



EETech User Guide

# McAfee Endpoint Encryption for PC 7.0

For use with ePolicy Orchestrator 4.6 Software

## **COPYRIGHT**

Copyright © 2012 McAfee, Inc. Do not copy without permission.

## **TRADEMARK ATTRIBUTIONS**

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
	Audience . . . . .	5
	Using this guide . . . . .	5
	What does EETech do . . . . .	6
	Preparing for EETech rescue . . . . .	9
	Understanding the daily authorization code . . . . .	10
	Using EETech . . . . .	10
	Export the recovery information file from McAfee ePO . . . . .	10
<b>2</b>	<b>EETech PE</b>	<b>13</b>
	Add EETech to BartPE V1 Recovery CD/DVD . . . . .	13
	Add EETech to a Microsoft WinPE V3 32-bit CD/DVD . . . . .	15
	Add EEOpalTech to a Microsoft WinPE V3 32-bit CD/DVD . . . . .	22
	Add EETech to a Microsoft WinPE V3 64-bit CD/DVD . . . . .	28
	Authenticate with token . . . . .	32
	Authenticate with recovery file . . . . .	33
	Authorize with daily authorization code . . . . .	34
	Remove EEPC with token and file authentication . . . . .	35
	View the workspace . . . . .	36
	Encrypt or decrypt sectors . . . . .	37
	Restore the Master Boot Record (MBR) . . . . .	39
<b>3</b>	<b>EETech Standalone</b>	<b>41</b>
	Create EETech Standalone bootable disk . . . . .	41
	Create EEOpalTech Standalone bootable disk . . . . .	42
	Boot from EETech and EEOpalTech Standalone boot disks . . . . .	43
	Perform emergency boot . . . . .	44
	Remove EEPC with token authentication . . . . .	45
	View the workspace . . . . .	46
	Encrypt or decrypt sectors . . . . .	47
	Restore the Master Boot Record (MBR) . . . . .	48
<b>4</b>	<b>Glossary</b>	<b>51</b>
	<b>Index</b>	<b>53</b>



# 1

## Introduction

McAfee® Endpoint Encryption for PC (EEPC) delivers powerful encryption that protects data from unauthorized access, loss, and exposure. With data breaches on the rise, it is important to protect information assets and comply with privacy regulations.

EETech (WinPE Version 1 and 3, and BartPE), EEOpalTech (WinPE Version 3), EETech (Standalone), EEOpalTech (Standalone), and EETech UEFI WinPE 4 are McAfee's system recovery tools used in conjunction with EEPC.

EETech (Standalone) and EEOpalTech (Standalone) are system recovery tools that are smaller in size and are available ready-made, and allow the administrator to perform normal recovery functions. EETech (WinPE V1 and V3) and EEOpalTech (WinPE V3) are more capable and possesses A43 file explorer and better USB support, but requires the user to have a WinPE license.

### Contents

- ▶ *Audience*
- ▶ *Using this guide*
- ▶ *What does EETech do*
- ▶ *Preparing for EETech rescue*
- ▶ *Understanding the daily authorization code*
- ▶ *Using EETech*
- ▶ *Export the recovery information file from McAfee ePO*

---

## Audience

This guide is mainly intended for experienced system administrators, security managers, and corporate security administrators. Knowledge of PC boot process (BIOS/MBR and UEFI/GPT), full-disk encryption, and a general understanding of the aims of centrally managed security are required.

---

## Using this guide

This guide helps corporate security administrators to understand the system rescue tools, EETech and EEOpalTech (Standalone) and EETech and EEOpalTech (WinPE). This document includes procedures to recover data from systems that are unrecoverable using endpoint encryption features like self-recovery and administrative recovery.

---

## What does EETech do

EETech is the name given to a family of tools which are used for rescue and disaster-recovery of EEPc systems, which have an error which that makes self or administrative recovery of the system impossible.

These are the examples of reasons why rescue might be necessary:

- The EEPc Pre-Boot File System (PBFS) has become corrupted, preventing authentication in the normal fashion.
- A third party defragmentation tool has been used without suitable exclusions being set, which has moved the PBFS host file, despite the OS locking the file. The PBFS is no longer available to allow authentication to occur in a normal fashion.
- A rootkit has infected the MBR of the system.

There are several differing functions that are provided by the EETech family, and a number of tools which provide a mixture of the functions for different applications. It is recommended that the expert tools listed below are only used by experienced EEPc administrators. For emergency boot purposes, a rudimentary tool (which provides capability for emergency boot only) is provided to allow inexperienced users to perform the rescue.

These expert tools are provided for comprehensive rescue with PE environments (WinPE and BartPE), and might be used on both BIOS and UEFI booting systems.

- EETech (WinPE 3.x and BartPE)
- EEOpalTech (WinPE 3.1 only)
- EETech UEFI (WinPE4)

These expert tools are provided for comprehensive rescue when booting from floppy, CD, or USB stick:

- EETech (Standalone) for software encryption on BIOS based systems
- EEOpalTech (Standalone) for Opal encryption on BIOS based systems
- EETech (UEFI) for software and Opal encryption on UEFI based systems



On UEFI systems, SecureBoot should be disabled in order to use EETech.

These rudimentary tools are provided for performing only emergency boot from floppy, CD, or USB stick:

- EEBoot for software encryption on BIOS based systems
- EEOpalBoot for Opal encryption on BIOS based systems

Functionality is similar between EETech and EEOpalTech. However, since Opal disks are self-encrypting disks, Opal versions of EETech do not include certain features relating to encrypting and decrypting data such as Crypt Sectors and Force Crypt Sectors.



For EEPc, Opal disks are supported only using Advanced Host Controller Interface (AHCI) mode.

Feature	Function	EETech WinPE	EETech Standalone	EEOpalTech WinPE	EEOpalTech Standalone	EEBoot	EEOpalBoot
Emergency boot	<p>Allows you to boot through to Windows by authenticating through EETech instead of the normal PBA.</p> <p>Once successfully booted into Windows, the PBFS will be rebuilt and all user data will be synchronized again from the server.</p> <p>It should be considered as the first-line rescue capability and will resolve the majority of issues.</p>		✓		✓	✓	✓
Retrieve data	<p>Allows you to authenticate (and therefore unlock) the disk within a PE environment and thence copy data off or onto the disk.</p> <p>Useful to pull data off an encrypted drive without requiring to boot from the drive.</p>	✓		✓			
Remove Endpoint Encryption	<p>Allows you to remove Endpoint Encryption from the disk after decrypting the disk. Should not be used in preference to server-initiated removal via policy.</p> <p>Useful if ePO policy fails to be enforced.</p> <p>You are recommended to take a sector level copy of the disk before attempting this operation.</p>		✓		✓		

<b>Feature</b>	<b>Function</b>	<b>EETech WinPE</b>	<b>EETech Standalone</b>	<b>EEOpalTech WinPE</b>	<b>EEOpalTech Standalone</b>	<b>EEBoot</b>	<b>EEOpalBoot</b>
Crypt Sectors	<p>Allows you to manually encrypt or decrypt areas of the disk, ensuring that only areas that are currently not encrypted are allowed to be encrypted, and only areas that are currently encrypted are allowed to be decrypted.</p> <p>It should be considered only if other rescue options have failed, and only once a sector level copy has been made.</p>	✓	✓	✓	✓		
Force Crypt Sectors	<p>Allows you to manually encrypt or decrypt areas of the disk, but does not prevent encrypted areas of the disk from being encrypted (leading to multiple-encryption), or decrypted areas of the disk from being decrypted (leading to multiple-decryption).</p> <p>Since this allows multiple encryption or decryption to be performed, should be considered only as a last resort, and only once a sector level copy has been made.</p>	✓	✓	✓	✓		



Feature	Function	EETech WinPE	EETech Standalone	EEOpalTech WinPE	EEOpalTech Standalone	EEBoot	EEOpalBoot
Repair metadata	<p>Allows you to repair various pieces of EEPK metadata in case of corruption; for example, repairing the Disk Information metadata.</p> <p>Useful in the case of unknown corruption.</p> <p>You are recommended to take a sector level copy of the disk before attempting this operation.</p>		✓		✓		
View metadata	<p>Allows you to read EEPK metadata; for example, view the Disk Keycheck value, which can be used to locate a system key in the McAfee ePO database.</p> <p>Useful in the case that a system has been deleted from McAfee ePO making export of the recovery file impossible without knowing the Keycheck value.</p>	✓	✓	✓	✓		

## Preparing for EETech rescue

EETech contains some powerful rescue tools, and should not be used without proper understanding of how the tools work since some of the tools can damage the data on disks if used without due care and attention.

We recommend that you take time to create and trial the various EETech rescue tools in a test environment to gain familiarity with the tools before a real-life rescue situation occurs.

If in doubt, contact McAfee Support for assistance.

We also strongly recommended that, prior to performing any EETech rescue (with the exception of Emergency Boot), a sector-level copy of the disk is taken as a backup. Should you perform a step which inadvertently damages some of the data on the disk, the backup will allow you to try the rescue again.

---

## Understanding the daily authorization code

In order to prevent unskilled personnel from using the powerful features in EETech, some recovery operations in EETech require authorization. The user authorizes these features by typing a four-digit code into the authorization screen. This daily authorization code is also known as Code of the Day (COD).

Customers can download the code of the day tool from the McAfee website.



All EETech operations require authentication. However, only the administrative operations require authorization with the 4-digit daily authorization code.

The following operations do not require the daily authorization code:

- Viewing and retrieving data from the disk (EETech BartPE only or EETech WinPE V1 only)
- Using the workspace utility to view sectors on the disk
- Using the disk information utility to identify encrypted regions on the disk
- Setting the encryption algorithm used by EETech
- Setting the boot disk on which EETech performs its operations

The following operations do require the daily authorization code:

- Removing Endpoint Encryption (decrypting the disk and restoring the Windows MBR)
- Repairing disk information
- Using the crypt sectors and force crypt sectors utilities to manually encrypt or decrypt specific sectors
- Editing the disk crypt state
- Restoring the MBR
- Performing an emergency boot (feature available in EETech Standalone and EEOpalTech Standalone)

---

## Using EETech

In general, the method for using EETech is as follows:

- Start EETech
- Authenticate, either by providing user credentials or a recovery XML file
- Set the boot disk (if required) to make sure that EETech authenticates the correct disk
- Authorize EETech if the function you are about to perform requires it
- Perform the rescue operation

---

## Export the recovery information file from McAfee ePO

Exporting the recovery information is an optional step. In most recoveries, the administrator can authenticate by simply entering their credentials (or other token data). However, if the PBFS has

become corrupted, it may be impossible to authenticate a user via password or other token in EETech, since the data files containing the user's token data may be corrupted.

