SPECOPS PASSWORD POLICY

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 PASSWORD POLICY

Specops Password Policy helps you increase password security in your Microsoft Active Directory 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, compromised password list, dictionaries and passphrase settings.

Take a segmented approach and customize settings to the security needs of different user populations. Assign users who have access to sensitive data more complexity, without hindering usability for less privileged users. Alternatively, replace complexity by allowing passphrases to enforce secure policies without burdening users.

Enhance security by blocking the use of custom dictionary words unique to your organization. With the Specops Breached Password Protection service, Specops Password Policy can block the use of more than 4 billion unique known compromised passwords. The service checks for passwords found in leaked data as well as passwords found by our extensive honeypot system that monitors for passwords being used in brute force attacks happening right now.

FEATURE HIGHLIGHTS	SPECOPS SETTINGS	MICROSOFT FGPP SETTINGS	MICROSOFT ENTRA (AZURE AD) PASSWORD PROTECTION SETTINGS
Dictionary attacks & password leaked lists You can use a password dictionary, a file containing commonly used and/or compromised passwords, to prevent users from creating passwords that are susceptible to dictionary attacks.			
Create custom dictionary lists	Yes (no limit)	No	Yes (up to 1000 terms, minimum 4 characters)
Blocks passwords used in password spray attacks happening right now	Yes (new compromised passwords added daily)	No	Partially (only uses base terms in global list)
Blocked list includes 3rd party breached passwords (as recommended by orgs like NIST and NCSC)	Yes (over 4 billion unique compromised passwords)	No	No (“banned” list is not a leaked list)
Check for use of compromised passwords against daily updated list once a day	Yes	No	No

FEATURE HIGHLIGHTS	SPECOPS SETTINGS	MICROSOFT FGPP SETTINGS	MICROSOFT ENTRA (AZURE AD) PASSWORD PROTECTION SETTINGS
Ban partial use of dictionary list word	Yes (full or partial)	N/A	No
Ban use of user's first or last name	Yes (full or partial)	No	No partial ban
Block 3-letter words, abbreviations, and acronyms	Yes	N/A	No (minimum 4-characters)
Ban common character substitution	Yes	No	Missing several
Password / Passphrase complexity Complexity is commonly the character types (lower case, upper case, numeric, and special) used in the password. However, complexity is ineffective if it is predictable.			
5/5 character types	Yes	Only 3/5 types	N/A
Disallow consecutive identical characters	Yes	No	N/A
Disallow common character types at the beginning	Yes	No	N/A
Passphrase support	Yes	No	N/A
Password expirations/ history			
Password expiration reminders	Email, Balloon tip	Balloon tip only	N/A
Disallow part of current password	Yes	No	N/A
Min. number of changed characters	Yes	No	N/A

FEATURE HIGHLIGHTS	SPECOPS SETTINGS	MICROSOFT FGPP SETTINGS	MICROSOFT ENTRA (AZURE AD) PASSWORD PROTECTION SETTINGS
Password length-based aging	Yes	No	N/A
Other			
Dedicated password policy reporting tool	Yes	No	No
Dynamic password policy feedback display at password change	Yes	No	N/A
NIST and NCSC password policy templates	Yes	No	N/A
Customize end-user client failed password change message	Yes	No	N/A

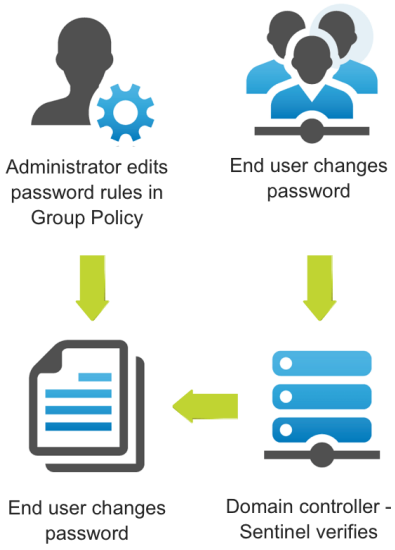
How does it work?

Specops Password Policy is built on the Group Policy engine in Active Directory and works in conjunction with existing password policy functions. It consists of the following components and does not require any additional servers or resources in your environment.

