

HP Data Protector Notebook Extension 6.20

Installation and administration guide

Part Number: n/a
First edition: May 2010



Legal and notice information

© Copyright 2010 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.

Microsoft®, Windows®, Windows® XP, Windows NT®, and Windows Vista® are U.S. registered trademarks of Microsoft Corporation.

Contents

About this guide	7
Intended audience	7
Document conventions and symbols	7
General Information	8
HP technical support	8
Subscription service	9
HP websites	9
Documentation feedback	9
1 Overview and prerequisites	11
Overview of Notebook Extension	11
Overview of installing Notebook Extension	12
Prerequisites	12
Policy Server	12
Database	14
Notebook Extension Agents	14
2 Installing the Notebook Extension Policy Server	15
Quick Installation	15
Detailed installation	16
Updating the Policy Server	18
3 Configuring your Notebook Extension protection policies	21
Initial Setup after installing Notebook Extension	21
Configuring for the first time	22
Configuring the remaining policies	26
Other configuration tasks	28
Determining how many Agents can be supported	29
Factors affecting sizing	29
Sizing recommendations	30
Data Vault	30
Policy Server	30

Networking considerations	31
4 Installing Notebook Extension Agents	33
Installing Notebook Extension Agents on individual client machines	33
Prerequisites	33
Installation procedure	34
Deploying Notebook Extension Agents across an Enterprise	35
Kit contents	35
Deployment and installation procedure	36
Updating Agents	37
Automatic Agent update using the Agent Update Policy	38
Manual Agent Update	38
5 How to get support for Notebook Extension	41
Glossary	43
Index	47

Figures

1 Notebook Extension architecture	11
---	----

Tables

1 Document conventions	7
------------------------------	---

About this guide

This guide provides information about:

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

Intended audience

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

- Windows administration

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Blue text: Table 1 on page 7	Cross-reference links and e-mail addresses
Blue, underlined text: http://www.hp.com	website addresses
Bold text	<ul style="list-style-type: none">• 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
<i>Italic</i> text	Text emphasis

Convention	Element
Monospace text	<ul style="list-style-type: none"> • File and directory names • System output • Code • Commands, their arguments, and argument values
<i>Monospace, italic</i> text	<ul style="list-style-type: none"> • 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 Notebook Extension 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 updates, and other product resources.

HP websites

For additional information, see the following HP websites:

- <http://www.hp.com>
- <http://www.hp.com/go/storage>
- <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 Notebook Extension

HP Data Protector Notebook Extension 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.

There must be one or more file servers. File servers contain shared folders, called Data Vaults, to which user data is backed up by Notebook Extension.

The Notebook Extension architecture is illustrated in the following diagram:

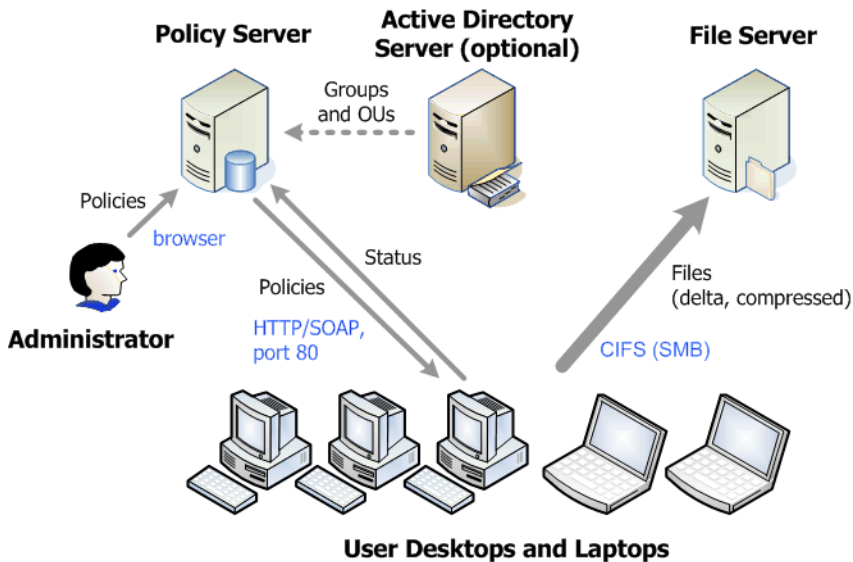


Figure 1 Notebook Extension architecture

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 file servers. For performance reasons, it is best not to have any Notebook Extension software apart from the Cleanup software running on these.

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.

Overview of installing Notebook Extension

There are three stages to installing Notebook Extension:

- 1. Install the Notebook Extension Policy Server.**
See [Chapter 2](#) on page 15.
- 2. Configure protection policies.**
See [Chapter 3](#) on page 21.
- 3. Install Notebook Extension Agents on laptops and desktops.**
See [Chapter 4](#) on page 33.

