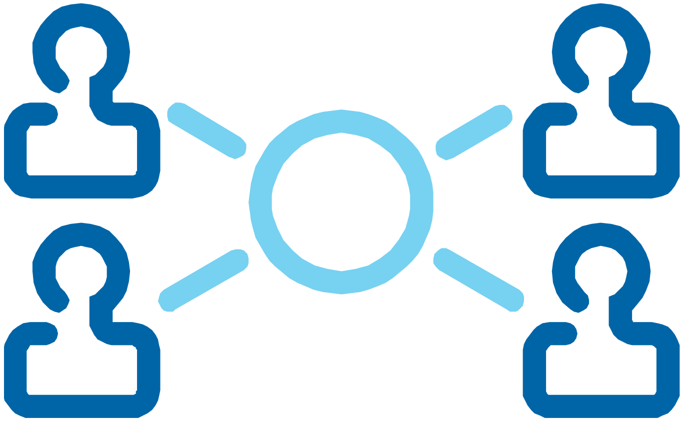
Setting the Lockout Policies on a Windows 2012 Standard Server

June 13, 2013

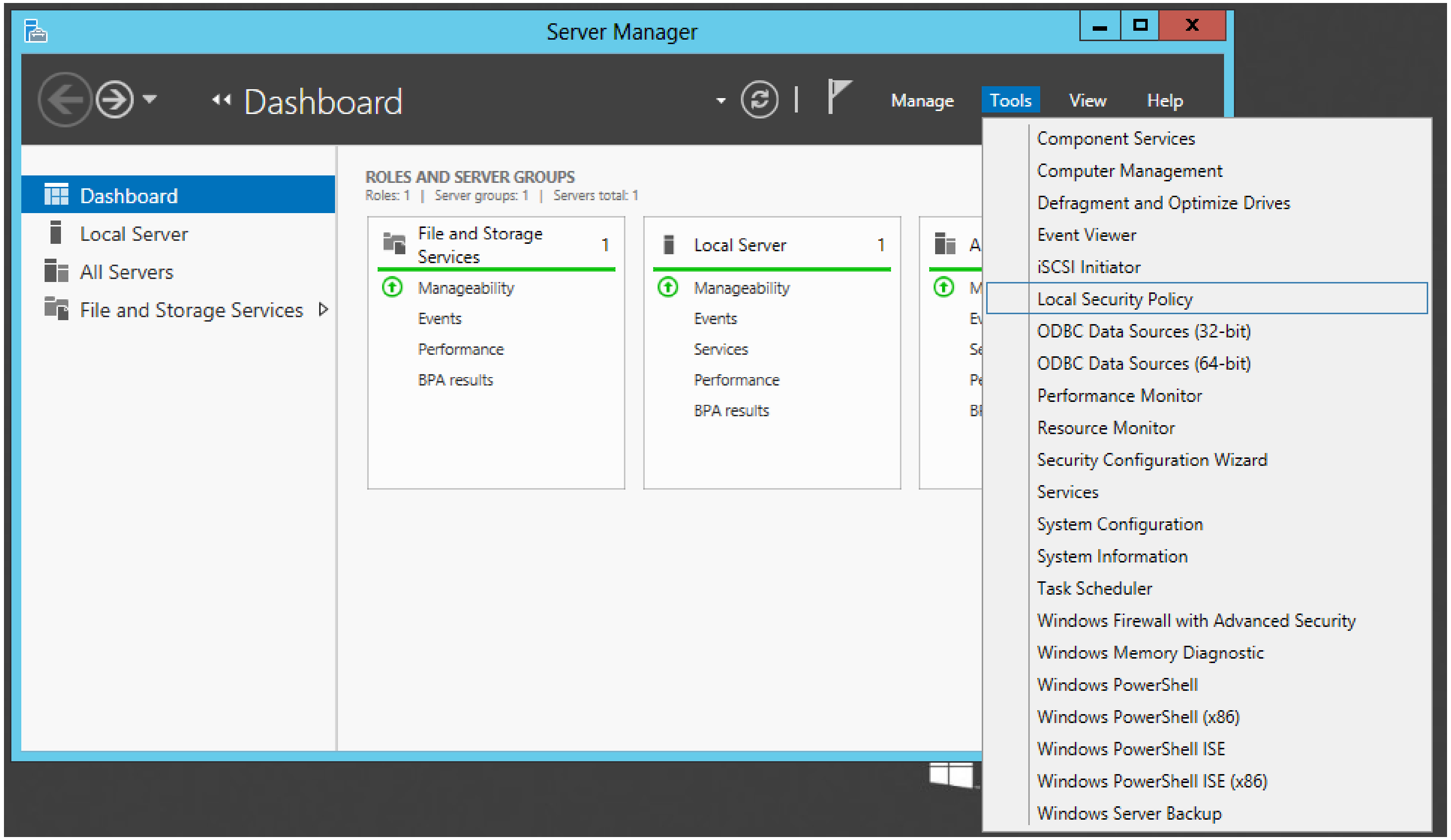
Security for Administrators

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.



