

HP Data Protector for PCs 7.0 설치 및 관리 가이드

HP 제품 번호: 해당 사항 없음
2011년 6월 발행
제1판



© Copyright 2011 Hewlett-Packard Development Company, L.P.

기밀 컴퓨터 소프트웨어. 소유, 사용 또는 복사하려면 HP가 발급한 유효한 라이선스가 필요합니다. 미국 정부의 경우 FAR 12.211 및 FAR 12.212에 따라 상용 컴퓨터 소프트웨어, 컴퓨터 소프트웨어 설명서 및 상용 품목에 관한 기술 데이터는 벤더 표준 상용 라이선스에 의거하여 사용 허가를 받게 됩니다.

본 문서에 포함된 정보는 사전 통보 없이 변경될 수 있습니다. HP 제품 및 서비스에 대한 유일한 보증은 이러한 제품 및 서비스에 동봉된 명시적 보증서에 설명되어 있습니다. 본 문서의 어떤 것도 추가 보증을 구성하는 것으로 해석되어서는 안 됩니다. HP는 본 문서에 포함된 기술적 또는 편집상의 오류나 누락에 대해 책임을 지지 않습니다.

Microsoft®, Windows®, Windows® XP, Windows NT® 및 Windows Vista®는 Microsoft Corporation의 미국 등록 상표입니다.

목차

가이드 정보.....	5
대상 독자.....	5
문서 규칙 및 기호.....	5
일반 정보.....	6
HP 기술 지원 팀.....	6
구독 서비스.....	6
HP 웹 사이트.....	6
설명서 피드백.....	7
1 개요 및 필수 구성 요소.....	8
Data Protector for PCs에 대한 개요.....	8
Data Vault.....	9
인증서 처리.....	10
자체 서명된 인증서.....	10
가져온 인증서.....	10
인증서 교환.....	11
Data Protector for PCs 설치에 대한 개요.....	11
필수 구성 요소.....	11
Policy Server.....	11
데이터베이스.....	12
Data Protector for PCs 웹 Data Vault 서버.....	13
Data Protector for PCs Agent.....	13
2 Data Protector for PCs Policy Server 설치.....	14
빠른 설치.....	14
자세한 설치.....	15
3 웹 Data Vault 서버 설치, 구성 및 유지.....	18
웹 Data Vault 서버 설치 및 구성.....	18
웹 Data Vault 유지.....	19
Windows 파일 공유 Data Vault에서 웹 Data Vault로 데이터 이전.....	19
CLI에서 웹 Data Vault 옵션 구성(DvConfig).....	20
4 Data Protector for PCs 보호 정책 구성.....	22
Data Protector for PCs 설치 후 초기 설정.....	22
처음으로 구성.....	23
남아 있는 정책 구성.....	26
기타 구성 작업.....	29
지원할 수 있는 Agent 수 결정.....	30
크기 조정에 영향을 미치는 요소.....	30
크기 조정 권장 사항.....	30
Data Vault.....	30
Policy Server.....	31
네트워킹 고려 사항.....	32

5 다중 스레드 정리 구성.....	33
CLI에서 DPNECleanup.exe 사용.....	33
6 Data Protector for PCs Agent 설치.....	35
개별 클라이언트 컴퓨터에 Data Protector for PCs Agent 설치.....	35
필수 구성 요소.....	35
설치 절차.....	35
엔터프라이즈 전체에 Data Protector for PCs Agent 배포.....	36
키트 내용물.....	36
배포 및 설치 절차.....	37
7 Data Protector for PCs 업데이트.....	39
Policy Server 업데이트.....	39
Agent 업데이트.....	39
Agent 업데이트 정책을 사용하여 Agent 자동 업데이트.....	40
Agent 수동 업데이트.....	40
8 Data Protector for PCs에 대한 지원을 받는 방법.....	41
용어 설명.....	42
색인.....	44

가이드 정보

본 가이드에서는 다음 항목에 대한 정보를 제공합니다.

- HP Data Protector for PCs 설치
- HP Data Protector for PCs 정책 구성
- 사용자 데스크톱 및 노트북에 설치되어 있는 HP Data Protector for PCs Agent 소프트웨어
- 지원할 수 있는 Agent 수 결정
- Data Protector for PCs에 대한 지원 받기

대상 독자

HP Data Protector for PCs를 설치하고 구성하기를 원하는 관리자를 대상으로 하고 있는 본 가이드에는 다음 작업에 익숙해 질 수 있는 유용한 정보가 담겨 있습니다.

- Windows 관리

문서 규칙 및 기호

규칙	요소
파란색 텍스트: "가이드 정보" (5 페이지)	상호 참조 링크 및 전자 메일 주소
파란색, 밑줄 텍스트: http://www.hp.com	웹 사이트 주소
굵은 텍스트	<ul style="list-style-type: none">• 눌러져 있는 키• 상자와 같은 GUI 요소에 입력된 텍스트• 메뉴 및 목록 항목, 단추, 탭 및 확인란과 같은 클릭되었거나 선택된 GUI 요소
기울임꼴 텍스트	텍스트 강조
고정폭 텍스트	<ul style="list-style-type: none">• 파일 및 디렉터리 이름• 시스템 출력• 코드• 명령, 인수 및 인수 값
고정폭, 기울임꼴 텍스트	<ul style="list-style-type: none">• 코드 변수• 명령 변수
고정폭, 굵은 텍스트	강조된 고정폭 텍스트

① **중요:** 명확한 정보 또는 자세한 지침을 제공하십시오.

참고: 추가 정보를 제공하십시오.

일반 정보

Data Protector for PCs에 대한 일반 정보는 <http://www.hp.com/go/dataprotector>에서 확인할 수 있습니다.

HP 기술 지원 팀

전세계의 기술 지원 팀 정보는 HP 지원 웹 사이트를 참조하십시오.

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

HP에 문의하기 전에 다음과 같은 정보를 수집하십시오.

- 제품 모델 이름 및 번호
- 기술 지원 등록 번호(해당하는 경우)
- 제품 일련 번호
- 오류 메시지
- 운영 체제 유형 및 개정 수준
- 자세한 질문

구독 서비스

HP는 Subscriber's Choice for Business 웹 사이트에서 사용자의 제품을 등록할 것을 권장합니다.

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

등록을 마치면 제품 향상, 새로운 드라이버 버전, 펌웨어 업그레이드 및 기타 제품 리소스에 대한 전자 메일 알림을 받게 됩니다.

HP 웹 사이트

추가 정보는 다음 HP 웹 사이트를 참조하십시오.

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

설명서 피드백

HP는 사용자 여러분의 피드백을 환영합니다.

제품 설명서에 대한 의견 및 제안이 있는 경우 DP.DocFeedback@hp.com으로 메시지를 보내 주십시오. 모든 제출 자료는 HP의 자산이 됩니다.

1 개요 및 필수 구성 요소

Data Protector for PCs에 대한 개요

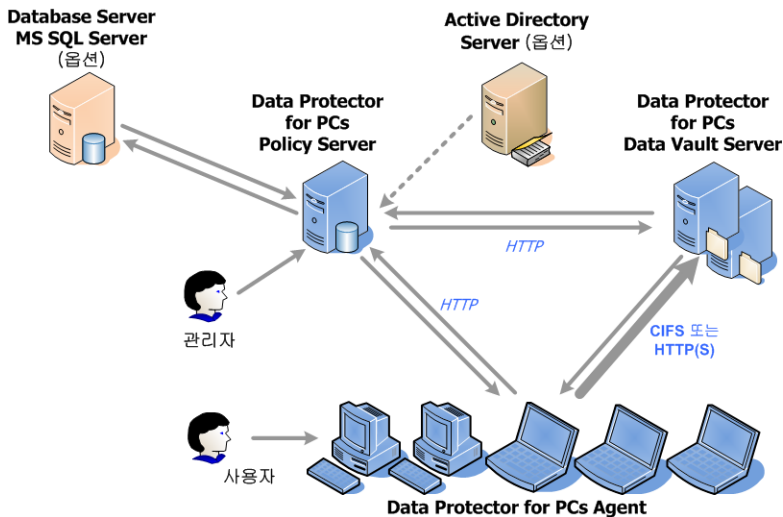
HP Data Protector for PCs는 Policy Server와 Agent라는 두 개의 주요 소프트웨어 구성 요소로 구성되어 있습니다. Policy Server는 Windows 서버에서 실행됩니다. 지원되는 버전에 대해서는 지원 매트릭스를 참조하십시오(<https://h20230.www2.hp.com/selfsolve/manuals>). Agent는 각 데스크톱 및 랩톱의 백그라운드에서 실행됩니다.

Policy Server는 또한 Active Directory 서버에 포함된 그룹 및 조직 단위에 액세스할 수 있습니다.

사용자의 데이터는 Data Vault로 백업됩니다. Data Vault 서버는 Policy Server와 별개여야 합니다. 권장하는 웹 Data Vault 대신 Windows 파일 공유 Data Vault를 사용하고 있는 경우 Windows 파일 공유 Data Vault는 파일 서버에 있는 하나 이상의 Windows 파일 공유에 있습니다.

Data Protector for PCs 구조는 아래 다이어그램에 나와 있습니다.

그림 1 Data Protector for PCs 구조



다양한 정책은 데스크톱 및 랩톱으로부터 백업되는 파일 및 이러한 백업이 저장되는 위치를 제어합니다. Policy Server 콘솔을 통해 이러한 정책을 정의합니다. 그러면 정책은 HTTP 포트 80을 통해 SOAP 프로토콜을 사용하여 Agent에 자동으로 배포되어 Policy Server에 저장됩니다.

Agent는 이러한 정책을 실행합니다. 사용자가 정책에 따라 보호된 데이터 파일을 변경하면 이전 버전이 데스크톱/랩톱의 로컬 하드 디스크에 생성되며 파일에 대한 변경 사항은 압축되어 해당하는 모든 Data Vault로 복사됩니다.

파일이 백업될 때마다 Agent는 사용자가 수행한 파일 변경 사항에 대한 감사 내역을 포함하고 있는 Policy Server에 알립니다. 또한 각 Agent는 정기적으로 "상태" 정보를 Policy Server로 보냅니다. Policy Server 콘솔을 통해 이 데이터의 보고서를 생성할 수 있습니다.

Data Vault는 Data Vault 서버에 저장되어 있습니다. 클라이언트 데이터는 각기 다른 두 개의 프로토콜, CIFS(Windows 파일 공유 Data Vault용) 또는 HTTP(웹 Data Vault용)를 사용하여 Data Vault로 복사됩니다.

Data Vault 서버는 Policy Server와 별개인 시스템에 있어야 합니다. HTTPS의 경우 웹 Data Vault 서버 소프트웨어는 Data Protector for PCs Cleanup 소프트웨어와 함께 해당 시스템에서 실행됩니다. Windows 파일 공유 Data Vault의 경우 Cleanup 소프트웨어만 해당 시스템에 설치됩니다.

Active Directory를 사용하는 경우 Policy Server를 구성하여 그룹 및 조직 단위에 액세스할 수 있습니다. 그런 다음 그룹 또는 조직 구성 단위 구성원 자격을 바탕으로 Data Vault를 사용자에게 할당할 수 있습니다. 또한 해당 구성원 자격을 바탕으로 보고서에서 사용자를 선택할 수도 있습니다.

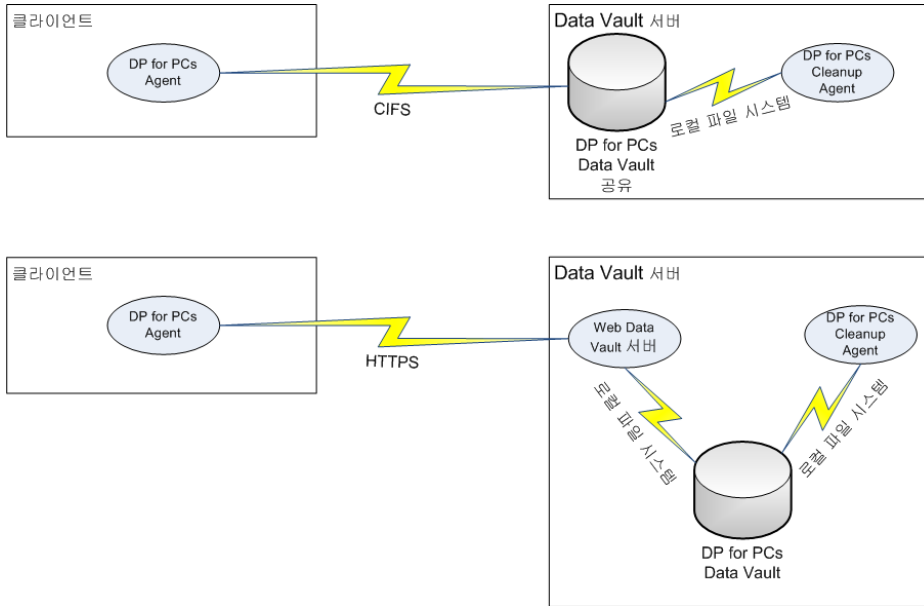
Data Vault

다음은 Data Protector for PCs와 함께 사용할 수 있는 2가지 Data Vault입니다.

