

HP ProtectTools Security Manager 설명서

HP Compaq 비즈니스 데스크탑



© Copyright 2006 Hewlett-Packard
Development Company, L.P. 이 정보는 사전
통지 없이 변경될 수 있습니다.

Microsoft 와 Windows 는 미국 및 기타 국가
에서 Microsoft Corporation 의 상표입니다.

Intel 및 SpeedStep 은 미국 및 기타 국가
에서 Intel Corporation 의 상표입니다.

HP 제품 및 서비스에 대한 유일한 보증은 제
품 및 서비스와 함께 동봉된 보증서에 명시
되어 있습니다. 본 설명서에는 어떠한 추가
보증 내용도 들어 있지 않습니다. HP 는 본
설명서에 대한 기술상 또는 편집상의 오류나
누락에 대해 책임을 지지 않습니다.

본 설명서에 들어 있는 소유 정보는 저작권
법에 의해 보호를 받습니다. Hewlett-
Packard Company 의 사전 서면 동의 없이
본 설명서의 어떠한 부분도 복사하거나, 재발
행하거나, 다른 언어로 번역할 수 없습니다.

HP ProtectTools Security Manager 설명서

HP Compaq 비즈니스 데스크탑

초판(2006년 8월)

문서 일련 번호: 431330-AD1

본 설명서 정보

본 설명서는 HP ProtectTools Security Manager 구성 및 사용 방법에 대해 설명합니다.



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 소개

HP ProtectTools Security Manager	1
ProtectTools Security Manager 액세스	1
보안 역할 이해	2
ProtectTools 암호 관리	2
다단계 인증 인증서 관리자 로그인	4
보안 암호 만들기	5
고급 작업	6
ProtectTools 설정 관리	6
Java 카드 파워온 인증 지원 활성화 및 비활성화	6
Embedded Security 에 대한 파워온 인증 지원 활성화 및 비활성화	6
Computer Setup 암호 관리	7
파워온 암호 설정(사용 가능한 경우)	7
파워온 암호 변경(사용 가능한 경우)	7
시스템 설정	8
파워온 인증 지원 변경	8
사용자 계정 변경	9
Computer Setup 관리자 암호 설정	9
Computer Setup 관리자 암호 변경	9
파워온 인증의 사전 공격 방어 동작	11
Dictionary Attack Defense(사전 공격 방어)	11

2 HP BIOS Configuration for ProtectTools

기본 개념	13
BIOS 설정 변경	13

3 HP Embedded Security for ProtectTools

기본 개념	15
설정 절차	16

4 HP Credential Manager for ProtectTools

기본 개념	17
시작 절차	17
처음 로그인	18

5 HP Java Card Security for ProtectTools

기본 개념	19
-------------	----

6 타사 솔루션

7 원격 배치용 HP Client Manager

배경	23
초기화	23
유지 관리	23

8 문제 해결

ProtectTools 용 인증서 관리자	25
ProtectTools 용 내장 보안	29
기타	36

용어	39
----------	----

색인	43
----------	----

1 소개

HP ProtectTools Security Manager

ProtectTools Security Manager 소프트웨어는 컴퓨터, 네트워크 및 중요한 데이터에 대한 무단 액세스를 차단하는 데 도움이 되는 보안 기능을 제공합니다. 다음 모듈을 통해 강화된 보안 기능을 제공합니다.

- HP BIOS Configuration for ProtectTools
- HP Embedded Security for ProtectTools
- HP Credential Manager for ProtectTools
- HP Java Card Security for ProtectTools

모델에 따라 컴퓨터에서 사용할 수 있는 모듈이 다릅니다. ProtectTools 모듈은 사전 설치되어 있거나 컴퓨터와 함께 CD로 제공되거나 HP 웹 사이트에서 구입할 수 있습니다. 자세한 내용을 보려면 <http://www.hp.com> 을 참조하십시오.



주 ProtectTools 모듈에 대한 자세한 지침은 ProtectTools 도움말 화면을 참조하십시오.

TPM(Trusted Platform Module)을 사용하려면, TPM 이 포함된 플랫폼에 TSS(TCG Software Stack)와 내장 보안 소프트웨어가 있어야 합니다. 일부 모델에는 TSS 가 제공됩니다. TSS 가 제공되지 않으면 HP 에서 구입할 수 있습니다. 또한, 일부 모델의 경우 TPM 활성화 소프트웨어는 별도로 구입해야만 합니다. 자세한 내용은 [타사 솔루션](#) 을 참조하십시오.

ProtectTools Security Manager 액세스

Microsoft Windows 제어판에서 ProtectTools Security Manager 에 액세스하려면 다음과 같이 하십시오.

- ▲ Windows XP 의 경우: 시작 > 제어판 > 보안 센터 > **ProtectTools Security Manager** 를 누릅니다.
- ▲ Windows 2000 의 경우: 시작 > 모든 프로그램 > **HP ProtectTools Security Manager** 를 누릅니다.



주 인증서 관리자 모듈을 구성한 후 Windows 로그인 화면에서 인증서 관리자로 바로 로그인할 수 있습니다. 자세한 내용은 [HP Credential Manager for ProtectTools](#) 를 참조하십시오.

보안 역할 이해

컴퓨터의 보안 관리에 있어서(특히 대형 조직의 경우) 다양한 유형의 관리자와 사용자 간에 책임과 권리를 분리하는 것이 중요합니다.



주 소규모 조직이나 개인적으로 사용하는 경우에는 이러한 역할을 동일한 사람이 모두 수행할 수도 있습니다.

ProtectTools 의 경우, 보안 의무와 권한을 다음과 같은 역할들로 분리할 수 있습니다.

- 보안 관리자-회사나 네트워크의 보안 수준을 정의하고, **Java** 카드, 생체인식 리더, **USB** 토큰 등 배치할 보안 기능을 결정합니다.



주 ProtectTools 의 많은 기능은 보안 관리자가 HP 와 협력하여 사용자 정의할 수 있습니다. 자세한 내용은 <http://www.hp.com> 을 참조하십시오.

- IT 관리자-보안 관리자가 정의한 보안 기능을 적용하고 관리합니다. 일부 기능을 활성화하거나 비활성화할 수도 있습니다. 예를 들어, 보안 관리자가 **Java** 카드를 배치하기로 결정하면 IT 관리자는 **Java** 카드 BIOS 보안 모드를 활성화할 수 있습니다.
- 사용자-보안 기능을 사용합니다. 예를 들어, 보안 관리자와 IT 관리자가 시스템에 대해 **Java** 카드를 활성화하면, 사용자는 **Java** 카드 PIN 을 설정하고 인증에 그 카드를 사용할 수 있습니다.

관리자가 최종 사용자 권한과 사용자 액세스를 제한하는 경우 “최선의 방법”을 수행할 것을 권장합니다.

ProtectTools 암호 관리

대부분의 ProtectTools Security Manager 기능은 암호에 의해 보호됩니다. 다음 표에 일반적으로 사용되는 암호, 암호가 설정되는 소프트웨어 모듈 및 암호 기능이 설명되어 있습니다.

IT 관리자만 설정 및 사용할 수 있는 암호의 경우에는 표에 표시되어 있습니다. 다른 모든 암호는 일반 사용자 또는 관리자가 설정할 수 있습니다.

표 1-1 암호 관리

ProtectTools 암호	설정되는 ProtectTools 모듈	기능
Computer Setup 관리자 암호	BIOS 구성, IT 관리자가 설정	BIOS Computer Setup 유틸리티 및 보안 설정에 대한 액세스를 보호합니다.
주 BIOS 관리자, F10 Setup 또는 Security Setup 암호라고도 함		
파워온 암호	BIOS 구성	HP ProtectTools 파워온 인증 지원은 전원이 켜진 컴퓨터에 대한 무단 액세스를 방지하기 위해 설계된 TPM 기반 보안 도구입니다. 파워온 인증 지원은 HP ProtectTools Embedded Security 기본 사용자 암호를 사용합니다. Computer Setup 에서 파워온 인증을 활성화하면, 처음/다음 Embedded Security 기본 사용자 키가 초기화될 때 암호가 설정됩니다. Embedded Security TPM 칩은 파워온 인증 암호를 보호합니다.

표 1-1 암호 관리 (계속)








