HP ProtectTools

시작하기

초판: 2011 년 1 월

문서 부품 번호: 638391-AD1

목차

1 보안 소개

HP ProtectTools Security Manager 소프트웨어는 컴퓨터, 네트워크 및 중요 데이터에 대한 무단 액세스를 차단하는 보안 기능을 제공합니다.

응용프로그램	기능
HP ProtectTools 관리 콘솔(관리자용)	• 액세스할 때 Microsoft Windows 관리자 권한이 있어야 합니다. • 관리자가 구성하여 사용자가 사용할 수 없는 모듈에 대한 액세스를 제공합니다. • 최초 보안 설정을 허용하고 모든 사용자의 옵션 또는 요구 사항을 구성합니다.
HP ProtectTools Security Manager(사용자용)	• 관리자가 제공한 옵션을 사용자가 구성할 수 있습니다. • 관리자가 사용자에게 일부 HP ProtectTools 모듈에 대한 제한적 제어를 제공할 수 있습니다.

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.

참고: 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 관리 콘솔(관리자용)	• Security Manager 설치 마법사를 사용하여 보안 수준 및 보안 로그온 방법을 설정 및 구성합니다. • 사용자에게 숨겨진 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(사용자용)	• 암호를 구성, 설정 및 변경합니다. • Windows 암호, 지문, 스마트 카드 등의 사용자 인증 정보를 구성 및 변경합니다. • File Sanitizer 파쇄, 블리치 및 기타 설정을 구성 및 변경합니다. • Device Access Manager 에 대한 설정을 확인합니다. • HP ProtectTools 의 Computrace 를 구성합니다. • 기본 설정과 백업 및 복원 옵션을 구성합니다.
HP ProtectTools 의 Credential Manager(Password Manager)	• 사용자 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. • 계정 보안을 강화하기 위해 더 강력한 암호를 만듭니다. Password Manager 가 자동으로 정보를 입력하고 제출합니다.
HP ProtectTools Drive Encryption(일부 모델만 해당)	• 완전한 전체 볼륨 하드 드라이브 암호화를 제공합니다. • 데이터를 해독하고 액세스하기 위한 부팅 전 인증을 강제 실행합니다.
File Sanitizer for HP ProtectTools	• 컴퓨터에 저장된 자산(예: 응용프로그램 파일, 기록 컨텐츠 또는 웹 관련 컨텐츠, 기타 기밀 데이터 등의 민감한 정보)을 파쇄하고 하드 드라이브에서 삭제된 자산을 주기적으로 블리치합니다.
Device Access Manager for HP ProtectTools(일부 모델만 해당)	• IT 관리자가 사용자 프로파일을 기준으로 장치에 대한 액세스를 제어할 수 있습니다. • 권한 없는 사용자가 외장 스토리지 미디어를 사용하여 데이터를 제거하거나 외장 미디어에서 시스템으로 바이러스가 침입하는 것을 방지합니다. • 관리자가 특정 개인 또는 사용자 그룹에 대해 쓰기 가능 장치에 대한 액세스를 비활성화할 수 있습니다.
HP ProtectTools Privacy Manager(일부 모델만 해당)	• Microsoft 전자 우편 및 Microsoft Office 문서를 사용할 경우 통신의 근원, 무결성 및 보안을 검증하는 인증서를 얻는 데 사용됩니다.

모듈	주요 기능
Computrace for HP ProtectTools(별매)	• 안전한 자산 추적을 제공합니다. • 사용자 활동, 하드웨어 및 소프트웨어 변경 사항을 모니터링합니다. • 하드 드라이브가 다시 포맷되거나 교체된 경우에도 활성 상태를 유지합니다. • 활성화하려면 별도로 추적 가입을 구매해야 합니다.
Embedded Security for HP ProtectTools(일부 모델만 해당)	• 컴퓨터에 저장된 사용자 데이터 및 인증 정보에 대한 무단 액세스를 차단하기 위해 TPM(Trusted Platform Module) 내장 보안 칩을 사용합니다. • 사용자 파일 및 폴더 정보를 보호하는 데 유용한 PSD(개인 보안 드라이브)를 생성합니다. • 보호된 디지털 인증서 작업을 위해 타사 응용프로그램(예: Microsoft Outlook, Internet Explorer)을 지원합니다.

HP ProtectTools 보안 제품 설명 및 일반 사용 예

대부분의 HP ProtectTools 보안 제품에는 암호를 분실하거나 사용할 수 없거나 잊어버린 경우 또는 기업 보안팀에서 액세스가 필요할 경우 액세스를 얻기 위한 사용자 인증(일반적으로 암호) 및 관리 백업이 포함되어 있습니다.

참고: 일부 HP ProtectTools 보안 제품은 데이터에 대한 액세스를 제한하도록 설계되었습니다. 타인이 정보에 무단 액세스하는 것보다 차라리 정보를 잃는 것이 더 나을 정도로 중요한 데이터는 암호화해야 합니다. 모든 데이터를 안전한 위치에 백업하는 것이 좋습니다.

Credential Manager for HP ProtectTools

Credential Manager(Security Manager 의 일부)는 사용자 이름과 암호를 저장하며, 이를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

- 인터넷 액세스 또는 전자 우편에 대한 로그인 이름 및 암호를 저장합니다.
- 웹 사이트 또는 전자 우편에 사용자를 자동으로 로그인합니다.
- 인증을 관리 및 정리합니다.
- 웹 또는 네트워크 자산을 선택하고 링크에 직접 액세스합니다.
- 필요할 경우 이름과 암호를 확인합니다.

예 1: 대규모 제조업체의 한 구매 대행인이 대부분의 기업 거래를 인터넷에서 처리하면서 로그인 정보가 필요한 몇 개의 유명 웹 사이트에 자주 방문합니다. 이 대행인은 보안을 중요하게 생각해서 모든 계정에 다른 암호를 사용하고 있는데, Credential Manager 를 사용하여 웹 링크에 다른 사용자 이름과 암호를 대응시키기로 결정합니다. 로그인하는 웹 사이트에 가면 Credential Manager 가 인증 정보를 자동으로 제시합니다. 사용자 이름과 암호를 확인하려면 Credential Manager 를 구성하여 해당 정보를 표시할 수도 있습니다.

Credential Manager 는 인증을 관리 및 정리하는 데에도 사용할 수 있습니다. 사용자가 웹 또는 네트워크 자산을 선택하고 링크에 직접 액세스할 수 있으며, 필요할 경우 사용자 이름과 암호를 확인할 수 있습니다.

예 2: 업무량이 많은 공인 회계사가 승진을 한 후 전체 회계팀을 관리하게 됩니다. 이 팀은 많은 고객의 웹 계정에 로그인해야 하는데 각 계정은 다른 로그인 정보를 사용합니다. 이 로그인 정보는 다른 직원과 공유해야 하기 때문에 기밀 유지가 문제입니다. 이 공인 회계사는 Credential Manager for HP ProtectTools 내에서 모든 웹 링크, 회사 사용자 이름 및 암호를 정리하기로 결정합니다. 정리를 마치고 직원에게 Credential Manager 를 배포한 후 직원들은 자신들이 사용하는 로그인 인증 정보를 모르는 상태에서 웹 계정을 사용할 수 있게 됩니다.

Drive Encryption for HP ProtectTools

Drive Encryption 은 전체 컴퓨터 하드 드라이브 또는 보조 드라이브의 데이터에 대한 액세스를 제한하는 데 사용하며 자체 암호화 드라이브를 관리할 수도 있습니다.

예 1: 한 의사가 컴퓨터 하드 드라이브에 저장된 데이터에 자신만 액세스할 수 있기를 원합니다. 이 의사는 Windows 로그인 전에 부팅 전 인증을 요구하는 Drive Encryption 을 활성화합니다. 설정 후 이 하드 드라이브는 운영 체제가 시작되기 전 암호 없이 액세스가 불가능하게 됩니다. SED(Self-Encryption Drive) 옵션을 사용하여 데이터를 암호화하도록 선택하여 드라이브 보안을 더욱 강화할 수 있습니다.

Embedded Security for HP ProtectTools 및 Drive Encryption for HP ProtectTools 모두 원래의 마더보드에 구속되어 있기 때문에 드라이브를 제거한 후에도 암호화된 데이터에 액세스할 수 없습니다.

예 2: 한 병원 관리자가 의사와 권한 있는 담당자만이 개인 암호를 공유하지 않고 로컬 컴퓨터의 데이터에 액세스할 수 있도록 하려고 합니다. IT 부서에서 관리자, 의사 및 권한 있는 모든 담당자를 Drive Encryption 사용자로 추가합니다. 이제 권한 있는 담당자만 개인 사용자 이름 및 암호를 사용하여 컴퓨터 또는 도메인을 부팅할 수 있습니다.

File Sanitizer for HP ProtectTools

File Sanitizer for HP ProtectTools 는 인터넷 브라우저 활동, 임시 파일, 이전에 삭제된 데이터 또는 기타 모든 정보를 포함한 데이터를 영구적으로 삭제하는 데 사용합니다. File Sanitizer 는 수동으로 실행하거나 사용자가 지정한 일정에 따라 자동으로 실행하도록 구성할 수 있습니다.

예 1: 한 변호사는 종종 민감한 고객 정보를 처리하면서 삭제한 파일의 데이터를 복구할 수 없도록 하려고 합니다. 이 변호사가 File Sanitizer 를 사용하여 삭제한 파일을 "파쇄"하면 복구는 거의 불가능합니다.

일반적으로 Windows 에서 데이터를 삭제하면 실제로 하드 드라이브에서 데이터가 삭제되지는 않습니다. 대신, 하드 드라이브 섹터를 향후 사용 가능하다고 표시합니다. 그 위에 데이터를 기록하기 전까지는 인터넷에서 제공되는 일반적인 도구를 사용하여 쉽게 복구할 수 있습니다. File Sanitizer 는 섹터에 임의 데이터를 기록하여(필요할 경우 여러 번) 삭제한 데이터를 읽을 수 없거나 복구할 수 없도록 만듭니다.

예 2: 한 연구가가 로그오프할 때 삭제한 데이터, 임시 파일, 브라우저 활동 등을 자동으로 파쇄하려고 합니다. 이 연구가는 File Sanitizer 를 사용하여 일반 파일 또는 사용자 지정 파일을 자동으로 영구 삭제하는 "파쇄" 일정을 지정할 수 있습니다.

Device Access Manager for HP ProtectTools

Device Access Manager for HP ProtectTools 를 사용하여 데이터를 복사할 수 있는 USB 플래시 드라이브에 대한 무단 액세스를 차단할 수 있습니다. 또한 CD/DVD 드라이브에 대한 액세스, USB 장치 제어, 네트워크 연결 등을 제한할 수도 있으며, 관리자가 드라이브에 액세스할 수 있는 시간과 기간을 지정할 수도 있습니다. 예를 들어 외부 공급업체가 회사 컴퓨터에 액세스해야 하지만, 데이터를 USB 드라이브로 복사하면 안 되는 상황이 있습니다. 관리자는 Device Access Manager for HP ProtectTools 를 사용하여 하드웨어에 대한 액세스를 제한 및 관리할 수 있습니다.

예 1: 한 의료기기 공급업체의 관리자가 회사 정보와 함께 개인 의료 기록을 자주 처리합니다. 직원들이 이 데이터에 액세스해야 하지만 USB 드라이브 또는 다른 외장 스토리지 미디어를 사용하여 컴퓨터에서 데이터를 제거하지 않도록 하는 것이 매우 중요합니다. 네트워크는 안전하지만, 컴퓨터에는 데이터가 복사 및 도난 당할 위험이 있는 CD 버너와 USB 포트가 있습니다. 이 관리자는 Device Access Manager 를 사용하여 USB 포트와 CD 버너를 사용할 수 없도록 비활성화합니다. USB 포트는 차단되었지만 마우스와 키보드는 계속 작동합니다.

예 2: 한 보험 회사가 직원들이 집에서 개인 소프트웨어 또는 데이터를 설치 또는 로드하지 못하게 하려고 합니다. 일부 직원은 모든 컴퓨터에서 USB 포트에 액세스할 수 있어야 합니다. 이 IT 관리자는 Device Access Manager 를 사용하여 일부 직원에 대한 액세스를 허용하는 동시에 그 외 다른 사람의 외부 액세스를 차단합니다.

Privacy Manager for HP ProtectTools

Privacy Manager for HP ProtectTools 는 인터넷 전자 우편 통신의 보안을 유지하는 데 사용됩니다. 사용자는 인증된 수신자만 열 수 있는 전자 우편을 만들고 보낼 수 있습니다. Privacy Manager 를 사용하면 타인이 정보에 무단 액세스하거나 정보를 가로챌 수 없습니다.

예 1: 한 주식 중개인이 자신의 전자 우편이 특정 고객에게만 전달되도록 하고 아무도 전자 우편 계정을 위조하거나 무단 로그인할 수 없도록 하려고 합니다. 이 주식 중개인은 Privacy Manager 에 자신과 고객을 등록합니다. Privacy Manager 는 각 사용자에게 CA(인증서)를 발급합니다. 주식 중개인과 고객은 이 도구를 사용하여 전자 우편을 주고받기 전에 반드시 인증을 받아야 합니다.

Privacy Manager for HP ProtectTools 를 사용하면 검증 및 인증된 수신자와 손쉽게 전자 우편을 주고받을 수 있습니다. 전자 우편 서비스를 암호화할 수도 있는데, 이 암호화 과정은 인터넷에서 일반 신용카드로 구매할 때 사용되는 것과 유사합니다.

예 2: 한 CEO 는 자신이 전자 우편을 통해 보낸 정보를 이사회 구성원만 볼 수 있게 하려고 합니다. 이 CEO 는 이사들과 주고받는 전자 우편을 암호화하는 옵션을 사용합니다. CEO 와 이사들은 Privacy Manager 인증서를 통해 암호화 키의 사본을 갖고 기밀 전자 우편의 암호를 해제할 수 있습니다.

Computrace for HP ProtectTools(이전의 LoJack Pro)

Computrace for HP ProtectTools(별도 구매)는 도난 당한 컴퓨터에서 인터넷에 액세스할 때 위치를 추적하는 서비스입니다.

예 1: 한 학교의 교장이 IT 팀에 학교의 모든 컴퓨터를 파악하라는 지시를 내렸습니다. 컴퓨터의 재고 목록을 작성한 후 IT 관리자는 컴퓨터를 분실할 경우 추적할 수 있도록 모든 컴퓨터를 Computrace 에 등록하였습니다. 최근 이 학교에서 컴퓨터 몇 대가 분실되자 IT 관리자가 관계 당국 및 Computrace 담당자에게 이 사실을 알렸습니다. 컴퓨터 위치가 파악되었고 관계당국에 의해 학교로 반환되었습니다.

Computrace for HP ProtectTools 는 또한 컴퓨터를 원격으로 관리하고 위치를 파악할 수 있으며 컴퓨터 사용 상태 및 응용프로그램을 모니터링할 수 있습니다.

예 2: 한 부동산 회사가 전 세계적으로 컴퓨터를 관리 및 업데이트하려고 합니다. 이 회사는 Computrace 를 사용하여 각 컴퓨터에 IT 담당자를 보내지 않고도 컴퓨터를 모니터링 및 업데이트합니다.

Embedded Security for HP ProtectTools(일부 모델만 해당)

Embedded Security for HP ProtectTools 를 사용하여 개인 보안 드라이브를 만들 수 있습니다. 이 기능을 통해 PC 에서 가상 드라이브 파티션을 만들어 액세스하기 전까지 완벽히 숨길 수 있습니다. Embedded Security 는 데이터를 비밀로 보호해야 하는 모든 곳에서 사용하면서 나머지 데이터는 암호화하지 않을 수 있습니다.

예 1: 한 창고 관리자의 컴퓨터를 하루 종일 여러 명의 작업자가 가끔씩 액세스합니다. 이 관리자는 컴퓨터의 기밀 창고 데이터를 암호화하고 숨기며 하드 드라이브가 도난당하더라도 데이터의 암호를 해제하거나 읽을 수 없도록 데이터를 안전하게 유지하기를 원합니다. 이 창고 관리자는 Embedded Security 를 활성화하고 기밀 데이터를 개인 보안 드라이브로 이동합니다. 그러면 다른 하드 드라이브와 마찬가지로 암호를 입력해서 기밀 데이터에 액세스할 수 있습니다. 개인 보안 드라이브에서 로그오프하거나 재부팅하면 올바른 암호 없이 해당 드라이브를 보거나 열 수 없습니다. 작업자들이 컴퓨터에 액세스하더라도 기밀 데이터를 볼 수 없습니다.

Embedded Security 는 마더보드에 위치한 하드웨어 TPM(Trusted Platform Module) 칩 안에 암호화 키를 보호합니다. Embedded Security 는 누군가가 해독 암호를 추측하려고 시도할 경우 암호 공격에 저항하는 최소 요구 사항을 충족하는 유일한 암호화 도구입니다. 이 도구를 통해 전체 드라이브 및 전자 우편을 암호화할 수도 있습니다.

예 2: 한 주식 중개인이 휴대용 드라이브를 사용하여 매우 민감한 데이터를 다른 컴퓨터로 이동하려고 합니다. 이 주식 중개인은 타인이 암호를 무단으로 알아 내더라도 두 컴퓨터에서만 이 드라이브를 열 수 있도록 하려고 합니다. 그래서 Embedded Security TPM 마이그레이션을 사용하여 두 번째 컴퓨터에 데이터를 해독하는 데 필요한 암호화 키를 저장합니다. 이동 과정 중에는 암호를 알더라도 두 물리적 컴퓨터에서만 데이터를 해독할 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 운영 체제에 대한 액세스를 차단할 수 있습니다. 다음 장을 참조하십시오.
  - Security Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Embedded Security for HP ProtectTools 모듈에서 제공하는 개인 보안 드라이브 기능은 인증 없이 민감한 데이터에 액세스할 수 없도록 해당 데이터 암호화합니다. 다음 장을 참조하십시오.
  - Embedded Security for HP ProtectTools
- Computrace 는 컴퓨터를 도난당한 후 컴퓨터의 위치를 추적할 수 있습니다. 다음 장을 참조하십시오.
  - Computrace for HP ProtectTools

중요한 데이터의 액세스 제한

외부 감사인이 현장에서 컴퓨터에 대한 액세스를 허용 받고 민감한 재무 데이터를 검토하는 경우를 가정하겠습니다. 다음 기능을 사용하여 데이터에 대한 액세스를 제한할 수 있습니다.

- IT 관리자가 Device Access Manager for HP ProtectTools 에서 쓰기 가능 장치에 대한 액세스를 제한하여 하드 드라이브에서 민감한 정보를 인쇄하거나 이동식 미디어로 복사하지 못하도록 설정할 수 있습니다.

내부 또는 외부에서 들어오는 무단 액세스 차단

보안되지 않은 업무용 컴퓨터에 대한 무단 액세스는 재무 업무, 임원 또는 R&D 팀의 정보와 같은 기업 네트워크 자원과 병록, 개인 재무 기록과 같은 개인 정보에 대해 현실적으로 매우 위험한 상황을 의미합니다. 다음 기능을 사용하여 무단 액세스를 차단할 수 있습니다.

- 부팅 전 인증 기능을 활성화하면 운영 체제에 대한 액세스를 차단할 수 있습니다. 다음 장을 참조하십시오.
  - Password Manager for HP ProtectTools
  - Embedded Security for HP ProtectTools
  - Drive Encryption for HP ProtectTools
- Password Manager 는 무단 사용자가 암호를 구하거나 암호로 보호된 응용프로그램에 액세스하는 것을 방지하는 데 효과적입니다.
- IT 관리자가 Device Access Manager for HP ProtectTools 에서 쓰기 가능 장치에 대한 액세스를 제한하여 하드 드라이브에서 민감한 정보를 복사하지 못하도록 설정할 수 있습니다.
- File Sanitizer 를 사용하면 중요 파일과 폴더를 파쇄하거나 하드 드라이브에서 삭제된 자산을 블리치하여 데이터를 안전하게 삭제합니다(삭제되었지만 복구 가능한 데이터 위에 쓰기).
- Privacy Manager 를 사용하면 Microsoft 전자 우편 또는 Microsoft Office 문서를 사용할 때 인증서를 받아 중요 정보를 안전하게 보내고 저장할 수 있습니다.

강력한 암호 정책 생성

여러 웹 기반 응용프로그램 및 데이터베이스에 대해 강력한 암호 정책을 사용하는 회사 정책이 실시될 경우 Security Manager 는 암호용 저장소와 Single Sign On 편의를 제공합니다.

추가 보안 요소

보안 역할 할당

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

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

HP ProtectTools 에서는 보안 책임과 권한이 다음과 같은 역할로 구분됩니다.

- 보안 담당자—회사와 네트워크의 보안 수준을 정의하며 Drive Encryption, Embedded Security 등 배포할 보안 기능을 결정합니다.

  참고: 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.
- IT 관리자—보안 담당자가 정의한 보안 기능을 적용 및 관리합니다. 일부 기능을 활성화 또는 비활성화할 수도 있습니다. 예를 들어 보안 담당자가 스마트 카드를 배포하기로 결정할 경우 IT 관리자는 암호 및 스마트 카드 모두를 활성화할 수 있습니다.
- 사용자—보안 기능을 사용합니다. 예를 들어 보안 담당자와 IT 관리자가 시스템에 스마트 카드를 활성화한 경우 사용자는 스마트 카드 PIN 을 설정하고 카드를 사용하여 인증할 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.
스마트 카드 PIN	Credential Manager	다단계 인증으로 사용할 수 있습니다. Windows 인증으로 사용할 수 있습니다. 스마트 카드 토큰이 선택된 경우 Drive Encryption 사용자를 인증합니다.
Emergency Recovery 토큰 암호	Embedded Security, IT 관리자가 설정	내장 보안 칩에 대한 백업 파일인 Emergency Recovery 토큰에 대한 액세스를 보호합니다.
소유자 암호	Embedded Security, IT 관리자가 설정	Embedded Security 의 모든 소유자 기능에 대한 무단 액세스로부터 시스템과 TPM 칩을 보호합니다.
BIOS 관리자 암호	Computer Setup, IT 관리자가 설정	Computer Setup 유틸리티에 대한 액세스를 보호합니다.

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.
- 암호에 사용자의 이름이나 생일, 애완동물 이름, 어머니의 이름과 같은 개인 정보를 사용하지 마십시오. 거꾸로 입력하는 경우도 마찬가지입니다.
- 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 설정 마법사로 시작하기

Security Manager 설정 마법사는 이 컴퓨터의 모든 사용자가 사용할 수 있는 보안 기능을 활성화하는 과정을 안내합니다. 관리 콘솔의 보안 기능 페이지에서 이러한 기능을 관리할 수도 있습니다.

Security Manager 설정 마법사를 통해 보안 기능을 설정하려면 다음과 같이 하십시오.

1. Windows 사이드바에 있는 HP ProtectTools 바탕 화면 가젯 아이콘 또는 작업 표시줄 오른쪽 끝에 있는 알림 영역의 작업 표시줄 아이콘에서 HP ProtectTools Security Manager 를 엽니다.

