# HP Client Security

시작하기

초판: 2013 년 8 월

문서 부품 번호: 735339-AD1

# 목차

# 1 HP Client Security Manager 소개

HP Client Security 를 사용하면 데이터, 장치 및 ID 를 보호할 수 있으므로 컴퓨터 보안이 향상됩니다.

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

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

**참고:** 본 설명서의 내용은 HP Client Security 소프트웨어 모듈이 이미 설치된 상태를 전제로 작성되었습니다.

## HP Client Security 의 기능

다음 표에는 HP Client Security 모듈의 주요 기능이 기재되어 있습니다.

| 모듈 | 주요 기능 |
|---|---|
| HP Client Security Manager | 관리자는 다음 기능을 수행할 수 있습니다.<br>• Windows®를 시작하기 전에 컴퓨터를 보호합니다<br>• 강력한 인증을 사용하여 Windows 계정을 보호<br>• 웹 사이트 및 응용프로그램을 위한 로그온과 암호 관리<br>• 쉽게 Windows 운영 체제 암호 변경<br>• 추가 보안과 편의를 위한 지문 사용<br>• 인증을 위한 스마트 카드, 비접촉식 카드 또는 근접 카드 설정<br>• Bluetooth 전화를 식별 방법으로 사용<br>• PIN 을 설정하여 인증 선택을 확장합니다<br>• 로그온 및 세션 정책 구성<br>• 프로그램 데이터 백업 및 복원<br>• HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager 및 HP Computrace 같은 응용프로그램 추가<br>일반 사용자는 다음 기능을 수행할 수 있습니다.<br>• 암호화 상태 및 Device Access Manager 설정을 봅니다.<br>• Computrace 를 활성화합니다.<br>• 기본 설정 및 백업과 복원 옵션을 구성합니다. |

| 모듈 | 주요 기능 |
| --- | --- |
| 암호 관리자 | 일반 사용자는 다음 기능을 수행할 수 있습니다.<br>• 사용자 이름과 암호를 구성하고 설정합니다.<br>• 전자 메일과 웹 계정의 향상된 계정 보안을 위해 보다 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.<br>• 계정이 손상된 것으로 표시하므로 유사한 인증 정보를 가진 다른 계정을 변경합니다.<br>• 지원되는 브라우저에서 로그온 데이터를 가져옵니다. |
| HP Drive Encryption(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). |
| HP Device Access Manager | • 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. |
| HP Trust Circles | • 파일 및 문서 보안을 제공합니다.<br>• 사용자가 지정한 폴더에 저장된 파일을 암호화하여 Trust Circles 내에서 보호합니다.<br>• Trust Circles 에 있는 구성원만 파일을 사용하고 공유할 수 있습니다. |
| 도난 회수(Computrace, 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 Client Security 제품 설명 및 일반적인 사용 사례

대부분의 HP Client Security 제품은 사용자 인증(일반적으로 암호)과 함께, 암호를 분실했거나 사용할 수 없거나 기억이 나지 않거나 회사 보안팀에서 액세스를 요청할 때를 대비한 관리용 예비 인증 기능을 모두 보유하고 있습니다.

**참고:** 일부 HP Client Security 제품은 데이터 액세스를 제한하도록 설계되어 있습니다. 내용이 중요하여 누출되기보다는 사라지는 편이 나은 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.
- 계정이 손상된 것으로 표시하므로 유사한 인증 정보를 가진 다른 계정을 변경합니다.
- 지원되는 브라우저에서 로그온 데이터를 가져옵니다.

**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:** 열심히 근무하는 한 직원이 승진되었고 이제 전체 회계 부서를 관리합니다. 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 직원은 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.

## HP Drive Encryption(일부 모델만 해당)

HP Drive Encryption 은 컴퓨터 하드 드라이브 또는 보조 드라이브 전체의 데이터에 대해 액세스를 제한할 때 사용합니다. Drive Encryption 은 또한 자체 암호 기능이 있는 드라이브도 관리할 수 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.

**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.

## HP Device Access Manager(일부 모델만 해당)

관리자는 HP Device Access Manager 를 통해 하드웨어 액세스를 제한하고 관리할 수 있습니다. Device Access Manager 를 이용하면 USB 플래시 드라이브를 무단으로 액세스해서 데이터를 복사하는 행위를 차단할 수 있습니다. 또한 CD/DVD 드라이브 액세스, USB 장치 제어, 네트워크 연결 등등의 제한도 가능합니다. 외부 공급업체에 회사 컴퓨터에 대한 액세스는 허용해야 하지만 USB 드라이브에 데이터를 복사할 수는 없도록 해야 하는 경우를 예로 들 수 있을 것입니다.

**예제 1:** 어느 의료용품 회사의 관리자는 개인 의료 기록과 회사 정보를 자주 취급합니다. 직원들은 이 데이터에 대한 액세스가 필요하지만, USB 드라이브나 기타 외부 저장 매체를 통해 해당 컴퓨터에서 데이터를 빼가는 일은 절대 없어야 합니다. 네트워크는 안전하지만, 해당 컴퓨터에는 CD 버너와 USB 포트가 있어 데이터 복사 또는 도난의 가능성이 있습니다. 관리자는 Device Access Manager 를 이용해서 USB 포트와 CD 버너를 쓸 수 없도록 비활성화합니다. USB 포트가 차단되더라도 마우스와 키보드는 정상 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(별도 구매)

Computrace(별도 구매)는 도난당한 컴퓨터의 위치를, 사용자가 인터넷에 액세스할 때마다, 추적할 수 있는 서비스입니다. Computrace 는 또한 원격으로 컴퓨터를 찾아 관리하고 컴퓨터 사용 상황과 응용 프로그램을 모니터링하는 데에도 도움이 됩니다.

**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 Client Security 의 여러 모듈은 서로 연동하여 다음과 같은 주요 보안 목표를 포함한 다양한 보안 문제를 해결할 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.
  - HP Client Security—13페이지의 HP Client Security 를 참조하십시오.
  - HP Drive Encryption—28페이지의 HP Drive Encryption(일부 모델만 해당) 부분을 참조하십시오.
- 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—50페이지의도난 회수(일부 모델만 해당) 부분을 참조하십시오.

## 민감한 데이터에 대한 액세스 제한

현장 근무 중인 감사관에게 민감한 재무 정보를 조회할 수 있는 컴퓨터 액세스 권한을 부여했더라도, 파일을 인쇄하거나 CD 와 같은 기록 장치에 저장하는 것은 막아야 할 것입니다. 다음 기능은 데이터 액세스를 제한하는 데 도움이 됩니다.

- IT 관리자는 HP Device Access Manager 를 이용해서 통신 장치에 대한 액세스를 제한함으로써 하드 드라이브에서 기밀 정보가 복사되는 것을 막을 수 있습니다. 자세한 내용은 41페이지의시스템 보기를 참조하십시오.

## 내부 또는 외부 위치에서의 무단 액세스 방지

보안되지 않은 업무용 컴퓨터에 대한 무단 액세스는 재무 업무, 임원 또는 연구개발팀의 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. (자세한 내용은 28페이지의 HP Drive Encryption(일부 모델만 해당)를 참조하십시오.)
- HP Client Security 를 사용하면 승인받지 않은 사용자가 암호를 얻거나 암호로 보호된 응용프로그램에 액세스할 수 없습니다. 자세한 내용은 13페이지의 HP Client Security 를 참조하십시오.
- IT 관리자는 HP Device Access Manager 를 이용해서 쓰기 가능한 장치에 대한 액세스를 제한함으로써 하드 드라이브에서 기밀 정보가 복사되는 것을 막을 수 있습니다. 자세한 내용은 40페이지의 HP 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 Password Manager 는 암호용 저장소와 Single Sign On 편의를 제공합니다. 자세한 내용은 18페이지의 Password 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 Client Security 에서는 보안 의무와 권한에 따라 다음과 같은 역할 구분이 가능합니다.

- 보안 책임자—회사 또는 네트워크의 보안 수준을 지정하고 Drive Encryption 등 설치할 보안 요소 및 기능을 결정합니다.

  **참고:** 보안 책임자는 HP 와 협력해서 HP Client Security 의 여러 기능을 사용자 정의할 수 있습니다. 자세한 내용은 http://www.hp.com 를 참조하십시오.

- IT 관리자—보안 담당자가 지정한 보안 기능을 적용 및 관리합니다. 일부 기능을 활성화하거나 비활성화할 수도 있습니다. 예를 들어, 보안 책임자가 스마트 카드를 배포하기로 결정했다면 IT 관리자는 Java 암호와 스마트 카드 모드를 활성화할 수 있습니다.
- 사용자—이와 같은 보안 기능을 사용합니다. 예를 들어, 보안 책임자와 IT 관리자가 시스템의 스마트 카드 기능을 활성화했다면 사용자는 스마트 카드 PIIN 을 설정해서 그 카드를 인증 용도에 사용할 수 있습니다.

⚠ **주의:** 관리자는 “모범 규준”에 따라 최종 사용자 권한과 사용자 액세스를 제한해야 합니다. 권한 없는 사용자에게 관리 권한을 부여해서는 안 됩니다.

## HP Client Security 암호 관리

HP Client Security 의 기능은 대부분 암호로 보호됩니다. 아래 표는 자주 사용되는 암호, 그 암호가 설정되는 소프트웨어 모듈, 그 암호의 기능 등을 정리한 것입니다.

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

| HP Client Security 암호 | 설정하는 모듈 | 기능 |
|---|---|---|
| Windows 로그온 암호 | Windows 제어판 또는 HP Client Security | 다양한 HP Client Security 기능에 액세스하기 위해 수동 로그온 및 인증 정보가 사용될 수 있습니다. |
| HP Client Security 백업 및 복구 암호 | HP Client Security, 개별 사용자 | HP Client Security 백업 및 복구 파일에 무단으로 액세스하지 못하도록 합니다. |
| 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.
- 예를 들어 “Mary2-2Cat45”의 경우와 같이 단어 또는 문구의 중간에 숫자 또는 특수문자를 넣습니다.
- 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 정보와 설정의 백업

HP Client Security 의 백업 및 복구 도구를, 설치된 일부 HP Client Security 모듈로부터 보안 인증 정보를 백업 및 복원할 수 있는, 일종의 중심점으로 활용할 수 있습니다.

# 2 시작

인증 정보와 함께 사용하기 위해 HP Client Security 를 설정하려면 다음 방법 중 하나로 HP Client Security 를 실행합니다. 일단 사용자가 마법사를 완료했으면 이 사용자가 다시 마법사를 실행할 수 없습니다.

1. 시작 또는 앱 화면에서 **HP Client Security** 앱을 클릭하거나 누릅니다(Windows 8).

   – 또는 –

   Windows 바탕 화면에서 **HP Client Security 가젯**을 클릭하거나 누릅니다(Windows 7).

   – 또는 –

   Windows 바탕 화면에서 작업 표시줄 오른쪽 끝에 있는 알림 영역에 있는 **HP Client Security** 아이콘을 두 번 클릭하거나 두 번 누릅니다.

   – 또는 –

   Windows 바탕 화면에서 알림 영역에 있는 **HP Client Security** 아이콘을 클릭하거나 누른 다음 **HP Client Security 열기**를 선택합니다.

2. HP Client Security 설치 마법사는 환영 페이지가 표시된 상태에서 시작됩니다.

3. 시작 화면을 읽고 Windows 암호를 입력하여 ID 를 확인한 후에 **다음**을 클릭하거나 누릅니다.

   아직 Windows 암호를 생성하지 않은 경우에는 암호를 생성하라는 메시지가 나타납니다. 다른 사람의 무단 액세스로부터 Windows 계정을 보호하거나 HP Client Security 기능을 사용하려면 Windows 암호가 필요합니다.

4. HP SpareKey 페이지에서 세 가지 보안 질문을 선택합니다. 각 질문에 대한 답변을 입력하고 **다음**을 누릅니다. 사용자 정의 질문도 허용됩니다. 자세한 내용은 14페이지의 HP SpareKey—암호 복구을 참조하십시오.

5. 지문 페이지에서 필요한 최소 지문 개수를 등록한 후에 **다음**을 클릭하거나 누릅니다. 자세한 내용은 13페이지의지문을 참조하십시오.

6. Drive Encryption 페이지에서 암호화를 활성화하고 암호화 키를 백업한 후에 **다음**을 클릭하거나 누릅니다. 자세한 내용은 HP Drive Encryption 소프트웨어 도움말을 참조하십시오.

   **참고:** 사용자가 관리자이고 HP Client Security 설치 마법사를 이전에 관리자가 구성하지 않은 시나리오에 적용됩니다.

7. 마법사의 마지막 페이지에서 **마침**을 클릭하거나 누릅니다.

   이 페이지는 기능의 상태와 인증 정보를 제공합니다.

8. HP Client Security 설치 마법사는 Just In Time 인증 및 File Sanitizer 기능의 활성화를 보장합니다. 자세한 내용은 HP Device Access Manager 소프트웨어 도움말 및 HP File Sanitizer 소프트웨어 도움말을 참조하십시오.

   **참고:** 사용자가 관리자이고 HP Client Security 설치 마법사를 이전에 관리자가 구성하지 않은 시나리오에 적용됩니다.

## HP Client Security 열기

다음과 같은 방법 중 하나로 HP Client Security 를 열 수 있습니다.

**참고:** HP Client Security 설치 마법사는 HP Client Security 응용프로그램을 실행하기 전에 완료해야 합니다.

- 시작 또는 앱 화면에서 **HP Client Security** 앱을 클릭하거나 누릅니다.

  – 또는 –

  Windows 바탕 화면에서 **HP Client Security** 가젯을 클릭하거나 누릅니다(Windows 7).

  – 또는 –

  Windows 바탕 화면에서 작업 표시줄 오른쪽 끝에 있는 알림 영역에 있는 **HP Client Security** 아이콘을 두 번 클릭하거나 두 번 누릅니다.

  – 또는 –

  Windows 바탕 화면에서 알림 영역에 있는 **HP Client Security** 아이콘을 클릭하거나 누른 다음 **HP Client Security 열기**를 선택합니다.