<p>Java 카드 관리자 암호</p> <p> 주 BIOS 관리자 카드 암호라고도 함</p>	Java 카드 보안, IT 관리자가 설정	<p>식별 목적으로 Java 카드를 컴퓨터에 연결합니다.</p> <p>컴퓨터 관리자가 Computer Setup 암호를 활성화 또는 비활성화하고, 새 관리자 카드를 생성하고, 사용자나 관리자 카드를 복원하기 위한 복구 파일을 만들 수 있습니다.</p>
Java 카드 PIN	Java 카드 보안	<p>선택 사양인 Java 카드와 리더가 사용되는 경우 Java 카드 콘텐츠 및 컴퓨터에 대한 액세스를 보호합니다. Java 카드 사용자 암호가 핀과 일치하는지 확인합니다. 이것은 Java 카드 인증을 등록하는데 사용됩니다.</p>
Java 카드 복구 파일 암호(사용 가능한 경우)	Java 카드 보안	<p>BIOS 암호를 포함한 복구 파일에 대한 액세스를 보호합니다.</p>
<p>Java 카드 사용자 암호(사용 가능한 경우)</p> <p> 주 BIOS 사용자 카드 암호라고도 함</p>	Java 카드 보안	<p>식별을 위해 Java 카드를 컴퓨터에 연결합니다.</p> <p>사용자가 사용자 카드를 복원하기 위한 복구 파일을 만들 수 있습니다.</p>
<p>기본 사용자 암호</p> <p> 주 Embedded Security 암호, TPM Preboot 암호라고도 함</p>	Embedded Security	<p>보안 전자 우편, 파일 및 폴더 암호화 등의 Embedded Security 기능 액세스에 사용합니다. BIOS 파워온 인증 지원 암호로 설정된 경우, 컴퓨터가 켜져 있거나 재시작 또는 절전 모드에서 복원되었을 때 컴퓨터 콘텐츠에 대한 액세스를 보호합니다. 또한 PSD(Personal Secure Drive)에 대한 인증과 TPM 인증 등록에 사용됩니다.</p>
<p>응급 복구 토큰 암호</p> <p> 주 응급 복구 토큰 키라고도 함</p>	Embedded Security, IT 관리자가 설정	<p>TPM 내장 보안 칩에 대한 백업 파일인 응급 복구 토큰에 대한 액세스를 보호합니다.</p>
소유자 암호	Embedded Security, IT 관리자가 설정	<p>Embedded Security 의 모든 소유자 기능에 대한 무단 액세스로부터 시스템과 TPM 칩을 보호합니다.</p>
인증서 관리자 로그인 암호	인증서 관리자	<p>이 암호는 다음 두 가지 옵션을 제공합니다.</p> <ul style="list-style-type: none"> Windows 로그인 프로세스에서 사용하여 Windows 및 인증서 관리자를 동시에 액세스할 수 있습니다. Microsoft Windows 에 로그인한 후 인증서 관리자에 액세스하기 위해 별도로 로그인할 때 사용할 수 있습니다.
인증서 관리자 복구 파일 암호	인증서 관리자, IT 관리자가 설정	<p>인증서 관리자 복구 파일에 대한 액세스를 보호합니다.</p>
Windows 로그인 암호	Windows 제어판	<p>수동 로그인이나 Java 카드에 저장하여 사용할 수 있습니다.</p>
백업 스케줄러 암호	Embedded Security, IT 관리자가 설정	<p>내장 보안에 대한 백업 스케줄러를 설정합니다.</p>

표 1-1 암호 관리 (계속)

	<p>주 내장 보안에 대한 백업 스케줄러를 구성하기 위해 Windows 사용자 암호가 사용됩니다.</p>		
	<p>주 가져온 인증서에는 각각 해당 인증서에 대한 특정한 암호가 있습니다.</p>	<p>PKCS #12 가져오기 암호 Embedded Security, IT 관리자가 설정</p>	<p>다른 인증서를 가져올 경우 이 인증서의 암호화 키에 사용되는 암호입니다.</p>  <p>주 일반적인 소프트웨어 작동에는 필요하지 않습니다. 사용자는 중요한 인증서를 보내기 위해 내장 보안을 사용할 때 이 암호를 설정할 수 있습니다.</p>
		<p>Embedded Security, IT 관리자가 설정</p>	<p>기본 사용자 암호를 잊어버린 경우 사용자가 암호를 재설정할 수 있는 도구가 제공되는데, 이 재설정 작업을 수행하는 데 사용되는 암호입니다.</p>
	<p>주 복구 에이전트는 어떤 로컬 시스템 관리자나 될 수 있습니다. 복구 에이전트가 만들어지면 해당 관리자로 로그인하여야 하며 암호가 필요합니다. 복구 에이전트는 모든 사용자의 암호화된 데이터를 단지 여는 작업을 수행하는 것으로 암호를 해독할 수 있습니다(마법사가 필요 없음).</p>	<p>Microsoft 복구 에이전트 관리자 암호 Microsoft, IT 보안 관리자가 설정</p>	<p>PSD(Personal Secure Drive) 암호화된 데이터가 복구될 수 있는지 확인합니다. 자세한 내용은 http://www.microsoft.com/technet/prodtechnol/winxpro/support/dataprot.mspx 를 참조하십시오.</p>  <p>주 일반적인 소프트웨어 작동에는 필요하지 않습니다. 사용자는 중요한 인증서를 보내기 위해 내장 보안을 사용할 때 이 암호를 설정할 수 있습니다.</p>
<p>가상 토큰 마스터 PIN</p>		<p>인증서 관리자</p>	<p>인증서 관리자로 소유자 인증서를 저장하는 사용자 옵션</p>
<p>가상 토큰 사용자 PIN</p>		<p>인증서 관리자</p>	<p>인증서 관리자로 소유자 인증서를 저장하는 사용자 옵션</p>
<p>ID 백업 마법사 암호</p>		<p>인증서 관리자, IT 관리자가 설정</p>	<p>인증서 관리자를 사용할 때 ID 백업에 대한 액세스를 보호하기 위해 사용합니다.</p>
<p>가상 토큰 인증 암호</p>		<p>인증서 관리자</p>	<p>인증서 관리자로 가상 토큰 인증을 등록할 때 사용합니다.</p>
<p>TPM 인증 별칭</p>		<p>인증서 관리자</p>	<p>인증서 관리자에서 관리자나 사용자의 기본 사용자 암호 대신에 사용합니다.</p>
<p>지문 로그인</p>		<p>인증서 관리자</p>	<p>인증서 관리자는 사용자가 Windows 암호 로그인을 사용이 편리하고 안전한 지문 로그인으로 교체할 수 있도록 합니다. 암호와는 달리 지문 인증서는 공유, 수여, 도난 또는 추측될 수 없습니다. 인증서 관리자에서 사용합니다.</p>
<p>USB 토큰 인증</p>		<p>인증서 관리자</p>	<p>인증서 관리자에서 암호 대신 토큰 인증으로 사용합니다.</p>

다단계 인증 인증서 관리자 로그인

인증서 관리자 로그인은 Windows 운영체제에 로그인할 때 다단계 인증 기술을 사용할 수 있게 합니다. 이것은 강력한 다단계 인증을 설정하여 표준 Windows 암호 로그인의 보안을 높여줍니다. 또한 사

용자 암호를 기억할 필요가 없으므로 로그인 과정이 훨씬 간편해집니다. 인증서 관리자 로그온의 특별한 기능은 여러 계정의 인증서를 하나의 사용자 ID 로 통합하는 것입니다. 이것은 다단계 인증을 한 번만 사용하여 동일한 인증서 세트로 다른 Windows 계정에 여러 번 액세스할 수 있도록 합니다.

다단계 사용자 인증은 사용자 암호, 동적 또는 1 회용 암호, TPM, Java 카드, USB 토큰, 가상 토큰 및 생체인식 등을 조합하여 사용하는 것을 지원합니다. 또한 인증서 관리자는 동일한 응용프로그램이나 서비스에 대한 여러 사용자 액세스 권한을 허용하여 대체 인증 방법을 지원합니다. 사용자는 모든 인증서, 응용프로그램 암호, 네트워크 계정을 통합하여 User Identity(사용자 ID)라고 하는 단일 데이터 유닛으로 통합할 수 있습니다. User Identity(사용자 ID)는 다단계 인증에 의해 암호화되고 보호됩니다.

보안 암호 만들기

암호를 만들 때는 먼저 프로그램에서 설정한 규칙을 따라야 합니다. 그러나 일반적으로 다음 지침을 따르면, 강력한 암호를 만들고 암호가 손상되는 것을 줄일 수 있습니다.

- 6 자 이상의 암호를 사용합니다. 8 자 이상이 더 바람직합니다.
- 암호에 대소문자를 혼용합니다.
- 가능한 경우에는 언제나 알파벳 문자와 특수 문자 및 구두점을 혼용하여 만듭니다.
- 키 워드의 글자를 특수 문자나 숫자로 대체합니다. 예를 들어, 숫자 1 을 l 또는 L 자 대신 사용합니다.
- 두 가지 이상의 언어에서 단어를 조합합니다.
- 숫자나 특수 문자를 단어나 구의 중간에 삽입하여 분리합니다. 예를 들어, “Mary22Cat45”와 같이 만듭니다.
- 사전에서 찾을 수 있는 암호를 사용하지 않습니다.
- 이름이나 생일, 애완동물 이름 또는 어머니의 결혼 전 성 등 기타 개인적인 정보를 암호로 사용하지 않습니다. 거꾸로 적는 것도 안됩니다.
- 정기적으로 암호를 변경합니다. 문자 몇 개만 추가하여 변경할 수도 있습니다.
- 암호를 기록해 놓는 경우 컴퓨터 근처의 눈에 잘 띄는 장소에 보관하지 않습니다.
- 암호를 전자 우편과 같은 파일 형태로 컴퓨터에 저장해 두지 않습니다.
- 계정을 공유하거나 다른 사람에게 암호를 말하지 않습니다.

고급 작업

ProtectTools 설정 관리

ProtectTools Security Manager의 일부 기능은 BIOS 구성에서 관리할 수 있습니다.

Java 카드 파워온 인증 지원 활성화 및 비활성화

이 옵션이 사용 가능할 경우, 이것을 활성화하면 컴퓨터를 켤 때 사용자 인증을 위해 Java 카드를 사용할 수 있습니다.



주 파워온 인증 기능을 완전히 활성화하려면 ProtectTools 용 Java 카드 보안 모듈을 사용하여 Java 카드를 구성해야 합니다.

Java 카드 파워온 인증 지원을 활성화하려면 다음과 같이 하십시오.

1. 시작 > 모든 프로그램 > **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **BIOS Configuration(BIOS 구성)**을 선택합니다.
3. BIOS 관리자 암호 프롬프트에 Computer Setup 관리자 암호를 입력한 다음 **OK(확인)**를 누릅니다.
4. 왼쪽 창에서 **Security(보안)**를 선택합니다.
5. **Java Card Security(Java 카드 보안)** 아래에서 **Enable(활성화)**을 선택합니다.



주 Java 카드 파워온 인증을 비활성화하려면 **Disable(비활성화)**을 선택합니다.

6. **Apply(적용)**를 누른 다음 **ProtectTools** 창에서 **OK(확인)**를 눌러 변경 사항을 저장합니다.