In this case, EEPC provides a capability whereby the system's recovery data may be exported to a *plain-text* file, thence taken to the affected system, and used to authenticate the system without EETech needing to access the PBFS.

This section describes how to export the recovery data.



The recovery file contains secret data which will allow access to the encrypted system to which it relates. It must therefore be handled securely, and shredded (not just deleted) from the file system where it is placed once the recovery operation has been completed.

Use this task to export the recovery information file for the desired system from McAfee ePO. Every system that is encrypted using the EEPC software has a recovery information file in McAfee. This file can be used to authenticate the system in EETech. For more information, see the Endpoint Encryption system recovery section in the Product Guide.

### Before you begin

You must have the **Allow export of machine key recovery information** option enabled under **Recovery Options** to perform this task.

### Task

For option definitions, click ? in the interface.

- 1 Insert your choice of removable media, such as floppy disk or USB drive, to the system where McAfee ePO is present.
- 2 Click **Menu | Systems | System Tree** in the McAfee ePO server to open the **Systems** page. Select the desired group under System Tree pane on the left.
- 3 Select the desired system, then click **Actions | Endpoint Encryption | Export Recovery Information**. The **Export Recovery Information** confirmation page appears.
- 4 Click **Yes** to export the recovery information file. The **Export Recovery Information** page appears with the Export information (.xml) file.
- 5 Right-click the .xml file and save it to the inserted removable media such as floppy disk or USB drive.



The Recovery Information file has a general format of the client system name (.xml). Make sure to handle the file securely and shred (not just delete) the file once recovery is completed.

**Introduction**

Export the recovery information file from McAfee ePO

# 2

## EETech PE

EETech PE refers to WinPE and BartPE of versions 1 and 3. EETech can be run in Standalone mode or as a Windows application. When using the EETech Windows application it can be run from PE environments. This provides the administrator a Windows-like environment and allows the administrator to recover data without having to fully decrypt the disk.

Licensing requirements dictate that you must build these tools yourself from your licensed copy of Windows, since license restrictions mean that McAfee are unable to distribute the Windows components required.



It is entirely the responsibility of the qualified system administrators and security managers to take appropriate precautions while using EETech (PE V1 and V3) recovery tool. EETech provides very low level control of the disk and administrative error when using this tool can result in the loss of data. We recommend that only experienced administrators work with EETech.

Make sure that you do not restart the client system when EETech is decrypting the disk while running from a PE environment. For more information, refer to this KnowledgeBase article <https://kc.mcafee.com/corporate/index?page=content&id=KB74056>.

### Contents

- ▶ *Add EETech to BartPE V1 Recovery CD/DVD*
- ▶ *Add EETech to a Microsoft WinPE V3 32-bit CD/DVD*
- ▶ *Add EEOpalTech to a Microsoft WinPE V3 32-bit CD/DVD*
- ▶ *Add EETech to a Microsoft WinPE V3 64-bit CD/DVD*
- ▶ *Authenticate with token*
- ▶ *Authenticate with recovery file*
- ▶ *Authorize with daily authorization code*
- ▶ *Remove EEPC with token and file authentication*
- ▶ *View the workspace*
- ▶ *Encrypt or decrypt sectors*
- ▶ *Restore the Master Boot Record (MBR)*

---

## Add EETech to BartPE V1 Recovery CD/DVD

Bart's PE Builder helps you build a "BartPE" (Bart Pre-installed Environment) bootable Windows CD/DVD from the original Windows XP Operating System.

Before you create the BartPE, you need to have the Windows XP \i386 folder. The i386 folder holds the files used to install, repair, modify, update, and rebuild Windows. This can be found on the root directory of a Windows XP Professional installation CD.



This section is applicable for bootable CD/DVD and not for USB drives.

EETech is a Windows application that can be added to BartPE using the BartPE plug-in architecture. When the user boots the unrecoverable system with BartPE, the first page that appears is the Endpoint Encryption interface.

This is followed by a dialog box that prompts the user to start network services. You can start the network services if you have added the drivers for your Ethernet card to the BartPE build, otherwise click **No**.

### Task

- 1 Download the latest **BartPe** install file.



Refer to <http://www.nu2.nu/pebuilder/> website for the required information and download links.

- 2 Install **BartPe** to the default install locations of your local system.
- 3 Open Microsoft Windows Explorer and navigate to the **\pebuilderxxxxx\plugin** folder.



**xxxxx** denotes the version number of BartPE.

- 4 Extract **EETech.zip** to the desired location. Copy **Win32** folder from **EETechWinPE** folder to the **\pebuilderxxxxx\plugin** folder.
- 5 Create a subfolder called **EEPC** inside the **\pebuilderxxxxx** folder.
- 6 Copy the **i386** folder to the root drive **C:\**.
- 7 Launch **BartPe**. The **BartPE CD/DVD Builder** page appears.
- 8 Type or browse to the path for the Windows installation files (**i386** folder) in the **C:\** drive.
- 9 Type or browse to the path to include other files and folders from this directory in the **Custom** field.
- 10 Type a folder name, for instance, **EEPC** in the Output field to store the files that PE Builder copies. Make sure that the location you type is relative to your **\pebuilder** directory.



If you need to specify an absolute path, you must change the **EEPC** path absolute in the **Builder | Options** dialog.

- 11 Use the **Media output** pane to specify whether you want to create a BartPE or an **ISO image**.



You can click the **Plugins** button to add, edit, enable/disable, configure or remove plugins from the list.

- 12 Click **Build** to write the ISO image to a BartPE.



When you select the **Burn to CD/DVD** option, it directly writes the ISO image to the inserted BartPE. You can also create the ISO image and burn it to a BartPE later.

- 13 Boot the system from the **EETech WinPE V1 Recovery CD/DVD**. The **Endpoint Encryption** interface appears.
- 14 Click **Go | Programs | McAfee EETech**. The **McAfee EETech** page appears.

## Add EETech to a Microsoft WinPE V3 32-bit CD/DVD

Use this task to create a bootable WinPE recovery CD/DVD from the Windows 7 Operating System. To do this, you need to configure a WinPE 3.0 to include the plug-in for EEPC, which supports the x86 (32-bit) architecture.

### Before you begin

The following information is intended for System Administrators when modifying the registry details:

- Registry modifications are irreversible and if done incorrectly can cause system failure.
- We recommend that you back up your registry and understand the restore process, before you proceed with the registry modification. For more information, see <http://support.microsoft.com/kb/256986>.
- Make sure that you do not run a .REG file, which is not considered to be a genuine registry import file.
- Make sure not to combine the 32-bit and 64-bit architectures.

### Task

- 1 Download Windows Automated Installation Kit (AIK) for Windows 7 from the Microsoft website.
- 2 Install AIK on Windows 7 (32-bit) Operating System either by burning it to a CD/DVD or extracting it using WinRAR. The WinPE 3.0 is setup.
- 3 Click **Windows | All programs | Microsoft Windows AIK | Deployment Tools** and run Deployment Tools as Administrator to open the Deployment Tools command prompt.

- 4 Run the `copype.cmd` command.

Syntax: `copype.cmd <architecture> <destination>`

Where

- `<architecture>` can be x86, amd64, or ia64
- `<destination>` is a path to the local directory

Open this path `C:\Program Files\Windows AIK\Tools\PETools`

and enter this command `copype.cmd x86 C:\winpe_x86`

This command creates the required directory structure and copies all the necessary files for that architecture.

- 5 Open the command prompt and mount the *Windows PE image (Winpe.wim)* base to the Mount directory to access the WinPE 3.0 image.

Open this path `C:\Program Files\Windows AIK\Tools\x86\Serviceing`

and enter this command `Dism.exe /Mount-Wim /WimFile:C:\winpe_x86\winpe.wim /index:1 /MountDir:C:\winpe_x86\mount`

- 6 Edit the WinPE 3.0 environment as follows:
  - a Open regedit and load the system hive under **[HKEY\_LOCAL\_MACHINE]**.
  - b Click **HKEY\_LOCAL\_MACHINE, File, and Load Hive**. The Load Hive pop-up appears.
  - c From the mounted WinPE image, navigate to this system file `C:\winpe_x86\mount\ Windows\System32\Config\SYSTEM`.

- d Name the WinPE hive; for instance pe3.
- e Access this Registry entry [HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}].
- f Edit the multi-string upper filters with values in the specified order:
  - MfeEpePC**
  - PartMgr**
- g Right click HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services and create the **MfeEpePC** and **MfeEEAlg** keys.