# 3 중소기업을 위한 쉬운 시작 가이드

이 장에서는 HP Client Security for Small Business 에서 자주 사용되는 유용한 옵션을 활성화할 때 진행하는 기본적인 절차를 설명합니다. 이 소프트웨어에는 기본 설정을 세밀하게 조정하고 액세스 제어 권한을 설정할 수 있는 수 많은 도구와 옵션이 있습니다. 이 간편 설치 설명서의 목적은 설치/설정에 들어가는 시간과 노력을 최소화면서 각 모듈을 작동 준비하는 데 있습니다. 설명이 더 필요하면 더 알아보고자 하는 모듈을 선택한 다음, 오른쪽 상단 모서리의 **?** 또는 도움말 버튼을 클릭하십시오. 이 버튼을 클릭하면 현재 표시된 창과 관련하여 도움이 되는 정보가 자동으로 표시됩니다.

## 시작하기

1. Windows 바탕화면에서 작업 표시줄 오른쪽 끝 알림 영역에 있는 **HP Client Security** 아이콘을 두 번 클릭해서 HP Client Security 를 엽니다.
2. Windows 암호를 입력하거나 Windows 암호를 만듭니다.
3. HP Client Security 설치 마법사를 완료합니다.

Windows 로그인 중 HP Client Security 가 인증을 한 번만 요구하도록 설정하려면 26페이지의보안 기능을 참조하십시오.

## 암호 관리자

누구나, 특히 로그온을 필요로 하는 웹사이트나 응용프로그램을 정기적으로 이용하는 경우에는 더욱, 상당히 많은 수의 암호를 갖고 있습니다. 일반적인 사용자들은 모든 응용프로그램과 웹사이트에 동일한 암호를 사용하거나, 창의적으로 각기 다른 암호를 여러 개 만든 후 어디에 어느 암호를 설정했는지 즉시 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.
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 Ctrl+Windows 키+h 의 키 조합을 사용하여 Password Manager 를 연 다음 **로그인**을 클릭하여 저장된 바로 가기를 시작하고 인증합니다.

Password Manager 의 **편집** 옵션을 이용하면 이름과 로그인 이름, 그리고 암호까지 확인하고 수정할 수 있습니다.

HP Client Security for Small Business 는 모든 인증 정보와 설정을 다른 컴퓨터에 백업 및/또는 복사할 수 있게 해줍니다.

# HP Device Access Manager

Device Access Manager 는 다양한 내부 및 외부 저장 장치의 사용을 제한해서 데이터가 회사 밖으로 빠져나가지 않고 하드 드라이브에 안전하게 남아 있게 해줍니다. 사용자에게 데이터 액세스는 허용하되 CD 나 mp3 플레이어, USB 메모리에 복사하지는 못하게 하는 것을 예로 들 수 있습니다.

1. **Device Access Manager** 를 엽니다(40페이지의 Device Access Manager 열기 참조).

   현재 사용자의 액세스 권한이 표시됩니다.

2. 사용자, 그룹 또는 장치 액세스 권한을 변경하려면 **변경**을 클릭하거나 누릅니다. 자세한 내용은 41페이지의시스템 보기을 참조하십시오.

# HP Drive Encryption

HP Drive Encryption 은 하드 드라이브 전체를 암호화해서 데이터를 보호하는 용도로 사용됩니다. PC 를 도난 당하거나 하드 드라이브를 원래의 컴퓨터에서 빼서 다른 컴퓨터에 장착하더라도 그 하드 드라이브의 데이터는 안전하게 보호됩니다.

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

Windows 사용자 계정, 인증 도메인, HP Drive Encryption, Password Manager, HP Client Security 등 다수의 소프트웨어 모듈이 암호를 자동으로 동기화하기 때문에 더욱 편리합니다.

HP Client Security 설정 마법사를 사용하여 초기 설정하는 동안 HP Drive Encryption 을 설정하려면 8페이지의시작를 참조하십시오.

# 4 HP Client Security

HP Client Security 홈 페이지는 HP Client Security 기능, 응용프로그램, 설정 등에 쉽게 액세스할 수 있는 중앙 위치입니다. 홈 페이지는 3 개 섹션으로 나뉩니다.

- **데이터**—데이터 보안을 관리하는 데 사용되는 응용프로그램에 대한 액세스를 제공합니다.
- **장치**—장치 보안을 관리하는 데 사용되는 응용프로그램에 대한 액세스를 제공합니다.
- **ID**—인증 정보의 등록과 관리를 제공합니다.

커서를 응용프로그램 타일로 이동하여 응용프로그램의 설명을 표시합니다.

HP Client Security 는 페이지는 페이지 하단에 있는 사용자 및 관리자 설정에 대한 링크를 제공할 수 있습니다. HP Client Security 는 **Gear**(기어) (설정) 아이콘을 누르거나 클릭하여 고급 설정 및 기능에 대한 액세스를 제공합니다.

## ID 기능, 응용프로그램 및 설정

HP Client Security 에서 제공하는 ID 기능, 응용프로그램 및 설정은 디지털 신원의 다양한 측면을 관리하는 기능을 지원합니다. HP Client Security 홈 페이지 중 하나를 클릭하거나 누른 다음 Windows 암호를 입력합니다.

- **지문**—지문 인증 정보를 등록하고 관리합니다.
- **SpareKey**—다른 인증 정보를 분실했거나 찾을 수 없는 경우 컴퓨터에 로그인하는 데 사용할 수 있는 HP SpareKey 인증 정보를 설정하고 관리합니다. 잊어버린 암호를 재설정할 수도 있습니다.
- **Windows 암호**—Windows 암호를 변경하는 쉬운 액세스를 제공합니다.
- **Bluetooth 장치**—Bluetooth 장치를 등록하고 관리할 수 있습니다.
- **카드**—스마트 카드, 비접촉식 카드 및 근접 카드를 등록하고 관리할 수 있습니다.
- **PIN**—PIN 인증 정보를 등록하고 관리할 수 있습니다.
- **RSA SecurID**—RSA SecurID 인증 정보를 등록하고 관리할 수 있습니다(적절한 설정이 되어 있는 경우).
- **Password Manager**—온라인 계정 및 응용프로그램에 대한 암호를 관리할 수 있습니다.

### 지문

HP Client Security 설치 마법사는 지문을 설정하거나 “등록”하는 프로세스를 안내합니다.

지문 페이지에서 지문을 등록하거나 삭제할 수도 있으며 HP Client Security 홈 페이지에서 **지문** 아이콘을 클릭하거나 눌러 액세스할 수 있습니다.

1. 지문 페이지에서 지문이 등록될 때까지 손가락을 문지르십시오.

   등록하는 데 필요한 손가락 번호가 페이지에 표시됩니다. 검지와 중지가 좋습니다.

2. 이전에 등록된 지문을 삭제하려면 **삭제**를 클릭하거나 누릅니다.
3. 손가락을 추가로 등록하려면 **Enroll an additional fingerprint**(추가 지문 등록)를 클릭하거나 누릅니다.
4. 페이지를 종료하기 전에 **저장**을 클릭하거나 누릅니다.

⚠ **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**.

- 관리자가 등록, 정확도 및 기타 설정을 지정할 수 있는 지문 관리자 설정에 액세스하려면 **Administrative Settings**(관리자 설정)를 클릭하거나 누릅니다(관리자 권한이 필요).
- 지문 인식 지문 모양과 동작을 관리하는 설정을 지정할 수 있는 사용자 설정에 액세스하려면 **사용자 설정**을 클릭하거나 누릅니다.

### 지문 관리자 설정

관리자는 지문 인식기의 등록, 정확도 및 기타 설정을 지정할 수 있습니다. 관리자 권한이 필요합니다.

- 지문 인증 정보의 관리자 설정에 액세스하려면 지문 페이지에서 **Administrative Settings**(관리자 설정)를 클릭하거나 누릅니다.

- **사용자 등록**—사용자가 등록할 수 있는 최소 및 최대 지문 수를 선택할 수 있습니다.
- **인식**—슬라이더를 이동하여 손가락을 문지를 때 지문 인식기에 사용되는 민감도를 조정할 수 있습니다.

  지문을 일관되게 인식할 수 없을 경우 인식 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.

### 지문 사용자 설정

지문 사용자 설정 페이지에서 지문 인식 모양과 동작을 관리하는 설정을 지정할 수 있습니다.

- 지문 인증 정보의 사용자 설정에 액세스하려면 지문 페이지에서 **사용자 설정**을 클릭하거나 누릅니다.

- **사운드 피드백 활성화**—기본적으로 지문을 인식시키면 HP Client Security 가 특정 프로그램 이벤트마다 다른 사운드를 재생하면서 오디오 피드백을 제공합니다. Windows 제어판의 사운드 설정에 있는 사운드 탭에서 이러한 이벤트에 새 사운드를 지정하거나 확인란을 선택 해제하여 사운드 피드백을 비활성화할 수 있습니다.
- **스캔 품질 피드백 표시**—품질과 관계없이 모든 지문 인식 결과를 표시하려면 확인란을 선택합니다. 품질이 좋은 지문 인식 결과만 표시하려면 확인란을 선택 해제합니다.

## HP SpareKey—암호 복구

SpareKey 를 사용하면 세 가지 보안 질문에 답변하여 지원 플랫폼의 컴퓨터에 액세스할 수 있습니다.

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

HP SpareKey 를 설정하려면:

1. 마법사의 HP SpareKey 페이지에서 세 가지 보안 질문을 선택한 다음 각 질문에 대한 답변을 입력합니다.

   미리 정의된 목록에서 질문을 선택하거나 직접 질문을 작성할 수 있습니다.

2. **등록**을 클릭하거나 누릅니다.

HP SpareKey 를 삭제하려면:

- **SpareKey 삭제**를 클릭하거나 누릅니다.

SpareKey 를 설정하면 파워온 인증 로그온 화면이나 Windows 시작 화면에서 SpareKey 를 사용하여 컴퓨터에 액세스할 수 있습니다.

SpareKey 페이지에 대한 다른 질문을 선택하거나 질문을 변경할 수 있습니다. 이 페이지는 HP Client Security 홈 페이지의 암호 복구 타일에서 액세스합니다.

관리자가 HP SpareKey 인증 정보와 관련한 설정을 지정할 수 있는 HP SpareKey 설정에 액세스하려면 **설정**을 클릭합니다(관리자 권한 필요).

### HP SpareKey 설정

HP SpareKey 설정 페이지에서 HP SpareKey 인증 정보의 동작과 사용을 관리하는 설정을 지정할 수 있습니다.

▲ HP SpareKey 설정 페이지를 시작하려면 HP SpareKey 페이지에서 **설정**을 클릭하거나 누릅니다(관리자 권한 필요).

관리자는 다음 설정을 선택할 수 있습니다.

- HP SpareKey 설정 과정에서 각 사용자에게 제공되는 질문을 지정합니다.
- 세 가지 사용자 정의 보안 질문을 사용자에게 제공되는 목록에 추가합니다.
- 사용자가 자신의 보안 질문을 작성할 수 있는지 여부를 선택합니다.
- 암호 복구를 위해 HP SpareKey 를 사용할 수 있는 인증 환경(Windows 또는 파워온 인증)을 지정합니다.

## Windows 암호

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

Windows 암호를 변경하려면:

1. HP Client Security 홈 페이지에서 **Windows 암호**를 클릭하거나 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 클릭하거나 눌러 현재 암호를 입력한 새 암호로 즉시 변경합니다.

## Bluetooth 장치

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 클릭하거나 누릅니다.

관리자가 Bluetooth 장치용 설정을 지정할 수 있는 15페이지의 Bluetooth 장치 설정 페이지에 액세스하려면 **설정**을 클릭합니다(관리자 권한 필요).

### Bluetooth 장치 설정

관리자는 Bluetooth 장치 인증 정보의 동작과 사용을 관리하는 다음 설정을 지정할 수 있습니다.

### 자동 인증

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity**(ID 를 확인하는 동안 연결된 Bluetooth 등록 장치 자동 사용)—사용자 동작을 요구하지 않고 인증에 Bluetooth 인증 정보를 사용할 수 있도록 하려면 확인란을 선택하고 이 옵션을 비활성화하려면 확인란 선택을 해제합니다.

### Bluetooth 근접성

- **등록된 Bluetooth 장치가 컴퓨터 범위 밖으로 움직일 때 컴퓨터 잠금**—로그인하는 동안 연결된 Bluetooth 장치가 범위 밖으로 움직일 때 컴퓨터를 잠그려면 확인란을 선택하고, 이 옵션을 사용하지 않으려면 확인란의 선택을 취소합니다.

**참고:** 이 기능을 이용하려면 컴퓨터의 Bluetooth 모듈이 이 기능을 지원해야 합니다.

## 카드

HP Client Security 는 컴퓨터 칩이 들어 있는 작은 플라스틱 카드인 다양한 종류의 식별 카드를 지원할 수 있습니다. 여기에는 스마트 카드, 비접촉식 카드 및 근접 카드가 포함됩니다. 관리자가 제조업체의 관련 드라이버를 설치하고 카드를 인증 정보로 활성화할 경우 이러한 카드 중 하나와 적절한 카드 리더를 컴퓨터에 연결하면 카드를 인증 정보로 사용할 수 있습니다.

스마트 카드의 경우 제조업체는 HP Client Security 의 보안 알고리즘에 사용되는 보안 인증서 및 PIN 관리를 설치할 도구를 제공해야 합니다. PIN 으로 사용되는 숫자나 문자 유형은 다양할 수 있습니다. 사용할 스마트 카드는 관리자가 먼저 초기화해야 합니다.

다음 스마트 카드 형식을 HP Client Security 에서 지원합니다.

- CSP
- PKCS11

HP Client Security 는 다음과 같은 유형의 비접촉식 카드를 지원합니다.

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

다음 근접 카드를 HP Client Security 에서 지원합니다.

- HID 근접 카드

스마트 카드를 등록하려면:

1. 연결된 스마트 카드 리더에 카드를 삽입합니다.
2. 카드가 인식되면 카드의 PIN 을 입력한 다음 **등록**을 클릭하거나 누릅니다.

스마트 카드 PIN 을 변경하려면:

1. 연결된 스마트 카드 리더에 카드를 삽입합니다.
2. 카드가 인식되면 카드의 PIN 을 입력한 다음 **인증**을 클릭하거나 누릅니다.
3. **PIN 변경**을 클릭하거나 누른 다음 새 PIN 을 입력합니다.

비접촉식 카드 또는 근접 카드를 등록하려면:

1. 카드를 해당 리더에 가까이 가져다 댑니다.
2. 카드가 인식되면 **등록**을 클릭하거나 누릅니다.

등록된 카드를 삭제하려면:

1. 카드 리더에 카드를 가져다 댑니다.
2. 스마트 카드의 경우 카드에 할당된 PIN 을 입력한 다음 **인증**을 클릭하거나 누릅니다.
3. **삭제**를 클릭하거나 누릅니다.

