Windows FDE ME and MI Encryption Installation Guide

The CheckPoint encryption software for Windows has both a USB drive encryption product (ME) and a full disk encryption product (MI).

CheckPoint Media Encryption (formerly Pointsec Protector) is used to encrypt USB storage devices and external hard drives.

CheckPoint Full Disk Encryption MI is used to encrypt internal hard drives.

The latest information on encryption at VMC (including supported platforms, known issues, etc.) can be found here: http://www.mc.vanderbilt.edu/root/vumc.php?site=InfoPrivacySecurity&doc=17072.

Purchasing and Attaining the software - The software should be purchased and attained from the ITS Software Store: http://its.vanderbilt.edu/software/.

Installing the software

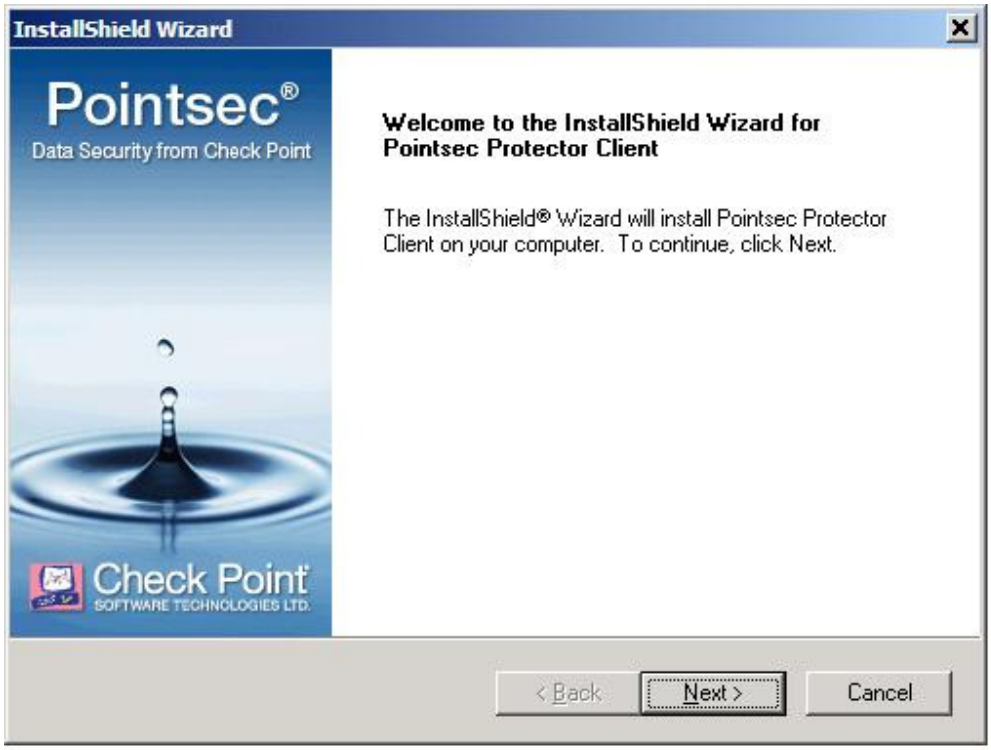
CheckPoint ME (Protector):

CheckPoint ME (Protector) should be installed before encrypting the hard drives with MI. It can be installed silently or manually.

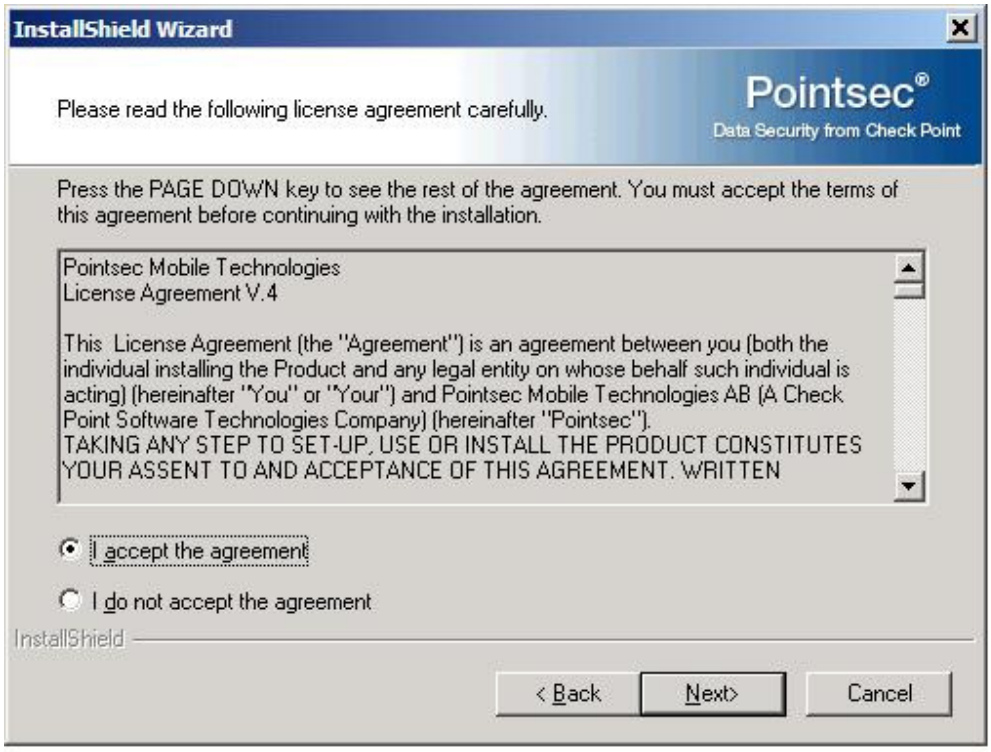
To install it silently via a command line use the following:

\\share\setup.exe -s -f1\\share\setup.iss with \\share being the location of the file share the installation folder is on.

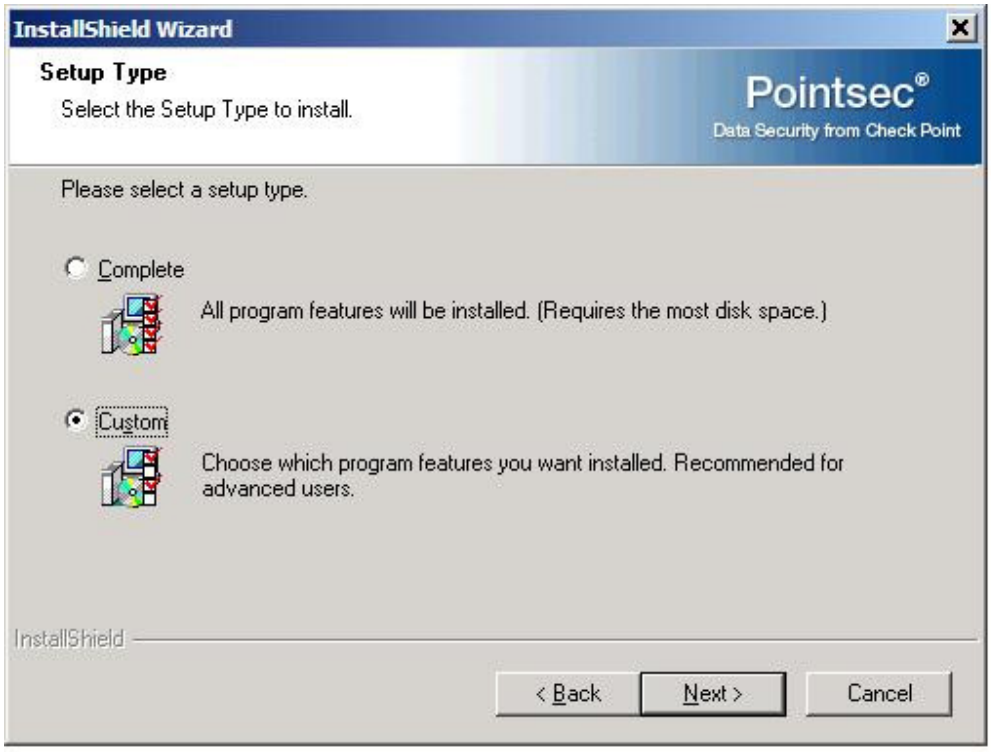
To install manually via a GUI: Login as administrator and run setup.exe. You should see the following screen and click Next



