HP ProtectTools
사용 설명서

초판: 2009 년 11 월

문서 부품 번호: 593308-AD1

목차

1 보안 소개

HP ProtectTools Security Manager 소프트웨어는 컴퓨터, 네트워크 및 중요 데이터에 대한 무단 액세스를 차단하는 보안 기능을 제공합니다. HP ProtectTools Security Manager 의 관리 권한은 관리 콘솔 기능을 통해 부여됩니다.

HP ProtectTools 관리 콘솔을 사용하여 로컬 관리자가 수행할 수 있는 작업은 다음과 같습니다.

- 보안 기능 활성화 또는 비활성화
- 로컬 관리자의 지문 및 이 컴퓨터의 다른 사용자의 지문 등록
- 얼굴 인식용 하나 이상의 사진 등록
- 인식용 스마트 카드 설정
- 인식을 위해 필요한 자격 증명 지정
- 컴퓨터 사용자 관리
- 장치 특정 매개변수 조정
- 설치된 Security Manager 응용 프로그램 구성
- 추가 Security Manager 응용 프로그램 추가

Security Manager 대시보드를 사용하여 일반 사용자가 수행할 수 있는 작업은 다음과 같습니다.

- 관리자가 제공한 옵션 구성
- 일부 HP ProtectTools 모듈의 제한된 컨트롤 허용

컴퓨터에서 사용할 수 있는 소프트웨어 모듈은 모델에 따라 다릅니다.

HP ProtectTools 소프트웨어 모듈은 미리 설치 또는 로드되거나, HP 웹 사이트에서 다운로드하여 사용할 수 있습니다. 자세한 내용은 http://www.hp.com 을 참조하십시오.

주: 본 설명서에서 제공하는 지침은 사용자의 컴퓨터에 해당 HP ProtectTools 소프트웨어 모듈이 설치되었다는 가정하에 작성되었습니다.

HP ProtectTools 기능

다음 표에는 HP ProtecTools 모듈의 주요 기능이 기재되어 있습니다.

모듈	주요 기능
HP ProtectTools Security Manager 관리 콘솔(관리자용)	• Security Manager 설치 마법사를 사용하여 보안 수준 및 보안 로그온 방법을 설정 및 구성합니다. • 기본 사용자에게는 표시되지 않는 옵션을 구성합니다. • Device Access Manager 구성 및 사용자 액세스를 구성합니다. • 관리자 도구를 사용하여 HP ProtectTools 사용자를 추가 및 제거하고 사용자 상태를 확인합니다.
HP ProtectTools Security Manager(일반 사용자용)	• 사용자 이름 및 암호를 구성, 설정 및 변경합니다. • Windows 암호 및 스마트 카드와 같은 사용자의 인증 정보를 구성하고 변경합니다. • File Sanitizer Shred, 블리치 및 설정을 구성하고 변경합니다. • Device Access Manager 에 대한 설정을 확인합니다. • 기본 설정, 백업 및 복구 옵션을 구성합니다.
HP ProtectTools 의 Credential Manager(Password Manager)	• 사용자의 이름과 암호를 저장, 구성 및 보호합니다. • 빠르고 안전한 액세스를 위해 웹 사이트 및 프로그램의 로그온 화면을 설정합니다. • 암호 관리자에 웹 사이트 사용자 이름과 암호를 입력하여 저장합니다. 다음번에 이 사이트를 다시 방문하면 암호 관리자가 이 정보를 자동으로 입력하고 제출합니다. • 더욱 높은 계정 보안을 위해 강력한 암호를 만듭니다. 암호 관리자가 이 정보를 자동으로 입력하고 제출합니다.
HP ProtectTools Drive Encryption (일부 모델만 해당)	• 완전한 전체 용량 하드 드라이브 암호화를 제공합니다. • 데이터의 암호를 해독하고 액세스하기 위해 부팅 전 인증을 강제 실행합니다.
HP ProtectTools Privacy Manager (일부 모델만 해당)	• 고급 로그온 기법을 사용하여 이메일, Microsoft® Office 문서, IM (Instant Messaging) 통신의 보안과 소스, 무결성을 검증합니다.
HP ProtectTools File Sanitizer	• 컴퓨터의 디지털 자산(응용프로그램 파일, 기록 내용 또는 웹 관련 내용, 다른 기밀 데이터를 포함한 중요한 정보)을 안전하게 파쇄하고 하드 드라이브를 정기적으로 블리치할 수 있습니다.
HP ProtectTools Device Access Manager (일부 모델만 해당)	• IT 관리자가 사용자 프로파일을 기반으로 장치 액세스를 제어하도록 합니다. • 허가받지 않은 사용자가 외부 저장 장치를 사용하여 데이터를 제거하거나 시스템에 바이러스를 퍼뜨리는 것을 방지합니다. • 관리자가 특정 개인 또는 사용자 그룹의 쓰기 가능한 장치에 대한 액세스를 비활성화할 수 있습니다.

주요 보안 목표 달성

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

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

도난 방지

도난의 예로는 공항 보안 검사 장소에서 기밀 데이터나 고객 정보를 포함하고 있는 컴퓨터를 도난 당하는 경우가 있습니다. 다음 기능은 이러한 도난으로부터 시스템을 보호하는 데 매우 유용합니다.

- 부팅 전 인증 기능을 활성화하면 운영체제에 대한 액세스 차단에 도움이 됩니다. 다음 절차를 참조하십시오.
  - Security Manager
  - Drive Encryption

중요한 데이터의 액세스 제한

감사자가 현장에서 작업하면서 컴퓨터에서 기밀 재무 정보를 확인할 수 있도록 허가 받은 경우, 여러분은 이 감사자가 파일을 인쇄하거나 CD 와 같은 쓰기 가능한 장치에 저장하기를 원하지 않을 것입니다. 다음 기능은 데이터 액세스를 제한하는 데 도움이 됩니다.

- HP ProtectTools Device Access Manager 를 사용하면 IT 관리자가 쓰기 가능한 장치에 액세스하는 것을 제한해 기밀 정보를 인쇄하거나 하드 드라이브에서 탈착식 미디어로 복사하는 것을 금할 수 있습니다.

내부 또는 외부에서 들어오는 무단 액세스 차단

안전하지 않은 업무용 PC 에 무단 액세스하면 경리부, 임원, 연구개발팀의 정보와 같은 기업 네트워크 리소스 그리고 환자 기록이나 개인 금융 기록과 같은 개인 정보에 매우 심각한 위험을 초래할 수 있습니다. 다음과 같은 기능이 무단 액세스를 방지하는 데 도움이 됩니다.

- 부팅 전 인증 기능을 활성화하면 운영체제에 대한 액세스 차단에 도움이 됩니다. 다음 절차를 참조하십시오.
  - Password Manager
  - Drive Encryption
- Password Manager 는 무단 사용자가 암호를 구하거나 암호로 보호된 응용프로그램에 액세스하는 것을 방지하는 데 효과적입니다.
- HP ProtectTools Device Access Manager 를 사용하면 IT 관리자가 쓰기 가능한 장치에 액세스하는 것을 제한해 하드 드라이브에서 기밀 정보를 인쇄하지 못하도록 할 수 있습니다.

- File Sanitizer 를 통해 중요 파일 및 폴더를 파쇄하거나 하드 드라이브를 블리치하여 안전하게 데이터를 삭제할 수 있습니다(삭제되었지만 복구 가능한 데이터에 덮어쓰기).
- DriveLock 은 하드 드라이브를 분리해 안전하지 않은 시스템에 설치하더라도 데이터에 액세스하지 못하도록 하는 데 효과적입니다.

강력한 암호 정책 생성

수 많은 웹 기반 응용프로그램과 데이터베이스에 대해 강력한 암호 정책을 시행할 것을 의무화할 경우, Security Manager 가 암호 및 SSO 편의를 위해 안전한 저장소 역할을 합니다.

추가 보안 요소

보안 역할 할당

컴퓨터 보안(특히 대규모 조직의 경우)을 관리할 때는 책임과 권한을 여러 관리자와 사용자에게 분배하는 과정이 중요합니다.

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

HP ProtectTools 에서는 보안 책임과 권한이 다음과 같은 역할로 구분됩니다.

- 보안 관리자—회사나 네트워크의 보안 수준을 정의하고, Java™ 카드, 생체 인식기, USB 토큰 등 배치할 보안 기능을 결정합니다.

  주: HP ProtectTools 의 많은 기능은 HP 와의 협력을 통해 보안 담당자가 사용자 정의할 수 있습니다. 자세한 내용은 HP 웹 사이트 http://www.hp.com 을 참고하십시오.

- 관리자—보안 담당자가 정의한 보안 기능을 적용 및 관리합니다. 또한 일부 기능을 활성화 및 비활성화할 수 있습니다. 예를 들어, 보안 담당자가 Java 카드를 배포하기로 결정한 경우, IT 관리자는 Java 카드 BIOS 보안 모드를 활성화할 수 있습니다.

- 사용자—보안 기능을 사용합니다. 예를 들어, 보안 관리자와 IT 관리자가 시스템에 대해 Java Card 를 활성화하면, 사용자는 Java Card PIN 을 설정하고 인증에 그 카드를 사용할 수 있습니다.

△ 주의: 관리자는 "모범 규준"에 따라 최종 사용자 권한과 사용자 액세스를 제한해야 합니다.

무단 사용자에게는 관리 권한을 부여하지 말아야 합니다.

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.

IT 관리자만이 설정하고 사용하는 암호는 별도로 구분하여 표시합니다. 기타 모든 암호는 정식 사용자나 관리자가 설정할 수 있습니다.

HP ProtectTools 암호	아래 모듈에서 설정	기능
Windows 로그온 암호	Windows® 제어판 또는 HP ProtectTools Security Manager	다양한 Security Manager 기능에 액세스하기 위해 수동 로그온 및 인증 정보가 사용될 수 있습니다.
Security Manager 백업 및 복구 암호	Security Manager, 개별 사용자	Security Manager 백업 및 복구 파일에 무단으로 액세스하지 못하도록 합니다.
Java™ 카드 PIN	Java Card Security	Java Card 내용에 무단으로 액세스하지 못하도록 하고 Java Card 사용자를 인증합니다. Java Card PIN 을 파워온 인증에 사용하면 Computer Setup 유틸리티와 컴퓨터 내용에 대한 무단 액세스를 방지할 수 있습니다. Java Card 토큰을 선택한 경우, Drive Encryption 모듈의 사용자를 인증합니다.

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.

HP ProtectTools 인증 정보 백업 및 복원

HP ProtectTools 의 백업 및 복구 기능을 사용하여 HP ProtectTools 인증 데이터 및 설정을 선택하고 백업할 수 있습니다.

2 설치 마법사 시작하기

HP ProtectTools 설치 마법사는 Security Manager 에서 가장 일반적으로 사용하는 기능을 설치하는 과정을 안내해 줍니다. 하지만 HP ProtecTools 관리 콘솔에는 그 밖에도 사용할 수 있는 기능이 많이 있습니다. Windows 시작 메뉴를 통해 액세스할 수 있는 콘솔에서 추가 보안 기능과 더불어 이 마법사에서 볼 수 있는 설정을 구성할 수 있습니다. 이 설정은 해당 컴퓨터와 이 컴퓨터를 공유하는 모든 사용자에게 적용됩니다.

1. 컴퓨터를 설치한 후 1 주일 정도 있다가 로그온할 때 또는 관리 권한이 있는 사용자가 처음으로 지문 인식기에 손가락을 갖다 댄 경우, Security Manager 설치 마법사가 자동으로 실행되어 기본적인 프로그램 구성 절차를 안내해 줍니다. 컴퓨터를 설정하는 것에 대한 동영상 튜토리얼이 자동으로 시작됩니다.

   또는

   Windows 사이드바의 **가젯** 아이콘 또는 작업 표시줄 오른쪽 끝의 알림 영역에 있는 작업 표시줄 아이콘을 통해서 HP ProtectTools Security Manager 를 열 수 있습니다.

   

   가젯 아이콘의 상단 표시줄 색을 통해 다음 상태 중 하나를 표시합니다.

   - 빨간색—HP ProtectTools 가 설치되지 않았거나 ProtectTools 모듈 중 하나에 오류가 발생했습니다.
   - 노란색—Security Manager 의 응용프로그램 상태 페이지에서 수행해야 하는 설정 변경을 확인하십시오.
   - 파란색—HP ProtectTools 이 설치되었고 올바르게 작동하고 있습니다.

   주: Windows XP 에서는 가젯 아이콘을 사용할 수 없습니다.

   또는

   시작을 누르고 **모든 프로그램**을 누른 다음 **HP ProtectTools 관리 콘솔**을 누릅니다.

2. 시작 화면을 읽고 **다음**을 누릅니다.

   주: 시작 화면에서 하나의 옵션을 선택하여 마법사의 추가 표시를 비활성화할 수 있습니다.

3. 설치 마법사에서 ID 확인을 요청할 것입니다.

   Windows 암호를 입력하거나 지문 인식기에 손가락을 댄 후 **다음**을 누릅니다.

   지문 인식기나 스마트 카드를 이용할 수 없는 경우에는 Windows 암호 입력 창이 나타납니다. 향후에 인증이 필요할 때에는 반드시 이 암호를 사용해야 합니다.

   아직 Windows 암호를 만들지 않은 경우, 암호를 만들기 위한 창이 나타납니다. 허가 받지 않은 사람이 액세스하지 못하도록 Windows 를 보호하고 HP ProtectTools Security Manager 기능을 사용하기 위해 Windows 암호가 필요합니다.

4. 이 설치 마법사는 이 컴퓨터의 모든 사용자에게 적용되는 보안 기능을 설정하는 절차를 안내해 줄 것입니다.

   - Windows 로그온 보안은 특정 인증 정보를 사용해야만 액세스를 허용하도록 하여 Windows 계정을 보호합니다.
   - Drive Encryption 이 하드 드라이브를 암호화해 데이터를 보호하므로 권한이 없는 사람들은 정보를 확인할 수 없습니다.
   - Pre-Boot Security 는 Windows 를 시작하기 전에 권한이 없는 사람들이 액세스하지 못하도록 하여 컴퓨터를 보호합니다.

   주: Pre-Boot Security 는 컴퓨터 BIOS 에서 지원하지 않는 경우 사용할 수 없습니다.

   보안 기능을 활성화하려면 확인란을 선택하십시오. 기능을 많이 선택할수록 컴퓨터의 보안이 더욱 강화됩니다.

5. 마법사의 마지막 페이지에서 **마침**을 누릅니다.

   Security Manager 대시보드가 표시됩니다.

주: 마법사를 완료하지 않은 경우 자동으로 두 번 이상 실행됩니다. 실행된 후, 작업 표시줄의 오른쪽 끝에 있는 알림 영역에 나타나는 알림 풍선을 통해서 설치가 완료될 때까지 마법사에 액세스할 수 있습니다(비활성화하지 않은 경우).

3 HP ProtectTools Security Manager 관리 콘솔

HP ProtectTools Security Manager 의 관리 권한은 관리 콘솔을 통해 부여됩니다.

주: HP ProtectTools 관리에는 관리자 권한이 필요합니다.

이 콘솔에서 제공하는 기능은 다음과 같습니다.

- 보안 기능 활성화 또는 비활성화
- 컴퓨터 사용자 관리
- 장치 특정 매개변수 조정
- Security Manager 응용프로그램 구성
- 추가 Security Manager 응용프로그램 추가

▲ HP ProtectTools Security Manager 응용프로그램을 사용하려면 시작 메뉴에서 HP ProtectTools Security Manager 를 시작하거나 작업 표시줄 오른쪽 끝의 알림 영역에서 Security Manager 아이콘을 마우스 오른쪽 버튼으로 누릅니다.

HP ProtectTools 관리 콘솔 및 이 응용프로그램은 이 컴퓨터를 공유하는 모든 사용자가 사용할 수 있습니다.

관리 콘솔 열기

시스템 정책 설정 또는 소프트웨어 구성과 같은 관리 작업을 수행하려면 다음과 같이 콘솔을 엽니다.

- **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools 관리 콘솔**을 누릅니다.

  또는

  Security Manager 대시보드의 왼쪽 패널에서 **관리**를 누릅니다.

지문 등록이나 Security Manager 사용 등 사용자 작업을 수행하려면 다음과 같이 콘솔을 엽니다.

- **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.

  또는

  작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools Security Manager** 아이콘을 두 번 누릅니다.

관리 콘솔 사용

Security Manager 관리 콘솔은 HP ProtectTools Security Manager 관리의 중심 위치입니다.

이 콘솔의 구성 요소는 다음과 같습니다.

- **도구**—컴퓨터의 보안을 구성하는 데 필요한 다음의 범주를 표시합니다.
  - **홈**—보안 작업을 선택하여 수행할 수 있습니다.
  - **시스템**—사용자와 장치에 대한 보안 기능 및 인증을 구성할 수 있습니다.
  - **응용프로그램**—HP ProtectTools Security Manager 및 Security Manager 응용프로그램의 일반 설정을 볼 수 있습니다.
  - **데이터**—데이터를 보호해 주는 Security Manager 응용프로그램 링크의 확장 메뉴를 제공합니다.
- **관리 도구**—추가 도구에 대한 정보를 제공합니다. 이 패널은 다음 선택 사항을 표시합니다.
  - **HP ProtectTools Security Manager 설치 마법사**—HP ProtectTools Security Manager 설치 과정을 안내해줍니다.
  - **도움말**—도움말 파일을 열어 Security Manager 및 사전 설치된 응용프로그램에 대한 정보를 볼 수 있습니다. 응용프로그램 안에서는 도움말을 추가할 수도 있습니다.
  - **정보**—버전 번호 및 저작권 공지 같은 HP ProtectTools Security Manager 관련 정보를 표시합니다.
- **Main area(메인 영역)**—응용프로그램별 화면을 표시합니다.

4 시스템 구성

시스템 그룹은 HP ProtectTools 관리 콘솔 화면의 왼쪽에 있는 도구 메뉴 패널에서 액세스할 수 있습니다. 이 그룹의 응용프로그램을 사용하여 컴퓨터, 사용자 및 장치에 대한 정책과 설정을 관리할 수 있습니다.

시스템 그룹에는 다음 응용프로그램이 포함되어 있습니다.

- **보안**—사용자가 이 컴퓨터와 상호 작용하는 방법을 관리하는 기능, 인증 및 설정을 관리합니다.
- **사용자**—이 컴퓨터의 사용자를 설정, 관리 및 등록합니다.
- **장치**—컴퓨터에 내장되거나 연결된 보안 장치의 설정을 관리합니다.

컴퓨터에 대한 인증 설정

인증 응용프로그램 내에서 이 컴퓨터에 구현할 보안 기능을 선택하고, 컴퓨터에 대한 액세스를 관리하는 정책을 설정하고, 추가 고급 설정을 구성할 수 있습니다. 사용자 세션 중 Windows 에 로그온하거나 웹 사이트와 프로그램에 로그온할 경우 사용자의 각 클래스를 인증하는 데 필요한 인증 정보를 지정할 수 있습니다.

컴퓨터에 대한 인증을 설정하려면 다음과 같이 하십시오.

1. 보안 패널 메뉴에서 **인증**을 누릅니다.
2. 로그온 인증을 구성하려면 **로그온 정책** 탭을 눌러 변경한 뒤 **적용**을 누릅니다.
3. 세션 인증을 구성하려면 **세션 정책** 탭을 눌러 변경한 뒤 **적용**을 누릅니다.

로그온 정책

Windows 에 로그온할 때 사용자를 인증하는 데 필요한 인증 정보를 관리하는 정책을 정의하려면 다음과 같이 하십시오.

1. 도구 메뉴에서 **보안**, **인증**을 차례로 누릅니다.
2. **로그온 정책** 탭에서 사용자 범주를 누릅니다.
3. 선택한 범주의 사용자에게 필요한 인증 정보를 지정합니다. 하나 이상의 인증 정보를 지정해야 합니다.
4. 사용자 인증을 위해 지정한 자격증명 중 어느 1 개만 있어도 되는지, 아니면 모두 있어야 하는지 선택합니다. 사용자가 컴퓨터에 액세스하는 것도 차단할 수 있습니다.
5. **적용**을 누릅니다.

세션 정책

Windows 세션 중 HP ProtectTools 응용프로그램에 액세스하는 데 필요한 인증 정보를 관리하는 정책을 정의하려면 다음과 같이 하십시오.

1. 도구 메뉴에서 **보안**, **인증**을 차례로 누릅니다.
2. **세션 정책** 탭에서 사용자 범주를 누릅니다.
3. 선택한 범주의 사용자에게 필요한 인증 정보를 지정합니다.
4. 사용자 인증을 위해 지정한 인증 정보 중 하나만 있어도 되는지, 아니면 모두 있어야 하는지 선택합니다. HP ProtectTools 에 액세스하는 데 인증을 요구하지 않을 수도 있습니다.
5. **적용**을 누릅니다.

설정

다음 보안 설정 중 하나 이상을 허용할 수 있습니다.

- **한 단계 로그온 허용**—BIOS 또는 암호화된 디스크 수준에서 인증을 수행한 경우 이 컴퓨터의 사용자가 Windows 로그온을 건너뛸 수 있습니다.
- **Windows 로그온에 HP SpareKey 인증 허용**—Security Manager 에서 다른 인증 정책이 필요한데도 이 컴퓨터의 모든 사용자가 HP SpareKey 기능을 사용하여 Windows 에 로그온할 수 있습니다.

설정을 편집하려면 다음과 같이 하십시오.

1. 활성화하거나 비활성화할 특정 설정을 누릅니다.
2. **적용**을 눌러 변경 사항을 저장합니다.

사용자 관리

사용자 응용프로그램 내에서 이 컴퓨터의 HP ProtectTools 사용자를 모니터링하고 관리할 수 있습니다.

Security Manager 를 통해 설정된 정책을 충족시킬 수 있는 적합한 인증 정보를 등록했는지 여부에 상관 없이 모든 HP ProtectTools 사용자가 나열되고 이러한 정책에 대해 확인됩니다.

사용자를 관리하려면 다음 설정에서 선택하십시오.

- 추가 사용자를 추가하려면 **Add(추가)**를 누릅니다.
- 사용자를 삭제하려면 지우려는 사용자를 누르고 난 다음 **Delete(삭제)**를 누릅니다.
- 지문을 등록하거나 사용자를 위해 추가 인증 정보를 설정하기 위해 사용자를 누른 다음 **Enroll(등록)**을 누릅니다.
- 특정 사용자에 대한 정책을 보려면 사용자를 선택하고 아래 창에서 정책을 봅니다.

장치 설정 지정

장치 응용프로그램 내에서 HP ProtectTools Security Manager 에서 인식할 수 있는 내장되거나 연결된 보안 장치에 사용할 수 있는 설정을 지정할 수 있습니다.

지문

지문 페이지에는 등록, 민감도 및 고급 탭이 있습니다.

등록

사용자가 등록할 수 있는 최소 및 최대 지문 수를 선택할 수 있습니다.

지문 인식기에서 모든 데이터를 지울 수도 있습니다.

