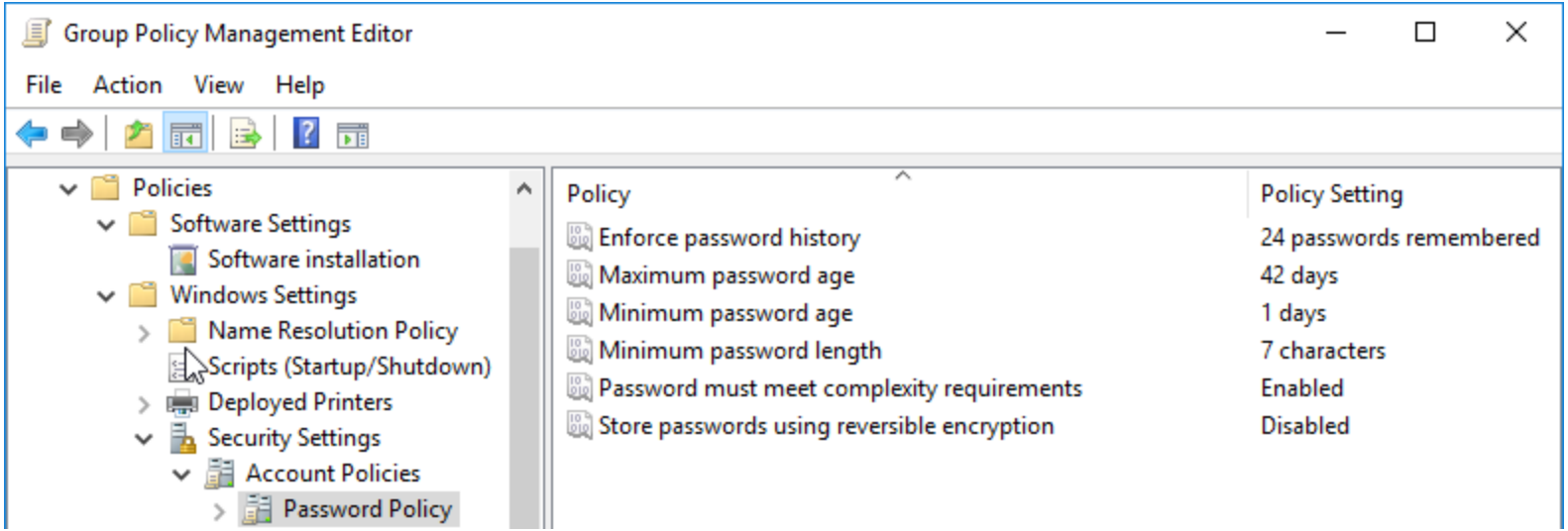
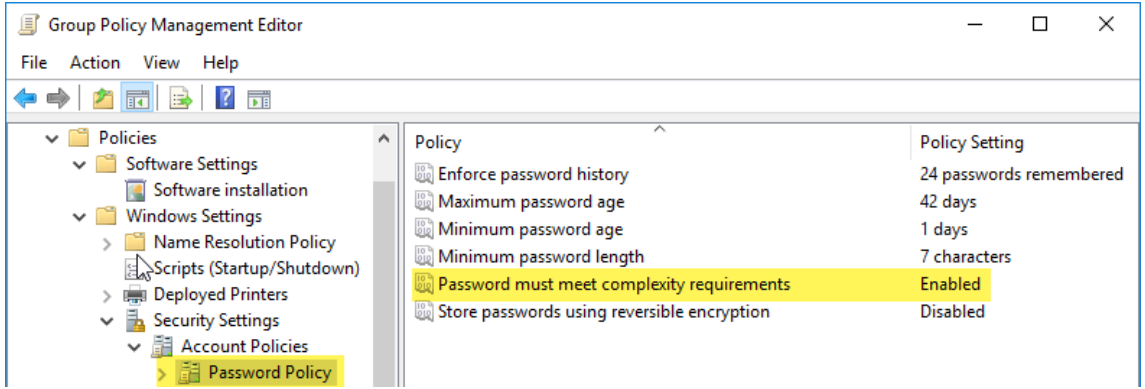
