

HP Data Protector Notebook Extension 6.10

Installations- und Administrationshandbuch

Teilenummer: n/v
Erste Ausgabe: September 2009



Rechtlicher Hinweis und Informationen

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Die in diesem Dokument enthaltenen Informationen können jederzeit ohne Ankündigung geändert werden. Für HP Produkte und Services gilt ausschließlich die Herstellergarantie, die in den Garantieerklärungen der jeweiligen Produkte und Services explizit beschrieben wird. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten. HP übernimmt keine Haftung für technische oder redaktionelle Fehler oder für die Vollständigkeit der Angaben in diesem Dokument.

Microsoft®, Windows®, Windows XP, Windows NT® und Windows Vista® sind eingetragene Warenzeichen der Microsoft Corporation.

Inhalt

Informationen zu diesem Dokument	7
Zielgruppe	7
Zugehörige Dokumente	7
Dokumentkonventionen und -symbole	8
Allgemeine Informationen	9
Technischer Support von HP	9
Abonnementservice	9
HP Websites	9
Feedback zur Dokumentation	10
1 Übersicht und Voraussetzungen	11
Übersicht zu Notebook Extension	11
Notebook Extension installieren – Übersicht	13
Voraussetzungen	13
Policy Server	13
Datenbank	14
Notebook Extension-Agenten	14
2 Notebook Extension-Policy Server installieren	15
Schnellinstallation	15
Benutzerdefinierte Installation	16
3 Notebook Extension-Schutzrichtlinien konfigurieren	19
Ersteinrichtung nach der Installation von Notebook Extension	19
Erstkonfiguration	21
Weitere Richtlinien konfigurieren	25
Weitere Konfigurationsschritte	26
Anzahl der unterstützten Agenten festlegen	28
Faktoren für die Größenbestimmung	28
Empfehlungen für die Größenbestimmung	29
Data Vault	29
Policy Server	29

Überlegungen bei Netzwerken	30
4 Notebook Extension-Agenten installieren	33
Notebook Extension-Agenten auf einzelnen Benutzercomputern installieren	33
Voraussetzungen	33
Installationsprozedur	33
Notebook Extension-Agenten unternehmensweit bereitstellen	35
Inhalt des Kits	35
Bereitstellungs- und Installationsprozedur	36
5 Unterstützung für Notebook Extension anfordern	39
Stichwortverzeichnis	41

Abbildungen

1 Notebook Extension-Architektur	12
--	----

Tabellen

1 Dokumentkonventionen	8
------------------------------	---

Informationen zu diesem Dokument

In diesem Handbuch sind Informationen zu Folgendem enthalten:

- HP Data Protector Notebook Extension installieren
- Richtlinien für HP Data Protector Notebook Extension konfigurieren
- Software "HP Data Protector Notebook Extension Agent" auf den Desktop-PCs und Notebooks der Benutzer
- Anzahl der unterstützten Agenten festlegen

Zielgruppe

Dieses Handbuch richtet sich an Administratoren, die HP Data Protector Notebook Extension installieren und konfigurieren möchten. Vorkenntnisse in folgenden Bereichen sind von Vorteil:

- HP Data Protector
- Windows-Administration

Zugehörige Dokumente

Zu HP Data Protector sind eine Reihe von Handbüchern verfügbar. Eine vollständige Liste finden Sie im Vorwort jedes dieser Handbücher.

Sie finden diese Dokumente auch auf der Website für Handbücher zu HP Softwareprodukten:

<https://h20230.www2.hp.com/selfsolve/manuals>

Dokumentkonventionen und -symbole

Tabelle 1 Dokumentkonventionen

Konventionen	Element
Blauer Text: Tabelle 1 auf Seite 8	Querverweislinks und E-Mail-Adressen
Blauer, unterstrichener Text: http://www.hp.com	Website-Adressen
Gefetteter Text	<ul style="list-style-type: none">• Tasten, die gedrückt werden• Text, der in ein Oberflächenelement, z. B. ein Feld, eingegeben wird• Oberflächenelemente, auf die geklickt wird oder die ausgewählt werden, z. B. Menü- und Listeneinträge, Schaltflächen und Kontrollkästchen
<i>Kursiver Text</i>	Betonter Text
Nichtproportionaler Text	<ul style="list-style-type: none">• Datei- und Verzeichnisnamen• Systemausgabe• Code• Befehle, deren Argumente und Argumentwerte
<i>Nichtproportionaler, kursiver Text</i>	<ul style="list-style-type: none">• Codevariablen• Befehlsvariablen
Nichtproportionaler, gefetteter Text	Betonter, nichtproportionaler Text

❗ **WICHTIG:**

Enthält Erklärungen oder spezielle Anweisungen.

📝 **HINWEIS:**

Enthält zusätzliche Informationen.

Allgemeine Informationen

Allgemeine Informationen zu Notebook Extension finden Sie unter <http://www.hp.com/go/dataprotector>.

Technischer Support von HP

Informationen zum technischen Support weltweit finden Sie auf der HP Support Website:

<http://www.hp.com/support>

Bevor Sie sich an HP wenden, stellen Sie folgende Informationen zusammen:

- Namen und Nummern des Produktmodells
- Registrierungsnummer für den technischen Support (falls zutreffend)
- Produktseriennummern
- Fehlermeldungen
- Betriebssystemtyp und Versionsnummer
- Detailfragen

Abonnementservice

HP empfiehlt, dass Sie Ihr Produkt auf der Website "Subscriber's Choice for Business" registrieren:

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

Nach der Registrierung erhalten Sie E-Mail-Benachrichtigungen über Produktverbesserungen, neue Treiberversionen, Firmwareaktualisierungen und andere Produktressourcen.

HP Websites

Weitere Informationen finden Sie auf folgenden 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>

Feedback zur Dokumentation

HP freut sich über Ihr Feedback.

Wenn Sie Anmerkungen und Vorschläge zur Produktdokumentation machen möchten, senden Sie eine Nachricht an DP.DocFeedback@hp.com. Alle Einsendungen werden Eigentum von HP.

1 Übersicht und Voraussetzungen

Übersicht zu Notebook Extension

HP Data Protector Notebook Extension besteht im Wesentlichen aus zwei Softwarekomponenten, dem Policy Server und den Agenten. Der Policy Server wird auf einem Windows Server ausgeführt. Informationen zu unterstützten Versionen finden Sie in der Supportmatrix (<https://h20230.www2.hp.com/selfsolve/manuals>). Die Agenten werden auf den einzelnen Desktop-PCs und Notebooks im Hintergrund ausgeführt.

Der Policy Server kann auch auf Gruppen und Organisationseinheiten auf einem Active Directory Server zugreifen.

Mindestens ein Dateiserver muss vorhanden sein. Dateiserver enthalten gemeinsam genutzte Ordner, Data Vaults genannt, in die Notebook Extension die Benutzerdaten zur Datensicherung kopiert.

Die Architektur von Notebook Extension wird in folgender Abbildung dargestellt:

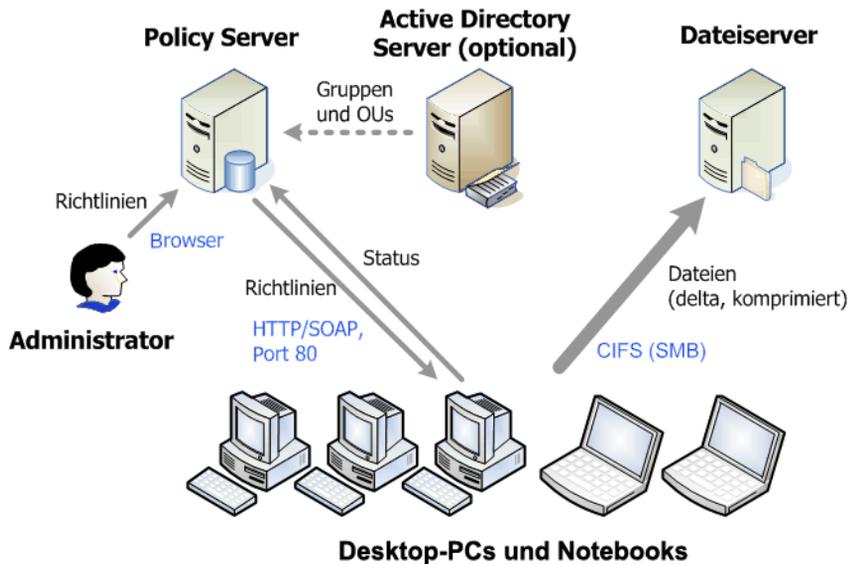


Abbildung 1 Notebook Extension-Architektur

In den verschiedenen Richtlinien ist festgelegt, welche Dateien von den Desktop-PCs und Notebooks gesichert werden und wo diese Sicherungen gespeichert werden. Die Richtlinien werden in der Policy Server-Konsole definiert. Anschließend werden die Richtlinien automatisch mithilfe des SOAP-Protokolls über HTTP-Port 80 an die Agenten verteilt. Die Richtlinien befinden sich auf dem Policy Server.

