Encryption Validation FAQs

Note: The most current version of encryption is "***Symantec Encryption Desktop"*.** Existing Guardian Edge and Symantec "***Endpoint***" Encryption installations will no longer be supported after June 2015. These versions will need to be updated to the Symantec Encryption Desktop product. Decrypting and removing existing installations of the older software versions will be required before upgrading. All new laptops owned by the university will need to have the current version of Symantec Encryption Desktop installed.

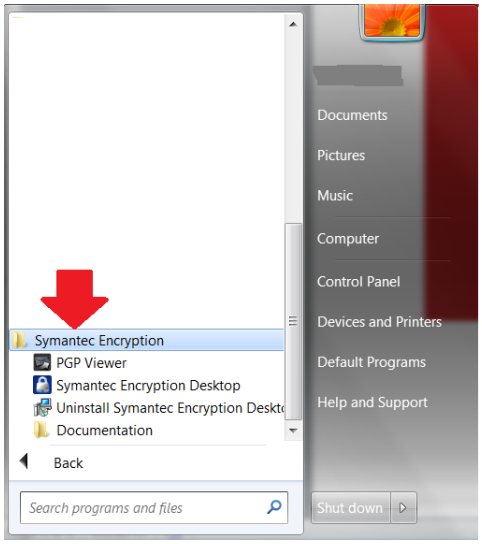
PC's and Macs:

1. **Question:** How can I tell that my Windows PC has the University's hard disk encryption solution installed?

   Answer: When you power up your machine you will see the following logo displayed, once you hit enter you will be prompted to enter your userid and password. Note: older versions of the encryption client may demonstrate the same logo but will include "alt/ctrl/del" under the cardinal bird logo.

2. **Question**: How can I tell that my computer has the University's hard disk encryption solution installed if I don't want to power off my computer?

   Answer: You can go to your programs list and you will see the Symantec Encryption client listed in the programs list on your computer (see example below). Note: It is important to note the distinction between "Symantec Endpoint Encryption and Guardian Edge (old)" and "Symantec Encryption Desktop (PGP) (new)". If you are using an older version you could see any of these terms listed in your programs list.



3. **Question:** How do I verify that encryption is installed on my Mac?

   Answer: FileVault 2 uses full disk, XTS-AES 128 encryption to help keep your data secure. Using FileVault 2, you can encrypt the contents of your entire drive. FileVault 2 is available from the Security & Privacy pane of System Preferences. Click the FileVault tab in the Security & Privacy pane to validate that FileVault is enabled.

   Information Source: http://support.apple.com/kb/ht4790

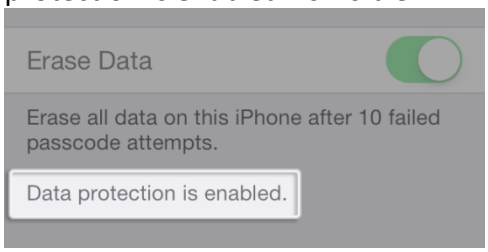
iPad and iPhones:

4. **Question**: How can I verify encryption on my iPad and iPhone?

   Answer: If you are using a Passcode on your device then the system is encrypted.

   Data protection is available for devices that offer hardware encryption, including iPhone 3GS and later, all iPad models, and iPod touch (3rd generation and later). Data protection enhances the built-in hardware encryption by protecting the hardware encryption keys with your passcode and or fingerprint. This provides an additional layer of protection for your email messages attachments, and third-party applications.

   Enable data protection by configuring a passcode for your device:
   Tap **Settings > General > Passcode**. On newer phones tab **Settings** > **Touch ID & Passcode**.
   1. Follow the prompts to create a passcode.
   2. After the passcode is set, scroll down to the bottom of the screen and verify that "Data protection is enabled" is visible.



Additional Passcode tips
Use these passcode settings to maximize passcode security:
- Set Require Passcode to Immediately.
- **Disable** “Simple Passcode” to use longer, alphanumeric passcodes.
- Enable Erase Data to automatically erase the device after ten failed passcode attempts.
- Review and disable the services listed under “allow access when locked”.
- Validate that the “Erase Data” function is enabled.

This information was obtained from the following source: http://support.apple.com/kb/HT4175

Android Devices:

5. **Question:** How do I verify that my Android device is encrypted?

   Answer: You will know that your device has been encrypted when you see the label "Encrypted" in the Security submenu, or when your device asks for your password to decrypt the storage.

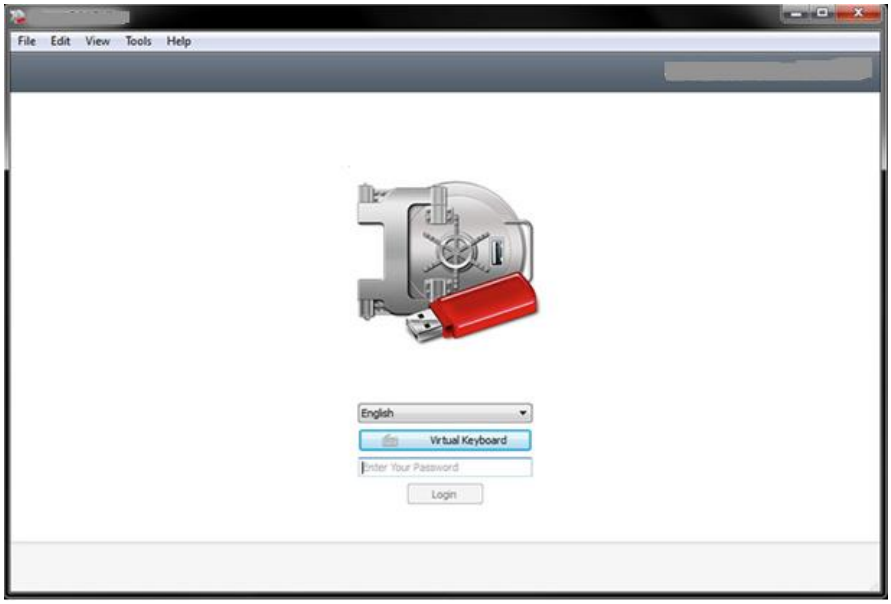
   Technical Details:
   http://source.android.com/devices/tech/encryption/index.html
   https://source.android.com/devices/tech/encryption/android_crypto_implementation.html

Other Removable Storage Devices:

6. **Question**: How do I verify that my flash drive or other removable storage device is encrypted?

   Answer: A removable storage device/USB/Flash Drive that has security enabled in it must be "unlocked" with a password or security code before it can be used.

   Example:



For further assistance please contact your Tier 1 or the IT HelpDesk at 852-7997.