

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 PGPUiversalWebFull.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 Keys	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 do-not-reply@pgpstore.com 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:

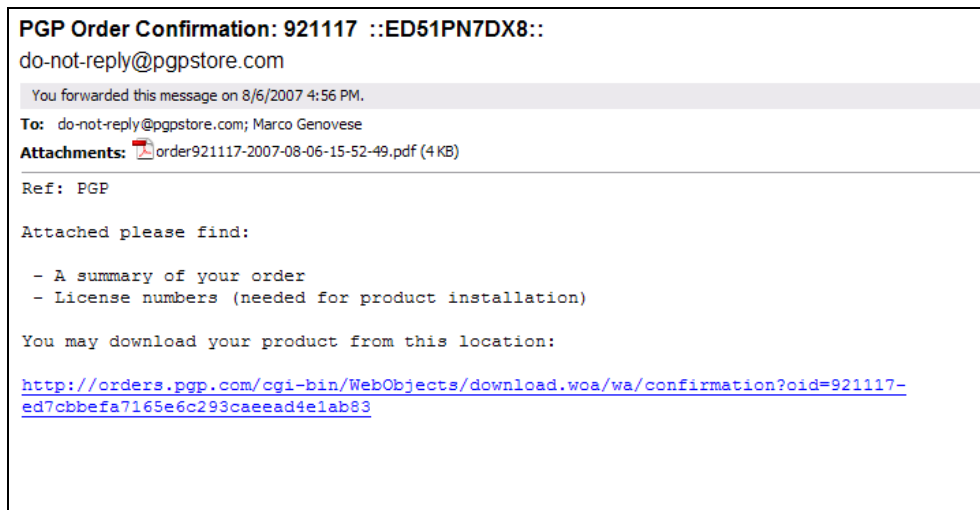


Figure 1: PGP Evaluation Email

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.

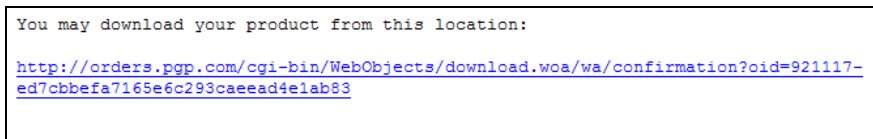


Figure 2: Download Link

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

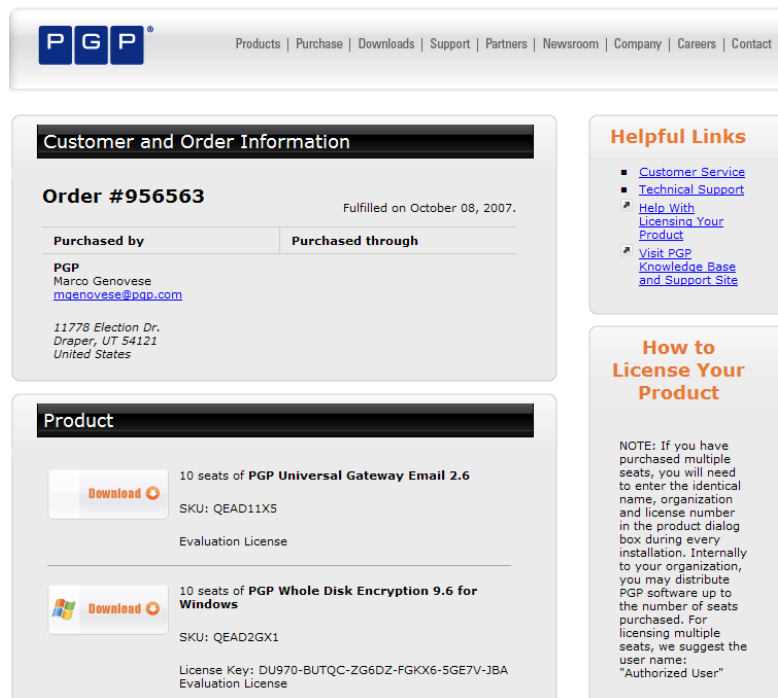


Figure 3: Download Website

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

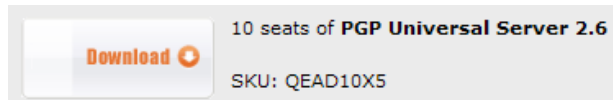


Figure 4: Download Button

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

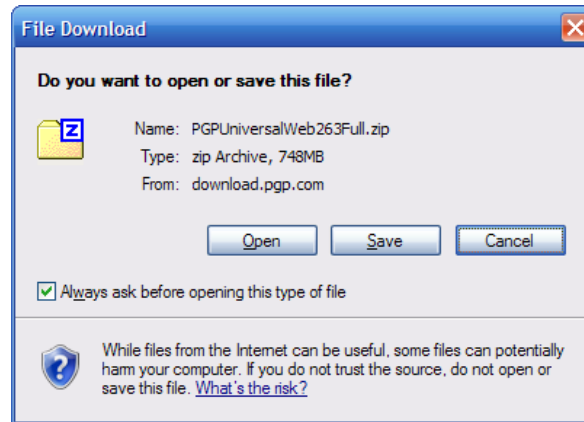


Figure 5: Universal Evaluation Download

6. **Save the PGPUниверsalWebFull.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 PGPUниверsalWebFull.zip file.

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

Name	Size	Packed Size	Modified
PGPUниверsalWeb263Full_Inner.zip	748 M	748 M	2007-08-13 11:29
PGPUниверsalWeb263Full_Inner.zip.sig	280 B	280 B	2007-08-13 11:29

Figure 6: Contents of PGPUниверsalWebFull.zip file

8. **Double-Click** on the PGPUниверsalWebFull_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
LDAP Server Schemas	0 B	0 B	2007-08-13 11:24
PGP Desktop	0 B	0 B	2007-08-13 11:27
PGP Universal Satellite	0 B	0 B	2007-08-13 11:27
PGP Universal Server	0 B	0 B	2007-08-13 11:25
ReadMe.htm	58 K	11 K	2007-08-13 11:24
License.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.



Name	Size	Packed Size	Modified
 PGPUniversalServer263.iso	598 M	559 M	2007-08-13 11:25
 PGPUniversalServer263.iso.sig	280 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 [here](#).

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.

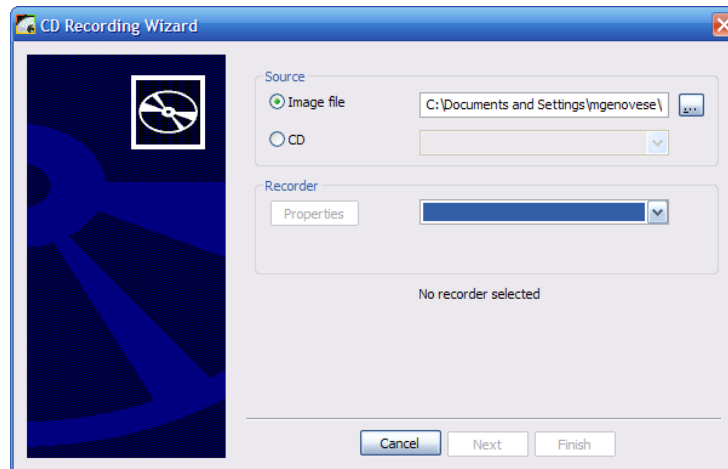


Figure 9: CD Recording Wizard

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:

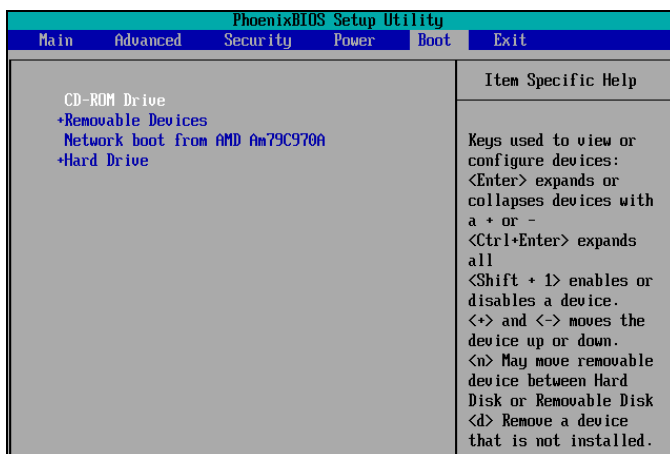


Figure 10: Bios Setup Utility screen

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.

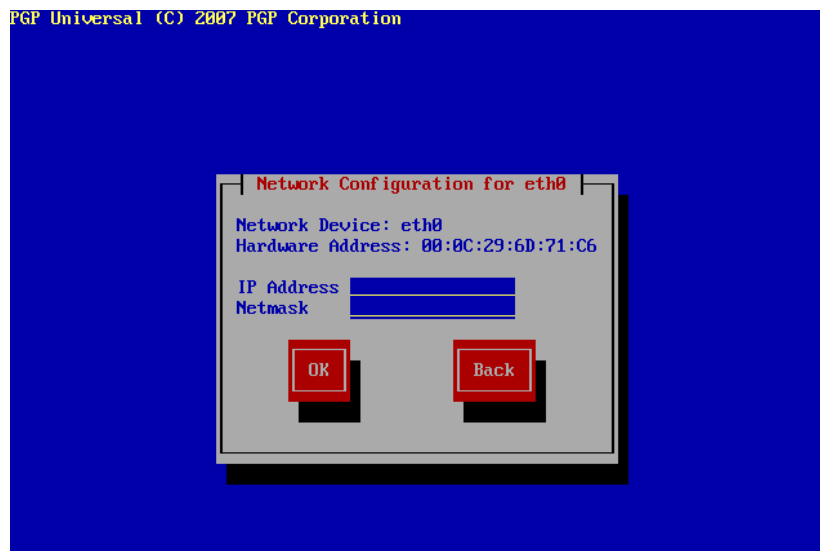


Figure 12: Network Configuration Settings

- 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

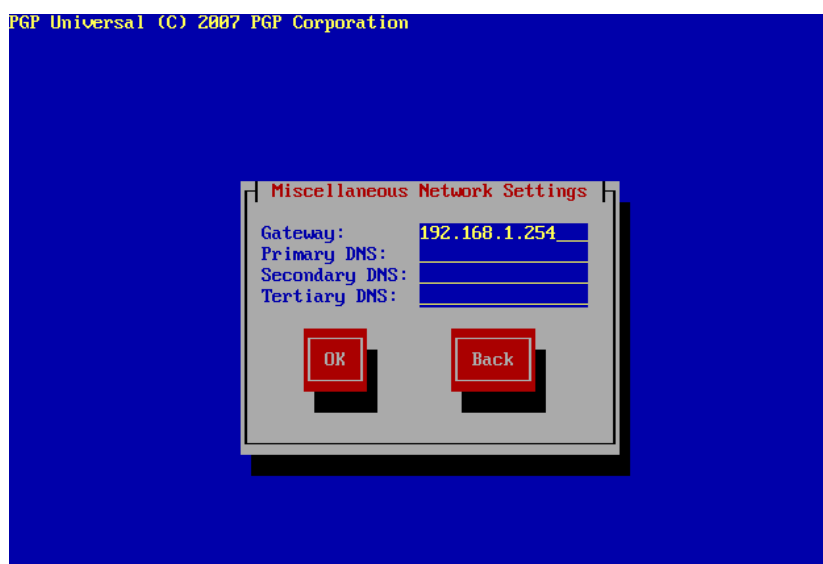


Figure 13: Miscellaneous Network Settings

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

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

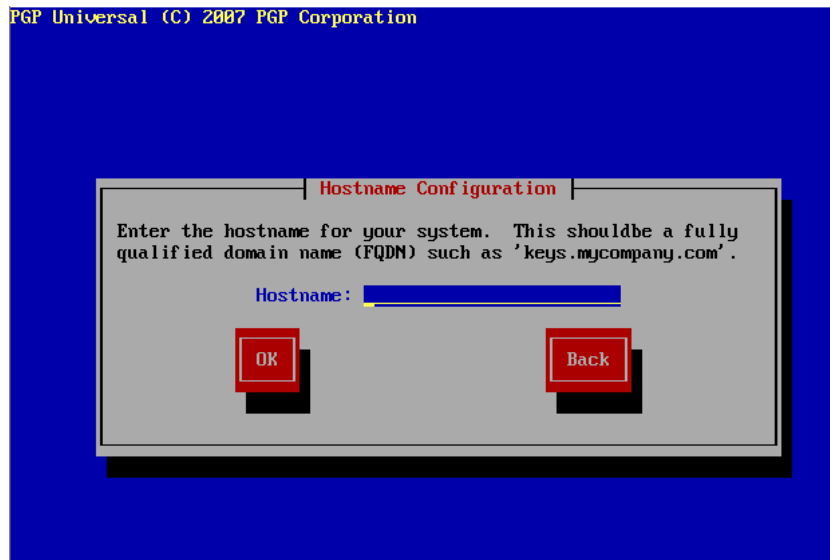


Figure 14: Hostname Configuration screen

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:

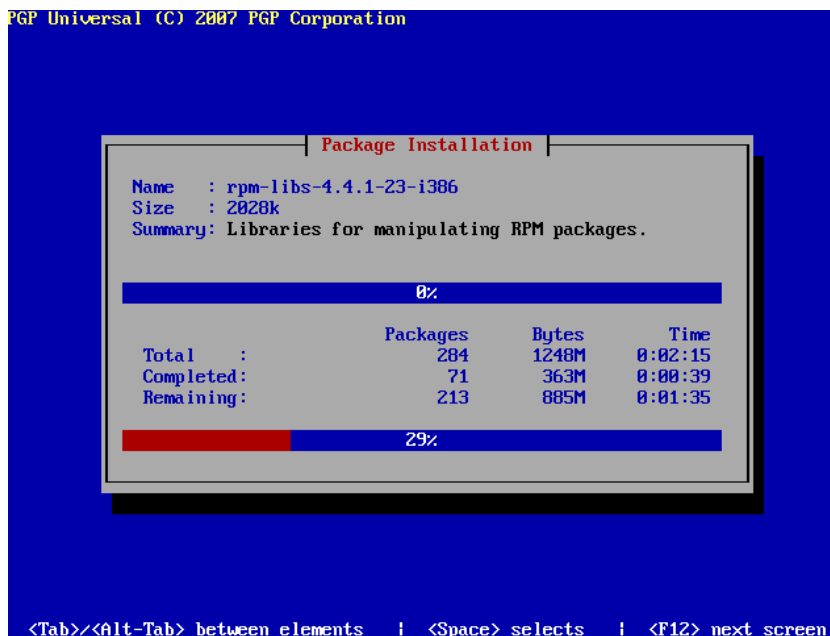


Figure 15: Universal Install Progress

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:

```
PGP Universal Server release 3.0.0.2881 (Ovid)
Kernel 2.6.18-128.4.1.el5PAE on an i686

PGP Universal Server Administration is available via web interface
Connect to https://10.217.100.13:9000


keys login: _
```

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**  [Continue to this website](#) as you are receiving this message because the Universal™ Server does not yet have a valid SSL Certificate.

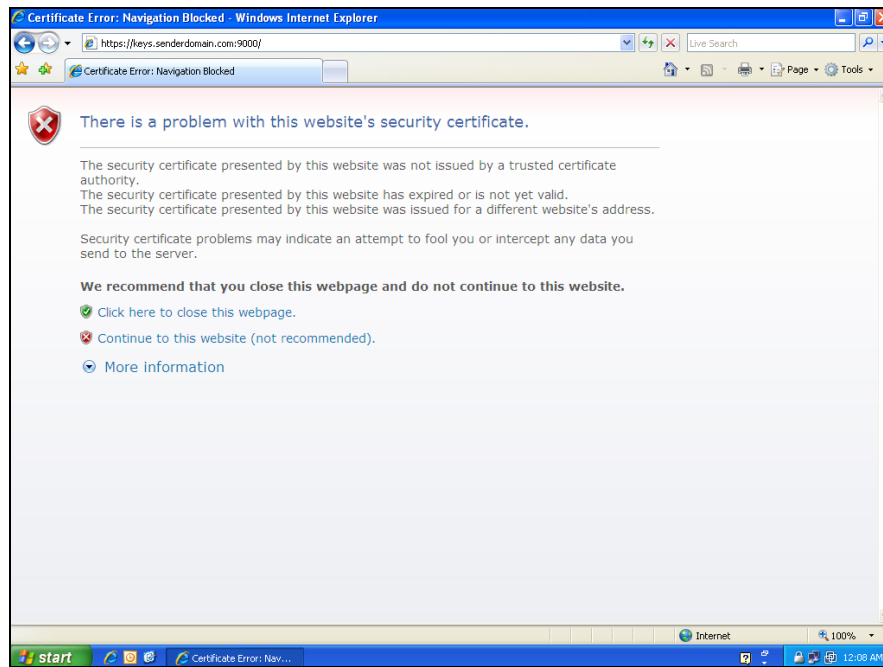


Figure 17: SSL Certificate Warning

You will now see the welcome screen as seen below.

