HP ProtectTools
사용 설명서

HP ProtectTools 사용 설명서

HP Compaq 비즈니스 PC

초판: 2008 년 7 월

문서 부품 번호: 491163-AD1

본 설명서 정보

이 설명서는 해당 컴퓨터 모델 업그레이드에 대한 기본 정보를 제공합니다.

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

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

주: 이런 텍스트는 중요한 추가 정보를 제공합니다.

목차

1 보안 소개

HP ProtectTools Security Manager for Administrators 소프트웨어는 컴퓨터, 네트워크 및 중요한 데이터에 대한 무단 액세스를 차단하는 데 도움이 되는 보안 기능을 제공합니다. 다음과 같은 소프트웨어 모듈을 통해 강화된 보안 기능이 제공됩니다.

- HP ProtectTools Credential Manager
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- HP ProtectTools File Sanitizer
- HP ProtectTools Java Card Security
- HP ProtectTools BIOS Configuration
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools

주: Credential Manager, Java Card Security 및 Drive Encryption 은 Security Manager 설치 마법사를 통해 구성됩니다.

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

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

HP ProtectTools 기능

다음 표에는 HP ProtectTools 모듈의 주요 기능이 설명되어 있습니다.

모듈	주요 기능
HP ProtectTools Security Manager for Administrators	• 관리자는 Security Manager 설치 마법사를 통해 보안 수준 및 보안 로그온 방법을 설정 및 구성할 수 있습니다. • 또한 사용자도 설치 마법사를 통해 자신의 로그온 방법을 구성할 수 있습니다. • 관리자 도구를 사용하여 ProtectTools 사용자를 추가 및 제거하거나 사용자 상태를 볼 수 있습니다. • 설치된 HP ProtectTools 모듈로부터 보안 모듈을 백업 및 복원합니다.
HP ProtectTools Credential Manager	• Credential Manager 가 개인 암호 저장소 역할을 하여 사용자 인증 정보를 자동으로 기억하고 적용하는 SSO(Single Sign On) 기능으로 로그온 프로세스를 능률화합니다. • SSO 는 Java™ Card 와 생체 인식 등 여러 보안 기술의 조합을 요구하여 사용자 인증 시 추가 보호 기능도 제공합니다. • 암호 저장은 소프트웨어 암호화를 통해 보호하고 Java Card 나 생체 인식 등 TPM 내장 보안 칩 및/또는 보안 장치 인증을 이용하여 강화할 수 있습니다.
Drive Encryption for HP ProtectTools	• Drive Encryption 은 완전한 풀 볼륨 하드 드라이브 암호화를 제공합니다. • Drive Encryption 은 하드 드라이브에 있는 데이터의 암호를 해독하거나 액세스하기 전에 사전 부팅 인증을 수행하도록 합니다.
Privacy Manager for HP ProtectTools	• Privacy Manager 는 Microsoft 메일, Microsoft Office 문서 및 Live Messenger 사용 시 소스, 무결성, 통신 보안 등을 확인하는 인증서를 얻는 데 사용되는 도구입니다.
HP ProtectTools File Sanitizer	• File Sanitizer 를 통해 컴퓨터의 디지털 자산을 안전하게 파쇄(응용프로그램 파일, 기록 컨텐트 또는 웹 관련 컨텐트, 기타 기밀 데이터 등 매우 중요한 정보를 안전하게 삭제하는 작업)하거나 하드 드라이브를 정기적으로 블리치(데이터를 쉽게 복구할 수 없도록 만들기 위해 이전에 삭제되었지만 여전히 하드 드라이브에 남아 있는 데이터를 다시 덮어쓰는 작업)할 수 있습니다.
HP ProtectTools Java Card Security	• Java 카드 보안은 Java 카드를 위한 관리 소프트웨어 인터페이스입니다. Java 카드는 액세스 권한 부여를 위해 카드 및 PIN 번호가 필요한 인증 데이터를 보호하는 개인 보안 장치입니다. 인증서 관리자, 드라이브 암호화, HP BIOS 또는 타사 액세스 지점에 액세스하는 데 Java 카드를 사용할 수 있습니다. • Java 카드 보안은 하드 드라이브가 부팅되기 전에 사용자 인증을 위한 HP ProtectTools Java 카드를 구성합니다. 내장 보안, Jave 카드 및 암호를 사용하여 Java 카드 보안에 액세스할 수 있습니다. • Java Card Security 는 관리자용 Java Card 와 사용자용 Java Card 를 별도로 구성합니다.

모듈	주요 기능
HP ProtectTools BIOS Configuration	• BIOS 구성은 활성 사용자 및 관리자 암호 관리에 대한 액세스를 제공합니다. • BIOS 구성은 Computer Setup(컴퓨터 설정)이라고 하는 부팅전 BIOS 구성 유틸리티에 대한 대안을 제공합니다. • BIOS 구성은 자동 DriveLock 을 지원하는데, 이 기능은 내장 보안 칩으로 강화할 수 있으며, 시스템에서 제거하더라도 사용자가 내장 보안 칩 사용자 암호 외에 어떠한 추가 암호를 기억할 필요 없이 하드 드라이브를 무단 액세스로부터 보호합니다.
Embedded Security for HP ProtectTools	• Embedded Security 모듈은 TPM(Trusted Platform Module) 내장 보안 칩을 사용하여 PC 에 로컬 저장된 인증 정보나 중요한 사용자 데이터에 대한 무단 액세스를 차단해 줍니다. • 내장 보안은 PSD(Personal Secure Drive) 생성을 허용하는데, 이는 사용자 파일과 폴더 정보를 보호하는 데 유용합니다. • Embedded Security 는 보안 디지털 인증서 작업에 타사 응용프로그램(예: Microsoft Outlook, Internet Explorer)을 사용하도록 지원합니다.
Device Access Manager for HP ProtectTools	• IT 관리자는 Device Access Manager 를 통해 USB 포트, 광 드라이브와 같은 장치에 대한 액세스를 사용자 프로필에 따라 제어할 수 있습니다. • Device Access Manager 는 권한이 없는 사용자가 외부 저장 미디어를 사용하여 데이터를 제거하거나 외부 미디어의 바이러스를 시스템에 감염시키는 행위를 방지합니다. • 관리자는 특정 개인이나 사용자 그룹이 쓰기 가능 장치에 액세스하지 못하도록 차단할 수 있습니다.

HP ProtectTools 보안 액세스

Windows® 제어판에서 HP ProtectTools Security Manager for Administrators 에 액세스하려면 다음과 같이 하십시오.

▲ Windows Vista®인 경우 **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager for Administrators** 를 누릅니다.

또는

Windows XP 에서 **시작**을 누르고 **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.

주: HP ProtectTools 관리자가 아니라면 HP ProtectTools 를 비관리자 모드로 실행하여 정보는 볼 수 있지만 정보를 변경할 수는 없습니다.

주: Credential Manager 모듈을 구성한 후 Windows 로그온 화면에서 Credential Manager 로 바로 로그인하여 HP ProtectTools 를 열 수도 있습니다. 자세한 내용은 24페이지의 Credential Manager 로 Windows 에 로그온을 참조하십시오.

주요 보안 목표 달성

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

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

계획된 절도에 대한 대비

이런 사건의 예로 컴퓨터 또는 컴퓨터에 담겨 있는 기밀 데이터 및 고객 정보를 계획적으로 절도하려는 경우를 들 수 있습니다. 이러한 사건은 개방된 사무실 환경 또는 보안이 이루어지지 않는 곳에서 쉽

게 발생할 수 있습니다. 다음 기능은 컴퓨터를 도난당한 경우 컴퓨터에 저장된 데이터를 보호하는 데 도움이 됩니다.

- 부팅 전 인증 기능을 활성화하면 운영체제에 대한 액세스 차단에 도움이 됩니다. 다음 절차를 참조하십시오.
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- DriveLock 은 하드 드라이브를 제거하여 안전하지 않은 시스템에 설치하는 경우라도 데이터에 액세스하지 못하도록 할 수 있습니다.
- HP ProtectTools Embedded Security 에 포함된 PSD(개인 보안 드라이브) 기능은 중요 데이터를 암호화하여 인증을 거쳐야만 액세스할 수 있도록 합니다. 다음 절차를 참조하십시오.
  - Embedded Security "72페이지의 설정 절차"
  - "74페이지의 개인 보안 드라이브 사용"

중요 데이터에 대한 액세스 제한

현장에서 근무 중인 회계사에게 중요한 재무 데이터를 검토할 수 있도록 컴퓨터 액세스 권한을 주었다고 가정합시다. 이 회계사가 파일을 인쇄하거나 CD 와 같은 쓰기 가능 장치에 저장하지는 못하게 해야 할 것입니다. 데이터 액세스를 제한하는 기능은 다음과 같습니다.

- IT 관리자는 Device Access Manager for HP ProtectTools 를 통해 쓰기 가능 장치에 대한 액세스를 제한함으로써 하드 드라이브에서 이동식 미디어로 중요한 정보가 인쇄되거나 복사되지 않도록 할 수 있습니다. 80페이지의 장치 클래스 구성(고급)을 참조하십시오.
- DriveLock 은 하드 드라이브를 제거하여 안전하지 않은 시스템에 설치하는 경우라도 데이터에 액세스하지 못하도록 할 수 있습니다.

내부 또는 외부에서 들어오는 무단 액세스 차단

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

- 부팅 전 인증 기능을 활성화하면 운영체제에 대한 액세스 차단에 도움이 됩니다. 다음 절차를 참조하십시오.
  - Credential Manager
  - Embedded Security
  - Drive Encryption
- HP ProtectTools Embedded Security 는 다음과 같은 절차를 통해 PC 에 로컬 저장된 인증서 또는 중요한 사용자 데이터를 보호합니다.
  - Embedded Security "72페이지의 설정 절차"
  - "74페이지의 개인 보안 드라이브 사용"

- HP ProtectTools Credential Manager 는 다음 절차를 사용하여 권한 없는 사용자가 암호로 보호되는 응용프로그램에 액세스하거나 그러한 암호를 획득하지 못하도록 합니다.
  - Credential Manager "20페이지의 설정 절차"
  - "25페이지의 Single Sign On 사용"
- IT 관리자는 Device Access Manager for HP ProtectTools 를 통해 쓰기 가능 장치에 대한 액세스를 제한함으로써 하드 드라이브에서 중요한 정보가 복사되지 않도록 할 수 있습니다. 78페이지의 기본 구성을 참조하십시오.
- PSD(개인 보안 드라이브) 기능은 다음 절차에 따라 중요한 데이터를 암호화하여 인증 없이는 액세스하지 못하도록 합니다.
  - Embedded Security "72페이지의 설정 절차"
  - "74페이지의 개인 보안 드라이브 사용"
- File Sanitizer 를 통해 자산을 파쇄하거나 하드 드라이브를 블리치(데이터를 쉽게 복구할 수 없도록 만들기 위해 이전에 삭제되었지만 여전히 하드 드라이브에 남아 있는 데이터를 다시 쓰는 작업)함으로써 데이터를 안전하게 삭제할 수 있습니다.
- Privacy Manager 를 통해 Microsoft 메일, Office 문서 및 Live Messenger 사용 시 안전하고 확실하게 중요한 정보를 전송하거나 저장할 수 있도록 해주는 인증서를 얻을 수 있습니다.

강력한 암호 정책 생성

십여 가지의 웹 기반 응용프로그램과 데이터베이스에 대해 강력한 암호 정책을 사용하도록 요구하는 요건을 준수해야 할 경우, HP ProtectTools Credential Manager 는 다음 절차에 따라 암호 및 Single Sign On 편의 기능에 사용할 수 있는 보안 저장소를 제공합니다.

- Credential Manager "20페이지의 설정 절차"
- "25페이지의 Single Sign On 사용"

Embedded Security for HP ProtectTools 는 더욱 강력한 보안을 위하여 사용자 이름 및 암호 저장소를 보호합니다. 이를 통해 사용자는 암호를 적어 놓거나 기억할 필요 없이 여러 개의 강력한 암호를 유지할 수 있습니다. Embedded Security 의 72페이지의 설정 절차를 참조하십시오.

추가 보안 요소

보안 역할 분배

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

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

HP ProtectTools 에서는 보안 책임과 권한이 다음과 같은 역할로 구분됩니다.

- 보안 관리자 - 회사나 네트워크의 보안 수준을 정의하고, Java™ 카드, 생체 인식기, USB 토큰 등 배치할 보안 기능을 결정합니다.
- IT 관리자 - 보안 담당자가 정의한 보안 기능을 적용 및 관리합니다. 또한 일부 기능을 활성화 및 비활성화할 수 있습니다. 예를 들어, 보안 관리자가 Java Card 를 배치하기로 결정하면 IT 관리자는 Java Card BIOS 보안 모드를 활성화할 수 있습니다.
- 사용자 - 보안 기능을 사용합니다. 예를 들어, 보안 관리자와 IT 관리자가 시스템에 대해 Java Card 를 활성화하면, 사용자는 Java Card PIN 을 설정하고 인증에 그 카드를 사용할 수 있습니다.

HP ProtectTools 암호 관리

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

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

HP ProtectTools 암호	HP ProtectTools 모듈에서 설정	기능
Credential Manager 로그온 암호	Credential Manager	이 암호는 다음과 같은 2 가지 옵션을 제공합니다. • Windows 에 로그온한 후에 별도의 로그온을 통해 Credential Manager 에 액세스하는 데 사용할 수 있습니다. • Windows 로그온 과정 대신 사용하여 Windows 와 Credential Manager 에 동시에 액세스할 수 있습니다.
Credential Manager 복구 파일 암호	Credential Manager, IT 관리자가 설정	Credential Manager 복구 파일에 무단으로 액세스하지 못하도록 합니다.
기본 사용자 키 암호 주: Embedded Security 암호라고도 함	Embedded Security	보안 전자 우편, 파일, 폴더 암호화와 같은 Embedded Security 기능에 액세스하는 데 사용됩니다. 파워온 인증에 사용할 경우, 컴퓨터를 켜거나, 재시작하거나, 최대 절전 모드에서 복원할 때 컴퓨터 내용에 무단으로 액세스하지 못하도록 합니다.
응급 복구 토큰 암호 주: 응급 복구 토큰 키 암호라고도 함	Embedded Security, IT 관리자가 설정	내장 보안 칩용 백업 파일인 응급 복구 토큰에 무단으로 액세스하지 못하도록 합니다.

HP ProtectTools 암호	HP ProtectTools 모듈에서 설정	기능
소유자 암호	Embedded Security, IT 관리자가 설정	Embedded Security 의 모든 소유자 기능에 대한 무단 액세스를 차단하여 시스템 및 TMP 칩을 보호합니다.
Java™ 카드 PIN	Java Card Security	Java Card 내용에 무단으로 액세스하지 못하도록 하고 Java Card 사용자를 인증합니다. Java Card PIN 을 파워온 인증에 사용하면 Computer Setup 유틸리티와 컴퓨터 내용에 대한 무단 액세스를 방지할 수 있습니다. Java Card 토큰을 선택한 경우, Drive Encryption 모듈의 사용자를 인증합니다.
Computer Setup 암호 주: BIOS 관리자, F10 설정 또는 보안 설정 암호라고도 함	BIOS Configuration, IT 관리자가 설정	Computer Setup 유틸리티에 무단으로 액세스하지 못하도록 합니다.
파워온 암호	BIOS Configuration	컴퓨터를 켜거나, 재시작하거나, 최대 절전 모드에서 복원할 때 컴퓨터 내용에 무단으로 액세스하지 못하도록 합니다.
Windows 로그온 암호	Windows 제어판	수동 로그온에 사용하거나 Java Card 에 저장할 수 있습니다.

보안 암호 만들기

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

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

HP ProtectTools 인증 정보 백업 및 복원

지원되는 모든 HP ProtectTools 모듈에서 인증 정보를 백업 및 복원하려면 다음을 참조하십시오.

인증 정보 및 설정 백업

다음과 같이 인증 정보를 백업할 수 있습니다.

- HP ProtectTools Drive Encryption 을 사용하여 HP ProtectTools 인증 정보를 선택하고 백업합니다.

  온라인 Drive Encryption 키 복구 서비스에 등록하여 암호화 키 백업 사본을 저장할 수도 있기 때문에 암호가 생각나지 않고 로컬 백업에 액세스하지 못하는 경우에도 컴퓨터에 액세스할 수 있습니다.

  주: 인터넷에 연결되어 있고 유효한 전자 우편 주소가 있어야 이 서비스를 통해 암호를 복구하거나 등록할 수 있습니다.

- HP ProtectTools Embedded Security 를 사용하여 HP ProtectTools 인증 정보를 백업합니다.
- HP ProtectTools Security Manager for Administrators 의 Backup and Recovery 도구를 사용하여 한 곳에서, 설치된 HP ProtectTools 모듈로부터 보안 인증서를 백업 및 복원할 수 있습니다.

2 HP ProtectTools Security Manager for Administrators

HP ProtectTools Security Manager for Administrators 정보

HP ProtectTools Security Manager for Administrators 는 컴퓨터, 네트워크 및 중요한 데이터에 대한 무단 액세스를 차단하는 데 도움이 되는 보안 기능을 제공합니다. Security Manager 는 확장이 가능하여 새로운 위협이 발생하면 새로운 기술을 제공하여 문제를 해결할 수 있도록 합니다.

초기 보안 설정을 위해 HP ProtectTools Security Manager for Administrators 모듈을 사용하십시오. Security Manager 는 중앙 집중화된 인터페이스를 통해 다음과 같은 기능을 제공합니다.

- **Getting Started**(시작하기) - 설치 마법사가 Windows 운영체제 관리자에게 사전 부팅 환경, Credential Manager 및 Drive Encryption 에서 사용되는 보안 로그인 방법과 보안 수준의 구성을 안내합니다. 사용자도 설치 마법사를 통해 자신의 보안 로그인 방법을 구성할 수 있습니다. 자세한 내용은 11페이지의 시작하기 - HP ProtectTools Security Manager for Administrators 구성 및 13페이지의 Getting Started(시작하기) – 사용자 보안 로그인 방법 구성을 참조하십시오.
- **Administrators Tools**(관리자 도구) - Windows 관리자는 관리자 도구를 통해 ProtectTools 사용자를 추가 및 제거하거나 사용자 상태를 볼 수 있습니다. 자세한 내용은 14페이지의 Administrator Tools(관리자 도구) – 사용자 관리(관리자 전용)를 참조하십시오.
- **Backup and Restore**(백업 및 복원) - 설치된 HP ProtectTools 모듈로부터 보안 인증서를 백업 및 복원합니다. 자세한 내용은 16페이지의 Backup and Restore(백업 및 복원)을 참조하십시오.
- **Settings**(설정) - 다양한 항목의 동작을 사용자 정의할 수 있습니다. 자세한 내용은 19페이지의 Settings(설정)을 참조하십시오.

Security Manager 의 중앙 집중화된 사용자 인터페이스에는 컴퓨터 보안을 극대화하기 위한 애드온 소프트웨어 모듈 목록도 있습니다. 사용 가능한 모듈을 원하는 만큼 선택하고 구성할 수 있습니다.

시작하기 - HP ProtectTools Security Manager for Administrators 구성

Windows 관리자는 Getting Started 설치 마법사를 통해 보안 수준 및 보안 로그인 방법을 설정하거나 업데이트할 수 있습니다.

또한 사용자는 설치 마법사를 사용하여 보안 로그온 방법을 구성할 수 있습니다.

주: Windows 관리자는 언제든지 설치 마법사를 실행하여 보안 수준 또는 보안 로그인 방법을 변경할 수 있습니다.

Windows 관리자는 설치 마법사의 안내에 따라 Security Manager 를 구성할 수 있습니다.

1. HP ProtectTools Security Manager for Administrators 에서 **Getting Started**(시작하기), **Security Manager Setup**(보안 관리자 설정) 버튼을 누릅니다. Security Manager 기능에 대한 설명이 시작됩니다.
2. 설치 마법사의 다음 재생 시 Security Manager 기능에 대한 설명 데모를 생략하고 싶다면, 가능한 경우 “Welcome(시작)” 페이지에서 **Automatically play video when wizard starts**(마법사 시작과 함께 데모 자동 재생) 확인란의 선택을 해제합니다.
3. 해당 페이지를 읽은 후 **Next**(다음)를 누릅니다.
4. “Set Levels of Security(보안 수준 설정)” 페이지에서 보안 수준을 선택합니다. 다음 보안 수준 중 한 개 이상을 선택할 수 있습니다.
   - HP Credential Manager - Windows 계정을 보호합니다.
   - Pre-boot Security(일부 모듈) - Windows 가 시작되기 전에 컴퓨터를 보호합니다.
   - HP Drive Encryption - 하드 드라이브를 암호화하여 컴퓨터를 보호합니다. 이 옵션을 선택하는 경우 이동식 저장 장치의 고유 암호화 키를 백업해야 합니다.

   주: 선택 항목에 따라 Security 미터가 달라집니다. 보안 수준을 많이 선택할수록 컴퓨터는 더욱 안전해집니다.

   보안 수준을 선택한 다음 **Next**(다음)를 누릅니다.

5. 4 단계에서 선택한 보안 수준에 따라 다음 중 한 개 이상의 페이지가 표시됩니다.

   - Windows 계정 보호 - Security Manager 가 각 보안 수준에 대하여 암호를 동기화해야 하기 때문에 Windows 암호가 필요합니다.

     Windows 암호를 입력하고 확인하거나, 이미 설정된 암호가 있다면 해당 암호를 입력한 후 **Next**(다음)를 누릅니다.

   - Windows 시작 전 시스템 보호(선택 사양) - 본인 또는 사용자가 BIOS 관리자 암호를 알고 있는 경우 해당 암호를 입력합니다. BIOS 관리자 암호를 입력하면 해당 Windows 관리자 또는 사용자는 BIOS 관리자가 됩니다.

   주: BIOS 관리자 암호가 존재하지 않는 경우에는 먼저 암호를 설정해야 합니다. BIOS 관리자 암호를 입력하면 본인이 BIOS 관리자가 됩니다.

   BIOS 관리자 암호를 입력하고 확인하거나, 이미 설정된 암호가 있다면 해당 암호를 입력한 후 **Next**(다음)를 누릅니다.

   - 하드 드라이브를 암호화하여 데이터 보호 – 암호화 키를 저장하려면 반드시 USB 저장 장치를 사용해야 합니다. 암호화할 드라이브를 선택(최소 한 개 이상 선택)하고 저장 장치를 해당 슬롯에 삽입한 다음 암호화 키를 저장할 저장 장치를 선택하고 **Next**(다음)를 누릅니다.

6. "Set Security Login Methods(보안 로그인 방법 설정)" 페이지에서 로그인 방법을 하나 이상 선택합니다.

   a. 1 단계에서 보안 로그인 방법을 하나 이상 선택합니다.

   주: 이러한 선택 사항은 관리자와 사용자 모두에게 적용됩니다.

   b. 보안 수준을 높이고 싶다면 컴퓨터 로그인 시 1 단계에서 선택한 보안 로그인 방법을 *모두* 사용하도록 요구하는 확인란을 2 단계에서 선택합니다.

   컴퓨터 로그인 시 선택한 보안 로그인 방법 중 *하나*를 사용하도록 허용하려면 위의 확인란을 선택하지 마십시오.

   주의: 위의 확인란을 선택한 경우 사용자가 아직 자신의 로그인 방법(Windows 암호, 지문 인증 및/또는 HP ProtectTools Java™ Card)을 설정하지 않았다면 컴퓨터에 로그인할 수 없습니다. 이 옵션은 먼저 모든 사용자가 자신의 로그인 방법을 설정한 후에 선택하는 것이 좋습니다.

   c. **Next**(다음)를 누릅니다. 선택 사항을 검토할 수 있는 요약 페이지가 열립니다.

7. "Review and Enable Security Settings(보안 설정 검토 및 활성화)" 페이지에서 **Enable**(활성화)을 누릅니다.

   Enable(활성화)을 누르면 컴퓨터의 보안 사항이 선택한 대로 설정됩니다. 보안 설정이 완료될 때까지는 이전 마법사 페이지로 돌아갈 수 없습니다. 설정을 변경하려면 마법사를 완료한 후 다시 실행해야 합니다.

8. 6 단계에서 선택한 보안 로그인 방법에 따라 다음 중 하나 이상의 페이지가 표시됩니다. 화면의 지침을 따른 후 **Next**(다음)를 누릅니다.

   - "지문 등록" - 화면에서 등록하려는 손가락에 해당하는 손가락을 누른 다음(최소 2 개 이상의 손가락을 등록해야 함) 선택한 손가락을 지문 센서 위에 천천히 찍고 완전히 찍힐 때까지 같은 손가락을 계속 찍습니다. 선택한 다른 손가락도 이 프로세스를 반복하여 등록하고 **Finish**(마침)를 누릅니다.

   - "HP ProtectTools Java Card 등록" - HP ProtectTools Java Card 를 넣고 Java Card PIN 을 입력한 다음 **Finish**(마침)를 누릅니다.

9. "Congratulations(완료)" 페이지에서 선택 사항을 검토한 다음 **Done**(완료)을 누릅니다.