Embedded Security 에 대한 파워온 인증 지원 활성화 및 비활성화

이 옵션이 사용 가능한 경우, 이것을 활성화하면 컴퓨터를 켤 때 시스템에서 사용자 인증을 위해 TPM 내장 보안 칩을 사용할 수 있습니다.



주 파워온 인증 기능을 완전히 활성화하려면 ProtectTools 용 Embedded Security 모듈을 사용하여 TPM 내장 보안 칩을 구성해야 합니다.

내장 보안에 대한 파워온 인증 지원을 활성화하려면 다음과 같이 하십시오.

1. 시작 > 모든 프로그램 > **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **BIOS Configuration(BIOS 구성)**을 선택합니다.
3. BIOS 관리자 암호 프롬프트에 Computer Setup 관리자 암호를 입력한 다음 **OK(확인)**를 누릅니다.
4. 왼쪽 창에서 **Security(보안)**를 선택합니다.
5. **Embedded Security(내장 보안)** 아래에서 **Enable Power-On Authentication Support(파워온 인증 지원 활성화)**를 선택합니다.



주 Embedded Security 에 대한 파워온 인증을 비활성화하려면 **Disable(비활성화)**을 선택합니다.

6. **Apply(적용)**를 누른 다음 **ProtectTools** 창에서 **OK(확인)**를 눌러 변경 사항을 저장합니다.

Computer Setup 암호 관리

BIOS 구성을 사용하여 Computer Setup 의 파워온 및 설정 암호를 설정하고 변경할 수 있습니다. 또한 다양한 암호 설정을 관리할 수 있습니다.



주의 BIOS 구성의 **Passwords(암호)** 페이지에서 설정한 암호는 **ProtectTools** 창에서 **Apply(적용)** 또는 **OK(확인)** 버튼을 누르면 즉시 저장됩니다. 이전 암호를 모르면 암호 설정을 원상태로 되돌릴 수 없으므로 설정한 암호가 무엇인지 반드시 기억해야 합니다.

파워온 암호는 무단 사용으로부터 컴퓨터를 보호할 수 있습니다.



주 파워온 암호를 설정한 후 **Passwords(암호)** 페이지의 **Set(설정)** 버튼은 **Change(변경)** 버튼으로 교체됩니다.

Computer Setup 관리자 암호는 Computer Setup 의 구성 설정과 시스템 식별 정보를 보호합니다. 이 암호가 설정된 후 Computer Setup 에 액세스하려면 암호를 입력해야 합니다.

관리자 암호를 설정한 경우에는 ProtectTools 의 BIOS 구성 부분을 열기 전에 암호를 입력하라는 메시지가 표시됩니다.



주 관리자 암호를 설정한 후 **Passwords(암호)** 페이지의 **Set(설정)** 버튼은 **Change(변경)** 버튼으로 교체됩니다.

파워온 암호 설정(사용 가능한 경우)

파워온 암호를 설정하려면 다음과 같이 하십시오.

1. 시작 > 모든 프로그램 > **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **BIOS Configuration(BIOS 구성)**을 선택한 다음 **Security(보안)**를 선택합니다.
3. 오른쪽 창에서 **Power-On Password(파워온 암호)** 옆의 **Set(설정)**를 누릅니다.
4. **Enter Password(암호 입력)** 및 **Verify Password(암호 확인)** 상자에 암호를 입력하고 확인합니다.
5. **Passwords(암호)** 대화상자에서 **OK(확인)**를 누릅니다.
6. **Apply(적용)**를 누른 다음 **ProtectTools** 창에서 **OK(확인)**를 눌러 변경 사항을 저장합니다.

파워온 암호 변경(사용 가능한 경우)

파워온 암호를 변경하려면 다음과 같이 하십시오.

1. 시작 > 모든 프로그램 > **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **BIOS Configuration(BIOS 구성)**을 선택한 다음 **Security(보안)**를 선택합니다.
3. 오른쪽 창에서 **Power-On Password(파워온 암호)** 옆의 **Change(변경)**를 누릅니다.
4. **Old Password(이전 암호)** 상자에 현재의 암호를 입력합니다.

5. **Enter Password(암호 입력)** 및 **Verify Password(암호 확인)** 상자에 새 암호를 설정하고 확인합니다.
6. **Passwords(암호)** 대화상자에서 **OK(확인)**를 누릅니다.
7. **Apply(적용)**를 누른 다음 **ProtectTools** 창에서 **OK(확인)**를 눌러 변경 사항을 저장합니다.

시스템 설정

1. HP ProtectTools Embedded Security 를 초기화합니다.
2. 기본 사용자 키를 초기화합니다.

HP 파워온 인증 지원은 기본 사용자 키가 설정되고 파워온에 대한 기본 사용자 암호가 설정되면 바로 시작됩니다. 다음 재부팅 후 HP ProtectTools 파워온 인증 지원이 초기화되고 컴퓨터를 시작하기 위해서는 반드시 기본 사용자 암호를 사용해야 합니다. 파워온 인증 지원이 작동하면, BIOS 설정 입력 옵션은 표시되지 않습니다. 사용자가 파워온 인증 지원 창에서 설정 암호를 입력하면 BIOS 로 들어갑니다.

Embedded Security 기본 사용자 암호가 이미 설정되어 있으면 파워온 인증을 사용하여 암호 보호를 설정하기 위해서는 암호를 변경해야 합니다.

파워온 인증 지원 변경

암호 파워온 인증 지원은 내장 기본 사용자 암호를 사용합니다. 암호를 변경하려면 다음과 같이 하십시오.

1. F10 BIOS 설정으로 들어가서(위 설정 단계에 설명한 설정 암호가 있어야 함) **Security(보안) > Embedded Security Device(내장 보안 장치) > Reset authentication credential(인증서 재설정)**로 이동합니다.
2. 화살표 키를 눌러 설정을 **Do not reset(재설정하지 않음)**에서 **Reset(재설정)**으로 변경합니다.
3. **Security Manager(보안 관리자) > Embedded Security(내장 보안) > User Settings(사용자 설정) > Basic User Password(기본 사용자 암호) > Change(변경)**로 이동합니다.
4. 이전 암호를 입력한 다음 새 암호를 입력하고 확인합니다.
5. 파워온 인증 지원으로 재부팅합니다.

암호 창에 이전 암호를 먼저 입력하라는 메시지가 나타납니다.

6. 이전 암호를 입력하고 새 암호를 입력합니다. 새 암호를 세 번 잘못 입력하면 암호가 잘못되었다는 메시지가 표시된 창이 나타나고 파워온 인증이 원래의 Embedded Security 암호 F1 = Boot 로 되돌아 갑니다.

이때, 암호는 동기화되지 않고 사용자는 재동기화를 위해 Embedded Security 암호를 다시 변경해야 합니다.

사용자 계정 변경

파워온 인증은 한 번에 한 명의 사용자만 지원합니다. 파워온 인증을 제어하는 사용자 계정을 변경하려면 다음과 같이 하십시오.

1. **F10 BIOS > Security(보안) > Embedded Security Device(내장 보안 장치) > Reset authentication credential(인증서 재설정)**로 이동합니다.
2. 화살표 키를 눌러 커서를 옆으로 이동한 다음 아무 키나 눌러 계속합니다.
3. **F10** 을 두 번 누른 다음 **Enter** 를 눌러 **Save Changes and Exit(변경 사항 저장 후 종료)**를 실행합니다.
4. 변경할 대상 **Microsoft Windows** 사용자를 만들고 로그인합니다.
5. **Embedded Security** 를 열고 새 **Windows** 사용자 계정에 대한 기본 사용자 키를 초기화합니다. 기본 사용자 키가 이미 있으면, 파워온 인증의 소유권을 취득하도록 기본 사용자 암호를 변경합니다.

파워온 인증은 이제 새 사용자의 기본 사용자 암호만을 받아들입니다.



주의 소프트웨어 암호화, 하드웨어 암호화 및 하드웨어를 통해 데이터를 보호할 수 있는 많은 제품이 나와 있습니다. 대부분의 제품이 암호를 사용하여 관리됩니다. 이러한 도구와 암호를 잘못 관리하면 데이터 손실, 하드웨어 잠금이나 교체 상황까지 발생할 수 있습니다. 따라서 이러한 도구를 사용하기 전에 모든 해당 도움말 파일을 검토하십시오.

Computer Setup 관리자 암호 설정

Computer Setup 관리자 암호를 설정하려면 다음과 같이 하십시오.

1. 시작 > 모든 프로그램 > **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **BIOS Configuration(BIOS 구성)**을 선택한 다음 **Security(보안)**를 선택합니다.
3. 오른쪽 창에서 **Setup Password(암호 설정)** 옆의 **Set(설정)**를 누릅니다.
4. **Enter Password(암호 입력)** 및 **Verify Password(암호 확인)** 상자에 암호를 입력하고 확인합니다.
5. **Passwords(암호)** 대화상자에서 **OK(확인)**를 누릅니다.
6. **Apply(적용)**를 누른 다음 **ProtectTools** 창에서 **OK(확인)**를 눌러 변경 사항을 저장합니다.

Computer Setup 관리자 암호 변경

Computer Setup 관리자 암호를 변경하려면 다음과 같이 하십시오.

1. 시작 > 모든 프로그램 > **HP ProtectTools Security Manager** 를 선택합니다.
2. 왼쪽 창에서 **BIOS Configuration(BIOS 구성)**을 선택한 다음 **Security(보안)**를 선택합니다.
3. 오른쪽 창에서 **Setup Password(암호 설정)** 옆의 **Change(변경)**를 누릅니다.
4. **Old Password(이전 암호)** 상자에 현재의 암호를 입력합니다.
5. **Enter Password(암호 입력)** 및 **Verify Password(암호 확인)** 상자에 새 암호를 설정하고 확인합니다.

