

Dell EMC PowerEdge T350

Referenzhandbuch für BIOS und UEFI

Hinweise, Vorsichtshinweise und Warnungen

 **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

 **VORSICHT:** Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

 **WARNUNG:** Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Kapitel 1: Vor-Betriebssystem-Verwaltungsanwendungen.....	4
System-Setup-Programm.....	4
System-BIOS.....	5
iDRAC Settings.....	20
Device Settings (Geräteeinstellungen).....	20
Service Tag Settings.....	20
Dell Lifecycle Controller.....	20
Integrierte Systemverwaltung.....	20
Start-Manager.....	21
PXE-Boot.....	21

Vor-Betriebssystem-Verwaltungsanwendungen

Sie können grundlegende Einstellungen und Funktionen des Systems ohne Starten des Betriebssystems mithilfe der System-Firmware verwalten.

Optionen zum Verwalten der Vor-Betriebssystemanwendungen

Sie können eine der folgenden Optionen verwenden, um die Vor-Betriebssystemanwendungen zu verwalten:

- System-Setup-Programm
- Dell Lifecycle Controller
- Start-Manager
- Vorstartausführungsumgebung (Preboot eXecution Environment, PXE)

Themen:

- [System-Setup-Programm](#)
- [Dell Lifecycle Controller](#)
- [Start-Manager](#)
- [PXE-Boot](#)

System-Setup-Programm

Über die Option **System Setup** können Sie die BIOS-Einstellungen, die iDRAC-Einstellungen und die Geräteeinstellungen des Systems konfigurieren.

Sie können über eine der folgenden Schnittstellen auf das System-Setup zugreifen:

- Grafische Benutzeroberfläche: Um auf das iDRAC-Dashboard zuzugreifen, klicken Sie auf **Konfiguration > BIOS-Einstellungen**.
- Textbrowser: Um den Textbrowser zu aktivieren, verwenden Sie die Konsolenumleitung.

Um **System Setup** aufzurufen, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **System Setup Main Menu**.

i ANMERKUNG: Wenn der Ladevorgang des Betriebssystems beginnt, bevor Sie F2 gedrückt haben, lassen Sie das System den Startvorgang vollständig ausführen. Starten Sie dann das System neu und versuchen Sie es erneut.

Die Optionen im Bildschirm **System-Setup-Hauptmenü** werden in der folgenden Tabelle beschrieben:

Tabelle 1. System-Setup-Hauptmenü

Option	Beschreibung
System-BIOS	Ermöglicht Ihnen die Konfiguration der BIOS-Einstellungen.
iDRAC Settings	Ermöglicht Ihnen die Konfiguration der iDRAC-Einstellungen. Das Dienstprogramm für iDRAC-Einstellungen ist eine Oberfläche für das Einrichten und Konfigurieren der iDRAC-Parameter unter Verwendung von UEFI (Unified Extensible Firmware Interface (Vereinheitlichte erweiterbare Firmware-Schnittstelle)). Mit dem Dienstprogramm für iDRAC-Einstellungen können verschiedene iDRAC-Parameter aktiviert oder deaktiviert werden. Weitere Informationen zur Verwendung dieses Dienstprogramms finden


Tabelle 1. System-Setup-Hauptmenü (fortgesetzt)

Option	Beschreibung
	Sie im <i>Benutzerhandbuch für Integrated Dell Remote Access Controller</i> unter www.dell.com/poweredge manuals .
Device Settings (Geräteeinstellungen)	Ermöglicht Ihnen die Konfiguration von Geräteeinstellungen für Geräte wie Speicher-Controller oder Netzwerkkarten.
Service Tag Settings	Ermöglicht die Konfiguration des Service-Tag des Systems.

System-BIOS

Um den Bildschirm **System BIOS** anzuzeigen, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **System Setup Main Menu > System BIOS**.

Tabelle 2. Details zu System BIOS

Option	Beschreibung
Systeminformationen	Gibt Informationen zum System an, wie den Namen des Systemmodells, die BIOS-Version und die Service-Tag-Nummer.
Speichereinstellungen	Gibt Informationen und Optionen zum installierten Arbeitsspeicher an.
Prozessoreinstellungen	Gibt Informationen und Optionen zum Prozessor an, wie Taktrate und Cachegröße.
SATA-Einstellungen	Gibt Optionen an, mit denen der integrierte SATA-Controller und die zugehörigen Ports aktiviert oder deaktiviert werden können.
Boot Settings (Starteinstellungen)	Zeigt Optionen an, mit denen der Startmodus (UEFI) festgelegt wird. Ermöglicht es Ihnen, UEFI-Starteinstellungen zu ändern.
Netzwerkeinstellungen	Legt die Optionen zum Verwalten der UEFI Network Settings (Netzwerkeinstellungen) und Boot Protokolle. Legacy-Netzwerkeinstellungen verwaltet werden über das Menü Device Settings (Geräteeinstellungen) verwaltet.  ANMERKUNG: Die Netzwerkeinstellungen werden im BIOS-Startmodus nicht unterstützt.
Integrierte Geräte	Gibt Optionen zur Verwaltung der Controller und Ports von integrierten Geräten an und legt die dazugehörigen Funktionen und Optionen fest.
Serielle Kommunikation	Gibt Optionen zur Verwaltung der seriellen Schnittstellen an und legt die dazugehörigen Funktionen und Optionen fest.
Systemprofileinstellungen	Gibt Optionen an, mit denen die Einstellungen für die Energieverwaltung des Prozessors, die Speichertaktrate usw. geändert werden können.
Systemsicherheit	Gibt Optionen zur Konfiguration der Sicherheitseinstellungen des System wie Systemkennwort, Setup-Kennwort und Sicherheit des Trusted Platform Module (TPM) und UEFI Secure Boot an. Drücken Sie den Netzschalter des System.
Redundante Betriebssystemsteuerung	Legt die Informationen des redundanten Betriebssystems für die Steuerung des redundanten Betriebssystems fest.
Verschiedene Einstellungen	Gibt Optionen an, mit denen das Systemdatum, die Uhrzeit usw. geändert werden können.

Systeminformationen

Um den Bildschirm **Systeminformationen** anzuzeigen, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **System-Setup-Hauptmenü > System-BIOS > Systeminformationen**.

Tabelle 3. Systeminformationen – Details

Option	Beschreibung
System Model Name (Name des Systemmodells)	Gibt den Namen des Systemmodells an.
System BIOS Version (BIOS-Version des Systems)	Gibt die auf dem System installierte BIOS-Version an.
System Management Engine-Version (Verwaltungs-Engine-Version des Systems)	Gibt die aktuelle Version der Management Engine-Firmware an.
System Service Tag (Service-Tag-Nummer des Systems)	Gibt die Service-Tag-Nummer des Systems an.
System Manufacturer (Systemhersteller)	Gibt den Namen des Systemherstellers an.
System Manufacturer Contact Information (Kontaktinformationen des Systemherstellers)	Gibt die Kontaktinformationen des Systemherstellers an.
System CPLD Version (CPLD-Version des Systems)	Gibt die aktuelle Systemversion der Firmware des komplexen, programmierbaren Logikgeräts (CPLD-Firmware) an.
UEFI Compliance Version (UEFI-Compliance-Version)	Gibt die UEFI-Compliance-Stufe der System-Firmware an.

Speichereinstellungen

Um den Bildschirm **Speichereinstellungen** anzuzeigen, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **Hauptmenü des System-Setups > System-BIOS > Speichereinstellungen**.

Tabelle 4. Details zu Speichereinstellungen

Option	Beschreibung
System Memory Size	Gibt die Größe des Systemspeichers an.
System Memory Type	Gibt den Typ des im System installierten Hauptspeichers an.
System Memory Speed	Gibt die Geschwindigkeit des Systemspeichers an.
System Memory Voltage	Gibt die Spannung des Systemspeichers an.
Video Memory	Gibt die Größe des Videospeichers an.
System Memory Testing	Gibt an, ob während des Systemstarts Systemspeichertests ausgeführt werden. Die zwei verfügbaren Optionen sind Aktiviert und Deaktiviert . Diese Option ist standardmäßig auf Disabled festgelegt.
Memory Operating Mode	Gibt den Speicherbetriebsmodus an. Diese Option ist verfügbar und standardmäßig auf Optimierungsmodus eingestellt.
Current State of Memory Operating Mode	Gibt den aktuellen Zustand des Speicherbetriebsmodus an.
Arbeitsspeichertraining	<p>Wenn die Option auf Schnell festgelegt ist und die Speicherkonfiguration nicht geändert wird, verwendet das System zuvor gespeicherte Speicher-Trainingsparameter zum Training der Speichersubsysteme und die Systemstartzeit wird reduziert. Wenn die Speicherkonfiguration geändert wird, aktiviert das System automatisch Beim nächsten Start neu trainieren, um die Schritte zum einmaligen vollständigen Speichertraining zu erzwingen. Anschließend wird wieder Schnell eingestellt.</p> <p>Wenn die Option auf Beim nächsten Start neu trainieren festgelegt ist, führt das System beim nächsten Einschalten die Schritte zum einmaligen vollständigen Speichertraining aus und die Startzeit wird beim nächsten Start verzögert.</p> <p>Wenn die Option auf Aktiviert gesetzt ist, führt das System bei jedem Einschalten die erzwungenen Schritte zum vollständigen Speichertraining durch und die Startzeit wird bei jedem Neustart verzögert.</p>

Tabelle 4. Details zu Speichereinstellungen (fortgesetzt)

Option	Beschreibung
Korrigierbare Fehlerprotokollierung	Aktiviert oder deaktiviert korrigierbare Fehlerprotokollierung. Diese Option ist standardmäßig auf Enabled festgelegt.

