데스크탑 관리 설명서

HP 비즈니스 PC

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

데스크탑 관리 설명서

HP 비즈니스 PC

제 4 판(2009 년 9 월)

문서 일련 번호: 581009-AD1

본 설명서 정보

본 설명서는 일부 모델에 사전 설치된 보안 및 관리 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 정보가 유실될 수 있습니다.

주: 이런 텍스트는 중요한 추가 정보를 제공합니다.

목차

1 데스크탑 관리 개요

HP Client Management Solutions 는 네트워크 환경에서 데스크탑, 워크스테이션 및 노트북 PC 를 관리하고 제어하기 위한 표준 기반 솔루션을 제공합니다. HP 는 1995 년 업계 최초로 완벽하게 관리할 수 있는 데스크탑 PC 를 도입하면서 데스크탑 관리라는 새로운 분야의 선도 업체로 부상했습니다. 현재 HP 는 관리 기술에 대한 특허를 보유하고 있습니다. 그 후로 HP 는 데스크탑과 워크스테이션 및 노트북 PC 의 효율적인 배치, 구성 및 관리에 필요한 표준과 인프라를 개발하는 데 주도적으로 노력해 왔습니다. 또한 독자적인 관리 소프트웨어인 HP Client Management Solutions 를 개발하고 이 제품과 타사 관리 소프트웨어 솔루션과의 호환성을 위해 이들 제공업체와 긴밀한 협력 관계를 유지하고 있습니다. HP Client Management Solutions 는 PC 수명 주기 동안 총 소유 비용과 유지관리 비용을 낮추는 솔루션을 제공하기 위한 HP 의 목표를 달성하는 데 있어서 핵심 요소입니다.

데스크탑 관리에 대한 주요 특성 및 기능은 다음과 같습니다.

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

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

2 초기 구성 및 배치

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

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

- 사전 설치된 소프트웨어 이미지를 개별화한 후 추가 소프트웨어 응용프로그램 설치
- 소프트웨어 배포 도구(예: HP Client Automation Standard Edition, HP Client Automation Enterprise Edition(Radia 기술 기반))를 사용하여 사전 설치된 소프트웨어를 사용자 정의된 소프트웨어 이미지로 교체합니다.
- 디스크 복제 프로세스를 사용하여 내용을 한 하드 드라이브에서 다른 하드 드라이브로 복사

최상의 배치 방법은 IT 환경 및 프로세스에 따라 다릅니다.

ROM 기반 설치 및 ACPI 하드웨어는 시스템 소프트웨어 복구, 구성 관리 및 문제 해결, 전원 관리 등을 폭넓게 지원합니다.

HP Client Automation Agent

HP Client Automation Standard 및 Enterprise Editions 모두에서 사용하는 관리 에이전트는 컴퓨터에 사전 로드됩니다. 이 관리 에이전트를 설치하면 HP 관리 콘솔과 통신할 수 있습니다.

HP Client Automation Agent 를 설치하려면 다음과 같이 하십시오.

1. **시작**을 누릅니다.
2. **모든 프로그램**을 누릅니다.
3. **HP Manageability** 를 누릅니다.
4. 해당 **HP Management Agent Readme** 를 눌러 원하는 언어를 선택합니다.
5. Readme 파일에 포함된 지침을 검토하고 이에 따라 HP Client Automation Agent 를 설치합니다.

HP Client Automation Agent 는 모든 HP Client Automation 솔루션을 활성화하는 데 필요한 핵심 인프라 구성 요소입니다. HP 구성 관리 솔루션을 구현하는 데 필요한 다른 인프라 구성 요소에 대한 자세한 내용은 http://h20229.www2.hp.com/solutions/ascm/index.html 을 참조하십시오.

HP Client Manager

HPCM(HP Client Manager)은 지원되는 모든 HP 비즈니스 데스크탑, 노트북, 워크스테이션 및 HP Blade PC 에 사용할 수 있는 Symantec 에서 개발한 무료 솔루션입니다. HPCM 은 HP 특정 도구(예: System Software Manager, HP Instant Support Professional Edition, HP Client Management Interface)를 통합하여 지원되는 모든 HP 하드웨어를 한 곳에서 관리, 추적 및 모니터링할 수 있습니다.

HP Client Manager 7.0 은 관리자가 다음과 같은 관리 작업을 한꺼번에 수행할 수 있는 새로운 포털 페이지를 제공합니다.

- 인벤토리
- 경고
- BIOS 관리
- 드라이버 업데이트
- HP Instant Support Health Scan and Diagnostics 수행
- 내장 보안 작업 수행
- 최근 3-6 개월간의 전체 HP Health Alert Trend 확인
- HP Instant Support Health Scan and Diagnostics 로 지원되는 컴퓨터의 전체 준수 사항 확인
- HP 컴퓨터 요약 사항 확인 – 지원되는 여러 데스크탑, 노트북, 워크스테이션, HP Blade PC 등 분석
- 경고 확인: 자산, 임계값, 하드웨어 상태
- 보고서
- 특정 HP 도구를 업데이트하는 관리 작업

HPCM 은 http://www.symantec.com/business/theme.jsp 의 **Strategic Partner Products** 에서 **HP Client Manager** 를 눌러 다운로드할 수 있습니다. 영구 무료 라이센스도 다운로드 페이지에서 다운받을 수 있습니다.

HPCM "사용 방법" 비디오도 http://www.symantec.com/connect 에 게시되어 있습니다. HPCM 내의 다양한 작업에 대한 단계별 비디오를 보려면 **HP Client Manager 7.0** 을 검색하십시오.

3 원격 시스템 설치

Remote System Installation(원격 시스템 설치)을 통해 PXE(Preboot Execution Environment)를 초기화하여 네트워크 서버에 있는 소프트웨어 및 구성 정보를 사용하는 시스템을 시작하고 설치할 수 있습니다. 일반적으로 시스템 설치 및 구성 도구로 사용되는 Remote System Installation(원격 시스템 설치)은 다음 작업에 사용할 수 있습니다.

- 하드 드라이브 포맷
- 한 대 이상의 새 PC 에 소프트웨어 이미지 배치
- 플래시 ROM 의 시스템 BIOS 원격 업데이트(13페이지의 원격 ROM 플래시 참조)

주: Microsoft Windows 운영체제 내에 시스템 BIOS 플래시 기능이 있습니다.

- 시스템 BIOS 설정 구성

Remote System Installation(원격 시스템 설치)을 초기화하려는 경우 컴퓨터 부팅 시 HP 로고 화면의 오른쪽 하단에 **F12 = Network Service Boot**(F12 = 네트워크 서비스 부팅) 메시지가 나타나면 F12 키를 누릅니다. 화면의 지시에 따라 프로세스를 계속 진행합니다. 기본 부팅 순서는 항상 PXE 부팅을 시도하도록 변경할 수 있는 BIOS 구성 설정입니다.

4 소프트웨어 업데이트 및 관리

HP 는 데스크탑, 워크스테이션 및 노트북에서 소프트웨어를 관리하고 업데이트하는 데 사용할 수 있는 여러 가지 도구를 제공합니다.

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard 및 Enterprise Edition
- Symantec 의 HP Client Manager
- Altiris Client Management Suite
- Microsoft System Center 및 SMS 제품용 HP Client Catalog
- Active Management Technology 를 사용하는 Intel vPro 기반 PC
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

IT 부서에서 사용하는 시스템 관리 도구에 상관없이 하드웨어 및 소프트웨어 자산을 관리하는 일은 IT 비용을 낮추고 비즈니스에 발 빠르게 대응하는 데 중요한 역할을 합니다. IT 관리자는 간단한 스크립트를 작성하고 이를 직접 선택한 관리 솔루션에 통합하여 HP Client Management Interface 에 액세스할 수 있습니다.

HP CMI(HP Client Management Interface)를 사용하면 새 HP 비즈니스 컴퓨터를 관리되는 IT 환경에 원활하게 통합할 수 있습니다. HP CMI 는 업계에서 유명한 산업 시스템 관리 도구(예: Microsoft Systems Management Server, IBM Tivoli Software, HP Operations 등)와 HP 에서 개발한 사용자 정의 관리 응용프로그램을 사용하여 HP 비즈니스 컴퓨터의 통합을 단순화하는 인터페이스를 제공합니다. HP CMI 를 사용하는 경우 시스템 관리 도구 및 응용프로그램이 클라이언트 컴퓨터와 직접 통신하므로 에이전트 또는 연결단자 소프트웨어와 통합하지 않아도 되기 때문에 자세한 클라이언트 인벤토리를 요청하고 상태 정보를 수신하며 시스템 BIOS 설정을 관리할 수 있습니다.

HP Client Management Interface 는 MS WMI(Microsoft Windows Management Interface), WBEM (Web-Based Enterprise Management) SMBIOS(System Management BIOS) 및 ACPI(Advanced Configuration and Power Interface)와 같은 업계 표준을 기반으로 합니다. HP CMI 는 HP Client

Management Solutions 에서 활용하는 기본적인 기술입니다. HP 는 HP CMI 를 통해 유동적인 HP 클라이언트 컴퓨터 관리 방법을 제공합니다.

