10 important Windows Group Policy settings need to be done immediately

Configure the 10 Group Policy below carefully and enjoy better Windows security for your computer.

One of the most common ways to configure a Microsoft Windows machine is to use Group Policy. These are settings related to registration on the computer, configuration of security and behavior settings when operating the machine. Group Policy can be opened from Active Directory (from the client) or configured right on the computer (local). Windows 8.1 and Windows Server 2012 R2 machines have more than 3,700 settings for the operating system.

Here are **10 important Group Policy settings** that you need to consider. Not only should you stop at these 10 settings because every reasonable setting will help reduce the risk. But these 10 options will decide almost all.

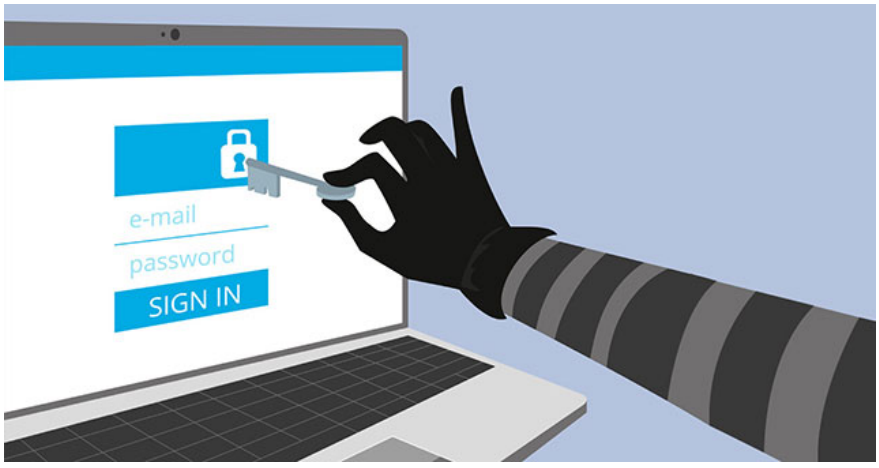
If set up correctly for these 10 names, you will create a safer Windows environment. All are in **Computer Configuration / Windows Setting / Security Settings.**

1. Change the Local Administrator account name

If bad guys don't know admin account names, they will take more time to hack. Rename the admin account that cannot be done automatically, but you must do it yourself.

2. Disable guest account

One of the worst things you do is turn on this account. It grants multiple access rights to Windows machines and does not need a password. Thankfully, there is an option to disable this feature by default,



Set up Group Policy properly to secure Windows machines

3. Disable LM and NTLM v1

LM **(LAN Manager)** and NTLM v1 authentication protocol are very vulnerable to attack. Please use **NTLM v2** and **Kerberos.** By default, almost all Windows machines accept all 4 protocols. Unless you have an old machine (more than 10 years) and haven't patched it, it's rare to use the old protocol. May disable them by default.

4. Disable storing LM

LM password hashing is easy to convert to plain text. Don't let Windows save them on the drive, where hackers can use the tool to find out. It is disabled by default.

5. Minimum password length

Password length for normal users should be at least 12 characters - 15 characters or more with higher level accounts. Windows passwords are not very safe if there are less than 12 characters. To be the most secure in the Windows authentication world, it should be 15. So it almost closes every back door.

Unfortunately, setting up the old Group Policy only has a maximum of 14 characters. Use **Fine-Grained Password Policies,** although it's not easy to set up and configure on Windows Server 2008 R2 (and older), but with Windows Server 2012, it's easy.

6. Maximum life of the password

Passwords with 14 characters or less are not used for longer than 90 days. The default Windows maximum password duration is 42 days, so you can use this number or increase it to 90 days if you want. Some security experts say that using a password for up to a year is fine if it has 15 or more characters. However, remember that the longer the time limit, the higher the risk of someone stealing and using it to access another person's account. Better short-term use is still better.

7. Event Logs

Many victims of the attack have been able to detect them early if they turn on Event Logs and have a habit of checking them. Make sure you use the recommended settings in the **Microsoft Security Compliance Manager** tool and use **Audit Subcategories.**

8. Disable anonymous SID attendance

Security Identifiers are the numbers assigned to each user, group, and security object on Windows or **Active Directory.** In the first versions of Windows, unproven users can query these numbers to identify important users (such as administrators) and groups, hackers would love to exploit this. This rollout can be disabled by default.

9. Don't leave anonymous accounts in the group of people

This setting along with previous settings when configured incorrectly will allow an anonymous user to access the system further than allowed. Both settings can be turned on by default (disable anonymous access) since 2000.

10. Turn on user account control (User Account Control - UAC)

Since Windows Vista, UAC is the number 1 protection tool when browsing the web. Yet many people turn off because of old information about software compatibility issues. Most of these problems are gone, the rest can be solved with Microsoft's free incompatible detection utility. If you disable UAC, you will be in more danger on Windows NT than newer OSs. UAC is enabled by default.

New OS versions are set by default quite a lot

If you notice, you will see that 7 of 10 of these settings are correctly configured on Windows Vista, Windows Server 2008 and later. No need to waste time figuring out all 3,700 Group Policy settings, please configure it correctly.