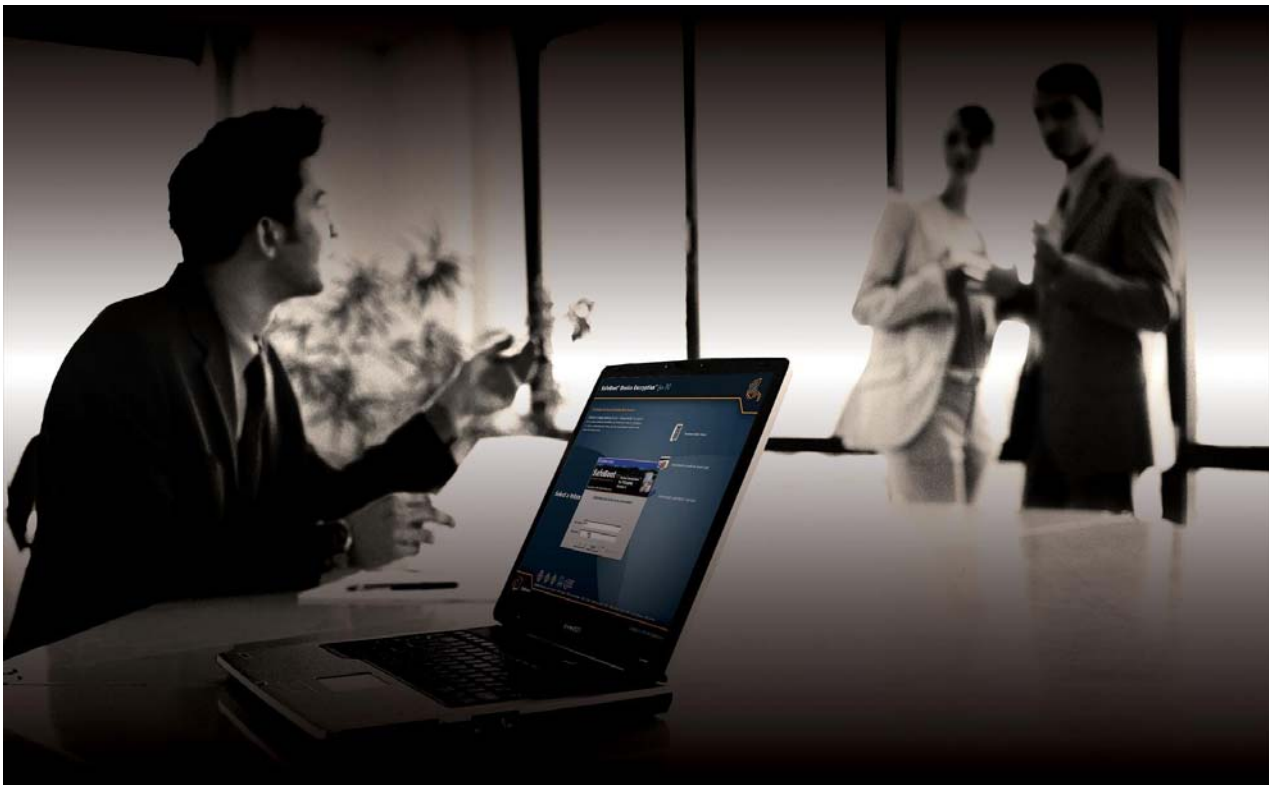
McAfee Endpoint Encryption Administrators Guide



McAfee Endpoint Encryption Overview

The McAfee Endpoint Encryption (MEE) product (formerly known as Safeboot) is the new ITT standard for full disk encryption (FDE). At this time, only laptops require FDE however the long term goal may be to encrypt non-mobile devices such as desktops and workstations. Encryption on all laptops is **mandatory** which is documented in the ITT IT Security Policy 70-02.

MEE uses AES-256 and RC5-1024 encryption algorithms which provide the strongest data encryption available today. For more technical details please visit:
http://mcafee.com/us/local_content/datasheets/ds_endpoint_encryption.pdf

All McAfee Endpoint Encryption Documentation is available on the ITT portal:
Collaboration Project: Safeboot - McAfee Endpoint Encryption
https://my.itt.com/portal/server.pt/gateway/PTARGS_32_0_345_0_-1_47/http;/pcollab.sfdc.ittind.com;11930/collab/do/project/overview?projID=319799

McAfee Endpoint Encryption Package and Policy Settings

The MEE packages have been prepackaged with the following settings:

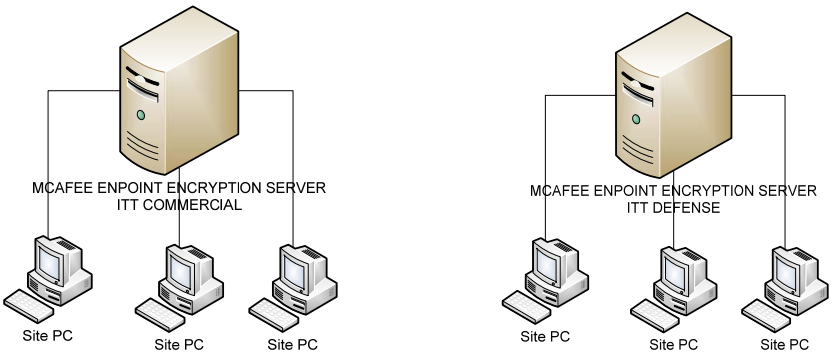
- Suppress installation dialogues boxes
- Suppress reboot after installation

It is expected that the end user will eventually reboot after installation or the VC staff will setup a scheduled reboot using the Altiris toolset.

The MEE policy is configured for mostly the default options with the exception of settings such as “do not display last logged in user name”. The policy is setup to use the windows integrated login feature which bypasses the MEE pre-boot screen. All policy settings are controlled by the MEE servers.

McAfee Endpoint Encryption Infrastructure Design

There are two MEE infrastructures – one for ITT Commercial businesses and one for ITT Defense businesses. The diagram below outlines this.



McAfee Endpoint Encryption Deployment Overview

Deployment of the McAfee Endpoint Encryption software can be conducted in three ways. Both the Altiris Notification Server (central) and Altiris Deployment Server (local) can be used to deploy this software. The MEE product can also be installed manually, although this is not preferred.

Deployment Prerequisites

The MEE deployment and tracking will depend heavily on the Altiris NS. As such, every machine must have the Altiris NS client deployed – ***NO EXCEPTIONS***! Below is a quick reference to the Altiris NS client and command-line parameters for your region.

Defense: AEXNSC.EXE client location - \\01altirisnsna2\packages\NS 6 R8 client\

Command line: Aexnsc.exe -s -a ns="01AltirisNsNa2.de.ittind.com" nsweb="01AltirisNsNa2.de.ittind.com /Altiris" NOSTARTMENU /s /diags

North America Commercial: AEXNSC.EXE client location - \\01altirisnsna1\Altiris NS 6 R8\

Command line: Aexnsc.exe -s -a ns="01AltirisNsNa2.de.ittind.com" nsweb="01AltirisNsNa2.de.ittind.com /Altiris" NOSTARTMENU /s /diags

EMEA Commercial: AEXNSC.EXE client location - \\01altirisnsna1\Altiris NS 6 R8\

> Command line: Aexnsc.exe --s -a ns="46altirisnsemea.emea.itt.net" nsweb="http://46altirisnsemea.emea.itt.net/Altiris" NOSTARTMENU /s /diags

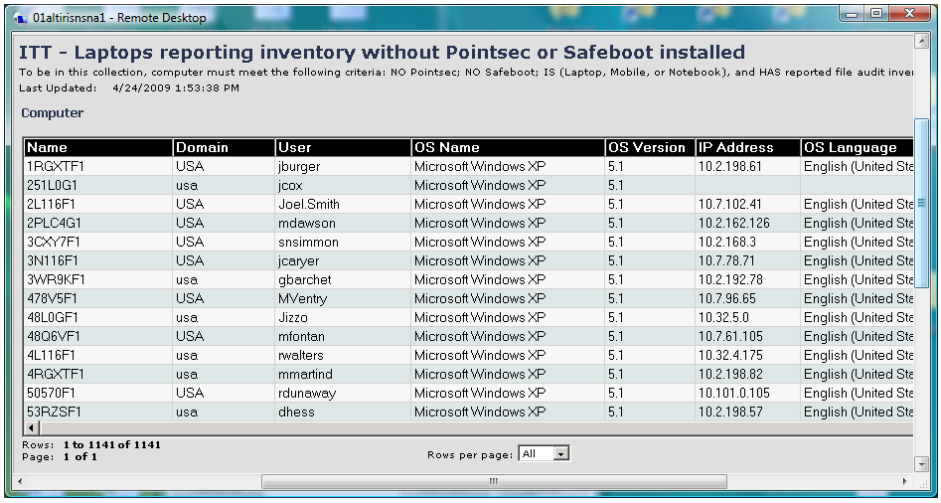
APAC Commercial: AEXNSC.EXE client location - \\01altirisnsna1\Altiris NS 6 R8\

> Command line: Aexnsc.exe -s -a ns="86altirisnsapac.asia-pac.itt.net" nsweb="http://86altirisnsapac.asia-pac.itt.net/Altiris" NOSTARTMENU /s /diags

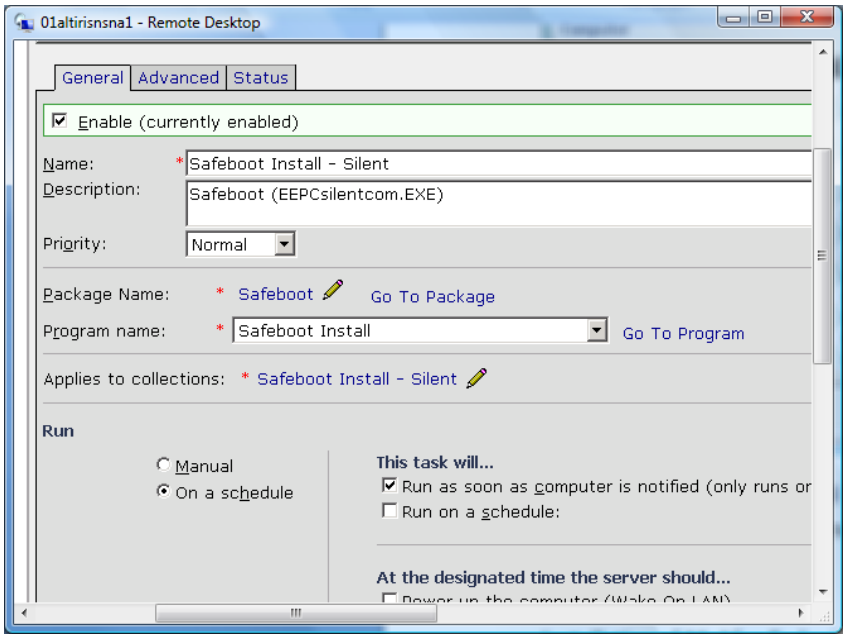
Initial Deployment of McAfee Endpoint Encryption

The initial deployment of MEE will target ***only*** those laptops that aren't encrypted and will be done primarily from the Altiris NS. **A site can opt to use the Altiris DS for initial deployment however you must inform Brad Marr of this first**. A collection in each Altiris NS was created with specific criteria to identify the candidate nodes to receive the MEE software. The criteria are:

- Laptops only
- Full inventory has been forwarded
- No Pointsec installed on the system
- No Safeboot installed on the system



Machines in this collection will be associated with the NS deployment task and as they connect the MEE software is installed in silent mode. The encryption process will not begin until the machine is rebooted.



