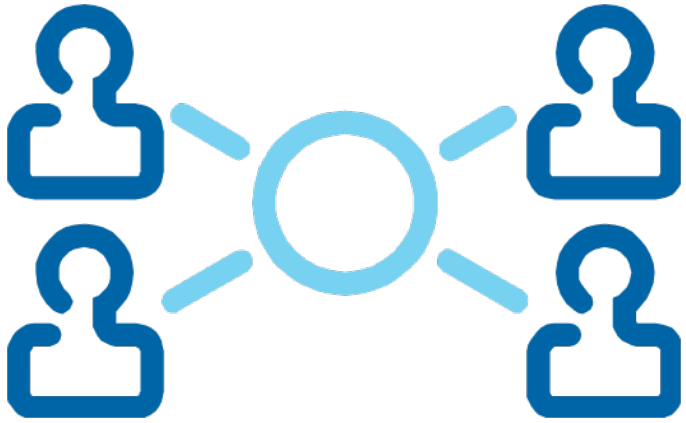
Setting the Local Security Policies

April 28, 2010

Security for Administrators

While larger companies have their servers secured in secluded and well protected areas, in a small business, servers can be in rooms around other employees. We want to have password security somewhat more complex than what we see on the Internet. We need to set the password policy after loading the computer, the Service Packs and Windows Updates and prior to adding our administrators.



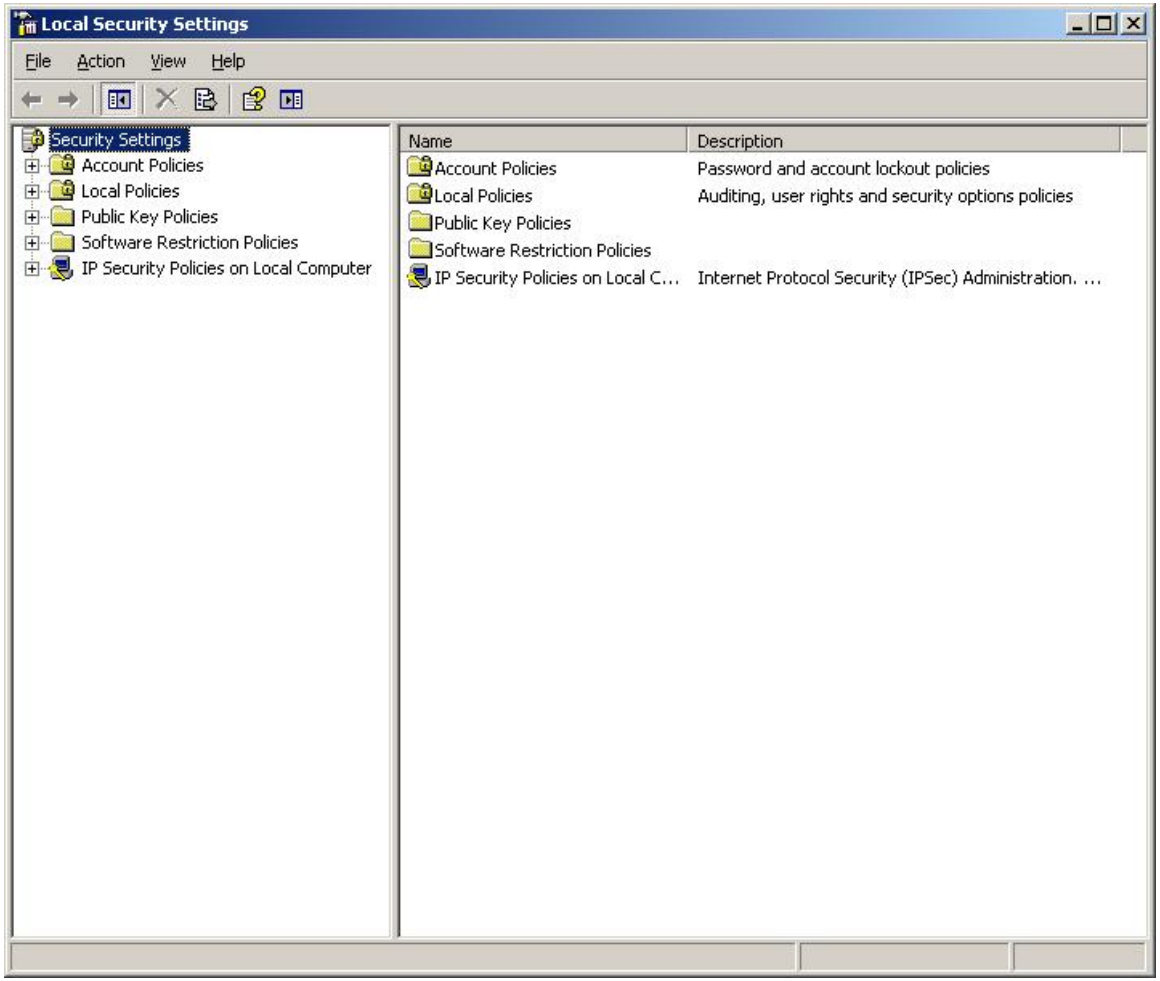
Setup Local Policies

To set the local polices for the Windows server, we select the Start button, Administrative Tools and then Local Security Policy.

The Local Security Settings Window

The Local Security Setting window appears and we can notice the Account Policies, Local Policies, Public Key Policies, Software Restriction Policies and IP Security Policies on Local Computer in the left pane.