카드가 등록되면 **Enrolled Cards**(등록된 카드) 아래 카드 세부 정보가 표시됩니다. 카드가 삭제되면 목록에서 제거됩니다.

관리자가 카드 인증 정보와 관련된 설정을 지정할 수 있는 근접, 비접촉식 및 스마트 카드 설정에 액세스하려면 **설정**을 클릭하거나 누릅니다(관리자 권한 필요).

### 근접, 비접촉식 및 스마트 카드 설정

카드 설정에 액세스하려면 목록에서 카드를 클릭하거나 누른 다음 표시되는 화살표를 클릭하거나 누릅니다.

스마트 카드 PIN 을 변경하려면:

1. 카드 리더에 카드를 가져다 댑니다.
2. 카드에 할당된 PIN 을 입력한 다음 **계속**을 클릭하거나 누릅니다.
3. 새 PIN 을 입력하고 확인한 다음 **계속**을 클릭하거나 누릅니다.

스마트 카드 PIN 을 초기화하려면:

1. 카드 리더에 카드를 가져다 댑니다.
2. 카드에 할당된 PIN 을 입력한 다음 **계속**을 클릭하거나 누릅니다.
3. 새 PIN 을 입력하고 확인한 다음 **계속**을 클릭하거나 누릅니다.
4. **예**를 클릭하거나 눌러 초기화를 확인합니다.

카드 데이터를 지우려면:

1. 카드 리더에 카드를 가져다 댑니다.
2. 카드에 할당된 PIN(스마트 카드의 경우만 해당)을 입력한 다음 **계속**을 클릭하거나 누릅니다.
3. **예**를 클릭하거나 눌러 삭제를 확인합니다.

## 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 입력하고 다시 한 번 입력하여 확인한 다음 **적용**을 클릭하거나 누릅니다.

PIN 을 삭제하려면:

▲ **삭제**를 클릭하거나 누른 다음 **예**를 클릭하거나 눌러 확인합니다.

관리자가 PIN 인증 정보와 관련된 설정을 지정할 수 있는 PIN 설정에 액세스하려면 **설정**을 클릭하거나 누릅니다(관리자 권한 필요).

### PIN 설정

PIN 설정 페이지에서 PIN 인증 정보에 대한 최소 및 최대 허용 가능한 길이를 지정할 수 있습니다.

## RSA SecurID

관리자가 RSA 를 인증 정보로 활성화했고 다음 조건에 해당하는 경우 RSA SecurID 인증 정보를 등록하거나 삭제할 수 있습니다.

**참고:** 적절한 설정이 필요합니다.

- RSA Server 에 사용자를 만들어야 합니다.
- 사용자와 컴퓨터에 할당된 RSA SecurID 토큰이 RSA Server 도메인에 가입되어 있어야 합니다.
- SecurID 소프트웨어가 컴퓨터에 설치되어 있어야 합니다.
- 적절히 구성된 RSA Server 에 연결할 수 있어야 합니다.

RSA SecurID 인증 정보를 등록하려면:

▲ RSA SecurID 사용자 이름과 암호(사용자 환경에 따라 RSA SecurID 토큰 코드 또는 PIN+토큰 코드)를 입력한 다음 **적용**을 클릭하거나 누릅니다.

성공적으로 등록되면 "RSA SecurID 인증 정보가 등록되었습니다"라는 메시지가 표시되고 삭제 버튼이 활성화됩니다.

RSA SecurID 인증 정보를 삭제하려면 다음과 같이 하십시오.

▲ **삭제**를 클릭한 다음 "RSA SecurID 인증 정보를 삭제하시겠습니까?"라고 묻는 팝업 대화 상자에서 **예**를 선택합니다.

## Password Manager

웹 사이트 및 응용프로그램에 로그온하면 Password Manager 를 사용할 때 더욱 쉽고 안전하게 이용할 수 있습니다. Password Manager 를 사용하면 따로 적거나 기억할 필요 없이 더욱 강력한 암호를 생성하고 지문, 스마트 카드, 근접 카드, 비접촉식 카드, Bluetooth 전화기, PIN, RSA 또는 Windows 암호로 쉽고 빠르게 로그온할 수 있습니다.

**참고:** 웹 로그온 화면의 구조는 계속 바뀌므로 Password Manager 는 일부 사이트를 지원하지 못할 수 있습니다.

Password Manager 는 다음과 같은 옵션을 제공합니다.

### Password Manager 페이지

- 웹 페이지 또는 응용프로그램을 자동으로 시작할 계정을 클릭하거나 누르고 로그온합니다.
- 범주를 사용하여 계정을 분류합니다.

### 암호 강도

- 암호에 보안 위험이 있는지 여부를 파악
- 로그인 데이터를 추가할 때 웹 사이트와 응용프로그램에 사용되는 개인 암호의 강도를 확인하십시오.
- 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 클릭하거나 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.

- **Add [somedomain.com] to the Password Manager**(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**—HP Client Security 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 생성되고 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**—HP Client Security 도움말을 표시합니다.

**참고:** 이 컴퓨터의 관리자 구성에 따라 HP Client Security 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 프로그램으로 이동한 후에 이러한 로그온을 사용할 수 있습니다.

로그온을 추가하려면:

1. 웹 사이트나 프로그램에 대한 로그온 화면을 엽니다.
2. **Password Manager** 아이콘을 클릭하거나 누른 다음 로그온 화면이 웹 사이트용인지 프로그램용인지에 따라 다음 중 하나를 클릭하거나 누릅니다.
   - 웹 사이트의 경우 **Add [domain name] to Password Manager**(Password Manager 에 [domain name] 추가)를 클릭하거나 누릅니다.
   - 프로그램의 경우 **Add this logon screen to Password Manager**(Password Manager 에 이 로그온 화면 추가)를 클릭하거나 누릅니다.
3. 로그온 데이터를 입력합니다. 화면의 로그온 필드와 대화 상자의 해당 필드에는 굵은 주황색 테두리가 표시됩니다.
   a. 로그온 필드를 미리 서식이 지정된 선택 사항 중 하나로 채우려면 필드 오른쪽에 있는 화살표를 클릭하거나 누릅니다.
   b. 이 로그온의 암호를 보려면 **암호 표시**를 클릭하거나 누릅니다.
   c. 로그온 필드를 채웠지만 제출하지 않으려면 **자동으로 로그온 데이터 제출** 확인란을 선택 해제합니다.
   d. **확인**을 클릭하거나 누르고 사용할 인증 방법(지문, 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 클릭하거나 누릅니다.
      - 로그온에 필요한 각 필드의 확인란을 선택하거나, 로그온에 필요하지 않은 필드의 확인란을 선택 해제합니다.
      - **닫기**를 클릭하거나 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:

1. 웹 사이트나 프로그램에 대한 로그온 화면을 엽니다.
2. 로그온 정보를 편집할 수 있는 대화 상자를 표시하려면 **Password Manager** 아이콘을 클릭하거나 누르고 **로그온 편집**을 클릭하거나 누릅니다.

   화면의 로그온 필드와 대화 상자의 해당 필드에는 굵은 주황색 테두리가 표시됩니다.

   로그온을 클릭하거나 눌러 편집 옵션을 표시한 다음 **편집**을 선택하여 Password Manager 페이지 내에서 계정 정보를 편집할 수도 있습니다.
3. 로그온 정보를 편집합니다.
   - **계정 이름**을 편집하려면 필드에 새 이름을 입력합니다.
   - **범주** 이름을 추가하거나 편집하려면 **범주** 필드에 이름을 입력하거나 수정합니다.
   - 미리 서식이 지정된 선택 사항 중 하나를 사용하여 **사용자 이름** 로그온 필드를 선택하려면 채우려면 필드 오른쪽에 있는 아래쪽 화살표를 클릭하거나 누릅니다.

Password Manager 아이콘 컨텍스트 메뉴의 편집 명령에서 로그온을 편집할 때만 미리 서식이 지정된 선택 사항을 사용할 수 있습니다.

- 미리 서식이 지정된 선택 사항 중 하나를 사용하여 **암호** 로그온 필드를 선택하려면 채우려면 필드 오른쪽에 있는 아래쪽 화살표를 클릭하거나 누릅니다.

  Password Manager 아이콘 컨텍스트 메뉴의 편집 명령에서 로그온을 편집할 때만 미리 서식이 지정된 선택 사항을 사용할 수 있습니다.

- 추가 필드를 화면에서 로그온으로 추가하려면 **추가 필드**를 클릭하거나 누릅니다.
- 이 로그온의 암호를 보려면 **암호 표시** 아이콘을 클릭하거나 누릅니다.
- 로그온 필드를 채웠지만 제출하지 않으려면 **자동으로 로그온 데이터 제출** 확인란을 선택 해제합니다.
- 이 아이콘에 손상된 암호가 있는 것으로 표시하려면 **This password is compromised**(이 암호는 손상되었음) 확인란을 선택합니다.

  변경 내용을 저장한 후 같은 암호를 공유하는 다른 모든 로그온도 손상된 것으로 표시됩니다. 그런 다음 해당 계정을 각각 방문하여 필요에 따라 암호를 변경할 수 있습니다.

4. **확인**을 클릭하거나 누릅니다.

## Password Manager 빠른 링크 메뉴 사용

Password Manager 에서는 쉽고 빠르게 로그온을 생성한 웹 사이트와 프로그램을 실행할 수 있습니다. **Password Manager Quick Links**(Password Manager 빠른 링크) 메뉴 또는 HP Client Security 내의 Password Manager 페이지에서 프로그램이나 웹 사이트 로그온을 두 번 클릭하거나 눌러 로그온 화면을 열고 로그온 데이터를 입력합니다.

로그온을 만들면 Password Manager **빠른 링크** 메뉴에 자동으로 추가됩니다.

**빠른 링크** 메뉴를 표시하려면:

▲ **Password Manager** 핫키 조합을 누릅니다(Ctrl+Windows 키+h 가 초기 설정입니다). 핫키 조합을 변경하려면 HP Client Security 홈 페이지에서 **Password Manager** 를 클릭한 다음 **설정**을 클릭하거나 누릅니다.

## 로그온을 범주로 구성

로그온을 정리할 범주를 1 개 이상 생성합니다.

로그온을 범주에 할당하려면:

1. HP Client Security 홈 페이지에서 **Password Manager** 를 클릭하거나 누릅니다.
2. 계정 항목을 클릭하거나 누른 다음 **편집**을 클릭하거나 누릅니다.
3. **범주** 필드에 범주 이름을 입력합니다.
4. **저장**을 클릭하거나 누릅니다.

범주에서 계정을 제거하려면:

1. HP Client Security 홈 페이지에서 **Password Manager** 를 클릭하거나 누릅니다.
2. 계정 항목을 클릭하거나 누른 다음 **편집**을 클릭하거나 누릅니다.
3. **범주** 필드에서 범주 이름을 삭제합니다.
4. **저장**을 클릭하거나 누릅니다.

범주 이름을 변경하려면:

1. HP Client Security 홈 페이지에서 **Password Manager** 를 클릭하거나 누릅니다.
2. 계정 항목을 클릭하거나 누른 다음 **편집**을 클릭하거나 누릅니다.
3. **범주** 필드에서 범주 이름을 변경합니다.
4. **저장**을 클릭하거나 누릅니다.

## 로그온 관리

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

로그온은 Password Manager 페이지에 나열됩니다.

로그온을 관리하려면:

1. HP Client Security 홈 페이지에서 **Password Manager** 를 클릭하거나 누릅니다.
2. 기존 로그온을 클릭하거나 누르고 다음 옵션 중 하나를 선택한 후 화면의 지시를 따릅니다.
   - **편집**—로그온을 편집합니다. 자세한 내용은 20페이지의로그온 편집을 참조하십시오.
   - **로그인**—선택한 계정에 로그인합니다.
   - **삭제**—선택한 계정의 로그온을 삭제합니다.

웹 사이트나 프로그램에 대한 로그인을 더 추가하려면:

1. 웹 사이트나 프로그램에 대한 로그온 화면을 엽니다.
2. **Password Manager** 아이콘을 클릭하거나 눌러 컨텍스트 메뉴를 표시합니다.
3. **로그온 추가**를 클릭하거나 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.

계정에 대한 Password Manager 로그온을 만드는 동안 암호를 입력하면 암호의 강도를 나타내기 위해 암호 아래 색상 막대가 표시됩니다. 색상은 다음 값을 나타냅니다.

- **빨간색**—약함
- **노란색**—보통
- **녹색**—강함

## 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 클릭하거나 누른 다음 **아이콘 설정**을 클릭하거나 눌러 Password Manager 에서 로그온 사이트를 관리하는 방법을 사용자 정의합니다.
   - **로그온 화면에 로그온을 추가하라는 메시지 표시**—아직 로그온이 설정되지 않은 로그온 화면이 표시될 때 로그온을 추가할 것인지 묻는 메시지를 표시하려면 이 옵션을 클릭하거나 누릅니다.
   - **이 화면 제외**—이 로그온 화면에 대한 로그온을 추가할 것인지 다시 묻지 않으려면 이 확인란을 선택합니다.
   - **로그온 화면에 로그온을 추가하라는 메시지를 표시 안 함**—라디오 버튼을 선택합니다.
2. 이전에 제외한 화면에 대한 로그온을 추가하려면 다음과 같이 하십시오.
   a. 이전에 제외한 웹 사이트에 로그온합니다.
   b. Password Manager 가 이 사이트에 대한 암호를 기억하도록 하려면 팝업 대화 상자에서 **기억**을 클릭하거나 눌러 암호를 저장하고 화면 로그온을 만듭니다.
3. 추가 Password Manager 설정에 액세스하려면 Password Manager 아이콘을 클릭하거나 누르고 **Password Manager 열기**를 클릭하거나 누른 다음 Password Manager 페이지에서 **설정**을 클릭하거나 누릅니다.

## 로그온 가져오기 및 내보내기

HP Password Manager 가져오기 및 내보내기 페이지에서 웹 브라우저가 컴퓨터에 저장한 로그온을 가져올 수 있습니다. HP Client Security 백업 파일에서 데이터를 가져오고 HP Client Security 백업 파일로 데이터를 내보낼 수도 있습니다.

▲ 가져오기 및 내보내기 페이지를 실행하려면 Password Manager 페이지에서 **가져오기 및 내보내기**를 클릭하거나 누릅니다.

