



# PGP Universal™ Server 2.5

Unternehmensweite Verschlüsselung mit einer einzigen Managementkonsole

Teil der PGP® Encryption Platform



## Mehrere PGP-Anwendungen installieren und zentral verwalten

PGP Universal Server erleichtert die Installation, verwaltet Anwender und Schlüssel automatisch, setzt Richtlinien durch und erstellt Berichte für beliebig viele Verschlüsselungsanwendungen:

- Unternehmen können mit einer einzigen Verschlüsselungsanwendung beginnen und später weitere Anwendungen einführen sowie Kunden und Geschäftspartner einbeziehen.
- Bei Bedarf kann die Lösung durch Hinzufügen von Anwendungen oder einer zentralen Verwaltung skaliert werden.
- Das Produkt integriert sich in vorhandene Infrastrukturen und unterstützt mehrere Standards.
- Unternehmen können aktuelle und zukünftige Verschlüsselungsanforderungen mit einem einzigen System verwalten.

## Umsetzen von Richtlinien in mehreren Anwendungen

Mit PGP Universal Server können Unternehmen ihre spezifischen Risiko-, Audit- und Compliance-Anforderungen effektiv erfüllen.

- Unternehmen konfigurieren Richtlinien zentral und setzen diese für mehrere Verschlüsselungsanwendungen um
- Sicherheitsbeauftragte vermeiden inkonsistente oder falsch konfigurierte Richtlinien
- Administratoren legen die Richtlinien einmal fest und konzentrieren sich dann auf andere Aufgaben

## Automatisierte Installation und einfacher Betrieb

PGP Universal Server automatisiert die Installation, Konfiguration, Schlüsselverwaltung und Richtlinienumsetzung. Administratoren verwalten die Lösung über vertraute Werkzeuge und Arbeitsschritte wie die Benutzerverwaltung oder die Konfiguration von Richtlinien und anderen Parametern.

PGP Universal Server verringert den Verwaltungsaufwand und sorgt dafür, dass Richtlinien konsequent umgesetzt werden. Darüber hinaus verwaltet der Server die Anwender, stellt Richtlinien bereit und überwacht, protokolliert und aktualisiert die Anwendungen.

## Nutzen für das Unternehmen

### Geringere Betriebskosten

Administratoren konfigurieren die Verschlüsselungsrichtlinien mit PGP Universal Server effizient über eine einzige Benutzeroberfläche, damit sie sich auf wesentliche Aufgaben konzentrieren können. Dies senkt die Betriebskosten. Die Alternative, nämlich der Einsatz mehrerer, nicht zentral verwalteter Produkte, würde den Aufwand für Schulungen, die Anzahl von Konsolen, die Konfiguration von Richtlinien, die Aktualisierung von Anwendungen vervielfachen.

### Risiken minimieren und Richtlinien vereinheitlichen

Mit der gemeinsamen und konsistenten Anwenderoberfläche von PGP Universal Server können Administratoren einen Satz von Verschlüsselungsrichtlinien für alle Anwendungen festlegen. Dieses Konzept reduziert das oft übersehene Risiko falsch oder inkonsistent definierter Richtlinien:

- Geringeres Potenzial für Fehlkonfigurationen
- Zentrale Kontrolle und Verwaltung
- Konsistente Definition und Umsetzung von Richtlinien

### Aktualisierte Revisionsanforderungen erfüllen

Wenn sich die Revisionsanforderungen verändern, können Administratoren mit PGP Universal Server schnell die benötigten Konfigurationen bereitstellen und sich dann wieder auf ihre Hauptprojekte konzentrieren. Administratoren sparen die Zeit, die andererseits für die Überprüfung mehrerer Verschlüsselungsanwendungen notwendig wäre, weil sie mit PGP Universal Server die Richtlinien, Protokolle und Berichte für mehrere Applikationen zentral definieren können.

