Secure and simpler authentication

ThinC-AUTH Biometric Security Keys with Azure AD Identity

From Ensurity and Microsoft

ensurity Microsoft

Passwords are a liability and a burden

81%

Of breaches leverage stolen or weak passwords.

Source: Verizon 2017 Data Breach Investigations Report

62%

Of users admit to reusing passwords.

Source: Password Reuse Abounds, New Survey Shows, DarkReading

20-50%

Of all help desk calls are for password resets.

Source: Gartner Group

Do you want to overcome your password pains?

Poor user experiences

- Fragmented, anxiety-inducing authentication experiences
- Multi-step and repetitive user processes to gain access to different devices and applications

Password-related security risks

- Passwords are easily compromised due to its blatant reuse
- Weak encryption of password management software
- Risky forms of two-factor authentication

Heavy administrative burden

- Increased support costs around password management
- Stunted employee productivity due to tedious password resets

Replace passwords with ThinC-AUTH biometric FIDO2 security keys

Maps people to unique biometric identifiers to authenticate.

Is aligned with FIDO U2F and FIDO2 standards.

Supports OATH-HOTP/TOTP authentication standards.

Has an open, scalable, and interoperable approach.

Provides a biometric 360° touch sensor that is private by design.

Safely authenticate to Windows 10 devices

Unlock the triple impact

Authenticate seamlessly

- Go passwordless.
- Eliminate the need to memorize and enter credentials repeatedly to gain access to resources.
- Improve user experiences with a single biometric security key for login.

Step up security with biometrics

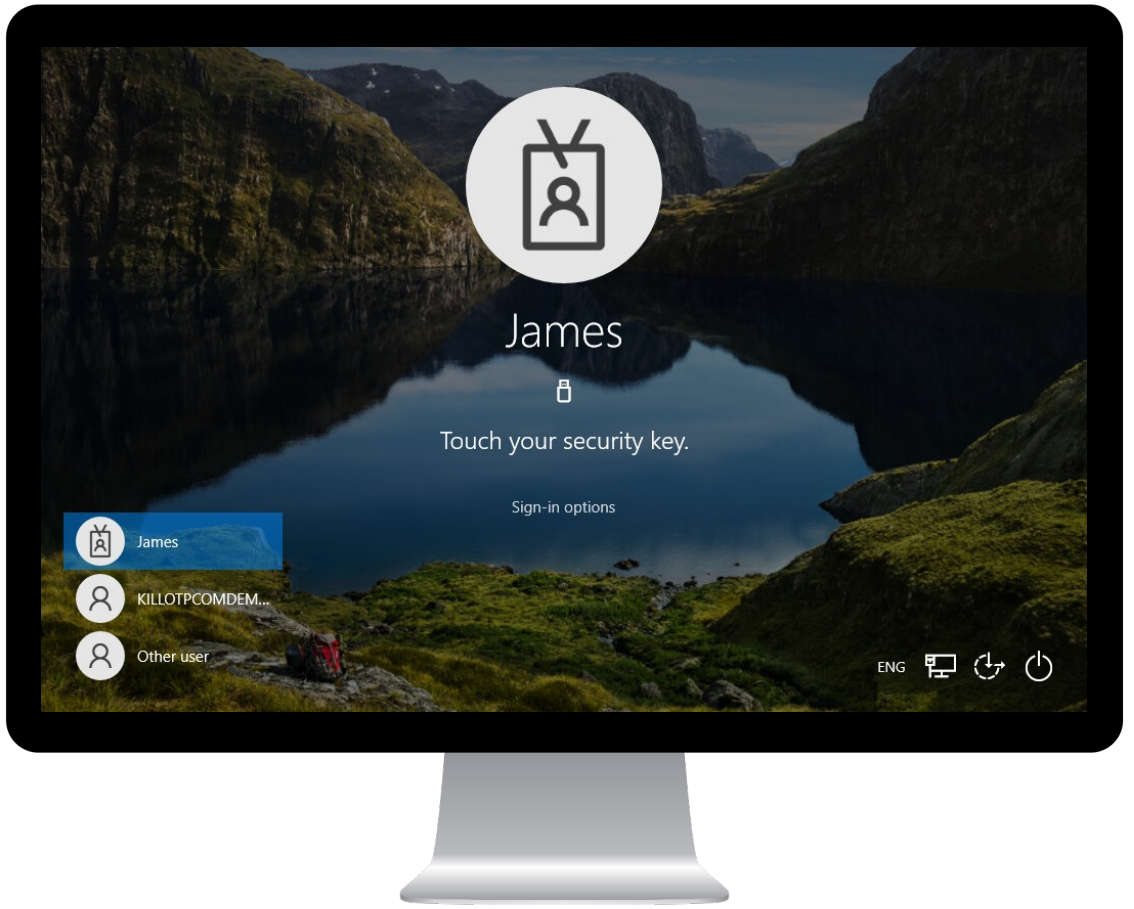
- Reduce the risk of phishing, credential stuffing, brute force attacks, corporate account takeover, and more.
- Gain peace of mind with biometrics—greater identity assurance based on unique human features.

Save time, cut costs

- Save your workforce time and money by streamlining operations and removing employee blockers.
- Eliminate tedious authentication protocols and required password resets.
- Provide single sign-on.

