PGP® Reviewer's Guide

April 2007

PGP® Whole Disk Encryption

Version 1.0

Table of Contents

Overview

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

For use by individual professionals or within the enterprise environment, PGP Whole Disk Encryption provides comprehensive, non-stop disk encryption, enabling quick, cost-effective protection for data on PCs, 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.

This Reviewer's Guide will introduce you to the PGP Whole Disk Encryption product, highlight its features, and walk you through its installation and use. In addition, this guide will also cover how PGP Whole Disk Encryption integrates with PGP Universal™ Server, the management console for the PGP® Encryption Platform, an enterprise encryption framework for shared user management, policy, and provisioning automated across multiple, integrated encryption applications.

For Reviewers

This guide is designed to assist professional journalists reviewing the PGP Whole Disk Encryption product as part of writing an article for a computing or information security publication. The guide assumes the reader has general computer knowledge as well as experience installing and configuring Windows software.

Additional detailed information on PGP Whole Disk Encryption is available in the *PGP Desktop for Windows User's Guide* and the *PGP Whole Disk Encryption Quick Start Guide* included with the product.

Goals

By reading this document, the reader will:

- Evaluate the selection criteria enterprises consider when evaluating full disk encryption to protect sensitive data on laptops and removable media
- Learn how PGP Whole Disk Encryption transparently and automatically provides comprehensive data protection without impacting end-user productivity
- Understand the advantage of managing PGP Whole Disk Encryption installations with PGP Universal Server to enforce encryption policies and maintain corporate access to encrypted data, without impacting IT administration

Required Equipment

Installing and testing PGP Whole Disk Encryption requires a laptop or desktop machine meeting the following minimum system requirements:

- **Operating system** – Windows 2000 (SP4), Windows XP (SP1 or SP2), Microsoft Windows XP Tablet PC Edition 2005 (requires attached keyboard), or Windows Vista (all 32-bit editions)
- **Memory** – 128MB RAM (256MB recommended)
- **Free disk space** – 64MB free disk space

Introduction

As today's mobile computing and distributed remote office trends boost productivity, they may represent a significant risk for enterprises. Increased convenience and portability also may increase the potential for a system to be lost, stolen, or misused without the owner's knowledge. Resulting breaches of customer data, personnel records, or patient information not only compromise individual privacy and business confidentiality, but may result in significant financial repercussions.

Organizations faced with a breach may be compelled by law to notify customers or take other actions that result in lost business, increased call center activity, additional no-cost services, and legal defense expenses that can easily amount to millions of dollars. Third-party research has shown that even a small breach of 2,500 records can result in $1 million of immediate direct costs for the affected organization, and a significant breach compromising 150,000 customer records can result in more than $10 million in immediate direct costs. However, the long-term effects of lost business, a tarnished reputation, brand equity damage, and resulting legal expenses dwarf the immediate costs resulting from a breach.[1]

Protecting all data stored on laptops and desktop computers using full disk encryption, thereby encrypting all files stored on a disk, allows organizations to address the potential consequences resulting from a breach. Even in the event of a system loss or theft, data stored on a system secured with full disk encryption is inaccessible without valid authentication credentials. And because all data encryption occurs in the background, full disk encryption does not affect end-user productivity.

Organizations considering full disk encryption commonly evaluate solutions based on similar enterprise requirements:

1. **End-user productivity** – The solution should remain transparent at all times and not interfere with end-user productivity.
2. **Enhanced data security** – Beyond full disk encryption, the solution should provide options for protecting and controlling USB flash drives as well as files stored on shared systems and files and directory archives shared with others by policy.
3. **Centralized management** – The solution should allow for central management that enables administrators and help desk staff to easily support remote users.
4. **Business continuity** – Encrypted data needs be accessible (according to policy) not only today, but for years to come.
5. **Enterprise systems integration** – The solution should leverage the organization's existing infrastructure (such as directories and systems management tools) to expedite deployment and automate management and should also deploy as a single system that can be expanded later to multi-application encryption.

PGP Corporation's full disk encryption solution, PGP Whole Disk Encryption, allows organizations to immediately begin addressing business risks along with adherence to external regulations and internal audit requirements. In addition to protecting all files stored on a system, PGP Whole Disk Encryption protects data stored on USB flash drives. When deployed with and managed by PGP Universal Server's central management console, organizations can also centrally define and enforce encryption policies while ensuring corporate access to encrypted data, when needed.

[1] The Ponemon Institute, "2006 Annual Study: Cost of a Data Breach", November 2006

By deploying PGP Whole Disk Encryption with PGP Universal Server, organizations also gain access to the PGP Encryption Platform architecture, allowing them to continue addressing threats and risk mitigation. The PGP Encryption Platform architecture enables multiple applications to share policy, provisioning, user management, and directory services integration. This approach allows customers to add multi-application encryption, including email, network file, and instant messaging (IM) encryption, to their PGP Whole Disk Encryption deployment. By addressing one set of risks today with PGP Whole Disk Encryption and PGP Universal Server, organizations will be well-prepared to address emerging information privacy and protection requirements in the future.

PGP Whole Disk Encryption

PGP Whole Disk Encryption is a member of the PGP Desktop family of applications. You can use PGP Whole Disk Encryption to lock down the entire contents of your system or an external or USB flash drive you specify. Using full disk encryption to protect your boot drive means you do not have to worry if your computer is lost or stolen because boot sectors, system files, and swap files are all encrypted.

In addition to providing full disk encryption, PGP Whole Disk Encryption also provides:

- **PGP® Virtual Disk** – Uses part of your hard drive space as an encrypted virtual disk volume with its own drive letter. You can create additional users for a volume, allowing people you authorize to access it. A PGP Virtual Disk is like a safe: the perfect place to store sensitive files. When the door of the safe is open (when the volume is mounted), you can change files stored in it, take files out, and move files in. Otherwise (when the volume is unmounted), all the data on the volume is protected.
- **PGP® Zip** – Adds any combination of files and folders to an encrypted, compressed, portable archive. PGP Whole Disk Encryption or PGP Desktop Email must be installed on a system to create or open a PGP Zip archive. PGP Zip is a tool for securely archiving your sensitive data, whether you want to distribute it to others or back it up.
- **PGP® Self-Decrypting Archive (SDA)** – Puts files and folders into an encrypted, compressed package that can be opened on a Windows system that does not have PGP Whole Disk Encryption or another client from the PGP Desktop family installed. SDAs are the perfect solution for securely exchanging files with someone who does not have PGP software installed.
- **PGP® Shredder** – Completely destroys files and folders so that even file recovery software cannot recover them. Deleting a file using the Windows Recycle Bin does not actually delete it; it sits on your drive and eventually gets overwritten. Until then, it is easy for an attacker to recover that file. In comparison, PGP Shredder immediately overwrites files multiple times. This process is so effective that even sophisticated disk recovery software cannot recover these files. The PGP Shredder feature also completely wipes free space on your drives so deleted data is truly unrecoverable.

