The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement. Version 10.3.0. Last updated: January 2013.

Legal Notice

Copyright (c) 2013 Symantec Corporation. All rights reserved.
Symantec, the Symantec Logo, PGP, Pretty Good Privacy, and the PGP logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.
The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
Symantec Home Page (http://www.symantec.com)
Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1
## Contents

### Introduction
- About Symantec Drive Encryption 5
- About PGP Whole Disk Encryption Command Line 5
- Important Terms 6
- Audience 7
- System Requirements 7
- Installing and Uninstalling 7
- Encrypting a Drive 9
- Technical Support 9
  - Contacting Technical Support 10
  - Licensing and registration 10
  - Customer service 10
  - Support agreement resources 11

### The Command-Line Interface
- Overview 13
- Scripting 14
- Editing the Path 14
- WDE-ADMIN Active Directory Group 15
- Passphrases 15

### Licensing
- Overview 17
- --license-authorize 17
- Licensing via a Proxy Server 18

### Generic Commands
- --help (-h) 21
- --version 22

### Disk Information Commands
- --enum 23
- --info 24
- --show-config 25
- --status 25

### Authenticating Users with PGP BootGuard
- Overview 27

### User Management Commands
- --add-user 29
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>--change-passphrase</td>
<td>30</td>
</tr>
<tr>
<td>--change-userdomain</td>
<td>31</td>
</tr>
<tr>
<td>--list-users</td>
<td>33</td>
</tr>
<tr>
<td>--offload (deprecated command)</td>
<td>33</td>
</tr>
<tr>
<td>--remove-user</td>
<td>34</td>
</tr>
<tr>
<td>--verify-user</td>
<td>34</td>
</tr>
</tbody>
</table>

| Disk Management                              | 37   |
| --auth                                       | 37   |
| --instrument                                | 38   |
| --uninstrument                               | 38   |

| Disk Operation                               | 41   |
| --decrypt                                    | 41   |
| --encrypt                                    | 42   |
| --resume                                     | 43   |
| --secure                                     | 43   |
| --stop                                       | 44   |

| Boot Bypass Commands                         | 47   |
| --add-bypass                                 | 47   |
| --check-bypass                               | 48   |
| --remove-bypass                              | 49   |

| Recovery Token Commands                      | 51   |
| --new-wdrt                                   | 51   |

| PGP BootGuard Customization Commands         | 53   |
| --set-background                             | 53   |
| --set-language                               | 54   |
| --set-sound                                  | 55   |
| --set-start                                  | 56   |
| --set-text                                   | 56   |

| Local Self Recovery                          | 59   |
| --recovery-configure                         | 59   |
| --recovery-questions                         | 61   |
| --recovery-verify                            | 62   |
| --recovery-remove                            | 62   |
| --recovery-change-passphrase                 | 63   |

