Dell EMC

BIOS 및 UEFI 참조 가이드

참고, 주의 및 경고

노트: 참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 중요 정보를 제공합니다.

주의: 주의사항은 하드웨어의 손상 또는 데이터 유실 위험을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.

경고: 경고는 재산 손실, 신체적 상해 또는 사망 위험이 있음을 알려줍니다.

© 2019 - 2020 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC 및 기타 상표는 Dell Inc. 또는 그 자회사의 상표입니다. 다른 상표는 해당 소유자의 상표일 수 있습니다.

목차

장 1: 사전 운영 체제 관리 애플리케이션 4
시스템 설치 프로그램 4
System BIOS(시스템 BIOS) 5
iDRAC 설정 유틸리티 19
장치 설정 19
Dell Lifecycle Controller 19
내장형 시스템 관리 20
부팅 관리자 20
PXE 부팅 20

1

사전 운영 체제 관리 애플리케이션

시스템 펌웨어를 사용하여 운영 체제로 부팅하지 않고 시스템의 기본 설정 및 기능을 관리할 수 있습니다.

사전 운영 체제 응용프로그램을 관리할 수 있는 옵션

다음 옵션 중 하나를 사용하여 사전 운영 체제 애플리케이션을 관리할 수 있습니다.

- 시스템 설치 프로그램
- Dell Lifecycle Controller
- 부팅 관리자
- 사전 부팅 실행 환경(PXE)

주제:

- 시스템 설치 프로그램
- Dell Lifecycle Controller
- 부팅 관리자
- PXE 부팅

시스템 설치 프로그램

System Setup 옵션을 사용하여 시스템의 BIOS 설정, iDRAC 설정 및 디바이스 설정을 구성할 수 있습니다.

다음 인터페이스 중 하나를 사용하여 시스템 설정에 액세스할 수 있습니다.

- GUI(Graphical User Interface) - iDRAC 대시보드에 액세스하려면 **Configuration**을 클릭하고 **BIOS Settings**를 클릭합니다.
- 텍스트 브라우저 - 브라우저는 콘솔 리디렉션을 사용하여 활성화됩니다.

System Setup을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **System Setup Main Menu**를 클릭합니다.

노트: <F2> 키를 누르기 전에 운영 체제가 로드되기 시작하면 시스템 부팅이 완료될 때까지 기다린 다음 시스템을 재시작하고 다시 시도합니다.

System Setup Main Menu 화면 세부 정보는 다음과 같습니다.

표 1. 시스템 설정 기본 메뉴

옵션	설명
System BIOS(시스템 BIOS)	BIOS 설정을 구성할 수 있습니다.
iDRAC Settings	iDRAC 설정을 구성할 수 있습니다. iDRAC Settings(idrac 설정) 유틸리티는 UEFI (Unified Extensible 펌웨어 인터페이스; Small Computer System Interface)를 사용하여 iDRAC 매개 변수를 설정하고 구성하려면 인터페이스를. iDRAC 설정 유틸리티를 사용하여 다양한 iDRAC 매개 변수를 활성화하거나 비활성화할 수 있습니다. 이 유틸리티에 대한 자세한 정보는 www.dell.com/poweredgemanuals에서 *Integrated Dell Remote Access Controller 사용자 가이드*를 참조하십시오.
장치 설정	스토리지 컨트롤러 또는 네트워크 카드와 같은 디바이스의 디바이스 설정을 구성할 수 있습니다.

System BIOS(시스템 BIOS)

System BIOS 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **System Setup Main Menu** > **System BIOS**를 클릭합니다.

표 2. 시스템 BIOS 세부 정보

옵션	설명
시스템 정보	시스템 모델 이름, BIOS 버전, 서비스 태그 등 시스템에 대한 정보를 표시합니다.
메모리 설정	설치된 메모리와 관련된 정보 및 옵션을 표시합니다.
프로세서 설정	프로세서와 관련된 속도, 캐시 크기 등의 정보 및 옵션을 표시합니다.
SATA 설정	내장형 SATA 컨트롤러 및 포트를 활성화하거나 비활성화하는 옵션을 표시합니다.
NVMe 설정	네트워크 설정을 변경할 수 있는 옵션을 표시합니다. RAID 어레이에 구성할 NVMe 드라이브가 시스템에 포함되어 있다면 **SATA 설정** 메뉴에서 이 필드와 **내장 SATA** 필드를 **RAID** 모드로 설정해야 합니다. 설정을 **UEFI 부팅 모드를 변경해야 하는 경우 수도 있습니다**. 그렇지 않으면, 이 필드 **가 비 RAID** 모드로(제한됨)로 설정되어야 합니다.
부팅 설정	부팅 모드(BIOS 또는 UEFI)를 지정하는 옵션을 표시합니다. UEFI 및 BIOS 부팅 설정을 수정할 수 있습니다.
Network Settings(네트워크 설정)	UEFI 네트워크 설정을 관리하는 옵션 및 부팅 프로토콜을 지정합니다. 레거시 네트워크 설정은 **디바이스 설정** 메뉴에서 관리됩니다. **노트:** 네트워크 설정은 BIOS 부팅 모드에서 지원되지 않습니다.
내장형 장치	내장형 디바이스 컨트롤러 및 포트를 관리하고 관련 기능 및 옵션을 지정하는 옵션을 지정합니다.
직렬 통신	직렬 포트를 관리하고 관련 기능 및 옵션을 지정하는 옵션을 지정합니다.
시스템 프로필 설정	프로세서 전원 관리 설정, 메모리 주파수 등을 변경하는 옵션을 표시합니다.
시스템 보안	시스템 암호, 설정 암호, TPM(Trusted Platform Module) 보안 등의 시스템 보안 설정을 구성하는 옵션을 표시합니다. 또한, 시스템의 전원 버튼을 관리합니다.
이중화 OS 제어	이중화 OS 제어에 대한 이중화 OS 정보를 설정합니다.
기타 설정	시스템 날짜, 시간 등을 변경하는 옵션을 표시합니다.

시스템 정보

System Information 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **System Setup Main Menu** > **System BIOS** > **System Information**을 클릭합니다.

표 3. System Information 세부 정보

옵션	설명
System Model Name(시스템 모델 이름)	시스템 모델 이름을 표시합니다.
System BIOS Version(시스템 BIOS 버전)	시스템에 설치된 BIOS 버전을 표시합니다.
System Service Tag(시스템 서비스 태그)	시스템 서비스 태그를 표시합니다.
System Manufacturer(시스템 제조업체)	시스템 제조업체 이름을 표시합니다.
System Manufacturer Contact Information(시스템 제조업체 연락처 정보)	시스템 제조업체의 연락처 정보를 표시합니다.
System CPLD Version(시스템 CPLD 버전)	시스템 CPLD(복잡한 프로그래밍 가능 논리 장치) 펌웨어의 현재 버전을 표시합니다.
UEFI 준수 버전	시스템 펌웨어의 UEFI 규정 준수 수준을 표시합니다.
AGESA Version	AGESA 참조 코드 버전을 지정합니다.

표 3. System Information 세부 정보 (계속)

옵션	설명
SMU Version	SMU 펌웨어 버전을 지정합니다.
DXIO Version	DXIO 펌웨어 버전을 지정합니다.

메모리 설정

메모리 설정 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **시스템 설정 기본 메뉴** > **시스템 BIOS** > **메모리 설정**을 클릭합니다.

