**TrueCrypt**

**TrueCrypt Drive Encryption Software Overview**

TrueCrypt is an open source drive and partition encryption tool. Vanderbilt University Medical Center recommends utilizing TrueCrypt for full disk encryption when use of the enterprise solution (PointSec Full Disk Encryption and PointSec Protector) is not possible.

The TrueCrypt software is available at [http://www.truecrypt.org](http://www.truecrypt.org).

TrueCrypt can currently encrypt the following operating systems:

- Windows Vista
- Windows Vista x64 (64-bit) Edition
- Windows XP
- Windows XP x64 (64-bit) Edition
- Windows Server 2008
- Windows Server 2008 x64 (64-bit)
- Windows Server 2003
- Windows Server 2003 x64 (64-bit)
- Mac OS X 10.4 Tiger
- Mac OS X 10.5 Leopard
- Linux (kernel 2.4, 2.6, or compatible)

While TrueCrypt provides excellent data protection, there are several points which users should aware of:

- TrueCrypt offers no centralized key management or key escrow services. **As such, a lost or forgotten password will result in irreversible data loss.** TrueCrypt uses strong encryption algorithms, and “cracking” the encryption in the case of a forgotten password is not possible.
- TrueCrypt is not FIPS-140 certified. While TrueCrypt does use FIPS-140 compliant encryption algorithms, it has not gone through the compliance certification process. Some governmental agencies require that data be encrypted with FIPS-140 compliant encryption products.
- TrueCrypt offers only Pre-Boot Authentication. This means that there is a password that must be entered before the machine will begin booting into the operating system. If a machine is remotely restarted, it will halt at the pre-boot authentication screen until the user physically enters the password on the local keyboard.
Installing TrueCrypt

1. **Download the TrueCrypt software**
   The TrueCrypt software can be downloaded from [http://www.truecrypt.org](http://www.truecrypt.org). There is a “Downloads” menu option, and the appropriate operating system should be selected.

2. **Execute the Installer**
   Double-click the installer that was downloaded in step 1. This will begin the installation.

3. **Accept the License Agreement**
   Check the “I accept and agree to be bound by the license terms” checkbox, and click “Accept” to continue.

4. **Select the Installation Mode**
   For a standard installation, select the “Install” option and click “Next” to continue.
5. **Setup Options**
   For most users, the default setup options may be selected. Once options are selected, click “Install”.

6. **Finishing the Installation**
   TrueCrypt will install the necessary files, and will display this screen. Click on “Finish” to complete the installation.

   At this point, the TrueCrypt software is installed, but nothing is encrypted.
Configuring TrueCrypt to encrypt your hard drive

1. **Launch the TrueCrypt software**
   From the Start Menu, select All Programs, TrueCrypt. The TrueCrypt user interface will load.

2. **Select Full Disk Encryption**
   Choose the “System” menu option, then the “Encrypt System Partition/Drive” option.

3. **Select Type of System Encryption**
   For most users, “Normal” is the correct option to choose. The “Hidden” option is only used in specific circumstances if an Operating System or Partition needs to be hidden from view.

   Click “Next” to continue.
4. **Select what to encrypt**
Most users will want to select “Encrypt the whole drive”.

Click “Next” to continue.

5. **Select number of operating systems**
For most users, there is only a single operating system on each machine, so “Single-boot” will be selected.

Click “Next” to continue.

6. **Select encryption algorithm**
The recommended algorithm is AES (the US government’s Advanced Encryption Standard). The defaults are fine for most users.

Click “Next” to continue.
7. **Select password/passphrase**
   Enter and confirm the password. **It is critical that you remember this password** – failure to do so will result in complete and unrecoverable data loss.

   Click “Next” to continue.

8. **Random data collection**
   Move the mouse around the window as instructed. 10-20 seconds of movement should collect enough random data.

   Click “Next” to continue.

9. **Key Generation**
   Key generation is automatic.

   Click “Next” to continue.
10. **Rescue Disk creation**

   The Rescue Disk will serve the following purposes:
   
   - If the TrueCrypt Boot Loader screen does not appear after you start your computer (or if Windows does not boot), the TrueCrypt Boot Loader may be damaged. The TrueCrypt Rescue Disk allows you restore it and thus to regain access to your encrypted system and data (however, note that you will still have to enter the correct password).
   
   - If you repeatedly enter the correct password but TrueCrypt says that the password is incorrect, it is possible that the master key or other critical data are damaged. The TrueCrypt Rescue Disk allows you to restore them and thus to regain access to your encrypted system and data (however, note that you will still have to enter the correct password).
   
   - If the TrueCrypt Boot Loader is damaged or infected with malware, you can avoid running it by booting directly from the TrueCrypt Rescue Disk. Insert your Rescue Disk into your CD/DVD drive and then enter your password in the Rescue Disk screen.
   
   - If Windows is damaged and cannot start, the TrueCrypt Rescue Disk allows you to permanently decrypt the partition/drive before Windows starts.
   
   - Your TrueCrypt Rescue Disk contains a backup of the original content of the first drive track (made before the TrueCrypt Boot Loader was written to it) and allows you to restore it if necessary. The first track of a boot drive typically contains a system loader or boot manager.

Creating a Rescue Disk is a critical part of the process, and is not optional. TrueCrypt will not allow you to encrypt your hard drive if you do not create this rescue disk.

11. **Rescue Disk Recording**

   TrueCrypt requires that the rescue disk image be burned to a CDROM or DVD.

   A link in this window points to sources for CD/DVD recording software. Unfortunately, the Native Windows CD Recording capabilities does not provide a method for writing .iso images to CD/DVD, so a 3rd party application is required.
12. **Rescue Disk Verification**  
After the .iso image is burned to a CD or DVD, TrueCrypt will verify that the media can be properly read. After confirming the rescue disk creation, the encryption process can continue.

Click “Next” to continue.

13. **Wipe Mode**  
Select “None” – wipe mode is generally only necessary when the data on the drive is so sensitive that its loss would constitute a threat to national security.

Click “Next” to continue.

14. **Encryption Pretest**  
Before encrypting the drive, TrueCrypt performs a pre-test to ensure that there are no obvious problems. The pre-test involves a reboot.

Click “Test” to continue.
15. **Pretest Completion**

Upon completion of a successful pre-test, the system will be ready for encryption.

Before clicking on “Encrypt”, make sure that the device is attached to power (in the case of a laptop) and that it can operate uninterrupted.

Encryption speed varies greatly depending on hard drive size, processor speed, and available RAM. However, most machines should encrypt in 1-4 hours.

16. **Encryption**

Once the “Encrypt” option is selected, the system encryption will begin. TrueCrypt will show the percentage completion, and estimate the amount of remaining time until the drive is fully encrypted.

If at any time you need to shut down or stop the encryption process, you may select “Defer”, and then later resume the encryption process.

Keep in mind that the initial drive encryption is a one-time process. Once the initial encryption has been completed, all future encryption and decryption takes place dynamically without any user interaction.

*Congratulations – your hard drive is now fully encrypted with TrueCrypt!*