PGP Desktop for Windows

Quick Start Guide
Version 10.2

What is PGP Desktop?

PGP Desktop provides comprehensive security for desktops and laptops, making it possible for enterprises, workgroups, and individuals to protect sensitive information without changing the existing IT infrastructure or disrupting work processes. This award winning, easy-to-use solution encrypts email, files, virtual volumes, and entire disks from a single desktop application.

The PGP Desktop family of applications have been combined into several bundles.

- **PGP Desktop Professional** includes PGP Desktop Email and PGP Whole Disk Encryption
- **PGP Desktop Storage** includes PGP Whole Disk Encryption and PGP NetShare
- **PGP Desktop Corporate** includes PGP Desktop Email, PGP Whole Disk Encryption, and PGP NetShare

PGP Desktop Email

Use PGP Desktop Email to automatically and transparently encrypt, sign, decrypt, and verify email message through policies you defined for you by administrators, or policies you control if you are not part of a PGP Universal Server-managed environment.

PGP NetShare

Use PGP NetShare to let authorized users share protected files in a shared space--such as a file server, shared folder, or USB removable drive.

PGP Whole Disk Encryption

Use PGP Whole Disk Encryption (PGP WDE) to lock down the entire contents of your system or an external or USB flash drive you specify.

In addition, use PGP Desktop to:

- Use part of your hard drive space as an encrypted virtual disk volume with its own drive letter.
- Create protected Zip archives.
- Completely destroy files and folders so that nothing can recover them.

Contents

New to PGP Desktop?

Use this step-by-step guide to get started. You will find that, with PGP Desktop, protecting your data will be as easy as turning a key in a lock.

- This *Quick Start Guide* helps you install PGP Desktop and get started.
- The *PGP Desktop User's Guide* provides more detailed information on PGP Desktop. In it, you will learn what a keypair is, why you might want to create one, how to create one, and how to exchange keys with others so you can encrypt your own data and share data securely with others.

  Note: A PGP Desktop license provides you with access to a certain set of PGP Desktop features. Certain other features of PGP Desktop may require a different license. For more information, see the Licensing section of the *PGP Desktop User's Guide*.

- For deployment, management, and policy enforcement information for PGP Desktop, see the *PGP Universal Server Administrator's Guide*.

Understanding the Basics

PGP Desktop uses keys to encrypt, sign, decrypt, and verify your messages.

After installation, PGP Desktop prompts you to create a PGP keypair. A keypair is the combination of a private key and a public key.

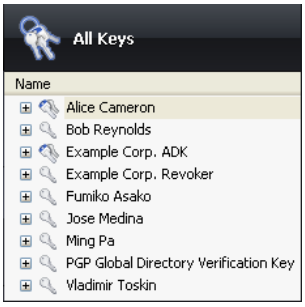
- Keep your *private key* and its passphrase private, as the name suggests. If someone gets your private key and its

passphrase, they can read your messages and impersonate you to others. Your private key decrypts incoming encrypted messages and signs outgoing messages.

- Your *public key* you can give to everyone. It does not have a passphrase. Your public key encrypts messages that only your private key can decrypt and verifies your signed messages.

Your keyring holds both your keypairs and the public keys of others, which you use to send encrypted messages to them. Click the PGP Keys Control Box to see the keys on your keyring:

1. The icon for a PGP keypair has two keys, denoting the private and the public key. Alice Cameron has a PGP keypair in this illustration, for example.
2. The icons for the public keys of others have just one key. Ming Pa's public key, for example, has been added to the keyring shown in this illustration.



What Am I Installing?

PGP Desktop uses licensing to provide access to the features you purchase. Depending on the license you have, some or all of the PGP Desktop family of applications will be active.

This document contains instructions for viewing the features activated by your license.

PGP Desktop Email is a member of the PGP Desktop family of applications. You can use PGP Desktop Email to automatically and transparently encrypt, sign, decrypt, and verify email messages through policies you control. You can also use PGP Desktop Email to encrypt IM sessions for clients such as AIM and iChat. Both users must have PGP Desktop Email enabled.

PGP Viewer is a member of the PGP Desktop family of applications. You can use PGP Viewer to decrypt, verify and display email messages outside of the mail stream. You can also use PGP Viewer to decrypt and view legacy IMAP/SMTP/POP email content.

PGP NetShare is a member of the PGP Desktop family of applications. You can use PGP NetShare to authorize users to share protected files in a shared space, such as on a corporate file server, in a shared folder, or on a removable media such as a USB drive. The encrypted files in the Protected Folder continue to appear as normal application files to the authorized users; anyone else with physical access to the files can see them but not use them.

PGP Whole Disk Encryption (PGP WDE) is a member of the PGP Desktop family of applications. You can use PGP WDE to lock down the entire contents of your system or an external or USB flash drive you specify. Boot sectors, system files, and swap files are all encrypted. Whole disk encrypting your boot drive means you do not have to worry if your computer is lost or stolen: to access your data, an attacker would need the appropriate passphrase.

PGP Virtual Disk volumes uses part of your hard drive space as an encrypted virtual disk volume with its own drive letter. A PGP Virtual Disk is the perfect place for storing your sensitive files; it is as if you have stored them in a safe. When the door of the safe is open (when the volume is mounted), you can change files stored in it, take files out of it, and move files into it. Otherwise (when the volume is unmounted), all the data on the volume is protected.

PGP Zip adds any combination of files and folders to an encrypted, compressed, portable archive. PGP Desktop must be installed on a system to create or open a PGP Zip archive. PGP Zip is a tool for securely archiving your sensitive data, whether you want to distribute it to others or back it up.

PGP Shredder completely destroys files and folders so that even file recovery software cannot recover them. Deleting a file using the Windows Recycle Bin (on Windows systems) or Trash (on Mac OS X systems) does not actually delete it; it sits on your drive and eventually gets overwritten. Until then, it is trivial for an attacker to recover that file. PGP Shredder, in contrast, immediately overwrites files multiple times. This is so effective that even sophisticated disk recovery software cannot recover these files. This feature also completely wipes free space on your drives so your deleted data is truly unrecoverable.