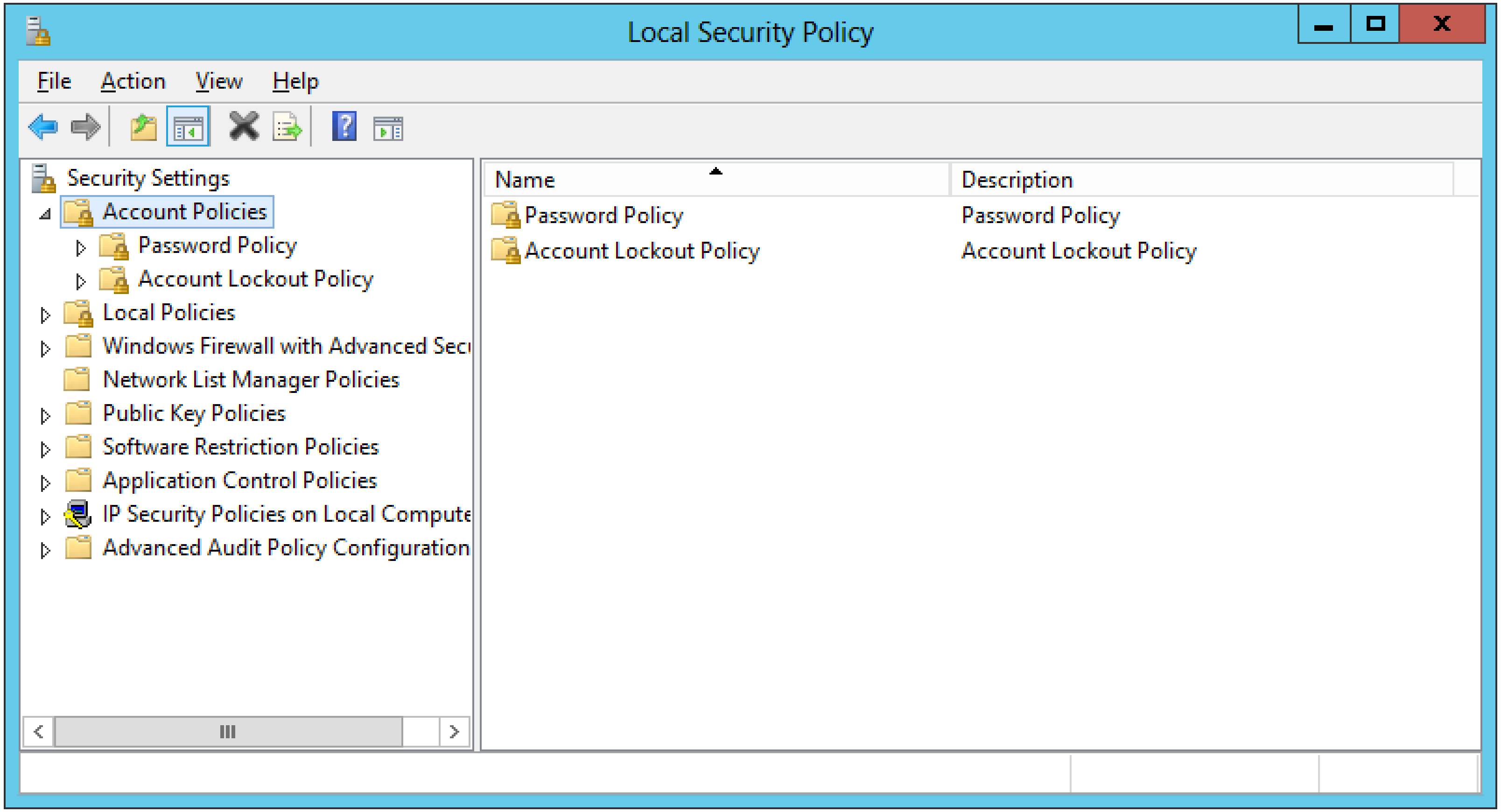
Setup Security Policies

To set the security polices for the Windows 2012 Standard Server, we select the Server Manager button and select Tools. From the list we choose Local Security Policies.



Local Security Policies

The Local Security Policies window will open. In the left pane, we select Account Policies and