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, malware botnets, 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 <u>Specops Password Auditor</u> 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.

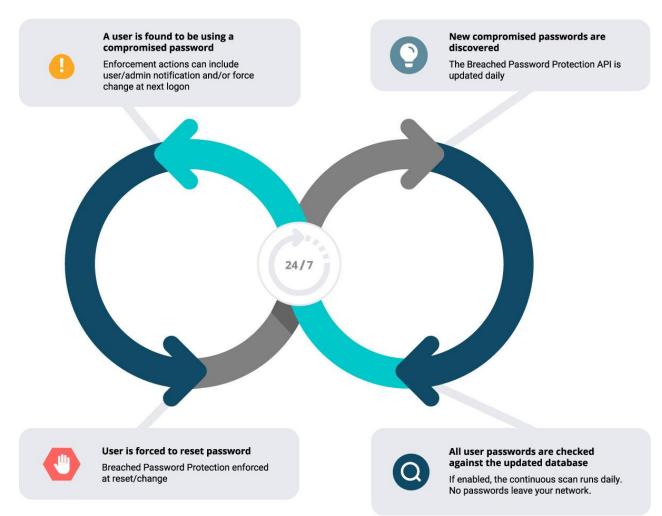




Continuous scanning with Specops Breached Password Protection

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 3 rd party breached passwords (as recommended by NIST, NCSC etc.)	n/a	No (not a 3 rd 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?

Test users when here a Final recolfication From email JoseEmylaco com To UberEmail: CC	nn v	Tex	t message notification et message he password your Windows iselowed pesswords. You will he	(Inset Placeholder) accurt "Sankcourtisms' in the been found on the list of			
Continuous Using the other Complete # Contained to damage Torce series to damage Teal series them have a Teal them at series them have a Contained to the teal a Contained to	UP Compromised passwords password is found to be compromised assavord is found to be compromised From name Password Notifications	Tex	ext message The paseword for your Windows :	account %SamAccountName% has been found on the list of			
Email users when their Text users when their Text users when their Text users when their Text users when their ViserShare To ViserShare Cc	password is bound to be compromised assessed is bound to be compromised from name Password Notifications	Tex	ext message The paseword for your Windows :	account %SamAccountName% has been found on the list of			
From email Jos Emploro com To "UserEmail". CC	Password Notifications	Tex	ext message The paseword for your Windows :	account %SamAccountName% has been found on the list of			
Joe@myloo.com To 1.Usefmañ. CC	Password Notifications	The	The password for your Windows	account %SamAccountName% has been found on the list of			
To 13.beefinal?). CC		Th	The password for your Windows is isallowed passwords. You will ha	account %SamAccountName% has been found on the list of ave to change it the next time you sign in.			
UberEnal% CC	NCC .	dis	isalowed passwords, you will he	ave to change it the next time you sign in.			
22	RCC .			usaloweu passwords, nou will nave to change il the next time you sign in.			
	BCC.		and the second se				
E black							
Subject							
Invalid Windows password	(Insert Placeholder)	1					
Body							
	The password for your Windows account %SamAccountName% has been found on the list of disallowed passwords. You will have to change it the next time you sign in.						
Edit Send Test Er							

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.

Password Change							
Continuous	When users change password Prevent passwords from the local E Enable checking passwords via the Fore users to change compron Check passwords when being re Email users when their new pass Text users when their new pass	Complete API lised passwords at next sign-in set, in addition to changed word is found to be compromised					
	Email notification			Text message notification			
	From email	From name		Text message	(Insert Placeholder)	v	
	Joe@myloco.com	Password Notifications		The password for your Windows acco	s account %SamAccountName% was just changed to	a a	
	то			password that is not allowed. It	ou will have to change it the next time you sign in.		
	%UserEmail%						
	сс всс						
	lacey thacker@specopssoft.com						
	Subject						
	Invalid Windows password	(Insert Placeholder) 🗸 🗸					
	Body					v	
	The password for your Window	password for your Windows account %SamAccountName% was changed to a password that is not allowed. You will have to ge it the next time you sign in.		Send Test Test Message			
East Send Test Email							

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 HavelBeenPwned 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.

Our sources also include stolen passwords from malware botnets, and 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 <u>here</u>.



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.

