

ZENworks 11 SP4 Troubleshooting Full Disk Encryption

October 2016

Novell.

This document provides troubleshooting guidelines for common problems related to ZENworks 11 SP4 Full Disk Encryption. If, after completing the troubleshooting steps, the problem is not resolved, you should contact [Novell Technical Support \(https://www.novell.com/support/\)](https://www.novell.com/support/) for additional help.

- ◆ Section 1, “Windows PE Emergency Recovery Disk (ERD) is not working,” on page 1
- ◆ Section 2, “Only one volume is allowed to decrypt when using the ERD for multiple encrypted volumes,” on page 1
- ◆ Section 3, “Resetting an Opal drive wipes data from the drive,” on page 2
- ◆ Section 4, “Unable to apply Full Disk Encryption to an Opal drive,” on page 3
- ◆ Section 5, “Full Disk Encryption policy fails on Opal devices during version upgrade,” on page 3
- ◆ Section 6, “The ZENworks PBA is not booting to the Windows operating system,” on page 4
- ◆ Section 7, “The ZENworks Endpoint Security service (ZESService) is crashing,” on page 7
- ◆ Section 8, “Full Disk Encryption will not install on a ZENworks-imaged Windows XP device,” on page 7
- ◆ Section 9, “New disk drive not encrypting with existing Full Disk Encryption policy,” on page 8
- ◆ Section 10, “Legal Notices,” on page 8
- ◆ Section 11, “Third-Party Material,” on page 8

1 Windows PE Emergency Recovery Disk (ERD) is not working

- Make sure you have installed the correct WAIK architecture (32-bit vs 64-bit)
- If you have 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 burning the ERD to a DVD rather than a CD.

2 Only one volume is allowed to decrypt when using the ERD for multiple encrypted volumes

This issue can occur during emergency recovery when the ERI file is created under the following conditions:

- ◆ During encryption of a Windows x86 32 bit operating system, the workflow creates cached ERI files before the device reboots.
- ◆ The device has a Disk Encryption policy enforced with more than one drive being encrypted using the **Encrypt all local fixed volumes** option in the policy configuration.

or

- ◆ The device has a Disk Encryption policy enforced using the **Encrypt specific local fixed volumes** option configured, with more than one local fixed volume added in the policy configuration.

To create an ERI file that will avoid this issue and enable encryption for all volumes during emergency recovery, do the following:

- 1 Reboot the device after the encryption is complete, and manually create a new ERI file using one of the options below:
 - ◆ **Use a quick task in the ZENworks Control Center:**
 1. In ZENworks Control Center, click **Devices > Workstations**.
 2. Select the check box next to the device in the Workstations list.
 3. Click **Quick Tasks > FDE - Force Device to Send ERI File to Server**.
 4. Wait for the task to complete, and then verify that the ERI file is displayed in the device's ERI list.
 - ◆ **Use a command from the Full Disk Encryption Agent on the device:**

This option requires knowledge of the FDE Admin password.

 1. Open the ZENworks Agent on the device, and click **Full Disk Encryption** in the navigation menu.
 2. Click **About** under Full Disk Encryption Agent Actions.
 3. Click **Commands** in the Full Disk Encryption dialog box, followed by **Create ERI** in the Commands dialog box.
 4. Provide a password for the ERI file, and then click **OK** to create it.
- 2 If desired, you can save the ERI file to separate location, such as a USB drive; however, the new ERI file is also in the cache on the server.

3 Resetting an Opal drive wipes data from the drive

Resetting an Opal drive wipes all data from the drive and returns it to its original state.

1. Make sure you know the drive's Physical Security ID (PSID). The PSID is a unique 32-character alphanumeric string printed on the drive's label.
2. Boot the device using an Emergency Recovery Disk.

For information about creating an ERD, see "[Windows Powershell script to create a Windows PE emergency recovery disk for ZENworks Full Disk Encryption](#)".
3. When the Recovery application is launched, click **File > End** to exit the application.
4. In the Command Prompt window, change to the `x:\Program Files\FinallySecure` directory.
5. Run the TOPAL utility to reset the drive:

```
topal -rtp 0
```

If the drive is not drive 0, replace 0 with the correct drive number.
6. Follow the prompts to enter the PID and reset the drive.

