Configure Domain User Password Policy

- **Access Group Policy Management (Tools/Group Policy Manage)**
- **Right click on Default domain policy, Click on Edit**
- **(Computer configuration/Policies/Windows Settings/Security Settings/Account Policies/Password Policy)**

Enforce password history

This security setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.

This policy enables administrators to enhance security by ensuring that old passwords are not reused continually.

Default:

24 on domain controllers.

0 on stand-alone servers.

Note: By default, member computers follow the configuration of their domain controllers.

To maintain the effectiveness of the password history, do not allow passwords to be changed immediately after they were just changed by also enabling the Minimum password age security policy setting. For information about the minimum password age security policy setting, see Minimum password age

Maximum password age

This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the Minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

Note: It is a security best practice to have passwords expire every 30 to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to crack a user's password and have access to your network resources.

Default: 42.

Minimum password age

This security setting determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 998 days, or you can allow changes immediately by setting the number of days to 0.

The minimum password age must be less than the Maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998.

Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite. The default setting does not follow this recommendation, so that an administrator can specify a password for a user and then require the user to change the administrator-defined password when the user logs on. If the password history is set to 0, the user does not have to choose a new password. For this reason, Enforce password history is set to 1 by default.

Default:

1 on domain controllers.

0 on stand-alone servers.

Note: By default, member computers follow the configuration of their domain controllers.

Minimum password length

This security setting determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.

Default:

7 on domain controllers.

0 on stand-alone servers.

Note: By default, member computers follow the configuration of their domain controllers.

This security setting determines whether passwords must meet complexity requirements.

If this policy is enabled, passwords must meet the following minimum requirements:

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.

Default:

Enabled on domain controllers.

Disabled on stand-alone servers.

Note: By default, member computers follow the configuration of their domain controllers.

Store passwords using reversible encryption

This security setting determines whether the operating system stores passwords using reversible encryption.

This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

This policy is required when using Challenge-Handshake Authentication Protocol (CHAP) authentication through remote access or Internet Authentication Services (IAS). It is also required when using Digest Authentication in Internet Information Services (IIS).

Default: Disabled.

Account lockout duration

This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

Account lockout threshold

This security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers count as failed logon attempts.

Default: 0.

Reset account lockout counter after

This security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes.

If an account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.