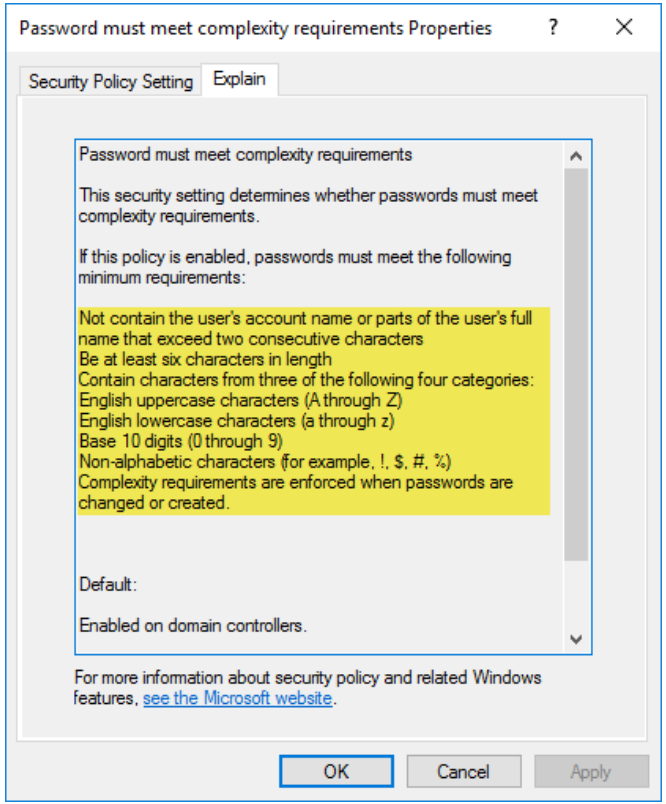
Securing Passwords with GPO Password Policies



