HP ProtectTools for Small Business 보안 소프트웨어, 버전 5.10

사용 설명서

HP ProtectTools for Small Business 보안 소프트웨어 버전 5.10 사용 설명서

HP 비즈니스 PC

제 2 판: 2010 년 5 월

문서 부품 번호: 610663-AD2

본 설명서 정보

이 설명서에서는 HP ProtectTools for Small Business 보안 소프트웨어에 대한 정보를 제공합니다.

⚠ **경고!** 지시 사항을 따르지 않으면 부상을 당하거나 생명을 잃을 수 있습니다.

△ **주의:** 지시 사항을 따르지 않으면 장비가 손상되거나 정보가 유실될 수 있습니다.

참고: 이런 텍스트는 중요한 추가 정보를 제공합니다.

목차

1 보안 소개

HP 는 사용자가 PC, 데이터 및 비즈니스를 보호할 수 있는 적절한 보안 소프트웨어를 고심하느라 귀한 시간을 낭비하지 않고 비즈니스를 운영 및 확장시키는 데에만 집중해야 한다는 사실을 잘 알고 있습니다.

사용이 간편하면서도 비즈니스 자산을 강력하게 보호할 수 있는 보안 솔루션을 미리 고려해 두는 것이 중요합니다. 보안은 "있으면 좋은 것"이 아니라 "반드시 필요한 것"입니다.

HP 에서는 손쉽게 구현하고 간편하게 사용할 수 있는 보안 프로그램인 HP ProtectTools for Small Business 를 제공하고 있습니다.

HP ProtectTools for Small Business 는 컴퓨터 및 중요한 데이터에 대한 무단 액세스를 차단할 수 있는 기능을 제공하는 보안 소프트웨어로, 다양한 HP ProtectTools 소프트웨어 모듈을 통해 강화된 보안 기능이 제공됩니다.

HP ProtectTools for Small Business 는 HP ProtectTools Security Manager Administrative Console 및 HP ProtectTools Security Manager(일반 사용자용)의 두 가지 버전으로 제공됩니다. 관리자 버전 및 사용자 버전 모두 **시작 > 모든 프로그램** 메뉴에서 사용할 수 있습니다.

기능	특징
HP ProtectTools Security Manager Administrative Console	• 액세스하려면 Microsoft Windows 시스템 관리자 권한 필요 • 모듈에 대한 액세스는 관리자가 구성하며 일반 사용자는 사용할 수 없음 • 모든 사용자가 초기 보안 설정 및 옵션 또는 요구 사항 구성 가능
HP ProtectTools Security Manager(일반 사용자용)	• 관리자가 제공한 옵션을 사용자가 구성 가능 • 액세스 제한 및 일부 HP ProtectTools 모듈의 제한적인 컨트롤만 사용자에게 허용

HP ProtectTools 소프트웨어 모듈은 사전 설치 또는 사전 로드되어 있거나, 구성 가능한 옵션 또는 애프터 마켓 옵션으로 제공됩니다. 자세한 내용은 http://www.hp.com 을 참조하십시오.

HP ProtectTools 기능

다음 표에서는 HP ProtectTools for Small Business 모듈의 주요 기능에 대해 설명합니다.

모듈	주요 기능
HP ProtectTools Security Manager Administrative Console	• 관리자는 Security Manager 설치 마법사를 통해 보안 수준 및 보안 로그온 방법을 설정 및 구성할 수 있습니다. • 기본 사용자에게 옵션을 숨기도록 구성합니다. • Device Access Manager 구성 및 사용자 액세스를 구성합니다. • 관리자 도구를 사용하여 HP ProtectTools 사용자를 추가 및 제거하거나 사용자 상태를 볼 수 있습니다.
HP ProtectTools Security Manager(일반 사용자용)	• 사용자 이름과 암호를 구성, 설정 및 변경합니다. • Windows 암호와 스마트 카드 같은 사용자 인증 정보를 구성 및 변경합니다. • File Sanitizer 파쇄, 블리치 및 설정을 구성 및 변경합니다. • Device Access Manager 에 대한 설정을 봅니다. • 기본 설정과 백업 및 복원 옵션을 구성합니다.
Credential Manager for HP ProtectTools(암호 관리자)	• 사용자 이름 및 암호를 저장, 구성 및 보호하도록 설계되었습니다. • 신속하고 안전하게 액세스할 수 있는 웹 사이트 및 프로그램의 로그온 화면을 설정할 수 있습니다. • 액세스하는 여러 웹 사이트에 대한 사용자 이름 및 암호를 저장하려는 경우 암호 관리자에 사용자 이름과 암호를 입력하면 다시 기억할 필요가 없습니다. 다음에 해당 사이트를 방문하면 암호 관리자가 해당 데이터를 자동으로 채우고 제출합니다. • 따로 기록하거나 기억할 필요가 없는 강력한 암호를 작성할 수 있어 계정 보안이 강화됩니다.
Drive Encryption for HP ProtectTools	• 완벽한 전체 볼륨 하드 드라이브 암호화를 제공합니다. • 하드 드라이브에 있는 데이터의 암호를 해독하거나 액세스하기 전에 사전 부팅 인증을 수행하도록 합니다. • 중요한 기밀 정보를 보호하기 위해 법적 요건이나 업계 요구 사항을 준수하도록 도와줍니다. • 전체 하드 드라이브를 암호화하여 무단 액세스로부터 데이터를 보호합니다. PC 를 도난 당한 적이 있고, 드라이브를 기존 시스템에서 분리하여 다른 시스템에 장착하는 경우 데이터가 손상되지 않습니다.

모듈	주요 기능
File Sanitizer for HP ProtectTools	• Windows 에서 데이터를 삭제해도 하드 드라이브에서 그 내용이 완전히 제거되는 것은 아닙니다. Windows 에서는 데이터에 대한 참조만 삭제합니다. 다른 파일이 하드 드라이브의 동일한 영역에 새로운 정보를 덮어쓸 때까지 해당 데이터는 하드 드라이브에 남아 있습니다. 그러나 File Sanitizer 를 사용하면 문서, 웹 브라우저 기록, 임시 파일 등을 완전하게 그리고 자동으로 지울 수 있습니다. • 컴퓨터에서 중요한 파일과 폴더(개인 정보 또는 파일, 기록 데이터/웹 관련 데이터 또는 다른 데이터 구성 요소)를 안전하게 지우고(또는 파쇄하고) 하드 드라이브를 정기적으로 블리치(이전에 삭제한 데이터만 덮어씀)할 수 있습니다.
Device Access Manager for HP ProtectTools	• 사용자 프로필에 따라 미디어 드라이브, USB, 기타 하드웨어 장치에 대한 액세스를 제어할 수 있습니다. • 중요한 데이터를 저장하는 사용자의 권한을 제한할 수 있습니다. • 사용자가 외부 저장 장치(예: 개인용 뮤직 플레이어)를 사용하여 PC 또는 네트워크에서 데이터를 복사하지 못하도록 합니다. • 사용자가 외부 미디어에서 시스템에 바이러스를 감염시키지 못하도록 합니다. • 사용자 또는 사용자 그룹별로 장치 그룹(예: USB 키, 쓰기 가능 장치, 개인용 뮤직 플레이어 등)을 선택적으로 비활성화할 수 있습니다. 관리자 암호를 사용하는 사용자는 로그온하여 PC 에서 정보를 복사할 수 있지만 그 외의 사용자는 이러한 작업을 수행할 수 없습니다.

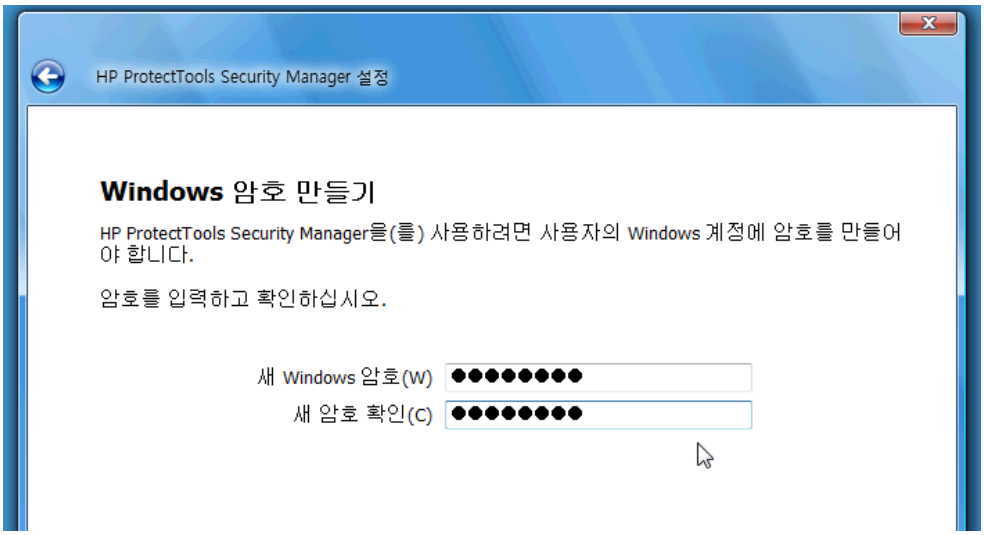
2 가장 유용한 옵션에 대해 설명하는 간편 설치 설명서

이 간편 설치 설명서는 HP ProtectTools for Small Business 에서 가장 일반적이고 유용한 옵션을 활성화하는 기본 단계를 시각적으로 보여 줍니다. HP ProtectTools for Small Business 에는 기본 설정을 조정하고 액세스 제어를 설정하는 데 사용할 수 있는 다양한 도구 및 옵션이 있습니다. 간편 설치 설명서는 설치에 드는 노력과 시간을 최소화하면서 각 모듈을 실행하는 방식에 대해 집중적으로 다루고 있습니다. 자세한 내용을 보려면 관련 모듈을 선택하고 "?"를 누르거나 오른쪽 상단에 있는 도움말 버튼을 누르십시오. 이 버튼을 누르면 현재 표시된 창에 대한 유용한 정보가 자동으로 제공됩니다.

시작하기

1. 가젯 아이콘이나 작업 표시줄 아이콘(금색 방패 모양)을 사용하여 HP ProtectTools Security Manager 를 열거나 **시작 > 모든 프로그램 > HP** 를 누릅니다.

2. Windows 암호를 입력하거나 Windows 암호를 만듭니다.

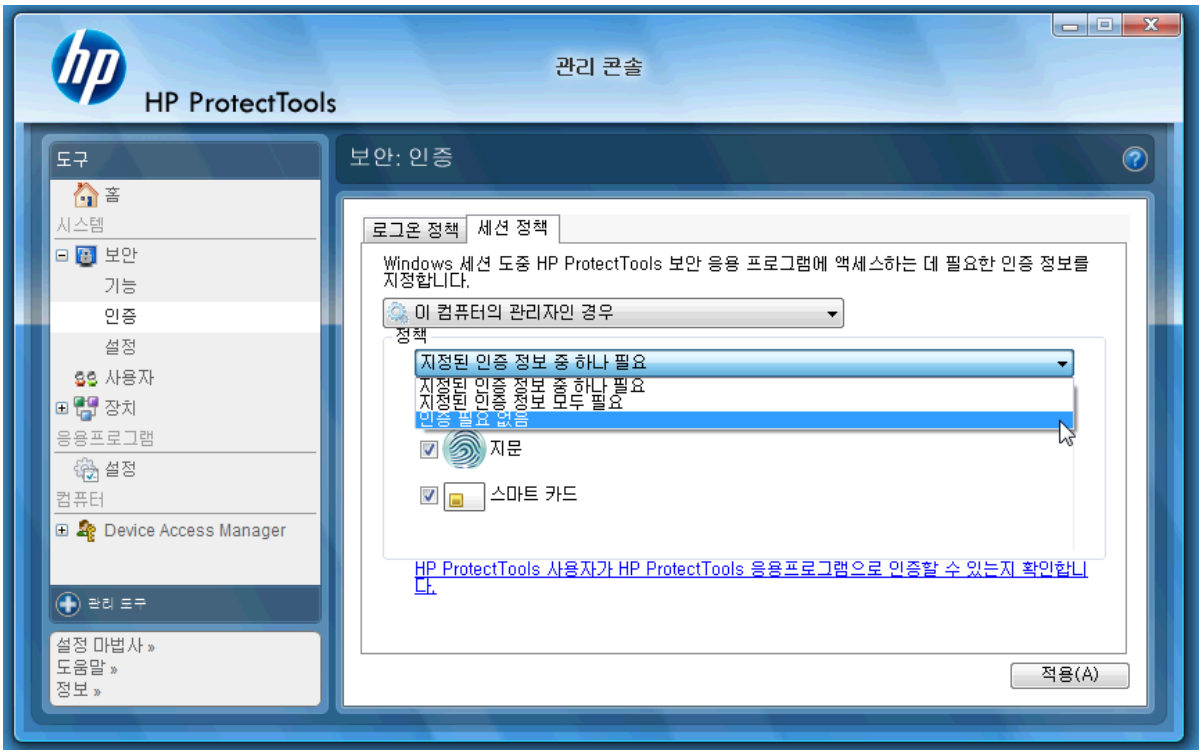


3. 설정 마법사를 완료합니다.

참고: 기본적으로 HP ProtectTools Security Manager 는 강력한 인증 정책으로 설정되어 있습니다.

이 설정은 Windows 에 로그인되어 있는 동안 무단 액세스를 차단하기 위한 것으로, 높은 수준의 보안이 필요하거나 사용자가 자주 자리를 비우는 경우 사용해야 합니다. 이 설정을 변경하려면 세션 정책 탭을 누르고 원하는 항목을 선택합니다.

전체 세션에 대해 초기 Windows 로그인만 사용하도록 HP ProtectTools Security Manager 를 구성하려면 다음과 같이 구성을 변경하십시오.



Windows 로그인 중 HP ProtectTools Security Manager 에서 한 번만 인증하도록 하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP > HP ProtectTools Administrative Console** 을 선택합니다.
2. 왼쪽 **도구** 창의 **보안** 그룹에서 **인증**을 선택합니다.
3. **세션 정책** 탭을 누르고 **정책** 아래의 드롭다운 메뉴에서 **인증 필요 없음**을 선택합니다.
4. 완료하면 **적용** 버튼을 누릅니다.

