PGP® Whole Disk Encryption

Deployment Guide

10.2
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Who Should Read This Guide</td>
<td>3</td>
</tr>
<tr>
<td>Important Terms</td>
<td>3</td>
</tr>
<tr>
<td>Other Relevant Resources</td>
<td>4</td>
</tr>
<tr>
<td>Technical Support</td>
<td>5</td>
</tr>
<tr>
<td>Contacting Technical Support</td>
<td>5</td>
</tr>
<tr>
<td>Licensing and registration</td>
<td>6</td>
</tr>
<tr>
<td>Customer service</td>
<td>6</td>
</tr>
<tr>
<td>Support agreement resources</td>
<td>6</td>
</tr>
<tr>
<td>Understanding PGP Whole Disk Encryption</td>
<td>9</td>
</tr>
<tr>
<td>About PGP Whole Disk Encryption</td>
<td>9</td>
</tr>
<tr>
<td>Components of a Typical PGP WDE Deployment</td>
<td>10</td>
</tr>
<tr>
<td>How Does PGP Whole Disk Encryption Work?</td>
<td>10</td>
</tr>
<tr>
<td>About PGP Universal Server</td>
<td>11</td>
</tr>
<tr>
<td>Major Steps</td>
<td>13</td>
</tr>
<tr>
<td>Preparation</td>
<td>15</td>
</tr>
<tr>
<td>Placing the PGP Universal Server in Your Network</td>
<td>15</td>
</tr>
<tr>
<td>Adding the PGP Universal Server to your Network</td>
<td>16</td>
</tr>
<tr>
<td>Deployment Options</td>
<td>16</td>
</tr>
<tr>
<td>Configuring your Firewall</td>
<td>16</td>
</tr>
<tr>
<td>Understanding Enrollment</td>
<td>17</td>
</tr>
<tr>
<td>Understanding the Two Enrollment Paths</td>
<td>18</td>
</tr>
<tr>
<td>Understanding the LDAP Directory Synchronization Feature</td>
<td>18</td>
</tr>
<tr>
<td>Understanding Policies</td>
<td>19</td>
</tr>
<tr>
<td>Preparing End-User Systems</td>
<td>19</td>
</tr>
<tr>
<td>Installation and Configuration</td>
<td>21</td>
</tr>
<tr>
<td>Before You Install</td>
<td>21</td>
</tr>
<tr>
<td>Installing the Server Software</td>
<td>21</td>
</tr>
<tr>
<td>Configuring the PGP Universal Server</td>
<td>23</td>
</tr>
<tr>
<td>Removing Unneeded Services</td>
<td>23</td>
</tr>
<tr>
<td>Setting Up Administrators</td>
<td>24</td>
</tr>
<tr>
<td>Establishing Backups</td>
<td>24</td>
</tr>
<tr>
<td>Securing your PGP Universal Server</td>
<td>25</td>
</tr>
<tr>
<td>Configuring Policies</td>
<td>25</td>
</tr>
<tr>
<td>Configuring the LDAP Directory Synchronization Feature</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Enrollment</td>
<td>27</td>
</tr>
<tr>
<td>Email Enrollment</td>
<td>27</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Directory Synchronization Enrollment</td>
<td>28</td>
</tr>
<tr>
<td>Establishing PGP WDE Client Settings</td>
<td>29</td>
</tr>
<tr>
<td>General Settings</td>
<td>29</td>
</tr>
<tr>
<td>Key Settings</td>
<td>30</td>
</tr>
<tr>
<td>Key Generation Settings</td>
<td>30</td>
</tr>
<tr>
<td>Key Mode Settings</td>
<td>31</td>
</tr>
<tr>
<td>Certificates Settings</td>
<td>31</td>
</tr>
<tr>
<td>Options Settings</td>
<td>33</td>
</tr>
<tr>
<td>PGP Desktop Settings</td>
<td>33</td>
</tr>
<tr>
<td>General Tab</td>
<td>34</td>
</tr>
<tr>
<td>Messaging &amp; Keys Tab</td>
<td>36</td>
</tr>
<tr>
<td>File Encryption Tab</td>
<td>37</td>
</tr>
<tr>
<td>NetShare Tab</td>
<td>38</td>
</tr>
<tr>
<td>Disk Encryption Tab</td>
<td>38</td>
</tr>
<tr>
<td>Licensing Settings</td>
<td>43</td>
</tr>
<tr>
<td>Creating the PGP WDE Client Installer</td>
<td>45</td>
</tr>
<tr>
<td>Creating an Installer with Auto-Detect Policy</td>
<td>45</td>
</tr>
<tr>
<td>Creating an Installer with Preset Policy</td>
<td>46</td>
</tr>
<tr>
<td>Creating an Installer with No Policy Settings</td>
<td>47</td>
</tr>
<tr>
<td>Controlling PGP WDE Components</td>
<td>49</td>
</tr>
<tr>
<td>Testing the PGP WDE Client Installer</td>
<td>51</td>
</tr>
<tr>
<td>Deploying the PGP WDE Client Installer</td>
<td>53</td>
</tr>
<tr>
<td>Assisting Your PGP WDE Users</td>
<td>55</td>
</tr>
<tr>
<td>The End-User Experience</td>
<td>57</td>
</tr>
<tr>
<td>During the Installation Process</td>
<td>57</td>
</tr>
<tr>
<td>During WDE Setup</td>
<td>58</td>
</tr>
<tr>
<td>During Normal Usage</td>
<td>58</td>
</tr>
</tbody>
</table>
Overview

This Guide describes how to create, deploy, and manage the PGP Whole Disk Encryption (WDE) product in an enterprise environment, using the PGP Universal Server product as the management console.

Some of the information in this Guide also applies to deploying any PGP Desktop client product.

Who Should Read This Guide

This Guide assumes you are an IT or support professional who will be performing one or more of the following deployment tasks:

- Setting up and configuring the PGP Universal Server as the management console.
- Understanding and configuring PGP WDE client options.
- Creating, testing, and distributing the PGP WDE client installers.
- Preparing your end users for a successful installation.

This Guide assumes you have already read the *PGP Universal Server Administrator's Guide* and have installed and used a PGP Universal Server.

**Note:** PGP Corporation strongly recommends you take the time to understand your goals for the software products available from PGP Corporation and your organization's plans for them, both now and in the future. The decisions you make now in deploying PGP WDE affect how you can do things in the future. For example, your choice of key mode now will impact decisions you make later.

Important Terms

**PGP Whole Disk Encryption:** A software product from PGP Corporation that secures files stored on protected drives with transparent full disk encryption. It also includes other encryption features. PGP Whole Disk Encryption is available for Windows, Mac OS X, and Linux systems.
**Overview**

Other Relevant Resources

**full disk encryption:** A security industry term for encryption of all data on a drive below the application layer.

**PGP Universal Server:** A software/hardware product from PGP Corporation used for configuration and management of PGP Corporation encryption applications, including PGP WDE.

**Whole Disk Recovery Token:** A feature of PGP WDE where a recovery token is created that can later be used to recover access to a drive if the normal authentication method is no longer available.

**key mode:** One of the four "modes" in which a PGP keypair can be created. Different key modes are more appropriate for different usage scenarios, so be sure to pick the key mode most appropriate for your needs.

**LDAP directory synchronization:** an optional feature of PGP Universal that lets your PGP Universal Server query your organization's LDAP directory server (a Microsoft Active Directory server, for example), thus taking advantage of existing information about configured users and their authentication credentials.

**enrollment:** A process during installation of PGP WDE client software where the PGP WDE client synchronizes with the PGP Universal Server. The enrollment process establishes the relationship between the client and the server, binding the managed client to the specific PGP Universal Server. During enrollment, and when appropriate afterwards, the PGP WDE client receives encryption keys, policies, and management updates from the PGP Universal Server.

---

**Other Relevant Resources**

*Note:* This document focuses on details surrounding deployment of the PGP WDE product. However, the first step in deploying PGP WDE is to install and configure the PGP Universal Server product, which you will use to manage your PGP WDE clients. Deployment of the PGP Universal Server itself is described at a very high level in this document. Refer to the *PGP Universal Administrator's Guide* for detailed deployment information.

Use this *PGP WDE Deployment Guide* in conjunction with the following resources:

- **PGP Universal Administrator's Guide:** The *Administrator's Guide* explains how to set up the PGP Universal Server you will be using as a management console. Specifically, the *PGP Universal Administrator's Guide* describes configuring your PGP Universal Server, using the server to establish settings for your PGP WDE clients, and creating PGP WDE client installers.

- **PGP Universal Installation Guide:** The *Installation Guide* describes how to install the PGP Universal software onto a system.

- **PGP WDE Quick Start Guide (QSG):** The *Quick Start Guide* introduces you to the features of the PGP WDE product. Consider distributing the PGP WDE QSG to your end users to introduce them to the product.

- **PGP Desktop User's Guide:** The *User's Guide* describes how to use PGP WDE on Windows and Mac OS X systems. If you want more information about the PGP WDE product than is provided in the PGP WDE QSG, consult the *PGP Desktop User's Guide*.

- **PGP WDE for Linux User's Guide:** The *User's Guide* describes how to use PGP WDE on Linux systems.
Technical Support

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

Symantec’s support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information
Overview

Technical Support

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan  
customercares_apac@symantec.com

Europe, Middle-East, Africa  
semea@symantec.com

North America, Latin America  
supportsolutions@symantec.com
2

Understanding PGP Whole Disk Encryption

This section tells you about PGP WDE and shows a typical PGP WDE deployment.

In This Chapter

About PGP Whole Disk Encryption ................................................................. 9
Components of a Typical PGP WDE Deployment ............................................. 10
How Does PGP Whole Disk Encryption Work? ............................................... 10
About PGP Universal Server ........................................................................... 11

About PGP Whole Disk Encryption

PGP WDE is a software product from PGP Corporation that secures files stored on protected drives with transparent full disk encryption. If a protected system is lost or stolen, data stored on the protected drive is completely inaccessible without the proper authentication.

Note: PGP WDE runs on Windows, Mac OS X, and Linux systems. Only Intel-based systems running Mac OS X 10.4.10 or later support whole disk encryption of the boot disk. PGP WDE on Linux systems has a command-line interface and supports PGP WDE functionality only.

The PGP WDE product also provides the following functionality for your Windows and Mac OS X users:

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

PGP WDE is both a product sold by PGP Corporation and a feature in several PGP Corporation products.

