

HP Data Protector for PCs 7.0 – Sizing

First published August 2011, Latest version, V 1, Aug 2011

Technical white paper

Table of contents

Abstract.....	2
Introduction.....	2
Solution description.....	2
Cleanup	4
Data Vault sizing	5
Disk space requirements	5
Sizing example.....	6
Weekly Cleanup.....	7
How to influence the total size of handled files	8
Policy Server sizing.....	15
Reporting data retention	15
Network considerations.....	16
Monitoring the Data Vault Server and Cleanup.....	16
Best practices	18
Administration	18
End-user.....	19
Summary	22
Rules of thumb	22
For more information.....	23



Abstract

This white paper provides information on how to size HP Data Protector for PCs 7.0 environments. It will guide you through the process of sizing, provide recommendations how to size your Data Vault and Policy Server, and answer questions that may arise.

For details on installation refer to the *HP Data Protector for PCs 7.0 Installation and Administration Guide*.

Introduction

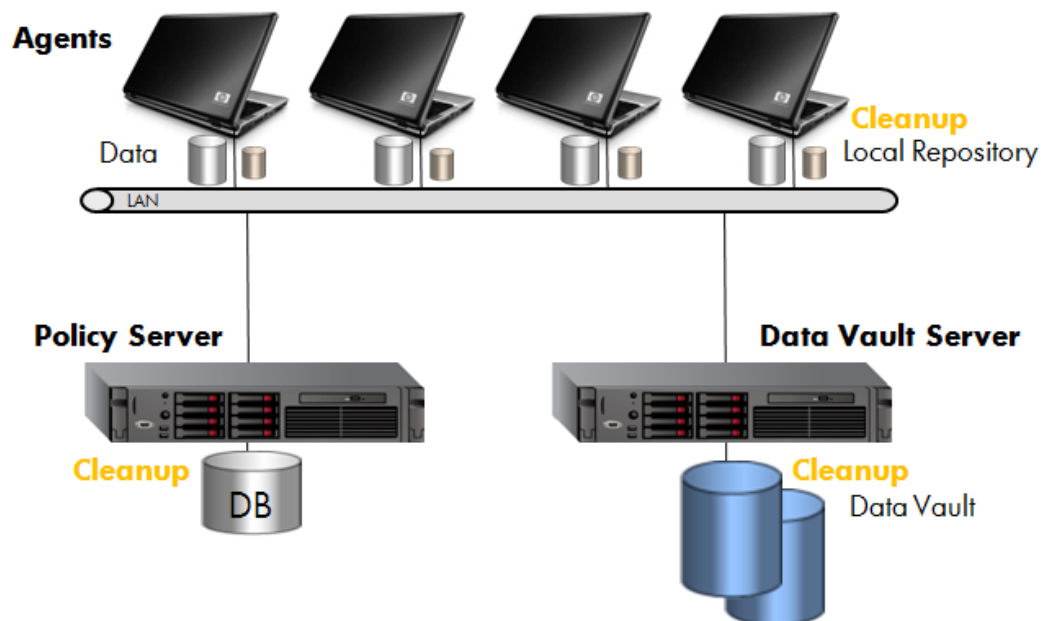
HP Data Protector for PCs is an expansion of HP Data Protector (HP's high performance backup and recovery software), designed specifically for notebooks and desktops. Data Protector for PCs ensures the availability of business data on PCs without compromising productivity or mobility. It provides the ability to enforce central protection policies and optimize bandwidth and storage capacity for all notebooks and desktops in the organization.

As an important component of HP's Data Protector product portfolio, Data Protector for PCs is an integral part of a complete backup and recovery strategy. Appropriate for companies in any industry, it is the ideal solution for increasing productivity of your employees and avoiding the business risks and costs associated with PC data loss.

Solution description

Data Protector for PCs consists of three components. In each client, an **Agent** establishes a local storage area (Local Repository) to hold active files until connection to the network occurs and to keep files protected with CFP (Continuous File Protection) for offline recovery. When a network connection is detected, files are transferred automatically for backup to a dedicated defined **Data Vault**. The overall system management is administered by a central **Policy Server**.

Figure 1: Data Protector for PCs architecture



There are two varieties of Data Vault possible with Data Protector for PCs:

- Web Data Vaults—based on HTTPS protocol. These provide the best level of security and better throughput in high latency environments, and so are recommended.
- Windows file share Data Vaults—based on CIFS protocol, used in earlier versions of Data Protector for PCs.

The data structure of both types of Data Vault is the same, so you can convert existing Windows file share Data Vaults to Web Data Vaults. For more details on Data Vaults and Data Vault migration, see the *HP Data Protector for PCs 7.0 Installation and Administration Guide*.

Sizing a Data Protector for PCs environment is complex. There are two areas where sizing is important, the Data Vault and the Policy Server. When talking about a Windows file share Data Vault you also need to consider the network latency.

Data Vaults

Sizing a Data Vault needs to answer various questions in order to determine how many Agents can be supported in your environment:

- How much data can be supported per Data Vault?
- How big does the Data Vault need to be for a specific amount of Agent user data?
- How many CPUs/cores are needed for processing the data?

The technical factors that influence how much data that can be processed on a Data Vault, and the number of users a specific environment can support, include:

- The processing power on the Data Vault (for the nightly consolidation of backup data)
- The network and I/O bandwidth on the Data Vault server
- Disk space on the Data Vault server

Policy Server

For the Policy Server, the main questions are:

- How many Agents can be accommodated with the standard Microsoft SQL Server Express Edition?
- Are there any specific SQL considerations?
- Does the network bandwidth influence Policy Server sizing?
- How much processing power is needed?

Data Vaults are the biggest consideration when thinking about sizing. A major factor that determines how many Agents a Data Vault can support is **Cleanup**. In this whitepaper we will start by looking at Cleanup and how it affects sizing considerations, then move on to look at **Data Vaults**, after that take a look at the **Policy Server**, and finally **Network Considerations**. At the end, we will look at some other best practices that have some bearing on sizing.

Cleanup

The Local Repositories on user computers and the Data Vaults on file servers need to be periodically maintained to remove versions that are outdated based on the retention settings defined in file protection policies. This important process of Data Protector for PCs is performed by the **Cleanup** software.

Cleanup occurs on each of the three components of Data Protector for PCs, and consolidates all file versions on the Data Vault and the Local Repository and maintains the SQL database on the Policy Server.

Data Protector for PCs is delivered with default Cleanup settings: cleanup of Data Vaults and the Policy Server occurs every midnight, cleanup of Local Repositories on Agents every hour.

As the Cleanup process on the Policy Server just maintains the outdated reporting data, it has no effect on sizing of the Policy Server or Data Vault.

Also Cleanup settings of Local Repositories have no immediate influence on the sizing itself. But as the version creation of OFP (Open File Protection) files is directly connected to the Local Repository Cleanup, changing the Cleanup settings will affect how often Data Protector for PCs creates a version of the OFP files (by default, every hour), which results in how much data is created per Agent.

The Data Vault Cleanup process affects Data Vault sizing. Before Cleanup can maintain the data on the Data Vault server, it needs to decrypt and uncompress the data. After the maintenance, the data needs to be compressed and encrypted again.