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, Notebook Extension 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

Notebook Extension 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 Notebook Extension, you can install an instance of Microsoft's SQL Server Express Edition.

Notebook Extension Agents

Notebook Extension Agent software can be installed on users' desktops and notebooks running Windows. For supported platforms, see the Support Matrix.

2 Installing the Notebook Extension Policy Server



NOTE:

You can update an existing Notebook Extension Policy Server installation to a newer version by following the standard installation procedure. See “[Updating the Policy Server](#)” on page 18 for more details.

Quick Installation

See [Policy Server](#), page 12 for requirements for the Notebook Extension Policy Server.

1. Insert the Notebook Extension 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 Notebook Extension Policy Server requires access to a Microsoft SQL Server database. Select **Use existing DataProtectorNE 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 Notebook Extension Policy Server** page of the wizard to begin the installation.
5. When the installation is finished, you need to install the Cleanup software. Click **Install** on the **Install Data Protector Notebook Extension Data Vault Cleanup** screen.
6. When the installation finishes, click **Next** . You can then choose to run the Notebook Extension Policy Server Console.

 **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.

Detailed installation

 **NOTE:**

Windows 2003 server only: You can only install the Notebook Extension 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 Notebook Extension Policy Server installation.

1. Insert the Notebook Extension 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 Notebook Extension 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 2.0If 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 Notebook Extension 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 Notebook Extension Policy Server software

- a. On the Welcome screen, click **Next** to begin the installation.
 - The Notebook Extension Policy Server Console will be installed as a Web application in the virtual directory `C:\Inetpub\wwwroot\dpnepolicy`.
 - The Notebook Extension 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 Notebook Extension centrally from the Notebook Extension Policy Server Console. Because the console is browser-based, you can manage Notebook Extension from any computer that can establish a browser connection to the Policy Server (using HTTP port 80).

To run the Notebook Extension 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.
-

Updating the Policy Server

You can update an existing Notebook Extension 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.

Existing Agents using the former version of Notebook Extension will continue to work as before. You can either update them using the Manual Update or "silently" by using the Agent Update Policy. See ["Updating Agents"](#) on page 37 for more details.

Update procedure:

1. Insert the Notebook Extension 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 Notebook Extension page of the wizard to begin the upgrade.
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 Notebook Extension 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.

3 Configuring your Notebook Extension protection policies

Initial Setup after installing Notebook Extension

Immediately after installing Notebook Extension, you are presented with the Initial Setup window in the Policy Server Console. Before you can set up policies for Notebook Extension, 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 Notebook Extension. 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 Notebook Extension 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 Notebook Extension, 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 Notebook Extension.

If you are evaluating Notebook Extension, you can use it for 60 days to protect an unlimited number of users without further licensing. When you purchase Notebook Extension, 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 Notebook Extension 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 Notebook Extension, configure other elements of Notebook Extension in the order in the next section.

Configuring for the first time

Notebook Extension 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 Notebook Extension Agent software on users' desktops and notebooks.

 **NOTE:**

Instead of configuring new policies, you can modify the policies that come pre-configured with Notebook Extension. 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 Notebook Extension Agents and executed on the users' desktops and laptops.

1. Run the Notebook Extension 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 Notebook Extension Policy Server. You must be logged in as "administrator" on the server.

2. **Configure Data Vault policies.**

Data Vault Policies set the destination 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. A destination is usually a network share. 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*.

Requirements for Data Vaults:

Notebook Extension uses standard Windows file shares to store the protected files backed up from users' desktops and laptops. 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 Notebook Extension with a small number of installed Agents, it may be useful to make the Policy Server and Data Vault file server the same machine.

Notebook Extension 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.

To create a Data Vault policy:

- a. Click **Policies** in the left navigation pane.
- b. Click **Set the Data Vault Policy**.
- c. Click **Create a new Data Vault policy**.
- d. Follow the instructions on the window.

 **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:

- 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 Notebook Extension operation, each time a user changes a Notebook Extension 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.

Notebook Extension 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.

Notebook Extension includes two examples: *Microsoft Outlook* and *Microsoft Outlook Express*. You can start with these policies or build your own.



NOTE:

Notebook Extension 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 copy 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.

 **IMPORTANT:**

At this point you have configured all the basic policies Notebook Extension needs. Notebook Extension 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 [Chapter 4](#) on page 33). Later, you can return to review and configure the remaining Notebook Extension 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.

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”](#) on page 22).

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 Local Repositories on user computers and the Data Vaults on file 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.

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.

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 Notebook Extension Agent version that is to be used by all of your Notebook Extension-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 Notebook Extension.

License your Notebook Extension software.