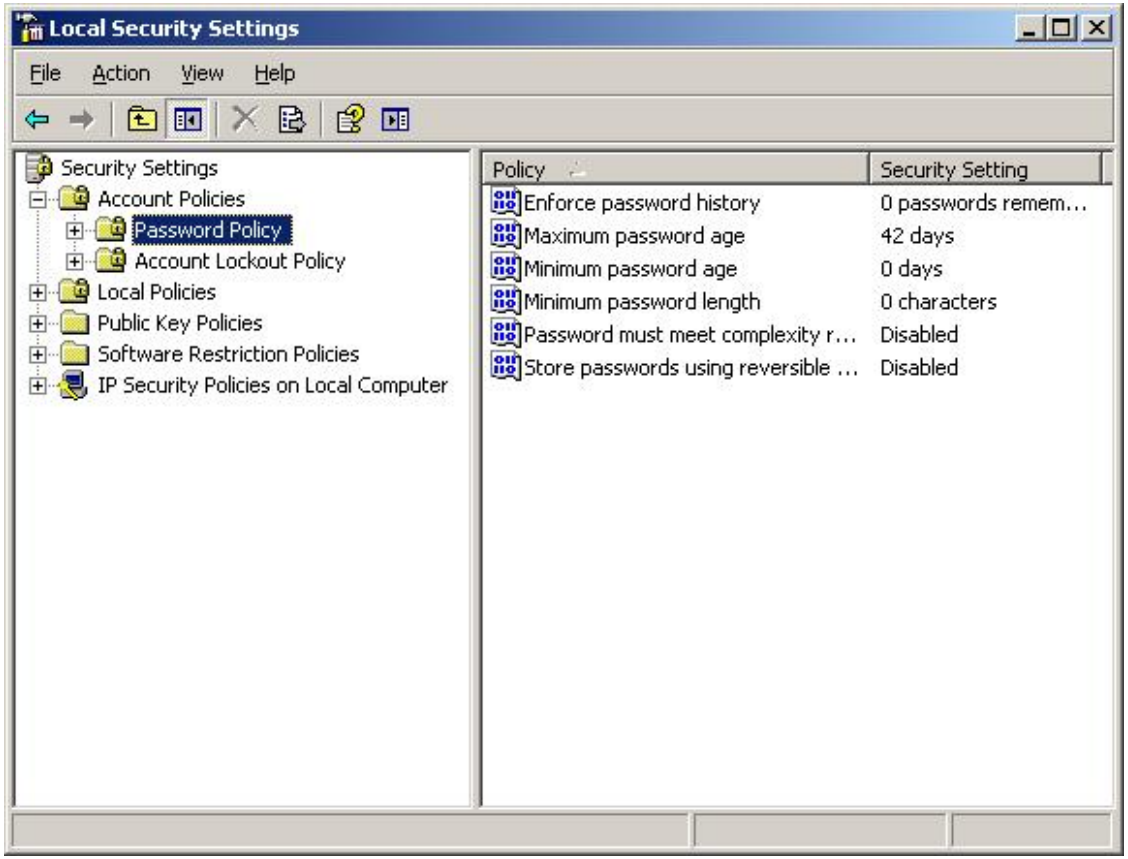
We need to double click on the Account Policies.



The Password Policy

There are six polices under the Password Policy heading.

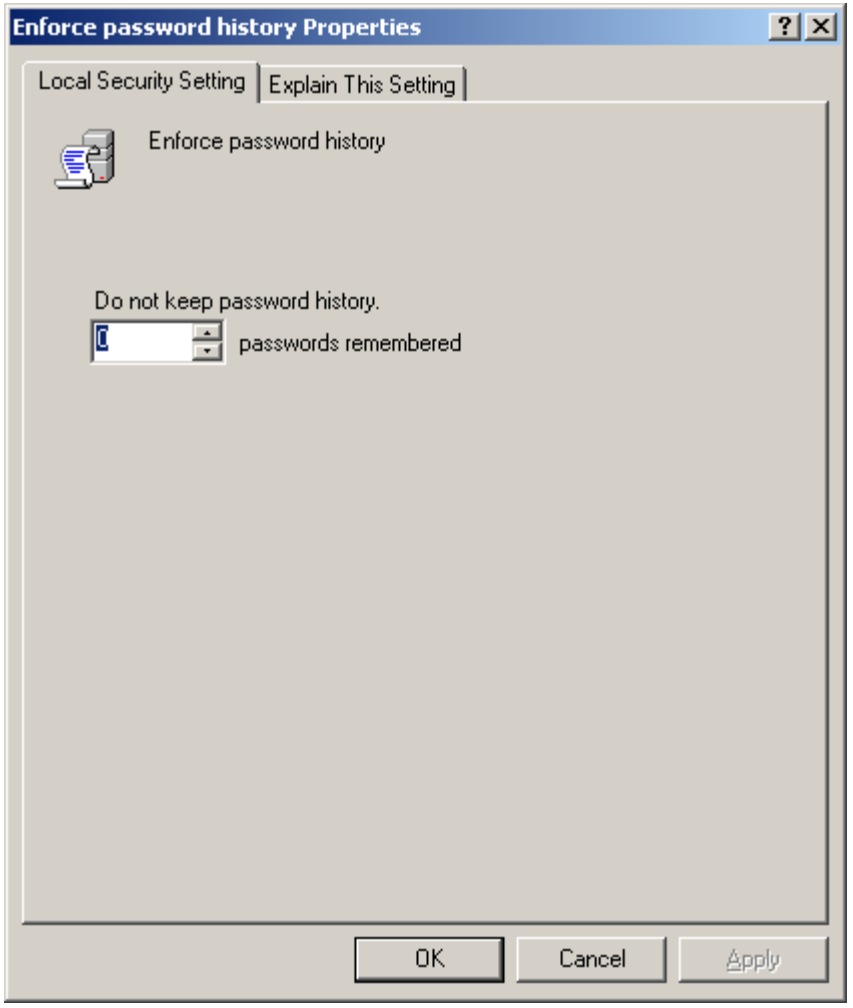
- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password must meet complexity requirement
- Store passwords using reversible encryption



