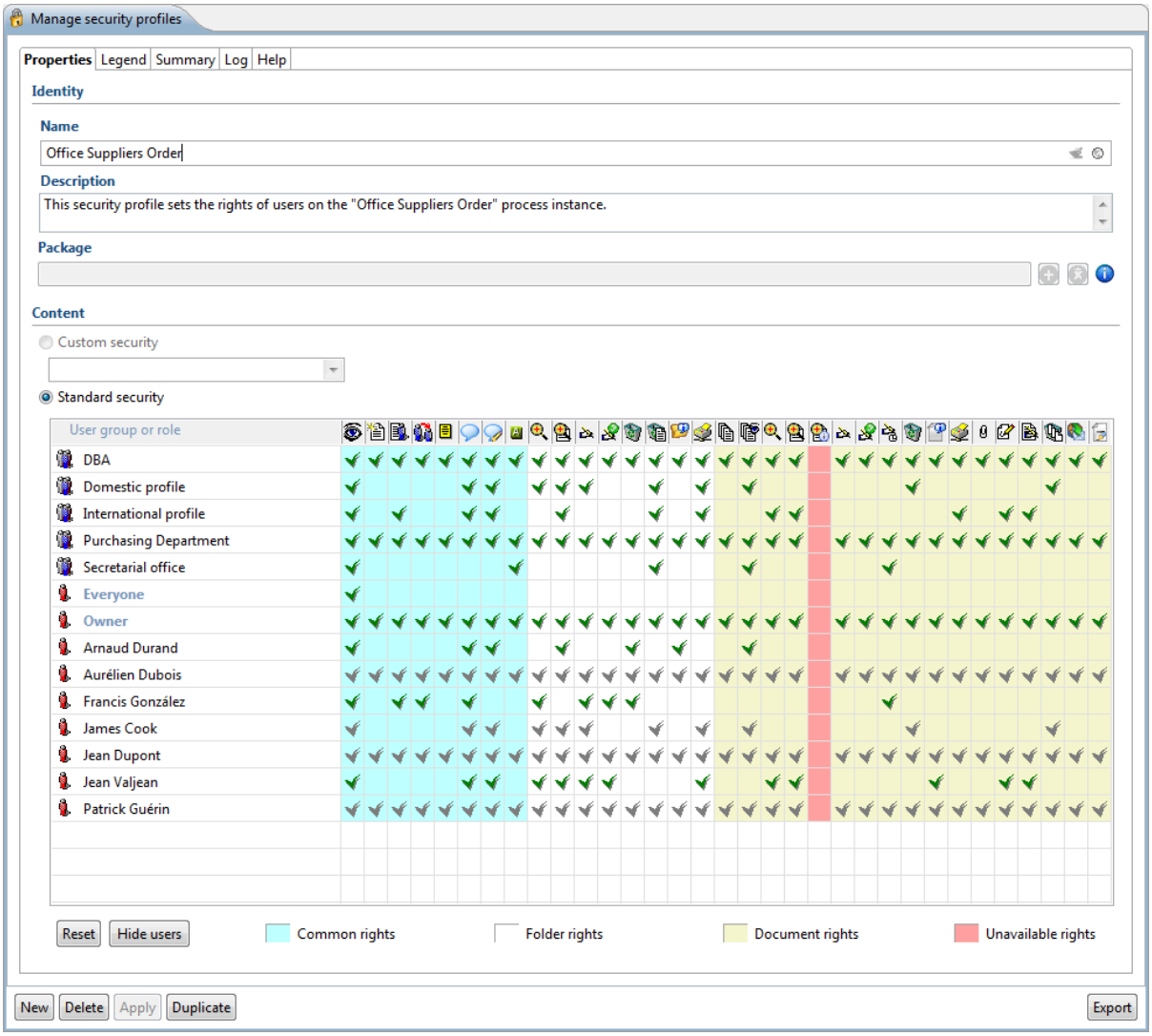


*To use the "**Access rights**" tool, you need to either belong to the DBA group or to have the "**Modify access rights**" access right on the current object.*

*The DBA group members can **always** modify the access rights, even when the corresponding checkbox is unchecked.*

What is a security profile?

