SPECOPS BREACHED PASSWORD PROTECTION

Datasheet

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

SPECOPS BREACHED PASSWORD PROTECTION

Specops Breached Password Protection is a service that checks your Active Directory passwords against a continuously updated list of compromised passwords. The list contains over 2 billion passwords from major breach incidents as well as passwords used in real attacks happening right now. During a password change in Active Directory, the service will block and notify users if the password they have chosen is found in the banned list.

How does it work?

There are two editions of the Breached Password Protection service, Complete and Express. Both are included when you enable Breached Password Protection in Specops Password Policy.

- Breached Password Protection Complete is over 2 billion passwords strong and connects to your network via an API key. When enabled, the service will check your users' passwords during a password change or reset and notify them via email or SMS if that password was found to be a known breached one and can require them to change it at next logon.

- Breached Password Protection Express is an optimized subset of the larger Complete list. When enabled, the service will check your users' passwords during a password change and block them immediately from using that password. Admins can also configure nightly scans against the Express list. The Express list is also used when running a Password Auditor scan.

You can enable one or the other per your security preferences but we recommend enabling both if you are able.

For more on the Specops Breached Password Protection technical requirements, see our reference material.

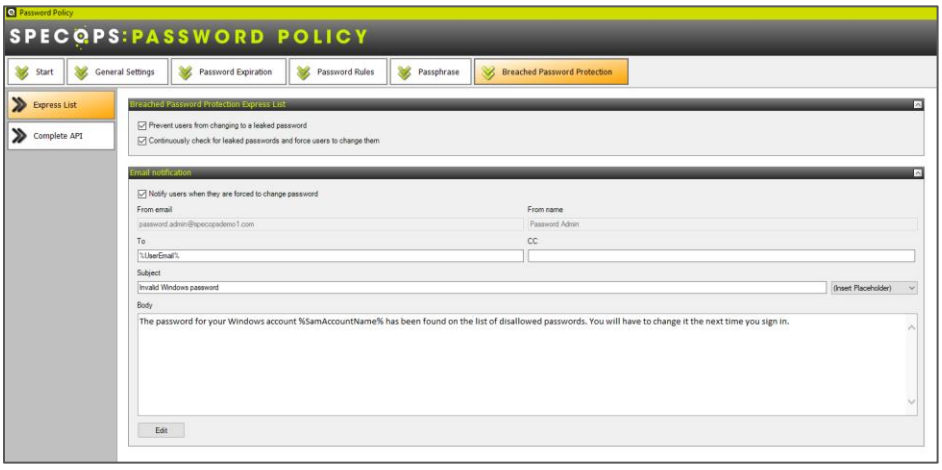
Features

FEATURES	ACTIVE DIRECTORY	AZURE AD PASSWORD PROTECTION	SPECOPS BREACHED PASSWORD PROTECTION
Blocked list includes 3rd party breached passwords (as recommended by orgs like NIST and NCSC)	n/a	No (not a 3rd party list, per Microsoft)	Yes
Protects against the use of over 2 billion known breached passwords	n/a	No (fuzzy matches over 1 million)	Yes

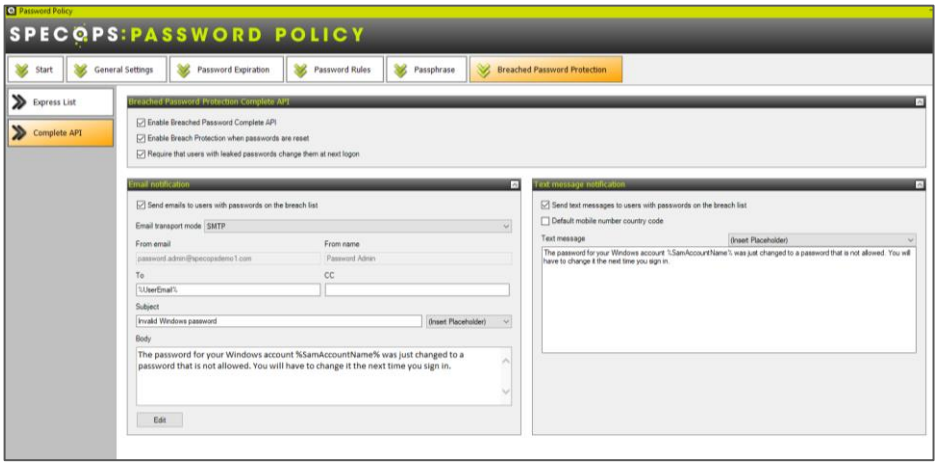
FEATURES	ACTIVE DIRECTORY	AZURE AD PASSWORD PROTECTION	SPECOPS BREACHED PASSWORD PROTECTION
Blocks passwords used in password spray attacks happening right now	n/a	Partially (only uses base terms on global list)	Yes
Updates to blocked list offer immediate protection	n/a	Yes	Yes
Offers protection on domain controllers not connected to an external internet	n/a	No	Yes (with Express)
On-screen explanation of why the password is rejected	n/a	No (not on-prem)	Yes
Off-screen notifications of breached password	n/a	No	Yes (text and email)

