COMPARISON

Specops Password Policy & Breached Password Protection vs. Microsoft Entra Password Protection (formerly Azure AD)

ABOUT SPECOPS Specops Software is the leading provider of password management and authentication solutions. Specops protects your business data by blocking weak passwords and securing user authentication. Every day thousands of organizations use Specops Software to protect business data. For more information, please visit specopssoft.com

HOW MICROSOFT ENTRA PASSWORD PROTECTION WORKS

Microsoft Entra (Azure AD) Password Protection comes included in P1/P2 Entra ID (Azure AD) plans. The name indicates users are protected from using bad passwords but that's not the case. If an organization is serious about securing its Active Directory environment, whether on-prem or in the cloud, Entra ID built-in protections simply aren't enough on their own.

You might be under the impression that Entra is 'good enough' and doesn't need augmenting to deal with breached passwords. But this isn't reality. We'll walk through a real-world example of how Microsoft Entra Password Protection misses breached passwords. Then we'll show how the two lists that it uses to check your users' passwords against are lacking, for different reasons. The Global Banned Password List

The "Global Banned Password List" is not a list of leaked passwords and does not fulfill compliance recommendations for a password deny list.

Unlike Specops Breached Password Protection, the Global Banned Password List does not include third-party data like that of Have I Been Pwned or other known breached password lists. Microsoft instead relies solely on its own analysis of what passwords are being used in various Entra ID environments. Microsoft does not disclose any of the contents of its list.

Regulatory recommendations like that of NIST or NCSC include using a list of known breached passwords. Specops Breached Password Protection fulfills this recommendation.

Microsoft does not state the number of passwords on the list. They say it is small compared to other third-party lists but that with fuzzy matching it can block millions of password variations from their smaller banned list.

Specops Breached Password Protection Complete is a larger banned password list, currently at over 4 billion unique compromised passwords.

[New research] How good is Microsoft Entra at catching breached passwords?

We've run some research to compare the password blocking capabilities of Entra ID and Specops' Breached Password Protection. We've also looked at HaveIBeenPwned, for an additional data point.

Methodology

1. A random sample of 5,000 passwords was taken from the Alien_Txtbase infostealer logs released in May 2025 (chosen to allow other breached corpora time to process leaks).

2. Scripts were written to check the sample against the HIBP API and to attempt password changes on a target DC.

3. An Entra ID environment was deployed with the Entra ID Proxy and the Microsoft Entra Password Protection Agent; the DC had a single GPO applying the filter in **block** mode (no other policies or custom dictionary enabled), so any blocked changes would be attributable to the password filter.

4. Explicit checks against Breached Password Protection (BPP) were unnecessary because the dataset already exists in BPP and all records would be blocked. Note that June/July are not the most recent infostealer entries in BPP; older data was intentionally used for these samples. To assess coverage trends, the same random 5,000-record sample was also taken from a recent infostealer dump obtained from a dark-web forum.

Results of our analysis

The results align with expectations: the intentionally older dataset shows better coverage with HIBP due to sufficient time for inclusion via added breaches or law-enforcement sources. Entra ID, however, performs significantly worse, as shown by the number of password changes not blocked by its filter. Most passwords from as far back as May are not blocked by Entra ID.

Entra ID

Month	May	June	July	October
Missed	4,650	4,644	4,653	4,534
Blocked	348	354	347	466
Blocked %	**6.96%**	**7.08%**	**6.96%**	**9.32%**

HIBP

Month	May	June	July	October
Missed	338	334	710	2,441
Blocked	4,662	4,666	4,290	2,559
Blocked %	**93.24%**	**93.32%**	**85.8%**	**51.18%**

Specops

Month	May	June	July	October
Missed	0	0	0	0
Blocked	5,000	5,000	5,000	5,000
Blocked %	**100%**	**100%**	**100%**	**100%**

What does this mean?

Takeaways differ between HIBP and Entra ID due to their underlying design philosophies. HIBP is not limited to its public API; its dataset is also used by several competitors as their sole breached-corpus source (e.g., ManageEngine ADSelfService Plus, Open Password Filter).