Getting Started(시작하기) – 사용자 보안 로그인 방법 구성

Windows 관리자가 보안 수준 및 보안 로그인 방법을 구성하고 나면 사용자가 설치 마법사를 실행하여 컴퓨터에서 자신을 HP ProtectTools 사용자로 추가할 수 있습니다.

주: 설치 마법사를 실행하는 사용자는 대부분의 마법사 페이지를 볼 수 있습니다. 그러나 "Set Levels of Security(보안 수준 설정)" 및 "Set Security Login Methods(보안 로그인 방법 설정)" 페이지는 관리자 전용 작업이므로 사용자가 구성할 수 없습니다.

1. 컴퓨터에 로그인합니다.
2. Security Manager 에서 **Getting Started**(시작하기), **Security Manager Setup**(보안 관리자 설정) 버튼을 누릅니다.
3. 설치 마법사의 다음 재생 시 Security Manager 기능에 대한 설명 데모를 생략하고 싶다면, "Welcome(시작)" 페이지에서 **Automatically play video when wizard starts**(마법사 시작과 함께 데모 자동 재생) 확인란의 선택을 해제합니다.
4. 해당 페이지를 읽은 후 **Next**(다음)를 누릅니다.
5. "Set Levels of Security(보안 수준 설정)" 페이지에서 **Next**(다음)를 누릅니다.
6. 관리자가 설정해 놓은 보안 수준에 따라 다음 중 하나 이상의 페이지가 표시됩니다.

   - Windows 계정 보호 - Security Manager 가 각 보안 수준에 대하여 암호를 동기화해야 하므로 Windows 암호가 필요합니다.

     주: 보안 수준을 HP Credential Manager 만 선택한 경우 Credential Manager 가 Windows 암호를 이미 알고 있기 때문에 Windows 암호를 입력하라는 메시지가 나타나지 않습니다.

     Windows 암호를 입력하고 확인하거나, 이미 설정된 암호가 있다면 해당 암호를 입력한 후 **Next**(다음)를 누릅니다.

   - Windows 시작 전 시스템 보호(선택 사양) – BIOS 관리자 암호를 알고 있는 경우 해당 암호를 입력합니다. BIOS 관리자 암호를 입력하면, 해당 Windows 관리자 또는 사용자는 BIOS 관리자가 됩니다.

     주: BIOS 관리자 암호가 존재하지 않는 경우에는 먼저 암호를 설정해야 합니다. BIOS 관리자 암호를 입력하면, 본인이 BIOS 관리자가 됩니다.

     BIOS 관리자 암호를 입력하고 확인하거나, 이미 설정된 암호가 있다면 해당 암호를 입력한 후 **Next**(다음)를 누릅니다.

7. "Set Security Login Methods(보안 로그인 방법 설정)" 페이지에서 **Next**(다음)를 누릅니다.

8. “Review and Enable Security Settings(보안 설정 검토 및 활성화)” 페이지에서 **Enable**(활성화)을 누릅니다.

9. 관리자가 설정해 놓은 보안 로그인 방법에 따라 다음 중 하나 이상의 페이지가 표시됩니다. 화면의 지침을 따른 후 **Next**(다음)를 누릅니다.

   - “지문 등록” – 화면에서 등록하려는 손가락에 해당하는 손가락을 누른 다음(최소 2 개 이상의 손가락을 등록해야 함) 선택한 손가락을 지문 센서 위에 천천히 찍고 완전히 찍힐 때까지 같은 손가락을 계속 찍습니다. 선택한 다른 손가락도 이 프로세스를 반복하여 등록하고 **Finish**(마침)를 누릅니다.

   - “HP ProtectTools Java Card 등록” - HP ProtectTools Java Card 를 넣고 Java Card PIN 을 입력한 다음 **Finish**(마침)를 누릅니다.

10. “Congratulations(완료)” 페이지에서 선택 사항을 검토한 다음 **Done**(완료)을 누릅니다.

Security Manager 구성 후 로그인

로그인 방법은 Windows 관리자가 구성 단계에서 선택한 보안 수준 및 보안 로그인 방법에 따라 달라집니다. 가능한 로그인 방법은 다음과 같습니다.

- 세 개의 보안 수준이 모두 구성되었으며 보안 로그인 방법이 *모두* 요구되는 경우, 컴퓨터가 처음 켜지면 사용자는 구성된 방법을 모두 사용하여 로그인해야 합니다. 이렇게 하면 사용자가 Windows 에 로그인됩니다.

- 세 개의 보안 수준이 모두 구성되었으며 보안 로그인 방법 중 *하나*를 사용하도록 허용되는 경우, 컴퓨터가 처음 켜지면 사용자는 구성된 보안 로그인 방법 중 하나를 사용하여 로그인할 수 있습니다. 이렇게 하면 사용자가 Windows 에 로그인됩니다.

- HP Drive Encryption 및 HP Credential Manager 보안 수준이 구성되었으며 보안 로그인 방법이 *모두* 요구되는 경우, HP Drive Encryption 로그인 화면이 열리면 사용자는 구성된 방법을 모두 사용하여 로그인해야 합니다. 이렇게 하면 사용자가 Windows 에 로그인됩니다.

- HP Drive Encryption 및 HP Credential Manager 보안 수준이 구성되었으며 구성된 보안 로그인 방법 중 *하나*를 사용하도록 허용되는 경우, HP Drive Encryption 로그인 화면이 열리면 사용자는 보안 로그인 방법 중 하나를 사용하여 로그인할 수 있습니다. 이렇게 하면 사용자가 Windows 에 로그인됩니다.

- HP Credential Manager 보안 수준이 구성되었으며 *모든* 보안 로그인 방법이 요구되는 경우, Credential Manager 로그인 화면이 열리면 사용자는 구성된 방법을 모두 사용하여 로그인해야 합니다. 이렇게 하면 사용자가 Windows 에 로그인됩니다.

- HP Credential Manager 보안 수준 옵션이 구성되었으며 구성된 보안 로그인 방법 중 *하나*를 사용하도록 허용되는 경우, Credential Manager 로그인 화면이 열리면 사용자는 보안 로그인 방법 중 하나를 사용하여 로그인할 수 있습니다. 이렇게 하면 사용자가 Windows 에 로그인됩니다.

주: HP Credential Manager 보안 수준이 구성된 경우 사용자는 다른 보안 수준에서 요구되는 보안 로그인 방법에 관계없이 Windows 로그인 화면에서 Windows 암호를 입력해야 합니다.

Administrator Tools(관리자 도구) – 사용자 관리(관리자 전용)

Windows 관리자는 관리자 도구 기능을 사용하여 HP ProtectTools 사용자를 추가 및 제거하거나 사용자 상태를 볼 수 있습니다.

관리자 도구의 Administrator 및 User 탭에서는 선택된 보안 로그인 방법들을 보여주며 사용자가 한 가지 방법을 선택하여 사용할 수 있는지 또는 모든 방법을 사용해야 하는지 보여줍니다. 보안 수준 또는 보안 로그인 방법을 변경하려는 경우 설치 마법사를 실행해야만 변경이 가능합니다.

사용자 추가

Windows 관리자는 사용자 목록에 다른 관리자 또는 일반 사용자를 추가할 수 있습니다. 추가 프로세스는 모두 동일합니다.

주: 사용자를 추가하려면 해당 사용자가 컴퓨터에 Windows 사용자 계정을 가지고 있어야 하며 그 자리에 함께 있으면서 암호를 입력해야 합니다.

사용자를 사용자 목록에 추가하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager for Administrators** 를 누릅니다.
2. **Administrator Tools**(관리자 도구)를 누릅니다.
3. **Manage Users**(사용자 관리) 버튼을 누릅니다.
4. **Administrator**(관리자) 또는 **User**(사용자) 탭을 선택합니다.
5. **Add**(추가)를 누릅니다.
6. 추가하려는 계정의 사용자 이름을 클릭하거나 **User Name**(사용자 이름) 상자에 이름을 입력한 후 **Next**(다음)를 누릅니다.

   주: 기존의 Windows 계정을 사용해야 하며, 해당 이름을 클릭하거나 이름을 정확히 입력해야 합니다. 이 대화상자를 통해 Windows 사용자 계정을 수정하거나 추가할 수는 없습니다.

7. 선택한 계정에 대해 Windows 암호를 입력한 다음 **OK**(확인)를 누릅니다.

   주: 지문 및/또는 HP ProtectTools Java Card 보안 로그인 방법으로 로그인하려면, 사용자는 먼저 컴퓨터에 로그인한 다음 설치 마법사를 실행하여 해당 로그인 방법을 구성해야 합니다.

사용자 제거

주: 이 절차로는 Windows 사용자 계정이 삭제되지 않고 Security Manager 에서 해당 계정만 제거됩니다. 사용자를 완전히 제거하려면 Security Manager 와 Windows 모두에서 제거해야 합니다.

사용자 목록에서 사용자를 제거하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager for Administrators** 를 누릅니다.
2. **Administrator Tools**(관리자 도구)를 누릅니다.
3. **Manage Users**(사용자 관리) 버튼을 누릅니다.
4. **Administrator**(관리자) 또는 **User**(사용자) 탭을 선택합니다.
5. 제거하려는 계정의 사용자 이름을 누른 다음 **Remove**(제거)를 누릅니다.

   주: Administrator 목록에 관리자가 한 명만 있는 경우에는 관리자를 제거할 수 없습니다.

6. 확인 대화상자에서 **Yes**(예)를 누릅니다.

사용자 상태 확인

Administrator Tools 의 Administrator 및 User 탭에서는 각 사용자의 현재 상태를 보여 줍니다.

- **Green check mark**(녹색 확인 표시) – 사용자가 요구되는 보안 로그인 방법을 구성하였음을 나타냅니다.
- **Yellow exclamation point**(노란색 느낌표) – 사용자가 한 개 이상의 요구되는 또는 허용되는 보안 로그인 방법을 구성하지 않았음을 나타냅니다. 예를 들어 Windows 관리자가 두 개 이상의 보안 로그인 방법을 구성한 경우 이는 둘 중 하나의 방법으로 컴퓨터에 로그인할 수 있음을 나타내므로, 이미 한 가지 방법을 구성해 놓은 사용자는 그 방법을 통해 로그인할 수 있습니다. 노란색 느낌표는 Windows 관리자에게 해당 사용자가 다른 보안 로그인 방법을 구성하지 않았음을 알려 주는 것입니다.
- **Red X**(빨간색 X) – 사용자가 요구되는 보안 로그인 방법을 구성하지 않아 로그인 시도 시 컴퓨터에 액세스할 수 없음을 나타냅니다. 해당 사용자는 설치 마법사를 실행하여 요구되는 로그인 방법을 구성해야 합니다.
- **Blank**(공백) – 보안 로그인 방법이 필요하지 않음을 나타냅니다.

Backup and Restore(백업 및 복원)

HP ProtectTools Backup and Restore 를 사용하여 한 곳에서, 설치된 HP ProtectTools 모듈로부터 보안 인증서를 백업 및 복원할 수 있습니다.

Security Manager 에서 **Backup and Restore**(백업 및 복원)를 누른 후 다음 버튼 중 하나를 누릅니다.

- **Backup Options**(백업 옵션) 버튼 – 백업 설정을 구성할 수 있습니다. 자세한 내용은 16페이지의 백업 마법사 사용을 참조하십시오.
- **Backup**(백업) 버튼 – 모든 보안 인증서를 신속하게 백업할 수 있습니다.

주: 백업을 수행하기 전에 **Backup Options**(백업 옵션) 버튼을 통해 백업 설정을 구성해야 합니다.

- **Schedule Backups**(백업 예약) 버튼 – 백업 예약을 설정할 수 있습니다. 예약과 관련하여 도움이 필요하다면 Windows 도움말에서 "작업 예약" 항목을 검색해 보십시오.

주: 백업을 예약하기 전에 먼저 **Backup Options**(백업 옵션) 버튼을 통해 백업 설정을 구성해야 합니다.

- **Restore**(복원) 버튼 – 이전에 백업한 보안 인증서를 복원할 수 있습니다. 자세한 내용은 18페이지의 복원 마법사 사용을 참조하십시오.

△ 주의: HP ProtectTools Backup and Restore 이외의 방법을 통해 생성된 백업 파일(예를 들어, 특정 보안 모듈을 통해 이전에 생성된 파일)은 HP ProtectTools Backup and Restore 와 호환되지 않기 때문에 HP ProtectTools Backup and Restore 또는 해당 보안 모듈의 새로운 버전에 의해 복원되지 않습니다. HP ProtectTools Backup and Restore 를 통해 새로운 백업 파일을 만드는 것이 좋습니다.

백업 마법사 사용

1. Security Manager 에서 **Backup and Restore**(백업 및 복원)를 누른 다음 **Backup Options**(백업 옵션)를 눌러 백업 마법사를 시작합니다.
2. 다음 백업 마법사 실행 시 "Welcome(시작)" 페이지를 생략하고 싶으면 **Show Welcome Screen**(시작 화면 표시) 확인란의 선택을 해제합니다.

3. **Next**(다음)를 누릅니다. “Security Modules(보안 모듈)” 페이지가 열립니다.

4. 다음 하위 섹션을 참조하여 계속합니다.

Security Modules(보안 모듈)

백업할 모듈을 선택하려면 다음 단계를 따르십시오.

1. 행의 시작 부분에 있는 확인란을 선택한 다음 해당 모듈을 백업 목록에 추가합니다. 백업 목록의 모든 모듈을 빠르게 추가하거나 제거하려면 **Select All**(모두 선택) 또는 **Clear All**(모두 지우기) 버튼을 누릅니다. 해당 모듈의 상태 열에 “Ready(준비)” 또는 “Needs Authentication(인증 필요)”이 표시되어야만 선택할 수 있습니다.

   주: 모듈이 준비되지 않은 경우에는 확인란을 선택할 수 없습니다. 모듈 상태를 업데이트한 다음에는 해당 열의 오른쪽에 있는 **Refresh**(새로 고침) 버튼을 눌러 상태 필드를 업데이트합니다. 모든 모듈의 상태를 업데이트하려면 **Refresh All**(모두 새로 고침) 버튼을 누릅니다.

2. 필요한 경우, 선택한 각 모듈의 인증 열에 요구되는 값을 입력합니다. 장치의 인증서 데이터에 액세스하려면 보안 장치에 인증 값을 입력해야 할 수도 있습니다. 인증 값에는 암호, PIN 등이 포함됩니다.

3. **Next**(다음)를 누릅니다. ”File Location(파일 위치)” 페이지가 열립니다.

File Location(파일 위치)

“File Location(파일 위치)” 페이지에서는 백업 저장 파일 및 보안 토큰 파일의 위치를 선택할 수 있습니다.

보안 토큰 파일은 백업 저장 파일을 암호화하는 데 사용되는 키를 안전하게 저장합니다. 암호는 보안 토큰 파일의 내용을 암호화합니다. 보안 토큰 파일을 오프라인 위치(USB 플래시 드라이브, 디스크 또는 기타 미디어)에 저장하면 보안 토큰 파일을 *가지고* 있고 암호를 *알고* 있어야만 저장 파일의 백업 데이터에 액세스할 수 있기 때문에 두 가지 수준의 보안이 제공됩니다. 따라서 저장 파일과 토큰 파일은 각기 다른 위치에 저장되어 있는 두 개의 다른 이동식 미디어에 저장하는 것이 좋습니다.

파일 위치를 구성하려면 다음과 같이 하십시오.

1. 저장 파일과 보안 토큰 파일을 저장할 파일 이름 및 위치를 확인 또는 변경합니다. 위치를 변경하려면 **Edit**(편집) 버튼을 누른 다음 새로운 파일 이름을 입력하거나 **Browse**(찾아보기)를 눌러 새로운 위치를 선택합니다. 파일 확장명 .ptb 가 파일 이름에 자동으로 추가됩니다.

   주: 주어진 저장 파일의 각 모듈에 대해 한 개의 백업 데이터 인스턴스만 허용됩니다. 기존의 저장 파일을 지정하면 선택한 모듈의 데이터를 저장 파일 안에 덮어쓰거나 다른 저장 파일을 지정하라는 옵션이 제공됩니다. 기존의 저장 파일을 지정하면 파일 전체가 아니라 선택한 모듈에 대한 백업 데이터만 덮어쓰기됩니다.

2. 보안 토큰 및 암호를 사용하여 저장 파일을 암호화하고 보호하려면 **Password protect the storage file**(암호를 통한 저장 파일 보호)을 누릅니다. 그런 다음 보안 토큰 파일을 암호화할 암호를 입력하고 확인합니다.

3. 암호를 안전하게 캐시(저장)하도록 시스템을 구성하려면 **Remember all passwords and authentication values**(모든 암호 및 인증 값 기억)를 누릅니다. 이렇게 하면 무인 백업이 활성화됩니다. 이 기능을 활성화하면 보안 모듈에 입력된 모든 인증 값도 캐시할 수 있습니다.

4. 백업을 시작하려면 **Backup Now**(지금 백업)를 누르고, 백업을 지금 수행하지 않고 백업 구성을 저장하려면 **Next**(다음)를 누릅니다.

   백업 시작을 선택하면 작업이 끝나면서 “Backup Complete(백업 완료)” 페이지가 열립니다.

Backup Complete(백업 완료)

"Backup Complete(백업 완료)" 페이지는 백업 작업의 상태를 나타냅니다.

1. 오류를 포함하여 백업 작업에 관한 자세한 내용을 보려면 **View Log**(로그 보기)를 누릅니다.
2. **Finish**(마침)를 눌러 마법사를 종료합니다.

복원 마법사 사용

1. Security Manager 에서 **Backup and Restore**(백업 및 복원)를 누른 다음 **Restore**(복원)를 눌러 복원 마법사를 시작합니다.
2. 다음 복원 마법사 실행 시 "Welcome(시작)" 페이지를 생략하고 싶으면 **Show Welcome Screen**(시작 화면 표시) 확인란의 선택을 해제합니다.
3. **Next**(다음)를 누릅니다. "File Location(파일 위치)" 페이지가 열립니다.
4. 다음 하위 섹션을 참조하여 계속합니다.

File Location(파일 위치)

"File Location(파일 위치)" 페이지에서는 복원할 보안 인증서를 포함하고 있는 백업 저장 파일 및 보안 토큰 파일(가능한 경우)의 위치를 선택할 수 있습니다.

백업 파일의 위치를 선택하려면 다음 단계를 따르십시오.

1. 저장 파일이 페이지에 표시되지 않으면 **Edit**(편집) 버튼을 누른 다음 **Browse**(찾아보기)를 눌러 파일을 찾아봅니다.
2. 보안 토큰 파일이 페이지에 표시되지 않으면 **Edit**(편집) 버튼을 누른 다음 **Browse**(찾아보기)를 눌러 보안 토큰 파일의 위치를 찾아봅니다.
3. 필요한 경우 파일의 암호를 입력합니다.
4. **Next**(다음)를 누릅니다. "Security Modules(보안 모듈)" 페이지가 열립니다.

Security Modules(보안 모듈)

이 페이지에서는 "File Location(파일 위치)" 페이지에서 선택한 파일의 백업 데이터를 가진 설치된 모듈을 모두 표시합니다.

복원할 모듈을 선택하려면 다음과 같이 하십시오.

1. 각 행의 시작 부분에 있는 확인란을 선택한 다음 해당 모듈을 복원 목록에 추가합니다. 복원 목록의 모듈을 빠르게 추가하거나 제거하려면 **Select All**(모두 선택) 또는 **Clear All**(모두 지우기) 버튼을 누릅니다. 해당 모듈의 상태 열에 "Ready(준비)" 또는 "Needs Authentication(인증 필요)"이 표시되어야만 선택할 수 있습니다.

   주: 모듈이 준비되지 않은 경우에는 확인란을 선택할 수 없습니다. 모듈 상태를 업데이트한 다음에는 해당 열의 오른쪽에 있는 **Refresh**(새로 고침) 버튼을 눌러 상태 필드를 업데이트합니다. 모든 모듈의 상태를 업데이트하려면 **Refresh All**(모두 새로 고침) 버튼을 누릅니다.

2. 필요한 경우, 선택한 각 모듈의 인증 열에 요구되는 값을 입력합니다. 복원할 보안 장치에 액세스하려면 인증 값이 필요할 수도 있습니다. 인증 값에는 암호, PIN 등이 포함됩니다. 필드에 입력된 값은 즉시 확인됩니다.

3. **Next**(다음)를 누릅니다. "Confirmation(확인)" 페이지가 열립니다.

Confirmation(확인)

1. 복원 설정을 변경하려면 **Previous**(이전)를 눌러 복원 구성 화면으로 돌아갑니다.
2. 목록에 나열된 모듈의 인증서를 복원하고 싶은지 다시 한 번 확인한 다음 **Restore Now**(지금 복원)를 눌러 복원을 시작합니다.
3. 복원할 파일을 선택하고 **Finish**(마침)를 누릅니다.
4. 확인 대화상자에서 **Yes**(예)를 누릅니다.

△ 주의: 인증서를 복원하면 기존의 인증서가 덮어쓰기되어 데이터 손실 또는 시스템 잠금이 발생할 수 있습니다.

Restore Complete(복원 완료)

"Restore Complete(복원 완료)" 페이지는 복원 작업의 상태를 나타냅니다.

- 오류를 포함하여 복원 작업에 관한 자세한 내용을 보려면 **View Log**(로그 보기)를 누릅니다.
- **Finish**(마침)를 눌러 마법사를 종료합니다.

Settings(설정)

HP ProtectTools Security Manager for Administrators 에서 **Settings**(설정)를 눌러 설정 옵션을 변경합니다.

다음과 같은 Security Manager 설정을 사용할 수 있습니다.

- 호스트를 시작하고 특정 페이지를 활성화하거나 특정 응용프로그램을 시작하려면 **Show icon on the taskbar**(작업 표시줄에 아이콘 표시) 확인란을 선택하여 작업 표시줄 아이콘을 표시합니다.
- 설치된 모듈에서 생성되는 알림을 표시하려면 **Show Security Desktop Notifications**(보안 데스크탑 알림 표시) 확인란을 선택합니다.
- 백업 마법사의 "Welcome(시작)" 페이지를 보거나 생략합니다.
- 복원 마법사의 "Welcome(시작)" 페이지를 보거나 생략합니다.

3 HP ProtectTools Credential Manager

HP ProtectTools Credential Manager 는 다음과 같은 보안 기능으로 사용자 컴퓨터에 대한 무단 액세스를 차단합니다.

- Windows 로그온 시 Java Card 또는 생체인식 리더 등을 사용하여 암호를 대체하는 기능. 자세한 내용은 21페이지의 인증 정보 등록을 참조하십시오.
- 웹 사이트, 응용프로그램, 보호되는 네트워크 자원에 대한 인증 정보를 자동 기억하는 Single Sign On 기능
- Java Card 및 생체 인식기와 같은 선택 사양 보안 장치 지원
- 컴퓨터를 잠금 해제할 때 선택 사양 보안 장치를 통해 인증을 요구하는 등의 추가 보안 설정 지원

설정 절차

Credential Manger 에 로그온

구성에 따라 다음 방법 중 한 가지를 사용하여 Credential Manager 에 로그온할 수 있습니다.

- 알림 영역의 HP ProtectTools Security Manager for Administrators 아이콘
- Windows Vista®의 경우 **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager for Administrators** 를 누릅니다.
- Windows XP 의 경우 **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager** 를 누릅니다.

주: Windows Vista 에서 관리자용 HP ProtectTools Security Manager 를 시작하여 변경해야 합니다.

인증서 관리자에 로그온한 후 지문이나 Java 카드와 같은 인증서를 추가로 등록할 수 있습니다. 자세한 내용은 21페이지의 인증 정보 등록을 참조하십시오.

다음 번 로그온할 때 로그온 정책을 선택하고 등록된 인증 정보를 원하는 대로 조합하여 사용할 수 있습니다.

Credential Manager Logon Wizard(Credential Manager 로그온 마법사) 사용

Credential Manager Logon Wizard 를 사용하여 Credential Manger 에 로그온하려면 다음과 같이 하십시오.

1. 다음 방법 중 하나로 Credential Manager Logon Wizard(Credential Manager 로그온 마법사)를 엽니다.
   - Windows 로그온 화면에서 엽니다.
   - 알림 영역에서 **HP ProtectTools Security Manager for Administrators** 아이콘을 두 번 눌러 엽니다.
   - HP ProtectTools Security Manager for Administrators 의 "Credential Manager(인증서 관리자)" 페이지에서 화면 오른쪽 상단에 있는 **Log On**(로그온) 링크를 눌러 엽니다.
2. 화면의 지침에 따라 Credential Manager 에 로그온합니다.

인증 정보 등록

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

지문 등록

지문 인식기를 사용하면 Windows 암호 대신 지문 인증을 사용하여 Windows 에 로그온할 수 있습니다.

지문 인식기 설정

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **My Identity**(내 ID)를 누른 다음 **Register Fingerprints**(지문 등록)를 누릅니다.
3. 화면 지침을 따라 지문 등록 및 지문 인식기 설정을 완료합니다.
4. 다른 Windows 사용자에 대해 지문 인식기를 설정하려면 해당 사용자로 Windows 에 로그온한 후 위의 단계를 반복합니다.

등록된 지문을 사용하여 Windows 에 로그온

1. 지문 등록 직후 Windows 를 재시작합니다.
2. Windows 시작 화면이 나타나면 등록된 손가락 중 하나를 통과시켜 Windows 에 로그온합니다.