This section will focus on providing a step-by-step guide to installing and using PGP Whole Disk Encryption to protect a laptop or desktop machine's boot drive and data stored on a removable USB drive. In addition, it will show how PGP Whole Disk Encryption can be used in conjunction with PGP Virtual Disk to further compartmentalize and protect sensitive data.

Installation Process

Before You Install

Before you begin the installation, verify that your system meets these minimum requirements:

- **Operating system** – Windows 2000 (SP4), Windows XP (SP1 or SP2), Microsoft Windows XP Tablet PC Edition 2005 (requires attached keyboard), or Windows Vista (any 32-bit edition)
- **Memory** – 128MB RAM (256MB recommended)
- **Free disk space** – 64MB free disk space

Installing PGP Whole Disk Encryption

PGP Corporation delivers software via an electronic download accessed from a link provided to the customer by email on completion of the order process. You will need to follow the link in the email to download the software in preparation for installation. In addition, you will need to note the license key provided in the same email message to successfully license the product during the installation process.

To install PGP Whole Disk Encryption:

1. Locate the PGP Whole Disk Encryption installer program. The installer program is an .MSI file, which you can retrieve from PGP Corporation via the link in the email you received as part of the fulfillment of your order.
2. Double-click the PGP Whole Disk Encryption installer.
3. Accept the license agreement and review the release notes before proceeding with install.

When the installation of PGP Whole Disk Encryption is complete, you are prompted to restart your computer. Once the computer restarts, as soon as you see the Windows Desktop, the PGP Setup Assistant starts automatically. The PGP Setup Assistant displays a series of screens that ask you questions and uses your answers to configure PGP Whole Disk Encryption appropriately:

1. Click "Yes" to enable PGP Whole Disk Encryption for your account and click **Next**.
2. Enter the Name and Organization as it appears on the license you received via email and click **Next**.
3. Enter the license number from license you received via email and click **Next**. The PGP Whole Disk Encryption client will contact the PGP licensing server via the network to authorize your license and then display a summary of the features enabled by your license. License authorization requires your machine to be on the network. In the event that you are not able to authorize your license, you may contact PGP Corporation to receive a manual license authorization.
4. Select "I am a new user" and click **Next** to create a new PGP key. Although PGP keys are not required for full disk encryption functionality, they can be used to protect PGP Virtual Disks or digitally sign PGP Zip files.
5. Enter your email address and click **Next**.

6. Enter a passphrase and click **Next**. This passphrase will be used to protect your PGP private key, which is used to decrypt and digitally sign data.
7. Your PGP key is generated and the PGP Setup Assistant is complete. Click **Finish** to dismiss the congratulations dialog.

The PGP Setup Assistant does not configure all PGP Whole Disk Encryption settings. When you finish going through the PGP Setup Assistant screens, you can then configure those settings not covered in the PGP Setup Assistant.

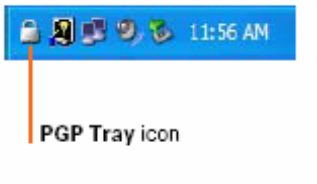
Managing PGP Whole Disk Encryption with PGP Universal Server

PGP Universal Server offers the ability to manage installations of PGP Whole Disk Encryption. Managing an installation of PGP Whole Disk Encryption clients with PGP Universal Server has the advantage that the administrator can centrally define policy to force encryption of boot drives and removable media. Central management of policy eliminates the need for the user to take specific action to protect sensitive data and ensures compliance with corporate security policy.

The Main Screen

Once installation is complete, you can start PGP Whole Disk Encryption using any of the following methods:

- Double-click the **PGP Tray** icon.
- Right-click the **PGP Tray** icon and then select **Open PGP Desktop**.
- From the **Start** menu, select **Programs > PGP > PGP Desktop**.



Once opened, the PGP Whole Disk Encryption main screen gives you easy access to its features. The remainder of this section will focus on using the functionality in the PGP Disk section (shown in Figure 1 on page 8) to exercise full disk encryption–related functionality.

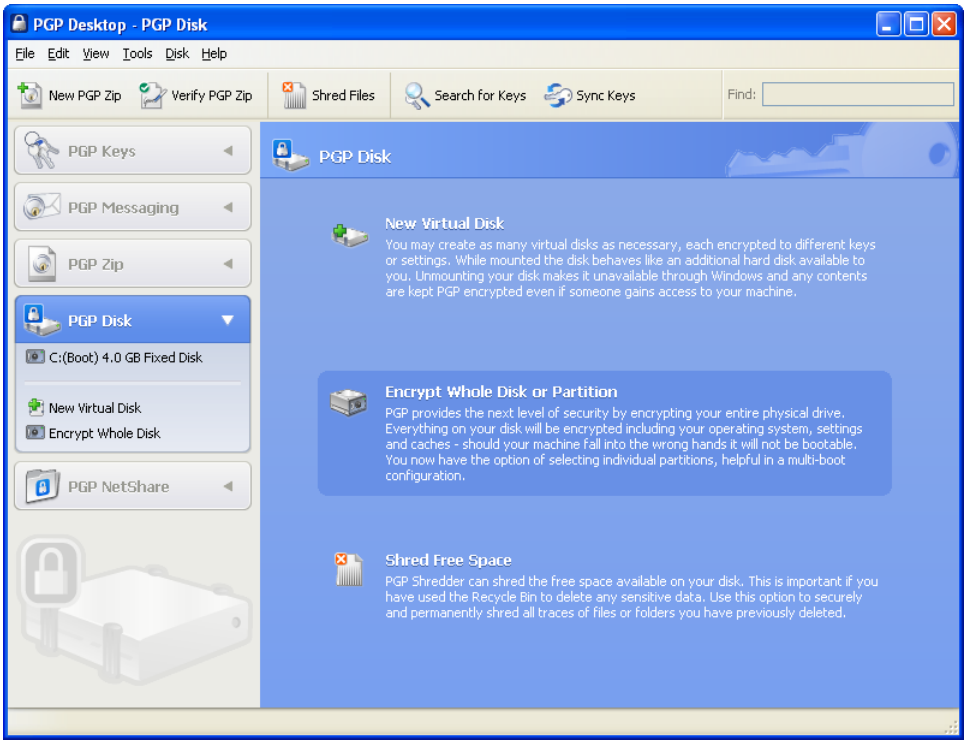


Figure 1: The main PGP Whole Disk Encryption user interface

Encrypting a Drive

In this section, you will encrypt a drive using PGP Whole Disk Encryption's Single Sign-On feature. The Single Sign-On feature synchronizes the PGP Whole Disk Encryption authentication process with the one used by Microsoft Windows, simplifying the authentication process. Using Single Sign-On, the user authenticates to both PGP Whole Disk Encryption and Windows by entering only one set of credentials when starting the machine.