<p>| Options                                      | 65   |
| &quot;Secure&quot; Options                             | 68   |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>--admin-authorization</td>
<td>68</td>
</tr>
<tr>
<td>--admin-passphrase</td>
<td>68</td>
</tr>
<tr>
<td>--all</td>
<td>69</td>
</tr>
<tr>
<td>--answers-file</td>
<td>69</td>
</tr>
<tr>
<td>--auto-start</td>
<td>69</td>
</tr>
<tr>
<td>--beep</td>
<td>69</td>
</tr>
<tr>
<td>--count</td>
<td>70</td>
</tr>
<tr>
<td>--dedicated-mode</td>
<td>70</td>
</tr>
<tr>
<td>--disk (-d)</td>
<td>70</td>
</tr>
<tr>
<td>--display</td>
<td>70</td>
</tr>
<tr>
<td>--domain-name (--domain)</td>
<td>71</td>
</tr>
<tr>
<td>--fast-mode</td>
<td>71</td>
</tr>
<tr>
<td>--image</td>
<td>71</td>
</tr>
<tr>
<td>--interactive</td>
<td>72</td>
</tr>
<tr>
<td>--keyboard</td>
<td>72</td>
</tr>
<tr>
<td>--keyid</td>
<td>72</td>
</tr>
<tr>
<td>--license-email</td>
<td>73</td>
</tr>
<tr>
<td>--license-name</td>
<td>73</td>
</tr>
<tr>
<td>--license-number</td>
<td>73</td>
</tr>
<tr>
<td>--license-organization</td>
<td>74</td>
</tr>
<tr>
<td>--message</td>
<td>74</td>
</tr>
<tr>
<td>--new-domain</td>
<td>74</td>
</tr>
<tr>
<td>--new-passphrase</td>
<td>74</td>
</tr>
<tr>
<td>--no-beep</td>
<td>75</td>
</tr>
<tr>
<td>--partition</td>
<td>75</td>
</tr>
<tr>
<td>--passphrase (-p)</td>
<td>75</td>
</tr>
<tr>
<td>--proxy-passphrase</td>
<td>76</td>
</tr>
<tr>
<td>--proxy-server</td>
<td>76</td>
</tr>
<tr>
<td>--proxy-username</td>
<td>76</td>
</tr>
<tr>
<td>--questions-file</td>
<td>77</td>
</tr>
<tr>
<td>--recovery-token (--wdrt, --rt)</td>
<td>77</td>
</tr>
<tr>
<td>--safe-mode (--safe)</td>
<td>77</td>
</tr>
<tr>
<td>--sso</td>
<td>77</td>
</tr>
<tr>
<td>--username (-u, --user)</td>
<td>78</td>
</tr>
<tr>
<td>--xml</td>
<td>78</td>
</tr>
</tbody>
</table>

**Quick Reference**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands</td>
<td>79</td>
</tr>
<tr>
<td>Options</td>
<td>80</td>
</tr>
</tbody>
</table>

**Troubleshooting**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>83</td>
</tr>
<tr>
<td>Problems at PGP BootGuard</td>
<td>84</td>
</tr>
</tbody>
</table>
Introduction

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

In This Chapter

About Symantec Drive Encryption ................................................................. 5
About PGP Whole Disk Encryption Command Line ........................................ 5
Important Terms ......................................................................................... 6
Audience ..................................................................................................... 7
System Requirements .................................................................................. 7
Installing and Uninstalling .......................................................................... 7
Encrypting a Drive ...................................................................................... 9
Technical Support ...................................................................................... 9

About Symantec Drive Encryption

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

For more information about Symantec Drive Encryption, see the:
- Symantec Encryption Desktop User’s Guide
- Symantec Drive Encryption Quick Start Guide

About PGP Whole Disk Encryption Command Line

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

Note: Not all Symantec Drive Encryption functions are available via the command line.

Symantec Drive Encryption 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.
Important Terms

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

- **Symantec Drive Encryption**: a standalone product from Symantec Corporation and a feature of Symantec Encryption 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. Symantec Drive Encryption functionality is available via a graphical user interface and through a command-line interface.

- **PGP Whole Disk Encryption Command Line**: the command-line interface to Symantec Drive Encryption functionality. Because Symantec Drive Encryption is available on both Windows and Mac OS X systems, you can use the Symantec Drive Encryption 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 Symantec 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 Symantec Encryption Management Server if the disk is part of a Symantec Encryption Management Server-managed environment.

- **Symantec Encryption Management Server**: a management console for securing data from Symantec 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 Symantec Drive Encryption functions from the command line.

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

---

**System Requirements**

PGP Whole Disk Encryption Command Line has the same requirements as Symantec Drive Encryption for Windows or Mac OSX. If Symantec Drive Encryption is installed on a system, then PGP Whole Disk Encryption Command Line is also installed and available for use.

---

**Installing and Uninstalling**

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

To uninstall PGP Whole Disk Encryption Command Line, simply uninstall Symantec Drive Encryption or Symantec Encryption Desktop.
Encrypting a Drive

To encrypt a drive requires several things: the drive must be instrumented, there must be at least one authorized user on the drive, and the encryption process must be started.

