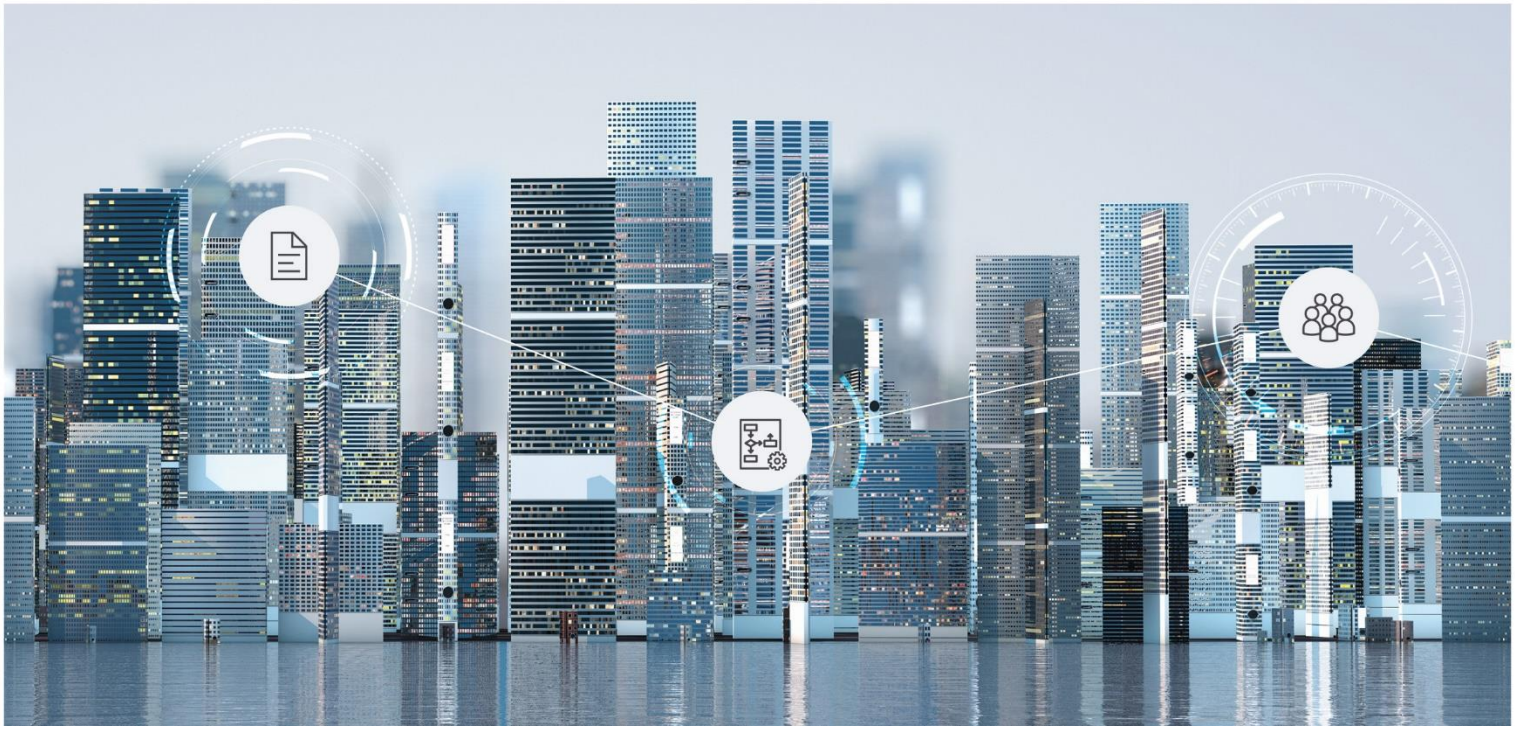
Fabasoft



White Paper

Fabasoft Folio Access Definitions

Fabasoft Folio 2023 Update Rollup 2

Contents

1 Introduction

This document describes the use of access definitions in Fabasoft Folio.

2 Software Requirements

System environment: All information contained in this document implicitly assumes a Microsoft Windows environment or a Linux environment.

