ZENworks 2020 Update 2 Troubleshooting Full Disk Encryption

August 2021

- "Windows PE Emergency Recovery Disk (ERD) is not working" on page 1
- "Issues with PBA login or boot sequence" on page 2
- "The ZENworks Endpoint Security service (ZESService) is crashing" on page 8
- "New disk drive not encrypting with existing Full Disk Encryption policy" on page 8
- "Legal Notice" on page 8

Windows PE Emergency Recovery Disk (ERD) is not working

- Make sure you have installed the correct WAIK architecture (32-bit vs 64-bit)
- (Windows 7 only) If you manually created the ERD, use the PowerShell script provided in the Cool Solutions "Windows Powershell script to create a Windows PE emergency recovery disk for ZENworks Full Disk Encryption" article.

Try creating the ERD using the ADK for Windows instead of Windows AIK. See "Creating a Windows PE Emergency Recovery Disk" in *ZENworks Full Disk Encryption Emergency Recovery Reference*.

The ZENworks PBA is not booting to the Windows operating system

Symptoms: After logging in to the PBA, the user encounters a black screen or GRUB error and the device does not boot the operating system.

To resolve this issue, you need to repair the device's master boot record or GUID partitions tables so that the device boots directly to the operating system.

1. Reboot the device that is having the issue.

2. When the black screen displays the text "Full Disk Encryption," press **Ctrl + G** on the keyboard.

   NOTE: The Full Disk Encryption text only displays for 2 seconds. The Ctrl + G command must be executed while the text is still visible.

3. A menu opens with several DMI boot options. Choose **Full Disk Encryption Simple PBA** to repair the boot sequence and load the Simple PBA login prompt.

4. Log in with authorized credentials.

You need to then modify the Direct Media Interface (DMI) file provided by ZENworks Full Disk Encryption so that it includes the correct settings to boot the device.

IMPORTANT: ZENworks added a new Linux kernel in ZENworks 2017 Update that resolves many of the PBA hardware issues that can occur when applying a new Full Disk Encryption policy.

The procedure provided below was written for ZENworks Full Disk Encryption versions prior to 2017 Update 1 and it uses the DMI settings from those versions as examples. Although this ZENworks version uses the new default DMI settings, the process for modifying the DMI file is still applicable in the event of an unknown PBA issue in ZENworks.

1. Repair the device's MBR or GPT:

   - **Windows 7:** Boot the device from a Windows 7 installation disk. When the Windows 7 splash screen displays, click **Repair your computer**. After the scan completes, select the Windows installation to repair and continue. If you are prompted to repair the problem automatically, select **No**. When the System Recovery Options dialog is displayed, click the **Command Prompt** option, then enter `bootrec.exe / fixmbr` at the command prompt. You should see a success message after running the command. Type `exit` to exit out of the command prompt and continue to boot into Windows.

   - **Windows 8 or Windows 10:**

2. Modify the `dmi.ini` file settings:

   The `dmi.ini` file provides the boot method to be used to transition from the Linux kernel to the Windows operating system. The file contains a default boot setting and a list of known hardware configurations that require different boot settings. The default setting is applied unless the device's hardware configuration is in the list. The dmi.ini file's default setting and first few entries are shown below:

`Screen` [default]

```
KICKSTART=FAST

[FUJITSU SIEMENS,LIFEBOOK C1110]
DMI_SYS_VENDOR=FUJITSU SIEMENS
DMI_PRODUCT_NAME=LIFEBOOK C1110
KICKSTART=BIOS

[LENOVO,20021,2959]
DMI_SYS_VENDOR=LENOVO
DMI_PRODUCT_NAME=20021,2959
KICKSTART=BIOS

[LENOVO,0831CTO]
DMI_SYS_VENDOR=LENOVO
DMI_PRODUCT_NAME=0831CTO
KICKSTART=KEXEC
KERNEL_PARAM=pci=snb-enable-ahci-to-legacy
```
`/ Screen`

`Para` You need to discover the correct settings for your device and add an entry to the dmi.ini file. This discovery is a trial and error process; you will need to try different settings until one enables the machine to boot successfully. `/ Para`

a. `OrderedList` `ListItem` `Para` On the device, open a command prompt with Administrator privileges, change to the `Filename` `c:\windows\nac\sbs` `/ Filename` directory, then run the `Literal` `dmiconfig dump` `/ Literal` command to see the device's current dmi.ini settings. `/ Para`