표 4. 메모리 설정 세부 정보

옵션	설명
시스템 메모리 크기	시스템의 메모리 크기를 표시합니다.
시스템 메모리 유형	시스템에 설치된 메모리 유형을 표시합니다.
시스템 메모리 속도	시스템 메모리 속도를 표시합니다.
시스템 메모리 전압	시스템 메모리 전압을 표시합니다.
비디오 메모리	비디오 메모리 크기를 표시합니다.
시스템 메모리 테스트	시스템 부팅 중에 시스템 메모리 테스트가 실행되는지 여부를 지정합니다. 사용할 수 있는 2개의 옵션은 **활성화** 및 **비활성화**입니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
DRAM 리프레시 지연	**CPU 메모리 컨트롤러**를 활성화하여 **REFRESH** 명령 실행을 지연시키면 일부 워크로드의 성과를 향상시킬 수 있습니다. 이는 지연 시간을 최소화하여 메모리 컨트롤러가 **REFRESH** 명령을 일정 간격으로 실행하도록 합니다. 인텔 기반 서버의 경우 이 설정은 8Gb 밀도의 DRAM을 사용하는 DIMM으로 구성된 시스템에만 영향을 줍니다. 기본적으로 이 옵션은 **최소**로 설정됩니다.
메모리 작동 모드	메모리 작동 모드를 지정합니다. 기본적으로 이 옵션은 **최적화 모드**로 설정됩니다.
메모리 작동 모드의 현재 상태	메모리 작동 모드의 현재 상태를 지정합니다.
메모리 인터리빙	메모리 인터리빙 옵션을 활성화 또는 비활성화합니다. 사용할 수 있는 2개의 옵션은 **자동** 및 **비활성화**입니다. 이 옵션은 기본값으로 **자동**으로 설정됩니다.
편의적 자동 새로 고침	편의적 자동 새로 고침 기능을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
수정 가능한 오류 저널링	수정 가능한 오류 로깅을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.

프로세서 설정

프로세서 설정 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **시스템 설정 기본 메뉴** > **시스템 BIOS** > **프로세서 설정**을 클릭합니다.

표 5. 프로세서 설정 세부 정보

옵션	설명
논리 프로세서	각 프로세서 코어는 최대 2개의 논리 프로세서를 지원합니다. 이 옵션이 **활성화**로 설정되는 경우, BIOS는 모든 논리 프로세서를 표시합니다. 이 옵션이 **비활성화**로 설정되는 경우, BIOS는 코어당 1개의 논리 프로세서만 표시합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
가상화 기술	프로세서의 가상화 기술을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.

표 5. 프로세서 설정 세부 정보 (계속)

옵션	설명
IOMMU 지원	IOMMU 지원을 활성화 또는 비활성화합니다. IVRS ACPI 표를 생성하는 데 필요합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
L1 스트림 HW 프리페처	L1 스트림 하드웨어 프리페처를 활성화 또는 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
L2 스트림 HW 프리페처	L2 스트림 하드웨어 프리페처를 활성화 또는 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
MADT 코어 열거	MADT 코어 열거를 지정합니다. 기본적으로 이 옵션은 **선형**으로 설정됩니다.
소켓당 NUMA 노드 수	소켓당 NUMA 노드의 수를 지정합니다. 기본적으로 이 옵션은 **1**로 설정됩니다.
CCX를 NUMA 도메인으로	CCX를 NUMA 도메인으로 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
최소 SEV 비ES ASID	Secure Encrypted Virtualization ES 및 비ES를 사용할 수 있는 주소 공간 ID의 수를 정합니다. 기본적으로 이 옵션은 **1**로 설정됩니다.
x2APIC 모드	x2APIC 모드를 활성화 또는 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다. **노트:** 2개의 CPU 64코어 구성의 경우 256스레드가 활성화된 경우(BIOS 설정: 모든 CCD, 코어 및 논리 프로세서 활성화) x2APIC 모드를 전환할 수 없습니다.
프로세서당 CCD의 수	각 프로세서에서 활성화된 CCD의 개수를 제어합니다. 기본적으로 이 옵션은 **모두**로 설정됩니다.
CCD별 코어 개수	CCD별 코어 개수를 지정합니다. 기본적으로 이 옵션은 **모두**로 설정됩니다.
프로세서 코어 속도	프로세서의 최대 코어 주파수를 표시합니다.
프로세서 n	**노트:** CPU 수에 따라 최대 n개의 프로세서가 나열될 수 있습니다. 시스템에 설치된 각 프로세서에 대해 다음 설정이 표시됩니다.

표 6. 프로세서 및 세부 정보

옵션	설명
제품군-모델-스테핑	AMD에서 정의한 대로 프로세서의 제품군, 모델 및 스테핑을 지정합니다.
브랜드	브랜드 이름을 표시합니다.
수준 2 캐시	전체 L2 캐시를 표시합니다.
수준 3 캐시	전체 L3 캐시를 표시합니다.
코어 수	프로세서당 코어 수를 표시합니다.
마이크로코드	프로세서 마이크로코드 버전을 지정합니다.

SATA 설정

SATA Settings 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **System Setup Main Menu** > **System BIOS** > **SATA Settings**를 클릭합니다.

표 7. SATA Settings 세부 정보

옵션	설명
내장형 SATA	내장형 SATA 옵션을 **Off**, **AHCI mode** 또는 **RAID modes**로 설정할 수 있습니다. 이 옵션은 기본값으로 **AHCI Mode(AHCI 모드)**로 설정됩니다. **노트:** 1. 설정을 UEFI 부팅 모드를 변경해야 하는 경우 수도 있습니다. 그렇지 않으면, 이 필드를 비RAID 모드로 설정해야 합니다. 2. ESXi 및 Ubuntu OS는 RAID 모드에서 지원되지 않습니다.
Security Freeze Lock	POST 중 **Security Freeze Lock** 명령을 내장형 SATA 드라이브로 전송합니다. 이 옵션은 AHCI 모드에만 적용됩니다. 이 옵션은 기본적으로 **Enabled(활성화)**로 설정됩니다.
쓰기 캐시	POST 중 내장형 SATA 드라이브에 대한 명령을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **Disabled(비활성화)**로 설정됩니다.
포트 n	선택한 장치에 대한 드라이브 종류를 설정합니다. **AHCI mode(AHCI 모드)** 또는 **RAID Mode(RAID 모드)**에 대한 BIOS 지원을 항상 사용할 수 있습니다. **표 8. 포트 n**

표 8. 포트 n

옵션	설명
모델	선택한 장치의 드라이브 모델을 표시합니다.
드라이브 유형	SATA 포트에 연결된 드라이브의 종류를 표시합니다.
용량	드라이브의 전체 용량을 표시합니다. 옵티컬 드라이브와 같은 이동식 미디어 디바이스에 대해서는 이 필드가 정의되지 않습니다.

NVMe 설정

이 옵션은 NVMe 드라이브 모드를 설정합니다. RAID 어레이에 구성할 NVMe 드라이브가 시스템에 포함되어 있다면 SATA Settings 메뉴에서 이 필드와 Embedded SATA 필드를 RAID Mode로 설정해야 합니다. Boot Menu 설정을 UEFI로 변경해야 할 수도 있습니다. 기본적으로 이 옵션은 **Non-RAID** 모드로 설정됩니다.

부팅 설정

Boot Settings(부팅 설정) 화면을 사용하여 부팅 모드를 **BIOS** 또는 **UEFI**로 설정할 수 있습니다. 또한 부팅 순서를 지정할 수 있습니다.

- **UEFI**: UEFI(Unified Extensible Firmware Interface)는 운영 체제와 플랫폼 펌웨어 사이의 새로운 인터페이스입니다. 이 인터페이스는 운영 체제 및 해당 로더에 사용할 수 있는 부팅 및 런타임 서비스 콜과 플랫폼 관련 정보를 포함하는 데이터 테이블로 구성되어 있습니다. 다음 이점은 **Boot Mode(부팅 모드)**가 **UEFI**로 설정된 경우 사용 가능합니다.
  - 2TB보다 큰 드라이브 파티션 지원.
  - 고급 보안(예: UEFI 보안 부팅).
  - 보다 빠른 부팅 시간.

