데스크탑 관리 설명서
비즈니스 데스크탑

문서 부품 번호: 312947-AD2

2003년 9월

본 설명서는 일부 모델에 사전 설치된 보안 및 Intelligent Manageability (지능 관리형) 기능의 사용에 대한 정의 및 지침을 제공합니다.

경고: 지시 사항을 따르지 않으면 부상을 당하거나 생명을 잃을 수 있습니다.

주의: 지시 사항을 따르지 않으면 장비가 손상되거나 정보를 유실할 수 있습니다.

데스크탑 관리 설명서
비즈니스 데스크탑

제 2판(2003년 9월)
문서 부품 번호: 312947-AD2

목차

데스크탑 관리 설명서

색인

데스크탑 관리 설명서

HP 지능형 관리 기능은 네트워크 환경하에서 데스크탑, 워크스테이션 및 노트북 PC를 관리하기 위한 표준 기반 솔루션을 제공합니다. HP는 1995년에 업계 최초로 완벽하게 관리할 수 있는 데스크탑 PC를 도입하면서 데스크탑 관리의 편리성을 개척했습니다. HP는 관리 기술면에서 특허를 받았습니다. 이후 HP는 업계 선두에서 데스크탑, 워크스테이션 및 노트북 PC를 효율적으로 배치, 구성 및 관리하는 데 필요한 표준 및 인프라(Infrastructure)를 개발해 오고 있으며, 산업 전반의 성과를 이끌어 내었습니다. 또한 HP는 Intelligent Manageability와 이러한 제품 간의 호환성을 보장하기 위해 업계 선두의 관리 소프트웨어 솔루션 제공업체와 긴밀하게 협력하고 있습니다. 지능형 관리 기능은 주요 업무 측면으로 데스크탑 PC 사용 솔루션의 4단계(계획, 배치, 관리 및 전환)에서 사용자를 지원합니다.

데스크탑 관리에 대한 주요 특성 및 기능은 다음과 같습니다.

- 초기 구성 및 배치
- 원격 시스템 설치
- 소프트웨어 업데이트 및 관리
- ROM 플래시
- 자산 추적 및 보안
- 오류 알림 및 복구

본 설명서에 설명되어 있는 특정 기능에 대한 지원은 모델 또는 소프트웨어 버전에 따라 다를 수 있습니다.

초기 구성 및 배치

이 컴퓨터에서는 사전 설치된 소프트웨어 이미지가 함께 제공됩니다. 간단한 소프트웨어 "개별화" 작업 후 컴퓨터를 사용할 수 있습니다.

사전 설치된 소프트웨어 이미지와 사용자 정의된 일련의 시스템 및 응용프로그램을 교체할 수 있습니다. 다음과 같은 몇 가지 방법으로 사용자 정의된 소프트웨어 이미지를 배치할 수 있습니다.

- 사전 설치된 소프트웨어 이미지 묶음을 해제한 후 추가 소프트웨어 응용프로그램 설치
- Altiris Deployment Solution™과 같은 소프트웨어 배치 도구를 사용하여 사전 설치된 소프트웨어를 사용자 정의 소프트웨어 이미지로 교체
- 디스크 복제 프로세스를 사용하여 내용을 한 하드 드라이브에서 다른 하드 드라이브로 복사

최상의 배치 방법은 정보 기술 환경 및 프로세스에 따라 다릅니다. HP Lifecycle Solutions 웹 사이트 (http://h18000.www1.hp.com/solutions/pcsolutions)의 PC 배치 섹션은 최상의 배치 방법을 선택하는 데 유용한 정보를 제공합니다.

Restore Plus! CD, ROM 기반 설치 및 ACPI 하드웨어는 시스템 소프트웨어 복구, 구성 관리와 문제 해결 및 전원 관리를 폭 넓게 지원합니다.

원격 시스템 설치

원격 시스템 설치 기능을 통해 PXE(Preboot Execution Environment)를 시작하여 네트워크 서버에 있는 소프트웨어 및 구성 정보를 사용하는 시스템을 시작하고 설치할 수 있습니다. 원격 시스템 설치 기능은 일반적으로 시스템 설치 및 구성 도구로 사용되며 다음 작업에 사용할 수 있습니다.

- 하드 드라이브 포맷
- 한 대 이상의 새 PC에 소프트웨어 이미지 배치
- 플래시 ROM의 시스템 BIOS 원격 업데이트(7페이지의 "원격 ROM 플래시")
- 시스템 BIOS 설정 구성

원격 시스템 설치를 초기화하려면 HP 로고 화면의 우측 하단에 F12 = Network Service Boot 메시지가 나타날 때 **F12**를 누릅니다. 화면의 지시를 따라 프로세스를 계속 진행합니다. 기본 부팅 순서는 항상 PXE 부팅을 시도하도록 변경할 수 있는 BIOS 구성 설정입니다.

HP 및 Altiris, Inc.는 파트너십을 통해 보다 쉽고 빠르게 회사 PC를 배치하고 관리하여 총소유 비용을 현격하게 절감하고 HP PC를 전사적 환경에서 최상으로 관리할 수 있는 클라이언트 PC로 만드는 도구를 제공합니다.

소프트웨어 업데이트 및 관리

HP는 Altiris, Altiris PC Transplant Pro, HP 클라이언트 관리자 소프트웨어, Altiris 솔루션, 시스템 소프트웨어 관리자, Proactive Change Notification 및 ActiveUpdate와 같이 데스크탑과 워크스테이션에서 소프트웨어를 관리하고 업데이트할 수 있는 여러 도구를 제공합니다.

HP 클라이언트 관리자 소프트웨어

지능형 HP CMS(HP 클라이언트 관리자 소프트웨어)는 Altiris의 HP Intelligent Manageability 기술과 긴밀하게 통합되어 HP 액세스 장치에 다음을 포함한 뛰어난 하드웨어 관리 기능을 제공합니다.

- 자산 관리를 위한 하드웨어 인벤토리 세부 정보 보기
- PC 상태 확인 감시 및 진단
- 하드웨어 환경의 변경 사항에 대한 사전 알림
- 시스템의 과열 경고, 메모리 경보 등과 같은 업무에 중요한 세부 정보에 대한 웹 액세스 가능 보고
- 장치 드라이버 및 ROM BIOS와 같은 시스템 소프트웨어 원격 업데이트
- 부팅 순서의 원격 변경

HP 클라이언트 관리자에 대한 자세한 내용을 보려면 http://h18000.www1.hp.com/im/client_mgr.html을 참조하십시오.

Altiris 솔루션

HP 클라이언트 관리 솔루션은 모든 IT 사용 분야에서 HP 클라이언트 장치의 중앙 하드웨어 관리 기능을 제공합니다.

- 인벤토리 및 자산 관리
  - SW 라이센스 준수
  - PC 추적 및 보고
  - 임대 계약, 고정 자산 추적
- 배치 및 이동
  - Microsoft Windows 2000 또는 Windows XP Professional 또는 Home Edition 이동

- ❏ 시스템 배치
- ❏ 원하는 대로 이동

■ 헬프 데스크 및 문제 해결

- ❏ 헬프 데스크 티켓 관리
- ❏ 원격 문제 해결
- ❏ 원격 문제 해결 방법
- ❏ 클라이언트 피해 복구

■ 소프트웨어 및 작업 관리

- ❏ 지속적인 데스크탑 관리
- ❏ HP 시스템 소프트웨어 배치
- ❏ 응용프로그램 자가 진단

일부 데스크탑 및 노트북 모델에는 Altiris 관리 에이전트가 출하 시 로드된 이미지의 일부로 포함됩니다. 이 에이전트를 사용하여 Altiris 배치 솔루션과 통신할 수 있으며 새 하드웨어 배치를 완성하거나 사용 방법이 간단한 마법사를 사용하여 새 운영 체제로 자유롭게 이동할 수 있습니다. Altiris 솔루션은 사용하기 쉬운 소프트웨어 분산 기능을 제공합니다. Altiris 솔루션 소프트웨어를 시스템 소프트웨어 관리자나 HP 클라이언트 관리자와 결합하여 사용하면 관리자는 중앙 콘솔에서 ROM BIOS와 장치 드라이버 소프트웨어를 업데이트할 수 있습니다.

자세한 내용은 http://www.hp.com/go/easydeploy를 참조하십시오.

Altiris PC Transplant Pro

Altiris PC Transplant Pro를 사용하면 PC에서 이전 설정, 기본 설정 및 데이터를 보존하고 새 환경으로 빠르고 쉽게 이동할 수 있습니다. 업그레이드에 소요되는 시간은 몇 분밖에 걸리지 않으며 사용자는 데스크탑 성능에 만족할 것입니다.

모든 기능을 갖춘 30일 평가판을 다운로드하는 자세한 방법은 http://h18000.www1.hp.com/im/prodinfo.html#deploy를 참조하십시오.

시스템 소프트웨어 관리자(System Software Manager)

SSM(시스템 소프트웨어 관리자)은 사용자가 여러 시스템에 시스템 수준의 소프트웨어를 동시에 업데이트할 수 있도록 하는 유틸리티입니다. PC 클라이언트 시스템에서 실행하는 경우 SSM은 하드웨어와 소프트웨어 버전을 모두 감지한 후 파일 저장소라고도 알려진 중앙 저장소에서 해당 소프트웨어를 업데이트합니다. SSM이 지원하는 드라이버 버전은 드라이버 다운로드 웹 사이트 및 지원 소프트웨어 CD에서 특수 아이콘으로 표시됩니다. SSM에 대한 유틸리티를 다운로드하거나 자세한 내용을 보려면 http://h18000.www1.hp.com/im/ssmwp.html을 참조하십시오.

Proactive Change Notification

Proactive Change Notification 프로그램은 다음과 같은 이유로 가입자의 선택 보안 웹 사이트를 사용합니다.

- 최대 60일 이전에 대부분의 상업용 컴퓨터와 서버의 하드웨어 및 소프트웨어 변경 사항을 PCN(Proactive Change Notification) 전자 우편으로 사용자에게 자동 전송합니다.
- 대부분의 상업용 컴퓨터와 서버용 Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins 및 Dirver Alerts를 포함한 전자 우편을 사전에 자동으로 사용자에게 전송합니다.

개인 프로파일을 작성하면 특정 IT 환경에 적합한 정보만 받을 수 있습니다. Proactive Change Notification 프로그램 및 사용자 정의 프로파일 작성에 대한 자세한 내용은 http://www.hp.com/go/pcn을 참조하십시오.