시스템 관리 소프트웨어와 함께 HP Client Management Interface 를 사용하여 다음을 수행할 수 있습니다.

- 자세한 클라이언트 인벤토리 정보 요청 – 센서 정보(예: 팬 속도, 전압 및 온도)를 포함하여 프로세서, 하드 드라이브, 메모리, BIOS, 드라이버에 대한 자세한 정보를 캡처합니다.
- 상태 정보 수신 – 시스템 관리 콘솔, 응용프로그램 또는 로컬 클라이언트 컴퓨터로 전송되는 다양한 범위의 클라이언트 하드웨어 경고(예: 과열, 팬 정지 및 하드웨어 구성 변경)를 등록합니다. 하드웨어 이벤트가 발생하면 경고가 실시간으로 전송됩니다.
- 시스템 BIOS 설정 관리 – 각 시스템으로 이동하지 않고도 임의의 또는 모든 클라이언트 시스템의 시스템 관리 콘솔에서 원격으로 BIOS 암호 및 컴퓨터 부팅 순서를 설정 및 변경하는 F10 기능을 수행합니다.

HP Client Management Interface 에 대한 자세한 내용은 http://www.hp.com/go/hpcmi/를 참조하십시오.

HP SoftPaq Download Manager

HP SoftPaq Download Manager 는 사용자 환경에서 HP 클라이언트 PC 모델에 맞는 소프트웨어 업데이트를 찾아 다운로드할 수 있는 편리한 무료 인터페이스입니다. 사용하는 모델, 운영체제 및 언어를 지정하여 필요한 Softpaq 을 빠르게 찾고 정렬하여 선택할 수 있습니다. HP SoftPaq Download Manager 를 다운로드하려면 http://www.hp.com/go/sdm 을 방문하십시오.

HP System Software Manager

HP SSM(System Software Manager)은 HP 비즈니스 PC 에 대한 장치 드라이버 및 BIOS 업데이트 원격 배포를 자동화하는 무료 유틸리티입니다. SSM 을 실행하면 사용자의 조작 없이 자동으로 각 네트워크 클라이언트 시스템에 설치된 드라이버와 BIOS 의 버전을 확인하고 해당 인벤토리를 테스트를 거쳐 중앙 파일 저장소에 저장된 시스템 소프트웨어 SoftPaq 과 비교합니다. 그런 다음 네트워크 PC 의 버전이 낮은 시스템 소프트웨어를 파일 저장소에 있는 최신 버전으로 업데이트합니다. SSM 은 올바른 클라이언트 시스템 모델에 대한 SoftPaq 배포만 허용하므로 관리자는 안심하고 SSM 을 사용하여 효율적으로 시스템 소프트웨어를 최신으로 유지할 수 있습니다.

System Software Manager 는 HP Client Automation 솔루션, Symantec 의 HP Client Manager 및 Microsoft SMS(Systems Management Server)와 같은 기업용 소프트웨어 배포 도구와 통합됩니다. SSM 을 사용하면 사용자가 만들었거나 타사에서 제공하는 업데이트를 SSM 형식으로 패키지화하여 배포할 수 있습니다.

SSM 은 http://www.hp.com/go/ssm 에서 무료로 다운로드할 수 있습니다.

주: SSM 은 Windows BitLocker 드라이브 암호화가 설정되고 TPM 측정을 사용하여 BitLocker 키를 보호하는 시스템에서 현재 원격 ROM 플래시를 지원하지 않습니다. BIOS 를 플래시하면 BitLocker 에서 플랫폼에 대해 생성한 신뢰할 수 있는 서명이 무효화되기 때문입니다. 시스템 BIOS 를 플래시하려면 그룹 정책을 통해 BitLocker 를 비활성화하십시오.

BitLocker 키를 무효화하지 않도록 BIOS 의 TPM 측정을 하지 않고 BitLocker 가 지원되도록 설정할 수 있습니다. 응급 복구를 대비하여 BitLocker 인증서의 백업을 안전하게 유지하는 것이 좋습니다.

HP ProtectTools Security Manager

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

HP ProtectTools Security Manager 는 다른 모든 모듈에서 액세스할 수 있는 단일 콘솔입니다.

- HP ProtectTools Credential Manager
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- HP ProtectTools File Sanitizer
- HP ProtectTools Java Card Security
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro for HP ProtectTools(HP ProtectTools LoJack)

HP ProtectTools 는 HP ProtectTools Security Manager 와 HP ProtectTools Administrative Console 이라는 사용할 수 있는 두 가지 버전을 제공합니다. 관리자 버전과 사용자 버전은 **시작 > 모든 프로그램** 메뉴에서 사용할 수 있습니다.

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

HP ProtectTools 소프트웨어 모듈은 사전 설치 또는 사전 로드되어 있거나 HP 웹 사이트에서 다운로드할 수 있습니다. 특정 HP Pro 데스크탑의 경우 HP ProtectTools 는 선택 사양 부품으로 제공됩니다. 자세한 내용은 http://www.hp.com/products/security 를 참조하십시오.

HP Client Automation Starter 및 Standard Editions

HP Client Automation 은 Windows Vista, Windows XP 및 HP 씬 클라이언트 환경에 적합한 하드웨어 및 소프트웨어 관리 솔루션으로 신속하게 배치하고 간편하게 사용할 수 있으며 향후 요구 사항에 대비할 수 있도록 합니다. 이 관리 솔루션은 두 가지 버전으로 제공됩니다.

- Starter Edition 은 하드웨어 및 소프트웨어 인벤토리, 원격 제어, HP 경고 모니터링, HP BIOS 및 드라이버 업데이트, HP Protect Tools 와의 통합, Intel AMT 에 대한 추가 지원을 제공하는 HP 데스크톱, 노트북 및 워크스테이션 관리용 제품이며 HP 씬 클라이언트의 배치 및 관리도 지원합니다. 이 버전은 무료입니다.
- Standard Edition 에는 Starter Edition 에서 제공하는 모든 기능이 포함되어 있으며 추가로 Windows 배치 및 마이그레이션, 패치 관리 기능, 소프트웨어 배포 및 소프트웨어 사용 측정 기능이 있습니다. 이 버전을 사용하려면 구입해야 합니다.

HP Client Automation Starter 및 Standard Edition 은 계속해서 변화하는 대규모, 이기종 IT 환경을 자동으로 관리할 수 있도록 HP Client Automation Enterprise Edition(Radia 기술 기반)으로의 마이그레이션 경로를 제공합니다.

HP Client Automation 솔루션에 대한 자세한 내용은 http://www.hp.com/go/client 를 참조하십시오.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition 은 관리자가 인벤토리, 배치, 패치 작업을 수행하고 이기종 클라이언트 플랫폼에 있는 소프트웨어와 컨텐츠를 지속적으로 관리할 수 있는 정책 기반 솔루션입니다. HP Client Automation Enterprise Edition 을 통해 IT 전문가는 다음 작업을 수행할 수 있습니다.

- 마이그레이션 및 은퇴 기간 동안 검색, 배치, 지속적인 관리 등의 전체 수명 주기 관리 절차를 자동화
- 전체 소프트웨어 스택(운영체제, 응용프로그램, 패치, 설정 및 컨텐츠)을 바람직한 상태로 자동 배치 및 지속적인 관리
- 이기종 또는 독립형 인프라 형태인 데스크톱, 워크스테이션 및 노트북 등 실질적인 모든 장치에서 소프트웨어를 관리
- 대부분의 운영체제에서 소프트웨어를 관리

HP 는 지속적인 구성 관리를 통해 고객에게 IT 비용 절감과 소프트웨어 및 컨텐츠 출시 기간 단축 혜택을 제공했으며 이에 따라 사용자의 생산성과 만족도가 향상되었습니다.

HP Client Automation 솔루션에 대한 자세한 내용은 http://www.hp.com/go/client 를 참조하십시오.

Symantec 의 HP Client Manager

Altiris 와 함께 개발한 Symantec 의 HP Client Manager 는 지원되는 모든 HP 비즈니스 데스크탑, 노트북 및 워크스테이션 모델에서 무료로 사용할 수 있습니다. SSM 은 HP Client Manager 에 통합되어 있으며 HP 클라이언트 시스템의 하드웨어적 측면을 중앙에서 추적, 감시 및 관리할 수 있도록 합니다.

Symantec 의 HP Client Manager 를 사용하여 다음과 같은 작업을 수행할 수 있습니다.

- CPU, 메모리, 비디오, 보안 설정 등의 주요 하드웨어 정보 확인
- 사전에 문제를 해결할 수 있도록 시스템 상태 감시
- 각 PC 로 이동하지 않고도 드라이버 및 BIOS 업데이트 자동 설치
- BIOS 및 보안 설정 원격 구성
- 빠른 하드웨어 문제 해결 프로세스 자동화

HP Instant Support 도구와의 완벽한 통합으로 하드웨어 문제 해결 시간 단축

- 진단 – HP 데스크탑, 노트북 및 워크스테이션 모델에서 원격으로 보고서 실행 및 보기
- 시스템 상태 검사 – 설치된 HP 클라이언트 시스템에 알려진 하드웨어 문제가 있는지 검사
- 액티브 채팅 – HP 고객 지원 센터에 연결하여 문제 해결
- HP 기술 자료 – 전문가 정보 연결
- 하드웨어 문제를 신속하게 해결하기 위한 자동화된 SoftPaq 수집 및 전달 프로세스
- HP ProtectTools 내장 보안 칩을 사용하여 시스템 식별, 목록화 및 초기화
- 클라이언트 시스템에서 로컬로 표시되는 상태 경고 옵션
- 타사 클라이언트의 기본적인 인벤토리 정보 보고
- TPM 보안 칩 설정 및 구성

- 중앙에서 클라이언트 백업 및 복구 예약
- Intel AMT 관리를 위한 지원 추가

Symantec 의 HP Client Manager 에 대한 자세한 내용은 http://www.hp.com/go/clientmanager 를 참조하십시오.

