

efalia ecm

# Security

## Accounts

Efalia ECM is a system that combines security with flexibility.
User and rights management always ensures that documents are only available to users who have previously been assigned the appropriate permissions, regardless of the type of login used for the system:

- Efalia ECM Built-in accounts
- Microsoft Windows accounts
- Microsoft Active Directory accounts
- Microsoft Azure Active Directory Accounts

Efalia ECM accounts can each be configured with an expiry date so that access to the data expires automatically at the end of an internship or an audit, for example.
For easier security management within the Efalia ECM system, individual user accounts can then be sorted into groups.

- **User and rights management**
- **2-Factor-Authentication**
- **Encryption**

## Encryption

Efalia ECM Server is an IIS web service and therefore not only benefits from IIS encryption options and the use of appropriate certificates to protect the data traffic between server and client.
The Efalia ECM system itself also offers various options for encrypting the data it stores.
Thus, in addition to encryption within the Efalia ECM Container option, AES256 encryption at file level is also available.

## 2-Factor-Authentication

The 2FA provides additional security for systems that use Efalia ECM accounts or Microsoft Azure Active Directory accounts for user login.
This protection can be activated per account.
For these accounts, a code is required in addition to the user password, which is generated by a Microsoft or Google Authenticator.
Of course, the validity can also be set individually.



efalia ecm

# Security

## Data Access

The basic structure in Efalia ECM is a cabinet.
A system can contain several cabinets.
The cabinets are structured into document types, which in turn can be linked to fields.

- Efalia ECM System
    - Cabinet
        - Document Type
            - Fields

Each of the above elements also represents a level that can be used to define access rights.
To access a document, a Efalia ECM account must have permissions for the cabinet and the corresponding document type. Even if an account has permissions at these two levels, individual documents within a document type can be excluded from access via filters at field level.
All security settings within cabinets, can be set for an individual user or a groups.

- **Controlled Access**
- **Audit Trail**
- **Blacklist**

## Auditing

All activity within the Efalia ECM can be logged, and exported for future reporting.
For each document, a history is kept that holds details on the activities associated with the document.
These details include information about the account, the action and the time an activity took place.
In this way, it is always traceable when and by which account a transaction was done.

## Additional Protection

Efalia ECM goes even further. In addition to the numerous possibilities within user and rights management, the system offers additional protection via a blacklist. This ensures that suspicious accounts or IP addresses are automatically blocked as soon as a defined threshold value is reached.

efalia
smart content suite on a human scale

Information in this brochure is correct at the time of publication, but due to on-going development, product specifications are subject to change without notice. Errors and omissions excepted.
Copyright © 2024 Efalia GmbH. All other trademarks are the property of their respective companies.