

Re: Delegate Control... Reset Passwords

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-11/msg00983

- *From:* "Jorge Silva" <jorgesilva_pt@xxxxxxxxxxxx>
 - *Date:* Tue, 18 Nov 2008 20:35:34 -0000
-

Hi

pwdLastSet makes sense because you WANT to have the ability to select the option to force the user to change the password in the next logon. You don't want that Admins keep the users password. Of course you can tell the user to change it by it self, but there are many companies that have this procedure – After resetting a PW, force the user to change it. You need for that Read and Write permissions in pwdLastSet attribute.

For that check:

<http://support.microsoft.com/kb/296999>

Don't use existing AD groups to do that, create your own Groups and assign the necessary permissions to do their job. check the haow at:

RESET USER PASSWORDS

<http://blogs.dirteam.com/blogs/jorge/archive/2006/01/05/369.aspx>

--

I hope that the information above helps you.

Have a Nice day.

Jorge Silva

MCSE, MVP Directory Services

Please no e-mails, any questions should be posted in the NewsGroup

This posting is provided "AS IS" with no warranties, and confers no rights.

"JPolicelli [MVP-DS]" <JPolicelliMVPDS@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:%23H0dHoZSJHA.1148@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I typically do not. What is it that you want them to do with this attribute?

--

JPolicelli, MVP – Directory Services

This posting is provided "AS IS" with no warranties and confers no rights!

<http://johnpolicelli.wordpress.com/>

"Mark Z." <MarkZ@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

<news:C5249BEC-756C-4EB9-84EA-EBA5340B73A1@xxxxxxxxxxxxxxxxxxxx>

Re: Delegate Control... Reset Passwords

Did you also delegate them permission to the pwdLastSet attribute?

"JPolicelli [MVP-DS]" wrote:

The Account Operators group is the wrong group to use. This group has the permissions to create/delete InetOrgPerson objects, computer objects, group objects, and user objects on every OU in the domain by default. The goal is to reset passwords for users in selected OU's, but not all.

You are headed in the right direction Otto. Your "PCAdmins, Reset Password, <not inherited>, User Objects" line indicates that you setup the appropriate permission to meet your goal. If you run the DSACLs command, what does it show for the PCAdmins group? You should see something like this for the permission in question:
Inherited to user

Allow DOMAINNAME\PCAdmins Reset Password

Another question...is this problem applicable to password resets for all users or a subset of users? If it is the latter, check whether the applicable user(s) is/are a member of a protected group:
Account Operators
Server Operators
Print Operators
Backup Operators
Domain Admins
Schema Admins
Enterprise Admins
Cert Publishers

If they are, then permissions on these objects are not inherited from the Domain ACL or OU ACLs. You need to delegate permissions on the AdminSDHolder object.

JPolicelli, MVP – Directory Services
This posting is provided "AS IS" with no warranties and confers no rights!

Re: Delegate Control... Reset Passwords

<http://johnpolicelli.wordpress.com/>

"Meinolf Weber" <meiweb(nospam)@gmx.de> wrote in message
<news:ff16fb66e2168cb171bbe074530@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

> Hello Otto,
>
> Are the not working accounts members of the "Account operators" group?
>
> Best regards
>
> Meinolf Weber
> Disclaimer: This posting is provided "AS IS" with no warranties, and confers
> no rights.
> ** Please do NOT email, only reply to Newsgroups
> ** HELP us help YOU!!!
http://www.blakjak.demon.co.uk/mul_crss.htm
>
>
>> I have a group of admins that are able to reset passwords for users >> in
>> selected OU's, but not all. Security settings appear the same on all
>> OU's, but these admins all receive the message "Access Denied" when
>> trying to reset passords. Here is my configuration:
>>
>> ADUC = <domain.com>\Admins
>> Security Group – "PCAdmins"; 7 members
>> OU Structure:
>> <domain.com>\Community\Name1\Computers
>> <domain.com>\Community\Name1\Users
>> <domain.com>\Community\Name2\Computers
>> <domain.com>\Community\Name2\Users
>> etc...
>> Security placed on "Users" OU as follows:
>> – PCAdmins, Read/Write Property, <not inherited>, User Objects
>> – PCAdmins, Reset Password, <not inherited>, User Objects
>> – PCAdmins, Read,
OU=Community,DC=domain,DC=Com, This object and all
>> child
>> objects
>> – PCAdmins, Create/Delete Computer Objects,
DC=domain,DC=Com, This
>> object

Re: Delegate Control... Reset Passwords

>> and all child objects

>> Thank you.

>>

>

>