# HP ProtectTools

시작하기

초판: 2012 년 8 월

문서 부품 번호: 702113-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 Security Manager 관리 콘솔(관리자용) | • 액세스할 때 Microsoft Windows® 관리자 권한이 있어야 합니다.<br>• 관리자가 구성하여 사용자가 사용할 수 없는 모듈에 대한 액세스를 제공합니다.<br>• 최초 보안 설정을 허용하고 모든 사용자의 옵션 또는 요구 사항을 구성합니다. |
| HP ProtectTools Security Manager 사용자 콘솔(사용자용) | • 관리자가 제공한 옵션을 사용자가 구성할 수 있습니다.<br>• 관리자가 사용자에게 일부 HP ProtectTools 모듈에 대한 제한적 제어를 제공할 수 있습니다. |

컴퓨터에서 사용할 수 있는 소프트웨어 모듈은 컴퓨터 모델에 따라 다를 수 있습니다.

HP ProtectTools 소프트웨어 모듈은 사전 설치되어 있거나 사전 로드되어 있을 수 있으며 HP 웹 사이트에서 다운로드할 수도 있습니다. 자세한 내용은 http://www.hp.com 을 참조하십시오.

**참고:** 이 설명서의 지침은 사용자가 적절한 HP ProtectTools 소프트웨어 모듈을 이미 설치했다고 가정하고 작성되었습니다.

## HP ProtectTools 기능

다음 표에는 HP ProtectTools 모듈의 주요 기능에 대한 설명이 나와 있습니다.

| 모듈 | 주요 기능 |
|---|---|
| HP ProtectTools Security Manager 관리 콘솔 | 관리자는 다음 기능을 수행할 수 있습니다.<br>• Security Manager 설정 마법사를 사용하여 보안 수준과 보안 로그온 방법을 설정하고 구성합니다.<br>• 사용자에게 숨겨진 옵션을 구성합니다.<br>• Drive Encryption 을 활성화하고 사용자 액세스를 구성합니다.<br>• Device Access Manager 정책과 사용자 액세스를 구성합니다.<br>• 관리자 도구를 사용하여 HP ProtectTools 사용자를 추가 및 제거하고 사용자 상태를 확인합니다. |
| HP ProtectTools Security Manager 사용자 콘솔 | 일반 사용자는 다음 기능을 수행할 수 있습니다.<br>• 암호화 상태와 Device Access Manager 에 대한 설정을 확인합니다.<br>• Computrace for HP ProtectTools 를 활성화합니다.<br>• 기본 설정과 백업 및 복원 옵션을 구성합니다. |

| 모듈 | 주요 기능 |
| --- | --- |
| Credential Manager | 일반 사용자는 다음 기능을 수행할 수 있습니다.<br>• 사용자 이름과 암호를 변경합니다.<br>• Windows 암호, 지문, 얼굴 이미지, 스마트 카드, 근접 카드, 비접촉식 카드 등의 사용자 인증 정보를 구성하고 변경합니다. |
| 암호 관리자 | 일반 사용자는 다음 기능을 수행할 수 있습니다.<br>• 사용자 이름과 암호를 구성하고 설정합니다.<br>• 계정 보안을 강화하기 위해 더 강력한 암호를 만듭니다. Password Manager 가 자동으로 정보를 입력하고 제출합니다.<br>• 사용자 인증 정보를 자동으로 기억하고 적용하는 Single Sign-On 기능을 사용하여 로그온 프로세스를 간소화합니다. |
| Drive Encryption for HP ProtectTools(일부 모델만 해당) | • 완전한 전체 볼륨 하드 드라이브 암호화를 제공합니다.<br>• 데이터를 해독하고 액세스하기 위한 사전 부팅 인증을 강제 실행합니다.<br>• 자체 암호화 드라이브를 활성화하는 옵션을 제공합니다(일부 모델만 해당). |
| Device Access Manager for HP ProtectTools(일부 모델만 해당) | • IT 관리자가 사용자 프로필을 기준으로 장치에 대한 액세스를 제어할 수 있습니다.<br>• 권한 없는 사용자가 외장 스토리지 미디어를 사용하여 데이터를 제거하거나 외장 미디어에서 시스템으로 바이러스가 침입하는 것을 방지합니다.<br>• 관리자가 특정 개인 또는 사용자 그룹에 대해 통신 장치에 대한 액세스를 비활성화할 수 있습니다. |
| 도난 회수(Computrace for HP ProtectTools, 별도 구매) | • 활성화하려면 별도로 추적 가입을 구매해야 합니다.<br>• 안전한 자산 추적을 제공합니다.<br>• 사용자 활동, 하드웨어 및 소프트웨어 변경 사항을 모니터링합니다.<br>• 하드 드라이브가 다시 포맷되거나 교체된 경우에도 활성 상태를 유지합니다. |

# 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.

## 암호 관리자

Password Manager 에서는 사용자 이름과 암호를 저장하고 다음과 같은 작업을 수행할 수 있습니다.

- 인터넷 액세스 또는 전자 메일에 대한 로그인 이름과 암호를 저장합니다.
- 웹 사이트 또는 전자 메일에 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, Password Manager 를 사용하여 웹 링크에 다른 사용자 이름과 암호를 대응시키기로 결정합니다. 로그온하는 웹 사이트에 가면 Password Manager 가 인증 정보를 자동으로 제시합니다. 사용자 이름과 암호를 확인하려면 Password Manager 를 구성하여 해당 정보를 표시할 수도 있습니다.

Password Manager 는 인증을 관리하고 정리하는 데도 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 로그온해야 하는데 각 계정은 다른 로그인 정보를 사용합니다. 이 로그인 정보는 다른 직원과 공유해야 하기 때문에 기밀 유지가 문제입니다. 이 공인 회계사는 Password Manager 내에서 모든 웹 링크, 회사 사용자 이름 및 암호를 정리하기로 결정합니다. 정리를 마치고 직원에게 Password Manager 를 배포한 후 직원들은 자신들이 사용하는 로그인 인증 정보를 모르는 상태에서 웹 계정을 사용할 수 있게 됩니다.

## Drive Encryption for HP ProtectTools(일부 모델만 해당)

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 사전 부팅 인증을 요구하는 Drive Encryption 을 활성화합니다. 설정 후 이 하드 드라이브는 운영 체제가 시작되기 전 암호 없이 액세스가 불가능하게 됩니다. 자체 암호화 드라이브 옵션을 사용하여 데이터를 암호화하도록 선택하여 드라이브 보안을 더욱 강화할 수 있습니다.

Drive Encryption for HP ProtectTools 는 원래의 시스템 보드에 구속되어 있기 때문에 드라이브가 제거된 경우에도 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.

## Device Access Manager for HP ProtectTools(일부 모델만 해당)

관리자는 Device Access Manager for HP ProtectTools 를 사용하여 하드웨어에 대한 액세스를 제한 및 관리할 수 있습니다. 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, 예를 들어 외부 공급업체가 회사 컴퓨터에 액세스해야 하지만, 데이터를 USB 드라이브로 복사하면 안 되는 상황이 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.

## Computrace for HP ProtectTools(이전의 LoJack Pro)(별매)

Computrace for HP ProtectTools(별도 구매)는 도난 당한 컴퓨터에서 인터넷에 액세스할 때 위치를 추적하는 서비스입니다. Computrace for HP ProtectTools 는 또한 컴퓨터를 원격으로 관리하고 위치를 파악할 수 있으며 컴퓨터 사용 상태 및 응용 프로그램을 모니터링할 수 있습니다.

**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.

**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.

# 주요 보안 목표 달성

HP ProtectTools 모듈은 다음과 같은 주요 보안 목표를 비롯한 다양한 보안 문제에 대한 해결 방법을 제공하기 위해 함께 작동할 수 있습니다.

- 표적 도난으로부터 보호
- 민감한 데이터에 대한 액세스 제한
- 내부 또는 외부 위치에서의 무단 액세스 방지
- 강력한 암호 정책 만들기

## 표적 도난으로부터 보호

표적 도난의 예로 공항 보안 검색대에서 기밀 데이터와 고객 정보가 포함된 컴퓨터를 도난당하는 경우를 들 수 있습니다. 다음 기능을 사용하여 표적 도난으로부터 보호할 수 있습니다.

- 부팅 전 인증 기능을 활성화하면 운영 체제에 대한 액세스를 차단할 수 있습니다.
  - Security Manager for HP ProtectTools—24페이지의 HP ProtectTools Security Manager 참조.
  - Drive Encryption for HP ProtectTools—38페이지의 Drive Encryption for HP ProtectTools(일부 모델만 해당) 참조.
- 암호화는 하드 드라이브가 제거되어 보안되지 않은 시스템에 설치된 경우에도 데이터에 액세스할 수 없도록 하는 데 도움이 됩니다.
- Computrace 는 컴퓨터를 도난당한 후 컴퓨터의 위치를 추적할 수 있습니다.
  - Computrace for HP ProtectTools—56페이지의도난 회수(일부 모델만 해당) 참조.

## 민감한 데이터에 대한 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 통신 장치에 대한 액세스를 제한하여 하드 드라이브에서 민감한 정보를 복사하지 못하도록 설정할 수 있습니다. 48페이지의장치 클래스 구성을 참조하십시오.

## 내부 또는 외부 위치에서의 무단 액세스 방지

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.
  - Security Manager for HP ProtectTools—24페이지의 HP ProtectTools Security Manager 참조.
  - Drive Encryption for HP ProtectTools—38페이지의 Drive Encryption for HP ProtectTools(일부 모델만 해당) 참조.
- Security Manager 는 권한 없는 사용자가 암호를 얻거나 암호로 보호되는 응용프로그램에 액세스하지 못하도록 하는 데 도움이 됩니다. 24페이지의 HP ProtectTools Security Manager 를 참조하십시오.
- IT 관리자가 Device Access Manager for HP ProtectTools 에서 쓰기 가능 장치에 대한 액세스를 제한하여 하드 드라이브에서 민감한 정보를 복사하지 못하도록 설정할 수 있습니다. 46페이지의 HP ProtectTools Device Access Manager(일부 모델만 해당)를 참조하십시오.

## 강력한 암호 정책 만들기

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. 24페이지의 HP ProtectTools Security Manager 를 참조하십시오.

# 추가 보안 요소

## 보안 역할 할당

특히 대규모 조직의 경우 컴퓨터 보안 관리에서 명심해야 할 중요한 방법은 다양한 유형의 관리자와 사용자에게 책임과 권한을 분산시키는 것입니다.

**참고:** 소규모 조직이나 개인 사용의 경우 이러한 역할을 모두 동일한 사람이 담당할 수 있습니다.

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

- 보안 담당자—회사와 네트워크의 보안 수준을 정의하며 Drive Encryption 과 같은 배포할 보안 기능을 결정합니다.

  **참고:** 보안 담당자는 HP 와 협력하여 HP ProtectTools 의 많은 기능을 사용자 정의할 수 있습니다. 자세한 내용은 http://www.hp.com 을 참조하십시오.
- 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 최종 사용자 권한과 사용자 액세스를 제한하는 데 “모범 사례”를 따르도록 권장 받습니다.

권한 없는 사용자에게 관리 권한을 부여해서는 안 됩니다.

## HP ProtectTools 암호 관리

HP ProtectTools Security Manager 기능은 대부분 암호로 보안됩니다. 다음 표에는 일반적으로 사용되는 암호, 암호가 설정되는 소프트웨어 모듈 및 암호 기능이 나열되어 있습니다.

IT 관리자만 설정하고 사용하는 암호도 이 표에 나와 있습니다. 다른 모든 암호는 일반 사용자나 관리자가 설정할 수 있습니다.

| HP ProtectTools 암호 | 설정하는 모듈 | 기능 |
|---|---|---|
| Windows 로그온 암호 | Windows 제어판 또는 HP ProtectTools Security Manager | 다양한 Security Manager 기능에 액세스하기 위한 수동 로그온 및 인증에 사용할 수 있습니다. |
| Security Manager 백업 및 복구 암호 | Security Manager, 개별 사용자가 설정 | Security Manager 백업 및 복구 파일에 대한 액세스를 보호합니다. |
| 스마트 카드 PIN | Credential Manager | 다단계 인증으로 사용할 수 있습니다.<br>Windows 인증으로 사용할 수 있습니다.<br>스마트 카드가 선택된 경우 Drive Encryption 사용자를 인증합니다. |

### 안전한 암호 만들기

암호를 만들 때 먼저 프로그램에 의해 설정된 사양을 모두 따라야 합니다. 그러나 강력한 암호를 만들고 암호가 손상될 가능성을 줄이기 위해 다음 지침을 일반적으로 고려해야 합니다.

