

Forum:[Hack Forums](#)

Thread: [Using TrueCrypt for full disk encryption on windows](#)

Spolen - August 24, 2011, 2:57 pm

I don't currently have all of the screenshots because my computer is fucked and certain software wont work, but as soon as I get all of the screen shots for this I will update this with them.

if you don't understand something in this tutorial, or you see inconsistencies in the tutorial, or anything is wrong at all, let me know and i will do my damndest to clarify.

This is the very first tutorial I have ever written so please be kind, I'm not the best with explaining things.

In this tutorial I am going to be assuming a few things here:

1. I assume you are not running multiple operating systems side by side.

and

2. I assume that you are running windows (I've never used truecrypt on Linux or Os x yet.).

Step 1. Install TrueCrypt

A) Go to <http://www.truecrypt.org>

B) Click on "Downloads" in the menu at the top of the screen

C) Scroll down to find the "Latest Stable Version"

D) Find the "Download" button for Windows

D) Click the "Download" button

E) Click "Run" on the dialog box that appears, if it doesn't say "Run" then save it and run it
afterword

F) Check the box to accept the terms, and then click the accept button

[\[IMG\]http://img834.imageshack.us/img834/9203/tcaccept.th.jpg](http://img834.imageshack.us/img834/9203/tcaccept.th.jpg)[\[IMG\]](#)

G) Make sure the install option is selected and click "Next"

[\[IMG\]http://img843.imageshack.us/img843/59/tcinstall1.th.jpg](http://img843.imageshack.us/img843/59/tcinstall1.th.jpg)[\[IMG\]](#)

H) Make sure you at least associate .tc extension with TrueCrypt then click "Install"

[\[IMG\]http://img855.imageshack.us/img855/2367/tcinstall2.th.jpg](http://img855.imageshack.us/img855/2367/tcinstall2.th.jpg)[\[IMG\]](#)

I) After installation is complete it will ask you if you want to view the tutorial, I recommend reading it because it will cover topics that this tutorial Wont

Step 2. Encrypt your hard drive

A) Open TrueCrypt

[\[IMG\]http://img69.imageshack.us/img69/7501/tcfirstrun.th.jpg](http://img69.imageshack.us/img69/7501/tcfirstrun.th.jpg)[\[IMG\]](#)

B) Click the system menu at the top of the truecrypt menu and go to "Encrypt System"

Partition/Drive"

C) A screen should popup now with two options make sure that the option for Normal is selected and click next

D) check the button to encrypt the whole drive and click next

E) it should now ask if you want to encrypt the host protected area, to be safe click no, and then click next

F) Check the radio button for single-boot and click next

G) Now it will come up with the "Encryption Options" make the encryption algorithm AES and the hash algorithm RIPEMD-160, it should be these by default, click next

H) Now it asks you to create a password, make sure you write it down to memorize it and then destroy the paper after memorizing, the password should contain 20 or more characters upper case lower case numbers and special characters, after creating the password click next

I) on the next screen just randomly move your mouse around the window for a little bit and then click next.

J) Click Next on the Keys Generated screen

K) its gonna have you create a rescue disc now, choose where to save the ISO, after finding a good spot click next

L) now it wants you to burn the disc, which i recommend doing, but if you don't want to burn the disc, which is a bad idea in the first place, you can mount the image using alcohol 120. (you can download a trial at <http://www.alcohol-soft.com>)

M) Once you burn the rescue disc put it in you're disc drive and click next

N) it should now tell you that the disc was verified, click next

O) Now comes my favorite part, choosing the wipe mode the higher the wipe mode the harder it is to recover your overwritten data, but also the higher the wipe mode the slower it takes to encrypt, I'd recommend using either 3 or 7 pass even though i use 35. click next

P) now you should see a message confirming what i just said about it taking longer the higher the wipe mode, click yes if you wanna stick with the wipe mode you chose, otherwise click no and re choose

Q) now its gonna want to run a system encryption pretest, bookmark this page now because its gonna restart your computer, now click test and it will popup a screen with important notes that you can print, if you have a printer print this now, after printing click OK now its gonna tell you to restart your computer, make sure you save everything you need to, and bookmark this tutorial so you can come back to it after you restart your pc. before you restart I'm gonna tell you something, when your computer restarts its gonna ask for your password, just enter the password you made in section H of step 2, now click yes to restart.

R) Welcome back, I'm gonna assume the test completed successfully, if so you will have a TrueCrypt window up that says Pretest Completed when you have enough time where you wont need to use the computer for a while click on Encrypt. if you can print the screen that pops up next then click ok. Now it should start encrypting, don't worry if you need to use the computer while its still encrypting, just click on Pause and then when you're done click Resume and it continues encrypting.

S) After it successfully completes, click on finish and you're done.

D3vildog - August 25, 2011, 6:20 pm

So after it is done, is it just the regular windows login, but if you put in your long ass password it boots the secret OS with secret data partition?

Spolen - August 25, 2011, 9:12 pm

(Aug 25, 2011 06:20 PM)D3vildog Wrote: [\[CITE\]](#) So after it is done, is it just the regular windows login, but if you put in your long ass password it boots the secret OS with secret data partition?After its all encrypted, when you boot up your PC, it loads the truecrypt boot loader,

[IMG]<http://img856.imageshack.us/img856/2898/8atruecryptbootloader.th.png>[/IMG]

If you set it up with the hidden OS, then the hidden OS has a separate password of its own, so you have a password for the regular OS, and a password for the hidden OS, they have it setup that way in case someone forces you to put your password in, you can just put in the regular password, and your hidden OS is still encrypted and all of your sensitive data on the hidden OS is safe, and they're none the wiser.

