PGP® Integration Guide

October 2007

PGP Universal Server™ 2.5
SmartLine DeviceLock® 6.2

Version 1.0

Table of Contents

INTRODUCTION **3**

STRUCTURE **3**

CAVEATS **4**

POLICY OVERVIEW **4**

SPAN OF CONTROL 4
COMPUTER "GROUPS" 4

SETUP **5**

1. PGP UNIVERSAL SERVER AND PGP DESKTOP 5
2. CREATE DEVICELOCK® POLICY 7
   Enable PGP Integration *7*
   Removable Permissions *7*
   Set Removable Policy *8*
4. CREATE BLOCKED MESSAGE (OPTIONAL) 9
5. POLICY TRANSMISSION 10

POLICY OPTIONS **10**

FORCED ENCRYPTION 10
PERMIT DECRYPTION 10
DISTRIBUTING PRE-ENCRYPTED DRIVES 11
DEVICELOCK® OPTIONS 12

USER EXPERIENCE **13**

ENCRYPTED USB OR FIREWIRE STORAGE DEVICE INSERTED 13
UNENCRYPTED USB OR FIREWIRE STORAGE DEVICE INSERTED 13

TROUBLESHOOTING **14**

PGP UNIVERSAL SERVER 14
SMARTLINE DEVICELOCK® 14

Introduction

SmartLine DeviceLock® is an enterprise-grade solution for controlling, monitoring, and logging access to removable media, portable devices, and communication interfaces. By implementing policies at the endpoints, SmartLine's solution effectively controls and monitors all I/O activities. Unauthorized transactions are blocked, and all transactions are monitored and logged. Security administrators can define granular policies that assign permissions to users or PCs to access any device, media, or communication interface.

The PGP® Encryption Platform provides a strategic enterprise encryption framework for key management, policy, and automated provisioning across multiple, integrated encryption applications. The integration of PGP Universal Server, PGP® Desktop, and SmartLine DeviceLock® enables organizations to deploy automated encryption as needed with the data security functions required to enforce robust security policy. This data-centric approach protects data in motion and in transit anywhere, anytime.

Structure

This guide outlines the configuration and management of highly granular port control policy using these software components:

Company	Management Component	Client
PGP Corporation	PGP Universal Server 2.5 or greater	Any PGP Desktop 9.5 or greater product with PGP® Whole Disk Encryption
SmartLine	• DeviceLock® Snap-in for Microsoft Group Policy Management • DeviceLock® Management Console (MMC) for direct computer management • DeviceLock® Enterprise Manager (DLEM) console for managing multiple computers simultaneously	DeviceLock® Service 6.2 or greater

Table 1: Software and Version Requirements

In this setup, DeviceLock® permits or denies device use for a group of users or computers. DeviceLock® can granularly manage access by device port, device class, device type, device model, device ID, time-of-day, and day-of-week. DeviceLock® can also require attached devices (see Table 2) to be encrypted by PGP Desktop's Whole Disk Encryption feature. Many PGP Desktop products are compatible with this configuration, but PGP Whole Disk Encryption is a required component.

The combination of PGP Desktop and the DeviceLock® Service permits greater policy granularity than is available from each separate product. How is policy delivered by each product? How is policy created and what policy combinations are permissible? This guide will address policy design, policy deployment, and policy management issues. However, this is not an installation guide for either

product. The software packages shown in Table 1 on page 3 should already be deployed prior to using this guide.

Caveats

PGP Universal Server's "forced encryption" option is used in this guide. This option increases security and simplifies deployment, but reduces the granularity of this integration. See the Enforced Encryption section in "Policy Options" on page 10 for more details.

