PGP Whole Disk Encryption Command Line

User's Guide

Version Information

PGP Whole Disk Encryption Command Line User's Guide. Version 10.0.0. Released January 2010.

Copyright Information

Trademark Information

Licensing and Patent Information

The IDEA cryptographic cipher described in U.S. patent number 5,214,703 is licensed from Ascom Tech AG. The CAST-128 encryption algorithm, implemented from RFC 2144, is available worldwide on a royalty-free basis for commercial and non-commercial uses. PGP Corporation has secured a license to the patent rights contained in the patent application Serial Number 10/655,563 by The Regents of the University of California, entitled Block Cipher Mode of Operation for Constructing a Wide-blocksize block Cipher from a Conventional Block Cipher. Some third-party software included in PGP Universal Server is licensed under the GNU General Public License (GPL). PGP Universal Server as a whole is not licensed under the GPL. If you would like a copy of the source code for the GPL software included in PGP Universal Server, contact *PGP Support* (https://support.pgp.com). PGP Corporation may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents.

Acknowledgments

This product includes or may include:

– The Zip and ZLib compression code, created by Mark Adler and Jean-Loup Gailly, is used with permission from the free Info-ZIP implementation, developed by zlib (http://www.zlib.net). – Libxml2, the XML C parser and toolkit developed for the Gnome project and distributed and copyrighted under the MIT License found at http://www.opensource.org/licenses/mit-license.html. Copyright © 2007 by the Open Source Initiative. – bzip2 1.0, a freely available high-quality data compressor, is copyrighted by Julian Seward, © 1996-2005. – Application server (http://jakarta.apache.org/), web server (http://www.apache.org/), Jakarta Commons (http://jakarta.apache.org/commons/license.html) and log4j, a Java-based library used to parse HTML, developed by the Apache Software Foundation. The license is at www.apache.org/licenses/LICENSE-2.0.txt. – Castor, an open-source, data-binding framework for moving data from XML to Java programming language objects and from Java to databases, is released by the ExoLab Group under an Apache 2.0-style license, available at http://www.castor.org/license.html. – Xalan, an open-source software library from the Apache Software Foundation that implements the XSLT XML transformation language and the XPath XML query language, is released under the Apache Software License, version 1.1, available at http://xml.apache.org/xalan-j/#license1.1. – Apache Axis is an implementation of the SOAP ("Simple Object Access Protocol") used for communications between various PGP products is provided under the Apache license found at http://www.apache.org/licenses/LICENSE-2.0.txt. – mx4j, an open-source implementation of the Java Management Extensions (JMX), is released under an Apache-style license, available at http://mx4j.sourceforge.net/docs/ch01s06.html. – jpeglib version 6a is based in part on the work of the Independent JPEG Group. (http://www.ijg.org/) – libxslt the XSLT C library developed for the GNOME project and used for XML transformations is distributed under the MIT License http://www.opensource.org/licenses/mit-license.html. – PCRE version 4.5 Perl regular expression compiler, copyrighted and distributed by University of Cambridge. ©1997-2006. The license agreement is at http://www.pcre.org/license.txt. – BIND Balanced Binary Tree Library and Domain Name System (DNS) protocols developed and copyrighted by Internet Systems Consortium, Inc. (http://www.isc.org) – Free BSD implementation of daemon developed by The FreeBSD Project, © 1994-2006. – Simple Network Management Protocol Library developed and copyrighted by Carnegie Mellon University © 1989, 1991, 1992, Networks Associates Technology, Inc, © 2001- 2003, Cambridge Broadband Ltd. © 2001- 2003, Sun Microsystems, Inc., © 2003, Sparta, Inc, © 2003-2006, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. The license agreement for these is at http://net-snmp.sourceforge.net/about/license.html. -- NTP version 4.2 developed by Network Time Protocol and copyrighted to various contributors. – Lightweight Directory Access Protocol developed and copyrighted by OpenLDAP Foundation. OpenLDAP is an open-source implementation of the Lightweight Directory Access Protocol (LDAP). Copyright © 1999-2003, The OpenLDAP Foundation. The license agreement is at http://www.openldap.org/software/release/license.html. Secure shell OpenSSH version 4.2.1 developed by OpenBSD project is released by the OpenBSD Project under a BSD-style license, available at http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD. – PC/SC Lite is a free implementation of PC/SC, a specification for SmartCard integration is released under the BSD license. -- Postfix, an open source mail transfer agent (MTA), is released under the IBM Public License 1.0, available at http://www.opensource.org/licenses/ibmpl.php. – PostgreSQL, a free software object-relational database management system, is released under a BSD-style license, available at http://www.postgresql.org/about/licence. – PostgreSQL JDBC driver, a free Java program used to connect to a PostgreSQL database using standard, database independent Java code, (c) 1997-2005, PostgreSQL Global Development Group, is released under a BSD-style license, available at http://jdbc.postgresql.org/license.html. -- PostgreSQL Regular Expression Library, a free software object-relational database management system, is released under a BSD-style license, available at http://www.postgresql.org/about/licence. -- 21.vixie-cron is the Vixie version of cron, a standard UNIX daemon that runs specified programs at scheduled times. Copyright © 1993, 1994 by Paul Vixie; used by permission. -- JacORB, a Java object used to facilitate communication between processes written in Java and the data layer, is open source licensed under the GNU Library General Public License (LGPL) available at http://www.jacorb.org/lgpl.html. Copyright © 2006 The JacORB Project. -- TAO (The ACE ORB) is an open-source implementation of a CORBA Object Request Broker (ORB), and is used for communication between processes written in C/C++ and the data layer. Copyright (c) 1993-2006 by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University. The open source software license is available at http://www.cs.wustl.edu/~schmidt/ACE-copying.html. -- libcURL, a library for downloading files via common network services, is open source software provided under a MIT/X derivate license available at http://curl.haxx.se/docs/copyright.html. Copyright (c) 1996 - 2007, Daniel Stenberg. – libuuid, a library used to generate unique identifiers, is released under a BSD-style license, available at http://thunk.org/hg/e2fsprogs/?file/fe55db3e508c/lib/uuid/COPYING. Copyright (C) 1996, 1997 Theodore Ts'o. – libpopt, a library that parses command line options, is released under the terms of the GNU Free Documentation License available at http://directory.fsf.org/libs/COPYING.DOC. Copyright © 2000-2003 Free Software Foundation, Inc. – gSOAP, a development tool for Windows clients to communicate with the Intel Corporation AMT chipset on a motherboard, is distributed under the GNU Public License, available at

http://www.cs.fsu.edu/~engelen/soaplicense.html. -- Windows Template Library (WTL) is used for developing user interface components and is distributed under the Common Public License v1.0 found at http://opensource.org/licenses/cpl1.0.php. -- The Perl Kit provides several independent utilities used to automate a variety of maintenance functions and is provided under the Perl Artistic License, found at http://www.perl.com/pub/a/language/misc/Artistic.html. -- rEFIt - libeg, provides a graphical interface library for EFI, including image rendering, text rendering, and alpha blending, and is distributed under the license found at http://refit.svn.sourceforge.net/viewvc/*checkout*/refit/trunk/refit/LICENSE.txt?revision=288. Copyright (c) 2006 Christoph Pfisterer. All rights reserved. -- Java Radius Client, used to authenticate PGP Universal Web Messenger users via Radius, is distributed under the Lesser General Public License (LGPL) found at http://www.gnu.org/licenses/lgpl.html. -- Yahoo! User Interface (YUI) library version 2.5.2, a Web UI interface library for AJAX. Copyright (c) 2009, Yahoo! Inc. All rights reserved. Released under a BSD-style license, available at http://developer.yahoo.com/yui/license.html. -- JSON-lib version 2.2.1, a Java library used to convert Java objects to JSON (JavaScript Object Notation) objects for AJAX. Distributed under the Apache 2.0 license, available at http://json-lib.sourceforge.net/license.html. -- EZMorph, used by JSON-lib, is distributed under the Apache 2.0 license, available at http://ezmorph.sourceforge.net/license.html. -- Apache Commons Lang, used by JSON-lib, is distributed under the Apache 2.0 license, available at http://commons.apache.org/license.html. -- Apache Commons BeanUtils, used by JSON-lib, is distributed under the Apache 2.0 license, available at http://commons.apache.org/license.html.

Export Information

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restricts the export and re-export of certain products and technical data.

Limitations

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement provided with the software. The information in this document is subject to change without notice. PGP Corporation does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by PGP Corporation.

Contents

Introduction 5

About PGP Whole Disk Encryption 5
About PGP Whole Disk Encryption Command Line 5
Important Terms 6
Audience 7
System Requirements 7
Installing and Uninstalling 7
PGP Whole Disk Encrypting a Drive 8

The Command-Line Interface 9

Overview 9
Scripting 10
Editing the Path 10
WDE-ADMIN Active Directory Group 11
Passphrases 11

Licensing 13

Overview 13
--license-authorize 13
Licensing via a Proxy Server 14

Generic Commands 17

--help (-h) 17
--version 18

Disk Information Commands 19

--enum 19
--info 20
--show-config 21
--status 22

User Management Commands 23

--add-user 23
--change-passphrase 25
--change-userdomain 25
--list-user 26
--offload 27
--remove-user 27
--verify-user 28

Disk Management 31

--auth 31
--instrument 32
--uninstrument 32

Disk Operation 33

--decrypt 33
--encrypt 34
--resume 35
--secure 36
--stop 37

Boot Bypass Commands 39

--add-bypass 39
--check-bypass 40
--remove-bypass 41

Recovery Token Commands 43

--new-wdrt 43

PGP BootGuard Customization Commands 45

--set-background 45
--set-language 46
--set-sound 47
--set-start 48
--set-text 49

Local Self Recovery 51

--recovery-configure 52
--recovery-questions 53
--recovery-verify 54
--recovery-remove 55
--recovery-change-passphrase 55
Authenticating if you Have Forgotten Your Passphrase 56

Options 59

"Secure" Options 62
--admin-authorization 62
--admin-passphrase 62
--all 63
--answers-file 63
--auto-start 63
--beep 63
--dedicated-mode 64
--disk (-d) 64
--display 64
--domain-name 65
--fast-mode 65
--image 65
--interactive 66
--keyboard 66
--keyid 66
--license-email 67
--license-name 67
--license-number 67
--license-organization 68
--message 68
--new-domain 68
--new-passphrase 69
--no-beep 69
--partition 69
--passphrase (-p) 70
--proxy-passphrase 70
--proxy-server 71
--proxy-username 71
--questions-file 71
--recovery-token 72
--safe-mode 72
--sso 72
--username 73
--xml 73

Quick Reference 75

Commands 75
Options 77

Troubleshooting 79

Overview 79
Encryption Does Not Begin 80
Encryption Does Not Finish 82
Problems at PGP BootGuard 83

1 Introduction

This User's Guide tells you how to use PGP Whole Disk Encryption Command Line.

In This Chapter

About PGP Whole Disk Encryption 5
About PGP Whole Disk Encryption Command Line 5
Important Terms 6
Audience 7
System Requirements 7
Installing and Uninstalling 7
PGP Whole Disk Encrypting a Drive 8

About PGP Whole Disk Encryption

PGP Whole Disk Encryption (WDE) is a software product from PGP Corporation that uses encryption to lock down the entire contents of a boot disk, partition, external disk, or removable disk.

For more information about PGP WDE, see the:

- *PGP Desktop User's Guide*
- *PGP WDE Quick Start Guide*
- *PGP WDE Data Sheet* (available via the PGP WDE page on the PGP Corporation website)

About PGP Whole Disk Encryption Command Line

PGP Whole Disk Encryption Command Line gives you access to PGP WDE functionality using a command-line interface. Accessing PGP WDE functions from the command line is useful for scripting PGP WDE functions, troubleshooting problems, or if the graphical user interface is not available.

Note: Not all PGP WDE functions are available via the command line.