Credential Manager for HP ProtectTools(암호 관리자)

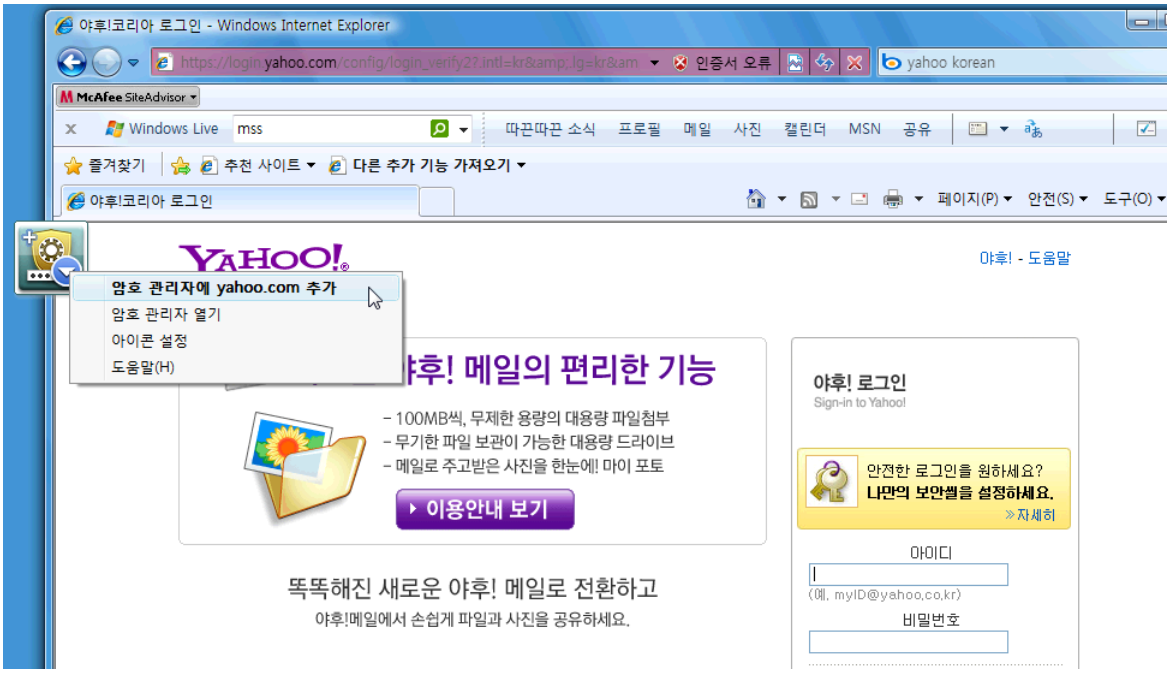
모든 사용자는 여러 개의 암호를 사용합니다. 특히 일상적으로 웹 사이트에 액세스하거나 로그인이 필요한 응용프로그램을 사용하는 경우에는 더욱 그러합니다. 보통 사용자는 모든 응용프로그램 및 웹 사이트에 동일한 암호를 사용하거나 아니면 정말 독자적인 암호를 만들더라도 어떤 응용프로그램에 어떤 암호를 사용해야 하는지를 곧 잊어버리곤 합니다.

중요하지 않은 사이트의 암호는 자동으로 입력해 주거나, 기억해야 할 사이트와 잊어도 상관이 없는 사이트를 구분해 주는 소프트웨어가 있으면 좋지 않을까요? Credential Manager for HP ProtectTools 는 바로 이러한 기능을 제공해 주는 암호 관리자입니다. PC 에 로그온하면 Credential Manager 는 필요한 암호 또는 인증서를 제공해 줍니다.

인증서를 요구하는 응용프로그램 또는 웹 사이트에 액세스하면 Credential Manager 는 자동으로 해당 사이트를 인식하고 소프트웨어에 해당 정보를 저장할지 묻습니다. 저장을 선택하면 해당 암호를 다시 기억할 필요가 없습니다. 특정 사이트에서는 이 소프트웨어를 사용하지 않으려는 경우 정보 저장 요청을 거부할 수 있습니다.

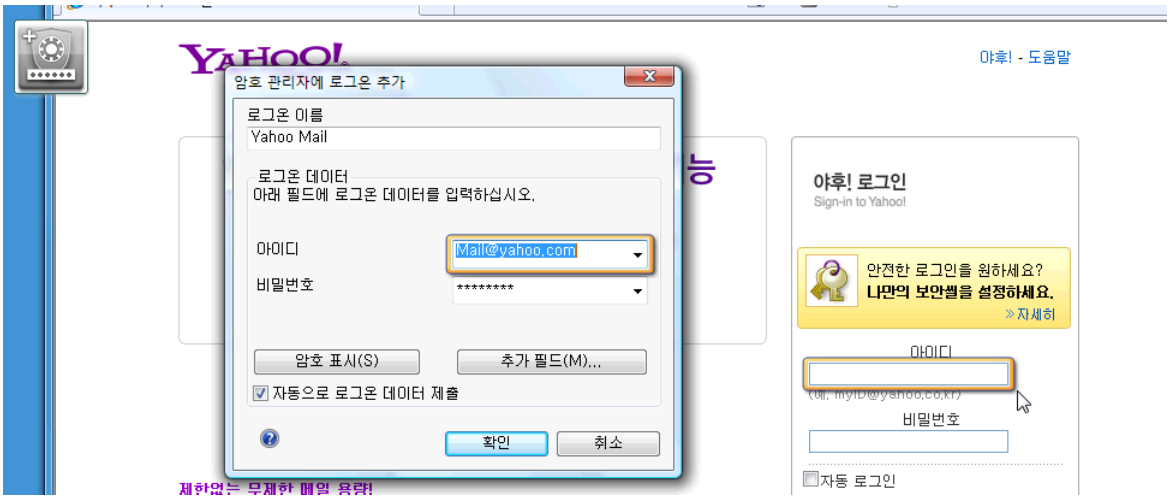
웹 위치, 사용자 이름 및 암호를 저장하려면 다음과 같이 하십시오.

1. 예를 들어, 웹 메일 계정으로 이동하여 Credential Manager 에 웹 인증을 추가하도록 요청합니다(아이콘 누름).



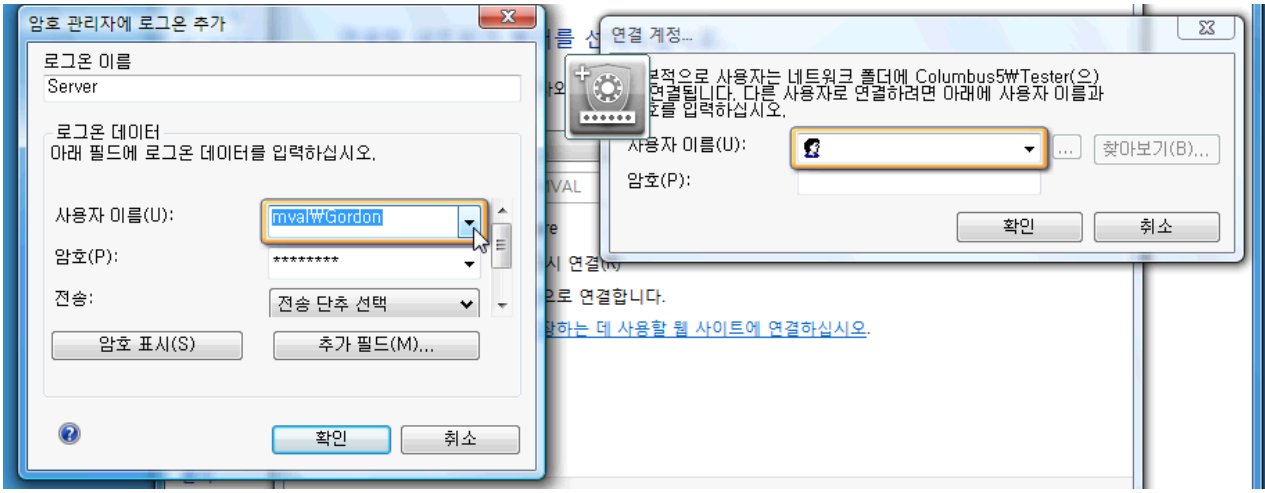
2. 링크의 이름을 지정하고(선택 사항) Credential Manager 에 사용자 이름과 암호를 입력합니다.

참고: 그러면 이후 방문 시에도 웹 페이지에서 Credential Manager 가 사용할 영역이 강조 표시됩니다.



3. 완료하면 **확인** 버튼을 누릅니다.

4. 또한 Credential Manager 에서 네트워크 공유 또는 네트워크 드라이브 매핑에 사용되는 사용자 이름과 암호도 저장할 수 있습니다.



Credential Manager 에 저장된 인증 정보 보기 및 관리

Credential Manager 의 장점은 한 곳에서 인증 정보를 보고, 관리하고, 백업하고, 실행할 수 있다는 점입니다. 또한 Windows 에서 저장된 사이트를 실행할 수도 있습니다.

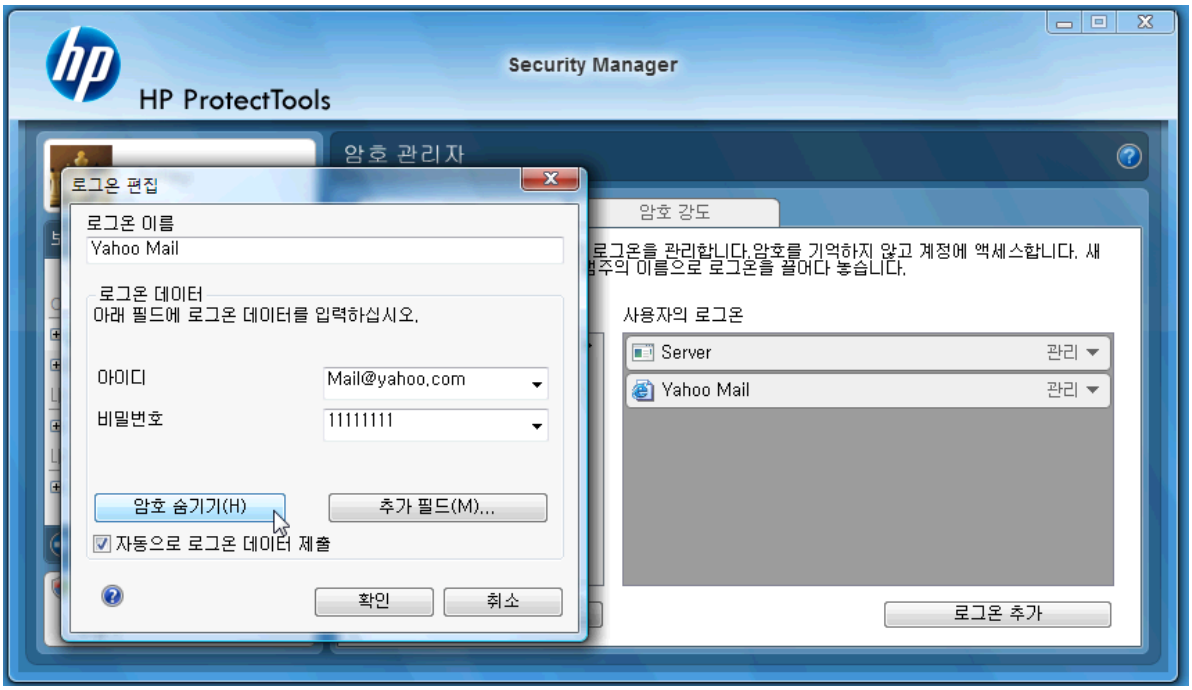
암호 관리자를 열려면 다음 두 가지 방법 중 하나를 사용하십시오.

- Ctrl + Windows + H 키 조합을 사용하여 암호 관리자를 엽니다. **열기**를 선택하면 저장된 바로 가기를 빠르게 실행 및 인증할 수 있습니다.

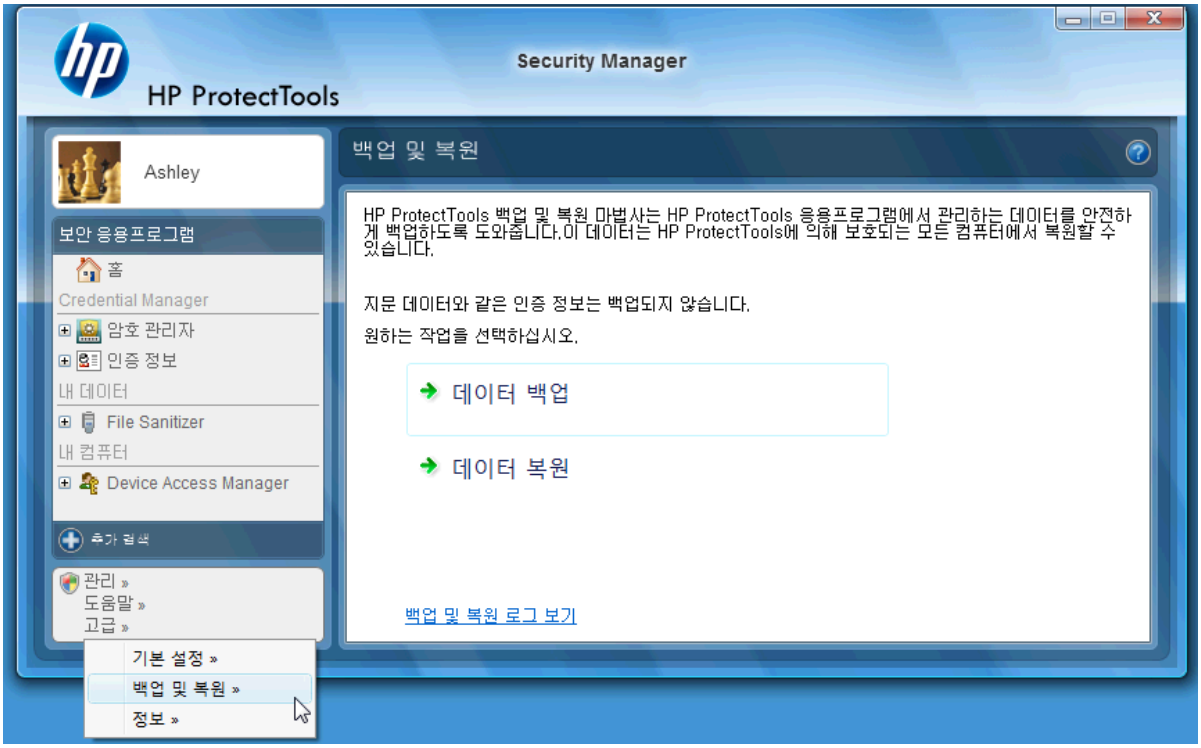
또는

- 암호 관리자에서 **관리** 탭을 선택하여 인증 정보를 편집할 수 있는 HP ProtectTools Security Manager 를 엽니다.

Credential Manager 의 **편집** 옵션을 사용하면 이름 및 로그인 이름을 보고 수정할 수 있으며 암호도 확인할 수 있습니다.



HP ProtectTools for Small Business 에서 모든 인증 정보 및 설정을 다른 PC 로 백업하거나 복사할 수 있습니다.


