보안

사용자 설명서

First Edition: March 2006

문서 부품 번호: 406809-AD1

목차

1 보안 기능

주 보안 솔루션은 방어벽 역할을 하도록 설계되었지만 컴퓨터의 잘못된 취급이나 도난 위험까지 방지할 수는 없습니다.

주 이 컴퓨터는 온라인 보안 기반 추적 및 복구 서비스인 CompuTrace 를 지원합니다. 컴퓨터를 도난 당한 경우 CompuTrace 는 무단 사용자가 인터넷에 액세스하면 컴퓨터를 추적할 수 있습니다. CompuTrace 를 사용하려면 해당 소프트웨어를 구입하고 서비스에 가입해야 합니다. CompuTrace 소프트웨어 주문에 대한 자세한 내용은 http://www.hpshopping.com 을 참조하십시오.

이 컴퓨터에 제공되는 보안 기능을 통해 다양한 위험으로부터 컴퓨터, 개인 정보 및 데이터를 보호할 수 있습니다. 컴퓨터를 사용하는 방법에 따라 필요한 보안 기능이 달라집니다.

Microsoft® Windows® 운영체제는 특정 보안 기능을 제공합니다. 추가 보안 기능은 다음 표에 나와 있습니다. 이러한 추가 보안 기능은 대부분 Computer Setup 유틸리티(이후 Computer Setup 이라고 함)에서 구성할 수 있습니다.

보호 대상	사용할 보안 기능
컴퓨터의 무단 사용	• 암호 또는 스마트 카드를 이용한 파워온 인증 • ProtectTools Security Manager
Computer Setup(f10)에 무단 액세스	Computer Setup*의 설정 암호
하드 드라이브 내용에 무단 액세스	Computer Setup*의 DriveLock 암호
Computer Setup(f10) 암호의 무단 재설정	Computer Setup 의 고급 보안 기능
광 드라이브, 디스켓 드라이브 또는 내부 네트워크 어댑터로부터의 무단 시작	Computer Setup*의 부팅 옵션 기능
Windows 사용자 계정에 무단 액세스	Credential Manager for ProtectTools
데이터에 무단 액세스	• 방화벽 소프트웨어 • Windows 업데이트 • ProtectTools Security Manager
Computer Setup 설정 및 다른 시스템 식별 정보에 무단 액세스	Computer Setup*의 설정 암호
컴퓨터 도난	보안 케이블 슬롯(선택 사양인 보안 케이블과 함께 사용)
*Computer Setup 은 컴퓨터를 켜거나 재시작할 때 f10 키를 눌러 액세스할 수 있는 비 Windows 유틸리티입니다. Computer Setup 을 사용하는 경우 이동하거나 항목을 선택하려면 컴퓨터의 키를 사용해야 합니다.	

2 암호

대부분 보안 기능은 암호를 사용합니다. 암호를 설정할 때마다 암호를 기록하여 컴퓨터 이외의 안전한 장소에 보관하십시오. 다음 암호 관련 고려사항을 유념하십시오.

- 설정 암호, 파워온 암호 및 DriveLock 암호는 Computer Setup 에서 설정되고 시스템 BIOS 에 의해 관리됩니다.
- 일반적인 ProtectTools 기능 이외에 Computer Setup 에서 ProtectTools Security Manager 암호인 스마트 카드 PIN 과 내장 보안 암호를 활성화하여 BIOS 암호를 보호할 수 있습니다. 스마트 카드 PIN 은 지원되는 스마트 카드 리더에서 사용되며 내장 보안 암호는 내장 보안 칩(선택 사양)에서 사용됩니다.
- Windows 암호는 Windows 운영체제에서만 설정됩니다.
- Computer Setup 에서 설정한 설정 암호를 잊어버리면 Computer Setup 에 액세스할 수 없습니다.
- Computer Setup 에서 고급 보안 기능을 활성화한 다음 설정 암호 또는 파워온 암호를 잊어버리면 컴퓨터에 액세스할 수 없고 더 이상 컴퓨터를 사용할 수 없게 됩니다. 자세한 내용은 고객 지원 센터 또는 서비스 업체에 문의하십시오.
- Computer Setup 에서 설정한 파워온 암호 및 설정 암호를 잊어버리면 컴퓨터를 켜거나 최대 절전 모드에서 복원할 수 없습니다. 자세한 내용은 고객 지원 센터 또는 서비스 업체에 문의하십시오.
- Computer Setup 에서 설정한 사용자 및 마스터 DriveLock 암호를 잊어버리면 암호로 보호되는 하드 드라이버가 영구적으로 잠기고 더 이상 사용할 수 없게 됩니다.

다음 표에서는 일반적으로 사용되는 Computer Setup 암호와 Windows 암호를 나열하고 해당 기능을 설명합니다.

Computer Setup 암호	기능
설정 암호	Computer Setup 에 무단으로 액세스하지 못하도록 합니다.
파워온 암호	컴퓨터를 켜거나, 재시작하거나, 최대 절전 모드에서 복원할 때 컴퓨터 내용에 무단으로 액세스하지 못하도록 합니다.
DriveLock 마스터 암호	DriveLock 에 의해 보호되는 내장 하드 드라이브에 무단으로 액세스하지 못하도록 하며 DriveLock 보호 기능을 해제하는 데 사용됩니다.
DriveLock 사용자 암호	DriveLock 에 의해 보호되는 내장 하드 드라이브에 무단으로 액세스하지 못하도록 합니다.

Computer Setup 암호	기능
스마트 카드 PIN	스마트 카드 및 Java™ 카드 내용에 무단으로 액세스하지 못하도록 하며 스마트 카드 리더와 스마트 카드나 Java 카드를 사용하는 경우 컴퓨터에 무단으로 액세스하지 못하도록 합니다.
내장 보안 암호	BIOS 암호로 활성화된 경우 컴퓨터를 켜거나, 재시작하거나, 최대 절전 모드에서 복원할 때 컴퓨터 내용에 무단으로 액세스하지 못하도록 합니다. 이 암호로 이 보안 기능을 지원하려면 내장 보안 칩(선택 사양)이 필요합니다.

Windows 암호	기능
관리자 암호*	Windows 관리자 수준의 컴퓨터 내용에 무단으로 액세스하지 못하도록 합니다.
사용자 암호	Windows 사용자 계정에 무단으로 액세스하지 못하도록 합니다. 컴퓨터 내용에도 무단으로 액세스하지 못하도록 하며 대기 모드에서 재개하거나 최대 절전 모드에서 복원할 때 이 암호를 입력해야 합니다.
*Windows 관리자 암호 또는 Windows 사용자 암호 설정에 대한 자세한 내용을 보려면 **시작 > 도움말 및 지원**을 선택합니다.	

암호 설정을 위한 지침

Computer Setup 기능 및 Windows 보안 기능에 대해 동일한 암호를 사용할 수 있습니다. 또한 여러 Computer Setup 기능에 대해 동일한 암호를 사용할 수도 있습니다.

Computer Setup 에서 설정하는 암호

- 문자와 숫자를 조합하여 최대 32 자까지 가능하며 대소문자를 구분하지 않습니다.
- 암호를 설정 및 입력할 때는 동일한 키를 사용해야 합니다. 예를 들어 키보드 숫자 키로 암호를 설정한 경우 이후에 내장 숫자 키패드로 숫자를 입력하려고 하면 암호가 인식되지 않습니다.

  주 일부 모델에는 키보드 숫자 키와 같은 기능을 하는 별도의 숫자 키패드가 포함됩니다.

- Computer Setup 프롬프트에서 입력해야 합니다. Windows 에서 설정된 암호는 Windows 프롬프트에서 입력해야 합니다.

암호를 생성하고 저장하는 경우 참고 사항:

- 암호를 생성할 때는 프로그램에서 설정한 요구 사항을 따르십시오.
- 암호를 기록하여 컴퓨터 이외의 안전한 장소에 보관해 두십시오.
- 컴퓨터의 파일에 암호를 저장하지 마십시오.
- 외부인이 쉽게 알아낼 수 있는 이름 또는 기타 개인 정보를 사용하지 마십시오.

Computer Setup 설정 암호

Computer Setup 설정 암호는 Computer Setup 의 구성 설정과 시스템 식별 정보를 보호합니다. 이 암호를 설정한 후에 Computer Setup 에 액세스하고 Computer Setup 에서 변경하려면 해당 암호를 입력해야 합니다.

설정 암호

- Windows 관리자 암호와 같을 수도 있지만 바꿔가며 사용할 수는 없습니다.
- 설정, 입력, 변경 또는 삭제 시 표시되지 않습니다.
- 동일한 키를 사용하여 설정 및 입력해야 합니다. 예를 들어 키보드 숫자 키로 설정 암호를 설정한 경우 이후에 내장 숫자 키패드 숫자 키로 숫자를 입력하면 암호가 인식되지 않습니다.
- 문자와 숫자를 조합하여 최대 32 자까지 가능하며 대소문자를 구분하지 않습니다.

설정 암호 설정

설정 암호는 Computer Setup 에서 설정, 변경 및 삭제합니다.

설정 암호를 관리하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > Setup password** 를 선택한 다음 enter 키를 누릅니다.
   - 설정 암호를 설정하려면 다음과 같이 하십시오.

     New password 및 **Verify new password** 필드에 암호를 입력하고 f10 키를 누릅니다.
   - 관리자 암호를 변경하려면 다음과 같이 하십시오.

     Old password 필드에 현재 암호를 입력하고 **New password** 및 **Verify new password** 필드에 새 암호를 입력한 다음 f10 키를 누릅니다.
   - 설정 암호를 삭제하려면 다음과 같이 하십시오.

     Old password 필드에 현재 암호를 입력한 다음 f10 키를 누릅니다.
3. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

설정 암호 입력

Setup password 프롬프트에서 암호를 설정할 때 사용한 키를 사용하여 암호를 입력한 다음 Enter 를 누릅니다. 설정 암호를 3 회 이상 잘못 입력하면 컴퓨터를 재시작한 후 다시 시도해야 합니다.

Computer Setup 파워온 암호

Computer Setup 파워온 암호는 컴퓨터의 무단 사용을 방지합니다. 이 암호를 설정하면 컴퓨터를 켤 때마다 해당 암호를 입력해야 합니다.

파워온 암호

- 설정, 입력, 변경 또는 삭제 시 표시되지 않습니다.
- 동일한 키를 사용하여 설정 및 입력해야 합니다. 예를 들어 키보드 숫자 키로 파워온 암호를 설정한 경우 이후에 내장 숫자 키패드 숫자 키로 숫자를 입력하면 암호가 인식되지 않습니다.
- 문자와 숫자를 조합하여 최대 32 자까지 가능하며 대소문자를 구분하지 않습니다.

파워온 암호 설정

파워온 암호는 Computer Setup 에서 설정, 변경 및 삭제합니다.

파워온 암호를 관리하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > Power-On password** 를 선택한 다음 enter 키를 누릅니다.
   - 파워온 암호를 설정하려면 다음과 같이 하십시오.

     New password 및 **Verify new password** 필드에 암호를 입력하고 f10 키를 누릅니다.
   - 파워온 암호를 변경하려면 다음과 같이 하십시오.

     Old password 필드에 현재 암호를 입력하고 **New password** 및 **Verify new password** 필드에 새 암호를 입력한 다음 f10 키를 누릅니다.
   - 파워온 암호를 삭제하려면 다음과 같이 하십시오.

     Old password 필드에 현재 암호를 입력한 다음 f10 키를 누릅니다.
3. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

파워온 암호 입력

Power-on Password 프롬프트에서 암호를 설정할 때 사용한 키를 사용하여 암호를 입력한 다음 enter 키를 누릅니다. 파워온 암호를 3 회 이상 잘못 입력하면 컴퓨터를 껐다가 켠 후 다시 시도해야 합니다.

재시작 시 파워온 암호 필요

컴퓨터를 시작할 때뿐 아니라 재시작할 때도 항상 파워온 암호를 입력하도록 할 수 있습니다.

Computer Setup 에서 이 기능을 활성화 또는 비활성화하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > Password options > Require password on restart** 를 선택한 다음 enter 키를 누릅니다.
3. 화살표 키로 이 암호 기능을 활성화하거나 비활성화한 다음 f10 키를 누릅니다.
4. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

Computer Setup DriveLock

주의 DriveLock 으로 보호되는 하드 드라이버를 영구적으로 사용할 수 없게 되는 상황이 발생하지 않도록 하려면 DriveLock 사용자 암호와 DriveLock 마스터 암호를 기록해서 컴퓨터 이외의 안전한 장소에 보관해 두십시오. 두 DriveLock 암호를 모두 잊어버리면 하드 드라이브가 영구적으로 잠기고 더 이상 사용할 수 없게 됩니다.

DriveLock 보호 기능은 하드 드라이브 내용에 대한 무단 액세스를 방지합니다. DriveLock 은 컴퓨터의 내장 하드 드라이브에만 적용할 수 있습니다. DriveLock 보호 기능을 드라이브에 적용한 후 드라이브에 액세스하려면 암호를 입력해야 합니다. DriveLock 암호로 액세스하려면 내장 하드 드라이브가 도킹 장치(선택 사양)나 외장 MultiBay 가 아닌 컴퓨터에 삽입되어 있어야 합니다.

DriveLock 보호 기능을 내장 하드 드라이브에 적용하려면 사용자 암호와 마스터 암호를 Computer Setup 에서 설정해야 합니다. DriveLock 보호 기능 사용에 대한 다음 고려사항을 유념하십시오.

- DriveLock 보호 기능을 하드 드라이브에 적용한 후에는 사용자 암호나 마스터 암호를 입력해야만 하드 드라이브에 액세스할 수 있습니다.
- 사용자 암호의 소유자는 보호되는 하드 드라이브를 매일 사용하는 사용자여야 합니다. 마스터 암호는 시스템 관리자나 하드 드라이브를 매일 사용하는 사용자가 소유할 수 있습니다.
- 사용자 암호와 마스터 암호는 같을 수 있습니다.
- 드라이브에서 DriveLock 보호 기능을 해제하는 경우에만 사용자 암호 또는 마스터 암호를 삭제할 수 있습니다. 마스터 암호만으로 드라이브에서 DriveLock 보호 기능을 해제할 수 있습니다.

주 파워온 암호와 DriveLock 사용자 암호가 같은 경우 파워온 암호와 DriveLock 사용자 암호를 모두 입력하는 대신 파워온 암호만 입력하라는 메시지가 표시됩니다.

DriveLock 암호 설정

Computer Setup 에서 DriveLock 설정에 액세스하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > DriveLock passwords** 를 선택한 다음 enter 키를 누릅니다.
3. 보호할 하드 드라이브의 위치를 선택한 다음 f10 키를 누릅니다.
4. 화살표 키로 **Protection** 필드에서 **Enable** 을 선택한 다음 f10 키를 누릅니다.
5. 경고를 읽은 다음, 계속 진행하려면 f10 키를 누릅니다.
6. **New password** 및 **Verify new password** 필드에 사용자 암호를 입력한 다음 f10 키를 누릅니다.
7. **New password** 및 **Verify new password** 필드에 마스터 암호를 입력한 다음 f10 키를 누릅니다.
8. 선택한 드라이브에 DriveLock 보호 기능을 적용할지 확인하려면 확인 필드에 DriveLock 을 입력한 다음 f10 키를 누릅니다.
9. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

DriveLock 암호 입력

하드 드라이브가 도킹 장치(선택 사양)나 외장 MultiBay 가 아닌 컴퓨터에 삽입되어 있는지 확인하십시오.

DriveLock HDD Bay Password 프롬프트에서 암호를 설정할 때 사용한 키를 사용하여 사용자 또는 마스터 암호를 입력한 다음 enter 키를 누릅니다.

암호를 2 회 이상 잘못 입력하면 컴퓨터를 재시작한 후 다시 시도해야 합니다.

DriveLock 암호 변경

Computer Setup 에서 DriveLock 설정에 액세스하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > DriveLock passwords** 를 선택한 다음 enter 키를 누릅니다.
3. 화살표 키로 내장 하드 드라이브의 위치를 선택한 다음 f10 키를 누릅니다.
4. 화살표 키로 변경하려는 암호 필드를 선택합니다. **Old password** 필드에 현재 암호를 입력하고 **New password** 필드 및 **Verify new password** 필드에 새 암호를 입력합니다. 그런 다음 f10 키를 누릅니다.
5. **Confirm New Password** 필드에 새 암호를 다시 입력한 다음 enter 키를 누릅니다.
6. 설정 알림 메시지가 표시될 때 enter 키를 눌러 변경 사항을 저장합니다.
7. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

DriveLock 보호 기능 해제

Computer Setup 에서 DriveLock 설정에 액세스하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > DriveLock passwords** 를 선택한 다음 enter 키를 누릅니다.
3. 화살표 키로 내장 하드 드라이브의 위치를 선택한 다음 f10 키를 누릅니다.
4. 화살표 키로 **Protection** 필드에서 **Disable** 을 선택한 다음 f10 키를 누릅니다.
5. **Old password** 필드에 마스터 암호를 입력합니다. 그런 다음 f10 키를 누릅니다.
6. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

3 Computer Setup 보안 기능

장치 보안

Computer Setup 의 Boot options(부팅 옵션) 메뉴 또는 Port options(포트 옵션) 메뉴에서 시스템 장치를 활성화하거나 비활성화할 수 있습니다.

Computer Setup 에서 시스템 장치를 비활성화하거나 다시 활성화하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **System Configuration > Boot options** 또는 **System Configuration > Port options** 를 선택한 다음 기본 설정을 입력합니다.
3. 기본 설정을 확인하려면 f10 키를 누릅니다.
4. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

Computer Setup 고급 보안

△ 주의 컴퓨터를 영구적으로 사용할 수 없게 되는 상황이 발생하지 않도록 하려면 구성한 설정 암호, 파워온 암호, 스마트 카드 PIN 을 컴퓨터 이외의 안전한 장소에 보관하십시오. 이러한 암호나 PIN 이 없으면 컴퓨터의 잠금을 해제할 수 없습니다.

고급 보안 기능은 시스템에 대한 액세스 권한을 부여하기 전에 구성한 설정 암호, 파워온 암호 또는 스마트 카드 PIN 을 통한 사용자 인증을 요구함으로써 파워온 보안을 강화합니다.

고급 보안 설정

Computer Setup 에서 고급 보안을 활성화하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > Password options** 를 선택한 다음 enter 키를 누릅니다.
3. 화살표 키로 **Stringent security** 필드를 선택합니다.
4. 경고를 읽고 f10 키를 눌러 계속 진행합니다.
5. 컴퓨터를 켤 때마다 고급 보안 기능을 활성화하려면 f10 키를 누릅니다.
6. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

고급 보안 해제

Computer Setup 의 고급 보안을 해제하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 화살표 키로 **Security > Password options** 를 선택한 다음 enter 키를 누릅니다.
3. 화살표 키로 **Stringent security** 필드에서 **Disable** 을 선택한 다음 f10 키를 누릅니다.
4. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

Computer Setup 시스템 정보

Computer Setup 의 시스템 정보 기능은 두 가지 유형의 시스템 정보를 제공합니다.

- 컴퓨터 모델 및 배터리 팩에 대한 식별 정보
- 프로세서, 캐시, 메모리, ROM, 비디오 버전, 키보드 컨트롤러 버전에 대한 사양 정보

이 일반 시스템 정보를 보려면 화살표 키로 File > System Information 을 선택합니다.

주 이 정보에 대한 무단 액세스를 방지하려면 Computer Setup 에서 설정 암호를 생성해야 합니다. 자세한 내용은 "설정 암호 설정"을 참조하십시오.

Computer Setup 시스템 ID

Computer Setup 의 시스템 ID 기능을 사용하면 컴퓨터 자산 태그 또는 소유권 태그를 표시하거나 입력할 수 있습니다.

주 이 정보에 대한 무단 액세스를 방지하려면 Computer Setup 에서 설정 암호를 생성해야 합니다. 자세한 내용은 "설정 암호 설정"을 참조하십시오.

이 기능을 관리하려면 다음과 같이 하십시오.

1. 컴퓨터를 켜거나 재시작하고 화면 왼쪽 하단에 "F10 = ROM Based Setup(ROM 기반 설정)" 메시지가 나타나면 f10 키를 눌러 Computer Setup 을 엽니다.
2. 시스템 구성 요소의 식별 태그 ID 를 보거나 입력하려면 화살표 키로 **Security > System IDs** 를 선택합니다.
3. 정보 또는 기본 설정을 확인하려면 f10 키를 누릅니다.
4. 기본 설정을 저장하려면 화살표 키를 사용하여 **File > Save changes and exit** 을 선택한 다음 화면의 지시를 따릅니다.

   컴퓨터를 재시작하면 저장한 설정이 적용됩니다.

4 바이러스 백신 소프트웨어

컴퓨터에서 전자 우편, 네트워크 또는 인터넷에 액세스하는 경우 컴퓨터가 컴퓨터 바이러스에 노출됩니다. 컴퓨터 바이러스는 운영체제, 응용프로그램 또는 유틸리티를 사용할 수 없게 만들거나 비정상적으로 작동하게 할 수 있습니다.

바이러스 백신 소프트웨어를 사용하면 대부분의 바이러스를 발견하여 삭제할 수 있으며, 대부분의 경우 바이러스로 인해 손상된 내용을 복구할 수 있습니다. 새로 발견된 바이러스로부터 보호하려면 바이러스 백신 소프트웨어를 최신 버전으로 업데이트해야 합니다.

이 컴퓨터에는 Norton Internet Security 소프트웨어가 사전 설치되어 있습니다. Norton Internet Security 소프트웨어에 대한 자세한 정보를 보려면 **시작 > 모든 프로그램 > Norton Internet Security > 도움말 및 지원**을 선택합니다.

컴퓨터 바이러스에 대한 자세한 정보를 보려면 도움말 및 지원 센터의 검색 필드에 바이러스를 입력합니다.

5 방화벽 소프트웨어

컴퓨터에서 전자 우편, 네트워크 또는 인터넷에 액세스하는 경우 다른 외부인이 사용자 정보, 컴퓨터 및 사용자가 보유한 정보에 액세스할 수 있습니다. 컴퓨터에 사전 설치된 방화벽 소프트웨어를 사용하여 개인 정보를 보호할 수 있습니다.

방화벽은 로깅, 보고 및 자동 알림 등의 기능을 포함하고 있어서 송수신되는 모든 트래픽을 모니터링합니다. 자세한 내용은 방화벽 설명서를 참조하거나 방화벽 제조업체에 문의하십시오.

주 어떤 환경에서는 방화벽이 인터넷 게임에 대한 액세스를 차단하거나, 네트워크상의 프린터 또는 파일 공유를 방해하거나, 인증된 전자 우편 첨부를 차단할 수 있습니다. 문제를 일시적으로 해결하려면 방화벽을 비활성화하고 필요한 작업을 수행한 다음 방화벽을 다시 활성화하십시오. 문제를 영구적으로 해결하려면 방화벽을 다시 구성하십시오.

6 중요 보안 업데이트(일부 모델만 해당)

△ **주의** 보안 침해 및 컴퓨터 바이러스로부터 컴퓨터를 보호하려면 Microsoft 에서 알림을 받은 즉시 모든 중요 업데이트를 설치하는 것이 좋습니다.

컴퓨터가 구성된 후 배포된 추가 업데이트를 제공하기 위해 *Windows XP 용 중요 보안 업데이트* 디스크가 컴퓨터와 함께 제공될 수 있습니다.

Windows XP 용 중요 보안 업데이트 디스크를 사용하여 시스템을 업데이트하려면 다음과 같이 하십시오.

1. 드라이브에 디스크를 넣습니다. 디스크가 자동으로 설치 응용프로그램을 실행합니다.
2. 화면 지시에 따라 모든 업데이트를 설치합니다. 설치 과정은 수 분 정도 걸릴 수 있습니다.
3. 디스크를 꺼냅니다.

컴퓨터가 출하된 *후* 운영체제 및 기타 소프트웨어에 대한 추가 업데이트가 제공될 수 있습니다. 제공되는 모든 업데이트가 컴퓨터에 설치되어 있는지 확인하려면 다음과 같이 하십시오.

- 매월 Windows Update 를 실행하여 Microsoft 에서 제공하는 최신 소프트웨어를 설치합니다.
- Microsoft 웹 사이트 또는 도움말 및 지원 센터의 업데이트 링크를 통해 업데이트를 설치합니다.

7 ProtectTools Security Manager(일부 모델만 해당)

일부 컴퓨터 모델에는 ProtectTools Security Manager 가 사전 설치되어 있습니다. 이 소프트웨어는 Microsoft Windows 제어판에서 액세스할 수 있습니다. 이 소프트웨어는 컴퓨터, 네트워크 및 중요 데이터에 대한 무단 액세스를 방지하는 보안 기능을 제공합니다. ProtectTools Security Manager 는 다음 모듈을 통해 향상된 기능을 제공하는 보안 콘솔입니다.

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

컴퓨터 모델에 따라 추가 모듈이 사전 설치 또는 사전 로드되어 있을 수 있으며 HP 웹 사이트에서 다운로드할 수도 있습니다. 자세한 내용은 http://www.hp.com 을 참조하십시오.

Embedded Security for ProtectTools

주 Embedded Security for ProtectTools 를 사용하려면 컴퓨터에 TPM(Trusted Platform Module) 내장 보안 칩(선택 사양)을 설치해야 합니다.

Embedded Security for ProtectTools 는 다음을 포함하여 사용자 데이터 또는 인증 정보에 대한 무단 액세스를 방지하는 보안 기능을 제공합니다.

- 소유권, 소유자 암호문 관리 등 관리 기능
- 사용자 등록, 사용자 암호문 관리 등 사용자 기능
- 사용자 데이터 보호를 위해 향상된 Microsoft EFS 및 Personal Secure Drive 설정 등 설정 구성
- 키 계층 백업 및 복원 등 관리 기능
- 내장 보안을 사용하는 경우 보호되는 디지털 인증서 작업을 위한 타사 응용프로그램(Microsoft Outlook 및 Internet Explorer) 지원

TPM 내장 보안 칩(선택 사양)은 다른 ProtectTools Security Manager 보안 기능을 향상 및 활성화합니다. 예를 들어 Credential Manager for ProtectTools 는 사용자가 Windows 에 로그온하는 경우 내장 칩을 인증 요소로 사용할 수 있습니다. 일부 모델에서 TPM 내장 보안 칩은 BIOS Configuration for ProtectTools 를 통해 액세스할 수 있는 향상된 BIOS 보안 기능을 활성화하기도 합니다.

자세한 내용은 Embedded Security for ProtectTools 온라인 도움말을 참조하십시오.

Credential Manager for ProtectTools

Credential Manager for ProtectTools 는 다음을 포함하여 컴퓨터에 대한 무단 액세스를 방지하는 보안 기능을 제공합니다.

- 스마트 카드를 통해 Windows 에 로그온하는 경우와 같이 Microsoft Windows 에 로그온할 때 암호 대체 수단
- 웹 사이트, 응용프로그램, 보안 네트워크 자원에 대한 인증 정보를 자동으로 기억하는 Single Sign On 기능
- 스마트 카드와 지문 인식기 등 보안 장치(선택 사양) 지원

자세한 내용은 Credential Manager for ProtectTools 온라인 도움말을 참조하십시오.

BIOS Configuration for ProtectTools

BIOS Configuration for ProtectTools 는 ProtectTools Security Manager 응용프로그램에서 BIOS (Computer Setup) 보안 및 구성 설정에 대한 액세스를 제공합니다. 또한 Computer Setup 에서 관리하는 시스템 보안 기능에 사용자가 보다 효율적으로 액세스할 수 있도록 해줍니다.

BIOS Configuration for ProtectTools 기능을 통해 다음을 수행할 수 있습니다.

- 파워온 암호 및 설정 암호 관리
- 스마트 카드 암호 및 내장 보안 인증 등 기타 파워온 인증 기능 구성
- CD-ROM 부팅이나 다른 하드웨어 포트와 같은 하드웨어 기능 활성화 및 비활성화
- MultiBoot 활성화 및 부팅 순서 변경과 같은 부팅 옵션 구성

주 BIOS Configuration for ProtectTools 의 많은 기능은 Computer Setup 에서도 사용 가능합니다.

자세한 내용은 BIOS Configuration for ProtectTools 온라인 도움말을 참조하십시오.

Smart Card Security for ProtectTools

Smart Card Security for ProtectTools 는 선택 사양인 스마트 카드 리더가 장착된 컴퓨터의 스마트 카드 설정과 구성을 관리합니다.

주 스마트 카드와 Java 카드 모두 스마트 카드 리더를 사용합니다.

Smart Card Security for ProtectTools 기능을 통해 다음을 수행할 수 있습니다.

- 스마트 카드 보안 기능 액세스 향상된 보안 기능은 선택 사양인 ProtectTools Smart Card 와 스마트 카드 리더에 의해 지원됩니다.
- Credential Manager for ProtectTools 와 함께 사용할 수 있도록 ProtectTools Smart Card 초기화.
- BIOS 와 함께 부팅 전 상태에서 스마트 카드 인증을 활성화하고 관리자와 사용자에 대해 별도의 스마트 카드 구성. 이 작업을 수행하려면 운영체제를 로드하기 전에 스마트 카드를 넣고 선택적으로 PIN 을 입력해야 합니다.
- 스마트 카드 사용자 인증에 사용되는 암호 설정 및 변경.
- 스마트 카드에 저장된 스마트 카드 BIOS 암호 백업 및 복원.

자세한 내용은 Smart Card Security for ProtectTools 온라인 도움말을 참조하십시오.

Java Card Security for ProtectTools

Java™ Card Security for ProtectTools 는 선택 사양인 스마트 카드 리더가 장착된 컴퓨터의 Java 카드 설정과 구성을 관리합니다.

주 Java 카드와 스마트 카드 모두 스마트 카드 리더를 사용합니다.

Java Card Security for ProtectTools 기능을 통해 다음을 수행할 수 있습니다.

- Java 카드 보안 기능 액세스 향상된 보안 기능은 선택 사양인 ProtectTools Java Card 와 스마트 카드 리더에 의해 지원됩니다.
- Credential Manager for ProtectTools 와 함께 Java 카드를 사용할 수 있도록 해주는 고유한 PIN 생성.
- BIOS 와 함께 부팅 전 상태에서 Java 카드 인증을 활성화하고 관리자와 사용자에 대해 별도의 Java 카드 구성. 이 작업을 수행하려면 운영체제를 로드하기 전에 Java 카드를 넣고 PIN 을 입력해야 합니다.
- Java 카드 사용자 인증에 사용되는 ID 설정 및 변경.
- Java 카드에 저장되는 Java 카드 ID 백업 및 복원.

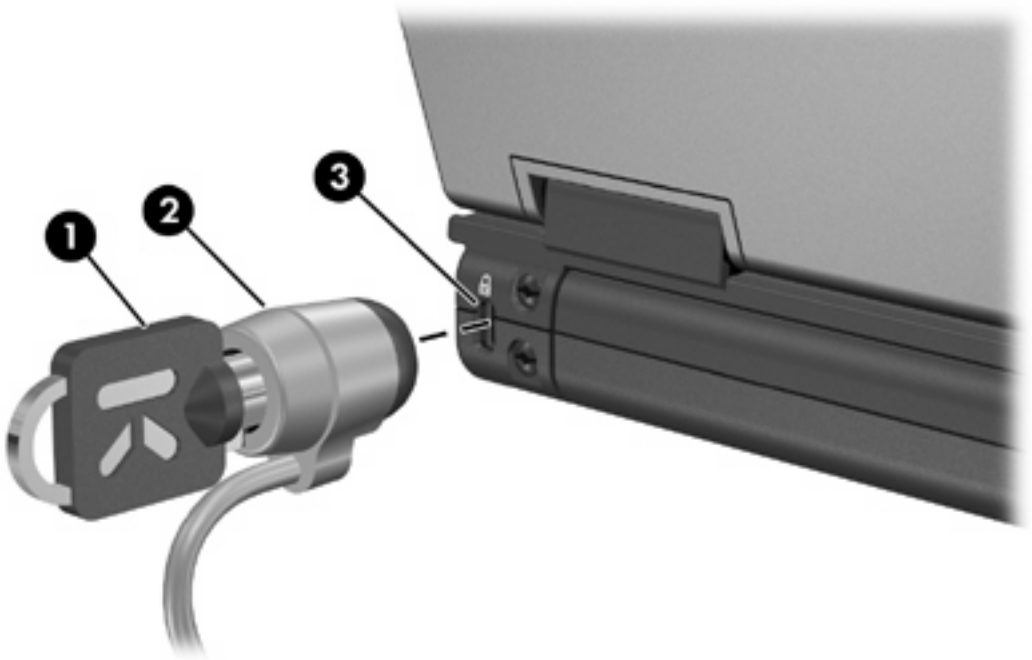
자세한 내용은 Java Card Security for ProtectTools 온라인 도움말을 참조하십시오.

8 보안 케이블

주 보안 케이블은 방어벽의 역할을 하도록 설계되어 있지만 컴퓨터의 잘못된 취급이나 도난 위험까지 방지할 수는 없습니다.

보안 케이블을 설치하려면 다음과 같이 하십시오.

1. 고정된 물체에 보안 케이블을 연결합니다.
2. 키 **(1)**를 케이블 잠금 장치 **(2)**에 넣습니다.
3. 케이블 잠금 장치를 컴퓨터의 보안 케이블 슬롯 **(3)**에 꽂은 다음 키를 사용하여 케이블 잠금 장치를 잠급니다.



주 사용 중인 컴퓨터는 그림과 다를 수도 있습니다. 보안 케이블 슬롯의 위치는 모델에 따라 다릅니다.

9 지문 인식기(일부 모델만 해당)

지문 인식기 사용

주 지문 인식기의 위치는 모델에 따라 다릅니다.

지문 등록

지문 인식기를 통해 Windows 암호 대신 ProtectTools Security Manager 에 등록된 지문을 사용하여 Windows 에 로그온할 수 있습니다.

지문 인식기가 내장된 HP 컴퓨터를 사용하든 선택 사양 지문 인식기를 사용하든, 지문으로 Windows 에 로그온하려면 다음 2 단계를 거쳐야 합니다.

1. 지문 인식기를 설정합니다.
2. 등록된 지문을 사용하여 Windows 에 로그온합니다.

1 단계: 지문 인식기 설정

주 선택 사양 지문 인식기를 사용할 경우, 다음 단계를 수행하기 전에 인식기와 컴퓨터를 연결합니다.

지문 인식기를 설정하려면 다음과 같이 하십시오.

1. Windows 에서 작업 표시줄의 알림 영역에 있는 **Credential Manager** 아이콘을 두 번 누릅니다.

   또는

   시작 > 모든 프로그램 > ProtectTools Security Manager 를 선택한 다음 왼쪽에 있는 **Credential Manager** 탭을 누릅니다.

2. "My Identity(내 ID)" 페이지의 오른쪽 위에 있는 **Log On(로그온)**을 누릅니다.

   Credential Manager Logon Wizard 가 열립니다.

3. "Introduce Yourself(자기 소개)" 페이지에서 기본 사용자 이름을 사용하려면 Next(다음)를 누릅니다.

   주 이 컴퓨터에 등록된 다른 사용자가 있는 경우, Windows 사용자 이름을 입력하여 지문을 등록할 사람을 선택할 수 있습니다.

4. "Enter Password(암호 입력)" 페이지에서 사용자의 Windows 암호를 설정한 경우 해당 암호를 입력합니다. 그렇지 않은 경우 **Finish(마침)**를 누릅니다.

5. "My Services and Applications(내 서비스 및 응용프로그램)" 페이지에서 **Register Fingerprints (지문 등록)**를 누릅니다.

   주 기본적으로 Credential Manager 에는 손가락 두 개 이상의 지문을 등록해야 합니다.

6. Credential Manager Registration Wizard 가 열리면 지문 센서 위로 지문을 위에서 아래로 천천히 통과시킵니다.

   주 첫 번째 지문을 등록할 기본 손가락은 오른쪽 집게 손가락입니다. 오른손 또는 왼손에서 먼저 등록할 손가락을 눌러 기본값을 변경할 수 있습니다. 손가락을 누르면 테두리가 표시되어 선택되었음을 나타냅니다.

7. 화면의 손가락이 녹색으로 바뀔 때까지 같은 손가락을 지문 센서 위로 계속해서 통과시킵니다.

   주 각 손가락을 통과시키면 진행률 표시기에 진행 상태가 표시됩니다. 지문을 등록하려면 손가락을 여러 번 통과시켜야 합니다.

   주 지문 등록 절차 중에 재시작이 필요하면 화면에 강조 표시된 손가락을 마우스 오른쪽 버튼으로 누르고 **Start Over(재시작)**를 누릅니다.

8. 화면에서 등록할 다른 손가락을 누른 다음 6 ~ 7 단계를 반복합니다.

   주의 설정을 완료하려면 손가락 두 개 이상의 지문을 등록해야 합니다.

   주 손가락 두 개의 지문을 등록하기 전에 **Finish(마침)**를 누른 경우, 오류 메시지가 표시됩니다. **OK(확인)**를 눌러 계속합니다.

9. 손가락 두 개 이상의 지문을 등록한 후 **Finish(마침)**, **OK(확인)**를 차례로 누릅니다.

10. 다른 Windows 사용자에 대해 지문 인식기를 설정하려면 해당 사용자로 Windows 에 로그온한 후 1 ~ 9 단계를 반복합니다.

2 단계: 등록된 지문을 사용하여 Windows 에 로그온

지문을 사용하여 Windows 에 로그온하려면 다음과 같이 하십시오.

1. 지문을 등록한 후 바로 Windows 를 재시작합니다.

2. 화면 왼쪽 위에서 **Log on to Credential Manager(Credential Manager 에 로그온)**를 누릅니다.

3. **Credential Manager Logon Wizard** 대화 상자에서 사용자 이름을 누르는 대신 등록된 손가락을 통과시켜 Windows 에 로그온합니다.

4. Windows 암호를 입력하여 지문을 암호와 연결합니다.

주 처음으로 지문을 사용하여 Windows 에 로그온하고 Windows 암호가 있는 경우, 암호를 지문과 연결하려면 해당 암호를 입력해야 합니다. 암호를 지문과 연결한 후에는 지문 인식기를 사용할 때 Windows 암호를 다시 입력하지 않아도 됩니다.

색인