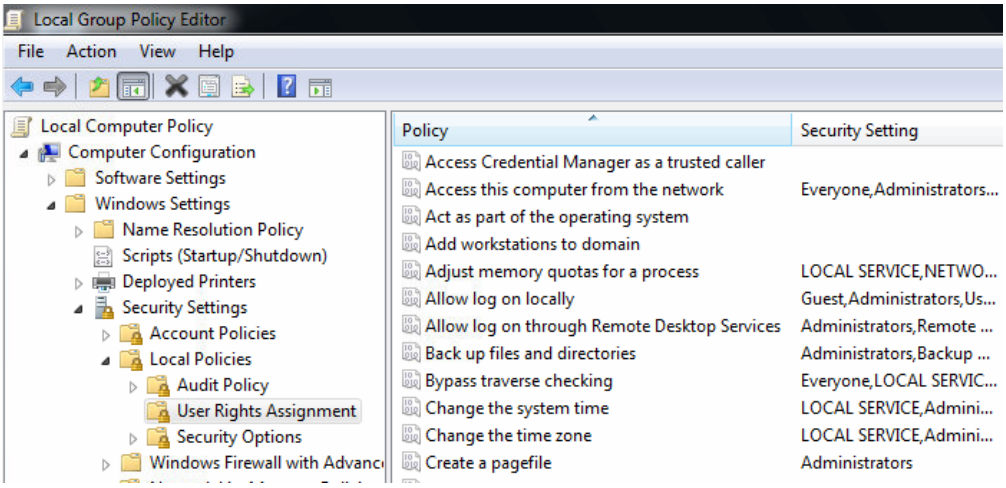
USER ACCOUNT POLICIES IN WINDOWS 7

Local Group Policy Editor

We can manage user rights and accounts policies using local policy editor. To open Local Group Policy Editor in Windows 7, we can enter "gpedit.msc" in search and click on the *gpedit* option in search results. In Policy Editor we can then go to Computer Configuration > Windows Settings > Security Settings . Here, the first thing we will check is User Rights Assignment under Local Policies.

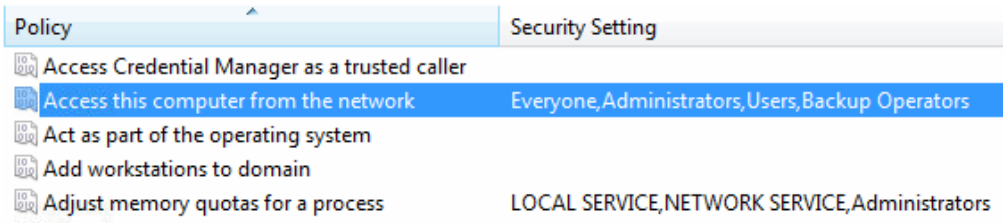


Policy Editor

User Rights Assignment

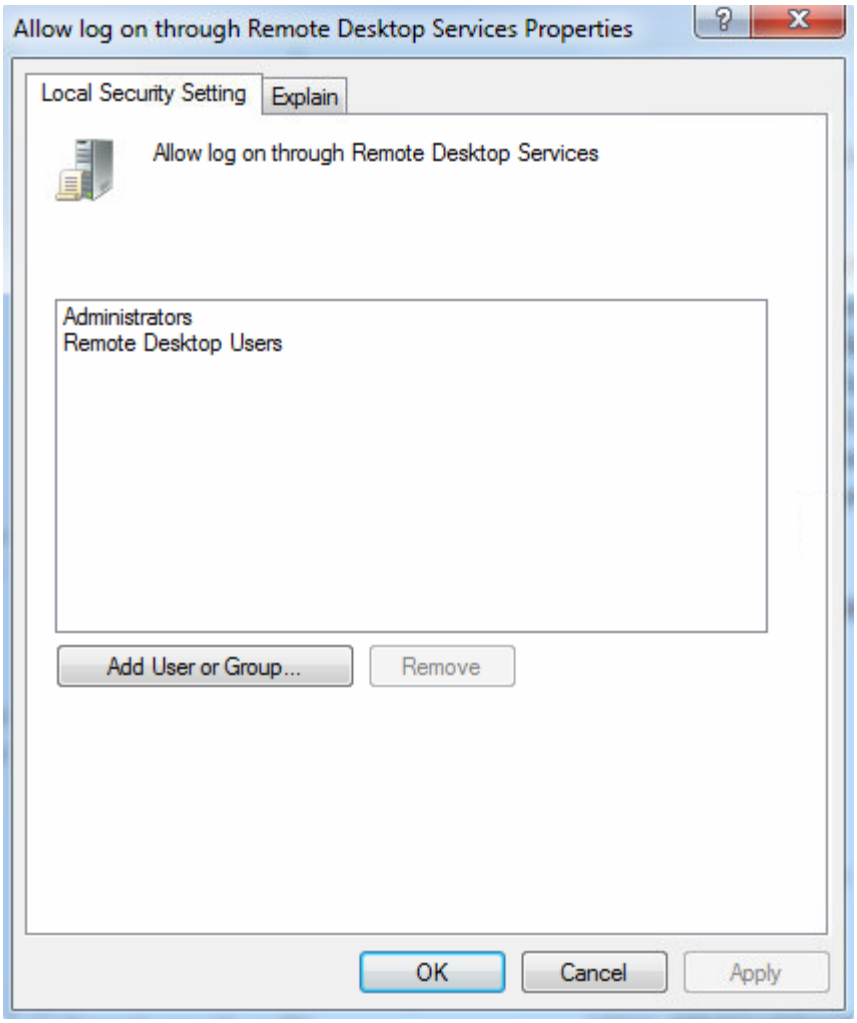
In this section we will first see a predefined policies that are set on our machine. For example, we can see who (which groups of users) can access this computer

