1KOSMOS

# 1Kosmos BlockID and Microsoft

## Better Together Guide

## Overview

Microsoft continues to be a leader in enterprise identity and security solutions such as Entra ID (formerly Azure AD) and Windows Hello for Business. As companies expand outside of the Windows workstation and Microsoft Cloud, organizations will be presented with new identity and authentication challenges. By combining the BlockID identity and passwordless features with the Microsoft environment and Windows Hello for Business, organizations can simplify the user experience and leverage their investment in Microsoft's technologies, creating a win-win for both the organization and its users.

This document describes the procedure to configure the BlockID platform as a passwordless authentication solution for your organization's Microsoft users by combining the BlockID identity and passwordless features with Windows Hello for Business, organizations can simplify the user experience and leverage their investment in Microsoft. This integration will allow your users to log in to their Microsoft account leveraging their biometrics. The biometric options include TouchID/FaceID and LiveID.

## Windows Hello for Business (WH for Business)

With the acceleration of remote and hybrid workforce models, maintaining robust user authentication has moved from an important to imperative security control. Organizations integrated into the Microsoft ecosystem can move towards a Zero Trust security model with WH for  Business.

WH for Business, which was new to Windows 10, increases security by providing a streamlined user sign-in that replaces passwords with strong two-factor authentication. Organizations that use Active Directory  (AD) or Entra ID (Azure AD) create a seamless, user-friendly experience that combines an enrolled device with a biometric (fingerprint or facial recognition) to authenticate users. WH for Business gives users a way to authenticate easily and securely to incorporate:

- Microsoft accounts including Office 365, Teams, etc.
- AD accounts
- Azure AD accounts
- Fast ID Online (FIDO2) two Identity Provider Services or Relying Party Services

**Unlike the traditional password plus additional factor approach, WH for Business brings everything necessary for authenticating a user together in a single bundle.**

Unlike the traditional password plus additional factor approach, WH for Business brings everything necessary for authenticating a user together in a single bundle. After registering a device that stores the password and biometric, it becomes all three things necessary for strong authentication. It is now a thing someone has (the device) storing the thing someone knows (a password) bound to something someone is (a biometric).

By binding the vetted identity to the individual using biometrics, companies enhance their authentication processes, reducing the risks associated with successful social engineering, credential theft, credential stuffing, and brute force attacks.

## Business Challenge

WH for Business brings the Microsoft ecosystems the authentication protection necessary for better securing the Microsoft-based elements of the corporate stack, whether user workstations, on-premise servers, or cloud-based resources. However, as organizations build out complex hybrid and multi-cloud, and multi-platformed infrastructures (non-Microsoft and/or legacy Microsoft) many will find that they need additional technologies to improve their Microsoft deployments.

