HP ProtectTools
사용 설명서

제 2 판: 2007 년 10 월

문서 부품 번호: 451271-AD2

목차

1 보안 소개

HP ProtectTools Security Manager 소프트웨어는 컴퓨터, 네트워크 및 중요 데이터에 대한 무단 액세스를 차단하는 보안 기능을 제공합니다. 고급 보안 기능을 제공하는 소프트웨어 모듈은 다음과 같습니다.

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

컴퓨터에서 사용할 수 있는 소프트웨어 모듈은 모델에 따라 다릅니다. 예를 들어, HP ProtectTools Embedded Security 를 사용하려면 TPM(Trusted Platform Module) 내장 보안 칩이 컴퓨터에 설치되어 있어야 합니다.

HP ProtectTools 소프트웨어 모듈은 사전 설치 또는 사전 로드되어 있거나 HP 웹 사이트에서 다운로드할 수 있습니다. HP Compaq Desktop 을 선택하면 애프터 마켓 옵션으로 HP ProtectTools 를 사용할 수 있습니다. 자세한 내용을 보려면 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 Credential Manager	• 개인 암호 저장소 역할을 하는 인증서 관리자는 SSO(single sign on) 기능을 제공하고 사용자가 암호 이외에도 사용자 인증을 위한 보다 엄격한 보안을 정의하고 배포할 수 있도록 합니다. • 저장된 암호는 암호화를 통해 보호되며 TPM 내장 보안 칩을 통해 더욱 보강될 수 있습니다. • Single Sign On 기능 이외에도 인증서 관리자는 암호를 사용하는 사용자 인증을 위해 Java™ 카드 또는 생체 인식과 같이 다양한 보안 인증 기술을 함께 사용할 수 있는 기능을 제공합니다.
HP ProtectTools Embedded Security	• 내장 보안은 보안 사용자 및 관리자 옵션을 관리하여 EFS (Windows Encrypting File System)와 같이 로컬 컴퓨터에서 TPM 기술을 사용하는 다양한 암호화 키를 보호합니다. PSD (Personal Secure Drive) 및 타사 디지털 인증서가 이에 해당합니다. • 내장 보안은 TPM(Trusted Platform Module) 내장 보안 칩을 사용하여 기밀 사용자 데이터 또는 PC 에 로컬로 저장된 인증서에 무단으로 액세스 하는 것을 방지합니다. TPM 은 암호화 키에 대한 보안 저장 및 키 생성 기능을 제공합니다. 또한 암호 공격에 대비하여 강력한 방어 기능을 제공합니다. • 사용자 데이터 보호를 위해 내장 보안을 사용하여 시스템에서 데이터를 볼 수 없게 하는 가상 드라이브인 PSD(personal secure drive)를 만들 수 있습니다. • Embedded Security 는 보안 디지털 인증서 작업에 타사 응용프로그램(예: Microsoft Outlook, Internet Explorer)을 사용하도록 지원합니다.
HP ProtectTools Java Card Security	• 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. • 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.
HP ProtectTools BIOS Configuration	• BIOS Configuration 을 통해 사용자 및 관리자의 파워온 암호 관리에 액세스할 수 있습니다. • BIOS Configuration 은 부팅 전 BIOS Configuration 유틸리티인 F10 Setup 을 대신합니다.

모듈	주요 기능
HP ProtectTools Drive Encryption	• Drive Encryption 모듈은 하드 드라이브의 볼륨 전체를 완벽하게 암호화합니다. • 드라이브 암호화는 사전 부팅 인증을 사용하여 암호를 해독하고 데이터에 액세스합니다. • 드라이브 암호화는 파티션, 하드 드라이브 및 멀티 하드 드라이브를 암호하는 데 사용하는 인증 관리 도구를 제공합니다.
Device Access Manager for HP ProtectTools	• 장치 액세스 관리자는 데이터 저장소 및 전송 하드웨어(USB, COM & LPT 포트, 개인 음악 플레이어, CD 드라이브, 네트워크 인터페이스 카드 등)를 개인적으로 관리할 수 있도록 합니다. • 또한 장치 액세스 관리자는 사용자 및 사용자 그룹이 하드웨어에서 읽고 쓰거나 데이터에 액세스하는 권한을 허용 또는 거부할 수 있도록 관리할 수 있습니다.

HP ProtectTools 보안 액세스

Windows® 제어판에서 HP ProtectTools 보안에 액세스하려면 다음과 같이 하십시오.

- **시작 > 모든 프로그램 > HP ProtectTools Security Manager**(또는 Windows Vista 의 경우 **HP ProtectTools Security Manager for Administrators**)를 선택합니다.

주: Credential Manager 모듈을 구성한 후에는 Windows 로그온 화면에서 직접 Credential Manager 에 로그온하여 HP ProtectTools 를 열 수도 있습니다. 자세한 내용은 “15페이지의 인증서 관리자로 Windows 에 로그온”을 참조하십시오.

Windows Vista 의 경우 관리자는 드라이브 암호화에 액세스할 때 반드시 “HP ProtectTools Security Manager for Administrators”를 사용해야 합니다.

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 생성 및 사용

계획된 절도에 대한 대비

이런 사건의 예로 밀폐된 공간이나 개방된 환경에서 기밀 데이터 및 고객 정보가 담긴 컴퓨터를 계획적으로 절도하려는 경우를 들 수 있습니다. 다음 기능은 계획된 절도를 예방하는 데 도움이 됩니다.

- 부팅 전 인증 기능을 활성화하면 운영체제에 대한 액세스 차단에 도움이 됩니다. 다음 절차를 참조하십시오.
  - “32페이지의 Java Card 이름 할당”
  - “41페이지의 HP ProtectTools Device Access Manager”
  - “46페이지의 HP ProtectTools Drive Encryption”
- DriveLock 은 하드 드라이브를 분리하여 보안 장치가 없는 시스템에 설치하더라도 데이터에 액세스할 수 없도록 합니다. “38페이지의 보안”을 참조하십시오.
- 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 “25페이지의 설정 절차”
  - “27페이지의 개인 보안 드라이브 사용”

중요 데이터에 대한 액세스 제한

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

- IT 관리자는 HP ProtectTools Device Access Manager 를 사용하여 쓰기 가능 장치에 대한 액세스를 제한함으로써 하드 드라이브의 중요 정보를 이동식 미디어로 복사하거나 인쇄하지 못하도록 할 수 있습니다. “44페이지의 장치 클래스 구성(고급)”을 참조하십시오.
- DriveLock 은 하드 드라이브를 분리하여 보안 장치가 없는 시스템에 설치하더라도 데이터에 액세스할 수 없도록 합니다. “38페이지의 보안”을 참조하십시오.

내부 또는 외부에서 들어오는 무단 액세스 차단

내부 또는 외부에서 기밀 데이터 및 고객 정보가 들어 있는 PC 에 액세스할 수 있다면 권한이 없는 사용자들이 기업 네트워크 리소스에 침입하거나 재무 서비스, 중역 또는 R&D 팀의 데이터에 접근할 수 있습니다. 다음 기능은 무단 액세스를 차단하는 데 도움이 됩니다.

- 부팅 전 인증 기능을 활성화하면 운영체제에 대한 액세스 차단에 도움이 됩니다. 다음 절차를 참조하십시오.
  - "32페이지의 Java Card 이름 할당"
  - "46페이지의 HP ProtectTools Drive Encryption"
- HP ProtectTools Embedded Security 는 다음과 같은 절차를 통해 PC 에 로컬 저장된 인증서 또는 중요한 사용자 데이터를 보호합니다.
  - Embedded Security "25페이지의 설정 절차"
  - "27페이지의 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 "12페이지의 설정 절차"
  - "16페이지의 Single Sign On 사용"
- IT 관리자는 HP ProtectTools Device Access Manager 를 사용하여 쓰기 가능 장치에 대한 액세스를 제한함으로써 하드 드라이브의 중요 정보를 복사하지 못하도록 합니다. 43페이지의 기본 구성을 참조하십시오.
- PSD(개인 보안 드라이브) 기능은 다음 절차에 따라 중요한 데이터를 암호화하여 인증 없이는 액세스하지 못하도록 합니다.
  - Embedded Security "25페이지의 설정 절차"
  - "27페이지의 개인 보안 드라이브 사용"

강력한 암호 생성 및 사용

웹 사이트 또는 보안 응용프로그램에 액세스하려면 일반적으로 암호가 필요합니다. 이때 사용자는 이렇게 무수한 응용프로그램 및 웹 사이트에 아주 간단한 암호를 사용하려 하거나, 설사 복잡하고 독특한 암호를 만든다 하더라도 각 응용프로그램에 해당하는 암호를 제대로 구분하여 기억하지 못하는 경향이 있습니다. Credential Manager for HP ProtectTools 는 다음 절차에 따라 암호 및 Single Sign On 기능에 대한 보안 저장소를 제공합니다.

- 8페이지의 보안 암호 만들기
- Credential Manager "12페이지의 설정 절차"
- "16페이지의 Single Sign On 사용"

보다 강력한 보안을 원하는 경우, HP ProtectTools Embedded Security 로 사용자 이름 및 암호 저장소를 보호합니다. 이로써 사용자들은 여러 개의 강력한 암호를 일일이 기억하거나 적어놓지 않고도 관리할 수 있게 됩니다. Embedded Security "25페이지의 설정 절차"를 참조하십시오.

