



Rack-Soft, LLC 2002-2008

# 4PSA Total Backup 2.0.0 for Plesk 8 / Plesk 7.x Reloaded User's Guide



# User's Guide

Manual Version \$Change: 36814 \$. \$Revision: #18 \$ at \$DateTime: 2008/04/21 17:13:07 \$

For suggestions regarding this manual contact:

[docs@4psa.com](mailto:docs@4psa.com)

Copyright © 2002-2008 Rack-Soft, LLC

All rights reserved

Distribution of this work or derivative of this work is prohibited unless prior written permission is obtained from the copyright holder.

4PSA is a Registered Trademark of Rack-Soft, LLC.

Plesk is a Registered Trademark of Parallels, Inc.

Linux is a Registered Trademark of Linus Torvalds.

RedHat is a Registered Trademark of Red Hat Software, Inc.

FreeBSD is a Registered Trademark of FreeBSD, Inc.

All other trademarks and copyrights are property of their respective owners.

# Table of Contents

<b>Preface</b> .....	5
Who Should Read This Guide .....	5
<b>Chapter 1. About 4PSA Total Backup 2.0.0</b> .....	6
4PSA Total Backup 2.0.0 Features .....	6
<b>Chapter 2. The Administrator Module</b> .....	8
1. Backup Sessions .....	9
Log Messages Explained .....	10
2. Log Management .....	12
Deleting the logs .....	12
Search Options .....	12
History Results .....	12
3. Settings .....	13
Backup Reports .....	13
Backup Setup .....	13
Server Backup Settings .....	14
Backup Schedule Period .....	16
Remote Storage Settings .....	16
Maintenance Settings .....	18
Interface Settings .....	19
GnuPG Keys Management .....	19
4. License Management .....	21
<b>Chapter 3. Backup Tips &amp; Tricks</b> .....	22
1. Comparison between Tar and <code>pleskbackup</code> .....	22
2. Why Do I Need the Remote Storage Facility? .....	23
3. How to Restore? .....	24
Restore Using <code>tbrestore</code> .....	24
Restore Files from Tar Archives .....	24
Restore the MySQL Databases .....	27
Restore the PostgreSQL Databases .....	28
4. Low Level Settings .....	28

**Appendix A. Server Compatibility** ..... 30

# Preface

## Who Should Read This Guide

This User's Guide must be read by the administrator of the Plesk server or by the person responsible with the server backups.



## Chapter 1

# About 4PSA Total Backup 2.0.0

4PSA Total Backup 2.0.0 is a server-level application that provides an advanced automated backup system for Plesk servers. The application consists of a single administrator module that allows the server administrator to control various backup options and track the history of the backup processes through the integrated logging mechanism.

## 4PSA Total Backup 2.0.0 Features

- Automate server backup (administrator only)
- Backup exception email alerting
- Multi volume backups supported
- Incremental and full backups supported
- Backup files encryption
- Configurable backup cycle

- Configurable number of backups stored on local and storage server
- Can restore files, directories and databases
- Advanced logging functions
- Quality of Service functions
- Remote backup storage capabilities with the following features:
  - Supports FTP and SSH protocol for storage to remote servers
  - SSH protocol compression, bandwidth limitation
  - Automatic transfer of archives to remote servers
  - Backup files integrity checks
- Backup in Plesk native format option
- Exclude directories from backup



## Chapter 2

# The Administrator Module

The 4PSA Total Backup administrator module can be accessed by logging in the Plesk with the admin account. To access the 4PSA Total Backup interface, in the Custom navigation menu click the [4PSA Total Backup](#) link.

The 4PSA Total Backup toolbar is available on top of the application's interface. The toolbar makes it easy for the server administrator to perform the following operations:

- view details about backup sessions
- view the history of the backup operations outcome
- view a report about 4PSA Total Backup
- modify various parameters that control the behavior of 4PSA Total Backup
- manage GnuPG public and private keys
- manage the local and remote storage features
- change interface settings

- manage the 4PSA Total Backup license

## 1. Backup Sessions

4PSA Total Backup keeps a detailed log of all the operations performed during a backup. The logging mechanism helps you identify problems that may occur during the backup operation.

To access this area, in the toolbar click the Sessions button.

In the Backup sessions area the server administrator can view the backup actions of the latest backup cycle performed by the backup engine. This cycle is divided in backup sessions. For every backup session displayed on this page, the starting and completion date are available.