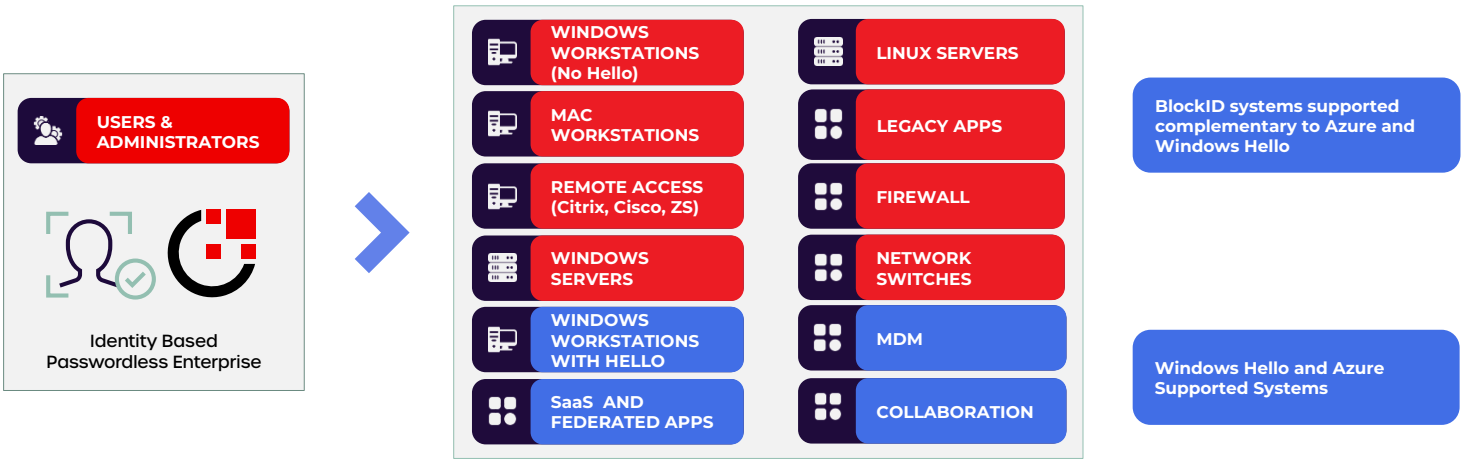
# Modernization and Agility

WH for Business offers robust authentication capabilities for Windows product lines. However, as organizations leverage the value that a multi-cloud strategy provides, WH for Business only covers a portion of the IT landscape. WH for Business interfaces directly with devices, specifically Windows devices, but does not provide zero trust for cloud resources or across multi-cloud deployments. This leads to complexity requiring additional tools, monitoring, and operational costs.

Some examples of technical challenges and gaps include:

- **InTune:** Eases deployment but increases costs.
- **Virtual machine (VM) and Virtual Desktop Infrastructure (VDI):** Both lack the security requirement (a Trusted Platform Module) necessary for interfacing with WH for Business.
- **Certificate Authority (CA):** Requires distributing certificates to end-users for enterprise deployments.
- **Certificate Revocation List (CRL):** Needs to have every client involved to access it.
- **Kerberized SSH server:** Requires implementation of additional steps.
- **Server components:** Limits organizations to Windows Operating System (OS) components and agents.
- **Non SAML applications:** Limits compatibility and extensibility into other applications or services.
- **Non-Microsoft platforms:** No support for workstations outside of the Microsoft ecosystem like Mac, Linux and Unix.i

***Microsoft Windows Hello + 1Kosmos - Identity Based Passwordless***




***1Kosmos supports Microsoft's Entra and vision for a verified identity and conditional access to any application.***

## Rigid Hardware and Operating System

WH for Business provides iron-clad security for Windows PCs, workstations, or assets that can be joined with AD and Azure AD and meet the hardware requirements. For organizations that only use  Windows OS devices, WH for Business is a perfect fit. Unfortunately, this limits the organization's ability to invest in hardware. As companies look to diversify their IT technology stacks, only running  Windows OS limits their options. Often, they find themselves either limiting their hardware purchases or investing in multiple vendor-supplied authentication tools.

**This creates three distinct business-level problems aligned to the technology:**

1. The organization must ensure that a device supports WH for Business or purchase its employees' specific hardware, increasing capital costs.
2. This requirement limits the ability to adopt cutting-edge technologies that may not support  Windows OS.
3. If companies want to create a more flexible hardware catalog, they need to invest in multiple vendor-supplied authentication tools which increases the possibility of a security gap and creates IT complexity.

Some technology limitations that companies face include:

- **Implementation:** Only works for systems running Windows 10 OS and joined with AD or  Azure AD. Windows 8 and older are not compatible.
- **Infrastructure:** Limits technology choices like macOS, Linux, Citrix, virtual desktop, and virtual machines.

- **Legacy technology:** Lacks interoperability with legacy/internally built technologies, older hardware, and earlier Windows OS versions.
- **Inflexible:** The private key remains on the workstation/laptop with no mechanism for transference to other devices and is limited to logical access.

## Multiple-Touch End-User Experience

Security tools need to provide end-users with a seamless experience or else they fail to adopt them. WH for Business offers a low-touch approach to authentication for Windows 10 devices that are joined to AD or Azure AD. However, the additional security comes with multiple touch points that negatively impact the user experience. Since the IT department enrolls devices, not users, updating corporate hardware requires end-users to take additional steps.

- **Operational costs:** Increases the time staff takes to implement and users.
- **End-user frustration:** Negatively impacts user experience when they need to enroll a new device as they need to remember their username and password.
- **Reduced productivity:** Takes workforce members time to re-authenticate a newly enrolled device to each application.
- **Increased human-error risk:** Enrolls a device instead of user identity, increasing the potential for a device not in an asset catalog.
- **Passwords are still required:** As users transition to a new device, their corporate credential is still required to begin that transition before WH is available for login.