ActiveUpdate

ActiveUpdate는 HP의 클라이언트 기반 응용프로그램입니다. ActiveUpdate 클라이언트는 로컬 시스템에서 실행되며, 사용자 정의 프로파일을 사용하여 대부분의 HP 상업용 컴퓨터와 서버에 대한 소프트웨어 업데이트를 사전에 자동으로 다운로드합니다. 이 다운로드된 소프트웨어 업데이트는 HP 클라이언트 관리자 소프트웨어 및 시스템 소프트웨어 관리자가 배치하고자 하는 시스템에 지능적으로 배치될 수 있습니다.

ActiveUpdate, 응용프로그램 다운로드 및 사용자 정의 프로파일 작성에 관한 자세한 내용을 보려면 http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html을 참조하십시오.

ROM 플래시

이 컴퓨터는 프로그래밍할 수 있는 플래시 ROM(읽기 전용 메모리)이 함께 제공됩니다. Computer Setup(F10) 유틸리티에서 암호를 설정하여 ROM을 실수로 업데이트하거나 덮어 쓰지 않도록 보호할 수 있습니다. 이 기능은 컴퓨터의 작동 무결성을 보장하는 데 중요합니다. ROM을 업그레이드할 필요가 있는 경우 다음과 같이 하십시오.

- HP에서 업그레이드된 ROMPaq 디스켓을 주문하십시오.
- http://h18000.www1.hp.com/im/ssmwp.html에서 최신 ROMPaq 이미지를 다운로드 하십시오.

주의: 최대 ROM 보호를 위해 설정 암호를 설정해야 합니다. 암호 설정은 무단 ROM 업그레이드를 방지합니다. 시스템 관리자는 시스템 소프트웨어 관리자(System Software Manager)를 사용하여 동시에 한 대 이상의 PC에 암호를 설정할 수 있습니다. 자세한 내용은 http://h18000.www1.hp.com/im/ssmwp.html을 참조하십시오.

원격 ROM 플래시

시스템 관리자는 원격 ROM 플래시를 사용하여 중앙 네트워크 관리 콘솔에서 직접 원격 HP 컴퓨터에 ROM을 안전하게 업그레이드할 수 있습니다. 시스템 관리자가 여러 컴퓨터와 PC에서 원격으로 이 작업을 수행할 수 있으므로 네트워크를 통해 HP PC ROM 이미지를 보다 일관성 있게 배치하고 효율적으로 제어할 수 있을 뿐만 아니라 생산성을 향상하고 총소유 비용을 절감할 수 있게 되었습니다.

컴퓨터의 전원을 켜거나 Remote Wakeup(원격 시작) 동안 켜 놓아야 원격 ROM 플래시를 사용할 수 있습니다.

원격 ROM 플래시에 대한 자세한 내용은 http://h18000.www1.hp.com/im/prodinfo.html에서 HP 클라이언트 관리자 소프트웨어 또는 시스템 소프트웨어 관리자를 참조하십시오.

HPQFlash

HPQFlash 유틸리티는 Windows 운영 체제를 통해 각 PC의 시스템 ROM을 로컬에서 업데이트하거나 복원하는 데 사용됩니다.

HPQFlash에 대한 자세한 내용은 http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html을 참조하십시오.

FailSafe 부트 블록 ROM

ROM을 업그레이드하는 동안 정전과 같은 ROM 플래시 오류가 발생할 경우 FailSafe 부트 블록 ROM을 사용하여 시스템을 복구할 수 있습니다. 부트 블록은 시스템에 전원이 공급될 때 유효한 시스템 ROM 플래시를 확인하는 플래시 보호 ROM 섹션입니다.

- 시스템 ROM이 유효하면 시스템이 정상적으로 시작합니다.
- 시스템 ROM이 유효성 검사에 실패하면 FailSafe 부트 블록 ROM은 유효한 이미지로 시스템 ROM을 프로그래밍하는 ROMPaq 디스켓에서 시스템을 시작하도록 지원합니다.

부트 블록에서 유효하지 않은 시스템 ROM을 감지하면 시스템 전원 LED 표시등이 2초 간격으로 매초마다 한 번씩 8번 깜박입니다. 또한 여덟 번의 경고음이 동시에 들립니다. 일부 모델의 경우 부트 블록 복구 모드 메시지가 화면에 표시됩니다.

부트 블록 복구 모드로 들어간 후 시스템을 복구하려면 다음 단계를 모두 따르십시오.

1. 디스켓 드라이브에 디스켓이 들어 있는 경우 디스켓을 꺼내고 전원을 끕니다.
2. ROMPaq 디스켓을 디스켓 드라이브에 넣습니다.
3. 시스템 전원을 켭니다.
4. ROMPaq 디스켓이 없으면 디스켓을 넣고 컴퓨터를 재시작하라는 메시지가 표시됩니다.
5. 암호가 설정되어 있는 경우 Caps Lock 표시등이 켜지고 암호를 입력하라는 메시지가 표시됩니다.
6. 설정된 암호를 입력합니다.

7. 성공적으로 시스템이 디스켓에서 시작하고 ROM을 다시 프로그래밍하면 세 개의 키보드 표시등이 켜집니다. 소리가 점점 커지는 연속 경고음은 성공적으로 완료되었음을 의미합니다.
8. 디스켓을 꺼내고 전원을 끕니다.
9. 컴퓨터를 재시작하려면 전원을 켭니다.

아래 표는 PS/2 키보드가 연결되어 있는 경우 부트 블록 ROM이 사용하는 다양한 키보드 표시등 조합과 각 조합에 대한 의미와 동작을 설명합니다.

부트 블록 ROM에서 사용되는 키보드 표시등 조합

FailSafe Boot Block 모드	키보드 LED 색상	키보드 LED 작동	상태/메시지
Num Lock	녹색	켜짐	ROMPaq 디스켓이 없음. 오류가 있거나 드라이브가 준비되지 않았습니다.
Caps Lock	녹색	켜짐	암호를 입력하십시오.
Num, Caps, Scroll Lock	녹색	N, C, SL 한 번에 하나씩 연속적으로 깜박임	키보드가 네트워크 모드에서 잠겼습니다.
Num, Caps, Scroll Lock	녹색	켜짐	부트 블록 ROM이 성공적으로 플래시되었습니다. 전원을 끄고 재부팅하십시오.

✎ USB 키보드의 진단 표시등이 깜박이지 않습니다.

설정 복제

관리자는 다음 절차를 통해 같은 모델의 다른 컴퓨터에 설정 구성을 쉽게 복사할 수 있습니다. 또한 더 빠르고 일관성 있게 여러 컴퓨터를 구성할 수 있습니다.

두 절차 모두 HP 드라이브 키와 같은 디스켓 드라이브 또는 지원되는 USB 플래시 미디어 장치가 필요합니다.

단일 컴퓨터에 복사

주의: 설치 구성은 모델에 따라 다릅니다. 원 컴퓨터와 대상 컴퓨터가 같은 모델이 아닌 경우 파일 시스템 오류가 발생할 수 있습니다. 예를 들어, D510 Ultra-slim Desktop에서 D510 e-pc로 설치 구성을 복사하지 마십시오.

1. 복사할 설치 구성을 선택합니다. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. 디스켓 또는 USB 플래시 미디어 장치를 삽입합니다.
4. **File(파일) > Save to Diskette(디스켓에 저장)**을 누릅니다. 화면 지침에 따라 구성 디스켓 또는 USB 플래시 미디어 장치를 작성합니다.
5. 구성할 컴퓨터를 끄고 구성 디스켓 또는 USB 플래시 미디어 장치를 삽입합니다.
6. 구성할 컴퓨터를 켭니다. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 건너뜁니다.
7. **File(파일) > Restore from Diskette(디스켓에서 복원)**을 누른 다음 화면 지침을 따릅니다.
8. 구성이 완료되면 컴퓨터를 다시 시작합니다.

여러 컴퓨터에 복사

주의: 설치 구성은 모델에 따라 다릅니다. 원 컴퓨터와 대상 컴퓨터가 같은 모델이 아닌 경우 파일 시스템 오류가 발생할 수 있습니다. 예를 들어, D510 Ultra-slim Desktop에서 D510 e-pc로 설치 구성을 복사하지 마십시오.

이 방법은 구성 디스켓 또는 USB 플래시 미디어 장치를 준비하는 데 시간이 조금 걸리지만 상당히 빠르게 대상 컴퓨터에 구성을 복사할 수 있습니다.

Windows 2000에서는 부팅 디스켓을 만들 수 없습니다. 이 과정에서 또는 부팅용 USB 플래시 미디어 장치를 만들 때 부팅 디스켓이 필요합니다. 부팅 디스켓을 만드는 데 Windows 9x 또는 Windows XP를 사용할 수 없는 경우, 대신 단일 컴퓨터에 복사하는 방법을 사용하십시오(10페이지의 "단일 컴퓨터에 복사" 참조).

1. 부팅 디스켓 또는 USB 플래시 미디어 장치를 만듭니다. 12페이지의 "부팅 디스켓", 13페이지의 "지원되는 USB 플래시 미디어 장치" 또는 16페이지의 "지원되지 않는 USB 플래시 미디어 장치"를 참조하십시오.

주의: 일부 컴퓨터는 USB 플래시 미디어 장치에서 부팅되지 않습니다. Computer Setup(F10) 유틸리티에서 기본 부팅 순서가 USB 장치 다음에 하드 드라이브인 경우, 컴퓨터는 USB 플래시 미디어 장치에서 부팅될 수 있습니다. 그렇지 않으면 부팅 디스켓을 사용해야 합니다.

2. 복사할 설치 구성을 선택합니다. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
3. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

4. 부팅 디스켓 또는 USB 플래시 미디어 장치를 삽입합니다.
5. **File(파일) > Save to Diskette(디스켓에 저장)**을 누릅니다. 화면 지침에 따라 구성 디스켓 또는 USB 플래시 미디어 장치를 작성합니다.
6. 설정 복제용 BIOS 유틸리티(repset.exe)를 다운로드하고 구성 디스켓 또는 USB 플래시 미디어 장치에 복사합니다. 이 유틸리티는 http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html에서 찾을 수 있습니다.
7. 구성 디스켓 또는 USB 플래시 미디어 장치에서 다음 명령어가 포함된 autoexec.bat 파일을 만듭니다.

   repset.exe

8. 구성할 컴퓨터를 끕니다. 구성 디스켓 또는 USB 플래시 미디어 장치를 삽입하고 컴퓨터를 켭니다. 구성 유틸리티가 자동으로 실행됩니다.
9. 구성이 완료되면 컴퓨터를 다시 시작합니다.

