

Re: Enforce Password Aging... Gracefully

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-12/msg00265

- *From:* jwd <jwd@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 7 Dec 2007 02:26:02 -0800
-

You could write a script to change the pwdLastSet attribute for all users to a date that is within 90 days of the date when the policy is enforced. Set the policy to prompt users 14/20 days or whatever before the password expires. There will then be no immediate effect when you enforce the policy and users will be prompted a set number of days before the passwords expire.

As said before you cant do this OU by OU as if you set some pwdLastSet attributes and enforce the policy the ones you didnt set will be expired immediately.

The tricky bit however is setting the pwdLastSet attribute. This will need to be done via a script. The pwdLastSet attribute is an Interger8 (64 bit) value which represents the number of 100 nanoseconds intervals between when the password was last set and January 1st 1601. You would need to do a bit of maths to work out what value you would need to set it too. You should be able to find some guides for setting this attribute if you search for pwdLastSet.

Best Regards
Joe Dunn MCSE

"Mr_Huang" wrote:

Hi Joe,
all i want is to have alerts when the user logon or (even lock the screen) before the password expires, is it possible to do so?
since i'm not much familiar with the vbscripting, not sure if i could write a script and change the expiry date manually with certain OU, so i can roll out this phase by phase.
Thanks,
huang

On Dec 6, 5:13 pm, jwd <j...@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

If the users passwords are more than 90 days old when you enforce the policy

Re: Enforce Password Aging... Gracefully

then they will be expired and the users prompted to change the next time they login. This can not be done OU by OU as the password policy is domain wide.

There is no "grace period" policy setting as you mention – if the passwords are older than the policy allows they will be expired. What you can do though is inform your users maybe several weeks before hand that this policy will be enforced and ask them to change their passwords on their own accord. These passwords will then not be expired when you enforce the policy as they are within the 90 days. If people choose to ignore this then they will be forced to change if their passwords are more then 90 days old when you enforce the policy.

If the passwords are younger than 90 days but do not match the length and complexity requirements then they will not be forced to change when the policy is enforced as these requirements are only checked when the password is set.

Best Regards
Joe Dunn MCSE