PGP NetShare Command Line User Guide

Last updated: July 2020

Copyright statement

Contents

1 Introduction

This guide provides information on how to use the PGP NetShare Command Line application.

In This Chapter

About PGP NetShare Command Line

PGP™ NetShare Command Line is a software product that lets a defined set of users access files in a shared, protected space (such as on a corporate file server, in a shared folder, or even removable media such as a thumb drive).

The files are protected by encryption, but continue to appear (to the users who have access rights) as normal application files. Anyone without access rights to the files, but who can access the shared space, can see the files but does not have access to the content.

PGP NetShare Command Line can be purchased as a standalone product, as one product among several products for example, Symantec Desktop Email or Symantec Drive Encryption), or as part of Symantec Encryption Desktop.

For more information about Symantec File Share Encyption, see the:

- *Symantec Encryption Desktop User's Guide*
- *Symantec File Share Encyption Quick Start Guide*

About PGP NetShare Command Line

PGP NetShare Command Line gives you access to Symantec File Share Encyption functionality using a command-line interface.

Accessing Symantec File Share Encyption functions from the command line is useful for scripting Symantec File Share Encyption functions, troubleshooting problems, or if the graphical user interface is not available.

Note: Not all Symantec File Share Encyption functions are available via the command line.

PGP NetShare Command Line is always in one of two operation modes:

- desktop. Symantec Encryption Desktop is also installed on the system.
- standalone. Symantec Encryption Desktop is not installed on the same system.

Run the `--version` command to see what operation mode PGP NetShare Command Line is in.

When you run the `--help` command, only those commands, options, and flags that are available in the current operation mode are displayed.

Audience

This User's Guide is for anyone who is going to be using PGP NetShare Command Line to perform Symantec File Share Encyption functions from the command line.

It assumes you are familiar with using Symantec File Share Encyption via the graphical user interface in the standalone product or as part of Symantec Encryption Desktop.

System Requirements

The system requirements for PGP NetShare Command Line are the same as for Symantec File Share Encyption itself; if Symantec File Share Encyption (standalone or as part of Symantec Encryption Desktop) installs on a system, PGP NetShare Command Line (pgpnetshare.exe) will also install and be usable.

Installing and Uninstalling

PGP NetShare Command Line (pgpnetshare.exe) is installed automatically when Symantec File Share Encyption is installed on a system.

The default location for either installation is: `C:\Program Files\PGP Corporation\PGP Desktop\pgpnetshare.exe`.

To uninstall PGP NetShare Command Line, simply uninstall Symantec File Share Encyption or Symantec Encryption Desktop.

Upgrading to Version 10.1 or Above

Changes were made to PGP NetShare Command Line in Version 10.1, resulting in some commands, options, and flags from previous versions being removed.

If you scripted previous versions of PGP NetShare Command Line, make sure to check your scripts to ensure that they do not reference commands, options, or flags that are no longer in the product.

Working with Group Keys

Starting with Symantec Encryption Management Server 3.2 and PGP NetShare Command Line 10.2, your Symantec Encryption Management Server administrator can create group keys that you can use with PGP NetShare Command Line.

Note: Group keys are different than using Active Directory groups. Using a group key adds only the single key to a protected folder. Using an Active Directory group adds every key found for members of that group.

About Group Keys

The group key is intended to be used as a single key to encrypt or decrypt Symantec File Share Encyption-protected files and folders.

The group key can be created by Symantec Encryption Management Server administrators *only*. Intended to be used with active synchronization with Active Directory, the group key reduces the overhead associated with encrypting a file/folder to a large number of keys. Your Symantec Encryption Management Server administrator can map file server access/encryption policies to Active Directory security groups.

Note: For detailed information about creating group keys, refer to the *Symantec Encryption Management Server Administrator's Guide* or contact your Symantec Encryption Management Server administrator.

When a member of the group associated with the group key leaves your organization or no longer requires access to protected folders, you should re-encrypt your folders to ensure access is denied to that member.

Using Group Keys

To use group keys with PGP NetShare Command Line:

- To encrypt or re-encrypt using the *public* portion of a group key, specify it on the command line when using the `--recipient` command.

- To unlock, re-encrypt, or decrypt using the *private* portion of a group key in a Symantec Encryption Management Server-managed environment, authenticated access to the Symantec Encryption Management Server managing the desired group key is required. Under these circumstances PGP NetShare Command Line will automatically use the enrolled user's information to authenticate.
- To unlock, re-encrypt, or decrypt using the *private* portion of a group key in a standalone environment, you must specify the Symantec Encryption Management Server managing the desired group key, the user and the user's passphrase on the command line in order to access the private portion of the group key.

Technical Support

For information about Symantec Enterprise Security Support offerings, you can visit our website at the following URL:

https://support.broadcom.com/security

2 The Command-Line Interface

This section describes the command-line interface of PGP NetShare Command Line.

In This Chapter

Overview

PGP NetShare Command Line uses a command-line interface. You enter a valid command at the command prompt and press **Enter**. PGP NetShare Command Line responds appropriately based on what you entered (if you entered a valid command) or with an error message (if you entered an invalid or incorrectly structured command).

All PGP NetShare Command Line commands have a *long form*: the text "pgpnetshare", a space, two hyphens "--", and then the command name.

For example:

```
    C:\>pgpnetshare --help [Enter]
```

is the command to display the built-in help information.

(The command prompt, C:\>, and [Enter] will no longer be shown in examples.)

A few commands also have a *short form*: one hyphen and then a single letter that substitutes for the command name. For example:

```
    pgpnetshare -h
```

is the short form of the command to access help.

Short forms of commands are noted where appropriate.

Scripting

PGP NetShare Command Line commands can easily be inserted into scripts for automating common tasks, such as creating a Protected Folder, re-encrypting a Protected Folder, or verifying files and folders in a Protected Folder.

PGP NetShare Command Line commands can easily be added to scripts written with scripting languages such as Perl or Python.

Editing the Path on a System

By default, the PGP NetShare Command Line application, pgpnetshare.exe, is installed in C:\Program Files\PGP Corporation\PGP Desktop\.

To use PGP NetShare Command Line using the Windows Command Prompt application, you need to navigate to the PGP NetShare Command Line directory to execute commands (or the commands will fail).

If you wish to be able to execute PGP NetShare Command Line commands from any location when using Windows Command Prompt, you need to change the path on the system to include the location of the PGP NetShare Command Line application.

To add the PGP NetShare Command Line application to your path on a Windows 7 or Vista system:

1. On the Windows desktop, right click the **Computer** icon, then select **Properties**.
2. On the left side of the **System Control Panel** screen, click **Advanced System Settings**.
3. If you are prompted for permission to continue, click **Continue**.
4. At the bottom of the **System Properties** screen, click **Environment Variables**.
5. In the **System Variables** section at the bottom of the **Environment Variables** screen, select **Path**, then click **Edit**.
6. At the end of the existing **Variable value** line, enter a semicolon (;), then add the path to the PGP NetShare Command Line application
7. Click **OK** to save the change, then close the windows you opened.

To add the PGP NetShare Command Line application to your path on a Windows XP or 2000 system:

1. On the Windows desktop, right click the **My Computer** icon, then select **Properties**.
2. On the **System Properties** dialog, click the **Advanced** tab.
3. At the bottom of the **Advanced** tab, click **Environment Variables**.
4. In the **System Variables** section at the bottom of the **Environment Variables** screen, select **Path**, then click **Edit**.
5. At the end of the existing **Variable value** line, enter a semicolon (;), then add the path to the PGP NetShare Command Line application.

