ManageEngine

Azure Active Directory Password Protection

Vs

ManageEngine ADSelfService Plus

www.adselfserviceplus.com

Azure Active Directory (AD) Password Protection is a feature that aims to help organizations eliminate the risk of weak and commonly used passwords. Basically, it acts as a password filter that rejects frequently used, easily hackable passwords, such as Password123, Qwerty11, 123456, etc.

ADSelfService Plus is an integrated Active Directory self-service password management and single sign-on (SSO) solution. The Password Policy Enforcer feature in ADSelfService Plus accomplishes everything that Azure AD Password Protection does and more.

The table below provides a detailed comparison between ADSelfService Plus' Password Policy Enforcer and Azure AD Password Protection.

Features	ADSelfService Plus	Azure AD Password Protection
Prevents banned passwords	✓	✓
Enables you to add custom values to the banned password list	✓	✓
Provides visibility into all banned passwords	✓	✗
Settings can be enforced granularly based on OU and group	✓	✗
Password cannot contain part of the username	✓	✓
Applies to on-premises AD	✓	✓ (requires Azure AD P1 subscription)
Applies to Azure AD	✓	✓ (through password sync)
Display customized error message in Windows logon screen during password change	Just over $2 per user, per year	$12 per user, per year (only for Azure AD with ability to add custom banned passwords) $72 per user, per year (for on-premises AD)

ADSelfService Plus versus AD Group Policy Password Policy Settings

Beyond banned passwords, ADSelfService Plus also provides other advanced password policy settings that are not available in on-premises AD. These settings help organizations improve password security and comply with regulations such as the National Institute of Standards and Technology (NIST). The following table compares ADSelfService Plus to Domain Password Policy Settings available in on-premises AD.

Features	ADSelfService Plus	Active Directory Password Policy Settings
Password cannot contain patterns such as qwerty, asdf, 1234, etc.	✓	✗
Password cannot contain palindromes (characters that read the same backward as forward, such as racecar or the number 10801)	✓	✗
Password must contain at least one Unicode character	✓	✗
Password cannot repeat a character more than two times in a row	✓	✗
Password cannot contain five consecutive characters from an old password	✓	✗
Password must begin with a letter	✓	✗
Users can bypass complexity requirements when the password length exceeds a predefined limit (say, 20 characters)	✓	✗
Maximum password length	✓	✗
Minimum password length	✓	✓
Password cannot contain five consecutive characters that are in the username	✓	✗
Option to force any or all of these character group requirements: • Uppercase characters • Lowercase characters • Special characters • Numeric characters	✓ (All four can be enforced)	✓ (Only three are enforced)

Summary

ADSelfService Plus is a powerful alternative to Azure AD Password Protection for several reasons. It compensates for the lack of advanced policies and customization options in Azure AD Password Protection and AD Password Policy Settings, and with pricing starting at just over $2 per user, per year, it's a lot more affordable. With ADSelfService Plus, organizations can reduce help desk calls, improve password security and the end-user experience, and comply with password requirements mandated by IT best practices, government, and industry regulations.