Die Agenten führen diese Richtlinien aus. Wenn ein Benutzer eine Datei ändert, die gemäß einer der Richtlinien geschützt wird, wird auf der lokalen Festplatte des Desktop-PCs oder Notebooks eine Vorgängerversion erstellt, und Änderungen an der Datei werden komprimiert und auf die entsprechenden Data Vaults kopiert.

Wenn Dateien gesichert werden, benachrichtigt der Agent den Policy Server, der ein Prüfprotokoll der von Benutzern vorgenommenen Änderungen enthält. Zusätzlich sendet jeder Agent regelmäßig Statusinformationen an den Policy Server. Berichte zu diesen Daten können über die Policy Server-Konsole generiert werden.

Data Vaults befinden sich auf Dateiservern. Zur Leistungsoptimierung sollte keine weitere Notebook Extension-Software außer der darauf ausgeführten Cleanup-Software verwendet werden.

Wenn Sie Active Directory verwenden, können Sie den Policy Server so konfigurieren, dass er auf Ihre Gruppen und Organisationseinheiten zugreift. Anschließend können Sie den Benutzern auf der Grundlage ihrer Zugehörigkeit zu Gruppen oder Organisationseinheiten Data Vaults zuweisen. Auch in Berichten können Sie Benutzer auf der Grundlage ihrer Zugehörigkeit auswählen.

Notebook Extension installieren – Übersicht

Die Installation von Notebook Extension umfasst drei Schritte:

1. Installieren Sie den Notebook Extension Policy Server.

Informationen hierzu finden Sie in [Kapitel 2](#) auf Seite 15

2. Konfigurieren Sie Schutzrichtlinien.

Informationen hierzu finden Sie in [Kapitel 3](#) auf Seite 19

3. Installieren Sie die Notebook Extension-Agenten auf den Notebooks und Desktop-PCs.

Informationen hierzu finden Sie in [Kapitel 4](#) auf Seite 33

Voraussetzungen

Policy Server

Informationen zu unterstützten Betriebssystemen finden Sie in der Supportmatrix.



HINWEIS:

Der Policy Server wird bei der Installation in einem 64-Bit-Windows-Betriebssystem im 32-Bit-Kompatibilitätsmodus ausgeführt.

Auf dem Server muss Folgendes installiert sein:

- Internet Information Services 5.0, 6.0 oder neuere Version mit Unterstützung für ASP.NET-Anwendungen
- Microsoft ASP.NET 2.0

Außerdem muss Folgendes auf dem Server installiert sein. Wenn diese Komponenten nicht installiert sind, wird Ihnen im Installationsassistenten angeboten, sie von der CD-ROM zu installieren.

- Microsoft Installer 3.1 oder neuere Version (erforderlich für .NET Framework 2.0 SP1).
- Microsoft .NET Framework 2.0 SP1 oder neuere Version. Der Assistent installiert Version 2.0 SP1.

- Microsoft SQL Express (wenn keine andere SQL-Version vorhanden ist)

Datenbank

Notebook Extension erfordert den Zugriff auf eine Microsoft SQL Server-Datenbank. Informationen zu unterstützten Versionen finden Sie in der Supportmatrix.

Mithilfe von Microsoft Enterprise Manager können Sie den Authentifizierungsmodus Ihrer SQL-Server-Installation wie folgt ermitteln und ändern:

1. Klicken Sie mit der rechten Maustaste auf die SQL-Server-Instanz, wählen Sie **Eigenschaften** aus, und klicken Sie auf die Registerkarte **Sicherheit**.
2. Die Option **SQL Server- und Windows-Authentifizierungsmodus** sollte bereits ausgewählt sein (nicht ausschließlich die **Windows-Authentifizierung**). Wenn dies nicht der Fall ist, aktivieren Sie die Option, und klicken Sie auf **OK**.

Alternativ können Sie während der Installation von Notebook Extension eine Instanz der Microsoft SQL Server Express Edition installieren.

Notebook Extension-Agenten

Notebook Extension-Agentensoftware kann auf Desktop-PCs und Notebooks von Benutzern installiert werden, auf denen Windows ausgeführt wird. Informationen zu unterstützten Plattformen finden Sie in der Supportmatrix.

2 Notebook Extension-Policy Server installieren

Schnellinstallation

Im Abschnitt **“Policy Server”** auf Seite 13 finden Sie Informationen zu den Voraussetzungen für den Notebook Extension-Policy Server.

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der CD-ROM doppelt auf `setup.hta` klicken.
2. Befolgen Sie die angezeigten Anweisungen.
3. Der Notebook Extension-Policy Server benötigt Zugriff auf eine Microsoft SQL Server-Datenbank. Wählen Sie **Vorhandene DataProtectorNE-Instanz von Microsoft SQL Server Express verwenden** oder **Vorhandene Instanz von Microsoft SQL Server verwenden** aus. Wenn Sie auswählen, dass ein vorhandener SQL-Server verwendet werden soll, müssen Sie die Verbindungszeichenfolge für den Datenbankserver und Anmeldeinformationen für ein Konto mit ausreichenden Rechten zum Erstellen einer neuen Datenbank angeben.
4. Klicken Sie auf der Seite **Data Protector Notebook Extension Policy Server installieren** des Assistenten auf **Installieren**, um die Installation zu starten.
5. Wenn die Installation abgeschlossen ist, müssen Sie die Cleanup-Software installieren. Klicken Sie in der Anzeige **Data Protector Notebook Extension Data Vault Cleanup installieren** auf **Installieren**.
6. Wenn die Installation abgeschlossen ist, klicken Sie auf **Weiter**. Anschließend können Sie die Policy Server-Konsole von Notebook Extension starten.

 **HINWEIS:**

Während der Installation wird auf dem Policy Server die Cleanup-Software installiert. Zur Optimierung der Leistung wird empfohlen, diese auch in den Data Vaults zu installieren.

Benutzerdefinierte Installation

 **HINWEIS:**

Der Notebook Extension-Policy Server kann nur dann von einer im Netzwerk freigegebenen CD-ROM oder von einer Netzwerkdateifreigabe installiert werden, wenn die Laufzeitsicherheitsrichtlinie für NET 2.0 Framework bei diesem Server für die Sicherheitszone "Lokales Intranet" auf *Voll vertrauenswürdig* eingestellt ist. Wenn Ihr Server nicht über ein lokales CD-ROM-Laufwerk verfügt, ändern Sie die Laufzeitsicherheitsrichtlinie für die Sicherheitszone "Lokales Intranet" mithilfe des in den Verwaltungstools enthaltenen Konfigurationstools für .NET Framework 2.0 in *Voll vertrauenswürdig* oder kopieren Sie den Ordner "Server" von der CD auf eine lokale Festplatte auf dem Server.

Um die Notebook Extension-Policy Server-Installation durchführen zu können, müssen Sie bei einem Konto mit "Administrator"-Rechten angemeldet sein.