HP ProtectTools 바탕 화면 가젯 아이콘에 있는 배너 색상은 다음 상태 중 하나를 나타냅니다.

- 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.

가젯 아이콘 아래쪽에 다음 상태 중 하나를 나타내는 메시지가 표시됩니다.

- **지금 설정**—관리자가 가젯 아이콘을 클릭하고 Security Manager 설정 마법사를 실행하여 컴퓨터의 인증 정보를 구성해야 합니다.

  설정 마법사는 독립형 응용프로그램입니다.

- **지금 등록**—사용자가 가젯 아이콘을 클릭하고 Security Manager 시작 마법사를 실행하여 인증 정보를 등록해야 합니다.

  Security Manager 대시보드에 시작 마법사가 표시됩니다.

- **지금 확인**—가젯 아이콘을 클릭하면 보안 응용프로그램 상태 페이지에 자세한 내용이 표시됩니다.

참고: Windows XP 에서는 HP ProtectTools 바탕 화면 가젯 아이콘을 사용할 수 없습니다.

또는

시작, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다. 왼쪽 창에서 **설정 마법사**를 클릭합니다.

2. 시작 화면을 읽고 **다음**을 클릭합니다.

3. Windows 암호를 입력하여 신원을 확인한 후 **다음**을 클릭합니다.

   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. SpareKey 페이지에서 세 가지 보안 질문을 선택하고 각 질문에 대한 답변을 입력한 후 **다음**을 클릭합니다.

   다른 질문을 선택하거나 Security Manager 대시보드의 **Credential Manager** 아래 SpareKey 페이지에서 답변을 변경할 수 있습니다.

참고: 이 SpareKey 설정은 관리자 권한이 있는 사용자에게만 적용됩니다.

5. 확인란을 선택하여 보안 기능을 활성화한 후 **다음**을 클릭합니다.

   기능을 많이 선택할수록 컴퓨터의 보안이 강화됩니다.

참고: 이러한 설정은 모든 사용자에게 적용됩니다. 아무 확인란도 선택하지 않으면 설정 마법사가 인증 정보를 등록하라는 메시지를 표시하지 않습니다.

- **Windows 로그온 보안**—액세스하려는 사용자에게 특정 인증 정보를 요구하여 Windows 계정을 보호합니다.
- **Drive Encryption**—하드 드라이브를 암호화하여 적절한 권한이 없는 사용자가 정보를 읽을 수 없도록 데이터를 보호합니다.
- **Pre-Boot Security**—Windows 가 시작되기 전에 권한이 없는 사용자가 액세스할 수 없도록 컴퓨터를 보호합니다.

  참고: BIOS 에서 Pre-Boot Security 를 지원하지 않을 경우에는 이 기능을 사용할 수 없습니다.

6. 설정 마법사에서 인증 정보를 “등록”하라는 메시지가 표시됩니다.

   지문 인식기나 스마트 카드 또는 웹캠을 사용할 수 없는 경우 Windows 암호를 입력하라는 메시지가 나타납니다. 등록 후에는 인증이 필요할 때마다 등록한 인증 정보를 사용하여 신원을 확인할 수 있습니다.

참고: 이러한 인증 정보의 등록은 관리자 권한이 있는 사용자에게만 적용됩니다.

7. 마법사의 마지막 페이지에서 **마침**을 누릅니다.

   Security Manager 대시보드 홈페이지가 표시됩니다.

3 HP ProtectTools Security Manager 관리 콘솔

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

분실되거나 도난당한 컴퓨터의 복구를 지원하기 위해 Security Manager 대시보드에서 기타 응용프로그램을 사용할 수 있습니다(일부 모델에만 해당).

이 콘솔을 사용하면 로컬 관리자가 다음 작업을 수행할 수 있습니다.

- 보안 기능 활성화 또는 비활성화
- 인증에 필요한 인증 정보 지정
- 컴퓨터 사용자 관리
- 장치별 매개 변수 조정
- 설치된 Security Manager 응용프로그램 구성
- 기타 Security Manager 응용프로그램 추가

HP ProtectTools 관리 콘솔 열기

시스템 정책 설정이나 소프트웨어 구성과 같은 관리자 작업의 경우 다음과 같이 콘솔을 엽니다.

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

  또는

  Security Manager 의 왼쪽 패널에서 **관리**를 누른 다음 **관리 콘솔**을 누릅니다.

관리 콘솔 사용

HP ProtectTools 관리 콘솔은 HP ProtectTools Security Manager 기능과 응용프로그램을 관리하는 중앙 위치입니다.

▲ HP ProtectTools 관리 콘솔을 열려면 **시작**, **모든 프로그램**, **HP**, **HP ProtectTools 관리 콘솔**을 차례로 누르십시오.

또는

Security Manager 의 왼쪽 패널에서 **관리**를 누른 다음 **관리 콘솔**을 누릅니다.

콘솔은 다음 구성 요소로 구성되어 있습니다.

- **홈**—다음과 같은 보안 옵션을 구성할 수 있습니다.
  - **시스템 보안 강화**
  - **강력한 인증 요구**
  - **HP ProtectTools 사용자 관리**
  - **HP ProtectTools 를 중앙에서 관리하는 방법 보기**
- **시스템**—사용자와 장치에 대해 다음과 같은 보안 기능과 인증을 구성할 수 있습니다.
  - **보안**
  - **사용자**
  - **인증 정보**
- **응용프로그램**—HP ProtectTools Security Manager 와 Security Manager 응용프로그램에 대한 설정을 구성할 수 있습니다.
- **데이터**—데이터를 보호하는 Security Manager 응용프로그램에 대한 링크의 확장 메뉴를 제공합니다.
- **중앙 관리**—추가 해결 방법, 제품 업데이트 및 메시지에 액세스할 수 있는 탭을 표시합니다.
- **설치 마법사**—HP ProtectTools Security Manager 를 설치하는 과정을 안내합니다.
- **정보**—버전 번호와 저작권 고지와 같은 HP ProtectTools Security Manager 에 대한 정보를 표시합니다.
- **주 영역**—응용프로그램별 화면을 표시합니다.

  ?—관리 콘솔 소프트웨어 도움말을 표시합니다. 이 아이콘은 창 프레임 오른쪽 상단 최소화/최대화 아이콘 옆에 있습니다.

시스템 구성

시스템 그룹은 HP ProtectTools 관리 콘솔 왼쪽에 있는 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 방식을 관리하는 설정, 인증 및 기능을 관리합니다.
- **사용자**—이 컴퓨터의 사용자를 설정, 관리 및 등록합니다.
- **인증 정보**—컴퓨터에 내장되거나 연결된 보안 장치의 설정을 관리합니다.

컴퓨터에 대한 인증 설정

인증 응용프로그램 내에서 컴퓨터에 대한 액세스를 관리하는 정책을 설정할 수 있습니다. Windows 에 로그온하거나 사용자 세션 중 웹 사이트와 프로그램에 로그온할 경우 각 클래스의 사용자를 인증하는 데 필요한 인증 정보를 지정할 수 있습니다.

컴퓨터에 인증을 설정하려면 다음과 같이 하십시오.

1. 관리 콘솔의 왼쪽 패널에서 **보안**을 클릭한 다음 **인증**을 클릭합니다.
2. 로그온 인증을 구성하려면 **로그온 정책** 탭을 클릭하고 변경한 다음 **적용**을 클릭합니다.
3. 세션 인증을 구성하려면 **세션 정책** 탭을 클릭하고 변경한 다음 **적용**을 클릭합니다.

로그온 정책

Windows 에 로그온할 때 사용자 인증에 필요한 인증 정보를 관리하는 정책을 정의하려면 다음과 같이 하십시오.

1. 관리 콘솔의 왼쪽 패널에서 **보안**을 클릭한 다음 **인증**을 클릭합니다.
2. **로그온 정책** 탭에서 아래쪽 화살표를 클릭한 다음 사용자 범주를 선택합니다.
   - **이 컴퓨터의 관리자인 경우**
   - **관리자가 아닌 사용자의 경우**
3. 선택한 범주의 사용자에게 요구되는 인증 정보를 지정합니다.
4. 사용자를 인증하기 위해 지정된 인증 정보 중 하나만 요구할지 또는 지정한 인증 정보 모두를 요구할지를 선택합니다.
5. **적용**을 클릭합니다.

세션 정책

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

1. 관리 콘솔의 왼쪽 패널에서 **보안**을 클릭한 다음 **인증**을 클릭합니다.
2. **세션 정책** 탭에서 아래쪽 화살표를 클릭한 다음 사용자 범주를 선택합니다.
   - **이 컴퓨터의 관리자인 경우**
   - **관리자가 아닌 사용자의 경우**
3. 아래쪽 화살표를 클릭한 다음 선택한 사용자 범주에 요구되는 인증 정보를 선택합니다.
   - **지정된 인증 정보 중 하나 요구**

     참고: 인증 정보에 대한 확인란을 모두 선택 해제하면 **인증 필요 없음**을 선택한 것과 같습니다.
   - **지정된 인증 정보 모두 필요**
   - **인증 필요 없음**—이 옵션을 선택하면 창에서 모든 인증 정보가 해제됩니다.
4. **적용**을 클릭합니다.

설정

1. 다음 설정을 활성화하려면 확인란을 선택하고 비활성화하려면 확인란을 선택 해제합니다.

   One Step logon 허용—BIOS 또는 암호화된 디스크 수준에서 인증을 수행한 경우 이 컴퓨터의 사용자가 Windows 로그온을 생략할 수 있습니다.
2. **적용**을 클릭합니다.

사용자 관리

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

사용자들이 적절한 인증 정보를 등록해서 Security Manager 를 통해 설정된 정책을 충족시킬 수 있는가 여부와 상관없이 모든 HP ProtectTools 사용자가 나열되고 이러한 정책에 대한 확인이 이루어집니다.

사용자를 관리하려면 다음 설정 중에서 선택하십시오.

- 다른 사용자를 추가하려면 **추가**를 클릭합니다.
- 사용자를 삭제하려면 해당 사용자를 누른 후 **삭제**를 클릭합니다.
- 사용자에 대한 추가 인증 정보를 설정하려면 해당 사용자를 클릭한 후 **등록**을 클릭합니다.
- 특정 사용자의 정책을 보려면 해당 사용자를 선택한 다음 아래쪽 창에서 정책을 봅니다.

인증 정보

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

SpareKey

Windows 로그온에 SpareKey 인증을 허용할지 여부를 구성할 수 있고, SpareKey 등록 도중 사용자에게 표시될 보안 질문을 관리할 수 있습니다.

1. Windows 로그온에 SpareKey 인증 사용을 활성화하려면 확인란을 선택하고 비활성화하려면 확인란을 선택 해제합니다.
2. SpareKey 등록 도중 사용자에게 표시될 보안 질문을 선택합니다. 최대 세 개의 사용자 정의 질문을 지정하거나 사용자가 직접 패스프레이즈를 입력하도록 허용할 수 있습니다.
3. **적용**을 누릅니다.

지문

컴퓨터에 지문 인식기가 설치되거나 연결된 경우 지문 페이지에 다음 탭이 표시됩니다.

- **등록**—사용자가 등록할 수 있는 최소 및 최대 지문 수를 선택할 수 있습니다.

  지문 인식기에서 모든 데이터를 지울 수도 있습니다.

  ⚠ **주의:** 지문 인식기에서 전체 데이터를 지우면 관리자를 비롯한 모든 사용자의 지문 데이터 전체가 지워집니다. 지문만 사용하도록 로그온 정책이 설정된 경우 모든 사용자가 해당 컴퓨터에 로그온 할 수 없습니다.

- **민감도**—슬라이더를 이동하여 지문을 문지를 때 지문 인식기에 사용되는 민감도를 조정할 수 있습니다.

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

- **고급**—다음 옵션 중 하나를 선택하여 전원을 절약하고 시각적 피드백을 향상시키도록 지문 인식기를 구성할 수 있습니다.
  - **최적화됨**—필요한 경우 지문 인식기가 활성화됩니다. 인식기를 처음 사용하는 경우 약간 지연될 수 있습니다.
  - **전원 절약**—지문 인식기의 응답이 느리지만 전력을 적게 사용합니다.
  - **전체 전원**—지문 인식기를 언제든 사용할 수 있지만 전력을 많이 사용합니다.

스마트 카드

컴퓨터에 스마트 카드 리더가 설치되어 있거나 연결된 경우 스마트 카드 페이지에 다음과 같이 두 개의 탭이 표시됩니다.

- **설정**—스마트 카드를 제거하면 컴퓨터를 자동으로 잠글 수 있습니다.

참고: Windows 에 로그인할 때 인증 정보로 스마트 카드를 사용한 경우에만 컴퓨터가 잠깁니다. Windows 에 로그인하는 데 사용하지 않는 스마트 카드를 제거하면 컴퓨터가 잠기지 않습니다.

- **관리**—다음 옵션 중에서 선택합니다.
  - **스마트 카드 초기화**—HP Protect Tools 와 함께 사용할 스마트 카드를 준비합니다. HP ProtectTools(비대칭 키 쌍 및 관련 인증서 포함)를 사용하지 않고 이전에 스마트 카드를 초기화한 경우, 특정 인증서를 사용한 초기화가 필요하지 않는 한 다시 초기화하지 않아도 됩니다.
  - **스마트 카드 PIN 변경**—스마트 카드와 함께 사용되는 PIN 을 변경할 수 있습니다.
  - **HP ProtectTools 데이터만 삭제**—카드 초기화 도중 만든 HP ProtectTools 인증서만 삭제합니다. 다른 데이터는 카드에서 삭제하지 않습니다.
  - **스마트 카드의 모든 데이터 삭제**—지정된 스마트 카드의 모든 데이터를 삭제합니다. 이 카드는 더 이상 HP ProtectTools 또는 다른 응용프로그램에서 사용할 수 없습니다.

참고: 스마트 카드에서 지원하지 않는 기능은 사용할 수 없습니다.

▲ **적용**을 누릅니다.

얼굴

컴퓨터에 웹캠이 설치되거나 연결된 경우 Face Recognition 프로그램이 설치되어 있으면 컴퓨터 보안 위반으로 발생하는 어려움과 사용 편의성의 균형을 위해 Face Recognition 에 대한 보안 수준을 설정할 수 있습니다.

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. **인증 정보**를 누른 다음 **얼굴**을 누릅니다.
3. 편의성을 높이려면 슬라이더를 눌러 왼쪽으로 이동하고, 정확도를 높이려면 슬라이더를 눌러 오른쪽으로 이동합니다.
   - **낮음**—등록된 사용자가 손쉽게 한계 상황에 대한 액세스를 얻게 하려면 슬라이더 막대를 눌러 **낮음** 위치로 이동합니다.
   - **보통**—보안과 편의성 사이에서 적절한 조합을 제공하거나 무단 로그온이 발생할 수 있는 위치에 기밀 정보 또는 컴퓨터가 있는 경우 슬라이더 막대를 눌러 **보통** 위치로 이동합니다.
   - **높음**—등록된 장면 또는 현재 조명이 정상보다 어둡고 잘못 수락될 가능성이 낮은 경우 사용자가 액세스를 얻기가 더 어려워지게 하려면 슬라이더 막대를 눌러 **높음** 위치로 이동합니다.
4. **고급**을 누르고 추가 보안을 구성합니다. 자세한 내용은 35페이지의고급 사용자 설정을 참조하십시오.
5. **적용**을 누릅니다.

응용프로그램 구성

설정을 사용하면 현재 설치된 HP ProtectTools Security Manager 응용프로그램의 동작을 사용자 정의할 수 있습니다.

응용프로그램 설정을 수정하려면 다음과 같이 하십시오.

1. 관리 콘솔의 왼쪽 패널에서 **응용프로그램** 아래 **설정**을 클릭합니다.
2. 특정 설정을 활성화하려면 해당 설정 옆의 확인란을 선택하고 비활성화하려면 확인란을 선택 해제합니다.
3. **적용**을 클릭합니다.

일반 탭

일반 탭에서 사용할 수 있는 설정은 다음과 같습니다.

- **관리자일 때 설치 마법사를 자동으로 실행 안 함**—이 옵션을 선택하면 로그온할 때 마법사가 자동으로 실행되지 않습니다.
- **사용자일 때 시작 마법사를 자동으로 실행 안 함**—이 옵션을 선택하면 로그온할 때 사용자 설정이 자동으로 실행되지 않습니다.

응용프로그램 탭

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

- **응용프로그램 상태**—모든 응용프로그램에 대한 상태를 표시합니다.
- **Password Manager**—컴퓨터의 모든 사용자에 대해 Password Manager 를 활성화합니다.
- **Privacy Manager**—컴퓨터의 모든 사용자에 대해 Privacy Manager 를 활성화합니다.
- **중앙 관리 링크 활성화**—이 컴퓨터의 모든 사용자가 **중앙 관리**를 클릭해서 HP ProtectTools Security Manager 에 응용프로그램을 추가할 수 있습니다.

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

중앙 관리

다른 응용프로그램을 사용하여 Security Manager 에 새 관리 도구를 추가할 수 있습니다. 이 컴퓨터의 관리자는 설정 페이지에서 이 기능을 비활성화할 수 있습니다. 중앙 관리 페이지에는 두 개의 탭이 있습니다.

- **비즈니스 솔루션**—인터넷 연결을 사용할 수 있는 경우, DigitalPersona 웹 사이트 (http://www.digitalpersona.com/)에 액세스하면 새 응용프로그램을 확인할 수 있습니다.
- **업데이트 및 메시지**
  - 새 응용프로그램 및 업데이트에 대한 정보를 받아 보려면 **새 응용 프로그램 및 업데이트 관련 정보 수신** 확인란을 선택합니다.
  - 자동 업데이트 일정을 설정하려면 일 수를 선택합니다.
  - 업데이트를 확인하려면 **지금 확인**을 클릭합니다.

4 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 암호를 관리합니다.
- Windows® 운영체제 암호를 쉽게 변경합니다.
- 프로그램 기본 설정을 구성합니다.
- 더 강력한 보안과 편의를 위해 지문을 사용합니다.
- 인증을 위해 하나 이상의 장면을 등록합니다.
- 인증용 스마트 카드를 설정합니다.
- 프로그램 데이터를 백업 및 복원합니다.
- 응용프로그램을 추가합니다.

Security Manager 열기

다음과 같은 방법으로 Security Manager 를 열 수 있습니다.

- **시작**, **모든 프로그램**, **HP**, **HP ProtectTools Security Manager** 를 차례로 누릅니다.
- 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 누릅니다.
- **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누르고 **HP ProtectTools Security Manager 열기**를 누릅니다.
- **HP ProtectTools** 바탕 화면 가젯 아이콘을 클릭합니다.
- 핫키 조합 ctrl+Windows 로고 키+h 를 눌러 **Security Manager 빠른 링크** 메뉴를 엽니다.

  핫키 조합 변경에 대한 자세한 내용은 31페이지의설정을 참조하십시오.

Security Manager 대시보드 사용

Security Manager 대시보드는 Security Manager 기능, 응용프로그램, 설정 등에 쉽게 액세스할 수 있는 중앙 위치입니다.

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

대시보드에는 다음 구성 요소가 표시됩니다.

- **ID 카드**—로그인한 사용자 계정을 식별하기 위한 Windows 사용자 이름 및 선택된 사진을 표시합니다.
- **보안 응용프로그램**—다음 보안 범주를 구성하기 위한 링크의 확장 메뉴를 표시합니다.
  - **홈**—암호를 관리하거나 인증 정보를 설정하거나 보안 응용프로그램의 상태를 확인합니다.
  - **상태**—HP ProtectTools 보안 응용프로그램의 상태를 확인합니다.

참고: 컴퓨터에 설치되어 있지 않은 응용프로그램은 다음 목록에 표시되지 않습니다.

- **내 로그온**—Password Manager, Credential Manager, 암호, SpareKey, 스마트 카드, 얼굴 및 지문을 사용하여 사용자 인증 정보를 관리합니다.
- **내 데이터**—Drive Encryption 및 File Sanitizer 를 사용하여 데이터의 보안을 관리합니다.
- **내 컴퓨터**—Device Access Manager 를 사용하여 컴퓨터의 보안을 관리합니다.
- **내 통신**—Privacy Manager 를 사용하여 통신의 보안을 관리합니다.
- **관리**—관리자는 다음 옵션에 액세스할 수 있습니다.
  - **관리 콘솔**—관리자가 보안 및 사용자를 관리할 수 있습니다.
  - **중앙 관리**—관리자가 추가 해결 방법, 제품 업데이트 및 메시지에 액세스할 수 있습니다.
- **고급**—다음 항목을 비롯한 추가 기능에 액세스하기 위한 명령을 표시합니다.
  - **기본 설정**—Security Manager 설정을 개별화할 수 있습니다.
  - **백업 및 복원**—데이터를 백업하거나 복원할 수 있습니다.
  - **정보**—버전 번호와 저작권 고지와 같은 HP ProtectTools Security Manager 에 대한 정보를 표시합니다.
- **주 영역**—응용프로그램별 화면을 표시합니다.
- **?**—Security Manager 소프트웨어 도움말을 표시합니다. 이 아이콘은 창 오른쪽 상단 최소화/최대화 아이콘 옆에 있습니다.

보안 응용프로그램 상태

다음 두 곳에서 설치된 보안 응용프로그램의 상태를 확인할 수 있습니다.

- **HP ProtectTools 바탕 화면 가젯**

  HP ProtectTools 가젯 아이콘 위의 배너 색상이 변경되면서 설치된 보안 응용프로그램의 전체 보안 상태가 반영됩니다.

  - **빨간색**—경고
  - **노란색**—주의: 구성되지 않음
  - **파란색**—양호

  가젯 아이콘 아래쪽에 다음 상태 중 하나를 나타내는 메시지가 표시됩니다.

  - **지금 설정**—관리자가 가젯 아이콘을 클릭하고 Security Manager 설정 마법사를 실행하여 컴퓨터의 인증 정보를 구성해야 합니다.

    설정 마법사는 독립형 응용프로그램입니다.

  - **지금 등록**—사용자가 가젯 아이콘을 클릭하고 Security Manager 시작 마법사를 실행하여 인증 정보를 등록해야 합니다.

    Security Manager 대시보드에 시작 마법사가 표시됩니다.

  - **지금 확인**—가젯 아이콘을 클릭하면 보안 응용프로그램 상태 페이지에 자세한 내용이 표시됩니다.

- **보안 응용프로그램 상태 페이지**—Security Manager 대시보드에서 **상태**를 클릭하면 설치한 보안 응용프로그램의 전체 상태 및 각 응용프로그램별 특정 상태가 표시됩니다.

내 로그온

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

- **Password Manager**—Windows 암호, 지문 또는 스마트 카드로 인증하여 웹 사이트와 프로그램을 실행하고 로그온할 수 있는 빠른 링크를 생성 및 관리합니다.
- **인증 정보**—손쉽게 Windows 암호를 변경하거나 지문을 등록하거나 스마트 카드를 설정할 수 있습니다.

관리자는 **관리**를 클릭한 후 대시보드 왼쪽 하단에 있는 **중앙 관리**를 클릭하여 응용프로그램을 추가할 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

Password Manager 아이콘은 웹 페이지 또는 응용프로그램 로그온 화면의 왼쪽 상단에 표시됩니다. 해당 웹 사이트 또는 응용프로그램에 대한 로그온이 아직 생성되지 않은 경우 아이콘에 더하기(+) 기호가 표시됩니다.

