



ADSelfService Plus' Password Policy Enforcer

VS.

**Active Directory
Group Policy Object-based
password policy**

VS.

**Active Directory
Fine-grained password policies**

Why strong password policies matter

Passwords are the first line of defense against cyberattacks, which highlights the importance of having a strong password. Some hackers find that cracking passwords is the easiest way to gain access to a user account in Windows Active Directory. This doesn't come as a surprise when considering the password policy and controls in Active Directory haven't been changed in over a decade. Hackers can use age-old hacking strategies like brute-force attacks, dictionary attacks, and rainbow table attacks to acquire these passwords.

How good is the Microsoft password policy?

Microsoft allows you to apply password policies to your Active Directory users with a combination of a Group Policy Object (GPO)-based domain password policy and fine-grained password policies (FGPPs). One major difference between the two methods is that with FGPPs, there can be more than one password policy in the same domain. It's important to remember that regardless of what you choose, the provided password controls are the same.

Enhanced password security with ADSelfService Plus

The best way to enhance security is by implementing a solution that both protects your Active Directory passwords and works well with GPO- and FGPP-based policies. This solution should allow additional control over password policies without requiring a complete redesign of your current AD environment.

The ADSelfService Plus advantage

- Create multiple password policies for a single Active Directory domain and assign them to users based on OUs and groups.
- Enhance your password policy with ADSelfService Plus' password policy settings, and safeguard users' passwords from various password attacks.
- Enforce your enhanced password policy settings when users change their password through the Windows logon (Ctrl+Alt+Del) screen as well as when admins reset passwords through Active Directory Users and Computers (ADUC).
- Display your chosen password requirements to end users during change password operations on the Ctrl+Alt+Del screen.

The following chart compares the password policy settings of ManageEngine's ADSelfService Plus with those in Windows Active Directory.

| Features | ADSelfService Plus Password Policy Enforcer | Group Policy Object password policy | Fine-grained password policies |
|---|---|---|--------------------------------------|
| Key features | | | |
| Option to force any or all of the below character group requirements: * Uppercase characters * Lowercase characters * Special characters * Numeric characters | ✓ (All four can be enforced) | ✓ (Only three are enforced) | ✓ (Only three are enforced) |
| Option to force Unicode characters | ✓ | ✗ | ✗ |
| Breached password protection | ✓ | ✗ | ✗ |
| Password must not be a dictionary word | ✓ | ✗ | ✗ |
| Option to include a custom dictionary | ✓ | ✗ | ✗ |
| Password must not include specific patterns | ✓ | ✗ | ✗ |
| Password must not be a palindrome | ✓ | ✗ | ✗ |
| Restricts the use of previously used passwords | ✓ | ✓ | ✓ |
| Password cannot repeat a character more than N times in a row | ✓ | ✗ | ✗ |
| Password cannot contain N consecutive characters from an old password | ✓ | ✗ | ✗ |
| Password cannot contain N consecutive characters that are in the username | ✓ | ✗ | ✗ |
| Password must begin with a letter | ✓ | ✗ | ✗ |
| Allow users to bypass complexity requirements when password length exceeds a predefined limit (say, 20 characters) | ✓ | ✗ | ✗ |
| Maximum password length | ✓ | ✓ | ✓ |
| Minimum password length | ✓ | ✓ | ✓ |

| Other features | | | |
|---|---|---|-------------------------|
| Password policies can be enforced granularly based on OUs and groups | ✓ | ✗ | ✗ (Group-based only) |
| Password policy enforcement during a password change from the Windows logon screen | ✓ | ✓ | ✓ |
| Password policy enforcement during password resets by admins from ADUC | ✓ | ✓ | ✓ |
| The exact password complexity requirements are displayed to end users in the Windows logon screen during change password operations | ✓ | ✗ | ✗ |

Conclusion

Microsoft's password policy controls won't protect your Active Directory users' passwords. Though FGPPs allow you to have more than one password policy for a domain, the password controls are the same as Group Policy's, and deployment is only possible through group membership, not through OUs.

ADSelfService Plus—with its **Password Policy Enforcer**—provides a complete solution that protects your Active Directory domain users' passwords. The ability to have multiple password policies in a single domain distributed through user group memberships or OUs is beneficial for most Active Directory installations. You can protect passwords against dictionary and password pattern attacks, which is vital to mitigate cyberattacks that utilize these techniques. In a nutshell, ADSelfService Plus is a secure password solution for any Active Directory domain.



Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus

RecoveryManager Plus | M365 Manager Plus

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces.

For more information about ADSelfService Plus, visit
www.manageengine.com/products/self-service-password.

\$ Get Quote

↓ Download