Universal Server 30 Day Whole Disk Evaluation Quick Start Guide

Welcome to the PGP Universal[™] Server Whole Disk Encryption evaluation program! In the following documentation you will find information to help you integrate PGP Universal[™] Server into your enterprise environment.

This document covers the following topics:

- 1. The PGP Universal Evaluation Email
- 2. Downloading and Burning an ISO image of the Universal OS
- 3. Initial install and Universal settings configuration
- 4. Basic overview of the Universal OS
- 5. Integration with Active Directory
- 6. Desktop Client Policy and Licensing
- 7. Creation and Deployment of a PGP Desktop Client
- 8. Whole Disk Encryption Client Install and Enrollment

The guide is designed for the individual looking for a basic understanding of the PGP Universal[™] Server Product so it can be evaluated in their production/test environment.

Table of Contents

Table of Contents	2
Table of Figures	3
The PGP Universal Evaluation Email	5
The Universal [™] Server ISO Image	6
Downloading the PGP Universal ISO	6
Burning The Universal ISO	9
PGP Universal [™] Server Installation and Configuration	10
Installing From the Universal DVD	10
Basic Overview of the Universal OS	22
Integration with Active Directory	25
PGP Desktop Client Policy	31
About the Single Sign On Feature	31
Using Single Sign On	31
Logging In with Single Sign On	31
How Single Sign On Works	31
Configuring PGP Desktop Client Policy	31
Creation and Deployment of a PGP Desktop Client	39
Whole Disk Encryption Client Install and Enrollment	40

Table of Figures

Figure 1: PGP Evaluation Email	5
Figure 2: Download Link	6
Figure 3: Download Website	6
Figure 4: Download Button	7
Figure 5: Universal Evaluation Download	7
Figure 6: Contents of PGPUniversalWebFull.zip file	7
Figure 7: PGP Universal Zip	7
Figure 8: ISO Image	8
Figure 9: CD Recording Wizard	9
Figure 10: Bios Setup Utility screen	10
Figure 11: Setup Boot Screen	10
Figure 12: Network Configuration Settings	11
Figure 13: Miscellaneous Network Settings	11
Figure 14: Hostname Configuration screen	12
Figure 15: Universal Install Progress	12
Figure 16: Universal [™] Server fully booted	13
Figure 17: SSL Certificate Warning	14
Figure 18: Welcome to your PGP Universal Server!	14
Figure 19: End User License Agreement	15
Figure 20: Universal Setup Type	15
Figure 21: Date & Time	16
Figure 22: Network Setup	16
Figure 23: Proxy Configuration	17
Figure 24: Settings Confirmation	17
Figure 25: Network Changes Notification	18
Figure 26: Server License	18
Figure 27: Administrator Information	19
Figure 28: Managed Domain	20
Figure 29: Directory Server	20
Figure 30: Ignition Kevs	21
Figure 31: Backup Organization Key	21
Figure 32: PGP Universal [™] Server Confirmation	22
Figure 33: Universal Administration login screen	23
Figure 34: Welcome Screen	23
Figure 35: System Overview	24
Figure 36: Consumers Groups	24
Figure 37: Consumer Policy	25
Figure 38: Directory Synchronization	25
Figure 39: Directory Synchronization	26
Figure 41: Directory Synchronization – AD Hostname entered	27
Figure 44: Directory Synchronization – Sample Records	28
Figure 45: Directory Synchronization – Settings	29
Figure 46: Directory Synchronization Settings	29
Figure 48: Internal User Policy screen	30
Figure 49: Consumer Policy	32
Figure 50: Default Policy	32
Figure 52: PGP Desktop Settings	33
	-

Figure 52: PGP Desktop Settings	34
Figure 53: SSO Policy	35
Figure 54: Standard Passphrase User	36
Figure 49: Consumer Policy	37
Figure 55: PGP Desktop License Options	38
Figure 56: Desktop License	38
Figure 57: Groups	39
Figure 58: Download PGP Clients	39
Figure 59: Mail Server Binding	40
Figure 60: PGP MSI	40
Figure 61: End User License Agreement	41
Figure 62: Release Notes	41
Figure 63: Restart System	42
Figure 64: PGP Enterprise Enrollment	42
Figure 65: Enrolling	43
Figure 66: User Type	43
Figure 67: Encryption Assistant	44
Figure 68: Passphrase Assignment	44
Figure 69: Complete the enrollment	45
Figure 70: Congratulations	45
Figure 71: PGP Boot Guard	46

The PGP Universal Evaluation Email

The evaluation email will be sent to the address you specified to the PGP Sales Representative during the initial product evaluation communication.

Evaluation emails come from <u>do-not-reply@pgpstore.com</u> and have a subject that will look something like this: "PGP Order Confirmation: 921117 ::ED51PN7DX8::". The email will also contain a PDF attachment with your Evaluation Summary as well as a link from which you will download the Universal[™] Server ISO image.

The first set of numbers shown in the Subject after the word 'Confirmation:' is your order number and will be unique to your Evaluation. In the example shown, the order number would be 921117.

The Evaluation email you will receive looks like the message shown below:

PGP Order Confirmation: 921117 ::ED51PN7DX8:: do-not-reply@pgpstore.com
You forwarded this message on 8/6/2007 4:56 PM.
To: do-not-reply@pgpstore.com; Marco Genovese
Attachments: 🗾 order921117-2007-08-06-15-52-49.pdf (4 KB)
Ref: PGP
Attached please find:
- A summary of your order - License numbers (needed for product installation)
You may download your product from this location:
http://orders.pgp.com/cgi-bin/WebObjects/download.woa/wa/confirmation?oid=921117- ed7cbbefa7165e6c293caeead4e1ab83

Figure 1: PGP Evaluation Email

The Universal[™] Server ISO Image

PGP Universal[™] Server is a soft appliance designed from the ground up as an encryption platform. It may run on a number of hardware platforms, and as such is delivered to you as an ISO image. PGP Universal[™] is its own Operating System, and once loaded onto dedicated hardware it completely takes over the host machine. Since it is an OS it needs to be written to CD media in a specific format so it is bootable. The ISO standard allows for this to be done with the least end user effort. The steps that follow will explain how to download the ISO image and then burn it to DVD media from an ISO.

Downloading the PGP Universal ISO

- **1. Open the Evaluation Email** that you received and was referenced in the previous chapter.
- 2. Click on the link to download the software as seen below.



Figure 2: Download Link

3. On the web page that opens you will see many options and items as in the example below.

PGP	Products Purchase Downloads Support Partners Nev	vsroom Company Careers Cont
Customer and Order	Information	Helpful Links
Order #956563	Fulfilled on October 08, 2007.	<u>Customer Service</u> <u>Technical Support</u> <u>Help With</u> Licensing Your
Purchased by	Purchased through	Product
PGP Marco Genovese mgenovese@pap.com		 Visit PGP Knowledge Base and Support Site
11778 Election Dr. Draper, UT 54121 United States		How to
		Droduct
Product Bownload O SKU: QEA Evaluation	f PGP Universal Gateway Email 2.6 D11X5 License	NOTE: If you have purchased multiple seats, you will need to enter the identical name, organization and license number in the product dialog botalierion. Inter nally to a very containation
Bownload O SkU: QEA	f PGP Whole Disk Encryption 9.6 for D2GX1 ay: DU970-BUTQC-ZG6DZ-FGKX6-5GE7V-JBA	You may distribute PGP software up to the number of seats purchased. For licensing multiple seats, we suggest the user name: "Authorized User"
Evaluation	ure 3: Download Website	3

4. Press and hold the **Ctrl** key on your computer and **Click the Download button** for the Universal Server as pictured below.

Download O	10 seats of PGP Universal Server 2.6
Download	SKU: QEAD10X5

Figure 4: Download Button

5. The following screen will then display prompting you to save the PGPUniversalWebFull.zip file.

File Dow	nload 🛛 🔀
Do you	want to open or save this file?
	Name: PGPUniversalWeb263Full.zip Type: zip Archive, 748MB From: download.pgp.com
☑ Al <u>w</u> a	Open Save Cancel
?	While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. <u>What's the risk?</u>

Figure 5: Universal Evaluation Download

6. Save the PGPUniversalWebFull.zip file to a location of your choice. *Do not choose the Open option.* Save the file where you can easily find it, such as the "My Documents" folder.

