Protection and Application of User Login Data

The given user rights regulate the access to cell data and to selected system operations. Jedox stores level 1 and 2 right objects and users and their passwords in the Jedox In-Memory Database system. For information on regulating user access to Jedox data, see Administration of User Rights. To create a special Jedox administrator account with limited access rights, see Admin User Accounts.

Requests for a Jedox database can only be made with a valid login. These logins must be adequately protected with passwords. The Jedox databases are special CSV files in the directory `..\olap\data`. To avoid unwanted access to these files, this directory should be protected using the existing security options of the operating system and additional encryption algorithms.

By default, the password for the admin user, as well for other users, is stored within the System database in system cube #_USER_USER_PROPERTIES. The password is stored using a PBKDF2 algorithm with more than 4000 iterations and random salt. The cube #_USER_USER_PROPERTIES corresponds to the file database_CUBE_0.csv. Everyone who has read/write access to these files can see/change the content. Therefore, it is necessary to protect this system database accordingly.

Note: To use the PBKDF2 algorithm, you need to change the passwords stored in older versions of Jedox. You only have to do this

once.

You can no longer retrieve user passwords from the **System** database via the In-Memory Database API. The API calls that retrieve the cell value of the “password” element return an access right error for anyone making the call, regardless of the user rights.

If you need password retrieval for debugging purposes, you can enable it in the `palo.ini` configuration file by setting the following entry: `enable-password-retrieval`.

Note: In future versions of Jedox the option of changing a password through direct cell writeback will no longer be possible. You will only be able to change a password in the UI of Jedox Web and the Excel Add-in, or using the API function CHANGE_PASSWORD. Groovy scripts in Integrator also allow you to change your password.

Setting a password policy

The parameter `password-pattern` in palo.ini allows you to change the password settings concerning the password length and the password pattern/complexity. Any attempt to change the password password changing attempt that does not match the defined pattern will result in an error displayed in the Change Password dialog. The password pattern can be defined by the key `password-pattern <regular_expression>`. If the new password does not match the pattern, an error message (error code 1004) is returned.

Currently, Jedox users are not automatically prompted to change their password.

Note for Jedox Web users: In the Jedox Web connection dialog, the mark the **Use login credentials** checkbox to use the assigned rights. Otherwise, Jedox Web will use the rights of the user name entered for the connection. Access rights can be defined for connections in a similar way to other objects, on the **Security** dialog of a connection. For example, a connection that statically applies to a user with high-level access (e.g. for Jedox Integrator) can be set to be inaccessible to lower-level user groups.

Unprotected connections can be used by any given Jedox user, such as in the In-Memory Database-related dialogs (e.g. **Paste View**).