6 Click **OK** to save the change, then close the windows you opened.

Configuration File

The PGP NetShare Command Line configuration file holds settings that affect how PGP NetShare Command Line works.

The PGP NetShare Command Line configuration file (PGPprefs.xml) cannot be changed by PGP NetShare Command Line itself: any changes need to be edited manually.

The PGP NetShare Command Line configuration file is located:

- Windows XP: **C:\Documents and Settings\[Local User]\Application Data\PGP Corporation\PGP\**.
- Windows 7 and Vista: **C:\Users\[Local User]\AppData\Roaming\PGP Corporation\PGP\**.

Note: Configuration file settings in PGPprefs.xml are shared among *all* Symantec Encryption Desktop applications on the system.

Configuration file settings you can use with PGP NetShare Command Line are:

- **Output File** (`CLoutputFile`). Specifies the output file (default is not set in the configuration file; defaults to stdout). The output file is used for output messages. See *--output-file* for more information.
- **Private keyring file** (`privateKeyringFile`). The filename or path and filename to the private keyring file. The default is **secring.skr,** located in the default PGP NetShare Command Line home directory. See *--private-keyring* for more information.
- **Public keyring file** (`publicKeyringFile`). The filename or path and filename to the public keyring file. The default is **pubring.pkr,** located in the default PGP NetShare Command Line home directory. See *--public-keyring* for more information.
- **Keyservers** (`keyservers`). Specifies the keyserver(s) to be searched for keys.
- **Always encrypt to keys** (`alwaysEncryptToKeys`). Specifies keys that should always be added implicitly when encrypting and re-encrypting.
- **Configured Symantec Encryption Management Server** (`adminGroupServer`). Specifies the Symantec Encryption Management Server used for activity logging, key and Active Directory group queries. Only available in configured installs with Symantec Encryption Desktop.
- **Enrollment Cookie** (`adminConfigCookie`). Authenticates the user against a Symantec Encryption Management Server for an operation. Only available in configured installs with Symantec Encryption Desktop.
- **Location Blacklist** (`blackListContent, enableBlackList`). Entries in the Blacklist specify those locations that should never be encrypted by PGP NetShare Command Line.
- **Organization ADK** (`ADKKeyID, useADK`). Specifies the centralized organization ADK (Additional Decryption Key). Usually only available in configured installs with Symantec Encryption Desktop.

- **Policy ADK** (`policyADK, usePolicyADK`). Specifies a policy-specific ADK. Usually only available in configured installs with Symantec Encryption Desktop.
- **Manage Individual Files** (`allowAdvancedUserMode`). Controls whether the user is allowed to manage (encrypt, decrypt, or re-encrypt) single files, as opposed to folders that might contain files.

Environment Variables

PGP NetShare Command Line behavior can be changed using environment variables.

Environment variables have the lowest priority compared to the command line and the configuration file. Settings for either will override environment variables. However, if a value for an item is not specified on the command line or in the configuration file, the environment variable will be used. Environment variables cannot be disabled; if they are present, they are implemented. To disable an environment variable, remove it. Setting a Boolean environment variable will activate it, regardless of the value to which it is set.

Environment variables that can be implemented for PGP NetShare Command Line are:

- **PGP_LOCAL_MODE**. This is a Boolean environment variable that forces PGP NetShare Command Line to run in local mode. The default is unset. See `--local-mode` for more information.

  Usage: `PGP_LOCAL_MODE=1`

- **PGP_HOME_DIR**. This is a string environment variable that overrides the default home directory, pointing it to the path supplied in the variable. The default is unset. See `--home-dir` for more information.

  Usage: `PGP_HOME_DIR=C:\Documents and Settings\<current user>\Application Data\PGP Corporation\PGP\`

- **PGP_PASSPHRASE**. This is a string environment variable that lets you set your passphrase. The default is unset. See `--passphrase` for more information.

  Usage: `PGP_PASSPHRASE="1Killer*Whale"`

Creating Environment Variables

PGP NetShare Command Line lets you create environment variables to control certain behaviors.

To create `an` environment variable on a Windows 7 system:

1. Right click the **Computer** icon on your desktop and choose **Properties**.
2. On the **System** window, click on **Advanced system settings** in the left pane.
3. On the **System Properties** window, select the **Advanced** tab and then click on **Environment Variables** near the bottom of the window.
4. In the **User Variables** section of the **Environment Variables** screen, click **New**.
5. In the **Variable name** field, enter a name for the variable you are creating.

For example, if you were setting the PGP_HOME_DIR environment variable, you would enter:

```
PGP_HOME_DIR
```

6 In the **Variable value** field, enter a value appropriate for the variable you are creating.

For example, if you were setting the PGP_HOME_DIR environment variable, you could enter:

```
C:\PGP\PGPhomedir\
```

7 Click **OK**.

The **Environment Variables** screen reappears. The environment variable you created displays in the **User variables** list.

8 Click **OK**.

9 On the **System Properties** window, click **Apply** then click **OK**.

10 Close the **System** window.

Passphrases

For consistency, all example passphrases in this guide are shown in single quotation marks ('). Putting passphrases between single quotation marks ensures that reserved characters and spaces are interpreted correctly when entered on the command line.

If you do not use any reserved characters or spaces in your passphrases, then you do not have to enclose them in single quotation marks.

On Windows systems, if you have a space in a passphrase, you must enclose the passphrase in single or double quotation marks when you enter it on the command line. Also, double quotation marks (") as part of the passphrase must be escaped with a preceding double quotation mark.

For example, if you want to use

Thomas "Stonewall" Jackson

as your passphrase, you would have to enter it as

'Thomas ""Stonewall"" Jackson'

on the command line. You need the quotation marks at the beginning and end for the spaces and you need to escape each double quotation mark used in the passphrase with another double quotation mark.

Note: If you are having problems entering certain characters in your passphrases, check the information about how to handle reserved characters for the operating system or shell interpreter you are using.

XML Output

PGP NetShare Command Line gives you the option to save some output in XML format.

If you desire properly formatted XML output, do not copy the XML output from the console window and then paste it; this could introduce extraneous newline characters into the output.

Instead, use either of these two methods:

Use the `--output-file` option.

```
pgpnetshare --list-xml <XMLcontent> output-file 'c:\acllist-xml'
```

- Pipe the output directly to a file:

```
pgpnetshare --list-xml <XMLcontent> > 'c:\acllist-xml'
```

Searching for Keys on Remote Servers

By default, PGP NetShare Command Line searches for keys on the local system.

If you want PGP NetShare Command Line to search for keys on a remote keyserver, a Symantec Encryption Management Server for example, you must explicitly tell it to search there.

There are two commands to search for keys on a remote keyserver:

- `--universal-server` searches for keys on the specified Symantec Encryption Management Server.
- `--remote` searches for keys on the specified keyserver.