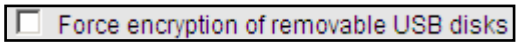
Policy Overview

Span of Control

Policy Issue	PGP Universal Server	SmartLine DeviceLock®
Computer Group Policies	✘	✓
Controlled Devices	PGP Desktop users with PGP Whole Disk Encryption and storage devices attached via USB or FireWire	Users with attached storage, CD/DVD/CDR, floppy, modem, infrared, WiFi, Bluetooth, FireWire, USB, and COM & LTP ports
Default Policy	Permit All	Permit All

Table 2: Policy Comparison

By default, PGP Universal Server permits **full** unencrypted read/write capability for all attached removable storage devices. This capability can be restricted by the PGP® NetShare and PGP Whole Disk Encryption products and by the PGP Universal Server option shown at right, which forces encryption for USB and FireWire devices.



By contrast, DeviceLock® can apply policy to particular types of USB devices and to a much broader variety of devices that are unknown to PGP Universal Server, such as infrared ports and WiFi devices.

Computer "Groups"

As shown in Table 2, DeviceLock® permits policy to be applied to "groups" of computers. These groups are actually Microsoft Active Directory (AD) container structures such as Domains and/or Organization Units (OUs.) Because policy by computer is not supported by PGP Universal Server, do not rely solely on "computer groups" to enforce policy. If Group Policy is the policy delivery mechanism, assign all users to at least one user policy in PGP Universal Server and make sure their AD accounts reside in a container (Domain or OU) that is managed by a linked DeviceLock® Group Policy ObjectGPO.

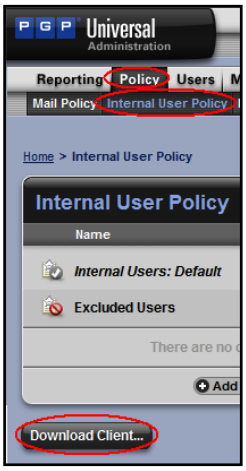
Setup

There are many ways to set up integrated encryption policy. This guide presumes a specific policy example, uses specific tools, and then discusses optional modifications. The assumptions are:

- PGP Universal Server has been installed.
- All machines have the DeviceLock® Service and bound PGP Desktop clients installed.
- All unencrypted removable storage devices are read-only.
- Removable storage devices are writeable only after they have been secured with PGP Whole Disk Encryption.

The following steps are used to define and disseminate policy using both products. A review of each step and its purpose precedes a discussion of the possible policy options.

1. PGP Universal Server and PGP Desktop



For the client machine, PGP Desktop with PGP Whole Disk Encryption encrypts or decrypts removable storage. PGP Desktop clients can be "bound" to the settings within PGP Universal Server. MSI files used to install bound clients are downloaded from PGP Universal Server, as shown at right. If PGP Desktop clients are bound, they can be forced to encrypt removable devices with PGP Whole Disk Encryption. If they are not bound, PGP Desktop users can choose to encrypt devices on their own.

Step 1: PGP Universal Server should be configured to enforce bound PGP Desktop users to apply whole disk encryption to removable devices. Edit the internal user policy, as shown in Figure 1 (below):

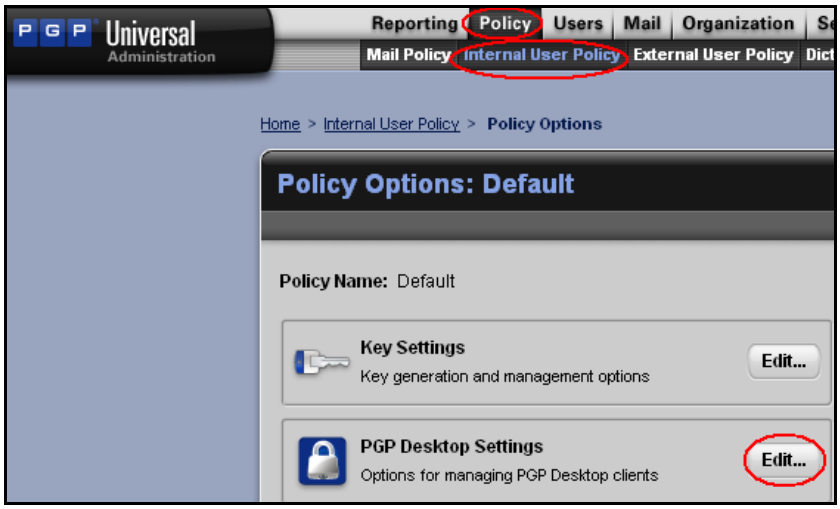


Figure 1: Modify Internal User Policy

Step 2: Select the option to enforce whole disk encryption of USB and FireWire devices. Figure 2 is a shortened version of this screen. Note that bound users are not permitted to encrypt and decrypt. This option is discussed further on page 10.