△ 주의: 지문 인식기의 모든 데이터 정리는 관리자를 포함한 모든 사용자의 지문 정보를 삭제합니다. 로그온 정책이 지문만 필요한 경우 모든 사용자가 컴퓨터에 로그온하지 못할 수 있습니다.

민감도

지문을 스캔할 때 지문 인식기에 사용되는 민감도를 조정하려면 슬라이더를 이동하십시오.

지문을 일관되게 인식할 수 없을 경우 민감도 설정을 낮춰야 할 수도 있습니다. 민감도 설정을 높이면 지문 스캔 시 다양한 환경에 대한 민감도가 증가되어 잘못 수용할 가능성이 줄어듭니다. 중간-높음 설정은 보안과 편의성을 동시에 적절하게 제공합니다.

고급

컴퓨터가 배터리 전원으로 실행되는 동안 전원을 절약하도록 지문 인식기를 구성할 수 있습니다.

스마트 카드

스마트 카드를 제거하면 컴퓨터가 자동으로 잠기도록 구성할 수 있습니다. 하지만 컴퓨터는 Windows 에 로그인할 때 스마트 카드를 인증 정보로 사용할 경우에만 잠깁니다. Windows 에 로그인할 때 사용되지 않는 스마트 카드를 제거하면 컴퓨터가 잠기지 않습니다.

▲ 스마트 카드를 제거할 때 컴퓨터 잠금을 활성화하거나 비활성화하는 확인란을 선택합니다.

얼굴

컴퓨터의 사용 편의와 보안 결함의 어려움을 균형 잡기 위해 얼굴 인식용 보안 수준을 설정할 수 있습니다.

1. **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools Administrative Console(HP ProtectTools 관리 콘솔)**을 누릅니다.
2. **Devices(장치)**를 누른 다음 **Face(얼굴)**을 누릅니다.

3. 슬라이더를 눌러 왼쪽으로 이동하여 간편하게 하거나 오른쪽으로 이동하여 정확하게 합니다.

   - **Convenience(간편)**—등록된 사용자가 가장자리 위치에서 액세스하기 쉽게 하기 위해 슬라이더 바를 눌러 **Convenience(간편)** 위치로 이동합니다.
   - **Balance(균형)**—보안과 유용성간의 좋은 균형점을 제공하거나 민감한 정보 또는 허가받지 않은 로그온 시도가 발생할 수 있는 곳에 컴퓨터가 위치한 경우 슬라이더 바를 눌러 **Balance(균형)** 위치로 이동합니다.
   - **Accuracy(정확)**—등록된 사진 또는 현재 조명 조건이 잘못된 수용이 쉽게 발생할 수 있는 보통 이하인 경우 사용자가 액세스하기 어렵게 하려면 슬라이더 바를 눌러 **Accuracy(정확)** 위치로 이동합니다.

   주: 보안 수준은 모든 사용자에게 적용됩니다.

4. **Apply(적용)**를 누릅니다.

고급 설정

1. **시작**, **모든 프로그램**, **HP**를 차례로 누른 다음 **HP ProtectTools Administrative Console(HP ProtectTools 관리 콘솔)**을 누릅니다.
2. **Devices(장치)**를 누른 다음 **Face(얼굴)**을 누릅니다.
3. **Advanced(고급)**를 누릅니다.

   - **Windows 에 로그온하기 위해 사용자 이름이 필요하지는 않습니다.**
     - 사용자가 Windows 에 사용자 이름 없이 로그온할 수 있게 하기 위해 확인란을 선택합니다.
     - 로그온에 사용자 이름이 필요하게 하려면 확인란을 선택 해제합니다.
   - **얼굴 로그온용 PIN 사용 적용**—개별 사용자 설정에 필요한 확인란을 선택하고 로그온용 PIN(개인 식별 번호)을 사용합니다.
     - **PIN 허용 최소 길이**—위/아래 화살표를 눌러 PIN 에 필요한 최소 글자수를 증가시키거나 감소시킵니다.
     - **PIN 허용 최대 길이**—위/아래 화살표를 눌러 PIN 에 허용되는 최대 글자수를 증가시키거나 감소시킵니다.
     - **PIN 입력 시도 최대 횟수**—위/아래 화살표를 눌러 PIN 에 다시 입력할 수 있는 최대 횟수를 증가시키거나 감소시킵니다.

4. **확인**을 누릅니다.

5 응용프로그램 구성

응용프로그램 그룹은 HP ProtectTools 관리 콘솔의 왼쪽에 있는 보안 응용프로그램 메뉴 패널에서 액세스할 수 있습니다. 설정을 사용하면 현재 설치된 HP ProtectTools Security Manager 응용프로그램의 동작을 사용자 정의할 수 있습니다.

응용프로그램 설정을 편집하려면 다음과 같이 하십시오.

1. **응용프로그램** 그룹의 도구 메뉴에서 **설정**을 누릅니다.
2. 활성화하거나 비활성화할 특정 설정을 누릅니다.
3. **적용**을 눌러 변경 사항을 저장합니다.

일반 탭

일반 탭에서 사용할 수 있는 설정은 다음과 같습니다.

- **관리자용 설정 마법사를 자동으로 실행하지 않습니다.**—이 옵션을 선택하면 로그온 시 마법사가 자동으로 실행되는 것을 막을 수 있습니다.
- **사용자를 위해 시작 마법사를 자동으로 실행하지 않습니다.**—이 옵션을 선택하면 로그온 시 마법사가 자동으로 실행되는 것을 막을 수 있습니다.

응용프로그램 탭

여기에 표시된 설정은 Security Manager 에 새 응용프로그램이 추가되면 변경할 수 있습니다. 기본값으로 표시되는 최소 설정은 다음과 같습니다.

- **Applications status(응용 프로그램 상태)**—모든 응용 프로그램을 위해 상태가 표시되도록 활성화합니다.
- **Password Manager**—컴퓨터의 모든 사용자에 대해 Password Manager 응용프로그램을 활성화합니다.
- **Privacy Manager**—컴퓨터의 모든 사용자가 Privacy Manager 를 이용할 수 있도록 허용합니다.
- **추가 검색 버튼 활성화**—이 컴퓨터의 모든 사용자가 **[+] 추가 검색** 버튼을 눌러 HP ProtectTools Security Manager 에 응용프로그램을 추가할 수 있습니다.

모든 응용프로그램을 기본 설정으로 되돌리려면 **기본값 복원** 버튼을 누릅니다.

6 관리 도구

추가 응용프로그램을 Security Manager 에 새로운 관리 도구를 추가할 수 있는 추가 응용프로그램을 사용할 수 있습니다. 이 컴퓨터의 관리자는 설정 응용프로그램을 통해 이 기능을 비활성화할 수 있습니다.

추가 관리 도구를 추가하려면 **[+] 관리 도구**를 누릅니다.

업데이트 및 메시지

인터넷 연결을 이용할 수 있는 경우, 새로운 응용프로그램을 확인하거나 자동 업데이트 예약 설정을 위해 DigitalPersona 웹사이트(http://www.digitalpersona.com/)에 액세스할 수 있습니다.

1. 새로운 응용프로그램 및 업데이트에 대한 정보를 요청하려면 **새 응용 프로그램 및 업데이트 관련 정보를 수신합니다.** 확인란을 선택합니다.
2. 자동 업데이트 일정을 설정하려면 날짜 수를 선택합니다.
3. 업데이트를 확인하려면 **지금 확인**을 누릅니다.

7 HP ProtectTools Security Manager

HP ProtectTools Security Manager 에서는 컴퓨터 보안이 크게 강화됩니다.

미리 로드된 Security Manager 응용프로그램을 사용할 수 있고 추가 응용프로그램을 웹에서 즉시 다운로드할 수 있습니다.

- 로그온 및 암호 관리
- 쉽게 Windows® 운영체제 암호 변경
- 프로그램 기본 설정 구성
- 추가 보안과 편의를 위한 지문 사용
- 인증용 하나 이상의 사진 등록
- 인증용 스마트 카드 설정
- 프로그램 데이터 백업 및 복원
- 더 많은 응용프로그램 추가

HP ProtectTools Security Manager 열기

다음 중 한 방식으로 HP ProtectTools Security Manager 를 열 수 있습니다.

- **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.
- 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 누릅니다.
- **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **HP ProtectTools Security Manager 열기**를 누릅니다.
- Windows 사이드바에서 **Security Manager ID 카드** 가젯을 누릅니다.
- Ctrl+Windows+H 핫키 조합을 눌러 Security Manager Quick Links 메뉴를 엽니다.

Security Manager 대시보드 사용

Security Manager 대시보드는 Security Manager 기능, 응용프로그램, 설정에 간편하게 액세스할 수 있는 중앙 위치입니다.

▲ Security Manager 대시보드를 열려면 **시작**, **모든 프로그램**, **HP**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.

이 대시보드의 구성 요소는 다음과 같습니다.

- **ID 카드**—Windows 사용자 이름 및 로그온한 사용자 계정을 인식하는 지정 사진을 표시합니다.
- **보안 응용프로그램**—다음의 보안 범주를 구성하는 데 필요한 링크 확장 메뉴를 표시합니다.
  - **Credential Manager**
  - **내 데이터**
- **추가 검색**—ID, 데이터 및 통신의 보안을 강화하는 데 필요한 추가 응용프로그램을 찾을 수 있는 페이지를 엽니다.
- **Main area(메인 영역)**—응용프로그램별 화면을 표시합니다.
- **관리**—HP ProtectTools 관리 콘솔을 엽니다.
- **도움말 버튼**—현재 화면에 대한 정보를 표시합니다.
- **고급**—다음의 옵션에 액세스할 수 있습니다.
  - **기본 설정**—Security Manager 설정을 개인 설정할 수 있습니다.
  - **백업 및 복원**—데이터를 백업 및 복원할 수 있습니다.
  - **정보**—Security Manager 의 버전 정보를 표시합니다.

설정 절차

인증 정보 등록

My Identity(내 신원) 페이지에서 다양한 인증 방법이나 인증서를 등록할 수 있습니다. 등록한 후에는 해당 방법을 사용하여 Security Manager 에 로그온할 수 있습니다.

지문 등록

컴퓨터에 지문 인식기가 내장되어 있거나 연결되어 있다면, HP ProtectTools Security Manager 설치 마법사가 지문 설정(또는 "등록") 절차를 안내합니다.

1. 양손의 윤곽선이 표시됩니다. 이미 등록된 손가락은 녹색으로 표시됩니다. 윤곽선 위에 손가락을 놓고 누릅니다.

   주: 이전에 등록된 지문을 삭제하려면 삭제하려는 지문의 손가락을 누르십시오.

2. 등록하려는 손가락을 선택했을 때 지문이 성공적으로 등록될 때까지 손가락을 스캔하기 위한 프롬프트가 나타납니다. 등록된 손가락은 윤곽선이 녹색으로 강조 표시됩니다.

3. 최소 두 개의 손가락 이상을 등록해야 합니다. 검지 또는 중지로 등록하는 것이 좋습니다. 다른 손가락에 1~3 단계를 반복합니다.

4. **Next(다음)**를 누르고 화면의 지시를 따릅니다.

주: Getting Started(시작하기) 절차로 지문을 등록할 때 지문 정보는 **Next(다음)**를 누를 때까지 저장되지 않습니다. 잠시 컴퓨터를 작동하지 않은 채로 두거나 프로그램을 닫을 때 변경 사항은 저장되지 않습니다.

사진 등록

얼굴 로그온을 사용하기 위해 하나 이상의 사진을 등록해야 합니다.

HP ProtectTools Security Manager 설치 마법사에서 새로운 사진을 등록하려면 다음과 같이 하십시오.

1. 화면의 오른쪽 사이드바에 있는 **HP ProtectTools Security Manager** 아이콘을 누릅니다.

2. Windows® 암호를 입력한 후 **Next(다음)**를 누릅니다.

3. **Enable security features(보안 기능 작동)**아래에서 **Windows Logon Security(Windows 로그온 보안)** 확인란을 선택한 다음 **Next(다음)**를 누릅니다.

4. **Choose your credentials(인증 정보 선택)**아래에서 **Face(얼굴)** 확인란을 선택한 다음 **Next(다음)**를 누릅니다.

5. **새 사진 그룹 등록**을 누릅니다.

등록이 성공한 후 다음 조건들 중 하나 이상이 변경되어서 로그온에 어려움을 겪은 경우 새로운 사진을 등록할 수도 있습니다.

- 얼굴을 마지막으로 등록한 이후로 상당히 변한 경우
- 조명이 이전 등록과 상당히 다른 경우
- 지난 등록에 안경을 낀(또는 끼지 않은) 경우

주: 사진 등록이 잘되지 않으면 웹캠에 더 가까이 가십시오. 어느 종류의 사진 촬영이나 비디오 카메라 촬영과 마찬가지로 조명과 대비는 매우 중요합니다. 촬영 조명을 배경이 아닌 전경에 맞춰야 합니다. Face Recognition 에서 바로 사용자 인증이 되지 않으면 조명을 조절하여 사진 재등록을 시도할 수 있습니다.

HP ProtectTools Security Manager 에서 새로운 사진을 등록하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.
2. **Credentials(인증 정보)**를 누른 다음 **Face(얼굴)**를 누릅니다.
3. **새 사진 그룹 등록**을 누릅니다.

고급 사용자 설정

1. **시작**을 누르고 **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.
2. **인증 정보 설정**을 누른 다음 **얼굴**을 누릅니다.
3. **고급** 버튼을 누르고 다음 옵션을 선택합니다.
   a. 얼굴 로그온용 PIN 의 사용을 요구하려면 **PIN 만들기**를 누르고 Windows 암호를 입력한 다음 새로운 PIN 을 입력한 후 새 PIN 을 다시 입력하여 확인합니다.
   b. 필요에 따라 추가 설정을 선택합니다. 이 설정은 현재 사용자에게만 적용됩니다.
      - **얼굴 인식 이벤트 중에 소리 재생**
        - 얼굴 인식이 성공하거나 실패했을 때 소리를 재생하려면 확인란을 선택합니다.
        - 이 옵션을 비활성화하려면 확인란을 선택 해제합니다.
      - **로그온이 실패했을 때 사진을 업데이트하기 위한 창이 나타납니다.**
        - 얼굴 로그온이 실패했을 때 사용자가 사진을 업데이트할 수 있도록 확인란을 선택합니다. 확인이 "불확실"에 도달한 경우 사용자가 다음에 로그온의 성공 횟수를 늘리기 위해 현재 사진 그룹에 "실패"로 로그온된 실제 이미지의 삽입 여부를 결정하라는 메시지가 나타납니다.
        - 이 옵션을 비활성화하려면 확인란을 선택 해제합니다.
      - **로그온이 실패했을 때 새로운 사진을 등록하기 위해 프롬프트가 나타납니다.**
        - 얼굴 로그온이 실패하고 확인이 "불확실"까지 도달하지 못한 경우, 사용자가 새로운 사진을 등록하기 위한 프롬프트를 나타내기 위해 확인란을 선택합니다. 이것은 다음에 성공적인 로그온 기회를 높입니다.
        - 이 옵션을 비활성화하려면 확인란을 선택 해제합니다.
   c. 새 사진을 등록하려면 **새 사진 그룹 등록**을 누른 다음 화면 지침을 따르십시오.

Windows 암호 변경

Security Manager 에서 Windows 제어판보다 쉽고 빠르게 Windows 암호를 변경할 수 있습니다.

Windows 암호를 변경하려면 다음과 같이 하십시오.

1. Security Manager 대시보드에서 **Credentials(자격 인증)**을 누른 다음 **Password(암호)**를 누릅니다.
2. **현재 Windows 암호** 텍스트 상자에 현재 암호를 입력합니다.
3. **새 Windows 암호** 텍스트 상자에 새 암호를 입력하고 **새 암호 확인** 텍스트 상자에 다시 입력합니다.
4. **변경**을 눌러 현재 암호를 입력한 새 암호로 즉시 변경합니다.

스마트 카드 설정

스마트 카드 로그온을 선택했다면, 그리고 컴퓨터에 스마트 카드 리더기가 내장되어 있거나 이를 연결한 경우, Security Manager 설치 마법사가 스마트 카드 PIN(개인 식별 번호)을 설정하라고 요구할 것입니다.

스마트 카드 PIN 을 설정하려면 다음과 같이 하십시오.

1. **Set up smart card(스마트 카드 설정)**에서 PIN 을 입력하고 확인합니다.

   PIN 을 변경할 수도 있습니다. 현재 PIN 을 입력한 다음 새로운 PIN 을 입력합니다.

2. 계속하려면 **Next(다음)**를 누르고 화면의 지시를 따릅니다.

또는

▲ Security Manager 대시보드에서 **Credentials(자격 인증)**을 누른 다음 **Smart Card(스마트 카드)**를 누릅니다.

- 스마트 카드 PIN 을 설정하려면 **Set up smart card(스마트 카드 설정)** 아래에 PIN 을 입력하고 확인하십시오.
- PIN 을 변경하려면 먼저 현재 PIN 을 입력한 다음 새로운 PIN 을 입력하고 확인하십시오.

일반 작업

이 그룹에 포함된 응용프로그램으로 디지털 신원의 다양한 측면을 쉽게 관리할 수 있습니다.

- **Security Manager**—Quick Links 를 만들고 관리하기 때문에, Windows 암호, 지문 또는 스마트 카드로 인증을 받아 웹사이트나 프로그램을 실행해 로그온할 수 있습니다.
- **인증 정보**—편리하게 Windows 암호를 변경하거나 지문을 등록하거나 스마트 카드를 설정할 수 있습니다.

더 많은 응용프로그램을 추가하려면 대시보드 왼쪽 하단에서 **[+] 추가 검색** 버튼을 누르십시오. 이 버튼은 관리자에 의해 비활성화될 수 있습니다.

Password Manager

Windows, 웹 사이트 및 응용프로그램에 로그온하면 Password Manager 를 사용할 때 더욱 쉽고 안전하게 이용할 수 있습니다. Password Manager 를 사용하면 따로 적거나 기억할 필요 없는 보다 강력한 암호를 생성하고 지문, 스마트 카드 또는 Windows 암호로 쉽고 빠르게 로그온할 수 있습니다.

Password Manager 는 다음과 같은 옵션을 제공합니다.

- 관리 탭에서 로그온 추가, 편집 또는 삭제
- 설정된 후에 빠른 링크를 사용하여 기본 브라우저를 실행하고 웹 사이트나 프로그램에 로그온
- 끌어서 놓기 방식으로 빠른 링크를 범주로 구성
- 암호에 보안 위험이 있는지 여부를 파악하고 새 사이트에 사용할 복잡하고 강력한 암호를 자동으로 생성

웹 페이지 또는 프로그램 로그온 화면에서 표시되는 암호 관리자 아이콘을 통해 다양한 암호 관리자 기능을 이용할 수 있습니다. 이 아이콘을 누르면 다음 옵션 중에서 선택할 수 있는 컨텍스트 메뉴가 표시됩니다.

로그온이 아직 생성되지 않은 웹 페이지 또는 프로그램

다음 옵션이 컨텍스트 메뉴에 표시됩니다.

- **Password Manager 에 [somedomain.com] 추가**—현재 로그온 화면에 대한 로그온을 추가할 수 있습니다.
- **Password Manager 열기**—Password Manager 를 실행합니다.
- **아이콘 설정**—Password Manager 아이콘이 표시되는 조건을 지정할 수 있습니다.
- **도움말**—Password Manager 소프트웨어 도움말을 표시합니다.

로그온이 이미 생성된 웹 페이지 또는 프로그램

다음 옵션이 컨텍스트 메뉴에 표시됩니다.

- **로그온 데이터 채우기**—로그온 필드에 로그온 데이터를 기입하고 페이지를 제출합니다(로그온이 생성되거나 최근에 편집되었을 때 제출 작업이 지정된 경우).
- **로그온 편집**—이 웹 사이트에 대한 로그온 데이터를 편집할 수 있습니다.
- **새 계정 추가**—로그온에 계정을 추가할 수 있습니다.

- **Password Manager 열기**—Password Manager 응용프로그램을 실행합니다.
- **도움말**—Password Manager 소프트웨어 도움말을 표시합니다.

주: 이 컴퓨터의 관리자 설정에 따라 Security Manager 에서 사용자의 신원을 확인할 때 여러 개의 인증 정보를 요구할 수 있습니다.

로그온 추가

로그온 정보를 한 번 입력하여 웹 사이트 또는 프로그램에 대한 로그온을 쉽게 추가할 수 있습니다. 이후에는 암호 관리자에서 자동으로 이 정보를 입력해 줍니다. 웹 사이트 또는 프로그램을 이용한 후 이 로그온을 사용하거나, **로그온** 메뉴에서 로그온을 눌러 암호 관리자가 웹 사이트 또는 프로그램을 열고 로그온하도록 할 수 있습니다.

로그온을 추가하려면 다음과 같이 하십시오.

1. 웹 사이트나 프로그램에 대한 로그온 화면을 엽니다.
2. **Password Manager** 아이콘의 화살표를 누른 다음 로그온 화면이 웹 사이트용인지 프로그램용인지에 따라 다음 중 하나를 누릅니다.
   - 웹 사이트의 경우 **Password Manager 에 [domain name] 추가**를 누릅니다.
   - 프로그램의 경우 **Password Manager 에 이 로그온 화면 추가**를 누릅니다.
3. 로그온 데이터를 입력합니다. 화면의 로그온 필드와 대화 상자에서 해당되는 필드가 굵은 오렌지색 테두리로 식별됩니다. **Password Manager Manage(암호 관리자 관리)** 탭에서 **로그온 추가**를 눌러 이 대화 상자를 표시할 수 있습니다. 일부 옵션은 컴퓨터에 연결된 보안 장치에 따라(예를 들어, Ctrl+Windows+H 핫키를 사용하여 지문 스캔 또는 스마트 카드 삽입) 다릅니다.
   a. 미리 구성된 선택중 하나로 로그온 필드를 채우기 위해 필드 오른쪽으로 화살표를 누릅니다.
   b. 이 로그온을 위한 암호를 보려면 **Show password(암호 보기)**를 누릅니다.
   c. 제출하지 않고 로그온 필드를 채우려면 **Automatically submit logon data(로그온 데이터 자동 제출)** 확인란을 선택 해제합니다.
   d. **OK(확인)**을 누르고 **Fingerprints(지문)**, **Password(암호)** 또는 **Face(얼굴)** 중 사용하려는 인증 방법을 누른 다음 선택된 인증 방법으로 로그온합니다.

      플러스 기호가 Password Manager 아이콘에서 사라져 로그온이 만들어진 것을 알 수 있습니다.
   e. Password Manager 가 로그온 필드를 발견하지 못한 경우 **More fields(더 많은 필드)**를 누릅니다.
      i. 로그온에 필요한 개별 필드 확인란을 선택하거나 로그온에 필요 없는 필드를 선택 해제합니다.
      ii. Password Manager 가 모든 로그온 필드를 찾지 못한 경우 계속하기 원하는지 묻는 메시지가 나타납니다. **Yes(예)**를 누릅니다.
      iii. 로그온 필드가 채워진 채로 대화 상자가 나타납니다. 각 필드의 아이콘을 누르고 적당한 로그온 필드에 끌어온 다음 웹사이트에 등록하기 위해 버튼을 누릅니다.

