UPPWISE INDIA

www.uppwise.com



**Quaterly Development Planning**

**Q4-2023**

**Feature Title:**

SSO Improvement

**Priority:**

High

**Submitted By:**

SPM

**Target Users:**

Standard Product Users – Customer Side (Robert Walters)

**Feature Description:**

Upgrading the signing algorithm from SHA-1 to SHA-256 strengthens the security posture of the SSO system, enhances data integrity, ensures compliance with industry standards, and helps mitigate the risks associated with cryptographic vulnerabilities. It is an important step towards maintaining a secure and resilient SSO environment.

**Acceptance Criteria:**

* Need to check at our overall login mechanism with SSO
* Login mechanism improvement based on form authentication
* Need to add algorithm with SHA-256 from SHA-1

**Feature Benefits:**

**Enhanced Security:**

* SHA-256 offers significantly stronger cryptographic security compared to SHA-1.
* It provides better resistance against collision attacks and other cryptographic vulnerabilities.

**Compliance Requirements:**

* Many security standards and regulations, such as PCI DSS and NIST guidelines, recommend or require the use of SHA-256 for cryptographic operations.
* Upgrading to SHA-256 helps ensure compliance with these standards and regulations.

**Protection Against Attacks:**

* SHA-1 has known vulnerabilities and is susceptible to attacks, including collision attacks.
* Upgrading to SHA-256 mitigates the risk of potential attacks exploiting weaknesses in SHA-1.

**Data Integrity:**

* SHA-256 enhances data integrity by providing a stronger hash function.
* It ensures that data transmitted during the SSO process remains tamper-proof and secure.