



# PGP® Whole Disk Encryption

Vertrauliche Daten auf Festplatten und Wechseldatenträgern schützen

Teil der PGP® Encryption Plattform



## Umfassende Festplattenverschlüsselung für den Schutz aller Dateien auf Desktops, Laptops und Wechseldatenträgern

Mobile Computer steigern die Produktivität des Anwenders und werden deshalb in der Industrie immer beliebter. Mit der Mobilität verbindet sich jedoch gleichzeitig das Risiko von Verlust oder Diebstahl. Die Offenlegung sensibler Daten kann zu erheblichen finanziellen Verlusten, zu schweren rechtlichen Konsequenzen oder zur Schädigung des Unternehmensrufs führen.

PGP Whole Disk Encryption kann als Einzelplatzinstallation oder im gesamten Unternehmen eingesetzt werden. Diese Anwendung bietet umfassende, durchgängige Verschlüsselung von Festplatten und damit den schnellen, kostengünstigen Schutz von Daten auf PCs, Laptops und Wechseldatenträgern. Die verschlüsselten Daten werden ständig vor unbefugtem Zugriff geschützt. Dies bedeutet bewährte Sicherheit für geistiges Eigentum, für die Daten von Kunden und Geschäftspartnern sowie für den Ruf des Unternehmens.

### Vollständiger Laufwerksschutz

Mit PGP Whole Disk Encryption wird der gesamte Datenbestand eines Laptops, Desktops, externen Laufwerks oder USB-Flash-Laufwerks einschließlich der Boot-Sektoren sowie der System- und Auslagerungsdateien geschützt. Die Verschlüsselung ist für den Anwender transparent, Daten werden automatisch geschützt.

### PGP Encryption Plattform

Mit der PGP® Encryption Plattform verfügt ein Unternehmen über das Grundgerüst für die strategische Verschlüsselung. Das Management gemeinsam genutzter Anwenderdaten, die Richtlinienverwaltung und die Bereitstellung erfolgen dabei anwendungsübergreifend und automatisch. Die Anwendung PGP Whole Disk Encryption basiert ebenfalls auf der PGP Encryption Plattform und ermöglicht die Nutzung vorhandener Anwender, Schlüssel und Konfigurationen, womit sich die Implementierung und die Umsetzung von Richtlinien zusätzlich beschleunigt. PGP Whole Disk Encryption kann in Kombination mit anderen PGP-Verschlüsselungslösungen eingesetzt werden, um verschiedene Sicherheitsebenen abzudecken.

## Nutzen für das Unternehmen

### Schnelle Implementierung

- Die unbeaufsichtigte Installation mithilfe von standardisierten Implementierungstools minimiert den Aufwand für den Endanwender und reduziert die Häufigkeit von Helpdesk-Anfragen.
- Der Einsatz von MSI-Standard-Softwarepaketen vereinfacht die Implementierung von vorkonfigurierten Clients und verkürzt die Bereitstellungszeit der Anwendung.

### Niedrigere Betriebs- und Wartungskosten

- Die webbasierte Managementkonsole von PGP Universal™ Server bietet vereinfachte und intuitive Funktionen für die Richtlinien- und Client-Verwaltung. Die Nutzung einer einzigen Managementplattform eliminiert die Notwendigkeit zur Verwaltung und Wartung mehrerer Konsolen und Server.
- Automatische Updates werden direkt vom PGP Universal Server bezogen, so dass keine zusätzlichen Installationspakete erstellt und implementiert werden müssen.

### Zuverlässiger Zugriff auf geschützte Daten

Die von PGP Corporation patentierte Additional Decryption Key-Technologie (ADK) ermöglicht Unternehmen den Zugriff auf geschützte Daten ohne Verwendung von Master-Passwörtern oder geteilten Schlüsseln.

## Vorteile für Arbeitsgruppen

### Anmeldung mehrerer Anwender an einer Workstation

Mehrere Anwender können mit individuellen Authentifizierungsdaten auf dasselbe PGP-verschlüsselte Laufwerk zugreifen und eine Workstation ohne Risiko gemeinsam nutzen.

### Einfacher, unkomplizierter Betrieb

Mit Kontextmenüs und einer intuitiven grafischen Anwenderoberfläche lässt sich PGP Whole Disk Encryption ganz einfach bedienen.

## Merkmale und Funktionen

### Neu: Schnellerer und verbesserter Schutz

Beschleunigung der Verschlüsselungsfunktionen, eine effektivere Nutzung des Prozessors und Schutzmechanismen für Stromausfälle verbessern die Bedienbarkeit für Anwender.