Prozessoreinstellungen

Um den Bildschirm **Prozessoreinstellungen** anzuzeigen, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **Hauptmenü des System-Setups > System-BIOS > Prozessoreinstellungen**.

Tabelle 5. Details zu Prozessoreinstellungen

Option	Beschreibung
Logischer Prozessor	Jeder Prozessorkern unterstützt bis zu zwei logische Prozessoren. Wenn die Option Logical Processor (Logischer Prozessor) auf Enabled (Aktiviert) gesetzt ist, zeigt das BIOS alle logischen Prozessoren an. Wenn die Option auf Disabled (Deaktiviert) gesetzt ist, zeigt das BIOS pro Kern nur einen Prozessor an. Diese Option ist standardmäßig auf Enabled festgelegt.
Virtualisierungstechnologie	Aktiviert oder deaktiviert die Virtualization Technology für den Prozessor. Diese Option ist standardmäßig festgelegt auf Standardmäßig Aktiviert .
Nachbarspeicher Zeilen-Prefetch	Ermöglicht das Optimieren des Systems für Anwendungen, bei denen eine starke Nutzung des sequenziellen Speicherzugriffs benötigt wird. Diese Option ist standardmäßig auf Enabled festgelegt. Für Anwendungen, bei denen eine starke Nutzung des wahlfreien Speicherzugriffs benötigt wird, kann diese Option deaktiviert werden.
Hardware-Vorabruf	Aktiviert oder deaktiviert den Hardware-Vorabruf. Diese Option ist standardmäßig auf Enabled festgelegt.
LLC-Prefetch	Aktiviert oder deaktiviert den LLC-Prefetch auf allen Threads. Diese Option ist standardmäßig auf Enabled festgelegt.
Deadline LLC Verteilung	Aktiviert oder deaktiviert die Deadline LLC-Verteilung. Diese Option ist standardmäßig auf Enabled festgelegt. Sie können diese Option aktivieren, um die Deadlines in LLC anzugeben, oder deaktivieren Sie die Option, um keine Deadlines in LLC anzugeben.
Verzeichnis-AtoS	Aktiviert oder deaktiviert Verzeichnis-AtoS. Die AtoS-Optimierung reduziert die Remote-Latenzzeit für wiederholte Lesezugriffe, ohne in die Aufzeichnung einzugreifen. Diese Option ist standardmäßig auf Disabled festgelegt.
x2APIC-Modus	Aktivieren oder Deaktivieren des x2APIC-Modus. Diese Option ist standardmäßig auf Enabled festgelegt. i ANMERKUNG: Bei einer Konfiguration mit zwei Prozessoren und 64 Cores ist der x2APIC-Modus nicht umschaltbar, wenn 256 Threads aktiviert sind (BIOS-Einstellungen: Alle CCD, Cores und logischen Prozessoren aktiviert).
Anzahl der Kerne pro Prozessor	In der Standardeinstellung ist diese Option auf All (Alle).
Prozessorkern-Taktrate	Gibt die maximale Taktrate der Prozessorkerne an.

Tabelle 6. Prozessordetails

Option	Beschreibung
Family-Model-Stepping	Gibt Reihe, Modell und Steppingwert des Prozessors gemäß der Definition von Intel an.


Tabelle 6. Prozessordetails (fortgesetzt)

Option	Beschreibung
Marke	Gibt den Markennamen an.
Level 2 Cache (Level 2-Cache)	Gibt die Gesamtgröße des L2-Caches an.
Level 3 Cache (Level 3-Cache)	Gibt die Gesamtgröße des L3-Caches an.
Mikrocode	Legt die Version des Prozessor-Microcodes fest.

SATA-Einstellungen

Um den Bildschirm **SATA-Einstellungen** anzuzeigen, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **System-BIOS > SATA-Einstellungen**.

Tabelle 7. SATA-Einstellungen – Details

Option	Beschreibung								
Embedded SATA	Ermöglicht das Einstellen der integrierten SATA-Option auf den Modus Aus , AHCI-Modus oder RAID-Modus . Diese Option ist standardmäßig auf AHCI Mode (AHCI-Modus) eingestellt.  ANMERKUNG: 1. Es gibt keine ESXi- und Ubuntu-Unterstützung im RAID-Modus.								
Security Freeze Lock	Sendet während des POST einen Absturzsperren -Befehl an die integrierten SATA-Laufwerke. Diese Option gilt nur für den Modus AHCI. Diese Option ist standardmäßig auf Enabled festgelegt.								
Write Cache	Aktiviert oder deaktiviert den Befehl für integrierte SATA-Laufwerke während des POST-Tests. Diese Option ist standardmäßig auf Disabled festgelegt.								
Port n	Legt den Laufwerkstyp des ausgewählten Geräts fest. Für die Modi AHCI und RAID ist die BIOS-Unterstützung immer aktiviert. Tabelle 8. Port n <table border="1" data-bbox="544 1258 1481 1590"> <thead> <tr> <th>Optionen</th> <th>Beschreibungen</th> </tr> </thead> <tbody> <tr> <td>Modell</td> <td>Gibt das Laufwerksmodell des ausgewählten Geräts an.</td> </tr> <tr> <td>Laufwerkstyp</td> <td>Gibt den Typ des Laufwerks an, das am SATA-Anschluss angeschlossen ist.</td> </tr> <tr> <td>Kapazität</td> <td>Gibt die Gesamtkapazität des Laufwerks an. Für Geräte mit Wechselmedien, wie z. B. für optische Laufwerke, ist dieses Feld nicht definiert.</td> </tr> </tbody> </table>	Optionen	Beschreibungen	Modell	Gibt das Laufwerksmodell des ausgewählten Geräts an.	Laufwerkstyp	Gibt den Typ des Laufwerks an, das am SATA-Anschluss angeschlossen ist.	Kapazität	Gibt die Gesamtkapazität des Laufwerks an. Für Geräte mit Wechselmedien, wie z. B. für optische Laufwerke, ist dieses Feld nicht definiert.
Optionen	Beschreibungen								
Modell	Gibt das Laufwerksmodell des ausgewählten Geräts an.								
Laufwerkstyp	Gibt den Typ des Laufwerks an, das am SATA-Anschluss angeschlossen ist.								
Kapazität	Gibt die Gesamtkapazität des Laufwerks an. Für Geräte mit Wechselmedien, wie z. B. für optische Laufwerke, ist dieses Feld nicht definiert.								

Boot Settings (Starteinstellungen)

Die **Starteinstellungen** unterstützen nur den **UEFI**-Modus.

- **UEFI:** Das „Unified Extensible Firmware Interface (UEFI)“ (Vereinheitlichte erweiterbare Firmware-Schnittstelle) ist eine neue Schnittstelle zwischen Betriebssystem und Plattform-Firmware. Die Schnittstelle besteht aus Datentabellen mit auf die Plattform bezogenen Informationen sowie Serviceabrufen zu Start- und Laufzeit, die dem Betriebssystem und seinem Loader zur Verfügung stehen. Die folgenden Vorzüge sind verfügbar, wenn der **Boot Mode** (Startmodus) auf **UEFI** gesetzt ist:
 - Unterstützung für Laufwerkpartitionen mit mehr als 2 TB.
 - Erweiterte Sicherheit (z. B. „UEFI Secure Boot“ (Sicherer UEFI-Start)).
 - Kürzere Startzeit.

Schalten Sie zum Anzeigen des Bildschirms **Boot Settings** das System ein, drücken Sie F2 und klicken Sie auf **System BIOS > Boot Settings**.