- 웹 Data Vault - HTTPS 프로토콜에 기반합니다. 대기 시간이 많은 환경에서 최고 보안 수준과 더 우수한 처리량을 제공하므로 권장됩니다.
- Windows 파일 공유 Data Vault - CIFS 프로토콜에 기반하며 Data Protector for PCs 초기 버전에서 사용됩니다.

두 가지 Data Vault 유형의 데이터 구조는 동일하므로 기존 Windows 파일 공유 Data Vault를 웹 Data Vault로 변환할 수 있습니다.

그림 2 Windows 파일 공유와 웹 Data Vault 비교



인증서 처리

SSL을 웹 Data Vault에 필수적으로 사용해야 합니다. 인증서 유형은 웹 Data Vault를 설치하는 동안 결정됩니다. 예를 들어 평가 목적으로 우수한 성능을 즉시 발휘할 수 있는 제품을 제공하기 위해 자체 서명된 인증서를 사용하여 웹 Data Vault 서버를 설치할 수 있습니다. 자체 서명된 인증서는 신뢰된 인증 기관(CA)에서 발행한 인증서만큼 안전하지 않습니다. 완전 보안을 위해 신뢰된 인증 기관에서 서명한 Data Vault 서버용 인증서를 사용 환경 내로 가져와 서버 구성 요소에 추가해야 합니다.

자체 서명된 인증서

Data Vault 정책 생성 시 자체 서명된 인증서 허용 여부를 정의할 수 있습니다. 이 경우 Agent 측면에서는 아무런 조치도 수행할 필요가 없습니다. 설치를 통해 발급된 자체 서명된 인증서는 유효 기한이 20년입니다.

가져온 인증서

가져오기 절차를 수행하려면 개인 키와 공개 키가 들어 있는 일치하는 인증서가 모두 포함되어 있는 PEM 형식의 단일 파일이 필요합니다. 해당 파일은 웹 Data Vault 서버 구성 디렉터리에 있는 그대로 복사됩니다. 인증서 파일 생성에 사용된 절차에 따라 해당 파일이 암호화될 수도 있습니다. 암호화되어 있는 경우, 웹 Data Vault 서버를 실행하는 Windows 서비스 프로세스에는 비밀번호를 해독할 수 있는 대화식 프롬프트가 나타납니다. 예를 들어, 설치하는 동안 및 시스템을 다시 부팅한 다음 추후에 서비스를 다시 시작할 때마다 프롬프트가 나타납니다. 웹 서버 구성 파일에 이 비밀번호를 수동으로 추가하여 프롬프트가 나타나지 않도록 할 수 있지만 설치 프로세스는 이를 지원

하지 않습니다. 암호화된 인증서 파일을 보유하고 인증서 파일 옆에 있는 파일에 비밀번호를 저장하는 것은 바람직하지 않습니다.

참고:

“신뢰된 인증 기관”이라는 용어에는 Agent를 실행하는 클라이언트 컴퓨터가 이 CA를 신뢰할 수 있다고 여기고 해당 기관에서 서명한 인증서를 수락한다는 의미가 내포되어 있습니다. CA의 인증서와 아마도 해당 체인의 추가 인증서가 추가되어서 클라이언트 컴퓨터의 Windows 인증서 저장소가 이미 적절히 설정되어 있을 것으로 가정합니다. Agent에는 이러한 신뢰를 구축하기 위한 어떠한 메커니즘도 포함되어 있지 않습니다. Agent는 Windows 메커니즘에 의존합니다.

인증서 교환

CLI 단락 “CLI에서 웹 Data Vault 옵션 구성(DvConfig)” (20 페이지)에서 설명하고 있는 DvConfig 유틸리티를 사용하여 설치 후 언제든지 웹 Data Vault 서버의 인증서를 교환할 수 있습니다. 따라서, 예를 들면 자체 서명된 인증서를 사용하여 처음에 설정한 설치를 다시 구성하여 가져온 인증서를 사용할 수 있습니다.

Data Protector for PCs 설치에 대한 개요

참고: Data Protector for PCs 설치를 업데이트하고 있는 경우 “Data Protector for PCs 업데이트” (39 페이지)를 참조하십시오.

Data Protector for PCs를 설치할 수 있는 세 가지 단계가 있습니다.

1. **Data Protector for PCs Policy Server를 설치합니다.**
“Data Protector for PCs Policy Server 설치” (14 페이지)를 참조하십시오.
2. **Data Protector for PCs 웹 Data Vault 서버 소프트웨어를 설치합니다.**
“웹 Data Vault 서버 설치, 구성 및 유지” (18 페이지)를 참조하십시오.
3. **보호 정책을 구성합니다.**
“Data Protector for PCs 보호 정책 구성” (22 페이지)를 참조하십시오.
4. **랩톱 및 데스크톱에 Data Protector for PCs Agent를 설치합니다.**
“Data Protector for PCs Agent 설치” (35 페이지)를 참조하십시오.

필수 구성 요소

Policy Server

지원되는 운영 체제에 대해서는 지원 매트릭스를 참조하십시오.

참고: Windows 2003 64비트 운영 체제에 설치: Policy Server는 64비트 Windows 운영 체제에서 32비트 호환 모드로 실행됩니다. 즉 IIS(인터넷 정보 서비스)는 32비트 모드로 실행되어야 합니다. 그렇지 않은 경우 설치 시 필수 구성 요소를 확인하는 동안 32비트 모드로 실행되고 있지 않음이 감지됩니다. 32비트 모드로 IIS를 설정할 수 있는 옵션이 제공됩니다. IIS를 64비트 모드로 실행해야 하는 서버에 다른 웹 응용 프로그램(예: Outlook Web Access 등과 같은 웹 메일이 있는 Microsoft Exchange 2007)이 있는 경우 해당 서버에 Policy Server를 설치할 수 없습니다. Windows 2008에 Policy Server를 설치하는 경우에는 적용되지 않습니다.

서버에는 다음 항목이 설치되어 있어야 합니다.

- ASP.NET 응용 프로그램을 지원하는 인터넷 정보 서비스 6.0, 7.0, 7.5 이상
Windows 2003의 경우 IIS 6.0은 필수 구성 요소이며 설치되어 있어야 Policy Server를 설치할 수 있습니다. Windows 2008의 경우 Data Protector for PCs는 IIS 7.0 및 7.5가 설치되어 있지 않은 경우 이에 대한 설치를 제공합니다.

- Microsoft ASP.NET 2.0

또한 서버에 다음 항목도 설치해야 합니다.

- Microsoft Installer 3.1 이상(.NET Framework 2.0 SP1에 필요).
- Microsoft .NET Framework 2.0 SP1 이상. 해당 마법사가 버전 2.0 SP1을 설치합니다.
- Microsoft SQL Express(다른 SQL 버전이 없는 경우)

또한 인터넷 정보 서비스 7.0 및 7.5에 한해 다음 IIS 구성 요소가 필요합니다. 설치되어 있지 않은 경우 마법사를 통해 다음 항목을 설치할 수 있습니다.

- IIS Static Content Web Server - 정적 html 파일, 문서 및 이미지 제공에 필요
- IIS ASP.NET - ASP.NET 2.0 및 .NET Framework 배포에 필요
- IIS Security - Policy Server 콘솔에 사용한 통합된 Windows 인증을 사용하는 데 필요
- IIS 6 Management Compatibility—가능한 한 같은 방식으로 설치 프로그램이 IIS 6 및 IIS 7을 구성할 수 있도록 하기 위해 필요

데이터베이스

Data Protector for PCs를 사용하려면 Microsoft SQL Server 데이터베이스에 액세스해야 합니다. 지원되는 버전에 대해서는 지원 매트릭스를 참조하십시오.

Microsoft Enterprise Manager를 사용하여 SQL Server 설치의 인증 모드를 확인 및 변경할 수 있습니다.

1. SQL Server 인스턴스를 마우스 오른쪽 단추로 클릭하고 속성을 선택한 다음 보안 탭을 클릭합니다.

2. **Windows만** 옵션 대신 **SQL Server 및 Windows** 옵션이 이미 선택되어 있어야 합니다. 선택되어 있지 않으면 해당 옵션을 선택하고 **확인**을 클릭합니다.

또한 Data Protector for PCs를 설치하는 동안 Microsoft SQL Server Express Edition의 인스턴스를 설치할 수 있습니다.

Data Protector for PCs 웹 Data Vault 서버

- 웹 Data Vault 서버는 Policy Server와 다른 시스템에 설치되어 있어야 합니다. 같은 시스템에 웹 Data Vault 서버를 설치할 수 있지만 이는 평가 목적에만 적합합니다.
- Java Runtime 환경 버전 1.6 이상이 설치되어 있어야 합니다.
- 변수 JAVA_HOME 및 JRE_HOME는 Java Runtime 설치 디렉터리를 가리켜야 합니다.

Data Protector for PCs Agent

Data Protector for PCs Agent 소프트웨어는 Windows를 실행하는 사용자의 데스크톱 및 노트북에 설치될 수 있습니다. 지원되는 플랫폼에 대해서는 지원 매트릭스를 참조하십시오.

2 Data Protector for PCs Policy Server 설치

참고: 표준 설치 절차에 따라 기존 Data Protector for PCs Policy Server 설치를 최신 버전으로 업데이트할 수 있습니다. 자세한 내용은 “Policy Server 업데이트” (39 페이지)를 참조하십시오.

빠른 설치

Data Protector for PCs Policy Server에 대한 요구 사항은 “Policy Server” (11 페이지)를 참조하십시오.

1. Data Protector for PCs 설치 CD-ROM을 삽입합니다. 설치 마법사가 자동으로 시작되지 않으면 설치 CD-ROM의 해당 루트에서 `setup.hta`를 두 번 클릭하여 수동으로 실행합니다.
2. 화면상의 지침을 따릅니다.
3. Data Protector for PCs Policy Server를 사용하려면 Microsoft SQL Server 데이터베이스에 액세스해야 합니다. **Microsoft SQL Server Express의 기존 Data Protector for PCs 인스턴스 사용**을 선택하거나 **Microsoft SQL Server의 기존 인스턴스 사용**을 클릭합니다. 기존 SQL Server를 사용하기로 결정한 경우 데이터베이스 서버 연결 스트링 및 새 데이터베이스를 생성할 수 있는 충분한 권한을 가진 계정에 대한 자격 증명을 제공해야 합니다.
4. 마법사의 **Data Protector for PCs Policy Server** 설치 페이지에서 **설치**를 클릭하여 설치를 시작합니다.
5. 설치가 완료되면 **다음**을 클릭합니다. 그러면 Data Protector for PCs Policy Server 콘솔 실행을 선택할 수 있습니다.
6. 별도의 시스템에 웹 Data Vault 서버를 설치합니다. 주 설치 화면에서 **Data Vault 설치**를 클릭합니다.

참고: Cleanup 소프트웨어는 설치 중에 웹 Data Vault 서버 소프트웨어와 항상 함께 설치됩니다. 성능을 최적화하기 위해 Windows 파일 공유 Data Vault만 호스트하는 Data Vault 서버는 Data Vault에 로컬로 설치하는 것이 좋습니다.

자세한 설치

참고:

Windows 2003 서버만 해당: 이 서버의 .NET 2.0 Framework 런타임 보안 정책이 로컬 인트라넷 보안 영역에 대해 **완전 신뢰**로 설정되어 있는 경우 네트워크를 통해 공유된 CD-ROM 또는 네트워크 파일 공유에서 Data Protector for PCs Policy Server를 설치할 수 있습니다. 서버에 로컬 CD-ROM 드라이브가 없는 경우 관리 도구의 .NET Framework 2.0 구성 도구를 사용하여 로컬 인트라넷 보안 영역에 대한 런타임 보안 정책을 **완전 신뢰**로 변경하거나 CD의 "Server" 폴더를 서버의 로컬 디스크로 복사합니다.

"관리자" 권한으로 계정에 로그인하여 Data Protector for PCs Policy Server 설치를 수행해야 합니다.

1. Data Protector for PCs 설치 CD-ROM을 삽입합니다. 설치 마법사가 자동으로 시작되지 않으면 설치 CD-ROM의 해당 루트에서 `setup.hta`를 두 번 클릭하여 수동으로 실행합니다.
2. **Policy Server** 설치를 클릭합니다.
메시지가 나타나면 **이 프로그램을 디스크에 저장** 대신 현재 위치에서 이 프로그램을 열기 또는 실행을 선택합니다.
3. Data Protector for PCs Policy Server를 사용하려면 .NET Framework 2.0 SP1이 필요합니다. 아직 설치되어 있지 않은 경우 CD-ROM에서 .NET Framework 2.0 SP1을 설치할 것인지 물어보는 메시지가 나타납니다.
설치하려면 Windows Installer 3.1 이상이 필요하므로 필요한 경우 CD에서 Windows Installer 3.1을 설치할 것인지 물어보는 메시지가 나타납니다.
4. 설치 마법사가 다음과 같은 기타 필수 구성 요소가 설치되어 있는지 확인합니다.
 - IIS(인터넷 정보 서비스)
 - ASP.NET 2.0둘 중 하나가 설치되어 있지 않은 경우 목록에 있는 해당 필수 구성 요소를 클릭하여 해당 구성 요소를 설치하는 방법에 대한 자세한 내용을 확인합니다.
다음을 클릭합니다.
5. Microsoft SQL Server를 설치합니다.
Microsoft SQL Server의 기존 인스턴스를 사용하는 방법:
 - a. **Microsoft SQL Server의 기존 인스턴스 사용**을 클릭합니다.
 - b. **데이터베이스 서버** 필드에 기존 데이터베이스 서버에 대한 연결 스트링을 입력합니다.