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Wenn der Installationsassistent nicht automatisch gestartet wird, starten Sie ihn manuell, indem Sie im Stammverzeichnis der CD-ROM doppelt auf `setup.hta` klicken.
2. Klicken Sie auf **Policy Server installieren**.
Wenn eine entsprechende Abfrage angezeigt wird, wählen Sie **Öffnen** (oder **Ausführen**) aus, um das Programm an der aktuellen Speicherposition zu öffnen bzw. auszuführen. Wählen Sie nicht die Option **Speichern** aus.
3. Der Notebook Extension-Policy Server erfordert .NET Framework 2.0 SP1. Wenn dies noch nicht installiert ist, werden Sie gefragt, ob Sie es von der CD-ROM installieren möchten.
Die Installation erfordert Windows Installer 3.1 oder eine neuere Version. Falls diese Anwendung nicht installiert ist, werden Sie gefragt, ob Sie Windows Installer 3.1 von der CD installieren möchten.
4. Der Installationsassistent prüft, ob die folgende erforderliche Software installiert ist:

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

Wenn eine dieser Komponenten nicht vorhanden ist, klicken Sie auf den entsprechenden Eintrag in der Liste, um Informationen zur Installation zu erhalten. Klicken Sie auf **Weiter**.

5. Installieren Sie Microsoft SQL Server.

So verwenden Sie eine vorhandene Instanz von Microsoft SQL Server:

- Klicken Sie auf **Vorhandene Instanz von Microsoft SQL Server verwenden**.
- Geben Sie im Feld **Datenbankserver** die Verbindungszeichenfolge für den vorhandenen Datenbankserver ein.
- Geben Sie in die Felder **Benutzername** und **Passwort** die Anmeldedaten für ein Konto mit ausreichenden Rechten zum Erstellen einer neuen Datenbank ein. In der Regel ist dies das Konto für den Systemadministrator.
- Klicken Sie auf **Weiter**. Mit den eingegebenen Verbindungsinformationen wird ein Test der Verbindung zum vorhandenen Datenbankserver durchgeführt. Wenn der Test erfolgreich ist, geht der Assistent zu Schritt 6 über.

So installieren Sie die Notebook Extension-Instanz der Microsoft SQL Server Express Edition:

- Wählen Sie **DataProtectorNE-Instanz von Microsoft SQL Server Express installieren** aus, und klicken Sie auf **Weiter**.
- Klicken Sie auf **Installieren**, um eine Instanz von Microsoft SQL Server 2005 Express Edition mit dem Namen "DataProtectorNE" zu installieren. Klicken Sie auf **Weiter**, wenn die Installation abgeschlossen ist.

6. Installieren Sie die Policy Server-Software von Notebook Extension.

- Klicken Sie auf der Eingangsanzeige auf **Weiter**, um die Installation zu starten.
 - Die Policy Server-Konsole von Notebook Extension wird als Webanwendung im virtuellen Verzeichnis `C:\Inetpub\wwwroot\dpnepolicy` installiert.
 - Der Webservice von Notebook Extension wird unter `C:\Inetpub\wwwroot\dpnepolicyservice` installiert.

Beide verwenden das HTTP-Protokoll an Port 80.
- Klicken Sie auf **Schließen** und **Weiter**, wenn die Installation des Policy Servers abgeschlossen ist.

7. Anschließend muss das Cleanup-Programm installiert werden. Klicken Sie auf **Installieren**, um die Installation zu starten.

8. Wenn die Cleanup-Installation abgeschlossen ist, klicken Sie auf **Weiter**.

Notebook Extension wird zentral über die Policy Server-Konsole von Notebook Extension verwaltet. Da die Konsole browserbasiert ist, können Sie Notebook Extension von jedem Computer aus verwalten, der eine Browserverbindung zum Policy Server herstellen kann (über HTTP-Port 80).

Um die Policy Server-Konsole von Notebook Extension mit einem Browser auf dem Policy Server auszuführen, lassen Sie die Option **Data Protector Notebook Extension Policy Server Console ausführen** markiert, und klicken Sie auf **Fertig stellen**.



HINWEIS:

Während der Installation wird auf dem Policy Server die Cleanup-Software installiert. Zur Optimierung der Leistung empfiehlt es sich außerdem, die Software in den Data Vaults zu installieren.

3 Notebook Extension-Schutzrichtlinien konfigurieren

Ersteinrichtung nach der Installation von Notebook Extension

Direkt nach der Installation von Notebook Extension wird das Fenster für die Ersteinrichtung angezeigt. Bevor Sie die Policy Server-Konsole öffnen und Notebook Extension ausführen können, müssen Sie drei Konfigurationsschritte ausführen:

- **Geben Sie die Informationen zu einem HP Data Protector Cell Manager im Netzwerk ein.**

Bevor Notebook Extension gestartet werden kann, muss eine Verbindung zum Cell Manager hergestellt werden. Klicken Sie auf **HP Data Protector Cell Manager einrichten**, um die Informationen einzugeben.

- **Definieren oder importieren Sie ein Verschlüsselungspasswort.**

Aus Sicherheitsgründen müssen Sie ein Verschlüsselungspasswort definieren, bevor Sie Notebook Extension verwenden können. Damit wird sichergestellt, dass alle Dateien auf dem Benutzercomputer verschlüsselt werden und verschlüsselt über das Netzwerk übertragen werden. Es wird dasselbe Passwort verwendet, um die Dateien aller Benutzer und aller zentral konfigurierten Data Vaults zu verschlüsseln.

- Zentral (über die Policy Server-Konsole) definierte Data Vaults verwenden zur Verschlüsselung immer das Notebook Extension-Verschlüsselungspasswort.
- Bei lokal (von Benutzern über deren Computer) definierten Data Vaults können die Benutzer jeweils auswählen, ob die Verschlüsselung verwendet werden soll, und eigene Passwörter festlegen.

Bei der Erstinstallation von Notebook Extension müssen Sie ein Passwort **generieren** oder **importieren**, bevor Sie fortfahren können. Nach der Generierung eines

Passworts sollten Sie dieses zur Sicherheit **exportieren**. Dabei wird es an einem gesicherten Speicherort gespeichert. Später können Sie es zum Importieren verwenden.

Klicken Sie auf **Verschlüsselungsrichtlinie festlegen**, um das Passwort zu verwalten, und befolgen Sie die angezeigten Anweisungen.



HINWEIS:

Nachdem ein Passwort generiert oder importiert wurde, kann es nicht mehr geändert werden.

- **Lizenzieren Sie Data Protector Notebook Extension.**

Mit der Testversion von Notebook Extension können Sie 60 Tage lang Notebook Extension ohne weitere Lizenzierung eine beliebige Anzahl von Benutzern schützen. Wenn Sie Notebook Extension kaufen, müssen Sie den "HP License Key Delivery Service" unter <https://webware.hp.com/welcome.asp> öffnen, um einen Lizenzschlüssel herunterzuladen, den Sie dann eingeben können. Sie können die folgenden Lizenzen kaufen:

- TA032AA oder TA032AAE für 100 Agenten
- TA033AA oder TA033AAE für 1000 Agenten

Sie müssen vor dem Ende der Testperiode einen dauerhaft gültigen Lizenzschlüssel eingeben. Wenn Sie dies nicht tun, können die Agenten nach 60 Tagen keine Daten mehr in ihre Local Repositories oder Data Vaults kopieren. Allerdings können zuvor geschützte Dateiversionen immer noch wiederhergestellt werden.

Klicken Sie zur Verwaltung der Lizenzen auf **Lizenzverwaltung** und auf **Geben Sie einen Lizenzschlüssel für Benutzer von Data Protector Notebook Extension ein**. Befolgen Sie die angezeigten Anweisungen.



HINWEIS:

Lizenzen werden an Agenten verteilt, wenn die Agenten installiert werden.

Nach Abschluss dieser Konfigurationsschritte steht Ihnen der volle Funktionsumfang der Policy Server-Konsole zur Verfügung. Wenn Sie Notebook Extension soeben erst installiert haben, konfigurieren Sie die weiteren Elemente von Notebook Extension in der unten angegebenen Reihenfolge.