- 6 자가 넘는 암호를 사용합니다(9 자 이상이 좋음).
- 암호 전반에서 대/소문자를 섞어서 사용합니다.
- 가능한 한 영숫자를 섞어서 사용하고 특수 기호와 구두점을 포함합니다.
- 키 단어에서 문자 대신 특수 기호나 숫자를 사용합니다. 예를 들어, 문자 I 또는 L 대신 숫자 1 을 사용할 수 있습니다.
- 둘 이상의 언어로 된 단어를 조합합니다.
- “Mary2-2Cat45”와 같이 중간에 숫자나 특수 문자를 넣어 단어 또는 구를 분리합니다.
- 사전에 나타나는 암호를 사용하지 마십시오.
- 암호에 사용자의 이름이나 생일, 애완동물 이름, 어머니의 이름과 같은 개인 정보를 사용하지 마십시오. 거꾸로 입력하는 경우도 마찬가지입니다.
- 정기적으로 암호를 변경합니다. 증가하는 두세 문자만 변경할 수도 있습니다.
- 암호를 적어 두는 경우 컴퓨터에서 아주 가깝고 눈에 잘 띄는 곳에 두지 마십시오.
- 컴퓨터의 파일(예: 전자 메일)에 암호를 저장하지 마십시오.
- 계정을 공유하거나 다른 사람에게 암호를 알려주지 마십시오.

## 인증 정보 및 설정 백업

다음과 같은 방법을 사용하여 인증 정보를 백업할 수 있습니다.

- Drive Encryption for HP ProtectTools 를 사용하여 HP ProtectTools 인증 정보를 선택하고 백업합니다.
- 설치된 일부 HP ProtectTools 모듈에서 보안 인증 정보를 백업하고 복원할 수 있는 중앙 위치로 HP ProtectTools Security Manager 의 백업 및 복구 도구를 사용합니다.

# 2 시작

HP ProtectTools 의 설정을 구성하려면 HP Client Security 설치 마법사 또는 HP ProtectTools Security Manager 설치 마법사를 사용합니다.

HP Client Security 설치 마법사를 완료한 후 응용 프로그램 상태가 HP Client Security 대시보드에 표시됩니다.

## HP Client Security 설치 마법사

**참고:** HP ProtectTools 를 관리하려면 관리자 권한이 필요합니다.

HP Client Security 설치 마법사는 Security Manager 에서 가장 일반적으로 사용되는 기능을 설치하는 과정을 안내합니다. 이전에 HP Client Security 설치 마법사를 완료하지 않은 경우, 다음 방법 중 하나를 통해 HP Client Security 설치 마법사를 실행할 수 있습니다.

▲ 시작 화면에서 **HP Client Security** 앱을 클릭하거나 누릅니다.

– 또는 –

Windows 데스크톱에서 **HP ProtectTools** 가젯을 클릭하거나 누릅니다.

페이지가 다음 순서로 표시됩니다.

1. **Windows 암호**—Windows 암호를 입력합니다.

   이렇게 하면 강력한 인증을 사용하여 Windows 계정이 보호됩니다.

2. **SpareKey**—SpareKey 옵션을 등록하려면 세 가지 보안 질문을 선택합니다.

3. **지문 등록**—지문 인식기 및 관련 드라이버가 설치되어 있으면 지문을 등록할 수 있습니다. 최소 2 개의 지문을 선택하여 등록해야 합니다.

4. **Drive Encryption**—Drive Encryption for HP ProtectTools 가 설치되어 있으면 기본 드라이브에서 암호를 활성화할 수 있습니다.

   - 일반 하드 드라이브의 소프트웨어 암호화
   - 자체 암호화 드라이브가 감지된 경우 하드웨어 암호화.

   암호화를 활성화하기 전에 다음 중 하나 이상에 암호화 키를 저장해야 합니다.

   **참고:** 이번에 마법사를 취소하면 Windows 및 Drive Encryption 인증을 활성화할 수 없게 됩니다.

   - FAT 32 형식의 USB 플래시 드라이브 같은 **이동 미디어**.
     - Drive Encryption 페이지가 표시되기 전에 이동식 장치가 하나 감지된 경우 이 옵션이 기본적으로 선택됩니다.
     - 이동식 장치가 두 개 이상 감지된 경우에는 표시된 드라이브 중 하나를 선택합니다.
   - **SkyDrive**—인터넷 연결이 감지된 경우 이 옵션을 사용할 수 있습니다.

Windows® Live ID 가 필요합니다. ID 및 암호를 입력하거나, 등록하여 ID 를 하나 만드십시오.

5. 완료 페이지에 성공을 알리는 메시지가 표시되고, Drive Encryption 을 활성화하기 위해 재부팅하라는 메시지가 표시됩니다.

# HP ProtectTools Security Manager 설치 마법사

**참고:** HP ProtectTools 를 관리하려면 관리자 권한이 필요합니다.

HP ProtectTools Security Manager 설치 마법사는 Security Manager 의 기능을 설정하는 과정을 안내합니다. 마법사에 있는 설정뿐만 아니라 관리자는 관리 콘솔을 통해 많은 추가 보안 기능을 구성할 수 있습니다. 이러한 설정은 컴퓨터와 컴퓨터를 공유하는 모든 사용자에게 적용됩니다.

HP ProtectTools Security Manager 설치 마법사를 실행하려면

▲ 관리 콘솔의 왼쪽 패널에서 **설치 마법사**를 클릭한 다음 설정이 완료될 때까지 화면에 나타난 지시를 따릅니다.

관리자는 HP ProtectTools Security Manager 사용자 콘솔에서 관리 콘솔을 실행할 수 있습니다. 자세한 내용은 14페이지의 HP ProtectTools Security Manager 관리 콘솔를 참조하십시오.

이 컴퓨터를 공유하는 모든 사용자는 Security Manager 와 해당 응용 프로그램을 사용할 수 있습니다.

# HP Client Security 대시보드

이전에 HP Client Security 설치 마법사를 완료한 경우 HP Client Security 를 열려면

▲ 시작 화면에서 hp 를 입력한 다음 **HP Client Security** 를 선택합니다.

대시보드에 각 응용 프로그램의 기능에 대한 간략한 개요 및 관련 상태가 표시됩니다.

▲ 응용 프로그램 행을 클릭하거나 두드리면 선택한 응용 프로그램에 대한 자세한 정보가 표시됩니다.

- **지금 구성** 버튼은 아직 구성되지 않은 응용 프로그램을 나타냅니다. 버튼을 클릭하거나 두드려 응용 프로그램 페이지를 열고 응용 프로그램을 구성합니다.
- **설정** 버튼은 상태가 정상인 응용 프로그램을 나타냅니다. 버튼을 클릭하거나 두드려 응용 프로그램의 설정에 액세스합니다.
- **사용자 콘솔**은 사용자 구성을 위해 실행됩니다.
- **관리 콘솔**은 구성하는 데 관리자 권한이 필요한 경우에 실행됩니다.
- **상태 대시보드**는 사용자 콘솔이나 관리 콘솔이 실행된 후 열린 상태로 있으며, 설정을 구성하고 콘솔을 닫으면 상태가 새로 고쳐집니다.

# 3 중소기업을 위한 쉬운 시작 가이드

이 장은 HP ProtectTools for Small Business 내에서 가장 일반적이고 유용한 옵션을 활성화하는 기본 단계를 보여 주기 위해 작성되었습니다. 이 소프트웨어에서는 기본 설정을 미세 조정하고 액세스 제어를 설정하는 데 사용할 수 있는 다양한 도구와 옵션이 있습니다. 이 쉬운 시작 가이드는 가장 적은 설정 노력과 시간으로 각 모듈을 실행하는 데 중점을 둡니다. 자세한 내용을 보려면 관심이 있는 모듈을 선택하고 **?**를 누르거나 오른쪽 상단에 있는 도움말 버튼을 누르십시오. 이 버튼을 누르면 현재 표시된 창에서 도움이 되는 정보가 자동으로 제공됩니다.

## 시작하기

1. Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭하여 HP ProtectTools Security Manager 를 엽니다.
2. Windows 암호를 입력하거나 Windows 암호를 만듭니다.
3. 설정 마법사를 완료합니다.

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

이 설정은 Windows 에 로그인한 동안 무단 액세스를 방지하도록 설계되었으며 높은 보안이 필요하거나 사용자가 업무 시간 중에 시스템에서 자주 자리를 비우는 경우에 사용해야 합니다. 이 설정을 변경하려면 세션 정책 탭을 누르고 원하는 항목을 선택합니다.

HP ProtectTools Security Manager 를 사용하려면 Windows 로그인 동안 한 번의 인증을 해야 합니다. 다음 절차를 따르십시오.

1. Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭하여 HP ProtectTools Security Manager 를 엽니다.
2. 왼쪽 창에서 **관리**를 클릭한 다음 **관리 콘솔**을 클릭합니다.
3. **시스템** 아래의 왼쪽 창에서 **보안** 그룹에 있는 **인증**을 선택합니다.
4. **세션 정책** 탭을 클릭한 다음 세션에 대한 로그인 조합 요구 사항을 선택합니다. 이러한 선택을 되돌리려면 **기본값 복원**을 클릭합니다.
5. 완료되면 **적용** 버튼을 누릅니다.

## 암호 관리자

암호! 우리는 꽤 많은 암호를 가지고 있습니다. – 특히 정기적으로 웹 사이트에 액세스하거나 로그온해야 하는 응용 프로그램을 사용할 경우에는 더욱 그렇습니다. 일반적인 사용자는 모든 응용 프로그램과 웹 사이트에 동일한 암호를 사용하거나 창의력을 십분 발휘하여 암호를 만든 다음 어떤 응용 프로그램에 어떤 암호를 사용했는지 금방 잊어버립니다.

Password Manager 는 자동으로 사용자의 암호를 기억하거나, 기억해야 할 사이트와 생략해야 할 사이트를 식별하는 기능을 제공합니다. 일단 컴퓨터에 로그온하면 응용 프로그램 또는 웹 사이트를 이용할 수 있도록 Password Manager 에서 암호나 인증 정보를 제공합니다.

사용자가 인증 정보가 필요한 응용프로그램이나 웹 사이트에 액세스하는 경우 Password Manager 는 사이트를 자동으로 인식하고 사용자 정보를 기억하도록 할 것인지 묻습니다. 특정 사이트를 제외하려면 이 요청을 거부할 수 있습니다.

웹 위치, 사용자 이름 및 암호를 저장하려면 다음과 같이 하십시오.

1. 예를 들어 이용할 웹 사이트 또는 응용 프로그램으로 이동한 다음 웹 페이지의 왼쪽 상단 모서리에 있는 Password Manager 아이콘을 클릭하여 웹 인증을 추가합니다.
2. 링크의 이름을 지정하고(선택 사항) 사용자 이름과 암호를 Password Manager 에 입력합니다.

**참고:** Password Manager 가 현재와 이후 방문에 사용할 영역이 강조 표시됩니다.

3. 완료되면 **확인** 버튼을 누릅니다.
4. Password Manager 는 네트워크 공유나 매핑된 네트워크 드라이브에 대한 사용자 이름과 암호도 저장할 수 있습니다.

## Password Manager 에 저장된 인증 확인 및 관리

Password Manager 를 사용하여 중앙 위치에서 인증을 확인, 관리, 백업 및 실행할 수 있습니다. Password Manager 는 저장된 사이트를 Windows 에서 실행하는 기능도 지원합니다.

Password Manager 를 열려면 다음 두 방법 중 하나를 사용합니다.

- 키보드 조합 Ctrl+Windows 로고 키+h 를 사용하여 Password Manager 를 연 다음 **열기**를 눌러 저장된 바로 가기를 실행하고 인증합니다.

  – 또는 –

- Password Manager 의 **관리** 탭을 선택하여 HP ProtectTools Security Manager 를 열고 인증 정보를 편집합니다.

Password Manager 의 **편집** 옵션으로 이름과 로그인 이름을 보거나 수정하고 암호를 표시할 수도 있습니다.

HP ProtectTools for Small Business 를 사용하면 모든 인증 정보 및 설정을 다른 컴퓨터에 백업 및/또는 복사할 수 있습니다.

# Device Access Manager for HP ProtectTools

Device Access Manager 를 사용하여 데이터가 하드 드라이브에서 안전하게 유지되고 외부로 유출되지 않도록 다양한 내부 및 외부 저장 장치의 사용을 제한할 수 있습니다. 예를 들어, 사용자가 데이터에 액세스할 수 있도록 허용하지만 CD, 개인용 음악 플레이어 또는 USB 메모리 장치에 복사하는 것은 차단할 수 있습니다. 이를 설정하는 쉬운 방법은 다음과 같습니다.

1. Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭하여 HP ProtectTools Security Manager 사용자 콘솔을 엽니다.
2. HP ProtectTools Security Manager 의 왼쪽 창에서 **관리**를 클릭한 다음 **관리 콘솔**을 클릭합니다.
3. **Device Access Manager** 를 클릭한 다음 **장치 클래스 구성**을 클릭합니다.
4. 다음 단계는 다른 모든 사람이 차단된 동안 계속 액세스할 수 있는 사용자를 선택하는 것입니다.
5. 제한할 하드웨어 장치를 선택한 다음 **적용** 버튼을 눌러 프로세스를 마칩니다.
6. **추가**를 선택하고 **고급**을 클릭한 다음 **지금 찾기**를 클릭합니다.
7. 원하는 사용자를 선택한 다음 **확인 > 확인 > 적용**을 클릭합니다.

   선택 사항이 **사용자/그룹** 상자에 표시됩니다.
8. 사용자가 사용할 **장치 클래스**를 선택하고 **허용** 또는 **거부**를 선택한 다음 **적용**을 클릭합니다.

# Drive Encryption for HP ProtectTools

Drive Encryption for HP ProtectTools 는 전체 하드 드라이브를 암호화하여 데이터를 보호하는 데 사용됩니다. PC 를 도난당하거나 하드 드라이브가 원래 컴퓨터에서 제거되어 다른 컴퓨터에 장착되는 경우에도 하드 드라이브의 데이터는 보호된 상태로 유지됩니다.

추가 보안 혜택은 Drive Encryption 에서 운영 체제를 시작하기 전에 사용자 이름과 암호를 사용하여 충분하게 인증하도록 요구하는 것입니다. 이 절차를 사전 부팅 인증이라고 합니다.

사용자에게 편리하도록 Windows 사용자 계정, 도메인, Drive Encryption for HP ProtectTools, Password Manager 및 HP ProtectTools Security Manager 를 비롯한 여러 소프트웨어 모듈이 암호를 자동으로 동기화합니다.

Drive Encryption for HP ProtectTools 를 활성화하려면 다음의 간단한 단계를 수행하십시오.

1. Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭하여 HP ProtectTools Security Manager 를 엽니다.
2. 왼쪽 창에서 **관리**를 클릭한 다음 **관리 콘솔**을 클릭합니다.
3. 왼쪽 창에서 **설정 마법사**를 클릭합니다.
4. 시작 화면에서 **다음**을 선택합니다.
5. Windows 암호를 입력하여 활성화 마법사를 시작하고 **다음**을 누릅니다.
6. SpareKey 를 원하지 않는 경우 건너뜁니다.
7. **Drive Encryption** 확인란을 선택하고 **다음**을 누릅니다.
8. 암호화할 드라이브를 선택하고 **다음**을 누릅니다.
9. Drive Encryption 구성 창에서 암호화 복구 키를 보관할 USB 플래시 드라이브 또는 기타 외부 장치를 요구합니다. 사전 부팅 암호를 분실하거나 사전 부팅에 실패할 경우 이 복구 키가 데이터를 복구하거나 드라이브에 액세스하는 데 사용되므로 안전하게 보관해야 합니다.

10. **다음**을 누르고 프로세스를 완료한 다음 **마침**을 누릅니다. USB 플래시 드라이브를 제거한 다음 준비가 되면 컴퓨터를 다시 부팅합니다.

11. 시스템이 시작되면 Drive Encryption 에서 Windows 암호를 요청합니다. 암호를 입력한 다음 **확인**을 누릅니다.

**참고:** 드라이브가 암호화되는 동안 컴퓨터가 느리게 실행되는 것처럼 보일 수도 있습니다. 완전히 암호화되면 성능이 정상적으로 돌아옵니다. 드라이브에 있는 데이터에 액세스되면 관리자의 요구에 따라 데이터가 암호화되거나 데이터의 암호가 해제됩니다.

Drive Encryption 인증은 Windows 로그인을 통해 Windows 데스크톱으로 직접 "연결"하므로 암호를 두 번 입력할 필요가 없습니다.

# 4 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 사용자 콘솔에서 기타 응용 프로그램을 사용할 수 있습니다(일부 모델에만 해당).

이 관리 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

## 시작

HP ProtectTools 의 설정을 구성하려면 HP Client Security 설치 마법사 또는 HP ProtectTools Security Manager 설치 마법사를 사용합니다.

HP Client Security 설치 마법사를 완료한 후 응용 프로그램 상태가 HP Client Security 대시보드에 표시됩니다.

### HP Client Security 설치 마법사

**참고:** HP ProtectTools 를 관리하려면 관리자 권한이 필요합니다.

HP Client Security 설치 마법사는 Security Manager 에서 가장 일반적으로 사용되는 기능을 설치하는 과정을 안내합니다. 이전에 HP Client Security 설치 마법사를 완료하지 않은 경우, 다음 방법 중 하나를 통해 HP Client Security 설치 마법사를 실행할 수 있습니다.

▲ 시작 화면에서 **HP Client Security** 앱을 클릭하거나 누릅니다.

– 또는 –

Windows 데스크톱에서 **HP ProtectTools** 가젯을 클릭하거나 누릅니다.

페이지가 다음 순서로 표시됩니다.

1. **Windows 암호**—Windows 암호를 입력합니다.

   이렇게 하면 강력한 인증을 사용하여 Windows 계정이 보호됩니다.

2. **SpareKey**—SpareKey 옵션을 등록하려면 세 가지 보안 질문을 선택합니다.

3. **지문 등록**—지문 인식기 및 관련 드라이버가 설치되어 있으면 지문을 등록할 수 있습니다. 최소 2 개의 지문을 선택하여 등록해야 합니다.

4. **Drive Encryption**—Drive Encryption for HP ProtectTools 가 설치되어 있으면 기본 드라이브에서 암호를 활성화할 수 있습니다.

   - 일반 하드 드라이브의 소프트웨어 암호화
   - 자체 암호화 드라이브가 감지된 경우 하드웨어 암호화.

   암호화를 활성화하기 전에 다음 중 하나 이상에 암호화 키를 저장해야 합니다.

   **참고:** 이번에 마법사를 취소하면 Windows 및 Drive Encryption 인증을 활성화할 수 없게 됩니다.

   - FAT 32 형식의 USB 플래시 드라이브 같은 **이동 미디어**.
     - Drive Encryption 페이지가 표시되기 전에 이동식 장치가 하나 감지된 경우 이 옵션이 기본적으로 선택됩니다.
     - 이동식 장치가 두 개 이상 감지된 경우에는 표시된 드라이브 중 하나를 선택합니다.
   - **SkyDrive**—인터넷 연결이 감지된 경우 이 옵션을 사용할 수 있습니다.

     Windows® Live ID 가 필요합니다. ID 및 암호를 입력하거나, 등록하여 ID 를 하나 만드십시오.

5. 완료 페이지에 성공을 알리는 메시지가 표시되고, Drive Encryption 을 활성화하기 위해 재부팅하라는 메시지가 표시됩니다.

## HP ProtectTools Security Manager 설치 마법사

**참고:** HP ProtectTools 를 관리하려면 관리자 권한이 필요합니다.

HP ProtectTools Security Manager 설치 마법사는 Security Manager 의 기능을 설정하는 과정을 안내합니다. 마법사에 있는 설정뿐만 아니라 관리자는 관리 콘솔을 통해 많은 추가 보안 기능을 구성할 수 있습니다. 이러한 설정은 컴퓨터와 컴퓨터를 공유하는 모든 사용자에게 적용됩니다.

HP ProtectTools Security Manager 설치 마법사를 실행하려면

▲ 관리 콘솔의 왼쪽 패널에서 **설치 마법사**를 클릭한 다음 설정이 완료될 때까지 화면에 나타난 지시를 따릅니다.

관리자는 HP ProtectTools Security Manager 사용자 콘솔에서 관리 콘솔을 실행할 수 있습니다. 자세한 내용은 14페이지의 HP ProtectTools Security Manager 관리 콘솔를 참조하십시오.

이 컴퓨터를 공유하는 모든 사용자는 Security Manager 와 해당 응용 프로그램을 사용할 수 있습니다.

## HP Client Security 대시보드

이전에 HP Client Security 설치 마법사를 완료한 경우 HP Client Security 를 열려면

▲ 시작 화면에서 hp 를 입력한 다음 **HP Client Security** 를 선택합니다.

대시보드에 각 응용 프로그램의 기능에 대한 간략한 개요 및 관련 상태가 표시됩니다.

▲ 응용 프로그램 행을 클릭하거나 두드리면 선택한 응용 프로그램에 대한 자세한 정보가 표시됩니다.

- **지금 구성** 버튼은 아직 구성되지 않은 응용 프로그램을 나타냅니다. 버튼을 클릭하거나 두드려 응용 프로그램 페이지를 열고 응용 프로그램을 구성합니다.
- **설정** 버튼은 상태가 정상인 응용 프로그램을 나타냅니다. 버튼을 클릭하거나 두드려 응용 프로그램의 설정에 액세스합니다.
- **사용자 콘솔**은 사용자 구성을 위해 실행됩니다.

- **관리 콘솔**은 구성하는 데 관리자 권한이 필요한 경우에 실행됩니다.
- **상태 대시보드**는 사용자 콘솔이나 관리 콘솔이 실행된 후 열린 상태로 있으며, 설정을 구성하고 콘솔을 닫으면 상태가 새로 고쳐집니다.

# HP ProtectTools 관리 콘솔 열기

시스템 정책 설정이나 소프트웨어 구성 같은 관리 작업을 위해 HP ProtectTools 관리 콘솔을 사용합니다. HP ProtectTools Security Manager 를 열어 관리 콘솔에 액세스합니다.

1. Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭합니다.

   – 또는 –

   **제어판**에서 **시스템 및 보안**을 선택한 다음 **HP ProtectTools Security Manager** 를 선택합니다.
2. Security Manager 사용자 콘솔의 왼쪽 패널에서 **관리**를 누른 다음 **관리 콘솔**을 클릭합니다.

# 관리 콘솔 사용

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

1. Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭합니다.

   – 또는 –

   **제어판**에서 **시스템 및 보안**을 선택한 다음 **HP ProtectTools Security Manager** 를 선택합니다.
2. Security Manager 사용자 콘솔의 왼쪽 패널에서 **관리**를 누른 다음 **관리 콘솔**을 클릭합니다.

관리 콘솔에는 왼쪽 패널에 있는 홈 아래에 다음 선택이 표시됩니다.

- **시스템**—사용자와 장치에 대한 다음과 같은 보안 기능과 인증을 구성할 수 있습니다.
  - **보안**
  - **사용자**
  - **인증 정보**
- **응용 프로그램**—HP ProtectTools Security Manager 와 Security Manager 응용 프로그램에 대한 설정을 구성할 수 있습니다.
- **데이터**—Drive Encryption(일부 모델만 해당)에 대한 설정을 구성할 수 있습니다.
- **컴퓨터**—Device Access Manager 에 대한 설정을 구성할 수 있습니다.
- **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**—응용 프로그램별 화면을 표시합니다.

  **?**—관리 콘솔 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 관리 및 구성합니다.

## 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 대한 인증을 설정하려면 다음과 같이 하십시오.

1. 관리 콘솔의 왼쪽 패널에서 **보안**을 누른 다음 **인증**을 누릅니다.
2. 로그온 인증을 구성하려면 **로그온 정책** 탭을 눌러 변경한 다음 **적용**을 누릅니다.
3. 세션 인증을 구성하려면 **세션 정책** 탭을 눌러 변경한 다음 **적용**을 누릅니다.

### 로그온 정책

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

1. 관리 콘솔의 왼쪽 패널에서 **보안**을 누른 다음 **인증**을 누릅니다.
2. **로그온 정책** 탭에서 관리자 또는 표준 사용자 같은 사용자 범주를 선택합니다.
3. 인증 정보를 클릭하여 편집 대화 상자를 표시합니다.
4. 두 인증 정보의 조합을 요청하려면 아래쪽 화살표를 눌러 각 인증 정보를 선택한 다음 **확인**을 누릅니다.
5. 인증 정보를 제거하려면 **X** 를 누르거나 인증 정보를 마우스 오른쪽 버튼으로 누른 다음 **삭제**를 누릅니다.
6. 구성 대화 상자에 있는 **예**를 누릅니다.
7. 사용자가 로그온할 수 있는지 확인하려면 **HP ProtectTools 에 로그온할 수 있는지 확인**을 누릅니다.
8. 원래 설정으로 되돌리려면 **기본값 복원**을 누릅니다.
9. **적용**을 누릅니다.