  노트: NVMe 드라이브에서 부팅하기 위해서는 UEFI 부팅 모드만 사용해야 합니다.
- **BIOS**: **BIOS 부팅 모드**는 기존 부팅 모드입니다. 이 모드는 이전 버전과의 호환성을 위해 유지됩니다.

Boot Settings 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **System Setup Main Menu** > **System BIOS** > **Boot Settings**를 클릭합니다.

표 9. Boot Settings 세부 정보

옵션	설명
Boot Mode	시스템의 부팅 모드를 설정할 수 있습니다. 운영 체제에서 UEFI를 지원하는 경우 이 옵션을 UEFI로 설정할 수 있습니다. 이 필드를 BIOS로 설정하면 UEFI를 지원하지 않는 운영 체제와의 호환성을 유지할 수 있습니다. 기본적으로 이 옵션은 **UEFI**로 설정됩니다. **주의: 운영 체제가 설치된 부팅 모드가 아닌 다른 부팅 모드로 전환하면 시스템이 부팅되지 않을 수 있습니다.** **노트:** 이 필드를 UEFI로 설정하는 경우 **BIOS 부팅 설정** 메뉴가 비활성화됩니다.
Boot Sequence Retry	**Boot Sequence Retry(부팅 순서 재시도)** 기능을 활성화하거나 비활성화합니다. 이 필드가 활성화되고 시스템이 부팅에 실패하는 경우 시스템은 30초 후에 부팅 순서를 다시 시도합니다. 이 옵션은 기본적으로 **Enabled(활성화)**로 설정됩니다.
하드 디스크 페일오버	하드 디스크 페일오버를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **Disabled(비활성화)**로 설정됩니다.
일반 USB 부팅	일반 USB 부팅 자리 표시자를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **Disabled(비활성화)**로 설정됩니다.
하드 디스크 드라이브 자리 표시자	하드 디스크 드라이브 고정 장치를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **Disabled(비활성화)**로 설정됩니다.
모든 Sysprep 순서 및 변수 지우기	**없음**으로 설정하면 BIOS가 아무 작업도 하지 않습니다. **예**로 설정하면 BIOS가 SysPrepOrder 및 SysPrep ####의 변수를 삭제합니다. 이 옵션은 일회성 옵션으로, 변수 삭제 시 없음으로 재설정됩니다. 이 설정은 **UEFI 부팅 모드**에서만 사용할 수 있습니다. 기본적으로 이 옵션은 **None(없음)**로 설정됩니다.
UEFI 부팅 설정	UEFI 부팅 순서를 지정합니다. UEFI 부팅 옵션을 활성화 또는 비활성화합니다. **노트:** 이 옵션은 UEFI 부팅 순서를 제어합니다. 목록의 첫 번째 옵션이 먼저 수행됩니다. **표 10. UEFI 부팅 설정** 옵션: **UEFI 부팅 순서** — 부트 디바이스 순서를 변경할 수 있습니다. 옵션: **부팅 옵션 활성화/비활성화** — 부트 디바이스를 활성화 또는 비활성화하도록 선택할 수 있습니다.

시스템 부팅 모드 선택

시스템 설정을 사용하면 운영 체제를 설치하는 경우 다음의 부팅 모드를 지정할 수 있습니다.

- 기본값인 UEFI 부팅 모드는 향상된 64비트 부팅 인터페이스입니다.

  UEFI 모드로 시스템이 부팅되도록 구성한 경우 시스템 BIOS가 교체됩니다.

1. **System Setup Main Menu(시스템 설정 기본 메뉴)**에서 **Boot Settings(부팅 설정)**를 클릭한 후 **Boot Mode(부팅 모드)**를 선택합니다.
2. 시스템을 부팅할 UEFI 부팅 모드를 선택합니다.

   주의: 운영 체제가 설치된 부팅 모드가 아닌 다른 부팅 모드로 전환하면 시스템이 부팅되지 않을 수 있습니다.
3. 시스템이 지정된 부팅 모드에서 부팅된 후 해당 모드에서 운영 체제를 설치합니다.

노트: UEFI 부팅 모드에서 운영 체제를 설치하려면 운영 체제가 UEFI와 호환되어야 합니다. DOS 및 32비트 운영 체제는 UEFI를 지원하지 않으며 BIOS 부팅 모드에서만 설치될 수 있습니다.

노트: 지원되는 운영 체제에 대한 최신 정보를 보려면 www.dell.com/ossupport 페이지로 이동하십시오.

부팅 순서 변경

이 작업 정보

USB 키 또는 광학 드라이브에서 부팅하려는 경우 부팅 순서를 변경해야 할 수도 있습니다. **부팅 모드**로 **BIOS**를 선택한 경우 다음 지침이 달라질 수 있습니다.

노트: 드라이브 부팅 순서 변경은 BIOS 부팅 모드에서만 지원됩니다.

단계

1. **시스템 설정 기본 메뉴** 화면에서 **시스템 BIOS** > **부팅 설정** > **UEFI 부팅 설정** > **UEFI 부팅 순서**를 클릭합니다.
2. 화살표 키를 사용하여 부팅 장치를 선택하고 + 및 - 키를 사용하여 순서대로 장치를 아래 또는 위로 이동합니다.
3. **Exit(종료)**를 클릭하고 **Yes(예)**를 클릭하여 설정을 저장합니다.

   노트: 또한, 필요에 따라 부팅 순서 디바이스를 활성화하거나 비활성화할 수 있습니다.

네트워크 설정

네트워크 설정 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **시스템 설정 기본 메뉴** > **시스템 BIOS** > **네트워크 설정**을 클릭합니다.

노트: Linux 네트워크 성능 설정에 대한 자세한 정보는 AMD.com에서 *AMD EPYC 프로세서 기반 서버의 Linux 네트워크 튜닝 가이드*를 참조하십시오.

노트: 네트워크 설정은 BIOS 부팅 모드에서 지원되지 않습니다.

표 11. 네트워크 설정 세부 정보

옵션	설명
UEFI PXE 설정	UEFI PXE 디바이스의 구성을 제어할 수 있습니다.
PXE 디바이스 n(n = 1~4)	디바이스를 활성화 또는 비활성화합니다. 활성화된 경우 UEFI PXE 부팅 옵션이 디바이스에 대해 생성됩니다.
PXE 디바이스 n 설정(n = 1~4)	PXE 디바이스의 구성을 제어할 수 있습니다.
UEFI HTTP 설정	UEFI HTTP 디바이스의 구성을 제어할 수 있습니다.
HTTP 디바이스 n(n = 1~4)	디바이스를 활성화 또는 비활성화합니다. 활성화된 경우 UEFI HTTP 부팅 옵션이 디바이스에 대해 생성됩니다.
HTTP 디바이스 n 설정(n = 1~4)	HTTP 디바이스의 구성을 제어할 수 있습니다.
UEFI iSCSI 설정	iSCSI 디바이스의 구성을 제어할 수 있습니다.

표 12. PXE 디바이스 n 설정 세부 정보

옵션	설명
인터페이스	PXE 디바이스에 사용되는 NIC 인터페이스를 지정합니다.
프로토콜	PXE 디바이스에 사용되는 프로토콜을 지정합니다. 이 옵션은 **IPv4** 또는 **IPv6**으로 설정됩니다. 기본적으로 이 옵션은 **IPv4**로 설정됩니다.
VLAN	PXE 디바이스의 VLAN을 활성화합니다. 이 옵션은 **활성화** 또는 **비활성화**로 설정됩니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
VLAN ID	PXE 디바이스의 VLAN ID를 표시합니다.
VLAN 우선 순위	PXE 디바이스의 VLAN 우선 순위를 표시합니다.