then Password Policies. A list of Password Policies will appear in the right pane.

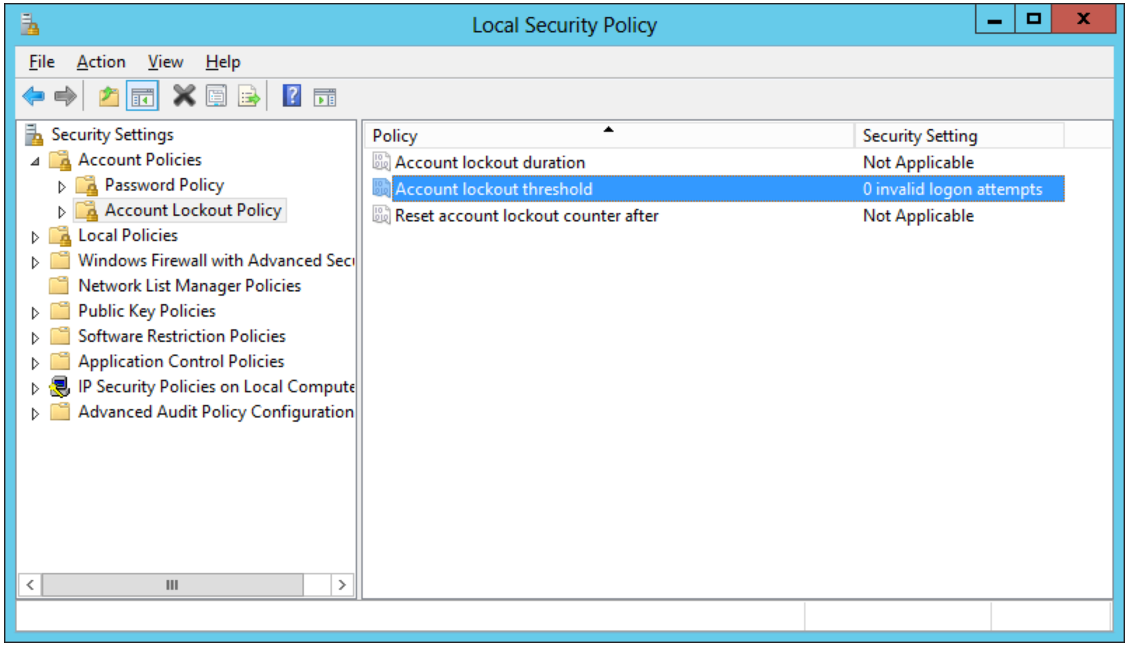

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Description
Password Policy	Password Policy
Account Lockout Policy	Account Lockout Policy

Account Lockout Policy

There are three polices under the Account Lockout Policy heading.

