

# Re: Prevent changes to Administrator password

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2008-10/msg01495](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2008-10/msg01495)

---

- *From:* "Jorge de Almeida Pinto [MVP - DS]"  
<[SubstituteThisWithMyFullNameSeparatedByDots@xxxxxxxxxx](mailto:SubstituteThisWithMyFullNameSeparatedByDots@xxxxxxxxxx)>
  - *Date:* Tue, 28 Oct 2008 08:22:47 +0100
- 

all those proposed changes won't do you any good. You can set a million DENY ACEs for a certain DA and in a few clicks that same DA undoes what you have done.

rule of thumb:

- \* A DA can do ANYthing!
- \* You cannot prevent a DA from doing ANYTHING
- \* End of story

see a similar story:

<http://blogs.dirteam.com/blogs/jorge/archive/2006/12/28/Granting-admin-level-access-for-the-OS-on-DCs-but-no>

--

Cheers,  
(HOPEFULLY THIS INFORMATION HELPS YOU!)

# Jorge de Almeida Pinto # MVP Identity & Access - Directory Services #

BLOG (WEB-BASED)--> <http://blogs.dirteam.com/blogs/jorge/default.aspx>

BLOG (RSS-FEEDS)--> <http://blogs.dirteam.com/blogs/jorge/rss.aspx>

-----  
\* How to ask a question --> <http://support.microsoft.com/?id=555375>

- \* This posting is provided "AS IS" with no warranties and confers no rights!
  - \* Always test ANY suggestion in a test environment before implementing!
- 

#####  
#####  
-----

"John Policelli [MVP - DS]" <[JohnPolicelliMVPDS@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:JohnPolicelliMVPDS@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
<news:4478301B-2C17-4599-ADCB-E388F3515E60@xxxxxxxxxxxxxxxxxxxxx>

I am aware that a DA can become EA. However, if you put the right controls in place, you can also mitigate this.

Re: Prevent changes to Administrator password

As I previously mentioned, I was throwing a "potential option". I was upfront with this in my first response to this post. I did not state it is tried, tested, and true. However, it is a starting point for the user who posted this question.

Nonetheless, you make a good point Deji, you would also need to ensure the DAs in question do not have the ability to change group membership on the Restricted Admins group to mitigate against what you propose Deji. You would also need to make sure the DAs in question cannot elevate their rights to EA, which is feasible.

I still agree with everyone – don't give DA to anyone you do not trust. However, you can build on my potential option if you want to find a way to try to mitigate this risk instead of living with the risk.

--

Please rate my posts: helpful/not helpful/answer/not an answer.

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

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

"A, Deji" wrote:

You are aware that a DA can become an EA, right? And that the DA, with the know-how, can overwrite pretty much any definition in the domain. I'm sure that you know all these. But (just thinking about your proposition, having not tried it out yet), what if the DA in question just simply removes his/her account from the Restricted Admin group and clears the flag?

Deji

"John Policelli [MVP – DS]"  
<JohnPolicelliMVPDS@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
wrote in message  
[news:196E5FDF-271B-4A6E-A365-14749F76B74C@xxxxxxxxxxxxxxxxxxxx](mailto:news:196E5FDF-271B-4A6E-A365-14749F76B74C@xxxxxxxxxxxxxxxxxxxx)  
> By adding the Deny Write Permissions ACE, these individuals will not >  
> have  
> the  
> permission to modify the ACL on AdminSDHolder. This is what prevents  
> them.  
> -- > Please rate my posts: helpful/not helpful/answer/not an answer.  
>  
> This posting is provided "AS IS" with no warranties and confers no >  
> rights!  
> ALWAYS TEST!  
>  
> Blog: <http://johnpolicelli.wordpress.com>