A log entry consists of three fields:

- Date – The system time when the logged action occurred (day month year, hh:mm:ss)
- Action taken – Action performed by 4PSA Total Backup
- Outcome – The outcome of the backup operation, which can be success or failure.

The following events are logged:

- disk space exceeded
- backup operation starting and completion time
- outcome of files backup operation
- outcome of databases backup operation
- outcome of remote connection establishment
- file transmission errors
- remote file system operations
- database operations

This information is logged in the database and in a file. The log file is located in Local archives directory path field (defined in the Settings area) and the file is called action.log. You may want to setup a log rotation system for this file or empty it periodically.

## Log Messages Explained

- backup session [session no] started – Marks the start of the backup session.
- using passive FTP transfer mode – Indicates that passive ftp transfer mode is being used.
- using active FTP transfer mode – Indicates that active ftp transfer mode is being used.
- do\_backup is already running. Backup cannot start twice! – 4PSA Total Backup engine is running. Most likely the old instance didn't end due to an error. Check the logs and eliminate the error cause. 4PSA Total Backup can not continue.
- 4PSA Total Backup GPG keys not found, backups will be made without encryption – If GPG has to be used and no keys are found the backup process will continue, but the backups will not be encrypted.
- disk space absolute limit check failed (available=[avail], required=[req]) – The absolute available disk space (MB) is below the set limit.
- disk space relative limit check failed (available=[avail] required=[req]) – The relative available disk space (percentage %) is below the set limit.
- [bktool] backup with no compression started – Indicates the start of a backup using the backup tool [bktool] (tar or pleskbackup) without compression.
- [bktool] backup with [comptool] compression started – Indicates the start of a backup using the backup tool [bktool] (tar or pleskbackup) and the compression tool [comptool] (gzip or bzip2).
- [bktool] backup with no compression [status] – Indicates the outcome of the backup process ([status] which can be "failed" or "succeeded") using the backup tool [bktool] (tar or pleskbackup) without compression.
- [bktool] backup with [comptool] compression [status] – Indicates the outcome of the backup process ([status] which can be "failed" or "succeeded") using the backup tool [bktool] (tar or pleskbackup) and the compression tool [comptool] (gzip or bzip2).
- an unexpected condition occurred during the backup! – Indicates that one of the issued commands failed to execute.
- MySQL databases dump with no compression started – Indicates the start of a MySQL dump without compression process.

- MySQL databases dump with [comptool] compression started – Indicates the start of a MySQL dump without compression process. The compression tool [comptool] can be gzip or bzip2.
- MySQL databases dump with no compression failed – The `mysqldump` process could not be started (`mysqldump` utility is missing or some other error occurred).
- MySQL databases dump with [comptool] compression failed – The `mysqldump` process could not be started (`mysqldump` utility is missing or some other error occurred).
- MySQL databases dump with no compression [status] – Indicates the outcome of the MySQL dump process without compression ([status] can be "failed" or "succeeded").
- MySQL databases dump with [comptool] compression [status] – Indicates the outcome of the MySQL dump process ([status] can be "failed" or "succeeded") using the compression tool [comptool] (can be gzip or bzip2).
- PostgreSQL databases dump with no compression started – Indicates the start of the PostgreSQL dump process without compression.
- PostgreSQL databases dump with [comptool] compression started – Indicates the start of the PostgreSQL dump process using the compression tool [comptool] (can be gzip or bzip2).
- PostgreSQL databases dump with no compression [status] – Indicates the outcome of the PostgreSQL dump process without compression ([status] can be "failed" or "succeeded").
- PostgreSQL databases dump with [comptool] compression [status] – Indicates the outcome the PostgreSQL dump process ([status] can be "failed" or "succeeded") using the [comptool] compression tool (can be gzip or bzip2).
- FTP transfer error while trying to export [path] transfer failed – An error occurred while trying to upload the backup files to the FTP server.
- FTP Backups validation failed – The transferred backup files failed the validation check. This can occur only if FTP Transfer Validation is enabled.
- FTP Backups validation successful – The transferred backup files were successfully validated. The validation occurs only if FTP Transfer Validation is enabled.
- FTP transfer of [path] succeeded – The backup files were successfully uploaded to the FTP site.
- post FTP transfer operations succeeded – The post FTP transfer operations were completed successfully.


- post FTP transfer operations failed – The post FTP transfer operations failed to complete.
- SSH transfer of [path] [status] – Indicates the outcome of the backup files transfer operation to the SSH server ([status] can be "failed" or "succeeded").
- post SSH transfer operations [status] – Indicates the outcome of the post SSH transfer operations ([status] can be "failed" or "succeeded").
- backup session [session no] ended – Marks the end of the backup session.

