Mac Symantec Encryption Desktop (PGP) Install Guide

Owen Buckvar on December 17, 2019

Symantec Encryption Desktop (PGP) for Mac is no longer available. Dell Data Protection Encryption (DDPE) will be replacing PGP for macs, please clickhere[1] for more information!

Symantec Encryption Desktop (PGP) Mac OS X system requirements

This section covers Symantec Encryption Desktop (PGP) version 10.3.1 [Build 13266]
System Requirements

- Apple Mac OS X 10.7.x, 10.8.x, 10.9.x
- Intel Processor
- 512 MB of RAM
- 64 MB hard disk space

Apple Boot Camp is **not** supported see Symantec's tech article https://support.symantec.com/business/support/index?page=content&id=TECH212700 [2]

Software Incompatibilities with Symantec Encryption Desktop (PGP)
Symantec Encryption Desktop is incompatible with other disk encryption software. Decrypt and if applicable remove the other encryption software before installing Symantec Encryption Desktop.

- Apple FileVault 2
- CheckPoint FDE

PGP WDE Supported Disk Types
The PGP WDE feature protects the contents of the following types of disks:

- Desktop or laptop disks, including solid-state drives
- External disks, excluding music devices and digital cameras

- USB flash disks

Do not use PGP WDE to encrypt server hardware. PGP WDE is not supported on Mac OS X Server Hardware

PGP WDE Unsupported Disk Types

- Disks formatted using the APM partition scheme
- Any type of server hardware, including RAID disk drives
- Diskettes and CD-RW/DVD-RWs

Compatible Email Client Software
Symantec Encryption Desktop (PGP) will, in most cases, work without problems with any Internet-standards-based email client that runs on Mac OS X 10.7.x, Mac OS X 10.8.x, Mac OS X 10.9.x

- Apple Mail 3.5, 4.0 Microsoft Entourage 2008 SP1
- Entourage is compatible for POP/IMAP only. "Exchange Mode" is supported when using the Entourage Scripts included with Symantec Encryption Desktop (PGP). Automatic proxying is not supported with the scripts. For more information on using the scripts, see "Integrating with Entourage 2008" in the Symantec Encryption Desktop (PGP) for Mac OS X User's Guide
- Lotus Notes 8.5.2
- Microsoft Outlook for Mac 2011

Instant Messaging Client Compatibility
Symantec Encryption Desktop (PGP) is compatible with the following instant messaging clients when encrypting AIM instant messages, file transfers, and direct connections:

- iChat 4.0, 5.0 SL
- Other instant messaging clients may work for basic instant messaging, but have not been certified for use

Anti-Virus Client Software Compatibility for Macintosh

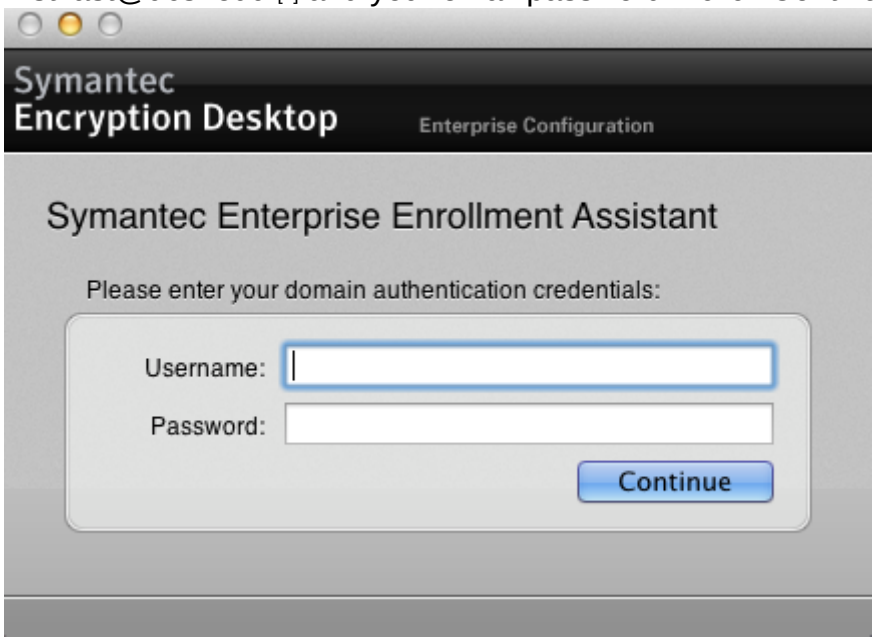
- Norton Antivirus 11 and Norton Internet Security 3.0: To use Symantec Encryption Desktop (PGP) with email and instant messaging, you must disable the Vulnerability Protection option in Norton. To do this, select Auto Protection and then disable the option for Vulnerability Protection." [18130]
- ClamXav: ClamXav is not compatible with PGP WDE on Mac OS X systems. [25682]
- VirusBarrier X6: VirusBarrier X6 is not compatible with PGP WDE on Mac OS X systems. [28849]

Install Instructions

Symantec Encryption Desktop (PGP) Mac OS X Install Guide Installation Instructions