Tabelle 9. Details zu Boot Settings


Option	Beschreibung
Boot Sequence Retry	Aktiviert oder deaktiviert die Funktion zur Wiederholung der Startreihenfolge oder setzt das System zurück. Wenn diese Option auf Aktiviert gesetzt ist, versucht das System bei einem fehlgeschlagenen Startversuch nach 30 Sekunden die Startreihenfolge erneut. Wenn diese Option auf Zurücksetzen gesetzt ist, wird das System nach einem fehlgeschlagenen Startversuch sofort neu gestartet. Diese Option ist standardmäßig auf Enabled festgelegt.
Generic USB Boot	Aktiviert oder deaktiviert den generischen USB-Start-Platzhalter. Diese Option ist standardmäßig auf Disabled festgelegt.
Hard-disk Drive Placeholder	Aktiviert bzw. deaktiviert den Festplattenplatzhalter. Diese Option ist standardmäßig auf Disabled festgelegt.
Clean all Sysprep order and variables	Wenn die Option auf Keine festgelegt ist, führt das BIOS keine Aktion durch. Wenn die Option auf Yes festgelegt ist, löscht das BIOS die Variablen von Sysprep #### und SysPrepOrder. Diese Option ist eine einmalige Option, sie wird beim Löschen von Variablen auf None zurückgesetzt. Diese Einstellungen stehen nur im UEFI-Startmodus zur Verfügung. In der Standardeinstellung ist diese Option auf None (Keine).
UEFI-Starteinstellungen	Gibt die UEFI-Startreihenfolge an. Aktiviert oder deaktiviert UEFI-Startoptionen.  ANMERKUNG: Über diese Option wird die UEFI-Startreihenfolge gesteuert. Die erste Option in der Liste wird zuerst versucht.

Tabelle 10. UEFI-Starteinstellungen

Option	Beschreibung
UEFI-Startsequenz	Ermöglicht Ihnen die Änderung der Reihenfolge der Startgeräte.
Startoptionen aktivieren/deaktivieren	Diese Funktion ermöglicht Ihnen die Auswahl der aktivierten oder deaktivierten Startgeräte.

Ändern der Startreihenfolge

Info über diese Aufgabe

Möglicherweise müssen Sie die Startreihenfolge ändern, wenn Sie von einem USB-Schlüssel oder einem optischen Laufwerk aus den Startvorgang durchführen möchten.

Schritte

1. Klicken Sie im Bildschirm **System Setup Main Menu** (System-Setup-Hauptmenü) auf **System BIOS > Boot Settings > UEFI Boot Settings > UEFI Boot Sequence** („System-BIOS“ > „Starteinstellungen“ > „Starteinstellungen für UEFI“ > „Startreihenfolge für UEFI“).
2. Wählen Sie mit den Pfeiltasten ein Startgerät aus und verwenden Sie die Tasten mit dem Plus- und Minuszeichen („+“ und „-“), um das Gerät in der Reihenfolge nach unten oder nach oben zu verschieben.
3. Klicken Sie auf **Exit** (Beenden) und auf **Yes** (Ja), um die Einstellungen beim Beenden zu speichern.

 **ANMERKUNG:** Sie können Geräte in der Startreihenfolge nach Bedarf auch aktivieren oder deaktivieren.

Netzwerkeinstellungen

Schalten Sie zum Anzeigen des Bildschirms **Network Settings** das System ein, drücken Sie F2 und klicken Sie auf **System Setup Main Menu > System BIOS > Network Settings**.


 **ANMERKUNG:** Die Netzwerkeinstellungen werden im BIOS-Startmodus nicht unterstützt.

Tabelle 11. Details zu Network Settings

Option	Beschreibung
UEFI PXE Settings (UEFI-PXE-Einstellungen)	Ermöglicht die Steuerung der UEFI PXE-Gerätekonfiguration.
PXE Device n (n = 1 bis 4)	Aktiviert oder deaktiviert das Gerät. Wenn diese Option aktiviert ist, wird eine UEFI-PXE-Startoption für das Gerät erstellt.
PXE Device n Settings (n = 1 bis 4)	Ermöglicht die Steuerung der PXE-Gerätekonfiguration.
UEFI HTTP Settings (UEFI-HTTP-Einstellungen)	Ermöglicht die Steuerung der UEFI HTTP-Gerätekonfiguration.
HTTP Device n (HTTP-Gerät n) (n = 1 bis 4)	Aktiviert oder deaktiviert das Gerät. Wenn diese Option auf aktiviert ist, wird eine UEFI-HTTP-Startoption für das Gerät erstellt.
HTTP Device n Settings (n = 1 bis 4)	Ermöglicht die Steuerung der HTTP-Gerätekonfiguration.
UEFI-iSCSI-Einstellungen	Ermöglicht die Steuerung der iSCSI-Gerätekonfiguration.

Tabelle 12. Details zu PXE Device n Settings

Option	Beschreibung
Schnittstelle	Gibt die für das PXE-Gerät verwendete NIC-Schnittstelle an.
Protokoll	Gibt das Protokoll an, das für das PXE-Gerät verwendet wird. Diese Option ist auf IPv4 oder IPv6 eingestellt. In der Standardeinstellung ist diese Option auf IPv4 .
VLAN	Aktiviert VLAN für das PXE-Gerät. Diese Option ist standardmäßig auf Enable (Aktivieren) oder Disable (Deaktivieren) eingestellt. Diese Option ist standardmäßig auf Deaktivieren festgelegt.
VLAN-ID	Zeigt die VLAN-ID für das PXE-Gerät.
VLAN-Priorität	Zeigt die VLAN-Priorität für das PXE-Gerät.

Tabelle 13. Details zum Bildschirm UEFI iSCSI Settings

Option	Beschreibung
iSCSI-Initiator-Name	Legt den Namen des iSCSI-Initiators im IQN-Format fest.
iSCSI Device 1	Aktiviert oder deaktiviert das iSCSI-Gerät. Wenn diese Option deaktiviert ist, wird eine UEFI-Startoption für das iSCSI-Gerät automatisch erstellt. Diese Option ist standardmäßig auf Disabled (Deaktiviert) eingestellt.
iSCSI Device 1 Settings	Ermöglicht die Steuerung der iSCSI-Gerätekonfiguration.

Tabelle 14. Details zum Bildschirm iSCSI Device1 Settings

Option	Beschreibung
Verbindung 1	Aktiviert oder deaktiviert die iSCSI-Verbindung. Diese Option ist standardmäßig auf Deaktivieren festgelegt.
Verbindung 2	Aktiviert oder deaktiviert die iSCSI-Verbindung. Diese Option ist standardmäßig auf Deaktivieren festgelegt.
Einstellungen für Verbindung 1	Ermöglicht die Steuerung der Konfiguration der iSCSI-Verbindung.
Einstellungen für Verbindung 2	Ermöglicht die Steuerung der Konfiguration der iSCSI-Verbindung.
Reihenfolge der Verbindung	Ermöglicht das Festlegen der Reihenfolge der Verbindungsversuche für die iSCSI-Verbindungen.

Integrierte Geräte

Wenn Sie den Bildschirm **Integrierte Geräte** anzeigen möchten, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **Hauptmenü des System-Setups > System-BIOS > Integrierte Geräte**.