Authenticate seamlessly

- **Single key for hundreds of services**
- **Passwordless login to Windows Hello**
- **Authentication in <750 milliseconds**
- **Covers up to 30 FIDO2 applications**



Step up security with biometrics

Strengthen your security architecture

Eliminate the risk of impersonation

Reduce the need for user-controlled PINs

Unique cryptographic keys for every website

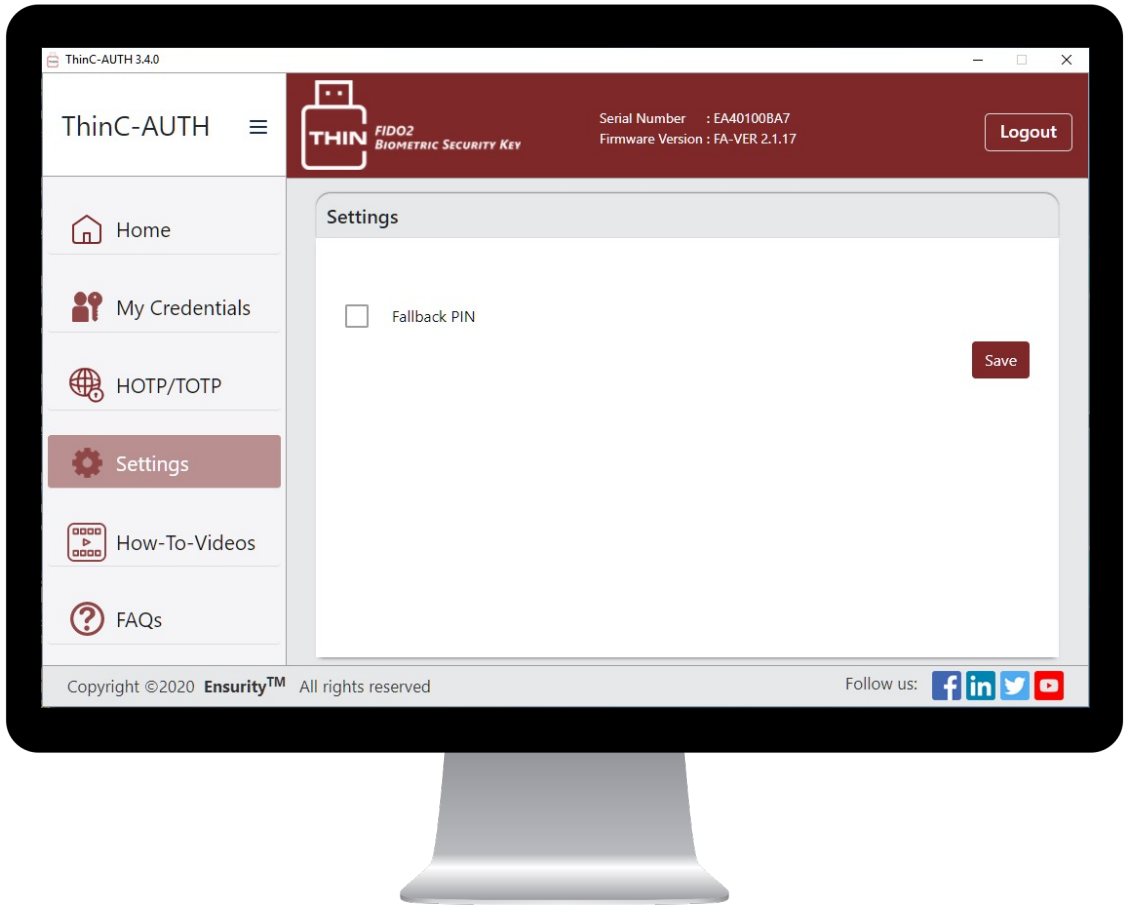
Save time, cut costs

Decreased IT workload

No expensive password or PIN managers

Improved user experiences

Secure authentication to your Azure AD account



Why choose ThinC-AUTH Biometric Security Keys?

Easy and fast to implement

A large IT BPO implemented the solution in only three weeks and eliminated password sharing completely.

Powerful biometrics

A national Government agency is rolling out Ensurity's biometric security keys for employees facilitating large financial transactions.

Convenient and cost effective

By implementing a single device, a global IT company was able to offer remote employees seamless PC login and single sign-on to company resources on-premises and in the cloud.

Case studies

Leading BPO

Challenge

A top Indian multinational IT services company needed a solution to prevent employees from sharing passwords and security tokens and enable secure access to enterprise systems via any work PC, including FIDO2 authentication to Office 365 applications.

Solution

Configured work PCs (Windows 10 Pro) as Azure AD–joined systems and provided employees with FIDO2-certified ThinC-AUTH Biometric Security Keys to multiple geographic locations.

Results

Employees could log in to their enterprise systems without entering any passwords.

Financial Establishment

Public Financial Management System - PFMS
O/o Controller General of Accounts, Ministry of Finance

Challenge

A public financial management reforms center that has applications accessible to thousands of designated users doing multiple financial transactions needed to integrate secure multi-factor authentication while keeping their solution hosted on their on-premises datacenter.

Solution

Deployed Ensurity's FIDO2 server for their on-premises datacenter and supplied ThinC-AUTH Biometric Security Keys with authentication requirements, including both PIN and registered fingerprints.

Results

Users could log in to their critical applications while furnishing both a PIN and their enrolled biometrics.

Next steps

Learn more about **ThinC-AUTH biometric FIDO2 security keys** today.

Explore the free starter kit.

Thank you