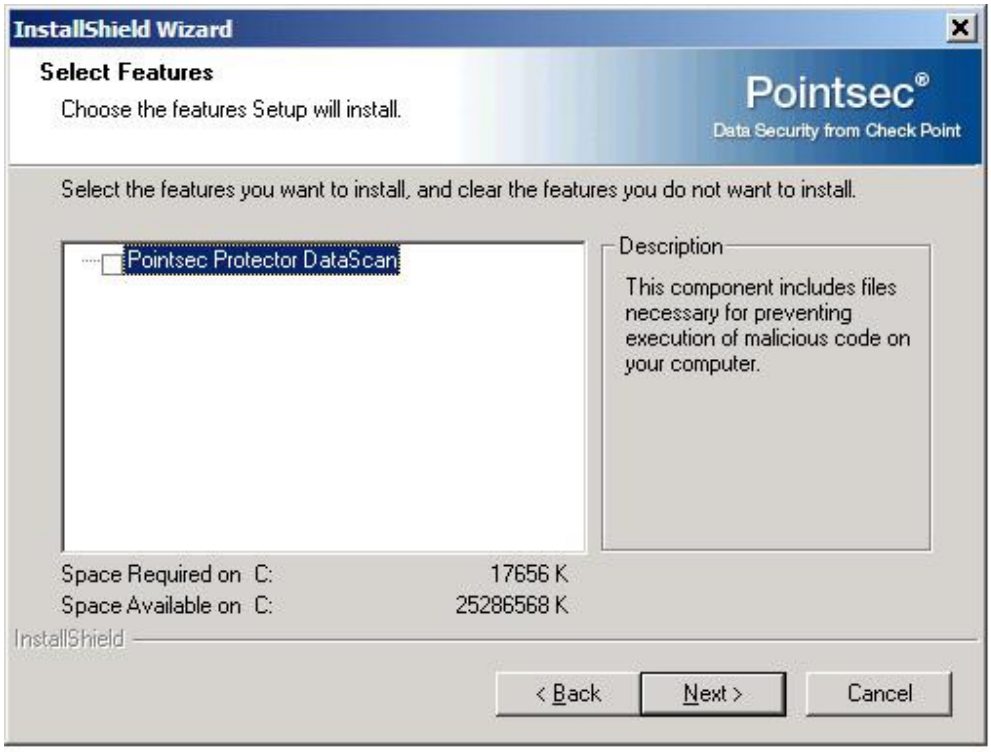
You will need to accept the license agreement, then click Next



