Apparo Fast Edit

Encryption

Version 3.3

1 Encryption in database and XML files

Apparo Fast Edit is automatically encrypting passwords and connection settings with AES 256.

Affected are database and email connections stored in the Apparo repository database or stored in XML files after exporting the connections.

1.1 Encryption of database connections

The following settings of DB-connections are encryted in the repository database and exported XML files:

Username, password, port, dbname, sql commands and additional parameters

1.2 Encryption of email connections

The following settings of email-connections are encryted in the repository database and exported XML files:

Username, host, recipient email address, trusted servers, pop & smtp username, pop & smtp password

1.3 Encryption of Apparo Configuration XML files

In the following settings of the Apparo Configuration Manager and in the file configuration_32.xml:

Windows service user password, passwords for SSL certificates, LDAP and Active Directory credentials

1.4 Encryption of user logins

The Qlik and ÍBM Cognos Analytics versions are embedded and are using the portal and security system of the underlying BI system. The encryption is therefore managed by Qlik or IBM Cognos Analytics.

The standalone version is usually using Active Directory, which is managing the encryption.

We recommend to always use SSL in all versions.

1.5 Usage of encrypted (password) strings

It is possible to copy the encrypted pass strings and use it directly. The advantage: Designer users do not know the passwords when creating connections.

Syntax:
CRYPTED:PASS-STRING

Application areas:

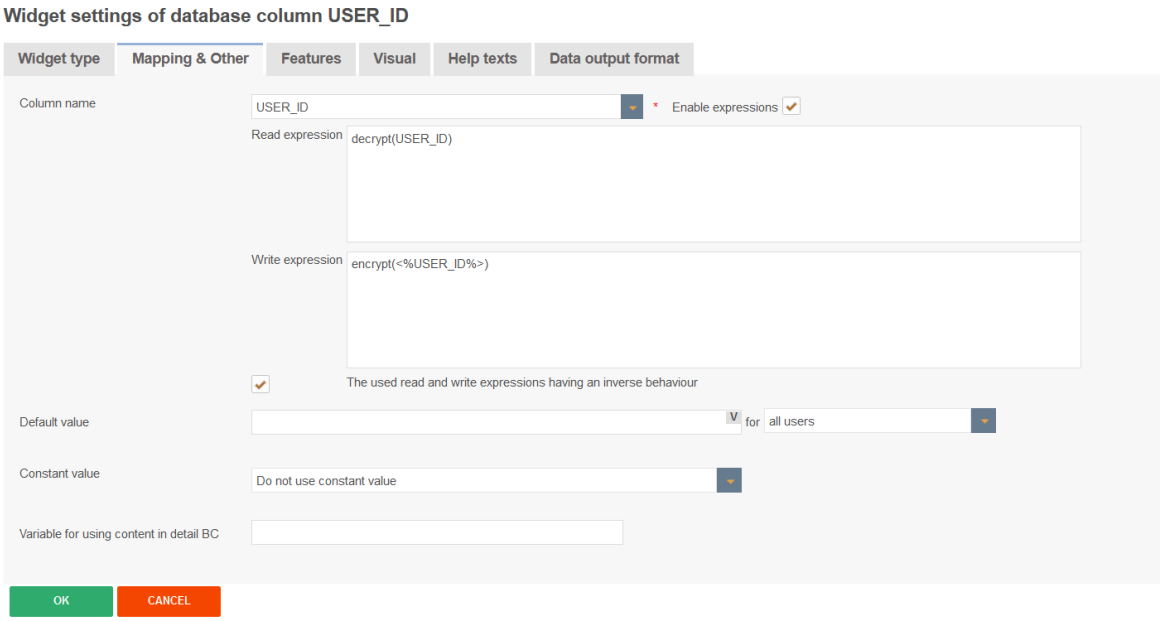
- In Apparo Configuration Manager settings of another installation (e.g. test, development, multi environment application servers)
- In database connections
- In email connections

2 Data encryption

Data encryption is usually done at database level.

2.1 Encryption on widget level

In some cases, where only certain database columns need to be encrypted, this can be done using expressions:



2.2 Password style output

All widgets also can be setup to hide the entered data with password style:

This can be activated in the features tab: