CCH Tax and Accounting

ProSystem *fx* Engagement

Encryption Best Practices

8/9/2006

CCH
a Wolters Kluwer business

In the past several months, the Engagement support team has received a number of inquiries regarding recommendations and compatibility with third-party encryption software packages. This paper provides a brief overview of this topic, as well as some information on three packages that have received a limited amount of testing with Engagement.

Encryption allows for the protection of data located on a computer. Generally speaking, encryption scrambles the data in a complex, but logical pattern, so that it cannot be accessed without the correct key. Depending on the encryption software used, the access key may be provided by a password, a hardware key, or even fingerprint recognition.

There are different types of encryption, and different methods to apply encryption to data. These include whole drive encryption (the encryption of an entire physical hard disk or partition), virtual drive encryption (the encryption of a virtual disk that is generally a large encrypted file located on an unencrypted disk), and single file encryption (the encryption of a single file on an unencrypted disk). As each of these methods are valid ways to approach the encryption of data, their use depends greatly on what type of data is being protected.

The following is a list of things to look for in an encryption software package that will work successfully with Engagement and help ensure data security. Whole disk encryption or virtual disk encryption is required for Engagement. Single file encryption methods will not work properly.

- It must be transparent to all applications running on the machine.
- It must be able to do on-the-fly, transparent data encryption.
- It must be able to encrypt the entire disk/storage medium that the application is running on.

The following is a list of encryption software packages that have received limited testing with Engagement.

- PGP – Version 9.0 (www.pgp.com)
- TrueCrypt - Version 4.2a (www.truecrypt.org)
- CyberAngel – Build 550 (www.TheCyberAngel.com)

When Engagement is installed on a PGP, TrueCrypt, or CyberAngel virtual drive, you will need to manually start PFXSYNPFTService.exe, PfxEngDesktopService.exe, and PfxConvertService.exe after a machine reboot. The three services are located in PfxEngagement\WM and PfxEngagement\Common folders. Double click the file and verify that it is running in Task Manager.

PGP – The above-mentioned services do not require a manual start after reboot when using the “Encrypt the entire C drive” feature. The services will start automatically, which is the normal behavior. PGP offers all three forms of encryption mentioned above, but will only work properly with whole disk and virtual disk encryption.

TrueCrypt/CyberAngel – If you receive a LocalAdmin or CentralAdmin error when logging into the Administrator or Workpaper Management module, simply stop and restart the SQL Server Service Manager using the services control panel.

If the encryption software being used does not meet the above requirements, Engagement may not work correctly, or may not be encrypted properly. For additional assistance, please call Engagement support at 800-739-9998 and select Option 6 then Option 2.