Specops Password Policy

Manage password policies across your organization! In today's digital landscape, where authentication protects identities and data, password attacks are an unpleasant reality. An effective password policy is essential to protecting the network, and sensitive data. 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, 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 banning dictionary words and allowing passphrases to enforce secure policies without burdening users. Manage password security across your organization simply and effectively!

Feature highlights	Specops settings	Microsoft FGPP settings
Dictionary 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
OOTB dictionary lists	Yes	No
Import dictionary lists	Yes	No
Password / Passphrase complexity Complexity is commonly the character types (lower case, upper case, numeric, and special) used in a password. However, complexity is ineffective if it is predictable.		
4/4 character types	Yes	Only 3/4 character types
Disallow consecutive identical characters	Yes	No
Disallow common character types at the beginning	Yes	No
Passphrase support	Yes	No
Password length / Passphrases		
Enforce minimum and maximum password length	Yes	Yes
Enable users to use passphrases	Yes	No

Password expirations / history		
Password expiration reminders	Email, Balloon tip	Balloon tip only
Minimum number of changed characters	Yes	No
Disallow part of current password	Yes	No
Other		
Dedicated reporting tool	Yes	No
Dynamic password policy display	Yes	No
OOTB NIST and NCSC password policy templates	Yes	No

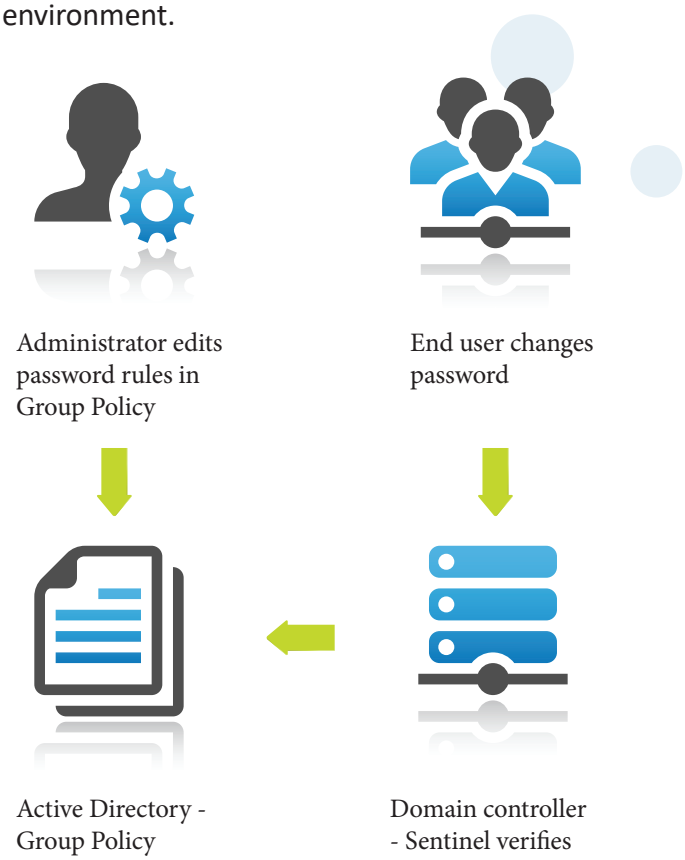
How does it work?

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.

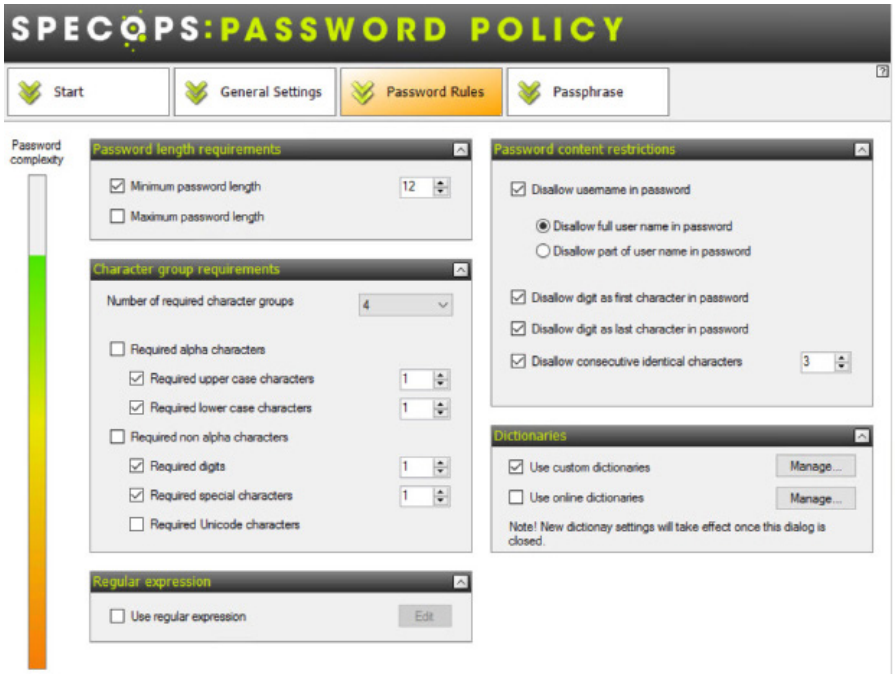
Administration Tools: Configures the central aspects of the solution, and enables the creation of Specops Password Policy settings in GPOs.

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 notifiers 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 security related weaknesses, specifically related to password settings.

The collected information is used to display multiple interactive reports containing user and password policy information.

Why customers choose Specops?

"Instead of telling users to create secure passwords, force them to, by using password filtering software. Specops has created a pretty powerful, yet easy to use, password filtering solution." *Michael Walker, Senior Consultant at Secure State* https://warroom.securestate.com/password-filtering/

"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/