Before You Encrypt a Drive

To ensure success in protecting a drive, it's important to consider the following best practices prior to beginning encryption:

- **Determine whether your target disk is supported.** PGP Whole Disk Encryption protects desktop or laptop disks (either partitions or the entire disk), external disks, and USB flash disks. It does **not** support CD-RW/DVD-RWs and servers.
- **Back up the disk before you encrypt it.** Before you encrypt your disk, be sure to back it up so that you will not lose any data if your laptop or computer is lost or stolen
- **Ensure the health of the disk before you encrypt it.** If PGP Whole Disk Encryption encounters disk errors during encryption, it will pause encryption so you can repair the disk errors. However, it is more efficient to repair errors before you initiate encryption. Use a third-party scan disk utility that has the ability to perform a low-level integrity check and repair any inconsistencies with the drive that could lead to errors. The Microsoft Windows's check disk (chkdsk.exe) utility is not sufficient for detecting these issues on the target hard drive. Instead, PGP Corporation recommends you use software applications such as

SpinRite or Norton Disk Doctor™ that can correct errors that would otherwise disrupt encryption.

- **Be certain that you will have AC power** for the duration of the encryption process. Because encryption is a CPU-intensive process, encryption cannot begin on a laptop computer that is running on battery power. The computer **must** be on AC power. If a laptop computer goes on battery power during the initial encryption process (or a later decryption or re-encryption process) PGP Whole Disk Encryption pauses its activity. When you restore AC power, the encryption, decryption, or re-encryption process resumes automatically.

Encrypting the Drive

To encrypt your main boot drive using full disk encryption (see Figure 2 below):

1. Click **Encrypt Whole Disk** in the **PGP Disk Control box**.
2. Select the drive or partition to be encrypted.
3. Click **New Passphrase User** to add users who authenticate using a passphrase.
    a. Choose **Use Windows Password** to use your Windows credentials for authentication.
    b. Enter your Windows login password when prompted, and then click **Finish**.
4. Click **Encrypt**.

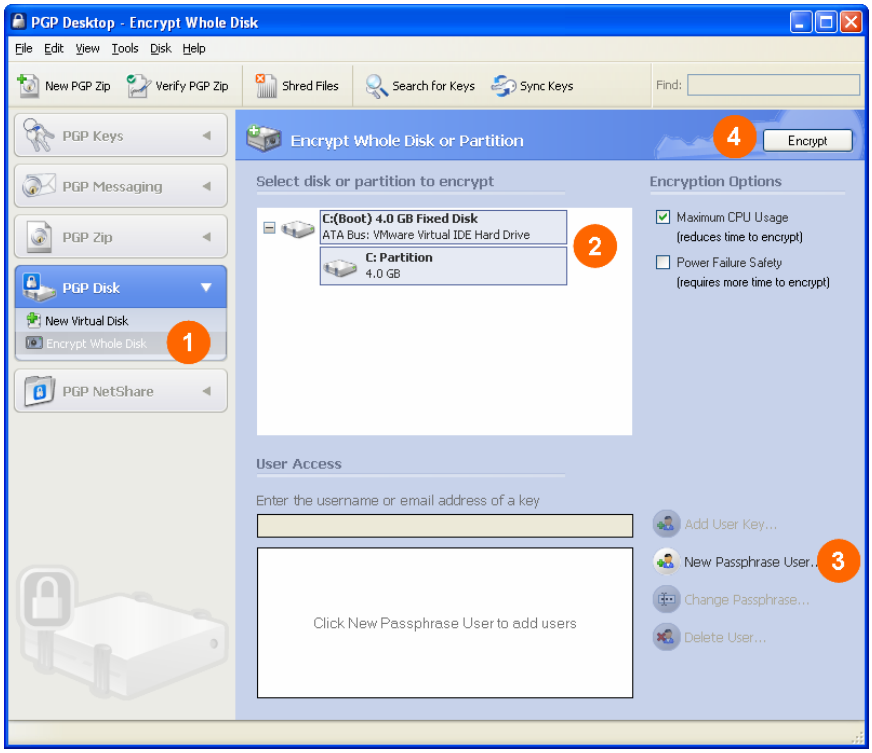


Figure 2: Encrypting a drive with PGP Whole Disk Encryption

Once encryption starts, you can continue to use your system as normal. PGP Whole Disk Encryption automatically slows the encryption process if you are using the system. The system returns to normal operation when the encryption process is complete.

During encryption, you can stop the encryption process temporarily by clicking **Stop**, then clicking **Pause** in the dialog box that appears. To resume, click **Resume**. You may be prompted for the appropriate authentication credentials. You can also choose to shutdown or send a machine into hibernation while this initial encryption process is underway. The encryption process will continue when you restart the machine.

Using an Encrypted Drive

Once a boot or secondary disk is protected with PGP Whole Disk Encryption, your computer will boot up in a different way to protect the boot disk—or a secondary fixed disk—on your system. To experience the authentication process once a disk is protected:

1. Start or restart the system that has a disk or partition protected by PGP Whole Disk Encryption.
2. On startup, the PGP Bootguard log-in screen appears (see Figure 3).
3. Type a valid passphrase and press **Enter**. If you make a typing error, or think you might have made a typing error, press **Esc** to clear all characters and start again.
4. If you entered a valid passphrase, the PGP Bootguard log-in screen disappears and the system boots normally. If you entered an invalid passphrase, an error message appears. Try typing the passphrase again.

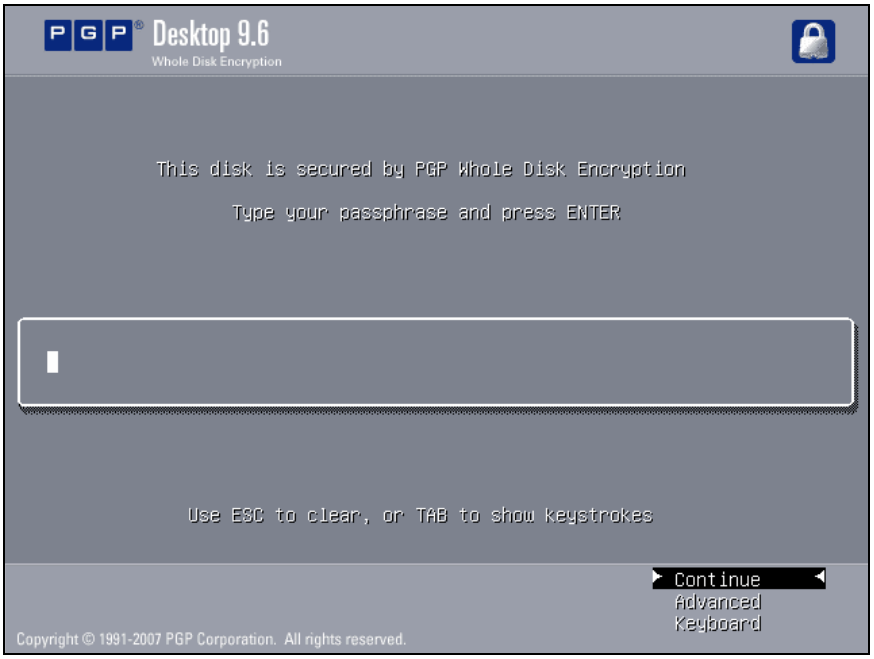


Figure 3: The PGP Bootguard log-in screen

After you have authenticated to PGP Bootguard, your operating system will boot as normal. If you enabled Single Sign-On, PGP Whole Disk Encryption will also authenticate you to Windows, eliminating the need to authenticate a second time. Once your operating system begins booting, all of your data is encrypted and decrypted automatically, as needed. With most computers, after the disk is completely encrypted, there is no noticeable slowdown of your activities.