3 Commands

This section describes PGP NetShare Command Line commands:

- `--version`, which displays PGP NetShare Command Line version information.
- `--help`, which provides a brief description of the commands and options available in PGP NetShare Command Line.
- `--encrypt`, which creates a Protected Folder and specifies who can access the files.
- `--decrypt`, which decrypts an existing Protected Folder and the files in it.
- `--reencrypt`, which modifies who can access files in a Protected Folder.
- `--reencrypt-full`, which modifies who can access files in a Protected Folder and reencrypts the files.
- `--reencrypt-delta`, which reencrypts files and folders in delta mode.
- `--reencrypt-clone`, which reencrypts files and folders in clone mode.
- `--list`, which lists the file or folder access control list (ACL).
- `--list-xml`, which lists the file or folder ACL in XML format.
- `--verify`, which displays information about the specified protected file or directory.
- `--lock-all`, which clears symmetric keys cached by PGP NetShare Command Line
- `--unlock`, which unlocks a file or folder.
- `--set-driver`, which sets the state of the PGP NetShare Command Line driver, active or passive.
- `--get-driver`, which displays the current state of the PGP NetShare Command Line driver, active or passive.

In This Chapter

--version

The `--version` command displays information about the version of PGP NetShare Command Line you are using, including the current operation mode: desktop or standalone.

The usage format is:

```
pgpnetshare --version [options]
```

Where:

`[options]` let you modify the command. Options are:

`--verbose`, which displays additional information about the operation.

Examples:

```
pgpnetshare --version
```

PGP NetShare Command Line responds with version information in the format:

```
PGP NetShare Command Line version 10.3.0 (Build 8228),
mode(desktop)
```

--help (-h)

The `--help` command provides a brief description of the commands, options, and flags available in PGP NetShare Command Line.

Only the commands, options, and flags that are available for the current operation mode (desktop or standalone) are displayed when you run `--help`.

The long form is:

```
pgpnetshare --help
```

The short form is:

```
pgpnetshare -h
```

The response to either version of the `--help` command is:

```
PGP NetShare command line tool.

Usage: PGPNetShare – action [--options,...]
```

--encrypt (-e)

The `--encrypt` command encrypts a specified file or directory and specifies who can access the files. Use `--encrypt` for the initial creation of a shared space protected by Symantec File Share Encyption, called a Protected Folder.

If you specify a directory to be encrypted, all files and directories under that directory are recursively encrypted; do not specify any files or directories under the directory you specify. Directories are marked as Protected Folders and files in those zones are protected.

You must designate the users who can access the files in the Protected Folder using the key IDs of their PGP keys. The key ID of a PGP key in Symantec File Share Encyption or Symantec Encryption Desktop is shown on the Key Properties screen for the key. To find a key ID, go to the PGP Keys control box, select All Keys, right click on the key whose key ID you want to know, select Key Properties, then find the ID field on the Key Properties screen. You do not need to enter the leading **0x** of the key ID.

To specify multiple users or groups who can access the files in the Protected Folder, use the `--recipient` command once for each user or the `--group` command once for each group.

If you specify a recipient who is required to use an ADK, that recipient and the ADK user will both appear on the access control list (ACL); meaning both will have cryptographic access to the protected files.

The usage format is:

```
pgpnetshare --encrypt <input> [input2 ...] --recipient  <user>
--group <group_name> --signer <signer> --passphrase <phrase>
--public-keyring <pubring> --private-keyring <priring> --output
<target> --universal-server <server> --adk <adkkey>
--output-file <logoutput> [ --halt-on-error --local-mode
--remote --preserve --verbose ]
```

Where:

- `--encrypt` is the command specifying that a Protected Folder be created.

  `<input>` is the directory or file to be encrypted. You can list multiple directories or files if desired.

- `--recipient` is the option specifying that the listed users are to be part of the ACL being created for the Protected Folder being created. The ACL lists those users who have cryptographic access to the files in the Protected Folder.

  `<user>` is the key ID of a PGP key (EFDDCE3C, for example) on the system on which you are running PGP NetShare Command Line. These can be either the keypairs or the public keys of the users who will be added to the ACL. If you specify a public key, those users must have the corresponding private key on their system when they attempt to access files in the Protected Folder.

- `--signer` is the option specifying the user on the local system whose private key will be used to sign the files in the Protected Folder.

  `<signer>` is the key ID of the PGP keypair whose private key will be used to sign the files in the Protected Folder. This user must have a private key on the local system. This user does not have to be listed as a recipient, meaning this user does not have to be someone who can access the files in the Protected Folder once it is created.

- `--passphrase` is the option specifying the passphrase of the private key being used to sign the files in the Protected Folder being created.

  `<phrase>` is the actual passphrase of the private key being used to sign the files in the Protected Folder.

- `--group` is the option specifying that you want the members of an Active Directory group to be able to access the files in the Protected Folder being created. You are not required to use this option.

  `<group_name>` is the name of an Active Directory group that includes the users you want to be able to access the files in the Protected Folder.

- `--public-keyring` is the option specifying that a public keyring file should be used for an operation

  `<pubring>` is the filename of the public keyring file.

- `--private-keyring` is the option specifying that private keyring file should be used for an operation.

  `<priring>` is the filename of the private keyring file.

- `--output` is the option specifying a target location to be used for an operation.

  `<target>` is the path to the target location.

- `--universal-server` is the option specifying that a Symantec Encryption Management Server be used for an operation.

<server> is the specific Symantec Encryption Management Server to use.

- --adk is the option specifying that an Additional Decryption Key (ADK) be used for an operation.

  <adkkey> is the key ID of the ADK to be used.

- --output-file is the option specifying that messages be written to a log file for an operation.

  <logoutput> is the path to the log file.

Optional flags are:

- --halt-on-error, which stops operation if an error occurs.
- --local-mode, which forces the use of local mode; passphrase and keyring caches are not enabled or used.
- --remote, which searches for keys on a remote keyserver.
- --preserve, which preserves certain file attributes.
- --verbose, which displays additional information about the operation being performed.

Example:

-
  ```
  pgpnetshare --encrypt C:\Projects\HR\ProjectX --recipient
  EFDDCE3C --recipient CCB81F3C --recipient C092007E --signer
  EFDDCE3C --passphrase '1Killer*Whale '
  ```

  In this example, the folder "ProjectX" is being turned into a Protected Folder; all files and folders in that folder will be protected using encryption by Symantec File Share Encyption. Three users are on the ACL; meaning only they will be able to access the files, Alice Cameron (EFDDCE3C), Jose Medina (CCB81F3C), and Ming Pa (C092007E). Alice Cameron's private key, which is on the local system, is being used to sign the files in the Protected Folder, and the passphrase to her key is provided.

-
  ```
  pgpnetshare --encrypt C:\Projects\HR\ProjectX --group HR4
  --signer EFDDCE3C --passphrase '1Killer*Whale'
  ```

  In this example, the folder "ProjectX" is being turned into a Protected Folder; all files and folders in that folder will be protected using encryption by Symantec File Share Encyption. The users in the Active Directory group HR4 will be added to the ACL, meaning only those users will have cryptographic access to the files in the Protected Folder. The private key of Alice Cameron (EFDDCE3C), which is on the local system and who is in the specified Active Directory group, is being used to sign the files in the Protected Folder, and the passphrase to her key is provided.

--decrypt

The --decrypt command decrypts the specified files or directories. The short form is -d.

Using this command takes a Protected Folder or files and removes Symantec File Share Encyption encryption from it. Use this command when you no longer need the Protected Folder. All files and folders in the subfolder will be decrypted.

If you specify a directory to be decrypted, all files and directories under the target directory are recursively decrypted. If you specify a directory, do not specify any files or directories under the directory you specify.