Installation of McAfee Endpoint Encryption

Altiris Notification Server

The MEE software is staged and ready for deployment on the Altiris Notification Server in your region. Simply just submit a helpdesk ticket to your regional service center requesting deployment of this software and a member of the enterprise desktop team will assist. When submitting the ticket, ensure you include the machine name(s) that you would like MEE deployed to.

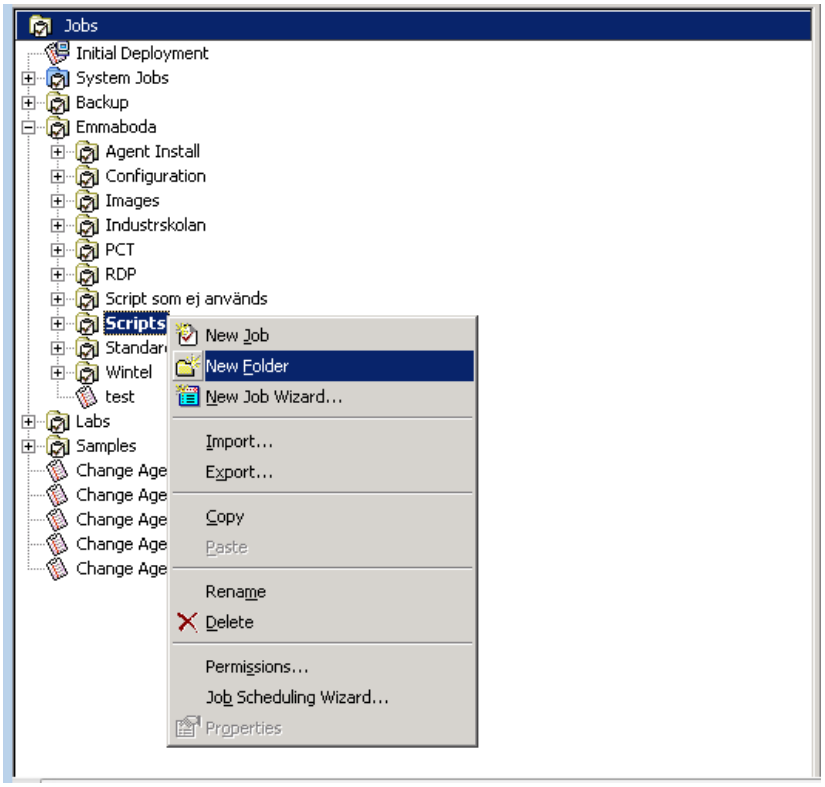
Altiris Deployment Server

The following process is for setup and deployment of the McAfee Endpoint Encryption software on a Altiris deployment server.

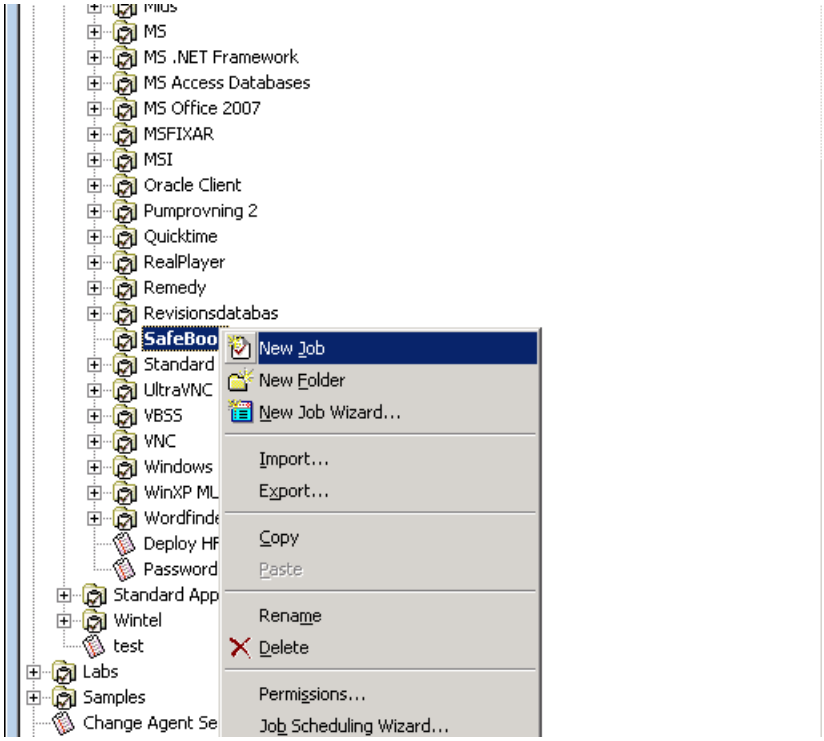
1. ***For Commercial sites ONLY***, download the installation-file "EEPCsilentcom.exe" from \\01mcsbootna1\packages\ and place it on your Deployment Server.

   For Defense sites ONLY, download the installation-file "EEPCsilsentdef.exe" from \\01mcsbootna2\packages\ and place it on your Deployment Server.

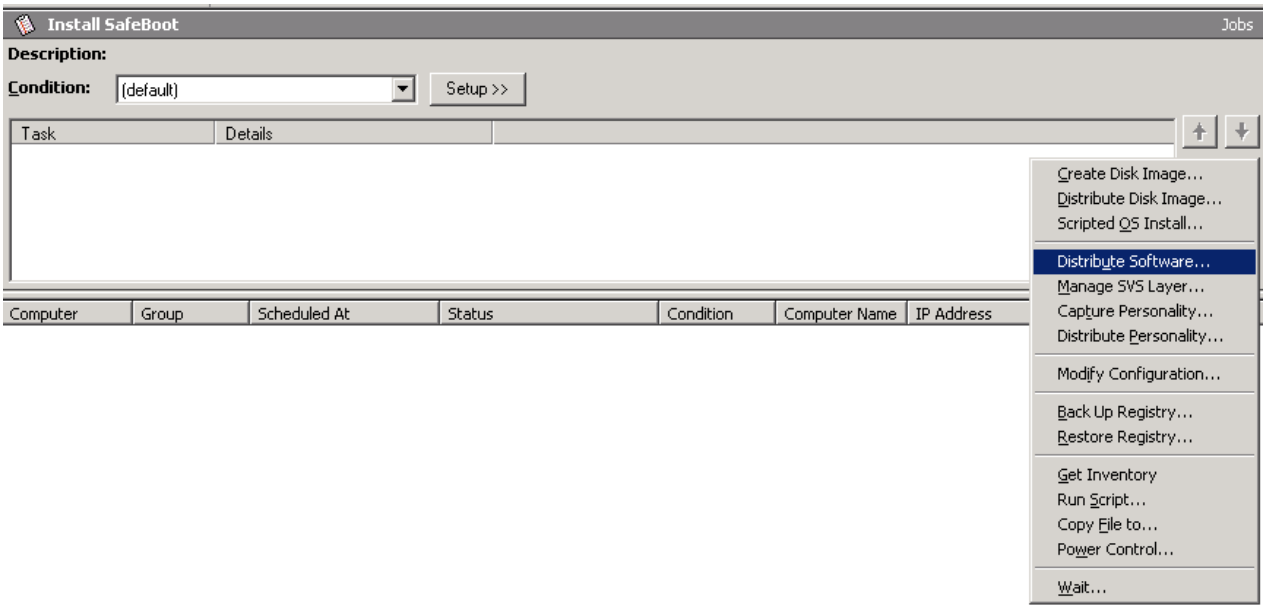
2. On the DS console, create a new folder and name it "SafeBoot".



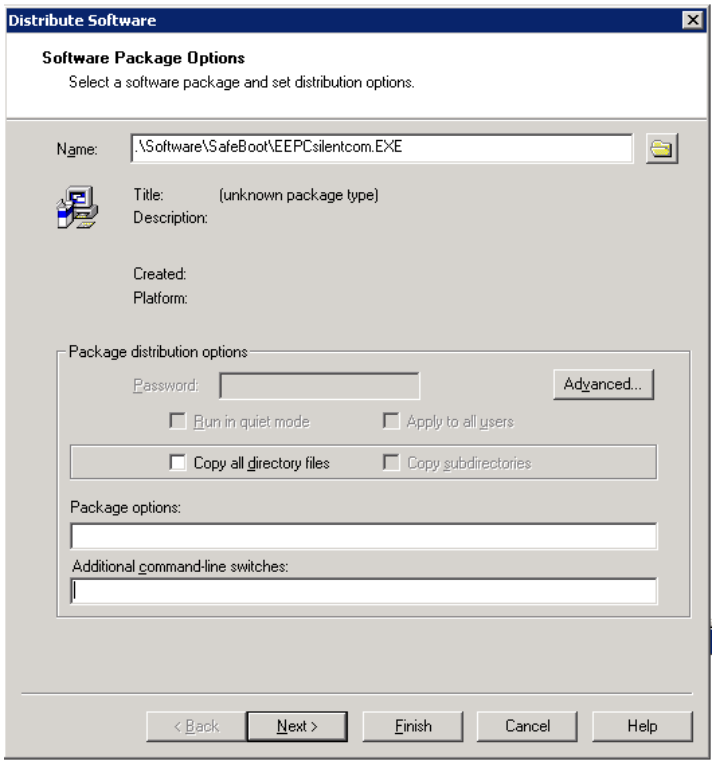
3. Create a new job and name it ”Install SafeBoot”.



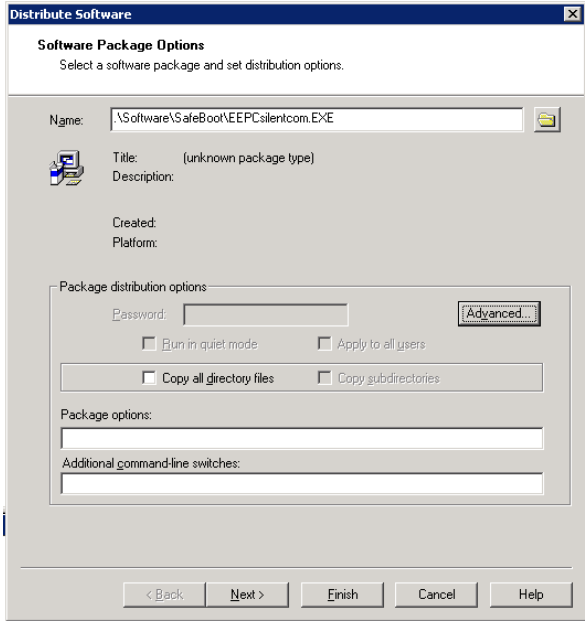
4. Highlight the job and in the upper right corner click Add and select “Distribute Software”.



