

ZENworks 11 SP4 Full Disk Encryption Deployment on Self-Encrypting Drives

October 2016

Novell

ZENworks Full Disk Encryption supports all self-encrypting hard drives that are compliant with the *Trusted Computing Group OPAL 2.0* specification.

This Quick Start helps you deploy ZENworks Full Disk Encryption to OPAL 2.0 compliant self-encrypting drives.


WARNING: When applying a full disk encryption policy, ensure that the encryption process is not interrupted prematurely with a power change on the disk drive(s); otherwise, all data on the disk can be lost due to disk corruption. You can check the encryption status on the device by accessing **Full Disk Encryption > About** in the ZENworks Adaptive Agent.

Disk corruption due to power change has only been noted on secondary drives, but it may also be applicable to primary drives. For this reason, the following precautions are strongly recommended before applying a full disk encryption policy to a device:

- ♦ If possible, select the AES algorithm when configuring the full disk encryption policy.

Selecting the AES algorithm should preclude disk corruption from occurring in the event of a power-down during encryption. However, the additional precautions are best practices that will reduce the risk of possible disk corruption.

- ♦ Pre-configure devices receiving the policy so that power options are set to never automatically shut off, hibernate, or sleep.
 - ♦ Inform all device users of the need to keep their devices running during the encryption process, to include avoiding *Sleep* and *Hibernation* options.
-

Task	Details
<input type="checkbox"/> Decide which encryption mode to apply to the drive.	<p>The two modes of support are:</p> <ul style="list-style-type: none"> ♦ Pre-boot authentication with software-based encryption: This mode is supported on <i>ALL</i> OPAL 2.0 compliant drives. <p>Pre-boot authentication is the process of authenticating a user to a device before the device boots to the primary operating system. Using ZENworks pre-boot authentication (ZENworks PBA) in conjunction with Windows login greatly enhances drive security. Software-based encryption adds a second layer of encryption to the drive's native hardware encryption.</p> <ul style="list-style-type: none"> ♦ Pre-boot authentication with drive locking: This mode is supported on <i>SOME</i> OPAL 2.0 compliant drives. Support is limited because of variations in the way drive manufacturers implement the OPAL 2.0 specification related to drive locking. <p>When using this mode, drive locking is initiated during ZENworks PBA initialization. After user authentication occurs through the ZENworks PBA, the drive is unlocked. The drive remains unlocked until it is powered off, at which point it is locked again. Only the drive's native hardware encryption is used; ZENworks does not apply software-based encryption in this mode.</p> <p>For a list of known drive-locking compatible and incompatible drives, see ZENworks 11 SP4 Full Disk Encryption Self-Encrypting Drive Support.</p> <p>For help testing a drive for drive-locking compatibility, see ZENworks 11 SP4 Full Disk Encryption Self-Encrypting Drive Compatibility Testing.</p>
<input type="checkbox"/> Make sure the Windows device with the self-encrypting drive meets the requirements for a ZENworks managed device.	<p>The Windows device must meet certain requirements to support the ZENworks Adaptive Agent as well as the ZENworks Full Disk Encryption Agent.</p> <p>See Managed Device Requirements in the ZENworks 11 SP4 Full Disk Encryption Agent Reference.</p>
<input type="checkbox"/> Install the ZENworks Adaptive Agent on the Windows device (if necessary) and make sure that Full Disk Encryption is enabled.	<p>If the ZENworks Adaptive Agent is not installed on the device and you need help installing the agent, see Deploying the ZENworks Adaptive Agent in the ZENworks 11 SP4 Discovery, Deployment, and Retirement Reference.</p> <p>Check that ZENworks Full Disk Encryption is enabled by double-clicking the ZENworks icon  in the system tray of the device to display the ZENworks Adaptive 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 11 SP4 Adaptive Agent Reference.</p>

Task	Details
<input type="checkbox"/> Create the Disk Encryption policy to apply to the device.	<p>The Disk Encryption policy contains the pre-boot authentication and encryption settings to apply to the device. Create a Disk Encryption policy that is configured as follows:</p> <ul style="list-style-type: none"> ♦ The Enable software encryption of Opal compliant self-encrypting drives option is turned OFF. Turning off this option causes drive-locking to be enabled and software encryption to be disabled. ♦ Pre-boot authentication is enabled and configured. <p>For help creating the policy, see Creating a Disk Encryption Policy in the <i>ZENworks 11 SP4 Full Disk Encryption Policy Reference</i>.</p>
<input type="checkbox"/> Assign the policy to the device.	<p>If you have multiple devices with the same self-encrypting drive, you should initially assign the policy to one device and ensure that it works on the device before rolling the policy out to other devices.</p> <p>For help assigning the policy, see “Assigning a Disk Encryption Policy” in the <i>ZENworks 11 SP4 Full Disk Encryption Policy Reference</i>.</p>
<input type="checkbox"/> Enforce the policy on the device.	<p>On the device, right-click the ZENworks icon, then click Refresh to apply the policy. After the device reboots, log in to the ZENworks PBA and boot to the Windows operating system.</p> <p>If the ZENworks PBA does not display or does not present a log in option AND you did not previously test the drive for drive-locking compatibility, the drive might not be compatible. Use a Emergency Recovery Disk to boot and reset the drive (see “Resetting an Opal drive” in <i>ZENworks 11 SP4 Troubleshooting Full Disk Encryption</i>), then test for drive-locking compatibility (see <i>ZENworks 11 SP4 Full Disk Encryption Self-Encrypting Drive Compatibility Testing</i>).</p> <p>If you can log in to the ZENworks PBA but the device then fails to boot to Windows, see “The ZENworks PBA is not booting to the Windows operating system” in <i>ZENworks 11 SP4 Troubleshooting Full Disk Encryption</i>.</p>
<input type="checkbox"/> Check the policy status.	<p>On the device, double-click the ZENworks icon, then click Full Disk Encryption. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box. The Status field displays the current policy status. When initial enforcement is complete, the status will be Policy enforced, with drive encrypted.</p>

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.

Third-Party Material

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