Registering a Smart Card or Token(스마트 카드 또는 토큰 등록)

스마트 카드는 신용카드 크기만한 플라스틱 카드이며 그 안에는 정보와 함께 로드할 수 있는 내장 마이크로칩이 들어있습니다. 스마트 카드는 개인 사용자들의 정보를 보호하고 이들을 인증합니다. 스마트 카드로 네트워크에 로그온하면 암호 기반 식별을 사용할 때 강력한 인증 방식을 제공하며 사용자를 도메인에서 인증할 때 소유 증명을 제공할 수 있습니다.

USB 토큰은 단지 폼팩터가 다른 스마트 카드입니다. 플라스틱 신용 플랫폼에 스마트 칩을 배치하기보다는 스마트 칩을 USB 키라고 하는 플라스틱 토큰에 집어넣습니다. 스마트 카드와 토큰의 주요 차이점은 액세스 인터페이스에 있습니다. 카드에는 판독기가 필요하지만 토큰은 아무 USB 포트에나 직접 연결합니다. 인증 정보를 보관하고 제공하는 핵심 기능에는 차이가 없습니다.

USB 토큰은 강력한 인증에 사용합니다. 보안을 강화하고 안전한 정보 액세스를 보장합니다.

주: 이 절차를 진행하려면 카드 리더가 구성되어 있어야 합니다. 리더가 설치되어 있지 않은 경우 23페이지의 가상 토큰 생성에 설명된 가상 토큰을 등록할 수 있습니다.

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **My Identity**(내 ID)를 누른 다음 **Register Smart Card or Token**(스마트 카드 또는 토큰 등록)을 누릅니다.
3. **Device Type** 대화 상자에서 원하는 장치 유형을 누른 다음 **Next**(다음)를 누릅니다.
4. 장치 유형으로 스마트 카드나 USB 토큰을 선택한 경우 USB 포트에 스마트 카드를 넣거나 토큰을 연결해야 합니다.

   주: 스마트 카드가 들어있지 않거나 USB 토큰이 연결되지 않았다면 Select Token 대화 상자에서 Next 버튼이 비활성화됩니다.
5. Device Type 대화 상자에서 **Next**(다음)를 선택합니다.

   Token Properties 대화 상자가 나타납니다.
6. User PIN 을 입력하고 **Register smart card or token for authentication**(인증용 스마트 카드 또는 토큰 등록)을 선택한 다음 **Finish**(마침)를 누릅니다.

기타 인증 정보 등록

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **My Identity**(내 ID)를 누른 다음 **Register Credentials** 을 누릅니다.

   Credential Manager Registration Wizard 가 열립니다.
3. 화면 지침을 따릅니다.

일반 작업

모든 사용자는 Credential Manager 의 "My Identity(내 ID)" 페이지에 액세스할 수 있습니다. "My Identity(내 ID)" 페이지에서 다음과 같은 작업을 수행할 수 있습니다.

- Windows 로그온 암호 변경
- 토큰 PIN 변경
- 워크스테이션 잠금

주: 이 옵션은 Credential Manager 의 기본 로그온 프롬프트가 활성화되어 있는 경우에만 사용할 수 있습니다. 30페이지의 예 1 - “Advanced Settings(고급 설정)” 페이지를 사용하여 Credential Manager 에서 Windows 로그온 허용을 참조하십시오.

가상 토큰 생성

가상 토큰은 Java Card 또는 USB Token 과 매우 유사한 원리로 작동합니다. 가상 토큰은 컴퓨터 하드 드라이브나 Windows 레지스트리에 저장됩니다. 가상 토큰으로 로그온하는 경우 인증을 완료하기 위해 사용자 PIN 을 입력해야 합니다.

새 가상 토큰을 생성하려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **My Identity**(내 ID)를 누른 다음 **Register Smart Card or Token**(스마트 카드 또는 토큰 등록)을 누릅니다.
3. **Device Type** 대화 상자에서 **Virtual Token** 을 누른 다음 **Next**(다음)를 누릅니다.
4. 토큰 이름과 위치를 지정하고 **Next**(다음)를 누릅니다.

   새 가상 토큰이 파일이나 Windows 레지스트리 데이트베이스에 저장될 수도 있습니다.
5. Token Properties 대화 상자에서 새로 생성된 가상 토큰을 위한 Master PIN 과 User PIN 을 지정하고 **Register smart card or token for authentication**(인증용 스마트 카드 또는 토큰 등록)을 선택한 다음 **Finish**(마침)를 누릅니다.

   Token Properties 대화 상자가 나타납니다.
6. User PIN 을 입력하고 **Register smart card or token for authentication**(인증용 스마트 카드 또는 토큰 등록)을 선택한 다음 **Finish**(마침)를 누릅니다.

Windows 로그온 암호 변경

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **My Identity**(내 ID)를 누른 다음 **Register Fingerprints**(지문 등록)를 누릅니다.
3. **Old Password**(이전 암호) 입력란에 기존 암호를 입력합니다.
4. **New password**(새 암호) 입력란에 새 암호를 입력하고 **Confirm password**(암호 확인) 입력란에 다시 입력합니다.
5. **Finish**(마침)를 누릅니다.

토큰 PIN 변경

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **My Identity**(내 ID)를 누른 다음 **Change Token PIN**(토큰 PIN 변경)을 누릅니다.
3. Device Type 대화 상자에서 원하는 장치 유형을 누른 다음 **Next**(마침)를 누릅니다.
4. PIN 을 변경할 토큰을 선택한 다음 **Next**(다음)를 누릅니다.
5. 화면에 표시되는 지침에 따라 PIN 변경을 완료합니다.

주: 토큰 PIN 을 몇 차례 연속해서 잘못 입력하면 토큰이 잠겨버립니다. 그러면 이를 해제할 때까지 이 토큰을 사용할 수 없습니다.

컴퓨터 잠금 (워크스테이션)

이 기능은 Credential Manager 를 사용하는 Windows 에 로그온하는 경우에만 사용할 수 있습니다. 자리를 비웠을 때 컴퓨터의 보안을 유지하려면 "Lock Workstation(워크스테이션 잠금)" 기능을 사용합니다. 이 기능은 권한이 없는 사용자가 컴퓨터에 무단으로 액세스하는 것을 차단합니다. 해당 컴퓨터의 사용자와 관리자 그룹 구성원만 잠금을 해제할 수 있습니다.

주: 이 옵션은 Credential Manager 의 기본 로그온 프롬프트가 활성화되어 있는 경우에만 사용할 수 있습니다. 30페이지의 예 1 - “Advanced Settings(고급 설정)” 페이지를 사용하여 Credential Manager 에서 Windows 로그온 허용을 참조하십시오.

보안을 강화하기 위해 Java Card, 생체인식 리더 또는 토큰을 통해 컴퓨터의 잠금을 해제하도록 워크스테이션 잠금 기능을 구성할 수 있습니다. 자세한 내용은 30페이지의 Credential Manager 설정 구성를 참조하십시오.

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **My Identity**(내 ID)를 누릅니다.
3. **Lock Workstation**(워크스테이션 잠금)을 눌러 컴퓨터를 즉시 잠급니다.

   컴퓨터의 잠금을 해제하려면 Windows 암호나 Credential Manager Logon Wizard 를 사용해야 합니다.

Windows 로그온 사용

Credential Manager 를 사용하여 로컬 컴퓨터 또는 네트워크 도메인의 Windows 에 로그온할 수 있습니다. Credential Manager 에 처음으로 로그온할 때 사용자의 로컬 Windows 계정이 자동으로 Windows 로그온 서비스 계정으로 추가됩니다.

Credential Manager 로 Windows 에 로그온

Credential Manager 를 사용하여 Windows 네트워크나 로컬 계정에 로그온할 수 있습니다.

1. Windows 에 로그온할 수 있도록 지문을 등록한 경우, 손가락을 통과시켜 로그온합니다.
2. Windows XP 에서 Windows 로그온 지문을 등록하지 않은 경우 지문 아이콘 옆 화면의 왼쪽 윗 부분의 키보드 아이콘을 누릅니다. Credential Manager Logon Wizard 가 열립니다.

   Windows Vista 에서 Windows 로그온 지문을 등록하지 않은 경우 로그온 화면에서 **Credential Manager** 아이콘을 누릅니다. Credential Manager Logon Wizard 가 열립니다.

3. **User name**(사용자 이름) 화살표를 누른 다음 해당하는 사용자 이름을 누릅니다.
4. **Password**(암호) 입력란에 암호를 입력하고 **Next**(다음)를 누릅니다.
5. **More**(상세 정보)를 선택한 다음 **Wizard Options** 을 누릅니다.
   a. 이 사용자 이름을 다음에 컴퓨터에 로그온할 때 기본 사용자 이름으로 사용하려면 **Use last user name on next logon**(다음 번 로그온 시 마지막 사용한 사용자 이름 사용) 확인란을 선택합니다.
   b. 이 로그온 정책을 기본 방법으로 지정하려면 **Use last policy on next logon**(다음 번 로그온 시 마지막 사용한 정책 사용) 확인란을 선택합니다.
6. 화면 지침을 따릅니다. 인증 정보가 올바르다면 Windows 계정과 Credential Manager 에 로그온됩니다.

Single Sign On 사용

Credential Manage 에는 여러 인터넷 및 Windows 프로그램에 대한 사용자 이름과 암호를 저장하고, 등록된 프로그램에 액세스할 때 자동으로 로그온 인증 정보를 입력하는 Single Sign On 기능이 있습니다.

주: Single Sign On 의 주요 기능은 보안과 개인 정보 보호입니다. 모든 인증 정보는 암호화되며 Credential Manager 에 로그온한 다음에만 사용할 수 있습니다.

주: 또한 Java Card, 지문 리더 또는 토큰을 통해 보안 사이트나 보안 프로그램에 로그온하기 전에 인증서를 확인하도록 SSO(Single Sign On)를 구성할 수도 있습니다. 이 구성은 은행 계좌 번호와 같은 개인 정보가 담긴 프로그램이나 웹 사이트에 로그온할 때 특히 유용합니다. 자세한 내용은 30페이지의 Credential Manager 설정 구성을 참조하십시오.

새 응용프로그램 등록

Credential Manager 에서는 사용자가 Credential Manager 에 로그온한 상태에서 실행한 응용프로그램을 등록할 것인지 묻는 메시지가 표시됩니다. 응용프로그램은 수동으로 등록할 수도 있습니다.

자동 등록 사용

1. 로그온해야 할 응용프로그램을 엽니다.
2. 프로그램 또는 웹 사이트 암호 대화 상자에서 Credential Manager SSO 아이콘을 누릅니다.
3. 해당 프로그램 또는 웹 사이트의 암호를 입력하고 **확인**을 누릅니다. **Credential Manager Single Sign On** 대화 상자가 열립니다.
4. **More**(상세 정보)를 누르고 다음 옵션 중에서 선택합니다.
   - Do not use SSO for this site or application(이 사이트나 응용프로그램에 SSO 를 사용하지 않음)
   - Prompt to select account for this application(이 응용프로그램에 대한 계정 선택 요청 메시지 표시)
   - Fill in credentials but do not submit(인증 정보만 입력하고 제출하지 않음)

- Authenticate user before submitting credentials(인증 정보 제출 전에 사용자 인증)
- Show SSO shortcut for this application(이 응용프로그램에 대한 SSO 바로 가기 표시)

5. **Yes**(예)를 눌러 등록을 완료합니다.

수동(끌어다 놓기) 등록 사용

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누른 다음 왼쪽 창에 있는 **Services and Applications**(서비스 및 응용프로그램)를 누릅니다.
2. **Manage Applications and Credentials**(응용프로그램 및 인증서 관리)를 누릅니다.

   Credential Manager Single Sign On 대화 상자가 나타납니다.
3. 미리 등록된 웹 사이트나 응용프로그램을 수정 또는 제거하려면 목록에서 원하는 기록을 선택합니다.
4. 화면 지침을 따릅니다.

응용프로그램 및 인증 정보 관리

응용프로그램 속성 수정

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누른 다음 왼쪽 창에 있는 **Services and Applications**(서비스 및 응용프로그램)를 누릅니다.
2. **Manage Applications and Credentials**(응용프로그램 및 인증서 관리)를 누릅니다.

   Credential Manager Single Sign On 대화 상자가 나타납니다.
3. 수정할 응용프로그램 항목을 누른 다음 **Properties**(속성)를 누릅니다.
4. **General**(일반) 탭을 눌러 응용프로그램 이름과 설명을 수정합니다. 각 설정 옆에 있는 확인란을 선택하거나 선택 취소하여 설정을 적절히 변경합니다.
5. **Script**(스크립트) 탭을 눌러 SSO 응용프로그램 스크립트를 확인 및 편집합니다.
6. **확인**을 누릅니다.

Single Sign On 에서 응용프로그램 제거

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누른 다음 왼쪽 창에 있는 **Services and Applications**(서비스 및 응용프로그램)를 누릅니다.
2. **Manage Applications and Credentials**(응용프로그램 및 인증서 관리)를 누릅니다.

   Credential Manager Single Sign On 대화 상자가 나타납니다.
3. 제거할 응용프로그램 항목을 누른 다음 **Remove**(제거)를 누릅니다.
4. 확인 대화 상자에서 **Yes**(예)를 누릅니다.
5. **확인**을 누릅니다.

응용프로그램 내보내기

응용프로그램을 내보내서 Single Sign On 응용프로그램 스크립트의 백업 사본을 만들 수 있습니다. 백업 사본은 Single Sign On 데이터 복구에 사용됩니다. 이 파일은 인증 정보만 포함하는 ID 백업 파일을 보완하는 역할을 합니다.

응용프로그램을 내보내려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누른 다음 왼쪽 창에 있는 **Services and Applications**(서비스 및 응용프로그램)를 누릅니다.
2. **Manage Applications and Credentials**(응용프로그램 및 인증서 관리)를 누릅니다.

   Credential Manager Single Sign On 대화 상자가 나타납니다.
3. 내보낼 응용프로그램 항목을 누른 다음 **More**(상세 정보)를 누릅니다.
4. 화면 지침에 따라 내보내기를 완료합니다.
5. **확인**을 누릅니다.

응용프로그램 가져오기

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누른 다음 왼쪽 창에 있는 **Services and Applications**(서비스 및 응용프로그램)를 누릅니다.
2. **Manage Applications and Credentials**(응용프로그램 및 인증서 관리)를 누릅니다.

   Credential Manager Single Sign On 대화 상자가 나타납니다.
3. 가져올 응용프로그램 항목을 누른 다음 **More**(상세 정보)를 누릅니다.
4. 화면 지침에 따라 가져오기를 완료합니다.
5. **확인**을 누릅니다.

인증 정보 수정

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누른 다음 **Services and Applications**(서비스 및 응용프로그램)를 누릅니다.
2. **Manage Applications and Credentials**(응용프로그램 및 인증서 관리)를 누릅니다.

   Credential Manager Single Sign On 대화 상자가 나타납니다.
3. 수정할 응용프로그램 항목을 누른 다음 **More**(상세 정보)를 누릅니다.
4. 다음과 같은 옵션을 선택할 수 있습니다.
   - 응용프로그램
     - 새로 추가
     - 제거
     - 속성

- 스크립트 가져오기
- 스크립트 내보내기

- 인증 정보
  - 새로 만들기
- 암호 보기

주: 암호를 보기 전에 ID 를 인증해야 합니다.

5. 화면 지침을 따릅니다.
6. **확인**을 누릅니다.

응용프로그램 보호 사용

이 기능을 사용하여 응용프로그램에 대한 액세스를 구성할 수 있습니다. 다음과 같은 기준에 근거하여 액세스를 제한할 수 있습니다.

- 사용자 범주
- 사용 시간
- 사용자 작동 중지

응용프로그램 액세스 제한

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누른 다음 **Services and Applications**(서비스 및 응용프로그램)를 누릅니다.
2. **Application Protection**(응용프로그램 보호)을 누른 다음 **Manage Protected Applications**(보호된 응용프로그램 관리)를 누릅니다.
3. 관리할 액세스에 대한 사용자 범주를 선택합니다.

주: 범주가 모두가 아닌 경우, **Override default settings**(기본 설정 무시)를 선택하여 모두 범주에 대한 설정을 무시해야 할 수 있습니다.

4. **Add**(추가)를 누릅니다.

   Add a Program Wizard(프로그램 마법사 추가)가 열립니다.
5. 화면 지침을 따릅니다.

응용프로그램에서 보호 제거

응용프로그램에서 제한을 제거하려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **Services and Applications**(서비스 및 응용프로그램)을 누릅니다.
3. **Application Protection**(응용프로그램 보호)을 누른 다음 **Manage Protected Applications**(보호된 응용프로그램 관리)를 누릅니다.
4. 관리할 액세스에 대한 사용자 범주를 선택합니다.

주: 범주가 모두가 아닌 경우, **Override default settings**(기본 설정 무시)를 눌러 모두 범주에 대한 설정을 무시해야 할 수 있습니다.

5. 제거할 응용프로그램 항목을 누른 다음 **Remove**(제거)를 누릅니다.
6. **확인**을 누릅니다.

보호되는 응용프로그램에 대한 제한 설정 변경

1. **Application Protection**(응용프로그램 보호)을 누른 다음 **Manage Protected Applications**(보호된 응용프로그램 관리)를 누릅니다.
2. 관리할 액세스에 대한 사용자 범주를 선택합니다.

주: 범주가 모두가 아닌 경우, **Override default settings**(기본 설정 무시)를 눌러 모두 범주에 대한 설정을 무시해야 할 수 있습니다.

3. 변경할 응용프로그램을 누른 다음 **Properties**(속성)를 누릅니다. 해당 응용프로그램의 **Properties**(속성) 대화 상자가 열립니다.
4. **General**(일반) 탭을 누릅니다. 다음 설정 중 하나를 선택합니다.
   - Disabled(비활성화)(사용할 수 없음)
   - Enabled(활성화)(제한 없이 사용 가능)
   - Restricted(제한)(설정에 따라 사용)
5. 제한을 선택한 경우에는 다음 설정을 사용할 수 있습니다.
   a. 시간, 요일, 또는 날짜에 따라 사용을 제한하려는 경우, **Schedule**(예약) 탭을 누르고 설정을 구성합니다.
   b. 작동 중지 여부에 따라 사용을 제한하려는 경우, **Advanced**(고급) 탭을 누르고 작동 중지 기간을 선택합니다.
6. **확인**을 눌러 응용프로그램 **Properties**(속성) 대화 상자를 닫습니다.
7. **확인**을 누릅니다.

고급 작업(관리자 전용)

Credential Manager 의 “Multifactor Authentication(다단계 인증)” 페이지 및 “Settings(설정)” 페이지는 관리자 권한을 가진 사용자만 사용할 수 있습니다. 이 페이지에서 다음과 같은 작업을 수행할 수 있습니다.

- 인증 정보 속성 구성
- Credential Manager 설정 구성

인증 정보 속성 구성

“Multifactor Authentication(다단계 인증)” 페이지의 Credentials 탭에서는 사용 가능한 인증 방법의 목록을 보거나 설정을 수정할 수 있습니다.

인증 정보를 구성하려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **Multifactor Authentication**(다단계 인증)을 누릅니다.
3. **Credentials**(인증 정보) 탭을 누릅니다.
4. 수정할 인증 정보 유형을 누릅니다. 다음 중 한 가지 방법으로 인증 정보를 수정할 수 있습니다.
   - 인증 정보를 등록하려면 **Register**(등록)를 누르고 화면 지침에 따릅니다.
   - 인증 정보를 삭제하려면 확인 대화 상자에서 **Clear**(지우기)를 누른 다음 **Yes**(예)를 누릅니다.
   - 인증 정보 속성을 수정하려면 **Properties**(속성)를 누른 다음 화면 지침에 따릅니다.
5. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

Credential Manager 설정 구성

"Settings(설정)" 페이지에서는 다음과 같은 탭을 사용하여 다양한 설정에 액세스하거나 설정을 수정할 수 있습니다.

- General(일반) - 기본 구성에 대한 설정을 수정할 수 있습니다.
- Single Sign On - 현재 사용자에 대한 Single Sign On 의 동작 방법(예: 로그온 화면 탐지, 등록된 로그온 대화 상자로 자동 로그온, 암호 표시 등의 처리) 설정을 수정할 수 있습니다.
- Services and Applications(서비스 및 응용프로그램) - 사용 가능한 서비스를 확인하고 이러한 서비스에 대한 설정을 수정할 수 있습니다.
- Security(보안) - 지문 인식기 소프트웨어를 선택하고 지문 인식기의 보안 수준을 조정할 수 있습니다.
- Smart Cards and Tokens(스마트 카드 및 토큰) - 사용 가능한 모든 Java Card 및 토큰의 속성을 확인하고 수정할 수 있습니다.

Credential Manager 설정을 수정하려면 다음과 같이 하십시오.

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **Settings**(설정)을 누릅니다.
3. 수정할 설정에 해당하는 탭을 누릅니다.
4. 화면 지침에 따라 설정을 수정합니다.
5. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

예 1 - "Advanced Settings(고급 설정)" 페이지를 사용하여 Credential Manager 에서 Windows 로그온 허용

1. HP ProtectTools Security Manager for Administrators 에서 왼쪽 창에 있는 **Credential Manager**(인증서 관리자)를 누릅니다.
2. **Settings**(설정)을 누릅니다.

3. **General**(일반) 탭을 누릅니다.

4. **Select the way users log on to Windows**(사용자의 Windows 로그온 방법 선택)에서 **Use Credential Manager to log on to Windows**(인증서 관리자를 통해 Windows 에 로그온) 확인란을 선택합니다.

5. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

6. 컴퓨터를 재시작합니다.

주: **Use Credential Manager to log on to Windows**(인증서 관리자를 통해 Windows 에 로그온) 확인란을 선택하면 컴퓨터를 잠글 수 있습니다. 24페이지의 컴퓨터 잠금 (워크스테이션)을 참조하십시오.

주: Windows XP 의 경우 위의 절차와 약간 다를 수 있습니다.

예 2 - "Advanced Settings(고급 설정)" 페이지를 사용하여 Single Sign On 에 앞서 사용자 확인 요구

1. HP ProtectTools Security Manager for Administrators 에서 **Credential Manager**(인증서 관리자)를 누른 다음 **Settings**(설정)를 누릅니다.

2. **Single Sign On** 탭을 누릅니다.

3. **When registered logon dialog or Web page is visited**(등록된 로그온 대화 상자 또는 웹 페이지를 방문할 때)에서 **Authenticate user before submitting credentials**(인증 정보 제출 전에 사용자 인증) 확인란을 선택합니다.

4. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

5. 컴퓨터를 재시작합니다.

4 Drive Encryption for HP ProtectTools

△ 주의: Drive Encryption 모듈을 설치 제거하려는 경우 또는 백업 및 복원 솔루션을 사용하고 있는 경우에는, 먼저 암호화된 모든 드라이브의 암호를 해독해야 합니다. 그렇지 않으면 Drive Encryption 복구 서비스에 등록되어 있지 않은 이상 암호화된 드라이브의 데이터에 액세스할 수 없습니다. Drive Encryption 모듈을 재설치하면 암호화된 드라이브에 액세스할 수 없게 됩니다.

설치 절차

Drive Encryption 열기

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. **Drive Encryption** 을 누릅니다.

일반 작업

Drive Encryption 활성화

HP ProtectTools Security Manager for Administrators 설치 마법사를 통해 Drive Encryption 을 활성화합니다.

Drive Encryption 비활성화

HP ProtectTools Security Manager for Administrators 설치 마법사를 통해 Drive Encryption 을 비활성화합니다.

Drive Encryption 이 활성화된 후 로그인

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

주: Windows 관리자가 HP ProtectTools Security Manager for Administrators 의 Pre-boot Security 를 활성화한 경우에는 Drive Encryption 로그온 화면에서 로그인하는 대신 컴퓨터가 켜지면 바로 컴퓨터에 로그인할 수 있습니다.

1. 사용자 이름을 선택한 다음 Windows 암호 또는 Java™ Card PIN 을 입력하거나 등록된 손가락을 통과시킵니다.
2. **OK**(확인)를 누릅니다.

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

고급 작업

Drive Encryption 관리 (관리자 작업)

"Encryption Management(암화화 관리)" 페이지에서 Windows 관리자는 Drive Encryption 상태를 확인 및 변경 (활성 또는 비활성)하거나 컴퓨터의 모든 하드 드라이브 상태를 확인 및 암호화할 수 있습니다.

TPM-보호 암호 활성화

Embedded Security for HP ProtectTools 를 사용하여 TPM 을 활성화합니다. 활성화한 다음 Drive Encryption 로그온 화면에서 로그인하려면 Windows 사용자 이름 및 암호가 필요합니다.

주: 암호는 TPM 보안 칩으로 보호되기 때문에 하드 드라이브를 다른 컴퓨터로 옮긴 경우 TPM 설정을 옮긴 컴퓨터로 마이그레이션해야 데이터에 액세스할 수 있습니다.

1. Embedded Security for HP ProtectTools 를 사용하여 TPM 을 활성화합니다.
2. Drive Encryption 을 연 다음 **암호화 관리**를 누릅니다.
3. **TPM-protected password**(TPM 보호 암호) 확인란을 선택합니다.