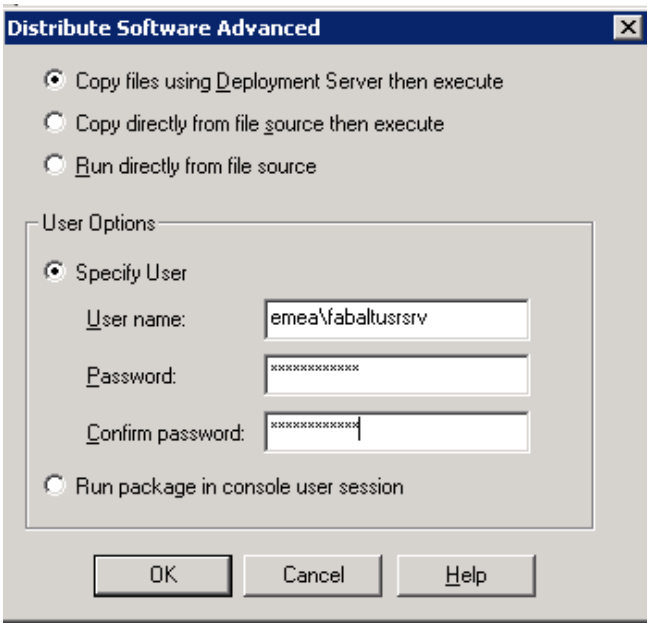
5. Click the browse button, browse to the SafeBoot folder and select “EEPCsilentcom.EXE”. The installation-file is re-packaged to run silent so no extra switches are needed.



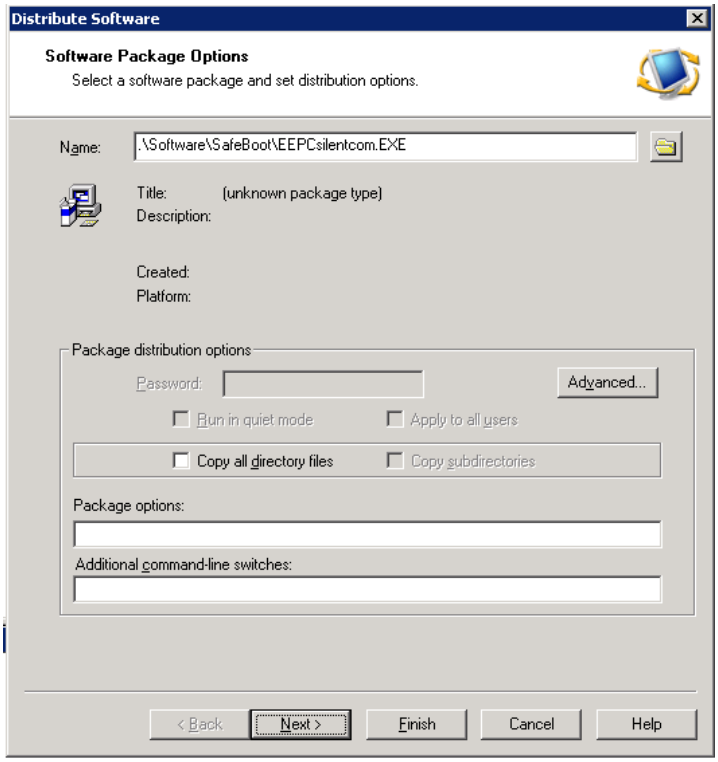
6. NOTE: If your users are NOT local administrators on their machines you need to specify an account that is a local administrator. Click “Advanced” button.



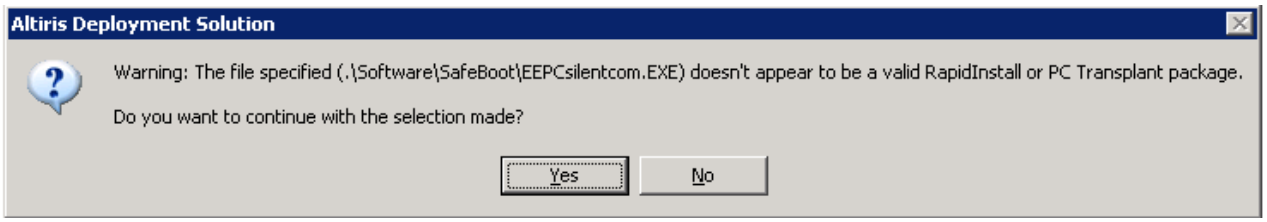
7. Type in user name, password and confirm it. Do not forget to add domain in front of user name followed by a backslash. Click “OK”.



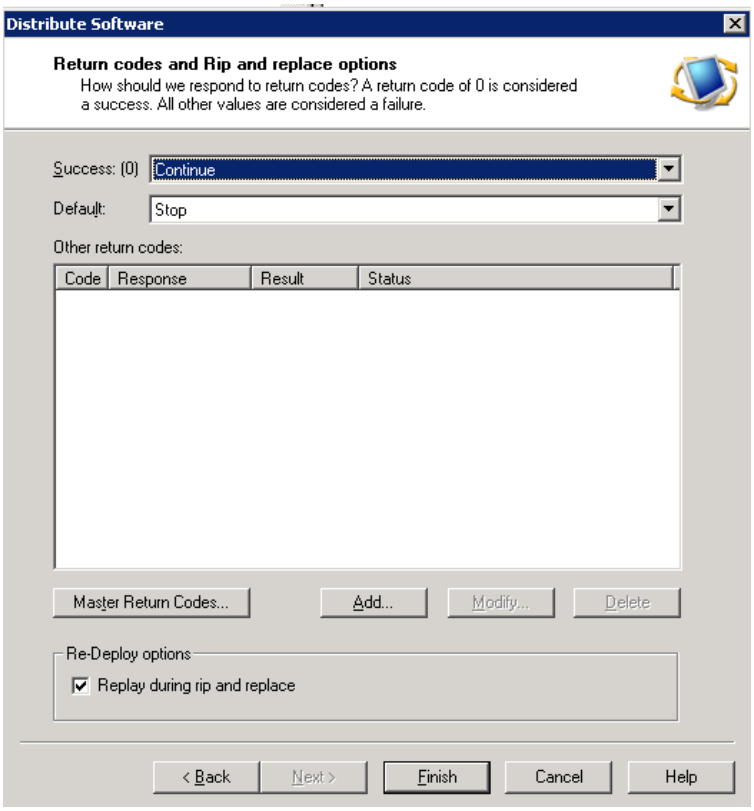
8. Click “Next”.



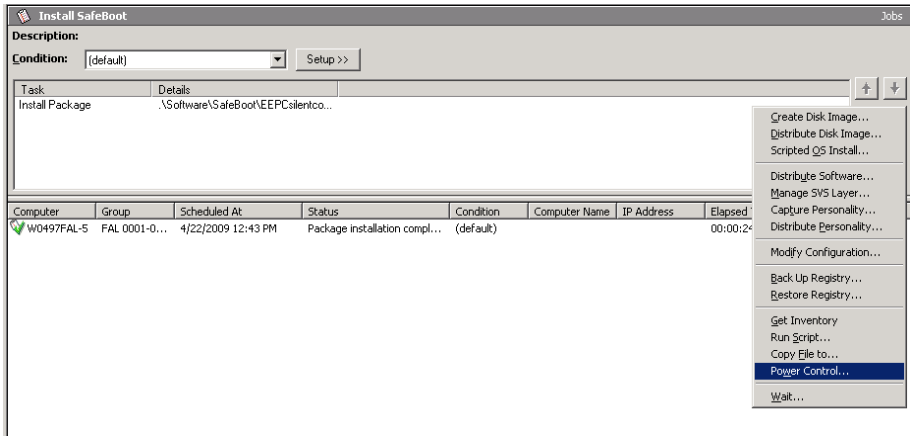
9. You will probably get this warning. Click “Yes”.



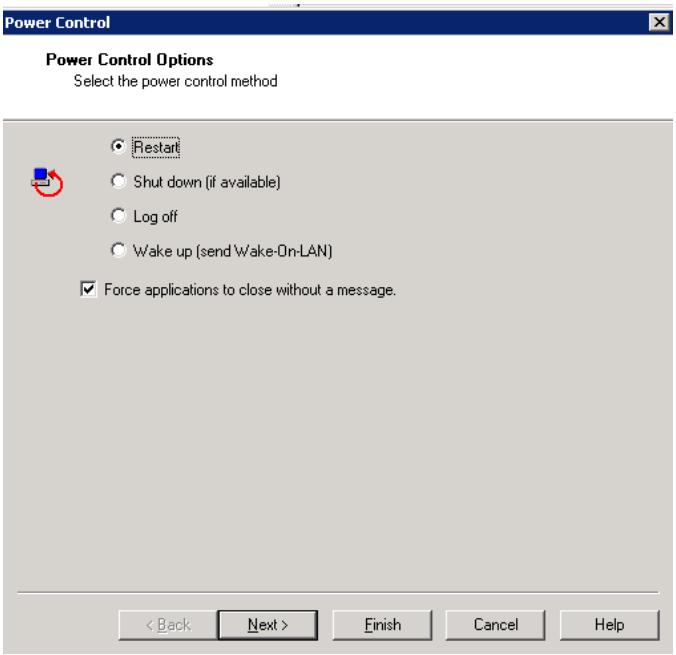
10. Click “Finish”.



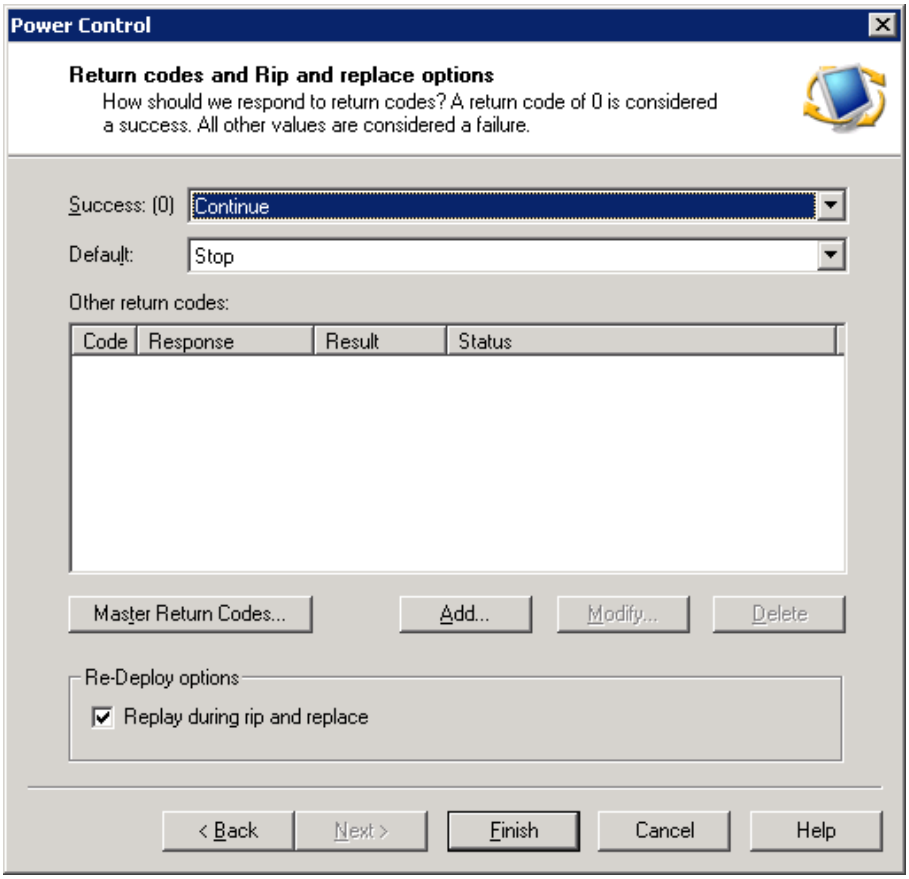
11. **NOTE:** The machine needs a restart in order for the encryption to start. If you want the machine to restart automatically add a Power Control task to the existing job. You can also create a separate job with the restart option. Just copy the job and name it "Install SafeBoot – Force Restart".



