SPECOPS

SPECOPS SOFTWARE

Specops Password Policy & Breached Password Protection vs. Azure AD Password Protection

HOW AZURE AD PASSWORD PROTECTION WORKS

Azure AD Password Protection comes included in P1/P2 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, Azure AD built-in "protections" are not enough.

Azure AD Password Protection includes two lists that it uses to check your users' passwords against. Both 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 Password Policy's Breached Password Protection, the Global Banned Password List does not include third-party data like that of Have I Been Pwned (HIBP) or other known breached password lists. Microsoft instead relies solely on its own analysis of what passwords are being used in various Azure AD 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 do mention it is small compared to other third-party lists but that with fuzzy matching it can block millions of password variations of the words on their smaller banned list.

Specops Password Policy's Breached Password Protection Complete is a larger banned password list, currently at over 2 billion passwords.

Microsoft's Password Scoring Method: "5 Wrongs Make a Right"

"Even if a user's password contains a banned password, the password may still be accepted if the overall password is strong enough otherwise."

Microsoft does not block the use of passwords found on its Global Banned Password List or a configured Custom Banned Password List. Instead, the use of a banned word is only one part of Microsoft's formula for whether or not a new password will be accepted.

To pass Microsoft's password filter, a user's password must score 5 points. The use of a banned word is worth one point but that alone does not disqualify a password.

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 like 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.

The entry 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, SPR, BPP)

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

Microsoft doesn't always block the use of words from the Custom Banned Password List. Microsoft's "5 Wrongs Make a Right" approach to password scoring means that a word on your custom list can be 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 and Other Compromised Passwords

The infamous password breaches, Collections leaks #1-5, contain over a billion compromised passwords. Microsoft ignores them along with other third-party and real attack 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 along with ones our own threat research team has discovered being used to attack Windows networks right now. Both sets pass Azure AD's filter.

Leaked Passwords Accepted by Azure AD

Yuantuo2012
FQRG7CS493
Groupd2013
D1lakiss
Indya123

Passwords Observed in Real Attacks Accepted by Azure AD

almalinux8svm
dbname=template0
shabixuege!@#
P@ssw0rd5tgb
adminbigdata

The Specops Password Policy password deny list contains the above known breached passwords and over 2 billion more compromised passwords, including ones used in real attacks today or are on known breached password lists.

More Than Just Security Issues, User Experience is Lacking

Azure AD Password Protection is likely to increase IT service desk calls

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

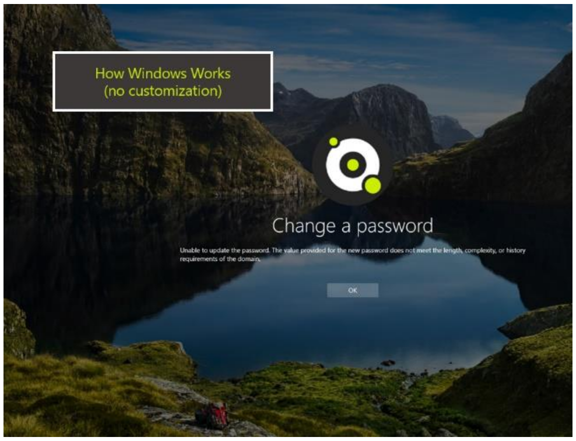
Azure AD is likely to increase calls to the IT service desk for two main reasons.

#1 - Lack of custom password rejection messaging

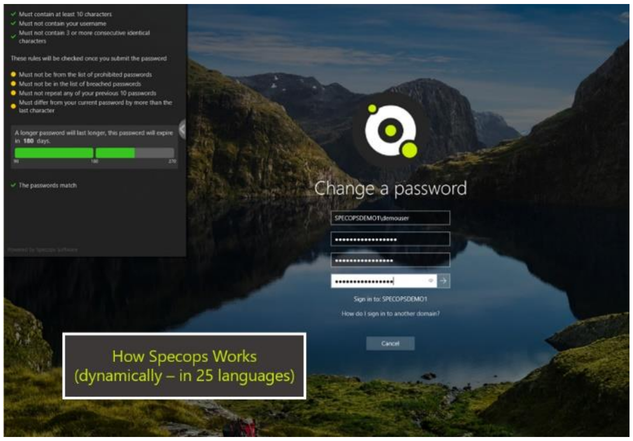
As shown in the above quote from Microsoft's documentation, Azure AD does not permit admins to customize the standard Windows error messages users see upon password rejection.

> *"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.



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



✓ Must contain at least 10 characters
✓ Must not contain your username
✓ Must not contain 3 or more consecutive identical characters

These rules will be checked once you submit the password

● Must not be from the list of prohibited passwords
● Must not be in the list of breached passwords
● Must not repeat any of your previous 10 passwords
● Must differ from your current password by more than the last character

A longer password will last longer, this password will expire in **180** days.

✓ The passwords match

SPECOPSDEMO1\demouser

Sign in to: SPECOPSDEMO1

90
180
270
Change a password
How do I sign in to another domain?
Cancel
How Specops Works
(dynamically – in 25 languages)

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 Password Policy also enables admins to customize the message that user receives, including displaying the found dictionary word.

#2 - The inherent complexity of Azure AD's Password Protection scoring

The password scoring used in the Azure AD 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, IT admin logs identify on which password list a rejected password entry was found.

WHAT WE RECOMMEND

You don’t need to abandon Azure AD or O365 to implement stronger password policies or to block users from using leaked passwords.

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

About Specops Password Policy and Breached Password Protection

Specops Password Policy helps you increase password security in your on-prem Microsoft Active Directory or hybrid Azure AD environment. The tool extends the functionality of Group Policy and simplifies the management of fine-grained password policies.

Specops Password Policy can target any GPO level, group, user, or computer with password complexity, dictionaries and passphrase settings. With Specops Password Policy and Breached Password Protection, companies can block over 2 billion compromised passwords in Active Directory. These compromised 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.

Our research team’s attack monitoring data collection systems update the service daily and ensure networks are protected from real world password attacks happening right now. The Breached Password Protection service blocks these banned passwords in Active Directory with customizable end-user messaging that helps reduce calls to the service desk. Breached Password Protection is available as a secure list in the cloud or stored locally in your environment.

Interested in seeing how Specops Password Policy + Breached Password Protection work in your environment?

Click here to set up a demo or trial today.