HP ProtectTools
Security Manager
Ashley
보안 응용프로그램
홈
Credential Manager
암호 관리자
인증 정보
내 데이터
File Sanitizer
내 컴퓨터
Device Access Manager
관리 »
도움말 »
고급 »
기본 설정 »
백업 및 복원 »
정보 »
백업 및 복원
HP ProtectTools 백업 및 복원 마법사는 HP ProtectTools 응용프로그램에서 관리하는 데이터를 안전하게 백업하도록 도와줍니다.이 데이터는 HP ProtectTools에 의해 보호되는 모든 컴퓨터에서 복원할 수 있습니다.
지문 데이터와 같은 인증 정보는 백업되지 않습니다.
원하는 작업을 선택하십시오.
데이터 백업
데이터 복원
백업 및 복원 로그 보기

File Sanitizer for HP ProtectTools

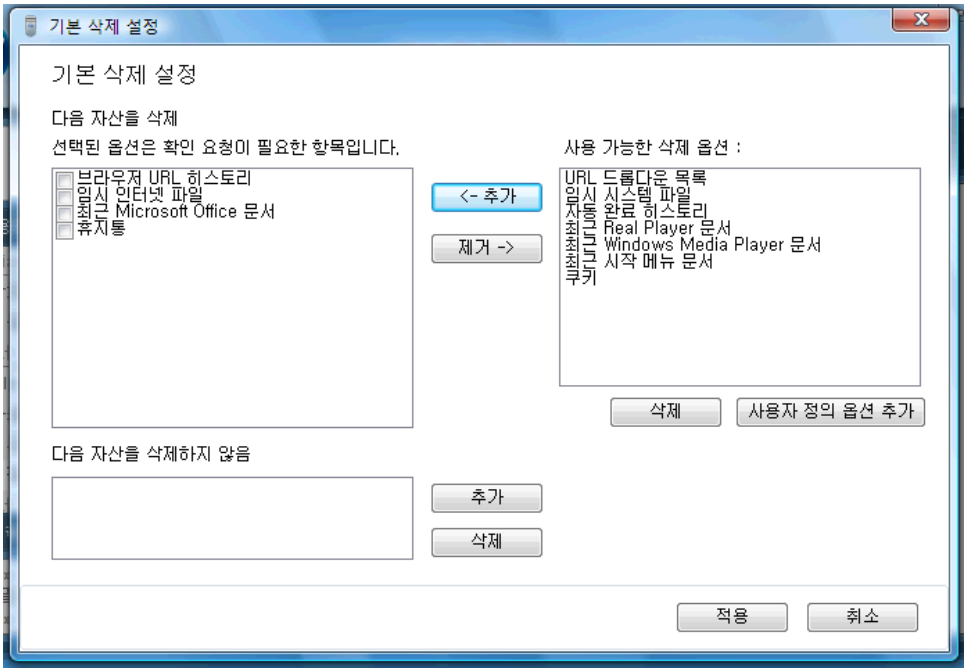
File Sanitizer 는 허가받지 않은 사람이 삭제된 데이터를 복구하기가 매우 어렵도록 설계되었습니다. 여기에는 브라우저 기록을 포함하여 선택한 파일 및 폴더를 수동으로 지우거나 정기적으로 지우도록 예약할 수 있는 여러 가지 옵션이 들어 있습니다.

간단한 몇 가지 구성 설정은 다음과 같습니다.

삭제된 데이터를 영구적으로 지우려면 더 이상 필요하지 않은 파일 또는 폴더를 선택하십시오.

1. **Security Manager** > **File Sanitizer** > **설정**으로 이동합니다. **기본 삭제 설정**을 선택하고 **세부 정보 보기** 버튼을 누릅니다.

2. 기본 삭제 설정 창의 오른쪽 영역에서 정기적으로 영구 삭제할 항목을 선택하고 **<-추가** 버튼을 눌러 선택한 항목을 삭제 목록으로 옮깁니다.



3. 먼저 휴지통을 선택하고 파쇄 기능을 사용해 지우려는 다른 항목을 추가합니다.

4. 영구적으로 지울 항목을 모두 선택하면 **적용** 버튼을 누릅니다.

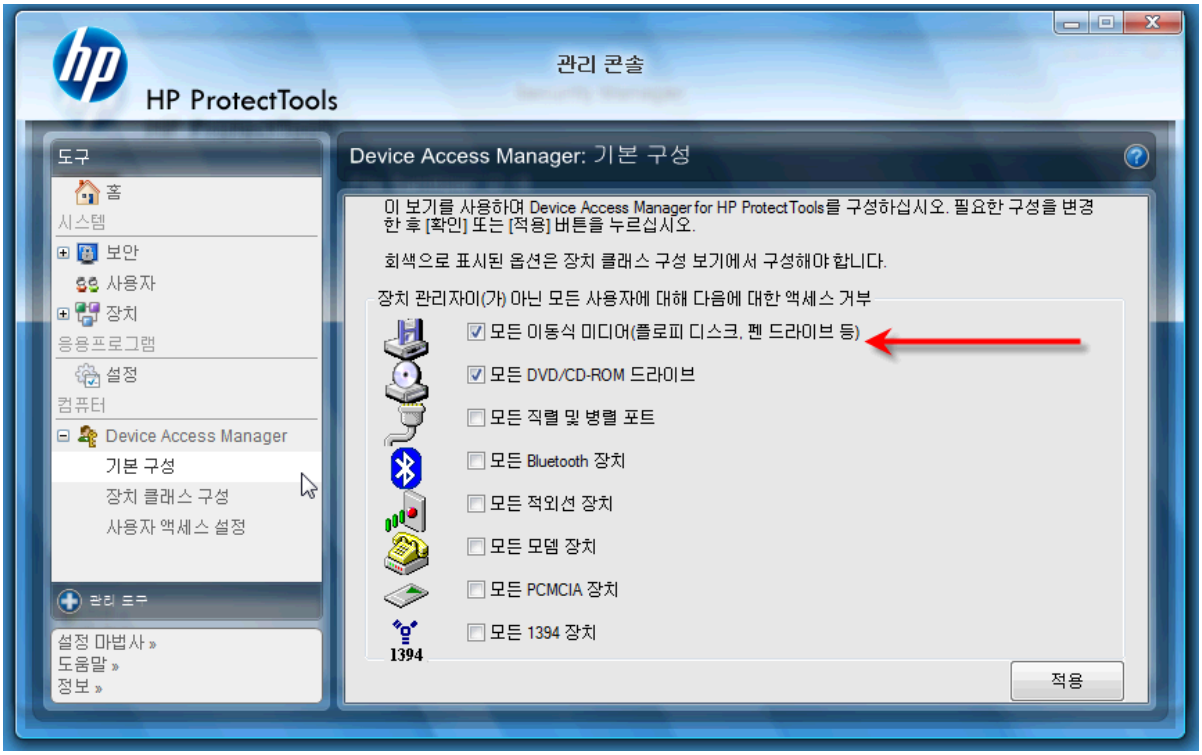
5. **파쇄** 옵션으로 이동하고 작업을 실행할 시간을 구성합니다. **지금 파쇄** 버튼을 누르면 앞서 구성한 기본 삭제 설정 창에서 선택한 항목이 즉시 지워집니다.

6. 파쇄가 시작되고 완료될 때마다 작업 표시줄에 작은 풍선 팝업 창이 나타납니다.

Device Access Manager for HP ProtectTools

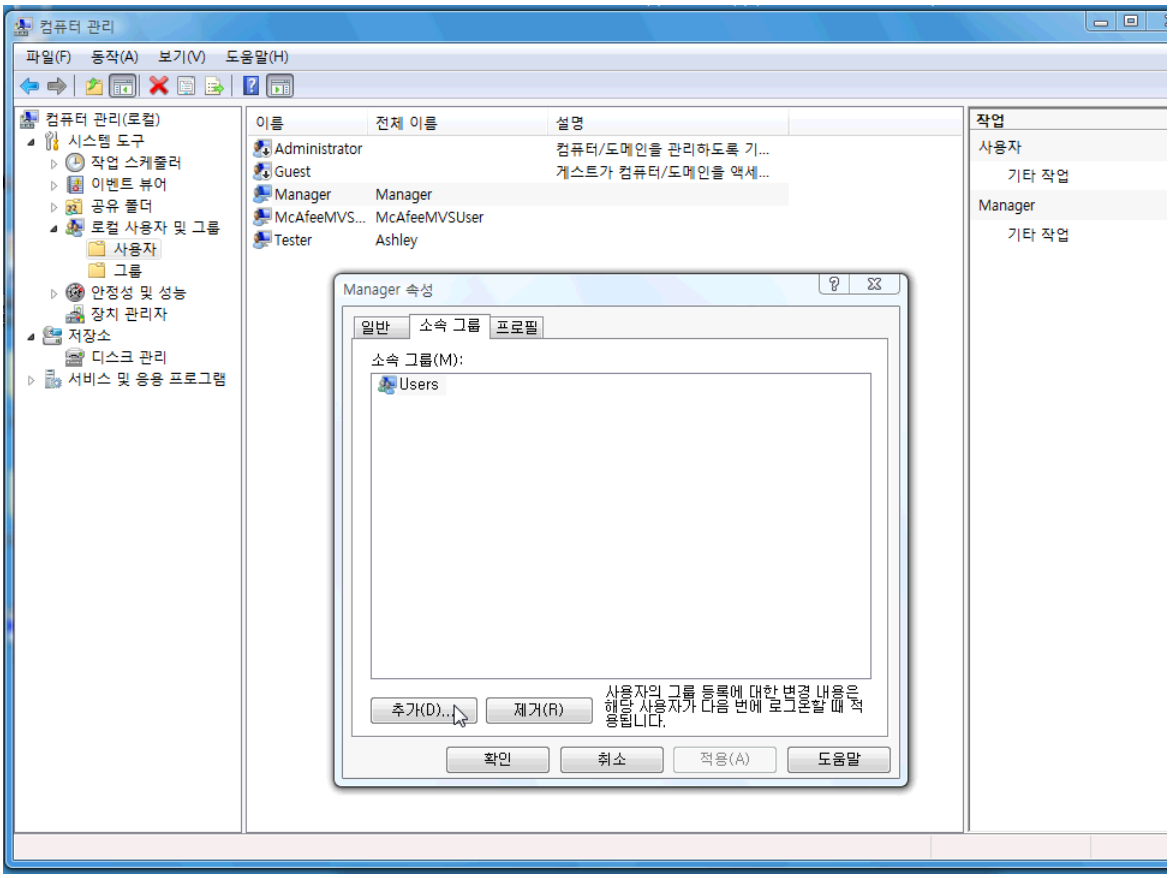
Device Access Manager 는 데이터를 하드 드라이브에 안전하게 보관하고 외부로 유출되지 않도록 다양한 내/외부 저장 장치의 사용을 제한하는 데 사용할 수 있습니다. 예를 들어, 데이터에 대한 사용자 액세스를 허용하지만 CD, 개인용 뮤직 플레이어 또는 USB 메모리 장치로 복사하지 못하도록 설정할 수 있습니다. 다음과 같이 이 설정을 간편하게 지정할 수 있습니다.

1. **시작 > 모든 프로그램 > HP > 관리 콘솔 > Device Access Manager > 기본 구성**을 선택합니다.
2. 제한하려는 하드웨어 장치를 선택하고 **적용** 버튼을 눌러 프로세스를 완료합니다.

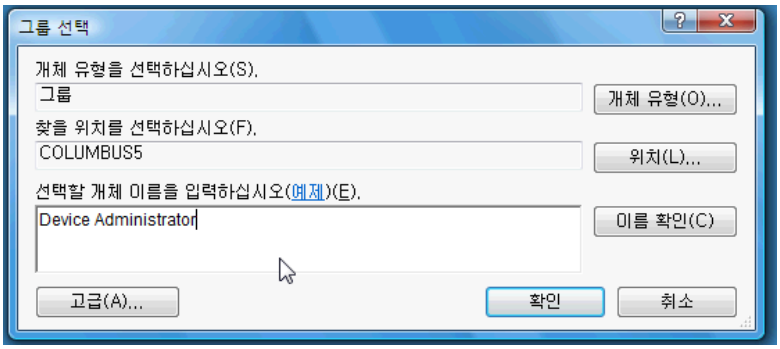


3. 이후 단계에서는 다른 모든 사용자는 차단하면서 액세스 권한을 계속 부여할 대상을 선택합니다.
4. **내 컴퓨터**로 이동하여 선택한 다음 마우스 오른쪽 버튼을 누르고 **관리 > 컴퓨터 관리 > 시스템 도구 > 로컬 사용자 및 그룹 > 사용자**를 선택합니다.
5. 차단된 하드웨어에 대한 액세스 권한을 계속 유지할 사용자(이 예에서는 "Manager")를 두 번 누릅니다.

6. **소속 그룹** 탭에서 **추가** 버튼을 누릅니다.



7. **그룹 선택** 창에서 **고급** 옵션을 사용하거나 "Device Administrators" 그룹을 입력할 수 있습니다. **확인** 버튼을 누른 다음, 다시 확인 버튼을 눌러 창을 닫습니다. 로그오프했다가 다시 로그온해야 권한을 얻을 수 있습니다.



이제 "Device Administrators" 그룹의 사용자가 아닌 사람은 CD 드라이브, USB 드라이브, 개인용 뮤직 플레이어 등 모든 내/외부 저장 장치 드라이브를 사용할 수 없게 됩니다.

Drive Encryption for HP ProtectTools

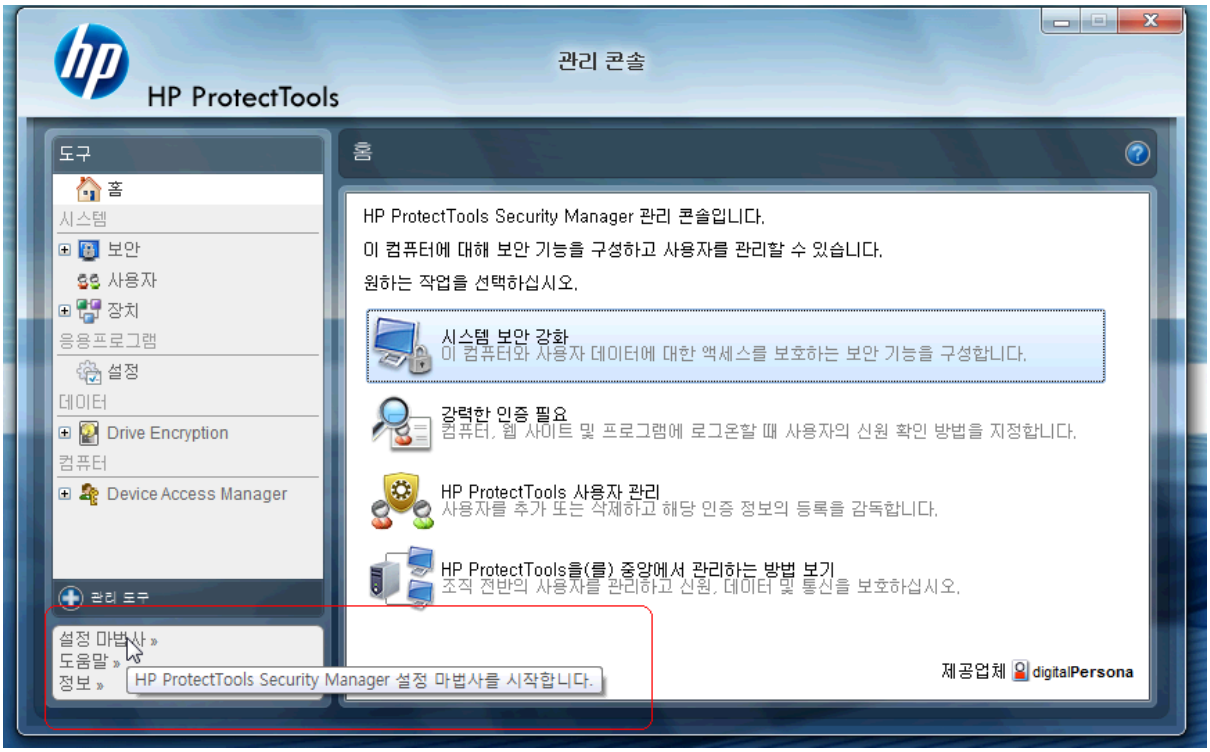
Drive Encryption for HP ProtectTools 는 전체 하드 드라이브를 암호화하여 데이터를 보호해 주는 소프트웨어입니다. PC 를 도난 당하거나 하드 드라이브를 기존 시스템에서 분리하여 다른 시스템에 장착하는 경우에도 하드 드라이브의 데이터는 계속 보호됩니다.