4 Unable to apply Full Disk Encryption to an Opal drive

- ❑ Are you using a supported drive? Because of differences in the way manufacturers implement Opal technology, some Opal drives might not work. For a list of supported drives, see [ZENworks 11 SP4 Full Disk Encryption Self-Encrypting Drive Support](#).
- ❑ Is the drive not accepting a new Full Disk Encryption policy? In versions prior to 11.3.1, new policies were being corrupted on the drive's dCARD. This is fixed in 11.3.1. The only solution to this issue is to reset the drive to its original state and start over. Resetting the drive wipes all data on the drive. To reset the drive:
 1. Make sure you know the drive's Physical Security ID (PSID). The PSID is a unique 32-character alphanumeric string printed on the drive's label.
 2. Boot the device using an Emergency Recovery Disk.
 3. When the Recovery application is launched, click **File** > **End** to exit the application.
 4. In the Command Prompt window, change to the `x:\Program Files\FinallySecure` directory.
 5. Run the TOPAL utility to reset the drive:

```
topal -rtp 0
```

If the drive is not drive 0, replace 0 with the correct drive number.
 6. Follow the prompts to enter the PID and reset the drive.

5 Full Disk Encryption policy fails on Opal devices during version upgrade

Support for optional software encryption on Opal devices began in ZENworks 11.4.0. When upgrading from 11.3.x to 11.4.x or later versions, the procedure below must be followed to use an existing Full Disk Encryption policy after version upgrade.

If no Full Disk Encryption policy is in force on the Opal device (11.3.x versions) during upgrade, or if upgrading from 11.4.0 or later versions of ZENworks on the Opal device with an encryption policy enforced, the procedure is not required.

1. Remove the Full Disk Encryption policy from the ZENworks 11.3.x device before upgrading to 11.4.x or later versions, including the reboot process.

See [Policy Removal](#) in the [ZENworks 11 SP4 Full Disk Encryption Policy Reference](#) for more information.

NOTE: You do not need to delete the policy. The policy can be applied again after version upgrade.

2. Using the ZENworks Control Center, remove the Full Disk Encryption Agent from the Opal device that has the encryption policy enforced.

See [Using ZENworks Control Center to Uninstall the Full Disk Encryption Agent](#) in the [ZENworks 11 SP4 Full Disk Encryption Agent Reference](#) for more information.

3. When you have confirmed that the Full Disk Encryption Agent is removed from the device, upgrade to an 11.4.0 or newer version of ZENworks. See [Novell Downloads](#).
4. Return to the ZENworks Control Center, and reinstall the Full Disk Encryption Agent on the Opal device.

See [Agent Features](#) in the [ZENworks 11 SP4 Adaptive Agent Reference](#) for more information about installation settings.

5. Reassign the Full Disk Encryption policy to the Opal device.

See [Assigning a Disk Encryption Policy](#) in the [ZENworks 11 SP4 Full Disk Encryption Policy Reference](#) for more information on policy assignment.

NOTE: When the policy is enforced, software encryption will be the default setting on the policy. To remove the software encryption, edit the policy's [Encryption Settings](#) for software encryption of Opal drives.

6 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.

After pre-boot authentication occurs, the BIOS settings must be correctly set for Windows. With older or unusual hardware configurations, the standard ZENworks PBA boot method and Linux kernel configuration used to provide the BIOS settings might not work, resulting in hardware that does not function correctly or is not recognized by Windows.

To resolve this issue, you need to repair the device's master boot record (MBR) so that the device boots directly to the operating system. 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.

1. Repair the device's MBR:

- ♦ **Windows XP:** Boot the device from a Windows XP installation disk. Press R to use the Recovery Console. Enter the number that corresponds to your operating system (it will usually be 1) and then enter the Administrator password. Type `fixmbr`, type `y`. When finished, type `exit` to close the Recovery Console and boot to Windows.
- ♦ **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.

If you don't have a Windows 7 installation disk, you can use a Windows 7 system recovery disk. To create the disk on a working Windows 7 machine, click **Start > All Programs > Maintenance > Create a System Repair Disc**.

- ♦ **Windows 8 or Windows 10:** Boot the device from a Windows 8 or Windows 10 installation disk, respectively. When the Windows splash screen displays, click **Repair your computer**. On the next screen, select **Troubleshoot**, then select **Advanced options**. From the Advanced options, launch a command prompt, then enter `bootrec.exe /fixmbr`. When the operation is finished, reboot the device.

If you don't have a Windows 8 or Windows 10 installation disk, you can use a Windows 8 or Windows 10 system recovery disk.