Enforce Password History

Password history is a policy that keeps individuals from toggling with just a handful or two different passwords. Many people juggle between two or three passwords to fool the poorly setup server. For example, the first password can be R1PVanWinkle and the second secret phrase is St0ryB0ard21. If we do not enforce the password remembered variable, they can just toggle between the two every 30 days.

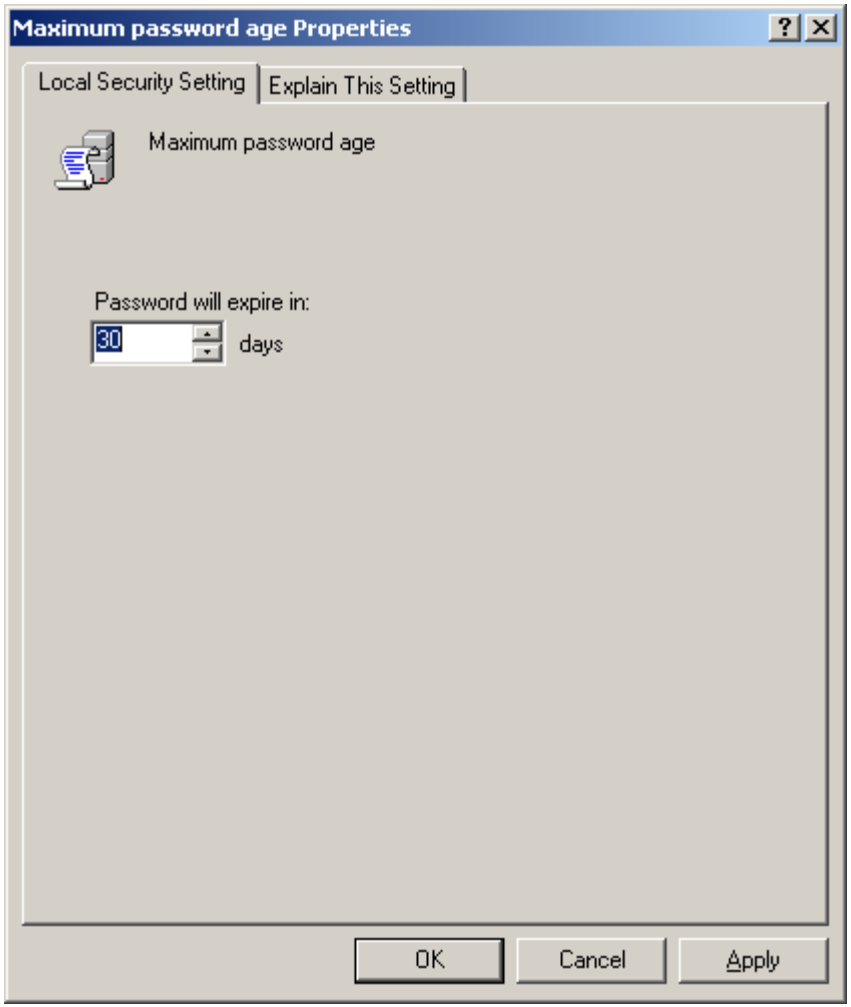
The default for password history is 0, however we will change the number to the maximum of 24.



Maximum Password Age

Maximum password age can range between 1 to 999 days. One day is extreme and nearly a thousand days, we might as well keep the password permanent. Many professionals believe that 15 to 30 days range is appropriate.