8. Click the  button.



Figure 18: Welcome to your PGP Universal Server!

9. Read and **Click** the  button to continue.

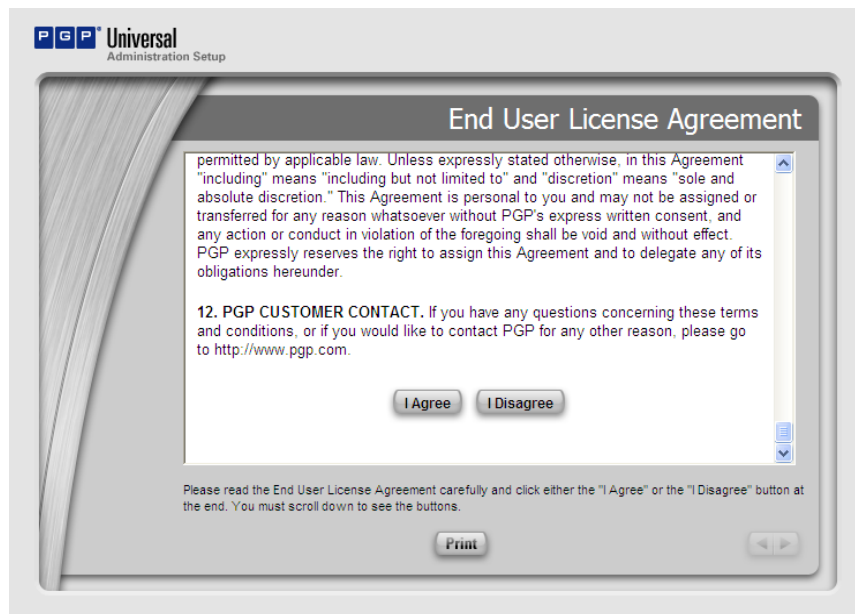


Figure 19: End User License Agreement

The Setup Type screen will display as shown below.

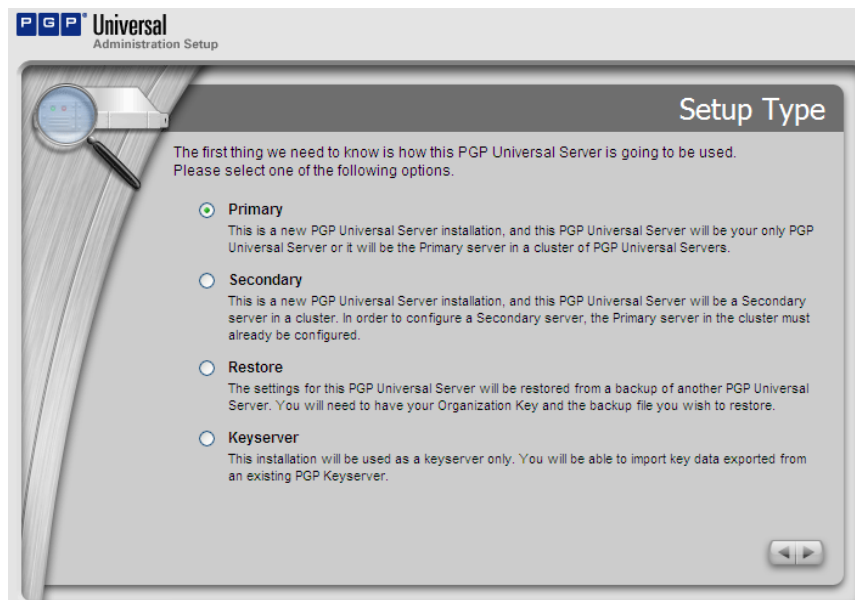


Figure 20: Universal Setup Type

10. Select “Primary” and Click .

The Date and time screen will display.

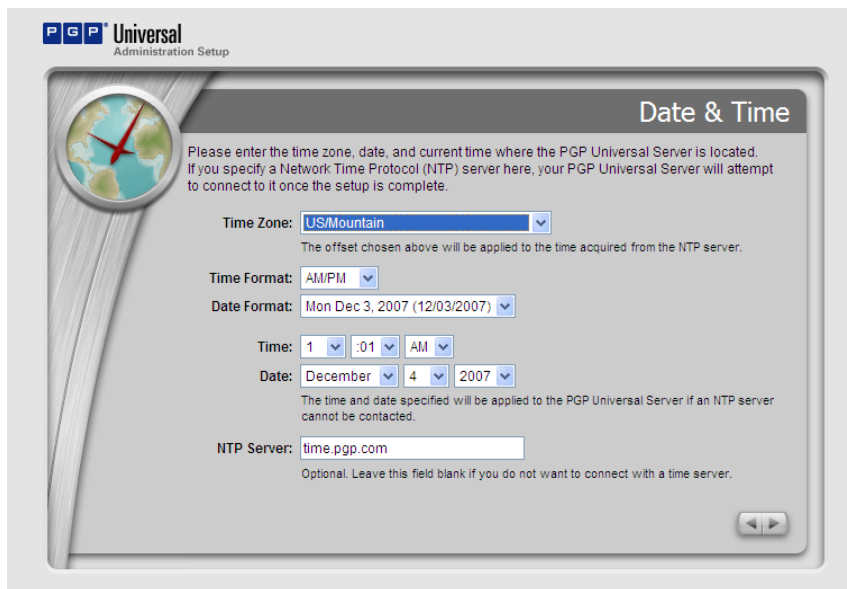


Figure 21: Date & Time

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

The Network Setup screen will display, as shown below.

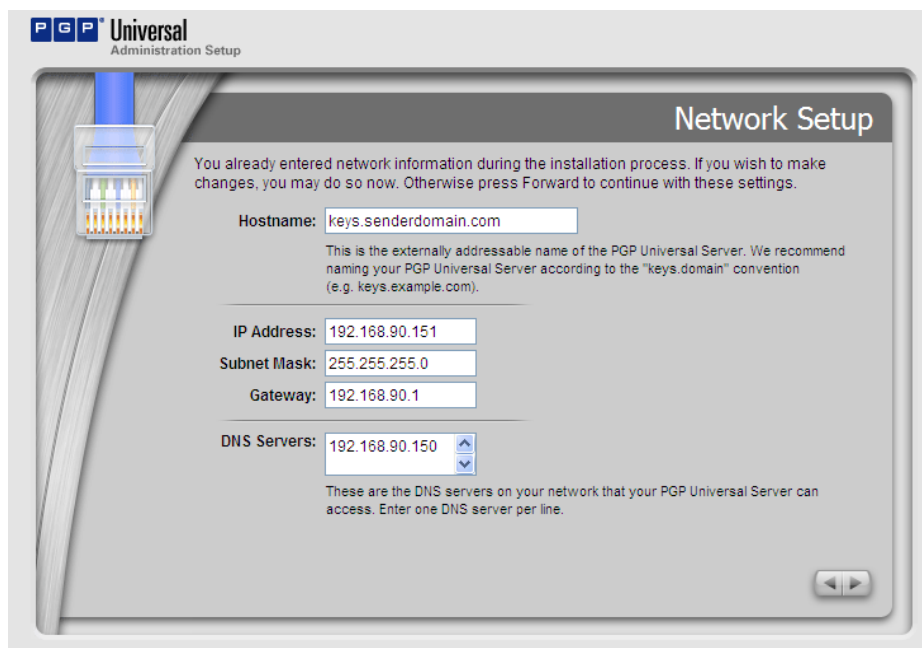


Figure 22: Network Setup

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

The Proxy Configuration screen will display.

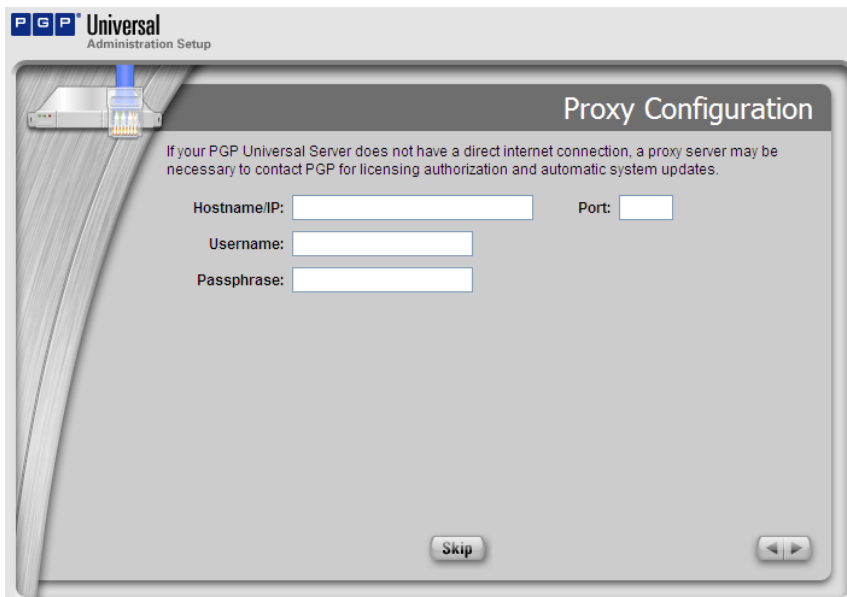


Figure 23: Proxy Configuration

- 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.

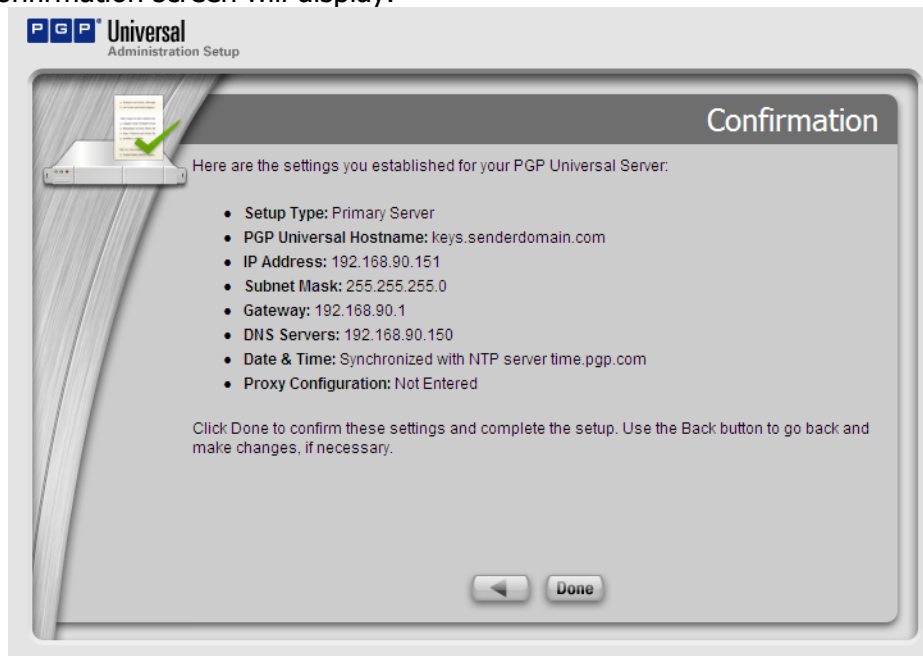


Figure 24: Settings Confirmation

- 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.

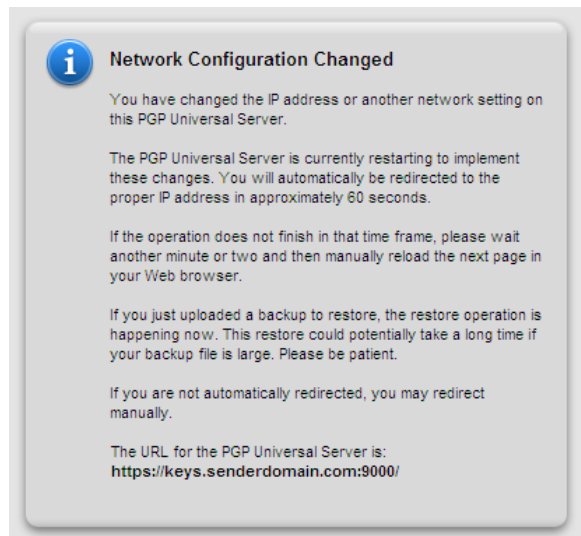


Figure 25: Network Changes Notification

Please wait until the Licensing Screen displays.

Figure 26: Server License

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


License Name: John Doe

License Organization: ACME

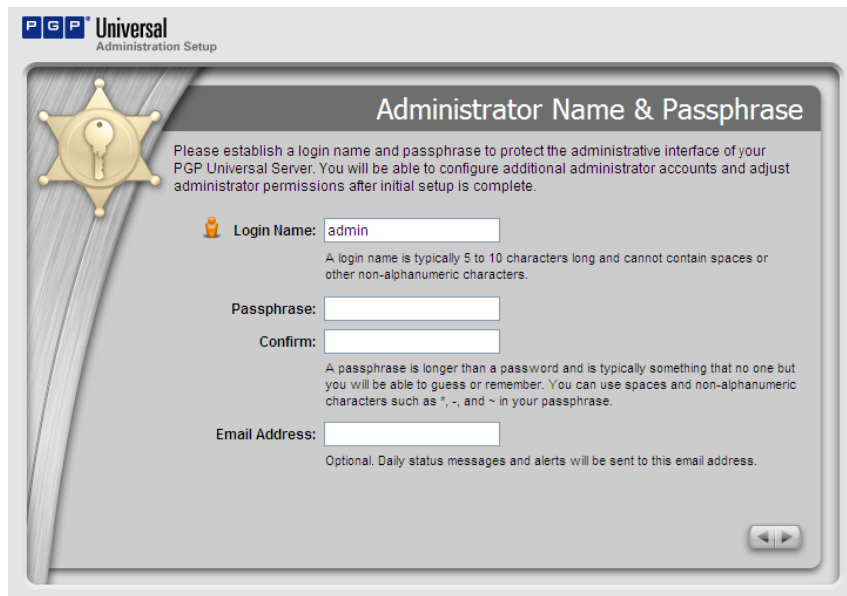
License Email: jdoe@acme.com

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 will need to perform a manual authorization. To do this, simply **Click** the  button and input the license authorization information.

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



The screenshot shows the 'Administrator Name & Passphrase' setup screen for PGP Universal. The title bar reads 'PGP Universal Administration Setup'. The main heading is 'Administrator Name & Passphrase'. Below the heading, a message states: 'Please establish a login name and passphrase to protect the administrative interface of your PGP Universal Server. You will be able to configure additional administrator accounts and adjust administrator permissions after initial setup is complete.' On the left, there is a gold star icon with a keyhole. The form contains three input fields: 'Login Name' (with 'admin' entered), 'Passphrase', and 'Confirm'. Below the 'Passphrase' field, a note explains that a passphrase is longer than a password and typically something no one but you can remember, allowing for spaces and non-alphanumeric characters like *, -, and ~. Below the 'Confirm' field, another note explains that a passphrase is longer than a password and typically something no one but you can remember, allowing for spaces and non-alphanumeric characters like *, -, and ~. At the bottom, there is an 'Email Address' field with a note: 'Optional. Daily status messages and alerts will be sent to this email address.' A navigation bar at the bottom right contains a back arrow and a forward arrow.

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.