추가 보안 요소

보안 역할 할당

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

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

HP ProtectTools 에서는 보안 책임과 권한이 다음과 같은 역할로 구분됩니다.

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

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

- 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.
소유자 암호	Embedded Security, IT 관리자가 설정	Embedded Security 의 모든 소유자 기능에 대한 무단 액세스를 차단하여 시스템 및 TMP 칩을 보호합니다.

HP ProtectTools 암호	HP ProtectTools 모듈에서 설정	기능
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 Setup 또는 Security Setup 암호라고도 합니다.	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 Backup and Restore

HP ProtectTools Backup and Restore 는 지원되는 모든 HP ProtectTools 모듈에서 간편하고 빠른 인증 번호 백업 및 복원 방법을 제공합니다.

인증 정보 및 설정 백업

다음과 같이 인증 정보를 백업할 수 있습니다.

- HP ProtectTools Backup Wizard(HP ProtectTools 백업 마법사)를 사용하여 HP ProtectTools 모듈을 선택하고 백업
- 미리 선택한 HP ProtectTools 모듈을 백업

주: 이 방법을 사용하려면 먼저 백업 옵션을 설정해야 합니다.

- 백업 예약

주: 이 방법을 사용하려면 먼저 백업 옵션을 설정해야 합니다.

HP ProtectTools Backup Wizard(HP ProtectTools 백업 마법사)를 사용하여 HP ProtectTools 모듈을 선택하고 백업

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **HP ProtectTools** 를 누른 다음 **Backup and Restore**(백업 및 복원)를 누릅니다.
3. 오른쪽 창에서 **Backup Options**(백업 옵션)를 누릅니다. HP ProtectTools Backup Wizard(HP ProtectTools 백업 마법사)가 열립니다. 화면에 나타나는 지침에 따라 인증 정보를 백업합니다.

백업 옵션 설정

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **HP ProtectTools** 를 누른 다음 **Backup and Restore**(백업 및 복원)를 누릅니다.
3. 오른쪽 창에서 **Backup Options**(백업 옵션)를 누릅니다. HP ProtectTools Backup Wizard(HP ProtectTools 백업 마법사)가 열립니다.
4. 화면 지침을 따릅니다.
5. **Storage File Password**(저장 파일 암호)를 설정하고 확인한 뒤 **Remember all passwords and authentication values for future automated backups**(자동 백업을 위해 모든 암호 및 인증값 기억)를 선택합니다.
6. **Save Settings**(설정 저장)를 누르고 **Finish**(마침)를 누릅니다.

미리 선택한 HP ProtectTools 모듈을 백업

주: 이 방법을 사용하려면 먼저 백업 옵션을 설정해야 합니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **HP ProtectTools** 를 누른 다음 **Backup and Restore**(백업 및 복원)를 누릅니다.
3. 오른쪽 창에서 **Backup**(백업)을 누릅니다.

백업 예약

주: 이 방법을 사용하려면 먼저 백업 옵션을 설정해야 합니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **HP ProtectTools** 를 누른 다음 **Backup and Restore**(백업 및 복원)를 누릅니다.
3. 오른쪽 창에서 **Schedule Backups**(백업 예약)를 누릅니다.
4. **Task**(작업) 탭에서 **Enabled**(활성화) 확인란을 선택하여 예약 백업을 활성화합니다.

5. **Set Password**(암호 설정)를 누른 뒤 **Set Password**(암호 설정) 대화상자에 암호를 입력하고 확인합니다. **OK**(확인)를 누릅니다.

6. **Apply**(적용)를 누릅니다. **Schedule**(예약) 탭을 누릅니다. **Schedule Task**(작업 예약) 화살표를 누르고 자동 백업 주기를 선택합니다.

7. **Start time**(시작 시간)에서 **Start time**(시작 시간) 화살표를 사용하여 백업을 시작할 정확한 시간을 선택합니다.

8. **Advanced**(고급)를 누르고 시작 날짜, 종료 날짜, 반복 작업 설정 등을 선택합니다. **Apply**(적용)를 누릅니다.

9. **Settings**(설정)를 누르고 **Scheduled Task Completed**(예약 작업 완료), **Idle Time**(유휴 시간) 및 **Power Management**(전원 관리) 등의 설정을 선택합니다.

10. **Apply**(적용)를 누르고 **OK**(확인)를 눌러 대화상자를 닫습니다.

인증 정보 복구

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.

2. 왼쪽 창에서 **HP ProtectTools** 를 누른 다음 **Backup and Restore**(백업 및 복원)를 누릅니다.

3. 오른쪽 창에서 **Restore**(복원)를 누릅니다. HP ProtectTools Restore Wizard(HP ProtectTools 복원 마법사)가 열립니다. 화면 지침을 따릅니다.

설정 구성

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.

2. 왼쪽 창에서 **HP ProtectTools** 를 누른 다음 **Settings**(설정)를 누릅니다.

3. 오른쪽 창에서 원하는 설정을 선택하고 **OK**(확인)를 누릅니다.

2 HP ProtectTools Credential Manager

인증서 관리자는 사용자가 암호 이외에도 사용자 인증을 위한 보다 엄격한 보안을 정의하고 배포할 수 있도록 하며 SSO(single sign on) 기능을 제공하는 개인 암호 저장소 역할을 합니다. Credential Manager for HP ProtectTools 는 다음과 같은 보안 기능을 사용하여 사용자 컴퓨터에 대한 무단 액세스를 방지합니다.

- Windows 로그온 시 스마트 카드 또는 생체인식 리더 등을 사용하여 암호 대체. 자세한 내용은 "12페이지의 인증 정보 등록"을 참조하십시오.
- 웹 사이트, 응용프로그램, 보호되는 네트워크 자원에 대한 인증 정보를 자동 기억하는 Single Sign On 기능
- 스마트 카드 및 생체 인식 리더와 같은 선택 사양 보안 장치 지원
- 컴퓨터를 잠금 해제할 때 선택 사양 보안 장치를 통해 인증을 요구하는 등의 추가 보안 설정 지원

설정 절차

인증서 관리자에 로그온

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

- Credential Manager 로그온 마법사(권장)
- 알림 영역의 HP ProtectTools Security Manager 아이콘
- HP ProtectTools Security Manager

주: Windows 로그온 화면의 인증서 관리자 로그온 프롬프트를 사용하면 Windows 에도 동시에 로그온됩니다.

Credential Manager 를 처음 열 때는 기존 Windows 로그온 암호로 로그온합니다. 그러면 Windows 로그온 인증 정보를 바탕으로 Credential Manager 계정이 자동 생성됩니다.

Credential Manager 에 로그온한 후 지문이나 Java Card 와 같은 인증서를 추가로 등록할 수 있습니다. 자세한 내용은 “12페이지의 인증 정보 등록”을 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

인증서 관리자 로그온 마법사를 사용하여 인증서 관리자에 로그온하려면 다음 단계를 수행하십시오.

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** 아이콘을 두 번 눌러 엽니다.
   - ProtectTools Security Manager 의 “Credential Manager” 페이지에서 창 오른쪽 위에 있는 **Log On**(로그온) 링크를 눌러 엽니다.
2. 화면의 지침에 따라 Credential Manager 에 로그온합니다.

첫 로그온

시작에 앞서 관리자 계정으로 Windows 에 로그온해야 합니다. 이때 Credential Manager 에는 로그온하지 않습니다.

1. 알림 영역의 HP ProtectTools Security Manager 아이콘을 두 번 눌러 HP ProtectTools Security Manager 를 엽니다. HP ProtectTools Security Manager 창이 열립니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 오른쪽 창의 오른쪽 위에서 **Log On**(로그온)을 누릅니다. Credential Manager Logon Wizard(Credential Manager 로그온 마법사)가 열립니다.
3. **Password**(암호) 입력란에 Windows 암호를 입력하고 **Next**(다음)를 누릅니다.

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 통해 Windows 암호 대신 또는 이 암호와 함께 인증용 지문을 사용하여 Windows 에 로그온할 수 있습니다.

지문 인식기 설정

1. Credential Manager 에 로그온한 다음, 지문 인식기 위에 손가락을 통과시킵니다. Credential Manager Registration Wizard(Credential Manager 등록 마법사)가 열립니다.
2. 화면의 지침에 따라 지문 등록과 지문 인식기 설정을 완료합니다.
3. 다른 Windows 사용자에 대해 지문 인식기를 설정하려면 해당 사용자로 Windows 에 로그온한 후 1~2 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.

Java Card, USB eToken 또는 가상 토큰 등록

주: 이 과정을 진행하려면 카드 리더나 스마트 카드 키보드가 구성되어 있어야 합니다. 스마트 카드를 사용하지 않기로 선택한 경우 "14페이지의 가상 토큰 생성"에 설명된 가상 토큰을 등록할 수 있습니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
3. 오른쪽 창에서 **Register Smart Card or Token**(스마트 카드 또는 토큰 등록)을 누릅니다. Credential Manager Registration Wizard(Credential Manager 등록 마법사)가 열립니다.
4. 화면 지침을 따릅니다.

USB eToken 등록

1. USB eToken 드라이버가 설치되어 있는지 확인합니다.

   주: 자세한 내용은 USB eToken 사용 설명서를 참조하십시오.

2. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
3. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
4. 오른쪽 창에서 **Register Smart Card or Token**(스마트 카드 또는 토큰 등록)을 누릅니다. Credential Manager Registration Wizard(Credential Manager 등록 마법사)가 열립니다.
5. 화면 지침을 따릅니다.

기타 인증 정보 등록

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
3. 오른쪽 창에서 **Register Credentials**(인증 정보 등록)를 누릅니다. Credential Manager Registration Wizard(Credential Manager 등록 마법사)가 열립니다.
4. 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.

- 가상 토큰 생성
- Windows 로그온 암호 변경
- 토큰 PIN 관리
- ID 관리
- 컴퓨터 잠금

주: 이 옵션은 Credential Manager 클래식 로그온 프롬프트가 활성화된 경우에만 사용할 수 있습니다. 23페이지의 예 1 - “Advanced Settings(고급 설정)” 페이지를 사용하여 Credential Manager 에서 Windows 로그온 허용을 참조하십시오.

가상 토큰 생성

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

새 가상 토큰을 생성하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
3. 오른쪽 창에서 **Virtual Token**(가상 토큰)을 누릅니다. Credential Manager Registration Wizard (Credential Manager 등록 마법사)가 열립니다.

주: **Virtual Token**(가상 토큰) 옵션이 없으면 “13페이지의 기타 인증 정보 등록”의 절차를 사용하십시오.

4. 화면 지침을 따릅니다.

Windows 로그온 암호 변경

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
3. 오른쪽 창에서 **Change Windows Password**(Windows 암호 변경)를 누릅니다.
4. **Old Password**(이전 암호) 입력란에 기존 암호를 입력합니다.
5. **New password**(새 암호) 입력란에 새 암호를 입력하고 **Confirm password**(암호 확인) 입력란에 다시 입력합니다.
6. **Finish**(마침)를 누릅니다.

토큰 PIN 변경

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
3. 오른쪽 창에서 **Change Token PIN**(토큰 PIN 변경)을 누릅니다.

4. PIN 을 변경할 토큰을 선택한 다음 **Next**(다음)를 누릅니다.
5. 화면에 표시되는 지침에 따라 PIN 변경을 완료합니다.

ID 관리

시스템에서 ID 지우기

주: Windows 사용자 계정에는 영향을 미치지 않습니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
3. 오른쪽 창에서 **Clear Identity for this Account**(이 계정 ID 지우기)를 누릅니다.
4. 확인 대화상자에서 **Yes**(예)를 누릅니다. ID 가 로그오프된 다음 시스템에서 제거됩니다.

컴퓨터 잠금

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 클래식 로그온 프롬프트가 활성화된 경우에만 사용할 수 있습니다. 23페이지의 예 1 - "Advanced Settings(고급 설정)" 페이지를 사용하여 Credential Manager 에서 Windows 로그온 허용을 참조하십시오.

보안을 강화하려면 컴퓨터를 잠금 해제하는 데 Java Card, 생체 인식기, 토큰을 요구하도록 Lock Workstation(워크스테이션 잠금) 기능을 구성할 수 있습니다. 자세한 내용은 "22페이지의 Credential Manager 설정 구성"을 참조하십시오.

컴퓨터를 잠그려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누릅니다.
3. 오른쪽 창에서 **Lock Workstation**(워크스테이션 잠금)을 누릅니다. Windows 로그온 화면이 표시됩니다. 컴퓨터의 잠금을 해제하려면 Windows 암호나 Credential Manager Logon Wizard (Credential Manager 로그온 마법사)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.

인증서 관리자로 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 에 로그온할 수 있도록 지문을 등록하지 않은 경우, 지문 아이콘 옆의 화면 왼쪽 위에 있는 키보드 아이콘을 누릅니다. Credential Manager Logon Wizard(Credential Manager 로그온 마법사)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**(자세히) **> Wizard Options**(마법사 옵션)를 선택합니다.
   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.

계정 추가

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창에서 **Windows Logon**(Windows 로그온)을 누른 다음 **Add a Network Account**(네트워크 계정 추가)를 누릅니다. Add Network Account Wizard(네트워크 계정 추가 마법사)가 열립니다.
4. 화면 지침을 따릅니다.

계정 제거

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창에서 **Windows Logon**(Windows 로그온)을 누른 다음 **Manage Network Accounts**(네트워크 계정 관리)를 누릅니다. **Manage Network Accounts**(네트워크 계정 관리) 대화상자가 열립니다.
4. 제거할 계정을 누른 다음 **Remove**(제거)를 누릅니다.
5. 확인 대화상자에서 **Yes**(예)를 누릅니다.
6. **OK**(확인)를 누릅니다.

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 보안 사이트 또는 프로그램에 로그온하기 전에 Java Card, 지문 인식기, 토큰 등을 사용하여 인증 정보의 유효성을 검사하도록 Single Sign On 을 구성할 수 있습니다. 이 기능은 특히 은행 계좌 번호와 같은 개인 정보가 포함된 프로그램이나 웹 사이트에 로그온할 때 유용합니다. 자세한 내용은 22페이지의 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 대화상자에서 Credential Manager SSO 아이콘을 누릅니다.
3. 해당 프로그램 또는 웹 사이트의 암호를 입력하고 **OK(확인)**를 누릅니다. **Credential Manager Single Sign On** 대화상자가 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. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창에서 **Single Sign On** 을 누른 다음 **Register New Application**(새 응용프로그램 등록)을 누릅니다. SSO Application Wizard(SSO 응용프로그램 마법사)가 열립니다.
4. 화면 지침을 따릅니다.

응용프로그램 및 인증 정보 관리

응용프로그램 속성 수정

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **Single Sign On** 에서 **Manage Applications and Credentials**(응용프로그램 및 인증 정보 관리)를 누릅니다.
4. 수정할 응용프로그램 항목을 누른 다음 **Properties**(속성)를 누릅니다.
5. **General**(일반) 탭을 눌러 응용프로그램 이름과 설명을 수정합니다. 각 설정 옆에 있는 확인란을 선택하거나 선택 취소하여 설정을 적절히 변경합니다.
6. **Script**(스크립트) 탭을 눌러 SSO 응용프로그램 스크립트를 확인 및 편집합니다.
7. **OK**(확인)를 누릅니다.

Single Sign On 에서 응용프로그램 제거

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.

3. 오른쪽 창의 **Single Sign On** 에서 **Manage Applications and Credentials**(응용프로그램 및 인증 정보 관리)를 누릅니다.
4. 제거할 응용프로그램 항목을 누른 다음 **Remove**(제거)를 누릅니다.
5. 확인 대화상자에서 **Yes**(예)를 누릅니다.
6. **OK**(확인)를 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. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **Single Sign On** 에서 **Manage Applications and Credentials**(응용프로그램 및 인증 정보 관리)를 누릅니다.
4. 내보내려는 응용프로그램 항목을 누른 다음 **More**(자세히) **> Applications**(응용프로그램) **> Export Script**(스크립트 내보내기)를 누릅니다.
5. 화면 지침에 따라 내보내기를 완료합니다.
6. **OK**(확인)를 누릅니다.

응용프로그램 가져오기

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **Single Sign On** 에서 **Manage Applications and Credentials**(응용프로그램 및 인증 정보 관리)를 누릅니다.
4. 가져오려는 응용프로그램 항목을 누른 다음 **More**(자세히) **> Applications**(응용프로그램) **> Import Script**(스크립트 가져오기)를 선택합니다.
5. 화면 지침에 따라 가져오기를 완료합니다.
6. **OK**(확인)를 누릅니다.

인증 정보 수정

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **Single Sign On** 에서 **Manage Applications and Credentials**(응용프로그램 및 인증 정보 관리)를 누릅니다.
4. 수정할 응용프로그램 항목을 누른 다음 **More**(상세 정보)를 누릅니다.

5. 다음 옵션 중 하나를 선택합니다.
   - 응용프로그램
     - 새로 추가
     - 제거
     - 속성
     - 스크립트 가져오기
     - 스크립트 내보내기
   - 인증 정보
     - 새로 만들기
   - 암호 보기

   주: 암호를 보기 전에 ID 를 인증해야 합니다.
6. 화면 지침을 따릅니다.
7. **OK**(확인)를 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. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **Application Protection**(응용프로그램 보호) 아래에서 **Manage Protected Applications**(보호되는 응용프로그램 관리)를 누릅니다. **Application Protection Service**(응용프로그램 보호 서비스) 대화상자가 열립니다.
4. 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.
5. **Add**(추가)를 누릅니다. Add a Program Wizard(프로그램 추가 마법사)가 열립니다.
6. 화면 지침을 따릅니다.

응용프로그램에서 보호 제거

응용프로그램에서 제한을 제거하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **Application Protection**(응용프로그램 보호) 아래에서 **Manage Protected Applications**(보호되는 응용프로그램 관리)를 누릅니다. **Application Protection Service**(응용프로그램 보호 서비스) 대화상자가 열립니다.
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. **OK**(확인)를 누릅니다.

보호되는 응용프로그램에 대한 제한 설정 변경

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **Application Protection**(응용프로그램 보호) 아래에서 **Manage Protected Applications**(보호되는 응용프로그램 관리)를 누릅니다. **Application Protection Service**(응용프로그램 보호 서비스) 대화상자가 열립니다.
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. 변경할 응용프로그램을 누른 다음 **Properties**(속성)를 누릅니다. 해당 응용프로그램의 **Properties**(속성) 대화상자가 열립니다.
6. **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)
7. 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.
8. **OK**(확인)를 눌러 응용프로그램 **Properties**(속성) 대화상자를 닫습니다.
9. **OK**(확인)를 누릅니다.

