Configuring Password Policies

The security provided by a password system depends on the passwords being kept secret at all times. Thus, a password is vulnerable to compromise whenever it is used, stored, or even known. In a password-based authentication mechanism implemented on a system, passwords are vulnerable to compromise at several essential stages related to password assignment, distributions, management, and use:

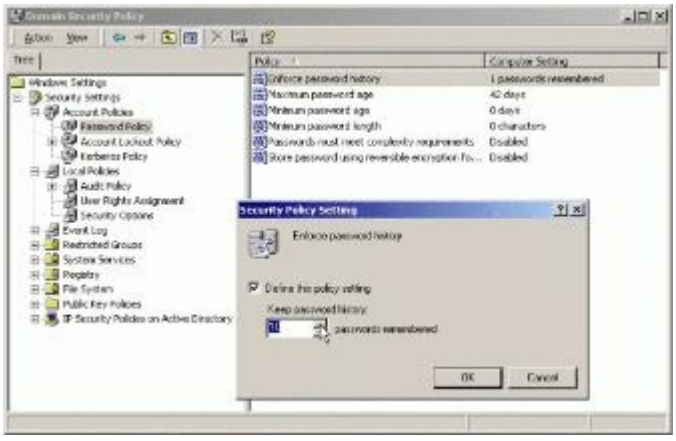
- A password must be initially assigned to a user when enrolled on the system;
- A user's password must be changed periodically;
- The system must maintain a "password database;"
- Users must remember their passwords;
- Users must enter their passwords into the system at authentication time; and
- Employees may not disclose their passwords to anyone. This includes administrators and IT managers.

Password policies can be set depending on the needs of the organization. For example, it is possible to specify minimum password length, no blank passwords, and maximum and minimum password age. It is also possible to prevent users from reusing passwords and ensure that they use specific characters in their passwords, making the passwords more difficult to crack. The uses of these policies are described and implemented as follows:

Note: Procedures for setting initial user passwords are provided in subsection "Creating user accounts" of this document.

- **Enforce Password History: Enforce password history** sets how frequently old passwords can be reused. This policy can be used to discourage users from changing back and forth between a set of common passwords. Windows 2000 can store up to 24 passwords for each user in the password history. By default, Windows 2000 stores one password in the password history.

  To disable this feature, set the size of the password history to zero. To enable this feature, set the size of the password history using the **passwords remembered** field. Windows 2000 will then track old passwords using a password history that is unique for each user, and users will not be allowed to reuse any of the stored passwords.

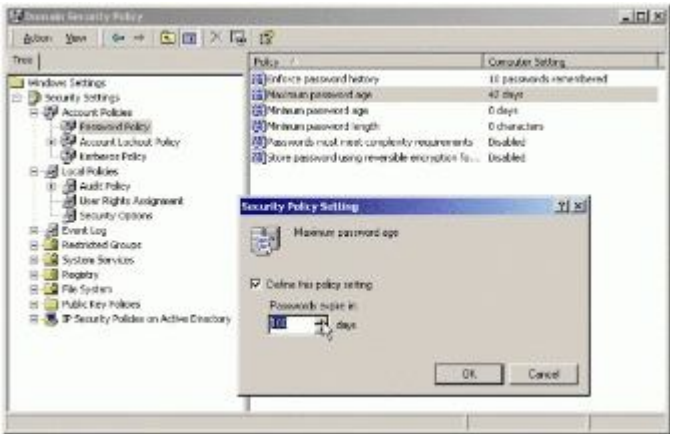


  Note: To discourage users from cheating **Enforce password history**, they should not be allowed to change passwords immediately. This will prevent users from changing their passwords several times to get back to their old passwords.

- **Maximum Password Age: Maximum password age** determines how long users can keep a password before they have to change it. The aim is to periodically force users to change their passwords. When this feature is used, set a value that makes sense for the specific network environment it is being applied to. Generally, a shorter period is

used when security is very important and a longer period when security is less important.

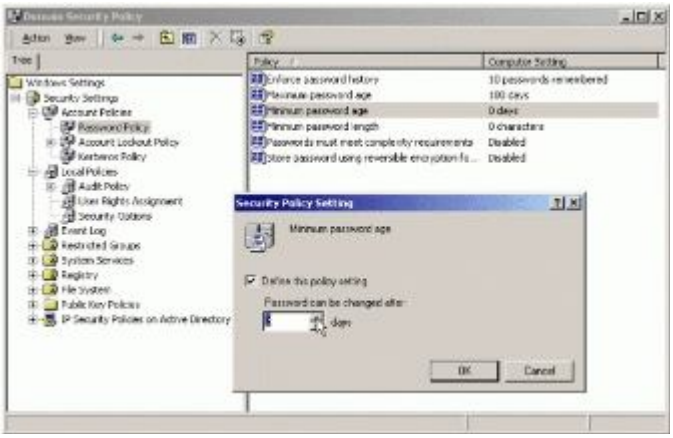
The default expiration date is 42 days; however, it can be set to any value from 0 to 999. A value of zero specifies that passwords do not expire. Although it may be tempting to set no expiration date, users should change passwords regularly to ensure the network's security. Where security is a concern, good values are 30, 60, or 90 days. Where security is less important, good values are 120, 150, or 180 days.