There are two ways to encrypt a drive:

- **Single command, --secure**: this one command does all three of the above actions. It instruments the drive, creates an authorized user, and encrypts the drive. This command is most useful when you have just installed Symantec Drive Encryption and thus have not instrumented any drives, created any authorized users, or encrypted any drives.

- **Multiple commands**: for scenarios where the disk is already instrumented or the user has already been added, use --instrument, --add-user, and finally --encrypt.

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our Web site at the following URL:

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan  
customercare_apac@symantec.com
Europe, Middle-East, Africa  
semea@symantec.com
North America, Latin America  
supportsolutions@symantec.com
3

The Command-Line Interface

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

In This Chapter

Overview .......................................................................................................................... 13
Scripting .......................................................................................................................... 14
Editing the Path ............................................................................................................. 14
WDE-ADMIN Active Directory Group ........................................................................... 15
Passphrases ...................................................................................................................... 15

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 Windows Symantec Drive Encryption clients in a Symantec Encryption Management Server environment and using Active Directory, you can create a special Active Directory group. With this group, you can authenticate commands with the group administrator passphrase in place of the user passphrase. This means you can run commands on your managed Symantec Drive Encryption 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.

This feature applies only to Windows installations of PGP Whole Disk Encryption Command Line.

Refer to the *Symantec Encryption Management Server 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 don't feel safe if my data isn't protected

as your passphrase, you would have to enter it as

'I don\'t feel safe if my data isn\'t protected'

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.
Licensing

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

In This Chapter

Overview .......................................................... 17
--license-authorize ........................................... 17
Licensing via a Proxy Server .................................. 18

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-cccccc-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:

```
pgpwd --license-authorize --license-name "Alice Cameron"
 --license-number "aaaaa-bbbbb-ccccc-dddd-dddddd-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.)
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) ......................................................................................................................... 21
--version.......................................................................................................................... 22

--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:

```bash
gpgwde --help
```

The short form usage format is:

```bash
gpgwde -h
```

**Note:** There are differences between the commands and options produced with the **--help** command (the Help contents) and those in this guide. The Help contents lists commands and options related to disk groups. In contrast, this guide omits any mention of disk groups. Use disk group commands and options only with the supervision of your Symantec customer representative.

Example:

```bash
gpgwde --help
PGP WDE command line tool.
Usage: gpgwde - action [--options,...]
```

This example shows the response to the **--help** command.
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 10.3.0 (Build 5282)
Copyright (C) 2012 Symantec Corporation
Request sent to Version was successful
```

This example shows the response to the `--version` command.
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 Symantec Drive Encryption 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** ............................................................................................................................. 23
- **--info** ................................................................................................................................ 24
- **--show-config** ..................................................................................................................... 25
- **--status** ................................................................................................................................ 25

**--enum**

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

Provides general status information for the specified disk.

Use the **--status** command for Symantec Drive Encryption-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

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 Symantec Drive Encryption.
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