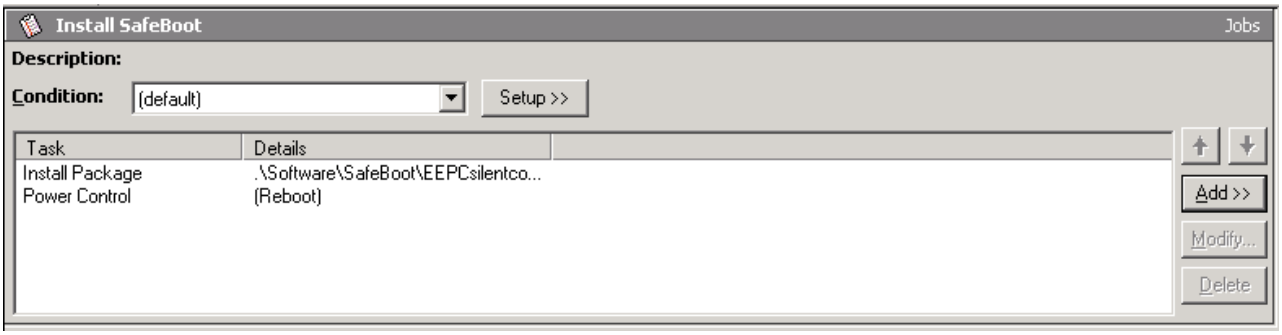
12. If you want to reboot after install, check "Restart" and "Force applications to close without a message". Click "Next".



13. Click “Finish”.



14. Make sure “Power Control” is the second task to be executed in the job.



15. Associate machines with tasks

Manual Deployment

This deployment method should only be used when Altiris NS or Altiris DS cannot be used or if the machine is offline. ***Keep in mind that every machine with MEE must connect to the network at least once to begin the encryption process.***

1. ***For Commercial sites ONLY***, download the installation-file "EEPCsilentcom.exe" from \\01mcsbootna1\packages\ and place it on your Deployment Server.

   For Defense sites ONLY, download the installation-file "EEPCsilsentdef.exe" from \\01mcsbootna2\packages\ and place it on your Deployment Server.

2. Install MEE software on target machine

3. Once complete, reboot machine to begin encryption process.

Uninstall of McAfee Endpoint Encryption

There are two ways to uninstall MEE from a PC. One is to uninstall from the MEE console and the other is to uninstall using the MEE boot CD.

Uninstall for networked machines

For machines that are on the network, and require uninstall of MEE, simply just submit a ticket to the regional service center and an enterprise desktop staff member will associate the uninstall task in the MEE console. The uninstall process is silent with no forced reboot.

Uninstall for off-network machines

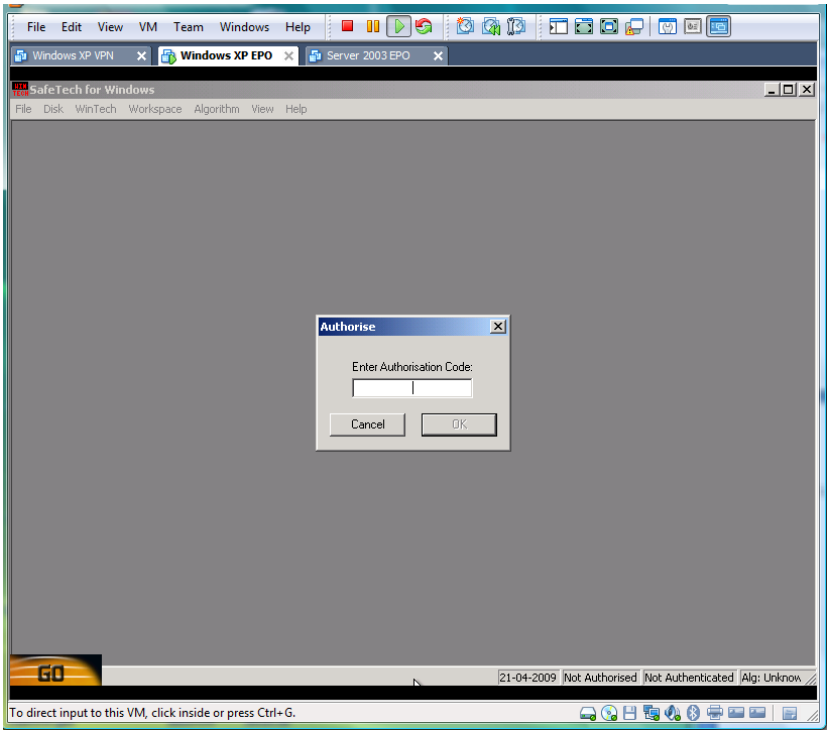
In the event that a machine is off the network, and requires uninstall of MEE, then you must use the following process.

Prerequisites: To uninstall MEE on a machine not attached to the network, ***you must have the Regional McAfee Endpoint Encryption credentials and the McAfee Endpoint Encryption Authorization code****. Both of these can be obtained from the service center.*

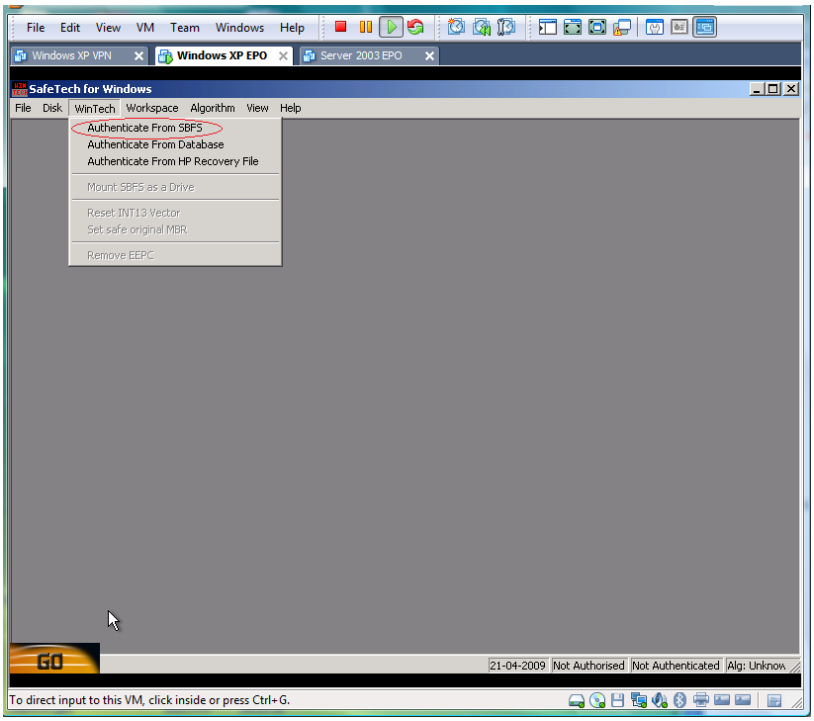
1. Create a Wintech CD from the wintech.iso located on the file share \\10.32.88.55\packages
2. Boot up off of the Wintech CD on the laptop you plan to uninstall MEE from
3. Select "No" when asked if you would like network support

4. Go to the “Go” button at the bottom left of the screen and select “Programs” -> “SafeBoot Wintech”

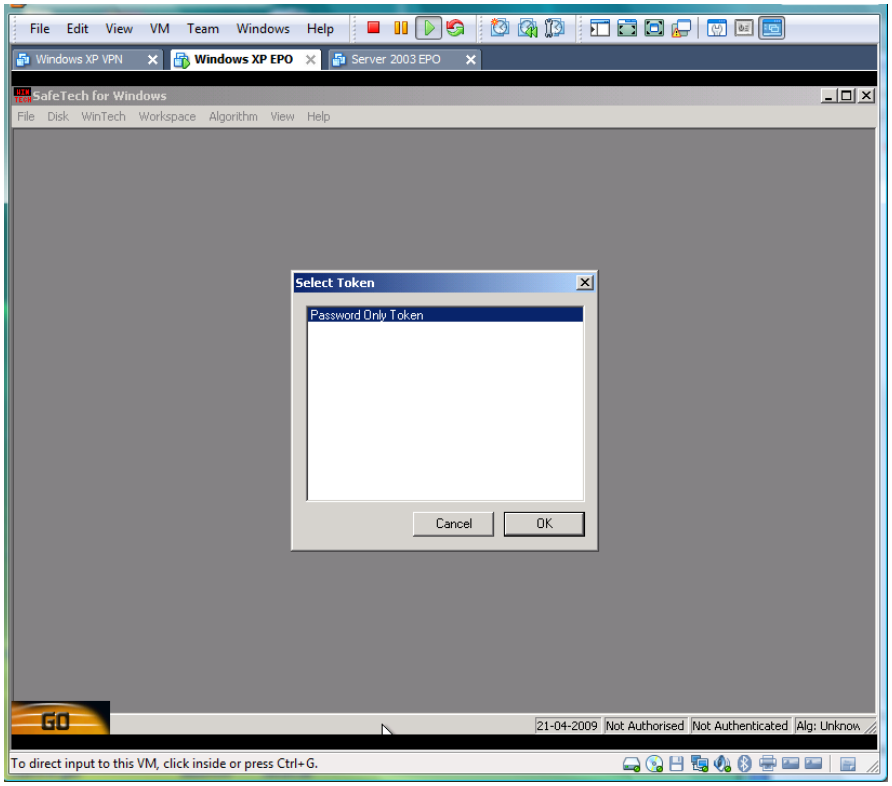
5. Enter in authorization code and click ok



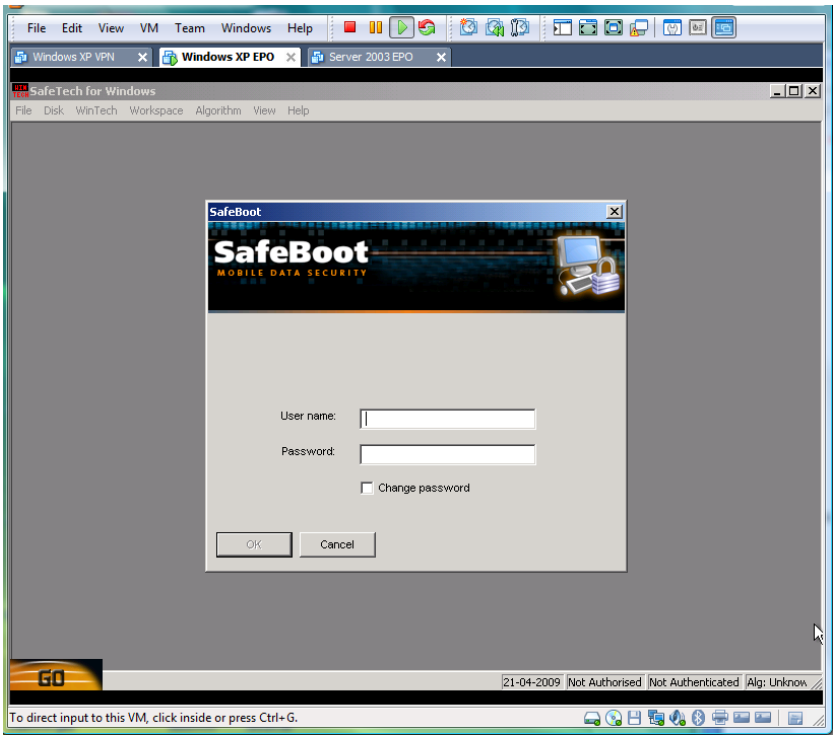
6. Select the “Wintech” menu and choose the “Authenticate From SBFS” option