If you are evaluating Notebook Extension, you can use it for 60 days to protect an unlimited number of users without further licensing. When you purchase Notebook Extension, 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 Notebook Extension 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 Notebook Extension. 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 Notebook Extension 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 Notebook Extension, 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 Notebook Extension 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 Notebook Extension 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

The following hardware specifications are a solid basis for a Data Vault:

- 1 x 3 GHz dual-core processor
- 2 GB RAM
- 1.5 TB disk capacity

Such a Data Vault can support a user population of up to **1,000** Agents if the average data characteristics are approximately as follows:

- Average number of protected files: 3000
- Average total size of protected files on local disk: 4 GB¹
- Average total size on the Data Vault (compressed): 1 GB

If you need to protect more data on average than in this example, consider distributing end-user data across several Data Vaults. 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.

If your users have less data on average, you may be able to host more than 1,000 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.

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

¹Assuming a mix of 3.5 GB of files under Continuous File Protection and 0.5 GB of files under Open File Protection

with DPNE imposes a maximum database size of 4 GB, and no more than 5,000 Agents² 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.

A Policy Server can run on the same server as a Data Vault or separately.

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

In general, HP does not recommend performing an initial update from Notebook Extension 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. Notebook Extension 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.

²Using the default setting for "reporting data retention" on the Policy Server of 30 days.

4 Installing Notebook Extension Agents



NOTE:

If you update the version of the Notebook Extension Server, existing Agents using the former version of Notebook Extension will continue to work as before. You can either update them using the Manual Update or "silently" by using the Agent Update Policy. See [“Updating Agents”](#) on page 37 for more details.



NOTE:

Licenses are distributed to Agents when the Agents are installed.

Notebook Extension Agents can be installed in two ways:

- Individually on each client machine. See [“Installing Notebook Extension Agents on individual client machines”](#) on page 33.
- Deployed across an Enterprise from a file server accessible to all client machines. See [“Deploying Notebook Extension Agents across an Enterprise”](#) on page 35.


Installing Notebook Extension Agents on individual client machines

Prerequisites

Notebook Extension 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 Notebook Extension 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 Notebook Extension 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 Notebook Extension 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 Notebook Extension icon in the system tray (one of these, depending on the status of your protection: ).
7. Test that the Notebook Extension 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 Notebook Extension 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 Notebook Extension repository.
8. Repeat steps 1 through 8 for other user desktops and laptops that you want protected by Notebook Extension.

Deploying Notebook Extension Agents across an Enterprise

You can initially deploy Notebook Extension Agents across an Enterprise using the Notebook Extension 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 Notebook Extension 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 Notebook Extension Policy Server Console.

Kit contents

The Notebook Extension Deployment Kit contains the following components:

<code>SetupConfig.exe</code>	Creates and edits the initialization file.
<code>StartInstall.exe</code>	Starts <code>Setup.exe</code> as a privileged user.
<code>Setup.exe</code>	Installs the prerequisites and <code>DataProtectorNE.ini</code> .
<code>DataProtectorNE.msi</code>	Notebook Extension Windows Installer package to install the Agent software.
<code>DataProtectorNE64.msi</code>	Notebook Extension Windows Installer package to install the Agent software on 64-bit machines.
<code>DataProtectorNE*.*.mst</code>	Notebook Extension 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	Notebook Extension 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 Notebook Extension 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 **Notebook Extension 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 Notebook Extension 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 Notebook Extension. 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 Notebook Extension is already installed. If it is not or the version is out of date, it installs Notebook Extension.

 **NOTE:**

Any errors encountered in steps 4–7 will log a message on the Notebook Extension Policy Server and in the Application Event Log on the local computer.

You can check the progress of your Agent deployment using the Notebook Extension Policy Server Console:

1. Log in to the Notebook Extension 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.

Updating Agents

If you update the version of the Notebook Extension Server, existing Agents using the former version of Notebook Extension will continue to work as before. You can

either update them using the Manual Update or “silently” by using the Agent Update Policy.

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 Notebook Extension 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 Notebook Extension Policy Server.

1. Insert the Notebook Extension 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 Notebook Extension 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.

5 How to get support for Notebook Extension

Notebook Extension comes with one year of maintenance. This entitles you to:

- Telephone support, to speak with a Support Technician.
- Updates of the Notebook Extension Server and Notebook Extension 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	<i>(Windows specific term)</i> 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.
Agent	Notebook Extension software that runs on each users' desktop/laptop. It communicates with the Policy Server via Web services (SOAP and XML) over TCP port 80.
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 Data Vaults are cleaned up by a computer assigned through the Data Vault policy. The cleanup policy applies to all users.
console	The browser-based console is where you centrally define Notebook Extension policies. You must be a member of the Administrator's group.
Continuous File Protection	Continuous File Protection is Notebook Extension'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. Notebook Extension 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 Notebook Extension operation, each time a user changes a Notebook Extension continuously-protected file, only information about the changes is copied to the Data Vault.