- c. **로그인 및 비밀번호** 필드에 새 데이터베이스를 생성할 수 있는 충분한 권한이 있는 계정에 대한 자격 증명을 입력합니다. 보통 "sa" 계정이 됩니다.
- d. **다음**을 클릭합니다. 입력한 연결 정보는 기존 데이터베이스 서버에 대한 연결을 테스트하는 데 사용됩니다. 연결에 성공한 경우 마법사는 6단계로 넘어갑니다.

Microsoft SQL Server Express Edition의 Data Protector for PCs 인스턴스를 설치하는 방법:

- a. **Microsoft SQL Server Express의 DataProtectorNE 인스턴스 설치를** 선택하고 **다음**을 클릭합니다.
 - b. **설치**를 클릭하여 "DataProtectorNE"라는 이름을 가진 Microsoft SQL Server 2005 Express Edition의 인스턴스를 설치합니다. 설치가 완료되면 **다음**을 클릭합니다.
- 6.** Data Protector for PCs Policy Server 소프트웨어를 설치합니다.
- a. 시작 화면에서 **다음**을 클릭하여 설치를 시작합니다.
 - Data Protector for PCs Policy Server 콘솔은 가상 디렉터리 C:\Inetpub\wwwroot\dpnepolicy에 웹 응용 프로그램으로 설치됩니다.
 - Data Protector for PCs 웹 서비스는 C:\Inetpub\wwwroot\dpnepolicyservice에 설치됩니다.
 두 개 모두 포트 80에서 HTTP 프로토콜을 사용합니다.
 - b. Policy Server 설치가 완료되면 **닫기** 및 **다음**을 클릭합니다.
- 7.** 이제 Cleanup 프로그램을 설치해야 합니다. **설치**를 클릭하여 설치를 시작합니다.
- 8.** Cleanup 설치가 완료되면 **다음**을 클릭합니다.

Data Protector for PCs Policy Server 콘솔의 중앙에서 Data Protector for PCs를 관리합니다. 콘솔은 브라우저 기반이므로 Policy Server(HTTP 포트 80 사용)에 대한 브라우저 연결을 구축할 수 있는 모든 컴퓨터에서 Data Protector for PCs를 관리할 수 있습니다.

Policy Server의 브라우저에서 Data Protector for PCs Policy Server 콘솔을 실행하려면 **Policy Server 콘솔 실행** 확인란을 선택된 상태로 두고 **마침**을 클릭합니다.

참고: Cleanup 소프트웨어는 설치 중에 Policy Server에 설치됩니다. 또한 성능을 최적화하기 위해 Cleanup 소프트웨어를 Data Vaults에 설치하는 것이 좋습니다.

참고:

Policy Server 콘솔에 대한 브라우저 설정: 브라우저에서 Policy Server 콘솔 페이지를 표시하는 데 문제가 있는 경우 브라우저 보안 설정을 확인하십시오. Console을 사용하려면 다음을 수행해야 합니다.

- JavaScript를 활성화해야 합니다.
- dpnepolicy 웹 사이트에 대해 팝업 차단기를 비활성화해야 합니다.
- 특정 브라우저 및 브라우저의 버전에 따라 기타 제한적인 보안 설정을 수정해야 할 수도 있습니다.

Microsoft SharePoint에 설치: Policy Server가 Microsoft SharePoint를 실행하는 서버에 설치되어 있는 경우 Policy Server 콘솔을 실행하면 404 오류 “페이지를 찾을 수 없습니다”가 나타날 수도 있습니다. 기술 자료 문서(<http://support.microsoft.com/kb/828810>)에 문제 및 해결 방법이 설명되어 있습니다. 이 문제는 모든 ASP.NET 웹 응용 프로그램에 적용되지만 Policy Server에는 적용되지 않습니다.

SharePoint를 사용하는 서버에서 Policy Server를 실행하려면 다음을 수행해야 합니다.

1. SharePoint 관리 도구를 사용하여 다음과 같은 두 개의 Policy Server 웹 응용 프로그램에 대한 제외를 생성합니다. dpnepolicy 및 dpnepolicyservice.
2. 두 개의 Policy Server web.config 파일(dpnepolicy\web.config 및 dpnepolicyservice\web.config)을 수정하여 앞에서 언급한 Microsoft 기술 자료 문서에 설명된 대로 <httpHandlers> 및 <trust> XML 코드를 추가합니다.

3 웹 Data Vault 서버 설치, 구성 및 유지

웹 Data Vault 서버 설치 및 구성

참고: Policy Server와 다른 시스템에 웹 Data Vault 서버를 설치합니다. 같은 시스템에 웹 Data Vault 서버를 설치할 수 있지만 이는 평가 목적에만 적합합니다.

1. Data Protector for PCs 설치 CD-ROM을 삽입합니다. 설치 마법사가 자동으로 시작되지 않으면 설치 CD-ROM의 해당 루트에서 `setup.hta`를 두 번 클릭하여 수동으로 실행합니다.
2. **Data Vault 설치**를 클릭합니다.
3. 다음 중 하나를 선택합니다.
 - **웹 Data Vault 서버(권장)**. 이를 선택하면 서버에 Cleanup 소프트웨어도 설치됩니다.
 - **Windows 파일 공유 Data Vault용 Cleanup 소프트웨어**. Windows 파일 공유 Data Vault만 사용하려면 이 항목을 선택합니다.

자세한 정보는 [“Data Vault” \(9 페이지\)](#)를 참조하십시오.

4. 화면상의 지침에 따라 설치 단계를 완료합니다.
5. Policy Server에서 라이선스를 가져와서 웹 Data Vault 서버를 설치하고 있는 경우 웹 Data Vault 구성을 시작합니다.

서버 설정 화면에 서버의 FQDN(정규화된 도메인 이름) 및 SSL 포트를 입력합니다. Policy Server에 웹 Data Vault 정책을 구성할 때 동일한 FQDN을 사용해야 합니다. 모든 클라이언트 시스템에서 이름을 확인할 수 있어야 합니다. 그렇지 않으면 클라이언트 시스템 일부를 이 서버의 Data Vault에 백업할 수 없게 됩니다.
6. 인증서 설정 화면에서 다음 중 하나를 선택해야 합니다.
 - 신뢰된 인증 기관(CA)이 발행한 기존 SSL 인증서 가져오기. 이는 권장 옵션이며 최상위 수준의 보안을 제공합니다.
 - 자체 서명한 SSL 인증서 생성. 이는 낮은 수준의 보안을 제공하며 평가 목적으로만 사용해야 합니다.

참고: DvConfig 유틸리티를 사용하여 설치 후 언제든지 웹 Data Vault 서버에 있는 인증서를 교환할 수 있습니다. 인증서 교환에는 가져온 인증서를 사용하기 위해 자체 서명한 인증서로 설치를 다시 구성하는 것이 포함되어 있습니다. [“CLI에서 웹 Data Vault 옵션 구성\(DvConfig\)” \(20 페이지\)](#)을 참조하십시오.

7. 웹 Data Vault 서버의 두 가지 사용자 유형에 대한 이름을 입력해 달라는 화면이 다음에 나타납니다.
 - **관리자** - Data Vault 생성 및 삭제, 클라이언트 백업 데이터 이전과 같은 관리 작업 담당

- **백업 사용자** - 파일 백업 및 복원과 같은 최종 사용자 작업 수행

이러한 사용자는 Data Protector for PCs 웹 Data Vault 서버에만 있습니다. 이 서버의 웹 Data Vault를 생성 또는 편집할 때 두 가지 유형의 사용자에 대한 세부 정보를 모두 입력해야 합니다.

참고: 비밀번호는 최소 8자 이상이어야 합니다.

8. **다음 및 마침**을 차례로 클릭하여 웹 Data Vault 서버의 설치 및 구성, Cleanup 소프트웨어의 설치를 완료합니다.

웹 Data Vault 유지

1. Data Vault 정책 페이지에 서버의 정규화된 도메인 이름 및 SSL 포트, 백업 사용자 계정 자격 증명을 입력합니다. 그런 다음 **Data Vault 구성**을 클릭합니다.
2. 관리자 계정 자격 증명을 제출하면 웹 Data Vault 서버 유지 페이지가 표시됩니다. 여기서 기존 웹 Data Vault를 선택하거나 삭제할 수 있습니다. 새 Data Vault를 추가할 수도 있습니다.

참고: 다른 Data Vault 정책에 현재 연결되어 있지 않은 기존 Data Vault만 선택할 수 있습니다.

3. 페이지 맨 아래에 있는 **저장**을 클릭하여 Data Vault 정책이 저장되었는지 확인합니다.
4. 새로운 Data Vault를 추가했다면 Vault의 존재 여부와 적절한 구성에 대해 선택적으로 테스트할 수 있습니다.

Windows 파일 공유 Data Vault에서 웹 Data Vault로 데이터 이전

Data Vault의 데이터 레이어아웃은 Windows 파일 공유 Data Vault 및 HTTPS 웹 Data Vault 모두와 여전히 같습니다. 이는 기존 DPNE 6.x Data Vault에서 새로운 웹 Data Vault로 데이터를 이전할 수 있음을 의미합니다.

참고: 같은 Policy Server에 속해 있거나 같은 암호화된 비밀번호를 공유하고 있는 Data Vault에 대해서만 데이터 이전을 수행할 수 있습니다.

데이터 이전을 수행할 수 있는 두 가지 시나리오가 있습니다.

- 같은 시스템을 사용하여 웹 Data Vault에 호스트합니다.

참고: Windows 파일 공유 및 웹 Data Vault를 통해 같은 디렉터리에 동시에 액세스하는 것은 지원되지 않습니다.

- 전체 Data Vault를 다른 시스템으로 옮깁니다.

두 경우 모두 웹 Data Vault 서버가 데이터가 있어야 하는 시스템에 로컬로 설치되어 있어야 합니다.

기존 Windows 파일 공유 Data Vault에서 웹 Data Vault로 데이터를 이전하려면

참고:

- 비 작업 시간에 이전을 수행하여 백업 실행에 대한 효과를 최대화하십시오.
- Windows 작업 관리자에서 DPNECleanup.exe가 현재 실행되고 있지 않은지 확인하십시오.
- Policy Server의 정리 정책을 확인하여 DPNECleanup.exe가 이전 기간 동안 실행 되도록 예약되어 있지 않은지 확인하십시오.

1. 웹 Data Vault 서버를 설치하고 Policy Server 및 Agent를 7.0 버전으로 업데이트합니다. 7.0 버전을 설치한 후에 모든 Agent가 재부팅을 수행했는지 확인한 다음에만 데이터를 웹 Data Vault로 백업하는 작업을 시작할 수 있습니다.
2. Agent가 데이터를 Data Vault로 복사하는 것을 중지할 수 있도록 Data Vault 정책 페이지에서 해당 Windows 파일 공유 정책을 비활성화합니다.
3. 웹 Data Vault와 동일한 디렉터리를 사용하려는 경우 CIFS를 통해 해당 디렉터리를 공유하는 것을 중지합니다.
4. 웹 Data Vault가 Windows 파일 공유 Data Vault와 다른 서버에 있는 경우 67자를 초과하지 않는 해당 컴퓨터의 폴더 경로로 데이터를 복사해야 합니다. Data Vault가 같은 서버에 있는 경우 다른 이유로 의도적으로 복사하지 않는 한 데이터를 새 위치로 복사할 필요가 없습니다.
5. 새로운 웹 Data Vault를 생성하기 전에 초기 업데이트 프로세스의 동작을 결정합니다. 모든 Agent가 초기 업데이트를 수행하여 백업 데이터가 이미 기존 Data Vault에 완료되어 있는 경우에는 초기 업데이트를 건너뛸 수 있습니다. 초기 업데이트를 건너뛸 수 있는 옵션은 Data Vault 정책과 직접 관련된 일부는 아니지만 참조된 복사 정책의 일부입니다. 적절한 옵션을 선택할 수 있는 Data Vault 정책이 있는지 (즉 "초기 업데이트"가 꺼져 있고 해당 제한과 일정 설정이 있는지) 확인합니다. 이를 위해 새로운 복사 정책을 생성하거나 기존 정책(이 경우 영향을 받는 해당 복사 정책을 참조하는 모든 Data Vault 정책)을 수정합니다.
6. 웹 Data Vault에 대한 새로운 Data Vault 정책을 생성하고 저장합니다. 새로운 웹 Data Vault를 생성하면 폴더 경로를 제공해야 하며 이 폴더 경로는 이전하려는 Windows 파일 공유 Data Vault의 실제 데이터가 있는 경로가 됩니다. 5단계에서 생성한 복사 정책을 선택합니다. 원래 Windows 파일 공유 Data Vault 정책에서 수행했던 것과 동일한 방식으로 Data Vault 정책에 대한 다른 옵션을 설정합니다(예: 네트워크 설정, Active Directory 설정).
7. Agent가 새로운 웹 Data Vault로 파일을 성공적으로 백업하고 있다고 확신하면 원래 Windows 파일 공유 Data Vault 정책을 삭제합니다.

