

## Forum:[Hack Forums](#)

Thread: [How&To Gain Admin Access on a Limited Account. \(Admin At School\)](#)

?lixir - October 1, 2013, 6:12 pm

- 1) Use this method on your own equipment.
- 2) I am not responsible for your actions.
- 3) This only has been tested on XP and will only work with a domain.

Alright heres how to do it. First find a computer you have never logged into.

Log into it, and as its loading it will say "Applying account settings", or "Applying desktop settings" something like that.

Unplug the ethernet cable from the back.

BOOM you're an offline admin.

Make all your changes and what not. As soon as you plug the cable back in, you will become limited again.

Found this out back in middle school (year 6 for you non americants).

Now impress your friends and stop making these threads.

Aura - October 1, 2013, 6:16 pm

- (Oct 1, 2013 06:12 PM)Dr. Caspers Wrote: [\[CITE\]](#) 1) Use this method on your own equipment.  
2) I am not responsible for your actions.  
3) This only has been tested on XP and will only work with a domain.

Alright heres how to do it. First find a computer you have never logged into.

Log into it, and as its loading it will say "Applying account settings", or "Applying desktop settings" something like that.

Unplug the ethernet cable from the back.

BOOM you're an offline admin.

Make all your changes and what not. As soon as you plug the cable back in, you will become limited again.

Found this out back in middle school (year 6 for you non americants).

Now impress your friends and stop making these threads.

Will this also bypass the GPO's that are in effect on the account you're using ?

Let's say I'm a limited user and I use your trick and become an offline Admin. Also let's say the Registry and disabled via a GPO. Will I be able to open it anyway and bypass that GPO or so I still stay a "limited admin" user ?

?lixir - October 1, 2013, 6:19 pm

(Oct 1, 2013 06:16 PM)Aura. Wrote: [\[CITE\]](#) GPOaccount

A GPO? As in the software network admins/teachers use to govern the students? Kind of like a RAT?

If so, yes. It will not be able to establish the original connection and set the correct settings.

**Aura** - October 1, 2013, 6:27 pm

(Oct 1, 2013 06:19 PM)Dr. Caspers Wrote: [\[CITE\]](#) A GPO? As in the software network admins/teachers use to govern the students? Kind of like a RAT?

If so, yes. It will not be able to establish the original connection and set the correct settings.  
No, GPO in the sense of Group Policy Objects.

You can see it as permissions you can create and manage and you then apply them on : groups, users, computers, etc.

As an exemple, you can create a GPO that when applied on a user, will grant him a full Internet access when in the other hand, regular users have a limited Internet access (no access to Youtube, Facebook, etc.)

But what if the GPOs are directly linked to the user account and not the computer, will they still be in effect ?

**?lixir** - October 1, 2013, 6:42 pm

(Oct 1, 2013 06:27 PM)Aura. Wrote: [\[CITE\]](#) No, GPO in the sense of Group Policy Objects.

You can see it as permissions you can create and manage and you then apply them on : groups, users, computers, etc.

As an exemple, you can create a GPO that when applied on a user, will grant him a full Internet access when in the other hand, regular users have a limited Internet access (no access to Youtube, Facebook, etc.)

But what if the GPOs are directly linked to the user account and not the computer, will they still be in effect ?

No, since the account cannot pull the GPO from the domain, they are not set. But they have to use a computer that has not be logged into before. Otherwise the GPO will be in effect most certainly.

**Aura** - October 1, 2013, 6:45 pm

(Oct 1, 2013 06:42 PM)Dr. Caspers Wrote: [\[CITE\]](#) No, since the account cannot pull the GPO from the domain, they are not set. But they have to use a computer that has not be logged into before. Otherwise the GPO will be in effect most certainly.

If we delete the profile of the user and then try to connect, it will act as if it was the first time it connects, correct ? Then will it work or are the GPOs still be in a cache somewhere on the computer ?

Sorry I'm asking alot of question but I just want to see how well this method works. So far, it looks promising.

**Nyan HF** - October 1, 2013, 6:46 pm

Wow this is a great thread man. This. Wow.

This has opened up many ideas, thank you again (:

**?lixir** - October 1, 2013, 6:47 pm

(Oct 1, 2013 06:45 PM)Aura. Wrote: [\[CITE\]](#) If we delete the profile of the user and then try to connect, it will act as if it was the first time it connects, correct ? Then will it work or are the GPOs still be in a cache somewhere on the computer ?

Sorry I'm asking alot of question but I just want to see how well this method works. So far, it looks promising.