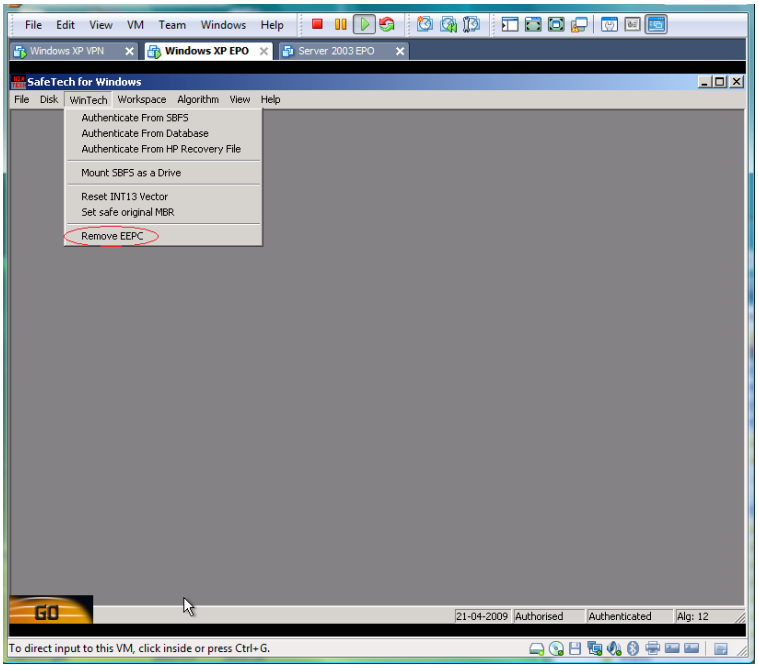
7. Click OK at the Select Token screen



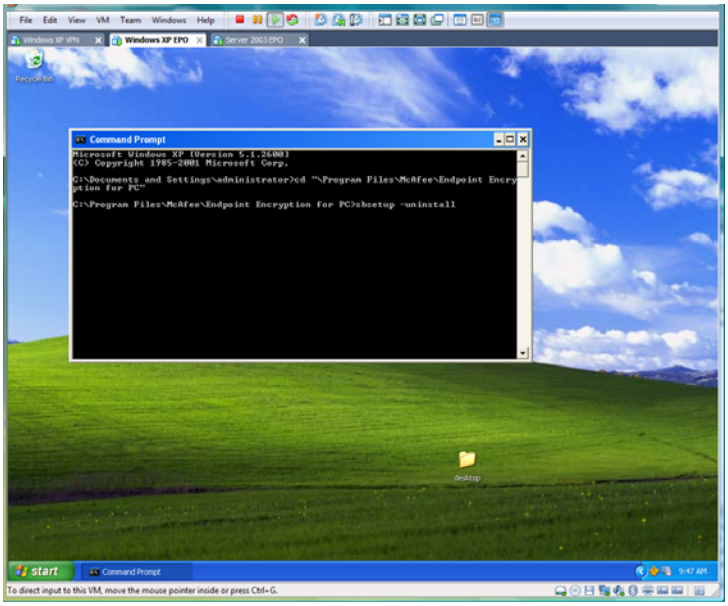
8. Enter your credentials provided for you by the service center



9. The window below on the bottom right should both show authorized and authenticated. Choose the Wintech menu and select the “Remove EEPC” option.

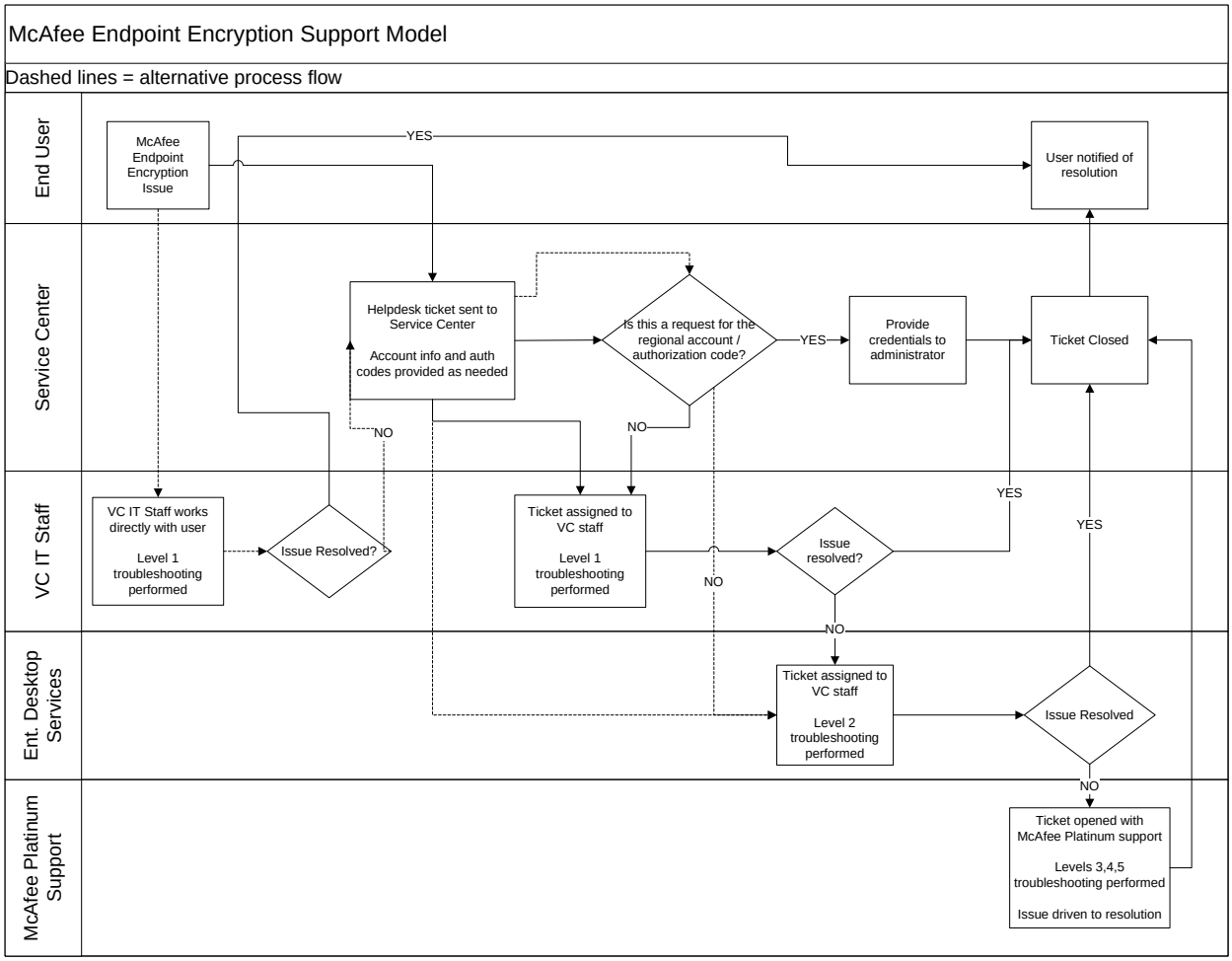


10. After the removal process is complete, disconnect the machine from the network and reboot the machine. After the machine is at the Windows desktop, bring up a command prompt, change directory by typing in cd \"program files\mcafee\endpoint encryption for pc".
11. Type in "sbsetup –uninstall" at the prompt



McAfee Endpoint Encryption Support Model

The support model for all McAfee Endpoint Encryption issues is shown in the flowchart below.



Support Processes

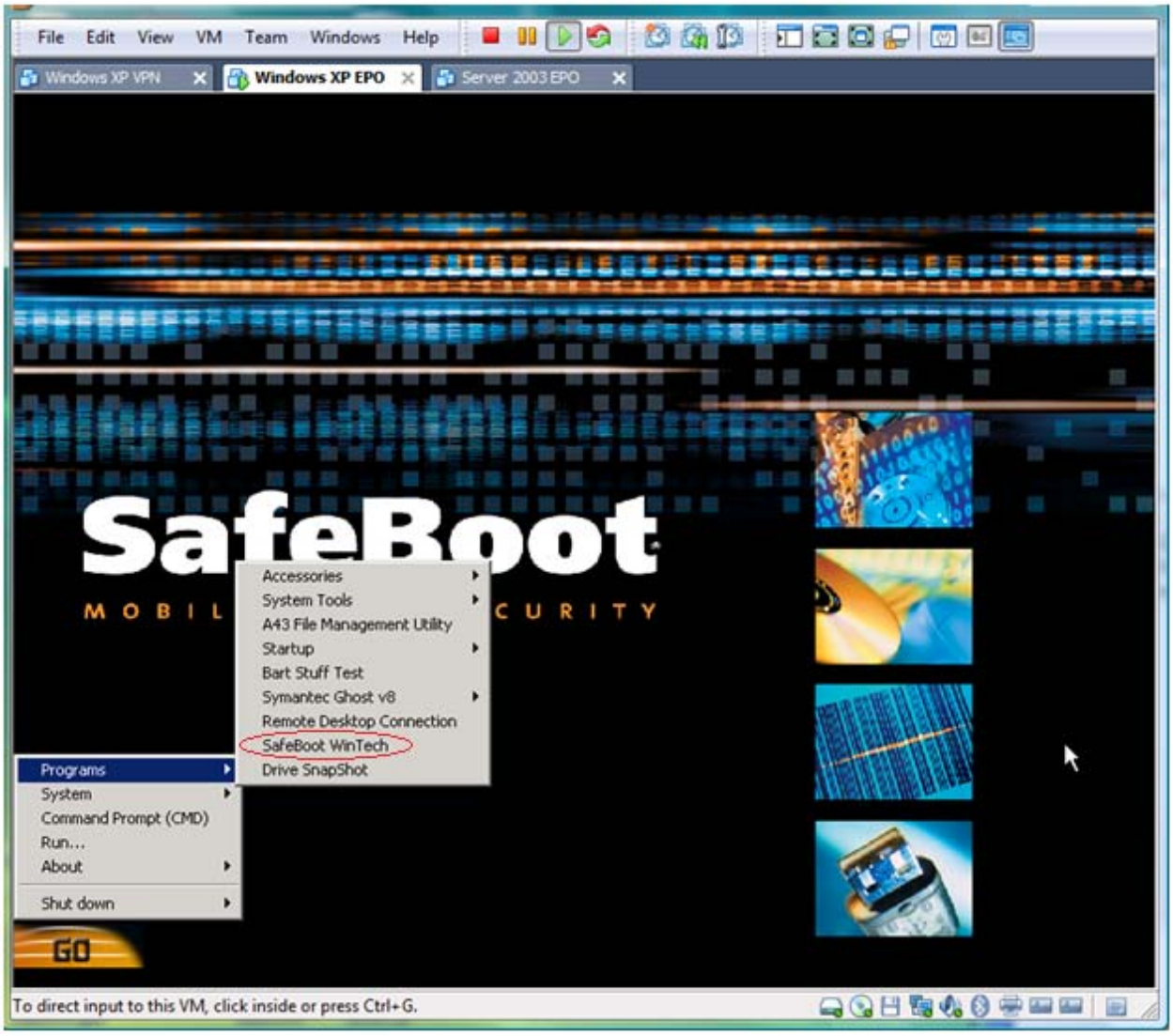
Besides decrypting MEE, there may be scenarios where you need to recover data from the drive. Although rare, the MBR records could become corrupt and need restored. The processes below highlight these support process.