개별 드라이브 암호화 또는 암호 해제

1. Drive Encryption 을 연 다음 **암호화 관리**를 누릅니다.
2. **암호화 변경**을 누릅니다.
3. 암호화 변경 대화 상자에서 암호화하거나 암호 해제하려는 각 하드 드라이브 옆의 확인란을 선택 또는 선택 해제한 후 **확인**을 누릅니다.

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

백업 및 복구 (관리자 작업)

"Recovery(복구)" 페이지에서 Windows 관리자는 암호화 키를 백업하거나 복구할 수 있습니다.

백업 키 생성

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

1. Drive Encryption 을 연 후 **복구**를 누릅니다.
2. **키 백업**을 누릅니다.
3. "Select Backup Disk(백업 디스크 선택)" 페이지에서 암호화 키를 백업할 장치 이름을 누른 후 **Next**(다음)를 누릅니다.

4. 다음 페이지에 표시된 정보를 읽은 후 **다음**을 누릅니다.

   암호화 키가 선택한 저장 장치에 저장됩니다.

5. 확인 대화 상자가 표시되면 **확인**을 누릅니다.

온라인 복구 등록

온라인 Drive Encryption 키 복구 서비스에서는 암호화 키 백업 사본을 저장하기 때문에 암호가 생각나지 않는 경우에도 백업 암호 없이 컴퓨터에 액세스할 수 있습니다.

주: 인터넷에 연결되어 있고 유효한 전자 우편 주소가 있어야 이 서비스를 통해 암호를 복구하거나 등록할 수 있습니다.

1. Drive Encryption 을 연 후 **복구**를 누릅니다.
2. **Register**(등록)를 누릅니다.
3. 다음 옵션 중 하나를 누릅니다.
   - 이 PC 에 대한 새 복구 계정을 만들겠습니다. 이 옵션을 선택한 경우 전자 우편 주소와 기타 정보를 입력한 다음 **다음**을 누릅니다.
   - 기존 웹 복구 계정에 이 PC 를 추가하겠습니다.
4. 암호를 생성 및 확인하고 보안 질문을 선택 및 답을 입력한 다음 **다음**을 누릅니다.

   주: 계정 활성화 코드는 입력한 전자 우편 주소로 전송됩니다.

5. 활성화 코드를 입력한 다음 **다음**을 누릅니다.
6. 컴퓨터 일련 번호를 입력한 다음 **다음**을 누릅니다.

   주: 컴퓨터 일련 번호를 찾으려면 **시작**을 클릭한 다음 **도움말 및 지원**을 클릭합니다.

7. 가입 쿠폰이 없는 경우 **쿠폰을 구입하려면 여기를 누르십시오**. 링크를 누릅니다.

   링크를 누르면 SafeBoot 복구 서비스 웹 사이트로 연결됩니다. 마법사를 종료하지 마십시오.

8. **Purchase Coupon Codes**(쿠폰 코드 구입)를 누릅니다.
9. 국가, 컴퓨터 유형을 선택한 다음 **Start**(시작)를 누릅니다.
10. 1 년 가입 옵션 또는 3 년 가입 옵션 옆에 있는 **Buy**(구입)를 누릅니다.
11. **Checkout**(결제)을 누릅니다.
12. 계약 내용을 읽은 다음 **Accept**(동의)를 누릅니다.
13. 대금 청구 정보를 입력한 다음 **Continue**(계속)를 누릅니다.
14. 신용 카드 정보를 입력한 다음 **Make Payment**(비용 계산)를 누릅니다.
15. 쿠폰 코드를 기록한 다음 마법사에서 “Account Activation(계정 활성화)” 페이지로 돌아갑니다.
16. 계정 활성화 코드를 입력한 다음 **다음**을 누릅니다.
17. 확인 대화 상자가 표시되면 **확인**을 누릅니다.

기존 온라인 복구 계정 관리

암호가 기억나지 않거나, 개인 설정을 수정하거나, 온라인 복구 계정에 사용하는 암호를 재설정하거나, 계정을 보거나 갱신하려는 경우 온라인 복구 계정을 생성하면 SafeBoot 복구 서비스 웹 사이트에 액세스하여 컴퓨터에 대한 액세스를 복구할 수 있습니다.

1. Drive Encryption 을 연 후 **복구**를 누릅니다.
2. **Manage**(관리)를 누릅니다.
3. "SafeBoot Recovery Service(SafeBoot 복구 서비스)" 웹 페이지가 열리면 **Recovery Service Account**(복구 서비스 계정) 또는 **Recovery Process**(복구 프로세스)를 누릅니다.
4. 복구 서비스 로그온 페이지에서 전자 우편 주소, 암호를 입력하고 상자에 표시되는 숫자 및 문자도 입력합니다.
5. **Logon**(로그온)을 누릅니다.
6. **Profile**(프로필)을 눌러 전화 번호 또는 대금 청구 주소와 같은 개인 정보를 업데이트합니다.

   또는

   Reset Password(암호 재설정)를 눌러 암호를 재설정하거나 변경합니다.

   또는

   My Subscription(가입 내역)을 눌러 현재 가입 정보를 확인합니다.

주: 또한 "My Subscription(가입 내역)" 페이지에서 가입 정보를 갱신할 수 있습니다. **Renew Subscription**(가입 갱신)을 눌러 이 작업을 수행합니다.

복구 수행

로컬 복구 수행

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

   복구 프로세스가 완료되면 컴퓨터가 시작됩니다.

주: 복구를 수행한 후 암호를 재설정하는 것이 좋습니다.

온라인 복구 수행

주: 이 단원에서는 인터넷 연결을 통해 다른 컴퓨터에 액세스할 때 온라인 복구를 수행하는 방법에 대해 설명합니다. 해당 컴퓨터에 액세스할 수 없는 경우 HP 기술 지원으로 문의하십시오.

1. 컴퓨터의 전원을 켭니다.
2. HP ProtectTools Drive Encryption 로그온 대화 상자가 열리면 **취소**를 누릅니다.
3. 화면 왼쪽 아래에 있는 **옵션**을 누른 다음 **복구**를 누릅니다.
4. **웹 복구**를 누르고 **다음**을 누릅니다.
5. 클라이언트 코드를 기록한 다음 **다음**을 누릅니다.
6. 인터넷으로 연결된 다른 컴퓨터에서 SafeBoot 복구 서비스 웹 사이트(http://www.safeboot-hp.com)에 액세스합니다.
7. **Recovery Process**(프로세스 복구)를 누릅니다.
8. 복구 서비스 로그온 페이지에서 전자 우편 주소, 암호를 입력하고 상자에 표시되는 숫자 및 문자도 입력합니다.
9. **Logon**(로그온)을 누릅니다.
10. **Recovery Process**(프로세스 복구)를 누릅니다.
11. 복구하려는 컴퓨터에서 기록한 클라이언트 코드를 입력하고 상자에 나타나는 숫자와 문자를 입력합니다.
12. **Submit**(제출)을 누릅니다.
13. 응답 키의 각 줄을 기록합니다.
14. SafeBoot 복구 서비스 웹 사이트에서 기록한 첫 번째 줄의 응답 키를 복구하려는 컴퓨터에 입력한 다음 **Enter**(입력)을 누릅니다.
15. 두 번째 줄의 응답 키를 입력한 다음 **Enter**(입력)을 누릅니다.
16. 세 번째 줄의 응답 키를 입력한 다음 **Enter**(입력)을 누릅니다.
17. 네 번째 줄의 응답 키를 입력한 다음 **Enter**(입력)을 누릅니다.

    주: 네 번째 줄의 응답 키가 처음 3 개의 응답 키보다 짧습니다.

18. **마침**을 누릅니다.

주: 복구를 수행한 후 암호를 재설정하는 것이 좋습니다.

5 Privacy Manager for HP ProtectTools

Privacy Manager 는 Microsoft 메일, Microsoft Office 문서 및 Live Messenger 사용 시 소스, 무결성, 통신 보안 등을 확인하는 인증서를 얻는 데 사용되는 도구입니다.

Privacy Manager 는 HP ProtectTools Security Manager for Administrators 에서 제공되는 보안 인프라를 활용하며, 여기에는 다음과 같은 보안 로그온 방법들이 포함됩니다.

- 지문 인증
- Windows® 암호
- HP ProtectTools Java™ Card
- Virtual Token(가상 토큰)
- Embedded Security for HP ProtectTools 기본 사용자 키

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

Privacy Manager 열기

Privacy Manager 를 열려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. **Privacy Manager: Sign and Chat**(Privacy Manager: 서명 및 채팅)을 누릅니다.

또는

작업 표시줄의 오른쪽 끝에 있는 알림 영역에서 **HP ProtectTools** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **Privacy Manager: Sign and Chat**(Privacy Manager: 서명 및 채팅)을 선택하고 **Configuration**(구성)을 누릅니다.

또는

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

또는

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

설치 절차

Privacy Manager 인증서 관리

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

Privacy Manager 인증서 요청 및 설치

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

Privacy Manager 인증서 요청

1. Privacy Manager 를 열고 **Certificate Manager**(인증서 관리자)를 누릅니다.
2. **Privacy Manager Certificate** Request(요청)를 누릅니다.
3. “Welcome(시작)” 페이지의 내용을 읽은 후 **Next**(다음)를 누릅니다.
4. “License Agreement(사용권 계약)” 페이지에서 사용권 계약을 읽습니다.
5. **Check here to accept the terms of this license agreement**(여기를 눌러 사용권 계약 내용에 동의합니다) 옆의 확인란이 선택되었는지 확인하고 **Next**(다음)를 누릅니다.
6. “Your Certificate Details(인증서 세부 정보)” 페이지에 필요한 정보를 입력한 후 **Next**(다음)를 누릅니다.
7. “Certificate Request Accepted(인증서 요청 동의함)” 페이지에서 **Finish**(마침)를 누릅니다.

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

Privacy Manager 인증서 설치

1. Privacy Manager 인증서가 첨부된 전자 우편을 받으면 전자 우편을 열고 메시지의 오른쪽 아래 모퉁이에 있는 **Setup**(설치) 버튼을 누릅니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.
3. “Certificate Installed(인증서 설치됨)” 페이지에서 **Next**(다음)를 누릅니다.
4. “Certificate Backup(인증서 백업)” 페이지에 백업 파일의 위치와 이름을 입력하거나 **Browse**(찾아보기)를 눌러 위치를 검색합니다.

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

5. 암호를 입력하고 확인한 후 **Next**(다음)를 누릅니다.

6. 선택한 보안 로그온 방법을 사용하여 인증합니다.
7. 신뢰할 수 있는 연락처 초대를 시작하도록 선택한 경우 화면의 지침을 따르십시오.

   또는

   Cancel(취소)을 누른 경우 Trusted Contact(신뢰할 수 있는 연락처)을 나중에 추가하는 방법은 Managing Trusted Contacts 을 참조하십시오.

Privacy Manager 인증서 세부 정보 보기

1. Privacy Manager 를 열고 **Certificate Manager**(인증서 관리자)를 누릅니다.
2. **Privacy Manager Certificate**(개인 정보 관리자 인증서)를 누릅니다.
3. **Certificate details**(인증서 세부 정보)를 누릅니다.
4. 세부 정보 보기를 마쳤으면 **OK**(확인)를 누릅니다.

Privacy Manager 인증서 갱신

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

1. Privacy Manager 를 열고 **Certificate Manager**(인증서 관리자)를 누릅니다.
2. **Privacy Manager Certificate**(개인 정보 관리자 인증서)를 누릅니다.
3. **Renew certificate**(인증서 갱신)을 누릅니다.
4. 화면에 표시되는 지침에 따라 새 Privacy Manager 인증서를 구입합니다.

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

기본 Privacy Manager 인증서 설정

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

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

1. Privacy Manager 를 열고 **Certificate Manager**(인증서 관리자)를 누릅니다.
2. 기본 인증서로 사용하려는 Privacy Manager 인증서를 누른 다음 **Set default**(기본값으로 설정)를 누릅니다.
3. **OK**(확인)를 누릅니다.

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

Privacy Manager 인증서 삭제

Privacy Manager 인증서를 삭제하면 파일을 열 수 없으며 인증서로 암호화된 데이터도 볼 수 없습니다. 실수로 Privacy Manager 인증서를 삭제한 경우 인증서를 설치할 때 만들었던 백업 파일을 사용하여 인증서를 복원할 수 있습니다.

Privacy Manager 를 삭제하려면 다음과 같이 하십시오.

1. Privacy Manager 를 열고 **Certificate Manager**(인증서 관리자)를 누릅니다.
2. 삭제하려는 Privacy Manager 인증서를 누른 다음 **Advanced**(고급)를 누릅니다.
3. **Delete**(삭제)를 누릅니다.
4. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.
5. **Close**(닫기)를 누른 다음 **Apply**(적용)를 누릅니다.

Privacy Manager 인증서 복원

실수로 Privacy Manager 인증서를 삭제한 경우 인증서를 설치하거나 내보냈을 때 만들었던 백업 파일을 사용하여 인증서를 복원할 수 있습니다. 복원을 수행하려면 다음과 같이 하십시오.

1. Privacy Manager 를 열고 **Migration**(마이그레이션)을 누릅니다.
2. **Import migration file**(마이그레이션 파일 가져오기)을 누릅니다.
3. "Migration File(마이그레이션 파일)" 페이지에서 **Browse**(찾아보기)를 눌러 Privacy Manager 인증서를 설치하거나 내보낼 때 만들었던 .dppsm 파일을 검색한 후 **Next**(다음)를 누릅니다.
4. "Migration File Import(마이그레이션 파일 가져오기)" 페이지에서 **Finish**(마침)를 누릅니다.
5. **Close**(닫기)를 누른 다음 **Apply**(적용)를 누릅니다.

주: 자세한 내용은 Privacy Manager 인증서 설치 또는 내보내기 및 Trusted Contacts(신뢰할 수 있는 연락처)를 참조하십시오.

Privacy Manager 인증서 해지

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

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

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

신뢰할 수 있는 연락처 관리

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

신뢰할 수 있는 연락처 추가

1. 사용자가 신뢰할 수 있는 연락처 수신자에게 전자 우편 초대 요청을 보냅니다.
2. 신뢰할 수 있는 연락처 수신자가 전자 우편 요청에 응답합니다.
3. 신뢰할 수 있는 연락처 수신자로부터 전자 우편 응답을 받고 Accept(수락)를 누릅니다.

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

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

신뢰할 수 있는 연락처 추가

1. Privacy Manager 를 열고 **Trusted Contacts Manager**(신뢰할 수 있는 연락처 관리자)를 누른 다음 **Invite Contacts**(연락처 초대)를 누릅니다.

   또는

   Microsoft Outlook 의 도구 모음에서 **Send Securely**(안전하게 보내기) 옆의 아래쪽 화살표를 누른 다음 **Invite Contacts**(연락처 초대)를 누릅니다.
2. Select Certificate(인증서 선택) 대화 상자가 열리면 사용하려는 Privacy Manager 인증서를 누른 다음 **OK**(확인)를 누릅니다.
3. Trusted Contact Invitation(신뢰할 수 있는 연락처 초대) 대화 상자가 열리면 대화 상자의 내용을 읽은 다음 **OK**(확인)를 누릅니다.

   전자 우편이 자동으로 생성됩니다.
4. 신뢰할 수 있는 연락처로 추가할 수신자의 전자 우편 주소를 하나 이상 입력합니다.
5. 텍스트를 수정하고 서명합니다(선택 사항).
6. **Send**(보내기)를 누릅니다.

   주: Privacy Manager 인증서를 받지 않은 경우 신뢰할 수 있는 연락처 요청을 보내려면 Privacy Manager 인증서가 있어야 한다는 메시지를 받게 됩니다. OK(확인)를 눌러 Certificate Request Wizard(인증서 요청 마법사)를 시작합니다.
7. 선택한 보안 로그온 방법을 사용하여 인증합니다.
8. 수신자로부터 신뢰할 수 있는 연락처 초대 요청을 수락하는 전자 우편을 받으면 전자 우편의 오른쪽 아래 모퉁이에 있는 Accept(수락)를 누릅니다.

   수신자가 신뢰할 수 있는 연락처 목록에 추가되었음을 확인할 수 있는 대화 상자가 열립니다.
9. **OK**(확인)를 누릅니다.

Microsoft Outlook 주소록을 사용하여 신뢰할 수 있는 연락처 추가

1. Privacy Manager 를 열어 **Trusted Contacts Manager**(신뢰할 수 있는 연락처 관리자), **Invite Contacts**(연락처 초대)를 차례로 누릅니다.

   또는

   Microsoft Outlook 의 도구 모음에서 **Send Securely**(안전하게 보내기) 옆의 아래쪽 화살표를 누른 다음 **Invite All My Outlook Contacts**(Outlook 의 모든 연락처 초대)을 누릅니다.

2. "Trusted Contact Invitation(신뢰할 수 있는 연락처 초대)" 페이지가 열리면 신뢰할 수 있는 연락처로 추가하려는 수신자의 전자 우편 주소를 선택하고 **Next**(다음)를 누릅니다.

3. "Sending Invitation(초대 요청 보내기)" 페이지가 열리면 **Finish**(마침)를 누릅니다.

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

4. 텍스트를 수정하고 서명합니다(선택 사항).

5. **Send**(보내기)를 누릅니다.

주: Privacy Manager 인증서를 받지 않은 경우 신뢰할 수 있는 연락처 요청을 보내려면 Privacy Manager 인증서가 있어야 한다는 메시지를 받게 됩니다. **OK**(확인)를 눌러 인증서 요청 마법사를 시작합니다.

6. 선택한 보안 로그온 방법을 사용하여 인증합니다.

주: 신뢰할 수 있는 연락처 수신자가 전자 우편을 받으면 전자 우편을 열고 오른쪽 아래 모퉁이에 있는 Accept(수락)를 누른 다음 확인 대화 상자가 열리면 OK(확인)를 누릅니다.

7. 수신자로부터 신뢰할 수 있는 연락처 초대 요청을 수락하는 전자 우편을 받으면 전자 우편의 오른쪽 아래 모퉁이에 있는 Accept(수락)를 누릅니다.

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

8. **OK**(확인)를 누릅니다.

신뢰할 수 있는 연락처 세부 정보 보기

1. Privacy Manager 를 열고 **Trusted Contacts Manager**(신뢰할 수 있는 연락처 관리자)를 누릅니다.

2. 신뢰할 수 있는 연락처를 누릅니다.

3. **Contact details**(연락처 세부 정보)를 누릅니다.

4. 세부 정보 보기를 마쳤으면 **OK**(확인)를 누릅니다.

신뢰할 수 있는 연락처 삭제

1. Privacy Manager 를 열고 **Trusted Contacts Manager**(신뢰할 수 있는 연락처 관리자)를 누릅니다.

2. 삭제하려는 신뢰할 수 있는 연락처를 누릅니다.

3. **Delete contact**(연락처 삭제)를 누릅니다.

4. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.

신뢰할 수 있는 연락처의 해지 상태 확인

1. Privacy Manager 를 열고 **Trusted Contacts Manager**(신뢰할 수 있는 연락처 관리자)를 누릅니다.
2. 신뢰할 수 있는 연락처를 누릅니다.
3. **Advanced**(고급) 버튼을 누릅니다.

   Advanced Trusted Contact Management(신뢰할 수 있는 연락처 고급 관리) 대화 상자가 열립니다.
4. **Check Revocation**(해지 확인)을 누릅니다.
5. **Close**(닫기)를 누릅니다.

일반 작업

Microsoft Office 에서 Privacy Manager 사용

Privacy Manager 인증서를 설치하면 모든 Microsoft Word, Microsoft Excel 및 Microsoft PowerPoint 문서의 도구 모음 오른쪽에 Sign and Encrypt(서명 및 암호화) 버튼이 표시됩니다.

Microsoft Office 문서에서 Privacy Manager 구성

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

또는

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

   또는

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

Microsoft Office 문서 서명

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

나중에 문서를 편집하려면 다음과 같이 하십시오.

1. 화면 왼쪽 상단에 있는 **Office** 버튼을 누릅니다.
2. **Prepare**(준비)를 누른 다음 **Mark as Final**(최종본으로 표시)을 누릅니다.

3. 확인 대화 상자가 표시되면 **Yes**(예)를 누르고 작업을 계속합니다.

4. 편집을 마치면 문서에 다시 서명합니다.

Microsoft Word 또는 Microsoft Excel 문서 서명 시 서명 줄 추가

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

1. Microsoft Word 또는 Microsoft Excel 에서 문서를 만들고 저장합니다.

2. **Home**(홈) 메뉴를 누릅니다.

3. **Sign and Encrypt**(서명 및 암호화) 옆의 아래쪽 화살표를 누른 다음 **Add Signature Line Before Signing**(서명하기 전에 서명 줄 추가)을 누릅니다.

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

4. **Sign and Encrypt**(서명 및 암호화) 옆의 아래쪽 화살표를 누른 다음 **Sign Document**(문서에 서명하기)를 누릅니다.

5. 선택한 보안 로그온 방법을 사용하여 인증합니다.

Microsoft Word 또는 Microsoft Excel 문서에 추천 서명자 추가

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

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

1. Microsoft Word 또는 Microsoft Excel 에서 문서를 만들고 저장합니다.

2. **Insert**(삽입) 메뉴를 누릅니다.

3. 도구 모음의 **Text**(텍스트) 그룹에서 **Signature Line**(서명 줄) 옆의 화살표를 누른 다음 **Privacy Manager Signature Provider**(Privacy Manager 서명 공급자)를 누릅니다.

   Signature Setup(서명 설정) 대화 상자가 열립니다.

4. **Suggested signer**(추천 서명자) 아래에 있는 상자에 추천 서명자 이름을 입력합니다.

5. **Instructions to the signer**(서명자에게 지시) 아래에 있는 상자에 추천 서명자에게 지시할 메시지를 입력합니다.

주: 이 메시지는 제목 위치에 표시되고 문서가 서명되면 메시지가 삭제되거나 사용자의 제목으로 바뀝니다.

6. **Show sign date in signature line**(서명 줄에 서명 날짜 표시) 확인란을 선택하여 날짜를 표시합니다.

7. **Show signer's title in signature line**(서명 줄에 서명자의 제목 표시) 확인란을 선택하여 제목을 표시합니다.

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

8. **OK**(확인)를 누릅니다.

Adding a suggested signer's signature line(추천 서명자의 서명 줄 추가)

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

문서에 서명하려면 다음과 같이 하십시오.

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

   문서의 소유자가 지정한 설정에 따라 서명 줄이 표시됩니다.

Microsoft Office 문서 암호화

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

Microsoft Office 문서를 암호화하려면 다음과 같이 하십시오.

1. Microsoft Word, Microsoft Excel 또는 Microsoft PowerPoint 에서 문서를 만들고 저장합니다.
2. **Home**(홈) 메뉴를 누릅니다.
3. **Sign and Encrypt**(서명 및 암호화) 옆의 아래쪽 화살표를 누른 다음 **Encrypt Document**(문서 암호화)를 누릅니다.

   Select Trusted Contacts(신뢰할 수 있는 연락처 선택) 대화 상자가 열립니다.
4. 문서를 열고 내용을 볼 수 있도록 하려는 신뢰할 수 있는 연락처의 이름을 누릅니다.

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

5. **OK**(확인)를 누릅니다.
6. 선택한 보안 로그온 방법을 사용하여 인증합니다.

문서를 나중에 편집하려면 **Signing a Microsoft Office Document** (Microsoft Office 문서 서명)의 절차를 따르십시오. 암호화를 제거하면 문서를 편집할 수 있습니다. 문서를 다시 암호화하려면 이 섹션의 절차를 따르십시오.

Microsoft Office 문서에서 암호화 제거

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

Microsoft Office 문서에서 암호화를 제거하려면 다음과 같이 하십시오.

1. 암호화된 Microsoft Word, Microsoft Excel 또는 Microsoft PowerPoint 문서를 엽니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.

3. **Home**(홈) 메뉴를 누릅니다.

4. **Sign and Encrypt**(서명 및 암호화) 옆의 아래쪽 화살표를 누른 다음 **Remove Encryption**(암호화 제거)을 누릅니다.

암호화된 Microsoft Office 문서 보내기

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

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

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

1. Microsoft Outlook 에서 **새로 만들기** 또는 **회신**을 누릅니다.

2. 전자 우편 메시지를 입력합니다.

3. Microsoft Office 문서를 첨부합니다.

4. 자세한 지침은 전자 우편 메시지 봉인 및 보내기를 참조하십시오.

서명이 있는 Microsoft Office 문서 보기

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

서명이 있는 Microsoft Office 문서를 열면 문서 옆에 Signatures(서명) 대화 상자가 열리고 문서에 서명한 사용자의 이름과 서명한 날짜가 표시됩니다. 마우스 오른쪽 버튼으로 이름을 눌러 세부 정보를 볼 수 있습니다.

암호화된 Microsoft Office 문서 보기

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

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

Microsoft Outlook 에서 Privacy Manager 사용

Privacy Manager 를 설치하면 Microsoft Outlook 의 도구 모음에 Privacy(개인 정보) 버튼이 표시되고 각 Microsoft Outlook 전자 우편 메시지의 도구 모음에 Send Securely(안전하게 보내기) 버튼이 표시됩니다.

