PGP Managed Whole Disk Encryption

Common Criteria Supplemental

Version Information

PGP mWDE Common Criteria Supplement. PGP Whole Disk Encryption Version 9.10.0. Released February 2009.

Copyright Information

Trademark Information

Licensing and Patent Information

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

Acknowledgments

This product includes or may include:

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

http://www.cs.fsu.edu/~engelen/soaplicense.html. ● Windows Template Library (WTL) is used for developing user interface components and is distributed under the Common Public License v1.0 found at http://opensource.org/licenses/cpl1.0.php. ● The Perl Kit provides several independent utilities used to automate a variety of maintenance functions and is provided under the Perl Artistic License, found at http://www.perl.com/pub/a/language/misc/Artistic.html. ● rEFIt - libeg, provides a graphical interface library for EFI, including image rendering, text rendering, and alpha blending, and is distributed under the license found at http://refit.svn.sourceforge.net/viewvc/*checkout*/refit/trunk/refit/LICENSE.txt?revision=288. Copyright (c) 2006 Christoph Pfisterer. All rights reserved. ● Java Radius Client, used to authenticate PGP Universal Web Messenger users via Radius, is distributed under the Lesser General Public License (LGPL) found at http://www.gnu.org/licenses/lgpl.html.

Export Information

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

Limitations

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

Contents

Purpose 1

Definitions 1
Acronyms 3

PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10 supplement 5

Receipt and preparation of TOE and Environment 5
Integrity checking of downloaded file 6
Guidance Documents 7
Common Criteria Excluded Aspects 9
Verification of Common Criteria components 9
Usage Assumptions 10
Applicability of the PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10 10
What is PGP Whole Disk Encryption? 10
What Am I Installing? 11
System Requirements 11
Create a Recovery CD 11
Creating PGP Virtual Disk Volumes 11
Creating a PGP Zip Archive 11
PGP Self-Decrypting Archive 12
Using PGP Shredder to Shred Files 12
Shredding Free Space 12
Disabling features not applicable to the CC Evaluated Configuration 12
Verification of CC Evaluated installation 13

PGP Desktop for Windows User's Guide 15

Applicability of the PGP Desktop for Windows User's Guide 16
About PGP Desktop 9.10 for Windows 16
PGP Desktop Basics 17
Installing PGP Desktop 17
The PGP Desktop User Interface 18
Working with PGP Keys 18
Managing PGP Keys 18
Securing Email Messages 19
Securing Instant Messaging 19
Protecting Disks with PGP Whole Disk Encryption 19
Using PGP Virtual Disks 19
Using PGP NetShare 19
Using PGP Zip 19
Shredding Files with PGP Shredder 20
Storing Keys on Smart Cards and Tokens 20

Setting PGP Desktop Options 20
Working with Passwords and Passphrases 20
Using PGP Desktop with PGP Universal Server 20
Messaging with Lotus Notes and MAPI 20

Reference Documents 21

1 Purpose

The purpose of this document/assurance measure is to supplement the existing Target of Evaluation (TOE) documentation for the PGP® managed Whole Disk Encryption (mWDE) application. Conformance with this supplemental instruction, in addition to the applicable sections of the primary documentation, is intended to result in deployment and configuration of the TOE consistent with the *Common Criteria*[1] evaluated configuration identified in the PGP mWDE Security Target. This document satisfies the requirements of Common Criteria Assurance Measures, AGD_OPE.1 (Operational User Guidance) and AGD_PRE.1 (Preparative Procedures).

In This Chapter

Definitions..... 1
Acronyms..... 3

Definitions

Authorized User	Refer to the local user of the mWDE PGP application. Since authentication during bootup of the platform is required in order to access/decrypt the protected physical disk, this user is referred to as an authorized user.
Disk Access Key	Refers to a symmetric key created from the user passphrase/token used to encrypt the Link Key in the following decryption sequence – passphrase/token decrypts Disk Access Key which decrypts Link Key which is used to decrypt the (Disk) Session Key which decrypts disk data.

[1] Common Criteria is an Information Technology Security Evaluation program adopted by the National Information Assurance Partnership (NIAP). NIAP is collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NIAP has established the Common Criteria Evaluation Validated Scheme (CCEVS) to validate IT products. Common Criteria is also referred to as ISO 15408.