▲ **Password Manager** 아이콘을 누르면 다음 옵션 중에서 선택할 수 있는 컨텍스트 메뉴가 표시됩니다.

로그온이 아직 생성되지 않은 웹 페이지나 프로그램의 경우

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**—Security Manager 소프트웨어 도움말을 표시합니다.

로그온이 이미 생성된 웹 페이지나 프로그램의 경우

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.

- **로그온 추가**—로그온에 계정을 추가할 수 있습니다.
- **Password Manager 열기**—Password Manager 를 실행합니다.
- **도움말**—Security Manager 소프트웨어 도움말을 표시합니다.

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

로그온 추가

웹 사이트나 프로그램에 대한 로그온을 쉽게 추가할 수 있습니다. 로그온 정보를 한 번 입력하기만 하면 그 다음부터 Password Manager 가 자동으로 정보를 입력합니다. 웹 사이트나 프로그램을 탐색한 후에 이러한 로그온을 사용할 수 있고 **로그온** 메뉴에서 로그온을 누르면 Password Manager 에서 웹 사이트나 프로그램을 열어 둔 채로 로그온할 수 있습니다.

로그온을 추가하려면:

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 상자의 해당 필드에는 굵은 주황색 테두리가 표시됩니다. **Password Manager 관리** 탭에서 **로그온 추가**를 클릭하여 이 대화 상자를 표시할 수도 있습니다. 컴퓨터에 연결된 보안 장치에 따라 ctrl+Windows 로고 키+h 핫키를 사용하거나 지문을 인식시키거나 스마트 카드를 넣는 등의 옵션이 적용됩니다.
   a. 로그온 필드를 미리 서식이 지정된 선택 사항 중 하나로 채우려면 필드 오른쪽에 있는 화살표를 누릅니다.
   b. 이 로그온의 암호를 보려면 **암호 표시**를 누릅니다.
   c. 로그온 필드를 채웠지만 제출하지 않으려면 **자동으로 로그온 데이터 제출** 확인란을 선택 해제합니다.
   d. VeriSign VIP 보안을 활성화하려면 **I want VIP security on this site**(이 사이트에서 VIP 보안 사용) 확인란을 선택하십시오.

      이 옵션은 VIP(VeriSign Identity Protection)를 사용할 수 있는 사이트에만 표시됩니다. 사이트에서 지원하는 경우 일반적인 인증 방법을 통해 VIP 보안 코드가 자동으로 작성되도록 선택할 수도 있습니다.
   e. **확인**을 누르고 사용할 인증 방법(지문, 암호 또는 얼굴)을 누른 후 선택한 인증 방법으로 로그온합니다.

      Password Manager 아이콘에서 더하기(+) 기호가 제거되면 로그온이 생성된 것입니다.
   f. Password Manager 가 로그온 필드를 검색하지 못하면 **추가 필드**를 누릅니다.
      - 로그온에 필요한 각 필드의 확인란을 선택하거나, 로그온에 필요하지 않은 필드의 확인란을 선택 해제합니다.
      - Password Manager 가 모든 로그온 필드를 검색하지 못하면 계속할 것인지 묻는 메시지가 표시됩니다. **예**를 누릅니다.

- 로그온 필드가 채워진 대화 상자가 열립니다. 각 필드의 아이콘을 누르고 해당 로그온 필드로 끌어온 다음 버튼을 눌러 웹 사이트에 로그인합니다.

참고: 사이트의 로그온 데이터 입력 시 수동 모드를 사용하면 이후에 동일한 웹 사이트에 로그온할 때 계속해서 이 방법을 사용해야 합니다.

참고: 로그온 데이터 입력에 대한 수동 모드는 Internet Explorer 8 에서만 사용할 수 있습니다.

- **닫기**를 누릅니다.

해당 웹 사이트에 액세스하거나 해당 프로그램을 열 때마다 웹 사이트 또는 응용프로그램 로그온 화면의 왼쪽 상단에 **Password Manager** 아이콘이 표시되며, 이는 로그온 시 등록한 인증 정보를 사용할 수 있음을 나타냅니다.

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.
   - 미리 서식이 지정된 선택 사항 중 하나를 사용하여 **사용자 이름** 로그온 필드를 선택하려면 채우려면 필드 오른쪽에 있는 아래쪽 화살표를 누릅니다.
   - 미리 서식이 지정된 선택 사항 중 하나를 사용하여 **암호** 로그온 필드를 선택하려면 필드 오른쪽에 있는 아래쪽 화살표를 누릅니다.
   - VeriSign VIP 보안을 활성화하려면 **I want VIP security on this site**(이 사이트에서 VIP 보안 사용) 확인란을 선택하십시오.

     이 옵션은 VeriSign VIP 보안을 사용할 수 있는 사이트에만 표시됩니다. 사이트에서 지원하는 경우 일반적인 인증 방법을 통해 VIP 보안 코드가 자동으로 작성되도록 선택할 수도 있습니다.
   - 추가 필드를 화면에서 로그온으로 추가하려면 **추가 필드**를 누릅니다.
   - 이 로그온의 암호를 보려면 **암호 표시**를 누릅니다.
   - 로그온 필드를 채웠지만 제출하지 않으려면 **자동으로 로그온 데이터 제출** 확인란을 선택 해제합니다.
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 입력합니다.

로그온이 생성되면 Password Manager **로그온** 메뉴에 자동으로 추가됩니다.

로그온 메뉴를 표시하려면:

1. **Password Manager** 핫키 조합(ctrl+Windows 로고 키+h 로 기본 설정되어 있음)을 누릅니다. 핫키 조합을 변경하려면 Security Manager 대시보드에서 **Password Manager** 를 클릭한 다음 **설정**을 클릭합니다.
2. 컴퓨터에 내장되어 있거나 연결된 지문 인식기에 지문을 대거나 Windows 암호를 입력합니다.

로그온을 범주로 구성

로그온을 정리할 범주를 1 개 이상 생성하고, 원하는 범주로 로그온을 끌어다 놓습니다.

범주를 추가하려면:

1. Security Manager 대시보드에서 **Password Manager** 를 누릅니다.
2. **관리** 탭을 누르고 **범주 추가**를 누릅니다.
3. 범주의 이름을 입력합니다.
4. **확인**을 누릅니다.

로그온을 범주에 추가하려면:

1. 원하는 로그온 위에 마우스 포인터를 놓습니다.
2. 왼쪽 마우스 버튼을 길게 누릅니다.
3. 로그온을 범주 목록으로 끌어 옵니다. 범주 위로 마우스 포인터를 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 여러 로그온 계정에 대한 로그온 정보를 하나의 중앙 위치에서 쉽게 관리할 수 있습니다.

로그온은 **관리** 탭에 나열됩니다. 동일한 웹 사이트에 대해 로그온이 여러 개 생성된 경우 각 로그온이 웹 사이트 이름 아래에 나열되고 로그온 목록에서 들여쓰기됩니다.

로그온을 관리하려면:

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

- **로그온 추가**—**로그온 추가**를 누르고 화면의 지시를 따릅니다.
- **사용자의 로그온**—기존 로그온을 누르고 다음 옵션 중 하나를 선택한 후 화면의 지시를 따릅니다.
  - **열기**—기존 로그온이 있는 웹 사이트나 프로그램을 엽니다.
  - **추가**—로그온을 추가합니다. 자세한 내용은 26페이지의로그온 추가를 참조하십시오.

- **편집**—로그온을 편집합니다. 자세한 내용은 27페이지의로그온 편집을 참조하십시오.
- **삭제**—기존 로그온이 있는 웹 사이트나 프로그램을 삭제합니다.

- **범주 추가—범주 추가**를 누르고 화면의 지시를 따릅니다. 자세한 내용은 28페이지의로그온을 범주로 구성을 참조하십시오.

웹 사이트나 프로그램에 대한 로그온을 더 추가하려면:

1. 웹 사이트나 프로그램에 대한 로그온 화면을 엽니다.
2. **Password Manager** 아이콘을 눌러 컨텍스트 메뉴를 표시합니다.
3. **로그온 추가**를 누른 다음 화면의 지시를 따릅니다.

암호 강도 평가

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 더하기(+) 기호를 표시하여 화면에 대한 로그온을 추가할 것인지 묻습니다.

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

   - **로그온 화면에 로그온을 추가하라는 메시지를 표시**—아직 로그온이 설정되지 않은 로그온 화면이 표시될 때 로그온을 추가할 것인지 묻는 메시지를 표시하려면 이 옵션을 누릅니다.
   - **이 화면 제외**—이 로그온 화면에 대한 로그온을 추가할 것인지 다시 묻지 않으려면 이 확인란을 선택합니다.

     이전에 제외한 화면에 대한 로그온을 추가하려면 다음과 같이 하십시오.

     - 이전에 제외한 웹 사이트 로그온이나 프로그램 페이지가 표시되는 동안 Security Manager 대시보드를 열고 **Password Manager** 를 누릅니다.
     - **로그온 추가**를 누릅니다.

       현재 화면 필드에 나열된 웹 사이트 로그온 화면 또는 프로그램과 함께 로그온 추가 대화 상자가 열립니다.
     - **계속**을 누릅니다.

       Password Manager 에 로그온 추가 화면이 표시됩니다.

- 화면의 지시를 따릅니다. 자세한 내용은 26페이지의로그온 추가를 참조하십시오.
- 이 웹 사이트 로그온 또는 프로그램 화면을 열 때마다 **Password Manager** 아이콘이 표시됩니다.

2. 로그온 화면에 대한 로그온을 추가하라는 메시지를 표시하는 옵션을 비활성화하려면 확인란을 선택합니다.
3. 추가 Password Manager 설정에 액세스하려면 Security Manager 대시보드에서 **Password Manager** 를 누르고 **설정**을 누릅니다.

VIP(VeriSign Identity Protection)

VeriSign VIP 를 지원하는 웹 사이트와 함께 사용하기 위해 VeriSign VIP Access 토큰을 생성할 수 있습니다. 이러한 토큰은 Password Manager 에서 VeriSign VIP 를 지원하는 로그온 화면에 끌어다 놓거나 해당 필드에 수동으로 입력한 토큰 사용을 통합하는 자동화된 로그온을 생성하는 데 사용됩니다.

Security Manager 대시보드 또는 VeriSign VIP 를 지원하는 웹 사이트에서 VeriSign VIP 를 활성화하고 토큰을 만들 수 있습니다. 토큰을 사용하려면 토큰을 사용할 각 웹 사이트에 해당 토큰을 등록해야 합니다.

토큰을 등록하여 처음 사용한 후에는 일반적인 로그온 인증 정보에 추가되거나(선택 사항) 제출될 수 있습니다. 토큰 추가를 허용하지 않는 사이트의 경우 토큰을 끌어다 놓거나 토큰 정보를 수동으로 입력할 수 있습니다.

Security Manager 대시보드에서 VeriSign VIP 를 활성화하고 VeriSign VIP 토큰을 생성하려면 다음과 같이 하십시오.

1. Security Manager 대시보드를 엽니다. 자세한 내용은 22페이지의 Security Manager 열기를 참조하십시오.
2. **Password Manager** 를 누르고 **VIP** 를 누릅니다.
3. **VIP 획득**을 클릭합니다.

   VeriSign VIP 토큰이 생성되고 VeriSign VIP 페이지에 표시됩니다. 이제 이 페이지에 액세스할 때마다 토큰이 표시됩니다.

웹 사이트에서 VeriSign VIP 를 활성화하고 VeriSign VIP 토큰을 만들려면 다음과 같이 하십시오.

1. VeriSign VIP 를 지원하는 웹 사이트에 방문할 때마다 Password Manager 에서 알려줍니다.
2. 화면에 대한 로그온을 만듭니다. 자세한 내용은 26페이지의로그온 추가를 참조하십시오.
3. 로그온 만들기 대화 상자에서 **VIP 를 사용하여 계정 보안 강화**를 선택합니다.

웹 사이트에 대한 VeriSign VIP 토큰을 등록하려면 다음과 같이 하십시오.

1. VeriSign VIP 를 지원하는 웹 사이트에 수동으로 로그온하거나 Password Manager 로그온을 통해 로그온합니다.
2. 표시되는 VeriSign VIP 풍선을 눌러 이 사이트에 대한 로그온을 만듭니다.
3. Password Manager 에 로그온 추가 대화 상자에서 **I want VIP security on this site**(이 사이트에서 VIP 보안 사용)를 선택합니다.

   이 옵션은 VeriSign VIP 보안을 사용할 수 있는 사이트에만 표시됩니다. 사이트에서 지원하는 경우 일반적인 인증 방법을 통해 VIP 보안 코드가 자동으로 작성되도록 선택할 수도 있습니다.

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 더하기(+) 기호가 표시되며, 이는 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. **ctrl+win+h 로 Password Manager 열기**—**Password Manager 빠른 링크** 메뉴를 여는 기본 핫키는 ctrl+Windows 로고 키+h 입니다. 핫키를 변경하려면 이 옵션을 클릭하고 새로운 키 조합을 입력합니다. 조합에는 ctrl, alt 또는 shift 중 하나 이상과 임의의 알파벳 또는 숫자 키를 포함할 수 있습니다.
3. **적용**을 눌러 변경 사항을 저장합니다.

Credential Manager

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

사용 가능한 인증 정보는 이 컴퓨터에 내장되거나 연결되어 있는 보안 장치에 따라 다를 수 있습니다. **내 로그온** 아래에 있는 **Credential Manager** 를 누르면 지원되는 인증 정보와 요구 사항, 현재 상태가 표시되며 다음과 같은 내용이 포함되어 있습니다.

- 암호
- SpareKey
- 지문
- 스마트 카드
- 얼굴

인증 정보를 등록하거나 변경하려면 링크를 누르고 화면의 지시를 따릅니다.

Windows 암호 변경

Security Manager 를 사용하면 Windows 제어판에서보다 쉽고 빠르게 Windows 암호를 변경할 수 있습니다.

Windows 암호를 변경하려면 다음과 같이 하십시오.

1. Security Manager 대시보드에서 **Credential Manager** 를 누른 다음 **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.

SpareKey 설정

SpareKey 를 사용하면 이전에 관리자가 정의한 목록에서 세 가지 보안 질문에 답변하여 지원 플랫폼의 컴퓨터에 액세스할 수 있습니다.

시작 마법사의 초기 설정 과정 중에 개인 SpareKey 를 설정하라는 메시지가 HP ProtectTools Security Manager 에 표시됩니다.

SpareKey 를 설정하려면

1. 마법사의 SpareKey 페이지에서 세 가지 보안 질문을 선택한 다음 각 질문에 대한 답변을 입력합니다.
2. **다음**을 누릅니다.

다른 질문을 선택하거나 **Credential Manager** 아래의 SpareKey 페이지에서 답변을 변경할 수 있습니다.

SpareKey 를 설정하면 부팅 전 로그온 화면이나 Windows 시작 화면에서 SpareKey 를 사용하여 컴퓨터에 액세스할 수 있습니다.

지문 등록

지문 인식기가 컴퓨터에 내장되어 있거나 연결된 경우 HP ProtectTools Security Manager 가 시작 마법사의 초기 설정 과정 중에 지문을 설정하거나 "등록"하라는 메시지를 표시합니다. Security Manager 대시보드의 **Credential Manager** 에 있는 지문 페이지에서 지문을 등록할 수도 있습니다.

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

참고: 이전에 등록한 지문을 삭제하려면 해당 손가락을 누르십시오.

2. 등록할 손가락을 선택하면 지문이 성공적으로 등록될 때까지 해당 손가락을 인식시키라는 메시지가 나타납니다. 등록된 손가락은 윤곽선에 녹색으로 표시됩니다.
3. 최소한 두 손가락, 가능하면 검지와 중지를 등록하는 것이 좋습니다. 다른 손가락에 대해 1~2 단계를 반복합니다.
4. **다음**을 클릭한 후 화면의 지시를 따릅니다.

주의: 시작하기 프로세스를 통해 지문을 등록하는 경우는 **다음**을 클릭할 때까지 지문 정보가 저장되지 않습니다. 컴퓨터를 한동안 사용하지 않은 상태로 두거나 프로그램을 닫으면 변경한 내용이 저장되지 **않습니다**.

스마트 카드 설정

인증용으로 사용할 스마트 카드는 관리자가 먼저 초기화하고 등록해야 합니다.

스마트 카드 초기화

HP ProtectTools Security Manager 는 다양한 스마트 카드를 지원합니다. PIN 번호로 사용되는 숫자나 문자 유형은 다양할 수 있습니다. 스마트 카드 제조업체는 HP ProtectTools 의 보안 알고리즘에 사용될 보안 인증서 및 관리 PIN 을 설치할 도구를 제공해야 합니다.

참고: ActivIdentity 소프트웨어를 반드시 설치해야 합니다.

1. 카드 리더에 카드를 넣습니다.
2. **시작**, **모든 프로그램** 및 **ActivClient PIN 초기화 도구**를 차례로 클릭합니다.
3. PIN 을 입력하고 확인합니다.
4. **다음**을 클릭합니다.

스마트 카드 소프트웨어에서 잠금 해제 키를 제공합니다. 대부분의 스마트 카드는 잘못된 PIN 이 5 회 입력되면 스스로 잠깁니다. 이 키는 카드를 잠금 해제할 때 사용합니다.

5. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
6. **인증 정보**와 **스마트 카드**를 차례로 클릭합니다.
7. **관리** 탭을 클릭합니다.
8. **스마트 카드 설정**을 선택합니다.
9. PIN 을 입력하고 **적용**을 클릭한 다음 화면의 지시를 따릅니다.
10. 스마트 카드를 초기화한 후에는 스마트 카드를 등록해야 합니다.

스마트 카드 등록

스마트 카드를 초기화한 후에는 관리자가 다음과 같이 HP ProtectTools 관리 콘솔에서 스마트 카드를 인증 방법으로 등록할 수 있습니다.

1. **중앙 관리**에 있는 **설정 마법사**를 클릭합니다.
2. 시작 페이지에서 **다음**을 클릭한 후 Windows 암호를 입력합니다.
3. SpareKey 페이지에서 **SpareKey 설정 건너뛰기**를 클릭합니다(SpareKey 정보를 업데이트하지 않을 경우).
4. 보안 기능 활성화 페이지에서 **다음**을 클릭합니다.
5. 인증 정보 선택 페이지에서 **스마트 카드 설정**을 선택하고 **다음**을 클릭합니다.
6. 스마트 카드 페이지에서 PIN 을 입력하고 **다음**을 클릭합니다.
7. **마침**을 클릭합니다.

Security Manager 에서도 스마트 카드를 등록할 수 있습니다. 자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

스마트 카드 구성

컴퓨터에 스마트 카드 리더가 설치되어 있거나 연결된 경우 스마트 카드 페이지에 다음과 같이 두 개의 탭이 표시됩니다.

- **설정**—스마트 카드를 제거하면 컴퓨터를 자동으로 잠글 수 있습니다.

참고: Windows 에 로그인할 때 인증 정보로 스마트 카드를 사용한 경우에만 컴퓨터가 잠깁니다. Windows 에 로그인하는 데 사용하지 않는 스마트 카드를 제거하면 컴퓨터가 잠기지 않습니다.

- **관리**—다음 옵션 중에서 선택합니다.
  - **스마트 카드 초기화**—HP Protect Tools 와 함께 사용할 스마트 카드를 준비합니다. HP ProtectTools(비대칭 키 쌍 및 관련 인증서 포함)를 사용하지 않고 이전에 스마트 카드를 초기화한 경우, 특정 인증서를 사용한 초기화가 필요하지 않는 한 다시 초기화하지 않아도 됩니다.
  - **스마트 카드 PIN 변경**—스마트 카드와 함께 사용되는 PIN 을 변경할 수 있습니다.

- **HP ProtectTools 데이터만 삭제**—카드 초기화 도중 만든 HP ProtectTools 인증서만 삭제합니다. 다른 데이터는 카드에서 삭제하지 않습니다.
- **스마트 카드의 모든 데이터 삭제**—지정된 스마트 카드의 모든 데이터를 삭제합니다. 이 카드는 더 이상 HP ProtectTools 또는 다른 응용프로그램에서 사용할 수 없습니다.

참고: 스마트 카드에서 지원하지 않는 기능은 사용할 수 없습니다.

▲ **적용**을 누릅니다.

얼굴 로그온에 사용할 사진 그룹 등록

웹캠이 컴퓨터에 내장되어 있거나 연결된 경우 시작 마법사의 초기 설정 과정 중에 장면을 설정하거나 "등록"하라는 메시지가 HP ProtectTools Security Manager 에 표시됩니다. Security Manager 대시보드에서 **Credential Manager** 아래에 있는 얼굴 로그온 페이지에서 사진 그룹을 등록할 수도 있습니다.

얼굴 인식 로그온을 사용하려면 하나 이상의 장면을 등록해야 합니다. 성공적으로 등록한 후에는, 다음 조건 중 하나 이상이 변경되어 로그온하기 어려운 경우 새로운 장면을 등록할 수도 있습니다.

- 마지막으로 등록한 이후로 얼굴이 상당히 달라진 경우
- 이전 등록과 비교해 조명 상태가 상당히 달라진 경우
- 마지막으로 등록할 당시에는 안경을 쓴(또는 안 쓴) 상태였던 경우

참고: 장면을 등록하기 어려운 경우 웹캠 가까이 이동해 보십시오.

시작 마법사에서 사진 그룹을 등록하려면:

1. 마법사의 얼굴 페이지에서 **고급**을 누르고 추가 보안을 구성합니다. 자세한 내용은 35페이지의 고급 사용자 설정을 참조하십시오.
2. **확인**을 누릅니다.
3. **시작**을 누르거나, 이전에 등록한 사진 그룹이 있는 경우 **새 사진 그룹 등록**을 누릅니다.
4. 추가 보안 옵션을 선택하지 않은 경우 추가 보안 옵션을 선택하라는 메시지가 표시됩니다. 화면의 지시를 따른 후 **다음**을 클릭합니다. 자세한 내용은 35페이지의고급 사용자 설정을 참조하십시오.
5. **카메라** 아이콘을 누른 후 화면의 지시에 따라 사진 그룹을 등록합니다.

   화면의 지시를 따르고 사진 그룹을 캡처하는 동안 이미지를 확인하십시오.
6. **다음**을 누릅니다.
7. **마침**을 누릅니다.

다음과 같은 방법으로도 Security Manager 대시보드에서 사진 그룹을 등록할 수 있습니다.

1. Security Manager 대시보드를 엽니다. 자세한 내용은 22페이지의 Security Manager 열기를 참조하십시오.
2. **내 로그온**에서 **Credential Manager** 를 누른 다음 **얼굴**을 누릅니다.
3. **고급**을 누르고 추가 보안을 구성합니다. 자세한 내용은 35페이지의고급 사용자 설정을 참조하십시오.
4. **확인**을 누릅니다.