Key Management manages PGP keys, both your keypairs and the public keys of others. You use your private key to decrypt messages sent to you encrypted to your public key and to secure your PGP Virtual Disk volumes. You use public keys to encrypt messages to others or to add users to PGP Virtual Disk volumes.

System Requirements

PGP Desktop can be installed on systems running the following versions of Microsoft Windows operating systems:

- Windows XP Professional 32-bit (Service Pack 2 or 3), Windows XP Professional 64-bit (Service Pack 2), Windows XP Home Edition (Service Pack 2 or 3), Microsoft Windows XP Tablet PC Edition 2005 SP2, Windows Vista (all 32- and 64-bit editions, including Service Pack 2), Windows 7 (all 32- and 64-bit editions, including Service Pack 1), Windows Server 2003 (Service Pack 1 and 2).

The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

Note: PGP Whole Disk Encryption (PGP WDE) is not compatible with other third-party software that could

bypass the PGP WDE protection on the Master Boot Record (MBR) and write to or modify the MBR. This includes such off-line defragmentation tools that bypass the PGP WDE file system protection in the OS or system restore tools that replace the MBR.

PGP Whole Disk Encryption on Windows Servers

PGP Whole Disk Encryption (WDE) is supported on all client versions above as well as the following Windows Server versions:

- Windows Server 2003 SP 2 (32- and 64-bit editions); Windows Server 2008 64-bit SP 1 and 2; Windows Server 2008 R2 64-bit
- VMWare ESXi4 (supported Microsoft Windows Servers operating in a virtual environment)

For additional system requirements and best practices information, go to the the *Symantec Knowledgebase* (*http://www.symantec.com/business/support/index?page=home*) and search for TECH149613, "PGP Whole Disk Encryption on Windows Servers".

PGP Whole Disk Encryption on Tablet PCs

PGP Whole Disk Encryption is supported on Tablet PCs that meet the following additional requirements:

- Dell Latitude XT1 and XT2 Tablet PC Touch Screen Laptops (undocked)
- 1024 x 768 x 16 screen display running SVGA mode
- Optional physical keyboard

Hardware Requirements

- 512 MB of RAM
- 64 MB hard disk space

Installing PGP Desktop

Symantec Corporation recommends exiting all open applications before you begin the install. The installation process requires a system restart.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Desktop installer may be configured with specific features and/or settings.

To install PGP Desktop

1. Locate the PGP Desktop installation program you downloaded.

   The installer program may have been distributed by your PGP administrator using the Microsoft SMS deployment tool.
2. Double-click the installer.
3. Follow the on-screen instructions.
4. Reboot your system when instructed.
5. When your system restarts, follow the on-screen instructions to configure PGP Desktop.

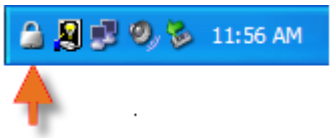
Licensing

To see what features your license supports, open PGP Desktop and select **Help > License**. Those features with a checkmark are supported by the active license.

Starting PGP Desktop

To start PGP Desktop, use any of the following methods:

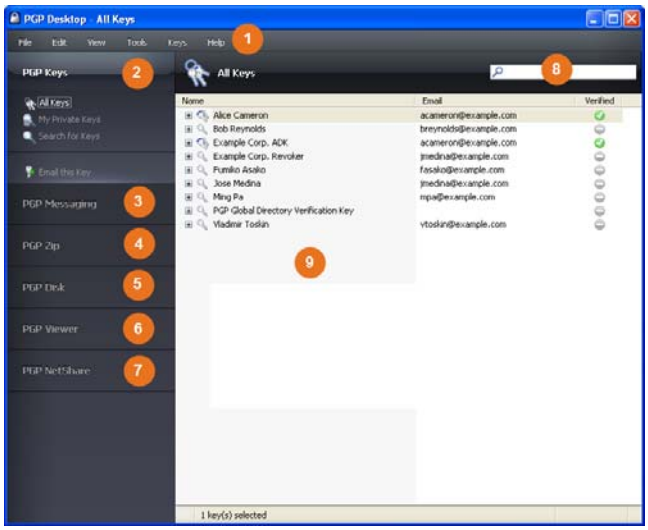
- Double-click the PGP Tray icon.



- Right-click the PGP Tray icon and then select **Open PGP Desktop**.
- From the **Start** menu, select **Programs > PGP > PGP Desktop**.

The PGP Desktop Main Screen

The PGP Desktop application window is your main interface to the product.



The PGP Desktop main screen includes:

1	**The Menu bar**. Gives you access to PGP Desktop commands. The menus on the Menu bar change depending on which Control box is selected.
2	**The PGP Keys Control Box**. Gives you control of PGP keys.
3	**The PGP Messaging Control Box**. Gives you control over PGP Messaging.

4	**The PGP Zip Control Box**. Gives you control of PGP Zip, as well as the PGP Zip Assistant, which helps you create new PGP Zip archives.
5	**The PGP Disk Control Box**. Gives you control of PGP Disk.
6	**The PGP Viewer Control Box**. Gives you the ability to decrypt, verify, and display messages *outside* the mail stream.
7	**The PGP NetShare Control Box**. Gives you control of PGP NetShare.
8	**The PGP Desktop Work area**. Displays information and actions you can take for the selected Control box.
9	**PGP Keys Find box.** Use to search for keys on your keyring. As you type text in this box, PGP Desktop displays search results based on either name or email address.

Each Control box expands to show available options, and collapses to save space (only the Control Box banner displays). Expand a Control Box by clicking its banner.

Using PGP Desktop Email

PGP Desktop Email automatically and transparently encrypts and signs outgoing messages and decrypts and verifies incoming messages. All you need to do is to send and receive your email just as you always have; PGP Desktop Email will take care of the rest.

Sending Encrypted Email

After installation, PGP Desktop Email inserts itself between your email client and your mail server and watches your email traffic.