Administration Tools: Configures the central aspects of the solution, and enables the creation of Specops Password Policy settings in GPOs.

Sentinel: Verifies whether a new password matches the Specops Password Policy settings assigned to the user. The Sentinel is a password filter at the domain controllers.

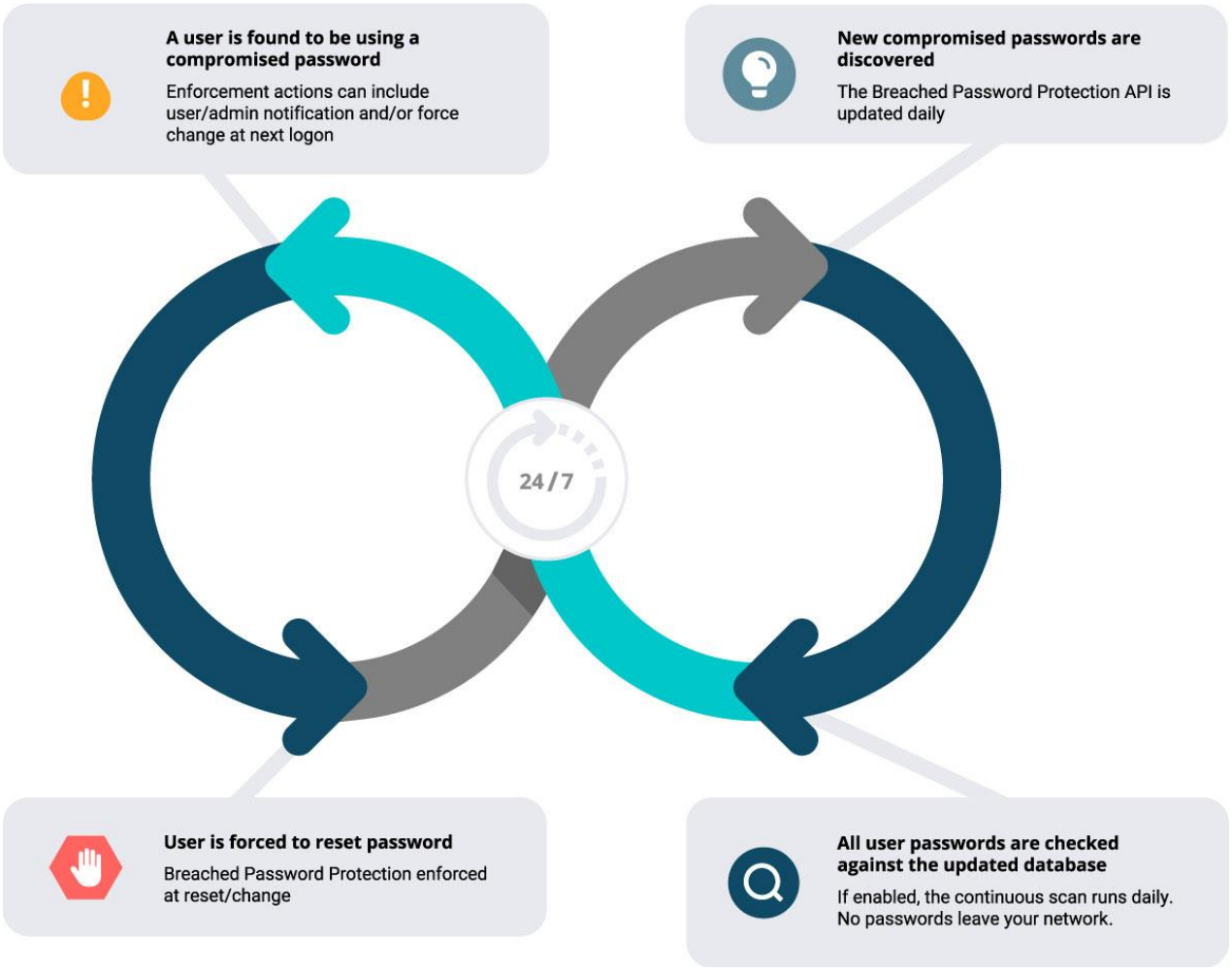
Client (optional): Displays the password policy rules when a user fails to meet the policy criteria when changing their password. Also notifies users when their passwords are about to expire.