Microsoft Password Complexity Requirements

In Windows 10 and Active Directory, we can enable Microsoft's **Password must meet complexity requirements** policy, which ensures user passwords are complex. This is enabled by default in the Default Domain Policy in AD.



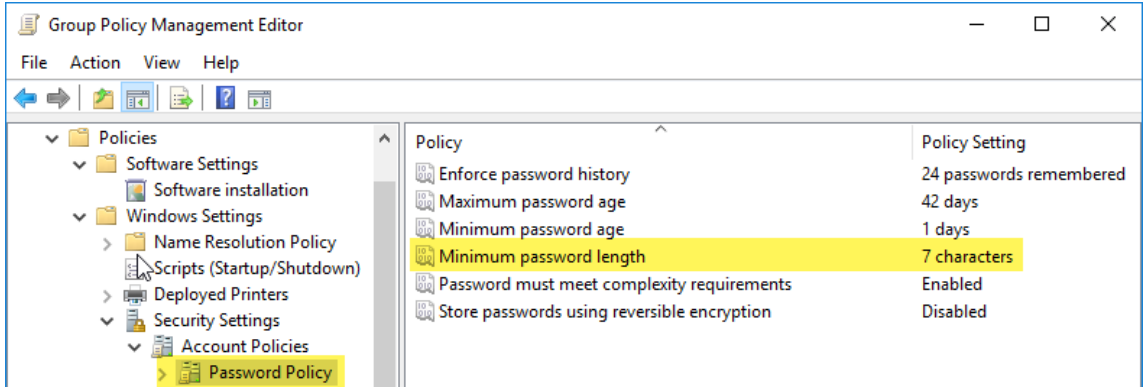


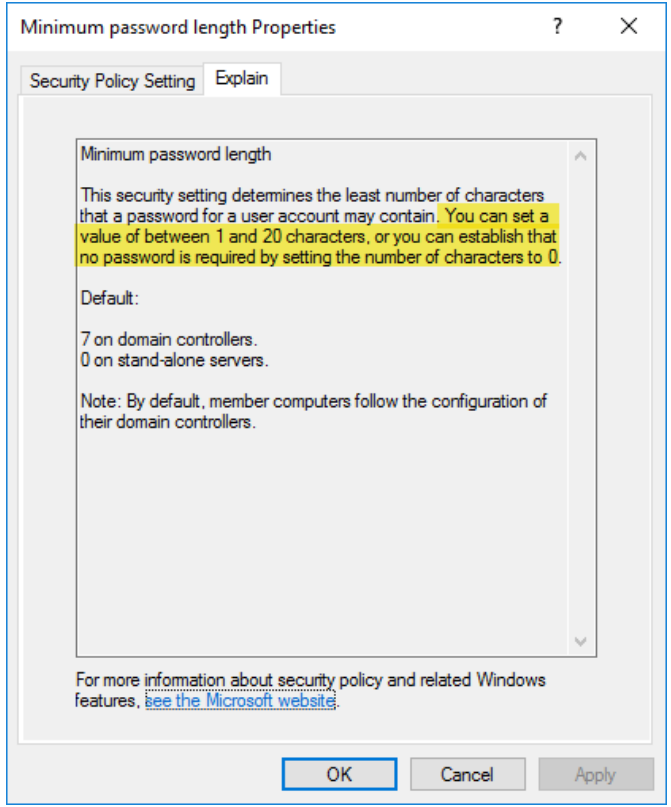
Password Complexity Requirement Details

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
  - Complexity requirements are enforced when passwords are changed or created.

Microsoft Minimum Password Length

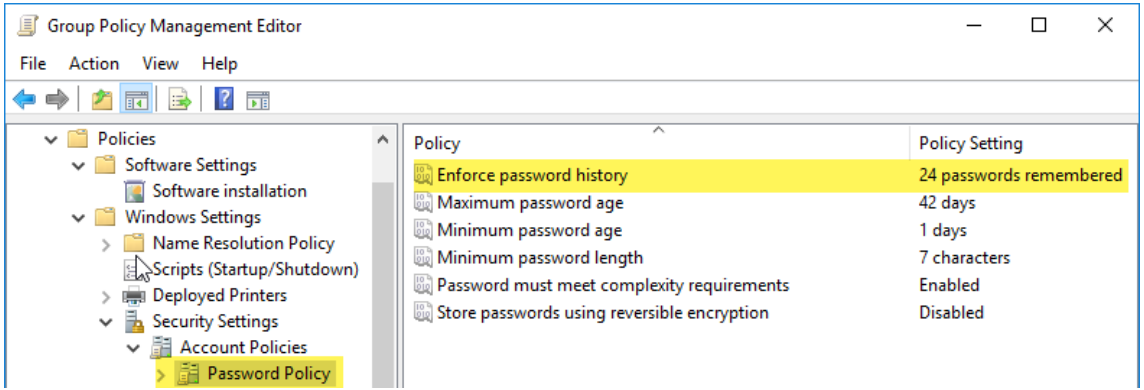
We can also enable Microsoft's **Minimum password length** policy to further make a password more secure, which ensures user passwords are complex. This value is set to 7 by default for the Default Domain Policy in AD.