## 2. Log Management

In this area, the server administrator can search, view and delete backup operations logs based on several criteria.

To access the Log Management area, in the toolbar click the Logs button.

### Deleting the logs

You are able to clear the entire logs list. Just click the  Clear logs icon located in the Tools section at the top of the page.

### Search Options

In this section, the server administrator can choose the search criteria and search the backup operation logs. The following criteria are available:

- From and To – Search for logs included between two dates in year–month–day format.
- Outcome – Search for logs with a specified finish status, which can be success or failure.
- Show – Limit the number of results to view in one page.

### History Results

Based on the chosen search criteria, 4PSA Total Backup displays the logs that matched your input. Every log entry consists of three fields:

- Date – The system time when the logged action occurred (day month year, hh:mm:ss)
- Action taken – Action performed by 4PSA Total Backup
- Outcome – The outcome of the backup operation, which can be success or failure.

### 3. Settings

In this area, the server administrator can:

- view a 4PSA Total Backup report
- modify various parameters that control the behavior of 4PSA Total Backup
- manage the local and remote storage features
- manage GnuPG public and private keys
- change interface settings

To access this area, in the toolbar click the Settings button.



#### Note

Before running 4PSA Total Backup for the first time you must adjust these settings.

### Backup Reports

The Product version field displays the version of the 4PSA Total Backup installed on the server.

### Backup Setup

This section allows the server administrator to enable/disable the backup engine and to setup the following options:

- Backup active – When this option is enabled, the backup engine will run as scheduled. When it is disabled, no backups will be performed.
- Send email notifications on errors – If this option is enabled, an email message containing a description of the error that has occurred in the backup process will be sent to the email address specified in the Administrator email field.

- Administrator email – The email address of the server or backup administrator. This must be a valid address.

## Server Backup Settings

This section allows the server administrator to setup various options that control the backup process flow.

- Backup tool – By default, the tar software is used to perform system backups. Alternatively, if you have installed the Plesk `pleskbackup` utility, you can use it for the backup operation.
- Compression tool – You can choose to compress the archive files generated by the backup operation in order to save disk space. There are two compression tools that you can use: `gzip` or `bzip2`. Due to a restriction of the `pleskbackup` tool, you cannot use `bzip2` compression for archives created using `pleskbackup`.



### Note

Creating compressed archives is not recommended because a single modified bit in a compressed archive can make the restoration process impossible.

- Multi volume archives – You can choose the size of the backup archives. Select a volume size only if you want the backup archives to be split in several, equally sized files. These smaller files are better for easy storage on external devices with a limited storage capacity (CD, DVD). You can choose from several preset file sizes.
- Backup MySQL databases – When this option is enabled, the `mysqldump` tool will be used to make a full backup of all your MySQL databases.
- Backup PostgreSQL databases – When this option is enabled, the `pgdump` tool will be used to make a full backup of all your PostgreSQL databases. This setting is valid only when the backup tool is tar.



### Note

The "Backup MySQL" databases and "Backup PostgreSQL databases" settings are valid (and required) only when the backup tool is tar. `pleskbackup` integrates databases backup.

- Local archives directory path – This is the directory where the backup archives will be stored. It should be a local path. We recommend you to

use a path located on a different physical disk, especially if you do not use a remote storage facility.

This directory will contain the backup cycles directories, which will be named `bak_yyyy_mm_dd_hh_mm_ss`, containing the year, month, day, hour, minute and second when the cycle had begun.



#### Note


Use an empty directory because the contents of this directory will be erased when the backup archives are copied. Avoid using directory names that contain spaces.

- Backup cycle – When the tar software is used to perform backups, setting the backup cycle to a value greater than 1 will result in creating incremental backups with the specified cycle length. Incremental backups are part of a backup technique that consists in creating a full backup of the system at the beginning of the backup cycle and then in creating backups of the files that were modified after the initial full backup. This backup technique has the advantage of creating smaller backup files, therefore saving disk space and minimizing system load.



#### Note

When the `pleskbackup` software is used, the backup cycle represents the number of backup files that will be stored on your machine.

- Reset backup cycle – Reset the 4PSA Total Backup cycle.
- GPG Encryption – Use GnuPG to encrypt the backup files. The administrator can manage the GPG public and private keys by clicking the  Edit keys icon.