A security profile is a **predefined set of access rights** that an administrator creates from the Administration Tool in order to assign it to the corresponding Gargantua database production objects:



Setting security profiles allows you to implement a consistent policy regarding the access rights to similar production objects:

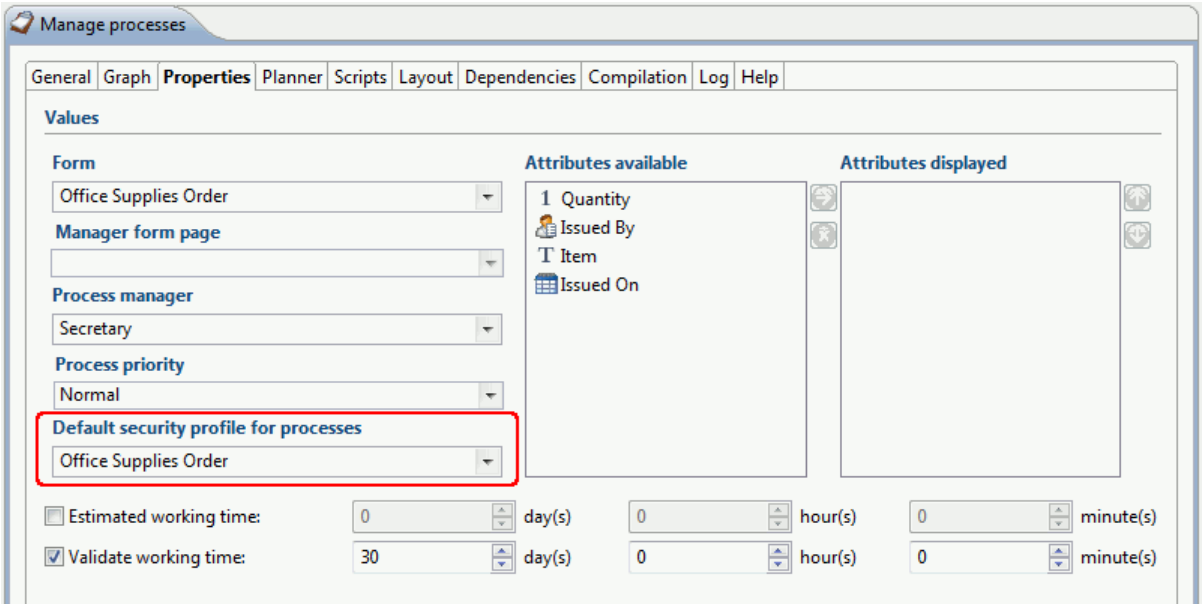
- They avoid having to check again all the boxes everytime you want to set the same access rights on a new object;
- They allow you to modify the access rights of several objects in one click, without having to modify them for each object: the changes made on a security profile in the Administration Tool are automatically applied to all the objects this profile is assigned to.

Access rights cascading inheritance

Cascading inheritance applies to all the access rights and security profiles, in the case of objects that have just been created and/or that cannot have their own access rights (see Access rights and database security levels).

This means that:

- Folders inherit by default the database access rights.
- Sub-folders inherit by default the parent folder access rights.
- Documents inherit by default the parent folder or process instance access rights.
- Process instances inherit by default the database access rights, unless a default security profile has been assigned to the process.



If you copy and paste a document inside a database with the tool, the copy will inherit by default its new parent access rights.

What is the "Security profile" system attribute for?

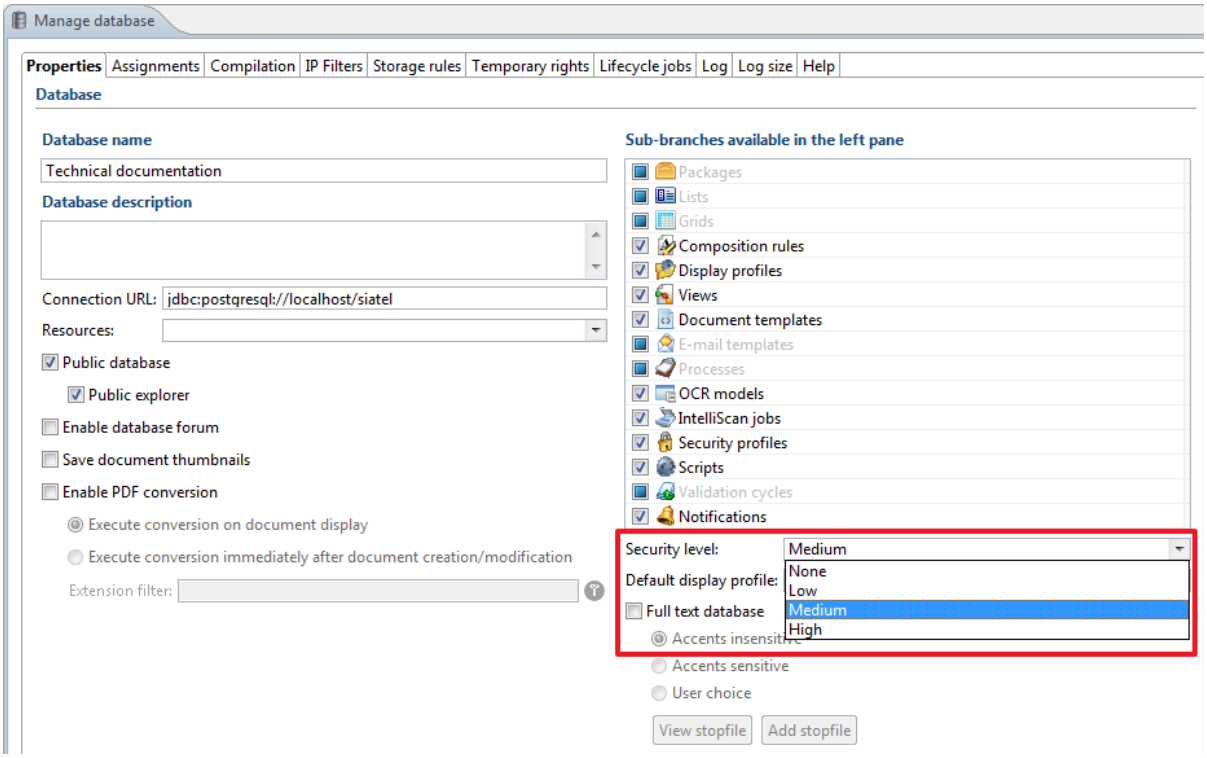
A **Security profile** system attribute can be added to a Gargantua form from the **Content** tab of its management screen.