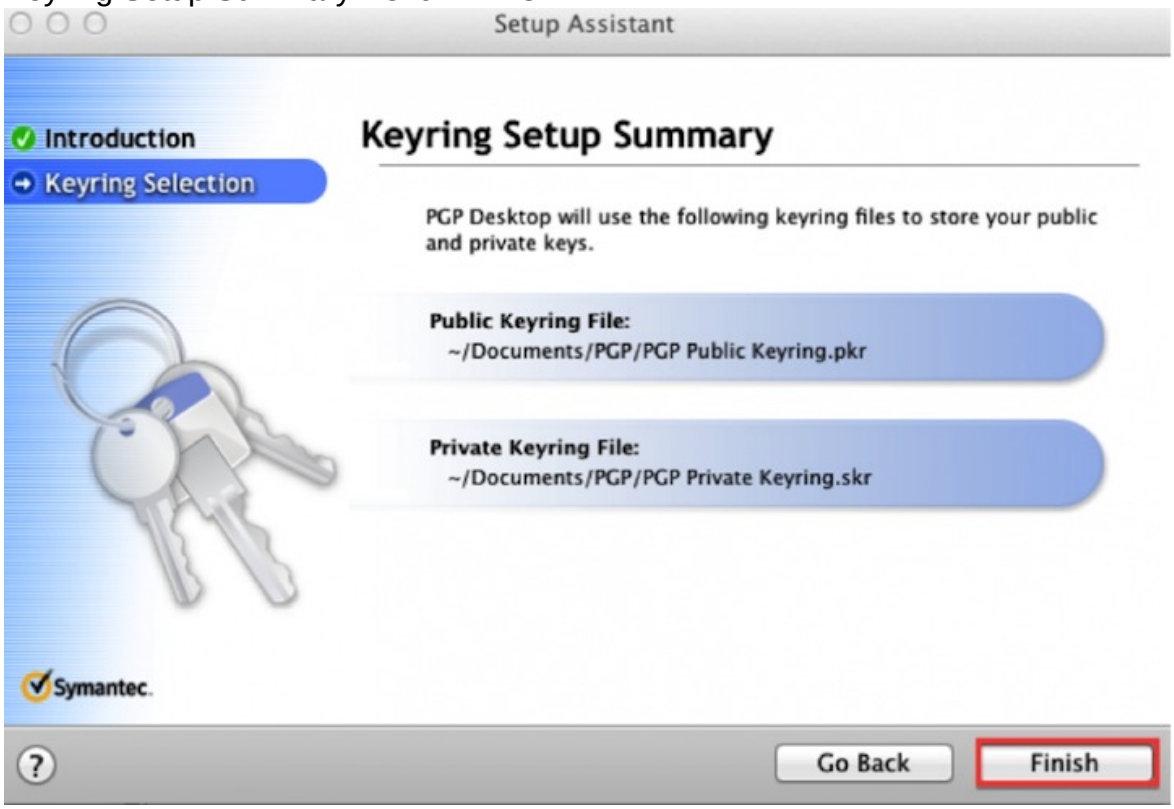
If using another disk encryption software, decrypt and if applicable remove the other encryption software before installing Symantec Encryption Desktop (PGP). Ex. FileVault, Checkpoint FDE

1. Download the client installer from http://software.ucsf.edu/applications/pgp.html [3]
2. Double click the compressed file and double click on PGP.pkg
3. Follow the on-screen instructions
4. When prompted restart the system
5. After installing Symantec Encryption Desktop (PGP) and restarting PGP Setup Assistant will launch to complete enrollment. Enter in your UCSF Email address, first.last@ucsf.edu [4] and your email password ? click Continue



6. Introduction screen ? Select "I am a new user" and click Continue

7. Keyring Setup Summary - Click "Finish"



Whole Disk Encryption Best Practices

- Determine whether your target disk is supported. PGP WDE feature protects desktop or

laptop disks (either partitions, or the entire disk), external disks, and USB flash disks
- Back up the disk before you encrypt it. Before you encrypt your disk, be sure to back it up so that you won?t lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk
- Ensure the health of the disk before you encrypt it. If PGP WDE encounters disk errors during encryption, it will pause encryption so you can repair the disk errors. However, it is more efficient to repair errors before you initiate encryption
- System meets UCSF?s minimum security standards
- Screen lock configured
- Anti Virus, Anti Spyware and software firewall
- /policies/ucsf-minimum-security-standards-electronic-information-resources [5]
- Be certain that you will have AC power for the duration of the encryption process