#### Note

The GPG encryption is recommended only for advanced users who have a deeper understanding of the process. It is not recommended to encrypt large backup files because the backup process will be very slow.

## Backup Schedule Period

This section allows the server administrator to setup various options that control when the backup process is executed.

- Schedule backup tool to run on – You can set the time when the backup operation automatically starts. This is done by adding an entry in your system's crontab manager table in order to schedule the backup operation. The backup operation will be automatically performed when the time specified by the date fields matches the current time. The following time fields are available:
- Minute – The range of accepted values is 0 – 59.
- Hour – The range of accepted values is 0 – 23.
- Day of the Month – The range of accepted values is 1 – 31.
- Month – The range of accepted values is 1 – 12.
- Day of the Week – The range of accepted values is 0 – 7. When specifying day of week: day 1 is considered Monday, day 6 is considered Saturday while both day 0 and day 7 are considered Sunday.



### Note

You can also use an asterisk (\*) which indicates that any value is matched.

Lists of numbers are also allowed, e.g. "0,15,30,45" for the Minute field.

Example: If you want to schedule backups every night at 2:15, the settings must be the following:

Minute: 15

Hour: 2

Day of the Month: \*

Month: \*

Day of the Week: \*

## Remote Storage Settings

4PSA Total Backup has the option to keep a copy of the backup archives on a remote machine such as a backup server or a dedicated storage facility.

When this option is enabled, the server administrator must provide the following connection details required to connect and transfer files on the remote machine:

- Remote storage facility – 4PSA Total Backup is able to automatically save a copy of the backup archives on a remote storage facility by using the FTP or SSH protocols. Use the available dropdown list to choose between Don't use remote storage, Connect using SSH or Connect using FTP. SSH is the recommended method since it provides increased security and an improved mechanism for error detection / correction.



#### Note

When using SSH, your machine must be able to login with no password to the remote server, using key passing. The public key of your server must be placed in the remote server's authorized key list. This technique is called key exchange.

- Remote machine IP address – The IP address of the remote server.
- Remote machine hostname - The hostname of the remote machine.
- Remote machine port - The port of the remote server. Default values: 22 for a SSH connection, 21 for an FTP connection.
- Use for remote connection – Use this radioboxes to choose how to connect to the remote machine: using the IP address or the hostname. One of the Remote machine IP address or Remote machine hostname options must be filled in based on that choice.
- Remote machine login name – The user name required to connect to the remote machine.
- Remote machine password – The password required to connect to the remote machine using the specified user name.



#### Note

The password field is required only for transfers through FTP. It will be ignored if you previously chose to transfer your files through SSH.

- Remote machine storage dir – The directory on the remote machine where the backup files will be stored. Do not place other content in this directory as it might be erased. Avoid using directory names that contain spaces.
- Limit transfer bandwidth to - The maximum limit of the bandwidth transfer.

- Enable compression - If this check box is checked, the backup files will be compressed using SSH compression. This type of compression is worth using if your connection is slow (for example, a modem connection). The efficiency of the compression depends on the type of the file, and varies widely. It is close to 0% for already compressed files like zip and often 50% or even more for text files.



#### Note

The **Limit transfer bandwidth to** and **Enable compression** are available only if the **Remote storage facility** is set to **Connect using SSH**.

- FTP transfer mode – The transfer mode can be active or passive. In passive mode, the administrator initiates the data connection by connecting to the data port. Passive mode is often necessary for operations performed behind firewalls that do not permit incoming connections. You might need to disable the passive mode if the FTP server does not support passive operations. Active mode can be used when the server accepts incoming connections.
- FTP transfer validation – If enabled, the sizes of the transferred files are compared with the sizes of the original files.



#### Note

If you have troubles with the storage of the backup files on the FTP server, you can try to disable the FTP transfer validation. Make sure that files are transferred properly to the FTP server.



#### Note

The **FTP transfer mode** and **FTP transfer validation** options are available only if the **Remote storage facility** is set to **Connect using FTP**

## Maintenance Settings

The server administrator can change the following storage settings:

- Don't perform any backup if free disk space is below – The backup operation will fail to start if the free disk space on the Local archives directory path is below the chosen value. You can specify an absolute

value (in MB) e.g. 1000 MB or a relative value (in %) e.g. 10% of the Local archives directory path's full size.


- Keep a local copy of # cycles – The number of backup cycles that will be stored on the local machine.
- Keep remotely # cycles – The number of backup cycles that will be stored on the remote machine.
- Delete history records older than # months – In order to prevent the backup history records getting too large, the records that are older than a specified number of months can be deleted.