## Remote/Hybrid Workforce

Remote and hybrid workforce models are the future of business. With employees no longer protected by on-premise network security, identity, and authentication become mission-critical security controls. Companies often put Virtual Private Networks (VPNs) and Virtual Desktop clients in place to help protect company information.

However, remote and hybrid workforce models also mean that organizations have less control over their endpoint devices. Analyst Gartner believes that 80% of worker tasks take place on mobile devices. In the consumer technology space, many employees purchase Android, macOS, iOS, or iPadOS devices, leaving them to choose between security and productivity. Since WH for Business only works with Windows 10 OS devices, IT departments must find another solution for passwordless access if they choose a macOS, iOS, or iPadOS personal device.

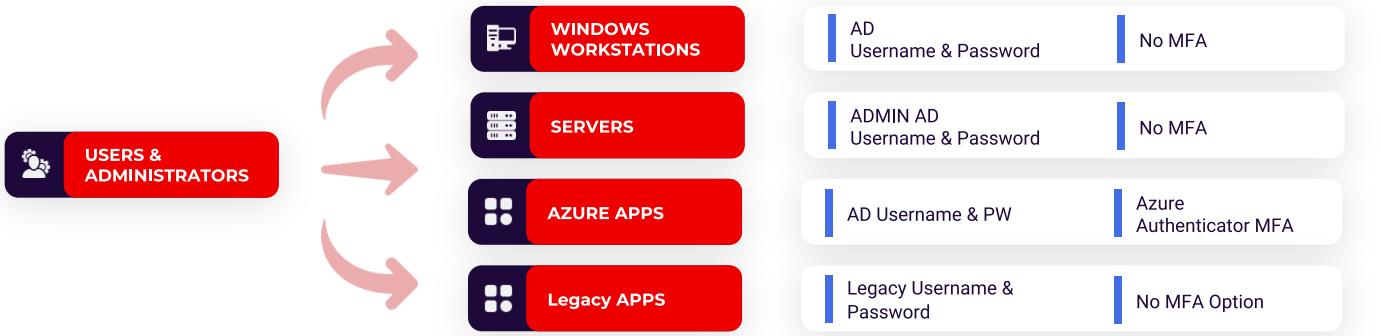
When meeting the new demands of a hybrid workforce, companies face challenges such as:

- **Reduced productivity:** Leaves employees unable to authenticate when using devices running operating systems other than Windows 10.
- **Virtual Desktop Infrastructure (VDI):** While WH for Business does have a private key stored on it, there is no mechanism to utilize this for virtualized environments. Another solution must be used.
- **Virtual Private Networks (VPNs):** WH for Business lacks native VPN support for protocols such as Radius and SAML and may require Kerberos which is often seen as a legacy protocol.

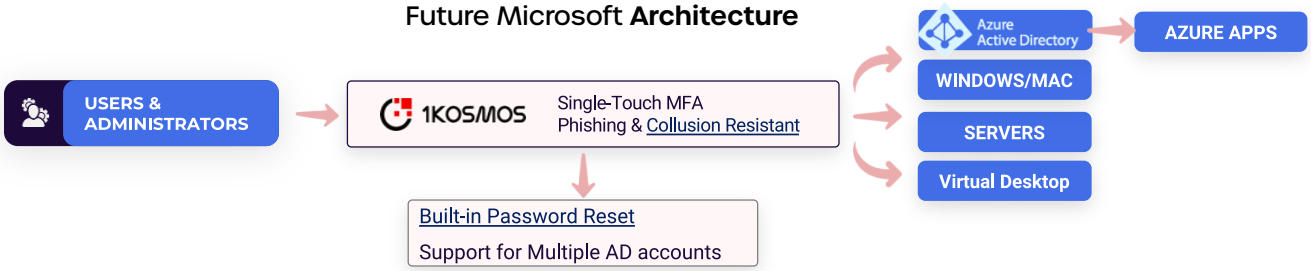
# 1Kosmos + Microsoft = Better Together

To fully secure the remote/hybrid workforce and embrace digital transformation, organizations need to enhance Windows Hello and the MS Authenticator by utilizing solutions for diverse operating systems, security tools, cloud-based resources, legacy web-based resources, and other nonstandard applications.