PGP WDE command line functionality is available for both Windows and Mac OS X systems. This Guide covers both versions. Differences between the two versions are noted where applicable.

Note: The Mac OS X Safe Boot feature does not work on a boot disk that has been whole disk encrypted; if you hold down the Shift key to enter Safe Boot, the system will fail to boot after authenticating at the PGP BootGuard screen.

Important Terms

Understanding the following terms will help make it easier to use PGP Whole Disk Encryption Command Line:

- **PGP Whole Disk Encryption (PGP WDE):** a standalone product from PGP Corporation and a feature of PGP Desktop that lets you encrypt the entire contents of a disk; boot disks, partitions, and non-boot disks such as USB thumb drives can all be whole disk encrypted. PGP WDE functionality is available via a graphical user interface and through a command-line interface.
- **PGP WDE command line:** the command-line interface to PGP WDE functionality. Because PGP WDE is available on both Windows and Mac OS X systems, you can use the PGP WDE command line interface using command line utilities such as the Command Prompt application, cmd.exe, on Windows systems or the Terminal application on Mac OS X systems.
- **passphrase user:** a user who can authenticate to an encrypted disk using a passphrase.
- **public-key user:** a user who can authenticate to an encrypted disk using the passphrase to the corresponding private key.
- **encrypt:** the process of "scrambling" data so that it is not usable unless you properly authenticate.
- **decrypt:** the process of "unscrambling" encrypted data.
- **master boot record (MBR):** software on a disk that is "in front" of the partition table; that is, it is implemented during the startup process *before* the operating system itself. The instructions in the MBR tells the system how to boot.
- **instrument:** a part of the process of whole disk encrypting a disk/partition where the Windows or Mac OS X MBR is replaced with the PGPMBR.
- **PGPMBR:** an MBR from PGP Corporation that implements the PGP BootGuard. Once a disk is instrumented, even if it is not fully encrypted, subsequent startups will bring up the PGP BootGuard.
- **PGP BootGuard:** the screen that appears after instrumenting a disk that requires proper authentication for the boot process to continue. If proper authentication is *not* provided, the boot process will not continue; the operating system will not load and the system will not be usable.

- **uninstrument:** removing the PGPMBR and replacing it with the original Windows or Mac OS X MBR (which was saved when the disk was instrumented).
- **whole disk recovery token (WDRT):** an additional passphrase for a whole disk encrypted disk that is passed to the appropriate PGP Universal Server if the disk is part of a PGP Universal-managed environment.
- **PGP Universal Server:** a management console for securing data from PGP Corporation.
- **recovery:** the process of restoring access to a disk/partition that has been whole disk encrypted but now cannot be decrypted.

Audience

This User's Guide is for anyone who is going to be using PGP Whole Disk Encryption Command Line to perform PGP WDE functions from the command line.

It assumes you are familiar with using PGP WDE via the graphical user interface, either in the standalone product or as part of PGP Desktop.

System Requirements

The system requirements for PGP Whole Disk Encryption Command Line are the same as for PGP WDE itself; if PGP WDE (standalone or as part of PGP Desktop) installs on a system, PGP Whole Disk Encryption Command Line will also install and be usable.

Installing and Uninstalling

PGP Whole Disk Encryption Command Line is installed automatically when PGP WDE or PGP Desktop is installed on a system.

To uninstall PGP Whole Disk Encryption Command Line, simply uninstall PGP WDE or PGP Desktop.

PGP Whole Disk Encrypting a Drive

To PGP Whole Disk Encrypt a drive requires several things: the drive must be instrumented, there must be at least one authorized user on the drive, and the drive must be encrypted.

There are two ways to PGP Whole Disk Encrypt a drive:

- **using a single command, --secure:** this one command instruments the drive, creates an authorized user, and encrypts the drive. This command is most useful when you have just installed PGP Whole Disk Encryption Command Line and thus have not instrumented any drives, created any authorized users, or encrypted any drives.
- **using multiple commands:** for scenarios where you do not need all three things required to PGP Whole Disk Encrypt at drive, or if you just prefer using individual commands, you can use `--instrument`, `--add-user`, and finally `--encrypt` to PGP Whole Disk Encrypt a drive.

2 The Command-Line Interface

This section describes the command-line interface used by PGP Whole Disk Encryption Command Line.

In This Chapter

Overview 9
Scripting 10
Editing the Path 10
WDE-ADMIN Active Directory Group 11
Passphrases 11

Overview

PGP Whole Disk Encryption Command Line uses a command-line interface.

You enter a valid command at the command prompt and press **Enter** or **return**. PGP Whole Disk Encryption Command Line responds based on what you entered: with success (if you entered a valid command) or with an error message (if you entered an invalid or incorrectly structured command).

All PGP Whole Disk Encryption Command Line commands have a *long form*: the text "pgpwde", a space, two hyphens "--", the command name, and options (if appropriate).

For example:

```
C:\>pgpwde --help [Enter]
```

is the command to display the built-in help information. It has no options.

(The command prompt, C:\> in the above example, and [Enter] will no longer be shown in examples; only the necessary commands and options will be shown.)

A few commands also have a *short form*: either one hyphen and then a single letter or two hyphens and two letters.

For example:

`-h` for help instead of `--help`

`--aa` for administrative authorization instead of `--admin-authorization`

You can mix long forms and short forms in a single command.

Short forms are noted where appropriate.

Scripting

PGP Whole Disk Encryption Command Line commands can easily be inserted into scripts for automating common tasks, such as encrypting a disk or getting information about an encrypted disk.

PGP Whole Disk Encryption Command Line commands can easily be added to scripts written with scripting languages such as Perl or Python.

Editing the Path

By default, the PGP Whole Disk Encryption Command Line application, pgpwde.exe, is installed in C:\Program Files\PGP Corporation\PGP Desktop\ on Windows systems.

To use PGP Whole Disk Encryption Command Line using the Windows Command Prompt application, you need to navigate to the PGP Whole Disk Encryption Command Line directory to execute commands (or the commands will fail).

If you wish to be able to execute PGP Whole Disk Encryption Command Line commands from any location when using Windows Command Prompt, you need to change the path on the system to include the location of the PGP Whole Disk Encryption Command Line application.

Note: On Mac OS X systems, you can use the Terminal application that ships with Mac OS X as your command line editor. You can enter commands from any location on the system; you do not have to navigate to a specific location.

To add the PGP Whole Disk Encryption Command Line application to your path on a Windows 7 or Vista system:

1. On the Windows desktop, right click the **Computer** icon, then select **Properties**.
2. On the left side of the **System Control Panel** screen, click **Advanced System Settings**.
3. If you are prompted for permission to continue, click **Continue**.
4. At the bottom of the **System Properties** screen, click **Environment Variables**.
5. In the **System Variables** section at the bottom of the **Environment Variables** screen, select **Path**, then click **Edit**.

6 At the end of the existing **Variable value** line, enter a semicolon (;), then add the path to the PGP Whole Disk Encryption Command Line application

7 Click **OK** to save the change, then close the windows you opened.

To add the PGP Whole Disk Encryption Command Line application to your path on a Windows XP or 2000 system:

1 On the Windows desktop, right click the **My Computer** icon, then select **Properties**.

2 On the **System Properties** dialog, click the **Advanced** tab.

3 At the bottom of the **Advanced** tab, click **Environment Variables**.

4 In the **System Variables** section at the bottom of the **Environment Variables** screen, select **Path**, then click **Edit**.

5 At the end of the existing **Variable value** line, enter a semicolon (;), then add the path to the PGP Whole Disk Encryption Command Line application.

6 Click **OK** to save the change, then close the windows you opened.

WDE-ADMIN Active Directory Group

If you are an administrator of PGP WDE clients in a PGP Universal environment and using Active Directory, you can create a special Active Directory group to allow you to run commands on your managed PGP WDE clients without knowing the passphrase of a user on the encrypted disk.

This special Active Directory group, which *must* be called WDE-ADMIN, must be a security group, not a distribution group.

Using the `--admin-authorization` option is useful for running administrative tasks in an enterprise.

Refer to the *PGP Universal Administrator's Guide* for more information about creating and using the WDE-ADMIN Active Directory group.

Passphrases

For consistency, all example passphrases in this guide are shown in single quotation marks ('). Putting passphrases between single quotation marks ensures that reserved characters and spaces are interpreted correctly.

If you do not use any reserved characters or spaces in your passphrases, then you do not have to enclose them in single quotation marks.

On Windows systems, if you have a space in a passphrase, you must enclose the passphrase in single or double quotation marks when you enter it. Also, double quotation marks (") as part of the passphrase must be escaped with a preceding double quotation mark.

For example, if you want to use

Thomas "Stonewall" Jackson

as your passphrase, you would have to enter it as

'Thomas ""Stonewall"" Jackson'

on the command line. You need the quotation marks at the beginning and end for the spaces and you need to escape each double quotation mark used in the passphrase with another double quotation mark.

If you do enclose your passphrases in single quotation marks, and you have a single quotation mark as part of a passphrase on a *NIX system, you must escape the single quotation mark that is part of the passphrase. Escaping means you need to put another special character in front of the character; in this case, a backslash (\).

For example, if you enclose your passphrases in single quotation marks and you want to use

I can't believe it's not butter

as your passphrase, you would have to enter it as

'I can\'t believe it\'s not butter'

on the command line. You need the quotation marks at the beginning and end for the spaces and you need to escape each single quotation mark used in the passphrase with a backslash.

Note: If you are having problems entering certain characters in your passphrases, check the information about how to handle reserved characters for the operating system or shell interpreter you are using.

3 Licensing

This section describes how to license PGP Whole Disk Encryption Command Line.

In This Chapter

Overview 13
–license-authorize 13
Licensing via a Proxy Server 14

Overview

PGP Whole Disk Encryption Command Line requires a valid license to operate. This section describes how to license PGP Whole Disk Encryption Command Line if it is currently unlicensed or if you want to change to a different license.

PGP Whole Disk Encryption Command Line supports the following licensing scenarios:

- Using a License Number. This is the normal method to license PGP Whole Disk Encryption Command Line. You must have your license information and a working connection to the Internet.
- Through a Proxy Server. If you connect to the Internet through a proxy server, use this method to license PGP Whole Disk Encryption Command Line. You must have your license information and the appropriate proxy server information.

The licensing command is `--license-authorize`.

Once PGP Whole Disk Encryption Command Line is correctly installed and licensed on your system, you can encrypt your drive.

--license-authorize

Use `--license-authorize` to license PGP Whole Disk Encryption Command Line.

The usage format is:

```
pgpwde --license-authorize --license-name <name> --
license-number <number> [--license-email <emailaddress>]
[--license-organization <org>]
```

Where:

- `--license-authorize` is the command to license PGP Whole Disk Encryption Command Line.
- `--license-name` is the option to specify the user.

  `<name>` is your name or a descriptive name.
- `--license-number` is the option to enter a license number.

  `<number>` is a valid license number for PGP Whole Disk Encryption Command Line.
- `--license-email` is the option to enter an email address.

  `<emailaddress>` is a valid email address.
- `--license-organization` is the option to enter an organization.

  `<org>` is the name of your organization.

If you decide not to enter a license email, you may see a warning message but your license will authorize.

Example:

```
pgpwde --license-authorize --license-name "Alice
Cameron"
--license-number "aaaaa-bbbbb-ccccc-ddddd-eeeee-fff"
--license-email "acameron@example.com"
--license-organization "Example Corporation"
```

(When entering this text, it all goes on a single line.)

Licensing via a Proxy Server

If the Internet access of the system hosting PGP Whole Disk Encryption Command Line is via an HTTP proxy connection, you can still license PGP Whole Disk Encryption Command Line directly; you simply need to add the necessary proxy information.

Use `--license-authorize` to license PGP Whole Disk Encryption Command Line via a proxy server.

