How to Use the Biometric Sign-in Tools Included in Windows 10

Before you enroll to activate the biometric sign-in capabilities of Windows 10, ask yourself why Microsoft decided to introduce their enterprise customers to biometric technology?

Security was certainly a primary driver for adding a biometric element to Windows 10. Organizations have known for quite some time that common passwords were not the answer to online security. Many felt that adjusting their password policies to include complex or sophisticated passwords that would include caps, numbers, and symbols would be the solution to strong security. Yet the fact is that most phishing attacks and data breaches all start with a compromised password.

The security that biometrics offers is as unique as your fingerprint itself. Fingerprint biometric technology has long been the go-to identifier for law enforcement and consistently grades as the most trusted form of identification. Your biometrics are unique to you; even identical twins have different biometric characteristics.

Unlike a password, PIN number or card, your biometrics cannot be lost, stolen or shared. That’s why biometric authentication is trusted by the federal government, leading hospitals and the top financial institutions in the world. It’s secure!

Convenience is also a key benefit for customers that us biometric technology. They eliminate the need to enter complex passwords in favor of static-free one-touch instant authentication. For organizations that require employees to authenticate dozens or hundreds of times per day, biometric sign-in can vastly improve workflow and contribute to running a lean yet secure operation.

A hybrid example of the security and convenience delivered by biometric authentication is showcased in environments that have roving workers and shared workstations such as banks, retail, healthcare and call centers. With biometric authentication, users migrate seamlessly and sign-in without friction as they move from device to device.

Seventy-five percent of millennials are comfortable using biometrics today, versus only 58 percent of those over age 55.

Consumers are openly embracing fingerprint authentication and Microsoft wants to deliver tools and apps that customers want. When you have millions of early adopters already using fingerprint sign-in on their phones and as they bank and shop online, it's sensible to address this growing audience.

70% of Consumers want biometrics in the workplace. Based on responses from 1,000 US adults who have experience using biometrics to log into accounts. Respondents cited speed (35%), not having to remember passwords (33%), and security (31%) as the main reasons for looking favorably on biometric authentication.

Now that we know some of the reasons why Microsoft launched the biometric solutions, let's identify some very affordable ways to unleash the power of your biometrics.

The fastest and easiest way to start is to purchase a fingerprint scanner if there is not one already on the device. There are dozens of fingerprint scanners on the market at various price-points.

The market value of Windows 10 which includes biometric technology has current potential and can expand much more into the future. As of September 2019, 14% of organizations have made the migration to Windows 10, and this number is expected to rise as the End of Life date for Windows 7 is slowly approaching. Unfortunately, though, 22% of respondents expect their companies to still use Windows 7 after its end of life date.

Windows has a usage rate of 87.9%, as in Windows OS is installing on 87.9% of the world's machines. If most of these users migrate to Windows 10 before on near the date in 2020, then there is a lot of potential for Windows Hello to be broadcasted and much hope for biometrics as a sign-in. As of right now, 800 million devices are running Windows 10, and this number is expected to increase drastically over the next years.

BIO-key fingerprint scanners have been TESTED & QUALIFIED by Microsoft to support Windows Hello, the biometric sign-in platform offered on Windows 10. The scanners come in three (3) different models, all of which connect to the USB port of the device. EcoID, SidePass, and SideSwipe are compact, durable and most important they are native to the Windows sign-in platform. Customers just plug the device in and take a moment to enroll their fingerprints. All of the scanners are offered at a very affordable $39.99 and are available through Amazon or through the company direct (Quantities of 50+).

Want more than a device sign in? Most every person that starts using biometrics to unlock their device asks, "How can I use my biometric to sign in to other apps?" It's a fact, once an end-user experiences the ease of one-touch authentication, they want more.

ID Director for Windows is a software program that integrates with Active Directory to extend the biometric authentication capability across the entire organization. Offered as a SaaS service enterprise customers simply pay a monthly per-user cost to activate the strongest form of authentication. ID Director for Windows can deliver the convenience of single sign-on (SSO) or be positioned as the strongest form of multifactor authentication (MFA).

Launching your own biometric authentication solution is easy. For device sign-in simply purchase a BIO-key fingerprint scanner and take 1-2 minutes to enroll.

Adding a layer of biometric authentication across the organization is easy too. It starts with a quick online demo and then a proof of concept, where we test the technology “in your environment” to ensure for a non-disruptive and successful deployment.

Biometric authentication helps prevent phishing attacks because there is no password to be compromised. Biometric authentication also reduces the risk of data breaches.

If you’re an IT leader, the next time you purchase a cup of coffee, consider that for about $3.00 per month / per user you can lock down online security with biometric technology. Join us for a demo and a cup of coffee on us!