

Re: AD 2000, Blank passwords, and Group Policy

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2004-09/0611.html>

From: Steven L Umbach (*n9rou_at_n0-spam-for-me-comcast.net*)

Date: 09/16/04

Date: Thu, 16 Sep 2004 05:26:20 GMT

OK. I set up an account with password policy enforced and experienced the same as you did. I have never seen that before as I never use blank passwords so I learned something new today. The only thing I can suggest is to leave the accounts as they are and when their passwords [or lack of password] expires, hopefully those with a blank password will have to enter a new password that complies with policy to be able to logon. Otherwise you will have to disable [NOT undefined] any password requirements for minimum password length and complexity and the configure those accounts to change password at next logon. When done doing that, then enable the password policy requirements again. I tested this and it will force a user with a blank password to change their password at next logon and it must comply with password policy. They can just leave their old password as blank if they did not use one when they are prompted to enter it. They will have to enter their new password twice.

I don't know of a way offhand to search and change specific users passwords in a batch file though you may want to post in a Windows scripting newsgroup for that You might be able to use something like the resource tool addusers to export users to a file, import it into a spreadsheet or such. Delete all but the users you want to change and import them back in. By default addusers gives users a blank password and requires the user to change password at next logon. You can also give a user a password by using the " net user username password " while at the keyboard and a tool from SysInternals allows you to change passwords on remote computers.

<http://support.microsoft.com/default.aspx?scid=kb:en-us:301940> — will work in a W2K domain

http://www.petri.co.il/download_free_reskit_tools.htm — download here.

<http://www.sysinternals.com/ntw2k/freeware/pspasswd.shtml> — Ppasswd link You probably could make a batch file with this.

A couple other things to check out. Take a look at Hyena from SomarSoft. They offer a trial period download and it can massage user accounts in many ways that you can not in Windows 2000. If there is a Windows XP Pro computer on the domain you can install Adminpak on it for Windows 2003 which will allow you to logon to it as a domain admin and use the Active Directory command line tools to search for and change user accounts. For instance you could do a query for all accounts to find which have the password never expires attribute enabled by using dsquery user piped to the dsget user commands. You could also move all users that need password never expires disabled into an OU and then use dsquery piped to dsmod to query for those users and

then change their accounts to remove the password never expires attribute as in "dsquery user OU=needtochange,DC=mydomain,DC=Com | dsmod user -pwdneverexpires no". The same can be done to configure users to require they change their passwords at next logon using " | dsmod user -mustchpwd yes " The last link explains much more about the AD command line tools. --- Steve

http://www.somarsoft.com/somarsoft_main.htm

<http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc>

"JASlaughter" <JASlaughter@discussions.microsoft.com> wrote in message news:77D6D583-C5FA-4B53-896E-41308BC01C70@microsoft.com...

> *Oops, I think I failed to make it clear, that the although many users have
> blank passwords, the new policy set in place is set to require a minimum
> length password. I could set the policy to not enforce this until after all
> users have changed their passwords, but then I run into the problem of users
> not following my direction (I'm very much remote and actually have no direct
> contact with them). Not only that, but currently existing users also have
> 'Password does not expire' set, so they won't run into the max password age
> fix either. (Don't look at me, I didn't set up this thing, just trying to
> help a friend)*
>
> *Because this policy is now in-place, I cannot use the 'Force' checkbox as it
> will give an error stating that changes could not be made since their current
> password fails the domain security policy. What I'm looking for is a way to
> force them to change their password without making their passwords meet this
> requirement first. Actually, as it is now, I cannot make -any- changes to a
> user that has a blank password because their passwords donot meet the policy
> requirement.*
>
> *If I -must- assign a password first, then is there a way to batch create
> passwords for these users?*
>
> *"Steven L Umbach" wrote:*
>
>> *I just created a user with a blank password on my test W2K dc and after I created
>> the
>> user I was able to go back and select "must change password at next logon" without
>> a
>> problem. Make sure that "user can not change password" is not enabled for that
>> user
>> you are having a problem with. While not an elegant solution, you could set the
>> maximum password age to short duration such as ten days [temporarily of course,
>> maybe
>> one week] which would require users to change their passwords if older than the
>> maximum [most probably are very old if using blank] and do not have password
>> never
>> expires set in their account properties, which would cause some grief with users
>> but
>> you got do what you got do. Just be sure to inform users of any new password rules
>> with examples of what will and will not work. VPN logons are not always logons to
>> the*

>> domain. It may help if you have the users specify the domain name when they logon
>> which requires that the VPN connectoid properties be changed to show the three
>> lines – logon name, password, domain. Shortening the maximum password age would
>> force
>> users to change their passwords to gain access to domain resources. Just be sure
>> the
>> minimum password age is not more than the maximum password age. I would strongly
>> encourage users to change their password voluntarily before you force a change and
>> you could enforce minimum password length and complexity before you enforce
>> maximum
>> password age . --- Steve
>>
>>
>> "JASlaughter" <JASlaughter@discussions.microsoft.com> wrote in message
>> news:FEB81AD8-CE49-4AF3-B03F-A3993BE8983A@microsoft.com...
>> > Hello,
>> >
>> > I have a situation that I cannot seem to solve. I've looked on the web and
>> > even went through my old 2000 MCSE study books.
>> >
>> > Here is my situation:
>> >
>> > Issue #1
>> > =====
>> > I need to force users to change their password upon next logon –without–
>> > changing their currently _blank_ password. AD U/C won't let me set that
>> > option on a user with a blank password.
>> >
>> > If I absolutely have to create a password for these users to accomplish
>> > this, is there a way to create a password for all users with a currently
>> > blank one? (It could be the same for all users).
>> >
>> > Issue #2
>> > =====
>> > I'm connecting remotely via Kerio's VPN service (just FYI). When connecting
>> > to a resource with a user that –does– have the force password change checked,
>> > I'm not prompted to change my password. I seem to be able to connect using
>> > my old password.
>> >
>> > Can someone out there point me in the right direction?
>>
>>
>>