Note: Windows 2000 notifies users when they're getting close to the password expiration date. Anytime the expiration date is less than 30 days away, users see a warning when they log on stating that they have to change their password within so many days.

- **Minimum Password Age: Minimum password age** determines how long users must keep a password before they can change it. This field can be set to prevent users from cheating the password system by entering a new password and then changing it right back to the old one.

  By default, Windows 2000 lets users change their passwords immediately. To prevent this, set a specific minimum age. Reasonable settings are from three to seven days. In this way, users are less inclined to switch back to an old password but are able to change their passwords in a reasonable amount of time if they want to.



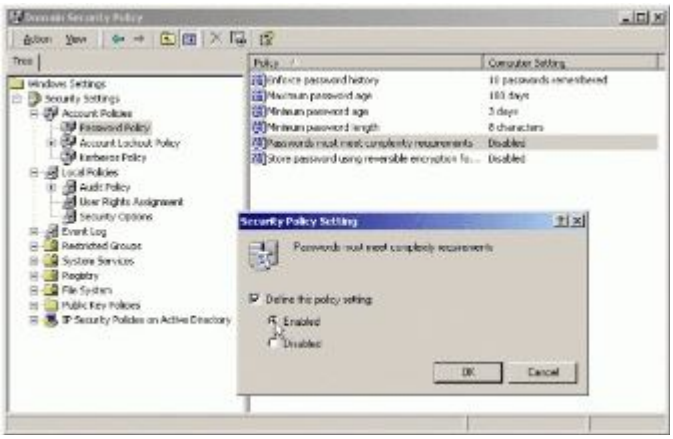
- **Minimum Password Length: Minimum password length** sets the minimum number of characters for a password. If it hasn't been changed already, the default setting should be changed immediately. The default is to allow empty passwords (passwords with zero characters), which is definitely not a good idea.

  For security reasons, passwords of at least eight characters are required. The reason for this is that long passwords are usually harder to crack than short ones. If greater security is needed, the minimum password length can be set to a maximum of 14 characters.

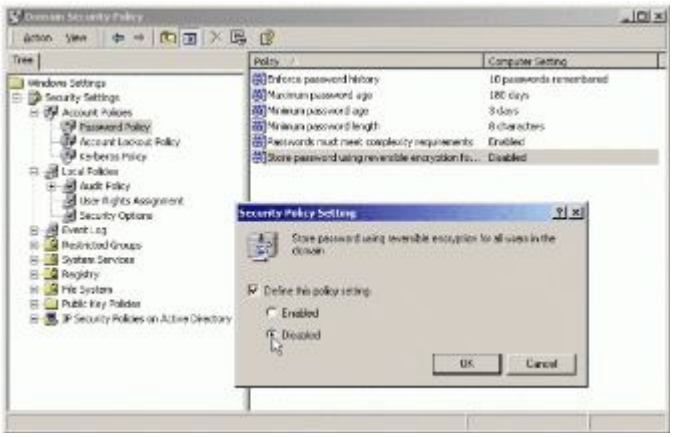
  Note: The minimum password length for the Evaluated Configuration is 8 characters.

- **Passwords Must Meet Complexity Requirements:** Beyond the basic password and account policies, Windows 2000 includes facilities for creating additional password controls. The functions implemented by enabling the **Passwords must meet complexity requirements** setting in Password Policy are enforced when a user or administrator attempts to change the password for a user account. For example, the strong password filter requires that passwords contain characters from at least three (3) of the following four (4) classes:

Description	Examples
1. English Upper Case Letters	A, B, C, ... Z
2. English Lower Case Letters	a, b, c, ... z
3. Westernized Arabic Numerals	0, 1, 2, ... 9
4. Non-alphanumeric ("special characters")	For example, !,$,#,%).



- **Store Password Using Reversible Encryption:** Passwords in the password database are encrypted. This encryption cannot normally be reversed. If there is a need to allow the encryption to be reversed, enable **Store password using reversible encryption for all users in the domain**. Passwords are then stored with reversible encryption and can be recovered in case of emergency. Enabling this feature is **not recommended**.



Top Of Page