Drive Encryption 에서는 시스템이 부팅되기 전에 사용자 이름과 암호를 통해 올바르게 인증하도록 요구하여 더욱 강력한 보안을 제공합니다. 이 프로세스를 사전 부팅 인증이라고 합니다.

Windows 사용자, 도메인, Credential Manager for HP ProtectTools 및 Drive Encryption 을 비롯한 HP ProtectTools Security Manager 의 모든 인터페이스에서 암호를 동기화하여 이 프로세스를 간편하게 수행할 수 있습니다.

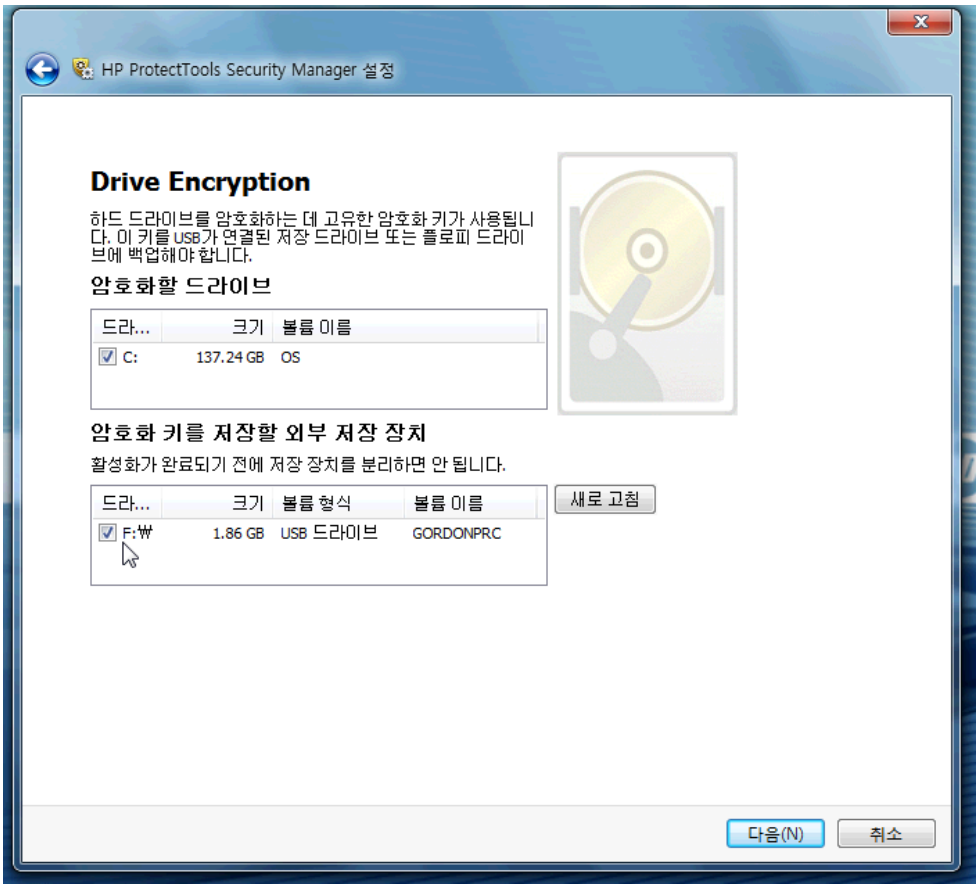
Drive Encryption for HP ProtectTools 를 활성화하려면 다음 단계를 수행하십시오.

1. **시작 > 모든 프로그램 > HP > HP ProtectTools 관리 콘솔 > 관리 도구 > 설정 마법사**를 클릭합니다. 다음과 같은 화면이 나타납니다.



2. 시작 화면에서 **다음**을 선택합니다.
3. 활성화 마법사를 시작하고 **다음**을 선택합니다. 활성화 마법사를 시작하려면 Windows 암호가 필요합니다.
4. **Drive Encryption** 상자를 선택하고 **다음**을 클릭합니다.

5. 아래와 같은 Drive Encryption 구성 창에 암호화할 드라이브가 표시되고 암호화 복구 키를 저장할 USB 플래시 드라이브가 요구됩니다. 사전 부팅 암호를 잊어버렸거나 사전 부팅 암호에 오류가 발생할 때 데이터를 복구하거나 드라이브에 액세스해야 하는 경우 이 복구 키를 사용해야 하므로 안전하게 보관하십시오.



6. **다음**을 선택하여 프로세스를 완료하고 **마침**을 선택합니다. 메시지가 표시되면 USB 플래시 드라이브를 분리하고 준비가 되었으면 시스템을 재부팅합니다.

7. 하드 드라이브에서 시스템이 부팅될 때 Drive Encryption 에서는 Windows 암호를 입력하도록 요청합니다. 암호를 입력하고 **확인**을 클릭합니다.

참고: 드라이브가 암호화되는 동안 컴퓨터가 천천히 실행될 수 있습니다. 암호화가 완료되면 시스템이 정상적으로 돌아옵니다. 드라이브의 데이터에 액세스할 때 필요에 따라 드라이브가 암호화되거나 해독됩니다.

또한 Drive Encryption 인증이 Credential Manager Windows 로그인을 통해 데스크톱에 바로 "연결"되어 암호를 두 번 입력하지 않아도 됩니다.

3 HP ProtectTools for Small Business 이점

HP ProtectTools for Small Business 보안 소프트웨어 액세스

Windows 시작 메뉴에서 HP ProtectTools Security Manager 에 액세스하려면 다음과 같이 하십시오.

▲ Windows 의 경우 **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.

Windows 시작 메뉴에서 HP ProtectTools Security Manager Administrative Console 에 액세스하려면 다음과 같이 하십시오.

▲ Windows 의 경우 **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.

주요 보안 목표 달성

HP ProtectTools 모듈을 함께 사용하여 다음과 같은 주요 보안 목표를 비롯하여 다양한 보안 문제를 해결할 수 있습니다.

- 중요 데이터에 대한 액세스 제한
- 내부 또는 외부에서 들어오는 무단 액세스 차단
- 강력한 암호 정책 생성

중요 데이터에 대한 액세스 제한

현장에서 작업 중인 계약직 감사원이 중요한 재무 데이터를 검토할 수 있는 컴퓨터에 대한 액세스 권한을 부여 받았다고 가정해 보겠습니다. 이 감사원이 파일을 인쇄하거나 CD 같은 쓰기 가능 장치에 저장할 수 없도록 지정하고 싶습니다. 다음 기능을 사용하면 데이터 액세스를 제한할 수 있습니다.

관리자는 Device Access Manager for HP ProtectTools 를 통해 쓰기 가능 장치에 대한 액세스를 제한함으로써 하드 드라이브에서 이동식 미디어로 중요한 정보가 인쇄되거나 복사되지 않도록 할 수 있습니다. 43페이지의 장치 클래스 구성(고급)을 참조하십시오.

내부 또는 외부에서 들어오는 무단 액세스 차단

안전하지 않은 비즈니스 PC 에 무단으로 액세스하면 재무 담당, 경영진 또는 R&D 팀과 관련된 정보에서 특허 기록이나 개인 재무 기록 같은 개인용 정보에 이르는 중요한 데이터가 위험해집니다. 다음 기능을 사용하면 무단 액세스를 방지할 수 있습니다.

- 사전 부팅 인증 기능은 운영 체제에 대한 액세스를 차단합니다(사용되는 경우). 다음 장을 참조하십시오.
  - 32페이지의 Credential Manager for HP ProtectTools(암호 관리자)
  - 29페이지의 Drive Encryption for HP ProtectTools
- Credential Manager for HP ProtectTools 는 무단 사용자가 암호를 알게 되거나 암호로 보호되는 응용프로그램에 액세스하지 못하도록 합니다. 다음 장을 참조하십시오.
  - 32페이지의 Credential Manager for HP ProtectTools(암호 관리자)
- 관리자는 Device Access Manager for HP ProtectTools 를 통해 쓰기 가능 장치에 대한 액세스를 제한함으로써 하드 드라이브에서 중요한 정보가 복사되지 않도록 할 수 있습니다. 다음 장을 참조하십시오.
  - 42페이지의 Device Access Manager for HP ProtectTools
- File Sanitizer 를 통해 중요한 파일이나 폴더를 파쇄하거나 하드 드라이브를 블리치(데이터를 쉽게 복구할 수 없도록 하기 위해 이전에 삭제되었지만 여전히 하드 드라이브에 남아 있는 데이터를 다시 쓰는 작업)함으로써 데이터를 안전하게 삭제할 수 있습니다. 다음 장을 참조하십시오.
  - 36페이지의 HP ProtectTools File Sanitizer

강력한 암호 정책 생성

다양한 웹 기반 응용프로그램 및 데이터베이스에 강력한 암호 정책(해킹하기 어려운 복잡한 암호)을 사용해야 하는 경우, Credential Manager for HP ProtectTools 는 안전한 암호 저장소와 편리한 SSO (Single Sign On) 기능을 제공합니다. 다음 장을 참조하십시오.

- 32페이지의 Credential Manager for HP ProtectTools(암호 관리자)

추가 보안 요소

보안 역할 분배

데이터를 안전하게 보호하기 위한 한 가지 중요한 관행은 책임과 권한을 여러 관리자와 사용자에게 분배하는 것입니다.

참고: 소규모 조직이나 개인 사용자의 경우, 한 사람이 이러한 역할을 모두 수행할 수도 있습니다.

HP ProtectTools for Small Business 에서는 보안 의무와 권한을 다음과 같은 역할로 나눌 수 있습니다.

- 관리자 - 보안 기능을 적용하고 관리합니다. 또한 일부 기능의 사용 여부를 설정할 수 있습니다.
- 사용자 - 보안 기능을 사용합니다.

HP ProtectTools 암호 관리

대부분의 HP ProtectTools Security Manager 기능은 암호로 보호됩니다. 다음 표는 일반적으로 사용되는 암호, 암호가 설정된 소프트웨어 모듈 및 암호 기능을 나열합니다.

이 표에는 관리자만 설정하고 사용하는 암호도 나와 있습니다. 그 외의 다른 모든 암호는 일반 사용자가 설정할 수 있습니다.

HP ProtectTools 암호	HP ProtectTools 모듈에서 설정	기능
암호 관리자 로그온 암호	암호 관리자	이 암호는 다음과 같은 2 가지 옵션을 제공합니다. • Windows 에 로그온한 후 암호 관리자에 액세스하기 위해 별도로 로그온하는 데 사용합니다. • Windows 로그온 프로세스 대신 사용하여 Windows 및 암호 관리자에 동시에 액세스할 수 있습니다.
Computer Setup 암호 **참고:** BIOS 관리자, F10 설정 또는 보안 설정 암호라고도 함	BIOS, 관리자가 설정	Computer Setup 유틸리티에 무단으로 액세스하지 못하도록 합니다.
파워온 암호	BIOS	컴퓨터를 켜거나, 재시작하거나, 최대 절전 모드에서 복원할 때 컴퓨터 내용에 무단으로 액세스하지 못하도록 합니다.
Windows 로그온 암호	Windows 제어판	수동 로그온 시 사용할 수 있습니다.

보안 암호 만들기

암호를 만들 때는 우선 프로그램이 설정한 규격에 맞아야 합니다. 그러나 일반적으로 다음과 같은 지침에 따라 강력한 암호를 작성하면 암호 노출 위험을 줄일 수 있습니다.

- 6 자 이상의 암호를 사용합니다. 8 자 이상이면 더 좋습니다.
- 암호에 대소문자를 혼용합니다.
- 가능한 경우 영숫자를 혼용하고 특수 문자와 문장 부호를 포함합니다.
- 키워드의 일부 문자를 특수 문자나 숫자로 대체합니다. 예를 들어 L 이나 I 대신 숫자 1 을 사용할 수 있습니다.
- 둘 이상의 언어로 된 단어를 조합합니다.
- "Mary2-2Cat45"처럼 숫자나 특수 문자를 가운데에 넣어 단어나 구를 구분합니다.
- 사전에 나오는 단어를 암호로 사용하지 않습니다.
- 이름이나, 생일, 애완동물 이름, 어머니의 성과 같은 개인 정보를 암호로 사용하지 않으며, 이러한 정보를 역순으로 적은 암호도 사용하지 않습니다.
- 정기적으로 암호를 변경합니다. 일부 문자를 늘리는 방법으로 변경할 수도 있습니다.
- 암호를 기록할 경우, 기록한 암호를 컴퓨터 근처의 눈에 띄는 장소에 보관하지 않습니다.

- 암호를 전자 우편이나 컴퓨터 내에 파일로 저장하지 않습니다.
- 계정을 공유하거나 다른 사람에게 암호를 알리지 않습니다.

인증 정보 및 설정 백업

HP ProtectTools Security Manager의 백업 및 복구 도구를 사용하여 한 곳에서, 설치된 HP ProtectTools 모듈에서 보안 인증서를 백업 및 복원할 수 있습니다.

4 HP ProtectTools Security Manager Administrative Console

HP ProtectTools Administrative Console 정보

HP ProtectTools Security Manager 는 관리 콘솔을 통해 관리합니다.

로컬 관리자는 이 콘솔에서 다음을 수행할 수 있습니다.

- 보안 기능의 사용 여부 설정
- 컴퓨터 사용자 관리
- 장치 고유 매개변수 조정
- Security Manager 응용프로그램 구성
- Security Manager 응용프로그램 추가

관리 콘솔 사용

Security Manager Administrative Console 은 HP ProtectTools Security Manager 를 관리하는 중심 지점의 역할을 합니다.

콘솔을 열려면 다음과 같이 하십시오.

- **시작 > 모든 프로그램 > HP ProtectTools Administrative Console** 을 선택합니다. 또는
- Security Manager 콘솔의 왼쪽 하단에서 **관리** 링크를 누릅니다.

관리 콘솔은 두 개의 창으로 구성되어 있습니다. 왼쪽 창과 오른쪽 창이 있는데, 왼쪽 창에는 관리 도구가 있고 오른쪽 창에는 도구를 구성하는 작업 영역이 있습니다.

관리 콘솔 왼쪽 창은 다음으로 구성되어 있습니다.

- **홈** - 보안 기능 사용, 보안 인증 정보 지정, 사용자 관리 등 자주 사용하는 작업에 쉽게 액세스할 수 있습니다.
- **시스템** - 스마트 카드 리더와 같은 인증 장치, 시스템 전체의 보안 기능, 사용자의 구성을 관리합니다.
- **응용프로그램** - Security Manager 및 해당 응용프로그램의 동작을 구성하는 도구를 제공합니다.
- **데이터** - 암호화 키를 백업 및 복구하는 도구를 제공합니다.

- **컴퓨터** - PC 보안을 약화시킬 수 있는 다양한 장치를 선별적으로 비활성화하고 여러 사용자 및 그룹의 액세스 권한을 설정하는 고급 보안 옵션을 제공합니다.
- **관리 도구** - Security Manager 의 기능을 확장하고 새 응용프로그램과 업데이트에 대한 최신 정보를 유지하는 방법을 제공하는 추가 관리 응용프로그램 및 도구가 있는 웹 페이지가 기본 브라우저에서 열립니다.
- **링크** - 다음과 같은 항목을 제공합니다.
  - **설정 마법사** - Security Manager 의 초기 구성을 안내하는 설치 마법사를 실행합니다.
  - **도움말** - Security Manager 및 해당 응용프로그램에 대한 정보를 제공하는 도움말 파일을 엽니다.
  - **정보** - 버전 번호와 저작권 고지 사항 등 Security Manager 에 대한 정보를 표시합니다.