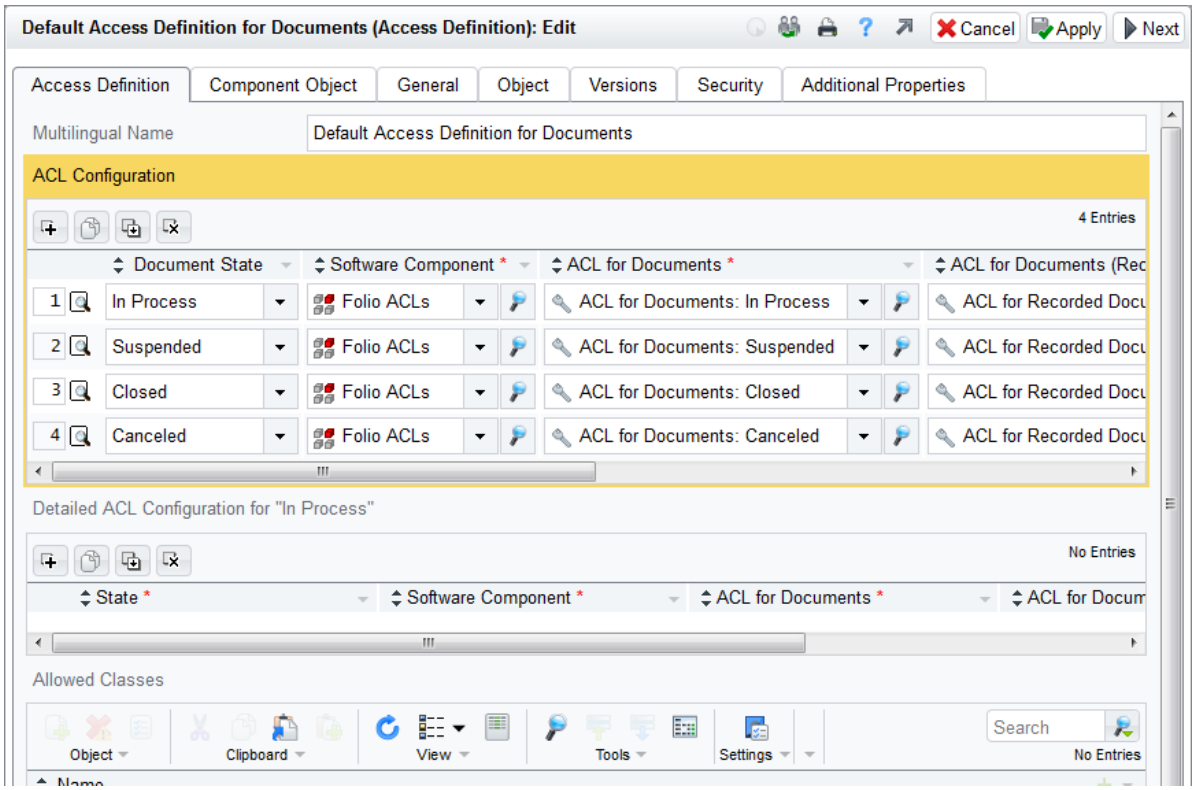
Supported platforms: For detailed information on supported operating systems and software see the software product information on the Fabasoft distribution media.

3 Access Definitions

By means of access definitions the ACLs for each single status of an object are defined.

3.1 Structure of an Access Definition

An access definition is structured as follows:

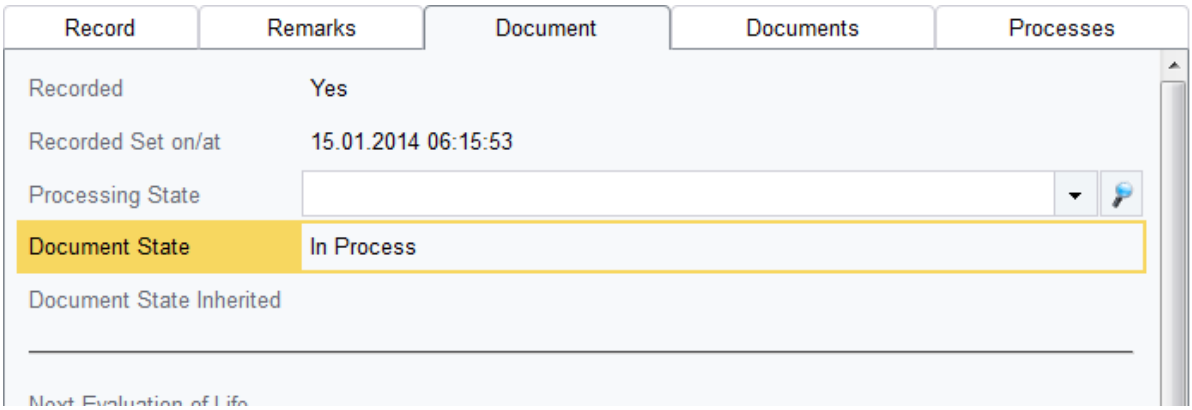


- *Multilingual Name*
  Name of the access definition.
- *ACL Configuration*
  In this composite property the ACL for each document state is set. In addition, the ACL for each state of a recorded document (registered document) is set.
- *Detailed ACL Configuration for "In Process"*
  In this area a specific definition for the "In Process" state can be entered.

- *Allowed Classes*
  In this area the object classes are entered, for which the access definition can be used.

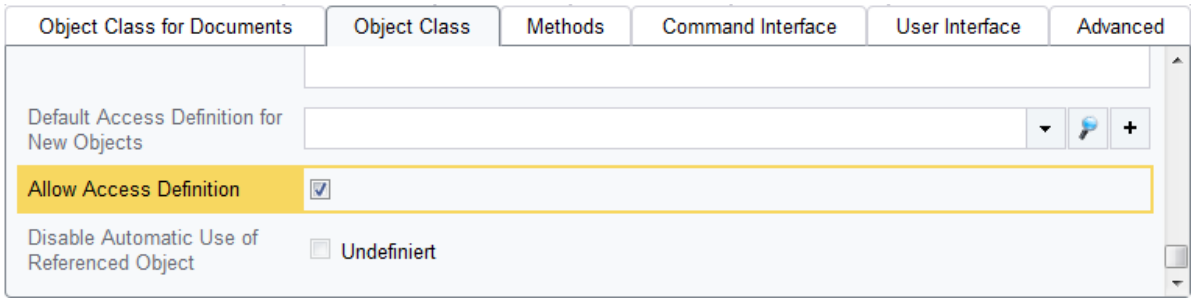
Example for ACL assignment: According to the access definitions shown above, for a free object with status "In Process" the ACL *ACL for Documents: In Process* applies.

Note: The state of an object can be seen on the "Document" tab in the *Document State* field.

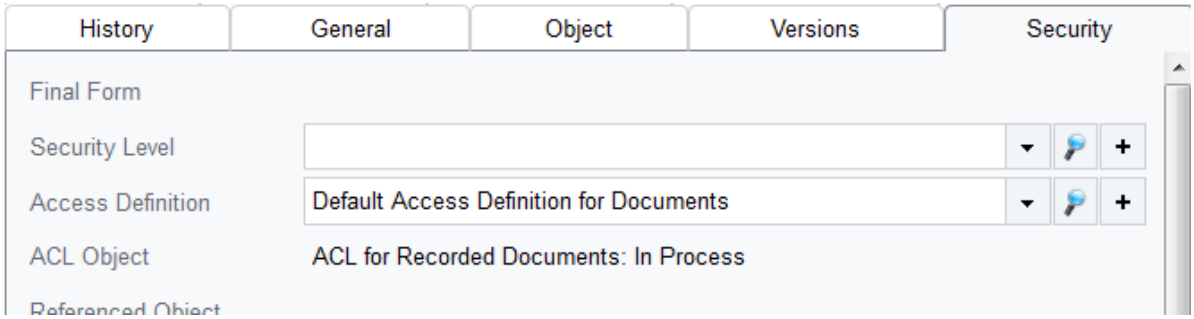


3.2 Select Access Definition

Access Definitions are selected on the "Security" tab in the *Access Definition* field. The ACL calculated from the access definition is entered in the *ACL Object* field. Per default business objects (Record, Case, Incoming, Outgoing) obtain the *Standard Access Definition for Documents*. Content objects per default do not get an access definition, except in the object class on the "Object Class" tab *Allow Access Definition* has been selected and the access definition has been propagated (see chapter 3.6 "Propagating Access Definitions").

