HP Data Protector for PCs 7.0 Installation and Administration Guide

HP Part Number: n/a
Published: June 2011
Edition: First

Contents

About this guide

This guide provides information about:

- Installing HP Data Protector for PCs
- Configuring HP Data Protector for PCs policies
- HP Data Protector for PCs Agent software on users' desktops and notebooks
- Determining how many Agents can be supported
- Getting support for Data Protector for PCs

Intended audience

This guide is intended for administrators wishing to install and configure HP Data Protector for PCs. It will be helpful to have some familiarity with:

- Windows administration

Document conventions and symbols

Convention	Element
Blue text: About this guide	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	website addresses
Bold text	• Keys that are pressed • Text typed into a GUI element, such as a box • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	Text emphasis
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic` text	• Code variables • Command variables
`Monospace, bold` text	Emphasized monospace text

ⓘ **IMPORTANT:** Provides clarifying information or specific instructions.

NOTE: Provides additional information.

General Information

General information about Data Protector for PCs can be found at http://www.hp.com/go/dataprotector.

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/e-updates

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware upgrades, and other product resources.

HP websites

For additional information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/dataprotector
- https://h20230.www2.hp.com/selfsolve/manuals
- http://www.hp.com/support/manuals
- http://www.hp.com/support/downloads

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to **DP.DocFeedback@hp.com**. All submissions become the property of HP.

1 Overview and prerequisites

Overview of Data Protector for PCs

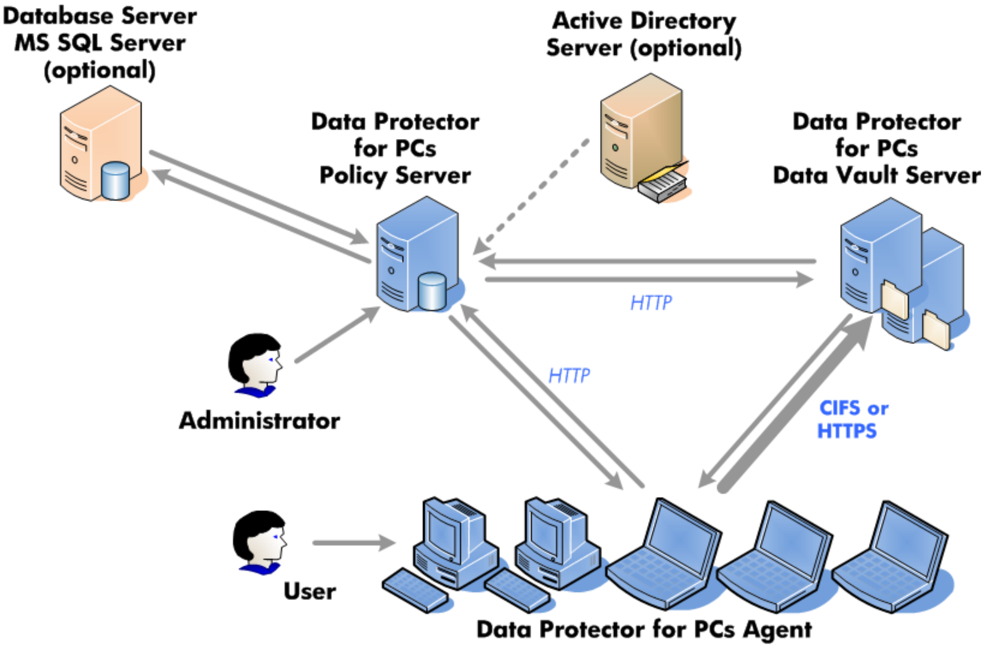
HP Data Protector for PCs consists of two major software components, the Policy Server and the Agents. The Policy Server runs on a Windows server—see the Support Matrix for supported versions (https://h20230.www2.hp.com/selfsolve/manuals). Agents run in the background on each desktop or laptop.

The Policy Server can also access groups and organizational units contained in an Active Directory server.

Users' data is backed up to Data Vaults. The Data Vault Server should be separate from the Policy Server. If you are using Windows file share Data Vaults instead of the recommended Web Data Vaults, they are situated on one or more Windows file shares on file servers.

The Data Protector for PCs architecture is illustrated in the following diagram:

Figure 1 Data Protector for PCs architecture



Various policies control what files are backed up from desktops and laptops and where these backups are kept. You define these through the Policy Server Console. The policies are then automatically distributed to the Agents, using the SOAP protocol over HTTP port 80. The policies are held on the Policy Server.

The Agents execute these policies. When a user changes a data file protected according to the policies, a previous version is created on the local hard disk of the desktop/laptop and changes to the file are compressed and copied to all applicable Data Vaults.

Whenever files are backed up, the Agent notifies the Policy Server, which contains an audit history of file changes made by users. Additionally, each Agent periodically sends “health” information to the Policy Server. You can generate reports of this data through the Policy Server Console.

Data Vaults are held on the Data Vault Server. Client data is copied to the Data Vaults using two different protocols: CIFS (for Windows file share Data Vaults) or HTTP (for Web Data Vaults).

The Data Vault Server should be on a separate system from the Policy Server. For HTTPS, the Web Data Vault Server software runs on it, together with Data Protector for PCs Cleanup software. For Windows file share Data Vaults, only the Cleanup software is installed on it.

If you use Active Directory, you can configure the Policy Server to access your groups and organizational units. You can then assign Data Vaults to users based on their group or organizational unit membership. You can also select users in reports based on their membership.

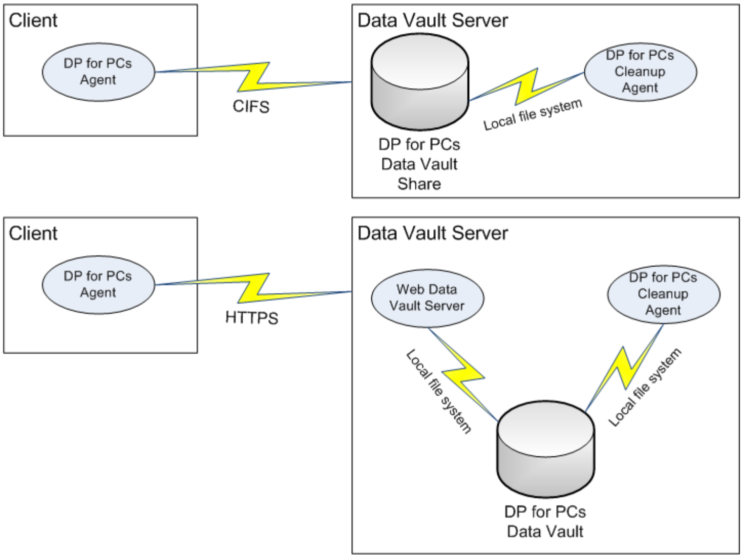
Data Vaults

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

Figure 2 Comparison of Windows file share and Web Data Vaults



Certificate handling

Use of SSL is mandatory for Web Data Vaults. The type of certificate is determined during the installation of Web Data Vault. In order to provide a product that can work right out-of-the-box, for example, for evaluation purposes, you can install the Web Data Vault Server with a self-signed certificate. This is not as secure as a certificate issued by trusted authority (CA) For full security, you should import a certificate for the Data Vault Server signed by an authority trusted within your environment and add it to the server component.

Self-signed certificates

When creating a Data Vault Policy, you can define whether a self-signed certificate is allowed. No action is necessary on the Agent side in this case. A self-signed certificate issued by installation is limited to 20 years.

