

How to add Bitlocker Support to WinPE

In this Article, I will show you how you can add Bitlocker Support to WinPE 10. After implementing this, you are able to manage Bitlocker using `manage-bde` command within WinPE.

Usecase:



Sometimes it is quite useful to be able to unlock a Bitlocker encrypted Drive within WinPE. This is necessary if the user is unable to boot the installed OS and has local Data on the encrypted Drive.

There are some other methods to get the local Data on the drive – for example, you can dismount the Harddisk and connect the encrypted Harddisk to another Computer using a USB – Cable. Then you are asked to provide the Bitlocker Recovery Key.

But sometimes this is not possible especially when a User is in a branch office where no IT Admin can help the User to dismount the Harddisk and plug it into another computer. Then this article would be helpful.

Optional but in most cases not necessary: You could extend this method to run a Script within WinPE to request the Bitlocker Recovery Key from your MBAM (Microsoft Bitlocker Administration and Monitoring) Server and unlock the Harddisk using a Web Service.

I think this is also a very good way, but I unlocking a Harddisk is normally not a daily task - so it is not necessary to automate it that high.

Prerequisites:

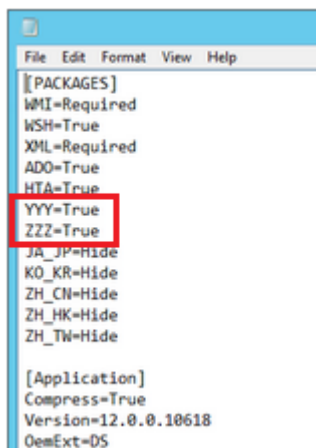
- Deployment Solution 8.5 (should also work with 8.0 and 8.1)
- Installed Network Boot Service (NBS)
- WinPE10 as a Preboot Environment (should also work with WinPE 4.0 and WinPE 5.x)

1. On your SMP Server, create a Backup of a file called **default.bdc**. You can find this file in the folder <Install Drive >Program Files\Altiris\Deployment\BDC\bootwiz
2. Edit the original default.bdc File using Notepad and add the following to Lines into the [PACKAGES] Section

YYY=True

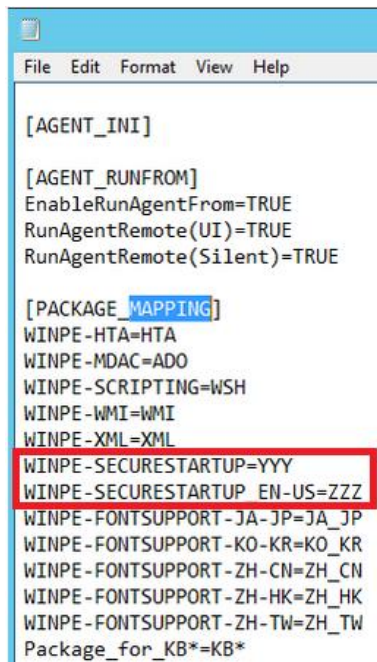
ZZZ=True

Your file should look like this



3. On your SMP Server, create a Backup of a file called WinPE10x64.ini. You can find this file in the folder: <Install Drive >Program Files\Altiris\Deployment\BDC\bootwiz\Platforms
4. Edit the original **WinPE10x64.ini** File and scroll down to the Section **[PACKAGE MAPPING]** and add the following to Lines to the Section

Optional: The same steps need to be done for WinPE10x86.ini File if you want to add Bitlocker support for WinPEx86.



```
[AGENT_INI]

[AGENT_RUNFROM]
EnableRunAgentFrom=TRUE
RunAgentRemote(UI)=TRUE
RunAgentRemote(Silent)=TRUE

[PACKAGE_MAPPING]
WINPE-HTA=HTA
WINPE-MDAC=ADO
WINPE-SCRIPTING=WSH
WINPE-WMI=WMI
WINPE-XML=XML
WINPE-SECURESTARTUP=YYY
WINPE-SECURESTARTUP_EN-US=ZZZ
WINPE-FONTSUPPORT-JA-JP=JA_JP
WINPE-FONTSUPPORT-KO-KR=KO_KR
WINPE-FONTSUPPORT-ZH-CN=ZH_CN
WINPE-FONTSUPPORT-ZH-HK=ZH_HK
WINPE-FONTSUPPORT-ZH-TW=ZH_TW
Package_for_KB*=KB*
```

This will add the WinPE-Securestartup and the appropriate Languagepack. If you only add WINPE-SECURESTARTUP managing Bitlocker with manage-bde.exe command will **not** work!!!