Figure 2: Force Whole Disk Encryption for Bound Clients

Save this configuration change. All bound clients created after this change will include this option. Any bound clients that are deployed before this change will realize the new policy after 24 hours or when they next login, whichever comes first.

For now, assume DeviceLock® is configured to permit all devices. Users under the control of the Figure 2 policy setting will see the screen shown in Figure 3 when they install a new device. Within 30 seconds, the user must decide whether to encrypt the device or use the device in a read-only mode called “Lock”. After 30 seconds, “Lock” is selected automatically and the device is unmodified and unwriteable. Without DeviceLock®, this same policy would have to apply to all devices.

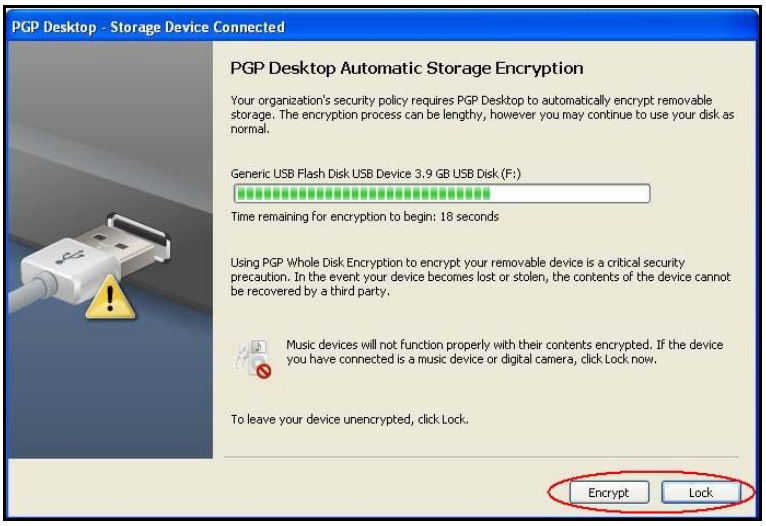


Figure 3: Encrypt or Lock

2. Create DeviceLock® Policy

The remaining configuration steps occur within DeviceLock®, using either the DeviceLock® snap-in for the Microsoft Group Policy Management Console (GPMC), the raw DeviceLock® Management MMC Console, or the DeviceLock® Enterprise Manager (DLEM).

Enable PGP Integration

Enable PGP Integration, as shown in Figure 4:

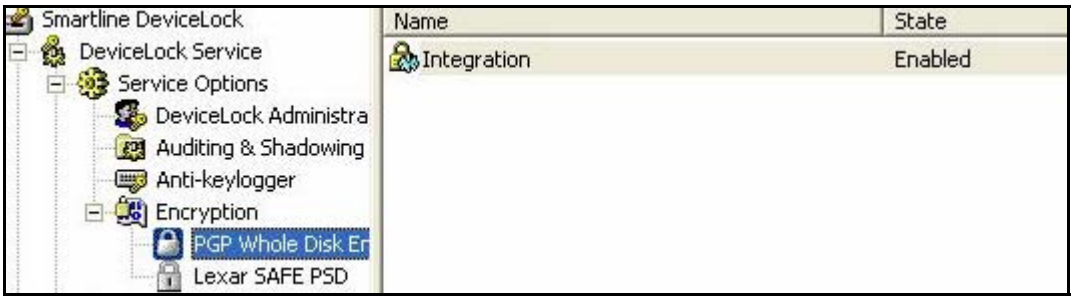


Figure 4: Set Removable Permissions

Set Removable Permissions

Set permissions for removable devices, as shown in Figure 5:

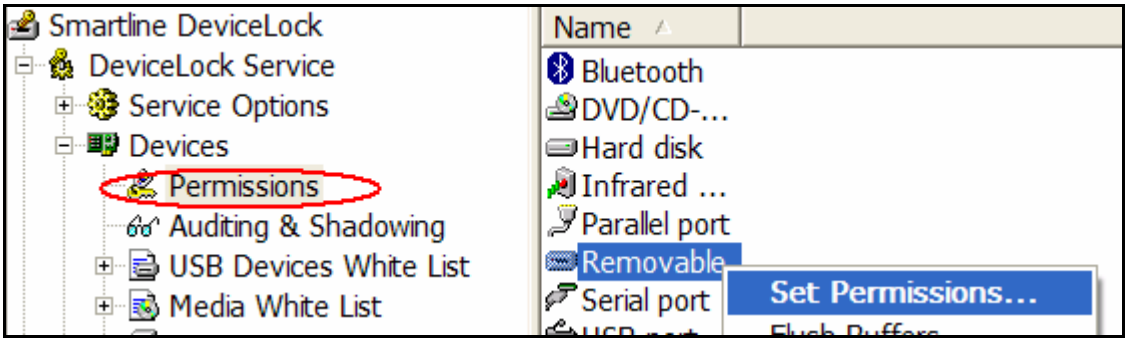


Figure 5: Set Removable Permissions

Set Removable Policy

Figure 6 demonstrates the application of group policy to accounting users. Unencrypted devices are granted read-only and eject permission. Full read and write access is granted for removable devices that have been encrypted via PGP Whole Disk Encryption. Other encryption technologies are not recognized by this setting.

This setting works in concert with PGP Universal Server policy, which can require that unencrypted storage devices are encrypted upon insertion or "locked" for read-only access.

