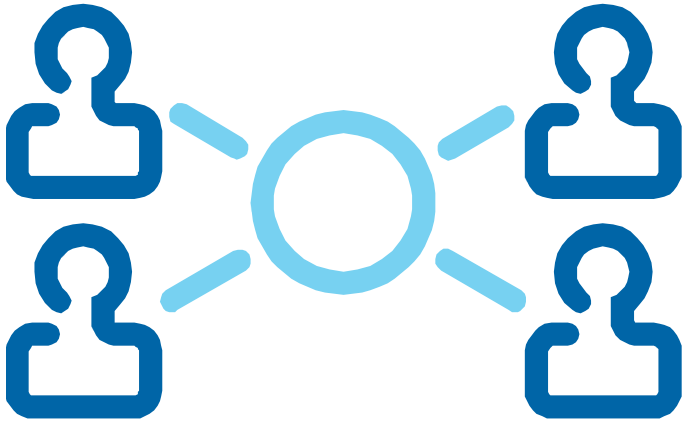
Setting the Domain Security Lockout Policies

July 13, 2011

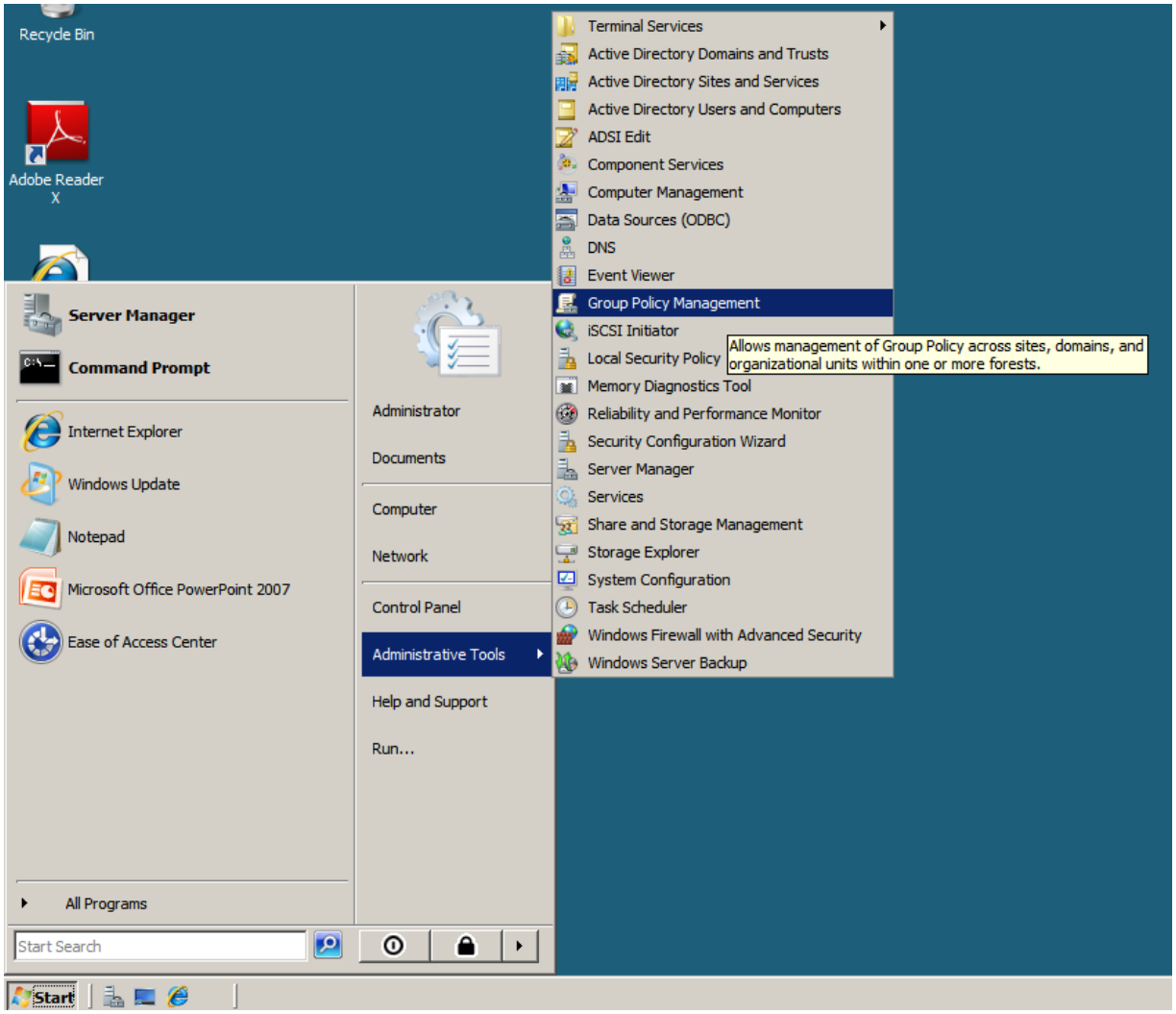
Security for Administrators

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.