The usage format is:

```
pgpwde --license-authorize --license-name <name>
--license-number <number> [--license-email
<emailaddress>] [--license-organization <org>] [--proxy-
server <proxyserver>] [--proxy-username <proxyusername>]
[--proxy-passphrase <proxypass>]
```

Where:

- `--license-authorize` is the command to license PGP Whole Disk Encryption Command Line.
- `--license-name` is the option to specify the user.

  `<name>` is your name or a descriptive name.
- `--license-number` is the option to enter a license number.

  `<number>` is a valid license number for PGP Whole Disk Encryption Command Line.
- `--license-email` is the option to enter an email address.

  `<emailaddress>` is a valid email address.
- `--license-organization` is the option to enter an organization.

  `<org>` is the name of your organization.
- `--proxy-server` is the command to go through a proxy server to access the Internet.

  `<proxyserver>` is the appropriate proxy server.
- `--proxy-username` is the command to specify a user on the proxy server when authentication is required.

  `<proxyusername>` is a valid username on the specified proxy server.
- `--proxy-passphrase` is the option to specify the passphrase of the specified user when authentication is required.

  `<proxypass>` is the passphrase for the specified user on the proxy server.

Example:

```
pgpwde --license-authorize --license-name "Alice
Cameron"
--license-number "aaaaa-bbbbb-ccccc-ddddd-eeeee-fff"
--license-email "acameron@example.com"
--license-organization "Example Corporation"
--proxy-server "proxyserver.example.com"
--proxy-username "acameron"
--proxy-passphrase 'a_cameron1492sailedblue'
```

(When entering this text, it all goes on a single line.)

4 Generic Commands

PGP Whole Disk Encryption Command Line generic commands are:

- `--help (-h)`, which shows basic help information for PGP Whole Disk Encryption Command Line.
- `--version`, which shows version information for PGP Whole Disk Encryption Command Line.

In This Chapter

–help (-h) 17
–version 18

--help (-h)

The `--help` command provides a brief description of the commands and options available in PGP Whole Disk Encryption Command Line.

The long form usage format is:

```
pgpwde --help
```

The short form usage format is:

```
pgpwde -h
```

Example:

```
pgpwde --help
PGP WDE command line tool.
Commands:
   Generic:
-h  --help        this help message
    --version     show version information
```

and so on.

This example shows the response to the `--help` command.

--version

The `--version` command displays information about the version of PGP Whole Disk Encryption Command Line you are using.

The usage format is:

```
pgpwde --version
```

Example:

```
pgpwde --version
PGP WDE, Version 10.0.0
Copyright (C) 2010 PGP Corporation
```

This example shows the response to the `--version` command.

5 Disk Information Commands

PGP Whole Disk Encryption Command Line includes several commands that provide information about the disks on a system and their status:

- `--enum`: Tells you about the disks on the system, including disk designation.
- `--status`: Gives you PGP WDE information about a disk on the system.
- `--show-config`: Gives you PGP BootGuard information about a disk on the system.
- `--info`: Gives you general information about a disk on the system.

In This Chapter

–enum 19
–info 20
–show-config 21
–status 22

--enum

The `--enum` command displays disk designations (for example, Disk 0 as the boot disk), which is used in other PGP Whole Disk Encryption Command Line commands.

The usage format is:

```
pgpwde --enum
```

Where:

`--enum` displays information about the disks on your system.

Examples:

- `pgpwde --enum`

```
Total number of installed fixed/removable storage
device (excluding floppy and CDROM): 1

Disk 0 has 1 online volumes:
```

volume C is on partition 2 with offset 80325

Enumerate disks completed

This example shows that the system has one disk, Disk 0, which is drive letter C and is the boot disk. Drive 0 is the boot disk in most cases on Windows and Mac OS X systems.

- `pgpwde --enum`

Total number of installed fixed/removable storage
device (excluding floppy and CDROM): 2

Disk 0 has 1 online volumes:

volume C is on partition 2 with offset 80325

Disk 1 has 1 online volumes:

volume F is on partition 1 with offset 245

Enumerate disks completed

This example shows information for the boot disk and a USB token on the system; the token is Disk 1 and drive letter F.

You can find out more information about the disks on your Windows system in the Disk Management section of the Computer Management tool (compmgmt.msc). You can find out more information about the disks on your Mac OS X system using the Disk Utility application (/Applications/Utilities/Disk Utility).

--info

The `--info` command provides general status information for the specified disk.

Use the `--status` command for PGP WDE-specific information about a disk.

Information you can see about a disk using `--info` includes:

- model information.
- total number of sectors on the disk.

The usage format is:

```
pgpwde --info --disk <number>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.

Examples:

- `pgpwde --info --disk 0`

  ```
  Disk information for disk disk 0.
  Model Number: ST910021AS
  Total number of sectors on disk: 192426569
  Display disk information completed
  ```

  This example shows the model number and sectors for a boot disk.

- `pgpwde --info --disk 1`

  ```
  Disk information for disk 1.
     Model Number: SanDisk U3 Titanium USB 2.18
     Total number of sectors on disk: 4001425
  Display disk information completed
  ```

  This example shows the model number and sectors for a USB thumb drive.

--show-config

The `--show-config` command displays information about how PGP BootGuard is configured on an encrypted disk.

No information displays if the command is run on a disk that is not encrypted by PGP WDE.

The usage format is:

```
pgpwde --show-config --disk <number>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.

Examples:

- `pgpwde --show-config --disk 0`

  ```
           Login Message:
  Display Startup Screen: No
       Use Audio Prompts: No
            User lockout: Disabled
      Allow user decrypt: Yes
  Show configuration information completed
  ```

  This example shows the PGP BootGuard information for a boot disk that is encrypted.

--status

The `--status` command provides PGP WDE-specific status information for the specified disk.

(Use the `--info` command for general information about a disk.)

Information you can see about a disk using `--status` includes:

- whether or not the disk is instrumented.
- whether or not the disk is whole disk encrypted.
- the number of sectors on the disk.
- the highwater mark (the number of encrypted sectors on the disk).

Note: If you are decrypting a disk, and you want to check progress, you can run `--status` periodically and check the high water mark; this number decreases as the decryption progresses.

The usage format is:

```
pgpwde --status --disk <number>
```

Where:

- `--disk is the option specifying to which disk on the system the information applies.`
- `<number> is the disk number on the system.`

Examples:

- `pgpwde --status --disk 0`

  ```
  Disk disk0 is instrumented by bootguard.
      Current key is valid.
  Whole disk encrypted
     Total sectors: 192426569  highwatermark: 192426569
  Disk status completed
  ```

  In this example, Disk 0 is instrumented by PGP BootGuard, the current key used for authentication is valid, the disk is encrypted, the total number of sectors on the disk is 192426569, and the high water mark (the number of sectors encrypted) is 192426569.

- `pgpwde --status --disk 1`

Disk disk 1 is not instrumented by bootguard.

Disk status completed

In this example, disk 1 is *not* instrumented by PGP BootGuard.

6 User Management Commands

The user management commands are:

- `--add-user`: Adds user to disk or group.
- `--change-passphrase`: Changes passphrase of specified user or group.
- `--change-userdomain`: Changes authentication domain of specified user or group.
- `--list-user`: Lists authorized users on an encrypted disk.
- `--offload`: Offloads passphrase user information onto specified device.
- `--remove-user`: Removes user from specified disk or group.
- `--verify-user`: Verifies passphrase of user or group.

In This Chapter

–add-user 23
–change-passphrase 25
–change-userdomain 25
–list-user 26
–offload 27
–remove-user 27
–verify-user 28

--add-user

The `--add-user` command adds an authorized user to the encrypted disk.

The usage format is:

```
pgpwde --add-user --disk <number> --domain-name <domain>
--sso --passphrase <phrase> --username <user> --admin-
authorization | --admin-passphrase <pass> | --recovery-
token <string>
```

Where:

- `--disk` specifies the disk to which the operation applies.

- `<number>` is the disk number on the system.
- `--username` specifies a username for an operation.
- `<user>` is the username of the user being added.
- `--domain-name` specifies the name of the domain to which the user authenticates. The default is the login domain.
- `<domain>` is the domain to which the user authenticates.
- `--sso` specifies to create the user as a single sign-on (SSO) user, which means that the Windows passphrase for logging in to the disk will also be automatically used to authenticate to the encrypted disk.
- `--passphrase` specifies the passphrase for an operation.
- `<pass>` is the passphrase the user being added will use to authenticate.
- `--username` specifies a username for an operation.
- `<user>` is the username of the user being added.
- `--admin-authorization` specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.
- `--admin-passphrase` specifies that the passphrase of an authorized user on the encrypted disk will be used to authenticate the adding of the new user account.
- `<phrase>` is the passphrase of an authorized user on the disk.
- `--recovery-token` specifies that the disk's recovery token (WDRT) will be used for authentication.
- `<string>` is the WDRT string.

Example:

- ```
  pgpwde --add-user --disk 0 --username "Alice Cameron"
  --passphrase 'Frodo@Baggins22' --admin-passphrase
  'Sam&Gamgee44'

  Add user completed
  ```

  This example shows a new passphrase user, Alice Cameron, being added to a boot disk with a passphrase of Frodo@Baggins22. The passphrase (Sam&Gamgee44) of an existing user on the disk is used to authenticate.

- ```
  pgpwde --add-user --disk 0 --sso --username "Alice
  Cameron" --domain EXAMPLECORP --passphrase
  'Frodo@Baggins22' --admin-authorization

  Add user completed
  ```

  This example shows a new SSO user, in domain EXAMPLECORP, being added to a boot disk by a member of the WDE-ADMIN Active Directory group.

--change-passphrase

The `--change-passphrase` command lets you change the passphrase of a passphrase user on an encrypted disk.

The usage format is:

```
pgpwde --change-passphrase --disk <number> --username
<user> --new-passphrase <newpass> --passphrase <phrase>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--username` specifies the existing user whose passphrase is being changed.
- `<user>` is the username of the existing user whose passphrase is being changed.
- `--new-passphrase` specifies that you are changing an existing passphrase to a new passphrase.
- `<newpass>` is the text of the new passphrase.
- `--passphrase` specifies the existing passphrase.
- `<phrase>` is the passphrase that is being changed.

Example:

- `pgpwde --change-passphrase --disk 0 --username "Alice Cameron" --new-passphrase 'Sam&Gamgee44' --passphrase 'Frodo@Baggins22'`

  This example shows an existing passphrase user on an encrypted disk changing their passphrase.

--change-userdomain

The `--change-userdomain` command lets you change the user domain to which an authorized user authenticates.

This command is useful for organizations going through a domain migration.

The usage format is:

```
pgpwde --change-userdomain --disk <number> --new-domain
<domain> --username <user>
```

Where:

- `--disk` specifies the disk to which the operation applies.

- <number> is the disk number on the system.
- --new-domain specifies the new domain to which the user will authenticate.
- <domain> is the name of the new authentication domain.
- --username specifies a username for the operation.
- <user> is the username of an existing user who is being removed.

Example:

- pgpwde --change-userdomain --disk 0 --new-domain EXAMPLECORP --username "Alice Cameron"

  Domain change completed

  This example shows the authentication domain of user Alice Cameron being changed to EXAMPLECORP.

--list-user

The --list-users command lists those users who are authorized users on the specified encrypted disk.

The usage format is:

```
pgpwde --list-users --disk <number>
```

Where:

- --disk specifies the disk to which the operation applies.
- <number> is the disk number on the system.

Example:

- pgpwde --list-users --disk 0

  ```
  Total of 1 users:
      User 0: Name: Alice Cameron Type: Symmetric-SSO
  domain: EXAMPLECORP
  System Record Information:
     Serial Number: 1
           Disk ID: EXAMPLECORP.MSHOME.Alice Cameron.
         Disk UUID: 32eca196-7d16-4f83-9159-f7228af85594
        Group UUID: 32eca196-7d16-4f83-9159-f7228af85594
  List users on disk completed
  ```

  This example shows the users who can authenticate to the specified boot disk.

--offload

The `--offload` command offloads passphrase user information to a two-factor device, such as a USB thumb drive.

After adding the two-factor device to the system, you can determine its disk number using the `--enum` command.

The usage format is:

```
pgpwde --offload --target <target> --passphrase <phrase>
[--interactive]
```

Where:

- `--target` specifies the target disk for the user information (the source disk is the boot disk).
- `<target>` is the disk number of the two-factor device on the system.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase of an authorized user on the encrypted disk.
- `--interactive` specifies that a passphrase be prompted for instead of entered on the command line.

Example:

- `pgpwde --offload --disk 2 --passphrase 'Frodo@Baggins22'`

  This example shows user information being offloaded from the boot disk to a two-factor device that is disk 2 on the system.

--remove-user

The `--remove-user` command removes a user who is currently authorized on the encrypted disk.

The usage format is:

```
pgpwde --remove-user --disk <number> --username <user>
--admin-authorization | --admin-passphrase <pass>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--username` specifies a username for the operation.
- `<user>` is the username of an existing user who is being removed.

--admin-authorization specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.

- `--admin-passphrase` specifies that the passphrase of an authorized user on the encrypted disk will be used to authenticate the removal of the user.
- `<phrase>` is the passphrase of an authorized user on the disk.

Example:

- `pgpwde --remove-user --disk 0 --username "Alice Cameron" --admin-authorization`

  `Remove user completed`

  This example shows user Alice Cameron being removed from the boot disk by a member of the WDE-ADMIN Active Directory group.

--verify-user

The `--verify-user` command verifies the passphrase of a user who is an authorized user of an encrypted disk.

The usage format is:

```
pgpwde --verify-user --disk <number> --passphrase
<phrase> --username <user> | --keyid <keyid>
```

Where:

- `--disk` specifies to which disk on the system the information applies.
- `<number>` is the disk number on the system.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase of an authorized user on the disk.
- `--username` specifies a username for an operation.
- `<user>` is the username of an authorized user account on the disk.
- `--keyid` specifies a user by key ID for an operation.
- `<keyid>` is the key ID of an authorized user on the disk.

Example:

- `pgpwde --verify-user --disk 0 --passphrase 'Frodo@Baggins44' --username "Alice Cameron"`

  `Successfully verified user Alice Cameron`

  This example shows passphrase user Alice Cameron's passphrase being verified via her username.

- `pgpwde --verify-user --disk 0 --passphrase 'Frodo@Baggins44' --keyid 0x12345678`

  ```
  Successfully verified user Alice Cameron
  ```

  This example shows PGP key user Alice Cameron's passphrase being verified via the key ID of her PGP key.

7 Disk Management

The disk management commands are:

- `--auth`: Lets you authenticate to an encrypted disk.
- `--instrument`: Installs PGP WDE configuration information on specified disk.
- `--uninstrument`: Removes WDE configuration from specified disk.

In This Chapter

–auth 31
–instrument 32
–uninstrument 32

--auth

The `--auth` command lets you authenticate to an encrypted disk.

In most cases, if a disk needs authentication, the user will be prompted to authenticate to the disk by pgptray. If pgptray is not running, you can use `--auth` to authenticate.

The usage format is:

```
pgpwde --auth --disk <number> --passphrase <phrase>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase of an authorized user on the disk.

Example:

- `pgpwde --auth --disk 0 --passphrase 'Sam&Gamgee44'`

  This example shows a user on an encrypted disk authenticating to the boot disk, disk 0.

--instrument

The `--instrument` command replaces the Windows or Mac OS X MBR with the PGPMBR.

Instrumenting the disk or partition is the first step in the process of securing a disk; it is followed by adding a passphrase user and then encrypting the disk. These three actions can be done individually, in that order, or all at once using the `--secure` command.

The usage format is:

```
pgpwde --instrument --disk <number>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.

Example:

- `pgpwde --instrument --disk 0`

  This example shows a boot disk being instrumented.

--uninstrument

The `--uninstrument` command replaces the PGPMBR with the original (saved) Windows or Mac OS X MBR. The removes the requirement to authenticate at the PGP BootGuard screen when starting the system.

Uninstrumenting a disk is normally done as part of the decryption process, so this command is not normally used on its own.

Caution: You can only uninstrument a disk that has been instrumented but nothing else. You cannot uninstrument an encrypted disk.

The usage format is:

```
pgpwde --uninstrument --disk <number>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.

Example:

- `pgpwde --uninstrument --disk 0`

  This example shows a boot disk being uninstrumented.

8 Disk Operation

The disk operation commands are:

- `--decrypt`: Decrypts the specified disk.
- `--encrypt`: Encrypts the specified disk.
- `--resume`: Resumes a halted encrypt or decrypt process.
- `--secure:` Encrypts a disk to a specified user and passphrase.
- `--stop`: Halts an encrypt or decrypt process.

In This Chapter

–decrypt 33
–encrypt 34
–resume 35
–secure 35
–stop 36

--decrypt

The `--decrypt` command starts the process of decrypting an encrypted disk.

If the disk is still being encrypted, you need to stop the encryption process using `--stop` before you can begin to decrypt it.

Note: If you are decrypting a disk, and you want to check progress, you can run `--disk-status` periodically and check the high water mark; this number decreases as the decryption progresses.

The usage format is:

```
pgpwde --decrypt --disk <number> --admin-authorization |
--passphrase <phrase> --all --partition <partnumber>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.

- `--admin-authorization` specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase of an authorized user on the disk.
- `--all` specifies that all partitions should be decrypted.
- `--partition` specifies that only the listed partition should be decrypted.
- `<partnumber>` is the partition to be decrypted.

Examples:

- `pgpwde --decrypt --disk 0 --passphrase 'Frodo*1*Baggins22'`

  This example shows a boot disk being decrypted.

--encrypt

The `--encrypt` command begins the process of whole disk encrypting a disk.

Once the encryption process has started, you can stop it using `--stop`.

Three options are available for encrypting:

- `--dedicated-mode`: Uses maximum computer power to encrypt faster; your system is less responsive during encryption.
- `--fast-mode`: Skips unused sectors, so encryption of the disk is faster.
- `--safe-mode`: Allows encryption to be resumed without loss of data if power is lost during encryption; encryption takes longer.

The usage format is:

```
pgpwde --encrypt --disk <number> --passphrase <phrase> |
--keyid <keyid> --all --partition <partnumber>
--dedicated-mode --fast-mode --safe-mode
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase of an authorized user on the disk.
- `--keyid` specifies a user by key ID for an operation.
- `<keyid>` is the key ID of an authorized user on the disk.
- `--all` specifies that all partitions should be decrypted.
- `--partition` specifies that only the listed partition should be encrypted.

- `<partnumber>` is the partition to be encrypted.
- `--dedicated-mode` specifies that dedicated mode (uses maximum computer power to encrypt faster) be used in the encryption process.
- `--fast-mode` specifies that fast mode (skipping unused sectors) be used in the encryption process.
- `--safe-mode` specifies that safe mode (encryption can be resumed without loss of data if power is lost) be used in the encryption process.

Example:

- `pgpwde --encrypt --disk 0 --passphrase 'Frodo*1*Baggins22' --fast-mode --all`

  This example shows encryption of a boot disk being started using fast mode. Authentication is provided by a authorized passphrase user; all partitions are to be encrypted.

--resume

The `--resume` command resumes a stopped process, either encrypting or decrypting a disk.

The usage format is:

```
pgpwde --resume --disk <number> --passphrase <phrase>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase of an authorized user on the disk.

Example:

- `pgpwde --resume --disk 0 --passphrase 'Frodo@Baggins44'`

  This example shows encryption being resumed on a boot disk.

--secure

The `--secure` command encrypts a disk to a specified user and passphrase. In essence, it does three things that can also be done separately: it instruments the disk, adds a passphrase user, and encrypts the disk.

The usage format is:

```
pgpwde --secure --disk <number> --username <name>
--passphrase <phrase> --keyid <keyid> --all --partition
<partnumber> --dedicated --fast --safe
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase of an authorized user on the disk.
- `--keyid` specifies a user by key ID for an operation.
- `<keyid>` is the key ID of an authorized user on the disk.
- `--all` specifies that all partitions should be decrypted.
- `--partition` specifies that only the listed partition should be encrypted.
- `<partnumber>` is the partition to be encrypted.
- `--dedicated-mode` specifies that dedicated mode (uses maximum computer power to encrypt faster) be used in the encryption process.
- `--fast-mode` specifies that fast mode (skipping unused sectors) be used in the encryption process.
- `--safe-mode` specifies that safe mode (encryption can be resumed without loss of data if power is lost) be used in the encryption process.

Example:

- `pgpwde --secure --disk 0 --username "Alice Cameron" --passphrase 'Frodo*1*Baggins22' --all --fast-mode`

  This example shows a boot disk being secured (instrumented and encrypted, with a new passphrase user).

--stop

The `--stop` command stops the current process, either encrypting or decrypting a disk.

The usage format is:

```
pgpwde --stop --disk <number>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.

Example:

- `pgpwde --stop --disk 0`

  This example shows the encryption or decryption process on disk 0 being stopped.

9 Boot Bypass Commands

The Boot Bypass feature lets you reboot a system one time without having to authenticate at the PGP BootGuard screen.

Boot Bypass can be set for boot disks only.

Boot Bypass is generally used for remote deployment or upgrade scenarios when a reboot is required; patch management, for example.

The Boot Bypass commands are:

- `--add-bypass`: Enables the specified disk for Boot Bypass.
- `--check-bypass`: Checks to see if the specified disk is enabled for Boot Bypass.
- `--remove-bypass`: Removes Boot Bypass from a disk where it is enabled.

In This Chapter

--add-bypass 39
--check-bypass 40
--remove-bypass 41

--add-bypass

The `--add-bypass` command enables a system for Boot Bypass, a one-time-only bypass of the PGP BootGuard screen.

The usage format is:

```
pgpwde --add-bypass --disk <number> --admin-
authorization | --admin-passphrase <phrase>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--admin-authorization` specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.

- `--admin-passphrase` specifies that the passphrase of an authorized user on the encrypted disk will be used to authenticate.
- `<phrase>` is the passphrase of an authorized user on the disk.

Example:

- `pgpwde --add-bypass --disk 0 --admin-passphrase 'bilbo@baggins42'`

  `Add bypass completed`

  This example shows that Boot Bypass was added to the boot disk on a system using the passphrase of an authorized user on the disk.

--check-bypass

The `--check-bypass` command tells you if Boot Bypass is configured for the specified disk.

The usage format is:

```
pgpwde -check-bypass --disk <number> --admin-
authorization | --admin-passphrase <phrase>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--admin-authorization` specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.
- `--admin-passphrase` specifies that the passphrase of an authorized user on the encrypted disk will be used to authenticate.
- `<phrase>` is the passphrase of an authorized user on the disk.

Examples:

- `pgpwde --check-bypass --disk 0 --admin-passphrase 'bilbo@baggins42'`

  `Successfully verified Bypass User`

  This example shows that Disk 0 is configured for Boot Bypass via the presence of the "Bypass User."

- `pgpwde --check-bypass --disk 0 --admin-passphrase 'bilbo@baggins42'`

  `No Bypass User configured`

  This example shows that Disk 0 is **not** configured for Boot Bypass.

--remove-bypass

The `--remove-bypass` command removes Boot Bypass for the specified disk.

The usage format is:

```
pgpwde --remove-bypass --disk <number> --admin-
authorization | --admin-passphrase <phrase>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--admin-authorization` specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.
- `--admin-passphrase` specifies that the passphrase of an authorized user on the encrypted disk will be used to authenticate.
- `<phrase>` is the passphrase of an authorized user on the disk.

Example:

- `pgpwde --remove-bypass --disk 0 --admin-passphrase 'bilbo@baggins42'`

  `Remove bypass completed`

  This example shows the removal of Boot Bypass from a disk.

10 Recovery Token Commands

In PGP Universal-managed environments with the appropriate policy, Whole Disk Recovery Tokens (WDRTs) are created automatically when a disk, partition, or removable disk is whole disk encrypted. They are sent to the PGP Universal Server managing security for the disk or partition when they are created.

WDRTs can be used to access the disk or partition in case the passphrase or authentication token is lost.

Once a WDRT is used, it cannot be used again. A new WDRT must be generated for the system. All new WDRTs are also automatically sent to the PGP Universal Server managing the disk when the new WDRT is created.

Because the first WDRT for a system is created automatically, the only command related to WDRTs is to create a new WDRT.

The recovery token commands are:

- `--new-wdrt`: Creates a new WDRT after use.

In This Chapter

–new-wdrt.....43

--new-wdrt

The `--new-wdrt` command creates a new WDRT (recovery token) when the previous WDRT has been used.

The usage format is:

```
pgpwde --new-wdrt --disk <number> --admin-authorization
| --admin-passphrase <phrase> --recovery-token <string>
```

Where:

- –new-wdrt specifies the creation of a new WDRT.
- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--admin-authorization` specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.

- `--admin-passphrase` specifies that the passphrase of an authorized user on the encrypted disk will be used to authenticate the adding of the new user account.
- `<phrase>` is the passphrase of an authorized user on the disk.
- `--recovery-token` specifies that a recovery token (WDRT) will be created to replace the used one.
- `<string>` is the WDRT string.

Example:

- ```
  pgpwde --new-wdrt --disk 0 --admin-passphrase
  'bilbo@baggins44' --recovery-token 'Gandalf-
  Bilbo+Merry=OneRing'

  Create a new WDRT completed
  ```

  This example shows a new WDRT (recovery token) being created.
  ```

11 PGP BootGuard Customization Commands

PGP WDE Command Line includes commands for modifying the default PGP BootGuard screen.

The PGP BootGuard customization commands are:

- `--set-background`: Lets you specify a custom PGP BootGuard screen background.
- `--set-language`: Lets you specify a language for the PGP BootGuard display and keyboard.
- `--set-sound`: Enables or disables audio prompts on the PGP BootGuard screen.
- `--set-start`: Lets you specify a custom PGP BootGuard startup screen background.
- `--set-text`: Lets you specify a text message for the PGP BootGuard authentication screen.

In This Chapter

--set-background 45
--set-language 46
--set-sound 47
--set-start 48
--set-text 49

--set-background

The `--set-background` command lets you specify a custom background image for the PGP BootGuard authentication screen.

Custom background images must be created according to the following specifications:

- XPM files only.
- Image size of 640 by 480.

- Palette of 15 colors only, including black (one color is reserved for fonts). You do not have to use all 15 colors in the image.
- 8-bit RGB only (cannot be 16-bit RGB). You can verify you are using 8 bit by looking at the XPM header using a text editor: 8-bit values appear as #285A83 (one hex triplet), 16-bit values appears as #28285A5A8383 (two hex triplets).

Note: If you specify an image that does not meet these requirements, a default text-only screen will be used.

Graphics applications that support the XPM file format include Graphic Converter on Mac OS X, GIMP on Mac OS X/FreeBSD and UNIX/LINUX, and the Convert command on Linux.

The new background image will display when the PGP BootGuard authentication screen next appears.

The usage format is:

```
pgpwde --set-background --disk <number> --image <file>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--image` specifies the image file to use as the custom background.
- `<file>` is the name of the XPM file.

Example:

- `pgpwde --set-background --disk 0 --image "corplogo.xpm"`

  `Background Image Updated`

  `Set custom background image completed`

  This example shows an image file, corplogo.xpm, being set as the background image for the PGP BootGuard authentication screen.

--set-language

The `--set-language` command lets you specify the languages that will be used by PGP BootGuard for display and for the keyboard.

You can specify one language and one display from the list of supported languages. You are not required to use the same language for both.

Options not specified are not changed. So if you specify a new language for text, the existing keyboard setting is not changed. The response to the –set-language command shows both the previous settings and the new settings, for both display and keyboard.

Changes will take effect on the next system startup.

The usage format is:

```
pgpwde --set-language --disk <number> --display <view>
--keyboard <type>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--display` specifies the language to be used for viewing.
- `<view>` is desired language ID for the display: **default** (keep existing language), **de**, **en**, **es**, **fr**, or **jp**.
- `--keyboard` specifies the language to be used for typing text.
- `<type>` is the desired language for the keyboard: **default** (keep existing language), **de**, **en**, **en-gb**, **es**, **fr**, or **jp**.

Example:

- `pgpwde --set-language --disk 0 --display jp --keyboard jp`

  ```
  Boot language is set to Keyboard=en   Display=en

  Boot language now set to Keyboard=jp  Display=en
  ```

  This example shows Japanese being specified for both display and keyboard in PGP BootGuard.

--set-sound

The `--set-sound` command lets you enable or disable the use of audio clues for actions that occur during the PGP BootGuard authentication process. Audio clues are disabled by default.

Audio clues can help vision-impaired users more easily navigate the PGP BootGuard authentication process.

When enabled, the system will play audible tone combinations during the PGP BootGuard authentication process. Each tone combination begins with a middle sound and is followed by either a higher tone, another middle tone, or a lower tone.

The three combinations are:

- **Ready for passphrase/pin entry:** When the system is first ready for passphrase/pin entry, the middle-middle tone combination plays.
- **Successful authentication:** If the authentication attempt was successful, the middle-high tone combination plays. The system then continues booting.

- **Unsuccessful authentication:** If the authentication attempt was unsuccessful, the middle-low tone combination plays. The PGP BootGuard authentication screen displays and the passphrase field is cleared for another authentication attempt.

The tone combinations cannot be customized; you can only decide whether to enable audio clues or disable them.

Changes will take effect on the next system startup.

The usage format is:

```
pgpwde --set-sound --disk <number> --beep | --no-beep
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--beep` enables audio clues.
- `--no-beep` disables audio clues.

Example:

- `pgpwde --set-sound --disk 0 --beep`

  `Accessibility Sounds set to [ON]`

  This example shows audio clues being enabled.

--set-start

The `--set-start` command lets you display a custom startup image for PGP BootGuard that appears *before* the authentication screen. Press any key to make the startup screen disappear.

Custom startup images must be created according to the following specifications:

- XPM files only.
- Image size of 640 by 480.
- Palette of 15 colors only, including black (one color is reserved for fonts). You do not have to use all 15 colors in the image.
- 8-bit RGB only (cannot be 16-bit RGB). You can verify you are using 8 bit by looking at the XPM header using a text editor: 8-bit values appear as #285A83 (one hex triplet), 16-bit values appears as #28285A5A8383 (two hex triplets).

Graphics applications that support the XPM file format include Graphic Converter on Mac OS X, GIMP on Mac OS X/FreeBSD and UNIX/LINUX, and the Convert command on Linux.

The new startup image will display on the next system startup (unless Boot Bypass is used).

The usage format is:

```
pgpwde --set-start --disk <number> --image <file>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--image` specifies the image file to use as the startup screen.
- `<file>` is the name of the XPM file.

Example:

- `pgpwde --set-start --disk 0 --image "corpsplash.xpm"`

  `Start Image Updated`

  `Set custom startup image completed`

  This example shows an image file, corpsplash.xpm, being set as the PGP BootGuard startup image.

--set-text

The `--set-text` command lets you specify text that will display when the PGP BootGuard screen appears.

You can disable the display of text by entering no text where the message would go.

You can enter one line of text, up to 80 characters (including spaces). The default text is: "Forgot your passphrase? Please contact your IT department or Security Administrator."

Note: Text must go in quotation marks or only the text up to the first space will display. The quotation marks do not display.

Changes will take effect on the next system startup.

The usage format is:

```
pgpwde --set-text --disk <number> --message <text>
```

Where:

- `--disk` specifies the disk to which the operation applies.
- `<number>` is the disk number on the system.
- `--message` specifies new text for the PGP BootGuard screen.
- `<text>` is the text you want to display. If left empty, no text will display.

Examples:

- `pgpwde --set-text --disk 0 --message "You must change your login passphrase monthly."`

  ```
  Custom message Updated

  Set custom authentication screen text completed
  ```

  This example shows a new text message for the PGP BootGuard screen.

- `pgpwde --set-text --disk 0 --message`

  ```
  Custom message Updated

  Set custom authentication screen text completed
  ```

  This example shows the display of text for the PGP BootGuard screen being disabled.

12 Local Self Recovery

Local self recovery lets you authenticate to PGP BootGuard even if you have forgotten your passphrase.

Note: Local self recovery only works if you configure it *before* you lose your passphrase; PGP Corporation recommends configuring it immediately after licensing PGP Whole Disk Encryption Command Line if you plan on using it.

When you configure local self recovery, you create five security questions; three must be answered correctly to authenticate to PGP BootGuard.

Note: If you are using PGP Whole Disk Encryption Command Line in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled the option for local self recovery. Your administrator may also have specified that local self recovery be configured during enrollment. In this case, you are prompted to enter the security questions as as you set up PGP Whole Disk Encryption Command Line.

The local self recovery commands are:

- `--recovery-configure`: Configures the local self recovery feature.
- `--recovery-questions`: Displays local self recovery questions.
- `--recovery-verify`: Verifies existing local self recovery questions and answers.
- `--recovery-remove`: Removes existing local self recovery questions and answers.
- `--recovery-change-passphrase`: Changes a forgotten passphrase.

How to authenticate to PGP BootGuard if you have forgotten your passphrase, but you configured local self recovery, is described in Authenticating if you have Forgotten Your Passphrase.

In This Chapter

--recovery-configure 52
--recovery-questions 53
--recovery-verify 54
--recovery-remove 55
--recovery-change-passphrase 55
Authenticating if you Have Forgotten Your Passphrase 56

--recovery-configure

The `--recovery-configure` command configures local self recovery.

You can configure the required five questions and answers in either of two ways:

- **text files:** you create two text files; one text file with five questions, each on separate lines, and a second text file with five answers to those questions, again each on a separate line.
- **interactively** (`--interactive`): You will be prompted for five questions and their corresponding answers.

You can also use `--interactive` to have PGP Whole Disk Encryption Command Line interactively prompt for a passphrase. To do this, use `--interactive` on the command line instead of `--passphrase` and the passphrase.

Note: Text files and `--interactive` are mutually exclusive. Use one method or the other.

You will need to be able to correctly answer three of the five questions if you forget your passphrase and need to authenticate to PGP BootGuard using `--recovery-verify`.

The usage format is:

```
pgpwde --recovery-configure --user <username>
--passphrase <phrase> [--disk <disknumber>]
[--questions-file <questions>] [--answers-file
<answers>] [--interactive]
```

Where:

- `--recovery-configure` specifies that you are configuring local self recovery.
- `--user` specifies which user account is being used.
- `<username>` is the name of the user account.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase for specified user account.
- `--disk` specifies disk on the system for which local self recovery is being configured.
- `<disknumber>` is the disk number on the system. Disk 0, the boot disk, is the default.
- `--questions-file` specifies the five questions will be in a text file.
- `<questions>` is the path to the text file with the five questions, each on its own line.

- `--answers-file` specifies the five answers will be in a text file.
- `<answers>` is the path to the text file with the five answers, each on its own line.
- `--interactive` specifies you will be prompted for the five questions and answers.

Examples:

- ```
  pgpwde --recovery-configure --user "Alice Cameron"
  --passphrase 'bilbo#baggins+Frodo' --disk 0
  --interactive
  ```

  This example shows local self recovery being configured for user Alice Cameron using interactive questions and answers.

- ```
  pgpwde --recovery-configure --user "Alice Cameron"
  --passphrase 'bilbo#baggins+Frodo' --disk 0 --questions-
  file "C:\pgpwde\questions.txt" --answers-file
  "C:\pgpwde\answers.txt"
  ```

  This example shows local self recovery being configured for user Alice Cameron with the five questions and answers in the specified text files on a Windows system.

