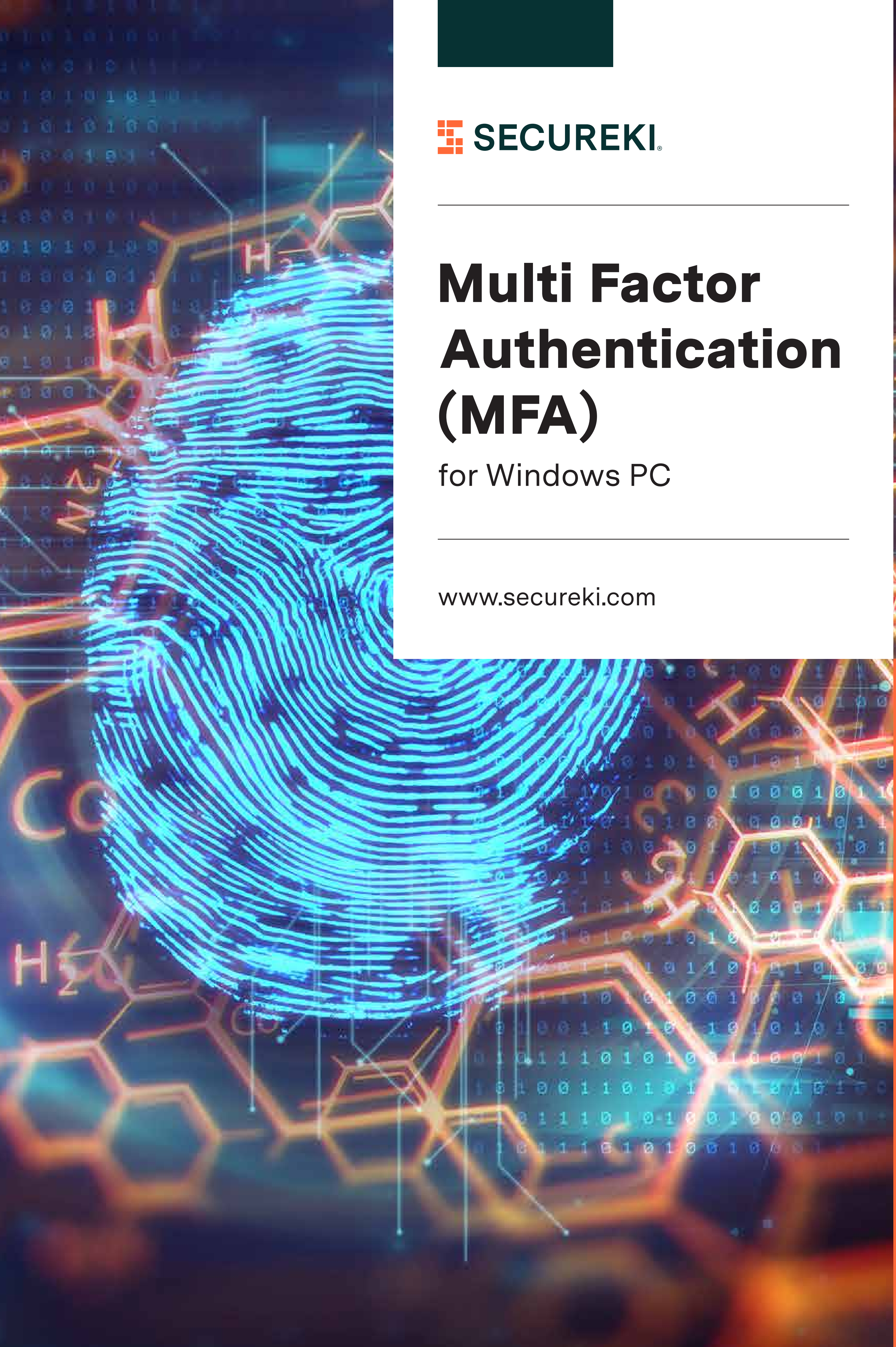


SECUREKI®

Multi Factor Authentication (MFA)

for Windows PC

www.secureki.com

Multi Factor Authentication (MFA)

for Windows PC

Think Your Passwords are Safe?