When *incoming* messages arrive, PGP Desktop Email intercepts them before they get to your inbox and automatically attempts to decrypt and verify them; it uses your private keys to decrypt and the public keys of others to verify. When it is done with your messages, PGP Desktop Email delivers them to your inbox.

In most cases, you do not have to do anything special; decrypted incoming messages will appear in your inbox just like any other incoming messages.

When you send *outgoing* messages, PGP Desktop Email intercepts them on the way to your mail server and automatically attempts to encrypt and sign them, based on configured policies.

Again, you do not have to do anything special; just create your messages using your email client and send them—PGP Desktop Email handles everything else.

Details of how PGP Desktop Email transparently handles your incoming and outgoing messaging is found in the following sections.

Incoming Messages

PGP Desktop Email handles incoming messages based on their content:

- **Not encrypted or signed**. If a message is not encrypted or signed, PGP Desktop Email just passes it along to your email client. You can read the message as is, so there is nothing for PGP Desktop Email to do to it.
- **Encrypted but not signed**. If a message is encrypted, PGP Desktop Email attempts to decrypt it so that you can read it. It will look first on your keyring for the private key that can decrypt the message. If it finds the private key, PGP Desktop Email uses it to decrypt the message and then passes the message to your email client. If it cannot find the private key, PGP Desktop Email passes it to your email client still encrypted. It will look something like this.

```
-----BEGIN PGP MESSAGE-----
Version: PGP Desktop 10.0

qANQR1DBwUwDMvpGQkaZ1HwBD/0f5F8QKtY+1NVzwQw4xQ/EPu0DOmLrMZVVNQVn
rYvHPoSAcn6C3zFpO996akjRioOBGa62hkLpkjQi3QEGpBtqMP1F64TUxqHkpLNH
ISN+7zEA7EYTtV+3ErREOH6yQgJ+sQGm6sjRjddYYvTG6hGa9f2wX+ZDLAIK6SrA
f4ZNQfNvkowMmJXS78Sz7LEGE5d5wM68kKB/FflvfYz1w360QgauIXmom9F8294p
fNaWAnhQlRif/la/MuYs0WkTLPQpdBXhgZqVKaE85gsCrwqXfMAGDEYfrsCAb1Ne
nMWJNtXsRYVpstmpNBZuVHOljKrXE4YEAPk48MOD1Yi54NJxYwvury79oDoxDlJh
o9yh9v5f071orpLFceW8WmLX4qJaGds0VqdwQRRnfwbWnbgsdljD2cmijyOq+bcy
3hZknIEGbb7GTKaKo1cj+y9u5aFDh49lA9qLyHTWwLuHYV/j/wtBPfPZpjGYvACV
FqRDEO8hYzxKc/foQwlIMdo+nymZEQItTTdBCaESxm5v+jBWfn0xhUK/EVylkAHm
n27x2m9PdwzxriQjgrxI8Lda7DTJWYmA8ol20ClQZqrqvAmqIKL4CpCkyhPuRwIg
nan80KN/USfzK+Vi9juxM1ls5oGYz0DtL6KnLnGGpTlu6yLsU2SB7iIbVe330ukj
zMLXgdLAKQFSItPMVeKqJPxQrMrLlEYr6hE7fcAYmUMwXe8w60e7H2OwEIme2Y9V
eVocs5p9Iau7w987Ifbh1odEb+QEwJMavv5jBcaE1ZhxAYLfrIdXBb1REeuQGjmj
FuCHf6BGgTp9HlNjw92iR5qSintROh2KmwTa5oGbDNnEEAAQJp8sI+6129FLpLgF
z7/wzmnKFngV4OgILxyPCRvS6Pbo30wAgJehhqDzC9kEkmXd6J7t/caDEMUsnHC1
qTBAScHRB+8eN5yrUrZ5YUqhNvpR/vVN6odPEnX4mbrMsClv4uXRYSv5ofGHJT0U
=8hVs
-----END PGP MESSAGE-----
```

- **Signed but not encrypted**. If a message is signed, PGP Desktop Email attempts to verify the signature. It will look at the following locations in this order for the appropriate public key: your default keying, the keyserver at keys.domain, where domain is the domain of the sender of the message, the PGP Global Directory (keyserver.pgp.com), any then other configured keyservers. If PGP Desktop Email finds the appropriate public key, it will attempt to verify the signature and then pass the message to your email client. If it cannot find the appropriate public key, it will pass the message to your email client unverified.
- **Encrypted and signed**. If a message is encrypted and signed, PGP Desktop Email will first try to find the private key to decrypt the message, then try to find the public key to verify it.

Outgoing Messages

PGP Desktop Email handles your outgoing email messages based on policies, sets of instructions that can be set up to handle any situation.

Default Policies

PGP Desktop Email includes four default policies:

- **Mailing List Admin Requests**. Administrative requests to mailing lists are sent in the clear; that is, not encrypted or signed.
- **Mail List Submissions**. Submissions to mailing lists are sent signed (so they can be authenticated) but not encrypted.

- **Require Encryption: [PGP] Confidential**. Any message flagged as confidential in your email client or containing the text "[PGP]" in the subject line must be encrypted to a valid recipient public key or it will not be sent. This policy gives you a way to easily handle messages that *must* be sent encrypted or not sent at all.
- **Opportunistic Encryption**. Specifies that any message for which a key to encrypt cannot be found should be sent without encryption (in the clear). Having this policy as the last policy in the list ensures that your messages will be sent (unless you flag the message as Confidential), albeit in the clear, even if a key to encrypt it to the recipient cannot be found.

Creating New Policies

PGP Desktop Email includes the ability to create and use new policies in addition to the four default policies. You can create policies based on a wide variety of criteria. If you are using PGP Desktop Email in a PGP Universal Server-managed environment, your messaging policies and other settings may be controlled by your organization's PGP administrator.

For complete information about how to create and implement messaging policies, see the *PGP Desktop User's Guide*.

Was My Message Encrypted?

Because PGP Desktop Email does its work automatically and transparently, from time to time you may find yourself wondering, was my message really sent encrypted? The answer is probably yes, but there are ways to make certain.