부팅 장치 만들기

부팅 디스켓

이 지침은 Windows XP Professional 및 Home Edition용입니다. Windows 2000은 부팅 디스켓 작성 기능을 지원하지 않습니다.

1. 디스켓 드라이브에 디스켓을 넣습니다.
2. **시작**을 누른 다음 **내 컴퓨터**를 누릅니다.
3. 디스켓 드라이브를 마우스 오른쪽 버튼으로 누른 다음 **포맷**을 누릅니다.
4. **MS-DOS 시작 디스크 만들기** 확인란을 선택한 다음 **시작**을 누릅니다.

11페이지의 "여러 컴퓨터에 복사"로 되돌아 갑니다.

지원되는 USB 플래시 미디어 장치

HP 드라이브 키 또는 DiskOnKey와 같은 지원되는 장치에는 사전 설치된 이미지가 있어 간단하게 부팅 장치로 만들 수 있습니다. 사용하는 드라이브 키에 이 이미지가 없는 경우, 이 단원 뒷부분의 절차를 수행하십시오(16페이지의 "지원되지 않는 USB 플래시 미디어 장치" 참조).

주의: 일부 컴퓨터는 USB 플래시 미디어 장치에서 부팅되지 않습니다. Computer Setup(F10) 유틸리티에서 기본 부팅 순서가 USB 장치 다음에 하드 드라이브인 경우, 컴퓨터는 USB 플래시 미디어 장치에서 부팅될 수 있습니다. 그렇지 않으면 부팅 디스켓을 사용해야 합니다.

부팅 USB 플래시 미디어 장치를 만들려면 다음이 필요합니다.

- 다음 시스템 중 하나가 필요합니다.
  - Compaq Evo D510 Ultra-slim Desktop
  - Compaq Evo D510 Convertible Minitower/Small Form Factor
  - HP Compaq 비즈니스 데스크탑 d530 시리즈 - Ultra-slim Desktop, Small Form Factor 또는 Convertible Minitower
  - Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c 또는 N1000c 노트북
  - Compaq Presario 1500 또는 2800 노트북

  각 BIOS에 따라 향후 시스템에서 HP 드라이브 키 부팅을 지원할 수도 있습니다.

주의: 상기 나열된 제품 외의 컴퓨터를 사용하는 경우, Computer Setup(F10) 유틸리티의 기본 부팅 순서가 USB 장치 다음에 하드 드라이브인지 확인하십시오.

- 다음 저장 장치 모듈 중 하나가 필요합니다.
  - 16MB HP 드라이브 키
  - 32MB HP 드라이브 키
  - 32MB DiskOnKey
  - 64MB HP 드라이브 키
  - 64MB DiskOnKey

- ❏ 128MB HP 드라이브 키
- ❏ 128MB DiskOnKey

■ FDISK 및 SYS 프로그램이 있는 부팅 DOS 디스켓. SYS를 사용할 수 없는 경우, FORMAT이 사용될 수 있으며, 드라이브 키의 모든 기존 파일이 손실됩니다.

1. 컴퓨터를 끕니다.
2. 드라이브 키를 컴퓨터의 USB 포트 중 하나에 삽입하고 USB 디스켓 드라이브를 제외한 다른 USB 저장 장치를 모두 제거합니다.
3. FDISK.COM 및 SYS.COM 또는 FORMAT.COM이 있는 부팅 DOS 디스켓을 디스켓 드라이브에 삽입하고 컴퓨터를 켜서 DOS 디스켓으로 부팅합니다.
4. **FDISK**를 입력하고 Enter를 눌러 A:\ 프롬프트에서 FDISK를 실행합니다. 메시지가 나타나면 **Yes(예)(Y)**를 눌러 대용량 디스크를 지원하도록 설정합니다.
5. Choice [**5**]를 입력하여 시스템의 드라이브를 표시합니다. 나열된 드라이브 중 크기가 가장 일치하는 드라이브가 드라이브 키가 됩니다. 일반적으로 목록의 가장 마지막에 있는 드라이브입니다. 드라이브 문자를 메모해 두십시오.

   드라이브 키 드라이브: _____

주의: 드라이브가 드라이브 키와 일치하지 않은 경우, 진행하지 마십시오. 데이터를 잃을 수도 있습니다. USB 포트를 모두 검사하여 추가 저장 장치가 있는지 확인합니다. 추가 저장 장치가 있으면 삭제하고 컴퓨터를 재부팅한 다음 단계 4를 수행합니다. 추가 저장 장치가 없으면 시스템에서 드라이브 키를 지원하지 않거나 드라이브 키에 결함이 있는 경우입니다. 드라이브 키를 부팅용으로 만들려고 하지 마십시오.

6. **Esc** 키를 눌러 FDISK를 종료하고 A:\ 프롬프트로 돌아갑니다.
7. 부팅용 DOS 디스켓에 SYS.COM이 있는 경우 단계 8로 이동하고, 없는 경우 단계 9로 이동합니다.
8. A:\ 프롬프트에 **SYS x:**를 입력합니다. x는 위에서 메모한 드라이브 문자입니다. 단계 13으로 이동합니다.

주의: 드라이브 키에 대해 올바른 드라이브 문자를 입력했는지 확인하십시오.

시스템 파일이 전송된 후에 SYS가 A:\ 프롬프트로 돌아갑니다.

9. 보관할 파일을 드라이브 키에서 다른 드라이브(예: 시스템의 내장 하드 드라이브)의 임시 디렉토리로 복사합니다.
10. A:\ 프롬프트에 **FORMAT /S X:**를 입력합니다. X는 이전에 메모한 드라이브 문자입니다.

주의: 드라이브 키에 대해 올바른 드라이브 문자를 입력했는지 확인하십시오.

FORMAT을 입력하면 각 단계마다 계속 진행할지 여부를 묻는 경고 메시지가 나타납니다. 메시지가 나타날 때마다 **y**를 입력합니다. FORMAT을 실행하면 드라이브 키를 포맷하고 시스템 파일을 추가하고 볼륨 레이블을 묻습니다.

11. 레이블이 없는 경우 **Enter**를 누르거나 필요한 경우 레이블을 입력합니다.
12. 단계 9에서 저장한 파일을 드라이브 키에 다시 복사합니다.
13. 디스켓을 꺼내고 컴퓨터를 재부팅합니다. 컴퓨터가 C 드라이브처럼 드라이브 키에서 부팅됩니다.

기본 부팅 순서는 컴퓨터마다 다르며 Computer Setup(F10) 유틸리티에서 변경할 수 있습니다.

Windows 9x에서 DOS 버전을 사용한 경우, Windows 로고 화면이 잠시 나타납니다. 이 화면을 나타나지 않게 하려면 드라이브 키의 루트 디렉토리에 LOGO.SYS라는 빈 파일을 추가합니다.

11페이지의 "여러 컴퓨터에 복사"로 되돌아 갑니다.

지원되지 않는 USB 플래시 미디어 장치

주의: 일부 컴퓨터는 USB 플래시 미디어 장치에서 부팅되지 않습니다. Computer Setup(F10) 유틸리티에서 기본 부팅 순서가 USB 장치 다음에 하드 드라이브인 경우, 컴퓨터는 USB 플래시 미디어 장치에서 부팅될 수 있습니다. 그렇지 않으면 부팅 디스켓을 사용해야 합니다.

부팅 USB 플래시 미디어 장치를 만들려면 다음이 필요합니다.

- 다음 시스템 중 하나가 필요합니다.
  - ❏ Compaq Evo D510 Ultra-slim Desktop
  - ❏ Compaq Evo D510 Convertible Minitower/Small Form Factor
  - ❏ HP Compaq 비즈니스 데스크탑 d530 시리즈 - Ultra-slim Desktop, Small Form Factor 또는 Convertible Minitower
  - ❏ Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c 또는 N1000c 노트북
  - ❏ Compaq Presario 1500 또는 2800 노트북

  각 BIOS에 따라 향후 시스템에서 USB 플래시 미디어 장치 부팅을 지원할 수도 있습니다.

주의: 상기 나열된 제품 외의 컴퓨터를 사용하는 경우, Computer Setup(F10) 유틸리티의 기본 부팅 순서가 USB 장치 다음에 하드 드라이브인지 확인하십시오.

- FDISK 및 SYS 프로그램이 있는 부팅 DOS 디스켓. SYS를 사용할 수 없는 경우, FORMAT이 사용될 수 있으며, 드라이브 키의 모든 기존 파일이 손실됩니다.

1. SCSI, ATA RAID 또는 SATA 드라이브가 장착된 시스템에 PCI 카드가 있는 경우, 컴퓨터를 끄고 전원 코드를 분리합니다.

주의: 전원 코드를 반드시 분리해야 합니다.

2. 컴퓨터를 열고 PCI 카드를 제거합니다.
3. USB 플래시 미디어 장치를 컴퓨터의 USB 포트 중 하나에 삽입하고 USB 디스켓 드라이브를 제외한 다른 USB 저장 장치를 모두 제거합니다. 컴퓨터 덮개를 닫습니다.

4. 전원 코드를 연결하고 컴퓨터를 켭니다. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 눌러 Computer Setup 유틸리티로 이동합니다.
5. **Advanced/PCI devices(고급/PCI 장치)**로 이동하여 IDE 및 SATA 컨트롤러를 비활성화합니다. SATA 컨트롤러가 비활성화되면 컨트롤러가 할당된 IRQ를 메모합니다. 나중에 IRQ를 다시 할당해야 합니다. 변경 사항을 확인하고 Setup 유틸리티를 종료합니다.

   SATA IRQ: _____
6. FDISK.COM 및 SYS.COM 또는 FORMAT.COM이 있는 부팅 DOS 디스켓을 디스켓 드라이브에 삽입하고 컴퓨터를 켜서 DOS 디스켓으로 부팅합니다.
7. FDISK를 실행하고 USB 플래시 미디어 장치에 기존 파티션이 있으면 삭제합니다. 새 파티션을 생성하고 활성화합니다. **Esc** 키를 눌러 FDISK를 종료합니다.
8. FDISK를 종료할 때 시스템이 자동으로 다시 시작되지 않는 경우, **Ctrl**+**Alt**+**Del** 키를 눌러 DOS 디스켓에서 재부팅합니다.
9. A:\ 프롬프트에서 **FORMAT C: /S**를 입력하고 **Enter** 키를 누릅니다. FORMAT을 실행하면 USB 플래시 미디어 장치를 포맷하고 시스템 파일을 추가하고 볼륨 레이블을 묻습니다.
10. 레이블이 없는 경우 **Enter**를 누르거나 필요한 경우 레이블을 입력합니다.
11. 컴퓨터의 전원을 끈 후 전원 코드를 뽑습니다. 컴퓨터를 열고 이전에 제거한 PCI 카드를 다시 설치합니다. 컴퓨터 덮개를 닫습니다.
12. 전원 코드를 연결하고 디스켓을 꺼낸 다음 컴퓨터를 켭니다.
13. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 눌러 Computer Setup 유틸리티로 이동합니다.
14. **Advanced/PCI Devices(고급/PCI 장치)**로 이동하고 단계 5에서 비활성화한 IDE 및 SATA 컨트롤러를 다시 활성화합니다. SATA 컨트롤러를 원래 IRQ에 놓습니다.
15. 변경 사항을 저장하고 종료합니다. 컴퓨터가 C 드라이브처럼 USB 플래시 미디어 장치에서 부팅됩니다.

