# Signed BIOS Firmware Update

## Important Information

This document provides information on the Signed BIOS update feature supported on the following Dell PowerEdge systems:

- R910
- R210 II
- T110 II

**NOTE:** By default, the Signed BIOS update feature is enabled on the 12th generation PowerEdge systems.

## Signed BIOS Update Firmware Feature

Signed BIOS update is a feature with digital signature that is authenticated by a public key and has a built-in feature to prevent unauthorized BIOS modifications. These BIOSes are designed and implemented as outlined by the National Institute of Standards and Technology (NIST) under the BIOS Protection Guidelines known as *Special Publication 800-147*.

Signed BIOS update provides enhanced protection features like authentication updates, firmware locking, and non-bypassability.

By default, this option is disabled in the BIOS settings. Once enabled, this feature cannot be disabled and back-flash to a non-NIST compliant BIOS is also not allowed.

Table 1 lists the minimum BIOS version that supports the Signed BIOS update feature on the respective PowerEdge systems.

**Table 1. BIOS Versions That Support The Signed BIOS Update Feature**

| PowerEdge System | BIOS Version |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# System Setup Options Update

Table 2 lists the new feature of the BIOS settings under the **System Security** screen.

**Table 2. System Security Screen Option**

| Option | Description |
|---|---|
| Signed BIOS Update | Allows you to enable the Signed BIOS update feature on the system. By default, this option is disabled.<br>**NOTE:** Currently, this feature is supported on PowerEdge R910, R210 II, and T110 II 11G systems only. |

# Enabling The Signed BIOS Update Feature

You can enable Signed BIOS update on your system during the BIOS setup or using the Unified Server Configurator (USC).

## Enabling The Signed BIOS Update From The BIOS Setup

1. Press <F2> to enter the system BIOS setup.
2. Navigate to the **System Security** option.

**NOTE:** By default, the **Signed BIOS Update** field is **Disabled**.

3. Select the **Signed BIOS Update** option and press the right arrow key to select **Enabled**.

   A warning message is displayed. Press any key to close the message.
4. Press the right arrow key again to select **Enabled** and press <Enter>.

   The **Signed BIOS Update** feature is enabled.

## Enabling The Signed BIOS Update Using USC

To enable **Signed BIOS Update** on your system using Dell USC-LCE:

1. Navigate to the **System BIOS Settings** page.

**NOTE:** By default, the **Signed BIOS Update** field is **Disabled**.

2 Under **System Security,** from the **Signed BIOS Update** drop-down menu, select **Enabled**.

The **Signed BIOS Update** feature is enabled.

# 签名 BIOS 固件更新

## 重要信息

本文档提供签名 BIOS 更新功能的信息，该更新功能受以下 Dell PowerEdge 系统支持：

- R910
- R210 II
- T110 II

**注**：默认情况下，签名 BIOS 更新功能在第 12 代 PowerEdge 系统上启用。

## 签名 BIOS 更新固件功能

签名 BIOS 更新是一个带数字签名的功能，该功能经公共密钥验证并具有内置的防止未经授权进行 BIOS 修改的功能。这些 BIOS 的设计和实施是依照国家标准技术研究所 （NIST）制定的纲要进行的，根据的是 BIOS 保护指南即*特别公布 800-147*。

签名 BIOS 更新提供了增强的保护功能，如验证更新、固件锁定、和不可旁路性。

**注**：默认情况下，该选项在 BIOS 设置中是禁用的。一旦启用，该功能便不能再被禁用，并且也不允许刷回到符合非 NIST 的 BIOS。

表 1 列出了在各自 PowerEdge 系统上支持签名 BIOS 更新功能的 BIOS 最低版本。

**表 1。 支持签名 BIOS 更新功能的 BIOS 版本**

| PowerEdge 系统 | BIOS 版本 |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# 系统设置选项更新

表 2 列出了 System Security （系统安全）屏幕下的 BIOS 设置的新功能。

**表 2。 系统安全屏幕选项**

| 选项 | 说明 |
| --- | --- |
| Signed BIOS Update （签名 BIOS 更新） | 允许您在系统上启用签名 BIOS 更新功能。默认情况下，此选项为禁用。<br>**注：当前，该功能仅在 PowerEdge R910、R210 II、和 T110 II 11G 系统上受支持。** |