Check Custom as the setup type and click Next

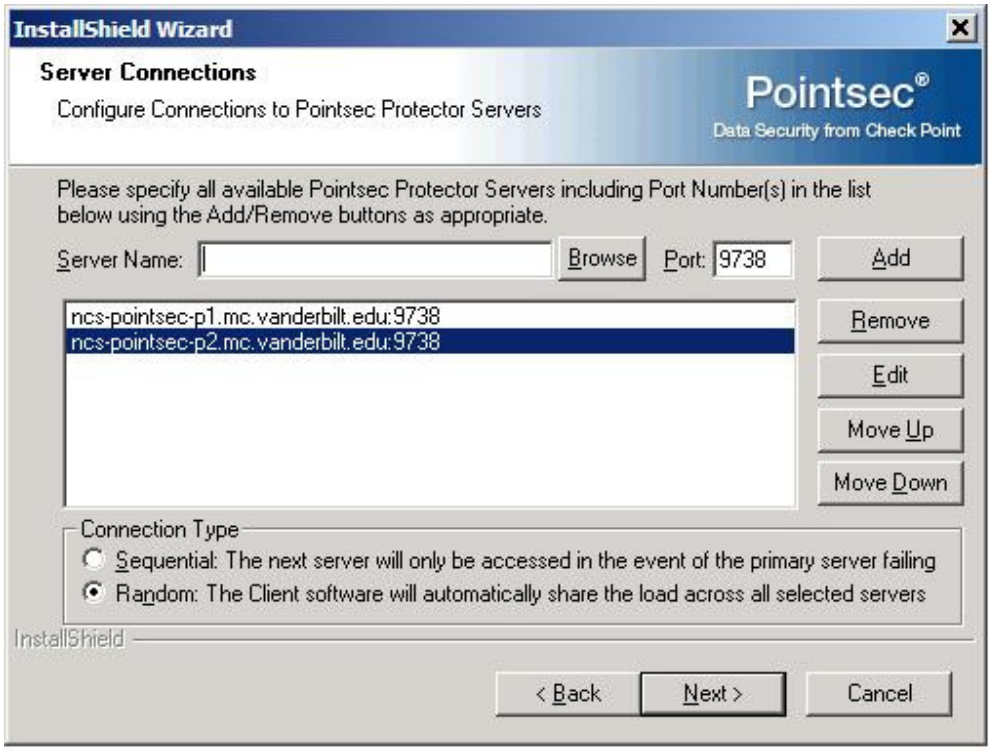


Make sure Pointsec Protector DataScan is NOT checked and click Next

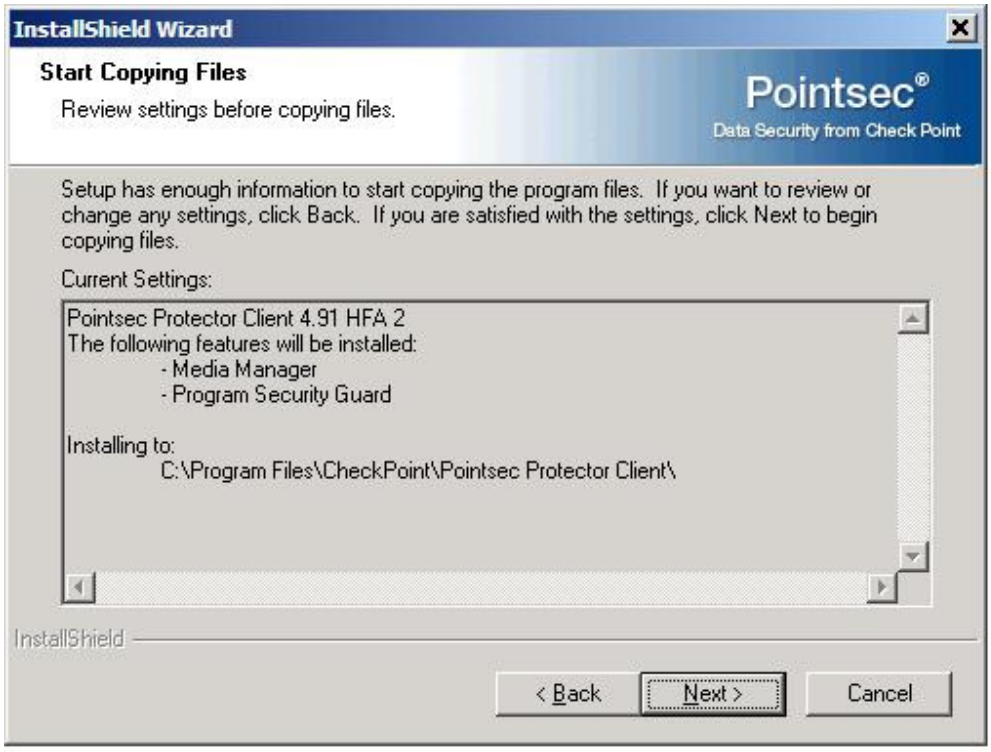


Under Server Name enter **ncs-pointsec-p1.mc.vanderbilt.edu** and click Add. Then also add **ncs-pointsec-p2.mc.vanderbilt.edu**, both with port **9738**. Note – you may get an error that it can't find the server. If you do, verify that the name is correct, then click Okay.

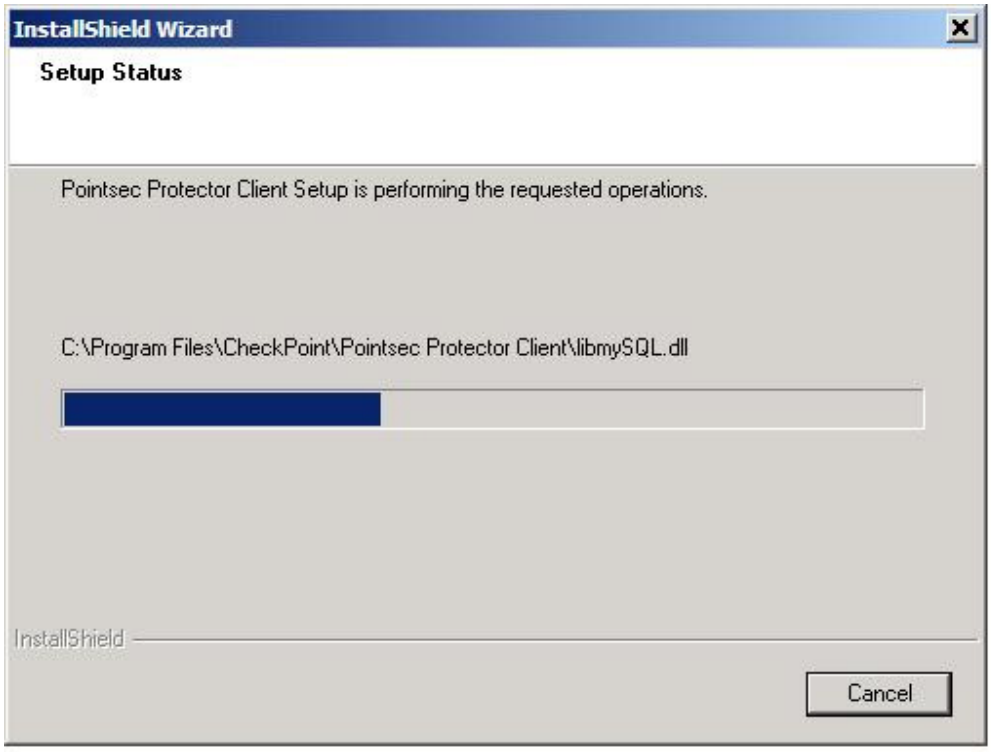
Under Connection Type click **Random** then click Next