Link Key	Refers to a symmetric key used to link multiple disks within a single platform. Note role in decrypt sequence under Disk Access Key definition.
Managed WDE	Refers to the TOE application, which is the PGP Desktop platform with only PGP WDE enabled. The managed prefix indicates that it includes the ability to be remotely managed through a PGP Universal Server in the Operational Environment.
Partition Encryption	Refers to the encryption of a specific partition of the physical drive on the local platform by the TOE to one or more passphrases or cryptographic keys.
PGP Desktop	Refers to the portion of the PGP mWDE TOE software that executes as an application when selected following the Operating System boot process. The PGP Desktop is also a generic term used for the application from PGP corporation upon which PGP WDE executes.
PGP Universal Server	Refers to a server component within the Operational Environment which can be used to manage multiple instances of PGP mWDE TOE installations throughout the deployed network. Within the context of this ST this could be either a PGP Universal Server or the Generic Equivalent.
Pre-Boot	Refers to security functions or actions taken prior to the platform Operating System completes the booting process. The authentication process for the TOE occurs during this stage.
Post-Boot	Refers to security functions or actions taken following the platform Operating System completing the booting process.
Recovery Key	This refers to a secondary key, created without user intervention by the PGP SDK cryptographic module for use in the event the original passphrase used for whole disk encryption is forgotten. This key is stored in the Operational Environment within the PGP Universal Server.
Session Key	This refers to the symmetric key used by the TOE for whole disk or partition encryption. This key is encrypted by the Link Key.

Virtual Disk Encryption	Refer to the creation of a separate disk representation on the physical drive on the local platform of a specified size which is encrypted by the TOE to one or more passphrases or cryptographic keys. (excluded from TOE, CC evaluated configuration)
Windows	Refers to the Operating System component of the TOE: Microsoft Windows XP Professional SP2
Whole Disk Encryption	Refers to the encryption of the entire physical drive on the local platform to one or more passphrases or cryptographic keys by the TOE , requiring passphrase authentication at the Disk BIOS level to complete the boot process.
Whole Disk Recovery Token	Refers to a passphrase/token created by the mWDE TSF during whole disk/partition encryption operations. This produces an additional passphrase that can be used to access the physical drive or partition in the event the authorized user forgets the user created passphrase. This recovery passphrase/token is stored on the PGP Universal Server (or equivalent) in the Operational Environment.

Acronyms

3DES	Triple DES
AES	Advanced Encryption Standard
CC	Common Criteria
DES	Data Encryption Standard
DLL	Dynamic Link Library
FIPS	Federal Information Processing Standard
GUI	Graphic User Interface
mWDE	Managed WDE
NIST	National Institute (of) Standards & Technology
NTFS	NT File System (Windows File System)
OEAP	Optimal Asymmetric Encryption Padding
PGP	Pretty Good Privacy (and sponsor corporate name)

PIN	Personal Identification Number
RNG	Random Number Generator
RTF	Rich Text Format
SDK	Software Developers Kit
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSC	TOE Scope of Control
TSF	TOE Security Functionality
UI	User Interface (subsystem)
WDE	Whole Disk Encryption
WDRT	Whole Disk Recovery Token
XML	Extended Markup Language

2 PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10 supplement

This section supplements the PGP Whole Disk Encryption for Windows Quick Start Guide in accordance with AGD_PRE.1 Common Criteria Assurance Measure requirements.

Before you begin: The Users of the PGP mWDE application must review all associated documentation and guidance prior to proceeding with installation and use of the TOE application. All documentation and guidance can be found in the documents listed in *Reference Documents* (on page 21) in addition to this supplement.

In This Chapter

Receipt and preparation of TOE and Environment 5
Common Criteria Excluded Aspects 9
Verification of Common Criteria components 9
Usage Assumptions 10
Applicability of the PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10 10
Disabling features not applicable to the CC Evaluated Configuration 12
Verification of CC Evaluated installation 13

Receipt and preparation of TOE and Environment

Receipt

- The PGP mWDE TOE application is a subset of a PGP Desktop product installation and is acquired through a download from a secure server. The transfer of the file is made through an encrypted session. Upon receiving the downloaded file, Users should perform a Hash operation on the file to verify the provided SHA1 hash value using the following method:

Integrity checking of downloaded file

Complete the following steps to verify the files downloaded are not corrupted or modified prior to proceeding with installation:

1. Go to http://www.pgp.com/about_pgp_corporation/corporatekeys.html
2. Go to https://keyserver.pgp.com
   - **a** Search on 0xFA85D00F (PGP Corporation Release Key)
   - **b** Download above key as .asc format
3. Download and install GNUPG for platform of choice – GNUPG can be obtained from this location:

   http://www.gnupg.org/download/index.en.html
   http://www.gnupg.org/download/index.en.html

   The remaining steps describe Command Line instructions and return values provided by GNUPG.
4. Import public key from step 2B:

   ```
   % gpg --import key  key0x53691E61FA85D00F.asc
   ```

   ```
   gpg: key FA85D00F: public key "PGP Corporation Release Key <release-key@pgp.com> <mailto:release-key@pgp.com> " imported
   ```
5. Verify TOE, this example uses PGPDesktop991_Windows.zip

   ```
   % unzip PGPDesktop991_Windows.zip
   ```

   TOE unzips to:

   PGPDesktop991_Windows_Inner.zip

   PGPDesktop991_Windows_Inner.zip.sig

   ```
   % gpg --verify PGPDesktop991_Windows_Inner.zip.sig
   ```

   ```
   gpg: Signature made Mon 22 Dec 2008 02:31:27 PM PST using RSA key ID FA85D00F
   ```

   ```
   gpg: Good signature from "PGP Corporation Release Key <release-key@pgp.com> <mailto:release-key@pgp.com> "
   ```

   ```
   gpg: aka "PGP Corporation Release Key <re@pgp.com> <mailto:re@pgp.com> "
   ```

   ```
   gpg: aka "PGP Corporation PGP Universal Release Key 1.X"
   ```
6. This final step demonstrates that a change to a file within the zip results in a failed integrity check. Open up `PGPDesktop991_Windows_Inner.zip` and attempt to add/delete a file into/from the zip.
7. Verify the signature again to step 5.

   ```
   % gpg --verify PGPDesktop991_Windows_Inner.zip.sig
   ```

```
    gpg: Signature made Mon 22 Dec 2008 02:31:27 PM PST
using RSA key ID FA85D00F

    gpg: BAD signature from "PGP Corporation Release
Key <release-key@pgp.com> mailto:release-key@pgp.com"
```

If the "Good Signature" result is indicated above, the User is assured that the received product download is complete and unmodified.

Upon installation and entry of the applicable license key, the only PGP Desktop features provided will the the mWDE TOE application as specified for the Common Criteria Evaluation configuration.

Guidance documents required for installation and administration of the PGP mWDE TOE are downloaded separately from the application above but using the same essential process. The following guidance documents apply to the CC Evaluated configuration and should be downloaded and consulted prior to deployment of the TOE.

Guidance Documents

The following guidance documents are provided with the TOE upon delivery in accordance with EAL 4 requirements:

A *PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10.0*

B *PGP Desktop for Windows Quick Start Guide Version 9.10.0*

C *PGP® Desktop for Windows User's Guide, PGP Desktop Version 9.10*

D *PGP® Desktop: Managed Whole Disk Encryption Only Edition Version 9.10 Security Target EAL 4 augmented ALC_FLR.1*

E *PGP Universal Server Administrator's Guide*. PGP Universal Server Version 2.10.0 Released March 2009 – *only Chapter 26: Configuring PGP Desktop Installations*

PGP® Desktop Version 9.10.0 for Windows Release Notes

Environment preparation

- The PGP mWDE application should be installed on the following platform - evaluated as part of the Common Criteria Evaluated configuration:
  - **Hardware:** General purpose laptop or desktop capable of running Microsoft® Windows XP Professional SP2 (if Trusted Platform modules are used see table below for supported hardware)
  - **Operating System:** Microsoft Windows XP Professional SP2
- The following Operational Environment must be in place prior to installation in order to support the mWDE "managed" operations:

- Hardware:
- Hardware for PGP Universal Server as specified:
  http://www.pgp.com/products/universal_server/tech_specs.html
  http://www.pgp.com/products/universal_server/tech_specs.html

  or

  a General Purpose Server capable of running XML/SOAP commands to/from mWDE TOE installations

  and

  General Purpose Server for supporting Active Directory/LDAP authentication server (to support Universal Server enrollment process)
- USB Tokens/Smartcards (if applicable) – the following are supported by the mWDE TOE:

ActiveIdentity ActivClientCAC cards, 2005 models
Aladdin eToken 64K, 2048-bit RSA-capable1
Aladdin eToken PRO USB Key 32K, 2048-bit RSA-capable1
Aladdin eToken PRO without 2048-bit capability (older smart cards)1
Athena ASEKey Crypto USB Token for Microsoft ILM2
Athena ASECard Crypto Smart Card for Microsoft ILM2
EMC RSA SecurID SID800 Token3
Charismathics CryptoIdentity plug 'n' crypt Smart Card only stick
S-Trust StarCOS smart card4
Rainbow iKey 3000

- The following Trusted Platform Module systems are supported for use with the mWDE TOE application:

Hewlett-Packard Compaq nx6325 (Infineon TPM with HP BIOS)
Dell D630 (Broadcom TPM)
Lenovo ThinkPad T60 (Atmel TPM)
Fujitsu LifeBook T2010, (Infineon TPM with Phoenix BIOS)
Panasonic Toughbook T5, W5, or Y5 (Infineon TPM with Matsushita BIOS)

- Software:

  PGP Universal Server 2.10 software *or*

  Generic implementation: OS support capable of running a Web Server to host XML/SOAP - gSOAP toolkit 2.7.10

  - Authentication Server OS: Windows Server 2003 Active Directory R2 Standard, Enterprise or Datacenter edition (AD/LDAP)

- Associated software for supported Trusted Platform Modules listed in hardware above
- Associated software for supported Token/Smartcards as listed above.

Common Criteria Excluded Aspects

The following functions related to PGP Desktop and the mWDE TOE application are excluded from the Common Criteria Evaluated configuration and therefore should not be enabled or used for a Common Criteria deployment:

- mWDE application software updates pushed from the PGP Universal Server in the Operational Environment
- Bypass Feature
- PGP Zip
- PGP Shredder
- PGP Virtual Disk
- USB removable drive encryption
- Recovery Disk (decrypts WDE protected drive)

Verification of Common Criteria components

The following are authorized devices for the Common Criteria Evaluated configuration. Assure that installation processes resulting in the following Common Criteria Evaluated configuration:

TOE software:

PGP Desktop for Windows Version 9.10: Enterprise Whole Disk Encryption only edition

Operational Environment:

Operational Environment components as listed in *PGP® Desktop Version 9.10.0 for Windows Release Notes* (on page 7): Environment Preparation (per the applicable approach – PGP Universal Server or Generic Open version)

Note: Physical protection must be afforded to all Operational Environment resources, including the PGP Universal Server as stated below:

- The PGP Universal Server is located in a physically secure server room environment.

Usage Assumptions

The Common Criteria Evaluated Configuration requires the following assumptions be supported in usage of the mWDE TOE application. These assumptions should be assured either through facility or procedural provisions.

- Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
- The Operational Environment shall provide an accurate time source for use in time stamps.

Applicability of the PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10

The follow section identifies aspects of the mWDE Quick Start Guide that do not apply to the Common Criteria Evaluated configuration due to exclusions as listed in *Common Criteria Excluded Aspects* (on page 9). These aspect are identified by an IGNORE designation indicating that these aspects of the applicable manuals should be ignored for a Common Criteria deployment. It may be assumed that any items not listed here as exceptions apply as written.

What is PGP Whole Disk Encryption?

IGNORE the following references which relate to features not supported for Common Criteria:

- Use part of your hard drive space as an encrypted virtual disk volume with its own drive letter.
- Create secure, encrypted Zip archives.
- Put files and folders into a single encrypted, compressed package that can be opened on Windows systems that do not have PGP Desktop Email or PGP Desktop installed.
- Completely destroy files and folders so that even file recovery software cannot recover them.
- Securely erase free space on your drives so that your deleted data is truly unrecoverable.
- References to USB Encryption, which is excluded from the CC evaluated configuration.

What Am I Installing?

IGNORE references in this section to:

- PGP Virtual Disk volumes
- PGP Zip
- PGP Shredder
- Key Management
- USB Encryption

Note: The "Installing PGP Whole Disk Encryption" section applies in its entirety to the Common Criteria Evaluated Configuration; however, the following features must be disabled using the PGP Universal Server (or equivalent) as described in *Disabling features not applicable to the CC Evaluated Configuration* (on page 12).