고급 작업(관리자 전용)

Credential Manager 의 “Authentication and Credentials(인증 및 인증 정보)” 페이지와 “Advanced Settings(고급 설정)” 페이지는 관리자 권한이 있는 사용자만 사용할 수 있습니다. 이러한 페이지에서 다음과 같은 작업을 수행할 수 있습니다.

- 사용자와 관리자의 로그온 방법 지정
- 사용자 정의 인증 요구 사항 구성
- 인증 정보 속성 구성
- Credential Manager 설정 구성

사용자와 관리자의 로그온 방법 지정

“Authentication and Credentials(인증 및 인증 정보)” 페이지에서 사용자 또는 관리자에 필요한 인증 정보 유형 또는 조합을 지정할 수 있습니다.

사용자 또는 관리자의 로그온 방법을 지정하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창에서 **Authentication**(인증) 탭을 누릅니다.
4. 범주 목록에서 범주(**Users**(사용자) 또는 **Administrators**(관리자))를 누릅니다.
5. 목록에서 인증 방법 유형 또는 조합을 누릅니다.
6. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

사용자 정의 인증 요구 사항 구성

원하는 인증 정보 집합이 “Authentication and Credentials(인증 및 인증 정보)” 페이지의 인증 탭에 없는 경우 사용자 정의 요구 사항을 만들 수 있습니다.

사용자 정의 요구 사항을 구성하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창에서 **Authentication**(인증) 탭을 누릅니다.
4. 범주 목록에서 범주(**Users**(사용자) 또는 **Administrators**(관리자))를 누릅니다.
5. 인증 방법 목록에서 **Custom**(사용자 정의)을 누릅니다.
6. **Configure**(구성)를 누릅니다.
7. 사용할 인증 방법을 선택합니다.
8. 다음 중 하나를 눌러 방법 조합을 선택합니다.
   - Use AND to combine the authentication methods(AND 로 인증 방법 조합):

     (사용자는 로그온할 때마다 선택한 방법을 모두 사용하여 인증해야 합니다.)
   - Use OR to require one of two or more authentication methods(OR 로 두 가지 이상 인증 방법 중 한 가지 요구)

(사용자는 로그온할 때마다 선택한 방법 중 하나를 선택할 수 있습니다.)

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

인증 정보 속성 구성

"Authentication and Credentials(인증 및 인증 정보)" 페이지의 Credentials(인증 정보) 탭에서 사용 가능한 방법 목록을 확인하고 설정을 수정할 수 있습니다.

인증 정보를 구성하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Authentication and Credentials**(인증 및 인증 정보)를 누릅니다.
3. 오른쪽 창의 **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 대화상자에서 **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)" 페이지에서 다음 탭을 사용하여 다양한 설정에 액세스하고 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 대화상자로 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. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Settings**(설정)를 누릅니다.
3. 오른쪽 창에서 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. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Settings**(설정)를 누릅니다.
3. 오른쪽 창에서 **General**(일반) 탭을 누릅니다.
4. **Select the way users log on to Windows**(Windows 에 로그온하는 방법 선택)(재시작 필요) 아래에서 **Use Credential Manager with classic logon prompt**(클래식 로그온 프롬프트와 함께 Credential Manager 사용) 확인란을 선택합니다.
5. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.
6. 컴퓨터를 재시작합니다.

주: **Use Credential Manager with classic logon prompt**(클래식 로그온 프롬프트와 함께 Credential Manager 사용) 확인란을 선택하면 사용자가 컴퓨터를 잠글 수 있습니다. 15페이지의 컴퓨터 잠금을 참조하십시오.

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

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Credential Manager** 를 누른 다음 **Settings**(설정)를 누릅니다.
3. 오른쪽 창에서 **Single Sign On** 탭을 누릅니다.
4. **When registered logon dialog or Web page is visited**(등록된 로그온 대화상자 또는 웹 페이지를 방문할 때)에서 **Authenticate user before submitting credentials**(인증 정보 제출 전에 사용자 인증) 확인란을 선택합니다.
5. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.
6. 컴퓨터를 재시작합니다.

3 HP ProtectTools Embedded Security

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(Encrypting File System) 파일 및 폴더 암호화 강화
- 숨겨진 드라이브에서 사용자 데이터 보호를 위한 PSD(personal secure drive) 생성
- 키 계층 백업 및 복원 등의 데이터 관리 기능
- Embedded Security 소프트웨어를 사용할 때 보안 디지털 인증서 작업에 타사 응용프로그램(예: Microsoft Outlook, Internet Explorer) 지원

TPM 내장 보안 칩은 HP ProtectTools Security Manager 의 기능을 강화할 뿐만 아니라 더욱 다양한 기능을 사용할 수 있게 해줍니다. 예를 들어, Credential Manager for HP ProtectTools 는 사용자가 Windows 에 로그온할 때 내장 칩을 인증 요소의 하나로 사용할 수 있습니다. 선택 모델에서는 TPM 내장 보안 칩이 BIOS Configuration for HP ProtectTools 을 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.

내장 보안 칩 활성화

내장 보안 칩은 Computer Setup 유틸리티에서 활성화해야 합니다. 이 절차는 HP ProtectTools BIOS Configuration 에서 수행할 수 없습니다.

내장 보안 칩을 활성화하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 다시 시작한 후 화면 왼쪽 하단에 **F10 = ROM Based Setup** 메시지가 나타나면 F10 키를 눌러 Computer Setup 에 액세스합니다.
2. 관리자 암호를 설정하지 않은 경우 화살표 키를 사용하여 **Security > Setup password** 를 선택한 다음 Enter 키를 누릅니다.
3. **New password** 및 **Verify new password** 상자에 암호를 입력한 다음 F10 키를 누릅니다.
4. **Security** 메뉴에서 화살표 키를 사용하여 **TPM Embedded Security** 를 선택한 다음 Enter 키를 누릅니다.
5. **Embedded Security** 에서 장치가 숨김 상태인 경우 **Available** 을 선택합니다.
6. **Embedded security device state** 를 선택하고 **Enable** 로 변경하십시오.
7. F10 키를 눌러 Embedded Security 구성 변경을 수락합니다.
8. 기본 설정을 저장하고 Computer Setup 을 종료하려면 화살표 키를 사용하여 **File > Save Changes and Exit** 를 선택합니다. 그런 다음 화면의 지시를 따르십시오.

내장 보안 칩 초기화

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

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

내장 보안 칩을 초기화하려면 다음과 같이 하십시오.

1. 작업 표시줄의 오른쪽 끝에 있는 알림 영역에서 HP ProtectTools Security Manager 아이콘을 마우스 오른쪽 버튼으로 누른 후 **Embedded Security Initialization**(Embedded Security 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 **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
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 온라인 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.

- Windows 에 있는 파일 및 폴더만 암호화할 수 있습니다. MS—DOS 파티션의 파일 및 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. **OK**(확인)를 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 온라인 도움말 및 해당 전자 우편의 온라인 도움말을 참조하십시오.

기본 사용자 키 암호 변경

기본 사용자 키 암호를 변경하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
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. **OK**(확인)를 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 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Backup**(백업)을 누릅니다.
3. 오른쪽 창에서 **Backup**(백업)을 누릅니다. Embedded Security 백업 마법사가 열립니다.
4. 화면 지침을 따릅니다.

백업 파일에서 인증서 데이터 복원

백업 파일에서 데이터를 복원하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Embedded Security** 를 누른 다음 **Backup**(백업)을 누릅니다.
3. 오른쪽 창에서 **Restore**(복원)를 누릅니다. Embedded Security 백업 마법사가 열립니다.
4. 화면 지침을 따릅니다.

소유자 암호 변경

소유자 암호를 변경하려면 다음과 같이 하십시오.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
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. **OK**(확인)를 누릅니다.

사용자 암호 재설정

관리자는 사용자가 잊은 암호를 재설정하도록 지원할 수 있습니다. 자세한 내용은 온라인 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 > HP ProtectTools Security Manager** 를 선택합니다.
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 > HP ProtectTools Security Manager** 를 선택합니다.
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 온라인 도움말을 참조하십시오.

4 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. **시작 > 모든 프로그램 > 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. **시작 > 모든 프로그램 > 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. **시작 > 모든 프로그램 > 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. **시작 > 모든 프로그램 > 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. **시작 > 모든 프로그램 > 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 "8페이지의 HP ProtectTools Backup and Restore"를 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. **시작 > 모든 프로그램 > 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. **시작 > 모든 프로그램 > 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.

5 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 사용할 수 있습니다. F10 Setup 사용에 대한 자세한 지침은 컴퓨터 또는 BIOS 업데이트에 들어 있는 Computer Setup (F10) 유틸리티 설명서를 참조하십시오.

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.

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)

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)

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)

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)
- AMT Options(AMT 옵션)

6 HP ProtectTools Device Access Manager

이 보안 도구는 관리자만 사용할 수 있습니다. 장치 액세스 관리자를 사용하면 데이터 저장 장치 및 전송 하드웨어(USB, COM & LPT 포트, 개인 음악 플레이어, CD 드라이브, 네트워크 인터페이스 카드 등)를 사용자 정의에 맞게 관리할 수 있습니다. 또한 사용자 및 사용자 그룹이 하드웨어에서 읽고 쓰거나 데이터에 액세스하는 권한을 허용 또는 거부할 수 있도록 관리할 수도 있습니다.