      주: 사이트에 로그온 데이터 입력 수동 모드를 사용한 후 향후에 동일 웹 사이트에 로그온하기 위해 이 방법을 계속 사용해야 합니다.

주: 로그온 데이터 등록 수동 모드는 Internet Explorer 8 에서만 이용할 수 있습니다.

iv. **Close(닫기)**를 누릅니다.

웹사이트에 액세스하거나 프로그램을 열 때마다 로그온 하기 위해 등록된 인증 정보를 사용할 수 있다고 나타내는 Password Manager 아이콘이 나타납니다.

로그온 편집

로그온을 편집하려면 다음과 같이 하십시오.

1. 웹 사이트나 프로그램에 대한 로그온 화면을 엽니다.
2. 로그온 정보를 편집할 수 있는 대화 상자를 표시하려면 **Password Manager** 아이콘의 화살표를 누르고 **로그온 편집**을 누릅니다. 화면의 로그온 필드와 대화 상자의 해당 필드는 굵은 주황색 테두리로 식별됩니다.

   Password Manager 관리 탭에서 **원하는 로그온 편집**을 눌러 이 대화 상자를 표시할 수도 있습니다.
3. 로그온 정보를 편집합니다.
   - 로그온 필드를 미리 서식이 지정된 선택 사항 중 하나로 채우려면 필드 오른쪽에 있는 화살표를 누릅니다.
   - 추가 필드를 로그온 화면에서 추가하려면 **More fields(더 많은 필드)**를 클릭합니다.
   - 로그온 필드를 채웠지만 제출하지 않으려면 **로그온 데이터 제출** 확인란을 선택 해제합니다.
   - 이 로그온의 암호를 보려면 **암호 표시**를 누릅니다.
4. **확인**을 누릅니다.

로그온 메뉴 사용

Password Manager 에서는 쉽고 빠르게 로그온을 생성한 웹 사이트와 프로그램을 실행할 수 있습니다. **로그온** 메뉴 또는 **Password Manager** 의 **관리** 탭에서 프로그램이나 웹 사이트 로그온을 두 번 눌러 로그온 화면을 열고 로그온 데이터를 채웁니다.

로그온이 생성되면 Password Manager 로그온 메뉴에 자동으로 추가됩니다.

로그온 메뉴를 표시하려면 다음과 같이 하십시오.

1. **암호 관리자** 핫키 조합을 누릅니다. Ctrl+Windows+H 가 제조 시 기본 설정입니다. 핫 키 조합을 바꾸려면 **암호 관리자**를 누른 다음 **설정**을 누릅니다.
2. 컴퓨터에 내장되거나 연결된 지문 인식기를 사용하여 지문을 스캔합니다.

로그온을 범주로 구성

범주를 사용하여 로그온을 정리할 수 있습니다. 먼저 하나 이상의 범주를 생성하고, 원하는 범주로 로그온을 끌어다 놓습니다.

범주를 추가하려면 다음과 같이 하십시오.

1. Security Manager 대시보드에서 **Password Manager** 를 누릅니다.
2. **관리** 탭을 누른 다음 **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 길게 누릅니다.
3. 로그온을 범주 목록으로 끌어 옵니다. 범주 위로 마우스를 이동하면 범주가 강조 표시됩니다.
4. 원하는 범주가 강조 표시되면 마우스 버튼에서 손을 뗍니다.

로그온이 범주로 이동하는 것이 아니라 선택한 범주로 복사되는 것뿐입니다. 동일한 로그온을 여러 범주에 추가할 수 있고, **모두**를 누르면 로그온을 모두 표시할 수 있습니다.

로그온 관리

Password Manager 에서는 사용자 이름, 암호 및 다중 로그온 계정에 대한 로그온 정보를 중앙 위치에서 쉽게 관리할 수 있습니다.

사용자의 로그온은 관리 탭에 나열되어 있습니다. 동일한 웹 사이트에 대해 여러 로그온이 생성되면 각 로그온이 웹 사이트 이름 아래에 나열되고 로그온 목록에서 들여쓰기되어 있습니다.

로그온을 관리하려면 다음과 같이 하십시오.

Security Manager 대시보드에서 **Password Manager** 를 누르고 **관리** 탭을 누릅니다.

- **로그온 추가**—**로그온 추가**를 누르고 화면의 지시를 따릅니다.
- **로그온 편집**—로그온을 누르고 **편집**을 누른 다음 로그온 데이터를 변경합니다.
- **로그온 삭제**—로그온을 누르고 **삭제**를 누릅니다.

웹 사이트 또는 프로그램에 대해 추가 로그온을 추가하려면

1. 웹 사이트나 프로그램에 대한 로그온 화면을 엽니다.
2. **Password Manager** 아이콘을 눌러 바로 가기 메뉴를 표시합니다.
3. **Add additional logon(추가 로그온 추가)**을 누른 다음 화면의 지시에 따릅니다.

암호 수준 확인

웹 사이트와 프로그램의 로그온에 강력한 암호를 사용하는 것은 사용자의 신원 보호에 매우 중요한 요소입니다.

Password Manager 는 웹 사이트 및 프로그램에 로그온하는 데 사용된 각 암호의 강도를 즉석에서 자동으로 분석하여 손쉽게 보안을 감시하고 강화할 수 있습니다.

Password Manager 아이콘 설정

Password Manager 는 웹 사이트 및 프로그램에 대한 로그온 화면을 식별하려고 시도합니다. 이 과정에서 로그온을 생성하지 않은 로그온 화면이 감지되면 Password Manager 아이콘에 "+" 기호를 표시하여 화면에 대한 로그온을 추가할 것인지 묻습니다.

아이콘 화살표를 누른 다음 **아이콘 설정**을 눌러 **Password Manager** 에서 로그온 사이트를 관리하는 방법을 사용자 정의합니다.

- **로그온 화면에 로그온을 추가하라는 메시지 표시**—아직 로그온이 설정되지 않은 로그온 화면이 표시될 때 로그온을 추가할 것인지 물으려면 이 옵션을 누릅니다.
- **이 화면 제외**—확인란을 선택하면 암호 관리자가 이 로그온 화면에 대한 로그온 추가 메시지를 다시 표시하지 않습니다.

추가 Password Manager 설정에 액세스하려면 Security Manager 대시보드에서 **Password Manager**를 누르고 **설정**을 누릅니다.

설정

HP ProtectTools Security Manager 의 개인 설정을 지정할 수 있습니다.

1. **로그온 화면에 로그온을 추가하라는 메시지 표시**—웹 사이트나 프로그램 로그온 화면이 감지될 때마다 Password Manager 아이콘에 플러스(+) 기호가 표시되어 사용자가 이 화면의 로그온을 암호 저장소에 추가할 수 있음을 나타냅니다. 이 기능을 비활성화하려면 **아이콘 설정** 대화 상자에서 **로그온 화면에 로그온을 추가하라는 메시지 표시** 옆의 확인란을 선택 해제합니다.
2. **Open Password Manager with ctrl+Windows+h(다음을 사용하여 암호 관리자 열기 Ctrl +Windows+H)**—암호 관리자 빠른 링크 메뉴를 여는 기본 핫키는 Ctrl+Windows+H 입니다. 이 핫키를 변경하려면 이 옵션을 누르고 새로운 키 조합을 입력합니다. 키 조합은 다음 중 하나 이상을 포함할 수 있습니다. Ctrl, Alt, Shift, 알파벳 또는 숫자 키
3. **적용**을 눌러 변경 사항을 저장합니다.

인증 정보

Security Manager 인증 정보를 사용하여 사용자의 신원을 확인할 수 있습니다. 이 컴퓨터의 로컬 관리자는 사용자가 Windows 계정, 웹 사이트 또는 프로그램에 로그온할 때 신원을 입증하는 데 어떤 인증 정보를 사용할 지 설정할 수 있습니다.

사용 가능한 인증 정보는 이 컴퓨터에 내장되거나 연결되어 있는 보안 장치에 따라 다양합니다. 지원되는 각 인증 정보는 **내 신원, 인증 정보** 그룹 내에 항목으로 있게 됩니다.

사용 가능한 인증 정보, 요구 사항 및 현재 상태가 나열되며 다음을 포함할 수 있습니다.

- 지문
- 암호
- 스마트 카드
- 얼굴

인증 정보를 등록하거나 변경하려면 링크를 누르고 화면의 지시를 따릅니다.

개인 ID 카드

ID 카드는 이 Windows 계정의 소유자로 사용자를 고유하게 식별하여 사용자가 선택한 사용자 이름과 사진을 표시합니다. ID 카드는 Security Manager 페이지 왼쪽 상단에 Windows 사이드바 가젯으로 돌출되어 표시됩니다.

Security Manager 에 빠르게 액세스하는 방법 중 하나는 Windows 사이드바에서 ID 카드를 누르는 것입니다.

사진과 이름 표시 방식을 변경할 수 있습니다. 기본적으로 Windows 설치 중 선택한 전체 Windows 사용자 이름과 사진이 표시됩니다.

표시된 이름을 변경하려면 다음과 같이 하십시오.

1. Security Manager 대시보드에서 왼쪽 상단의 **ID 카드** 아이콘을 누릅니다.
2. Windows 계정에 입력한 이름이 표시된 확인란을 누릅니다. 시스템에서 이 계정에 대한 Windows 사용자 이름을 표시합니다.
3. 이름을 변경하려면 새 이름을 입력한 다음 **저장** 버튼을 누릅니다.

표시된 사진을 변경하려면 다음과 같이 하십시오.

1. Security Manager 대시보드에서 왼쪽 상단의 **ID 카드**를 누릅니다.
2. **사진 선택** 버튼을 누르고 이미지를 누른 다음 **저장** 버튼을 누릅니다.

기본 설정 지정

HP ProtectTools Security Manager 의 설정을 개인 설정할 수 있습니다. Security Manager 대시보드에서 **고급**을 누른 다음 **기본 설정**을 누릅니다. 사용 가능한 설정은 일반 및 지문 탭에 표시됩니다.

일반

일반 탭에서 사용할 수 있는 설정은 다음과 같습니다.

모양—작업 표시줄에 아이콘 표시

- 작업 표시줄에 아이콘을 표시할 수 있게 하려면 하려면 확인란을 선택합니다.
- 작업 표시줄에 아이콘을 표시하지 않으려면 확인란을 선택합니다.

지문

지문 탭에서 사용할 수 있는 설정은 다음과 같습니다.

- **빠른 작동**—빠른 작동을 사용하여 지문을 스캔하는 동안 지정된 키를 누르고 있으면 수행되는 Security Manager 작업을 선택합니다.

  나열된 키 중 하나에서 빠른 동작을 지정하려면 **(키) + Fingerprint(지문)** 옵션을 누른 다음 메뉴에서 이용할 수 있는 것 중 하나를 선택합니다.

- **지문 스캔 피드백**—지문 인식기를 이용할 수 있을 때만 나타납니다. 이 설정을 이용하여 지문을 스캔할 때 발생하는 피드백을 조정합니다.

  - **사운드 피드백 활성화**—Security Manager 는 지문이 스캔될 때 특정 프로그램 이벤트에 다른 소리를 재생하는 오디오 피드백을 제공합니다. Windows 제어판의 사운드 탭으로 이벤트에 새로운 소리를 지정하거나 이 옵션을 선택 해제하여 사운드 피드백을 비활성화할 수 있습니다.

  - **스캔 품질 피드백 표시**

    품질에 상관없이 모든 스캔을 표시하려면 확인란을 선택합니다.

    좋은 품질의 스캔을 표시하려면 확인란을 선택 해제합니다.

데이터 백업 및 복원

Security Manager 데이터를 정기적으로 백업하는 것이 좋습니다. 백업 빈도는 데이터 변경 주기에 따라 다릅니다. 예를 들어, 새 로그온을 매일 추가하는 경우 데이터를 일 단위로 백업해야 합니다.

백업은 컴퓨터 간의 마이그레이션에도 사용할 수 있으며 이를 가져오기/내보내기라고 합니다.

주: 이 기능으로는 데이터만 백업됩니다.

백업 파일에서 데이터를 복원하려면 백업된 데이터를 받을 컴퓨터에 HP ProtectTools Security Manager 를 설치해야 합니다.

데이터를 백업하려면 다음과 같이 하십시오.

1. 왼쪽 패널에서 **고급**을 누르고 **백업 및 복원**을 누릅니다.
2. **데이터 백업**을 누릅니다.
3. 함께 백업하려는 모듈을 선택합니다. 대부분의 경우 모두 선택하는 것이 좋습니다.
4. 저장 파일의 이름을 입력합니다. 파일은 기본적으로 문서 폴더에 저장됩니다. 다른 위치를 지정하려면 **찾아보기**를 누릅니다.
5. 파일을 보호하려면 암호를 입력합니다.
6. 사용자의 신원을 확인합니다.
7. **마침**을 누릅니다.

데이터를 복원하려면 다음과 같이 하십시오.

1. 왼쪽 패널에서 **고급**을 누르고 **백업 및 복원**을 누릅니다.
2. **데이터 복원**을 누릅니다.

3. 이전에 생성된 저장 파일을 선택합니다. 제공된 필드에 경로를 입력하거나 **찾아보기**를 누를 수 있습니다.
4. 파일 보호를 위해 사용한 암호를 입력합니다.
5. 복원하려는 데이터의 모듈을 선택합니다. 대부분의 경우 전체 모듈 목록이 이에 해당합니다.
6. **마침**을 누릅니다.

추가 검색

이 프로그램의 새로운 기능을 제공하는 추가 응용프로그램을 찾아볼 수 있습니다.

Security Manager 대시보드에서 **[+] 추가 검색**을 눌러 추가 응용프로그램을 찾아볼 수 있습니다.

주: 대시보드의 왼쪽 아래에 **[+] 추가 검색** 링크가 없다면 이 컴퓨터의 관리자가 비활성화한 것입니다.

업데이트 및 메시지

1. 새로운 응용프로그램 및 업데이트에 대한 정보를 요청하려면 **새 응용 프로그램 및 업데이트 관련 정보를 수신합니다.** 확인란을 선택합니다.
2. 자동 업데이트 일정을 설정하려면 날짜 수를 선택합니다.
3. 업데이트를 확인하려면 **지금 확인**을 누릅니다.

보안 응용프로그램 상태

Security Manager 응용 프로그램 상태 페이지는 설치된 보안 응용 프로그램의 전반적인 상태를 나타냅니다. 이 페이지는 응용 프로그램의 설치 및 설정 상태를 보여줍니다. Security Manager 대시보드를 열고 **Check the status of the security applications(보안 응용 프로그램 상태 확인)**을 눌렀을 때, **Security Applications(보안 응용 프로그램)**을 눌렀을 때 또는 화면 오른쪽의 Windows 사이드바의 **가젯** 아이콘에서 **Check Now(지금 확인)**를 눌렀을 때 요약이 자동으로 표시됩니다.

8 HP ProtectTools Drive Encryption(일부 모델만 해당)

△ **주의:** Drive Encryption 모듈을 제거하려면 우선 모든 암호화된 드라이브를 해제해야 합니다. 그렇지 않을 경우, Drive Encryption 복구 서비스에 등록하지 않는 한 암호화 된 드라이브에 들어있는 데이터에는 액세스할 수 없습니다. Drive Encryption 모듈을 다시 설치하면 그 전에 암호화한 드라이브에는 액세스할 수 없습니다.

HP ProtectTools Drive Encryption 은 컴퓨터 하드 드라이브를 암호화하여 데이터를 완벽하게 보호합니다. Drive Encryption 이 활성화되어 있는 경우 Drive Encryption 로그온 화면에서 로그온을 해야 Windows® 운영 체제가 시작됩니다.

HP ProtectTools 설치 마법사를 사용하여 Windows 관리자는 Drive Encryption 활성화, 암호화 키 백업, 사용자 추가 및 삭제, Drive Encryption 비활성화를 수행할 수 있습니다. 자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

Drive Encryption 에서 수행할 수 있는 작업은 다음과 같습니다.

- 암호화 관리

  개별 드라이브 암호화 또는 암호 해제

  주: 내장 하드 드라이브만 암호화할 수 있습니다.

- 복구
  - 백업 키 생성
  - 복구 수행

설치 절차

Drive Encryption 열기

1. **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools 관리 콘솔**을 누릅니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누릅니다.

일반 작업

Drive Encryption 활성화

HP ProtectTools 설치 마법사를 사용하여 Drive Encryption 을 활성화합니다.

주: 또한 이 마법사는 사용자를 추가하고 삭제하는 데 사용됩니다.

또는

1. **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools 관리 콘솔**을 누릅니다.
2. 왼쪽 창에서 **보안**을 누른 다음 **기능**을 누릅니다.
3. **Drive Encryption** 확인란을 선택한 다음 **다음**을 누릅니다.
4. **암호화할 드라이브** 아래에서 암호화하려는 하드 드라이브의 확인란을 선택합니다.
5. 해당 슬롯에 저장 장치를 넣습니다.

   주: 암호화 키를 저장하려면 FAT32 형식의 USB 저장 장치를 사용해야 합니다.

6. **암호화 키를 저장할 외부 저장 장치** 아래에서 암호화 키를 저장할 저장 장치의 확인란을 선택합니다.
7. **적용**을 누릅니다.

   드라이브 암호화가 시작됩니다.

자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

Drive Encryption 비활성화

HP ProtectTools 설치 마법사를 사용하여 Drive Encryption 을 비활성화합니다. 자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

또는

1. **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools 관리 콘솔**을 누릅니다.
2. 왼쪽 창에서 **보안**을 누른 다음 **기능**을 누릅니다.
3. **Drive Encryption** 확인란을 선택 해제한 다음 **적용**을 누릅니다.

   드라이브 암호화가 시작됩니다.

Drive Encryption 이 활성화된 후 로그인

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

주: Windows 관리자가 HP ProtectTools Security Manager 에서 Pre-boot Security(부팅 전 보안)를 활성화하면 Drive Encryption 로그온 화면에서 로그인하지 않아도 컴퓨터가 켜지면 즉시 로그인됩니다.

1. 사용자 이름을 선택한 다음 Windows 암호 또는 Java™ Card PIN 을 입력하거나 등록된 손가락을 인식시킵니다.
2. **확인**을 누릅니다.

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

하드 드라이브를 암호화하여 데이터 보호

HP ProtectTools 설치 마법사를 이용해 하드 드라이브를 암호화해 데이터를 보호하십시오.

1. Security Manager 에서 **시작**을 누른 다음 **Security Manager Setup** 아이콘을 누릅니다. Security Manager 기능을 설명하는 데모가 시작됩니다. Drive Encryption 페이지에서 Security Manager 를 시작할 수도 있습니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **암호화 관리**를 누릅니다.
3. **암호화 변경**을 누릅니다.
4. 암호화할 드라이브를 한 개 이상 선택합니다.

주: 하드 드라이브를 암호화하는 것이 좋습니다.

암호화 상태 확인

HP ProtectTools Security Manager 를 사용하여 암호화 상태를 확인할 수 있습니다.

주: 드라이브 암호화 상태는 HP ProtectTools 관리 콘솔을 사용하여 변경해야 합니다.

1. **HP ProtectTools Security Manager** 를 엽니다.
2. **내 데이터** 아래에서 **암호화 상태**를 누릅니다.

   Drive Encryption 이 활성화된 경우 드라이브 상태에는 다음 상태 코드 중 하나가 표시됩니다.

   - 활성
   - 비활성
   - 암호화되지 않음
   - 암호화됨
   - 암호화 중
   - 암호 해독 중

   하드 드라이브가 암호화 또는 암호 해독 중인 경우 진행 표시줄에는 진행률 및 암호화 또는 암호 해독이 완료될 때까지 남은 시간이 표시됩니다.

고급 작업

Drive Encryption 관리 (관리자 작업)

암호화 관리 페이지에서 관리자는 Drive Encryption 상태를 확인 및 변경(활성 또는 비활성)하거나 컴퓨터의 모든 하드 드라이브의 암호화 상태를 확인할 수 있습니다.

- 비활성 상태인 경우 Windows 관리자가 HP ProtectTools Security Manager 에서 Drive Encryption 을 활성화하지 않았으므로 하드 드라이브가 보호되지 않습니다. HP ProtectTools Security Manager 설치 마법사를 사용하여 Drive Encryption 을 활성화합니다.
- 활성 상태인 경우 Drive Encryption 은 활성화되고 구성되어 있는 상태입니다. 드라이브 상태는 다음 중 하나에 해당합니다.
  - 암호화되지 않음
  - 암호화됨
  - 암호화 중
  - 암호 해독 중

개별 드라이브 암호화 또는 암호 해제

컴퓨터의 다중 하드 드라이브를 암호화하거나 이미 암호화된 드라이브를 암호 해제하려는 경우 암호화 변경 기능을 사용할 수 있습니다.

1. **HP ProtectTools 관리 콘솔**을 열고 **Drive Encryption**, **암호화 관리**를 차례로 누릅니다.
2. **암호화 변경**을 누릅니다.
3. 암호화 변경 대화 상자에서 암호화하거나 암호 해제하려는 각 하드 드라이브 옆의 확인란을 선택 또는 선택 해제한 후 **확인**을 누릅니다.

주: 드라이브를 암호화 또는 암호 해제할 때 진행 표시줄에는 현재 세션에서 절차가 완료될 때까지 남은 시간이 표시됩니다. 암호화가 진행되는 동안 컴퓨터가 종료되거나 절전, 대기 모드 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)

복구 페이지에서 관리자는 암호화 키를 백업하거나 복구할 수 있습니다.

로컬 Drive Encryption 키 백업 — Drive Encryption 을 활성화한 다음 이동식 미디어에 암호화 키를 백업할 수 있습니다.

백업 키 생성

암호화된 드라이브의 암호화 키를 이동식 저장 장치에 백업할 수 있습니다.

△ 주의: 백업 키가 들어 있는 저장 장치를 안전한 곳에 보관해 두십시오. 암호를 잊어버리거나 Java Card 를 잃어버리면 이 장치를 통해서만 하드 드라이브에 액세스할 수 있습니다.

1. **HP ProtectTools 관리 콘솔**을 열고 **Drive Encryption**, **복구**를 차례로 누릅니다.
2. **키 백업**을 누릅니다.

3. 백업 디스크 선택 페이지에서 암호화 키를 백업할 장치의 확인란을 선택한 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 **마침**을 누릅니다.

복구 수행

암호가 기억나지 않는 경우 다음 방법을 사용하여 복구를 수행할 수 있습니다.

1. 컴퓨터의 전원을 켭니다.
2. 백업 키를 저장한 이동식 저장 장치를 넣습니다.
3. HP ProtectTools Drive Encryption 로그온 대화 상자가 열리면 **취소**를 누릅니다.
4. 화면 왼쪽 아래에 있는 **옵션**을 누른 다음 **복구**를 누릅니다.
5. 백업 키가 들어 있는 파일을 선택하거나 **찾아보기**를 눌러 파일을 검색한 다음 **다음**을 누릅니다.
6. 확인 대화 상자가 표시되면 **확인**을 누릅니다.

