Security in Odoo

Aside from manually managing access using custom code, Odoo provides two main data-driven mechanisms to manage or restrict access to data.

Both mechanisms are linked to specific users through *groups*: a user belongs to any number of groups, and security mechanisms are associated to groups, thus applying security mechamisms to users.

**Access Control**

Managed by the ir.model.access records, defines access to a whole model.

Each access control has a model to which it grants permissions, the permissions it grants and optionally a group.

Access controls are additive, for a given model a user has access all permissions granted to any of its groups: if the user belongs to one group which allows writing and another which allows deleting, they can both write and delete.

If no group is specified, the access control applies to all users, otherwise it only applies to the members of the given group.

Available permissions are creation (perm\_create), searching and reading (perm\_read), updating existing records (perm\_write) and deleting existing records (perm\_unlink)

**Record Rules**

Record rules are conditions that records must satisfy for an operation (create, read, update or delete) to be allowed. It is applied record-by-record after access control has been applied.

A record rule has:

* a model on which it applies
* a set of permissions to which it applies (e.g. if perm\_read is set, the rule will only be checked when reading a record)
* a set of user groups to which the rule applies, if no group is specified the rule is *global*
* a [domain](https://www.odoo.com/documentation/10.0/reference/orm.html#reference-orm-domains) used to check whether a given record matches the rule (and is accessible) or does not (and is not accessible). The domain is evaluated with two variables in context: user is the current user's record and time is the [time module](https://docs.python.org/2/library/time.html)

Global rules and group rules (rules restricted to specific groups versus groups applying to all users) are used quite differently:

* Global rules are subtractive, they *must all* be matched for a record to be accessible
* Group rules are additive, if *any* of them matches (and all global rules match) then the record is accessible

This means the first *group rule* restricts access, but any further *group rule* expands it, while *global rules* can only ever restrict access (or have no effect).

Warning

record rules do not apply to the Administrator user

although access rules do

**Field Access**

New in version 7.0.

An ORM [Field](https://www.odoo.com/documentation/10.0/reference/orm.html#odoo.fields.Field) can have a groups attribute providing a list of groups (as a comma-separated string of [external identifiers](https://www.odoo.com/documentation/10.0/glossary.html#term-external-identifiers)).

If the current user is not in one of the listed groups, he will not have access to the field:

* restricted fields are automatically removed from requested views
* restricted fields are removed from [fields\_get()](https://www.odoo.com/documentation/10.0/reference/orm.html#odoo.models.Model.fields_get) responses
* attempts to (explicitly) read from or write to restricted fields results in an access error

**Workflow transition rules**

Workflow transitions can be restricted to a specific group. Users outside the group can not trigger the transition.