5. **시작**을 누르거나, 이전에 등록한 사진 그룹이 있는 경우 **새 사진 그룹 등록**을 누릅니다.
6. 추가 보안 옵션을 선택하지 않은 경우 추가 보안 옵션을 선택하라는 메시지가 표시됩니다. 화면의 지시를 따른 후 **다음**을 클릭합니다. 자세한 내용은 35페이지의고급 사용자 설정을 참조하십시오.
7. **카메라** 아이콘을 누른 후 화면의 지시에 따라 사진 그룹을 등록합니다.

   화면의 지시를 따르고 사진 그룹을 캡처하는 동안 이미지를 확인하십시오.

자세한 내용은 얼굴 로그온 페이지 오른쪽 상단에 있는 파란색 **?** 아이콘을 눌러 Face Recognition 소프트웨어 도움말을 참조하십시오.

고급 사용자 설정

추가 보안을 선택하지 않은 경우 추가 보안 페이지에도 이러한 옵션이 표시됩니다.

1. Security Manager 대시보드를 엽니다. 자세한 내용은 22페이지의 Security Manager 열기를 참조하십시오.
2. **내 로그온**에서 **Credential Manager** 를 누른 다음 **얼굴**을 누릅니다.
3. **고급**을 눌러 다음 보안 옵션을 구성합니다.

   a. **보안** 탭—다음 옵션 중 하나를 선택합니다.

   - **추가 보안 사용 안 함**—얼굴 로그온에 대한 추가 보안을 사용하지 않으려면 이 옵션을 선택합니다.
   - **추가 보안을 위해 PIN 사용**—얼굴 로그온에 사용자별 PIN 을 사용하려면 이 옵션을 선택합니다.
     - **PIN 만들기**를 누릅니다.
     - Windows 암호를 입력합니다.
     - 새 PIN 을 입력한 후 한 번 더 입력하여 새 PIN 을 확인합니다.

       PIN 을 생성하고 나면 **변경**, **재설정** 또는 **PIN 제거** 옵션 중에서 선택할 수 있습니다.
   - **추가 보안을 위해 Bluetooth 사용**—Face Recognition 에 Bluetooth 가 지원되는 휴대폰을 연결하려면 이 옵션을 선택합니다. Windows 로그온 과정에서 얼굴이 인증되면 Face Recognition 에서 연결된 Bluetooth 휴대폰이 있는지 확인합니다. Bluetooth 가 지원되는 휴대폰이 있는 경우 Windows 에 로그온할 수 있습니다.
     - 컴퓨터와 휴대폰에서 Bluetooth 가 활성화되어 있는지 확인하십시오.

       Bluetooth 가 지원되는 휴대폰이 없는 경우 연결된 Bluetooth 휴대폰을 활성화하고 로그온 프로세스를 다시 시작하라는 메시지가 표시됩니다. 30 초 후에 Face Recognition 창이 일시 정지됩니다. 로그온 프로세스를 초기화하려면 **카메라** 아이콘을 누릅니다. Bluetooth 가 지원되는 휴대폰이 없는 경우 일반적인 Windows 암호를 사용하여 로그온할 수 있습니다.
     - **추가**를 누릅니다.
     - Bluetooth 장치가 표시되면 해당 장치를 선택한 후 **다음**을 누릅니다.

확인을 누릅니다.

b. **기타 설정** 탭—확인란을 선택하여 다음 옵션 중 하나 이상을 활성화하거나 확인란을 선택 해제하여 옵션을 비활성화합니다. 이러한 설정은 현재 사용자에게만 적용됩니다.

- **얼굴 인식 이벤트용 소리 재생**—얼굴 로그온에 성공하거나 실패할 경우 소리를 재생합니다.
- **로그온 실패 시 얼굴 사진 업데이트**—얼굴 로그온에 실패했지만 암호를 정확히 입력하는 경우 향후 얼굴 인식 로그온의 성공률을 높이기 위해 일련의 이미지를 저장하라는 메시지가 나타납니다.
- **로그온 실패 시 새 얼굴 사진 등록**—암호를 정확히 입력했는데도 얼굴 로그온에 실패한 경우 향후 얼굴 인식 로그온의 성공률을 높이기 위해 새 얼굴 사진을 등록하라는 메시지가 나타납니다.

확인을 누릅니다.

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 돌출되어 표시됩니다.

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

표시된 이름을 변경하려면:

1. Security Manager 대시보드를 엽니다. 자세한 내용은 22페이지의 Security Manager 열기를 참조하십시오.
2. 대시보드의 왼쪽 상단에 있는 ID 카드를 누릅니다.
3. 이 계정에 대한 Windows 사용자 이름이 표시된 상자를 누르고 새 이름을 입력한 다음 **저장**을 누릅니다.

표시된 사진을 변경하려면:

1. Security Manager 대시보드를 엽니다. 자세한 내용은 22페이지의 Security Manager 열기를 참조하십시오.
2. 대시보드의 왼쪽 상단에 있는 ID 카드를 누릅니다.
3. **사진 선택**을 누르고 이미지를 누른 다음 **저장**을 누릅니다.

기본 설정 구성

HP ProtectTools Security Manager 에 대한 개인 설정을 지정할 수 있습니다. Security Manager 대시보드에서 **고급**을 누르고 **기본 설정**을 누릅니다. 사용 가능한 설정이 **일반** 탭과 **지문** 탭에 표시됩니다.

일반 탭

모양—작업 표시줄 알림 영역에 아이콘 표시

- 작업 표시줄에 아이콘 표시를 활성화하려면 확인란을 선택합니다.
- 작업 표시줄에 아이콘 표시를 비활성화하려면 확인란을 선택 해제합니다.

지문 탭

참고: 컴퓨터에 지문 인식기와 올바른 드라이버가 설치된 경우에만 **지문** 탭을 사용할 수 있습니다.

- **빠른 동작**—지문을 대고 있는 동안 지정된 키를 누를 때 수행할 Security Manager 작업을 선택할 수 있습니다.

  나열된 키 중 하나에 빠른 동작을 지정하려면 **(키) + 지문** 옵션을 누른 다음 메뉴에서 사용 가능한 작업 중 하나를 선택합니다.

- **지문 스캔 피드백**—지문 인식기가 사용 가능한 경우에만 표시됩니다. 이 설정을 사용하여 지문을 인식시킬 때 발생하는 피드백을 조정할 수 있습니다.

  - **사운드 피드백 활성화**—지문을 인식시키면 Security Manager 가 특정 프로그램 이벤트마다 다른 사운드를 재생하면서 오디오 피드백을 제공합니다. Windows 제어판의 **사운드** 탭에서 이러한 이벤트에 새 사운드를 지정하거나 이 옵션을 선택 해제하여 사운드 피드백을 비활성화할 수 있습니다.

  - **스캔 품질 피드백 표시**

품질에 관계없이 모든 지문 인식 결과를 표시하려면 확인란을 선택합니다.

품질이 좋은 지문 인식 결과만 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.

참고: 이 기능으로는 데이터만 백업됩니다.

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

데이터를 백업하려면:

1. Security Manager 대시보드를 엽니다. 자세한 내용은 22페이지의 Security Manager 열기를 참조하십시오.
2. 대시보드의 왼쪽 패널에서 **고급**을 클릭하고 **백업 및 복원**을 클릭합니다.
3. **데이터 백업**을 누릅니다.
4. 함께 백업하려는 모듈을 선택합니다. 대부분의 경우 전체 모듈을 선택합니다.
5. 사용자의 신원을 확인합니다.
6. 저장 파일의 이름을 입력합니다. 파일은 기본적으로 문서 폴더에 저장됩니다. 다른 위치를 지정하려면 **찾아보기**를 누릅니다.
7. 파일을 보호하려면 암호를 입력합니다.
8. **마침**을 누릅니다.

데이터를 복원하려면:

1. Security Manager 대시보드를 엽니다. 자세한 내용은 22페이지의 Security Manager 열기를 참조하십시오.
2. 대시보드의 왼쪽 패널에서 **고급**을 클릭하고 **백업 및 복원**을 클릭합니다.
3. **데이터 복원**을 누릅니다.
4. 이전에 만든 저장 파일을 선택합니다. 제공된 필드에 경로를 입력하거나 **찾아보기**를 누릅니다.
5. 파일 보호를 위해 사용한 암호를 입력합니다.
6. 데이터를 복원할 모듈을 선택합니다. 대부분의 경우 나열된 전체 모듈을 선택합니다.
7. Windows 암호를 확인합니다.
8. **마침**을 누릅니다.

5 Drive Encryption for HP ProtectTools(일부 모델만 해당)

Drive Encryption for HP ProtectTools 는 컴퓨터와 하드 드라이브를 암호화하여 데이터를 완벽하게 보호합니다. Drive Encryption 이 활성화되어 있는 경우 Windows® 운영 체제가 시작되기 전에 표시되는 Drive Encryption 로그인 화면에서 로그인해야 합니다.

Windows 관리자는 HP ProtectTools Security Manager 설정 마법사를 사용하여 Drive Encryption 활성화, 암호화 키 백업, 드라이브 선택/선택 해제를 수행할 수 있습니다. 자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

Drive Encryption 에서 수행할 수 있는 작업은 다음과 같습니다.

- Drive Encryption 설정 선택:
  - TPM 으로 보호된 암호 활성화
  - 소프트웨어 암호화를 사용하여 개별 드라이브 또는 파티션의 암호화 또는 암호 해제
  - 하드웨어 암호화를 사용하여 개별 자체 암호화 드라이브의 암호화 또는 암호 해제
  - 절전 또는 대기 모드를 비활성화하여 항상 Drive Encrytion 부팅 전 인증을 요구함으로써 더 강력한 보안 제공

참고: 내부 SATA 및 외부 eSATA 하드 드라이브만 암호화할 수 있습니다.

- 백업 키 만들기
- Drive Encryption 키 복구
- 암호, 등록된 지문 또는 스마트 카드 PIN 을 사용하여 Drive Encryption 부팅 전 인증 활성화

Drive Encryption 열기

관리자는 HP ProtectTools 관리 콘솔에서 Drive Encryption 에 액세스할 수 있습니다.

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 클릭합니다.

일반 작업

표준 하드 드라이브의 Drive Encryption 활성화

소프트웨어 암호화를 사용하여 표준 하드 드라이브를 암호화합니다. Drive Encryption 을 활성화하려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager 설정 마법사를 사용하여 Drive Encryption 을 활성화합니다.
2. **보안 기능 활성화** 페이지가 표시될 때까지 화면의 지시를 따른 다음 아래의 4 단계에서 계속합니다.

또는

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. 왼쪽 창에서 **보안** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **기능**을 클릭합니다.
4. **Drive Encryption** 확인란을 선택한 다음 **다음**을 누릅니다.

참고: 암호화할 하드 드라이브를 선택하지 않으면 Drive Encryption 부팅 전 인증이 활성화되지만 드라이브는 암호화되지 않습니다.

5. **암호화할 드라이브**에서 암호화하려는 하드 드라이브의 확인란을 선택한 후 **다음**을 클릭합니다.
6. 암호화 키를 백업하려면 해당 슬롯에 저장 장치를 넣습니다.

참고: 암호화 키를 저장하려면 FAT32 형식의 USB 저장 장치를 사용해야 합니다. 플로피 디스크, USB 메모리 스틱, SD(Secure Digital) 메모리 카드 또는 MMC 를 백업에 사용할 수 있습니다.

7. **Drive Encryption 키 백업**에서 암호화 키를 저장할 저장 장치의 확인란을 선택합니다.
8. **다음**을 클릭합니다.

참고: 컴퓨터가 다시 시작됩니다.

Drive Encryption 이 활성화됩니다. 드라이브 암호화는 드라이브의 크기에 따라 몇 시간이 걸릴 수도 있습니다.

자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

자체 암호화 드라이브의 Drive Encryption 활성화

자체 암호화 드라이브 관리에 대한 TCG(Trusted Computing Group)의 OPAL 규격을 충족하는 자체 암호화 드라이브는 소프트웨어 암호화 또는 하드웨어 암호화를 사용하여 암호화할 수 있습니다. 자체 암호화 드라이브의 Drive Encryption 을 활성화하려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager 설정 마법사를 사용하여 Drive Encryption 을 활성화합니다.
2. **보안 기능 활성화** 페이지가 표시될 때까지 화면의 지시를 따른 다음 아래 "소프트웨어 암호화" 또는 "하드웨어 암호화"에 있는 4 단계를 계속 진행합니다.

참고: 컴퓨터에 자체 암호화 드라이브 관리에 대한 Trusted Computing Group 의 OPAL 규격을 충족하는 자체 암호화 드라이브가 없는 경우는 하드웨어 암호화 옵션을 사용할 수 없으며 기본적으로 소프트웨어 암호화가 사용됩니다.

자체 암호화 드라이브와 표준 하드 드라이브가 혼합된 경우 하드웨어 암호화 옵션을 사용할 수 없으며 기본적으로 소프트웨어 암호화가 사용됩니다.

또는

소프트웨어 암호화

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. 왼쪽 창에서 **보안** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **기능**을 클릭합니다.
4. **Drive Encryption** 확인란을 선택한 후 **다음**을 클릭합니다.
5. **암호화할 드라이브**에서 암호화하려는 하드 드라이브의 확인란을 선택한 후 **다음**을 클릭합니다.
6. 암호화 키를 백업하려면 해당 슬롯에 저장 장치를 넣습니다.

참고: 암호화 키를 저장하려면 FAT32 형식의 USB 저장 장치를 사용해야 합니다. 플로피 디스크, USB 메모리 스틱, SD(Secure Digital) 메모리 카드 또는 MMC 를 백업에 사용할 수 있습니다.

7. **Drive Encryption 키 백업**에서 암호화 키를 저장할 저장 장치의 확인란을 선택합니다.
8. **적용**을 클릭합니다.

참고: 컴퓨터가 다시 시작됩니다.

Drive Encryption 이 활성화됩니다. 드라이브 암호화는 드라이브의 크기에 따라 몇 시간이 걸릴 수도 있습니다.

하드웨어 암호화

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. 왼쪽 창에서 **보안** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **기능**을 클릭합니다.
4. **Drive Encryption** 확인란을 선택한 후 **다음**을 클릭합니다.

참고: 하나의 드라이브만 표시될 경우 드라이브 확인란이 자동으로 선택되고 비활성화됩니다.

두 개 이상의 드라이브만 표시될 경우 드라이브 확인란이 자동으로 선택되지만 비활성화되지는 않습니다.

최소한 하나 이상의 드라이브를 선택하기 전까지는 **다음** 버튼을 사용할 수 없습니다.

5. 화면 아래쪽에서 **하드 드라이브 암호화 사용**을 선택합니다.
6. **암호화할 드라이브**에서 암호화하려는 하드 드라이브의 확인란을 선택한 후 **다음**을 클릭합니다.
7. 암호화 키를 백업하려면 해당 슬롯에 저장 장치를 넣습니다.

참고: 암호화 키를 저장하려면 FAT32 형식의 USB 저장 장치를 사용해야 합니다. 플로피 디스크, USB 메모리 스틱, SD(Secure Digital) 메모리 카드 또는 MMC 를 백업에 사용할 수 있습니다.

8. **Drive Encryption 키 백업**에서 암호화 키를 저장할 저장 장치의 확인란을 선택합니다.
9. **적용**을 클릭합니다.

참고: 컴퓨터를 다시 시작해야 합니다.

Drive Encryption 이 활성화됩니다. 드라이브 암호화는 몇 분이 걸릴 수 있습니다.

자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

Drive Encryption 비활성화

관리자는 HP ProtectTools Security Manager 설정 마법사를 사용하여 Drive Encryption 을 비활성화할 수 있습니다. 자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

▲ **보안 기능 활성화** 페이지가 표시될 때까지 화면의 지시를 따른 다음 아래의 4 단계에서 계속합니다.

또는

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. 왼쪽 창에서 **보안** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **기능**을 클릭합니다.
4. **Drive Encryption** 확인란을 선택 해제한 후 **다음**을 클릭합니다.

   드라이브 암호화의 비활성화가 시작됩니다.

참고: 소프트웨어 암호화를 사용한 경우 암호 해제가 시작됩니다. 드라이브의 크기에 따라 몇 시간이 걸릴 수도 있습니다. 암호 해제가 완료되면 Drive Encryption 이 비활성화됩니다.

하드웨어 암호화를 사용한 경우 드라이브의 암호가 즉시 해제되며(몇 분 소요) Drive Encryption 이 비활성화됩니다.

드라이브를 비활성화한 후에는 컴퓨터를 다시 시작해야 합니다.

Drive Encryption 이 활성화된 후 로그인

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

참고: 하드웨어 암호화를 실행한 경우 반드시 컴퓨터를 끄십시오. 컴퓨터를 끄지 않고 다시 시작하면 Drive Encryption 부팅 전 인증 화면이 표시되지 않습니다.

참고: 소프트웨어 또는 하드웨어 암호화가 활성화되어 있는 상태에서 절전 또는 대기 모드가 해제되면 Drive Encryption 부팅 전 인증이 표시되지 않습니다.

최대 절전 모드가 해제되면 Drive Encryption 부팅 전 인증이 표시됩니다.

참고: Windows 관리자가 HP ProtectTools Security Manager 에 부팅 전 보안을 설정한 경우는 Drive Encryption 로그인 화면에서 로그인하는 것이 아니라 컴퓨터를 켠 직후 컴퓨터에 로그인할 수 있습니다.

1. 사용자 이름을 선택한 다음 Windows 암호 또는 스마트 카드 PIN 을 입력하거나 등록된 손가락을 인식시킵니다.

참고: 다음 스마트 카드가 지원됩니다.

스마트 카드

- ActivIdentity 64K V2C 스마트 카드
- ActivIdentity SIM 48010-B DEC06
- ActivIdentity USB 키 V3.0 ZFG-48001-A

PCMCIA 리더

- Express Card 54 SCR3340 내부 리더
- SCR 201
- SCR 243(HP 브랜드)
- ActivCard
- Omnikey 4040
- Cisco

USB 리더

- ActivCard USB v2
- ActivCard USB v3
- ActivCard USB SCR 3310
- Omnikey Cardman 3121
- Omnikey Cardman 3021
- ACR32
- HP Smart Card 터미널

2. **확인**을 누릅니다.

참고: Drive Encryption 로그인 화면에서 복구 키를 사용하여 로그인하면 Windows 로그인 화면에서 암호, 스마트 카드 PIN 또는 등록된 지문을 사용하여 인증하라는 메시지가 표시됩니다.

하드 드라이브를 암호화하여 데이터 보호

HP ProtectTools Security Manager 설정 마법사를 사용하여 하드 드라이브를 암호화하여 데이터를 보호하는 것이 좋습니다.

1. 왼쪽 창에서 **Drive Encryption** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
2. **설정**을 클릭합니다.
3. 소프트웨어 암호화 드라이브의 경우 암호화할 드라이브 파티션을 선택합니다.

참고: 하나 이상의 표준 하드 드라이브와 하나 이상의 자체 암호화 드라이브가 있는 복합 드라이브 시나리오에도 적용됩니다.

또는

▲ 하드웨어 암호화 드라이브의 경우 암호화할 드라이브를 선택합니다. 하나 이상의 드라이브를 선택해야 합니다.

암호화 상태 확인

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

참고: 관리자는 HP ProtectTools 관리 콘솔에서 드라이브 암호화 상태를 변경할 수 있습니다.

1. HP ProtectTools Security Manager 를 엽니다.
2. 내 데이터에서 **Drive Encryption** 을 클릭합니다.

   소프트웨어 암호화의 경우 **드라이브 상태**에 다음 상태 코드 중 하나가 표시됩니다.

   - 활성화됨
   - 비활성화됨
   - 암호화되지 않음
   - 암호화됨
   - 암호화 중
   - 암호 해독 중

   하드웨어 암호화의 경우 **드라이브 상태**에 다음 상태 코드가 표시됩니다.

   - 암호화됨

   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)

관리자는 Drive Encryption 의 설정 페이지를 사용하여 Drive Encryption 의 상태(활성화됨, 비활성화 또는 하드웨어 암호화 활성화됨)를 확인 및 변경하고 컴퓨터의 모든 하드 드라이브의 암호화 상태를 확인할 수 있습니다.

참고: 하드웨어 암호화는 설정 페이지에서 변경할 수 없습니다.

- 상태가 비활성인 경우 Windows 관리자가 아직 Drive Encryption 을 활성화하지 않았고 하드 드라이브가 보호되고 있지 않은 것입니다. HP ProtectTools Security Manager 설정 마법사를 사용하여 Drive Encryption 을 활성화합니다.
- 활성 상태인 경우 Drive Encryption 이 활성화 및 구성된 것입니다. 드라이브는 다음 상태 중 하나입니다.

소프트웨어 암호화

- 암호화되지 않음
- 암호화됨
- 암호화 중
- 암호 해독 중

하드웨어 암호화

- 암호화됨

개별 드라이브 암호화 또는 암호 해제(소프트웨어 암호화만 해당)

관리자는 설정 페이지를 사용하여 컴퓨터에 하나 이상의 하드 드라이브를 암호화하거나 이미 암호화된 드라이브의 암호를 해제할 수 있습니다.

1. HP ProtectTools 관리 콘솔을 엽니다.
2. 왼쪽 창에서 **Drive Encryption** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **설정**을 클릭합니다.
4. **드라이브 상태**에서 암호화 또는 암호 해제하려는 하드 드라이브 옆의 확인란을 선택 또는 해제한 다음 **적용**을 클릭합니다.

참고: 하드 드라이브가 암호화 또는 암호 해독 중인 경우 진행 표시줄에 현재 세션이 완료될 때까지 남은 시간이 표시됩니다.

컴퓨터를 종료하거나 암호화 프로세스 중 절전/대기 또는 최대 절전 모드가 시작된 다음 다시 시작하면 진행 표시줄의 남은 시간은 초기화되지만 실제 암호화는 마지막에 정지된 지점부터 재개됩니다. 진행 표시줄은 백분율로 표시되며 남은 시간은 이전 진행률을 반영하여 더 빠르게 바뀝니다.

참고: 동적 파티션이 지원되지 않습니다. 파티션이 사용 가능한 것으로 표시되는 경우 동적 파티션은 선택해도 암호화할 수 없습니다. 동적 파티션은 파티션을 압축해서 디스크 관리 내에 새 파티션을 생성할 때 만들어 집니다.

파티션이 동적 파티션으로 변환될 경우 경고가 표시됩니다.

백업 및 복구(관리자 작업)

Drive Encryption 을 활성화하면 관리자가 암호화 키 백업 페이지를 사용하여 암호화 키를 이동식 미디어에 백업하고 복구를 수행할 수 있습니다.

암호화 키 백업

관리자는 이동식 저장 장치에 암호화 드라이브의 암호화 키를 백업할 수 있습니다.

⚠ **주의:** 백업 키가 들어 있는 저장 장치를 안전한 장소에 보관하십시오. 암호가 생각나지 않거나 스마트 키를 잃어 버렸거나 등록된 지문이 없을 경우 이 저장 장치로만 하드 드라이브에 액세스할 수 있습니다.

1. HP ProtectTools 관리 콘솔을 엽니다.
2. 왼쪽 창에서 **Drive Encryption** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **암호화 키 백업**을 클릭합니다.
4. 암호화 키를 백업하는 데 사용하는 저장 장치를 삽입합니다.
5. **드라이브**에서 암호화 키를 백업할 장치의 확인란을 선택합니다.
6. **키 백업**을 누릅니다.
7. 표시되는 페이지에서 정보를 읽은 후 **다음**을 클릭합니다. 선택한 저장 장치에 암호화 키가 저장됩니다.