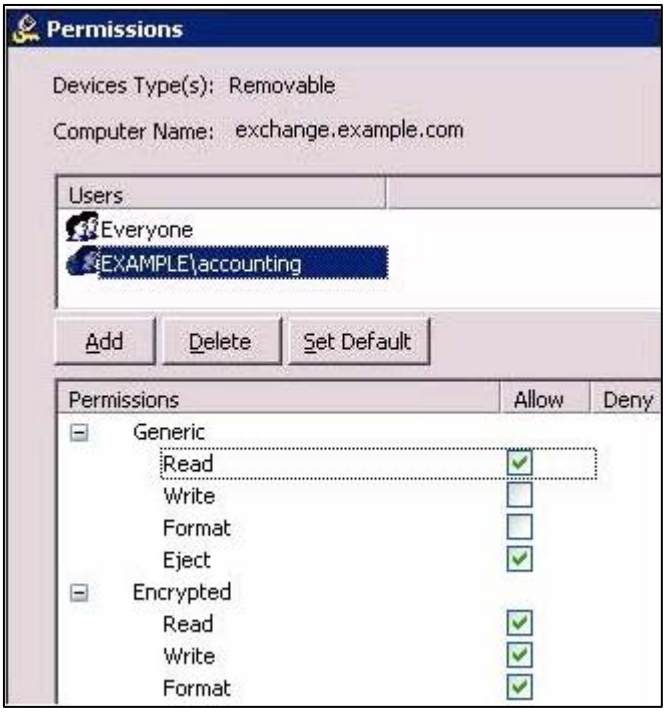


Figure 6: Set Encryption Policy

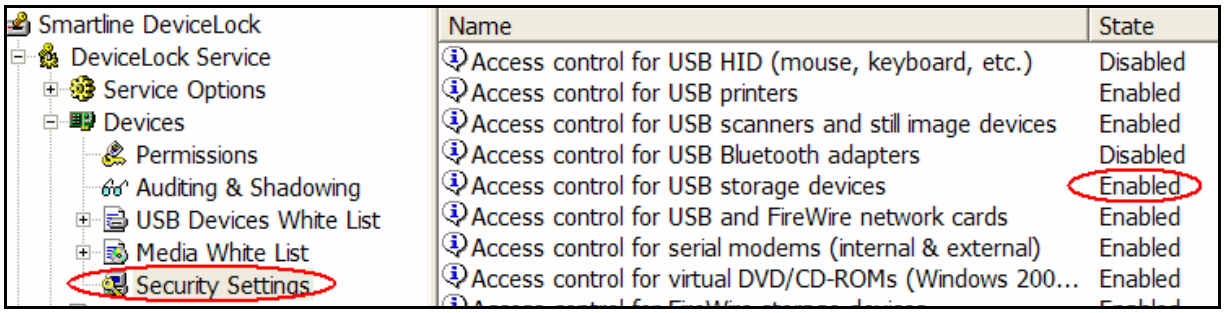
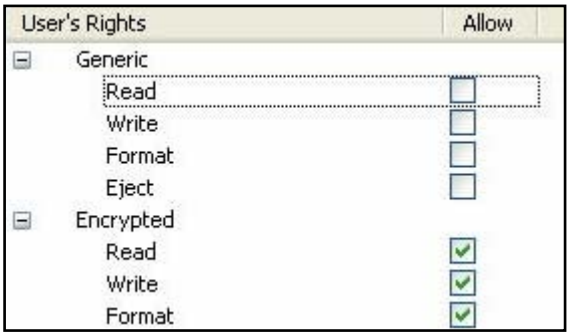


Figure 7: Access Control

Make sure that access control for USB storage devices is enabled, as shown in Figure 7. This setting will generally block USB storage device access except as users/groups are granted access in the USB Port & Removable "Permissions" lists.

4. Create Blocked Message (optional)

The policy shown at right is stricter than the policy created on page 8. This policy only permits encrypted removable devices. In this instance, an inserted unencrypted device will not be accessible even if the drive letter appears in the client's "My Computer" window.



To provide some indication of why the unencrypted device is not visible, enable the display of a blocked message. Start by selecting "Service Options," as shown in Figure 7.

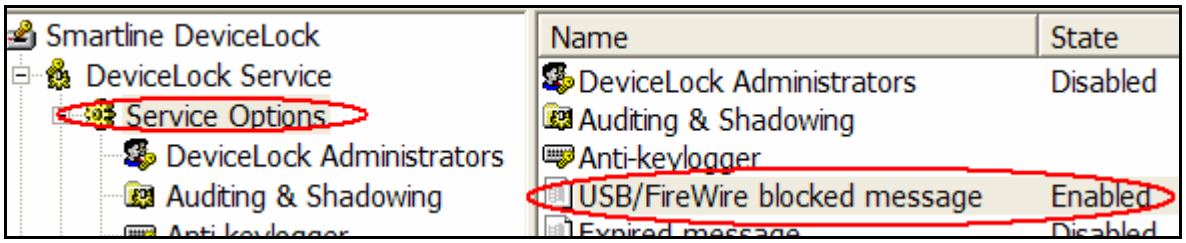
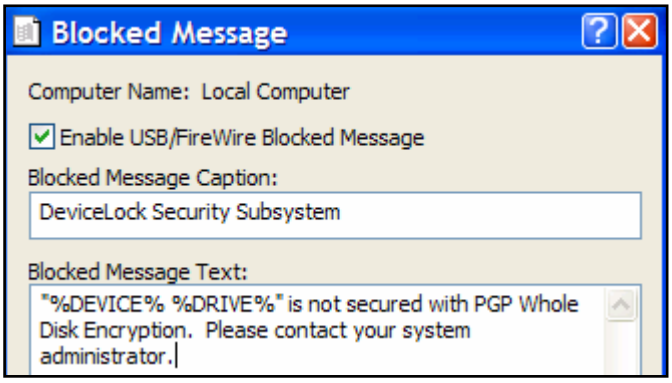


Figure 7: Enable Blocked Message

Create an appropriate error message, as shown at right. This message will appear in the system tray when an unencrypted or unauthorized device is inserted into the client machine.



5. Policy Transmission

Table 3 shows the different mechanisms PGP Universal Server and DeviceLock® use to drive policy. PGP Universal Server cannot push policy to the PGP Desktop clients. Generally, PGP Universal Server policy is "set and forget," whereas DeviceLock® policy will change as new security devices are implemented and approved.