When this Guide refers to "PGP WDE," it refers to the PGP WDE product. Bear in mind, however, that "whole disk encryption" is only one feature of the PGP WDE product on Windows and Mac OS X systems. On Linux systems, whole disk encryption is the only feature.
Components of a Typical PGP WDE Deployment

The following are elements of a typical PGP WDE deployment:

1. **PGP Whole Disk Encryption** is a software product that locks down the contents of your system. To deploy PGP WDE, you must install the PGP WDE software on a client system via a customized installer you create using the PGP Universal Server.

2. **PGP Universal Server** is a platform for creation and management of PGP Corporation encryption applications, including PGP WDE. The PGP Universal Server must be able to communicate with your PGP WDE clients so that it can:
   - provide a pre-configured installer for the system.
   - enroll and bind the client to the server.
   - provide and enforce policies.
   - provide recovery options.

3. **Directory/LDAP Server** (for example, Active Directory). An LDAP server:
   - provides an authentication mechanism during PGP WDE client enrollment/installation.
   - enables you to synchronize groups for policy application.
   - leverages existing information about the user (email, DN, user certs, and so on).

4. Your **DNS server** needs to be configured to support your PGP Universal Server; be sure to coordinate with your IT group to ensure a successful installation.

How Does PGP Whole Disk Encryption Work?

The following is an overview of the PGP WDE encryption process and subsequent user experience.

1. The PGP WDE passphrase or token user...
2. ... encrypts the boot drive on their system automatically or manually.
3. The drive is transparently encrypted sector by physical sector.
4. Once encryption begins, and thereafter, the PGP WDE user must authenticate via the PGP BootGuard screen.
5 To access the system, the user enters a passphrase or inserts the USB token (Windows and Mac OS X systems only) and then authenticates.

6 If the Single Sign-On feature is enabled on Windows systems, the system automatically logs in to Microsoft Windows.

System behavior is the same as it was prior to encryption.

About PGP Universal Server

**PGP Universal Server** is a platform for central management and deployment of PGP Corporation encryption applications, including PGP WDE. You use the PGP Universal Server to configure PGP WDE client options, provide custom policies and settings for your PGP WDE users, create the client installers, and manage the clients after installation (including Whole Disk Recovery Tokens for each managed client, for example).
This Guide is organized into sections that correspond with the order PGP Corporation recommends you use to deploy PGP WDE. Depending on your environment, you may perform some of these tasks in a slightly different order.

This Guide covers the steps to take to configure and deploy PGP WDE clients using a PGP Universal Server as the management console:

1  **Preparation.** Learn what you need to do before you install the PGP Universal Server, including:
   - where to put your PGP Universal Server in your network.
   - what you need to know to add the PGP Universal Server to your network.
   - how to configure your firewall to support the PGP Universal Server.
   - how to choose the enrollment method your PGP WDE users will use.
   - how to set up LDAP directory synchronization (if applicable).

2  **Installation and configuration.** Describes the process of installing the PGP Universal Server software and steps you through the configuration wizard. All PGP Universal setups go through this process, but there are some things specific to deployments.

3  **Configuring the PGP Universal Server.** Describes the features of your PGP Universal Server that impact your deployment:
   - directory synchronization
   - enrollment
   - administrative user email setup
   - automated backups
   - removal of unneeded services
   - other desirable services
   - policies

4  **Setting PGP WDE client options.** Summarizes the PGP WDE settings you control so that you can appropriately configure them to reflect your organization’s security requirements.

5  **Creating the PGP WDE client installer.** Describes the process of creating the actual client installer executable.

6  **Testing the client installer.** Lists ways you can test your client installer before full deployment.

7  **Deploying the client installer to end users.** Provides options for deploying the client installer executable to your end users.

8  **Assisting your users.** Discusses some of the things you can do to help prepare your end users for the new software they will be receiving.
Preparation

Preparation consists of things you need to do or to understand before you begin installing your PGP Universal Server as your management console:

- Where to put your PGP Universal Server in your network.
- What you need to know to add the PGP Universal Server to your network.
- How to configure your firewall to support the PGP Universal Server.
- Understanding the LDAP Directory Synchronization feature.
- Understanding policy options.
- Understanding enrollment methods.
- Making sure the systems on which PGP WDE will be installed are appropriately prepared.

In This Chapter

Placing the PGP Universal Server in Your Network ................................................15
Adding the PGP Universal Server to your Network................................................. 16
Configuring your Firewall............................................................................................ 16
Understanding Enrollment.......................................................................................... 17
Understanding the Two Enrollment Paths ...............................................................18
Understanding the LDAP Directory Synchronization Feature ..............................18
Understanding Policies ...............................................................................................19
Preparing End-User Systems.......................................................................................19

Placing the PGP Universal Server in Your Network

As a best practice, PGP Corporation recommends placing the PGP Universal Server in your DMZ for use as a management console for your PGP WDE deployment.

This allows both internal and external users access to the server (for example, if you have laptop users who travel, you cannot count on them being on the VPN when they install the PGP WDE client).

For details on the tasks involved in placing your server, see the PGP Universal Administrator’s Guide.
Adding the PGP Universal Server to your Network

Once you have determined a network location for your PGP Universal Server, you must do the following:

**Note:** You may need to consult with your network and/or system engineering teams to support the deployment of your PGP Universal Server.

- Assign an appropriate IP address to the PGP Universal Server.
- Configure the appropriate subnet and gateway.
- Configure the appropriate hostname and DNS.

**Note:** The use of forward and reverse DNS is required; using a host files is not sufficient.

Make sure the DNS includes appropriate A and PTR records that are in place prior to installation of the PGP Universal Server.

Also make sure the DNS is reachable by the PGP Universal Server in the DMZ.

Deployment Options

There are other options to consider at this point:

- Do you want to replace the default self-signed server SSL certificate with a real SSL certificate?

  PGP Corporation strongly recommends that you obtain a valid SSL/TLS certificate for each of your PGP Universal Servers from a public Certificate Authority (CA), such as GeoTrust, available at the PGP Online Store (https://store.pgp.com/). This ensures that clients will have confidence in establishing secure communications with your servers. An in-house CA will not be recognized by the PGP WDE client.

- Are you going to use DNS round robin or a load balancer with your PGP Universal Server?

  If so, acquire the proper number of IP addresses or VIP addresses required for each machine in the cluster as well as proper DNS forward and reverse pointers. Getting this information in advance will help to ensure a smooth implementation.

Configuring your Firewall

The PGP WDE clients you are deploying will be in contact with your PGP Universal Server management server on a regular basis. They must be able to communicate with each other; otherwise, many aspects of your deployment will not work. Also, the management console needs certain ports open on your firewall for a variety of purposes.

Firewall changes should be done before you install the PGP Universal Server.

Specifically:
Clients must be able to access the management server via HTTPS on port 443; allow traffic in both directions.

The management server must be able to make LDAP and LDAPS queries on ports 389 and 636, respectively, to the LDAP server you are using for directory synchronization.

If you are using email enrollment, no LDAP connectivity is required internally, but external LDAP access may be required to support other PGP WDE functionality; key lookups or file/folder encryption, for example.

The management server needs Internet access on port 80 for updates and licensing. Only outbound access on port 80 is required.

Licensing can be done manually without Internet connectivity, but requires pre-authorization from PGP Customer Support (support.pgp.com).

The management server needs FTP or SCP access on ports 21 or 22, respectively, for delivery of backups to an appropriate location.

Regular backups are important to support the ability to recover from unexpected failure of the PGP Universal Server. PGP Corporation strongly recommends you set up regular schedule of backups of the data on your PGP Universal Server.

You will be configuring the PGP Universal Server you are using as a management server via its web-based administrative interface using HTTPS on port 9000, so this port needs to be open.

Enabling SSH access to the management server on port 22 will give you access should web-based access be down for some reason.

Notification emails from the management server to administrators of the PGP Universal Server are sent via SMTP on port 25, so that port should be open between the PGP Universal Server and the mail server that will accept email from administrators.

---

**Understanding Enrollment**

PGP WDE clients synchronize with their PGP Universal Server during installation via the PGP client *enrollment* process. Once enrolled with their PGP Universal Server, clients receive encryption keys, policies, and management updates from the PGP Universal Server. The enrollment process establishes the relationship between the client and the server, binding the managed client to the specific PGP Universal Server.

There are two methods for enrolling your PGP WDE users:

- **LDAP Directory Synchronization**: Requires that the LDAP Directory Synchronization feature be enabled (and correctly configured) and the *Enroll clients using directory synchronization* checkbox be selected on the Directory Synchronization screen in the PGP Universal Server's management interface. To enroll, the client will provide authentication credentials to the LDAP directory specified in the LDAP Directory Synchronization feature.
- **Email**: Requires only that the PGP WDE client and the management server are able to communicate via SMTP email. This method is available for all client installations, provided there is a usable email account on the client system. This method is available even if the PGP Universal Server is not performing email encryption. To enroll with a server, the client sends an email to the PGP Universal Server. The PGP Universal Server will process the email message and then send an email message back to the PGP WDE client, which will use the return email to finalize the enrollment process, and then continue with the installation.

---

### Understanding the Two Enrollment Paths

There are two basic "paths" for deciding how to configure the LDAP Directory Synchronization feature, policies, and enrollment methods:

- If you have an up-to-date LDAP directory server in your organization, you will probably want to enable the LDAP Directory Synchronization feature (and turn enrollment on), select **Auto detect policies**, and use the LDAP Directory Synchronization feature for enrollment. This leverages the information in your LDAP directory and simplifies the job of the administrator.

- If you do **not** have an up-to-date LDAP directory server in your organization, you will want to keep the LDAP Directory Synchronization feature disabled, select **Preset policy**, and use email enrollment.

---

### Understanding the LDAP Directory Synchronization Feature

LDAP Directory Synchronization is a feature of PGP Universal which, if enabled (it is disabled by default), can be used with your PGP WDE deployment. Enabling this feature lets your PGP Universal Server query your organization’s LDAP directory server for information about users and import the appropriate users, thus taking advantage of existing information about users and their authentication credentials.

**Note:** Proper LDAP syntax must be used when you work with the LDAP Directory Synchronization feature.

There are three LDAP Directory Synchronization configuration options:

- **LDAP Directory Synchronization enabled, enrollment on.** The specified LDAP directory will be used to determine which users are in what groups for the purposes of applying the appropriate policy and for enrollment.