기본 부팅 순서는 컴퓨터마다 다르며 Computer Setup(F10) 유틸리티에서 변경할 수 있습니다.

Windows 9x에서 DOS 버전을 사용한 경우, Windows 로고 화면이 잠시 나타납니다. 이 화면을 나타나지 않게 하려면 드라이브 키의 루트 디렉토리에 LOGO.SYS라는 빈 파일을 추가합니다.

11페이지의 "여러 컴퓨터에 복사"로 되돌아 갑니다.

이중 상태 전원 버튼

ACPI(Advanced Configuration and Power Interface)를 Windows 2000, Windows XP Professional 및 Home Edition에서 사용할 수 있도록 설정하면 전원 버튼을 켜기/끄기 스위치나 일시 중단 버튼으로 사용할 수 있습니다. 대기 상태 기능은 전원을 완전히 끄지 않는 대신에 컴퓨터를 저전력 대기 상태로 만듭니다. 이 기능을 사용하면 응용프로그램을 닫지 않고도 전원을 신속하게 끄고 데이터 손실 없이 동일한 작업 상태로 신속하게 돌아갈 수 있습니다.

전원 버튼의 구성을 변경하려면 다음 단계를 완료하십시오.

1. Windows 2000에서 **시작** 버튼을 마우스 왼쪽 버튼으로 누른 다음 **설정 > 제어판 > 전원 옵션**을 선택합니다.

   Windows XP Professional 및 Home Edition에서 **시작** 버튼을 마우스 왼쪽 버튼으로 누른 다음 **제어판 > 성능 및 유지 관리 > 전원 옵션**을 선택합니다.

2. **전원 옵션 등록 정보**에서 **고급** 탭을 선택합니다.
3. **전원** 단추 섹션에서 원하는 전원 버튼 설정을 선택합니다.

전원 버튼을 대기 상태 버튼처럼 작동하도록 구성한 후 전원 버튼을 눌러 시스템을 저전력 상태(대기 상태)로 설정하십시오. 전원 버튼을 다시 눌러 시스템을 대기 상태에서 완전 전력 상태로 빠르게 변경하십시오. 시스템의 모든 전원을 완전히 끄려면 4초 동안 전원 버튼을 누르십시오.

주의: 시스템이 작동하고 있는 경우 전원 버튼을 사용하여 컴퓨터를 끄지 마십시오. 시스템이 제대로 종료되지 않은 상태에서 전원을 끄면 하드 드라이브의 데이터가 손상되거나 손실될 수 있습니다.

월드 와이드 웹 사이트

HP 엔지니어는 HP와 타사 공급업체가 개발한 소프트웨어를 엄격하게 테스트 및 디버깅하고 운영 체제별 지원 소프트웨어를 개발하여 HP 컴퓨터에 대한 성능, 호환성 및 신뢰성을 보장합니다.

새 운영 체제나 증보판 운영 체제로 전환할 경우 해당 운영 체제용으로 제작된 지원 소프트웨어를 실행해야 합니다. 컴퓨터에 설치된 버전과 다른 Microsoft Windows 버전을 실행하려면 해당 장치 드라이버와 유틸리티를 설치하여 모든 기능이 제대로 지원되고 작동하는지 확인해야 합니다.

HP는 최신 지원 소프트웨어를 보다 쉽게 찾아서 액세스하고, 평가 및 설치할 수 있도록 노력해 왔습니다. 웹 사이트 (http://www.hp.com/support)에서 소프트웨어를 다운로드 받을 수 있습니다.

웹 사이트에서 HP 컴퓨터가 최신 Microsoft Windows 운영 체제를 실행하는 데 필요한 최신 장치 드라이버, 유틸리티 및 플래시 가능한 ROM 이미지를 찾을 수 있습니다.

블록 및 파트너 구축

HP 관리 솔루션은 다른 시스템 관리 응용프로그램을 통합하고 다음과 같은 산업 표준을 준수합니다.

- DMI(데스크탑 관리 인터페이스) 2.0
- WOL(Wake on LAN) 기술
- ACPI
- SMBIOS
- PXE(Pre-boot Execution) 지원

자산 추적 및 보안

컴퓨터에 추가된 자산 추적 기능은 HP Insight Manager, HP 클라이언트 관리자(HP Client Manager) 또는 기타 시스템 관리 응용프로그램을 사용하여 관리할 수 있는 중요한 자산 추적 데이터를 제공합니다. 자산 추적 기능과 해당 제품 간의 완벽한 자동 통합으로 사용자 환경에 가장 적합한 관리 도구를 선택하고 기존 도구에 대한 투자를 활용할 수 있습니다.

HP는 중요한 부품 및 정보에 대한 액세스를 제어하는 솔루션을 제공합니다. ProtectTools 내장 보안 장치는 데이터에 대한 무단 액세스를 방지하며 시스템 무결성을 검사하고 시스템에 액세스하려는 다른 사용자를 인증합니다. 일부 모델에서 사용할 수 있는 ProtectTools, Smart Cover Sensor 및 Smart Cover Lock과 같은 보안 기능은 개인용 컴퓨터의 내부 부품에 대한 무단 액세스를 차단합니다. 병렬, 직렬 또는 USB 포트를 비활성화하거나 이동식 매체 부팅 기능을 비활성화하여 중요한 데이터 자산을 보호할 수 있습니다. Memory Change 및 Smart Cover Sensor 경보는 시스템 관리 응용프로그램에 자동으로 전달되어 컴퓨터의 내부 부품과 관련된 사전 알림 기능을 제공할 수 있습니다.

Protect Tools, Smart Cover Sensor 및 Smart Cover Lock은 일부 시스템의 선택 사양으로 사용할 수 있습니다.

다음 유틸리티를 사용하여 HP 컴퓨터의 보안 설정을 관리하십시오.

- 로컬에서 Compaq Computer Setup 유틸리티 사용. Computer Setup 유틸리티 사용에 대한 추가 정보와 지침은 컴퓨터와 함께 제공된 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.
- 원격으로 HP 클라이언트 관리자(HP Client Manager) 또는 시스템 소프트웨어 관리자(System Software Manager) 사용. 이 소프트웨어를 사용하여 간단한 명령행 유틸리티에서 보안 설정을 안전하고 일관성 있게 배치하고 제어할 수 있습니다.

다음 표와 섹션은 Computer Setup(F10) 유틸리티를 통해 로컬에서 관리되는 컴퓨터의 보안 기능에 대한 설명입니다.

보안 기능 개요

기능	용도	설정 방법
이동식 미디어 부트 제어	이동식 미디어 드라이브에서 부팅을 방지합니다(일부 드라이브에서 사용 가능).	Computer Setup(F10) 유틸리티 메뉴에서 설정
직렬, 병렬, USB 또는 적외선 인터페이스 제어	통합된 직렬, 병렬, USB(범용 직렬 버스) 또는 적외선 인터페이스를 통한 데이터 전송을 방지합니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정
시작 암호	암호를 입력할 때까지 컴퓨터 사용을 방지합니다. 이 기능은 내부 시스템 시작 및 재시작 모두 적용할 수 있습니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정
설정 암호	암호를 입력할 때까지 컴퓨터 재구성(Computer Setup 유틸리티 사용)을 방지합니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정
내장 보안 장치	암호화 및 암호 보호를 사용하여 데이터에 대한 무단 액세스를 차단합니다. 시스템 무결성을 검사하고 시스템에 액세스하려는 다른 사용자를 인증합니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정
DriveLock	멀티베이 하드 드라이브의 데이터에 대한 무단 액세스를 차단합니다. 이 기능은 특정 모델에만 적용됩니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정
Smart Cover Sensor	컴퓨터 덮개나 측면 패널이 열려 있음을 나타냅니다. 덮개나 측면 패널을 연 후 컴퓨터를 재시작 시 암호를 요구하도록 설정할 수 있습니다. 이 기능에 대한 자세한 내용은 *Documentation Library* CD의 *하드웨어 참조 설명서*를 참조하십시오. 이 기능은 특정 모델에만 적용됩니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정

✎ Computer Setup에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오. 보안 기능 지원은 해당 컴퓨터 구성에 따라 다를 수 있습니다.

보안 기능 개요*(계속)*

기능	용도	설정 방법
MBR(마스터 부트 레코드) 보안	현재 부팅 디스크의 마스터 부트 레코드를 실수로든 고의로든 변경하지 못하게 할 수 있으며 MBR을 마지막 상태로 복구할 수 있는 방법을 제공합니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정
Memory Change Alerts	메모리 모듈이 추가, 이동 또는 제거될 때 감지하고 사용자와 시스템 관리자에게 알립니다.	Memory Change Alerts 활성화에 대한 내용은 온라인 *Intelligent Manageability 설명서*를 참조하십시오.

✎ Computer Setup에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오. 보안 기능 지원은 해당 컴퓨터 구성에 따라 다를 수 있습니다.

보안 기능 개요*(계속)*

기능	용도	설정 방법
소유자 태그	암호로 보호되는 시스템을 시작하는 동안 시스템 관리자가 정의한 대로 소유자 태그를 표시합니다.	Computer Setup(F10) 유틸리티 메뉴에서 설정
케이블 잠금 장치	불필요한 구성 변경이나 부품 제거를 방지하기 위해 컴퓨터 내부에 액세스하지 못하도록 합니다. 또한 도난 방지를 위해 고정된 위치에 컴퓨터를 안전하게 보호하기 위해 사용할 수 있습니다.	고정된 위치에 컴퓨터를 안전하게 보호하도록 케이블 잠금 장치 설치
보안 루프 장치	불필요한 구성 변경이나 부품 제거를 방지하기 위해 컴퓨터 내부에 액세스하지 못하도록 합니다.	불필요한 구성 변경이나 부품 제거를 방지하기 위해 보안 루프에 잠금 장치 설치

✎ Computer Setup에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오. 보안 기능 지원은 해당 컴퓨터 구성에 따라 다를 수 있습니다.

