

# Re: Changing workstation Admin password through AD

---

*Source:*

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active\\_directory/2007-05/msg00068.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2007-05/msg00068.html)

---

- *From:* "Ken Aldrich" <[supportw@xxxxxxxxxxxxxxxxxx](mailto:supportw@xxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 9 May 2007 17:56:37 -0500
- 

Brian,

I don't want to sound contrarian, but there are a lot of organizations where bouncing every member server and workstation monthly is not practical. Some companies have strict change control policies that mandate patches of that nature only be applied once a quarter, or at other intervals of scheduled maintenance. The intervals in password change policies do not always line up with these schedules.

On the other side of that, some people cannot simply tell their auditors, "I'm sure the password must have gotten reset sometime in the last week because we patched all our computers."

At some point they may need to show a log, or proof. What if some workstations or servers were turned off for an extended period of time and were not patched? Sometimes the patching process fails and computers are not properly patched or rebooted. These hosts would not update their passwords if you were relying on that scripted process... and the only way to determine that would be to look at patch logs or some other type of log.

When you have a dependency like this, if your patch process develops a problem and does not patch each and every host, you may have a "finding" in your audit for failure to patch. But, if you rely on patching to force other processes such as this one, then you may multiply how many "findings" you have in an audit. Again, this is not a strong argument that would apply to everyone, but for some people it is a very important consideration.

There are some people out there that need to have a more precise change mechanism, or more importantly, a more precise logging mechanism for accountability.

Anyway, those are some of the considerations or "down sides" to using the GPO/startup script method... in addition to what Joe mentioned. They certainly are not an issue for everyone, but there are still a lot of people that do need workarounds for these concerns.

--

Ken Aldrich  
DSRAZOR for Windows

Re: Changing workstation Admin password through AD

Visual Click Software, Inc.  
www.visualclick.com

"Brian Desmond [MVP]" <brian@xxxxxxxxxxxxxxxx> wrote in message  
news:ePW4ETOkHHA.4516@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Should be getting bounced at least once a month for patches I'd hope.

--

Thanks,  
Brian Desmond  
Windows Server MVP – Directory Services

www.briandesmond.com

"Ken Aldrich" <supportw@xxxxxxxxxxxxxxxx> wrote in message  
news:OUr0pWLkHHA.4800@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Joe,

Those are great points and it is good for you to mention them. I see that startup script method recommended a lot on forums and I wonder how many people realize what you have said.

The other point is that in many organizations machines do not get rebooted very often... or even logged off. In that case, how can you be sure that passwords are being updated? Or that the password ages will be relatively similar? The only way to be sure is to force a reboot of everyone's computers... that just does not fly in many organizations. There are better methods available in that environment.

--

Ken Aldrich  
DSRAZOR for Windows  
Visual Click Software, Inc.  
www.visualclick.com

"Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx> wrote in message  
news:uM9wr\$DkHHA.4676@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

See now this isn't really safe... Anyone who can get to power user or admin level on a workstation will have a path to get that batch file and anyone with physical access to a machine can get admin regardless of what their "official" access level is. The machine has to have read access to the file in order for it to work and to get to a point where

Re: Changing workstation Admin password through AD

you can access sysvol as that machine isn't very difficult.  
Also someone  
could always just run a network sniffer and watch the clear  
text script  
come down over the wire.

--

Joe Richards Microsoft MVP Windows Server Directory  
Services  
Author of O'Reilly Active Directory Third Edition  
[www.joeware.net](http://www.joeware.net)

---O'Reilly Active Directory Third Edition now  
available---

<http://www.joeware.net/win/ad3e.htm>

Myweb wrote:

Hello Joey,

Add a simple batchfile to the startup script  
of the computer settings  
part (pw.bat for example).

```
net user administrator password
```

Remove domain users and everyone from  
the security, add only system and  
administrators with Full and domain  
computers with read and execute. If  
the workstation starts up the password will  
apply.

Best regards

Myweb

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

I would like to do the  
following:

1. Rename the  
Administrator account
2. Change the password to  
the Administrator account

Re: Changing workstation Admin password through AD

3. Create a dummy Administrator account  
4. Disable the new account called Administrator.  
I know how to rename the administrator's account, but how can I do the other three steps without visiting each workstation. I would like to push this out through AD if possible. Any suggestions are appreciated.