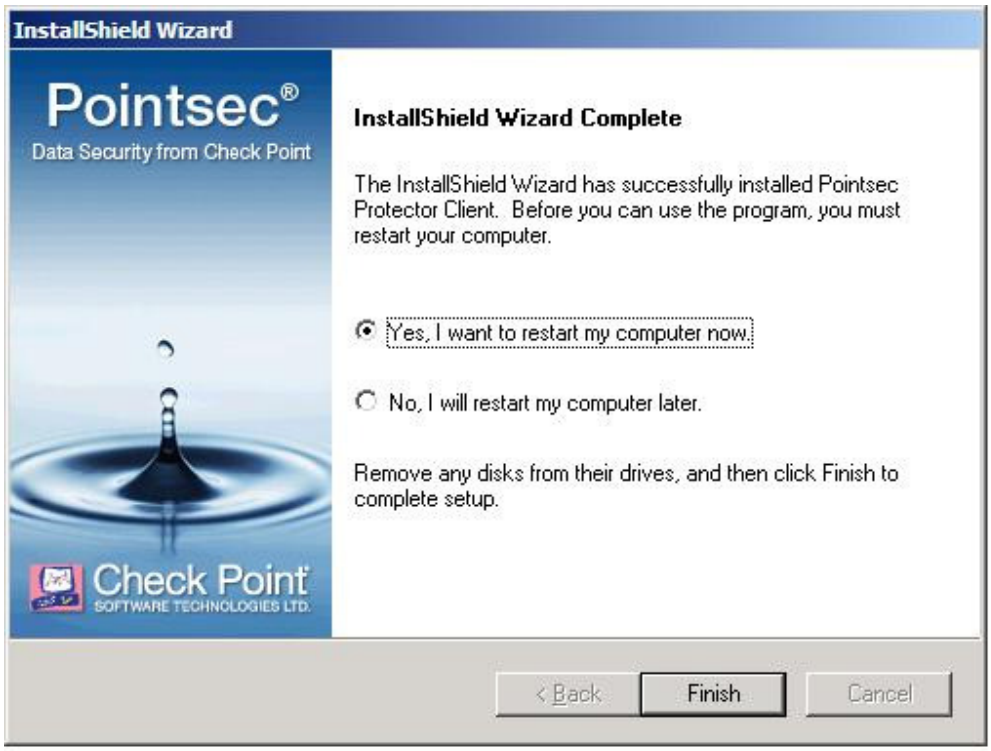
Click Next


InstallShield Wizard
Start Copying Files
Review settings before copying files.
Pointsec®
Data Security from Check Point
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Pointsec Protector Client 4.91 HFA 2
The following features will be installed:
- Media Manager
- Program Security Guard
Installing to:
C:\Program Files\CheckPoint\Pointsec Protector Client\
InstallShield
< Back
Next >
Cancel

An installation update screen will show up



You will be prompted to restart the computer when the installation has completed. Click Finish



Once the computer has restarted, the USB encryption will be in place.

It is strongly recommended that users take advantage of the Password Vault at: https://ncs.mc.vanderbilt.edu/UT001/DeviceSecurity/HomePage.aspx in case they forget their passwords.

CheckPoint Windows Full Disk Encryption MI:

CheckPoint FDE MI installation is a multi step process.

Pre-Installation Information of CheckPoint Windows FDE (Pointsec)

The pre-installation steps for installing the software are:

1. Backup all the data on the computer
2. Remove any existing encryption software
3. Run check disk
4. Run defrag
5. Review the latest information at:
http://www.mc.vanderbilt.edu/root/vumc.php?site=InfoPrivacySecurity&doc=21650

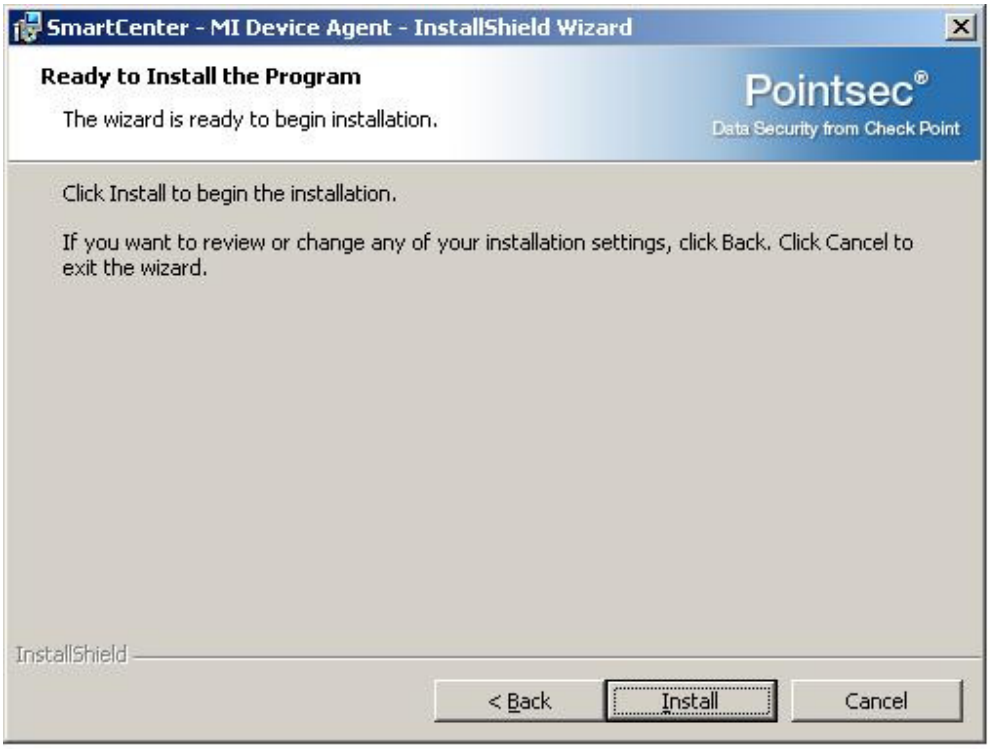
The encryption failure rate has been very minimal and can be lessened by performing the steps above. When the encryption is being done, it reads and writes the entire hard drive which will stress the drive. So if the drive is in marginal shape, this might cause it to fail. While the steps above take time, skipping them could result in the loss of data.