   컴퓨터가 시작됩니다.

주: 복구를 수행한 후 암호를 재설정하는 것이 좋습니다.

9 HP ProtectTools Privacy Manager (일부 모델만 해당)

이메일, Microsoft® Office 문서 또는 인스턴트 메시징(IM) 사용 시 HP ProtectTools 용 Privacy Manager 를 통해 고급 보안 로그온(인증) 방법을 사용하여 소스, 무결성 및 통신 보안을 확인할 수 있습니다.

Privacy Manager 는 HP ProtectTools Security Manager 에서 제공하며 다음과 같은 보안 로그온 방법으로 구성된 보안 인프라를 활용합니다.

- 지문 인증
- Windows® 암호
- HP ProtectTools Java™ Card

Privacy Manager 에서 위의 보안 로그온 방법 중 하나를 사용하면 됩니다.

Privacy Manager 에는 다음 사항이 필요합니다.

- HP ProtectTools Security Manager 5.00 이상
- Windows® 7, Windows Vista® 또는 Windows XP 운영 체제
- Microsoft Outlook 2007 또는 Microsoft Outlook 2003
- 유효한 전자 우편 계정

주: 보안 기능에 액세스하려면 먼저 Privacy Manager 인증서(디지털 인증서)를 요청하고 Privacy Manager 에 설치해야 합니다. Privacy Manager 인증서 요청에 대한 자세한 내용은 44페이지의 Privacy Manager 인증서 요청 및 설치를 참조하십시오.

설치 절차

Privacy Manager 열기

Privacy Manager 를 열려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.
2. **Privacy Manager** 를 누릅니다.

또는

작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **Privacy Manager**, **Configuration(구성)**을 차례로 누릅니다.

또는

Microsoft Outlook 전자 우편 메시지의 도구 모음에서 **Send Securely(안전하게 보내기)** 옆의 아래쪽 화살표를 누른 다음 **Certificates(인증서)** 또는 **Trusted Contacts(신뢰할 수 있는 연락처)**를 누릅니다.

또는

Microsoft Outlook 문서의 도구 모음에서 **Sign and Encrypt(등록 및 암호화)** 옆의 아래쪽 화살표를 누른 다음 **Certificates(인증서)** 또는 **Trusted Contacts(신뢰할 수 있는 연락처)**를 누릅니다.

Privacy Manager 인증서 관리

Privacy Manager 인증서는 PKI(공용 키 인프라)라는 암호화 기술을 사용하여 데이터와 메시지를 보호합니다. PKI 를 사용하려면 암호화 키와 CA(인증 기관)에서 발행한 Privacy Manager 인증서가 있어야 합니다. 정기적인 인증만을 요구하는 대부분의 데이터 암호화 및 인증 소프트웨어와는 달리, Privacy Manager 에서는 전자 우편 메시지 또는 암호화 키를 사용하는 Microsoft Office 문서에 서명할 때마다 인증 작업이 필요합니다. Privacy Manager 를 사용하면 중요한 정보를 저장하고 전송할 수 있는 과정이 보다 안전해집니다.

다음 작업을 수행할 수 있습니다.

- Privacy Manager 인증서 요청 및 설치
- Privacy Manager 인증서 세부 정보 보기
- Privacy Manager 인증서 갱신
- 사용 가능한 인증서가 여러 개일 경우 Privacy Manager 에서 사용할 기본 Privacy Manager 인증서 설정
- Privacy Manager 인증서 삭제 및 해지(고급)

Privacy Manager 인증서 요청 및 설치

Privacy Manager 기능을 사용하려면 먼저 유효한 전자 우편 주소를 사용하여 Privacy Manager 내에서 Privacy Manager 인증서를 요청하고 설치해야 합니다. Privacy Manager 인증서를 요청하고 있는 컴퓨터의 Microsoft Outlook 계정을 전자 우편 주소로 설정해야 합니다.

Privacy Manager 인증서 요청

1. Privacy Manager 를 열고 **인증서**를 누릅니다.
2. **Privacy Manager 인증서 요청**을 누릅니다.
3. 시작 페이지의 내용을 읽은 후 **다음**을 누릅니다.
4. 사용권 계약 페이지에서 사용권 계약을 읽습니다.
5. **여기를 눌러 사용권 계약 내용에 동의합니다** 옆의 확인란이 선택되었는지 확인하고 **다음**을 누릅니다.
6. 인증서 세부 정보 페이지에 필요한 정보를 입력한 후 **다음**을 누릅니다.
7. "인증서 요청 동의함" 페이지에서 **마침**을 누릅니다.
8. **확인**을 눌러 인증서를 닫습니다.

Microsoft Outlook 에서 Privacy Manager 인증서가 첨부된 전자 우편을 받게 됩니다.

사전 할당된 Privacy Manager 기업용 인증서 받기

1. 아웃룩에서 귀하에게 미리 할당된 Corporate Certificate 를 나타내는 이메일을 엽니다.
2. **받기**를 누릅니다.
3. Microsoft Outlook 에서 Privacy Manager 인증서가 첨부된 전자 우편을 받게 됩니다.
4. 인증서를 설치하려면 45페이지의 Privacy Manager 인증서 설치를 참조하십시오.

Privacy Manager 인증서 설치

1. Privacy Manager 인증서가 첨부된 전자 우편을 받으면 전자 우편을 열고 Outlook 2007 에서 메시지의 오른쪽 하단 또는 Outlook 2003 의 왼쪽 상단에 있는 **설정** 버튼을 누릅니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.
3. 인증서 설치 완료 페이지에서 **다음**을 누릅니다.
4. 인증서 백업 페이지에 백업 파일의 위치와 이름을 입력하거나 **찾아보기**를 눌러 위치를 검색합니다.

△ **주의:** 하드 드라이브가 아닌 다른 위치에 파일을 저장하고 안전한 장소에 보관해야 합니다. 이 파일은 사용자가 사용할 목적으로만 보관해야 하고, Privacy Manager 인증서 및 관련 키를 복원해야 하는 경우에 필요합니다.

5. 암호를 입력하고 확인한 후 **다음**을 누릅니다.
6. 선택한 보안 로그온 방법을 사용하여 인증합니다.
7. 신뢰할 수 있는 연락처 초대 프로세스를 시작하려면, 49페이지의 Microsoft Outlook 연락처를 사용하여 신뢰할 수 있는 연락처 추가의 2 단계부터 시작해 화면 지시에 따릅니다.

   또는

   취소를 누른 경우 신뢰할 수 있는 연락처를 나중에 추가하는 방법은 48페이지의 신뢰할 수 있는 연락처 추가를 참조하십시오.

Privacy Manager 인증서 세부 정보 보기

1. Privacy Manager 를 열고 **인증서**를 누릅니다.
2. Privacy Manager 인증서를 누릅니다.
3. **인증서 세부 정보**를 누릅니다.
4. 세부 정보 보기를 마치면 **확인**을 누릅니다.

Privacy Manager 인증서 갱신

Privacy Manager 인증서의 만료 날짜가 가까워지면 인증서를 갱신하라는 알림을 받게 됩니다.

1. Privacy Manager 를 열고 **인증서**를 누릅니다.
2. **인증서 갱신**을 누릅니다.
3. 화면에 표시되는 지침에 따라 새 Privacy Manager 인증서를 구입합니다.

주: Privacy Manager 인증서 갱신 과정으로 이전 Privacy Manager 인증서를 대체할 수는 없습니다. 새 Privacy Manager 인증서를 구입하고 44페이지의 Privacy Manager 인증서 요청 및 설치에 나와 있는 동일한 절차에 따라 설치해야 합니다.

기본 Privacy Manager 인증서 설정

컴퓨터에 다른 인증 기관에서 발행한 추가 인증서가 설치되어 있더라도 Privacy Manager 에서는 Privacy Manager 인증서만 표시됩니다.

컴퓨터에 Privacy Manager 에서 설치한 Privacy Manager 인증서가 둘 이상 있는 경우 그 중 하나를 기본 인증서로 지정할 수 있습니다.

1. Privacy Manager 를 열고 **인증서**를 누릅니다.
2. 기본 인증서로 사용하려는 Privacy Manager 인증서를 누른 다음 **기본값으로 설정**을 누릅니다.
3. **확인**을 누릅니다.

주: 기본 Privacy Manager 인증서를 반드시 사용할 필요는 없습니다. 다양한 Privacy Manager 기능을 통해 사용하려는 Privacy Manager 인증서를 선택할 수 있습니다.

Privacy Manager 인증서 삭제

Privacy Manager 인증서를 삭제하면 파일을 열 수 없으며 인증서로 암호화된 데이터도 볼 수 없습니다. 실수로 Privacy Manager 인증서를 삭제한 경우 인증서를 설치할 때 만들었던 백업 파일을 사용하여 인증서를 복원할 수 있습니다. 자세한 내용은 47페이지의 Privacy Manager 인증서 복원을 참조하십시오.

Privacy Manager 인증서를 삭제하려면 다음과 같이 하십시오.

1. Privacy Manager 를 열고 **인증서**를 누릅니다.
2. 삭제하려는 Privacy Manager 인증서를 누른 다음 **고급**을 누릅니다.
3. **삭제**를 누릅니다.

4. 확인 대화 상자가 표시되면 **예**를 누릅니다.
5. **닫기**를 누른 다음 **적용**을 누릅니다.

Privacy Manager 인증서 복원

Privacy Manager 인증서를 설치하는 과정에서 해당 인증서의 백업 사본을 만들어야 합니다. 또한 마이그레이션 페이지에서 백업 사본을 만들 수 있습니다. 이 백업 사본은 다른 컴퓨터로 마이그레이션하거나 인증서를 동일한 컴퓨터로 복원할 때 사용할 수 있습니다.

1. Privacy Manager 를 열고 **마이그레이션**을 누릅니다.
2. **복원**을 누릅니다.
3. 마이그레이션 파일 페이지에서 **찾아보기**를 눌러 백업 프로세스에서 만든 .dppsm 파일을 검색한 후 **다음**을 누릅니다.
4. 백업을 만들 때 사용했던 암호를 입력한 후 **다음**을 누릅니다.
5. **마침**을 누릅니다.
6. **확인**을 누릅니다.

자세한 내용은 45페이지의 Privacy Manager 인증서 설치 또는 62페이지의 Privacy Manager 인증서 및 신뢰할 수 있는 연락처 백업을 참조하십시오.

Privacy Manager 인증서 해지

인증서의 보안이 노출될 위험이 있다고 생각되는 경우 사용자의 인증서를 해지할 수 있습니다. 해지하려면 다음과 같이 하십시오.

주: 해지된 Privacy Manager 인증서는 삭제되지 않습니다. 이 인증서는 암호화된 파일을 보는 데 사용될 수 있습니다.

1. Privacy Manager 를 열고 **인증서**를 누릅니다.
2. **고급**을 누릅니다.
3. 해지하려는 Privacy Manager 인증서를 누른 다음 **해지**를 누릅니다.
4. 확인 대화 상자가 표시되면 **예**를 누릅니다.
5. 선택한 보안 로그온 방법을 사용하여 인증합니다.
6. 화면의 지침을 따릅니다.

신뢰할 수 있는 연락처 관리

신뢰할 수 있는 연락처란 서로 안전하게 대화할 수 있도록 Privacy Manager 인증서를 교환한 사용자를 말합니다.

Trusted Contacts Manager 에서는 다음 작업을 수행할 수 있습니다.

- 신뢰할 수 있는 연락처의 세부 정보 보기
- 신뢰할 수 있는 연락처 삭제
- 신뢰할 수 있는 연락처의 해지 상태 확인(고급)

신뢰할 수 있는 연락처 추가

신뢰할 수 있는 연락처를 추가하는 과정은 다음과 같은 세 가지 단계로 이루어집니다.

1. 사용자가 신뢰할 수 있는 연락처 수신자에게 전자 우편 초대 요청을 보냅니다.
2. 신뢰할 수 있는 연락처 수신자가 전자 우편 요청에 응답합니다.
3. 신뢰할 수 있는 연락처 수신자로부터 전자 우편 응답을 받고 **수락**을 누릅니다.

개별 수신자에게 신뢰할 수 있는 연락처 전자 우편 초대 요청을 보내거나 Microsoft Outlook 주소록에 있는 모든 연락처로 초대 요청을 보낼 수 있습니다.

다음 단원을 참조하여 신뢰할 수 있는 연락처를 추가하십시오.

주: 신뢰할 수 있는 연락처 초대 요청에 응답하려면 신뢰할 수 있는 연락처 수신자의 컴퓨터에 Privacy Manager 가 설치되어 있거나 대체 클라이언트가 설치되어 있어야 합니다. 대체 클라이언트 설치에 대한 자세한 내용을 보려면 DigitalPersona 웹 사이트(http://DigitalPersona.com/PrivacyManager)에 액세스하십시오.

신뢰할 수 있는 연락처 추가

1. Privacy Manager 를 열고 **신뢰할 수 있는 연락처 관리자**를 누른 다음 **연락처 초대**를 누릅니다.

   또는

   Microsoft Outlook 의 도구 모음에서 **안전하게 보내기** 옆의 아래쪽 화살표를 누른 다음 **연락처 초대**를 누릅니다.

2. 인증서 선택 대화 상자가 열리면 사용하려는 Privacy Manager 인증서를 누른 다음 **확인**을 누릅니다.

3. 신뢰할 수 있는 연락처 초대 대화 상자가 열리면 대화 상자의 내용을 읽은 다음 **확인**을 누릅니다.

   전자 우편이 자동으로 생성됩니다.

4. 신뢰할 수 있는 연락처로 추가할 수신자의 전자 우편 주소를 하나 이상 입력합니다.

5. 텍스트를 수정하고 서명합니다(선택 사항).

6. **보내기**를 누릅니다.

   주: Privacy Manager 인증서를 받지 않은 경우 신뢰할 수 있는 연락처 요청을 보내려면 Privacy Manager 인증서가 있어야 한다는 메시지를 받게 됩니다. **확인**을 눌러 인증서 요청 마법사를 시작합니다. 자세한 내용은 44페이지의 Privacy Manager 인증서 요청 및 설치를 참조하십시오.

7. 선택한 보안 로그온 방법을 사용하여 인증합니다.

   주: 신뢰할 수 있는 연락처 수신자가 전자 우편을 받으면 전자 우편을 열고 오른쪽 아래 모퉁이에 있는 **수락**을 누른 다음 대화 상자가 열리면 **확인**을 누릅니다.

8. 수신자로부터 신뢰할 수 있는 연락처 초대 요청을 수락하는 전자 우편을 받으면 전자 우편의 오른쪽 아래 모퉁이에 있는 **수락**을 누릅니다.

   수신자가 신뢰할 수 있는 연락처 목록에 추가되었음을 알리는 대화 상자가 열립니다.

9. **확인**을 누릅니다.

Microsoft Outlook 연락처를 사용하여 신뢰할 수 있는 연락처 추가

1. Privacy Manager 를 열고 **신뢰할 수 있는 연락처 관리자**를 누른 다음 **연락처 초대**를 누릅니다.

   또는

   Microsoft Outlook 의 도구 모음에서 **안전하게 보내기** 옆의 아래쪽 화살표를 누른 다음 **Outlook 의 모든 연락처 초대**를 누릅니다.

2. 신뢰할 수 있는 연락처 초대 페이지가 열리면 신뢰할 수 있는 연락처로 추가하려는 수신자의 이메일 주소를 선택하고 **다음**을 누릅니다.

3. 초대 요청 보내기 페이지가 열리면 **마침**을 누릅니다.

   선택한 Microsoft Outlook 전자 우편 주소가 나열된 전자 우편이 자동으로 생성됩니다.

4. 텍스트를 수정하고 서명합니다(선택 사항).

5. **보내기**를 누릅니다.

주: Privacy Manager 인증서를 받지 않은 경우 신뢰할 수 있는 연락처 요청을 보내려면 Privacy Manager 인증서가 있어야 한다는 메시지를 받게 됩니다. **확인**을 눌러 인증서 요청 마법사를 시작합니다. 자세한 내용은 44페이지의 Privacy Manager 인증서 요청 및 설치를 참조하십시오.

6. 선택한 보안 로그온 방법을 사용하여 인증합니다.

주: 신뢰할 수 있는 연락처 수신자가 전자 우편을 받으면 전자 우편을 열고 오른쪽 아래 모퉁이에 있는 **수락**을 누른 다음 대화 상자가 열리면 **확인**을 누릅니다.

7. 수신자로부터 신뢰할 수 있는 연락처 초대 요청을 수락하는 전자 우편을 받으면 전자 우편의 오른쪽 아래 모퉁이에 있는 **수락**을 누릅니다.

   수신자가 신뢰할 수 있는 연락처 목록에 추가되었음을 확인할 수 있는 대화 상자가 열립니다.

8. **확인**을 누릅니다.

신뢰할 수 있는 연락처 세부 정보 보기

1. Privacy Manager 를 열고 **신뢰할 수 있는 연락처**를 누릅니다.
2. 신뢰할 수 있는 연락처를 누릅니다.
3. **연락처 세부 정보**를 누릅니다.
4. 세부 정보 보기를 마쳤으면 **확인**을 누릅니다.

신뢰할 수 있는 연락처 삭제

1. Privacy Manager 를 열고 **신뢰할 수 있는 연락처**를 누릅니다.
2. 삭제하려는 신뢰할 수 있는 연락처를 누릅니다.
3. **연락처 삭제**를 누릅니다.
4. 확인 대화 상자가 표시되면 **예**를 누릅니다.

신뢰할 수 있는 연락처의 해지 상태 확인

신뢰할 수 있는 연락처가 Privacy Manager 인증서를 해지했는지 확인하려면 다음과 같이 하십시오.

1. Privacy Manager 를 열고 **신뢰할 수 있는 연락처**를 누릅니다.
2. 신뢰할 수 있는 연락처를 누릅니다.
3. **고급**버튼을 누릅니다.

   신뢰할 수 있는 연락처 고급 관리 대화 상자가 열립니다.
4. **해지 확인**을 누릅니다.
5. **닫기**를 누릅니다.

일반 작업

다음 Microsoft 제품에서 Privacy Manager 를 사용할 수 있습니다.

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Microsoft Outlook 에서 Privacy Manager 사용

Privacy Manager 를 설치하면 Microsoft Outlook 의 도구 모음에 Privacy(개인 정보) 버튼이 표시되고 각 Microsoft Outlook 전자 우편 메시지의 도구 모음에 Send Securely(안전하게 보내기) 버튼이 표시됩니다. **Privacy(개인 정보)** 또는 **Send Securely(안전하게 보내기)** 버튼 옆의 아래쪽 화살표를 누르면 다음 옵션 중에서 선택할 수 있습니다.

- Sign and Send(서명하고 보내기) (Send Securely(안전하게 보내기) 버튼에만 해당)—이 옵션을 사용하면 전자 우편에 디지털 서명을 추가하고 선택한 보안 로그온 방법을 통해 인증한 후 전자 우편을 보낼 수 있습니다.
- Seal for Trusted Contacts and Send(신뢰할 수 있는 연락처에 대해 봉인하고 보내기)(Send Securely(안전하게 보내기) 버튼에만 해당)—이 옵션을 사용하면 디지털 서명을 추가하고 이메일을 암호화하며 선택한 보안 로그온 방법을 통해 인증한 후 이메일을 보낼 수 있습니다.
- Invite Contacts(연락처 초대)—이 옵션을 사용하면 신뢰할 수 있는 연락처 초대 요청을 보낼 수 있습니다. 자세한 내용은 48페이지의 신뢰할 수 있는 연락처 추가를 참조하십시오.
- Invite Outlook Contacts(Outlook 의 연락처 초대)—이 옵션을 사용하면 Microsoft Outlook 주소록의 모든 연락처로 신뢰할 수 있는 연락처 초대 요청을 보낼 수 있습니다. 자세한 내용은 49페이지의 Microsoft Outlook 연락처를 사용하여 신뢰할 수 있는 연락처 추가를 참조하십시오.
- Open the Privacy Manager software(Privacy Manager 소프트웨어 열기)—Certificates(인증서), Trusted Contacts(신뢰할 수 있는 연락처) 및 Settings(설정) 옵션을 사용하면 Privacy Manager 소프트웨어를 열어 현재 설정을 추가하거나 보거나 또는 변경할 수 있습니다. 자세한 내용은 51페이지의 Microsoft Outlook 용 Privacy Manager 구성를 참조하십시오.

Microsoft Outlook 용 Privacy Manager 구성

1. Privacy Manager 를 열고 **Settings(설정)**를 누른 다음 **E-mail(전자 우편)** 탭을 누릅니다.

   또는

   기본 Microsoft Outlook 도구 모음에서 **Send Securely(안전하게 보내기)**(Outlook 2003 에서는 **Privacy(개인 정보)**) 옆에 있는 아래 방향 화살표를 누른 다음 **Settings(설정)**을 누릅니다.

   또는

   Microsoft 전자 우편 메시지의 도구 모음에서 **Send Securely(안전하게 보내기)** 옆의 아래쪽 화살표를 누른 다음 **Settings(설정)**를 누릅니다.

2. 전자 우편을 안전하게 보낼 때 수행하려는 동작을 선택하고 **OK(확인)**를 누릅니다.

전자 우편 메시지에 서명하고 보내기

1. Microsoft Outlook 에서 **New(새로 만들기)** 또는 **Reply(회신)**를 누릅니다.
2. 전자 우편 메시지를 입력합니다.

3. **Send Securely(안전하게 보내기)**(Outlook 2003 에서는 **Privacy(개인 정보)**) 옆에 있는 아래 방향 화살표를 누른 다음 **Sign and Send(서명하고 보내기)**를 누릅니다.

4. 선택한 보안 로그온 방법을 사용하여 인증합니다.

전자 우편 메시지 봉인하고 보내기

디지털 서명이 되어 있고 봉인된(암호화된) 전자 우편 메시지는 신뢰할 수 있는 연락처 목록에서 선택된 사람만 볼 수 있습니다.

신뢰할 수 있는 연락처에 전자 우편 메시지를 봉인하고 보내려면 다음과 같이 하십시오.

1. Microsoft Outlook 에서 **New(새로 만들기)** 또는 **Reply(회신)**를 누릅니다.

2. 전자 우편 메시지를 입력합니다.

3. **Send Securely(안전하게 보내기)**(Outlook 2003 에서는 **Privacy(개인 정보)**) 옆에 있는 아래 방향 화살표를 누른 다음 **Seal for Trusted Contacts and Send(신뢰할 수 있는 연락처에 서명하고 보내기)**를 누릅니다.

4. 선택한 보안 로그온 방법을 사용하여 인증합니다.

봉인된 전자 우편 메시지 보기

봉인된 전자 우편 메시지를 열면 전자 우편 제목에 보안 레이블이 표시됩니다. 보안 레이블의 내용은 다음과 같습니다.