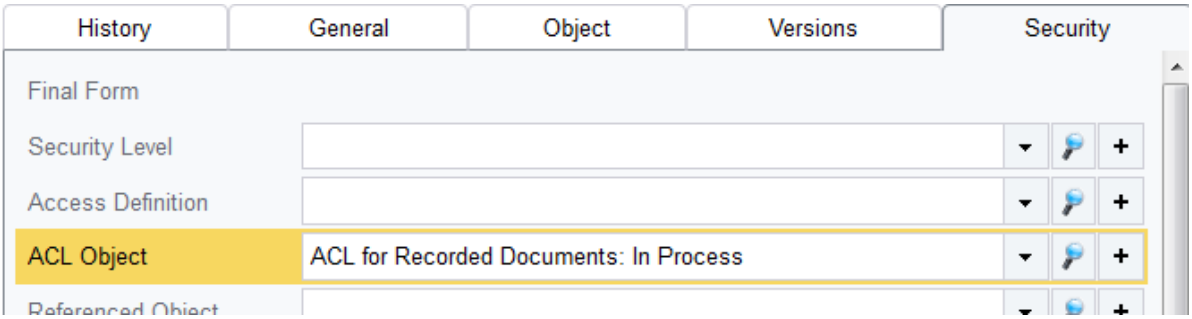


If an access definition is defined the ACL object cannot be changed.



3.3 Remove Access Definition

If an access definition is removed, still the ACL is valid for the object. The ACL object can then be changed.



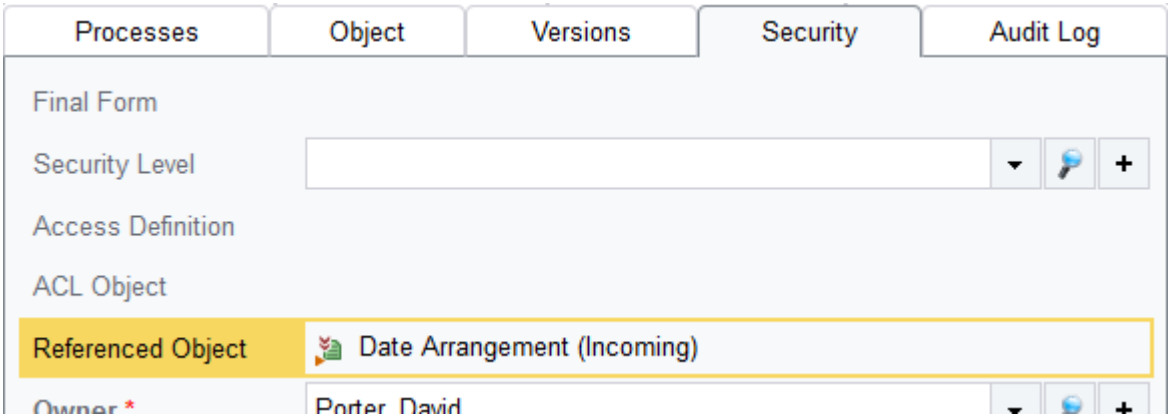
3.4 Select ACL

On the "Security" tab in the *ACL Object* field an ACL for the object can be selected. The ACL object can only be changed if no access definition has been set.

3.5 Referenced Object

On the “Security” tab the *Referenced Object* field is available. If an object is entered in this field, the security settings of the referenced object are taken.

A referenced object is automatically entered in child business objects and content objects, if the condition for propagation is satisfied (see 3.6 “Propagating Access Definitions”).).



The following settings are taken from the *Referenced Object*:

- *ACL Object*
  The *ACL Object* of the *Referenced Object* also applies to the current object.
- *Change Access*
- *Read Access*
- *Propagated Users/Groups With Change Access*
- *Propagated Users/Groups With Read Access*
- *Propagated Security*

To define own security settings (independent from the *Referenced Object*), the referenced object has to be removed from the *Referenced Object* field. Subsequently, the *Access Definition* and the *ACL Object* can be changed.

