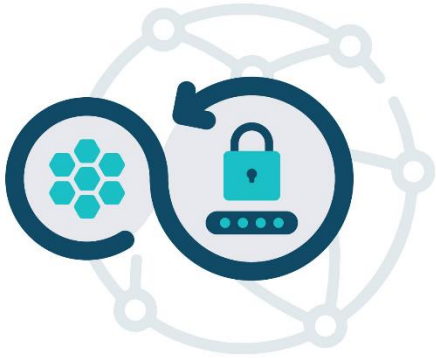
SPECOPS BREACHED PASSWORD PROTECTION

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 continuously checks your Active Directory passwords against a daily updated list of compromised passwords. The list contains over 4 billion unique passwords from major breach incidents as well as passwords used in real attacks happening right now.



The compromised password check can occur (1) during a daily scan and/or (2) during a password change in Active Directory. Users are prevented from choosing compromised password at change and can be enforced to change their password at next logon when a compromised password is found during a daily scan.

How does it work?

Two different databases of Breached Password Protection exist and both are available to use when you enable Breached Password Protection in Specops Password Policy:

- **Breached Password Protection Complete.** This database is updated daily and is over 4 billion passwords strong. The database connects to your network via an API key.

- **Breached Password Protection Express.** This database is an optimized subset of the larger Complete list. The Express list is also used when running a Specops Password Auditor scan.

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

There are two events that can be configured to run the Breached Password Protection service, during password change and daily continuous scans. Both are included when you enable Breached Password Protection in Specops Password Policy.

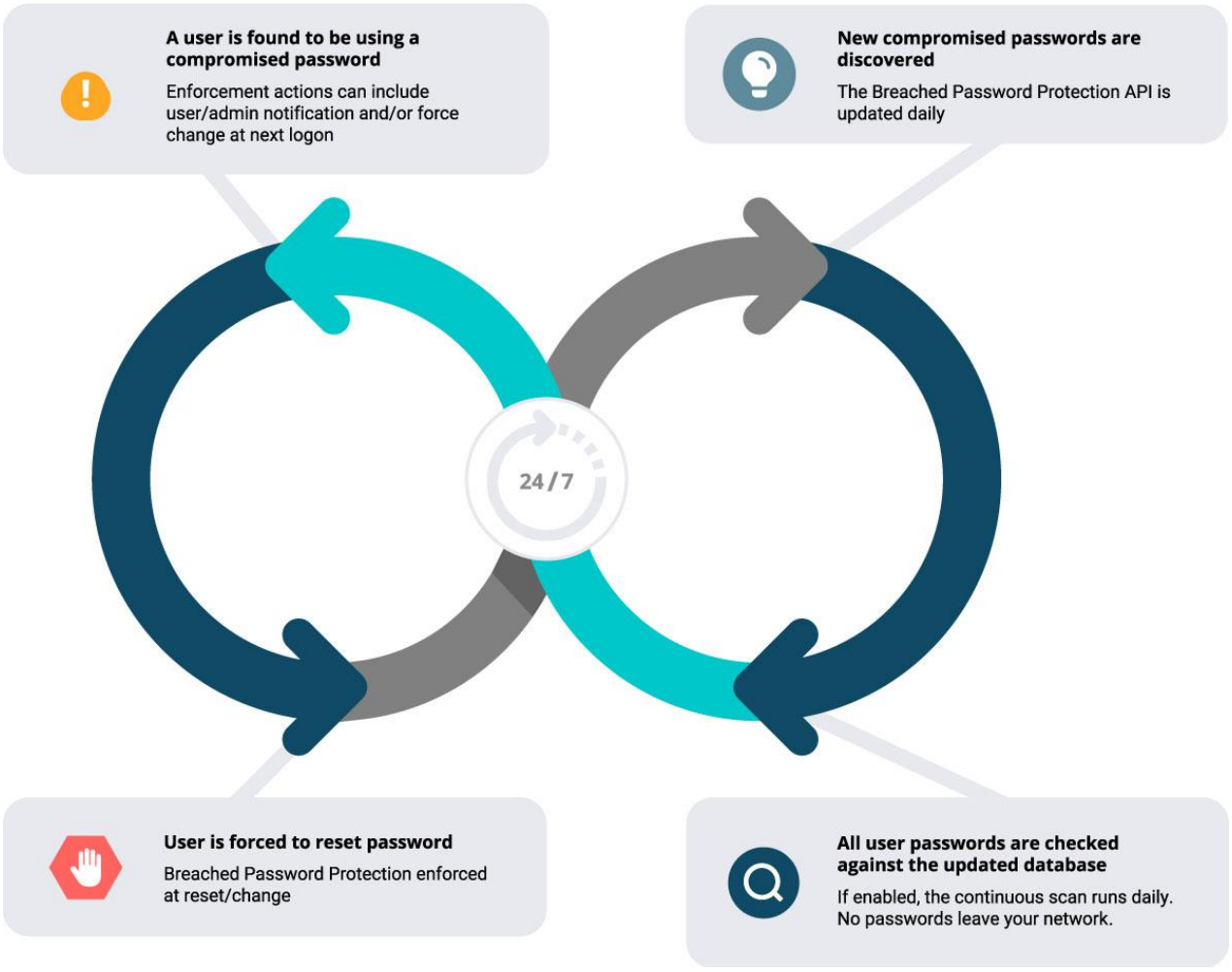
- **Continuous scans.** When configured, Breached Password Protection can check for passwords against a daily updated database. Admins can choose to remediate a found compromised password via enforcing change at next logon or notify users or admins via email or text.