- **LDAP Directory Synchronization enabled, enrollment off.** The specified LDAP directory will be used to determine which users are in what groups for the purposes of applying the appropriate policy, but **not** for enrollment purposes. (Email enrollment will be used).

- **Disabled.** LDAP Directory Synchronization is disabled; the PGP Universal Server will not check any LDAP directories in your organization either for users to be imported or for enrollment. (Email enrollment will be used).
Understanding Policies

There are three methods available to determine how your PGP WDE users will receive internal user policies from the PGP Universal Server; which one you choose depends on your particular circumstances.

The three policy methods are:

- **No policy.** Your PGP WDE users can do anything their license allows; they will not receive any policies from the PGP Universal management console.

- **Auto detect policy.** Your PGP WDE users are constrained by the policy that applies to the LDAP directory group they are in. (This option requires that you enable the LDAP Directory Synchronization feature.) Using this policy option means that the most appropriate policy will be selected automatically and applied for the LDAP directory group your users are in. Users could have a different policy applied in the future if a new policy is created that is more appropriate for their LDAP directory group.

- **Preset policy.** Your PGP WDE users are constrained by the settings of the selected preset policy, either default policy or a custom policy you create. You can change the settings of the selected preset policy in the future and the new settings will apply to the users constrained by the policy, with the exception of actions taken at installation.

Preparing End-User Systems

PGP Corporation strongly recommends you check the PGP Desktop, PGP WDE for Linux, and PGP Universal Release Notes to make sure the systems in your deployment environment are ready for installation of both the server and WDE client.

- Make sure clients meet the listed minimum system requirements.
- Determine whether the email clients used in your environment are supported clients.
- Verify that your anti-virus and firewall software is compatible.
- Review the list of known software conflicts and ensure you will not encounter these in your deployment.
- Ensure that target client systems include scandisk (Windows chkdsk.exe, for example, or SpinRite or Norton Disk Doctor, if available) and defragmentation (Windows defrag.exe, for example, or PerfectDisk, if available) software, for preparing their drives for installation of PGP WDE.
This section describes the installation process at a high level. For a more detailed description of each activity, see the *PGP Universal Administrator's Guide*.

In This Chapter

Before You Install ................................................................. 21
Installing the Server Software ............................................. 21

Before You Install

Before you install the software, ensure you have the following available to you:

- The appropriate hardware on which to install the PGP Universal Server software. The current PGP Universal Server Certified Hardware List is located in the most recent version of the *PGP Universal Release Notes*.
- The most recent version of the PGP Universal Server software.
- The most recent version of the *PGP Universal Administrator's Guide*.


Installing the Server Software

1. Perform the default installation of the PGP Universal Server software, as described in the *PGP Universal Server Installation Guide*.
2. Configure the server using the Setup Assistant. Connect to the PGP Universal Server when the standard installation is complete, as described in the *PGP Universal Server Installation Guide*.
3. On the Welcome screen, read the text, then click the Forward arrow to continue.
4. On the End User License Agreement screen, read the text of the License Agreement, then click the I Agree button.
5. On the Setup Type screen, select New Installation, then click the Forward arrow to continue.
6. On the Date & Time screen, enter the appropriate information, then click the Forward arrow to continue.
7. On the Network Setup screen, verify that the information you entered in the standard installation is correct, and then click the Forward arrow to continue.
8 On the Proxy Configuration screen, click Skip to continue.

9 On the Confirmation screen, verify that the information is correct, and then click Done.
   The server will reboot.

10 When the Licensing screen appears, enter the appropriate licensing information for the PGP Universal Server you are using as a management console, and click Save.

11 On the Administrator Name & Passphrase screen, enter the appropriate information, and then continue.

12 On the Mail Processing screen, select Gateway Placement, and then continue.

13 On the Mail Server Selection screen, enter the appropriate information, and then continue.

14 On the Ignition Keys screen, make the desired selection, and then continue.

15 On the Ignition Keys screen that appears, enter the appropriate information, and then continue.

16 On the Backup Organization Key screen, enter a passphrase to protect your Organization Key, then click Backup Key. An Organization Key will be generated. This key allows you to restore your PGP Universal Server from a backup, should that be necessary. (The other use of an Organization Key, to sign the keys created by the PGP Universal Server, does not apply if you are using the PGP Universal Server only as a management server.)

17 When the Confirmation screen appears, check to make sure the settings are correct, and then click Done.
There are multiple aspects of the PGP Universal Server that you should configure to get it ready for use as a management console:

- Removing unneeded services.
- Setting up administrators.
- Establishing settings for backups.
- Securing the server.
- Configuring policies.
- Configuring the LDAP Directory Synchronization feature (if applicable).
- Configuring enrollment.

In This Chapter

Removing Unneeded Services ................................................................. 23
Setting Up Administrators ................................................................. 24
Establishing Backups ...................................................................... 24
Securing your PGP Universal Server ............................................... 25
Configuring Policies ......................................................................... 25
Configuring the LDAP Directory Synchronization Feature .................. 26
Configuring Enrollment ................................................................... 27

Removing Unneeded Services

Some services provided by the PGP Universal Server are unnecessary if the server is being used only as a management console for PGP WDE clients. PGP Corporation recommends modifying the default settings of these services, as described below, for optimal operation of your management console.

Do the following:

- Navigate to Mail > Proxies and delete the SMTP proxy; it is not needed.
- Navigate to Mail > Mail Routes. Delete all existing entries and add a new entry with an asterisk (*) as the domain name and the IP address of the mail server that will accept mail for delivery from the PGP Universal Server. This will force the PGP Universal Server not to use DNS for mail queries; instead, it will send all mail to the specified mail route.
- Navigate to Services > Web Messenger. Click Disable to deactivate the service.
- Navigate to Services > Keyserver. Click Disable to deactivate the service.
Your PGP Universal Server offers a number of other services that you may or may not want to activate if you are using the server only as a management server. For more information about these services, see the PGP Universal Administrator’s Guide.

Setting Up Administrators

PGP Universal Servers allow multiple administrators and supports different roles for administrators. You can set up an administrator whose access would be limited to handling just Whole Disk Recovery Tokens, for example.

During installation, you create one administrator; this administrator is a superuser, which means they have access to all PGP Universal functionality.

To create additional administrators:

1. From the System > Administrators card, click Add Administrator.
2. In the Login Name field, enter a login name for the new administrator.
3. In the Passphrase field, enter a passphrase for this administrator.
4. In the Confirm field, enter the same passphrase again.
5. In the Email field, enter the email address of the new administrator.
6. Select the Daily Status Email checkbox if you want the new administrator to receive a daily status email for your system.
7. From the Role list, select the role for the new administrator. The privileges for the selected role appear.
8. Click Save. The new administrator is added.

For more information about administrators, see the PGP Universal Administrator’s Guide.

Establishing Backups

PGP Universal Server provides two ways to back up your data: scheduled backups and on-demand backups. Backup files can be stored on the PGP Universal Server, or they can be automatically sent via FTP or via SCP, to a location you specify.

To establish automatic backups

1. Navigate to the System > Backups screen of the administrative interface, and click Backup Schedule. The Backup Schedule dialog appears.
2. Click Enable Scheduled Backups if it is not already selected.
3. Select the boxes representing the names of the days of the week on which you want backups performed.
4. Specify a time for the backups to begin in the Start backups at field.
5. Click Save.
To perform an on-demand backup

1. Navigate to the System > System Backups screen of the administrative interface.
2. Click Backup Now.
3. Enter a Backup Name and click Backup.

A backup of your data is performed immediately. When the backup is complete, it displays in the Backups list.

For more information about backups, see the PGP Universal Administrator’s Guide.

Securing your PGP Universal Server

You can use hardware or software Ignition Keys to protect the data on your PGP Universal Server:

- **Hardware Token Ignition Keys.** When you insert a PKCS#11 token in the PGP Universal Server, the PGP Universal Server will detect it and allow you to use it as an Ignition Key. The token must contain a single key, which must be protected by a PIN. You can cache the token’s PIN so that you do not need to enter the PIN at restart, just have the token present.

- **Soft-Ignition Passphrase Ignition Keys.** A passphrase you specify protects the PGP Universal Server.

For more information about Ignition Keys, see the PGP Universal Administrator’s Guide.

Configuring Policies

As administrator, you control a variety of settings on the PGP WDE software your end users will be using, including key settings, PGP WDE client settings, directory services, client updates, and proxy server settings.

These policies are called consumer policies; the settings here control how your PGP WDE users will use the product. These policies have nothing to do with the mail processing policies that can also be configured on a PGP Universal Server.

To begin configuring policies for your PGP WDE end users, navigate to Consumers > Consumer Policy. The Consumer Policy card appears.

By default, one internal user policy is always created: Default.

You have several options at this point:

- Configure the default Default policy so that it conforms to your organization's security policies and use that policy for your PGP WDE users.

- Create a new consumer policy, configure that policy so that it conforms to your organization's security policies, and then use the new policy for your PGP WDE users.
Configuring the PGP Universal Server

Configuring the LDAP Directory Synchronization Feature

Create multiple new consumer policies, configure them appropriately, and then use them for your PGP WDE users. For example, if your organization’s security policies calls for stronger security for executives or certain departments, you could create multiple internal user policies to support this.

To configure consumer policies, refer to Establishing PGP WDE Client Settings (on page 29).

For more information about these settings, refer to the PGP Universal Administrator's Guide.

Configuring the LDAP Directory Synchronization Feature

If you have an up-to-date LDAP directory server in your organization, you will probably want to enable the LDAP Directory Synchronization feature on your PGP Universal Server so that you can use your LDAP server for auto-detecting policies and enrollment. This both leverages the information in your LDAP directory and simplifies the job of the administrator.

To enable the LDAP Directory Synchronization feature

1. Navigate to the Consumers > Directory Synchronization screen in the administrative interface. The Directory Synchronization card appears.
2. Select Enable if LDAP Directory Synchronization is disabled.
3. Click Add LDAP Directory.
4. In the Name field, enter a name for the LDAP directory you are adding.
5. From the Type drop-down menu, select the type of directory: choose Active Directory or OpenLDAP (RFC 1274). Active Directory is the default setting.

Microsoft Active Directory uses the sAMAccountName attribute for user information. OpenLDAP-based directories use the attribute uid for user information. PGP Universal Server queries user information using only the necessary attributes, providing faster results when querying user information.

