ZENworks Full Disk Encryption Self-Encrypting Drive Compatibility Testing

December 2016

MICRO FOCUS

This document provides instructions for testing OPAL 2.0 self-encrypting drives for *drive-locking compatibility* with ZENworks Full Disk Encryption.

For a list of known drive-locking compatible and incompatible drives, see *ZENworks Full Disk Encryption Self-Encrypting Drive Support*.

1 Why Test for Drive-Locking Compatibility?

Knowing if a self-encrypting drive is drive-locking compatible lets you choose the correct policy mode:

- **Pre-boot authentication with drive locking (compatible drives):** This mode is only supported on OPAL 2.0 compliant drives with drive-locking that is compatible with ZENworks Full Disk Encryption. When using this mode, drive locking is initiated during ZENworks PBA initialization. After user authentication occurs through the ZENworks PBA, the drive is unlocked until it is powered off. Only the drive's native hardware encryption is used; ZENworks does not apply software-based encryption in this mode.
- **Pre-boot authentication with software-based encryption (incompatible drives):** This mode is supported on *ALL* OPAL 2.0 compliant drives. Instead of using OPAL drive-locking, ZENworks Full Disk Encryption applies software-based encryption to add a second layer of encryption to the drive's native hardware encryption.

The Disk Encryption policy includes an **Enable software encryption on Opal compliant self-encrypting drives** option that turns off drive locking and turns on software encryption. You need to use this option with all drives that are incompatible with drive locking. With drives that are compatible, you can use either drive locking or software-based encryption.

2 Testing Drive-Locking Compatibility

1 Identify a device that has the drive you want to test.

Always test a single device before rolling it out to other devices that have the same drive model.

2 Prepare the device for the test:

2a If necessary, register the device in your ZENworks Management Zone.

You install the ZENworks Agent on the device to register it. For help, see "Manually Deploying the Agent on Windows" in the *ZENworks Discovery, Deployment, and Retirement Reference*.

2b Make sure that ZENworks Full Disk Encryption is enabled on the device.

Right-click the ZENworks icon in the system tray of the device, and select **Technician Application** to display the ZENworks Agent properties. If **Full Disk Encryption** is displayed in the left navigation pane, ZENworks Full Disk Encryption is enabled on the device.

For help enabling ZENworks Full Disk Encryption, see "Configuring Agent Settings on the Device Level" in the *ZENworks Agent Reference*.

2c Take an image of the device.

Re-imaging is the easiest way to recover a device if its drive is not compatible with Full Disk Encryption.

3 Test the device to ensure that the ZENworks PBA can interface with the device hardware.

Before you can test the drive for OPAL compatibility, you need to ensure that the ZENworks PBA can interface with the device hardware. If the ZENworks PBA cannot interface with the device hardware, it fails at startup in the same way it would if the drive were incompatible. Therefore, you need to ensure hardware compatibility before testing for OPAL compatibility. You do this by applying a Disk Encryption policy that is configured to not perform drive locking and then verifying that the ZENworks PBA can boot to the Windows operating system.

3a Create a Disk Encryption policy that is configured as follows:

- The **Enable software encryption of Opal compliant self-encrypting drives** option is turned on.
- Pre-boot authentication is enabled and configured.

For help creating the policy, see “Creating a Disk Encryption Policy” in the *ZENworks Full Disk Encryption Policy Reference*.

3b Assign the policy to the device.

For help assigning the policy, see “Assigning a Disk Encryption Policy” in the *ZENworks Full Disk Encryption Policy Reference*.

3c On the device, right-click the ZENworks icon, then click **Refresh** to apply the policy.

3d When the ZENworks PBA displays, enter your authentication credentials.

If Windows launches, the ZENworks PBA can interface with the device hardware. If you encounter a black screen or GRUB error, the ZENworks PBA cannot interface with the device hardware with its current boot settings. You need to modify the boot settings using the instructions provided in “The ZENworks PBA is not booting to the Windows operating system” in *ZENworks 2017 Troubleshooting Full Disk Encryption*.

3e After you find the correct boot settings, save a copy of the modified `dmi.ini` file to a location other than the device (for example, a removable USB drive).

4 Test the device for OPAL compatibility.

4a Create a Disk Encryption policy that is configured as follows:

- The **Enable software encryption of Opal compliant self-encrypting drives** option *is not* turned on.
- Pre-boot authentication is enabled and configured.
- If you had to modify the dmi.ini file to enable the ZENworks PBA to interface with the device hardware (Step 3), add your changes to the policy’s DMI Settings so that the appropriate boot settings are applied in the policy.

For help creating the policy, see “Creating a Disk Encryption Policy” in the *ZENworks Full Disk Encryption Policy Reference*.

4b Assign the policy to the device.

For help assigning the policy, see “Assigning a Disk Encryption Policy” in the *ZENworks Full Disk Encryption Policy Reference*.

4c On the device, right-click the ZENworks icon, then click **Refresh** to apply the policy.

After the device reboots, if the ZENworks PBA displays and you can log in and boot to the Windows operating system, the drive is compatible.

If the ZENworks PBA does not display or present a log in option, the drive is not compatible and you need to use the Emergency Recovery Disk to boot and reset the drive. For help, see “Resetting an Opal drive” in *ZENworks 2017 Troubleshooting Full Disk Encryption*.

5 If the drive is compatible, enable the Disk Encryption policy (with the software encryption option *disabled*) to devices that have the same drive model.

or

If the drive is incompatible, enable the Disk Encryption policy (with the software encryption option *enabled*) to devices that have the same drive model.

3 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/.

Copyright © 2016 Micro Focus Software, Inc. All Rights Reserved.

4 Third-Party Material

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