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

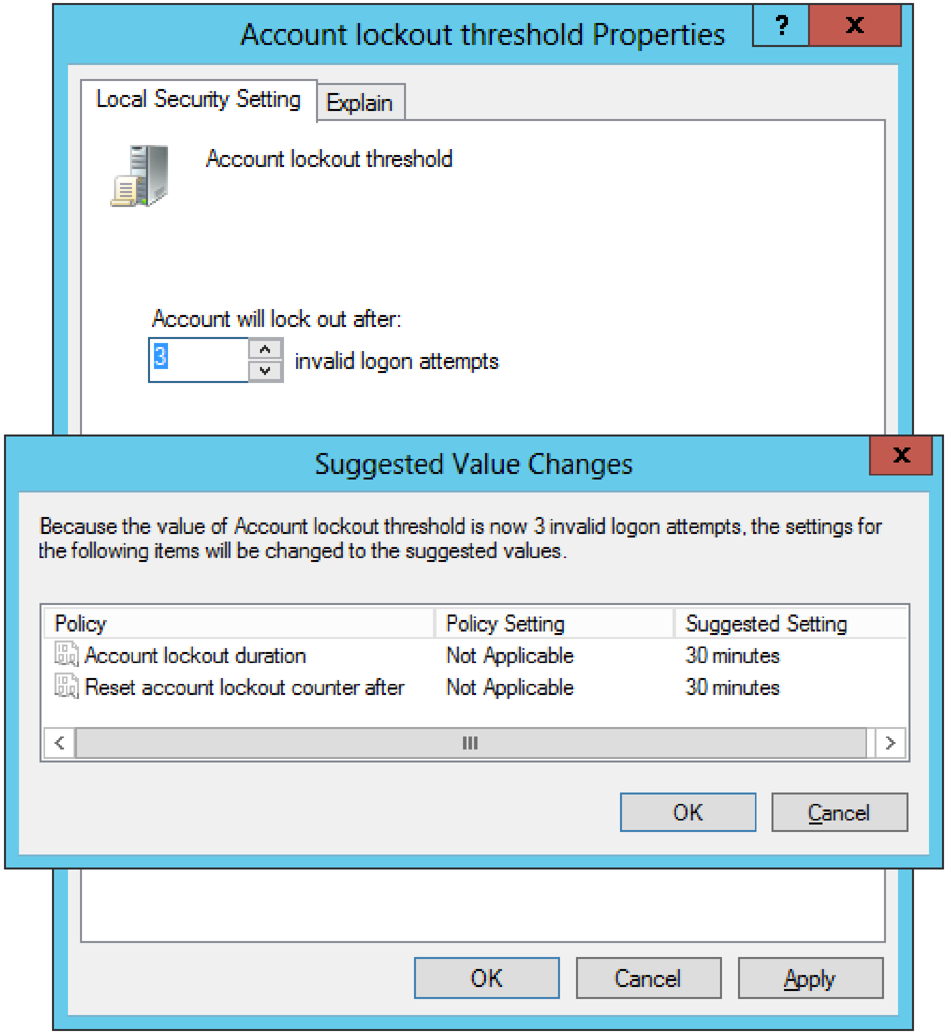

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

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 0 tries. When we apply the new setting, the other two policies will be set to 30 minutes for their duration.



Account lockout threshold Properties

Account lockout threshold

Account will lock out after:
3 invalid logon attempts

Suggested Value Changes

Because the value of Account lockout threshold is now 3 invalid logon attempts, the settings for the following items will be changed to the suggested values.

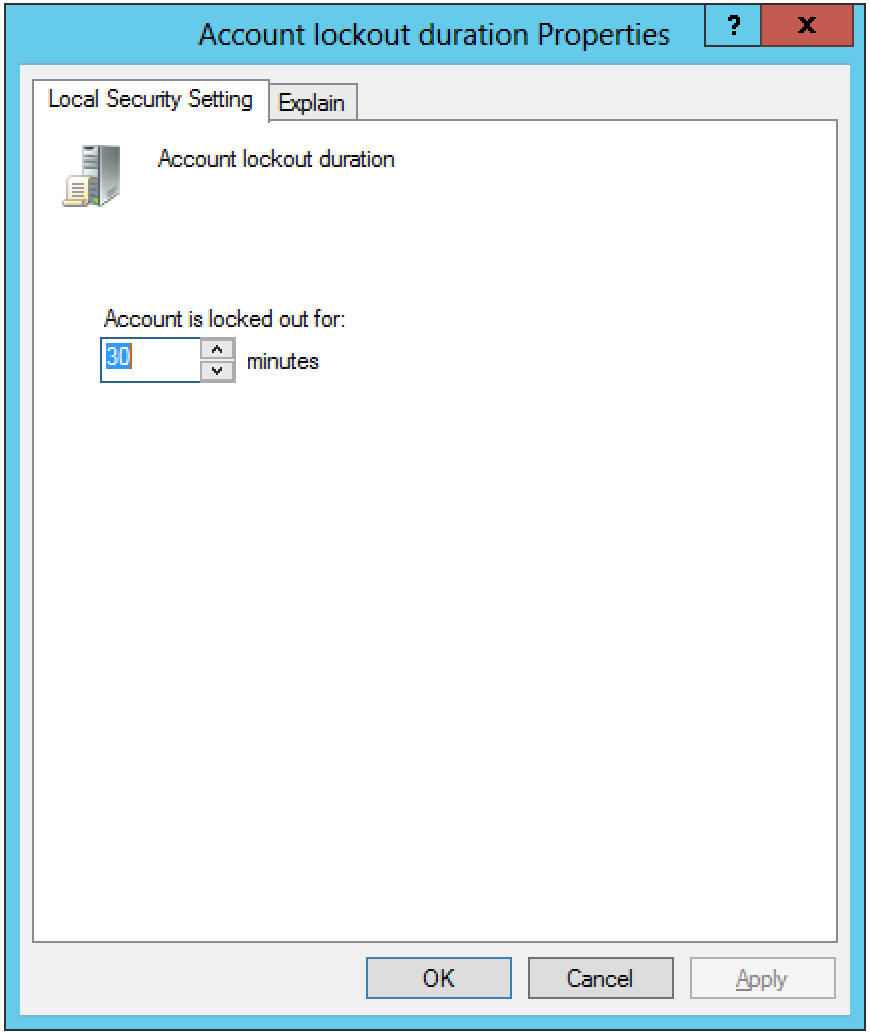
Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Applicable	30 minutes
Reset account lockout counter after	Not Applicable	30 minutes