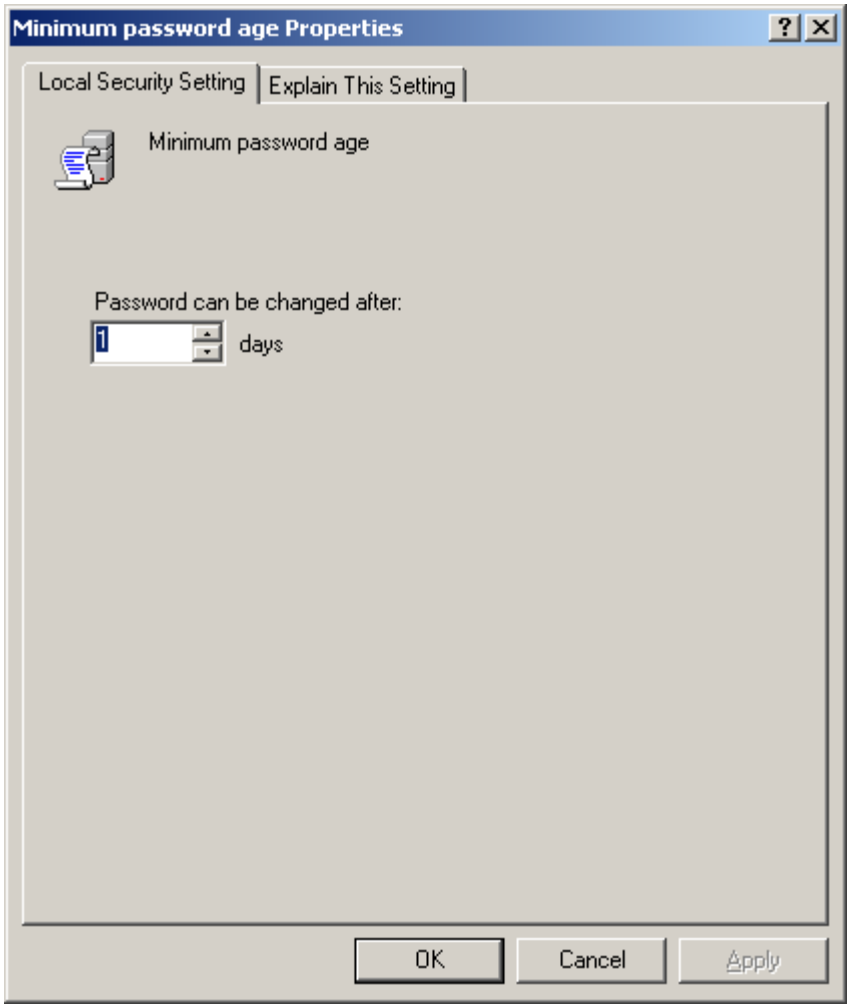
The system default is 42 days, however, we will require the staff to change their password every 30 days.



Minimum Password Age

Minimum password age can range between 1 to 998 days. By increasing the number of days, we can help enforce the time until the computer user return to their favorite password. If this is a problem in your department, we can increase the number of days to 29, one below the maximum days we set.

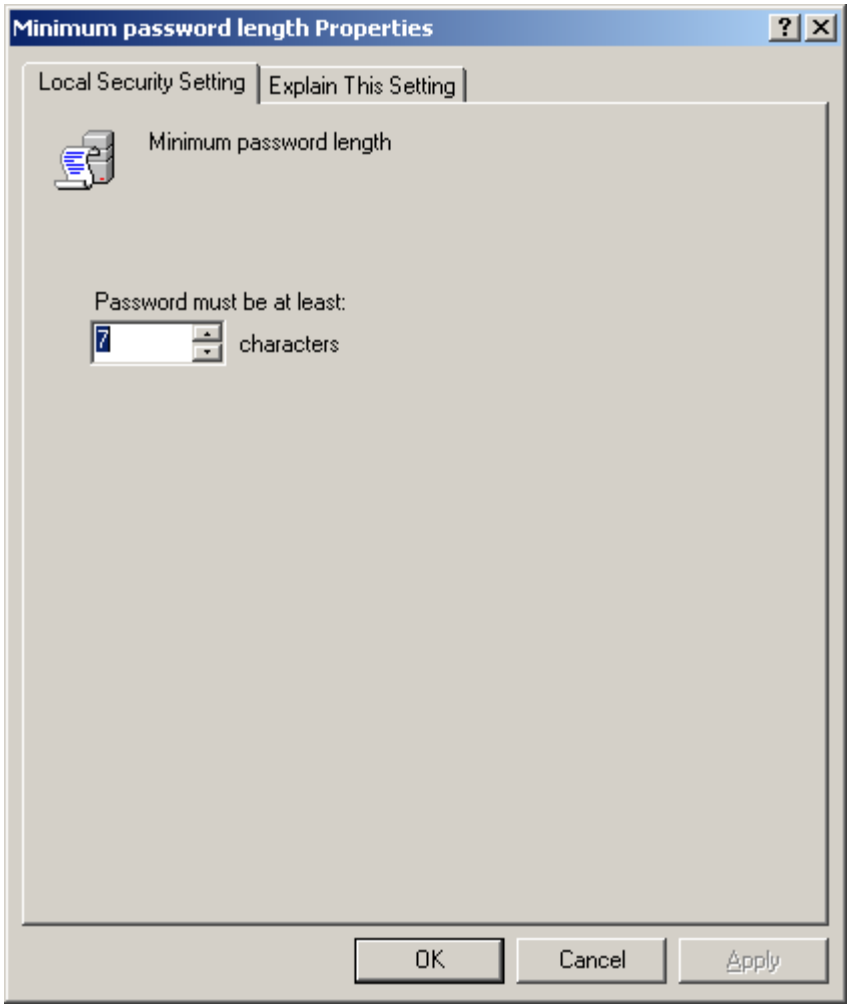
The system default is 1 day, and we will keep the personnel from changing their password for one day.



Minimum Password Length

Minimum password length is one of the two policies that help us create a smart password criteria. We need at least 6 characters and then we what those symbols to be upper case, lower case letters, numbers and special characters.