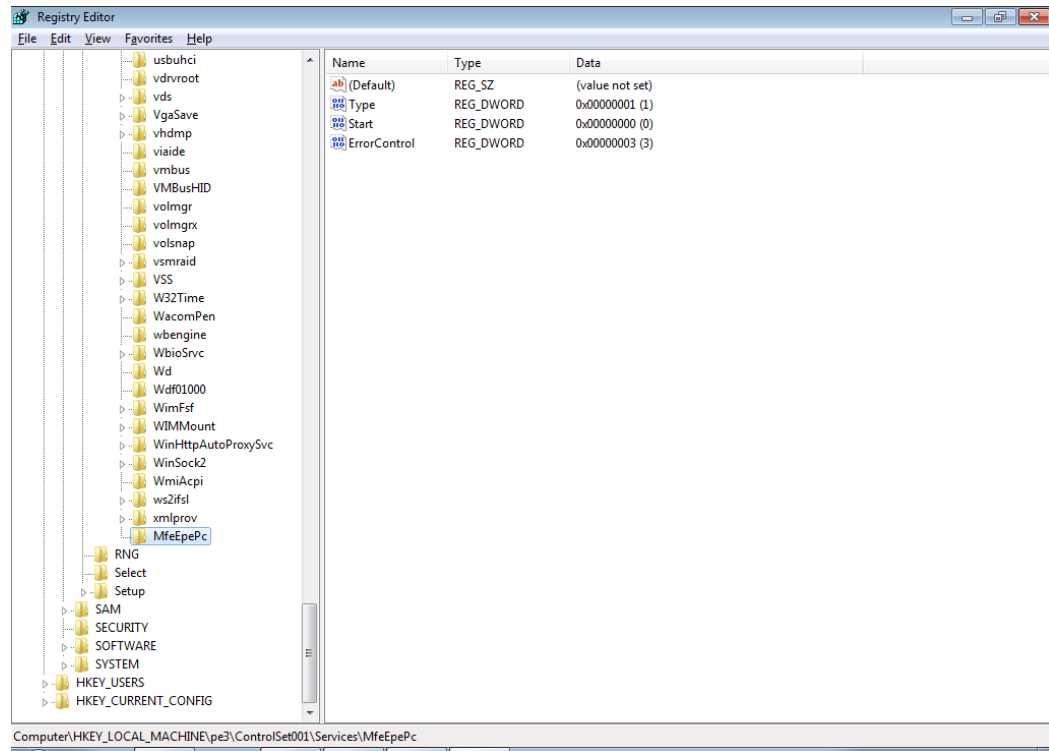
h Modify the values of the created keys as follows:

- [HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services\MfeEpePC]

**"Type"=dword:00000001**

**"Start"=dword:00000000**

**"ErrorControl"=dword:00000003**



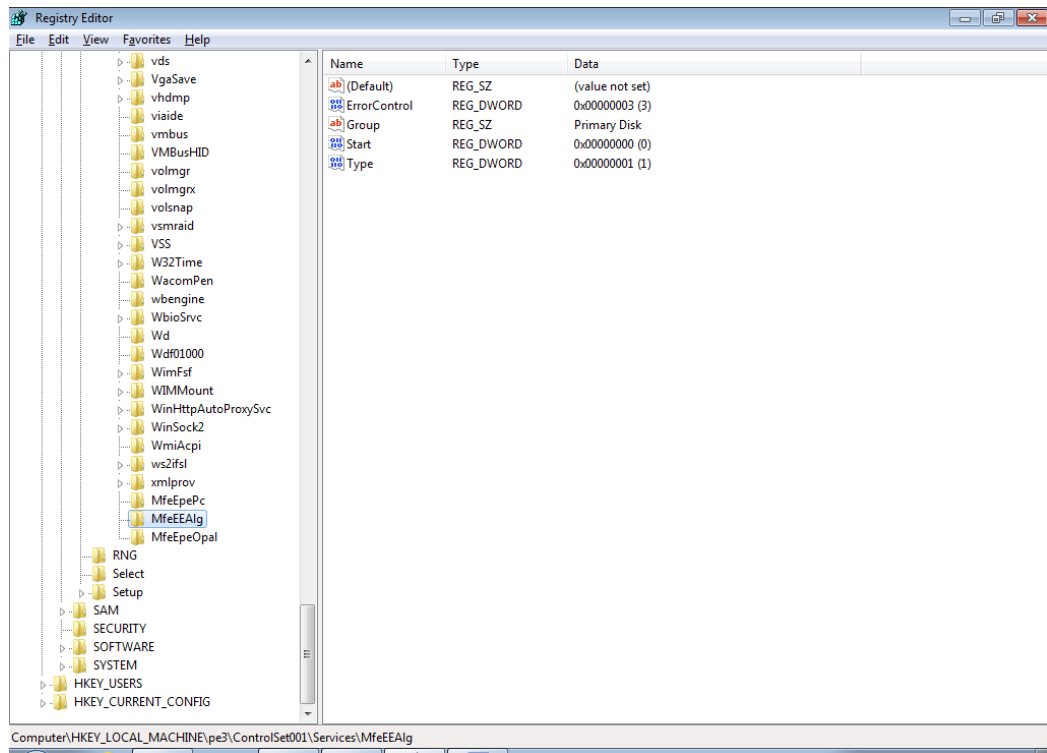
- [HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services\MfeEEAlg]

**"Type"=dword:00000001**

**"Start"=dword:00000000**

**"ErrorControl"=dword:00000003**

**"Group"=string:Primary Disk**



- i Click pe3, then click **File | Unload hive** to unload the WinPE mounted hive.

- j Close the Registry Directory.
- k Add the EEPK files to appropriate locations in the mounted WinPE image as mentioned in the following tables.



Before you copy the files, you need to create folders as follows:

**Table 2-1 Folders to be created**

Location	Folder to be created
C:\Winpe_x86\mount\Program Files\	Endpoint Encryption
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	EpeReaders
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	EpeTokens
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	Locale
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	Theme

Copy the following EEPK files into the image from the Win32 folder found in the build.

**Table 2-2 Files to be copied**

Location	Files to be copied
C:\Winpe_X86\mount\Windows\System32\Drivers\	MfeEpePC.sys MfeEEAlg.sys
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	EETech.exe
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\EpeReaders	EpeReaderPcsc.dll
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\EpeTokens	EpeTokenPassword.dll EpeTokenSmartcard.dll
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\Locale	Locale.xml

**Table 2-2 Files to be copied** *(continued)*

Location	Files to be copied
C:\Winpe_x86\mount\Program Files \Endpoint Encryption\Locale \English-US	Please use the Language of your choice. e.g. English-US Core-0409.xml Tech-0409.xml
C:\Winpe_x86\mount\Program Files \Endpoint Encryption\Theme	Background.png BootManager.xml CJK_Tahoma12.pbf CJK_Tahoma8.pbf CJK_Tahoma8B.pbf EpeTechAuthorize.xml EpeTechCryptSectors.xml EpeTechDiskInfo.xml EpeTechEditCryptList.xml EpeTechEditRegion.xml EpeTechFilePicker.xml EpeTechMainWnd.xml EpeTechRemoveEpe.xml EpeTechSectorPicker.xml EpeTechSelectAlg.xml EpeTechSetBootDisk.xml EpeTechWorkspace.xml EpeTechRestoreMBR.xml ErrorMessageBox.xml Language.xml LatinASCII_Tahoma12B.pbf LatinASCII_Tahoma18B.pbf LatinASCII_Tahoma8.pbf LatinASCII_Tahoma8B.pbf Logon.xml LogonBanner.png MessageBox.xml Modules.xml NewPassword.xml OsLogon.xml OsNewPassword.xml PasswordToken.xml Progress.xml QAEnrolWizard.xml QaEnrolWizardBanner.png

**Table 2-2 Files to be copied** *(continued)*

Location	Files to be copied
	RecoverLocal.xml
	RecoverLocalBanner.png
	RecoverRemote.xml
	RecoverRemoteBanner.png
	RecoveryType.xml
	RecoveryTypeBanner.png
	SelectUser.xml
	SelectUserBanner.png
	Tech-0409.xml
	Theme.xml
	TimeoutDialog.xml
	TokenInit.xml
	TokenSelect.xml



Make sure to close all Windows Explorer windows and clear the Recycle Bin.

7 Commit the changes in this path `C:\Program Files\Windows AIK\Tools\x86\Servicing` by performing these steps:

- a To commit changes to WIM, enter this command `Dism.exe /Unmount-Wim /MountDir:C:\winpe_x86\mount\ /Commit`
- b To copy the new WIM image to boot ISO, enter this command `copy C:\winpe_x86\winpe.wim C:\winpe_x86\ISO\sources\boot.wim /Y`
- c To create a bootable iso image, enter this command `oscdimg -n -bc:\winpe_x86\etfsboot.com C:\winpe_x86\ISO C:\winpe_x86\winpe_x86.iso`

The iso for WinPE3 32-bit for EETech can be found at `C:\winpe_x86\winpe_x86.iso`

8 Burn this iso to a CD/DVD and boot the system from the CD/DVD.



Make sure that you do not boot the system from WinPE V3 CD/DVD when the decryption is in progress.

9 In the command prompt, enter these commands:

```
cd\
cd Program Files\Endpoint Encryption
EETech.exe
```

The EETech screen appears.

## Add EEOpaTech to a Microsoft WinPE V3 32-bit CD/DVD

Use this task to create a bootable EEOpaTech WinPE V3 32-bit recovery CD/DVD from the Windows 7 Operating System. To do this, you need to configure WinPE 3.0 to include the Opal plug-in for EEPC, which supports only the x86 (32-bit) architecture.

### Before you begin

The following information is intended for System Administrators when modifying the registry details:

- Registry modifications are irreversible and if done incorrectly can cause system failure.
- We recommend that you back up your registry and understand the restore process, before you proceed with the registry modification. For more information, see <http://support.microsoft.com/kb/256986>.
- Make sure that you do not run a .REG file, which is not considered to be a genuine registry import file.

### Task

- 1 Download Windows Automated Installation Kit (AIK) for Windows 7 from the Microsoft website.
- 2 Install AIK on Windows 7 (32-bit) Operating System either by burning it to a CD/DVD or extracting it using WinRAR. The WinPE 3.0 is setup.
- 3 Click **Windows | All programs | Microsoft Windows AIK | Deployment Tools** and run Deployment Tools as Administrator to open the Deployment Tools command prompt.

- 4 Run the `copype.cmd` command.

Syntax: `copype.cmd <architecture> <destination>`

Where `<architecture>` can be `x86`, `amd64`, or `ia64` and

`<destination>` is a path to the local directory.

Open this path `C:\Program Files\Windows AIK\Tools\PETools`

and enter this command `copype.cmd x86 C:\winpe_x86`

This command creates the required directory structure and copies all the necessary files for that architecture.

- 5 Open the command prompt and mount the *Windows PE image (Winpe.wim)* base to the Mount directory to access the WinPE 3.0 image.