- **Password change.** When configured, Breached Password Protection can block the use of compromised passwords during a password change event. Users will be immediately prevented from using any password found on the Express list. When configured to check passwords against the Complete database during password change, admins can choose to remediate a found compromised password via enforcing change at next logon or notify users or admins via email or text.

Continuous scanning with Specops Breached Password Protection

The continuous scan feature checks all Active Directory passwords against the Breached Password Protection API for compromise once a day during the scheduled Periodic Scanning. If enabled, the API is updated daily with newly discovered compromised passwords from our password honeypot system in addition to newly discovered password leaks when they occur.

No passwords leave the local network.



Optional remediation actions include enforcing change at next logon or notifying via text or email. The email notification can be configured to notify any desired user (including admins).

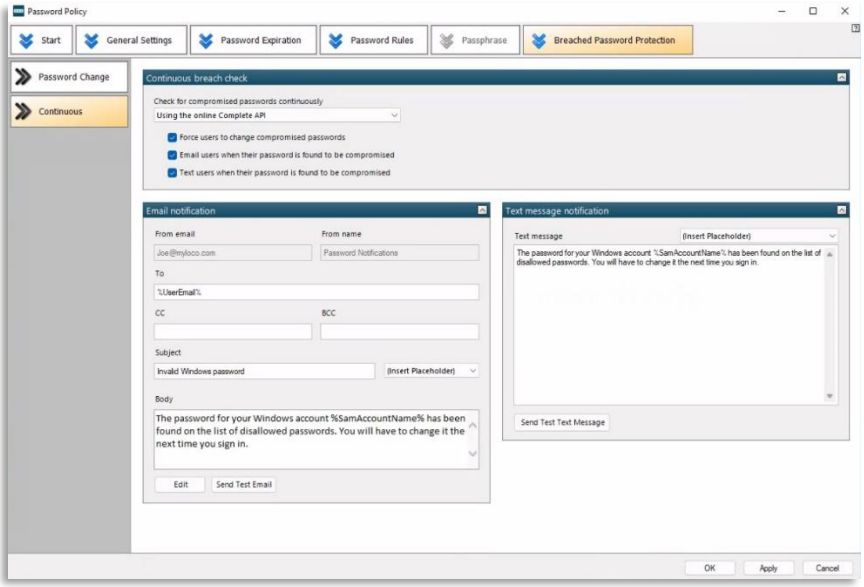
The latest results of the scan can be found in the event logs as well as the Periodic Scanning reporting page in the Admin interface.