Once a disk is encrypted, PGP Whole Disk Encryption provides:

- **Comprehensive protection** – PGP Whole Disk Encryption locks down the entire contents of a laptop or desktop, including boot sectors, system, and swap files. Encryption protects the contents from being read in the event the system is stolen or lost.
- **Transparent, automatic security** – Once a user is authenticated, all the user's files are available as normal. Files are encrypted and decrypted transparently without requiring any change to applications or the way the user works with files.
- **Painless initial encryption process** – End users remain productive during the installation process because initial encryption occurs silently in the background.
- **Simplified authentication** – When a user's authentication passphrase is synchronized to his/her Windows login credentials, PGP Whole Disk Encryption provides Single Sign-on capabilities that require the user to enter only one passphrase to authenticate all the way through to Windows. Unlike other approaches to Single Sign-on, PGP Whole Disk Encryption does not modify or replace the Windows authentication system (Windows GINA), eliminating the risk of system conflicts and incompatibilities with existing software.

Protecting Removable Media

PGP Whole Disk Encryption can also protect removable media and extend protection to data carried around on easily lost devices, such as USB drives. To encrypt a removable USB drive, insert the drive and follow the same directions as in the "Encrypting the Drive" section (beginning on page 9), selecting the USB drive instead of the boot drive for encryption.

Because removable drives can be inserted and removed at any time, authentication for PGP Whole Disk Encryption–protected removable media is performed when the removable drive is inserted. To access a PGP Whole Disk Encryption–protected removable drive:

1. Insert a PGP Whole Disk Encryption–protected USB drive into a machine running PGP Whole Disk Encryption.
2. On insertion, the authentication screen appears (see Figure 4 on page 12).
3. Type in a valid passphrase and press **Enter**. If you make a typing error, or think you might have made a typing error, press **Esc** to clear all characters and start again.
4. Click **OK**.

Figure 4: Authenticating to a PGP Whole Disk Encryption–protected USB drive

After you have authenticated, all your data on the removable drive is encrypted and decrypted automatically, as needed. An encrypted USB drive can be read on any machine equipped with PGP Whole Disk Encryption, provided the correct authentication credentials are entered.

Encrypting a removable drive with PGP Whole Disk Encryption provides these benefits:

- **Transparent data protection for removable drives** – Encrypting a removable drive extends full disk encryption protection to removable media, eliminating the risk of a data breach arising from a lost or stolen USB drive. Data copied to the drive is automatically encrypted and decrypted on-the-fly without changing the user's normal behavior.
- **Painless initial encryption process** – End users remain productive during the initial encryption process because it occurs in the background.

Compartmentalized File Protection using PGP Virtual Disk

The PGP Virtual Disk feature differs from PGP Whole Disk Encryption in that PGP Virtual Disks perform like additional volumes on your system that can be locked, even while you are using your computer. These volumes are like a vault where you can store files needing protection. There is no actual physical disk—only the virtual one the PGP Virtual Disk feature creates and manages.

PGP Whole Disk Encryption and the PGP Virtual Disk feature work independently, so you can use them at the same time. This option is especially useful to provide an additional level of protection on systems that may be shared between several users. Using PGP Virtual Disk on a shared machine allows each user to protect his/her files from other users of the same machine.

To create a new PGP Virtual Disk (see Figure 5 on page 13):

1. Click **New Virtual Disk** in the PGP Disk Control box.
2. Type a **Name** for the volume.
3. Specify a **Disk File Location** for the volume.
4. Select your mount preferences:
    a. Select a drive letter for the volume to **Mount as**.

b. Select **Mount at Startup** to have your new volume mount automatically at startup.

5. Click **Create** and enter the passphrase for your PGP key.

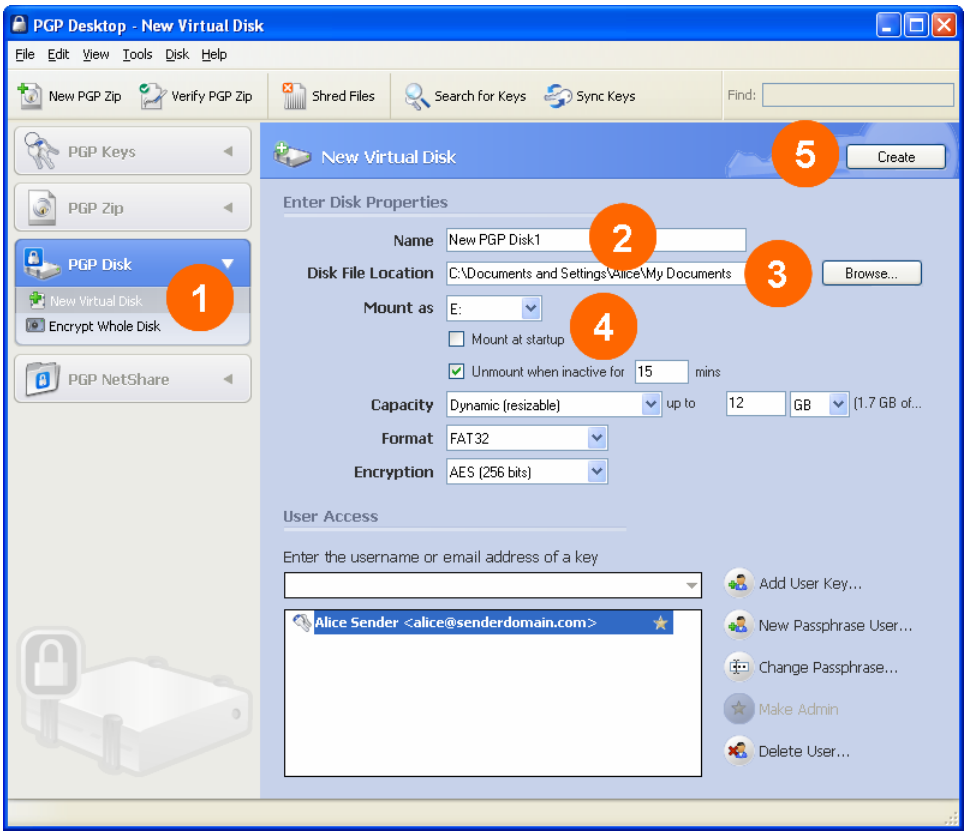


Figure 5: Creating a PGP Virtual Disk

A progress bar indicates how much of the PGP Virtual Disk has been initialized and formatted. When complete, your new PGP Virtual Disk appears in the PGP Disk control area and is available under the drive letter configured in Step 4.a. By default, the PGP Virtual Disk will be protected by the PGP key you created using the PGP Setup Assistant.