정책이 저장되면 Agent는 HTTPS 프로토콜을 사용하여 해당 데이터를 새로운 웹 Data Vault로 복사하는 것을 재개합니다.

CLI에서 웹 Data Vault 옵션 구성(DvConfig)

CLI에서 이 유틸리티를 사용하면 백업 사용자 및 관리자 그리고 해당 비밀번호와 같은 웹 Data Vault의 구성 매개 변수를 변경하고, 새 인증서를 가져오고, SSL을 변경하며 자체 서명한 새 인증서를 생성할 수 있습니다.

임의 매개 변수를 변경하기 전에 Windows 서비스 HP Data Protector for PCs Data Vault 서버를 중지하여 웹 Data Vault 서버를 중지해야 합니다.

변경한 후 웹 Data Vault 서비스를 다시 시작합니다. 업데이트한 정책은 Agent로 재배포됩니다.

참고: DvConfig를 사용하여 웹 Data Vault 서버의 SSL 포트 또는 백업 사용자 이름 또는 비밀번호를 변경하면 Policy Server의 해당 Data Vault 정책을 변경하여 일치하는지 확인하십시오.

사용법:

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

-adminUser login:password

DvAdmin 계정에 대한 자격 증명을 설정합니다. 주어진 로그인 또는 비밀번호가 없으면 기본값인 "DvAdmin"이 사용됩니다.

-backupUser login:password

DvBackup 계정에 대한 자격 증명을 설정합니다. 주어진 로그인 또는 비밀번호가 없으면 기본값인 "DvBackup"이 사용됩니다.

-h

이 메시지를 인쇄합니다.

-i certfile

기존 인증서를 가져옵니다.

-p portSSL 포트를 설정합니다.

-s hostname

정규화된 도메인 이름에 대한 자체 서명한 인증서를 생성합니다.

-v

버전 정보를 인쇄하고 종료합니다.

4 Data Protector for PCs 보호 정책 구성

Data Protector for PCs 설치 후 초기 설정

Data Protector for PCs를 설치한 직후 Policy Server 콘솔에 초기 설정 창이 나타납니다. Data Protector for PCs에 대한 정책을 설정하려면 다음과 같은 두 개의 구성 단계를 완료해야 합니다.

1. 암호화된 비밀번호를 정의하거나 가져옵니다.

보안상의 이유로 암호화된 비밀번호를 정의해야 Data Protector for PCs를 사용할 수 있습니다. 이렇게 하면 모든 파일이 사용자의 컴퓨터에서 암호화되고 암호화된 상태로 네트워크를 통해 전송됩니다. 같은 비밀번호를 사용하여 모든 사용자 및 중앙에서 구성된 모든 Data Vault의 파일을 암호화합니다.

- 중앙에서 정의된 Data Vault(Policy Server 콘솔을 통해 정의)는 항상 Data Protector for PCs 암호화된 비밀번호에 근거한 암호화를 사용합니다.
- 로컬로 정의된 Data Vault(해당 컴퓨터를 통해 사용자가 정의)의 경우 사용자는 암호화 사용 여부를 선택하고 고유한 비밀번호를 선택할 수 있습니다.

Data Protector for PCs를 처음으로 설치하는 경우 비밀번호를 **생성**하거나 **가져와야** 계속 진행할 수 있습니다. 비밀번호를 생성한 후에는 안전을 위해 비밀번호를 **내보냅니다**. 그러면 안전한 위치에 비밀번호가 저장되고 나중에 가져오는 데 비밀번호를 사용할 수 있습니다.

암호화 정책 설정을 클릭하여 비밀번호를 관리하고 창에 나타난 지침을 따릅니다.

참고: 비밀번호를 생성하거나 가져온 후에는 비밀번호를 변경할 수 없습니다.

2. Data Protector for PCs의 라이선스를 취득합니다.

Data Protector for PCs를 평가하고 있는 경우 사용자를 무제한으로 보호하기 위해 Data Protector for PCs를 추가 라이선스 없이 60일 동안 사용할 수 있습니다. Data Protector for PCs를 구입하는 경우 HP License Key Delivery Service (<https://webware.hp.com/welcome.asp>)로 이동하여 입력할 수 있는 라이선스 키를 다운로드합니다. 다음 라이선스를 구입할 수 있습니다.

- Agent 100개를 위한 TA032AA 또는 TA032AAE
- Agent 1,000개를 위한 TA033AA 또는 TA033AAE
- Agent 100개를 위한 TA036AA 또는 TA036AAE + HP Data Protector Starter Pack Windows(B6961BA 또는 B6961BAE)

평가 기간이 끝나기 전에 영구 라이선스 키를 입력해야 합니다. 평가 기간 내에 입력하지 않고 60일이 지나면 Agent는 데이터를 더 이상 해당 Local Repository 또는 Data Vault로 복사할 수 없게 됩니다. 그러나 이전에 보호된 파일 버전은 계속 복구할 수 있습니다.

라이선스 관리를 클릭하여 라이선스를 관리한 다음 **Data Protector for PCs 사용자에 대한 라이선스 키 입력**을 클릭합니다. 창에 나타난 지침을 따릅니다.

참고: Agent가 설치되면 라이선스는 Agent에 배포됩니다.

이러한 구성 단계를 완료하면 완벽하게 작동하는 Policy Server 콘솔을 사용할 수 있습니다. Data Protector for PCs를 지금 방금 설치한 경우 다음 절에 나오는 순서에 따라 Data Protector for PCs의 다른 요소를 구성합니다.

처음으로 구성

Data Protector for PCs는 대부분의 조직에 충분한 정책이 미리 구성된 상태로 제공됩니다. 처음에 Data Vault, 복사 및 파일 보호 정책을 구성한 다음 Data Protector for PCs Agent 소프트웨어를 사용자의 데스크톱 및 노트북에 설치하는 것이 좋습니다.

참고: 새 정책을 구성하는 대신 Data Protector for PCs가 미리 구성된 상태로 제공되는 정책을 수정할 수 있습니다. 각 단계에서 **새로운 정책 생성** 대신 **기존 정책 편집**을 선택하기만 하면 됩니다.

Policy Server 콘솔에서 설치에 대한 보호 정책을 구성합니다. 중앙에서 정의하는 정책은 모든 Data Protector for PCs Agent에 배포되며 사용자의 데스크톱 및 랩톱에서 실행됩니다.

1. 설치 마법사가 끝날 때 또는 다음 URL을 사용하는 브라우저에서 언제든지 Data Protector for PCs Policy Server 콘솔을 실행합니다.

`http://policyserver/dpnepolicy/`

여기서 "policyserver"는 Data Protector for PCs Policy Server의 이름입니다. 서버에 "관리자"로 로그인해야 합니다.

2. **Data Vault 정책을 구성합니다.**

Data Vault 정책은 정책으로 보호된 사용자 파일의 지속적인 백업 대상(웹 Data Vault 또는 Windows 파일 공유)을 설정합니다. 파일이 변경되면 이전 버전 및 편집된 파일을 하나 이상의 대상으로 자동으로 백업할 수 있습니다. 각 사용자 그룹에 하나 이상의 Data Vault를 할당할 수 있습니다. 예를 들어 **Sales**라는 Data Vault 정책을 정의하고 이를 사용자 그룹 **Dallas.Sales**, **San Francisco.Sales**, **Chicago.Sales** 및 **Atlanta.Sales**에 할당할 수 있습니다.

- 중앙에서 정의된 Data Vault(Policy Server 콘솔을 통해 정의)는 항상 Data Protector for PCs 암호화된 비밀번호에 근거한 암호화를 사용합니다.
- 로컬로 정의된 Data Vault(해당 Agent 소프트웨어를 통해 사용자가 정의)의 경우 사용자는 암호화 사용 여부를 선택하고 고유한 비밀번호를 선택할 수 있습니다.

참고: 모든 Data Vault에 대한 요구 사항:

Data Protector for PCs는 원래 파일이 있던 같은 파일 서버에 백업된 파일에 대한 액세스 권한(ACL)을 설정합니다. 즉, 해당 컴퓨터의 원래 파일에 액세스할 수 있는 경우 사용자는 백업된 파일을 복구만 할 수 있음을 의미합니다.

Windows 파일 공유 Data Vault에 대한 요구 사항:

표준 Windows 파일 공유 Data Vault를 사용하고 있는 경우 Policy Server와 같은 컴퓨터일 필요가 없는 Windows 파일 서버에서 공유되어야 합니다. 그러나 설치된 Agent의 수가 적은 Data Protector for PCs를 평가만 하고 있는 경우 Policy Server와 Data Vault 파일 서버를 같은 시스템으로 만드는 것이 유용할 수도 있습니다.

Data Vault 정책을 생성하는 방법:

- 왼쪽 탐색 창에서 **정책 > Data Vaults > Data Vault 정책**을 클릭합니다.
 - 새로운 Data Vault 정책 생성**을 클릭합니다.
 - 창에 나타난 지침을 따릅니다. 프로세스는 웹 기반을 선택하느냐 Windows 파일 공유 Data Vault 유형을 선택하느냐에 따라 달라집니다.
-

참고: Data Vault 생성 시 폴더 또는 공유 경로 길이는 66자를 초과해서는 안 됩니다.

모범 사례:

당분간은 복사 정책을 "기본 설정"으로 유지합니다.

Windows 파일 공유 Data Vault에 대한 정리

- Data Vault가 이 Policy Server에 있는 경우 이 컴퓨터의 이름을 기본 설정으로 유지합니다.
- Data Vault가 다른 Windows 파일 서버에 있는 경우 Data Vault Cleanup 소프트웨어를 해당 서버에 설치하고 해당 컴퓨터를 Cleanup Machine으로 지정합니다.

3. 복사 정책을 구성합니다.

복사 정책은 Data Vault에 동시 복사할 수 있는 클라이언트 수에 대한 제한을 설정합니다. 또한 지속적인 백업을 보완하기 위해 초기 및 예약된 Data Vault 업데이트도 정의합니다. 각 복사 정책을 하나 이상의 Data Vault에 할당할 수 있습니다.

복사 정책은 다음 항목을 정의합니다.

- Data Vault에 파일을 동시 복사할 수 있는 Agent 수
- 사용자에 대한 모든 예상 파일이 Data Vault에 있는지 확인하고, 없는 경우 누락된 모든 파일을 복사하는 정기 업데이트 일정. 이 과정에서 모든 사용자 파일이 Data Vault에 제대로 복사되었는지 추가로 확인합니다.
- 초기 업데이트** 또는 복사를 수행해야 합니다. 정상적인 Data Protector for PCs 작동 중 사용자가 Data Protector for PCs에서 지속적으로 보호되는 파일을 변

경할 때마다 변경되는 파일의 정보만 Data Vault에 복사해야 하므로 초기 업데이트가 필요합니다.

기본 복사 정책은 설정된 명시적 복사 정책이 없는 모든 Data Vault에 적용됩니다. 기본 복사 정책에 대한 설정을 변경할 수 있지만 삭제하거나 이름을 바꿀 수는 없습니다.

복사 정책을 생성하는 방법:

- a. 왼쪽 탐색 창에서 **정책**을 클릭합니다.
- b. **복사 정책 설정**을 클릭합니다.
- c. **새로운 복사 정책 생성**을 클릭합니다.
- d. 창에 나타난 지침을 따릅니다.

모범 사례

- **제한:** 일반 작업 시간으로 기간을 설정하고 다른 시간에 대한 제한을 낮게 설정합니다.
- **초기 업데이트:** 초기 업데이트를 설정하여 파일 보호 정책에 의해 보호된 모든 사용자 파일이 백업되는지 확인합니다.
- **매주/매일 파일 업데이트:** 업데이트에는 파일 복사(있는 경우)가 거의 포함되지 않으므로 Data Vault 업데이트를 설정하여 정책으로 보호되는 모든 사용자 파일이 적절히 백업되는지 확인합니다.

4. 파일 보호 정책을 구성합니다.

파일 보호 정책을 사용하면 보호할 파일 및 이전 버전을 보존할 기간을 지정할 수 있습니다. 예를 들어 Word 문서, Excel 스프레드시트 및 PowerPoint 프레젠테이션에 대해 **Office 문서**라는 파일 보호 정책을 정의할 수 있습니다.

로컬 디스크 드라이브에 저장된 파일을 보호할 수 있습니다.

아래와 같은 두 가지 유형의 정책이 있습니다.

- **Continuous File Protection** - 이 방법을 사용하면 파일을 디스크에 저장하거나 삭제할 때마다 실시간으로 파일을 보호할 수 있습니다. 일반적으로 메뉴에서 **저장**을 선택할 수 있는 파일이나 문서는 Continuous File Protection 정책으로 보호해야 합니다.

Data Protector for PCs에는 다양한 예제 정책이 포함되어 있습니다. 설치가 끝나면 다음과 같은 세 가지 항목이 기본적으로 선택되어 있습니다. **Office 문서**, **소프트웨어 개발** 및 **웹 문서**. 이러한 정책으로 시작하거나 사용자 고유의 정책을 작성할 수 있습니다.

- **Open File Protection** - 이 방법을 사용하면 정기적으로(보통 1시간마다 한 번) 파일 "스냅샷"을 찍어 파일을 보호할 수 있습니다. 일반적으로는 100MB 이상으로 매우 크거나, 거의 매일 열거나, **저장** 메뉴 옵션을 사용할 수 없는 파일은 이 방법으로 보호해야 합니다. 이러한 유형에 속하는 일반 파일은 전자 메일 및 데이터베이스 파일입니다.