Altiris Client Management Suite

Altiris Client Management Suite 는 데스크탑, 노트북 및 워크스테이션의 전체 수명 주기 동안 소프트웨어를 관리할 수 있는 사용이 간편한 솔루션입니다. Client Management Suite 에는 다음과 같은 Altiris 제품이 들어 있습니다.

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution
- Application Management Solution
- Carbon Copy Solution

Altiris Client Management Suite 에 대한 자세한 내용은 http://www.symantec.com/business/client-management-suite 를 참조하십시오.

Microsoft System Center 및 SMS Products 용 HP Client Catalog

HP Client Catalog 를 사용하면 Microsoft 제품을 사용하는 IT 전문가들이 HP 비즈니스 PC 에 대한 HP 소프트웨어 업데이트(Softpaqs)의 배치를 자동화할 수 있습니다. 카탈로그 파일에는 HP 비즈니스 데스크탑, 노트북 및 워크스테이션에 대한 자세한 플랫폼 정보가 포함되어 있습니다. 사용자 정의 인벤토리 및 Microsoft 제품의 업데이트 기능과 함께 사용하여, 관리되는 HP 클라이언트 컴퓨터에 자동화된 드라이버 및 패치 업데이트를 제공할 수 있습니다.

HP Client Catalog 에서 지원하는 Microsoft 제품은 다음과 같습니다.

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server(SMS) 2003 R2

SMS 용 HP Client Catalog 에 대한 자세한 내용은 http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html 를 참조하십시오.

원격 관리 기술

모델에는 vPro 기술 또는 표준 기술이 포함되어 있습니다. 두 기술 모두 네트워크로 연결된 컴퓨팅 자산의 검색, 치료 및 보호 기능을 향상시키고 시스템이나 운영체제의 작동 상태 등 PC 를 관리할 수 있습니다.

비즈니스 데스크탑에서 사용할 수 있는 세 가지 형태의 원격 관리 기능은 ASF(Alert Standard Format), AMT(Intel Active Management Technology), DASH(Desktop and mobile Architecture for Systems Hardware)입니다.

원격 관리 기술에는 다음과 같은 기능이 있습니다.

- 네트워크 검색
- 하드웨어 인벤토리 정보
- 플랫폼 상태 모니터링
- 전원 관리 – 전원 켜기/끄기, 전원 주기
- 원격 진단 및 복구
  - 텍스트 콘솔 리디렉션 - 부팅 단계에서 원격 PC 의 콘솔 제어
  - 미디어 리디렉션 - 원격 부팅 드라이브, 디스크 또는 ISO 이미지(AMT 플랫폼의 IDE-R(IDE-리디렉션) 및 USB 미디어 리디렉션)에서 시스템 부팅
- 하드웨어 기반 분리 및 복구 – 바이러스와 유사한 활동을 발견한 경우 PC 네트워크 액세스를 제한 또는 차단
- 플랫폼 이벤트 추적 및 감사
- 원격 액세스 및 구성을 위해 통합된 웹 서버 관리 포털
- HP 의 관리 콘솔 파트너에 통합된 원격 관리 기술

주: 일부 플랫폼에서는 일부 기능을 사용할 수 없습니다.

Intel Management Engine 구성

주: Intel vPro 기술 개요는 http://www.intel.com/vpro 를 참조하십시오.

HP 와 관련된 Intel vPro 기술에 자세한 내용은 http://www.hp.com/support 에서 제공하는 백서를 참조하십시오. 해당 국가/지역 및 언어를 선택하고 **제품 지원 및 문제해결 정보 보기**를 선택한 다음 컴퓨터의 모델 번호를 입력하고 Enter 키를 누릅니다. **Resources**(리소스) 범주에서 **Manuals (guides, supplements, addendums, etc)**(사용 설명서(설명서, 보충 사항, 수정 사항 등))을 누릅니다. **Quick jump to manuals by category**(범주별로 설명서 바로 가기)에서 **White papers**(백서)를 누릅니다.

사용할 수 있는 관리 기술은 다음과 같습니다.

- AMT(DASH 1.0 포함)
- ASF
- DASH 1.1(Broadcom NIC 사용)

ASF 와 AMT 를 동시에 구성할 수는 없지만 ASF 와 AMT 모두 지원됩니다.

AMT 또는 ASF 에 적합한 Intel vPro 시스템을 구성하려면 다음을 수행하십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Microsoft Windows 의 경우, **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 단축키 Ctrl+P 를 누릅니다.

주: 적절한 시점에 Ctrl+P 를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 Ctrl+P 를 눌러야 유틸리티에 액세스할 수 있습니다.

이 단축키를 누르면 Intel Management Engine BIOS Execution(MEBx) 설정 유틸리티가 시작됩니다. 이 유틸리티에서는 관리 기술의 다양한 측면을 구성할 수 있습니다. 구성 옵션은 다음과 같습니다.

- 주 메뉴
  - Intel® ME Configuration(Intel® ME 구성)
  - Intel® AMT Configuration(Intel® AMT 구성)
  - Change Intel® ME Password(Intel® ME 암호 변경)
  - Exit
- Intel® ME Platform Configuration(Intel® ME 플랫폼 구성)
  - Intel® ME State Control(Intel® ME 상태 제어)(활성화/비활성화)
  - Intel® ME Firmware Local Update(Intel® ME 펌웨어 로컬 업데이트)(활성화/비활성화)
  - Intel® ME Features Control(Intel® ME 기능 제어)
  - Intel® ME Power Control(Intel® ME 전원 제어)
- Intel® AMT Configuration(Intel® AMT 구성)
  - 호스트 이름
  - TCP/IP
  - Provision Model(프로비전 모델)(Enterprise, SMB)
  - 설정 및 구성
  - Un-Provision
  - SOL/IDE-R(활성화/비활성화)
  - 암호 정책
  - Secure Firmware Update(보안 펌웨어 업데이트)(활성화/비활성화)
  - Set PRTC(PRTC 설정)
  - Idle Timeout(유휴 제한 시간)
- Change Intel® ME Password(Intel® ME 암호 변경)(이 암호를 변경하는 것이 좋습니다. 기본 암호는 **admin** 입니다.)

원격으로 AMT 시스템을 관리하려면 관리자가 AMT 를 지원하는 원격 콘솔을 사용해야 합니다. HP, Altiris, Microsoft SMS 와 같은 엔터프라이즈 관리 콘솔은 공급업체에서 구할 수 있습니다. SMB 모드에서 클라이언트는 웹 브라우저 인터페이스를 제공합니다. 이 기능에 액세스하려면 네트워크상의 다른 시스템에서 브라우저를 열고 http://host_name:16992 를 입력합니다. 여기서 host_name 은 시스템에 지정된 이름입니다. 호스트 이름 대신 IP 주소를 사용할 수도 있습니다.

Broadcom DASH 지원 NIC 로 시스템을 구성하려면 다음과 같이 하십시오.

http://www.hp.com 사이트의 **제품지원 & 문제해결**에서 최신 설명서를 확인한 후 해당 모델을 선택하고 **Manuals**(설명서)를 선택한 다음 DASH 또는 Broadcom NIC 관련 **White papers**(백서)를 선택합니다.

Verdiem Surveyor

Verdiem Surveyor 는 PC 에너지 비용을 관리하는 데 도움을 주는 소프트웨어 솔루션입니다. Surveyor 는 각 PC 에서 소비하는 에너지의 양을 측정하고 보고합니다. 또한 PC 전원 설정을 제어하여 관리자는 전체 네트워크에서 에너지 절약을 위한 전략을 쉽게 구현할 수 있습니다. Surveyor 에이전트가 포함된 HP SoftPaq 는 HP 지원 사이트에서 다운로드하여 지원되는 상업용 데스크탑 모델에 설치할 수 있습니다. PC 관리를 위한 Surveyor 라이센스는 HP 담당자를 통해 구입할 수 있습니다.

HP Proactive Change Notification

Proactive Change Notification 프로그램은 Subscriber's Choice 웹 사이트를 사용하여 다음 작업을 수행합니다.

- 최대 60 일 이전에 대부분의 상업용 컴퓨터와 서버의 하드웨어 및 소프트웨어 변경 사항을 알리는 PCN(Proactive Change Notification) 전자 우편을 사전에 자동으로 사용자에게 전송합니다.
- 대부분의 상업용 컴퓨터와 서버용 Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins 및 Dirver Alerts 를 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 작성 방법에 대한 자세한 내용은 http://h30046.www3.hp.com/subhub.php 를 참조하십시오.