Microsoft Outlook 용 Privacy Manager 구성

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

   또는

   Microsoft Outlook 도구 모음에서 **Privacy**(개인 정보) 옆의 아래쪽 화살표를 누른 다음 **Settings**(설정)를 누릅니다.

   또는

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

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

전자 우편 메시지에 서명하고 보내기

- Microsoft Outlook 에서 **새로 만들기** 또는 **회신**을 누릅니다.
- 전자 우편 메시지를 입력합니다.
- **Send Securely**(안전하게 보내기) 옆의 아래쪽 화살표를 누른 다음 **Sign and Send**(서명하고 보내기)를 누릅니다.
- 선택한 보안 로그온 방법을 사용하여 인증합니다.

전자 우편 메시지 봉인하고 보내기

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

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

1. Microsoft Outlook 에서 **새로 만들기** 또는 **회신**을 누릅니다.
2. 전자 우편 메시지를 입력합니다.
3. **Send Securely**(안전하게 보내기) 옆의 아래쪽 화살표를 누른 다음 **Seal for Trusted Contacts and Send**(신뢰할 수 있는 연락처에 대해 봉인하고 보내기)를 누릅니다.
4. 선택한 보안 로그온 방법을 사용하여 인증합니다.

봉인된 전자 우편 메시지 보기

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

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

Windows Live Messenger 에서 Privacy Manager 사용

Privacy Manager Chat 작업 추가

Windows Live Messenger 에 Privacy Manager Chat 기능을 추가하려면 다음과 같이 하십시오.

1. Windows Live Home 에 로그인합니다.
2. **Windows Live** 아이콘을 누른 다음 **Windows Live 서비스**를 누릅니다.
3. **갤러리**를 누른 다음 **메신저**를 누릅니다.
4. **플러그인**을 누른 다음 **안전 및 보안**을 누릅니다.
5. **Privacy Manager Chat** 을 누른 다음 화면의 지침을 따릅니다.

Privacy Manager Chat 시작

주: Privacy Manager Chat 을 사용하려면 양쪽 사용자의 컴퓨터에 Privacy Manager 와 Privacy Manager 인증서가 설치되어 있어야 합니다. Privacy Manager 인증서 설치에 관한 자세한 내용은 5 페이지 Privacy Manager 인증서 요청 및 설치를 참조하십시오.

1. Windows Live Messenger 에서 Privacy Manager Chat 을 시작하려면 다음 두 가지 절차 중 하나를 수행하십시오.

   a. 마우스 오른쪽 버튼으로 Live Messenger 의 온라인 대화 상대를 누른 다음 **플러그인 시작**을 선택합니다.

   b. **Start Privacy Manager Chat**(Privacy Manager Chat 시작)을 누릅니다.

   또는

   a. Live Messenger 의 온라인 대화 상대를 두 번 누른 다음 **Conversation**(대화하기) 메뉴를 누릅니다.

   b. **Action**(플러그인)을 누른 다음 **Start Privacy Manager Chat**(Privacy Manager Chat 시작)을 누릅니다

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

2. **Start**(시작)를 눌러 보안 채팅을 시작합니다.

Windows Live Messenger 용 Privacy Manager Chat 구성

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

   또는

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

   또는

   Privacy Manager History Viewer(Privacy Manager 대화 기록 뷰어)에서 **Settings**(설정) 버튼을 누릅니다.

2. Privacy Manager Chat 사용 후 세션이 잠길 때까지 걸리는 대기 시간을 지정하려면 Lock session **after _ minutes of inactivity**(_분간 사용하지 않으면 세션 잠금) 상자에서 숫자를 선택합니다.
3. 대화 세션의 대화 기록 폴더를 지정하려면 **Browse**(찾아보기)를 눌러 폴더를 찾은 후 **OK**(확인)를 누릅니다.

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

5. **OK**(확인)를 누릅니다.

Privacy Manager Chat 창에서 채팅하기

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

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

대화 기록 보기

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

Chat History Viewer(대화 기록 뷰어) 시작

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.

2. **Privacy Manager: Sign and Chat**(Privacy Manager: 서명 및 채팅)을 누른 다음 **Chat History Viewer**(대화 기록 뷰어)를 누릅니다.

   또는

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

   또는

   ▲ "Chat Configuration(Chat 구성)" 페이지에서 **Start Live Messenger History Viewer**(Live Messenger 대화 기록 뷰어 시작)를 누릅니다.

모든 세션 표시

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

1. Chat History Viewer(대화 기록 뷰어)에서 마우스 오른쪽 버튼으로 세션을 누른 다음 **Reveal All Sessions**(모든 세션 표시)를 선택합니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.

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

특정 계정의 세션 표시

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

1. Chat History Viewer(대화 기록 뷰어)에서 마우스 오른쪽 버튼으로 세션을 누른 다음 **Reveal Session**(세션 표시)를 선택합니다.
2. 선택한 보안 로그온 방법을 사용하여 인증합니다.

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

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

세션 ID 보기

- Chat History View(대화 기록 보기)에서 마우스 오른쪽 버튼으로 표시된 세션을 누르고 **View Session ID**(세션 ID 보기)를 선택합니다.

세션 보기

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

1. Chat History Viewer(대화 기록 뷰어)에서 마우스 오른쪽 버튼으로 세션을 누른 다음 **View**(보기)를 선택합니다.
2. 메시지가 표시되면 선택한 보안 로그온 방법을 사용하여 인증합니다.

   세션 내용이 해독됩니다.

특정 텍스트에 대한 세션 검색

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

1. Chat History Viewer(대화 기록 뷰어)에서 **Search**(검색) 버튼을 누릅니다.
2. 검색 텍스트를 입력하고 원하는 검색 매개 변수를 구성한 다음 **OK**(확인)를 누릅니다.

   뷰어 창에 해당 텍스트를 포함하는 세션이 강조 표시됩니다.

세션 삭제

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

열 추가 또는 제거

기본적으로 Chat History Viewer(대화 기록 뷰어)에 가장 자주 사용되는 세 개의 열이 표시됩니다. 디스플레이에 추가 열을 추가하거나 디스플레이에서 열을 제거할 수 있습니다.

디스플레이에 열을 추가하려면 다음과 같이 하십시오.

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

디스플레이에서 열을 제거하려면 다음과 같이 하십시오.

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

표시된 세션 필터링

Chat History Viewer(대화 기록 뷰어)에 모든 계정에 대한 세션 목록이 표시됩니다.

특정 계정에 대한 세션 표시

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

날짜 범위를 기준으로 세션 표시

1. Chat History View(대화 기록 뷰어)에서 **Advanced Filter**(고급 필터) 아이콘을 누릅니다.

   Advanced Filter(고급 필터) 대화 상자가 열립니다.
2. **Display only sessions within specified date range**(특정 날짜 범위 내의 세션만 표시)의 확인란을 선택합니다.
3. **From date**(시작 날짜) 및 **To date**(종료 날짜) 상자에 연도, 월, 일을 입력하거나 달력 옆의 화살표를 눌러 날짜를 선택합니다.
4. **OK**(확인)를 누릅니다.

기본 폴더가 아닌 다른 폴더에 저장된 세션 표시

1. Chat History View(대화 기록 뷰어)에서 **Advanced Filter**(고급 필터) 아이콘을 누릅니다.
2. **Use an alternate history files folder**(다른 기록 파일 폴더 사용)의 확인란을 선택합니다.
3. 폴더 위치를 입력하거나 **Browse**(찾아보기)를 눌러 폴더를 찾습니다.
4. **OK**(확인)를 누릅니다.

고급 작업

다른 컴퓨터로 Privacy Manager 인증서 및 신뢰할 수 있는 연락처 마이그레이션

Privacy Manager 인증서 및 신뢰할 수 있는 연락처를 다른 컴퓨터로 안전하게 마이그레이션할 수 있습니다. 암호로 저장된 파일 형태로 네트워크 위치나 이동식 저장 장치로 내보낸 다음 해당 파일을 새 컴퓨터로 가져오면 됩니다.

Privacy Manager 인증서 및 신뢰할 수 있는 연락처 내보내기

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

1. Privacy Manager 를 열고 **Migration**(마이그레이션)을 누릅니다.
2. **Export migration file**(마이그레이션 파일 내보내기)을 누릅니다.
3. "Select Data(데이터 선택)" 페이지에서 마이그레이션 파일에 포함할 데이터 범주를 선택한 후 **Next**(다음)를 누릅니다.
4. "Migration File(마이그레이션 파일)" 페이지에서 파일 이름을 입력하거나 **Browse**(찾아보기)를 눌러 위치를 찾은 후 **Next**(다음)를 누릅니다.
5. 암호를 입력하고 확인한 후 **Next**(다음)를 누릅니다.

주: 암호를 안전한 곳에 보관하십시오. 마이그레이션 파일을 가져올 때 이 암호가 필요합니다.

6. 선택한 보안 로그온 방법을 사용하여 인증합니다.
7. "Migration File Saved(마이그레이션 파일 저장 완료)" 페이지에서 **Finish**(마침)를 누릅니다.

Privacy Manager 인증서 및 신뢰할 수 있는 연락처 가져오기

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

1. Privacy Manager 를 열고 **Migration**(마이그레이션)을 누릅니다.
2. **Import migration file**(마이그레이션 파일 가져오기)을 누릅니다.
3. "Select Data(데이터 선택)" 페이지에서 마이그레이션 파일에 포함할 데이터 범주를 선택한 후 **Next**(다음)를 누릅니다.
4. "Migration File(마이그레이션 파일)" 페이지에서 파일 이름을 입력하거나 **Browse**(찾아보기)를 눌러 위치를 찾은 후 **Next**(다음)를 누릅니다.
5. "Migration File Import(마이그레이션 파일 가져오기)" 페이지에서 **Finish**(마침)를 누릅니다.

6 HP ProtectTools File Sanitizer

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

주: File Sanitizer 는 현재 하드 드라이브에서만 작동됩니다.

파쇄 정보

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

자산을 파쇄할 때 데이터를 손상시키는 알고리즘이 호출되므로 원래 자산을 가상으로 검색하지 못하게 한다는 점에서 파쇄는 일반적인 Windows® 삭제(File Sanitizer 에서는 기본 삭제라고도 함)와 다릅니다.

파쇄 프로필(High Security(높은 보안), Medium Security(중간 보안) 또는 Low Security(낮은 보안))을 선택하면 파쇄를 위해 미리 정의된 자산 목록 및 삭제 방법이 자동으로 선택됩니다. 또한 파쇄 프로필을 사용자 정의하여 파쇄 주기, 파쇄할 자산, 파쇄하기 전에 확인할 자산, 파쇄하지 않을 자산을 각각 지정할 수 있습니다.

자동 파쇄 예약을 설정할 수 있으며 수동으로 언제든지 자산을 파쇄할 수도 있습니다.

여유 공간 블리치 정보

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

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

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

설치 절차

File Sanitizer 열기

File Sanitizer 를 열려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. **File Sanitizer** 를 누릅니다.

   또는

- **File Sanitizer** 을 두 번 누릅니다.

  또는

- 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 HP ProtectTools 아이콘을 마우스 오른쪽 버튼으로 누른 다음 File Sanitizer, Open File Sanitizer(File Sanitizer 열기)를 차례로 누릅니다.

여유 공간 블리치 예약 설정

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

여유 공간 블리치 예약을 설정하려면 다음과 같이 하십시오.

1. File Sanitizer 를 열고 **Free Space Bleaching**(여유 공간 블리치)을 누릅니다.
2. **Activate Scheduler**(스케줄러 활성화) 확인란을 선택하고 Windows 암호를 입력한 다음 하드 드라이브를 블리치할 날짜와 시간을 입력합니다.
3. **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

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

파쇄 프로필 선택 또는 생성

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

미리 정의된 파쇄 프로필 선택

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

미리 정의된 파쇄 프로필을 선택하려면 다음과 같이 하십시오.

1. **File Sanitizer** 를 열고 **Settings** 을 누릅니다.
2. 미리 정의된 파쇄 프로필을 누릅니다.
3. **View Details**(세부 정보 보기)를 누르면 파쇄하도록 선택된 자산 목록을 볼 수 있습니다.

4. **Shred the following**(다음 자산을 파쇄)에서 파쇄하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.

5. **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

파쇄 프로필 사용자 정의

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

1. File Sanitizer 를 열고 **Settings**(설정), **Advanced Security Settings**(고급 보안 설정), **View Details**(세부 정보 보기)를 차례로 누릅니다.

2. 파쇄 주기를 지정합니다.

주: 선택한 파쇄 주기만큼 각 자산이 파쇄됩니다. 예를 들어 파쇄 주기를 세 번으로 선택한 경우 데이터를 손상시키는 알고리즘이 각각 세 번 실행됩니다. 높은 보안 파쇄 주기를 선택한 경우 파쇄 작업에 상당히 오랜 시간이 걸릴 수 있지만 파쇄 주기를 늘릴수록 컴퓨터의 보안이 강화됩니다.

3. 다음 방법을 통해 파쇄하려는 자산을 선택합니다.

   a. **Available shred options**(사용 가능한 파쇄 옵션)에서 자산을 선택한 다음 **Add**(추가)를 누릅니다.

   b. 사용자 정의 자산을 추가하려면 Add Custom Option(사용자 정의 추가 옵션)을 누르고 파일 이름이나 폴더 이름을 입력한 다음 **OK**(확인)를 누릅니다. 추가하려는 사용자 정의 자산을 누른 다음 **Add**(추가)를 누릅니다.

   주: 사용 가능한 파쇄 옵션에서 자산을 삭제하려면 삭제하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.

4. **Shred the following**(다음 자산을 파쇄)에서 파쇄하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.

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

5. **Do not shred the following**(다음 자산을 파쇄하지 않음)에서 **Add**(추가)를 눌러 파쇄하지 않으려는 특정 자산을 선택합니다.

주: 특정 자산에 대한 파쇄 방지는 파일 확장자에 대해서만 수행됩니다. 예를 들어 .BMP 파일 확장자를 추가한 경우 .BMP 확장자를 가진 모든 파일은 파쇄되지 않습니다.

차단 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.

6. 파쇄 프로필 구성을 완료하면 **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

기본 삭제 프로필 사용자 정의

기본 삭제 프로필에서는 자산을 파쇄하지 않는 일반적인 자산 삭제를 수행합니다. 기본 삭제 프로필을 사용자 정의할 때 기본 삭제할 자산, 기본 삭제를 실행하기 전에 확인할 자산, 기본 삭제하지 않을 자산을 각각 지정할 수 있습니다.

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

1. **File Sanitizer** 를 열고 **Settings**(설정), **Simple Delete Setting**(기본 삭제 설정), **View Details**(세부 정보 보기)를 차례로 누릅니다.
2. 다음 방법을 통해 삭제하려는 자산을 선택합니다.
   a. **Available delete options**(사용 가능한 삭제 옵션)에서 삭제하려는 자산을 누른 다음 **Add**(추가)를 누릅니다.
   b. 사용자 정의 자산을 추가하려면 **Add Custom Option**(사용자 정의 추가 옵션)을 누르고 파일 이름이나 폴더 이름을 입력한 다음 **OK**(확인)를 누릅니다. 추가하려는 사용자 정의 자산을 누른 다음 **Add**(추가)를 누릅니다.

   주: 사용 가능한 삭제 옵션에서 자산을 삭제하려면 삭제하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.
3. **Delete the following**(다음 자산을 삭제)에서 삭제하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.

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

4. **Do not shred the following**(다음 자산을 파쇄하지 않음)에서 **Add**(추가)를 눌러 파쇄하지 않으려는 특정 자산을 선택합니다.

주: 특정 자산에 대한 삭제 방지는 파일 확장자에 대해서만 수행됩니다. 예를 들어 .BMP 파일 확장자를 추가한 경우 .BMP 확장자를 가진 모든 파일은 삭제되지 않습니다.

차단 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.

5. 기본 삭제 프로필 구성을 완료하면 **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

파쇄 예약 설정

1. File Sanitizer 를 열고 **Shred**(파쇄)를 누릅니다.
2. 파쇄 옵션을 선택합니다.
   - **Windows startup**(Windows 시작)— Windows 가 시작될 때 선택한 모든 자산을 파쇄하려면 이 옵션을 선택합니다.
   - **Windows shutdown**(Windows 종료)— Windows 가 종료될 때 선택한 모든 자산을 파쇄하려면 이 옵션을 선택합니다.

     주: 이 옵션을 선택하면 Windows 가 종료될 때 선택한 자산을 계속 파쇄할 것인지 아니면 해당 프로세스를 건너뛸 것인지를 묻는 대화 상자가 표시됩니다. 파쇄 프로세스를 건너뛰려면 Yes(예)를 누르고 파쇄를 계속하려면 No(아니오)를 누릅니다.
   - **Web browser quit**(웹 브라우저 종료) — 웹 브라우저를 닫을 때 브라우저 URL 히스토리와 같은 선택한 모든 웹 관련 자산을 파쇄하려면 이 옵션을 선택합니다.

- **Web browser quit**(웹 브라우저 종료) — 웹 브라우저를 닫을 때 브라우저 URL 히스토리와 같은 선택한 모든 웹 관련 자산을 파쇄하려면 이 옵션을 선택합니다.
- **Scheduler**(스케줄러) — Activate Scheduler(스케줄러 활성화) 확인란을 선택하고 Windows 암호를 입력한 다음 선택한 자산을 파쇄할 날짜와 시간을 입력합니다.

3. **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

여유 공간 블리치 예약 설정

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

여유 공간 블리치 예약을 설정하려면 다음과 같이 하십시오.

1. File Sanitizer 를 열고 **Free Space Bleaching**(여유 공간 블리치)을 누릅니다.
2. **Activate Scheduler**(스케줄러 활성화) 확인란을 선택하고 Windows 암호를 입력한 다음 하드 드라이브를 블리치할 날짜와 시간을 입력합니다.
3. **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

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

파쇄 프로필 선택 또는 생성

미리 정의된 파쇄 프로필 선택

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

미리 정의된 파쇄 프로필을 선택하려면 다음과 같이 하십시오.

1. **File Sanitizer** 를 열고 **Settings** 을 누릅니다.
2. 미리 정의된 파쇄 프로필을 누릅니다.
3. **View Details**(세부 정보 보기)를 누르면 파쇄하도록 선택된 자산 목록을 볼 수 있습니다.
4. **Shred the following**(다음 자산을 파쇄)에서 파쇄하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.
5. **Cancel**(취소)을 누른 다음 **OK**(확인)를 누릅니다.

파쇄 프로필 사용자 정의

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

1. File Sanitizer 를 열고 **Settings**(설정), **Advanced Security Settings**(고급 보안 설정), **View Details**(세부 정보 보기)를 차례로 누릅니다.
2. 파쇄 주기를 지정합니다.

주: 선택한 파쇄 주기만큼 각 자산이 파쇄됩니다. 예를 들어 파쇄 주기를 세 번으로 선택한 경우 데이터를 손상시키는 알고리즘이 각각 세 번 실행됩니다. 높은 보안 파쇄 주기를 선택한 경우 파쇄 작업에 상당히 오랜 시간이 걸릴 수 있지만 파쇄 주기를 늘릴수록 컴퓨터의 보안이 강화됩니다.

3. 다음 방법을 통해 파쇄하려는 자산을 선택합니다.
   a. **Available shred options**(사용 가능한 파쇄 옵션)에서 자산을 선택한 다음 **Add**(추가)를 누릅니다.
   b. 사용자 정의 자산을 추가하려면 Add Custom Option(사용자 정의 추가 옵션)을 누르고 파일 이름이나 폴더 이름을 입력한 다음 **OK**(확인)를 누릅니다. 추가하려는 사용자 정의 자산을 누른 다음 **Add**(추가)를 누릅니다.

주: 사용 가능한 파쇄 옵션에서 자산을 삭제하려면 삭제하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.

4. **Shred the following**(다음 자산을 파쇄)에서 파쇄하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.

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

5. **Do not shred the following**(다음 자산을 파쇄하지 않음)에서 **Add**(추가)를 눌러 파쇄하지 않으려는 특정 자산을 선택합니다.

주: 특정 자산에 대한 파쇄 방지는 파일 확장자에 대해서만 수행됩니다. 예를 들어 .BMP 파일 확장자를 추가한 경우 .BMP 확장자를 가진 모든 파일은 파쇄되지 않습니다.

차단 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.

6. 파쇄 프로필 구성을 완료하면 **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

기본 삭제 프로필 사용자 정의

기본 삭제 프로필에서는 자산을 파쇄하지 않는 일반적인 자산 삭제를 수행합니다. 기본 삭제 프로필을 사용자 정의할 때 기본 삭제할 자산, 기본 삭제를 실행하기 전에 확인할 자산, 기본 삭제하지 않을 자산을 각각 지정할 수 있습니다.

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

1. **File Sanitizer** 를 열고 **Settings**(설정), **Simple Delete Setting**(기본 삭제 설정), **View Details**(세부 정보 보기)를 차례로 누릅니다.
2. 다음 방법을 통해 삭제하려는 자산을 선택합니다.
   - **Available delete options**(사용 가능한 삭제 옵션)에서 삭제하려는 자산을 누른 다음 **Add**(추가)를 누릅니다.
   - 사용자 정의 자산을 추가하려면 **Add Custom Option**(사용자 정의 추가 옵션)을 누르고 파일 이름이나 폴더 이름을 입력한 다음 **OK**(확인)를 누릅니다. 추가하려는 사용자 정의 자산을 누른 다음 **Add**(추가)를 누릅니다.

     주: 사용 가능한 삭제 옵션에서 자산을 삭제하려면 삭제하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.
3. **Delete the following**(다음 자산을 삭제)에서 삭제하기 전에 확인하려는 자산 옆에 있는 확인란을 선택합니다.

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

4. **Do not delete the following**(다음 자산을 삭제하지 않음)에서 **Add**(추가)를 눌러 삭제하지 않으려는 특정 자산을 선택합니다.

주: 특정 자산에 대한 삭제 방지는 파일 확장자에 대해서만 수행됩니다. 예를 들어 .BMP 파일 확장자를 추가한 경우 .BMP 확장자를 가진 모든 파일은 삭제되지 않습니다.

차단 목록에서 자산을 제거하려면 제거하려는 자산을 누른 다음 **Delete**(삭제)를 누릅니다.

5. 기본 삭제 프로필 구성을 완료하면 **Apply**(적용)를 누른 다음 **OK**(확인)를 누릅니다.

일반 작업

키 시퀀스를 사용하여 파쇄 시작

키 시퀀스를 지정하려면 다음과 같이 하십시오.

1. **File Sanitizer** 를 열고 **Shred**(파쇄)를 누릅니다.
2. **Key sequence**(키 시퀀스) 확인란을 선택합니다.
3. 사용 가능한 상자에 문자를 입력한 다음 **CTRL**, **ALT** 또는 **SHIFT** 상자를 누르거나 모두 선택합니다.

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

주: 키 시퀀스 선택은 키 시퀀스를 직접 구성하는 것과 다릅니다.

키 시퀀스를 사용하여 파쇄를 시작하려면 다음과 같이 하십시오.

1. Ctrl, Alt 또는 Shift 키(또는 자신이 지정한 키 조합)를 누른 상태에서 선택한 문자를 누릅니다.
2. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.

File Sanitizer 아이콘 사용

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

1. 파쇄하려는 문서 또는 폴더로 이동합니다.
2. 파쇄하려는 자산을 바탕 화면의 File Sanitizer 아이콘으로 끌어다 놓습니다.
3. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.
4. **Yes**(예)를 눌러 제거하려는 선택한 사용자를 확인합니다.

단일 자산 수동 파쇄

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

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

   주: 선택한 자산은 하나의 파일 또는 폴더일 수 있습니다.

3. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.

또는

1. 바탕 화면에서 **File Sanitizer** 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **Shred One**(단일 자산 파쇄)을 누릅니다.
2. Browse(찾아보기) 대화 상자가 열리면 파쇄하려는 자산으로 이동한 다음 **OK**(확인)를 누릅니다.
3. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.

또는

1. File Sanitizer 를 열고 **Shred**(파쇄)를 누릅니다.
2. **Browse**(찾아보기) 버튼을 누릅니다.
3. Browse(찾아보기) 대화 상자가 열리면 파쇄하려는 자산으로 이동한 다음 **OK**(확인)를 누릅니다.
4. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.

모든 항목 수동 파쇄

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

또는

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

여유 공간 블리치 수동 활성화

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

또는

1. File Sanitizer 를 열고 **Free Space Bleaching**(여유 공간 블리치)을 누릅니다.
2. **Bleach Now**(지금 블리치)를 누릅니다.
3. 확인 대화 상자가 표시되면 **Yes**(예)를 누릅니다.

파쇄 또는 여유 공간 블리치 작업 중단

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

작업을 중단하려면 다음과 같이 하십시오.

▲ 메시지를 누른 다음 **Stop**(중지)을 눌러 작업을 취소합니다.

로그 파일 보기

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

주: 파쇄되거나 블리치된 파일은 로그 파일에 기록되지 않습니다.