Figure 2: Cleanup process



Note: Cleanup runs in multithreaded mode. With the help of an Auto-Adjuster, Cleanup will always use the given resources in best way. It is possible to change Cleanup starting parameters (see “Configuring multithreaded cleanup” in the *Installation Guide*), but in most environments this is not recommended and default settings will give you the best results.

Changing the Data Vault Cleanup start time may influence the Data Vault sizing, as described later in this document.

Data Vault sizing

As described in the previous section, Data Vault sizing is influenced mainly by the Cleanup process that maintains the Data Vault's data. It is not so important how many clients are supported per Data Vault, the main question is how much data can be handled by the Cleanup process.

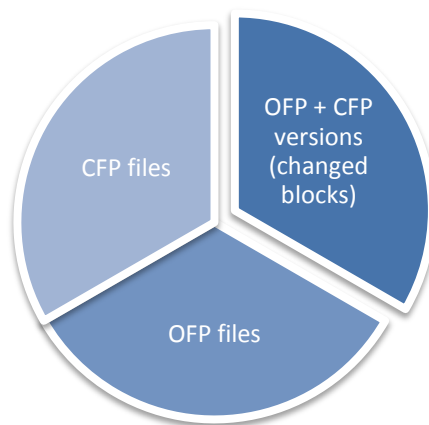
Important: It is highly recommended that the Cleanup process runs only in non-business hours, which limits the Cleanup time.

When you have calculated how much data can be handled, you can easily use this figure to determine how many Agents can be supported per Data Vault.

The quantity of data that can be handled refers to the *total size of handled files*.

The *total size of handled files* is the sum of all CFP files + OFP files + file versions (delta blocks).

Figure 3: Total size of handled files



Disk space requirements

The total size of handled files is also the disk space needed on the Data Vault. This implies the question, how to calculate the needed disk space on the Data Vault?

Disk space requirements are influenced by many factors, of which the main ones are:

1. Total size of protected files on Agents
2. Compression ratio (different for different file types)
3. Change rate (if "number of days" is used in the retention criteria settings)
4. Ratio of the number of CFP files to OFP files
5. Encryption overhead

As a rule of thumb for most environments, such as a standard office system, you can reckon 10 GB of protected data on an Agent requires 4 GB of disk space on the Data Vault.

To get an idea how much data needs to be protected on Agents in your environment you need to check the Agents themselves. The tool **windirstat** may be helpful to get an overview of which files reside on the Agent. The tool is available for download at <http://windirstat.info/>.

Be aware that you will always see some Agents that do not fit into your standard Agent behavior and may have much more data to be protected. Therefore you should always have enough buffer in your disk space sizing.

Sizing example

Settings

In this example we want to size a Data Protector for PCs setup with default settings. Default settings mean:

- Data Vault Cleanup is configured to run daily at midnight.
- Local Repository Cleanup is configured to run every hour.
- Retention criteria:
 - Number of days to keep versions when the existing file is changed: 30
 - Number of days to keep versions after the file is deleted: 15
- The default set of policies is enabled (Office Documents, Software Development, Web Documents, Windows Mail).

Cleanup time

We will assume the environment we want to size is running a 12 hour business. As it is highly recommended not to run the Cleanup process during business hours, 12 non-business hours are left in which to run the Cleanup.

The Data Vault Server hardware recommendations are as follows:

- Windows File Share Data Vault: 3 GHz dual core, 4 GB RAM
- Web Data Vault: 3 GHz quad core, 4 GB RAM

With this hardware, we can clean 14 TB of backup data in 12 hours Cleanup time.

Note: The quad core CPU on Web Data Vault is needed as the web server requires CPU time.

Note: To be sure the Cleanup only runs in non-business hours, change the Data Vault Cleanup start time to start directly after business hours are finished (see [How to set the Cleanup Policy?](#)).

Number of supported Agents

An Agent in this environment has the following data characteristics:

- Average number of protected files: 5000
- Average total size of protected files on its local disk: 10 GB

Using the rule of thumb given in [Disk space requirements](#) above, the average total size on the Data Vault will be 4 GB per Agent (remembering that this depends highly on the compression rate, data change rate, and so on). This allows around 3500 Agents to be connected to this Data Vault.

Summary – daily Cleanup, default settings

The calculation of how many Agents can be supported is done in two steps.

1. Calculate how much data can be supported per Data Vault. This is influenced by the Cleanup time and by the hardware, the policy settings and the cleanup time.

Data Vault type	Windows File Share DV	Web DV
Hardware	3 GHz dual core, 4 GB RAM	3 GHz quad core, 4 GB RAM
Cleanup time (daily)	12 hours	12 hours
Supported DV total size	14 TB	14 TB

- Calculate how many Agents can be supported per Data Vault. This is influenced by the supported Data Vault size, the disk space needed per Agent which is influenced by the policy settings (file protection policy, cleanup policy).

Data Vault type	Windows File Share DV	Web DV
Policy settings	default	default
DV disk space per Agent	4 GB	4 GB
Supported Agents per DV	3500	3500

Weekly Cleanup

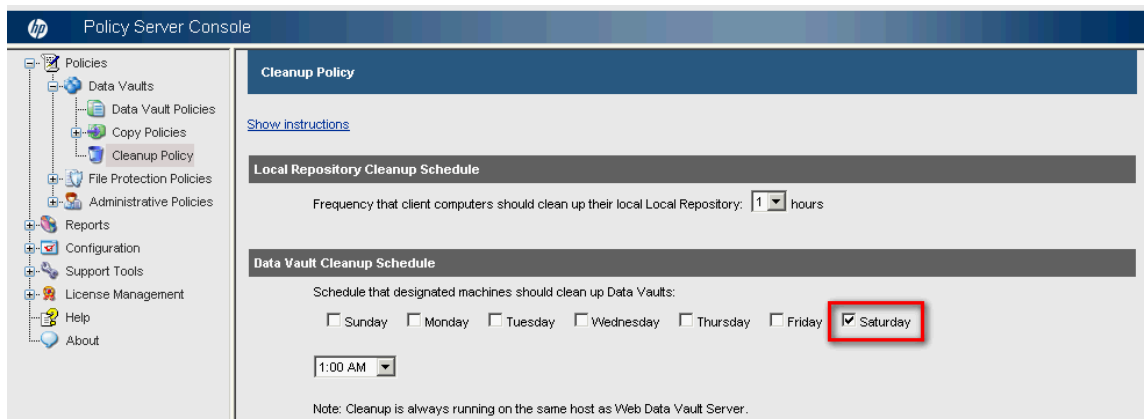
So that the Data Vault can support more users, run the Cleanup process only at weekends, starting on Friday evening or early Saturday morning, so that it has maximum time in which to run.

A weekly Cleanup can handle a greater *total size of handled files* in a Cleanup session than daily Cleanup. The Cleanup can delete more outdated versions in one session. The advantage is that the Cleanup needs to decrypt/uncompress and compress/encrypt all the data only once.

In order to change the Cleanup schedule:

- Open the **Cleanup Policy** page in the Policy Server Administrator console and change the **Data Vault Cleanup Schedule**.
- Uncheck all days except Friday or Saturday:
 - For Friday, pick a start time late in the evening, such as 10:00 pm.
 - For Saturday, pick a start time early in the morning, such as 1:00 am.