# 启用签名 BIOS 更新功能

您可以在 BIOS 设置期间或使用 Unified Server Configurator （USC）来在系统上启用签名 BIOS 更新。

## 通过 BIOS 设置来启用签名 BIOS 更新

1. 按 <F2> 进入系统 BIOS 设置。
2. 导航至 System Security （系统安全）选项。

**注：默认情况下， Signed BIOS Update （签名 BIOS 更新）字段为 Disabled （已禁用）。**

3. 选择 Signed BIOS Update （签名 BIOS 更新）选项并按右箭头键以选择 Enabled （已启用）。

   显示一条警告消息。按任意键关闭消息。

4. 再次按右箭头键以选择 Enabled （已启用）并按 <Enter>。

   Signed BIOS Update （签名 BIOS 更新）功能现已启用。

## 使用 USC 启用签名 BIOS 更新

要使用 Dell USC-LCE 启用系统上的 Signed BIOS Update（签名 BIOS 更新）：

1. 导航至 System BIOS Settings （系统 BIOS 设置）页面。

**注：默认情况下，Signed BIOS Update （签名 BIOS 更新）字段为 Disabled （已禁用）。**

2. 在 System Security（系统安全）下，从 Signed BIOS Update（签名 BIOS 更新）下拉菜单，选择 Enabled （已启用）。

   Signed BIOS Update （签名 BIOS 更新）功能现已启用。

# Mise à jour de micrologiciel BIOS signée

## Informations importantes

Ce document contient des informations sur la fonction de mise à jour du BIOS signée prise en charge sur les systèmes Dell PowerEdge suivants :

- R910
- R210 II
- T110 II

**REMARQUE :** par défaut, la fonction de mise à jour du BIOS signée est activée sur les systèmes PowerEdge de 12e génération.

## Fonction de micrologiciel de mise à jour du BIOS signée

La mise à jour du BIOS signée est une fonction dotée d'une signature numérique qui est authentifiée par une clé publique et possède une fonction intégrée pour empêcher les modifications du BIOS non autorisées. Ces BIOS sont conçus et implémentés tel que défini par le NIST ?(National Institute of Standards and Technology - Institut national des normes et de la technologie) sous les Consignes de protection du BIOS connues sous le nom de *Special Publication 800-147*.

La mise à jour BIOS signée fournit des fonctions de protection optimisées telles que des fonctions d'authentification, le verrouillage de micrologiciel et le non contournement.

**REMARQUE :** par défaut, cette option est désactivée dans les paramètres du BIOS. Une fois activée, cette fonction ne peut pas être désactivée et le retour (back-flash) à un BIOS non conforme au NIST n'est pas autorisé.

Tableau 1 répertorie la version BIOS minimale qui prend en charge la fonction de mise à jour BIOS signée sur les systèmes PowerEdge respectifs.

**Tableau 1. Versions du BIOS qui prennent en charge la fonction de mise à jour BIOS signée**

| Système PowerEdge | Version du BIOS |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# Mise à jour des options de configuration du système

Le Tableau 2 répertorie la nouvelle fonction des paramètres du BIOS sous l'écran **Sécurité du système**.

**Tableau 2. Option de l'écran Sécurité du système**

| Option | Description |
|---|---|
| Mise à jour du BIOS signée | Vous permet d'activer la fonction de mise à jour du BIOS signée sur le système. Par défaut, cette option est désactivée.<br>**REMARQUE :** actuellement, cette fonction est prise en charge uniquement par les systèmes PowerEdge R910, R210 II et T110 II 11G. |

# Activation de la fonction de mise à jour du BIOS signée

Vous pouvez activer la mise à jour du BIOS signée sur votre système lors de la configuration du BIOS ou de l'utilisation de l'USC (Unified Server Configurator - Configurateur de serveur unifié).

## Activation de la mise à jour du BIOS signée à partir de la configuration du BIOS

1. Appuyez sur <F2> pour accéder à la configuration du BIOS système.
2. Naviguez jusqu'à l'option **Sécurité de système**.

**REMARQUE :** par défaut, le champ **Mise à jour du BIOS signée** est **Désactivé**.

3 Sélectionnez l'option **Mise à jour du BIOS signée** et appuyez sur la touche flèche droite pour sélectionner **Activé**.

Un message d'avertissement s'affiche. Appuyez sur n'importe quelle touche pour fermer le message.

4 Appuyez sur la touche flèche droite pour sélectionner **Activé** et appuyez sur <Entrée>.

La fonction **Mise à jour du BIOS signée** est activée.

