

1Kosmos + Windows Hello for Business

Extend a Windows Hello for Business (WHfB) deployment



The Business Challenge

Windows Hello for Business (WHfB) provides a new, passwordless credential for Windows 10 compatible devices. It implements 2FA/MFA, meaning multilayered security, which is much more difficult to bypass than the protection that hinges solely on a username and password combination. But, WHfB does not eliminate passwords completely and is limited to Windows 10 and compatible devices.

Using 1Kosmos combined with WHfB enables the following benefits:

- **Trust on First Use:** Enable secure passwordless access to new devices without requiring the use of user ID / password.
- **Secure Non-Windows Devices:** Provide passwordless access to macOS, Linux, and Unix.
- **Virtual and Higher Privilege Environments:** Implement passwordless access to domain controllers, virtual desktop, and virtual machines.
- **Legacy technology:** Provide interoperability with legacy/internally built technologies.
- **End-user frustration:** For applications where you can not eliminate passwords, users can reset their password through the BlockID app or user portal, eliminating the need for helpdesk support. This also lets you reset the AD password for when you need to set up windows hello for the first time.



BlockID fills in the gaps WHfB can introduce, and can easily exist alongside a WHfB deployment.

The 1Kosmos Advantage

With BlockID users login with a LiveID biometric tied to a proofed and verified identity, ensuring the user is who they claim to be. And because it's delivered with a distributed identity architecture certified to NIST, FIDO, and PAD-2 requirements, it puts an immutable, private and reusable user identity at the core of your Zero Trust security for strong and continuous authentication.

Integration is easy because we've built interoperability into the platform and use an SDK / API to work with other systems and customer applications. What differentiates us is our identity-based authentication which ties a proofed and verified identity to the access request. This means that the employee's biometric is the authentication method. By implementing 1Kosmos, users will log in to their Windows, Mac, or Unix desktop with a passwordless experience using real biometrics that verify liveness. BlockID fills in the gaps WHfB can introduce, and can easily exist alongside a WHfB deployment. There are three core areas of consideration in which 1Kosmos BlockID helps organizations improve their security posture and move toward a Zero Trust architecture:

- Support previous generations of Windows as well as Linux, Unix, and macOS.
- Include devices that are not compatible with device biometrics, providing backward compatibility with your passwordless implementation.
- Managing security for contractors who have their own devices that might not meet the WHfB requirements.

The authentication flexibility of 1Kosmos BlockID works with any operating system, including Windows, Mac, Linux, Unix, and Android. Leveraging the device's built-in FIDO2 tokens, BlockID gives organizations a way to enforce their Windows Hello for Business authentication controls without the Windows 10 operating system requirements. This means that employees and third-party contractors can use any device they want without compromising a company's Identity perimeter.





Phishing Proof

IKosmos BlockID eliminates passwords and identifies users with high assurance to defeat identity-based ransomware, phishing and data breach attacks. This doesn't simply hide passwords, it eliminates passwords. Users never know or see their credentials and as a result, the credentials cannot be hacked.

Trust On First Use (TOFU)

IKosmos BlockID eliminates the "Trust on First Use" (TOFU) gap created when users transition to new systems and are required to provide a username and password. With BlockID the user's identity gets bound to their credential - it's not simply tied to a device - verifying identity at each and every access request.

Support Linux, Unix, and Mac OS

BlockID supports biometrics, but does not require a username and password with each new login to a new system or a new terminal. It also supports a wide variety of hardware and operating systems including Mac and Unix/Linux ecosystems.

The support for various operating systems and hardware configurations will also help close the security gap contractors can inject. Since it can be difficult to manage a contractor's system configuration. By implementing BlockID, a contractor would log in to critical applications without needing a password from day one.