Figure 4: Cleanup configured every Saturday at 1:00 am



Note: Weekly Cleanup has some disadvantages that you should consider:

- The list of files presented for restore from a Data Vault will be out-of-date by up to one week. Users can always trigger a manual rescan of their data on the Data Vault to get an up-to-date view.
- Backup versions will still exist beyond their time for obsolescence for up to a week because the Cleanup only runs at weekends.
- Quota management is not up-to-date. If users exceed their quota, they may have to wait until Cleanup has run to free space on the Data Vault again. On the other hand, exceeding the quota may not be immediately recognized by the system because space usage reporting is part of the Cleanup process.
- Reporting data (Data Vault reports) will be out-of-date by up to one week.

Summary – weekly Cleanup, default settings

Run the Data Vault Cleanup only at weekends. A weekly Cleanup has the advantage of being able to handle more data in just one Cleanup session. It needs to decrypt/uncompress and compress/encrypt all the data only once, and can delete more outdated versions in one session. With the same hardware as in the previous sizing example, the amount of data that can be handled will increase up to 40 TB. This should increase the number of Agents that can be supported by a Data Vault with 40 TB disk space to 10,000, given the same average data characteristics.

Data Vault type	Windows File Share DV	Web DV
Hardware	3 GHz dual core, 4 GB RAM	3 GHz quad core, 4 GB RAM
Supported DV total size	40 TB	40 TB
Policy settings	default	default
DV disk space per Agent	4 GB	4 GB
Supported Agents per DV	10.000	10.000

Note: The figures in the table are for default policy settings for an Agent with the following data characteristics:

- Average number of protected files: 5000
- Average total size of protected files on local disk: 10 GB

How to influence the total size of handled files

The example above are based on default policy settings. Changing these settings will influence the sizing of a Data Vault.

Does a change in the retention criteria for the protected files affect Data Vault sizing?

- Yes, changing the default retention time parameters will change the sizing of a Data Vault.
- A longer retention time and more file versions to be kept will increase the *Total size of handled files*.
 - A shorter retention time and fewer file versions to be kept will decrease the *Total size of handled files*.

Does adding new files to the list of protected files affect Data Vault sizing?

Yes, adding more files to the list of protected files will increase the *total size of handled files* on Data Vault disk.

Does the frequency of change of protected files affect the Data Vault sizing?

Only if a retention criterion is based on the number of days a version should be kept, when user behavior will influence the *total size of handled files* on Data Vault disk.

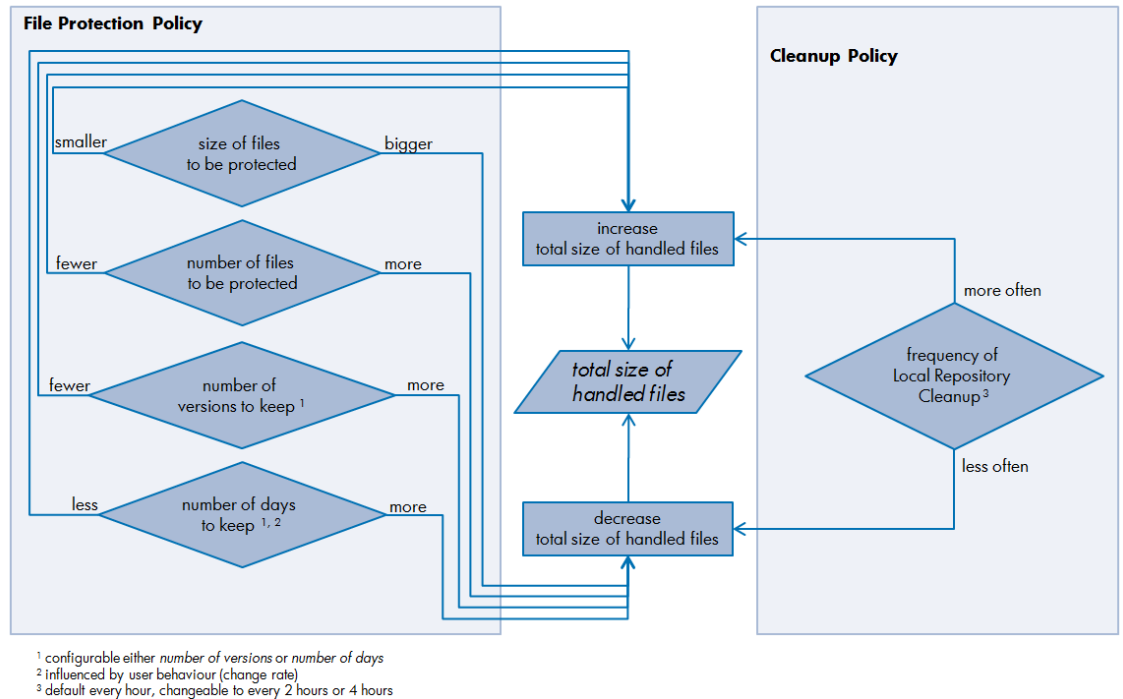
Does the number and size of files covered by configured protection policies influence the Data Vault sizing?

Yes, the number and size of files will influence the *total size of handled files*, which will influence the Cleanup run time.

Does the frequency of Local Repository Cleanup influence the Data Vault sizing?

Yes, changing the frequency of Local Repository Cleanup will influence the Data Vault sizing. The Local Repository Cleanup creates the version for files protected with OFF.

Figure 5: What influences the *total size of handled files*?



User data retention settings

There are two different ways of defining how many versions of files are kept: by time range or by number of versions. Which you should pick depends on how your users usually work.

For example if your users frequently switch between tasks, they usually also work on different sets of files. For such users, retention by date might be a good choice. Their versions could be kept for 30 days, for instance. Versions older than that would be removed from the Data Vault (and Local Repository as well) but at least one version would always stay there even if it had been created more than 30 days ago.

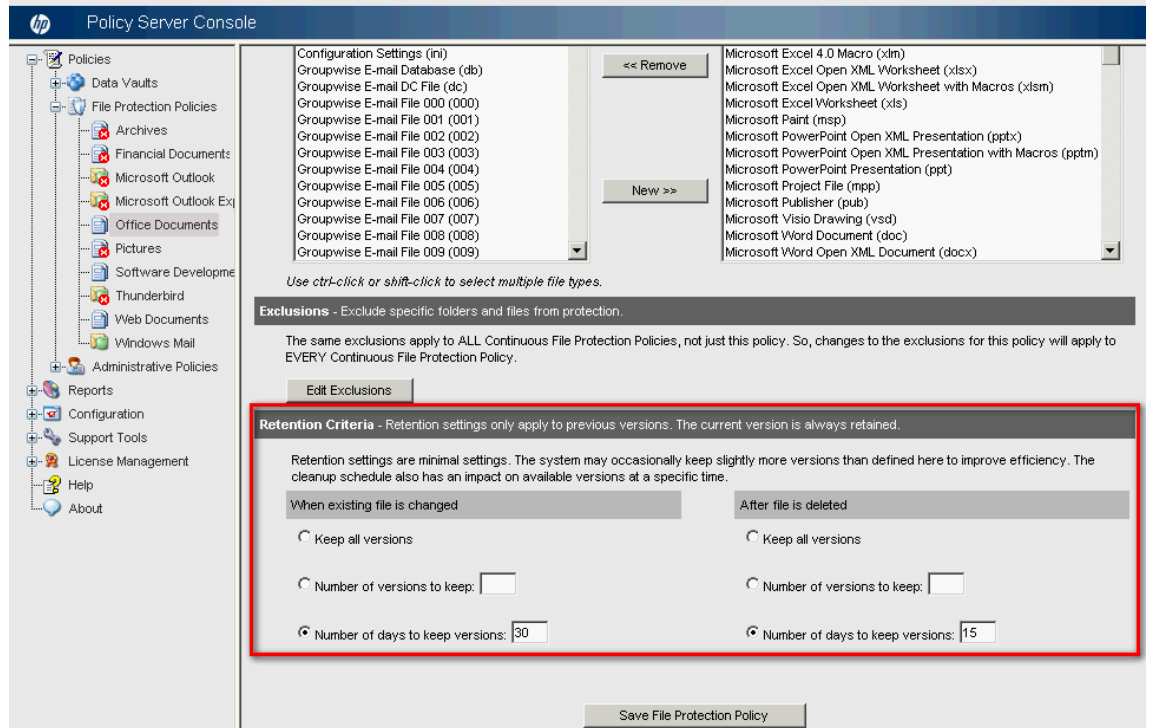
In this mode, the number of versions kept for each file tends towards 1 over time.