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:

```
[default]
KICKSTART=FAST

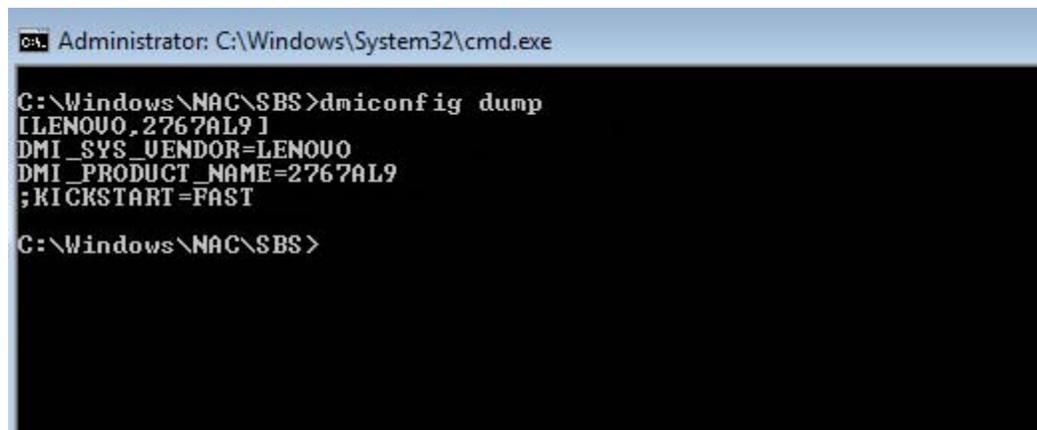
[FUJITSU SIEMENS,LIFEBOOK C1110]
DMI_SYS_VENDOR=FUJITSU SIEMENS
DMI_PRODUCT_NAME=LIFEBOOK C1110
KICKSTART=BIOS

[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
```

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.

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



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

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

C:\Windows\NAC\SBS>
```

- b. 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:

```

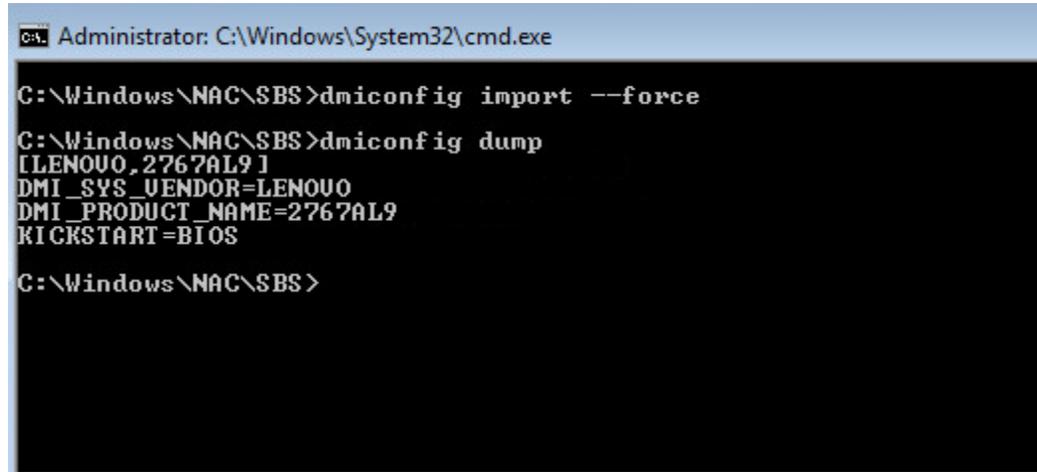
dmi.ini - Notepad
File Edit Format View Help
[LENOVO,2767AL9]
DMI_SYS_VENDOR=LENOVO
DMI_PRODUCT_NAME=2767AL9
KICKSTART=BIOS

```

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.

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

- c. In the `c:\windows\nac\sbs` directory, make a backup copy of the current `dmi.ini` file, then copy your edited `dmi.ini` file to the directory.
- d. Open a command prompt with Administrator privileges, change to the `c:\windows\nac\sbs` directory, then run the `dmiconfig import --force` command to import the settings from the new `dmi.ini` file. Run `dmiconfig dump` to verify the change.



```
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>
```

- e. 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.
- f. After you find the correct setting, you can edit your Full Disk Encryption policy to add it to the policy's `dmi.ini` file (ZENworks Control Center > **Policies** > Full Disk Encryption policy details > **DMI Settings** tab > **Edit**).

7 The ZENworks Endpoint Security service (ZESService) is crashing

- Check to see if the device is using the Intel IRRT driver. This driver causes the device to crash and is not supported. If the device is using the driver:
 1. Disable the driver through the device's adapter settings.
 2. Reboot the device to BIOS and change from IRRT to AHCI mode.

8 Full Disk Encryption will not install on a ZENworks-imaged Windows XP device

Full Disk Encryption creates a 100 MB partition on the device when the policy is first applied. On Windows XP devices that have been imaged by ZENworks, Full Disk Encryption can't create the partition unless there is unallocated disk space.

- Use a partition management tool to designate at least 120 MB as unallocated disk space, then apply the Full Disk Encryption policy again.

9 New disk drive not encrypting with existing Full Disk Encryption policy

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.

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.

For information about removing, editing, and applying Full Disk Encryption policies, see the [ZENworks 11 SP4 Full Disk Encryption Policy Reference](#).

10 Legal Notices

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

Copyright © 2016 Novell, Inc. All Rights Reserved.

11 Third-Party Material

All third-party trademarks are the property of their respective owners.