The usage format is:

```
pgpnetshare --decrypt <input> [input2 ...] --passphrase <phrase>
--public-keyring <pubring> --private-keyring <priring> --output
<target> [ --halt-on-error --local-mode --preserve --verbose
--force ]
```

Where:

- `--decrypt` is the command specifying that the files/folders in the Protected Folder be decrypted.

  `<input>` is the files or directories to be decrypted.

- `--passphrase` is the option specifying that the passphrase of the private key used to sign the files in the Protected Folder needs to be used.

  `<phrase>` is the actual passphrase of the private key used to sign the files in the Protected Folder.

- `--public-keyring` is the option specifying that a public keyring file should be used for an operation

  `<pubring>` is the filename of the public keyring file.

- `--private-keyring` is the option specifying that private keyring file should be used for an operation.

  `<priring>` is the filename of the private keyring file.

- `--output` is the option specifying a target location to be used for an operation.

  `<target>` is the path to the target location.

Optional flags are:

- `--halt-on-error`, which stops operation if an error occurs.
- `--local-mode`, which forces the use of local mode; passphrase and keyring caches are not enabled or used.
- `--preserve`, which preserves certain file attributes.
- `--verbose`, which displays additional information about the operation being performed.
- `--force`, which searches for keys on a remote keyserver.

Examples:

```
pgpnetshare --decrypt C:\Projects\HR\ProjectX\ --passphrase
'1Killer*Whale'
```

In this example, the folder "ProjectX" is being decrypted; all files and folders in that folder will no longer be protected as part of a Protected Folder. The passphrase to the private key on the local system being used to sign the files is provided.

--reencrypt (-r)

The `--reencrypt` command creates a new ACL from scratch that replaces an existing ACL. Files and folders that are no currently protected will be encrypted using the new ACL. The short form is `-r`.

`--reencrypt` changes the metadata of already encrypted files but does not re-encrypt the encrypted data.

This allows you to easily modify who can access the files in the Protected Folder without having to reencrypt the files themselves, which is a longer process and not necessary if you are simply changing access rights.

The usage format is:

```
pgpnetshare --reencrypt <input> [input2 ...] --recipient <user>
[-recipient <user> ...] --group <group> --signer <signer>
--passphrase <phrase> --public-keyring <pubring>
--private-keyring <priring> --output <target> --universal-server
<server> --adk <adkkey> [ --halt-on-error --local-mode --remote
-- preserve --verbose ]
```

Where:

- `--reencrypt` is the command specifying that the ACL is going to change and then be reencrypted.

  `<input>` is the files or directories affected by the `--reencrypt` command.

- `--recipient` is the option specifying that the listed users are to be added to the ACL, giving them cryptographic access to the files in the Protected Folder.

  `<user>` is the key ID of a PGP key (EFDDCE3C, for example) on the local system that you are adding to the ACL.

- `--group` is the option specifying that you want the members of the listed Active Directory group to be able to access the files in the Protected Folder. You are not required to use this option.

  `<group>` is the name of an Active Directory group that includes the users you want to be able to access the files in the Protected Folder.

- `--signer` is the option specifying the user on the local system whose private key will be used to sign the files in the Protected Folder.

  `<signer>` is the key ID of the PGP key whose private key will be used to sign the files in the Protected Folder. This user must have a private key on the local system.

- `--passphrase` is the option specifying the passphrase of the private key being used to sign the files in the Protected Folder being created.

  `<phrase>` is the actual passphrase of the private key being used to sign the files in the Protected Folder.

- `--public-keyring` is the option specifying that a public keyring file should be used for an operation

  `<pubring>` is the filename of the public keyring file.

- `--private-keyring` is the option specifying that private keyring file should be used for an operation.

  `<priring>` is the filename of the private keyring file.
- `--output` is the option specifying a target location to be used for an operation.

  `<target>` is the path to the target location.
- `--universal-server` is the option specifying that a Symantec Encryption Management Server be used for an operation.

  `<server>` is the specific Symantec Encryption Management Server to use.
- `--adk` is the option specifying that an Additional Decryption Key (ADK) be used for an operation.

  `<adkkey>` is the key ID of the ADK to be used.

Optional flags are:

- `--halt-on-error`, which stops operation if an error occurs.
- `--local-mode`, which forces the use of local mode; passphrase and keyring caches are not enabled or used.
- `--remote`, which searches for keys on a remote keyserver.
- `--preserve`, which preserves certain file attributes.
- `--verbose`, which displays additional information about the operation being performed.

Example:

```
pgpnetshare --reencrypt C:\Projects\HR\ProjectX -r ABCD1234 -r
EFGH5678 --signer EFDDCE3C --passphrase '1Killer*Whale'
```

In this example, an existing Protected Folder (C:\Projects\HR\ProjectX) is having two additional users added (the users whose PGP key IDs are ABCD1234 EFGH5678). The key ID of a private key that was already on the ACL (EFDDCE3C) is being used to sign the files in the Protected Folder, and the passphrase to that key is provided.

--reencrypt-full

The `--reencrypt-full` command creates a new ACL from scratch that replaces an existing ACL **and** reencrypts both the ACL and the encrypted files themselves. This allows you to modify who can access the files in the Protected Folder and reencrypt the files themselves at the same time.

Note: Symantec recommends using the `--reencrypt-full` command whenever you remove a user or group from the ACL or whenever you are refreshing the ACL when users have been removed from a group. This strengthens the security of your Symantec File Share Encyption files.

The usage format is:

```
pgpnetshare --reencrypt-full <input> [input2 ...] --recipient
<user> [-recipient <user> ...] --group <group> --signer <signer>
--passphrase <phrase> --public-keyring <pubring>
--private-keyring <priring> --output <target> --universal-server
<server> --adk <adkkey> [ --halt-on-error --local-mode --remote
-- preserve --verbose ]
```

Where:

- `--reencrypt-full` is the command specifying that the ACL is going to change and then be reencrypted and that the files in the Protected folder are to be reencrypted.

  `<input>` is the files or directories affected by the `--reencrypt-full` command.

- `--recipient` is the option specifying that the listed users are to be added to the ACL, giving them cryptographic access to the files in the Protected Folder.

  `<user>` is the key ID of a PGP key (EFDDCE3C, for example) on the local system that you are adding to the ACL.

- `--signer` is the option specifying the user on the local system whose private key will be used to sign the files in the Protected Folder.

  `<signer>` is the key ID of the PGP key whose private key will be used to sign the files in the Protected Folder. This user must have a private key on the local system.

- `--passphrase` is the option specifying the passphrase of the private key being used to sign the files in the Protected Folder being created.

  `<phrase>` is the actual passphrase of the private key being used to sign the files in the Protected Folder.

- `--group` is the option specifying that you want the members of the listed Active Directory group to be able to access the files in the Protected Folder. You are not required to use this option.

  `<group>` is the name of an Active Directory group that includes the users you want to be able to access the files in the Protected Folder.

- `--public-keyring` is the option specifying that a public keyring file should be used for an operation

  `<pubring>` is the filename of the public keyring file.

- `--private-keyring` is the option specifying that private keyring file should be used for an operation.

  `<priring>` is the filename of the private keyring file.

- `--output` is the option specifying a target location to be used for an operation.

  `<target>` is the path to the target location.

- `--universal-server` is the option specifying that a Symantec Encryption Management Server be used for an operation.

  `<server>` is the specific Symantec Encryption Management Server to use.