암호화 키 복구

관리자는 암호화 키가 저장된 이동식 저장 장치에서 암호화 키를 복구할 수 있습니다.

1. 컴퓨터의 전원을 켭니다.
2. 백업 키를 저장한 이동식 저장 장치를 넣습니다.
3. Drive Encryption for HP ProtectTools 로그인 대화 상자가 열리면 **옵션**을 클릭합니다.
4. **복구**를 클릭합니다.
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.

참고: 복구를 수행한 후 암호를 재설정하는 것이 좋습니다.

6 HP ProtectTools Privacy Manager(일부 모델만 해당)

Privacy Manager for HP ProtectTools 를 사용하면 고급 보안 로그인(인증) 방법을 사용하여 전자 우편이나 Microsoft® Office 문서 사용 시 통신의 보안 및 무결성, 원본 등을 확인할 수 있습니다.

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

- 지문 인증
- Windows® 암호
- 스마트 카드
- 얼굴 인식

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

Privacy Manager 열기

Privacy Manager 를 열려면 다음과 같이 하십시오.

- Microsoft Outlook 에서 Outlook 에만 있는 기능에 액세스하려면 **메시지** 탭의 **개인 정보** 그룹에서 **안전하게 보내기**를 클릭합니다.
- Microsoft Office 문서에서 대부분의 기능에 액세스하려면 **홈** 탭의 **개인 정보** 그룹에서 **서명 및 암호화**를 클릭합니다.
- 추가 기능에 액세스하려면 HP ProtectTools Security Manager 대시보드에 액세스합니다.
  - **시작**, **모든 프로그램**, **HP**, **HP ProtectTools Security Manager** 및 **Privacy Manager** 를 차례로 클릭합니다.

    또는

  - **HP ProtectTools** 바탕 화면 가젯 아이콘을 클릭합니다.

    또는

  - 작업 표시줄의 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 클릭한 다음 **Privacy Manager** 및 **구성**을 차례로 클릭합니다.

설치 절차

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.

인증서 관리자에서는 다음 작업을 수행할 수 있습니다.

- 49페이지의 Privacy Manager 인증서 요청
- 50페이지의미리 지정된 기업용 Privacy Manager 인증서 받기
- 51페이지의기본 Privacy Manager 인증서 설치
- 50페이지의제 3 자 인증서 가져오기
- 51페이지의 Privacy Manager 인증서 세부 정보 보기
- 51페이지의 Privacy Manager 인증서 갱신
- 51페이지의기본 Privacy Manager 인증서 설치
- 51페이지의 Privacy Manager 인증서 삭제
- 52페이지의 Privacy Manager 인증서 복원
- 52페이지의 Privacy Manager 인증서 해지

Privacy Manager 인증서 요청

Privacy Manager 기능을 사용하기 전에 유효한 전자 우편 주소를 사용하여 Privacy Manager 인증서를 요청 및 설치해야 합니다(Privacy Manager 내에서). Privacy Manager 인증서를 요청할 때 사용한 컴퓨터에서 Microsoft Outlook 내에 전자 우편 주소를 계정으로 설정해야 합니다.

1. Privacy Manager 를 열고 **인증서**를 클릭합니다.
2. **Privacy Manager 인증서 요청**을 클릭합니다.
3. 시작 페이지에서 내용을 읽고 **다음**을 클릭합니다.
4. 사용권 계약 페이지에서 사용권 계약을 읽습니다.
5. **이 사용권 계약에 동의하면 여기를 선택** 옆의 확인란을 선택한 후 **다음**을 클릭합니다.
6. 인증서 세부 정보 페이지에서 필요한 정보를 입력하고 **다음**을 클릭합니다.
7. 인증서 요청이 수락되었습니다 페이지에서 **마침**을 클릭합니다.

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

미리 지정된 기업용 Privacy Manager 인증서 받기

1. Outlook 에서 기업용 인증서가 귀하에게 미리 지정되었다는 내용으로 수신한 전자 우편을 엽니다.
2. **받기**를 클릭합니다.

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

인증서를 설치하려면 50페이지의 Privacy Manager 인증서 설치를 참조하십시오.

Privacy Manager 인증서 설치

1. Privacy Manager 인증서가 첨부된 전자 우편을 받으면 전자 우편을 연 다음, Outlook 2007 또는 Outlook 2010 에서 메시지의 오른쪽 하단 또는 Outlook 2003 의 왼쪽 상단에 있는 **설정** 버튼을 클릭합니다.
2. 선택한 보안 로그인 방법을 사용하여 인증합니다.
3. 인증서 설치 완료 페이지에서 **다음**을 클릭합니다.
4. 인증서 백업 페이지에 백업 파일의 위치 및 이름을 입력하거나 **찾아보기**를 클릭해서 위치를 검색합니다.

⚠ **주의:** 하드 드라이브 이외의 다른 위치에 파일을 저장한 다음 안전한 장소에 보관하십시오. 이 파일은 사용자 본인만 사용해야 하며 Privacy Manager 인증서 및 관련 키를 복원해야 하는 경우에 필요합니다.

5. 암호를 입력하고 확인한 후 **다음**을 클릭합니다.
6. 선택한 보안 로그인 방법을 사용하여 인증합니다.
7. 신뢰할 수 있는 연락처 초대를 시작하도록 선택한 경우 54페이지의 Microsoft Outlook 연락처를 사용하여 신뢰할 수 있는 연락처 추가 항목의 2 단계부터 시작하는 화면의 지시를 따르십시오.

   또는

   취소를 클릭하는 경우 52페이지의신뢰할 수 있는 연락처 관리에서 신뢰할 수 있는 연락처를 나중에 추가하는 방법을 참조하십시오.

제 3 자 인증서 가져오기

인증서 가져오기 마법사를 통해 제 3 자 인증서를 Privacy Manager 로 가져올 수 있습니다.

이 기능을 사용하려면 HP ProtectTools 관리 콘솔에서 **Privacy Manager** 페이지의 **제 3 자 인증서 사용 허용** 설정이 활성화되어 있어야 합니다.

1. Privacy Manager 를 열고 **인증서**를 클릭합니다.
2. **인증서 관리자** 탭을 선택한 다음 **인증서 가져오기**를 클릭합니다.

   인증서 가져오기가 허용되지 않는 경우 이 버튼이 표시되지 않습니다.
3. 이 컴퓨터에 이미 설치된 인증서를 가져올지 아니면 PFX(개인 정보 교환/PKCS#12) 파일로 저장된 인증서를 가져올지를 선택하고 **다음**을 클릭합니다.
   - 이 컴퓨터에 설치된 인증서를 가져오려면 원하는 인증서를 선택하고 **다음**을 클릭합니다.
   - PFX 인증서를 선택하려면 **찾아보기**를 클릭하고 PFX 파일의 위치로 이동한 후 **다음**을 클릭합니다. PFX 파일 암호를 입력하고 **다음**을 클릭합니다.

4. 가져오기 절차가 완료되면 **다음**을 클릭합니다.
5. 가져온 인증서를 백업할 수 있는 옵션이 제공됩니다.

   인증서는 컴퓨터 하드 드라이브 이외의 위치에 백업해 두는 것이 좋습니다.

Privacy Manager 인증서 세부 정보 보기

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

Privacy Manager 인증서 갱신

Privacy Manager 인증서의 만료가 가까워지면 갱신해야 한다는 알림을 받게 됩니다.

1. Privacy Manager 를 열고 **인증서**를 클릭합니다.
2. **인증서 갱신**을 클릭합니다.
3. 화면의 지시에 따라 새로운 Privacy Manager 인증서를 가져옵니다.

참고: Privacy Manager 인증서를 갱신하더라도 이전 Privacy Manager 인증서가 대체되는 것은 아닙니다. 49페이지의 Privacy Manager 인증서 요청와 동일한 절차에 따라 새로운 Privacy Manager 인증서를 얻고 설치해야 합니다.

Microsoft Certificate Authority 를 사용하여 회사에서 발행한 기업용 인증서의 경우, CA 관리자는 원래 인증서와 동일한 개인 키를 사용하여 인증서를 갱신하거나 동일한 개인 키를 사용하여 새로운 인증서를 발행해야 합니다.

기본 Privacy Manager 인증서 설치

컴퓨터에 다른 인증 기관의 인증서가 추가로 설치되어 있더라도 Privacy Manager 에서는 Privacy Manager 인증서만 볼 수 있습니다.

Privacy Manager 에서 설치한 Privacy Manager 인증서가 2 개 이상인 경우 하나를 기본 인증서로 지정할 수 있습니다.

1. Privacy Manager 를 열고 **인증서**를 클릭합니다.
2. 기본으로 사용하려는 Privacy Manager 인증서를 클릭한 다음 **기본값으로 설정**을 클릭합니다.
3. **확인**을 클릭합니다.

참고: 기본 Privacy Manager 인증서를 사용하지 않아도 됩니다. 다양한 Privacy Manager 기능 중에서, 아무 Privacy Manager 인증서를 선택하여 사용할 수 있습니다.

Privacy Manager 인증서 삭제

Privacy Manager 인증서를 삭제하면 해당 인증서로 암호화한 데이터를 보거나 파일을 열 수 없습니다. Privacy Manager 인증서를 실수로 삭제한 경우에는 인증서를 설치할 때 만든 백업 파일을 사용하여 복원할 수 있습니다. 자세한 내용은 52페이지의 Privacy Manager 인증서 복원을 참조하십시오.

Privacy Manager 인증서를 삭제하려면 다음과 같이 하십시오.

1. Privacy Manager 를 열고 **인증서**를 클릭합니다.
2. 삭제하려는 Privacy Manager 인증서를 클릭한 다음 **고급**을 클릭합니다.
3. **삭제**를 클릭합니다.
4. 확인 대화 상자가 표시되면 **예**를 클릭합니다.
5. **닫기**를 클릭한 다음 **적용**을 클릭합니다.

Privacy Manager 인증서 복원

Privacy Manager 인증서를 설치하는 과정에서 해당 인증서의 백업 사본을 만들어야 합니다. 또한 마이그레이션 페이지에서도 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 클릭합니다.
2. **복원**을 클릭합니다.
3. 마이그레이션 파일 페이지에서 **찾아보기**를 눌러 백업 과정에서 만든 .dppsm 파일을 검색한 후 **다음**을 클릭합니다.
4. 백업을 만들 때 사용했던 암호를 입력한 후 **다음**을 클릭합니다.
5. **마침**을 클릭합니다.

자세한 내용은 50페이지의 Privacy Manager 인증서 설치 또는 62페이지의 Privacy Manager 인증서 및 신뢰할 수 있는 연락처 백업을 참조하십시오.

Privacy Manager 인증서 해지

Privacy Manager 인증서의 보안이 침해되었다고 생각되면 인증서를 해지할 수 있습니다.

참고: 해지한 Privacy Manager 인증서는 삭제된 것이 아닙니다. 이 인증서를 사용하여 암호화된 파일을 볼 수 있습니다.

1. Privacy Manager 를 열고 **인증서**를 클릭합니다.
2. **고급**을 클릭합니다.
3. 해지하려는 Privacy Manager 인증서를 클릭한 다음 **해지**를 클릭합니다.
4. 확인 대화 상자가 표시되면 **예**를 클릭합니다.
5. 선택한 보안 로그인 방법을 사용하여 인증합니다.
6. 화면의 지시를 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 받은 다음 **동의**를 누릅니다.

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

다음 단원을 참조하여 신뢰할 수 있는 연락처를 추가하십시오.

참고: 신뢰할 수 있는 연락처 초대 요청에 응답하려면, 신뢰할 수 있는 연락처 수신자가 Privacy Manager 를 컴퓨터에 설치했거나 대체 클라이언트를 설치했어야 합니다. 대체 클라이언트 설치에 대한 자세한 내용은 DigitalPersona 웹 사이트 http://digitalpersona.com/privacymanager/download 를 참조하십시오.

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 추가하려는 수신자의 전자 우편 주소를 입력합니다.

5. 텍스트를 수정하고 서명합니다(선택 사항).

6. **보내기**를 누릅니다.

   참고: Privacy Manager 인증서를 얻지 않은 경우 신뢰할 수 있는 연락처 요청을 보내려면 Privacy Manager 인증서가 필요하다는 메시지가 나타납니다. 인증서 요청 마법사를 실행하려면 **확인**을 클릭합니다. 자세한 내용은 49페이지의 Privacy Manager 인증서 요청을 참조하십시오.

7. 선택한 보안 로그인 방법을 사용하여 인증합니다.

   참고: 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 연락처 초대**를 누릅니다.

2. 신뢰할 수 있는 연락처 초대 페이지가 열리면 신뢰할 수 있는 연락처로 추가하려는 수신자의 전자 우편 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.

   참고: Privacy Manager 인증서를 얻지 않은 경우 신뢰할 수 있는 연락처 요청을 보내려면 Privacy Manager 인증서가 필요하다는 메시지가 나타납니다. 인증서 요청 마법사를 실행하려면 **확인**을 클릭합니다. 자세한 내용은 49페이지의 Privacy Manager 인증서 요청을 참조하십시오.

6. 선택한 보안 로그인 방법을 사용하여 인증합니다.

   참고: 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 연 다음 **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 연 다음 **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 연 다음 **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

Microsoft Outlook 에서 Privacy Manager 사용

Privacy Manager 가 설치되면 Microsoft Outlook 도구 모음에 개인 정보 버튼이 표시되고 각 Microsoft Outlook 전자 우편 메시지의 도구 모음에 안전하게 보내기 버튼이 표시됩니다. **개인 정보** 또는 **안전하게 보내기** 옆의 아래쪽 화살표를 누르면 다음 옵션 중에서 선택할 수 있습니다.

- **메시지에 서명하고 보내기**(안전하게 보내기 버튼만)—이 옵션은 전자 우편에 디지털 서명을 추가하고, 사용자가 선택한 보안 로그인 방법을 사용하여 인증한 후 보냅니다.
- **신뢰할 수 있는 연락처에 대해 봉인하고 메시지 보내기**(안전하게 보내기 버튼만)—이 옵션은 디지털 서명을 추가하고 전자 우편을 암호화하며, 사용자가 선택한 보안 로그인 방법을 사용하여 인증한 후 보냅니다.
- **연락처 초대**—이 옵션을 통해 신뢰할 수 있는 연락처 초대 요청을 보낼 수 있습니다. 자세한 내용은 53페이지의신뢰할 수 있는 연락처 추가를 참조하십시오.
- **Outlook 의 연락처 초대**-이 옵션을 통해 Microsoft Outlook 주소록의 모든 연락처로 신뢰할 수 있는 연락처 초대 요청을 보낼 수 있습니다. 자세한 내용은 54페이지의 Microsoft Outlook 연락처를 사용하여 신뢰할 수 있는 연락처 추가를 참조하십시오.
- **Privacy Manager 소프트웨어 열기**—인증서, 신뢰할 수 있는 연락처 및 설정 옵션을 사용하여 Privacy Manager 소프트웨어를 열고 현재 설정을 추가, 확인 또는 변경할 수 있습니다. 자세한 내용은 49페이지의 Privacy Manager 인증서 관리, 52페이지의신뢰할 수 있는 연락처 관리 또는 56페이지의 Microsoft Outlook 에서 Privacy Manager 구성을 참조하십시오.

Microsoft Outlook 에서 Privacy Manager 구성

1. Privacy Manager 를 열고 **설정**을 누른 다음 **전자 우편**탭을 누릅니다.

   또는

   Microsoft Outlook 주 도구 모음에서 **안전하게 보내기**(Outlook 2003 의 **개인 정보**) 옆의 아래쪽 화살표를 누른 다음 **설정**을 누릅니다.

   또는

   Microsoft 전자 우편 메시지의 도구 모음에서 **안전하게 보내기**옆의 아래쪽 화살표를 누른 다음 **설정**을 누릅니다.

2. 전자 우편을 안전하게 보낼 때 수행하려는 동작을 선택하고 **확인**을 누릅니다.

전자 우편 메시지에 서명하고 보내기

1. Microsoft Outlook 에서 **새로 만들기**또는 **회신**을 누릅니다.
2. 전자 우편 메시지를 입력합니다.

3. **안전하게 보내기**(Outlook 2003 의 **개인 정보**) 옆의 아래쪽 화살표를 누른 다음 **서명하고 보내기**를 누릅니다.

4. 선택한 보안 로그인 방법을 사용하여 인증합니다.

전자 우편 메시지를 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 **새로 만들기**또는 **회신**을 누릅니다.

2. 전자 우편 메시지를 입력합니다.

3. **안전하게 보내기**(Outlook 2003 의 **개인 정보**) 옆의 아래쪽 화살표를 누른 다음 **신뢰할 수 있는 연락처에 대해 봉인하고 보내기**를 누릅니다.

4. 선택한 보안 로그인 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

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

- **문서에 서명하기**—이 옵션은 문서에 디지털 서명을 추가합니다.
- **서명하기 전에 서명 줄 추가**(Microsoft Word 및 Microsoft Excel 만 해당)—기본적으로, Microsoft Word 또는 Microsoft Excel 문서가 서명되어 있거나 암호화된 경우 서명 줄이 추가됩니다. 이 옵션을 끄려면 **서명 줄 추가**를 눌러 확인 표시를 제거합니다.
- **문서 암호화**—이 옵션은 디지털 서명을 추가하고 문서를 암호화합니다.
- **암호화 제거**—이 옵션은 문서에서 암호화를 제거합니다.
- **Privacy Manager 소프트웨어 열기**—인증서, 신뢰할 수 있는 연락처 및 설정 옵션을 사용하여 Privacy Manager 소프트웨어를 열고 현재 설정을 추가, 확인 또는 변경할 수 있습니다. 자세한 내용은 49페이지의 Privacy Manager 인증서 관리, 52페이지의신뢰할 수 있는 연락처 관리 또는 58페이지의 Microsoft Office 에서 Privacy Manager 구성을 참조하십시오.

Microsoft Office 에서 Privacy Manager 구성

1. Privacy Manager 를 열고 **설정**을 누른 다음 **문서**탭을 누릅니다.

   또는

   Microsoft Office 문서의 도구 모음에서 **서명 및 암호화**옆의 아래쪽 화살표를 누른 다음 **설정**을 누릅니다.

2. 구성할 동작을 선택한 다음 **확인**을 누릅니다.

Microsoft Office 문서에 서명하기

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

나중에 문서를 편집하려면 다음과 같이 하십시오.

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

Microsoft Word 또는 Microsoft Excel 문서에 서명할 때 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. **홈**메뉴를 누릅니다.
3. **서명 및 암호화**옆의 아래쪽 화살표를 누른 다음 **서명하기 전에 서명 줄 추가**를 누릅니다.

   참고: 이 옵션을 선택하면 서명하기 전에 서명 줄 추가 옆에 확인 표시가 나타납니다. 기본적으로 이 옵션이 활성화되어 있습니다.

4. **서명 및 암호화**옆의 아래쪽 화살표를 누른 다음 **문서에 서명하기**를 누릅니다.
5. 선택한 보안 로그인 방법을 사용하여 인증합니다.

Microsoft Word 또는 Microsoft Excel 문서에 추천 서명자 추가

추천 서명자를 지정하여 문서에 서명 줄을 둘 이상 추가할 수 있습니다. 추천 서명자는 문서에 서명줄을 추가하도록 Microsoft Word 또는 Microsoft Excel 문서의 소유자가 지정한 사용자입니다. 추천 서명자는 본인이거나, 다른 사람을 지정하여 해당 문서에 서명하도록 할 수 있습니다. 예를 들어, 부서의 모든 구성원이 서명해야 하는 문서를 준비하는 경우 해당 문서의 마지막 페이지 아래쪽에 이러한 사용자를 위한 서명 줄과 함께 특정 날짜에 서명하도록 하는 지침을 포함할 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. **삽입**메뉴를 누릅니다.
3. 도구 모음의 **텍스트**그룹에서 **서명 줄**옆의 화살표를 누른 다음 **Privacy Manager 서명 공급자**를 누릅니다.

   서명 설정 대화 상자가 열립니다.
4. **추천 서명자**아래에 있는 상자에 추천 서명자 이름을 입력합니다.
5. **서명자에게 지시**아래에 있는 상자에 추천 서명자에게 지시할 메시지를 입력합니다.

   참고: 이 메시지는 제목 위치에 표시되고 문서가 서명되면 메시지가 삭제되거나 사용자의 제목으로 바뀝니다.
6. **서명 줄에 서명 날짜 표시**확인란을 선택하여 날짜를 표시합니다.
7. **서명 줄에 서명자의 제목 표시**확인란을 선택하여 제목을 표시합니다.

   참고: 문서의 소유자는 자신의 문서에 추천 서명자를 지정합니다. 추천 서명자가 서명 줄에 날짜 및/또는 제목을 표시할 수 있도록 하려면 **서명 줄에 서명 날짜 표시** 및/또는 **서명 줄에 서명자 제목 표시** 확인란을 선택해야 합니다.
8. **확인**을 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 로그인 방법을 사용하여 인증합니다.

   문서의 소유자가 지정한 설정에 따라 서명 줄이 표시됩니다.

Microsoft Office 문서 암호화

본인 및 신뢰할 수 있는 연락처의 대상에 대해 Microsoft Office 문서를 암호화할 수 있습니다. 문서를 암호화하고 닫으면, 본인 및 본인이 목록에서 선택한 신뢰할 수 있는 연락처의 대상은 인증을 거쳐야 문서를 열 수 있습니다.

Microsoft Office 문서를 암호화하려면 다음과 같이 하십시오.

1. Microsoft Word, Microsoft Excel 또는 Microsoft PowerPoint 에서 문서를 만들고 저장합니다.
2. **홈**메뉴를 누릅니다.
3. **서명 및 암호화** 옆에 있는 아래쪽 화살표를 누른 다음 **문서 암호화**를 누릅니다.

   신뢰할 수 있는 연락처 선택 대화 상자가 열립니다.
4. 문서를 열고 내용을 볼 수 있도록 하려는 신뢰할 수 있는 연락처의 이름을 누릅니다.

참고: 신뢰할 수 있는 연락처의 이름을 여러 개 선택하려면 ctrl 키를 누른 상태에서 각각의 이름을 누릅니다.

5. **확인**을 누릅니다.

나중에 문서를 편집하려면 60페이지의 Microsoft Office 문서에서 암호화 제거에 나와 있는 단계를 따릅니다. 암호화가 제거되면 문서를 편집할 수 있습니다. 문서를 다시 암호화하려면 이 단원에 나와 있는 단계를 따릅니다.

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 로그인 방법을 사용하여 인증합니다.
3. **홈**메뉴를 누릅니다.
4. **서명 및 암호화** 옆에 있는 아래쪽 화살표를 누른 다음 **암호화 제거**를 누릅니다.

암호화된 Microsoft Office 문서 보내기

전자 우편에 직접 서명하거나 암호화하지 않고, 암호화된 Microsoft Office 문서를 전자 우편 메시지에 첨부할 수 있습니다. 이렇게 하려면 첨부 파일이 있는 일반적인 전자 우편의 경우와 마찬가지로, 서명되거나 암호화된 문서가 첨부된 전자 우편을 생성하고 전송해야 합니다.

