# ZENworks Full Disk Encryption 2017 Update 1 Overview

July 2017

ZENworks Full Disk Encryption uses software-based encryption and pre-boot authentication to protect the data on a device's hard disk when the device is powered off or in hibernation mode. The disk encryption and pre-boot authentication settings are applied to the device through a Disk Encryption policy.

## 1 Disk Encryption

ZENworks Full Disk Encryption supports encryption on standard, solid state, and self-encrypted 3.5 or 2.5 inch IDE, PATA, or SATA disks.

Full Disk Encryption does sector-based software 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. For an authenticated user, accessing data on the encrypted disk is no different than accessing data on an unencrypted disk.

You can choose the industry-standard encryption algorithm (AES, Blowfish, DES, or DESX) and the key length that best meets your organizations requirements.

---

**NOTE:** The cryptographic module used in ZENworks Full Disk Encryption to encrypt hard drives is *not* Federal Information Processing Standard (FIPS) 140-2 certified. However, the cryptographic module implements standards consistent with FIPS 140-2 Level 1 certification.

---

## 2 Pre-Boot Authentication

ZENworks Full Disk Encryption protects a device's data when the device is powered off or in hibernation mode. As soon as someone successfully logs in to the Windows operating system, the encrypted volumes are no longer protected and the data can be freely accessed. To provide increased login security, you can use ZENworks Pre-Boot Authentication (ZENworks PBA).

The ZENworks PBA is a Linux-based component. When the Disk Encryption policy is applied to a device with a standard hard disk, a 500 MB partition containing a Linux kernel and the ZENworks PBA is created on the hard disk.

During normal operation, the device boots to the Linux partition and loads the ZENworks PBA. 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.

The Linux partition is hardened to increase security, and the ZENworks PBA is protected from alteration through the use of MD5 checksums and uses strong encryption for authentication keys.

ZENworks Pre-Boot Authentication is strongly recommended. If you don't use the ZENworks PBA, encrypted data is protected only by Windows authentication.

For more information about ZENworks Pre-Boot Authentication, see the *ZENworks Full Disk Encryption PBA Reference*

# 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/.