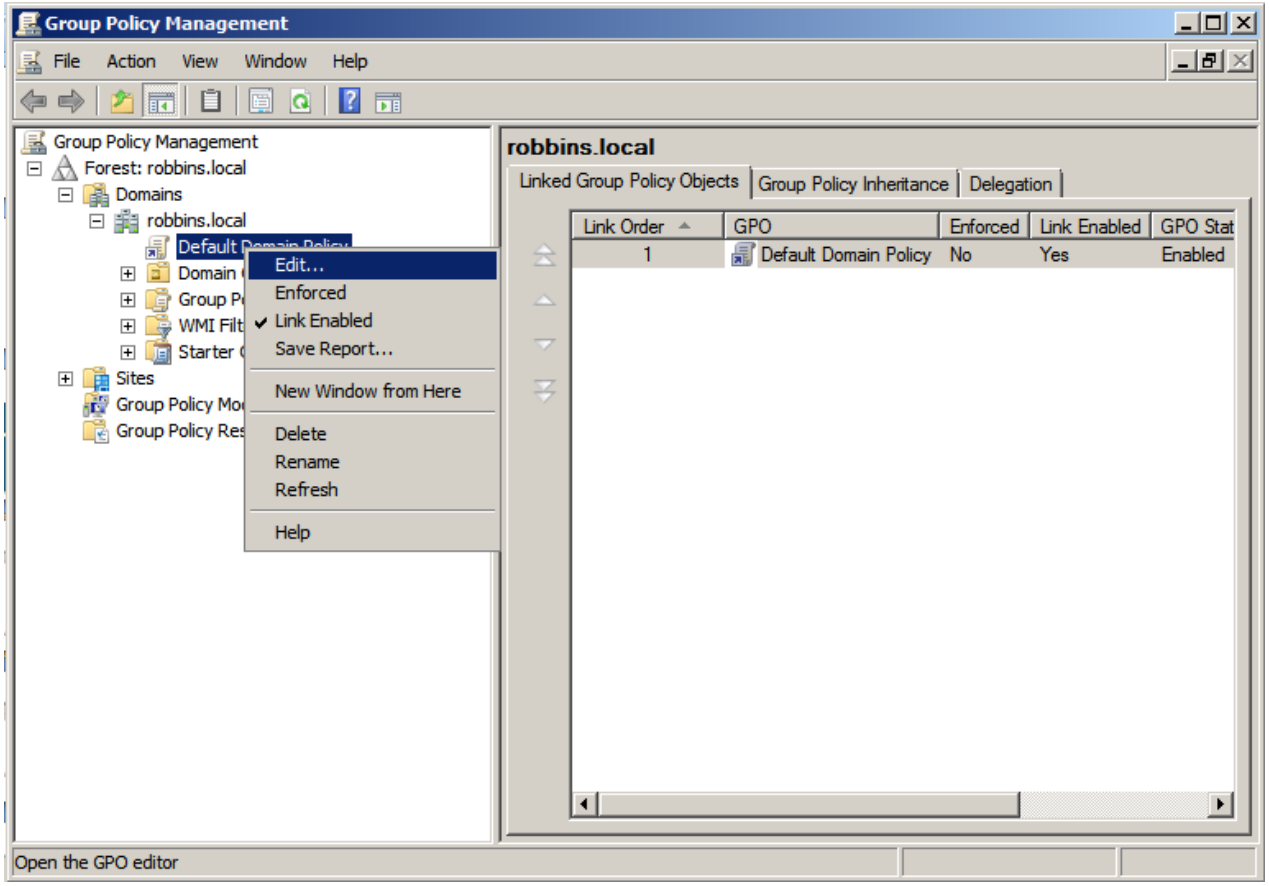
Setup Domain Policies

To set the domain polices for the Windows 2008 server, we select the Start button, Administrative Tools and then Group Policy Management.



Group Policy Management