Now you are ready to open the PGPUniversalWebFull.zip file.

7. Double-Click on the folder PGPUniversalWebFull.zip to display the contents of the archive, as shown in the example below.

Name	Size	Packed Size	Modified
PGPUniversalWeb263Full_Inner.zip	748 M	748 M	2007-08-13 11:29
PGPUniversalWeb263Full_Inner.zip.sig	280 B	280 B	2007-08-13 11:29

Figure 6: Contents of PGPUniversalWebFull.zip file

8. **Double-Click** on the PGPUniversalWebFull_Inner.zip. You will now see folders and files similar to the example below.

Name	Size	Packed Size	Modified
Documentation	0 B	0 B	2007-08-13 11:24
DAP Server Schemas	0 B	0 B	2007-08-13 11:24
Desktop	0 B	0 B	2007-08-13 11:27
DGP Universal Satellite	0 B	0 B	2007-08-13 11:27
DGP Universal Server	0 B	0 B	2007-08-13 11:25
🖉 Read Me.htm	58 K	11 K	2007-08-13 11:24
Cucense.htm	72 K	14 K	2007-08-13 11:24

Figure 7: PGP Universal Zip

9. Double-Click on the **PGP Universal Server folder** and your window should display contents similar to what is shown below.

M 559 M	2007-08-13 11:25	
) B 280 E	2007-08-13 11:25	
3	3 M 559 M D B 280 E	M 559 M 2007-08-13 11:25 D B 280 B 2007-08-13 11:25

Figure 8: ISO Image

10. Drag the **PGPUniversalServer.iso** file out of the zip folder **to your computer's desktop** or other location of your choice. At this time the ISO will extract; once the ISO image is completely extracted continue to the next step.

Burning The Universal ISO

Note: Make sure that you have a writable DVD upon which the ISO will be burned.

Note: Be sure you have burning software capable of handling ISO images. Roxio, Nero and others will be able to do this task. If you do not have software of this nature you can download ISO Recorder V2 free of charge to accomplish the task. ISO Recorder V2 is available <u>here</u>.

The instructions shown on the following pages were created using ISO Recorder V2. The steps you would take using other DVD Burning software will be similar.

1. **Right-Click on** the **PGPUniversalServer.iso** and choose the option to open with ISO Recorder. You will be greeted with a screen like the one below.

CD Recording Wizard		E
Ð	Source ③ Image file 〇 CD	C:\Documents and Settings\mgenovese\
	Recorder Properties	
		No recorder selected
		Cancel Next Finish

Figure 9: CD Recording Wizard

2. On the Recorder drop-down **select the DVD drive** you wish to burn to, **Click** and then .

The ISO will be burned to the DVD making it bootable and ready for installation.

PGP Universal[™] Server Installation and Configuration

PGP Universal[™] Server installs just like any other OS and requires some basic initial setup and configuration. In this section we will cover the installation of the Universal[™] Server and initial settings that need to be configured.

Installing From the Universal DVD

1. Insert the Universal disc into the computer's DVD-ROM drive and make sure that the BIOS is set to boot from DVD-ROM first as shown below:



Figure 10: Bios Setup Utility screen

Boot your computer from the DVD-ROM device. Once you have booted from the DVD-ROM you will see a screen like the one shown below.



Figure 11: Setup Boot Screen

2. Press the Enter key to load Universal[™] Server.

You will hear the DVD-ROM drive spin as the Universal image is loaded. After Universal has finished loading you will be greeted with the Network Configuration screen, as shown below. Here you input the IP and Netmask information for the Universal[™] Server in *your* network.

PGP Universal (C) 20	07 PGP Corporation
	Network Configuration for eth0 Network Device: eth0 Hardware Address: 00:0C:29:6D:71:C6 IP Address Netmask
	OK Back

Figure 12: Network Configuration Settings

3. Enter the IP Address and Netmask values for your Universal[™] Server in dotted decimal format.

Use the **Tab** key to navigate among the fields and **Click** to continue.

The Miscellaneous Network Settings screen displays as shown below



Figure 13: Miscellaneous Network Settings

4. Enter the information as it pertains to your network and Press

You will see the Hostname Configuration screen display, as shown below.

PGP Univ	ersal (C) 2007 FGP Corporation
	Hostname Configuration Enter the hostname for your system. This shouldbe a fully qualified domain name (FQDN) such as 'keys.mycompany.com'. Hostname:
	Back

Figure 14: Hostname Configuration screen

5. Enter the Domain Name (FQDN) for Universal[™] Server and Click

Universal[™] Server will begin to format and install on your hardware with the settings you specified. Your display will look similar to the one below while this occurs:

Name : rpm-libs- Size : 2028k Summary: Libraries	Package Installat 4.4.1-23-i386 for manipulating	ion	jes.
	0%		
	Packages	Bytes	Tim
Total :	284	1248M	0:02:1
Completed: Remaining:	213	363M 885M	0:00:3
_	29%		

The installation is self-completing and the DVD may not be removed until universal is done loading on the hardware. When the Universal[™] Server has booted fully after installing you will see the following screen:



Figure 16: Universal[™] Server fully booted

You may now access Universal[™] Server at the IP you specified (it also displays on the root screen) on port 9000. Once you connect to the Universal you can finish the setup process.

6. From another PC that has IP connectivity to Universal[™] Server open a web browser and navigate to the following URL:

https://<IP_Address_of_Universal>:9000

7. If you receive a security warning like the one shown below Click
 ^{Some Continue to this website} as you are receiving this message because the Universal[™] Server does not yet have a valid SSL Certificate.



Figure 17: SSL Certificate Warning

You will now see the welcome screen as seen below.

8. Click the button.

	Benvenuti _{欢迎}
	歡 迎 Bienvenue Welcome
T	Willkommen ようこそ
11	Welcome to your PGP Universal Server!
	As this is the first time you have connected to this PGP Universal Server, we need to ask a few questions to get you up and running.
	We will use your answers to configure many of the settings on this PGP Universal Server. You can modify these and other settings at any time once setup is complete. Click the Forward button to proceed.

Figure 18: Welcome to your PGP Universal Server!

9. Read and Click the button to continue.



Figure 19: End User License Agreement

The Setup Type screen will display as shown below.



Figure 20: Universal Setup Type

10. Select "Primary" and **Click**

The Date and time screen will display.

	Date & Time
Please enter the ti If you specify a Ne to connect to it on	ime zone, date, and current time where the PGP Universal Server is located, twork Time Protocol (NTP) server here, your PGP Universal Server will attempt ze the setup is complete.
Time Zone:	US/Mountain
	The offset chosen above will be applied to the time acquired from the NTP server.
Time Format:	AM/PM 💌
Date Format:	Mon Dec 3, 2007 (12/03/2007) 💌
Time:	1 💌 :01 💌 AM 💌
Date:	December 💙 4 💙 2007 🗸
1	The time and date specified will be applied to the PGP Universal Server if an NTP server cannot be contacted.
NTP Server:	time.pgp.com
	Optional. Leave this field blank if you do not want to connect with a time server.

Figure 21: Date & Time

11. Adjust the date and time as required and **Click**

The Network Setup screen will display, as shown below.

	Network Setup
You already entere changes, you may	ed network information during the installation process. If you wish to make do so now. Otherwise press Forward to continue with these settings.
Hostname:	keys.senderdomain.com
	This is the externally addressable name of the PGP Universal Server. We recommend naming your PGP Universal Server according to the "keys.domain" convention (e.g. keys.example.com).
IP Address:	192.168.90.151
Subnet Mask:	255.255.255.0
Gateway:	192.168.90.1
DNS Servers:	192.168.90.150
	These are the DNS servers on your network that your PGP Universal Server can access. Enter one DNS server per line.
	(4)P

Figure 22: Network Setup

12. Enter the appropriate values for each of the fields and **Click**

The Proxy Configuration screen will display.

PGP [°] Universal Administration Setup	
	Proxy Configuration
If your PGP Univers necessary to conta	al Server does not have a direct internet connection, a proxy server may be ct PGP for licensing authorization and automatic system updates.
Hostname/IP:	Port:
Username:	
Passphrase:	
	Skip

Figure 23: Proxy Configuration

13. If your network uses a Proxy Server to connect to the internet, enter the appropriate data and **Click** . Otherwise, **Click** .

The Confirmation screen will display.