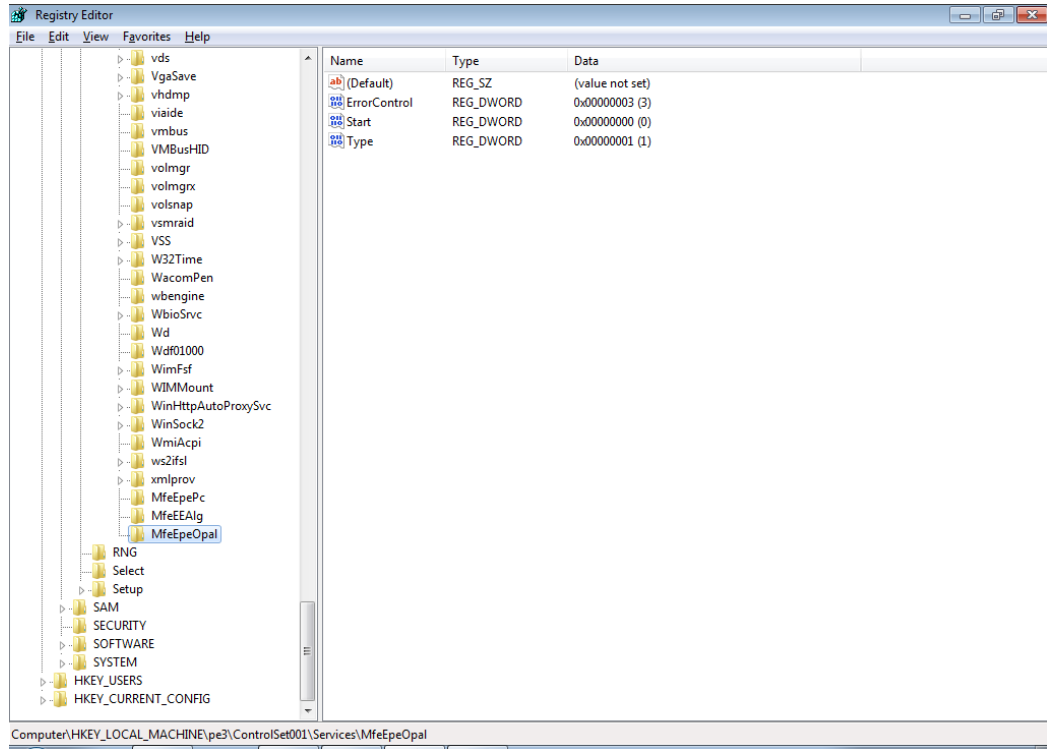
Open this path `C:\Program Files\Windows AIK\Tools\x86\Serviceing`

and enter this command `Dism.exe /Mount-Wim /WimFile:C:\winpe_x86\winpe.wim /index:1 /MountDir:C:\winpe_x86\mount`

- 6 Edit the WinPE 3.0 environment as follows:
  - a Open `regedit` and load the system hive under `[HKEY_LOCAL_MACHINE]`.
  - b Click `HKEY_LOCAL_MACHINE`, `File`, and `Load Hive`. The Load Hive pop-up appears.
  - c From the mounted WinPE image, navigate to this system file `C:\winpe_x86\mount\ Windows\System32\Config\SYSTEM`.
  - d Name the WinPE hive; for instance `pe3`.

- e Access this Registry entry [HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}].
- f Edit the multi-string upper filters with values:
  - MfeEpeOpal**
  - MfeEpePC**
  - PartMgr**
- g Right click HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services and create the **MfeEpeOpal**, **MfeEpePC** and **MfeEEAlg** keys.

- h Modify the values of the created keys as follows:
- **[HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services\MfeEpeOpal]**  
**"Type"=dword:00000001**  
**"Start"=dword:00000000**  
**"ErrorControl"=dword:00000003**



- **[HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services\MfeEpePC]**  
**"Type"=dword:00000001**  
**"Start"=dword:00000000**  
**"ErrorControl"=dword:00000003**
  - **[HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services\MfeEEAlg]**  
**"Type"=dword:00000001**  
**"Start"=dword:00000000**  
**"ErrorControl"=dword:00000003**  
**"Group"=string:Primary Disk**
- i Click pe3, then click File | Unload hive to unload the WinPE mounted hive.



- j Close the Registry Directory.
- k Add the EEPK files to appropriate locations in the mounted WinPE image as mentioned in the following tables.



Before you copy the files, you need to create folders as follows:

**Table 2-3 Folders to be created**

Location	Folder to be created
C:\Winpe_x86\mount\Program Files\	Endpoint Encryption
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	EpeReaders
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	EpeTokens
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	Locale
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	Theme

Copy the following EEPK files into the image from the Opal folder found in the build.

**Table 2-4 Files to be copied**

Location	Files to be copied
C:\Winpe_X86\mount\Windows\System32\Drivers\	MfeEpeOpal.sys MfeEpePC.sys MfeEEAlg.sys
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\	EEOpalTech.exe EpeOpalATASec4SATA.dll
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\EpeReaders	EpeReaderPcsc.dll
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\EpeTokens	EpeTokenPassword.dll EpeTokenSmartcard.dll
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\Locale	Locale.xml

**Table 2-4 Files to be copied** *(continued)*

Location	Files to be copied
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\Locale\English-US	Please use the Language of your choice, for example, English-US Core-0409.xml Tech-0409.xml
C:\Winpe_x86\mount\Program Files\Endpoint Encryption\Theme	Background.png BootManager.xml CJK_Tahoma12.pbf CJK_Tahoma8.pbf CJK_Tahoma8B.pbf EpeTechAuthorize.xml EpeTechCryptSectors.xml EpeTechDiskInfo.xml EpeTechEditCryptList.xml EpeTechEditRegion.xml EpeTechFilePicker.xml EpeTechMainWnd.xml EpeTechRemoveEpe.xml EpeTechSectorPicker.xml EpeTechSelectAlg.xml EpeTechSetBootDisk.xml EpeTechWorkspace.xml EpeTechRestoreMBR.xml ErrorMessageBox.xml Language.xml LatinASCII_Tahoma12B.pbf LatinASCII_Tahoma18B.pbf LatinASCII_Tahoma8.pbf LatinASCII_Tahoma8B.pbf Logon.xml LogonBanner.png MessageBox.xml Modules.xml NewPassword.xml OsLogon.xml OsNewPassword.xml PasswordToken.xml Progress.xml QANrolWizard.xml

**Table 2-4 Files to be copied** (continued)

Location	Files to be copied
	QaEnrolWizardBanner.png
	RecoverLocal.xml
	RecoverLocalBanner.png
	RecoverRemote.xml
	RecoverRemoteBanner.png
	RecoveryType.xml
	RecoveryTypeBanner.png
	SelectUser.xml
	SelectUserBanner.png
	Tech-0409.xml
	Theme.xml
	TimeoutDialog.xml
	TokenInit.xml
	TokenSelect.xml



Make sure to close all Windows Explorer windows and clear the Recycle Bin.

**7** Commit the changes in this path `C:\Program Files\Windows AIK\Tools\x86\Servicing` by performing these steps:

- a** To commit changes to WIM, enter this command `Dism.exe /Unmount-Wim /MountDir:C:\winpe_x86\mount\ /Commit`
- b** To copy the new WIM image to boot ISO, enter this command `copy C:\winpe_x86\winpe.wim C:\winpe_x86\ISO\sources\boot.wim /Y`
- c** To create a bootable iso image, enter this command `oscdimg -n -bc:\winpe_x86\etfsboot.com C:\winpe_x86\ISO C:\winpe_x86\winpe_x86.iso`

The iso for WinPE3 32-bit for EEOpalTech can be found at `C:\winpe_x86\winpe_x86.iso`

**8** Burn this iso to a CD/DVD and boot the system from the CD/DVD.

**9** In the command prompt, enter these commands:

```
cd\
cd Program Files\Endpoint Encryption
EEOpalTech.exe
```

The McAfee EETech (Opal) screen appears.

## Add EETech to a Microsoft WinPE V3 64-bit CD/DVD

Use this task to create a bootable WinPE recovery CD/DVD from the Windows 7 (64-bit) Operating System. To do this, you need to configure a WinPE 3.0 to include the 64-bit plug-in for EEPC.

### Before you begin

The following are the pre-requisites that you must know before you create the WinPE 64-bit CD/DVD:

- Registry modifications are irreversible and if done incorrectly can cause system failure.
- We recommend that you back up your registry and understand the restore process, before you proceed with the registry modification. For more information, see <http://support.microsoft.com/kb/256986>.
- Make sure that you do not run a .REG file, which is not considered to be a genuine registry import file.
- Make sure that you do not combine the 32-bit and 64-bit architectures.
- Make sure that you rename the EETech64.exe file (found in the Win64 folder within the build) to EETech.exe.
- WinPE 64-bit is limited to file and password authentication; token support is not available.

### Task

- 1 Download Windows Automated Installation Kit (AIK) for Windows 7 from the Microsoft website.
- 2 Install AIK on Windows 7 (64-bit) Operating System either by burning it to a CD/DVD or extracting it using WinRAR. The WinPE 3.0 is setup.
- 3 Click **Windows | All programs | Microsoft Windows AIK | Deployment Tools** and run Deployment Tools as Administrator to open the Deployment Tools command prompt.

- 4 Run the `copype.cmd` command.

Syntax: `copype.cmd <architecture> <destination>`

Where

- `<architecture>` can be x86, amd64, or ia64
- `<destination>` is a path to the local directory

Open this path `C:\Program Files\Windows AIK\Tools\PETools`

and enter this command `copype.cmd amd64 C:\winpe_amd64`


This command creates the required directory structure and copies all the necessary files for the specified architecture.

- 5 Open the command prompt and mount the *Windows PE image (Winpe.wim)* base to the Mount directory to access the WinPE 3.0 image.