Re: Prevent changes to Administrator password

>  
>  
> "A, Deji" wrote:  
>  
>> John,  
>>  
>> what is to prevent these admins from undoing all these deny >>  
permissions  
>> you  
>> are setting, do whatever they want to do, then set it back to whatever  
>> you've recommended? Are you implying that these modifications will  
>> actively  
>> prevent a Domain Admin from messing with an object in his/her domain?  
>>  
>> Just curious.  
>>  
>> Deji  
>>  
>> "John Policelli [MVP – DS]"  
>> <JohnPolicelliMVPDS@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>  
>> wrote in message  
>>  
>> [news:56E9E7F2-F207-4396-81DB-AD9900317B60@xxxxxxxxxxxxxxxxxxxx](mailto:news:56E9E7F2-F207-4396-81DB-AD9900317B60@xxxxxxxxxxxxxxxxxxxx)  
>> >I agree with everyone on this post...you should not give DA if you do  
>> >not  
>> > trust someone. However, the reality is there are cases where you may  
>> > need  
>> > to  
>> > give DA to someone. Also, just because you do not want them to >> >  
change  
>> > the  
>> > password of the Administrator account in the root domain, does not >>  
> mean  
>> > you  
>> > do not trust them. So I am giving you a potential option to help you  
>> > mitigate  
>> > the risk of these individuals changing the password on the  
>> > RootDomain\Administrator account.  
>> >  
>> > First, you need to understand that permissions on the  
>> > RootDomain\Administrator account are applied via AdminSDHolder so  
>> > you  
>> > need  
>> > to  
>> > modify the permissions on the AdminSDHolder object in the root >> >  
domain.  
>> > Keep  
>> > in mind that doing this will prevent these individuals from >> >  
resetting  
>> > the  
>> > password for any user that is a member of a group that is protected >> >

## Re: Prevent changes to Administrator password

by  
>>> AdminSDHolder and prevent these users from modifying the ACL on  
any  
>>> user  
>>> that  
>>> is a member of the AdminSDHolder group. You need to decide whether  
>>> this  
>>> is  
>>> feasible based on your delegation requirements. If you decide that >>>  
this  
>>> is  
>>> feasible, this is something you can TEST. Remember, these are pretty  
>>> serious  
>>> changes, so test the heck out of it in your environment before  
>>> implementing  
>>> it into production.  
>>>  
>>> 1) Create a group in your root domain (call it whatever you want, >>>  
but  
>>> I'll  
>>> refer to it as "Restricted Admins")  
>>> 2) Modify the AdminSDHolder in your root domain as follows:  
>>> – Deny the Restricted Admins group the Reset Password permission  
>>> – Deny the Restricted Admins group the Write Permissions permission  
>>>  
>>> You can view the following for more information on modifying  
>>> AdminSDHolder  
>>> permissions.  
>>> -- >>> John Policelli  
>>>  
>>> Blog: <http://johnpolicelli.wordpress.com>  
>>>  
>>> This posting is provided "AS IS" with no warranties and confers no  
>>> rights!  
>>> Always test before proceeding.  
>>>  
>>>  
>>> "Taz1972" wrote:  
>>>  
>>>> Hello,  
>>>>  
>>>> I administer a server 2003 AD domain which spans many sites across  
>>>> the  
>>>> globe. Problem is there are too many people who knew the root  
>>>> administrator  
>>>> password (which contains enterprise admin rights), so I decided to  
>>>> change  
>>>> the  
>>>> password. I then gave the other admins new accounts with just >>>>  
domain  
>>>> admin

Re: Prevent changes to Administrator password

>> >> rights so they have just enough rights to do their jobs. They do >> >>  
not  
>> >> need  
>> >> enterprise admin rights.  
>> >>  
>> >> The problem is that the other admins can change the root >> >>  
administrator  
>> >> password at their leisure, and this is not what I want them to be >> >>  
able  
>> >> to  
>> >> do!  
>> >>  
>> >> How can I prevent then from changing the password of the root  
>> >> administrator  
>> >> account? Is there a registry hack or GPO setting that can do this? >>  
>> Is  
>> >> this  
>> >> even possible to prevent?  
>> >>  
>> >> Hopefully there is some way to solve this, and I would greatly  
>> >> appreciate  
>> >> your quick advise.  
>> >>  
>> >> Thank you,  
>> >> Admin  
>> >>  
>>  
>>