## Activation de la mise à jour du BIOS signée à l'aide d'USC

Pour activer la **Mise à jour du BIOS signée** sur votre système à l'aide de Dell USC-LE :

1 Naviguez jusqu'à la page **Paramètres BIOS du système**.

**REMARQUE :** par défaut, le champ **Mise à jour du BIOS signée** est **Désactivé**.

2 Sous **Sécurité de système**, du menu déroulant **Mise à jour du BIOS signée**, sélectionnez **Activé**.

La fonction **Mise à jour du BIOS signée** est activée.

# Signierte BIOS-Firmware-Aktualisierung

## Wichtige Informationen

Dieses Dokument enthält Informationen zur signierten BIOS-Aktualisierungsfunktion, die von den folgenden Dell PowerEdge-Systemen unterstützt wird:

- R910
- R210 II
- T110 II

**ANMERKUNG:** Standardmäßig ist die signierte BIOS-Aktualisierungsfunktion auf den PowerEdge-Systemen der 12. Generation aktiviert.

## Signierte BIOS-Firmware-Aktualisierungsfunktion

Die signierte BIOS-Aktualisierung ist eine Funktion mit digitaler Signatur, die durch einen öffentlichen Schlüssel authentifiziert wird und zudem eine integrierte Funktion enthält, die nicht-freigegebene BIOS-Änderungen verhindert. Diese BIOSe sind entworfen und durchgeführt, wie durch das National Institute of Standards and Technology (NIST) unter den BIOS-Schutzrichtlinien dargelegt, bekannt als *Special Publication 800-147*.

Die signierte BIOS-Aktualisierung enthält erweiterte Schutzfunktionen wie Aktualisierungen der Authentifizierung, Firmware-Verriegelungen und Verhinderung von Umgehungsversuchen.

**ANMERKUNG:** Standardmäßig ist diese Option in den BIOS-Einstellungen deaktiviert. Wurde diese Funktion einmal aktiviert, so kann sie nicht mehr deaktiviert werden. Das Zurücksetzen auf ein nicht-NIST(National Institute of Standards and Technology) - kompatibles BIOS ist ebenfalls nicht gestattet.

Tabelle 1 listet die minimale BIOS-Version auf, die die signierte BIOS-Aktualisierungsfunktion auf den entsprechenden PowerEdge-Systemen unterstützt.

**Tabelle 1. BIOS-Versionen, die die signierte BIOS-Aktualisierungsfunktion unterstützen**

| PowerEdge-System | BIOS Version |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# Aktualisierung der System-Setup-Optionen

Tabelle 2 listet die neue Funktion der BIOS-Einstellungen unter dem Bildschirm **Systemsicherheit** auf.

**Tabelle 2. Bildschirmoption „Systemsicherheit"**

| Option | Beschreibung |
|---|---|
| Signierte BIOS-Aktualisierung | Ermöglicht Ihnen, die signierte BIOS-Aktualisierungsfunktion auf Ihrem System zu aktivieren. Standardmäßig ist diese Funktion deaktiviert.<br>**ANMERKUNG:** Derzeit wird diese Funktion nur von PowerEdge R910-, R210 II- und T110 II 11G-Systemen unterstützt. |

# Aktivieren der signierten BIOS-Aktualisierungsfunktion

Sie können die signierte BIOS-Aktualisierung auf Ihrem System während des BIOS-Setup oder unter Verwendung des Unified Server Configurator (USC) aktivieren.

### So aktivieren Sie die signierte BIOS-Aktualisierung durch das BIOS-Setup

1. Drücken Sie <F2>, um das System-BIOS-Setup aufzurufen.
2. Navigieren Sie zur Option **Systemsicherheit**.

**ANMERKUNG:** Standardmäßig ist das Feld **signierte BIOS-Aktualisierung Deaktiviert**.

3 Wählen Sie die Option **signierte BIOS-Aktualisierung** aus und drücken Sie die rechte Pfeiltaste, um **Aktiviert** auszuwählen.

Es wird eine Warnmeldung angezeigt. Drücken Sie eine beliebige Taste, um die Meldung zu schließen.

4 Drücken Sie erneut die rechte Pfeiltaste, um **Aktiviert** auszuwählen und drücken Sie <Enter>.

Die Funktion **signierte BIOS-Aktualisierung** ist aktiviert.

### Aktivieren der signierten BIOS-Aktualisierung unter Verwendung von USC

So aktivieren Sie die **signierte BIOS-Aktualisierung** auf Ihrem System unter Verwendung von Dell USC-LCE:

1 Navigieren Sie zur Seite **System-BIOS-Einstellungen**.

**ANMERKUNG:** Standardmäßig ist das Feld **signierte BIOS-Aktualisierung Deaktiviert**.

2 Wählen Sie unter **Systemsicherheit** vom Drop-Down-Menü **Signierte BIOS-Aktualisierung Aktiviert** aus.

Die Funktion **signierte BIOS-Aktualisierung** ist aktiviert.