On the other hand if your users tend to resume work on older documents again after a period of time, they may prefer certain number of versions to be kept, for example, the last 20 versions. Then, even after interrupting work on a document for more than a month they can still review and restore older versions. In this mode, the number of versions for a file stays constant after reaching the maximum. This second mode tends to increase storage requirements slightly, but these extra versions are mostly only compressed deltas.

As far as Cleanup is concerned, keeping a certain number of versions rather than for a fixed time makes Cleanup quicker. If you are already at the limit regarding the time the cleanup process needs at nights and if changing the mode is acceptable to your user base you should switch to keeping a number of versions mode and observe the cleanup runtime changes after that. This will give you an idea how many more users you can add to the environment.

To change the retention criteria, open the File Protection Policy and change settings in **Retention Criteria** section:

Figure 6: Retention criteria



Back up only needed files

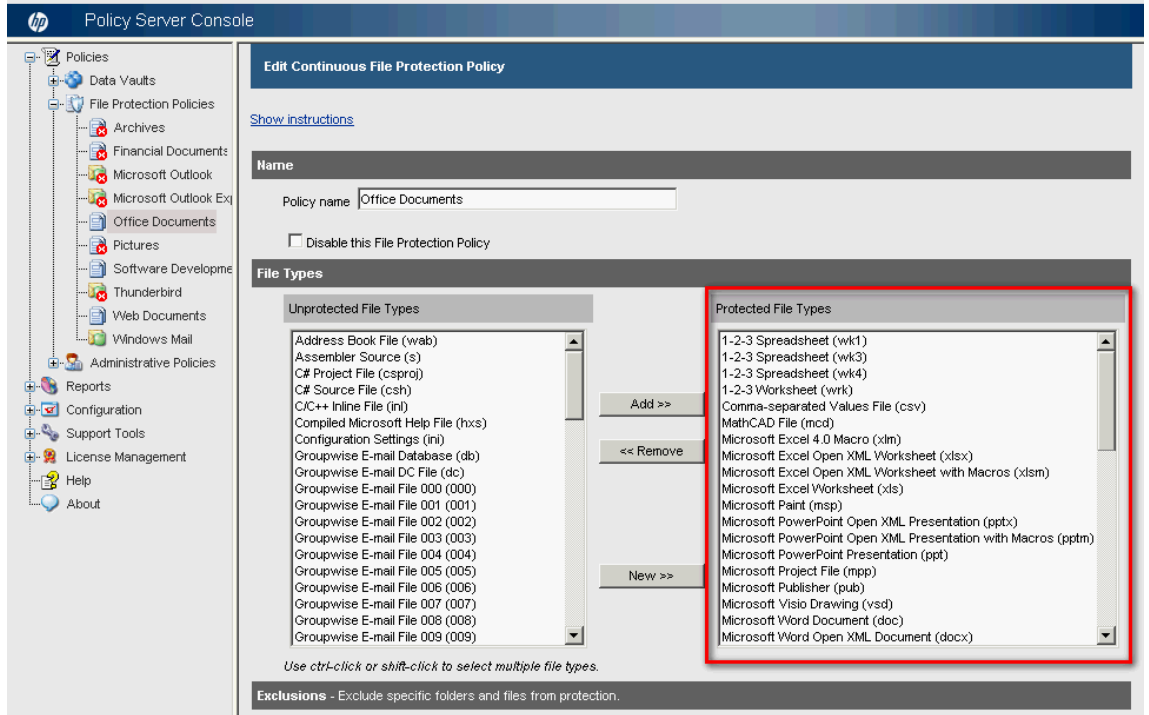
Be sure to back up only needed files. HP Data Protector for PCs is delivered with a default set of policies. These policies fulfil the need of most environments, but not all.

Protected file types

Check the file protection policies in the Policy Server Console to be sure you are only backing up files you want to be backed up.

Open the Policy Server Console, select **Policies > File Protection Policies** and check your enabled policies for unwanted files.

Figure 7: Protected files types



Edit exclusions

In addition, you may alter the exclusion settings and add more. In the File Protection Policy, click **Edit Exclusions**. In next screen, you have the option of adding an exclusion rule.