암호 보안

시작 암호는 컴퓨터를 켜거나 재시작할 때마다 응용프로그램이나 데이터에 액세스할 때 암호를 입력하도록 설정하여 컴퓨터의 무단 사용을 방지합니다. 설정 암호는 특히 Computer Setup에 대한 무단 액세스를 방지하며 시작 암호에 대해 우선적으로 적용하는 데 사용될 수도 있습니다. 즉, 시작 암호를 입력하라는 메시지가 표시될 때 설정 암호를 입력하면 컴퓨터에 액세스할 수 있습니다.

네트워크 전체에 걸친 설정 암호는 시작 암호가 설정되어 있는 경우 시스템 관리자가 이 암호를 몰라도 모든 네트워크 시스템에 로그인하여 유지 관리할 수 있도록 설정할 수 있습니다.

Computer Setup을 사용하여 설정 암호 설정

시스템에 내장 보안 장치가 장착되어 있는 경우, 29페이지의 "내장 보안"을 참조하십시오.

Computer Setup을 통해 설정 암호를 설정하면 암호를 입력할 때까지 컴퓨터의 재구성(Computer Setup(F10) 유틸리티 사용)을 방지합니다.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. **Security(보안)**를 선택한 후 **Setup Password(설정 암호)**를 선택하고 화면의 지침을 따르십시오.
4. 종료하기 전에 **File(파일) > Save Changes and Exit(변경 사항 저장 후 종료)**를 누릅니다.

Computer Setup을 사용하여 시작 암호 사용 설정

Computer Setup을 통해 시작 암호를 설정하면 전원이 켜졌을 때 암호를 입력하지 않으면 컴퓨터에 액세스할 수 없습니다. 시작 암호가 설정되면 Computer Setup이 Security(보안) 메뉴 아래에 Password Options(암호 옵션)를 표시합니다. 암호 옵션은 Password Prompt on Warm Boot(웜 부팅시 암호 프롬프트)를 포함합니다. Password Prompt on Warm Boot(웜 부팅 시 암호 프롬프트)가 활성화되면 컴퓨터를 다시 부팅할 때마다 암호를 입력해야 합니다.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. **Security(보안)**를 선택한 후 **Power-On Password(시작 암호)**를 선택하고 화면의 지침을 따르십시오.
4. 종료하기 전에 **File(파일) > Save Changes and Exit(변경 사항 저장 후 종료)**를 누릅니다.

시작 암호 입력

시작 암호를 입력하려면 다음 단계를 모두 따르십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 키 아이콘이 모니터에 나타나면 현재 사용하는 암호를 입력한 후 **Enter** 키를 누릅니다.

주의하여 입력하십시오. 입력한 문자는 보안상의 이유로 화면에 나타나지 않습니다.

틀린 암호를 입력하면 깨진 키 아이콘이 나타납니다. 다시 시도하십시오. 3번 실패할 경우 컴퓨터를 끈 후 다시 켜야 계속할 수 있습니다.

설정 암호 입력

시스템에 내장 보안 장치가 장착되어 있는 경우, 29페이지의 "내장 보안"을 참조하십시오.

설정 암호가 컴퓨터에 설정되면 Computer Setup을 실행할 때마다 암호를 입력하라는 메시지가 표시됩니다.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. 키 아이콘이 모니터에 나타나면 설정 암호를 입력한 후 **Enter**를 누르십시오.

주의하여 입력하십시오. 입력한 문자는 보안상의 이유로 화면에 나타나지 않습니다.

틀린 암호를 입력하면 깨진 키 아이콘이 나타납니다. 다시 시도하십시오. 3번 실패할 경우 컴퓨터를 끈 후 다시 켜야 계속할 수 있습니다.

시작 또는 설정 암호 변경

시스템에 내장 보안 장치가 장착되어 있는 경우, 29페이지의 "내장 보안"을 참조하십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다. 설정 암호를 변경하려면 **Computer Setup**을 실행합니다.
2. 키 아이콘이 나타나면 다음과 같이 이전 암호, 슬래시(/)나 대체 구분 문자, 새 암호, 다른 슬래시(/)나 대체 구분 문자 및 새 암호를 다시 입력하십시오.
   이전 암호/새 암호/새 암호

주의하여 입력하십시오. 입력한 문자는 보안상의 이유로 화면에 나타나지 않습니다.

3. **Enter** 키를 누릅니다.

새 암호는 컴퓨터를 다음에 켤 때 적용됩니다.

대체 구분 문자에 대한 자세한 내용은 28페이지의 "국가별 키보드 구분 문자"를 참조하십시오. 시작 암호와 설정 암호는 Computer Setup의 Security(보안) 옵션을 사용하여 변경할 수도 있습니다.

시작 또는 설정 암호 삭제

시스템에 내장 보안 장치가 장착되어 있는 경우, 29페이지의 "내장 보안"을 참조하십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다. 설정 암호를 삭제하려면 **Computer Setup**을 실행합니다.
2. 키 아이콘이 나타나면 다음과 같이 이전 암호 다음에 슬래시(/)나 대체 구분 문자를 입력하십시오.
   이전 암호/
3. **Enter** 키를 누릅니다.

대체 구분 문자에 대한 자세한 내용은 28페이지의 "국가별 키보드 구분 문자"를 참조하십시오. 시작 암호와 설정 암호는 Computer Setup의 Security(보안) 옵션을 사용하여 변경할 수도 있습니다.

국가별 키보드 구분 문자

각 키보드는 국가별 요구사항에 부합하도록 설계되었습니다. 암호를 변경하거나 삭제할 때 사용하는 구문과 키는 컴퓨터와 함께 제공되는 키보드에 따라 다릅니다.

국가별 키보드 구분 문자

그리스어	-	스위스어	-	태국어	/
남미어	-	스페인어	-	터키어	.
노르웨이어	-	슬로바키아어	/	포르투갈어	-
대만어	/	아랍어	/	폴란드어	-
덴마크어	-	영어(미국)	/	프랑스어	!
독일어	-	영어(영국)	/	프랑스어(캐나다)	é
러시아어	/	이탈리아어	-	한국어	/
벨기에어	=	일본어	/	헝가리어	-
브라질어	/	중국어	/	히브리어	.
스웨덴어/핀란드어	/	체코어	-	BHCSY*	-

*보스니아 헤르체고비나, 크로아티아, 슬로베니아 및 유고슬라비아

암호 삭제

암호를 모르면 컴퓨터에 액세스할 수 없습니다. 암호 삭제에 대한 지침은 *문제 해결 설명서*를 참조하십시오.

시스템에 내장 보안 장치가 장착되어 있는 경우, "내장 보안"을 참조하십시오.

내장 보안

ProtectTools 내장 보안 장치는 암호화와 암호 보호를 결합하여 EFS (내장 파일 시스템) 파일/폴더 암호화의 보안을 강화하고 Microsoft Outlook 및 Outlook Express의 전자 우편을 보호합니다. ProtectTools는 일부 비즈니스 데스크탑에서 CTO(Configured-To-Order) 옵션처럼 사용할 수 있습니다. ProtectTools는 데이터 보안을 가장 중요하게 여기는 HP 고객을 대상으로 합니다. 데이터에 대한 무단 액세스는 데이터 손실보다 훨씬 더 위험합니다. ProtectTools는 다음 네 개의 암호를 사용합니다.

- (F10) 설정—Computer Setup(F10) 유틸리티를 실행하고 ProtectTools를 활성화/비활성화합니다.
- 소유권 취득—시스템 관리자가 설정하고 사용하며 사용자를 인증하고 보안 매개변수를 설정합니다.
- 응급 복구 토큰—시스템 관리자가 설정하며 컴퓨터 또는 ProtectTools 칩에 오류가 발생한 경우 복구를 허용합니다.
- 기본 사용자—최종 사용자가 설정하고 사용합니다.

최종 사용자의 암호를 잃은 경우, 암호화된 데이터를 복구할 수 없습니다. 따라서 ProtectTools는 사용자의 드라이브에 저장된 데이터를 시스템 정보 시스템에 복제하거나 정기적으로 백업할 때 사용하는 것이 가장 안전합니다.

ProtectTools 내장 보안 장치는 일부 비즈니스 데스크탑에 옵션으로 설치된 TCPA 1.1 호환 보안 칩입니다. 각 ProtectTools 내장 보안 칩은 각 컴퓨터마다 고유합니다. 각 칩은 다른 컴퓨터 구성 요소(프로세서, 메모리 또는 운영 체제 등)와 독립적으로 키 보안 프로세스를 수행합니다.

ProtectTools 내장 보안 가능 컴퓨터는 Microsoft Windows 2000이나 Windows XP Professional 또는 Home Edition에서 고유한 보안 기능을 보완하고 개선합니다. 예를 들어, 운영 체제는 EFS 기반의 로컬 파일 및 폴더를 암호화할 수 있으며, ProtectTools 내장 보안 장치는 실리콘 안에 보관되어 있는 플랫폼의 루트 키에서 암호화 키를 만들어 추가 보안 기능을 제공합니다. 이 프로세스는 암호화 키 "래핑(wrapping)"으로 알려져 있습니다. ProtectTools는 ProtectTools가 없는 컴퓨터에 대한 네트워크 액세스를 차단하지 않습니다.

ProtectTools 내장 보안 장치의 주요 기능은 다음과 같습니다.

- 플랫폼 인증
- 저장 장치 보호
- 데이터 무결성

주의: 암호를 안전하게 보관하십시오. **암호화된 데이터는 암호가 없으면 액세스하거나 복구할 수 없습니다**.

암호 설정

설정

F10 Setup 유틸리티를 사용하여 설정 암호를 만들고 내장 보안 장치를 설정할 수 있습니다.

1. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

2. 위쪽 또는 아래쪽 화살표를 사용하여 언어를 선택한 다음 **Enter**를 누릅니다.
3. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **Security(보안)** 탭으로 이동한 다음 위쪽 또는 아래쪽 화살표 키를 사용하여 **Setup Password(암호 설정)**로 이동합니다. **Enter** 키를 누릅니다.

4. 암호를 입력하고 확인합니다. **F10** 키를 눌러 암호를 적용합니다.

주의하여 입력하십시오. 입력한 문자는 보안상의 이유로 화면에 나타나지 않습니다.