This attribute then displays in read-only mode in the Web Client. It allows users to know if a security profile has been applied, and which one, even if they do not have the **Modify access rights** access right.

Access rights and database security levels

The access rights precision depends on the security level set for the corresponding Gargantua database:

- If the database does not have any security (**None** security level), the **Access rights** tool does not display in the Web Client: all the users that can access the content of the database can perform all the operations on all the production objects (to the extent of the privileges they have been granted).
- If the database has a **Simple** security level, you can set access rights at database level: they will apply to all the production objects of the database.
- If the database has a **Medium** security level, you can set access rights at folder and process level: they will apply automatically to the documents contained by the folder or process.
- If the database has a **High** security level, you can set access rights for each object, including documents.



When a **None**, **Medium** or **High** security level is applied to a database (when creating it, or later), it gets by default the following access rights:

- The DBA group members and the object owner have all the access rights.
- The other users only have the rights to see that objects exist. They cannot perform any operation.

User group or role																															
DBA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
HR Assistant																															
HR Manager																															
Everyone	✓																														
Owner	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Admin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Amy Smith																															

Creating a new security profile

To create a new security profile, proceed as follows:

1. In the left pane of the Administration Tool, expand the branch corresponding to the Gargantua database of your choice.
2. Click the **Security profiles** sub-branch.

   The list of security profiles displays in the right pane.

3. In the bottom left corner of the right pane, click the **New** button.

   The new security profile management screen displays.

4. In the **Identity** section, fill in the **Name** field, and, if you want, the **Description** field.
5. Assign the access rights of your choice to users, groups and/or roles by clicking the corresponding boxes in the **Content** table.

   You can check all the boxes of a row by double-clicking the user, group, or role name. (Double-click again to uncheck all the boxes.)

   If you do not check any box, all the users will be granted all the access rights.