6. In the Bind DN field, type the Distinguished Name of a valid user that exists in the LDAP directory. PGP Universal Server will use this as the user name to bind (log in) to the LDAP directory. This DN must match the name of an existing user in the directory. Binding determines the permission granted for the duration of a connection.

7. In the Passphrase field, type the passphrase to use for authentication to the DN. If you want to bind to the LDAP directory anonymously, leave these fields blank. If no DN is provided, PGP Universal Server will attempt to bind anonymously.

8. Go to the LDAP Servers tab and add at least one LDAP server.
9. Go to the Base Distinguished Names tab to specify any BaseDNs you want to use as the basis for searches within this directory.
10. Go to the Consumer Matching Rules tab if you want to set rules for which email addresses should be searched for in this LDAP directory.
11. Click Save.
Configuring Enrollment

As described previously, there are two methods available for enrollment:

- **Email (the default).** Requires only that the PGP WDE client and the PGP Universal management server be able to communicate via SMTP email. This method is available for all client installations, as long as there is a usable email account on the client system, even if the PGP Universal Server is not performing email encryption or is out of the mailflow.

- **LDAP Directory Synchronization.** Requires that the LDAP Directory Synchronization feature be enabled (and correctly configured) and that the “Enroll clients using directory synchronization” option be selected on the Directory Synchronization card. To enroll, the client will provide authentication credentials to the LDAP directory specified in the LDAP Directory Synchronization feature.

The following information is common to both methods of enrollment:

- Port 443 must be open between your PGP WDE clients and the PGP Universal Server. This is the port the PGP WDE clients use to get policy and receive encryption keys. Enrollment will fail if port 443 is blocked.

- On the Organization > Managed Domains screen, make sure that your managed domain matches up with the domain you use for email. **You must do this even if you are not using the messaging functionality of the PGP Universal Server.** For example, if you have an email address of jsmith@eng.example.com and the managed domain configured on your PGP Universal Server is example.com, enrollment will not work because the domain does not exactly match what is configured on the PGP Universal Server. It is possible to configure multiple email domains on the PGP Universal Server; configuring eng.example.com as an additional domain would solve the problem.

- Make sure you have DNS properly configured, including pointer records, or enrollment may fail.

**Email Enrollment**

To configure email enrollment:

- Navigate to the Mail > Mail Routes screen on your PGP Universal Server and add a route from the protected domain to the hostname of your mail server. For example, you could use the domain name eng.example.com and the hostname/IP mail.eng.example.com (or whatever your mail server address is).

  If you have already configured a mail route using an asterisk (*) as the domain name and the IP address of the mail server that will accept mail for delivery from the PGP Universal Server, you do not need to configure another mail route.

- Make sure port 25 is open between your PGP Universal Server and your mail server and make sure your mail server accepts SMTP (Domino servers might not by default, for example).
When your PGP WDE users install PGP WDE on their systems, an Enrollment Assistant will appear, asking them to open their email client, check for new messages, and open the enrollment email message the management server sends them. It is critical that your users open the message, as it puts a cookie onto their system. This cookie is required for the successful completion of the enrollment process.

**LDAP Directory Synchronization Enrollment**

*You may want to use tools such as ADSIedit (from the Windows Support tools section of your Server OS CD) or SoftTerra’s ldapbrowser from ldapbrowser.com to facilitate LDAP Directory Synchronization enrollment. This ensures that proper LDAP syntax is used.*

Your directory schema must contain certain attributes for you to use LDAP Directory Synchronization enrollment. Every user is required to have an email address in the attribute mail.

Other settings to check include:

- cn, mail
- smtpProxyAddress (or proxyAddress SMTP:)
- uid
- sAMAccountName
- Usercertificate
- binary

All these attributes (except Usercertificate and binary) need to be present in the directory. The attribute of your LDAP filter needs to be present as well.

When your PGP WDE users install PGP WDE on their systems, they will be prompted for their username and password on the LDAP directory. Ensure that they do this, as it is required for the successful completion of the enrollment process.
Establishing PGP WDE Client Settings

The PGP WDE client is installed on each system in your deployment. Consider the following topics when planning to configure PGP WDE clients:

- Specifying the appropriate key settings.
- Establishing PGP Desktop settings for your clients.
- Configuring other internal user policy settings.

Note: There are a few features of PGP WDE that are supported on Windows systems but not on Mac OS X or Linux systems. If you configure these features for your Windows clients and also create Mac OS X and/or Linux clients, the settings for these features will be ignored on the Mac OS X and Linux systems; all other settings will work normally.

In This Chapter

General Settings............................................................................................................ 29
Key Settings................................................................................................................... 30
PGP Desktop Settings................................................................................................... 33
Licensing Settings ........................................................................................................ 43

General Settings

These settings are found on the three tabs at the bottom of the Policy Options card (Consumers > Consumer Policy > [policy] > General > Edit).

The Directory Services tab of the Policy Options card is different depending on whether you are editing the Everyone Consumer Group or a policy you created.

- If you are editing a user-created policy, you can assign policies to internal users based on their directory attributes, if the LDAP Directory Synchronization feature is enabled. Refer to the PGP Universal Administrator's Guide for more information.

- Notify users of software updates and automatically download. Select if you want your PGP WDE client have updated software clients automatically downloaded.

- Use an HTTPS Proxy Server for PGP client communications. Select if your PGP WDE clients connect to the PGP Universal Server through a proxy server.

- Hostname. Enter the hostname of the HTTPS proxy server.
- Port. Enter the port used to access the HTTPS proxy server.
- Additional Decryption Key. Click the Import button and select a key to be used as an Additional Decryption Key for this consumer policy.
Establishing PGP WDE Client Settings

Key Settings

These settings apply to the PGP keys that your PGP WDE users can create. The settings are found on the tabs of the PGP Universal Server management console (Consumers > Consumer Policy > [policy] > Keys > Edit).

Key Generation Settings

The settings on the Generation tab:

- **Type**: Select the default key type for your PGP WDE users, either RSA or DH/DSS. The default is RSA.
- **Generate a separate signing subkey**: Check if you want your PGP WDE users to be able to generate separate signing subkeys.
- **Key Size**: Select the default key size for your PGP WDE users. Available options are 1024, 1536, 2048, 3072, and 4096.
- **Supported Ciphers**: Deselect any cipher you do not want your users to be able to use.
- **Preferred Cipher**: Select the cipher you want your end users to use if no algorithm is specified; you can select any supported cipher. The default is AES.
- **Supported Hashes**: Deselect any hash type you do not want your end users to be able to use.
- **Preferred Hash**: Select the hash you want your end users to use if no hash is specified; you can select any supported hash. The default is SHA-2-256.
- **Supported Compression**: Deselect any compression type you do not want your end users to be able to use. None means data will not be compressed before it is encrypted.
- **Preferred Compression**: Select the compression type you want your end users to use if no compression type is specified; you can select any supported compression type. The default is ZLIB.
- **Auto-Renew Keys Every**: Select an auto-renewal time frame for the keys of your PGP WDE users. Internal keys will automatically be renewed in the time frame you specify unless they have exceeded the inactivity threshold in Stop Renewing After. Select Never renew if you want your internal keys never to renew; this means the keys will never expire, regardless of inactivity.
- **Stop Renewing After**: Specify a period of inactivity after which a key will not be automatically renewed. Select Never stop renewing if you want keys of your PGP WDE users to be continually renewed. The question you should ask yourself here is how long a period of inactivity for a given user should be before you reasonably conclude that the user account is no longer in use.

- **Edit XML Preferences**: Clicking the Edit Preferences button lets you edit XML policy preferences. Do not use the XML Preferences Editor without help from PGP Support. Misconfiguring the preferences can cause your PGP WDE installations to stop working properly.
It is generally a good idea to set the auto-renewal time to be fairly short. This helps ensure that the PGP Universal Server manages itself without you needing to delete a user manually in the event someone leaves your organization.

Key Mode Settings

The options on the Management tab let you select which key modes your PGP WDE users will be able to select when they create keys. You must allow at least one key mode.

**Note:** The decisions you make now in deploying PGP WDE, including selecting a key mode, affect how you can deploy and use other PGP Corporation products in the future.

Available options are:

- **Server Key Mode (SKM).** Select this option if you want the PGP Universal Server to generate and manage the keys of your PGP WDE users.
- **Client Key Mode (CKM).** Select this option if you want your PGP WDE users to be able to generate and manage their own PGP keys.
- **Guarded Key Mode (GKM).** Select this option if you want your PGP WDE users to be able to generate and manage their own keys, and you also want encrypted copies of users’ private keys stored on the PGP Universal Server as a backup for the end user.
- **Server Client Key Mode (SCKM).** Select this option if you want private encryption keys shared between your PGP WDE users and the PGP Universal Server, and private signing keys stored only on the clients. SCKM supports PGP WDE, PGP NetShare, and PGP Messaging users.

For more information, see the *PGP Universal Administrator's Guide*.

Certificates Settings

The settings on the Certificates tab:

- **Use the username as the Common Name (CN):** Select to have the consumer’s username be the common name to which the certificate is issued.
- **Country (C):** Select to specify the country.
- **State/Province (ST):** Select to specify the name of the state or province, as appropriate. Do not abbreviate the state or province name. For example, type “California,” not “CA.”
- **Locality (L):** Select to specify the name of the city or locality, as appropriate.
- **Organization (O):** Select to specify the name of your organization or company.
- **Organizational Unit (OU):** Select to specify the name of your organization’s unit, as appropriate.
- **Create end entity certificate (omit Basic Constraints):** Select this option if you do not want to create CA certificates. Deselect this option to create CA certificates.
- **CRL Distribution point:** Select this option to put the CRL distribution point into the certificate. The CRL distribution point is specified from Services > Certificate Revocation.
**Establishing PGP WDE Client Settings**

### Key Settings

- **Derive key usage extension values from key**: This setting allows generated certificates to have the same usage flags as are on the matching PGP key.

- **Set non-repudiation key usage**: Non-repudiation is a usage flag specific to X.509 certificates. If you select this option, users with this usage will be able to sign S/MIME messages with non-repudiation. Non-repudiation, which provides assurance of the source and integrity of the message, is required in some environments.

Allowed Key Usages control what usage flags (certificate attributes) a generated certificate is permitted to request, not what usage flags the certificate will actually have.

- **Digital Signature (digitalSignature)**: Allows the certificate to have a signing usage flag.