- PGP Zip
- PGP Shredder
- PGP Virtual Disk
- USB removable drive encryption

System Requirements

IGNORE references in this section to any OS other than:

- Microsoft Windows XP Professional SP2 (the only OS evaluated as part of Common Criteria)

Create a Recovery CD

IGNORE this section in its entirety

Creating PGP Virtual Disk Volumes

IGNORE this section in its entirety

Creating a PGP Zip Archive

IGNORE this section in its entirety

PGP Self-Decrypting Archive

IGNORE this section in its entirety

Using PGP Shredder to Shred Files

IGNORE this section in its entirety

Shredding Free Space

IGNORE this section in its entirety

Disabling features not applicable to the CC Evaluated Configuration

The following procedure disables features that are excluded from the CC Evaluated Configuration including:

- PGP Zip
- PGP Shredder
- PGP Virtual Disk
- USB removable drive encryption

Exporting Policy from PGP Universal (or Equivalent)

Review the following reference prior to completing the configuration instructions for mWDE listed below:

PGP Universal Server Administrator's Guide PGP Universal Server – Chapter 26 "Configuring PGP Desktop Installations" only. This section describes the process of creating policies that can be pushed to mWDE TOE installations, including disabling features.

Windows Managed WDE Feature Settings for Common Criteria Environments

PGP Desktop settings can be established using the PGP Universal Server (or equivalent) for the default internal user policy as well as any custom internal user policy you create. Each of these can have different sets of PGP Desktop settings.

To establish PGP Desktop settings resulting in the mWDE TOE CC Configuration:

1. From the PGP Universal Server, on the Internal User Policy card, click the name of the Internal Users: Default policy or a custom internal user policy.

   The Policy Options card appears.

2. Click the Edit button for PGP Desktop Settings.

   The appropriate PGP Desktop card appears, titled with the policy name.

   - Disable PGP Zip
     - From the PGP Desktop card, select File & Disk.
     - Deselect PGP Zip to disable the PGP Zip feature; it will not appear in the PGP Desktop user interface and it will not be available to your users.
   - Disable PGP Shredder
     - From the PGP Desktop card, select File & Disk.
     - Deselect PGP Shredder to disable the PGP Shredder feature; it will not appear in the user interface and it will not be available to your users.
   - Disable PGP Virtual Disk
     - From the PGP Desktop card, select File & Disk.
     - Deselect PGP Virtual Disk to disable the PGP Virtual Disk feature; it will not appear in the PGP Desktop user interface and it will not be available to your users.
   - Disable USB removable drive encryption
     - From the PGP Desktop card, select WDE.
     - Deselect all removable disk options from the User-Initiated Whole Disk Encryption Permissions function.
     - Do not select Enable automatic encryption or locking of removable devices.

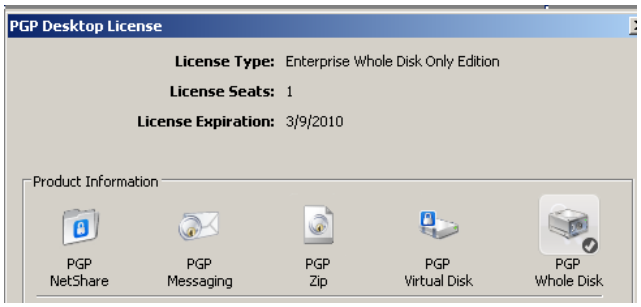
Verification of CC Evaluated installation

Upon following the aforementioned steps, the TOE application should be limited to the Whole Disk Encryption function. The PGP Keys portion of the GUI will be shown but is excluded from the Evaluated configuration and therefore should not be used as a matter of local policy. In addition, creation/use of a Recovery Disk and the Bypass feature is disallowed for the CC Evaluated configuration and should be restricted based on local policy.

Verification:

Upon launching the TOE application, open the Help menu and select the License option. The displayed License should state: License type: "Enterprise Whole Disk Only Edition". The icons shown below this License information should indicate the following:

- PGP Netshare – deselected, no check box (disabled)
- PGP Messaging - deselected, no check box (disabled)
- PGP ZIP - deselected, no check box (disabled)
- PGP Virtual Disk - deselected, no check box (disabled)
- PGP Whole Disk– selected, checkbox (enabled)



Verify that the PGP Shredder ICON is *not* on the Desktop and operational

3 PGP Desktop for Windows User's Guide

This section supplements the PGP Desktop for Windows User Guide in accordance with AGD_OPE.1 Common Criteria Assurance Measure requirements.

