

# Include Permissions

---

Daisy allows to do inclusions in documents. This can be either other Daisy documents (through the "daisy:" syntax) or when published through the Daisy Wiki, any URL resolvable by Cocoon (the framework on which the Daisy Wiki is implemented). However, allowing document authors to include any arbitrary URL might introduce security issues. For example, one could retrieve content from the file system using a "file:" URL. Also, the "http:" URLs are resolved behind the firewall (if any) which might be a problem too.

Therefore, by default, all external inclusions are disallowed. You can give access for certain schemes or URLs through a configuration file. This file is located at:

```
<wikidata directory>/external-include-rules.xml
```

This file has a `<rules>` root element containing `<rule>` children:

```
<?xml version="1.0"?>
<rules>
  <rule ... />
  <rule ... />
</rules>
```

Each rule element can have the following attributes:

- `scheme`: http, file, cocoon, etc.
- `value`: the value which should be checked, is one of: uri, host, ip (host and ip do not make sense for all schemes)
- `matchType`: how the value should be matched, one of:
  - string
  - stringIgnoreCase
  - wildcard
  - wildcardIgnoreCase
  - regexp
  - regexpIgnoreCase
  - subdir (see further on for more details)
- `matchValue`: the value (or regexp or wildcard expr) to be matched against
- `portFrom` (optional, only for HTTP)
- `portTo` (optional, only for HTTP)
- `permission`: grant or deny

There are two possibilities:

- either the `<rule>` element has only the scheme and permission attributes, to globally allow a scheme
- or it has all attributes (except for the optional `portFrom` and `portTo`)

Evaluation of the rules:

- start situation: all inclusions are denied.
- all rules are processed, top to bottom, later results overwriting earlier results.

Example:

```
<?xml version="1.0"?>
<rules>
  <rule scheme="http" value="uri" matchType="stringIgnoreCase"
```

```
    matchValue="http://www.somehost.com/somefile.xml" permission="grant"/>
<rule scheme="http" value="ip" matchType="wildcard" matchValue="67.19.2.*"
    portFrom="80" portTo="80" permission="grant"/>
<rule scheme="http" value="host" matchType="stringIgnoreCase"
    matchValue="blogs.cocoonddev.org" permission="deny"/>
<rule scheme="cocoon" value="uri" matchType="wildcardIgnoreCase"
    matchValue="cocoon://daisy/ext/**" permission="grant"/>
<rule scheme="file" value="uri" matchType="subdir"
    matchValue="/home/bruno/tmp" permission="grant"/>
</rules>
```

Some more notes on the matchtypes:

- `wildcard` uses the cocoon wildcard matcher. This means one `*` matches any character except for slash (`/`), while `**` matches any character
- `regexp` uses the default Java regexp engine. You will usually want to start them with `^` and end them with `$`.
- `subdir` is a special case, which should only be used with the file scheme. It constructs a `java.io.File` object for the value and the `matchValue`, takes their canonical path (which is absolute and unique), and check whether the first starts with the second.

Further notes:

- changes to the `external-include-rules.xml` file are immediately detected, thus do not need a restart of the Daisy Wiki.