백그라운드 서비스 시작

장치 프로필을 적용하려면 HP ProtectTools Device Locking/Auditing 백그라운드 서비스를 실행해야 합니다. 처음으로 장치 프로필을 적용하려고 하면 HP ProtectTools Security Manager 에서 백그라운드 서비스 시작 여부를 묻는 대화상자가 열립니다. 백그라운드 서비스를 시작하려면 **예**를 클릭하고 시스템이 부팅할 때마다 자동으로 시작되도록 설정합니다.

기본 구성

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

- 관리자 외의 모든 사용자에 대한 모든 이동식 미디어(플로피 디스크, 펜 드라이브, USB 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 모든 Bluetooth, 적외선, 모뎀, PCMCIA, 개인 음악 플레이어 및 모든 1394(FireWire) 장치의 액세스 거부

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

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
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. 일부 클래스에서는 읽기 전용 또는 쓰기 액세스를 구성하는 옵션을 허용합니다.

사용자 또는 그룹 추가

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
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) **> Find Now**(지금 찾기)를 선택하여 추가할 사용자 또는 그룹을 검색합니다.
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 > HP ProtectTools Security Manager** 를 선택합니다.
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 > HP ProtectTools Security Manager** 를 선택합니다.
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.

특정 그룹의 한 사용자에 대해 장치 클래스에 대한 액세스 허용

특정 그룹의 한 사용자에게만 장치에 대한 액세스를 허용하고 그 그룹의 나머지 사용자에 대해서는 액세스를 거부할 수 있습니다.

그룹의 한 사용자에 대해서만 액세스를 허용하려면 다음과 같이 합니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
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) 아래에서 액세스를 거부할 그룹을 추가합니다.
5. 액세스를 거부할 그룹 옆에 있는 **Deny**(거부)를 누릅니다.
6. 해당 클래스 아래의 폴더로 이동한 후 특정 사용자를 추가합니다. **Allow**(허용)를 눌러 해당 사용자에게 액세스 권한을 부여합니다.
7. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

그룹의 한 사용자에 대해 특정 장치에 대한 액세스 허용

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

특정 장치에 대해 그룹의 한 사용자에게만 액세스를 허용하려면 다음과 같이 합니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Device Access Manager** 를 누른 다음 **Device Class Configuration**(장치 클래스 구성)을 누릅니다.
3. 장치 목록에서 구성할 장치 클래스를 누른 다음 그 아래의 폴더로 이동합니다.
4. **User/Groups**(사용자/그룹) 아래에서 액세스를 거부할 그룹을 추가합니다.
5. 액세스를 거부할 그룹 옆에 있는 **Deny**(거부)를 누릅니다.
6. 장치 목록에서 사용자에게 액세스를 허용할 특정 장치로 이동합니다.
7. **Add**(추가)를 누릅니다. **Select Users or Groups**(사용자 또는 그룹 선택) 대화 상자가 열립니다.
8. **Advanced**(고급) **> Find Now**(지금 찾기)를 선택하여 추가할 사용자 또는 그룹을 검색합니다.
9. 액세스를 허용할 사용자를 누른 다음 **OK**(확인)를 누릅니다.
10. **Allow**(허용)를 눌러 해당 사용자에게 액세스 권한을 부여합니다.
11. **Apply**(적용), **OK**(확인)를 차례로 누릅니다.

7 HP ProtectTools Drive Encryption

Drive encryption for HP ProtectTools 는 단일 하드 드라이브, 파티션 또는 멀티 하드 드라이브의 모든 정보를 암호화하므로 권한이 없는 사용자가 읽을 수 없습니다.

△ **주의:** 설치한 Drive Encryption 모듈을 제거하려면 암호화된 모든 드라이브의 암호를 해독해야 합니다. 암호를 해독하지 않을 경우 Drive Encryption 복구 서비스에 등록하기 전에는 암호화된 드라이브의 데이터를 액세스할 수 없습니다. 자세한 내용은 “49페이지의 복구”를 참조하십시오. Drive Encryption 모듈을 다시 설치해도 암호화된 드라이브에 액세스할 수 없습니다.

암호화 관리

드라이브 암호화

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **Encryption Management**(암호화 관리)를 누릅니다.
3. 오른쪽 창에서 **Activate**(활성화)를 누릅니다. HP ProtectTools Drive Encryption 마법사가 열립니다.
4. 화면 지침을 따라 암호화를 활성화합니다.

주: 복구 정보를 저장할 디스켓, 플래시 저장 장치 또는 다른 USB 연결 저장 미디어를 지정해야 합니다.

암호화 변경

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **Encryption Management**(암호화 관리)를 누릅니다.
3. 오른쪽 창에서 **Change encryption**(암호화 변경)을 누릅니다. **Change Encryption**(암호화 변경) 대화상자에서 암호화할 디스크를 선택하고 **OK**(확인)를 누릅니다.
4. **OK**(확인)를 다시 눌러 암호화를 시작합니다.

드라이브 암호 해독

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **Encryption Management**(암호화 관리)를 누릅니다.
3. 오른쪽 창에서 **Deactivate**(암호 해독)를 누릅니다.

사용자 관리 기능이 있습니다

사용자 추가

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **User Management**(사용자 관리)를 누릅니다.
3. 오른쪽 창에서 **Add**(추가)를 누릅니다. **User Name**(사용자 이름) 목록에서 사용자 이름을 누르거나 **Username**(사용자 이름) 상자에 사용자 이름을 입력합니다. **Next**(다음)를 누릅니다.
4. 선택한 사용자의 Windows 암호를 입력하고 **Next**(다음)를 누릅니다.
5. 새 사용자에 대한 인증 방법을 선택하고 **Finish**(마침)를 누릅니다.

사용자 제거

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **User Management**(사용자 관리)를 누릅니다.
3. 오른쪽 창의 **User Name**(사용자 이름) 목록에서 제거할 사용자 이름을 누릅니다. **Remove**(제거)를 누릅니다.
4. **Yes**(예)를 눌러 선택한 사용자를 제거할 것인지 확인합니다.

토큰 변경

사용자에 대한 인증 방법을 다음과 같이 변경합니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **User Management**(사용자 관리)를 누릅니다.
3. 오른쪽 창의 **User Name**(사용자 이름) 목록에서 사용자 이름을 선택하고 **Change Token**(토큰 변경)을 누릅니다.
4. 사용자의 Windows 암호를 입력하고 **Next**(다음)를 누릅니다.
5. 새 인증 방법을 선택하고 **Finish**(마침)를 누릅니다.
6. 인증 방법으로 Java Card 를 선택한 경우 Java Card 암호를 묻는 메시지가 표시되면 암호를 입력하고 **OK**(확인)를 누릅니다.

암호 설정

다음과 같이 암호를 설정하거나 사용자에 대한 인증 방법을 변경합니다.

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **User Management**(사용자 관리)를 누릅니다.
3. 오른쪽 창의 **User Name**(사용자 이름) 목록에서 사용자를 선택하고 **Set Password**(암호 설정)를 누릅니다.
4. 사용자의 Windows 암호를 입력하고 **Next**(다음)를 누릅니다.
5. 새 인증 방법을 선택하고 **Finish**(마침)를 누릅니다.
6. 인증 방법으로 Java Card 를 선택한 경우 Java Card 암호를 묻는 메시지가 표시되면 암호를 입력하고 **OK**(확인)를 누릅니다.

복구

다음 두 가지 안전 장치를 사용할 수 있습니다.

- 암호를 잊으면 암호화된 드라이브에 액세스할 수 없습니다. 그러나 이 경우, Drive Encryption 복구 서비스에 등록하여 컴퓨터에 액세스할 수 있습니다.
- 드라이브 암호화 키를 디스켓, 플래시 저장 장치 또는 다른 USB 연결 저장 미디어에 백업할 수 있습니다.

Drive Encryption 복구 서비스 등록

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **Recovery**(복구)를 누릅니다.
3. 오른쪽 창에서 **Click here to register**(여기를 눌러 등록)를 누릅니다. 요청된 정보를 입력하여 보안 백업 절차를 완료합니다.

드라이브 암호화 키 백업

1. **시작 > 모든 프로그램 > HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **Drive Encryption** 을 누른 다음 **Recovery**(복구)를 누릅니다.
3. 오른쪽 창에서 **Click here to backup your keys**(여기를 눌러 키 백업)를 누릅니다.
4. 복구 정보를 저장할 디스켓, 플래시 저장 장치 또는 다른 USB 연결 저장 미디어를 선택하고 **Next**(다음)를 누릅니다. HP ProtectTools Drive Encryption 마법사가 열립니다.
5. 화면 지침을 따라 드라이브 암호화 키를 백업합니다.

주: 복구 정보를 저장할 디스켓, 플래시 저장 장치 또는 다른 USB 연결 저장 미디어를 지정해야 합니다.