# Signed BIOS ファームウェアアップデート

## 重要情報

本書には、次の Dell PowerEdge システムでサポートされている Signed BIOS アップデート機能についての情報が記載されています。

- R910
- R210 II
- T110 II

**メモ：**Signed BIOS アップデート機能は、第 12 世代 PowerEdge システムではデフォルトで有効化されています。

## Signed BIOS アップデートファームウェア機能

Signed BIOS アップデートは、公開鍵によって認証されたデジタル署名付きの機能で、不正な BIOS 修正を防ぐためのビルトイン機能を備えています。これらの BIOS は、Special Publication 800-147 として知られる BIOS 保護ガイドラインに基づいた米国国立標準技術研究所（NIST、National Institute of Standards and Technology）の概説通りに設計および実装されています。

Signed BIOS アップデートは、認証アップデート、ファームウェアロック、および非バイパス性といった拡張保護機能を提供します。

**メモ：**デフォルトで、このオプションは BIOS 設定で無効化されています。この機能は、一度有効化されると無効化することはできず、NIST 非準拠の BIOS へのバックフラッシュは許可されません。

表 1 は、それぞれの PowerEdge システムにおける Signed BIOS アップデート機能をサポートする最小 BIOS バージョンをリストします。

2012 年 12 月

**表 1　Signed BIOS アップデート機能をサポートする BIOS バージョン**

| PowerEdge システム | BIOS Version（BIOS バージョン） |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# セットアップユーティリティオプションアップデート

表 2 は、**システムセキュリティ** 画面にある BIOS 設定の新機能をリストします。

**表 2　システムセキュリティ画面オプション**

| オプション | 説明 |
|---|---|
| Signed BIOS Update（Singed BIOS アップデート） | システムで Signed BIOS アップデート機能を有効化することができます。このオプションはデフォルトでは無効になっています。<br>**メモ：**現在、この機能は PowerEdge R910、R210 II、および T110 II 11G システムのみでサポートされています。 |

# Signed BIOS アップデート機能の有効化

お使いのシステムの Signed BIOS アップデートは、BIOS セットアップ中に、または Unified Server Configurator（USC）を使用して有効化できます。

## BIOS セットアップからの Signed BIOS アップデートの有効化

1. <F2> キーを押して BIOS セットアップを起動します。
2. **System Security**（システムセキュリティ）オプションに移動します。

**メモ：**デフォルトで、**Signed BIOS Update**（Signed BIOS アップデート）フィールドは **Disabled**（無効）になっています。

3. **Signed BIOS Update**（Signed BIOS アップデート）オプションを選択し、右矢印キーを押して **Enabled**（有効）を選択します。

   警告メッセージが表示されます。任意のキーを押してメッセージを閉じます。
4. 右矢印キーを再度押して **Enabled**（有効）を選択し、<Enter> を押します。

   **Signed BIOS アップデート** 機能が有効化されました。

### USC を使用した Signed BIOS アップデートの有効化

Dell USC-LCE を使用してお使いのシステム上の **Signed BIOS アップデート** を有効化するには、次の手順を実行します。

1 **System BIOS Settings**（システム BIOS 設定）ページに移動します。

**メモ：**デフォルトで、**Signed BIOS Update**（Signed BIOS アップデート）フィールドは **Disabled**（無効）になっています。

2 **Signed BIOS Update**（Signed BIOS アップデート）ドロップダウンメニューの **System Security**（システムセキュリティ）で、**Enabled**（有効）を選択します。

**Signed BIOS アップデート** 機能が有効化されました。

# 서명된 BIOS 펌웨어 업데이트

## 중요 정보

이 문서는 다음의 Dell PowerEdge 시스템을 지원하는 서명된 BIOS 업데이트 기능에 대한 정보를 제공합니다 :

- R910
- R210 II
- T110 II

**주 :** 서명된 BIOS 업데이트 기능이 12 세대 PowerEdge 시스템에서 기본적으로 활성화됩니다 .

## 서명된 BIOS 업데이트 펌웨어 기능

서명된 BIOS 업데이트는 공개 키로 인증된 디지털 서명을 갖춘 기능으로 권한이 없는 BIOS 수정을 막기 위한 기능을 내장하고 있습니다 . 이 BIOS 는 국제 표준 기술 연구소 (NIST) 에서 정한 일명 *특수 간행물 800-147* 이라 불리는 BIOS 보호 지침에 의거하여 고안되고 구현되었습니다 .