### Auf die Erwartungen von morgen vorbereitet

PGP Universal Server ist die Basis der PGP Encryption Platform, einem Grundgerüst, das folgende Möglichkeiten bietet:

- Modulare Erweiterung und Anpassung der benötigten Sicherheitsanwendungen
- Verwendung integrierter Anwendungen von Drittherstellern, z. B. von Research In Motion® (RIM®)

## Merkmale und Funktionen

### Neu: Erweiterte Verschlüsselungsrichtlinien

Mit PGP Universal Server definieren Administratoren Richtlinien für mehrere Verschlüsselungsanwendungen.

- Die Richtlinien können die Verschlüsselung von E-Mails anhand von Inhalt, Übertragungsmethode, Sender, Empfänger und anderen Kriterien initiieren.
- Die erweiterte Mail Policy-Engine gibt Administratoren eine differenzierte Kontrolle des E-Mail-Verkehrs und der Verschlüsselung.
- Verschiedenen Gruppen können verschiedene Richtlinien zugeordnet werden. Unternehmen können so die Anforderungen zu den Themen Revision, Informationssicherheit und Organisationsstruktur leichter abbilden.

### Einheitliche, webbasierte Verwaltungskonsole

Die einheitliche, webbasierte Verwaltungsoberfläche von PGP Universal bietet die folgenden Möglichkeiten:

- Verwaltung von Anwendern, Schlüsseln und Richtlinien sowie Systemüberwachung und Berichterstellung
- Rollenbasierte Administration zur Zuweisung von Verwaltungsaufgaben

### Integration in bestehende Systeme

PGP Universal Server nutzt bestehende Investitionen, indem es sich in bestehende PKIs, Systemverwaltungen, Spam- und Content-Filter optimal integriert.

### Protokollierung, Überwachung und Berichterstellung

PGP Universal Server listet alle Verschlüsselungsvorgänge in einem Ereignisprotokoll auf. Administratoren können diese Informationen über die webbasierte Konsole oder per SNMP abrufen.

### Installation von zentral verwalteten Anwendungen

PGP Universal Server die Erstellung von Client-Installationsroutinen für PGP-Anwendungen direkt über eine webbasierte Konsole:

- Setups für Microsoft Windows und Apple Mac OS X
- Die MSI-Pakete sind mit üblichen Mechanismen der Softwareverteilung kompatibel, z.B. Microsoft SMS

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.

## Gesicherter Langzeitzugriff auf Daten

PGP Universal Server sichert den Langzeitzugriff auf verschlüsselte Daten.

- Die von PGP Corporation patentierte Additional Decryption Key-Technologie (ADK) gewährleistet im Unternehmen den Zugriff auf verschlüsselte Daten, E-Mails und Dateiserver.
- Anwender können mithilfe eines einmal verwendbaren Wiederherstellungspassworts Zugriff auf ihren mit PGP Whole Disk Encryption geschützte Computer zurückerhalten.

## Technische Daten

### Systemvoraussetzungen

- Hardware: Aktuelle Informationen zu unterstützten Hardwarekonfigurationen finden Sie unter [www.pgp.com/products/universal\\_server/tech\\_specs.html](http://www.pgp.com/products/universal_server/tech_specs.html)
- Virtualisierung: VMware ESX Server

### Unterstützte Webbrowser für die Administration

- Apple Safari
- Microsoft Internet Explorer
- Mozilla Firefox

### Standardisierte Schnittstellen

- HTTPS
- LDAP/S
- SOAPS

### Verzeichnisintegration

- Microsoft Active Directory
- Novell eDirectory
- PGP® Global Directory

### Schlüssel- und Zertifikatsverwaltung

- OpenPGP
- X.509 v3

### Verwaltbare Verschlüsselungsanwendungen

- PGP Universal™ Gateway Email
- PGP® Desktop Email
- PGP® Desktop Professional
- PGP® Desktop Storage
- PGP® Desktop Enterprise
- PGP® NetShare
- PGP® Whole Disk Encryption
- PGP® Support Package für BlackBerry®

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