Figure 8: Edit exclusions

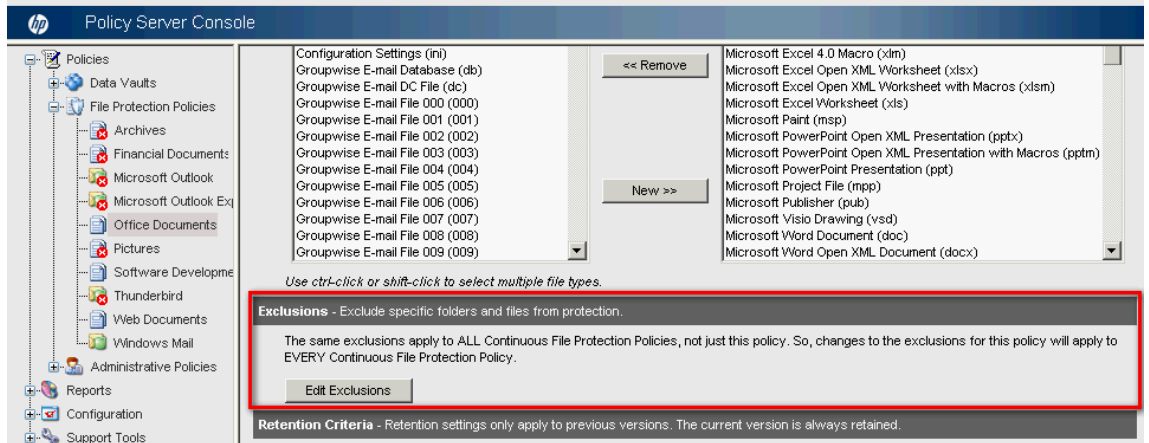
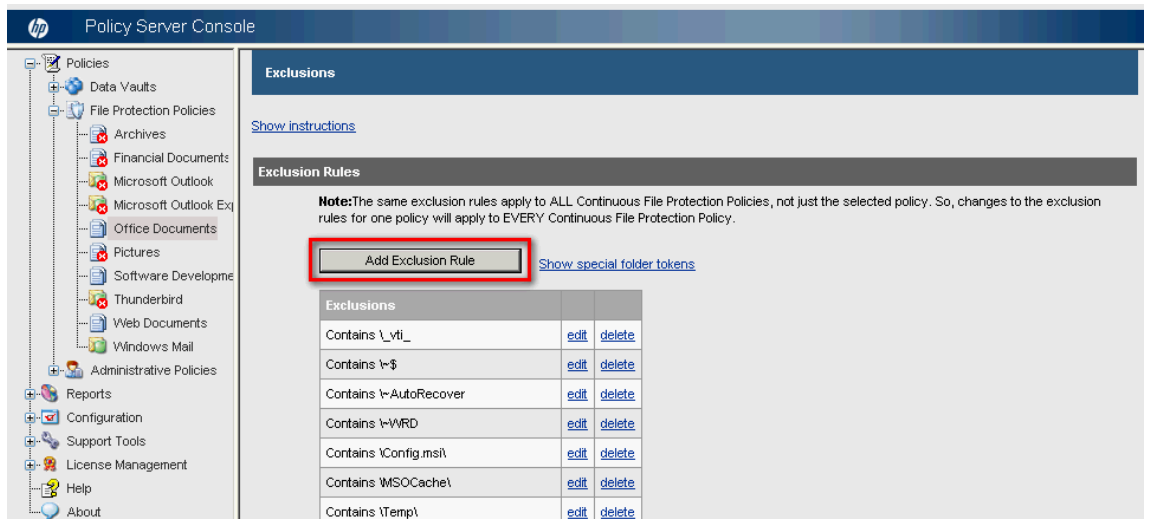


Figure 9: Add exclusion rule



Follow the instructions on the window.

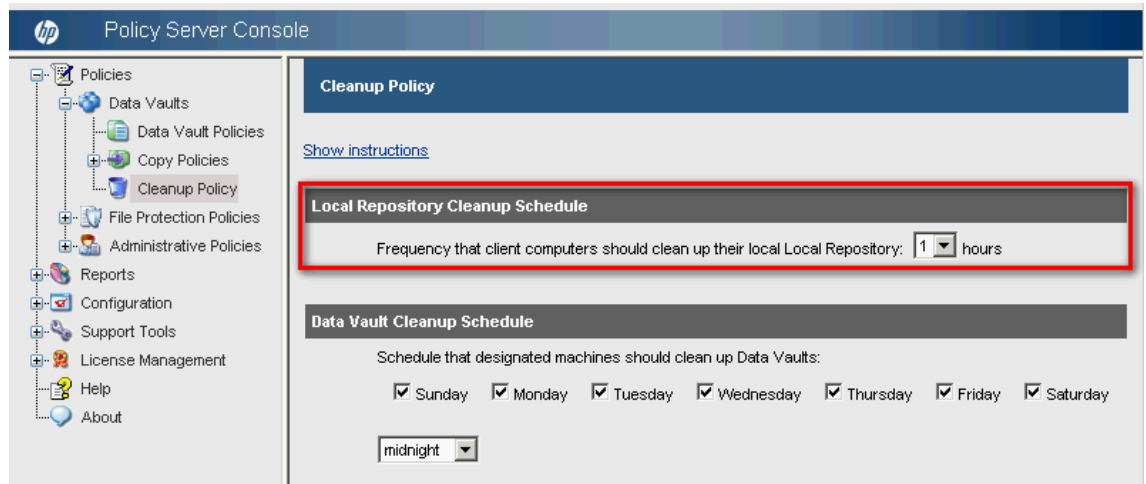
Tip: Add a central exclusion that end-users can use to store files that should not be backed up. This could be very helpful if you are working with quotas (see [Working with quotas](#)) and end-users are exceeding the quota settings.

Note: The same exclusion rules apply to *all* Continuous File Protection policies, not just the selected policy. So, changes to the exclusion rules for one policy will apply to every Continuous File Protection policy.

Local Repository Cleanup policy settings

The Data Protector for PCs Local Repositories on user computers need to be cleaned up periodically to remove versions that are older than the retention settings defined in the file protection policies and to create OFF versions. In order to change the settings, choose **Policies** in the left navigation pane and click **Set the Cleanup Policy**.

Figure 10: Cleanup Policy



Follow the instructions on the window.

Recommendation: Leave the frequency at the default of 1 hour. Changing it to 2 hours or 4 hours will save a small amount on Data Vault disk space but you will lose the ability of having a restore point of every hour.

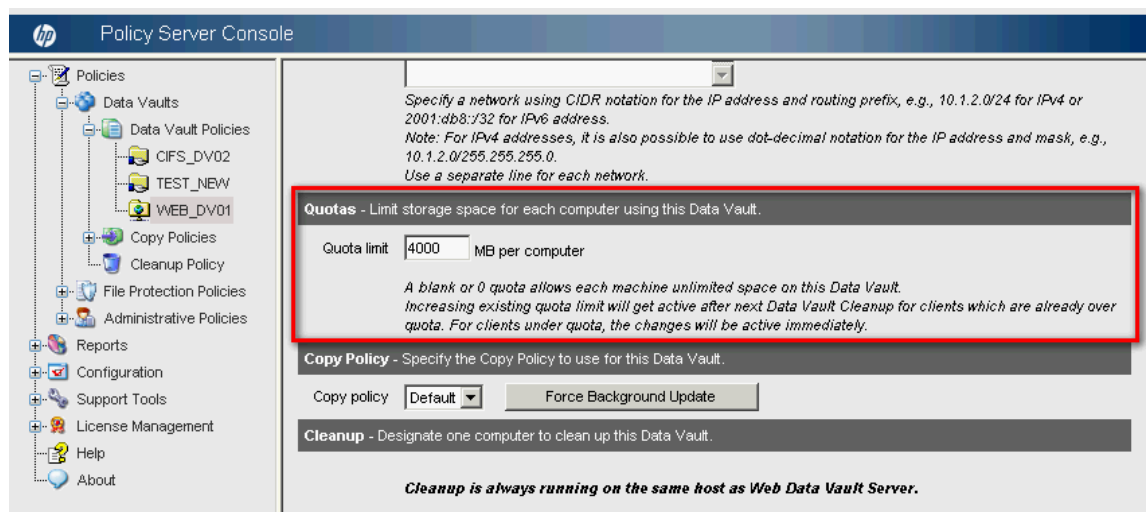
Working with quotas

Quotas help you to limit the amount of data per Agent and make sure that the Data Vault does not exceed its limits.

For the examples above, a quota limit of 4 GB would be helpful.

To set the quota, choose **Policies** in left navigation pane of the Policy Server Console, and select **Data Vaults > Data Vaults Policies**. Open the Data Vault Policy and set the quota.

Figure 11: Quota settings



Tip: Start with quotas from the beginning. This makes sure that Data Vault will not be filled up.

When working with quotas, it is recommended to offer end-users a directory that will not be backed up. End-users may also add their own exclusions (in the Agent Help, see the topic “How to Set Up Exclusion Rules”).