- 전자 우편에 서명한 사람의 ID 를 확인하는 데 사용되는 인증서
- 전자 우편에 서명한 사람의 인증서를 확인하는 데 사용되는 제품

Microsoft Office 2007 문서에서 Privacy Manager 사용

주: Privacy Manager 는 Microsoft 2007 문서에서만 사용할 수 있습니다.

Privacy Manager 인증서를 설치하면 모든 Microsoft Word, Microsoft Excel 및 Microsoft PowerPoint 문서의 도구 모음 오른쪽에 Sign and Encrypt(서명 및 암호화) 버튼이 표시됩니다. **Sign and Encrypt(서명 및 암호화)** 옆의 아래쪽 화살표를 누르면 다음 옵션 중에서 선택할 수 있습니다.

- 문서에 서명—이 옵션은 문서에 디지털 서명을 추가합니다.
- 서명하기 전에 서명 줄 추가(Microsoft Word 및 Microsoft Excel 에만 해당)—기본적으로 Microsoft Word 또는 Microsoft Excel 문서를 서명하거나 암호화하면 서명 줄이 추가됩니다. 이 옵션을 끄려면 **Add Signature Line(서명 줄 추가)**을 눌러 확인란의 표시를 제거합니다.
- 문서 암호화—이 옵션을 사용하면 문서에 디지털 서명을 추가하고 문서를 암호화할 수 있습니다.
- 암호화 제거—이 옵션을 사용하면 문서에서 암호화를 제거할 수 있습니다.
- Privacy Manager 소프트웨어 열기—Certificates(인증서), Trusted Contacts(신뢰할 수 있는 연락처) 및 Settings(설정) 옵션을 사용하면 Privacy Manager 소프트웨어를 열어 현재 설정을 추가하거나 보거나 또는 변경할 수 있습니다. 자세한 내용은 44페이지의 Privacy Manager 인증서 관리, 47페이지의 신뢰할 수 있는 연락처 관리 또는 53페이지의 Microsoft Office 용 Privacy Manager 구성을 참조하십시오.

Microsoft Office 용 Privacy Manager 구성

1. Privacy Manager 를 열고 **Settings(설정)**를 누른 다음 **Documents(문서)** 탭을 누릅니다.

   또는

   Microsoft Office 문서의 도구 모음에서 **Sign and Encrypt(서명 및 암호화)** 옆의 아래쪽 화살표를 누른 다음 **Settings(설정)**를 누릅니다.

2. 구성할 동작을 선택한 다음 **OK(확인)**를 누릅니다.

Microsoft Office 문서 서명

1. Microsoft Word, Microsoft Excel 또는 Microsoft PowerPoint 에서 문서를 만들고 저장합니다.
2. **Sign and Encrypt(서명 및 암호화)** 옆의 아래쪽 화살표를 누른 다음 **Sign Document(문서에 서명하기)**를 누릅니다.
3. 선택한 보안 로그온 방법을 사용하여 인증합니다.
4. 확인 대화 상자가 열리면 대화 상자의 내용을 읽은 다음 **OK(확인)**를 누릅니다.

나중에 문서를 편집하려면 다음과 같이 하십시오.

1. 화면 왼쪽 상단에 있는 **Office** 버튼을 누릅니다.
2. **Prepare(준비)**를 누른 다음 **Mark as Final(최종본으로 표시)**을 누릅니다.
3. 확인 대화 상자가 표시되면 **Yes(예)**를 누르고 작업을 계속합니다.
4. 편집을 마치면 문서에 다시 서명합니다.

Microsoft Word 또는 Microsoft Excel 문서 서명 시 서명 줄 추가

Microsoft Word 또는 Microsoft Excel 문서를 서명할 때 다음과 같은 방법으로 Privacy Manager 를 사용하여 서명 줄을 추가할 수 있습니다.

1. Microsoft Word 또는 Microsoft Excel 에서 문서를 만들고 저장합니다.
2. **Home(홈)** 메뉴를 누릅니다.
3. **Sign and Encrypt(서명 및 암호화)** 옆의 아래쪽 화살표를 누른 다음 **Add Signature Line Before Signing(서명하기 전에 서명 줄 추가)**을 누릅니다.

   주: 이 옵션을 선택하면 Add Signature Line Before Signing(서명하기 전에 서명 줄 추가) 옆에 확인 표시가 나타납니다. 기본적으로 이 옵션이 활성화되어 있습니다.

4. **Sign and Encrypt(서명 및 암호화)** 옆의 아래쪽 화살표를 누른 다음 **Sign Document(문서에 서명하기)**를 누릅니다.
5. 선택한 보안 로그온 방법을 사용하여 인증합니다.

Microsoft Word 또는 Microsoft Excel 문서에 추천 서명자 추가

추천 서명자를 지정하여 문서에 서명 줄을 둘 이상 추가할 수 있습니다. 추천 서명자란 Microsoft Word 또는 Microsoft Excel 문서의 소유자가 문서에 서명 줄을 추가하도록 지정한 사용자를 말합니다. 추천 서명자는 사용자 본인이 될 수도 있으며, 사용자가 원하는 다른 사람을 문서에 서명할 수 있도록 추천 서명자로 지정할 수도 있습니다. 예를 들어, 부서의 모든 직원이 서명해야 하는 문서를 작성

하는 경우 문서의 마지막 페이지 아래쪽에 날짜별로 서명할 것을 지시하는 서명 줄을 포함시킬 수 있습니다.

Microsoft Word 또는 Microsoft Excel 문서에 추천 서명자를 추가하려면 다음과 같이 하십시오.

1. Microsoft Word 또는 Microsoft Excel 에서 문서를 만들고 저장합니다.
2. **Insert(삽입)** 메뉴를 누릅니다.
3. 도구 모음의 **Text(텍스트)** 그룹에서 **Signature Line(서명 줄)** 옆의 화살표를 누른 다음 **Privacy Manager Signature Provider(Privacy Manager 서명 공급자)**를 누릅니다.

   Signature Setup(서명 설정) 대화 상자가 열립니다.
4. **추천 서명자** 아래에 있는 텍스트 상자에 추천 서명자 이름을 입력합니다.
5. **서명자 지침** 아래에 있는 텍스트 상자에 추천 서명자에게 표시할 메시지를 입력합니다.

   주: 이 메시지는 제목 위치에 표시되고 문서가 서명되면 메시지가 삭제되거나 사용자의 제목으로 바뀝니다.
6. **Show sign date in signature line(서명 줄에 서명 날짜 표시)** 확인란을 선택하여 날짜를 표시합니다.
7. **Show signer's title in signature line(서명 줄에 서명자의 제목 표시)** 확인란을 선택하여 제목을 표시합니다.

   주: 문서의 소유자가 문서에 추천 서명자를 지정하기 때문에 **Show sign date in signature line (서명 줄에 서명 날짜 표시)** 및/또는 **Show signer's title in signature line(서명 줄에 서명자의 제목 표시)** 확인란이 선택되어 있지 않으면 서명자의 문서 설정을 날짜나 제목을 표시하도록 구성한 경우에도 추천 서명자는 서명 줄에 날짜 및/또는 제목을 표시할 수 없게 됩니다.
8. **OK(확인)**를 누릅니다.

추천 서명자의 서명 줄 추가

추천 서명자가 문서를 열면 서명자 이름이 대괄호 안에 표시되어 서명이 필요함을 나타냅니다.

문서에 서명하려면 다음과 같이 하십시오.

1. 해당 서명 줄을 두 번 누릅니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.

   문서의 소유자가 지정한 설정에 따라 서명 줄이 표시됩니다.

Microsoft Office 문서 암호화

사용자와 신뢰할 수 있는 연락처 대상만이 볼 수 있도록 Microsoft Office 문서를 암호화할 수 있습니다. 문서를 암호화하고 닫을 때 사용자와 목록에서 선택한 Trusted Contact(신뢰할 수 있는 연락처) 대상은 이 문서를 다시 열기 전에 먼저 인증해야 합니다.

Microsoft Office 문서를 암호화하려면 다음과 같이 하십시오.

1. Microsoft Word, Microsoft Excel 또는 Microsoft PowerPoint 에서 문서를 만들고 저장합니다.
2. **Home(홈)** 메뉴를 누릅니다.

3. **Sign and Encrypt(서명 및 암호화)** 옆의 아래쪽 화살표를 누른 다음 **Encrypt Document(문서 암호화)**를 누릅니다.

   Select Trusted Contacts(신뢰할 수 있는 연락처 선택) 대화 상자가 열립니다.

4. 문서를 열고 내용을 볼 수 있도록 하려는 신뢰할 수 있는 연락처의 이름을 누릅니다.

주: 신뢰할 수 있는 연락처 이름을 여러 개 선택하려면 ctrl 키를 누른 채 각 이름을 누릅니다.

5. **OK(확인)**를 누릅니다.

문서를 나중에 편집하려면 55페이지의 Microsoft Office 문서에서 암호화 제거의 절차를 따르십시오. 암호화를 제거하면 문서를 편집할 수 있습니다. 이 단원의 절차에 따라 문서를 다시 암호화하십시오.

Microsoft Office 문서에서 암호화 제거

Microsoft Office 문서에서 암호화를 제거하면 사용자와 신뢰할 수 있는 연락처 대상이 문서의 내용을 열고 보기 위해 인증하지 않아도 됩니다.

Microsoft Office 문서에서 암호화를 제거하려면 다음과 같이 하십시오.

1. 암호화된 Microsoft Word, Microsoft Excel 또는 Microsoft PowerPoint 문서를 엽니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.
3. **Home(홈)** 메뉴를 누릅니다.
4. **Sign and Encrypt(서명 및 암호화)** 옆의 아래쪽 화살표를 누른 다음 **Remove Encryption(암호화 제거)**을 누릅니다.

암호화된 Microsoft Office 문서 보내기

전자 우편 자체를 서명하거나 암호화하지 않고 전자 우편 메시지에 암호화된 Microsoft Office 문서를 첨부할 수 있습니다. 평소에 첨부 파일이 있는 일반 전자 우편을 보내는 것처럼 서명이 있거나 암호화된 문서가 있는 전자 우편을 만들고 보내면 됩니다.

그러나 보안을 최적화하기 위해서는 서명이 있거나 암호화된 Microsoft Office 문서를 첨부할 때 전자 우편을 암호화하는 것이 좋습니다.

서명이 있거나 암호화된 Microsoft Office 문서와 함께 봉인된 전자 우편을 보내려면 다음과 같이 하십시오.

1. Microsoft Outlook 에서 **New(새로 만들기)** 또는 **Reply(회신)**를 누릅니다.
2. 전자 우편 메시지를 입력합니다.
3. Microsoft Office 문서를 첨부합니다.
4. 자세한 지침은 52페이지의 전자 우편 메시지 봉인하고 보내기를 참조하십시오.

서명이 있는 Microsoft Office 문서 보기

주: 서명이 있는 Microsoft Office 문서를 보려는 경우 Privacy Manager 인증서가 없어도 됩니다.

서명한 Microsoft Office 문서를 열면, 문서 창 아래 부분에 있는 상태 표시줄에 디지털 서명 아이콘이 표시됩니다.

1. **디지털 서명** 아이콘을 눌러 서명 대화상자를 열면, 문서에 서명한 모든 사용자의 이름과 각 사용자가 서명한 날짜를 볼 수 있습니다.
2. 각 서명에 대한 자세한 내용을 보려면, 서명 대화상자에서 이름을 마우스 오른쪽 버튼으로 누르고 '서명 세부사항'을 선택합니다.

암호화된 Microsoft Office 문서 보기

다른 컴퓨터에서 암호화된 Microsoft Office 문서를 보려면 해당 컴퓨터에 Privacy Manager 가 설치되어 있어야 합니다. 또한 파일을 암호화할 때 사용한 Privacy Manager 인증서를 복원해야 합니다.

암호화된 Microsoft Office 문서를 보려는 신뢰할 수 있는 연락처 대상이 Privacy Manager 인증서를 보유하고 있고 해당 사용자의 컴퓨터에 Privacy Manager 가 설치되어 있어야 합니다. 또한 암호화된 Microsoft Office 문서의 소유자가 신뢰할 수 있는 연락처 대상을 선택해야 합니다.

Windows Live Messenger 에서 Privacy Manager 사용

Privacy Manager 를 사용하여 Windows Live Messenger 에 다음과 같은 보안 통신 기능을 추가할 수 있습니다.

- **보안 채팅**—전자 상거래 보안에 사용되는 동일한 기술인 XML 프로토콜을 통해 SSL/TLS (Secure Sockets Layer/Transport Layer Security)를 사용하여 메시지가 전송됩니다.
- **수신자 정보 표시**—메시지를 보내기 전에 수신자의 부재 여부와 ID 를 확인할 수 있습니다.
- **서명이 있는 메시지**—메시지에 전자 서명을 할 수 있습니다. 메시지가 변경되는 경우 수신자가 메시지를 받을 때 유효하지 않은 메시지로 표시됩니다.
- **표시/숨기기 기능**—Privacy Manager Chat 창에서 일부 또는 전체 메시지를 숨길 수 있습니다. 내용이 숨겨져 있는 메시지를 보낼 수 있습니다. 메시지를 표시하기 전에 인증이 필요합니다.
- **안전한 대화 기록**—대화 세션의 로그가 저장되기 전에 암호화되고 로그를 보려면 인증이 필요합니다.
- **자동 잠금/잠금 해제**—Privacy Manager Chat 창을 잠그고 잠금을 해제하거나 지정한 시간 동안 작업하지 않을 경우 자동으로 잠기도록 설정할 수 있습니다.

Privacy Manager Chat 세션 시작

주: Privacy Manager Chat 을 사용하려면 양쪽 사용자의 컴퓨터에 Privacy Manager 와 Privacy Manager 인증서가 설치되어 있어야 합니다. Privacy Manager 인증서 설치에 대한 자세한 내용은 44페이지의 Privacy Manager 인증서 요청 및 설치를 참조하십시오.

1. Windows Live Messenger 에서 Privacy Manager Chat 을 시작하려면 다음 중 하나의 절차를 수행하십시오.
   a. 마우스 오른쪽 버튼으로 Live Messenger 의 온라인 대화 상대를 누른 다음 **플러그인 시작**을 선택합니다.
   b. **대화 시작**을 누릅니다.

또는

a. Live Messenger 의 온라인 대화 상대를 두 번 누른 다음 **See a list of activities(활동 목록 보기)** 메뉴를 선택합니다.

b. **동작**을 누른 다음 **대화 시작**을 누릅니다.

또는

a. 알림 영역에서 **ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누르고, **HP ProtectTools 용 Privacy Manager** 와 **대화 시작**을 차례로 누릅니다.

b. Live Messenger 에서 **동작: 활동 시작**을 누른 다음 **Privacy Manager 대화**를 선택합니다.

주: 각 사용자는 Live Messenger 에서 온라인 상태이어야 하며, 다른 사람의 Live Messenger 온라인 창에 표시되어 있어야 합니다. 온라인 사용자를 눌러 선택합니다.

Privacy Manager 는 Privacy Manager Chat 을 시작할 대화 상대에게 초대 요청을 보냅니다. 초대받은 대화 상대가 수락하면 Privacy Manager Chat 창이 열립니다. 초대받은 대화 상대의 컴퓨터에 Privacy Manager 가 설치되어 있지 않으면 Privacy Manager 를 다운로드하라는 메시지가 나타납니다.

2. **Start(시작)**를 눌러 보안 채팅을 시작합니다.

Windows Live Messenger 용 Privacy Manager 구성

1. Privacy Manager Chat 에서 **Settings(설정)** 버튼을 누릅니다.

   또는

   Privacy Manager 에서 **Settings(설정)**를 누른 다음 **Chat(채팅)** 탭을 누릅니다.

   또는

   Privacy Manager Live Messenger History Viewer 에서 **Settings(설정)** 버튼을 누릅니다.

2. Privacy Manager Chat 사용 후 세션이 잠길 때까지 걸리는 대기 시간을 지정하려면 **Lock session after _ minutes of activity(_분간 사용하지 않으면 세션 잠금)** 목록에서 숫자를 선택합니다.

3. 대화 세션의 대화 기록 폴더를 지정하려면 **Browse(찾아보기)**를 눌러 폴더를 찾은 후 **OK(확인)**를 누릅니다.

4. 세션을 닫을 때 자동으로 암호화하고 저장하려면 **Automatically save secure chat history(보안 대화 기록 자동 저장)**의 확인란을 선택합니다.

5. **OK(확인)**를 누릅니다.

Privacy Manager Chat 창에서 채팅하기

Privacy Manager Chat 을 시작하면 Windows Live Messenger 에 Privacy Manager Chat 창이 열립니다. Privacy Manager Chat 의 사용 방법은 기본 Windows Live Messenger 와 유사하지만 Privacy Manager Chat 창에는 다음과 같은 기능이 추가되어 있습니다.

- **Save(저장)**—이 버튼을 누르면 구성 설정에서 지정한 폴더에 대화 세션을 저장할 수 있습니다. 또한 Privacy Manager Chat 을 닫을 때 각 세션이 자동으로 저장되도록 구성할 수도 있습니다.
- **Hide all(모두 숨기기)** 및 **Show all(모두 표시)**—해당 버튼을 누르면 Secure Communications(안전 대화하기) 창에 표시된 메시지를 확장하거나 축소할 수 있습니다. 메시지 머리글을 눌러 개별 메시지를 숨기거나 표시할 수도 있습니다.
- **Are you there?(안녕하세요?)**—이 버튼을 누르면 대화 상대에게 인증을 요청할 수 있습니다.
- **Lock(잠금)**—이 버튼을 누르면 Privacy Manager Chat 창을 닫고 Chat Entry(채팅 항목) 창으로 돌아갈 수 있습니다. Secure Communications(안전 대화하기) 창을 다시 표시하려면 **Resume the session(세션 다시 시작)**을 누른 다음 선택한 보안 로그온 방법을 사용하여 인증합니다.
- **Send(보내기)**—이 버튼을 누르면 대화 상대에게 암호화된 메시지를 보낼 수 있습니다.
- **Send signed(서명하고 보내기)**—이 확인란을 선택하면 메시지를 전자 서명하고 암호화할 수 있습니다. 메시지가 변경되는 경우 수신자가 메시지를 받을 때 유효하지 않은 메시지로 표시됩니다. 사용자는 서명이 있는 메시지를 보낼 때마다 인증해야 합니다.
- **Send hidden(숨김으로 보내기)**—이 확인란을 선택하면 메시지 제목만 표시되도록 메시지를 암호화하고 보낼 수 있습니다. 대화 상대가 메시지 내용을 읽으려면 인증해야 합니다.

대화 기록 보기

Privacy Manager Chat: Live Messenger History Viewer 에 암호화된 Privacy Manager Chat 세션 파일이 나타납니다. Privacy Manager Chat 창에서 **Save(저장)**를 누르거나 Privacy Manager 의 Chat(채팅) 탭에서 자동 저장을 구성하여 세션을 저장할 수 있습니다. 뷰어에서 각 세션에는 (암호화된) Contact Screen Name(연락처 대화명) 및 세션을 시작하고 종료한 날짜와 시간이 표시됩니다. 기본적으로 세션에는 사용자가 설정한 전자 우편 계정이 표시됩니다. **Display history for(대화 기록 표시 대상)** 메뉴를 사용하여 대화 기록을 볼 특정 계정만 선택할 수 있습니다.

뷰어에서는 다음 작업을 수행할 수 있습니다.

- 59페이지의 모든 세션 표시
- 59페이지의 특정 계정의 세션 표시
- 59페이지의 세션 ID 보기
- 59페이지의 세션 보기
- 60페이지의 특정 텍스트에 대한 세션 검색
- 60페이지의 세션 삭제
- 60페이지의 열 추가 또는 제거
- 60페이지의 표시된 세션 필터링

Live Messenger History Viewer 를 시작하려면 다음과 같이 하십시오.

- 알림 영역에서, 작업 표시줄 맨 오른쪽에 있는 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누르고 **Privacy Manager: HP ProtectTools 용**을 누른 다음 **Live Messenger History Viewer**를 누릅니다.

또는

- Chat 세션에서 **History Viewer(대화 기록 뷰어)** 또는 **History(대화 기록)**를 누릅니다.

모든 세션 표시

모든 세션 표시에는 현재 선택된 세션 및 동일한 계정의 모든 세션에 대한 암호가 해독된 Contact Screen Name(연락처 대화명)이 표시됩니다.

저장한 모든 대화 기록 세션을 표시하려면 다음과 같이 하십시오.

1. Live Messenger History Viewer 에서 마우스 오른쪽 버튼으로 아무 세션이나 누른 다음 **Reveal All Sessions(모든 세션 표시)**를 선택합니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.

   Contact Screen Names(연락처 대화명)의 암호가 해독됩니다.
3. 원하는 세션을 두 번 눌러 내용을 봅니다.

특정 계정의 세션 표시

세션 표시에는 현재 선택된 세션에 대한 암호가 해독된 Contact Screen Name(연락처 대화명)이 표시됩니다.

특정 대화 기록 세션을 표시하려면 다음과 같이 하십시오.

1. Live Messenger History Viewer 에서 마우스 오른쪽 버튼으로 아무 세션이나 누른 다음 **Reveal Session(세션 표시)**를 선택합니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.

   Contact Screen Name(연락처 대화명)의 암호가 해독됩니다.
3. 원하는 표시된 세션을 두 번 눌러 내용을 봅니다.

주: 동일한 인증서로 암호화된 추가 세션에는 잠금 해제 아이콘이 표시되는데 이는 추가 인증 없이 추가 세션을 두 번 눌러 세션의 내용을 볼 수 있음을 의미합니다. 다른 인증서로 암호화된 세션에는 잠금 아이콘이 표시되는데 이는 Contact Screen Names(연락처 대화명) 또는 세션의 내용을 보려면 먼저 세션에 대해 추가 인증을 해야 함을 의미합니다.

세션 ID 보기

세션 ID 를 보려면 다음과 같이 하십시오.

- Live Messenger History Viewer 에서 마우스 오른쪽 버튼으로 표시된 아무 세션을 누른 다음 **View session ID(세션 ID 보기)**를 선택합니다.

세션 보기

세션 보기에서는 보려는 파일이 열립니다. 세션이 이전에 표시되지 않았으면(암호가 해독된 Contact Screen Name(연락처 대화명) 표시) 세션이 열리면서 동시에 표시됩니다.

Live Messenger 대화 기록 세션을 보려면 다음과 같이 하십시오.

1. Live Messenger History Viewer 에서 마우스 오른쪽 버튼으로 아무 세션이나 누른 다음 **View(보기)**를 선택합니다.
2. 메시지가 표시되면 선택한 보안 로그온 방법을 사용하여 인증합니다.

   세션 내용이 해독됩니다.

특정 텍스트에 대한 세션 검색

뷰어 창에 표시된 (암호가 해독된) 세션의 텍스트만 검색할 수 있습니다. 이러한 세션은 일반 텍스트에 Contact Screen Name(연락처 대화명)이 표시되는 세션입니다.

대화 기록 세션의 텍스트를 검색하려면 다음과 같이 하십시오.

