This Quick Start helps you deploy ZENworks Full Disk Encryption to IDE, SATA, and PATA hard disks.

With hard disks, ZENworks Full Disk Encryption provides sector-based encryption of the entire disk or selected volumes (partitions). All files on a volume are software 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 a 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 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐ Make sure the hard drive meets the requirements for full disk encryption.</td>
<td>See “Managed Device Requirements” in the ZENworks Full Disk Encryption Agent Reference.</td>
</tr>
<tr>
<td>☐ Make sure the Windows device with the hard drive meets the requirements for a ZENworks managed device.</td>
<td>The Windows device must meet certain requirements to support the ZENworks Agent as well as the ZENworks Full Disk Encryption Agent. See “Managed Device Requirements” in the ZENworks Full Disk Encryption Agent Reference.</td>
</tr>
</tbody>
</table>
Install the ZENworks Agent on the Windows device (if necessary) and make sure that Full Disk Encryption is enabled.

Create the Disk Encryption policy to apply to the device.

Assign the policy to the device.

Enforce the policy on the device.

Check the encryption status.

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 2008 - 2019 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (Micro Focus) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.