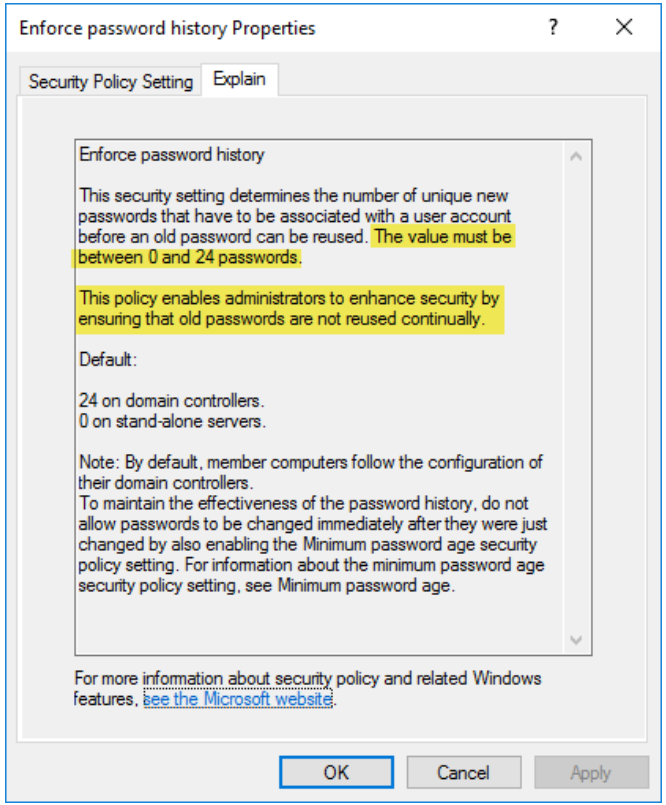




Microsoft Enforce Password History

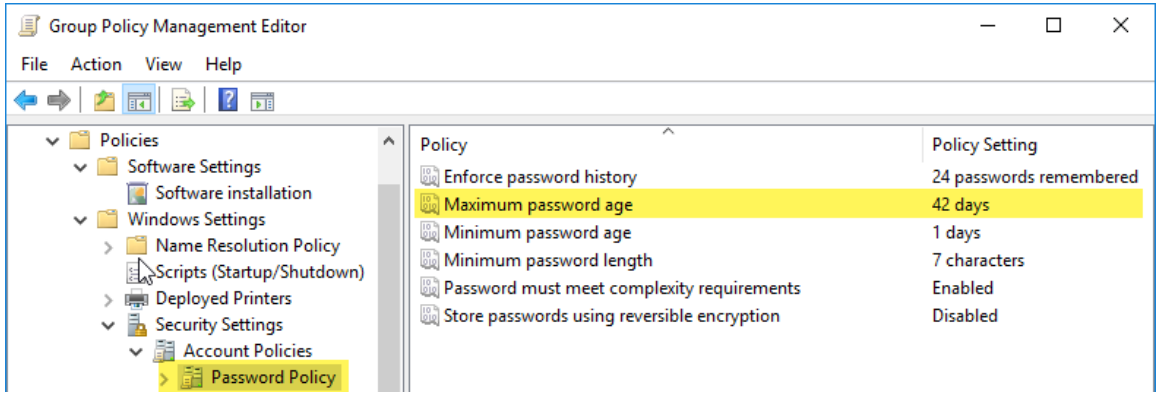
We can also enable Microsoft's **Enforce Password History** policy to further make a password more secure, which ensures user's don't reset their password to previously used passwords. This value is set to 24 by default for the Default Domain Policy in AD.

