PowerEdge R450 – Informationsaktualisierung – Technisches Datenblatt

November 2022
Rev. 1

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.

Inhaltsverzeichnis

1

Übersicht

Die Informationen in diesem Dokument ersetzen die Informationen in den entsprechenden Abschnitten des Installations- und Service-Handbuchs Referenzhandbuchs für BIOS und UEFI und der Technischen Daten.

Eine vollständige Liste der Informationen finden Sie in den Dokumenten unter https://www.dell.com/poweredgemanuals.

Themen:

Revisionsverlauf

Dieser Abschnitt enthält eine Beschreibung der Dokumentänderungen.

Tabelle 1. Revisionsverlauf des Dokuments

Dokumentversionen	Datum	Beschreibung der Änderungen
1	November 2022	1. Hinweis für neue Stromzwischenplatine hinzugefügt 2. Mindestkonfiguration für POST aktualisiert 3. BIOS, Systemsicherheit aktualisiert 4. Netzteile aktualisiert

2

Informationsaktualisierung

Themen:

Stromzwischenplatine entfernen

Voraussetzungen

1. Befolgen Sie die Sicherheitshinweise unter Sicherheitshinweise.
2. Befolgen Sie die Anweisungen unter Vor der Arbeit an Komponenten im Inneren Ihres Systems.
3. Entfernen Sie die Luftstromverkleidung.
4. Entfernen Sie das Netzteil oder den Netzteilplatzhalter.
5. Trennen Sie alle Kabel, die mit der Stromzwischenplatine verbunden sind.

ANMERKUNG: Systeme, die ab November 2022 ausgeliefert werden, verfügen möglicherweise über eine andere Stromverteilungsplatine und andere Anschlüsse.

Schritte

1. Entfernen Sie mit einem Kreuzschlitzschraubenzieher (Größe 2) die Schrauben, mit denen die Stromzwischenplatine am System befestigt ist.

   ANMERKUNG: Merken Sie sich, wie das Kabel verlegt ist, wenn Sie es aus dem System entfernen.

2. Heben Sie die Stromzwischenplatine aus dem System heraus.

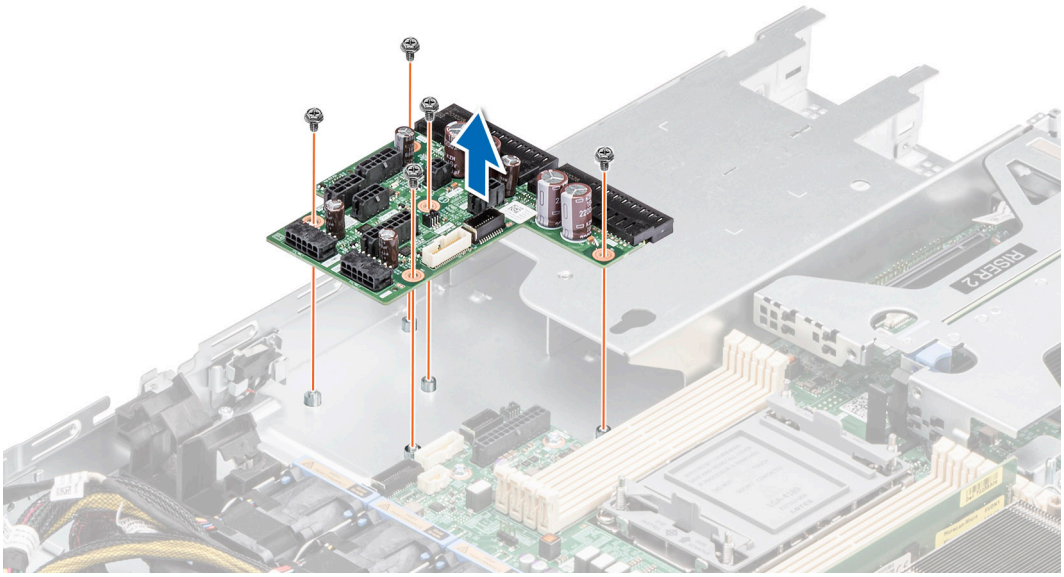

Abbildung 1. Stromzwischenplatine entfernen

Nächste Schritte

Setzen Sie die Stromzwischenplatine wieder ein.