Open this path `C:\Program Files\Windows AIK\Tools\amd64\Serviceing`

and enter this command `Dism.exe /Mount-Wim /WimFile:C:\winpe_amd64\winpe.wim /index:1 /MountDir:C:\winpe_amd64\mount`

- 6 Edit the WinPE 3.0 environment as follows:
  - a Open regedit and load the system hive under [HKEY\_LOCAL\_MACHINE].
  - b Click HKEY\_LOCAL\_MACHINE, File, and Load Hive. The Load Hive pop-up appears.
  - c From the mounted WinPE image, navigate to this system file C:\winpe\_amd64\mount\ Windows \System32\Config\SYSTEM.
  - d Name the WinPE hive; for instance pe3.
  - e Access this Registry entry [HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\Control\Class \{4D36E967-E325-11CE-BFC1-08002BE10318}].
  - f Edit the multi-string upper filters with values:
    - MfeEpePC**
    - PartMgr**
  - g Right click HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services and create the **MfeEpePC** and **MfeEEAlg** keys.
  - h Modify the values of the created keys as follows:
 

 The keys are still 32-bit dword even though you are using a 64-bit system.

    - [HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services\MfeEpePC]
      - "Type"=dword:00000001
      - "Start"=dword:00000000
      - "ErrorControl"=dword:00000003
    - [HKEY\_LOCAL\_MACHINE\pe3\ControlSet001\services\MfeEEAlg]
      - "Type"=dword:00000001
      - "Start"=dword:00000000
      - "ErrorControl"=dword:00000003
      - "Group"=string:Primary Disk
  - i Click pe3, then click File | Unload hive to unload the WinPE mounted hive.

- j Close the Registry Directory.
- k Add the EEPK files to the required locations in the mounted WinPE image as mentioned in the following tables.



Before you copy the files, you need to create folders as follows:

**Table 2-5 Folders to be created**

Location	Folder to be created
C:\Winpe_amd64\mount\Program Files\	Endpoint Encryption
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\	EpeReaders
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\	EpeTokens
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\	Locale
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\	Theme

Copy the following EEPK files into the image from the Win64 folder found in the build.

**Table 2-6 Files to be copied**

Location	Files to be copied
C:\Winpe_amd64\mount\Windows\System32\Drivers\	MfeEpePC.sys MfeEEAlg.sys
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\	EETech.exe
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\EpeTokens	EpeTokenPassword.dll
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\Locale	Locale.xml

**Table 2-6 Files to be copied** *(continued)*

Location	Files to be copied
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\Locale\English-US	Please use the Language of your choice. e.g. English-US Core-0409.xml Tech-0409.xml
C:\Winpe_amd64\mount\Program Files\Endpoint Encryption\Theme	Background.png BootManager.xml CJK_Tahoma12.pbf CJK_Tahoma8.pbf CJK_Tahoma8B.pbf EpeTechAuthorize.xml EpeTechCryptSectors.xml EpeTechDiskInfo.xml EpeTechEditCryptList.xml EpeTechEditRegion.xml EpeTechFilePicker.xml EpeTechMainWnd.xml EpeTechRemoveEpe.xml EpeTechSectorPicker.xml EpeTechSelectAlg.xml EpeTechSetBootDisk.xml EpeTechWorkspace.xml EpeTechRestoreMBR.xml ErrorMessageBox.xml Language.xml LatinASCII_Tahoma12B.pbf LatinASCII_Tahoma18B.pbf LatinASCII_Tahoma8.pbf LatinASCII_Tahoma8B.pbf Logon.xml LogonBanner.png MessageBox.xml Modules.xml NewPassword.xml OsLogon.xml SelectUser.xml OsNewPassword.xml PasswordToken.xml Progress.xml QAnrolWizard.xml

**Table 2-6 Files to be copied** (continued)

Location	Files to be copied
	QaEnrolWizardBanner.png
	RecoverLocal.xml
	RecoverLocalBanner.png
	RecoverRemote.xml
	RecoverRemoteBanner.png
	RecoveryType.xml
	RecoveryTypeBanner.png
	SelectUserBanner.png
	Tech-0409.xml
	Theme.xml
	TimeoutDialog.xml
	TokenInit.xml
	TokenSelect.xml

7 Commit the changes in this path `C:\Program Files\Windows AIK\Tools\amd64\Servicing` by performing these steps:

- a To commit changes to WIM, enter this command `Dism.exe /Unmount-Wim /MountDir:C:\winpe_amd64\mount\ /Commit`
- b To copy the new WIM image to boot ISO, enter this command `copy C:\winpe_amd64\winpe.wim C:\winpe_amd64\ISO\sources\boot.wim /Y`
- c To create a bootable iso image, enter this command `oscdimg -n -bc:\winpe_amd64\etfsboot.com C:\winpe_amd64\ISO C:\winpe_amd64\winpe_amd64.iso`

The iso for WinPE3 64-bit for EETech can be found at `C:\winpe_amd64\winpe_amd64.iso`

8 Burn this iso to a CD/DVD and boot the client system from the CD/DVD.



Make sure that you do not boot the system from WinPE V3 CD/DVD when the decryption is in progress.

9 In the command prompt, enter these commands:

```
cd\
cd Program Files\Endpoint Encryption
EETech.exe
```

The EETech screen appears.

## Authenticate with token

Use this task to authenticate with a token to enable recovery tasks.

### Before you begin

Before proceeding with this task, make sure that you have the EETech WinPE V1/V3 Recovery boot disk.



**Task**

- 1 Make sure that the system's main power supply is plugged in for this task. Do not attempt to perform this task on battery only.
- 2 Boot the system with the **EETech WinPE boot disc**. This loads the **Endpoint Encryption** interface.
- 3 You can open the EETech screen in two different ways:
  - a For BartPE, Click **Go | Programs | McAfee EETech**. The EETech screen appears.
  - b For WinPE V3, in the command prompt, enter these commands:

```
cd\  
cd Program Files\Endpoint Encryption  
  
EETech.exe Or EEOpalTech.exe
```

The EETech screen appears.
- 4 Click **Token** under **Authentication**. The **Endpoint Encryption Logon** page appears and prompts for the **Endpoint Encryption** credentials for the system.
- 5 Type the **Username** and **Password** for the client system and click **Logon**. On providing the correct credential, the **Authentication** status changes to **Authenticated with Token**.

---

## Authenticate with recovery file

Use this task to authenticate the recovery procedures using the **Recovery Information File (.xml)**. The administrator needs to export the **Recovery Information File** for the desired system from the McAfee ePO server.

**Before you begin**

Before proceeding with this task, you must have the following:

- The EETech WinPE boot disk.
- The floppy drive or USB containing the **Recovery Information File (.xml)**.
- The daily Authorization/Access code.



Users can download the code of the day tool from the McAfee website.

Make sure to note that authenticating with recovery file is an optional procedure that you can follow. We recommend you to use token authentication.

**Task**

- 1 Make sure that the system's main power supply is plugged in for this task. Do not attempt to perform this task on battery only.
- 2 Boot the system with the **EETech WinPE V1/V3 Recovery CD/DVD**. This loads the **Endpoint Encryption** interface.

- 3 You can open the EETech screen in two different ways:
  - a For BartPE, Click **Go | Programs | McAfee EETech**. The EETech screen appears.
  - b For WinPE V3, in the command prompt, enter these commands:

```
cd\  
cd Program Files\Endpoint Encryption  
  
EETech.exe Or EEOpalTech.exe
```

The EETech screen appears.
- 4 Click **File** under **Authentication**, then browse and select the **Recovery Information File (.xml)** from the floppy disk or USB drive, then click **OK**. On selecting the right file, the **Authentication** status changes to **Authenticated with File**.
- 5 Once the recovery is completed, make sure that the recovery file is shredded using a secure file deletion tool.

---

## Authorize with daily authorization code

Use this task to gain administrative access to EETech with the daily authorization code. This code is only required for certain tasks in EETech, so retrieve the code when the recovery procedure in this document states that it is required.

### Before you begin

Ensure that the system's main power supply is plugged in for this task. Do not attempt to perform this task on battery only.

Before proceeding with this task, you must have the following:

- The EETech WinPE boot disk.
- The daily Authorization/Access code.



Users can download the code of the day tool from the McAfee website.

### Task

- 1 Boot the system with the **EETech WinPE V1/V3 Recovery CD/DVD**. This loads the **Endpoint Encryption** interface.
- 2 You can open the EETech screen in two different ways:
  - a For BartPE, Click **Go | Programs | McAfee EETech**. The EETech screen appears.
  - b For WinPE V3, in the command prompt, enter these commands:


```
cd\  
cd Program Files\Endpoint Encryption  
  
EETech.exe Or EEOpalTech.exe
```

The EETech screen appears.
- 3 Click **Authorize** under **Authorization**. The **Authorize** dialog box appears.
- 4 Type the daily **Authorization/Access Code** and click **OK**. On typing the correct authorization code for the day, the **Authorization** status changes to **Authorized**.

## Remove EEPC with token and file authentication

Use this task in the following situations when:


- Windows becomes corrupt.
- You cannot access the data of an encrypted system.
- Encryption or decryption fails.

 Removing EEPC with token authentication fully decrypts the system and restores the Windows MBR.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech WinPE boot disk.
- The daily Authorization/Access code.


 Users can download the code of the day tool from the McAfee website.

### Task

- 1 Backup the system by taking an image of the disk that includes every sector of the hard disk (including sector zero).
- 2 Make sure that the system's main power supply is plugged in for this task. Do not attempt to perform this task on battery only.
- 3 Boot the system with **EETech WinPE boot disk**.
- 4 You can open the EETech screen in two different ways:
  - a For BartPE, Click **Go | Programs | McAfee EETech**. The EETech screen appears.
  - b For WinPE V3, in the command prompt, enter these commands:

```
cd\  
cd Program Files\Endpoint Encryption  
EETech.exe OR EEOpalTech.exe
```

The EETech screen appears.
- 5 Authenticate with **Token** or **Recovery Information File (.xml)** and confirm the authentication status.
- 6 Authorize with daily **Authorization** code and confirm the authorization status.
- 7 Bring the disk offline.

 Make sure to note that this step might or might not be required. If required, follow Step 8. If not, skip Step 8.

- 8 Click **Remove EE** under **Actions**. The **Remove EE** page appears.



If you enter valid authentication and authorization in EETech, clicking the **Remove EE** button might not work because the Windows 7 PE environments bring the disk online. To resolve this issue, you must bring the disk offline prior to attempting to Remove EE. To bring the disk offline, you must use `DiskPart`, which is available in Windows 7 PE. Launch the Windows command prompt, and enter these commands.

```
diskpart
select disk 0
offline disk
```

- 9 Click **Remove** to begin the removal. This begins the process of decryption, and once completed removes Endpoint Encryption by installing the Windows boot sector. This process might take several hours to complete.