Erstkonfiguration

In Notebook Extension sind verschiedene Richtlinien vorkonfiguriert, die für die meisten Organisationen ausreichen. Es wird empfohlen, zuerst die Data Vault-, Kopie- und Dateischutzrichtlinien zu konfigurieren und anschließend die Notebook Extension-Agentensoftware auf den Desktop-PCs und Notebooks der Benutzer zu installieren.



HINWEIS:

Statt neue Richtlinien zu konfigurieren, können Sie auch die vorkonfigurierten Richtlinien von Notebook Extension ändern. Klicken Sie einfach auf **Vorhandene Richtlinie bearbeiten**, statt in den einzelnen Schritten jedes Mal **Neue Richtlinie erstellen** auszuwählen.

Die Schutzrichtlinien für Ihre Installation konfigurieren Sie über die Policy Server-Konsole. Die Richtlinien, die Sie zentral definieren, werden an alle Notebook Extension-Agenten verteilt und auf den Desktop-PCs und Notebooks der Benutzer ausgeführt.

1. Sie können die Policy Server-Konsole von Notebook Extension nach Abschluss des Installationsassistenten ausführen oder zu jedem beliebigen anderen Zeitpunkt über die folgende URL aufrufen:

`http://policyserver/dpnepolicy/`

wobei "policyserver" der Name Ihres Notebook Extension-Policy Servers ist. Sie müssen als "Administrator" beim Server angemeldet sein.

2. **Data Vault-Richtlinien konfigurieren.**

In Data Vault-Richtlinien wird das Speicherziel für die kontinuierliche Sicherung von durch Richtlinien geschützten Benutzerdateien angegeben. Wenn eine Datei geändert wird, können die Vorgängerversion und die geänderte Datei automatisch an einem oder mehreren Speicherzielen gesichert werden. Ein Zielort ist meistens eine Netzwerkfreigabe. Jeder Benutzergruppe können ein oder mehrere Data Vaults zugewiesen werden. Sie können beispielsweise eine Data Vault-Richtlinie mit dem Namen *Sales* definieren und diese Ihren Benutzergruppen *Dallas.Sales*, *San Francisco.Sales*, *Chicago.Sales* und *Atlanta.Sales* zuordnen.

Voraussetzungen für Data Vaults:

Notebook Extension verwendet zum Speichern der geschützten Dateien, die von den Desktop-PCs und Notebooks der Benutzer gesichert werden, normale Windows-Dateifreigaben. Die Dateifreigaben sollten sich auf einem Windows

Dateiserver befinden, der sich nicht auf demselben Computer wie der Policy Server befinden muss. Wenn Sie jedoch nur die Testversion von Notebook Extension mit einer kleineren Anzahl von installierten Agenten verwenden, ist es möglicherweise praktischer, für den Policy Server und den Data Vault-Dateiserver denselben Computer zu verwenden.

Notebook Extension legt für die auf dem Dateiserver gesicherten Dateien die gleichen Zugriffsberechtigungen (ACLs) fest, die für die Originaldatei gelten. Dies bedeutet, dass die Benutzer gesicherte Dateien nur wiederherstellen können, wenn Sie die ursprünglichen Dateien auf ihren Computern öffnen können.

So erstellen Sie eine Data Vault-Richtlinie:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Data Vault-Richtlinie festlegen**.
- c. Klicken Sie auf **Neue Data Vault-Richtlinie erstellen**.
- d. Befolgen Sie die angezeigten Anweisungen.



HINWEIS:

Wenn Sie einen Data Vault erstellen, darf der Pfad des Ordners oder der Freigabe nicht länger als 66 Zeichen sein.

Empfohlene Einstellungen:

Lassen Sie die Einstellung für "Kopierrichtlinie" zunächst unverändert bei "Standard".

Für das Cleanup:

- Wenn sich der Data Vault auf diesem Policy Server befindet, lassen Sie die Standardeinstellung für den Namen des Computers unverändert.
- Wenn sich der Data Vault auf einem anderen Windows-Dateiserver befindet, installieren Sie die Cleanup-Software für Data Vaults auf diesem Server, und geben Sie diesen Computer als Cleanup-Computer an.

3. Kopierrichtlinien konfigurieren.

Eine Kopierrichtlinie begrenzt die Anzahl der Benutzercomputer, die gleichzeitig in einen Data Vault kopieren können. Außerdem definiert sie Anfangsaktualisierungen und geplante Aktualisierungen des Data Vaults zur Ergänzung der kontinuierlichen Sicherung. Jede Kopierrichtlinie kann einem oder mehreren Data Vaults zugewiesen werden.

Kopierrichtlinien definieren Folgendes:

- Anzahl der Agenten, die gleichzeitig Dateien auf Ihre Data Vaults kopieren können.

- Zeitplan für regelmäßige Aktualisierungen, bei denen geprüft wird, ob alle erwarteten Dateien für einen Benutzer auf dem Data Vault vorhanden sind. Falls dies nicht der Fall ist, werden die fehlenden Dateien kopiert. Damit wird noch einmal sichergestellt, dass alle Benutzerdateien ordnungsgemäß auf den Data Vault kopiert wurden.
- Ob eine **Anfangsaktualisierung** (oder -kopie) durchgeführt werden soll. Die Anfangsaktualisierung wird benötigt, da während des normalen Betriebs von Notebook Extension nur Informationen über die Änderungen in den Data Vault kopiert werden, wenn ein Benutzer eine im Continuous-Modus geschützte Datei von Notebook Extension ändert.

Die Standard-Kopierrichtlinie gilt für alle Data Vaults, für die keine eigenen Kopier Richtlinien festgelegt sind. Die Einstellungen der Standard-Kopierrichtlinie können geändert werden, umbenannt oder gelöscht werden kann sie jedoch nicht.

So erstellen Sie eine Kopierrichtlinie:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Kopier Richtlinien festlegen**.
- c. Klicken Sie auf **Neue Kopierrichtlinie erstellen**.
- d. Befolgen Sie die angezeigten Anweisungen.

Empfohlene Einstellungen:

- **Drosseln:** Geben Sie als Zeitraum Ihre normalen Geschäftszeiten an, und legen Sie für andere Zeiten eine geringere Drosselungsgrenze fest.
- **Anfangsaktualisierung:** Aktivieren Sie die Anfangsaktualisierung, um sicherzustellen, dass alle gemäß den Dateischutzrichtlinien geschützten Benutzerdateien gesichert werden.
- **Dateien wöchentlich/monatlich aktualisieren:** Da eine Aktualisierung nur wenige oder gar keine Dateikopien beinhalten sollte, aktivieren Sie die Data Vault-Aktualisierungen, um sicherzustellen, dass alle durch Richtlinien geschützten Benutzerdateien ordnungsgemäß gesichert werden.

4. Konfigurieren Sie Dateischutzrichtlinien.

Mit Dateischutzrichtlinien können Sie angeben, welche Dateien geschützt werden und wie lange Vorgängerversionen aufbewahrt werden sollen. Sie können beispielsweise eine Dateischutzrichtlinie mit dem Namen *Office-Dokumente* für Word-Dokumente, Excel-Dateien und PowerPoint-Präsentationen definieren.

Auf lokalen Festplatten gespeicherte Dateien werden immer geschützt.

Es gibt zwei verschiedene Typen von Richtlinien:

- **Continuous File Protection** – bietet Echtzeitschutz für Dateien bei jedem Speichern oder Löschen. Im Allgemeinen sollten alle Dateien oder Dokumente,

bei denen Sie über ein Menü die Option **Speichern** auswählen können, mit einer Continuous File Protection-Richtlinie geschützt werden.

Notebook Extension enthält drei Beispiele: *Office-Dokumente*, *Software-Entwicklung* und *Webdokumente*. Sie können diese Richtlinien als Ausgangspunkt verwenden oder eigene erstellen.