from the network, who can log on locally, who can log on trough Remote Desktop, who can back up files, etc. For example, in our case we see that users in groups "Everyone", "Administrators", "Users", and "Backup Operators" can access our computer from the network.



Network Access Policy

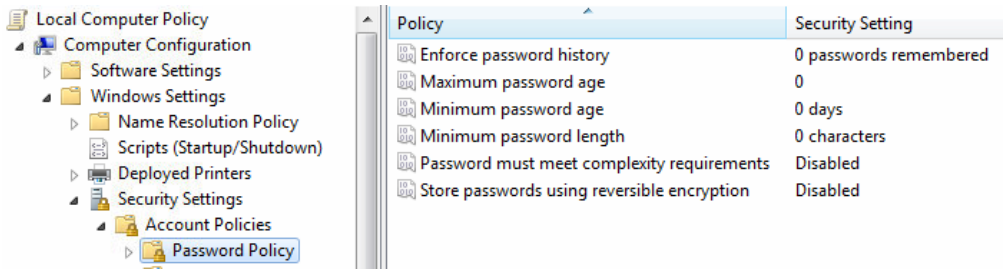
Of course, we can change those settings to suit our needs. For example, if we select "Allow log on trough Remote Desktop Services" policy, we we add specific user or group of users to the list, or remove them.



Remote Desktop Users

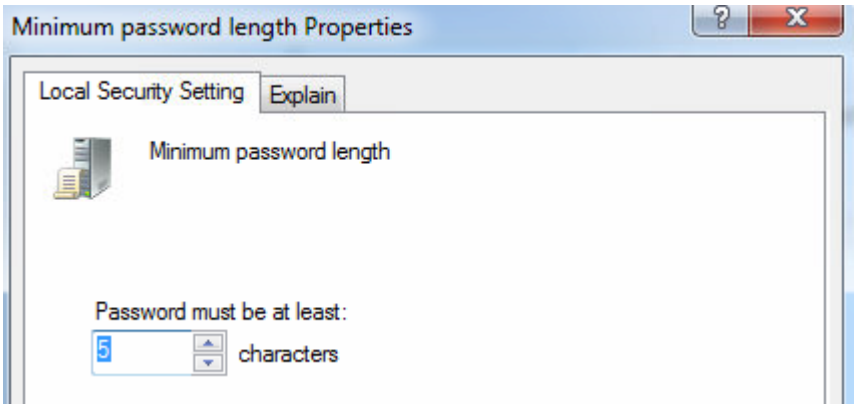
Account Policies

Under Security Settings let's check Account Policies. Under Password Policy we can change things such as maximum and minimum password age, minimum password length and complexity requirements, etc.