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 **새로 만들기**또는 **회신**을 누릅니다.
2. 전자 우편 메시지를 입력합니다.
3. Microsoft Office 문서를 첨부합니다.
4. 자세한 지침은 57페이지의전자 우편 메시지를 봉인하고 보내기를 참조하십시오.

서명된 Microsoft Office 문서 보기

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

서명이 있는 Microsoft Office 문서를 열면 디지털 서명 아이콘이 문서 창 하단의 상태 표시줄에 표시됩니다.

1. **디지털 서명** 아이콘을 눌러 문서에 서명한 모든 사용자의 이름 및 서명 날짜를 표시하는 서명 대화 상자의 표시를 전환합니다.
2. 각 서명에 대한 추가 정보를 보려면 서명 대화 상자에서 마우스 오른쪽 버튼으로 이름을 누른 다음 **서명 세부 정보**를 선택합니다.

암호화된 Microsoft Office 문서 보기

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

인증서를 분실한 경우, 암호화된 Microsoft Office 문서를 보려면 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.

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 연 다음 **마이그레이션**을 누릅니다.
2. **백업**을 누릅니다.
3. 데이터 선택 페이지에서 마이그레이션 파일에 포함할 데이터 범주를 선택하고 **다음**을 누릅니다.
4. 마이그레이션 파일 페이지에서 파일 이름을 입력하거나 **찾아보기**를 눌러 위치를 검색한 후 **다음**을 누릅니다.
5. 암호를 입력하고 확인한 후 **다음**을 누릅니다.

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

6. 선택한 보안 로그인 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 연 다음 **마이그레이션**을 누릅니다.
2. **복원**을 누릅니다.
3. 마이그레이션 파일 페이지에서 **찾아보기**를 눌러 파일을 검색한 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 Microsoft Outlook 에서 개별적으로 활성화 또는 비활성화되어 있을 수 있습니다.

7 HP ProtectTools File Sanitizer

File Sanitizer 를 사용하면 컴퓨터의 자산(예: 개인 정보 또는 파일, 기록 데이터 또는 웹 관련 데이터, 기타 데이터 구성 요소)을 안전하게 파쇄하고 하드 드라이브에서 삭제된 자산을 정기적으로 블리치할 수 있습니다.

참고: 이 버전의 File Sanitizer 는 컴퓨터 하드 드라이브만 지원합니다.

파쇄

파쇄는 일반적인 Windows® 삭제(Sanitizer 에서는 기본 삭제라고도 함)와는 다릅니다. File Sanitizer 를 사용하여 자산을 파쇄하면 파일을 의미 없는 데이터로 덮어써서 기존 자산을 검색할 수 없게 됩니다. 그러나 Windows 기본 삭제의 경우 과학 수사 방식을 사용하여 복구할 수 있는 상태 또는 하드 드라이브에 온전한 상태로 파일이나 자산을 남겨 둡니다.

높은 보안, **중간 보안**, **낮은 보안**의 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 지정하여 파쇄 프로파일을 사용자 정의할 수 있습니다. 자세한 내용은 68페이지의파쇄 프로파일 선택 또는 만들기를 참조하십시오.

자동 파쇄 일정을 설정하거나 작업 표시줄 오른쪽 끝에 있는 알림 영역의 **HP ProtectTools** 아이콘을 사용하여 수동으로 파쇄를 활성화할 수 있습니다. 자세한 내용은 67페이지의파쇄 일정 설정, 72페이지의자산 한 개를 수동으로 파쇄 또는 72페이지의선택한 모든 항목을 수동으로 파쇄를 참조하십시오.

참고: .dll 파일은 휴지통으로 이동한 경우에만 파쇄되어 시스템에서 제거됩니다.

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.

참고: File Sanitizer 에서 **기본 삭제 설정**을 선택하거나 자산을 Windows 휴지통으로 이동하거나 수동으로 자산을 삭제하여 삭제하는 자산에 대해 때때로 여유 공간 블리치 기능을 사용할 수 있습니다. 여유 공간 블리치는 파쇄된 자산에 대해 추가 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 67페이지의여유 공간 블리치 예약 설정 또는 73페이지의여유 공간 블리치를 수동으로 활성화를 참조하십시오.

File Sanitizer 열기

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools Security Manager** 를 차례로 클릭합니다.
2. **File Sanitizer** 를 클릭합니다.

또는

- 바탕 화면에서 **File Sanitizer** 아이콘을 두 번 클릭합니다.

또는

- 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 클릭한 다음 **File Sanitizer** 및 **File Sanitizer 열기**를 차례로 클릭합니다.

설치 절차

파쇄 일정 설정

미리 정의된 파쇄 프로파일을 선택하거나 파쇄 프로파일을 만들 수 있습니다. 자세한 내용은 68페이지의파쇄 프로파일 선택 또는 만들기를 참조하십시오. 자산을 언제든지 수동으로 파쇄할 수도 있습니다. 자세한 내용은 71페이지의키 시퀀스를 사용하여 파쇄 시작을 참조하십시오.

참고: 예약된 작업은 지정된 시간에 시작됩니다. 예약된 시간에 컴퓨터가 꺼져 있거나 절전/대기 모드인 경우 File Sanitizer 는 작업을 다시 시작하지 않습니다.

1. File Sanitizer 를 연 다음 **파쇄**를 누릅니다.
2. 다음 중 하나 이상의 파쇄 옵션을 선택합니다.
   - **Windows 종료**—Windows 를 종료할 때 모든 선택한 자산을 파쇄합니다.

     참고: 시스템 종료 시 선택한 자산을 파쇄할지 아니면 이 과정을 건너뛸지 묻는 대화 상자가 열립니다.

     예를 눌러 파쇄 과정을 건너뛰거나 **아니요**를 눌러 파쇄를 계속합니다.
   - **웹 브라우저 열기**—웹 브라우저를 열 때 브라우저 URL 히스토리와 같은 선택한 웹 관련 자산을 모두 파쇄합니다.
   - **웹 브라우저 종료**—웹 브라우저를 닫을 때 브라우저 URL 히스토리와 같은 선택한 웹 관련 자산을 모두 파쇄합니다.
   - **키 시퀀스**—키 시퀀스를 지정하여 파쇄를 초기화할 수 있습니다. 자세한 내용은 71페이지의키 시퀀스를 사용하여 파쇄 시작을 참조하십시오.

참고: .dll 파일은 휴지통으로 이동한 경우에만 파쇄되어 시스템에서 제거됩니다.

3. 선택한 자산을 파쇄할 향후 일정을 예약하려면 **스케줄러 활성화** 확인란을 선택하여 Windows 암호를 입력한 다음 날짜와 시간을 선택합니다.
4. **적용**을 누릅니다.

여유 공간 블리치 예약 설정

File Sanitizer 에서 **기본 삭제 설정**을 선택하거나 자산을 Windows 휴지통으로 이동하거나 수동으로 자산을 삭제하여 삭제하는 자산에 대해 때때로 여유 공간 블리치 기능을 사용할 수 있습니다. 여유 공간 블리치는 파쇄된 자산에 대해 추가 보안을 제공하지 않습니다.

참고: 예약된 작업은 지정된 시간에 시작됩니다. 예약된 시간에 컴퓨터가 꺼져 있거나 절전/대기 모드인 경우 File Sanitizer 는 작업을 다시 시작하지 않습니다.

1. File Sanitizer 를 연 다음 **블리치**를 누릅니다.
2. 하드 드라이브에서 삭제된 데이터를 블리치할 시간을 예약하려면 **스케줄러 활성화** 확인란을 선택한 다음 Windows 암호를 입력하고 요일과 시간을 선택합니다.
3. **적용**을 누릅니다.

참고: 여유 공간 블리치 작업에는 상당한 시간이 소요될 수 있습니다. 여유 공간 블리치 작업은 백그라운드로 수행되지만 프로세서 사용 증가로 인해 컴퓨터의 성능에 영향을 끼칠 수 있습니다.

파쇄 프로파일 선택 또는 만들기

미리 정의된 프로파일을 선택하거나 프로파일을 만들어 제거 방법을 지정하고 파쇄할 자산을 선택할 수 있습니다.

미리 정의된 파쇄 프로파일 선택

미리 정의된 파쇄 프로파일을 선택하면 미리 정의된 제거 방법 및 자산 목록이 자동으로 선택됩니다. 파쇄하도록 선택한 미리 정의된 자산 목록을 볼 수도 있습니다.

1. File Sanitizer 를 연 다음 **설정**을 누릅니다.
2. 다음과 같은 미리 정의된 파쇄 프로파일을 누릅니다.
   - **높음**
   - **보통**
   - **낮음**
3. 파쇄하도록 선택한 자산을 보려면 **세부 정보 보기**를 누릅니다.
   a. **선택한 항목이 파쇄되고 확인 메시지가 표시됩니다. 선택하지 않은 항목은 확인 메시지 없이 파쇄됩니다.**—파쇄하기 전에 확인 메시지를 표시하려면 확인란을 선택하고, 확인 메시지를 표시하지 않고 파쇄하려면 확인란을 선택 해제합니다.

   참고: 자산에 대한 확인란이 선택 해제된 경우에도 자산이 파쇄됩니다.

   b. **적용**을 누릅니다.
4. **적용**을 누릅니다.

파쇄 프로파일 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 주기 횟수를 선택합니다.

참고: 각 자산에 대해 선택한 파쇄 주기 횟수가 실행됩니다. 예를 들어 파쇄 주기를 3 으로 선택한 경우 데이터를 손상시키는 알고리즘이 각각 세 번 실행됩니다. 더 높은 보안 수준의 파쇄 주기를 선택하는 경우 파쇄하는 데 상당한 시간이 소요될 수 있습니다. 그러나 파쇄 주기 회수를 더 많이 지정할수록 데이터가 검색될 확률이 낮아집니다.

3. 파쇄할 자산을 선택하려면:
   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.
   c. **열기**를 누른 다음 **확인**을 누릅니다.
   d. **사용 가능한 파쇄 옵션**에서 사용자 정의 자산을 누른 다음 **추가**를 누릅니다.

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

4. **선택한 항목이 파쇄되고 확인 메시지가 표시됩니다. 선택하지 않은 항목은 확인 메시지 없이 파쇄됩니다.**—파쇄하기 전에 확인 메시지를 표시하려면 확인란을 선택하고, 확인 메시지를 표시하지 않고 파쇄하려면 확인란을 선택 해제합니다.

참고: 자산에 대한 확인란이 선택 해제된 경우에도 자산이 파쇄됩니다.

파쇄 목록에서 자산을 제거하려면 자산을 누른 다음 **제거**를 누릅니다.

5. 파일 또는 폴더가 자동 파쇄되지 않도록 설정하려면:

   a. **다음 자산을 파쇄하지 않음**에서 **추가**를 누른 다음 해당 파일 또는 폴더가 있는 경로를 찾거나 입력합니다.

   b. **열기**를 누른 다음 **확인**을 누릅니다.

   제외 목록에서 자산을 제거하려면 자산을 누른 다음 **삭제**를 누릅니다.

6. **적용**을 누릅니다.

기본 삭제 프로파일 사용자 정의

기본 삭제 프로파일은 자산을 파쇄하지 않고 기본적인 삭제만 실행합니다. 포함할 자산, 삭제하기 전에 확인할 자산 및 제외할 자산 등을 지정하여 기본 삭제 프로파일을 사용자 정의할 수 있습니다.

참고: **기본 삭제 설정**을 선택하는 경우 수동으로 삭제한 자산이나 Windows 휴지통을 통해 삭제한 자산에 대해 때때로 여유 공간 블리치 기능을 사용할 수 있습니다.

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 옵션 추가**를 누르고 해당 파일 또는 폴더가 있는 경로를 찾거나 입력한 다음 **확인**을 누릅니다.

   c. 사용자 정의 자산을 누른 다음 **추가**를 누릅니다.

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

3. **선택한 항목이 파쇄되고 확인 메시지가 표시됩니다. 선택하지 않은 항목은 확인 메시지 없이 파쇄됩니다.**—파쇄하기 전에 확인 메시지를 표시하려면 확인란을 선택하고, 확인 메시지를 표시하지 않고 파쇄하려면 확인란을 선택 해제합니다.

참고: 자산에 대한 확인란이 선택 해제된 경우에도 자산이 파쇄됩니다.

삭제 목록에서 자산을 제거하려면 자산을 누른 다음 **제거**를 누릅니다.

4. 자산이 자동 삭제되지 않도록 설정하려면:

   a. **다음 자산을 삭제하지 않음**에서 **추가**를 누른 다음 해당 파일 또는 폴더가 있는 경로를 찾거나 입력합니다.

   b. **열기**를 누른 다음 **확인**을 누릅니다.

제외 목록에서 자산을 제거하려면 자산을 누른 다음 **삭제**를 누릅니다.

5. **적용**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 71페이지의키 시퀀스를 사용하여 파쇄 시작을 참조하십시오.
- File Sanitizer 아이콘을 사용하여 파쇄 시작—이 기능은 Windows 의 끌어서 놓기 기능과 유사합니다. 자세한 내용은 72페이지의 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 72페이지의자산 한 개를 수동으로 파쇄 또는 72페이지의선택한 모든 항목을 수동으로 파쇄를 참조하십시오.
- 여유 공간 블리치를 수동으로 활성화—이 기능을 사용하면 여유 공간 블리치를 수동으로 활성화할 수 있습니다. 자세한 내용은 73페이지의여유 공간 블리치를 수동으로 활성화를 참조하십시오.
- 파쇄 또는 여유 공간 블리치 작업 중단—이 기능을 사용하면 파쇄 또는 여유 공간 블리치 작업을 중지할 수 있습니다. 자세한 내용은 73페이지의파쇄 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 73페이지의로그 파일 보기를 참조하십시오.

참고: 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

1. File Sanitizer 를 연 다음 **파쇄**를 누릅니다.
2. **키 시퀀스** 확인란을 선택합니다.
3. 사용 가능한 상자에 문자를 입력합니다.
4. **CTRL** 상자 또는 **ALT** 상자를 선택한 다음 **SHIFT** 상자를 선택합니다.

   예를 들어 s 키와 ctrl+shift 를 사용하여 자동 파쇄를 시작하려면 상자에 s 를 입력한 다음 **CTRL** 및 **SHIFT** 옵션을 선택합니다.

참고: 키 시퀀스 선택은 키 시퀀스를 직접 구성하는 것과 다릅니다.

키 시퀀스를 사용하여 파쇄를 시작하려면 다음과 같이 하십시오.

1. 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. 자산을 바탕 화면의 **File Sanitizer** 아이콘으로 끌어 옵니다.
3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

자산 한 개를 수동으로 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.

   참고: 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 연 다음 **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.

선택한 모든 항목을 수동으로 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 연 다음 **파쇄**를 누릅니다.
2. **지금 파쇄** 버튼을 누릅니다.
3. 확인 대화 상자가 표시되면 **예**를 누릅니다.

여유 공간 블리치를 수동으로 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 연 다음 **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 작업이 진행 중인 경우 작업 표시줄 오른쪽 끝의 알림 영역에 있는 HP ProtectTools Security Manager 아이콘 위에 메시지가 표시됩니다. 메시지에는 파쇄 또는 여유 공간 블리치 프로세스에 대한 세부 정보(완료된 정도)가 표시되며 작업을 중단할 수 있는 옵션을 제공합니다.

▲ 작업을 취소하려면 메시지를 누른 다음 **중지**를 누릅니다.

로그 파일 보기

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

참고: 파쇄되거나 블리치된 파일은 로그 파일에 기록되지 않습니다.

파쇄 작업에 대한 로그 파일 한 개와 여유 공간 블리치 작업에 대한 별도의 로그 파일 한 개가 생성됩니다. 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

64 비트 시스템의 경우 로그 파일은 하드 드라이브의 다음 위치에 있습니다.

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[사용자 이름]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[사용자 이름]*_DiskBleachLog.txt

8 HP ProtectTools Device Access Manager(일부 모델만 해당)

HP ProtectTools Device Access Manager 는 데이터 전송 장치를 비활성화하여 데이터에 대한 액세스를 제어합니다.

참고: 마우스, 키보드, 터치패드 및 지문 인식기 같은 휴먼 인터페이스/입력 장치는 Device Access Manager 로 제어할 수 없습니다. 자세한 내용은 84페이지의관리되지 않는 장치 클래스를 참조하십시오.

Windows® 운영체제 관리자는 HP ProtectTools Device Access Manager 를 사용하여 시스템의 장치에 대한 액세스를 제어하고 무단 액세스를 차단합니다.

- 각 사용자에 대해 장치 프로필을 생성하여 액세스를 허용 또는 거부할 장치를 정의할 수 있습니다.
- Just In Time 인증(JITA)을 사용하면 미리 정의된 사용자가 스스로 인증하여 거부된 장치에 액세스할 수 있습니다.
- 관리자 및 신뢰할 수 있는 사용자를 장치 관리자 그룹에 추가하면 Device Access Manager 에서 지정한 장치 액세스 제한이 적용되지 않습니다. 이 그룹의 구성원 자격은 고급 설정을 사용하여 관리합니다.
- 그룹 구성원 자격 또는 개인 사용자에 따라 장치 액세스를 허용하거나 거부할 수 있습니다.
- CD-ROM 드라이브, DVD 드라이브와 같은 종류의 장치의 경우 읽기 액세스와 쓰기 액세스를 별도로 허용하거나 거부할 수 있습니다.

Device Access Manager 열기

1. 관리자로 로그인합니다.
2. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
3. 왼쪽 창에서 **Device Access Manager** 를 클릭합니다.

HP ProtectTools Security Manager 를 사용하여 HP ProtectTools Device Access Manager 정책을 확인할 수 있습니다. 이 콘솔은 읽기 전용입니다.

설정 절차

장치 액세스 구성

HP ProtectTools Device Access Manager 는 다음과 같은 네 가지 보기를 제공합니다.

- **단순 구성**—장치 관리자 그룹의 구성원 자격에 따라 장치 클래스에 대한 액세스를 허용 또는 거부합니다.
- **장치 클래스 구성**—특정 사용자 또는 그룹에게 장치 유형 또는 특정 장치에 대한 액세스를 허용하거나 거부합니다.
- **Just In Time 인증(JITA) 구성**—Just In Time 인증(JITA)을 구성하면 선택된 사용자가 스스로 인증하여 DVD/CD-ROM 드라이브 또는 이동 미디어에 액세스할 수 있습니다.
- **고급 설정**—C 또는 시스템 드라이브 같이 Device Access Manager 가 액세스를 제한하지 않는 드라이브 문자 목록을 구성합니다. 이 보기에서 장치 관리자 그룹의 구성원 자격도 관리할 수 있습니다.

단순 구성

관리자는 **단순 구성** 보기를 사용하여 장치 관리자가 아닌 사용자에 대해 다음과 같은 종류의 장치에 대한 액세스를 허용하거나 거부할 수 있습니다.

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

장치 관리자 이외의 모든 사용자에게 어떤 종류의 장치에 대한 액세스를 허용하거나 거부하려면 다음과 같이 하십시오.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **단순 구성**을 누릅니다.
2. 액세스를 거부하려면 오른쪽 창에서 장치 클래스 또는 특정 장치에 대한 확인란을 선택합니다. 액세스를 허용하려면 장치 클래스 또는 특정 장치에 대한 확인란의 선택을 취소합니다.

   확인란이 비활성화되어 있으면 액세스 시나리오에 영향을 주는 값이 **장치 클래스 구성** 보기 내에서 변경된 것입니다. 기본 설정으로 재설정하려면 **장치 클래스 구성** 보기에서 **재설정**을 누릅니다.
3. **적용**을 누릅니다.

   참고: 백그라운드 서비스가 실행되고 있지 않은 경우 백그라운드 서비스를 시작할지 묻는 대화상자가 열립니다. **예**를 누릅니다.
4. **확인**을 누릅니다.

백그라운드 서비스 시작

처음으로 신규 정책이 정의되거나 적용된 경우 HP ProtectTools Device Locking/Auditing 백그라운드 서비스가 자동으로 시작되며 시스템 시작 시 항상 자동으로 실행되도록 설정됩니다.

참고: 백그라운드 서비스 프롬프트가 표시되기 전에 장치 프로필을 정의해야 합니다.

관리자는 또한 다음과 같이 백그라운드 서비스를 시작하거나 중지할 수 있습니다.

1. Windows 7 의 경우 **시작**, **제어판**, **시스템 및 보안**을 차례로 누릅니다.

   또는

   Windows Vista®의 경우 **시작**, **제어판**, **시스템 및 유지 관리**를 차례로 누릅니다.

   또는

   Windows XP 의 경우 **시작**, **제어판**, **성능 및 유지 관리**를 차례로 누릅니다.

2. **관리 도구**, **서비스**를 차례로 누릅니다.
3. **HP ProtectTools Device Locking/Auditing** 서비스를 선택합니다.
4. **시작**을 눌러 서비스를 시작합니다.

   또는

   서비스가 실행 중인 경우 서비스를 중지하려면 **중지**를 누릅니다.

Device Locking/Auditing 서비스를 중지해도 장치 잠금이 중지되지는 않습니다. 장치 잠금은 두 가지 구성 요소에 의해 적용됩니다.

- Device Locking/Auditing 서비스
- DAMDrv.sys 드라이버

서비스를 시작하면 장치 드라이버가 시작되지만 서비스를 중지한다고 해서 드라이버가 중지되지는 않습니다.

백그라운드 서비스가 실행되고 있는지 확인하려면 명령 프롬프트 창을 연 다음 sc query flcdlock 을 입력합니다.

장치 드라이버가 실행되고 있는지 확인하려면 명령 프롬프트 창을 연 다음 sc query damdrv 를 입력합니다.

장치 클래스 구성

관리자는 장치 클래스 또는 특정 장치에 액세스할 수 있는 권한이 허용되거나 거부된 사용자 및 그룹 목록을 확인하고 수정할 수 있습니다.

장치 클래스 구성 보기는 다음 섹션으로 이루어집니다.

- **장치 목록**—시스템에 설치되어 있거나 이전에 설치되었던 모든 장치 클래스 및 장치를 표시합니다.
  - 장치 클래스에는 대개 보호 기능이 적용되며 선택된 사용자 또는 그룹은 장치 클래스의 모든 장치에 액세스할 수 있습니다.
  - 특정 장치에도 보호 기능을 적용할 수 있습니다.
- **사용자 목록**—선택된 장치 클래스 또는 특정 장치에 대해 액세스가 허용되었거나 거부된 모든 사용자 및 그룹이 표시됩니다.
  - 특정 사용자 또는 해당 사용자가 속한 그룹에 대해 사용자 목록 항목을 만들 수 있습니다.
  - 사용자 목록의 사용자 또는 그룹 항목을 사용할 수 없는 경우 장치 목록의 장치 클래스 또는 클래스 폴더에서 설정이 상속된 것입니다.
  - DVD 및 CD-ROM 과 같은 일부 장치 클래스는 읽기 작업과 쓰기 작업에 대한 액세스를 별도로 허용하거나 거부하여 좀더 세부적으로 제어할 수 있습니다.