표 13. HTTP 디바이스 n 설정 세부 정보

옵션	설명
인터페이스	HTTP 디바이스에 사용되는 NIC 인터페이스를 지정합니다.

표 13. HTTP 디바이스 n 설정 세부 정보 (계속)

옵션	설명
프로토콜	HTTP 디바이스에 사용되는 프로토콜을 지정합니다. 이 옵션은 **IPv4** 또는 **IPv6**으로 설정됩니다. 기본적으로 이 옵션은 **IPv4**로 설정됩니다.
VLAN	HTTP 디바이스의 VLAN을 활성화합니다. 이 옵션은 **활성화** 또는 **비활성화**로 설정됩니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
VLAN ID	HTTP 디바이스의 VLAN ID를 표시합니다.
VLAN 우선 순위	HTTP 디바이스의 VLAN 우선 순위를 표시합니다.
DHCP	이 HTTP 디바이스에 대해 DHCP를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
IP 주소	HTTP 디바이스의 IP 주소를 지정합니다.
서브넷 마스크	HTTP 디바이스의 서브넷 마스크를 지정합니다.
게이트웨이	HTTP 디바이스의 게이트웨이를 지정합니다.
DHCP를 통한 DNS 정보	DHCP의 DNS 정보를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
기본 DNS	HTTP 디바이스의 기본 DNS 서버 IP 주소를 지정합니다.
보조 DNS	HTTP 디바이스의 보조 DNS 서버 IP 주소를 지정합니다.
URI	지정되지 않은 경우 DHCP 서버에서 URI 확보

표 14. UEFI iSCSI 설정 화면 세부 정보

옵션	설명
iSCSI 초기자 이름	IQN 형식의 iSCSI 초기자 이름을 지정합니다.
iSCSI Device1	iSCSI 디바이스를 활성화 또는 비활성화합니다. 비활성화된 경우 UEFI 부팅 옵션이 iSCSI 디바이스를 위해 자동으로 생성됩니다. 이 옵션은 기본값으로 **비활성화**로 설정됩니다.
iSCSI Device1 설정	iSCSI 디바이스의 구성을 제어할 수 있습니다.

표 15. ISCSI Device1 설정 화면 세부 정보

옵션	설명
연결 1	iSCSI 연결을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
연결 2	iSCSI 연결을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
연결 1 설정	iSCSI 연결의 구성을 제어할 수 있습니다.
연결 2 설정	iSCSI 연결의 구성을 제어할 수 있습니다.
연결 순서	iSCSI 연결을 시도하는 순서를 제어할 수 있습니다.

내장형 디바이스

내장형 디바이스 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **시스템 설정 기본 메뉴** > **시스템 BIOS** > **내장형 디바이스**를 클릭합니다.

표 16. 내장형 디바이스 세부 정보

옵션	설명
사용자 액세스 가능 USB 포트	사용자 액세스 가능 USB 포트를 구성합니다. **후면 포트만 켜기**를 선택하면 전면 USB 포트가 비활성화되고 **모든 포트 끄기**를 선택하면 모든 전면 및 후면 USB 포트가 비활성화되며 **모든 포트 끄기(동적)**를 선택하면 POST 중 모든 전면 및 후면 USB 포트가 비활성화됩니다. 기본적으로 이 옵션은 **모든 포트 켜기**로 설정됩니다.

표 16. 내장형 디바이스 세부 정보 (계속)

옵션	설명
	사용자가 액세스할 수 있는 USB 포트가 **모든 포트 끄기(동적)**로 설정되면 **전면 포트만 활성화** 옵션이 활성화됩니다. • **전면 포트만 활성화**: OS 런타임 중 전면 USB 포트를 활성화하거나 비활성화합니다. USB 키보드 및 마우스는 선택에 따라 부팅 프로세스 동안 특정 USB 포트에서 여전히 기능합니다. 부팅 프로세스가 완료된 후 USB 포트가 설정에 따라 활성화되거나 비활성화됩니다.
내부 USB 포트	**내부 USB 포트**를 활성화하거나 비활성화합니다. 이 옵션은 **켜기** 또는 **끄기**로 설정됩니다. 기본적으로 이 옵션은 **켜기**로 설정됩니다.
iDRAC Direct USB 포트	iDRAC Direct USB 포트는 호스트를 볼 수 없고 iDRAC가 독점적으로 관리합니다. 이 옵션은 **켜기** 또는 **끄기**로 설정됩니다. **끄기**로 설정하는 경우, iDRAC 포트 관리되는 이에 설치된 모든 USB 디바이스를 감지하지 않습니다. 기본적으로 이 옵션은 **켜기**로 설정됩니다.
내장형 RAID 컨트롤러	내부 RAID 컨트롤러 포트를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
내장형 NIC1 및 NIC2	**내장형 NIC1 및 NIC2** 옵션을 활성화하거나 비활성화합니다. **비활성화(OS)**로 설정할 경우에도 내장형 관리 컨트롤러에 의해 NIC가 공유 네트워크 액세스를 사용할 수 있습니다. 시스템의 NIC 관리 유틸리티를 사용하여 **내장형 NIC1 및 NIC2** 옵션을 구성합니다.
내장형 비디오 컨트롤러	기본 디스플레이로 내장형 비디오 컨트롤러의 사용을 활성화하거나 비활성화합니다. **활성화**로 설정된 경우 추가 그래픽 카드가 설치되어 있어도 내장형 비디오 컨트롤러가 기본 디스플레이가 됩니다. **비활성화**로 설정된 경우 추가 그래픽 카드가 기본 디스플레이로 사용됩니다. BIOS는 POST 도중이나 사전 부팅 환경에서 추가 비디오와 내장형 비디오 양쪽으로 디스플레이를 출력합니다. 그러면 운영 체제가 부팅되기 직전에 내장형 비디오가 비활성화됩니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다. **노트:** 시스템에 여러 개의 추가 그래픽 카드가 설치된 경우 PCI 열거 중 발견된 첫 번째 카드가 기본 비디오로 선택됩니다. 기본 비디오로 사용할 카드를 제어하려면 슬롯의 카드를 다시 정렬해야 할 수도 있습니다.
내장형 비디오 컨트롤러의 현재 상태	내장형 비디오 컨트롤러의 현재 상태를 보여줍니다. **내장형 비디오 컨트롤러의 현재 상태** 옵션은 읽기 전용 필드입니다. 내장형 비디오 컨트롤러가 시스템의 유일한 디스플레이 기능인 경우(즉, 추가 그래픽 카드가 설치되어 있지 않은 경우) **내장형 비디오 컨트롤러**가 **비활성화**로 설정되어도 내장형 비디오 컨트롤러가 자동으로 기본 디스플레이로 사용됩니다.
PCIe 기본 IO 버스	**활성화**로 설정하면 버스 주소(10진수)를 제공하여 기본 IO 버스의 엔드 디바이스를 선택할 수 있습니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
향상된 기본 IO	**활성화**로 설정하면 기본 IO가 활성화되어 있는 루트 복잡성에 대한 LCLK 속도가 자동으로 600MHz(유효 593MHz)로 설정됩니다.
SR-IOV 글로벌 활성화	SR-IOV(Single Root I/O Virtualization) 디바이스의 BIOS 구성을 활성화 또는 비활성화합니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
내부 SD 카드 포트	IDSDM(Internal Dual SD Module)의 내부 SD 카드 포트를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **켜기**로 설정됩니다.
내부 SD 카드 이중화	IDSDM(Internal Dual SD Module)의 이중화 모드를 구성합니다. **Mirror**(미러) 모드로 설정된 경우 데이터가 두 SD 카드에 모두 기록됩니다. 카드 중 하나의 오류 및 교체 후 오류가 있는 카드의, 활성 카드의 데이터는 시스템 부팅 중 오프라인으로 카드를 복사됩니다. 때 내부 SD 카드 중복성이 설정 **Disabled(사용 안 함)로**, 기본 SD 카드만은 OS이 확인할 수 있습니다. 기본적으로 이 옵션은 **Mirror**로 설정됩니다.