Removing Endpoint Encryption through EETech does not uninstall the EEAgent or EEPC components from the operating system. When you restart the system, the OS will load and these components will synchronize with the McAfee ePolicy Orchestrator server and apply the current policy which might reactivate the system. If you wish to prevent Endpoint Encryption from activating and encrypting, disconnect the system from the network or change its policy in the McAfee ePolicy Orchestrator before restarting the system. When configuring the Endpoint Encryption policy, uncheck the **Enable Policy** option in the **General** tab. Make sure that you do this only for the selected system and not for all systems in the System Tree.

For instructions on configuring policies, refer to McAfee Endpoint Encryption for PC Product Guide.

## View the workspace

The Workspace allows you to view the ranges of sectors read from the disk. This option opens the Workspace window that allows users to read sector ranges.

By default, there is nothing loaded into the workspace. The workspace is not a view of the disk, rather it is only a view of what the user loads into it. The user can choose to load the ranges of sectors. Once the user loads any of these, it is displayed in the workspace.



It is entirely the responsibility of the qualified system administrators and security managers to take appropriate precautions before performing this task. The user needs to take maximum care while performing this task, otherwise, it may cause the system to become corrupt and that might result in the loss of data. Contact McAfee support for assistance on how to use the EETech Workspace.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech WinPE V1/V3 Recovery CD/DVD boot disk.
- The daily Authorization/Access code.



Users can download the code of the day tool from the McAfee website.

- **Recovery Information File (.xml)** or **Authentication Token**

**Task**

- 1 Take a sector level backup of the drive being processed.
- 2 Boot the system with the **EETech WinPE boot disk**. This loads the **Endpoint Encryption** interface.
- 3 You can open the EETech screen in two different ways:
  - a For BartPE, Click **Go | Programs | McAfee EETech**. The EETech screen appears.
  - b For WinPE V3, in the command prompt, enter these commands:

```
cd\  
cd Program Files\Endpoint Encryption  
  
EETech.exe OR EEOpalTech.exe
```

The EETech screen appears.
- 4 Authorize with daily **Authorization** code and confirm the authorization status.
- 5 Authenticate with **Token** or **Recovery Information File (.xml)** and confirm the authentication status.
- 6 Click **Workspace** under **Actions**. The **Workspace** page appears with following options:
  - **Load From File** - Loads the file and displays the bytes that comprise it.
  - **Save To File** - This option saves the current data in the workspace to the file.
  - **Load From Disk** - This loads bytes from a continuous range of sectors on the disk.
  - **Save To Disk** - This option saves the current data in the workspace to a continuous range of sectors on the disk.
  - **Zero Workspace** - This option fills the workspace with zeros.
  - **Set workspace Alg** - Use this option to select and set the desired algorithm to use in the workspace for encryption or decryption.
  - **Encrypt Workspace** - This option encrypts the entire contents of the workspace.
  - **Decrypt Workspace** - This option decrypts the entire contents of the workspace.
- 7 Click **First Sector** to view the first sector of the workspace.
- 8 Click **Previous Sector** to view the previous sector of the current sector of the workspace.
- 9 Click **Next Sector** to view the next sector of the current sector of the workspace.
- 10 Click **Last Sector** to view the last sector of the workspace.

---

## Encrypt or decrypt sectors

The Crypt Sector feature allows you to safely manipulate which sectors are encrypted on the disk. Make sure to note that there is no check to ensure that you are using the correct key for the machine; use of the wrong key could corrupt data.

The disk maintains a list of regions of the disk which are encrypted, and regions of the disk which are not; this list is called the crypt list.

This option uses the crypt list to validate the ranges you submit to make sure that you cannot inadvertently encrypt sectors, which are already encrypted, or decrypt sectors which are currently not encrypted. This option supports also supports power fail protection.

**Crypt Sector** option cannot be used if Endpoint Encryption has become corrupt on the disk, or the crypt state has been corrupted. The **Force Crypt Sectors** option can be used in such cases, but this provides no protection and must therefore be used with extreme caution.

Changing the encryption state of areas of the disk with this feature makes appropriate modifications to the disk crypt list which will persist until the next policy enforcement. For example, if you use this feature to decrypt a specific partition, the next time you boot the machine to windows and the policy is enforced, Endpoint Encryption will re-encrypt the partition according to the policy applied.



EETech now displays the Disk Crypt List and Edit Disk Crypt State information in decimal instead of hexadecimal.

A manual removal of Endpoint Encryption can be accomplished by decrypting the entire disk using this feature, and then performing a Restore MBR operation that will replace the MBR with the Windows MBR, thus deactivating EEPC.



It is entirely the responsibility of the qualified system administrators and security managers to take appropriate precautions before performing this task. EETech provides very low level control of the disk and administrative error when using this tool can result in the loss of data. We recommend that only experienced administrators work with EETech.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech WinPE V1/V3 Recovery CD/DVD boot disk.
- The daily Authorization/Access code.



Users can download the code of the day tool from the McAfee website.

- **Recovery Information File (.xml) or Authentication Token**

### Task

- 1 Take a sector level backup of the drive being processed.
- 2 Boot the system with the **EETech WinPE V1/V3 Recovery CD/DVD**. This loads the **Endpoint Encryption** interface.
- 3 You can open the EETech screen in two different ways:
  - a For BartPE, Click **Go | Programs | McAfee EETech**. The EETech screen appears.
  - b For WinPE V3, in the command prompt, enter these commands:
 

```
cd\  
cd Program Files\Endpoint Encryption  
EETech.exe OR EEOpalTech.exe
```

 The EETech screen appears.
- 4 Authorize with daily **Authorization** code and confirm the authorization status.
- 5 Authenticate with **Token** or **Recovery Information File (.xml)** and confirm the authentication status.
- 6 Click **Set Boot Disk** and select the relevant boot disk from the **Set Boot Disk** page.
- 7 Click **Set Algorithm** and select the desired algorithm from the **Select Algorithm** page.

- 8 Click **Crypt Sectors** and select the disk from the **Select Disk** list, then type the **Start Sector** and the **Number of Sectors**.
- 9 Click **Encrypt/Decrypt** to encrypt/decrypt a range of sectors.

---

## Restore the Master Boot Record (MBR)

The MBR is the first sector of the boot disk. It is that part of the hard drive which tells the operating system what to boot and from where to boot.

When Endpoint Encryption activates, a backup of the Windows MBR is sent up to the server for use in recovery scenarios, and can be exported from ePO through the **Recovery Information file (.xml)**.

This feature allows you to deactivate Endpoint Encryption on a manually decrypted boot disk by restoring the Windows MBR (preserving the in-situ partition table) to the disk. Do not use this feature on secondary (non-boot) disks.



Performing this operation on an encrypted boot disk will render the system non-bootable.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech WinPE boot disk.
- The floppy drive or USB containing the recovery information file (**.xml**) and this must be plugged in before booting from the BartPE Boot CD/DVD boot disk.
- A system authorized with the authorization code.

### Task

- 1 Take a sector level backup of the drive being processed.
- 2 Manually decrypt the disk using the Crypt Sectors feature.
- 3 Boot the system with the **EETech WinPE V1/V3 Recovery CD/DVD**. This loads the **Endpoint Encryption** interface.
- 4 You can open the EETech screen in two different ways:
  - a For BartPE, Click **Go | Programs | McAfee EETech**. The EETech screen appears.
  - b For WinPE V3, in the command prompt, enter these commands:

```
cd\  
cd Program Files\Endpoint Encryption  
EETech.exe OR EEOpalTech.exe
```

The EETech screen appears.
- 5 Authorize with daily **Authorization** code and confirm the authorization status.
- 6 Authenticate with **Token** or **Recovery Information File (.xml)** and confirm the authentication status.

7 Click **Restore MBR** under **Disk Operations**. The confirmation page appears.

8 Click **Yes** to confirm that you want to overwrite the Master Boot Record.



The MBR will be replaced with the one that was present on the disk before Endpoint Encryption for PC was activated.



This feature should only be performed on a boot disk, and where the data on the disk is not encrypted, as the operating system is encrypted.



# 3

## EETech Standalone

This chapter explains some of the common tasks that can be undertaken using McAfee's system recovery tool, the standalone version of the EETech. Make sure that you exercise caution for all EETech procedures.

Make sure to refer the **Authenticate with token** and **Authorize with daily authorization code** procedures in the EETech PE section.



Make sure to note that file recovery is possible only with EETech PE and not EETech Standalone.

### Contents

- ▶ *Create EETech Standalone bootable disk*
- ▶ *Create EEOpalTech Standalone bootable disk*
- ▶ *Boot from EETech and EEOpalTech Standalone boot disks*
- ▶ *Perform emergency boot*
- ▶ *Remove EEPC with token authentication*
- ▶ *View the workspace*
- ▶ *Encrypt or decrypt sectors*
- ▶ *Restore the Master Boot Record (MBR)*

---

## Create EETech Standalone bootable disk

McAfee EETech (Standalone) is a disaster recovery tool that allows the administrator to perform normal recovery functions. It enhances the user experience with a simplified process of creating the EETech boot disk. You can create the boot disk by running a simple command from the command prompt.

### Before you begin

Before proceeding with this task, you must have the following:

- **A:** drive in your computer and a floppy disk
  - A Compact Disk (CD) drive in your computer and a CD
  - A Universal Serial Bus (USB) drive in your computer and a USB
- For a bootable floppy:
    - 1 Extract **EETech.zip** and place the **Standalone** folder in the desired location.
    - 2 Insert the floppy disk and format it.

- 3 Point to the **Standalone** folder from the command prompt.
  - 4 Run the command **Bootdisk.exe EETech.RTB a:** from the command prompt. The bootable floppy is created.
- For a bootable CD:
    - 1 Extract **EETech.zip** and place the **Standalone** folder in the desired location.
    - 2 Insert the CD.
    - 3 Point to the **Standalone** folder from the command prompt.
    - 4 Run the command **Bootdisk.exe EETech.RTB <filename>.dsk** from the command prompt.
    - 5 Copy <filename>.dsk into the bootable CD (with bootable option selected) and burn it. The bootable CD is created.