The next time you mount the PGP Virtual Disk, you will be prompted to enter your passphrase to authenticate to the drive. Once the drive is mounted, any files copied to the PGP Virtual Disk will be automatically encrypted. You can create, copy, move, and delete files and folders on a PGP Virtual Disk just as you normally do with any other disk on your system.

Anyone else who has access to the volume (either on the same computer or over the network) can also access the data stored there. The data is not protected until you unmount the volume. To unmount a PGP Virtual Disk from Windows Explorer, right-click on the PGP Virtual Disk file, then select **PGP** > **Unmount PGP Virtual Disk** from the shortcut menu.

Protecting files with PGP Virtual Disk provides these benefits:

- **Compartmentalized file protection** – PGP Virtual Disks can be used to augment PGP Whole Disk Encryption on machines shared by multiple users. PGP Virtual Disk allows users to protect their personal files from unauthorized access by other authorized users on the same system.
- **Simplified file transportation** – PGP Virtual Disks are self-contained encrypted files that can be burned to CD to securely archive data or copied to removable media to simplify transporting large numbers of sensitive files.

Enterprise Management Option: PGP Universal Server

PGP Universal Server enables organizations to control deployment, automate user and key management, enforce policy, and centralize reporting for one or more PGP Encryption Platform–enabled encryption applications.

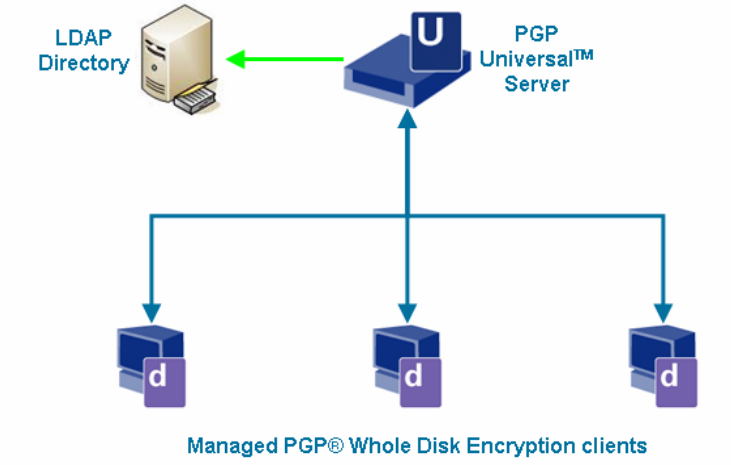


Figure 6: Overview of a PGP Universal Server–managed installation

In a PGP Universal Server–managed PGP Whole Disk Encryption deployment, such as that shown in see Figure 6, PGP Universal Server provides these benefits:

- **Centralized policy configuration and enforcement** – Using PGP Universal Server's unified Web-based administrative interface, an administrator can force installations of PGP Whole Disk Encryption to automatically encrypt the boot drive and encrypt removable media inserted into a user's machine. An administrator may assign different policies to different groups, allowing organizations to tailor encryption policies to meet their audit, data security, and organizational requirements.
- **Enterprise integration** – PGP Universal Server can optionally leverage investments in enterprise directories to automatically apply policy based on existing user group definitions in LDAP directories. This integration allows administrators to focus on familiar tasks,

including establishing groups in the corporate directory, to quickly assign policy and configuration through PGP Universal Server.

- **Assured access to secured data** – Managed PGP Whole Disk Encryption deployments automatically generate and storage a unique one-time-use recovery passphrase in PGP Universal Server. This recovery passphrase enables remote assistance and recovery of encrypted data in the event a user forgets the passphrase or when the organization requires access to the data, according to policy and regulatory requirements.

PGP Universal Server is deployed as a dedicated software appliance on standard x86 hardware. PGP Universal Server installs its own dedicated, security-hardened operating system to provide all the components required to manage installations of PGP Whole Disk Encryption as well as PGP® NetShare, PGP Desktop Email, PGP® Desktop Enterprise, and PGP® Desktop Storage clients. Once PGP Universal Server is installed, an administrator uses it to generate an MSI installer for PGP Whole Disk Encryption, which can then be deployed using standard software distribution systems such as Microsoft Systems Management Server (SMS).

This guide focuses on providing an overview of management of a PGP Whole Disk Encryption deployment by PGP Universal Server. This overview illustrates the administrator and end-user experience when PGP Universal Server is used to force boot drive encryption on installation, force encryption of removable media, and gain access to a protected system when the end user forgets his/her passphrase. For more information on PGP Universal Server, please contact your PGP representative.

Forcing Boot Drive Encryption

PGP Universal Server allows an administrator to define full disk encryption policies for groups of users, forcing a user's boot drive to be encrypted once the PGP Whole Disk Encryption client is installed.

Driving Encryption Policy Using LDAP

An administrator can drive define and enforce policy for PGP Whole Disk Encryption users based on existing information in an LDAP directory. This option allows the organization to define different policies for different organizational groups without requiring the administrator to duplicate group definitions that already exist in the corporate directory. Figure 7 on page 16 shows the main administration screen that lists the policy groups defined by the administrator.

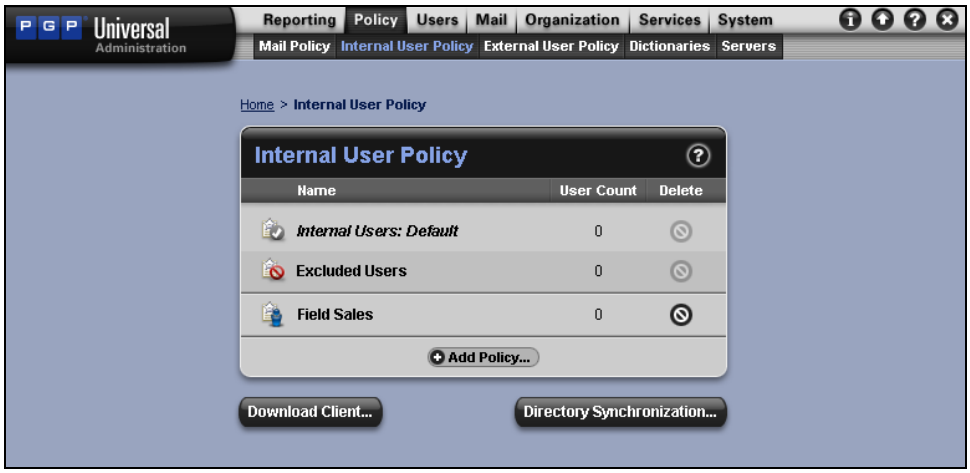


Figure 7: The PGP Universal Server list of internal policy groups

In Figure 7, the administrator has established a group called "Field Sales" to be used to define the policy for users who need to have their boot drives protected with PGP Whole Disk Encryption. To establish which users will belong to this policy group, the administrator points PGP Universal Server to the existing LDAP directory using the "Directory Synchronization" button and configuring the LDAP connection settings as shown in Figure 8 (below).