### 세션 정책

Windows 세션 중 인증을 수행하는 데 필요한 인증 정보를 관리하는 정책을 정의하려면 다음과 같이 하십시오.

1. 관리 콘솔의 왼쪽 패널에서 **보안**을 누른 다음 **인증**을 누릅니다.
2. **세션온 정책** 탭에서 관리자 또는 표준 사용자 같은 사용자 범주를 선택합니다.
3. 인증 정보를 클릭하여 편집 대화 상자를 표시합니다.

4. 두 인증 정보의 조합을 요청하려면 아래쪽 화살표를 눌러 각 인증 정보를 선택한 다음 **확인**을 누릅니다.
5. 인증 정보를 제거하려면 **X** 를 누르거나 인증 정보를 마우스 오른쪽 버튼으로 누른 다음 **삭제**를 누릅니다.
6. 구성 대화 상자에 있는 **예**를 누릅니다.
7. 사용자가 로그온할 수 있는지 확인하려면 **HP ProtectTools 에 로그온할 수 있는지 확인**을 누릅니다.
8. 원래 설정으로 되돌리려면 **기본값 복원**을 누릅니다.
9. **적용**을 누릅니다.

## 설정

BIOS 또는 Drive Encryption 수준에서 인증을 이미 수행한 경우 이 컴퓨터의 사용자가 Windows 로그온을 생략할 수 있도록 하려면 다음과 같이 하십시오.

1. 관리 콘솔의 왼쪽 패널에서 **보안**을 누른 다음 **설정**을 누릅니다.
2. **One Step logon 허용**—One Step logon 을 활성화하려면 확인란을 선택하고 비활성화하려면 확인란을 선택 해제합니다.
3. **적용**을 누릅니다.

## 사용자 관리

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

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

사용자를 관리하려면 다음 설정 중에서 선택하십시오.

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

## 인증 정보

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

### SpareKey

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

1. SpareKey 등록 도중 사용자에게 표시될 보안 질문을 선택합니다.

   최대 세 개의 사용자 정의 질문을 지정하거나 사용자가 직접 암호를 입력하도록 허용할 수 있습니다.
2. Windows 로그온 SpareKey 복구를 허용하려면 확인란을 선택합니다.
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 손가락을 스와이프할 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.

## 얼굴

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

1. **인증 정보**를 누른 다음 **얼굴**을 누릅니다.
2. 편의성을 높이려면 슬라이더를 눌러 왼쪽으로 이동하고, 정확도를 높이려면 슬라이더를 눌러 오른쪽으로 이동합니다.
   - **낮음**—등록된 사용자가 손쉽게 한계 상황에 대한 액세스를 얻게 하려면 슬라이더 막대를 클릭하여 **낮음** 위치로 이동합니다.
   - **보통**—보안과 편의성 사이에서 적절한 조합을 제공하려거나 무단 로그온이 발생할 수 있는 위치에 기밀 정보 또는 컴퓨터가 있는 경우, 슬라이더 막대를 클릭하여 **보통** 위치로 이동합니다.
   - **높음**—등록된 장면 또는 현재 조명이 정상보다 어둡고 잘못 수락될 가능성이 낮은 경우 사용자가 액세스를 얻기가 더 어려워지게 하려면 슬라이더 막대를 클릭하여 **높음** 위치로 이동합니다.
3. 원래 값으로 설정을 되돌리려면 **기본값 복원**을 누릅니다.
4. **적용**을 누릅니다.

## 스마트 카드

인증용으로 사용할 스마트 카드는 관리자가 먼저 초기화해야 합니다. Windows 에서는 대부분의 CSP 및 PKCS11 표준 스마트 카드를 지원합니다.

### 스마트 카드 초기화

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

**참고:** 스마트 카드 미들웨어를 반드시 설치해야 합니다.

1. 사용 중인 스마트 카드용 미들웨어(예: ActivIdentity 스마트 카드용 ActivClient 6.x)를 가져와 설치합니다.
2. 스마트 카드를 리더에 삽입합니다.
3. 스마트 카드를 초기화(포맷)합니다.
   a. 스마트 카드 초기화 도구를 시작하고, 스마트 카드를 리더에 삽입할 때 표시될 수도 있습니다.
   b. 화면의 지시를 따라 PIN 을 설정합니다.
   c. 나중에 참조할 수 있도록 잠금 해제 코드를 적어둡니다.
4. 키 쌍과 인증서를 만듭니다.
   a. **HP ProtectTools 관리 콘솔**을 실행합니다.
   b. **인증 정보**를 누르고 **스마트 카드**를 누른 다음 **관리** 탭을 누릅니다.
   c. **스마트 카드 초기화**가 선택되어 있는지 확인하십시오.
   d. PIN 을 입력하고 **적용**을 누른 다음 화면의 지시를 따릅니다.

   스마트 카드를 초기화한 후에는 스마트 카드를 등록해야 합니다.

### 스마트 카드 등록

스마트 카드를 초기화한 후 관리자는 다음과 같이 스마트 카드를 HP ProtectTools 관리 콘솔에서 인증 방법으로 등록할 수 있습니다.

1. **설치 마법사**를 클릭합니다.
2. **시작** 화면에서 **다음**을 클릭합니다.
3. Windows 암호를 입력하고 **다음**을 누릅니다.
4. **SpareKey** 페이지에서 **SpareKey 설정 건너뛰기**를 누르고(SpareKey 정보를 업데이트하지 않을 경우) **다음**을 누릅니다.
5. **Enable security features**(보안 기능 활성화)에서 **다음**을 누릅니다.
6. **인증 정보 선택** 페이지에서 **스마트 카드**를 선택하고 **다음**을 누릅니다.
7. **스마트 카드** 페이지에서 PIN 을 입력한 후 **다음**을 누릅니다.
8. **마침**을 누릅니다.

Security Manager 사용자 콘솔에서도 스마트 카드를 등록할 수 있습니다. 자세한 내용은 스마트 카드 페이지 오른쪽 상단에 있는 파란색 **?** 아이콘을 클릭하여 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

### 스마트 카드 구성

컴퓨터에 스마트 카드 리더가 설치되거나 연결된 경우 스마트 카드 페이지에 두 개의 탭이 표시됩니다.

- **설정**—**스마트 카드 제거 시 컴퓨터 잠금** 확인란을 선택하여 스마트 카드 제거 시 컴퓨터가 자동으로 잠기도록 구성한 다음 **적용**을 클릭합니다.

**참고:** 컴퓨터는 Windows 에 로그인할 때 스마트 카드를 인증 정보로 사용할 경우에만 잠깁니다. Windows 에 로그인할 때 사용되지 않는 스마트 카드를 제거하면 컴퓨터가 잠기지 않습니다.

- **관리**—다음 옵션 중에서 선택합니다.
  - **스마트 카드 초기화**—HP ProtectTools 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 응용 프로그램에서 사용할 수 없습니다.

**참고:** 스마트 카드에서 지원하지 않는 기능이나 관련 미들웨어는 사용할 수 없습니다.

▲ **적용**을 누릅니다.

## 비접촉식 카드

비접촉식 카드는 컴퓨터 칩이 들어있는 작은 플라스틱 카드입니다. 제조업체의 관련 드라이버가 설치되었고 비접촉식 카드를 인증 정보로 선택한 경우 비접촉식 카드 리더를 컴퓨터에 연결하면 비접촉식 카드를 인증에 사용할 수 있습니다. HP ProtectTools 는 다음과 같은 유형의 비접촉식 카드를 지원합니다.

- 비접촉식 HID iCLASS 메모리 카드
- 비접촉식 MiFare Classic 1k, 4k 및 미니 메모리 카드

▲ 비접촉식 카드를 설정하려면 비접촉식 카드를 리더에 매우 가까이 대고 화면의 지시를 따른 다음 **적용**을 누릅니다.

## 근접 카드

근접 카드는 컴퓨터 칩이 들어있는 작은 플라스틱 카드입니다. 제조업체의 관련 드라이버가 설치되었고 근접 카드를 인증 정보로 선택한 경우 근접 카드 리더를 컴퓨터에 연결하면 추가 보안을 위해 다른 인증 정보와 연계해서 근접 카드를 사용할 수 있습니다.

▲ 근접 카드를 설정하려면 근접 카드를 리더에 매우 가까이 댄 다음 **적용**을 누릅니다.

## Bluetooth

Bluetooth 를 인증 정보로® 선택하고 Bluetooth 전화가 컴퓨터에 연결된 경우 컴퓨터에 Bluetooth 기능이 있으면 추가 보안을 위해 다른 인증 정보와 연계하여 Bluetooth 전화를 사용할 수 있습니다. Bluetooth 설정을 다음과 같이 지정하십시오.

▲ 자동 인증을 허용하려면 확인란을 선택한 다음 **적용**을 누릅니다.

### PIN

PIN 을 인증 정보로 선택한 경우 추가 보안을 위해 PIN 을 다른 인증 정보와 연계해서 사용할 수 있습니다. PIN 설정을 다음과 같이 지정하십시오.

1. 위쪽 또는 아래쪽 화살표를 눌러 최소 PIN 길이를 선택합니다.

   최대 8 자리까지 입력할 수 있습니다.

2. **적용**을 누릅니다.

# 응용프로그램

관리 콘솔의 왼쪽 패널에서 응용프로그램 아래 설정 페이지에는 최근에 설치된 HP ProtectTools Security Manager 응용프로그램을 사용자 정의할 수 있는 두 개의 탭이 포함되어 있습니다.

▲ 관리 콘솔의 왼쪽 패널에서 **응용프로그램** 아래 **설정**을 누릅니다.

## 일반 탭

**일반** 탭에서 다음 설정을 사용할 수 있습니다.

- **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.

1. 특정 설정을 활성화하려면 해당 설정 옆의 확인란을 선택하고 비활성화하려면 확인란을 선택 해제합니다.
2. **적용**을 누릅니다.

## 응용프로그램 탭

관리자는 다음 응용프로그램을 활성화 또는 비활성화할 수 있습니다.

- **상태**—모든 응용 프로그램을 활성화하려면 확인란을 선택하고 비활성화하려면 확인란을 선택 해제합니다.
- **Password Manager**—컴퓨터의 모든 사용자에 대해 Password Manager 를 활성화합니다.

1. 특정 설정을 활성화하려면 해당 설정 옆의 확인란을 선택하고 비활성화하려면 확인란을 선택 해제합니다.
2. **적용**을 누릅니다.

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

# 데이터

관리 콘솔 왼쪽 패널의 데이터 섹션에서는 다음 응용 프로그램에 대한 설정을 구성할 수 있습니다.

- **Drive Encryption**—설정을 구성하고 드라이브 상태를 표시합니다. 자세한 내용은 Drive Encryption 페이지 오른쪽 상단에 있는 파란색 **?** 아이콘을 클릭하여 Drive Encryption 소프트웨어 도움말을 참조하십시오.

# 컴퓨터

관리 콘솔 왼쪽 패널의 컴퓨터 섹션에서는 Device Access Manager 응용프로그램에 대한 설정을 구성할 수 있습니다.

- 단순 구성
- 장치 클래스 구성
- Just-in-Time-인증(JITA) 구성
- 고급 설정

자세한 내용은 Device Access Manager 페이지 오른쪽 상단에 있는 파란색 **?** 아이콘을 눌러 Device Access Manager 소프트웨어 도움말을 참조하십시오.

# 5 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.
- 쉽게 Windows® 운영 체제 암호를 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 방법 중 하나로 Security Manager 를 열 수 있습니다.

▲ Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭합니다.

– 또는 –

**제어판**에서 **시스템 및 보안**을 선택한 다음 **HP ProtectTools Security Manager** 를 선택합니다.

## Security Manager 사용자 콘솔 사용

Security Manager 사용자 콘솔은 Security Manager 기능, 응용 프로그램, 설정 등에 쉽게 액세스할 수 있는 중앙 위치입니다. 사용자 콘솔에는 다음 구성 요소가 표시됩니다.

- **ID 카드**—로그온한 사용자 계정을 식별하기 위한 Windows 사용자 이름과 아이콘을 표시합니다.
- **보안 응용 프로그램**—다음 보안 범주를 구성하기 위한 링크의 확장 메뉴를 표시합니다.
  - **홈**—암호를 관리하거나 인증 정보를 설정하거나 보안 응용 프로그램의 상태를 확인합니다.
  - **도난 회수**—Computrace for HP ProtectTools(별도 구매)
- **내 로그온**—Password Manager 및 Credential Manager 를 사용하여 사용자 인증 정보를 관리합니다.
- **내 데이터**—Drive Encryption 을 사용하여 데이터의 보안을 관리합니다.