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 duration Properties

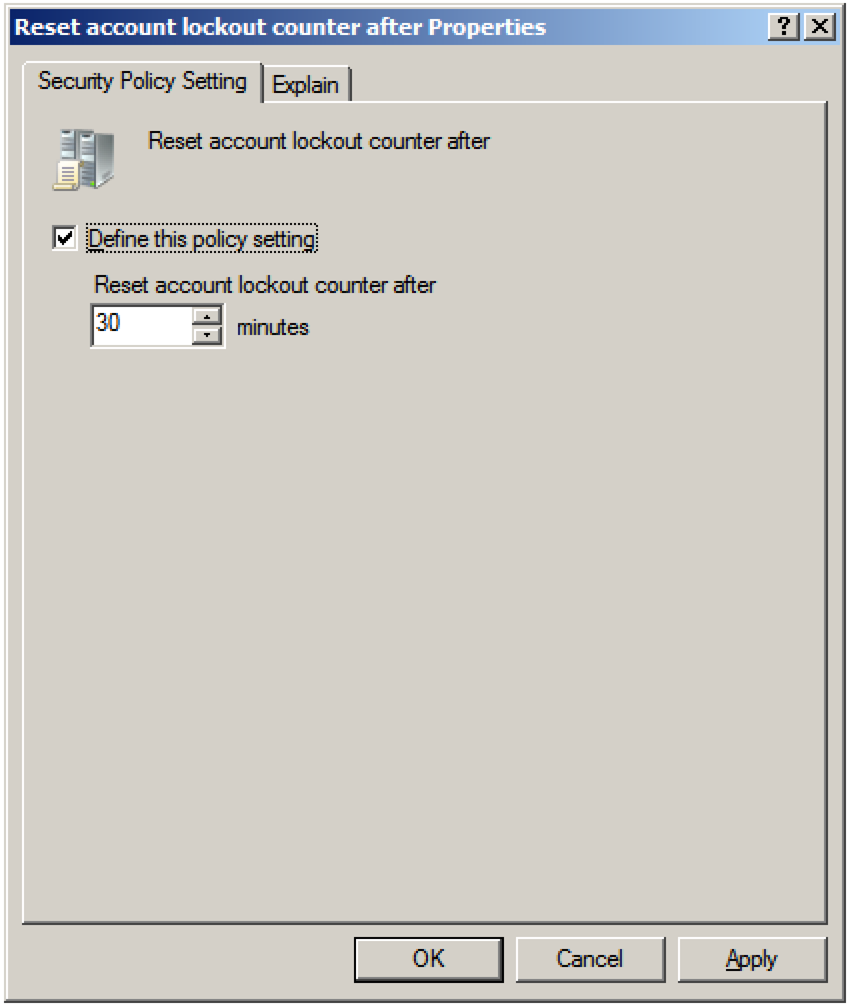
Account lockout duration

Account is locked out for:
30 minutes

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.