5. 위쪽 또는 아래쪽 화살표 키를 사용하여 **Embedded Security Device(내장 보안 장치)**로 이동합니다. **Enter**를 누릅니다.
6. 대화 상자에서 **Embedded Security Device—Disable(내장 보안 장치—사용 안함)**이 선택되어 있는 경우, 왼쪽 또는 오른쪽 화살표 키를 사용하여 **Embedded Security Device—Enable(내장 보안 장치—사용함)**로 변경합니다. 변경 사항을 적용하려면 **F10** 키를 누릅니다.

주의: Reset to Factory Settings-Reset(기본값으로 복원—재설정)을 선택하면 모든 키가 삭제되고 백업하지 않은 암호화된 데이터는 복구할 수 없게 됩니다(31페이지의 "소유권 취득 및 응급 복구 토큰" 참조). 메시지가 나타났을 때 **Reset(재설정)**만 선택하면 암호화된 데이터를 복구할 수 있습니다(34페이지의 "암호화된 데이터 복구" 참조).

7. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **File(파일)**로 이동합니다. 위쪽 또는 아래쪽 화살표 키를 사용하여 **Save Changes and Exit (변경 사항 저장 후 종료)**로 이동합니다. **Enter** 키를 누른 다음 **F10** 키를 눌러 확인합니다.

소유권 취득 및 응급 복구 토큰

소유권 취득 암호는 보안 플랫폼을 활성화 또는 비활성화하고 사용자를 인증하는 데 필요합니다. 내장 보안 장치에 장애가 발생한 경우, 응급 복구 장치에서 사용자를 인증하고 데이터 액세스를 허용합니다.

1. Windows XP Professional 또는 Home Edition을 사용하는 경우 **시작 > 모든 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > Embedded Security Initialization Wizard(내장 보안 시작 마법사)**를 누릅니다.

   Windows 2000을 사용하는 경우, **시작 > 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > Embedded Security Initialization Wizard(내장 보안 시작 마법사)**를 누릅니다.
2. **Next(다음)**을 누릅니다.
3. 소유권 취득 암호를 입력하고 확인한 다음 **Next(다음)**를 누릅니다.

주의하여 입력하십시오. 입력한 문자는 보안상의 이유로 화면에 나타나지 않습니다.

4. 기본 복구 아카이브 위치를 적용하려면 **Next(다음)**를 누릅니다.
5. 응급 복구 토큰 암호를 입력하고 확인한 다음 **Next(다음)**를 누릅니다.
6. 응급 복구 토큰 키를 저장할 디스켓을 삽입합니다. **Browse(찾아보기)**를 누르고 디스켓을 선택합니다.

주의: 응급 복구 토큰 키는 컴퓨터 또는 내장 보안 칩에 장애가 발생한 경우 암호화된 데이터를 복구하는 데 사용됩니다. **키가 없으면 데이터를 복구할 수 없습니다**. (기본 사용자 암호가 없으면 데이터에 액세스할 수 없습니다.) 이 디스켓을 안전한 장소에 보관해 두십시오.

7. **Save(저장)**를 눌러 위치 및 기본 파일 이름을 적용한 다음 **Next(다음)**를 누릅니다.
8. 보안 플랫폼이 시작되기 전에 **Next(다음)**를 눌러 설정을 확인합니다.

내장 보안 기능이 시작되지 않는다는 메시지가 나타날 수도 있습니다. 메시지를 누르지 마십시오. 나중에 누르라는 메시지가 나타나며, 이 메시지는 몇 초 후에 닫힙니다.

9. 로컬 정책 구성을 생략하려면 **Next(다음)**를 누릅니다.
10. **Start Embedded Security User Initialization Wizard(내장 보안 사용자 시작 마법사 시작)** 확인란이 선택되어 있는지 확인한 다음 **Finish(마침)**를 누릅니다.

이제 사용자 시작 마법사가 자동으로 시작됩니다.

기본 사용자

사용자가 시작하는 동안 기본 사용자 암호가 만들어집니다. 이 암호는 암호화된 데이터를 입력하고 액세스하는 데 필요합니다.

주의: 기본 사용자 암호를 보호하십시오. **이 암호가 없으면 암호화된 데이터를 액세스하거나 복구할 수 없습니다**.

1. 사용자 시작 마법사가 열리지 않는 경우 다음을 수행하십시오.

   Windows XP Professional 또는 Home Edition을 사용하는 경우, **시작 > 모든 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > User Initialization Wizard(사용자 시작 마법사)**를 누릅니다.

   Windows 2000을 사용하는 경우, **시작 > 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > User Initialization Wizard(사용자 시작 마법사)**를 누릅니다.

2. **Next(다음)**을 누릅니다.
3. 기본 사용자 키 암호를 입력하고 확인한 다음 **Next(다음)**를 누릅니다.

주의하여 입력하십시오. 입력한 문자는 보안상의 이유로 화면에 나타나지 않습니다.

4. **Next(다음)**를 눌러 설정을 확인합니다.
5. 해당 보안 기능을 선택하고 **Next(다음)**를 누릅니다.
6. 해당 전자 우편 클라이언트를 선택한 후 **Next(다음)**를 누릅니다.
7. **Next(다음)**를 눌러 암호화 인증서를 적용합니다.
8. **Next(다음)**를 눌러 설정을 확인합니다.
9. **Finish(마침)**를 누릅니다.
10. 컴퓨터를 다시 시작합니다.

암호화된 데이터 복구

ProtectTools 칩을 교체한 후 데이터를 복구하려면 다음이 필요합니다.

- SPEmRecToken.xml —응급 복구 토큰 키
- SPEmRecArchive.xml—숨겨진 폴더, 기본 위치: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools 암호
  - ❏ 설정
  - ❏ 소유권 취득
  - ❏ 응급 복구 토큰
  - ❏ 기본 사용자

1. 컴퓨터를 다시 시작합니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. 설정 암호를 입력한 다음 **Enter**를 누릅니다.
4. 위쪽 또는 아래쪽 화살표를 사용하여 언어를 선택한 다음 **Enter**를 누릅니다.
5. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **Security(보안)** 탭으로 이동한 다음 위쪽 또는 아래쪽 화살표 키를 사용하여 **Embedded Security Device(내장 보안 장치)**로 이동합니다. **Enter**를 누릅니다.
6. **Embedded Security Device—Disable(내장 보안 장치—사용 안함)**만 사용할 수 있는 경우 다음을 수행하십시오.
   a. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **Embedded Security Device—Enable(내장 보안 장치—사용함)**로 변경합니다. 변경 사항을 적용하려면 **F10** 키를 누릅니다.
   b. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **File(파일)**로 이동합니다. 위쪽 또는 아래쪽 화살표 키를 사용하여 **Save Changes and Exit(변경 사항 저장 후 종료)**로 이동합니다. **Enter**를 누른 다음 **F10** 키를 눌러 확인합니다.
   c. 단계 1로 이동합니다.

두 가지 선택을 사용할 수 있는 경우, 단계 7로 이동합니다.

7. 위쪽 또는 아래쪽 화살표 키를 사용하여 **Reset to Factory Settings—Do Not Reset(기본값으로 복원—재설정하지 않음)**으로 이동합니다. 왼쪽 또는 오른쪽 화살표 키를 한 번 누릅니다.

   다음 메시지가 나타납니다. 설정을 저장하고 종료한 경우, 이 작업을 수행하면 내장 보안 장치가 초기 설정으로 복원됩니다. 계속하려면 아무 키나 누르십시오.

   Enter를 누릅니다.

8. 이제 **Reset to Factory Settings—Reset(기본값으로 복원—재설정)**이 선택됩니다. 변경 사항을 적용하려면 **F10** 키를 누릅니다.
9. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **File(파일)**로 이동합니다. 위쪽 또는 아래쪽 화살표 키를 사용하여 **Save Changes and Exit (변경 사항 저장 후 종료)**로 이동합니다. **Enter**를 누른 다음 **F10** 키를 눌러 확인합니다.
10. 컴퓨터를 다시 시작합니다.
11. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

12. 설정 암호를 입력한 다음 **Enter**를 누릅니다.
13. 위쪽 또는 아래쪽 화살표를 사용하여 언어를 선택한 다음 **Enter**를 누릅니다.
14. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **Security(보안)** 탭으로 이동한 다음 위쪽 또는 아래쪽 화살표 키를 사용하여 **Embedded Security Device(내장 보안 장치)**로 이동합니다. **Enter**를 누릅니다.
15. 대화 상자에서 **Embedded Security Device—Disable(내장 보안 장치—사용 안함)**이 선택되어 있는 경우, 왼쪽 또는 오른쪽 화살표 키를 사용하여 **Embedded Security Device—Enable(내장 보안 장치—사용함)**로 변경합니다. **F10** 키를 누릅니다.
16. 왼쪽 또는 오른쪽 화살표 키를 사용하여 **File(파일)**로 이동합니다. 위쪽 또는 아래쪽 화살표 키를 사용하여 **Save Changes and Exit (변경 사항 저장 후 종료)**로 이동합니다. **Enter**를 누른 다음 **F10** 키를 눌러 확인합니다.

17. Windows가 열리면 다음을 수행하십시오.

    Windows XP Professional 또는 Home Edition을 사용하는 경우 **시작 > 모든 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > Embedded Security Initialization Wizard(내장 보안 시작 마법사)**를 누릅니다.

    Windows 2000을 사용하는 경우, **시작 > 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > Embedded Security Initialization Wizard(내장 보안 시작 마법사)**를 누릅니다.

18. **Next(다음)**을 누릅니다.

19. 소유권 취득 암호를 입력하고 확인합니다. **Next(다음)**를 누릅니다.

주의하여 입력하십시오. 입력한 문자는 보안상의 이유로 화면에 나타나지 않습니다.

20. **Create a New Recovery Archive(새 복구 아카이브 생성)**가 선택되어 있는지 확인합니다. **Recovery archive location(복구 아카이브 위치)**에서 **Browse(찾아보기)**를 누릅니다.

21. 기본 파일 이름을 적용하지 마십시오. 원래 파일을 대체하지 않도록 새 파일 이름을 입력합니다.

22. **Save(저장)**를 누른 후 **Next(다음)**를 누릅니다.

23. 응급 복구 토큰 암호를 입력하고 확인한 다음 **Next(다음)**를 누릅니다.

24. 응급 복구 토큰 키를 저장할 디스켓을 삽입합니다. **Browse(찾아보기)**를 누르고 디스켓을 선택합니다.