1. Live Messenger History Viewer 에서 **Search(검색)** 버튼을 누릅니다.
2. 검색 텍스트를 입력하고 원하는 검색 매개 변수를 구성한 다음 **OK(확인)**를 누릅니다.

   뷰어 창에 해당 텍스트를 포함하는 세션이 강조 표시됩니다.

세션 삭제

1. 대화 기록 세션을 선택하려면 다음과 같이 하십시오.
2. **Delete(삭제)**를 누릅니다.

열 추가 또는 제거

기본적으로 Live Messenger History Viewer 에는 가장 자주 사용되는 열 3 개가 표시됩니다. 디스플레이에 추가 열을 추가하거나 디스플레이에서 열을 제거할 수 있습니다.

디스플레이에 열을 추가하려면 다음과 같이 하십시오.

1. 마우스 오른쪽 버튼으로 열 머리글을 누른 다음 **Add/Remove Columns(열 추가/제거)**를 선택합니다.
2. 왼쪽 패널에서 열 머리글을 선택한 다음 **Add(추가)**를 눌러 오른쪽 패널로 옮깁니다.

디스플레이에서 열을 제거하려면 다음과 같이 하십시오.

1. 마우스 오른쪽 버튼으로 열 머리글을 누른 다음 **Add/Remove Columns(열 추가/제거)**를 선택합니다.
2. 오른쪽 패널에서 열 머리글을 선택한 다음 **Remove(제거)**를 눌러 왼쪽 패널로 옮깁니다.

표시된 세션 필터링

Live Messenger History Viewer 에 모든 계정에 대한 세션 목록이 표시됩니다. 또한 표시된 세션을 다음을 기준으로 필터링할 수도 있습니다.

- 특정 계정. 자세한 내용은 61페이지의 특정 계정에 대한 세션 표시를 참조하십시오.
- 날짜 범위. 자세한 내용은 61페이지의 날짜 범위를 기준으로 세션 표시를 참조하십시오.
- 다른 폴더. 자세한 내용은 61페이지의 기본 폴더가 아닌 다른 폴더에 저장된 세션 표시를 참조하십시오.

특정 계정에 대한 세션 표시

▲ Live Messenger History Viewer(Live Messenger 대화 기록 뷰어)에서 **Display history for(대화 기록을 표시할 대상)** 메뉴의 계정을 선택합니다.

날짜 범위를 기준으로 세션 표시

1. Live Messenger History View 에서 **Advanced Filter(고급 필터)** 아이콘을 누릅니다.

   Advanced Filter(고급 필터) 대화 상자가 열립니다.

2. **Display only sessions within specified date range(특정 날짜 범위 내의 세션만 표시)**의 확인란을 선택합니다.

3. **시작 날짜** 및 **종료 날짜** 상자에 연도, 월, 일을 입력하거나 달력 옆의 화살표를 눌러 날짜를 선택합니다.

4. **OK(확인)**를 누릅니다.

기본 폴더가 아닌 다른 폴더에 저장된 세션 표시

1. Live Messenger History View 에서 **Advanced Filter(고급 필터)** 아이콘을 누릅니다.

2. **Use an alternate history files folder(다른 기록 파일 폴더 사용)**의 확인란을 선택합니다.

3. 폴더 위치를 입력하거나 **Browse(찾아보기)**를 눌러 폴더를 찾습니다.

4. **OK(확인)**를 누릅니다.

고급 작업

다른 컴퓨터로 Privacy Manager 인증서 및 신뢰할 수 있는 연락처 마이그레이션

Privacy Manager 인증서 및 신뢰할 수 있는 연락처를 다른 컴퓨터로 안전하게 마이그레이션하거나 안전하게 보관하기 위해 백업할 수 있습니다. 암호로 보호된 파일 형태로 네트워크 위치나 이동식 저장 장치로 데이터를 백업한 다음 해당 파일을 새 컴퓨터로 복원하면 됩니다.

Privacy Manager 인증서 및 신뢰할 수 있는 연락처 백업

암호로 보호된 파일로 Privacy Manager 인증서 및 신뢰할 수 있는 연락처를 백업하려면 다음과 같이 하십시오.

1. Privacy Manager 를 열고 **마이그레이션**을 누릅니다.
2. **백업**을 누릅니다.
3. 데이터 선택 페이지에서 마이그레이션 파일에 포함할 데이터 범주를 선택한 후 **다음**을 누릅니다.
4. 마이그레이션 파일 페이지에서 파일 이름을 입력하거나 **찾아보기**를 눌러 위치를 찾은 후 **다음**을 누릅니다.
5. 암호를 입력하고 확인한 후 **다음**을 누릅니다.

주: 마이그레이션 파일을 복원할 때 암호가 필요하므로 암호를 안전한 곳에 보관하십시오.

6. 선택한 보안 로그온 방법을 사용하여 인증합니다.
7. 마이그레이션 파일 저장 완료 페이지에서 **마침**을 누릅니다.

Privacy Manager 인증서 및 신뢰할 수 있는 연락처 복원

Privacy Manager 인증서 및 신뢰할 수 있는 연락처를 마이그레이션 과정의 일부로 다른 컴퓨터에서 또는 동일한 컴퓨터로 복원하려면 다음과 같이 하십시오.

1. Privacy Manager 를 열고 **마이그레이션**을 누릅니다.
2. **복원**을 누릅니다.
3. 마이그레이션 파일 페이지에서 **찾아보기**를 눌러 파일을 찾은 후 **다음**을 누릅니다.
4. 백업 파일을 만들 때 사용했던 암호를 입력한 후 **다음**을 누릅니다.
5. 마이그레이션 파일 페이지에서 **마침**을 누릅니다.

Privacy Manager 의 중앙 관리

Privacy Manager 설치는 관리자에 의해 사용자 정의된 중앙화된 설치의 일부일 수 있습니다. 다음 중 하나 이상의 기능은 활성화 또는 비활성화되었을 수 있습니다.

- **인증서 사용 정책**—귀하는 Comodo 에서 발행하는 Privacy Manager 인증서의 사용이 제한되어 있거나 다른 인증 기관에서 발행한 디지털 인증서의 사용이 허용되어 있을 수 있습니다.
- **암호화 정책**—암호화 기능이 Microsoft Office 또는 Outlook 및 Windows Live Messenger 에서 개별적으로 활성화 또는 비활성화되어 있을 수 있습니다.

10 HP ProtectTools File Sanitizer

File Sanitizer 는 컴퓨터에서 자산(개인 정보 또는 파일, 기록 데이터/웹 관련 데이터 또는 다른 데이터 구성 요소)을 안전하게 파쇄하고 하드 드라이브를 정기적으로 블리치하는 데 사용되는 도구입니다.

주: 이 버전의 File Sanitizer 는 시스템 하드 드라이브만 지원합니다.

파쇄

File Sanitizer 를 사용하여 자산을 파쇄할 때 데이터를 가리는 알고리즘이 나타나 원래 자산을 가상으로 검색하지 못하게 한다는 점에서 파쇄는 File Sanitizer 에서는 기본 삭제로도 알려진 일반적인 Windows® 삭제와 다릅니다. Windows 기본 삭제는 하드 드라이버의 파일 또는 자산을 원래 상태로 두거나 파일 또는 자산을 복구하기 위해 수사적인 방법을 사용할 수 있는 상태로 둡니다.

높은 보안, 중간 보안, 낮은 보안의 파쇄 프로파일을 선택한 경우 파쇄에 대해 미리 정의된 자산 목록 및 제거 방법이 자동으로 선택됩니다. 또한 파쇄 주기 횟수, 파쇄할 자산, 파쇄하기 전에 확인할 자산 및 파쇄에서 제외할 자산 등을 지정할 수 있는 파쇄 프로파일을 사용자 정의할 수 있습니다. 자세한 내용은 68페이지의 파쇄 프로필 선택 또는 생성을 참조하십시오.

자동 파쇄 일정을 설정할 수 있으며 원할 때 언제든지 수동으로 자산을 파쇄할 수도 있습니다. 자세한 내용은 67페이지의 파쇄 예약 설정, 71페이지의 단일 자산 수동 파쇄 또는 71페이지의 모든 항목 수동 파쇄를 참조하십시오.

주: .dll 파일은 해당 파일이 휴지통으로 옮겨진 경우에만 시스템에서 파쇄 및 제거할 수 있습니다.

여유 공간 블리치

Windows 에서 자산을 삭제해도 하드 드라이브에 있는 자산의 내용이 완전히 제거되지는 않습니다. Windows 에서는 자산에 대한 참조만 제거합니다. 하드 드라이브의 동일한 영역에 새로운 정보를 가진 다른 자산을 덮어쓸 때까지 해당 자산의 내용은 계속 남아 있습니다.

여유 공간 블리치를 사용하면 삭제된 자산에 임의의 데이터를 안전하게 덮어쓸 수 있어 사용자가 삭제된 자산의 원래 내용을 볼 수 없도록 할 수 있습니다.

주: 여유 공간 블리치는 휴지통을 사용하여 제거하는 자산이나 수동으로 제거하는 자산을 위한 작업입니다. 여유 공간 블리치는 파쇄된 자산에 대한 추가적인 보안을 제공하지 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. 자세한 내용은 67페이지의 여유 공간 블리치 예약 설정 또는 72페이지의 여유 공간 블리치 수동 활성화를 참조하십시오.

설치 절차

File Sanitizer 열기

File Sanitizer 를 열려면 다음과 같이 하십시오.

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

또는

▲ 바탕 화면에서 **File Sanitizer** 아이콘을 두 번 누릅니다.

또는

▲ 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer**, **File Sanitizer 열기**를 차례로 누릅니다.

파쇄 예약 설정

주: 미리 정의된 파쇄 프로파일을 선택하거나 파쇄 프로파일 만들기에 대한 자세한 내용은 68페이지의 파쇄 프로필 선택 또는 생성을 참조하십시오.

주: 수동으로 자산 파쇄하기에 대한 자세한 내용은 71페이지의 단일 자산 수동 파쇄를 참조하십시오.

1. File Sanitizer 를 열고 **파쇄**를 누릅니다.
2. 파쇄 옵션을 선택합니다.
   - **Windows 종료**—Windows 를 종료할 때 모든 선택한 자산을 파쇄하려면 이 옵션을 선택합니다.

     주: 이 옵션을 선택하면 종료할 때 선택한 자산 파쇄를 계속할지 또는 이 절차를 건너뛸지 여부를 묻는 대화 상자가 나타납니다. **예**를 눌러 파쇄 절차를 건너뛰거나 **아니요**를 눌러 파쇄를 계속합니다.
   - **웹 브라우저 열기**—웹 브라우저를 열 때 브라우저 URL 히스토리와 같은 선택한 웹 관련 자산을 모두 파쇄하려면 이 옵션을 선택합니다.
   - **웹 브라우저 종료**—웹 브라우저를 닫을 때 브라우저 URL 히스토리와 같은 선택한 웹 관련 자산을 모두 파쇄하려면 이 옵션을 선택합니다.
   - **키 시퀀스**—키 시퀀스를 사용하여 파쇄를 초기화하려면 이 옵션을 선택합니다.
   - **스케줄러**—**스케줄러 활성화** 확인란을 선택하여 Windows 암호를 입력한 다음 선택한 자산을 파쇄할 날짜 및 시간을 입력합니다.

   주: .dll 파일은 해당 파일이 휴지통으로 옮겨진 경우에만 시스템에서 파쇄 및 제거할 수 있습니다.
3. **적용**을 누른 다음 **확인**을 누릅니다.

여유 공간 블리치 예약 설정

주: 여유 공간 블리치는 휴지통을 사용하여 제거하는 자산이나 수동으로 제거하는 자산을 위한 작업입니다. 여유 공간 블리치는 파쇄된 자산에 대한 추가적인 보안을 제공하지 않습니다.

여유 공간 블리치 예약을 설정하려면 다음과 같이 하십시오.

1. File Sanitizer 를 열고 **여유 공간 블리치**를 누릅니다.
2. **스케줄러 활성화** 확인란을 선택하고 Windows 암호를 입력한 다음 하드 드라이브를 블리치할 날짜와 시간을 입력합니다.
3. **적용**을 누른 다음 **확인**을 누릅니다.

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

파쇄 프로필 선택 또는 생성

미리 정의된 프로필을 선택하거나 고유한 프로필을 생성하면 파쇄할 자산을 선택하고 제거 방법을 지정할 수 있습니다.

미리 정의된 파쇄 프로필 선택

미리 정의된 파쇄 프로필(높은 보안, 중간 보안 또는 낮은 보안)을 선택하면 미리 정의된 자산 목록 및 삭제 방법이 자동으로 선택됩니다. **세부 정보 보기** 버튼을 누르면 파쇄를 위해 선택된 미리 정의된 자산 목록을 볼 수 있습니다.

미리 정의된 파쇄 프로필을 선택하려면 다음과 같이 하십시오.

1. File Sanitizer 를 열고 **설정**을 누릅니다.
2. 미리 정의된 파쇄 프로필을 누릅니다.
3. **세부 정보 보기**를 누르면 파쇄하도록 선택된 자산 목록을 볼 수 있습니다.
4. **다음 자산을 파쇄**에서 파쇄하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.
5. **적용**을 누른 다음 **확인**을 누릅니다.

파쇄 프로필 사용자 정의

파쇄 프로필을 생성할 때 파쇄 주기, 파쇄할 자산, 파쇄하기 전에 확인할 자산, 파쇄하지 않을 자산을 각각 지정할 수 있습니다.

1. File Sanitizer 를 열고 **설정**, **고급 보안 설정**, **세부 정보 보기**를 차례로 누릅니다.
2. 파쇄 주기를 지정합니다.

주: 선택한 파쇄 주기의 횟수는 각 자산마다 실행됩니다. 예를 들면 파쇄 주기를 3 번으로 선택한 경우 데이터를 가리는 알고리즘은 개별적으로 3 번 실행됩니다. 높은 보안 파쇄 주기를 선택하면 파쇄를 하는 데 시간이 상당히 오래 걸릴 수 있지만, 파쇄 주기 횟수를 높게 지정할수록 그만큼 데이터가 검색될 확률이 낮아집니다.

3. 다음 방법을 통해 파쇄하려는 자산을 선택합니다.
   a. **사용 가능한 파쇄 옵션**에서 자산을 선택한 다음 **추가**를 누릅니다.
   b. 사용자 정의 자산을 추가하려면 **사용자 정의 옵션 추가**를 누른 다음 해당 파일 또는 폴더가 있는 경로를 찾거나 입력합니다. **열기**를 누른 다음 **확인**을 누릅니다. **사용 가능한 파쇄 옵션**에서 사용자 정의 자산을 누른 다음 **추가**를 누릅니다.

주: 사용 가능한 파쇄 옵션에서 자산을 삭제하려면 해당 자산을 누른 다음 **삭제**를 누릅니다.

4. **다음 자산을 파쇄**에서 파쇄하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.

주: 파쇄 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **제거**를 누릅니다.

5. 파일 또는 폴더가 자동 파쇄되지 않도록 설정하려면 **다음 자산을 파쇄하지 않음**에서 **추가**를 누른 다음 해당 파일 또는 폴더가 있는 경로를 찾거나 입력합니다. **열기**를 누른 다음 **확인**을 누릅니다.

주: 차단 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **삭제**를 누릅니다.

6. 파쇄 프로필 구성을 완료하면 **적용**을 누른 다음 **확인**을 누릅니다.

기본 삭제 프로필 사용자 정의

기본 삭제 프로파일은 파쇄를 하지 않고 표준 자산 삭제를 수행합니다. 기본 삭제 프로파일을 사용자 정의할 때에는 기본 삭제할 자산, 기본 삭제하기 전에 확인할 자산, 기본 삭제에서 제외할 자산 등을 지정합니다.

주: 기본 삭제 옵션을 사용하는 경우 수동으로 삭제한 자산이나 Windows 휴지통을 통해 삭제한 자산에 대해 때때로 여유 공간 블리치 기능을 사용할 수 있습니다.

기본 삭제 프로파일을 사용자 정의하려면 다음과 같이 하십시오.

1. File Sanitizer 를 열고 **설정**, **기본 삭제 설정**, **세부 정보 보기**를 차례로 누릅니다.
2. 다음 방법을 통해 삭제하려는 자산을 선택합니다.
   a. **사용 가능한 삭제 옵션**에서 삭제하려는 자산을 누른 다음 **추가**를 누릅니다.
   b. 사용자 정의 자산을 추가하려면 **사용자 정의 추가 옵션**을 누르고 파일 이름이나 폴더 이름을 입력한 다음 **확인**을 누릅니다. 추가하려는 사용자 정의 자산을 누른 다음 **추가**를 누릅니다.

주: 사용 가능한 삭제 옵션에서 자산을 삭제하려면 삭제하려는 자산을 누른 다음 **삭제**를 누릅니다.

3. **다음 자산을 삭제**에서 삭제하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.

주: 삭제 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **제거**를 누릅니다.

4. **다음 자산을 삭제하지 않음**에서 **추가**를 눌러 삭제하지 않으려는 특정 자산을 선택합니다.

주: 차단 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **삭제**를 누릅니다.

5. 기본 삭제 프로필 구성을 완료하면 **적용**을 누른 다음 **확인**을 누릅니다.

일반 작업

File Sanitizer 를 사용하여 다음 작업을 수행할 수 있습니다.

- 키 시퀀스를 사용하여 파쇄 시작—이 기능을 사용하면 파쇄를 시작하는 키 시퀀스(예: ctrl+alt+s)를 생성할 수 있습니다. 자세한 내용은 70페이지의 키 시퀀스를 사용하여 파쇄 시작을 참조하십시오.
- File Sanitizer 아이콘을 사용하여 파쇄 시작—이 기능은 Windows 의 끌어서 놓기 기능과 유사합니다. 자세한 내용은 71페이지의 File Sanitizer 아이콘 사용을 참조하십시오.
- 특정 자산 또는 선택한 모든 자산을 수동으로 파쇄—이 기능을 사용하면 항목을 수동으로 파쇄할 수 있어 정기적인 파쇄 예약이 실행될 때까지 기다릴 필요가 없습니다. 자세한 내용은 71페이지의 단일 자산 수동 파쇄 또는 71페이지의 모든 항목 수동 파쇄를 참조하십시오.
- 여유 공간 블리치를 수동으로 활성화—이 기능을 사용하면 여유 공간 블리치를 수동으로 활성화할 수 있습니다. 자세한 내용은 72페이지의 여유 공간 블리치 수동 활성화를 참조하십시오.
- 파쇄 또는 여유 공간 블리치 작업 중단—이 기능을 사용하면 파쇄 또는 여유 공간 블리치 작업을 중지할 수 있습니다. 자세한 내용은 72페이지의 파쇄 또는 여유 공간 블리치 작업 중단을 참조하십시오.
- 로그 파일 보기—이 기능을 사용하여 마지막 파쇄 및 여유 공간 블리치 작업 시 오류가 발생한 파쇄 및 여유 공간 블리치에 대한 로그 파일을 볼 수 있습니다. 자세한 내용은 72페이지의 로그 파일 보기를 참조하십시오.

주: 파쇄 또는 여유 공간 블리치 작업에 상당히 오랜 시간이 걸릴 수 있습니다. 파쇄 및 여유 공간 블리치를 백그라운드 작업으로 수행하더라도 프로세스 사용량이 증가하여 컴퓨터가 느려질 수 있습니다.

키 시퀀스를 사용하여 파쇄 시작

키 시퀀스를 지정하려면 다음과 같이 하십시오.

1. File Sanitizer 를 열고 **파쇄**를 누릅니다.
2. **키 시퀀스** 확인란을 선택합니다.
3. 텍스트 상자에 문자를 입력합니다.
4. **CTRL** 확인란 또는 **ALT** 확인란을 선택한 다음 **SHIFT** 상자를 선택합니다.

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

주: 키 시퀀스 선택은 키 시퀀스를 직접 구성하는 것과 다릅니다.

키 시퀀스를 사용하여 파쇄를 시작하려면 다음과 같이 하십시오.

1. shift 키 및 ctrl 키 또는 alt 키(또는 직접 지정한 키 조합)를 누른 상태에서 선택한 문자를 누릅니다.
2. 확인 대화 상자가 표시되면 **예**를 누릅니다.

File Sanitizer 아이콘 사용

△ 주의: 파쇄된 자산은 복구할 수 없습니다. 수동 파쇄할 항목을 선택할 때에는 신중을 기하십시오.

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

단일 자산 수동 파쇄

△ 주의: 파쇄된 자산은 복구할 수 없습니다. 수동 파쇄할 항목을 선택할 때에는 신중을 기하십시오.

1. 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer**, **단일 자산 파쇄**를 차례로 누릅니다.
2. 찾아보기 대화 상자가 열리면 파쇄하려는 자산으로 이동한 다음 **확인**을 누릅니다.

   주: 선택한 자산은 하나의 파일 또는 폴더일 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 파쇄하려는 자산으로 이동한 다음 **확인**을 누릅니다.
3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

또는

1. File Sanitizer 를 열고 **파쇄**를 누릅니다.
2. **찾아보기** 버튼을 누릅니다.
3. 찾아보기 대화 상자가 열리면 파쇄하려는 자산으로 이동한 다음 **확인**을 누릅니다.
4. 확인 대화 상자가 표시되면 **예**를 누릅니다.

모든 항목 수동 파쇄

1. 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer**, **지금 파쇄**를 차례로 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.

또는

1. File Sanitizer 를 열고 **파쇄**를 누릅니다.
2. **지금 파쇄** 버튼을 누릅니다.
3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

여유 공간 블리치 수동 활성화

1. 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **File Sanitizer**, **지금 블리치**를 차례로 누릅니다.
2. 확인 대화 상자가 표시되면 **예**를 누릅니다.

또는

1. File Sanitizer 를 열고 **여유 공간 블리치**를 누릅니다.
2. **지금 블리치**를 누릅니다.
3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

파쇄 또는 여유 공간 블리치 작업 중단

파쇄 또는 여유 공간 블리치 작업을 진행하는 동안 알림 영역의 HP ProtectTools Security Manager 아이콘 위에 메시지가 표시됩니다. 이 메시지에는 파쇄 또는 여유 공간 블리치 프로세스(진행률)에 대한 세부 정보와 작업 중단 옵션이 제공됩니다.

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.

주: 파쇄되거나 블리치된 파일은 로그 파일에 기록되지 않습니다.

파쇄 작업에 로그 파일을 하나 만들고 여유 공간 블리치 작업에 다른 로그 파일을 하나 더 만듭니다. 두 로그 파일은 하드 드라이브의 다음 위치에 있습니다.

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

11 HP ProtectTools Device Access Manager (일부 모델만 해당)

Windows® 관리자는 HP ProtectTools Device Access Manager 를 사용해 시스템에서 장치 액세스를 통제하고 무단 액세스를 방지합니다.

