ZENworks 11 SP4 Full Disk Encryption Deployment on Standard Drives

October 2016

Novell

This Quick Start helps you deploy ZENworks Full Disk Encryption to IDE, SATA, and PATA standard hard disks (non-self encrypting disks).

With standard hard disks, ZENworks Full Disk Encryption provides sector-based encryption of the entire disk or selected volumes (partitions). All files on a volume are encrypted, including any temporary files, swap files, or operating system files. Because all files are encrypted, the data cannot be accessed when booting the computer from external media such as a CD-ROM, floppy disk, or USB drive. You can choose the industry-standard encryption algorithm (AES, Blowfish, DES, or DESX) and key length that best meets your organizations requirements.

As an added layer of security, ZENworks Full Disk Encryption provides optional pre-boot authentication. With pre-boot authentication, the device boots to a Linux partition and loads the ZENworks Pre-Boot Authentication (PBA) module. As soon as the user provides the appropriate credentials (user ID/password or smart card), the PBA terminates and the Windows operating system boots, providing access to the encrypted data on the previously hidden and inaccessible Windows 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
❒	Make sure the hard drive meets the requirements for full disk encryption.	See Standard Hard Disk Requirements in the *ZENworks 11 SP4 Full Disk Encryption Agent Reference*.

	Task	Details
❒	Make sure the Windows device with the hard drive meets the requirements for a ZENworks managed device.	The Windows device must meet certain requirements to support the ZENworks Adaptive Agent as well as the ZENworks Full Disk Encryption Agent. See Managed Device Requirements in the *ZENworks 11 SP4 Full Disk Encryption Agent Reference*.
❒	Install the ZENworks Adaptive Agent on the Windows device (if necessary) and make sure that Full Disk Encryption is enabled.	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*. Check that ZENworks Full Disk Encryption is enabled by double-clicking the ZENworks icon in the notification area 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*.
❒	Create the Disk Encryption policy to apply to the device.	The Disk Encryption policy contains the encryption and pre-boot authentication settings to apply to the device. For help creating the policy, see Creating a Disk Encryption Policy in the *ZENworks 11 SP4 Full Disk Encryption Policy Reference*.
❒	Assign the policy to the device.	For help assigning the policy, see "Assigning a Disk Encryption Policy" in the *ZENworks 11 SP4 Full Disk Encryption Policy Reference*.
❒	Enforce the policy on the device.	On the device, right-click ZENworks icon, then click **Refresh** to apply the policy. After the device reboots, log in to the ZENworks PBA (if the PBA is enabled) and boot to the Windows operating system. 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 *ZENworks 11 SP4 Troubleshooting Full Disk Encryption*.
❒	Check the encryption status.	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 encryption status. When initial encryption is complete, the status will be **Policy enforced, with drive encrypted**.

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/.

Third-Party Material

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