ManageEngine

Comparison Document

# ADSelfService Plus' Password Policy Enforcer

Vs

# Active Directory Group Policy Object-based password policy

Vs

# Active Directory Fine-grained password policies

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 controls and password policy 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 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 the GPO and FGPP-based policies. This solution should allow additional control over password policies without requiring a complete redesign of your current AD environment.

With the **Password Policy Enforcer** in ADSelfService Plus, you get exactly that.

## The ADSelfService Plus advantage

- Enable multiple password policies in a single Active Directory domain that can be assigned 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.

| Feature | ADSelfService Plus' Password Policy Enforcer | Group Policy Object password policy | Fine-grained password policies |
|---|---|---|---|
| **Key features** | | | |
| Password must not be a dictionary word | ✓ | ✗ | ✗ |
| Password must not include specific patterns | ✓ | ✗ | ✗ |
| Password must not be a palindrome | ✓ | ✗ | ✗ |
| Password must contain at least one Unicode character | ✓ | ✗ | ✗ |
| Password history enforcement during password resets by admins through ADUC | ✓ | ✗ | ✗ |
| 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 | ✓ | ✗ | ✗ |

| | | | |
|---|---|---|---|
| Allow users to bypass complexity requirements when 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 | ✓ | ✗ | ✗ |
| **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 is displayed to end users in the Windows logon screen during change password operations | ✓ | ✗ | ✗ |

| Mandatory character group requirements | | | |
|---|---|---|---|
| Option to force any or all of the below character group requirements:<br>• Uppercase characters<br>• Lowercase characters<br>• Special characters<br>• Numeric characters | ✓ (All four can be enforced.) | ✓ (Only three are enforced.) | ✓ (Only three are enforced.) |
| Option to force Unicode characters | ✓ | ✗ | ✗ |

## Conclusion

Microsoft has not improved the security of their password policy controls in terms of protecting 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 with Group Policy and the deployment is only 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 though user group memberships or OUs is beneficial for most Active Directory installations. The ability to protect passwords against dictionary and password pattern attacks is important for mitigating cyberattacks that utilize these techniques. In a nutshell, ADSelfService Plus is a secure password solution for any Active Directory domain.