Provides Symantec Drive Encryption-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:

```
pgpwd --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:

- `pgpwd --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.

- `pgpwd --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.
7

Authenticating Users with PGP BootGuard

This section describes actions you can take at the PGP BootGuard screen.

In This Chapter

Overview ................................................................. 27

Overview

Your computer boots up in a different way once you use PGP Whole Disk Encryption Command Line to protect the boot disk—or a secondary fixed disk—on your system. On power-up, the first thing you see is the PGP BootGuard log-in screen asking for your username, passphrase, and domain. The screen also provides other ways to authenticate yourself, without requiring a passphrase. When you properly authenticate, PGP Whole Disk Encryption Command Line decrypts the disk.

When you use a Symantec Drive Encryption-encrypted disk, it is decrypted and opened automatically as needed. With most modern computers, after the disk is completely encrypted, there is no noticeable slowdown of your activities.

After you unlock a disk or partition, its files are available to you—as well as anyone else who can physically use your system. Your files are unlocked until you lock them again by shutting down your computer.

When you shut down a system with an encrypted boot disk or partition or if you remove an encrypted removable disk from the system, all files on the disk or partition remain encrypted and fully protected—data is never written to the disk or partition in an unencrypted form. Proper authentication (passphrase, token, private key, or WDRT) is required to make the files accessible again.

On the PGP BootGuard log-in screen you can:

- Authenticate an encrypted boot or secondary disk or partition on the system.
- View information about the disks or partitions on your system.
- Authenticate if you have forgotten your passphrase.
- Choose your keyboard layout.

For more information, see the Symantec Encryption Desktop User Guide.
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 ....................................................................................................................... 29
--change-passphrase..................................................................................................... 30
--change-userdomain.................................................................................................... 31
--list-users ...................................................................................................................... 33
--offload (deprecated command) .................................................................................. 33
--remove-user .................................................................................................................. 34
--verify-user ................................................................................................................... 34

--add-user

Adds an authorized user to the encrypted disk.

The usage format is:

    pgpwd --add-user --disk <number> --domain-name <domain> --sso
    --passphrase <phrase> --username <user> --admin-authorization
    <phrase> | --admin-passphrase <pass> | --admin-keyid <string>
    | --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.
--add-user

(Windows only) creates 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.

--username specifies a username for an operation.

--sso

(Windows only) creates 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.

--username specifies a username for an operation.

--admin-authorization (Windows only) 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.

--username specifies a username for an operation.

--admin-keyid is an administrator's key ID

--recovery-token specifies that the disk's recovery token (WDRT) will be used for authentication.

Example:

```
pgpwde --add-user --disk 0 --username "Alice Cameron" --username "Alice Cameron" --domain EXAMPLECORP --passphrase 'Frodo@Baggins22' --admin-passphrase 'Sam&Gamgee44' --admin-authorization --admin-keyid is an administrator's key ID --recovery-token specifies that the disk's recovery token (WDRT) will be used for authentication.
```

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
```

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**

Changes the passphrase of a passphrase user on an encrypted disk.

The usage format is:
User Management Commands

--change-userdomain

Changes 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-passphrase --disk <number> --username <user> --domain-name <domain> --new-passphrase <newpass> --passphrase <phrase> | --auth-administrator <phrase> | --admin-passphrase <phrase> | --admin-keyid <string> | --recovery-token <string> | --interactive
```

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.
- `--domain-name` (Windows and Linux only) specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
- `<domain>` is the domain for the user account.
- `--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.
- `--admin-authorization` (Windows only) 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.
- `--admin-keyid` is an administrator's key ID
- `<string>` key ID
- `--recovery-token` uses disk's recovery token (WDRT) for authentication.
- `<string>` is the WDRT string.

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.
pgpwde --change-userdomain --disk <number> --new-domain <domain> --username <user> --sso --domain-name <domain> --passphrase <phrase> | --admin-authorization | --admin-passphrase <pass> | --admin-keyid | --recovery-token <string>

Where:

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

- **--new-domain** (Windows and Linux only) 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.

- **--sso** (Windows only) specifies that the user is a single sign-on (SSO) user.

- **--domain-name** (Windows and Linux only) specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
  
  *<domain>* is the domain for the user account.

- **--passphrase** specifies the passphrase for an operation.
  
  *<pass>* is the user passphrase.

- **--admin-authorization** (Windows only) 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.

- **--admin-keyid** is an administrator’s key ID
  
  *<string>* key ID

- **--recovery-token** specifies that the disk’s recovery token (WDRT) will be used for authentication.
  
  *<string>* is the WDRT string.

Example:

```
pgwde --change-userdomain --disk 0 --new-domain EXAMPLECORP --username "Alice Cameron" --passphrase "Frodo@Baggins22" --sso --admin-passphrase "adminPassphrase"
```

Domain change completed

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

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 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 (deprecated 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>
```

Where:
- `--offload` specifies that you are offloading passphrase user information to a two-factor device.
- `--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.
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**

Removes a user who is currently authorized on the encrypted disk.