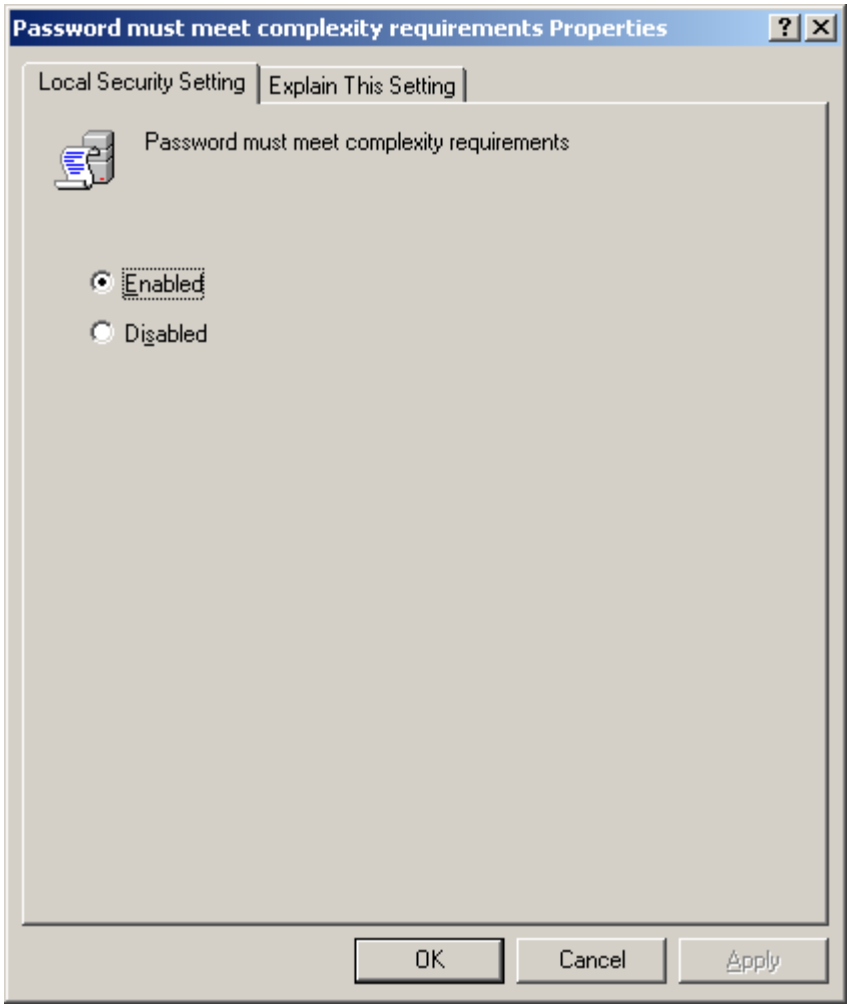
We will set the password to 7 characters.



Password Must Meet Complexity Requirement

Password must meet complexity requirement is the second of the two policies that help us create a smart password. We need to enable the regulation and then we will have to have three of the four criteria which are upper case, lower case letters, numbers and special characters in the password.

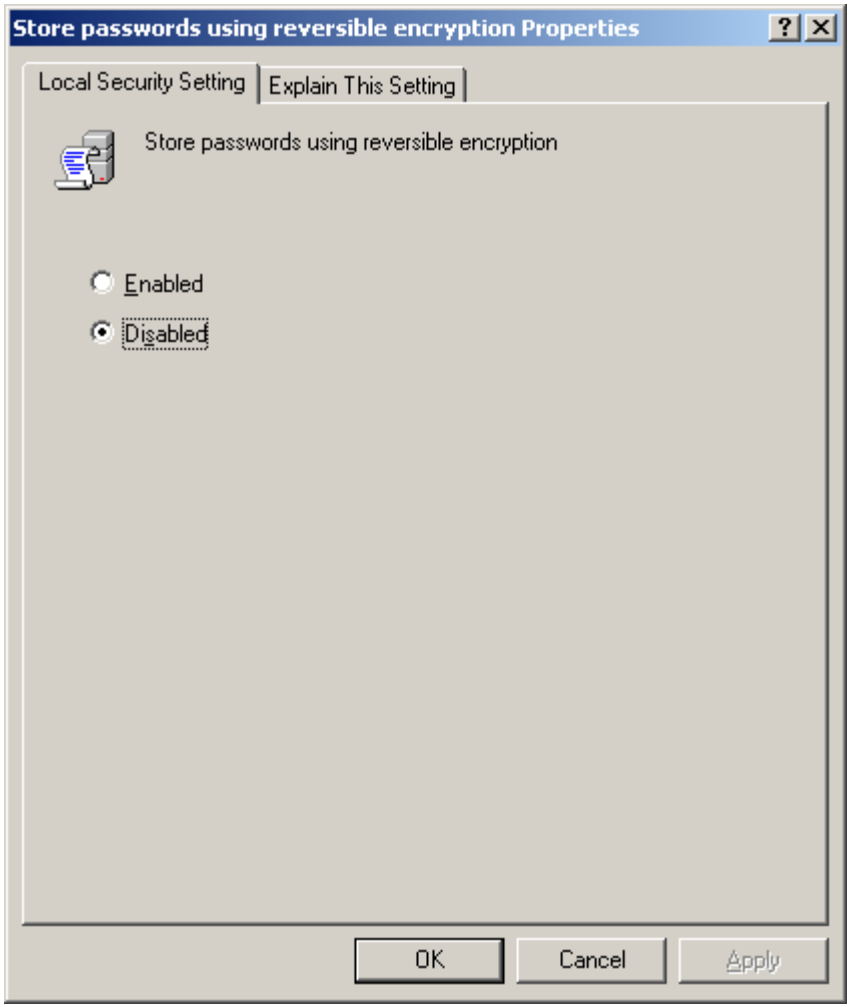
We will enable the rule.