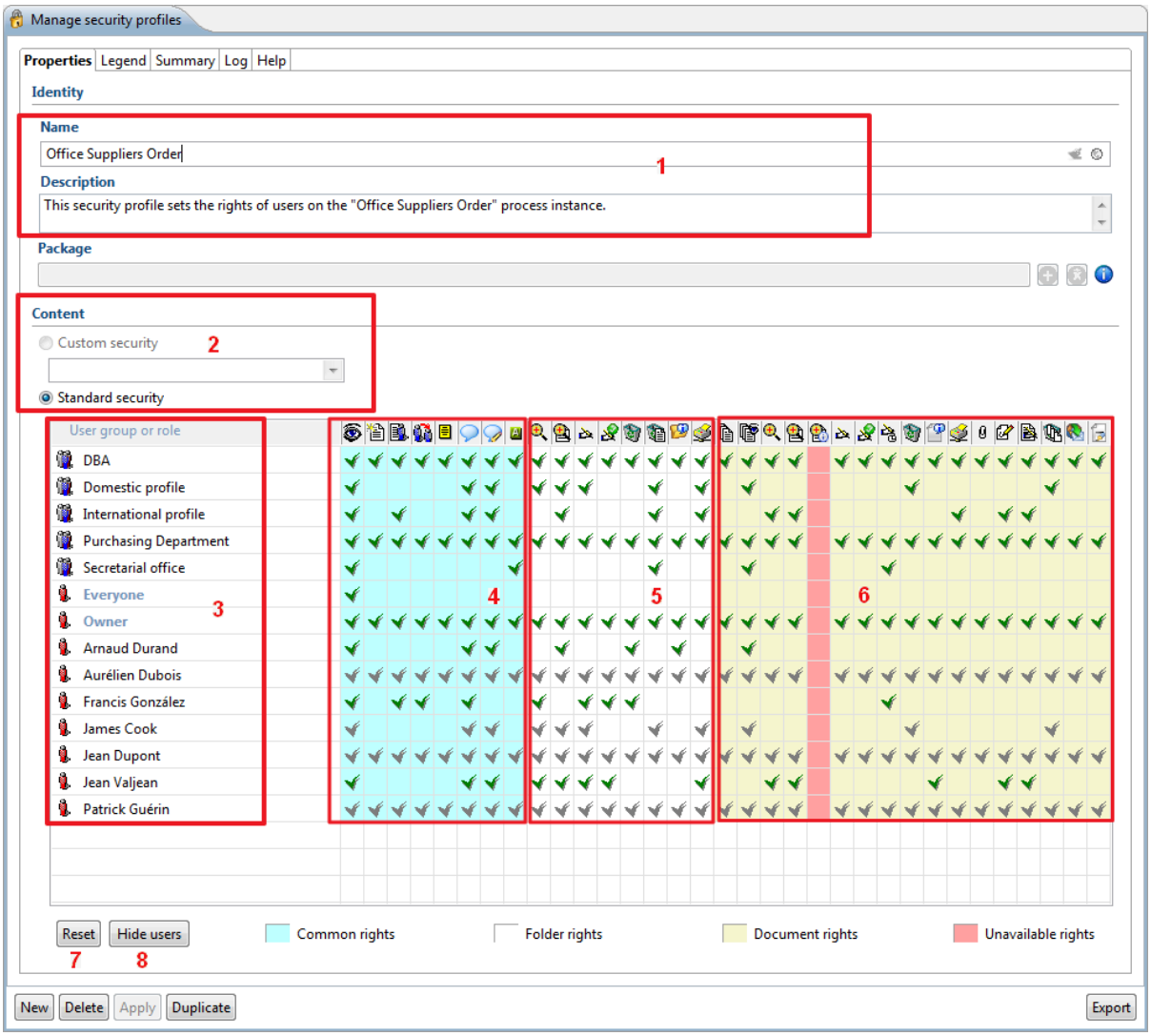
6. When you are finished, click the **Apply** button in the bottom left corner of the right pane.

   The new security profile has been saved: you can now assign it to production objects from the Web Client.

Security profiles management screen

Global structure

The security profiles management screen is as follows:



1. Fields containing basic information about the current security profile (name and description);
2. Radio buttons allowing you to choose between a normal security profile and a custom security profile (only available if custom developments regarding security profiles have been provided by SIATEL);
3. Column containing the names of the groups, roles and – if you have clicked the **Show users** button – users assigned to the database; the **Everyone** row allows you to assign a set of access rights to all users, while the **Owner** row corresponds to the object creator (unless the object ownership was transferred to another user);
4. Columns corresponding to the access rights that apply whatever object the security profile is used on:

folder, process, document, etc.

5. Columns corresponding to the access rights that apply if the security profile is used on a folder or a process;
6. Columns corresponding to the access rights that apply if the security profile is used on a document or a pin.
7. **Reset** button allowing you to delete all the checks from the security profile in one clic, in order to start with an empty table;
8. **Show users/Hide users** button allowing you to list individual users (besides groups, roles…) in the access rights table, in order to give them specific access rights;

Access rights applying to all production objects

The access rights applying to all production objects are the following:

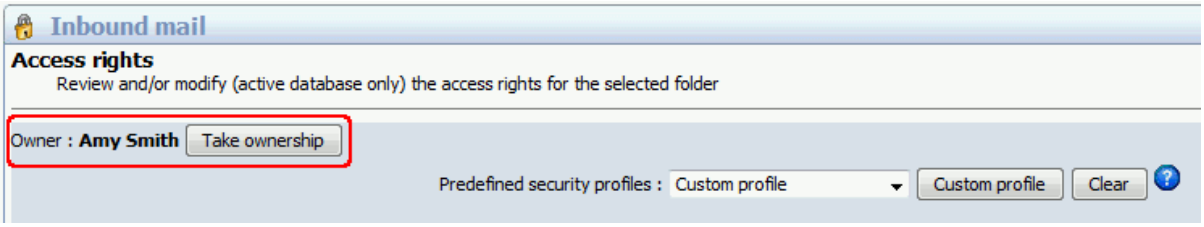
- **See object's name in lists**: Users with this access right can see the name and location of the object in the classification tree, in the documents list, and in search results, but they cannot perform any other operation on it.

