Authentication in Megaladata

In the server editions, you must log in to use Megaladata. For this purpose, you need to authenticate using one of the following methods:

- Entering a username and password on the home page
- Using your login and password in the URL
- Using the LDAP server (for the Enterprise edition)
- Using OpenID (for the Enterprise edition)

Your login and password should be provided by the administrator, but there is a default user login configured for the case of software installation: `user`, with no password.

Authentication in URL

Generally, URL with authentication parameters is as follows:

```
http://login:password@address
```

where

- `login`: User's login name. Can contain letters (A–Z, a–z), digits (0–9), and the characters "_", "-", "." (underscore, hyphen, period). Spaces must be URL-encoded (as %20). Other special characters may also require URL encoding.
- `password`: Can contain any characters.
- `address`: URL address of the Megaladata server web interface.

▼ URL examples

> ```
> http://user@localhost/app/
> ```
>
> ```
> http://viewer:12345@support/app/
> ```

It is possible to combine such authentication method with LDAP.

> Authentication in URL is not available in Safari. Configuration is required in Firefox.
> If Megaladata is accessed from the Internet, it is recommended to configure the server for operation via the HTTPS protocol.

Firefox settings

In Firefox 128.0 and below, a warning may be displayed when transferring authentication parameters to URL. To avoid the warning, configure the Apache server to request HTTP Basic authentication.

▼ Example of Firefox configuration for localhost

Along with `http://localhost/app/`, create a web server alias (e.g., `http://localhost/app-basicauth/`) pointing to the application's original path (e.g., `/app/`). When this alias URL is accessed via Firefox, the Apache configuration below will trigger HTTP Basic authentication.

You need to create a password file (commonly named `.htpasswd`) containing usernames and hashed passwords. Refer to the official Apache documentation on htpasswd for instructions. In case you only need to configure the default user access (login: `user`, no password), all you need to do is add a line containing "`user`" and empty password in the `.htpasswd` file.

In the Apache configuration file `studio.site.conf`, set HTTP Basic Auth for `http://localhost/app-basicauth/` and specify the path to `.htpasswd`:

```
<If "%{HTTP_USER_AGENT} =~ /Firefox/ && %{REQUEST_URI} =~ /\/app-basicauth\//">
    AuthType Basic
    AuthName Documents
    AuthBasicProvider file
    AuthUserFile "/path/to/.htpasswd"
    Require valid-user
</If>
<Else>
    Require all granted
</Else>
```

As a result, when accessing the alias URL (`http://localhost/app-basicauth/`) via Firefox, the browser should prompt for credentials with the following message: "You are about to log in to the site "localhost" with the username "user"".

OpenID authentication

A user can also log in via OpenID authentication using *AccessToken*. The token contains information about the user's roles and rights to access shared folders. This information would be extracted and used for authentication.

To use this login technique, you need to first set up the **OpenID parameters** on the Administration page. If these are not configured, OpenID authentication will not be employed.

After the necessary parameters have been set up, a new button will appear on the login page: **Login with OpenID**.

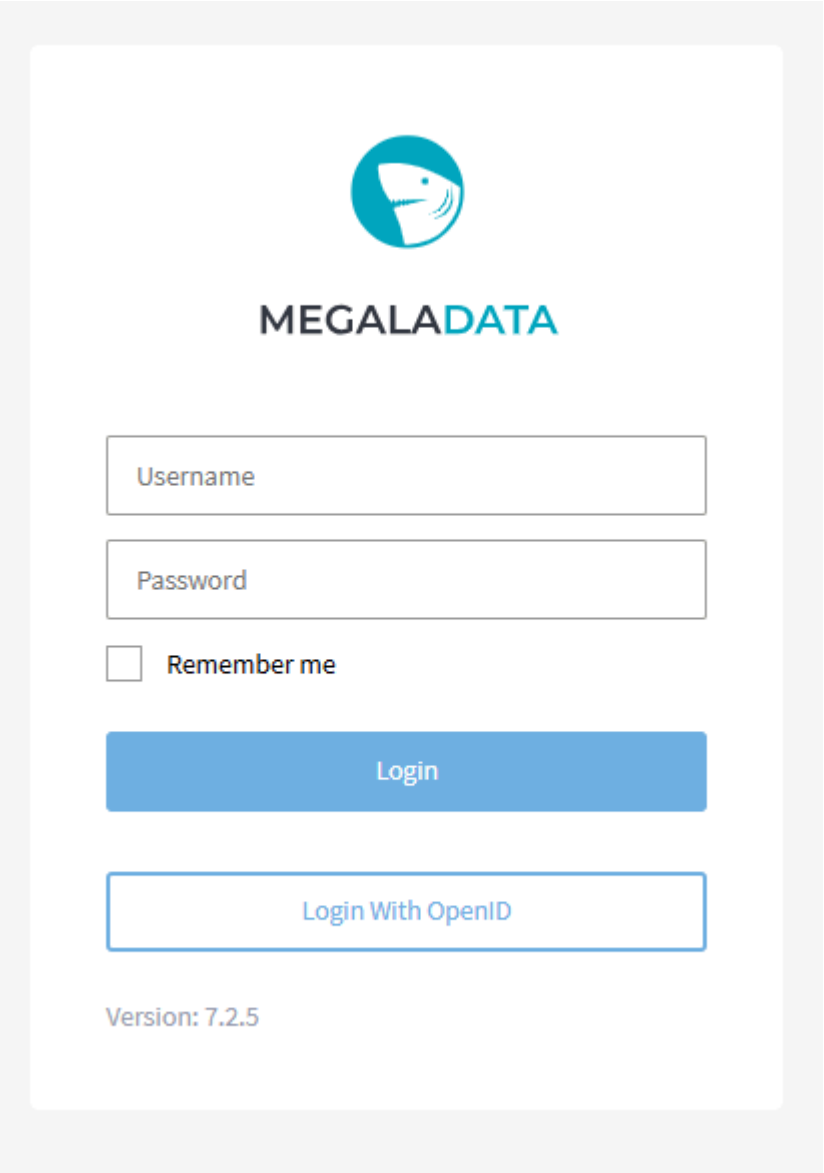

Figure 1. Login page

Clicking this button redirects to the identification control page, where the user can enter their login and password (the single sign-on scheme).

To set up the OpenID authentication mode, use the configuration file.

Read on: Package Structure and Usage