# Longhorn is ready to provide multi-domain passwords

I've heard for 7 years a sentence: 'I wish Microsoft allowed multi-domain password policies in a single domain'. And now that has come true! The next generation of Microsoft servers, with the source name Longhorn, will provide this functionality in a very specific way.

**I've heard for 7 years a sentence: 'I *wish Microsoft allowed multi-domain password policies in a single domain* '. And now that has come true! The next generation of Microsoft servers, with the source name Longhorn, will provide this functionality in a very specific way.** After a long wait, now one of the most requested components for Windows Active Directory has been met. Does Windows 2000 and Windows 2003 provide this component? If your answer is yes, after reading this article, you will understand how wrong that view is, and also know Longhorn's ability in this area.

**Deploy domain password policy with Active Directory Windows 2000/2003**

During the installation of Windows Active Directory for a Domain Controller, two Group Policy Objects (GPOs), ie group policy objects, are created. These GPOs are named Default Domain Controllers Policy and Default Domain Policy. First, of course we will target domain controllers, which are linked to the Domain Controller organizational unit (OU) but only to the OU during the new Active Directory installation process. The primary responsibility of this GPO is to set user privileges for the Domain Controller, as well as some other mixed security settings.

The Default Domain Policy links to the domain node during the entire installation process, with a default responsibility. That's setting Password Policy for all user accounts in the domain. Password Policies are only one of three different sections in the Account Policies area. There are also Account Lockout Policies and Kerberos Policies.

Within the Default Domain Policy, the settings for controlling domain user account passwords and key limits are created, as shown in Figure 1, Figure 2 below.

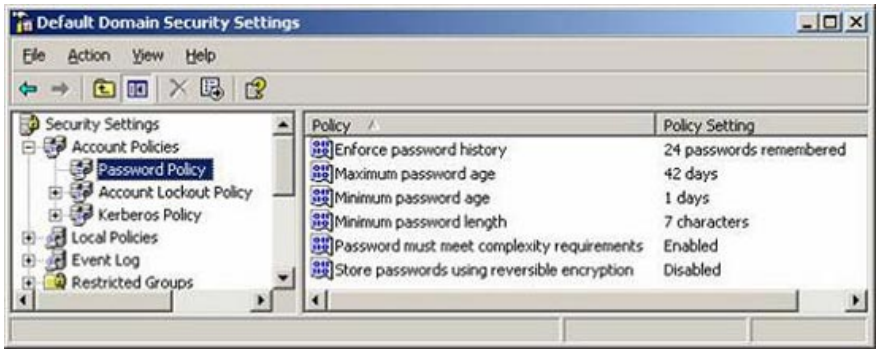


*Figure 1* : Password Policies settings.

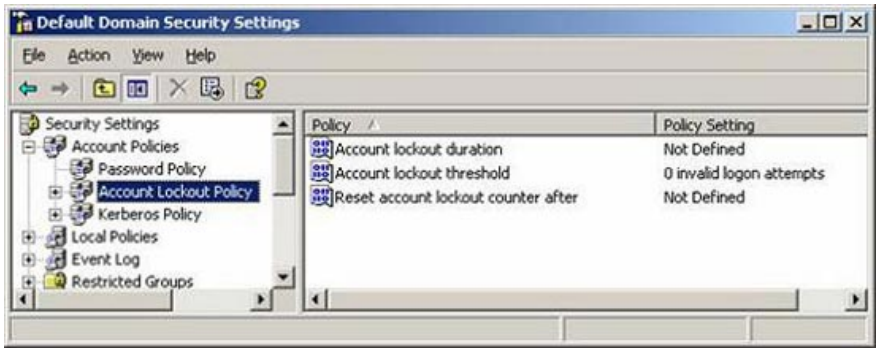


*Figure 2* : Settings Account Lockout Policies.

If the default values ??are not welcome, you can edit them. There are two ways to do this: update the Default Domain Policy to achieve the desired Password Policy settings. Or do not change the default GPO and create another GPO. Then link it to the domain, configure with the desired Password Policy settings and other settings and move to a higher priority than the Default Domain Policy, as shown in Figure 3.

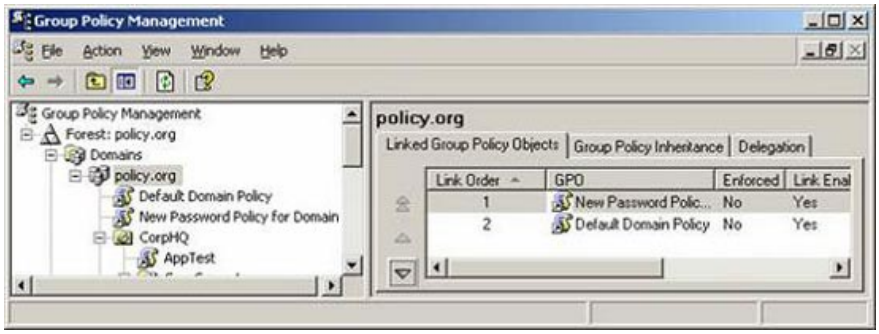


Figure 3: New GPO with higher priority is created to provide
Password Policy for all user accounts in the domain.

