

Re: Remove Administrator Account from Administrators Group

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2007-08/msg00408.html

- *From:* "Thomas M." <NoEmailReplies@xxxxxxxxxx>
 - *Date:* Tue, 28 Aug 2007 12:36:53 -0600
-

And that's really all we are trying to do. I am in charge of limiting user rights for employees ranging from the receptionist to high-level IT staff, including Exchange Server administrators with 10 years of experience. We figure that renaming the Administrator account is not going to stop a determined Exchange Server administrator with the knowledge and rights to get around things, but it might stop the less knowledgeable and less motivated, and so therefore it's a step in the right direction. Also, we are renaming the account to something sufficiently random (renaming it to "Admin" would be pretty pointless since that could be easily guessed by a remote user).

Going back the issue of high-level IT staff, given their knowledge and rights it may not be possible from a technical perspective to stop them from working around security policies, but there are other options available, such as disciplinary actions, that may dissuade people from attempting to circumvent security.

--Tom

"Mathieu CHATEAU" <gollum123@xxxxxxxx> wrote in message news:85ADE192-7904-4327-AC59-703E8C59DEB2@xxxxxxxxxxxxxxxx

indeed, that just help if someone try to break it remotely (so without the knowledge it's not the default name)

--

Cordialement,
Mathieu CHATEAU
<http://lordoftheping.blogspot.com>

"G Johansson" <fantomen@xxxxxxxxxxxxxxxx> wrote in message news:O9s3NuX6HHA.5164@xxxxxxxxxxxxxxxx

Re: Remove Administrator Account from Administrators Group

Just for your information, renaming the administrator account is not really a security option since it will still have same SID.

--

G Johansson
fantomen@xxxxxxxxxxxxxxxxx
<http://GPfaq.se>

"Thomas M." <NoEmailReplies@xxxxxxxxxxx> skrev i meddelandet
<news:%23iWcSTO6HHA.1208@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Yep. That part I got. I was just not seeing where to find the policy to rename the local Administrator account. I'm trying Mathieu's suggestion for that, and will post back here once I have tested it.

--Tom

"Paul O" <polson@xxxxxxxxxxx> wrote in message
<news:ui9eVvP6HHA.1484@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I use GPMC Computer Config>Windows Settings>Security Settings>Restricted Groups to add or remove local groups from the local admin group. Look up 'Restricted Groups' on MS or the web for more info.

PaulO

"Thomas M."
<NoEmailReplies@xxxxxxxxxxx> wrote in message
<news:u7zTcgM6HHA.3716@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

We are in the process of creating a group policy that will limit user rights on the desktop. A major element of our group policy is that it will push down the local Administrators group, which will contain a domain group for Network Administrators so that we will have administrator rights to all

Re: Remove Administrator Account from Administrators Group

machines. Currently, the local Administrator account is a member of the Administrators group that is pushed down by the group policy. Our security officer would like us to either remove the local Administrator account from the group policy, or push it down under a different name. In other words, if you were to logon to a PC that gets the group policy, and check the local Administrators group, you would not see the local Administrator account listed as a member, but you might see an account called something like "SecureDesktop" that would be the local Administrator account under a different name.

Given that you can't manually remove the local Administrator account from the local Administrators group (you get a message akin to, "This action is not allowed for built-in accounts"), I would say that what our security officer is asking may not be possible. However, I am very new to group policies and thought that I should seek some expert advice on whether or not this can be achieved through a group policy.

Is there a way through a group policy to remove the local

Re: Remove Administrator Account from Administrators Group

Administrator account from
the local Administrators
group, or to push
it down under a different
name?

--Tom