Tip: To monitor how much of the quota your end-users are using, run the Data Vault detail report. It shows what percentage of the quota is used. To make it easy to spot which end-users (Agents) are near their quota limit, the total used disk space is shown in blue if it is above 80% of quota, and in red if the total used disk space is above 90% of quota.

Figure 12: Data Vault detail report – quota usage colored

<i>Computer</i>	<i>Path</i>	<i>CFP Files</i>	<i>CFP Files With Versions</i>	<i>CFP File Space</i>	<i>CFP Version Space</i>	<i>OFF Files</i>	<i>OFF Files With Versions</i>	<i>OFF File Space</i>	<i>OFF Version Space</i>
002	\\backup\9FE346E0327F59BFD10F656A7067328B	593	50	178.2 MB (5.94%)	50.5 MB (1.66%)	13	3	252.3 MB (8.41%)	32.4 MB (1.08%)
006	\\backup\1BED401953D91C2EE5A51A07D4000B75	851	18	37.8 MB (1.26%)	2.4 MB (0.08%)	15	3	424.8 MB (14.16%)	28.2 MB (0.94%)
055	\\backup\BCD04C129BDB188BF6A372E511CE4333	2,624	7	584.3 MB (19.48%)	44.0 KB (0.00%)	0	0	0.0 KB (0.00%)	0.0 KB (0.00%)
218	\\backup\3613E0E6761F230C5825494AC3BFADB	14,869	168	2.4 GB (81.07%)	13.7 MB (0.46%)	2	2	1.9 MB (0.06%)	32.0 KB (0.00%)
292	\\backup\FB2A00AF52B3333CD757D03925080F2A	2,688	0	80.0 MB (2.67%)	0.0 KB (0.00%)	11	0	6.6 MB (0.22%)	0.0 KB (0.00%)
382	\\backup\CFCE0D169E77DBB12CFC5FDB66BF54F	2,036	14	887.5 MB (29.58%)	2.1 MB (0.07%)	226	5	1.9 GB (63.66%)	32.0 KB (0.00%)

Policy Server sizing

The amount of traffic generated on the Policy Server depends directly on the number of Agents hosted by the server. Using the Express edition of Microsoft SQL Server included with Data Protector for PCs imposes a maximum database size of 4 GB, and (using the default setting for “reporting data retention” on the Policy Server of 30 days) no more than 5,000 Agents can be supported.

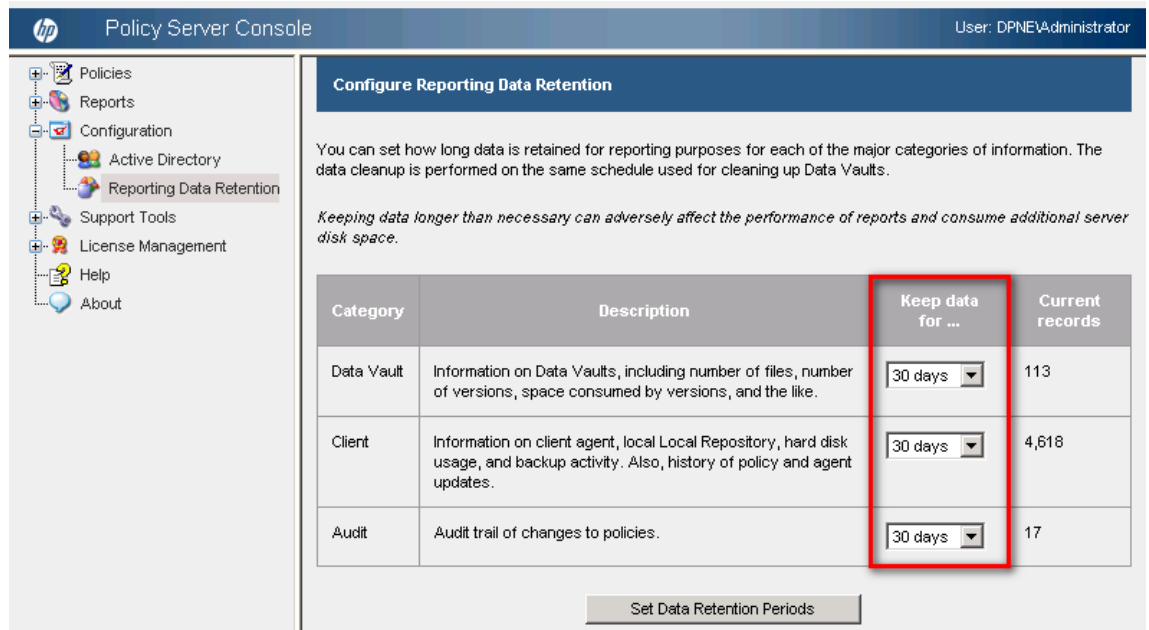
If you need to support more than 5,000 Agents in your environment, you can either have additional Policy Servers or replace MS SQL Express with a full version of Microsoft SQL Server. In this way, the Policy Server can easily scale up to 50,000 Agents. If you decide to use the full version of Microsoft SQL Server, consider upgrading the Policy Server’s main memory to at least 3 GB. For performance reasons, the Policy Server should run on a separate server from the Data Vault Server. It is possible to run them on the same server, but this is only advisable for evaluation purposes.

There must be at least one Policy Server, but it is not necessary to have matching number of Data Vaults and Policy Servers.

Reporting data retention

The reporting data retention affects the number of Agents a Policy Server can support. You can change the reporting data retention settings in the Policy Server Console. To do this, select **Configuration > Reporting Data Retention**.

Figure 13: Configure reporting data retention



You can choose between the following retention settings:

30 days, 60 days, 90 days, 6 months, 1 year, forever

Note: If you change the number of days from the default settings, you need to adapt the number of supported Agents on SQL Server Express. For example, if you double the number of retention time from 30 days (default) to 60 days, you need to halve the number of supported Agents on SQL Server Express.

Network considerations

Note: Web Data Vaults are not affected by high latency. The following applies only to Windows file share Data Vaults.

In general on Windows file share Data Vaults, HP does not recommend performing an initial update from Data Protector for PCs Agents to Data Vaults if the network latency between the two is higher than 50 ms. This usually applies to home offices or remote offices on a slow WAN connection. The initial update will work but it will take a very long time.

If your environment includes offices at several sites and the network latency for some of them is greater than 50 ms, consider installing Data Vaults at more than one site so that all offices can reach at least one Data Vault with a latency of 50 ms or less.

Once the initial update is complete, updates can be performed from any location on your corporate network or even from a home office. They are usually small enough to work well even over slow network connections.

If the initial update has to be performed via a high-latency connection, it may take several days to complete, but it can be interrupted without harm. Data Protector for PCs will continue the update at the point at which it stopped as soon as it reconnects to the Data Vault.

Tip: If you do not know what the latency between your offices is, use the `ping` command from a computer at one site to ping a computer at another site. Each successful ping will report the latency.