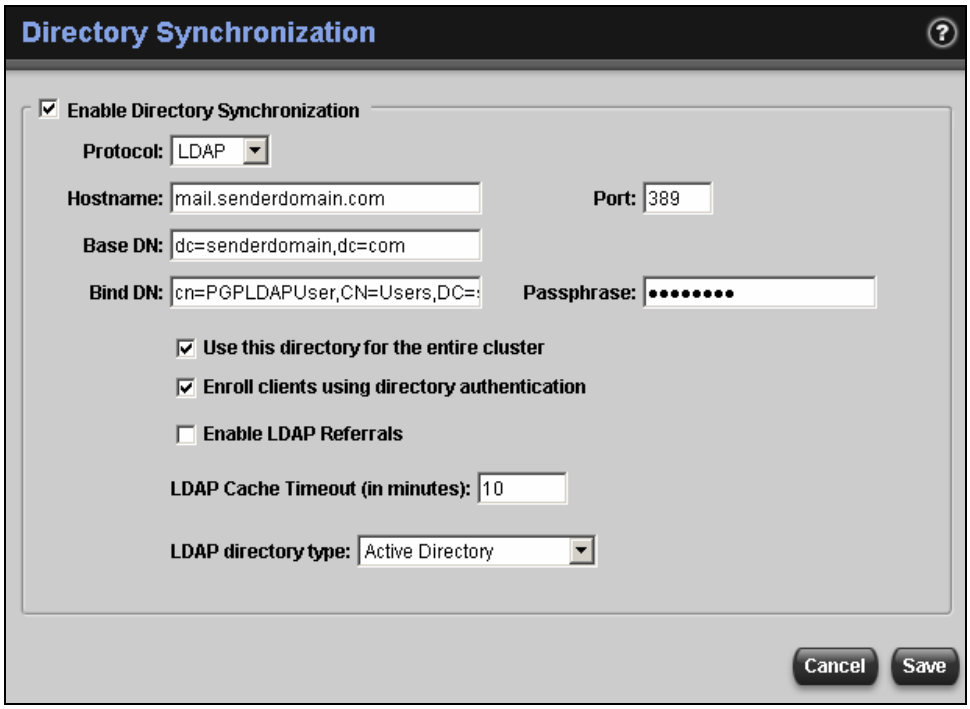


Figure 8: Integrating PGP Universal Server with an existing LDAP Directory

Within the "Field Sales" policy, the administrator configures the LDAP attributes that will be used to determine if the "Field Sales" policy applies to a given user (see Figure 9).

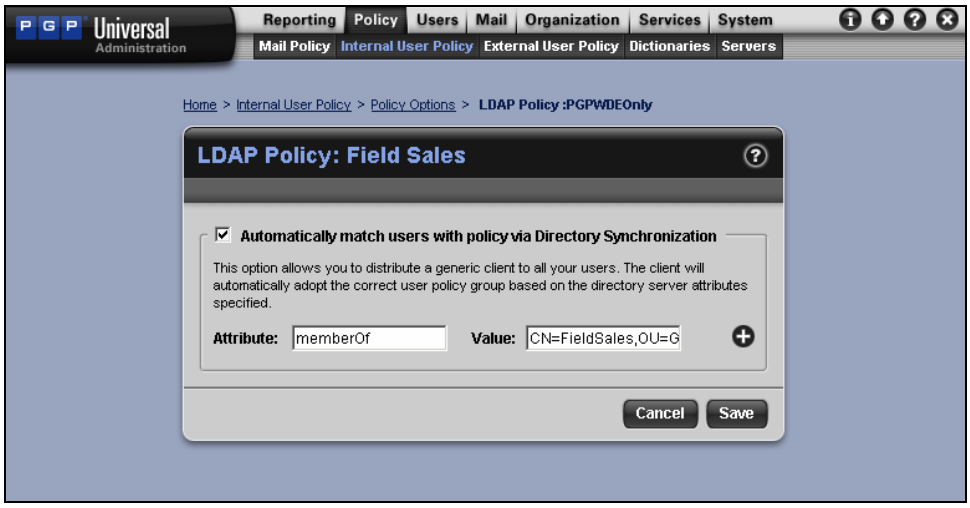


Figure 9: Configuring the LDAP attributes for the "Field Sales" policy

With the "Field Sales" policy configured as shown in Figure 9, the PGP Whole Disk Encryption software will automatically apply the settings in the "Field Sales" policy to any users that belong to the Field Sales group in the LDAP directory.

By leveraging existing information in an LDAP directory, PGP Universal Server provides these benefits:

- **Automated application of policy** – Using LDAP synchronization, PGP Universal Server and PGP Whole Disk Encryption automatically determine which policy setting to apply without requiring the administrator to assign policies on a user-by-user basis. Policies are driven by preexisting definitions of organization groups defined in the corporate directory.
- **Dynamic policy updates** – Changes to PGP Universal Server's policy settings or the LDAP directory settings automatically update the policy enforced by the PGP Whole Disk Encryption client. For example, if a user changes departments within the company, the changes made to the user's LDAP directory attributes will be detected by PGP Universal Server, resulting in an automatic update to the policy applied by the user's copy of PGP Whole Disk Encryption. No additional administrative intervention is required to ensure the user is transferred to a different policy group.

Defining Whole Disk Encryption Policy

The administrator can use a policy group to determine which features and functionality will be enforced by the PGP Whole Disk Encryption client for a set of users. Figure 10 shows the PGP Whole Disk Encryption options for the "Field Sales" policy group shown in the previous section.

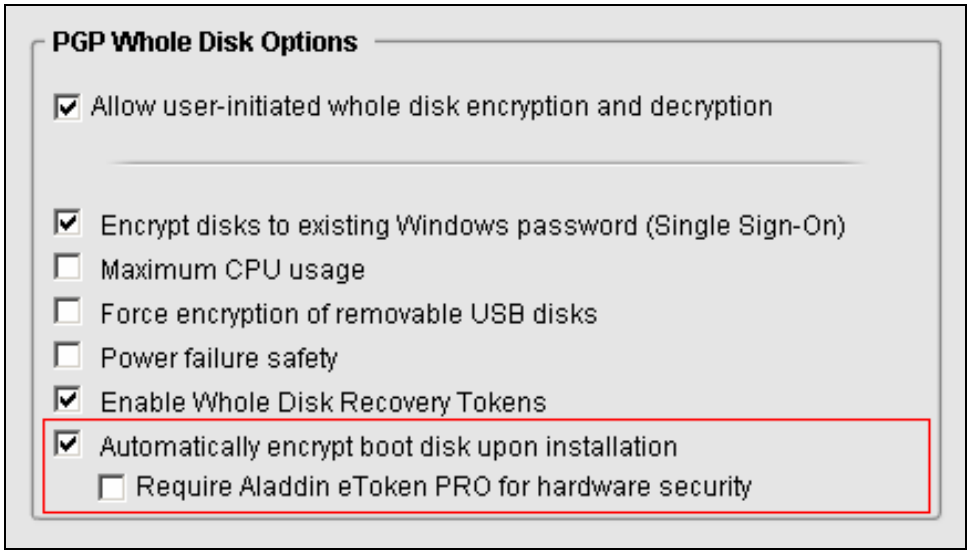


Figure 10: The PGP Whole Disk Encryption options for a policy group

PGP Universal Server's policy group feature provides these benefits:

- **Enforced protection of corporate data** – By checking the "Automatically encrypt boot disk upon installation" option, an administrator forces the PGP Whole Disk Encryption installer to encrypt the boot drive, ensuring protection of data without requiring user action. No administrator action is required to encrypt the drive.
- **Enforced authentication mechanism** – An administrator can choose the "Encrypt disks to existing Windows password" option to allow users to use their existing Windows login to authenticate to PGP Whole Disk Encryption, simplifying the authentication process. Alternatively, the administrator can choose "Require Aladdin eToken PRO for hardware security" to enforce use of two-factor authentication, thereby increasing the protection provided to data encrypted by PGP Whole Disk Encryption.

Monitoring PGP Whole Disk Encryption Installations

When deploying a full disk encryption solution, it is important for an organization to be able to monitor the status of protection within the company. This capability is important for system monitoring and auditing, especially to confirm encryption usage in the event a system is lost or stolen. Managed PGP Whole Disk Encryption clients report the status of encryption to the PGP Universal Server system log, shown in Figure 11 on page 19.

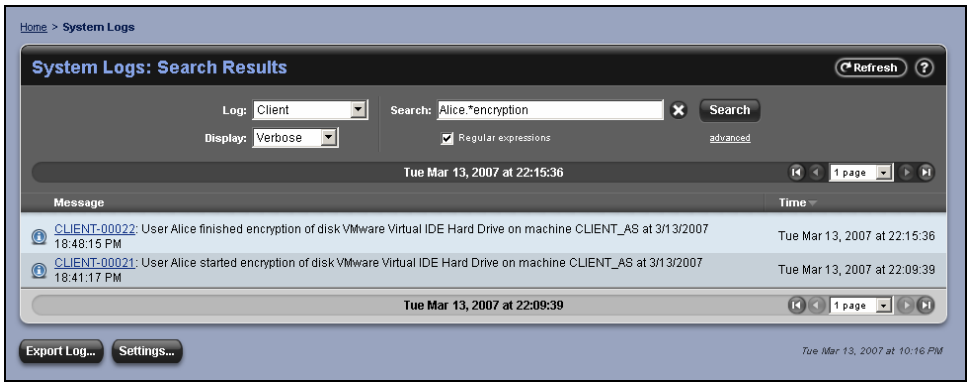


Figure 11: The PGP Universal Server system log

The PGP Universal Server system log provides the following:

- **Event logging for managed PGP Whole Disk Encryption installations –** Using the PGP Universal Server system log, an administrator can monitor the state of full disk protection within the organization as well as determine which systems have been protected with PGP Whole Disk Encryption. Event logging simplifies the process of proving protection in the event a laptop is lost or stolen.

Forcing Removable Media Encryption

PGP Universal Server policy can not only force users to encrypt their boot drive, but also can force users to protect removable USB media inserted into their computer. Forced encryption of removable USB media is enabled using a single checkbox in the policy configuration, as shown in Figure 12.

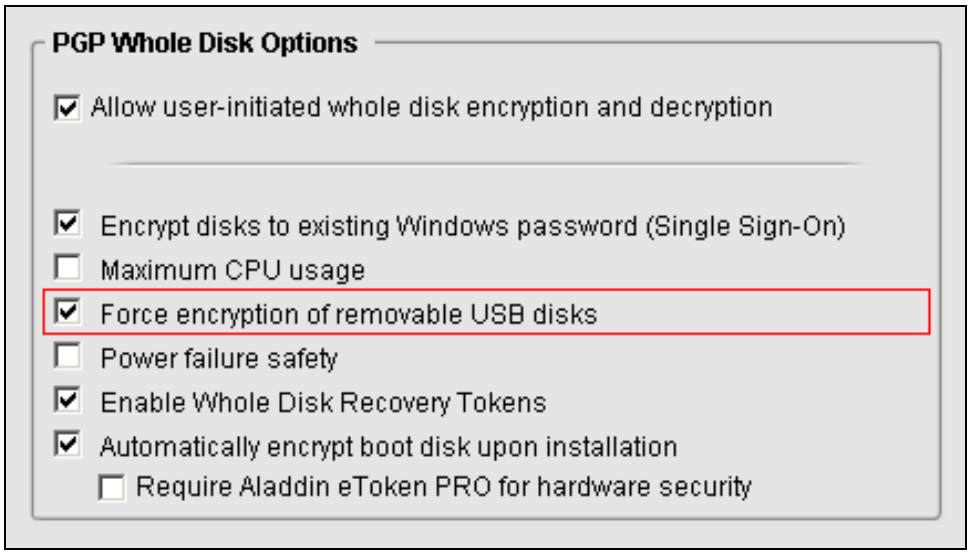


Figure 12: Enabling forced encryption of USB disks for a policy group

Once an administrator has enabled forced encryption of USB media, users will be prompted to encrypt unprotected USB drives when they are inserted into their computer (see Figure 13).

Figure 13: Forcing the user to encrypt a removable USB drive

PGP Whole Disk Encryption will automatically encrypt the drive unless the user chooses to "lock" the device, which results in **not** encrypting the drive and mounting it as a read-only drive. An encrypted USB drive can be read on any machine equipped with PGP Whole Disk Encryption, provided the correct authentication credentials are entered.

By forcing encryption of removable media, PGP Whole Disk Encryption and PGP Universal Server provide these benefits:

- **Centrally enforced protection for removable drives –** Encrypting a removable drive extends full disk encryption protection to removable media, eliminating the risk of a data breach arising from a lost or stolen USB drive. By enforcing encryption of removable devices automatically, PGP Universal Server eliminates the uncertainty of relying on users to take explicit action to secure data placed on removable devices.
- **Assured access to encrypted data –** PGP Universal Server's recovery passphrase feature ensures an organization can access a PGP Whole Disk Encryption–protected removable drive, enabling a user to reset a forgotten passphrase or an administrator to recover data (according to security policy or regulatory requirements) when an employee is unavailable or leaves the organization.

Maintaining Corporate Access to Encrypted Data

It is possible that a user will forget his/her PGP Whole Disk Encryption passphrase at some point and will require a way to access protected data and reset the passphrase. PGP Universal Server–managed PGP Whole Disk Encryption clients automatically generate and store unique one-time-use recovery passphrases in PGP Universal Server to enable recovery of access to encrypted data on boot, secondary, and removable drives, according to policy.