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

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

7 HP ProtectTools Java Card Security

Java Card Security for HP ProtectTools 모듈은 HP 스마트 카드 키보드와 함께 사용할 수 있도록 Java 카드의 설정 및 구성을 관리합니다. HP Java 카드는 ATM 카드에 PIN 번호를 사용하는 것처럼 액세스 권한 부여를 위한 카드 및 PIN 번호에 필요한 인증 데이터를 보호하는 개인 보안 장치입니다. 이러한 Java 카드는 인증서 관리자, 드라이브 암호화, HP BIOS 또는 타사 액세스의 모든 지점에 액세스하는 데 사용할 수 있습니다.

Java Card Security 모듈이 있으면 다음 작업이 가능합니다.

- Java Card Security 기능에 액세스
- Computer Setup 유틸리티와 연동하여 파워온 환경에서 Java Card 인증을 활성화
- 관리자용 및 사용자용 Java Card 를 별도로 구성 사용자가 Java Card 를 넣고 PIN 을 입력해야 운영체제가 로드됨
- Java Card 사용자 인증에 사용되는 PIN 설정 및 변경

일반 작업

"General(일반)" 페이지에서는 다음 작업을 수행할 수 있습니다.

- Java Card PIN 변경
- 카드 리더 또는 스마트 카드 키보드 선택

주: 카드 리더는 Java Card 와 스마트 카드를 모두 사용합니다. 이 기능은 컴퓨터에 여러 대의 카드 리더가 있는 경우에 사용할 수 있습니다.

Java Card PIN 변경

Java Card PIN 을 변경하려면 다음과 같이 하십시오.

주: Java Card PIN 은 4~8 자의 숫자여야 합니다.

1. Windows Vista 인 경우 **시작 > 모든 프로그램 > HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Java Card Security** 를 누른 다음 **General**(일반)을 누릅니다.
3. Java Card(기존 PIN 사용)를 카드 리더에 삽입합니다.
4. 오른쪽 창에서 **Change**(변경)를 누릅니다.
5. **Change PIN**(PIN 변경) 대화상자의 **Current PIN**(현재 PIN) 입력란에 현재 PIN 을 입력합니다.

6. **New PIN**(새 PIN) 입력란에 새 PIN 을 입력한 다음 **Confirm New PIN**(새 PIN 확인) 입력란에 PIN 을 다시 입력합니다.

7. **OK**(확인)를 누릅니다.

카드 리더 선택

Java Card 를 사용하기 전에 Java Card Security 모듈에서 올바른 카드 리더를 선택해야 합니다. 올바른 리더를 선택하지 않은 경우 일부 기능을 사용할 수 없거나 기능이 정확히 표시되지 않을 수 있습니다. 또한 Windows 장치 관리자에 표시된 것과 같이 카드 리더 드라이버를 바르게 설치해야 합니다.

카드 리더를 선택하려면 다음과 같이 하십시오.

1. Windows Vista 인 경우 **시작 > 모든 프로그램 > HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 선택합니다.

2. 왼쪽 창에서 **Java Card Security** 를 누른 다음 **General**(일반)을 누릅니다.

3. Java Card 를 카드 리더에 삽입합니다.

4. 오른쪽 창의 **Smart Card Reader**(스마트 카드 리더)에서 해당 리더를 누릅니다.

고급 작업(관리자 전용)

"Advanced(고급)" 페이지에서는 다음 작업을 수행할 수 있습니다.

- Java Card PIN 할당
- Java Card 이름 할당
- 파워온 인증 설정
- Java Card 백업 및 복원

주: Windows 관리자 권한이 있어야 "고급" 페이지가 표시됩니다.

Java Card PIN 할당

Java Card 의 이름과 PIN 을 지정해야 Java Card Security 모듈에서 사용할 수 있습니다.

Java Card PIN 을 할당하려면 다음과 같이 하십시오.

주: Java Card PIN 은 4~8 자의 숫자여야 합니다.

1. Windows Vista 인 경우 **시작 > 모든 프로그램 > HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 선택합니다.

2. 왼쪽 창에서 **Java Card Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.

3. 새 Java Card 를 카드 리더에 삽입합니다.

4. **New Card**(새 카드) 대화상자가 열리면 **New display name**(새 디스플레이 이름) 입력란에 새 이름을, **New PIN**(새 PIN) 입력란에 새 PIN 을 입력한 다음 **Confirm New PIN**(새 PIN 확인) 입력란에 새 PIN 을 한 번 더 입력합니다.

5. **OK**(확인)를 누릅니다.

Java Card 이름 할당

파워온 인증에 Java Card 를 사용하려면 먼저 Java Card 에 이름을 할당해야 합니다.

Java Card 에 이름을 할당하려면 다음과 같이 하십시오.

1. Windows Vista 인 경우 **시작 > 모든 프로그램 > HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Java Card Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.
3. Java Card 를 카드 리더에 삽입합니다.

> **주:** 이 카드에 PIN 을 할당하지 않은 경우 **New Card**(새 카드) 대화상자가 나타나고 여기에 새 이름과 PIN 을 입력할 수 있습니다.

4. 오른쪽 창의 **Display name**(디스플레이 이름)에서 **Change**(변경)를 누릅니다.
5. **Name**(이름) 입력란에 Java Card 의 이름을 입력합니다.
6. **PIN** 입력란에 현재 Java Card PIN 을 입력합니다.
7. **OK**(확인)를 누릅니다.

파워온 인증 설정

파워온 인증이 활성화되면 Java Card 를 통해 컴퓨터를 시작해야 합니다.

Java Card 파워온 인증을 활성화하는 과정은 다음 단계로 구성됩니다.

1. BIOS Configuration 또는 Computer Setup 에서 Java Card 파워온 인증 지원을 활성화합니다.
2. Java Card Security 에서 Java Card 파워온 인증을 활성화합니다.
3. 관리자 Java Card 를 만들어 활성화합니다.

Java Card 파워온 인증 활성화 및 관리자 Java Card 생성

Java Card 파워온 인증을 활성화하려면 다음과 같이 하십시오.

1. Windows Vista 인 경우 **시작 > 모든 프로그램 > HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Java Card Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.
3. Java Card 를 카드 리더에 삽입합니다.

주: 이 카드에 이름과 PIN 을 할당하지 않은 경우 **New Card**(새 카드) 대화상자가 나타나고 여기에 새 이름과 PIN 을 입력할 수 있습니다.

4. 오른쪽 창의 **Power-on authentication**(파워온 인증) 아래에서 **Enable**(활성화) 확인란을 선택합니다.
5. **Computer Setup Password**(Computer Setup 암호) 대화상자에 Computer Setup 암호를 입력하고 **OK**(확인)를 누릅니다.
6. DriveLock 을 활성화하지 않은 경우 Java Card PIN 을 입력한 다음 **OK**(확인)를 누릅니다.

   또는

   DriveLock 을 활성화한 경우에는 다음을 수행합니다.

   a. **Make Java card identity unique**(고유한 Java Card ID)를 누릅니다.

      또는

      Make the Java card identity the same as the DriveLock password(Java Card ID 를 DriveLock 암호와 동일하게 함)를 누릅니다.

      주: 컴퓨터에서 DriveLock 이 활성화된 경우, Java Card ID 를 DriveLock 사용자 암호와 동일하게 설정할 수 있습니다. 이렇게 하면 컴퓨터를 시작할 때 Java Card 만으로 DriveLock 과 Java Card 에 대해 동시에 유효성 검사를 할 수 있습니다.

   b. 해당하는 경우 **DriveLock password**(DriveLock 암호) 입력란에 DriveLock 사용자 암호를 입력한 다음 **Confirm password**(암호 확인) 입력란에 다시 입력합니다.

   c. Java Card PIN 을 입력합니다.

   d. **OK**(확인)를 누릅니다.

7. 복구 파일을 작성하라는 메시지가 나타납니다. 복구 파일을 나중에 작성하려면 **Cancel**(취소)을 누르고, 지금 작성하려면 **OK**(확인)를 누른 다음 HP ProtectTools Backup Wizard (HP ProtectTools 백업 마법사) 화면의 지침에 따르십시오.

주: 자세한 내용은 9페이지의 HP ProtectTools 인증 정보 백업 및 복원을 참조하십시오.

사용자 Java Card 생성

주: 사용자 Java Card 를 만들려면 파워온 인증과 관리자 카드를 설정해야 합니다.

사용자 Java Card 를 만들려면 다음과 같이 하십시오.

1. Windows Vista 인 경우 **시작 > 모든 프로그램 > HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Java Card Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.
3. 사용자 카드로 사용할 Java Card 를 삽입합니다.
4. 오른쪽 창의 **Power-on authentication**(파워온 인증)에서 **User card identity**(사용자 카드 ID) 옆의 **Create**(생성)를 누릅니다.
5. 사용자 Java Card 의 PIN 을 입력한 다음 **OK**(확인)를 누릅니다.

Java Card 파워온 인증 비활성화

Java Card 파워온 인증을 비활성화하면 컴퓨터 액세스에 Java Card 를 사용할 필요가 없게 됩니다.

1. Windows Vista 인 경우 **시작 > 모든 프로그램 > HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Java Card Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.
3. 관리자 Java Card 를 넣습니다.
4. 오른쪽 창의 **Power-on authentication**(파워온 인증)에서 **Enable**(활성화) 확인란의 선택을 취소합니다.
5. 사용자 Java Card 의 PIN 을 입력한 다음 **OK**(확인)를 누릅니다.

8 BIOS Configuration for HP ProtectTools

BIOS Configuration for HP ProtectTools 을 사용하면 사용자에게 Computer Setup 에서 관리하는 시스템 보안 기능에 대한 Windows 액세스 권한을 부여하는 Computer Setup 유틸리티 보안 및 구성 설정에 액세스할 수 있습니다. BIOS Configuration for HP ProtectTools 에 들어 있는 옵션은 다음과 같습니다.

- File(파일)
- Storage(저장 장치)
- 보안
- Power(전원)
- Advanced(고급)

주: 특정 Computer Setup 옵션에 대한 지원 여부는 하드웨어 구성에 따라 다를 수 있습니다.

BIOS Configuration 을 사용하면 시작 시 F10 키를 눌러 Computer Setup 을 실행해야만 액세스할 수 있는 다양한 컴퓨터 설정을 관리할 수 있습니다. BIOS Configuration 으로 다음과 같은 목표를 달성할 수 있습니다.

- 파워온 암호 및 관리자 암호 관리
- 내장 보안 인증 지원 활성화 등 기타 파워온 인증 기능 구성
- 하드웨어 기능 활성화/비활성화(이동식 미디어 부팅 또는 여러 하드웨어 포트 등)
- MultiBoot 활성화, 부팅 순서 변경과 같은 부팅 옵션 구성

주: BIOS Configuration for HP ProtectTools 의 모든 기능은 F10 Setup 에서도 사용 가능합니다. F10 Setup 사용에 관한 자세한 지침은 컴퓨터 또는 BIOS 업데이트에 포함된 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

일반 작업

BIOS Configuration 을 사용하면 다양한 컴퓨터 설정을 관리할 수 있습니다. 다른 방법으로 이러한 설정에 액세스하려면 시작 시 F10 키를 누르고 Computer Setup 에 들어가야 합니다.

Accessing BIOS Configuration(BIOS 구성 액세스)

BIOS Configuration 에 액세스하려면 다음과 같이 하십시오.

1. **시작**, **설정**, **제어판**을 차례로 누릅니다.
2. **HP ProtectTools Security Manager for Administrators** 를 누른 다음 **BIOS Configuration** (BIOS 구성)을 누릅니다.

   또한 작업 표시줄 오른쪽 끝에 있는 알림 영역에서 아이콘을 눌러 BIOS Configuration 에 액세스할 수 있습니다.

   주: HP ProtectTools Security Manager for Administrators 아이콘을 표시하려면 알림 영역의 **Show Hidden Icons**(숨겨진 아이콘 표시) 아이콘(**<** 또는 **<<**)을 누릅니다.

   - 알림 영역의 **HP ProtectTools Security Manager for Administrators** 아이콘을 마우스 오른쪽 버튼으로 누릅니다.
   - **BIOS Configuration** 을 누릅니다.
3. HP ProtectTools 사용자일 경우 Windows 암호를 입력합니다.
   - Windows 암호를 정확하게 입력했지만 BIOS 관리자가 아닌 경우에는 보안 수준 설정에 따라 변경 권한이 달라집니다.

     주: HP ProtectTools 사용자는 BIOS 관리자일 수도 있고 아닐 수도 있습니다.
   - Windows 암호를 잘못 입력한 경우 BIOS Configuration 설정에 대한 보기 권한만 주어집니다(변경 불가).
4. HP ProtectTools 사용자가 아닐 경우 BIOS Configuration 소프트웨어는 BIOS 관리자 암호가 설정되어 있는지 확인합니다.
   - BIOS 관리자 암호가 설정되어 있는 경우 암호를 입력해야 합니다.
     - BIOS 관리자 암호를 제대로 입력한 사용자에게는 BIOS Configuration 설정에 대한 보기 및 변경 권한이 모두 주어집니다.
     - BIOS 관리자 암호가 설정되어 있지만 암호를 입력할 수 없거나 잘못 입력한 경우 BIOS Configuration 설정에 대한 보기 권한만 주어집니다(변경 불가).
   - BIOS 관리자 암호가 설정되어 있지 않은 경우에는 BIOS Configuration 설정에 대한 보기 및 변경 권한이 모두 주어집니다.

설정 확인 또는 변경

구성 설정을 보거나 변경하려면

1. BIOS Configuration 페이지 중 하나를 누릅니다.
2. 변경한 다음 **Apply**(적용)를 눌러 변경 사항을 저장합니다.
3. BIOS Configuration 을 종료하고 컴퓨터를 재시작합니다.

   컴퓨터를 재시작하면 변경 사항이 적용됩니다.

주: 암호 변경은 컴퓨터를 재시작할 필요없이 즉시 적용됩니다.

File(파일)

BIOS Configuration for HP ProtectTools 의 파일 옵션에서는 프로세서 유형, 시스템 BIOS 이름 및 버전, 섀시, 일련 번호 등과 같은 시스템 정보를 제공합니다. 이 중 유일하게 편집 가능한 파일 데이터는 Asset Tracking Number 이며, 다른 모든 데이터는 읽기 전용으로 제공됩니다.

주: 파일 옵션에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

Storage(저장 장치)

BIOS Configuration for HP ProtectTools 의 저장 장치 옵션은 컴퓨터에서 구성된 모든 부팅 장치에 대한 정보를 제공하고 해당 장치에 맞는 설정을 지정할 수 있게 해줍니다. 저장 장치에서 액세스할 수 있는 설정은 다음과 같습니다.

- Device Configuration(장치 구성)
- Storage Options(저장 장치 옵션)
- DPS Self-Test(DPS 자가 진단 테스트)
- Boot Order(부팅 순서)

주: 저장 장치 옵션에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

Security(보안)

BIOS Configuration for HP ProtectTools 의 보안 옵션에서는 보안 및 암호와 관련된 모든 설정을 한 눈에 볼 수 있습니다. 여기에 해당하는 설정은 다음과 같습니다.

- Setup Password(설정 암호)
- Power-On Password(파워온 암호)
- Password Options(암호 옵션)
- Smart Cover(일부 모델)
- Device security(장치 보안)
- Network Service Boot(네트워크 서비스 부팅)
- System ID(시스템 ID)

- DriveLock 보안
- System Security(일부 모델)
- Setup Security Level(보안 수준 설정)

주: 보안 옵션에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

Power(전원)

BIOS Configuration for HP ProtectTools 에 들어 있는 전원 옵션은 하드웨어 수준에 맞게 전원 관리를 제어할 수 있는 설정을 제공합니다. 여기에 해당하는 설정은 다음과 같습니다.

- OS Power Management(운영체제 전원 관리)
- Hardware Power Management(하드웨어 전원 관리)
- Thermal(열)

주: 전원 옵션에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

Advanced(고급)

BIOS Configuration for HP ProtectTools 의 고급 옵션에 들어 있는 설정은 고급 사용자를 위한 설정입니다. 여기에 해당하는 설정은 다음과 같습니다.

- Power-On Options(파워온 옵션)
- Execute Memory Test(메모리 테스트 실행)(일부 모델)
- BIOS Power-On(BIOS 파워온)
- Onboard Devices(내장 장치)
- PCI Devices(PCI 장치)
- PCI VGA Configuration(PCI VGA 구성)
- Bus Options(버스 옵션)
- Device Options(장치 옵션)
- Management Devices(관리 장치)
- Management Operations(관리 작업)

주: 고급 옵션에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

9 Embedded Security for HP ProtectTools

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

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

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

TPM 내장 보안 칩은 HP ProtectTools Security Manager for Administrators 의 보안 기능을 강화할 뿐만 아니라 더욱 다양한 기능을 사용할 수 있게 해줍니다. 예를 들어, Credential Manager for HP ProtectTools 는 사용자가 Windows 에 로그온할 때 TPM 내장 칩을 인증 요소의 하나로 사용할 수 있습니다. 일부 모델에서는 TPM 내장 보안 칩이 BIOS Configuration for HP ProtectTools 를 통해 액세스할 수 있는 향상된 BIOS 보안 기능을 제공하기도 합니다.

설정 절차

△ 주의: 보안 위험을 줄이려면 IT 관리자가 즉시 내장 보안 칩을 초기화하는 것이 좋습니다. 내장 보안 칩의 초기화에 실패하면 무단 사용자, 컴퓨터 웜 또는 바이러스 등이 컴퓨터를 소유하여 응급 복구 아카이브 처리, 사용자 액세스 설정 구성 등 소유자의 작업을 제어할 수도 있습니다.

다음 두 단원의 절차에 따라 내장 보안 칩을 활성화 및 초기화하십시오.

Computer Setup 에서 내장 보안 칩 활성화

아래에 설명한 것처럼 내장 보안 칩은 Quick Initialization Wizard 또는 Computer Setup 유틸리티에서 활성화될 수 있습니다. 이 절차는 BIOS Configuration for HP ProtectTools 에서 수행되지 않습니다.

Computer Setup 에서 내장 보안 칩을 활성화하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 다시 시작하고 F10 = ROM Based Setup 메시지가 화면의 왼쪽 아래에 나타나면 F10 키를 눌러 Computer Setup 을 엽니다.
2. 관리자 암호를 설정하지 않은 경우, 화살표 키를 사용하여 **Security**(보안), **Setup password**(설정 암호)를 선택한 다음 Enter 키를 누릅니다.
3. **New password**(새 암호) 및 **Verify new password**(새 암호 확인) 입력란에 암호를 입력하고 F10 키를 누릅니다.
4. **Security**(보안) 메뉴에서 화살표 키를 사용하여 **TPM Embedded Security** 를 선택한 다음 Enter 키를 누릅니다.
5. **Embedded Security** 에서 장치가 숨김 상태인 경우 **Available**(사용 가능)을 선택합니다.
6. **Embedded security device state**(내장 보안 장치 상태)를 선택하고 **Enable**(활성화)로 변경하십시오.
7. F10 키를 눌러 Embedded Security 구성에 대한 변경사항을 수락합니다.
8. 기본 설정을 저장하고 Computer Setup 을 종료하려면 화살표 키를 사용하여 **File**(파일), **Save Changes and Exit**(변경 사항 저장 후 종료)를 선택한 다음 화면 지침을 따릅니다.

내장 보안 칩 초기화

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

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

내장 보안 칩을 초기화하려면 다음과 같이 하십시오.

1. 작업 표시줄의 가장 오른쪽에 있는 알림 영역의 HP ProtectTools Security Manager for Administrators 아이콘을 마우스 오른쪽 버튼으로 누른 다음 **Embedded Security Initialization**(내장 보안 초기화)을 선택합니다.

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

2. 화면 지침을 따릅니다.

기본 사용자 계정 설정

Embedded Security 에서 기본 사용자 계정을 설정하면 다음 작업이 완료됩니다.

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

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

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

1. Embedded Security User Initialization Wizard(Embedded Security 사용자 초기화 마법사)가 열려 있지 않은 경우 Windows Vista 에서는 **시작**, **모든 프로그램**을 누른 다음 **HP ProtectTools Security Manager for Administrators** 를 누르고 Windows XP 에서는 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Embedded Security**, **User Settings**(사용자 설정)를 차례로 누릅니다.
3. 오른쪽 창의 **Embedded Security Features**(Embedded Security 기능)에서 **Configure**(구성)를 누릅니다.

   Embedded Security User Initialization Wizard(Embedded Security 사용자 초기화 마법사)가 열립니다.

4. 화면 지침을 따릅니다.

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

일반 작업

기본 사용자 계정을 설정한 후 다음 작업을 수행할 수 있습니다.

- 파일 및 폴더 암호화
- 암호화된 전자 우편 송수신

개인 보안 드라이브 사용

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

파일 및 폴더 암호화

암호화된 파일을 사용할 경우 다음 규칙을 알아 두어야 합니다.

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

파일 및 폴더를 암호화하려면 다음과 같이 하십시오.

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

암호화된 전자 우편 송수신

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

기본 사용자 키 암호 변경

기본 사용자 키 암호를 변경하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Embedded Security**, **User Settings**(사용자 설정)를 차례로 누릅니다.
3. 오른쪽 창의 **Basic User Key password**(기본 사용자 키 암호)에서 **Change**(변경)를 누릅니다.
4. 이전 암호를 입력한 다음 새 암호를 설정하고 확인합니다.
5. **확인**을 누릅니다.

고급 작업

백업 및 복원

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

백업 파일 생성

백업 파일을 생성하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Backup**(백업)을 누릅니다.
3. 오른쪽 창에서 **Backup**(백업)을 누릅니다. HP ProtectTools Embedded Security Backup Wizard (HP ProtectTools Embedded Security 백업 마법사)가 열립니다.
4. 화면 지침을 따릅니다.

백업 파일에서 인증서 데이터 복원

백업 파일에서 데이터를 복원하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Backup**(백업)을 누릅니다.
3. 오른쪽 창에서 **Restore**(복원)를 누릅니다. HP ProtectTools Embedded Security Backup Wizard (HP ProtectTools Embedded Security 백업 마법사)가 열립니다.
4. 화면 지침을 따릅니다.

소유자 암호 변경

소유자 암호를 변경하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.

3. 오른쪽 창의 **Owner Password**(소유자 암호)에서 **Change**(변경)를 누릅니다.
4. 이전 소유자 암호를 입력한 다음 새 소유자 암호를 설정하고 확인합니다.
5. **확인**을 누릅니다.

사용자 암호 재설정

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

Embedded Security 활성화 및 비활성화

보안 기능 없이 작업하고자 할 경우, Embedded Security 기능을 비활성화할 수 있습니다.

다음과 같이 2 가지 다른 단계로 Embedded Security 기능을 활성화 또는 비활성화할 수 있습니다.

- 임시 비활성화 - 이 옵션을 사용하면 Windows 재시작 시 자동으로 내장 보안이 다시 활성화됩니다. 이 옵션은 기본적으로 모든 사용자가 사용할 수 있습니다.
- 영구 비활성화 - 이 옵션을 사용하면 Embedded Security 를 다시 활성화할 때 소유자 암호가 필요합니다. 이 옵션은 관리자만 사용할 수 있습니다.

Embedded Security 영구 비활성화

Embedded Security 를 영구 비활성화하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.
3. 오른쪽 창의 **Embedded Security** 에서 **Disable**(비활성화)을 누릅니다.
4. 프롬프트에서 소유자 암호를 입력하고 **OK**(확인)를 누릅니다.

Embedded Security 영구 비활성화 후 활성화

Embedded Security 를 영구 비활성화한 후 활성화하려면 다음과 같이 하십시오.

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Advanced**(고급)를 누릅니다.
3. 오른쪽 창의 **Embedded Security** 에서 **Disable**(비활성화)을 누릅니다.
4. 프롬프트에서 소유자 암호를 입력하고 **OK**(확인)를 누릅니다.

Migration Wizard(마이그레이션 마법사)로 키 마이그레이션

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

마이그레이션에 대한 자세한 내용은 Embedded Security 소프트웨어 도움말을 참조하십시오.

10 Device Access Manager for HP ProtectTools

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

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

백그라운드 서비스 시작

장치 프로파일이 적용되도록 하려면 HP ProtectTools Device Locking/Auditing 백그라운드 서비스를 실행해야 합니다. 장치 프로파일의 적용을 처음 시도하면 HP ProtectTools Security Manager for Administrators 에서 백그라운드 서비스를 시작하기 원하는지 묻는 대화 상자가 열립니다. **Yes**(예)를 누르면 백그라운드 서비스가 시작되고 시스템이 부팅될 때마다 서비스가 자동 시작되도록 설정됩니다.

기본 구성

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

- 관리자 외의 모든 사용자에 대해 USB 장치의 액세스 거부
- 관리자 외의 모든 사용자에 대해 모든 이동식 미디어(플로피 디스크, 펜 드라이브 등)의 액세스 거부
- 관리자 외의 모든 사용자에 대해 모든 DVD/CD-ROM 드라이브의 액세스 거부
- 관리자 외의 모든 사용자에 대해 모든 직렬 및 병렬 포트의 액세스 거부

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

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **Simple Configuration**(기본 구성)을 누릅니다.
3. 오른쪽 창에서 액세스를 거부할 장치의 확인란을 선택합니다.
4. **Apply**(적용)를 누릅니다.

주: 백그라운드 서비스가 실행되고 있지 않을 경우 지금 시작됩니다. **Yes**(예)를 눌러 허용합니다.