표 16. 내장형 디바이스 세부 정보 (계속)

옵션	설명
내부 SD 기본 카드	기본적으로 기본 SD 카드가 SD 카드 1로 선택됩니다. SD 카드 1이 없는 경우, 컨트롤러가 SD 카드 2를 기본 SD 카드로 선택합니다. 기본적으로 이 옵션은 **SD Card 1**로 설정됩니다.
OS Watchdog 타이머	시스템이 응답을 멈추는 경우, 이러한 와치독 타이머가 운영 체제 복구에 도움을 줍니다. 이 옵션이 **활성화**로 설정되는 경우, 운영 체제가 타이머를 초기화합니다. 이 옵션이 **비활성화**(기본값)로 설정되면 타이머는 시스템에 영향을 주지 않습니다.
메모리 매핑된 I/O 제한	MMIO가 매핑되는 위치를 제어합니다. **1TB** 옵션은 1TB 초과 시 MMIO를 지원하지 못하는 특정 OS를 위해 설계되었습니다. 기본값으로 이 옵션은 **8TB**로 설정됩니다. 기본값 옵션은 시스템에서 지원하는 최대 주소로, 대부분의 경우에 권장됩니다.
슬롯 비활성화	시스템에서 사용 가능한 PCIe 슬롯을 활성화하거나 비활성화합니다. 슬롯 비활성화 기능은 지정된 슬롯에 설치된 PCIe 카드의 구성을 제어합니다. 슬롯 비활성화는 설치된 주변 기기 카드로 인해 운영 체제에 부팅할 수 없거나 어플라이언스 시작이 지연되는 경우에만 사용해야 합니다. 슬롯이 비활성화되면 옵션 ROM과 UEFI 드라이버가 모두 비활성화됩니다. 시스템에 있는 슬롯만 제어할 수 있습니다. **Slot n**: 활성화 또는 비활성화하거나 PCIe 슬롯 n의 부팅 드라이버만 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
슬롯 분기	**슬롯 검색 분기 설정**에서는 **플랫폼 기본 분기** 및 **수동 분기 제어**를 사용할 수 있습니다. 기본 옵션은 **플랫폼 기본 분기**로 설정되어 있습니다. 슬롯 분기 필드는 **수동 분기 제어**로 설정된 경우 액세스 가능하고 **플랫폼 기본 분기**로 설정된 경우 회색으로 표시됩니다.

직렬 통신

직렬 통신 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **시스템 설정 기본 메뉴** > **시스템 BIOS** > **직렬 통신**을 클릭합니다.

노트: 직렬 포트는 PowerEdge R6525 시스템의 경우 선택 사항입니다. 직렬 통신 옵션은 직렬 COM 포트가 시스템에 설치되어 있는 경우에만 적용됩니다.

표 17. 직렬 통신 세부 정보

옵션	설명
직렬 통신	BIOS에서 직렬 통신 디바이스(직렬 디바이스 1 및 직렬 디바이스 2)를 선택합니다. 또한 BIOS 콘솔 재지정이 활성화될 수 있고 포트 주소를 지정할 수 있습니다. 이 옵션은 기본값으로 **자동**으로 설정됩니다.
직렬 포트 주소	직렬 디바이스의 포트 주소를 설정할 수 있습니다. 기본적으로 이 옵션은 **직렬 디바이스 1=COM2, 직렬 디바이스 2=COM1**로 설정됩니다. **노트:** SOL(Serial Over LAN) 기능으로는 직렬 디바이스 2만 사용할 수 있습니다. SOL을 통한 콘솔 재지정을 사용하려면 콘솔 재지정 및 직렬 디바이스에 대해 동일한 포트 주소를 구성합니다. **노트:** 시스템을 부팅할 때마다 BIOS가 iDRAC에 저장된 직렬 MUX 설정을 동기화합니다. 직렬 MUX 설정은 iDRAC에서 독립적으로 변경할 수 있습니다. BIOS 설정 유틸리티에서 BIOS 기본 설정을 로드해도 직렬 MUX 설정이 직렬 디바이스 1의 기본 설정으로 되돌아가는 것은 아닙니다.
외부 직렬 커넥터	이 옵션으로 외부 직렬 커넥터를 사용해 **직렬 디바이스 1**, **직렬 디바이스 2** 또는 **원격 액세스 디바이스**에 연결할 수 있습니다. 기본적으로 이 옵션은 **직렬 디바이스 1**로 설정되어 있습니다. **노트:** SOL(Serial Over LAN)에는 직렬 디바이스 2만 사용할 수 있습니다. SOL을 통한 콘솔 재지정을 사용하려면 콘솔 재지정 및 직렬 디바이스에 대해 동일한 포트 주소를 구성합니다.

표 17. 직렬 통신 세부 정보 (계속)

옵션	설명
	노트: 시스템이 부팅할 때마다 BIOS는 iDRAC에 저장된 직렬 MUX 설정을 동기화합니다. 직렬 MUX 설정은 iDRAC에서 독립적으로 변경할 수 있습니다. BIOS 설정 유틸리티에서 BIOS 기본 설정을 로드해도 이 설정이 직렬 디바이스 1의 기본 설정으로 되돌아가는 것은 아닙니다.
안전 보드 레이드	콘솔 재지정에 사용되는 안전 보드 레이드를 지정합니다. BIOS에서는 보드 레이드를 자동으로 결정하려고 합니다. 이 시도가 실패한 경우에만 이 안전 보드 레이드가 사용되며, 안전 보드 레이드 값은 변경되지 않아야 합니다. 기본적으로 이 옵션은 **115200**으로 설정됩니다.
원격 터미널 유형	원격 콘솔 터미널 유형을 설정할 수 있습니다. 기본적으로 이 옵션은 **VT100/VT220**으로 설정됩니다.
부팅 후 재지정	운영 체제 로딩 시 BIOS 콘솔 재지정을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.

시스템 프로필 설정

시스템 프로필 설정 화면을 보려면 <F2> 키를 누른 다음 **시스템 설정 기본 화면** > **시스템 BIOS** > **시스템 프로필 설정**을 클릭합니다.