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 2. 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 3. TPM 1.2-Sicherheitsinformationen

Option	Beschreibung	
TPM-Informationen		
TPM Security	**ANMERKUNG:** Das TPM-Menü ist nur verfügbar, wenn das TPM-Modul installiert ist. Ermöglicht es Ihnen, den Berichtsmodus des TPMs zu steuern. Standardmäßig ist die Option **TPM Security** (TPM-Sicherheit) auf **Off** (Deaktiviert) eingestellt. Die Felder "TPM Status" (TPM-Status) und "TPM Activation" (TPM-Aktivierung) können nur geändert werden, falls das Feld **TPM Status** (TPM-Status) auf **On with Pre-boot Measurements** (Aktiviert mit Maßnahmen vor dem Start) oder **On without Pre-boot Measurements** (Aktiviert ohne Maßnahmen vor dem Start) gesetzt ist. Wenn TPM 1.2 installiert wird, wird die Option **TPM-Sicherheit** auf **Aus**, **Aktiviert mit Maßnahmen vor dem Start**, oder **Aktiviert ohne Maßnahmen vor dem Start** festgelegt.	
TPM-Informationen	Zeigt den Betriebszustand des TPM an.	
TPM Firmware	Zeigt die TPM-Firmware-Version an.	
TPM Status	Gibt den TPM-Status an.	
TPM-Befehl	Setzen Sie das TPM (Trusted Platform Module) ein. Bei der Einstellung **Keine** wird kein Befehl an das TPM gesendet. Bei der Einstellung **Aktivieren** ist das TPM aktiviert. Bei der Einstellung **Deactivate (Deaktivieren)**, ist das TPM deaktiviert. Bei der Einstellung **löschen**, werden alle Inhalte des TPM gelöscht. In der Standardeinstellung ist diese Option auf **None** (Keine).	
Erweiterte TPM-Einstellungen	**TPM PPI Bypass Provision (Bereitstellung der TPM-PPI-Kennwortumgehung)**	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	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.

Tabelle 3. TPM 1.2-Sicherheitsinformationen (fortgesetzt)

Option	Beschreibung	
	TPM-PPI-Kennwortumgehung)	

Tabelle 4. TPM 2.0-Sicherheitsinformationen

Option	Beschreibung	
TPM-Informationen		
TPM Security	**ANMERKUNG:** Das TPM-Menü ist nur verfügbar, wenn das TPM-Modul installiert ist. Ermöglicht es Ihnen, den Berichtsmodus des TPMs zu steuern. Standardmäßig ist die Option **TPM Security** (TPM-Sicherheit) auf **Off** (Deaktiviert) eingestellt. 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).	
TPM-Informationen	Zeigt den Betriebszustand des TPM an.	
TPM Firmware	Zeigt die TPM-Firmware-Version an.	
TPM Hierarchy	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. Wenn diese Einstellung auf **Disabled** (Deaktiviert) festgelegt ist, können die Speicher- und Endorsement Key-Hierarchien nicht verwendet werden. 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.	
Erweiterte TPM-Einstellungen	**TPM PPI Bypass Provision (Bereitstellung der TPM-PPI-Kennwortumgehung)**	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-Kennwortumgehung)	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-Algorithmuszu 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 5. 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.
Speicherverschlüsselung	Aktiviert oder deaktiviert Intel Total Memory Encryption (TME) und Multi-Tenant (Intel® TME-MT). Wenn die Option auf **Deaktiviert** gesetzt ist, deaktiviert das BIOS die TME- und die MK-TME-Technologie. Wenn die Option auf **Single Key** gesetzt ist, aktiviert das BIOS die TME-Technologie. Wenn die Option auf **Multiple Keys (Mehrere Tasten)** gesetzt ist, aktiviert das BIOS die TME-MT-Technologie. Die Option CPU Physical Address Limit (CPU-Begrenzung physischer Adressen) muss für die Auswahl der Option Multiple Keys (Mehrere Schlüssel) deaktiviert sein. Diese Option ist standardmäßig auf **Disabled** festgelegt.
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.
In-Band-Zugriff auf SGX-Paketinformationen	Ermöglicht Ihnen den Zugriff auf die In-Band-Option der Intel Software Guard Extension (SGX)-Paketinformationen. Diese Option ist standardmäßig auf **Aus** eingestellt.
PPMRR-Größe	Legt die PPMRR-Größe fest.
SGX-QoS	Aktiviert oder deaktiviert die SGX-Quality of Service.
Eingabetyp für Eigentümer-EPOCH auswählen	Ermöglicht die Auswahl von **In neue zufällige Eigentümer-EPOCHs ändern** oder **Manuelle benutzerdefinierte Eigentümer-EPOCHs**. Jedes EPOCH hat 64 Bit. Nach dem Generieren einer neuen EPOCH durch Auswählen von **In neue zufällige Eigentümer-EPOCHs ändern** wird die Auswahl auf **Manuelle benutzerdefinierte Eigentümer-EPOCHs** zurückgesetzt.
	Software Guard Extensions Epoch n: Legt die Werte der Software Guard Extensions EPOCHs fest.
Aktivieren von Schreibvorgängen auf SGXLEPUBKEYHASH[3:0] von BS/SW	Aktiviert oder deaktiviert die Option „Aktivieren von Schreibvorgängen auf SGXLEPUBKEYHASH[3:0] von BS/SW“.
	SGX LE Public Key Hash0: Legt die Bytes von 0–7 für den SGX Launch Enclave Public Key Hash fest.
	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.
Aktivieren/Deaktivieren des SGX Auto MP Registration Agent	Aktiviert oder deaktiviert die SGX Auto MP-Registrierung. Der MP-Registrierungs-Agent ist für die Registrierung der Plattform verantwortlich.
SGX-Werkseinstellungen	Ermöglicht das Zurücksetzen der SGX-Option auf die Werkseinstellungen. Diese Option ist standardmäßig auf **Aus** eingestellt.
Netzschalter	Aktiviert oder deaktiviert den Netzschalter auf der Vorderseite des System. Diese Option ist standardmäßig auf **Enabled (Aktiviert)** 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).