When a user loses his/her passphrase, the PGP Universal Server administrator can access this recovery passphrase from the administration console and provide it to the user (see Figure 14).

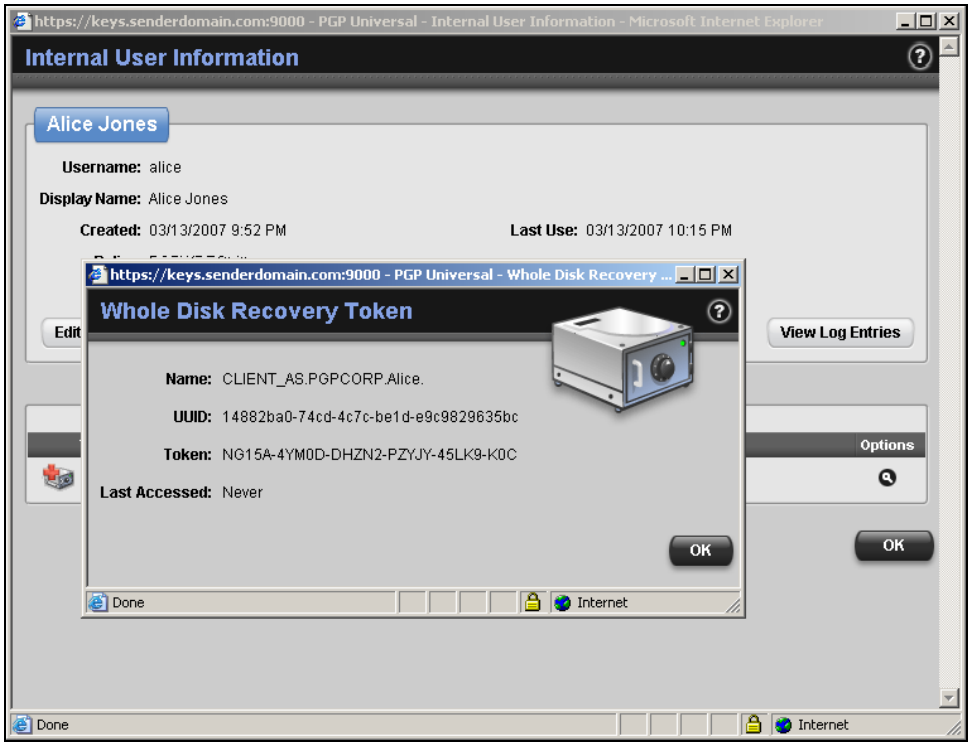


Figure 14: Accessing the recovery passphrase in PGP Universal Server

The administrator provides the recovery passphrase (the **Token** displayed in Figure 14) to the user, who uses it to authenticate to PGP Whole Disk Encryption. After authenticating to PGP Whole Disk Encryption, the user will be forced to establish a new passphrase. PGP Whole Disk Encryption will contact the PGP Universal Server to establish a new recovery passphrase to enable future recovery access.

PGP Universal Server's management of recovery passphrases for PGP Whole Disk Encryption clients provides these benefits:

- **Assured access to encrypted data –** PGP Universal Server's recovery passphrase feature ensures an organization can access a PGP Whole Disk Encryption–protected system, enabling a user to reset a forgotten passphrase, to recover data (according to security policy or regulatory requirements) when an employee is unavailable or leaves the organization, or to perform regular IT maintenance.

- **Controlled access to recovery passphrases –** PGP Universal Server's role-based administration capabilities ensure that only authorized administrators can access recovery passphrases. Each recovery passphrase is unique to a machine and regenerated by PGP Whole Disk Encryption automatically once it has been used, ensuring that a recovery passphrase can not be reused on the same machine or across machines.

Summary

This guide has demonstrated how PGP Whole Disk Encryption provides comprehensive, non-stop disk encryption, enabling quick, cost-effective protection for data on PCs, laptops, and removable media. Using PGP Whole Disk Encryption, an organization can lock down the entire contents of users' laptops, desktops, external drives, or USB flash drives, including boot sectors, system, and swap files. The application of encryption policy is transparent to the user, automatically protecting data without requiring user action or impacting user productivity.

Enterprises can also manage PGP Whole Disk Encryption policies by deploying PGP Universal Server. PGP Universal Server enforces disk encryption policies for boot drives and removable media, ensuring encrypted data is continuously safeguarded from unauthorized access. Encryption policy can be driven from existing organization group definitions in LDAP directories, minimizing the configuration required by the administrator to define encryption policy. In addition, PGP Universal Server enables remote assistance and ensures corporate access to encrypted data (according to security policy or regulatory requirements) by storing a unique one-time-use recovery passphrase for each managed PGP Whole Disk Encryption client.

As information moves throughout an organization, there are numerous opportunities for potential compromise. PGP Whole Disk Encryption allows an organization to immediately address the risks associated with data stored on laptops, desktops, and removable storage devices. The same data stored locally on disk drives can also be transferred via email or instant messaging both within the organization and externally to partners and customers. As an integrated application of the PGP Encryption Platform, PGP Whole Disk Encryption allows organizations to further address risk mitigation by adding additional encryption applications, such as PGP NetShare for file server encryption, using PGP Universal Server.

For More Information

User Documentation

The "PGP Desktop for Windows User's Guide" and "PGP Desktop for Windows Release Notes" were installed on your system when you installed the PGP Whole Disk Encryption product. By default, these files are installed in C:\Program Files\PGP Corporation\PGP Desktop\Documentation. These documents are also available directly from the PGP Corporation website:

- **PGP Product User Guides:** http://www.pgp.com/downloads/user_guides/index.html

Technical Support

- Reviewers requiring additional technical support as part of the review process should contact their PGP representative directly to obtain assistance.

- All PGP Whole Disk Encryption clients include a minimum of 1 year of PGP Basic Support, accessible via the Web and phone. For PGP Product Support and Customer Service, please visit the PGP Support Portal: https://www.pgp.com/support.
- PGP Corporation maintains a large and active community forum monitored by members of the PGP staff to respond to questions and issues posed by users of PGP products. To access the PGP Support forums, please go to: http://forums.pgpsupport.com.
- For any other contacts at PGP Corporation, please go to the Contact Us section of the PGP website: www.pgp.com/company/contact.html.

Research Reports

PGP Corporation, in conjunction with third-party analysts, periodically releases research reports quantifying the cost and risk of data breaches, the need for full disk encryption, and other information security trends. These reports are freely available from the PGP website (registration may be required):

- **Research Reports:** http://www.pgp.com/downloads/research_reports/index.html

PGP Corporation

3460 West Bayshore Road
Palo Alto, CA 94303 USA
Tel: +1 650 319 9000
Fax: +1 650 319 9001
Sales: +1 877 228 9747
Support: support.pgp.com
Website: www.pgp.com