

Re: WinXP Pro "Users" Group Restrictions Affect Administrator Accounts

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-10/0922.html

From: David Jones (*kk7gw_at_yahoo.com*)

Date: 10/05/03

Date: Sat, 4 Oct 2003 18:43:55 -0700

Oh, I get it. From your original post it sounded like you were doing this to prevent *other* users from running as Admin, but now I understand what you're doing.

>-----Original Message-----

>It does kind of suck that the GUI tools don't enumerate the fact that

>these "special" SIDs are part of the Users group, and therefore all

>Userids that logon are part of that group. I like your idea about

>creating a special group to put the denyable users in. I didn't do

>that, I just removed the inheritance of the security properties from

>the folder in question, manually propagated those permissions, and

>then removed the Users group from the permissions.

There is no

>"deny" at all in there right now, but the Users group isn't mentioned

>at all, either explicitly or by inheritance in the folder's

>permissions anymore. I didn't like having to have one folder in the

>drive with a complete set of custom permissions though.

I'm going

>back to do it your way.

>

>With regard to the password in a text file issue, it's not the

>administrator password that's in the text file, it's the password to

>the User privilege only userid that's in the text file.

I'm kind of

>running my system backwards from the typical suggestion. Normally
>they suggest you run everything with a non-privileged userid and use
>runas to run individual programs with administrator privileges.
>That's obviously the safest route, but it's also a real pain in the
>butt, because so much stuff requires administrator privileges to run.
>My compromise solution was to log on with an administrator privileged
>account, but run applications that access the Internet, like IE and
>Outlook, under an account with just regular User privileges, as these
>are the ones most likely to get hit with a virus or trojan attempt.
>It took a while to get everything setup right and migrate settings and
>cookies from my administrator level account to the User level one, but
>now that it's done everything works just fine. The version of runas
>that allows the password on the command line is used to run the User
>level account, not the administrator level one. I've got my shortcuts
>and associations for all the pertinent file types (e.g. htm, html,
>mht, etc.) setup to run the .cmd file that invokes IE under the User
>account.
>
>Thanks for the tip on the special deny group.
>
>
>Scott
>
>
>On Fri, 3 Oct 2003 18:53:31 -0700, "David Jones" <kk7gw@yahoo.com>
>wrote:
>
>>A few points.
>>
>>One, by putting an Administrator password in a .cmd file
>>that is not encrypted, with the decryption mechanism only
>>available to authorized people, you've just created a

>>HUGE security risk.
>>
>>Anyone with physical access to the computer that you've
>>done that on can now get an Administrator username and
>>password.
>>NTFS permissions are nice and all, but there are a
>>variety of ways for a determined person to get around
>>them. The only true secure method when folks have
>>physical access to a machine is an encrypted password,
>>with decryption only available to authorized people.
>>
>>As to your Deny questions, by default, the special
>>SIDs "NT Authority\Authorized Users" and "NT
>>Authority\Interactive" are members of the Users group.
>>This means that any user account on the system, and
>>anyone who logs in via the console or Terminal
Services,
>>is made a part of the Users group.
>>
>>The recommended way to do this is what you've
discovered
>>already, or create a custom security group that
contains
>>the accounts you want to deny, then deny access to that
>>group.

>>>-----Original Message-----
>>>Hi folks:
>>>
>>>I'm running WinXP Pro in a workgroup environment (no
>>domain server)
>>>with simple file sharing turned off (i.e. using
>>the "old" NT4 and
>>>Win2K file security). All my drives are NTFS. I
>>usually just run my
>>>stuff under an account with administrator privileges,
but
>>I run
>>>programs that access the Internet (e.g. IE, Outlook,
>>etc.) under a
>>>userid that's only part of the Users group. Someone
>>created a version
>>>of "runas" that lets you put in the password on the
>>command line
>>>rather than being prompted for it, so it's not too
hard
>>to change file

>>>associations and desktop icons to point to a ".cmd"
file
>>that runs IE,
>>>Outlook, news reader, and their associated file types
>>with a seperate
>>>userid from the one you are logged on with.
>>>
>>>I wanted to protect a couple of directories where I
keep
>>things like
>>>passwords and financial information from the userid
>>running under the
>>>Users group just in case some kind of snoopware
program
>>got invoked
>>>via IE or Outlook and went searching through my hard
>>drives. By
>>>default I had the Users group setup with generic read
>>authority for
>>>all the drives, and write authority for just it's own
>>documents and
>>>settings folder (this was by individual userid as
setup
>>by WinXP
>>>versus the Users group as a whole), it's temp variable
>>folder, the
>>>place where the outlook data file was, and the folder
I
>>use to
>>>download files from the Internet.
>>>
>>>I went to the folder that had the financial stuff and
>>put a "Deny"
>>>entry on it for the Users group by checking the deny
>>full control box,
>>>which put checkmarks all the way down the column.
After
>>doing that I
>>>clicked the advanced button and looked at the
>>permissions and it
>>>showed all the regular permissions inherited from the
>>top of the
>>>drive tree and the "Deny" permission for group Users
as
>>not
>>>inherited, which all looked fine. However, after
doing
>>that I found
>>>out that I could no longer access the directory from
my
>>account with

>>>administrators privileges either. I verified that my
>>administrators
>>>account was not part of the Users group (the account I
>>use is not the
>>>built in administrator's account, but another one I
>>created). I can't
>>>figure out why my administrator level account gets
>>locked out when I
>>>disallow access by the Users group, unless the Users
>>group is really a
>>>built-in security principle group like Authenticated
>>Users, SYSTEM,
>>>Everyone, and that any accounts you create are
>>automatically part of
>>>the Users group even though it doesn't show up that
way
>>when you look
>>>at which groups you belong to. Can anyone confirm or
>>deny that this
>>>is the case?
>>>
>>>I ended up solving my problem by just removing the
Users
>>group from
>>>the folder I wanted protected, but this required that
I
>>change to
>>>folder to not inherit any security properties from
>>higher in the drive
>>>tree, and set each of the permissions on the folder
>>manually. I'd
>>>rather have it set where it inherits the security from
>>above and the
>>>only "extra" permission I have is one to explicitly
deny
>>the group
>>>Users.
>>>
>>>Thanks for your assistance.
>>>
>>>Scott
>>>.br/>>>>
>
>
>