  > ***The DBA group members can always see that an object exists, even though the corresponding checkbox is unchecked.***

- **Create objects**: Users with this access right can create folders and documents inside the current object.
- **Modify access rights**: Users with this access right can modify the current object access rights using the **Access rights** tool.

  > ***The DBA group members can always modify the access rights of an object, even though the corresponding checkbox is unchecked.***

- **Take ownership**: Users with this access right can take the ownership of the current object if it has been created by another user. This operation is done by clicking the **Take ownership** button located in the access rights modification frame:



> ***Users allowed to take ownership on an object can only do it if they also have the "Modify access rights" access right.***

- **Create note**: Users with this access right can use the tool to add notes to the current folder or document. They can also view all the notes attached to the document.

> ***To view the existing note of a folder (by clicking again the tool), users also need to have the "View folder attributes" access right. To modify the note, they also need to have the "Modify folder attributes" access right.***
>
> ***To modify a note attached to a document, users also need to have the "View document attributes" and "Modify document attributes" access rights.***

- **Read the forum**: Users with this access right can read the discussions in the forum about the current object.
- **Write in the forum**: Users with this access right can post messages in the forum about the current object.
- **Archive**: Users with this access right can use the **Move to archive database** tool to transfer the current object from the active part of the database to the archive part.

> ***If a user is allowed to archive a folder or a pin, he is also allowed to archive the children objects it contains, regardless of their individual access rights.***

Access rights applying only to folders and processes

The access rights that only apply to folders and processes are the following:

- **View folder attributes**: Users with this access right can display the form of the current folder or process, and view the attributes in read-only mode.
- **View files' contents**: Users with this access right can view the content of the files located in the current folder or process. For databases with a **High** security level, they also need to have the **View file's contents** access right for each document.
- **Modify folder attributes**: Users with this access right can modify the form attributes of the current folder or process (if they also have the **View folder attributes** access right).
- **Change form for folder**: Users with this access right can modify the type of the current folder by selecting a new form for it in the **Choose a folder type** drop-down list.

> ***This operation will make you lose all the attribute data, as it will not be available in the new form.***
> ***To select a new form for a folder, users also need to have the "View folder attributes" and "Modify folder attributes" access rights.***

- **Delete folder**: Users with this access right can delete the current folder using the **Delete current folder** tool. They can delete not only the folder, but also the children objects it contains, regardless of their individual access rights.
- **Delete folder contents**: Users with this access right can delete the documents located in the current folder. For databases with a **High** security level, they also need to have the **Delete document** access right for each document.
- **View folder log**: Users with this access right can view the log of the current folder or process by clicking the **Display the activity log for the selected folder** tool (from the Explorer), or the **Display the activity log for the selected object** tool (from the search utility).
- **Print folder content**: Users with this access right can print the documents located in the current folder. They also need to have the **View files' contents** access right. For databases with a **High** security level, they also need to have the **Print document** and **View file's content** access rights for each document.

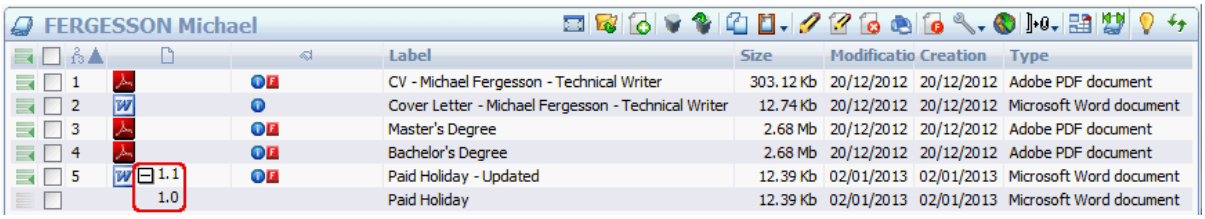
Access rights applying only to documents

The access rights that only apply to documents are the following:

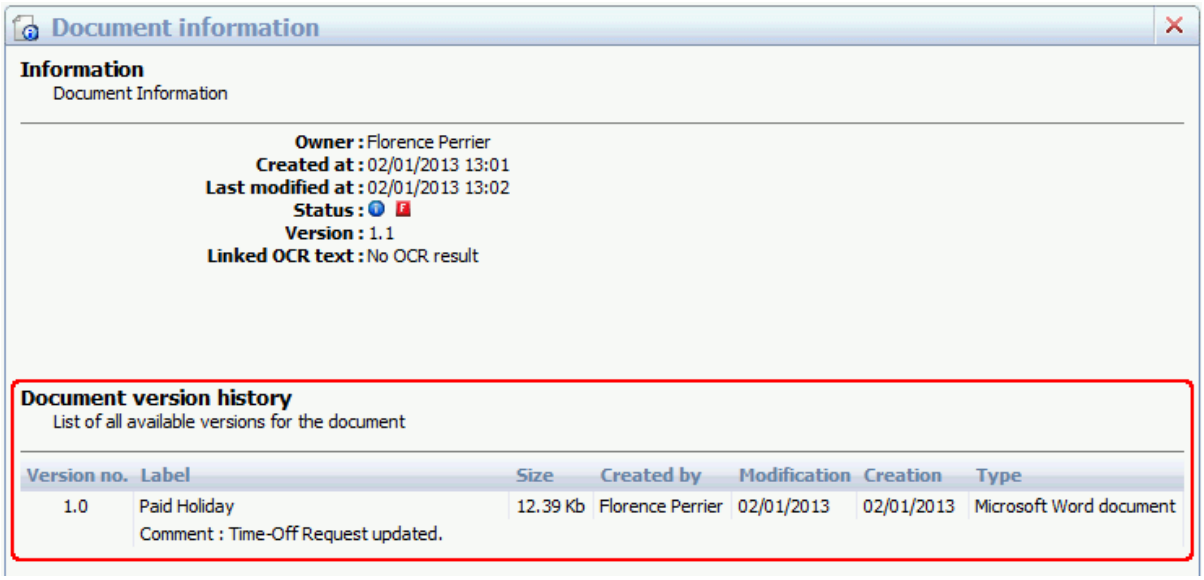
- **Create version**: Users with this access right can upload a new file and decide whether they want to replace the current document or create a new version of it, either major or minor. Without the corresponding additional access rights, they cannot download the current document, lock it, or view its previous versions.

> ***To create document versions, users also need to have the "View file's contents" and "Modify document" access rights, and the "View files' contents" access right at parent folder level.***

- **View versions**: Users with this access right can view the previous versions of the current document in the documents list:



They can also access the document version history using the **Document information** tool of the Web Client:



- **View document attributes**: Users with this access right can display the form of the current document and view the attributes in read-only mode.
- **View file's contents**: Users with this access right can view the content of the file associated to the current document (if they also have the **View files' contents** access right at parent folder level).
- **View source file**:
  - If PDF conversion is enabled on the database, the **View source file** access right is editable. Users with this access right can view the original version of the file associated to the current document, with the ActiveX plugin mode (and not only the HTML and PDF versions), if they also have the **View files' contents** access right on the document and at parent folder level.
  - If PDF conversion is disabled on the database, the **View source file** access right is not editable: the corresponding column displays in red. The PDF version of documents being unavailable, users can always access the original version, with the ActiveX plugin mode.
- **Modify document attributes**: Users with this access right can modify the form attributes of the current document (if they also have the **View document attributes** access right).
- **Change form for document**: Users with this access right can modify the type of the current document by selecting a new form for it in the **Choose a folder type** drop-down list.

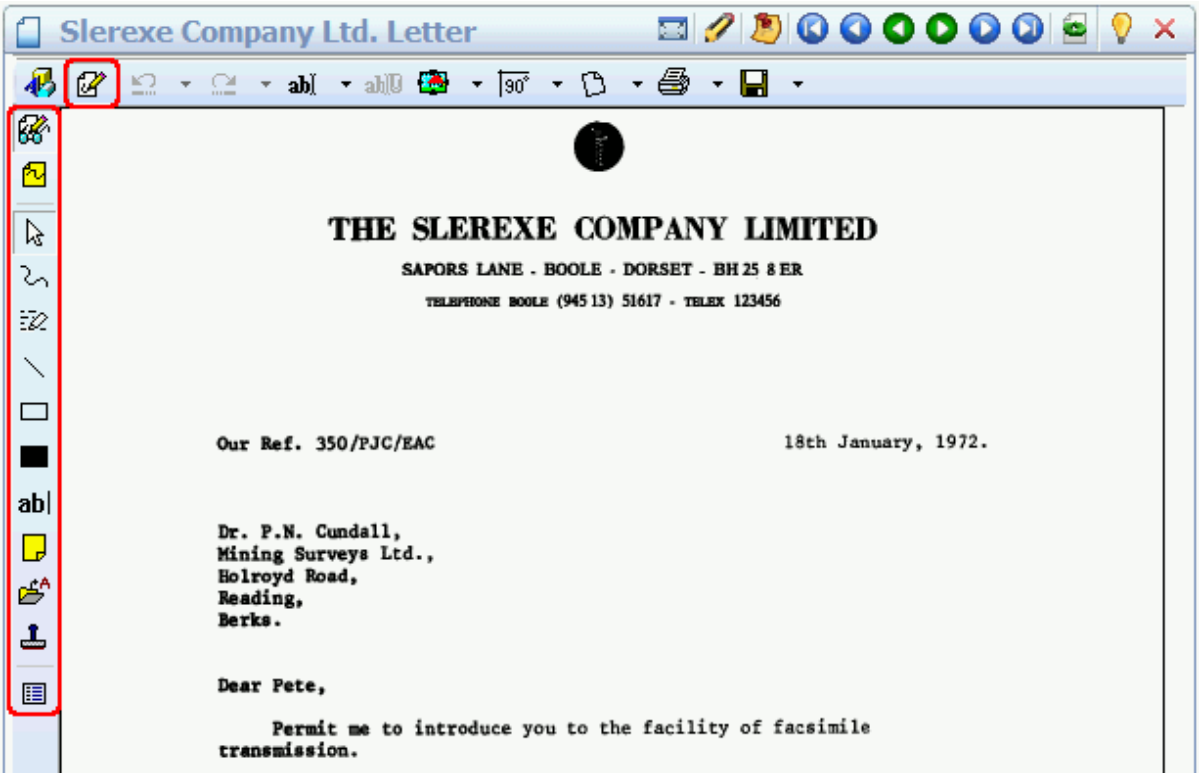
> ***This operation will make you lose all the attribute data, as it will not be available in the new form.***
>
> ***To select a new form for a document, users also need to have the "View document attributes" and "Modify document attributes" access rights.***