PGP [*] Universal Administration Setup	
	Confirmation
Here are the settings you established for your PGP Universal Server:	
Setup Type: Primary Server PGP Universal Hostname: keys.senderdomain.com IP Address: 192.168.90.151 Subnet Mask: 255.255.255.0 Gateway: 192.168.90.1 DNS Servers: 192.168.90.150 Date & Time: Synchronized with NTP server time.pgp.com Proxy Configuration: Not Entered	
Click Done to confirm these settings and complete the setup. Use the f make changes, if necessary.	Back button to go back and

Figure 24: Settings Confirmation

14. Review your configured settings for accuracy then **Click** to write the changes to Universal[™] Server.

While PGP Universal[™] Server implements its configuration changes a notification will display like the one shown below.



Figure 25: Network Changes Notification

Please wait until the Licensing Screen displays.

PGP		Licensing
	Your PGP Universal Server requires a valid license. If you w Manual and paste it into the License Authorization box. If yo address, use your own. Click Skip to enter this information	vere sent a license authorization, click ur license does not include an email later.
	Licensee Name:	
	Licensee Organization:	
	Licensee Email:	
	License Number:	
	Manual Skip	

Figure 26: Server License

15. Input the license information from PGP, example as follows:

License Name: John Doe License Organization: ACME License Email: jdoe@acme.com License Number: DVWX7-EH6QP-KEKL5-4XPD9-JQLBG-3PC

NOTE: You must enter the license info *exactly* as it was sent you in the email message. On the original page from which you downloaded the Universal[™] Server software you may also perform a manual authorization of your license.

If you do not have internet connectivity you mill need to perform a manual authorization. To do this, simply **Click** the Manual button and input the license authorization information.

Click to continue and the Administrator Name and Password screen will display.

1	<i>¶</i>	Administrator Name & Passphrase
A HA	Please establish a login PGP Universal Server. N administrator permissio	n name and passphrase to protect the administrative interface of your /ou will be able to configure additional administrator accounts and adjust ons after initial setup is complete.
	🚊 Login Name:	admin A login name is typically 5 to 10 characters long and cannot contain spaces or other non-alphanumeric characters.
	Passphrase:	
	Confirm:	A passphrase is longer than a password and is typically something that no one but you will be able to guess or remember. You can use spaces and non-alphanumeric characters such as *, -, and ~ in your passphrase.
	Email Address:	Optional. Daily status messages and alerts will be sent to this email address.

Figure 27: Administrator Information

16. Enter a Login Name and Passphrase that you will remember. You may optionally enter an email address which will receive the daily status email messages. When complete **Click .**

The Managed Domain screen displays.



Figure 28: Managed Domain

17. Enter your domain name (FQDN) and **Click**

The Directory Server screen displays.

l ion Setup
Directory Server
If your organization uses an LDAP directory server (such as Microsoft Active Directory), PGP Universal Server can query this directory to obtain certain information about your internal users and mailing lists.
Enter the IP address or the fully qualified hostname of the directory server. If you do not want to configure a directory server, click the Skip button to continue.
Directory Server:
Directory Type: Active Directory
Skip (

Figure 29: Directory Server

18. Enter the name of your Active Directory server for AD integration or the name of your Open LDAP server. If you are not sure of the name you can contact your network administrator who should have this information.

.

When complete Click

The Ignition Key screen displays.

PGP Universa	tion Setup	
		Ignition Keys
	To protect your PGP Univ physical access to the se Key's token or passphras	ersal Server's confidential information from an attacker who gains erver, you may configure an Ignition Key. Once configured, the Ignition se is required for PGP Universal services to be available on startup.
1971	If you would like to config Forward. Click Skip to by	ure an Ignition Key for your PGP Universal Server, select a type and click pass this option.
	0 9 :	Hardware Token Ignition Key The private key is stored on a PKCS11 token. You will need to have a token ready with a suitable PGP key generated on it. Consult the Administrator's Guide for more details.
	•	Soft-Ignition Key With Passphrase This option will require the Administrator to provide a special passphrase upon starting the server.
		(Skip)

Figure 30: Ignition Keys

19. For this evaluation we recommend that you skip this step. **Click** . The Backup Organization Key screen displays. This is where you create the key to which all backups and the Universal secure areas are encrypted.

PGP Universal Administratio	n Setup		
A	y	Backup Organization Key	1
	We strongly recom critical to your PGF sign the keys for y onto a fresh PGP I	nmend that you back up your Organization Key now. Your Organization Key is P Universal Server. It represents the identity of your organization, and is used to our Internal Users. You will also need this key later to restore your backups Jniversal Server.	
	Enter an optional (passphrase and click Backup Key.	
	Passphrase:		
	Confirm:	Optional. This encrypts the copy of the Organization Key you're about to download.	
		Backup Key	

Figure 31: Backup Organization Key

20. Enter a password that you will not forget.

You may click Backup Key to save a copy of your Backup Key for future restore functions. Make sure and save this key to a secure location. **Click** to continue. The Confirmation screen displays.

PGP Universal Administration Setup	
	Confirmation
Here are the settings you established in Setup Type: Primary Server License: Not Entered Admin Login Name: admin Mail Processing Placement: G Mail Server Primary Domain: s Mail Server Hostname: mail.se Directory Server: Not Entered Ignition Key: Not Created	for your PGP Universal Server: ateway ienderdomain.com inderdomain.com
Click Done to confirm these settings a make changes, if necessary.	nd complete the setup. Use the Back button to go back and

Figure 32: PGP Universal[™] Server Confirmation

21. Click on the Confirmation screen.

You are now finished with the initial setup!

Please wait for the PGP Universal Logon Screen to appear.

Basic Overview of the Universal OS

In this section we provide an overview of the Universal[™] Server Operating System as a whole and the different relevant navigational tabs presented in the GUI.

PGP Universal[™] Server provides an HTTPS-based GUI for its administration. The first time you login to Universal[™] Server you will be greeted with a logon screen asking for your Administrator Credentials that we set up earlier.

1. From a browser interface, **navigate to your Universal™ Server** by entering the fully qualified domain name of the Universal on port 9000. For example, if your domain name was acme.com, you would enter the following into your browser's address bar:

https://keys.acme.com:9000

You will be prompted with the universal Administration login screen as shown below.

PGP Universal Administration	
Username: Passphrase:	Login

Figure 33: Universal Administration login screen

2. Enter your credentials and Click

The Welcome to PGP Universal[™] screen displays. From this screen you may read assorted help documents and manuals as well as watch videos on the PGP Universal[™] experience.

Note: this material is always available within the Universal GUI by simply Clicking the icon that located in the upper right corner of the GUI.



Figure 34: Welcome Screen

3. Click Close

The Universal System Overview screen displays. At the top of the screen you will see the different tabs that control settings for Policy, Users, Mail, Organization, Services and System. There are also sub-tabs for each of these tabs that go deeper on each subject. The sub-tab options change based upon the selected tab.

The Universal System Overview screen displays the system status as well as other information including policies and user counts.

Syst	em Overview			((* Refresh
keys.p	gpdisk.net			Thu Jun 24	, 2010 at 10:28 AM
Sys	CPU Usage Messag	ge Activity Whole Disk Encryptic	on Services	Web Messenger https://keys.pgpdisk.net: 0 users	Stopped
			92	Keyserver Idap://keys.pgpdisk.net:6 30 keys	Running
	75%			SNMP	Stopped
	50%			Verified Directory http://keys.pgpdisk.net:8 0 users	Stopped
	25% 0%			Mail Proxies	Stopped
	12PM 4PM	8PM 12AM 4AM	вам	Certificate Revocation	Stopped
	Nice	• System • User		Universal Services Protocol	Running

4. Click the **Consumers** tab.

You will see the Consumers Groups page.

P G P Unive	rsal	Reporting	Consumers Keys Mail Se	ervices System			0008
Adminis	stration	Groups Users Devices	Consumer Policy Managed Dom	ains Directory Synchronization	on		
♠ Groups							
	Groups					?	
			16 Custom Groups				
	Name 🔺	Description		Consumer Policy	Est. Members	Delete	
	🔯 Everyone	All consumers manage	ed by PGP Universal.	Excluded	31	0	
	Excluded	Consumers you do not consumer policy applie	t want to treat as part of any group. No es to these consumers.	Excluded	0	0	
		Figure 36: 0	Consumers Grou	os			

5. Click on Consumer Policy

You will see the Consumer Policy screen as shown below. This screen displays the currently enrolled users and the policy and options that apply to them.