Notifier Alerts

PGP Desktop Notifier alerts are a feature of PGP Desktop that both tell you what is going on with your messaging and give you control over it.

For example, when you send an encrypted message, the Notifier alert appears in the lower right corner of your screen. It shows:

- Subject.
- Who it is being sent to.
- Keys found for the recipient.
- Status of the message.

To view more information about the message being sent, click **More**. Now you also see:

- What PGP Desktop Email did to the message.
- Who signed the message.

For more information about Notifiers, see the *PGP Desktop User's Guide*.

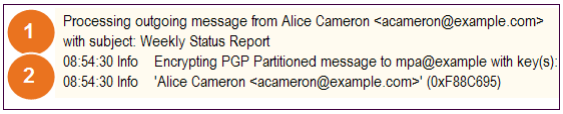
Note: In a PGP Universal Server-managed environment, your administrator may have specified certain notifications settings (for example, whether notifications are to be displayed or the location of the notifier). In this case, you may not see any notifier messages at all.

PGP Log

The PGP Log lists a variety of actions that PGP Desktop is taking to secure your messaging.

For example, the message whose Notifiers are shown above generated this entry in the PGP Log. It shows:

1. That an outgoing message was sent, who sent it, and what the subject was.
2. The time it was encrypted, the email address it was encrypted to, and the email address it was sent from.



Using PGP Viewer

In normal usage, PGP Desktop sits between your email client (Mozilla Thunderbird, for example) and your email server so that PGP Desktop can encrypt and sign outgoing messages and decrypt and verify incoming messages. When PGP Desktop is doing this, it is called "in the mail stream."

Use PGP Viewer to decrypt, verify, and display messages *outside* the mail stream.

Opening an Encrypted Message or File

Use PGP Viewer to open (decrypt, verify, and display) encrypted message files of the following types:

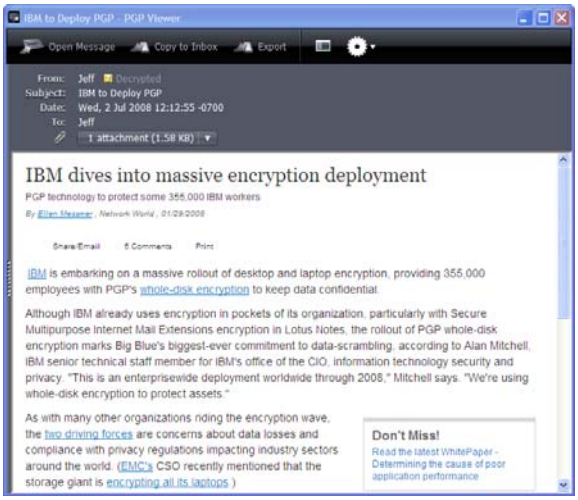
- ***.pgp:** Created by a PGP application.
- ***.eml**: Created by Outlook Express or Thunderbird.
- ***.emlx**: Created by Apple's Mail.app program on Mac OS X systems.
- ***.msg**: Created by Microsoft Outlook.

When PGP Viewer opens an encrypted message, it does not overwrite the encrypted text. The original message remains intact.

To decrypt, verify, and display an encrypted message from a file

1. Open PGP Viewer. To do this, select the PGP icon in the system tray and then select PGP Viewer or from within PGP Desktop select the PGP Viewer control box.
2. Click **Open File in PGP Viewer** or pull down the **Viewer** menu and select **Open File in PGP Viewer**. The **Open Message File** dialog appears.

3 In the Open Message File dialog box, navigate to the file you want to open, select it, then click **Open**. PGP Viewer decrypts, verifies, and displays the message in a separate window.



Tip: You can drag and drop the file you want to open onto the portion of the PGP Viewer windows that displays: **Drag Email or Files Here**. PGP Viewer opens the file, decrypts and verifies it, and displays the message.

4 To open another message, click **Open Message** in the toolbar, navigate to the desired file, select it, then click **Open**. PGP Viewer decrypts, verifies, and displays the message. A pane on the left side of the PGP Viewer screen is displayed so that you can see all open messages.

5 To open a pane on the left side of the PGP Viewer window or to close the pane if it is open, click the Pane button on the toolbar.

Copying Email Messages to Your Inbox

Use PGP Viewer to copy plaintext versions of decrypted messages to the inbox of your email client.

To copy a message to the inbox of your email client

1 With the message in the PGP Viewer window, click **Copy to Inbox**. The Copy to Inbox confirmation dialog box displays the name of the email client to which the message will be copied. To change this setting, see the PGP Viewer Preferences.

2 Click **OK** to continue. If you are copying a message to the Mozilla Thunderbird email client for the first time, a dialog box displays, advising that you must install an add-on.

Click **Yes** to install the add-on and follow the on-screen instructions or click **No**. You must be using Thunderbird 2.0 or greater to install the add-on.

3 PGP Viewer opens your email client and copies a plaintext version of the message to the inbox.

Exporting Email Messages

Use PGP Viewer to export a decrypted message to a file.

To export a message from PGP Viewer to a file

1 With the message displayed in the PGP Viewer window, click **Export**. The Export Message File dialog is displayed.

2 In the Export Message File dialog box, specify the desired location, filename, and format for the file, then click **Save**. PGP Viewer saves the file to the specified location.

Specifying Additional Options

Use the Tools button on the PGP Viewer Toolbar (on the far right) to specify several PGP Viewer features:

- **Text Encoding**: Specify the text encoding format for the message currently being displayed by PGP Viewer.
- **Show Remote Images**: Display external resources (images, CSS style sheets, iframe content, and so on) for the message currently being displayed by PGP Viewer. You can specify that PGP Viewer automatically displays external resources in Preferences.
- **View Message Source**: Display the source of the message currently being displayed by PGP Viewer. Viewing the message source can tell you more information about the message.
- **Preferences**: Display the PGP Viewer Preferences dialog box.