- **Open File Protection**– schützt die Dateien, indem in regelmäßigen Abständen (in der Regel einmal pro Stunde) eine "Momentaufnahme" von der Datei gemacht wird. Normalerweise sollte jede Datei, die entweder sehr groß ist (über 100 MB), die den größten Teil des Tages geöffnet ist oder die nicht über die Menüoption **Speichern** verfügt, mit diesem Verfahren geschützt werden. Häufig vorkommende Dateien diesen Typs sind E-Mail- und Datenbankdateien.

In Notebook Extension sind dazu zwei Beispiele vorhanden: *Microsoft Outlook* und *Microsoft Outlook Express*. Sie können diese Richtlinien als Ausgangspunkt verwenden oder eigene erstellen.

So erstellen Sie eine Dateischutzrichtlinie:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Dateischutzrichtlinien festlegen**.
- c. Klicken Sie entweder auf **Neue Continuous File Protection-Richtlinie erstellen** oder auf **Neue Open File Protection-Richtlinie erstellen**.
- d. Befolgen Sie die angezeigten Anweisungen.



HINWEIS:

Achten Sie beim Erstellen von Kopierichtlinien und beim Festlegen von Ausschluss- und Einschlussregeln darauf, dass Dateierweiterungen bei den Richtlinien für Open File Protection nicht länger als 9 Zeichen und bei den Richtlinien für Continuous File Protection nicht länger als 29 Zeichen sein dürfen.

❗ **WICHTIG:**

Zu diesem Zeitpunkt haben Sie alle grundlegenden Richtlinien konfiguriert, die von Notebook Extension benötigt werden. In Notebook Extension sind noch weitere Richtlinien vorkonfiguriert, die für die meisten Organisationen ausreichen. Es wird empfohlen, zu diesem Zeitpunkt mit der Installation der Agenten auf den Desktop-PCs und Notebooks Ihrer Benutzer zu beginnen (siehe [Kapitel 4](#) auf Seite 33). Später können Sie die restlichen Notebook Extension-Richtlinien prüfen und konfigurieren, z. B. die Richtlinien für das Cleanup, die Benutzerkontrolle, die Agentenaktualisierung und der Erhalt von Berichtsdaten.

Weitere Richtlinien konfigurieren

1. Konfigurieren Sie den Active Directory-Zugriff.

Wenn Sie Data Vaults bestimmten Gruppen oder Organisationseinheiten zuweisen oder Berichte für bestimmte Gruppen oder Organisationseinheiten erstellen möchten, müssen Sie den Policy Server so konfigurieren, dass er auf Ihr Active Directory zugreifen kann.

Durch das Konfigurieren des Active Directory-Zugriffs wird die Option **Mitglieder von Gruppen und Organisationseinheiten** für Data Vaults aktiviert (siehe ["Erstkonfiguration"](#) auf Seite 21).

So konfigurieren Sie den Active-Directory-Zugriff:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Konfiguration**.
- b. Klicken Sie auf **Active-Directory-Zugriff konfigurieren**.
- c. Befolgen Sie die angezeigten Anweisungen.

2. Konfigurieren Sie die Cleanup-Richtlinie.

Für die Local Repositories auf den Benutzercomputern und die Data Vaults auf den Dateiservern muss regelmäßig ein Cleanup durchgeführt werden, um Versionen zu entfernen, die gemäß den Erhalteeinstellungen in den Dateischutzrichtlinien zu alt sind.

So konfigurieren Sie die Cleanup-Richtlinie:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Cleanup-Richtlinie festlegen**.
- c. Befolgen Sie die angezeigten Anweisungen.

Empfohlene Einstellungen:

- **Cleanup-Zeitplan für Local Repository:** Behalten Sie den Standardwert von 1 Stunde bei.

- **Cleanup-Zeitplan für Data Vault:** Die Standardeinstellung (Cleanup täglich um Mitternacht) sollte für die meisten Installationen geeignet sein.

3. Konfigurieren Sie die Benutzerkontrollrichtlinie.

Die Benutzerkontrollrichtlinie bestimmt, wie viel Kontrolle die Benutzer über die Unternehmensrichtlinien haben, die an ihre Computer verteilt wurden.

So konfigurieren Sie die Benutzerkontrollrichtlinie:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Benutzerkontrollrichtlinie festlegen**.
- c. Befolgen Sie die angezeigten Anweisungen.

Empfohlene Einstellungen:

Wählen Sie für **Selbständige Wiederherstellung** die Einstellung **Benutzerkontrolle zulassen** aus. Alle anderen Richtlinien können Sie **ausblenden**.

4. Konfigurieren Sie die Richtlinie für die Agentenaktualisierung.

Die Richtlinie gibt an, welche Version des Notebook Extension-Agenten auf allen von Notebook Extension geschützten Desktop-PCs und Notebooks verwendet werden soll. Der Agent wird auf allen Computern automatisch auf diese Version aktualisiert.

So konfigurieren Sie die Agentenaktualisierungsrichtlinie:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
- b. Klicken Sie auf **Agentenaktualisierungsrichtlinie festlegen**.
- c. Befolgen Sie die angezeigten Anweisungen.

5. Erhalt von Berichtsdaten konfigurieren.

Damit wird für jede Hauptkategorie von Informationen festgelegt, wie lange die Daten für Berichtszwecke aufbewahrt werden sollen.

So konfigurieren Sie den Erhalt von Berichtsdaten:

- a. Klicken Sie im Navigationsbereich auf der linken Seite auf **Konfiguration**.
- b. Klicken Sie auf **Erhalt von Berichtsdaten konfigurieren**.
- c. Befolgen Sie die angezeigten Anweisungen.

Weitere Konfigurationsschritte

Diese Schritte werden normalerweise bei der Erstinstallation von Notebook Extension durchgeführt.

Lizenzieren Sie Ihre Notebook Extension-Software.

Mit der Testversion von Notebook Extension können Sie 60 Tage lang Notebook Extension ohne weitere Lizenzierung eine beliebige Anzahl von Benutzern schützen. Wenn Sie Notebook Extension kaufen, müssen Sie den "HP License Key Delivery Service" unter <https://webware.hp.com/welcome.asp> öffnen, um einen Lizenzschlüssel herunterzuladen, den Sie dann eingeben können.

So geben Sie ein Lizenzpasswort ein:

1. Klicken Sie im Navigationsbereich auf der linken Seite auf **Lizenzverwaltung**.
2. Klicken Sie auf **Geben Sie ein Passwort für Benutzer von Data Protector Notebook Extension ein**.
3. Befolgen Sie die angezeigten Anweisungen.



HINWEIS:

Lizenzen werden an Agenten verteilt, wenn die Agenten installiert werden.

Lizenzen verschieben

Wenn Sie eine IP-Adresse des Policy Servers ändern müssen, um den Server in ein anderes System zu verschieben, oder wenn Sie Lizenzen von einem Policy Server zu einem anderen verschieben müssen, kontaktieren Sie den "HP License Key Delivery Service" unter <https://webware.hp.com/welcome.asp>, um die Lizenzen zu aktualisieren.

Definieren, importieren und exportieren Sie ein Verschlüsselungspasswort.

Aus Sicherheitsgründen müssen Sie ein Verschlüsselungspasswort definieren, bevor Sie Notebook Extension verwenden können. Damit wird sichergestellt, dass alle Dateien auf dem Benutzercomputer verschlüsselt werden und verschlüsselt über das Netzwerk übertragen werden. Es wird dasselbe Passwort verwendet, um die Dateien aller Benutzer und aller zentral konfigurierten Data Vaults zu verschlüsseln.

- Zentral (über die Policy Server-Konsole) definierte Data Vaults verwenden zur Verschlüsselung immer das Notebook Extension-Verschlüsselungspasswort.
- Bei lokal (von Benutzern über deren Computer) definierten Data Vaults können die Benutzer eigene Passwörter auswählen und festlegen, ob die Verschlüsselung verwendet werden soll.

Bei der Erstinstallation von Notebook Extension müssen Sie entweder ein Passwort generieren oder eines importieren, bevor Sie fortfahren können. Nach der Generierung eines Passworts sollten Sie dieses zur Sicherheit exportieren. Dabei wird es an einem sicheren Speicherort abgelegt. Später können Sie es zum Importieren verwenden.