**참고:** 응용 프로그램이 설치되지 않은 경우 이 항목이 표시되지 않습니다.

- **내 컴퓨터**—Device Access Manager 를 사용하여 컴퓨터의 보안을 관리합니다.

**참고:** 응용 프로그램이 설치되지 않은 경우 이 항목이 표시되지 않습니다.

- **관리**—관리자가 **관리 콘솔**에 액세스하여 보안 및 사용자를 관리할 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**—응용 프로그램별 화면을 표시합니다.
- **?**—Security Manager 사용자 콘솔 도움말을 표시합니다. 이 아이콘은 창 프레임 오른쪽 상단 최소화/최대화 아이콘 옆에 있습니다.

# 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.

이름이 표시되는 방식을 변경할 수 있습니다. 기본적으로 Windows 설치 중 선택한 전체 Windows 사용자 이름과 사진이 표시됩니다.

표시된 이름을 변경하려면:

1. Security Manager 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.
2. 사용자 콘솔의 왼쪽 상단에 있는 ID 카드를 클릭합니다.
3. 이 계정에 대한 Windows 사용자 이름이 표시된 상자를 누르고 새 이름을 입력한 다음 **저장**을 누릅니다.

# 내 로그온

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

- **Password Manager**—Windows 암호, 지문, 얼굴, 스마트 카드, 근접 카드, 비접촉식 카드, Bluetooth 전화 또는 PIN 으로 인증하여 웹 사이트와 프로그램을 실행하고 로그온할 수 있는 빠른 링크를 생성 및 관리합니다.
- **Credential Manager**—편리하게 Windows 암호를 변경하거나 지문 또는 얼굴을 등록하거나 스마트 카드, 비접촉식 카드, 근접 카드, Bluetooth 전화 또는 PIN 을 설정할 수 있습니다.

관리자는 **관리**를 누른 후 대시보드 왼쪽 하단에 있는 **중앙 관리**를 클릭하여 사용 가능한 추가 보안 응용프로그램에 관한 정보에 액세스할 수 있습니다.

## Password Manager

Windows, 웹 사이트 및 응용 프로그램에 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, 얼굴, 스마트 카드, 근접 카드, 비접촉식 카드, PIN 또는 Windows 암호로 쉽고 빠르게 로그온할 수 있습니다.

Password Manager 는 다음과 같은 옵션을 제공합니다.

### 탭 관리

- 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 파악

### 암호 강도 탭

- 웹 사이트 및 응용프로그램에 사용할 개인 암호의 강도와 전체적인 암호 강도를 확인
- 암호 강도는 빨간색, 노란색 또는 녹색 상태 표시기로 표시

**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.

- Password Manager 에 [somedomain.com] 추가하기
- Password Manager 열기
- 아이콘 설정
- 도움말

## 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 도움말을 표시합니다.

## 로그온이 이미 생성된 웹 페이지나 프로그램의 경우

다음 옵션이 컨텍스트 메뉴에 표시됩니다.

- **로그온 데이터 입력**—신원 확인 페이지를 표시합니다. 성공적으로 인증된 경우 로그온 필드에 로그온 데이터가 자동으로 입력되고 페이지가 제출됩니다(로그온이 생성되거나 최근에 편집되었을 때 제출 작업이 지정된 경우).
- **로그온 편집**—이 웹 사이트에 대한 로그온 데이터를 편집할 수 있습니다.
- **로그온 추가**—Password Manager 에 계정을 추가할 수 있습니다.
- **Password Manager 열기**—Password Manager 를 실행합니다.
- **도움말**—Security Manager 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 **Password Manager 빠른 링크** 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. Ctrl+Windows 로고 키+h 핫키를 사용하거나 손가락을 문질러 **Password Manager 관리** 탭에서 **로그온 추가**를 눌러 이 대화 상자를 표시할 수도 있습니다.
   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. **확인**을 누르고 사용할 인증 방법(지문, 얼굴, 스마트 카드, 근접 카드, 비접촉식 카드, Bluetooth 전화, PIN 또는 암호)을 선택한 후 선택한 인증 방법으로 로그온합니다.

      **Password Manager** 아이콘에서 더하기(+) 기호가 제거되면 로그온이 생성된 것입니다.
   e. Password Manager 가 로그온 필드를 검색하지 못하면 **추가 필드**를 누릅니다.
      - 로그온에 필요한 각 필드의 확인란을 선택하거나, 로그온에 필요하지 않은 필드의 확인란을 선택 해제합니다.
      - **닫기**를 누릅니다.

해당 웹 사이트에 액세스하거나 해당 프로그램을 열 때마다 웹 사이트 또는 응용프로그램 로그온 화면 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 필드에는 굵은 주황색 테두리가 표시됩니다.

   **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.
   - 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.

## Password Manager 빠른 링크 메뉴 사용

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

로그온이 생성되면 Password Manager **빠른 링크** 메뉴에 자동으로 추가됩니다.

**빠른 링크** 메뉴를 표시하려면:

1. **Password Manager** 핫키 조합(ctrl+Windows 로고 키+h 로 기본 설정되어 있음)을 누릅니다. 핫키 조합을 변경하려면 Security Manager 사용자 콘솔에서 **Password Manager** 를 두 번 클릭한 다음 **설정**을 클릭합니다.
2. 컴퓨터에 내장되거나 연결된 지문 인식기를 사용하여 지문을 스캔하거나 Windows 암호를 입력합니다.

## 로그온을 범주로 구성

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

범주를 추가하려면:

1. Security Manager 사용자 콘솔에서 **Password Manager** 를 클릭합니다.
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 다중 로그온이 생성된 경우 각 로그온이 웹 사이트 이름 아래에 나열되고 로그온 목록에서 들여쓰기됩니다.

로그온을 관리하려면:

▲ Security Manager 사용자 콘솔에서 **Password Manager** 를 클릭하고 **관리** 탭을 클릭합니다.

- **로그온 추가**—**로그온 추가**를 클릭하고 화면의 지시를 따릅니다.
- **사용자의 로그온**—기존 로그온을 클릭하고 다음 옵션 중 하나를 선택한 후 화면의 지시를 따릅니다.
  - **열기**—기존 로그온이 있는 웹 사이트 또는 프로그램을 엽니다.
  - **추가**—로그온을 추가합니다. 자세한 내용은 27페이지의로그온 추가를 참조하십시오.
  - **편집**—로그온을 편집합니다. 자세한 내용은 27페이지의로그온 편집를 참조하십시오.
  - **삭제**—기존 로그온이 있는 웹 사이트 또는 프로그램을 삭제합니다.
- **범주 추가**—**범주 추가**를 클릭하고 화면의 지시를 따릅니다. 자세한 내용은 28페이지의로그온을 범주로 구성를 참조하십시오.

웹 사이트나 프로그램에 대한 로그인을 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.

**암호 강도** 탭에서 빨간색, 노란색 또는 녹색 상태 표시기는 웹 사이트 및 응용프로그램에 사용할 개인 암호의 강도와 전체적인 암호 강도를 나타냅니다.

## 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. 아이콘을 클릭한 다음 **아이콘 설정**을 클릭하여 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 클릭합니다.
   - **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 사용자 콘솔을 열고 **Password Manager** 를 클릭합니다.
- **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 27페이지의로그온 추가를 참조하십시오.
- 이 웹 사이트 로그온 또는 프로그램 화면을 열 때마다 **Password Manager** 아이콘이 표시됩니다.

**로그온 화면에 로그온을 추가하라는 메시지를 표시 안 함**—라디오 버튼을 선택합니다.

2. 추가 Password Manager 설정에 액세스하려면 Security Manager 사용자 콘솔에서 **Password Manager** 를 두 번 클릭하고 **설정**을 클릭합니다.

### 설정

Password Manager 의 개인 설정을 다음과 같이 지정할 수 있습니다.

1. **로그온 화면에 로그온을 추가하라는 메시지 표시**—웹 사이트나 프로그램 로그온 화면이 감지될 때마다 **Password Manager** 아이콘에 더하기(+) 기호가 표시되어 이 화면의 로그온을 **로그온** 메뉴에 추가할 수 있음을 나타냅니다. 이 기능을 비활성화하려면 **로그온 화면에 로그온을 추가하라는 메시지 표시** 옆에 있는 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. 바로 가기 키를 변경하려면 이 옵션을 클릭하고 새로운 키 조합을 입력합니다. 바로 가기 키 조합에는 ctrl, alt 또는 shift 및 임의의 알파벳 또는 숫자 키 중 하나 이상이 포함될 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
- 얼굴
- 스마트 카드
- 비접촉식 카드
- 근접 카드

- Bluetooth
- PIN

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 사용자 콘솔에서 **Credential Manager** 를 클릭한 다음 **암호**를 클릭합니다.
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.

HP ProtectTools Security Manager 설치 마법사의 초기 설정 과정 중에 HP ProtectTools Security Manager 가 개인 SpareKey 를 설정하라는 메시지를 표시합니다.

SpareKey 를 설정하려면:

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

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

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

## 지문 등록

관리자가 **인증 정보 선택** 화면에서 지문을 선택하고 지문 인식기가 컴퓨터에 내장되었거나 연결된 경우 HP ProtectTools Security Manager 설치 마법사가 지문을 설정하거나 "등록"하는 단계를 안내합니다. Security Manager 대시보드의 **Credential Manager** 에 있는 지문 페이지에서 지문을 등록할 수도 있습니다.

1. 마법사의 지문 페이지에 양손의 윤곽선이 표시됩니다. 이미 등록된 손가락은 강조 표시됩니다. 윤곽선 위에 손가락을 대고 누릅니다.

   **참고:** 이전에 등록한 지문을 삭제하려면 해당 손가락으로 누르십시오.

2. 지문이 성공적으로 등록될 때까지 해당 손가락을 문지르라는 메시지가 나타납니다. 등록된 손가락은 윤곽선에 강조 표시됩니다.
3. 적어도 두 손가락, 가능하면 검지와 중지를 등록해야 합니다. 다른 손가락에 대해 1~2 단계를 반복합니다.
4. **다음**을 클릭한 후 화면의 지시를 따릅니다.

⚠ **주의:** 마법사를 통해 지문을 등록하는 경우 **다음**을 누를 때까지 지문 정보가 저장되지 않습니다. 컴퓨터를 한동안 사용하지 않은 상태로 두거나 프로그램을 닫으면 변경한 내용이 저장되지 **않습니다**.

## 얼굴 로그온에 사용할 사진 그룹 등록

얼굴 로그온을 선택한 경우 웹캠이 컴퓨터에 내장되어 있거나 연결되어 있으면, Security Manager 설치 마법사는 장면을 등록하라는 메시지를 표시합니다. Security Manager 사용자 콘솔에서 **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.

HP ProtectTools Security Manager 설치 마법사를 사용하여 새로운 장면을 등록하려면 다음과 같이 하십시오.

1. 마법사의 얼굴 로그온 페이지에서 **고급**을 누른 다음 추가 옵션을 구성합니다. 자세한 내용은 33페이지의고급 사용자 설정을 참조하십시오.
2. **확인**을 누릅니다.
3. **시작**을 누르거나, 이전에 등록한 사진 그룹이 있는 경우 **새 사진 그룹 등록**을 누릅니다.
4. 장면을 등록하는 동안 **비디오 재생**을 클릭하여 데모를 볼 수 있습니다.

   처음 등록하는 경우 데모 비디오를 볼 것인지 묻는 대화 상자가 나타납니다. **예** 또는 **아니요**를 누릅니다.
5. 어두운 조명에서 소프트웨어는 화면을 자동으로 밝게 해주며, 배경 조명을 변경하려면 **전구** 아이콘을 누릅니다.
6. **카메라** 아이콘을 누른 후 화면의 지시에 따라 사진 그룹을 등록합니다.

   **참고:** 장면을 캡처하는 동안 얼굴을 이미지 방향으로 돌려 이미지를 확인하십시오.
7. **다음**을 누릅니다.

다음과 같은 방법으로도 Security Manager 사용자 콘솔에서 사진 그룹을 등록할 수 있습니다.