Tabelle 5. Details zu Systemsicherheit (fortgesetzt)

<table>
<tr><th>Option</th><th>Beschreibung</th></tr>
<tr><td></td><td>ANMERKUNG: Das Hostsystem wird erst eingeschaltet, wenn iDRAC Root of Trust (RoT) abgeschlossen ist. Das Einschalten des Hosts wird nach dem Anlegen der Wechselspannung um mindestens 90 Sekunden verzögert.</td></tr>
<tr><td>Verzögerung bei Netzstromwiederherstellung</td><td>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.</td></tr>
<tr><td>User Defined Delay (Benutzerdefinierte Verzögerung) (60 bis 600 s)</td><td>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.</td></tr>
<tr><td>Variabler UEFI-Zugriff</td><td>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.</td></tr>
<tr><td>In-Band Benutzeroberfläche</td><td>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.
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.</td></tr>
<tr><td>SMM-Sicherheitsmigration</td><td>Aktiviert oder deaktiviert die UEFI SMM Security Migration-Schutzmaßnahmen. Es ist für die Unterstützung von Windows 2022 aktiviert.</td></tr>
<tr><td>Sicherer Start</td><td>Ermöglicht den sicheren Start, indem das BIOS jedes Vorstart-Image mit den Zertifikaten in der Sicherungsstartrichtlinie bzw. Regel für sicheren Start authentifiziert. „Secure Start“ (Sicherer Start) ist in der Standardeinstellung deaktiviert. Sicherer Start ist standardmäßig auf Standard festgelegt.</td></tr>
<tr><td>Regel für sicheren Start</td><td>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.</td></tr>
<tr><td>Secure Boot Mode</td><td>Legt fest, wie das BIOS die Regel für sicheren Start Objekte (PK, KEK, db, dbx).
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“.
Tabelle 6. Secure Boot Mode
<table>
<tr><th>Optionen</th><th>Beschreibungen</th></tr>
<tr><td>Benutzermodi</td><td>Im Benutzermodus, PK muss installiert sein, und das BIOS führt die Signaturüberprüfung auf programmatischer versucht, Regel zum Aktualisieren Objekte.
Das BIOS nicht zugelassener programmatischer Übergänge zwischen Modi.</td></tr>
</table></td></tr>
</table>

Tabelle 5. Details zu Systemsicherheit (fortgesetzt)

<table>
<tr><th>Option</th><th>Beschreibung</th></tr>
<tr><td></td><td>
Tabelle 6. Secure Boot Mode (fortgesetzt)
<table>
<tr><th>Optionen</th><th>Beschreibungen</th></tr>
<tr><td>Audit-Modus</td><td>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.

Der Audit Mode (Audit-Modus) eignet sich für die programmgesteuerte Festlegung eines Satzes von Richtlinienobjekten.</td></tr>
<tr><td>Modus Bereitgestellt</td><td>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.