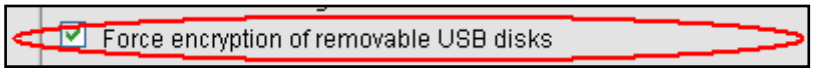
Action	PGP Universal Server	SmartLine DeviceLock®
Push: Admin manually sends policy	N/A	DeviceLock® Management MMC console or DLEM console
Push: Automatic policy updates	N/A	If setup via Microsoft GPO, every 90 minutes by default
Pull: Client requests policy from server	Requested by client every 24 hours or at user login	At user login or if GPO is in force, select Start / Run: gpupdate /force

Table 3: Policy Communications

Policy Options

Forced Encryption

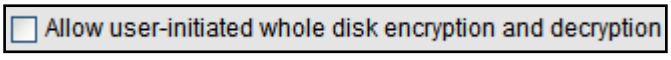
As discussed on page 6, PGP Universal Server policy can force all USB and FireWire devices to be whole disk encrypted. This option has a variety of policy and process implications. If both boxes are checked and a user inserts an unencrypted USB or FireWire drive, the "encrypt or lock" message shown on page 6 will appear.



Enabling forced encryption is a two-sided coin. It permits simpler deployment because any unencrypted storage device can easily be encrypted by an end user and put to use. Unlike DeviceLock®, however, PGP Universal Server does not distinguish one device from another. And PGP Universal Server policy trumps DeviceLock® policy. This setup eliminates the ability to manage devices distinctly. One viable alternative is to disable forced encryption and distribute encrypted drives to users. This option is discussed on page 11.

Permit Decryption

PGP Universal Server also provides an option that controls a bound user's ability to encrypt and decrypt devices. If the user is permitted to decrypt the USB or FireWire drive, an encrypted drive can be placed into a machine and decrypted. The USB or FireWire drive can then be transported without encryption, which may break policy. To prevent this possibility, disable "allow user-initiated whole disk encryption and decryption", as shown here.

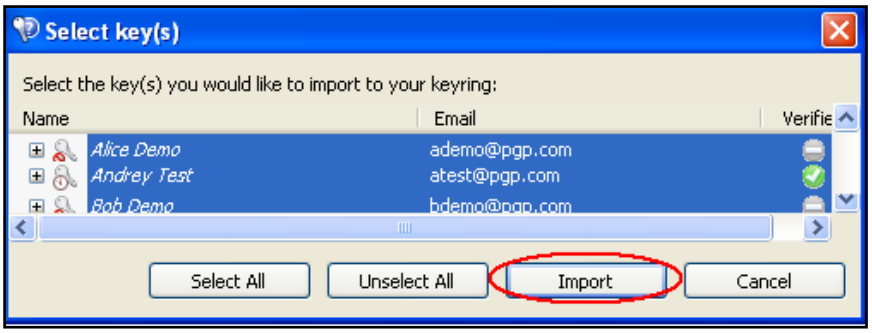


If the user-initiated option is disabled, sensitive data cannot be removed without whole disk encryption. This configuration also permits the USB or FireWire device to be "force encrypted" upon first insertion.

Distributing Pre-Encrypted Drives

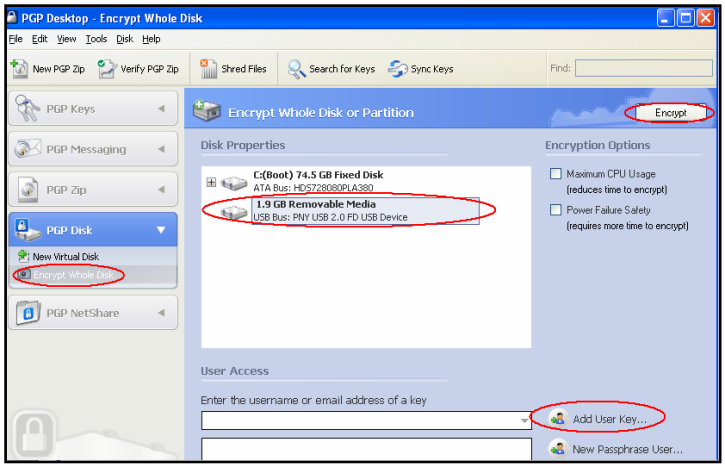
If desired, bulk distribution of whole disk encrypted USB or FireWire devices can be performed using the administrator's copy of PGP Desktop. Begin by searching for all user keys, as shown below. Select all the keys in the result and export all keys to a file. Minimize PGP Desktop.