Subscriber's Choice

Subscriber's Choice 는 HP 의 클라이언트 기반 서비스입니다.

HP 는 사용자의 프로파일에 따라 사용자에게 적합한 제품 정보, 기능 설명이나 드라이버 및 경보/알림 지원 기능을 제공합니다.

Subscriber's Choice 드라이버 및 지원 경고/알림 기능은 프로파일에 기입한 정보를 검토 및 검색할 수 있을 때 전자 우편으로 이를 알려 줍니다. Subscriber's Choice 및 사용자 정의 프로파일 작성 방법에 대한 자세한 내용은 http://h30046.www3.hp.com/subhub.php 를 참조하십시오.

단종된 솔루션

Altiris Local Recovery 및 Dantz Retrospect 소프트웨어 패키지는 HP 비즈니스 데스크탑, 노트북 또는 워크스테이션에 더 이상 제공되지 않습니다.

5 ROM 플래시

컴퓨터의 BIOS 는 프로그래밍 가능한 플래시 ROM(Read Only Memory)에 저장됩니다. Computer Setup(F10) 유틸리티에서 설정 암호를 설정하면 실수로 업데이트하거나 덮어쓰지 않도록 ROM 을 보호할 수 있습니다. 이는 컴퓨터의 운영 무결성을 위해 매우 중요합니다. BIOS 를 업그레이드해야 할 경우에는 HP 드라이버 및 지원 페이지(http://www.hp.com/support/files)에서 최신 BIOS 이미지를 다운로드할 수 있습니다.

△ **주의:** ROM 보안을 극대화하기 위해 설정 암호를 지정하십시오. 설정 암호는 무단 ROM 업그레이드를 방지합니다. System Software Manager 를 사용하면 시스템 관리자가 하나 이상의 PC 에서 동시에 설정 암호를 설정할 수 있습니다. 자세한 내용은 http://www.hp.com/go/ssm 을 참조하십시오.

원격 ROM 플래시

시스템 관리자는 원격 ROM 플래시를 통해 중앙 네트워크 관리 콘솔에서 직접 원격 HP 컴퓨터의 BIOS 를 안전하게 업그레이드할 수 있습니다. 시스템 관리자가 여러 컴퓨터에서 이 작업을 원격으로 수행할 수 있으므로 네트워크상의 HP PC BIOS 이미지를 일관성 있게 배치하고 제어할 수 있습니다. 또한 생산성을 향상하고 총 소유비용을 절감할 수 있게 되었습니다.

주: SSM 은 Windows BitLocker 드라이브 암호화가 설정되고 TPM 측정을 사용하여 BitLocker 키를 보호하는 시스템에서 현재 원격 ROM 플래시를 지원하지 않습니다. BIOS 를 플래시하면 BitLocker 에서 플랫폼에 대해 생성한 신뢰할 수 있는 서명이 무효화되기 때문입니다. 시스템 BIOS 를 플래시하려면 그룹 정책을 통해 BitLocker 를 비활성화하십시오.

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

원격 ROM 플래시에 대한 자세한 내용은 http://www.hp.com/go/ssm/에서 HP Client Manager Software 또는 System Software Manager 를 참조하십시오.

HPQFlash

HPQFlash 유틸리티는 Windows 운영체제에서 각 PC 의 시스템 BIOS 를 로컬에서 업데이트하거나 복원하는 데 사용됩니다.

HPQFlash 에 대한 자세한 내용은 http://www.hp.com/support/files 를 방문해 화면에 표시된 확인 메시지에 모델 번호를 입력하여 확인하실 수 있습니다.

6 Boot Block Emergency Recovery Mode (부팅 블록 응급 복구 모드)

흔하지는 않지만 ROM 플래시 오류가 발생할 경우 Boot Block Emergency Recovery Mode(부팅 블록 응급 복구 모드)를 통해 시스템을 복구할 수 있습니다. 예를 들어 BIOS 업그레이드 동안 정전이 발생한 경우 ROM 플래시가 불안정해질 수 있습니다. 이런 경우 시스템 BIOS 를 사용할 수 없게 됩니다. 부팅 블록은 시스템이 켜질 때 유효한 시스템 BIOS 이미지를 확인하는 코드를 포함하는 플래시 보호 ROM 섹션입니다.

- 시스템 BIOS 이미지가 유효하면 시스템이 정상적으로 시작합니다.
- 시스템 BIOS 이미지가 유효하지 않으면 failsafe Boot Block BIOS(failsafe 부팅 블록 BIOS)는 충분한 지원 기능을 제공하여 BIOS 이미지 파일에 대해 이동식 미디어를 검색합니다. 적절한 BIOS 이미지 파일을 찾은 경우 ROM 에 자동으로 플래시됩니다.

유효하지 않은 시스템 BIOS 이미지가 감지된 경우 시스템 전원 표시등이 빨간색으로 매초마다 한 번씩 8 번 깜박입니다. 동시에 스피커에서 8 번 경보음이 울립니다. 비디오 옵션 ROM 이미지를 포함하는 시스템 ROM 부분이 손상되지 않은 경우 **Boot Block Emergency Recovery Mode**(부팅 블록 응급 복구 모드)가 화면에 표시됩니다.

Boot Block Emergency Recovery Mode(부팅 블록 응급 복구 모드)로 들어간 후 시스템을 복구하려면 다음 단계를 모두 따르십시오.

1. 컴퓨터를 끕니다.
2. 루트 디렉토리에 원하는 BIOS 이미지가 들어 있는 CD 또는 USB 플래시 장치를 넣습니다.

   주: 이 미디어는 FAT12, FAT16 또는 FAT32 파일 시스템을 사용하여 포맷해야 합니다.

3. 컴퓨터의 전원을 켭니다.

   적절한 BIOS 이미지를 찾을 수 없는 경우 BIOS 이미지 파일이 들어 있는 미디어를 넣으라는 메시지가 나타납니다.

   시스템이 성공적으로 ROM 을 다시 프로그래밍한 경우 자동으로 컴퓨터가 꺼집니다.

4. BIOS 를 업그레이드하는 데 사용된 이동식 미디어를 꺼냅니다.
5. 전원을 켜고 컴퓨터를 다시 시작합니다.

주: BIOS 이미지 파일이 들어 있는 CD 가 광 드라이브에 있을 때 BitLocker 는 Windows Vista 가 부팅되지 않게 해줍니다. BitLocker 가 활성화되어 있으면 Windows Vista 로 부팅하기 전에 이 CD 를 제거하십시오.

7 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.

주: 두 절차 모두 디스켓 드라이브 또는 지원되는 USB 플래시 드라이브가 필요합니다.

주: SSM(System Software Manager)은 Windows 운영체제 내의 컴퓨터 설정 정보를 복제하는 데 사용할 수 있습니다. 자세한 내용은 http://www.hp.com/go/ssm 의 SSM 사용 설명서를 참조하십시오.

단일 컴퓨터에 복사

△ 주의: 설치 구성은 모델에 따라 다릅니다. 소스 컴퓨터와 대상 컴퓨터가 같은 모델이 아닌 경우 파일 시스템 오류가 발생할 수 있습니다. 예를 들어 설정 구성을 dc7xxx PC 에서 dx7xxx PC 로 복사하지 마십시오.

1. 복사할 설치 구성을 선택합니다. 컴퓨터를 끕니다. Windows 의 경우 **시작 > 시스템 종료 > 컴퓨터 끄기**를 누릅니다.
2. USB 플래시 미디어 장치를 사용하는 경우에는 지금 넣습니다.
3. 컴퓨터의 전원을 켭니다.
4. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

   주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

5. 디스켓을 사용하는 경우에는 지금 넣습니다.
6. **File**(파일) > **Replicated Setup**(복제된 설정) > **Save to Removable Media**(이동식 미디어에 저장)를 누릅니다. 화면 지침에 따라 구성 디스켓 또는 USB 플래시 미디어 장치를 만듭니다.
7. 구성할 컴퓨터를 끄고 구성 디스켓 또는 USB 플래시 미디어 장치를 삽입합니다.
8. 구성할 컴퓨터를 켭니다.
9. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.
10. **File**(파일) > **Replicated Setup**(복제된 설정) > **Restore from Removable Media**(이동식 미디어에서 복원)를 누르고 화면에 나타나는 지침을 따릅니다.
11. 구성이 완료되면 컴퓨터를 다시 시작합니다.

여러 컴퓨터에 복사

△ **주의:** 설치 구성은 모델에 따라 다릅니다. 소스 컴퓨터와 대상 컴퓨터가 같은 모델이 아닌 경우 파일 시스템 오류가 발생할 수 있습니다. 예를 들어 설정 구성을 dc7xxx PC 에서 dx7xxx PC 로 복사하지 마십시오.

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

주: 이 과정이나 부팅용 USB 플래시 미디어 장치를 만들 때 부팅 디스켓이 필요합니다. Windows XP 에서 부팅 디스켓 만들기를 사용할 수 없는 경우 대신 단일 컴퓨터에 복사하는 방법을 사용하십시오 (15페이지의 단일 컴퓨터에 복사 참조).