브라우저에서 암호를 가져오려면:

1. 암호를 가져오려는 브라우저를 클릭하거나 누릅니다(설치된 브라우저만 표시됨).
2. 암호를 가져오지 않으려는 계정의 확인란은 선택을 해제합니다.
3. **가져오기**를 클릭하거나 누릅니다.

가져오기 및 내보내기 페이지의 관련 링크(**Other Options**(기타 옵션) 아래에 있음)를 통해 HP Client Security 백업 파일에서 데이터를 가져오거나 데이터를 내보낼 수 있습니다.

**참고:** 이 기능은 Password Manager 데이터만 가져오고 내보냅니다. 추가 HP Client Security 데이터 백업 및 복원에 대한 자세한 내용은 27페이지의데이터 백업 및 복원을 참조하십시오.

HP Client Security 백업 파일에서 데이터를 가져오려면:

1. HP Password Manager 가져오기 및 내보내기 페이지에서 **Import data from an HP Client Security backup file**(HP Client Security 백업 파일에서 데이터 가져오기)을 클릭하거나 누릅니다.
2. 사용자의 신원을 확인합니다.
3. 이전에 만든 백업 파일을 선택하거나 제공된 필드에 경로를 입력한 다음 **찾아보기**를 클릭하거나 누릅니다.

4. 파일을 보호하는 데 사용되는 암호를 입력한 후 **다음**을 클릭하거나 누릅니다.
5. **복원**을 클릭하거나 누릅니다.

HP Client Security 백업 파일로 데이터를 내보내려면:

1. HP Password Manager 가져오기 및 내보내기 페이지에서 **Export data from an HP Client Security backup file**(HP Client Security 백업 파일로 데이터 내보내기)을 클릭하거나 누릅니다.
2. ID 를 확인한 후 **다음**을 클릭하거나 누릅니다.
3. 백업 파일의 이름을 입력합니다. 파일은 기본적으로 문서 폴더에 저장됩니다. 다른 위치를 지정하려면 **찾아보기**를 클릭하거나 누릅니다.
4. 파일을 보호하기 위한 암호를 입력하고 확인한 다음 **저장**을 클릭하거나 누릅니다.

### 설정

Password Manager 의 개인 설정을 다음과 같이 지정할 수 있습니다.

- **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.

- **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 클릭하거나 누른 다음 새로운 키 조합을 입력합니다. 조합에는 ctrl, alt 또는 shift 중 하나 이상과 임의의 알파벳 또는 숫자 키를 포함할 수 있습니다.

  Windows 또는 Windows 응용프로그램용으로 예약된 조합은 사용할 수 없습니다.

- 기본값으로 설정을 되돌리려면 **기본값 복원**을 클릭하거나 누릅니다.

## 고급 설정

관리자는 HP Client Security 홈 페이지에서 **Gear**(기어) (설정) 아이콘을 선택하여 다음 옵션에 액세스할 수 있습니다.

- **Administrator Policies**(관리자 정책)—관리자를 위한 로그온과 세션 정책을 구성할 수 있습니다.
- **Standard User Policies**(표준 사용자 정책)—표준 사용자를 위한 로그온과 세션 정책을 구성할 수 있습니다.
- **보안 기능**—강력한 인증을 사용하여 Windows 계정을 보호하거나 Windows 를 시작하기 전에 인증을 활성화하여 컴퓨터의 보안을 증가시킬 수 있습니다.
- **사용자**—사용자 및 인증 정보를 관리할 수 있습니다.
- **My Policies**(내 정책)—자신의 인증 정책과 등록 상태를 검토할 수 있습니다.
- **백업 및 복원**—HP Client Security 데이터를 백업하거나 복원할 수 있습니다.
- **About HP Client Security**(HP Client Security 정보)—HP Client Security 에 대한 버전 정보를 표시합니다.

## 관리자 정책

이 컴퓨터의 관리자를 위한 로그온과 세션 정책을 구성할 수 있습니다. 이곳에서 설정한 로그온 정책은 로컬 관리자가 Windows 에 로그온하는 데 필요한 인증 정보를 관리합니다. 이곳에서 설정한 세션 정책은 로컬 관리자가 Windows 세션 내에서 ID 를 확인하는 데 필요한 인증 정보를 관리합니다.

기본적으로 모든 새 정책 또는 변경된 정책은 **적용**을 누르거나 클릭한 직후에 시행됩니다.

새 정책을 추가하려면:

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **Administrator Policies**(관리자 정책)를 클릭하거나 누릅니다.
3. **Add new policy**(새 정책 추가)를 클릭하거나 누릅니다.
4. 아래 화살표를 클릭하여 새 정책을 위한 기본 및 보조 인증 정보(선택 사항)를 선택한 다음 **추가**를 클릭하거나 누릅니다.
5. **적용**을 누릅니다.

새 정책 또는 변경된 정책의 시행을 연기하려면:

1. **Enforce this policy immediately**(이 정책을 즉시 시행)를 클릭하거나 누릅니다.
2. **Enforce this policy on the specific date**(특정한 날짜에 이 정책 시행)를 선택합니다.
3. 날짜를 입력하거나 팝업 달력을 사용하여 이 정책을 시행할 날짜를 선택합니다.
4. 원할 경우 새 정책에 대해 사용자에게 알릴 시간을 선택합니다.
5. **적용**을 누릅니다.

## 표준 사용자 정책

이 컴퓨터의 표준 사용자를 위한 로그온과 세션 정책을 구성할 수 있습니다. 이곳에서 설정한 로그온 정책은 표준 사용자가 Windows 에 로그온하는 데 필요한 인증 정보를 관리합니다. 이곳에서 설정한 세션 정책은 표준 사용자가 Windows 세션 내에서 ID 를 확인하는 데 필요한 인증 정보를 관리합니다.

기본적으로 모든 새 정책 또는 변경된 정책은 **적용**을 누르거나 클릭한 직후에 시행됩니다.

새 정책을 추가하려면:

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **표준 사용자 정책**을 클릭하거나 누릅니다.
3. **Add new policy**(새 정책 추가)를 클릭하거나 누릅니다.
4. 아래 화살표를 클릭하여 새 정책을 위한 기본 및 보조 인증 정보(선택 사항)를 선택한 다음 **추가**를 클릭하거나 누릅니다.
5. **적용**을 누릅니다.

새 정책 또는 변경된 정책의 시행을 연기하려면:

1. **Enforce this policy immediately**(이 정책을 즉시 시행)를 클릭하거나 누릅니다.
2. **Enforce this policy on the specific date**(특정한 날짜에 이 정책 시행)를 선택합니다.
3. 날짜를 입력하거나 팝업 달력을 사용하여 이 정책을 시행할 날짜를 선택합니다.
4. 원할 경우 새 정책에 대해 사용자에게 알릴 시간을 선택합니다.
5. **적용**을 누릅니다.

# 보안 기능

컴퓨터에 대한 무단 액세스를 방지하는 데 도움이 되는 HP Client Security 기능을 활성화할 수 있습니다.

보안 기능을 설정하려면:

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **보안 기능**을 클릭하거나 누릅니다.
3. 확인란을 선택하여 보안 기능을 활성화한 다음 **적용**을 클릭하거나 누릅니다. 기능을 많이 선택할수록 컴퓨터의 보안이 강화됩니다.

   이러한 설정은 모든 사용자에게 적용됩니다.

   - **Windows 로그온 보안**—액세스하려는 사용자에게 HP Client Security 인증 정보를 요구하여 Windows 계정을 보호합니다.
   - **사전 부팅 보안(파워온 인증)**—Windows 가 시작되기 전에 컴퓨터를 보호합니다. BIOS 에서 지원하지 않을 경우 이 선택 기능은 사용할 수 없습니다.
   - **One Step logon 허용**—이 설정을 사용하면 파워온 인증 또는 Drive Encryption 수준에서 이전에 인증을 수행한 경우 Windows 로그온을 건너뛸 수 있습니다.
4. **사용자**를 클릭하거나 누른 다음 사용자의 타일을 클릭하거나 누릅니다.

# 사용자

이 컴퓨터의 HP Client Security 사용자를 모니터링하고 관리할 수 있습니다.

다른 Windows 사용자를 HP Client Security 에 추가하려면:

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **사용자**를 클릭하거나 누릅니다.
3. **Add another Windows user to HP Client Security**(다른 Windows 사용자를 HP Client Security 에 추가)를 클릭하거나 누릅니다.
4. 추가할 사용자 이름을 입력한 다음 **확인**을 클릭하거나 누릅니다.
5. 사용자의 Windows 암호를 입력합니다.

   추가된 사용자의 타일이 사용자 페이지에 표시됩니다.

HP Client Security 에서 Windows 사용자를 삭제하려면:

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **사용자**를 클릭하거나 누릅니다.
3. 삭제하려는 사용자 이름을 클릭하거나 누릅니다.
4. **사용자 삭제**를 클릭하거나 누른 다음 **예**를 눌러 확인합니다.

사용자에 대해 시행된 로그온과 세션 정책의 요약을 표시하려면:

▲ **사용자**를 클릭하거나 누른 다음 사용자의 타일을 클릭하거나 누릅니다.

# 내 정책

인증 정책과 등록 상태를 표시할 수 있습니다. 내 정책 페이지는 관리자 정책과 표준 사용자 정책 페이지도 제공합니다.

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **My Policies**(내 정책)를 클릭하거나 누릅니다.

   현재 로그온한 사용자에 대해 시행된 로그온과 세션 정책이 표시됩니다.

내 정책 페이지는 25페이지의관리자 정책 및 25페이지의표준 사용자 정책에 대한 링크도 제공합니다.

# 데이터 백업 및 복원

HP Client Security 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 만 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 Client Security 를 설치해야 합니다.

데이터를 백업하려면:

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **Administrator Policies**(관리자 정책)를 클릭하거나 누릅니다.
3. **백업 및 복원**을 클릭하거나 누릅니다.
4. **백업**을 클릭하거나 누른 다음 ID 를 확인합니다.
5. 백업에 포함하려는 모듈을 선택한 후 **다음**을 클릭하거나 누릅니다.
6. 저장 파일의 이름을 입력합니다. 파일은 기본적으로 문서 폴더에 저장됩니다. 다른 위치를 지정하려면 **찾아보기** 를 클릭하거나 누릅니다.
7. 파일을 보호하려면 암호를 입력하고 확인합니다.
8. **저장**을 클릭하거나 누릅니다.

데이터를 복원하려면:

1. HP Client Security 홈 페이지에서 **Gear**(기어) 아이콘을 클릭하거나 누릅니다.
2. 고급 설정 페이지에서 **Administrator Policies**(관리자 정책)를 클릭하거나 누릅니다.
3. **백업 및 복원**을 클릭하거나 누릅니다.
4. **복원**을 선택한 다음 ID 를 확인합니다.
5. 이전에 만든 저장 파일을 선택합니다. 제공된 필드에 경로를 입력합니다. 다른 위치를 지정하려면 **찾아보기** 를 클릭하거나 누릅니다.
6. 파일을 보호하는 데 사용되는 암호를 입력한 후 **다음**을 클릭하거나 누릅니다.
7. 데이터를 복원할 모듈을 선택합니다.
8. **복원**을 클릭하거나 누릅니다.

# 5 HP Drive Encryption(일부 모델만 해당)

HP Drive Encryption 은 컴퓨터의 데이터를 암호화함으로써 데이터를 완벽하게 보호합니다. Drive Encryption 이 활성화되어 있는 경우 Drive Encryption 로그온 화면에서 로그온을 해야 Windows® 운영 체제가 시작됩니다.

Windows 관리자는 HP Client Security 홈 화면을 사용하여 Drive Encryption 활성화, 암호화 키 백업, 암호화를 위한 드라이브 또는 파티션을 선택하거나 선택 해제할 수 있습니다. 자세한 내용은 HP Client Security 소프트웨어 도움말을 참조하십시오.

Drive Encryption 에서 수행할 수 있는 작업은 다음과 같습니다.

- Drive Encryption 설정 선택:
  - 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 Client Security 를 열고 Drive Encryption 에 액세스할 수 있습니다.

1. 시작 화면에서 **HP Client Security** 응용프로그램을 클릭하거나 누릅니다(Windows 8).

   또는

   Windows 바탕 화면에서 작업 표시줄 오른쪽 끝의 알림 영역에 있는 **HP Client Security** 아이콘을 두 번 클릭하거나 두 번 누릅니다.

2. **Drive Encryption** 아이콘을 클릭하거나 누릅니다.

# 일반 작업

## 표준 하드 드라이브에 대한 Drive Encryption 활성화

소프트웨어 암호화를 사용하여 표준 하드 드라이브를 암호화합니다. 드라이브 또는 디스크 파티션을 암호화하려면 다음과 같이 하십시오.

1. **Drive Encryption** 을 시작합니다. 자세한 내용은 28페이지의 Drive Encryption 열기을 참조하십시오.
2. 암호화할 드라이브나 파티션의 확인란을 선택한 다음 **백업 키**를 클릭하거나 누릅니다.

**참고:** 향상된 보안을 위해 **보안 향상을 위해 절전 모드 비활성화** 확인란을 선택합니다. 절전 모드를 비활성화하면 드라이브의 잠금을 해제하는 데 사용되는 인증 정보가 메모리에 저장될 위험이 전혀 없습니다.

3. 하나 이상의 백업 옵션을 선택한 다음 **백업**을 클릭하거나 누릅니다. 자세한 내용은 32페이지의 암호화 키 백업을 참조하십시오.
4. 암호화 키가 백업되는 동안 작업을 계속할 수 있습니다. 컴퓨터를 재부팅하지 마십시오.

**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 Client Security 소프트웨어 도움말을 참조하십시오.

## 자가 암호화 드라이브에 대한 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. 하드웨어 암호화가 소프트웨어 암호화보다 훨씬 빠릅니다. 그러나 암호화할 디스크 파티션을 선택할 수 없습니다. 모든 디스크 파티션을 포함하여 전체 디스크가 암호화됩니다.

특정 파티션을 암호화하려면 소프트웨어 암호화를 사용해야 합니다. **Only allow hardware encryption for Self-Encrypting Drives (SEDs)**(자체 암호화 드라이브(SED)에 대해 하드웨어 암호화만 허용) 확인란을 선택 해제해야 합니다.

자체 암호화 드라이브의 Drive Encryption 을 활성화하려면 다음과 같이 하십시오.