`InformalFigure` `MediaObject` `ImageObject`
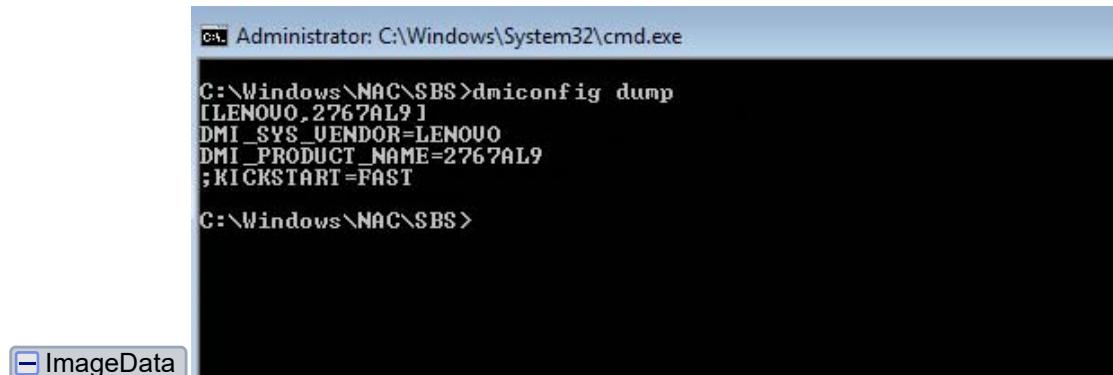
`ImageData`
`/ ImageObject` `/ MediaObject` `/ InformalFigure` `/ ListItem`

b. ListItem Para Create a new dmi.ini text file on your desktop and copy the results from the dmiconfig dump into the file. Edit the last line to remove the semicolon and change the KICKSTART value to another boot option (listed below), as shown in the following example: / Para

InformalFigure MediaObject ImageObject

ImageData

```
dmi.ini - Notepad
File  Edit  Format  View  Help
[LENOVO,2767AL9]
DMI_SYS_VENDOR=LENOVO
DMI_PRODUCT_NAME=2767AL9
KICKSTART=BIOS
```

/ ImageObject

/ MediaObject / InformalFigure

Para Finding the correct setting is a trial and error process. The possible DMI settings are listed below in the order we recommend trying them. For some settings, recommendations are given for when to use them. / Para

InformalTable TGroup / InformalTable / ListItem

Para **Setting** / Para	Para **Example** / Para

Para Literal KICKSTART=BIOS / Literal / Para
 	
Para This setting is effective in resolving issues where the ZENworks PBA displays the credential or user capture prompt but then fails to boot to Windows. / Para
	Screen `[LENOVO,2767AL9]`
	`DMI_SYS_VENDOR=LENOVO`
	`DMI_PRODUCT_NAME=2767AL9`
	`KICKSTART=BIOS` / Screen

Para Literal KICKSTART=KEXEC / Literal / Para	Screen `[LENOVO,2767AL9]`
	`DMI_SYS_VENDOR=LENOVO`
	`DMI_PRODUCT_NAME=2767AL9`
	`KICKSTART=KEXEC` / Screen

Para Literal KICKSTART=FAST / Literal / Para	Screen `[LENOVO,2767AL9]`
	`DMI_SYS_VENDOR=LENOVO`
	`DMI_PRODUCT_NAME=2767AL9`
	`KICKSTART=FAST` / Screen

Para Setting / Para	Para Example / Para
Para Literal KICKSTART=KEXEC KERNEL_PARAM=pci=snb-enable-ahci-to-legacy / Literal / Para	Screen `[LENOVO,2767AL9]` `DMI_SYS_VENDOR=LENOVO` `DMI_PRODUCT_NAME=2767AL9` `KICKSTART=KEXEC` `KERNEL_PARAM=pci=snb-enable-ahci-to-legacy` / Screen
Para Literal KICKSTART=KEXEC KERNEL=/boot/bzImage-acpi / Literal / Para Para This setting is effective in resolving issues where the ZENworks PBA screen displays but the credential or user capture prompt never displays. / Para	Screen `[LENOVO,2767AL9]` `DMI_SYS_VENDOR=LENOVO` `DMI_PRODUCT_NAME=2767AL9` `KICKSTART=KEXEC` `KERNEL=/boot/bzImage-acpi` / Screen
Para Literal KICKSTART=KEXEC KERNEL_PARAM=pci=snb-enable-ahci-to-legacy KERNEL=/boot/bzImage-acpi / Literal / Para	Screen `[LENOVO,2767AL9]` `DMI_SYS_VENDOR=LENOVO` `DMI_PRODUCT_NAME=2767AL9` `KICKSTART=KEXEC` `KERNEL_PARAM=pci=snb-enable-ahci-to-legacy` `KERNEL=/boot/bzImage-acpi` / Screen

c. ListItem Para In the Filename `c:\windows\nac\sbs` / Filename directory, make a backup copy of the current Filename `dmi.ini` / Filename file, then copy your edited Filename `dmi.ini` / Filename file to the directory. / Para / ListItem