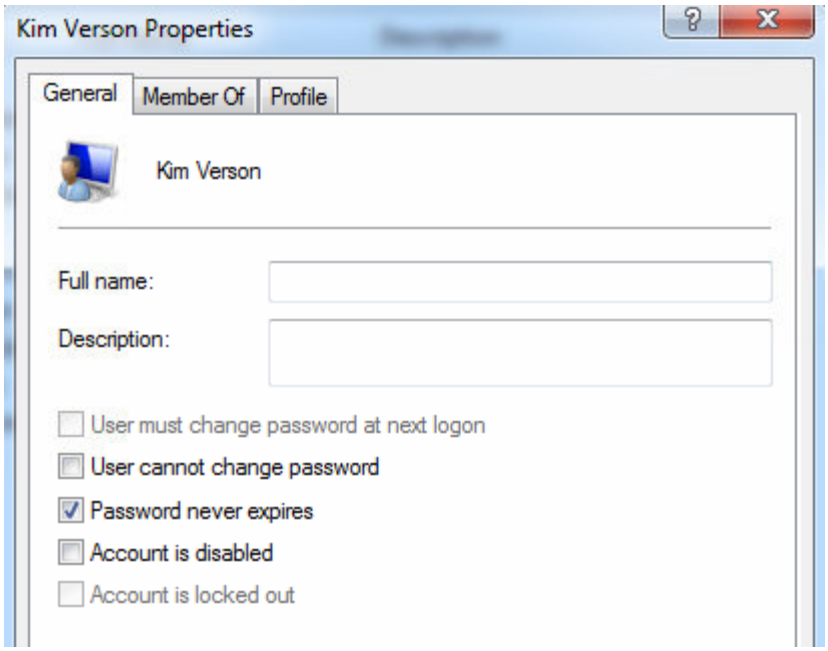
Password Policy

In our case these settings are not configured, but we can change that to suit our needs. For example, it is a good idea to change the minimum length of passwords from 0, to prevent blank passwords.



Minimum Password Length

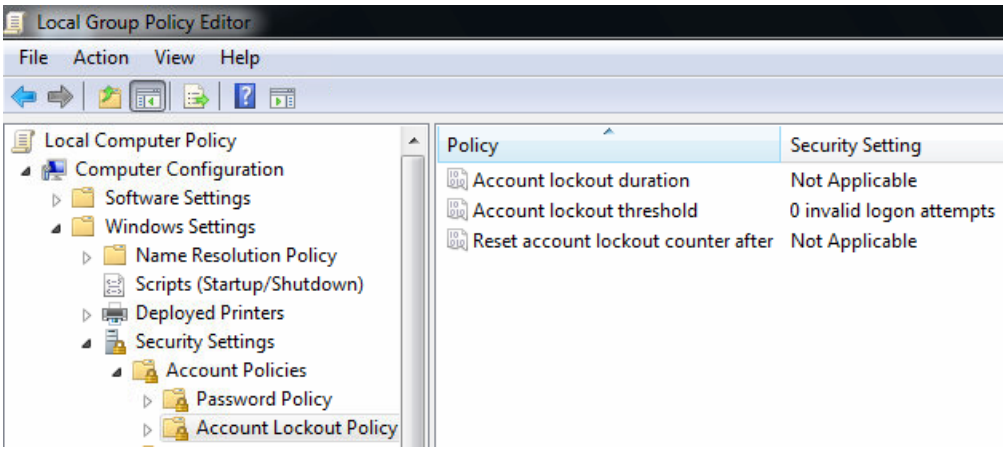
If we set the "Minimum password age" option to 5, users who change password won't be able to change it again for 5 days. Minimum and Maximum password age options are only applied to users which don't have "Password never expires" option set. For example, user Kim Verson has "Password never expires" option checked, so minimum and maximum password age is not applied to Kim (we have used Local Users and Groups in Computer Management to check this).



Password Never Expires option

If we enable Password history policy, users will have to use unique passwords every time they change it. Maximum password age has to be configured for password history to take effect. Maximum password age enforces users to change passwords after specified length of time. Password complexity policy prevents using simple passwords which are easy to crack. If we set that option, users will have to use special characters in their passwords, with minimum of 6 characters, and won't be able to use dictionary words or any part of user login. If we set the "Store passwords using reversible encryption" should not be set, since passwords will essentially be readable as plaint text.

The next thing we can check is Account Lockout policy.



Account Lockout

Keep in mind that these account lockout policy applies to all users on local computer, including the Administrator account. If we only have one administrative account on the machine and that account gets locked out, we won't have any way to log in to the machine with the user which has administrative rights any more. This is the case on local machines, so we should be careful when setting account lockout policy on local machines. The value of 0 in "Account lockout threshold" means that accounts won't be locked out. If we specify some other number here, the system will count invalid log on attempts and then lockout the user after the specified threshold. We can also specify the duration of the lockout and how much time the counter of invalid log on attempts is remembered.

Source: http://www.utilizewindows.com/7/security/477-user-account-policies-in-windows-7