The usage format is:

```
pgpwde --remove-user --disk <number> --username <user> [--domain-name <domain>] --admin-authorization | --admin-passphrase <pass> | --interactive
```

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.

- **--domain-name** (Windows and Linux only) specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
  
  `<domain>` is the domain for the user account.

- **--admin-authorization** (Windows only) 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.

- **--interactive** specifies that a passphrase be prompted for instead of entered on the command line.

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**

Verifies the passphrase of a user who is an authorized user of an encrypted disk.
The usage format is:

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

Where:

- `--disk` specifies to which disk on the system the information applies.
- `<number>` is the disk number on the system.
- `--username` specifies a username for an operation.
- `<user>` is the username of an authorized user account on the disk.
- `--domain` specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
- `<domain>` is the domain for the user account.
- `--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.
- `--interactive` specifies that a passphrase be prompted for instead of entered on the command line.

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.
Disk Management

Disk management commands set disk properties.

In This Chapter

--auth ............................................................................................................................37
--instrument ...................................................................................................................38
--uninstrument ..............................................................................................................38

--auth

Authenticates a user to an encrypted disk, for use when PGP Tray is not running.

The usage format is:

```
pgpwde --auth --disk <number> --passphrase <phrase> | --auth-administrator <phrase> | --admin-passphrase <phrase> | --admin-keyid <string> | --recovery-token <string> | --interactive
```

Where:

- **--auth** specifies you are authenticating to an encrypted disk.
- **--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.
- **--admin-authorization** (Windows only) 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.
- **--admin-keyid** is an administrator's key ID
  <string> key ID
- **--recovery-token** uses disk's recovery token (WDRT) for authentication.
  <string> is the WDRT string.
- **--interactive** specifies that a passphrase be prompted for instead of entered on the command line.

In most cases, if a disk needs authentication, PGP Tray prompts the user for credentials. If PGP Tray is not running, use --auth to authenticate.
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.
Disk Operation

Disk operation commands control disk encryption and decryption.

In This Chapter

--decrypt .......................................................................................................................... 41
--encrypt .......................................................................................................................... 42
--resume ............................................................................................................................ 43
--secure ............................................................................................................................... 43
--stop .................................................................................................................................... 44

--decrypt

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

The usage format is:

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

Where:

- --decrypt specifies that the disk is to be decrypted.
- --disk specifies the disk to which the operation applies.
  - <number> is the disk number on the system.
- --admin-authorization (Windows only) 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.
- --recovery-token uses disk's recovery token (WDRT) for authentication.
  - <string> is the WDRT string.
- --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.

Decryption cannot begin until encryption is completed or stopped. To stop encryption that is in process, use the --stop command.
If you begin to decrypt an encrypted disk, you can pause the decrypt and then re-start the decrypt process, but you cannot stop the decrypt and then encrypt just the portion that was decrypted. If you begin to decrypt an encrypted drive, you must fully decrypt it before you can re-encrypt it.

To check progress on the decryption process, use the --status command.

To decrypt disks that are encrypted with the --partition option, include the --partition option in the --decrypt command.

**Note:** For Mac installations with Apple Boot Camp, decrypt your disk only from the Mac OS X partition. If you instead decrypt from the Windows partition, the Windows boot partition may become corrupted.

Examples:

- `pgpwde --decrypt --disk 0 --passphrase 'Frodo*1*Baggins22'
  This example shows a boot disk being decrypted.

**Note:** The --partition option cannot decrypt a specific partition of a disk if all partitions of the disk were encrypted at a time using --secure or --encrypt command. Use --partition to decrypt a specific disk partition only when the partition was encrypted individually.