Curious why we are using **YYY** and **ZZZ**? Here is the explanation:

WINPE-SECURESTARTUP requires WINPE-WMI if you are trying to add WINPE-Securestartup before WINPE-WMI it will fail. So to make sure WINPE-WMI is already added to the WINPE Bootfile we have to use the alphabet to accomplish this. So (WINPE-)WMI will be added to the Bootfile before YYY and ZZZ (which are the short names for WINPE-Securestartup and WINPE-Securestartup_EN-US

Manage-bde.exe command is included in the WINPE-Securestartup.cab File. You can find these Files on the SMP Server in a Folder called:

<Install Drive>\Program

Files\Altiris\Deployment\BDC\waik_winpe10\Tools\PETools\amd64\WinPE_FPs

Name	Date modified	Type	Size
pt-pt	09.07.2018 14:34	File folder	
ro-ro	09.07.2018 14:34	File folder	
ru-ru	09.07.2018 14:34	File folder	
sk-sk	09.07.2018 14:34	File folder	
sl-si	09.07.2018 14:34	File folder	
sr-latn-rs	09.07.2018 14:34	File folder	
sv-se	09.07.2018 14:34	File folder	
th-th	09.07.2018 14:34	File folder	
tr-tr	09.07.2018 14:34	File folder	
uk-ua	09.07.2018 14:34	File folder	
zh-cn	09.07.2018 14:34	File folder	
zh-tw	09.07.2018 14:34	File folder	
WinPE-DismCmdlets.cab	29.09.2017 00:12	Cabinet File	53 KB
WinPE-Dot3Svc.cab	29.09.2017 00:19	Cabinet File	1 606 KB
WinPE-EnhancedStorage.cab	28.09.2017 23:57	Cabinet File	92 KB
WinPE-FMAPI.cab	28.09.2017 23:59	Cabinet File	42 KB
WinPE-Fonts-Legacy.cab	29.09.2017 00:16	Cabinet File	3 129 KB
WinPE-FontSupport-JA-JP.cab	29.09.2017 00:20	Cabinet File	20 500 KB
WinPE-FontSupport-KO-KR.cab	28.09.2017 23:45	Cabinet File	10 194 KB
WinPE-FontSupport-WinRE.cab	28.09.2017 23:50	Cabinet File	2 616 KB
WinPE-FontSupport-ZH-CN.cab	29.09.2017 00:40	Cabinet File	34 760 KB
WinPE-FontSupport-ZH-HK.cab	29.09.2017 00:38	Cabinet File	29 999 KB
WinPE-FontSupport-ZH-TW.cab	29.09.2017 00:37	Cabinet File	29 994 KB
WinPE-GamingPeripherals.cab	29.09.2017 00:20	Cabinet File	322 KB
WinPE-HTA.cab	29.09.2017 01:35	Cabinet File	34 801 KB
WinPE-LegacySetup.cab	29.09.2017 02:35	Cabinet File	8 899 KB
WinPE-MDAC.cab	29.09.2017 01:11	Cabinet File	6 765 KB
WinPE-NetFx.cab	29.09.2017 02:43	Cabinet File	120 757 KB
WinPE-PlatformId.cab	29.09.2017 01:04	Cabinet File	586 KB
WinPE-PowerShell.cab	29.09.2017 01:30	Cabinet File	3 236 KB
WinPE-PPPoE.cab	29.09.2017 00:29	Cabinet File	369 KB
WinPE-RNDIS.cab	28.09.2017 23:50	Cabinet File	37 KB
WinPE-Scripting.cab	29.09.2017 01:06	Cabinet File	4 969 KB
WinPE-SecureBootCmdlets.cab	29.09.2017 00:03	Cabinet File	23 KB
WinPE-SecureStartup.cab	29.09.2017 01:14	Cabinet File	550 KB
WinPE-SecureStartup_en-us.cab	29.09.2017 00:45	Cabinet File	30 KB
WinPE-Setup.cab	29.09.2017 02:34	Cabinet File	11 654 KB

Go to the folder **en-us** and copy the File called: **WINPE-Securestatup_EN-US.cab** to **D:\Program Files\Altiris\Deployment\BDC\waik_winpe10\Tools\PETools\amd64\WinPE_FPs**
Take a look at the screenshot above.

After you have finished all the steps in this article, you can recreate your Preboot Environment within the SMP Console or create a new one for example with the name: **WinPE10_with_Bitlocker_support**. If you want, you can revert all the changes.