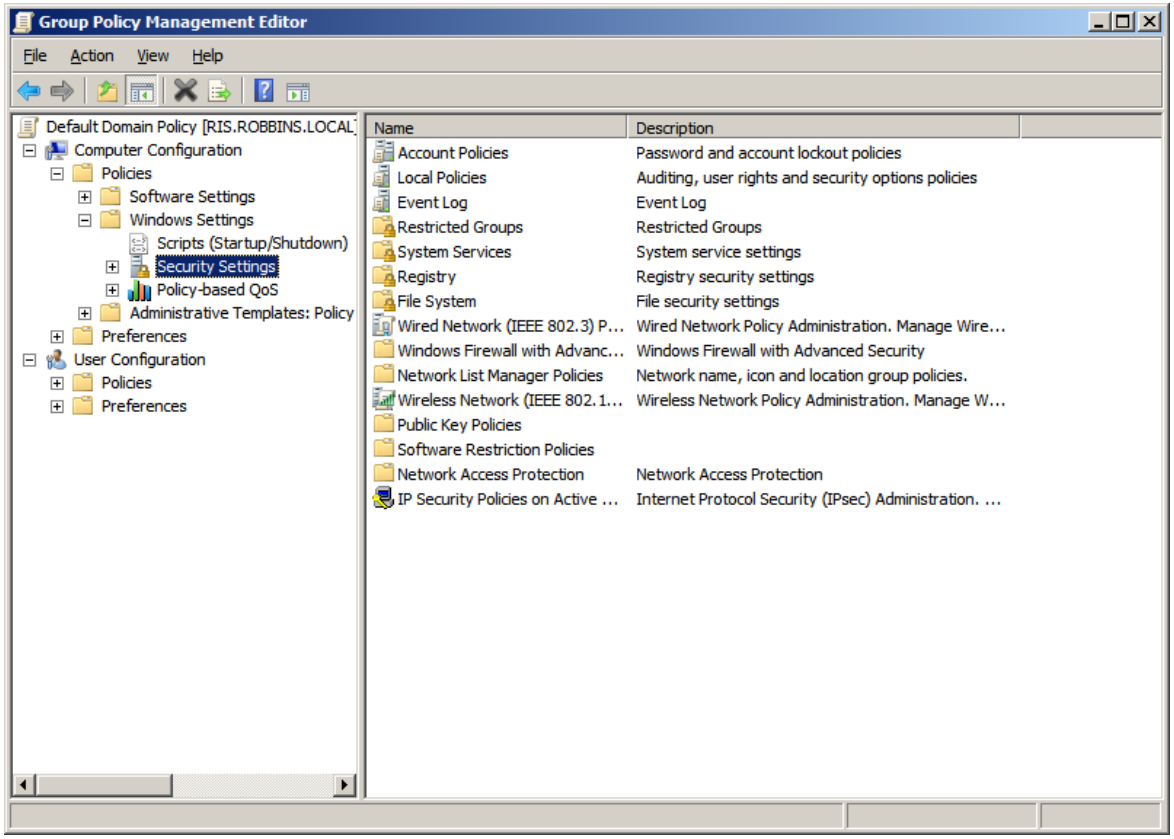
The Group Policy Management window will open and we expand the Forest: robbins.local, then Domains and the Default Domain Policy. We should right click on the Default Domain Policy and select Edit.