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.

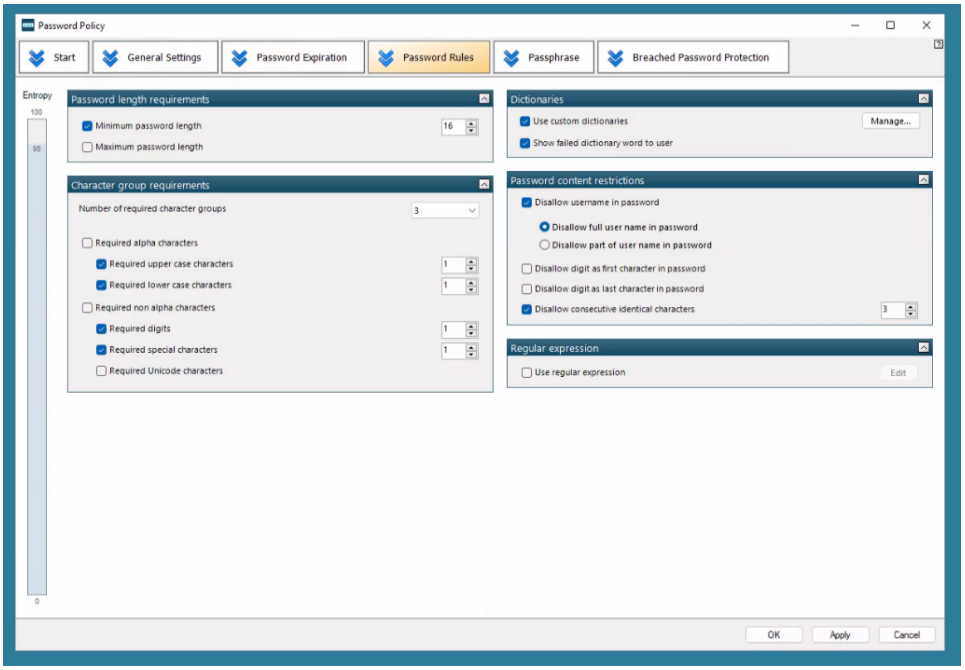


Optional remediation actions include enforcing change at next logon or notifying via text or email. The email notification can be configured to notify any desired user (including admins).

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.

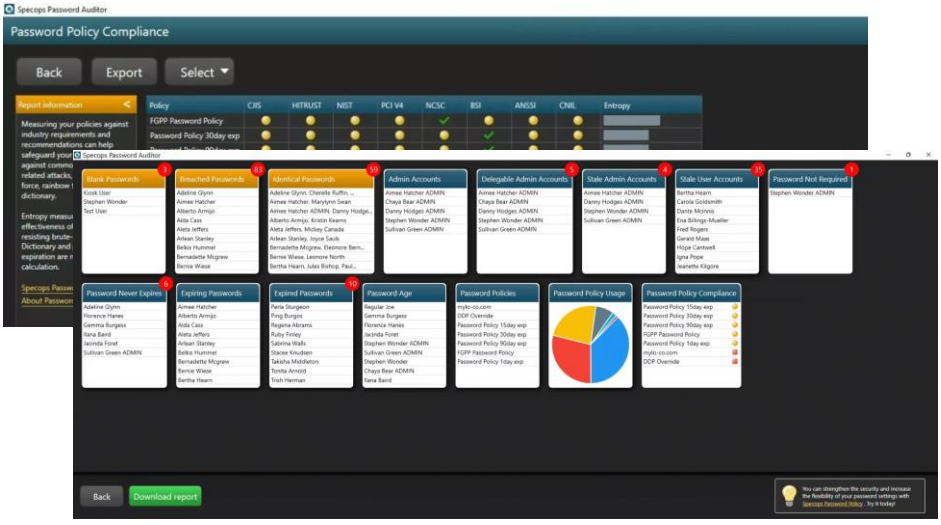
What does it look like?