- `--adk` is the option specifying that an Additional Decryption Key (ADK) be used for an operation.

`<adkkey>` is the key ID of the ADK to be used.

Optional flags are:

- `--halt-on-error`, which stops operation if an error occurs.
- `--local-mode`, which forces the use of local mode; passphrase and keyring caches are not enabled or used.
- `--remote`, which searches for keys on a remote keyserver.
- `--preserve`, which preserves certain file attributes.
- `--verbose`, which displays additional information about the operation being performed.

Example:

```
pgpnetshare --reencrypt-full C:\Projects\HR\ProjectX -r CCB81F3C
--signer EFDDCE3C --passphrase '1Killer*Whale'
```

In this example, an existing Protected Folder (C:\Projects\HR\ProjectX) is having a user added to the ACL (the user whose PGP key ID is CCB81F3C). Because a user not on the ACL added a file to the Protected Folder, the `--reencrypt-full` command is being used so that all of the files in the Protected Folder will be encrypted to a different underlying key. The key ID of a private key that was already on the ACL (EFDDCE3C) is being used to sign the files in the Protected Folder, and the passphrase to that key is provided.

--reencrypt-delta

The `--reencrypt-delta` command allows specified recipients to be added or removed from an existing ACL.

By default, `--reencrypt-delta` does not re-encrypt the already encrypted data; it re-encrypts the metadata. You can force it to re-encrypt the data using `--reencrypt-full` as an option.

The usage format is:

```
pgpnetshare --reencrypt-delta <input> [input2 ...] --recipient
<user> [-recipient <user> ...] --group <group> --signer <signer>
--passphrase <phrase> --public-keyring <pubring>
--private-keyring <priring> --universal-server <server> --adk
<adkkey> [ --halt-on-error --local-mode --remote -- preserve
--verbose ]
```

Where:

- `--reencrypt-delta` is the command specifying that certain recipients will be added to or removed from the ACL, which will then be re-reencrypted.

  `<input>` is the files or directories affected by the `--reencrypt` command.

- `--recipient` is the option specifying that the listed users are to be added to the ACL, giving them cryptographic access to the files in the Protected Folder.

  `<user>` is the key ID of a PGP key (EFDDCE3C, for example) on the local system that you are adding to the ACL.

- --group is the option specifying that you want the members of the listed Active Directory group to be able to access the files in the Protected Folder. You are not required to use this option.

  <group> is the name of an Active Directory group that includes the users you want to be able to access the files in the Protected Folder.

- --signer is the option specifying the user on the local system whose private key will be used to sign the files in the Protected Folder.

  <signer> is the key ID of the PGP key whose private key will be used to sign the files in the Protected Folder. This user must have a private key on the local system.

- --passphrase is the option specifying the passphrase of the private key being used to sign the files in the Protected Folder being created.

  <phrase> is the actual passphrase of the private key being used to sign the files in the Protected Folder.

- --public-keyring is the option specifying that a public keyring file should be used for an operation

  <pubring> is the filename of the public keyring file.

- --private-keyring is the option specifying that private keyring file should be used for an operation.

  <priring> is the filename of the private keyring file.

- --universal-server is the option specifying that a Symantec Encryption Management Server be used for an operation.

  <server> is the specific Symantec Encryption Management Server to use.

- --adk is the option specifying that an Additional Decryption Key (ADK) be used for an operation.

  <adkkey> is the key ID of the ADK to be used.

Optional flags are:

- --halt-on-error, which stops operation if an error occurs.
- --local-mode, which forces the use of local mode; passphrase and keyring caches are not enabled or used.
- --remote, which searches for keys on a remote keyserver.
- --preserve, which preserves certain file attributes.
- --verbose, which displays additional information about the operation being performed.

Example:

```
pgpnetshare --reencrypt-delta -r ABCD1234 --recipient-remove
EFGH5678
```

In this example, the user with PGP key ABCD1234 is being added to the ACL, while the user with PGP key EFGH5678 is being removed.

--reencrypt-clone

The `--reeencrypt-clone` command consolidates a folder tree recursively using an existing ACL as a template. Files and folders that are not encrypted will be encrypted according to the template ACL.

`--reencrypt-clone` does not re-resolve keys, groups, or ADKs. The signature is also retained, as the ACL does not change.

The usage format is:

```
pgpnetshare --reencrypt-clone <input> [input2 ...] --passphrase
<phrase> --public-keyring <pubring> --private-keyring <priring>
--output <target> [ --halt-on-error --local-mode -- preserve
--verbose ]
```

Where:

- `--reencrypt-clone` is the command specifying that the ACL is going to change and then be reencrypted.

  `<input>` is the files or directories affected by the `--reencrypt` command.

- `--passphrase` is the option specifying the passphrase of the private key being used to sign the files in the Protected Folder being created.

  `<phrase>` is the actual passphrase of the private key being used to sign the files in the Protected Folder.

- `--public-keyring` is the option specifying that a public keyring file should be used for an operation

  `<pubring>` is the filename of the public keyring file.

- `--private-keyring` is the option specifying that private keyring file should be used for an operation.

  `<priring>` is the filename of the private keyring file.

- `--output` is the option specifying a target location to be used for an operation.

  `<target>` is the path to the target location.

Optional flags are:

- `--halt-on-error`, which stops operation if an error occurs.
- `--local-mode`, which forces the use of local mode; passphrase and keyring caches are not enabled or used.
- `--preserve`, which preserves certain file attributes.
- `--verbose`, which displays additional information about the operation being performed.

Example:

```
pgpnetshare --reencrypt-clone -i source -p password -o target
--reencrypt-full
```

In this example, the target is consolidated using the ACL of source as a template, and the data is fully re-encrypted by specifying the `--reencrypt-full` command as an option.

--list (-l)

The `--list` command displays the current ACL of a file or folder. All keys (user ID and key ID) and groups (including members) are displayed.

The short form is `-l`.

The usage format is:

```
pgpnetshare --list <input> [input2 ...] --output-file <logoutput>
```

Where:

- `--list` is the command specifying that you want to display the current ACL of the specified protected file or directory.

  `<input>` is the file or directory to be listed.

  Optional flags are:

  - `--output-file` is the option specifying that messages be written to a log file for an operation.

    `<logoutput>` is the path to the log file.

Example:

```
pgpnetshare --list C:\Projects\HR\ProjectX --output-file
C:\Projects\HR\Logs\ProjectX.txt
```

In this example, the protected directory "ProjectX" is being listed.

--list-xml

The `--list-xml` command displays the current ACL of a file or folder, just like the `--list` command; the `--list-xml` command, however, outputs information in XML format.

All keys (user ID and key ID) and groups (including members) are output.

The usage format is:

```
pgpnetshare --list-xml <input> [input2 ...] --output-file
<logoutput>
```

Where:

- `--list-xml` is the command specifying that you want to display the current ACL of the specified protected file or directory in XML format.

  `<input>` is the file or directory to be listed.

  Optional flags are:

- `--output-file` is the option specifying that messages be written to a log file for an operation.

  `<logoutput>` is the path to the log file.

Example:

```
pgpnetshare --list-xml C:\Projects\HR\ProjectX --output-file
C:\Projects\HR\Logs\ProjectX.xml
```

In this example, the protected directory "ProjectX" is being listed, with the output in XML format.

--verify (-v)

The `--verify` command recursively verifies the integrity of a folder tree.