Current Microsoft **Architecture**




Future Microsoft **Architecture**






## How does BlockID enhance WH for Business?

To set up a new workstation or laptop, WH for Business requires a user to type in their AD username and password, create a PIN, and enroll their biometric. In effect, they are "exchanging" an AD password for a biometric for machine authentication. While this makes subsequent logins much easier, it has a user experience challenge often referred to as "TOFU", or "Trust on First Use". The goal is to go passwordless, but you need a password to "set it up".

Furthermore, once a user relies on biometric authentication instead of passwords, this means that they will be using their password less frequently. However, they will still need it for some legacy applications until they can all be phased out. As they rely on passwordless, they will be more likely to forget their password.

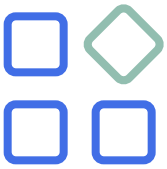
BlockID has a "reset legacy password" feature that allows users to reset an account with their mobile and biometrics (see a video demonstration here). With this feature, users can reset their AD (or any other) account for those rare occasions when they need to use it, such as setting up WH for Business on a new machine or accessing a legacy HR website.

To achieve this capability, BlockID provides Identity-Based Authentication to any requesting device or service. Once identity is established (via flexible enrollment scenarios), this identity can be used across any IT system without having to prove who they are a second time.

WH for Business allows enrolling devices. WH for Business uses a device as the authentication method. When organizations enroll devices, they link the device to the identity. This means that every time the person authenticates to a new application or resource, they need to link the device to that application to set up a cryptographic secret. The user's identity is not involved in the process,  but rather a legacy username and password.

BlockID enrolls users. Conversely, BlockID utilizes the cryptographic keys provided by the DID as the authentication method and the device as a delivery mechanism. BlockID starts with users, gathering all identity verification information and digitally signing it. Users store their government-issued ID information, such as passports or driver's licenses, in the BlockID application (this is optional,  and customers can choose to enable or disable this feature). Then, they register and store their  LiveID with facial recognition in the application to enhance the DID with biometric data. Finally,  when they log into a corporate resource, the BlockID application compares the FaceID with their company ID and personal identification sources. This creates a device and operating system-agnostic three-way authentication process.

Once users create their DIDs, they can use that verification and authentication information anywhere. This means that any device with BlockID can authenticate to any network, software, or device for a single source of multi-factor authentication that eliminates the need for passwords and legacy MFA solutions.



## Say “Hello” to Diverse Hardware Assets

Because BlockID starts with identity instead of devices, organizations implementing WH for Business can extend their deployment to any hardware or operating system. BlockID extends WH for Business capabilities by creating a Universal Web Login (UWL) to authenticate into any web-based asset. By adding four lines of JavaScript code to any login page, employees can use their DID plus their biometrics to authenticate to any device. Yes, this is the power of Identity-Based Authentication based on Decentralized Identifiers!

This functionality gives organizations a way to extend their WH for Business by removing the need for a Microsoft device-based token. BlockID supports a wider array of devices running Windows 10, previous generations of Windows, Linux, Citrix, and Mac operating systems.

With BlockID, organizations extend their WH for Business authentication investment to the technology that best meets their business objectives.

## Say “Hello” to a Modernized Identity Stack

BlockID gives companies a way to on-premise and cloud-based ecosystems with identity-based authentication. BlockID, like WH for Business, utilizes a FIDO2 server architecture and supports a wide range of FIDO. Because Identity is presented on “the first touch” of a new machine or website, BlockID automates the configuration of the “cryptographic secret” between the user and the remote site or OS.

This capability also enables organizations to integrate DID authentication into their legacy or internally built systems, covering a wide range of digital services.

## Say “Hello” To Enhanced Productivity

1Kosmos is not the only organization to embrace DIDs. Microsoft has recognized that DIDs are the way of the future when dealing with identity and has an entire practice working on bringing DIDs to market. 1Kosmos and Microsoft are both involved in various industry efforts such as the W3C DID working group and the FIDO Alliance, with the goal being to fix the broken user authentication experience. Because 1Kosmos combines a strong Identity with DIDs, organizations can embrace Microsoft’s WH for Business and leverage the standards-based BlockID platform to cover missing platforms and web services.