1. 부팅 디스켓 또는 USB 플래시 미디어 장치를 만듭니다. 17페이지의 지원되는 USB 플래시 미디어 장치 또는 18페이지의 지원되지 않는 USB 플래시 미디어 장치를 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 끕니다. Windows 의 경우 **시작 > 시스템 종료 > 컴퓨터 끄기**를 누릅니다.
3. USB 플래시 미디어 장치를 사용하는 경우 지금 넣으십시오.
4. 컴퓨터의 전원을 켭니다.
5. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

   주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

6. 디스켓을 사용하는 경우 지금 넣으십시오.
7. **File**(파일) > **Replicated Setup**(복제된 설정) > **Save to Removable Media**(이동식 미디어에 저장)를 누릅니다. 화면 지침에 따라 구성 디스켓 또는 USB 플래시 미디어 장치를 만듭니다.
8. 설정 복제용 BIOS 유틸리티(repset.exe)를 다운로드하고 구성 디스켓 또는 USB 플래시 미디어 장치에 복사합니다. 이 유틸리티를 받으려면 http://welcome.hp.com/country/us/en/support.html 에서 컴퓨터 모델 번호를 입력하십시오.
9. 구성 디스켓 또는 USB 플래시 미디어 장치에서 다음 명령어가 포함된 autoexec.bat 파일을 만듭니다.

   repset.exe

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

부팅 장치 만들기

지원되는 USB 플래시 미디어 장치

지원되는 장치에는 부팅 과정을 간소화하기 위해 사전 설치된 이미지가 있습니다. 모든 HP 또는 Compaq 및 대부분의 다른 USB 플래시 미디어 장치에는 이러한 사전 설치된 이미지가 있습니다. 사용 중인 USB 플래시 미디어 장치에 사전 설치된 이미지가 없는 경우 이 단원 뒷부분에 있는 절차를 수행하십시오(18페이지의 지원되지 않는 USB 플래시 미디어 장치 참조).

부팅 USB 플래시 미디어 장치를 만들려면 다음이 필요합니다.

- 지원되는 USB 플래시 미디어 장치
- FDISK 및 SYS 프로그램이 있는 부팅용 DOS 디스켓. SYS 를 사용할 수 없는 경우 FORMAT 을 사용해도 되지만 USB 플래시 미디어 장치의 기존 파일을 모두 잃게 됩니다.
- USB 플래시 미디어 장치에서 부팅할 수 있는 PC

△ **주의:** 일부 구형 PC 는 USB 플래시 미디어 장치에서 부팅할 수 없습니다. 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.

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

   USB 플래시 미디어 장치 드라이브: _____

   △ **주의:** 드라이브가 USB 플래시 미디어 장치와 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 4 를 수행합니다. 추가 저장 장치가 없으면 시스템에서 USB 플래시 미디어 장치를 지원하지 않거나 USB 플래시 미디어 장치에 결함이 있는 경우입니다. USB 플래시 미디어 장치를 부팅용으로 만들려고 시도하지 마십시오.
6. Esc 키를 눌러 FDISK 를 종료하고 **A:** 프롬프트로 돌아갑니다.
7. 부팅용 DOS 디스켓에 SYS.COM 이 있는 경우 단계 8 로 이동하고, 없는 경우 단계 9 로 이동합니다.
8. **A:** 프롬프트에 SYS x:를 입력합니다. x 는 위에서 메모한 드라이브 문자입니다.

   △ **주의:** USB 플래시 미디어 장치에 대해 올바른 드라이브 문자를 입력했는지 확인하십시오.

   시스템 파일이 전송된 후에 SYS 가 **A:** 프롬프트로 돌아갑니다. 단계 13 으로 이동합니다.
9. 보관할 파일을 USB 플래시 미디어 장치에서 다른 드라이브(예: 시스템의 내장 하드 드라이브)의 임시 디렉토리로 복사합니다.

10. **A:** 프롬프트에 FORMAT /S X:를 입력합니다. 여기서 X 는 이전에 메모한 드라이브 문자입니다.

△ **주의:** USB 플래시 미디어 장치에 대해 올바른 드라이브 문자를 입력했는지 확인하십시오.

FORMAT 을 입력하면 각 단계마다 계속 진행할지 여부를 묻는 메시지가 나타납니다. 메시지가 나타날 때마다 Y 를 입력합니다. FORMAT 을 실행하면 USB 플래시 미디어 장치를 포맷하고 시스템 파일을 추가하며 볼륨 레이블을 묻습니다.

11. 레이블이 없는 경우 Enter 키를 누르거나 필요한 경우 레이블을 입력합니다.

12. 단계 9 에서 저장한 파일을 USB 플래시 미디어 장치에 다시 복사합니다.

13. 디스켓을 꺼내고 컴퓨터를 재부팅합니다. 컴퓨터가 C 드라이브 등 USB 플래시 미디어 장치에서 부팅됩니다.

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

Windows 9x 에서 DOS 버전을 사용한 경우 Windows 로고 화면이 잠시 나타납니다. 이 화면을 나타나지 않게 하려면 USB 플래시 미디어 장치의 루트 디렉토리에 LOGO.SYS 라는 빈 파일을 추가합니다.

16페이지의 여러 컴퓨터에 복사로 돌아갑니다.

지원되지 않는 USB 플래시 미디어 장치

부팅 USB 플래시 미디어 장치를 만들려면 다음이 필요합니다.

- USB 플래시 미디어 장치
- FDISK 및 SYS 프로그램이 있는 부팅용 DOS 디스켓. SYS 를 사용할 수 없는 경우 FORMAT 을 사용해도 되지만 USB 플래시 미디어 장치의 기존 파일을 모두 잃게 됩니다.
- USB 플래시 미디어 장치에서 부팅할 수 있는 PC

△ **주의:** 일부 구형 PC 는 USB 플래시 미디어 장치에서 부팅할 수 없습니다. 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.

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.

5. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

6. **Advanced**(고급) > **PCI Devices**(PCI 장치)로 이동하여 PATA 및 SATA 컨트롤러를 비활성화합니다. SATA 컨트롤러가 비활성화되면 컨트롤러가 할당된 IRQ 를 메모합니다. 나중에 IRQ 를 다시 할당해야 합니다. 변경 사항을 확인하고 Setup 유틸리티를 종료합니다.

   SATA IRQ: _____

7. FDISK.COM 및 SYS.COM 또는 FORMAT.COM 이 있는 부팅 DOS 디스켓을 디스켓 드라이브에 삽입하고 컴퓨터를 켜서 DOS 디스켓으로 부팅합니다.

8. FDISK 를 실행하고 USB 플래시 미디어 장치에 기존 파티션이 있으면 삭제합니다. 새 파티션을 생성하고 활성화합니다. Esc 키를 눌러 FDISK 를 종료합니다.

9. FDISK 를 종료할 때 시스템이 자동으로 다시 시작되지 않는 경우, Ctrl+Alt+Del 를 눌러 DOS 디스켓에서 재부팅합니다.

10. **A:** 프롬프트에 FORMAT C: /S 를 입력하고 Enter 키를 누릅니다. FORMAT 을 실행하면 USB 플래시 미디어 장치를 포맷하고 시스템 파일을 추가하고 볼륨 레이블을 묻습니다.

11. 레이블이 없는 경우 Enter 키를 누르거나 필요한 경우 레이블을 입력합니다.

12. 컴퓨터의 전원을 끈 후 전원 코드를 뽑습니다. 컴퓨터를 열고 이전에 제거한 PCI 카드를 다시 설치합니다. 컴퓨터 덮개를 닫습니다.

13. 전원 코드를 연결하고 디스켓을 꺼낸 다음 컴퓨터를 켭니다.

14. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

15. **Advanced** > **PCI Devices** 로 이동하여 6 단계에서 비활성화한 PATA 및 SATA 컨트롤러를 다시 활성화한 다음 SATA 컨트롤러를 원래 IRQ 에 놓습니다.

16. 변경 사항을 저장하고 종료합니다. 컴퓨터가 C 드라이브 등 USB 플래시 미디어 장치에서 부팅됩니다.

주: 기본 부팅 순서는 컴퓨터마다 다르며 Computer Setup(F10) 유틸리티에서 변경할 수 있습니다. 자세한 내용은 *Computer Setup(F10) 유틸리티*를 참조하십시오.

Windows 9x 에서 DOS 버전을 사용한 경우 Windows 로고 화면이 잠시 나타납니다. 이 화면을 나타나지 않게 하려면 USB 플래시 미디어 장치의 루트 디렉토리에 LOGO.SYS 라는 빈 파일을 추가합니다.

16페이지의 여러 컴퓨터에 복사로 돌아갑니다.

8 이중 상태 전원 버튼

ACPI(Advanced Configuration and Power Interface)가 활성화된 경우 전원 버튼을 on/off 스위치나 대기 버튼으로 사용할 수 있습니다. 대기 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. **시작** 버튼을 마우스 왼쪽 버튼으로 누른 다음 **제어판 > 전원 옵션**을 선택합니다.
2. **전원 옵션 등록 정보**에서 **고급** 탭을 선택합니다.
3. **전원 버튼** 섹션에서 **대기 모드**를 선택합니다.