 **HINWEIS:**

Nachdem ein Passwort generiert oder importiert wurde, kann es nicht mehr geändert werden.

So verwalten Sie ein Verschlüsselungspasswort:

1. Klicken Sie im Navigationsbereich auf der linken Seite auf **Richtlinien**.
2. Klicken Sie auf **Verschlüsselungsrichtlinie**.
3. Befolgen Sie die angezeigten Anweisungen.

Anzahl der unterstützten Agenten festlegen

Es ist nicht ganz einfach, generelle Regeln festzulegen, die für alle Umgebungen zutreffen. Daher wird in den hier erläuterten Fällen klar der Kontext beschrieben, für den die angegebenen Zahlen zutreffen.

Faktoren für die Größenbestimmung

Die Größenbestimmung in einer Notebook Extension-Umgebung ist sehr komplex. Es gibt u.a. folgende technische Faktoren, die die Anzahl der Benutzer beeinflussen, die in einer bestimmten Umgebung unterstützt werden können:

- Die Verarbeitungsleistung in einem Data Vault (bei der Konsolidierung der Sicherungsdaten in der Nacht)
- Netzwerk- und E/A-Bandbreite auf dem Data Vault-Server
- Plattenspeicherplatz auf dem Data Vault-Server
- Größe der SQL Server-Datenbank auf dem Policy Server
- Netzwerkbandbreite und Verarbeitungsleistung auf dem Policy Server

Welcher dieser Faktoren einen Engpass in einer bestimmten Installation darstellen kann, wird durch die Konfigurationseinstellungen und Nutzungsmuster in Notebook Extension bestimmt:

- Anzahl der Benutzer in einem Data Vault
- Anzahl und Größe der von den Dateischutzrichtlinien abgedeckten Richtlinien
- Änderungshäufigkeit der geschützten Dateien
- Erhalteeinstellungen für geschützte Dateitypen

Empfehlungen für die Größenbestimmung

Data Vault

Folgende Hardwarespezifikationen bilden eine solide Basis für einen Data Vault:

- 1 x 3 GHz Dual-Core-Prozessor
- 2 GB RAM
- 1,5 TB Festplattenspeicherkapazität

Ein solcher Data Vault kann eine Benutzerpopulation von bis zu **1.000** Agenten unterstützen, wenn sich das durchschnittliche Datenaufkommen wie folgt charakterisieren lässt:

- Anzahl der geschützten Dateien: 3000
- Durchschnittliche Gesamtgröße der geschützten Dateien auf lokalen Festplatten: 4 GB¹
- Durchschnittliche Gesamtgröße auf dem Data Vault (komprimiert): 1 GB

Wenn Sie durchschnittlich mehr Daten schützen müssen, als in diesem Beispiel angegeben, ist es gegebenenfalls besser, die Endbenutzerdaten auf mehrere Data Vaults zu verteilen. Eine einfache Erhöhung der Festplattenkapazität auf dem Data Vault schafft mehr Platz für Daten, aber der Data Vault kann die Konsolidierung der Sicherungsdaten in der Nacht nicht mehr auf effiziente Weise durchführen.

Wenn Ihre Benutzer im Durchschnitt weniger Daten haben, können Sie eventuell mehr als 1.000 Benutzer auf einem Data Vault hosten.



HINWEIS:

Um die bestmögliche Leistung zu erzielen, empfiehlt HP, das Betriebssystem auf dem Data Vault und die Sicherungsdaten auf physisch getrennten Festplatten zu speichern.

Policy Server

Die Menge des Datenverkehrs, der auf dem Policy Server generiert wird, hängt direkt von der Anzahl Agenten ab, die von einem Server gehostet werden. Die in DPNE

¹Ausgehend von einer Mischung aus 3,5 GB für Dateien mit Continuous File Protection und 0,5 GB für Dateien mit Open File Protection

enthaltene Express Edition von MS SQL Server legt eine maximale Datenbankgröße von 4 GB fest, wobei nicht mehr als 5.000 Agenten² unterstützt werden können.

Wenn Sie mehr als 5.000 Agenten in Ihrer Umgebung unterstützen müssen, können Sie entweder zusätzliche Policy Server einsetzen oder MS SQL Express durch eine Vollversion von Microsoft SQL Server ersetzen. Auf diese Art kann der Policy Server ohne weiteres bis zu 50.000 Agenten unterstützen. Wenn Sie die Vollversion von MS SQL Server verwenden möchten, sollten Sie den Hauptspeicher der Policy Server auf mindestens 3 GB aufrüsten.

Ein Policy Server kann auf demselben Server wie der Data Vault oder getrennt ausgeführt werden.

Es wird mindestens ein Policy Server benötigt, aber nicht unbedingt eine identische Anzahl von Data Vaults und Policy Servern.

Überlegungen bei Netzwerken

Normalerweise empfiehlt HP die Durchführung einer Anfangsaktualisierung von Notebook Extension-Agenten auf Data Vaults nicht, wenn die Latenz (Verzögerungszeit) des Netzwerks zwischen den beiden höher als 50 ms ist. Dies gilt in der Regel für Home oder Remote Offices mit einer langsamen WAN-Verbindung. Die Anfangsaktualisierung funktioniert zwar, dauert aber sehr lange.

Wenn Ihre Umgebung Büros an mehreren Standorten umfasst und die Netzwerklatenz für einige von diesen größer als 50 ms ist, sollten Sie Data Vaults an mehr als einem Ort installieren, damit alle Büros mindestens einen Data Vault mit einer Latenz von 50 ms oder weniger erreichen können.

Sobald die Anfangsaktualisierung beendet ist, können von jedem Standort in Ihrem Unternehmensnetzwerk oder sogar von einem Home Office aus Aktualisierungen durchgeführt werden. Diese sind in der Regel klein genug, damit sie auch über langsame Netzwerkverbindungen gut funktionieren.

Wenn die Anfangsaktualisierung über eine Hochlatenzverbindung durchgeführt werden muss, kann dies mehrere Tage in Anspruch nehmen. Sie kann jedoch ohne Probleme unterbrochen werden. Die Aktualisierung wird von Notebook Extension an dem Punkt wieder aufgenommen, an dem sie unterbrochen wurde, sobald die Verbindung zum Data Vault wiederhergestellt wird.

²Unter Verwendung der Standardeinstellung für die "Erhalt von Berichtsdaten" auf dem Policy Server von 30 Tagen.

 **TIPP:**

Wenn Sie nicht wissen, wie hoch die Latenz zwischen Ihren Büros ist, verwenden Sie den `ping`-Befehl von einem Computer an einem Standort, um die Erreichbarkeit eines Computers an einem anderen Standorts sowie die Dauer des Datenverkehrs zwischen den beiden festzustellen. Bei jedem erfolgreichen `ping`-Befehl wird die Latenz angegeben.

4 Notebook Extension-Agenten installieren



HINWEIS:

Lizenzen werden an Agenten verteilt, wenn die Agenten installiert werden.

Es gibt zwei Möglichkeiten, Notebook Extension-Agenten zu installieren:

- Installation auf allen Benutzercomputern einzeln. Informationen hierzu finden Sie in ["Notebook Extension-Agenten auf einzelnen Benutzercomputern installieren"](#) auf Seite 33
- Unternehmensweite Bereitstellung über einen Dateiserver, auf den alle Benutzercomputer zugreifen können. Informationen hierzu finden Sie in ["Notebook Extension-Agenten unternehmensweit bereitstellen"](#) auf Seite 35

Notebook Extension-Agenten auf einzelnen Benutzercomputern installieren

Voraussetzungen

Notebook Extension-Agentensoftware kann auf Desktop-PCs und Notebooks von Benutzern installiert werden, auf denen Windows ausgeführt wird. Informationen zu unterstützten Plattformen finden Sie in der Supportmatrix.

Sie müssen mit einem Konto mit Administratorrechten angemeldet sein.