Using PGP NetShare

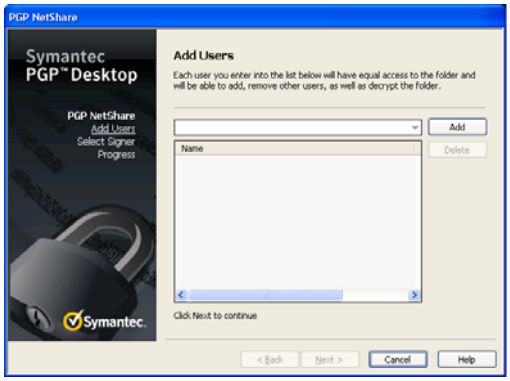
The PGP NetShare feature allows authorized users to share protected files. You must first create a Protected Folder and specify those users you want to be authorized to use the files.

1 Click **Add Folder** in the PGP NetShare Control Box. The Select Folder screen appears.

2 Click **Browse**, then select the folder you want to protect.

3 In the **Description** field, type a description for the Protected Folder you ware creating or leave blank to use the default name.

4 Click **Next**. The Add Users screen appears.



5 To specify users of the files in the Protected Folder, click the down arrow icon, select a user, then click **Add**. Remember to add yourself if you want to access the files in the Protected Folder.

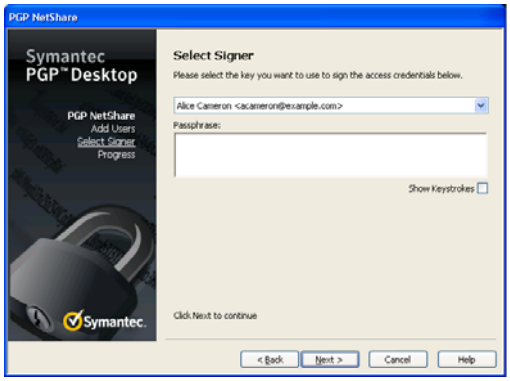
PGP NetShare does not notify users that they can access the protected files; it is the responsibility of the creator of a new Protected Folder to notify users.

6 To assign roles to each user, right-click the user's name and select the role:

- **Admin**: Create only one Admin per PGP NetShare protected folder. This role has full read/write rights to the folder, can add and remove users, assign roles to other users, and can promote another user to be the Admin.
- **Group Admin**: Create as many Group Admins as you need for each PGP NetShare protected folder. This role has full read/write rights to the folder, can add and remove users, and assign roles to other users.
- **User**: Create as many Users as you need for each PGP NetShare protected folder. This role has full read/write rights to the folder.

You can change a user's role at any time after the protected folder is created. Click on the protected folder in the PGP Desktop, and right-click the user's name to change the role.

7 Click **Next**. The Select Signer screen appears.



8 Select one private key from the private keys on the local keyring and enter the appropriate passphrase (if the passphrase is not cached). This key will be used to secure the PGP NetShare configuration information for the Protected Folder and the files in it.

9 Click **Next**. The Progress screen appears. The files in the specified Protected Folder are encrypted and the specified users are authorized to use the files. If any files, such as system files, were skipped, they are listed here.

10 Click **Finish**.

Integrating with Symantec Data Loss Prevention

Symantec Data Loss Prevention discovers, monitors, and protects confidential data. When integrated with PGP NetShare, Symantec Data Loss Prevention performs these actions on endpoint local disks and on internal networks, using PGP NetShare to protect (encrypt) sensitive files, without user intervention.

Symantec Data Loss Prevention uses two methods to identify sensitive files, as specified by the Data Loss Administrator:

- **Data in Motion (DIM)**. This method monitors data that is in transit, including data that is copied, moved from or to the local disk, or saved.
- **Data at Rest (DAR)**. This method discovers stationary data.

When Symantec Data Loss Prevention identifies a sensitive file, it encrypts the file:

- Whether or not the file is in a Protected Folder.
- Using the keys specified by the Data Loss Administrator.

When Symantec Data Loss Prevention encrypts a file:

- The keys may or may not be the same keys as those defined by the Admin or Group Admin of the protected file.
- The file may be decrypted then re-encrypted if the file is already encrypted by PGP NetShare. Decryption requires that the file owner be logged on.
- Provides the same user interface as files encrypted by PGP NetShare:
  - Displays the same lock icon.
  - Allows you to view the encryption keys associated with a file in the Properties dialog box under the PGP NetShare tab. DIM files show 'DLP Auto Encrypt' as the Signing Key; DAR files show the KEY ID. For more information, see Accessing the Properties of a Protected File or Folder.
  - Allows you to add or remove users from the access list if you are the Admin or Group Admin.

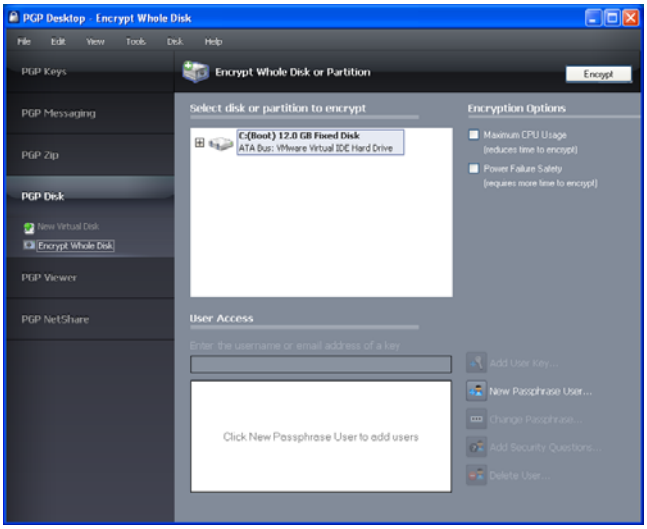
Using PGP WDE to Encrypt a Drive

The PGP WDE feature locks down the entire contents of your system or an external or USB flash drive you specify.

The encryption algorithm used by PGP WDE is AES256. The hashing algorithm is SHA-1. FAT16, FAT32, and NTFS formatted drives are supported. There is no minimum or maximum size. If the drive is supported by the operating system (or your hardware BIOS for the boot drive), it should work with PGP WDE.

Caution: Symantec Corporation recommends, as a best practice, that you back up your data before encrypting your disk.