What does it look like?

You configure Specops Breached Password Protection settings inside your Specops Password Policy admin screen.



Configure when users are forced to change passwords, as well as the content of your email and text notifications. Choose if you'd like to use your own mail server or the Specops service to send your email notifications.



Configure when users are forced to change passwords as well as the text of your email notifications.

Frequently Asked Questions

How often is the list updated?

Our team is constantly working on updating the list used in Specops Breached Password Protection. Breached Password Protection Complete, our API-connected list, is updated immediately upon our team finding new additions (at least once a day). Breached Password Protection Express, the condensed downloadable list, is updated every few months.

Where do you find the passwords added to the list?

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.

Do you have the ___ breach? What are your sources for the list?

For security reasons, we don't reveal the full contents of Specops Breached Password Protection. However, we can share that the over 2 billion password list includes the HaveIBeenPwned list, the latest Collection lists, as well as thousands of other known leaked lists, as recommended by regulatory bodies such as NIST, CMMC, NCSC and others.

In addition to known breaches, our research team also actively monitors for passwords being used in real password spray attacks happening right now. Our team's attack monitoring data collection system updates the service daily and ensures organization users are blocked from choosing those passwords at change/reset immediately.

Are passwords sent externally with Specops Breached Password Protection?

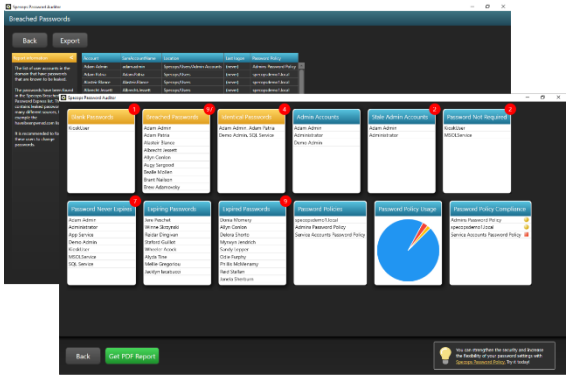
No. The Sentinel Password Filter generates a bcrypt hash of the user's new password. Neither the password nor the bcrypt hash is exposed. The first few bytes of the bcrypt hash are used to query a set of matching hashes. The match takes place on the domain controller, within the organization's network.

I have another question…

Have a question you don't see answered here? We'd be happy to answer it. Reach out to your Specops representative or contact us here.

Find Out How Many of Your Users' Passwords Are Vulnerable

Specops Password Auditor is a free tool that scans and checks passwords of Active Directory user accounts against our list of compromised passwords. The Auditor also provides a full view of the administrator accounts in an organization's domain, including stale/inactive admin accounts. From a single view, you can identify vulnerabilities that can assist you with your security plan.



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

Get a Demo of Specops Breached Password Protection

Ready to see how Specops Breached Password Protection works in your environment? Specops Breached Password Protection is a part of Specops Password Policy, an Active Directory tool that extends the functionality of Group Policy, and simplifies the management of fine-grained password policies

Click here to set up a demo or trial today of Specops Password Policy and Breached Password Protection.

★★★★½

UNQUESTIONABLY MORE SECURE

"The new dictionary and deny list capabilities are designed to give admins even more control over user's passwords and allow for passwords that are unquestionably more secure."

- Brien Posey, 15-time Microsoft MVP