Installationsprozedur

1. Legen Sie die CD-ROM für die Installation von Notebook Extension ein. Der Installationsassistent sollte automatisch gestartet werden. Andernfalls starten Sie

ihn manuell, indem Sie im Stammverzeichnis der CD-ROM doppelt auf `setup.hta` klicken.

2. Klicken Sie auf **Data Protector Notebook Extension Agentensoftware installieren oder aktualisieren**. Wenn ein Dialogfeld zum Öffnen oder Speichern angezeigt wird, wählen Sie **Öffnen** (bzw. **Ausführen**) aus.
3. Wenn auf dem Benutzercomputer nicht Microsoft Windows Installer 3.1 oder eine neuere Version installiert ist, bietet der Assistent die Installation an. Wenn das Dialogfeld für die Aktualisierung von Windows Installer angezeigt wird, klicken Sie auf **OK**, um die Installation zu starten.
4. Wenn auf dem Benutzercomputer nicht Microsoft .NET Framework 2.0 SP1 oder eine neuere Version installiert ist, bietet der Assistent die Installation an. Wenn das Dialogfeld für die Installation von Microsoft .NET Framework 2.0 SP1 angezeigt wird, klicken Sie auf **OK**, um die Installation zu starten.

Nach Abschluss der Installation und der Konfiguration werden Sie aufgefordert, einen Neustart Ihres Systems durchzuführen, falls auf dem Policy Server eine Open File Protection-Richtlinie definiert ist. Klicken Sie auf **Neustart**.

5. Der Assistent installiert den Notebook Extension-Agenten automatisch. Befolgen Sie die angezeigten Anweisungen. Während der Installation werden Sie aufgefordert, Informationen zum Policy Server einzugeben.
6. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**. In der Taskleiste sollte jetzt ein Notebook Extension-Symbol angezeigt werden.
7. Überprüfen Sie wie folgt, ob der Notebook Extension-Agent ordnungsgemäß funktioniert:
 - a. Öffnen oder erstellen Sie eine Testdatei, wie z. B. ein Word-Dokument oder eine Excel-Datei, und legen Sie sie beispielsweise auf dem Desktop ab. Nehmen Sie einige Änderungen vor, und klicken Sie auf **Speichern**.
 - b. Klicken Sie auf dem Desktop, im Windows Explorer oder in einem Dialogfeld zum Öffnen einer Datei mit der rechten Maustaste auf die Testdatei. Im Menü, das daraufhin geöffnet wird, sollten drei Notebook Extension-Einträge angezeigt werden (**Dateien finden und wiederherstellen...**, **Version kopieren** und **Version öffnen mit XXX**).
 - c. Wählen Sie **Version öffnen mit XXX...** aus. Daraufhin sollte eine Liste der Versionen des soeben erstellten oder bearbeiteten Dokuments, jeweils mit Zeitmarke versehen, angezeigt werden. Wenn Sie eine der Versionen auswählen, wird das Dokument in der entsprechenden Anwendung im Nur-Lese-Modus geöffnet. Auf diese Weise kann ein Benutzer eine ältere Version eines seiner Dokumente aus dem lokalen Notebook Extension-Repository wiederherstellen.

8. Wiederholen Sie die Schritte 1 bis 8 für alle anderen Desktop-PCs und Notebooks, die mit Notebook Extension geschützt werden sollen.

Notebook Extension-Agenten unternehmensweit bereitstellen

Für die Erstinstallation können Sie Notebook Extension-Agenten mithilfe des Notebook Extension Agent Deployment Kits, das auf der Installations-CD-ROM enthalten ist, unternehmensweit bereitstellen.

HINWEIS:

Sie können das Deployment Kit auf Vista-PCs, auf denen die Benutzerkontensteuerung aktiviert ist, nicht verwenden. Um dieses Problem zu beheben, deaktivieren Sie die Benutzerkontensteuerung, oder installieren Sie den Agenten interaktiv.

In der im Folgenden beschriebenen Prozedur kopieren Sie das Notebook Extension Agent Deployment Kit im Ordner `CD-ROM:\Agent` in ein Verzeichnis auf einem Dateiserver, auf das alle Benutzer zugreifen können. Anschließend erstellen Sie in diesem Verzeichnis mithilfe von `SetupConfig.exe` eine Parameterdatei. Zum Schluss richten Sie einen Mechanismus ein, mit dem die Datei `StartInstall.exe` im gemeinsam genutzten Verzeichnis von jedem Benutzercomputer aus ausgeführt werden kann. Hierfür können Sie z. B. ein Anmeldescript verwenden. Anschließend können Sie die Bereitstellung über die Policy Server-Konsole von Notebook Extension mithilfe des Agenten-Bereitstellungsberichts überwachen.

Inhalt des Kits

Das Notebook Extension Deployment Kit enthält die folgenden Komponenten:

<code>SetupConfig.exe</code>	Erstellt und bearbeitet die Initialisierungsdatei.
<code>StartInstall.exe</code>	Startet die Datei <code>Setup.exe</code> als privilegierter Benutzer.
<code>Setup.exe</code>	Installiert die Voraussetzungen und die Datei <code>DataProtectorNE.ini</code> .

DataProtectorNE.msi	Windows Installer-Paket für Notebook Extension zur Installation der Agentensoftware.
WindowsInstaller.exe	Aktualisiert Windows Installer (erforderlich für die .NET-Installation).
NetFx20SP1_x64.exe, NetFx20SP1_x86.exe	Installiert NET Framework 2.0 SP1.
Setup.ini	Konfigurationsparameterdatei für die Notebook Extension-Installation. Diese Datei wird von der Datei SetupConfig.exe (siehe Schritt 4 unten) erstellt.

Bereitstellungs- und Installationsprozedur

1. Kopieren Sie die Dateien im Verzeichnis "Agent" der Verteilungs-CD-ROM in ein Verzeichnis, auf das alle Benutzer, die das Notebook Extension Agent Deployment Kit verwenden werden, zugreifen können. Dabei kann es sich beispielsweise um ein Verzeichnis einer NetLogon-Freigabe handeln, z. B. \\IhrServer\DPNEDeploy.
2. Stellen Sie sicher, dass das neu erstellte Verzeichnis die oben aufgeführten Dateien enthält. Alle anderen Dateien können Sie löschen.
3. Öffnen Sie ein DOS-Befehlsfenster (cmd.exe) und wechseln Sie mit dem Befehl cd zu dem in Schritt 1 erstellten Verzeichnis.
4. Führen Sie die Datei SetupConfig.exe aus, um die Parameterdatei Setup.ini zu erstellen. Beim erstmaligen Ausführen der Datei SetupConfig.exe, müssen Sie für alle Parameter Werte eingeben. Danach können Sie die Datei SetupConfig.exe bei Bedarf erneut ausführen, um die Parameter zu ändern. Wenn Sie keine Parameter ändern möchten, drücken Sie einfach die Eingabetaste.

Die folgenden Parameter sind erforderlich:

- **UNC-Pfad zu den Installationspaketen** – der vollständige Pfad zum gemeinsam genutzten Verzeichnis, in das die Dateien in Schritt 1 kopiert wurden, z. B. \\IhrServer\DPNEDeploy.
- Der Name des **Notebook Extension-Policy Servers**. Dabei kann es sich um einen NetBIOS-Namen wie IHRSERVER oder einen vollständig qualifizierten Domännennamen wie IhrServer.IhreFirma.com handeln.