- **Non-repudiation (nonRepudiation)**: This setting allows the certificate to contain a non-repudiation usage flag, but does not actually apply the usage flag. Both this setting and Set non-repudiation key usage must be selected for the certificate to be used for non-repudiation.

- **Key Encipherment (keyEncipherment)**: Allows the certificate to be used to encrypt other keys or certificates.

- **Data Encipherment (dataEncipherment)**: Allows the certificate to be used for encryption.

- **Key Agreement (keyAgreement)**: Allows the use of the certificate for key exchange protocols; for example, Diffie-Hellman key exchange.

- **Encipher only (encipherOnly)**: Allows the certificate to be used for encryption only.

- **Decipher only (decipherOnly)**: Allows the certificate to be used for decryption only.

- **TLS WWW Server Authentication**: Allows the certificate to be used for TLS/SSL server authentication.

- **TLS WWW Client Authentication**: Allows the certificate to be used for TLS/SSL client authentication.

- **Email Protection**: Allows the certificate to protect email messages using S/MIME.

- **Import X.509 certificates as**: Select PGP Bundle Keys, PGP Wrapper Keys, or User selectable.
  - PGP Bundle Keys bundles user X.509 signing and encryption certificates into a single identity. This is the recommended option.
  - PGP Wrapper Keys allows user X.509 signing and encryption certificates to be imported as separate identities. This option is not recommended because it only functions in an exclusively S/MIME environment.
  - User selectable allows your PGP WDE users to choose how to import their smartcard X.509 certificates.

- **Storage of keys on detected smart cards**: Select **Attempt** or **Require**.
  - **Attempt** means that PGP WDE will attempt to store new keys created by your PGP WDE users on supported smartcards that are detected, but will not require a supported smartcard in order to create a new key.
  - **Require** means that new keys your PGP WDE users create must be stored on a supported smartcard. They will not be able to create a key unless it can be stored on a smartcard.
Establishing PGP WDE Client Settings

Options Settings

The settings on the Options tab:

- **Use of CAPI-based credentials.** Select **Force**, **Prefer**, or **Ignore**.

**Allow users to receive encrypted email.** Enable if you want your PGP WDE users to receive encrypted email. Disable to prevent them from receiving encrypted email.

- **Enforce minimum passphrase length of X characters.** Enable if you want to require a minimum number of characters in passphrases for new keys created by your PGP WDE users. The default is eight characters.

- **Enforce minimum passphrase quality of X%.** Enable if you want to require a minimum passphrase quality level for new keys created by your PGP WDE users.

- **Saving passphrases.** Select one of the three options that will apply to your end users entering their passphrases:
  - **Save passphrases for the current session only.** Automatically saves passphrases in memory until your end user logs off their computer. If you enable this option, your end users will be prompted for their passphrase once per private key. They will not be prompted to enter it again for the same key until they log off their computer.
  
  **Caution:** If you select this option, it is very important to tell your end users to log off their computers before leaving it unattended. Passphrases can remain cached for weeks if they never log off, allowing anyone to read their encrypted messages or encrypt messages with their key while they are away from their computer.

  - **Save passphrases for X (hh:mm:ss).** Automatically saves passphrases in memory for the specified duration of time. If you enable this option, your end users will be prompted for their passphrases once for the initial signing or decrypting task; they will not be prompted to enter it again until the specified time has elapsed. The default setting is 0:3:0 (3 minutes).

  - **Do not save passphrases.** Prevents your end users’ passphrases from being stored in memory. If you enable this option, your end users must enter their passphrase each time it is needed.

**PGP Desktop Settings**

There are multiple ways for you to control what your users can do with PGP WDE clients when it is installed on their systems:

- **License settings:** The traditional method of controlling what your users can do with PGP WDE clients is for your organization to purchase licenses that support the features you want. So if you want your users to whole disk encrypt their drives, you purchase licenses that include support for PGP Whole Disk Encryption.
Establishing PGP WDE Client Settings

PGP Desktop Settings

- **Feature settings**: Once your organization purchases the appropriate licenses, you (the PGP administrator) establish settings for each feature that support your organization’s security policies. So if PGP WDE is supported by license, for example, you can control whether or not removable USB disks inserted on your users’ systems must be encrypted.

- **Feature control**: Another way to control what your users can do with PGP WDE clients is by controlling not just the settings for a feature but the feature itself. So if your organization has licenses for all employees that support PGP Shredder, for example, but you have a subset of employees that do not need this feature, you can create a client installer just for this subset of users that does not contain the PGP Shredder feature. Feature control is available for all major features of PGP WDE clients. Features that are disabled do not appear in the PGP WDE user interface.

- **Component control**: You can also control what your users can do with PGP WDE clients by editing the MSI client installer file to disable PGP Desktop components *(for Windows clients only)*. If your organization does not use Lotus Notes or Groupwise for messaging, for example, you could disable these components to limit any potential compatibility issues. This is accomplished by using Microsoft’s msixexec application to disable components after the client installer file is created. To reenable a component that has been disabled requires a reinstall of PGP Desktop with the component enabled. Components that are disabled do not appear in the PGP Desktop user interface. See *Controlling PGP Desktop Components* (see “*Controlling PGP WDE Components*” on page 49) for more information.

To establish PGP Desktop settings for your PGP WDE clients, go to **Consumers > Consumer Policy > [policy] > PGP Desktop > Desktop**. The settings are spread over five tabs.

### General Tab

The fields on the General tab control permissions and keys; they also include some general settings. For detailed descriptions of these settings, see the *PGP Universal Administrator’s Guide*.

The fields on the General tab are:

- **Allow users to change options**: When selected, lets your PGP WDE users change the settings that you, their administrator, have established. Deselect this option to prevent them from changing these settings.

- **Allow user-initiated key generation**: When selected, lets your PGP WDE users create new keys and subkeys—in addition to the key created during installation. Deselect to prevent them from creating new keys after installation and from making certain changes to their keypairs, such as adding and removing ADKs, appointing and removing third-party key revokers, or creating and using subkeys.

- **Allow user-initiated key signing**: When selected, lets your PGP WDE users sign keys. Deselect to prevent them from signing keys. You may need to do this to enforce centralized control over the validity of keys in your organization.

- **Allow conventional encryption and self-decrypting archives**: When selected, lets your PGP WDE users conventionally encrypt files using a passphrase instead of a key, or create self-decrypting archives (SDAs). Note that conventionally encrypted and self-decrypting files cannot be decrypted by your organization’s ADK, which may conflict with your data recovery policy. Deselect to prevent users from conventionally encrypting files or creating SDAs.
- **Always encrypt to user’s key.** When selected, every message your PGP WDE users send will be encrypted to their key. This is in addition to any other user- or system-specified key; for example, the ADK. Deselect if you do not want messages to be automatically encrypted to the user’s key. Users can still manually encrypt their messages to their key.

- **Automatically synchronize keys with servers.** When selected, PGP WDE will automatically keep your users’ keys synchronized with configured servers (when enabled, user key data synchronizes every 24 hours with the data on the PGP Universal Server). Deselect this option to prevent automatic synchronization of keys.

- **Automatically set up Key Reconstruction.** When selected, key reconstruction is set up automatically for your PGP WDE users when new keys are created. The key reconstruction data is stored on the PGP Universal Server. Keys created on smartcards and tokens are not compatible with key reconstruction. For information on key reconstruction, see the *PGP Desktop User’s Guide* and the *Inside PGP Key Reconstruction White Paper* on the PGP Corporation website.

- **Override default keyring locations.** When selected, lets you enter locations for keyrings that override the default locations for Windows and/or Mac OS X systems. This means that your users’ keyrings will be created in and backed up to the location(s) you specify instead of the default keyring locations. The default keyring location for Windows is `C:\Documents and Settings\[user]\My Documents\PGP`. The default keyring location for Mac OS X is `[/user]/Documents/PGP/`.

- **Enable RDD with Intel Anti-Theft Technology.** When selected, Intel Anti-Theft Technology is activated on your users’ systems. This feature is available only on supported hardware and operating systems; it also requires a separate license. Refer to the *PGP Universal Administrator’s Guide* for more information.

- **Enable Silent Enrollment.** When selected, only essential Setup Assistant screens will appear during enrollment; non-essential screens will be suppressed and default settings will be used. This option reduces the number of screens your users must navigate during enrollment.

  This option requires both the use of the LDAP Directory Synchronization feature and that the **Allow/Deny/Require encryption of disks to existing Windows Single Sign-On** password option (on the **WDE Tab** (see "Disk Encryption Tab" on page 38)) be set to **Require**.

- **Activate FIPS 140-2 operational and integrity checks.** When selected, FIPS operational tests will be active on your PGP WDE users’ systems the next time PGP WDE is started. This may slow performance on those systems.

- **Show PGP Desktop in system tray/menu.** When selected, the PGP WDE padlock icon appears in the system tray of your PGP WDE users when PGP WDE is active on their systems. The icon provides access to some PGP WDE features without requiring users to launch the whole application. Deselect to hide the icon.

- **Hide the option to disable PGP Services.** When selected, the Stop PGP Services option will not appear on the PGP tray menu for your PGP WDE users. This prevents your users from using this menu option to disable PGP WDE services on their system.

- **Send client logs to PGP Universal every X minutes.** When selected, specifies how often PGP WDE client logs are sent to the associated PGP Universal management console. The default is 5 minutes.
Establishing PGP WDE Client Settings

PGP Desktop Settings

- **Download policy updates from PGP Universal every X hours.** When selected, specifies how often the PGP WDE client will download policy updates from the associated PGP Universal management console. The default is 24 hours.

**Messaging & Keys Tab**

The fields on the Messaging & Keys tab control email messaging, instant messaging, and key management. For detailed descriptions of these settings, see the *PGP Universal Administrator’s Guide*.

The fields on the Messaging & Keys tab are:

- **Email Messaging.** Deselect to disable the Email Messaging feature; it will not appear in the user interface.

- **Search for keys on PGP Desktop keyrings when encrypting or verifying email.** When selected, lets your PGP WDE users import keys into their keyring so that they can encrypt or verify messages without needing to refer to the PGP Universal Server for key information. This allows your PGP WDE users to operate as if they were not bound to the PGP Universal Server, even if they are. Deselect to prevent them from searching for keys on their own keyring when encrypting or verifying email.