Make sure that you select the **Bootable** option.

- For a bootable USB:
    - 1 Extract **EETech.zip** and copy the **Standalone** folder in the desired location.
    - 2 Insert the USB and format it using command line.
- 3 Point to the **Standalone** folder from the command prompt.
  - 4 Run the command **Bootdisk.exe EETech.RTB <drive letter>:** from the command prompt. The bootable USB is created.



Make sure that you note the drive letter of the USB drive. For instance, consider the USB drive as 'g'.



The right click format (FAT 32) and quick format (FAT32) does not work on all USB or hardware combinations.



When using bootable USB, you have to explicitly perform the **Set Boot Disk** operation.



On some BIOS, EETech does not function properly when booted from the USB drive. This happens because of the way in which certain BIOS recognize and handle the bootable USB drive during and after the boot process. In this situation, we recommend that you use alternative methods (for example, floppy or CD) for booting EETech.

## Create EEOpalTech Standalone bootable disk

McAfee EEOpalTech (Standalone) is a disaster recovery tool that allows the administrator to perform normal recovery functions. It enhances the user experience with a simplified process of creating the EEOpalTech boot disk. You can create the boot disk just by running a simple command from the command prompt.

### Before you begin


Before proceeding with this task, you must have the following:

- **A:** drive in your computer and a floppy disk
- A Compact Disk (CD) drive in your computer and a CD
- A Universal Serial Bus (USB) drive in your computer and a USB


The Opal specification states that an Opal drive will automatically lock when the drive is powered down, and PBA will be displayed only after the drive is powered down. However, when EEPC is active within Windows, if you restart the system the drive is locked by EEPC, and hence the PBA appears after restarts, hibernation, or power cycle.

Using EETech the behavior is different. After you have authenticated the drive using EETech, the drive is unlocked and PBA will not then be displayed until the drive is powered down. When you quit EETech, the system will restart and, since the drive has been unlocked by your authentication, PBA will not be displayed. Make sure to note that this is an expected behavior.

- For a bootable floppy:
  - 1 Extract **EETech.zip** and place the **Standalone** folder in the desired location.
  - 2 Insert the floppy disk and format it.
  - 3 Point to the **Standalone** folder from the command prompt.
  - 4 Run the command **Bootdisk.exe EEOpalTech.RTB a:** from the command prompt. The bootable floppy is created.
- For a bootable CD:
  - 1 Extract **EETech.zip** and place the **Standalone** folder in the desired location.
  - 2 Insert the CD.
  - 3 Point to the **Standalone** folder from the command prompt.
  - 4 Run the command **Bootdisk.exe EEOpalTech.RTB <filename>.dsk** from the command prompt.
  - 5 Copy **<filename>.dsk** into the bootable CD (with bootable option selected) and burn it. The bootable CD is created.
- For a bootable USB:
  - 1 Extract **EETech.zip** and copy the **Standalone** folder in the desired location.
  - 2 Insert the USB and format it using command line.



Make sure that you note the drive letter of the USB drive. For instance, consider the USB drive as 'g'.



The right click format (FAT 32) and quick format (FAT32) does not work on all USB or hardware combinations.
  - 3 Point to the **Standalone** folder from the command prompt.
  - 4 Run the command **Bootdisk.exe EEOpalTech.RTB <drive letter>:** from the command prompt. The bootable USB is created.

---

## Boot from EETech and EEOpalTech Standalone boot disks

EETech and EEOpalTech are accessed through EETech and EEOpalTech Standalone bootable CD, USB, and floppy respectively. When the user boots the unrecoverable system with EETech and EEOpalTech

Standalone boot disks, the first page that appears is McAfee EETech interface and McAfee EEOpalTech interface respectively.

### Task

- 1 Boot the unrecoverable system with the **EETech (Standalone) boot floppy/CD/USB**. The **McAfee EETech** interface appears.
- 2 Boot the unrecoverable system with the **EEOpalTech (Standalone) boot floppy/CD/USB**. The **McAfee EEOpalTech** interface appears.

The McAfee EEOpalTech interface is a minimized version of McAfee EETech interface and does not support viewing the workspace, encrypting or decrypting sectors, and restoring the MBR functionalities.



Make sure to note that some Opal drives will lock if you fail authentication more than several times. If this happens, you should power-cycle the system to allow authentication to occur.

## Perform emergency boot

You can perform the emergency boot when an EEPK installed system fails to boot or when the Endpoint Encryption logon page is corrupt.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech (Standalone) boot disk.
- The floppy drive or USB containing the **Recovery Information File (.xml)**.
- The daily Authorization/Access code.



Users with a valid support contract with McAfee can obtain the daily Authorization code from McAfee Support.

### Task

- 1 Since an Emergency Boot will not touch data on the drive until the next policy enforcement occurs, when in Windows; it is not necessary to create a sector level backup of the disk during Emergency Booting.
- 2 Restart the unrecoverable system using the EETech (Standalone) boot disk. This loads the **McAfee EETech** interface.
- 3 Authorize with daily **Authorization** code and confirm the authorization status.
- 4 Click **Enable USB** under **Actions**. The **McAfee EETech** dialogue appears with the **USB enabled** message.
- 5 Click **OK** to close the dialogue.
- 6 Click **File** under **Authentication**, then browse and select the **Recovery Information File (.xml)** from the floppy disk or USB drive, then click **OK**. On selecting the right file, the **Authentication** status changes to **Authenticated**.

Or

Authenticate with **Token** and confirm the authentication status changes to **Authenticated**.

- 7 You may need to use the **Select Boot Disk** option to specify which drive EETech will try to boot from. This is dependent on the implementation of the BIOS, and whether you have booted from floppy drive, CD, or USB drive.
- 8 Click **Emergency Boot** under **Actions**. The **EETech will now emergency boot into the operating system** message appears.
- 9 Click **OK** to confirm the emergency boot.



When the system boots into Windows, if there is a network connection to the McAfee ePO server, then the system synchronizes with McAfee ePO and fully repairs itself by rebuilding the PBFS and re-synchronizing all data from the server. You can confirm this by right-clicking **McAfee Agent Tray**, then clicking **Quick Settings | Endpoint Encryption status**.



If the McAfee Agent is unable to establish connection with the McAfee ePO Server, continue to use the **EETech Emergency Boot** option to boot the system until a connection to the server is made.

## Remove EEPK with token authentication

Use this task to remove EEPK with token authentication.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech (Standalone) boot disk.
- The daily Authorization/Access code.



Users can download the code of the day tool from the McAfee website.

Use this task in the following situations when:

- Windows becomes corrupt.
- You cannot access the data of an encrypted system.
- Encryption or decryption fails.

### Task

- 1 Take a sector level backup before performing this operation.
- 2 Make sure that the system's main power supply is plugged in for this task. Do not attempt to perform this task on battery only.
- 3 Restart the unrecoverable system using the EETech (Standalone) boot disk. This loads the **McAfee EETech** interface.
- 4 Authorize with daily **Authorization** code and confirm the authorization status.
- 5 Authenticate with **Token** and confirm the authentication status changes to **Authenticated**.

- 6 Click **Remove EE** under **Actions**. The **Remove EE** page appears.
- 7 Click **Remove** to begin the removal. This removes encryption and boot sector from the client system, however, this does not remove Endpoint Encryption client files. It might take a few hours to perform the decryption and complete the operation depending on the system performance and the storage capacity of the drive or partition.

Removing Endpoint Encryption through EETech does not uninstall the EEAgent or EEPC components from the operating system. When you restart the system, the OS will load and these components will synchronize with the McAfee ePolicy Orchestrator server and apply the current policy. If you wish to prevent Endpoint Encryption from activating and encrypting, disconnect the system from the network or change its policy in the McAfee ePolicy Orchestrator before restarting the system. When configuring the Endpoint Encryption policy and uncheck the Enable Policy option in the General tab. Ensure that you do this only for the selected system and not for all systems in the System Tree.

For instructions on configuring policies, refer to McAfee Endpoint Encryption for PC Product Guide.

## View the workspace

The Workspace allows you to view the ranges of sectors read from the disk. This option opens the Workspace window that allows users to read sector ranges.

By default, there is nothing loaded into the workspace. The workspace is not a view of the disk, rather it is only a view of what the user loads into it. The user can choose to load the ranges of sectors. Once the user loads any of these, it is displayed in the workspace.



It is entirely the responsibility of the qualified system administrators and security managers to take appropriate precautions before performing this task. The user needs to take maximum care while performing this task, otherwise, it may cause the system to become corrupt and that might result in the loss of data. Contact McAfee support for assistance on how to use the EETech workspace.

Before proceeding with this task, you must have the following:

- The EETech (Standalone) boot disk
- The daily Authorization/Access code



Users with a valid support contract with McAfee can obtain the daily Authorization code from McAfee Support.

- **Recovery Information File (.xml) or Authentication Token**

### Task

- 1 Boot the system with the **EETech (Standalone) boot disk**. This loads the **McAfee EETech** interface.
- 2 Authorize with daily **Authorization** code and confirm the authorization status.
- 3 Authenticate with **Token** or **Recovery Information File (.xml)** and confirm the authentication status.
- 4 Click **Workspace** under **Actions**. The **Workspace** page appears with following options:
  - **Load From File** - Loads the file and displays the bytes that comprise it.
  - **Save To File** - This option saves the current data in the workspace to the file.
  - **Load From Disk** - This loads bytes from a continuous range of sectors on the disk.

- **Save To Disk** - This option saves the current data in the workspace to a continuous range of sectors on the disk.
  - **Zero Workspace** - This option fills the workspace with zeros.
  - **Set workspace Alg** - Use this option to select and set the desired algorithm to use in the workspace for encryption or decryption.
  - **Encrypt Workspace** - This option encrypts the entire contents of the workspace.
  - **Decrypt Workspace** - This option decrypts the entire contents of the workspace.
- 5 Click **First Sector** to view the first sector from the disk.
  - 6 Click **Previous Sector** to view the previous sector of the current sector from the disk.
  - 7 Click **Next Sector** to view the next sector of the current sector from the disk.
  - 8 Click **Last Sector** to view the last sector from the disk.