Mark Passes dt. Gook User Stephen Wonder Ted User	Adeline Gyon Adeline G Almes H9524r Almes Ho Almes Honga Almes Ho		o Ownella Ruffin in Manyon Sean in Admits Daviny Healige	Adves Accounts Arme Harber ADMA Days Ben KRMH Deny Hodger ADMA Deny Hodger ADMA		Arrian Hashar ADMIN Dema N Denny Hodges ADMIN Carole D		accessed Not Required	l.
	And Ann Ann	Breached Passwords							
		Back Expo							
Fanoword Never Equiv	1	Import information 🛛 🗧	Access			Location			
Formula Hateri	Alte	The last of upper promotion free	Werdy Super	Wends Super	wendproper@reglaca.com	ingle-course Corporate/Usery/Standard/HE-sprice	4 19/1/2002 632.26 PM	11 dep age	79-days
Germa Burgest	435	domain that have passworth	Veses Labor	Virgen Bahap	vices behop@re/ocs.com	m/o-co.com/Corporate/Users/Standard/HII europ	# 11/1/2002 634/35 PM	linknown wer most changel	Entered .
Terra Dainé Jestinda Panet	Alet	that are income to be compromised.	Salarya Wala	Salarina.Walls	utrinanal Dryten.com	right county Corporate Damy Danderd Mill sprice	4 (mover)	Setteren, user must change!	Espired
Salivan Grave ACMIN	Della Della				nate fining@regions.com	replo-co.com/Corporate/User/Standard/HE-opera			
	See.	The passwords have been found in the Species Establish Personnel Express lat. This list	Prop Burgers	Pinallurate	ang hurges ill malace.com	m/o-co.com/Corporate/Users/Standard/Hit-conce		linknown sear must change!	Speed
i.	and the second		Perfa Skarpron	PerlaStorgeon	perfasturgeon@repleco.com	right course Corporate Units Standard HE sprin	4 11/1/2002 P-10/07 PM	Beliteven, user most changed	Espirat
				Nia Stevens	niastevens@mekxis.com	make-co-com/Corporate/Uvery/Standard/HR-concer		11 days app	
		paratements from many different economy for ecomplex free hare-beenging and a set for	Network Bucher	NethenielBucher	where bucher Brelass.com	myle-co.com/Corporate/Useru/Standard/Hill-once	8 10/28/2022 7:11:00 PM	11 days ago	
					withered that and my faco com	Inglo-co.com/Corporate/Unru/Danderd/HE-sprce		11 days app	
		It is recommended to from	Millada Getter	Mikada Cireton	mAsels.ortion@muloce.com	Intercoron/Corporate/Ures/Sandard118 since	# 11/1/2022 7/07/09 PM	11 600 022	
			Mickey Canada	Mickey Canada	wickey.canada@wy/cco.com	myle-co.com/Corporate/Uvery/Standard/HT-corce	4 10/28/2022 T.04:50 PM	11 days ago	
					marytom searching terminent	regio courses Corporate Divers Danderd MR enviro	# (sne)		
		Marge Mcclandon	Margs Mcclendan	margamederdor@myloco.com	replo co.com/Corporate/Uvers/Standard118 synce	# 11/1/2022 655.49 PM	11 days ago		
Back Download to					waters.wccdwylocs.com	myle-co.com/Corporate/Users/Standard/HE-co.co		11 days ago	
	to share the second			Man Fields	man Falls Directors com	regio-in-core/Corporate/Users/Danderd/HE corce	d (new)	11 days ago	
	road rept		Julease Dodge	Aufearen Dootge	Lieuro dodge@replace.com	replo-co.com/Corporate/Users/Standard/HE-synce	d (sever)	11 dept ago	
					inceres/stitles/sss.com	myle-co.com/Corporate/Ukers/Standard/HII-conce		11 days ago	
			Jeanette Kilgore	Jeanette Kilgore	manete Algore@ mytoco.com	mple-co.com/Corporate/Uvers/Standard ME-sprce	d (never)	11 days ago	
						inglo-co.com/Corporate/Uvers/Standard/HR epice			
			kiels Whitey	Millio Walley	deluntite@rejso.com	m/o-co.com/Corporate/Uvery/Standard/HI sorce		11 days app	
			Rope Caribeell	HopeCarbert	hope control @refunction	high-coconsCorporate/Users/Danderd101-spron	d (sever)	11 days app	
					hare-entry@nyloco.com	replo-courses Corporato Unaro Standard Hill opera	a 10/26/2022 7/16/16 PM	11 days ago	
			Geold Maan	GeraldNam	grestdmass@mploce.com	info-co-consCorporate/Users/StandardHII synce	d (new)	11 dep ago	
			Gerrena Burgers	Commaillargen	germahagen@nylocacon	type co.com/Corporate/User/DanderdME opror		55 days ago	
					Bonnesbares@wyleco.com	regio co.com/Corporate/Users/Standard108 once		55 days ago	
					eue/hment@en/loca.com	regio-co.com/Corporate/Users/Standard/HR spece		11 days ago	
			Emerting Lockhort	Energia Lockhard	enectes locktert@w/eco.com	Inde-corors/Corporate/Users/Standard/Will-corors	# 15/1/2002 745/29 PM	11 days man	4 days

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

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

<u>Click here</u> 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