Reset account lockout counter after Properties

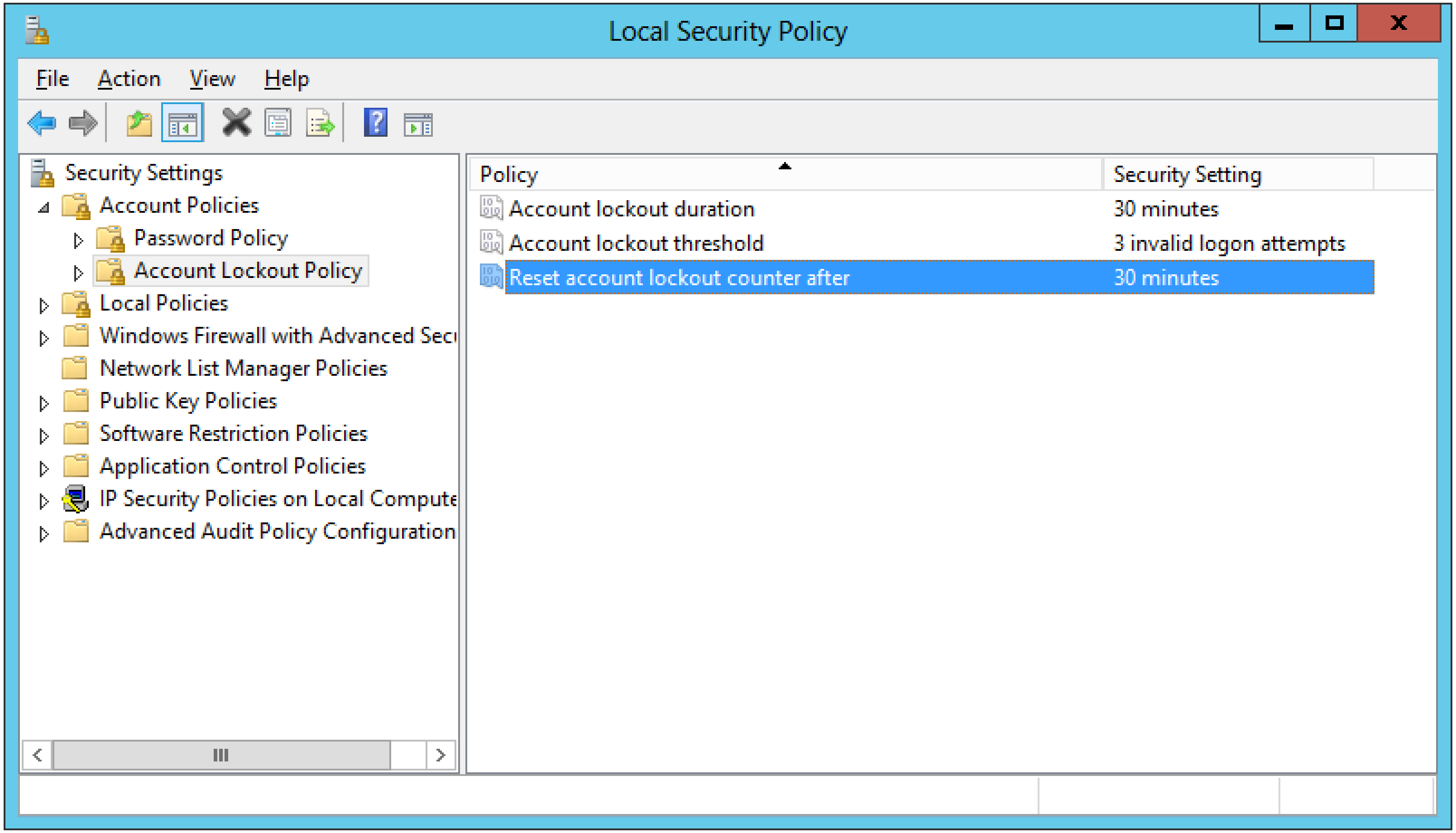
Reset account lockout counter after

☑ Define this policy setting