표 18. 시스템 프로필 설정 세부 정보

옵션	설명
시스템 프로필	시스템 암호를 설정할 수 있습니다. **시스템 프로필** 옵션을 사용자 정의 이외의 다른 모드로 설정하는 경우, BIOS가 자동으로 나머지 옵션을 설정합니다. 모드가 **사용자 정의**로 설정된 경우에만 사용자가 나머지 옵션을 변경할 수 있습니다. 기본적으로 이 옵션은 **와트당 성능(OS)**으로 설정됩니다. 기타 옵션에는 **성능** 및 **사용자 지정**이 포함되어 있습니다. **노트: 시스템 프로필** 옵션이 **사용자 정의**로 설정된 경우에만 시스템 프로필 설정 화면에 모든 매개 변수가 표시됩니다.
CPU 전원 관리	CPU 전원 관리를 설정합니다. 이 옵션은 기본값으로 **OS DBPM**으로 설정됩니다. 기타 옵션에는 **최대 성능**이 포함되어 있습니다.
메모리 주파수	시스템 메모리 속도를 설정합니다. **최대 성능** 또는 지정 속도를 선택할 수 있습니다. 기본적으로 이 옵션은 **최고의 성능**으로 설정됩니다.
터보 부스트	프로세서가 터보 부스트 모드에서 작동하거나 작동하지 않도록 설정합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
C 상태	프로세서가 사용 가능한 모든 전원 상태에서 작동하거나 작동하지 않도록 설정합니다. C 상태를 사용하면 프로세서가 유휴 시 저전력 상태로 전환할 수 있습니다. **활성화**(OS 제어) 또는 **자율**(하드웨어 제어가 지원되는 경우)로 설정하면 프로세서가 사용할 수 있는 모든 전원 상태로 작동하여 전력을 절감할 수 있지만, 메모리 지연과 주파수 지터가 늘어날 수도 있습니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
쓰기 데이터 CRC	**활성화**로 설정하면 '쓰기' 작업 중 DDR4 데이터 버스 문제가 감지 및 수정됩니다. 성능에 영향을 미치는 CRC 비트 세대를 위해 2개의 주기가 추가로 필요합니다. 시스템 프로필을 **사용자 정의**으로 설정하지 않는 한 읽기 전용입니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
메모리 패트롤 스크럽	메모리 패트롤 스크럽 모드를 설정합니다. 기본적으로 이 옵션은 **표준**으로 설정됩니다.
메모리 갱신율	1x 또는 2x 중 하나로 메모리 갱신율을 설정합니다. 기본적으로 이 옵션은 **1x**로 설정됩니다.
PCI ASPM L1 링크 전원 관리	PCI Slot ASPM L1 링크를 전원 관리를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **활성화**로 설정됩니다.
결정론 슬라이더	시스템 결정론을 **전원 결정론** 또는 **성능 결정론**으로 설정합니다. 기본적으로 이 옵션은 **전원 결정론**으로 설정되어 있습니다.
효율성 최적화 모드	효율성 최적화 모드는 편의적으로 주파수/전원을 줄여 와트당 성능을 극대화합니다. 효율성 최적화 모드를 활성화하거나 비활성화합니다.

표 18. 시스템 프로필 설정 세부 정보 (계속)

옵션	설명
알고리즘 성능 향상 비활성화 (ApbDis)	알고리즘 성능 향상 비활성화(ApbDis)를 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
DLWM(Dynamic Link Width Management)	링크에서 트래픽이 감지되지 않을 때 x16에서 x8(기본값)까지의 소켓 간 xGMI 링크 너비를 줄입니다. 기본적으로 이 옵션은 **강제 취소**로 설정됩니다.

시스템 보안

System Security 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **System Setup Main Menu** > **System BIOS** > **System Security**를 클릭합니다.

표 19. System Security 세부 정보

옵션	설명
CPU AES-NI	고급 암호화 표준 명령 집합(AES-NI)을 사용해 암호화 및 암호 해독을 수행하여 응용프로그램의 속도를 향상시키며 기본적으로 활성화로 설정됩니다. 이 옵션은 기본적으로 **활성화**로 설정됩니다.
System Password	시스템 암호를 설정합니다. 이 옵션은 기본적으로 **활성화**로 설정되며, 시스템에 암호 점퍼가 설치되어 있지 않은 경우 읽기 전용입니다.
Setup Password	시스템 암호를 설정합니다. 시스템에 암호 점퍼가 설치되지 않은 경우 이 옵션은 읽기 전용입니다.
Password Status	시스템 암호를 잠급니다. 이 옵션은 기본적으로 **잠금 해제**로 설정됩니다.

표 20. TPM 1.2 security 정보

옵션	설명
TPM Security	**노트:** TPM 메뉴는 TPM 모듈이 설치되어 있는 경우에만 사용할 수 있습니다. 시스템의 부팅 모드를 설정할 수 있습니다. 기본적으로 **TPM Security**(TPM 보안) 옵션은 **Off**(끄기)로 설정됩니다. **TPM 상태** 필드가 **사전 부팅 검사를 통해 켜기** 또는 **사전 부팅 검사 없이 켜기**로 설정된 경우에는 TPM 상태 및 TPM 활성화만 수정할 수 있습니다. TPM 1.2가 설치되면 **TPM 보안** 옵션이 **끄기**, **사전 부팅 검사를 통해 켜기** 또는 **사전 부팅 검사 없이 켜기**로 설정됩니다. TPM 2.0이 설치되면 **TPM 보안** 옵션이 **켜기** 또는 **끄기**로 설정됩니다. 이 옵션은 기본적으로 **off(끄기)**로 설정됩니다.
TPM Information	TPM의 작동 상태를 변경합니다. 이 옵션은 기본적으로 **변경 없음**로 설정됩니다.
TPM Firmware	TPM의 펌웨어 버전을 표시합니다.
TPM Status	TPM 상태를 표시합니다.
TPM Command	TPM(Trusted Platform Module)을 설치합니다. 로 설정되면 **None(없음)**, 없음 명령이 TPM로 전송됩니다. 로 설정되면 **Activate(활성화)**, TPM이 활성화되어 있고 활성화된. **Deactivate(비활성화)로 설정하는 경우** TPM이 사용되지 않고 비활성화됩니다. **지우기를 설정하면**, TPM의 모든 내용이 지워집니다. 기본적으로 이 옵션은 **None(없음)**로 설정됩니다.

표 21. TPM 2.0 security 정보

옵션	설명
TPM Information	TPM의 작동 상태를 변경합니다. 이 옵션은 기본적으로 **변경 없음**로 설정됩니다.
TPM Firmware	TPM의 펌웨어 버전을 표시합니다.
TPM Hierarchy	스토리지 및 인증 계층 구조를 활성화 또는 비활성화하거나 지울 수 있습니다. **활성화**로 설정한 경우 스토리지 및 인증 계층 구조를 사용할 수 있습니다. **비활성화**로 설정한 경우 스토리지 및 인증 계층 구조를 사용할 수 없습니다.

표 21. TPM 2.0 security 정보 (계속)

옵션	설명
	지우기로 설정한 경우 스토리지 및 인증 계층 구조에서 모든 값이 지워진 후 **활성화**로 재설정됩니다.
TPM 고급 설정	TPM 고급 설정 세부 정보를 지정합니다.

표 22. System Security 세부 정보

옵션	설명
전원 버튼	시스템 전면에 있는 전원 버튼을 활성화하거나 비활성화합니다. 이 옵션은 기본적으로 **활성화**로 설정됩니다.
AC Power Recovery	시스템의 AC 전원이 복구된 후 시스템이 어떻게 반응할지 설정합니다. 기본적으로 이 옵션은 **Last(마지막)**로 설정됩니다.
AC Power Recovery Delay	AC 전원이 시스템에 복구된 후 시스템 전원을 켤 때 지연되는 시간을 설정합니다. 이 옵션은 기본적으로 **Immediate(즉시)**로 설정됩니다.
사용자 정의 지연(60초~600초)	**AC Power Recovery Delay(AC 전원 복구 지연)**에 대한 **User Defined(사용자 정의)** 옵션이 선택되어 있는 경우 **User Defined Delay(사용자 정의 지연)** 옵션을 설정합니다.
UEFI Variable Access	다양한 수준의 고정 UEFI 변수를 제공합니다. **표준**(기본값)으로 설정하면 UEFI 사양에 따라 운영 체제에서 UEFI 변수에 액세스할 수 있습니다. 로 설정되면 **제어**, 선택한 UEFI 변수가 환경 및 새 UEFI 부팅 항목 내에서 보호되는 강제로 현재 부팅 순서의 끝에 있는 수 있습니다.
Secure Boot	BIOS가 보안 부팅 정책 내의 인증서를 사용하여 각 사전 부팅 이미지를 인증하는 경우 보안 부팅을 활성화합니다. 기본적으로 보안 부팅은 **Disabled**로 설정되어 있습니다.
Secure Boot Policy	보안 부팅 정책이 **Standard**인 경우 BIOS에서 시스템 제조업체의 키 및 인증서를 사용하여 사전 부팅 이미지를 인증할 수 있습니다. 보안 부팅 정책이 **Custom**인 경우 BIOS가 사용자 정의 키 및 인증서를 사용합니다. 기본적으로 보안 부팅 정책은 **Standard**입니다.
Secure Boot Mode	구성 방법을 BIOS 개체(pk, KEK, db, dbx)는 보안 부팅 정책을 사용합니다. 경우 현재 모드가 **배포된 모드로 설정**, 사용 가능한 옵션은 **사용자 모드** 및 **배포된 모드**. 현재 모드가 **사용자 모드에 설정인 경우**, 사용 가능한 옵션은 **사용자 모드**, **모드**, 및 **배포된 모드를 감사**.
Secure Boot Policy Summary	보안 부팅이 인증된 이미지에 사용할 인증서 및 해시 목록을 표시합니다.
Secure Boot Custom Policy Settings	보안 부팅 사용자 지정 정책을 구성합니다. 이 옵션을 활성화하려면 보안 부팅 정책을 **사용자 지정하** 는 옵션을 설정.

