

Re: how to create domain policy to restrict users ???

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2005-05/msg00032.html

- *From:* "Bruce Sanderson" <bsanders@xxxxxxxx>
 - *Date:* Tue, 3 May 2005 23:33:22 -0700
-

As I said, if there are NO local user accounts, no one can logon "locally", so just don't create any local user accounts.

Re. your "one ore question" – That's a question of which (domain) user accounts are members of Local groups. By default, the group Domain Users gets added to the local Users group. If you remove Domain Users from the local Users group, then only those user accounts or Domain groups that are specifically added to the local Users group (or that are members of other local groups such as Administrators or Power Users) will be able to logon at that workstation.

You can populate local groups on workstations using the Restricted Groups in a GPO. However, to control who can logon on to particular wokrstations using GPOs probably means creating seperate OUs and GPOs linked to them, which could be a lot of OUs and GPOs.

In most cases, there is not really a good reason to restrict particular users to logging on only at particular workstations. Howerver if you do have such a reason, then I suggest populating the local Users (or Power User, or Administrators as appropriate) manually on each workstation.

—

Bruce Sanderson MVP Printing
<http://members.shaw.ca/bsanders>

It is perfectly useless to know the right answer to the wrong question.

"Kresna Rudy K" <KresnaRudyK@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:71C43CB5-9DA5-45B3-87A5-807C191C8527@xxxxxxxxxxxxxxxxxxxx

- > Hi Bruce
- > Yes, you are correct, I want to prevent user to use local user to login in
- > workstation.
- > It is a good idea to disable local user, so user have to use domain user
- > to
- > login in their workstation.

Re: how to create domain policy to restrict users ???

>
> One ore question :
> How to prevent domain user to login in specific workstation ?
> For example : user1 only can login in workstation1 but user1 cannot login
> in
> workstation2. Is it possible ???
>
>
> Thanks...
>
>
> "Bruce Sanderson" wrote:
>
>> I'm not sure I completely understand your situation and what you are
>> asking.
>> So, I've attempted to provide some information in this post based on what
>> I
>> have interpreted from your posts. Sorry if I'm off base and you already
>> know all this stuff. Futher, I'm assuming you have Windows XP
>> Professional
>> (Home can not join a Domain, so this discussion is not relevant to XP
>> Home).
>>
>> A "Domain user account" is always a "Domain user account". That is, in
>> the
>> logon panel (the one that appears after the user presses Ctrl+Alt+Del),
>> to
>> use a Domain User Account, the user MUST select the Domain Name, not the
>> local Computer Name in the third box (the Log onto: box). If the user
>> selects the Computer Name in the Log on to: box, but supplies a Domain
>> Username and password, the login attempt will fail.
>>
>> When the Log on to: box specifies the Domain Name, the local computer
>> will
>> not attempt to "authenticate" the user (verify the credentials) but will
>> send the username and password to a Domain Controller in the identified
>> Domain to do the authentication.
>>
>> When the Log on to: box is set to the local Computer name, the local
>> computer will attempt to authenticate the user against its own, local
>> security "database". Domain user accounts can NEVER be authenticated in
>> this situation.
>>
>> This is true even when the Domain User Account is specifically a member
>> of a
>> Local Group on the computer. I guess this is where I don't understand
>> your
>> item # 2.
>>
>> The only way a user can logon using a non-Domain user account is if there
>> is

Re: how to create domain policy to restrict users ???

>> in fact a non-Domain user account defined on that computer. So, if you
>> don't want users to use local computer accounts, don't create any on the
>> workstation computers. Also, don't add the Domain User account (or a
>> Domain
>> Group that the user is a member of) to the local Administrators group –
>> such
>> a use could create their own Local account.
>>
>> If, on a workstation computer you use Computer Management, System Tools,
>> Local User and Groups, Users and ADD a user account, this is a Local user
>> account even if the username is identical to the username of a Domain
>> User
>> account. You really don't want to do this because it will be confusing –
>> you have two completely independent user accounts with the same name. If
>> you have this situation, change the password on either the Local user
>> account or the Domain account so that they are different. Then, you can
>> verify that the Domain user account only works when the Domain Name is
>> selected in the Log on to: box and the Local user account only works when
>> the Computer Name is so selected.
>>
>> In most cases, there is no need and it is undesirable to have individual
>> Domain User accounts as members in Local Groups on computers. Usually,
>> one
>> would use a Group from the Domain rather than individual user accounts.
>>
>> With a GPO, you can control which User Accounts can actually log on at a
>> given computer. There are two related settings, both in Computer
>> Configuration, Windows Settings Security Settings, Local Policies, User
>> Rights Assignment. These settings are:
>>
>> Allow log on locally
>> Deny log on locally
>>
>> If you Enable Allow log on locally, you must specify all the groups (or
>> individual user accounts) that you want to have this right – all other
>> accounts won't be able to log on.
>>
>> If you Enable Deny log on locally, you can specify that specific user
>> accounts or groups that are to be Denied this right. If a given user
>> account
>> (possibly by virtue of Group membership) is in both the "Allow" and
>> "Deny"
>> lists, the Deny takes precedence.
>>
>> Normally, you would put Domain User accounts or Groups in these settings.
>> However, you can but unqualified names in them. Then, if a Local User
>> account's username matches that unqualified name, that Local User account
>> will be denied local logon. There is no way that I know of to specify
>> Local
>> Group names or "all Local User Accounts".
>>

Re: how to create domain policy to restrict users ???

