Dynamic Mount Utility

1.4

Administration Guide

Full Disk Encryption

22 September 2010
Important Information

Latest Version

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11588

For additional technical information, visit the Check Point Support Center
(http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 September 2010</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Dynamic Mount Utility 1.4 Administration Guide).
Contents

Important Information ................................................................. 3
Introduction .................................................................................. 5
   What's New ................................................................. 5
   Known Limitations ......................................................... 5
Set Up and Usage ....................................................................... 6
   Preparing Authentication .............................................. 6
   Preparing a BartPE CD ...................................................... 6
   Preparing a WinPE CD ....................................................... 6
   Installing in Windows ......................................................... 7
   Using the Dynamic Mount Utility ..................................... 7
Introduction

To access information on the hard disk of a Full Disk Encryption-protected machine without doing a Recovery, use the Dynamic Mount Utility of Full Disk Encryption. For example, use this utility to get data when other processes do not work because of an operating system failure. The Dynamic Mount Utility is hardware independent.

You can use the Dynamic Mount Utility:

- Instead of the Full Disk Encryption Alternative Boot Menu or slaving functionality.
- To access hard disks connected by USB.
- Without Full Disk Encryption.
- On a BartPE CD, WinPE CD, or on a regular Windows installation.

The Dynamic Mount Utility is supported on Pointsec PC versions 6.2.0 and higher, and on all versions of Full Disk Encryption.

What's New

- 64-bit support
- WinPE 2.0 and 3.0 support

Known Limitations

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00513055</td>
<td>PSWinRE.exe does not display a message when done. The utility works in the background and outputs the progress into Pointsec_PC_winRE.log.</td>
</tr>
<tr>
<td>00512932</td>
<td>An error occurs when unlocking a FAT volume with the Dynamic Mount Utility. Even if authenticating to the volume, you will only see garbage in Explorer when you are trying to examine the files.</td>
</tr>
<tr>
<td>00515351</td>
<td>Windows can crash with the Dynamic Mount Utility in standalone mode. The blue screen occurs after Windows is loaded (when Windows is searching for drivers for the disk). The blue screen code is: 0x05001146</td>
</tr>
</tbody>
</table>

**Workaround:**

Connect the encrypted disk to the machine before booting into Windows or WinPE. After that, start the Dynamic Mount Utility and unlock the drive. Do not unmount the unlocked drive in Windows or WinPE.
Set Up and Usage

In This Chapter

Preparing Authentication 6
Preparing a BartPE CD 6
Preparing a WinPE CD 6
Installing in Windows 7
Using the Dynamic Mount Utility 7

Preparing Authentication

You must authenticate to the Full Disk Encryption disk to unlock it.

- The user account name must have permissions for Recovery and Uninstall.
- On a computer with Windows Integrated Logon (WIL) active, you must authenticate with the WIL user name and password.

Preparing a BartPE CD

Prepare the Bart ISO image with the Full Disk Encryption Dynamic Mount plugin.

To run the Dynamic Mount Utility on a BartPE CD:
1. Install PE Builder (http://www.nu2.nu/pebuilder/).
2. Copy the FDE_Dynamic_Volume and FDE_Filter folders to the Plugin folder under the BartPE Creator.
4. Click Plugin and select Install for Check Point FDE - Dynamic mount utility and for Check Point FDE - Encryption filter driver.
5. Click Build.
6. Start the utility. Run: x:\<program files>\checkpoint\fde_dyn_disk.exe

Preparing a WinPE CD

Prepare the WinPE wim file with the Full Disk Encryption Dynamic Mount plugin (x86 or x64) and Full Disk Encryption filter driver (prot_2k.sys). You will use the PSWinRE tool. On a 64-bit computer, you must also add the Full Disk Encryption ccore64.sys file.

To run the Dynamic Mount Utility on a WinPE CD:
1. Install Windows AIK and create a wim file (x86 or x64).
2. Run: PSwinRE.exe
3. Configure the PSWinRE options:
   - Select the Full Disk Encryption filter driver: prot_2k.sys
   - If you use a 64-bit wim file, make sure ccore64.sys is in the same folder as prot_2k.sys. It will be selected automatically.
   - Select the utility folder: FDE_Dynamic_Volume_32 or FDE_Dynamic_Volume_64
4. If you mounted the WIM with Windows AIK, skip this step. If you did not mount the WIM already:
   a) Create an empty folder and enter its path in Select mount point.
b) Select **Mount WIM file** and enter the path to the *wim* file.
c) In **Imagex.exe location**, enter the path to the Windows AIK *imagex.exe* application.

5. Click **Apply**.
   The Full Disk Encryption filter driver and the Dynamic Mount Utility are installed in the *wim* file.

6. Use Window AIK to build a WinPE CD ISO file, using the *wim* file.
7. Boot from the WinPE CD.
8. Start the Dynamic Mount Utility. Run:
   ```
x:\<program files>\fde_dmu\fde_dmu_x86.exe
   or
   x:\<program files>\fde_dmu\fde_dmu_x64.exe
   ```
   This path is for WinPE only.

---

## Installing in Windows

You can use the Dynamic Mount Utility on a Windows installation if Full Disk Encryption is not installed.

**To install the Dynamic Mount Utility on Windows:**

1. Download the package from the User Center [here](https://supportcenter.checkpoint.com/supportcenter/portal).
2. Run **Check Point - Full Disk Encryption Dynamic Mount Utility.msi** as an Administrator.
3. Follow the on-screen instructions.
4. When prompted, reboot the computer.
5. Start the Dynamic Mount Utility from the **Start** menu.

---

## Using the Dynamic Mount Utility

You can use the Dynamic Mount Utility to read and write to an encrypted Full Disk Encryption disk. It does not change anything, by itself, on the accessed hard disk. It makes the disk writable.

The encrypted disk can be connected by USB or it can be internal.

**Important** - You should always power off a computer before you disconnect a USB-connected disk, to prevent data corruption.

**To use the Dynamic Mount Utility:**

1. Start the utility.
   The utility opens and shows a list of connected hard drives.
2. Select the disk with Full Disk Encryption to mount. If the selected hard drive fails to mount (it cannot be unlocked), click **Browse** and go to a recovery file. Then select the drive in the list.

   **Note** - Remote Help is not available if you authenticate to a recovery file.

3. When prompted, authenticate to the selected disk.

   **Note** - The **Set Max Failed Logons Before Reboot** system setting applies to authentication to the Dynamic Mount Utility. If you exceed the number of logons, you must reboot before you can try again to unlock the hard disk.