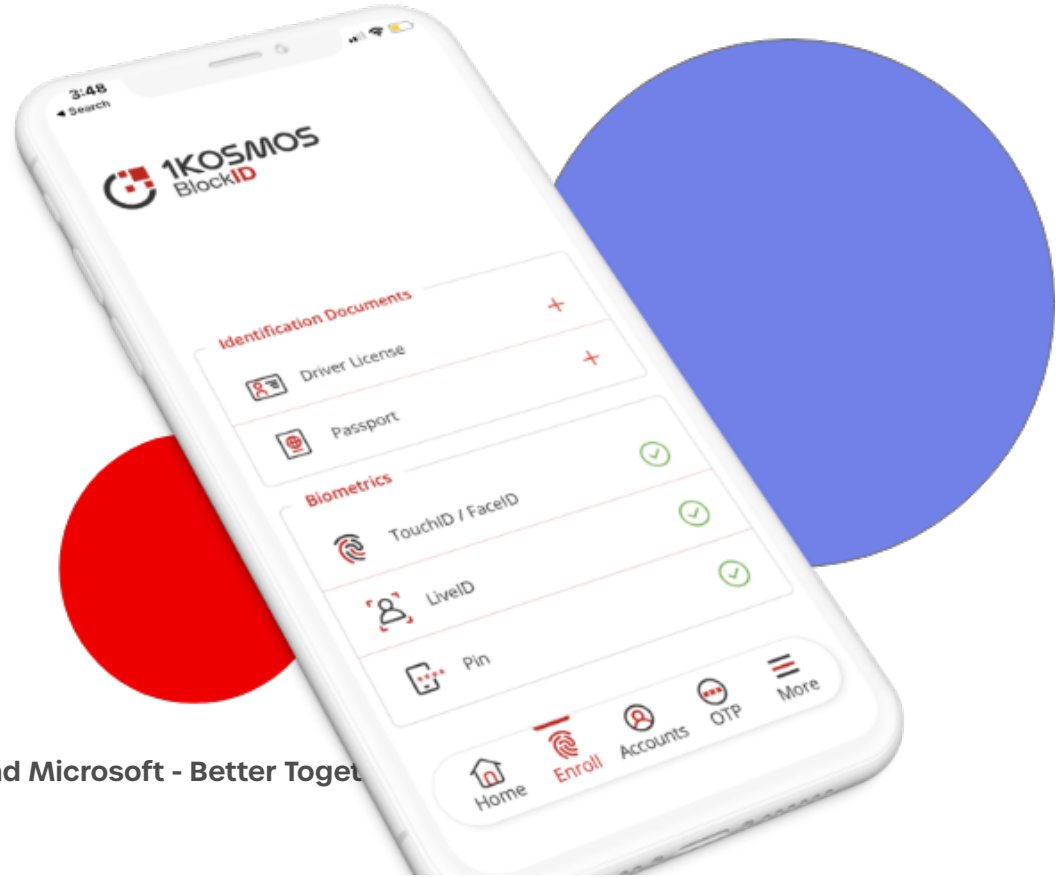
By leveraging the BlockID UWL (Universal Web Login) any service that does not support federated login protocols such as SAML or OIDC can now be supported, without requiring any application redesigns. By adding four lines of JavaScript to the web application login page, the user now has a secure channel that replaces the login ID and password. When a user scans the QR using their device, the BlockID software automatically pairs the keys and verifies their identity at the same time. Users no longer need to worry about complex passwords or cumbersome push notifications. With BlockID they can use their device-based or real biometric proof to access the resource.

## Say “Hello” to a More Secure Remote/ Hybrid Workforce

With organizations moving to hybrid workforce models, managing user-owned device access to cloud-based resources and collaborative tools is increasingly important. However, workforce members often want to use their own devices, such as smartphones, to do job-related tasks. Meanwhile, managing third-party contractors poses another user-owned device problem when they need to connect to resources from outside the corporate network.

For organizations implementing WH for Business, employees must use corporate-provided Windows  10 devices or other supported devices. Meanwhile, the organization cannot force its third-party contractors to purchase a WH for Business compatible device.

BlockID alleviates these security issues and gives workforce members the freedom they want.  BlockID works with any operating system, including Windows, Mac, and Android. Leveraging the device's built-in FIDO2 tokens, BlockID gives organizations a way to enforce their WH 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.



# 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 East Brunswick, NJ.

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