**Set up a local security account password policy (SAM)**

If you think that Password Policy can be set in a GPO linked to a new OU you created, you are right. But if you think that Password Policy settings in this new GPO will affect the user account in that OU, you are wrong. This is a very common misconception about how Password Policy works in Active Directory Windows 2000/2003 domains.

Settings created in these GPOs do not affect user accounts, but affect computer accounts. This is shown in Figure 1 above. You can see that the Account Policies section is clearly under the Computer Configuration node in the GPO.

The confusion is increasing due to the fact that the computer account does not have a password, and the user account does. To fix this, GPOs configure the SAM (security account manager) configuration on the computer, giving password limit controls for the local user account stored there.

Also note that Password Policies settings in the GPO linked to the default OU have a higher priority than the Default Domain Policy. Therefore, any settings made in the GPO linked to the OU will affect the domain level. This can be changed through the Enfored option on GPOs linked to the domain that has the desired Password Policy settings, as shown in Figure 4.

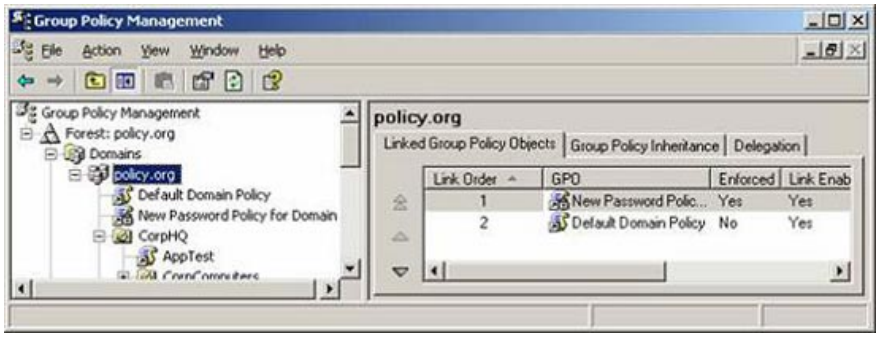


*Figure 4* : GPO linked to the domain with the Enforced option configuration.

**Longhorn domain password policy**

In Longhorn, the concept and operation of password policy settings for domain user accounts often have reverse results. Multi-domain password policies can now be applied to the same domain. Of course, this is a long-awaited component, long ago, from the time of Windows NT 4.0. This sentence has also become too familiar: 'I want a more comprehensive password for administrators compared to standard users in the domain'.

Now, you can create an optional password policy for any type of user in your environment. It could be people in HR, finance, staff, IT management, support staff .

The settings you will have during the transfer period are the same as in the current Group Policy Objects. The only thing is that you won't need to use Group Policy to configure them. With Longhorn, there are new objects in Active Directory for you to configure. That is Password Settings Object, which includes all the properties currently available in Password Policies and Account Lockout Policies.

To deploy, you need to create a new LDAP object named msDS-PasswordSettings below where Password Settings is stored. The LDAP path has the form: ' cn = Password Settings, cn = System, dc = domainname, dc = com '. Below this new object, you'll need to fill out the following attributes:

msDS-PasswordSettingsPrecedence: This is an important attribute, which can be controlled if a user has membership in multiple groups with different password policies set.

**msDS-PasswordReversibleEncryptionEnabled** : Enable / disable the function to know if the reverse encryption mechanism is supported.

**msDS-PasswordHistoryLength** : Determines how many passwords must be unique before it can be reused.

**msDS-PasswordComplexityEnabled** : Set a password mechanism that requires at least 6 characters, 3 or 4 character types and deny which password is used as the login name.

**msDS-MinimumPasswordLength** : Set the minimum length for the password.

**msDS-MinimumPasswordAge** : Determines how long the user must use the password before changing it.

**msDS-MaximumPasswordAge** : Determine how long users can use passwords before they are requested to change.

**msDS-LockoutObservationWindow** : Specifies the amount of time the wrong password counter will be reset.

**msDS-LockoutDuration** : Determine how long the account will be locked after too many incorrect password entries.

After the properties are configured, the new object will be linked to the Active Directory extension group. The affiliate program is complete in the step of adding the LDAP name of the group to the msDS-PSOAppliesTo attribute.

**Summary**

Longhorn will be presented with a number of new components, new technologies and new methods for controlling and managing objects in your business. Until now, one of the most impressive and fast components that will become popular is the ability to set multiple password policies in a single domain. You may have begun to think about the impact of the new functionality on your current system environment and start planning what you want to do for a long time.