SPECOPS PASSWORD POLICY

Datasheet

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 your settings to the security needs of various 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. Comply with industry regulations by blocking the use of over 2 billion known breached passwords, as well as passwords used in real spray attacks happening right now. Manage password security across your organization simply and effectively!

FEATURE HIGHLIGHTS	SPECOPS SETTINGS	MICROSOFT FGPP SETTINGS	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	Yes (up to 1000 terms, minimum 4 characters)
Blocks passwords used in password spray attacks happening right now	Yes	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	No	No (“banned” list is not a leaked list)
Find and remove leaked passwords already in use	Yes	No	No

FEATURE HIGHLIGHTS	SPECOPS SETTINGS	MICROSOFT FGPP SETTINGS	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 character 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	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

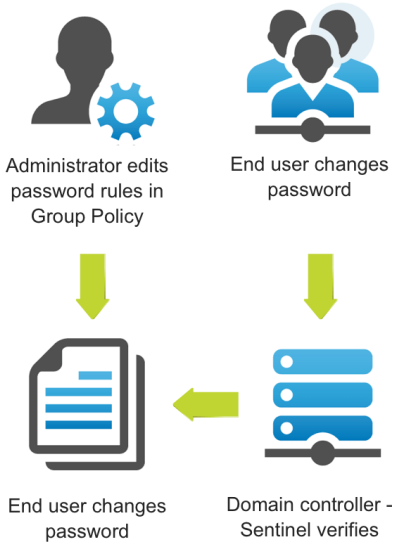
How does it work?

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.

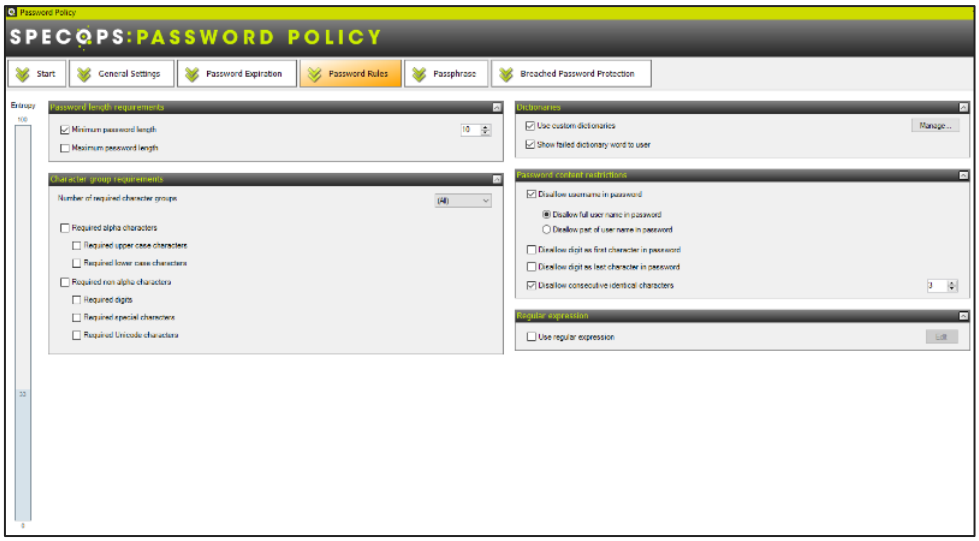
Sentinel: Verifies whether a new password matches the Specops Password Policy settings assigned to the user. The Sentinel is a password filter at the domain controllers.

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.



What does it look like?