- **Enable encrypt and sign buttons in Outlook MAPI for Windows.** When selected, buttons for encrypting and signing appear in Microsoft Outlook for your users.

- **Enable Out Of Mail Stream support (OOMS).** When selected, lets your PGP WDE users send emails per policy in support of Web Messenger or Smart Trailers when the PGP Universal server is out of the mailstream. When deselected, your PGP WDE users will not be able to send these messages if the PGP Universal Server is out of the mailstream.

- **Allow outbound PGP/MIME from MAPI accounts.** When selected, MAPI uses PGP/MIME to encrypt and encrypt and sign messages. If this option is not selected, MAPI uses PGP Partitioned. MAPI can send messages PGP/MIME signed whether this setting is enabled or disabled.

- **Add a comment to secured email.** When selected, appends the text in the box to clear-signed PGP blocks, including exported key files, and encrypted files and text. Deselect and leave the box empty if you do not want a comment to be appended to these messages.

- **Sign email stored in IMAP sent message folders.** When selected, lets your users choose to either **Sign**, **Encrypt**, or **Encrypt and Sign** messages stored in IMAP sent message folders on their systems.

- **Match IMAP folder name patterns.** PGP Universal Server provides a default list of IMAP sent folder names for supported mail clients. You can add to this list to specify additional IMAP folder name patterns to be secured. You can use a wildcard *.* Not case sensitive.

- **Allow users to follow local client policy.** When selected, lets your PGP WDE users take actions that follow local client policy, overriding the mail policy of the PGP Universal Server. This setting allows users to create messaging policies that could make their messaging less secure. Deselect to prevent users from overriding mail policy.

- **Mail policy.** Lets you control what happens to email when the PGP Universal Server cannot be reached by PGP WDE.
Establishing PGP WDE Client Settings

PGP Desktop Settings

- Standalone.
- Offline: Standalone.
- Offline: Block.
- Offline: Send Clear.

- **If client fails to download policy for X days.** Lets you establish how your PGP WDE clients will handle situations where policy cannot be downloaded from the PGP Universal management console for the specified period.
  - **Block outbound message.** Outbound messages are blocked when policy cannot be downloaded for the specified period.
  - **Apply last downloaded policy.** The last policy downloaded is used when policy cannot be downloaded for the specified period.

- **Use current PGP issued X.509 certificates instead of existing X.509 certificate.** Select if you are using a Lotus Notes mail server but you want your PGP WDE users to use a PGP x.509 certificate as the user’s active certificate in Lotus Notes, but only if the user is already using a non-PGP X.509 certificate. The Lotus Notes certificate is suppressed.

- **Add PGP issued X.509 certificate to Lotus Notes if no X.509 certificate exists.** Select if you want the PGP certificates to be inserted into the Lotus Notes certificate directory, whether the user has another certificate or not. Only available if Use PGP certificates instead of Lotus Notes certificate is selected.

- **Prefer Notes native encoding over PGP encoding.** Select if you are using Lotus Notes mail servers with Windows Notes clients and prefer to use native Notes encoding.

- **Instant Messaging.** Deselect to disable the Instant Messaging feature; it will not appear in the user interface.

- **Encrypt/Decrypt AOL Instant Messenger conversations.** When selected, the instant messages (IMs) between your PGP WDE users and other PGP WDE or PGP Desktop users are protected. Note that IMs will be protected only if both users are running PGP WDE or PGP Desktop software with this setting enabled. Deselect if you do not want these IM sessions to be protected.

- **Key Management.** Deselect to disable the Key Management feature; it will not appear in the user interface, preventing your users from managing their keys.

---

**File Encryption Tab**

The fields on the File encryption tab control settings for PGP Zip and PGP Shredder. For detailed descriptions of these settings, see the *PGP Universal Administrator's Guide*.

The fields on the File Encryption tab are:

- **PGP Zip.** Deselect to disable the PGP Zip feature; it will not appear in the user interface and it will not be available to your users.

- **PGP Shredder.** Deselect to disable the PGP Shredder feature; it will not appear in the user interface and it will not be available to your users.

- **Number of shredder passes.** Enter the number of shredder passes your PGP WDE users will use when they shred. The default is 3. The larger the number, the more secure the shred, but the longer the shred process takes.
Establishing PGP WDE Client Settings

PGP Desktop Settings

- **Warn user before shredding files.** When selected, your PGP WDE users will be warned before files on their system are shredded. Deselect to suppress this warning.

- **Automatically shred when emptying the Recycle Bin/Trash.** When selected, your PGP WDE users will have files they delete from their system shredded instead of just deleted. Deselect to prevent deleted files from being shredded.

NetShare Tab

The fields on the NetShare tab control settings for PGP NetShare. For detailed descriptions of these settings, see the *PGP Universal Administrator’s Guide*.

The fields on the NetShare tab are:

- **PGP NetShare for Windows.** Deselect to disable the PGP NetShare feature; it will not appear in the user interface. Does not apply to PGP WDE users.

- **Allow the user to create PGP NetShare folders.** Does not apply to PGP WDE users.

- **Allow the user to enable Advanced User Mode.** Does not apply to PGP WDE users.

- **Force the encryption of files in the following folders.** Does not apply to PGP WDE users.

- **Prevent the encryption of files in the following folders.** Does not apply to PGP WDE users.

- **Force the encryption of files associated with the following applications.** Does not apply to PGP WDE users.

- **Prevent the automatic decryption of files by the following applications.** Does not apply to PGP WDE users.

Disk Encryption Tab

The fields on the WDE tab control settings for PGP Virtual Disk and PGP Whole Disk Encryption.

**Note:** There are a few features of PGP WDE that are supported on Windows systems but not on Mac OS X or Linux systems. If you configure these features for your Windows clients and also create Mac OS X and/or Linux clients, the settings for these features will be ignored on the Mac OS X and Linux systems; all other settings will work normally.

The fields on the Disk Encryption tab are:

- **PGP Virtual Disk.** Deselect to disable the PGP Virtual Disk feature; it will not appear in the user interface and it will not be available to your users.

- **Automatically create PGP Virtual Disk on Windows clients upon installation.** When selected, a PGP Virtual Disk volume will be created automatically for your PGP WDE users using the Capacity and Format you specify.
Establishing PGP WDE Client Settings
PGP Desktop Settings

- **Unmount when inactive for X minutes.** When selected, the PGP Virtual Disk volumes of your PGP WDE users will be automatically unmounted after the specified number of minutes of inactivity on their systems. This could prevent the protected data on a PGP Virtual Disk volume from being available to unauthorized persons if you leave work without unmounting the volume, for example. Deselect to prevent PGP Virtual Disk volumes from being automatically unmounted because of inactivity.

- **Unmount on system sleep.** When selected, the PGP Virtual Disk volumes of your PGP WDE users will automatically unmount if the system goes to sleep. Some systems do not support sleep mode, so this option would not apply. Deselect to prevent unmount on sleep.

- **Prevent sleep if disk(s) cannot be unmounted.** When selected, the systems of your PGP WDE users will not sleep if, for some reason, a PGP Virtual Disk volume cannot be unmounted. Using this option could prevent loss of data. Deselect to permit sleep even if a volume cannot be unmounted.

- **PGP Portable.** Deselect to prevent your PGP WDE users from creating PGP Portable disks. Enable to allow this.

- **PGP Whole Disk Encryption.** Deselect to disable the PGP Whole Disk feature; it will not appear in the user interface. If you want your users to be able to use the PGP Whole Disk Encryption feature, do not deselect this field.

- **User-Initiated Whole Disk Encryption Permissions.** Specify which encryption tasks your PGP WDE users can do with internal and removable disks:
  - **Allow User Management.** Your PGP WDE users can add or remove other passphrase users from the user’s device.
  - **Allow Encryption.** Your PGP WDE users can initiate encryption of internal and/or removable disks. Automatic disk encryption during setup is not affected by this policy.
  - **Allow Decryption.** Your PGP WDE users can initiate decryption of internal and/or removable disks. If you do not enable this option, users will not be able to decrypt disks. Decryption after license expiration is not affected by this policy.

- **Store decryption policy on fixed disks.** When selected, the policy that specifies whether users can initiate decryption of the disk is stored on the encrypted disk. When the policy is stored on the disk, current and future versions of PGP WDE, as well as Windows PE tools and other recovery methods, will all be prevented from decrypting the disk. This information is not stored on removable disks.

- **Allow/Deny/Force encryption of disks to existing Windows Single Sign-On password.** When selected, you can decide to Allow, Deny, or Force the use of the Single Sign-On (SSO) feature of PGP WDE, which lets your users log into PGP WDE and Windows at the same time. Deselect to prevent your users from using the single sign-on feature of PGP WDE. Allow lets your users decide whether or not to use SSO, Deny prevents them from using it, Force requires them to use it. The SSO feature is only available for Windows clients.

**Note:** Using the Single Sign-On feature is both a popular feature and it can be leveraged to enforce PGP WDE passphrase quality alignment with your corporate passphrase quality requirements.

- **Automatically encrypt <volume type> at installation.** When selected, forces whole disk encryption of the boot disk, only the boot partition, or only the Windows partition when PGP WDE is installed. Deselect to disable this feature.
Establishing PGP WDE Client Settings

**PGP Desktop Settings**

- **Require <authentication method>**. When selected, you must specify a *required* method for securing the whole disk encrypted drive. This option is active only if *Automatically encrypt boot disk upon installation* is selected.

  The three security methods available are:

  - **standard passphrase authentication**: Requires that standard passphrase authentication be used to secure the drive. This is the default setting.
  - **supported smart cards for hardware security**: Requires that a supported smart card be used to secure the drive. The drive cannot be whole disk encrypted until a supported smart card is provided; for example, an Aladdin eToken. The smart card must be configured before attempting to use it to secure a drive and the system must *already* have the appropriate drivers installed. Keys created on smart cards and tokens are *not* compatible with PGP WDE’s key reconstruction feature.
  - **Trusted Platform Module (TPM)**: Requires that a system with a hardware TPM be used to secure the drive. The drive will not be whole disk encrypted unless a hardware TPM is present.

- **Force maximum CPU Usage**. When selected, makes the process of whole disk encrypting a drive faster by using more CPU cycles. Deselect to prevent extra CPU cycles from going to the whole disk encryption process. Some systems may experience lag during usage when Maximum CPU Usage is enabled. You can only select this option if *Automatically encrypt boot disk upon installation* is selected.