Double-click on the exported file and import all keys to the administrator's keyring, as shown below.



Insert the first USB drive into the administrator's PC. From the "PGP Disk" menu, select "Encrypt Whole Disk". Select "Add User Key" and choose the public key of the first user.

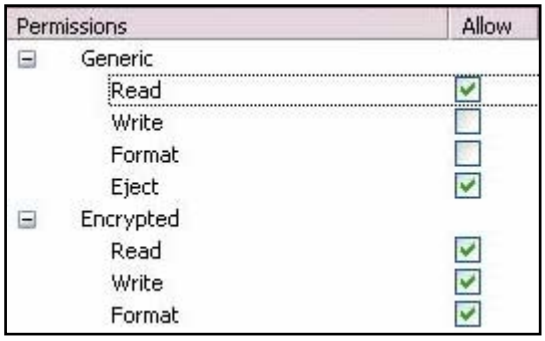
You must also add a second user with a passphrase. This could be the private key of the administrator or a randomly created user whose name and password is (or is not) recorded for future use. Select "Encrypt", as shown at right. When encryption begins, PGP Desktop will display this symbol  in the notification area.



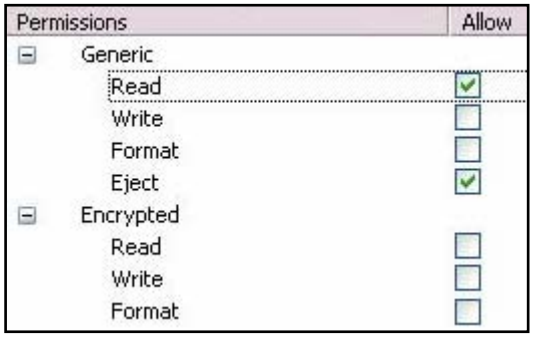
Encryption time depends on the size of the drive, the speed of the processor, and USB/FireWire port speed. When finished, insert the next USB drive and repeat the process.

DeviceLock® Options

The setup outlined by this guide resulted in the creation of the policy shown at right. If all "Allow" boxes are checked, all removable devices and all encrypted devices would have full read and write permission.



If the encrypted options are not selected, the PGP Desktop client will still recognize the encrypted device and request the passphrase. However, after the passphrase is entered, this DeviceLock® policy will prevent the drive from being recognized by the system. If forced PGP encryption is in place, the removable storage device will be unreadable after it is encrypted. If the encrypted device is placed into a system that permits encrypted devices, it will be accessible.



User Experience

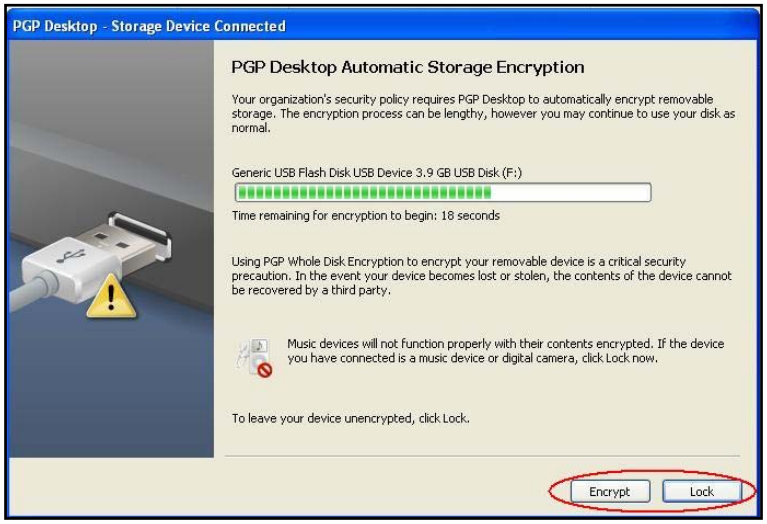
What is the sequence of events when a removable storage device is accessed? The PGP policy options are checked before the DeviceLock® policy is enforced.

