ZENworks 2017 Update 4 Troubleshooting Full Disk Encryption

January 2019

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

1 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 the *ZENworks Full Disk Encryption Emergency Recovery Reference*.
- Try burning the ERD to a DVD rather than a CD.

2 Issues with PBA login or boot sequence

After pre-boot authentication occurs, the BIOS or UEFI settings must be correctly set for Windows. With unusual DMI 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.

Beginning in ZENworks 2017 Update 2, the Full Disk Encryption Agent includes DMI menu options to repair the boot sequence for issues relating to these DMI configurations. This menu is accessible by using the Ctrl + G keyboard command at a brief point when Full Disk Encryption is shown during a device restart.

Menu boot options:

Full Disk Encryption PBA (previous)
Full Disk Encryption Simple PBA
Full Disk Encryption PBA (KICKSTART=FAST)
Full Disk Encryption PBA (KICKSTART=BIOS)
Full Disk Encryption PBA (KICKSTART=BIOS) low resolution
Full Disk Encryption PBA (KICKSTART=BIOS) without DRM
Full Disk Encryption Debug PBA (KICKSTART=FAST)
Full Disk Encryption Debug PBA (KICKSTART=BIOS)

Full Disk Encryption Debug PBA (KICKSTART=BIOS) without DRM

Windows Boot Manager

The two issues below are known issues that are resolved with the DMI repair options indicated. If you experience a different issue in the boot process on devices using PBA, you can troubleshoot by trying different options in this menu.

2.1 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.

2.2 The ZENworks PBA screen does not have a login prompt

Syptoms: When restarting an encrypted device with PBA, the PBA splash screen opens without a login prompt.

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 PBA (KICKSTART=BIOS) without DRM** to repair the boot sequence and load the PBA login screen.
4. Log in with authorized credentials.

3 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.

4 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 Full Disk Encryption Policy Reference*.

5 Legal Notice

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/.