표 23. Secure Boot Mode

옵션	설명
User Mode	**사용자 모드**에는 PK가 설치되어 있어야 하고 BIOS는 정책 개체를 업데이트하려는 프로그래밍 방식 시도에 대한 서명 검증을 수행합니다. BIOS 모드 간에 프로그래밍 방식으로 전환을을 인증되지 않을 수 있습니다.
Deployed Mode	**배포된 모드** 가를 가장 모드를 고정시킵니다. **배포된 모드**에는 PK가 설치되어 있어야 하고 BIOS는 정책 개체를 업데이트하려는 프로그래밍 방식 시도에 대한 서명 검증을 수행합니다. **배포된 모드** 프로그래밍 방식으로 모드 전환을 제한합니다.
Audit Mode	**감사 모드에서**,pk가 없습니다. BIOS 모드 간에 프로그래밍 방식으로 업데이트를 정책 개체, 및 전환을 인증되지 않습니다. BIOS는 사전 부팅 이미지를 서명 검증하고 이미지 실행 정보 표에 결과를 기록하지만 이미지가 검증을 통과했는지 실패했는지에 상관없이 이미지를 실행합니다. **감사 모드**는 정책 객체 작동 세트의 프로그래밍 방식 판단에 유용합니다.

시스템 및 설정 암호 생성

전제조건

암호 점퍼가 활성화되어 있는지 확인합니다. 암호 점퍼는 시스템 암호 및 설정 암호 기능을 활성화하거나 비활성화합니다. 자세한 정보는 시스템 보드 점퍼 설정 섹션을 참조하십시오.

노트: 암호 점퍼 설정이 비활성화된 경우 기존 시스템 암호 및 설정 암호가 삭제되고 시스템을 부팅하기 위해 시스템 암호를 제공하지 않아도 됩니다.

단계

1. 시스템 설정을 시작하려면 전원 켜기 또는 시스템을 재시작한 직후에 F2 키를 누릅니다.
2. **System Setup Main Menu(시스템 설정 기본 메뉴)** 화면에서 **System BIOS(시스템 BIOS)** > **System Security(시스템 보안)**을 클릭합니다.
3. **System Security(시스템 보안)** 화면에서 **Password Status(암호 상태)**가 **Unlocked(잠금 해제)**로 설정되었는지 확인합니다.
4. **System Password** 필드에 시스템 암호를 입력한 후 Enter 또는 Tab 키를 누릅니다.
   다음 지침을 따라 시스템 암호를 할당합니다.
   - 암호 길이는 최대 32글자입니다.

   시스템 암호를 다시 입력하라는 메시지가 나타납니다.
5. 시스템 암호를 다시 입력하고 **OK**를 클릭합니다.
6. **Setup Password(암호 설정)** 필드에 설정 암호를 입력한 후 Enter 또는 Tab 키를 누릅니다.
   설정 암호를 다시 입력하라는 메시지가 나타납니다.
7. 설정 암호를 다시 입력하고 **OK(확인)**를 클릭합니다.
8. Esc 키를 눌러 시스템 BIOS(시스템 BIOS) 화면으로 돌아갑니다. Esc 키를 다시 누릅니다.
   변경 내용을 저장하라는 메시지가 표시됩니다.
   노트: 암호 보호 기능은 시스템을 재부팅해야만 적용됩니다.

시스템 암호를 사용하여 시스템 보호

이 작업 정보

설정 암호를 지정하면 시스템 암호 대신 설정 암호를시스템사용할 수 있습니다.

단계

1. 시스템를 켜거나 재부팅합니다.
2. 시스템 암호를 입력하고 Enter를 누릅니다.

다음 단계

Password Status(암호 상태)를 **Locked(잠금)**로 설정한 경우, 재부팅 시 메시지가 나타나면 시스템 암호를 입력하고 Enter를 누릅니다.

노트: 잘못된 시스템 암호를 입력하면 시스템이 암호를 다시 입력하라는 메시지를 표시합니다. 암호를 세 번까지 다시 입력할 수 있습니다. 세 번째 암호 입력에도 실패하면 시스템가 작동을 멈췄고 전원을 꺼야 한다는 오류 메시지가 시스템에 표시됩니다. 시스템를 종료하고 다시 시작해도 올바른 암호를 입력할 때까지 오류 메시지가 계속 표시됩니다.

시스템 및 설정 암호를 삭제 또는 변경

전제조건

노트: **Password Status(암호 상태)**가 **Locked(잠김)**인 경우에는 기존 시스템 암호 또는 설정 암호를 삭제하거나 변경할 수 없습니다.

단계

1. 시스템 설정을 시작하려면 시스템를 켜거나 재시작한 직후에 F2를 누릅니다.
2. **System Setup Main Menu** 화면에서 **System BIOS** > **System Security**를 클릭합니다.
3. **시스템 보안** 화면에서 **암호 상태**가 **잠금 해제**로 설정되었는지 확인합니다.
4. **Setup Password(설정 암호)** 필드에서 기존 시스템 암호를 변경 또는 삭제한 후 Enter 또는 탭을 누릅니다.
5. **설정 암호** 필드에서, 기존 시스템 암호를 변경 또는 삭제한 후 Enter 또는 탭을 누릅니다.
   시스템 및 설정 암호를 변경하면 새 암호를 다시 입력하라는 메시지가 표시됩니다. 시스템 및 설정 암호를 삭제하면 삭제를 확인하는 메시지가 표시됩니다.
6. Esc 키를 눌러 **System BIOS(시스템 BIOS)** 화면으로 돌아갑니다. Esc 키를 다시 누르면 변경 사항을 저장하라는 메시지가 표시됩니다.
7. **Setup Password(설정 암호)**를 선택하고 기존 설정 암호를 변경하거나 삭제한 후 Enter 또는 Tab 키를 누릅니다.
   노트: 시스템 암호 또는 설정 암호를 변경하면 새 암호를 다시 입력하라는 메시지가 표시됩니다. 시스템 또는 설정 암호를 삭제하면 삭제 여부를 확인하는 메시지가 표시됩니다.

활성화된 설정 암호를 사용하여 시스템 운영

Setup Password(설정 암호)를 **Enabled(활성화됨)**로 설정한 경우 시스템 설정 옵션을 수정하기 전에 정확한 설정 암호를 입력합니다.

세 번 이상 잘못된 암호를 입력하면 시스템이 다음과 같은 메시지를 표시합니다.