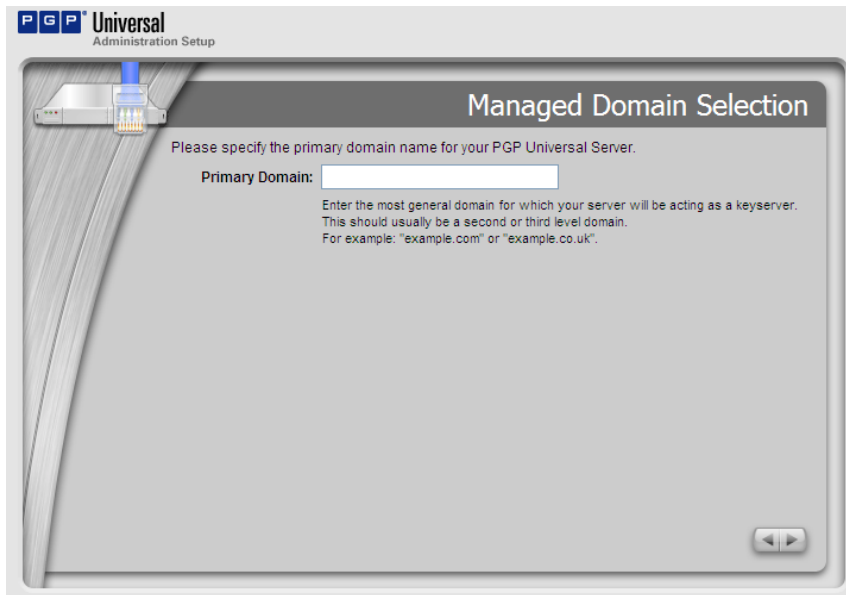


Figure 28: Managed Domain

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

The Directory Server screen displays.

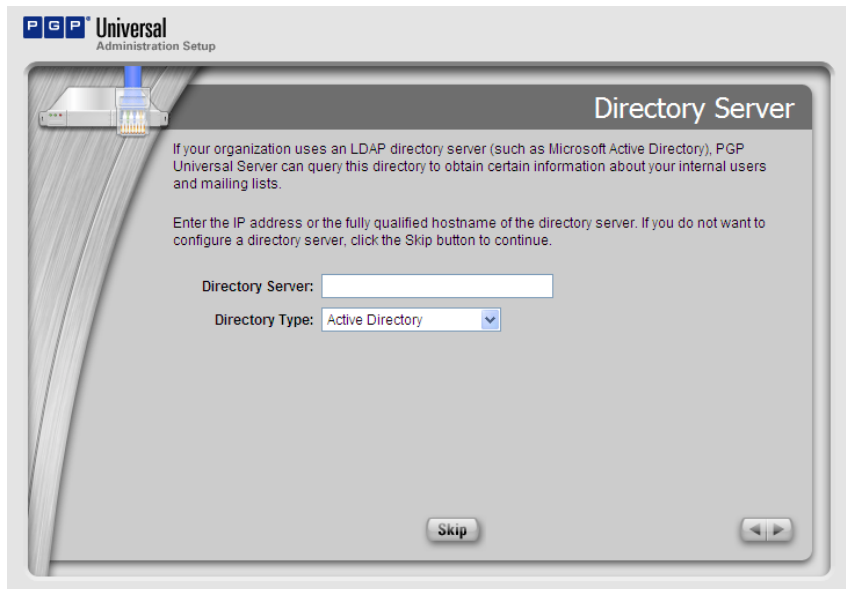


Figure 29: Directory Server

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.



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.



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.

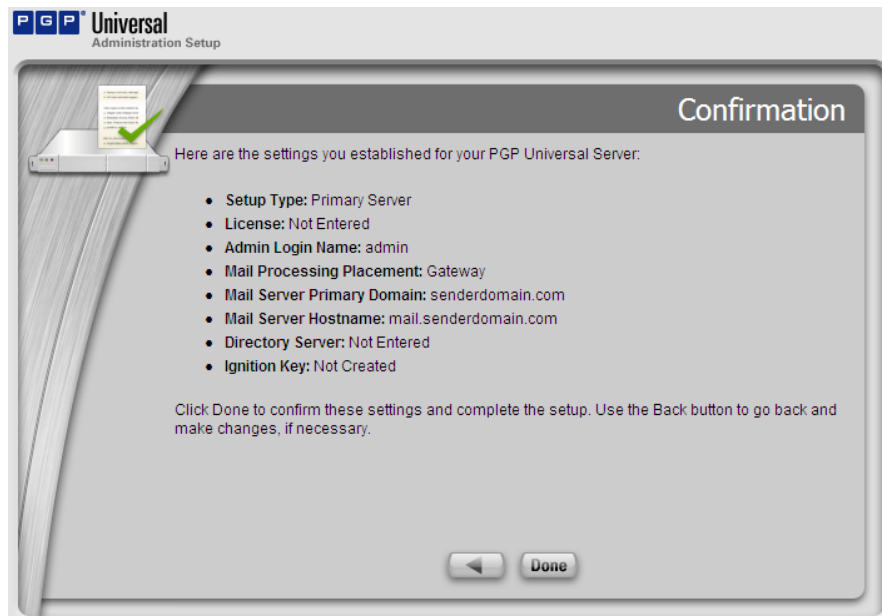


Figure 32: PGP Universal™ Server Confirmation

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.



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.

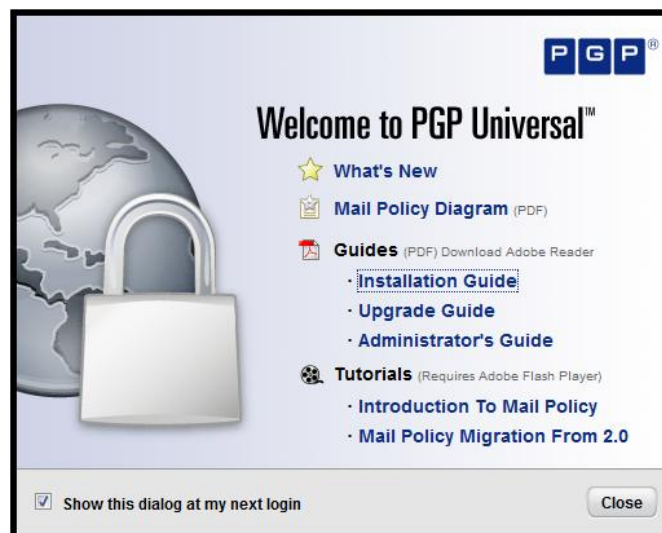


Figure 34: Welcome Screen

3. **Click** .

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.

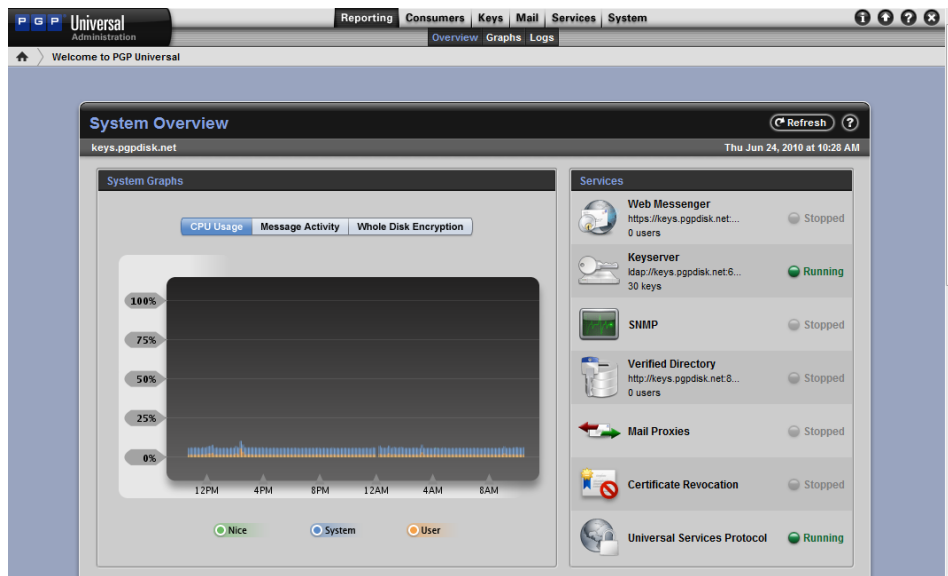


Figure 35: System Overview

4. Click the **Consumers** tab.

You will see the Consumers Groups page.

The screenshot displays the 'Groups' page of the PGP Universal Administration interface. The top navigation bar includes 'Reporting', 'Consumers', 'Keys', 'Mail', 'Services', and 'System'. The 'Consumers' tab is selected. The main content area shows a table of 16 Custom Groups. The table has columns for Name, Description, Consumer Policy, Est. Members, and Delete. The first two groups are 'Everyone' and 'Excluded'.

Name	Description	Consumer Policy	Est. Members	Delete
Everyone	All consumers managed by PGP Universal.	Excluded	31	
Excluded	Consumers you do not want to treat as part of any group. No consumer policy applies to these consumers.	Excluded	0	

Figure 36: Consumers Groups

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.

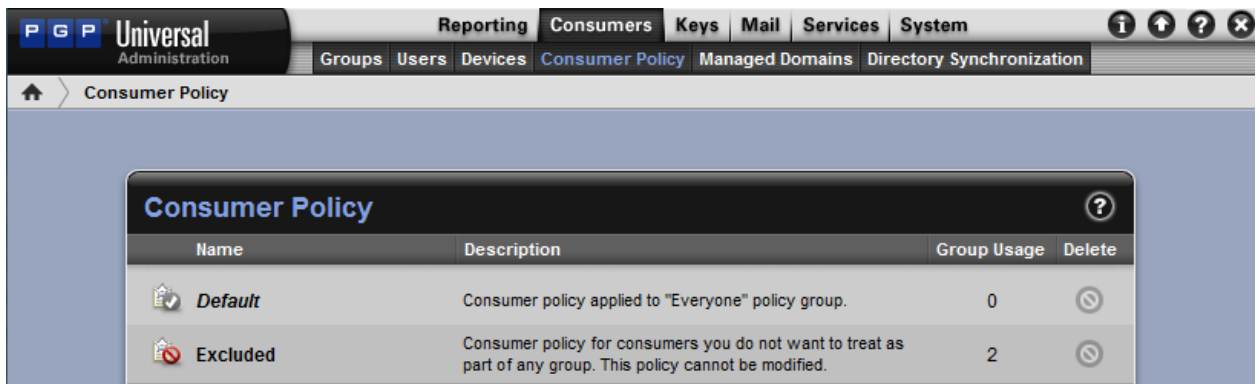


Figure 37: Consumer Policy

Each tab in the Universal™ 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 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.

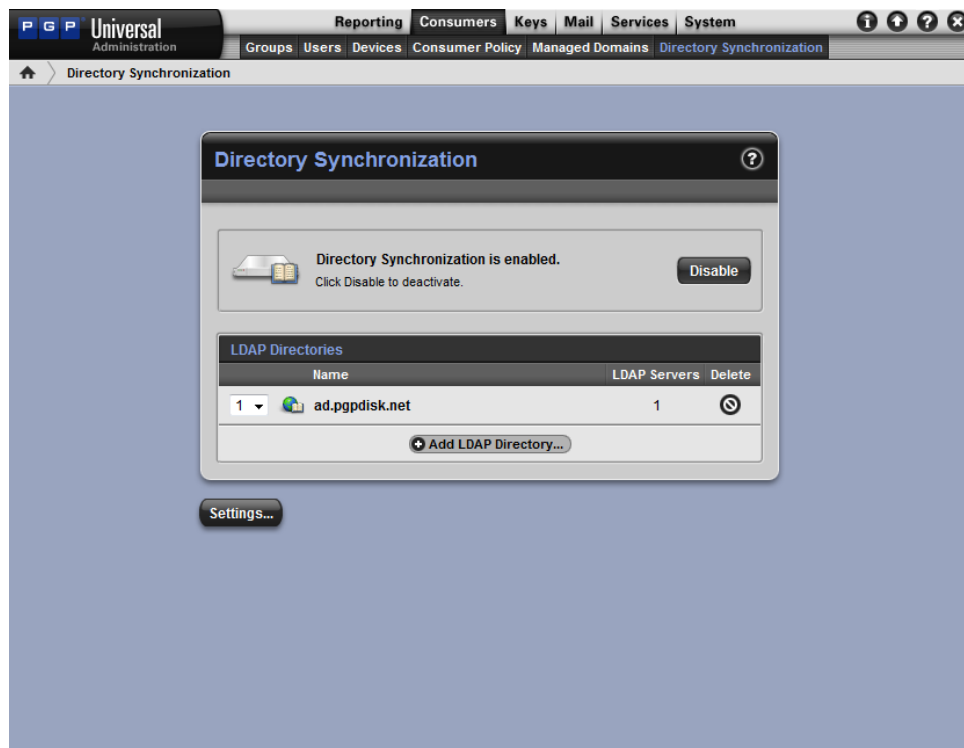


Figure 38: Directory Synchronization

2. Click the **+ 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.

The screenshot shows the 'Add LDAP Directory' window within the Universal Administration interface. The window has a title bar with a question mark icon. Below the title bar, there are tabs for 'LDAP Servers', 'Base Distinguished Names', and 'Consumer Matching Rules'. The 'LDAP Servers' tab is currently selected. The form contains the following fields and sections:

- Name:** A text input field.
- Type:** A dropdown menu with 'Active Directory' selected.
- LDAP Credentials:** A section with a description: 'These credentials are used when contacting LDAP servers associated with this LDAP Directory.' It contains two input fields: 'Bind DN:' and 'Passphrase:'.
- Base Distinguished Names:** A section with a description: 'Define and order Base Distinguished Names to be used for lookups. Base DN's may be entered manually or selected using the browser.' It features a list with one entry: '1' followed by a dropdown and a text input field for 'Base DN:'. A '+' icon is to the right of the input field.
- Browse Base DN's...:** A button located below the list.
- View Sample Records...:** A button at the bottom left.
- Cancel** and **Save** buttons at the bottom right.

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.

The screenshot shows the 'Edit LDAP Directory' window in the PGP Universal Administration interface. The window has a title bar with a question mark icon. Below the title bar, there's a breadcrumb trail: 'Directory Synchronization' > 'Edit LDAP Directory'. The main content area is divided into several sections:

- Name:** A text field containing 'ad.pgpdisk.net'.
- Type:** A dropdown menu set to 'Active Directory'.
- LDAP Credentials:** A section with a description: 'These credentials are used when contacting LDAP servers associated with this LDAP Directory.' It contains two fields: 'Bind DN:' with the value 'pgpuniversal@pgpdisk.net' and 'Passphrase:' with a masked value '.....'.
- LDAP Servers:** A tabbed interface with three tabs: 'LDAP Servers' (selected), 'Base Distinguished Names', and 'Consumer Matching Rules'. Below the tabs, there's a description: 'Define LDAP servers for the PGP Universal Server to search during lookups.' It contains three fields: 'Hostname:' with 'ad.pgpdisk.net', 'Port:' with '389', and 'Protocol:' with a dropdown set to 'LDAP'. To the right of these fields is a 'Test Connection' button and a plus icon (+).

At the bottom of the window, there are four buttons: 'View Sample Records...', 'Cancel', and 'Save'.