## Interface Settings

In this section, the server administrator can edit the following interface settings:

- Custom button title – The name of the custom button in the left panel. The server administrator can change the default nomination 4PSA Total Backup with a more descriptive name for his clients.
- Context help – The 4PSA Total Backup description that will appear in the navigation panel on the left.
- Language – Here all installed language packs are displayed. The interface will use the language pack setup in the account preference in Plesk. If this language pack is not available, the system will default to English. One can use only languages that have been installed in the Plesk interface.

## GnuPG Keys Management

To manage the public and private GPG keys, the server administrator must click the  Edit keys icon available in the Server backup settings area. In the GPG management page the administrator can generate GnuPG keys, import or export them, from/to the server. These keys are used when backup files are encrypted with GPG.

### Generate Keys

In this section, the server administrator can generate the GPG keys. The following details will be displayed:

- Real name – This is the name that will be displayed by the GPG key

- Email address – This is the email address displayed by the GPG key

To generate the GPG keys with these details, click the Generate button.



#### Note

Generating the keys may take several minutes, depending on the machine speed and randomness sources.

### Import Keys

In this section, the server administrator can import the GPG keys and upload them on the server. The following fields are available:

Public key – Use this field to enter the name of the file containing the public key to be imported or click the  button to locate the desired file.

Private key – Use this field to enter the name of the file containing the private key to be imported or click the  button to locate the desired file.

To upload the GPG keys, click the Upload button. The administrator can also enter the public and private key using the following fields:

- Public key – The server administrator can fill in the public key.
- Private key – The server administrator can fill in the private key.

To import the GPG keys, the server administrator must click the Import button. These keys must be created using the real name and email address displayed in the Generate keys area.



#### Note

After importing the keys, the server administrator must login to 4PSA Total Backup and issue the following command:  
`gpg --homedir /usr/local/tbackup/.gnupg --edit-key "Total Backup" trust`  
When prompted „Ultimately trust the imported key" the administrator should type **5** and **ENTER** . To exit the GPG console he must type **quit** and **ENTER**.

The server administrator **cannot use** the imported key unless he performs the above steps.

### Existing Keys

4PSA Total Backup displays in this area the GPG keys available on the server and allows the administrator to export these files on his computer. To download these keys to the local machine, the server administrator must click the Download button.

## 4. License Management

In this area, you can manage the 4PSA Total Backup license. The product requires a license key in order to work. The license key will be generated by 4PSA based on the server IP and Plesk version installed on the server.

You can use the following fields and controls to update or monitor your license:

- License key status – The status of the currently loaded license key
- Your server IP – This is the main IP address of your server. The license key must be issued for this IP, otherwise it will not work.
- License file – You can use this form to upload the license key to the server.



### Note

If you can access other pages in 4PSA Total Backup, this means that your license is valid and you do not have to upload a new one.

- Get license from licensing server - You can use this form to query the licensing server. This function can only be used when there is a license key loaded on the server. The first time you install the product you will be required to upload the license key.
- License key properties – This section contains details about the current license.



### Note

The Owned and Leased licenses automatically renew before the **License expire date**.



## Chapter 3

# Backup Tips & Tricks

This chapter explains general backup concepts that you can use in 4PSA Total Backup.

### 1. Comparison between Tar and **pleskbackup**

Most users cannot decide which backup tool to use. Here is a comparison between the `pleskbackup` and `tar` tools:

**Table 3.1.**

Criteria	Pleskbackup	Tar
Backup all server	No, only Plesk files	Yes, except several OS dependent directories
Backup particular directories	Not possible	Yes, you can adjust the list of directories that are backed up
Incremental backup	Not possible	Yes

Disk space required	Equal to the Plesk customer data, for every backup	Almost equal to the server data, but only once in the cycle (first backup)
Server load	High	Medium
Databases dump	Yes, automatically	Separate option
Time required for the first backup	Depends on server configuration and load. ~ 5Gb/hour	Depends on server configuration and load. Faster than <code>pleskbackup</code> .
Time required for the incremental backup sessions	As in the first backup session, no incremental support.	When performed daily, the time required by incremental backups is less than 15 min in most cases.
Restore difficulty	Easy with <code>pleskrestore</code>	Easy with <code>tbrestore</code>
Time required by restore	Very slow restore process	Fast restore process

We strongly advise you to use tar because it uses less server resources and a smaller amount of space to store archives. The restore process is much faster with tar than with `pleskbackup`, although inexperienced administrators might find it to be more difficult.