Tabelle 15. Details zu Integrierte Geräte

Option	Beschreibung
User Accessible USB Ports	<p>Legt die benutzerzugängliche USB-Schnittstellen fest. Durch die Auswahl der Option Nur hintere Anschlüsse aktiviert werden die vorderen USB-Anschlüsse deaktiviert und durch die Auswahl von Alle Anschlüsse deaktiviert werden sowohl die vorderen als auch die hinteren USB-Anschlüsse deaktiviert. -Vorgangs deaktiviert. Durch -Vorgangs deaktiviert. Diese Option ist standardmäßig auf Alle Ports aktiviert festgelegt.</p> <p>Je nach Auswahl funktionieren während des Startprozesses USB-Tastatur und -Maus an bestimmten USB-Schnittstellen. Nachdem der Betriebssystemtreiber geladen ist, sind die USB-Schnittstellen entsprechend der Einstellung dieses Feld aktiviert oder deaktiviert.</p>
Internal USB Port	<p>Aktiviert oder deaktiviert die interne USB-Schnittstelle. Diese Option ist auf On (An) oder Off (Aus) eingestellt. Diese Option ist standardmäßig auf On (Aktiviert) eingestellt.</p> <p>i ANMERKUNG: Der interne USB-Anschluss gilt nur für T150, da die Hardware von T350/R350/R250 ihn nicht unterstützt.</p>
iDRAC Direct USB Port	<p>Der iDRAC Direct-USB-Anschluss wird ausschließlich von iDRAC verwaltet und ist für den Host nicht sichtbar. Diese Option ist auf ON (An) oder OFF (Aus) eingestellt. Wenn OFF (Deaktiviert) eingestellt ist, erkennt iDRAC keine in diesem verwalteten Anschluss installierte USB-Geräte. Diese Option ist standardmäßig auf On (Aktiviert) eingestellt.</p>
Integrierte NIC1 und NIC2	<p>Aktivierung bzw. Deaktivierung der integrierten NIC1- und NIC2-Karten. Wenn die Einstellung auf Disabled (OS) (Deaktiviert (OS)) gesetzt ist, wird der NIC möglicherweise immer noch für freigegebenen Netzwerkzugriff durch den integrierten Management-Controller zur Verfügung stehen. Konfigurieren Sie die Integrierte NIC1- und NIC2-Optionen mithilfe der NIC-Verwaltungsprogramme auf dem Gerät. Diese Option ist standardmäßig auf Enabled festgelegt.</p>
I/OAT DMA Engine	<p>Aktiviert oder deaktiviert die I/O Acceleration Technology (I/OAT, Technologie zur Beschleunigung der Ein-/Ausgabeaktivität). I/OAT ist ein Satz von DMA-Funktionen zur Beschleunigung Netzwerkverkehr und geringerer CPU-Auslastung. Aktivieren Sie die Option nur, wenn Hardware und Software diese Funktion unterstützen. Diese Option ist standardmäßig auf Disabled festgelegt.</p>
Embedded Video Controller	<p>Aktiviert oder deaktiviert die Verwendung des integrierten Video-Controllers als primäre Anzeige. Bei der Einstellung Enabled (Aktiviert) fungiert der integrierte Video-Controller als primäre Anzeige, selbst wenn Add-In-Grafikkarten installiert sind. Bei der Einstellung Deaktiviert wird eine Add-in-Grafikkarte als primäre Anzeige verwendet. BIOS gibt während des Einschalt-Selbsttests (POST) und in der Umgebung vor dem Startvorgang sowohl für das primären Add-in-Video als auch für das integrierten Video Anzeigen aus. Das integrierte Video wird anschließend deaktiviert, direkt bevor das Betriebssystem gestartet wird. Diese Option ist standardmäßig auf Enabled festgelegt.</p> <p>i ANMERKUNG: Wenn mehrere Add-In-Grafikkarten im System installiert sind, wird die erste während der PCI-Nummerierung erkannte Karte als das primäres Video ausgewählt. Möglicherweise müssen Neuordnung der Karten in den Steckplätzen vorgenommen werden, um zu steuern, welche Karte das primäre Video ist.</p>
Current State of Embedded Video Controller	<p>Zeigt den aktuellen Status des eingebetteten Video-Controllers an. Der Current State of Embedded Video Controller (Aktueller Status des integrierten Video-Controllers) ist ein schreibgeschütztes Feld. Wenn der integrierte Video-Controller das einzige Anzeigegerät im System ist (d. h., wenn keine Add-in-Grafikkarte installiert ist), wird der integrierte Video-Controller automatisch als primäres Anzeigegerät verwenden. Das gilt auch, wenn die Einstellung Embedded Video Controller (Integrierter Video-Controller) auf Disabled (Deaktiviert) gesetzt ist.</p>
OS Watchdog Timer	<p>Wenn Ihr System nicht mehr reagiert, unterstützt Sie der Watchdog-Zeitgeber bei der Wiederherstellung des Betriebssystems. Wenn diese Option auf Enabled</p>

Tabelle 15. Details zu Integrierte Geräte (fortgesetzt)

Option	Beschreibung
	(Aktiviert) gestellt ist, initialisiert das Betriebssystem den Zeitgeber. Wenn diese Option auf Disabled (Deaktiviert), d.h. auf die Standardeinstellung, gesetzt ist, hat der Zeitgeber keine Auswirkungen auf das System.
Empty Slot Unhide (Leere Steckplätze einblenden)	Aktiviert oder deaktiviert die Root-Ports aller leeren Steckplätze, die für das BIOS und das Betriebssystem zugänglich sind. Diese Option ist standardmäßig auf Disabled festgelegt.
Speicher ordnete E/A über 4GB zu	Aktiviert oder deaktiviert die Unterstützung für PCIe-Geräte, die große Speichermengen erfordern. Aktivieren Sie diese Option nur für 64-Bit-Betriebssysteme bestimmt. Diese Option ist standardmäßig auf Aktiviert eingestellt.
Slot Disablement (Steckplatzdeaktivierung)	Aktiviert oder deaktiviert verfügbare PCIe-Steckplätze auf dem System. Die Funktion „Slot Disablement“ (Steckplatzdeaktivierung) steuert die Konfiguration der PCIe-Karten, die im angegebenen Steckplatz installiert sind. Steckplätze dürfen nur dann deaktiviert werden, wenn die installierte Peripheriegeräte-Karte das Starten des Betriebssystems verhindert oder Verzögerungen beim Gerätestart verursacht. Wenn der Steckplatz deaktiviert ist, sind sowohl die Option „ROM Driver“ (ROM-Treiber) als auch die Option „UEFI Driver“ (UEFI-Treiber) deaktiviert. Es können nur die Steckplätze gesteuert werden, die im System vorhanden sind.

Serielle Kommunikation

Wenn Sie den Bildschirm **Serielle Kommunikation** anzeigen möchten, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **Hauptmenü des System-Setups > System-BIOS > Serielle Kommunikation**.

Tabelle 16. Details zu Serielle Kommunikation

Option	Beschreibung
Serielle Kommunikation	Aktiviert die Optionen für serielle Kommunikation. Dient der Auswahl serieller Kommunikationsgeräte (Seriellles Gerät 1 und Seriellles Gerät 2) im BIOS. BIOS-Konsolenumleitung kann auch aktiviert werden, und die verwendete Portadresse lässt sich festlegen.
Serial Port Address	Ermöglicht das Festlegen der Anschlussadresse für serielle Geräte. Diese Option ist standardmäßig auf Seriellles Gerät1=COM2, Seriellles Gerät 2=COM1 eingestellt. <i>i</i> ANMERKUNG: Sie können für die SOL-(Seriell über LAN-)Funktion nur Serial Device 2 (Seriellles Gerät 2) verwenden. Um die Konsolenumleitung über SOL nutzen zu können, konfigurieren Sie für die Konsolenumleitung und das serielle Gerät dieselbe Anschlussadresse. <i>i</i> ANMERKUNG: Jedes Mal, wenn das System gestartet wird, synchronisiert das BIOS die im iDRAC gespeicherte serielle MUX-Einstellung. Die serielle MUX-Einstellung kann unabhängig in iDRAC geändert werden. Aus diesem Grund wird diese Einstellung beim Laden der BIOS-Standardeinstellungen aus dem BIOS-Setup-Dienstprogramm möglicherweise nicht immer auf die MUX-Einstellung von "Serial Device 1" (Seriellles Gerät 1) zurückgesetzt.
External Serial Connector	Mit dieser Option können Sie den externen seriellen Anschluss mit dem seriellen Gerät 1 , dem seriellen Gerät 2 oder dem Remote-Zugriffsgerät verknüpfen. Diese Option ist standardmäßig auf Serial Device 1 (Seriellles Gerät 1) eingestellt. <i>i</i> ANMERKUNG: Nur "Serial Device 2" (Seriellles Gerät 2) kann für "Serial over LAN (SOL)" (seriell über LAN) genutzt werden. Um die Konsolenumleitung über SOL nutzen zu können, konfigurieren Sie für die Konsolenumleitung und das serielle Gerät dieselbe Anschlussadresse. <i>i</i> ANMERKUNG: Jedes Mal, wenn das System gestartet wird, synchronisiert das BIOS die in iDRAC gespeicherte serielle MUX-Einstellung. Die serielle MUX-Einstellung kann unabhängig in iDRAC geändert werden. Aus diesem Grund wird diese Einstellung beim Laden der BIOS-Standardeinstellungen aus dem BIOS-

Tabelle 16. Details zu Serielle Kommunikation (fortgesetzt)

Option	Beschreibung
	Setup-Dienstprogramm möglicherweise nicht immer auf die Standardeinstellung von "Serial Device 1" (serielles Gerät 1) zurückgesetzt.
Failsafe Baud Rate	Zeigt die ausfallsichere Baudrate für die Konsolenumleitung an. Das BIOS versucht, die Baudrate automatisch zu bestimmen. Diese ausfallsichere Baudrate wird nur verwendet, wenn der Versuch fehlschlägt, und der Wert darf nicht geändert werden. Diese Option ist standardmäßig auf 115200 eingestellt.
Remote Terminal Type	Legt den Terminaltyp für die Remote-Konsole fest. Diese Option ist standardmäßig als VT100/VT220 eingestellt.
Redirection After Reboot	Ermöglicht das Aktivieren oder Deaktivieren der BIOS-Konsolenumleitung, wenn das Betriebssystem geladen wird. Diese Option ist standardmäßig auf Enabled festgelegt.

Systemprofileinstellungen

Um den Bildschirm **Systemprofileinstellungen** anzuzeigen, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **System-Setup-Hauptmenü > System-BIOS > Systemprofileinstellungen**.