Think again. Hackers can steal your static passwords in a bunch of different ways; it's easier than you might think. Hackers have hundreds of ways to seize your credentials, and their techniques become more and more sophisticated every day.

In 2012, password theft alone increased by **300%** with identity theft going up by **33%**.

Protect Your PCs

(Two Factor vs. Multifactor)

Granting access to Windows Endpoints with just a password presents a massive risk to businesses. When online privacy breaches and hacking is rampant everywhere you look, doing everything you can to protect yourself is critical. The more recent solution to password problems has been to add in a second factor that reduces the risk of a hacker using a stolen password. This usually takes the form of a computer generated one-time password (OTP). By enabling, and using two-factor `authentication in Windows Endpoints, you're doing more than the average consumer to protect yourself.

If two-factor authentication is combining something you know (your password), with something you have (your OTP) - isn't secure enough to protect your data and other assets, then adding in another factor will be. Multifactor authentication takes the combination of something you know and have - your password and OTP - and adds in a third factor. Your biometrics.

Using biometrics as the third factor in multifactor authentication provides a significant improvement over any other element because:

- **You can't lose your biometrics**
- **They are challenging to steal**
- **They are 100% unique to you and only you**

By setting up and using two-factor authentication in Windows Endpoints, along with your mobile phone's touch sensor biometric login and protection from SecureKi's Multifactor Biometric Authentication solution, you'll get the most protection possible for your Windows Endpoints.
The power of biometrics!

How to make it easier for users to login to the computer Windows OS while Maintaining Security?

- **Passwordless fast login with mobile biometrics or OTP to enhance user's experience and eliminating credential reuse**
- **Auto-login for users without the need to remember the password thus allowing reduction to zero or near-zero password reset calls**

How It Works

When users log in to their PCs with their domain credentials or local, they merely present the second factor of authentication as well. There's no extra authentication screen, or separate application — only the native Windows login prompt.

Users have a choice to key in the OTP number or using the mobile phone's fingerprint touch sensor for biometric authentication for the MFA (multi-factor authentication).

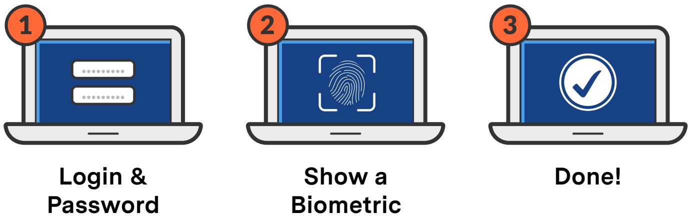
Authenticated users are then granted access to their local machine, securely and efficiently. To make login fast and straightforward as possible for employees, SecureKi supports a flexible set of "possession factors," including:

- **Mobile time-based OTP application**

- **Fingerprint Touch Sensor**

- **Offline 2FA Authentication**

This way, all three factors needed to provide true authentication are brought together with a simplified login process for users. SecureKi's MFA solution also supports the option to eliminate passwords, replacing them with a single biometric authentication process (FIDO Authenticated) for optimized convenience that still provides a high level of security. This way you can remove the security risks associated with passwords and migrate to a secure authentication system that works just by you being you.



1 **Login & Password**

2 **Show a Biometric**

3 **Done!**

SecureKi MFA Features

Secure the Windows OS

- Prevent stolen and lost password
- Prevent malwaret or hackers to compromise the login credentials
- Mitigate and prevent brute force attacks

Auto Login with Biometric

- Support mobile touch sensor
- Support Fujitsu Palm Vein scanner

Password Reset Function

- Provides password self-service-reset function through Biometrics without the need of administrator intervention to unlocked accounts

Various Login Options

- Support AD Login
- Login using Biometrics, Mobile OTP and Password Authentication

Support Offline Login using Mobile OTP