Figure 40: Directory Synchronization – AD Hostname 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`

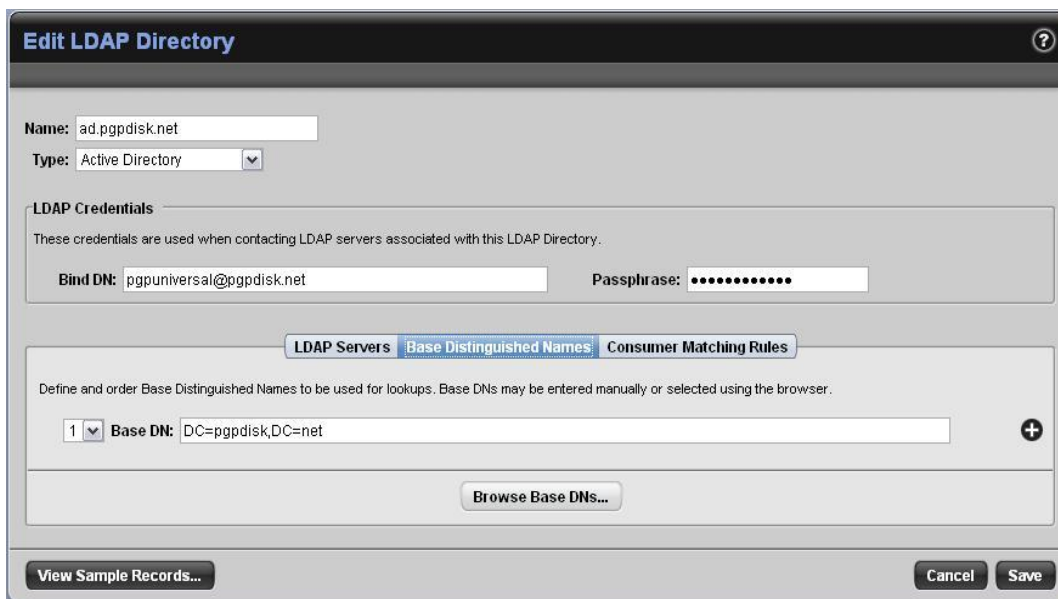
Note: This account used should have permission levels of 'Query' or higher.

7. Click **View Sample Records...** as shown below.



Figure 41: Directory Synchronization – Sample Records

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



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  to activate the new settings.

11. Click 

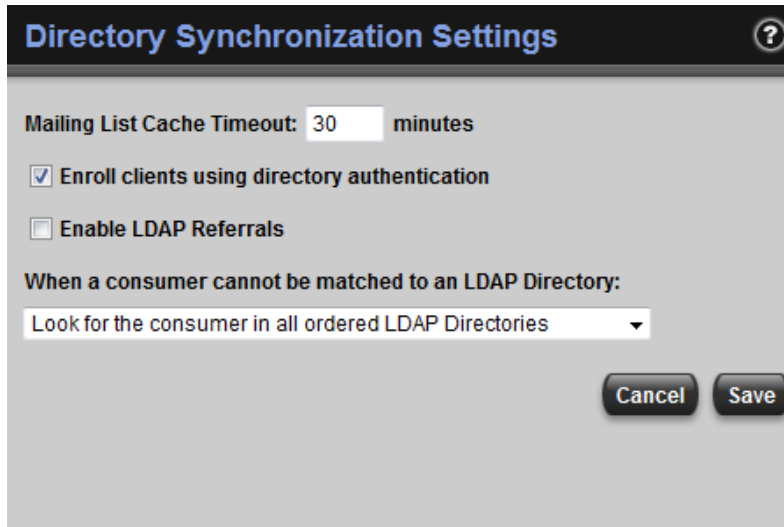



Figure 42: Directory Synchronization – Settings

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

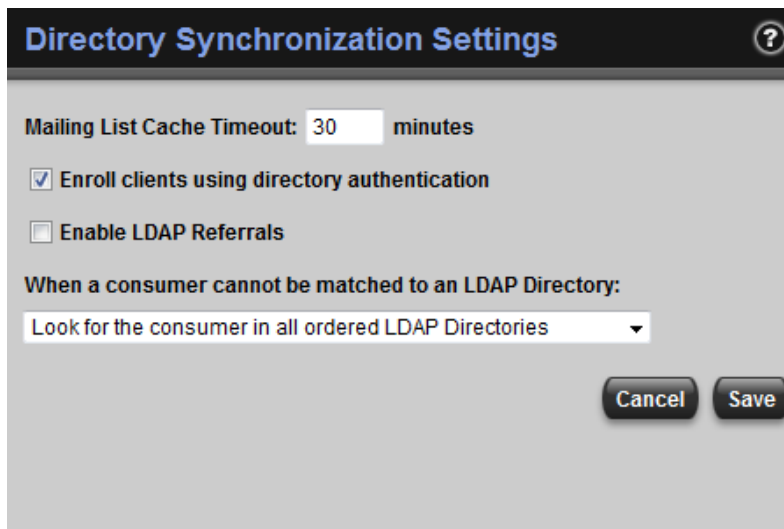


Figure 43: Directory Synchronization Settings

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

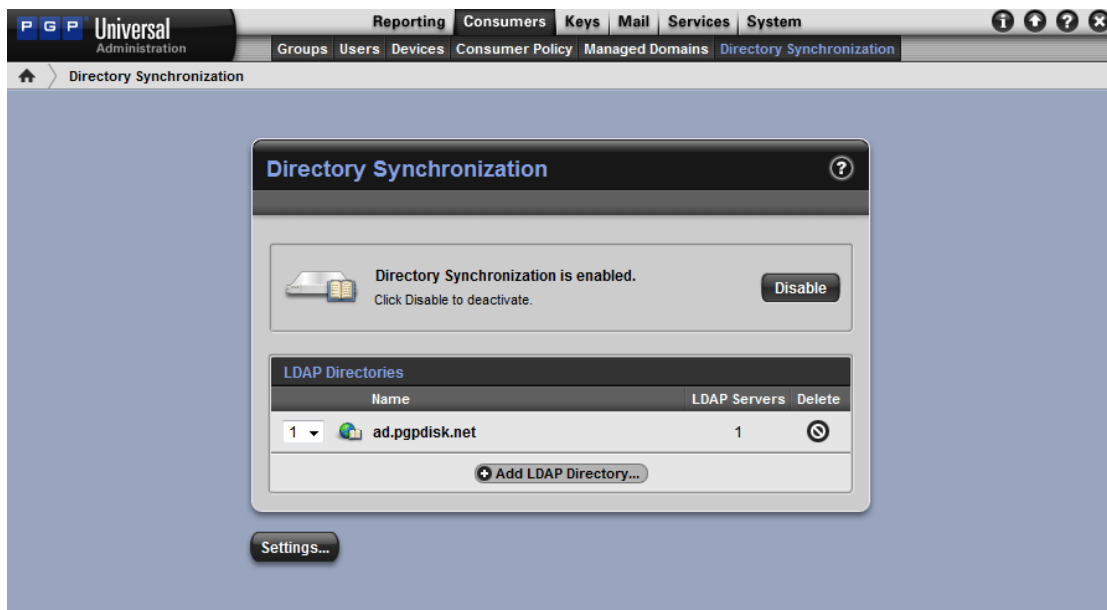


Figure 44: Internal User Policy screen

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.

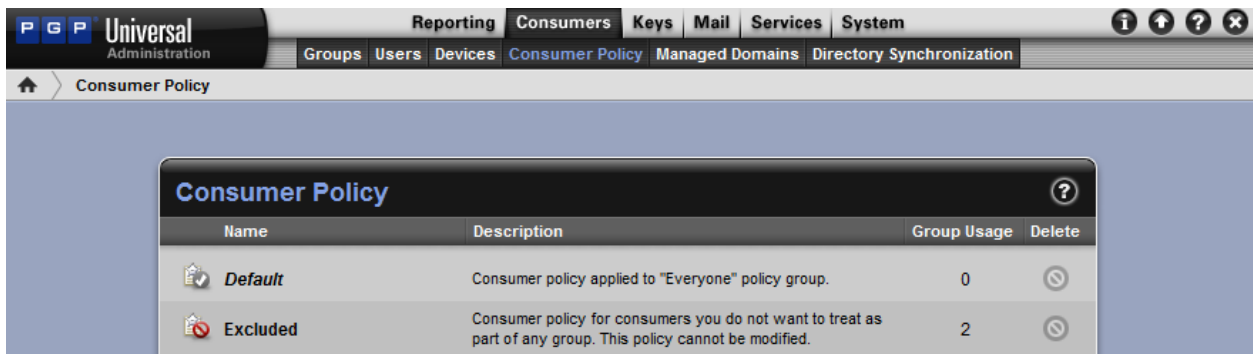


Figure 45: Consumer Policy

2. Click **Default** as shown above.

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

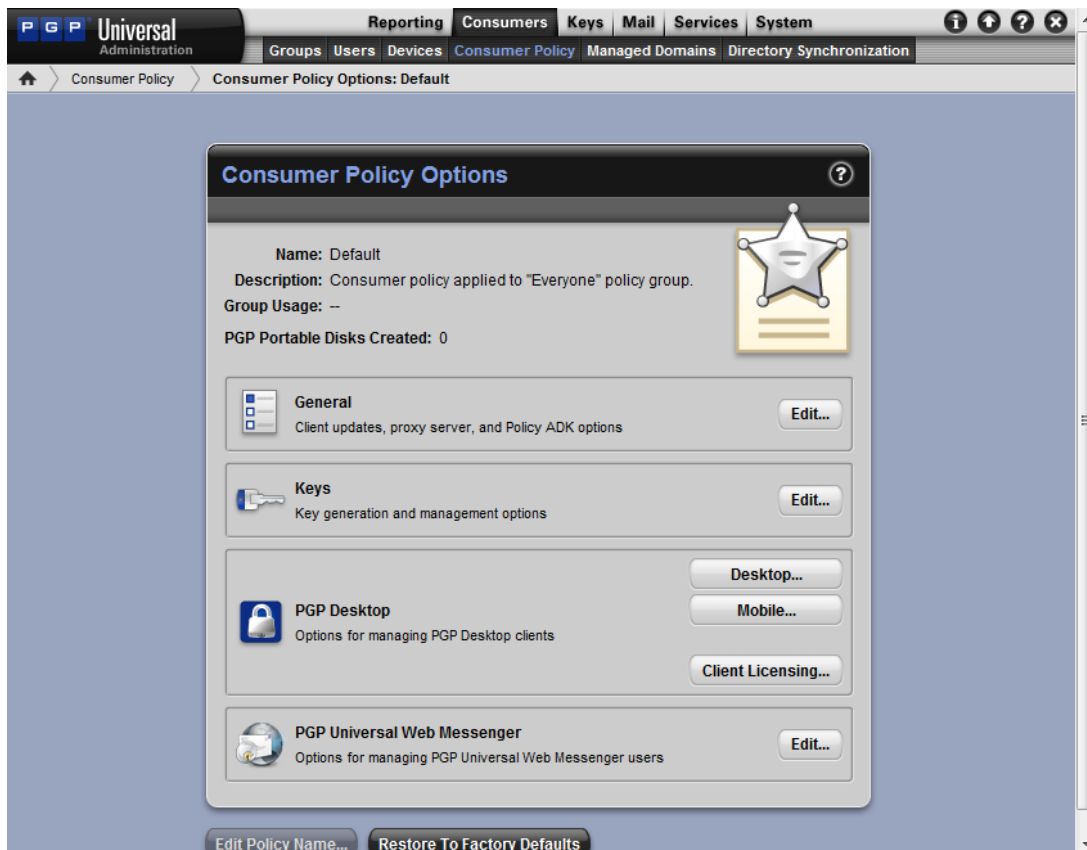


Figure 46: Default Policy

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 .

The PGP Desktop Settings displays.

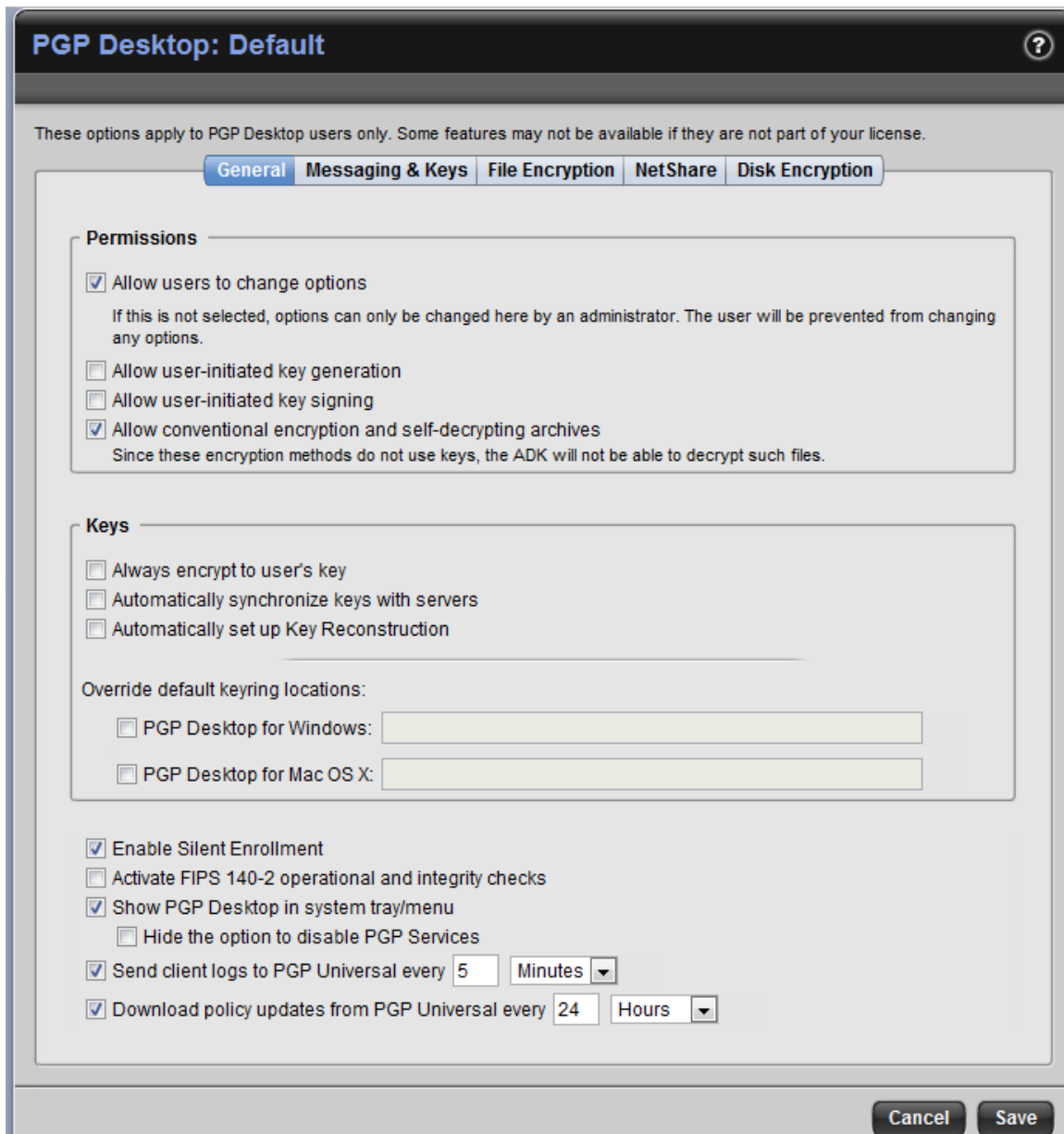


Figure 47: PGP Desktop Settings

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 ☒ **Enable Silent Enrollment** and match the settings seen below (**Do not enable Silent enrollment if this is for Mac testing or if you are not using SSO**):

PGP Desktop: Default

These options apply to PGP Desktop users only. Some features may not be available if they are not part of your license.

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
- ☒ Allow conventional encryption and self-decrypting archives
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
- ☐ Automatically set up Key Reconstruction

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 Minutes
- ☒ Download policy updates from PGP Universal every 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.

☒ **PGP Whole Disk Encryption**

User-initiated Whole Disk Encryption Permissions
Configure permissions for user-initiated whole disk encryption:

Operation	Internal Disks	Removable Disks
Allow User Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allow Encryption	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allow Decryption	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Store decryption policy on fixed disks

Force encryption of disks to existing Windows Single Sign-On password

☒ Automatically encrypt **Boot disk** at installation

Require: **standard passphrase authentication**

Note: Mac OS X clients only support automatic encryption of the boot disk using passphrase authentication.