Data recovery

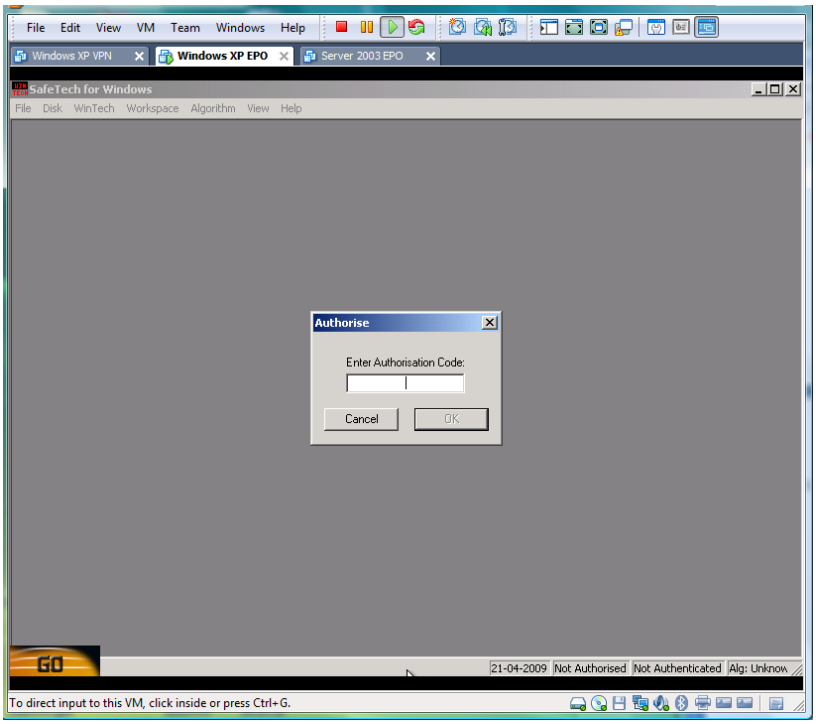
The purpose of this process is to show the VC IT staff how to recover data from a drive encrypted with MEE.

> *Prerequisites: You must have the MEE regional account credentials, the MEE recovery CD, and a external thumb drive to store the recovered data.*

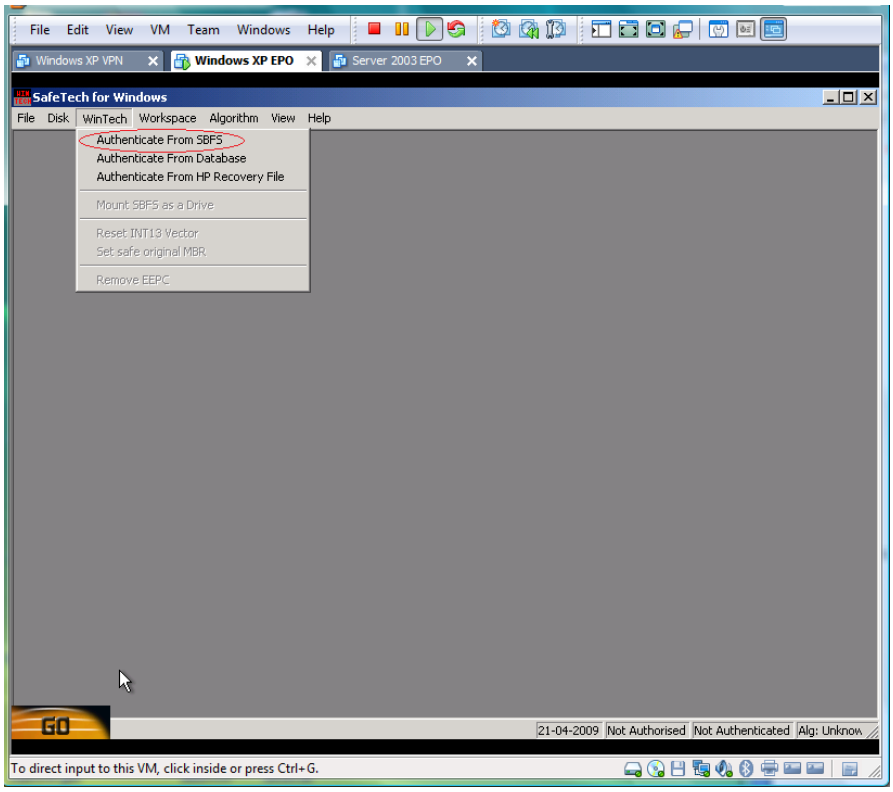
1. Create a Wintech CD from the wintech.iso located on the file share \\10.32.88.55\packages
2. Plug in the USB drive that you wish to use to back up the data onto. This drive must be plugged in before the computer is booted up to be recognized. ***This must be done before you boot using the Wintech CD.***
3. Boot up off of the Wintech CD
4. Select “No” when asked if you would like network support
5. Go to the “Go” button at the bottom left of the screen and select “Programs” -> “SafeBoot Wintech”



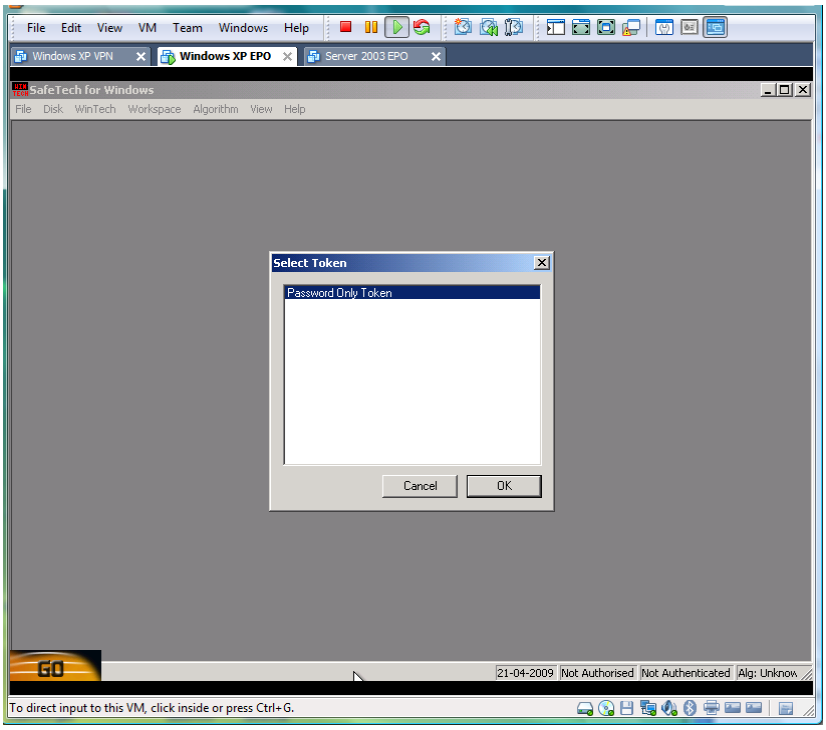
6. Click “Cancel” at the “Enter Authorization Code:” dialogue box



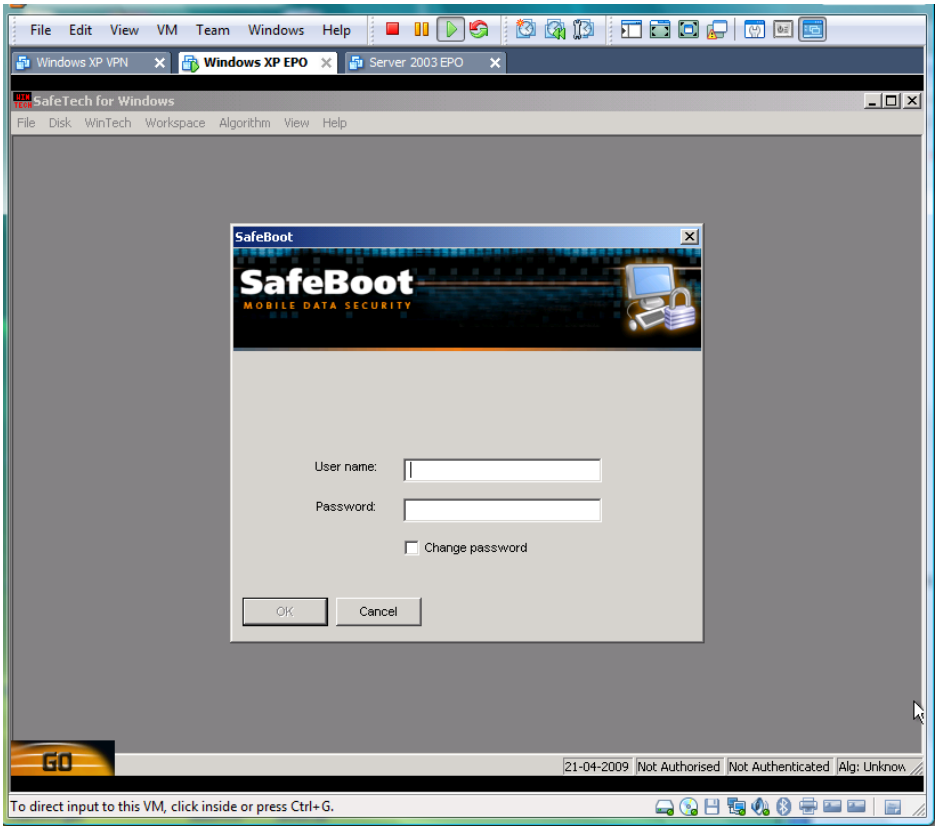
7. Select the “Wintech” menu and choose the “Authenticate From SBFS” option



