PGP® Whole Disk Encryption 9.9

Proactively secure confidential data on disks and removable media

Part of the PGP® Encryption Platform

Benefits

- **Easy, automatic operation** – Protects data without changing the user experience.
- **Enforced security policies** – Automatically enforce data protection with centrally managed policies.
- **Accelerated deployment** – Achieves full disk encryption using the existing infrastructure.
- **Reduced operation costs** – Result from centrally automating encryption policies.

PGP Customer Spotlight

H&R Block, the world's largest tax services company, deployed PGP® Whole Disk Encryption to more than 20,000 systems in a few weeks to demonstrate regulatory compliance and gain customer trust.

Comprehensive disk encryption for securing all files on desktops, laptops, or removable media

Mobile computers are quickly emerging as the industry standard for increasing user productivity. However, the portable nature of these devices increases the possibility of loss or theft. Consequent exposure of sensitive data can result in financial loss, legal ramifications, and brand damage.

PGP Whole Disk Encryption provides enterprises with comprehensive, nonstop disk encryption for Microsoft Windows and Apple Mac OS X, enabling quick, cost-effective protection for data on desktops, laptops, and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity.

PGP Whole Disk Encryption can be deployed in conjunction with an optional PGP Universal™ Server. With PGP Universal Server, organizations can centrally define security policy to enforce protection of sensitive data for groups of user defined in an enterprise directory. Centralized reporting and logging provides details on the status of protection provided by PGP Whole Disk Encryption in an organization to simplify meeting compliance and auditor requirements.

Full Disk Protection

PGP Whole Disk Encryption locks down the entire contents of a laptop, desktop, external drive, or USB flash drive, including boot sectors, system, and swap files. The encryption is transparent to the user, automatically protecting data.

PGP Encryption Platform–Enabled

PGP Whole Disk Encryption is a PGP Encryption Platform–enabled application. The PGP Encryption Platform provides a strategic enterprise encryption framework for shared user management, policy, and provisioning, automated across multiple, integrated encryption applications. As a PGP Encryption Platform–enabled application, PGP Whole Disk Encryption can be used with PGP Universal Server to manage existing policies, users, keys, and configurations, expediting deployment and policy enforcement. PGP Whole Disk Encryption can also be used in combination with other PGP encryption applications to provide multiple layers of security.

Easy, Automatic Operation

Once PGP Whole Disk Encryption is deployed, its operation is completely transparent— users simply continue to work as usual. The software automatically encrypts and decrypts data on-the-fly, ensuring data protection without requiring changes in users' behavior

- New: **Multi-platform disk encryption:** Pre-boot authentication and full disk encryption for Apple Mac OS X.
- New: **Expanded international keyboard support** – Use over 30 international keyboards in pre-boot authentication.
- **Single sign-on** – Provides simplified login experience using existing Windows' password.
- **Multiple ways to protect data** – Protect sensitive data in transport using PGP® Zip and PGP® Self-Decrypting Archive and in storage using PGP® Virtual Disk.

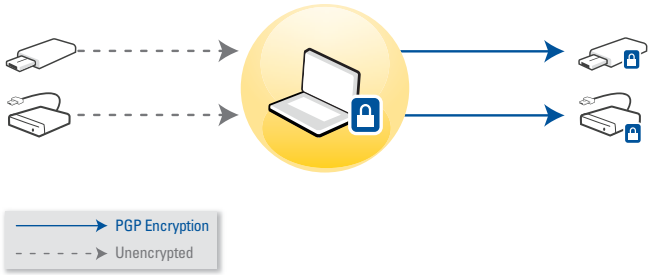
Enforced Security Policies

Security policy configured in PGP Universal Server ensures that local and removable media is encrypted, defending data transported on easily lost devices from unauthorized access.

- New: **Expanded device security policy** – Limit access to systems after failed pre-boot authentication login attempts.
- New: **PGP® Endpoint integration:** Prevent data loss and enforce device usage policies when used with PGP Endpoint.
- **Client controls** – Enable the organization to better meet security requirements by locking down which features are enabled, visible to the user, and enforced.
- **Status reporting** – Enables inspection and reporting on the state of disk encryption to satisfy regulatory requirements and help prevent a data breach.
- **Strong authentication options** – Perform pre-boot authentication using smart cards, USB tokens, and trusted platform modules (TPM).

Accelerated Deployment

Used together, PGP Whole Disk Encryption and PGP Universal Server's unified management console establish, enforce, and update security policy in real time. This combination reduces the time and effort required to deploy full disk encryption.



Comprehensive defense for local and remote media.

Reduced Operation Costs

With PGP Whole Disk Encryption, no special training is required for end users. This approach accelerates deployment time, reduces training costs, and avoids any increase in help desk calls.

PGP Universal Server Management

PGP Whole Disk Encryption can be centrally deployed and managed when used with PGP Universal Server (optional), enabling organizations to easily set and enforce data security polices throughout the enterprise.

- **Centrally enforced security policy** – Automatically enforces protection of sensitive data using security policies driven by an existing corporate directory.
- **Recovery passphrase** – Automatically generates and stores a unique one-time-use recovery passphrase to ensure authorized access to encrypted data.
- **Extensible protection** – When licensed for multiple applications, allows management of PGP® NetShare or any other PGP Encryption Platform–enabled application.

Technical Specifications

PGP Whole Disk Encryption supports Windows Vista (all 32- and 64-bit editions), Windows XP (32- and 64-bit editions), Windows 2000 Professional (SP4), and Mac OS X 10.4 and 10.5 (Intel only). For complete technical specifications and operating system supported functionality, 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

© 2008 PGP Corporation
WDEDS080918