1 Click **Encrypt Whole Disk** in the PGP Disk Control box.



2 Select the drive or partition to be encrypted.

3 Select **Maximum CPU Usage** to protect your disk as quickly as possible. The encryption process will take priority over other operations on your system.

4 Select **Power Failure Safety** if you think your system could lose power during the encryption process.

When **Power Failure Safety** is selected, the encryption process can safely resume if it is interrupted. This option can cause encryption to take longer to complete.

5 Click **Add User Key** to add users who will be able to authenticate to the whole disk encrypted drive using public-key cryptography.

If you are encrypting a fixed drive, you can only use a PGP keypair on an Aladdin eToken USB token. If you are encrypting a partition or a removable (non-fixed) drive, you can use any keypair on your system.

6 Click **New Passphrase User** to add users who authenticate using a passphrase, including if you want to use a USB flash device for two-factor authentication. Follow the instructions displayed in the PGP Disk Assistant dialog boxes.

If you are encrypting your boot drive, you have the option of using your Windows logon passphrase so that you only have to enter your credentials once on startup.

7 Click **Encrypt**.

Notes: To encrypt data on floppy disks or CD-RWs, use PGP Virtual Disk volumes; do not use PGP WDE.

You can use the PGP Whole Disk Encryption feature on a dual-boot system, as long as you boot to an operating system supported by PGP WDE (such as Windows XP, Windows 2000, or Windows Vista) and PGP Whole Disk Encryption is installed. Partition mode supports dual-booting with another operating system (such as Linux) as long as you encrypt only your Windows partition. The other operating system must be on another, non-encrypted partition.

Backup software works normally with PGP WDE; any files the software backs up will be decrypted *before* being backed up.

PGP WDE Best Practices

Symantec Corporation recommends the following best practices for preparing to encrypt your disk with PGP WDE. Please follow the recommendations below to protect your data during and after encryption.

Before you encrypt your disk, there are a few tasks you must perform to ensure successful initial encryption of the disk.

1 **Determine whether your target disk is supported**. PGP WDE feature protects desktop or laptop disks (either partitions, or the entire disk), external disks, and USB flash disks. CD-RW/DVD-RWs are *not* supported. See "Supported Disk Types" in the *PGP Desktop User's Guide* for more details on what types of disks are supported.

2 **Back up the disk before you encrypt it**. Before you encrypt your disk, be sure to back it up so that you won't lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk.

3 **Ensure the health of the disk before you encrypt it**. If PGP WDE encounters disk errors during encryption, it will pause encryption so you can repair the disk errors. However, it is more efficient to repair errors before you initiate encryption. For more information, see *Ensure Disk Health Before Encryption* (page 9).

4 **Create a recovery disk**. While the chances are extremely low that a master boot record could become corrupt on a boot disk or partition protected by PGP Whole Disk Encryption, it is possible. Before you encrypt a boot disk or partition using PGP Whole Disk Encryption, create a recovery disk. See *Create a Recovery CD (page 9)* for instructions on how to create a recovery disk.

5 **Be certain that you will have AC power** for the duration of the encryption process. See *Maintain Power Throughout Encryption* (page 9).

6 **Run a pilot test to ensure software compatibility**. As a good security practice, Symantec Corporation recommends testing PGP WDE on a small group of computers to ensure that PGP WDE is not in conflict with any software on the computer before rolling it out to a large number of computers. This is particularly useful in environments that use a standardized Corporate Operating Environment (COE) image. For a list of software known to have compatibility issues with PGP WDE, see *Run a Pilot Test to Ensure Software Compatibility* (page 9).

7 **Perform Disk Recovery on Decrypted Disks**. Where possible, as a best practice, if you need to perform any disk recovery activities on a disk protected with PGP Whole Disk Encryption (WDE), Symantec Corporation recommends that you first decrypt the disk. Do this by **Disk > Decrypt** in PGP Desktop, using your prepared PGP WDE Recovery Disk, or by connecting the hard disk via a USB cable to a second system and decrypting from that system's PGP Desktop software. Once the disk is decrypted, proceed with your recovery activities.

8 **Installing on a Windows Server system**. If you are installing PGP WDE on a Windows Server system, go to the the *Symantec Knowledgebase* (*http://www.symantec.com/business/support/index?page=home*) and search for TECH149613 for additional best practices information.

Ensure Disk Health Before Encryption

Symantec Corporation deliberately takes a conservative stance when encrypting drives, to prevent loss of data. It is not uncommon to encounter Cyclic Redundancy Check (CRC) errors while encrypting a hard disk. If PGP WDE encounters a hard drive or partition with bad sectors, PGP WDE will, by default, pause the encryption process. This pause allows you to remedy the problem before continuing with the encryption process, thus avoiding potential disk corruption and lost data.

To avoid disruption during encryption, Symantec Corporation recommends that you start with a healthy disk by correcting any disk errors prior to encrypting.

- Before you attempt to use PGP WDE, use a third-party scan disk utility that has the ability to perform a low-level integrity check and repair any inconsistencies with the drive that could lead to CRC errors. Microsoft Windows' check disk (chkdsk.exe) utility is not sufficient for detecting these issues on the target hard drive. Instead, use software such as SpinRite or Norton Disk Doctor™. These software applications can correct errors that would otherwise disrupt encryption.
- As a best practice, highly fragmented disks should be defragmented before you attempt to encrypt them.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, the bad sectors encountered during encryption are logged to the PGP Universal Server and the encryption process continues.

Create a Recovery CD

The following instructions use Roxio software for illustration purposes. The actual steps you perform may differ.

1 Make sure PGP Desktop and Roxio Easy Media Creator or Roxio Easy CD Creator (or other software that can create a CD from an ISO image) are installed on your system.