Make sure that if you recreate your Preboot Environemnt and you have reverted all the changes your Preboot Environment will not be able to support Bitlocker.

Troubleshooting

To enable logging for Bootwiz follow this link:

<https://www.symantec.com/docs/HOWTO84000>

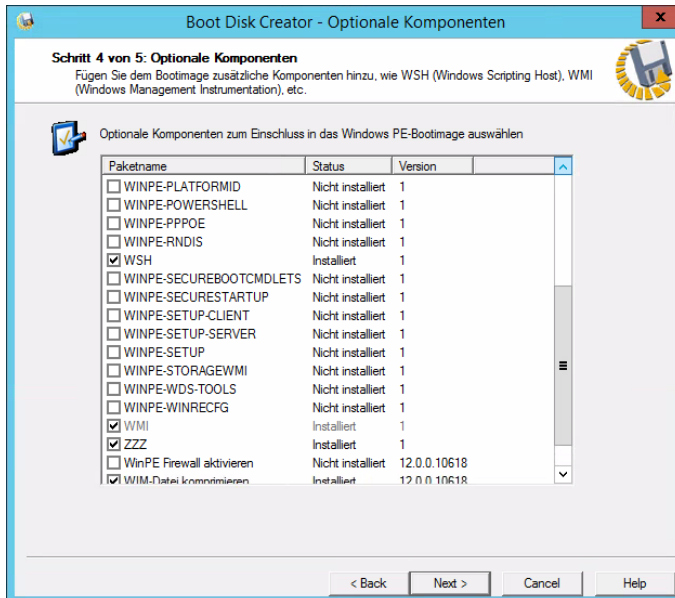
If something goes wrong, look at the Log (Dism.log)

The Dism Log is also very useful you can find it in:

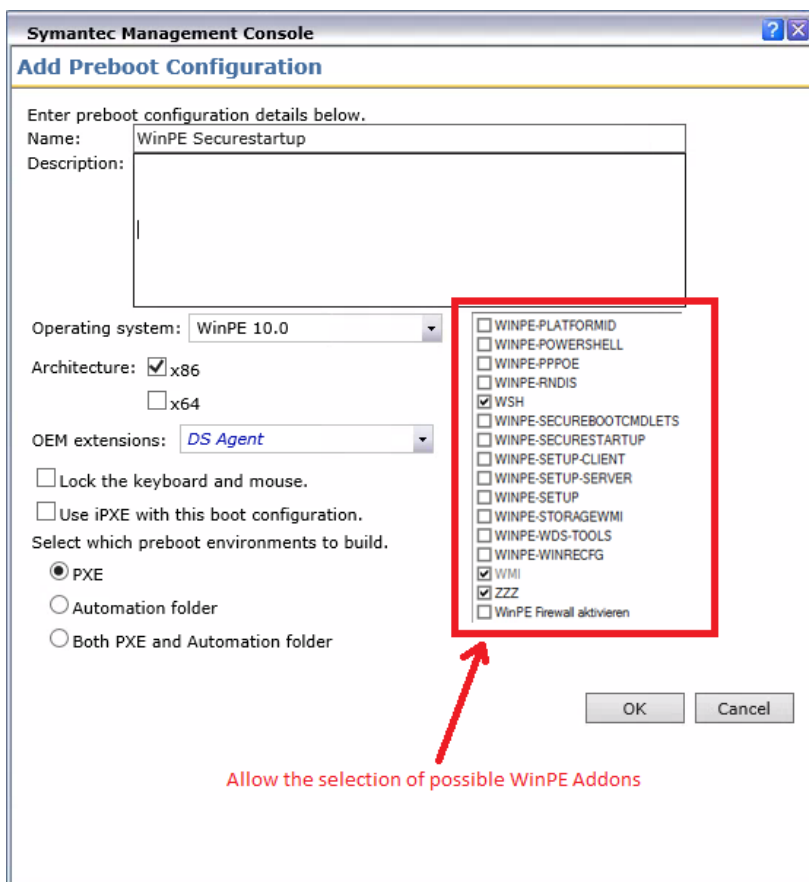
C:\windows\Logs\Dism\dism.log

What I wish from Symantec for the Future of the Product

Please allow a selection of packages when you are creating a new Preboot Environment like this is currently available when you manually run Bootwiz.exe



If you run Bootwiz manually, you will see a list of additional Components to install.



When creating new Preboot Environments allow the selection of possible WinPE Add-ons – this is far easier than modifying *.ini Files!!!