The Windows Security Settings

The Group Policy Management Editor window will open. We will expand Computer Configuration, Policies, Windows Settings, Security Settings and we can see the Account Policies at the top of the list in the right pane.

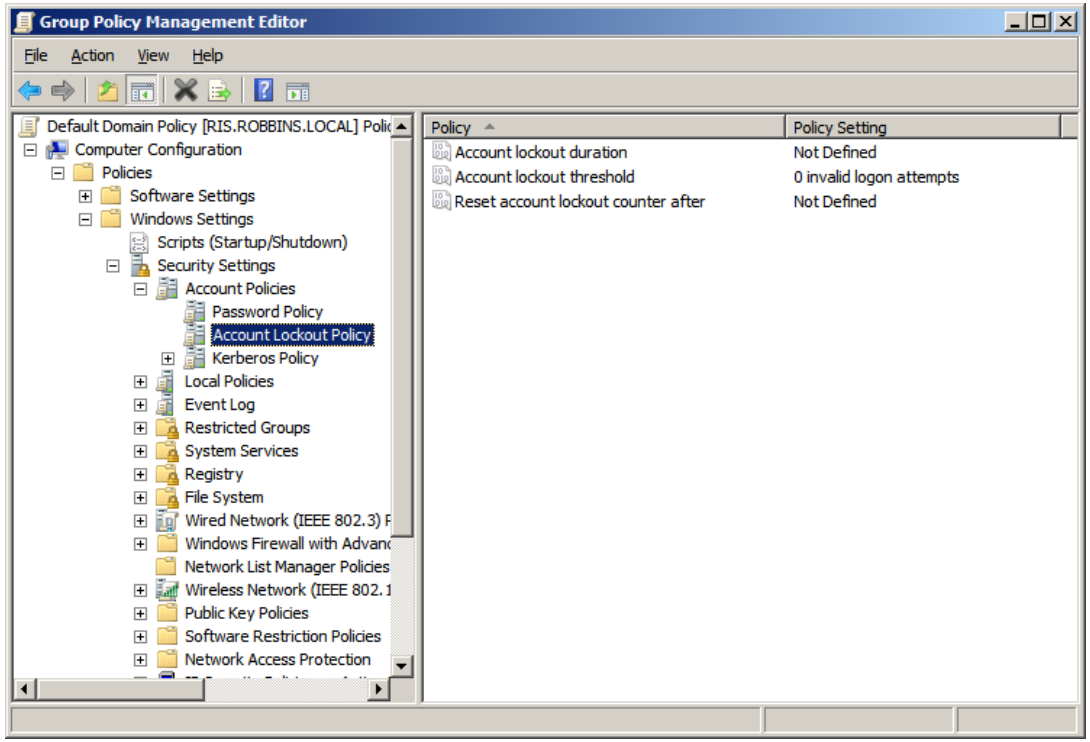
We need to double click on the Account Policies.



Account Lockout Policy

There are three polices under the Account Lockout Policy heading.

- Account Lockout Duration
- Account Lockout Threshold
- Reset Account Lockout Counter After