---

**--encrypt**

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

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` uses the maximum computer power to encrypt faster. With this mode, 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.

To use the --encrypt command, the drive to be encrypted must be instrumented and have at least one configured user. See the --secure (page 43) command.

To stop encryption that is in process, use the --stop command.

Note: For Mac installations with Apple Boot Camp, start the encryption from the Mac OS X partition.

Example:

```
pgpwde --encrypt --disk 0 --passphrase 'Frodo@Baggins44' --fast-mode --all
```

This example shows encryption being started using fast mode. Authentication is provided by an 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:
--stop

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

The usage format is:

```
pgpwde --stop --disk <number> --passphrase <phrase> | --admin-authorization <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.
- `--admin-authorization (Windows only)` specifies that the command is being performed by a member of the WDE-ADMIN Active Directory group.
  `<phrase>` a passphrase

Example:

```
pgpwde --stop --disk 0 --passphrase 'Frodo@Baggins44'
```
This example shows the encryption or decryption process on disk 0 being stopped.
Boot Bypass Commands

The boot bypass feature lets you reboot a system one or more times without having to authenticate at the PGP BootGuard screen.

**Caution:** Using the boot bypass feature weakens the protection provided by Symantec Drive Encryption. Pay extra attention to the physical security of systems when a bypass restart count exists. Use the `--remove-bypass` command to remove any unnecessary remaining bypass restarts.

Boot bypass is generally used for remote deployment or upgrade scenarios when one or more reboots is required; patch management, for example.

By default, boot bypass is disabled for a system. You must use the `--add-bypass` command to enable bypass restarts.

**Note:** All three boot bypass commands apply to the boot disk only, even if you specify another disk on the command line.

In This Chapter

--add-bypass ................................................................................................................... 47
--check-bypass ............................................................................................................ 48
--remove-bypass ............................................................................................................ 49

---add-bypass

Enables or disables bypass restarts for a system.

The usage format is:

```
pgpwd --add-bypass --disk <number> --count <bypassrestarts> -
-passphrase <phrase> | --admin-authorization | --admin-
passphrase <pass> | --admin-keyid <string> | --recovery-token
<string> | --interactive
```

Where:

- `--disk` specifies the disk to which the operation applies. Because bypass applies only to the boot disk, PGP Whole Disk Encryption Command Line ignores this option.
- `<number>` is the disk number on the system.
- `--count` specifies that bypass restarts are being configured the boot disk on the system.
```markdown
- `<bypassrestarts>` is the desired number of bypass restarts, with a maximum value of 4,294,967,295. A value of 0 (zero) disables bypass restarts. Values above 0 allows that many bypass restarts. In managed environments, `bypassrestarts` must not exceed the maximum bypass restarts set on Symantec Encryption Management Server.

- `--passphrase` specifies the passphrase for an operation.
  `<phrase>` is the passphrase of an authorized user on the disk.

- `--admin-authorization` (Windows only) 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.

- `--admin-keyid` is an administrator's key ID
  `<string>` key ID

- `--recovery-token` specifies that the disk's recovery token (WDRT) will be used for authentication.
  `<string>` is the WDRT string.

- `--interactive` specifies that a passphrase be prompted for instead of entered on the command line.

In a managed environment, the Symantec Encryption Management Server administrator can establish a preference on the Symantec Encryption Management Server that limits the number of bypass restarts that can be established using `--add-bypass`. The preference is called `wdeMaximumBypassRestarts`. Setting the preference to 0 (zero) disables boot bypass. Setting the preference to a value from 1 to 4,294,967,295 allows that many bypass restarts. If the preference does not exist on the Symantec Encryption Management Server, the value is set to 1, allowing one bypass restart for each system.

Example:

- `pgpwde --add-bypass --disk 0 --count 4 --admin-passphrase 'bilbo@baggins42'

  This example shows that four bypass restarts was added to the boot disk on the system using the passphrase of an authorized user on the disk.