6. **Passwords(암호)** 대화상자에서 **OK(확인)**를 누릅니다.
7. **Apply(적용)**를 누른 다음 **ProtectTools** 창에서 **OK(확인)**를 눌러 변경 사항을 저장합니다.

파워온 인증의 사전 공격 방어 동작

사전 공격은 보안 시스템을 중단시킬 목적으로 보안 시스템에 침입하기 위해 조직적으로 모든 가능한 암호를 테스트하는 방법입니다. **Embedded Security** 에 대한 사전 공격은 소유자 암호, 기본 사용자 암호 또는 암호 보호 키를 알아내려고 시도합니다. **Embedded Security** 는 향상된 **Dictionary Attack Defense**(사전 공격 방어) 기능을 제공합니다.

Dictionary Attack Defense(사전 공격 방어)

사전 암호 공격에 대한 **Embedded Security** 의 방어는 실패한 인증 시도를 감지하여 지정된 실패 임계값에 도달하면 **TPM** 을 임시로 비활성화하는 것입니다. 실패 임계값에 도달하면, **TPM** 이 비활성화되고 재부팅을 해야 할 뿐 아니라, 잠금 타임아웃이 더욱 길어집니다. 타임아웃 동안에는 정확한 암호를 입력해도 무시됩니다. 잘못된 암호를 입력하면 타임아웃이 두 배로 길어집니다.

이 프로세스에 대한 추가 설명서는 **Embedded Security** 도움말에 있습니다. **Welcome to the HP Embedded Security for ProtectTools Solution(HP Embedded Security for ProtectTools 솔루션 시작) > Advanced Embedded Security Operation(고급 Embedded Security 작업) > Dictionary Attack Defense(사전 공격 방어)**를 누릅니다.



주 정상적으로는 암호가 잘못된 경우 경고 메시지가 표시됩니다. 경고 메시지에는 **TPM** 이 비활성화되기 전까지 몇 번 더 암호를 입력할 수 있는 기회가 있는지 표시됩니다.

파워온 인증 프로세스는 운영체제가 로드되기 전에 **ROM** 에서 실행됩니다. 따라서, **Dictionary Attack Defense**(사전 공격 방어)가 작동 중이면 사용자에게 표시되는 경고는 X 키 기호뿐입니다.

2 HP BIOS Configuration for ProtectTools

기본 개념

ProtectTools 용 BIOS 구성은 **Computer Setup** 유틸리티 보안 및 구성 설정에 액세스할 수 있게 해줍니다. 이를 통해 **Computer Setup** 을 통해 관리되는 시스템 보안 기능을 **Windows** 에서 액세스할 수 있습니다.

BIOS 구성을 통해 다음을 수행할 수 있습니다.

- 파워온 암호 및 관리자 암호 관리
- 기타 파워온 인증 기능 구성(**Java** 카드 암호 및 내장 보안 인증 지원 기능 활성화 등)
- 하드웨어 기능 활성화/비활성화(**CD-ROM** 부팅 또는 여러 하드웨어 포트 등)
- 부팅 옵션 구성(멀티 부팅 활성화 및 부팅 순서 변경 등)



주 ProtectTools 용 BIOS 구성의 다양한 기능들은 **Computer Setup** 에서도 사용할 수 있습니다.

BIOS 설정 변경

BIOS 구성을 사용하면 다양한 컴퓨터 설정을 관리할 수 있으며, 이러한 설정은 시작 시 **F10** 키를 눌러 **Computer Setup** 유틸리티를 실행하여 액세스할 수도 있습니다. 설정 및 기능에 대한 정보는 컴퓨터와 함께 제공된 *Documentation and Diagnostics CD* 의 *Computer Setup(F10) 유틸리티 설명서* 를 참조하십시오. BIOS 구성에 대한 도움말 파일을 보려면 **Security Manager > BIOS Configuration (BIOS 구성) > Help(도움말)** 을 누릅니다.



주 ProtectTools BIOS 구성에 대한 자세한 지침은 ProtectTools 도움말 화면을 참조하십시오.

3 HP Embedded Security for ProtectTools

기본 개념

ProtectTools 용 Embedded Security 는 가능한 경우 사용자 데이터 또는 인증서에 대한 무단 액세스를 방지합니다. 이 모듈은 다음과 같은 보안 기능을 제공합니다.

- Microsoft EFS(Encrypting File System) 파일 및 폴더 암호화 강화
- 사용자 데이터 암호화를 위한 PSD(Personal Secure Drive) 생성
- 키 계층 구성 백업 및 복원 등의 데이터 관리 기능
- Embedded Security 소프트웨어를 사용하는 경우 보호된 디지털 인증서의 작동을 위해 MSCAPI 를 사용하는 타사 응용프로그램(예: Microsoft Outlook, Microsoft Internet Explorer) 및 PKCS#11 을 사용하는 타사 응용프로그램(예: Netscape) 지원

TPM(Trusted Platform Module) 내장 보안 칩은 ProtectTools Security Manager 의 보안 기능을 강화할 뿐만 아니라 더욱 다양한 기능을 사용할 수 있게 해줍니다. 예를 들어, ProtectTools 용 인증서 관리자는 사용자가 Windows 에 로그인할 때 TPM 내장 칩을 인증 요소의 하나로 사용할 수 있습니다. 일부 모델에서는 TPM 내장 보안 칩이 ProtectTools 용 BIOS 구성을 통해 액세스할 수 있는 향상된 BIOS 보안 기능을 제공하기도 합니다.

하드웨어는 TCG(Trusted Computing Group) 규격인 TPM 1.2 표준을 따르는 TPM 으로 구성되어 있습니다. 칩은 시스템 보드에 통합되어 있으며 일부 TPM 구현(구입 모델에 따라 다름)에서는 TPM 이 NIC 의 일부로 통합되어 있습니다. 이와 같은 NIC 및 TPM 구성에서는 온칩(on-chip) 메모리 및 오프칩(off-chip) 메모리, 기능, 펌웨어가 시스템 보드에 통합된 외장 플래시에 있습니다. 모든 TPM 기능은 플래시 또는 통신의 보안을 보장하기 위해 암호화되거나 보호됩니다.

이 소프트웨어는 PSD 라는 기능도 제공합니다. PSD 는 EFS 기반 파일/폴더 암호화에 추가된 보안 기능으로, AES(Advanced Encryption Standard) 암호화 알고리즘을 사용합니다. HP ProtectTools PSD (Personal Secure Drive)는 TPM 을 활성화하고 적합한 소프트웨어를 통해 소유권을 얻은 후 사용자 구성을 초기화해야만 작동합니다.

설정 절차



주의 보안 위험을 줄이기 위해 IT 관리자는 TPM 내장 보안 칩을 바로 초기화하는 것이 좋습니다. TPM 내장 보안 칩이 초기화되지 않은 경우 무단 사용자 또는 웜 바이러스가 컴퓨터에 액세스하거나, 바이러스가 TPM 내장 보안 칩을 초기화하여 PC에 대한 액세스를 제한할 수 있습니다.

TPM 내장 보안 칩은 BIOS Computer Setup 유틸리티, ProtectTools 용 BIOS 구성 또는 HP Client Manager를 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.



주 ProtectTools Embedded Security에 대한 자세한 지침은 ProtectTools 도움말 화면을 참조하십시오.

4 HP Credential Manager for ProtectTools

기본 개념

ProtectTools 용 인증서 관리자에는 다음과 같은 다양한 기능이 있어서 안전하고 편리한 컴퓨팅 환경을 제공합니다.

- Microsoft Windows 로그인 시 Java 카드 또는 생체인식 리더 등을 사용하여 암호 대체
- 웹 사이트, 응용프로그램 및 보호된 네트워크 리소스에 대한 자격 증명(사용자 ID 및 암호)을 자동으로 기억하는 SSO(Single Sign On) 기능
- Java 카드 및 생체인식 리더와 같은 선택 사양 보안 장치 지원
- 추가 보안 설정 지원(예: 컴퓨터 잠금 해제 및 응용프로그램 액세스 시 선택 사양 보안 장치를 통한 인증 요구)
- TPM 내장 보안 칩을 사용하여 저장된 암호에 대해 보다 강력한 암호화 제공

시작 절차

인증서 관리자를 시작하려면(사용 가능한 경우) 다음과 같이 하십시오.

1. 시작 > 제어판 > 보안 센터 > **ProtectTools Security Manager > Credential Manager**(인증서 관리자)를 누릅니다.
2. 창의 오른쪽 상단 모서리 부분에 있는 **Log On(로그온)**을 누릅니다.

다음과 같은 방법을 사용하여 인증서 관리자에 로그인할 수 있습니다.

- 인증서 관리자 로그인 마법사(권장)
- ProtectTools Security Manager



주 Windows 로그인 화면의 인증서 관리자 로그인 프롬프트를 통해 인증서 관리자에 로그인 하면 Windows 에도 동시에 로그인됩니다.

처음 로그인

인증서 관리자를 처음으로 연 경우 일반 **Windows** 로그인 암호로 로그인합니다. 그러면 **Windows** 로그인 자격 증명을 사용하여 인증서 관리자 계정이 자동으로 생성됩니다.

인증서 관리자에 로그인한 후 지문이나 **Java** 카드와 같은 인증서를 추가로 등록할 수 있습니다.

다음부터는 로그인할 때 로그인 정책을 선택하고 등록된 인증서를 원하는 대로 조합하여 사용할 수 있습니다.



주 ProtectTools Security Manager 에 대한 자세한 지침은 **ProtectTools** 도움말 화면을 참조하십시오.

5 HP Java Card Security for ProtectTools

기본 개념

ProtectTools 용 Java 카드 보안은 Java 카드 리더(선택 사양)가 장착된 컴퓨터에서 Java 카드의 설정 및 구성을 관리합니다.

ProtectTools 용 Java 카드 보안으로 다음을 수행할 수 있습니다.