Tabelle 17. Systemprofileinstellungen – Details


Option	Beschreibung
System Profile	Richtet das Systemprofil ein. Wenn die Option Systemprofil auf einen anderen Modus als Custom (Benutzerdefiniert) gesetzt wird, legt das BIOS automatisch die restlichen Optionen fest. Um die restlichen Optionen ändern zu können, muss der Modus auf Custom (Benutzerdefiniert) gesetzt werden. Diese Option ist standardmäßig auf Performance Per Watt (OS) (Leistung pro Watt (Betriebssystem)) eingestellt. Weitere Optionen sind Performance (Leistung) und Custom (Benutzerdefiniert).  ANMERKUNG: Alle Parameter auf dem Bildschirm für Systemprofileinstellungen sind nur verfügbar, wenn die Option System Profile (Systemprofil) auf Custom (Benutzerdefiniert) gesetzt ist.
CPU Power Management	Ermöglicht das Festlegen der CPU-Stromverwaltung. Diese Option ist standardmäßig auf OS DBPM eingestellt. Eine weitere Option ist Maximum Performance (Maximale Leistung).
Memory Frequency	Legt die Geschwindigkeit des Systemspeichers fest. Diese Option ist standardmäßig auf Maximum Performance (Maximale Leistung) festgelegt.
Turbo Boost	Aktiviert bzw. deaktiviert den Prozessorbetrieb im Turbo-Boost-Modus. Diese Option ist standardmäßig auf Enabled festgelegt.
C1E	Aktiviert oder deaktiviert den Wechsel des Prozessors in einen Zustand mit minimaler Leistung, sobald der Prozessor im Leerlauf arbeitet. Diese Option ist standardmäßig auf Aktiviert eingestellt.
C States	Aktiviert bzw. deaktiviert den Prozessorbetrieb in allen verfügbaren Stromzuständen. Mit C States kann der Prozessor im Leerlauf in einen niedrigeren Stromversorgungszustand versetzt werden. Wenn die Option auf Aktiviert (Betriebssystem-gesteuert) oder auf Autonom (falls die Steuerung durch Hardware unterstützt wird) eingestellt ist, kann der Prozessor in allen verfügbaren Stromversorgungszuständen betrieben werden, um Energie zu sparen. Dies kann jedoch dazu führen, dass die Speicherlatenz und der Frequenz-Jitter erhöht werden. Diese Option ist standardmäßig auf Enabled festgelegt.
Memory Refresh Rate	Legt die Speicheraktualisierungsrate auf 1x oder 2x fest. Diese Option ist standardmäßig auf 1x festgelegt.
Nicht-Kern-Frequenz	Ermöglicht Ihnen die Auswahl der Option Nicht-Kern-Frequenz . Im Modus Dynamic (Dynamisch) kann der Prozessor die Energieressourcen über alle Kerne und Uncores hinweg zur Laufzeit optimieren. Die Optimierung der Nicht-Kern-Frequenz zum Energiesparen oder zur Leistungsoptimierung ist von der Einstellung der Option Energieeffizienzregel abhängig.

Tabelle 17. Systemprofileinstellungen – Details (fortgesetzt)

Option	Beschreibung
Monitor/Mwait	<p>Ermöglicht das Aktivieren der Monitor-/Mwait-Anweisungen im Prozessor. Diese Option ist standardmäßig auf Aktiviert festgelegt; dies gilt für alle Systemprofile mit Ausnahme von Benutzerdefiniert.</p> <p>i ANMERKUNG: Diese Option kann nur deaktiviert werden, wenn die Option C States (C-States) im Modus Custom (Benutzerdefiniert) auf Disabled (Deaktiviert) gesetzt ist.</p> <p>i ANMERKUNG: Wenn die Option C States (C-States) im Modus Custom (Benutzerdefiniert) auf Enabled (Aktiviert) festgelegt ist, haben Änderungen der Monitor-/Mwait-Einstellung keine Auswirkungen auf die Stromversorgung oder die Leistung des Systems.</p>
PCI ASPM L1 Link Power Management	Aktiviert oder deaktiviert das PCI-ASPM-L1-Link-Energiemanagement . Diese Option ist standardmäßig auf Enabled festgelegt.

Systemsicherheit

Wenn Sie den Bildschirm **Systemsicherheit** anzeigen möchten, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **Hauptmenü des System-Setups > System-BIOS > Systemsicherheit**.

Tabelle 18. Details zu Systemsicherheit

Option	Beschreibung
CPU AES-NI	Verbessert die Geschwindigkeit von Anwendungen durch Verschlüsselung und Entschlüsselung unter Einsatz der AES-NI-Standardanweisungen und ist per Standardeinstellung auf Enabled (Aktiviert) gesetzt. Diese Option ist standardmäßig auf Enabled festgelegt.
System Password	Richtet das Systemkennwort ein. Diese Option ist standardmäßig auf Enabled (Aktiviert) gesetzt und ist schreibgeschützt, wenn der Jumper im System nicht installiert ist.
Setup-Kennwort	Richtet das Setupkennwort ein. Wenn der Kennwort-Jumper nicht im System installiert ist, ist diese Option schreibgeschützt.
Kennwortstatus	Sperrt das Systemkennwort. In der Standardeinstellung ist diese Option auf Unlocked (Entriegelt).
TPM-Informationen	Zeigt den Typ des Trusted Platform Module an, falls vorhanden.

Tabelle 19. TPM 2.0-Sicherheitsinformationen

Option	Beschreibung
TPM-Informationen	
TPM Security	<p>i ANMERKUNG: Das TPM-Menü ist nur verfügbar, wenn das TPM-Modul installiert ist.</p> <p>Ermöglicht es Ihnen, den Berichtsmodus des TPMs zu steuern. Standardmäßig ist die Option TPM Security (TPM-Sicherheit) auf Off (Deaktiviert) eingestellt.</p> <p>Wenn TPM 2.0 installiert wird, wird die Option TPM-Sicherheit auf Ein oder auf Aus festgelegt. In der Standardeinstellung ist diese Option auf Off (Deaktiviert).</p>
TPM-Informationen	Zeigt den Betriebszustand des TPM an.
TPM Firmware	Zeigt die TPM-Firmware-Version an.
TPM Hierarchy	<p>Dient zum Aktivieren, Deaktivieren oder Löschen von Speicher- und Endorsement Key-Hierarchien. Wenn diese Einstellung auf Enabled (Aktiviert) festgelegt ist, können die Speicher- und Endorsement Key-Hierarchien verwendet werden.</p> <p>Wenn diese Einstellung auf Disabled (Deaktiviert) festgelegt ist, können die Speicher- und Endorsement Key-Hierarchien nicht verwendet werden.</p> <p>Wenn diese Einstellung auf Clear (Löschen) festgelegt ist, werden alle Werte aus den Speicher- und Endorsement Key-Hierarchien gelöscht. Anschließend wird die Einstellung auf Enabled (Aktiviert) festgelegt.</p>

Tabelle 19. TPM 2.0-Sicherheitsinformationen (fortgesetzt)

Option	Beschreibung
Erweiterte TPM-Einstellungen	TPM PPI Bypass Provision (Bereitstellung der TPM-PPI-Kennwort umgehung) Wenn die Option auf Aktiviert festgelegt ist, kann das Betriebssystem Meldungen der physischen Anwesenheitsschnittstelle (PPI) umgehen, wenn Bereitstellungsvorgänge für die PPI-Advanced Configuration and Power Interface (ACPI) ausgegeben werden.
	TPM PPI Bypass Clear (Löschen der TPM-PPI-Kennwort umgehung) Wenn die Option auf Aktiviert festgelegt ist, kann das Betriebssystem Meldungen der physischen Anwesenheitsschnittstelle (PPI) umgehen, wenn Bereitstellungsvorgänge für die PPI-Advanced Configuration and Power Interface (ACPI) gelöscht werden.
	Auswahl des TPM2-Algorithmus Ermöglicht es dem Benutzer, die kryptografischen Algorithmen des Trusted Platform Module (TPM) zu ändern. Die verfügbaren Optionen sind von der TPM-Firmware abhängig. Um die Auswahl des TPM2-Algorithmus zu ermöglichen, muss die Intel(R) TXT-Technologie deaktiviert sein. Die Option „Auswahl des TPM2-Algorithmus“ unterstützt SHA1, SHA128, SHA256, SHA512 und SM3 durch Erkennen des TPM-Moduls. Diese Option ist standardmäßig auf SHA1 festgelegt.