PGPL	Iniversal	R	eporting Cons	umers Keys	Mail	Services	System	0	0	0	×
م	dministration	Groups Users	Devices Consu	mer Policy Ma	anaged Do	mains Di	irectory Synchroniza	tion			
A Cons	umer Policy										
	Consumer F	Policy						?			
	Name		Description				Group Usage	Delete			
	😰 Default		Consumer policy a	pplied to "Everyo	one" policy	group.	0	0			
	Excluded		Consumer policy for part of any group.	or consumers yo This policy cann	ou do not w ot be modif	ant to treat ied.	tas 2	0			

Figure 37: Consumer Policy

Each tab in the UniversalTM Server GUI has its own options and usage. Feel free to explore the different configuration tabs to see the various configuration options. At any time you can click the O for context sensitive help.

Integration with Active Directory

In this section we will review Active Directory (AD) integration and how configure Universal[™] Server to query the LDAP server for user groups and attributes.

1. Click the **Consumers** tab and then **Click** the **Directory Synchronization** tab.

The Directory Synchronization screen displays as shown below.

P G P Universal	Reporting Consumers Keys Mail	Services System	0008
Administration Groups	Users Devices Consumer Policy Managed D	omains Directory Synchroni	zation
Directory synchronization			
Director	/ Synchronization	?	
		-	
	Directory Synchronization is enabled.	Dischie	
	Click Disable to deactivate.	Disable	
LDAP Dire	ctories		
	Name	LDAP Servers Delete	
1 - 40	ad.pgpdisk.net	1 🕲	
	• Add LDAP Directory		
Settings			

Figure 38: Directory Synchronization

2. Click the O Add LDAP Directory... button.

This is where you configure Universal[™] Server with the specifics required to communicate with your AD server. The Add LDAP Directory window will display as show below.

G P Universal	Reporting Consumers Keys Mail Services System	0000
Administration	Groups Users Devices Consumer Policy Managed Domains Directory Synchronization	
Directory Synchronization	Add LDAP Directory	
Add LDAP Directo	ry	Ø
Name [,]		
Type: Active Directory		
Type: Neare Directory		
LDAP Credentials]
These credentials are used wh	en contacting LDAP servers associated with this LDAP Directory.	
Bind DN:	Passphrase:	
]
	LDAP Servers Base Distinguished Names Consumer Matching Rules	
Defensed and a Dese Disting		
Define and order Base Disting	uished Names to be used for lookups. Base DNs may be entered manually or selected using the browser.	
1 👻 Base DN:		•
	Browse Base DNs	
]
View Sample Records		Cancel Save
view Sample Recolds		Calleer Save

Figure 39: Directory Synchronization

3. Check with your Systems Administrator and the fill out the data into the rest of the fields, as shown below.

4. Enter the hostname of the AD Server.

Use the Fully Qualified Domain Name (FQDN). In this example, the name of our domain is pgpdisk.net, and the AD server's name is ad.pgpdisk.net, as shown in the example below.

P G P Universal	Reporting Consum	ners Keys Mail Services	System	0008
Administration	oups Users Devices Consume	er Policy Managed Domains Dire	ectory Synchronization	
igaa Directory Synchronization $igar>$ Edit	DAP Directory			
Edit LDAP Directory				?
Name: ad.pgpdisk.net	-			
Type: Active Directory				
LDAP Credentials				
These credentials are used when contact	ing LDAP servers associated with thi	s LDAP Directory.		
Rind DN: nanuniversal@pandis	c net	Dacenhraco,		
bild bit. pgpullversal@pgpuls	chet	Passpinase.		
	LDAP Servers Base Distingu	ished Names Consumer Match	hing Rules	
Define LDAP servers for the PGP Univer	al Server to search during lookups.			
Hostname: ad.pgpdisk.net	Port: 389	Protocol: LDAP -	Test Connection	C
View Sample Records				Cancel Save
Figure 40: I	irectory Synchroni	zation – AD Hostna	nme entered	

- **5. Specify the protocol** (LDAP or LDAPS) to use between Universal[™] Server and your AD server. For this evaluation we suggest that you leave the *Protocol* and *Port* settings to their default unless you use LDAPS on your AD server.
- **6.** Enter the Bind DN and Passphrase for Directory Synchronization. For the Bind DN use the User Principal Name (UPN) of the account. The UPN is in the format of an email address. In our example we used pgpuniversal@pgpdisk.net

Note: This account used should have permission levels of 'Query' or higher.



as shown below.

LDAP Sample	e Records		?
The following table sho your settings and try a	ows the first five results obta gain.	ined using the configured LDAP info	rmation. If no records were retrieved, please verify
Sample Records			
CN	User ID	Email Address	DN
			DC=pgpdisk,DC=net
Users			CN=Users,DC=pgpdisk,DC=net
Computers			CN=Computers,DC=pgpdisk,DC=net
			OU=Domain Controllers,DC=pgpdisk,DC=net
System			CN=System,DC=pgpdisk,DC=net
			ОК
Fie	aure 41: Directo	orv Synchronization	– Sample Records

- 8. If you do not get any sample records shown then validate that your Bind DN information is correct before continuing.

Edit LDAP Directory			?
Name: ad.pgpdisk.net			
Type: Active Directory			
LDAP Credentials			
These credentials are used when conta	cting LDAP servers associated with this L	DAP Directory.	
Bind DN: popuniversal@popdi	sknet	Passphrase:	
Dini Dini papani oroni Gpapa		, acobination	
	LDAP Servers Base Distinguis	hed Names Consumer Matching Rules	1
Define and order base Distinguished N	ames to be used for lookups. Base Divis m	ay be entered manually or selected using the browser.	
1 V Base DN: DC=pgpdisk	,DC=net		0
T.			
	Brow	se Base DNs	
			J
View Sample Records			Cancel Save

9. Click **Base Distinguished Names** tab and enter your Base DN of your domain. You can click the **Browse Base DNs** button to view or browse your DNs as needed.

10.Click Save to activate the new settings.11. Click Settings...

Directory Synchronization Settings					
Mailing List Cache Timeout: 30 minutes					
Enable LDAP Referrals					
Look for the consumer in all ordered LDAP Directories					
Cancel	Save				

Figure 42: Directory Synchronization – Settings

12. Check the Enroll clients using directory authentication box, as shown in the window below.

Directory Synchronization Settings				
Mailing List Cache Timeout: 30 minutes				
Enable LDAP Referrals				
When a consumer cannot be matched to an LDAP Directory:				
Look for the consumer in all ordered LDAP Directories				
Cancel	ve			

Figure 43: Directory Synchronization Settings

13. Click Save to activate the new settings, also make sure that the directory is enabled as seen below.

P G P Universal	Reporting Consumers Keys Mail Serv	ices System	0008
Administration	Groups Users Devices Consumer Policy Managed Domain	s Directory Synchroniza	tion
Directory Synchronization			
	Directory Synchronization	?	
	Directory Synchronization is enabled. Click Disable to deactivate.	Disable	
	LDAP Directories		
	Name L	DAP Servers Delete	
	1 👻 🜊 ad.pgpdisk.net	1 🔘	
	• Add LDAP Directory		
			/
	Settings		
	octango		

Figure 44: Internal User Policy screen

Congratulations! You have successfully configured Universal[™] Server to work with your Directory. This will enable you to leverage your user's group membership to apply customized security policies to your PGP Desktop clients.

PGP Desktop Consumer Policy

This section reviews the PGP Desktop Client policy and how it can be customized for your environment. PGP Universal[™] Server's policy engine allows you to embed your corporate or organizational security policies directly onto your user's desktop.

There are two common use cases for PGP Whole Disk Encryption – one being the use of Single Sign On and the other being users who will use a pre-boot authentication passphrase that differs from their Windows password. Let's take a moment to understand Single Sign On and how it works with PGP Desktop.

About the Single Sign On Feature

This synchronizes the PGP Whole Disk Encryption (WDE) authentication process with the one used by Microsoft Windows when starting the computer. Once the drive is encrypted the PGP WDE pre-boot authentication (Bootguard) screen appears whenever the system is started. Logging in at this point also logs you into your Windows session.