5. **확인**을 누릅니다.

장치 클래스 구성(고급)

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

사용자 또는 그룹 추가

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **Device Class Configuration**(장치 클래스 구성)을 누릅니다.
3. 장치 목록에서 구성할 장치 클래스를 누릅니다.
4. **Add**(추가)를 누릅니다. **Select Users or Groups**(사용자 또는 그룹 선택) 대화 상자가 열립니다.
5. **Advanced**(고급)를 누른 다음 **Find Now**(지금 찾기)를 눌러 사용자나 그룹을 찾아 추가합니다.
6. 사용 가능한 사용자 및 그룹 목록에 추가할 사용자 또는 그룹을 선택한 다음 **확인**을 누릅니다.
7. **확인**을 누릅니다.

사용자 또는 그룹 제거

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **Device Class Configuration**(장치 클래스 구성)을 누릅니다.
3. 장치 목록에서 구성할 장치 클래스를 누릅니다.
4. 제거할 사용자나 그룹을 누른 다음 **Remove**(제거)를 누릅니다.
5. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

사용자 또는 그룹에 대한 액세스 거부

1. **시작**, **모든 프로그램**을 누른 다음 Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators** 를, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다.
2. 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **Device Class Configuration**(장치 클래스 구성)을 누릅니다.
3. 장치 목록에서 구성할 장치 클래스를 누릅니다.
4. **User/Groups**(사용자/그룹)에서 액세스를 거부할 사용자나 그룹을 누릅니다.
5. 액세스를 거부할 사용자 또는 그룹 옆에 있는 **Deny**(거부)를 누릅니다.
6. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

11 문제 해결

HP ProtectTools Credential Manager

증상	설명	해결 방법
사용자가 Credential Manager 네트워크 계정 옵션을 사용하여 로그온할 도메인 계정을 선택할 수 있는데, TPM 인증을 사용하는 경우 이 옵션을 사용할 수 없습니다. 다른 인증 방법은 모두 제대로 작동함	TPM 인증을 사용하면 사용자는 로컬 컴퓨터에만 로그온됩니다.	Credential Manager Single Sign On 도구를 사용하면 사용자가 다른 계정도 인증할 수 있습니다.
Credential Manager 를 설치한 다음에 설치했다면 Credential Manager 에서 스마트 카드나 USB 토큰을 사용할 수 없습니다.	Credential Manager 에서 스마트 카드나 USB 토큰을 사용하려면 지원 소프트웨어(드라이버, PKCS#11 제공업체 등)를 반드시 Credential Manager 보다 먼저 설치해야 합니다. 이미 Credential Manager 를 설치한 상태라면 스마트 카드나 토큰 지원 소프트웨어를 설치한 다음에 아래 절차를 수행합니다.	Credential Manger 에 로그온 하십시오. HP ProtectTools Security Manager 에서 **Credential Manager**, **Advanced Settings** 을 누른 다음 **Smart Cards and Tokens** 탭을 누릅니다. 사용 가능한 토큰이 Local Tokens 에표시됩니다. Local Tokens 노드를 마우스 오른쪽 버튼으로 눌러 팝업 메뉴에 액세스한 다음 Scan for New Smart Cards and Tokens 를 선택합니다. 메시지가 표시되면 컴퓨터를 재시작합니다.
일부 응용프로그램 웹 페이지에서 사용자의 작업 수행 또는 완료를 중단하는 오류가 발생함	일부 웹 기반 응용프로그램에서 SSO (Single Sign On) 기능 패턴의 비활성화로 인해 작동이 중지되고 오류가 보고됩니다. 예를 들어, Internet Explorer 에서 오류가 발생했음을 나타내는 노란색 삼각형 느낌표(**!**)가 표시됩니다.	Credential Manager Single Sign On 은 모든 소프트웨어 웹 인터페이스를 지원하지 않습니다. SSO 지원을 해제하여 특정 웹 페이지의 SSO 지원을 비활성화합니다. Credential Manager 소프트웨어 도움말 파일에 들어있는 SSO 에 관한 전체 설명서를 참조하십시오. 해당 응용프로그램에 대해 비활성화할 수 없는 특정 SSO 의 경우 해당 지역 HP 서비스 및 지원 센터로 전화하여 세 번째 수준의 지원을 요청하십시오.
로그온 과정 동안 **Browse for Virtual Token**(가상 토큰 탐색) 옵션이 표시되지 않음	이 탐색 옵션은 보안상의 문제로 제거되었으므로 사용자가 Credential Manager 에 등록된 가상 토큰의 위치를 이동할 수 없습니다.	무단 사용자가 이 탐색 옵션을 사용하여 파일을 삭제하고, 이름을 변경하며, Windows 를 제어할 수 있다는 문제점 때문에 제거되었습니다.
도메인 관리자에게 권한이 있는데 Windows 암호를 변경하지 못함	이 현상은 도메인 관리자가 해당 도메인 및 로컬 PC 에 대해 관리자 권한을 가진 계정으로 도메인에 로그온한 다음 Credential Manager 에서 도메인 ID 를 등록한 경우 발생합니다. 도메인 관리자가 Credential Manager 에서 Windows 암호를 변경하려고 하면 **User account restriction(사용자 계정 제한)**	Credential Manager 는 **Change Windows password** (Windows 로그온 암호 변경)으로 도메인 사용자 계정 암호를 변경할 수 없습니다. Credential Manager 는 로컬 PC 계정 암호 변경만 할 수 있습니다. 도메인 사용자는 **Windows security**(Windows 보안)의 **Change password**(암호 변경) 옵션을 통해 자신의 암호를 변경할 수 있으나, 로컬 PC 에 물리적 계정이 없기 때문에

증상	설명	해결 방법
	이라는 로그온 실패 오류 메시지가 나타납니다.	Credential Manager 는 로그온 시 사용하는 암호만 변경할 수 있습니다.
Credential Manager 와 Corel WordPerfect 12 암호 GINA 가 호환되지 않는 문제	Credential Manager 에 로그온하여 WordPerfect 에서 문서를 작성한 후 암호로 보호되는 문서로 저장한 경우 Credential Manager 는 암호 GINA 를 수동 또는 자동으로 찾아내거나 알아낼 수 없습니다.	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
Credential Manager 가 화면에서 **Connect**(접속) 버튼을 인식하지 못함	RDP(Remote Desktop Connection)용 SSO 인증서가 **Connect**(접속)로 설정된 경우 SSO 는 다시 시작할 때 **Connect**(접속)가 아닌 **Save As**(다른 이름으로 저장)를 표시합니다.	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
TPM 으로 보호되는 Credential Manager 인증 정보가 모두 손실될 가능성이 있음	TPM 모듈이 제거되거나 손상된 경우 TPM 으로 보호되는 Credential Manager 의 모든 인증서가 소실됩니다.	이는 설계상의 이유입니다. TPM 모듈은 Credential Manager 의 인증서를 보호하도록 설계되었습니다. TPM 모듈을 제거하기 전에 Credential Manager 에서 ID 를 백업하도록 하십시오.
Windows XP 서비스 팩 1 의 경우 절전 모드에서 최대 절전 모드로 전환한 후 Credential Manager 에 로그온할 수 없음	시스템을 최대 절전 모드 및 절전 모드로 전환한 후 관리자 또는 사용자가 Credential Manager 에 로그온할 수 없고, 선택한 로그온 인증서(암호, 지문 또는 Java Card)에 관계없이 Windows 로그온 화면이 표시된 채로 남아 있습니다.	Windows Update 로 Windows 를 서비스 팩 2 로 업데이트하십시오. 문제 원인에 관한 자세한 내용은 http://www.microsoft.com 에서 Microsoft 기술 자료 문서 813301 을 참조하십시오. 로그온하려면 Credential Manager 를 먼저 선택한 후 로그온해야 합니다. Credential Manager 에 로그온하면 Windows 로그온 메시지(사용자가 Windows 로그온 옵션을 선택해야할 수 있음)가 표시된 후 로그온 과정을 완료하게 됩니다. Windows 에 먼저 로그온한 경우에는 Credential Manager 에 수동으로 로그온해야 합니다.
Embedded Security 를 복원하면 Credential Manager 오류가 발생함	ROM 이 출하 시 기본 설정으로 복원되면 Credential Manager 에서 인증서를 등록할 때 오류가 발생합니다.	Credential Manager 를 설치한 후 ROM 이 출하 시 기본 설정으로 재설정되면 Credential Manager 가 TPM 에 액세스할 수 없습니다. TPM 내장 보안 칩은 Computer Setup 유틸리티(F10 키), BIOS Configuration 또는 HP Client Manager 를 사용하여 활성화할 수 있습니다. Computer Setup 을 사용하여 TPM 내장 보안 칩을 활성화하려면 다음 단계를 수행합니다. 1. 컴퓨터를 켜거나 다시 시작한 다음 화면 왼쪽 하단 모서리에 **F10 = ROM Based Setup** 메시지가 나타나면 F10 키를 눌러 Computer Setup 을 엽니다. 2. 화살표 키를 사용하여 **Security(보안)**를 누른 다음 **Setup Password(설정 암호)**를 누릅니다. 암호를 설정합니다. 3. **Embedded Security Device(Embedded Security 장치)**를 선택합니다. 4. 화살표 키를 사용하여 **Embedded Security Device–Disable(Embedded Security 장치 사용 안 함)**을 선택합니다. 화살표 키를 사용하여

증상	설명	해결 방법
		Embedded Security Device–Enable (Embedded Security 장치 사용)로 변경합니다. 5. **Enable(활성화)**를 누른 다음 **Save changes and exit(변경 사항 저장 후 종료)**를 누릅니다. 향후 출시될 소프트웨어 릴리스를 위해 해결책을 모색 중입니다.
보안 **Restore Identity** (ID 복원) 프로세스에서 가상 토큰과의 연결이 손실됨	ID 를 복원하면 Credential Manager 의 로그온 화면에서 가상 토큰 위치와의 연결이 손실됩니다. Credential Manager 에 등록된 가상 토큰이 있더라도 연결을 복원하려면 토큰을 재등록해야 합니다.	이는 설계상의 이유입니다. ID 를 유지하지 않고 Credential Manager 를 제거하면 토큰의 시스템(서버) 부분이 손상되어 토큰의 클라이언트 부분이 ID 복원을 통해 복원되더라도 더 이상 해당 토큰을 사용하여 로그온할 수 없게 됩니다. HP 에서 장기적인 문제 해결책을 모색하고 있습니다.

Embedded Security for HP ProtectTools

증상	설명	해결 방법
PSD 의 암호화 폴더, 하위 폴더, 파일들에서 오류 메시지 발생	파일 및 폴더를 PSD 로 복사하고 폴더/파일 또는 폴더/하위 폴더를 암호화하려고 시도하면 **Error Applying Attributes (속성 적용 중 오류 발생)**라는 메시지가 나타납니다. C:\ 드라이브 또는 추가로 설치한 하드 드라이브에서 동일한 파일을 암호화할 수 있습니다.	이는 설계상의 이유입니다. 파일/폴더를 PSD 로 이동하면 자동으로 해당 파일/폴더가 암호화됩니다. 따라서 이중으로 암호화할 필요가 없습니다. PSD 에서 EFS 를 사용하여 이중으로 암호화를 시도할 경우 이 오류 메시지가 나타납니다.
멀티 부팅 플랫폼에서 다른 OS 에 대한 소유권을 얻을 수 없음	드라이브가 OS 멀티 부팅으로 설정되었을 경우 한 운영체제에서 플랫폼 초기화 마법사를 사용해서만 소유권을 얻을 수 있습니다.	보안을 고려한 설계상의 이유 때문입니다.
권한이 없는 관리자가 암호화된 EFS 폴더의 내용을 조회 및 삭제하고 이름을 변경하며 이동할 수 있음	폴더를 암호화한다고 해서 관리 권한이 없는 사용자가 폴더의 내용을 조회, 삭제, 이동하지 못하는 것은 아닙니다.	이는 설계상의 이유입니다. Embedded Security TPM 이 아닌 EFS 의 특징입니다. Embedded Security 는 Microsoft EFS 소프트웨어를 사용하며, EFS 는 모든 관리자에 대해 파일/폴더 액세스 권한을 유지합니다.
FAT32 를 사용하여 하드 드라이브 복원을 시도할 때 사용할 수 있는 암호화 옵션이 없음	FAT32 를 사용하여 하드 드라이브 복원을 시도할 경우 파일/폴더에 대해 EFS 를 사용하여 아무런 암호화 옵션을 사용할 수 없습니다.	이는 설계상의 이유입니다. FAT32 파티션으로 복원된 드라이브에 소프트웨어를 설치할 수 없음. Microsoft EFS 는 NTFS 만을 지원하며 FAT32 에서는 사용할 수 없습니다. 이는 Microsoft 의 EFS 와 관련된 특징으로서 HP ProtectTools 소프트웨어와는 상관이 없습니다.
사용자가 복구 아카이브 XML 파일을 암호화하거나 삭제할 수 있음	설계상, 이 폴더에 대한 ACL 이 설정되어 있지 않으므로 사용자가 이 파일을 우연히 또는 고의로 암호화하거나 삭제하여 파일을 액세스하지 못하게 만들 수 있습니다. 이 파일이 암호화되거나 삭제되면 아무도 TPM 소프트웨어를 사용할 수 없게됩니다.	이는 설계상의 이유입니다. 사용자는 응급 아카이브에 액세스하여 자신의 기본 사용자 키 백업본을 저장/업데이트할 수 있습니다. 복구 아카이브 파일을 암호화하거나 삭제하는 일이 없도록 사용자에게 주지시켜야 합니다.
Symantec Antivirus 또는 McAfee Total Protection 과 상호작용하는 Embedded Security EFS 는 암호화/복호화 및 스캔 시간이 더 깁니다.	암호화 한 파일이 Symantec Antivirus 나 McAfee Total Protection 바이러스 스캔을 방해하는 것입니다. Symantec Antivirus 또는 McAfee Total Protection 이 실행중이라면 Embedded Security EFS 로 파일을 암호화하는 데 시간이 더 오래 걸립니다.	Embedded Security EFS 파일을 검색하는 데 소요되는 시간을 단축하려면 검색을 시작하기 전에 암호화 암호를 입력하거나 암호화를 해독합니다. Embedded Security EFS 를 사용하여 데이터를 암호화/복호화하는 데 드는 시간을 줄이려면 Symantec Antivirus 나 McAfee Total Protection 에서 Auto-Protect 를 비활성화해야 합니다.
응급 복구 아카이브를 이동식 미디어에 저장할 수 없음	Embedded Security 초기화 과정에서 응급 복구 아카이브 경로를 생성할 때 MMC(MultiMediaCard) 또는 SD(Secure Digital) 메모리 카드를 삽입하면 오류 메시지가 표시됩니다.	이는 설계상의 이유입니다. 이동식 미디어에 복구 아카이브를 저장하는 것은 지원되지 않습니다. 복구 아카이브는 네트워크 드라이브나 C 드라이브가 아닌 다른 로컬 드라이브에 저장할 수 있습니다.

증상	설명	해결 방법
전원 차단으로 인해 Embedded Security 초기화가 중단되고 오류가 발생함	내장 보안 칩을 초기화하는 동안 전원이 차단되면 다음과 같은 문제가 발생합니다. • Embedded Security 초기화 마법사를 실행하려 하면 다음과 같은 오류가 표시됩니다. **The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner. (내장 보안 칩에 이미 Embedded Security 소유자가 있기 때문에 Embedded Security 를 초기화할 수 없습니다.)** • 사용자 초기화 마법사를 실행하려 하면 다음과 같은 오류가 표시됩니다. **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first. (Embedded Security 가 초기화되지 않았습니다. 마법사를 사용하려면 먼저 Embedded Security 를 초기화해야 합니다.)**	다음 절차를 수행하여 전원 차단을 복구합니다. **주:** 따로 지정되지 않은 한 화살표 키를 사용하여 메뉴나 메뉴 항목을 선택하고 값을 변경할 수 있습니다. 1. 컴퓨터를 시작하거나 다시 시작합니다. 2. **F10=Setup** 메시지가 화면에 나타나면 F10 키를 누릅니다. 3. 해당 언어 옵션을 선택합니다. 4. Enter 키를 누릅니다. 5. **Security**(보안)을 선택한 다음 **Embedded Security**(내장 보안)를 누릅니다. 6. **Embedded Security Device**(Embedded Security 장치) 옵션을 **Enable**(사용)로 설정합니다. 7. F10 키를 눌러 변경 사항을 적용합니다. 8. **File**(파일)을 선택한 다음 **Save Changes and Exit**(변경 사항 저장 후 종료)를 누릅니다. 9. Enter 키를 누릅니다. 10. F10 키를 눌러 변경 사항을 저장하고 유틸리티를 종료합니다.
TPM 모듈을 활성화한 후에 Computer Setup (F10 키) 유틸리티 암호를 삭제할 수 있음	TPM 모듈을 활성화하려면 Computer Setup(F10 키) 유틸리티 암호가 필요합니다. 모듈이 활성화되면 사용자는 암호를 삭제할 수 있습니다. 따라서 시스템에 직접 액세스할 수 있는 사용자가 TPM 모듈을 재설정하고 데이터 손실이 발생할 수 있습니다.	이는 설계상의 이유입니다. Computer Setup(F10 키) 유틸리티 암호는 암호를 아는 사용자만 삭제할 수 있습니다. 그러나 Computer Setup (F10 키) 유틸리티 암호를 항상 보호할 것을 권장합니다.
대기 상태 후 시스템을 활성화할 때 PSD 암호 상자가 표시되지 않음	PSD 생성 후 사용자가 시스템에 로그온하면 TPM 에서 기본 사용자 암호를 묻습니다. 사용자가 암호를 입력하지 않으면 시스템이 대기 모드로 들어가고, 작업을 재개해도 암호 대화 상자가 더 이상 표시되지 않습니다.	이는 설계상의 이유입니다. PSD 암호 상자를 다시 표시하려면 사용자가 로그오프한 후 다시 로그온해야 합니다.
보안 플랫폼 정책 변경 시 암호가 필요하지 않음	시스템에 대해 관리 권한이 있는 사용자는 보안 플랫폼 정책(시스템 및 사용자)에 액세스할 때 TPM 암호가 필요하지 않습니다.	이는 설계상의 이유입니다. 관리자는 TPM 사용자 초기화 여부에 상관 없이 보안 플랫폼 정책을 수정할 수 있습니다.
인증서를 볼 때 신뢰되지 않은 것으로 표시됨	HP ProtectTools 를 설정하고 사용자 초기화 마법사를 실행한 후 사용자는 발급된 인증서를 볼 수 있습니다. 그러나 인증서가 신뢰되지 않은 것으로 표시됩니다. 여기에서 설치 버튼을 눌러 인증서를 설치할 수 있지만 그렇게 해도 신뢰된 인증서가 설치되지 않습니다.	자체 서명 인증서는 신뢰되지 않습니다. 정상적으로 구성된 기업 환경에서 EFS 인증서는 온라인 인증 기관을 통해 발급되어야 신뢰됩니다.

증상	설명	해결 방법
다음과 같은 일시적인 암호화 및 암호 해독 오류 메시지가 발생함: **The process cannot access the file because it is being used by another process. (다른 프로세스에서 파일을 사용하고 있기 때문에 액세스할 수 없습니다.)**	운영체제나 다른 응용프로그램에서 파일이나 폴더를 처리하고 있지 않아도 파일 암호화/암호 해독 중 해당 파일을 다른 프로세스에서 사용하고 있다고 하면서 오류가 발생하는 경우가 있습니다.	이를 해결하려면 다음과 같이 하십시오. 1. 시스템을 다시 시작합니다. 2. 로그오프합니다. 3. 다시 로그온합니다.
새 데이터를 생성하거나 이전하기에 전에 저장 미디어를 제거할 경우 이동식 저장 장치에서 데이터 손실이 발생함	멀티베이 하드 드라이브와 같은 저장 미디어를 제거해도 PSD 가 계속 표시되며 PSD 에 데이터를 추가하거나 수정해도 오류가 발생하지 않습니다. 시스템을 다시 시작한 후 이동식 저장 장치를 제거한 동안 발생한 파일 변경 사항이 PSD 에 반영되지 않습니다.	데이터의 생성 또는 이전이 완료되기 전에는 PSD 를 제거하지 마십시오. 이 문제는 새로운 데이터를 생성하거나 이전하는 작업이 완료되기 전에 사용자가 PSD 에 액세스하여 하드 드라이브를 제거한 경우에만 발생합니다. 이동식 하드 드라이브가 장착되지 않았을 때 사용자가 PSD 에 액세스하려 하면 **the device is not ready(장치가 준비되지 않음)**라는 오류 메시지가 표시됩니다.
설치 제거 중 사용자가 기본 사용자를 초기화하지 않고 관리 도구를 열면 **Disable**(비활성화) 옵션을 사용할 수 없으며 관리 도구를 닫아야만 설치 제거 작업을 계속할 수 있음	사용자는 TPM 을 비활성화하지 않고 설치를 제거하거나, 먼저 관리 도구를 통해 TPM 을 비활성화한 후 설치를 제거할 수 있습니다. 관리 도구에 액세스하려면 기본 사용자 키를 초기화해야 합니다. 기본 초기화를 수행하지 않을 경우 사용자는 모든 옵션을 사용할 수 없습니다. **Click Yes to open Embedded Security Administration tool (Embedded Security 관리 도구를 열려면 예를 누르십시오.)** 대화 상자에서 사용자가 **Yes**(예)를 선택하여 관리 도구를 열었기 때문에 설치 제거 프로세스는 관리 도구가 닫힐 때까지 대기합니다. 사용자가 이 대화 상자에서 **No**(아니요)를 누르면 관리 도구가 열리지 않고 설치 제거 프로세스가 진행됩니다.	관리 도구는 TPM 칩을 비활성화하는 데 사용되지만 기본 사용자 키를 초기화해야만 이 옵션을 사용할 수 있습니다. 기본 사용자 키를 초기화하지 않았을 경우 설치 제거 프로세스를 계속하려면 **OK**(확인) 또는 **Cancel**(취소)을 선택합니다.
두 개의 사용자 계정에 PSD 를 생성한 후 128MB 시스템 구성에서 빠른 사용자 전환을 사용할 경우 시스템 잠금이 발생하는 경우가 있음	최소 RAM 사양으로 빠른 사용자 전환을 사용할 경우 시작(로그온) 화면이 표시되지 않고 검정색 화면이 표시되면서 키보드와 마우스가 작동하지 않는 잠금 상태가 될 수 있습니다.	주요 원인은 저사양 메모리 구성에서 발생하는 타이밍 문제일 수 있습니다. 통합 그래픽은 128MB 의 메모리 중 120MB 는 사용자가 이용하도록 남겨 두고 8MB 만 가져오는 UMA 아키텍처를 사용합니다. 두 사용자가 로그온하여 빠른 사용자 전환을 사용할 때 이 120MB 를 공유하면서 오류가 발생하는 것입니다. 해결 방법은 시스템을 재부팅하고 메모리 구성을 늘리는 것입니다. HP 의 보안 모듈에는 128MB 구성이 제공되지 않습니다.
EFS 사용자 인증(암호 요청) 시간이 초과되고 **access denied(액세스 거부)** 메시지가 표시됨	사용자가 **OK**(확인)를 누르거나 시스템이 대기 상태로 전환될 때 EFS 사용자 인증 암호가 다시 열립니다.	이는 설계상의 이유입니다. Microsoft EFS 와 관련된 문제를 방지하기 위해 오류 메시지를 표시하는 30 초 워치독 타이머가 개발되었습니다.
일본어 버전 설정 과정에서 기능 설명에 심각하진 않지만 텍스트 잘림 현상이 보임	설치 마법사의 사용자 설정 옵션의 기능 설명 부분이 잘립니다.	이 오류는 다음 버전에서 수정될 것입니다.

