

Pointsec Encryption Software Information for System Administrators

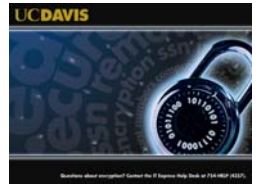


Table of Contents

This document describes the Pointsec for PC encryption software, IET Encryption Support Service, and software deployment process, and is intended for use by UC Davis system administrators.

| | |
|---|---|
| Introduction | 3 |
| Pointsec for PC Encryption Software | 3 |
| IET Encryption Support Service..... | 3 |
| Pointsec for PC Deployment Process | 4 |
| 1. Determining Need..... | 4 |
| 2. Reviewing/Completing Pre-install Checklist | 4 |
| 3. Consulting with IET Encryption Support Staff | 4 |
| 4. Obtaining & Installing Software | 4 |
| 5. Storing Restoration Files | 5 |
| References..... | 5 |
| Related Documentation | 5 |

Introduction

Both the UC Davis Cyber-safety Program policy ([PPM 310-22](#)) and the Whole Disk Encryption policy (expected in March 2007) require campus units to take measures to limit access to restricted information (e.g. social security numbers, California driver's license numbers, and financial account numbers) residing on computing systems. It is recommended that the data be removed from the system whenever possible. In cases where measures such as removal and/or obfuscation are not possible, it may be necessary to encrypt the data.

Recognizing the importance of protecting restricted information, the University of California Office of the President (UCOP) recently contracted with Pointsec for encryption software. To help the UC Davis community meet campus policy requirements for protecting restricted information, Information and Educational Technology (IET) offers the IET Encryption Support Service. The service provides supports to individuals and departments deploying Pointsec for PC encryption software. Additional details about the IET service and Pointsec for PC are provided below.

Pointsec for PC Encryption Software

Pointsec for PC is a Microsoft Windows compatible whole disk encryption software package currently supported on Windows XP and Windows 2000. Pointsec for PC encrypts all sectors on a drive partition using a strong encryption mechanism (256-bit AES). Because the entire partition is encrypted, Pointsec for PC protects sensitive files as well as data that might be found in temporary files, deleted files, swap files and similar areas that might be easily overlooked.

To minimize its performance impact and enhance its security the encryption process works through a kernel process much like a file system driver that is launched early in the boot process. After authenticating a valid user via password, dynamic token or smart card it passes control to the operating system. Pointsec for PC is transparent to the operating system; meaning the hard drive appears unencrypted to the both the operating system and all applications.

Pointsec for PC is designed as an enterprise solution as opposed to stand-alone software designed for a single user. It supports multiple users to allow for administrators, technical support and normal users each with discrete permissions and levels of privilege; and provides support functionality including a remote password reset process and disk recovery tools. Pointsec allows for flexible configurations to meet a range of needs.

Note: Pointsec Media Encryption (ME) is also supported by IET. Pointsec ME enables users to encrypt files, folders and removable media. The encrypted packages require no special software to open; recipients need only to know the password.

IET Encryption Support Service

The IET Encryption Support Service assists departments and individuals who are using Pointsec encryption software to protect restricted information residing on Windows systems. The service includes:

- Subsidization of Pointsec for PC Encryption Software - Some licenses for Pointsec for PC encryption software may be subsidized by IET. Subsidized licenses are granted at the discretion of the IT Security Coordinator based on demonstrated need and compliance with the Central Key Retention Agreement.
- Central Key Retention Agreement - IET Encryption Support staff will be responsible for securely storing restoration files on behalf of departments and individuals who have deployed Pointsec for PC on their systems. Individuals and departments requesting subsidization must provide the restoration files to IET to avoid being billed for the Pointsec license; those purchasing Pointsec licenses are strongly encouraged to do so as well. The IET Encryption Support staff will not have administrative access to the system operating system, but will have administrative access to the Pointsec application (which is invoked before the system is fully up and running).
- Training and Consultation - IET Encryption Support staff may provide training for system administrators who plan to deploy Pointsec for PC to one or more systems within their departments. Training may include procedures for installing Pointsec for PC and for retrieving the files required for central key retention.

Pointsec for PC Deployment Process

This section describes the steps you will need to take to deploy Pointsec for PC and the options that may be available along the way.

1. Determining Need

Consider the following when determining if encryption is the appropriate protective measure for your system(s):

- Has the system been scanned for sensitive data?
- Does the system contain sensitive data?
- Is it absolutely necessary for sensitive data to reside on that system?
- Is the system at risk for loss or theft?
- Does the system meet the minimum system requirements for Pointsec for PC? (see *Pre-installation Checklist* in the Related Documents section below)

If encryption is appropriate, you should be able to answer "yes" to four or more of the questions above.