1. **Drive Encryption** 을 시작합니다. 자세한 내용은 28페이지의 Drive Encryption 열기을 참조하십시오.
2. 암호화할 드라이브의 확인란을 선택한 다음 **백업 키**를 클릭하거나 누릅니다.

**참고:** 향상된 보안을 위해 **추가된 보안에 대해 절전 모드 비활성화** 확인란을 선택합니다. 절전 모드를 비활성화하면 드라이브의 잠금을 해제하는 데 사용되는 인증 정보가 메모리에 저장될 위험이 전혀 없습니다.

3. 하나 이상의 백업 옵션을 선택한 다음 **백업**을 클릭하거나 누릅니다. 자세한 내용은 32페이지의 암호화 키 백업을 참조하십시오.
4. 암호화 키가 백업되는 동안 작업을 계속할 수 있습니다. 컴퓨터를 재부팅하지 마십시오.

**참고:** 자체 암호화 드라이브의 경우 컴퓨터를 종료할 것인지 묻는 메시지가 나타납니다.

자세한 내용은 HP Client Security 소프트웨어 도움말을 참조하십시오.

## Drive Encryption 비활성화

1. **Drive Encryption** 을 시작합니다. 자세한 내용은 28페이지의 Drive Encryption 열기을 참조하십시오.
2. 모든 암호화된 드라이브의 확인란을 선택 해제한 다음 **적용**을 클릭하거나 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 이 활성화된 후 사용자 계정을 등록하면 컴퓨터를 켤 때 Drive Encryption 로그인 화면에 로그인해야 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 **Disable sleep mode for increased security**(보안 향상을 위해 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 Client Security 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 로그인할 수 있습니다.

### 단일 사용자 로그온:

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

### 다중 사용자 로그온:

1. **Select user to logon**(로그온할 사용자 선택) 페이지의 드롭다운 목록에서 로그온할 사용자를 선택하고 **다음**을 클릭하거나 누릅니다.
2. **로그온** 페이지에서 Windows 암호 또는 스마트 카드 PIN 을 입력하거나 등록된 손가락을 인식시킵니다.

**참고:** 다음 스마트 카드가 지원됩니다.

### 지원되는 스마트 카드

- Gemalto Cyberflex Access 64k V2c

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

## 추가 하드 드라이브 암호화

HP Drive Encryption 을 사용하여 하드 드라이브를 암호화하여 데이터를 보호하는 것이 좋습니다. 활성화 후에 다음 단계를 따라 추가된 모든 하드 드라이브나 만들어진 파티션을 암호화할 수 있습니다.

1. **Drive Encryption** 을 시작합니다. 자세한 내용은 28페이지의 Drive Encryption 열기을 참조하십시오.
2. 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 을 사용하여 컴퓨터에 있는 모든 하드 드라이브의 암호화 상태(암호화되지 않음 또는 암호화됨)를 보고 변경할 수 있습니다.

- 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)

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

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

1. **Drive Encryption** 을 시작합니다. 자세한 내용은 28페이지의 Drive Encryption 열기을 참조하십시오.
2. **드라이브 상태**에서 암호화 또는 암호 해제하려는 각 드라이브 파티션 옆의 확인란을 선택 또는 해제한 다음 **적용**을 클릭하거나 누릅니다.

**참고:** 파티션이 암호화 또는 암호 해제 중인 경우 진행 표시줄에는 파티션 암호화 진행률이 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.

## 디스크 관리

- **별명**—식별을 쉽게 하도록 드라이브나 파티션 이름을 지정할 수 있습니다.
- **Disconnected drives**(연결이 끊어진 드라이브)—Drive Encryption 은 컴퓨터에서 제거된 디스크를 추적할 수 있습니다. 컴퓨터에서 제거된 디스크는 자동으로 연결 끊김 목록으로 이동됩니다. 디스크가 시스템으로 반환된 경우 연결됨 목록에 다시 나타납니다.
- 연결이 끊어진 드라이브를 더 추적하거나 관리할 필요가 없는 경우 연결이 끊어진 드라이브를 연결이 끊어짐 목록에서 제거할 수 있습니다.
- Drive Encryption 는 모든 연결된 드라이브의 확인란을 선택 해제하고 연결 끊김 목록이 빌 때까지 활성 상태를 유지합니다.

## 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.

1. **Drive Encryption** 을 시작합니다. 자세한 내용은 28페이지의 Drive Encryption 열기을 참조하십시오.
2. 드라이브의 확인란을 선택한 다음 **백업 키**를 클릭하거나 누릅니다.
3. **Create HP Drive Encryption recovery key**(HP Drive Encryption 복구 키 만들기) 아래에서 다음 옵션 중 하나 이상을 선택합니다.
   - **이동식 저장소**—확인란을 선택한 다음 암호화 키를 저장할 저장 장치를 선택합니다.
   - **SkyDrive**—확인란을 선택합니다. 인터넷에 연결되어 있어야 합니다. Microsoft SkyDrive 에 로그인한 다음 **예**를 클릭하거나 누릅니다.

     **참고:** SkyDrive 에 저장된 HP Drive Encryption 백업 키를 사용하려면 SkyDrive 에서 이동식 저장 장치로 다운로드한 다음 저장 장치를 이 컴퓨터에 삽입해야 합니다.

   - **TPM**(일부 모델만 해당)—TPM 암호를 사용하여 데이터를 복구할 수 있습니다.

     **주의:** TPM 이 지워지고 컴퓨터가 손상된 경우 백업에 대한 액세스를 잃을 수 있습니다. 이 방법을 선택한 경우 다른 백업 방법도 선택해야 합니다.
4. **백업**을 클릭하거나 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 Drive Encryption 에 있는 **백업 키** 옵션을 선택하여 복구를 수행할 수 있습니다.

1. 백업 키를 저장한 이동식 저장 장치를 넣습니다.
2. 컴퓨터의 전원을 켭니다.
3. HP Drive Encryption 로그인 대화 상자가 표시되면 **복구**를 클릭하거나 누릅니다.
4. 백업 키가 들어 있는 파일 경로 또는 이름을 입력한 다음 **복구**를 클릭하거나 누릅니다.
5. 확인 대화 상자가 표시되면 **확인**을 클릭하거나 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 HP Client Security 소프트웨어 도움말을 참조하십시오.

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

1. 컴퓨터의 전원을 켭니다.
2. HP Drive Encryption 페이지가 표시되면 사용자 로그온 페이지로 이동합니다.
3. **SpareKey** 를 누릅니다.

**참고:** SpareKey 를 HP Client Security 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 로그인 화면에서 SpareKey 를 사용하여 로그온하면 Windows 로그온에서 추가 인증 정보로 사용자 계정에 액세스해야 합니다. 복구를 수행한 후 암호를 재설정하는 것이 좋습니다.

# 6 HP File Sanitizer(일부 모델만 해당)

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

File Sanitizer 는 다음과 같은 종류의 장치를 삭제하거나 블리치하는 데 사용할 수 없습니다.

- SSD 장치를 스팬하는 RAID 볼륨을 비롯한 SSD(Solid State Drive)
- USB, Firewire 또는 eSATA 인터페이스에 연결된 외장 드라이브

SSD 에서 파쇄 또는 블리치 작업을 시도하면 경고 메시지가 표시되고 작업이 수행되지 않습니다.

## 파쇄

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

향후 파쇄 시간을 예약하거나 HP Client Security 홈 화면에서 **File Sanitizer** 아이콘을 선택하거나 Windows 바탕 화면에서 **File Sanitizer** 아이콘을 사용하여 파쇄를 수동으로 활성화할 수 있습니다. 자세한 내용은 36페이지의파쇄 일정 설정, 38페이지의오른쪽 클릭 파쇄 또는 38페이지의파쇄 작업 수동으로 시작를 참조하십시오.

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

## 여유 공간 블리치

Windows 에서 자산을 삭제해도 하드 드라이브에서는 자산의 컨텐츠가 완전히 제거되지 않습니다. Windows 에서는 자산에 대한 참조 또는 하드 드라이브의 자산 위치만 삭제합니다. 자산의 컨텐츠는 다른 자산이 하드 드라이브의 동일한 위치에 새 정보를 덮어쓸 때까지 하드 드라이브에 그대로 유지됩니다.

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

**참고:** 여유 공간 블리치는 파쇄된 자산에 대해 추가 보안을 제공하지 않습니다.

향후 여유 공간 블리치 시간을 예약하거나 HP Client Security 홈 화면에서 **File Sanitizer** 아이콘을 선택하거나 Windows 바탕 화면에서 **File Sanitizer** 아이콘을 사용하여 이전에 파쇄한 자산의 여유 공간 블리치를 수동으로 활성화할 수 있습니다. 자세한 내용은 36페이지의여유 공간 블리치 예약 설정, 38페이지의여유 공간 블리치를 수동으로 시작 또는 37페이지의 File Sanitizer 아이콘 사용를 참조하십시오.

# File Sanitizer 열기

1. 시작 화면에서 **HP Client Security** 응용프로그램을 클릭하거나 누릅니다(Windows 8).

   또는

   Windows 바탕 화면에서 작업 표시줄 오른쪽 끝의 알림 영역에 있는 **HP Client Security** 아이콘을 두 번 클릭하거나 두 번 누릅니다.

2. **데이터** 아래에서 **File Sanitizer** 를 클릭하거나 누릅니다.

또는

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

– 또는 –

▲ Windows 바탕 화면에서 **File Sanitizer** 아이콘을 마우스 오른쪽 버튼으로 클릭하거나 길게 누른 다음 **File Sanitizer 열기**를 선택합니다.

# 설정 절차

**파쇄**—File Sanitizer 는 선택한 범주의 자산을 안전하게 삭제하거나 파쇄합니다.

1. **파쇄** 아래에서 파쇄할 각 파일 형식에 해당하는 확인란을 선택하거나 이러한 파일을 파쇄하지 않으려면 확인란 선택을 취소합니다.
   - **휴지통**—휴지통에 있는 모든 항목을 파쇄합니다.
   - **임시 시스템 파일**—시스템 임시 폴더에 있는 모든 파일을 파쇄합니다. 다음 환경 변수는 순서대로 검색되며 첫 번째로 검색된 경로가 시스템 폴더가 됩니다.
     - TMP
     - TEMP
   - **임시 인터넷 파일**—더욱 빠르게 볼 수 있도록 웹 브라우저에서 저장한 웹 페이지, 이미지 및 미디어 사본을 파쇄합니다.
   - **쿠키**—로그인 정보 등 웹 사이트에서 기본 설정을 저장하기 위해 컴퓨터에 저장한 모든 파일을 파쇄합니다.
2. 파쇄를 시작하려면 **파쇄**를 클릭하거나 누릅니다.

**블리치**—임의의 데이터를 여유 공간에 쓰고 삭제한 항목이 복원되지 않도록 합니다.

▲ 블리치를 시작하려면 **블리치**를 클릭하거나 누릅니다.

**File Sanitizer Options**(File Sanitizer 옵션)—확인란을 선택하여 다음 각 옵션을 활성화하거나 확인란을 선택 해제하여 옵션을 비활성화합니다.

- **Enable Desktop icon**(바탕 화면 아이콘 활성화)—Windows 바탕 화면에 File Sanitizer 아이콘을 표시합니다.
- **Enable right-click**(오른쪽 클릭 활성화)—자산을 마우스 오른쪽 버튼으로 클릭하거나 길게 누른 다음 **HP File Sanitizer – 파쇄**를 선택합니다.
- **Ask for Windows password before manual shredding**(수동 파쇄 전에 Windows 암호 묻기)—항목을 수동으로 파쇄하기 전에 Windows 암호를 사용한 인증을 요구합니다.
- **Shred Cookies and Temporary Internet Files on browser close**(브라우저를 닫을 때 쿠키와 임시 인터넷 파일 파쇄)—웹 브라우저를 닫을 때 브라우저 URL 히스토리와 같은 선택한 웹 관련 자산을 모두 파쇄합니다.

## 파쇄 일정 설정

자동으로 파쇄를 수행할 시간을 예약하거나 언제든지 자산을 수동으로 파쇄할 수도 있습니다. 자세한 내용은 35페이지의설정 절차을 참조하십시오.

1. File Sanitizer 를 연 다음 **설정**을 클릭하거나 누릅니다.
2. 선택한 자산을 파쇄할 향후 시간을 예약하려면 **Shred Schedule**(파쇄 일정) 아래에서 **안 함**, **한 번**, **매일**, **매주** 또는 **Monthly**(매월)를 선택한 다음 날짜와 시간을 선택합니다.
   a. 시간, 분 또는 AM/PM 필드를 클릭하거나 누릅니다.
   b. 원하는 값이 다른 필드와 같은 수준에 표시될 때까지 스크롤합니다.
   c. 시간 설정 필드 주변의 흰색 공간을 클릭하거나 누릅니다.
   d. 올바른 일정이 선택될 때까지 각 필드에 대해 반복합니다.
3. 다음 4 가지 유형의 자산이 나열됩니다.
   - **휴지통**—휴지통에 있는 모든 항목을 파쇄합니다.
   - **임시 시스템 파일**—시스템 임시 폴더에 있는 모든 파일을 파쇄합니다. 다음 환경 변수는 순서대로 검색되며 첫 번째로 검색된 경로가 시스템 폴더가 됩니다.
     - TMP
     - TEMP
   - **임시 인터넷 파일**—더욱 빠르게 볼 수 있도록 웹 브라우저에서 저장한 웹 페이지, 이미지 및 미디어 사본을 파쇄합니다.
   - **쿠키**—로그인 정보 등 웹 사이트에서 기본 설정을 저장하기 위해 컴퓨터에 저장한 모든 파일을 파쇄합니다.

   선택한 경우 이러한 자산은 예약된 시간에 파쇄됩니다.
4. 파쇄할 추가 사용자 정의 자산을 선택하려면:
   a. **Scheduled Shred List**(예약된 파쇄 목록) 아래에서 **폴더 추가**를 클릭하거나 누른 다음 파일 또는 폴더로 이동합니다.
   b. **열기**를 클릭하거나 누른 다음 **확인**을 클릭하거나 누릅니다.

   예약된 파쇄 목록에서 자산을 제거하려면 자산에 해당하는 확인란 선택을 취소합니다.

## 여유 공간 블리치 예약 설정

여유 공간 블리치는 파쇄된 자산에 대해 추가 보안을 제공하지 않습니다.