증상	설명	해결 방법
암호를 입력하라는 프롬프트에 암호를 입력하지 않아도 EFS 암호화가 작동함	사용자 암호 프롬프트 시간이 초과될 때까지 두면 파일이나 폴더에 대해 암호화가 계속 작동합니다.	이 기능은 Microsoft EFS 암호화의 기능이므로 암호 인증이 필요하지 않습니다. 암호 해독 시에는 사용자가 암호를 입력해야 합니다.
사용자 초기화 마법사에 보안 전자 우편이 지정되지 않은 경우 또는 사용자 정책에서 보안 전자 우편 구성이 비활성화된 경우에도 보안 전자 우편 기능이 지원됨	Embedded Security 소프트웨어와 마법사는 전자 우편 클라이언트(Outlook, Outlook Express 또는 Netscape)의 설정을 제어하지 않습니다.	이는 설계상의 이유입니다. TPM 전자 우편 설정 구성은 전자 우편 클라이언트 프로그램에서 암호화 설정을 직접 수정하는 것을 제한하지 않습니다. 보안 전자 우편의 사용은 타사 응용프로그램을 통해 설정 및 제어됩니다. HP 마법사는 간편하고 신속한 사용자 정의를 위해 세 가지 참조 응용프로그램을 연결할 수 있도록 합니다.
대량의 배치 작업을 동일한 PC 에서 두 번째로 실행하거나 이전에 초기화한 PC 에서 실행할 경우 응급 복구 및 응급 토큰 파일을 덮어씀. 복구 시 새 파일이 사용되지 않음	이전에 초기화한 HP ProtectTools Embedded Security 시스템에서 대량의 배치 작업을 실행할 경우 xml 파일을 덮어쓰므로 기존의 복구 아카이브 및 복구 토큰이 사용할 없게 됩니다.	xml 파일 덮어쓰기 문제를 해결하기 위한 작업이 진행 중이며 향후 SoftPaq 에서는 이 솔루션을 제공할 예정입니다.
Embedded Security 에서 사용자가 복원 작업을 수행하는 중 자동 로그온 스크립트가 작동하지 않음	사용자가 다음 작업을 수행한 후에 오류가 발생합니다. • 사용자가 Embedded Security 의 소유자와 사용자를 초기화한 후(기본 위치 **My Documents**(내 문서) 사용). • 사용자가 BIOS 에서 칩 설정을 출하시 기본 설정으로 되돌린 후. • 사용자가 컴퓨터를 재부팅한 후. • 사용자가 Embedded Security 복원을 시작한 후. 복원 프로세스 중 Credential Manager 는 Infineon TPM User Authentication 에 자동 로그온할 수 있는지 여부를 묻습니다. 사용자가 **Yes**(예)를 선택하면 텍스트 상자에 SPEmRecToken 위치가 자동으로 나타납니다. 이 위치가 정확하지 않을 경우 **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from(응급 복구 토큰을 입력하지 않았습니다. 응급 복구 토큰을 가져올 토큰 위치를 선택하십시오.)** 라는 메시지가 표시됩니다.	화면에 표시된 **Browse**(찾아보기) 버튼을 눌러 위치를 선택하고 복원 프로세스를 계속합니다.
빠른 사용자 전환 환경에서 여러 사용자 PSD 가 작동하지 않음	이 오류는 여러 사용자를 생성한 후 동일한 드라이브 문자로 PSD 를 지정한 경우에 발생합니다. PSD 로딩 시 사용자 간에 빠른 사용자 전환이 시도되면 두 번째 사용자의 PSD 가 사용할 수 없게 됩니다.	두 번째 사용자의 PSD 는 다른 드라이브 문자를 사용하도록 다시 구성하거나 첫 번째 사용자가 로그오프해야만 사용할 수 있습니다.
PSD 를 생성했던 보조 하드 드라이브를 포맷한 후 PSD 가 비활성화되고 삭제할 수 없게 됨	PSD 아이콘은 여전히 표시되지만 사용자가 PSD 에 액세스하려 하면 **drive is not accessible(드라이브에 액세스할 수 없음)**이라는 오류 메시지가 표시됩니다.	이는 설계상의 이유입니다. PSD 데이터 저장 위치에서 강제로 삭제하거나 연결을 해제하면 Embedded Security PSD 드라이브 에뮬레이션이 계속 작동하고

증상	설명	해결 방법
	사용자가 PSD 를 삭제할 수 없고 **your PSD is still in use, please be sure that your PSD contains no open files and is not accessed by another process(PSD 가 사용 중입니다. PSD 에 열려 있는 파일이 없는지 그리고 다른 프로세스에서 사용하고 있지 않은지 확인하십시오.)**라는 메시지가 표시됩니다. 사용자가 시스템을 재부팅하여 PSD 를 삭제해야 하며 재부팅 후에는 PSD 가 로드되지 않습니다.	손실된 데이터를 사용한 통신으로 인해 오류가 발생합니다. 해결책: 다음 재부팅 후 에뮬레이션 로딩이 실패하면 사용자가 이전의 PSD 에뮬레이션을 삭제하고 새 PSD 를 생성할 수 있습니다.
사용자가 자동 백업 아카이브에서 복원하는 중 내부 오류가 발생함	Embedded Security 에서 사용자가 자동 백업 아카이브에서 복원하는 **Restore under Backup**(백업에서 복원) 옵션을 누르고 **SPSystemBackup.xml** 을 선택할 경우 복원 마법사가 실패하고, **The selected Backup Archive does not match the restore reason. Please select another archive and continue (선택한 백업 아카이브가 복원 사유와 일치하지 않습니다. 다른 아카이브를 선택하고 계속하십시오.)**라는 오류 메시지가 표시됩니다.	SpBackupArchive.xml 이 필요한데 사용자가 **SpSystemBackup.xml** 을 선택할 경우 Embedded Security 마법사가 실패하고, **An internal Embedded Security error has been detected(Embedded Security 내부 오류가 발생했습니다.)**라는 메시지가 표시됩니다. 복원 사유와 일치하는 정확한 .xml 파일을 선택해야 합니다. 이 프로세스는 설계상에 따른 것으로서 오류가 아니지만, Embedded Security 내부 오류 메시지가 지워지지 않는 문제가 있으며 보다 구체적인 내용을 나타내야 합니다. 향후 제품에서 이 사항을 개선하기 위한 작업이 진행 중입니다.
보안 시스템이 여러 사용자와 관련된 복원 오류를 표시함	복원 과정에서 관리자가 복원할 사용자를 선택한 경우 선택되지 않은 사용자는 나중에 복원을 시도할 때 키를 복원할 수 없습니다. **decryption process failed (암호 해독 프로세스 실패)**라는 오류 메시지가 표시됩니다.	선택되지 않은 사용자는 다음에 예정된 일간 백업 실행 전에 TPM 을 재설정하고 복원 프로세스를 실행한 후 모든 사용자를 선택해야 복원될 수 있습니다. 자동 백업이 실행될 경우 복원되지 않은 사용자를 덮어쓰므로 그러한 사용자들의 데이터가 손실됩니다. 새로운 시스템 백업이 저장된 경우 이전에 선택되지 않은 사용자를 복원할 수 없습니다. 또한 사용자는 전체 시스템 백업을 복원해야 합니다. 아카이브 백업은 개별적으로 복원할 수 있습니다.
시스템 ROM 을 기본값으로 재설정하면 TPM 이 비활성화됨	시스템 ROM 을 기본값으로 재설정하면 Windows 에서 TPM 이 표시되지 않습니다. 이렇게 되면 보안 소프트웨어가 제대로 작동하지 않고 TPM 암호화된 데이터를 액세스할 수 없게 됩니다.	다음과 같이 BIOS 에서 TPM 을 활성화합니다. Computer Setup (F10) 유틸리티를 열고 **Security > Device security** 을 탐색한 다음 필드를 **Hidden**(숨김)에서 **Available**(사용)로 수정합니다.
매핑된 드라이브에서 자동 백업이 실행되지 않음	관리자가 Embedded Security 에서 Automatic Backup 을 설정할 때, **Windows > 작업 > 예약된 작업**으로 들어갑니다. 이 Windows 예약된 작업은 백업을 실행할 권한을 얻기 위해 NT AUTHORITY\SYSTEM 을 이용하여 설정합니다. 이는 어느 로컬 드라이브에서도 효과적입니다. 관리자가 자동 백업을 매핑된 드라이브에 저장하도록 구성한 경우에는 NT AUTHORITY\SYSTEM 이 매핑 드라이브를 사용할 수 있는 권한을 갖고 있지 않으므로 이 프로세스가 실패합니다. 자동 백업이 로그온 시 수행되도록 예약된 경우 Embedded Security TNA 아이콘은 **The Backup Archive location is**	이 문제를 해결하려면 NT AUTHORITY\SYSTEM 을 (컴퓨터 이름)\(관리자 이름)으로 변경하십시오. 이 설정은 예약된 작업을 수동으로 생성할 경우의 기본 설정입니다. 향후 제품 릴리스에서는 기본 설정에 컴퓨터 이름\관리자 이름을 포함할 예정입니다.

증상	설명	해결 방법
	currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again(백업 아카이브 위치에 현재 액세스할 수 없습니다. 백업 아카이브가 액세스 가능해질 때까지 임시 아카이브에 백업하려면 여기를 누르십시오.) 라는 메시지를 표시합니다. 그러나 자동 백업이 특정 시간에 예약된 경우에는 실패 메시지 없이 백업이 실패합니다.	
Embedded Security 가 Embedded Security GUI 에서 일시적으로 비활성화됨.	현재 4.0 소프트웨어는 HP Notebook 1.1B 구현에 맞춰 설계되었으며 HP Desktop 1.2 구현을 지원합니다. 이 비활성화 옵션은 TPM 1.1 플랫폼에 대한 소프트웨어 인터페이스에서 계속 지원됩니다.	다음 릴리스에서는 이 문제가 해결될 것입니다.

HP ProtectTools Device Access Manager

증상	설명	해결 방법
Device Access Manager 에서 장치에 대해 사용자 액세스를 거부했으나 장치가 여전히 액세스 가능함	Device Access Manager 에서 Simple Configuration(기본 구성) 및/또는 Device Class Configuration(장치 클래스 구성)을 사용하여 장치에 대한 사용자 액세스를 거부했습니다. 그런데 액세스를 거부해도 사용자가 장치를 계속 액세스할 수 있습니다.	HP ProtectTools Device Locking 서비스가 시작되었는지 확인하십시오. 관리 권한이 있는 사용자로서 **제어판 > 관리 도구 > 서비스**로 들어갑니다. **서비스** 창에서 **HP ProtectTools Device Locking/Auditing** 서비스를 찾습니다. 서비스를 시작하고 시작 유형을 **Automatic**(자동)으로 해야 합니다.
장치에 대해 갑자기 어떤 사용자는 갑자기 액세스가 허용되고 어떤 사용자는 액세스가 거부됨	Device Access Manager 를 사용하여 일부 장치에 대해 사용자 액세스를 거부하고 또 다른 장치에 대해 사용자 액세스를 허용했습니다. 해당 사용자가 시스템을 사용할 때 Device Access Manager 에서 액세스를 거부한 장치에는 액세스가 가능하고, Device Access Manager 에서 액세스를 허용한 장치에는 액세스가 불가능합니다.	Device Access Manager 에서 Device Class Configuration(장치 클래스 구성)을 사용하여 사용자 장치 설정을 검사해야 합니다. **Security Manager**, **Device Access Manager**, **Device Class Configuration** 를 차례로 누릅니다. Device Class 트리 레벨을 확장하여 해당 사용자에 적용되는 설정을 검토합니다. 사용자 또는 사용자들이 '사용자'나 '관리자' 등의 구성원일 수 있는 Windows 그룹에서 설정할 수 있는 “Deny” 사용권한이 있는지 확인합니다.
허용 또는 거부—어떤 사용 권한이 우선합니까?	Device Class Configuration(장치 클래스 구성)에 다음 구성이 설정되어 있습니다. • 장치 클래스 계층(예: DVD/CD-ROM 드라이브)의 동일한 수준에서 어떤 Windows 그룹(예: BUILTIN\Administrators)에는 Allow(허용) 사용 권한이 부여되어 있고, 또 다른 Windows 그룹(예: BUILTIN\Users)에는 Deny(거부) 사용 권한이 부여되어 있습니다. 한 사용자가 양쪽 그룹(예: Administrator)의 구성원일 경우 어떤 사용 권한이 우선합니까?	그 사용자는 장치에 액세스할 수 없습니다. Deny(거부) 설정이 Allow(허용) 설정보다 우선합니다. Windows 에서 장치에 대해 유효한 사용 권한을 적용하므로 액세스가 거부됩니다. 한 그룹은 액세스가 거부되고 한 그룹은 액세스가 허용되지만 사용자가 두 그룹 모두의 구성원이고, 액세스 거부는 액세스 허용보다 우선하므로 이 사용자는 액세스가 거부됩니다. 한 가지 해결 방법은 DVD/CD-ROM 드라이브 수준에서 Users 그룹에 대해 액세스를 거부하고, DVD/CD-ROM 드라이브 아래 수준에서 Administrators 그룹에 대해 액세스를 허용하는 것입니다. 또 다른 해결 방법은 별도의 Windows 그룹을 만들어 한 그룹에는 DVD/CD 에 대한 액세스를 허용하고 다른 그룹에는 DVD/CD 에 대한 액세스를 거부하는 것입니다. 그런 다음 해당 사용자를 해당 그룹에 추가합니다.

기타

영향 받은 소프트웨어–증상	설명	해결 방법
Security Manager 에서 **The security application can not be installed until the HP Protect Tools Security Manager is installed(HP Protect Tools Security Manager 를 설치해야만 보안 응용프로그램을 설치할 수 있습니다.)**라는 경고 메시지가 표시됨	Embedded Security, Java Card Security, 생체 인식과 같은 모든 보안 응용프로그램은 HP Security Manager 인터페이스에 추가하여 사용할 수 있는 확장 플러그인입니다. HP 인증 보안 플러그인을 사용하려면 먼저 Security Manager 를 설치해야 합니다.	보안 플러그인을 설치하려면 먼저 Security Manager 소프트웨어를 설치해야 합니다.
Broadcom 지원 TPM 을 포함하는 모델용 HP ProtectTools TPM Firmware Update Utility—HP 지원 웹 사이트를 통해 제공된 도구에서 **ownership required(소유권 필요)**를 보고함	Broadcom 지원 TPM 을 포함하는 모델용 TPM 펌웨어 유틸리티의 정상적인 동작입니다. 사용자는 펌웨어 업그레이드 도구를 사용하여 승인 키(EK) 소유 여부에 상관 없이 펌웨어를 업그레이드할 수 있습니다. EK 가 없을 경우 펌웨어 업그레이드를 수행하는 데 인증이 필요하지 않습니다. EK 가 있을 경우 업그레이드 시 소유자 인증이 필요하므로 TPM 소유자가 있어야 합니다. 업그레이드가 완료되면 플랫폼을 다시 시작해야 새로운 펌웨어가 적용됩니다. BIOS TPM 의 설정을 기본값으로 복원하면 소유권이 삭제되면서 Embedded Security 소프트웨어 플랫폼과 사용자 초기화 마법사를 구성할 때까지 펌웨어 업데이트를 수행할 수 없습니다. **주:** 펌웨어 업데이트 후에는 반드시 재부팅하도록 하십시오. 재부팅을 해야만 펌웨어 버전이 업데이트됩니다.	1. Embedded Security 소프트웨어를 다시 설치합니다. 2. 플랫폼 및 사용자 구성 마법사를 실행합니다. 3. 시스템에 Microsoft .NET framework 1.1 이 설치되어 있는지 확인합니다. a. **시작**을 누릅니다. b. **제어판**을 누릅니다. c. **프로그램 추가/제거**를 누릅니다. d. **Microsoft .NET Framework 1.1** 이 목록에 있는지 확인합니다. 4. 하드웨어 및 소프트웨어 구성을 확인합니다. a. **시작**을 누릅니다. b. **모든 프로그램**을 누릅니다. c. Windows Vista 인 경우 **HP ProtectTools Security Manager for Administrators**, Windows XP 인 경우 **HP ProtectTools Security Manager** 를 누릅니다. d. 트리 메뉴에서 **Embedded Security** 를 선택합니다. e. **More Details**(자세한 정보)를 누릅니다. 구성이 다음과 같아야 합니다. • Product version(제품 버전) = V4.0.1 • Embedded Security State(Embedded Security 상태): Chip State(칩 상태) = Enabled(활성), Owner State(소유자 상태) = Initialized(초기화됨), User State(사용자 상태) = Initialized(초기화됨) • Component Info(구성 요소 정보): TCG Spec. Version(버전) = 1.2 • Vendor(판매업체) = Broadcom Corporation

영향 받은 소프트웨어–증상	설명	해결 방법
		• FW Version(펌웨어 버전) = 2.18(또는 그 이상) • TPM Device driver library version(TPM 장치 드라이버 라이브러리 버전) 2.0.0.9(또는 그 이상) 5. FW 버전이 2.18 과 일치하지 않는다면 TPM 펌웨어를 다운받아 업데이트합니다. TPM Firmware SoftPaq 은 HP 웹 사이트(http://www.hp.com)에서 다운 받을 수 있습니다.
HP ProtectTools Security Manager–Security Manager 인터페이스를 종료할 때 가끔씩 오류가 반환됨	플러그인 응용프로그램이 모두 로드되기 전에 화면 상단 오른쪽의 닫기 버튼을 눌러 Security Manager 를 종료하면 가끔씩 (12 번에 1 번 정도) 오류가 발생합니다.	이 문제는 Security Manager 를 종료하거나 실행할 때 플러그인 서비스의 로드 시간에 따른 것입니다. PTHOST.exe 는 다른 플러그인 응용프로그램들을 포함하는 쉘 프로그램이므로 플러그인의 로드 시간(서비스)에 영향을 받습니다. 이 문제의 근본 원인은 플러그인이 완전히 로드되기 전에 쉘 프로그램을 종료했기 때문입니다. Security Manager 창의 상단에 서비스가 모두 로드되었다는 메시지가 표시되고 왼쪽 목록에 모든 플러그인이 나열될 때까지 기다리십시오. 플러그인이 모두 로드될 때까지 충분한 시간을 기다리면 문제를 방지할 수 있습니다.
HP ProtectTools—액세스가 제한되거나 관리자 권한 제어가 불가능하여 보안 위험이 발생함	클라이언트 PC 에 대한 액세스를 제어할 수 없을 경우 다음과 같은 많은 위험이 발생할 수 있습니다. • PSD 삭제 • 사용자 설정에 대한 악의적인 수정 • 보안 정책 및 기능의 사용 불가	관리자가 최종 사용자 권한과 사용자 액세스에 대해 “최선의 방법”을 수행할 것을 권장합니다. 무단 사용자에게는 관리 권한을 부여하지 말아야 합니다.
BIOS 및 OS Embedded Security 암호가 동기화되지 않음	사용자가 새 암호를 BIOS Embedded Security 암호로 승인하지 않은 경우 BIOS Embedded Security 암호는 F10 BIOS 를 통해 기존의 내장 보안 암호로 돌아갑니다.	설계상에 따른 정상적인 동작이며, 이러한 암호는 OS 기본 사용자 암호를 변경하고 BIOS Embedded Security 암호 프롬프트에서 이를 승인함으로써 동기화할 수 있습니다.
BIOS 에서 TPM Preboot 인증을 활성화한 후 시스템에 한 명의 사용자만 로그온할 수 있음	TPM BIOS PIN 은 사용자 설정을 초기화하는 첫 번째 사용자와 연결되어 있습니다. 컴퓨터에 여러 사용자 계정이 있을 경우 원칙적으로 첫 번째 사용자가 관리자입니다. 첫 번째 사용자는 자신의 TPM 사용자 PIN 을 다른 사용자에게 부여해서 로그온할 수 있도록 해야 합니다.	이는 설계상의 이유입니다. IT 부서에서 보안 솔루션 전개를 위한 강력한 보안 정책을 사용할 것을 권장하며, IT 관리자가 BIOS 관리자 암호를 구성하여 시스템 수준의 보안을 적용하도록 해야 합니다
사용자가 TPM 설정을 기본값으로 복원한 후 TPM preboot 를 활성화하려면 PIN 을 변경해야 함	사용자가 재설정 후 TPM BIOS 인증을 작동하기 위해 사용자 설정을 초기화하려면 PIN 을 변경하거나 다른 사용자를 생성해야 합니다. TPM BIOS 인증을 작동하기 위한 다른 옵션이 없습니다.	설계상에 따른 것으로서 설정을 기본값으로 복원하면 기본 사용자 키가 지워집니다. 자신의 사용자 PIN 을 변경하거나 새로운 사용자를 생성하여 기본 사용자 키를 다시 초기화해야 합니다.
Embedded Security 의 **Reset to Factory Settings**(기본 설정으로 복원)를 사용하여 **Power-on authentication support**(파워온 인증 지	Computer Setup 에서 Embedded Security 의 **Reset to Factory Settings**(기본 설정으로 복원) 옵션을 사용하여 **Power-on authentication support**(파워온 인증 지원) 옵션을 기본 설정으로 복원할 수 없습니다. **Power-on authentication support**(파워온 인증 지	**Reset to Factory Settings**(기본 설정으로 복원) 옵션은 Embedded Security 장치를 비활성화하므로 **Power-on authentication support**(파워온 인증 지원) 옵션을 비롯한 Embedded Security 옵션이 표시되지 않습니다. 그러나 Embedded Security 장치를 다시 활성화하면 **Power-on authentication support**(파워온 인증 지원) 옵션이 활성 상태로 유지됩니다.

영향 받은 소프트웨어–증상	설명	해결 방법
원) 설정을 기본값으로 복원할 수 없음	원) 옵션은 기본적으로 **Disable**(비활성)로 설정됩니다.	이를 해결하기 위한 작업이 진행 중이며 향후 웹 기반의 ROM SoftPaq 에 적용될 예정입니다.
부팅 중 보안 파워온 인증이 BIOS 암호를 오버랩함	파워온 인증은 사용자가 시스템에 로그온할 때 TPM 암호를 입력하도록 요청하며, 사용자가 F10 키를 눌러 BIOS 로 들어갈 경우 읽기 권한만 부여합니다.	BIOS 에서 쓰기 작업을 수행하려면 Power-on Authentication(파워온 인증) 창에 TPM 암호 대신 BIOS 암호를 입력해야 합니다.
소유자 암호가 변경된 후 Computer Setup 을 실행하면 BIOS 에서 이전 암호와 새 암호를 모두 물음	Embedded Security Windows 소프트웨어에서 소유자 암호를 변경한 후 Computer Setup 을 실행할 때 BIOS 에서 기존 암호와 새 암호를 모두 묻습니다.	이는 설계상의 이유입니다. 운영체제를 실행한 후 BIOS 가 TPM 과 통신할 수 없어서 TPM 암호문을 확인할 수 없기 때문에 발생하는 문제입니다.

용어

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

BIOS 관리자 암호. Computer Setup(컴퓨터 설정)의 *설정* 암호입니다.

BIOS 보안 모드. Java Card Security 이 활성화된 경우 이 모드를 설정하면 Java Card 와 유효한 PIN 이 있어야 사용자 인증이 가능함

BIOS 프로필. 저장하여 다른 계정에 적용할 수 있는 BIOS 구성 설정 그룹

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

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

Drive Encryption 키 복구 서비스. SafeBoot 복구 서비스는 암호화 키 사본을 저장하는 서비스로, 암호가 기억나지 않거나 로컬 백업 키에 대한 액세스 권한이 없는 경우 이 서비스를 사용하여 컴퓨터에 액세스할 수 있습니다. 백업 키에 온라인 액세스를 설정하려면 해당 서비스에 대한 계정을 만들어야 합니다.

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

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

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

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

PKI(공용 키 인프라) 인증서와 암호화 키를 작성, 사용, 관리하기 위한 인터페이스를 정의하는 표준

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

PSD(개인 보안 드라이브). 중요 정보를 위한 안전한 보관 영역 제공

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

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

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

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

TPM(Trusted Platform Module) 내장 보안 칩. HP ProtectTools Embedded Security Chip 의 일반적인 명칭입니다. TPM 은 암호화 키, 디지털 인증, 암호 등의 호스트 시스템 정보를 저장하여 사용자가 아닌 컴퓨터를 인증합니다. TPM 을 사용하면 도난 또는 외부 해커 공격의 위험을 최소화할 수 있습니다.

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

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

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

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

TXT. Trusted Execution Technology 의 약자. 컴퓨터의 소프트웨어 및 데이터를 향한 공격에 대해 보안을 제공하는 하드웨어 및 펌웨어.

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

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

Windows 사용자 계정. 네트워크나 개별 컴퓨터에 로그온하도록 승인된 개인 프로필

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

고급 보안. 파워온 및 관리자 암호와 기타 다른 형태의 파워온 인증에 대한 보호를 강화하는 BIOS 구성의 보안 기능

관리자. Windows 관리자 참조

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

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

대화 기록 뷰어. 암호화된 대화 기록 세션을 검색하고 볼 수 있도록 하는 Privacy Manager Chat 구성 요소

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

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

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

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

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

보안 로그온 방법. 컴퓨터에 로그인할 때 사용하는 방법

블리치. free space bleaching(여유 공간 블리치)을 참조하십시오.

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

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

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

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

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

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

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

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

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

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

암호화. 특정인만 해독할 수 있도록 데이터를 암호화하고 해독하는 기법

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

여유 공간 블리치. 삭제된 자산의 내용을 일그러뜨려 데이터 복구를 더욱 어렵게 만들기 위해 하드 드라이브의 삭제된 자산 위에 임의의 데이터를 덮어쓰는 보안 작업

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

인증 기관. 공용 키 인프라를 실행하는 데 필요한 인증서를 발급하는 서비스

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

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

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

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

재부팅. 컴퓨터를 재시작하는 과정

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

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

토큰. 보안 로그온 방법 참조.

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

파쇄 프로필. 지정된 삭제 방법 및 자산 목록입니다.

파쇄. 자산이 있는 데이터를 손상시키는 알고리즘을 실행하는 것을 말합니다.

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

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

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

활성화. Drive Encryption 기능에 액세스하기 위해 반드시 완료해야 하는 작업. Drive Encryption 은 HP ProtectTools Security Manager for Administrators 설치 마법사를 통해 활성화됩니다. 관리자만이 Drive Encryption 을 활성화할 수 있습니다. 활성화 프로세스는 소프트웨어 활성화와 드라이브 암호화, 사용자 계정 생성, 이동식 저장 장치에 초기 백업 암호화 키 생성으로 구성됩니다.

색인