- **Force power failure safety**. When selected, in the event of a power failure during whole disk encryption of a drive, the system can recover the data and restart encryption. Deselect to disable this feature. Initial encryption may take longer when Power failure safety is enabled. You can only select this option if *Automatically encrypt boot disk upon installation* is selected.

- **Lock passphrase user accounts on Windows clients after 3 failed login attempts**. Specify how many failed login attempts can occur before the encrypted disk is locked.

  If the disk is locked, all passphrase users lose access. All accounts on the disk are locked. Users will not be able to log in again without using a WDRT or other token. An administrator with a PGP WDE administrator key can also unlock the account. If one user logs in with a WDRT or other token, the disk unlocks and all passphrase users can log in again. Without a WDRT or other token, the disk is permanently locked.

- **Enable automatic encryption or locking of removable devices**. If you select this option, the Automatic Encryption dialog box appears when the user inserts an unencrypted removable disk. The Automatic Encryption dialog box warns the user that the disk will be either mounted read-only, or encrypted after the amount of time you specify. This prevents protected data from being copied onto an unprotected drive.

  This feature is only available for Windows clients. Refer to the *PGP Desktop for Windows User's Guide* for more information.

  - **Lock device as read-only and provide users with the option to encrypt**. If you select this option, the unencrypted disk is mounted read-only. Users can read the data on the disk, but cannot save anything to the disk. Users can choose to encrypt the disk instead.

  - **Automatically encrypt: 30 seconds, 1 minute, 2 minutes, 5 minutes, Immediately**. Dialog box displays a countdown until the device is encrypted. Removable drives on the system are encrypted after the dialog times out.
By default, PGP Desktop encrypts the drive to the existing credentials if the primary computer disk is encrypted. If the primary computer is not encrypted, PGP Desktop will try to encrypt the portable drive to another private key, if one is available. If there is no other private key, the user will be prompted to create a passphrase user account to use to encrypt the disk.

If a Whole Disk Recovery Token is required for encryption, then if the user attaches a previously unencrypted removable drive to the client computer while the PGP Universal Server cannot be reached, the removable disk cannot be encrypted and will be automatically unmounted. The removable disk cannot be used and the user will see the following error message: “The administrative server is not available for storing the administrative recovery token. Disk encryption cannot continue.”

- **Enable Whole Disk Recovery Tokens.** When selected, PGP administrators can remotely regain access to a drive that has been whole disk encrypted if the usual authentication method is unavailable (for example, if a user forgets their passphrase). Deselect to disable this option.

- **Allow configuration of WDE Local Self Recovery for Windows clients.** When selected, provides a way for users to access encrypted drives from the PGP BootGuard screen if they have forgotten their passphrases. Users can log in by answering security questions they have previously configured. When configured, users will not have to contact an administrator for assistance.

- **Display a list of users who are eligible for local self recovery at boot time.** When selected, PGP Whole Disk Encryption displays a list of all users on that computer who have configured Local Self Recovery.

- **Encrypt using AES-256/AES-128.** AES-256 is stronger, but requires PGP Desktop 10 or greater clients.

- **Encrypt Windows WDE and PGP Virtual Disks to a Disk Administrator key.** When selected, lets you add a public key which, if your users whole disk encrypt a drive, will be used to create a token-based user on the drive. Deselect to disable this option. This gives you a way to access the data on a whole disk encrypted drive or decrypt the drive if the user is unable or unwilling.

To import the public key, click **Import** and do one of the following:

- Select **Import Public Key File**, use the **Browse** button to navigate to the file of the public key you are importing (use PGP Desktop to create this file if it does not already exist), select the file, click **Open**, then click **Import**.

- Select **Import Public Key Block**, then paste the key block of the public key you are importing, then click **Import**.

To access the whole disk encrypted drive via the token-based user, the private key must be on a supported token/smart card. Use PGP Desktop to either create a keypair on or copy a keypair to a supported token/smart card. Refer to the PGP Desktop User’s Guide for more information about PGP keys and tokens/smart cards.

- **Encrypt Windows WDE disks to a Disk Administrator Passphrase.** When selected, lets you add a passphrase that permits a WDE administrator to log in at the PGP BootGuard screen; for example, to create an account on an encrypted disk for a new user. Does not require a hardware token. This feature does not support Single Sign-On. Click **Create** to create a passphrase.

- **Display simple authentication field.** Select if you want only a single authentication field to appear on the PGP BootGuard screen of your PGP WDE users.
• **Display detailed authentication fields.** Select if you want detailed authentication fields to appear on the PGP BootGuard screen of your PGP WDE users. Refer to the PGP Universal Server online help for detailed information.

• **Add additional text to the WDE BootGuard login screen.** When selected, lets you put in text that your users will see when the PGP WDE BootGuard screen appears on their system. You can use one line of text, up to 80 characters (including spaces). Deselect to disable this option.

• **Customize screen backgrounds.** When selected, lets you add custom background images that your users will see when the PGP WDE BootGuard screen appears on their system or choose a plain gray background. You can add an image for both the splash and the login screen. Deselect to disable this option.
  - To add a background image, select **Upload background image files**, then click **Browse** next to either **Splash Screen** or **Login Screen** and select an image for one or both.
  - To display a plain gray background, select **Display plain gray background**.

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

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

  For more information about creating custom background images for the PGP WDE BootGuard screen, refer to the PGP Universal online help.

• **Enable audio cues.** When selected, enables the use of audio clues for certain actions that occur during the PGP WDE Bootguard authentication process. These audio clues can help vision-impaired users more easily navigate the PGP WDE BootGuard process. Deselect to disable this option.

  If a user changes this setting, they must reboot their system to have the change take effect.

  When enabled, the user's system will play audible tone combinations during the PGP WDE BootGuard authentication process. Each tone combination starts with a middle sound and is followed by either a higher tone, another middle tone, or a lower tone. The three combinations are:
  - Ready for passphrase/pin entry: When the system is first ready for passphrase/pin entry, the middle-middle tone combination plays, indicating the user can enter their passphrase or pin.
  - Successful authentication: If the authentication attempt was successful, the middle-high tone combination plays, indicating success. The system then continues booting.
Establishing PGP WDE Client Settings

Licensing Settings

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

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

---

**Licensing Settings**

You enter your PGP WDE license information on the client Licensing screen (Consumers > Consumer Policy > PGP Desktop > Client Licensing). This information will be integrated in the PGP WDE client installers. You can enter information for multiple versions of PGP WDE.

On the Licensing tab, click the **Enter License** button for the appropriate version(s) of PGP WDE.

When the **Enter License Information** dialog appears, fill in the following fields:

- **Licensee Name.** Enter the name of the person under which the licenses were purchased.
- **Licensee Organization.** Enter the name of the organization that purchased the licenses.
- **Licensee Email.** Enter the email address of the person to contact regarding the license.
- **License Number.** Enter the license number to be used.

Click **Save** when you have finished entering information.
Creating the PGP WDE Client Installer

Once you have configured the settings for your PGP WDE client installers, there are three ways to actually create the PGP WDE client installer:

- with auto-detect policy.
- with preset policy.
- with no policy settings.

In This Chapter

Creating an Installer with Auto-Detect Policy.............................................................................45
Creating an Installer with Preset Policy ..................................................................................46
Creating an Installer with No Policy Settings............................................................................47

Creating an Installer with Auto-Detect Policy

This option for creating your PGP WDE client installers uses your organization's LDAP directory and requires that the LDAP Directory Synchronization feature already be enabled and appropriately configured on the PGP Universal Server.

To create a PGP Desktop installer with auto-detect policy

1 Create the custom user policies you want to be linked to your PGP WDE users. If you do not create any custom user policies, then your PGP WDE users will automatically be linked to the default policy. You can, however, create custom user policies in the future that may be linked to your PGP WDE users, depending on the settings in the custom policies.

2 Configure and save the settings on the PGP Desktop screen appropriately for these custom user policies. Refer to your PGP Universal Administrator's Guide for specific instructions.

3 Navigate to Consumers > Groups, then click Download Client. The Download PGP Clients card appears.

4 In the Client field, select PGP Desktop.

5 In the Platform field, select Mac OS X, Linux 32-bit, Linux 64-bit, Windows 32-bit, or Windows 64-bit, as appropriate.

6 In the Language field, select English, French, German, Japanese, or Spanish, as appropriate.

7 Make sure the Customize checkbox is selected. If it is not selected, select it.

8 Select Auto-detect Policy Group.
9 In the **PGP Universal Server** field, enter the PGP Universal Server you want the application to interact with. The PGP Universal Server you are using to create the installer is listed by default.

10 In the **Mail Server Binding** field, enter the name of the mail server you want bound to the PGP Universal Server. You must enter this information unless your users read mail directly from this PGP Universal Server. Customized client installations will not work without mail server binding. You can use the * wildcard character to bind automatically to any mail server. Mail policy will be enforced for any mail server to which the client connects. You can use the wildcard as follows: *, *.example.com, and example.*.com. If you are creating a binding for an internal MAPI email client, you must use the WINS name of the Exchange Server. If you are creating a binding for an internal Lotus Notes email client, you must use the fully qualified domain name of the Domino server.

11 Click **Download**. The PGP WDE client installer is created and downloaded to your system.

---

**Creating an Installer with Preset Policy**

This option for creating your PGP WDE client installers does not use an LDAP directory nor the LDAP Directory Synchronization feature.

**To create a PGP WDE client installer with preset policy**

1 Create the custom user policy you want to be linked to your PGP WDE users. If you do not create a custom user policy, then the Internal Users: Default policy will be the only policy with which you can link your PGP WDE users.

2 Configure the settings on the PGP Desktop screen appropriately for the custom user policy.

3 Navigate to **Consumers > Groups**, then click **Download PGP Clients**. The **Download PGP Clients** card appears.

4 In the **Client** field, select **PGP Desktop**.

5 In the **Platform** field, select **Mac OS X**, **Linux 32-bit**, **Linux 64-bit**, **Windows 32-bit**, or **Windows 64-bit**, as appropriate.

6 In the **Language** field, select **English**, **French**, **German**, **Japanese**, or **Spanish**, as appropriate.

7 Make sure the **Customize** checkbox is selected. If it is not selected, select it.

8 Select **Preset Policy Group**.

You can also select to embed policy and license information into the installer to force the clients to be disconnected from the PGP Universal Server. In this case, there is no connection between PGP WDE on your users' systems and the PGP Universal Server. The client will **not** receive any updated policy information from the PGP Universal management server, even if the policy is updated on the server side. Policy information normally downloaded during installation is instead embedded in the installer itself.