Re: how to create domain policy to restrict users ???

>> An explanation of these settings is available in the Group Policy
>> Editor's
>> Help (Help, Help Topics, Security Settings, Concepts, Security Settings
>> Description, Local Policies, User Rights Assignment).
>>
>> Be very careful with these because you can end up preventing anyone,
>> including Administrators from logging on at all!
>>
>> But, only user accounts that are members (directly or
>> indirectly) of the Administrators group on the computer can create Local
>> User accounts or adjust the membership of Local groups. So, if you don't
>> make users Administrators on the workstations, they can't create Local
>> User
>> accounts and thus you have prevented them from logging on using Local
>> User
>> accounts (unless they know the password of the Local Administrator user
>> account!) without any GPO at all. This is the usual approach.
>>
>> --
>> Bruce Sanderson MVP Printing
>> <http://members.shaw.ca/bsanders>
>>
>> It is perfectly useless to know the right answer to the wrong question.
>>
>>
>>
>> "Kresna Rudy K" <KresnaRudyK@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
>> news:A73FBECD-9331-45DA-836D-13D44B2E6DDF@xxxxxxxxxxxxxxxxxxxx
>> > Hi Bruce,
>> >
>> > Thanks for your answer...
>> >
>> > For item no 2, I explain to you the situation, I create user account in
>> > domain controller and I put it in local group, now user have 2 option
>> > (after
>> > users restart their pcs),
>> > user can login local (this computer) or login to domain controller (eg
>> > WINDC).
>> >
>> > I don't want users to login local (this computer), they must login to
>> > domain
>> >
>> > Is it possible ???
>> >
>> > Regards,
>> >
>> >
>> > "Bruce Sanderson" wrote:
>> >
>> >> You can use the Restricted Groups policy (Computer Configuration,
>> >> Windows

Re: how to create domain policy to restrict users ???

Re: how to create domain policy to restrict users ???

>>> Settings, Security Settings, Restricted Groups) to set local group
>>> membership on workstations (see
>>> <http://support.microsoft.com/?id=810076>).
>>> User accounts that are only members of the Local Users group can not
>>> "install" software.
>>>
>>> Unless a user's account is a member of one of the Local Groups (e.g.
>>> Administrators, Power Users, Users), they won't be able to logon
>>> locally.
>>> If a user can not logon locally, they won't be able to use their
>>> workstation
>>> at all, so I don't quite understand what you are attempting to
>>> accomplish
>>> with your item 2. By default, the Domain Group "Domain Users" is
>>> added
>>> to
>>> the Local Group called "Users" on Windows XP computers, but you can
>>> remove
>>> the Domain Users group if you want. By default ordinary "Users" can
>>> not
>>> logon to Domain Controllers locally.
>>>
>>> --
>>> Bruce Sanderson MVP Printing
>>> <http://members.shaw.ca/bsanders>
>>>
>>> It is perfectly useless to know the right answer to the wrong
>>> question.
>>>
>>>
>>>
>>> "Kresna Rudy K" <KresnaRudyK@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
>>> message
>>> <news:5005BA04-26EF-4DC0-917D-4EDC4B53FC93@xxxxxxxxxxxxxxxxxxxx>
>>> > Hi,
>>> >
>>> > I have win2003 as domain controller and 100 pc with win XP.
>>> >
>>> > My questions are :
>>> >
>>> > 1 : How to create domain policy to prevent users to install software
>>> > ?
>>> > (ofcourse only admin can install new software)
>>> > 2 : How to create domain policy to prevent users to login locally ?
>>> > 3 : Is it possible to disable floppydisk and cdrom via domain policy
>>> > ?
>>> >
>>> > please help
>>> >
>>> > Thanks...
>>> >

Re: how to create domain policy to restrict users ???

>> >>
>> >>
>> >>
>>
>>
>>
>>

• *Follow-Ups:*

◆ [Re: how to create domain policy to restrict users ???](#)

◇ *From:* Kresna Rudy K

• Prev by Date: [RE: GPMC SP!](#)

• Next by Date: [Runas causes application freeze](#)

• Previous by thread: [Re: how to create domain policy to restrict users ???](#)

• Next by thread: [Re: how to create domain policy to restrict users ???](#)

• Index(es):

◆ [Date](#)

◆ [Thread](#)