In This Chapter

Applicability of the PGP Desktop for Windows User's Guide 16

Security Audit for the PGP mWDE TOE

The TOE provides two levels of logging within the application. Logs are generated during Whole Disk Encryption events, changes to settings within the application and for authentication activities. The local logs provide a limited set of information available to the local user. A more detailed set of logs related to local use of the mWDE TOE are sent to the PGP Universal Server in the Operational Environment for review by the Universal Server Administrator. The local logs can be reviewed by selecting the Tools Menu and choosing "View Log" from the pull down menu. Logging can be disabled locally by un-checking the Enable Logging item on the list as shown below. Logs are still generated and sent to the PGP Universal Server regardless of this selection. It is recommended that users periodically review audit logs to be able to notice unauthorized access attempts or other potentially malicious activity.

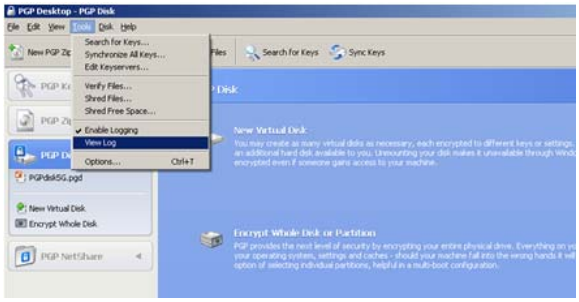
Protection of Audit logs

Audit logs processed from the mWDE TOE to the Universal Server (or equivalent) are managed using that resource in the Operational Environment. The PGP Universal Server does not have a separate log storage allocation; therefore, the full disk storage area is available for storage of logs. Universal Server Administrators should monitor drive space to assure adequate space remains for operational of the server as well as for the storage of logs. Logs may be exported to additional storage resources and deleted on the Universal Server using a command-line utility. The following reference describes logging on the Universal Server:

PGP Universal Server Administrator's Guide, PGP Universal Server Version 2.10

Audit logs processed on the local (client) machine are stored in application files that support the PGP application in a text format. Each day a separate text file is created for storing logs created on that day. These files are rotated among 7 text files, therefore, after 8 days local log records are overwritten. Given these retention restrictions, TOE operation could not result in a condition where disk space supporting the application or log generation could be depleted even given constant use.

These log files are also passed to the Universal Server where they may be archived beyond the 7 day limit. Local users wishing to review log files should verify contents within a 7 day period in the event unusual activity indicates a potential security event.



Details about viewing logs directly on the PGP Universal Server are included in the following reference but are outside the Scope of the CC Evaluation:

- *PGP Universal Server Administrator's Guide*. PGP Universal Server Version 2.10. Released March 2009

Applicability of the PGP Desktop for Windows User's Guide

The following section identifies aspects of the PGP Desktop for Windows User's Guide that do not apply to the Common Criteria Evaluated configuration due to exclusions as listed in *Common Criteria Excluded Aspects* (on page 9). These aspect are identified by an IGNORE designations indicating that these aspects of the applicable manuals should be ignored for a Common Criteria deployment. It may be assumed that any items not listed here as exceptions apply as written.

About PGP Desktop 9.10 for Windows

What's New in PGP Desktop for Windows Version 9.10:

- IGNORE references to PGP NetShare

- IGNORE references to PGP Messaging
- IGNORE references to PGP Virtual Disk volumes
- IGNORE references to PGP Shredder
- IGNORE references to PGP Zip

PGP Desktop Basics

PGP Product Components:

- IGNORE references to Mac OS X (not supported for CC Evaluated Configuration)
- IGNORE references to PGP Messaging
- IGNORE references to PGP NetShare
- IGNORE references to PGP Virtual Disk volumes
- IGNORE references to PGP Shredder
- IGNORE references to PGP Zip
- IGNORE reference to USB drive encryption

Using PGP Desktop for the First Time:

- IGNORE all Steps 1 – 9 as they are redundant to existing WDE installation guidance and include PGP Messaging references. PGP Messaging is excluded from the CC Evaluation.