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted! Must power down.
```

```
Password Invalid. Number of unsuccessful password attempts: <x> Maximum number of password attempts exceeded.System halted.
```

시스템을 종료하고 다시 시작해도 올바른 암호를 입력할 때까지 오류 메시지가 계속 표시됩니다. 다음 옵션은 예외입니다.

- **System Password(시스템 암호)** 설정이 **Enabled(활성화됨)**가 아니고 시스템 암호가 **Password Status(암호 상태)** 옵션을 통해 잠기지 않은 경우에는 시스템 암호를 지정할 수 있습니다. 자세한 내용은 시스템 보안 설정 화면 섹션을 참조하십시오.
- 기존의 시스템 암호는 비활성화하거나 변경할 수 없습니다.

노트: 시스템에서 암호 상태 옵션과 설정 암호 옵션을 함께 사용하면 시스템 암호가 무단으로 변경되지 않도록 방지할 수 있습니다.

이중화 OS 제어

이중화 OS 제어 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **시스템 설정 기본 화면** > **시스템 BIOS** > **이중화 OS 제어**를 클릭합니다.

표 24. 이중화 OS 제어 세부 정보

옵션	설명
이중화 OS 위치	다음 디바이스에서 백업 디스크를 선택할 수 있습니다. • **없음** • **IDSDM** • **AHCI 모드의 SATA 포트** • **BOSS PCIe 카드(내부 M.2 드라이브)** • **내부 USB** **노트:** BIOS에 포함되어 있지 않은 RAID 구성과 NVMe 카드는 이러한 구성에 있는 개별 드라이브를 구별할 수 있는 기능이 없습니다.
이중화 OS 상태	**노트:** **이중화 OS 위치**가 **없음**으로 설정된 경우 이 옵션이 비활성화됩니다. **표시**로 설정되면 백업 디스크가 부팅 목록 및 OS에 표시됩니다. **숨겨짐**으로 설정되면 백업 디스크가 비활성화되고 부팅 목록 및 OS에 표시되지 않습니다. 이 옵션은 기본값으로 **표시**로 설정됩니다.

표 24. 이중화 OS 제어 세부 정보 (계속)

옵션	설명
	노트: BIOS가 하드웨어의 디바이스를 비활성화하므로 OS로 액세스할 수 없습니다.
이중화 OS 부팅	**노트:** **이중화 OS 위치**가 **없음**으로 설정되거나 **이중화 OS 상태**가 **숨김**으로 설정되면 이 옵션이 비활성화됩니다. **활성화**로 설정되면 BIOS가 **이중화 OS 위치**에서 지정된 디바이스로 부팅됩니다. **비활성화**로 설정되면 BIOS가 현재 부팅 목록 설정을 유지합니다. 이 옵션은 기본적으로 **활성화**로 설정됩니다.

기타 설정

기타 설정 화면을 보려면 시스템을 켜고 <F2> 키를 누른 다음 **시스템 설정 기본 메뉴** > **시스템 BIOS** > **기타 설정**을 클릭합니다.

표 25. 기타 설정 세부 정보

옵션	설명
시스템 시간	시스템의 시간을 설정합니다.
시스템 날짜	시스템의 날짜를 설정합니다.
자산 태그	자산 태그를 표시하며, 보안 및 추적 용도로 자산 태그를 수정할 수 있습니다.
키보드 NumLock	시스템 부팅 시 NumLock을 활성화 또는 비활성화할지 설정할 수 있습니다. 기본적으로 이 옵션은 **공칭**으로 설정됩니다. **노트:** 84 키 키보드에는 이 옵션이 적용되지 않습니다.
오류 시 F1/F2 프롬프트	오류 시 F1/F2 프롬프트를 활성화하거나 비활성화합니다. 이 옵션은 기본적으로 **활성화**로 설정됩니다. F1/F2 프롬프트는 키보드 오류 또한 포함합니다.
기존 비디오 옵션 ROM 로드	기존 비디오 옵션 ROM 로드 옵션을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **비활성화**로 설정됩니다.
Dell Wyse P25/P45 BIOS 액세스	Dell Wyse P25/P45 BIOS 액세스를 활성화하거나 비활성화합니다. 이 옵션은 기본적으로 **활성화**로 설정됩니다.
전원 주기 요청	전원 주기 요청을 활성화하거나 비활성화합니다. 기본적으로 이 옵션은 **없음**으로 설정됩니다.

iDRAC 설정 유틸리티

iDRAC 설정 유틸리티는 UEFI를 사용하여 iDRAC 매개변수를 설정하고 구성하는 인터페이스입니다. iDRAC 설정 유틸리티를 사용하여 다양한 iDRAC 매개 변수를 활성화하거나 비활성화할 수 있습니다.

노트: iDRAC 설정 유틸리티의 일부 기능에 액세스하려면 iDRAC Enterprise 라이센스를 업그레이드해야 합니다.

iDRAC 사용에 대한 자세한 정보는 https://www.dell.com/idracmanuals에서 *Dell Integrated Dell Remote Access Controller 사용자 가이드*를 참조하십시오.

장치 설정

Device Settings에서 스토리지 컨트롤러 또는 네트워크 카드와 같은 디바이스 매개변수를 구성할 수 있습니다.

Dell Lifecycle Controller

Dell LC(Lifecycle Controller)는 시스템 배포, 구성, 업데이트, 유지 보수 및 진단을 포함하여 고급 내장형 시스템 관리 기능을 제공합니다. LC는 iDRAC 대역 외 솔루션 및 Dell 시스템 내장형 UEFI(Unified Extensible Firmware Interface) 애플리케이션의 일부로 제공됩니다.

내장형 시스템 관리

Dell Lifecycle Controller는 시스템의 수명주기 전체에 걸쳐 고급 내장형 시스템 관리를 제공합니다. Dell Lifecycle Controller는 부팅 순서 때 시작되며 운영 체제와 독립적으로 작동합니다.

노트: 특정 플랫폼 구성에서는 Lifecycle Controller가 제공하는 일부 기능이 지원되지 않을 수 있습니다.

Dell Lifecycle Controller 설정, 하드웨어 및 펌웨어 구성, 운영 체제 배포 등에 대한 자세한 정보는 https://www.dell.com/idracmanuals 에서 Dell Lifecycle Controller 문서 자료를 참조하십시오.

부팅 관리자

Boot Manager 옵션을 사용하면 부팅 옵션과 진단 유틸리티를 선택할 수 있습니다.

Boot Manager에 들어가려면 시스템을 켜고 <F11> 키를 누릅니다.

표 26. Boot Manager 세부 정보

옵션	설명
일반 부팅 계속	시스템에서는 먼저 부팅 순서의 첫 번째 항목에 해당하는 장치로 부팅을 시도합니다. 부팅 시도가 실패하면 부팅 순서의 다음 항목에 해당하는 장치로 부팅을 계속 시도합니다. 이러한 부팅 시도는 부팅에 성공하거나 시도할 부팅 옵션이 더 이상 없을 때까지 계속됩니다.
일회용 부팅 메뉴	부팅할 일회용 부팅 장치를 선택할 수 있는 부팅 메뉴에 액세스할 수 있습니다.
시스템 설정 시작	시스템 설정에 액세스할 수 있습니다.
출시 주기 컨트롤러	Boot Manager를 종료하고 Dell Lifecycle Controller 프로그램을 호출합니다.
시스템 유틸리티	진단 프로그램 시작, BIOS 업데이트 파일 탐색기, 시스템 재부팅과 같은 System Utilities 메뉴를 시작할 수 있습니다.

PXE 부팅

PXE(Preboot eXecution Environment) 옵션을 사용하여 네트워크에 연결된 시스템을 원격으로 부팅하고 구성할 수 있습니다.

PXE 부팅 옵션에 액세스하려면 시스템을 부팅한 다음 BIOS 설정에서 표준 부팅 순서를 사용하는 대신 POST 중에 <F12>를 누릅니다. 이렇게 하면 메뉴가 당겨지지 않거나 네트워크 디바이스의 관리가 허용됩니다.