---

## Encrypt or decrypt sectors

The Crypt Sector feature allows you to safely manipulate which sectors are encrypted on the disk. Make sure to note that there is no check to ensure that you are using the correct key for the machine; use of the wrong key could corrupt data.

The disk maintains a list of regions of the disk which are encrypted, and regions of the disk which are not; this list is called the crypt list.

This option uses the crypt list to validate the ranges you submit to make sure that you cannot inadvertently encrypt sectors, which are already encrypted, or decrypt sectors which are currently not encrypted. This option supports also supports power fail protection.

**Crypt Sector** option cannot be used if Endpoint Encryption has become corrupt on the disk, or the crypt state has been corrupted. The **Force Crypt Sectors** option can be used in such cases, but this provides no protection and must therefore be used with extreme caution.

Changing the encryption state of areas of the disk with this feature makes appropriate modifications to the disk crypt list which will persist until the next policy enforcement. For example, if you use this feature to decrypt a specific partition, the next time you boot the machine to windows and the policy is enforced, Endpoint Encryption will re-encrypt the partition according to the policy applied.

A manual removal of Endpoint Encryption can be accomplished by decrypting the entire disk using this feature, and then performing a Restore MBR operation that will replace the MBR with the Windows MBR, thus deactivating EEPC.



It is entirely the responsibility of the qualified system administrators and security managers to take appropriate precautions before performing this task. EETech provides very low level control of the disk and administrative error when using this tool can result in the loss of data. We recommend that only experienced administrators work with EETech.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech (Standalone) boot disk.
- The daily Authorization/Access code.



Users can download the code of the day tool from the McAfee website.

- **Recovery Information File (.xml) or Authentication Token**

### Task

- 1 Take a sector level backup of the drive being processed.
- 2 Boot the system with the **EETech (Standalone) boot disk**. This loads the **McAfee EETech** interface.
- 3 Authorize with daily **Authorization** code and confirm the authorization status.
- 4 Authenticate with **Token** or **Recovery Information File (.xml)** and confirm the authentication status.
- 5 Select the disk from the **Select Disk** list, then type the **Start Sector** and the **Number of Sectors**.
- 6 Click **Set Boot Disk** and select the relevant boot disk from the **Set Boot Disk** page.
- 7 Click **Set Algorithm** and select the desired algorithm from the **Select Algorithm** page.
- 8 Click **Crypt Sectors** and select the disk from the **Select Disk** list, then type the **Start Sector** and the **Number of Sectors**.
- 9 Click **Encrypt/Decrypt** to encrypt/decrypt a range of sectors.

---

## Restore the Master Boot Record (MBR)

The MBR is the first sector of the boot disk. It is that part of the hard drive which tells the operating system what to boot and from where to boot.

When Endpoint Encryption activates, a backup of the Windows MBR is sent up to the server for use in recovery scenarios, and can be exported from ePO through the **Recovery Information file (.xml)**.

This feature allows you to deactivate Endpoint Encryption on a manually decrypted boot disk by restoring the Windows MBR (preserving the in-situ partition table) to the disk. Do not use this feature on secondary (non-boot) disks.



Performing this operation on an encrypted boot disk will render the system non-bootable.

### Before you begin

Before proceeding with this task, you must have the following:

- The EETech (Standalone) boot disk.
- The floppy drive or USB containing the recovery information file (**.xml**) and this must be plugged in before booting from the EETech (Standalone) boot disk.
- A system authorized with the authorization code.

### Task

- 1 Take a sector level backup of the drive being processed.
- 2 Manually decrypt the disk using the **Crypt Sectors** feature.



- 3 Boot the system with the **EETech (Standalone) boot disk**. This loads the **McAfee EETech** interface.
- 4 Authorize with daily **Authorization** code and confirm the authorization status.
- 5 Authenticate with **Token** or **Recovery Information File (.xml)** and confirm the authentication status.
- 6 Click **Restore MBR** under **Disk Operations**. The confirmation page appears.
- 7 Click **Yes** to confirm that you want to overwrite the Master Boot Record.



The MBR will be replaced with the one that was present on the disk before Endpoint Encryption for PC was activated.




This feature should only be performed on a boot disk, and where the data on the disk is not encrypted, as the operating system is encrypted.







# 4

## Glossary

There are a number of options that are common to both EETech (WinPE V1 and V3) and EETech (Standalone). These options have the similar functionalities in both recovery methods. Options or topics common to EETech (WinPE V1 and V3) and EETech (Standalone) are listed in the table below.

Topic	Description
Disk Information	<ul style="list-style-type: none"><li>• <b>Disk Power Fail Status</b> - Endpoint Encryption for PC tracks the progress of encryption on the drive to ensure that if power is lost during encryption, the process is recoverable.</li><li>• <b>Status</b> - Determines whether the drive is currently in powerfail state. A status of <b>Inactive</b> indicates that the current encryption process has finished.</li><li>• <b>Disk Crypt List</b><ul style="list-style-type: none"><li>• <b>Crypt List Region Count</b> - The number of defined crypted areas of this logical disk. This usually corresponds to the number of partitions on the drive.<ul style="list-style-type: none"><li>• <b>Region</b> - Each region is defined as follows:<ul style="list-style-type: none"><li>• <b>Start Sector</b> - The physical start sector of the region</li><li>• <b>End Sector</b> - The last physical sector included in the region</li><li>• <b>Sector Count</b> - The number of sectors included in this region</li></ul></li></ul></li><li>• <b>Disk Partitions</b> - A section per Logical partition on this physical drive as follows:<ul style="list-style-type: none"><li>• <b>Partition Count</b> - The unique partition number.</li><li>• <b>Partition Type</b> - The file system detected on this partition.</li><li>• <b>Partition Bootable</b> - Whether the partition is bootable or not.</li><li>• <b>Partition Recognized</b> - Whether the partition is recognized as viable.</li><li>• <b>Partition Drive Letter</b> - The detected drive letter of this partition.</li><li>• <b>Partition Start Sector</b> - The physical start sector of the partition.</li><li>• <b>Partition End Sector</b> - The physical end sector of the partition.</li><li>• <b>Partition Sector Count</b> - The number of sectors in the partition.</li><li>• <b>Partition Bus Type</b> - Bus type used in particular partition.</li></ul></li></ul></li></ul>
Repair Disk Information	<p>The <b>Repair Disk Information</b> option fixes problems with any disk that is set as the boot disk. For this to work the crypt list portion must still be valid and the power fail state must be inactive.</p> <p>The disk information is stored in a chain of sectors. If the chain of sectors breaks, then it not possible for Endpoint Encryption to figure out what parts of the disk are encrypted and hence the user gets errors. The Repair Disk Information option attempts to repair the broken chain sectors.</p> <p> This option is not supported with the current McAfee EETech version.</p>

Topic	Description
<b>Force Crypt Sectors</b>	<p>Before using this option call McAfee Technical support for assistance.</p> <p>Unlike the <b>Crypt Sectors   Encrypt/Decrypt</b> option, the <b>Force Crypt Sectors</b> option does not consider the disk crypt state. It simply performs the operation blindly according to user input. Force Crypt does not support power fail, nor does it apply any logic or parameter validation on the input.</p> <p>You should use the <b>Force Crypt Sectors</b> option only when everything else fails. For example, when the on-disk structures are completely corrupted.</p> <p> This option will cause irretrievable data loss if used incorrectly. If you are forced to use this option, you should make a recording of each operation you apply to support in data recovery.</p> <p> Ensure that there is no possibility of losing power while using this option as this option does not support power fail protection.</p>
<b>Edit Disk Crypt State</b>	<p>The disk crypt state contains information about which range of sectors are encrypted. This option allows you to change the ranges.</p> <p> Call McAfee Technical support for assistance before using this option, because using this option inappropriately will cause irretrievable data loss.</p> <p> Ensure that there is no possibility of losing power while using this option as this option does not support power fail protection.</p>
<b>Set Algorithm</b>	<p>This is an option present under <b>Disk Operations</b> on the McAfee EETech page for setting the correct algorithm on a system.</p>
<b>Set Boot Disk</b>	<p>This option displays a list of disks from which the user can select a disk to use as the boot disk.</p>
<b>Code of the Day (COD)</b>	<p>Code of the Day is also known as daily authorization code. Certain recovery operations in EETech require administrative access. The user can get this access by typing this four-digit code (COD) into the authorization screen.</p>

# Index

- A**
  - Authenticate from file [36](#), [37](#), [39](#), [46–48](#)
  - Authenticate from token [35–37](#), [46](#), [47](#)
  - Authentication [32](#)
  - Authentication Code [44](#)
  - Authorization [34](#)
  - Authorization Code [34](#)
- B**
  - BartPE CD/DVD [35](#)
  - BartPE CD\DVD [13](#)
  - BartPe install file [13](#)
- C**
  - Code of the Day (COD) [10](#)
  - Create EEOpaITech Boot Disk [42](#)
  - Create EETech Boot Disk [41](#)
  - Crypt Sectors [37](#), [47](#)
- D**
  - Decrypt [37](#), [46](#), [47](#)
  - Decrypt workspace [36](#)
- E**
  - EE credential [45](#)
  - EETech [5](#), [13](#), [44](#)
  - Emergency Boot [44](#)
  - Encrypt [37](#), [46](#), [47](#)
  - Encrypt workspace [36](#)
  - Endpoint Encryption for PC [5](#)
- I**
  - ISO image [13](#)
- M**
  - Media Output [13](#)
- R**
  - Recovery [13](#), [41](#), [42](#)
  - Recovery Information file [39](#), [48](#)
  - Recovery Information File [44](#)
  - Remove EE [35](#), [45](#)
  - Restore MBR [39](#), [48](#)
- S**
  - Standalone boot CD, USB, and floppy [43](#)
- T**
  - token authentication [45](#)
  - Token Authentication [32](#)
- W**
  - WinPE [13](#)
  - Workspace [36](#), [46](#)