The following feature descriptions should be IGNORED as they are not supported by the TOE:

- Use PGP Virtual Disk to create a secure "virtual hard disk."
- Use PGP Zip to create compressed and encrypted PGP Zip archives.
- Use PGP Shredder to delete sensitive files that you no longer need..
- Use PGP NetShare to share files and folders securely and easily among any number of people—with maximum access control.

Installing PGP Desktop

System Requirements:

- IGNORE references that specify Operating Systems other than Microsoft Windows XP Professional SP2

Citrix and Terminal Services Compatibility:

- This section does not relate to the Common Criteria Evaluated configuration – IGNORE

Upgrading the Software:

- This section does not relate to the Common Criteria Evaluated configuration – IGNORE

Upgrading From Standalone to Managed PGP Desktop Builds:

- This section does not relate to the Common Criteria Evaluated configuration – IGNORE

Note: The "Installing PGP Desktop" section above applies in its entirety to the Common Criteria Evaluated Configuration; however, the following features must be disabled using the PGP Universal Server (or equivalent) as described in *Disabling features not applicable to the CC Evaluated Configuration* (on page 12).

- PGP Zip
- PGP Shredder
- PGP Virtual Disk
- USB removable drive encryption

The PGP Desktop User Interface

The PGP Desktop Main Screen:

- Note there may be reference made in this section that related to features that are disabled for the mWDE Common Criteria Evaluated configuration.

PGP Desktop Notifier alerts:

- IGNORE references in this section related to Messaging, Incoming & Outgoing Email messages, PGP NetShare and instant messaging as these features are not included in the CC Evaluated configuration.

Working with PGP Keys

IGNORE references that describes DH/DSS key generation – this does not apply to the TOE

Managing PGP Keys

IGNORE references Importing Keys from Certificates, Sign/Verify Operations, Shamir Secret Sharing and Key Reconstruction functionality which does not apply to the TOE.

Securing Email Messages

This section should be IGNORED in its entirety as this feature in not included in the mWDE CC evaluated configuration.

Securing Instant Messaging

This section should be IGNORED in its entirety as this feature in not included in the mWDE CC evaluated configuration.

Protecting Disks with PGP Whole Disk Encryption

IGNORE references related to the following functions which are not part of the CC Evaluation:

- USB Flash Encryption
- Public Key Authentication
- removable disk encryption
- Recovery Disk

Note: In this section the following suggestion is made regarding entering password characters during login – "To see the characters you type, press Tab before you begin typing." This is not recommended for the Common Criteria Evaluated configuration as it could allow passers-by to view your password entry.

Using PGP Virtual Disks

This section should be IGNORED in its entirety as this feature in not included in the mWDE CC evaluated configuration.

Using PGP NetShare

This section should be IGNORED in its entirety as this feature in not included in the mWDE CC evaluated configuration.

Using PGP Zip

This section should be IGNORED in its entirety as this feature in not included in the mWDE CC evaluated configuration.

Shredding Files with PGP Shredder

This section should be IGNORED in its entirety as this feature in not included in the mWDE CC evaluated configuration.

Storing Keys on Smart Cards and Tokens

This section relates to the mWDE TOE in its entirety.

Setting PGP Desktop Options

The following sections of this appendix should be IGNORED as they related to features that are not included in the CC Evaluated configuration:

- Messaging Options
- Proxy Options
- PGP NetShare Options
- Disk Options: PGP Virtual Disk Options
- Disk Options: PGP Shredder Options
- Notifier Options: all uses except related to Whole Disk Encryption

Working with Passwords and Passphrases

This section relates to the mWDE TOE in its entirety.

Using PGP Desktop with PGP Universal Server

This section relates to the mWDE TOE in its entirety.

Messaging with Lotus Notes and MAPI

This section should be IGNORED in its entirety as this feature in not included in the mWDE CC evaluated configuration.

A Reference Documents

A *PGP Whole Disk Encryption for Windows Quick Start Guide Version 9.10*

B *PGP® Desktop for Windows User's Guide, PGP Desktop Version 9.10*

C *PGP® Desktop: Managed Whole Disk Encryption Only Edition Version 9.10 Security Target EAL 4 augmented ALC_FLR.1*

D *PGP Universal Server Administrator's Guide*. PGP Universal Server Version 2.10.0 Released March 2009 – *only Chapter 26: Configuring PGP Desktop Installations*