That might work. I never had to delete profiles mainly because of my school being stocked with computers. To find more answers, you'll have to do some infield studies ;P Fully funded by your school of course lol.

**HellaCrow** - October 1, 2013, 6:49 pm

I may try, thanks you for the info.

**Aura** - October 1, 2013, 6:50 pm

(Oct 1, 2013 06:47 PM)Dr. Caspers Wrote: [\[CITE\]](#) That might work. I never had to delete profiles mainly because of my school being stocked with computers. To find more answers, you'll have to do some infield studies ;P Fully funded by your school of course lol.

I was thinking of trying it at work to be honest :P

I'll just put a Windows XP image on a test desktop or laptop and test it and I'll comeback to you probably tomorrow evening with the results !

**CryptoExchanger** - October 1, 2013, 6:51 pm

1) not responsible for anything you do

Now get a usb linux liveboot.

mount the windows partition and cd to C:\Windows\System32

replace sethc.exe with cmd.exe

log back into windows and press shift 5 times at login screen

a cmd screen will come up with admin rights, just net localgroup your way in

**?lixir** - October 1, 2013, 6:53 pm

(Oct 1, 2013 06:50 PM)Aura. Wrote: [\[CITE\]](#) I was thinking of trying it at work to be honest :P

I'll just put a Windows XP image on a test desktop or laptop and test it and I'll comeback to you probably tomorrow evening with the results !

You wont have to if your work is using windows. This is a design flaw, and i doubt they fixed this.

(Oct 1, 2013 06:51 PM)bananamango Wrote: [\[CITE\]](#) 1) not responsible for anything you do

Now get a usb linux liveboot.

mount the windows partition and cd to C:\Windows\System32

replace sethc.exe with cmd.exe

log back into windows and press shift 5 times at login screen

a cmd screen will come up with admin rights, just net localgroup your way in

Most Network Admins set a bios password.

**Aura** - October 1, 2013, 6:54 pm

(Oct 1, 2013 06:53 PM)Dr. Caspers Wrote: [\[CITE\]](#) You wont have to if your work is using windows. This is a design flaw, and i doubt they fixed this.

Yeah probably.

I just want to know if the method works if your profile is already created on the computer and you delete it.

I just want to do it for personnal knowledge ! And I'll share you the result.

**CryptoExchanger** - October 1, 2013, 6:58 pm

Quote: Most Network Admins set a bios password.

I know a lot of schools, including mine, don't use bios passwords, as updating all the schools computers would take forever for one person. Probably other reasons to.

**?lixir** - October 1, 2013, 6:59 pm

(Oct 1, 2013 06:58 PM)bananamango Wrote: [\[CITE\]](#) I know a lot of schools, including mine, don't use bios passwords, as updating all the schools computers would take forever for one person. Probably other reasons to.

They wouldn't need to update one by one. Just a simple network update....

If they do not have a bios password, than use your method.

**CryptoExchanger** - October 1, 2013, 7:01 pm

Of course, multiple working ways are always helpful. Good-luck.

**tony6r** - October 1, 2013, 11:50 pm

Thats impressive, but the whole point of being an admin in my case scenario would be to install stuff. LoL

**?lixir** - October 2, 2013, 7:54 am

(Oct 1, 2013 11:50 PM)tony6r Wrote: [\[CITE\]](#) Thats impressive, but the whole point of being an admin in my case scenario would be to install stuff. LoL You can install software with this method.

**OfficialShOtzz** - October 21, 2016, 6:02 am

(Oct 1, 2013 06:45 PM)Aur? Wrote: [\[CITE\]](#) If we delete the profile of the user and then try to connect, it will act as if it was the first time it connects, correct ? Then will it work or are the GPOs still be in a cache somewhere on the computer ?

Sorry I'm asking alot of question but I just want to see how well this method works. So far, it looks promising.

(Sorry for bringing this back)

So basically here is the position I am in.

My school has almost every aspect of the internet blocked, and I just gave up trying to directly bypass it. I have the IP address to login to the administrative panel for the iBoss Secure Web Gateway. But i have yet to find a username that works and along with that a password.

Right now i just use TOR that i have on a USB, and that is fine, but I really want to find a way to get into the iBoss panel.

Any suggestions??

**joshpetersman1960** - November 14, 2016, 2:20 pm

How can I make myself a permanent admin just so I can use cmd to make another account with admin and turn mine off?

**jarringleech74** - November 14, 2016, 9:17 pm

I already know this could get you expelled, but is this against the law?

**ReaperOfSoul** - November 15, 2016, 11:29 am

hmm, didnt work for me at school. My school must have a different system in place :(