Graphical Interface: Policy Configuration



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

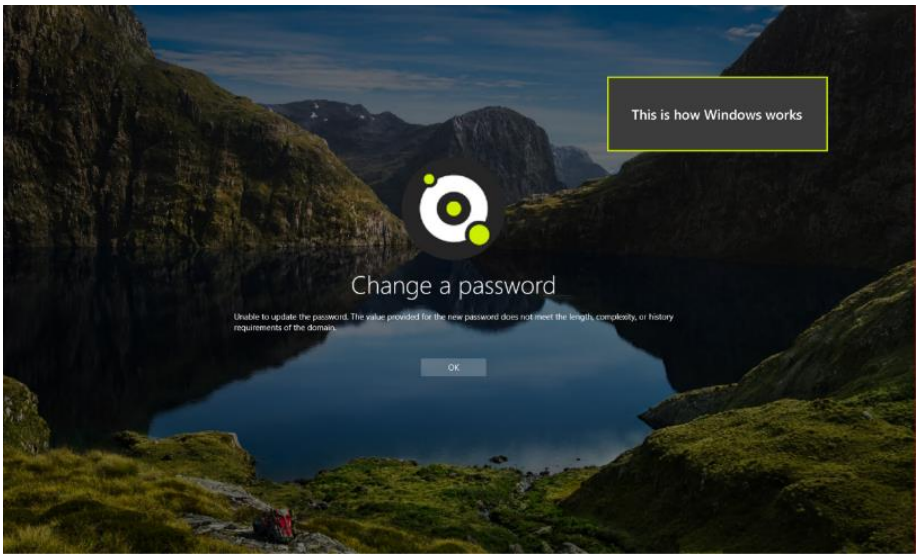
You can configure a password policy to use classic rules or passphrases.

Graphical Interface: Audit Reporting

The Specops Password Auditor component scans and detects password related vulnerabilities.

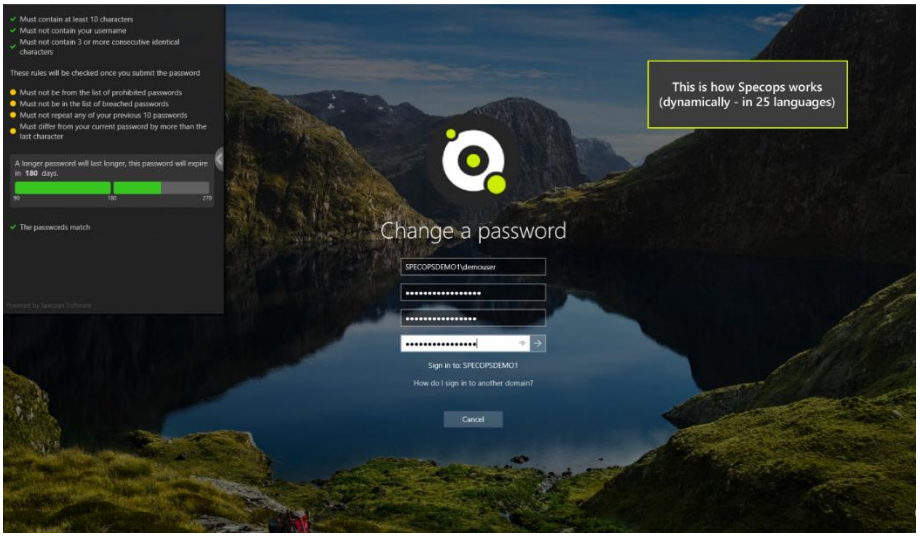
The scan results include multiple interactive reports with user and policy information, as well as a shareable PDF export.

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.

Why do customers choose Specops?

"If you are looking to strengthen passwords in Active Directory, you should definitely consider using Specops Password Policy. It's easy and intuitive to use, and works as advertised." *Vlatko Kosturjak, Security consultant* https://www.helpnetsecurity.com/2018/11/19/review-specops-password-policy/

"Creating a dictionary list of common words allows us to prevent easily predictable such as 'tombola' or 'bingo' from being used. We can restrict users from using part of their name, and prevent them from simply iterating the previous password - e.g. password1 to password2." *Tom Blackburn, Jr. Operational Support Engineer at Tombola* https://specopssoft.com/blog/tombolas-review-of-specops-password-policy-and-ureset/

"Specops Password Policy can target any GPO level, computer, user, or group population and has the added benefit of expanded password policy options, including the use of passphrases." *Timothy Warner, Microsoft Cloud and Datacenter Management (MVP)* https://4sysops.com/archives/specops-password-policy-enterprise-password-security/

"The tool is very easy to use, install quickly, and leverages existing Windows administration procedures to implement fine-grained password policies. Existing system administrators will find that integrating Specops Password Policy will require very little in terms to both time and effort, and the learning curve to use the product is minimal." *Richard Hicks, Microsoft Cloud and Datacenter Management (MVP)* http://techgenix.com/product-review-specops-password-policy/

"The new dictionary 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* http://techgenix.com/review-of-specops-password-policy/

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.