Overcome the business limitations of device biometrics

- Built-in biometrics do not work on the first login to any new workstation. The "fallback" mechanism is - you guessed it - a username and password.
- Built-in biometrics do not work on remote machines (RDP, VDI, Citrix, Domain Controllers). This leaves high risk systems exposed and hackers know this.
- When combined with IKosmos BlockID, WHfB can be extended to other web-based logins via our Universal Web Login Connector



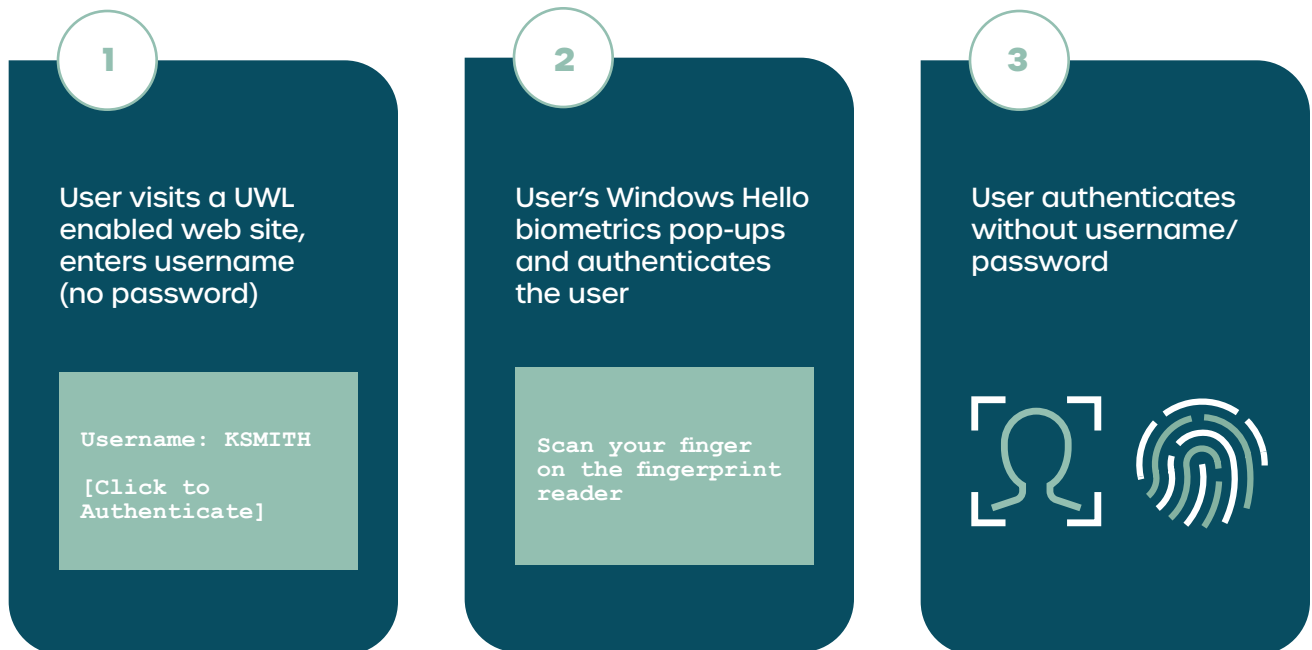


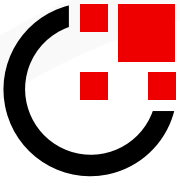
Accelerate progress toward a Zero Trust Architecture

The “Identity Pillar” of Zero Trust is arguably the most important one. Once you have verified the user identity, everything else becomes easier. IKosmos BlockID uses real biometrics to undeniably prove who is accessing your systems. This real biometric can easily be matched to a citizen, customer, or corporate identity, so you know with assurance that someone else is not gaining access to your online services.

Combine WHfB and IKosmos BlockID because they are better together

IKosmos BlockID combines the Windows Hello authentication experience with a WebAUTHn capable server. Integration is as easy as adding several lines of code to the target system’s web page. The BlockID Universal Web Login allows any non-federated login-capable system to go passwordless with no app redesign. This means Windows Hello can now be used to authenticate users into applications and services that previously were unavailable.





About 1Kosmos

1Kosmos BlockID is a distributed digital identity platform supporting both business-to-employee and business-to-consumer services that easily integrates with existing operating systems, applications, and IT security infrastructure to perform strong, verified identity-based authentication - eliminating the need for passwords, one-time codes, and more. By simplifying identity infrastructure, 1Kosmos drives both cost savings and user convenience while securing businesses and individuals from the harm and inconvenience of identity fraud. The company is headquartered in Somerset, New Jersey.

For more information, visit www.1kosmos.com or follow @1KosmosBlockID on Twitter.