Data Protector for PCs에는 **Microsoft Outlook, Microsoft Outlook Express, Windows Mail** 및 **Thunderbird**. 이러한 정책으로 시작하거나 사용자 고유의 정책을 작성할 수 있습니다.

참고: Data Protector for PCs는 Open File Protection 정책을 통해 EFS 암호화된 파일의 백업을 지원하지 않으므로 .pst와 같은 파일은 EFS 암호화되어서는 안 됩니다.

파일 보호 정책을 생성하려면

- a. 왼쪽 탐색 창에서 **정책**을 클릭합니다.
- b. **파일 보호 정책 설정**을 클릭합니다.
- c. **계속적인 파일 보호 정책 새롭게 생성** 또는 **개방 파일 보호 정책 새롭게 생성**을 클릭합니다.
- d. 창에 나타난 지침을 따릅니다.

참고: 파일 보호 정책을 생성하고 제외 또는 포함 규칙을 설정할 때 파일 확장명이 Open File Protection 정책의 경우 9자, Continuous File Protection 정책의 경우 29자를 초과해서는 안 됩니다.

Open File Protection 정책의 경우 포함 규칙에서 확장명이 없는 파일을 선택할 수 있습니다. Continuous File Protection 정책의 경우 확장명 없이 파일을 선택할 수 없습니다.

- ① **중요:** 현재 Data Protector for PCs가 필요로 하는 기본 정책이 모두 구성되어 있는 상태입니다. Data Protector for PCs는 대부분의 조직에 충분한 다른 정책이 미리 구성된 상태로 제공됩니다. 사용자의 데스크톱 및 랩톱에 Agent를 설치하는 것을 지금 바로 시작하는 것이 좋습니다([“Data Protector for PCs Agent 설치” \(35 페이지\)](#) 참조). 나중에 정리 정책, 사용자 정의 컨트롤 정책, Agent 업데이트 정책 및 데이터 보존 보고 정책과 같은 남아 있는 Data Protector for PCs 정책을 검토하고 구성하기 위해 돌아갈 수 있습니다.
-

남아 있는 정책 구성

1. **Active Directory 액세스**를 구성합니다.

참고: **Active Directory 그룹과 Data Vault 연결:** Data Vault 정책에서 Data Vault를 Active Directory 그룹과 연결시킬 수 있습니다. 연결된 그룹의 모든 일원은 연결된 Data Vault에 백업합니다. 개별 사용자는 연결시킬 수 없습니다. 또한 OU(조직 단위)를 연결시키는 경우 해당 OU 내의 그룹만이 연결됩니다. OU에 직접 소속되어 있는 모든 사용자는 Data Vault에 연결되지 않습니다. Active Directory 그룹의 목록에 배포 그룹과 같은 보안 그룹 이외의 그룹이 잘못 포함될 수도 있습니다. 그러나 보안 그룹만이 Data Vault와 실제로 연결됩니다.

여러 사용자: 두 명 이상의 사용자가 한 대의 컴퓨터를 공유하고 있는 경우 두 명 이상의 사용자는 같은 Active Directory 그룹에 속해야 합니다.

그룹 또는 조직 단위 별로 Data Vault를 할당하거나 그룹 또는 조직 단위 별로 보고하려면 Active Directory에 액세스할 수 있도록 Policy Server를 구성해야 합니다. Active Directory 액세스를 구성하면 Data Vault를 위한 **그룹 일원 및 조직 단위** 옵션을 사용할 수 있습니다(**“처음으로 구성”** (23 페이지) 참조).

Active Directory 액세스를 구성하는 방법:

- a. 왼쪽 탐색 창에서 **구성**을 클릭합니다.
- b. **Active Directory 액세스 구성**을 클릭합니다.
- c. 창에 나타난 지침을 따릅니다.

2. 정리 정책을 구성합니다.

파일 보호 정책에 정의된 보존 설정보다 오래된 버전을 제거하기 위해 사용자 컴퓨터의 Data Protector for PCs Local Repository 및 Data Vault 서버의 Data Vault를 정기적으로 정리해야 합니다.

정리 정책을 구성하는 방법:

- a. 왼쪽 탐색 창에서 **정책**을 클릭합니다.
- b. **정리 정책 설정**을 클릭합니다.
- c. 창에 나타난 지침을 따릅니다.

Data Vault가 더 많은 사용자를 지원할 수 있도록 금요일 저녁 또는 토요일 이른 아침에 시작해서 주말에만 정리 프로세스를 실행합니다. 이렇게 하면 정리 프로세스가 실행될 수 있는 시간을 최대한 확보할 수 있습니다.

- a. Policy Server 관리 콘솔에서 정리 정책 페이지를 열고 **Data Vault 정리 일정**을 변경합니다.
- b. 금요일 또는 토요일을 제외한 모든 요일을 선택 해제합니다.
 - 금요일의 경우 저녁 늦은 시간(예: 오후 10시)을 시작 시간으로 선택합니다.
 - 토요일의 경우 아침 이른 시간(새벽 1시)을 시작 시간으로 선택합니다.

주말에만 실행되는 정리의 경우:

- Data Vault에서 복원하기 위해 제공된 파일 목록은 늦어도 1주일 후에는 만료됩니다. 사용자는 항상 Data Vault에 있는 해당 데이터를 수동으로 다시 검사하여 최신 보기를 획득할 수 있습니다.
- 정리는 주말에만 실행되므로 백업 버전은 만료 시간이 지난 이후에도 최대 1주일까지 계속해서 존재합니다.
- 할당량 관리는 최신이 아닙니다. 사용자가 주어진 할당량을 초과하는 경우 사용자는 Data Vault의 사용 가능한 공간을 다시 확보하기 위해 정리가 실행될 때까지 기다려야 할지도 모릅니다. 반면 공간 사용 보고는 정리 프로세스의 일부이므로 시스템에서 할당량 초과를 즉시 인식하지 못할 수도 있습니다.

모범 사례

- **로컬 저장소 정리 일정:** 정리 일정을 기본값인 1시간으로 유지합니다.
- **Data Vault 정리 일정:** "매일 자정에 정리"에 대한 기본 설정은 대부분의 설치에 만족스러워야 합니다. Data Vault 용량에 대한 자세한 정보는 "[크기 조정 권장 사항](#)" (30 페이지)를 참조하십시오.
- CPU 및 디스크 활용도를 높이기 위해 재사용 가능 및 확장 가능한 방법으로 여러 스레드를 사용하여 DPNECleanup을 구성할 수 있으므로 더 많은 데이터를 저장할 수 있습니다. "[다중 스레드 정리 구성](#)" (33 페이지)을 참조하십시오.

3. 사용자 정의 컨트롤 정책을 구성합니다.

사용자 정의 컨트롤 정책은 컴퓨터에 배포된 회사 정책에 대한 사용자의 제어 수준을 결정할 수 있습니다.

사용자 정의 컨트롤 정책을 구성하는 방법:

- a. 왼쪽 탐색 창에서 **정책**을 클릭합니다.
- b. **사용자 정의 컨트롤 정책 설정**을 클릭합니다.
- c. 창에 나타난 지침을 따릅니다.

모범 사례

자체 서비스 복구에 대해 **사용자 정의 컨트롤 허용**을 설정합니다.

4. Agent 업데이트 정책을 구성합니다.

정책은 이 버전으로 자동 업데이트되는 Data Protector for PCs로 보호된 모든 데스크톱 및 랩톱에서 사용할 Data Protector for PCs Agent 버전을 지정합니다.

Agent 업데이트 정책을 구성하는 방법:

- a. 왼쪽 탐색 창에서 **정책**을 클릭합니다.
- b. **Agent 업데이트 정책 설정**을 클릭합니다.
- c. 창에 나타난 지침을 따릅니다.

5. 데이터 보존 보고를 구성합니다.

각각의 주요 정보 범주에 대해 보고용으로 데이터가 보관되는 기간을 설정할 수 있습니다.

데이터 보존 보고를 구성하는 방법:

- 왼쪽 탐색 창에서 **구성**을 클릭합니다.
- 데이터 보존 보고 구성**을 클릭합니다.
- 창에 나타난 지침을 따릅니다.

기타 구성 작업

기타 구성 작업은 보통 Data Protector for PCs를 처음으로 설치할 때 수행됩니다.

Data Protector for PCs 소프트웨어에 라이선스를 부여합니다.

Data Protector for PCs를 평가하고 있는 경우 사용자를 무제한으로 보호하기 위해 Data Protector for PCs를 추가 라이선스 없이 60일 동안 사용할 수 있습니다. Data Protector for PCs를 구입하는 경우 HP License Key Delivery Service (<https://webware.hp.com/welcome.asp>)로 이동하여 입력할 수 있는 라이선스 키를 다운로드합니다.

라이선스 키를 입력하려면

- 왼쪽 탐색 창에서 **라이선스 관리**를 클릭합니다.
- HP Data Protector for PCs사용자에 대한 라이선스 키 입력**을 클릭합니다.
- 창에 나타난 지침을 따릅니다.

입력할 여러 개의 라이선스가 있는 경우 각 줄에 라이선스 키 스트링 하나가 있는 텍스트 파일을 생성할 수 있습니다. 그런 다음 라이선스 키 가져오기 필드를 사용하여 파일을 가져올 수 있습니다.

참고: Agent가 설치되면 라이선스는 Agent에 배포됩니다.

라이선스 이동

해당 서버를 다른 시스템으로 옮기기 위해 Policy Server의 IP 주소를 변경해야 하거나 한 Policy Server에서 다른 서버로 라이선스를 옮겨야 하는 경우 HP License Key Delivery Service (<https://webware.hp.com/welcome.asp>)에 문의하십시오.

암호화된 비밀번호를 설정하고 가져오고 내보냅니다.

보안상의 이유로 암호화된 비밀번호를 정의해야 Data Protector for PCs를 사용할 수 있습니다. 이렇게 하면 모든 파일이 사용자의 컴퓨터에서 암호화되고 암호화된 상태로 네트워크를 통해 전송됩니다. 같은 비밀번호를 사용하여 모든 사용자 및 중앙에서 구성된 모든 Data Vault의 파일을 암호화합니다.

- 중앙에서 정의된 Data Vault(Policy Server 콘솔을 통해 정의)는 항상 Data Protector for PCs 암호화된 비밀번호에 근거한 암호화를 사용합니다.
- 로컬로 정의된 Data Vault(해당 컴퓨터를 통해 사용자가 정의)의 경우 사용자는 암호화 사용 여부를 선택하고 고유한 비밀번호를 선택할 수 있습니다.

Data Protector for PCs를 처음으로 설치하는 경우 비밀번호를 생성 또는 가져와야 계속 진행할 수 있습니다. 보안상의 이유로 비밀번호를 생성한 후에 비밀번호를 내보냅니다. 그러면 안전한 위치에 비밀번호가 저장되고 나중에 가져오는 데 비밀번호를 사용할 수 있습니다.

참고: 비밀번호를 생성하거나 가져온 후에는 비밀번호를 변경할 수 없습니다.

암호화된 비밀번호를 관리하려면

1. 왼쪽 탐색 창에서 **정책**을 클릭합니다.
2. **암호화 정책**을 클릭합니다.
3. 창에 나타난 지침을 따릅니다.

지원할 수 있는 Agent 수 결정

모든 환경에 유효한 일반적인 규칙을 부여하기는 어려우므로 여기에 제시된 사례에서는 주어진 수가 유효한 문맥에 대해 명확히 설명하고 있습니다.

크기 조정에 영향을 미치는 요소

Data Protector for PCs 환경의 크기를 조정하는 것은 복잡합니다. 특정 환경이 지원할 수 있는 사용자의 수에 영향을 미치는 기술적 요인에는 다음이 포함됩니다.

- Data Vault의 처리 전원(밤마다 수행하는 백업 데이터의 통합을 위해)
- Data Vault 서버의 네트워크 및 I/O 대역폭
- Data Vault 서버의 디스크 공간
- Policy Server의 SQL 데이터베이스 크기
- Policy Server의 네트워크 대역폭 및 처리 전원

다음 중 주어진 설치에서 병목 현상을 유발할 수 있는 것이 무엇인지는 Data Protector for PCs 구성과 사용 패턴 모두에 의해 결정됩니다.

- Data Vault의 사용자 수
- 구성된 보호 정책에 의해 보장되는 파일 수 및 크기
- 보호된 파일의 변경 빈도
- 보호된 파일 유형에 대한 보존 설정

크기 조정 권장 사항

Data Vault

평균 데이터 특징이 아래와 비슷할 경우 매일 수행되는 정리 일정을 통해 14TB 디스크 공간을 가진 Data Vault는 최대 **3,500** Agent 사용자를 지원할 수 있습니다.

- 보호된 파일의 평균 개수: 5000
- 로컬 디스크에 있는 보호된 파일의 평균 전체 크기: 10 GB

- Data Vault의 평균 전체 크기(압축): 4 GB

이 예에서 보다 평균적으로 더 많은 데이터를 보호해야 하는 경우 Data Vault의 단순히 늘어나는 디스크 용량은 데이터를 위한 공간을 추가로 확보하지만 Data Vault는 밤마다 수행되는 백업 데이터의 통합을 더 이상 적절한 시기에 완료할 수 없을지도 모릅니다. 다음 가능성을 고려하십시오.