Imported certificates

The import procedure expects a single file in PEM format containing both the private key and the matching certificate including the public key. Note that the file is copied to the Web Data Vault server configuration directory as is. Depending on the procedure used for creating the certificate file, it may be encrypted. In that case, the Windows service process running the Web Data Vault server will issue an interactive prompt to get the decryption password. This will happen during installation and also each time the service is restarted in the future, for example, after a system reboot. While it is possible for you to add this password manually to the Web server configuration file to avoid the prompt, the installation process does not support this. It is not advisable to have an encrypted certificate file and store the password in a file next to it.

NOTE:
The term “trusted authority” implies that the client machines running the Agents will consider this CA trustworthy and accept certificates signed by it. It is assumed that the Windows Certificate Stores of the client machines have already been set up appropriately by adding the certificate of the CA and possibly further certificates in their chains. The Agent does not include any mechanism for establishing this trust. It relies on Windows mechanisms.

Exchanging the certificate

You can exchange the certificate on the Web Data Vault Server at any time after installation by using the `DvConfig` utility described in the CLI paragraph “Configuring Web Data Vault options from the CLI (DvConfig)” (page 21). So for instance, you can reconfigure an installation initially set up with a self-signed certificate to use an imported certificate.

Overview of installing Data Protector for PCs

NOTE: If you are updating an installation of Data Protector for PCs, see “Updating Data Protector for PCs” (page 40).

There are four stages to installing Data Protector for PCs:

1. **Install the Data Protector for PCs Policy Server.**

   See “Installing the Data Protector for PCs Policy Server” (page 14).

2. **Install Data Protector for PCs Web Data Vault Server software.**

   See “Installing, configuring and maintaining the Web Data Vault Server” (page 18).

3. **Configure protection policies.**

   See “Configuring your Data Protector for PCs protection policies” (page 23).

4. **Install Data Protector for PCs Agents on laptops and desktops.**

   See “Installing Data Protector for PCs Agents” (page 36).

Prerequisites

Policy Server

For supported operating systems, see the Support Matrix.

NOTE: *Installation on Windows 2003 64-bit operating system:* The Policy Server runs in 32-bit compatibility mode on a 64-bit Windows operating system. This means that Internet Information Services (IIS) must be running in 32-bit mode. If it is not, the installation will detect this while checking the prerequisites. It will then give you the option of setting IIS into 32-bit mode. If there are other web applications on the server that require IIS to be in 64-bit mode (such as Microsoft Exchange 2007 with Web mail—Outlook Web Access), you will not be able to install the Policy Server on that server. This does not apply to installing a Policy Server on Windows 2008.

The server must have the following installed:

- Internet Information Services 6.0, 7.0, 7.5 or later with support for ASP.NET applications.

  For Windows 2003, IIS 6.0 is a prerequisite and must be installed before the Policy Server can be installed. For Windows 2008, Data Protector for PCs offers installation of IIS 7.0 and 7.5, if they are not installed.

- Microsoft ASP.NET 2.0

You also need the following installed on the server.

- Microsoft Installer 3.1 or later (required for .NET Framework 2.0 SP1)
- Microsoft .NET Framework 2.0 SP1 or later. The wizard will install version 2.0 SP1.
- Microsoft SQL Express (if no other SQL version is present)

Also, for Internet Information Services 7.0 and 7.5 only, the following IIS components are needed. If they are not installed, the wizard gives you the opportunity to install them:

- IIS Static Content Web Server—needed for serving static html files, documents, and images
- IIS ASP.NET—needed for deploying ASP.NET 2.0 and the .NET Framework
- IIS Security—needed for using the integrated Windows authentication used for the Policy Server console
- IIS 6 Management Compatibility— to allow the setup to configure IIS 6 and IIS 7 in the same way as far as possible

Database

Data Protector for PCs requires access to a Microsoft SQL Server database. See the Support Matrix for supported versions.

You can verify (and change) the authentication mode of your SQL Server installation using Microsoft Enterprise Manager:

1. Right-click on the SQL Server instance, choose **Properties**, and click the **Security** tab.

2. The **SQL Server and Windows** option (instead of the **Windows only** option) should already be selected. If not, select it and click **OK**.

Alternatively, during installation of Data Protector for PCs, you can install an instance of Microsoft's SQL Server Express Edition.

Data Protector for PCs Web Data Vault Server

- The Web Data Vault Server should be installed on a different system from the Policy Server. (It is possible to install it on the same system, but this is only suitable for evaluation purposes.)
- Java Runtime environment version 1.6 or later should be installed.
- The variables `JAVA_HOME` and `JRE_HOME` must point at the Java Runtime installation directory.

Data Protector for PCs Agents

Data Protector for PCs Agent software can be installed on users' desktops and notebooks running Windows. For supported platforms, see the Support Matrix.

2 Installing the Data Protector for PCs Policy Server

NOTE: You can update an existing Data Protector for PCs Policy Server installation to a newer version by following the standard installation procedure. See "Updating the Policy Server" (page 40) for more details.

Quick Installation

See "Policy Server" (page 11) for requirements for the Data Protector for PCs Policy Server.

1. Insert the Data Protector for PCs installation CD-ROM. If the installation wizard does not start automatically, run it manually by double-clicking `setup.hta` at the root of the installation CD-ROM.
2. Follow the instructions on-screen.
3. The Data Protector for PCs Policy Server requires access to a Microsoft SQL Server database. Select **Use existing Data Protector for PCs instance of Microsoft SQL Server Express** or click **Use an existing instance of Microsoft SQL Server** . If you choose to use an existing SQL Server, you need to provide the database server connection string and credentials for an account with sufficient privileges to create a new database.
4. Click **Install** on the **Install Data Protector for PCs Policy Server** page of the wizard to begin the installation.
5. When the installation finishes, click **Next**. You can then choose to run the Data Protector for PCs Policy Server Console.
6. Install the Web Data Vault Server on a separate system. Click **Install Data Vault** on the main installation screen.

NOTE: During installation, the Cleanup software is always installed together with the Web Data Vault Server software. For a Data Vault Server that hosts only Windows file share Data Vaults, it is recommended to install it locally on Data Vault in order to optimize performance.

Detailed installation

NOTE:

Windows 2003 server only: You can only install the Data Protector for PCs Policy Server from a CD-ROM shared over the network or from a network file share if the .NET 2.0 Framework Runtime Security Policy for this server is set to *Full Trust* for the Local Intranet Security Zone. If your server does not have a local CD-ROM drive, change the Runtime Security Policy for the Local Intranet Security Zone to *Full Trust* using the .NET Framework 2.0 Configuration tool in Administrative Tools, or copy the Server folder from the CD to a local disk on the server.

You must be logged into an account with “administrator” privileges to perform the Data Protector for PCs Policy Server installation.

1. Insert the Data Protector for PCs installation CD-ROM. If the installation wizard does not start automatically, run it manually by double-clicking `setup.hta` at the root of the installation CD-ROM.
2. Click on **Install Policy Server**.

   If asked, choose to **Open** (or **Run**) this program from its current location instead of **Save this program to disk**.
3. The Data Protector for PCs Policy Server requires .NET Framework 2.0 SP1. If this is not already installed, you are asked if you want to install it from the CD-ROM.

   The installation requires Windows Installer 3.1 or later, so if necessary, you are asked if you want to install Windows Installer 3.1 from the CD.
4. The installation wizard checks that the other prerequisites are installed:

   - Internet Information Services (IIS)
   - ASP.NET 2.0

   If either is missing, click on that prerequisite in the list for details of how to install it.

   Click **Next**.
5. Install the Microsoft SQL Server.

