# User Interface - Feature #5784

## multi-factor authentication

10/29/2021 10:08 AM - Greg Shah

| | | | |
|---|---|---|---|
| **Status:** | New | **Start date:** | |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **billable:** | No | **version:** | |
| **vendor_id:** | GCD | | |

**Description**

**Related issues:**

| | |
|---|---|
| Related to User Interface - Feature #3931: single sign-on for virtual desktop... | **Closed** |

### History

#### #1 - 10/29/2021 10:08 AM - Greg Shah

*- Related to Feature #3931: single sign-on for virtual desktop mode added*

#### #2 - 10/29/2021 10:32 AM - Greg Shah

Multi-Factor Authentication (MFA) or 2 Factor Authentication (2FA - a version of MFA with only 2 factors) is an important measure for adding security to modern systems. Relying upon a password alone is long since been proven to be a terrible idea. I expect that this will become a hard requirement for all business systems in the near future.

This task is envisioned to implement a foundation within FWD so that interactive logins can be secured via standard MFA approaches. I would want the following to be easily possible for any customer that is using our login facilities (virtual desktop mode, embedded mode, Swing GUI and even interactive ChUI cases).

- FIDO2 and Universal 2nd Factor (U2F) - this is widely used and can be integrated with Yubikey and other 3rd party hardware solutions
- Time-based One-Time Password (TOTP) and HMAC-based one-time password (HOTP) which can commonly be used from something like Google Authenticator
- SMS one time codes - this is not as secure because it can be bypassed with SIM spoofing/cloning/porting, but it is still much better than the alternative of nothing

I think in the browser case, we probably need to integrate with the MFA support of the browser itself since any usage of a USB or NFC key can only work with some hardware access.