## 2. Why Do I Need the Remote Storage Facility?

4PSA Total Backup is able to transfer files to a remote server in order to increase the reliability of the backup process. You have the possibility to store backup files locally. However, if you do not use a separate HDD, the backups are as exposed to a crash just as the other server files. Even with a dedicated backup HDD, data is not safe in case of a hacker attack.

Most Data Centers have dedicated backup facilities available for customers. If available, we recommend you to upload files to a remote computer using SSH.

In order to use SSH you must configure the server to log in the remote machine using key exchange, as explained bellow:

- The private and public keys of the backup server should be placed in `/root/.ssh`
- The `authorized_keys` file should reside in the `.ssh` directory of the remote server login account (for example `/home/backupaccount/.ssh`)



#### Note

**Do not use** the root account to login to the remote backup server.

## 3. How to Restore?

4PSA Total Backup archives can be restored automatically using `tbrestore` or manually using system level utils. Below you can find several recommendations for these operations.

### Restore Using `tbrestore`

The easiest way to restore system files, directories and MySQL databases is to use the 4PSA Total Backup restore script `tbrestore`. The `tbrestore` script is located in `/usr/local/tbackup` directory and represents an easy, yet advanced way to restore from 4PSA Total Backup archives. In order to start the restore process, launch `tbrestore` and follow the instructions. The script will prompt you for restore options and will guide you through this process.

### Restore Files from Tar Archives

To restore files from a tar archive, you can consult the tar documentation using the command `man tar`. Tar is a very flexible archiving tool and has many features that can be used to restore specific files, directories, etc.

Example 1: Restore from a multi volume tar backup that was compressed using `gzip`.

Go to the directory where the backup files are located using a command similar to this:

```
root@localhost ~ # cd /tbackup.backups
```

Go to the directory that contains the desired backup session using a command similar to this:

```
root@localhost tbackup.backups # cd bak_2008_03_10_08_33_38/  
bak-2-tar-2008-3-10
```

Assuming that in this directory you have files like `backup.tar.gz*` and `mysql.dmp.gz*`, issue the following commands:

```
#> ls backup.tar.gz* | grep -v "md5" | xargs cat | tar -C [dest_dir] -zxf -
```

```
#> ls mysql.dmp.gz* | grep -v "md5" | xargs cat | gzip -q -c -d > [dest_dir]/mysql.dmp
```

Example 2: Restore a directory from a multi volume tar backup that was compressed using bzip2.

Go to the directory where the backup files of 4PSA Total Backup are located using a command similar to this:

```
root@localhost ~ # cd /tbackup.backups
```

Access the backup cycle directory that contains the desired backup session:

```
root@localhost tbackup.backups # cd bak_2008_03_10_08_33_38/bak-2-tar-2008-3-10
```

Assuming that in this directory you have files like backup.tar.bz2\* and mysql.dmp.bz2\*, issue the following commands:

```
#> ls backup.tar.bz2* | grep -v "md5" | xargs cat | tar -C [dest_dir] -jxf - path/to/directory
```

```
#> ls mysql.dmp.bz2* | grep -v "md5" | xargs cat | bunzip2 -q -c -d > [dest_dir]/mysql.dmp
```

Example 3: Restore from a tar backup file that was compressed using gzip and encrypted using GnuPG.

Go to the directory where the backup files of 4PSA Total Backup are located using a command similar to this:

```
root@localhost ~ # cd /tbackup.backups
```

Access the backup cycle directory that contains the desired backup session:

```
root@localhost tbackup.backups # cd bak_2008_03_10_08_33_38/bak-2-tar-2008-3-10
```

Assuming that in this directory you have the files backup.tar.gz.gpg and mysql.dmp.gz.gpg, issue the following commands:

```
#> gpg --homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -o --d backup.tar.gz.gpg | gzip -q -c -d | tar -C ./ -xf -
```

```
#> gpg --homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -
o --d mysql.dmp.gz.gpg | gzip -q -c -d > [dest_dir]/mysql.dmp
```

Example 4: Restore from a tar backup file that was compressed using bzip2 and encrypted using GnuPG.