- **Temporary modifications**: This access right is not available yet.

- **Delete document**: Users with this access right can delete the current document (if they also have the **Delete folder contents** access right at parent folder level).
- **View document log**: Users with this access right can view the log of the current document by clicking the **Display the activity log for the selected document/object** tool.
- **Print document**: Users with this access right can print the current document. They also need to have the **View file's contents** access right and the **Print folder content** and **View files' content** access rights at parent folder level.
- **Pin**: Users with this access right can create and delete the pins containing the corresponding documents. They need to have this access right on all the documents of the pin.

> *To create and delete pins, users also need to have the **"Create objects"** access right at parent folder level.*

- **Annotate**: Users with this access right can use the **Annotations** toolbar of the activeX plugin to edit the .tif file associated to the current document:



> *To annotate a document, users also need to : be able to use the activeX plugin, have the **"View file's content"** and **"Modify document"** access rights, and have the **"View files' content"** at parent folder level.*

- **Modify document**: Users with this access right can upload a new file to replace the current document. They can also use the image editing tools of the activeX plugin. Without the corresponding

additional access rights, they cannot download the current document, lock it, or create a new version of it.

> ***To modify a document, users also need to have the "View file's contents" access right, and the "View files' contents" access right at parent folder level.***

- **Delete version**: Users with this access right can delete previous versions of the corresponding document using the tool of the Web Client.

> ***To delete previous versions of a documents, users also need to have the "View versions" and "Delete document" access rights, and the "Delete folder contents" access right at parent folder level.***

- **Download and email**: Users with this access right can download the current document and/or send it by email as an attachment, if they also have the **View file's contents** access right, and the **View files' contents** access right at parent folder level.
- **Sign digitally**: Users with this access right can sign digitally the current document using a digital certificate. If they have the **Sign physically** privilege, they can add an image signature to the document.

> ***To sign a document digitally, users also need to have the the "View file's contents" and "Modify document" access rights, and the "View files' contents" access right at parent folder level.***

- **Start a validation cycle**: Users with this access right can start a validation cycle and/or show its progress, using the tool of the Web Client.

Managing security profiles

Duplicating a security profile

You may want to duplicate a security profile, in order for example to create a slightly different one from the copy.

Proceed as follows:

1. In the left pane of the Administration Tool, expand the branch corresponding to the Gargantua database of your choice.
2. Click the **Security profiles** sub-branch.

   The list of security profiles displays in the right pane.

3. In the list, click the row of the security profile that you want to duplicate.
4. In the bottom left corner of the right pane, click the **Duplicate** button.

   A new security profile named “xxx **(1)**” displays in the list.

5. Click this new profile.

   The security profile management screen displays.

6. After applying the necessary modifications, click the the **Apply** button in the bottom left corner of the right pane.

   A new security profile based on the existing one has been created.

Exporting a security profile

You may want to export a security profile as an archive in .sxa format, in order to import it later into another database or onto another server.

Proceed as follows:

1. In the left pane of the Administration Tool, expand the branch corresponding to the Gargantua database of your choice.
2. Click the **Security profiles** sub-branch.

   The list of security profiles displays in the right pane.

3. In the list, click the row of the security profile that you want to duplicate.
4. In the bottom right corner of the right pane, click the **Export** button.

   A dialog allowing to select the objects to export displays.