- Java 카드 보안 기능에 액세스합니다.
- Java 카드를 초기화하여 ProtectTools 용 인증서 관리자 등과 같은 다른 ProtectTools 모듈과 함께 사용할 수 있도록 합니다.
- 가능한 경우, **Computer Setup** 유틸리티와 함께 사용하여 사전 부팅 환경에서 Java 카드 인증을 활성화하고 관리자 및 사용자에 대해 개별 Java 카드를 구성할 수 있습니다. 이렇게 하려면 운영 체제를 로드하기 전에 사용자가 Java 카드를 삽입하고 PIN(선택적)을 입력해야 합니다.
- 가능한 경우, Java 카드 사용자 인증에 사용되는 암호를 설정하고 변경합니다.
- 가능한 경우, Java 카드에 저장된 Java 카드 BIOS 암호를 백업 및 복원합니다.
- 가능한 경우, Java 카드에 BIOS 암호를 저장합니다.



주 ProtectTools Security Manager 에 대한 자세한 지침은 ProtectTools 도움말 화면을 참조하십시오.

6 타사 솔루션

TPM 이 설치된 플랫폼에는 TSS(TCG Software Stack) 및 내장 보안 소프트웨어가 모두 필요합니다. TSS 는 모든 모델에서 제공되며 내장 보안 소프트웨어는 일부 모델의 경우 별도로 구입해야 합니다. 이러한 경우 타사의 내장 보안 소프트웨어를 구입한 고객을 지원하기 위해 **NTRU TSS** 가 제공됩니다. 타사 솔루션 중에서는 **Wave Embassy Trust Suite** 를 사용하는 것이 좋습니다.

7 원격 배치용 HP Client Manager

배경

TPM(Trusted Platform Module)이 장착된 HP Trustworthy 플랫폼은 기본적으로 TPM 이 비활성화된 상태로 제공됩니다. TPM 활성화는 HP BIOS 적용 정책으로 보호되는 관리 옵션입니다. BIOS 구성 옵션(F10 옵션)에 들어가서 TPM 을 활성화하려면 관리자가 자리에 있어야 합니다. 또한 TCG(Trusted Computing Group)에서는 사용자가 실제로 자리에서 TPM 을 실행하도록 요구합니다. 이렇게 함으로써 옵트인 모델을 통해 사용자의 개인 정보 보호 권리를 보장하고, 악성 응용프로그램, 바이러스 또는 트로이 목마 등이 악의적 사용을 위해 TPM 을 활성화하지 못하도록 할 수 있습니다. 이러한 실재 증명과 관리자의 현장 상주 요건은 IT 관리자에게 이러한 기법을 전사적으로 구현해야 하는 과제를 부여합니다.

초기화

HPCM(HP Client Manager)은 기업 환경에서 원격으로 TPM 을 활성화하고 그 소유권을 취득할 수 있는 방법을 제공합니다. 이 방법은 IT 관리자의 실재는 요구하지 않으나 TCG 요구 사항은 충족합니다.

HPCM 을 사용하면 IT 관리자가 특정 BIOS 옵션을 설정하고 시스템을 재부팅하여 원격 시스템에서 TPM 을 활성화할 수 있습니다. 기본적으로 BIOS 는 재부팅 시 프롬프트를 표시하며 최종 사용자는 이에 대해 키를 눌러 TCG 에서 요구한 대로 실제로 자리에 있었다는 것을 증명해야 합니다. 그러면 원격 시스템 부팅이 진행되고 스크립트가 완료되어 시스템에서 TPM 소유권을 취득하게 됩니다. 이 과정에서 응급 복구 아카이브 및 응급 복구 토큰이 IT 관리자가 지정한 위치에 생성됩니다.

HPCM 은 사용자가 암호를 선택할 수 있도록 허용해야 하기 때문에 원격 시스템에서 TPM 사용자 초기화를 실행하지 않습니다. TPM 사용자 초기화는 반드시 해당 시스템의 최종 사용자가 수행해야 합니다.

유지 관리

HP Client Manager 를 사용하면 사용자 암호를 IT 관리자에게 알리지 않고 원격으로 재설정할 수 있습니다. 또한, 원격으로 사용자 인증서를 복구할 수도 있습니다. 이 두 가지 기능을 수행하려면 정확한 관리자 암호를 제공해야 합니다.

8 문제 해결

ProtectTools 용 인증서 관리자

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 1에 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 로그인 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 1에서만 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 로그인한 다음 인증서 관리자에서 도메인 ID 를 등록한 경우	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 변

증상	설명	해결 방법
	발생합니다. 도메인 관리자가 인증서 관리자에서 Windows 암호를 변경하려고 하면 User account restriction(사용자 계정 제한) 이라는 로그온 실패 오류 메시지가 나타납니다.	경 옵션을 통해서 암호를 변경할 수 있습니다. 하지만 로컬 PC에 물리적 계정을 가지고 있지 않으므로 인증서 관리자에서는 로그인에 사용되는 암호만을 변경할 수 있습니다.
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.	HP에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
Corel WordPerfect 12 암호 GINA와 관련한 비호환성 문제.	인증서 관리자에 로그인하여 WordPerfect에서 문서를 작성한 후 암호로 보호되는 문서로 저장한 경우 인증서 관리자는 암호 GINA를 수동 또는 자동으로 찾아내거나 알아낼 수 없습니다.	HP에서는 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 SSO는 다시 시작할 때 Connect(접속) 가 아닌 Save As(다른 이름으로 저장) 를 표시합니다.	HP에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
ATI Catalyst 구성 마법사를 인증서 관리자와 함께 사용할 수 없음.	인증서 관리자 SSO가 ATI Catalyst 구성 마법사와 충돌합니다.	인증서 관리자 SSO를 비활성화하십시오.
TPM 인증으로 로그인할 때 화면의 Back(뒤로) 버튼을 누르면 다른 인증 방법을 선택하는 옵션을 건너뛴다.	인증서 관리자에 대해 TPM 로그인 인증을 사용하는 사용자가 암호를 입력하는 경우 Back(뒤로) 버튼이 제대로 작동하지 않고 Windows 로그인 화면이 바로 표시됩니다.	HP에서는 제품 향상을 위해 해결 방법을 찾고 있습니다.
인증서 관리자가 구성과는 다르게 대기 상태가 해제될 때 자동으로 실행됨	use Credential Manager log on to Windows(Windows에 인증서 관리자 로그인 사용) 를 옵션으로 선택하지 않았는데, 시스템이 S3 일시 정지 모드로 들어간 후 작업을 재개하면 Windows에 인증서 관리자 로그온이 실행됩니다.	관리자 암호를 설정하지 않으면 인증서 관리자의 계정 제한 기능으로 인해 사용자가 인증서 관리자를 통해 Windows에 로그인할 수 없습니다. <ul style="list-style-type: none"> • 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. <ol style="list-style-type: none"> 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 TPM으로 보	TPM 모듈이 제거되거나 손상된 경우 TPM으로 보호되는 인증서 관리자의 모든 인증서가 소실됩니다.	이는 설계상의 이유입니다.

증상	설명	해결 방법
호되는 인증서 관리자의 모든 인증서가 소실됨.		TPM 모듈은 인증서 관리자의 인증서를 보호하도록 설계되었습니다. TPM 모듈을 제거하기 전에 인증서 관리자에서 ID 를 백업하도록 하십시오.
인증서 관리자가 Windows 2000 에서 기본 로그인으로 설정되지 않음.	Windows 2000 설치 과정에서 로그인 정책이 수동 또는 자동 로그온 관리로 설정됩니다. 자동 로그온이 선택된 경우 Windows 기본 레지스트리 설정에 따라 기본 자동 관리 로그인 값인 1 로 설정되며 인증서 관리자 설정보다 이 설정이 우선합니다.	이는 설계상의 이유입니다. 입력 생략을 위한 자동 관리 로그인 값에 대한 운영체제 수준 설정을 수정하려는 경우 HKEY_LOCAL_MACHINE/Software/Microsoft/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 로그인 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 로그인할 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 로그인 창에서 insert card(카드 삽입) 메시지가 표시됨.	Windows Credential Manager 시작 화면에, 장착된 Java 카드 리더가 없는 경우 insert card(카드 삽입) 를 사용하여 로그인할 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 로그인 인증서(암호, 지문 또는 Java 카드)에 관계없이 Windows 로그인 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.
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, ProtectTools 용 BIOS 구성 또는 HP Client

증상	설명	해결 방법
		<p>Manager 를 사용하여 활성화할 수 있습니다. TPM 내장 보안 칩을 활성화하려면 다음과 같이 하십시오.</p> <ol style="list-style-type: none"> 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. <p>향후 출시될 소프트웨어 릴리스를 위해 해결책을 모색 중입니다.</p>
<p>보안 Restore Identity(ID 복원) 프로세스에서 가상 토큰과의 연결이 소실됨.</p>	<p>ID 를 복원하면 인증서 관리자의 로그인 화면에서 가상 토큰 위치와의 연결이 손실됩니다. 인증서 관리자에 등록된 가상 토큰이 있더라도 연결을 복원하려면 토큰을 재등록해야 합니다.</p>	<p>이는 설계상의 이유입니다.</p> <p>ID 를 유지하지 않고 인증서 관리자를 제거하면 토큰의 시스템(서버) 부분이 손상되어 토큰의 클라이언트 부분이 ID 복원을 통해 복원되더라도 더 이상 해당 토큰을 사용하여 로그인할 수 없게 됩니다.</p> <p>HP 에서 장기적인 문제 해결책을 모색하고 있습니다.</p>

ProtectTools 용 내장 보안

증상	설명	해결 방법
PSD의 암호화 폴더, 하위 폴더, 파일들에서 오류 메시지 발생	파일 및 폴더를 PSD로 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 PSD로 이동하면 자동으로 해당 파일/폴더가 암호화됩니다. 따라서 이중으로 암호화할 필요가 없습니다. PSD에서 EFS를 사용하여 이중으로 암호화를 시도할 경우 이 오류 메시지가 나타납니다.
멀티 부팅 플랫폼에서 다른 OS에 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 EFS의 특징입니다. Embedded Security 는 Microsoft EFS 소프트웨어를 사용하며, EFS는 모든 관리자에 대해 파일/폴더 액세스 권한을 유지합니다.
Windows 2000에서는 EFS로 암호화된 폴더가 녹색으로 강조 표시되지 않습니다.	EFS로 암호화된 폴더는 Windows XP에서는 녹색으로 강조 표시되지만 Windows 2000에서는 강조 표시되지 않습니다.	이는 설계상의 이유입니다. Windows 2000에서는 암호화된 폴더가 녹색으로 강조 표시되지 않고 Windows XP에서는 강조 표시되는 것은 EFS의 특징입니다. 이 특징은 Embedded Security TPM 의 설치 여부와는 상관 없습니다.
Windows 2000에서 EFS로 암호화된 파일을 보기 위해 암호가 필요하지 않음	사용자가 Embedded Security 를 설정하고 관리자로 로그인한 후 로그오프하고 그런 다음 다시 관리자로 로그인한 경우 Windows 2000에서 파일/폴더를 암호 없이 계속 볼 수 있습니다. 이러한 경우는 Windows 2000에서 첫 번째 관리자 계정에서만 발생하며 두 번째 로그인하는 관리자 계정에서는 발생하지 않습니다.	이는 설계상의 이유입니다. Windows 2000의 EFS 특징입니다. Windows XP의 EFS는 기본적으로 사용자가 암호 없이 파일/폴더를 열도록 허용하지 않습니다.
FAT32 파티션으로 복원된 드라이브에 소프트웨어를 설치할 수 없음	FAT32를 사용하여 하드 드라이브 복원을 시도할 경우 파일/폴더에 대해 EFS를 사용하여 아무런 암호화 옵션을 사용할 수 없습니다.	이는 설계상의 이유입니다. Microsoft EFS는 NTFS만을 지원하며 FAT32에서는 사용할 수 없습니다. 이는 Microsoft의 EFS와 관련된 특징으로서 HP ProtectTools 소프트웨어와는 상관 없습니다.
Windows 2000 사용자가 숨김(\$\$) 공유를 통해 PSD에 네트워크로 연결할 수 있음	Windows 2000 사용자가 숨김(\$\$) 공유를 통해 PSD에 네트워크로 연결할 수 있습니다. 숨김 공유는 숨김(\$\$) 공유를 사용하여 네트워크를 통해 액세스할 수 있습니다.	일반적으로 PSD는 네트워크 상에서 공유되지 않으나 Windows 2000의 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 ACL이 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 EFS와 Symantec Antivirus	암호화된 파일은 Symantec Antivirus 또는 Norton Antivirus 2005의 바이러스 검색에 영향을 줍니다. 검색 과정에서	HP ProtectTools Embedded Security EFS 파일을 검색하는 데 소요되는 시간을 단축하려면 검색을 시작하기 전에 암호화 암호를 입력하거나 암호화를 해제합니다.

증상	설명	해결 방법
또는 Norton Antivirus 를 함께 사용할 경우 암호화/암호 해독 및 검색 시간이 오래 걸림	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 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.
전원 차단 후 Embedded Security 초기화 과정에서 소유권을 얻는 중 오류 발생	Embedded Security 칩을 초기화하는 동안 전원이 차단되면 다음과 같은 문제가 발생합니다. <ul style="list-style-type: none">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. <ol style="list-style-type: none">1. 컴퓨터를 시작하거나 다시 시작합니다.2. 화면에 F10=Setup 메시지가 나타나면(모니터 표시등에 녹색불이 들어오면) F10 을 누릅니다.3. 해당 언어 옵션을 선택합니다.4. Enter 키를 누릅니다.5. Security(보안) > Embedded Security 를 선택합니다.6. Embedded Security Device(Embedded Security 장치) 옵션을 Enable(사용)로 설정합니다.7. F10 을 눌러 변경 사항을 적용합니다.8. File(파일) > Save Changes and Exit(변경 저장 후 종료)를 선택합니다.9. Enter 를 누릅니다.10. F10 을 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) 유틸리티가 암호가 필요합니다. 모듈이 활성화되면 사용자는 암호를 삭제할 수 있습니다. 따라서 시스템에 직접 액세스할 수 있는 사용자가 TPM 모듈	이는 설계상의 이유입니다. Computer Setup(F10) 유틸리티 암호는 암호를 아는 사용자만 삭제할 수 있습니다. 그러나 Computer Setup (F10) 유틸리티 암호를 항상 보호할 것을 권장합니다.

증상	설명	해결 방법
	을 재설정하고 데이터 손실이 발생할 수 있습니다.	
대기 상태 후 시스템을 활성화할 때 PSD 암호 상자가 표시되지 않음	PSD 생성 후 사용자가 로그인하면 TPM에서 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 로그인 후 다시 로그인해야 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 2000에서 Microsoft EFS의 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 2000의 첫 번째 관리자 계정에 서만 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. 이 문제는 Microsoft EFS의 문제입니다. 자세한 내용은 http://www.microsoft.com 에서 Microsoft Knowledge Base Technical Article Q257705를 참조하십시오. 문서는 관리자만 열 수 있습니다.
인증서를 볼 때 신뢰되지 않은 것으로 표시됨	HP ProtectTools를 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.
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. <ol style="list-style-type: none">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 PSD가 계속 표시되며 PSD에 데이터를 추가하거나 수정해도 오류가 발생하지 않습니다. 시스템을 다시 시작한 후 이동식 저장 장치를 제거한 동안 발생한 파일 변경 사항이 PSD에 반영되지 않습니다.	이 문제는 새로운 데이터를 생성하거나 이전하는 작업이 완료되기 전에 사용자가 PSD를 액세스하여 하드 드라이브를 제거한 경우에만 발생합니다. 이동식 하드 드라이브가 장착되지 않았을 때 사용자가 PSD에 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 TPM을 비활성화하지 않고 설치를 제거하거나, 먼저 관리 도구를 통해 TPM을 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.	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) 를 선택합니다.

증상	설명	해결 방법
	<p>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(아니오)를 선택하면 관리 도구가 열리지 않고 설치 제거 프로세스가 진행됩니다.</p>	
<p>두 개의 사용자 계정에 PSD 를 생성한 후 128MB 시스템 구성에서 빠른 사용자 전환을 사용할 경우 시스템 잠금이 가끔씩 발생함</p>	<p>최소 RAM 사양으로 빠른 사용자 전환을 사용할 경우 로그인 화면이 표시되지 않고 검정색 화면이 표시되면서 키보드와 마우스가 작동하지 않을 수 있습니다.</p>	<p>주원인은 메모리가 낮은 구성에서 시간이 오래 걸리기 때문일 수 있습니다.</p> <p>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.</p> <p>이를 해결하려면 시스템을 재부팅한 후 메모리 구성을 늘리 방법을 사용합니다(HP 는 기본적으로 보안 모듈에 대한 128MB 구성은 제공하지 않음).</p>
<p>EFS 사용자 인증(암호 요청) 시간이 초과되고 access denied(액세스 거부) 메시지가 표시됨</p>	<p>OK(확인)를 누르거나 시간이 만료되어 대기 상태에서 돌아오면 EFS 사용자 인증 암호가 다시 열립니다.</p>	<p>이는 설계상의 이유입니다. Microsoft EFS 와 관련된 문제를 방지하기 위해 오류 메시지를 표시하는 30 초 워치독 타이머가 개발되었습니다.</p>
<p>일본어 버전 설정 과정에서 기능 설명에 심각한 이상이 보임</p>	<p>설치 마법사의 사용자 설정 옵션의 기능 설명 부분이 잘립니다.</p>	<p>이 오류는 다음 버전에서 수정될 것입니다.</p>
<p>암호를 입력하라는 프롬프트에 암호를 입력하지 않아도 EFS 암호화가 작동함</p>	<p>사용자 암호 프롬프트 시간이 초과될 때까지 두면 파일이나 폴더에 대해 암호화가 계속 작동합니다.</p>	<p>이 기능은 Microsoft EFS 암호화의 기능이므로 암호 인증이 필요하지 않습니다. 암호 해독 시에는 사용자가 암호를 입력해야 합니다.</p>
<p>사용자 초기화 마법사에서 전자 우편 보안 옵션을 선택하지 않거나 사용자 정책에서 전자 우편 보안 구성을 비활성화해도 전자 우편 보안이 지원됨</p>	<p>내장 보안 소프트웨어와 마법사는 전자 우편 클라이언트(Outlook, Outlook Express, Netscape 등)의 설정을 제어하지 않습니다.</p>	<p>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.</p>
<p>대량의 배치 작업을 동일한 PC 에서 두 번째로 실행하거나 이전에 초기화한 PC 에서 실행할 경우 응급 복구 및 응급 토큰 파일을 덮어쓰. 복구 시 새 파일이 사용되지 않음</p>	<p>이전에 초기화한 HP ProtectTools Embedded Security 시스템에서 대량의 배치 작업을 실행할 경우 xml 파일을 덮어쓰므로 기존의 복구 아카이브 및 복구 토큰이 노후화됩니다.</p>	<p>xml 파일 덮어쓰기 문제를 해결하기 위한 작업이 진행 중이며 향후 SoftPaq 에서는 이 솔루션을 제공할 예정입니다.</p>

증상	설명	해결 방법
Embedded Security 에서 사용자가 복원 작업 중 자동 로그인 스크립트가 작동하지 않음	<p>이 오류는 다음과 같은 경우에 발생합니다.</p> <ul style="list-style-type: none"> • 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 로그인할 수 있는지를 사용자에게 묻습니다. 사용자가 Yes(예)를 선택하면 텍스트 상자에 SPEmRecToken 위치가 자동으로 나타납니다. <p>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.</p>	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	<p>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.</p> <p>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 않은지 확인하십시오)라는 메시지가 표시됩니다. 사용자가 시스템을 재부팅하여 PSD 를 삭제해야 하며 재부팅 후에는 PSD 가 표시되지 않습니다.</p>	<p>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.</p> <p>해결책: 다음 재부팅 후 에뮬레이션 로딩이 실패하면 사용자가 이전의 PSD 에뮬레이션을 삭제하고 새 PSD 를 생성할 수 있습니다.</p>

증상	설명	해결 방법
자동 백업 아카이브에서 복원 시 내부 오류가 발생함	<p>다음과 같은 경우,</p> <ul style="list-style-type: none"> • 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 <p>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.</p>	<p>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)</p> <p>복원 사유와 일치하는 정확한 .xml 파일을 선택해야 합니다.</p> <p>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.</p>
보안 시스템이 여러 사용자와 관련된 복원 오류를 표시함	<p>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.</p>	<p>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.</p> <p>또한 사용자는 전체 시스템 백업을 복원해야 합니다. 아카이브 백업은 개별적으로 복원할 수 있습니다.</p>
시스템 ROM 을 기본값으로 재설정하면 TPM 이 비활성화됨	<p>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.</p>	<p>다음과 같이 BIOS 에서 TPM 을 활성화합니다.</p> <p>Computer Setup(F10) 유틸리티를 열고 Security > Device security 를 선택한 후 필드를 Hidden 에서 Available 로 수정합니다.</p>
자동 백업이 매핑된 드라이브에서 작동하지 않음	<p>관리자가 Embedded Security 에서 자동 백업을 설정하면 Windows > 작업 > 예약된 작업에 하나의 항목으로 추가됩니다 Windows 의 예약된 작업은 백업을 실행하기 위해 NT AUTHORITY\SYSTEM 을 사용하도록 설정되어 있습니다. 이 프로세스는 로컬 드라이브에 대해서는 제대로 실행됩니다.</p> <p>관리자가 자동 백업을 매핑된 드라이브에 저장하도록 구성한 경우에는 NT AUTHORITY\SYSTEM 이 매핑 드라이브를 사용할 수 있는 권한을 갖고 있지 않으므로 이 프로세스가 실패합니다.</p> <p>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 백</p>	<p>이 문제를 해결하려면 NT AUTHORITY\SYSTEM 을 (컴퓨터 이름)\(관리자 이름)으로 변경하십시오. 이 설정은 예약된 작업을 수동으로 생성할 경우의 기본 설정입니다.</p> <p>향후 제품 릴리스에서는 기본 설정에 컴퓨터 이름\관리자 이름을 포함할 예정입니다.</p>

증상	설명	해결 방법
	업이 특정 시간에 예약된 경우에는 실패 메시지 없이 백업이 실패합니다.	
Embedded Security GUI에서 Embedded Security 상태를 일시적으로 비활성화할 수 없음	현재 4.0 소프트웨어는 HP Notebook 1.1B 구현에 맞춰 설계되었으며 HP Desktop 1.2 구현을 지원하지 않습니다. 이 비활성화 옵션은 TPM 1.1 플랫폼에 대한 소프트웨어 인터페이스에서 계속 지원됩니다.	다음 릴리스에서는 이 문제가 해결될 것입니다.

영향 받은 소프트웨어-증상	설명	해결 방법
<p>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 Manager를 설치해야만 보안 응용 프로그램을 설치할 수 있습니다)</p>	<p>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 Manager를 설치해야 합니다.</p>	<p>보안 플러그인을 설치하기 전에 HP ProtectTools Security Manager 소프트웨어를 설치해야 합니다.</p>
<p>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</p>	<p>dc7600 및 Broadcom 지원 TPM 을 포함하는 모델용 TPM 펌웨어 유틸리티의 정상적인 동작입니다.</p> <p>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.</p> <p>EK 가 있을 경우 업그레이드 시 소유자 인증이 필요하므로 TPM 소유자가 있어야 합니다. 업그레이드가 완료되면 플랫폼을 다시 시작해야 새로운 펌웨어가 적용됩니다.</p> <p>BIOS TPM 의 설정을 기본값으로 복원하면 소유권이 삭제되면서 Embedded Security 소프트웨어 플랫폼과 사용자 초기화 마법사를 구성할 때까지 펌웨어 업데이트를 수행할 수 없습니다.</p> <p>*펌웨어 업데이트 후에는 반드시 재부팅하도록 하십시오. 재부팅을 해야만 펌웨어 버전이 업데이트됩니다.</p>	<ol style="list-style-type: none"> 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. <ol style="list-style-type: none"> a. 시작을 누릅니다. b. 제어판을 누릅니다. c. 프로그램 추가/제거를 누릅니다. d. Microsoft .NET Framework 1.1 이 목록에 있는지 확인합니다. 4. 하드웨어 및 소프트웨어 구성을 확인합니다. <ol style="list-style-type: none"> a. 시작을 누릅니다. b. 모든 프로그램을 누릅니다. c. HP ProtectTools Security Manager 를 누릅니다. d. 트리 메뉴에서 Embedded Security 를 선택합니다. e. More Details(자세한 정보)를 누릅니다. 구성이 다음과 같아야 합니다. <ul style="list-style-type: none"> • 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
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.	<ul style="list-style-type: none"> 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) <p>5. 펌웨어 버전이 2.18 이상이 아닐 경우 TPM 펌웨어를 다운로드합니다. TPM Firmware SoftPak은 http://www.hp.com 에서 다운로드할 수 있습니다.</p>
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. <ul style="list-style-type: none"> PSD 삭제 사용자 설정에 대한 악의적인 수정 보안 정책 및 기능의 사용 불가 	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. <p>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.</p> <p>관리자가 최종 사용자 권한과 사용자 액세스에 대해 "최선의 방법"을 수행할 것을 권장합니다.</p> <p>무단 사용자에게는 관리 권한을 부여하지 말아야 합니다.</p>
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 로그인할 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
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)	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)	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 활성화 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 SoftPak 에 적용될 예정입니다.
부팅 중 보안 파워온 인증이 BIOS 암호를 오버랩함	파워온 인증은 사용자가 시스템에 로그인할 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 사용자 암호를 변경한 후 Computer Setup 을 실행할 때 BIOS 에서 기존 암호와 새 암호를 모두 묻음	Embedded Security Windows 소프트웨어에서 사용자 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

AES(Advanced Encryption Standard) 128 비트 블록 데이터 대칭 암호화 기술입니다.

API(Application Programming Interface) 응용프로그램에서 다양한 작업을 수행하기 위해 사용할 수 있는 일련의 내부 운영체제 기능입니다.

BIOS 보안 모드 활성화된 경우 사용자 인증을 위해 Java 카드 및 유효한 PIN 을 필요로 하는 ProtectTools 용 Java 카드 보안 설정입니다.

BIOS 프로파일 다른 계정에 저장 및 적용할 수 있는 BIOS 구성 설정 그룹입니다.

CSP(Cryptographic Service Provider) 특정 암호화 기능을 수행하기 위해 정의된 인터페이스에서 사용할 수 있는 암호화 알고리즘의 제공자 또는 라이브러리로 MSCAPI 와 함께 작동하는 소프트웨어 구성 요소입니다.

EFS(Encrypting File System) 선택한 폴더 내의 모든 파일과 하위 폴더를 암호화하는 시스템으로 Microsoft Windows 2000 이상 버전에서 제공되는 투명한 파일 암호화 서비스입니다.

ID ProtectTools 인증서 관리자에서 특정 사용자에 대한 계정 또는 프로파일처럼 취급되는 인증서 및 설정 그룹입니다.

Java 카드 작은 크기의 하드웨어로 신용 카드와 크기와 모양이 비슷하며 소유자에 대한 식별 정보를 저장합니다. 컴퓨터에서 소유자를 인증하는 데 사용됩니다.

Java 카드 관리자 암호 시작 또는 재시작 시 식별을 위해 Computer Setup 에서 컴퓨터와 관리자 Java 카드를 연결하는 암호입니다. 이 암호는 관리자가 수동으로 설정하거나 임의로 생성할 수 있습니다.

Java 카드 사용자 암호 시작 또는 재시작 시 식별을 위해 Computer Setup 에서 컴퓨터와 사용자 Java 카드를 연결하는 암호입니다. 이 암호는 관리자가 수동으로 설정하거나 임의로 생성할 수 있습니다.

LPC(Low Pin Count) 플랫폼 칩셋과 연결하기 위해 HP ProtectTools Embedded Security 장치에서 사용하는 인터페이스를 정의합니다. 33Mhz 클럭 및 몇 개의 제어/상태 핀과 함께 4 비트의 주소/데이터 핀으로 버스가 구성됩니다.

MSCAPI(Microsoft Cryptographic API 또는 CryptoAPI) Windows 운영체제에 암호화 응용프로그램용 인터페이스를 제공하는 Microsoft 제공 API 입니다.

PKCS(Public Key Cryptographic Standards) 암호화 및 암호 해독에 사용하는 공개 키/개인 키를 정의하고 사용하는 표준입니다.

PKI(Public Key Infrastructure) 공개 키/개인 키 암호화 및 암호 해독을 사용하는 보안 시스템 구현을 정의하는 일반적인 용어입니다.

PSD(Personal Secure Drive) 중요한 데이터를 위한 보호된 저장 영역을 제공합니다. HP ProtectTools Embedded Security 에서 제공하는 기능으로, 이 응용프로그램은 사용자의 컴퓨터에 가상 드라이브를 생성하며 가상 드라이브로 옮겨진 파일/폴더는 자동으로 암호화됩니다.