Using Single Sign On

You choose the Single Sign-On feature when you protect a boot partition or an entire disk using PGP WDE. Encrypting using a Passphrase gives the option of either creating a new Passphrase or using your existing Windows login password. Using your Windows login password enables the Single Sign-On feature.

Logging In with Single Sign On

Once Single Sign-On is configured the PGP Bootguard screen appears when the system is started. If you provide the correct passphrase PGP WDE logs you in to the Windows session and provides access to those disk partitions encrypted with PGP WDE.

How Single Sign On Works

Single Sign-On utilizes the Windows Automatic Login feature. PGP WDE uses your configured authentication information to create, dynamically, specific registry entries when you attempt to log in. Note that your Windows password is never stored in the registry or in any form on the disk - neither encrypted, nor as clear text.

Configuring PGP Desktop Consumer Policy

First we will create a policy for the Single Sign On (SSO) users.

1. Click the **Consumers** tab and then the **Consumer Policy** tab.

The Consumer Policy screen will display as shown below.

2. Click Default as shown above.

This will open the Consumer Policy Options screen, from which you customize your policy settings.

P G P Universal	Reporting Consumers Keys Mail Services System	<u>0008</u>
Consumer Policy	Groups Users Devices Consumer Policy Managed Domains Directory Synchronization Consumer Policy Options: Default	
	Consumer Policy Options	
	Name: Default Description: Consumer policy applied to "Everyone" policy group. Group Usage:	
	PGP Portable Disks Created: 0	
	General Client updates, proxy server, and Policy ADK options	E
	Keys Key generation and management options	
	PGP Desktop Desktop Clients PGP Desktop Clients Client Licensing	
	PGP Universal Web Messenger Edit	
	Edit Policy Name Restore To Factory Defaults	•

Figure 46: Default Policy

This screen is divided into four sections – the two primary areas to configure – Key Settings and PGP Desktop Settings.

Key Settings allows you to specify the type of keys to be used and the parameters that affect them, including generation and renewal settings and other items such as passphrase requirements. Note that if you are only using Whole Disk Encryption you do *not have to create any keys* (keys are used for messaging and file encryption). Please consult with your PGP Reseller or PGP Systems Engineer for detailed discussion about the various key types that are appropriate for your environment.

PGP Desktop Settings is where you specify the control – or lack thereof – that you allow for your end users relative to their PGP Desktop software. This includes the ability to prevent them from decrypting or altering your pre-set policies, for instance.

3. In the PGP Desktop Settings pane, Click Desktop...

The PGP Desktop Settings displays.

	Gonoral	Moceaning 8	Kove I	ile Encryption	Not Sharo	Dick Encrypt	ion
	General	messaging d	k Keys I	ne cherypuon	Netonare	Disk Liferypt	
Permissions -							
Allow users	to change	options					
If this is not s	elected, opt	ions can only be	e changed	here by an admir	istrator. The u	iser will be preve	ented from changing
any options.			-				
Allow user-i	nitiated ke	y generation					
Allow user-i	nitiated ke	y signing	- 16 - 1	Kan anaki wa			
Since these e	ntional end	cryption and s ethods do not i	ell-decryp ise kevs fl	ting archives he ADK will not b	e able to decr	vot such files	
Kevs —							
Always encr	ypt to user	's key					
Automatical	ly synchron ly set up K	nze keys with ev Reconstrue	servers				
Automatical	iy set up it	eyrteconstruc	aon				
Override default	t keyring lo	cations:					
Override default	t keyring lo sktop for V	cations: Vindows:					
Override default	t keyring lo sktop for V	cations: Vindows:					
Override default	t keyring lo sktop for V sktop for N	cations: Vindows: Iac OS X:					
Override default	t keyring lo sktop for V sktop for N	cations: Vindows:					
Override default	t keyring lo sktop for V sktop for N nt Enrollm	cations: /indows: lac OS X: ent					
Override default	t keyring lo sktop for V sktop for N nt Enrollmo S 140-2 op	cations: Vindows: lac OS X: ent erational and	integrity o	hecks			
Override default	t keyring lo sktop for V sktop for N nt Enrollm S 140-2 op Desktop in	cations: /indows: lac OS X: ent erational and system tray/n disable PGP S	integrity o nenu Services	hecks			
Override default PGP De PGP De Constant Enable Siler Activate FIPS Show PGP I Hide the	t keyring lo sktop for V sktop for N nt Enrollme S 140-2 op Desktop in e option to logs to PG	cations: /indows: lac OS X: ent eerational and system tray/n disable PGP S P Universal e	integrity o nenu Services verv 5	thecks			
Override default PGP De PGP De Enable Sile Activate FIPS Show PGP I Hide the Send client	t keyring lo sktop for V sktop for N nt Enrollmo S 140-2 op Desktop in coption to logs to PG	cations: /indows: lac OS X: ent erational and system tray/n disable PGP S P Universal e	integrity o nenu Services very 5	thecks			

Figure 47: PGP Desktop Settings

Desktop Settings allows you to customize various configurable options for your end users. Checking the box for a given option enables that feature, and the absence of a checkmark disables the feature. Once you have selected your options you simply save them as a policy (and give the policy a unique name).

4. Check Che

PGP Desktop: Default					
General Messaging & Keys File Encryption NetShare Disk Encryption					
Permissions					
Allow users to change options					
If this is not selected, options can only be changed here by an administrator. The user will be prevented from changing any options.					
Allow user-initiated key generation					
Allow user-initiated key signing					
Since these encryption methods do not use keys, the ADK will not be able to decrypt such files.					
└ Keys					
Always encrypt to user's key					
Automatically synchronize keys with servers					
Override default keyring locations:					
PGP Desktop for Windows:					
PGP Desktop for Mac OS X:					
 Enable Silent Enrollment Activate FIPS 140-2 operational and integrity checks Show PGP Desktop in system tray/menu Hide the option to disable PGP Services Send client logs to PGP Universal every 5 Minutes Mownload policy updates from PGP Universal every 24 Hours 					
Cancel Save					

Figure 48: PGP Desktop Settings

- 5. Now configure the WDE options. Click the Disk Encryption tab.
- 6. You will now see the options in the pictures below. For SSO (Single Sign On) select the options as shown below.

	k encryption:	
Operation	Internal Disks	Removable Disks
Allow User Management		
Allow Encryption		
Allow Decryption		
Store decryption policy on fixed disks		
Force 💌 encryption of disks to existing W	indows Single Sign-On pas	sword
Automatically encrypt Boot disk	 at installation 	
Require: standard passphrase authen	tication 💌	
Note: Mac OS X clients only support automatic	encryption of the boot disk usi	ng passphrase authentication.
Force maximum CPU usage		
Force power failure safety		
Lock passphrase user accounts on Win	dows clients after 3 faile	d login attempts
Enable automatic encryption or locking o	of removable devices	
 Lock device as read-only and provide Encryption (Windows clients only) 	e users with the option to en	crypt with PGP Whole Disk
Encrypt with PGP Whole Disk Encryp	tion on Windows clients: 🛛	fter 30 seconds 👻
Enable Whole Disk Recovery Tokens		
Allow configuration of WDE Local Self Re	ecovery for Windows clients	
Display a list of users who are eligible	le for local self recovery at bo	oot time
ncrypt using: AES-128 💌 (Windows clie	ents only)	
Encrypt Windows WDE disks and PGP V Import a public PGP key file that may be used the disk requires the private partice of the PC	'irtual Disks to a Disk Admin to access a Whole Disk Encrypt P key to be on a supported sma	istrator Key ed disk or PGP Virtual Disk. Access rt card.
the disk requires the private portion of the PG		
Key: Import		

Figure 49: SSO Policy

- 7. Once you have selected the options to your liking **Click Save** on each screen to finish.
- 8. If you do not want to allow Single Sign On you are testing, Whole Disk Passphrase user check the options as shown below.

9. At this point **click Save** on each screen to finish.

Settings for standard passphrase user.