1. Security Manager 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.
2. **내 로그온**에서 **Credential Manager** 를 누른 다음 **얼굴**을 누릅니다.
3. **고급**을 눌러 추가 옵션을 구성합니다. 자세한 내용은 33페이지의고급 사용자 설정를 참조하십시오.
4. **확인**을 누릅니다.
5. **시작**을 누르거나, 이전에 등록한 사진 그룹이 있는 경우 **새 사진 그룹 등록**을 누릅니다.
6. Windows 암호를 입력하라는 메시지가 나타나면 암호를 입력하고 **다음**을 누릅니다.
7. 장면을 등록하는 동안 **비디오 재생**을 클릭하여 데모를 볼 수 있습니다.

   처음 등록하는 경우 데모 비디오를 볼 것인지 묻는 대화 상자가 나타납니다. **예** 또는 **아니요**를 누릅니다.

8. 어두운 조명에서 소프트웨어는 화면을 자동으로 밝게 해주며, 배경 조명을 변경하려면 **전구** 아이콘을 누릅니다.

9. **카메라** 아이콘을 누른 후 화면의 지시에 따라 사진 그룹을 등록합니다.

**참고:** 장면을 캡처하는 동안 얼굴을 이미지 방향으로 돌려 이미지를 확인하십시오.

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

### 인증

하나 이상의 장면을 등록한 후에는 사용자의 얼굴로 인증을 거쳐 컴퓨터에 로그온하거나 새 Windows 세션을 시작할 수 있습니다.

1. 인증 화면이 나타나고 카메라가 사용자의 얼굴을 감지하면 로그온 프로세스가 시작됩니다. 이때 로그온 프로세스는 5 초 안에 완료되어야 합니다. 성공적으로 얼굴이 인증된 경우 컴퓨터에 액세스할 수 있습니다.

2. 제한 시간이 지날 경우 Face Recognition 이 일시 중지됩니다. **카메라** 아이콘을 눌러 인증 절차를 다시 시작합니다.

**참고:** 조명이 충분하지 않아 Face Recognition 을 사용하여 로그온할 수 없다면 Windows 암호를 입력하여 컴퓨터에 로그온할 수 있습니다.

3. 컴퓨터에 로그온한 후, Face Recognition 로그온 기능을 더욱 강화하기 위해 추가로 사진을 등록하라는 메시지가 나타날 경우 **예**를 누릅니다.

### 야간 모드

너무 어두운 곳에서 얼굴 인식 로그온을 시도하는 경우 얼굴이 좀 더 환해질 수 있도록 얼굴 인식 로그온 화면 배경 색이 자동으로 흰색으로 전환됩니다.

얼굴 인식 로그온 화면 배경 색을 수동으로 전환하려면 **전구** 아이콘을 누릅니다.

### 학습

암호를 정확히 입력했는데도 얼굴 인식을 통해 컴퓨터에 로그온할 수 없는 경우, 향후 얼굴 인식 로그온의 성공률을 높이기 위해 일련의 이미지를 저장할 것을 묻는 메시지가 나타납니다.

### 장면 삭제

현재 등록된 장면을 삭제하려면 다음과 같이 하십시오.

1. Security Manager 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.

2. **내 로그온**에서 **Credential Manager** 를 누르고 **얼굴**을 누릅니다.

3. 삭제하려는 장면을 누른 후 **휴지통** 아이콘을 누릅니다.

4. 확인 대화 상자가 표시되면 **확인**을 누릅니다.

### 고급 사용자 설정

1. Security Manager 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.

2. **내 로그온**에서 **Credential Manager** 를 누른 다음 **얼굴**을 누릅니다.

3. **고급**을 눌러 다음 옵션을 구성합니다.

   **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 입력한 경우 향후 얼굴 인식 로그온의 성공률을 높이기 위해 캡처된 일련의 이미지를 저장하라는 메시지가 나타납니다.
   - **로그온 실패 시 새 얼굴 사진 등록**—얼굴 로그온에 실패했지만 암호를 정확히 입력한 경우 향후 얼굴 인식 로그온의 성공률을 높이기 위해 새 얼굴 사진을 등록하라는 메시지가 나타납니다.

4. 원래 값으로 설정을 되돌리려면 **기본값 복원**을 누릅니다.
5. **확인**을 누릅니다.

## 스마트 카드 설정

관리자가 스마트 카드를 인증 정보로 활성화하고 HP ProtectTools 관리 콘솔 소프트웨어 도움말에 나와 있는 단계를 수행했을 경우 스마트 카드 리더가 컴퓨터에 내장되었거나 연결되면 HP ProtectTools Security Manager 설치 마법사에서 스마트 카드를 삽입하고 설정하라는 메시지가 표시됩니다. Security Manager 사용자 콘솔의 **Credential Manager** 아래에 있는 스마트 카드 페이지에서 스마트 카드를 설정할 수도 있습니다.

**참고:** 사용할 스마트 카드는 관리자가 먼저 초기화해야 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 PIN 관리를 설치할 도구를 제공해야 합니다.

관리자는 제조업체 소프트웨어 및 HP ProtectTools 관리 콘솔을 사용하여 스마트 카드를 초기화할 수 있습니다. 자세한 내용은 HP ProtectTools 관리 콘솔 소프트웨어 도움말을 참조하십시오.

### 스마트 카드 등록

스마트 카드를 초기화한 후 사용자는 다음과 같이 스마트 카드를 Security Manager 에 등록할 수 있습니다.

1. Security Manager 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.
2. **Credential Manager** 와 **스마트 카드**를 차례로 누릅니다.
3. **설정**을 선택합니다.
4. Windows 암호와 PIN 을 입력한 후 **저장**을 누릅니다.

또한 관리자는 HP ProtectTools 관리 콘솔에서 스마트 카드를 등록할 수도 있습니다. 자세한 내용은 HP ProtectTools 관리 콘솔 소프트웨어 도움말을 참조하십시오.

### 스마트 카드 PIN 변경

스마트 카드 PIN 을 변경하려면:

1. 이전에 포맷되고 초기화된 스마트 카드를 넣습니다.
2. **스마트 카드 PIN 변경**을 선택합니다.
3. 이전 PIN 을 입력한 후 새 PIN 을 입력하고 확인합니다.

## 비접촉식 카드

비접촉식 카드는 컴퓨터 칩이 들어있는 작은 플라스틱 카드입니다. 관리자가 제조업체의 관련 드라이버를 설치하고 비접촉식 카드를 인증 정보로 활성화할 경우 비접촉식 카드 리더를 컴퓨터에 연결하면 비접촉식 카드를 인증 정보로 사용할 수 있습니다. HP ProtectTools 는 다음과 같은 유형의 비접촉식 카드를 지원합니다.

- 비접촉식 HID iCLASS 메모리 카드
- 비접촉식 MiFare Classic 1k, 4k 및 미니 메모리 카드

▲ 비접촉식 카드를 설정하려면 비접촉식 카드를 리더에 매우 가까이 대고 화면의 지시를 따른 다음 **적용**을 누릅니다.

## 근접 카드

근접 카드는 컴퓨터 칩이 들어있는 작은 플라스틱 카드입니다. 관리자가 제조업체에서 관련 드라이버를 설치하고 근접 카드를 인증 정보로 선택한 경우 근접 카드 리더를 컴퓨터에 연결하면 추가 보안을 위해 다른 인증 정보와 연계해서 근접 카드를 사용할 수 있습니다.

▲ 근접 카드를 설정하려면 비접촉식 카드를 리더에 매우 가까이 대고 화면의 지시를 따른 다음 **적용**을 누릅니다.

## Bluetooth

관리자가 Bluetooth 를 인증 정보로 선택한 경우 추가 보안을 위해 Bluetooth 전화를 다른 인증 정보와 연계해서 설정할 수 있습니다.

**참고:** Bluetooth 전화 장치만 지원됩니다.

1. 컴퓨터에 Bluetooth 기능이 활성화되어 있는지와 Bluetooth 전화가 검색 모드로 설정되어 있는지 확인하십시오. 전화를 연결하려면 Bluetooth 장치에 있는 자동 생성 코드를 입력해야 합니다. Bluetooth 장치 구성 설정에 따라 컴퓨터와 전화 간의 연결 코드를 비교해야 할 수 있습니다.
2. 등록할 전화기를 선택한 다음 **등록**을 누릅니다.
3. 확인 대화 상자가 표시되면 **확인**을 누릅니다.

## PIN

관리자가 PIN 을 인증 정보로 선택한 경우 추가 보안을 위해 PIN 을 다른 인증 정보와 연계해서 설정할 수 있습니다.

▲ 새 PIN 을 설정하려면 PIN 을 입력한 후 한 번 더 입력하여 확인합니다.

## 관리

관리자는 **관리**를 클릭하고 HP ProtectTools Security Manager 사용자 콘솔의 왼쪽 하단 패널에 있는 **관리 콘솔**을 선택하여 관리 콘솔 및 중앙 관리에 액세스할 수 있습니다.

자세한 내용은 HP ProtectTools 관리 콘솔 소프트웨어 도움말을 참조하십시오.

## 고급

사용자 콘솔의 왼쪽 하단 패널에서 **고급**을 클릭하여 다음 옵션에 액세스할 수 있습니다.

- **기본 설정**—Security Manager 에 대한 설정을 개별화할 수 있습니다.
- **백업 및 복원**—Security Manager 데이터를 백업하고 복원할 수 있습니다.
- **정보**—Security Manager 에 대한 버전 정보를 표시합니다.

## 기본 설정 구성

HP ProtectTools Security Manager 에 대한 개인 설정을 지정할 수 있습니다. Security Manager 사용자 콘솔에서 **고급**을 클릭하고 **기본 설정**을 클릭합니다. 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 설정에 있는 **사운드** 탭에서 이러한 이벤트에 새 사운드를 지정하거나 이 옵션을 선택 해제하여 사운드 피드백을 비활성화할 수 있습니다.
  - **스캔 품질 피드백 표시**

    품질에 관계 없이 모든 스캔을 표시하려면 확인란을 선택합니다.

    품질이 좋은 스캔만 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 Password Manager 와 Face Recognition 정보만 백업됩니다. Drive Encryption 에는 독립형 백업 방법이 있습니다. Device Access Manager 및 지문 인증 정보는 백업되지 않습니다.

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

데이터를 백업하려면:

1. Security Manager 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.
2. 사용자 콘솔의 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 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.
2. 사용자 콘솔의 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.

# 6 Drive Encryption for HP ProtectTools(일부 모델만 해당)

Drive Encryption for HP ProtectTools 는 컴퓨터의 데이터를 암호화함으로써 데이터를 완벽하게 보호합니다. Drive Encryption 이 활성화되어 있는 경우 Windows® 운영 체제가 시작되기 전에 표시되는 Drive Encryption 로그인 화면에서 로그온해야 합니다. Windows® 운영 체제가 시작됩니다.

Windows 관리자는 HP ProtectTools Security Manager(HP Client Security 설치 마법사, 고급 설치 마법사 또는 관리 콘손)를 사용하여 Drive Encryption 활성화, 암호화 키 백업, 암호화를 위한 드라이브 또는 파티션 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 보호 암호 활성화
  - 소프트웨어 암호화를 사용하여 개별 드라이브 또는 파티션을 암호화 또는 암호화 해제
  - 하드웨어 암호화를 사용하여 개별 자가 암호화 드라이브를 암호화 또는 암호화 해제
  - Drive Encryption 사전 부팅 인증이 항상 필요하도록 절전 모드 또는 대기 모드를 비활성화하여 보안 추가

**참고:** 암호화할 수 있는 대상은 내부 SATA 및 외부 eSATA 하드 드라이브로 한정됩니다.

- 백업 키 만들기
- 백업 키 및 HP SpareKey 를 사용하여 암호화된 컴퓨터에 대한 액세스 복구
- 암호, 등록된 지문 또는 스마트 카드 PIN 을 사용하여 Drive Encryption 부팅 전 인증 활성화

## Drive Encryption 열기

관리자는 HP ProtectTools Security Manager 사용자 콘솔을 열고 Drive Encryption 에 액세스할 수 있습니다.

1. Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭합니다.

   – 또는 –

   **제어판**에서 **시스템 및 보안**을 선택한 다음 **HP ProtectTools Security Manager** 를 선택합니다.
2. HP ProtectTools Security Manager 사용자 콘솔의 왼쪽 패널에서 **관리**를 선택한 다음 **관리 콘솔**을 선택합니다.
3. HP ProtectTools 관리 콘솔의 왼쪽 패널에서 **Drive Encryption** 을 선택합니다.

# 일반 작업

## 표준 하드 드라이브에 대한 Drive Encryption 활성화

표준 하드 드라이브는 소프트웨어 암호화를 통해 암호화됩니다. Drive Encryption 을 활성화하려면 다음과 같이 하십시오.