Setting up Whole Disk Encryption - Mac OS X

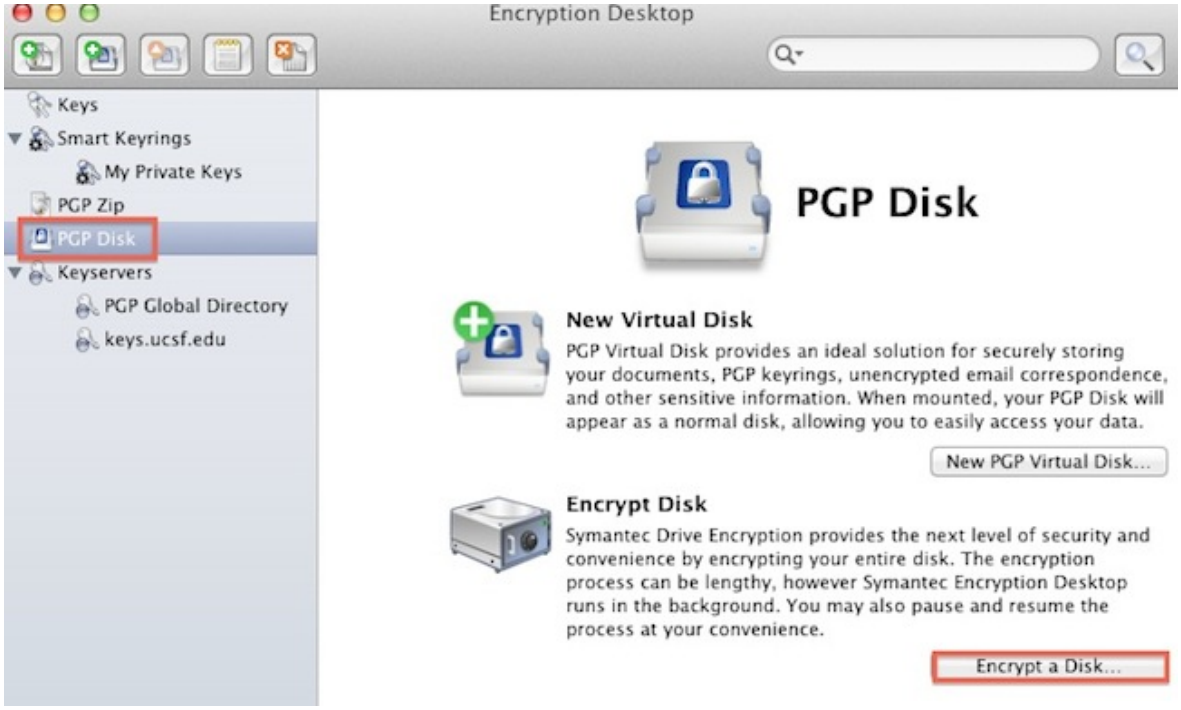
PGP WDE Warnings and Precautions

- Before encrypting review Whole Disk Encryption Best Practices
- A PGP encrypted disk must be decrypted before performing the following tasks:
    - Repartition encrypted hard drives
    - Running Boot Camp Assistant
    - Drive Recovery programs ? Disk Warrior
- Symantec Encryption Desktop (PGP) must be uninstalled before upgrading to a new operating system
    - ex. 10.7 or 10.8 to 10.9
- Do not perform a hard shut down on your Mac OS X system while Symantec Encryption Desktop (PGP) is encrypting or decrypting your disk
- Do not accept any Operating System updates while the disk is encrypting. If the update occurs automatically, do not restart your computer until the encryption process has completed
- Hibernation also called Safe Sleep is not supported with PGP WDE, when a Mac goes to sleep and runs out of battery power the Mac will shut down and not go into safe sleep. It?s important to turn off the machine if it will run out of battery power
- Running Boot Camp setup assistant or running Boot Camp on a PGP WDE drive will cause **data loss**
- Safe boot is not supported

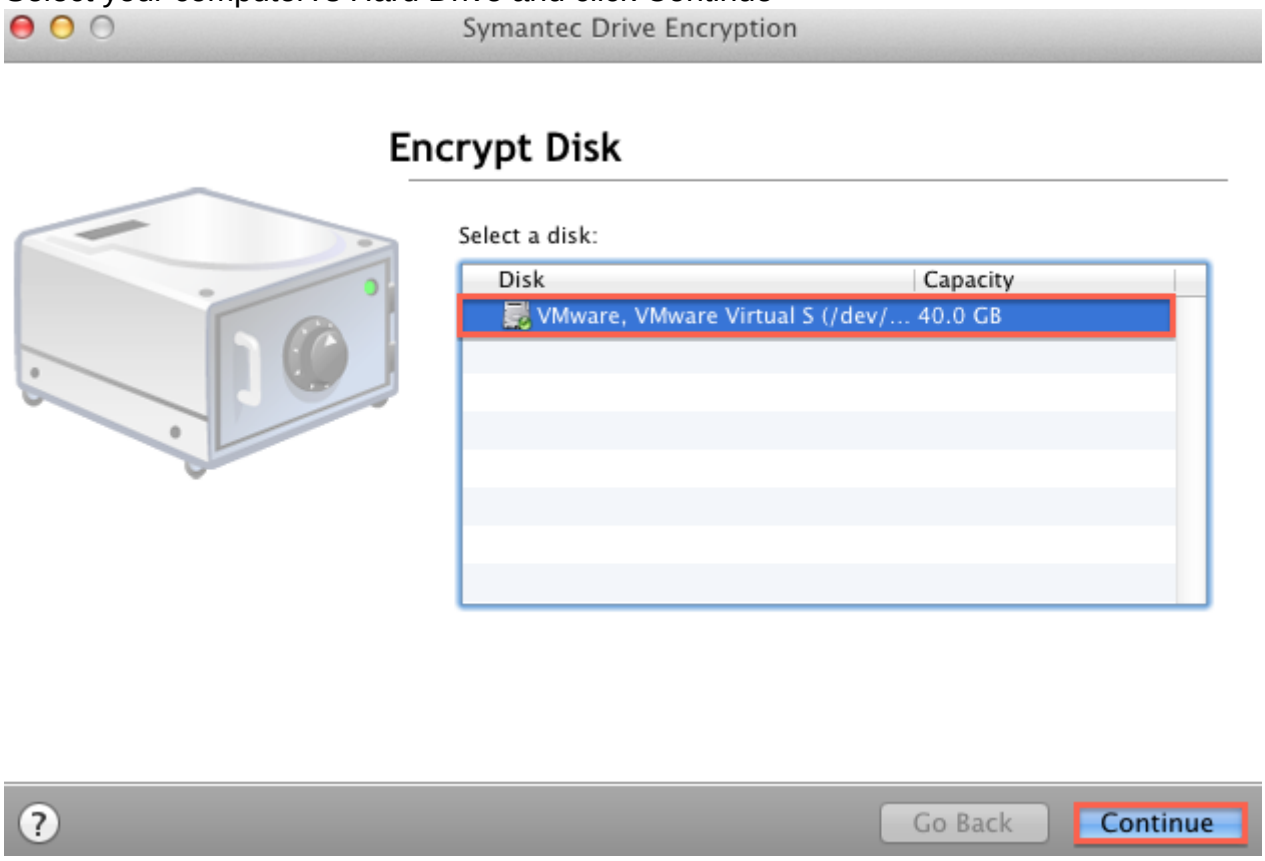
Ensure your system meets system requirements and a full backup has been made before encrypting.