설치 마법사로 시작하기

HP ProtectTools Security Manager 를 관리하려면 관리자 권한이 있어야 합니다.

HP ProtectTools Security Manager 설치 마법사는 보안 기능을 설정하는 과정을 안내합니다. 그러나 HP ProtectTools Security Manager Console 을 통해 다른 유용한 기능도 사용할 수 있습니다. 추가 보안 기능뿐 아니라 마법사에 있는 동일한 설정을 Windows 시작 메뉴 또는 관리 콘솔 내 링크로 액세스할 수 있는 콘솔을 통해 구성할 수 있습니다. 이 설정은 컴퓨터와 해당 컴퓨터를 공유하는 모든 사용자에게 적용됩니다.

Windows 에 처음 로그온하면 HP ProtectTools Security Manager 를 설정하라는 메시지가 나타납니다. 프로그램을 구성하는 기본 단계를 안내하는 Security Manager 설치 마법사를 실행하려면 **확인**을 누릅니다.

참고: 관리 콘솔의 왼쪽 창 하단 섹션에서 **보안 마법사**를 눌러 보안 마법사를 실행할 수도 있습니다.

설치가 완료될 때까지 설치 마법사 화면에 표시되는 지침을 따릅니다.

마법사를 완료하지 않으면 **이 마법사를 다시 표시하지 않음**을 누를 때까지 마법사가 자동으로 실행됩니다.

HP ProtectTools Security Manager 응용프로그램을 사용하려면 **시작** 메뉴에서 또는 작업 표시줄 알림 영역(시스템 트레이)의 **Security Manager** 아이콘을 마우스 오른쪽 버튼으로 눌러 HP ProtectTools Security Manager 를 실행합니다. Security Manager 콘솔과 해당 응용프로그램은 이 컴퓨터를 공유하는 모든 사용자가 사용할 수 있습니다.

시스템 구성

응용프로그램의 **시스템** 그룹은 관리 콘솔 왼쪽의 **도구** 메뉴에서 액세스합니다.

이 그룹에 속하는 응용프로그램을 사용하여 이 컴퓨터, 사용자 및 장치의 정책과 설정을 구성 및 관리할 수 있습니다.

시스템 그룹에 속하는 응용프로그램은 다음과 같습니다.

- **보안** - 보안 기능, 인증 정책 및 컴퓨터나 HP ProtectTools 응용프로그램에 로그온할 때 사용자 인증 방법을 제어하는 기타 설정을 관리합니다.
- **사용자** - 이 컴퓨터의 사용자를 설정, 관리 및 등록합니다.
- **장치** - 컴퓨터에 연결되거나 내장된 보안 장치의 설정을 관리합니다.

보안 기능 사용

여기서 사용하는 보안 기능은 이 컴퓨터의 모든 사용자에게 적용됩니다.

1. 관리 콘솔 왼쪽 창에서 **보안**을 확장하고 **기능**을 누릅니다.
2. 보안 기능을 사용하려면 **Windows 로그온 보안** 및/또는 **Drive Encryption** 옆의 확인란을 클릭합니다.
   - **Windows 로그온 보안** - 액세스할 때 특정 인증 정보를 요구하여 Windows 계정을 보호합니다.
   - **Drive Encryption** - 하드 드라이브를 암호화하고 올바른 인증이 없는 사용자는 정보를 읽을 수 없도록 하여 데이터를 보호합니다.
3. **다음** 버튼을 누릅니다.
4. **적용** 버튼을 누릅니다.

Security Manager 인증 정책 정의

이 컴퓨터의 Security Manager 인증 정책은 로그온과 세션이라는 두 탭에서 정의합니다. 이 탭에는 사용자 세션 동안 컴퓨터 및 HP ProtectTools 응용프로그램에 액세스할 때 각 사용자 클래스 인증에 필요한 인증서가 지정되어 있습니다.

로그온 탭

컴퓨터 액세스에 필요한 인증서를 지정하고 Windows 에 로그온하려면 다음과 같이 하십시오.

1. 관리 콘솔 왼쪽 창에서 **보안**을 확장하고 **인증**을 누릅니다.
2. **로그온** 탭의 드롭다운 목록에서 사용자 범주를 선택합니다.
3. **정책** 섹션에서 나열된 인증서 옆의 확인란을 눌러 선택한 사용자 범주에 필요한 인증서를 지정합니다. 인증서를 하나 이상 지정해야 합니다.
4. **정책** 섹션 드롭다운 목록에서 사용자를 인증하는 데 지정된 인증서가 모두 필요한지 또는 하나만 필요한지 여부를 선택합니다.
5. **적용** 버튼을 누릅니다.

세션 탭

Windows 세션 동안 HP ProtectTools 응용프로그램에 로그온할 때 사용자 인증에 필요한 인증서를 제어하는 정책을 정의하려면 다음과 같이 하십시오.

1. 관리 콘솔 왼쪽 창에서 **보안**을 확장하고 **인증**을 누릅니다.
2. **세션** 탭에서 사용자의 범주를 선택합니다.
3. **정책** 섹션에서 나열된 인증서 옆의 확인란을 눌러 선택한 사용자 범주에 필요한 인증서를 지정합니다. 인증서를 하나 이상 지정해야 합니다.
4. **정책** 섹션 드롭다운 목록에서 사용자를 인증하는 데 지정된 인증서가 모두 필요한지 또는 하나만 필요한지 여부를 선택합니다.
5. **적용** 버튼을 누릅니다.

설정 정의

사용 가능한 고급 보안 설정을 지정할 수 있습니다. 설정을 편집하려면 다음과 같이 하십시오.

1. 관리 콘솔 왼쪽 창에서 **보안**을 확장하고 **설정**을 누릅니다.
2. 특정 설정의 사용 여부를 지정하는 확인란을 누릅니다.
3. **적용** 버튼을 눌러 변경 사항을 저장합니다.

참고: **One Step logon 허용** 설정을 사용하면 BIOS 수준에서 인증되는 경우 이 컴퓨터의 사용자가 Windows 로그온을 건너뛸 수 있습니다.

사용자 관리

사용자 응용프로그램에서 Windows 관리자가 이 컴퓨터의 사용자와 사용자에게 영향을 주는 정책을 관리할 수 있습니다. 관리 콘솔에서 사용자 응용프로그램에 액세스하려면 **사용자**를 누릅니다.

HP ProtectTools 사용자가 표시되고 Security Manager 를 통해 설정된 인증 정책과 해당 정책을 충족시키기 위해 필요한 인증서에 따라 확인됩니다.

특정 사용자에게 적용되는 정책을 보려면 목록에서 사용자를 선택하고 **정책 보기** 버튼을 누릅니다.

인증서를 등록하는 동안 사용자를 관리하려면 목록에서 사용자를 선택하고 **등록** 버튼을 누릅니다.

사용자 추가

이 프로세스에서는 사용자를 로그온 목록에 추가합니다. 사용자를 추가하려면 해당 사용자가 컴퓨터에 Windows 사용자 계정을 가지고 있어야 하며 다음 절차를 진행하는 동안 그 자리에 함께 있으면서 암호를 입력해야 합니다.

사용자를 사용자 목록에 추가하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 관리 콘솔 왼쪽 창에서 **사용자**를 누릅니다.
3. **추가** 버튼을 누릅니다. **사용자 선택** 대화 상자가 열립니다.
4. **고급** 버튼을 누른 다음 **지금 찾기** 버튼을 눌러 추가할 사용자를 검색합니다.
5. 목록에 추가할 사용자를 누른 다음 **확인**을 누릅니다.
6. **사용자 선택** 대화 상자에서 **확인**을 누릅니다.
7. 선택한 계정에 대해 Windows 암호를 입력한 다음 **마침**을 누릅니다.

참고: 기존의 Windows 계정을 사용해야 하며 이름을 정확히 입력해야 합니다. 이 대화 상자를 통해 Windows 사용자 계정을 수정하거나 추가할 수는 없습니다.

사용자 제거

참고: 이 절차를 수행해도 Windows 사용자 계정은 삭제되지 않으며 Security Manager 에서 해당 계정만 제거됩니다. 사용자를 완전히 제거하려면 Security Manager 와 Windows 모두에서 제거해야 합니다.

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 관리 콘솔 왼쪽 창에서 **사용자**를 누릅니다.

3. 제거하려는 계정의 사용자 이름을 누른 다음 **삭제**를 누릅니다.
4. 확인 대화 상자에서 **예**를 누릅니다.

사용자 상태 확인

관리 콘솔의 사용자 섹션에는 각 사용자의 현재 상태가 표시됩니다.

- **녹색 확인 표시** – 사용자가 요구되는 보안 로그인 방법을 구성하였음을 나타냅니다.
- **빨간색 X** – 사용자가 요구되는 보안 로그인 방법을 구성하지 않아 로그인 시도 시 컴퓨터에 액세스할 수 없음을 나타냅니다. 해당 사용자는 설치 마법사를 실행하여 요구되는 로그인 방법을 구성해야 합니다.
- **공백** – 보안 로그인 방법이 필요하지 않음을 나타냅니다.

응용프로그램 설정 구성

설정 창에는 Security Manager 및 해당 응용프로그램의 동작을 구성하는 도구가 있습니다. 설정을 수정하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 관리 콘솔 왼쪽 창에서 **설정**을 누릅니다.
3. **일반** 탭에서 HP ProtectTools Security Manager 의 일반 설정을 선택한 다음 **적용** 버튼을 누릅니다.
4. **응용프로그램** 탭에서 사용 여부를 설정할 응용프로그램을 선택한 다음 **적용** 버튼을 누릅니다.

참고: 응용프로그램의 사용 여부 설정은 컴퓨터를 다시 시작해야 적용됩니다.

드라이브 암호화

Drive Encryption for HP ProtectTools 를 사용하여 컴퓨터 하드 드라이브를 암호화하면 드라이브가 컴퓨터에서 제거되었거나 데이터 복구 서비스를 받더라도 허가받지 않은 사람이 무단으로 하드 드라이브를 읽거나 액세스할 수 없습니다.

Drive Encryption 의 사용 여부를 설정하려면 Administrative Console 에서 설치 마법사를 누릅니다.

△ 주의: 암호화 키를 USB 플래시 드라이브에 백업하여 장치를 안전한 곳에 보관하십시오. 암호를 잊어버린 경우 이 장치를 통해서만 하드 드라이브에 액세스할 수 있습니다.

Drive Encryption for HP ProtectTools 사용에 대한 자세한 내용은 29페이지의 Drive Encryption for HP ProtectTools 를 참조하십시오.

장치 액세스 관리

Device Access Manager for HP ProtectTools 는 PC 의 보안을 약화시킬 수 있는 다양한 장치를 선별적으로 허용하는 고급 보안 옵션을 제공합니다. Device Access Manager for HP ProtectTools 사용에 대한 자세한 내용은 42페이지의 Device Access Manager for HP ProtectTools 를 참조하십시오.

5 HP ProtectTools Security Manager

HP ProtectTools Security Manager를 사용하면 컴퓨터의 보안을 대폭 향상시킬 수 있습니다. Security Manager 응용프로그램에서 수행할 수 있는 기능은 다음과 같습니다.

- 로그온 및 암호 관리
- 손쉽게 Windows 암호 변경
- 스마트 카드 등의 인증 정보 설정
- 하드 드라이브 파쇄 또는 블리치
- 드라이브 암호화 상태 보기
- 장치 액세스 설정 보기
- Security Manager 데이터 백업 및 복원

암호 관리

Credential Manager for HP ProtectTools(암호 관리자)는 사용자의 등록된 인증서로 인증하여 웹 사이트 및 프로그램을 실행하고 로그온할 수 있는 로그온을 만들고 관리합니다.

암호 관리에 대한 자세한 내용은 32페이지의 Credential Manager for HP ProtectTools(암호 관리자)를 참조하십시오.

인증서 설정

Security Manager 인증서는 사용자의 본인 확인을 위해 사용됩니다. 이 컴퓨터의 관리자는 Windows 계정, 웹 사이트 또는 프로그램에 로그온할 때 사용자 신분을 증명하기 위해 사용할 인증서를 설정할 수 있습니다.

사용 가능한 인증서는 컴퓨터에 연결되거나 내장된 보안 장치에 따라 다릅니다. 지원되는 인증서 목록은 인증서 그룹에 나와 있습니다.

Windows 암호 변경

Security Manager를 사용하면 Windows 제어판을 사용하는 것보다 쉽고 빠르게 Windows 암호를 변경할 수 있습니다.

Windows 암호를 변경하려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager 왼쪽 창에서 **인증서**를 누릅니다.
2. **Windows 암호**를 누릅니다.

3. **현재 Windows 암호** 상자에 현재 암호를 입력합니다.
4. **새 Windows 암호** 및 **새 암호 확인** 상자에 새 암호를 입력합니다.
5. **변경**을 누릅니다.

파일 파쇄 또는 블리치

File Sanitizer for HP ProtectTools 는 파일을 의미 없는 데이터로 덮어쓰는 방식으로 파일을 삭제합니다. "파쇄"라고 하는 이 프로세스는 삭제한 파일의 복구를 매우 어렵게 하여 정보 보안을 대폭 강화시켜 줍니다. 또한 File Sanitizer 는 "블리치"라는 프로세스를 통해 하드 드라이브에서 이전에 사용된 공간을 덮어쓰는 방식으로 정보 보안을 강화시키기도 합니다. File Sanitizer 를 사용하여 삭제한 파일은 운영 체제나 일반적으로 사용하는 다른 파일 복구 소프트웨어로 복구할 수 없습니다.

File Sanitizer for HP ProtectTools 사용에 대한 자세한 내용은 36페이지의 HP ProtectTools File Sanitizer 를 참조하십시오.

드라이브 암호화 상태 보기

Drive Encryption 은 Administrative Console 에서 Windows 관리자가 설정합니다. 사용자는 Security Manager 에서 암호화 상태를 볼 수 있습니다.

드라이브 암호화 상태를 보려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.
2. Security Manager 왼쪽 창에서 **암호화 상태**를 누릅니다. 암호화 상태 페이지에는 드라이브 암호화의 활성 여부와 암호화되거나 암호화되지 않은 드라이브가 표시됩니다.

장치 액세스 보기

Device Access 는 관리 콘솔에서 Windows 관리자가 설정합니다. 사용자는 Security Manager 에서 장치 액세스 설정을 볼 수 있습니다.

장치 액세스 설정을 보려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.
2. Security Manager 왼쪽 창에서 **Device Access Manager** 를 확장합니다.
3. 액세스가 거부된 장치를 보려면 **단순 구성**을 누릅니다. 옆에 확인란이 있는 장치는 액세스가 거부됩니다.
4. 액세스가 거부된 사용자나 그룹을 보려면 **장치 클래스 구성**을 누릅니다.
5. 장치 액세스가 거부되거나 허용된 사용자나 그룹을 보려면 장치를 누릅니다.

응용프로그램 추가

이 프로그램에 새 기능을 추가할 수 있는 추가 응용프로그램을 사용할 수 있습니다.

1. **시작**, **모든 프로그램**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.
2. Security Manager 왼쪽 창에서 **자세히 검색**을 누릅니다.