Entra ID

- Entra ID starts from a baseline of deleted words, maps to a banned word list, and applies a points calculation. This produces similar behavior across datasets: it

effectively **does not block breached passwords**. This makes it closer to a strong password policy with a banned-word list than a well-implemented, well-maintained leaked corpus.

- This stems from Microsoft's point-based weighting system, which also governs how the "breached list" is applied. Microsoft maintains its own breached list, normalizes passwords (e.g., P@ssw0rd → password), and blocks them only if they fail to score enough strength points (entropy). We will explain this system in detail in the next section.
- Organizations bound by standards such as NIST 800-63B or CJIS should note that Entra ID performs poorly at preventing the use of leaked passwords. This gap is driven by design rather than breach-to-coverage delay. It does not reliably block breached passwords and simple leaked passwords can still pass through filters. It should not be considered equivalent to BPP for compliance with standards such as NIST 800-63B or CJIS.
- Entra ID does not provide real-time protection; passwords are only evaluated at reset or change.

HIBP

- HIBP shows more variation between datasets; as time passes and leaks become more widely available, they are more likely to appear in the HIBP datasets. Older leaks have lower miss rates (especially compared to Entra ID), while recent leaks show larger gaps.
- HIBP has fewer misses because it is applied as a true breached corpus, similar to Specops' Breached Password Protection. However, because HIBP primarily relies on user and law-enforcement submissions, lag or omission may occur.
- Vendors depending on HIBP will therefore trail behind a fully maintained breached corpus, though this gap is far less severe than with Entra ID, since leaked credentials are at least blocked.

Specops

- Specops' Breached Password Protection exhibits short lag times due to the combination of Threat Intel operations, Specops honeypots, and human monitoring of breach activity.
- Specops Password Policy with Breached Password Protection provides significantly better breached-credential coverage than implementations relying on HIBP or Entra ID
- Specops Password Policy with Breached Password Protection blocks passwords immediately after they've been newly added to the breached corpus.

Why 'The Global Banned Password List' isn't enough

The "Global Banned Password List" is not a list of leaked passwords and does not fulfill compliance recommendations for a password deny list.

Unlike Specops Breached Password Protection, the Global Banned Password List does not include third-party data like that of Have I Been Pwned or other known breached password lists. Microsoft instead relies solely on its own analysis of what passwords are being used in various Entra ID environments. Microsoft does not disclose any of the contents of its list.

Regulatory recommendations like that of NIST or NCSC include using a list of known breached passwords. Specops Breached Password Protection fulfills this recommendation.

Microsoft does not state the number of passwords on the list. They say it is small compared to other third-party lists but that with fuzzy matching it can block millions of password variations from their smaller banned list.

Specops Breached Password Protection Complete is a larger banned password list, currently at over 5 billion unique compromised passwords.

Microsoft's password scoring method: "Five wrongs make a right"

Step 1: Normalization
First, the password entry is converted to all-lowercase. Microsoft states that common leetspeak character substitutions are also reversed; however, some common substitutions like €→e and 8→b are ignored.

With Character Substitution enabled, Specops Password Policy blocks common leetspeak characters including the following which Microsoft ignores.

4 = a; € = e; 6 = g; 7 = t; 8 = b; 9 = g; § = s

Step 2: Fuzzy match check
The normalized entry is checked against the banned lists for exact matches +/- 1 character difference.

Step 3: Substring match check
The normalized entry is also checked against the user's first name, last name and tenant name; however, partial matches (Jeff for Jeffrey) are ignored.

Specops Password Policy can block the full or partial use of a user's first or last name.

Step 4: Final scoring
If the normalized entry makes it past the previous checks, Microsoft gives it a score. One point is given for: each exact match to a word on the global banned list; each exact match to a word on the custom banned list; each remaining unique character.

Entries must pass all of the above checks and reach a score of 5 to be accepted.
Example scoring:
Micr0soft1! [microsoft] + [1] + [!] = 3 → Rejected
Micr0soft124! [microsoft] + [1] + [2] + [4] + [!] = 5 → Accepted

Meaning, Microsoft will accept passwords containing dictionary words and known leaked passwords.