1. After installing Symantec Encryption Desktop (PGP), open Applications -> Encryption Desktop

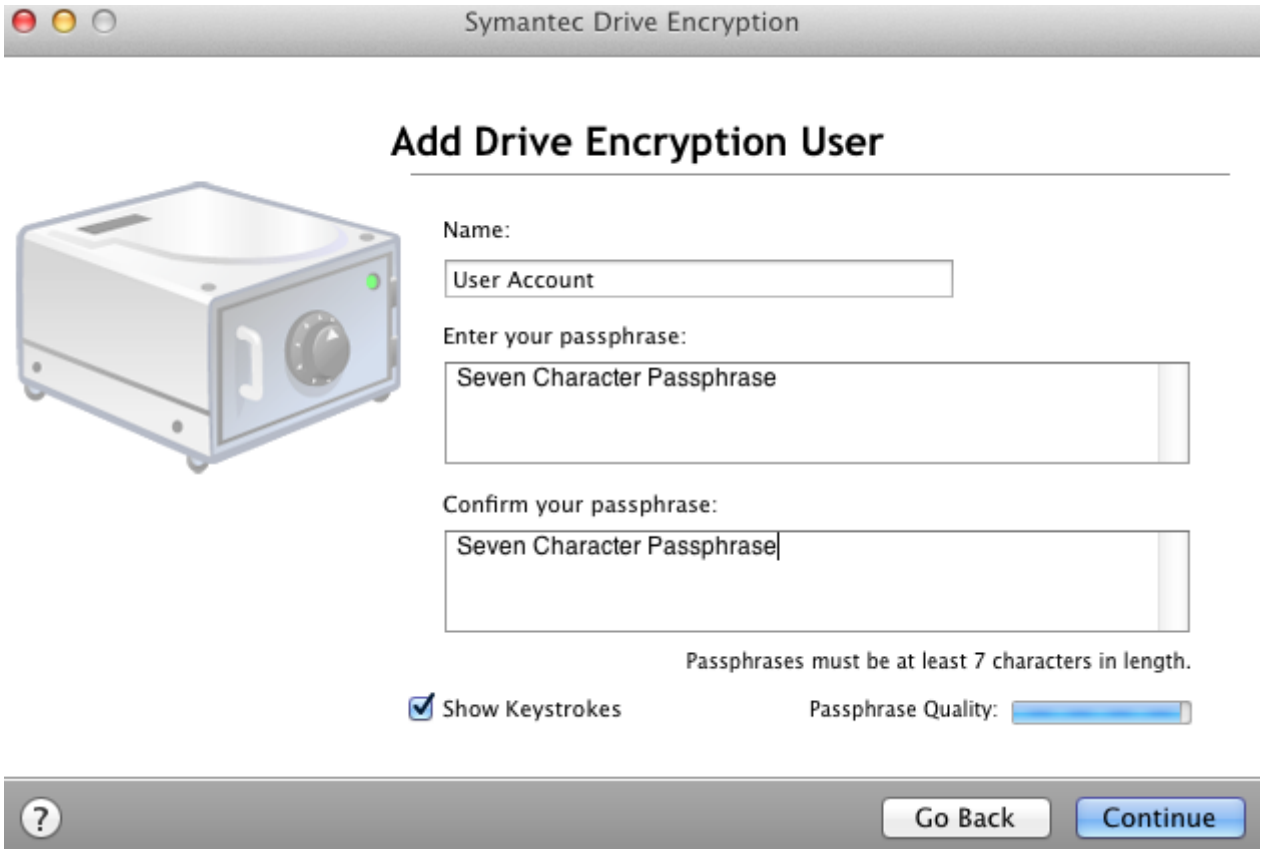
2. Click on PGP Disk then ?Encrypt a Disk?