1. File Sanitizer 를 연 다음 **설정**을 클릭하거나 누릅니다.
2. 하드 드라이브를 블리치할 향후 시간을 예약하려면 **블리치 예약**에서 **안 함**, **한 번**, **매일**, **매주** 또는 **매달**을 선택한 다음 날짜와 시간을 선택합니다.
   a. 시간, 분 또는 AM/PM 필드를 클릭하거나 누릅니다.
   b. 원하는 시간이 다른 필드와 같은 수준에 표시될 때까지 스크롤합니다.
   c. 시간 설정 필드 주변의 흰색 공간을 클릭하거나 누릅니다.
   d. 올바른 일정이 선택될 때까지 반복합니다.

**참고:** 여유 공간 블리치 작업에는 상당한 시간이 소요될 수 있습니다. 컴퓨터가 AC 전원에 연결되어 있는지 확인하십시오. 여유 공간 블리치 작업은 백그라운드로 수행되지만 프로세서 사용 증가로 인해 컴퓨터의 성능에 영향을 끼칠 수 있습니다. 수 시간 후 또는 컴퓨터를 사용하고 있지 않을 때 여유 공간 블리치 기능을 사용할 수 있습니다.

## 파쇄로부터 파일 보호

파일 또는 폴더가 파쇄되지 않도록 설정하려면:

1. File Sanitizer 를 연 다음 **설정**을 클릭하거나 누릅니다.
2. **Never Shred List**(파쇄 안 함 목록) 아래에서 **폴더 추가**를 클릭하거나 누른 다음 파일 또는 폴더로 이동합니다.
3. **열기**를 클릭하거나 누른 다음 **확인**을 클릭하거나 누릅니다.

**참고:** 이 목록의 파일은 목록에 남아 있는 한 보호됩니다.

제외 목록에서 자산을 제거하려면 자산에 해당하는 확인란 선택을 취소합니다.

# 일반 작업

File Sanitizer 를 이용해서 다음의 작업을 수행합니다.

- **File Sanitizer 아이콘을 사용하여 파쇄 시작**—Windows 바탕 화면의 **File Sanitizer** 아이콘에 파일을 끌어다 놓을 수 있습니다. 자세한 내용은 37페이지의 File Sanitizer 아이콘 사용을 참조하십시오.
- **특정 자산 또는 선택한 모든 자산을 수동으로 파쇄**—예정된 파쇄 시간을 기다리지 않고 언제든지 항목을 파쇄합니다. 자세한 내용은 38페이지의오른쪽 클릭 파쇄 또는 38페이지의파쇄 작업 수동으로 시작를 참조하십시오.
- **여유 공간 블리치 수동 활성화**—여유 공간 블리치를 언제든지 활성화합니다. 자세한 내용은 38페이지의여유 공간 블리치를 수동으로 시작을 참조하십시오.
- **로그 파일 보기**—최근 파쇄 또는 여유 공간 블리치 작업에서 발생한 오류 또는 실패 로그가 들어 있는 파쇄 또는 여유 공간 블리치 로그 파일을 봅니다. 자세한 내용은 39페이지의로그 파일 보기을 참조하십시오.

**참고:** 파쇄 또는 여유 공간 블리치 작업은 상당한 시간이 소요될 수 있습니다. 파쇄 및 여유 공간 블리칭은 백그라운드로 진행되지만 프로세서 사용량이 늘어나 컴퓨터의 성능에 영향을 줄 수 있습니다.

## File Sanitizer 아이콘 사용

**주의:** 파쇄된 자산을 복구할 수 없습니다. 수동으로 파쇄할 항목을 신중하게 고려하여 선택합니다.

파쇄 작업을 수동으로 시작하면 File Sanitizer 보기의 표준 파쇄 목록이 파쇄됩니다(35페이지의설정 절차 참조).

다음과 같은 방법 중 하나로 파쇄 작업을 수동으로 시작할 수 있습니다.

1. File Sanitizer 를 연 다음(35페이지의 File Sanitizer 열기 참조), **파쇄**를 클릭하거나 누릅니다.
2. 확인 대화 상자가 열리면 파쇄하려는 자산이 선택되었는지 확인한 다음 **확인**을 클릭하거나 누릅니다.

– 또는 –

1. Windows 바탕 화면에서 **File Sanitizer** 아이콘을 마우스 오른쪽 버튼으로 클릭하거나 길게 누른 다음 **지금 파쇄**를 클릭하거나 누릅니다.
2. 확인 대화 상자가 열리면 파쇄하려는 자산이 선택되었는지 확인한 다음 **파쇄**를 클릭하거나 누릅니다.

## 오른쪽 클릭 파쇄

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

File Sanitizer 보기에서 **Enable right-click shredding**(오른쪽 클릭 파쇄 활성화)을 선택한 경우 다음과 같이 자산을 파쇄할 수 있습니다.

1. 파쇄하려는 문서나 폴더로 이동합니다.
2. 파일이나 폴더를 마우스 오른쪽 버튼으로 클릭하거나 길게 눌러 **HP File Sanitizer – Shred**(HP File Sanitizer – 파쇄)를 선택합니다.

## 파쇄 작업 수동으로 시작

⚠ **주의:** 파쇄된 자산을 복구할 수 없습니다. 수동으로 파쇄할 항목을 신중하게 고려하여 선택합니다.

파쇄 작업을 수동으로 시작하면 File Sanitizer 보기의 표준 파쇄 목록이 파쇄됩니다(35페이지의설정 절차 참조).

다음과 같은 방법 중 하나로 파쇄 작업을 수동으로 시작할 수 있습니다.

1. File Sanitizer 를 연 다음(35페이지의 File Sanitizer 열기 참조), **파쇄**를 클릭하거나 누릅니다.
2. 확인 대화 상자가 열리면 파쇄하려는 자산이 선택되었는지 확인한 다음 **확인**을 클릭하거나 누릅니다.

– 또는 –

1. Windows 바탕 화면에서 **File Sanitizer** 아이콘을 마우스 오른쪽 버튼으로 클릭하거나 길게 누른 다음 **지금 파쇄**를 클릭하거나 누릅니다.
2. 확인 대화 상자가 열리면 파쇄하려는 자산이 선택되었는지 확인한 다음 **파쇄**를 클릭하거나 누릅니다.

## 여유 공간 블리치를 수동으로 시작

블리치 작업을 수동으로 시작하면 File Sanitizer 보기의 표준 파쇄 목록이 블리치됩니다(35페이지의설정 절차 참조).

다음과 같은 방법 중 하나로 블리치 작업을 수동으로 시작할 수 있습니다.

1. File Sanitizer 를 연 다음(35페이지의 File Sanitizer 열기 참조), **블리치**를 클릭하거나 누릅니다.
2. 확인 대화 상자가 표시되면 **확인**을 클릭하거나 누릅니다.

또는

1. Windows 바탕 화면에서 **File Sanitizer** 아이콘을 마우스 오른쪽 버튼으로 클릭하거나 길게 누른 다음 **지금 블리치**를 클릭하거나 누릅니다.
2. 확인 대화 상자가 표시되면 **블리치**를 클릭하거나 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:** 파쇄 또는 블리치된 파일은 로그 파일에 표시되지 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 폴더에 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 폴더에 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

# 7 HP Device Access Manager(일부 모델만 해당)

HP 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 43페이지의관리되지 않는 장치 클래스를 참조하십시오.

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

- 각 사용자에 대해 장치 프로필이 만들어져 액세스가 허용된 장치인지 거부된 장치인지 보여줍니다.
- JITA(Just In Time Authentication) 기능을 이용하면 미리 정의된 사용자가 자신을 스스로 인증하여 일반적으로는 액세스할 수 없는 장치에 액세스할 수 있습니다.
- 관리자와 신뢰할 수 있는 사용자를 장치 관리자 그룹에 추가하면 Device Access Manager 가 부과한 장치 액세스 제한을 면제받을 수 있습니다. 이 그룹의 멤버십은 고급 설정을 통해 관리됩니다.
- 장치 액세스는 그룹 멤버십을 기준으로 개별 사용자별로 허용하거나 거부할 수 있습니다.
- CD-ROM 드라이브나 DVD 드라이브와 같은 장치 클래스의 경우, 읽기 권한과 쓰기 권한을 개별적으로 허용 또는 거부할 수 있습니다.

HP Device Access Manager 는 HP Client Security 설치 마법사를 완료하는 동안 다음 설정으로 자동 구성됩니다.

- 관리자 및 사용자에 대해 JITA(Just In Time Authentication) 이동식 미디어가 활성화됩니다.
- 장치 정책은 다른 장치에 대한 모든 권한을 허용합니다.

## Device Access Manager 열기

1. 시작 화면에서 **HP Client Security** 응용프로그램을 클릭하거나 누릅니다(Windows 8).

   또는

   Windows 바탕 화면에서 작업 표시줄 오른쪽 끝의 알림 영역에 있는 **HP Client Security** 아이콘을 두 번 클릭하거나 두 번 누릅니다.

2. **장치** 아래에서 **Device Permissions**(장치 권한)를 클릭하거나 누릅니다.

   - 표준 사용자는 자신의 현재 장치 액세스 권한을 볼 수 있습니다(41페이지의사용자 보기 참조).
   - 관리자는 **변경**을 누른 다음 관리자 암호를 입력하여 컴퓨터에 현재 구성된 장치 액세스 권한을 보고 변경할 수 있습니다(41페이지의시스템 보기 참조).

## 사용자 보기

**Device Permission**(장치 권한)을 선택하면 사용자 보기가 표시됩니다. 정책에 따라 표준 사용자와 관리자는 이 컴퓨터에 있는 장치 클래스 또는 개별 장치에 대한 자신의 액세스 권한을 볼 수 있습니다.

- **현재 사용자**—현재 로그온한 사용자 이름이 표시됩니다.
- **장치 클래스**—장치 유형이 표시됩니다.
- **액세스**—장치 유형 또는 특정 장치에 현재 구성된 액세스 권한이 표시됩니다.
- **기간**—CD/DVD-ROM 드라이브 또는 이동식 디스크 드라이브에 액세스할 수 있는 시간 제한이 표시됩니다.
- **설정**—관리자는 Device Access Manager 에서 액세스를 제어하는 드라이브를 변경할 수 있습니다.

## 시스템 보기

시스템 보기에서 관리자는 사용자 그룹 또는 관리자 그룹에 대해 이 컴퓨터에 있는 장치에 대한 액세스 권한을 허용 또는 거부할 수 있습니다.

▲ 관리자는 **변경**을 누르고 관리자 암호를 입력한 후에 다음 옵션 중에서 선택하여 시스템 보기에 액세스할 수 있습니다.

- **Device Access Manager**—HP Device Access Manager 에서 Just In Time Authentication 을 켜거나 끄려면 **켜기** 또는 **끄기**를 클릭하거나 누릅니다.
- **Users and groups on this PC**(이 PC 의 사용자 및 그룹)—선택한 장치 클래스에 대한 액세스가 허용되거나 거부되는 사용자 그룹 또는 관리자 그룹을 표시합니다.
- **장치 클래스**—시스템에 설치되어 있거나 이전에 설치되었던 장치 클래스 및 장치를 표시합니다. 목록을 확장하려면 **+** 아이콘을 클릭합니다. 컴퓨터에 연결된 모든 장치가 표시되고 관리자 및 사용자 그룹이 확장되어 해당 구성원 자격을 보여줍니다. 장치 목록을 새로 고치려면 둥근 화살표(새로 고침) 아이콘을 클릭합니다.
  - 장치 클래스에는 대개 보호 기능이 적용되며 액세스 권한이 **허용**으로 설정된 경우 선택된 사용자 또는 그룹은 장치 클래스의 모든 장치에 액세스할 수 있습니다.
  - 특정 장치에도 보호 기능을 적용할 수 있습니다.
  - JITA(Just In Time Authentication)를 구성하면 선택된 사용자가 스스로 인증하여 DVD/CD-ROM 드라이브 또는 이동식 디스크 드라이브에 액세스할 수 있습니다. 자세한 내용은 42페이지의 JITA 구성을 참조하십시오.
  - 이동식 미디어(예: USB 플래시 드라이브), 직렬 및 병렬 포트, Bluetooth® 장치, 모뎀 장치, PCMCIA/ExpressCard 장치, 1394 장치, 지문 인식기 및 스마트 카드 리더 같은 다른 장치 클래스에 대한 액세스를 허용하거나 거부합니다. 지문 인식기와 스마트 카드 리더가 거부되는 경우 인증 정보로 사용할 수 있지만 세션 정책 수준에서는 사용할 수 없습니다.

    **참고:** Bluetooth 장치가 인증 정보로 사용되는 경우 Bluetooth 장치 액세스는 Device Access Manager 정책에 의해 제한되지 않아야 합니다.
  - 그룹 또는 장치 클래스 수준에서 설정을 선택하면 하위 개체에 설정을 적용할지 묻는 메시지가 나타납니다.

    **예**—설정이 전파됩니다.

    **아니요**—설정이 전파되지 않습니다.
  - DVD 및 CD-ROM 과 같은 일부 장치 클래스는 읽기 작업과 쓰기 작업에 대한 액세스를 별도로 허용하거나 거부하여 좀더 세부적으로 제어할 수 있습니다.

**참고:** 관리자 그룹을 사용자 목록에 추가할 수 없습니다.

- **액세스**—아래 화살표를 클릭하거나 누른 후에 다음 액세스 유형 중 하나를 선택하여 액세스를 허용하거나 거부합니다.
  - **허용 – 모든 권한**
  - **허용 – 읽기 전용**
  - **Allow – JITA Required**(허용 – JITA 필요)—자세한 내용은 42페이지의 JITA 구성을 참조하십시오.

    이 액세스 유형을 선택한 경우 **기간** 아래에서 아래 화살표를 클릭하거나 눌러 시간 제한을 선택합니다.
  - **거부**
- **기간**—아래 화살표를 클릭하거나 눌러 CD/DVD-ROM 드라이브 또는 이동식 디스크 드라이브 액세스를 위한 시간 제한을 선택합니다(42페이지의 JITA 구성 참조).

## JITA 구성

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

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

JITA 기간은 설정된 시간(분) 또는 무제한으로 인증됩니다. 무제한 사용자는 인증한 시간부터 시스템 로그오프 시간까지 장치에 액세스할 수 있습니다.