It checks whether the existing ACL of files and folders is the same as the folder's ACL where it started from. Files and folder with a different ACL are displayed, as are unprotected files and folders.

The short version is `-v`.

When a directory is specified, all files and directories under the specified directory are recursively processed. Do not specify any files or directories under the specified directory on the command line.

The usage format is:

```
pgpnetshare --verify <input> [input2 ...] --halt-on-error
--output-file --verbose
```

Where:

- `--verify` is the command specifying that you want to display information about the specified protected file or directory.

  `<input>` is the file or directory to be verified.

Optional flags are:

  - `--halt-on-error`, which stops operation if an error occurs.
  - `--output-file`, which specifies a file to which you can output log information.
  - `--verbose`, which displays additional information about the operation.

Example:

```
pgpnetshare --verify C:\Projects\HR\ProjectX --halt-on-error
```

In this example, the protected directory "ProjectX" is being verified. The process will stop if it encounters a file or folder with a different ACL.

--lock-all

The --lock-all command clears symmetric keys cached by PGP NetShare Command Line. It does not clear cached private keys, which can be used to gain access to "locked" files.

--lock-all is only available in desktop mode.

The usage format is:

```
pgpnetshare --lock-all
```

Where:

--lock-all is the command to lock all Symantec File Share Encyption-protected files and directories.

Example:

```
pgpnetshare --lock-all
```

Locks all Symantec File Share Encyption-protected files and directories.

--unlock

The --unlock command prepares access to files/folders such that a later access will not trigger an unlock dialog.

--unlock is only available in desktop mode.

This command can be used to unlock folders if no one is physically present to enter the necessary passphrase; this allows files dropped into a now unlocked folder to be transparently encrypted/decrypted.

The usage format is:

```
pgpnetshare --unlock <input> --public-keyring <pubring>
--private-keyring <priring> [input2 ...] --passphrase <phrase> [
--local-mode ]
```

Where:

- --unlock is the command specifying that you want to unlock the specified locked folder.

  <input> is the file or folder to be unlocked.

- --passphrase is the option specifying the passphrase of the private key that signed the locked folder.

  <phrase> is the actual passphrase of the private key used to sign the folder.

- --public-keyring is the option specifying that a public keyring file should be used for an operation

  <pubring> is the filename of the public keyring file.

- --private-keyring is the option specifying that private keyring file should be used for an operation.

`<priring>` is the filename of the private keyring file.

Optional flags are:

- `--local-mode`, which forces the use of local mode; passphrase and keyring caches are not enabled or used.

Example:

```
pgpnetshare --unlock C:\Projects\HR\ProjectX --passphrase
'1Killer*Whale'
```

In this example, the locked folder "ProjectX" is being unlocked. The files in this folder are signed by the private key whose passphrase is provided.

--set-driver

The `--set-driver` command sets the state of the Symantec File Share Encyption driver on the local system.

The default setting is active, which is appropriate for almost all cases. **Only change this state on the command line if you fully understand how it will affect PGP NetShare Command Line operation.**

There are two options:

- **active**: Symantec File Share Encyption is operating normally, the default setting.
- **passive**: Most Symantec File Share Encyption background functionality is disabled; this setting is useful if you want to disable most Symantec File Share Encyption functionality without affecting other Symantec Encryption Desktop services on the local system. The files in the Protected Folder remain protected by Symantec File Share Encyption encryption, but no one can open, edit, or save them. *If new files are added to a Protected Folder while the driver is set to passive, those files will not be protected.*

The usage format is:

```
pgpnetshare --set-driver <state>
```

Where:

- `--set-driver` is the command specifying that the driver state is to be set.

  `<state>` is the option specifying the desired state for the driver: **active** or **passive**.

Example:

```
pgpnetshare --set-driver active
```

Sets the Symantec File Share Encyption driver to an active state.

--get-driver

The `--get-driver` command shows the PGP NetShare Command Line driver state: active or passive.

`--get-driver` is only available in desktop mode.

Example:

```
pgpnetshare --get-driver
```

```
The current driver state is [active].
```

This example shows the results of the `--get-driver` command on a system where the driver is active.

4 Options

This section describes all PGP NetShare Command Line options:

- `--recipient`, which specifies a recipient to use for an operation.
- `--recipient-owner`, which specifies an administrator recipient for an operation.
- `--recipient-operator`, which specifies a group administrator recipient for an operation.
- `--recipient-remove`, which specifies a recipient to be removed.
- `--recipient-xml`, which specifies a list of recipients in XML format.
- `--group`, which specifies the name of an Active Directory group.
- `--group-operator`, which specifies an Active Directory group by a group administrator.
- `--signer`, which specifies the PGP key ID to which protected files are encrypted.
- `--signer-passphrase`, which specifies the passphrase of a signer.
- `--signer-passphrase-fd`, which specifies the passphrase of a signer from a file descriptor.
- `--passphrase`, which specifies the passphrase to use for an operation.
- `--passphrase-fd`, which reads `--passphrase` from a file descriptor.
- `--public-keyring`, which specifies the location of the public keyring file.
- `--private-keyring`, which specifies the location of the private keyring file.
- `--universal-server`, which specifies a Symantec Encryption Management Server.
- `--auth-username`, which specifies a username on a Symantec Encryption Management Server.
- `--auth-passphrase`, which specifies the passphrase of a user on a Symantec Encryption Management Server.
- `--auth-passphrase-fd`, which specifies the passphrase of a user on a Symantec Encryption Management Server from a file descriptor.
- `--input`, which specifies an explicit input or source to use for an operation.
- `--output`, which specifies an explicit output or target to use for an operation.
- `--output-file`, which specifies a file to which you can output log information.
- `--home-dir`, which specifies the location of the home directory.

The descriptions of some PGP NetShare Command Line options mention that they are "secure," as in "This option is not secure" or "--auth-passphrase is secure". In this context, "secure" means that the option’s argument is saved in non-pageable memory (when that option is available to applications). Options that are not "secure" are saved in normal system memory.

In This Chapter

--recipient (-r)

Specifies a recipient for the current operation. The short form is `-r`.

To specify multiple users who can access the files in the Protected Folder, use the `--recipient` command once for each user.

`--recipient` accepts a single key or key collection as an argument.

The default is not set. This option is not secure.

Example:

```
pgpnetshare --encrypt C:\Projects\HR\ProjectX --recipient EFDDCE3C
--recipient CCB81F3C --recipient C092007E --signer EFDDCE3C
--passphrase '1Killer*Whale'
```

In this example, three recipients are specified: EFDDCE3C, CCB81F3C, and C092007E. These are the three users who will be on the Access Control List, meaning they will have cryptographic access to the files in the Protected Folder being created.

--recipient-owner

Specifies a Symantec File Share Encyption administrator as the recipient for the current operation.

`--recipient-owner` accepts a single key or key collection as an argument.

The default is not set. This option is not secure.

--recipient-operator

Specifies a Symantec File Share Encyption group administrator as the recipient for the current operation.

`--recipient-operator` accepts a single key or key collection as an argument.

The default is not set. This option is not secure.

--recipient-remove

Used with the `--reencrypt-delta` command, removes a specific key or group from an ACL.

`--recipient-remove` does not support a key collection as an argument.

--recipient-xml

Specifies an XML-formatted file that contains a list of recipients for the current operation.

`--recipient-xml` cannot be mixed with other recipient options.