Encrypted USB or FireWire Storage Device Inserted

If the inserted device is already encrypted, a passphrase will be requested, as shown at right.

Unencrypted USB or FireWire Storage Device Inserted

If forced encryption (page 6) is enabled and the device is not whole disk encrypted, the user is prompted to encrypt or lock the device, regardless of DeviceLock® policy. However, PGP Desktop access to the device is strictly limited by DeviceLock® settings. For example, if encrypted removable devices are not permitted by DeviceLock®, PGP Desktop will be unable to successfully read the device.



When encryption begins, PGP Desktop will display this symbol  in the notification area. Whole disk encryption time depends on the size of the drive, the speed of the processor, and USB/FireWire port speed.

Troubleshooting

PGP Universal Server

PGP Universal's logging system features detailed logging. Administrative activities such as setting the forced encryption option are tracked in the Administration log. Figure 8 follows the bound PGP Desktop client from a client with a particular IP address as it connects and authenticates to PGP Universal Server. The movement and disposition of removable devices is not tracked by PGP Universal Server.

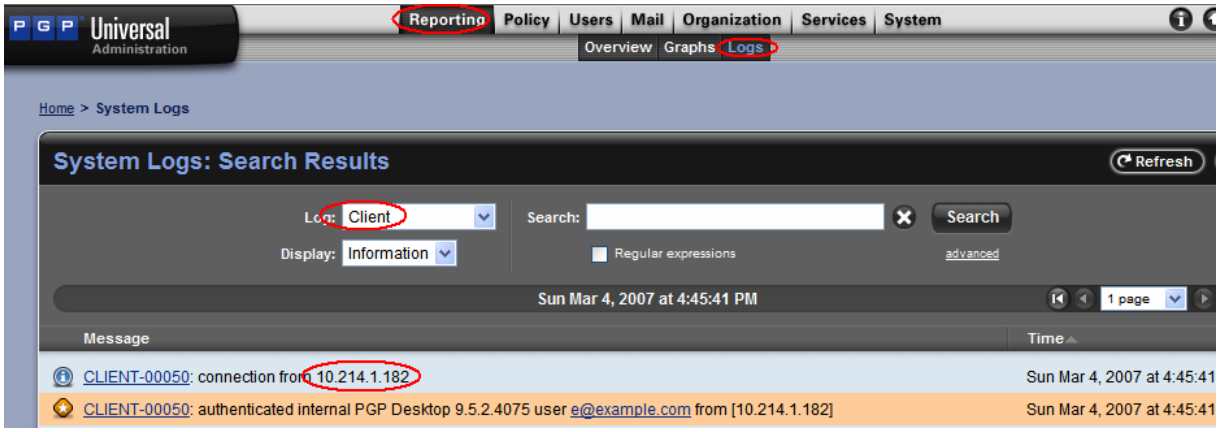


Figure 8: PGP Universal Server Client Log

SmartLine DeviceLock®

The DLEM permits access/auditing/shadowing permissions. The DLEM also tracks permissions and plug-n-play devices on all endpoints. These log views permit user activities and administrative actions to be collected, viewed, filtered, and sorted centrally on demand.

The optional DeviceLock® Enterprise Server component can be configured to automatically collect logs and shadow data to a central storage area for further analysis.

PGP Corporation

3460 West Bayshore Road
Palo Alto, CA 94303 USA
Tel: +1 650 319 9000
Fax: +1 650 319 9001
Sales: +1 888 515 4920
Support: support.pgp.com
Website: www.pgp.com