2 Open Roxio Easy Media Creator or Roxio Easy CD Creator and choose to create a Data CD Project.

3 Select **File > Record CD from CD Image**.

4 From the **Files of Type** menu, select **ISO Image Files (ISO)**.

5 Navigate to the PGP directory. The default location is `C:\Program Files\PGP Corporation\PGP Desktop\`.

6 Select `bootg.iso` and click **Open**.

7 Insert a blank, recordable CD into a CD drive on your system.

8 On the Record CD Setup screen, click **Start Recording**.

9 When the file is burned to the CD, click **OK**.

10 Remove the recovery CD from the drive and label it appropriately.

Caution: PGP WDE recovery disks are compatible only with the version of PGP Desktop that created the recovery CD. For example, if you attempt to use a 9.0.x recovery disk to decrypt a disk protected with PGP WDE 9.7 software, it will render the PGP WDE 9.7 disk inoperable.

Maintain Power Throughout Encryption

Because encryption is a CPU-intensive process, encryption cannot begin on a laptop computer that is running on battery power. The computer *must* be on AC power. If a laptop computer goes on battery power during the initial encryption process (or a later decryption or re-encryption process) PGP WDE pauses its activity. When you restore AC power, the encryption, decryption, or re-encryption process resumes automatically.

Regardless of the type of computer you are working with, your system must not lose power, or otherwise shut down unexpectedly, during the encryption process, unless you have selected the Power Failure Safety option.

Do not remove the power cord from the system before the encryption process is over. If loss of power during encryption is a possibility—or if you do not have an uninterruptible power supply for your computer—consider choosing the Power Failure Safety option, as described in the *PGP Desktop User's Guide*.

Caution: This holds true for removable disks, such as USB devices. Unless you have selected the **Power Failure Safety** option, you run the risk of corrupting the device if you remove it during encryption.

Run a Pilot Test to Ensure Software Compatibility

Certain other disk protection software is incompatible with PGP WDE and can cause serious disk problems, up to and including loss of data. Please note the following known

interoperability issues, and please review the PGP Desktop Release Notes for the latest updates to this list.

Software that is not compatible:

- Symantec Endpoint Encryption Full Disk
- Faronics Deep Freeze (any edition)
- Utimaco Safeguard Easy 3.x
- Absolute Software's CompuTrace laptop security and tracking product. PGP Whole Disk Encryption is compatible only with the BIOS configuration of CompuTrace. Using CompuTrace in MBR mode is not compatible.
- Hard disk encryption products from GuardianEdge Technologies: Encryption Anywhere Hard Disk and Encryption Plus Hard Disk products, formerly known as PC Guardian products.

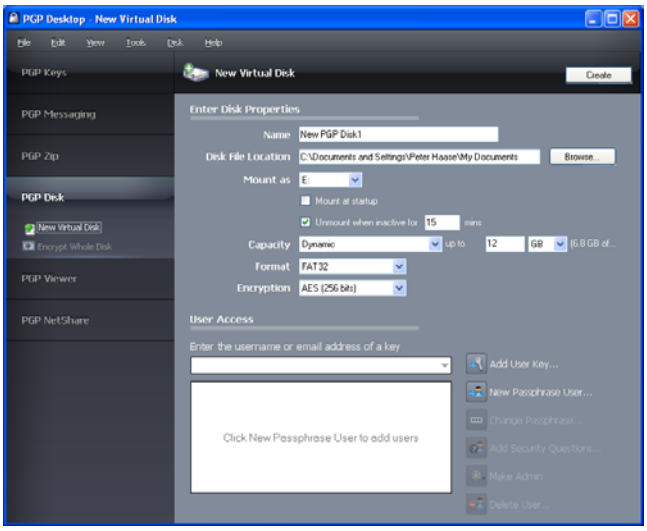
The following programs co-exist with PGP Desktop on the same system, but will block the PGP Whole Disk Encryption feature:

- Safeboot Solo
- SecureStar SCPP

Creating PGP Virtual Disk Volumes

The PGP Virtual Disk Volumes feature uses part of your hard drive space as an encrypted virtual disk volume with its own drive letter. You can create additional users for a volume so that people you authorize can also access the volume.

1 Click **New Virtual Disk** in the PGP Disk Control box.



2 Type a **Name** for the volume.

3 Specify a **Disk File Location** for the volume.

4 To specify your mount preferences, do the following::

- select a drive letter for the volume to **Mount as**.
- select **Mount at Startup** to have your new volume mount automatically at startup.
- select **Unmount when inactive for x mins** to have the volume automatically unmount when it has been inactive for the specified number of minutes.

5 From **Capacity**, select **Dynamic (resizeable)** if you want the volume to grow in size as you add files or **Fixed size** if you want the volume to always remain the same size.

6 Specify a file system **Format** for the volume.

7 Specify an **Encryption** algorithm for the volume.

8 Click **Add User Key** to add users who authenticate using public-key cryptography or click **New Passphrase User** to add users who authenticate using passphrases.

9 Click **Create**.

Use the **User Access** section to control existing users of a PGP Virtual Disk volume:

1 Click **Add User Key** to add users who authenticate using public-key cryptography.

2 Click **New Passphrase User** to add users who authenticate using passphrases.

3 Select a passphrase user, then click **Change Passphrase** to change their passphrase.

4 Select a user, then click **Make Admin** to give the user administrative rights.

5 Select a user, then click **Delete** to delete the user.

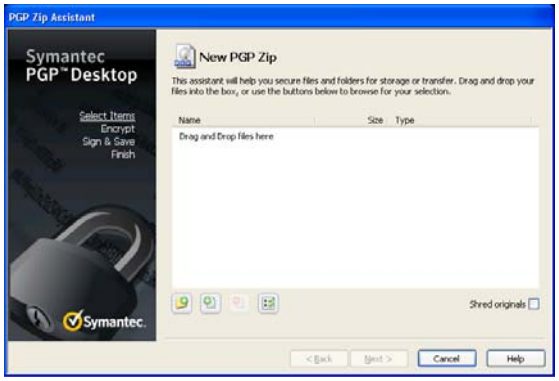
Creating a PGP Zip Archive

PGP Zip archives let you put any combination of files and folders into a compressed, portable archive. There are four kinds of PGP Zip archives:

- **Recipient keys**. Encrypts the archive to public keys. Only the holder of the corresponding private keys can open the archive. This is the most secure kind of PGP Zip archive. Recipients must be using PGP software (for Windows or Mac OS X).
- **Passphrase**. Encrypts the archive to a passphrase, which must be communicated to the recipients. Recipients must be using PGP software (for Windows or Mac OS X).
- **PGP Self-Decrypting Archive**. Encrypts the archive to a passphrase. Recipients do not need to be using PGP software to open it, but their computer must be running Microsoft Windows. The passphrase must be communicated to the recipients.
- **Sign only**. Signs the archive but does not encrypt it, allowing you to prove you are the sender. Recipients must be using PGP software (for Windows or Mac OS X) to open and verify the archive.