   To use an existing instance of Microsoft SQL Server:

   a. Click **Use an existing instance of Microsoft SQL Server**.

   b. In the **Database server** field, enter the connection string to the existing database server.

c. In the **Login** and **Password** fields, enter credentials for an account with sufficient privilege to create a new database. Usually, this will be the "sa" account.

d. Click **Next**. The connection information you entered will be used to make a test connection to the existing database server. If the connection succeeds, the wizard proceeds to step 6.

To install the Data Protector for PCs instance of Microsoft's SQL Server Express Edition:

a. Select **Install DataProtectorNE instance of Microsoft SQL Server Express** and click **Next**.

b. Click **Install** to install an instance of Microsoft SQL Server 2005 Express Edition named "DataProtectorNE". Click **Next** when the installation completes.

6. Install the Data Protector for PCs Policy Server software

   a. On the Welcome screen, click **Next** to begin the installation.

      - The Data Protector for PCs Policy Server Console will be installed as a Web application in the virtual directory `C:\Inetpub\wwwroot\dpnepolicy`.
      - The Data Protector for PCs Web service will be installed in `C:\Inetpub\wwwroot\dpnepolicyservice`.

      Both use the HTTP protocol on port 80.

   b. Click **Close** and **Next** when the Policy Server installation completes.

7. You now need to install the Cleanup program. Click **Install** to begin the installation.

8. When the Cleanup installation finishes, click **Next**.

   You administer Data Protector for PCs centrally from the Data Protector for PCs Policy Server Console. Because the console is browser-based, you can manage Data Protector for PCs from any computer that can establish a browser connection to the Policy Server (using HTTP port 80).

   To run the Data Protector for PCs Policy Server Console from a browser on the Policy Server, leave the **Run Policy Server Console** checkbox set and click **Finish**.

NOTE: During installation, the Cleanup software is installed on the Policy Server. It is also recommended that you install it on the Data Vaults in order to optimize performance.

NOTE:

Browser settings for the Policy Server Console: If you have problems displaying the Policy Server Console pages in your browser, check the browser security settings. The Console requires the following:

- JavaScript must be enabled.
- The popup blocker must be disabled for the `dpnepolicy` web site.
- Other restrictive security settings may need to be modified depending on your particular browser and its version.

Installation with Microsoft SharePoint: When the Policy Server is installed on a server running Microsoft SharePoint, you may get a 404 error "The page cannot be found" when you run the Policy Server Console. The Microsoft knowledge base article at http://support.microsoft.com/kb/828810 describes the issue and the resolution. Note that this issue applies to all ASP.NET web applications, not just the Policy Server.

For the Policy Server to run on a server using SharePoint, you need to do the following:

1. Use the SharePoint administration tools to create exclusions for the two Policy Server web applications: `dpnepolicy` and `dpnepolicyservice`.
2. Modify the two Policy Server `web.config` files (`dpnepolicy\web.config` and `dpnepolicyservice\web.config`) to add the `<httpHandlers>` and `<trust>` XML code as described in the Microsoft knowledge base article referenced above.

3 Installing, configuring and maintaining the Web Data Vault Server

Installing and configuring the Web Data Vault Server

NOTE: Install the Web Data Vault Server on a different system from the Policy Server. (It is possible to install it on the same system, but this is only suitable for evaluation purposes.)

1. Insert the Data Protector for PCs installation CD-ROM. If the installation wizard does not start automatically, run it manually by double-clicking `setup.hta` at the root of the installation CD-ROM.
2. Click **Install Data Vault**.
3. Choose between:
   - **Web Data Vault Server** (recommended). This also installs Cleanup software on the server.
   - **Cleanup software for Windows File Share Data Vault**. Select this if you are intending to use only Windows file share Data Vaults.

   See “Data Vaults” (page 9) for more information.
4. Follow the instructions on screen to complete the installation stage.
5. After getting a license from the Policy Server, if you are installing a Web Data Vault Server, you start configuring the Web Data Vault.

   On the Server Settings screen, enter the fully qualified domain name (FQDN) and SSL port of the server. You will need to use the same FQDN when configuring the Web Data Vault Policy on the Policy Server. The name must be resolvable by all client systems, otherwise it will not be possible to back up some of them to Data Vaults on this server.
6. On the Certificate Settings screen, you need to choose between:
   - Importing an existing SSL certificate issued by a trusted authority (CA). This is the recommended option, and provides the highest level of security.
   - Creating a self-signed SSL certificate. This provides a lower level of security and should only be used for evaluation purposes.

NOTE: You can exchange the certificate on the Web Data Vault Server at any time after installation by using the `DvConfig` utility. This includes reconfiguring an installation with a self-signed certificate to use an imported certificate. See "Configuring Web Data Vault options from the CLI (DvConfig)" (page 21).

7. The next screen asks you to provide names for two types of user of the Web Data Vault Server:

   - **Administrative user**—who looks after administrative tasks like creating and deleting Data Vaults and migrating client backup data.
   - **Backup user**—who performs end-user operations like the backup and restore of files.

   These users are specific to Data Protector for PCs Web Data Vault Server. You will need to enter details of both when creating or editing Web Data Vaults for this server.

   NOTE: Passwords must be at least 8 characters long.

8. Click **Next** and then **Finish** to complete the installation and configuration of the Web Data Vault Server and installation of the Cleanup software.

Maintaining the Web Data Vaults

1. On the Data Vault Policy page, enter the Server's fully-qualified domain name and SSL Port, and the Backup User account credentials. Then click **Configure Data Vault**.
2. Submit the Administrative User account credentials, and the Maintain Web Data Vault Server page is shown.

   Here you can select or delete existing Web Data Vaults. You can also add a new Data Vault.

   NOTE: You can only select an existing Data Vault is it not currently connected to another Data Vault Policy.

3. Make sure you save the Data Vault Policy by clicking **Save** at the bottom of the page.
4. If you have added a new Data Vault, you can optionally test the existence and proper configuration of the vault.

Migrating data from a Windows file share Data Vault to a Web Data Vault

The layout of data in a Data Vault remains the same for both Windows file share Data Vaults and HTTPS Web Data Vault. This means you can migrate data from existing DPNE 6.x Data Vaults to new Web Data Vaults.

NOTE: Data migration can be performed only for Data Vaults which belong to the same Policy Server or share the same encryption password.

There are two possible scenarios for data migration:

- Use the same system to host the Web Data Vault.

  NOTE: Accessing the same directory in parallel via a Windows file share and a Web Data Vault is not supported.

- Move the whole Data Vault to another system.

In both cases the Web Data Vault Server must be installed locally on the system on which the data should reside.

To migrate data from an existing Windows file share Data Vault to a Web Data Vault:

NOTE:

- Perform the migration in non-working hours to minimize the effect on running backups.
- Look in the Windows Task Manager to make sure `DPNECleanup.exe` is not currently running.
- Check the Cleanup Policy on the Policy Server to make sure that `DPNECleanup.exe` is not scheduled to run during the migration period.

1. Install Web Data Vault Server and update the Policy Server and Agents to version 7.0. Ensure that all Agents have performed a reboot after the installation of 7.0 as only then can they start backing up data to the Web Data Vault.
2. Disable the appropriate Windows file share policy on the Data Vault Policy Page, so that the Agents stop copying data to the Data Vault.
3. If you are going to use the same directory for the Web Data Vault, stop sharing the directory via CIFS.
4. If the Web Data Vault is on a different server from the Windows file share Data Vault, the data must be copied to that machine to a folder path that does not exceed 67 characters. If the Data Vault resides on the same server, there is no need to copy data to new location unless this is done intentionally for other reasons.
5. Before creating the new Web Data Vault, decide on the behavior of the initial update process. The initial update can be skipped if all Agents have performed an initial update, so that the backup data is already complete on the existing Data Vault. The option for skipping of initial update is not directly part of a Data Vault Policy but of the referenced Copy Policy. Make sure that a Data Vault Policy with the proper option selection exists (that is, with “initial update” turned off and appropriate throttling and schedule settings). Create a new Copy Policy for this, or modify an existing policy (in which case all Data Vault Policies that reference that Copy Policy will be affected).