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

Data Vault

A Data Vault is a shared folder 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). Users can be assigned one or more Data Vault policies, based on their group or organization unit membership.

initial update

Notebook Extension protects files continuously as users modify them by saving the changes. Whenever a user creates a new Data Vault, Notebook Extension 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 Notebook Extension 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 Notebook Extension. 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 Notebook Extension policy separately. The user control policy applies to all users.

Index

Symbols

.NET Framework, [16](#), [34](#)

A

accessing Active Directory, [26](#)

Active Directory, [11](#)

access, [26](#)

associating groups with Data Vaults,
[26](#)

Agent Deployment Kit contents, [35](#)

Agent Deployment report, [38](#)

Agent Update policy, [27](#)

Agents, [11](#)

how many can be supported, [29](#)

prerequisites, [14](#)

updating, [37](#)

Agents software

deploying across an Enterprise, [35](#)

installing, [33](#)

ASP.NET, [16](#)

audience, [7](#)

B

browser settings for Policy Server

Console, [18](#)

C

Cleanup policy, [27](#)

configuring

Active Directory access, [26](#)

Agent Update policy, [27](#)

Cleanup policy, [27](#)

Continuous File Protection policies, [25](#)

Copy policies, [24](#)

Data Vault policies, [23](#)

File Protection policies, [25](#)

Open File Protection policies, [25](#)

policies for the first time, [22](#)

Reporting Data Retention, [28](#)

User Control policy, [27](#)

console

browser settings, [18](#)

running, [17](#), [23](#)

console, running, [17](#), [23](#)

Continuous File Protection policies, [25](#)

conventions

document, [7](#)

Copy policies, [24](#)

D

Data Vault policies, [23](#)

Data Vaults

associating Active Directory groups,
[26](#)

requirements, [23](#)

server recommendations, [30](#)

database prerequisites, [14](#)

deploying Agent software, [35](#)

checking progress, [37](#)

procedure, [36](#)

- deployment
 - checking progress, 37
 - procedure, 36
- desktops, prerequisites, 14
- document
 - conventions, 7
- documentation
 - providing feedback, 9

E

- EFS-encrypted files, 25
- encryption password, 21, 28, 29
- entering a license key, 28
- entering an encryption password, 29
- evaluating Notebook Extension, 21, 28
- exporting encryption password, 21, 28

F

- File Protection policies, 25
 - Continuous, 25
 - Open, 25
- file servers, 11

H

- help
 - obtaining, 8
- HP
 - technical support, 8

I

- IIS, 16
- importing encryption password, 28
- Installation with Microsoft SharePoint, 18
- installing
 - Agents, 33
 - overview, 12
 - Policy Server, 15
 - SQL server, 17

- Internet Information Services, 16

L

- license key
 - entering, 28
- licenses
 - available, 22
 - moving, 28
- licensing, 21, 28

M

- moving licenses, 28

N

- network, sizing considerations, 31
- Notebook Extension
 - architecture, 11
 - installing Agents, 33
 - obtaining support, 41
 - overview, 11
- notebooks, prerequisites, 14

O

- Open File Protection policies, 25
- overview, 11

P

- password, 21, 28

- policies
 - Agent Update, [27](#)
 - Cleanup, [27](#)
 - configuring for the first time, [22](#)
 - Continuous File Protection, [25](#)
 - Copy, [24](#)
 - Data Vault, [23](#)
 - distribution of, [11](#)
 - File Protection, [25](#)
 - Open File Protection, [25](#)
 - Reporting Data Retention, [28](#)
 - User Control, [27](#)
- Policy Server, [11](#)
 - database prerequisites, [14](#)
 - installing, [15](#)
 - prerequisites, [12](#)
 - recommendations, [30](#)
 - updating, [18](#)
- Policy Server Console
 - browser settings, [18](#)
 - running, [17](#), [23](#)
- Policy Server Console, running, [17](#), [23](#)
- prerequisites, [12](#)

R

- Reporting Data Retention, [27](#)

S

- servers
 - file, [11](#)
 - Policy, [11](#)
- SharePoint
 - installing Policy Server with, [18](#)
- sizing considerations, [29](#)
 - Data Vault, [30](#)
 - network, [31](#)
 - Policy Server, [30](#)
- SQL database
 - prerequisites, [14](#)
- SQL server
 - installing, [17](#)

- Subscriber's Choice, HP, [9](#)
- support, [41](#)
- support matrix, [11](#)

T

- technical support, [8](#), [9](#)

U

- updating
 - Agents, [37](#)
 - Policy Server, [18](#)
- user computers, prerequisites, [14](#)
- User Control policy, [27](#)

W

- websites
 - HP, [9](#)
 - HP Subscriber's Choice for Business, [9](#)
- Windows Installer, [16](#), [34](#)