Modus Bereitgestellt schränkt die programmatischer Mode-Übergänge.</td></tr>
</table>
</td></tr>
<tr><td>Richtlinie zum sicheren Start – Übersicht</td><td>Gibt die Liste der Zertifikate und Hashes für den sicheren Start an, die beim sicheren Start für authentifizierte Images verwendet werden.</td></tr>
<tr><td>Benutzerdefinierte Einstellungen für die Richtlinie zum sicheren Start</td><td>Konfiguriert die Secure Boot Custom Policy. Um diese Option zu aktivieren, stellen Sie die sichere Startrichtlinie auf Custom (Benutzerdefinierte) Option. Die folgende Liste enthält Beschreibungen der verfügbaren benutzerdefinierten Einstellungen für die Secure Boot-Richtlinie:
Platform Key (PK): Importieren, Exportieren, Löschen oder Wiederherstellen des Plattformschlüssels (Platform Key, PK)
Key Exchange Key Database (KEK): Importieren, Exportieren, Löschen oder Wiederherstellen von Einträgen in der KEK-Datenbank (Key Exchange Key)
Authorized Signature Database (db): Importieren, Exportieren, Löschen oder Wiederherstellen von Einträgen in der Authorized Signature-Datenbank (db)
Forbidden Signature Database (dbx): Importieren, Exportieren, Löschen oder Wiederherstellen von Einträgen in der Forbidden Signature-Datenbank (dbx)
Delete All Policy Entries (PK, KEK, db, and dbx): Wiederherstellen der Standardeinträge des Systemherstellers für die PK-, KEK-, db- und dbx-Datenbank. Alle importierten Einträge werden entfernt.
Export Firmware Hash Values: Exportieren von Werten für Firmware-Images von Drittanbietern, wie z. B. Netzwerk-Controller-Firmware und Speicher-Controller-Firmware

Select Firmware Image: Dies ist eine Liste der Firmware-Images von Drittanbietern, die das System bei diesem Startvorgang zu laden versucht hat. Wählen Sie ein Image und anschließend „Export“ aus, um den SHA-256-Hash-Wert des Image in eine Datei zu schreiben.
Export Selected Entry: Schreiben des ausgewählten Datenbankeintrags in eine Datei

</td></tr>
</table>

Mindestkonfiguration für POST

Die im Folgenden aufgeführten Komponenten sind die Mindestkonfiguration für POST:

- Ein Netzteil
- Systemplatine
- Ein Prozessor in Sockel Prozessor 1
- Stromzwischenplatine (PIB) und Kabel
- Ein Speichermodul (DIMM) in Sockel A1 installiert

PSU – Technische Daten

Das PowerEdge R450-System unterstützt bis zu zwei Wechselstrom- oder Gleichstromnetzteile (PSUs).

Tabelle 7. PowerEdge R450 – Technische Daten für Netzteile

Stromversorgungseinheit	Klasse	Wärmeabgabe (maximal)	Frequency (Speicherta ktrate)	Spannung	Wechselstrom (AC)		Gleichstrom (DC)	Strom
					Hohe Netzspannung 200–240 V	Niedrige Netzspannung 100–120 V		
1100 W Gleichstrom	-	4265 BTU/h	-	-48–(-60) V	-	-	1100 W	27 A
800 Wim gemischten Modus	Platin	3.000 BTU/h	50/60 Hz	100-240 V Wechselstrom, autom. Bereichseinstellung	800 W	800 W	-	9,2–4,7 A
	-	3.000 BTU/h	-	240 V Gleichstrom	-	-	800 W	3,8 A
600 W im gemischten Modus	Platin	2250 BTU/h	50/60 Hz	100-240 V Wechselstrom, autom. Bereichseinstellung	600 W	600 W	-	7,1–3,6 A
	-	2250 BTU/h	-	240 V Gleichstrom	-	-	600 W	2,9 A
700 W im gemischten Modus	Titan	2.625 BTU/h	50/60 Hz	200 bis 240 VAC	700 W	-	-	4,1 A
	-	2.625 BTU/h	-	240 V Gleichstrom	-	-	700 W	3,4 A
1.100 W im gemischten Modus	Titan	4.125 BTU/h	50/60 Hz	100-240 V Wechselstrom	1100 W	1050 W	-	12 A–6,3 A
	-	4.125 BTU/h	-	240 V Gleichstrom	-	-	1100 W	5,2 A

ANMERKUNG: Dieses System ist außerdem für den Anschluss an IT-Stromsysteme mit einer Außenleiterspannung von höchstens 240 V konzipiert.

ANMERKUNG: Die Wärmeabgabe berechnet sich aus der Wattleistung des Netzteils.

ANMERKUNG: Verwenden Sie beim Auswählen und Aufrüsten der Systemkonfiguration den Dell Energy Smart Solution Advisor unter **Dell.com/ESSA**, um den Stromverbrauch des Systems zu prüfen und eine optimale Energienutzung zu gewährleisten.