

Re: Requiring domain password change

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2009-05/msg01149

- *From:* Davidi <Davidi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 26 May 2009 16:25:01 -0700
-

Thanks for the response. I'm ready to receive a number of support calls when we implement the new password change so I don't mind doing it in one big swoop.

– So, if I tell some users to change their passwords manually, let's say 7 days before I reset the Maximum Password Age (I'll probably switch our current setting from 0 to 365 days), those users won't be required to change their passwords again for 358 days, right?

– Also, if the user is logged on while the Maximum Password Age is changed will they still have access to their network resources (Exchange, network drives, SQL sessions) or will they be denied access from those resources until they log back on and change their password.

Thanks again!

"Richard Mueller [MVP]" wrote:

"Davidi" <Davidi@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:E598FB69-C36D-49B8-AE20-B3A7078E3103@xxxxxxxxxxxxxxxxxxxx

I want to require all domain users (except users accounts with passwords that do not expire) to change their password on a specific day. I understand that I need to set it from the Default Domain Policy but I'm not 100% sure that it's the "Maximum Password Age" setting that I need to change. Currently the maximum password age is set to 0 so we don't require users to change their passwords on set interval.

– Let's say today is Monday and I want them to change their network passwords on Thursday. Would I need to change the "maximum password age"

Re: Requiring domain password change

to
3 or 4 days? Is the timestamp for this value set once I change the value from 0 to 3?

– And if I don't want the passwords to expire again after I change the value to 3 or 4, I would assume I need to set it back to value 0 once everyone changes their password.

– Also, is there a way to set Windows to warn the user a day or two before they have to change their password?

Thanks.

If in the past you have had no password age requirements, then everyone's password was last set long ago. As soon as you assign a password age of a few days, almost everyone's password will be older than this value (unless the account was created and the initial password was set in the last few days). Everyone's password will be expired the next time they log on. I think you need to assign a password age on the day when passwords will expire. However, this means there will be a crush that day, as everyone's password will expire and users that are not used to this will call for support all at once.

A better approach might be to assign an extremely large value for maximum password age (not 0), so that no one's password will be expired. Then somehow divide your users into reasonable sized groups (maybe by OU or group membership). Then run a script or utility to expire the passwords for only the users in one of the groups. This is done by assigning the value 0 to the pwdLastSet attribute of the user object. This value is so far in the past that the password will be expired no matter how large the maximum password age policy is. If the groups are of reasonable size, the support requests will be manageable. Perhaps expire the passwords for one group per week. After everyone has had their password expired, you can reassign a more reasonable value for maximum password age.

--

Richard Mueller
MVP Directory Services
Hilltop Lab – <http://www.rlmueller.net>

--