1. **HP ProtectTools 관리 콘솔**을 실행합니다. 자세한 내용은 16페이지의 HP ProtectTools 관리 콘솔 열기를 참조하십시오.
2. 왼쪽 패널에서 **설치 마법사**를 클릭합니다.
3. **Drive Encryption** 확인란을 선택한 후 **다음**을 누릅니다.
4. 암호화 키를 백업하려면 이 키를 기록하기 위한 외부 저장 장치를 연결합니다. 이 키는 다른 방법이 실패한 경우 데이터에 액세스하는 데 사용해야 합니다.
5. **Back up Drive Encryption keys**(Drive Encryption 키 백업) 아래에서 암호화 키를 저장할 저장 장치의 확인란을 선택합니다.
6. **다음**을 누릅니다.

**참고:** 컴퓨터를 다시 시작하라는 메시지가 나타납니다. 다시 시작 후에 Windows 를 시작하기 전 인증을 요구하는 Drive Encryption 사전 부팅 화면이 표시됩니다.

Drive Encryption 이 활성화됩니다. 선택된 드라이브 파티션 암호화는 파티션의 개수 및 크기에 따라 몇 시간이 걸릴 수도 있습니다.

자세한 내용은 HP ProtectTools Security Manager 소프트웨어 도움말을 참조하십시오.

## 자가 암호화 드라이브에 대한 Drive Encryption 활성화

자가 암호화 드라이브 관리를 위한 Trusted Computing Group 의 OPAL 사양을 충족하는 자가 암호화 드라이브는 소프트웨어 암호화 또는 하드웨어 암호화를 사용하여 암호화할 수 있습니다. 자가 암호화 드라이브에 대한 Drive Encryption 을 활성화하려면 다음과 같이 하십시오.

**참고:** 하드웨어 암호화는 컴퓨터에 있는 모든 드라이브가 자체 암호화 드라이브 관리에 대한 TCG(Trusted Computing Group)의 OPAL 규격을 충족하는 자체 암호화 드라이브일 경우에만 사용할 수 있습니다. 이러한 경우 **하드웨어 드라이브 암호화 사용** 옵션을 사용할 수 있으며 하드웨어 또는 소프트웨어 암호화를 사용할 수 있습니다.

자체 암호화 드라이브와 표준 하드 드라이브가 혼합된 경우 **하드웨어 드라이브 암호화 사용** 옵션을 사용할 수 없으며 소프트웨어 암호화만 사용할 수 있습니다. 자세한 내용은 39페이지의표준 하드 드라이브에 대한 Drive Encryption 활성화를 참조하십시오.

▲ HP ProtectTools Security Manager 설치 마법사를 사용하여 Drive Encryption 을 활성화합니다.

– 또는 –

### 소프트웨어 암호화

1. **HP ProtectTools 관리 콘솔**을 실행합니다. 자세한 내용은 16페이지의 HP ProtectTools 관리 콘솔 열기를 참조하십시오.
2. 왼쪽 패널에서 **설치 마법사**를 클릭합니다.
3. **Drive Encryption** 확인란을 선택한 후 **다음**을 누릅니다.

**참고:** 화면 아래쪽에 **하드웨어 드라이브 암호화 사용** 옵션이 사용 가능한 경우 확인란을 선택 해제합니다.

4. **암호화할 드라이브** 아래에서 암호화하려는 하드 드라이브의 확인란을 선택한 후 **다음**을 누릅니다.
5. 암호화 키를 백업하려면 해당 슬롯에 저장 장치를 넣습니다.
6. **Back up Drive Encryption keys**(Drive Encryption 키 백업) 아래에서 암호화 키를 저장할 저장 장치의 확인란을 선택합니다.
7. **적용**을 누릅니다.

**참고:** 컴퓨터가 다시 시작됩니다.

Drive Encryption 이 활성화되었습니다. 드라이브의 크기에 따라 드라이브를 암호화하는 데 시간이 오래 걸릴 수 있습니다.

### 하드웨어 암호화

1. **HP ProtectTools 관리 콘솔**을 실행합니다. 자세한 내용은 16페이지의 HP ProtectTools 관리 콘솔 열기를 참조하십시오.
2. 왼쪽 패널에서 **설치 마법사**를 클릭합니다.
3. **Drive Encryption** 확인란을 선택한 다음 **다음**을 누릅니다.
4. 화면 아래쪽에 **하드웨어 드라이브 암호화 사용** 확인란이 사용 가능한 경우 확인란이 선택되었는지 확인합니다.

   확인란이 선택 해제되거나 사용할 수 없을 경우 소프트웨어 암호화가 적용됩니다. 자세한 내용은 39페이지의표준 하드 드라이브에 대한 Drive Encryption 활성화를 참조하십시오.
5. **암호화할 드라이브** 아래에서 암호화하려는 하드 드라이브의 확인란을 선택한 후 **다음**을 누릅니다.

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

두 개 이상의 드라이브만 표시될 경우 디스크 0 이 자동 선택되고 비활성화되지만 하드웨어 암호화에 대한 더 많은 하드 드라이브를 선택하는 옵션을 사용할 수 있습니다.

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

6. 암호화 키를 백업하려면 해당 슬롯에 저장 장치를 넣습니다.
7. **Back up Drive Encryption keys**(Drive Encryption 키 백업) 아래에서 암호화 키를 저장할 저장 장치의 확인란을 선택합니다.
8. **적용**을 누릅니다.

**참고:** 컴퓨터를 다시 시작하라는 메시지가 나타납니다. Windows 를 시작하기 전 인증을 요구하는 Drive Encryption 사전 부팅이 표시됩니다.

Drive Encryption 이 활성화되었습니다. 드라이브를 암호화하는 데 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.

1. **HP ProtectTools 관리 콘솔**을 실행합니다. 자세한 내용은 16페이지의 HP ProtectTools 관리 콘솔 열기를 참조하십시오.
2. 왼쪽 패널에서 **설치 마법사**를 클릭합니다.
3. **Drive Encryption** 확인란을 선택 해제한 후 **다음**을 누릅니다.

   Drive Encryption 비활성화가 시작됩니다.

**참고:** 소프트웨어 암호화를 사용한 경우 암호 해제가 시작됩니다. 암호화된 하드 드라이브 파티션의 크기에 따라 몇 시간이 걸릴 수도 있습니다. 암호 해제가 완료되면 Drive Encryption 이 비활성화됩니다.

하드웨어 암호화를 사용한 경우 드라이브의 암호가 즉시 해제되며 몇 분 후에 Drive Encryption 이 비활성화됩니다.

Drive Encryption 이 비활성화되면 하드웨어가 암호화될 경우 컴퓨터를 종료하라는 메시지가 나타나고 소프트웨어가 암호화될 경우 컴퓨터를 다시 시작하라는 메시지가 나타납니다.

## Drive Encryption 이 활성화된 후 로그인

Drive Encryption 을 활성화하고 사용자 계정을 등록한 이후 컴퓨터를 켜는 경우에는 Drive Encryption 로그인 화면에서 로그온해야 합니다.

**참고:** 소프트웨어 암호화 또는 하드웨어 암호화가 활성화되어 있는 상태에서 절전 또는 대기 모드가 해제되면 Drive Encryption 사전 부팅 인증이 표시되지 않습니다. 하드웨어 암호화는 절전 또는 대기 모드가 활성화되는 것을 차단하는 **추가된 보안에 대해 절전 모드 비활성화** 옵션을 제공합니다.

소프트웨어 또는 하드웨어 암호화 모두 활성화되어 있는 상태에서 최대 절전 모드가 해제되면 Drive Encryption 사전 부팅 인증이 표시됩니다.

**참고:** Windows 관리자가 HP ProtectTools Security Manager 에 BIOS 사전 부팅 보안을 설정하고 One-Step Logon 이 기본값으로 활성화된 경우 Drive Encryption 로그인 화면에서 다시 인증할 필요 없이 BIOS 사전 부팅에서 인증한 직후 컴퓨터에 로그온할 수 있습니다.

### 단일 사용자 로그온:

- **로그온** 페이지에서 Windows 암호, 스마트 카드 PIN, SpareKey, 얼굴을 입력하거나 등록된 손가락을 인식시킵니다.

### 다중 사용자 로그온:

1. **로그온할 사용자 선택** 페이지의 드롭 다운 목록에서 로그온할 사용자를 선택하고 **다음**을 누릅니다.
2. **로그온** 페이지에서 Windows 암호 또는 스마트 카드 PIN 을 입력하거나 등록된 손가락을 인식시킵니다.

**참고:** 다음 스마트 카드가 지원됩니다.

### 지원되는 스마트 카드

- ActivIdentity Oberthur Cosmopol IC 64k V5.2
- Gemalto Cyberflex Access 64k V2c
- ActivIdentity Activkey SIM (Gemalto Cyberflex Access 64k V2c)

**참고:** Drive Encryption 로그인 화면에서 복구 키를 사용하여 로그온하면 Windows 로그온에서 추가 인증 정보로 사용자 계정에 액세스해야 합니다.

## 하드 드라이브를 암호화하여 데이터 보호

HP ProtectTools Security Manager 설치 마법사를 사용하여 하드 드라이브를 암호화하여 데이터를 보호하는 것이 좋습니다. 활성화 후에 다음 단계를 따라 추가된 모든 하드 드라이브나 만들어진 파티션을 암호화할 수 있습니다.

1. 왼쪽 패널에서 **Drive Encryption** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
2. **설정**을 누릅니다.
3. 소프트웨어 암호화를 사용한 드라이브의 경우 암호화할 드라이브 파티션을 선택합니다.

**참고:** 이는 표준 하드 드라이브와 자가 암호화 드라이브가 각각 하나 이상 있는 혼합 형식의 드라이브 시나리오에도 적용됩니다.

– 또는 –

▲ 하드웨어 암호화 드라이브의 경우 암호화할 추가 드라이브를 선택합니다.

# 고급 작업

## Drive Encryption 관리(관리자 작업)

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

**참고:** 추가 하드 드라이브만 Drive Encryption 설정 페이지에서 하드웨어 암호화를 선택/선택 해제할 수 있습니다.

- 상태가 비활성인 경우 Windows 관리자가 아직 Drive Encryption 을 활성화하지 않았고 하드 드라이브가 보호되고 있지 않은 것입니다. HP ProtectTools Security Manager 설치 마법사를 사용하여 Drive Encryption 을 활성화합니다.
- 상태가 활성화됨인 경우 Drive Encryption 이 활성화되어 있고 구성되어 있습니다. 드라이브는 다음 상태 중 하나에 해당합니다.

### 소프트웨어 암호화

- 암호화되지 않음
- 암호화됨
- 암호화 중
- 암호 해독 중

하드웨어 암호화

- 암호화됨
- 암호화되지 않음(추가 드라이브에 해당)

## TPM 을 사용하여 보안 강화 사용(일부 모델만 해당)

TPM(Trusted Platform Module)이 활성화되고 Drive Encryption Enhanced Security with TPM(TPM 을 사용하여 보안 강화) 기능이 선택된 경우, Drive Encryption 암호는 TPM 보안 칩으로 보호됩니다. 하드 드라이브가 제거되고 다른 컴퓨터에 설치될 경우 드라이브에 대한 액세스가 거부됩니다.

**주의:** TPM 소유권은 Windows TPM.msc 와 공유할 수 없습니다.

**참고:** 암호는 TPM 보안 칩으로 보호되므로 하드 드라이브를 다른 컴퓨터로 옮긴 경우 TPM 설정을 옮긴 컴퓨터로 마이그레이션해야 데이터에 액세스할 수 있습니다.

**참고:** BIOS 설정에서 TPM 옵션이 활성화되어 있어야 합니다.

## 개별 드라이브 파티션의 암호화 또는 암호 해제(소프트웨어 암호화만 해당)

관리자는 Drive Encryption 설정 페이지를 사용하여 컴퓨터에 하나 이상의 하드 드라이브 파티션을 암호화하거나 이미 암호화된 드라이브 파티션의 암호를 해제할 수 있습니다.

1. **HP ProtectTools 관리 콘솔**을 실행합니다. 자세한 내용은 16페이지의 HP ProtectTools 관리 콘솔 열기를 참조하십시오.
2. 왼쪽 패널에서 **Drive Encryption** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **설정**을 누릅니다.
4. **드라이브 상태** 아래에서, 암호화하거나 암호화 해제하려는 각 하드 드라이브 옆의 확인란을 선택하거나 선택 해제한 후 **적용**을 누릅니다.