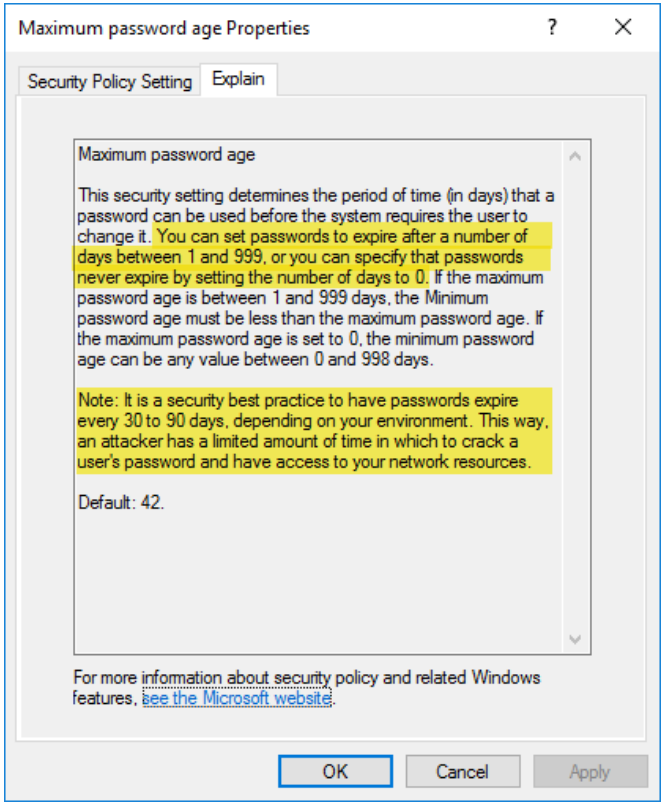




Microsoft Maximum Password Age

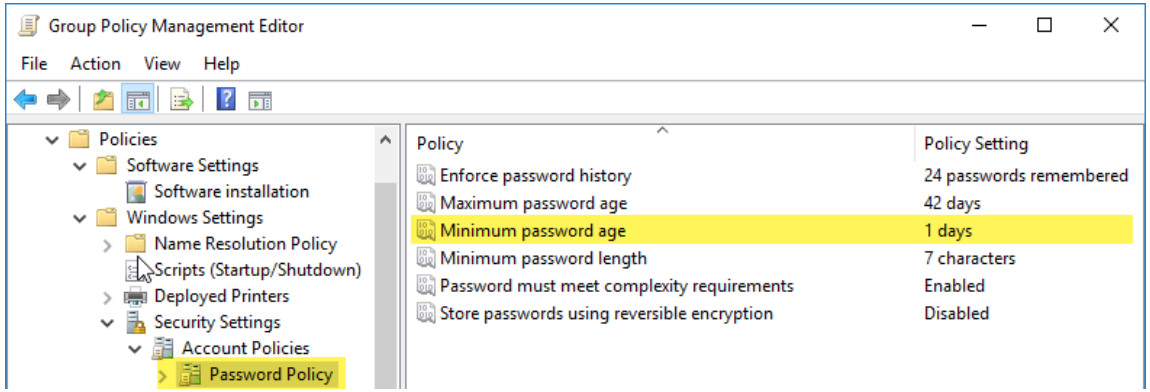
We can also enable Microsoft's **Maximum Password Age** policy to further make a password more secure, which ensures are changed after a certain amount of time. This value is set to 42 by default for the Default Domain Policy in AD.

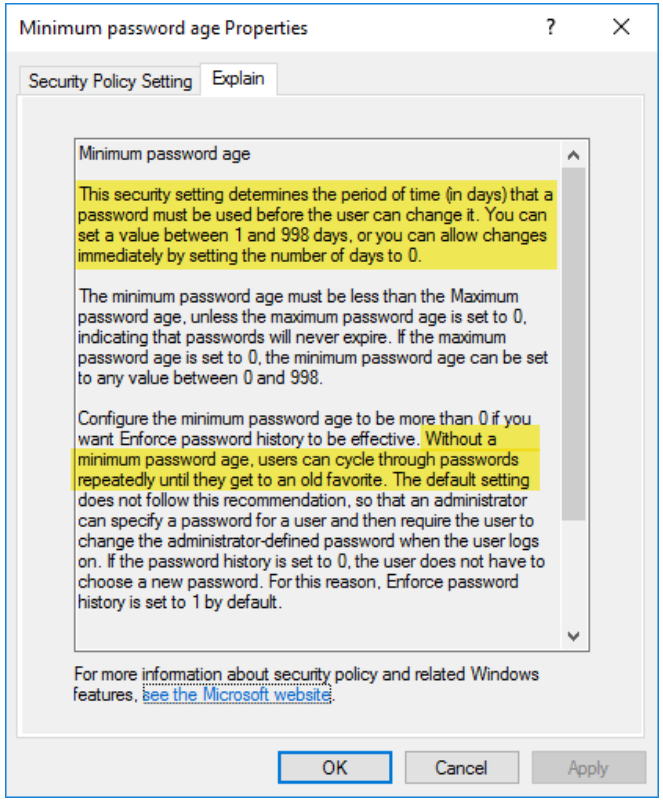




Microsoft Minimum Password Age

We can also enable Microsoft's **Minimum Password Age** policy to further make a password more secure, which ensures users must wait a certain amount of time before they can change a password. This value is set to 2 by default for the Default Domain Policy in AD.





Microsoft Reversible Encryption

We can also enable Microsoft's **Store Passwords using Reversible Encryption** policy if we want to be able to decrypt passwords and view them in plain text. This is not recommended and is disabled in the Default Domain Policy in AD. When disabled, passwords are stored as a hash that cannot be decrypted.