Reset account lockout counter after

30 minutes

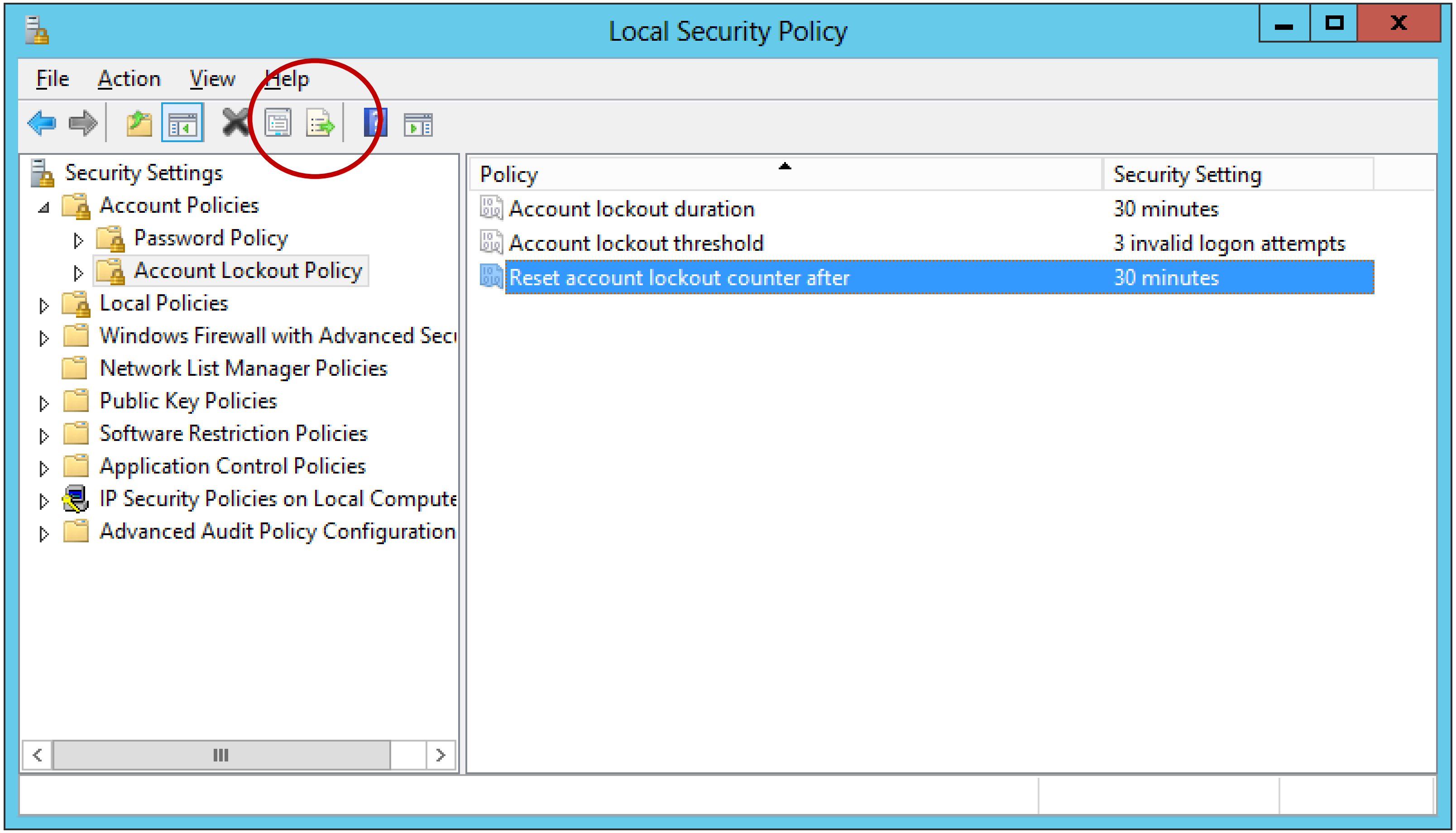
The Domain Security Account Lockout Settings