    다른 장치 및 클래스의 경우 읽기 및 쓰기 액세스 권한이 상속될 수 있습니다. 예를 들어 사용자 또는 그룹에 대해 상위 클래스에서 읽기 액세스는 상속되지만 쓰기 액세스는 거부될 수 있습니다.

    참고: **읽기** 확인란이 선택되어 있지 않은 경우 액세스 제어 항목이 장치에 대한 읽기 액세스에 영향을 주지 않을 뿐이지 읽기 액세스가 거부되는 것은 아닙니다.

    참고: 관리자 그룹을 사용자 목록에 추가할 수 없습니다. 대신 장치 관리자 그룹을 사용할 수 있습니다.

    예 1—사용자 또는 그룹에게 장치 또는 장치 클래스에 대한 쓰기 권한이 거부된 경우:

    동일한 사용자, 그룹 또는 그룹 구성원에게 장치 계층에서 해당 장치 아래에 있는 장치에 대해서만 쓰기 권한 또는 읽기+쓰기 권한이 허용될 수 있습니다.

    예 2—사용자 또는 그룹에게 장치 또는 장치 클래스에 대한 쓰기 권한이 허용된 경우:

    동일한 사용자, 그룹 또는 그룹 구성원에게 해당 장치 또는 장치 계층에서 해당 장치 아래에 있는 장치에 대해서만 쓰기 권한 또는 읽기+쓰기 권한이 거부될 수 있습니다.

    예 3—사용자 또는 그룹에게 장치 또는 장치 클래스에 대한 읽기 권한이 허용된 경우:

    동일한 사용자, 그룹 또는 그룹 구성원에게 해당 장치 또는 장치 계층에서 해당 장치 아래에 있는 장치에 대해서만 읽기 권한 또는 읽기+쓰기 권한이 거부될 수 있습니다.

    예 4—사용자 또는 그룹에게 장치 또는 장치 클래스에 대한 읽기 권한이 거부된 경우:

    동일한 사용자, 그룹 또는 그룹 구성원에게 장치 계층에서 해당 장치 아래에 있는 장치에 대해서만 권한 또는 읽기+쓰기 권한이 허용될 수 있습니다.

    예 5—사용자 또는 그룹에게 장치 또는 장치 클래스에 대한 읽기+쓰기 권한이 허용된 경우:

    동일한 사용자, 그룹 또는 그룹 구성원에게 해당 장치 또는 장치 계층에서 해당 장치 아래에 있는 장치에 대해서만 쓰기 권한 또는 읽기+쓰기 권한이 거부될 수 있습니다.

    예 6—사용자 또는 그룹에게 장치 또는 장치 클래스에 대한 읽기+쓰기 권한이 거부된 경우:

    동일한 사용자, 그룹 또는 그룹 구성원에게 장치 계층에서 해당 장치 아래에 있는 장치에 대해서만 읽기 권한 또는 읽기+쓰기 권한이 허용될 수 있습니다.

사용자 또는 그룹에게 액세스 거부

장치 또는 장치 클래스에 대한 사용자 또는 그룹의 액세스를 차단하려면 다음과 같이 하십시오.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 구성할 장치 클래스를 누릅니다.
   - **장치 클래스**
   - **모든 장치**
   - **개별 장치**
3. **사용자/그룹**에서 액세스를 거부할 사용자 또는 그룹을 누른 다음 **거부**를 누릅니다.
4. **적용**을 누릅니다.

참고: 사용자에 대해 동일한 장치 수준에서 거부 및 허용 설정이 설정된 경우 액세스 거부가 액세스 허용보다 우선합니다.

사용자 또는 그룹에게 액세스 허용

사용자 또는 그룹에게 장치 또는 장치 클래스에 대한 액세스 권한을 허용하려면 다음과 같이 하십시오.

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

   사용자 또는 그룹 선택 대화 상자가 열립니다.
4. **고급**을 누른 다음 **지금 찾기**를 눌러 추가할 사용자 또는 그룹을 검색합니다.
5. 사용 가능한 사용자 및 그룹 목록에 추가할 사용자 또는 그룹을 누른 다음 **확인**을 누릅니다.
6. 다시 한 번 **확인**을 누릅니다.
7. **허용**을 눌러 해당 사용자에게 액세스를 허용합니다.
8. **적용**을 누릅니다.

그룹의 한 사용자에게 장치 클래스에 대한 액세스 허용

그룹의 한 사용자에게 장치 클래스에 대한 액세스를 허용하고 그룹의 나머지 구성원에게는 액세스를 거부하려면 다음과 같이 하십시오.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 클릭한 다음 **장치 클래스 구성**을 클릭합니다.
2. 장치 목록에서 구성할 장치 클래스를 누릅니다.
   - **장치 클래스**
   - **모든 장치**
   - **개별 장치**
3. **사용자/그룹**에서 액세스를 거부할 그룹을 누른 다음 **거부**를 누릅니다.
4. 필요한 클래스 폴더 아래 폴더로 이동하여 특정 사용자를 추가합니다.
5. **허용**을 눌러 해당 사용자에게 액세스를 허용합니다.
6. **적용**을 누릅니다.

그룹의 한 사용자에게 특정 장치에 대한 액세스 허용

관리자는 다음과 같은 방법으로 그룹의 한 사용자에게 특정 장치에 대한 액세스를 허용하고 그룹의 나머지 구성원에게는 클래스의 모든 장치에 대한 액세스를 거부할 수 있습니다.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 구성할 장치 클래스를 누른 다음 해당 클래스 아래 폴더로 이동합니다.
3. **사용자/그룹**에서 액세스를 허용할 그룹 옆의 **허용**을 누릅니다.
4. 액세스를 거부할 그룹 옆의 **거부**를 누릅니다.
5. 장치 목록에서 사용자 액세스가 허용된 특정 장치로 이동합니다.
6. **추가**를 누릅니다.

   사용자 또는 그룹 선택 대화 상자가 열립니다.
7. **고급**을 누른 다음 **지금 찾기**를 눌러 추가할 사용자 또는 그룹을 검색합니다.
8. 액세스를 허용할 사용자를 누른 다음 **확인**을 누릅니다.
9. **허용**을 눌러 해당 사용자에게 액세스를 허용합니다.
10. **적용**을 누릅니다.

사용자 또는 그룹에 대한 설정 제거

사용자 또는 그룹의 장치 또는 장치 클래스에 대한 액세스 권한을 제거하려면 다음과 같이 하십시오.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **장치 클래스 구성**을 누릅니다.
2. 장치 목록에서 구성할 장치 클래스를 누릅니다.
   - **장치 클래스**
   - **모든 장치**
   - **개별 장치**
3. **사용자/그룹**에서 제거할 사용자 또는 그룹을 누른 다음 **제거**를 누릅니다.
4. **적용**을 누릅니다.

구성 재설정

⚠ **주의:** 구성을 재설정하면 장치 구성에 대한 모든 변경 내용이 무시되고 모든 설정이 기본 설정 값으로 되돌려집니다.

구성 설정을 기본값으로 재설정하려면 다음과 같이 하십시오.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **장치 클래스 구성**을 누릅니다.
2. **재설정**을 누릅니다.
3. **예**를 눌러 요청을 확인합니다.
4. **적용**을 누릅니다.

JITA 구성

JITA 구성을 사용하면 관리자가 Just In Time 인증(JITA)을 통해 장치에 액세스할 수 있는 사용자와 그룹 목록을 확인하고 수정할 수 있습니다.

JITA 를 활성화한 사용자의 경우 **장치 클래스 구성** 또는 **단순 구성** 보기에서 생성된 정책에서 제한한 일부 장치에 액세스할 수 있습니다.

- **시나리오**—단순 구성 정책은 장치 관리자 이외의 모든 사용자가 DVD/CD-ROM 드라이브에 액세스하는 경우 액세스를 거부하도록 구성되어 있습니다.
- **결과**—JITA 를 활성화한 사용자가 DVD/CD-ROM 드라이브에 액세스하려고 할 경우 JITA 를 비활성화한 사용자처럼 "액세스 거부" 메시지가 나타나고 JITA 액세스를 사용할지 묻는 풍선 메시지가 표시됩니다. 풍선 메시지를 클릭하면 사용자 인증 대화 상자가 표시됩니다. 사용자 인증 정보를 입력하면 DVD/CD-ROM 드라이브에 대한 액세스가 허용됩니다.

JITA 기간은 설정된 시간(분) 또는 0 분으로 인증됩니다. 0 분으로 인증된 JITA 기간은 만료되지 않습니다. 사용자는 인증한 시간부터 시스템 로그오프 시간까지 장치에 액세스할 수 있습니다.

JITA 기간을 연장할 수 있도록 구성되어 있는 경우 기간을 연장할 수 있습니다. 이 시나리오의 경우 JITA 기간 만료 1 분 전에 액세스를 연장하라는 메시지를 누르면 됩니다. 이때 재인증할 필요가 없습니다.

JITA 기간의 제한 여부에 관계없이 사용자가 시스템에서 로그오프하거나 다른 사용자가 로그인하면 JITA 기간이 만료됩니다. 다음에 사용자가 로그인하여 JITA 사용 장치에 액세스하려는 경우 인증 정보를 입력하라는 메시지가 표시됩니다.

JITA 는 다음 장치 클래스에서 사용할 수 있습니다.

- DVD/CD-ROM 드라이브
- 이동 미디어

사용자 또는 그룹용 JITA 생성

Just In Time 인증(JITA)을 사용하여 관리자는 장치에 대한 사용자 또는 그룹의 액세스를 허용할 수 있습니다.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **JITA 구성**을 누릅니다.
2. 장치의 드롭다운 메뉴에서 **이동 미디어** 또는 **DVD/CD-ROM 드라이브**를 선택합니다.
3. **+**를 눌러 JITA 구성에 사용자 또는 그룹을 추가합니다.
4. **활성화됨** 확인란을 선택합니다.
5. JITA 기간을 필요한 시간만큼 설정합니다.
6. **적용**을 누릅니다.

새로운 JITA 설정을 적용하려면 로그아웃 후 다시 로그인해야 합니다.

사용자 또는 그룹용 연장 가능한 JITA 생성

만료 전 사용자가 연장할 수 있는 Just In Time 인증(JITA)을 사용하여 관리자는 사용자 또는 그룹이 장치에 액세스하도록 허용할 수입니다.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **JITA 구성**을 누릅니다.
2. 장치의 드롭다운 메뉴에서 **이동 미디어** 또는 **DVD/CD-ROM 드라이브**를 선택합니다.
3. **+**를 눌러 JITA 구성에 사용자 또는 그룹을 추가합니다.
4. **활성화됨** 확인란을 선택합니다.
5. JITA 기간을 필요한 시간만큼 설정합니다.
6. **연장 가능** 확인란을 선택합니다.
7. **적용**을 누릅니다.

새로운 JITA 설정을 적용하려면 로그아웃 후 다시 로그인해야 합니다.

사용자 또는 그룹용 JITA 비활성화

Just In Time 인증(JITA)을 사용하여 관리자는 장치에 대한 사용자 또는 그룹의 액세스를 비활성화할 수 있습니다.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **JITA 구성**을 누릅니다.
2. 장치의 드롭다운 메뉴에서 **이동 미디어** 또는 **DVD/CD-ROM 드라이브**를 선택합니다.
3. JITA 를 비활성화할 사용자 또는 그룹을 선택합니다.
4. **활성화됨** 확인란을 선택 해제합니다.
5. **적용**을 누릅니다.

사용자가 로그인하여 장치 액세스를 시도하면 액세스가 거부됩니다.

고급 설정

고급 설정에서는 다음 기능을 제공합니다.

- 장치 관리자 그룹 관리
- Device Access Manager 에서 항상 액세스를 허용하는 드라이브 문자 관리

Device Access Manager 정책에서 지정하는 제한을 신뢰할 수 있는 사용자(장치 액세스에 대해)에게 적용하지 않으려면 장치 관리자 그룹을 사용합니다. 신뢰할 수 있는 사용자에는 일반적으로 시스템 관리자가 포함됩니다. 자세한 내용은 83페이지의장치 관리자 그룹을 참조하십시오.

고급 설정 보기에서 관리자는 Device Access Manager 가 모든 사용자에 대해 액세스를 제한하지 않는 드라이브 문자 목록을 구성할 수 있습니다.

참고: 드라이브 문자 목록이 구성되어 있으면 Device Access Manager 백그라운드 서비스가 실행되어야 합니다.

서비스를 시작하려면 다음과 같이 하십시오.

1. 단순 구성 정책(예: 장치 관리자 이외의 모든 사용자에게 이동 미디어에 대한 액세스 거부)을 적용합니다.

   또는

   관리자 권한이 있는 명령 프롬프트 창을 열고 다음을 입력합니다.

   sc start flcdlock

   enter 키를 누릅니다.

2. 서비스가 실행되면 드라이브 목록을 수정할 수 있습니다. Device Access Manager 의 제어가 필요하지 않은 장치의 드라이브 문자를 입력하십시오.

   실제 하드 디스크 또는 파티션의 드라이브 문자가 표시됩니다.

참고: 목록에 시스템 드라이브(일반적으로 C)가 포함되어 있는지 여부와 관계없이 모든 사용자가 시스템 드라이브에 액세스할 수 있습니다.

장치 관리자 그룹

Device Access Manager 가 설치되면 장치 관리자 그룹이 생성됩니다.

Device Access Manager 정책에서 지정하는 제한을 신뢰할 수 있는 사용자(장치 액세스에 대해)에게 적용하지 않으려면 장치 관리자 그룹을 사용합니다. 신뢰할 수 있는 사용자에는 일반적으로 시스템 관리자가 포함됩니다.

참고: 장치 관리자 그룹에 사용자를 추가하는 것으로 사용자에게 장치에 대한 액세스가 자동으로 허용되는 것은 아닙니다. **장치 클래스 구성** 보기에서 장치에 대한 사용자 그룹의 액세스가 거부된 경우 해당 그룹의 구성원이 장치에 액세스할 수 있도록 장치 관리자 그룹의 액세스를 허용해야 합니다. **단순 구성** 보기에서는 장치 관리자 그룹의 구성원이 아닌 사용자가 장치 클래스에 액세스할 수 없도록 거부할 수 있습니다.

장치 관리자 그룹에 사용자를 추가하려면 다음과 같이 하십시오.

1. **고급 설정** 보기에서 **+**를 선택합니다.
2. 신뢰할 수 있는 사용자의 이름을 입력합니다.

3. **확인**을 누릅니다.
4. **적용**을 누릅니다.

이 그룹의 구성원 자격을 관리하는 다른 방법은 다음과 같습니다.

- Windows 7 Professional 또는 Windows Vista 를 사용하는 경우 표준 "로컬 사용자 및 그룹" MMC 스냅인을 사용하여 사용자를 이 그룹에 추가할 수 있습니다.
- Windows 7, Vista 또는 XP Home 버전을 사용하는 경우 관리자 권한이 있는 계정에서 명령 프롬프트 창에 다음을 입력합니다.

  net localgroup "Device Administrators" username /add

  이 명령에서 "username"은 그룹에 추가하려는 사용자 이름입니다.

eSATA 지원

Device Access Manager 에서 eSATA 장치를 제어하려면 다음 항목이 구성되어 있어야 합니다.

1. 시스템을 시작할 때 드라이브가 연결되어 있어야 합니다.
2. **고급 설정** 보기를 사용하여 eSATA 드라이브 문자가 Device Access Manager 가 액세스를 거부하지 않는 드라이브 목록에 없는지 확인합니다. eSATA 드라이브 문자가 목록에 있는 경우 드라이브 문자를 삭제하고 **적용**을 누릅니다.
3. **단순 구성** 보기 또는 **장치 클래스 구성** 보기에서 이동 미디어 장치 클래스를 사용하여 장치를 제어할 수 있습니다.

관리되지 않는 장치 클래스

HP ProtectTools Device Access Manager 에서 관리되지 않는 장치 클래스는 다음과 같습니다.

- 입/출력 장치
  - 생체인식
  - 마우스
  - 키보드
  - 프린터
  - 플러그 앤드 플레이(PnP) 프린터
  - 프린터 업그레이드
  - 적외선 휴먼 인터페이스 장치
  - 스마트 카드 리더
  - 멀티 포트 직렬
  - 디스크 드라이브
  - 플로피 디스크 컨트롤러(FDC)

- 하드 디스크 컨트롤러(HDC)
- 휴먼 인터페이스 장치(HID) 클래스

- 전원
  - 배터리
  - 고급 전원 관리(APM) 지원
- 기타 장치
  - 컴퓨터
  - 디코더
  - 디스플레이
  - 프로세서
  - 시스템
  - 알 수 없음
  - 볼륨
  - 볼륨 스냅샷
  - 보안 장치
  - 보안 가속기
  - Intel® 통합 디스플레이 드라이버
  - 미디어 드라이버
  - 미디움 체인저
  - 다기능
  - Legacard
  - Net client(네트워크 클라이언트)
  - Net service(네트워크 서비스)
  - Net trans(네트워크 전송)
  - SCSI 어댑터

9 도난 회수

Computrace for HP ProtectTools(별도 구매)를 사용하여 컴퓨터를 원격으로 모니터링하고 관리하며 추적할 수 있습니다.

Computrace for HP ProtectTools 를 활성화한 후에는 Absolute Software 고객 센터에서 구성할 수 있습니다. 관리자는 고객 센터에서 Computrance for HP ProtectTools 를 구성하여 컴퓨터를 모니터링 및 관리할 수 있습니다. 시스템을 분실 또는 도난당한 경우 경찰에서 컴퓨터를 찾고 회수하는 데 고객 센터가 도움을 줄 수 있습니다. Computrance 를 하드 드라이브가 삭제 또는 교체되더라도 계속 작동하도록 구성할 수 있습니다.

Computrace for HP ProtectTools 를 활성화하려면 다음과 같이 하십시오.

1. 인터넷에 연결합니다.
2. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools Security Manager** 를 차례로 클릭합니다.
3. Security Manager 왼쪽 창에서 **도난 회수**를 클릭합니다.
4. Computrace 활성화 마법사를 시작하려면 **지금 활성화** 버튼을 클릭합니다.
5. 연락처 정보와 신용카드 결제 정보를 입력하거나 이미 구입한 제품 키를 입력합니다.

활성화 마법사가 안전하게 트랜잭션을 처리하고 Absolute Software 고객 센터 웹 사이트에 사용자 계정을 설정합니다. 완료되면 사용자의 고객 센터 계정 정보가 포함된 확인 전자 우편이 전송됩니다.

이전에 Computrace 활성화 마법사를 실행했었고 고객 센터 사용자 계정이 이미 있는 경우 HP 계정 담당자에게 연락하여 추가 라이선스를 구입할 수 있습니다.

고객 센터에 로그인하려면 다음과 같이 하십시오.

1. https://cc.absolute.com/으로 이동합니다.
2. **로그인 ID** 및 **암호** 필드에 확인 전자 우편으로 받은 인증 정보를 입력한 다음 **로그인** 버튼을 클릭합니다.

고객 센터에서는 다음과 같은 작업을 할 수 있습니다.

- 컴퓨터를 모니터링합니다.
- 원격 데이터를 보호합니다.
- Computrace 가 보호하는 모든 컴퓨터의 도난을 보고합니다.

▲ Computrace for HP ProtectTools 에 대해 자세히 알아 보려면 **추가 정보**를 클릭하십시오.

10 HP ProtectTools Embedded Security(일부 모델만 해당)

참고: HP ProtectTools Embedded Security 를 사용하기 위해서는 컴퓨터에 통합 TPM(Trusted Platform Module) 내장 보안 칩이 설치되어 있어야 합니다.

HP ProtectTools Embedded Security 모듈은 사용자 데이터나 인증 정보에 대한 무단 액세스를 방지합니다. 이 소프트웨어 모듈은 다음과 같은 보안 기능을 제공합니다.

- Microsoft® EFS(암호화 파일 시스템)를 통한 향상된 파일 및 폴더 암호화
- 사용자 데이터 보호를 위한 PSD(개인 보안 드라이브) 생성
- 키 계층 백업 및 복원 등의 데이터 관리 기능
- Embedded Security 소프트웨어를 사용할 때 보안 디지털 인증서 작업에 타사 응용프로그램(예: Microsoft Outlook, Internet Explorer) 지원

TPM 내장 보안 칩은 HP ProtectTools Security Manager 의 다른 보안 기능을 향상시키고 활성화합니다. 예를 들어, Credential Manager for HP ProtectTools 는 사용자가 Windows 에 로그온할 때 인증 요소로 내장 칩을 사용할 수 있습니다.

설정 절차

⚠ **주의:** 보안 위험을 줄이기 위해 IT 관리자가 내장 보안 칩을 즉시 초기화할 것을 권장합니다. 내장 보안 칩을 초기화하지 않을 경우 무단 사용자, 컴퓨터 웜 또는 바이러스가 컴퓨터를 장악하고 응급 복구 아카이브 처리, 사용자 액세스 설정과 같은 소유자 작업을 제어할 수 있습니다.

내장 보안 칩을 초기화하려면 다음 절의 단계를 따르십시오.

Computer Setup 에서 내장 보안 칩 활성화

내장 보안 칩은 빠른 초기화 마법사 또는 Computer Setup 유틸리티에서 활성화해야 합니다.

Computer Setup 에서 내장 보안 칩을 활성화하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 다시 시작하고 f10 = ROM Based Setup 메시지가 화면의 왼쪽 아래에 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 관리자 암호를 설정하지 않은 경우, 화살표 키를 사용하여 **Security**(보안), **Setup password**(암호 설정)를 선택한 다음 enter 키를 누릅니다.
3. **New password**(새 암호) 및 **Verify new password**(새 암호 확인) 입력란에 암호를 입력하고 f10 키를 누릅니다.
4. **Security**(보안) 메뉴에서 화살표 키를 사용하여 **TPM Embedded Security** 를 선택한 다음 enter 키를 누릅니다.
5. **Embedded Security** 에서 장치가 숨김 상태인 경우 **Available**(사용 가능)을 선택합니다.
6. **내장 보안 장치 상태**를 선택한 다음 설정을 **활성화**로 변경합니다.
7. f10 키를 눌러 Embedded Security 구성에 대한 변경사항을 수락합니다.
8. 기본 설정을 저장하고 Computer Setup 을 종료하려면 화살표를 사용하여 **파일**을 선택하고 **변경 내용 저장 및 종료**를 선택한 다음 화면의 지시를 따릅니다.

내장 보안 칩 초기화

Embedded Security 모듈의 초기화 프로세스 도중 다음과 같은 작업을 수행하게 됩니다.

- 내장 보안 칩의 모든 소유자 기능에 무단으로 액세스하지 못하도록 내장 보안 칩 소유자 암호 설정
- 모든 사용자에 대한 기본 사용자 키의 재암호화를 허용하는 보안 스토리지 영역인 응급 복구 아카이브 설정

내장 보안 칩을 초기화하려면 다음과 같이 하십시오.

1. 작업 표시줄의 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools Security Manager** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **내장 보안 초기화**를 선택합니다.

   HP ProtectTools Embedded Security Initialization Wizard(HP ProtectTools Embedded Security 초기화 마법사)가 열립니다.