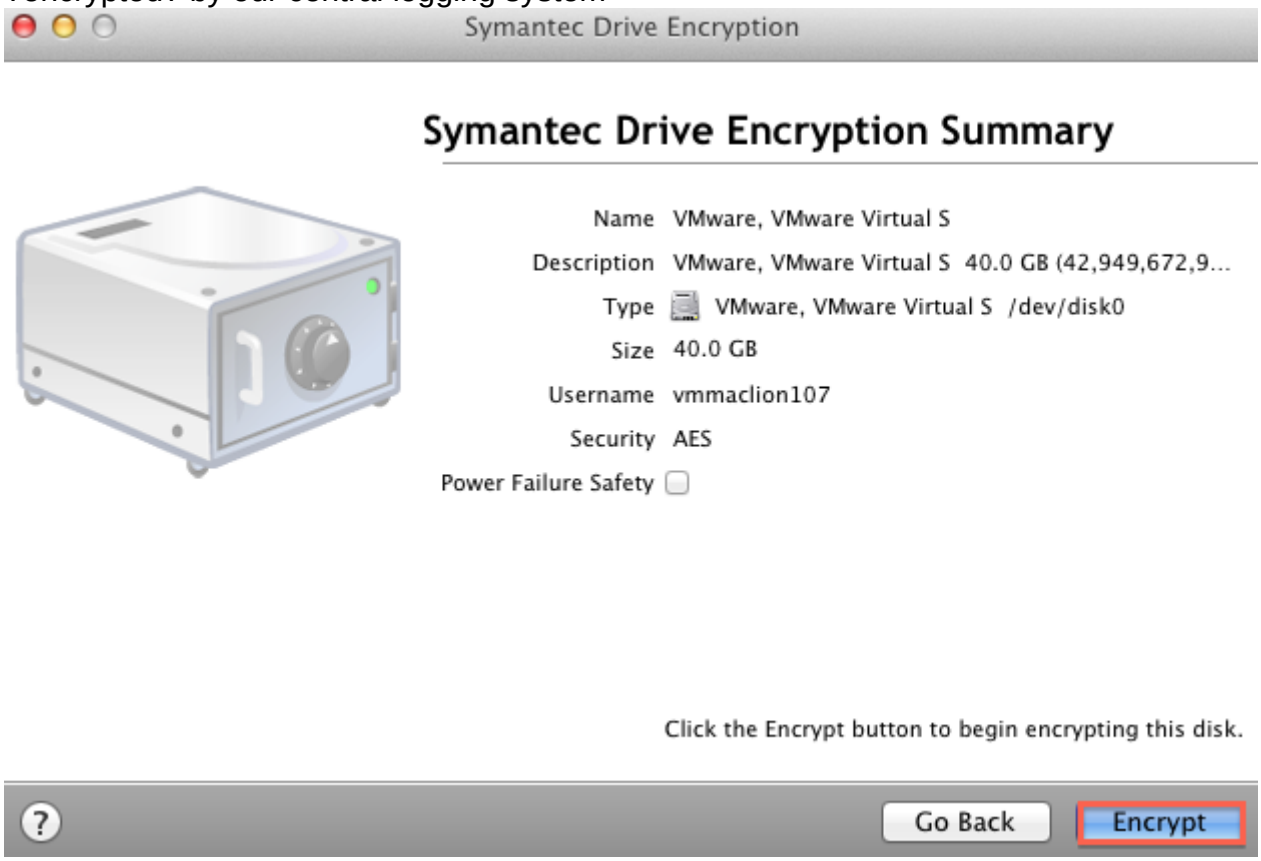
3. Select your computer?s Hard Drive and click Continue



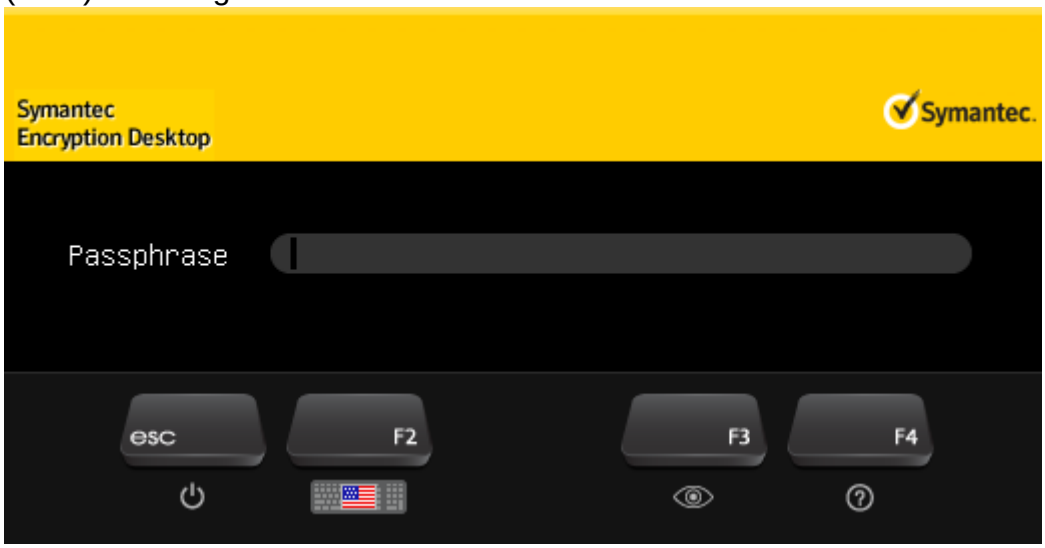
4. Create WDE passphrase user name and password. Minimum 7 characters then click Continue