--recovery-questions

The `--recovery-questions` command displays *configured* local self recovery questions.

Note: `--recovery-questions` only shows existing questions. You cannot modify or add questions using this command.

The usage format is:

```
pgpwde --recovery-questions --user <username>
[--disk <disknumber>]
```

Where:

- `--recovery-questions` specifies that you are configuring local self recovery.
- `--user` specifies which user account is being used.
- `<username>` is the name of the user account.
- `--disk` specifies disk on the system for which local self recovery is being configured.
- `<disknumber>` is the disk number on the system. Disk 0, the boot disk, is the default.

Example:

- `pgpwde --recovery-questions --user "Alice Cameron" --disk 0`

  This example displays the configured local self recovery questions for user Alice Cameron.

--recovery-verify

The `--recovery-verify` command lets you verify the configured local self recovery questions and answers. You can answer the five questions either using a text file or interactively.

Note: You cannot modify the local self recovery questions using `--recovery-verify`.

To authenticate to PGP BootGuard using the configured local self recovery questions and answers, see Recovering a Lost Passphrase.

The usage format is:

```
pgpwde --recovery-verify --user <username> [--disk <disknumber>] [--answers-file <answers>] [--interactive]
```

Where:

- `--recovery-verify` specifies that you are verifying existing local self recovery questions and answers.
- `--user` specifies which user account is being used.
- `<username>` is the name of the user account.
- `--disk` specifies the disk on the system for which the command is being performed.
- `<disknumber>` is the disk number on the system. Disk 0, the boot disk, is the default.
- `--answers-file` specifies the five answers will be in a text file.
- `<answers>` is the path to the text file with the five answers, each on its own line.
- `--interactive` specifies you will be prompted for the five answers and questions.

Example:

- `pgpwde --recovery-questions --user "Alice Cameron" --disk 0 --answers-file "C:\pgpwde\answers.txt"`

This example shows user Alice Cameron verifying configured local self recovery questions and answers using the file answers.txt on a Windows system.

--recovery-remove

The `--recovery-remove` command removes *configured* local self recovery questions and answers.

The usage format is:

```
pgpwde --recovery-remove --user <username> --passphrase
<phrase> [--disk <disknumber>]
```

Where:

- `--recovery-remove` specifies that you are removing configured local self recovery questions and answers.
- `--user` specifies which user account is being used.
- `<username>` is the name of the user account.
- `--passphrase` specifies the passphrase for an operation.
- `<phrase>` is the passphrase for specified user account.
- `--disk` specifies disk on the system for which local self recovery is being removed.
- `<disknumber>` is the disk number on the system. Disk 0, the boot disk, is the default.

Example:

- `pgpwde --recovery-remove --user "Alice Cameron" --passphrase 'bilbo#baggins+Frodo' --disk 0`

This example removes configured local self recovery questions and answers for user Alice Cameron.

--recovery-change-passphrase

The `--recovery-change-passphrase` command lets you create a new passphrase when you have forgotten your existing passphrase and authenticated to PGP BootGuard using local self recovery.

Note: PGP Corporation recommends creating a new passphrase as soon as you authenticate to PGP BootGuard after forgetting your passphrase and authenticating using local self recovery.

The usage format is:

```
pgpwde --recovery-change-passphrase --user <username>
[--disk <disknumber>] --new-passphrase <newpass>
[--answers-file <answers>]
```

Where:

- `--recovery-verify` specifies that you are authenticating to PGP BootGuard.
- `--user` specifies which user account is being used.
- `<username>` is the name of the user account.
- `--disk` specifies the disk on the system for which the command is being performed.
- `<disknumber>` is the disk number on the system. Disk 0, the boot disk, is the default.
- `--new-passphrase` specifies the five answers will be in a text file.
- `<newpass>` is the path to the text file with the five answers, each on its own line.
- `--answers-file` specifies the five answers will be in a text file.
- `<answers>` is the path to the text file with the five answers, each on its own line.

Example:

- ```
  pgpwde --recovery-change-passphrase --user "Alice
  Cameron" --disk 0 --new-passphrase
  'Bilbo%Baggins$Underhill' --answers-file
  "C:\pgpwde\answers.txt"
  ```

This example shows user Alice Cameron authenticating to PGP BootGuard using the answers in the file answers.txt.

Authenticating if you Have Forgotten Your Passphrase

If you have forgotten your passphrase and cannot authenticate to the PGP BootGuard screen, you can authenticate using local self recovery if you have previously configured it.

Note: Local self recovery *must* be configured in advance.

To authenticate at the PGP BootGuard screen using local self recovery

1. On the PGP BootGuard screen, use the arrow keys to select **Forgot Passphrase** in the lower right corner, then press **Enter**. A new screen appears, showing the first local self recovery question.
2. Enter the answer to the first question, then press **Enter**. The second question appears.
3. Enter the answer to the second question, then press **Enter**. The third question appears.
  ```

4 Enter the answer to the third question, then press **Enter**. The fourth questions appears.

5 Enter the answer to the fourth question, then press **Enter**. The fifth and last question appears.

6 Enter the answer to the fifth question, then press **Enter**.

If you entered three or more of the questions correctly, the PGP BootGuard screen goes away and the system boots normally.

If you did not enter three or more questions correctly, you are given another chance.

If you subsequently remember your original passphrase, you can continue using it. Using local self recovery does not remove your passphrase.

If you do not believe you will ever remember your original passphrase, you can change your passphrase after authenticating to PGP BootGuard using the `--recovery-change-passphrase` command. This means that you do not have to continue using the local self recovery questions to authenticate to PGP BootGuard. Using this command does remove your original passphrase, so it will not work if you remember it later.

13 Options

The PGP Whole Disk Encryption Command Line options are:

- `--admin-authorization`: Specifies that the command is authorized by member of the WDE-ADMIN Active Directory group.
- `--admin-passphrase`: Specifies the passphrase of an existing PGP WDE user.
- `--all`: Specifies the use of partition mode encryption on all partitions.
- `--answers-file:` Specifies the path to a text file with five answers.
- `--auto-start`: Starts encryption immediately.
- `--base-disk`: Specifies the disk number of the original group.
- `--beep`: Enables beep when PGP BootGuard screen appears.
- `--dedicated-mode`: Specifies that dedicated mode be used.
- `--disk (-d)`: Specifies the number of the target disk. Zero (0) is boot disk.
- `--display`: Specifies the PGP BootGuard display language.
- `--domain-name`: Specifies the user authentication domain.
- `--fast-mode`: Specifies that fast mode be used.
- `--image`: Specifies an image file to be used.
- `--interactive:` Specifies passphrases and questions/answers be asked interactively.
- `--keyboard`: Specifies the PGP BootGuard keyboard language.
- `--keyid`: Specifies the key ID of a PGP key.
- `--license-email:` Specifies an email address for the license holder.
- `--license-name:` Specifies the person who whom PGP Whole Disk Encryption Command Line is licensed.
- `--license-number:` Specifies a valid license number for PGP Whole Disk Encryption Command Line.
- `--license-organization:` Specifies an organization for the license holder.
- `--message`: Specifies custom message for PGP BootGuard screen.
- `--new-domain`: Specifies a new domain for a user.
- `--new-passphrase`: Specifies a new passphrase for an existing user.

- `--no-beep`: Disables beep when PGP BootGuard screen appears.
- `--partition`: Specifies a partition for an operation.
- `--passphrase (-p)`: Specifies a passphrase for an operation.
- `--proxy-passphrase:` Specifies the passphrase of the specified user on the proxy server.
- `--proxy-server:` Specifies a proxy server to go through to license PGP Whole Disk Encryption Command Line.
- `--proxy-username:` Specifies a user on the proxy server.
- `--questions-file:` Specifies the path to a text file with five questions.
- `--recovery-token`: Specifies a whole disk recovery token.
- `--safe-mode`: Specifies that safe mode be used.
- `--username (-u)`: Specifies a username for an operation.

In This Chapter

"Secure" Options 62
--admin-authorization 62
--admin-passphrase 62
--all 63
--answers-file 63
--auto-start 63
--beep 63
--dedicated-mode 64
--disk (-d) 64
--display 64
--domain-name 65
--fast-mode 65
--image 65
--interactive 66
--keyboard 66
--keyid 66
--license-email 67
--license-name 67
--license-number 67
--license-organization 68
--message 68
--new-domain 68
--new-passphrase 68
--no-beep 69
--partition 69
--passphrase (-p) 69
--proxy-passphrase 70
--proxy-server 70
--proxy-username 71
--questions-file 71
--recovery-token 72
--safe-mode 72
--sso 72
--username 73
--xml 73

"Secure" Options

The descriptions of some options in PGP Whole Disk Encryption Command Line mention that they are "secure," as in "This option is not secure". In this context, "secure" means that the option's argument is saved in non-pageable memory (when that option is available to applications). Options that are not "secure" are saved in normal system memory.

--admin-authorization

Specifies that the operation is authorized by a member of the WDE-ADMIN Active Directory group. In other words, by an administrator of PGP WDE clients in a PGP Universal-managed environment.

No passphrase is required on the command line when using this option. Instead, the administrator will be authenticated against the WDE-ADMIN group when the option is used.

This option can be shortened to `--aa`.

Example:

- `pgpwde --add-user --disk 0 --username "Alice Cameron" --passphrase 'Frodo@Baggins22'` **`--admin-authorization`** `--recovery-token 'Gandalf-Bilbo+Merry=OneRing'`

  `Add user completed`

  This example shows a new passphrase user being added to a boot disk with a recovery token by a member of the WDE-ADMIN Active Directory group.

--admin-passphrase

Specifies that the passphrase being used is that of an authorized user of the encrypted disk.

This option can be shortened to `--ap`.

Example:

- `pgpwde --add-user --disk 0 --username "Alice Cameron" --passphrase 'Frodo@Baggins22'` **`--admin-passphrase 'Sam&Gamgee44'`**

  `Add user completed`

This example shows a new passphrase user being added to a boot disk. The passphrase of an existing user on the disk is used to authenticate.

--all

Specifies that all partitions should be encrypted.

Example:

- `pgpwde --encrypt --disk 0 --passphrase 'Frodo*1*Baggins'` **`--all`**

  This example shows encryption of a boot disk being started using fast mode. All partitions are to be encrypted.

--answers-file

Specifies the path to a text file with five answers, each on a new line of the file.

Example:

- `pgpwde --recovery-configure --user "Alice Cameron" --passphrase 'bilbo#baggins+Frodo' --disk 0 --questions-file "C:\pgpwde\questions.txt"` **`--answers-file "C:\pgpwde\answers.txt"`**

This example shows local self recovery being configured for user Alice Cameron with the five questions and answers in the specified text files on a Windows system.

--auto-start

Specifies whether or not encryption should begin immediately. Options are `Yes` or `No`. The default is `No`.

Example:

- `pgpwde --verify-user` **`--auto-start Yes`** `--base-disk 0 --disk 1 --passphrase 'Sam&Gamgee44' --username "Jose Medina"`

  This example shows disk 1 on the system being added to the encrypted disk group. Encryption will begin immediately.

--beep

Specifies that audio clues for actions that occur during the PGP Bootguard authentication process should be enabled.

The default is audio clues are disabled.

Example:

- `pgpwde --set-sound --disk 0` **`--beep`**

  ```
  Accessibility Sounds set to [ON]
  ```

  This example shows audio clues being enabled.

--dedicated-mode

Specifies that Dedicated Mode should be used for the encryption process. Dedicated Mode uses maximum computer power to encrypt faster; your system is less responsive during encryption.

Example:

- `pgpwde --encrypt --disk 0 --passphrase 'Frodo*1*Baggins22'` **`--dedicated-mode`**

  This example shows encryption of a boot disk being started using Dedicated Mode.

--disk (-d)

Specifies the disk to which the operation applies.

Example:

```
pgpwde --info --disk 0
Disk information for disk 0.
   Model Number: ST910021AS
   Total number of sectors on disk: 192426569
Display disk information completed
```

This example shows general information being provided for disk 0.

--display

Specifies the display language for PGP BootGuard.

Example:

- `pgpwde --set-language --disk 0` **`--display jp`** `--keyboard jp`

  ```
  Boot language is set to Keyboard=en   Display=en
  Boot language now set to Keyboard=jp  Display=en
  ```

This example shows Japanese being specified for both display and keyboard in PGP BootGuard.

--domain-name

Specifies an authentication domain. The default is the login domain.

Example:

- `pgpwde --add-user --disk 0 --sso --username "Alice Cameron"` **--domain EXAMPLECORP** `--passphrase 'Frodo@Baggins22' --admin-passphrase 'Sam&Gamgee44'`

  `Add user completed`

  This example shows a new SSO user, in domain EXAMPLECORP, being added to a boot disk.

--fast-mode

Specifies that Fast Mode should be used for the encryption process. Skips unused sectors, so encryption of the disk is faster.

Example:

- `pgpwde --encrypt --disk 0 --passphrase 'Frodo*1*Baggins'` **--fast-mode**

  This example shows encryption of a boot disk being started using fast mode.

--image

Specifies an XPM file to use for an operation.

Example:

- `pgpwde --set-background --disk 0` **--image "corplogo.xpm"**

  `Background Image Updated`

  `Set custom background image completed`

  This example shows an image file, corplogo.xpm, being set as the background image for the PGP BootGuard authentication screen.

--interactive

Specifies that passphrases or questions and answers should be provided interactively, as opposed to coming from text files in the case of questions and answers.

Examples:

- `pgpwde --auth --disk 0` **--interactive**

  This example shows a user authenticating to a boot disk by providing the required passphrase interactively (being prompted for it) instead of entering it on the command line.

- `pgpwde --recovery-questions --user "Alice Cameron" --disk 0` **--interactive**

  This example shows user Alice Cameron verifying configured local self recovery questions and answers interactively.

--keyboard

Specifies the keyboard language for PGP BootGuard.

Example:

- `pgpwde --set-language --disk 0 --display jp` **--keyboard jp**

  ```
  Boot language is set to Keyboard=en   Display=en
  Boot language now set to Keyboard=jp  Display=en
  ```

  This example shows Japanese being specified for both display and keyboard in PGP BootGuard.

--keyid

Specifies the key ID of a PGP key.

Example:

- `pgpwde --verify-user --disk 0 --passphrase 'Frodo@Baggins44'` **--keyid 0x12345678**

  ```
  Successfully verified user Alice Cameron
  ```

  This example shows PGP key user Alice Cameron's passphrase being verified via the key ID of her PGP key.

--license-email

Specifies the email address of the person for whom the software is licensed.

This number is used to send license recovery emails and it cannot be changed once the license is authorized: if you do not specify an email during licensing, license recovery will not be possible.

Example:

```
pgp --license-authorize --license-name "Alice Cameron"
--license-email "alice@example.com" --license-organization
"Example Corporation" --license-number "5555-KMKM-44444-
33MMM-MM000-000" authorization.txt
```

This example shows Alice Cameron licensing PGP Whole Disk Encryption Command Line using her example.com email address.

--license-name

Specifies the name of the person for whom the software is licensed.

Example:

```
pgp --license-authorize --license-name "Alice Cameron" --
license-email "alice@example.com" --license-organization
"Example Corporation" --license-number "5555-KMKM-44444-
33MMM-MM000-000"
```

This example shows Alice Cameron licensing PGP Whole Disk Encryption Command Line.

--license-number

Specifies a valid PGP Whole Disk Encryption Command Line license number.

Example:

```
pgp --license-authorize --license-name "Alice Cameron"
--license-email "alice@example.com" --license-organization
"Example Corporation" --license-number "5555-KMKM-44444-
33MMM-MM000-000"
```

This example shows Alice Cameron licensing PGP Whole Disk Encryption Command Line using a valid license number.

--license-organization

Specifies the organization of the licensee.

Example:

```
pgp --license-authorize –license-name "Alice Cameron"
--license-email "alice@example.com" --license-organization
"Example Corporation" --license-number "5555-KMKM-44444-
33MMM-MM000-000"
```

This example shows Alice Cameron licensing PGP Whole Disk Encryption Command Line to her company, Example Corporation.

--message

Specifies text for the PGP BootGuard screen.

Example:

- `pgpwde --set-text --disk 0` **--message "You must change your login passphrase monthly."**

  ```
  Custom message Updated

  Set custom authentication screen text completed
  ```

  This example shows a new text message for the PGP BootGuard screen.

--new-domain

Specifies a new authentication domain for an authorized user.

Example:

- `pgpwde --change-userdomain --disk 0` **--new-domain EXAMPLECORP** `--username "Alice Cameron"`

  ```
  Domain change completed
  ```

  This example shows the authentication domain of user Alice Cameron being changed to `EXAMPLECORP`.

--new-passphrase

Specifies the new passphrase when a passphrase user is changing their passphrase.

Example:

- `pgpwde --change-passphrase --disk 0 --username "Alice Cameron"` **--new-passphrase 'Sam&Gamgee44'** `--passphrase 'Frodo@Baggins22'`

  This example shows an existing passphrase user on an encrypted disk changing their passphrase.

--no-beep

Specifies that audio clues for actions that occur during the PGP Bootguard authentication process should be disabled.

The default is audio clues are disabled.

Example:

- `pgpwde --set-sound --disk 0` **--no-beep**

  `Accessibility Sounds set to [OFF]`

  This example shows audio clues being enabled.

--partition

Specifies that only the listed partition should be encrypted.

Example:

- `pgpwde --decrypt --disk 0 --passphrase 'Frodo*1*Baggins22'` **--partition 3**

  This example shows partition 3 on the boot disk being decrypted.

--passphrase (-p)

Specifies the passphrase of an authorized user on an encrypted disk.

Example:

- `pgpwde --add-user --disk 0 --username "Alice Cameron"` **`--passphrase 'Frodo@Baggins22'`** `--admin-passphrase 'Sam&Gamgee44'`

  `Add user completed`

  This example shows a new passphrase user being added to a boot disk with a passphrase of Frodo@Baggins22. In this example, `--passphrase` is being used to specify the passphrase that the new user of the encrypted disk will use to access it.

- `pgpwde --offload --disk 2` **`--passphrase 'Frodo@Baggins22'`**

  This example shows user information being offloaded from the boot disk to a two-factor device. In this example, `--passphrase` is being used to authenticate the command.

--proxy-passphrase

Specifies the passphrase of the specified user on the proxy server.

Example:

```
pgpwde --license-authorize --license-name "Alice
Cameron"
--license-number "aaaaa-bbbbb-ccccc-ddddd-eeeee-fff"
--license-email "acameron@example.com"
--license-organization "Example Corporation"
--proxy-server "proxyserver.example.com"
--proxy-username "acameron"
--proxy-passphrase 'a_cameron1492sailedblue'
```

This example shows Alice Cameron licensing PGP Whole Disk Encryption Command Line using her passphrase on the specified proxy server.

--proxy-server

Specifies the proxy server to use for licensing.

Example:

```
pgpwde --license-authorize --license-name "Alice
Cameron"
--license-number "aaaaa-bbbbb-ccccc-ddddd-eeeee-fff"
--license-email "acameron@example.com"
--license-organization "Example Corporation"
--proxy-server "proxyserver.example.com"
--proxy-username "acameron"
--proxy-passphrase 'a_cameron1492sailedblue'
```

This example shows Alice Cameron licensing PGP Whole Disk Encryption Command Line via the specified proxy server.

--proxy-username

Specifies a username on the proxy server being used for licensing.

Example:

```
pgpwde --license-authorize --license-name "Alice
Cameron"
--license-number "aaaaa-bbbbb-ccccc-ddddd-eeeee-fff"
--license-email "acameron@example.com"
--license-organization "Example Corporation"
--proxy-server "proxyserver.example.com"
--proxy-username "acameron"
--proxy-passphrase 'a_cameron1492sailedblue'
```

This example shows Alice Cameron licensing PGP Whole Disk Encryption Command Line using her username on the specified proxy server.

--questions-file

Specifies the path to a text file with five questions, each on a new line of the file.

Example:

- `pgpwde --recovery-configure --user "Alice Cameron" --passphrase 'bilbo#baggins+Frodo' --disk 0 --questions-file "C:\pgpwde\questions.txt" --answers-file "C:\pgpwde\answers.txt"`

This example shows local self recovery being configured for user Alice Cameron with the five questions and answers in the specified text files on a Windows system.

--recovery-token

Specifies that a recovery token (WDRT) be created.

Example:

```
pgpwde --add-user --disk 0 --username "Alice Cameron"
--passphrase 'Frodo@Baggins22' --admin-passphrase
'Sam&Gamgee44' --recovery-token 'Gandalf-Bilbo+Merry=OneRing'
```

This example shows a new passphrase user being added to a boot disk with an associated recovery token.

--safe-mode

Specifies that safe mode should be used for the encryption process.

Safe mode allows encryption to be resumed without loss of data if power is lost during encryption; encryption takes longer.

Example:

- `pgpwde --encrypt --disk 0 --passphrase 'Frodo*1*Baggins22' --safe-mode`

  This example shows encryption of a boot disk being started using safe mode.

--sso

Specifies that the user being created should be created as a Single Sign-On (SSO) user

Example:

- `pgpwde --add-user --disk 0 --sso --username "Alice Cameron" --domain examplecorp1 --passphrase 'Frodo@Baggins22' --admin-passphrase 'Sam&Gamgee44'`