The syntax for a recipient in an XML-formatted file is:

```
<recipient>
<type>key</type>
<role>owner</role>
<keyid>0x12345678</keyid>
<name>test1 'test1@example.com'</name>
</recipient>
```

Where:

- Type can be one of `key`, `adk`, or `group`. If none is specified, `key` is used.

- Role can be one of `owner`, `operator`, or `user`. If none is specified, `user` is used.

--group (-g)

Specifies an Active Directory group whose users will be added to the ACL of the Protected Folder. The short form is `-g`.

To specify multiple groups who can access the files in the Protected Folder, use the `--group` command once for each group.

The default is not set. This option is not secure.

Example:

```
pgpnetshare --encrypt C:\Projects\HR\ProjectX --group HR4 --group
HR7 --signer EFD DCE3C --passphrase '1Killer*Whale'
```

In this example, the folder "ProjectX" is being turned into a Protected Folder. The users in Active Directory groups HR4 and HR7 will be added to the ACL, meaning only those users will have cryptographic access to the files in the Protected Folder.

The `--group` parameter is used for groups, such as distribution lists, and not for group keys.

Note: To encrypt or decrypt a folder or file using a group key, use the `--recipient` parameter with `--encrypt` or `--decrypt`.

--group-operator

Specifies the Symantec File Share Encyption administrative role (group administrator) for a group; used instead of `--group`.

All the members of the group share the group's role; a group cannot be the Owner (administrator).

The default is not set. This option is not secure.

--signer (s)

Specifies the key ID of the signing key being used to sign the meta data.

If the operation requires only a single passphrase (`--encrypt`, for example), then the regular passphrase option (`--passphrase`) can be used instead of `--signer-passphrase` or `--signer-passphrase-fd`.

The default is not set. This option is not secure.

Example:

```
pgpnetshare --encrypt C:\Projects\HR\ProjectX -r CCB81F3C -r
C092007E --signer EFDDCE3C --passphrase '1Killer*Whale'
```

In this example, the key with key ID EFDDCE3C is being used to sign the meta data. The option `--passphrase` is used to specify the passphrase of the key, as the operation only requires one passphrase. `--signer-passphrase` or `--signer-passphrase-fd` could have been used in place of `--passphrase`.

--signer-passphrase

Specifies the passphrase of the key being used to sign the meta data.

If the operation requires only a single passphrase (`--encrypt`, for example), then the regular passphrase option (`--passphrase`) can be used instead of `--signer-passphrase`.

--signer-passphrase-fd

Specifies the passphrase of the key being used to sign the meta data from a file descriptor.

If the operation requires only a single passphrase (`--encrypt`, for example), then the regular passphrase option (`--passphrase`) can be used instead of `--signer-passphrase-fd`.

--passphrase (-p)

Specifies a passphrase to use for the current operation. The short form is `-p`.

A passphrase can be specified by an environment variable. A passphrase specified on the command line always takes precedence over the environment variable.

By default, PGP NetShare Command Line integrates with an existing passphrase cache. This integration can be disabled using the `--local-mode` flag.

The default is not set. This option is secure.

Example:

```
pgpnetshare --encrypt C:\Projects\HR\ProjectX -r EFDDCE3C -r
ECCB81F3C -r EC092007E --signer EFDDCE3C --passphrase '1Killer*Whale'
```

In this example, a new Protected Folder is being created. The files in the Protected Folder will be encrypted to private key of user EFDDCE3C, requiring the passphrase of that key.

--passphrase-fd

Sets `--passphrase` to the data read from a file descriptor.

The default is not set. This option is secure. Requires a positive integer.

Reads double-byte characters on Windows and UTF-8 on UNIX. The version of the option that ends with "8" reads UTF-8 on Windows; this has no effect on UNIX, as UTF-8 is already being read there.

Note: Consult the help and/or documentation for the command shell being used for more information about how that command shell handles file descriptors.

Example:

```
pgp ... --passphrase-fd 7
```

Read passphrase from file descriptor 7.

--adk

Specifies the key ID of a key to be used as an ADK (additional decryption key).

If an organization ADK and/or a policy ADK are specified in the configuration file, they are always used; specifying an ADK on the command line does not override the organization and/or policy ADK.

If a specified ADK cannot be retrieved, the operation aborts.

--public-keyring

Changes the location of the public keyring file. The default order for keyring search is: specified on the command line, specified in the configuration file, then home directory/pubring.pkr. This option is not secure.

This option always specifies a file. Relative or absolute path information can be included, but the target must still be a file.

You can also set the location in the PGP NetShare Command Line configuration file.

You can specify a single file, relative path, or full path:

- File, relative to the personal directory.
- Relative path, relative to the current directory.
- Absolute path, recommended usage.

Example:

```
pgpnetshare --public-keyring C:\Documents and Settings\<current
user>\Application Data\PGP Corporation\PGP\pubring.pkr
```

This example shows the absolute path to the public keyring file.

--private-keyring

Changes the location of the private keyring file. The default order for keyring search is: specified on the command line, specified in the configuration file, then home directory/secring.skr. This option is not secure.

This option always specifies a file. Relative or absolute path information can be included, but the target must still be a file.

You can also set the location in the PGP NetShare Command Line configuration file; refer to Configuration File for more information.

You can specify a single file, relative path, or full path:

- File, relative to the personal directory
- Relative path, relative to the current directory
- Absolute path, recommended usage

Examples:

1 `pgp --private-keyring /home/dave/.pgp/secring-backup.skr`

Absolute path to the private keyring file.

2 `pgp --private ./secring.skr`

Relative path to the private keyring file.

--universal-server

Specifies a Symantec Encryption Management Server to search for keys or to resolve groups.

`--universal-server` takes the fully qualified domain name (FQDN) or IP address of the Symantec Encryption Management Server as an argument.

PGP NetShare Command Line supports connections to a Symantec Encryption Management Server via the USP or OCOS protocols.

--auth-username

Specifies a username used to authenticate to a Symantec Encryption Management Server for those operations that require authentication.

`--auth-username` takes a valid username on the Symantec Encryption Management Server as an argument.

--auth-passphrase

Specifies the passphrase to a username used to authenticate to a Symantec Encryption Management Server for those operations that require authentication.

`--auth-passphrase` takes a valid passphrase (for the specified username) on the Symantec Encryption Management Server as an argument.

--auth-passphrase-fd

Specifies the passphrase from a file descriptor to a username used to authenticate to a Symantec Encryption Management Server for those operations that require authentication.

`--auth-passphrase-fd` takes a file descriptor number that references a valid passphrase (for the specified username) on the Symantec Encryption Management Server as an argument.

--input (-i)

Specifies an explicit input or source to be used in an operation. The short form is `-i`.

`--input` is only available in standalone mode.

`--input` supports the special argument '-' to specify stdin (standard input).

The default is not set. If an operation requires input but does not get it, an error is returned. This option is not secure.

--output (-o)

Specifies an explicit output or target to be used in an operation. The short form is `-o`.

`--output` is only available in standalone mode.

`--output` supports the special argument '-' to specify stdout (standard output).

The default is not set. If a location/object cannot be determined from the output, an error is returned. This option is not secure.

--output-file

Specifies a file to which PGP NetShare Command Line messages will be output.

Text files are output as UTF8. To view on a Windows system, open in Notepad (specify UTF8 when opening the file if necessary).

The default is not set. This option is not secure.