8 문제 해결

Credential Manager for HP ProtectTools

증상	설명	해결 방법
사용자가 인증서 관리자 네트워크 계정 옵션을 사용하여 로그인할 도메인 계정을 선택할 수 있는데, TPM 인증을 사용하는 경우 이 옵션을 사용할 수 없음. 다른 인증 방법은 모두 제대로 작동함.	TPM 인증을 사용하면 사용자는 로컬 컴퓨터에만 로그인됩니다.	Credential Manager Single Sign On 도구를 사용하면 사용자가 다른 계정도 인증할 수 있습니다.
Windows XP 서비스 팩 1 에 로그인할 때 USB 토큰 인증서를 사용할 수 없음.	USB 토큰 소프트웨어를 설치하고 USB 토큰 인증서를 등록한 다음 인증서 관리자를 기본 로그인으로 설정했지만 USB 토큰이 인증서 관리자/GINA 로그온 목록에 나타나지 않거나 사용할 수 없습니다. Windows 로 다시 로그인할 때 인증서 관리자에서 로그오프했다가 다시 로그인하고 토큰을 기본 로그인으로 다시 선택하면 토큰 로그인이 정상적으로 작동합니다.	Windows XP 서비스 팩 1 에서만 이러한 현상이 나타납니다. Windows Update 를 통해 Windows 버전을 서비스 팩 2 로 업데이트하십시오. 서비스 팩 1 에서 문제를 해결하려면 다른 자격 증명(Windows 암호)을 사용하여 Windows 에 다시 로그인한 다음, 인증서 관리자에서 로그오프했다가 다시 로그인하십시오.
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 일부 소프트웨어 웹 인터페이스를 지원하지 않습니다. SSO 지원 기능을 해제하여 특정 웹 페이지에 대한 SSO 지원을 비활성화하십시오. 인증서 관리자 도움말 파일에서 SSO 에 대한 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.
로그인 프로세스에서 **Browse for Virtual Token**(가상 토큰 탐색) 옵션이 제공되지 않음.	이 탐색 옵션은 보안상의 문제로 제거되었으므로 사용자가 인증서 관리자에 등록된 가상 토큰의 위치를 이동할 수 없습니다.	무단 사용자가 이 탐색 옵션을 사용하여 파일을 삭제하고, 이름을 변경하며, Windows 를 제어할 수 있으므로 현재 제공되는 제품에서는 이 옵션이 제거되었습니다.
TPM 인증으로 로그인할 경우 **Network Accounts**(네트워크 계정) 옵션이 제공되지 않음.	**Network Accounts**(네트워크 계정) 옵션을 사용하면 로그인할 도메인 계정을 사용자가 선택할 수 있습니다. TPM 인증을 사용하는 경우 이 옵션을 사용할 수 없습니다.	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
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 인증서 관리자에서 도메인 ID 를 등록한 경우 발생합니다. 도메인 관리자가 인증서 관리자에서 Windows 암호를 변경하려고 하면 **User account restriction**(사용자	인증서 관리자는 **Change Windows password** (Windows 암호 변경)를 통해 도메인 사용자 계정 암호를 변경할 수 없으며, 로컬 PC 계정 암호만 변경할 수 있습니다. 도메인 사용자는 **Windows 보안 > 암호 변경** 옵션을 통해서 암호를 변경할 수 있습니다. 하지만 로컬 PC 에 물리적 계정을 가지고 있지 않으므로 인증서 관리자에서는 로그인에 사용되는 암호만을 변경할 수 있습니다.

증상	설명	해결 방법
	계정 제한)이라는 로그온 실패 오류 메시지가 나타납니다.	
반복을 방지하기 위해 인증서 관리자 SSO 기본 설정을 프롬프트로 설정해야 함	SSO 기본 설정은 사용자를 자동으로 기록하는 것입니다. 하지만 암호로 보호되는 문서를 작성할 때 첫 번째 문서를 작성하고 두 번째 문서를 작성할 경우 인증서 관리자는 마지막으로 기록된 암호 즉, 첫 번째 문서의 암호를 사용합니다.	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
Corel WordPerfect 12 암호 GINA 와 관련한 비호환성 문제.	인증서 관리자에 로그인하여 WordPerfect 에서 문서를 작성한 후 암호로 보호되는 문서로 저장한 경우 인증서 관리자는 암호 GINA 를 수동 또는 자동으로 찾아내거나 알아낼 수 없습니다.	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
인증서 관리자가 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.
ATI Catalyst 구성 마법사를 인증서 관리자와 함께 사용할 수 없음.	인증서 관리자 SSO 가 ATI Catalyst 구성 마법사와 충돌합니다.	인증서 관리자 SSO 를 비활성화하십시오.
TPM 인증으로 로그인할 때 화면의 **Back**(뒤로) 버튼을 누르면 다른 인증 방법을 선택하는 옵션을 건너뜀.	인증서 관리자에 대해 TPM 로그인 인증을 사용하는 사용자가 암호를 입력하는 경우 **Back**(뒤로) 버튼이 제대로 작동하지 않고 Windows 로그인 화면이 바로 표시됩니다.	HP 에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
인증서 관리자가 구성과는 다르게 대기 상태가 해제될 때 자동으로 실행됨	**use Credential Manager log on to Windows**(Windows 에 인증서 관리자 로그온 사용)를 옵션으로 선택하지 않았는데, 시스템이 S3 일시 정지 모드로 들어간 후 작업을 재개하면 Windows 에 인증서 관리자 로그온이 실행됩니다.	관리자 암호를 설정하지 않으면 인증서 관리자의 계정 제한 기능으로 인해 사용자가 인증서 관리자를 통해 Windows 에 로그온할 수 없습니다. • Java 카드/토큰이 없는 경우 인증서 관리자 로그인을 취소하면 Microsoft Windows 로그인이 나타납니다. 이때 로그인할 수 있습니다. • Java 카드/토큰을 사용하면 다음 문제 해결 방법을 통해 Java 카드 삽입 후 인증서 관리자 열기를 활성화/비활성화할 수 있습니다. 1. **Advanced Settings**(고급 설정)를 누릅니다. 2. **Service & Applications**(서비스 및 응용프로그램)를 누릅니다. 3. **Java Cards and Tokens**(Java 카드 및 토큰)를 누릅니다. 4. **when Java Card/token is inserted**(Java 카드/토큰 삽입 시)를 누릅니다. 5. **Advise to log-on**(로그온 메시지 표시) 확인란을 선택합니다.
TPM 모듈이 제거되거나 손상된 경우 TPM 으로 보호되는 인증서 관리자의 모든 인증서가 소실됨.	TPM 모듈이 제거되거나 손상된 경우 TPM 으로 보호되는 인증서 관리자의 모든 인증서가 소실됩니다.	이는 설계상의 이유입니다. TPM 모듈은 인증서 관리자의 인증서를 보호하도록 설계되었습니다. TPM 모듈을 제거하기 전에 인증서 관리자에서 ID 를 백업하도록 하십시오.
인증서 관리자가 Windows 2000 에서 기본 로그온으로 설정되지 않음.	Windows 2000 설치 과정에서 로그온 정책이 수동 또는 자동 로그온 관리로 설정됩니다. 자동 로그온이 선택된 경우 Windows 기본 레지스트리 설정에 따라 기본 자동 관리 로그온 값인 1 로 설정되	이는 설계상의 이유입니다. 입력 생략을 위한 자동 관리 로그온 값에 대한 운영체제 수준 설정을 수정하려는 경우 HKEY_LOCAL_MACHINE/Software/Microsoft/

증상	설명	해결 방법
	며 인증서 관리자 설정보다 이 설정이 우선합니다.	WindowsNT/CurrentVersion/WinLogon 에서 수정할 수 있습니다. **주의:** 레지스트리 편집기 사용에 따른 위험은 직접 책임져야 하므로 신중한 주의를 기울여야 합니다. 레지스트리 편집기(regedit)를 잘못 사용하면 심각한 문제가 발생하여 운영체제를 다시 설치해야 할 수 있습니다. 레지스트리 편집기를 잘못 사용하여 발생하는 문제는 반드시 해결할 수 있다는 보장이 없습니다.
지문 인식기 설치 및 등록 여부에 관계없이 지문 로그온 메시지가 나타남.	Windows 로그온을 선택하면 **You can place your finger on the fingerprint reader to log on to Credential Manager(지문 인식기에 손가락을 접촉하여 인증서 관리자에 로그온할 수 있습니다)라는 알림 메시지가 인증서 관리자 작업 표시줄에 나타납니다.**	이 알림 메시지는 지문 인증이 구성된 경우 이를 사용할 수 있다는 사실을 사용자에게 알리기 위한 것입니다.
리더가 장착되지 않은 경우 Windows 2000 에 대한 인증서 관리자 로그온 창에서 **insert card(카드 삽입)** 메시지가 표시됨.	Windows Credential Manager 시작 화면에, 장착된 Java 카드 리더가 없는 경우 **insert card(카드 삽입)**을 사용하여 로그온할 수 있다는 메시지가 표시됩니다.	이 알림 메시지는 Java 카드 인증이 구성된 경우 이를 사용할 수 있다는 사실을 사용자에게 알리기 위한 것입니다.
Windows XP 서비스 팩 1 의 경우 절전 모드에서 최대 절전 모드로 전환한 후 인증서 관리자에 로그인할 수 없음.	시스템을 최대 절전 모드 및 절전 모드로 전환한 후 관리자 또는 사용자가 인증서 관리자에 로그인할 수 없고, 선택한 로그온 인증서(암호, 지문 또는 Java 카드)에 관계없이 Windows 로그온 화면이 표시된 채로 남아 있습니다.	이 문제는 Microsoft 의 서비스 팩 2 에서 해결되었습니다. 이 문제의 원인에 대한 자세한 내용은 http://www.microsoft.com 에서 Microsoft 기술 자료 항목 813301 을 참조하십시오. 로그온하려면 인증서 관리자를 선택한 다음 로그인해야 합니다. 인증서 관리자에 로그인한 후, 로그인 프로세스를 완료하기 위해 Windows 에 로그인하라는 메시지가 표시되며 Windows 로그인 옵션을 선택해야 할 수 있습니다. Windows 에 먼저 로그인한 경우에는 인증서 관리자에 수동으로 로그인해야 합니다.