전원 버튼을 대기 버튼처럼 작동하도록 구성한 후 전원 버튼을 눌러 시스템을 저전력 상태(대기 상태)로 설정합니다. 전원 버튼을 다시 누르면 시스템이 대기 상태에서 완전 전력 상태로 바로 변경됩니다. 시스템의 모든 전원을 완전히 끄려면 4 초 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.

9 HP 웹 사이트 지원

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

새 운영체제나 증보판 운영체제로 전환할 경우 해당 운영체제용으로 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.

HP 는 최신 지원 소프트웨어를 간편하게 검색, 액세스, 평가 및 설치할 수 있는 지원 웹 사이트를 구축했습니다. http://www.hp.com/support 에서 소프트웨어를 다운로드할 수 있습니다.

웹 사이트에서는 HP 컴퓨터에서 최신 Microsoft Windows 운영체제를 실행하는 데 필요한 최신 장치 드라이버, 유틸리티 및 플래시 가능한 ROM 이미지를 제공합니다.

10 업계 표준

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

- WBEM(웹 기반 전사적 관리)
- WMI(Windows 관리 인터페이스)
- WOL(Wake on LAN) 기술
- ACPI
- SMBIOS
- PXE(Pre-boot Execution) 지원

11 자산 추적 및 보안

컴퓨터에 통합된 자산 추적 기능은 HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration 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.

HP 는 중요한 부품 및 정보에 대한 액세스를 제어하는 솔루션을 제공합니다. HP Embedded Security for ProtectTools 가 설치되어 있는 경우 데이터에 대한 무단 액세스를 방지하며 시스템 무결성을 검사하고 시스템에 액세스하려는 다른 사용자를 인증합니다. 자세한 내용은 http://www.hp.com/products/security 에서 *HP ProtectTools Security Manager 설명서*를 참조하십시오. 일부 모델에서 사용할 수 있는 HP Embedded Security for ProtectTools, Smart Cover Sensor, Smart Cover Lock 과 같은 보안 기능은 개인용 컴퓨터의 내부 구성 요소에 대한 무단 액세스를 차단합니다. 병렬, 직렬 또는 USB 포트를 비활성화하거나 이동식 미디어 부팅 기능을 비활성화하여 중요한 데이터 자산을 보호할 수 있습니다. Memory Change 및 Smart Cover Sensor 경고는 시스템 관리 응용프로그램에 자동으로 전달되어 컴퓨터의 내부 부품과 관련된 사전 알림 기능을 제공합니다.

주: HP ProtectTools 용 내장 보안, Smart Cover Sensor 및 Smart Cover Lock 은 일부 시스템의 선택 사양으로 사용할 수 있습니다.

다음 유틸리티를 사용하여 HP 컴퓨터의 보안 설정을 관리합니다.

- 로컬에서 Computer Setup(F10) 유틸리티 사용. Computer Setup 유틸리티 사용에 대한 추가 정보와 지침은 컴퓨터에 포함된 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.
- 원격으로 Symantec 의 HP Client Manager 소프트웨어, HP Client Automation 또는 System Software Manager 사용. 이 소프트웨어를 사용하여 보안 설정을 안전하고 일관성 있게 배치 및 제어할 수 있습니다.

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

표 11–1 보안 기능 개요

옵션	설명
Setup Password(암호 설정)	설정(관리자) 암호를 설정 및 활성화할 수 있습니다. **주:** 설정 암호를 설정한 경우 Windows 환경에서 Computer Setup 옵션을 변경하고, ROM 을 플래시하고, 변경 사항을 특정 플러그 앤 플레이 설정에 적용해야 합니다.
Power-On Password(파워온 암호 설정)	파워온 암호를 설정 및 활성화할 수 있습니다. 전원 주기 후 파워온 암호 프롬프트가 표시됩니다. 올바른 파워온 암호를 입력하지 않으면 장치가 부팅되지 않습니다. **주:** 아래 **Password Options**(암호 옵션)에서 활성화되지 않는 경우 Ctrl + Alt + Delete 또는 **Restart from Windows**(Windows 에서 다시 시작)와 같은 웜 부팅 시 암호가 나타나지 않습니다.

표 11-1 보안 기능 개요 (계속)

Password Options(암호 옵션) (이 선택 사항은 파워온 암호 또는 설정 암호가 설정되어 있는 경우에만 나타납니다.)	다음을 수행할 수 있습니다. • 레거시 리소스를 잠글 수 있습니다(설정 암호가 설정되어 있는 경우에 나타남). • 네트워크 서버 모드를 활성화/비활성화할 수 있습니다(파워온 암호가 설정되어 있는 경우에 나타남). • Ctrl+Alt+Delete 를 눌러 웜 부팅하는 경우 암호가 필요한지를 지정합니다(파워온 암호가 설정되어 있는 경우에 나타남). • 브라우저 모드 설정을 활성화/비활성화합니다(설정 암호가 설정되어 있는 경우에 나타남). 설정 암호를 입력하지 않으면 F10 설정 옵션을 변경할 수는 없지만 볼 수는 있습니다. • Stringent Password(강력한 암호)(파워온 암호가 설정되어 있는 경우에 나타남)를 활성화/비활성화할 수 있습니다. 활성화한 경우 내장 암호 점퍼를 생략하여 파워온 암호를 비활성화합니다. 자세한 내용은 *데스크탑 관리 설명서*를 참조하십시오.
Smart Cover(스마트 커버)(일부 모델)	다음을 수행할 수 있습니다. • Cover Lock(커버 잠금)을 잠금/잠금 해제할 수 있습니다. • 덮개 제거 센서를 사용하여 Disable/Notify User/Setup Password(비활성화/사용자 알림/암호 설정) 옵션을 설정할 수 있습니다. 주: *Notify User*(사용자 알림) 기능은 덮개가 제거된 것을 센서가 감지하여 사용자에게 알려 줍니다. 덮개가 제거된 것을 센서가 감지한 경우 컴퓨터를 부팅하려면 *Setup Password*(암호 설정)에 설정 암호를 입력해야 합니다. 이 기능은 일부 모델에서만 지원됩니다.
Device security(장치 보안)	다음 장치를 Device Available/Device Hidden(장치 사용/장치 숨김)으로 설정할 수 있습니다. • 직렬 포트 • 병렬 포트 • 뒷면 USB 포트 • 앞면 USB 포트 • 내부 USB 포트 • 시스템 오디오 • 네트워크 컨트롤러(일부 모델) • 레거시 디스켓 • 내장 보안 장치(일부 모델) • SATA0 • SATA1(일부 모델) • SATA2(일부 모델) • SATA3(일부 모델) • eSATA(일부 모델)
LoJack for HP ProtectTools(HP ProtectTools LoJack)	컴퓨터를 원격으로 모니터링, 관리 및 추적할 수 있습니다. 활성화된 LoJack Pro for HP ProtectTools(HP ProtectTools LoJack)는 Absolute Software 고객 센터에서 구성됩니다. 고객 센터에서 관리자는 LoJack Pro for HP ProtectTools(HP ProtectTools LoJack)를 구성하여 컴퓨터를 모니터링하거나 관리할 수 있습니다. 시스템이 잘못 배치되거나 도

표 11–1 보안 기능 개요 (계속)