Store Passwords Using Reversible Encryption

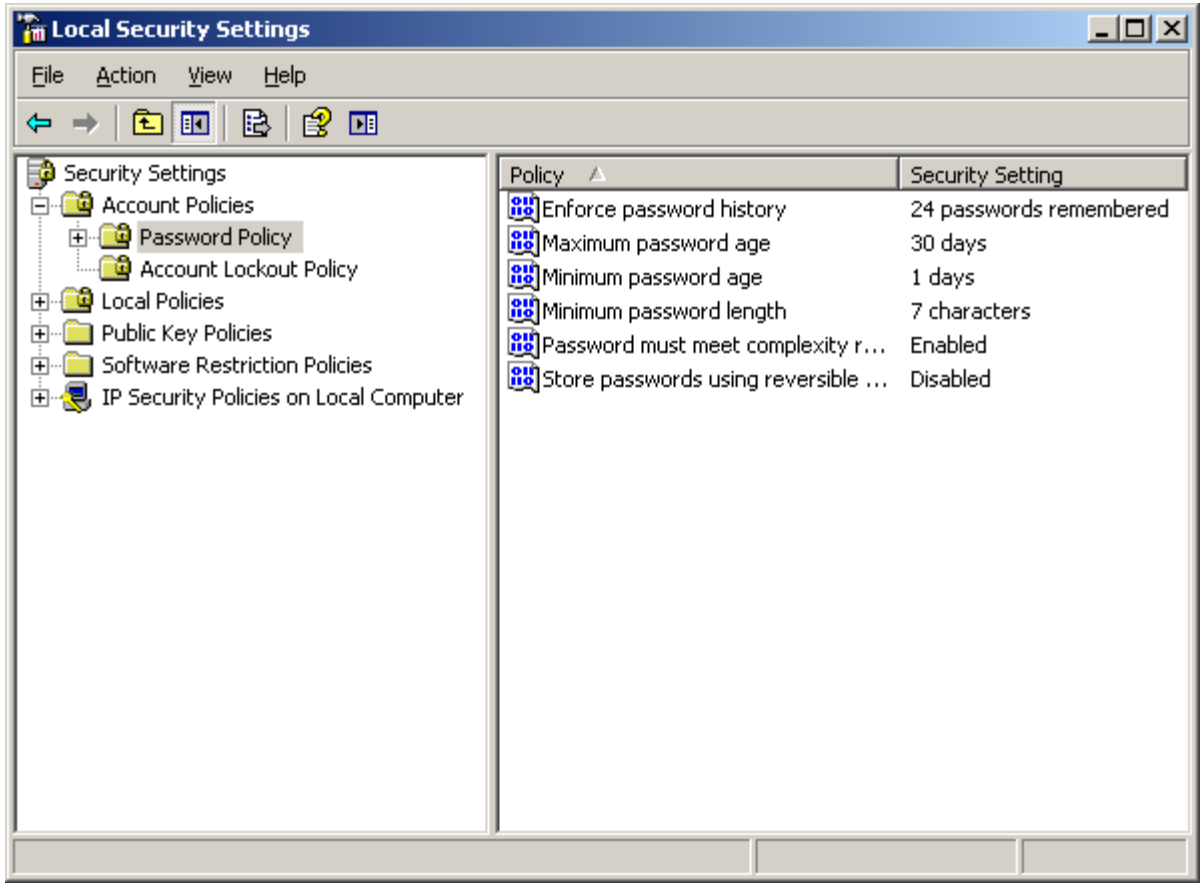
Only used in cases where applications need knowledge of user's passwords. We should leave the policy disabled unless required by a server application.

Default setting is disabled and we will keep it that way.



The Local Security Password Settings

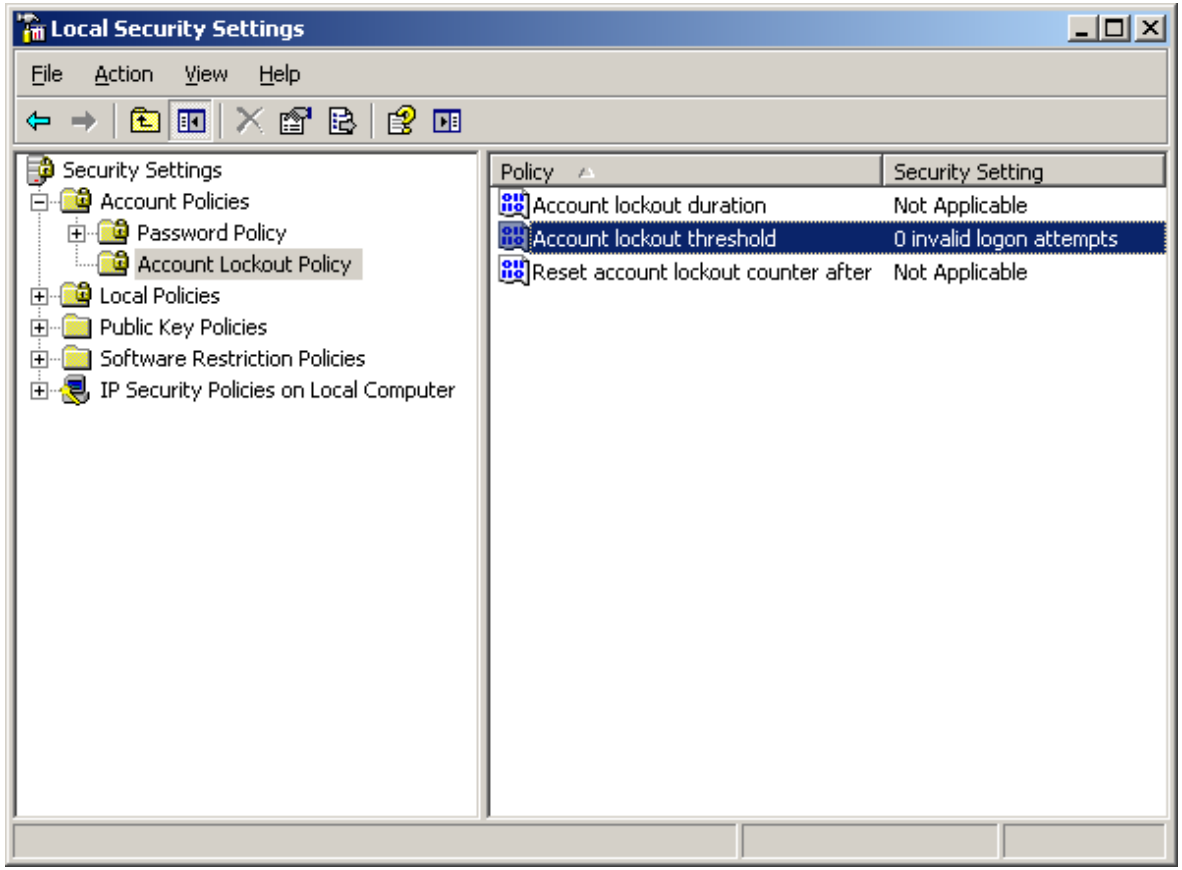
We can observe all of our password security changes in the right pane.