6. Create and save the new Data Vault Policy for the Web Data Vault. When you create a new Web Data Vault, you have to supply the folder path, and in this case, it will be the path where the actual data of the Windows file share Data Vault that you are migrating resides. Select the Copy Policy that you created in step 5. Set the other options for the Data Vault Policy in the same way as they were in the original Windows file share Data Vault policy (such as network settings, Active Directory settings).
7. When you are sure that the Agents are backing up files to the new Web Data Vault successfully, delete the original Windows file share Data Vault Policy.

After you have saved the policy, Agents will resume copying their data to the new Web Data Vault using the HTTPS protocol.

Configuring Web Data Vault options from the CLI (DvConfig)

Using this utility from the CLI enables you to change configuration parameters of a Web Data Vault like the Backup and Administrative users and their passwords, import a new certificate, change SSL, and create a new self-signed certificate.

Before you change any of parameters, you must stop the Web Data Vault Server by stopping the Windows service HP Data Protector for PCs Data Vault Server.

After you have made the changes, restart the Web Data Vault service. Any updated policies will be redistributed to Agents.

NOTE: If you use `DvConfig` to change the SSL port or Backup User name or password on the Web Data Vault server, make sure you change the corresponding Data Vault Policies on the Policy Server to match.

Usage:

```
DvConfig [-adminUser login:password -backupUser login:password]
 [-h] [-i certfile | -s hostname] [-p port] [-v]
```

`-adminUser` *`login`*`:`*`password`*

Set the credentials for the DvAdmin account. If no login or password is given, the default “DvAdmin” is used.

`-backupUser` *`login`*`:`*`password`*

Set the credentials for the DvBackup account. If no login or password is given, the default “DvBackup” is used.

`-h`

Print this message.

-i *`certfile`*

Import an existing certificate.

`-p` *`port`*

Set the SSL port.

`-s` *`hostname`*

Create a self-signed certificate for the fully-qualified domain name.

`-v`

Print the version information and exit.

4 Configuring your Data Protector for PCs protection policies

Initial Setup after installing Data Protector for PCs

Immediately after installing Data Protector for PCs, you are presented with the Initial Setup window in the Policy Server Console. Before you can set up policies for Data Protector for PCs, you must successfully complete two configuration steps:

1. **Define or import an encryption password.**

   For security, you must define an encryption password before you can use Data Protector for PCs. This ensures that all files are encrypted at the user computer and transmitted encrypted over the network. The same password is used to encrypt the files from all users and for all centrally-configured Data Vaults.

   - A centrally-defined Data Vault (defined through the Policy Server Console) will always use encryption based on the Data Protector for PCs encryption password.
   - With locally-defined Data Vaults (defined by users through their computers), users can each choose whether to use encryption or not, and choose their own passwords.

   When you first install Data Protector for PCs, you must either **generate** or **import** a password before you can continue. After generating a password, for your safety, **export** the password. This saves it to a secured location. You can then use it later for importing.

   Click **Set the Encryption Policy** to manage the password, and follow the instructions on the window.

   NOTE: After generating or importing a password, you cannot change it.

2. **License Data Protector for PCs.**

   If you are evaluating Data Protector for PCs, you can use it for 60 days to protect an unlimited number of users without further licensing. When you purchase Data Protector for PCs, you need to go to the HP License Key Delivery Service at https://webware.hp.com/welcome.asp, to download a license key which you can then enter. You can purchase the following licenses:

   - TA032AA or TA032AAE for 100 Agents
   - TA033AA or TA033AAE for 1000 Agents
   - TA036AA or TA036AAE for 100 Agents plus HP Data Protector Starter Pack Windows (B6961BA or B6961BAE)

   You must enter a permanent license key before the end of the evaluation period. If not, at the end of the 60 days, Agents will no longer be able to copy data to their

Local Repositories or to Data Vaults. It will still be possible to restore previously protected file versions, however.

Click **License Management** to manage licensing, then **Enter a license key for Data Protector for PCs users**. Follow the instructions on the window.

NOTE: Licenses are distributed to Agents when the Agents are installed.

After successfully completing these configuration steps, the fully-working Policy Server Console is available to you. If you have just installed Data Protector for PCs, configure other elements of Data Protector for PCs in the order in the next section.

Configuring for the first time

Data Protector for PCs comes pre-configured with policies that are sufficient for most organizations. You are recommended to configure Data Vault, Copy and File Protection policies first and then install your Data Protector for PCs Agent software on users' desktops and notebooks.

NOTE: Instead of configuring new policies, you can modify the policies that come pre-configured with Data Protector for PCs. Simply select **Edit an existing policy** instead of **Create a new policy** at each stage.

You configure protection policies for your installation from the Policy Server Console. The policies you define centrally are distributed to all the Data Protector for PCs Agents and executed on the users' desktops and laptops.

1. Run the Data Protector for PCs Policy Server Console at the end of the installation wizard, or any time from a browser using the URL:

   `http://`*`policyserver`*`/dpnepolicy/`

   where "*`policyserver`*" is the name of your Data Protector for PCs Policy Server. You must be logged in as "administrator" on the server.

2. **Configure Data Vault policies**.

   Data Vault Policies set the destination (a Web Data Vault or a Windows file share) for the continuous backup of policy-protected user files. When a file is changed, the previous version and the edited file can be automatically backed up to one or more destinations. Each user group can be assigned one or more Data Vaults. For example, you may define a Data Vault policy named *Sales* and assign it to your user groups *Dallas.Sales*, *San Francisco.Sales*, *Chicago.Sales*, and *Atlanta.Sales*.

   - A centrally-defined Data Vault (defined through the Policy Server Console) will always use encryption based on the Data Protector for PCs encryption password.
   - With locally-defined Data Vaults (defined by users through their Agent software), users can each choose whether to use encryption or not, and choose their own passwords.

NOTE: *Requirement for all Data Vaults:*

Data Protector for PCs will set the access permissions (ACLs) on the files backed up to the file server the same as on the original file. This means that users can only recover backed-up files if they can access the original files on their computers.

Requirement for Windows file share Data Vaults:

If you are using standard Windows file share Data Vaults, the shares should be on a Windows file server, which does not need to be the same machine as the Policy Server. However, if you are only evaluating Data Protector for PCs with a small number of installed Agents, it may be useful to make the Policy Server and Data Vault file server the same machine.

To create a Data Vault policy:

a. Click **Policies > Data Vaults > Data Vault Policies** in the left navigation pane.

b. Click **Create a new Data Vault policy**.

c. Follow the instructions on the window. The process is different depending on whether you select a WEB-based or Windows File Share Data Vault type.

NOTE: When you create a Data Vault, the folder or share path length must not be greater than 66 characters.

Best practices:

Leave the Copy Policy set to "Default" for now.

For Cleanup with Windows file share Data Vaults:

- If the Data Vault is on this Policy Server, keep the default setting of this machine's name.
- If the Data Vault is on a different Windows file server, install the Data Vault Cleanup software on it and designate that machine as the cleanup machine.

3. **Configure Copy policies**.