The Custom Banned Password List

This is Microsoft's competitive offering to Specops Password Policy's custom dictionary lists.

The Custom Banned Password List has a limit of 1000 words, and each entry must be at least 4 characters long.

Three letter combinations are common for many companies. This 4-character limitation means you can't block:

- Short company names or acronyms (like IBM, DSW, CBS, FOX, CNN, UPS, CVS, ATT, 3M)
- Shorter stock symbols (like GE, BBD, GM, BMY)
- Airport codes (like JFK, LHR, LAX, CDG, DXB, ARN, YYZ, FRA)
- Internal abbreviations (like product short names: SPP, BPP, SSD)

Specops Password Policy dictionary lists have no limit and allow entries of any length.

Microsoft doesn't always block words from the Custom Banned Password List. Microsoft's "5 Wrongs Make a Right" approach to scoring means that a word on your custom list is allowed as part of a longer password.

Weak Passwords Accepted by Azure AD
Specops124!
[specops] + [1] + [2] + [4] + [!] = 5 → Accepted

Password998!
[password] + [9] + [9] + [8] + [!] = 5 → Accepted

PasswordPasswordPasswordPassword9
[password] + [password] + [password] + [password] + [9] = 5 → Accepted

Specops Password Policy can block the use of any word on custom dictionary lists in a longer password.

Breached Passwords

The infamous password breaches, Collections leaks #1-5, contain over a billion compromised passwords. Microsoft ignores them along with other third-party data in its Global Banned Password List, leaving users vulnerable.

Below are just a few examples of the most common complex passwords found in Collection #2 that pass Microsoft's Password Protection filter.

Leaked Passwords Accepted by Azure AD
FQRG7CS493
Sojdlg123aljg
D1lakiss
Indya123

The Specops Password Policy password deny list includes the above known breached passwords and over 4 billion more unique compromised passwords.

While recommending removing expiry, Microsoft Entra (Azure AD) Password Protection only checks for compromised passwords at reset or change

> *"When users change or reset their passwords, these banned password lists are checked to enforce the use of strong passwords."*

Microsoft often strongly recommends getting rid of expiry, though we find most organizations are not ready for it. However, Microsoft Entra (Azure AD) Password Protection lacks any method for checking for compromised passwords outside of at change or reset. Fewer expiry events means that users covered by Microsoft Entra Password Protection have their password checked for compromise very infrequently.

Specops Password Policy offers continuous protection against the use of compromised passwords with a daily scan against the daily updated list as well as during password change.

More Than Security Gaps, User Experience is Lacking

Microsoft Entra Password Protection is likely to increase IT service desk calls

> *"Microsoft Entra (Azure AD) Password Protection has no control over the specific error message displayed by the client machine when a weak password is rejected."*

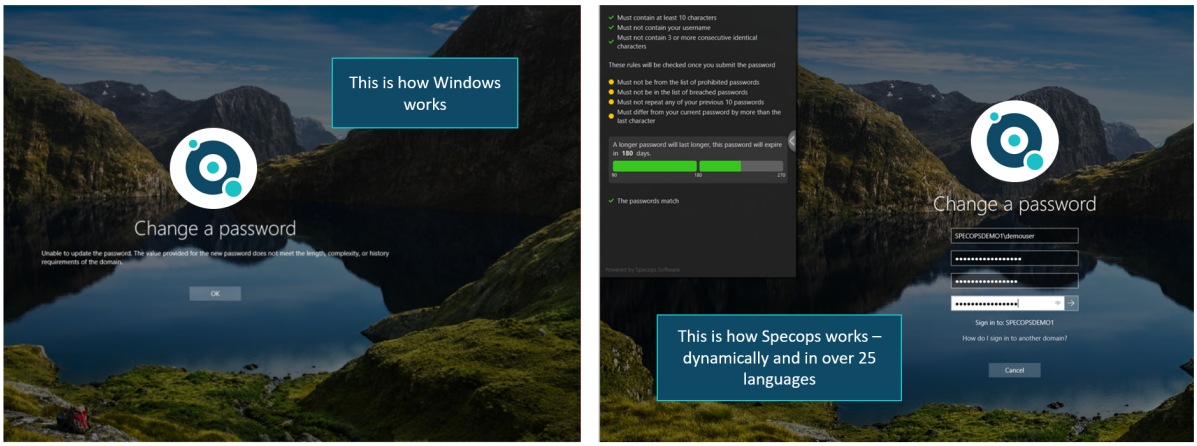
Microsoft Entra Password Protection is likely to increase calls to the IT service desk for two main reasons.