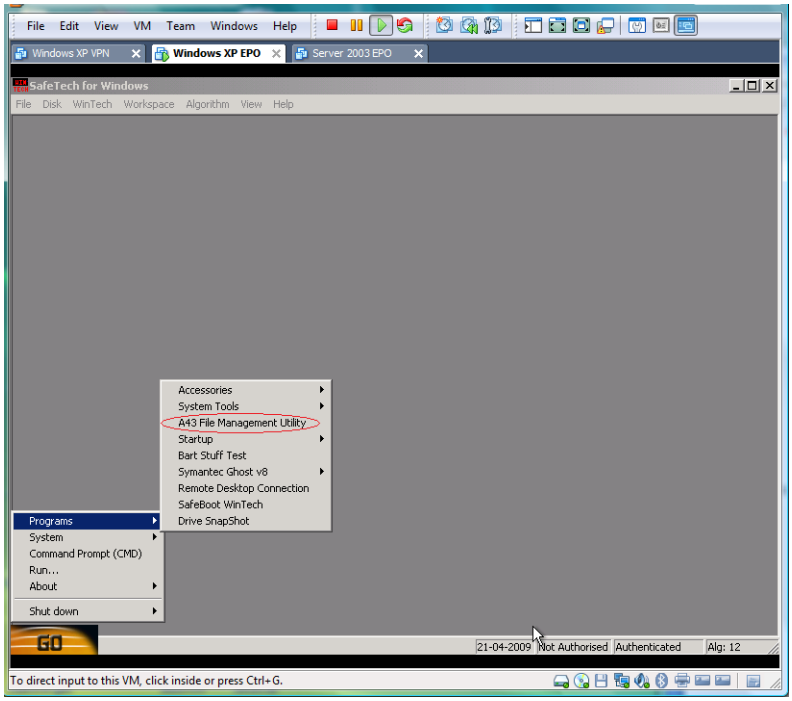
8. Click OK at the Select Token screen



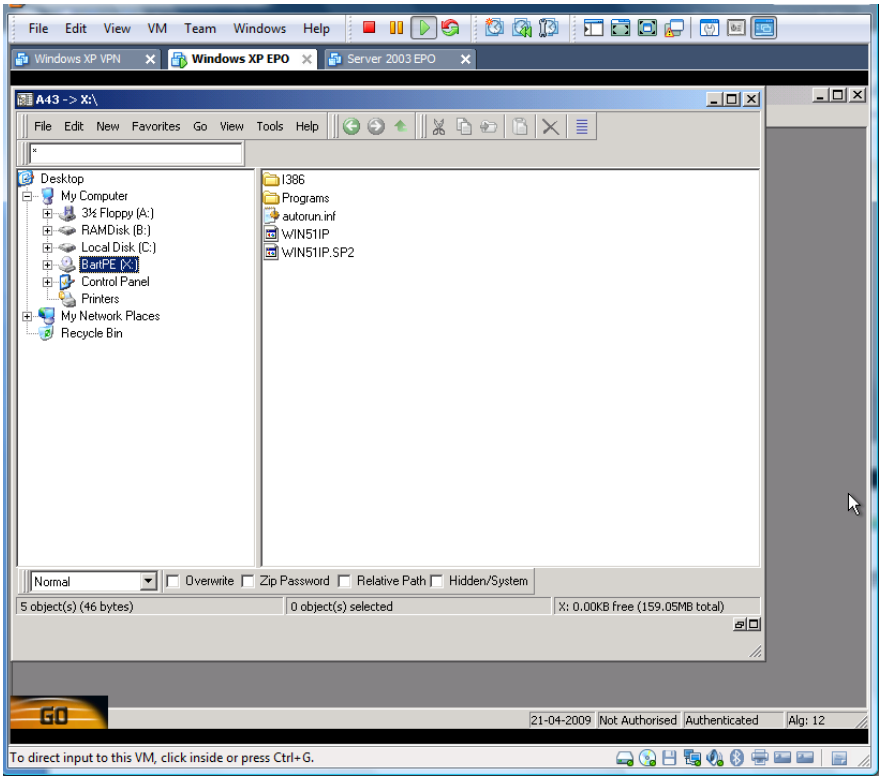
9. Enter your credentials provided for you by the Safeboot administrator



10. Go back to the “Go” button in the bottom left and choose the “A43 File Management Utility”



11. A file management utility would have opened up and the encrypted files should be visible on the C: drive. You can now transfer the files from the C: drive to the external USB drive plugged in.



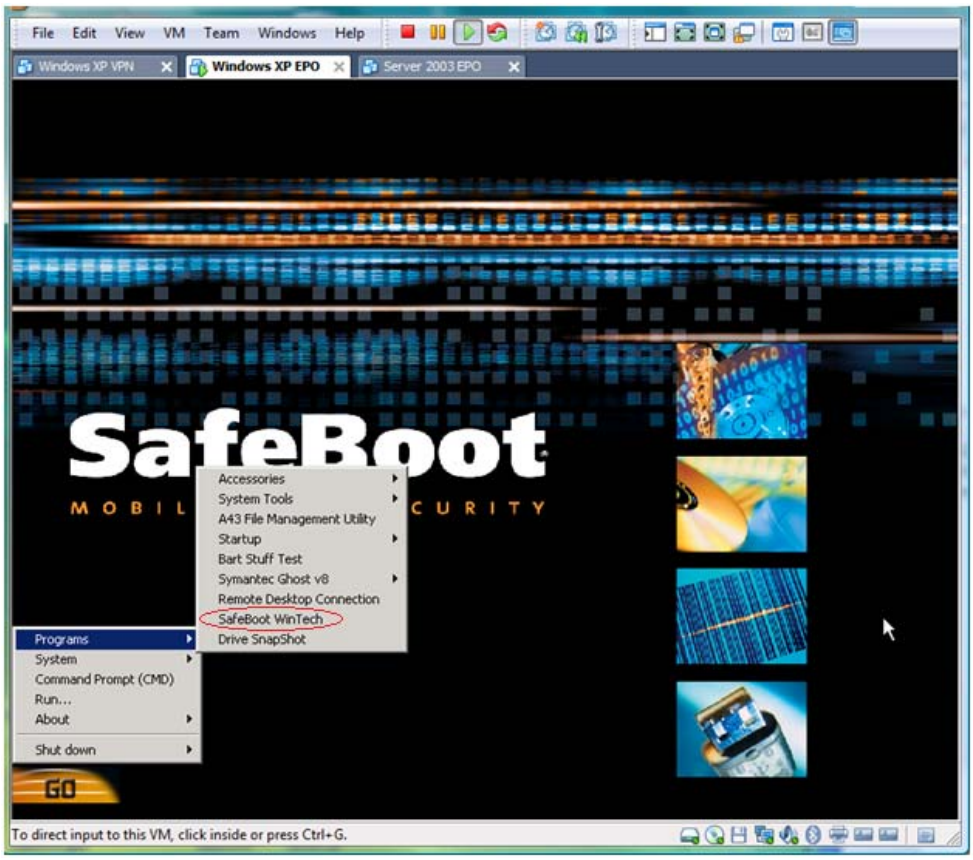
MBR recovery

In rare cases, the MBR file may be corrupted which leaves the laptop useless until restored. The following steps highlight this process.

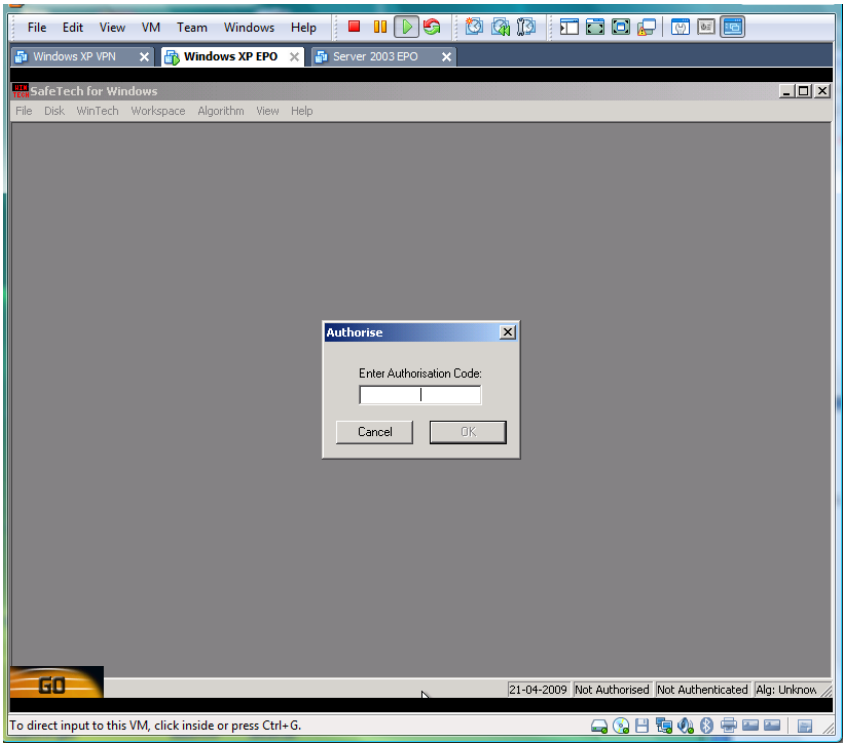
Prerequisites: In order to follow this process you must have the SDB file from the MEE console. This can be obtained by opening a ticket with the service center and the enterprise desktop team will provide this. Be sure to include the machine name in your request. Also, you must have the MEE recovery CD, MEE regional account credentials, and MEE authorization code.

1. Acquire the Database Configuration file (SDB) for the specific machine from the Safeboot Administrator. Put the SDB file onto a flash drive and plug it into the machine that you want to recover the MBR on.
2. Boot up off of the Wintech CD
3. Select “No” when asked if you would like network support

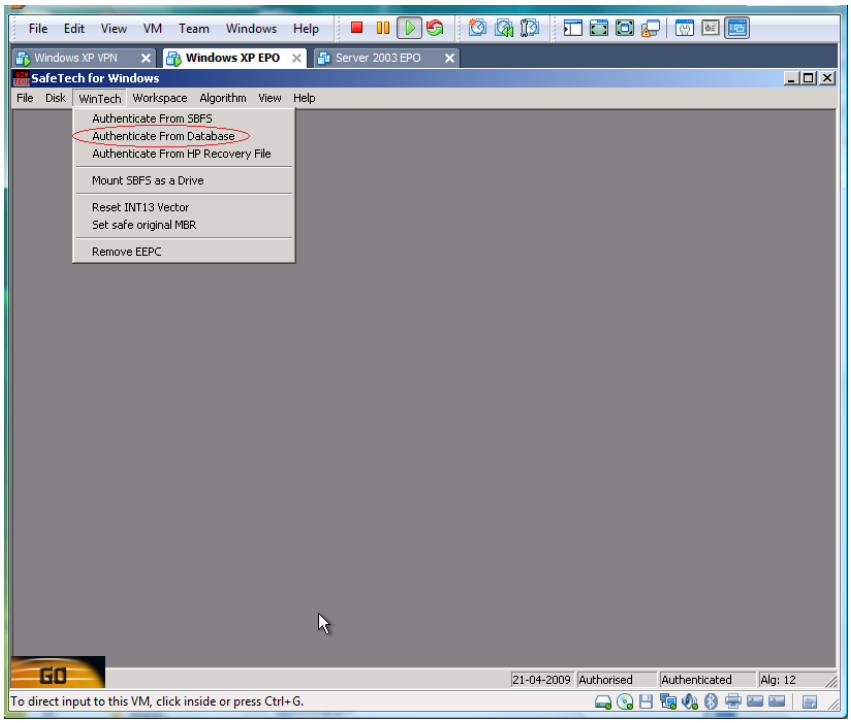
4. Go to the “Go” button at the bottom left of the screen and select “Programs” -> “SafeBoot Wintech