The Copy policy sets a limit on the number of clients that can copy to a Data Vault concurrently. It also defines initial and scheduled Data Vault updates to supplement the continuous backup. Each Copy policy can be assigned to one or more Data Vaults.

Copy policies define the following:

- How many Agents can copy files concurrently to your Data Vaults.
- A schedule for periodic updates, which check that all the expected files for a user exist on the Data Vault and, if they do not, copy any missing files. This

provides further assurance that all user files have been properly copied to the Data Vault.

- If an **initial update** (or copy) should be performed. The initial update is needed because during regular Data Protector for PCs operation, each time a user changes a Data Protector for PCs continuously-protected file, only information about the changes is copied to the Data Vault.

The default Copy policy applies to all Data Vaults that do not have an explicit Copy policy set. You can change the settings for the default Copy policy, but not delete or rename it.

To create a Copy policy:

a. Click **Policies** in the left navigation pane.

b. Click **Set the Copy Policies**.

c. Click **Create a new copy policy**.

d. Follow the instructions on the window.

Best practice:

- **Throttling**: Set the time period to your normal working hours and set a lower throttling limit for other times.
- **Initial update**: Enable initial update to ensure that all user files protected by the File Protection policies are backed up.
- **Update files every week/month**: Since an update should involve few, if any, file copies, enable Data Vault updates to ensure all policy-protected user files are properly backed up.

4. **Configure File Protection policies**.

File Protection Policies allow you to specify which files are to be protected and how long previous versions are to be retained. For example, you may define a File Protection Policy named *Office documents* for Word documents, Excel spreadsheets, and PowerPoint presentations.

Files stored on local disk drives can be protected.

There are two types of policy:

- **Continuous File Protection**—which provides real-time protection for files any time they are saved to disk or deleted. Generally, any file or document that allows you to select **Save** from a menu should be protected with a Continuous File Protection policy.

  Data Protector for PCs includes various example policies. Three are selected by default after installation: *Office Documents*, *Software Development*, and *Web Documents*. You can start with these policies or build your own.

- **Open File Protection**—which provides protection of files by periodically taking a “snapshot” of the file (usually once an hour). Generally, any file that is very large (over 100 MB), open most of the day, or lacks a **Save** menu option should be protected with this method. Common files of this type are e-mail and database files.

Data Protector for PCs includes four examples: *Microsoft Outlook*, *Microsoft Outlook Express*, *Windows Mail*, and *Thunderbird*. You can start with these policies or build your own.

NOTE: Data Protector for PCs does not support the backup of EFS-encrypted files with Open File Protection policies, so files such as `.pst` must not be EFS-encrypted.

To create a File Protection policy:

a. Click **Policies** in the left navigation pane.
b. Click **Set the File Protection Policies**.
c. Click either **Create a new Continuous File Protection Policy** or **Create a new Open File Protection Policy**.
d. Follow the instructions on the window.

NOTE: When you create File Protection policies and set exclusion or inclusion rules, file extensions must not be greater than 9 characters for Open File Protection policies and 29 characters for Continuous File Protection policies.

For Open File Protection policies, you can select files without extensions in inclusion rules. This is not possible for Continuous File Protection policies.

ⓘ **IMPORTANT:** At this point you have configured all the basic policies Data Protector for PCs needs. Data Protector for PCs comes preconfigured with other policies that are sufficient for most organizations. We recommend that you now begin installing Agents on your user desktops and laptops (see “Installing Data Protector for PCs Agents” (page 36)). Later, you can return to review and configure the remaining Data Protector for PCs policies, such as the Cleanup Policy, User Control Policy, Agent Update Policy, and Reporting Data Retention Policy.

Configuring the remaining policies

1. **Configure Active Directory access**.

NOTE: *Associating Active Directory groups with Data Vaults:* You can associate Data Vaults with Active Directory groups in the Data Vault Policy. All members of the associated groups will back up to the associated Data Vault. You cannot associate individual users. Further, if you associate an Organization Unit (OU), only the groups within that OU are associated. Any users that are directly in the OU are not associated with the Data Vault. The list of Active Directory groups may incorrectly include groups other than security groups, such as distribution groups. However, only security groups will actually be associated with the Data Vault.

Multiple users: If two or more users are sharing one computer, they must belong to the same Active Directory group.

If you want to assign Data Vaults by group or organizational units, or if you want to report by group or organizational unit, you need to configure the Policy Server so it can access your Active Directory.

Configuring Active Directory access enables the **Members of groups and organizational units** option for Data Vaults (see "Configuring for the first time" (page 24)).

To configure Active Directory access:

a. Click **Configuration** in the left navigation pane.

b. Click **Configure Active Directory access**.

c. Follow the instructions on the window.

2. **Configure the Cleanup policy**.

The Data Protector for PCs Local Repositories on user computers and the Data Vaults on Data Vault Servers need to be periodically cleaned up to remove versions that are older than the retention settings defined in the file protection policies.

To configure the Cleanup policy:

a. Click **Policies** in the left navigation pane.

b. Click **Set the Cleanup Policy**.

c. Follow the instructions on the window.

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. Open the Cleanup Policy page in the Policy Server admin console and change the **Data Vault Cleanup Schedule**.

b. Uncheck all days except Friday or Saturday:

- For Friday, pick a start time late in the evening, such as 10 pm.
- For Saturday, pick a start time early in the morning, such as 1 am.

With cleanup running only at weekends:

- The list of files presented for restore from a Data Vault will be out-of-date by up to a 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 have 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.

Best practice:

- **Local Repository Cleanup Schedule**: Leave it at the default of 1 hour.
- **Data Vault Cleanup Schedule**: The default settings of "clean up every day at midnight" should be satisfactory for most installations. See "Sizing recommendations" (page 32) for further information on Data Vault capacity.
- You can configure DPNECleanup to use multiple threads in a reusable and extendable way for better use of the CPU and disk, allowing more data to be stored. See "Configuring multithread cleanup" (page 34).

3. **Configure the User Control policy**.

   The User Control policy determines how much control users have over the corporate policies distributed to their computer.

   To configure the User Control policy:

   a. Click **Policies** in the left navigation pane.
   b. Click **Set the User Control Policy**.
   c. Follow the instructions on the window.

   Best practice:

   Set **allow user control** for **Self-service Recovery**.

4. **Configure the Agent Update policy**.

   The policy designates the Data Protector for PCs Agent version that is to be used by all of your Data Protector for PCs-protected desktops and laptops, which will automatically be updated to this version.

   To configure the Agent Update policy:

a. Click **Policies** in the left navigation pane.
b. Click **Set the Agent Update Policy**.
c. Follow the instructions on the window.

5. **Configure Reporting Data Retention**.

   This sets how long data is retained for reporting purposes for each of the major categories of information.

   To configure Reporting Data Retention:

   a. Click **Configuration** in the left navigation pane.
   b. Click **Configure Reporting Data Retention**.
   c. Follow the instructions on the window.

Other configuration tasks

These are usually performed when you first install Data Protector for PCs.

License your Data Protector for PCs software.

If you are evaluating Data Protector for PCs, you can use if for 60 days to protect an unlimited number of users without further licensing. When you purchase Data Protector for PCs, you need to go to the HP License Key Delivery Service at https://webware.hp.com/welcome.asp to download a license key which you can then enter.

To enter a license key:

1. Click **License Management** in the left navigation pane.
2. Click **Enter a license key for HP Data Protector for PCs users**.
3. Follow the instructions on the window.

If you have multiple licenses to enter, you can create a text file with one license key string on each line. You can then import the file using the Import License Key(s) field.