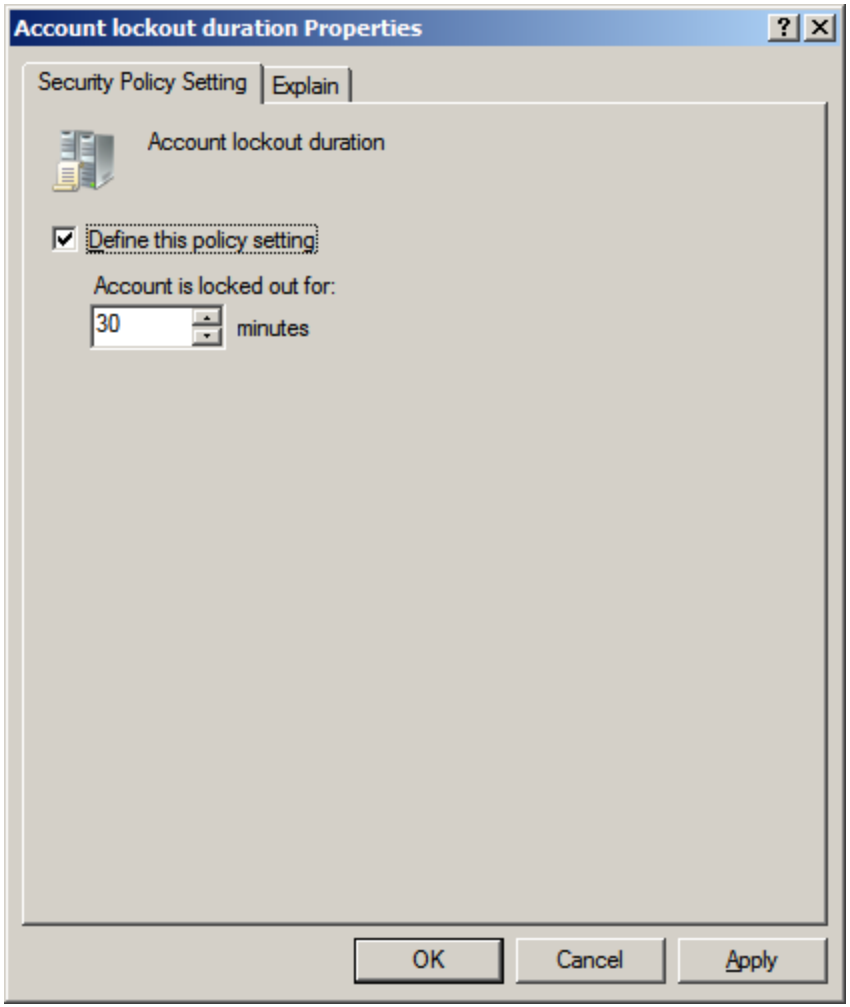


Account Lockout Duration

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.

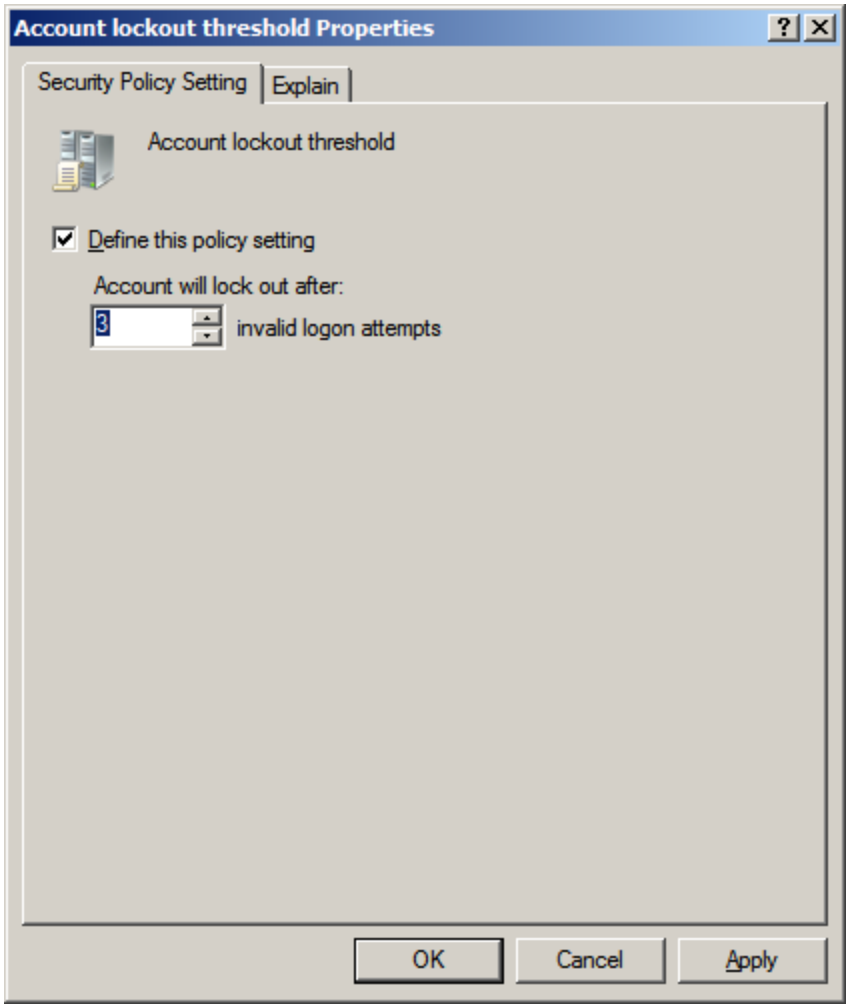
For our server, we set the time to 30 minutes.