- 주말에만 Data Vault 정리를 실행합니다. 이를 수행하는 방법에 대한 자세한 내용은 ["남아 있는 정책 구성" \(26 페이지\)](#)의 2단계 "정리 정책 구성"을 참조하십시오. 40TB 디스크 공간을 가진 Data Vault가 지원할 수 있는 Agent 수를 동일한 평균 데이터 특징이 주어진 10,000개로 늘려야 합니다.
- 여러 Data Vault에 최종 사용자 데이터를 배포하는 것을 고려합니다.

그러한 Data Vault에 대한 하드웨어 사양은 아래와 같습니다.

Data Vault 유형	매일 정리 (최대 3,500개의 Agent)	매주 정리 (최대 10,000개의 Agent)
Windows 파일 공유	3GHz 듀얼 코어, 4GB RAM, 14TB 디스크 공간	3GHz 듀얼 코어, 4GB RAM, 40TB 디스크 공간
웹 Data Vault	3GHz 쿼드 코어, 4GB RAM, 14TB 디스크 공간	3GHz 쿼드 코어, 4GB RAM, 40TB 디스크 공간

사용자가 평균 이하의 데이터 양을 가지고 있는 경우 Data Vault의 사용자 수 이상을 호스트할 수 있습니다.

참고: HP는 최상의 성능을 위해 Data Vault의 운영 체제 및 물리적으로 분리된 디스크에 백업 데이터를 유지할 것을 강력히 권장합니다.

최상의 성능을 위해 Data Vault 디스크를 정기적으로 조각 모음해야 합니다.

Policy Server

Policy Server에 발생한 트래픽 양은 서버가 호스트한 Agent 수와 직접적인 관련이 있습니다. Data Protector for PCs가 포함되어 있는 MS SQL Server의 Express Edition을 사용하면 4GB의 최대 데이터베이스 크기가 부과되며 5,000개 이하의 Agent를¹ 지원할 수 있습니다.

해당 환경에 5,000개 이상의 Agent를 지원해야 하는 경우 Policy Server를 추가하거나 MS SQL Express를 Microsoft SQL Server의 풀 버전으로 교체할 수 있습니다. 이 방법으로 Policy Server는 최대 50,000개까지 Agent를 쉽게 늘릴 수 있습니다. MS SQL Server의 풀 버전을 사용하기로 결정한 경우 Policy Server의 메인 메모리를 최소 3GB 이상으로 업그레이드하는 것을 고려하십시오.

성능상의 이유로 Policy Server는 Data Vault 서버와 별도인 서버에서 실행되어야 합니다. 같은 서버에서 둘 모두를 실행할 수 있지만 같은 서버에서 실행하는 것은 평가 목적에만 적합합니다.

1. Policy Server의 "데이터 보존 보고"에 대한 기본 설정인 30일 사용.

최소 하나 이상의 Policy Server가 있어야 하지만 Data Vault와 Policy Server의 수를 일치시킬 필요는 없습니다.

네트워킹 고려 사항

참고: 웹 Data Vault는 긴 대기 시간의 영향을 받지 않습니다. 다음은 Windows 파일 공유 Data Vault에만 적용됩니다.

들 사이의 네트워크 지연이 50ms 이상인 경우 일반적으로 Windows 파일 공유 Data Vault에 대해 HP는 Data Protector for PCs Agent에서 Data Vault로 초기 업데이트를 수행하는 것을 권장하지 않습니다. 이는 보통 WAN 연결이 느린 홈 오피스 또는 원격 사무실에 적용됩니다. 초기 업데이트가 수행되는 데 매우 오랜 시간이 소요됩니다.

여러 장소에 사무실이 위치해 있고 일부 사무실의 네트워크 지연이 50ms 이상인 환경의 경우 모든 사무실이 지연 시간이 50ms 미만인 최소 하나 이상의 Data Vault에 도달할 수 있도록 하나 이상의 장소에 Data Vault를 설치하는 것을 고려하십시오.

초기 업데이트가 완료되면 회사 네트워크를 통해 모든 위치에서 또는 홈 오피스에서 업데이트를 수행할 수 있습니다. 업데이트는 느린 네트워크 연결을 사용해서 진행할 수 있을 정도로 작습니다.

초기 업데이트를 지연 시간이 긴 연결을 통해 수행해야 하는 경우 업데이트가 완료되는 데 수일이 걸릴 수도 있지만 업데이트를 온전히 중단할 수 있습니다. Data Protector for PCs는 Data Vault에 다시 연결되자마자 중단된 시점부터 업데이트를 계속합니다.



팁: 사무실 간의 지연 시간을 모르는 경우 한 장소에 있는 컴퓨터에서 ping 명령을 사용하여 다른 장소에 있는 컴퓨터를 ping합니다. 각각의 ping이 완료되면 지연 시간을 보고합니다.

5 다중 스레드 정리 구성

DPNECleanup의 성능은 Data Vault에 있는 백업 사용자 데이터의 양을 제한합니다. CPU 및 디스크 활용도를 높이기 위해 재사용 가능 및 확장 가능한 방법으로 여러 스레드를 사용하여 DPNECleanup을 구성할 수 있으므로 더 많은 데이터를 저장할 수 있습니다.

다중 스레드 정리를 통해 스케줄러 인수 '-s'는 기본적으로 다중 스레드 정리와 자동 조정장치에 대한 1초 지연을 포함하는 기본 인수 '-e -f -u -p -d 1000'으로 이어집니다. 예를 들어 다중 스레드 실행을 비활성화하거나 이를 조정하기 위해 이러한 기본값을 사용하지 않으려면 스케줄러 호출에서 '-s' 인수를 삭제하거나 개별 CLI 인수를 추가합니다.

참고:

일부 환경에서 다중 스레드 정리를 비활성화하고 싶은 경우에도 Data Vault의 정리 호출을 위해 '-e -f -u'를 인수로 유지하는 것이 좋습니다.

CLI에서 DPNECleanup.exe 사용

DPNECleanup.exe에 대한 인수 -p는 정리가 초기화되고 병렬 엔진이 시작되도록 함으로써 다중 스레드 실행을 활성화합니다. 병렬 엔진은 7개의 선택적인 명령줄 인수를 제공합니다. DPNECleanup 실행 파일은 이러한 인수를 검색해서 병렬 엔진에 전달할 수 있습니다.

DPNECleanup은 -p가 설정되어 있지 않은 경우 직렬 모드로 실행됩니다. 직렬 모드에서 병렬 엔진은 전혀 사용되지 않습니다.

dpnecleanup

-a affinity

프로세서 선호도를 스레드가 사용할 CPU 코어에 대해 설정된 비트를 반영하는 주어진 수로 설정합니다.

-d delay

자동 조정장치가 해당 작업을 시작하기 전에 지연을 1,000분의 1초로 설정하면서 병렬 엔진에 많은 수의 스레드를 시작하고 일부 시스템 사용률을 생성할 수 있는 시간을 줍니다. 기본적으로 -s 인수는 1,000분의 1초 또는 1초의 지연을 유발합니다.

-m maxCpuUsage

원하는 최대 CPU 사용률(affinity에서 정의한 모든 코어)을 자동 조정장치가 도달하려고 하는 maxCpuUsage%로 설정합니다. maxCpuUsage는 1~100 사이의 정수여야 합니다. 기본값은 제한 없음(CPU 사용률 최대)을 의미하는 '0'입니다.

-o

자동 조정장치를 의미하는 상수 리소스는 비활성화되어 있으며 병렬 엔진은 동시 스레드의 수를 변경하지 않습니다. -r을 사용하여 동시 스레드의 수를 조정합니다. 인수 -d, -m 및 -q는 -o와 함께 실행될 때 무시됩니다.

-p

다중 스레드 정리를 활성화합니다.

-q maxQueueLength

자동 조정장치가 도달하려고 하는 원하는 최대 평균 디스크 큐 길이를 설정합니다. 값은 부동 소수점 숫자여야 합니다. 기본값은 2.0입니다.

-r resourceCount

동시 리소스(스레드)의 수를 주어진 수로 설정합니다. 시스템은 기본적으로 그리고 옵션 -o와 결합하여 2개(CPU 수)의 동시 스레드와 함께 작동합니다. 자동 조정장치가 실행되고 있는 경우 주어진 값은 스레드에 관한 동시 리소스의 제한을 나타냅니다. 여기에서 최대 개수의 기본값은 제한 없음을 의미하는 '0'입니다.

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

모든 스레드에 대한 프로세스 우선 순위를 설정합니다. 기본값은 Normal입니다.

-s

서버 정리. 중앙에서 정의되었든 아니면 사용자가 정의했든 이와 상관없이 모든 Data Vault에 대한 정리를 설정합니다. 명령이 실행되면 다중 스레드 동작을 통해 인수 '-e -f -u -p -d 1000'으로 대체됩니다.

-e

엔터프라이즈 정리. Policy Server에서 정책에 의해 중앙에서 정의된 모든 Data Vault에 대한 정리를 설정합니다.

-f

빠른 정리. 보통 Agent Cleanup은 시스템이 유틸 상태에 있는 경우에만 실행됩니다. 이 옵션을 통해 언제든지 Cleanup을 시작할 수 있습니다.

-u

사용자 정의 정리. 사용자가 생성한 로컬 정책에 의해 정의된 모든 로컬 Data Vault에 대한 정리를 설정합니다.

6 Data Protector for PCs Agent 설치

참고: Agent가 설치되면 라이선스는 Agent에 배포됩니다.

두 가지 방법으로 Data Protector for PCs Agent를 설치할 수 있습니다.

- 각 클라이언트 컴퓨터에 개별적으로 설치할 수 있습니다. “[개별 클라이언트 컴퓨터에 Data Protector for PCs Agent 설치](#)” (35 페이지)를 참조하십시오.
- 모든 클라이언트 컴퓨터에 액세스할 수 있는 파일 서버의 엔터프라이즈 전체에 배포됩니다. “[엔터프라이즈 전체에 Data Protector for PCs Agent 배포](#)” (36 페이지)를 참조하십시오.


개별 클라이언트 컴퓨터에 Data Protector for PCs Agent 설치

필수 구성 요소

Data Protector for PCs Agent 소프트웨어는 Windows를 실행하는 사용자의 데스크톱 및 노트북에 설치될 수 있습니다. 지원되는 플랫폼에 대해서는 지원 매트릭스를 참조하십시오.

"관리자" 권한으로 계정에 로그인해야 합니다.

설치 절차

1. Data Protector for PCs 설치 CD-ROM을 삽입합니다. 설치 마법사가 자동으로 시작되어야 합니다. 설치 마법사가 자동으로 시작되지 않으면 설치 CD-ROM의 해당 루트에서 `setup.hta`를 두 번 클릭하여 수동으로 실행합니다.
2. **Data Protector for PCs Agent 소프트웨어 설치 또는 업데이트**를 클릭합니다. "열기 또는 저장" 대화 상자가 나타난 경우 **열기** 또는 **실행**을 선택합니다.
3. 사용자 컴퓨터에 Microsoft Windows Installer 3.1 이상이 설치되어 있지 않은 경우 마법사를 통해 이를 설치할 수 있습니다. Windows Installer 업데이트 대화 상자가 나타나면 **확인**을 클릭하여 설치합니다.
4. 사용자 컴퓨터에 Microsoft .NET Framework 2.0 SP1 이상이 설치되어 있지 않은 경우 마법사를 통해 이를 설치할 수 있습니다. Microsoft .NET Framework 2.0 SP1 설치 대화 상자가 나타나면 **확인**을 클릭하여 설치합니다.
5. 마법사가 Data Protector for PCs Agent를 자동으로 설치합니다. 화면상의 지침을 따릅니다. 설치 중 Policy Server의 세부 정보를 입력해 달라는 창이 나타납니다.
6. 설치 및 구성이 완료되면 **마침**을 클릭합니다. Policy Server에 Open File Protection 정책이 설정되어 있으면 시스템을 다시 부팅할 것인지 묻는 메시지가 나타납니다. 이제 시스템 트레이에 Data Protector for PCs 아이콘이 나타납니다(하나의 아이콘이 나타나며 나타나는 아이콘은 보호 상태에 따라 다름: ).
7. Data Protector for PCs Agent가 올바르게 작동하는지 테스트합니다.

- a. 바탕 화면에 있는 Word 문서 또는 Excel 스프레드시트와 같은 테스트 파일을 선택하거나 생성합니다. 해당 문서를 적절히 변경한 다음 **저장**을 클릭합니다.
 - b. 바탕 화면, Windows 탐색기 또는 열기 대화 상자에서 테스트 파일을 마우스 오른쪽 단추로 클릭합니다. 다음과 같은 세 가지 Data Protector for PCs 항목이 메뉴에 나타납니다(**파일 검색 및 복구...**, **버전 복사 및 XXX에서 버전 열기...**).
 - c. **XXX에서 버전 열기...**를 선택하면 지금 방금 생성했거나 편집한 문서의 타임 스탬프 버전에 대한 목록이 나타납니다. 버전 하나를 선택하면 해당 응용 프로그램에서 읽기 전용 문서로 열립니다. 이런 식으로 사용자는 로컬 Data Protector for PCs 저장소에서 해당 문서의 이전 버전을 복구합니다.
8. Data Protector for PCs에 의해 보호되기를 원하는 다른 사용자 데스크톱 및 랩톱에 1~8단계를 반복 수행합니다.