**참고:** 파티션이 암호화 또는 암호 해제 중인 경우 진행 표시줄에는 파티션 암호화 진행률 및 완료될 때까지 남은 시간이 표시됩니다.

**참고:** 동적 파티션은 지원되지 않습니다. 파티션이 사용 가능한 상태로 표시되지만 선택했을 때 암호화할 수 없는 경우 이 파티션은 동적입니다. 디스크 관리 내에서 새로운 파티션을 만들기 위해 파티션을 축소할 경우 동적 파티션이 발생합니다.

파티션이 동적 파티션으로 변환될 경우 경고가 표시됩니다.

# 백업 및 복구(관리자 작업)

Drive Encryption 이 활성화되어 있으면 관리자는 암호화 키 백업 페이지를 사용하여 암호화 키를 이동식 미디어에 백업하고 복구를 수행할 수 있습니다.

## 암호화 키 백업

관리자는 이동식 저장 장치에 암호화된 드라이브에 대한 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 컴퓨터에 액세스할 수 있습니다. 또한 저장 장치가 Windows 에 액세스할 수 있기 때문에 저장 공간은 안전해야 합니다.

**참고:** 암호화 키를 저장하려면 FAT 32 또는 FAT16 형식의 USB 저장 장치를 사용해야 합니다. USB 메모리 스틱, SD(Secure Digital) 메모리 카드 또는 MultiMedia 카드(MMC)를 백업에 사용할 수 있습니다.

1. **HP ProtectTools 관리 콘솔**을 실행합니다. 자세한 내용은 16페이지의 HP ProtectTools 관리 콘솔 열기를 참조하십시오.
2. 왼쪽 패널에서 **Drive Encryption** 왼쪽의 **+** 아이콘을 클릭하여 사용 가능한 옵션을 표시합니다.
3. **암호화 키 백업**을 누릅니다.
4. 암호화 키를 백업하는 데 사용되는 저장 장치를 넣습니다.

**참고:** 암호화 키를 저장하려면 FAT32 형식의 USB 저장 장치를 사용해야 합니다. USB 메모리 스틱, SD(Secure Digital) 메모리 카드 또는 MultiMedia 카드(MMC)를 백업에 사용할 수 있습니다. 경우에 따라 SkyDrive 를 사용할 수도 있습니다.

5. **드라이브** 아래에서 암호화 키를 백업하려는 장치의 확인란을 선택합니다.
6. **키 백업**을 누릅니다.
7. 표시되는 페이지에서 정보를 읽은 후 **확인**을 누릅니다. 선택한 저장 장치에 암호화 키가 저장됩니다.

### 백업 키를 사용하여 활성화된 컴퓨터에 대한 액세스 복구

관리자는 활성화 시 이동식 저장 장치에 백업된 Drive Encryption 키를 사용하거나 Security Manager에 있는 **Drive Encryption 키 백업** 옵션을 선택하여 복구를 수행할 수 있습니다.

1. 백업 키를 저장한 이동식 저장 장치를 넣습니다.
2. 컴퓨터의 전원을 켭니다.
3. Drive Encryption for HP ProtectTools 로그인 대화 상자가 열리면 **옵션**을 클릭합니다.
4. **복구**를 누릅니다.
5. 백업 키가 들어 있는 파일 경로 또는 이름을 입력한 다음 **복구**를 누릅니다.

   – 또는 –

   **찾아보기**를 눌러 필요한 백업 파일을 검색하고 **확인**을 누른 다음 **복구**를 누릅니다.
6. 확인 대화 상자가 표시되면 **확인**을 누릅니다.

   Windows 로그온 화면이 표시됩니다.

**참고:** Drive Encryption 로그인 화면에서 복구 키를 사용하여 로그온하면 Windows 로그온에서 추가 인증 정보로 사용자 계정에 액세스해야 합니다. 복구를 수행한 후 암호를 재설정하는 것이 좋습니다.

## HP SpareKey 복구 수행

Drive encryption 사전 부팅에서 SpareKey 복구를 실행하려면 컴퓨터에 액세스하기 전에 보안 질문에 정확하게 답해야 합니다. SpareKey 복구 설정에 대한 자세한 내용은 Security Manager 소프트웨어 도움말을 참조하십시오.

암호가 기억나지 않는 경우 HP SpareKey 복구를 수행하려면 다음과 같이 하십시오.

1. 컴퓨터의 전원을 켭니다.
2. Drive Encryption for HP ProtectTools 페이지가 표시되면 사용자 로그온 페이지로 이동합니다.

3. **SpareKey** 를 누릅니다.

**참고:** SpareKey 를 Security Manager 에서 초기화하지 않은 경우 **SpareKey** 버튼을 사용할 수 없습니다.

4. 표시된 질문에 정확한 답을 입력한 다음 **로그온**을 누릅니다.

   Windows 로그온 화면이 표시됩니다.

**참고:** Drive Encryption 로그온 화면에서 SpareKey 를 사용하여 로그온하면 Windows 로그온에서 추가 인증 정보로 사용자 계정에 액세스해야 합니다. 복구를 수행한 후 암호를 재설정하는 것이 좋습니다.

# 암호화 상태 표시

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

**참고:** 관리자는 HP ProtectTools 관리 콘솔을 사용하여 드라이브 암호화 상태를 변경할 수 있습니다.

1. **HP ProtectTools 사용자 콘솔**을 실행합니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.
2. **내 데이터**에서 **Drive Encryption** 을 클릭합니다.

   소프트웨어 또는 하드웨어 암호화의 경우 드라이브 암호화 상태가 다음 중 하나로 표시됩니다.

   - 활성화됨
   - 비활성화됨

   소프트웨어 암호화의 경우 드라이브 암호화 상태가 각 하드 드라이브 또는 하드 드라이브 파티션에 대한 다음 중 하나로 표시됩니다.

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

   하드웨어 암호화의 경우 드라이브 암호화 상태가 다음 중 하나로 표시됩니다.

   - 암호화되지 않음
   - 암호화됨

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

# 7 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 54페이지의관리되지 않는 장치 클래스를 참조하십시오.

Windows® 운영 체제 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 로그온합니다.
2. **HP Client Security 대시보드**에서 **HP ProtectTools Security Manager** 를 실행합니다.

   – 또는 –

   Windows 데스크톱의 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 두 번 클릭합니다.

   – 또는 –

   **제어판**에서 **시스템 및 보안**을 선택한 다음 **HP ProtectTools Security Manager** 를 선택합니다.
3. HP ProtectTools Security Manager 사용자 콘솔의 왼쪽 패널에서 **관리**를 클릭한 다음 **관리 콘솔**을 선택합니다.
4. 관리 콘솔의 왼쪽 패널에서 **Device Access Manager** 를 클릭합니다.

표준 사용자의 경우 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 장치 클래스에 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

**참고:** Bluetooth 장치가 인증 정보로 사용되는 경우 Bluetooth 장치 액세스는 Device Access Manager 정책에 의해 제한되지 않아야 합니다.

- 모든 모뎀 장치
- 모든 PCMCIA/ExpressCard 장치
- 모든 1394 장치

장치 관리자가 아닌 모든 사용자에게 장치 클래스에 대한 액세스를 허용하거나 거부하려면 다음과 같이 하십시오.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 클릭한 다음 **단순 구성**을 클릭합니다.
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 대화 상자가 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.

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 열고 다음을 입력합니다. `sc query flcdlock`.

장치 드라이버가 실행되고 있는지 확인하려면 명령 프롬프트 창을 열고 다음을 입력합니다. `sc query damdrv`.

## 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 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 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 클릭한 다음 **장치 클래스 구성**을 클릭합니다.
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 콘솔**의 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 클릭한 다음 **장치 클래스 구성**을 클릭합니다.
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 클릭한 다음 **장치 클래스 구성**을 클릭합니다.
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.

**참고:** 고급 설정 페이지는 재설정되지 않습니다.

구성 설정을 기본값으로 재설정하려면 다음과 같이 하십시오.

1. HP ProtectTools 관리 콘솔의 왼쪽 창에서 **Device Access Manager** 를 클릭한 다음 **장치 클래스 구성**을 클릭합니다.
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 관리자가 아닌 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 누르면 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 로그온해야 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 로그온해야 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 53페이지의장치 관리자 그룹를 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. 장치 관리자가 아닌 모든 사용자의 이동 미디어에 대한 액세스 거부 등의 단순 구성 정책을 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.

장치 관리자 그룹을 사용하여 장치 액세스에 대해 신뢰할 수 있는 사용자를 Device Access Manager 정책에서 지정한 제한에서 제외할 수 있습니다. 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.

## eSATA 장치 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

# 8 도난 회수(일부 모델만 해당)

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. Security Manager 사용자 콘솔을 엽니다. 자세한 내용은 24페이지의 Security Manager 열기를 참조하십시오.
3. Security Manager 왼쪽 창에서 **도난 회수**를 클릭합니다.
4. **시작하기**를 눌러 Computrace 활성화 마법사를 시작합니다.
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 메일이 전송됩니다.

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

고객 센터에 로그온하려면 다음과 같이 하십시오.

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

# 9 지역화된 암호 예외

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

## 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. **제어판**을 사용하여 지원되는 키보드 레이아웃을 추가합니다(중국어 입력 언어에서 미국 영어 키보드를 추가).
  2. 기본 입력 방법으로 지원되는 키보드를 설정합니다.
  3. 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 문자에 대한 자세한 내용은 HP ProtectTools 관리 콘솔 소프트웨어 도움말을 참조하십시오.
  2. Security Manager 설치 마법사를 다시 실행한 후 새 Windows 암호를 입력합니다.

## 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.

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 | ﻷ,ﻹ 및 ﻵ 키는 두 개의 문자로 입력됩니다. | ﻷ,ﻹ 및 ﻵ 키는 한 개의 문자로 입력됩니다. | ﻷ,ﻹ 및 ﻵ 키는 한 개의 문자로 입력됩니다. |
| 캐나다 프랑스어 | caps lock 키를 누른 상태로 **ç**, **è**, **à** 및 **é** 문자를 입력하면 Windows 에서 **Ç**, **È**, **À** 및 **É** 문자로 입력됩니다. | caps lock 키를 누른 상태로 **ç**, **è**, **à** 및 **é** 문자를 입력하면 BIOS Preboot Security 에서 **ç**, **è**, **à** 및 **é** 문자로 입력됩니다. | caps lock 키를 누른 상태로 **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 |

| 언어 | Windows | BIOS | Drive Encryption |
| --- | --- | --- | --- |
| 영어(국제) | ◦ 맨 위 행의 ¡, ¤, ‘, ’, ¥ 및 × 키는 입력되지 않습니다.<br>◦ 두 번째 행의 å, ® 및 Þ 키는 입력되지 않습니다.<br>◦ 세 번째 행의 á, ð 및 ø 키는 입력되지 않습니다.<br>◦ 맨 아래 행의 æ 키는 입력되지 않습니다. | 해당 사항 없음 | 해당 사항 없음 |
| 체코어 | ◦ ğ 키는 입력되지 않습니다.<br>◦ į 키는 입력되지 않습니다.<br>◦ ų 키는 입력되지 않습니다.<br>◦ ė, ı 및 ż 키는 입력되지 않습니다.<br>◦ 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.<br>◦ 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 | 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 |

# 용어

**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 복구**
보안 질문에 올바르게 답변하여 컴퓨터에 액세스하는 기능

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

**ID 카드**
사용자 이름과 선택한 사진으로 데스크탑을 시각적으로 식별하는 Windows 바탕 화면 가젯.

**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

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

**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.

**TXT**
Trusted Execution Technology 의 약자로 보안 기술의 일종.

**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

**관리자**
*Windows 관리자*를 참조하십시오.

**관리 콘솔**
관리자가 HP ProtectTools 의 기능과 설정을 액세스하고 관리할 수 있는 중앙 위치

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

**네트워크 계정**
로컬 컴퓨터, 워크 그룹 또는 도메인에 있는 Windows 사용자 또는 관리자 계정

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

**로그온**
웹 사이트나 다른 프로그램에 로그온하는 데 사용할 수 있는 사용자 이름과 암호(및 기타 가능한 선택 정보)로 구성된 Security Manager 내의 객체

**백그라운드 서비스**
장치 액세스 제어 정책을 적용하기 위해 실행해야 하는 HP ProtectTools Device Locking/Auditing 백그라운드 서비스. 제어판의 관리 도구 옵션의 서비스 응용 프로그램에서 확인할 수 있습니다. 장치 액세스 제어 정책을 적용할 때 백그라운드 서비스가 실행되지 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 사용할 등록된 사용자의 이미지

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

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

**암호 해제**
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.

**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

**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.

**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