Rs ice - August 25, 2011, 9:19 pm

Thank for the tut, I'll try it I guess even though I'll prolly forget the pass

Spolen - August 25, 2011, 9:25 pm

(Aug 25, 2011 09:19 PM)Rs ice Wrote: [\[CITE\]](#) Thank for the tut, I'll try it I guess even though I'll prolly forget the pass

The password can be what ever you want, but they recommend 20 or more characters,

check out <http://www.passwordcard.org> that should help you remember your password

D3vildog - August 27, 2011, 12:51 pm

I wish you could mod the windows login so that it would do that, could I mod the program so instead of trucrpyt boot loader it says Windows Safe Mode Boot or something.

Spolen - August 27, 2011, 4:26 pm

(Aug 27, 2011 12:51 PM)D3vildog Wrote: [\[CITE\]](#) I wish you could mod the windows login so that it would do that, could I mod the program so instead of trucrpyt boot loader it says Windows Safe Mode Boot or something.

Once you encrypt the drive, go to the truecrypt system menu and click on settings, click the very top check box

[IMG]<http://img594.imageshack.us/img594/5489/tccustommessage.th.jpg>[/IMG]

and the text box underneath is where you put the message you want it to say when it boots up.

The message you put replaces the boot loader, when you see your message when you boot up type your password and hit enter.

sexynsmartjenny - September 18, 2011, 10:07 am

hi i am thinkiing about using truecrypt to encrypt by entire disk, but i was worried that this might slow down my computer performance since every time an data is moved, it has to decrypt and encrypt "on the fly". is there any issues anyone has witj using truecrypt. sorry it's too cold in my apartr5ment my hands are freezing and couldn't type

Spolen - September 20, 2011, 4:47 am

No there is no change in performance. I've used TrueCrypt for I believe close to two years now and there's no difference in the computers speed.

PS: Sorry for not replying sooner, I didn't realize this thread had new posts.

Spolen - October 8, 2011, 6:58 pm

If any one else needs any help, don't hesitate to ask.

Neurohazed - October 11, 2011, 6:51 pm

Can I do it with Linux and Windows simultaneously encrypting both?

Something like, first the truecrypt bootscreen and then someother bootloader like GRUB.

Spolen - October 12, 2011, 10:59 am

If you have windows and linux on two separate partitions, then you can encrypt the windows partition but according to their online documentation located at <http://www.truecrypt.org/docs/?s=system-encryption> you can only encrypt a windows operating system.

1) If you want to encrypt the windows partition separately and leave the Linux OS unencrypted you'll have to click on the system drop down menu on the TrueCrypt main window, and click on "Encrypt System Partition/Drive" Spoiler [\(Click to View\)](#)


2) Then it will ask what type of encryption you want, choose normal and click next. Spoiler [\(Click to View\)](#)


3) On the next screen make sure to check the partition encryption, not the whole drive
Spoiler [\(Click to View\)](#)


4) the next screen asks about how many operating systems are on your computer, since you have windows and Linux select multi-boot.
Spoiler [\(Click to View\)](#)


If you want to just encrypt the whole drive so both operating systems are encrypted at once refer to the spoiler in section 3 of this post and click on "encrypt the whole drive" and on the next screen it should ask about the host protected area, choose not to encrypt the host protected area. on the next screen select multi-boot. I personally have never encrypted the whole drive with multiple operating systems installed, so I cant say that encrypting the whole drive if you have windows and Linux will be safe, so I don't recommend it.

If you have any other questions let me know.

koda-coder - October 13, 2011, 5:45 am

thanks for help mate

nice tut thx bro really helped me out lol

integer - October 13, 2011, 9:54 am

There is a performance drop for encrypting your disk for older computers. You may not notice it on a good machine, but it does add extra load on your system.

Spolen - October 13, 2011, 1:57 pm

(Oct 13, 2011 05:45 AM)koda-coder Wrote: [\[CITE\]](#) thanks for help mate
nice tut thx bro really helped me out lol
No problem, I'm glad I could help.

(Oct 13, 2011 09:54 AM)matt Wrote: [\[CITE\]](#) There is a performance drop for encrypting your disk for older computers. You may not notice it on a good machine, but it does add extra load on your system.

You are right, but as long as you have at least a gigabyte of ram and a decent CPU you should be fine, it'll just take a little while to encrypt.

Spaz75 - June 1, 2014, 3:51 am

Thank you very much for the tutorial ;)

Arkamek - June 2, 2014, 10:02 am

Thank you very much for that work :)

mdavis12 - June 2, 2014, 10:26 am

i thought this project was discontinued recently due to "security concerns". i'd find another solution to encrypting sensitive data.

cyb3rc0de - June 5, 2014, 7:33 am

(Jun 2, 2014 10:26 AM)mdavis12 Wrote: [\[CITE\]](#) i thought this project was discontinued recently due to "security concerns". i'd find another solution to encrypting sensitive data.

No, its quite alive. Main developer got fed up from coding it. But since its open source its still viable :)

You can check dev progress on truecrypt.ch or truecrypt71a.com

SmokeyBluntson - June 5, 2014, 7:52 am

Hasn't truecrypt been compromised and currently useless, discontinued, and un-funded lol

Hexley - June 5, 2014, 7:53 am

Very nice thread and easy to follow; off topic: isn't truecrypt ending?

cyb3rc0de - June 5, 2014, 7:58 am

(Jun 5, 2014 07:53 AM)Hexley Wrote: [\[CITE\]](#) Very nice thread and easy to follow; off topic: isn't truecrypt ending?

Actually, main developer quit development. His project is still working perfectly fine and "software is vulnerable" is false info.

truecrypt.ch is about to fork it and continue development :D Don't worry, project is far away from dead ;)

Talu - June 5, 2014, 8:37 am

Yeah, I don't think this tut is relevant anymore.