사용자에게 제한된 JITA 기간이 주어진 경우 JITA 기간이 만료되기 1 분 전에 액세스를 연장할 것인지 묻는 메시지가 나타납니다. 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
- 이동식 디스크 드라이브

### 사용자 또는 그룹용 JITA 정책 생성

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

1. **Device Access Manager** 를 시작한 다음 **변경**을 클릭하거나 누릅니다.
2. 사용자 또는 그룹을 선택한 다음 **이동식 디스크 드라이브** 또는 **DVD/CD-ROM 드라이브**에 대한 **액세스**에서 아래 화살표를 클릭하거나 누른 다음 **Allow – JITA Required**(허용 – JITA 필요)를 선택합니다.
3. **기간**에서 아래 화살표를 클릭하거나 눌러 JITA 액세스를 위한 기간을 선택합니다.

새로운 JITA 설정을 적용하려면 로그아웃 후 다시 로그인해야 합니다.

### 사용자 또는 그룹용 JITA 정책 비활성화

Just In Time Authentication 을 사용하여 관리자는 장치에 대한 사용자 또는 그룹의 액세스를 비활성화할 수 있습니다.

1. **Device Access Manager** 를 시작한 다음 **변경**을 클릭하거나 누릅니다.
2. 사용자 또는 그룹을 선택한 다음 **이동식 디스크 드라이브** 또는 **DVD/CD-ROM 드라이브**에 대한 **액세스**에서 아래 화살표를 클릭하거나 누른 다음 **거부**를 선택합니다.

사용자가 로그인하여 장치 액세스를 시도하면 액세스가 거부됩니다.

# 설정

**설정** 보기를 사용하면 관리자는 Device Access Manager 에서 액세스를 제어하는 드라이브를 보고 변경할 수 있습니다.

**참고:** 드라이브 문자 목록이 구성되어 있으면 Device Access Manager 가 활성화되어 있어야 합니다 (41페이지의시스템 보기 참조).

## 관리되지 않는 장치 클래스

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

- 입/출력 장치
  - CD-ROM
  - 디스크 드라이브
  - 플로피 디스크 컨트롤러(FDC)
  - 하드 디스크 컨트롤러(HDC)
  - 휴먼 인터페이스 장치(HID) 클래스
  - 적외선 휴먼 인터페이스 장치
  - 마우스
  - 멀티 포트 직렬
  - 키보드
  - 플러그 앤드 플레이(PnP) 프린터
  - 프린터
  - 프린터 업그레이드
- 전원
  - 고급 전원 관리(APM) 지원
  - 배터리
- 기타 장치
  - 컴퓨터
  - 디코더
  - 디스플레이

- Intel® 통합 디스플레이 드라이버
- Legacard
- 미디어 드라이버
- 미디움 체인저
- 메모리 기술
- 모니터
- 다기능
- Net client(네트워크 클라이언트)
- Net service(네트워크 서비스)
- Net trans(네트워크 전송)
- 프로세서
- SCSI 어댑터
- 보안 가속기
- 보안 장치
- 시스템
- 알 수 없음
- 볼륨
- 볼륨 스냅샷

# 8 HP Trust Circles

HP Trust Circles 는 폴더 파일 암호화를 편리한 신뢰할 수 있는 서클 문서 공유 기능과 결합하는 파일 및 문서 보안 응용프로그램입니다. 응용프로그램은 사용자 지정 폴더에 저장된 파일을 암호화하여 트러스트 서클 내의 파일을 보호합니다. 일단 보호된 파일은 트러스트 서클의 구성원만 사용하고 공유할 수 있습니다. 보호된 파일을 비구성원이 수신하는 경우 파일은 암호화된 상태를 유지하고 비구성원은 내용에 액세스할 수 없습니다.

## Trust Circles 열기

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

   – 또는 –

   Windows 바탕 화면에서 작업 표시줄 오른쪽 끝의 알림 영역에 있는 **HP Client Security** 아이콘을 두 번 클릭합니다.

2. **데이터** 아래에서 **Trust Circles** 를 클릭하거나 누릅니다.

## 시작

전자 메일 초대를 보내고 회신하는 방법은 두 가지가 있습니다.

- **Using Microsoft® Outlook**(Microsoft® Outlook 사용)—Microsoft Outlook 과 Trust Circles 를 사용하면 다른 Trust Circle 사용자의 Trust Circle 초대와 응답 처리가 자동화됩니다.
- **Using Gmail, Yahoo, Outlook.com or other email services (SMTP)**(Gmail, Yahoo, Outlook.com 또는 다른 전자 메일 서비스(SMTP) 사용)—이름, 전자 메일 주소 및 암호를 입력하면 Trust Circles 는 사용자 전자 메일 서비스를 사용하여 선택된 구성원에게 트러스트 서클에 참가하도록 전자 메일 초대를 보냅니다.

기본 프로파일을 설정하려면:

1. 이름과 전자 메일 주소를 입력한 후에 **다음**을 클릭하거나 누릅니다.

   이름은 트러스트 서클에 참가하도록 초대를 받은 모든 구성원에게 표시됩니다. 전자 메일 주소는 초대를 보내거나 받거나 회신하는 데 사용됩니다.

2. 전자 메일 계정의 암호를 입력하고 **다음**을 클릭하거나 누릅니다.

   전자 메일 설정이 정확한지 확인하기 위한 테스트 전자 메일을 받게 됩니다.

   **참고:** 컴퓨터는 네트워크에 연결되어 있어야 합니다.

3. **Trust Circle Name**(Trust Circle 이름) 필드에 트러스트 서클의 이름을 입력한 후 **다음**을 클릭하거나 누릅니다.

4. 구성원과 폴더를 추가한 후 **다음**을 클릭하거나 누릅니다. 선택된 모든 폴더에 트러스트 서클이 만들어지고 선택된 모든 구성원에게 전자 메일 초대를 보냅니다. 어떤 이유로 초대를 보낼 수 없는 경우 알림이 표시됩니다. **Trust Circles** 를 클릭한 다음 트러스트 서클을 두 번 클릭하거나 두 번 눌러 Trust Circle 보기에서 언제든지 다시 구성원을 초대할 수 있습니다. 자세한 내용은 46페이지의 Trust Circles 을 참조하십시오.

# Trust Circles

전자 메일 주소를 입력한 후 초기 설정 과정에서 또는 Trust Circle 보기에서 트러스트 서클을 만들 수 있습니다.

▲ Trust Circle 보기에서 **Create Trust Circle**(Trust Circle 만들기)을 클릭하거나 누른 다음 트러스트 서클의 이름을 입력합니다.

- 트러스트 서클에 구성원을 추가하려면 **구성원** 옆의 **M+** 아이콘을 클릭하거나 누른 다음 화면의 지시를 따릅니다.
- 트러스트 서클에 폴더를 추가하려면 **폴더** 옆의 **+** 아이콘을 클릭하거나 누른 다음 화면의 지시를 따릅니다.

## 트러스트 서클에 폴더 추가

### 새 트러스트 서클에 폴더 추가:

- 트러스트 서클을 만드는 동안 **폴더** 옆의 **+** 아이콘을 클릭하거나 눌러 폴더를 추가한 다음 화면의 설명을 따릅니다.

  – 또는 –

- Windows 탐색기에서 현재 트러스트 서클의 일부가 아닌 폴더를 마우스 오른쪽 버튼으로 클릭하거나 누른 상태에서 **Trust Circle** 을 선택한 다음 **Create Trust Circle from Folder**(폴더에서 Trust Circle 만들기)를 선택합니다.

**힌트:** 폴더를 하나 이상 선택할 수 있습니다.

### 기존 Trust Circle 에 폴더 추가:

- Trust Circle 보기에서 **Trust Circles** 를 클릭하고 기존 트러스트 서클을 두 번 클릭하거나 두 번 눌러 현재 폴더를 표시하고 **폴더** 옆의 **+** 아이콘을 클릭하거나 누른 다음 화면의 지시를 따릅니다.

  – 또는 –

- Windows 탐색기에서 현재 트러스트 서클의 일부가 아닌 폴더를 마우스 오른쪽 버튼으로 클릭하거나 누른 상태에서 **Trust Circle** 을 선택한 다음 **폴더에서 Trust Circle 에 추가**를 선택합니다.

**힌트:** 폴더를 하나 이상 선택할 수 있습니다.

트러스트 서클에 폴더가 추가되었으면 Trust Circles 는 폴더와 내용을 자동으로 암호화합니다. 모든 파일이 암호화되고 나면 알림이 표시됩니다. 또한 폴더 내의 암호화된 폴더 아이콘과 파일 아이콘에 완벽하게 보호됨을 나타내는 녹색 잠금 기호가 표시됩니다.

## 트러스트 서클에 구성원 추가

트러스트 서클에 구성원을 추가하려면 세 단계가 필요합니다.

1. **초대**—먼저, 트러스트 서클의 소유자가 구성원을 초대합니다. 초대 전자 메일은 여러 사용자 또는 배포 목록/그룹에 보낼 수 있습니다.
2. **수락**—초대를 받은 사람은 초대를 수락할지 거부할지 여부를 선택합니다. 초대를 받은 사람이 초대를 수락하면 초대를 보낸 사람에게 전자 메일 응답이 보내집니다. 초대가 그룹으로 보내지면 각 구성원은 초대를 받으며 수락할지 거부할지 선택합니다.
3. **등록**—초대를 보낸 사람에게는 트러스트 서클에 구성원을 추가할지 여부를 결정할 최종 기회가 있습니다. 초대를 보낸 사람이 구성원을 등록하기로 결정하면 초대를 받는 사람에게 응답을 확인하는 전자 메일이 보내집니다. 초대를 보낸 사람과 초대를 받는 사람은 초대 프로세스의 보안을

선택적으로 확인할 수 있습니다. 초대를 받은 사람에게 확인 코드가 표시되며, 초대를 보낸 사람에게 전화하여 코드를 읽어 주어야 합니다. 코드가 확인되면 초대를 보낸 사람은 최종 등록 전자 메일을 보낼 수 있습니다.

**새 트러스트 서클에 구성원 추가:**

▲ 트러스트 서클을 만드는 동안 **구성원** 옆의 **M+** 아이콘을 클릭하거나 눌러 구성원을 추가한 다음 화면의 지시를 따릅니다.

- Outlook 을 사용 중인 경우 Outlook 주소록에서 연락처를 선택한 다음 **확인**을 클릭합니다.
- 다른 메일 서비스를 사용 중인 경우 Trust Circle 에 수동으로 새 전자 메일 주소를 추가하거나 Trust Circle 에 등록된 전자 메일 주소에서 검색하도록 할 수도 있습니다.

**기존 트러스트 서클에 구성원 추가:**

▲ Trust Circle 보기에서 **Trust Circles** 를 클릭하고 기존 트러스트 서클을 두 번 클릭하거나 두 번 눌러 현재 구성원을 표시하고 **구성원** 옆의 **M+** 아이콘을 클릭하거나 누른 다음 화면의 지시를 따릅니다.

- Outlook 을 사용 중인 경우 Outlook 주소록에서 연락처를 선택한 다음 **확인**을 클릭합니다.
- 다른 메일 서비스를 사용 중인 경우 Trust Circle 에 수동으로 새 전자 메일 주소를 추가하거나 Trust Circle 에 등록된 전자 메일 주소에서 검색하도록 할 수도 있습니다.

## 트러스트 서클에 파일 추가

다음과 같은 방법 중 하나로 트러스트 서클에 파일을 추가할 수 있습니다.

- 기존 트러스트 서클 폴더에 파일을 복사하거나 이동합니다.

  – 또는 –

- Windows 탐색기에서 현재 암호화되지 않은 파일을 마우스 오른쪽 버튼으로 클릭하거나 누르고 **Trust Circle** 을 선택한 다음 **암호화**를 선택합니다. 파일을 추가해야 하는 트러스트 서클을 선택하라는 메시지가 표시됩니다.

**힌트:** 파일을 하나 이상 선택할 수 있습니다.

## 암호화된 폴더

트러스트 서클의 구성원은 해당 트러스트 서클에 속하는 파일을 보고 편집할 수 있습니다.

**참고:** Trust Circle Manager/Reader 는 구성원 간에 파일을 동기화하지 않습니다.

파일은 전자 메일, ftp 또는 클라우드 저장소 공급자 같은 기존 방법을 통해 공유해야 합니다. 트러스트 서클 폴더 내에 복사, 이동 또는 만들어진 파일은 즉시 보호됩니다.

## 트러스트 서클에서 폴더 제거

트러스트 서클에서 폴더를 제거하면 폴더와 모든 내용이 암호화가 해제되고 보호가 제거됩니다.

- Trust Circle 보기에서 **Trust Circles** 를 클릭하거나 누르고 기존 트러스트 서클을 두 번 클릭하거나 두 번 눌러 현재 폴더를 표시하고 해당 폴더 옆의 **휴지통** 아이콘을 클릭하거나 누릅니다.

  – 또는 –

- Windows 탐색기에서 현재 트러스트 서클의 일부인 폴더를 마우스 오른쪽 버튼으로 클릭하거나 누른 상태에서 **Trust Circle** 을 선택한 다음 **트러스트 서클에서 제거**를 선택합니다.

**힌트:** 폴더를 하나 이상 선택할 수 있습니다.

## 트러스트 서클에서 파일 제거

Trust Circle 에서 파일을 제거하려면 Windows 탐색기에서 현재 암호화되지 않은 파일을 마우스 오른쪽 버튼으로 클릭하거나 누르고 **Trust Circle** 을 선택하고 **파일 복호화**를 선택합니다.

## 트러스트 서클에서 구성원 제거

완전히 등록된 구성원은 트러스트 서클에서 제거할 수 없습니다. 대안은 다른 모든 구성원과 함께 새 트러스트 서클을 만들고 모든 파일과 폴더를 새 트러스트 서클로 이동한 다음 기존 트러스트 서클을 삭제하는 것입니다. 이렇게 하면 구성원이 수신하는 새 파일에 액세스할 수 없게 되지만 이전에 공유되었던 모든 내용에는 기존 트러스트 서클 구성원이 계속 액세스할 수 있습니다.

구성원이 완전히 등록되지 않은 경우(구성원이 트러스트 서클에 참가하도록 초대를 받았거나 트러스트 서클 초대를 수락하지 않은 경우) 다음과 같은 방법 중 하나로 트러스트 서클에서 구성원을 제거할 수 있습니다.

- Trust Circle 보기에서 **Trust Circles** 을 클릭하거나 누른 다음 트러스트 서클을 두 번 클릭하거나 두 번 눌러 구성원의 현재 목록을 표시합니다. 제거할 구성원의 이름 옆에서 **휴지통** 아이콘을 클릭하거나 누릅니다.
- Trust Circle 보기에서 **구성원**을 클릭하거나 누른 다음 구성원을 두 번 클릭하거나 두 번 눌러 자신이 구성원으로 있는 트러스트 서클을 표시합니다. 트러스트 서클 옆의 **휴지통** 아이콘을 클릭하거나 눌러 해당 트러스트 서클에서 구성원을 제거합니다.