Installing the Device Agent

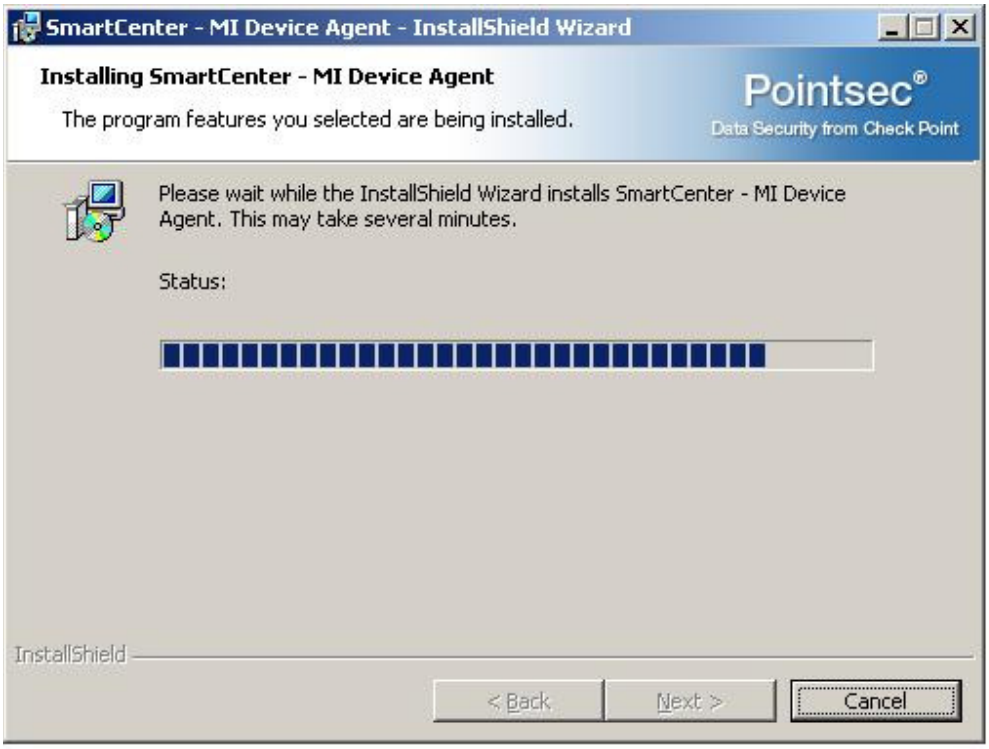
To install the device agent you will need to be logged in as administrator and run "Device Agent x.x.x.xxxx.msi" that came in the zip file from the software store.