3.5.1 Disabling Automatic Referencing

In some cases one would like to prevent the use of the referenced object for automatically evaluating the ACL and use another ACL for the current object instead. In Fabasoft Folio there are two possibilities to disable automatic referencing.

3.5.1.1 Disabling Automatic Referencing via Document Category

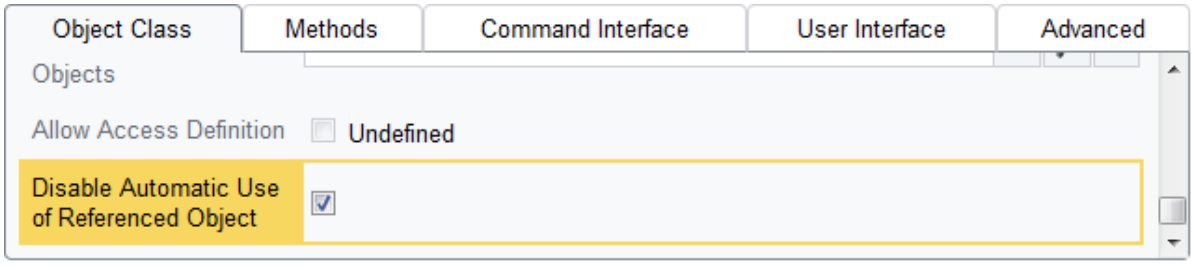
For objects of the object class *Document Category* the property *Disable Automatic Use of Referenced Object* is available. If this property is selected, the referenced object is not automatically set when objects of this document category are recorded. Instead only the access definition and the ACL are entered. Subsequently, the entered ACL is evaluated on the current object.

When changing the property *Disable Automatic Use of Referenced Object* of a document category, the existing objects of this document category remain untouched. The property *Disable Automatic Use of Referenced Object* is only evaluated when recording, rerecording or derecording an object.

Exception: The property *Disable Automatic Use of Referenced Object* is not evaluated if a content is recorded to a document. In this case, the document is always entered as referenced object for the content, because the content and the document form a unit.

3.5.1.2 Disable Automatic Referencing via Object Class

Analogously to the document category, the *Disable Automatic Use of Referenced Object* property is also available in object classes. By means of this property the use of the referenced object can be disabled domain-wide for a specific object class.



Note: If the use of the referenced object is deactivated for an object class, this cannot be overridden by the document category and so be canceled. By means of the *Disable Automatic Use of Referenced Object* property, the use of a referenced object can only be prevented and it is not possible to override a disabled referencing.

3.6 Propagating Access Definitions

Security settings are propagated to child business objects and content objects as a *Referenced Object*. The access definition is specified in the object class in the *Default Access Definition for New Objects* field ("Object Class" tab). An inheritance is possible considering the following condition:

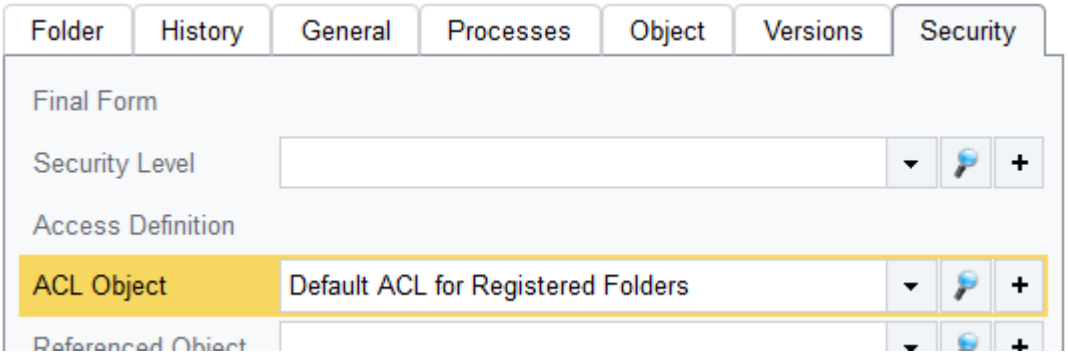
- *Access Definition* and *ACL Object* match the security settings of the parent business object.