	난 당한 경우 고객 센터에서는 지역 기관에 도움을 요청하여 컴퓨터를 찾아 복구할 수 있습니다. 구성이 완료되면 LoJack Pro 는 하드 드라이브가 지워지거나 교체되어도 계속 작동할 수 있습니다.
Network Service Boot (네트워크 서비스 부팅)	네트워크 서버에 설치된 운영체제에서 부팅하려면 컴퓨터의 기능을 활성화/비활성화합니다. NIC 모델에서만 사용할 수 있는 기능이므로 네트워트 컨트롤러는 PCI 확장 카드이거나 시스템 보드에 내장되어 있어야 합니다.
System ID(시스템 ID)	다음을 설정할 수 있습니다. • 자산 태그(18 바이트 ID), 즉 회사에서 이 컴퓨터에 할당한 자산 ID 번호 • 소유권 태그(POST 중 표시되는 80 바이트 ID) • 섀시 일련 번호 또는 UUID(Universal Unique Identifier) 번호 현재 섀시 일련 번호가 무효인 경우에만 UUID 를 갱신할 수 있음. 대체로 이러한 ID 번호는 출하 시 설정되며 시스템을 식별하는 고유 번호로 사용됩니다. • 시스템 ID 입력을 위한 키보드 로케일 설정(예: 한국어 또는 영어).
DriveLock Security (DriveLock 보안)	하드 드라이브의 마스터 암호 또는 사용자 암호를 지정하거나 수정할 수 있습니다. 이 기능을 활성화하면 POST 중에 드라이브 잠금 암호 중 하나를 입력하라는 메시지가 나타납니다. 두 암호가 모두 올바르게 입력되지 않은 경우 다음 번 콜드 부팅 시 두 암호 중 하나를 제대로 입력할 때까지 하드 드라이브에 액세스할 수 없습니다. **주:** 이 선택 사항은 DriveLock 기능을 지원하는 드라이브가 적어도 하나 이상 시스템에 연결되어 있는 경우에만 나타납니다.
Setup Security Level (보안 수준 설정)	설정 암호를 몰라도 일반 사용자가 지정된 설정 암호를 변경할 수 있도록 제한된 액세스를 허용하는 방법을 제공합니다. 이 기능을 사용하면 사용자가 시스템 설정을 확인하고 부차적인 옵션을 구성하는 동안 관리자의 핵심 설정 옵션 변경을 방지하는 유연성을 제공합니다. 관리자는 Setup Security Level(보안 수준 설정) 메뉴를 통해 상황에 따라 개별 설정 옵션에 대한 액세스 권한을 지정할 수 있습니다. 기본적으로 모든 설정 옵션에 설정 암호가 지정됩니다. 즉, 사용자가 옵션을 변경하려면 POST 동안 올바른 설정 암호를 입력해야 합니다. 관리자는 개별 항목을 None(없음)으로 설정할 수 있습니다. 즉, 잘못된 암호를 입력하여 설정에 액세스한 경우에도 사용자가 지정된 옵션을 변경할 수 있습니다. Power-On Password(파워온 암호)가 활성화된 경우 None(없음) 옵션이 Power-On Password(파워온 암호)로 바뀝니다. **주:** 설정 암호를 모르는 경우 설정을 입력하려면 Setup Browse Mode(설정 검색 모드)를 활성화해야 합니다.
System Security(시스템 보안)(일부 모델: 이 옵션은 하드웨어에 따라 다름)	Data Execution Prevention(데이터 실행 방지)(일부 모델)(활성화/비활성화) - 운영체제 보안 침해를 방지할 수 있습니다. Virtualization Technology(가상화 기술)(일부 모델)(활성화/비활성화) - 프로세서의 가상화 기능을 제어합니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다. Virtualization Technology Directed I/O(가상화 기술을 통한 I/O)(일부 모델)(활성화/비활성화) - 칩셋의 DMA 재맵핑 기능을 제어합니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다. Trusted Execution Technology(신뢰할 수 있는 실행 기술)(일부 모델)(활성화/비활성화) - 가상 장치를 지원하는 데 필요한 기본 프로세서 및 칩셋 기능을 제어합니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다. 이 기능을 활성화하려면 다음 기능이 활성화되어 있어야 합니다. • Embedded Security Device Support(내장 보안 장치 지원) • Virtualization Technology(가상화 기술) • Virtualization Technology Directed I/O(가상화 기술을 통한 I/O) Embedded Security Device Support(내장 보안 장치 지원)(일부 모델)(활성화/비활성화) - Embedded Security Device 를 활성화/비활성화합니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다.

표 11-1 보안 기능 개요 (계속)

	주: Embedded Security Device(내장 보안 장치)를 구성하려면 Setup Password(암호 설정)를 설정해야 합니다. • Reset to Factory Settings(일부 모델)(재설정하지 않음/재설정) - 기본 설정으로 복원하면 보안 키가 모두 삭제됩니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다. **주의:** Embedded Security Device(내장 보안 장치)는 대부분의 보안 체계에서 중요한 장치입니다. 보안 키를 지우면 Embedded Security Device(내장 보안 장치)로 보호되는 데이터에 액세스할 수 없습니다. Reset to Factory Settings 를 선택하면 심각한 데이터 손실이 발생할 수 있습니다. • Reset authentication credentials(출하 시 설정으로 재설정)(일부 모델)(재설정하지 않음/재설정) - Reset 을 선택하면 Power-on authentication support(파워온 인증 지원)가 비활성화되고 Embedded Security Device(내장 보안 장치)의 인증 정보가 삭제됩니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다. OS management of Embedded Security Device(OS 관리 내장 보안 장치)(일부 모델)(활성화/비활성화) - 이 옵션을 사용하여 사용자는 Embedded Security Device 운영체제 제어를 제한할 수 있습니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다. 이 옵션을 활성화하면 사용자는 Embedded Security Device OS(내장 보안 장치 OS) 제어를 제한할 수 있습니다. • Reset of Embedded Security Device through OS(OS 를 통해 내장 보안 장치 재설정)(일부 모델)(활성화/비활성화) - 이 옵션을 사용하면 사용자는 Embedded Security Device(내장 보안 장치)의 Reset to Factory Settings(출하 시 설정 재설정)를 요청하는 운영체제 기능을 제한할 수 있습니다. 이 설정을 변경하려면 컴퓨터를 껐다가 다시 켜야 합니다. **주:** 이 옵션을 활성화하려면 Setup Password(암호 설정)를 설정해야 합니다. PAVP(일부 모델)(비활성화됨/최소/최대) – PAVP 는 칩셋에서 Protected Audio Video Path(보호되는 오디오 비디오 경로)를 활성화할 수 있습니다. PAVP 는 재생 시 볼 수 없는 보호되는 일부 고화질 컨텐츠를 볼 수 있습니다. Max(최대)를 선택하면 PAVP 에만 96MB 의 시스템 메모리를 할당합니다.

암호 보안

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

시스템 관리자가 설정되어 있는 파워온 암호를 몰라도 모든 네트워크 시스템에 로그인하여 유지 관리할 수 있도록 네트워크 전체에 걸친 설정 암호를 설정할 수 있습니다.

주: SSM(System Software Manager)은 Windows 운영체제 내의 BIOS 암호를 만들고 관리하는 데 사용할 수 있습니다. 자세한 내용은 http://www.hp.com/go/ssm 의 SSM 사용 설명서를 참조하십시오.

주: HP CMI(HP Client Management Interface)는 Windows 운영체제 내의 BIOS 암호를 비롯하여 BIOS 설정 관리에 대한 액세스를 제공합니다. 자세한 내용은 http://www.hp.com/go/hpcmi 의 HP Client Management Interface 기술 백서를 참조하십시오.

Computer Setup 을 사용하여 설정 암호 설정

시스템에 내장 보안 장치가 장착되어 있는 경우 http://www.hp.com 의 *HP ProtectTools Security Manager 설명서*를 참조하십시오. Computer Setup 을 통해 설정 암호를 설정하면 암호를 입력하기 전에는 컴퓨터가 다시 구성되지 않도록 합니다(Computer Setup(F10) 유틸리티 사용).

1. 컴퓨터를 켜거나 다시 시작합니다. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

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

Computer Setup 을 사용하여 파워온 암호 설정

Computer Setup 을 통해 파워온 암호를 설정하면 전원이 켜졌을 때 암호를 입력하지 않으면 컴퓨터에 액세스할 수 없습니다. 파워온 암호가 설정되면 Computer Setup 에서 **Security** 메뉴 아래에 **Password Options**(암호 옵션)를 표시합니다. 암호 옵션은 **Password Prompt on Warm Boot**(웜 부팅에서 암호 프롬프트)를 포함합니다. **Password Prompt on Warm Boot**(웜 부팅에서 암호 프롬프트)가 활성화되면 컴퓨터를 다시 부팅할 때마다 암호를 입력해야 합니다.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

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

파워온 암호 입력

파워온 암호를 입력하려면 다음 단계를 완료하십시오.

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

주: 입력한 문자는 보안상의 이유로 화면에 나타나지 않으므로 주의하여 입력하십시오.

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

설정 암호 입력

시스템에 내장 보안 장치가 장착되어 있는 경우 http://www.hp.com 의 *HP ProtectTools Security Manager 설명서*를 참조하십시오.

컴퓨터에 설정 암호가 설정되어 있으면 Computer Setup 을 실행할 때마다 암호를 입력하라는 메시지가 표시됩니다.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

3. 키 아이콘이 모니터에 나타나면 설정 암호를 입력한 후 Enter 키를 누릅니다.

주: 입력한 문자는 보안상의 이유로 화면에 나타나지 않으므로 주의하여 입력하십시오.

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

파워온 또는 설정 암호 변경

시스템에 내장 보안 장치가 장착되어 있는 경우 http://www.hp.com 의 *HP ProtectTools Security Manager 설명서*를 참조하십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 파워온 암호를 변경하려면 단계 3 으로 이동하십시오.

   설정 암호를 변경하려면 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

3. 키 아이콘이 나타나면 다음과 같이 이전 암호, 슬래시(/)나 대체 구분 문자, 새 암호, 슬래시(/)나 대체 구분 문자 및 새 암호를 다시 입력합니다. 이전 암호/새 암호/새 암호

주: 입력한 문자는 보안상의 이유로 화면에 나타나지 않으므로 주의하여 입력하십시오.

4. Enter 키를 누릅니다.

새 암호는 다음에 컴퓨터를 켤 때 적용됩니다.

주: 대체 구분 문자에 대한 자세한 내용은 29페이지의 국가/지역별 키보드 구분 문자를 참조하십시오. 파워온 암호와 설정 암호는 Computer Setup 의 Security 옵션을 사용하여 변경할 수도 있습니다.

파워온 또는 설정 암호 삭제

시스템에 내장 보안 장치가 장착되어 있는 경우 http://www.hp.com 의 *HP ProtectTools Security Manager 설명서*를 참조하십시오.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 파워온 암호를 삭제하려면 단계 3 으로 이동합니다.

   설정 암호를 삭제하려면 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

   주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

3. 키 아이콘이 나타나면 다음과 같이 이전 암호 다음에 슬래시(/)나 대체 구분 문자를 입력하십시오. 이전 암호/
4. Enter 키를 누릅니다.