Go to the directory where the backup files of 4PSA Total Backup are located:

```
root@localhost ~ # cd /tbackup.backups
```

Access the backup cycle directory that contains the desired backup session:

```
root@localhost tbackup.backups # cd bak_2008_03_10_08_33_38/
bak-2-tar-2008-3-10
```

Assuming that you have in this directory the files `backup.tar.bz2.gpg` and `mysql.dmp.bz2.gpg`, issue the following commands:

```
#> gpg --homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -
o --d backup.tar.bz2.gpg | bunzip2 -q -c -d | tar -C [dest_dir] -xf -
```

```
#> gpg --homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -
o --d mysql.dmp.bz2.gpg | bunzip2 -q -c -d > [dest_dir]/mysql.dmp
```

Example 5: Restore a multi volume tar backup that was compressed using gzip and encrypted using GnuPG.

Go to the directory where the backup files of 4PSA Total Backup are located:

```
root@localhost ~ # cd /tbackup.backups
```

Access the backup cycle directory that contains the desired backup session:

```
root@localhost tbackup.backups # cd bak_2008_03_10_08_33_38/
bak-2-tar-2008-3-10
```

Assuming that you have in this directory files like `backup.tar.gz.gpg*` and `mysql.dmp.gz.gpg*`, issue the following commands:

```
#> ls backup.tar.gz.gpg* | grep -v "md5" | xargs cat | gpg --
homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -d - | gzip -
q -c -d | tar -C [dest_dir] -xf -
```

```
#> ls mysql.dmp.gz.gpg* | grep -v "md5" | xargs cat | gpg --
homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -d - | gzip -
q -c -d > [dest_dir]/mysql.dmp
```

Example 6: Restore a multi volume tar backup that was compressed using bzip2 and encrypted using GnuPG.

Go to the directory where the backup files of 4PSA Total Backup are located:

```
root@localhost ~ # cd /tbackup.backups
```

Access the backup cycle directory that contains the desired backup session:

```
root@localhost tbackup.backups # cd bak_2008_03_10_08_33_38/  
bak-2-tar-2008-3-10
```

Assuming that you have in this directory files like backup.tar.bz2.gpg\* and mysql.dmp.bz2.gpg\*, issue the following commands:

```
#> ls backup.tar.bz2.gpg* | grep -v "md5" | xargs cat | gpg --  
homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -d - | bzip2 -  
q -c -d | tar -C [dest_dir] -xf -
```

```
#> ls mysql.dmp.bz2.gpg* | grep -v "md5" | xargs cat | gpg --  
homedir /usr/local/tbackup/.gnupg/ -r "Total Backup" -d - | bzip2 -  
q -c -d > [dest_dir]/mysql.dmp
```

Let's assume that you have a backup cycle of seven days and the first backup day is Sunday. To restore the files on server as they were on Tuesday, you have to restore the Sunday archive, the Tuesday archive and the Wednesday archive.

In order to restore the server to the latest state you must restore all the backup archives from the last backup cycle. 4PSA Total Backup keeps the backup files in name incremented directories, so all you have to do is to access the directories in the backup order (1,2,3, ...n) and untar the files as described above.



#### Note

The incremental backup features allow you to restore the server to any previous state saved during the backup cycle.

## Restore the MySQL Databases

To restore the MySQL databases you must have the mysql.sql file. If it was compressed and/or encrypted you must first decompress and/or decrypt the mysql dump as described above. In order to load the sql file into Mysql you must issue the following command:

```
#> cat mysqlfile.sql* | /path/to/mysql -uadmin -p`cat /etc/psa/.psa.shadow`
```

You can use the `-force` option when errors are encountered during the MySQL files restore. However, this is not recommended.

## Restore the PostgreSQL Databases

To restore the PostgreSQL databases you must have the `postgresql.sql` file. If it was compressed and/or encrypted you must first decompress and/or decrypt the `postgresql` dump as described above. In order to load the `sql` file into PostgreSQL you must issue the command:

```
#> /path/to/psql -f postgresql.sql* template1
```

Due to the nature of SQL databases, they cannot be backed up incrementally, so every backup session in the cycle will contain the full MySQL and PostgreSQL database dumps.