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.

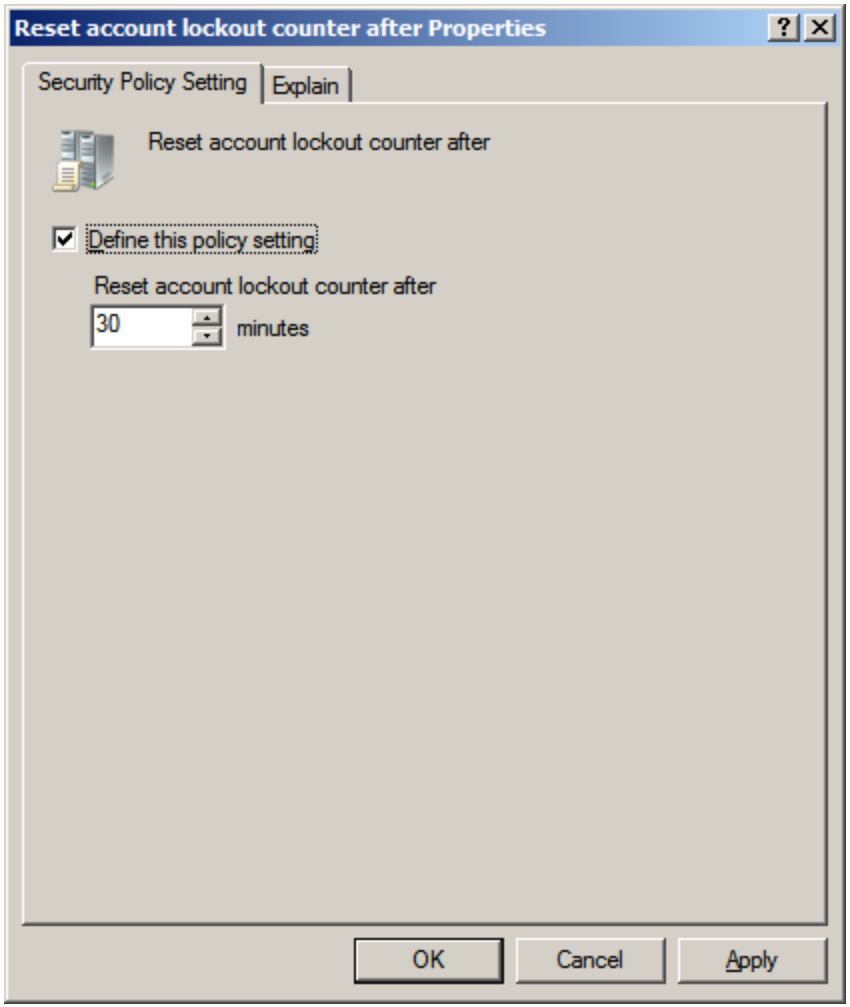
The default set by Microsoft when activated is 5 tries.