۲ 🔽	PGP Whole Disk Encryption]
	User-initiated Whole Disk Encryption Perm	nissions	
	Configure permissions for user-initiated whole dis	sk encryption:	
	Operation	Internal Disks	Removable Disks
	Allow User Management		
	Allow Encryption		
	Allow Decryption		
	Store decryption policy on fixed disks	3	
	Deny 💌 encryption of disks to existing W	/indows Single Sign-On pa	ssword
	Automatically encrypt Boot disk		
	Require: standard passphrase auther	tication -	
	Note: Mac OS X clients only support automati	c encryption of the boot disk us	sing passphrase authentication.
	Force maximum CPU usage		
	Force power failure safety		
	C Lock passphrase user accounts on Win	dows clients after 3 fai	led login attempts
	Enable automatic encryption or locking of	of removable devices	
	 Lock device as read-only and provid Encryption (Windows clients only) 	e users with the option to e	ncrypt with PGP Whole Disk
	Encrypt with PGP Whole Disk Encrypt	otion on Windows clients:	After 30 seconds 👻
	Enable Whole Disk Recovery Tokens		
	Allow configuration of WDE Local Self R	ecovery for Windows clients	3
	Display a list of users who are eligib	le for local self recovery at l	boot time
	Encrypt using: AES-128 💌 (Windows cli	ents only)	
	Encrypt Windows WDE disks and PGP \ Import a public PGP key file that may be used the disk requires the private portion of the PG	/irtual Disks to a Disk Admi to access a Whole Disk Encry P key to be on a supported sm	inistrator Key pted disk or PGP Virtual Disk. Accessing art card.
	Key: Import		
	Encrypt Windows WDE disks to a Disk A	dministrator Passphrase	
	Passphrase: Create		
	r doopin door orodoni		

Figure 50: Standard Passphrase User

10. We now need to license the policy, Click the Consumers tab and **then the Consumer Policy tab**.

The Consumer Policy screen will display as shown below.

Р	G	P Unive Admin	ersal istration	Groups	Reporting Users Devices	Consumers K Consumer Policy	eys Mail Managed D	Services omains Di	System rectory Sy	nchronization		00	08
♠	\rangle	Consume	r Policy										
			Cons	umer Polic	з у						?		
			N	ame	Des	cription	_	_		Group Usage	Delete		
			D 🖄	efault	Cons	sumer policy applied	to "Everyone"	policy group		0	\odot		
			<u>іо</u> е	xcluded	Con: part	sumer policy for cons of any group. This p	sumers you do olicy cannot be	o not want to e modified.	treat as	2	\odot		
					Figure 5	1: Consum	ner Poli	су					

11.Click Default as shown above.

This will open the Consumer Policy Options screen, from which you customize your policy settings.

Administration Groups Users Dev Consumer Policy Consumer Policy Options: D	ces Consumer Po fault	olicy Manage	d Domains D	irectory Synchro	pnization	
Consumer Policy Consumer Policy Options: D	fault					
Consumer Policy						
Consumer Policy						
Consumer Policy				-		
Consumer romey	Options			?		
Name: Default						
Description: Consumer	olicy applied to "Eve	eryone" polic	y group.			
Group Usage:				6		
PGP Portable Disks Creat	d: 0					
General				T dit		
Client updates, pro	y server, and Policy A	ADK options		Edit		
Keys				Edit		
Key generation and	management options					
				Jesktop		
PGP Desktop				Mobile		
Coptions for manage	g PGP Desktop clients	S				
			Clier	t Licensing		
PGP Universal W	eb Messenger			Edit		
Options for manage	g PGP Universal Web	messenger us	sers			
Edit Policy Name Rost	re To Factory Defa	ulte				

12. Click Client Licensing... as shown above.

The PGP license screen will display like shown below.



Figure 52: PGP Desktop License Options

13. Click the Enter License... to enter a PGP Desktop License for your end users.

The Enter License screen displays as shown below. Now enter your PGP Desktop license information.

Enter License Inf	ormation	?
Licensee Name:		
Licensee Organization:		
Licensee Email:		
License Number:		
Manual	Cancel	Save

Figure 53: Desktop License

- **14.** If a manual authorization is needed **click** the **Manual** button as seen above.
- 15. Once done click Save.
- **16. Click** we once more to finalize the changes on the Default Policy window and you are done.

The policy changes are pushed automatically to the clients once a day or upon reboot of the client computer.

Creation and Deployment of a PGP Desktop Client

The PGP Universal[™] Server creates an MSI that can be installed locally on a machine, incorporated into a corporate image or pushed via various software or SMS.

1. To create a PGP Desktop MSI we will **click** on the **Consumers** tab then **click Groups** on the Universal Server.

? Groups 16 Custom Groups Est. Members Delete Name Description **Consumer Policy** 🐌 Everyone All consumers managed by PGP Universal. Excluded 32 Consumers you do not want to treat as part of any group. No S Excluded Excluded 0 consumer policy applies to these consumers. View items per page: 25 💂 Policy Group Order... Download Client..

You will see The Groups Policy Screen as shown below.



2. We will then **click** on **Download Client**...

The Download PGP Clients screen will show as below.



Figure 55: Download PGP Clients

- **3.** Then check the Customize checkbox.
- **4.** Next we will input a * into the Mail Server Binding field if one does not already exist.



5. At this point we can now **click** the **Download** button to generate a client to install.

File Down	load - Security Warning 🛛 🛛 🗙
Do you	want to run or save this file?
i 🖗	Name: PGPDesktop.msi Type: Windows Installer Package, 27.2MB From: keys.senderdomain.com <u>R</u> un <u>S</u> ave <u>Cancel</u>
	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. <u>What's the risk?</u>
	Eiguro E7, DCD MET

Figure 57: PGP MSI

6. Click Save to download the PGP Desktop MSI to the location of your choice.

Whole Disk Encryption Client Install and Enrollment

In the section we will go over the install of the PGP Desktop Client as well as the Enrollment process. This process is designed to be as transparent and easy as possible to the end user and the administrator.

- 1. First we will start by installing the MSI we created in the last chapter on a laptop to be managed by the Universal Server. Double **click** the MSI once on the client machine to start the install process.
- 2. You may want to read through the End User License Agreement before continuing.

The PGP license agreement screen as shown below.

i PGP Desktop Setup	
License Agreement You must agree with the license agreement below to proceed.	5
PGP Corporation End User License Agreement	
By clicking the accept button or downloading or installing the Software, you agree to be bound by and become a party to this agreement. PGP's acceptance and fulfillment of your order are expressly conditioned on your agreement to these terms. If you do not agree to all of the terms of this agreement, you must click the button that indicates that you do not accept the terms of this agreement and you must not install the Software.	
Carefully read the following legal agreement ("Agreement") for the license of PGP software you are about to download or install, including any Updates and Upgrades	~
 I accept the license agreement 	
I do not accept the license agreement	
Next > Cancel	

Figure 58: End User License Agreement

- **3.** Click the "I accept" radio button \odot and hit the \square button.
- **4.** If you wish you can read through the release notes otherwise hit \square .

You will now see the release notes as shown below.



Figure 59: Release Notes

5. At this point the Desktop Client will begin to install. **Click** to restart and finish the process.

You will see the Installer Information Window like in the below screenshot.



Figure 60: Restart System

6. Upon reboot you will be greeted with the PGP Whole Disk Enrollment Assistant.

Windows Login Credentials Screen as shown below.

PGP Enrollment
PGP Desktop
Please enter your authentication credentials
Username: SSO
Password:
OK Cancel
Figure 61: PGP Enterprise Enrollment

7. Here you will put in the end users Domain Credentials and **click**.

PGP Enrollment Progress	
Enrolling with PGP Universal server	
Cancel	

Figure 62: Enrolling

6. After the PGP Desktop software contacts Universal[™] Server for policy update the PGP Setup Assistant will have enrolled you with the PGP Universal Server and will start encrypting the hard disk. On the bottom right of your screen you will see

the PGP lock in the taskbar showing encryption like so.

If you are not using Silent Enrollment you will see the following screens:

7. You will want to check I am a new user. and then once more.



Figure 63: User Type

8. We are now at the PGP Whole Disk Encryption Assistant **click** to continue.



Figure 64: Encryption Assistant

9. After **clicking** you will see the request for a user password to be inputted for PGP Whole Disk authentication at boot. In this example below I used the **Standard Whole Disk Passphrase**.

You will now see the Passphrase Assignment screen like below.

PGP Setup Assistant	
P G P Desktop	Passphrase Assignment Your boot disk will be protected by a passphrase. It is important that you keep this passphrase secret and do not write it down.
New User 🗸 Key Setup Key Generation Virtual Disk Whole Disk 🗸 Introduction 🗸	Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.
Passphrase Done Additional Features	Passphrase Quality: 36 %
0	
	< Back Next > Cancel Help

Figure 65: Passphrase Assignment

10.You will **click** After typing your password.