If you run this manually on the client you will get the following, click Next

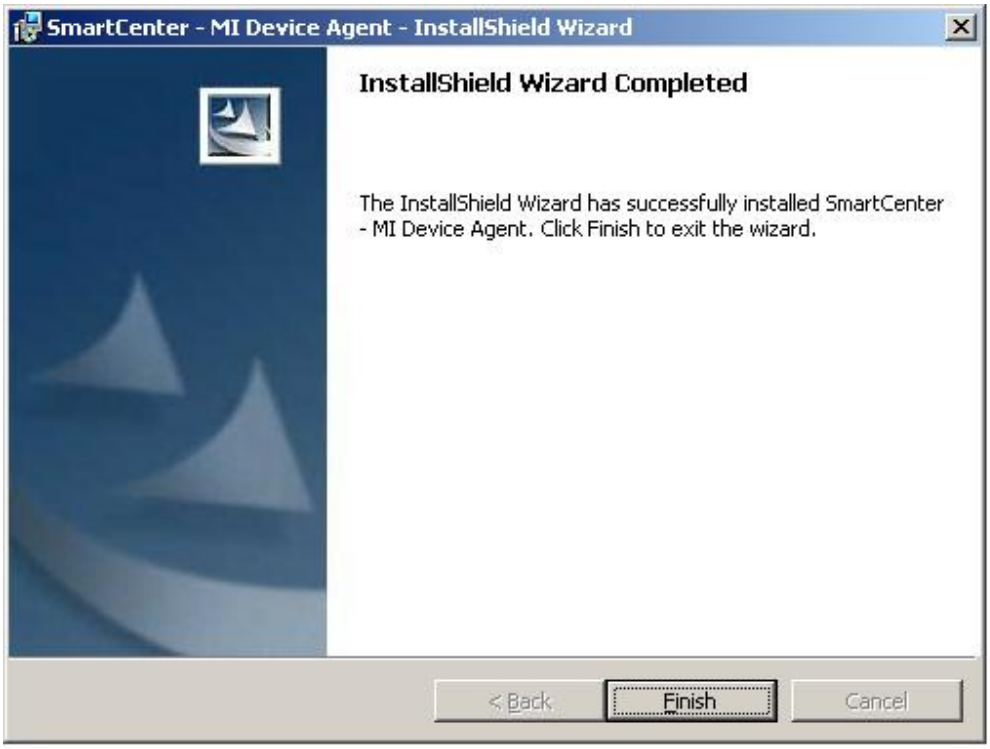
Click Install to continue the install



You will see a progress screen



When the installation completes, click Finish



The next step requires action from the MI Management Server.

When the device is ready to be encrypted:

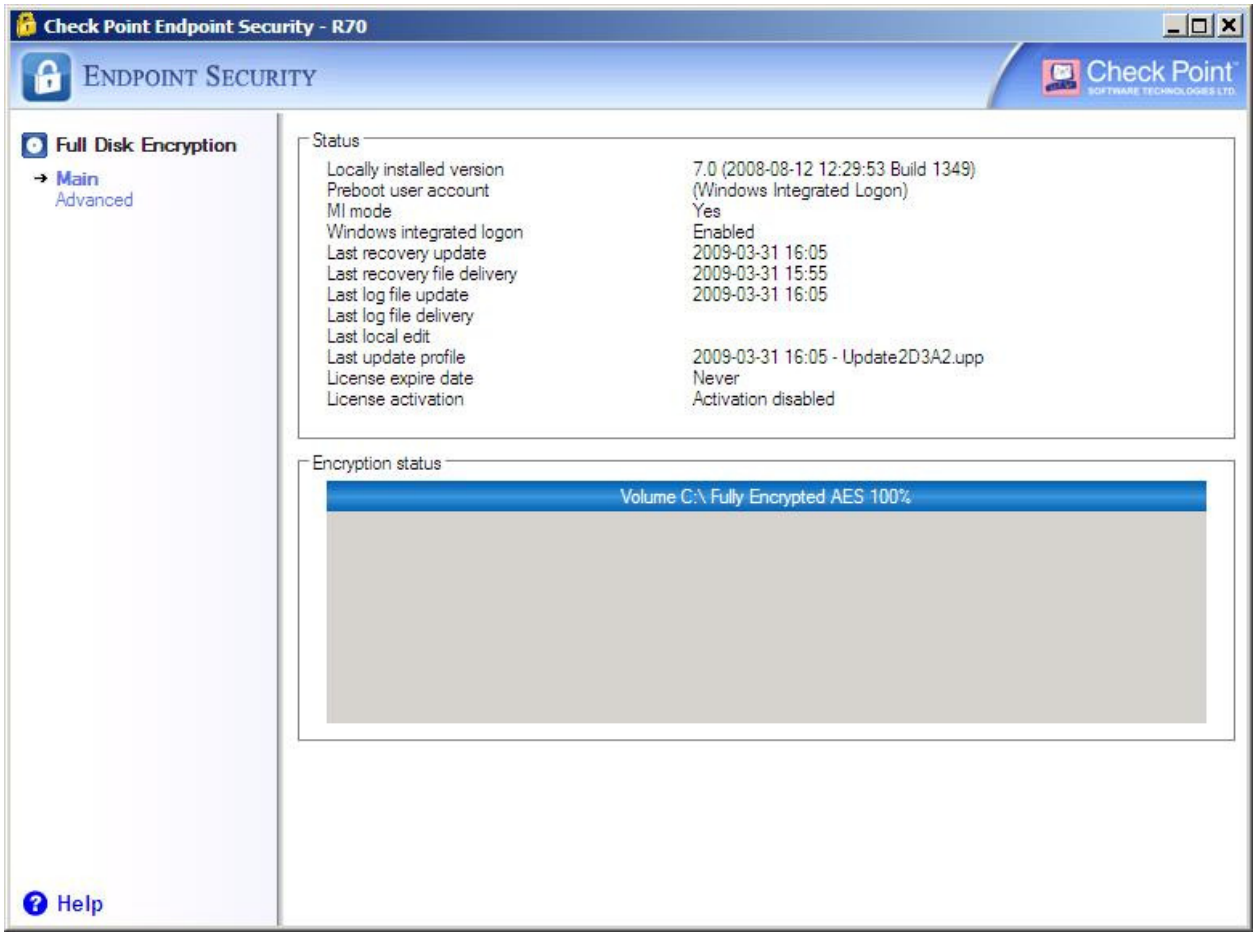
Open a service desk ticket (3-HELP) requesting that the computer be approved for encryption. You will need to provide the computer name and OU.

