

Forum:[Hack Forums](#)

Thread: [Getting around Symantec \(blech\)](#)

Electricdwarf - October 15, 2014, 6:03 pm

Some history I am going to school for programming and I had to purchase a laptop from the school. It is a decent computer yet there a few problems. I shall list them... now!

1. I am an administrator user, yet I am still blocked out of some features such as editing registry files and deleting certain files already on the computer.
2. They have installed Symantec Endpoint Protection and I cannot delete it for there is a password on the uninstall process. If I try to go into the C drive and delete the files manually SYSTEM tells me that I do not have permissions to do so.
3. I have tried every possible way that I as an unenlightened user could try to get around Symantec.
4. I am trying all of this so I can add an exception to Symantec and I cannot do to it all being locked by my schools IT department, and I doubt they will accept a request to add an exception to a steam_api.dll file so I can play a pirated game. ?

So are there any unsavory ways to get around this? I am resting all of my hopes in the hands of generous and kind hackers such as yourselves. Thank you for your time and have a good day/night!

Sharjah - October 15, 2014, 10:08 pm

why do you want to remove the anti-virus?

Electricdwarf - October 15, 2014, 10:53 pm

The SYSTEM admin (school) has placed it on my computer and it is calling false positives on .dll files that come with cracks for torrented files. Therefor I must remove the SYSTEM admin OR Symantec from my computer, either way leads to the same result. I am not able to access the exceptions menu due to the admin on Symantec (it has a password so I am stuck there) Can I brute force the symantec or will symantec stop it? If I can where do a begin? I payed 1500 dollars for this laptop and those damn school workers have blocked all but what they deem "essential" on here. I am just trying to access what is mine.

There is a SYSTEM admin that isnt visible in the Users in Control Panel that has access to all of these issues, if I can access that I can have full control of my laptop.

Arrandale - October 16, 2014, 12:28 am

You payed for the laptop and no full control of the system? -_- You must be mad bro... How about dual os bro?

--Still learning bro!

Sechs - October 16, 2014, 1:24 am

Removing SYSTEM is a very good idea for afterwards, you'll have to install from scratch. No more AV.

Seriously though, don't try to remove it. If you want to get rid of the AV, get a linux live-cd such as ubuntu, mint or similar. Linux doesn't respect Windows file- or security-permissions, so you're free to change anything you want. It's not the most comfortable way, but it'll work.

However, before actually doing this, read up on the school's terms of service or whatever they call it. There might very well be some paragraph that bans you from doing this and still doing it (and having them find out later) will probably get you in a much more dire position than not being able to play some pirated game.

There's always an option for a separate install. Consider that, too.

Cybride - October 16, 2014, 5:36 am

Quote:Anyway, if you are in a similar situation where you don't know the password to uninstall Endpoint Protection, then you'll be happy to know of a quick way to bypass the password and still uninstall the program.

When the password prompt comes up, go into Task Manager by pressing CTRL + ALT + DEL and choosing Task Manager, then click on the Processes tab. Now find the msixec.exe process and kill it!

Once you kill the process, the password prompt disappears and the uninstall continues!!

<http://helpdeskgeek.com/help-desk/uninstall-symantec-endpoint-protection-without-a-password/>

I wonder if this still works... wouldn't surprise me.

Another benefit of this is it's plausible deniability - not so easy with dual boot.

The downside however is, that this might only be one of multiple backdoors on your system.

Oh, and just asking your IT staff to disable it might also work.

Another guide tells you to simply stop the service...

<http://dottech.org/110272/how-to-stop-symantec-endpoint-protection-from-running-on-windows-guide/>