



PGP® Whole Disk Encryption Workgroup Edition

The full-disk encryption solution for small companies and workgroups

Part of the PGP® Encryption Platform

Benefits

- **Reduces risk of data loss** – encrypts desktops, laptops, and USB devices, protecting data and helping to meet partner and regulatory mandates for information security and privacy.
- **Simple, intuitive administration** – Configures policy using just a few clicks with an easy-to-use administration interface.
- **Supports compliance** – Detailed summary logs and reports show encryption status to help demonstrate compliance in the event of an audit.
- **Transparent user experience** – Automatic and background operation does not affect user productivity.

PGP Customer Spotlight

“A huge weight has been lifted off my shoulders since PGP Whole Disk Encryption was installed on my laptop. It’s a tremendous benefit to be able to take my laptop wherever I go and not have to worry.”

Jon Allen
Information Security Officer
Baylor University

Full-disk Encryption for Desktops, Laptops, and USB Devices

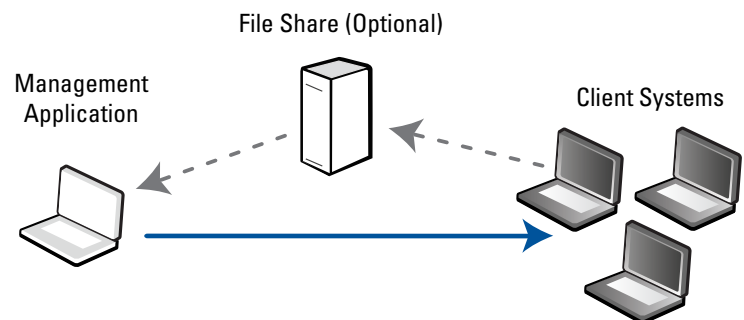
Mobile computers have quickly emerged as industry-standard tools for increasing communication and user productivity. Unfortunately, unprotected laptops and USB devices pose a critical risk to an enterprise’s most sensitive data: customer information, financial data, trade secrets, and other proprietary information. Exposure of this data can result in financial losses, legal ramifications, and brand damage.

Complete Solution

PGP® Whole Disk Encryption Workgroup Edition is a comprehensive full-disk protection solution that provides industry-leading encryption for desktops, laptops, and USB devices with simple administration.

No Specialized Training Required

With PGP Whole Disk Encryption Workgroup Edition, there are no servers or databases to configure and manage. Policy administration is easy to use and intuitive. PGP Whole Disk Encryption Workgroup Edition can be configured and deployed with a basic knowledge of Microsoft® Windows administration.



PGP Whole Disk Encryption Workgroup Edition Deployment

Reduces Risk of Data Loss

PGP® Whole Disk Encryption Workgroup Edition provides multi-layered data protection.

- **Disks and USB devices** – Protects internal and external disks and removable USB devices.
- **PGP® Virtual Disk, PGP® Zip** – Encrypt the entire contents of storage volumes and zip files automatically.
- **Automatic protection** – Policy-driven operation ensures that organizations can automatically enforce and protect data without user intervention.

Intuitive and Simple Administration

The simple management application can run on any existing Windows® system and does not require management of servers or databases.

- **Stamp-and-deploy** – Configures policy and creates a client installer with a few clicks. PGP Whole Disk Encryption clients can be deployed using any software deployment tool.
- **Remote and local help** – A one-time use recovery token or an administrator key provides secure data access to users who have forgotten or lost their passwords; keys may be stored on a tamper-proof smart card or hardware token.
- **Logging** – Detailed logs show encryption status and other attributes.

Transparent User Experience

After deployment of PGP Whole Disk Encryption Workgroup Edition, its operation is completely transparent to users.

- **Business as usual** – The software automatically encrypts and decrypts data on the fly, ensuring data protection without requiring changes in user behavior.
- **Single Sign-on** – Pre-boot authentication integrates with each user's existing Windows login credential to protect data against unauthorized access without burdening the user with remembering additional authentication credentials.

Supports Compliance

PGP Whole Disk Encryption Workgroup Edition helps support compliance demonstration in the event of an audit.

- **Detailed and summary reports** – Encryption status and systems encrypted reports readily support compliance initiatives.
- **Corporate access to data** – Administrators can access a protected device using an administrator key that may be stored on a tamper-proof smart card or hardware token. If a user forgets a password, leaves the organization, or is otherwise unavailable, data remains accessible to the organization in the case of an investigation or audit.

Technical Specifications

For complete technical specifications, please visit www.pgp.com.

PGP and the PGP logo are registered trademarks of PGP Corporation. Product and brand names used in the document may be trademarks or registered trademarks of their respective owners. Any such trademarks or registered trademarks are the sole property of their respective owners.



PGP Corporation
www.pgp.com

PGP Corporate Headquarters
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44 (0)20 8606 6000

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308

© 2009 PGP Corporation
WDEWEDS090324