Example:

```
pgpnetshare --output-file C:\Projects\HR\ProjectX\logs.txt
```

Specifies that the PGP NetShare Command Line output logs should be sent to a file called `logs.txt` in directory `C:\Projects\HR\ProjectX`.

--home-dir

Specifies the location of the home directory, the location where PGP NetShare Command Line looks for keyring files and the configuration file (PGPprefs.xml).

`--home-dir` can only be used in standalone mode; that is, *without* Symantec Encryption Desktop also installed on the same system.

You can specify a default home directory using the environment variable **PGP_HOME_DIR**. A home directory specified on the command line takes precedence over the environment variable.

5 Flags

This section describes all PGP NetShare Command Line flags:

- `--verbose`, which displays additional information about the operation.
- `--remote`, which searches for keys on a remote keyserver.
- `--forc`e, which forces the decryption of a file.
- `--halt-on-error`, which stops operation if an error occurs.
- `--local-mode`, which forces the use of local mode; passphrase and keyring caches are not enabled or used.
- `--preserve`, which preserves certain file attributes.
- `--quiet`, which limits the number of error messages displayed.

In This Chapter

--verbose

Enables verbose messages, which displays additional information about an operation. Using `--verbose` displays processed objects, errors, and the result of the operation.

The default message level is normal, which displays errors and the result of the operation.

Note: `--verbose` is not compatible with `--quiet`. You can use one or the other, but not both, for an operation.

The default is off.

--remote

Searches for keys on a remote keyserver. Use `--remote` if the needed keys are on a keyserver and not on the local keyring.

Using `--remote` specifies that the keyserver(s) specified in the configuration file will also be searched for the specified keys. Make sure the desired keyserver is specified in the configuration file.

Note: PGP NetShare Command Line does not search for keys on any keyserver unless instructed to do so using either `--remote` to specify a keyserver or `--universal-server` to specify a Symantec Encryption Management Server.

The default is off.

--force

Forces the decryption of a file. Only available for use with the `--decrypt` command.

Using `--force` skips the padding verification that is normally performed to ensure that the entire key chain is valid.

If a file is truncated or corrupted, it will not normally be decrypted. Use `--force` to decrypt these files to recover their data.

The default is off.

--halt-on-error

When specified, stops the operation if any error occurs.

When `--halt-on-error` is off, the default setting, PGP NetShare Command Line will stop an operation only if a severe or unrecoverable error occurs.

The default is off.

--local-mode

Forces the use of local mode; passphrase and keyring caches are disabled.

`--local-mode` controls whether or not PGP NetShare Command Line integrates with the PGP SDK managing the passphrase cache. When set, the passphrase cache and features that require the passphrase cache are disabled.

Local mode can also be set by an environment variable, but the command line flag takes precedence.

The default is off.

--preserve

Preserves certain file attributes.

Using `--preserve` controls whether certain properties are preserved by an operation. The last modified date and read-only attributes (Windows 32 only) are preserved.

The default is off.

--quiet

Enables quiet messages, which limits the amount of information that PGP NetShare Command Line displays about an operation (errors are suppressed).

The default message level is normal, which displays errors and the result of the operation.

Note: `--quiet` is not compatible with `--verbose`. You can use one or the other, but not both, for an operation.

`Use --quiet` with `--output` to prevent the corruption of the output stream.

The default is off.

A Quick Reference

This section lists and briefly describes all PGP NetShare Command Line commands, options, and flags.

In This Chapter

Commands

--version	Shows PGP NetShare Command Line version information.
--help (-h)	Shows basic help information for PGP NetShare Command Line.
--encrypt	Creates a Protected Folder and specifies who can access the files.
--decrypt	Decrypts an existing Protected Folder and the files in it.
--reencrypt	Modifies who can access files in a Protected Folder.
--reencrypt-full	Modifies who can access files in a Protected Folder and reencrypts them.
--reencrypt-delta	Reencrypts files and folders in delta mode.
--reencrypt-clone	Reencrypts files and folders in clone mode.
--list	Lists the file or folder access control list (ACL).
--list-xml	Lists the file or folder ACL in XML format.
--verify	Displays information about the specified protected file or directory.
--lock-all	Clears any cached symmetric keys.
--unlock	Provides access to the specified locked file or directory.
--set-driver	Sets the PGP NetShare Command Line driver state, active or passive.
--get-driver	Displays the current state of the PGP NetShare Command Line driver, active or passive.

Options

--recipient	Specifies a recipient for an operation.
--recipient-owner	Specifies an administrator recipient for an operation.
--recipient-operator	Specifies a group administrator recipient for an operation.
--recipient-remove	Specifies a recipient to be removed.

--recipient-xml Specifies a list of recipients in XML format.

--group (-g) Specifies an Active Directory group.

--group-operator Specifies an Active Directory by a group administrator.

--signer Specifies the PGP key ID to which protected files are encrypted.

--signer-passphrase Specifies the passphrase of a signer.

--signer-passphrase-fd Specifies the passphrase of a signer from a file descriptor.

--passphrase (-p) Specifies a passphrase for an operation.

--passphrase-fd Reads a passphrase from a file descriptor.

--adk Specifies an additional decryption key for an operation.

--public-keyring Specifies the location of the public keyring file.

--private-keyring Specifies the location of the private keyring file.

--universal-server Specifies a Symantec Encryption Management Server.

--auth-username Specifies a username on a Symantec Encryption Management Server.

--auth-passphrase Specifies the passphrase of a user on a Symantec Encryption Management Server.

--auth-passphrase-fd Specifies the passphrase of a user on a Symantec Encryption Management Server from a file descriptor.

--input Specifies an explicit input or source to use for an operation.

--output Specifies an explicit output or target to use for an operation.

--output-file Specifies a file for log output.

--home-dir Specifies the location of the home directory; can only be used in standalone mode.

Flags

--verbose Displays additional information about the operation.

--remote Searches for keys on a remote keyserver.

--force Forces the decryption of a file.

--halt-on-error Stops operation if an error occurs.

--local-mode Forces the use of local mode; passphrase and keyring caches are not enabled or used.

--preserve Preserves certain file attributes

--quiet Limits the number of errors messages displayed.

B Automated Copying

You can use PGP NetShare Command Line for automated copying of data.

There are two procedures, depending on your operation mode: standalone or desktop.

Copying in Standalone Mode

To perform an automated copying in standalone mode, use the `--reencrypt-clone` command with explicit input and output options.

For example:

-
  ```
  pgpetshare.exe --reencrypt-clone -input <C:\SOURCE> -output
  <C:\TARGET> -p <password>
  ```

  In this example, the files/folders are copied from SOURCE to TARGET, retaining the encryption of SOURCE. The target directory must already exist, but subdirectories are created automatically.

Copying in Desktop Mode

To perform an automated copying in desktop mode, two-stop approach is required, as explicit input and output options are not allowed in desktop mode.

For example:

1. Encrypt the target directory using PGP NetShare Command Line:

   ```
   pgpnetshare.exe --list-xml C:\SOURCE | pgpNetShare.exe -e
   C:\TARGET --recipient-xml - -s signer -p password
   ```

   In this example, PGP NetShare Command Line grabs the ACL of SOURCE and pipes it to another instance of PGP NetShare Command Line, which encrypts the input. The target directory must already exist.

2. Copy the files/folders from source to target using XCOPY. If the passphrase is not cached, you will be prompted to enter it.