Once approved on the management server; the next time the client polls the server (can take up to 4 hours); it will silently pull down and install the encryption software. At this point, the client computer needs to be restarted before the actual encryption will start. Because there is no notice given on the client when the software is installed, we recommend telling the user to restart the system when they leave for the day or for the LAN Manager to schedule a restart sometime after the user has left.

The normal time to encrypt a hard drive is about 15GB per hour depending on the speed of the computer and whether the computer is being used during the encryption process.

Other useful info:

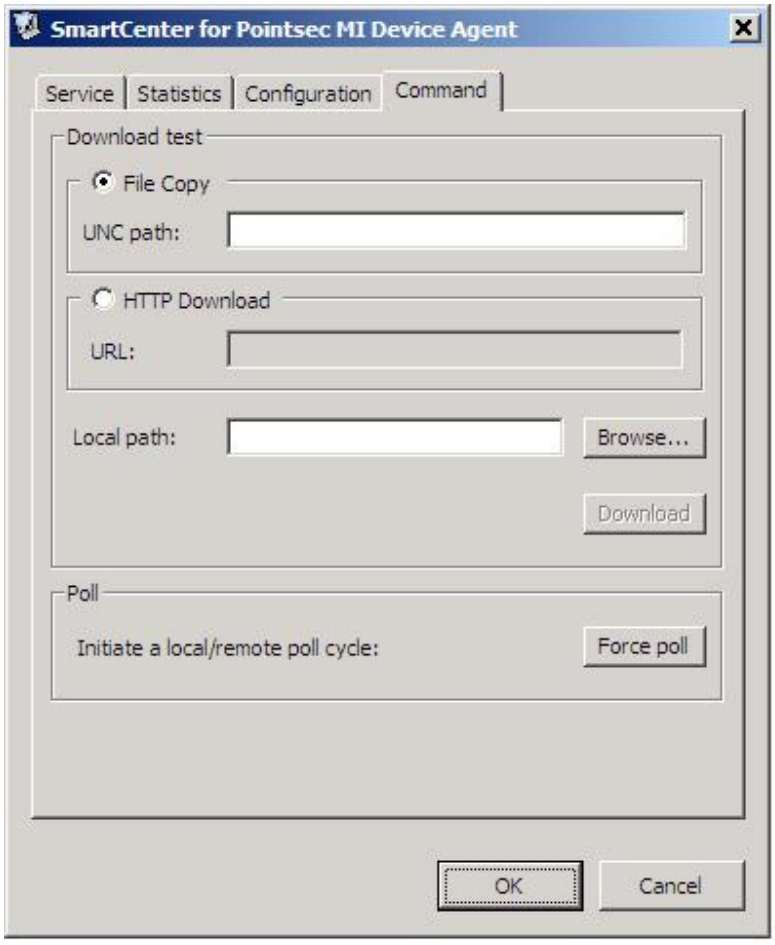
You can check the encryption process by going to: Start > Programs > Check Point > Endpoint Security > Check Point Endpoint Security. Then click on the yellow Check Point padlock icon in the bottom right tool bar and select Settings. This will open the following window showing (among other things) the encryption status:



When the encryption is complete, it will read 100%.

The Endpoint Security MI Device Agent GUI shows addition information and can be used to force the client to send and receive any updates from the server. Go to: Programs > Check Point > Endpoint Security > Endpoint Security MI Device Agent GUI on the client computer to open.

You can force the client to connect to the server by doing a “Force poll” under the Command tab of the MI Device Agent GUI (you will want to force a poll about 3 times to ensure that all the required data is exchanged).



You can see what modules are installed on the Configuration tab of the MI Device Agent GUI