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

Features

FEATURE HIGHLIGHT	ACTIVE DIRECTORY	MICROSOFT ENTRA (AZURE AD) PASSWORD PROTECTION	SPECOPS BREACHED PASSWORD PROTECTION
Blocked list includes 3rd party breached passwords (as recommended by NIST, NCSC etc.)	n/a	No (not a 3rd party list, per Microsoft)	Yes
Protects against the use of over 4 billion unique compromised passwords	n/a	No (fuzzy matches over 1 million)	Yes
Blocks passwords used in password spray attacks happening right now	n/a	Partially (only uses base terms on global list)	Yes
Offers protection on domain controllers not connected to an external internet	n/a	No	Yes (with Express)
On-screen explanation for password rejection	n/a	No (not on-prem)	Yes
Off-screen breached password notices	n/a	No	Yes (text and email)

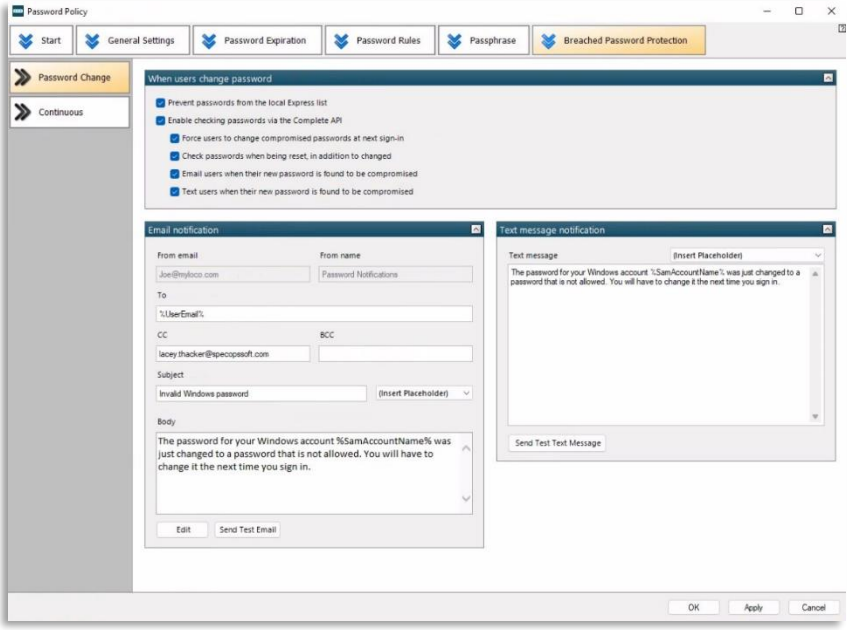
What does it look like?



Admins can configure Specops Breached Password Protection settings inside the Specops Password Policy admin screen.

Configure whether users are forced to change passwords, as well as the content of the email and text notifications.

Enable daily compromised password checks.



Configure whether users are forced to change compromised passwords at next logon as well as the text of the email notifications.

Make use of cc or bcc to alert IT or helpdesk staff.

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.

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 4 billion unique compromised 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?

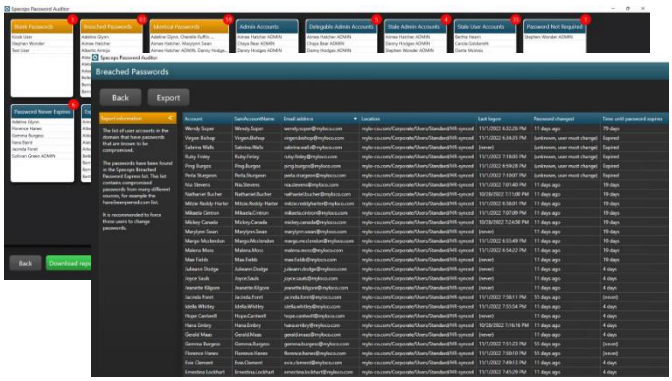
No. The Sentinel Password Filter generates a bcrypt hash of the user's new password. Neither the password nor the bcrypt hash is exposed. The first few bytes of the bcrypt hash are used to query a set of matching hashes. The match takes place on the domain controller, within the organization's network.

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.

What customers are saying

Gartner Peer Insights™
4.5 (38 Ratings)

Easy, fast to deploy, immediate return of investment.

Specops Password Management - A great addition to protecting your AD

Good password filtering with excellent on-screen immediate user feedback