NOTE: Licenses are distributed to Agents when the Agents are installed.

Moving Licenses

If you need to change the IP address of the Policy Server to move the server to another system, or you need to move licenses from one Policy Server to another, contact the HP License Key Delivery Service at https://webware.hp.com/welcome.asp.

Set, Import and Export an encryption password.

For security, you must define an encryption password before you can use Data Protector for PCs. This ensures that all files are encrypted at the user computer and transmitted encrypted over the network. The same password is used to encrypt the files from all users and for all centrally-configured Data Vaults.

- A centrally-defined Data Vault (defined through the Policy Server Console) will always use encryption based on the Data Protector for PCs encryption password.
- With locally-defined Data Vaults (defined by users through their computers), users can each choose whether to use encryption or not, and choose their own passwords.

When you first install Data Protector for PCs, you must either generate or import a password before you can continue. After generating a password, for your safety, export the password. This saves it to a secured location. You can then use it later for importing.

NOTE: After generating or importing a password, you cannot change it.

To manage your encryption password:

1. Click **Policies** in the left navigation pane.
2. Click **Encryption Policy**.
3. Follow the instructions on the window.

Determining how many Agents can be supported

It is difficult to give general rules that will hold true in all environments, so the cases given here clearly describe the context for which the given numbers are valid.

Factors affecting sizing

Sizing a Data Protector for PCs environment is complex. Technical factors that influence the number of users a specific environment can support include:

- Processing power on the Data Vault (for the nightly consolidation of backup data)
- Network and I/O bandwidth on the Data Vault server
- Disk space on the Data Vault server
- Size of the SQL database on the Policy Server
- Network bandwidth and processing power on the Policy Server

Which of these may generate a bottleneck in any given installation is determined by both the Data Protector for PCs configuration settings and patterns of use:

- Number of users on a Data Vault
- Number and size of files covered by the configured protection policies
- Frequency of change of the protected files
- Retention settings for protected file types

Sizing recommendations

Data Vault

With a daily cleanup schedule, a Data Vault with 14 TB disk space can support a user population of up to **3,500** Agents if the average data characteristics are approximately as follows:

- Average number of protected files: 5000
- Average total size of protected files on local disk: 10 GB
- Average total size on the Data Vault (compressed): 4 GB

If you need to protect more data on average than in this example, simply increasing disk capacity on the Data Vault will make more room for data but the Data Vault may not be able to complete the nightly consolidation of backup data in a timely fashion any more. Consider the following possibilities:

- Run the Data Vault cleanup only at weekends. See step 2 "Configure the Cleanup policy" in "Configuring the remaining policies" (page 27) for details of how to do this. 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.
- Consider distributing end-user data across several Data Vaults.

The hardware specifications for such Data Vaults are as follows:

Data Vault type	Daily cleanup (up to 3,500 Agents)	Weekly cleanup (up to 10,000 Agents)
Windows File Share	3 GHz dual core, 4 GB RAM, 14 TB disk space	3 GHz dual core, 4 GB RAM, 40 TB disk space
Web Data Vault	3 GHz quad core, 4 GB RAM, 14 TB disk space	3 GHz quad core, 4 GB RAM, 40 TB disk space

If your users have less data on average, you may be able to host more than these numbers of users on a Data Vault.

NOTE: HP strongly recommends that you keep the operating system of the Data Vault and the backup data on physically separate disks for best performance.

For best performance the Data Vault disk should be defragmented regularly.

Policy Server

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 MS SQL Server included with

Data Protector for PCs imposes a maximum database size of 4 GB, and no more than 5,000 Agents[1] 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 MS 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.

Networking 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.

[1] Using the default setting for "reporting data retention" on the Policy Server of 30 days.

5 Configuring multithread cleanup

The performance of `DPNECleanup` limits the amount of backup user data on a Data Vault. You can configure it to use multiple threads in a reusable and extendable way for better use of the CPU and disk, allowing more data to be stored.

With multithreaded Cleanup, the Scheduler argument '`-s`' leads to the default arguments '`-e -f -u -p -d 1000`', which include multithreaded cleanup by default and a delay of 1 second for the Auto-Adjuster. If you do not want to use these defaults, for example, to disable the multithreaded execution or to tune it, delete the '-s' argument from the Scheduler call and append the individual CLI arguments.

NOTE:

Although you might wish to disable multithreaded Cleanup under some circumstances, it is advisable to keep '`-e -f -u`' as arguments for the Cleanup call on the Data Vault.

Using DPNECleanup.exe from the CLI

The argument `-p` to `DPNECleanup.exe` lets the Cleanup initialize and start the Parallel Engine and thereby enables multithreaded execution. The Parallel Engine offers seven optional command line arguments. The DPNECleanup executable is able to retrieve these arguments and passes them through to the Parallel Engine.

DPNECleanup will run in serial mode if `-p` is not set. In this mode the Parallel Engine is not used at all.

```
dpnecleanup
```

`-a` *`affinity`*

Sets the processor affinity to the given number, which reflects set bits for the CPU cores to use by the threads.

`-d` *`delay`*

Sets the delay in milliseconds before the Auto-Adjuster begins its work, giving the Parallel Engine time to start up a number of threads and create some system utilization. By default the `–s` argument leads to a delay of 1000 milliseconds, or 1 second.

`-m` *`maxCpuUsage`*

Sets the desired maximum CPU usage (on all cores defined by *`affinity`*) to *`maxCpuUsage`*%, which the Auto-Adjuster will try to reach. *`maxCpuUsage`* should be an integer between 1 and 100. The default is '0' which stands for no limit (full CPU utilization).

`-o`

Constant resources, meaning the Auto-Adjuster is disabled and the Parallel Engine will not change the number of concurrent threads. Use `–r` to adjust the number of concurrent threads. The arguments `–d`, `–m` and `–q` are ignored when running with `–o`.

`-p`

Enables multithreaded Cleanup.

`-q` *`maxQueueLength`*

Sets the desired maximum average disk queue length, which the Auto-Adjuster will try to reach. The value should be a floating number. The default is 2.0.

`-r` *`resourceCount`*

Sets the number of concurrent resources (threads) to the given number. By default and in combination with option `–o`, the system will work with 2^(CPU count) concurrent threads. If the Auto-Adjuster is running, the given value will represent the limit of concurrent resources in terms of threads. Here the default for the maximum number is '0', which means there is no limit.

`-z [Idle|BelowNormal|Normal|AboveNormal|High|Realtime]`

Sets the process priority for all threads. The default is `Normal`.

`-s`

Server Cleanup. Sets Cleanup for all Data Vault, whether centrally or user defined. With multithreaded behavior, it is replaced by the arguments '`-e -f -u –p –d 1000`' when the command is executed.

`-e`

Enterprise Cleanup. Sets cleanup for all Data Vaults that are centrally defined by policies from the Policy Server.

`-f`

Fast Cleanup. Normally, Agent Cleanup will only run if the system is in an idle state. This option allows Cleanup to start at any time.

`-u`

User-defined Cleanup. Sets Cleanup for all local Data Vaults that are defined by local policies created by the user.

6 Installing Data Protector for PCs Agents

NOTE: Licenses are distributed to Agents when the Agents are installed.

Data Protector for PCs Agents can be installed in two ways:

- Individually on each client machine. See "Installing Data Protector for PCs Agents on individual client machines" (page 36).
- Deployed across an Enterprise from a file server accessible to all client machines. See "Deploying Data Protector for PCs Agents across an Enterprise" (page 37).