The Passphrase and Sign only PGP Zip types are described in detail in the *PGP Desktop User's Guide*; they are described briefly here.

1 Click **New PGP Zip** in the PGP Zip Control Box.



2 Drag and drop the files/folders you want to be in the archive or use the buttons to select them.

3 Select **Send original files to PGP Shredder when finished** if you want the files/folders you put into the archive to be shredded when the archive is created.

4 Click **Next**.

5 Select the desired kind of PGP Zip archive:

- **Recipient keys**
- **Passphrase**
- **PGP Self-Decrypting Archive**
- **Sign only**

6 Click **Next**.

Passphrase and **Sign only** are described in detail in the *PGP Desktop User's Guide*.

Refer to the appropriate section on the following pages for the kind of PGP Zip archive you specified.

Recipient Keys

The Add User Keys screen appears.

1 Click **Add** and use the User Selection screen to select the public keys of those persons who you want to be able to open the archive. If you want to be able to open the archive yourself, be sure to include your public key.

2 Click **Next**.

3 Choose a private key on the local system to use to sign the archive.

4 Specify a name and a location for the archive. The default name is the name of the first file or folder in the archive; the default location is the location of the files/folders going into the archive.

5 Click **Next**. The PGP Zip archive is created. The Finished screen displays information about the new archive.

6 Click **Finish**.

Note: The Passphrase type of PGP Zip archive is very similar to Recipient Keys, the difference being that a passphrase is used to protect the archive instead of a key.

Note: The Sign only type of PGP Zip archive is similar to Recipient Keys, the difference being that because the archive is only signed, not encrypted, you do not select public keys.

PGP Self-Decrypting Archive

The Create a passphrase screen appears.

1 Type a passphrase for the PGP Zip Self-Decrypting Archive (SDA), then type it again to confirm it.

2 Click **Next**.

3 Choose a private key on the local system to use to sign the archive.

4 Specify a name and a location for the archive. The default name is the name of the first file or folder in the archive; the default location is the location of the files/folders going into the archive.

5 Click **Next**. The PGP SDA is created.

6 Click **Finish**.

Using PGP Shred to Shred Files

The PGP Shredder feature completely destroys files and folders so that even sophisticated file recovery software cannot recover them. While both the PGP Shredder icon and the Windows Recycle Bin appear on your desktop, only PGP Shredder immediately overwrites the files you specify so that they are not recoverable.

You can shred files using any of the following methods:

- Using the PGP Shredder icon.
- Using the PGP toolbar.
- Using the PGP shortcut menu.

Shredding Files Using the PGP Shredder Icon

To shred files using the PGP Shredder icon

1 On your Windows desktop, drag the files and folders you want to shred into the PGP Shredder. A dialog box appears, asking you to confirm you want to shred the files.

2 Click **Yes**. The specified files and folders are shredded.

Shredding Files Using the PGP Toolbar

To shred files using the PGP Toolbar

1 In the PGP Desktop main application window, select **Tools > Shred Files**. The Open dialog box is displayed.

2 Select the files on your system you want to shred, then click **Open.** A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.

3 Click **Yes.** The files are securely deleted from your system.

Shredding Files Using the PGP Shortcut Menu

To shred files in Windows Explorer

1 In Windows Explorer, right-click files/folders you want to shred. A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.

2 Click **Yes.** The files are securely deleted from your system.

Note: If you do not use the PGP Shredder feature often, you can remove the PGP Shredder icon from your desktop via PGP Options. To do this, select **Tools > Options**, select the Disk tab, deselect the **Place PGP Shredder icon on the desktop** option, and then click **OK**.

Note: You can also use PGP Options to control the number of passes made when shredding (more passes is more secure but takes longer), whether files in the Windows Recycle Bin should be shredded when you empty it, and whether the warning dialog box is displayed when you shred.

Shredding Free Space

The PGP Shred Free Space feature completely shreds free space on your drives so that your deleted data is truly unrecoverable. Keep in mind that "free space" is actually a misnomer. What PGP Shred Free Space does is overwrite the portions of your hard drive that Windows believes to be empty; in fact, that space could be empty or it could be holding files Windows told you were deleted.

When you put files into the Windows Recycle Bin and empty it, the files are not really deleted; Windows just acts like there is nothing there and eventually overwrites the files. Until those files are overwritten, they are easy for an attacker to recover. PGP Shred Free Space overwrites this "free space" so that even disk recovery software cannot get those files back.

To shred free space on your disks

1 Open PGP Desktop.

2 Select **Tools > PGP Shred Free Space**.

3 On the Introduction screen, read the information, then click **Next**.

4 On the Gathering Information screen, in the **Shred drive** field, select the disk or volume you want shredded and the number of passes you want PGP Shred Free Space to perform.

The recommended guidelines for passes are:

- 3 passes for personal use.
- 10 passes for commercial use.
- 18 passes for military use.
- 26 passes for maximum security.

5 Choose whether to **Wipe internal NTFS data structures** (not available on all systems), then click **Next**.

This option shreds small (less than 1K) files in internal data structures that might otherwise not get shredded.

6 On the Perform Shred screen, click **Begin Shred**.

Note: Click **Schedule** to schedule a shred of your free space instead of doing it now. The Windows Task Scheduler must be installed on your system.

The length of the shred session depends on the number of passes you specified, the speed of the processor, how many other applications are running, and so on.

7 When the shred session is complete, click **Next**.

8 On the Completing screen, click **Finish**.

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Copyright and Trademarks