Examples:

- If in a non-recorded case using the *ACL for Documents: In Process* an incoming is created, the incoming gets the *ACL for Recorded Documents: In Process*. The case is not entered as *Referenced Object* in the incoming.
- If in a non-recorded case an outgoing is created, *Access Definition* and *ACL Object* are consistent. The case is entered as *Referenced Object*.
- If in a non-recorded case a content object is created, the case is referenced in the content object. If the content object is recorded in the non-recorded case, the content object gets a new ACL and the referenced object is removed.

If in the object class the *Default ACL for New Objects* is defined, the new created object gets this ACL. The ACL applies only to objects of this object class and is not inherited.

Exception: A folder in a business object (a recorded folder) does not inherit the security settings, because it is only used for structuring the business object. Per default the folder gets the *Default ACL for Registered Folders*. However, the ACL for each state can be defined analogously to the documents via access definition. The default ACL can be defined in the Folio configuration (see 3.8 "Configuration of Access Definitions").



3.7 Access Definitions in Templates

Templates take a special position in regard to security settings.

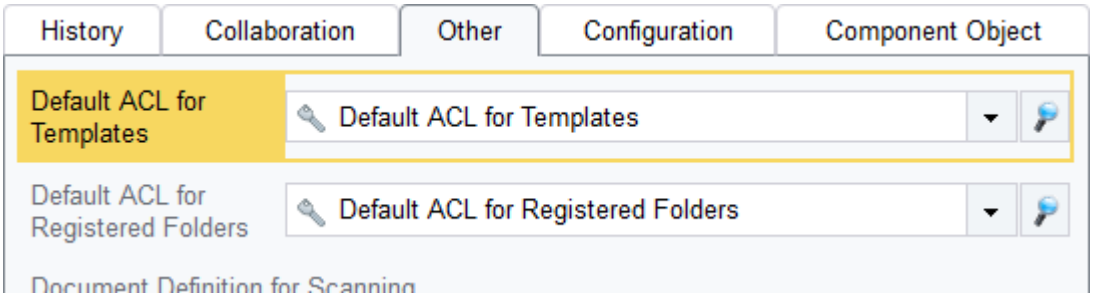
- Select access definition
  In templates it is technically possible to select an access definition. Since there are not state transitions in templates, selecting an access definition does not make sense.
- ACL object
  Per default a template receives the *Default ACL for Templates* (see 3.8 "Configuration of Access Definitions"). However, this ACL can be changed.
  If an object is created using a template, for the new object the conventional security settings are applied, regardless of the ACL of the template.
- ACL definition via referenced object
  In templates a *Referenced Object* can be defined, so that the security settings of the referenced

object are applied.
Note: The referenced object can only be specified when the ACL has been removed.

- State transitions of templates
  With templates, there are no state transitions.
- Referenced object
  Objects that are created based on a template get the ACL of the *Referenced Object* (assuming propagation is possible) and not the *Default ACL for Templates*.
- The template settings are only used for the initial security settings of objects that are created based on the template. A later change of the security settings in the template is not inherited.

3.8 Configuration of Access Definitions

In the Folio configuration on the "Other" tab in the fields *Default ACL for Templates* and *Default ACL for Registered Folders* their default ACLs can be defined.



3.9 Common Guidelines to Specify the Security Settings

Access Definitions can only be selected in object classes that are listed as *Allowed Classes* in the *Access Definition*. End users have the following options to specify security settings:

- For business objects
  Access definitions can be changed. The ACL object is set according to the access definition and can only be changed when the access definition has been removed.
- For content objects where access definitions are not allowed
  - Non-recorded content objects:
    No access definitions can be defined, provided no access definition has been set. The security setting can be changed via ACL object.
  - Recorded content objects
    The access definition can be changed. The ACL object is set according to the access definition and can only be changed, when the access definition has been removed.
- For content objects where access definitions are allowed:
  - Non-recorded content objects
    No access definitions can be defined, provided no access definition has been set. The security setting can be changed via ACL object.
  - Recorded content objects
    The access definition can be changed. The ACL object is set according to the access definition and can only be changed when the access definition has been removed.