Installing Data Protector for PCs Agents on individual client machines

Prerequisites

Data Protector for PCs Agents software can be installed on users' desktops and notebooks running Windows. For supported platforms, see the Support Matrix.

You must be logged into an account with "administrator" privileges.

Installation procedure

1. Insert the Data Protector for PCs installation CD-ROM. An installation wizard should start automatically. If it does not, run it manually by double-clicking `setup.hta` at the root of the installation CD-ROM.
2. Click **Install or Update Data Protector for PCs Agent Software**. Choose **Open** (or **Run**) if presented with an "Open or Save" dialog box.
3. If the user computer does not have Microsoft Windows Installer 3.1 or later installed, the wizard offers to install it. When the Update Windows Installer dialog box appears, click **OK** to install it.
4. If the user computer does not have Microsoft .NET Framework 2.0 SP1 or later installed, the wizard offers to install it. When the Install Microsoft .NET Framework 2.0 SP1 dialog box appears, click **OK** to install it.
5. The wizard automatically installs the Data Protector for PCs Agent. Follow the instructions on-screen. During the installation, you are asked to enter details of the Policy Server.
6. When the installation and configuration are complete, click **Finish**. If there is an Open File Protection policy set on the Policy Server, you are asked to reboot your system.

   You should now see a Data Protector for PCs icon in the system tray (one of these, depending on the status of your protection: DP DP DP).
7. Test that the Data Protector for PCs Agent is working properly:

a. Select or create a test file such as a Word document or Excel spreadsheet, say on the Desktop. Make a couple of changes to it and click **Save**.

b. Right-click on the test file from the Desktop, from Windows Explorer, or in an Open dialog box. You should see three Data Protector for PCs entries in the menu that appears (**Search and recover files...**, **Copy Version**, and **Open Version with *XXX*...**).

c. Select **Open Version with *XXX*...** and you should see a list of time-stamped versions of the document you just created or edited. If you select one of the versions, it will be opened as a read-only document in the appropriate application. That is how a user recovers a previous version of their documents from the local Data Protector for PCs repository.

8. Repeat steps 1 through 8 for other user desktops and laptops that you want protected by Data Protector for PCs.

Deploying Data Protector for PCs Agents across an Enterprise

You can initially deploy Data Protector for PCs Agents across an Enterprise using the Data Protector for PCs Agent Deployment Kit contained on the installation CD-ROM.

NOTE: You cannot use the Deployment Kit on Vista PCs that have UAC (User Account Control) enabled. To fix this, disable UAC or install the Agent interactively.

In the procedure described below, you first copy the Data Protector for PCs Agent Deployment Kit in `*CD-ROM*:\Agent` to a directory on a file server that is accessible to all your users. Then you create a parameter file within that directory using `SetupConfig.exe`. Finally, you establish a mechanism to run `StartInstall.exe` in the shared directory from each users' computer. For example, you can use a login script. You can then monitor your deployment using the Agent Deployment report from the Data Protector for PCs Policy Server Console.

Kit contents

The Data Protector for PCs Deployment Kit contains the following components:

`SetupConfig.exe`	Creates and edits the initialization file.
`StartInstall.exe`	Starts `Setup.exe` as a privileged user.
`Setup.exe`	Installs the prerequisites and `DataProtectorNE.ini`.
`DataProtectorNE.msi`	Data Protector for PCs Windows Installer package to install the Agent software.
`DataProtectorNE64.msi`	Data Protector for PCs Windows Installer package to install the Agent software on 64–bit machines.
`DataProtectorNE*.*.mst`	Data Protector for PCs Windows Installer packages to install localized Agent software.

`WindowsInstaller.exe`	Updates the Windows Installer (required for .NET installation).
`NetFx20SP1_x64.exe`, `NetFx20SP1_x86.exe`	Installs NET Framework 2.0 SP1.
`Setup.ini`	Data Protector for PCs installation setup parameter file. This file will be created using `SetupConfig.exe` (see step 4 below).

Deployment and installation procedure

1. Copy the files in the Agent directory of the distribution CD-ROM to a directory that is accessible to all users who intend to use the Data Protector for PCs Agent Deployment Kit. This could be the directory of a common netlogon share such as `\\yourserver\DPNEDeploy`.
2. Make sure the newly-created directory contains the files listed above. You can delete all other files.
3. Open a DOS command window (`cmd.exe`) and `cd` to the directory created in step 1.
4. Run `SetupConfig.exe` to create or edit the parameter file `Setup.ini`. The first time you run `SetupConfig.exe`, you must enter values for all parameters. After that, you can run `SetupConfig.exe` repeatedly to change parameters. If you do not want to change a parameter, simply press **Enter**.

   The required parameters are:

   - **UNC path to the installation packages** – the complete path to the shared directory in which the files were copied in step 1, such as `\\yourserver\DPNEDeploy`.
   - The name of the **Data Protector for PCs Policy Server**. This can be a NetBIOS name like `YOURSERVER`, or a fully-qualified domain name like `yourserver.yourcompany.com`.
   - **Username** – the username of a user with Administrator privileges on the computers using the Data Protector for PCs Agent Deployment Kit, such as a member of the Domain Admins group. It is typically a fully qualified username including domain, such as `YOURCOMPANY\JerryAdmin`.
   - **Password** – the password associated with the Username. You must type it twice to confirm it.
5. On the client computer, run `StartInstall.exe`, for example,`\\yourserver\DPNEDeploy\StartInstall`. This will then run `Setup.exe` in the background at low priority using the username and password specified in `Setup.ini`. This can be done as part of a logon script. Note that you cannot include it in a startup script because the machine account does not have sufficient network privileges.

6. `Setup.exe` determines if the client computer can support Data Protector for PCs. For supported Windows platforms, see the Support Matrix.
7. `Setup.exe` determines whether .NET Framework version 2.0 SP1 is installed. If not, it will be installed, after which you may need to reboot the computer.
8. `Setup.exe` determines whether Data Protector for PCs is already installed. If it is not or the version is out of date, it installs Data Protector for PCs.

NOTE:

Any errors encountered in steps 4–7 will log a message on the Data Protector for PCs Policy Server and in the Application Event Log on the local computer.

You can check the progress of your Agent deployment using the Data Protector for PCs Policy Server Console:

1. Log in to the Data Protector for PCs Policy Server Console.
2. Select **Agent Deployment** under **Reports** in the left navigation pane.

   You will see a summary of your initial deployment to date. It shows:

   - How many machines have successfully **finished** deployment.
   - The number for which deployment is **in progress**.
   - The number where deployment has **failed**.
3. Click on a number in the **Number of Machines** column to show a list of the machines in the selected deployment state.

   The current status of each machine is shown. For example, if the deployment failed on a particular machine, the **Information** column will give the error that occurred. You can get additional details about a machine by clicking on its NETBIOS name.

7 Updating Data Protector for PCs

If you are updating a version 6.*x* of Data Protector for PCs to 7.0, proceed in this order:

1. Update the Policy Server to 7.0. See “Updating the Policy Server” (page 40).
2. Install the Web Data Vault Server. See “Installing, configuring and maintaining the Web Data Vault Server” (page 18).
3. Update the Agents to 7.0.

   You can either update them using the Manual Update or "silently" by using the Agent Update Policy. See “Updating Agents” (page 40) for more details.

Updating the Policy Server

You can update an existing Data Protector for PCs Policy Server installation to a newer version by following the standard installation procedure. All existing configurations (such as Data Vault configuration, Licensing, and so on) will be available in the newer version.