증상	설명	해결 방법
Embedded Security 를 복원하면 인증서 관리자 오류가 발생함.	ROM 이 출하 시 기본 설정으로 복원되면 인증서 관리자에서 인증서를 등록할 때 오류가 발생합니다.	HP Credential Manager for ProtectTools 는 인증서 관리자를 설치한 후 ROM 이 출하 시 기본 설정으로 재설정되면 TPM 에 액세스하지 못합니다. TPM 내장 보안 칩은 BIOS Computer Setup 유틸리티, BIOS Configuration for HP ProtectTools 또는 HP Client Manager 를 사용하여 활성화할 수 있습니다. TPM 내장 보안 칩을 활성화하려면 다음과 같이 하십시오. 1. 컴퓨터를 켜거나 다시 시작한 후 화면 왼쪽 하단에 **F10 = ROM Based Setup** 메시지가 나타나면 F10 키를 눌러 Computer Setup 을 실행합니다. 2. 화살표 키를 사용하여 **Security > Setup Password** 를 선택합니다. 암호를 설정합니다. 3. **Embedded Security Device** 를 선택합니다. 4. 화살표 키를 사용하여 **Embedded Security Device–Disable** 을 선택합니다. 화살표 키를 사용하여 **Embedded Security Device–Enable** 로 변경합니다. 5. **Enable > Save changes and exit** 를 선택합니다. 향후 출시될 소프트웨어 릴리스를 위해 해결책을 모색 중입니다.
보안 **Restore Identity**(ID 복원) 프로세스에서 가상 토큰과의 연결이 소실됨.	ID 를 복원하면 인증서 관리자의 로그인 화면에서 가상 토큰 위치와의 연결이 손실됩니다. 인증서 관리자에 등록된 가상 토큰이 있더라도 연결을 복원하려면 토큰을 재등록해야 합니다.	이는 설계상의 이유입니다. ID 를 유지하지 않고 인증서 관리자를 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)이라는 메시지가 나타납니다. 외장 하드 드라이브의 C:\ 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.

증상	설명	해결 방법
Windows 2000 에서는 EFS 로 암호화된 폴더가 녹색으로 강조 표시되지 않습니다.	EFS 로 암호화된 폴더는 Windows XP 에서는 녹색으로 강조 표시되지만 Windows 2000 에서는 강조 표시되지 않습니다.	이는 설계상의 이유입니다. Windows 2000 에서는 암호화된 폴더가 녹색으로 강조 표시되지 않고 Windows XP 에서는 강조 표시되는 것은 EFS 의 특징입니다. 이 특징은 Embedded Security TPM 의 설치 여부와는 상관 없습니다.
Windows 2000 에서 EFS 로 암호화된 파일을 보기 위해 암호가 필요하지 않음	사용자가 Embedded Security 를 설정하고 관리자로 로그온한 후 로그오프하고 그런 다음 다시 관리자로 로그인한 경우 Windows 2000 에서 파일/폴더를 암호 없이 계속 볼 수 있습니다. 이러한 경우는 Windows 2000 에서 첫 번째 관리자 계정에서만 발생하며 두 번째 로그인하는 관리자 계정에서는 발생하지 않습니다.	이는 설계상의 이유입니다. Windows 2000 의 EFS 특징입니다. Windows XP 의 EFS 는 기본적으로 사용자가 암호 없이 파일/폴더를 열도록 허용하지 않습니다.
FAT32 파티션으로 복원된 드라이브에 소프트웨어를 설치할 수 없음	FAT32 를 사용하여 하드 드라이브 복원을 시도할 경우 파일/폴더에 대해 EFS 를 사용하여 아무런 암호화 옵션을 사용할 수 없습니다.	이는 설계상의 이유입니다. Microsoft EFS 는 NTFS 만을 지원하며 FAT32 에서는 사용할 수 없습니다. 이는 Microsoft 의 EFS 와 관련된 특징으로서 HP ProtectTools 소프트웨어와는 상관이 없습니다.
Windows 2000 사용자가 숨김($) 공유를 통해 PSD 에 네트워크로 연결할 수 있음	Windows 2000 사용자가 숨김($) 공유를 통해 PSD 에 네트워크로 연결할 수 있습니다. 숨김 공유는 숨김($) 공유를 사용하여 네트워크를 통해 액세스할 수 있습니다.	일반적으로 PSD 는 네트워크 상에서 공유되지 않으나 Windows 2000 의 경우 숨김($) 공유를 통해 공유가 가능합니다. 따라서 관리자 계정을 반드시 암호로 보호하는 것이 좋습니다.
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 없습니다.	이는 설계상의 이유입니다. 사용자는 응급 아카이브에 액세스하여 자신의 기본 사용자 키 백업본을 저장/업데이트할 수 있습니다. 보안을 위한 '최선의 방법'을 채택해야 하며 사용자가 복구 아카이브 파일을 절대로 암호화하거나 삭제하지 않도록 지침을 주어야 합니다.
HP ProtectTools Embedded Security EFS 와 Symantec Antivirus 또는 Norton Antivirus 를 함께 사용할 경우 암호화/암호 해독 및 검색 시간이 오래 걸림	암호화된 파일은 Symantec Antivirus 또는 Norton Antivirus 2005 의 바이러스 검색에 영향을 줍니다. 검색 과정에서 파일 10 개 정도마다 사용자에게 기본 사용자 암호를 입력하라는 프롬프트가 표시됩니다. 사용자가 암호를 입력하지 않으면 기본 사용자 암호 프롬프트 시간이 만료되고 NAV2005 가 검색을 계속합니다. Symantec Antivirus 또는 Norton Antivirus 실행 시 HP ProtectTools Embedded Security EFS 를 사용하여 파일을 암호화하면 시간이 오래 걸립니다.	HP ProtectTools Embedded Security EFS 파일을 검색하는 데 소요되는 시간을 단축하려면 검색을 시작하기 전에 암호화 암호를 입력하거나 암호화를 해독합니다. HP ProtectTools Embedded Security EFS 를 사용하여 데이터를 암호화/암호 해독하는 소요되는 시간을 단축하려면 Symantec Antivirus 또는 Norton Antivirus 에서 자동 보호 옵션을 비활성해야 합니다.
응급 복구 아카이브를 이동식 미디어에 저장할 수 없음	Embedded Security 초기화 과정에서 응급 복구 아카이브 경로를 생성할 때 MMC 또는 SD 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.
Windows 2000 프랑스어(프랑스) 환경에서 데이터를 암호화할 수 없음	파일 아이콘을 마우스 오른쪽 버튼으로 눌렀을 때 **Encrypt**(암호화) 항목이 표시되지 않습니다.	Microsoft 운영체제의 제한 사항입니다. 로케일을 다른 설정(예: 프랑스어(캐나다))으로 변경하면 **Encrypt**(암호화) 항목이 표시됩니다. 문제를 해결하려면 파일 아이콘을 마우스 오른쪽 버튼으로 누른 후 **Properties**(속성) **> Advanced**(고급) **> Encrypt Contents**(콘텐츠 암호화)를 선택하여 파일을 암호화합니다.