- 각 사용자에 대해 장치 프로필이 만들어져 액세스가 허용된 장치인지 거부된 장치인지 보여줍니다.
- 또한 사용자를 미리 정의된 장치 관리자 그룹과 같은 그룹으로 구성하거나 제어판의 관리 도구에 있는 컴퓨터 관리 옵션으로 그룹을 정의할 수 있습니다.
- 그룹 구성원 자격을 기준으로 액세스를 허용하거나 거부할 수 있습니다.
- CD-ROM 드라이브나 DVD 드라이브와 같은 장치 클래스일 경우, 읽기 권한과 쓰기 권한을 개별적으로 허용 또는 거부할 수 있습니다.

또한 장치 액세스 제어 정책을 읽고 수정할 수 있는 권한을 제한된 사용자에게 허용할 수 있습니다.

설정 절차

Device Access Manager 열기

Device Access Manager 를 열려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP** 를 차례로 누른 다음 **HP ProtectTools 관리 콘솔**을 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 누릅니다.

장치 액세스 구성

HP ProtectTools Device Access Manager 는 세 가지 창을 지원합니다.

- "간단한 구성" 창은 장치 관리자 그룹에 속한 사용자들에게 장치 클래스 액세스를 허용하거나 거부할 때 이용합니다.
- "장치 클래스 구성" 창은 특정 사용자 또는 그룹에게 장치 또는 특정 장치 유형에 대한 액세스를 허용하거나 거부할 때 이용합니다.
- "사용자 액세스 설정" 창은 사용자가 "간단한 구성" 및 "장치 클래스 구성" 정보를 보거나 수정할 수 있도록 허용할지 여부를 지정할 때 이용합니다.

장치 관리자 그룹

Device Access Manager 를 설치하면, 장치 관리자 그룹이 만들어집니다.

시스템 관리자는 간단한 장치 액세스 통제 정책을 마련해 사용자가 (장치 액세스에 대해) 신뢰할 수 있는 사용자로 분류되지 않는 한 장치 클래스 액세스를 거부할 수 있습니다. "신뢰할 수 있는 장치" 사용자와 "신뢰할 수 없는 장치" 사용자를 구별할 수 있는 좋은 방법은 "신뢰할 수 있는" 장치 사용자를 모두 장치 관리자 그룹에 포함시켜 놓는 것입니다. 간단한 구성이나 장치 클래스 구성 창을 통해 장치 관리자 그룹에 속한 사용자에게 장치 액세스 권한을 부여하면, "신뢰할 수 있는 장치" 사용자가 지정 장치 클래스에 완전하게 액세스할 수 있습니다.

주: 장치 관리자 그룹에 사용자를 추가한다고 해서 그 사용자에게 장치 액세스 권한이 자동으로 주어지는 것은 아닙니다. 하지만, 간단한 구성 창을 이용해 "신뢰할 수 있는 장치" 사용자에게 필요한 장치 클래스에 대한 액세스 권한을 부여할 수 있습니다.

장치 관리자 그룹에 사용자를 추가하려면, 다음과 같이 하십시오.

- Windows 7, Vista, XP Professional 인 경우, 표준 "로컬 사용자 및 그룹" MMC 스냅인을 사용하십시오.
- Windows 7, Vista®, XP 의 Home 버전인 경우, 권한이 있는 계정으로부터 명령 프롬프트 창에 다음과 같이 입력합니다.

  c:\> net localgroup “Device Administrators” username /ADD

기본 구성

관리자와 권한이 있는 사용자는 간단한 구성 창을 이용해 장치 관리자 외 모든 사용자에게 다음과 같은 장치 클래스에 대한 액세스 권한을 수정할 수 있습니다.

주: 사용자든 그룹이든 이 창을 이용해 장치 액세스 정보를 확인할 수 있으려면, **사용자 액세스 설정** 창에서 "읽기" 권한을 받아야 합니다. 사용자든 그룹이든 이 창을 이용해 장치 액세스 정보를 수정할 수 있으려면, **사용자 액세스 설정** 창에서 "변경" 권한을 받아야 합니다.

- 모든 이동식 미디어(디스켓, USB 플래스 드라이브 등)
- 모든 DVD/CD-ROM 드라이브
- 모든 직렬 및 병렬 포트
- 모든 Bluetooth® 장치
- 모든 적외선 장치
- 모든 모뎀 장치
- 모든 PCMCIA 장치
- 모든 1394 장치

장치 관리자 외의 모든 사용자에 대해 장치 클래스의 액세스를 허용하거나 거부하려면 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **간단한 구성**을 누릅니다.
2. 오른쪽 창에서, 액세스를 거부하려면 장치 클래스나 특정 장치에 해당하는 확인란을 선택합니다. 그 장치 클래스나 특정 장치에 대한 액세스를 허용하려면 이 확인란을 선택 해제합니다.

   확인란이 회색으로 변하면 장치 클래스 구성 창에서 액세스 상황에 영향을 미치는 값이 바뀐 것입니다. 이 값을 다시 간단한 설정으로 재설정하려면, 확인란을 눌러 설정하거나 설정을 해제한 다음 **예**를 눌러 확인합니다.
3. **저장** 아이콘을 누릅니다.

   주: 배경 서비스가 실행되고 있지 않다면, 대화상자가 열려 이 서비스를 시작할 것인지 묻습니다. **Yes(예)**를 누릅니다.
4. **확인**을 누릅니다.

백그라운드 서비스 시작

장치 프로필을 적용하려면, 먼저 HP ProtectTools Security Manager 에서 HP ProtectTools 장치 잠금/감사 배경 서비스를 시작할 것인지를 묻는 대화상자가 열립니다. **Yes(예)**를 누릅니다. 그러면 배경 서비스가 시작되고 시스템을 부팅할 때마다 자동으로 시작됩니다.

주: 배경 서비스 프롬프트가 나타나려면 먼저 장치 프로필을 정의해 두어야 합니다.

관리자는 이 서비스를 시작하거나 종료할 수도 있습니다.

1. **시작**, **제어판**을 차례로 누릅니다.
2. **관리 도구**, **서비스**를 차례로 누릅니다.
3. **HP ProtectTools 장치 잠금/감사** 서비스를 찾습니다.

장치 잠금/감사 서비스를 종료하더라도 장치 잠금이 종료되지 않습니다. 장치 잠금은 두 가지 구성요소에 강제 적용됩니다.

- 장치 잠금/감사 서비스
- DAMDrv.sys 드라이버

서비스를 시작하면 장치 드라이버가 시작되지만 서비스를 종료하더라도 드라이버가 종료되지 않습니다.

배경 서비스 실행 여부를 확인하려면, 명령 프롬프트 창을 열어 sc query flcdlock 을 입력합니다.

장치 드라이버 실행 여부를 확인하려면, 명령 프롬프트 창을 열어 sc query damdrv 를 입력합니다.

장치 클래스 구성

관리자와 권한을 받은 사용자는 장이 클래스나 특정 장치에 대한 액세스 권한이 허용되었거나 거부된 사용자 및 그룹 목록을 확인하고 수정할 수 있습니다.

주: 사용자든 그룹이든 이 창을 이용해 장치 액세스 정보를 확인할 수 있으려면, **사용자 액세스 설정** 창에서 "읽기" 권한을 받아야 합니다. 사용자든 그룹이든 이 창을 이용해 장치 액세스 정보를 수정할 수 있으려면, **사용자 액세스 설정** 창에서 "변경" 권한을 받아야 합니다.

장치 클래스 구성 창은 다음과 같은 섹션으로 구분되어 있습니다.

- **장치 목록**—시스템에 설치되어 있거나 이전에 시스템에 설치해 둔 모든 장치 클래스와 장치를 보여줍니다.
  - 보호는 보통 장치 클래스에 적용됩니다. 선택한 사용자나 그룹은 해당 장치 클래스에 있는 모든 장치에 액세스할 수 있습니다.
  - 특정 장치에도 보호를 적용할 수 있습니다.
- **사용자 목록**—선택한 장치 클래스나 특정 장치에 대해 액세스가 허용되었거나 거부된 모든 사용자 및 그룹을 보여줍니다.
  - 사용자 목록에는 특정 사용자를 입력할 수도 있고 그 사용자가 속해 있는 그룹을 입력할 수도 있습니다.
  - 사용자 목록에 있는 사용자나 그룹을 이용할 수 없다면, 장치 목록에 있는 장치 클래스로부터 또는 'Class' 폴더로부터 설정이 상속된 것입니다.
  - DVD 나 CD-ROM 등 일부 장치 클래스는 읽기와 쓰기 명령 권한을 개별적으로 허용하거나 거부함으로써 한층 더 강력히 통제할 수 있습니다.

    다른 장치와 클래스에는 읽기 및 쓰기 권한이 상속될 수 있습니다. 이를 테면, 보다 높은 클래스에서 읽기 액세스를 상속 받을 수 있지만 어느 사용자나 그룹에게는 쓰기 권한을 부여하지 않을 수도 있습니다.

    주: '읽기' 확인란을 비워두면, 액세스 통제 항목이 장치에 대한 읽기 권한에 영향을 미치지 못합니다. 장치에 대한 읽기 권한을 부여하지도 거부하지도 않습니다.

    예 1—어느 사용자나 그룹이 장치나 장치 클래스에 대한 쓰기 권한을 거부 당한 경우:

    이 사용자나 그룹 또는 같은 그룹에 속해 있는 사용자는 장치 계층에서 이 장치 아래 있는 장치에 대해서만 쓰기 권한이나 읽기+쓰기 권한을 받을 수 있습니다.

    예 2—어느 사용자나 그룹이 장치나 장치 클래스에 대한 쓰기 권한을 부여 받은 경우:

이 사용자나 그룹 또는 같은 그룹에 속해 있는 사용자는 해당 장치나 장치 계층에서 이 장치 아래 있는 장치에 대해서만 쓰기 권한이나 읽기+쓰기 권한을 거부 당할 수 있습니다.

예 3—어느 사용자나 그룹이 장치나 장치 클래스에 대한 읽기 권한을 부여 받은 경우:

이 사용자나 그룹 또는 같은 그룹에 속해 있는 사용자는 해당 장치나 장치 계층에서 이 장치 아래 있는 장치에 대해서만 읽기 권한이나 읽기+쓰기 권한을 거부 당할 수 있습니다.

예 4—어느 사용자나 그룹이 장치나 장치 클래스에 대한 읽기 권한을 거부 당한 경우:

이 사용자나 그룹 또는 같은 그룹에 속해 있는 사용자는 장치 계층에서 이 장치 아래 있는 장치에 대해서만 읽기 권한이나 읽기+쓰기 권한을 받을 수 있습니다.

예 5—어느 사용자나 그룹이 장치나 장치 클래스에 대한 읽기+쓰기 권한을 부여 받은 경우:

이 사용자나 그룹 또는 같은 그룹에 속해 있는 사용자는 해당 장치나 장치 계층에서 이 장치 아래 있는 장치에 대해서만 쓰기 권한이나 읽기+쓰기 권한을 거부 당할 수 있습니다.

예 6—어느 사용자나 그룹이 장치나 장치 클래스에 대한 읽기+쓰기 권한을 거부 당한 경우:

이 사용자나 그룹 또는 같은 그룹에 속해 있는 사용자는 장치 계층에서 이 장치 아래 있는 장치에 대해서만 읽기 권한이나 읽기+쓰기 권한을 받을 수 있습니다.

사용자나 그룹에 대한 액세스 거부

어느 사용자나 그룹이 장치나 장치 클래스에 액세스하지 못하도록 하려면, 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 구성할 장치 클래스를 누릅니다.
   - 장치 클래스
   - 모든 장치
   - 개별 장치
3. **사용자/그룹** 아래에서 액세스를 거부할 사용자나 그룹을 누릅니다.
4. 사용자나 그룹 옆에 있는 **거부**를 누릅니다.
5. **저장** 아이콘을 누릅니다.

주: 어느 사용자에 대해 동일 장치 레벨에서 거부 및 허용 설정이 모두 설정되어 있다면, 액세스 거부가 액세스 허용에 우선합니다.

사용자나 그룹에 액세스 허용

어느 사용자나 그룹이 장치나 장치 클래스에 액세스할 수 있도록 허용하려면, 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 다음 중 하나를 누릅니다.
   - 장치 클래스
   - 모든 장치
   - 개별 장치
3. **추가**를 누릅니다.

   그러면 **사용자 또는 그룹 선택** 대화상자가 열립니다.
4. **고급**을 누른 다음 **지금 찾기**를 눌러 사용자나 그룹을 찾아 추가합니다.
5. 가용 사용자 및 그룹 목록에 추가할 사용자나 그룹을 누르고 **확인**을 누릅니다.
6. **확인**을 다시 누릅니다.
7. **허용**을 눌러 해당 사용자나 그룹에게 액세스를 허용합니다.
8. **저장** 아이콘을 누릅니다.

사용자나 그룹에서 액세스 제거

어느 사용자나 그룹에서 장치나 장치 클래스에 액세스할 수 있는 권한을 제거하려면, 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 구성할 장치 클래스를 누릅니다.
   - 장치 클래스
   - 모든 장치
   - 개별 장치
3. **사용자/그룹** 아래서 제거하려는 사용자나 그룹을 누르고 **제거**를 누릅니다.
4. **저장** 아이콘을 누릅니다.

그룹의 한 사용자에 대해 장치 클래스에 대한 액세스 허용

어느 사용자 한 명에게는 장치 클래스에 대한 액세스를 허용하면서 이 사용자가 속한 그룹의 나머지 사용자들에게는 액세스를 거부하려면, 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 구성할 장치 클래스를 누릅니다.
   - 장치 클래스
   - 모든 장치
   - 개별 장치
3. **사용자/그룹** 아래에서 액세스를 거부하려는 그룹을 선택한 다음 **거부**를 누릅니다.
4. 해당 클래스 아래의 폴더로 이동한 다음 특정 사용자를 추가합니다.
5. **허용**을 눌러 해당 사용자에게 액세스 권한을 부여합니다.
6. **저장** 아이콘을 누릅니다.

그룹의 한 사용자에 대해 특정 장치에 대한 액세스 허용

관리자는 특정 장치에 대해 그룹의 한 사용자에게만 액세스를 허용하고, 해당 클래스의 모든 장치에 대해 해당 그룹의 나머지 사용자에 대해서는 액세스를 거부할 수 있습니다.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 구성할 장치 클래스를 누른 다음 그 아래의 폴더로 이동합니다.
3. **추가**를 누릅니다. 그러면 **사용자 또는 그룹 선택** 대화상자가 열립니다.
4. **고급**을 누른 다음 **지금 찾기**를 눌러 클래스의 모든 장치에 대한 액세스를 거부하려는 사용자 그룹을 검색합니다.
5. 해당 그룹을 누르고 **확인**을 누릅니다.
6. 장치 클래스 아래에서 사용자에게 액세스를 허용하려는 특정 장치를 찾습니다.
7. **추가**를 누릅니다. 그러면 **사용자 또는 그룹 선택** 대화상자가 열립니다.
8. **고급**을 누른 다음 **지금 찾기**를 눌러 사용자나 그룹을 찾아 추가합니다.
9. 액세스를 허용할 사용자를 누른 다음 **확인**을 누릅니다.
10. **허용**을 눌러 해당 사용자에게 액세스 권한을 부여합니다.
11. **저장** 아이콘을 누릅니다.

구성 재설정

△ **주의:** 구성을 변경하면 이전에 가해진 모든 장치 구성 변경 사항이 취소되고 모든 설정이 제조 시 기본값으로 되돌아갑니다.

구성 설정을 제조 시 기본값으로 재설정하려면 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **장치 클래스 구성**을 누릅니다.
2. **재설정** 버튼을 누릅니다.
3. **예**를 눌러 확인합니다.
4. **저장** 아이콘을 누릅니다.

고급 작업

구성 설정에 대한 액세스 통제

사용자 액세스 설정 창에서, 관리자는 "간단한 구성" 페이지와 "장치 클래스 구성" 페이지를 사용할 수 있도록 허용할 그룹이나 사용자를 지정합니다.

주: 사용자나 그룹은 "최대 사용자 관리자 권한"이 있어야만 사용자 액세스 설정 창에서 설정을 변경할 수 있습니다.

- 사용자나 그룹은 사용자 액세스 설정 창에서 "구성 설정 보기(읽기 전용)" 권한을 받아야만 "간단한 구성"과 "장치 클래스 구성" 정보를 확인할 수 있습니다.
- 사용자나 그룹은 사용자 액세스 설정 창에서 "구성 설정 변경" 권한을 받아야만 "간단한 구성"과 "장치 클래스 구성" 정보를 변경할 수 있습니다.

주: 관리자 그룹에 속한 사용자라도 "간단한 구성" 및 "장치 클래스 구성" 창을 보려면 "읽기" 권한이 있어야 하고 "간단한 구성" 및 "장치 클래스 구성" 창을 이용해 데이터를 변경하려면 "변경" 권한이 있어야 합니다.

주: 모든 사용자 및 그룹의 액세스 레벨을 평가한 다음, 어느 사용자에게 특정 액세스 레벨을 허용하지도 거부하지도 않았다면 그 사용자는 해당 레벨에 대한 액세스가 거부됩니다.

기존 그룹이나 사용자에게 액세스 허용

기존 그룹이나 사용자에게 구성 설정을 확인하거나 변경할 수 있는 권한을 허용하려면 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **사용자 액세스 설정**을 누릅니다.
2. 액세스를 허용할 그룹이나 사용자를 누릅니다.
3. **권한** 아래에서, 선택한 그룹이나 사용자에게 허용할 각 권한 유형에 대해 **허용**을 누릅니다.

   주: 허용된 권한은 누적됩니다. 예를 들어, “구성 설정 변경” 권한을 받은 사용자에게는 “구성 설정 보기(읽기 전용)” 권한도 자동으로 부여됩니다. “최대 사용자 관리자 권한”을 받은 사용자에게는 “구성 설정 변경”과 “구성 설정 보기(읽기 전용)” 권한도 함께 부여됩니다.

   - 최대 사용자 관리자 권한
   - 구성 설정 변경
   - 구성 설정 보기(읽기 전용)
4. **저장** 아이콘을 누릅니다.

기존 그룹이나 사용자에게 액세스 거부

기존 그룹이나 사용자에게 구성 설정을 확인하거나 변경할 수 있는 권한을 거부하려면 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **사용자 액세스 설정**을 누릅니다.
2. 액세스를 거부할 그룹이나 사용자를 누릅니다.

3. **권한** 아래에서, 선택한 그룹이나 사용자에게 거부할 각 권한 유형에 대해 **거부**를 누릅니다.
   - 최대 사용자 관리자 권한
   - 구성 설정 변경
   - 구성 설정 보기(읽기 전용)
4. **저장** 아이콘을 누릅니다.

새 그룹 또는 사용자 추가

새 그룹이나 사용자에게 구성 설정을 확인하거나 변경할 수 있는 권한을 허용하려면 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **사용자 액세스 설정**을 누릅니다.
2. **추가**를 누릅니다. 그러면 **사용자 또는 그룹 선택** 대화상자가 열립니다.
3. **고급**을 누른 다음 **지금 찾기**를 눌러 사용자나 그룹을 찾아 추가합니다.
4. 그룹이나 사용자를 누르고 **확인**을 누른 다음 **확인**을 다시 한 번 누릅니다.
5. **허용**을 눌러 해당 사용자에게 액세스 권한을 부여합니다.
6. **저장** 아이콘을 누릅니다.

그룹 또는 사용자 액세스 제거

그룹이나 사용자로부터 구성 설정을 확인하거나 변경할 수 있는 권한을 제거하려면 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**의 왼쪽 창에서 **Device Access Manager** 를 누르고 **사용자 액세스 설정**을 누릅니다.
2. 그룹이나 사용자를 누른 다음 **제거**를 누릅니다.
3. **저장** 아이콘을 누릅니다.

관련 자료

HP ProtectTools Device Access Manager 는 엔터프라이즈 제품 HP ProtectTools Enterprise Device Access Manager 와 호환됩니다. 이 엔터프라이즈 제품을 함께 사용하면, HP ProtectTools Device Access Manager 에서는 자체 기능에 대한 읽기 전용 액세스를 허용합니다.

HP ProtectTools Device Access Manager 에 대한 자세한 내용은 http://www.hp.com/hps/security/products 에서 확인하십시오.

12 HP ProtectTools 용 LoJack Pro

Absolute Software 의 Computrace 제품군을 사용하면 HP 컴퓨터를 추적하고 데이터 보호를 강화할 수 있습니다. 또한, Computrace LoJack 제품은 도난 컴퓨터 복구 작업에서의 기계적 손실 및 지원을 감소시킵니다.

Computrace 제품을 활성화하려면 다음과 같이 하십시오.

1. **시작**을 누르고 **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.
2. **Theft Recovery(도난 복구)**를 누른 다음 **Activate Now(지금 활성화)**를 누릅니다.

   HP ProtectTools 에서 사용할 수 있는 세 가지의 Computrace 제품 중의 하나를 선택하고 구입할 수 있는 가입 웹 사이트가 열립니다.

   - **Computrace Data Delete**—원격 데이터 삭제, 장치 결빙 및 기본 자료 추적 및 보고
   - **Computrace LoJack Pro**—원격 데이터 삭제, 장치 결빙, 기본 자료 추적 및 보고, 관리 도난 복구
   - **Computrace LoJack Pro Premium**—원격 데이터 삭제, 장치 결빙, 고급 자료 추적 및 보고, 관리 도난 복구, 지오로케이션 및 지오펜싱

컴퓨터가 배송될 때, Computrace Agent 가 꺼져 있더라도 Computrace Agent 는 HP 비즈니스 노트북의 BIOS 에 내장되어 있습니다. 가입 등록권을 구입하면 Agent 가 활성화됩니다. 내장 Agent 는 운영 체제를 다시 설치하고 하드 드라이브를 다시 포맷할 수 있습니다.

주: 가입 기간은 1 년부터 5 년까지 있습니다. 자세한 내용은 Absolute Software 가입 계약서를 참고하십시오. 일부 지역에서는 복구 기능을 이용하지 못할 수도 있습니다. WWAN 옵션이 설정된 일부 모델에서는 GPS 추적이 지원됩니다.