You will be greeted with the Whole Disk Completion screen like below.



Figure 66: Complete the enrollment

11. Click and then to start encryption of the entire hard drive.



Figure 67: Congratulations

- 12. On the bottom right of your screen you will see the PGP lock in the taskbar showing encryption like so.
- **13.** Below you can see the screen you will be greeted with on reboot of your machine. After putting your password you would be logged into Windows.



Figure 68: PGP Boot Guard

Using the Whole Disk Recovery Token (WDRT)

Purpose: To view and use the PGP Whole Disk Recovery Token (WDRT)

1. Access the Universal[™] Server The Universal[™] Server System Overview screen displays as shown below.

	Reporting Consumers Keys Ma Overview Graphs	ail Services System	0000
♠ > Welcome to PGP Univer	sal		
	System Overview	(Refresh)	
	System Graphs	Services	
	CPU Usage Message Activity Whole Disk Encryption	Web Messenger https://keys.pgpdisk.net Stopped 0 users	E
		Keyserver Idap //keys pgpdisk.net.6 © Running 17 keys	
	758	SNMP Stopped	
	508	Verified Directory http://keys.pgpdisk.net.8 Stopped 0 users	U
		Mail Proxies 🕞 Stopped	
	12PM 4PM 8PM 12AM 4AM 8AM 12	FM Certificate Revocation	
	Nice System User	Universal Services Protocol Running	
	Statistics Mail Que	eue	
	Server Version 3.0.0 Build (2881) Messag	jes 0	
	System Uptime 15d, 20h, 39m Size Total Messages Processed 371	0 KB	-

2. Click the Consumers tab. A screen similar shown below appears.

	Reporting Consumers Keys Mail Se	rvices System		
Gro	oups Users Devices Consumer Policy Managed Doma	ins Directory Synchronization	_	
Groups				?
	14 Custom Groups		_	
Name 🔺	Description	Consumer Policy	Est. Members	Delete
😥 Everyone	All consumers managed by PGP Universal.	Excluded	19	\odot
Secuded	Consumers you do not want to treat as part of any group. No consumer policy applies to these consumers.	Excluded	0	0
Executives		Executives	0	0
GW Email		<u>GW Email</u>	0	0
HelpDesk SSO (Can Decrypt)	1	HelpDesk SSO (Can Decrypt)	0	0
🏠 HR		HR	0	0
👔 HR Management		HR Management	2	0
NetShare		NetShare	0	0
PGP Portable		PGP Portable	0	0
Stamped-WDE-Stand-Alone		Stamped-WDE-Stand-Alone	0	0
🍙 Test lan	test to add manual users	Test	1	0
WDE Admin		WDE Admin	0	0
WDE Mac Users		WDE Mac Users	0	0
WDE SSO Slient Auto-Encryp	xt	WDE SSO Slient Auto-Encrypt	2	0
Whole Disk Encryption		Whole Disk Encryption	4	0
XYZ.com		XYZ.com	0	0

Then Click the Users tab.

PGP Universal		Reporting Groups Users Devices	Consumers Keys Mail Services Syst Consumer Policy Managed Domains Director	tem y Sync	hronization	_	_	0000	3
♠ 〉 All Users									
	All Users				Search all users	٩	• ?		
		All Users	Internal Users External Users						
	Neme	Email Address	19 Users	¥	Lastling	Antina			
	alico 000591	alice 000591@papetick.pot	Internal Licer Eventore	Reys	05/27/2000 2-27 PM				
	alice_000598	alice_000598@popdisk.net	Internal User Everyone	1	05/27/2009 2:37 PM	0			
	alice 000643	alice 000643@popdisk.net	Internal User Everyone	1	08/11/2009 8:18 AM	0			
	bob_000581	bob_000581@pgpdisk.net	Internal User Everyone	1	05/27/2009 2:27 PM	0			
	bob_000598	bob_000598@pgpdisk.net	Internal User Everyone	1	06/05/2009 12:56 PM	õ			
	🚊 Cindy Green	cindy@pgpdisk.net	Internal User HR Management	1	03/11/2010 10:22 AM	0			
	gpuser_000456	pgpuser@pgpdisk.net	Internal User Whole Disk Encryption	1	03/17/2010 11:21 AM	0			
	gpuser_000712	pgpuser_000712@pgpdisk.net	Internal User Everyone	0	01/12/2010 4:23 PM	0			
	🚊 pgpuser_000721	pgpuser_000721@pgpdisk.net	Internal User Everyone	0	01/28/2010 1:37 PM	0			
	🚊 pgpuser_000726	pgpuser_000726@pgpdisk.net	Internal User Everyone	1	03/02/2010 7:31 PM	0			
	gpuser_000728	pgpuser_000728@pgpdisk.net	Internal User Whole Disk Encryption	1	03/07/2010 10:04 PM	0			
	🚊 pgpuser_000736	pgpuser_000736@pgpdisk.net	Internal User Whole Disk Encryption	0	03/12/2010 8:47 AM	0			
	🚊 pgpuser_000738	pgpuser_000738@pgpdisk.net	Internal User Whole Disk Encryption	0	03/16/2010 9:23 AM	0			
	🚊 sso	sso@pgpdisk.net	Internal User WDE SSO Slient Auto-Encrypt	1	03/17/2010 10:04 AM	0			
	🚊 sso_000726	sso_000726@pgpdisk.net	Internal User Everyone	1	03/17/2010 8:30 AM	0			
	sso 000728	sso 000728@popdisk.net	Internal User, WDE SSO Slient Auto-Encrypt	1	03/06/2010 1:32 PM	0	1		

You will see a list of users displayed, including the user you just enrolled, displayed under **Internal Users** (by default the Users Tab defaults to the Internal Users Subtab). You may notice that under the Recovery Column there is an icon of a vault with a combination lock and a red cross on it.

This indicates the presence of a Whole Disk Recovery Token (WDRT) for that user. In our example, each user displayed has a WDRT.

3. Click on the name of your user or the icon next to it; in our case, we'll select the user pgpuser by clicking on his name ().

In the Figure below note how the window splits into an upper and lower section divided by the characteristics that may be accessed for that user (email address, PGP Keys and Whole Disk Recovery Tokens).

The upper section provides detail about the user. The lower half of the window reveals different data depending upon which of the three characteristics are being shown. As you can see, the Email Addresses variable is the default characteristic displayed.

P G P Universal	Reporting Consumers Keys Mail Services System	0000
Administration Groups U	sers Devices Consumer Policy Managed Domains Directory Synchronization	
Internal Users Internal User Information		
Internal User Information		(?)
pgpuser_000456		
Username: pgpuser_000456, pgpuser_000456@pgpdis	k.net	
Display Name: pgpuser_000456	UUID: 084e6780-80ef-4ea7-8ea5-2c43ee163635	
Created: 03/17/2010 11:06 AM	Last Use: 03/17/2010 11:21 AM	
Status: Published		
Policy Group: Whole Disk Encryption		
WDE Status: Unknown		
Edit Names		View Log Entries
Authentication		
Authentication		
► Attributes		
► Groups		
► Permissions		
► Managed Keys		

4. Click Whole Disk Encryption to reveal the Whole Disk Recovery Tokens (WDRTs) available for the user.

Note how the lower half of the screen changes to display the machines that have available WDRTs for the selected user as shown below.

Created: 02/	17/0040 44/06 444			Leat line 0	4e0780-80ei-4ea7-8e	80-204366103030		
Created: 03/	17/2010 11:06 AM			Last Use: 0.	S1772010 11:21 AM			
Policy Group: Wh	ole Disk Encryption							
WDF Status: Uni	known							
Edit Names							View Log Ent	ries
Authenticati	on							
 Attributes 								
								_
Groups								
Groups								
Permissions								
Managed Ke	ys							
Email Addres	sses							
V Whole Disk B	Encryption							
Computer	Disk ID	Common Name	Partition	Size Type	Last Seen	Status	Client	WDRT
📢 Client_AS	🝺 bc23ad65-b420-4596-a71a-c	C: VMware Virtual disk SC	1	2 GB Fixed	03/17/2010 11:22 AM	Unencrypted (Since 03/17/2010) 10.0.1.4020	0
WDE Login E	ailures							
THE LOGIN P	andres							

In this case, we have a single WDRT for the machine. To the right of the WDRT located under the Options Column is a magnifying glass <a> This icon is used to view the WDRT.

