OpenText ZENworks Full Disk Encryption

Deploy policies to guarantee you encrypt all hard disks containing sensitive data, ensuring that the data remains protected if the device is lost or stolen. Benefit from encryption that doesn't lock IT out of its management role.

Benefits

- OpenText ZENworks Full Disk Encryption meets the needs of your company's data protection security requirements and key regulations without making your fleet difficult to manage:
- Protect your company data with the proven reliability of encrypting the entire hard disk drive.
- Ensure that encrypted devices remain easy to manage across the enterprise. You can remotely unlock devices that are protected by full disk encryption and keep users productive while they work remotely.
- Ensure that you meet critical industryguidelines and government regulations for protecting customer and patient data.
- Leverage your experience with OpenText ZENworks to reduce the cost of implementing full disk encryption.

OpenText ZENworks Full Disk Encryption enables you to centrally enforce policies for encrypting entire hard disks on Windows 7, Windows 8, and Windows 10 machines in your organization. You manage them using the same web-based console and adaptive agent that you use for other OpenText ZENworks products.

Key features

OpenText ZENworks Full Disk Encryption is part of the OpenText ZENworks platform, which includes a unified web-based console, a single OpenText ZENworks adap-tive agent, and OpenText ZENworks server software. It offers the following integrated full disk encryp-tion features:

Protect your data

- Federal Information Processing Standards (FIPS) 140-2 Level 2 encryption module when used in conjunction with OPAL-compliant hardware encryption.
- FIPS 140-2 Level 1 encryption module when used with software-based encryption.
- Requires users to authenticate prior to booting the system, using either their username and password or their smartcardwith a personal identification number (PIN).
- Lets you immediately decommission any device that the OpenText ZENworks server can reach.
- Includes a stand-alone tool for testing OPAL self-encrypting drives to determine whether or not they are compatible with OpenText ZENworks Full Disk Encryption.

Centrally select the devices in your environment to encrypt

- A centralized browser-based interface allows you to quickly and easily create encryption policies for devices.
- A firewall-friendly agent allows you to deliver policies to any device that can connect to the OpenText ZENworks server using a standard HTTP web connection.
- Comprehensive policies to centrally manage OPAL-compliant hardware encryption and OpenText ZENworks software full disk encryption.

- An option lets you continue to use Windows authentication instead of preboot authentication, providing a secure hard drive without changing the end user experience.
- An enable encryption lockdown setting prevents drive decryption from occurring without administrator intervention when a full disk encryption policy is removed from a device.

Keep your users productive

- Users do not need to bring in their devices for you to encrypt them.
- Centralized key management means the help desk always has access to the encryption keys in the event of a hardware failure.
- Centralized preboot authentication override means help desk agents can grant access to users who forget their password.
- Transparent encryption means the users don’t see a difference in their experience, unless you require preboot authentication.
- Encryption and decryption occur in the background.

Learn more at http://www.opentext.com/products/zenworks-full-disk-encryption