#1 - Lack of custom password rejection messaging

As shown in the above quote from Microsoft's documentation, Entra ID (Azure AD) does not permit admins to customize the standard Windows error messages users see upon password rejection.

> *"Unable to update the password. The value provided does not meet the length, complexity, or history requirements of the domain."*

The above message is the only message users will see no matter the reason their password was rejected when changing or resetting their password on their machines.



This vague messaging is not likely to make it clear to the user what they need to change about their password in order to for it to be accepted.

With Specops Password Policy, users receive dynamic feedback at password change as they type. Specops also enables admins to customize the message that users receive, including displaying the found dictionary word.

#2 - The inherent complexity of Microsoft Entra (Azure AD) Password Protection scoring

The password scoring used in the Microsoft Entra Password Protection is complicated, and IT admin logs will tell you a password was rejected because it was found on the global or custom banned list but not tell you which.

This lack of transparency on rules for what is required means that the IT service desk will struggle to successfully identify issues users are having with setting passwords.

With Specops Password Policy, admin logs identify on which password list a rejected password entry was found.

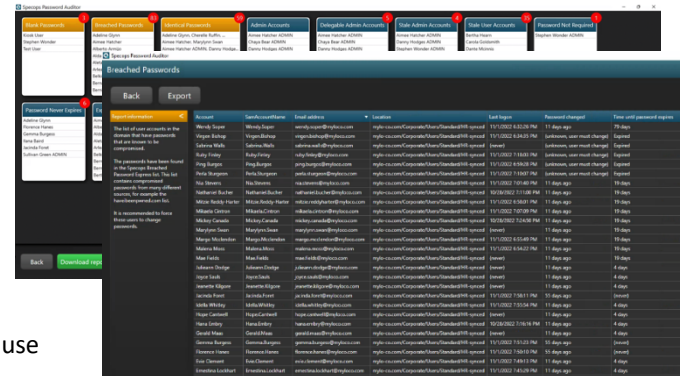
What We Recommend

You don't need to abandon Entra ID to implement stronger password policies or to block users from using compromised passwords.

You can instead set up Specops Password Policy and Breached Password Protection to enforce these policies in your on-prem environment and utilize a federation solution or Microsoft Entra (Azure AD) password write-back to enforce those policies for your users across environments.

Find out how many of your Entra ID (Azure AD) users' passwords are still compromised

Specops Password Auditor is a free read-only tool that scans and checks passwords of Active Directory user accounts against our list of compromised passwords.



Many of our customers who were relying only on Microsoft Entra (Azure AD) Password Protection have told us they were shocked to find how many compromised passwords were in use after running a Password Auditor scan.

It takes a single compromised password to create risk and potential compromise. Download your free copy of Specops Password Auditor here.

Get a demo of Specops Password Policy

Specops Password Policy helps increase password security in your on-prem Microsoft Active Directory or hybrid Entra ID (Azure AD) environment. The solution can target any GPO level, group, user, or computer with password complexity, dictionaries and passphrase settings. With Specops Breached Password Protection, IT teams can block over 4 billion unique compromised passwords. These passwords include ones used in real attacks today or are on known breached password lists, making it easy to comply with industry regulations such as those from NIST or NCSC.

Interested in seeing how Specops Password Policy and Breached Password Protection could work in your environment? Click here to set up a demo or trial today.