

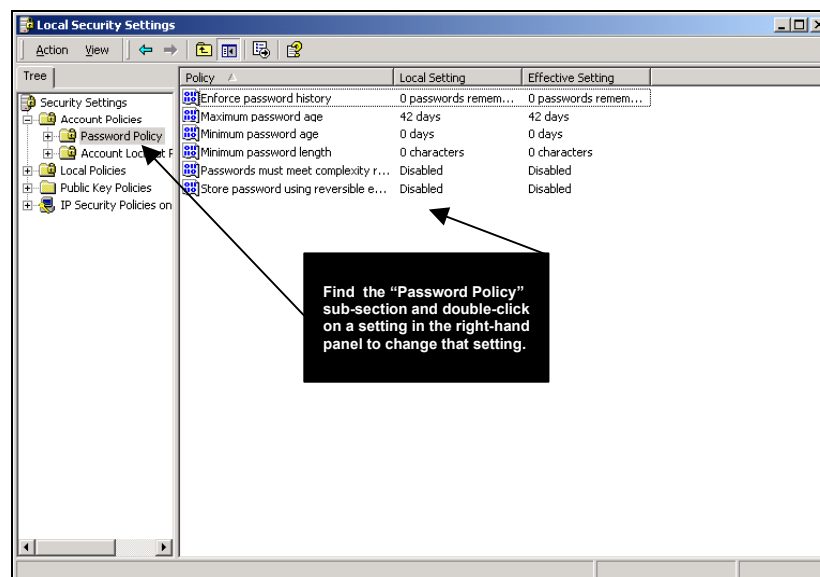
Changing the behaviour of Logon Passwords in Windows 2000

The default configuration settings of Windows 2000 is for all passwords to automatically expire after 42 days. When a password expires the user is prompted to change his password at the next logon. Many users will either want to change the 42-days default to a different number, or they will want to disable being forced to regularly change their logon password.

The above is just one of the settings that you can configure in Windows 2000 to change the behaviour of Logon Passwords.

Where to change the configuration options for Logon Passwords

- Go to **Start \ Settings \ Control Panel.**
- Double-click on **Administrative Tools.**
- Double-click on **Local Security Policy.**
- This opens up the “Local Security Policy” window which looks as illustrated below. This is where you change everything to do with Logon Passwords.



Setting the various options

Enforce Password History

You can configure Windows 2000 to remember x number of previous passwords so that, for added security, end-users cannot re-use previous passwords whenever they are prompted to enter a new password because their existing password has expired.

You can set this setting to anything between 0 and 24. Set it to **0 (zero)** if you do not want Windows 2000 to remember any previous passwords used by end-users.

Maximum Password Age

Through this setting you can configure Windows 2000 to force users to change their passwords at regular intervals. If you set this setting to **0 (zero)** then passwords will never expire and users will never be forced to change their passwords. If you set it to anything between 1 and 999 then after that number of days since your last change of password, Windows 2000 will force you to change your password.

Minimum Password Age

You can configure Windows 2000 to prevent users from changing their passwords too soon after their last change of password. If you set this setting to **0 (zero)** then users will be able to change passwords at any time that they choose to do and not just whenever the system forces them to change their password. If you set this setting to anything between 1 and 999, for example 3, then during the first three days after his last change of password an end-user will not be able to change his password again. On the 4th day, however, he will again be able to change his password.

Tip : If you wish to prevent users from being able to change their passwords other than when the system forces them to, then set this setting to the same number of days, or a higher number of days, than the "Maximum Password Age" setting.

Minimum Password Length

Use this setting if you wish to ensure that passwords are of a certain minimum length, thereby making them more secure through intruders not being able to guess them easily.

If you leave this setting set at the normal default of 0 (zero), then this tells Windows 2000 that your users are NOT required to have a password, ie. they can have a blank password. If you want security for your Windows 2000 PC, then you should change this default immediately.

If you decide to set this setting to something other than 0 (zero), then a good minimum for this setting is **5**. The maximum value for this setting is 14.

Passwords must meet complexity requirements

Through this setting you can configure Windows 2000 to force users to use highly complex passwords for increased security.

This setting is **disabled** by default - the result is that, as a user, you can use any password that you find easy to memorise. While it is a good thing for the end-user it is less secure as it means that users can choose passwords like "January", "Robert", etc..., passwords which can be guessed by potential intruders who know the end-user and what he/she might choose as a password. On the other hand, if you enable this setting Windows 2000 will force users to use passwords that are difficult to guess but which by the same token might also be difficult to remember by the end-user, e.g. "lf-jlEE64d", and that in itself may prove an ever worse security issue through users writing passwords down and sticking them on their monitors ! For this reason this setting is usually left **disabled**.

Store passwords using reversible encryption

This setting is **disabled** by default, providing the strongest level of security of user passwords.

Some organisations, however, prefer to enable this setting as it offers them a "back-door" entrance to passwords should all the passwords for the PC be forgotten or lost.

And, remember

The above instructions are valid only for standalone Windows 2000 PCs.

If your Windows 2000 PC is connected to a network, where your username and password are what allows you to access the network, then the configuration of Logon Passwords behaviour is always done on the network fileserver, centrally, not on each individual Windows 2000 PC.

ooooooooOooooooooo