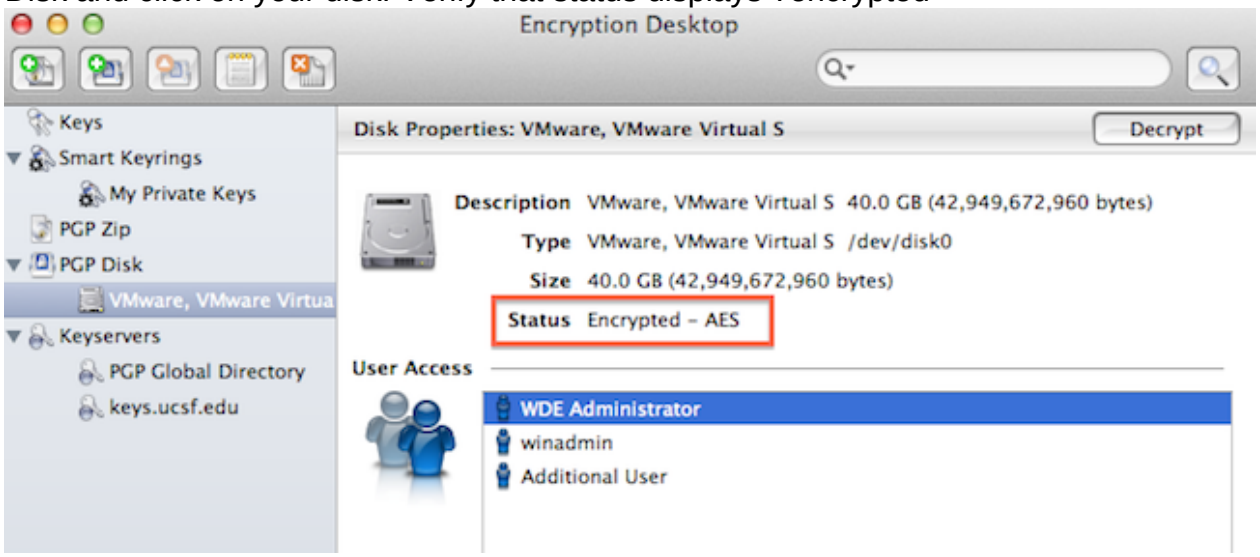
5. Click the Encrypt button to begin encrypting the disk. Encryption will take 4-12 hours to complete; you must verify that your system is encrypted to 100% before it is considered ?encrypted? by our central logging system



6. After encryption is enabled the system will have a **Pre-boot Authentication Screen** , only the passphrase user that was created in the beginning of this process will be able to authenticate. Additional users can be configured. See Symantec Encryption Desktop (PGP) User?s guide for more information



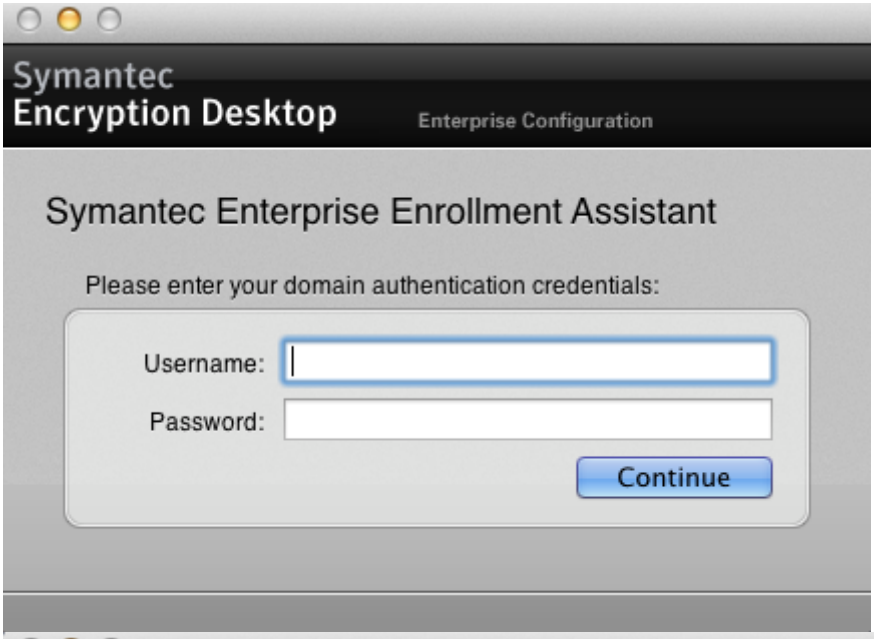
7. Verifying disk encryption. Open Symantec Encryption Desktop (PGP), expand PGP Disk and click on your disk. Verify that status displays ?encrypted"