☐ Force maximum CPU usage

☒ Force power failure safety

☐ Lock passphrase user accounts on Windows clients after **3** failed login attempts

☐ Enable automatic encryption or locking of removable devices

☒ Lock device as read-only and provide users with the option to encrypt with PGP Whole Disk Encryption (Windows clients only)

☐ Encrypt with PGP Whole Disk Encryption on Windows clients: **After 30 seconds**

☒ Enable Whole Disk Recovery Tokens

☐ Allow configuration of WDE Local Self Recovery for Windows clients

☒ Display a list of users who are eligible for local self recovery at boot time

Encrypt using: **AES-128** (Windows clients only)

☐ Encrypt Windows WDE disks and PGP Virtual Disks to a Disk Administrator Key
Import a public PGP key file that may be used to access a Whole Disk Encrypted disk or PGP Virtual Disk. Accessing the disk requires the private portion of the PGP key to be on a supported smart card.

Key:

☐ Encrypt Windows WDE disks to a Disk Administrator Passphrase

Passphrase:

Figure 49: SSO Policy

- Once you have selected the options to your liking **Click** on each screen to finish.
- 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.

The screenshot shows the 'PGP Whole Disk Encryption' configuration window. The 'User-initiated Whole Disk Encryption Permissions' section is active, showing a table of permissions for internal and removable disks. Below this, there are various settings for encryption, including a 'Deny' dropdown, 'Automatically encrypt' checkbox, 'Require' dropdown, and several checkboxes for CPU usage, power failure safety, and account locking. The 'Encrypt using' dropdown is set to 'AES-128'. The 'Key' field has an 'Import...' button, and the 'Passphrase' field has a 'Create...' button.

Operation	Internal Disks	Removable Disks
Allow User Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allow Encryption	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Allow Decryption	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☐ Store decryption policy on fixed disks

Deny encryption of disks to existing Windows Single Sign-On password

☒ Automatically encrypt Boot disk at installation

Require: standard passphrase authentication

Note: Mac OS X clients only support automatic encryption of the boot disk using passphrase authentication.

☐ Force maximum CPU usage

☒ Force power failure safety

☐ Lock passphrase user accounts on Windows clients after 3 failed login attempts

☐ Enable automatic encryption or locking of removable devices

☒ Lock device as read-only and provide users with the option to encrypt with PGP Whole Disk Encryption (Windows clients only)

☐ Encrypt with PGP Whole Disk Encryption on Windows clients: After 30 seconds

☒ Enable Whole Disk Recovery Tokens

☒ Allow configuration of WDE Local Self Recovery for Windows clients

☒ Display a list of users who are eligible for local self recovery at boot time

Encrypt using: AES-128 (Windows clients only)

☐ Encrypt Windows WDE disks and PGP Virtual Disks to a Disk Administrator Key

Import a public PGP key file that may be used to access a Whole Disk Encrypted disk or PGP Virtual Disk. Accessing the disk requires the private portion of the PGP key to be on a supported smart card.

Key: Import...

☐ Encrypt Windows WDE disks to a Disk Administrator Passphrase

Passphrase: Create...

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.

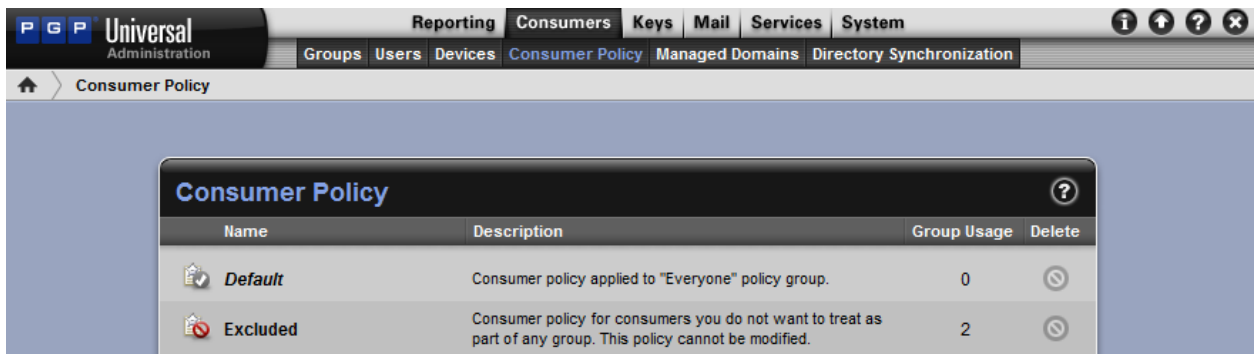


Figure 51: Consumer Policy

11. Click **Default** as shown above.

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



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

The PGP license screen will display like shown below.

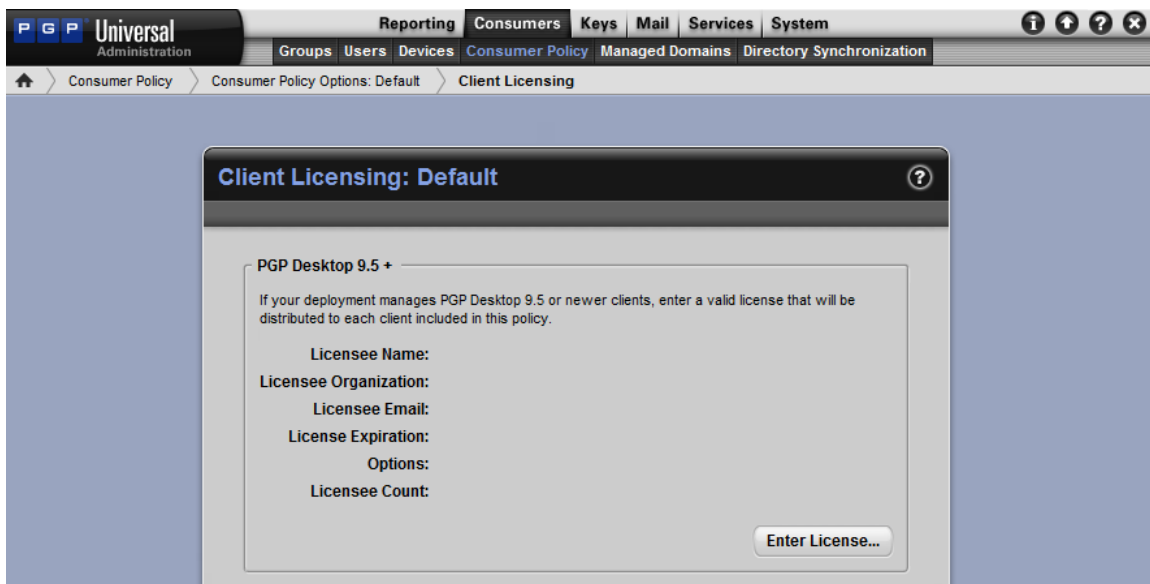


Figure 52: PGP Desktop License Options

13. Click the  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.

The screenshot shows a dialog box titled 'Enter License Information'. It contains four text input fields with labels: 'Licensee Name:', 'Licensee Organization:', 'Licensee Email:', and 'License Number:'. At the bottom of the dialog, there are three buttons: 'Manual', 'Cancel', and 'Save'.

Figure 53: Desktop License

14. If a manual authorization is needed **click** the  button as seen above.

15. Once done **click** .

16. Click  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.

You will see The Groups Policy Screen as shown below.

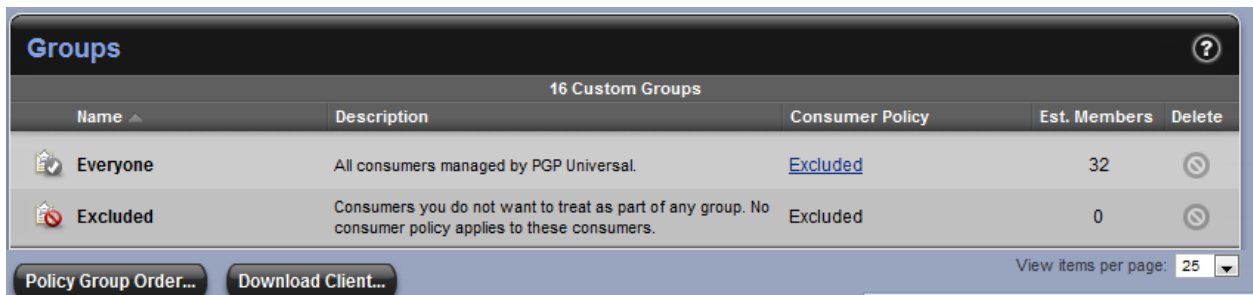


Figure 54: Groups

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

The Download PGP Clients screen will show as below.

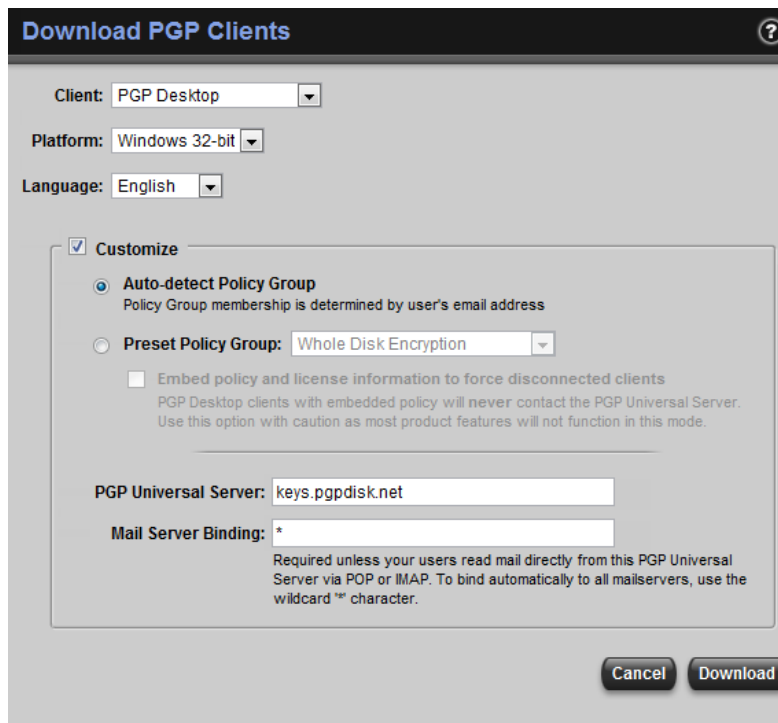
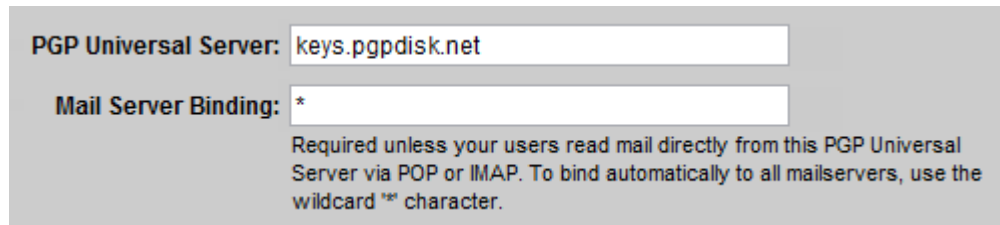


Figure 55: Download PGP Clients

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



PGP Universal Server:

Mail Server Binding:

Required unless your users read mail directly from this PGP Universal Server via POP or IMAP. To bind automatically to all mailservers, use the wildcard "*" character.

Figure 56: Mail Server Binding

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

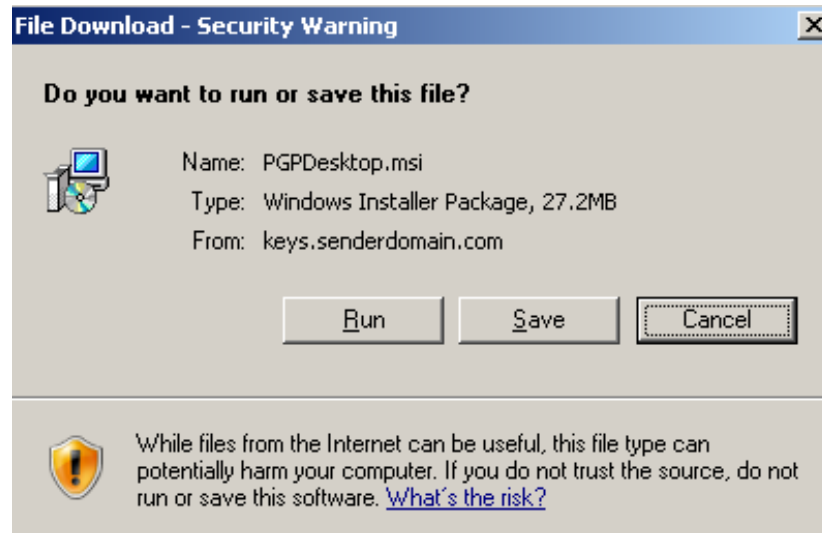


Figure 57: PGP MSI

6. **Click**  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.



Figure 58: End User License Agreement

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

You will now see the release notes as shown below.

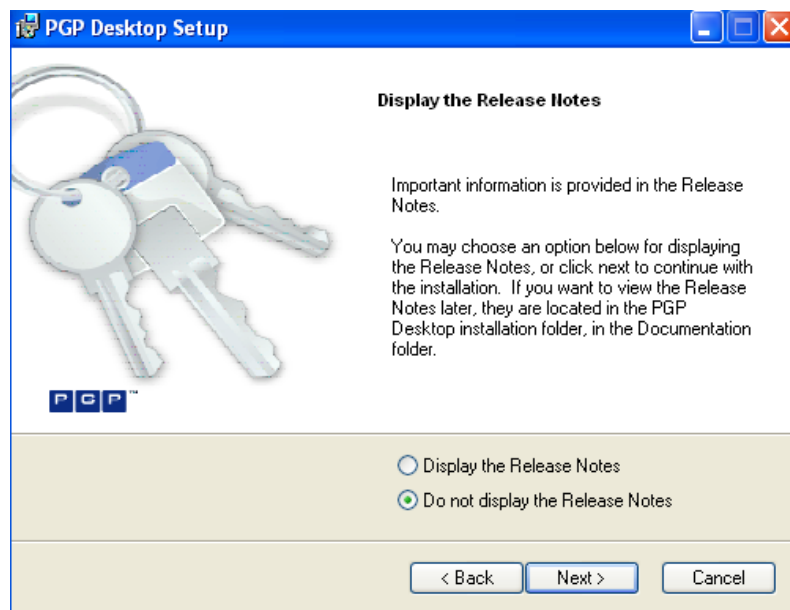



Figure 59: Release Notes

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.

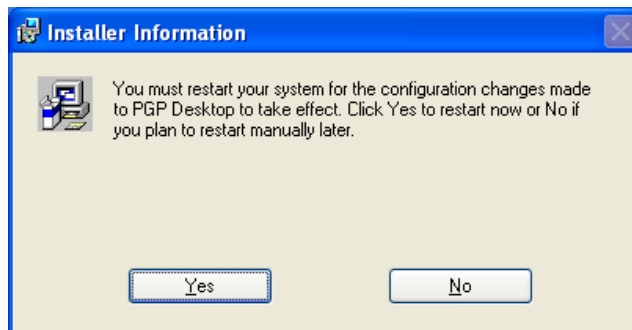


Figure 60: Restart System

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

Windows Login Credentials Screen as shown below.

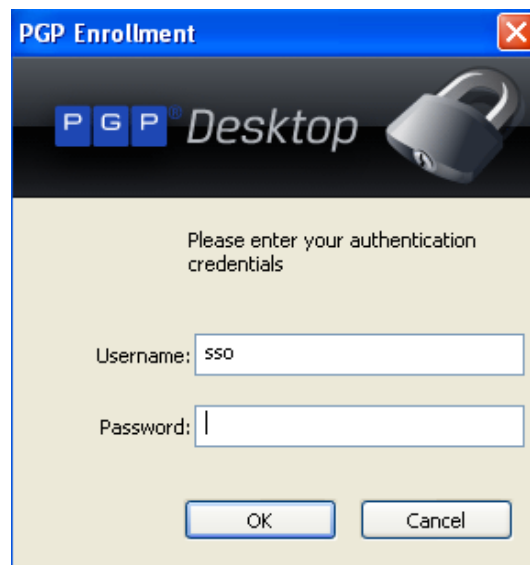


Figure 61: PGP Enterprise Enrollment

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

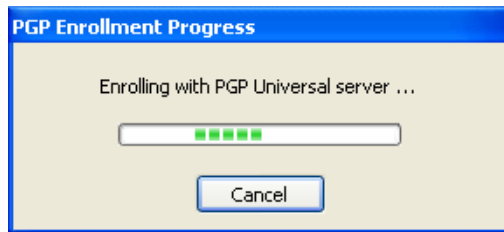



Figure 62: Enrolling

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.