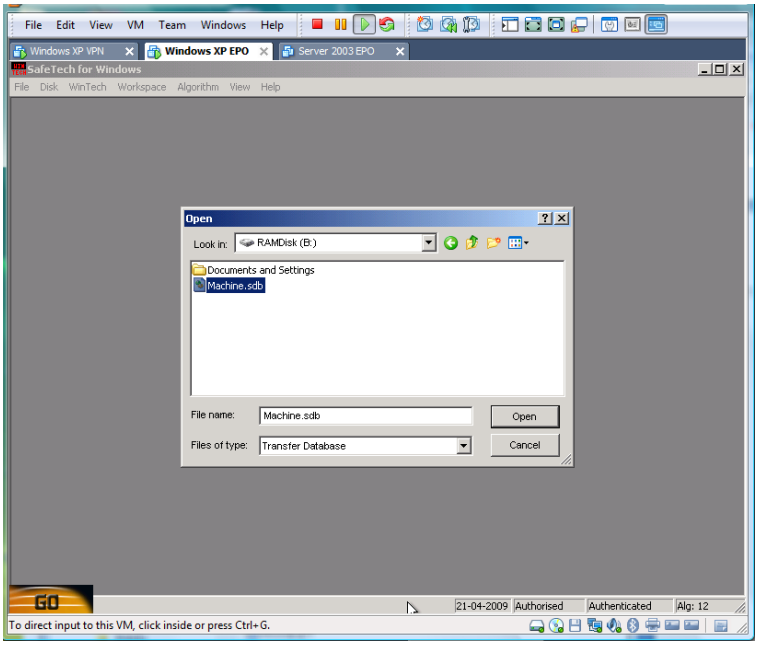
5. Enter the Authorization code provided by the administrator at the “Enter Authorization Code:” dialogue box. This code will change every day



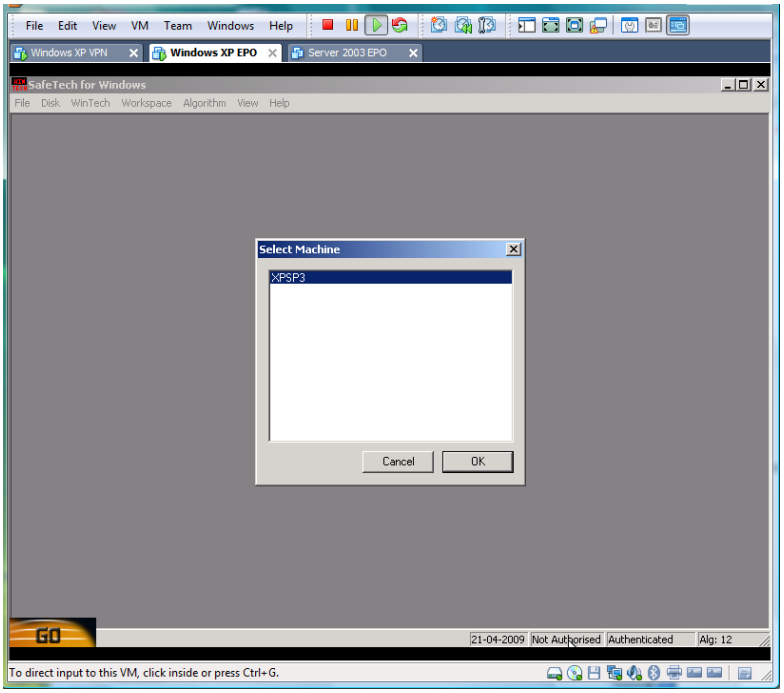
6. Select the “Wintech” menu and choose the “Authenticate From Database” option



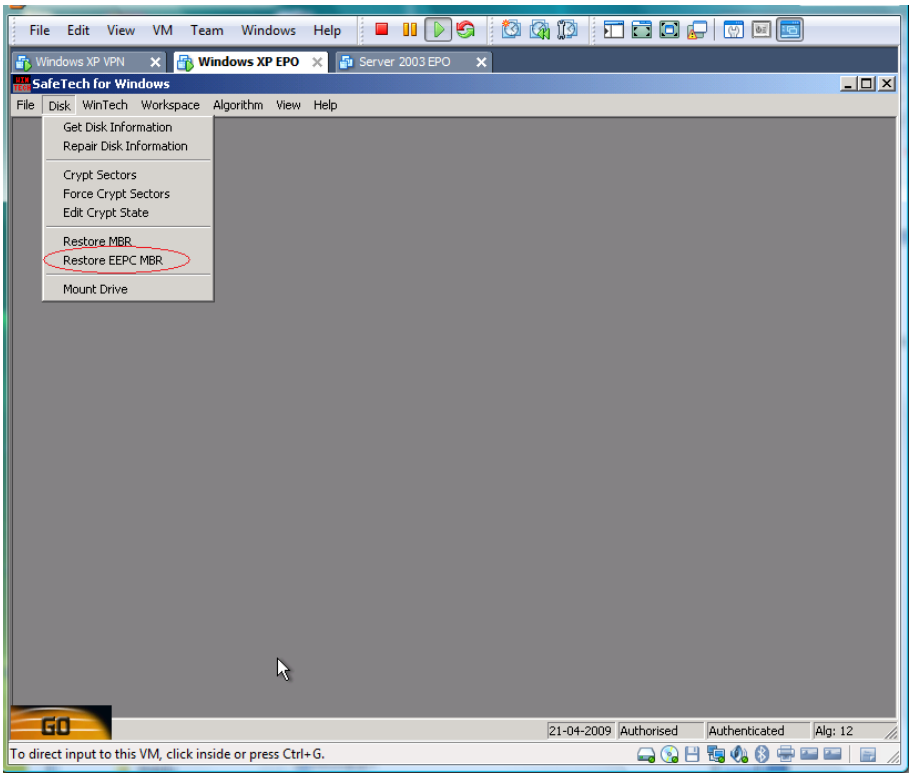
7. Navigate to the SDB file on the external flash drive and click “Open”.



8. Select the correct machine name and click OK



9. Click the “Disk” menu and choose the “Restore EEPC MBR” option



McAfee Endpoint Encryption Frequently Asked Questions

MEE Functionality, Performance, Compatibility

Q: Will the user’s laptop be slow once encryption begins?

A: On laptops that are fairly new (1 – 2 years old) the impact will be minimal to none. For older machines, the impact may be higher and will depend on disk I/O and memory.

Q: If a user shuts down in the middle of encryption, will this crash their system?

A: No, the encryption process can be stopped and started without issue.

Q: Is it possible for an end user to uninstall or stop McAfee Endpoint Encryption?

A: No, MEE encryption services cannot be stopped locally nor can the product be uninstalled without interaction from the MEE console or the recovery CD with proper credentials.

Q: With Pointsec, we were required to prep the drive using defrag and check disk commands. Is this required for MEE?

A: MEE does not require these steps and will detect and skip any sector deemed inadequate.

Q: Can CPU throttling be enforced in the Safeboot product so that performance issues are held to a minimum?
A: Safeboot will rely heavily on disk I/O during encryption and not necessarily CPU. There is no function to throttle disk I/O during encryption.

Q: Are there issues with using Safeboot on solid state drives?
A: Safeboot can be used to encrypt solid state drives however as the drive fills it may slow down.

Q: If Safeboot cannot encrypt Linux devices, are we to continue using Pointsec?
A: We should avoid using Pointsec unless absolutely necessary. Linux comes with an embedded encryption product which can be used until Safeboot is compatible with Linux.

Q: Will credit be given back to the VC for Pointsec licenses bought this year?
A: No although the cost different between Pointsec maintenance and Safeboot maintenance is expected to wash out these costs.

Q: Can Safeboot be embedded in an OS image?
A: No, it is not recommended to embed Safeboot onto an image unless that image will be only used on the same system the image was created from.

Q: Which platforms can Safeboot encrypt?
A: Windows XP 32 bit (not 64 bit), Windows Vista 32 bit and 64 bit

Q: What is the average time to encrypt a system?
A: Testing indicates that encryption time can vary from 2 hours to 10 hours. All of this depends on the size of the drive and performance of disk I/O.

Q: Are there minimum system recommendations?
A: There are not although the older the system, the longer it will take to encrypt initially.

Q: Can Safeboot encrypt thumb drives and other hard drives?
A: Safeboot has the capability to encrypt thumb drives although that function is disabled. Further testing and planning will be required to use this. Secondary hard drive and external SATA hard drives can and will be encrypted by Safeboot.

Q: Will Safeboot encrypt eSATA external drives?
A: Yes.

MEE for Linux

Q: Will MEE encrypt Linux?

A: At this time MEE will not encrypt Linux. The McAfee Technology Roadmap shows this will be available in Q1 of 2010. ITT will investigate more as that timeframe approaches.

MEE Security

Q: There are regional admin accounts and an authorization code needed for the removal of McAfee Endpoint Encryption. What controls are in place to ensure these aren't compromised?

A: The regional admin accounts have complex 12 character passwords that will change every 30 days using randomized algorithms. The McAfee authorization code can only be obtained from authorized ITT personnel who have credentials to access McAfee's service portal.

Traveling Users

Q: For users the travel, what is the best way to encrypt their laptops?

A: Since MEE is simple to deploy, you can deploy MEE to a user's laptop over VPN. Once deployed, the user can reboot and as soon as they re-connect via VPN the encryption process will start.

Pointsec

Q: What is the fastest way to decrypt / uninstall Pointsec?

A: Unfortunately there is no quick way to remove Pointsec from a system. If you can ensure the data on the system is backed up to date, you can reimage the machine. Otherwise, you will need to follow the Pointsec uninstall process which is available on the ITT portal <enter link here>.

MEE Console

Q: Will VC staff have access to the McAfee Endpoint Encryption Console?

A: At this time, the console will be managed by the enterprise desktop staff. As MEE becomes more prevalent in the environment, and requirements become clearer, we will be open to changing this strategy.

MEE Cost

Q: How will maintenance be handled?
A: Maintenance will be charged annually to all systems encrypted with Safeboot. This cost is approximately $5 US dollars per system.

Q: What is the license cost per system?
A: The license cost is approximately $25 USD per system.

Q: I expect my environment to change while conducting this deployment. How will we address this when charging back license costs?
A: The initial scope was generated based on a snapshot of the environment at a point in time. The list used for the initial deployment will be normalized to ensure the VC is only being charged for what was deployed.

ePO / MEE Integration

Q: Will MEE integrate with the ePO console?

A: Currently MEE is a separate product from ePO and does not integrate. The 2010 McAfee Technology Roadmap states the goal is to integrate MEE into ePO however. ITT will revisit this as 2010 approaches.

MEE Misc

Q: Is Safeboot CESG approved for using in Defence UK sites?
A: Yes, Safeboot is CESG approved (http://www.cesg.gov.uk/find_a/cert_products/index.cfm?menuSelected=1&displayPage=152&id=336)

Q: Can Safeboot be installed on a system that has hardware encryption enabled?
A: Conflict with hardware encryption and Safeboot has not been tested. It play it safe, the recommendation is to NOT deploy Safeboot to devices with hardware encryption enabled.

Q: Will site administrators get access to the regional account information to uninstall Safeboot?
A: Yes, ITT site administrators will be allowed to get the regional administrator credentials.

Q: How will you manage the credentials in the Defense Safeboot environment?
A: Defense credentials will be different from Commercial since there are two different Safeboot infrastructures. For additional details on Defense credentials email Brad Marr.

Q: How can I check on the status of MEE on a laptop?

A: In the system tray, there should be an icon which looks like a monitor with a lock over the top

Right click on this icon and select “show status”