Account Lockout Policy

There are three polices under the Account Lockout Policy heading.

- Account lockout duration
- Account lockout threshold
- Reset account lockout counter after

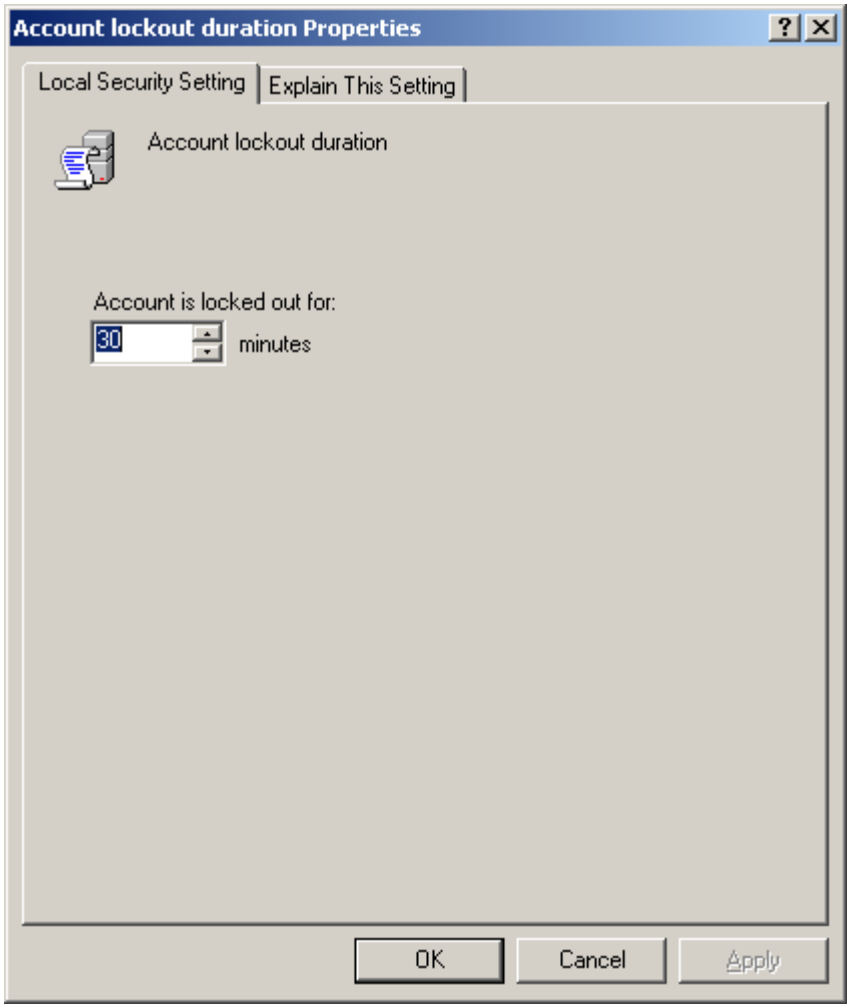


Account Lockout Duration

Account lockout occurs when a person tries to login to their or someone else's account and they have exceeded the maximum number of tries.

In this rule, we have set the lockout duration for 30 minutes before they can try to access their account again. For unattended servers, we can set the time to 2880 minutes which would be 48 hours for the weekend.