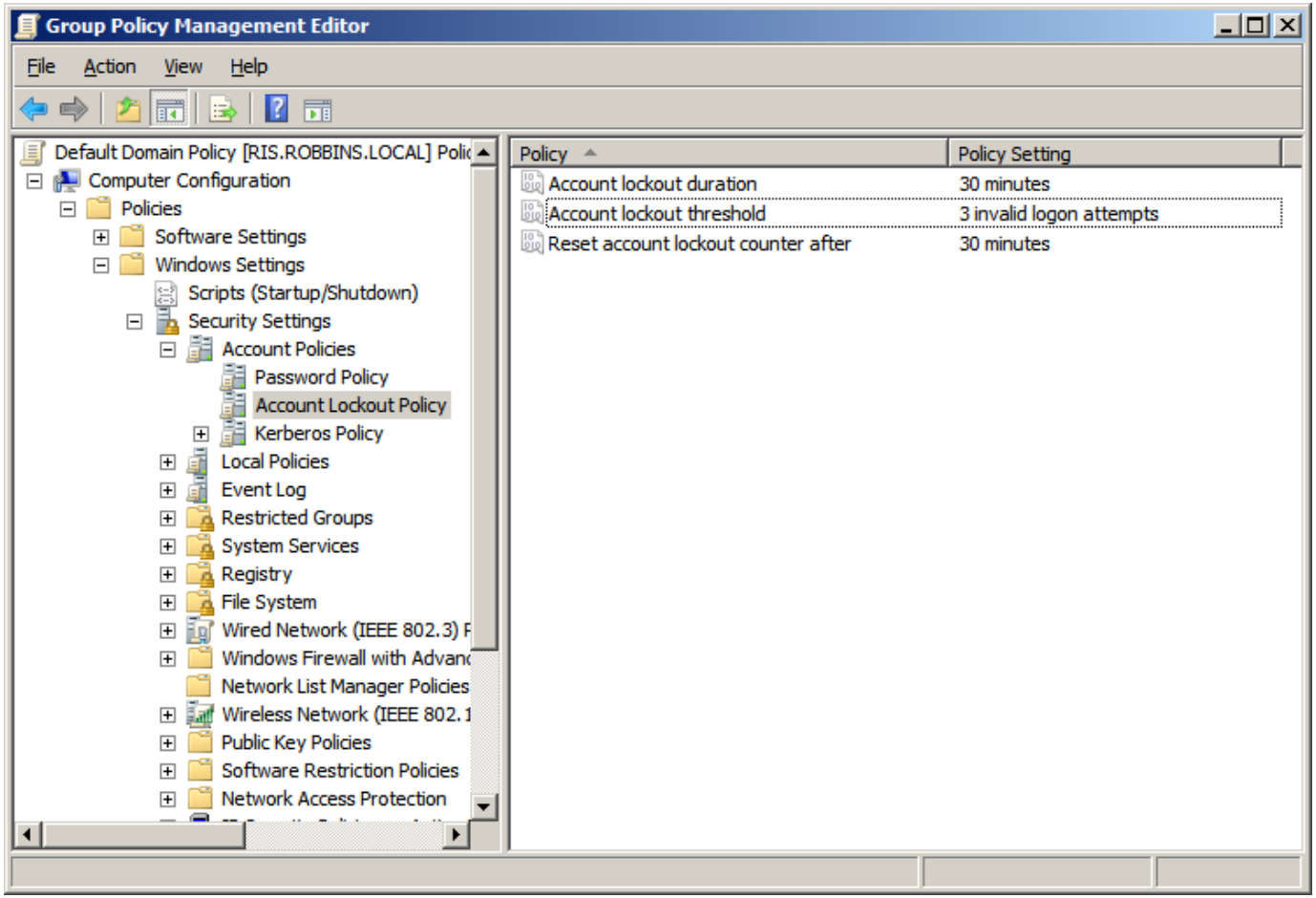
Reset Account Lockout Counter After

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 set by Microsoft is 30 minutes.



The Domain Security Account Lockout Settings



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