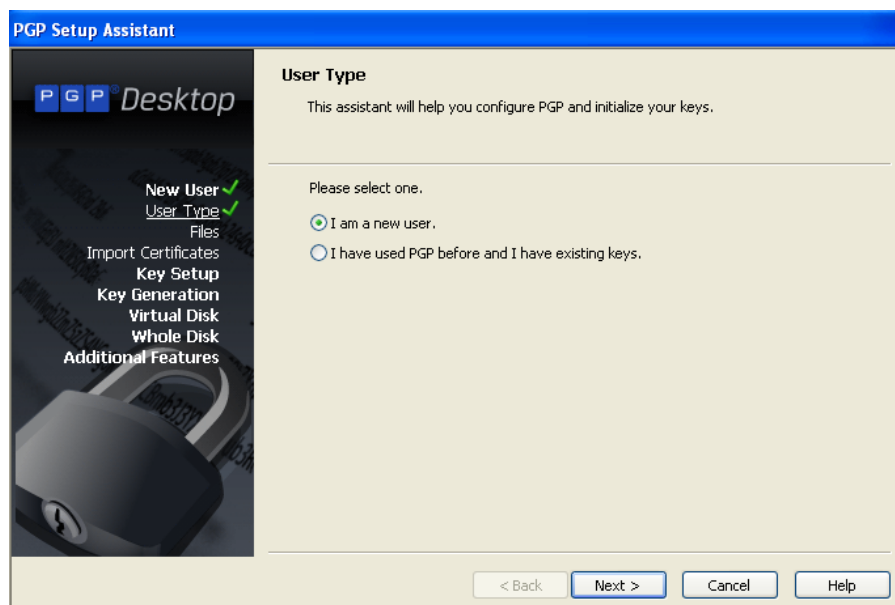


Figure 63: User Type

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

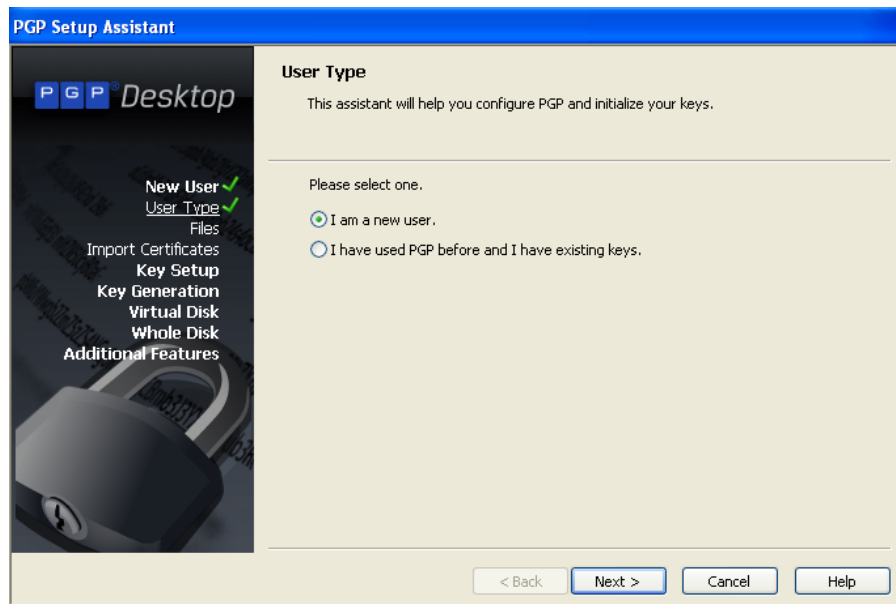



Figure 64: Encryption Assistant

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.

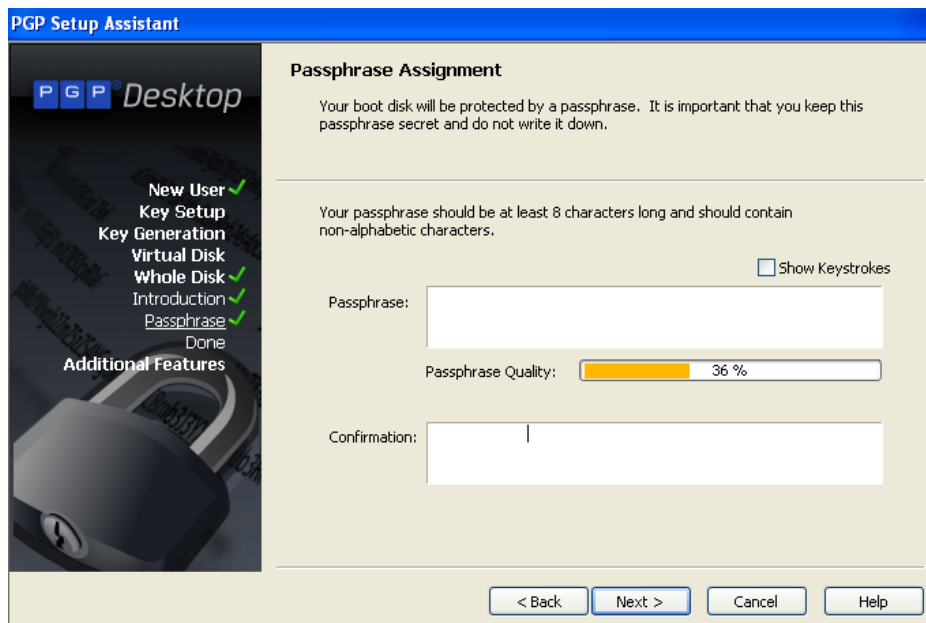



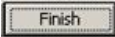
Figure 65: Passphrase Assignment

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.

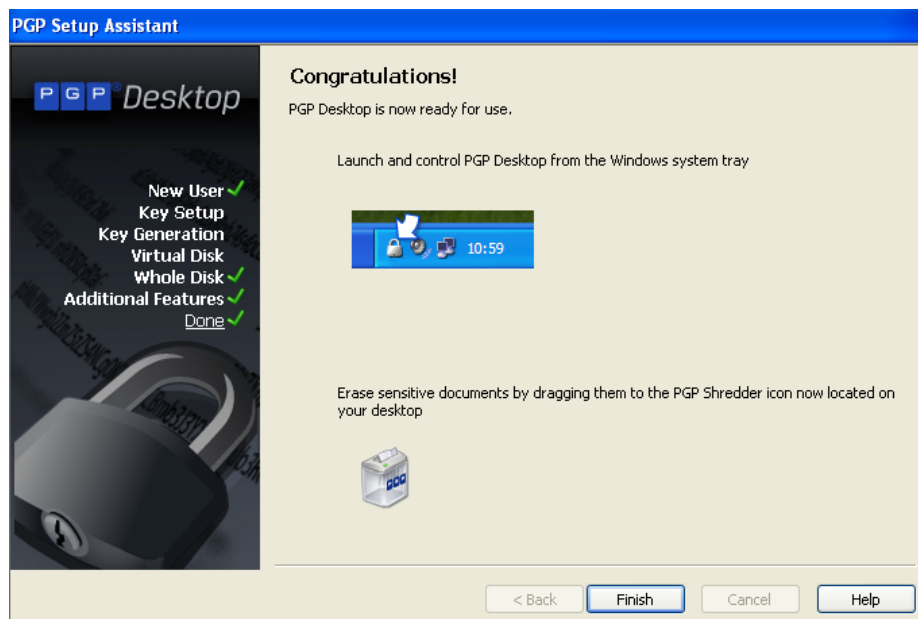



Figure 67: Congratulations

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.

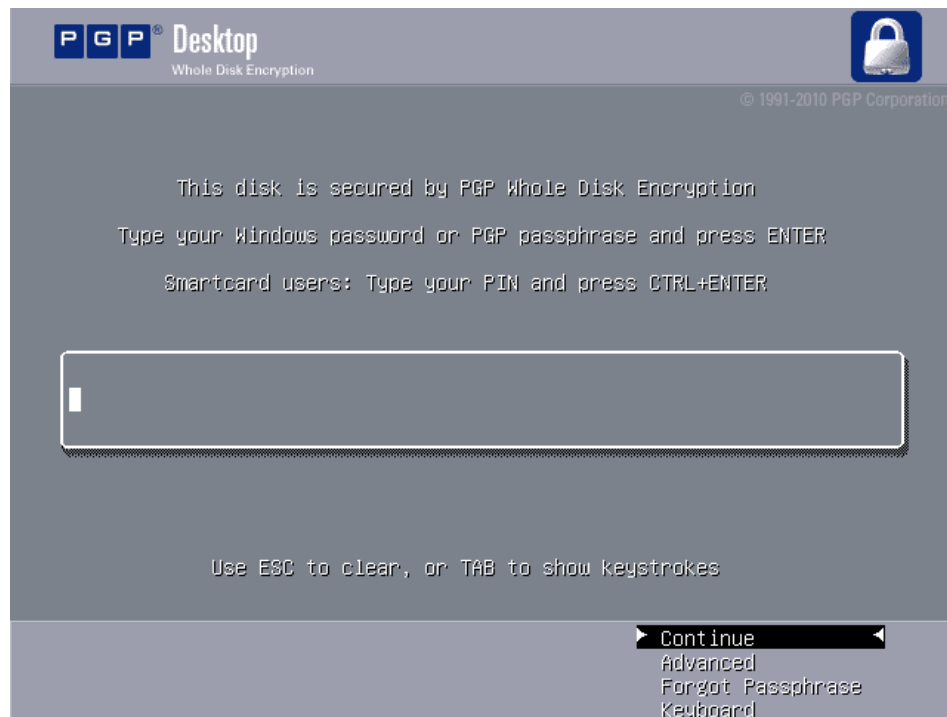
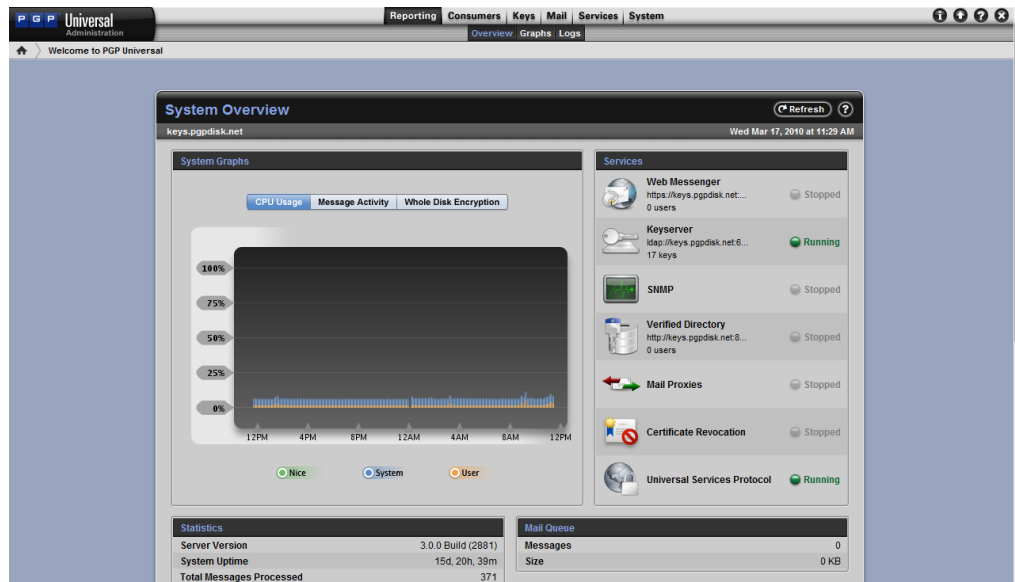


Figure 68: PGP Boot Guard

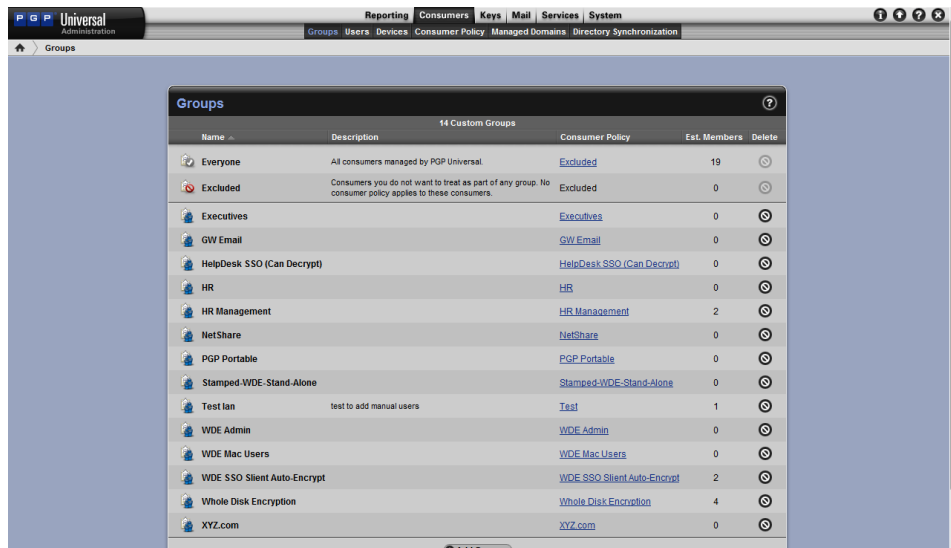
Using the Whole Disk Recovery Token (WDRT)

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

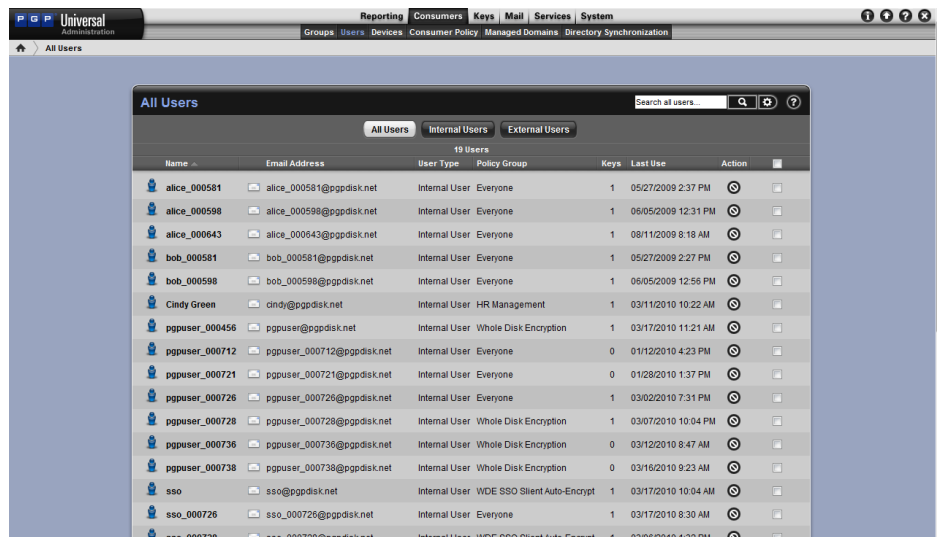
1. Access the Universal™ Server The Universal™ Server System Overview screen displays as shown below.