Required Service Information

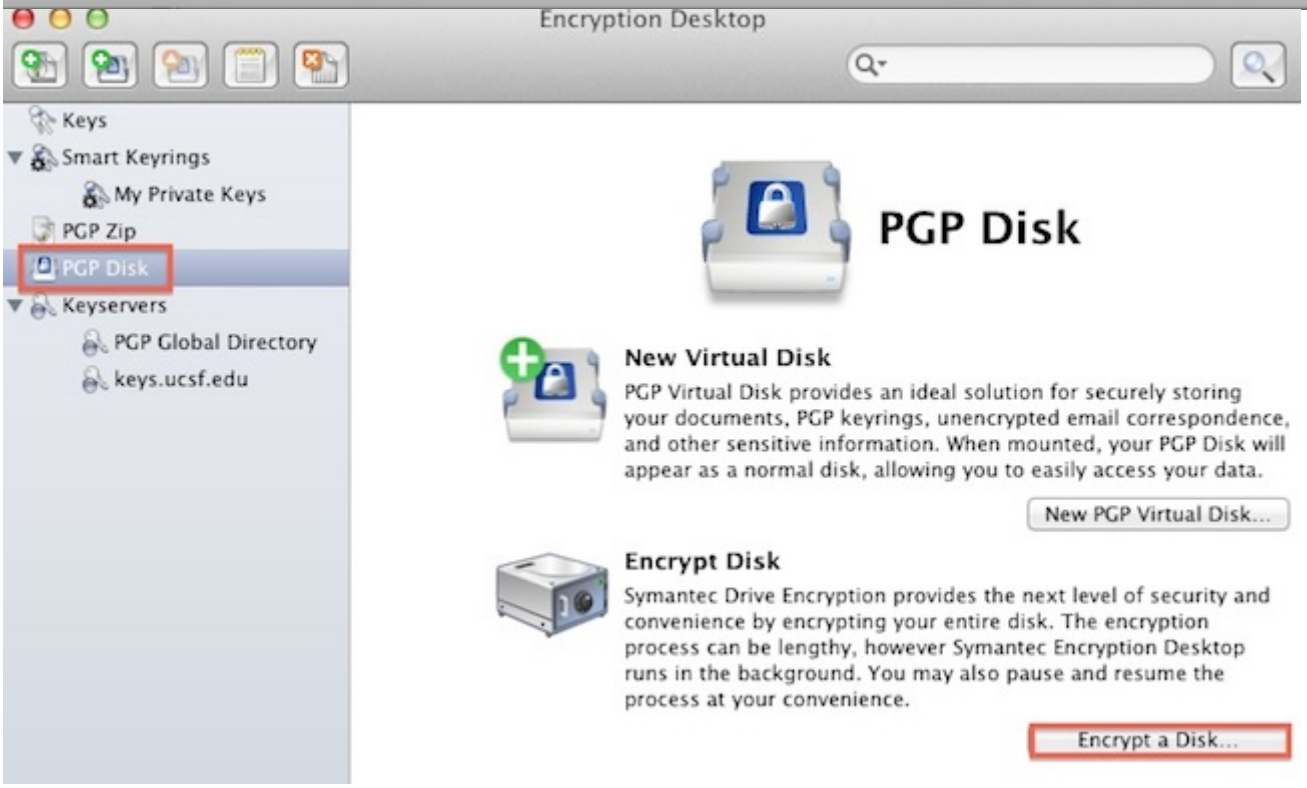
PGP [6]

Images


Symantec
Encryption Desktop
Enterprise Configuration
Symantec Enterprise Enrollment Assistant
Please enter your domain authentication credentials:
Username:
Password:
Continue

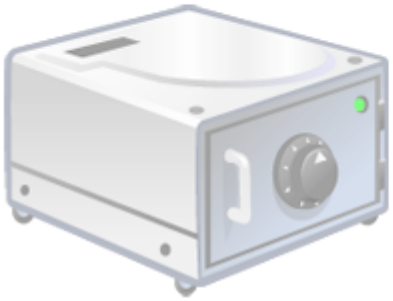

Setup Assistant
Introduction
Keyring Selection
Welcome to Symantec Encryption Desktop
Before continuing, please indicate whether you are new to PGP solutions, or if you have existing keyrings or keys.
I am a new user.
I've used PGP solutions before, and I already have keys.
I have additional key files to import.
Symantec.
Go Back
Continue


Setup Assistant
Introduction
Keyring Selection
Keyring Setup Summary
PGP Desktop will use the following keyring files to store your public and private keys.
Public Keyring File:
~/Documents/PGP/PGP Public Keyring.pkr
Private Keyring File:
~/Documents/PGP/PGP Private Keyring.skr
Symantec.
Go Back
Finish


Encryption Desktop
Keys
Smart Keyrings
My Private Keys
PGP Zip
PGP Disk
Keyservers
PGP Global Directory
keys.ucsf.edu
PGP Disk
New Virtual Disk
PGP Virtual Disk provides an ideal solution for securely storing your documents, PGP keyrings, unencrypted email correspondence, and other sensitive information. When mounted, your PGP Disk will appear as a normal disk, allowing you to easily access your data.
New PGP Virtual Disk...
Encrypt Disk
Symantec Drive Encryption provides the next level of security and convenience by encrypting your entire disk. The encryption process can be lengthy, however Symantec Encryption Desktop runs in the background. You may also pause and resume the process at your convenience.
Encrypt a Disk...

Symantec Drive Encryption

Encrypt Disk



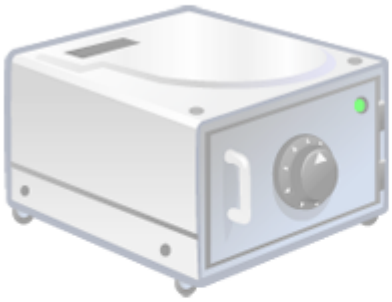
Select a disk:

Disk	Capacity
VMware, VMware Virtual S (/dev/...	40.0 GB

Go Back | Continue

Symantec Drive Encryption

Add Drive Encryption User



Name:

User Account

Enter your passphrase:

Seven Character Passphrase

Confirm your passphrase:

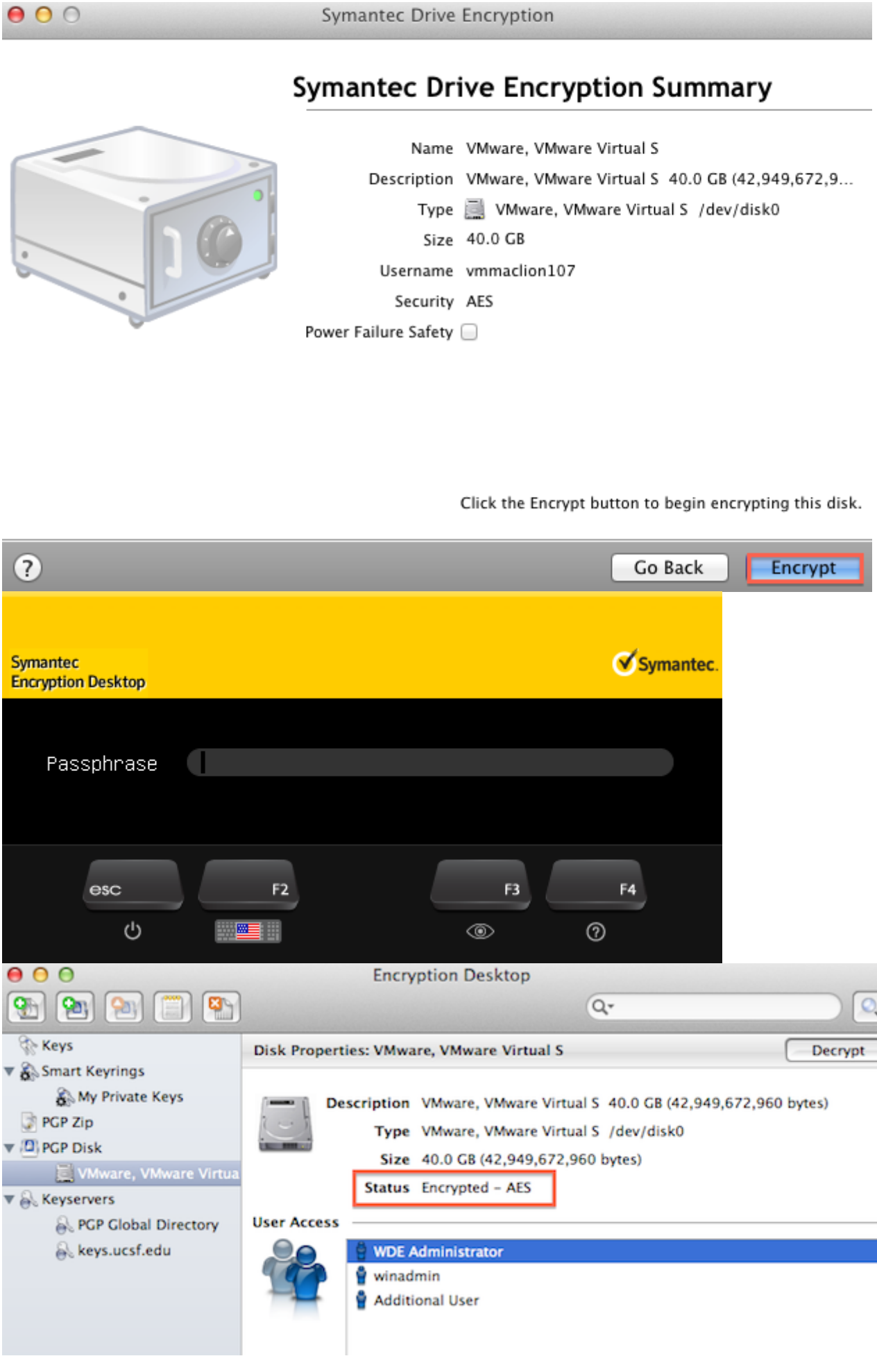
Seven Character Passphrase

Passphrases must be at least 7 characters in length.

Show Keystrokes

Passphrase Quality:

Go Back | Continue


Symantec Drive Encryption
Symantec Drive Encryption Summary
Name VMware, VMware Virtual S
Description VMware, VMware Virtual S 40.0 GB (42,949,672,9...
Type VMware, VMware Virtual S /dev/disk0
Size 40.0 GB
Username vmmaclion107
Security AES
Power Failure Safety
Click the Encrypt button to begin encrypting this disk.
Go Back
Encrypt
Symantec Encryption Desktop
Symantec.
Passphrase
esc
F2
F3
F4
Encryption Desktop
Keys
Smart Keyrings
My Private Keys
PGP Zip
PGP Disk
VMware, VMware Virtua
Keyservers
PGP Global Directory
keys.ucsf.edu
Disk Properties: VMware, VMware Virtual S
Decrypt
Description VMware, VMware Virtual S 40.0 GB (42,949,672,960 bytes)
Type VMware, VMware Virtual S /dev/disk0
Size 40.0 GB (42,949,672,960 bytes)
Status Encrypted – AES
User Access
WDE Administrator
winadmin
Additional User

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Site Login Site Index

Suggest an IT Improvement | © UC Regents

*/ //-->

Links
[1] https://it.ucsf.edu/services/dell-data-protection-encryption-ddpe
[2] https://support.symantec.com/business/support/index?page=content&id=TECH212700
[3] http://software.ucsf.edu/applications/pgp.html
[4] mailto:first.last@ucsf.edu
[5] https://it.ucsf.edu/policies/ucsf-minimum-security-standards-electronic-information-resources
[6] https://it.ucsf.edu/services/pgp