5. Check the checkbox corresponding to the security profile to export, and click **OK**.

   The file explorer displays.

6. Browse to the local or remote folder where you want to save the .sxa export, and click **Save**.

   A confirmation message displays.

7. Click **OK**.

   The security profile selected has been exported. You can now import it into the database of your choice.

Importing a security profile

To import a security profile, proceed as follows:

1. In the left pane of the Administration Tool, expand the branch corresponding to the Gargantua database of your choice.
2. Click the **Security profiles** sub-branch.

   The list of security profiles displays in the right pane.

3. In the bottom right corner of the right pane, click the **Import** button.

   The file explorer displays.

4. Browse to the folder where you have saved the .sxa export, and click **Open**.

   A dialog allowing to select the objects to import displays.

5. Check the checkbox corresponding to the security profile to import.

   Unlike other objects, the security profiles that you import cannot override existing security profiles with the same name, even if you check the "Overwrite" checkbox.

6. Click **OK**.

   A confirmation message displays.

7. Click **OK**.

   The security profile has been imported: it is now at the end of the security profiles list.

Deleting a security profile

To delete a security profile, proceed as follows:

1. In the left pane of the Administration Tool, expand the branch corresponding to the Gargantua

database of your choice.

2. Click the **Security profiles** sub-branch.

   The list of security profiles displays in the right pane.

3. In the list, click the row of the security profile that you want to delete.
4. In the bottom left corner of the right pane, click the **Delete** button.

   A confirmation message displays.

5. Click **Yes**.

   The security profile selected has been deleted: it does not display in the security profiles list any longer.

You can only delete a security profile if it is not assigned to any production object.

Assigning a predefined security profile to an object in the Web Client

The assignment of a predefined security profile to an object in the Web Client requires the creation of this security profile in the Administration tool.

To assign a security profile to a folder, process, document or all objects in a database:

1. In the Web Client, click on the object to which you want to assign the security profile.
2. In the toolbar, click on the icon (**Access rights**).

   The access rights modification frame is displayed in the right pane.

3. In the drop-down menu of the **Predefined security profiles** field, click on the security profile of your choice, to assign it to the selected object.
4. If the current object already contains other objects and you want to assign to them the same security profile, check the **Subfolders** and/or **Documents** checkboxes, at the bottom of the frame.
5. Click on **Apply**.

   A confirmation message is displayed. The security profile has been assigned to the current object and, if required, to its children.

Assigning a custom profile to an object

Instead of assigning a predefined security profile to an object, you can assign a **custom profile** to it. A custom profile allows you to assign rights to specific objects.

This feature is helpful in the following cases:

- If you have never defined any security profile in the Administration tool;
- For a subfolder or a document: if a folder already has a security profile but you do not want to assign it to all its subfolders or documents.

However: assigning too many custom profiles can easily bring confusion. Indeed, it can be hard to know which objects are assigned to a custom or predefined security profile. That is why it is strongly recommended to only use predefined security profiles.

To assign a custom security profile to an object:

1. In the Web Client, click on the object to which you want to assign the security profile.
2. In the toolbar, click on the icon (**Access rights**).

   The access rights modification frame is displayed in the right pane.

3. In the drop-down menu of the **Predefined security profiles** field, select **Custom profile**.
4. Check the checkboxes of the access rights table, depending on the rights you want to assign to the different users, groups or roles for this object.
5. If the current object already contains other objects and you want to assign them the same custom security profile, check the **Subfolders** and/or **Documents** checkboxes, at the bottom of the frame.
6. Click on **Apply**.

   A confirmation message is displayed. The custom security profile has been assigned to the current object and, if required, to its children.

Assigning a custom profile based on a predefined security profile to an object

If you want to assign a custom security profile to a specific object, based on a predefined security profile:

1. In the Web Client, click on the object to which you want to assign the security profile.
2. In the toolbar, click on the icon (**Access rights**).

   The access rights modification frame is displayed in the right pane.

3. In the drop-down menu of the **Predefined security profiles** field, click on the security profile of your

choice.

The access rights table is filled according to the chosen security profile.

4. Click on the **Custom profile** button: you can now define a custom security profile based on the predefined one, for the current object, by checking or unchecking several rights.

   The message **Selected security template is modified** is now displayed above the table.

   However, be careful: this custom profile will not be automatically updated if the predefined profile is changed in the Administration tool. Custom profiles can be tricky!

   The Clear button allows you to define a custom profile from an entirely empty table.

5. If the current object already contains other objects and you want to assign them the same custom security profile, check the **Subfolders** and/or **Documents** checkboxes, at the bottom of the frame.
6. Click on **Apply**.

   A confirmation message is displayed. The custom security profile has been assigned to the current object and, if required, to its children.