Administrator Experience



The password settings can be configured from the Group Policy Management Editor.

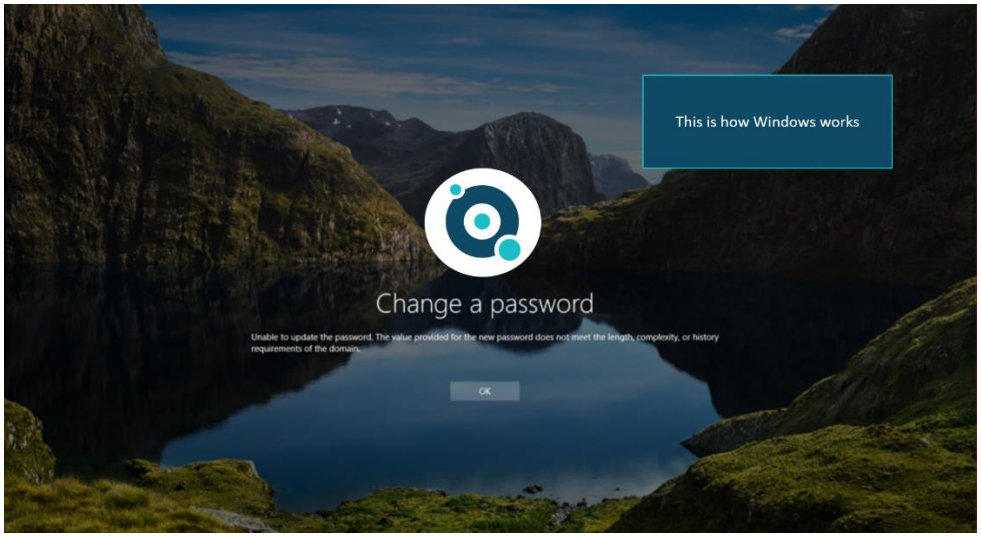
You can configure a password policy to use classic rules or passphrases.



The Password Auditor component scans and detects password related vulnerabilities.

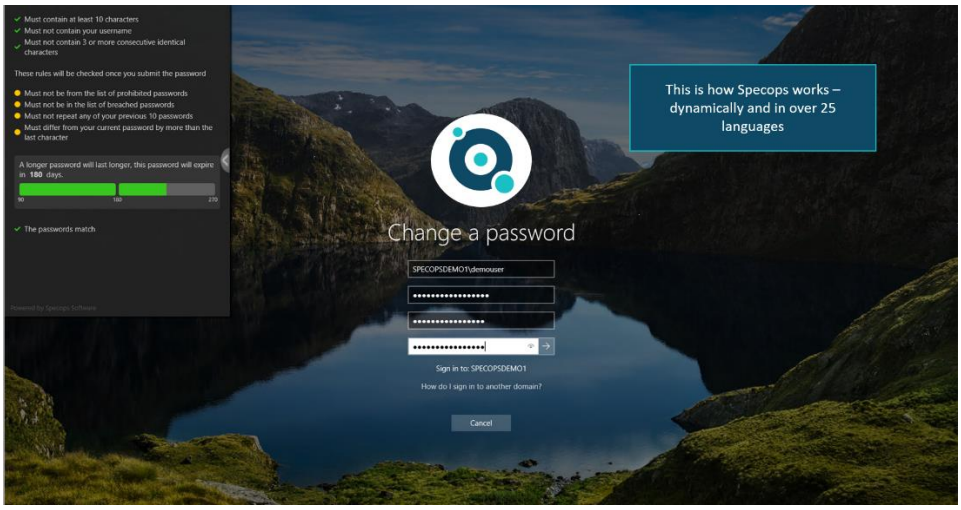
The results include multiple interactive reports with user and policy info, as well as a shareable PDF export.

End User Experience



Specops Password Policy allows you to customize the messages users see beyond the standard Windows message.

The display options include showing the found dictionary word or the rules the user has passed and still needs to pass.



Dynamic feedback at password change means end users get feedback as they type their new password.

The better end-user feedback means happier users and fewer calls to the helpdesk.

Get a Demo of Specops Password Policy

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

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