   참고: **자세히 검색** 링크가 없으면 컴퓨터의 관리자가 해당 링크를 사용하지 않도록 설정한 것입니다.

3. **응용프로그램 추가** 탭에서 추가 응용프로그램을 찾습니다.
4. **업데이트 및 메시지** 탭에서 **새 응용프로그램 및 업데이트 최신 정보 받기** 확인란을 누르고 업데이트 확인 간격(일)을 설정하여 새 응용프로그램 및 업데이트에 대한 최신 정보를 수신하거나 **지금 확인** 버튼을 눌러 업데이트를 바로 확인할 수 있습니다.

기본 설정 지정

기본 설정 페이지에서 **작업 표시줄에 아이콘 표시** 확인란을 선택하면 작업 표시줄 알림 영역(시스템 트레이)에 Security Manager 아이콘이 표시됩니다.

기본 설정 페이지에 액세스하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.
2. Security Manager 왼쪽 창에서 **고급**을 누른 다음 **기본 설정**을 누릅니다.
3. **작업 표시줄에 아이콘 표시** 확인란을 선택하거나 선택 취소하고 **적용**을 누릅니다.

백업 및 복원

Security Manager 데이터를 정기적으로 백업하는 것이 좋습니다. 백업 주기는 데이터를 변경하는 빈도에 따라 달라질 수 있습니다. 예를 들어 새 로그온을 매일 정기적으로 추가하는 경우 데이터를 매일 백업해야 합니다.

가져오기 및 내보내기 작업이라고도 하는 컴퓨터 간 마이그레이션에도 백업을 사용할 수 있습니다. 하지만 이 기능을 사용하면 데이터만 백업된다는 점에 주의하십시오.

다른 컴퓨터 또는 운영 체제를 다시 설치한 후 동일한 컴퓨터에 백업 파일을 복원하는 경우 시스템에 HP ProtectTools Security Manager 가 이미 설치되어 있어야 백업 파일에서 데이터를 복원할 수 있습니다.

데이터 백업

데이터를 백업하면 사용자가 입력한 암호로 보호되는 암호화된 파일에 로그온 및 인증 정보가 저장됩니다.

데이터를 백업하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.
2. Security Manager 왼쪽 창에서 **고급**을 누른 다음 **백업 및 복원**을 누릅니다.
3. **데이터 백업**을 누릅니다.

4. 백업에 포함할 모듈을 선택합니다. 대부분의 경우 모든 항목을 선택할 수 있습니다. **다음**을 누릅니다.
5. 사용자의 신분을 확인하는 암호를 입력하고 화살표 버튼을 누릅니다.
6. 저장 파일의 경로와 이름을 입력합니다. 기본적으로 파일은 문서 폴더에 저장됩니다. 다른 위치를 지정하려면 **찾아보기**를 누릅니다. **다음**을 누릅니다.
7. 파일을 보호하려면 암호를 입력하고 확인합니다.
8. **마침**을 누릅니다.

데이터 복원

Security Manager 의 백업 및 복원 기능을 통해 이전에 만든 암호로 보호되는 암호화된 파일에서 데이터를 복원합니다.

데이터를 복원하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.
2. Security Manager 왼쪽 창에서 **고급**을 누른 다음 **백업 및 복원**을 누릅니다.
3. **데이터 복원**을 누릅니다.
4. 저장 파일의 경로와 이름을 입력하거나 **찾아보기**를 누르고 파일을 선택합니다.
5. 파일 보호에 사용했던 암호를 입력하고 **다음**을 누릅니다.
6. 데이터를 복원할 모듈을 선택합니다. 대부분의 경우에는 나열된 모든 모듈이 이에 해당합니다. **다음**을 누릅니다.
7. **마침**을 누릅니다.

Windows 사용자 이름 및 사진 변경

Windows 사용자 이름 및 사진은 Security Manager 의 왼쪽 상단에 표시됩니다.

사용자 이름 및/또는 사진을 변경하려면 다음과 같이 하십시오.

1. Security Manager 에서 사용자 이름 및 사진이 있는 왼쪽 상단 섹션을 누릅니다.
2. 사용자 이름을 변경하려면 **Windows 사용자 이름** 상자에 이름을 입력합니다.
3. 사진을 변경하려면 **사진 선택** 버튼을 누르고 사진을 찾아 선택합니다.
4. **저장** 버튼을 눌러 변경 사항을 저장합니다.

6 Drive Encryption for HP ProtectTools

참고: Drive Encryption for HP ProtectTools 는 일부 모델에서만 사용 가능합니다.

오늘날 자신이나 같은 직장 동료 누구든지 컴퓨터를 도난당할 수 있으며 이로 인해 회사의 중요한 정보가 심각하게 손상될 수 있습니다. 컴퓨터 하드 드라이브에 저장된 모든 내용을 암호화하면 드라이브가 컴퓨터에서 제거되었거나 데이터 복구 서비스를 받더라도 허가받지 않은 사람이 무단으로 읽거나 액세스할 수 없습니다.

Drive Encryption for HP ProtectTools 소프트웨어를 사용하면 하드 드라이브가 암호화되어 데이터가 완전히 보호됩니다. Drive Encryption 이 활성화되면 Windows 시작 전에 표시되는 Drive Encryption 로그인 화면에서 로그인해야 합니다.

동일한 Windows 세션 동안 Drive Encryption 에서 무단 액세스가 방지되지 않습니다. PC 가 부팅되고 사용자 이름 및 암호를 입력하면 하드 드라이브의 데이터가 계속 암호화되지만 시스템의 모든 사용자가 사용할 수 있습니다. 자리를 비운 상태에서 컴퓨터를 사용하지 않을 때 Windows 세션을 암호로 보호하십시오.

참고: Drive Encryption for HP ProtectTools 는 HP ProtectTools Administrative Console 의 설치 마법사를 통해서만 사용할 수 있습니다.

참고: AMD 프로세서를 사용하는 시스템에 RAID 방식으로 구성된 경우에는 64 비트 운영 체제에서 Drive Encryption 이 지원되지 않습니다.

참고: Drive Encryption 은 Dictionary Attack 방지를 지원하지 않습니다.

Drive Encryption:

- 내장 하드 드라이브에 저장된 모든 내용 암호화
- 간편한 암호 액세스 및 사전 부팅 인증 제공
- Microsoft Windows XP, Windows Vista 및 Windows 7 지원

Drive Encryption for HP ProtectTools 에서 다음과 같은 다양한 작업을 수행할 수 있습니다.

- Drive Encryption 관리
  - 개별 드라이브의 사용 여부 설정
- 백업 및 복구
  - 백업 키 만들기
  - 복구 수행

△ **주의:** 암호화 키를 USB 플래시 드라이브에 백업하여 장치를 안전한 곳에 보관하십시오. 암호를 잊어버린 경우 이 장치를 통해서만 하드 드라이브에 액세스할 수 있습니다.

주의: Drive Encryption 모듈을 제거하려는 경우 또는 백업 및 복원 솔루션을 사용하고 있는 경우에는, 먼저 암호화된 모든 드라이브의 암호를 해독해야 합니다. 그렇지 않으면 암호화된 드라이브의 데이터에 액세스할 수 없게 됩니다. Drive Encryption 모듈을 재설치하면 암호화된 드라이브에 액세스할 수 없게 됩니다.

설치 절차

Drive Encryption 열기

1. **시작**, **모든 프로그램**, **HP ProtectTools Administrative Console** 을 차례로 누릅니다.
2. **Drive Encryption** 을 누릅니다.

일반 작업

Drive Encryption 활성화

HP ProtectTools Administrative Console 설치 마법사를 통해 Drive Encryption 을 활성화합니다.

Drive Encryption 비활성화

HP ProtectTools Administrative Console 설치 마법사를 통해 Drive Encryption 을 비활성화합니다.

Drive Encryption 이 활성화된 후 로그인

Drive Encryption 이 활성화된 후 사용자 계정을 등록하면 컴퓨터를 켤 때 Drive Encryption 로그온 화면에 로그인해야 합니다.

참고: Windows 관리자가 HP ProtectTools Administrative Console 의 Pre-boot Security 를 활성화한 경우에는 컴퓨터를 켠 후 Drive Encryption 로그온 화면에서 로그인하지 않고 바로 컴퓨터에 로그인할 수 있습니다.

참고: Drive Encryption 로그온 화면에서 복구 키를 사용하여 로그인하는 경우 Windows 로그온 화면에 Windows 사용자 이름을 선택하고 암호를 입력하라는 메시지가 표시됩니다.

고급 작업

Drive Encryption 관리(관리자 작업)

Drive Encryption 창에서 Windows 관리자는 Drive Encryption 의 상태(활성 또는 비활성)를 보고 변경하며 컴퓨터에 있는 모든 하드 드라이브의 암호화 상태를 볼 수 있습니다.

개별 드라이브 암호화 또는 암호 해제

1. Administrative Console 왼쪽 창에서 **Drive Encryption** 을 확장하고 **암호화 관리**를 누릅니다.
2. **암호화 변경** 버튼을 누릅니다.
3. 암호화 변경 대화 상자에서 암호화하거나 암호 해제하려는 각 하드 드라이브 옆의 확인란을 선택 또는 선택 해제한 후 **확인**을 누릅니다.

참고: 드라이브를 암호화 또는 암호 해제할 때 진행 표시줄에는 현재 세션에서 절차가 완료될 때까지 남은 시간이 표시됩니다. 암호화가 진행되는 동안 컴퓨터가 종료되거나 절전 또는 최대 절전 모드가 시작되어 컴퓨터가 재시작되는 경우 남은 시간은 처음으로 재설정되어 표시됩니다. 하지만 실제 암호화 과정은 마지막에 중단되었던 부분부터 시작됩니다. 따라서 남은 시간 및 진행 표시줄은 이전에 수행된 과정을 반영하여 빠르게 변합니다.

백업 및 복구(관리자 작업)

Drive Encryption: 백업 및 복구 창에서 Windows 관리자는 암호화 키를 백업 및 복구할 수 있습니다.

백업 키 생성

△ 주의: 암호를 잊어버린 경우 백업 키가 들어 있는 저장 장치를 통해서만 하드 드라이브에 액세스할 수 있으므로 이 저장 장치를 안전한 곳에 보관하십시오.

1. Administrative Console 왼쪽 창에서 **Drive Encryption** 을 확장하고 **백업 및 복구**를 누릅니다.
2. **백업 키** 버튼을 누릅니다.
3. "백업 디스크 선택" 페이지에서 암호화 키를 백업할 장치 이름을 누른 후 **다음**을 누릅니다.
4. 다음 페이지에 표시된 정보를 읽은 후 **다음**을 누릅니다.

   암호화 키가 선택한 저장 장치에 저장됩니다.
5. 확인 대화 상자가 표시되면 **확인**을 누릅니다.

참고: 복구 관리 및 수행에 대한 자세한 내용은 Drive Encryption for HP ProtectTools 도움말 파일을 참조하십시오.

7 Credential Manager for HP ProtectTools (암호 관리자)

암호 관리자를 사용하면 Windows, 웹 사이트 및 프로그램에 보다 쉽고 안전하게 로그온할 수 있습니다.

암호 관리자를 통해 신속하고 안전하게 액세스할 수 있는 웹 사이트 및 프로그램의 로그온 화면을 설정할 수 있습니다. 우선, 암호 관리자는 로그온 화면의 입력 상자에 사용자가 입력하는 로그온 및 특정 데이터를 인식합니다. 그런 다음 로그온 화면에서 사용자의 신분을 확인한 후 필요한 데이터를 자동으로 채워 제출합니다.

보다 신속하게 액세스하려면 직접 구성할 수 있는 단축키 조합을 사용하여 로그온 메뉴를 표시할 수 있습니다(기본값: Ctrl+Windows+H). 메뉴에서 로그온을 선택하기만 하면 암호 관리자가 웹 사이트나 프로그램을 실행하여 로그온 화면으로 이동한 다음 자동으로 로그온합니다.

사용자의 신분을 확인하기 위해 Windows 암호와 같은 HP ProtectTools for Small Business 인증서가 사용됩니다. 즉, 설정한 모든 로그온 화면에 로그온할 때는 동일한 인증서를 사용하게 됩니다. 따라서 따로 기록하거나 기억할 필요가 없는 강력한 암호를 작성하여 계정 보안을 강화할 수 있습니다.

암호 관리자를 사용하면 보안상 위험한 암호가 있는지 한 눈에 확인하고 새 사이트에 사용할 강력한 복합 암호를 자동으로 생성할 수 있습니다.

암호 관리자에서 로그온 및 암호를 확인하고 언제든지 편집할 수도 있습니다. 설정된 프로그램의 로그온 화면이나 웹 사이트 로그온 화면이 활성화 상태일 때 항상 표시되는 암호 관리자 아이콘에서도 다양한 암호 관리자 기능을 사용할 수 있습니다. 해당 아이콘을 누르면 다음 옵션을 선택할 수 있는 상황 메뉴가 표시됩니다.

로그온을 아직 생성하지 않은 웹페이지 또는 프로그램:

상황 메뉴에 다음과 같은 옵션이 표시됩니다.

- 암호 관리자에 [somedomain.com] 추가 – 현재 로그온 화면에 로그온을 추가하는 데 사용합니다.
- 암호 관리자 열기 – 암호 관리자 페이지에서 Security Manager 를 실행합니다.
- 암호 관리자 아이콘 설정 – 암호 관리자 아이콘이 표시되는 조건을 지정합니다.
- 도움말 – 암호 관리자 응용프로그램에 대한 온라인 도움말을 표시합니다.

로그온을 이미 생성한 웹페이지 또는 프로그램:

상황 메뉴에 다음과 같은 옵션이 표시됩니다.

- 로그온 데이터 채우기 – 로그온 데이터를 로그온 필드에 입력한 다음 페이지를 제출합니다(제출은 로그온을 만들거나 마지막으로 편집할 때 지정됨).
- 로그온 편집 – 이 웹 사이트의 로그온 데이터를 편집합니다.

- 로그온 추가 – 동일한 웹 사이트 또는 프로그램에 다른 로그온을 추가하는 데 사용합니다.
- 암호 관리자 열기 – 암호 관리자 페이지에서 Security Manager 대시보드를 실행합니다.
- 도움말 – 암호 관리자 응용프로그램에 대한 온라인 도움말을 표시합니다.

로그온 추가

로그온을 추가하려면 다음과 같이 하십시오.

1. 웹 사이트나 프로그램의 로그온 화면을 엽니다.
2. 암호 관리자 아이콘에서 화살표를 누른 다음 로그온 화면이 웹 사이트 또는 프로그램용인지에 따라 다음 중 하나를 선택합니다.
   - 웹 사이트 - **암호 관리자에 [도메인 이름] 추가**를 선택합니다.
   - 프로그램 - **암호 관리자에 이 로그온 화면 추가**를 선택합니다.
3. 로그온 데이터를 입력합니다. 화면의 로그온 필드와 대화 상자의 해당 필드는 굵은 주황색 테두리로 표시되어 있습니다. 이 대화 상자를 표시하는 다른 옵션도 지원됩니다(예: 암호 관리자 **관리** 탭에서 로그온 추가 선택). 일부 옵션은 컴퓨터에 연결된 보안 장치에 따라 다릅니다(예: Ctrl-H 단축키 사용 또는 스마트 카드 삽입).
   - 로그온 필드 오른쪽에 있는 화살표를 눌러 미리 서식이 지정된 옵션 중 하나로 필드를 채웁니다.
   - 화면에 있는 다른 필드를 선택적으로 로그온에 추가하려면 **다른 필드 선택**을 누릅니다.
   - 로그온 필드를 채우지만 제출하지는 않으려면 **로그온 데이터 제출**을 선택 취소합니다.
   - 이 로그온의 암호를 보려면 **암호 표시**를 누릅니다.
4. **확인**을 누릅니다. 로그온이 만들어졌는지 알 수 있도록 암호 관리자 아이콘에서 더하기(+) 기호가 제거됩니다.