25. 기본 키 이름을 적용하지 마십시오. 원래 키와 대체되지 않도록 새 키 이름을 입력합니다.

26. **Save(저장)**를 누른 후 **Next(다음)**를 누릅니다.

27. 보안 플랫폼이 시작되기 전에 **Next(다음)**를 눌러 설정을 확인합니다.

기본 사용자 키를 로드할 수 없다는 메시지가 표시될 수 있습니다. 메시지를 누르지 마십시오. 나중에 누르라는 메시지가 나타나며, 이 메시지는 몇 초 후에 닫힙니다.

28. 로컬 정책 구성을 생략하려면 **Next(다음)**를 누릅니다.
29. **Start Embedded Security User Initialization Wizard(내장 보안 사용자 시작 마법사 시작)** 확인란을 선택 취소합니다. **Finish(마침)**를 누릅니다.
30. 도구 모음에 있는 ProtectTools 아이콘을 마우스 오른쪽 버튼으로 누르고 **Initialize Embedded Security Restoration(내장 보안 복원 시작)**을 누릅니다.

    이렇게 하면 HP ProtectTools 내장 보안 시작 마법사가 시작됩니다.
31. **Next(다음)**를 누릅니다.
32. 원래 응급 복구 토큰 키가 저장되어 있는 디스켓을 삽입합니다. **Browse(찾아보기)**를 누른 다음 토큰을 찾아서 두 번 눌러 필드에 이름을 입력합니다. 기본값은 A:\SPEmRecToken.xml입니다.
33. 원래 토큰 암호를 입력한 다음 **Next(다음)**를 누릅니다.
34. **Browse(찾아보기)**를 누른 다음 원래 복구 아카이브를 찾아서 두 번 눌러 필드에 이름을 입력합니다. 기본값은 C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml입니다.
35. **Next(다음)**를 누릅니다.
36. 복원할 시스템을 누른 다음 **Next(다음)**를 누릅니다.
37. **Next(다음)**를 눌러 설정을 확인합니다.
38. 마법사에서 보안 플랫폼이 복원되었다는 알림 메시지를 표시하면 단계 39로 이동합니다.

    마법사에서 복원하지 못했다는 알림 메시지를 표시하면 단계 10으로 이동합니다. 암호, 토큰 위치 및 이름과 아카이브 위치 및 이름을 주의하여 확인합니다.
39. **Finish(마침)**를 누릅니다.
40. Windows XP Professional 또는 Home Edition을 사용하는 경우, **시작 > 모든 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > User Initialization Wizard(사용자 시작 마법사)**를 누릅니다.

    Windows 2000을 사용하는 경우, **시작 > 프로그램 > HP ProtectTools Embedded Security Tools(HP ProtectTools 내장 보안 도구) > User Initialization Wizard(사용자 시작 마법사)**를 누릅니다.

41. **Next(다음)**을 누릅니다.
42. **Recover your basic user key(기본 사용자 키 복구)**를 누른 다음 **Next(다음)**를 누릅니다.
43. 사용자를 선택하고 해당 사용자의 원래 기본 사용자 키 암호를 입력한 다음 **Next(다음)**를 누릅니다.
44. **Next(다음)**를 눌러 설정을 확인하고 기본 복구 데이터 위치를 적용합니다.

단계 45에서 49까지는 원래 기본 사용자 구성을 다시 설치합니다.

45. 해당 보안 기능을 선택하고 **Next(다음)**를 누릅니다.
46. 해당 전자 우편 클라이언트를 선택한 후 **Next(다음)**를 누릅니다.
47. **Encryption Certificate(암호화 인증서)**를 누르고 **Next(다음)**를 눌러 적용합니다.
48. **Next(다음)**를 눌러 설정을 확인합니다.
49. **Finish(마침)**를 누릅니다.
50. 컴퓨터를 다시 시작합니다.

주의: 기본 사용자 암호를 보호하십시오. **이 암호가 없으면 암호화된 데이터를 액세스하거나 복구할 수 없습니다**.

DriveLock

DriveLock은 멀티베이 하드 드라이브의 데이터에 대한 무단 액세스를 차단하는 산업 표준 보안 기능입니다. DriveLock은 Computer Setup에 대한 확장의 일환으로 구현되었습니다. DriveLock은 DriveLock 기능이 있는 하드 드라이브가 감지된 경우에만 사용할 수 있습니다.

DriveLock은 데이터 보안을 가장 중요하게 여기는 HP 고객을 대상으로 합니다. 이러한 고객의 경우 하드 드라이브의 비용과 여기에 저장된 데이터 손실은 해당 내용에 대한 무단 액세스로 야기되는 손해에 비하면 사소한 것에 지나지 않습니다. 이러한 보안 수준과 잊어버린 암호를 조정해야 하는 실질적인 필요성 간의 조화를 위해 HP 구현의 DriveLock은 두 가지 암호 보안 체계를 사용합니다. 한 개의 암호는 시스템 관리자가 설정하여 사용하고 또 다른 암호는 일반적으로 최종 사용자가 설정하여 사용합니다. 두 암호를 모두 잊어버린 경우 드라이

브 잠금을 해제하는 데 "다른 방법"이 없습니다. 따라서 DriveLock은 하드 드라이브에 저장된 데이터를 회사 정보 시스템에 복제하거나 정기적으로 백업할 때 가장 안전하게 사용됩니다.

두 개의 DriveLock 암호를 모두 잊어버린 경우 하드 드라이브는 못 쓰게 됩니다. 이전에 정의한 사용자 정의 프로파일과 일치하지 않는 사용자의 경우 심각한 위험을 초래할 수 있습니다. 사용자 정의 프로파일과 일치하는 사용자의 경우 하드 드라이브에 저장된 데이터 특성에 경미한 위험을 초래할 수 있습니다.

DriveLock 사용

DriveLock 옵션은 Computer Setup의 보안 메뉴 아래에 나타납니다. 사용자에게 마스터 암호를 설정하거나 DriveLock을 활성화하는 옵션이 표시됩니다. 사용자 암호를 입력해야 DriveLock을 활성화할 수 있습니다. 일반적으로 시스템 관리자가 DriveLock의 초기 구성을 수행하므로 먼저 마스터 암호를 설정해야 합니다. HP는 DriveLock을 활성화하거나 비활성 상태를 유지하는 것과 관계 없이 시스템 관리자에게 마스터 암호를 설정하도록 권장합니다. 따라서 나중에 드라이브가 잠기면 관리자가 DriveLock 설정을 수정할 수 있습니다. 마스터 암호가 설정되면 시스템 관리자는 DriveLock을 활성화하거나 비활성 상태를 유지할 수 있습니다.

잠긴 하드 드라이브가 있는 경우 POST는 장치의 잠금을 해제하는 암호를 요구합니다. 시작 암호가 설정되고 이 암호가 장치의 사용자 암호와 일치하면 POST 중 사용자에게 암호를 다시 입력하라는 메시지가 표시되지 않습니다. 일치하지 않으면 DriveLock 암호를 입력하라는 메시지를 표시합니다. 이때 마스터 암호나 사용자 암호를 사용할 수 있습니다. 사용자는 정확한 암호를 두 번 입력하게 됩니다. 두 번 입력해서 실패하면 POST는 계속되지만 드라이브에는 액세스할 수 없습니다.

DriveLock 응용프로그램

DriveLock 보안 기능은 시스템 관리자가 사용자에게 일부 컴퓨터에 사용하도록 멀티베이 하드 드라이브를 제공하는 기업 환경에서 가장 많이 사용됩니다. 시스템 관리자는 특히 DriveLock 마스터 암호 설정을 포함하여 멀티베이 하드 드라이브를 구성해야 합니다. 사용자가 사용자 암호를 잊어버리거나 장비가 다른 직원에게 전달될 경우, 항상 마스터 암호를 사용하여 사용자 암호를 재설정하고 하드 드라이브에 다시 액세스할 수 있습니다.

또한 HP는 DriveLock을 활성화하도록 선택한 회사 시스템 관리자에게 마스터 암호를 설정하고 유지 관리하기 위한 회사 정책을 설립하도록 권장합니다. 이렇게 해야 직원이 회사를 그만두기 전에 고의로든 실수로든 두 개의 DriveLock 암호를 설정하지 못하게 할 수 있습니다. 이러한 경우에 하드 드라이브는 못쓰게 되므로 교체해야 합니다. 또한 마스터 암호를 설정하지 않으면 시스템 관리자는 하드 드라이브가 잠겨져서 액세스할 수 없고 승인되지 않은 소프트웨어, 다른 자산 제어 기능 및 지원에 대해 일상적인 점검을 수행할 수 없습니다.

철저한 보안이 필요하지 않는 사용자의 경우 DriveLock을 활성화하지 않는 것이 좋습니다. 이러한 범주의 사용자에는 개인 사용자 또는 하드 드라이브의 중요한 데이터를 일반적으로 사용하기 위해 유지 관리하지 않는 사용자가 포함됩니다. 이러한 사용자의 경우 두 개의 암호를 모두 잊어버려서 발생하는 하드 드라이브의 잠재적인 손실이 데이터 DriveLock이 보호하도록 설계된 값보다 훨씬 더 큽니다. Computer Setup 및 DriveLock에 대한 액세스는 설정 암호를 통해 제한할 수 있습니다. 시스템 관리자는 설정 암호를 지정하고 최종 사용자에게 알려주지 않는 방식으로 사용자의 DriveLock 사용을 제한할 수 있습니다.

Smart Cover Sensor

Smart Cover Sensor는 일부 모델에서 사용할 수 있으며 컴퓨터 덮개나 측면 패널이 열린 경우에 사용자에게 경보를 보낼 수 있는 하드웨어와 소프트웨어 기술의 조합입니다. 다음 표에서 설명한 대로 세 가지 보호 수준이 있습니다.

Smart Cover Sensor 보호 수준

수준	설정	설명
단계 0	비활성화	Smart Cover Sensor가 비활성화됩니다(기본값).
단계 1	사용자에게 알림	컴퓨터가 재시작되면 컴퓨터 커버나 측면 패널이 열려 있음을 알리는 메시지가 화면에 표시됩니다.
단계 2	설정 암호	컴퓨터가 재시작되면 컴퓨터 커버나 측면 패널이 열려 있음을 알리는 메시지가 화면에 표시됩니다. 계속하려면 설정 암호를 입력해야 합니다.