2. 화면 지침을 따릅니다.

기본 사용자 계정 설정

Embedded Security 에서 기본 사용자 계정을 설정하면 다음 작업이 완료됩니다.

- 암호화된 정보를 보호하는 기본 사용자 키를 생성하고 기본 사용자 키를 보호하는 기본 사용자 키 암호를 설정합니다.
- 암호화된 파일과 폴더를 저장하기 위해 PSD(개인 보안 드라이브)를 설정합니다.

⚠ **주의:** 기본 사용자 키 암호를 잘 보관하십시오. 이 암호 없이는 암호화된 정보를 액세스하거나 복구할 수 없습니다.

기본 사용자 계정을 설정하고 사용자 보안 기능을 활성화하려면 다음과 같이 하십시오.

1. 내장 보안 사용자 초기화 마법사가 열려 있지 않은 경우 **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools Security Manager** 를 차례로 클릭합니다.
2. 왼쪽 창에서 **Embedded Security**, **User Settings**(사용자 설정)를 차례로 누릅니다.
3. 오른쪽 창의 **Embedded Security Features**(Embedded Security 기능)에서 **Configure**(구성)를 누릅니다.

   Embedded Security User Initialization Wizard(Embedded Security 사용자 초기화 마법사)가 열립니다.
4. 화면 지침을 따릅니다.

참고: 보안 전자 우편을 사용하려면 먼저 전자 우편 클라이언트가 Embedded Security 로 생성된 디지털 인증서를 사용하도록 구성해야 합니다. 디지털 인증서를 사용할 수 없는 경우, 인증 기관으로부터 인증서를 받아야 합니다. 전자 우편을 구성하고 디지털 인증서를 받는 방법은 전자 우편 클라이언트 소프트웨어 도움말을 참조하십시오.

일반 작업

기본 사용자 계정을 설정한 후 다음 작업을 수행할 수 있습니다.

- 파일 및 폴더 암호화
- 암호화된 전자 우편 송수신

개인 보안 드라이브 사용

PSD 를 설정한 후에는 다음에 로그온할 때 기본 사용자 키 암호를 입력하라는 메시지가 나타납니다. 기본 사용자 키 암호를 올바르게 입력하면 Windows 탐색기에서 PSD 에 직접 액세스할 수 있습니다.

파일 및 폴더 암호화

암호화된 파일을 사용할 경우 다음 규칙을 알아 두어야 합니다.

- NTFS 파티션의 파일과 폴더만 암호화할 수 있습니다. FAT 파티션의 파일과 폴더는 암호화할 수 없습니다.
- 시스템 파일과 압축 파일은 암호화할 수 없으며 암호화한 파일은 압축할 수 없습니다.
- 임시 폴더는 해커의 공격 대상이 될 수 있으므로 반드시 암호화해야 합니다.
- 파일이나 폴더를 최초로 암호화하면 복구 정책이 자동 설정됩니다. 이 정책은 사용자가 암호화 인증서와 개인 키를 분실한 경우, 복구 에이전트를 사용하여 정보를 암호화 해독할 수 있도록 합니다.

파일 및 폴더를 암호화하려면 다음과 같이 하십시오.

1. 암호화할 파일 또는 폴더를 마우스 오른쪽 버튼으로 누릅니다.
2. **Encrypt**(암호화)를 누릅니다.
3. 다음 옵션 중 하나를 누릅니다.
   - **Apply changes to this folder only**(이 폴더에만 변경사항 적용)
   - **Apply changes to this folder, subfolders, and files**(이 폴더, 하위 폴더 및 파일에 변경사항 적용)
4. **확인**을 누릅니다.

암호화된 전자 우편 송수신

Embedded Security 에서는 암호화된 전자 우편을 송수신할 수 있으나 절차는 전자 우편을 액세스하는 데 사용하는 프로그램에 따라 다릅니다. 자세한 내용은 Embedded Security 소프트웨어 도움말 및 해당 전자 우편 프로그램용 소프트웨어 도움말을 참조하십시오.

기본 사용자 키 암호 변경

기본 사용자 키 암호를 변경하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools Security Manager** 를 차례로 클릭합니다.
2. 왼쪽 창에서 **Embedded Security**, **User Settings**(사용자 설정)를 차례로 누릅니다.
3. 오른쪽 창의 **기본 사용자 암호**에서 **변경**을 클릭합니다.
4. 이전 암호를 입력한 다음 새 암호를 설정하고 확인합니다.
5. **확인**을 누릅니다.

고급 작업

관리자가 Embedded Security 에서 다음 작업을 수행할 수 있습니다.

- Embedded Security 인증 정보, Embedded Security 설정 및 개인 보안 드라이브 백업 및 복원
- 소유자 암호 변경
- 사용자 암호 재설정
- 사용자 보안 자격 증명을 원본 플랫폼에서 대상 플랫폼으로 안전하게 마이그레이션

백업 및 복원

Embedded Security 백업 기능은 응급 상황 시 복원할 인증 정보를 포함하는 아카이브를 생성합니다.

백업 파일 생성

백업 파일을 생성하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Backup**(백업)을 누릅니다.
3. 오른쪽 창에서 **구성**을 클릭합니다. HP Embedded Security for ProtectTools 백업 마법사가 열립니다.
4. 화면 지침을 따릅니다.

백업 파일에서 인증서 데이터 복원

백업 파일에서 데이터를 복원하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**, **HP** 및 **HP ProtectTools 관리 콘솔**을 차례로 클릭합니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Backup**(백업)을 누릅니다.
3. 오른쪽 창에서 **Restore all**(모두 복원)을 클릭합니다. HP Embedded Security for ProtectTools 백업 마법사가 열립니다.
4. 화면 지침을 따릅니다.

소유자 암호 변경

관리자는 소유자 암호를 변경할 수 있습니다.

1. **시작**, **모든 프로그램**, **HP** 을 차례로 클릭한 다음 **HP ProtectTools 관리 콘솔**을 클릭합니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.
3. 오른쪽 창의 **Owner Password**(소유자 암호)에서 **Change**(변경)를 누릅니다.
4. 이전 소유자 암호를 입력한 다음 새 소유자 암호를 설정하고 확인합니다.
5. **확인**을 누릅니다.

사용자 암호 재설정

관리자는 사용자가 잊은 암호를 재설정하도록 지원할 수 있습니다. 자세한 내용은 소프트웨어 도움말을 참조하십시오.

Migration Wizard(마이그레이션 마법사)로 키 마이그레이션

마이그레이션은 키와 인증서의 관리, 복원 및 이전을 위한 고급 관리 작업입니다.

마이그레이션에 대한 자세한 내용은 Embedded Security 소프트웨어 도움말을 참조하십시오.

11 지역화된 암호 예외

Preboot Security 수준 및 HP Drive Encryption 수준에서는 지역화된 암호 지원이 다음 섹션에 설명된 바와 같이 제한됩니다.

Windows IME 는 Preboot Security 수준 또는 HP Drive Encryption 수준에서 지원되지 않음

Windows 를 사용하는 경우 IME(입력기)를 선택하여 서양식 표준 키보드로 일본어 또는 중국어와 같은 복잡한 문자와 기호를 입력할 수 있습니다.

Preboot Security 또는 HP Drive Encryption 수준에서는 IME 가 지원되지 않습니다. Windows 암호는 Preboot Security 또는 HP Drive Encryption 의 로그인 화면에서 IME 를 사용하여 입력할 수 없으며, IME 를 사용하여 Windows 암호를 입력하면 계정이 잠길 수 있습니다. 경우에 따라 사용자가 암호를 입력할 때 Microsoft® Windows 에서 IME 가 표시되지 않을 수도 있습니다.

예를 들어 Windows XP 의 일부를 일본어 버전으로 설치하는 경우 기본 IME 는 Microsoft IME Standard 2002 for Japanese 이며, 실제로 키보드 레이아웃 E0010411 로 번역합니다. 단, 이는 IME 이지 키보드 레이아웃이 아닙니다. (키보드 레이아웃 개념을 확장하는 Microsoft 의 독자적인 IME 용 기술인 키보드 레이아웃 코딩 스키마가 사용됩니다.) BIOS Preboot Security 암호 프롬프트 또는 HP Drive Encryption 암호 프롬프트용 입력 환경에서 사용되는 키보드 레이아웃이 아니므로 이 IME 를 통해 입력된 암호는 HP ProtectTools 에서 거부됩니다. Microsoft IME Standard 2002 for Japanese 는 Microsoft Windows Vista®의 “일반 이름”과도 다릅니다. Windows 는 일부 IME 를 키보드 레이아웃으로 매핑합니다. 이 경우 기본 키보드 레이아웃 정의(16 진수 코드)가 사용되므로 IME 가 HP ProtectTools 에서 지원됩니다.

키보드 레이아웃 00000411 로 변환되는 다음과 같은 지원되는 키보드 레이아웃 중 하나로 전환하여 이 문제를 해결할 수 있습니다.

- Microsoft IME for Japanese
- 일본어 키보드 레이아웃
- Office 2007 IME for Japanese—Microsoft 또는 타사에서 IME 또는 입력기라는 용어를 사용하는 경우 실제 입력 방법이 IME 가 아닐 수 있으므로 혼동을 초래할 수 있습니다. 단, 소프트웨어에서는 16 진수 코드 표현으로 인식하므로 IME 에서 지원되는 키보드 레이아웃으로 매핑할 경우 HP ProtectTools 에서 이 구성을 지원할 수 있습니다.

⚠ **경고!** HP ProtectTools 배포 시 Windows IME 로 암호를 입력하면 거부됩니다.

지원되는 다른 키보드 레이아웃을 사용하여 암호 변경

미국 영어(409)와 같은 키보드 레이아웃을 사용하여 암호를 설정한 후 라틴 아메리카(080A)와 같은 지원되는 다른 키보드 레이아웃을 사용하여 암호를 변경할 경우, HP Drive Encryption 에서 변경된 암호를 사용할 수 있습니다. 단, 기존 암호에 없던 문자가 변경된 암호에 있는 경우 BIOS 에서 암호를 사용할 수 없습니다(예: ē).

참고: 관리자는 HP ProtectTools 사용자 관리 기능을 사용하여 HP ProtectTools 에서 사용자를 삭제한 후 운영 체제에서 적절한 키보드 레이아웃을 선택한 다음, 동일한 사용자에 대해 Security Manager 설정 마법사를 다시 실행하여 이 문제를 해결할 수 있습니다. 선택된 키보드 레이아웃이 BIOS 에 저장되며 이 키보드 레이아웃을 사용하여 입력한 암호가 BIOS 에 제대로 설정됩니다.

다른 키보드 레이아웃을 사용해도 같은 문자가 입력되는 문제가 발생할 수 있습니다. 예를 들어 미국 국제 키보드 레이아웃(20409)과 라틴 아메리카 키보드 레이아웃(080A)에서 모두 é 를 입력할 수 있으므로 키 입력 순서를 다르게 해야 합니다. 라틴 아메리카 키보드 레이아웃을 사용하여 암호를 처음 설정한 경우 나중에 미국 국제 키보드 레이아웃을 사용하여 암호를 변경해도 BIOS 에 라틴 아메리카 키보드 레이아웃이 계속 설정되어 있습니다.

특수 키 처리

- 중국어, 슬로바키아어, 캐나다 프랑스어 및 체코어

  사용자가 위 언어에 대한 키보드 레이아웃 중 하나를 선택한 후 암호(예: abcdef)를 입력할 경우 BIOS Preboot Security 및 HP Drive Encryption 에서 소문자는 shift 키를, 대문자는 shift 키 및 caps lock 키를 누른 상태에서 암호를 입력해야 하며, 숫자 암호는 숫자 키패드를 사용하여 입력해야 합니다.

- 한국어

  사용자가 지원되는 한국어 키보드 레이아웃을 선택한 후 암호를 입력할 경우 BIOS Preboot Security 및 HP Drive Encryption 에서 소문자는 오른쪽 alt 키를, 대문자는 오른쪽 alt 키 및 caps lock 키를 누른 상태에서 암호를 입력해야 합니다.

- 지원되지 않는 문자는 다음 표에 나열되어 있습니다.

언어	Windows	BIOS	Drive Encryption
아랍어	ﻻ, ﻷ 및 ﻹ 키는 두 개의 문자로 입력됩니다.	ﻻ, ﻷ 및 ﻹ 키는 한 개의 문자로 입력됩니다.	ﻻ, ﻷ 및 ﻹ 키는 한 개의 문자로 입력됩니다.
캐나다 프랑스어	Windows 에서 caps lock 키를 누르고 ç, è, à 및 é 문자를 입력하면 Ç, È, À 및 É 문자로 입력됩니다.	caps lock 키를 누르고 ç, è, à 및 é 문자를 입력하면 BIOS Preboot Security 에서 ç, è, à 및 é 문자로 입력됩니다.	caps lock 키를 누르고 ç, è, à 및 é 문자를 입력하면 HP Drive Encryption 에서 ç, è, à 및 é 문자로 입력됩니다.
스페인어	40a 는 지원되지 않지만 소프트웨어에서 c0a 로 변환되므로 사용할 수는 있습니다. 단, 키보드 레이아웃 간 약간의 차이가 있으므로 스페인어 사용자의 경우 Windows 키보드 레이아웃을 1040a(스페인어 변형) 또는 080a(라틴 아메리카)로 변경하는 것이 좋습니다.	해당 사항 없음	해당 사항 없음
영어(국제)	◦ 맨 위 행의 ¡, ¤, ‘, ’, ¥ 및 × 키는 입력되지 않습니다. ◦ 두 번째 행의 å, ® 및 Þ 키는 입력되지 않습니다. ◦ 세 번째 행의 á, ð 및 ø 키는 입력되지 않습니다. ◦ 맨 아래 행의 æ 키는 입력되지 않습니다.	해당 사항 없음	해당 사항 없음

언어	Windows	BIOS	Drive Encryption
체코어	◦ ğ 키는 입력되지 않습니다. ◦ į 키는 입력되지 않습니다. ◦ ų 키는 입력되지 않습니다. ◦ ė, ı 및 ż 키는 입력되지 않습니다. ◦ ģ, ķ, ļ, ņ 및 ţ 키는 입력되지 않습니다.	해당 사항 없음	해당 사항 없음
슬로바키아어	ż 키는 입력되지 않습니다.	◦ š, ś 및 ş 키의 경우 키보드 입력 시에는 입력되지 않지만 소프트 키보드에서는 사용할 수 있습니다. ◦ ţ 데드 키는 두 개의 문자로 입력됩니다.	해당 사항 없음
헝가리어	ż 키는 입력되지 않습니다.	ţ 키는 두 개의 문자로 입력됩니다.	해당 사항 없음
슬로베니아어	żŻ 키는 Windows 에서 입력되지 않으며 alt 키는 BIOS 에서 데드 키로 입력됩니다.	ú, Ú, ů, Ů, ş, Ş, ś, Ś, š 및 Š 키는 BIOS 에서 입력되지 않습니다.	해당 사항 없음
일본어	Windows XP 에서만 411 표준 일본어 키보드 레이아웃이 완벽하게 지원됩니다. Windows XP 에서 Microsoft Standard IME 2002 로 많이 사용되고 있는 IME 는 일반적으로 지원되지 않습니다. 그러나 실제로 테스팅해 본 결과, 간단한 문자의 경우 이 IME 와 411 키보드 레이아웃이 거의 유사하므로 지역화된 일본어 암호를 사용하여 BIOS 및 HP Drive Encryption 를 보호할 때 소프트웨어에서 이 IME 를 411 키보드 레이아웃으로 전환합니다. 가능한 경우 Microsoft Office 2007 IME 를 사용하는 것이 좋습니다. 이름은 IME 지만 실제로는 지원되는 키보드 레이아웃 411 입니다.	해당 사항 없음	해당 사항 없음

암호가 거부될 때 취해야 할 조치

다음과 같은 이유로 암호가 거부될 수 있습니다.

- 지원되지 않는 IME 를 사용합니다. 이 문제는 2 바이트 언어(한국어, 일본어, 중국어)에서 자주 발생하며, 이 문제를 해결하는 방법은 다음과 같습니다.

  1. **시작**, **제어판**을 차례로 클릭한 다음, **국가 및 언어 설정**을 클릭합니다.
  2. **언어** 탭을 클릭합니다.
  3. **자세히** 버튼을 클릭합니다.
  4. **설정** 탭에서 **추가** 버튼을 눌러 지원되는 키보드를 추가합니다(중국어 입력 언어에서 미국 키보드를 추가).
  5. 기본 입력 방법으로 지원되는 키보드를 설정합니다.
  6. HP ProtectTools 를 다시 시작한 후 암호를 다시 입력합니다.

- 지원되지 않는 문자를 사용합니다. 이 문제를 해결하는 방법은 다음과 같습니다.

  1. 지원되는 문자만 사용하도록 Windows 암호를 변경합니다. 지원되지 않는 문자는 98페이지의특수 키 처리에서 확인할 수 있습니다.
  2. Security Manager 설정 마법사를 다시 실행한 후 새 Windows 암호를 입력합니다.

용어

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

CA(Certification Authority)
공개 키 인프라를 실행하는 데 필요한 인증서를 발급하는 서비스

CSP(암호화 서비스 제공업체)
올바르게 정의된 인터페이스에서 사용 가능하며 특정 암호화 기능을 수행하기 위한 암호화 알고리즘의 제공업체 또는 라이브러리

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

Drive Encryption 로그온 화면
Windows 가 시작되기 전에 표시되는 로그온 화면. 사용자는 Windows 사용자 이름 및 암호 또는 스마트 카드 PIN 을 입력해야 합니다. 대부분의 경우 Drive Encryption 로그온 화면에 정확한 정보를 입력하면 Windows 로그온 화면에 다시 로그온할 필요 없이 바로 Windows 에 액세스할 수 있습니다.

DriveLock
하드 드라이브를 사용자에게 연결하고 컴퓨터가 시작될 때 사용자에게 정확한 DriveLock 암호를 입력하도록 요구하는 보안 기능

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

HP SpareKey
Drive Encryption 키의 백업 사본

ID
HP ProtectTools Security Manager 에서 특정 사용자의 프로파일 또는 계정처럼 취급되는 인증 정보 및 설정 그룹

ID 카드
사용자 이름과 선택한 사진으로 데스크탑을 시각적으로 식별하는 Windows 바탕 화면 가젯. HP ProtectTools 관리 콘솔을 열려면 ID 카드를 클릭하십시오.

JITA
Just In Time 인증(JITA)

PIN
개인 식별 번호

PKI
인증서 및 암호화 키의 생성, 사용 및 관리에 대한 인터페이스를 정의하는 공개 키 인프라 표준

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
컴퓨터와 대용량 저장 장치(예: 하드 드라이브와 광 드라이브) 사이의 데이터 전송 모드

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 Office 응용프로그램의 도구 모음에 표시되는 소프트웨어 버튼. 이 버튼을 클릭하면 Microsoft Office 문서를 서명, 암호화 또는 암호화 제거할 수 있습니다.

Single Sign On
인증 정보를 저장하고 Security Manager 를 사용하여 암호 인증을 요구하는 인터넷 및 Windows 응용프로그램에 액세스하는 기능입니다.

TPM(Trusted Platform Module) 내장 보안 칩
HP ProtectTools 내장 보안 칩을 가리키는 일반적인 용어. TPM 은 호스트 시스템에만 해당하는 암호화 키, 디지털 인증서, 암호 등의 정보를 저장하여 사용자가 아닌 컴퓨터를 인증합니다. TPM 은 물리적 절도 또는 외부 해커의 공격으로 컴퓨터의 정보가 손상될 위험을 최소화합니다.

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 일종.

USB 토큰
사용자에 대한 ID 정보를 저장하는 보안 장치. 스마트 카드 또는 생체 인식 리더와 마찬가지로 소유자를 컴퓨터에 인증하는 데 사용합니다.

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 로그온할 권한이 있는 개인용 프로파일

가상 토큰
스마트 카드 및 카드 리더처럼 작동하는 보안 기능. 토큰은 컴퓨터 하드 드라이브 또는 Windows 레지스트리에 저장됩니다. 가상 토큰으로 로그온하면 사용자 PIN 을 입력해야 인증이 완료됩니다.

관리자
*Windows 관리자*를 참조하십시오.

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, 워크 그룹 또는 도메인에 있는 Windows 사용자 또는 관리자 계정

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

도메인
같은 네트워크에 속하며 공통의 디렉터리 데이터베이스를 공유하는 컴퓨터 그룹. 도메인의 이름은 고유하며 각각 공통의 규칙 및 절차 집합을 가지고 있습니다.

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 Device Locking/Auditing 백그라운드 서비스. 제어판의 관리 도구 옵션의 서비스 응용프로그램에서 확인할 수 있습니다. 장치 액세스 제어 정책을 적용할 때 백그라운드 서비스가 실행되고 있지 않으면 HP ProtectTools Security Manager 에서 백그라운드 서비스를 시작합니다.

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 사람. 관리자 이외의 사용자에게는 Drive Encryption 에 대한 권한이 제한됩니다. 관리자 이외의 사용자는 등록(관리자의 승인이 있는 경우)과 로그온만 할 수 있습니다.

사진
인증에 사용되는 등록된 사용자의 사진.

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 파쇄하는 작업

스마트 카드
소유자에 대한 색별 정보가 저장되어 있고 신용 카드와 비슷한 크기와 모양의 작은 하드웨어. 소유자를 컴퓨터에 인증하는 데 사용됩니다.

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 대해 봉인
디지털 서명을 추가하고 전자 우편을 암호화하고 선택한 보안 로그온 방법을 통해 인증한 후 전자 우편을 보내는 작업

암호 해독
암호화에서 암호화된 데이터를 일반 텍스트로 변환하는 데 사용되는 절차

암호화
특정 개인만 디코딩할 수 있도록 데이터를 암호화 및 암호 해제하는 절차

암호화
권한 없는 수신자가 데이터를 읽을 수 없도록 일반 텍스트를 암호 텍스트로 변환하기 위한 암호화에 사용되는 절차(예: 알고리즘 사용). 데이터 암호화는 네트워크 보안의 기초로 여러 유형이 있습니다. 일반 유형에는 데이터 암호화 표준 및 공개 키 암호화가 포함됩니다.

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

응급 복구 아카이브
플랫폼 소유자 키 사이에서 기본 사용자 키를 재암호화할 수 있는 보호된 스토리지 영역

인증
사용자가 컴퓨터 액세스, 특정 프로그램의 설정 변경, 보안 데이터 보기 등의 작업을 수행할 권한이 있는지 여부를 확인하는 과정

인증서
인증 과정에서 사용자가 특정 작업에 대한 적격 여부를 증명하는 수단

자동 파쇄
File Sanitizer 에서 사용자가 설정할 수 있는 예약 파쇄

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 다시 시작하는 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 위치

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

토큰
*보안 로그온 방법*을 참조하십시오.

파쇄
자산이 있는 데이터를 손상시키는 알고리즘을 실행하는 작업

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

파쇄 프로필
지정된 삭제 방법 및 자산 목록입니다.

파워온 인증
컴퓨터를 켤 때 어떤 형태의 인증(예: 스마트 카드, 보안 칩, 암호 등)을 요구하는 보안 기능

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