Tabelle 20. Details zu Systemsicherheit

Option	Beschreibung
Intel(R) TXT	Ermöglicht das Aktivieren bzw. Deaktivieren der Option „Intel Trusted Execution Technology (TXT)“. Zur Aktivierung der Option Intel TXT müssen die Virtualisierungstechnologie und die TPM-Sicherheit für TPM 1.2 mit Maßnahmen vor dem Start aktiviert oder für TPM 2.0 mit dem SHA256-Algorithmus auf On (aktiviert) festgelegt werden. In der Standardeinstellung ist diese Option auf Off (Deaktiviert). Zur Unterstützung von Secure Launch (Firmware-Schutz) unter Windows 2022 wird sie auf On (aktiviert) gesetzt.
Intel(R) SGX	Ermöglicht das Festlegen der Option Intel Software Guard Extension (SGX). Um die Option Intel SGX zu aktivieren, muss der Prozessor SGX-fähig sein, die Speicherbelegung muss kompatibel sein (mindestens x8 identische DIMM1 bis DIMM8 pro CPU-Sockel, nicht unterstützt auf Konfiguration mit persistentem Speicher), der Speicher-Betriebsmodus muss im Optimizer-Modus eingestellt sein, die Speicherverschlüsselung muss aktiviert sein und Node Interleaving muss deaktiviert sein. Diese Option ist standardmäßig auf Aus eingestellt. Wenn diese Option auf Aus festgelegt ist, deaktiviert das BIOS die SGX-Technologie. Wenn diese Option auf Ein eingestellt ist, aktiviert das BIOS die SGX-Technologie. i ANMERKUNG: Beim Upgrade von einer früheren BIOS-Version auf BIOS 1.7.4 wird die SGX-Funktion deaktiviert. Im Menü „SGX Factory Reset“ im Setup-Menü „System Security“ muss der Benutzer SGX zunächst mit einem Zurücksetzen auf die Werkseinstellungen erneut aktivieren.
Software Guard Extensions Epoch n: Legt die Werte der Software Guard Extensions EPOCHs fest.	
SGX LE Public Key Hash0: Legt die Bytes von 0–7 für den SGX Launch Enclave Public Key Hash fest.	

Tabelle 20. Details zu Systemsicherheit (fortgesetzt)

Option	Beschreibung
SGX LE Public Key Hash1: Legt die Bytes von 8–15 für den SGX Launch Enclave Public Key Hash fest.	
SGX LE Public Key Hash2: Legt die Bytes von 16–23 für den SGX Launch Enclave Public Key Hash fest.	
SGX LE Public Key Hash3: Legt die Bytes von 24–31 für den SGX Launch Enclave Public Key Hash fest.	
Netzschalter	Aktiviert oder deaktiviert den Netzschalter auf der Vorderseite des System. Diese Option ist standardmäßig auf Disabled (Deaktiviert) gesetzt.
Netzstromwiederherstellung	Ermöglicht das Festlegen der Reaktion des Systems, nachdem die Netzstromversorgung des System wiederhergestellt wurde. In der Standardeinstellung ist diese Option auf Enabled (Aktiviert) . i ANMERKUNG: Das Hostsystem wird erst eingeschaltet, wenn iDRAC Root of Trust (RoT) abgeschlossen ist. Das Einschalten des Hosts wird nach dem Anlegen der Wechsellspannung um mindestens 90 Sekunden verzögert.
Verzögerung bei Netzstromwiederherstellung	Legt die Zeitverzögerung für die Systemeinschaltung fest, nachdem die Netzstromversorgung des Systems wiederhergestellt wurde. In der Standardeinstellung ist diese Option auf System (Sofort) gesetzt. In der Standardeinstellung ist diese Option auf Immediate (Sofort) . Wenn diese Option auf Sofort festgelegt ist, gibt es keine Verzögerung für das Hochfahren. Wenn diese Option auf Zufällig eingestellt ist, erzeugt das System eine zufällige Verzögerung für das Hochfahren. Wenn diese Option auf Benutzerdefiniert eingestellt ist, wird die Verzögerungszeit bis zum Hochfahren des Systems manuell festgelegt.
User Defined Delay (Benutzerdefinierte Verzögerung) (60 bis 600 s)	Legt die Option User Defined Delay (Benutzerdefinierte Verzögerung) fest, wenn die Option User Defined (Benutzerdefiniert) für AC Power Recovery Delay (Verzögerung bei Netzstromwiederherstellung) gewählt ist. Für die tatsächliche AC-Recovery-Zeit muss die Root-of-Trust-Zeit von iDRAC (ca. 50 Sekunden) hinzugefügt werden.
Variabler UEFI-Zugriff	Bietet unterschiedliche Grade von UEFI-Sicherungsvariablen. Wenn die Option auf Standard (Standardeinstellung) gesetzt ist, sind die UEFI-Variablen gemäß der UEFI-Spezifikation im Betriebssystem aufrufbar. Wenn die Option auf Controlled (Kontrolliert) gesetzt ist, werden die ausgewählten UEFI-Variablen in der Umgebung geschützt und neue UEFI-Starteinträge werden an das Ende der aktuellen Startreihenfolge gezwungen.
In-Band Benutzeroberfläche	Bei der Einstellung Deaktiviert blendet diese Einstellung Geräte der Management Engine (ME), HECI-Geräte und IPMI-Geräte des Systems gegenüber dem Betriebssystem aus. Dadurch wird verhindert, dass der Betriebssystem vom Ändern des ME Power Capping Einstellungen und blockiert den Zugriff auf alle In-Band -Management Tools. Alle Management verwaltet werden sollte über Out-of-Band-. Diese Option ist standardmäßig auf Aktiviert eingestellt. i ANMERKUNG: BIOS-Aktualisierung erfordert HECI Geräte in Betrieb sein und DUP Aktualisierungen erfordern IPMI-Schnittstelle in Betrieb sein. Diese Einstellung muss so eingestellt werden Aktiviert zu vermeiden Aktualisierungsfehler.
SMM-Sicherheitsmigration	Aktiviert oder deaktiviert die UEFI SMM Security Migration-Schutzmaßnahmen. Es ist für die Unterstützung von Windows 2022 aktiviert.
Sicherer Start	Ermöglicht den sicheren Start, indem das BIOS jedes Vorstart-Image mit den Zertifikaten in der Sicherheitsstartrichtlinie bzw. Regel für sicheren Start authentifiziert. „Secure Start“ (Sicherer Start) ist in der Standardeinstellung deaktiviert. Sicherer Start ist standardmäßig auf Standard festgelegt.
Regel für sicheren Start	Wenn die Richtlinie für den sicheren Start auf Standard eingestellt ist, authentifiziert das BIOS die Vorstart-Images mithilfe des Schlüssels und der Zertifikate des Systemherstellers. Wenn die Richtlinie für den sicheren Start auf Custom (Benutzerdefiniert) eingestellt ist, verwendet das BIOS benutzerdefinierte Schlüssel und Zertifikate. Die Richtlinie für den sicheren Start ist standardmäßig auf Standard festgelegt.

Tabelle 20. Details zu Systemsicherheit (fortgesetzt)

