Specops Password Policy vs Windows Hello for Business

Windows Hello for Business offers a convenient way for end users to sign-in on Windows devices, but several practical and security gaps remain. The Active Directory password still exists and Windows Hello for Business doesn't cover every device, legacy app, or shared-device scenario. **Specops Password Policy** can be used to identify and close those gaps.

Why Windows Hello for Business needs additional protection

- **Device-tied passkeys:** Passkeys are typically locked to a single device and users must enroll separately on each device.
- **Enrollment limits on shared devices:** Windows Hello limits enrollments, which creates problems for shared or kiosk workstations.
- **Underlying AD password still exists:** Even when users sign in without a password, the AD account password still exists and remains an attack vector.
- **Incomplete coverage (legacy apps / non-Windows):** Many legacy systems, non-Windows devices or services that don't support passkeys still require passwords.
- **Recovery and device-loss complexity:** If a device with passkeys is lost, recovery can be more complex than with traditional password workflows.
- **Device compromise risk:** If a device is compromised (malware), private keys stored on the device may be at risk.
- **PIN risk:** Once authenticated locally (PIN/biometric), SSO can grant wide access raising concerns about PIN reuse, observation, or weak PIN choices.
- **AD password storage & attack vectors:** AD stores hashes with no salting, increasing the risk of brute force / pass-the-hash exposure if hashes are obtained.

Where Specops Password Policy augments Windows Hello for Business

Limitation/Issue	Where Specops Password Policy can support
Many apps/devices don't support passkeys — passwords are still required for those services.	Fill the gaps left by the residual need for secure password controls in scenarios where passkeys aren't sufficient or widely supported. Learn more.
Shared / kiosk workstations (enrollment limits).	Manage and mitigate shared-device scenarios and policy edge cases that Windows Hello enrollment limits create. Learn more.
Windows Hello hides the password from users but the AD password remains and is vulnerable.	If the underlying passwords is weak or compromised, attackers can exploit it (e.g., in a passthehash attack). Sometimes it is even default or blank. Specops ensures passwords are strong and continuously scans your AD for compromise. Learn more.
Control privileged accounts Recovery from lost devices (passkeys) can be more complex than traditional password recovery.	Specops can be used to design and enforce recovery and policy workflows for cases where passkeys are lost or unavailable. Learn more.
Private key security depends on device integrity. Devices can still be vulnerable to malware.	Specops augments Windows Hello by addressing the persistent password/ AD risk that remains if device-based keys are compromised. Learn more.

Limitation/Issue	Where Specops Password Policy can support
Local PINs are often reused (banking PIN, bugler alarm etc.) or easy to steal/observe.	Specops helps mitigate downstream risks from local authentication by enforcing account and password controls where Windows Hello alone does not change AD password risk. Learn more.
The way AD stores hashes (NTHash) is unsalted and pass-the-hash attacks remain a concern.	Specops protects the remaining attack surface in AD (password hygiene / policy controls) to reduce the impact of hash-exposure scenarios. Learn more.

Specops offers easy deployment with your existing Active Directory infrastructure. Get in touch and we can explore how the right solution can fit with your organization.

Speak to an Expert