증상	설명	해결 방법
전원 차단 후 Embedded Security 초기화 과정에서 소유권을 얻는 중 오류 발생	Embedded Security 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(Embedded Security 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. 화면에 **F10=Setup** 메시지가 나타나면(모니터 표시등에 녹색불이 들어오면) F10 키를 누릅니다. 3. 해당 언어 옵션을 선택합니다. 4. Enter 키를 누릅니다. 5. **Security > Embedded Security** 를 선택합니다. 6. **Embedded Security Device** 옵션을 **Enable** 로 설정합니다. 7. F10 키를 눌러 변경 사항을 적용합니다. 8. **File**(파일) **> Save Changes and Exit**(변경 저장 후 종료)를 선택합니다. 9. Enter 키를 누릅니다. 10. F10 키를 눌러 변경 사항을 저장하고 F10 Setup 유틸리티를 종료합니다.
TPM 모듈을 활성화한 후에 Computer Setup (F10) 유틸리티 암호를 삭제할 수 있음	TPM 모듈을 활성화하려면 Computer Setup(F10) 유틸리가 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) 유틸리티 암호는 암호를 아는 사용자만 삭제할 수 있습니다. 그러나 Computer Setup (F10) 유틸리티 암호를 항상 보호할 것을 권장합니다.
대기 상태 후 시스템을 활성화할 때 PSD 암호 상자가 표시되지 않음	PSD 생성 후 사용자가 로그온하면 TPM 에서 기본 사용자 암호를 묻습니다. 사용자가 암호를 입력하지 않으면 시스템이 대기 모드로 들어가고 사용자가 작업을 재개해도 암호 대화상자가 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.
Windows 2000 에서 Microsoft EFS 의 일부 기능을 사용할 수 없음	관리자는 암호를 몰라도 시스템의 암호화된 정보를 액세스할 수 있습니다. 관리자가 틀린 암호를 입력하거나 암호 대화상자를 취소할 경우 정확한 암호를 입력한 것처럼 암호화된 파일이 열립니다. 이 상황은 데이터 암호화 시 보안 설정의 사용 여부에 상관 없이 발생하며, Windows 2000 의 첫 번째 관리자 계정에서만 발생합니다.	데이터 복구 정책에 따라 관리자는 복구 에이전트로 자동 지정됩니다. 사용자 키를 읽어 올 수 없을 경우(틀린 암호를 입력하거나 암호 입력 대화상자를 취소할 경우) 파일이 복구 키를 사용하여 자동 암호 해독됩니다. 이는 Microsoft EFS 로 인해 발생하는 문제입니다. 자세한 내용은 http://www.microsoft.com 에서 Microsoft Knowledge Base Technical Article Q257705 를 참조하십시오. 문서는 관리자만 열 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 발생할 경우가 있습니다.	이를 해결하려면 다음과 같이 하십시오. 1. 시스템을 다시 시작합니다. 2. 로그오프합니다. 3. 다시 로그인합니다.
새 데이터를 생성하거나 이전하기에 전에 저장 장치를 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.	이 문제는 새로운 데이터를 생성하거나 이전하는 작업이 완료되기 전에 사용자가 PSD 를 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) 대화상자에서 사용자가 **Yes**(예)를 선택하여 관리 도구를 열었기 때문에 설치 제거 프로세스는 관리 도구가 닫힐 때까지 대기합니다. 사용자가 이 대화상자에서 **No**(아니요)를 선택하면 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 가끔씩 발생함	최소 RAM 사양으로 빠른 사용자 전환을 사용할 경우 로그온 화면이 표시되지 않고 검정색 화면이 표시되면서 키보드와 마우스가 작동하지 않을 수 있습니다.	주원인은 메모리가 낮은 구성에서 시간이 오래 걸리기 때문일 수 있습니다. 통합 그래픽은 128MB 의 메모리 중 120MB 는 사용자가 이용하도록 남겨 두고 8MB 만 가져오는 UMA 아키텍처를 사용합니다. 두 사용자가 로그인하여 빠른 사용자 전환을 하면서 이 120MB 를 공유할 때 오류가 발생하는 것입니다. 이를 해결하려면 시스템을 재부팅한 후 메모리 구성을 늘리 방법을 사용합니다(HP 는 기본적으로 보안 모듈에 대한 128MB 구성은 제공하지 않음).
EFS 사용자 인증(암호 요청) 시간이 초과되고 **access denied**(액세스 거부) 메시지가 표시됨	**OK**(확인)를 누르거나 시간이 만료되어 대기 상태에서 돌아오면 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.
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.

증상	설명	해결 방법
사용자 초기화 마법사에서 전자 우편 보안 옵션을 선택하지 않거나 사용자 정책에서 전자 우편 보안 구성을 비활성화해도 전자 우편 보안이 지원됨	내장 보안 소프트웨어와 마법사는 전자 우편 클라이언트(Outlook, Outlook Express, Netscape 등)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 노후화됩니다.	xml 파일 덮어쓰기 문제를 해결하기 위한 작업이 진행 중이며 향후 SoftPaq 에서는 이 솔루션을 제공할 예정입니다.
Embedded Security 에서 사용자가 복원 작업 중 자동 로그온 스크립트가 작동하지 않음	이 오류는 다음과 같은 경우에 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 인증서 관리자는 Infineon TPM User Authentication 에 자동 로그온할 수 있는지를 사용자에게 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 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 사용 가능합니다.
PSD 를 생성했던 하드 드라이브를 포맷한 후 PSD 가 비활성화되고 삭제 불가능해짐	PSD 를 생성했던 보조 하드 드라이브를 포맷한 후 PSD 가 비활성화되고 삭제 불가능해집니다. PSD 아이콘은 여전히 표시되지만 사용자가 PSD 에 액세스하려 하면 **drive is not accessible(드라이브를 액세스할 수 없음)**이라는 오류 메시지가 표시됩니다. 사용자가 PSD 를 삭제할 수 없으며 **your PSD is still in use, please ensure 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**	이는 설계상의 이유입니다. PSD 데이터 저장 위치에서 강제로 삭제하거나 연결을 해제하면 Embedded Security PSD 드라이브 에뮬레이션이 계속 작동하고 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.

증상	설명	해결 방법
	않은지 확인하십시오)라는 메시지가 표시됩니다. 사용자가 시스템을 재부팅하여 PSD 를 삭제해야 하며 재부팅 후에는 PSD 가 표시되지 않습니다.	
자동 백업 아카이브에서 복원 시 내부 오류가 발생함	다음과 같은 경우, • 사용자가 자동 백업 아카이브로부터 복원하기 위해 HPPTSM 에서 Embedded Security 의 **Restore under Backup**(백업에서 복원) 옵션을 선택한 경우 • 사용자가 **SPSystemBackup .xml** 을 선택한 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 선택하면 Embedded Security 마법사가 실패하고 다음 메시지가 표시됩니다: **An internal Embedded Security error has been detected**(Embedded Security 내부 오류가 발생했습니다.) 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** 를 선택한 후 필드를 **Hidden** 에서 **Available** 로 수정합니다.
자동 백업이 매핑된 드라이브에서 작동하지 않음	관리자가 Embedded Security 에서 자동 백업을 설정하면 **Windows > 작업 > 예약된 작업**에 하나의 항목으로 추가됩니다. Windows 의 예약된 작업은 백업을 실행하기 위해 NT AUTHORITY\SYSTEM 을 사용하도록 설정되어 있습니다. 이 프로세스는 로컬 드라이브에 대해서는 제대로 실행됩니다. 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 로그인 시 수행되도록 예약된 경우 Embedded Security TNA 아이콘은 **The Backup Archive location is 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	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
	백업이 특정 시간에 예약된 경우에는 실패 메시지 없이 백업이 실패합니다.	
Embedded Security GUI 에서 Embedded Security 상태를 일시적으로 비활성화할 수 없음	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.

기타

영향 받은 소프트웨어–증상	설명	해결 방법
HP ProtectTools Security Manager–경고 수신: **The security application can not be installed until the HP Protect Tools Security Manager is installed(HP Protect Tools Security Manager 를 설치해야만 보안 응용 프로그램을 설치할 수 있습니다)**	Embedded Security, Java 카드, 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 설치하기 전에 HP ProtectTools Security Manager 소프트웨어를 설치해야 합니다.
dc7600 및 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	dc7600 및 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. *펌웨어 업데이트 후에는 반드시 재부팅하도록 하십시오. 재부팅을 해야만 펌웨어 버전이 업데이트됩니다.	1. HP ProtectTools 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. **HP ProtectTools Security Manager** 를 누릅니다.

영향 받은 소프트웨어–증상	설명	해결 방법
		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 • 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.** 펌웨어 버전이 2.18 이상이 아닐 경우 TPM 펌웨어를 다운로드합니다. TPM Firmware SoftPaq 은 http://www.hp.com 에서 다운로드할 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 * General–액세스 제한 및 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 로그인할 수 있도록 해야 합니다.	이는 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

영향 받은 소프트웨어–증상	설명	해결 방법
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 지원) 설정을 기본값으로 복원할 수 없음	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 지원) 옵션은 기본적으로 **Disable**(비활성)로 설정됩니다.	**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. 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 을 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.
Embedded Security Windows 소프트웨어에서 소유자 암호를 변경한 후 Computer Setup 을 실행할 때 BIOS 에서 기존 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 없으며 TPM 키 블록에서 TPM 암호문을 확인할 수 없어서 발생하는 문제입니다.

용어

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

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

FAT 파티션 File Allocation Table 의 약어로, 저장 매체를 인덱싱하는 방법

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

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

NTFS 파티션 NT File System 의 약어로, 저장 매체를 인덱싱하는 방법. 이 방법은 Windows Vista 및 Windows XP 표준입니다.

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

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

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(일부 모델만 해당) 매우 중요한 사용자 정보를 악의적인 공격자로부터 보호하는 내장 보안 칩. 특정 플랫폼에서의 신뢰 경로이기도 함. TPM 은 TCG(Trusted Computing Group) 규격에 부합하는 암호화 알고리즘과 작업을 제공합니다.

USB 토큰 사용자의 신원 정보를 저장하는 보안 장치. Java Card 나 생체 인식기와 같이 컴퓨터에서 소유자를 인증하는 데 사용됩니다.

Windows 사용자 계정 네트워크나 개별 컴퓨터에 로그온하도록 승인된 개인 프로필

가상 토큰 Java Card 및 리더와 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

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

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 키와 인증서의 관리, 복원, 이전을 가능하게 하는 작업

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

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

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

암호화(Cryptography) 특정인만 해독할 수 있도록 데이터를 암호화하고 해독하는 기법

암호화(Encryption) 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

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

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

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

인증 기관 공용 키 인프라를 실행하는 데 필요한 인증서를 발급하는 서비스

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

재부팅 컴퓨터를 재시작하는 과정

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

색인