S/MIME(Secure Multipurpose Internet Mail Extensions) PKCS 를 사용하는 보안 전자 메시징의 사양입니다. S/MIME 은 디지털 서명을 통한 인증과 암호화를 통한 개인 정보 보호 기능을 제공합니다.

SSO(Single Sign On) 인증 데이터를 저장하고 인터넷 및 Windows 응용프로그램에 액세스할 때 암호 인증을 요구하는 인증서 관리자를 사용할 수 있게 하는 기능입니다.

Stringent security(철저한 보안) 파워온 및 관리자 암호와 기타 파워온 인증 방식에 대해 강화된 보안을 제공하는 BIOS 구성 내의 보안 기능입니다.

TCG(Trusted Computing Group) “Trusted PC(신뢰할 수 있는 PC)”라는 개념을 장려하기 위해 구성된 업계 컨소시엄입니다. TCG가 TCG 로 대체되었습니다.

TCPA(Trusted Computing Platform Alliance) 신뢰할 수 있는 컴퓨팅 연합으로 현재 TCG 로 대체되었습니다.

TPM(Trusted Platform Module) 내장 보안 칩(일부 모델만 해당) 매우 중요한 사용자 정보를 악의적 공격으로부터 보호할 수 있는 통합 보안 칩입니다. 해당 플랫폼에서 트러스트 루트(Root-of-Trust)가 됩니다. TPM 은 TCG(Trusted Computing Group)의 사양을 준수하는 암호화 알고리즘 및 기능을 제공합니다. TPM 하드웨어 및 소프트웨어는 EFS 와 PSD(Personal Secure Drive)에서 사용되는 키를 보호함으로써 EFS 및 PSD 의 보안을 강화합니다. TPM 이 없는 시스템에서는 EFS 와 PSD 에서 사용되는 키가 일반적으로 하드 드라이브에 저장됩니다. 이것은 키의 보안을 취약하게 만듭니다. TPM 카드가 장착된 시스템의 경우에는 TPM 칩 상의 고정 TPM 사설 저장 루트 키가 EFS 와 PSD 에서 사용되는 키를 "래핑"하거나 보호합니다. 개인 키를 추출하기 위해 TPM 에 침입하는 것은 키를 얻기 위해 시스템 하드 드라이브를 해킹하는 것보다 훨씬 어렵습니다. 또한 TPM 은 Microsoft Outlook 및 Outlook Express 에서 S/MIME 을 통해 보안 전자 우편의 보안을 강화합니다. TPM 은 CSP (Cryptographic Service Provider)의 기능을 수행합니다. 키와 인증서는 TPM 하드웨어에 의해 생성 및/또는 지원되며, 소프트웨어만으로 구현된 수준보다 훨씬 강화된 보안을 제공합니다.

TSS(TCG Software Stack) TPM 이용에 필요한 서비스를 제공하며 그와 동일한 보안은 필요로 하지 않습니다. TPM 기능에 액세스하기 위한 표준 소프트웨어 인터페이스를 제공합니다. 키 백업, 키 마이그레이션, 플랫폼 인증 및 증명 등 TPM 의 기능을 완전히 사용하기 위해 응용프로그램들은 TSS 에 바로 기록합니다.

USB 토큰 사용자에 대한 식별 정보를 저장하는 보안 장치입니다. Java 카드나 생체인식 리더와 같이 컴퓨터에서 소유자를 인증하는 데 사용됩니다.

Windows 사용자 계정 네트워크나 개인 컴퓨터에 로그인할 수 있는 권한이 있는 개인의 프로필입니다.

가상 토큰 Java 카드 및 리더와 작동 방식이 매우 유사한 보안 기능입니다. 토큰은 컴퓨터 하드 드라이브나 Windows 레지스트리에 저장되고, 가상 토큰으로 로그인하면 인증 과정을 완료하기 위해 사용자 PIN 을 입력하라는 메시지가 나타납니다.

네트워크 계정 로컬 컴퓨터, 작업 그룹 또는 도메인 상의 Windows 사용자 또는 관리자 계정입니다.

도메인 네트워크의 일부로 공통 디렉토리 데이터베이스를 공유하는 컴퓨터 그룹입니다. 도메인은 고유한 이름을 가지며 각각 공통된 규칙과 절차의 집합이 있습니다.

디지털 서명 파일과 함께 전송되는 데이터로 자료의 발신자를 확인하고, 파일이 서명된 이후로 수정되지 않았다는 것을 확인해 줍니다.

디지털 인증서 디지털 인증서 소유자의 ID 와 디지털 정보에 서명하는 데 사용되는 한 쌍의 전자 키를 바인딩하는 방식으로 개인이나 회사의 신분을 확인하는 전자 인증서입니다.

마이그레이션 키와 인증서를 관리, 복원 및 전달하는 작업입니다.

생체인식 사용자를 식별하기 위해 지문과 같은 물리적 특성을 사용하는 인증서 범주입니다.

암호 표기법 데이터 암호화 및 암호 해독 방법으로, 특정인만 데이터를 디코딩할 수 있도록 하는 것입니다.

암호 해독 암호화된 데이터를 일반 텍스트로 변환하기 위해 암호 표기법에 사용되는 절차입니다.

암호화 권한이 없는 수신자가 데이터를 읽지 못하도록 일반 텍스트를 암호화된 텍스트로 변환하기 위해 암호 표기법에서 사용하는 절차입니다(예: 알고리즘 사용). 다양한 유형의 데이터 암호화가 있으며 암호화는 네트워크 보안의 기본입니다. 일반적인 유형으로는 데이터 암호화 표준 및 공개 키 암호화가 있습니다.

응급 복구 아카이브 기본 사용자 키를 한 플랫폼 소유자 키에서 다른 플랫폼 소유자 키로 재암호화할 수 있는 보호된 저장 영역입니다.

인증 사용자가 컴퓨터에 액세스하고 특정 프로그램에 대한 설정을 수정하거나 보안 데이터를 보는 등의 작업을 수행할 권한이 있는지 확인하는 절차입니다.

인증 기관 공개 키 인프라 실행에 필요한 인증서를 발급하는 서비스를 제공합니다.

인증서 인증 절차에서 특정 작업을 위해 사용자가 자격을 입증하는 수단입니다.

재부팅 컴퓨터를 다시 시작하는 프로세스입니다.

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

색인

B

BIOS

- 관리자 암호, 정의 2
- 관리자 카드 암호, 정의 3
- 사용자 카드 암호, 정의 3
- 설정 변경 13

C

Client Manager 23

Computer Setup

- 관리자 암호, 변경 9
- 관리자 암호, 정의 2
- 관리자 암호 설정 9
- 암호, 관리 7

F

F10 Setup 암호 2

I

ID 백업 마법사 암호 4

J

Java 카드

- PIN, 정의 3
- ProtectTools 용 보안 19
- 관리자 암호, 정의 3
- 복구 파일 암호, 정의 3
- 사용자 암호, 정의 3
- 파워온 인증 6

P

PKCS #12 가져오기 암호 4

ProtectTools

- Java 카드 보안 19
- Security Manager 모듈 1
- Security Manager 액세스 1
- 내장 보안 15
- 설정 관리 6
- 암호 관리 2
- 인증서 관리자 17

ProtectTools 용 BIOS 구성 13

ProtectTools 용 Embedded

Security

- 설치 16
- 암호 3
- 파워온 인증 6

ProtectTools 용 내장 보안

- 문제 해결 29

S

Security Manager, ProtectTools 1

T

TPM Preboot 암호 3

TPM 인증 별칭 4

TSS(TCG Software Stack) 1, 21

U

USB 토큰 인증 4

W

Windows

- 로그온 암호 3

ㄱ

가상 토큰 마스터 PIN 4

가상 토큰 사용자 PIN 4

가상 토큰 인증 암호 4

고급 작업 6

기본 사용자 암호, 정의 3

ㄴ

다단계 인증 인증서 관리자 로그 온 4

ㄷ

문제 해결

- ProtectTools 용 내장 보안 29

ProtectTools 용 인증서 관리

자 25

기타 36

ㅁ

백업 스케줄러 암호 3

보안

Java 카드 19

ProtectTools 에 내장 15

설정 암호 2

역할 2

보안 복구 에이전트 암호 4

ㅂ

사전 공격 11

설치, 인증서 관리자 17

소유자 암호, 정의 3

소프트웨어

ProtectTools Security Manager 1

ㅇ

암호

Computer Setup, 관리 7

Computer Setup 관리자 2

Computer Setup 관리자, 변 경 9

Computer Setup 관리자, 설 정 9

ID 백업 마법사 4

Java 카드 PIN 3

Java 카드 관리자 3

Java 카드 복구 파일 3

Java 카드 사용자 3

PKCS #12 가져오기 4

ProtectTools, 관리 2

TPM 인증 별칭 4

USB 토큰 인증 4

Windows 로그온 3

가상 토큰 마스터 PIN 4

가상 토큰 사용자 PIN	4
가상 토큰 인증	4
기본 사용자	3
백업 스케줄러	3
보안 복구 에이전트	4
소유자	3
암호 재설정 토큰	4
응급 복구 토큰	3
인증서 관리자 로그온	3
인증서 관리자 복구 파일	3
정의	2
지문 로그온	4
지침	5
파워온	2
파워온, 변경	7
파워온, 설정	7
암호 재설정 토큰	4
원격 배치, Client Manager	23
응급 복구 토큰 암호, 정의	3
인증서 관리자	
로그온	4, 18
로그온 암호	3
문제 해결	25
복구 파일 암호	3
설치	17

ㅈ

지문 로그온	4
--------	---

ㅊ

타사 솔루션	21
--------	----

ㅌ

파워온	
사전 공격	11
암호 변경	7
암호 설정	7
암호 정의	2
파워온 인증	
Java 카드	6
내장 보안	6