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



Then **Click the Users tab.**



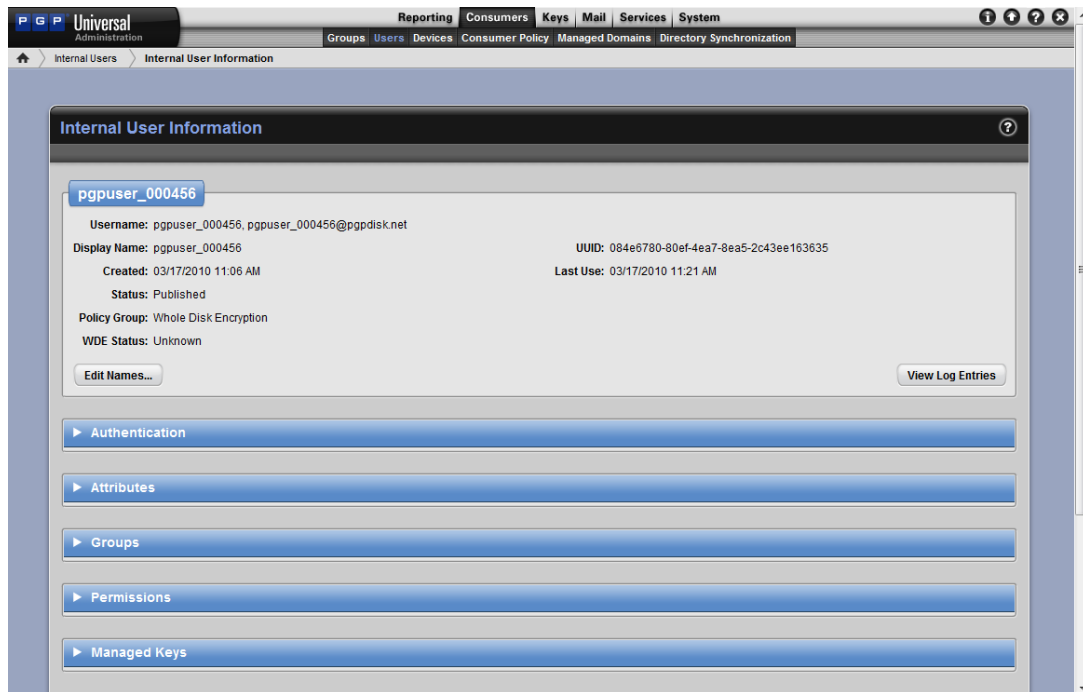
You will see a list of users displayed, including the user you just enrolled, displayed under **Internal Users** (by default the Users Tab defaults to the Internal Users Subtab). You may notice that under the Recovery Column there is an icon of a vault with a combination lock and a red cross on it.

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.



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

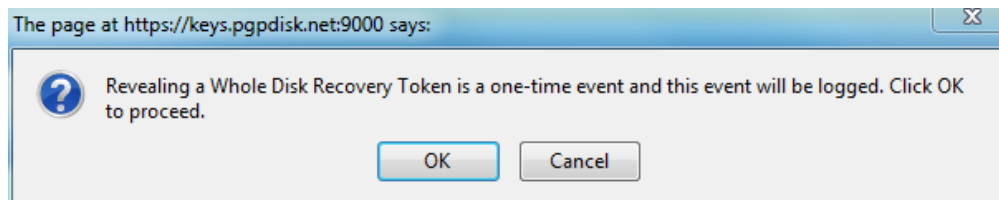
Note how the lower half of the screen changes to display the machines that have available WDRTs for the selected user as shown below.



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 . This icon is used to view the WDRT.

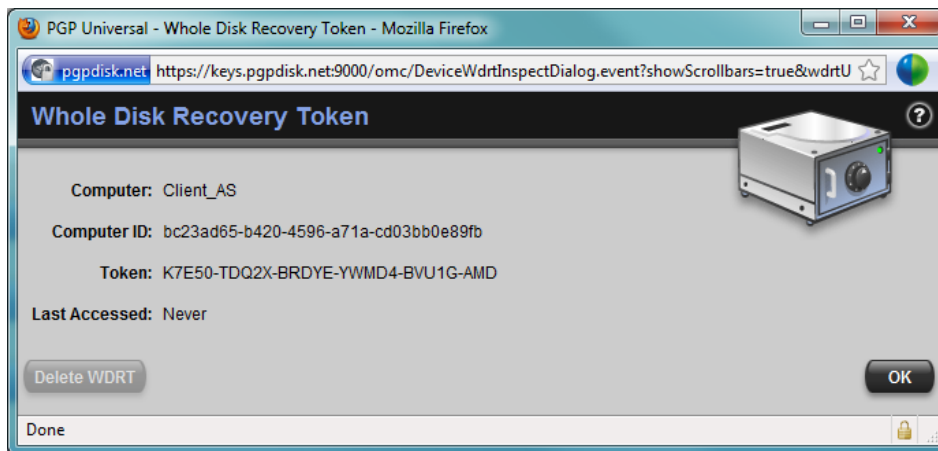
5. **Click** the magnifying glass .

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



6. **Click**  to view the WDRT.

Universal™ Server will display a new window with the Whole Disk Recovery Token as shown.



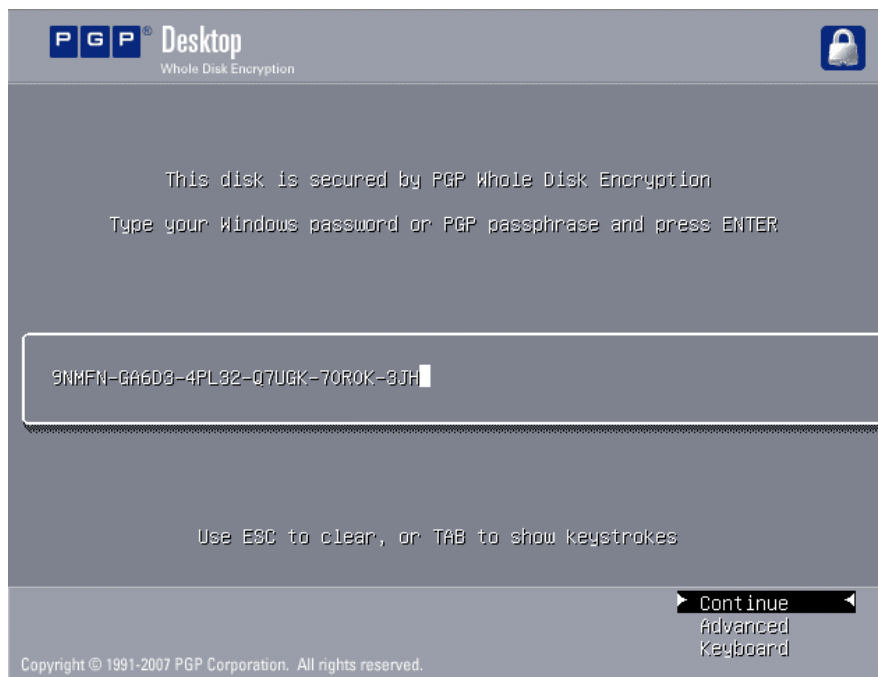
This Token acts as an additional Passphrase to access the encrypted disk. Note that your actual Token will be different than the one shown in this example.

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.

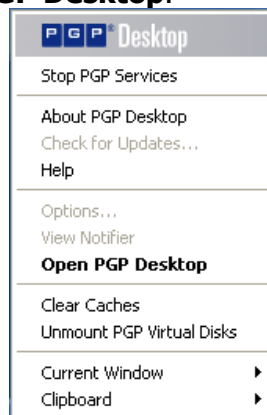
II. Decrypting an Encrypted Drive

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.

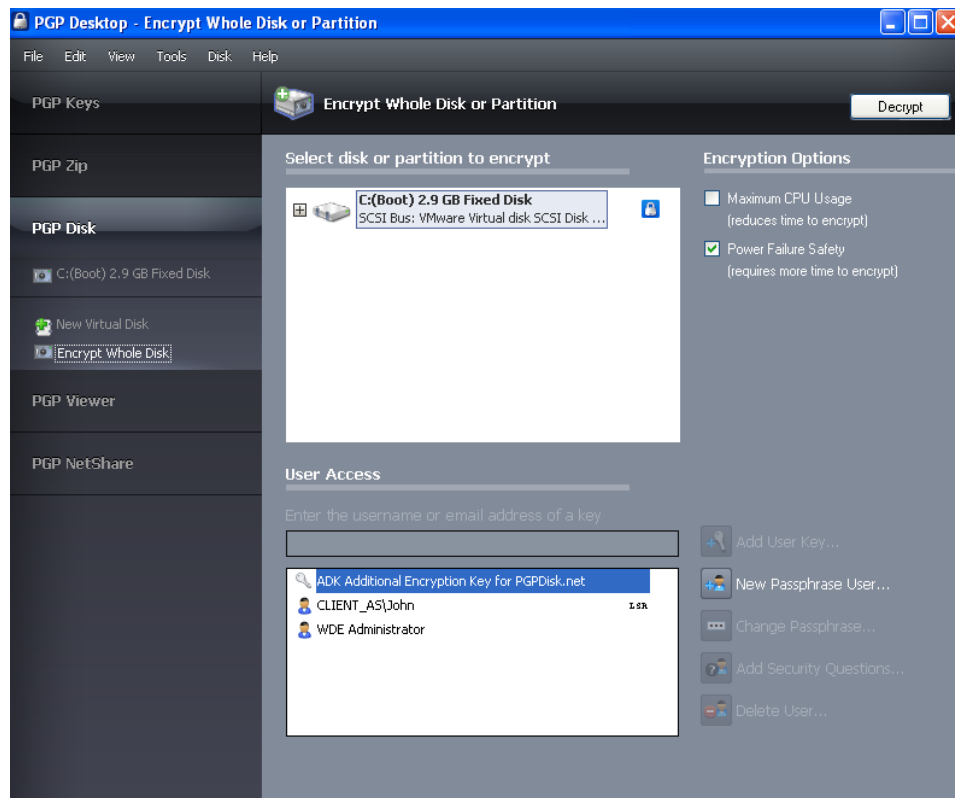
The detailed steps below walk you through the decryption of the USB Disk. Decrypting the Fixed Disk is an identical process, differing only in that for Step 3 of the process you would select the Fixed Disk instead of the USB Disk.

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

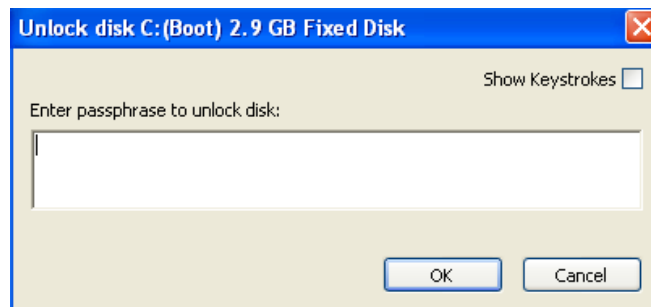


2. The PGP Desktop displays. Since the last time we used PGP Desktop we were in the PGP Disk Control Box we will return to that location when we restart PGP Desktop.

*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.*



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.

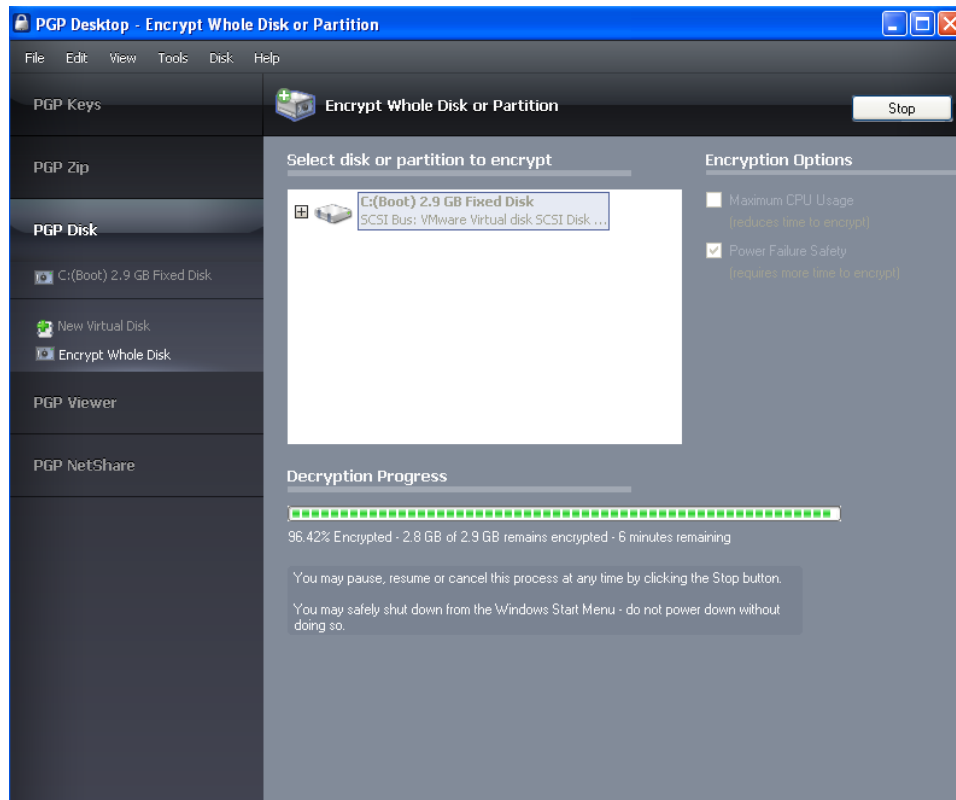


Enter the Passphrase and **Click** to decrypt the disk.

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.



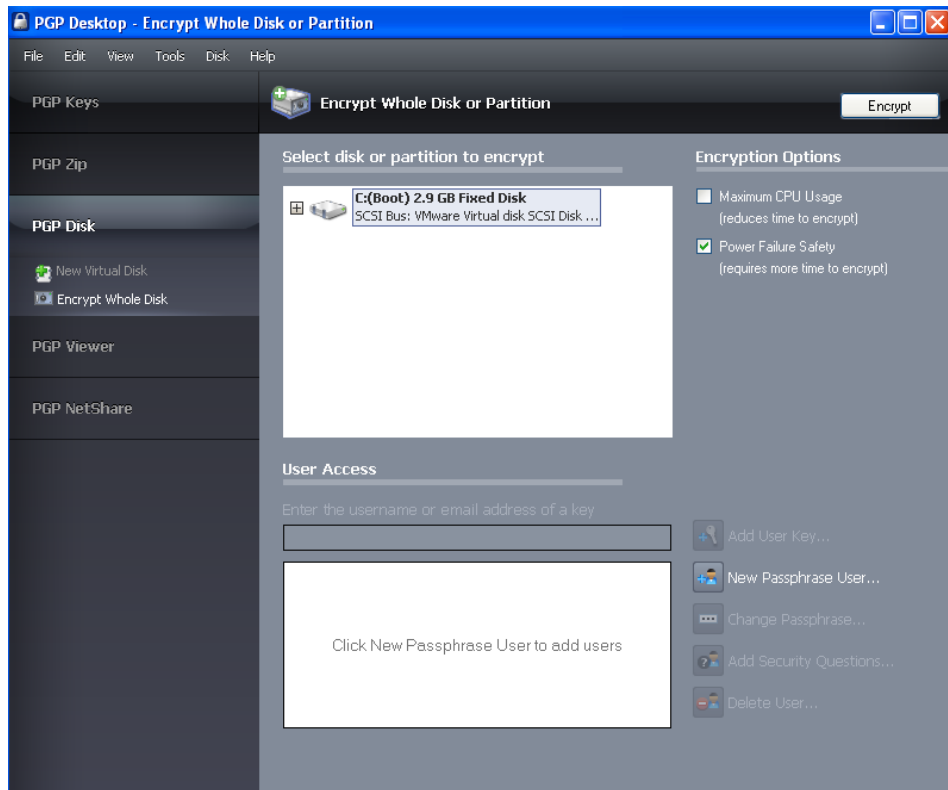
Finally, the PGP Tray icon will change to the Lock with a Spinning Disk indicating an active Whole Disk Operation, in this case decryption.

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.