엔터프라이즈 전체에 Data Protector for PCs Agent 배포

설치 CD-ROM에 포함된 Data Protector for PCs Agent 배포 키트를 사용하여 엔터프라이즈 전체에 Data Protector for PCs Agent를 처음에 배포할 수 있습니다.

참고: UAC(사용자 계정 컨트롤)가 활성화되어 있는 Vista PC에서는 배포 키트를 사용할 수 없습니다. 이를 해결하려면 UAC를 비활성화하거나 Agent를 대화형으로 설치합니다.

아래 절차에 따라 CD-ROM:\Agent에 있는 Data Protector for PCs Agent 배포 키트를 모든 사용자가 액세스할 수 있는 파일 서버의 디렉터리로 복사합니다. 그런 다음 SetupConfig.exe를 사용하여 해당 디렉터리 내에 매개 변수 파일을 생성합니다. 마지막으로 메커니즘을 구축하여 각 사용자 컴퓨터의 공유된 디렉터리에 있는 StartInstall.exe를 실행합니다. 예를 들어 로그인 스크립트를 사용할 수 있습니다. 그런 다음 Data Protector for PCs Policy Server 콘솔에서 Agent 배포 키트 보고서를 사용하여 배포를 모니터링할 수 있습니다.

키트 내용물

Data Protector for PCs 배포 키트에는 다음 구성 요소가 포함되어 있습니다.

SetupConfig.exe	초기화 파일을 생성하고 편집합니다.
StartInstall.exe	권한 있는 사용자로 Setup.exe를 시작합니다.
Setup.exe	필수 구성 요소 및 DataProtectorNE.ini를 설치합니다.
DataProtectorNE.msi	Agent 소프트웨어를 설치하기 위한 Data Protector for PCs Windows Installer 패키지
DataProtectorNE64.msi	Agent 소프트웨어를 64비트 컴퓨터에 설치하기 위한 Data Protector for PCs Windows Installer 패키지
DataProtectorNE*. *.mst	번역된 Agent 소프트웨어를 설치하기 위한 Data Protector for PCs Windows Installer 패키지

WindowsInstaller.exe

Windows Installer를 업데이트합니다(.NET installation 설치에 필요).

NetFx20SP1_x64.exe,
NetFx20SP1_x86.exe

NET Framework 2.0 SP1을 설치합니다.

Setup.ini

Data Protector for PCs 설치 매개 변수 파일. 이 파일은 SetupConfig.exe를 사용하여 생성됩니다 (아래 4단계 참조).

배포 및 설치 절차

1. 배포 CD-ROM의 Agent 디렉터리에 있는 파일을 Data Protector for PCs Agent 배포 키트를 사용하려고 하는 모든 사용자가 액세스할 수 있는 디렉터리로 복사합니다. 이 디렉터리는 \\yourserver\DPNEDeploy와 같은 일반적인 netlogon 공유의 디렉터리가 될 수 있습니다.
2. 새로 생성한 디렉터리에 위에서 언급한 파일이 포함되어 있는지 확인합니다. 다른 모든 파일을 삭제할 수 있습니다.
3. 1단계에서 생성한 디렉터리에 대해 DOS 명령 창(cmd.exe) 및 cd를 엽니다.
4. SetupConfig.exe를 실행하여 매개 변수 파일 Setup.ini를 생성하거나 편집합니다. SetupConfig.exe를 처음으로 실행할 때 모든 매개 변수에 대한 값을 입력해야 합니다. 그 후 SetupConfig.exe를 반복해서 실행하여 매개 변수를 변경할 수 있습니다. 매개 변수를 변경하지 않으려면 **Enter**를 누르기만 하면 됩니다. 필요한 매개 변수는 다음과 같습니다.
 - **설치 패키지에 대한 UNC 경로** - \\yourserver\DPNEDeploy와 같이 1단계에서 파일이 복사된 공유 디렉터리에 대한 완전한 경로
 - **Data Protector for PCs Policy Server**의 이름. 이 이름은 YOURSERVER와 같은 NetBIOS 이름 또는 yourserver.yourcompany.com과 같은 정규화된 도메인 이름이 될 수 있습니다.
 - **사용자 이름** - 도메인 관리 그룹의 일원 같은 Data Protector for PCs Agent 배포 키트를 사용하는 컴퓨터의 관리자 권한을 가지고 있는 사용자의 이름. YOURCOMPANY\JerryAdmin과 같은 도메인을 포함하고 있는 일반적인 정규화된 사용자 이름입니다.
 - **비밀번호** - 사용자 이름과 연결되어 있는 비밀번호. 확인을 위해 두 번 입력해야 합니다.
5. 클라이언트 컴퓨터에서 예를 들어 \\yourserver\DPNEDeploy\StartInstall에서 StartInstall.exe를 실행합니다. 그러면 Setup.ini에 지정된 사용자 이름과 비밀번호를 사용하여 Setup.exe가 백그라운드에서 낮은 우선 순위로 실행됩니다. 로그온 스크립트의 일부로 수행될 수 있습니다. 컴퓨터 계정에 충분한 네트워크 권한이 없으므로 시작 스크립트에 포함시킬 수 없습니다.
6. Setup.exe는 클라이언트 컴퓨터가 Data Protector for PCs를 지원할 수 있는지 여부를 결정합니다. 지원되는 Windows 플랫폼에 대해서는 지원 매트릭스를 참조하십시오.

7. Setup.exe는 .NET Framework 버전 2.0 SP1이 설치되어 있는지 여부를 확인합니다. 설치되어 있지 않은 경우 설치한 후 컴퓨터를 다시 부팅해야 할 수도 있습니다.
8. Setup.exe는 Data Protector for PCs가 이미 설치되어 있는지 여부를 확인합니다. 설치되어 있지 않거나 버전이 이전 버전이면 Data Protector for PCs를 설치합니다.

참고:

4-7단계에서 발생한 모든 오류는 Data Protector for PCs Policy Server 및 로컬 컴퓨터의 응용 프로그램 이벤트 로그에 메시지를 기록합니다.

Data Protector for PCs Policy Server 콘솔을 사용하여 Agent 배포 진행률을 확인할 수 있습니다.

1. Data Protector for PCs Policy Server 콘솔에 로그인합니다.
2. 왼쪽 탐색 창의 **보고서**에서 **Agent 배포**를 선택합니다.
지금까지의 초기 배포에 대한 요약이 표시됩니다. 다음과 같은 요약 내용이 표시됩니다.
 - 배포를 성공적으로 **완료한** 컴퓨터 수
 - **진행 중인** 배포 수
 - **실패한** 배포 수
3. **컴퓨터 수** 열에서 개수를 클릭하여 선택한 배포 상태에 컴퓨터의 목록을 표시합니다.
각 컴퓨터의 현재 상태가 표시됩니다. 예를 들어 특정 컴퓨터에서 배포가 실패한 경우 **정보** 열에 발생한 오류가 표시됩니다. 해당 NETBIOS 이름을 클릭하여 컴퓨터에 대한 세부 정보를 알아볼 수 있습니다.

7 Data Protector for PCs 업데이트

6.x 버전의 Data Protector for PCs를 7.0으로 업데이트하고 있는 경우 아래 순서에 따라 진행합니다.

1. Policy Server를 7.0으로 업데이트합니다. “Policy Server 업데이트” (39 페이지)를 참조하십시오.
2. 웹 Data Vault 서버를 설치합니다. “웹 Data Vault 서버 설치, 구성 및 유지” (18 페이지)의 웹 설치를 참조하십시오.
3. Agent를 7.0으로 업데이트합니다.

수동 업데이트를 사용하여 업데이트하거나 Agent 업데이트 정책을 사용하여 "자동으로" 업데이트할 수 있습니다. 자세한 내용은 “Agent 업데이트” (39 페이지)를 참조하십시오.

Policy Server 업데이트

표준 설치 절차에 따라 기존 Data Protector for PCs Policy Server 설치를 최신 버전으로 업데이트할 수 있습니다. 기존 모든 구성(예: Data Vault 구성, 라이선스 등)은 최신 버전에서 사용할 수 있습니다.

Policy Server 업데이트:

1. Data Protector for PCs 설치 CD-ROM을 삽입합니다. 설치 마법사가 자동으로 시작되지 않으면 설치 CD-ROM의 해당 루트에서 `setup.hta`를 두 번 클릭하여 수동으로 실행합니다.
2. 마법사의 Data Protector for PCs 설치 페이지에서 **Policy Server 설치**를 클릭하여 업데이트를 시작합니다.
3. 화면상의 지침을 따릅니다.
4. 설치 절차는 기존 Policy Server가 설치되어 있는지 여부를 감지하여 업데이트를 제공합니다.
5. 화면상의 지침을 따릅니다.
6. 설치가 완료되면 **다음**을 클릭합니다. 그러면 Data Protector for PCs Policy Server 콘솔 실행을 선택할 수 있습니다.

참고: Cleanup 소프트웨어가 Policy Server에 설치되어 있는 경우 이 소프트웨어도 업데이트해야 합니다. 수동으로 업데이트하거나 Agent 업데이트 정책을 사용하여 업데이트할 수 있습니다.

Agent 업데이트

Data Protector for PCs Server 버전을 업데이트하는 경우 Data Protector for PCs의 이전 버전을 사용하는 기존 Agent는 전과 변함없이 작동합니다. 수동 업데이트를 사용하여 업데이트하거나 Agent 업데이트 정책을 사용하여 "자동으로" 업데이트할 수 있습니다.

참고: 업데이트가 완료되면 Agent가 새로운 웹 Data Vault를 사용할 수 있도록 모든 Agent를 다시 부팅해야 합니다. 다시 부팅하라는 메시지가 시스템 트레이에 중선 메시지 형식으로 표시되며 해당 PC의 Data Protector for PCs 상태 패널의 요약 탭에도 표시됩니다.

Agent 업데이트 정책을 사용하여 Agent 자동 업데이트

Policy Server의 Agent 업데이트 정책을 사용하여 Agent를 "자동으로" 업데이트할 수 있습니다. 설치 패키지는 연결된 모든 클라이언트에게 자동으로 전달되고 완전히 자동화된 방식으로 업데이트가 완료됩니다. 최종 사용자의 간섭이 필요 없습니다.

1. Policy Server 콘솔에서 **정책->Agent 업데이트 정책**을 선택합니다.
2. Policy Server를 지금 방금 업데이트한 경우 설치 절차는 새 Agent 업데이트 패키지를 업로드한 상태입니다. Policy Server 콘솔에서 이 새 버전은 아직 선택되어 있지 않습니다.
새 Agent 버전을 선택하여 버전을 사용할 수 있는 상태로 만듭니다.
3. 제한을 조정하여 분당 허용된 최대 업데이트 수를 조정할 수 있습니다.
4. **Agent 업데이트 정책 저장**을 클릭합니다.
5. 이제 Agent는 최신 버전으로 자동 업데이트됩니다. 정리 Agent 또한 자동으로 업데이트됩니다.

참고: "Agent 배포" 보고서를 사용하여 Agent 업데이트 진행률을 확인할 수 있습니다.

Agent 수동 업데이트

기존 Data Protector for PCs Agent를 표준 설치 절차를 실행하여 최신 버전으로 업데이트할 수 있습니다.

Agent를 최신 버전으로 업데이트하기 전에 Agent 버전이 Data Protector for PCs Policy Server의 버전과 호환되는지 확인합니다.

1. Data Protector for PCs 설치 CD-ROM을 삽입합니다. 설치 마법사가 자동으로 시작되지 않으면 설치 CD-ROM의 해당 루트에서 `setup.hta`를 두 번 클릭하여 수동으로 실행합니다.
2. 마법사의 Data Protector for PCs 설치 페이지에서 **Agent 설치**를 클릭하여 업데이트를 시작합니다.
3. 화면상의 지침을 따릅니다.
4. 설치 절차는 기존 Agent가 설치되어 있는지 여부를 감지하여 업데이트를 제공합니다.
5. 화면상의 지침을 따릅니다.

8 Data Protector for PCs에 대한 지원을 받는 방법

1년 동안 Data Protector for PCs를 유지 관리해 줍니다. 지원되는 유지 관리 항목:

- 지원 전문가와 상담할 수 있는 전화 지원
- Data Protector for PCs Server 및 Data Protector for PCs Agent 소프트웨어 업데이트. Data Protector 웹 사이트에서 최신 버전 또는 CD-ROM 이미지를 다운로드할 수 있습니다. <http://www.hp.com/go/dataprotector>로 이동합니다.