13 문제 해결

HP ProtectTools Security Manager

증상	설명	해결 방법
스마트 카드와 USB 토큰을 Security Manager 설치 후에 설치했다면 Security Manager 에서 이 스마트 카드와 USB 토큰을 사용할 수 없습니다.	Security Manager 에서 스마트 카드나 USB 토큰을 사용하려면, Security Manager 를 설치하기 전에 지원 소프트웨어(드라이버, PKCS#11 공급자 등)를 설치해야 합니다. Security Manager 를 이미 설치해 두었다면 스마트 카드나 토큰 지원 소프트웨어를 설치한 후 다음 절차를 따르십시오.	Password Manager 에 로그온 하십시오. HP ProtectTools Security Manager 에서 **Password Manager**, **자격증명**, **스마트 카드**를 차례로 누릅니다. 메시지가 표시되면 컴퓨터를 재시작합니다.
일부 응용프로그램 웹 페이지에서 사용자의 작업 수행 또는 완료를 중단하는 오류가 발생함	일부 웹 기반 응용프로그램에서 SSO (Single Sign On) 기능 패턴의 비활성화로 인해 작동이 중지되고 오류가 보고됩니다. 예를 들어, Internet Explorer 에서 오류가 발생했음을 나타내는 노란색 삼각형 느낌표(**!**)가 표시됩니다.	Security Manager Single Sign On 이 모든 소프트웨어 웹 인터페이스를 지원하는 것은 아닙니다. 특정 웹 페이지에서 SSO 지원을 비활성화하려면 SSO 지원을 해제하면 됩니다. SSO 에 대해서는 Security Manager 도움말 파일에 있는 설명을 참조하십시오. 해당 응용프로그램에 대해 비활성화할 수 없는 특정 SSO 의 경우 해당 지역 HP 서비스 및 지원 센터로 전화하여 세 번째 수준의 지원을 요청하십시오.
로그온 과정 동안 **Browse for Virtual Token(가상 토큰 탐색)** 옵션이 표시되지 않음	찾기 옵션이 제거되어 보안 위험이 낮아졌기 때문에 사용자는 Password Manager 에서 등록한 가상 토큰 위치를 옮길 수 없습니다.	무단 사용자가 이 탐색 옵션을 사용하여 파일을 삭제하고, 이름을 변경하며, Windows 를 제어할 수 있다는 문제점 때문에 제거되었습니다.
도메인 관리자에게 권한이 있는데 Windows 암호를 변경하지 못함	그러기 위해서는 도메인 관리자가 도메인에 로그온해 그 도메인과 로컬 PC 에 대한 관리자 권한이 있는 계정을 사용해 Password Manager 에서 도메인 ID 를 등록해야 합니다. 도메인 관리자가 Password Manager 에서 Windows 암호를 변경하려고 하면, 관리자에게 로그온 실패 오류로 **사용자 계정 제한**이라는 오류 메시지가 나타납니다.	Password Manager 는 **Windows 암호 변경**을 통해 도메인 사용자 계정 암호를 변경할 수 없습니다. Security Manager 는 로컬 PC 계정 암호만 변경할 수 있습니다. 도메인 사용자는 **Windows 보안**의 **암호 변경** 옵션을 통해 암호를 바꿀 수 있으나 도메일 사용자가 로컬 PC 에 물리적 계좌를 가지고 있지 않아 자격증명 관리자는 로그인할 때 사용하는 암호만 변경할 수 있습니다.
Password Manager 는 Corel WordPerfect 12 암호 GINA 와 호환되지 않습니다.	사용자가 Password Manager 에 로그온해 WordPerfect 에서 문서를 작성하고 암호와 함께 저장하면, Password Manager 가 암호 GINA 를 수동으로든 자동으로든 감지하거나 인식할 수 없습니다.	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
Password Manager 는 화면 상의 **연결** 버튼을 인식하지 못합니다.	RDP(Remote Desktop Connection)용 SSO 인증서가 **Connect(접속)**로 설정된 경우 SSO 는 다시 시작할 때 **Connect**	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.

증상	설명	해결 방법
	(접속)가 아닌 **Save As(다른 이름으로 저장)**를 표시합니다.	
Windows XP SP1 에서는 대기 모드에서 최대 절전 모드로 바뀌면 암호 관리자에 로그온할 수 없습니다.	시스템을 최대 절전 모드에서 절전 모드로 바꾼 다음에, 관리자나 사용자는 암호 과닐자에 로그온할 수 없으며 로그온 자격증명(암호, 지문, Java Card) 선택 여하를 떠나 Windows 로그온 화면이 계속 열려 있습니다.	Windows Update 로 Windows 를 서비스 팩 2 로 업데이트하십시오. 문제 원인에 관한 자세한 내용은 http://www.microsoft.com 에서 Microsoft 기술 자료 문서 813301 을 참조하십시오. 사용자는 Password Manager 를 선택해야 로그온할 수 있습니다. 사용자는 Password Manager 에 로그온한 다음 Windows 에 로그온해(Windows 로그온 옵션을 선택할 수 있음) 로그온 프로세스를 완료할 것인지를 묻는 메시지가 나타납니다. Windows 에 처음 로그온하는 사용자는 Password Manager 에 직접 로그온해야 합니다.
보안 **Restore Identity(ID 복원)** 프로세스에서 가상 토큰과의 연결이 손실됨	사용자가 ID 를 다시 저장하면, 로그온 화면에서 Password Manager 와 가상 토큰 위치와의 연결이 끊어질 수 있습니다. Password Manager 가 가상 토큰을 등록하도록 하더라도 사용자는 그 토큰을 등록해야만 연결을 복구할 수 있습니다.	이는 설계상의 이유입니다. ID 를 유지하지 않고 Security Manager 를 제거할 경우, 토큰의 시스템(서버) 파트가 파기되기 때문에, ID 복원을 통해 토큰의 클라이언트 파트를 복구하더라도 더 이상 로그온 시 그 토큰을 사용할 수 없습니다. HP 에서 장기적인 문제 해결책을 모색하고 있습니다.

HP ProtectTools Device Access Manager

Device Access Manager 내에서 사용자에게 장치에 대한 액세스를 거부했는데 사용자가 장치에 여전히 액세스할 수 있습니다.

- **설명**—Device Access Manager 내에서 단순 구성 및/또는 장치 클래스 구성을 사용하여 사용자에게 장치에 대한 액세스를 거부했습니다. 액세스가 거부된 사용자가 여전히 장치에 액세스할 수 있습니다.
- **해결 방법**
  - HP ProtectTools Device Locking 서비스가 시작되었는지 확인합니다.
  - 관리자 권한으로 **제어판**을 실행한 다음 **시스템 및 유지 관리**를 누릅니다. 관리 도구 창에서 **서비스**를 누르고 **HP ProtectTools Device Locking/Auditing** 서비스를 검색합니다. 서비스가 시작되었는지 그리고 시작 유형이 **자동**인지 확인합니다.

장치에 대한 사용자의 액세스 권한이 예기치 않게 주어지거나 거부됩니다.

- **설명**—Device Access Manager 를 사용하여 사용자에게 일부 장치에 대한 액세스를 거부하고 일부 장치에 대한 액세스를 허용했습니다. 사용자가 시스템을 사용할 때 Device Access Manager 에서 액세스를 거부한 장치에 액세스할 수 있고 Device Access Manager 에서 액세스를 허용한 장치에 액세스가 거부됩니다.
- **해결 방법**
  - Device Access Manager 내의 장치 클래스 구성을 사용하여 사용자 및 장치 설정을 조사합니다.
  - **Security Manager**, **Device Access Manager**를 차례로 누른 다음 **Device Class Configuration**(장치 클래스 구성)을 누릅니다. 장치 클래스 트리의 수준을 확장하고 해당 사용자에게 적용되는 설정을 검토합니다. 사용자 또는 사용자가 속한 Windows 그룹(예: 사용자, 관리자)에 설정된 "거부" 권한을 확인합니다.

허용 또는 거부 중 어느 것이 우선?

- **설명**—장치 클래스 구성에서 다음 구성이 설정됩니다.
  - 장치 클래스 계층(예: DVD/CD-ROM 드라이브)의 동일한 수준에서 한 Windows 그룹(예: BUILTIN\Administrators)에는 허용 권한이 부여되고 다른 Windows 그룹(예: BUILTIN\Users)에는 거부 권한이 부여되었습니다.
  - 사용자가 두 그룹에 모두 속한 구성원(예: 관리자)인 경우 어느 권한이 우선합니까?
- **해결 방법**
  - 해당 사용자에게 장치에 대한 액세스가 거부됩니다. 거부가 허용보다 우선합니다.
  - 액세스가 거부되는 것은 Windows 에서 장치에 대한 유효 사용 권한을 설정하는 방식 때문입니다. 액세스가 거부된 그룹과 액세스가 허용된 그룹 모두에 속한 사용자는 액세스가 거부되며, 그 이유는 액세스 거부가 액세스 허용보다 우선 순위를 갖기 때문입니다.

- 이를 회피하는 한 가지 방법은 DVD/CD-ROM 드라이브 수준에서 "사용자" 그룹에게 액세스를 거부하고 DVD/CD-ROM 드라이브 아래 수준에서 "관리자" 그룹에게 액세스를 허용하는 것입니다.
- 또 다른 방법은 특정 Windows 그룹들을 만들어 한 그룹에게는 DVD/CD 에 대한 액세스를 허용하고 다른 그룹에게는 DVD/CD 에 대한 액세스를 거부한 다음 특정 사용자를 적절한 그룹에 추가하는 것입니다.

단순 구성 보기를 사용하여 장치 액세스 제어 정책을 정의할 수 있지만 관리자 사용자가 장치에 액세스할 수 없습니다.

- **설명**—단순 구성을 사용하여 사용자 및 게스트에게 액세스를 거부하고 장치 관리자에게 액세스를 허용했습니다.
- **해결 방법:** 장치 관리자 그룹에 관리자 사용자를 추가합니다.

기타

영향 받은 소프트웨어–증상	설명	해결 방법
Security Manager 에서 **The security application can not be installed until the HP Protect Tools Security Manager is installed(HP Protect Tools Security Manager 를 설치해야만 보안 응용 프로그램을 설치할 수 있습니다.)**라는 경고 메시지가 표시됨	Java Card Security 나 생체 인식과 같은 모든 보안 응용프로그램이 Security Manager 인터페이스에서 실행할 수 있는 플러그인입니다. Security Manager 를 설치해야 HP 가 승인한 보안 플러그인을 로드할 수 있습니다.	보안 플러그인을 설치하려면 먼저 Security Manager 소프트웨어를 설치해야 합니다.
HP ProtectTools Security Manager–Security Manager 인터페이스를 종료할 때 가끔씩 오류가 반환됨	플러그인 응용프로그램이 모두 로드되기 전에 화면 상단 오른쪽의 닫기 버튼을 눌러 Security Manager 를 종료하면 가끔씩 (12 번에 1 번 정도) 오류가 발생합니다.	이 문제는 Security Manager 를 종료하거나 실행할 때 플러그인 서비스의 로드 시간에 따른 것입니다. PTHOST.exe 는 다른 플러그인 응용프로그램들을 포함하는 쉘 프로그램이므로 플러그인의 로드 시간(서비스)에 영향을 받습니다. 이 문제의 근본 원인은 플러그인이 완전히 로드되기 전에 쉘 프로그램을 종료했기 때문입니다. Security Manager 창의 상단에 서비스가 모두 로드되었다는 메시지가 표시되고 왼쪽 목록에 모든 플러그인이 나열될 때까지 기다리십시오. 플러그인이 모두 로드될 때까지 충분한 시간을 기다리면 문제를 방지할 수 있습니다.
HP ProtectTools—액세스가 제한되거나 관리자 권한 제어가 불가능하여 보안 위험이 발생함	클라이언트 PC 에 대한 액세스를 제어할 수 없을 경우 다음과 같은 많은 위험이 발생할 수 있습니다. • PSD 삭제 • 사용자 설정에 대한 악의적인 수정 • 보안 정책 및 기능의 사용 불가	관리자는 “모범 규준”에 따라 최종 사용자 권한과 사용자 액세스를 제한해야 합니다. 무단 사용자에게는 관리 권한을 부여하지 말아야 합니다.

용어

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

CSP(암호화 서비스 제공업체) 잘 정의된 인터페이스에서 특정 암호화 기능을 수행하는 데 사용하는 암호화 알고리즘을 제공하는 업체 또는 암호화 알고리즘 라이브러리

Drive Encryption 하드 드라이브를 암호화해 데이터를 보호하므로 권한이 없는 사람들은 정보를 확인할 수 없습니다.

Drive Encryption 로그온 화면 로그온 화면은 Windows 가 시작되기 전에 표시됩니다. 사용자는 Windows 사용자 이름 및 암호/Java Card PIN 을 입력해야 합니다. 대부분의 경우 Drive Encryption 로그온 화면에 정확한 정보를 입력해야 Windows 로그온 화면에 다시 로그온할 필요 없이 바로 Windows 에 액세스할 수 있습니다.

DriveLock 컴퓨터를 시작할 때 하드 드라이브를 사용자와 연결하고 사용자에게 올바른 DriveLock 암호를 입력하도록 요구하는 보안 기능

EFS(암호화 파일 시스템) 선택한 폴더 내 모든 파일과 하위 폴더를 암호화하는 시스템

HP SpareKey Drive Encryption 키의 백업 사본입니다.

ID HP ProtectTools Security Manager 에서 특정 사용자에 대한 계정이나 프로필과 같이 간주되는 인증 정보 및 설정 그룹

ID 카드 사용자 이름과 선택한 사진을 가지고 시각적으로 데스크탑을 식별해 주는 Windows 사이드바 가젯. ID 카드를 눌러 HP ProtectTools 관리 콘솔을 엽니다.

Java Card 컴퓨터에 끼울 수 있는 탈착식 카드. 그 안에는 로그온 ID 정보가 들어있습니다. Drive Encryption 로그온 화면에서 Java Card 로 로그인하려면 Java Card 를 넣은 후 사용자 이름과 Java Card PIN 을 입력해야 합니다.

Live Messenger History Viewer 암호화된 대화 기록 세션을 검색하고 볼 수 있도록 하는 Privacy Manager Chat 구성 요소

PIN 개인 식별 번호입니다.

PKI 공용 키 인프라는 인증서와 암호화 키를 작성, 사용, 관리하기 위한 인터페이스를 정의하는 표준입니다.

Privacy Manager 인증서 전자 우편 메시지와 Microsoft Office 문서를 서명하고 암호화하는 등 암호화 작업에 사용할 때마다 인증을 요구하는 디지털 인증서

PSD 개인 보안 드라이브는 중요 정보를 위한 안전한 보관 영역을 제공합니다.

SATA 장치 모드 하드 드라이브, 광 드라이브와 같은 대용량 저장소 장치와 컴퓨터 간 데이터 전송 모드입니다.

Send Securely(안전하게 보내기) 버튼 Microsoft Outlook 전자 우편 메시지의 도구 모음에 표시되는 소프트웨어 버튼. 이 버튼을 누르면 Microsoft Outlook 전자 우편 메시지를 등록하거나 암호화할 수 있습니다.

Sign and Encrypt(서명 및 암호화) 버튼 Microsoft Outlook 응용프로그램의 도구 모음에 표시되는 소프트웨어 버튼. 이 버튼을 누르면 Microsoft Office 문서를 등록하거나 암호화하거나 암호화를 제거할수 있습니다.

Single Sign On 인증 정보를 저장하여, 사용자가 Security Manager 를 통해 암호 인증이 필요한 인터넷 및 Windows 응용프로그램에 액세스할 수 있도록 해주는 기능

Trusted Contact(신뢰할 수 있는 연락처) 신뢰할 수 있는 대화 상대 초대 요청을 수락자 사용자

Trusted Contact(신뢰할 수 있는 연락처) 목록 신뢰할 수 있는 연락처 목록

Trusted Contact(신뢰할 수 있는 연락처) 수신자 신뢰할 수 있는 연락처가 되도록 초대 요청을 받는 사용자

Trusted Contact(신뢰할 수 있는 연락처) 초대 신뢰할 수 있는 연락처가 되도록 요청하는 내용으로 발송되는 전자 우편

TXT Trusted Execution Technology 의 약자로 보안 기술의 일종입니다.

USB 토큰 사용자의 식원 정보를 저장하는 보안 장치. Java Card 나 생체 인식기처럼 컴퓨터에서 소유자를 인증하는 데 사용함.

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

Windows 로그온 보안 특정 자격증명을 사용해야만 액세스를 허용해 Windows 계정을 보호합니다.

Windows 사용자 계정 네트워크나 개별 컴퓨터에 로그온하도록 승인된 개인 프로필

가상 토큰 Java Card 및 카드 리더기와 유사하게 작동하는 보안 기능. 가상 토큰은 컴퓨터 하드 드라이브나 Windows 레지스트리에 저장됩니다. 가상 토큰으로 로그온하는 경우 인증을 완료하기 위해 사용자 PIN 을 입력해야 합니다.

관리자 Windows 관리자를 *참조하십시오*.

권한이 있는 사용자 사용자 액세스 설정 보기 권한을 받아 "간단한 구성"이나 "장치 클래스 구성" 창에서 구성 창을 확인하거나 수정할 수 있는 사용자

그룹 액세스 권한이 동일하거나 장치 클래스나 특정 장치에 대한 액세스가 거부된 사용자 그룹

기본 삭제 자산에 대한 Windows 참조를 삭제합니다. 여유 공간 블리치를 통해 손상된 데이터를 해당 자산에 덮어쓸 때까지 해당 자산의 내용은 하드 드라이브에 계속 남아 있습니다.

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

대시보드 HP ProtectTools 용 Security Manager 에서 기능 및 설정을 액세스하고 관리할 수 있는 중심 위치입니다.

대화 기록 세션 채팅 세션의 양쪽 대화 기록이 포함되어 있는 암호화된 파일

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

디지털 서명 파일과 함께 전송되어 자료 발송자와, 해당 파일이 서명 후 수정되지 않았음을 확인하는 데이터

디지털 인증서 디지털 인증서 소유자의 신원과 디지털 정보 서명에 사용되는 전자 키 쌍을 바인딩하여 개인이나 기업의 신원을 확인하는 전자 인증 정보

로그온 웹 사이트나 다른 프로그램에 로그온할 때 사용할 수 있는 사용자 이름과 암호(그리고 선택한 기타 정보)로 구성된 Security Manager 내 객체

마이그레이션 Privacy Manager 인증서와 신뢰할 수 있는 연락처의 관리, 복원, 이전을 가능하게 하는 작업

백그라운드 서비스 장치 액세스 제어 정책을 적용하기 위해 실행해야 하는 HP ProtectTools 장치 잠금/감사 배경 서비스. 제어판의 관리 도구 옵션에 있는 서비스 응용프로그램 안에서 확인할 수 있습니다. 아직 실행되고 있지 않다면, 장치 액세스 제어 정책을 적용할 때 HP ProtectTools Security Manager 가 이를 시작하려고 시도합니다.

백업 백업 기능을 사용해 중요한 프로그램 정보를 복사해 프로그램 외부 위치에 저장. 이 기능으로는 나중에 동일 컴퓨터나 다른 컴퓨터로 정보를 복구할 수 있습니다.

보안 로그온 방법 컴퓨터에 로그온할 때 사용하는 방법

복원 이전에 저장해 둔 백업 파일에서 프로그램 정보를 이 프로그램으로 복사하는 프로세스

사용자 Drive Encryption 에 등록한 모든 사람이 사용자입니다. 관리자 이외의 사용자에게는 Drive Encryption 에 대한 권한이 제한됩니다. 관리자 이외의 사용자는 등록(관리자의 승인이 있는 경우)과 로그온만 할 수 있습니다.

사진 등록된 사용자의 사진은 인증에 사용됩니다.

생체 인식 지문과 같은 신체적 특징으로 사용자의 신원을 파악하는 인증 정보의 범주

서명 줄 디지털 서명을 볼 수 있도록 표시하는 자리 표시자. 문서에 서명하면 서명자의 이름과 확인 방법이 표시됩니다. 서명 날짜와 서명자의 제목을 포함할 수도 있습니다.

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

스마트 카드 크기와 모양이 신용 카드와 유사하고 소유자에 대한 식별 정보를 저장하는 소형 하드웨어. 컴퓨터에서 소유자를 인증하는 데 사용함

신뢰할 수 있는 IM 대화 신뢰할 수 있는 발송자가 신뢰할 수 있는 연락처 대상에게 신뢰할 수 있는 메시지를 보내는 동안 진행되는 대화 세션

신뢰할 수 있는 메시지 신뢰할 수 있는 발송자가 신뢰할 수 있는 연락처 대상에게 신뢰할 수 있는 메시지를 보내는 동안 진행되는 대화 세션

신뢰할 수 있는 발송자 서명이 있거나 암호화된 전자 우편 및 Microsoft Office 문서를 보내는 신뢰할 수 있는 연락처

신뢰할 수 있는 연락처에 대한 봉인 디지털 서명을 추가하고 전자 우편을 암호화하고 선택한 보안 로그온 방법을 통해 인증한 후 전자 우편을 보내는 작업

암호 해독 암호 표기법에서 암호화된 데이터를 일반 텍스트로 변환하는 데 사용되는 절차

암호화 특정인만 해독할 수 있도록 데이터를 암호화하고 해독하는 기법

암호화 알고리즘 사용 등 일반 텍스트를 암호화 텍스트로 변환하여 권한이 없는 수신자가 데이터를 읽지 못하도록 암호화에 사용되는 절차. 데이터 암호화에는 여러 유형이 있으며 이러한 암호화는 네트워크 보안의 기본임. 공통 유형으로는 데이터 암호화 표준(DES)과 공용 키 암호화를 등이 있음

여유 공간 블리치 삭제된 자산에 임의의 데이터를 덮어써서 삭제된 자산의 내용을 볼 수 없도록 하는 보안 방법입니다.

응급 복구 아카이브 한 플랫폼 소유자 키로부터 다른 키로 기본 사용자 키를 다시 암호화할 수 있는 안전한 보관 영역

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

인증 기관 공용 키 인프라를 실행하는 데 필요한 인증서를 발급하는 서비스

인증서 사용자가 인증 과정 중 특정 작업에 대한 합당한 권한이 있음을 증명하는 방법

자동 파쇄 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.

장치 액세스 제어 정책 사용자가 액세스 권한을 받았거나 거부 당한 장치 목록

장치 클래스 드라이브와 같은 특정 유형의 모든 장치

재부팅 컴퓨터를 재시작하는 과정

지문 지문 이미지의 디지털 추출. 실제 지문 이미지는 절대로 Security Manager 로 저장할 수 없습니다.

추천 서명자 문서에 서명 줄을 추가하도록 Microsoft Word 또는 Microsoft Excel 문서의 소유자가 지정한 사용자

콘솔 HP ProtectTools Administrative Console 에서 기능 및 설정을 액세스하고 관리할 수 있는 중심 위치입니다.

키 시퀀스 특정 키의 조합으로, 이를 누르면 자동 파쇄가 시작됩니다(예: ctrl+alt+s).

토큰 보안 로그온 방법 참조.

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 Java Card, 보안 칩 또는 암호 등과 같이 컴퓨터를 켤 때 일정 형태의 인증을 요구하는 보안 기능입니다.

표시 사용자가 둘 이상의 대화 기록 세션 암호를 해독하여 일반 텍스트의 Contact Screen Name(연락처 대화명)을 표시하고 세션을 볼 수 있도록 하는 작업

해지 암호 사용자가 디지털 인증서를 요청할 때 생성되는 암호. 사용자가 디지털 인증서를 해지하려고 할 때 이 암호가 필요합니다. 따라서 사용자만 인증서를 해지할 수 있음을 보장합니다.

활성화 Drive Encryption 기능에 액세스하기 전에 완료되어야 하는 작업입니다. HP ProtectTools 설치 마법사를 사용해 Drive Encryption 을 활성화합니다. 이때 관리자만이 Drive Encryption 을 활성화할 수 있습니다. 활성화 과정에는 소프트웨어 활성화, 드라이브 암호화, 사용자 계정 생성, 이동식 저장 장치에 초기 백업 암호화 키 생성 등이 포함됩니다.

색인