Note: Cornell Spider and Power GREP software is available via the [Software Licensing Coordination Web site](#) to help you search systems for sensitive data.

2. Reviewing/Completing Pre-install Checklist

Not all Windows systems can use Pointsec for PC. The [Pointsec for PC: Pre-installation Checklist](#) (see <http://security.ucdavis.edu/encryption>) can help you determine if the system meets Pointsec installation requirements and ensure that the system is in good working order before you install the encryption software. IET-DES will complete this step if you have selected the *recharge* profile.

3. Consulting with IET Encryption Support Staff

- A. To initiate the process for obtaining a Pointsec license, complete and submit the [Consultation Request](#) form (see <http://security.ucdavis.edu/encryption>). When your request is received, you will be contacted by the IET Encryption Support staff (cybersecurity@ucdavis.edu) regarding your configuration profile. Two pre-configured profiles are available. The profile appropriate for you depends upon who will install the software, a system administrator in your department or IET-Desktop Enterprise Support (available on a recharge basis).

Note: Profiles can be adapted for your environment upon request, preferably prior to installation. Many settings can only be configured prior to installation; changing settings after installation requires re-running the install process in update mode.

- B. During consultation, IET Encryption Support staff will help determine if your request qualifies for subsidization.

4. Obtaining & Installing Software

- A. To obtain your Pointsec software, you will need to complete and submit the [Billing/Consent form](#) to Software Licensing.
- B. To install Pointsec for PC:
 1. Create a directory `c:\pointsec` on the machine to be encrypted. This is the default location that Pointsec will try to use to store its recovery information.
 2. Run the Pointsec installer from the media provided. The installer is the file "Pointsec for PC.msi", generally you can just double click this (assuming you have administrative rights). After a few seconds the program will prompt you to reboot.
 3. On rebooting Pointsec for PC installs code in the boot partition and reboots again, you will be now be prompted to enter a Pointsec login.
 4. Login to Pointsec. (This also verifies that you know an account before the machine is encrypted).

5. After a successful login Pointsec begins the Windows boot process. Log in to Windows as you would normally.
6. Once Pointsec creates the recovery file (*machine_name.rec*) in Pointsec, the c:\pointsec directory encryption begins.
7. IMPORTANT: Copy the recovery file to a safe location (ex: usb device, floppy, writable cd, email).
Note: You can work while the encryption is occurring. You can shutdown and reboot the computer. Encryption will resume. You can see the percentage encrypted from the system tray icon. The will take about 10 to 20gb/hr.
8. After the encryption process completes, send a copy of the recovery (.rec) and log (.log) files to cybersecurity@ucdavis.edu per the instructions below.

5. Storing Restoration Files

Once Pointsec has been installed, the following should be sent to cybersecurity@ucdavis.edu for secure storage:

- An email that includes your department name, your name, and the system serial number.
- The recovery file (*computer_name.rec*): This file will allow the drive to be decrypted if it becomes unbootable (assuming the drive itself is functional).
- The log file (*computer_name.log*): This file demonstrates that the partition was encrypted.

Note: Both the above files are encrypted.

IET-DES will complete this step if you have selected the *recharge* profile. You will receive a confirmation email when the IET Security Group (cybersecurity@ucdavis.edu) has received and processed your information. If you have not selected the *recharge* profile and the above information is not received in a timely manner, your DaFIS account may be charged for the Pointsec for PC license per the Central Key Retention Agreement.

Note: If you have purchased your Pointsec for PC license, you are encouraged to store the above information in a secure location.

References

- [UC Davis Cyber-safety Program Policy \(PPM-310-22\)](#)
Policy regarding campus electronic communications network security standards.
- [Family Educational Rights and Privacy Act \(FERPA\)](#)
US Department of Education site regarding FERPA rules.
- [Health Insurance Portability and Accountability Act \(HIPAA\)](#)
Links to HIPAA resources.
- [Computer Security: UC Davis Cyber-safety Program Policy](#)
Information and resources related to cyber-safety practices.
- [Computer Security: Encryption](#)
Information, resources and forms related to encryption on campus and Pointsec.
- [Computer Security: Encryption FAQ](#)
Frequently asked questions about encryption and Pointsec.

Related Documentation

- [Pointsec Information for System Administrators](#)
- [Pointsec Pre-installation Checklist](#)
- [Consultation Request form](#)
- [Billing/Consent form](#)