Specops Password Policy vs. Microsoft Entra ID Password Protection

Microsoft Entra ID Password Protection (formerly Azure AD Password Protection) offers a basic layer of security for users, but leaves you wide open to breached password risk. It's the easy option. But its built-in protections often fall short of regulatory requirements and real-world security needs. **Specops Password Policy** closes these gaps and improves your operational efficiency.

Where Microsoft Entra ID Password Protection falls short

- **Point/entropy model misses breaches**: Entra ID uses a scoring system that often allows leaked passwords to pass. In recent tests, it missed over 90% of a sample of 5,000 breached passwords.
- **No continuous scanning**: Entra ID only checks for compromised passwords at the moment of change or reset, leaving accounts vulnerable if a password is leaked later.
- **Limited custom lists**: The custom banned word list in Entra ID is limited to only 1,000 words and does not support words shorter than four characters.
- **Vague user feedback**: Rejection messages are vague and cannot be customized, often leading to increased help desk calls as users struggle to understand why a password was rejected.
- **Compliance risks**: Because Entra ID does not truly block all previously leaked passwords, it may fail to meet the strict expectations of frameworks like NIST 800-63B or CJIS.
- **Lack of granularity**: Dictionary rules in Entra ID are not Group Policy driven and apply to all users globally, rather than allowing for different policies for different groups.

How Specops bridges the gaps

Scenario	Specops Password Policy	Microsoft Entra ID Password Protection
Breached Password Coverage	Blocks over 5 billion compromised passwords, including data from live honeypots and thousands of leaked list sources updated daily.	Relies on a global banned list and a 5-point scoring system that often fails to block complex passwords found in real attacks.
Continuous Scanning	Performs continuous AD checks against the latest breach data, remediating compromised accounts immediately.	Only evaluates passwords during a reset or change event.
End-User Experience	Provides dynamic, real-time feedback at the password change screen with clear, customizable instructions to reduce help desk volume.	Uses a "5 wrongs makes a right" algorithm that is difficult to explain to users, paired with un-customizable messaging.
Custom Banned Lists	No limit on dictionary size or character length; blocks banned words regardless of leetspeak or character positioning.	Limited to 1,000 words; cannot block short words or handle complex leetspeak variations effectively.

Scenario	Specops Password Policy	Microsoft Entra ID Password Protection
Policy Flexibility	Fully Group Policy driven, allowing administrators to apply different settings, languages, and policies to specific users or groups.	Dictionary rules apply to all users; limited ability to vary complexity based on group membership in hybrid environments.
Regulatory Compliance	Makes it simple to comply with the password requirements for all major cybersecurity regulations and frameworks.	May fail audits due to its inability to block the full corpus of known leaked passwords.

Specops Password Policy offers easy deployment within your existing Active Directory infrastructure, plugging into both on-prem and hybrid environments in just a few hours. Speak to an expert today to see how Specops can strengthen your organization's identity security.

Speak to an Expert