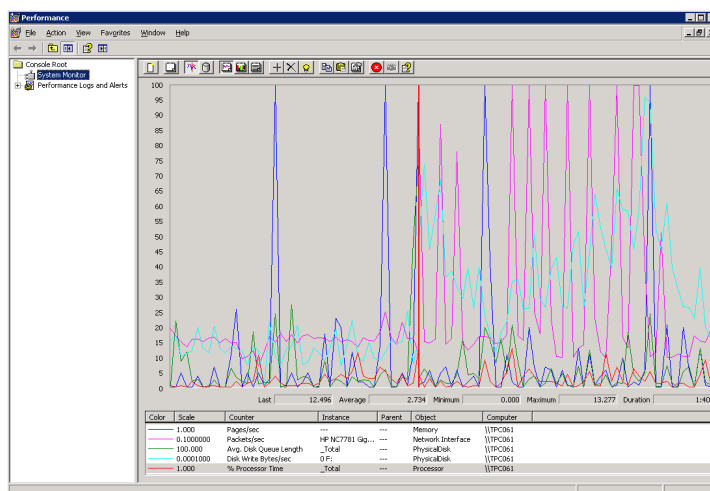
Monitoring the Data Vault Server and Cleanup

After deploying Data Protector for PCs Agents it is highly recommended to monitor the environment and check if the Data Vault and especially the Cleanup is able to handle the connected Agents.

Perfmon

In order to monitor the Data Vault Server you can use Microsoft's Performance Monitor (`perfmon.exe` — <http://technet.microsoft.com/en-us/library/bb490957.aspx>).

Figure 14: PerfMon



Checking Cleanup times

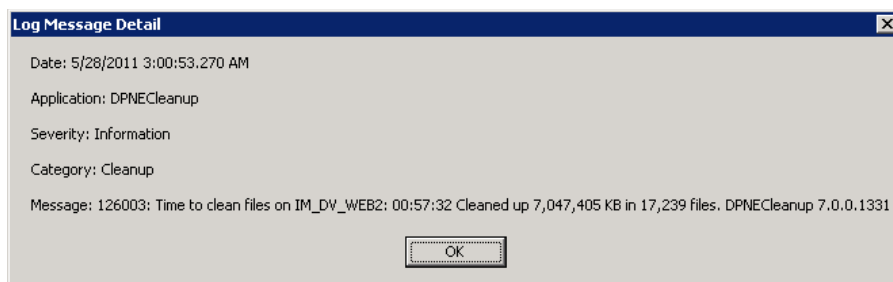
It is important to ensure that Cleanup does not run during business hours. This can be adjusted by changing the Cleanup start time (see [Data Vault Cleanup start time](#)).

To check the Cleanup time, open the Data Vault Server Cleanup Agent log:

1. On the Data Vault Server go to **Start > All Programs > Hewlett-Packard > HP Data Protector for PCs > Control Panel**.
2. In the Control Panel, choose **Health > Log > View Log Detail** and look for the message:

```
126003: Time to clean files on <DataVaultName>: hh:mm:ss Cleaned up *  
kB in * files.
```

Figure 15: Cleanup duration



Note: When running a daily Cleanup, the Cleanup should be finished before normal business hours start. You may need to change the default Cleanup start time settings (midnight) to achieve this (see [Data Vault Cleanup start time](#)).

Best practices

This section provides some additional best practices for Data Protector for PCs administrators and end-users. These tips are not directly connected to the sizing itself, but they are helpful when rolling out HP Data Protector for PCs.

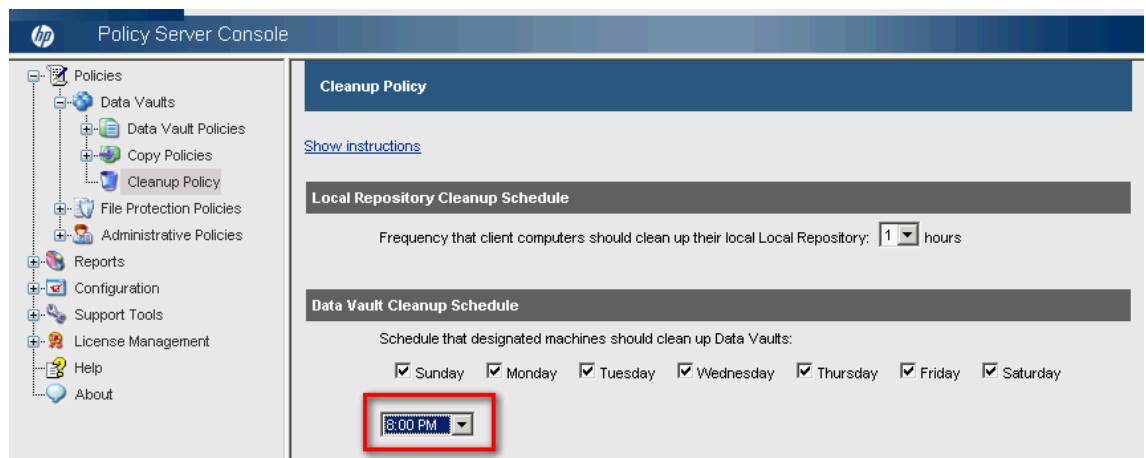
Administration

Data Vault Cleanup start time

If you need to change the default Cleanup start time (every day at midnight), go to **Policy Server Console > Policies > Data Vaults > Cleanup Policy**.

A use case for changing the Cleanup start time is if the Cleanup run time is expected to be longer than 8 hours and business hours start every day at 8 am.

Figure 16: Cleanup start time



In this case, you should set the Cleanup start time directly after business hours are finished (8 pm).

Throttling for initial update

Each Data Vault has an associated copy policy that includes a setting for the number of clients that are allowed to copy files concurrently. This restriction is called throttling and can be defined separately for office hours and non-office hours.

When setting up a new Data Vault and adding users to it, start with the default throttling settings and measure the resource usage (network, CPU, memory) on the server to determine whether there is room for increasing the numbers.

While this setting protects the Data Vault server from being overloaded, consider rolling out Data Protector for PCs to users in groups that are small multiples of the throttling setting. All the users that install Data Protector for PCs within a certain timeframe will immediately start an initial update (unless you switch this off). If there are more users than the throttling setting specifies, they will compete for the specified number of slots and each copy process will take longer. Note that the slots are only assigned to Agents on an hourly basis—once an Agent has used up this time it will have to queue again to get a new slot).

Switching off initial update

Note: Web Data Vaults are not affected by high latency. The following applies only to Windows file share Data Vaults.

If you expect many users to install Data Protector for PCs while being connected remotely (low network bandwidth, high latency), you may choose to deactivate initial copies. This way users will benefit from version management and backup for all protected files that they actually modify but will not have full backup sets of all protected files until they go to a location with a better connection and perform a manual copy.

End-user

Location for the initial update

Note: Web Data Vaults are not affected by high latency. The following applies only to Windows file share Data Vaults.

Initial copies are usually started directly after installation. Therefore the client machine should be connected to the Data Vault server via a high bandwidth/low latency network while doing the initial update. The status of the copy is visible in the Health pane of the Control Panel. The message `Update finished` appears when the initial update is complete.

Timing the start of the initial update

If there are active OFP settings on the Policy Server, the Data Protector for PCs Agent will immediately ask for a reboot of the system.

After this reboot, and if running on a system with many files, the Agent should be given enough time to build up the file list for the initial update before a reboot or shutdown can occur again (when the list is complete, the message `Update started` appears in the Control Panel health pane).

If the Agent is interrupted before it has compiled this list, it will have to start over again and this may take quite some time on systems with many files.