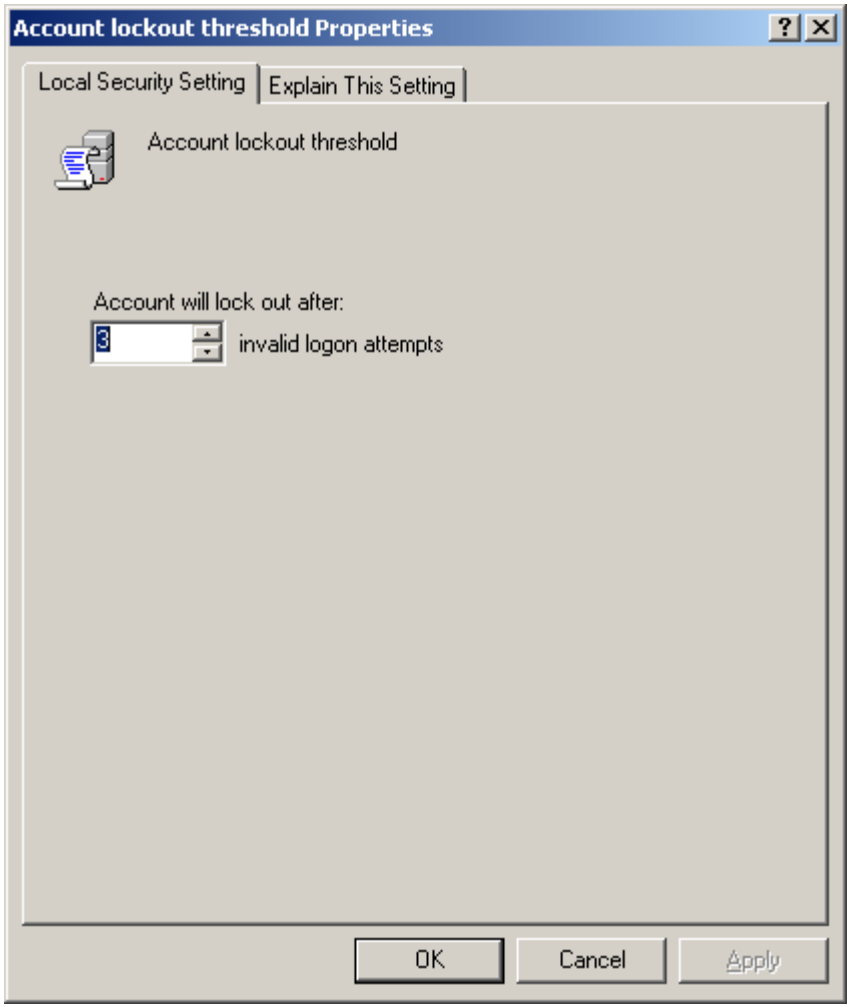
The default is unset. For our server, we set the time to 30 minutes.



Account Lockout Threshold

The lockout regulations continues with the maximum number of tries. In this rule, we have set the invalid logon attempts to 3 before they are locked out. This is the three strikes and you are out approach. We feel that if you do not know the password, you should contact a network administrator.

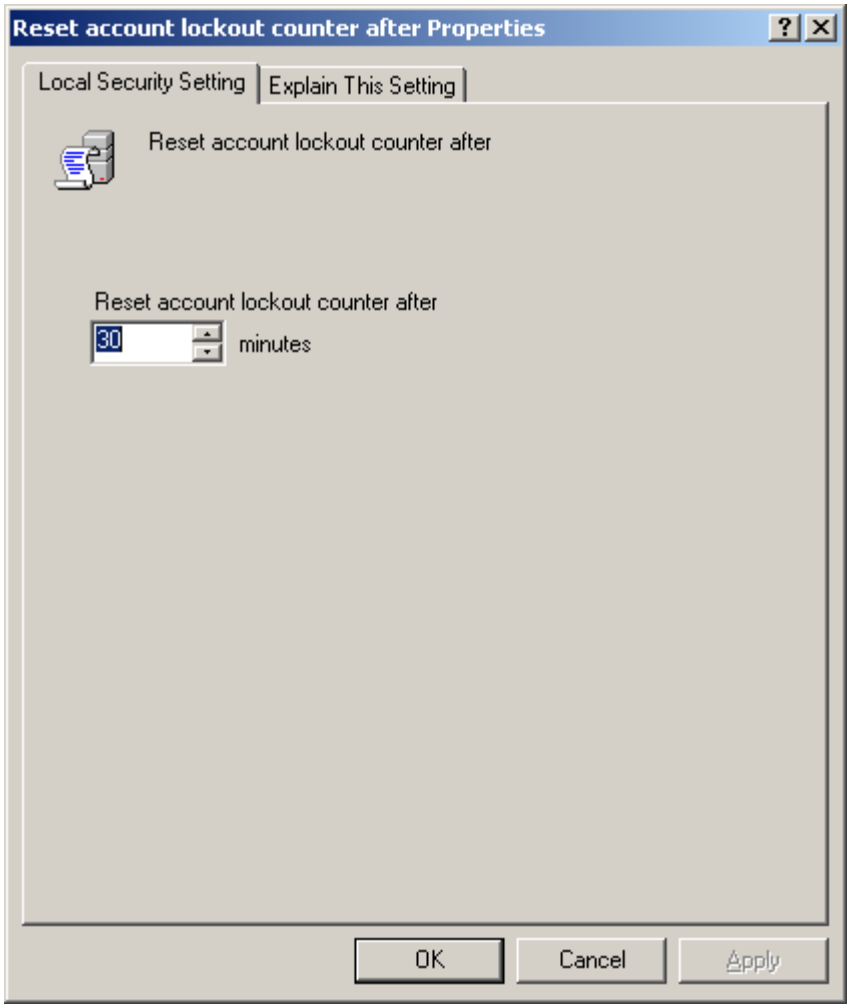
The default is unset.



Reset Account Lockout Counter After

When we mistype the password, the invalid logon attempt is recorded. Remember, we have only three tries. However, we let thirty minutes go by and the counter will reset the failed attempts back to zero.

The default is unset.



Account Lockout Policy Settings

We can observe all of our account lockout changes in the right pane.

In our next lesson, we will explore Local Polices.