---

**--check-bypass**

Indicates whether boot bypass is configured for the specified boot disk. If configured, it will also display the original and remaining bypass restart counts.

The usage format is:

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

Where:
```
--remove-bypass

Removes boot bypass from the system, including the original and remaining bypass restart counts.

The usage format is:

```
pgpwde --remove-bypass --disk <number> --passphrase <phrase> |
--admin-authorization | --admin-passphrase <pass> | --admin-keyid <string> | --recovery-token <string> | --interactive
```

Where:

- `--disk` specifies the disk to which the operation applies. Because bypass applies only to the boot disk, PGP Whole Disk Encryption Command Line ignores this option.
- `<number>` is the disk number on the system.
- `--admin-authorization` (Windows only) 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.
- `--admin-keyid` is an administrator's key ID
- `<string>` key ID

Examples:

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

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'
```

This example shows that Disk 0 is not configured for boot bypass.
--recovery-token specifies that the disk’s recovery token (WDRT) will be used for authentication.
<string> is the WDRT string.

--interactive specifies that a passphrase be prompted for instead of entered on the command line.

Example:

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

This example shows the removal of boot bypass from a disk.
Recovery Token Commands

In Symantec Encryption Management Server-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 Symantec Encryption Management 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 Symantec Encryption Management 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......................................................................................................................51

---

**--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> | --interactive
```

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** (Windows only) 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.
--new-wdrt

- **--recovery-token** specifies that a recovery token (WDRT) will be created to replace the used one.
  
  `<string>` is the WDRT string.

- **--interactive** specifies that a passphrase be prompted for instead of entered on the command line.

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.
13

PGP BootGuard Customization Commands

PGP Whole Disk Encryption Command Line includes commands for modifying the default PGP BootGuard screen.

The PGP BootGuard customization commands are:

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

In This Chapter

\(--\text{set\text{-}background}\) ...........................................................................................................53
\(--\text{set\text{-}language}\) ................................................................................................................54
\(--\text{set\text{-}sound}\) ......................................................................................................................55
\(--\text{set\text{-}start}\) ........................................................................................................................56
\(--\text{set\text{-}text}\) ........................................................................................................................56

\(--\text{set\text{-}background}\)

The \(--\text{set\text{-}background}\) 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).

\textbf{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:

```
pgwde --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:

```
pgwde --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 now set to Keyboard=jp  Display=jp

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.
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; Symantec 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 Symantec Encryption Management Server-managed environment, your Symantec Encryption Management 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 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`.................................................................59
- `--recovery-questions`...............................................................61
- `--recovery-verify`...................................................................62
- `--recovery-remove`..................................................................62
- `--recovery-change-passphrase`..................................................63

---

**--recovery-configure**

Configures local self recovery.

The usage format is:

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.
- `--domain-name` (Windows and Linux only) specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
- `<domain>` is the domain for 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.
- `--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.

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`.

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

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> [--domain-name <domain>] [--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.
- **--domain-name** (Windows and Linux only) specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
- **<domain>** is the domain for 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

Verifies the configured local self recovery questions and answers. You can answer the five questions using a text file or interactively.

The usage format is:

```
pgpwde --recovery-verify --user <username> [--domain-name <domain>] [--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.
- `--domain-name` (Windows and Linux only) specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
- `<domain>` is the domain for 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.

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

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

Removes configured local self recovery questions and answers.

The usage format is:
Local Self Recovery

--recovery-change-passphrase

Creates a new passphrase. Use this command when you have forgotten your existing passphrase and have authenticated to PGP BootGuard with local self recovery.

**Note:** Symantec 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> [--domain-name <domain>] [--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.