- **Benutzername** – der Benutzername eines Benutzers mit Administratorrechten auf den Computern, die das Notebook Extension Agent Deployment Kit verwenden, z. B. ein Mitglied aus der Gruppe der Domänenadministratoren. Dabei handelt es sich in der Regel um einen vollständig qualifizierten Benutzernamen einschließlich der Domäne, z. B. IHREFIRMA\JerryAdmin.
 - **Passwort** – das zum Benutzernamen gehörende Passwort. Dieses müssen Sie zweimal eingeben, um es zu bestätigen.
5. Führen Sie auf dem Benutzercomputer die Datei `StartInstall.exe` aus. Beispiel: `\\IhrServer\DPNEDeploy\StartInstall`. Mithilfe der Anmeldedaten (Benutzername und Passwort), die in der Datei `Setup.ini` angegeben sind, wird anschließend im Hintergrund mit geringer Priorität die Datei `Setup.exe` ausgeführt. Dies kann im Rahmen eines Anmeldescripts erfolgen. Beachten Sie, dass dafür kein Startscript verwendet werden kann, da das Computerkonto nicht über ausreichende Netzwerkberechtigungen verfügt.
 6. `Setup.exe` ermittelt, ob der Benutzercomputer Notebook Extension unterstützt. Informationen zu unterstützten Windows-Plattformen finden Sie in der Supportmatrix.
 7. `Setup.exe` ermittelt, ob .NET Framework Version 2.0 SP1 installiert ist. Wenn dies nicht der Fall ist, wird es installiert. Danach muss möglicherweise ein Neustart des Computers durchgeführt werden.
 8. `Setup.exe` ermittelt, ob Notebook Extension bereits installiert ist. Wenn dies nicht der Fall ist oder eine ältere Version installiert ist, wird Notebook Extension installiert.



HINWEIS:

Wenn in den Schritten 4 bis 7 Fehler auftreten, werden auf dem Notebook Extension-Policy Server und im Anwendungsereignisprotokoll auf dem lokalen Computer entsprechende Nachrichten protokolliert.

Den Fortschritt der Agent-Bereitstellung können Sie wie folgt über die Policy Server-Konsole von Notebook Extension überprüfen:

1. Melden Sie sich an der Policy Server-Konsole von Notebook Extension an.
2. Wählen Sie im Navigationsbereich auf der linken Seite unter **Berichte** den Eintrag **Agentenbereitstellung** aus.

Daraufhin wird eine Zusammenfassung des Fortschritts Ihrer Erstbereitstellung bis zu diesem Zeitpunkt angezeigt. Folgende Informationen sind enthalten:

- Anzahl der Computer, die die Bereitstellung erfolgreich **abgeschlossen** haben.

- Anzahl der Computer, bei denen die Bereitstellung gerade **in Bearbeitung** ist.
 - Anzahl der Computer, bei denen die Bereitstellung **fehlgeschlagen** ist.
3. Klicken Sie in der Spalte **Anzahl der Computer** auf eine Zahl, um eine Liste der Computer im entsprechenden Bereitstellungsstatus anzuzeigen.
- Zu jedem Computer wird der aktuelle Status angezeigt. Wenn die Bereitstellung beispielsweise auf einem bestimmten Computer fehlgeschlagen ist, wird in der Spalte **Informationen** der aufgetretene Fehler angezeigt. Weitere Informationen zu einem Computer erhalten Sie, indem Sie auf dessen NETBIOS-Namen klicken.

5 Unterstützung für Notebook Extension anfordern

In Notebook Extension ist ein Wartungsvertrag mit einjähriger Laufzeit enthalten. Dieser beinhaltet für Sie das Recht auf folgende Unterstützungsleistungen:

- Telefonische Unterstützung, direkter Kontakt zu einem Kundendiensttechniker.
- Aktualisierungen des Notebook Extension-Servers und der Notebook Extension-Agentensoftware. Die jeweils aktuellen Versionen oder CD-ROM-Images können von der Website für Data Protector heruntergeladen werden. Rufen Sie dazu die Seite <http://www.hp.com/go/dataprotector> auf.

Stichwortverzeichnis

Symbole

.NET Framework, 16, 34

A

Active Directory, 11
 Zugriff, 25
Agent Deployment Kit, Inhalt, 35
Agenten, 11
 Unterstützte Anzahl festlegen, 28
 Voraussetzungen, 14
Agentensoftware
 installieren, 33
 unternehmensweit bereitstellen, 35
Agentensoftware bereitstellen, 35
 Fortschritt überprüfen, 37
 Prozedur, 36
ASP.NET, 17

B

Benutzercomputer, Voraussetzungen, 14
Benutzerkontrollrichtlinie, 26
Bereitstellung
 Fortschritt überprüfen, 37
 Prozedur, 36

C

Cell Manager konfigurieren, 19
Cleanup-Richtlinie, 25

Continuous File Protection-Richtlinien, 24

D

Data Protector Cell Manager konfigurieren, 19
Data Vault-Richtlinien, 21
Data Vaults
 Serverempfehlungen, 29
 Voraussetzungen, 21
Dateischutzrichtlinien, 23
 Continuous, 24
 Open, 24
Dateiserver, 11
Datenbankvoraussetzungen, 14
Desktop-PCs, Voraussetzungen, 14
Dokument
 Konventionen, 8
 Zugehörige Dokumente, 7
Dokumentation
 Feedback geben, 10
 HP Website, 7

E

Erhalt von Berichtsdaten, 26

H

Hilfe
 erhalten, 9
HP
 Technischer Support, 9

I

- IIS, 17
- installieren
 - Agenten, 33
 - Policy Server, 15
 - SQL Server, 17
 - Übersicht, 13
- Internet Information Services, 17

K

- Konfigurieren
 - Active Directory-Zugriff, 25
 - Benutzerkontrollrichtlinie, 26
 - Cleanup-Richtlinie, 25
 - Data Vault-Richtlinien, 21
 - Dateischutzrichtlinien, 23
 - Erhalt von Berichtsdaten, 26
 - Erstkonfiguration der Richtlinien, 21
 - Kopierichtlinien, 22
 - Richtlinie für die Agentenaktualisierung, 26
 - Richtlinien für Continuous File Protection, 24
 - Richtlinien für Open File Protection, 24
- Konsole ausführen, 18, 21
- Konventionen
 - Dokument, 8
- Kopierichtlinien, 22

L

- Lizenzen
 - Lizenzschlüssel eingeben, 27
 - verfügbar, 20
 - verschieben, 27
- Lizenzen verschieben, 27
- Lizenzieren, 20, 26
- Lizenzschlüssel eingeben, 27

N

- Netzwerk, Überlegungen bei der Größenbestimmung, 30
- Notebook Extension
 - Agenten installieren, 33
 - Architektur, 12
 - Übersicht, 11
 - Unterstützung anfordern, 39
- Notebooks, Voraussetzungen, 14

P

- Passwort, 19, 27
- Policy Server, 11
 - Datenbankvoraussetzungen, 14
 - Empfehlungen, 29
 - installieren, 15
 - Voraussetzungen, 13
- Policy Server-Konsole ausführen, 18, 21

R

- Richtlinie für die Agentenaktualisierung, 26
- Richtlinien
 - Agentenaktualisierung, 26
 - Benutzerkontrolle, 26
 - Cleanup, 25
 - Continuous File Protection, 23
 - Data Vault, 21
 - Dateischutz, 23
 - Erhalt von Berichtsdaten, 26
 - Erstkonfiguration, 21
 - Kopie, 22
 - Open File Protection, 24
 - Verteilung von, 12
- Richtlinien für Open File Protection, 24

S

- Server
 - Datei, 11
 - Richtlinie, 11
- SQL Server
 - installieren, 17
- SQL-Datenbank
 - Voraussetzungen, 14
- Subscriber's Choice, HP, 9
- Supportmatrix, 11

T

- Technischer Support, 9
- Testversion von Notebook Extension, 20, 27

U

- Unterstützung, 39
- Überlegungen bei der Größenbestimmung, 28
 - Data Vault, 29
 - Netzwerk, 30
 - Policy Server, 29
- Übersicht, 11

V

- Verschlüsselungspasswort, 19, 27, 28
- Verschlüsselungspasswort eingeben, 28
- Verschlüsselungspasswort exportieren, 19, 27
- Verschlüsselungspasswort importieren, 19, 27
- Voraussetzungen, 13

W

- Websites
 - HP, 9
 - HP Subscriber's Choice for Business, 9
 - Produkthandbücher, 7
- Windows Installer, 16, 34

Z

- Zielgruppe, 7
- Zugehörige Dokumente, 7
- Zugriff auf Active Directory, 25

