Security

Authentication

Authentication is based on username/password.

Optionally 2-factor authentication can be set up using af mix of

- SMS sent to phone
- IP address of callers

Single sign on (optional)

Single sign on integration is included for

- ADFS
- LDAP (and AD)
- Google, Azure, Facebook, LinkedIn

A group membership synchronization exists for

- ADFS
- LDAP

Anonymous users (optional)

External users can access data via the following methods

- Create new records: Public link
  - Services can be protected by a CAPTCHA test
- Edit existing records: Specific link sent to user
  - Links can expire after certain amount of time

Authorization

User permissions are granted via inheritable group membership

Authorization schemes

- Field level control
- State model
- Data ownership

Additionally special roles can be assigned

- Administrator (backend)
- Bulk operations

Encryption

Transport encryption is based on SSL via HTTPS policies

- Cloud hosting includes option for free SSL certificates

Storage encryption is best handled via operating system measures

- Linux: LUKS
- Windows: Bitlocker

Passwords are hashed using BCrypt algorithm.

Protection

Platform complies with all requirements in OWASP level 2

- Hacking: SQL injection, XSS, CSRF
- Password policies

Revision #1
Created 7 April 2025 12:38:19 by Theis Villumsen
Updated 7 April 2025 12:38:53 by Theis Villumsen