

Re: Help – administrator locked out!

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2008-02/msg00506.html>

- *From:* Ageing Brilliantine Stick Insect
<AgeingBrilliantineStickInsect@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 13 Feb 2008 19:59:00 -0800
-

Update – I went to the site today. What I found was that I STILL didn't have the whole story.....(sigh)

It seems that all the users bar 1 changed their passwords in time. That user now keeps getting a 'change password' notification, but they can't change their password because every time they enter their 'old password', it has expired. The administrator account is not getting any password change messages, but none of our usual passwords work, so the administrator just can't log on.

I tried booting into Directory Restore Mode (I had been told by one of my colleagues that he had successfully logged on in safe mode), but the local admin passwords do not work either.....

Back to the drawing board!

"Thee Chicago Wolf" wrote:

But wait.....there's more! And the reason for my frustrations will become evident.

Just to recap, here's the WHOLE story so far.

6 months ago we decided to install a domain controller and a small domain in one of our remote offices. As I mentioned, we normally have a third party do all our server building etc, but as this was a small network(1 server, 5 users) the job was handed to me. In did a bog-standard install of a Windows 2003 DC, created all the users, put the server in, and tested all the user accounts. It was all going swimmingly. The next step was to hand the machine over to ANOTHER 3rd party. They were going to install an enterprise application on the server, on the workstations and train the staff. They had requested an administrator logon to be able to complete this work. As they would need a fair degree of freedom in setting things up, I gave them a domain admin account. They arrived onsite and spent 4 days doing their thing.

Re: Help – administrator locked out!

The day after they had finished I got a call from the users at this site telling me this enterprise app was not working. I went to the site. What I discovered was rather dismaying – the third party had told all the users to forget their normal user accounts that they had been using for a couple of weeks, and they were all now to log on using the domain admin account! Not only that, but he had helpfully put a sticky note on each PC with the password! These are PC's that are in easily-accessible public places. One of them is even attached to a cash drawer! Not only did this third party not consider this any sort of security risk, the manager of this site also considered it a fine practice!

So I start investigating why this app wasn't working. It seems the 3rd party had installed the app on the server and 1 PC. He had left no instructions for the people at the site, or for me, so I spent the next hour on the phone finding out how to get this thing working, and then another couple of hours setting up each workstation.

So what does my boss do about this? Maybe not pay their bill? Maybe charge them for the time I spent doing their work? Nope.....nothing.....why should she care – she has a lackey (me) that can waste my time doing that sort of stuff.

Anyway, fast forward about 6 months. I'm on holiday. I get a call from the boss. "What's the password on that server?". I tell her. "OK....see you in 3 weeks". 3 weeks later I get to work. The story I get is this : The users at this remote site began getting 'change your password' messages while I was on

leave. All but 2 of the users waited until their password had actually reached expiry before letting us know ('us' being my colleagues who weren't on leave), and even then, rather than just changing their passwords they just rang the help desk to say 'we cant get in. we had been getting messages to change our passwords, but we didnt'. Why they didn't is anyone's guess, but there you go. So the boss tells me that not even the administrator can log on (which is right) and can I research the subject and see if I can fix things. She then went away for 2 days.

So I started investigating. What I found was this – all the accounts apart from 2 could not log on. My colleagues had actually attended the site, but had not been able to fix the problem. My colleagues had also received detailed instructions from our 3rd party network/hardware people as to how to solve this problem (the old boot into DSR more, install srvany etc etc), but for some reason had not been able to follow these instructions, and also did not feel the need to tell me that they had the info that I had just been told to go and find on the net. Even more frustrating, one of my colleagues apparently had logged on successfully into safe mode (so at least our local admin password still works), but he 'didnt know how he had done it', and 'couldnt remember how to do it again'.....but I still hadn't been told this, so at this stage I headed for this forum, and posted my post.

Re: Help – administrator locked out!

So hopefully Wolf, you can see why my frustration boiled over when I read your response. Not only have I been sold an absolute dump by my colleagues, but now people thought I was some sort of script kiddie! To be quite honest it never occurred to me that my post could be construed in that way.

Anyway, I'll be off to this site today. Hopefully the local admin password still works and I will be able to get things functioning again.....I'll let you know of success or otherwise.

Ah yes, 'tis the life of an IT guy. When things are working great, no one praises you. The second something breaks or doesn't work, your ass is in a sling, never mind it's a vendor or 3rd party that's responsible. That's why I hate IT some times. No worries on the posting. I guess now you can understand why I reacted the way I did. There's always a bunch of 13 year olds at some grammar school trying to break into the systems of their sysadmins. While a lot of MVPs on this and the XP group are more than happy to give ANYONE the aforementioned tool to break the Admin password and "get them back in" to their locked out system, I don't. Anyone worth their IT mettle knows better. Or at least SHOULD know better. The Offline tool is a real enabling tool so I don't like to be an enabler, you know? There's a reason why people make password disks in case of emergency (break glass, ha ha). I can count on my fingers and toes how many times someone comes in with the "I got this laptop from a friend / family member / garage sale/ etc. and I don't know the Admin password, how do I get it or get into the system?" in the XP forum. I always say reformat and set your own password. When a person gets any kind of system, there's no business getting into someone else's stuff. Period. Format and start over like everyone else. It's just a standard practice. Tough luck if you can't get into someone ELSE'S system, you know? Hope the situation improves. Take care.

– Thee Chicago Wolf