  ```
  Add user completed
  ```

  This example shows a new SSO user being added to a boot disk.

--username

Identifies an authorized user of an encrypted disk by their username.

Example:

- `pgpwde --change-passphrase --disk 0` **--username "Alice Cameron"** `--new-passphrase 'Sam&Gamgee44' --passphrase 'Frodo@Baggins22'`

  This example shows an existing passphrase user on an encrypted disk changing their passphrase. They are identified by their username.

--xml

Lists returned information in XML format.

Note: To see the difference between standard returned data and returned data in XML format, simply run the command without `--xml` and then with `--xml`.

Example:

`pgpwde --list-users --disk 0` **--xml**

This command displays returned output in XML format.

A Quick Reference

This section lists and briefly describes all PGP Whole Disk Encryption Command Line commands and options.

In This Chapter

Commands.....75
Options.....77

Commands

Generic

--help (-h)	Shows basic help information for PGP Whole Disk Encryption Command Line.
--version (-V)	Shows PGP Whole Disk Encryption Command Line version information.

Licensing

--license-authorize	Licenses PGP Whole Disk Encryption Command Line.

Disk Information

--enum	Lists system disks and volumes.
--info	Lists general system disk information.
--show-config	Displays PGP BootGuard configuration information.
--status	Displays PGP WDE status of disk.

User Management

--add-user	Adds user to disk.
--change-passphrase	Changes passphrase of specified user.
--change-userdomain	Changes authentication domain of specified user.
--list-users	Lists authorized users on an encrypted disk.
--offload	Offloads passphrase user information onto specified device.
--remove-user	Removes user from specified disk.

--verify-user	Verifies passphrase of user.

Disk Management

--auth	Authenticates to an encrypted disk.
--instrument	Installs WDE configuration information on specified disk.
--uninstrument	Removes WDE configuration from specified disk.

Disk Operation

--decrypt	Decrypts the specified disk.
--encrypt	Encrypts the specified disk.
--resume	Resumes halted encrypt or decrypt process.
--secure	Encrypts a disk to a specified user and passphrase.
--stop	Halts encrypt or decrypt process.

Boot Bypass Commands

--add-bypass	Sets disk for one-time authentication bypass.
--check-bypass	Checks disk to see if authentication bypass is set.
--remove-bypass	Removes authentication bypass from disk.

Recovery Token

--new-wdrt	Creates a new WDRT after use.

PGP BootGuard Customization Commands

--set-background	Sets custom PGP BootGuard screen background.
--set-language	Sets PGP BootGuard display and keyboard languages.
--set-sound	Sets PGP BootGuard audio prompt.
--set-start	Sets custom PGP BootGuard startup screen background.
--set-text	Sets PGP BootGuard authentication screen text message.

Local Self Recovery

--recovery-configure	Configures the local self recovery feature.
--recovery-questions	Displays local self recovery questions.
--recovery-verify	Verifies existing local self recovery questions and answers.
--recovery-remove	Removes existing local self recovery questions and answers.
--recovery-change-passphrase	Changes a forgotten passphrase.

Options

--admin-authorization (--aa)	Command authorized by member of WDE-ADMIN AD group.
--admin-passphrase (--ap)	Specifies the passphrase of an existing WDE user.
--all	Specifies the use of partition mode encryption on all partitions.
--answers-file	Specifies the path to a text file with five answers.
--auto-start	Specifies whether or not encryption should begin immediately.
--beep	Enables beep when PGP BootGuard screen appears.
--dedicated-mode	Encrypts faster; system is less responsive.
--disk (-d)	Specifies the number of the target disk. Zero (0) is boot disk.
--display	Specifies the PGP BootGuard display language.
--domain-name	Specifies the user authentication domain.
--fast-mode	Skips unused sectors, so encryption is faster.
--image	Specifies an image file for an operation.
--interactive	Specifies passphrases or questions/answers should be prompted for.
--keyboard	Specifies the PGP BootGuard keyboard language.
--keyid	Specifies the key ID of a PGP key.
--license-email	Specifies the email address of the licensee.
--license-name	Specifies the name of the licensee.
--license-number	Specifies a valid license number
--license-organization	Specifies the organization of the licensee.
--message	Specifies a custom message for the PGP BootGuard screen.
--new-domain	Specifies a new domain for a user.
--new-passphrase	Specifies a new passphrase for an existing user.
--no-beep	Disables been when PGP BootGuard screen appears.
--partition	Specifies a partition for an operation.
--passphrase (-p)	Specifies a passphrase for an operation.
--proxy-passphrase	Specifies the passphrase of the user on the proxy server.
--proxy-server	Specifies the proxy server to use for licensing.
--proxy-username	Specifies a username on the proxy server being for licensing.
--questions-file	Specifies the path to a text file with five questions.
--recovery-token	Specifies a whole disk recovery token for authentication.

--safe-mode	Encryption can be resumed safely if power is lost during encryption.
--sso	Creates user as single sign-on user.
--username (-u)	Specifies a username for an operation.
--xml	Displays returned information in XML format.

B Troubleshooting

This section describes how PGP Whole Disk Encryption Command Line can be used to troubleshoot problems you might encounter when whole disk encrypting drives.

Note: These troubleshooting procedures can be used whether you are using the graphical user interface or the command-line interface of PGP Whole Disk Encryption.

In This Chapter

Overview....79
Encryption Does Not Begin....80
Encryption Does Not Finish....81
Problems at PGP BootGuard....83

Overview

The troubleshooting tips in this appendix assume:

- PGP Desktop or PGP WDE is correctly installed on the system.
- The PGP software is licensed to support PGP WDE.

  Refer to the section called "Licensing PGP Whole Disk Encryption" in the "Protecting Disks with PGP Whole Disk Encryption" chapter of the *PGP Desktop User's Guide* for more information.
- You have the PGP Desktop or PGP WDE user documentation available.

  PGP Desktop documentation is installed onto your computer during the installation process. To view it, select **Start > Programs > PGP > Documentation**. All documents are saved as Adobe Acrobat Portable Document Format (PDF) files. You can view and print these files with Adobe Acrobat Reader, available on the *Adobe Web site* (http://www.adobe.com).

Before using PGP Whole Disk Encryption Command Line to troubleshoot problems with PGP Whole Disk Encryption, PGP Corporation recommends checking existing resources for information about the issue you are experiencing:

- The *PGP Desktop Release Notes* include the latest information available about PGP WDE, including system requirements and known incompatibilities.
- The *PGP Desktop User's Guide* describes how to prepare a drive for encryption, how to encrypt it, and how to use it after encryption.

Encryption Does Not Begin

While the vast majority of drives can be encrypted without a problem, on some occasions you may find a drive where the encryption process does not start.

Perform the following steps:

1. Review the *PGP Desktop Release Notes* for issues that could be blocking encryption.

   Potential issues include unsupported operating systems and software incompatibilities. For example, to encrypt a boot disk on a Mac OS X system, you must be using an Intel-based Macintosh. If any issues are found, make the appropriate changes and then attempt encryption again.

2. If the first attempt at encryption was made using the graphical user interface, attempt to encrypt using PGP Whole Disk Encryption Command Line.

   Refer to the *–encrypt* command for more information.

If encryption still will not begin, you can use PGP Whole Disk Encryption Command Line to learn more information.

1. First, determine the boot drive on the system using the –enum command.

   ```
   pgpwde --enum
   ```

   The response will be something like:

   ```
   Total number of installed fixed/removable storage
   device (excluding floppy and CDROM): 1

   Disk 0 has 1 online volumes:

     volume C is on partition 2 with offset 80325

   Enumerate disks completed
   ```

   This example shows that the system has one disk, Disk 0, which is drive letter C and is the boot disk. You now know:

   - The boot drive can be whole disk encrypted, as it is Disk 0. Only boot disks that are Disk 0 can be whole disk encrypted.
   - That Disk 0 is the boot disk (which you need to know for subsequent commands).

2 Next, check the status of the boot drive using the –status command.

```
pgpwde --status --disk 0
```

Disk disk 0 is not instrumented by bootguard.

Disk status completed

This example shows the response for a disk that is not whole disk encrypted; that is, the disk is not instrumented by PGP BootGuard.

If a disk is encrypted or even partially encrypted, the response would be something like:

```
pgpwde --status --disk 0
Disk disk0 is instrumented by bootguard.
    Current key is valid.
Whole disk encrypted
   Total sectors: 192426569  highwatermark: 192426569
Disk status completed
```

This response or something similar would mean that the encryption process started but then stopped again. For information on dealing with a drive where encryption does not finish, refer to *Encryption Does Not Finish*.

If the problem continues, you will need to get further assistance.

- The PGP Support forums are user community forums hosted by PGP Corporation and monitored by PGP Corporation personnel. Check the PGP Whole Disk Encryption forums for more information.

  To access the PGP Support forums, please visit *PGP Support* (http://forum.pgp.com).

- The PGP Support Knowledge Base and PGP Technical Support may also be able to assist you with your issue.

  To access the PGP Support Knowledge Base or request PGP Technical Support, please visit *PGP Support Portal Web Site* (https://support.pgp.com). **Note that you may access portions of the PGP Support Knowledge Base without a support agreement; however, you must have a valid support agreement to request PGP Technical Support.**

Encryption Does Not Finish

Once encryption has started, most drives finish encryption normally. On some occasions, however, the encryption process may stop on its own. The cause is generally a problem with the drive being encrypted.

If the system being encrypted loses power during the process, encryption will automatically stop. Depending on whether or not you were using the Safe Mode option (`--safe-mode`), you have two options:

- If you were using Safe Mode, simply get the system back up and restart encryption. It should resume near the point where power was lost.
- If you were not using Safe Mode, get the system back up, decrypt the portion of the drive that was encrypted, and then restart encryption.

The best practice for a drive where encryption stopped automatically is to decrypt the partially encrypted drive, check it for problems, then start encryption again. Be sure to *fully decrypt* any drive on which encryption was started before checking it for problems.

Note: Refer to the *PGP Desktop User's Guide* for extensive information about preparing a drive for encryption.

If encryption stops before finishing (without losing power), perform the following steps:

1. Decrypt the portion of the drive that was encrypted.

   You can use the PGP WDE user interface or PGP WDE command line to decrypt.

2. When the drive is fully decrypted, check the status of the boot drive using the `--status` command.

   ```
   pgpwde --status --disk 0
   ```

Disk disk 0 is not instrumented by bootguard.

Disk status completed

This example shows the response for a disk that has been fully decrypted.

If the response to the `--status` command shows the drive still partially encrypted, make sure the drive is fully decrypted.

1. Next, check the health of the drive.

   Check the "Ensure Disk Health Before Encryption" section of the "Protecting Disks with PGP Whole Disk Encryption" chapter of the *PGP Desktop User's Guide* for more information.

2. Make the changes necessary to ensure the health of the drive.
3. Review the *PGP Desktop Release Notes* for issues that could be affecting encryption. If any issues are found, make the appropriate changes.

4 When all changes have been made, reboot the system.

5 Begin the encryption process again.

If the problem continues, you will need to get further assistance:

- The PGP Support forums are user community forums hosted by PGP Corporation and monitored by PGP Corporation personnel. Check the PGP Whole Disk Encryption forums for more information.

  To access the PGP Support forums, please visit *PGP Support* (http://forum.pgp.com).

- The PGP Support Knowledge Base and PGP Technical Support may also be able to assist you with your issue.

  To access the PGP Support Knowledge Base or request PGP Technical Support, please visit *PGP Support Portal Web Site* (https://support.pgp.com). **Note that you may access portions of the PGP Support Knowledge Base without a support agreement; however, you must have a valid support agreement to request PGP Technical Support.**

Problems at PGP BootGuard

On rare occasions, a drive may successfully encrypt but PGP BootGuard may prevent access to the system.

Most cases involving problems at the PGP BootGuard screen involve entering the passphrase correctly.

It's easy to spot a problem involving entering your passphrase: you enter what you believe is the correct passphrase and press **Enter** or **return**; PGP BootGuard displays the message "Incorrect authentication, please try again" instead of giving you access to your system.

If you cannot successfully enter your passphrase at the PGP BootGuard screen, perform the following steps:

1 Carefully re-enter your passphrase. You may have typed it incorrectly.

  To see the characters you are typing, press **Tab** then enter your passphrase.

2 Make sure **Caps Lock** is off, unless your passphrase is all capital letters.

3 Make sure you are using the correct keyboard layout. If the wrong keyboard layout is selected, you may inadvertently be typing the wrong characters.

  Select **Keyboard** on the main PGP BootGuard screen and press **Enter** or **return**. Available keyboard layouts are displayed; the selected keyboard layout is shown under the list. Select **Go Back** and press **Enter** or **return** to return to the main PGP BootGuard screen.

Refer to the *PGP Desktop Release Notes* and the *PGP Desktop User's Guide* for more information about supported keyboard layouts.

4. If there are other configured users for the drive, try the passphrases of these users.
5. If you have configured local self recovery, try using it to authenticate at PGP BootGuard. See Local Self Recovery for more information.
6. If you are in an enterprise environment, contact your PGP administrator for the PGP Whole Disk Recovery Token for the system.

If the problem continues, you will need to get further assistance.

- The PGP Support forums are user community forums hosted by PGP Corporation and monitored by PGP Corporation personnel. Check the PGP Whole Disk Encryption forums for more information.

  To access the PGP Support forums, please visit *PGP Support* (http://forum.pgp.com).

- The PGP Support Knowledge Base and PGP Technical Support may also be able to assist you with your issue.

  To access the PGP Support Knowledge Base or request PGP Technical Support, please visit *PGP Support Portal Web Site* (https://support.pgp.com). **Note that you may access portions of the PGP Support Knowledge Base without a support agreement; however, you must have a valid support agreement to request PGP Technical Support.**

If you are still unable to successfully access the system, you can use the recovery CD or diskette you created before you encrypted the drive. The recovery software will allow you to decrypt the drive. Refer to the *PGP Desktop User's Guide* for complete information.

If you did **not** create a recovery CD or diskette before you encrypted the drive, go to the PGP Support Knowledge Base and search for article 470. This article includes a pointer to a Web location from which you can download a recovery CD or diskette.