5. Click the magnifying glass 🔊 .

Universal[™] Server will display a dialogue box like the one shown below.



6. Click to view the WDRT.

Universal ${}^{\scriptscriptstyle \mathsf{TM}}$ Server will display a new window with the Whole Disk Recovery Token as shown.



This Token acts as an additional Passphrase to access the encrypted disk. Note that your actual Token will be different than the one shown in this example.

Now let's simulate the situation in which a user has forgotten his Passphrase and will need to use the WDRT to allow access to the contents of their encrypted computer.

Note: If you are viewing the PGP Universal[™] Server Administration console using your encrypted PC you will need to write down the Token portion of the WDRT prior to rebooting – that way you will have it for the next step.

7. Reboot your Whole Disk Encrypted PC.

You will be challenged for the Passphrase after the BIOS screen displays, as shown below.



8. When prompted by PGP for your Passphrase (which you have now forgotten) press the TAB key – this allows you to see your keystrokes onscreen as you type. Enter the Token from the WDRT as shown above, then press the Enter key.

Your PC will boot normally.

Congratulations! You have successfully used the Whole Disk Recovery Token and created a new Passphrase.

II. Decrypting an Encrypted Drive

Like encrypting, decrypting is a very easy process with PGP. Simply open PGP Desktop, navigate to PGP Disk, select the drive that you want to decrypt, click the decrypt button, enter the passphrase and the decryption will begin.

In the example below we have two encrypted disks on the system, a Fixed Disk Drive and a USB Disk Drive. Both are protected with PGP Whole Disk Encryption.

The detailed steps below walk you through the decryption of the USB Disk. Decrypting the Fixed Disk is an identical process, differing only in that for Step 3 of the process you would select the Fixed Disk instead of the USB Disk.

1. Click the PGPTray icon and from the pop-up menu that displays like the one below select **Open PGP Desktop**.



2. The PGP Desktop displays. Since the last time we used PGP Desktop we were in the PGP Disk Control Box we will return to that location when we restart PGP Desktop.

NOTE: If PGP Desktop does not display the PGP Disk controls in the Work Area, select the PGP Disk Control Box, Click on Encrypt Whole Disk or Partition and your screen will look like the one shown below.

PGP Desktop - Encrypt Whole I	Disk or Partition	
File Edit View Tools Disk H	ielp	
PGP Keys	Encrypt Whole Disk or Partition	Decrypt
PGP Zip	Select disk or partition to encrypt	Encryption Options
PGP Disk C:(Boot) 2:9 GB Fixed Disk C:(Boot) 2:9 GB Fixed Disk C:(Boot) 2:9 GB Fixed Disk C:(Boot) 2:9 GB Viewer	E:(Boot) 2.9 GB Fixed Disk SCSI Bus: VMware Virtual disk SCSI Disk	 Maximum CPU Usage (reduces time to encrypt) Power Failure Safety (requires more time to encrypt)
PGP NetShare	User Access Enter the username or email address of a key ADK Additional Encryption Key for PGPDisk.net CLIENT_AS\John z=x WDE Administrator	Add User Key New Passphrase User Change Passphrase Add Security Questions Delete User

- 3. Click C: Boot Fixed Disk and Click Decrypt.
- **4.** A window will display like the one shown below prompting for the Passphrase to unlock the disk.



Enter the Passphrase and **Click**

to decrypt the disk.

5. If you entered the correct Passphrase the decryption process will begin. PGP informs you of this in a few ways. First, the Notifier will display in the lower right corner of your screen as shown below.



Additionally, PGP Desktop will change to show the decryption status and an estimated completion time. In the screen shot below we can see the decryption has begun with approximately 6 minutes remaining until completion.

PGP Desktop - Encrypt Whole I	Disk or Partition	
File Edit View Tools Disk H	elp	
PGP Keys	Encrypt Whole Disk or Partition	Stop
PGP Zip	Select disk or partition to encrypt	Encryption Options
PGP Disk	E C:(Boot) 2.9 GB Fixed Disk SCSI Bus: VMware Virtual disk SCSI Disk	Maximum CPU Usage (reduces time to encrypt) Power Failure Safety (requires more time to encrypt)
😳 New Virtual Disk 🖾 Encrypt Whole Disk		
PGP Viewer		
PGP NetShare	Decryption Progress	
	96.42% Encrypted - 2.8 GB of 2.9 GB remains encrypted - 6 minutes	remaining
	You may pause, resume or cancel this process at any time by clicki	ng the Stop button.
	You may safely shut down from the Windows Start Menu - do not p doing so.	ower down without

Finally, the PGP Tray icon will change to the Lock with a Spinning Disk indicating an active Whole Disk Operation, in this case decryption.

NOTE: The duration of the decryption process is directly related to the size and speed of the drive. For reference, decrypting a Dell X200 Laptop equipped with a PIII-M @ 800Mhz and a 30GB 4200 RPM HDD completed in just over 2 hours.

6. When decryption completes the Notifier will display again. The message will look like the one shown.



The PGP Tray icon will also change back to the standard Lock icon when the decryption completes. If you are viewing PGP Desktop, the PGP Disk Work Area will now show the fixed boot drive as being unencrypted.

PGP Desktop - Encrypt Whole I	Disk or Partition	
File Edit View Tools Disk H	lelp	
PGP Keys	Encrypt Whole Disk or Partition	Encrypt
PGP Zip	Select disk or partition to encrypt	Encryption Options
PGP Disk New Virtual Disk Encrypt Whole Disk PGP Viewer PGP NetShare	E C:(Boot) 2.9 GB Fixed Disk SCSI Bus: VMware Virtual disk SCSI Disk	 Maximum CPU Usage (reduces time to encrypt) Power Failure Safety (requires more time to encrypt)
	User Access	
	Enter the username or email address of a key	Add User Key
	Click New Passphrase User to add users	New Passphrase User Change Passphrase Add Security Questions Delete User

You have successfully decrypted your Fixed Disk.

III. Uninstalling PGP Desktop Software

 Navigate to Start → All Programs → PGP → Uninstall PGP Desktop as shown below.



2. Click when challenged to uninstall the product and follow the onscreen prompts to continue the uninstalling the product.



3. A window will display like the one shown below while the uninstall initiates:



When PGP uninstalls it will notify you to remove your encryption keys as shown below. **Click OK** to continue.



PGP Desktop will continue uninstalling and will prompt you to reboot when finished, as shown below.

Recycle Bin		
Mozilis Firefox		
	PGP D PGP Desktop You must restart your system for the configuration changes made to PGP Desktop to take effect. Click Yes to restart now or No if you plan to restart manually later. Yes No	
		- ┍► 🛱 🔩 8:45 AM 3/17/2010

 Once your computer has rebooted log into Windows and Navigate to Start → Run and in the pop-up window provided type %appdata% and press Enter . A sample screen capture is shown below.



5. The execution of the command will display a new window that will look similar to the one shown below. Note the PGP Corporation Folder.

🔾 🗸 🖉 🖉 🖉	ik (C:) ▶ Users ▶ sso ▶ AppData ▶ Roaming	• • • •	Search Roaming		Q
Organize 👻 Include ir	n library 🔻 Share with 👻 New folder			•== •	
🔆 Favorites	Name	Date modified	Туре	Size	
🧮 Desktop	퉬 Identities	3/17/2010 7:55 AM	File folder		
🐌 Downloads	퉬 Media Center Programs	7/14/2009 1:48 AM	File folder		
Recent Places	퉬 Microsoft	3/17/2010 8:01 AM	File folder		
	퉬 Mozilla	3/17/2010 8:30 AM	File folder		
🥃 Libraries	PGP Corporation	3/17/2010 8:38 AM	File folder		
Documents					
J Music					
Pictures					
🛃 Videos					
Computer					
🐿 Network					
*					
E itoma					
5 items					
🚱 🙆 [~	· 🔁 🎪	8:47 AM 3/17/2010

- 6. Delete the PGP Corporation Folder and close the window.
- 7. Navigate to My Documents as shown below.



- 8. Locate the PGP Folder and Delete it.
- 9. Navigate to your Windows Desktop and Empty the trash.

You have now completely uninstalled the PGP Desktop software.