Option	Beschreibung								
Secure Boot Mode	<p>Legt fest, wie das BIOS die Regel für sicheren Start Objekte (PK, KEK, db, dbx).</p> <p>Wenn der aktuelle Modus eingestellt ist zum Modus „Bereitgestellt“, die verfügbaren Optionen sind Benutzermodus und Modus „Bereitgestellt“. Wenn die aktuelle Modus ist Benutzermodus, die verfügbaren Optionen sind Benutzermodus, Prüfmodus, und Modus „Bereitgestellt“.</p> <p>Tabelle 21. Secure Boot Mode</p> <table border="1"> <thead> <tr> <th>Optionen</th> <th>Beschreibungen</th> </tr> </thead> <tbody> <tr> <td>Benutzermodi</td> <td> <p>Im Benutzermodus, PK muss installiert sein, und das BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte.</p> <p>Das BIOS nicht zugelassener programmatischer Übergänge zwischen Modi.</p> </td> </tr> <tr> <td>Audit-Modus</td> <td> <p>Im Audit-Modus ist PK nicht vorhanden. Das BIOS bestätigt programmgesteuerte Aktualisierungen der Richtlinienobjekte und Übergänge zwischen den Modi nicht. Das BIOS führt eine Signaturüberprüfung der Vorstart-Images durch und protokolliert die Ergebnisse in der Ausführungsinformationen-Tabelle der Images, wobei die Images ausgeführt werden, unabhängig davon, ob sie die Prüfung bestanden haben oder nicht.</p> <p>Der Audit Mode (Audit-Modus) eignet sich für die programmgesteuerte Festlegung eines Satzes von Richtlinienobjekten.</p> </td> </tr> <tr> <td>Modus Bereitgestellt</td> <td> <p>Modus Bereitgestellt ist die sicherste Modus. Im Modus Bereitgestellt, PK muss installiert sein und der BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte.</p> <p>Modus Bereitgestellt schränkt die programmatischer Mode-Übergänge.</p> </td> </tr> </tbody> </table>	Optionen	Beschreibungen	Benutzermodi	<p>Im Benutzermodus, PK muss installiert sein, und das BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte.</p> <p>Das BIOS nicht zugelassener programmatischer Übergänge zwischen Modi.</p>	Audit-Modus	<p>Im Audit-Modus ist PK nicht vorhanden. Das BIOS bestätigt programmgesteuerte Aktualisierungen der Richtlinienobjekte und Übergänge zwischen den Modi nicht. Das BIOS führt eine Signaturüberprüfung der Vorstart-Images durch und protokolliert die Ergebnisse in der Ausführungsinformationen-Tabelle der Images, wobei die Images ausgeführt werden, unabhängig davon, ob sie die Prüfung bestanden haben oder nicht.</p> <p>Der Audit Mode (Audit-Modus) eignet sich für die programmgesteuerte Festlegung eines Satzes von Richtlinienobjekten.</p>	Modus Bereitgestellt	<p>Modus Bereitgestellt ist die sicherste Modus. Im Modus Bereitgestellt, PK muss installiert sein und der BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte.</p> <p>Modus Bereitgestellt schränkt die programmatischer Mode-Übergänge.</p>
Optionen	Beschreibungen								
Benutzermodi	<p>Im Benutzermodus, PK muss installiert sein, und das BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte.</p> <p>Das BIOS nicht zugelassener programmatischer Übergänge zwischen Modi.</p>								
Audit-Modus	<p>Im Audit-Modus ist PK nicht vorhanden. Das BIOS bestätigt programmgesteuerte Aktualisierungen der Richtlinienobjekte und Übergänge zwischen den Modi nicht. Das BIOS führt eine Signaturüberprüfung der Vorstart-Images durch und protokolliert die Ergebnisse in der Ausführungsinformationen-Tabelle der Images, wobei die Images ausgeführt werden, unabhängig davon, ob sie die Prüfung bestanden haben oder nicht.</p> <p>Der Audit Mode (Audit-Modus) eignet sich für die programmgesteuerte Festlegung eines Satzes von Richtlinienobjekten.</p>								
Modus Bereitgestellt	<p>Modus Bereitgestellt ist die sicherste Modus. Im Modus Bereitgestellt, PK muss installiert sein und der BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte.</p> <p>Modus Bereitgestellt schränkt die programmatischer Mode-Übergänge.</p>								
Richtlinie zum sicheren Start – Übersicht	Gibt die Liste der Zertifikate und Hashes für den sicheren Start an, die beim sicheren Start für authentifizierte Images verwendet werden.								
Benutzerdefinierte Einstellungen für die Richtlinie zum sicheren Start	Konfiguriert die Secure Boot Custom Policy. Um diese Option zu aktivieren, stellen Sie die sichere Startrichtlinie auf Custom (Benutzerdefinierte) Option.								

Erstellen eines System- und Setup-Kennworts

Voraussetzungen

Stellen Sie sicher, dass der Kennwort-Jumper aktiviert ist. Mithilfe des Kennwort-Jumpers werden die System- und Setup-Kennwortfunktionen aktiviert bzw. deaktiviert. Weitere Informationen finden Sie im Abschnitt „Jumper-Einstellungen auf der System“.

ANMERKUNG: Wenn die Kennwort-Jumper-Einstellung deaktiviert ist, werden das vorhandene „System Passwort“ (Systemkennwort) und „Setup Password“ (Setup-Kennwort) gelöscht und es ist nicht notwendig, das Systemkennwort zum Systemstart anzugeben.

Schritte


1. Drücken Sie zum Aufrufen des System-Setups unmittelbar nach dem Einschaltvorgang oder dem Neustart des Systems die Taste F2.
2. Klicken Sie auf dem Bildschirm **System Setup Main Menu** (System-Setup-Hauptmenü) auf **System BIOS (System-BIOS) > System Security (Systemsicherheit)**.
3. Überprüfen Sie im Bildschirm **Systemsicherheit**, ob die Option **Kennwortstatus** auf **Nicht gesperrt** gesetzt ist.
4. Geben Sie Ihr Systemkennwort in das Feld **System Password** (Systemkennwort) ein und drücken Sie die Eingabe- oder Tabulatortaste.

Verwenden Sie zum Zuweisen des Systemkennworts die folgenden Richtlinien:

- Kennwörter dürfen aus maximal 32 Zeichen bestehen.

In einer Meldung werden Sie aufgefordert, das Systemkennwort erneut einzugeben.

5. Geben Sie das Systemkennwort ein und klicken Sie dann auf **OK**.
6. Geben Sie Ihr Setup-Kennwort in das Feld **Setup-Kennwort** ein und drücken Sie die Eingabe- oder Tabulatortaste. In einer Meldung werden Sie aufgefordert, das Setup-Kennwort erneut einzugeben.
7. Geben Sie das Setup-Kennwort erneut ein und klicken Sie dann auf **OK**.
8. Drücken Sie die Taste „Esc“, um zum Bildschirm System-BIOS zurückzukehren. Drücken Sie erneut „Esc“.
In einer Meldung werden Sie aufgefordert, die Änderungen zu speichern.

 **ANMERKUNG:** Der Kennwortschutz wird erst wirksam, wenn das System neu gestartet wird.

Verwenden des Systemkennworts zur Systemsicherung

Info über diese Aufgabe


Wenn ein Setup-Kennwort vergeben wurde, wird das Setup-Kennwort vom System als alternatives Systemkennwort zugelassen.

Schritte

1. Schalten Sie das System ein oder starten Sie es neu.
2. Geben Sie das Systemkennwort ein und drücken Sie die Eingabetaste.


Nächste Schritte

Wenn die Option **Passwortstatus** auf **Gesperrt** gesetzt ist, geben Sie nach einer Aufforderung beim Neustart das Systemkennwort ein und drücken Sie die Eingabetaste.

 **ANMERKUNG:** Wenn ein falsches System eingegeben wird, zeigt das System eine Meldung an und fordert Sie zur erneuten Eingabe des Kennworts auf. Sie haben drei Versuche, um das korrekte Kennwort einzugeben. Nach dem dritten erfolglosen Versuch zeigt das System eine Fehlermeldung an, die darauf hinweist, dass das System angehalten wurde und ausgeschaltet werden muss. Auch nach dem Herunterfahren und Neustarten des System wird die Fehlermeldung angezeigt, bis das korrekte Kennwort eingegeben wurde.

Löschen oder Ändern eines System- und Setup-Kennworts

Voraussetzungen

 **ANMERKUNG:** Sie können ein vorhandenes System- oder Setup-Kennwort nicht löschen oder ändern, wenn **Password Status (Kennwortstatus)** auf **Locked (Gesperrt)** gesetzt ist.

Schritte

1. Zum Aufrufen des System-Setups drücken Sie unmittelbar nach einem Einschaltvorgang oder Neustart des System die Taste F2.
2. Klicken Sie im Bildschirm **System-Setup-Hauptmenü** auf **System-BIOS > Systemsicherheit**.
3. Überprüfen Sie im Bildschirm **System Security** (Systemsicherheit), ob die Option **Password Status** (Kennwortstatus) auf **Unlocked** (Nicht gesperrt) gesetzt ist.
4. Ändern oder löschen Sie im Feld **System Password (Systemkennwort)** das vorhandene Kennwort des System und drücken Sie dann die Eingabetaste oder die Tabulatortaste.
5. Ändern oder löschen Sie im Feld **Setup Password (Setup-Kennwort)** das vorhandene Setup-Kennwort und drücken Sie dann die Eingabetaste oder die Tabulatortaste.

Wenn Sie das System- und Setup-Kennwort ändern, werden Sie in einer Meldung aufgefordert, noch einmal das neue Kennwort einzugeben. Wenn Sie das System- und Setup-Kennwort löschen, werden Sie in einer Meldung aufgefordert, das Löschen zu bestätigen.

6. Drücken Sie die Taste „Esc“, um zum Bildschirm **System-BIOS** zurückzukehren. Drücken Sie <Esc> noch einmal, und Sie werden durch eine Meldung zum Speichern von Änderungen aufgefordert.
7. Wählen Sie die Option **Setup-Kennwort** aus, ändern oder löschen Sie das vorhandene Setup-Kennwort, und drücken Sie die Eingabetaste oder die Tabulatortaste.

ANMERKUNG: Wenn Sie das System- oder Setup-Kennwort ändern, werden Sie in einer Meldung aufgefordert, noch einmal das neue Kennwort einzugeben. Wenn Sie das System- oder Setup-Kennwort löschen, werden Sie in einer Meldung aufgefordert, das Löschen zu bestätigen.

Betrieb mit aktiviertem Setup-Kennwort

Wenn die Option **Setup-Kennwort** auf **Aktiviert** festgelegt ist, geben Sie das richtige Setup-Kennwort ein, bevor Sie die Optionen des System-Setups bearbeiten.