Updating the Policy Server:

1. Insert the Data Protector for PCs installation CD-ROM. If the installation wizard does not start automatically, run it manually by double-clicking `setup.hta` at the root of the installation CD-ROM.
2. Click **Install Policy Server** on the Install Data Protector for PCs page of the wizard to begin the update.
3. Follow the instructions on-screen.
4. The installation procedure will detect an existing Policy Server installation and offer an update.
5. Follow the instructions on-screen.
6. When the installation finishes, click **Next**. You can then choose to run the Data Protector for PCs Policy Server Console.

NOTE: If Cleanup software is installed on the Policy Server, you need to update it as well. You can either do this manually or by using the Agent Update Policy.

Updating Agents

If you update the version of the Data Protector for PCs Server, existing Agents using the former version of Data Protector for PCs will continue to work as before. You can either update them using the Manual Update or “silently” by using the Agent Update Policy.

NOTE: After updating, all Agents must reboot so that they can use the new Web Data Vaults. They are instructed to do this by balloon messages in the system tray, and also on the Summary tab of the Data Protector for PCs Health Panel on their PCs.

Automatic Agent update using the Agent Update Policy

Agents can be updated "silently" by using the Agent Update Policy of the Policy Server. The installation package will be delivered automatically to all connected clients and the update will complete in a fully automated fashion. The end-user will not be interrupted.

1. In the Policy Server Console, select **Policies->Agent Update Policy**.
2. If you have just updated your Policy Server, the installation procedure has uploaded a new Agent Update Package. In the Policy Server Console, this new version is not selected yet.

   Select the new Agent version to make the version available.
3. By adjusting the Throttling, you can adjust the maximum number of updates allowed per minute.
4. Click **Save Agent Update Policy**.
5. Now Agents will be updated automatically to the newest version. Also Cleanup Agents will be updated automatically.

NOTE: You can check the Agent update progress using the report: "Agent Deployment."

Manual Agent update

An existing Data Protector for PCs Agent can be updated to a newer version by executing the standard installation procedure.

Before updating the Agent to a newer version, make sure the Agent version is compliant with the version of the Data Protector for PCs Policy Server.

1. Insert the Data Protector for PCs installation CD-ROM. If the installation wizard does not start automatically, run it manually by double-clicking `setup.hta` at the root of the installation CD-ROM
2. Click **Install Agent** on the Install Data Protector for PCs page of the wizard to begin the update.
3. Follow the instructions on-screen.
4. The installation procedure will detect an existing Agent installation and offer an update.
5. Follow the instructions on-screen.

8 How to get support for Data Protector for PCs

Data Protector for PCs comes with one year of maintenance. This entitles you to:

- Telephone support, to speak with a Support Technician.
- Updates of the Data Protector for PCs Server and Data Protector for PCs Agent software. You can download the latest versions or a CD-ROM image from the Data Protector website. Browse to http://www.hp.com/go/dataprotector.

Glossary

Active Directory

(Windows specific term) The directory service in a Windows network. It contains information about resources on the network and makes them accessible to users and applications. The directory services provide a consistent way to name, describe, locate, access and manage resources regardless of the physical system they reside on.

Administrative user

A user on the Web Data Vault Server who looks after administrative tasks like creating and deleting Data Vaults and migrating client backup data.

Agent

Data Protector for PCs software that runs on each users' desktop/laptop. It communicates with the Policy Server via Web services (SOAP and XML) over TCP port 80.

Backup user

A user on the Web Data Vault Server who performs end-user operations like the backup and restore of files.

Cleanup policy

The retention periods set by the file protection policies are enforced by cleanup tasks that run periodically. The frequency is defined in the Cleanup policy. By default, users' Local Repositories are cleaned up every hour, and any locally-defined Data Vaults are cleaned up once a day. Centrally-defined Windows File share Data Vaults are cleaned up by a computer assigned through Data Vault Policy, and Web Data Vaults by cleanup running locally on the Data Vault Server. The cleanup policy applies to all users.

console

The browser-based console is where you centrally define Data Protector for PCs policies. You must be a member of the Administrator's group.

Continuous File Protection

Continuous File Protection is Data Protector for PCs's Continuous Data Protection method, which automatically stores changes in a file whenever the file is saved. This is suitable for data files that are saved by the user (as opposed to always-open files like databases or Outlook files). Each Continuous File Protection policy protects a group of files that are related in some way. Data Protector for PCs comes preconfigured with policies for commonly used types of files, such as Office Documents and Pictures. You can edit these File Protection Policies or create your own. The policy also specifies how long the previous versions of protected files are retained.

Copy policy

Copy policies define the following:

- How many Agents can copy files concurrently to your Data Vaults.
- A schedule for periodic updates, which check that all the expected files for a user exist on the Data Vault and, if they do not, copies any missing files. This provides further assurance that all user files have been properly copied to the Data Vault.
- If an *initial update* should be performed. The initial update is needed because during regular Data Protector for PCs operation, each time a user changes a Data Protector for PCs continuously-protected file, only information about the changes is copied to the Data Vault.

If you have just installed Data Protector for PCs, you need to set a Copy policy to make an initial update of all your users' protected files.

Data Vault

There are two types of Data Vault:

- Web Data Vaults. These use HTTPS protocol and provide the best level of security for the transmission of data between client PCs and the Data Vault and better throughput in high latency environments, and so are recommended..
- Windows file share Data Vaults. These are shared folders on a file server in which files are stored according to a Data Vault policy. The file server must support the Windows file sharing protocol (CIFS/SMB). They should not be used in environments with high network latency.

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.

Users can be assigned one or more Data Vault policies, based on their group or organization unit membership.

initial update

Data Protector for PCs protects files continuously as users modify them by saving the changes. Whenever a user creates a new Data Vault, Data Protector for PCs must make an initial update of all the user's protected files to the vault. Users can select how the initial update is done, immediately or in the background.

Local Repository

The Local Repository is a safe storage location on Agent computers that is used to store protected files and file changes, usually on the system hard disk drive. It is a hidden, system directory. Users can quickly recover a previous version by right-clicking on the file on the Desktop, in Windows Explorer, or in an Open dialog box. Files protected by Continuous File Protection policies are kept in a hidden directory on the local computer until they no longer satisfy the retention period. Files protected by Open File Protection policies are temporarily stored in the local Version Store only until they have been copied to the Data Vault. The path of the Local Repository is usually `C:\{DPNE}`.

Open File Protection

Open File Protection backs up files that are always open, such as Outlook Personal Folders and many database files by taking periodic file-level snapshots. This is sometimes called “near” Continuous Data Protection. An Open File Protection policy defines the protection for open files, defined by sets of inclusion and exclusion rules. For example, you might define a policy named “Outlook Personal Folders” that applies to Outlook `.pst` files by specifying an inclusion rule as “ends with '.pst'”. If you wanted to exclude archived `.pst` files, you could then create an exclusion rule as “contains 'archive'”. Policies also specify how long previous versions of protected files are retained. Open File Protection policies apply to all users.

policy

A policy is a set of rules, defined centrally in the Policy Server and executed by the Agent on each desktop/laptop/notebook.

Policy Server

The Policy Server provides the central management of Data Protector for PCs policies. It also collects status information from Agents and provides reports on their deployment and operation.

protected files

A protected file is one that is automatically backed up by Data Protector for PCs. The types of files that are protected are defined in the Continuous and Open File Protection policies.

User Control policy

This policy determines how much control individual users have over the Agent software running on their desktop/laptop/notebook. You can lock down the Agent so that policies are completely hidden from users, you can allow them to see policies but not change them, or you can let them add policies of their own. You can set the level of control on each major Data Protector for PCs policy separately. The user control policy applies to all users.

Index