용어 설명

Active Directory	(Windows 고유 용어) Windows 네트워크의 디렉터리 서비스. 네트워크 리소스에 대한 정보가 들어 있으며 사용자 및 응용 프로그램에 액세스할 수 있도록 합니다. 디렉터리 서비스는 서비스가 상주하는 실제 시스템에 상관없이 리소스의 이름을 지정하고 설명하고 위치를 지정하고 액세스 및 관리하는 일관된 방법을 제공합니다.
Agent	각 사용자의 데스크톱/랩톱에서 실행되는 Data Protector for PCs 소프트웨어. TCP 포트 80을 통해 웹 서비스(SOAP 및 XML)를 사용하여 Policy Server와 통신합니다.
Continuous File Protection	Continuous File Protection은 파일을 저장할 때마다 파일에 변경 사항을 자동으로 저장하는 Data Protector for PCs의 Continuous Data Protection 방법입니다. 이 정책은 사용자가 저장하는 데이터 파일에 적합합니다(데이터베이스 또는 Outlook 파일과 같이 항상 개방된 파일과 반대). 각 Continuous File Protection 정책은 어떠한 식으로든 관련되어 있는 파일 그룹을 보호합니다. Data Protector for PCs는 Office 문서 및 사진과 같은 흔히 사용되는 파일 유형에 대한 정책이 미리 구성된 상태로 제공됩니다. 이러한 파일 보호 정책을 편집하거나 사용자 고유의 정책을 만들 수 있습니다. 또한 보호된 파일의 이전 버전이 보존되는 기간을 지정할 수도 있습니다.
Data Vault	Data Vault에는 두 가지 유형이 있습니다. <ul style="list-style-type: none">• 웹 Data Vault. 웹 Data Vault는 HTTPS 프로토콜을 사용하고 클라이언트 PC와 Data Vault 사이에 데이터를 전송할 수 있도록 최상위 수준의 보안과 지연 시간이 긴 환경에 높은 처리량을 제공하며 이러한 사항이 권장됩니다.• Windows 파일 공유 Data Vault. Data Vault 정책에 따라 파일이 저장된 파일 서버에는 공유 폴더가 있습니다. 파일 서버는 Windows 파일 공유 프로토콜(CIFS/SMB)을 지원해야 합니다. 또한 대기 시간이 많은 환경에서는 사용할 수 없습니다. Data Vault의 두 가지 유형에 대한 데이터 구조는 모두 동일하므로 Windows 파일 공유 Data Vault를 웹 Data Vault로 변환할 수 있습니다. <p>사용자는 그룹 또는 조직 단위 구성원을 기반으로 하나 이상의 Data Vault 정책을 지정할 수 있습니다.</p>
Local Repository	Local Repository는 보통 시스템 하드 디스크 드라이브에 보호된 파일 및 파일 변경 사항을 저장하는 데 사용된 Agent 컴퓨터의 안전한 저장 위치입니다. Local Repository는 숨겨진 시스템 디렉터리입니다. 사용자는 바탕 화면, Windows 탐색기 또는 "열기" 대화 상자에서 해당 파일을 마우스 오른쪽 단추로 클릭하여 이전 버전을 빠르게 복구할 수 있습니다. Continuous File Protection 정책으로 보호되는 파일은 보존 기간에는 로컬 컴퓨터의 숨겨진 디렉터리에 보관됩니다. Open File Protection 정책에 의해 보호된 파일은 Data Vault로 복사될 때까지 로컬 버전 저장소에 임시로 저장됩니다. Local Repository 경로는 보통 <code>C:\{DPNE}</code> 입니다.
Open File Protection	Open File Protection은 Outlook 개인 폴더와 같은 항상 열려 있는 파일 및 많은 데이터베이스 파일을 정기적으로 파일 수준 스냅샷을 찍어서 백업합니다. 이는 때때로 "비슷한" Continuous Data Protection이라고 불리기도 합니다. Open File Protection 정책은 포함 및 제외 규칙 집합에 의해 정의된 열려 있는 파일에 대한 보호를 정의합니다. 예를 들어 포함 규칙을 "끝 스트링 '.pst'"로 지정하여 Outlook .pst 파일에 적용되는 "Outlook 개인 폴더"라는 정책을 정의할 수도 있습니다. 보관된 .pst 파일을 제외하려고 했던 경우 제외 규칙을 "포함 스트링 'archive'"로 생성할 수 있었습니다. 정책은 또한 보호된 파일의 이전 버전이 보존되는 기간도 지정합니다. Open File Protection 정책은 모든 사용자에게 적용됩니다.
Policy Server	Policy Server는 Data Protector for PCs 정책에 대한 중앙 관리를 제공합니다. 또한 Agent에서 상태 정보를 수집하고 배포 및 작업에 대한 보고서를 제공합니다.
관리자	Data Vault를 생성 및 삭제하고 클라이언트 백업 데이터 이전 등의 관리 작업을 수행하는 웹 Data Vault 서버의 사용자입니다.

백업 사용자	파일의 백업 및 복원 등의 최종 사용자 작업을 수행하는 웹 Data Vault 서버의 사용자입니다.
보호된 파일	보호된 파일은 Data Protector for PCs에 의해 자동으로 백업된 파일입니다. 보호되는 파일 유형은 Continuous File Protection 정책 및 Open File Protection 정책으로 정의됩니다.
복사 정책	<p>복사 정책은 다음 항목을 정의합니다.</p> <ul style="list-style-type: none"> • 파일을 Data Vault에 동시에 복사할 수 있는 Agent 수 • 사용자가 예상한 모든 파일이 Data Vault에 존재하는지 확인하는 정기 업데이트 일정에서 이 파일이 없을 경우 누락된 파일을 복사합니다. 이 과정에서 모든 사용자 파일이 Data Vault에 제대로 복사되었는지 추가로 확인합니다. • 초기 업데이트를 수행해야 하는 경우입니다. 정상적인 Data Protector for PCs 작동 중 사용자가 Data Protector for PCs에서 지속적으로 보호되는 파일을 변경할 때마다 변경되는 파일의 정보만 Data Vault에 복사해야 하므로 초기 업데이트가 필요합니다. <p>Data Protector for PCs를 지금 방금 설치한 경우 복사 정책을 설정하여 사용자의 보호된 파일을 모두 초기 업데이트해야 합니다.</p>
사용자 정의 컨트롤 정책	이 정책은 데스크톱/랩톱/노트북에서 실행되는 Agent 소프트웨어에 대해 개인 사용자가 가지는 제어 수준을 결정합니다. Agent를 잠가 사용자가 볼 수 없도록 정책을 완전히 숨기거나, 사용자가 정책을 변경하지 못하고 볼 수만 있도록 하거나, 사용자가 자신의 정책을 추가하도록 할 수 있습니다. 각 주요 Data Protector for PCs 정책에 대한 제어 수준을 별도로 설정할 수 있습니다. 사용자 정의 컨트롤 정책은 모든 사용자에게 적용됩니다.
정리 정책	파일 보호 정책에서 설정한 보존 기간은 정기적으로 실행되는 정리 작업에 의해 적용됩니다. 빈도는 정리 정책에서 정의됩니다. 기본적으로 사용자의 Local Repository는 매 시간 정리되고 로컬에서 정의된 모든 Data Vault는 하루에 한 번 정리됩니다. 중앙에서 정의된 Windows 파일 공유 Data Vault는 Data Vault 정책을 통해 할당된 컴퓨터에 의해 정리되고 웹 Data Vault는 Data Vault 서버에서 로컬로 실행되는 정리 소프트웨어에 의해 정리됩니다. 정리 정책은 모든 사용자에게 적용됩니다.
정책	정책은 Policy Server의 중앙에서 정의한 규칙 집합이고 각 데스크톱/랩톱/노트북에서 Agent에 의해 실행됩니다.
초기 업데이트	Data Protector for PCs는 사용자가 변경 사항을 저장하여 파일을 수정할 때 파일을 지속적으로 보호합니다. 사용자가 새로운 Data Vault를 생성할 때마다 Data Protector for PCs는 사용자의 보호된 모든 파일을 해당 Vault에 초기 업데이트해야 합니다. 사용자는 초기 업데이트가 수행되는 방법을 즉시 또는 백그라운드 중에서 선택할 수 있습니다.
콘솔	브라우저 기반 콘솔은 Data Protector for PCs 정책을 정의하는 중앙 위치입니다. 콘솔을 사용하려면 관리자 그룹의 구성원이어야 합니다.

색인

심볼

.NET Framework, 15, 35

A

Active Directory

그룹과 Data Vault 연결, 26
액세스, 26

Active Directory에 액세스, 26

Agent, 8

업데이트, 39
필수 구성 요소, 13

Agent 배포 보고서, 40

Agent 배포 키트 내용을, 36

Agent 소프트웨어

설치, 35
엔터프라이즈 전체에 배포, 36

Agent 소프트웨어 배포, 36

절차, 37

진행률 확인, 38

Agent 업데이트 정책, 28

Agents

지원할 수 있는 수, 30

ASP.NET, 15

C

Cleanup 소프트웨어, 18

CLI 명령

DPNECleanup, 33

DvConfig, 20

Continuous File Protection 정책, 25

D

Data Protector for PCs

Agent 설치, 35

개요, 8

구조, 8

지원 받기, 41

Data Protector for PCs 평가, 22, 29

Data Vault

Active Directory 그룹 연결, 26

Windows 파일 공유, 9

데이터 이전, 19

서버 권장 사항, 30

요구 사항, 24

웹, 9

Data Vault 정책, 23

DPNECleanup, 33

DvConfig, 20

E

EFS 암호화된 파일, 26

F

FQDN, 18

H

HP

기술 지원 팀, 6

HTTPS 프로토콜, 9

I

IIS, 15

M

Microsoft SharePoint에 설치, 17

O

Open File Protection 정책, 25

P

Policy Server, 8

권장 사항, 31

데이터베이스 필수 구성 요소, 12

설치, 14

업데이트, 39

필수 구성 요소, 11

Policy Server 콘솔

브라우저 설정, 17

실행, 16, 23

Policy Server 콘솔, 실행, 16, 23

Policy Server 콘솔의 브라우저 설정, 17

S

SharePoint

다음에 Policy Server 설치, 17

SQL 데이터베이스

필수 구성 요소, 12

SQL 서버

설치, 15

SSL 변경, 20

SSL 포트

변경, 20

입력, 18

Subscriber's Choice, HP, 6

W

Windows Installer, 15, 35

Windows 파일 공유 Data Vault
다음에서 데이터 이전, 19

ㄱ

가져온 인증서, 10

개요, 8

관리자

생성, 18

수정, 20

구성

Active Directory 액세스, 26

Agent 업데이트 정책, 28

Continuous File Protection 정책, 25

Data Vault 정책, 23

Open File Protection 정책, 25

다중 스레드 정리, 33

데이터 보존 보고, 29

복사 정책, 24

사용자 정의 컨트롤 정책, 28

웹 Data Vault 서버, 18

정리 정책, 27

처음으로 정책, 23

파일 보호 정책, 25

규칙

문서, 5

기술 지원 팀, 6

ㄴ

네트워크, 크기 조정 고려 사항, 32

노트북, 필수 구성 요소, 13

ㄷ

다중 스레드 정리, 33

데스크톱, 필수 구성 요소, 13

데이터 보존 보고, 29

데이터베이스 필수 구성 요소, 12

도움

연기, 6

독자, 5

ㄹ

라이선스, 22, 29

구입 가능, 22

이동, 29

라이선스 이동, 29

라이선스 키

입력, 29

라이선스 키 입력, 29

ㅁ

문서

규칙, 5

ㅂ

배포

절차, 37

진행률 확인, 38

백업 사용자

생성, 19

수정, 20

복사 정책, 24

비밀번호, 22, 29

ㅅ

사용자 정의 컨트롤 정책, 28

사용자 컴퓨터, 필수 구성 요소, 13

새로운 Data Vault로 데이터 이전, 19

생성

관리자, 18

백업 사용자, 19

서버

정책, 8

파일, 8

설명서

피드백 제공, 7

설치

Agent, 35

Cleanup 소프트웨어, 18

Policy Server, 14

SQL 서버, 15

개요, 11

웹 Data Vault 서버, 18

수정

관리자, 20

백업 사용자, 20

신뢰된 인증 기관, 11

ㅇ

암호화된 비밀번호, 22, 29, 30

암호화된 비밀번호 가져오기, 29

암호화된 비밀번호 내보내기, 22, 29

암호화된 비밀번호 입력, 30

업데이트

Agent, 39

Policy Server, 39

웹 Data Vault, 9

다음으로 데이터 이전, 19

삭제, 19

유지, 19

웹 Data Vault 삭제, 19

웹 Data Vault 서버, 8

구성, 18

설치, 18

필수 구성 요소, 13

웹 Data Vault 유지, 19

웹 사이트

HP, 6

HP Subscriber's Choice for Business, 6

인증서, 10, 18

교환, 11, 20

인증서 교환, 11

인터넷 정보 서비스, 15

ㅈ

자체 서명된 인증서, 10, 18

정리 정책, 27

정책

Agent 업데이트, 28

Continuous File Protection, 25

Data Vault, 24

Open File Protection, 25

데이터 보존 보고, 29

배포, 8

복사, 24

사용자 정의 컨트롤, 28

정리, 27

처음으로 구성, 23

파일 보호, 25

지원, 41

지원 매트릭스, 8

ㅋ

콘솔

브라우저 설정, 17

실행, 16, 23

콘솔, 실행, 16, 23

크기 조정 고려 사항, 30

Data Vault, 30

Policy Server, 31

네트워크, 32

ㅊ

파일 공유 Data Vault, 9

파일 보호 정책, 25

계속적, 25

열기, 25

파일 서버, 8

필수 구성 요소, 11