Wird auch beim dritten Versuch nicht das korrekte Passwort eingegeben, zeigt das System die folgende Meldung an:

Auch nach dem Ausschalten und Neustarten des Systems wird die Fehlermeldung angezeigt, bis das korrekte Kennwort eingegeben wurde. Die folgenden Optionen sind Ausnahmen:

- Wenn die Option **System-Kennwort** nicht auf **Aktiviert** festgelegt ist und nicht über die Option **Passwortstatus** gesperrt ist, können Sie ein System zuweisen. Weitere Informationen finden Sie im Abschnitt über den Bildschirm System.
- Ein vorhandenes System kann nicht deaktiviert oder geändert werden.

ANMERKUNG: Die Option „Password Status“ kann zusammen mit der Option „Setup Password“ verwendet werden, um das System vor unbefugten Änderungen zu schützen.

Redundante Betriebssystemsteuerung

Wenn Sie den Bildschirm **Redundante Betriebssystemsteuerung** anzeigen möchten, schalten Sie das System ein, drücken Sie F2 und klicken Sie auf **Hauptmenü des System-Setup > System- BIOS > Redundante Betriebssystemsteuerung**.

Tabelle 22. Details zu Redundante Betriebssystemsteuerung

Option	Beschreibung
Redundant OS Location	Ermöglicht Ihnen die Auswahl eines Sicherungslaufwerks für die folgenden Geräte: <ul style="list-style-type: none"> • Keine • BOSS-PCIe-Karten (Interne M.2- Laufwerke) • SATA-Anschluss A
Redundant OS State	<p>ANMERKUNG: Diese Option wird deaktiviert, falls Redundant OS Location (Redundantes Betriebssystem – Speicherort) auf None (Keiner) gesetzt wird.</p> <p>Wenn Visible (Sichtbar) eingestellt wird, ist das Sicherungslaufwerk in der Startliste und dem Betriebssystem ersichtlich. Wenn Hidden (Ausgeblendet) eingestellt wird, ist das Sicherungslaufwerk deaktiviert und ist nicht in der Startliste und dem Betriebssystem ersichtlich. Diese Option wird standardmäßig auf Visible (Sichtbar) eingestellt.</p> <p>ANMERKUNG: Das BIOS deaktiviert das Gerät in der Hardware, sodass das Betriebssystem nicht darauf zugreifen kann.</p>
Redundant OS Boot	<p>ANMERKUNG: Diese Option ist deaktiviert, falls Redundant OS Location (Redundantes Betriebssystem – Speicherort) auf None (Keiner) gesetzt wird, oder falls Redundant OS State (Redundantes Betriebssystem – Zustand) auf Hidden (Ausgeblendet) gesetzt wird.</p> <p>Falls Enabled (Aktiviert) eingestellt wird, startet das BIOS auf dem als Redundant OS Location (Redundantes Betriebssystem – Speicherort) angegebenen Gerät. Falls Disabled (Deaktiviert) eingestellt wird, behält das BIOS die aktuellen Einstellungen der Startliste bei. Diese Option ist standardmäßig auf Disabled festgelegt.</p>

Verschiedene Einstellungen

Schalten Sie zum Anzeigen des Bildschirms **Miscellaneous Settings** das System ein, drücken Sie F2 und klicken Sie auf **System Setup Main Menu > System BIOS > Miscellaneous Settings**.

Tabelle 23. Details zu Miscellaneous Settings

Option	Beschreibung
System Time (System-Uhrzeit)	Ermöglicht das Festlegen der Uhrzeit im System.
System Date (System-Datum)	Ermöglicht das Festlegen des Datums im System.
Asset Tag (Systemkennnummer)	Zeigt die Systemkennnummer an und ermöglicht ihre Änderung zum Zweck der Sicherheit und Überwachung.
Keyboard NumLock (Tastatur-Num-Sperre)	Ermöglicht das Festlegen, ob das System mit aktivierter oder deaktivierter Num-Sperre startet. Diese Option ist standardmäßig auf On (Aktiviert) eingestellt. i ANMERKUNG: Diese Option gilt nicht für Tastaturen mit 84 Tasten.
F1/F2 Prompt on Error	Aktiviert bzw. deaktiviert die F1/F2-Eingabeaufforderung bei einem Fehler. Diese Option ist standardmäßig auf Enabled festgelegt. Die F1/F2-Eingabeaufforderung umfasst auch Tastaturfehler.
Dell Wyse P25/P45 BIOS Access	Aktiviert oder deaktiviert den Dell Wyse P25/P45 BIOS-Zugriff. Diese Option ist standardmäßig auf Enabled festgelegt.
Power Cycle Request	Aktiviert oder deaktiviert die Anfrage für das Aus- und Einschalten des Systems. In der Standardeinstellung ist diese Option auf None (Keine).

iDRAC Settings

Die iDRAC-Einstellungen sind eine Oberfläche zur UEFI-basierten Einrichtung und Konfiguration der iDRAC-Parameter. Mit den iDRAC-Einstellungen können verschiedene iDRAC-Parameter aktiviert oder deaktiviert werden.

i **ANMERKUNG:** Für den Zugriff auf bestimmte Funktionen in den iDRAC-Einstellungen wird ein Upgrade der iDRAC Enterprise-Lizenz benötigt.

Weitere Informationen zur Verwendung des iDRAC finden Sie im Dokument *Benutzerhandbuch zum integrated Dell Remote Access Controller* unter <https://www.dell.com/idracmanuals>.

Device Settings (Geräteeinstellungen)

Mithilfe der **Geräteeinstellungen** können Sie Geräteparameter wie Speicher-Controller oder Netzwerkkarten konfigurieren.

Service Tag Settings

Mit den **Service-Tag-Einstellungen** können Sie die Service-Tag-Nummer des Systems konfigurieren.

Dell Lifecycle Controller

Der Dell Lifecycle Controller (LC) ist eine integrierte Lösung für erweiterte Systemverwaltung, die Funktionen für die Bereitstellung, Konfiguration und Aktualisierung von Systemen sowie für Wartung und Diagnose umfasst. Der LC wird als Teil der Out-of-band-Lösung iDRAC und der auf Dell Systemen integrierten UEFI-Anwendungen (Unified Extensible Firmware Interface) bereitgestellt.

Integrierte Systemverwaltung

Der Dell Lifecycle Controller ermöglicht eine erweiterte integrierte Systemverwaltung während des gesamten Lebenszyklus des Systems. Der Dell Lifecycle Controller wird während der Startsequenz gestartet und arbeitet unabhängig vom Betriebssystem.

i **ANMERKUNG:** Bestimmte Plattformkonfigurationen unterstützen möglicherweise nicht alle Funktionen des Dell Lifecycle Controller.

Weitere Informationen zur Einrichtung des Dell Lifecycle Controller, zur Konfiguration der Hardware und Firmware sowie zur Bereitstellung des Betriebssystems finden Sie in der Dokumentation zum Dell Lifecycle Controller unter <https://www.dell.com/idracmanuals>.

Start-Manager

Mit der Option **Start-Manager** können Sie Startoptionen und Diagnose-Dienstprogramme auswählen.

Um den **Start-Manager** aufzurufen, schalten Sie das System ein und drücken Sie die Taste F11.

Tabelle 24. Start-Manager – Details

Option	Beschreibung
Continue Normal Boot (Normalen Startvorgang fortsetzen)	Das System versucht, von den Geräten in der Startreihenfolge zu starten, beginnend mit dem ersten Eintrag. Wenn der Startvorgang fehlschlägt, setzt das Gerät den Vorgang mit dem nächsten Gerät in der Startreihenfolge fort, bis ein Startvorgang erfolgreich ist oder keine weiteren Startoptionen vorhanden sind.
One-shot Boot Menu (Einmaliges Startmenü)	Für den Zugriff auf das Startmenü, um ein einmaliges Startgerät auszuwählen.
Launch System Setup (System-Setup starten)	Ermöglicht den Zugriff auf das System-Setup.
Launch Lifecycle Controller (Starten des Lifecycle Controller)	Beendet den Start-Manager und ruft das Dell Lifecycle Controller-Programm auf.
Systemdienstprogramme	Ermöglicht das Starten von Systemdienstprogrammen wie z. B. „Diagnose starten“, „Explorer für BIOS-Aktualisierungsdateien“, „System neu starten“.

PXE-Boot

Sie können die PXE-Option (Preboot Execution Environment) zum Starten und Konfigurieren der vernetzten Systeme im Remote-Zugriff verwenden.

Um auf die Option **PXE-Start** zuzugreifen, starten Sie das System und drücken Sie dann während des POST die Taste F12, anstatt die Standard-Startreihenfolge aus dem BIOS-Setup zu verwenden. Es werden keine Menüs abgerufen und Sie können keine Netzwerkgeräte verwalten.