---

**Caution:** Use this option carefully, as most product features will **not** work in this mode.
In the **PGP Universal Server** field, enter the PGP Universal Server you want the application to interact with. The PGP Universal Server you are using to create the installer is listed by default.

In the **Mail Server Binding** field, enter the name of the mail server you want bound to the PGP Universal Server. You must enter this information unless your users read mail directly from this PGP Universal Server. Customized client installations will not work without mail server binding. You can use the * wildcard character to bind automatically to any mail server. Mail policy will be enforced for any mail server to which the client connects. You can use the wildcard as follows: *, *.example.com, and example.*.com. If you are creating a binding for an internal MAPI email client, you must use the WINS name of the Exchange Server. If you are creating a binding for an internal Lotus Notes email client, you must use the fully qualified domain name of the Domino server.

Click **Download**. The PGP WDE client installer is created and downloaded to your system.

---

**Creating an Installer with No Policy Settings**

You have the option of creating your PGP WDE client installer with no policy settings, which means that your PGP WDE users can do anything their license allows; they will not receive any policies from the PGP Universal management server. Note that this option is virtually the same as standalone usage, and defeats the purpose of using a PGP Universal Server to manage your PGP WDE users.

**To create a PGP Desktop installer with no associated policy**

1. Navigate to **Consumers > Groups**, then click **Download PGP Clients**. The **Download PGP Clients** card appears.
2. In the **Client** field, select **PGP Desktop**.
3. In the **Platform** field, select **Mac OS X**, **Linux 32-bit**, **Linux 64-bit**, **Windows 32-bit**, or **Windows 64-bit**, as appropriate.
4. In the **Language** field, select **English**, **French**, **German**, **Japanese**, or **Spanish**, as appropriate.
5. Make sure the **Customize** checkbox is deselected. If it is selected, deselect it.
6. Click **Download**. The PGP Desktop installer is created and downloaded to your system.
Controlling PGP WDE Components

One of the ways you can control what your users can do with PGP WDE is by disabling specific PGP WDE components. This is accomplished by using software to distribute your client installers that has the ability to specify switches to the msiexec.exe command line utility.

**Note:** This feature is available for Windows clients only.

Disabling a PGP WDE component means it will not appear in the PGP WDE user interface, and it ensures that there will not be any compatibility issues with the operating system or third-party products.

Upgrades, including automatic upgrades, honor the disabling of PGP WDE components and will not reenable disabled components unless the MSI file has been specifically edited to reenable the disabled component.

The following PGP WDE components can be disabled:

- **MAPI**: Means MAPI messaging will be disabled.
- **Notes**: Means Notes messaging will be disabled.
- **LSP**: Means the IM encryption feature and POP, SMTP, and IMAP message will be disabled.
- **SSO**: Means the PGP WDE Single Sign-On feature will be disabled.
- **WDE**: Means the PGP Whole Disk Encryption feature will be disabled.
- **NetShare**: Means the PGP NetShare feature will be disabled.
- **Groupwise**: Means Groupwise messaging will be disabled.
- **Memory lock**: Means the memory locking feature (which keeps sensitive data from leaving volatile memory) will be disabled. Disabling memory lock is available so that you can disable all kernel-level items, if desired. It should generally not be disabled unless you have a specific reason to do so.
- **Virtual Disk**: Means the PGP Virtual Disk feature will be disabled.

The syntax to disable PGP Desktop components is:

```
> msiexec /I pgpdesktop.msi PGP_INSTALL_[component]=0
```

Where `[component]` is the PGP Desktop component you want to disable:

- MAPI
- NOTES
- LSP
- SSO
- WDE
- NETSHARE
- GROUPWISE
- MEMLOCK
- VDISK
You can disable multiple PGP Desktop components using a single command. For example:

```bash
> msiexec /I pgpdesktop.msi PGP_INSTALL_MAPI=0
   PGP_INSTALL_NOTES=0 PGP_INSTALL_LSP=0
```

To reenable a PGP Desktop component that was disabled requires a reinstallation with the disabled component specifically reenabled. For example:

```bash
> msiexec /I pgpdesktop.msi PGP_INSTALL_MAPI=1
```
Once you have created a PGP WDE client installer with the desired settings for your PGP WDE users, PGP Corporation *strongly recommends* that you *not* immediately deploy it. Instead, test your client installer on as many representative machines as you can; you will save yourself a lot of time by finding and solving problems with the installer before your full deployment.

Naturally, if any of these tests have unexpected results, you will need to fix the problems and, if necessary, create an updated client installer.

Ways of testing your PGP WDE client installer include:

- Install it on a network that is separate from your production environment.
- Install it on a system configured with your standard corporate image.
- Install it on a system with your standard corporate image plus other software common in your organization, allowed or not.
- Run a pilot deployment to a small number of users or a single department.
Deploying the PGP WDE Client Installer

How you deploy the PGP WDE client installer to your users depends on your unique circumstances. Note that the PGP Universal Server, which manages your PGP WDE clients, cannot be used to deploy the client installer.

Some common methods include:
- Using an enterprise software distribution system such as SMS or Tivoli.
- Downloaded from a Web/file server.
- Distributed on CD, DVD, or thumb drive.

If you want to control PGP WDE components during deployment (see Controlling PGP WDE Components (on page 49)), make sure the deployment software you plan to use has the ability to specify switches to the msiexec.exe command line utility.
12

Assisting Your PGP WDE Users

There are a number of things that PGP Corporation recommends you do to help support your PGP WDE users:

- Provide your PGP WDE users with a document, created by your organization, that talks about PGP WDE: this document could include what PGP WDE is, what they are expected to use it for, what it does to their system, and what to do if they have problems with PGP WDE. For more information about what information you could include in such a document, refer to The End-User Experience.

- Tell them about steps they should take to make sure their drives are in good condition before they whole disk encrypt them, especially checking the drive for errors. PGP Corporation recommends a third-party scandisk utility such as SpinRite or Norton Disk Doctor, for example. Tell them that defragmenting the drive is also a good idea; recommend the built-in Windows utility or a third-party utility, such as PerfectDisk.

- Even if you do not provide your PGP WDE users with a document that talks about PGP WDE, you should definitely give them a written statement about what PGP WDE should be used for and what it must be used for. Include a summary of your official corporate security policies and how they can use PGP WDE to conform to those policies.

- Give them a copy of the PGP Whole Disk Encryption Quick Start Guide and the PGP Desktop User’s Guide. Strongly encourage them to read the Quick Start Guide before installing PGP WDE on their systems.

- Tell them about the other resources that are available to them: the built-in online help, the PGP Support Portal (https://support.pgp.com), and the PGP Support forum (http://forum.pgp.com).

- Tell them about steps they should take to make sure their drives are in good condition before they whole disk encrypt them, especially checking the drive for errors. PGP Corporation recommends a third-party scandisk utility such as SpinRite or Norton Disk Doctor, for example. Tell them that defragmenting the drive is also a good idea; recommend the built-in Windows utility or a third-party utility, such as PerfectDisk.

- Give them a phone number to call or an email address to write to in case they experience problems.

- Set up a system so that each user can report a successful installation.
Your PGP WDE users will notice changes to how they use their computer both during the installation of PGP WDE and afterwards. You can help ensure a successful end-user experience with PGP WDE by preparing your end users for these changes.

If you decide to provide your PGP WDE users with a document created by your organization, you may want to include some or all of the following points. Depending on configuration, some of these points may not apply to your PGP WDE users.

In This Chapter

During the Installation Process .................................................................57
During WDE Setup ......................................................................................58
During Normal Usage ................................................................................58

---

### During the Installation Process

The following items may impact your PGP WDE users during installation:

- The installation process begins by double-clicking the PGP WDE client installer. A reboot of the system is required when the installation process is complete.

- During the installation process, PGP WDE will coordinate with the PGP Universal Server and link to the most appropriate user policy. This linkage is based on how closely the settings for the particular user in the LDAP directory match the settings of the available user policies (if LDAP Directory Synchronization is being used). If you later add a more appropriate policy, the affected PGP WDE users will automatically become linked to the new, more appropriate policy. Note that the MSIE proxy setting of the user must be correct if they are enrolling from outside your corporate network.

- Unless Server Key Mode is the only allowed key mode, the installation process will prompt your PGP WDE users to create a PGP keypair. If you are allowing them to select between two or more keys modes, you should provide them with guidance regarding what is the best choice based on how they will be using the product.

- If you are not using encrypted email, have your PGP WDE users leave the email field blank when they are creating their PGP keypair and have them skip adding their public key to the PGP Global Directory. This will ensure that they do not get encrypted email they cannot decrypt.

- Part of the installation process includes a "cookie" being placed onto the systems of your PGP WDE users. This is required for communications between the system and the PGP Universal Server.
During WDE Setup

The following items may impact your PGP WDE users during setup:

- You can configure whole disk encryption of the boot drive on the systems of your PGP WDE users to begin automatically or you can let them start the process manually sometime after installation.
- Whole disk encryption of a drive is a background process; your PGP WDE users can continue to use their systems while the drive is being encrypted.
- The process of whole disk encrypting a drive can be paused, either manually or if the system is shut down or restarted, goes into standby mode, or on laptops if the system goes to battery power (you can only begin whole disk encrypting a drive on a laptop if the system is on AC power).
- On rare occasions, the whole disk encryption of a drive stops and displays the “Unable to instrument disk” error message. This usually occurs when there is not enough contiguous space available on the drive being encrypted, there are disk errors on the drive, or if Windows is reserving some of the space being used to encrypt the drive. The solution is to have the user check the drive for errors and defragment it, then try again to whole disk encrypt it.

During Normal Usage

The following items may impact your PGP WDE users during usage:

- On startup, the Bootguard screen will appear, requiring appropriate authentication before allowing access to data on the system.
- The PGP Tray icon will appear in the Windows System Tray (on Windows systems), providing easy access to many PGP WDE features.
- The Notifier screen will appear above the Windows System Tray when PGP WDE performs certain actions, providing information about the action being taken.
- PGP WDE functionality may change from time to time if the policies change that apply to a user. PGP WDE checks with the PGP Universal Server it is enrolled with for policy changes at startup, every 24 hours after startup, when email messages are sent (if email proxying is enabled).