Security configuration

This dokument describes the Security configuration for login as a user.

Password security

ttkf.server.security.password.reset.active

Default: false
Possibility: true | false

This is the global option to enable (true) or disable (false) the password management service that enforces the rules governing password security.

ttkf.server.security.password.history.size

Default: 4
Possible value: 1-N

Specifies the number of passwords in the history. A new user password must be different from the ones contained in the history. Each user has their own history.

The server provides restrictions for new passwords.
The following restrictions exist:

- Minimum character length (default 7)
- Username may not be contained in password
- First and last name may not be contained in password.
- RegEx condition. Default settings are:
  - At least one lower case character.
  - At least one upper case character.
  - At least one number.
  - At least one special character.

  By default, 3 of the 4 conditions must be met.

- The last N passwords of a user cannot be re-used as new password.

<u>The following optional settings exist to configure the password restrictions:</u>

ttkf.server.security.password.min.length

Default: 7

Minimum character length for a new password.

ttkf.server.security.password.regex.condition.enable

Default: true
Possibility: true | false

Activate the regex conditions for new passwords. The conditions are:

- At least one lower case character.
- At least one upper case character.
- At least one number.
- At least one special character.

ttkf.server.security.password.regex.condition.min.matches.to.pass

Default: 3

Possible value: 0-4

Description: At least n regex condition(s) must match for a new password. (see the previous setting for more information about regex conditions)

ttkf.server.security.password.expiration.days

Default: 90
Possibility: -1 to 365

Description: Specifies for how long (days) a password is valid. -1 disables the expiration check.