   주: 대체 구분 문자에 대한 자세한 내용은 29페이지의 국가/지역별 키보드 구분 문자를 참조하십시오. 파워온 암호와 설정 암호는 Computer Setup 의 Security 옵션을 사용하여 변경할 수도 있습니다.

국가/지역별 키보드 구분 문자

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

국가별 키보드 구분 문자

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

* 보스니아 헤르체고비나, 크로아티아, 몬테네그로, 세르비아 및 슬로베니아

암호 지우기

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

시스템에 내장 보안 장치가 장착되어 있는 경우 http://www.hp.com 의 *HP ProtectTools Security Manager 설명서*를 참조하십시오.

DriveLock

DriveLock 은 ATA 하드의 데이터에 대한 무단 액세스를 차단하는 업계 표준 보안 기능입니다. DriveLock 은 Computer Setup 의 확장으로 구현되었습니다. 이 기능은 ATA 보안 명령 모음을 지원하는 하드 드라이브가 감지될 때만 사용할 수 있습니다. DriveLock 은 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 DriveLock 은 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 드라이브 잠금을 해제하는 데 사용할 수 있는 "백도어"가 없습니다. 따라서 DriveLock 은 하드 드라이브에 저장된 데이터를 회사 정보 시스템에 복제하거나 정기적으로 백업할 때 가장 안전하게 사용됩니다. 두 개의 DriveLock 암호를 모두 잊어버린 경우 하드 드라이브를 사용할 수 없습니다. 이전에 정의한 고객 프로파일과 일치하지 않는 사용자의 경우 심각한 위험을 초래할 수 있습니다. 고객 프로파일과 일치하는 사용자의 경우 하드 드라이브에 저장된 데이터 특성에 경미한 위험을 초래할 수 있습니다.

DriveLock 사용

ATA 보안 명령 모음을 지원하는 하나 이상의 하드 드라이브가 감지된 경우 Computer Setup 의 Security) 메뉴 아래에 DriveLock 옵션이 나타납니다. 사용자에게 마스터 암호를 설정하거나 DriveLock 을 활성화하는 옵션이 표시됩니다. 사용자 암호를 입력해야 DriveLock 을 활성화할 수 있습니다. 일반적으로 시스템 관리자가 DriveLock 의 초기 구성을 수행하므로 먼저 마스터 암호를 설정해야 합니다. HP 는 DriveLock 을 활성화하거나 비활성 상태를 유지하는 것과 관계없이 시스템 관리자에게 마스터 암호를 설정하도록 권장합니다. 따라서 나중에 드라이브가 잠기면 관리자가 DriveLock 설정을 수정할 수 있습니다. 마스터 암호가 설정되면 시스템 관리자는 DriveLock 을 활성화하거나 비활성 상태를 유지할 수 있습니다.

잠긴 하드 드라이브가 있는 경우 POST 는 장치의 잠금을 해제하는 암호를 요구합니다. 파워온 암호가 설정되고 이 암호가 장치의 사용자 암호와 일치하면 POST 는 사용자에게 암호를 다시 입력하라는 메시지를 표시하지 않습니다. 그러나 일치하지 않으면 DriveLock 암호를 입력하라는 메시지를 표시합니다. 콜드 부팅 시 마스터 암호나 사용자 암호를 사용할 수 있습니다. 웜 부팅 시 이전 콜드 부팅 중 드라이브 잠금 해제에 사용한 암호를 입력합니다. 사용자는 정확한 암호를 두 번 입력하게 됩니다. 콜드 부팅 시 두 번의 암호 입력이 모두 실패한 경우 POST 는 계속되지만 드라이브에는 액세스할 수 없습니다. 웜 부팅 시 또는 Windows 에서 다시 시작할 때 두 번의 암호 입력이 모두 실패한 경우 POST 가 중지되고 컴퓨터의 전원을 껐다가 다시 켜라는 메시지가 나타납니다.

DriveLock 응용프로그램

DriveLock 보안 기능은 기업 환경에서 가장 많이 사용됩니다. 시스템 관리자는 특히 DriveLock 마스터 암호 및 임시 사용자 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.

DriveLock 을 다루는 회사 시스템 관리자가 마스터 암호 설정 및 유지 관리를 위한 회사 정책을 수립하는 것이 좋습니다. 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 DriveLock 을 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 DriveLock 이 보호하도록 설계된 값보다 훨씬 더 큽니다. Computer Setup 및 DriveLock 에 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

일부 모델에서 사용할 수 있는 Cover Removal Sensor 는 하드웨어와 소프트웨어 기술이 조합된 것으로 컴퓨터 덮개나 측면 패널이 열린 경우 사용자에게 경고합니다. 다음 표에서 설명한 대로 세 가지 보호 수준이 있습니다.

표 11–2 Smart Cover Sensor 보호 수준

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

주: 이러한 설정은 Computer Setup 을 사용하여 변경할 수 있습니다. Computer Setup 에 대한 자세한 내용은 *Computer Setup(F10) 유틸리티 설명서*를 참조하십시오.

Smart Cover Sensor 보호 수준 설정

Smart Cover Sensor 보호 수준을 설정하려면 다음 단계를 완료합니다.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

   주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

3. **Security**(보안) > **Smart Cover**(스마트 커버) > **Cover Removal Sensor**(커버 제거 센서)를 선택하고 원하는 보안 수준을 선택합니다.
4. 종료하기 전에 **File**(파일) > **Save Changes and Exit**(변경 사항 저장 후 종료)를 누릅니다.

Smart Cover Lock

Smart Cover Lock 은 일부 HP 컴퓨터에 설치된 소프트웨어로 제어할 수 있는 덮개 잠금 장치입니다. 이 잠금 장치는 내부 부품에 무단 접근하는 것을 방지합니다. 컴퓨터는 잠금 해제 위치로 설정된 SmartCover Lock 과 함께 제공됩니다.

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

주: Smart Cover Lock 은 일부 시스템의 선택 사양으로 사용합니다.

Smart Cover Lock 잠금

Smart Cover Lock 을 활성화하고 잠그려면 다음 단계를 완료합니다.

1. 컴퓨터를 켜거나 다시 시작합니다. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

3. **Security**(보안) > **Smart Cover**(스마트 커버) > **Cover Lock**(커버 잠금) > **Lock**(잠금) 옵션을 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. Windows 의 경우 **시작 > 시스템 종료 > 다시 시작**을 누릅니다.
2. 컴퓨터가 켜지고 운영체제로 부팅되기 전에 F10 키를 눌러 Computer Setup 으로 들어갑니다. 필요한 경우 Enter 키를 눌러 제목 화면을 생략하십시오.

주: 적절한 시점에 F10 키를 누르지 않으면 컴퓨터를 다시 시작하여 운영체제로 부팅되기 전에 다시 F10 키를 눌러야 유틸리티에 액세스할 수 있습니다.

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

Smart Cover FailSafe 키 사용

Smart Cover Lock 이 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 HP 가 제공하는 전문적인 도구입니다. 필요한 상황에 대비하여 공인 판매업체 또는 서비스 제공업체에 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.

케이블 잠금 장치

컴퓨터(일부 모델)의 뒷면은 작업 영역에서 컴퓨터를 물리적으로 보호할 수 있도록 케이블 잠금을 조정합니다.

그림으로 설명된 지침을 보려면 *하드웨어 참조 설명서*를 참조하십시오.

지문 인식 기술

HP 의 지문 인식 기술은 사용자 암호를 입력하지 않고도 네트워크 보안을 강화하고, 로그인 프로세스를 단순화하며, 회사 네트워크 관리와 관련된 비용을 절감합니다. 공급 가능한 가격 덕분에 이 기술은 최첨단의 보안성이 뛰어난 조직뿐만 아니라 일반 조직에도 적합합니다.

주: 지문 인식 기술에 대한 지원은 모델에 따라 다릅니다.

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.

컴퓨터가 HP Client Manager 로 관리되는 네트워크에 연결되어 있으면 해당 컴퓨터는 네트워크 관리 응용프로그램에 오류 알림을 전송합니다. HP Client Manager 소프트웨어를 사용하면 원격으로 진단 일정을 계획하여 관리되는 모든 PC 에 자동으로 실행하고 실패한 테스트에 대해 요약 보고서를 작성할 수 있습니다.

드라이브 보호 시스템

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

HP 컴퓨터를 만들 때 설치되는 각 하드 드라이브는 DPS 를 사용하여 테스트되고 주요 정보는 드라이브에 영구적으로 기록됩니다. DPS 가 실행될 때마다 테스트 결과가 하드 드라이브에 기록됩니다. 서비스 제공 업체는 이 정보를 사용하여 DPS 소프트웨어가 실행되었던 상태를 진단할 수 있습니다. DPS 에 대한 지침은 *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 정상 작동 범위를 초과하는 경우 내부 부품이 손상되거나 데이터가 손실되기 전에 조치를 취할 시간을 주도록 경고 메시지를 표시합니다.

△ 주의: 고온 상태에서는 시스템에 손상이 가거나 데이터를 잃을 수 있습니다.

색인