✎ 이러한 설정은 Computer Setup을 사용하여 변경할 수 있습니다. Computer Setup에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

Smart Cover Sensor 보호 수준 설정

Smart Cover Sensor 보호 수준을 설정하려면 다음 단계를 모두 따르십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. **Security(보안)**를 선택한 다음 **Smart Cover**를 선택하고 화면의 지침을 따릅니다.
4. 종료하기 전에 **File(파일) > Save Changes and Exit(변경 사항 저장 후 종료)**를 누릅니다.

Smart Cover Lock

Smart Cover Lock은 일부 HP 컴퓨터에 설치된 소프트웨어 제어 덮개 잠금 장치입니다. 이 잠금 장치는 내부 부품에 무단 접근하는 것을 방지합니다. 컴퓨터는 잠금 해제 위치로 설정된 Smart Cover Lock과 함께 제공됩니다.

주의: 최대 덮개 잠금 보안을 위해 설정 암호를 설정하십시오. 설정 암호는 Computer Setup 유틸리티에 대한 무단 액세스를 방지합니다.

Smart Cover Lock은 일부 시스템에서 선택 사양으로 사용할 수 있습니다.

Smart Cover Lock 잠금

Smart Cover Lock을 활성화하고 잠그려면 다음 단계를 모두 따르십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. **Security(보안)**, **Smart Cover** 및 **Locked(잠금)** 옵션을 차례로 선택합니다.
4. 종료하기 전에 **File(파일) > Save Changes and Exit(변경 사항 저장 후 종료)**를 누릅니다.

Smart Cover Lock 잠금 해제

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. **Security(보안) > Smart Cover > Unlocked(잠금 해제)**를 차례로 선택합니다.
4. 종료하기 전에 **File(파일) > Save Changes and Exit(변경 사항 저장 후 종료)**를 누릅니다.

Smart Cover FailSafe 키 사용

Smart Cover Lock이 활성화되어 있고 암호를 입력하여 잠금을 해제할 수 없는 경우 컴퓨터 덮개를 열려면 Smart Cover FailSafe 키가 필요합니다. 다음과 같은 경우에 이 키가 필요합니다.

- 전원 공급이 안되는 경우
- 시작이 안되는 경우
- PC 부품 고장(예: 프로세서 또는 전원 공급 장치)
- 암호를 잊어버린 경우

주의: Smart Cover FailSafe 키는 HP가 제공하는 전문 도구입니다. 공인 판매 업체나 서비스 제공 업체에 이 키를 미리 주문하십시오.

FailSafe 키를 구하려면 다음 중 하나를 수행하십시오.

- 공인 HP 대리점 또는 서비스 제공업체에 문의하십시오.
- 보증서에 기재된 해당 번호로 전화하십시오.

Smart Cover FailSafe 키 사용에 대한 자세한 내용은 *하드웨어 참조 설명서*를 참조하십시오.

MBR(마스터 부트 레코드) 보안

MBR(마스터 부트 레코드)에는 디스크에서 성공적으로 부팅하여 디스크에 저장된 데이터에 액세스하는 데 필요한 정보가 들어 있습니다. 마스터 부트 레코드 보안 기능을 사용하면 일부 컴퓨터 바이러스나 특정 디스크 유틸리티의 잘못된 사용으로 인해 MBR을 고의로든 실수로든 변경하지 않도록 할 수 있습니다. 이 기능을 사용하여 MBR을 마지막 상태로 복구할 수 있으며 시스템을 다시 시작할 때 MBR에 대한 변경 사항을 감지할 수 있습니다.

MBR 보안을 활성화하려면 다음 절차를 수행하십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. **Security(보안) > Master Boot Record Security(마스트 부트 레코드 보안) > Enabled(활성화)**를 차례로 선택합니다.
4. **Security(보안) > Save Master Boot Record(마스터 부트 레코드 저장)**를 차례로 선택합니다.
5. 종료하기 전에 **File(파일) > Save Changes and Exit(변경 사항 저장 후 종료)**를 누릅니다.

MBR 보안이 활성화되면 BIOS는 MS-DOS 또는 Windows 안전 모드 상태에서 현재 부팅 디스크의 MBR을 변경하지 못하도록 합니다.

대부분의 운영 체제는 현재 부팅 디스크의 MBR에 대한 액세스를 제어합니다. BIOS는 운영 체제가 실행 중일 때 발생할 수 있는 변경을 방지할 수 없습니다.

컴퓨터를 켜거나 재시작할 때마다 BIOS는 현재 부팅 디스크의 MBR과 이전에 저장한 MBR을 비교합니다. 변경 사항이 감지되고 현재 부팅 디스크가 MBR이 이전에 저장된 디스크와 같으면 다음 메시지가 표시됩니다.

1999—마스터 부트 레코드가 변경되었습니다.

아무 키나 눌러 Setup을 입력한 후 MBR 보안을 구성하십시오.

Computer Setup을 시작하고 다음과 같이 해야 합니다.

- 현재 부팅 디스크의 MBR을 저장합니다.
- 이전에 저장된 MBR을 복원하거나
- MBR 보안 기능을 해제합니다.

설정 암호가 있을 경우 이 암호를 알고 있어야 합니다.

변경 사항이 감지되고 현재 부팅 디스크가 MBR이 이전에 저장된 디스크와 같지 **않으면** 다음 메시지가 표시됩니다.

2000—마스터 부트 레코드 하드 드라이브가 변경되었습니다.

아무 키나 눌러 Setup을 입력한 후 MBR 보안을 구성하십시오.

Computer Setup을 시작하고 다음과 같이 해야 합니다.

- 현재 부팅 디스크의 MBR을 저장하거나
- MBR 보안 기능을 해제합니다.

설정 암호가 있을 경우 이 암호를 알고 있어야 합니다.

이전에 저장된 MBR이 손상되는 것과 같이 가능성이 희박한 경우 다음 메시지가 표시됩니다.

1998—마스터 부트 레코드를 찾을 수 없습니다.

아무 키나 눌러 Setup을 입력한 후 MBR 보안을 구성하십시오.

Computer Setup을 시작하고 다음과 같이 해야 합니다.

- 현재 부팅 디스크의 MBR을 저장하거나
- MBR 보안 기능을 해제합니다.

설정 암호가 있을 경우 이 암호를 알고 있어야 합니다.

현재 부팅 디스크를 분할하거나 포맷하기 전에

현재 부팅 디스크의 분할 또는 포맷을 변경하기 전에 MBR 보안이 비활성화되어 있는지 확인하십시오. FDISK 및 FORMAT과 같은 일부 디스크 유틸리티는 MBR 업데이트를 시도합니다. 디스크 분할 또는 포맷을 변경할 때 MBR 보안이 활성화되면 다음에 컴퓨터를 켜거나 재시작할 때 디스크 유틸리티의 오류 메시지나 MBR 보안의 경고를 받을 수 있습니다. MBR 보안을 비활성화하려면 다음 단계를 모두 따르십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 모니터 표시등에 녹색 불이 켜지면 **F10** 키를 누릅니다. 필요한 경우 **Enter**를 눌러 제목 화면을 생략하십시오.

적절한 순간에 **F10** 키를 누르지 않으면, 컴퓨터를 끄고 다시 켠 다음 **F10** 키를 다시 눌러 유틸리티에 액세스해야 합니다.

3. **Security(보안) > Master Boot Record Security(마스트 부트 레코드 보안) > Disabled(활성화)**를 차례로 선택합니다.
4. 종료하기 전에 **File(파일) > Save Changes and Exit(변경 사항 저장 후 종료)**를 누릅니다.

케이블 잠금 장치

컴퓨터의 뒷면은 작업 영역에서 컴퓨터를 물리적으로 보호할 수 있도록 케이블 잠금을 조정합니다.

그림으로 설명된 지침을 보려면 *Documentation Library* CD의 *하드웨어 참조 설명서*를 참조하십시오.

지문 인식 기술

HP의 지문 인식 기술은 사용자 암호를 입력하지 않고도 네트워크 보안을 강화하고, 로그인 프로세스를 단순화하며, 회사 네트워크 관리와 관련된 비용을 절감합니다. 가격이 알맞기 때문에 이 기술은 최첨단의 보안성이 뛰어난 조직뿐만 아니라 일반 조직에도 적합합니다.

지문 인식 기술에 대한 지원은 모델에 따라 다릅니다.

자세한 내용을 보려면 다음 웹 사이트를 참조하십시오.

http://h18000.www1.hp.com/solutions/security.

오류 알림 및 복구

오류 알림 및 복구 기능은 중요한 데이터 손실을 방지하고 예상치 못한 시스템 정지 시간을 최소화하는 혁신적인 하드웨어 및 소프트웨어 기술을 결합합니다.

오류 발생 시 오류 설명 및 권장 조치가 들어 있는 Local Alert 메시지를 표시합니다. 그러면 HP 클라이언트 관리자(HP Client Manager)를 사용하여 현재 시스템 상태를 볼 수 있습니다. 컴퓨터가 HP Insight Manager, HP 클라이언트 관리자(HP Client Manager)의 다른 시스템 관리 응용프로그램으로 관리되는 네트워크에 연결되어 있으면 해당 컴퓨터는 네트워크 관리 응용프로그램에 오류 알림을 보냅니다.

드라이브 보호 시스템

DPS(드라이브 보호 시스템)는 일부 HP 컴퓨터에 설치된 하드 드라이브에 내장된 진단 도구입니다. DPS는 보증되지 않은 하드 드라이브 교체로 발생할 수 있는 진단 문제를 지원하도록 설계되었습니다.

HP 컴퓨터가 구축될 때 설치된 각 하드 드라이브는 DPS를 사용하여 테스트되고 주요 정보는 드라이브에 영구적으로 기록됩니다. DPS가 실행될 때마다 테스트 결과가 하드 드라이브에 기록됩니다. 서비스 제공 업체는 이 정보를 사용하여 DPS 소프트웨어가 실행되었던 상태를 진단할 수 있습니다. DPS 사용에 대한 자세한 내용은 *문제 해결 설명서*를 참조하십시오.

과부하 허용 전원 공급 장치

통합된 과부하 허용 전원 공급 장치는 컴퓨터가 예상치 않은 전력 과부하 상태에 직면했을 때 신뢰성을 더욱 더 발휘합니다. 이 전원 공급 장치는 시스템 정지 시간이나 데이터 손실을 유발하지 않고 최대 2000 볼트의 전력 과부하를 견뎌냅니다.

열 감지기

열 감지기는 컴퓨터의 내부 온도를 추적하는 하드웨어 및 소프트웨어 기능입니다. 이 기능은 일반 범위를 초과할 때 내부 부품이 손상되거나 데이터가 손실되기 전에 조치를 취할 시간을 주도록 경고 메시지를 표시합니다.

색인