After the list is complete, interrupting the initial update is not an issue any more. The update will simply continue copying files to the vault at the point where it was interrupted.

Manual copy as a workaround

In some rare cases the initial update may still run into issues or be perceived to run too slowly. As a workaround, the user may want to invoke a manual copy instead. This differs from an initial update in two ways:

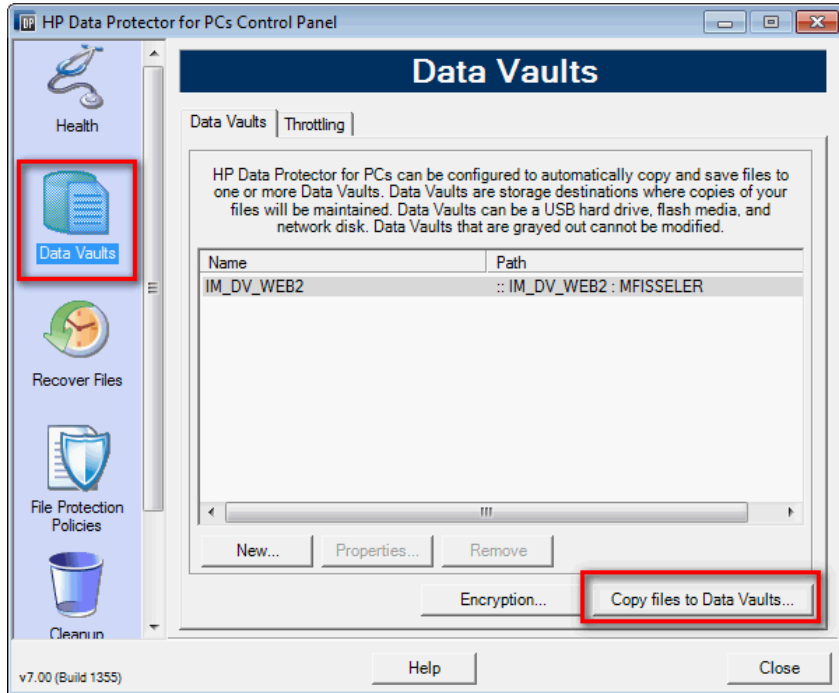
While the initial update runs in the background and takes care not to disturb the user's current task, a manual copy does not check for user activity and consumes more resources in order to finish faster.

All initial updates running against a certain Data Vault compete for a limited and configurable set of slots so that you can control how many copy operations can run in parallel. Manual copies are not limited in this way.

To start a manual copy:

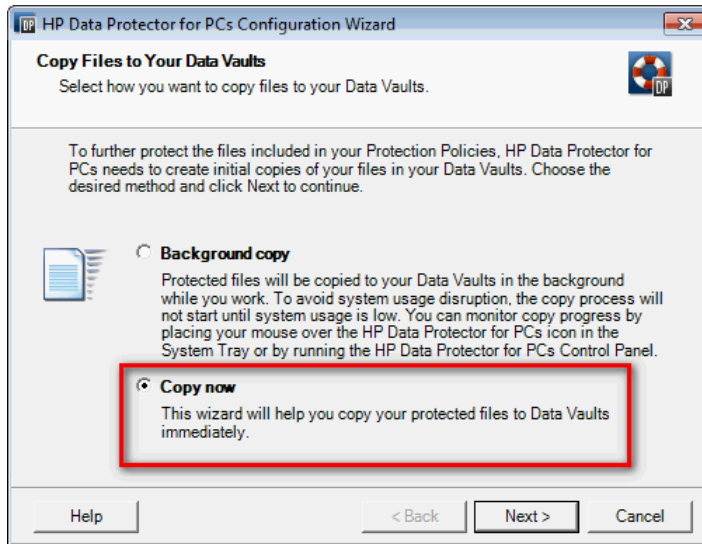
1. Open the Agent Control Panel.
2. In the Data Vault context, select **Copy files to Data Vault**. For more details, see the Agent Help.

Figure 17: Manual copy – Copy files to Data Vaults...



3. Follow the wizard.

Figure 18: Manual copy – Copy now



Note: Users should be cautioned not to use manual copies unless the initial update does not work, and they should consult the administrator/support before doing so.

Bandwidth throttling

You may want to implement data throttling in the following circumstances:

- If the Agent has too low a bandwidth connection, so that it can become completely saturated by the Data Protector for PCs data stream.
- If you do not want HP Data Protector for PCs processes to impact the performance of the internet connection significantly.

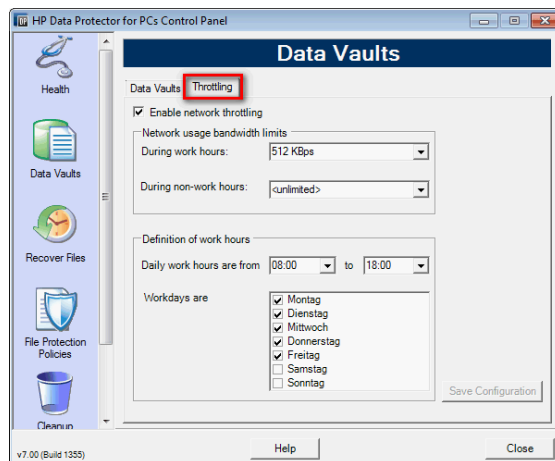
To enable throttling:

1. Run the Data Protector for PCs Control Panel, and click the Data Vaults icon.
2. Select the Throttling tab.
3. Check the **Enable network throttling** box and fill in the fields as you wish.

For the bandwidth limits, you can select from 16, 32, 64, 128, 256, 512 KBps, 1, 2, 5, 10 MBps, or <unlimited>.

4. Click **Save Configuration**.

Figure 19: Configure bandwidth throttling



Note: Data throttling is not supported on Windows XP clients. It works only in a Windows domain environment, not in workgroups.

Summary

It is difficult to give general rules that will hold true in all environments. The examples above should provide a starting point. The given numbers are valid for the hardware described in the examples.

As sizing depends on many factors there is no general formula available for calculating sizing with a Data Vault. You should use the rules of thumb (see next section) and the sizing examples above, and adapt them to your actual environment.

Rules of thumb

Some rules of thumb that should help to size your Data Protector for PCs environment:

- Having faster disks installed on the Data Vault location brings the need for more CPUs/cores.
- More CPUs/cores will reduce the Cleanup run time. (Note that the reduction is not linear.)
- A Web Data Vault needs more CPUs/cores than a Windows file share Data Vault.
- More RAM does not significantly improve the Cleanup run time.


Before installing a Data Protector for PCs environment, size the environment on numbers of a standard Agent which will be deployed in your environment.

Install the Agents in phases and not all at the same time. Monitor the environment from on the start, especially the Cleanup time on a Data Vault. If needed, adapt the settings.

For more information

To read more about HP Data Protector for PCs, go to:

- General webpage: www.hp.com/go/dppc (or www.hp.com/go/dpne)
- Interactive digital hub site: www.hp.com/go/imhub/dpne



Get connected
www.hp.com/go/getconnected

Current HP driver, support, and security alerts delivered directly to your desktop

Become a fan on  »

Follow on  »

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Trademark acknowledgments, if needed.

4AA3-5290ENA, Created July 2011