d. ListItem + Para

InformalFigure MediaObject ImageObject

```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\NAC\SBS>dmiconfig import --force

C:\Windows\NAC\SBS>dmiconfig dump
[LENOVO,2767AL9]
DMI_SYS_VENDOR=LENOVO
DMI_PRODUCT_NAME=2767AL9
KICKSTART=BIOS

C:\Windows\NAC\SBS>
```
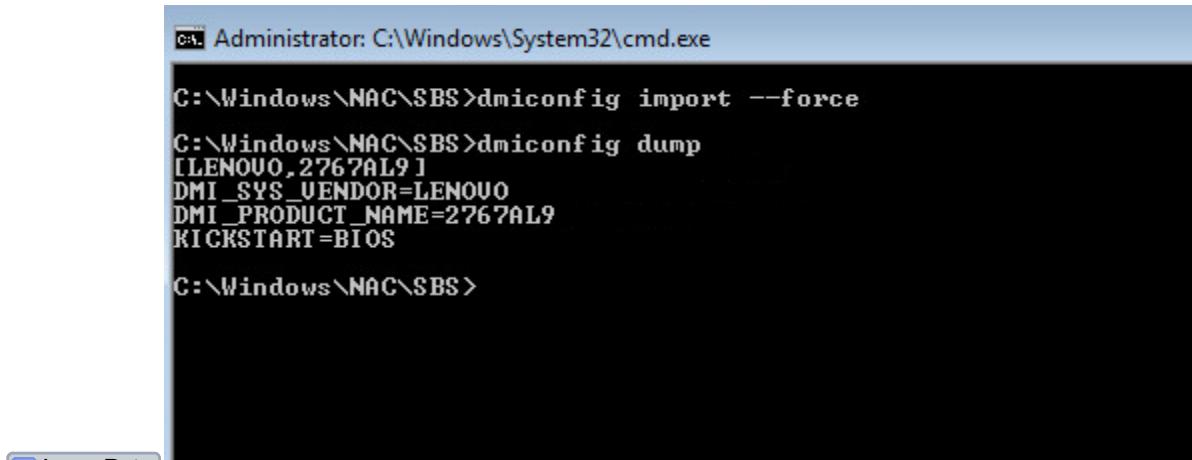
ImageData
/ ImageObject / MediaObject / InformalFigure / ListItem

e. ListItem Para Reboot the device. If the device fails to boot to the Windows operating system, repair the MBR, then repeat the above process using another setting. / Para / ListItem

f. ListItem Para After you find the correct setting, you can edit your Full Disk Encryption policy to add it to the policy's Filename `dmi.ini` / Filename file (ZENworks Control Center > GUIMenu Policies / GUIMenu > Full Disk Encryption policy details > GUIMenu DMI Settings / GUIMenu tab > GUIMenu Edit / GUIMenu). / Para / ListItem / OrderedList / ListItem / OrderedList / Sect2

Sect2 Title **The ZENworks PBA screen does not have a login prompt** / Title

FormalPara Title **Syptoms:** / Title Para When restarting an encrypted device with PBA, the PBA splash screen opens without a login prompt. / Para / FormalPara

Para To resolve this issue, you need to repair the device's master boot record or GUID partitions tables so that the device boots directly to the operating system. / Para

1 Procedure Step Para Reboot the device that is having the issue. / Para / Step

2 Step Para When the black screen displays the text Quote "Full Disk Encryption," / Quote press GUIMenu **Ctrl + G** / GUIMenu on the keyboard. / Para

Note **NOTE:** Para The Full Disk Encryption text only displays for 2 seconds. The Ctrl + G command must be executed while the text is still visible. / Para / Note / Step

3 Step Para A menu opens with several DMI boot options. Choose GUIMenu **Full Disk Encryption PBA (KICKSTART=BIOS) without DRM** / GUIMenu to repair the boot sequence and load the PBA login screen. / Para / Step

4 Step Para Log in with authorized credentials. / Para / Step / Procedure / Sect2 / Sect1

+ Sect1

Sect1 Title New disk drive not encrypting with existing Full Disk Encryption policy / Title

Para When you apply a Full Disk Encryption policy to a device, you have the option to encrypt all local fixed volumes or specify the volumes that will be encrypted. Once the policy is applied, the specified volumes are encrypted. / Para

Para If you add a new disk drive to the device, or you want to specify another volume on the device for encryption, the policy must be removed, including disk decryption, and then be reapplied to recognize the new volumes. If the existing policy is not set to encrypt all local fixed volumes, you need to edit the Local Fixed Volumes setting in the policy to recognize the new volumes before reapplying the policy and encrypting the drives. / Para

Para For information about removing, editing, and applying Full Disk Encryption policies, see the CiteTitle XRefExt *ZENworks Full Disk Encryption Policy Reference* / XRefExt / CiteTitle . / Para / Sect1

Sect1 Title Legal Notice / Title

Para For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see Ulink https://www.microfocus.com/about/legal/ / Ulink . / Para

Para Strong **© Copyright 2008 -** Phrase **2021** / Phrase **Micro Focus or one of its affiliates.** / Strong / Para

Para The only warranties for products and services of Micro Focus and its affiliates and licensors (Micro Focus) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice. / Para / Sect1 / Article