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

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

Export the Local Security Policy Account Lockout Settings

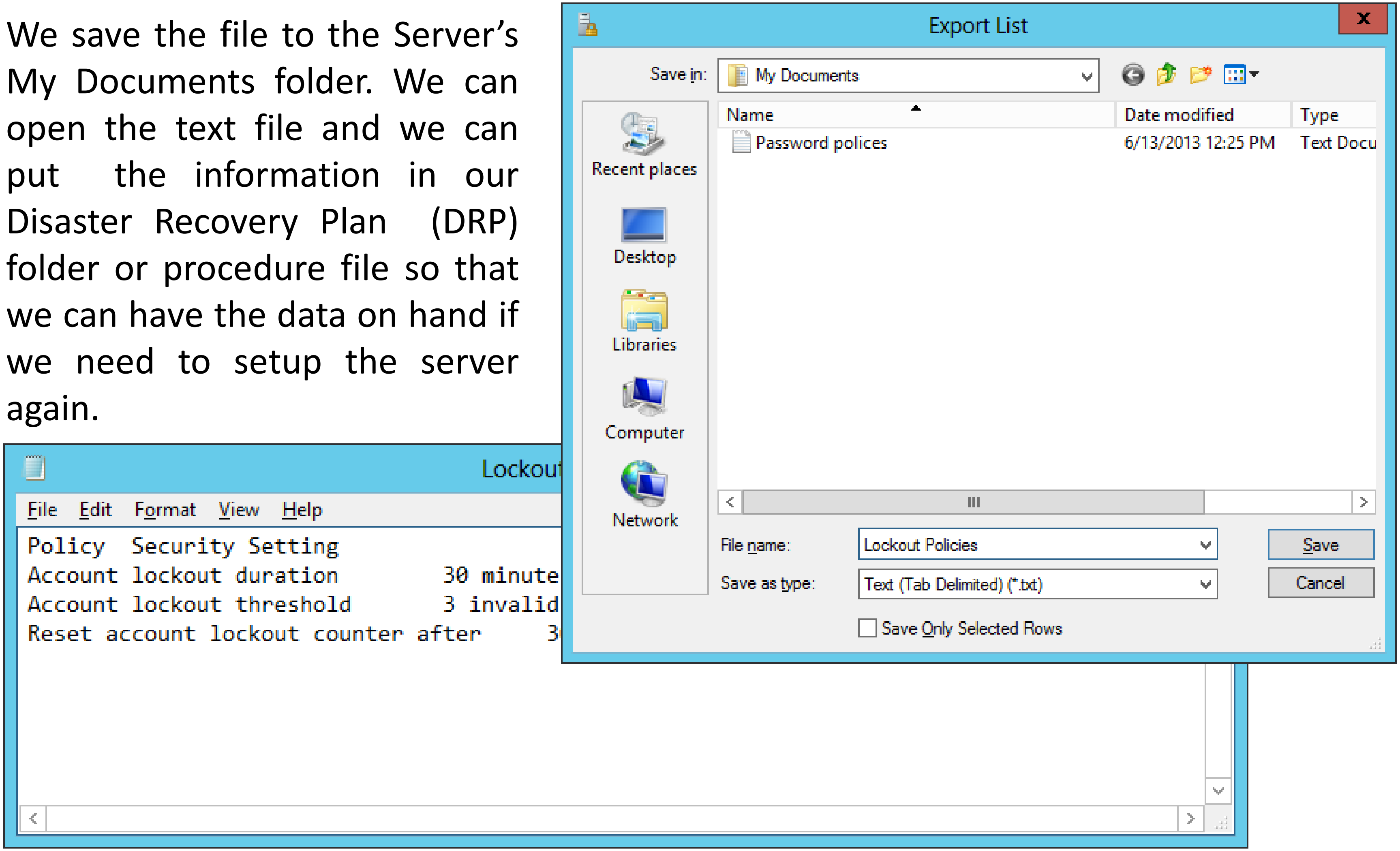

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

To export the settings to a text file, we push the Export icon at the top of the window.

Export List

We save the file to the Server’s My Documents folder. We can open the text file and we can put the information in our Disaster Recovery Plan (DRP) folder or procedure file so that we can have the data on hand if we need to setup the server again.



Name	Date modified	Type
Password polices	6/13/2013 12:25 PM	Text Docu

File name: Lockout Policies

Save as type: Text (Tab Delimited) (*.txt)

□ Save Only Selected Rows

```
Policy  Security Setting
Account lockout duration         30 minute
Account lockout threshold        3 invalid
Reset account lockout counter after      3
```