---

```
pgpwde --recovery-remove --user <username> [--domain-name <domain>] --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.
- `--domain-name` (Windows and Linux only) specifies the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.
- `<domain>` is the domain for 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.
--domain-names (Windows and Linux only) the domain for the user account. The default is the login domain if one has been established. This parameter is required for Windows clients in a Symantec Encryption Management Server-managed environment. It is also required for users that have a domain.

- <domain> is the domain for 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.
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 Symantec Drive Encryption 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
--recovery-change-passphrase
--admin-authorization
--admin-passphrase
--all
--answers-file
--auto-start
--beep
--count
--dedicated-mode
--disk (-d)
--display
--domain-name (--domain)
--fast-mode
--image
--interactive
--keyboard
--keyid
--license-email
--license-name
--license-number
--license-organization
--message
--new-domain
--new-passphrase
--no-beep
--partition
--passphrase (-p)
--proxy-passphrase
--proxy-server
--proxy-username
--questions-file
--recovery-token (--wdrt, --rt)
--safe-mode (--safe)
--sso
--username (-u, --user)
--xml
"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 Symantec Drive Encryption clients in a Symantec Encryption Management Server-managed environment. This option applies only to Windows installations.

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*B1*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.

--count

Specifies the number of bypass restarts being configured for the boot disk on a system. Only works with the --add-bypass command.

Valid values for --count are 0 through 4,294,967,295.

Setting --count to 0 disables the boot bypass feature on the system.

In a Symantec Encryption Management Server-managed environment, a preference constrains what values are valid for --count on the command line; you cannot set a value on the command line that is higher than the value set in the preference.

--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 now set to Keyboard=jp  Display=jp

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

---

**--domain-name (----domain)**

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

Example:

- `pgpwde --add-user --disk 0 --sso --username "Alice Cameron" --domain-name 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:

```
pgwde --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.

```
pgwde --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 (--wdrt, --rt)

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 (--safe)

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*l*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. This option is used only on Windows systems.

Example:
Options
--username (-u, --user)

- pgpwde --add-user --disk 0 --sso --username "Alice Cameron" --domain-name 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 (-u, --user)

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.
Quick Reference

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

In This Chapter

Commands............................................................................................................................ 79
Options............................................................................................................................. 80

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 Symantec Drive Encryption 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 Symantec Drive Encryption configuration information on specified disk.
Options

**--uninstrument** Removes Symantec Drive Encryption 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)** (Windows only) Command authorized by member of WDE-ADMIN AD group.
- **--admin-passphrase (--ap)** Specifies the passphrase of an existing Symantec Drive Encryption 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.
- **--count** Specifies the number of bypass restarts being configured.
Options

--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 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 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.
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 Symantec Drive Encryption.

In This Chapter

Overview ................................................................. 83
Problems at PGP BootGuard ........................................... 84

Overview

The troubleshooting tips in this appendix assume:

- Symantec Encryption Desktop or Symantec Drive Encryption is correctly installed on the system.
- The Symantec Encryption Desktop software is licensed to support Symantec Drive Encryption.
  
  Refer to the section called "Licensing Symantec Drive Encryption" in the "Protecting Disks with Symantec Drive Encryption" chapter of the *Symantec Encryption Desktop User's Guide* for more information.
- You have the Symantec Encryption Desktop or Symantec Drive Encryption user documentation available.
  
  Symantec Encryption Desktop documentation is installed onto your computer during the installation process. To view it, select Start > Programs > Symantec Encryption > 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 Symantec Drive Encryption, Symantec Corporation recommends checking existing resources for information about the issue you are experiencing:

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


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 (on page 59) for more information.

6. If you are in an enterprise environment, contact your Symantec Encryption Management Server administrator for the PGP Whole Disk Recovery Token for the system.

If the problem continues, you will need to get further assistance. For more information, see Technical Support (on page 9).

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 Symantec Encryption Desktop User’s Guide for complete information.

If you did not create a recovery CD or diskette before you encrypted the drive, go to www.symantec.com/support/ and search for TECH166098, "PGP Desktop Resolved Issues." This article includes a pointer to a Web location from which you can download a recovery CD or diskette.