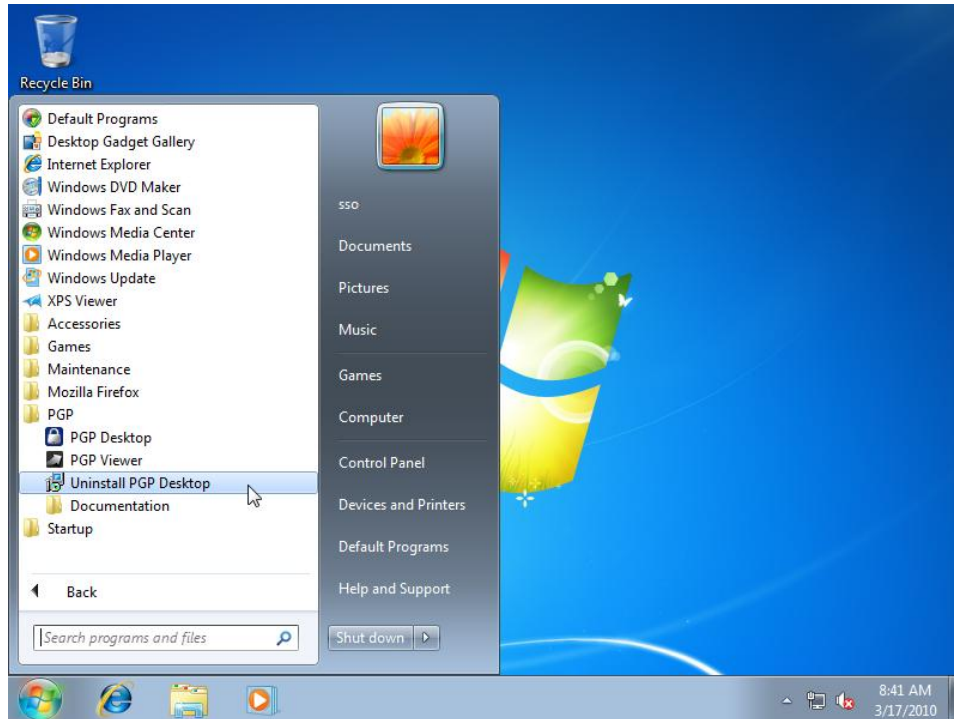
The PGP Tray icon will also change back to the standard Lock icon when the decryption completes. If you are viewing PGP Desktop, the PGP Disk Work Area will now show the fixed boot drive as being unencrypted.



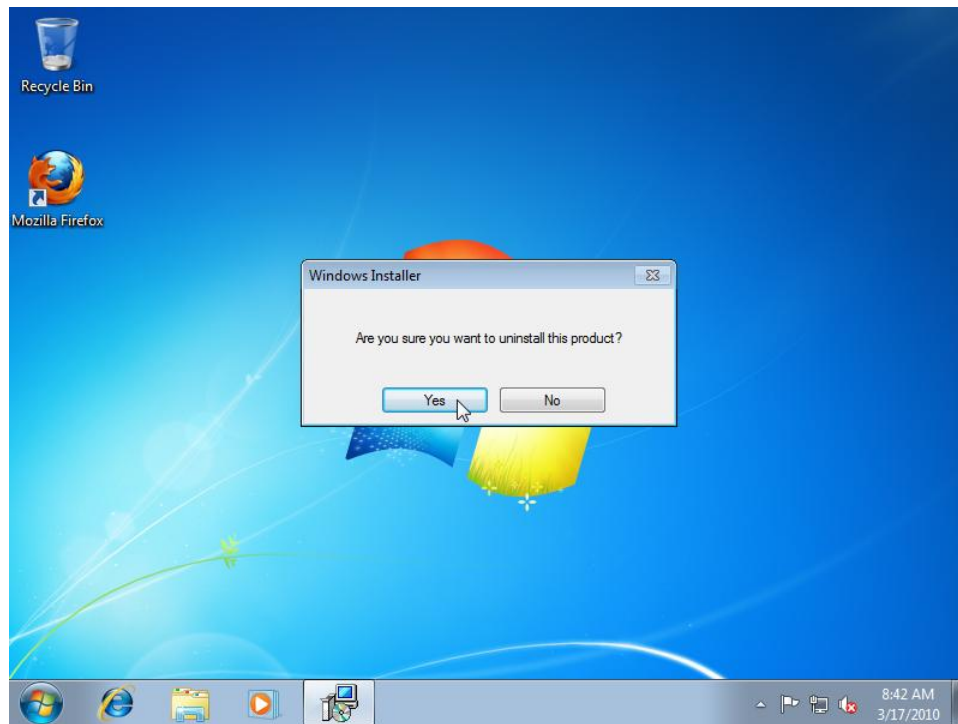
You have successfully decrypted your Fixed Disk.

III. Uninstalling PGP Desktop Software

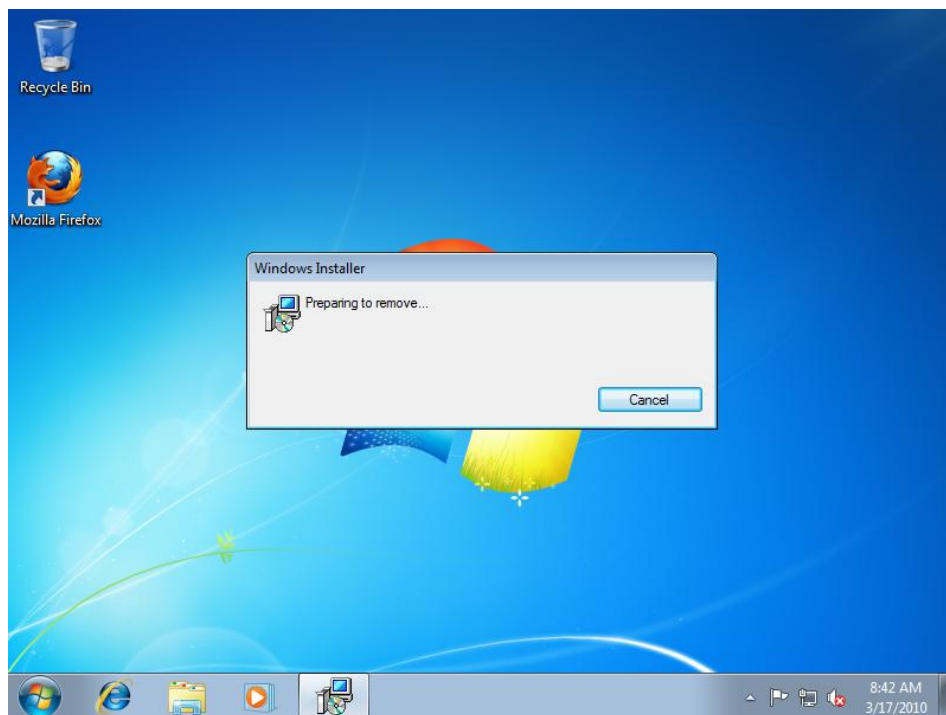
1. Navigate to **Start → All Programs → PGP → Uninstall PGP Desktop** as shown below.



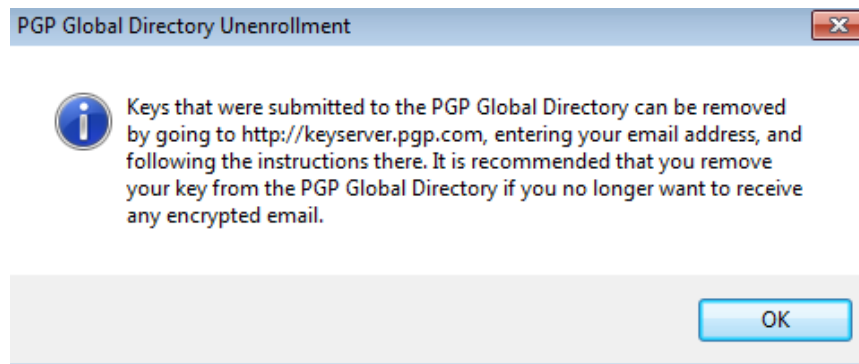
2. Click ☐ when challenged to uninstall the product and follow the onscreen prompts to continue the uninstalling the product.



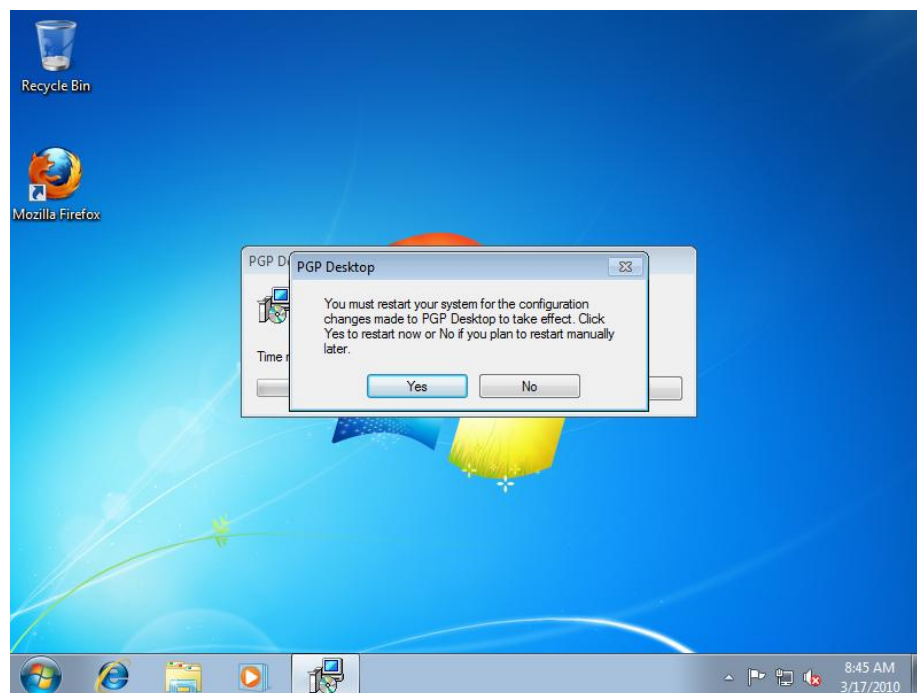
3. A window will display like the one shown below while the uninstall initiates:



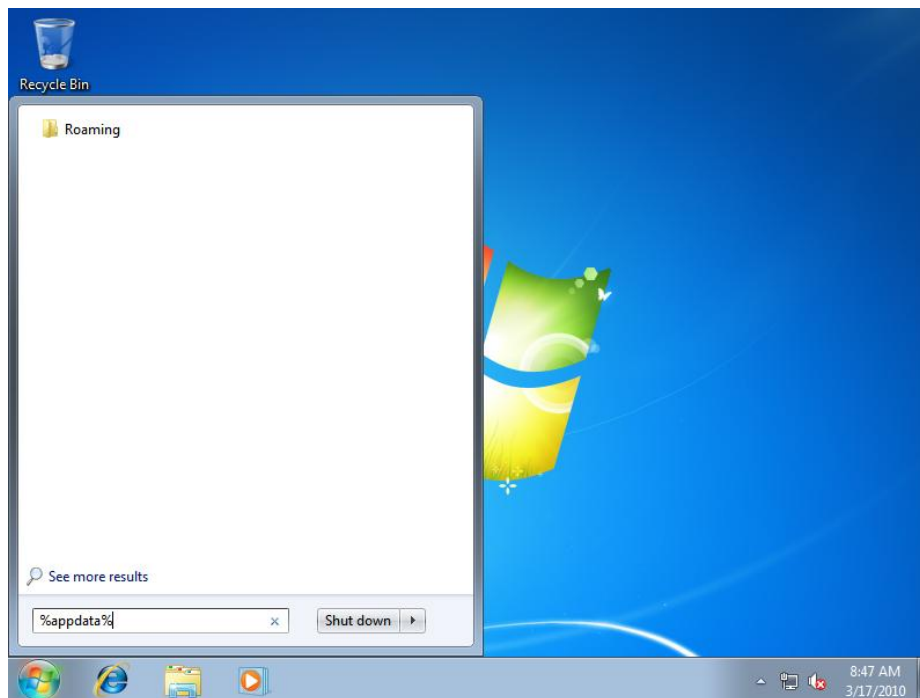
When PGP uninstalls it will notify you to remove your encryption keys as shown below. **Click OK** to continue.



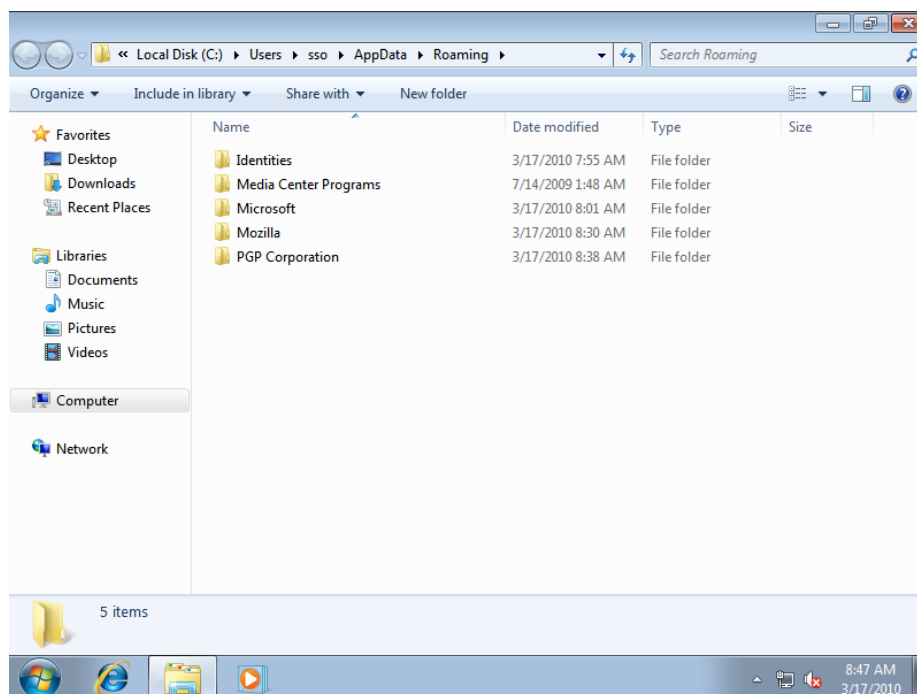
PGP Desktop will continue uninstalling and will prompt you to reboot when finished, as shown below.



4. 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.

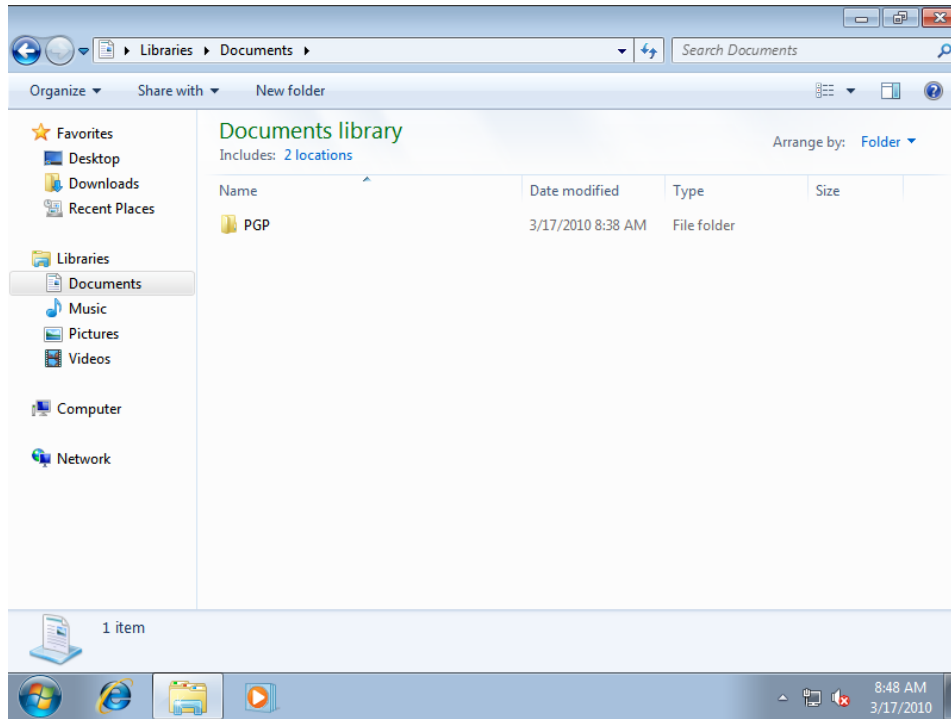


5. The execution of the command will display a new window that will look similar to the one shown below. Note the PGP Corporation Folder.



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.