## 4. Low Level Settings

The file `/usr/local/tbackup/paths.cfg` contains five directives. These directives cannot be modified using the browser interface:

- `tar_path` – The path where the `tar` tool is located. If the directive is empty or commented the default `tar` path on the operating system is used. (Example: `tar_path /usr/bin/tar`)
- `gpg_path` – The path to `gpg` tool. If the directive is empty or commented the default `tar` path on the operating system is used. (Example: `tar_path /usr/bin/gpg`)
- `md5_path` – The path to `md5sum` (under RedHat) or `md5` (under FreeBSD). If the directive is empty or commented the default path on the operating system is used. (Example: `md5_path /usr/local/md5sum`)
- `exclude_path` – Paths that are excluded during the backup operation, when `tar` is the used backup tool. Some paths are excluded from the backup in the default installation. If you have an additional HDD or another path that you want to exclude from the server backup in order to save space you must add it here. (Example: `exclude_path /opt /mnt /proc /sbin`)
- `include_path` – Use this setting when you do not want the entire server to be backed up. Only the directories in the `include_path` are saved in the `tar`

file. The exclude path is also considered. The directories required to restore Plesk are `/etc`, `/usr/lib`, `/usr/qmail` and `/usr/local/psa`.

- `tar_debug_file` – This file logs all tar operations. This setting is used for debugging purposes and it is recommended that you leave it empty.
- `log_level` – Syslog log level used by Total Backup backup agent. All 4PSA Total Backup logs are written to `/var/log/messages`.



#### Note

The Local archives directory path is automatically excluded. It is not necessary to add it here.

# Server Compatibility

4PSA Spam Guardian is shipped in different installation archives for different Plesk versions:

- Plesk 7.1.1 Reloaded and Plesk 7.5.3 Reloaded. These versions have Plesk7x prefix in the installation archive name.
- Plesk 7.5.4 and upper versions of Plesk 7.5 Reloaded. These versions have Plesk75 prefix in the installation archive name.
- Plesk 8.0 and upper versions. These versions have Plesk8 prefix in the installation archive name.

You have to download the build based on the Plesk version and operating system installed on your machine.

Below you can find the archive names for Plesk 8 versions, the archive names for other Plesk versions are built as specified above. For more details you can check the 4PSA Clients Area.

The file `sguardianXXX_buildXXXXXX.XX_Redhat7xPlesk8.tar.gz` provides compatibility with the following operating systems:

- RedHat Linux 7.3
- RedHat Enterprise Linux 2.1

The file `sguardianXXX_buildXXXXXX.XX_RHEL3Plesk8.tar.gz` provides compatibility with the following operating systems:

- RedHat Enterprise Linux 3.0
- Fedora Linux Core 1
- Fedora Linux Core 2
- CentOS 3.x
- RedHat Linux 9

The file `sguardianXXX_buildXXXXXX.XX_RHEL4Plesk8.tar.gz` provides compatibility with the following operating systems:

- RedHat Enterprise Linux 4.0
- CentOS 4.x

The file `sguardianXXX_buildXXXXXX.XX_RHEL5Plesk8.tar.gz` provides compatibility with the following operating systems:

- CentOS 5.x

The file `sguardianXXX_buildXXXXXX.XX_FC3Plesk8.tar.gz` provides compatibility with the following operating systems:

- Fedora Linux Core 3

The file `sguardianXXX_buildXXXXXX.XX_FC4Plesk8.tar.gz` provides compatibility with the following operating systems:

- Fedora Linux Core 4

The file `sguardianXXX_buildXXXXXX.XX_FC5Plesk8.tar.gz` provides compatibility with the following operating systems:

- Fedora Linux Core 5

The file `sguardianXXX_buildXXXXXX.XX_FC6Plesk8.tar.gz` provides compatibility with the following operating systems:

- Fedora Linux Core 6

The file `sguardianXXX_buildXXXXXX.XX_FC7Plesk8.tar.gz` provides compatibility with the following operating systems:

- Fedora Linux Core 7

The file `sguardianXXX_buildXXXXXX.XX_FreeBSD4Plesk8.tar.gz` provides compatibility with the following operating systems:

- FreeBSD 4.x

The file `sguardianXXX_buildXXXXXX.XX_FreeBSD5Plesk8.tar.gz` provides compatibility with Plesk 7.5.4 and later and the following operating systems:

- FreeBSD 5.x
- FreeBSD 6.x

The file `sguardianXXX_buildXXXXXX.XX_Suse93Plesk8.tar.gz` provides compatibility with the following operating systems:

- Suse 9.3

The file `sguardianXXX_buildXXXXXX.XX_Suse100Plesk8.tar.gz` provides compatibility with the following operating systems:

- Suse 10.x

The file `sguardianXXX_buildXXXXXX.XX_Debian31Plesk8.tar.gz` provides compatibility with the following operating systems:

- Debian 3.1
- Ubuntu 5.10
- Ubuntu 6.x