## 트러스트 서클 삭제

트러스트 서클을 삭제하려면 소유권이 있어야 합니다.

▲ Trust Circle 보기에서 **Trust Circles** 를 클릭하거나 누르고 삭제할 트러스트 서클 옆의 **휴지통** 아이콘을 클릭하거나 누릅니다.

그러면 페이지에서 트러스트 서클이 제거되고 트러스트 서클의 모든 구성원들에게 트러스트 서클이 삭제되었음을 알리는 전자 메일이 보내집니다. 해당 트러스트 서클에 포함된 모든 파일이나 폴더는 복호화됩니다.

# 기본 설정 지정

Trust Circle 보기에서 **기본 설정**을 클릭하거나 누릅니다. 세 가지 탭이 표시됩니다.

- **전자 메일 설정**

| 옵션 | 설명 |
|---|---|
| **사용자 이름** | 현재 사용 중인 사용자 이름이 표시됩니다. 변경하려면 텍스트 상자에 새 사용자 이름을 입력합니다. 변경 내용은 자동으로 저장됩니다. |
| **전자 메일 주소** | 현재 사용 중인 전자 메일 계정이 표시됩니다. 변경하려면 **Change Email Settings**(전자 메일 설정 변경)을 클릭하거나 누른 다음 화면의 지시를 따릅니다. |

| 옵션 | 설명 |
| --- | --- |
| **새 구성원 확인** | 다음 옵션 중에서 선택합니다.<br>◦ **Confirm Automatically**(자동으로 확인)—초대를 받은 사람으로부터 수락을 받은 후에 수동 입력 없이 트러스트 서클에 확인되며 확인 전자 메일이 초대를 받은 사람에게 보내집니다.<br>◦ **Confirm Manually**(수동으로 확인)—초대를 받은 사람으로부터 수락을 받은 후에 트러스트 서클에 새 구성원을 등록하려면 수동으로 입력해야 하며 확인 전자 메일이 초대를 받은 사람에게 보내집니다.<br>◦ **Require Verification**(확인 필요)—초대를 받은 사람으로부터 수락을 받은 후에 초대를 받은 사람을 완전히 등록하려면 확인 코드가 필요합니다. 트러스트 서클의 소유자는 초대를 받은 사람에게 연락하여 확인 코드를 받아야 합니다. 올바른 코드를 입력한 후에 확인 전자 메일이 보내집니다. |
| **정기적인 인증** | 정기적인 인증을 위해서는 사용자가 지정된 시간이 경과된 후에(분 단위로 기록) 민감한 작업을 수행하는 동안 Windows 암호를 입력해야 합니다. 이 설정을 사용하면 인증을 켜거나 끌 수 있습니다. |
| **인증 시간 초과** | 인증을 요청하기 전에 지정된 시간 초과 기간(분 단위로 기록)을 선택합니다. |
| **확인 메시지를 표시하지 않음** | 확인 메시지를 표시를 비활성화하려면 확인란을 선택하고 확인 메시지를 표시하려면 확인란을 선택 해제합니다. |
| **익명의 사용 추적을 통해 HP Trust Circle 을 개선하고자 함** | 프로그램에 참여하려면 확인란을 선택하고 참여하지 않으려면 확인란을 선택 해제합니다. |

- 백업/복원

| 옵션 | 설명 |
| --- | --- |
| **백업** | Trust Circle Manager/Reader 응용프로그램 데이터(설정과 트러스트 서클)를 백업 파일에 복사합니다. 충돌 또는 시스템 고장이 발생하는 경우 이 파일을 사용하여 Trust Circles 의 새로운 설치를 파일에 저장된 상태로 복원할 수 있습니다.<br>**참고:** Trust Circle 응용프로그램 데이터만 저장됩니다(트러스트 서클, 설정 및 구성원). 트러스트 서클의 실제 파일은 백업되지 않습니다. 이러한 파일은 별도로 백업해야 합니다.<br>Trust Circle 설정과 사용자 데이터를 백업하려면:<br>1. **백업**을 클릭하거나 누릅니다.<br>2. 백업 파일의 파일 이름과 디렉터리를 선택한 다음 **저장**을 클릭하거나 누릅니다.<br>3. 암호를 입력하고 확인한 다음 **확인**을 클릭하거나 누릅니다. 이 암호는 이 파일을 복원하는 데 필요합니다. |
| **복원** | 대개 시스템 충돌 또는 다른 컴퓨터로 마이그레이션한 후 백업 파일에서 설정과 트러스트 서클을 복원합니다.<br>Trust Circle Manager 설정과 사용자 데이터를 복원하려면:<br>1. **복원**을 클릭하거나 누릅니다.<br>2. 백업 파일의 디렉터리와 파일 이름을 탐색한 다음 **열기**를 클릭하거나 누릅니다.<br>3. 백업하는 동안 설정한 암호를 입력합니다. |

- **정보**—Trust Circle Manager/Reader 소프트웨어 버전이 표시됩니다. Trust Circle Manager 를 Pro 버전으로 업그레이드하거나 HP 개인 정보 보호 정책을 표시할 수 있는 링크가 표시됩니다.

# 9 도난 회수(일부 모델만 해당)

Computrace(별도 구매)를 이용하면 원격으로 컴퓨터를 모니터링, 관리, 추적할 수 있습니다.

활성화되면, Absolute Software 고객 센터에서 Computrace 를 구성합니다. 고객 센터에서 관리자가 컴퓨터 모니터링 및 관리가 가능하도록 Computrace 를 구성할 수 있습니다. 시스템이 제자리에 없거나 도난당하는 경우, 고객 센터는 지역 당국에서 컴퓨터를 찾고 회수하는 과정에 도움을 줄 수 있습니다. 적절히 구성된 Computrace 는 하드 드라이브를 삭제하거나 교체한 경우에도 기능을 수행합니다.

Computrace 활성화 방법:

1. 인터넷에 연결합니다.
2. HP Client Security 를 엽니다. 자세한 내용은 8페이지의 HP Client Security 열기을 참조하십시오.
3. **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 에 관해 정보가 더 필요하면 **자세한 정보**를 클릭하십시오.

# 10 지역화된 암호 예외

파워온 인증 수준 및 HP Drive Encryption 수준에서는 지역화된 암호 지원이 제한됩니다. 자세한 내용은 51페이지의 Windows IME 는 파워온 인증 수준 또는 Drive Encryption 수준에서 지원되지 않음을 참조하십시오.

## 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 Client Security 를 실행한 다음 Windows 암호를 입력합니다.

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

  1. 지원되는 문자만 사용하도록 Windows 암호를 변경합니다. 지원되지 않는 문자에 대한 자세한 내용은 52페이지의특수 키 처리을 참조하십시오.
  2. HP Client Security 를 실행한 다음 Windows 암호를 입력합니다.

## Windows IME 는 파워온 인증 수준 또는 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.

파워온 인증 또는 Drive Encryption 수준에서는 IME 가 지원되지 않습니다. Windows 암호는 파워온 인증 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 Client Security 에서 이 구성을 지원할 수 있습니다.

⚠ **경고!** HP Client Security 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 Client Security 사용자 페이지(홈 페이지에서 **Gear**(기어) 아이콘에서 액세스)를 사용하여 HP Client Security 에서 사용자를 삭제한 후 운영 체제에서 원하는 키보드 레이아웃을 선택한 다음, 동일한 사용자에 대해 HP Client Security 설치 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 앞의 키보드 레이아웃 중 하나를 선택한 후 암호(예: abcdef)를 입력할 경우 파워온 인증 및 HP Drive Encryption 에서 소문자는 shift 키를, 대문자는 shift 키와 caps lock 키를 누른 상태에서 같은 암호를 입력해야 합니다. 숫자 암호는 숫자 키패드를 사용하여 입력해야 합니다.

- 한국어

  사용자가 지원되는 한국어 키보드 레이아웃을 선택한 후 암호를 입력할 경우 파워온 인증 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 | Caps Lock 키를 누르고 ç, è, à 및 é 문자를 입력하면 Windows 에서 Ç, È, À 및 É 문자로 입력됩니다. | Caps Lock 키를 누르고 ç, è, à 및 é 문자를 입력하면 파워온 인증에서 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 |

| 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

**Bluetooth**
Bluetooth 가 지원되는 컴퓨터, 프린터, 마우스, 휴대폰 및 단거리 무선 통신을 위한 기타 장치를 활성화하기 위해 무선 송신을 사용하는 기술입니다.

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

**Drive Encryption 로그온 화면**
Drive Encryption 사전 부팅을 참조하십시오.

**Drive Encryption 사전 부팅 인증.**
Windows 가 시작되기 전에 표시되는 로그인 화면입니다. 사용자는 Windows 사용자 이름 및 암호 또는 스마트 카드 PIN 을 입력하거나 등록된 손가락을 문질러야 합니다. One Step logon 이 선택된 경우 Drive Encryption 로그인 화면에 정확한 정보를 입력하면 Windows 로그인 화면에 다시 로그인할 필요 없이 Windows 에 바로 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 Client Security 에서 특정 사용자에 대한 계정이나 프로필과 같이 간주되는 인증 정보 및 설정 그룹.

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

**Just In Time 인증(JITA)**
HP Device Access Manager 소프트웨어 도움말을 참조하십시오.

**PIN**
인증에 사용될 등록된 사용자의 개인 ID 번호입니다.

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

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

**TPM(Trusted Platform Module) 내장 보안 칩**
TPM 은 암호화 키, 디지털 인증서, 암호 등 호스트 시스템에 특유한 정보를 저장하여 사용자가 아니라 컴퓨터를 인증합니다. TPM 은 실제 절도 또는 외부 해커의 공격으로 인해 컴퓨터의 정보가 누출 및 손상될 위험을 최소화해줍니다.

**Trust Circle**
데이터를 신뢰할 수 있는 사용자의 정의된 그룹에 연결함으로써 데이터 봉쇄 기능을 제공합니다. 이렇게 하면 실수 또는 의도적으로 나쁜 의도를 가진 사람에게 데이터가 넘어가는 것이 방지됩니다. CryptoMill 의 Zero

Overhead Key Management 기술로 보호되는 데이터는 트러스트 서클에 암호 방식으로 연결됩니다. 따라서 트러스트 서클 외부로 문서 또는 기타 중요한 정보가 해독되는 것이 방지됩니다.

**Trust Circle Manager/Reader**
Trust Circle Reader 는 Trust Circle Manager 사용자가 보낸 초대만 수락할 수 있습니다. 그러나 Trust Circle Manager 를 사용하면 트러스트 서클을 만들 수 있습니다. 전자 메일을 통해 트러스트 서클로 사람을 초대하고 다른 사람의 트러스트 서클 초대를 수락하는 기능이 있습니다. 피어 간에 트러스트 서클이 설정되면 해당 트러스트 서클로 보호되는 파일은 안전하게 공유할 수 있습니다.

**Trust Circle 폴더**
트러스트 서클이 보호하는 폴더입니다.

**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 수 있는 권한이 있는 사용자입니다.

**관리자**
*Windows 관리자*를 참조하십시오.

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

**근접 카드**
근접 카드는 추가적인 보안을 위해 카드를 다른 인증 정보와 함께 사용할 수 있는 컴퓨터 칩이 들어있는 플라스틱 카드입니다.

**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 HP Client Security 내의 객체입니다.

**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

**비접촉식 카드**
인증에 사용할 수 있는 컴퓨터 칩이 들어있는 플라스틱 카드입니다.

**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.

**소프트웨어 암호화**
소프트웨어를 사용하여 하드 드라이브를 섹터별로 암호화합니다. 이 절차는 하드웨어 암호화보다 속도가 느립니다.

**수동 파쇄**
예정된 파쇄를 무시하고, 자산 또는 선택된 자산을 즉시 파쇄합니다.

**스마트 카드**
PIN 과 함께 인증에 사용할 수 있는 하드웨어 장치입니다.

**암호 해제**
암호화에서 암호화된 데이터를 일반 텍스트로 변환하는 데 사용되는 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**
임의의 데이터로 삭제된 자산 및 사용하지 않는 공간을 덮어씁니다. 이 과정을 통해 삭제된 자산이 줄어들기 때문에 기존 자산을 복원하기 더욱 어려워집니다.

**연결된 장치**
컴퓨터의 포트에 연결되어 있는 하드웨어 장치입니다.

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

**인증**
Windows 암호, 지문, 스마트 카드, 비접촉식 카드 또는 근접 카드와 같은 사용자의 인증 정보를 사용하여 사용자의 신원을 확인하는 과정입니다.

**인증 정보**
개별 사용자를 인증하는 데 사용되는 특정 정보 또는 하드웨어 장치입니다.

**자동 파쇄**
File Sanitizer 에 예약한 파쇄입니다.

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

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

**장치 클래스**
드라이브와 같은 특정 유형의 모든 장치

**재부팅**
컴퓨터를 다시 시작하는 과정

**지문**
지문 이미지를 디지털 방식으로 추출한 것입니다. 사용자의 실제 지문 이미지는 HP Client Security 에 저장되지 않습니다.

**파쇄**
자산에 포함된 데이터를 의미 없는 데이터로 덮어쓰는 알고리즘을 실행하는 것입니다.

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

**하드웨어 암호화**
암호화를 즉각 완료하려면 자가 암호화 드라이브 관리를 위한 Trusted Computing Group 의 OPAL 사양을 충족하는 자가 암호화 드라이브를 사용합니다. 하드웨어 암호화는 즉각적으로 이루어지고 단 몇 분밖에 걸리지 않는 반면 소프트웨어 암호화는 몇 시간이 걸릴 수 있습니다.

**홈 페이지**

HP Client Security 의 기능과 설정을 액세스하고 관리할 수 있는 중앙 위치입니다.

**활성화**

Drive Encryption 기능에 액세스하려면 먼저 완료되어야 하는 작업입니다. 관리자는 HP Client Security 설치 마법사 또는 HP Client Security 를 사용하여 Drive Encryption 을 활성화할 수 있습니다. 활성화 절차는 소프트웨어 활성화, 드라이브 암호화, 이동식 저장 장치에 초기 백업 암호화 키 만들기로 구성됩니다.

# 색인