### Neu: Integrierte Windows-Anmeldung

Die integrierte Anmeldung an Microsoft Windows erlaubt die Synchronisation von Passwörtern. Es ermöglicht so eine strikte Umsetzung der Richtlinien für Windows-Domain-Passwörter, ohne die Windows-Anmeldedaten zu verändern.

### Neu: Unterstützung von Mac OS X

Verschlüsselte Wechseldatenträger und sekundäre Festplatten können plattformübergreifend ausgetauscht werden.

### Neu: Verschlüsselung nach Partitionen

PGP Whole Disk Encryption verschlüsselt nach Partitionen und ist so zu Systemen mit mehreren Betriebssystemen und Wiederherstellungspartitionen kompatibel.

### Neu: Selbsterweiternde PGP Virtual Disk-Laufwerke

Selbsterweiternde PGP Virtual Disk-Laufwerke vergrößern sich automatisch, wenn der Datenbestand wächst. Damit entfällt die anfängliche Speicherplatzzuweisung.

### Zentrale Verwaltung, Installation und Richtlinien

Die automatische Bereitstellung, Anwender- und Schlüsselverwaltung sowie die Umsetzung von Richtlinien für die Verschlüsselung von E-Mails, Festplatten und Netzwerkdateien erfolgt mit der Managementkonsole von PGP Universal Server. Der rollenorientierte administrative Zugriff ermöglicht die Trennung von Verwaltungsaufgaben.

### Daten weitergeben oder gemeinsam nutzen

Mit PGP® Virtual Disk, PGP® Zip und PGP® Self-Decrypting Archive lassen sich verschlüsselte, vom Speichermedium unabhängige Datenpakete erstellen, in denen bestimmte Dateien transportiert und zur gemeinsamen Nutzung weitergegeben werden können.

### Sicheres Löschen von Dateien

PGP® Shredder und PGP® Wipe ermöglichen das sichere und endgültige Löschen aller digitalen Spuren einer Datei.

PGP und das PGP-Logo sind eingetragene Marken der PGP Corporation. Die in diesem Dokument erwähnten Produkt- und Markennamen sind Marken oder eingetragene Marken der jeweiligen Eigentümer. Alle solchen Marken oder eingetragenen Marken sind alleiniges Eigentum der jeweiligen Inhaber.

## Funktionen bei zentraler Verwaltung

### Zentral umgesetzte Sicherheitsrichtlinien

- Nutzung vorhandener LDAP- und Microsoft Active Directory-Dienste für die automatische Zuordnung von Richtlinien auf Basis von Anwendergruppenattributen.
- Policy übernimmt die Umsetzung von Richtlinien für die Laufwerksverschlüsselung und verhindert, dass Anwender Laufwerke entschlüsseln oder die Software deinstallieren.

### Ereignisprotokollierung

- Alle administrativen Vorgänge werden für Revisionen und Sicherheitsüberprüfungen protokolliert.

### Wiederherstellungspasswort

- Die automatische Generierung und zentrale Speicherung von eindeutigen, einmal verwendbaren Wiederherstellungspasswörtern ermöglichen die Remote-Unterstützung.
- Die automatische Rücksetzung des Wiederherstellungspassworts nach jeder Verwendung reduziert die administrativen Kosten.

## Technische Daten

### Unterstützte Betriebssysteme

- Windows XP SP1 oder SP2
- Windows 2000 Professional SP4
- Mac OS X 10.4 (nur für sekundäre Festplatten – Intel und PPC)

### Sprachen

- Englisch
- Deutsch
- Japanisch

### Authentifizierungsoptionen

- OpenPGP-Schlüssel (RFC 2440)
- X.509-Zertifikate

### Symmetrische Verschlüsselungsalgorithmen – PGP Whole Disk Encryption

- AES (256 bit)

### Zwei-Faktoren-Authentifizierung

Die aktuelle Liste der unterstützten Geräte zur Authentifizierung mit zwei Kriterien finden Sie unter [www.pgp.com/products/wholediskencryption/tech\\_specs.html#smartcards](http://www.pgp.com/products/wholediskencryption/tech_specs.html#smartcards)

(Aktuelle Produktspezifikationen finden Sie unter [www.pgp.com/products/wholediskencryption/tech\\_specs.html](http://www.pgp.com/products/wholediskencryption/tech_specs.html))

### Voraussetzungen für die zentrale Verwaltung

- PGP Universal Server 2.5\*

Weitere Informationen zu PGP Universal Server finden Sie unter [www.pgp.com/products/universal\\_server/tech\\_specs.html](http://www.pgp.com/products/universal_server/tech_specs.html)