이제 해당 웹 사이트로 이동하거나 프로그램을 실행할 때마다 등록된 인증서를 사용하여 로그온이 가능함을 나타내는 암호 관리자 아이콘이 표시됩니다.

로그온 편집

로그온을 편집하려면 다음과 같이 하십시오.

1. 웹 사이트나 프로그램의 로그온 화면을 엽니다.
2. 암호 관리자 아이콘에서 화살표를 누르고 **로그온 편집**을 선택하여 로그온 정보를 편집할 수 있는 대화 상자를 표시합니다. 화면의 로그온 필드 및 대화 상자의 해당 필드는 굵은 주황색 테두리로 표시되어 있습니다.
3. 로그온 정보를 편집합니다.
   - 로그온 필드 오른쪽에 있는 화살표를 눌러 미리 서식이 지정된 옵션 중 하나로 필드를 채웁니다.
   - 화면에 있는 다른 필드를 선택적으로 로그온에 추가하려면 **다른 필드 선택**을 누릅니다.

- 로그온 필드를 채우지만 제출하지는 않으려면 **로그온 데이터 제출**을 선택 취소합니다.
- 이 로그온의 암호를 보려면 암호 표시를 누릅니다.

4. **확인**을 누릅니다.

로그온 메뉴 사용

암호 관리자는 로그온을 만든 웹 사이트와 프로그램을 쉽고 빠르게 실행할 수 있게 합니다. 암호 관리자의 **관리** 탭 또는 로그온 메뉴에서 프로그램이나 웹 사이트를 두 번 누르면 로그온 화면이 실행되고 사용자의 로그온 데이터가 입력됩니다. 기본적으로, 해당 정보는 웹 사이트로 바로 제출됩니다. 처음 로그온 데이터를 설정하거나 편집할 때에 **계정 데이터 제출**을 선택 취소하더라도 이는 마찬가지입니다.

로그온을 생성하면 암호 관리자 로그온 메뉴에 자동으로 추가됩니다.

로그온 메뉴를 표시하려면 암호 관리자 단축키 조합을 누릅니다. Ctrl-H 가 기본값이지만, **암호 관리자 > 설정**에서 단축키 조합을 변경할 수 있습니다.

로그온 범주화

범주를 사용하면 로그온을 체계적으로 유지할 수 있습니다. 범주화는 하나 이상의 범주를 만들고 로그온을 원하는 범주에 끌어 놓으면 되는 간단한 방법입니다.

범주를 추가하려면 다음과 같이 하십시오.

1. Security Manager 왼쪽 창에서 **암호 관리자**를 선택합니다.
2. **관리** 탭을 선택하고 **범주 추가**를 누릅니다.
3. 범주의 이름을 입력합니다.
4. **확인**을 누릅니다.

로그온을 범주에 추가하려면 다음과 같이 하십시오.

1. 원하는 로그온 위에 마우스 포인터를 놓습니다.
2. 왼쪽 마우스 버튼을 누르고 있습니다.
3. 로그온을 범주 목록으로 끕니다. 범주 위로 마우스를 가져가면 해당 범주가 강조 표시됩니다.
4. 원하는 범주가 강조 표시되면 마우스 버튼을 놓습니다.

로그온은 범주로 이동하지 않으며 선택한 범주에 사본이 만들어지기만 합니다. 즉, 동일한 로그온을 둘 이상의 범주에 추가할 수 있습니다. **모두**를 누르면 언제든지 모든 로그온을 볼 수 있습니다.

로그온 관리

암호 관리자를 사용하면 사용자 이름, 암호, 여러 로그온 계정 등의 로그온 정보를 한 곳에서 쉽고 간편하게 관리할 수 있습니다.

로그온은 **관리** 탭에 나열되어 있습니다. 동일한 웹 사이트에 여러 개의 로그온을 만들 때마다 각 로그온이 웹 사이트 이름 아래에 나열되고 로그온 목록에도 추가됩니다.

로그온을 관리하려면 다음과 같이 하십시오.

Security Manager 왼쪽 창에서 **암호 관리자**를 선택하고 **관리** 탭을 누릅니다.

- 로그온 추가 – **로그온 추가**를 누르고 화면의 지침을 따릅니다.
- 로그온 편집 – 로그온을 선택하고 **편집**을 누릅니다. 그런 다음 로그온 데이터를 원하는 대로 변경합니다.
- 로그온 삭제 – 로그온을 선택하고 **삭제**를 누릅니다.

개별 웹 사이트나 프로그램에 다른 로그온을 추가하려면 다음과 같이 하십시오.

1. 웹 사이트나 프로그램의 로그온 화면을 실행합니다.
2. 암호 관리자 아이콘을 눌러 바로 가기 메뉴를 표시합니다.
3. **다른 로그온 추가**를 선택하고 화면의 지침을 따릅니다.

암호 강도 결정

사용자 신원 보호의 측면에서 사이트와 프로그램에 로그온할 때 강력한 암호를 사용하는 것은 중요합니다.

암호 관리자는 웹 사이트와 프로그램에 로그온할 때 사용하는 각 암호의 강도를 자동으로 바로 분석하여 손쉽게 보안 수준을 모니터링하고 강화할 수 있게 해 줍니다. 로그온 시 사용하는 암호의 강도는 암호 관리자 **암호 강도** 탭에서 확인할 수 있습니다.

암호 관리자 아이콘 설정

암호 관리자는 웹 사이트와 프로그램의 로그온 화면을 확인하려고 합니다. 로그온을 만들지 않은 로그온 화면이 있으면 암호 관리자에서 더하기("+") 기호가 있는 암호 관리자 아이콘을 표시하여 화면에 대한 로그온을 추가하라는 메시지를 표시합니다.

다음과 같은 설정을 구성할 수 있습니다.

- 항상 확인 – 암호 관리자에 로그온이 아직 설정되지 않은 로그온 화면이 표시될 때마다 로그온을 추가하라는 메시지를 표시하려면 이 옵션을 선택합니다.
- 이 화면에 대해 확인하지 않음 – 암호 관리자에 특정 로그온 화면에 대해 로그온을 추가하라는 메시지를 다시 표시하지 않으려면 이 옵션을 선택합니다.
- 확인 안 함 – 암호 관리자에 설정되지 않은 로그온 화면에 대한 메시지를 표시하지 않으려면 이 옵션을 선택합니다.

8 HP ProtectTools File Sanitizer

File Sanitizer 는 컴퓨터에서 중요한 파일과 폴더(개인 정보 또는 파일, 기록 데이터/웹 관련 데이터 또는 다른 데이터 구성 요소)를 안전하게 지우고 하드 드라이브를 정기적으로 블리치하는 데 사용되는 도구입니다.

참고: File Sanitizer 는 현재 하드 드라이브에서만 작동됩니다.

파쇄 정보

Windows 에서 파일 및/또는 폴더를 삭제해도 하드 드라이브에서 그 내용이 완전히 제거되는 것은 아닙니다. Windows 에서는 참조만 삭제합니다. 다른 파일이 하드 드라이브의 동일한 영역에 새로운 정보를 덮어쓸 때까지 해당 내용은 하드 드라이브에 남아 있습니다.

파쇄는 일반적인 Windows 삭제(File Sanitizer 에서는 기본 삭제라고 함)와 다릅니다. 데이터를 파쇄하면 해당 데이터를 다시 복구하는 것이 사실상 불가능하기 때문입니다.

파쇄 프로필(높은 보안, 중간 보안 또는 낮은 보안)을 선택하면 미리 정의된 파일 및/또는 폴더의 목록과 지우는 방법이 자동으로 선택됩니다. 또한 파쇄 프로필을 사용자 정의하여 파쇄 주기 횟수, 파쇄할 파일, 파쇄 전에 확인할 파일 및 파쇄에서 제외할 파일을 지정할 수도 있습니다.

자동 파쇄 예약을 설정하거나 원할 때마다 파일 및/또는 폴더를 수동으로 파쇄할 수도 있습니다.

여유 공간 블리치 정보

여유 공간 블리치를 통해 삭제된 파일 위에 임의 데이터를 덮어쓰는 방식으로 사용자가 삭제된 파일의 원래 내용을 보지 못하도록 할 수 있습니다.

참고: 여유 공간 블리치는 Windows 휴지통을 사용하여 삭제하거나 수동으로 삭제한 파일에 사용할 수 있습니다. 파쇄된 파일은 여유 공간 블리치를 사용하더라도 보안이 강화되지 않습니다.

자동 여유 공간 블리치 예약을 설정하거나 작업 표시줄 오른쪽 끝에 있는 알림 영역의 HP ProtectTools 아이콘을 사용하여 수동으로 여유 공간 블리치를 활성화할 수 있습니다.

설치 절차

File Sanitizer 열기

File Sanitizer 를 열려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.
2. Security Manager 왼쪽 창에서 **File Sanitizer** 를 누릅니다.

   또는

- **File Sanitizer** 를 두 번 누릅니다.

  또는

- 작업 표시줄의 가장 오른쪽에 있는 알림 영역의 HP ProtectTools 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer** 를 강조 표시하고 **File Sanitizer 열기**를 누릅니다.

여유 공간 블리치 예약 설정

여유 공간 블리치 예약을 설정하려면 다음과 같이 하십시오.

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **블리치**를 누릅니다.
2. **스케줄러 활성화** 확인란을 선택하고 Windows 암호를 입력한 다음 하드 드라이브를 블리치할 날짜와 시간을 입력합니다.
3. **저장** 아이콘을 누릅니다.

참고: 여유 공간 블리치 작업에 시간이 오래 걸릴 수 있습니다. 여유 공간 블리치를 백그라운드 작업으로 수행하더라도 프로세스 사용량이 증가하여 컴퓨터가 느려질 수 있습니다.

파쇄 예약 설정

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **파쇄**를 누릅니다.
2. 파쇄 옵션을 선택합니다.

- **Windows 종료** - Windows 종료 시 선택한 모든 파일을 파쇄하려면 이 옵션을 선택합니다.

  참고: 이 옵션을 선택하면 종료 시 선택한 파일의 파쇄를 계속할 것인지 아니면 해당 절차를 건너뛸 것인지 묻는 대화 상자가 표시됩니다. 파쇄 절차를 생략하려면 예를 누르고, 파쇄를 계속하려면 아니요를 누릅니다. Windows 에서 종료할 준비로 소프트웨어를 닫고 오류를 생성하므로 예 또는 아니요 옵션을 신속하게 선택해야 합니다. 파쇄를 계속하기 위해 아니요를 선택한 경우 Windows 에 File Sanitizer 가 응답하지 않는다는 오류 화면이 표시될 수 있습니다. File Sanitizer 에서 파쇄를 완료하게 한 다음 종료를 다시 시작합니다.

- **웹 브라우저 열기** - 웹 브라우저를 열 때 브라우저 URL 기록 등 선택한 웹 관련 파일을 모두 파쇄하려면 이 옵션을 선택합니다.
- **웹 브라우저 종료** - 웹 브라우저를 닫을 때 브라우저 URL 기록 등 선택한 웹 관련 파일을 모두 파쇄하려면 이 옵션을 선택합니다.

- **키 시퀀스** - 키 시퀀스를 사용하여 파쇄를 시작하려면 이 옵션을 선택합니다.
- **스케줄러** - 스케줄러 활성화 확인란을 선택하고 Windows 암호를 입력한 다음 선택한 파일을 파쇄할 날짜와 시간을 입력합니다.

3. **저장** 아이콘을 누릅니다.

파쇄 프로필 선택 또는 생성

미리 정의된 프로필을 선택하거나 개인 프로필을 작성하여 지우는 방법을 지정하고 파쇄할 파일 및/또는 폴더를 선택할 수 있습니다.

미리 정의된 파쇄 프로필 선택

미리 정의된 파쇄 프로필(높은 보안, 중간 보안 또는 낮은 보안)을 선택하면 미리 정의된 지우는 방법과 파일의 목록이 자동으로 선택됩니다. 세부 정보 보기 버튼을 누르면 파쇄하도록 선택한 미리 정의된 파일 목록을 확인할 수 있습니다.

미리 정의된 파쇄 프로필을 선택하려면 다음과 같이 하십시오.

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **설정**을 누릅니다.
2. 미리 정의된 파쇄 프로필을 누릅니다.
3. **세부 정보 보기**를 눌러 파쇄하기로 선택한 파일 목록을 확인합니다.
4. **다음 자산을 파쇄**에서 파쇄 전에 확인할 각 파일 옆의 확인란을 선택합니다.
5. **적용**을 누릅니다.

고급 보안 파쇄 프로필 사용자 정의

파쇄 프로필을 작성할 때 파쇄 주기 횟수, 파쇄할 파일, 파쇄 전에 확인할 파일 및 파쇄에서 제외할 파일을 지정할 수도 있습니다.

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **설정**을 누른 다음 **고급 보안 설정**을 선택하고 **자세히 보기**를 누릅니다.
2. 파쇄 주기를 지정합니다.

참고: 각 파일에 대해 선택한 파쇄 주기 횟수가 수행됩니다. 예를 들어, 파쇄 주기로 3 을 선택한 경우 데이터를 지우는 알고리즘이 각기 다른 시간대에 3 번 실행됩니다. 보안 수준이 높은 파쇄 주기를 선택한 경우 파쇄 작업이 상당히 오래 걸릴 수 있습니다. 그러나 지정한 파쇄 주기 횟수가 많을수록 컴퓨터의 보안이 강화됩니다.

3. 다음 방법을 통해 파쇄하려는 자산을 선택합니다.
   a. **사용 가능한 파쇄 옵션**에서 파일을 누른 다음 **추가**를 누릅니다.
   b. 사용자 정의 파일을 추가하려면 **사용자 정의 옵션 추가**를 누르고 파일 이름 또는 폴더 이름을 입력하거나 찾은 다음 **확인**을 누릅니다. 사용자 정의 파일을 누른 다음 **추가**를 누릅니다.

참고: 사용 가능한 파쇄 옵션에서 파일을 삭제하려면 원하는 파일을 누른 다음 **삭제**를 누르면 됩니다.

4. **다음 자산을 파쇄**에서 파쇄 전에 확인할 각 파일 옆의 확인란을 선택합니다.

참고: 파쇄 목록에서 파일을 제거하려면 원하는 파일을 누른 다음 **제거**를 누르면 됩니다.

5. **다음 자산을 파쇄하지 않음**에서 **추가**를 눌러 파쇄에서 제외할 특정 파일을 선택합니다.

6. 파쇄 프로필 구성을 마치면 **적용**을 누릅니다.

기본 삭제 프로필 사용자 정의

기본 삭제 프로필은 파쇄 없이 일반적인 파일 삭제를 수행합니다. 기본 삭제 프로필을 사용자 정의할 때 기본 삭제에 포함할 파일, 기본 삭제 실행 전에 확인할 파일 및 기본 삭제에서 제외할 파일을 지정합니다.

