ensurity
A Step Ahead!

Use Case - Electrical Automation

Implementation of **FIDO2** Sign-In for locally joined air-gapped workstations and servers within a power distribution company.

CUSTOMER	:	A Global Electrical Automation company / Deployment in Asia
DATE OF IMPLEMENTATION	:	December 2023
ENVIRONMENT	:	User authentication to their air-gapped local Active Directory (AD) joined Microsoft Windows systems using their username and password.
PROBLEM STATEMENT	:	• Deploy FIDO2-based authentication across local Active Directory (AD) connected Microsoft Windows PCs and Servers, ensuring secure access to a specific enterprise application using FIDO2 security keys. • Restrict employees from sharing their passwords. • Restrict access to system only with Biometric authentication. • Enable employees to login to any of the PC in the work area to access apps.

Solution Offered :

In response to these requirements, Ensurity has implemented the XSense IdP solution within the enterprises' on-premises data center. The inventory of ThinC-AUTH devices are managed by 'AMS Module' a life cycle management system within the XSense IdP. Furthermore, the ThinC-AUTH Biometric Security Keys are customized to accommodate the following solutions:

- Configured the ThinC-AUTH Security Keys with corporate licenses to specifically be used with XSense IdP and XSenseCPP (Credential Provider Plug-in). This functionality mandates users to utilize their registered biometrics bringing critical user attribution, while enhancing security measures.
- Supplied a customized Software Tool (Windows, macOS and Linux platforms) to enroll user fingerprints. This process is one-time activity and these settings will be saved directly to the connected ThinC-AUTH device.
- FIDO2 Security Key sign-in to Windows machines is supported in Hybrid and Azure AD environments. XSenseCPP extends support to airgap AD joined machines, for FIDO2 Security Key sign-in along with their domain credentials.

The Global Electrical Automation company was able to secure their systems and eliminate risks of credential sharing and attribute users access to its systems.