참고: 기본 삭제 옵션을 사용하는 경우 여유 공간 블리치를 정기적으로 실행하는 것이 좋습니다.

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **설정**을 누른 다음 **단순 삭제 설정**을 선택하고 **자세히 보기**를 누릅니다.

2. 삭제할 파일을 선택하려면 다음과 같이 하십시오.

   a. **사용 가능한 삭제 옵션**에서 파일을 누른 다음 **추가**를 누릅니다.

   b. 사용자 정의 파일을 추가하려면 **사용자 정의 옵션 추가**를 누르고 파일 이름 또는 폴더 이름을 입력하거나 찾은 다음 **확인**을 누릅니다. 사용자 정의 파일을 누른 다음 **추가**를 누릅니다.

   참고: 사용 가능한 삭제 옵션에서 파일을 삭제하려면 원하는 파일을 누른 다음 **삭제**를 누르면 됩니다.

3. **다음 자산을 삭제**에서 삭제 전에 확인할 각 파일 옆의 확인란을 선택합니다.

참고: 삭제 목록에서 파일을 제거하려면 원하는 파일을 누른 다음 **제거**를 누르면 됩니다.

4. **다음 자산을 삭제하지 않음**에서 **추가**를 눌러 파쇄에서 제외할 특정 파일을 선택합니다.

5. 단순 삭제 프로필 구성을 마치면 **적용**을 누릅니다.

일반 작업

키 시퀀스를 사용하여 파쇄 시작

키 시퀀스를 지정하려면 다음과 같이 하십시오.

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **파쇄**를 누릅니다.

2. **키 시퀀스** 확인란을 선택합니다.

3. 사용 가능한 상자에 문자를 입력한 다음 **CTRL**, **ALT** 또는 **SHIFT** 상자를 누르거나 모두 선택합니다.

   예를 들어 S 키와 Ctrl+Shift 를 사용하여 자동 파쇄를 시작하려면 상자에 S 를 입력한 다음 **CTRL** 및 **SHIFT** 옵션을 선택합니다.

참고: 키 시퀀스 선택은 키 시퀀스를 직접 구성하는 것과 다릅니다.

키 시퀀스를 사용하여 파쇄를 시작하려면 다음과 같이 하십시오.

1. Ctrl, Alt 또는 Shift 키(또는 자신이 지정한 키 조합)를 누른 상태에서 선택한 문자를 누릅니다.

2. 확인 대화 상자가 표시되면 **예**를 누릅니다.

File Sanitizer 아이콘 사용

△ 주의: 파쇄된 파일은 복구할 수 없으므로 수동 파쇄할 항목은 신중하게 선택하십시오.

1. 파쇄하려는 문서 또는 폴더로 이동합니다.
2. 바탕 화면의 File Sanitizer 아이콘으로 파일을 끕니다.
3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

단일 자산 수동 파쇄

△ 주의: 파쇄된 파일은 복구할 수 없으므로 수동 파쇄할 항목은 신중하게 선택하십시오.

1. 작업 표시줄의 가장 오른쪽에 있는 알림 영역의 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer** 를 강조 표시하고 **단일 자산 파쇄**를 누릅니다.
2. 찾아보기 대화 상자가 열리면 파쇄할 파일로 이동한 다음 **열기**를 누릅니다.

참고: 단일 파일이나 폴더를 선택할 수 있습니다.

3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

또는

1. 바탕 화면에서 **File Sanitizer** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **단일 자산 파쇄**를 누릅니다.
2. 찾아보기 대화 상자가 열리면 파쇄할 파일로 이동한 다음 **확인**을 누릅니다.
3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

또는

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **파쇄**를 누릅니다.
2. **찾아보기** 버튼을 누릅니다.
3. 찾아보기 대화 상자가 열리면 파쇄할 파일로 이동한 다음 **열기**를 누릅니다.
4. 확인 대화 상자가 표시되면 **예**를 누릅니다.

모든 항목 수동 파쇄

1. 작업 표시줄의 가장 오른쪽에 있는 알림 영역의 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer** 를 강조 표시하고 **지금 파쇄**를 누릅니다.
2. 확인 대화 상자가 표시되면 **예**를 누릅니다.

또는

1. 바탕 화면의 **File Sanitizer** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **지금 파쇄**를 누릅니다.
2. 확인 대화 상자가 표시되면 **예**를 누릅니다.

여유 공간 블리치 수동 활성화

1. 작업 표시줄의 가장 오른쪽에 있는 알림 영역의 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer** 를 강조 표시하고 **지금 블리치**를 누릅니다.
2. 블리치 작업이 시작되었음을 알리는 확인 메시지가 표시됩니다.

또는

1. Security Manager 왼쪽 창에서 **File Sanitizer** 를 확장하고 **블리치**를 누릅니다.
2. **지금 블리치**를 누릅니다.
3. 블리치 작업이 시작되었음을 알리는 확인 메시지가 표시됩니다.

파쇄 또는 여유 공간 블리치 작업 중단

파쇄 또는 여유 공간 블리치 작업이 진행 중이면 알림 영역의 HP ProtectTools Security Manager 아이콘 위에 메시지가 표시되어 파쇄 또는 여유 공간 블리치 작업에 관한 정보(완료율)와 작업을 중단할 수 있는 옵션을 제공합니다.

작업을 중단하려면 다음과 같이 하십시오.

▲ 메시지를 누른 다음 **중지**를 눌러 작업을 취소합니다.

로그 파일 보기

파쇄 또는 여유 공간 블리치 작업을 수행할 때마다, 발생한 오류에 대한 로그 파일이 만들어집니다. 이 로그 파일은 최근 수행된 파쇄 또는 여유 공간 블리치 작업에 따라 계속 업데이트됩니다.

참고: 파쇄되거나 블리치된 파일은 로그 파일에 기록되지 않습니다.

파쇄 작업과 여유 공간 블리치 작업을 수행하면 이 두 작업에 대한 로그 파일이 각각 만들어집니다. 이 로그 파일은 하드 드라이브의 다음 경로에 저장됩니다.

- C:\Program Files\Hewlett-Packard\File Sanitizer\[사용자 이름]_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer\[사용자 이름]_DiskBleachLog.txt

9 Device Access Manager for HP ProtectTools

이 보안 도구는 관리자만 사용할 수 있습니다. HP ProtectTools Device Access Manager 에는 사용자의 컴퓨터 시스템에 연결된 장치에 대한 무단 액세스를 차단하는 다음과 같은 보안 기능이 있습니다.

- 사용자별 장치 액세스 권한을 정의하는 장치 프로파일
- 그룹 구성원 자격을 기준으로 장치 액세스를 허용 또는 거부

참고: Device Access Manager 는 Windows 로컬 사용자와 그룹을 사용하여 액세스를 제어합니다. 따라서 로컬 사용자와 그룹을 지원하지 않는 Windows Home 버전에서는 Device Access Manager 가 올바르게 작동되지 않습니다. 그러나 사용자 설정에 DOS 명령을 사용하는 경우에는 Device Access Manager 가 Microsoft Windows Vista Home 버전에서 작동합니다. 자세한 내용은 Device Access Manager 도움말 파일을 참조하십시오.

백그라운드 서비스 시작

장치 프로필을 적용하려면 HP ProtectTools Device Locking/Auditing 백그라운드 서비스가 실행 중이어야 합니다. 장치 프로필을 처음 적용할 때는 HP ProtectTools Administrative Console 에서 백그라운드 서비스를 시작할 것인지 묻는 대화 상자가 열립니다. **예**를 누르면 백그라운드 서비스가 시작되고 시스템이 부팅될 때마다 서비스가 자동 시작되도록 설정됩니다.

기본 구성

초기화 과정에서 Device Access Manager 는 장치 관리자라고 하는 새 사용자 그룹을 만들어 관리자가 장치에 액세스하여 탐색할 수 있도록 합니다. 이 그룹에 Device Access Manager 단순 구성을 통해 컨트롤하는 장치에 대해 관리자 권한을 부여하려는 사용자를 추가합니다.

이 기능을 사용하여 다음 장치 클래스에 대해 액세스를 거부할 수 있습니다.

- 장치 관리자가 아닌 모든 사용자의 USB 장치
- 장치 관리자가 아닌 모든 사용자의 이동식 미디어(플로피 디스크, 개인용 뮤직 플레이어, 펜 드라이브 등)
- 장치 관리자가 아닌 모든 사용자의 DVD 및 CD-ROM 드라이브
- 장치 관리자가 아닌 모든 사용자의 직렬 및 병렬 포트

장치 관리자가 아닌 모든 사용자에 대해 장치 클래스별로 액세스를 거부하는 방법은 다음과 같습니다.

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **기본 구성**을 누릅니다.
3. 오른쪽 창에서 액세스를 거부할 장치의 확인란을 선택합니다.
4. **저장** 아이콘을 누릅니다.

   참고: 백그라운드 서비스가 실행되고 있지 않을 경우 지금 시작됩니다. **예**를 눌러 허용합니다.

5. **확인**을 누릅니다.

장치 클래스 구성(고급)

추가 설정을 사용하여 특정 사용자나 사용자 그룹에 대해 장치 액세스를 허용하거나 거부할 수 있습니다.

사용자 또는 그룹 추가

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 확장한 다음 **장치 클래스 구성**을 누릅니다.
3. 장치 목록에서 구성할 장치 클래스를 누릅니다.
4. **추가**를 누릅니다. **사용자 또는 그룹 선택** 대화 상자가 열립니다.
5. **고급**을 누른 다음 **지금 찾기**를 눌러 사용자나 그룹을 찾아 추가합니다.
6. 사용 가능한 사용자 및 그룹 목록에 추가할 사용자 또는 그룹을 선택한 다음 **확인**을 누릅니다.
7. **확인**을 누릅니다.

사용자 또는 그룹 제거

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 확장한 다음 **장치 클래스 구성**을 누릅니다.
3. 장치 목록에서 구성할 장치 클래스를 누릅니다.
4. 제거할 사용자나 그룹을 누른 다음 **제거**를 누릅니다.

사용자나 그룹에 대한 액세스 거부 또는 허용

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 확장한 다음 **장치 클래스 구성**을 누릅니다.
3. 장치 목록에서 구성할 장치 클래스를 누릅니다.
4. **사용자/그룹**에서 액세스를 거부할 사용자나 그룹을 누릅니다.

5. 액세스를 거부할 사용자 또는 그룹 옆에 있는 **거부**를 누릅니다.
6. **저장** 아이콘을 누른 다음 **확인**을 누릅니다.

사용자 액세스 설정(고급)

관리자는 사용자 액세스 설정에서 단순 구성 및 장치 클래스 구성 보기를 사용할 수 있는 사용자 및 그룹을 지정할 수 있습니다.

단순 구성 및 장치 클래스 구성 정보를 보려면 사용자나 그룹에 **구성 설정 보기(읽기 전용)** 액세스 권한이 부여되어야 합니다.

단순 구성 및 장치 클래스 구성 정보를 변경하려면 사용자나 그룹에 **구성 설정 변경** 액세스 권한이 부여되어야 합니다.

단순 구성 및 장치 클래스 구성 보기의 설정을 수정하려면 사용자나 그룹에 **완전한 사용자 관리자 권한** 액세스 권한이 부여되어야 합니다.

사용자 또는 그룹 추가

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 확장한 다음 **사용자 액세스 설정**을 누릅니다.
3. **추가**를 누릅니다. **사용자 또는 그룹 선택** 대화 상자가 열립니다.
4. **고급**을 누른 다음 **지금 찾기**를 눌러 추가할 사용자나 그룹을 검색합니다.
5. 사용 가능한 사용자 및 그룹 목록에 추가할 사용자나 그룹을 누른 다음 **확인**을 누릅니다.
6. **확인**을 누릅니다.
7. **저장** 아이콘을 누릅니다.

사용자 또는 그룹 제거

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 확장한 다음 **사용자 액세스 설정**을 누릅니다.
3. 제거하려는 사용자나 그룹을 누른 다음 **제거**를 누릅니다.
4. **저장** 아이콘을 누릅니다.

권한 허용 또는 거부

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Administrative Console** 을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 확장한 다음 **사용자 액세스 설정**을 누릅니다.
3. **그룹 또는 사용자 이름** 상자에서 사용자나 그룹 이름을 선택합니다.
4. **권한** 상자에서 해당 권한에 대해 **허용** 또는 **거부** 확인란을 선택합니다.
5. **저장** 아이콘을 누릅니다.

용어

Automatic Technology Manager(ATM).
네트워크 관리자가 BIOS 수준에서 시스템을 원격으로 관리할 수 있도록 하는 기능입니다.

Windows 관리자.
권한을 수정하고 다른 사용자를 관리할 수 있는 전체 권한을 가진 사용자를 의미함

Windows 사용자 계정.
네트워크나 개별 컴퓨터에 로그온하도록 승인된 개인 프로필

관리자.
Windows 관리자 참조

기본 삭제.
파일, 기록 또는 웹 관련 내용, 기타 기밀 데이터 등의 중요한 정보를 안전하게 삭제하는 방법

네트워크 계정.
로컬 컴퓨터, 작업 그룹 또는 도메인에 있는 Windows 사용자나 관리자 계정

도메인.
네트워크에 속하고 공용 디렉토리 데이터베이스를 공유하는 컴퓨터의 그룹 도메인의 이름은 고유하며, 각 도메인에는 일련의 공통 규칙과 절차가 있음

보안 로그온 방법.
컴퓨터에 로그인할 때 사용하는 방법

블리치.
여유 공간 블리치를 참조하십시오.

수동 파쇄.
자동 파쇄 예약에서 건너뛴 단일 자산 또는 선택한 자산을 즉시 파쇄할 수 있습니다.

여유 공간 블리치.
삭제된 파일의 내용을 왜곡하여 데이터 복구를 더욱 어렵게 만들기 위해 하드 드라이브의 삭제된 파일 위에 임의의 데이터를 덮어쓰는 보안 작업

인증.
사용자에게 컴퓨터 액세스, 특정 프로그램에 대한 설정 수정, 보안 데이터 확인 등과 같은 작업을 수행할 권한이 있는지 확인하는 과정

인증 정보.
인증 프로세스에서 사용자 이름 및 암호 등으로 특정 작업을 수행할 수 있는 자격이 있는지 증명하는 방법

자동 파쇄.
HP ProtectTools File Sanitizer 에서 사용자가 설정할 수 있는 예약 파쇄입니다.

자산.
개인 정보 또는 파일, 기록 및 웹 관련 데이터 등으로 이루어진 데이터 구성 요소로 하드 드라이브에 있습니다.

재부팅.
컴퓨터를 재시작하는 과정

키 시퀀스.
특정 키의 조합으로, 이를 누르면 자동 파쇄가 시작됩니다(예: Ctrl+Alt+S).

파쇄.
자산이 있는 데이터를 손상시키는 알고리즘을 실행하는 것을 말합니다.

파쇄 주기.
각 자산에 대한 파쇄 알고리즘 실행 횟수입니다. 선택한 파쇄 주기를 늘릴수록 컴퓨터의 보안이 강화됩니다.

파쇄 프로필.
지정된 삭제 방법 및 자산 목록입니다.

파워온 인증.
컴퓨터를 켤 때의 입력해야 하는 암호와 같이 특정 형식의 인증이 필요한 보안 기능

색인