서명된 BIOS 업데이트는 인증 업데이트 , 펌웨어 잠금 , 그리고 무관통력 (non-bypassability) 같은 고급 보호 기능을 제공합니다 .

**주 :** 이 옵션은 BIOS 설정에서 기본적으로 사용하지 않습니다 . 이 기능은 일단 활성화되면 비활성화될 수 없으며 비 NIST 준수 BIOS 로의 전환 또한 허락되지 않습니다 .

표 1 은 각 PowerEdge 시스템의 서명된 BIOS 업데이트 기능을 지원하는 최소 BIOS 버전을 나열합니다 .

**표 1. 서명된 BIOS 업데이트 기능을 지원하는 BIOS 버전**

| PowerEdge 시스템 | BIOS 버전 |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# 시스템 설정 옵션 업데이트

표 2 는 **시스템 보안** (System Security) 화면 아래 BIOS 설정의 새 기능을 나열합니다 .

**표 2. 시스템 보안 화면 옵션**

| 옵션 | 설명 |
|---|---|
| 서명된 BIOS 업데이트 | 시스템상의 서명된 BIOS 업데이트 기능을 사용 가능케 합니다 . 이 옵션은 기본적으로 사용하지 않습니다 .<br>**주 :** 최근 이 기능은 PowerEdge 의 R910, R210 II, 그리고 T110 II 11G 시스템만을 지원합니다 . |

# 서명된 BIOS 업데이트 기능 사용

BIOS 설정 중 혹은 통합 서버 구성기 (USC) 를 사용중인 시스템에 서명된 BIOS 업데이트를 사용할 수 있습니다 .

## BIOS 설정에서 서명된 BIOS 업데이트 사용

1. 시스템 BIOS 설정을 입력하기 위해 <F2> 를 누릅니다 .
2. **시스템 보안** (System Security) 옵션을 탐색합니다 .

**주 : 서명된 BIOS 업데이트** (Signed BIOS Update) 필드는 기본적으로 **비활성화** (Disabled) 입니다 .

3. **서명된** BIOS **업데이트** (Signed BIOS Update) 옵션을 선택하고 오른쪽 화살표를 눌러 **활성화** (Enabled) 를 선택합니다 .

   경고 메시지가 표시됩니다 . 아무 키나 눌러 메시지를 닫습니다 .

4. 활성화 (Enabled) 를 선택하기 위해 오른쪽 화살표를 다시 누르고 <Enter> 를 누릅니다 .

   **서명된** BIOS **업데이트** (Signed BIOS Update) 가 활성화됩니다 .

## USC 를 사용하여 서명된 BIOS 업데이트 활성화

Dell USC-LCE 를 사용하여 시스템상에서 **서명된** BIOS **업데이트** (Signed BIOS Update) 를 활성화하려면 :

1. **시스템** BIOS **설정** (System BIOS Settings) 페이지를 탐색합니다 .

**주 : 서명된** BIOS **업데이트** (Signed BIOS Update) 필드는 기본적으로 **비활성화** (Disabled) 입니다 .

2. **서명된** BIOS **업데이트** (Signed BIOS Update) 의 드롭 다운 메뉴의 **시스템 보안** (System Security) 아래의 **활성화** (Enabled) 를 선택합니다 .

   **서명된** BIOS **업데이트** (Signed BIOS Update) 가 활성화됩니다 .

# Actualización de firmware del BIOS firmado

## Información importante

Este documento proporciona información sobre la función de actualización del BIOS firmado compatible con los sistemas Dell PowerEdge siguientes:

- R910
- R210 II
- T110 II

**NOTA:** De manera predeterminada, la función de actualización del BIOS firmado está habilitada en los sistemas PowerEdge de 12º generación.

## Función de firmware de actualización del BIOS firmado

La actualización del BIOS firmado es una función con firma digital autenticada mediante una clave pública y tiene una función incorporada para impedir modificaciones no autorizadas del BIOS. Estos BIOS están diseñados y se implementan como lo indica el National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología - NIST) bajo las BIOS Protection Guidelines (Pautas de protección del BIOS) conocidas como *Special Publication 800-147* (Publicación Especial 800-147).

La actualización del BIOS firmado proporciona funciones de protección mejoradas como las actualizaciones de autenticación, el bloqueo del firmware y la inhabilitación de desvíos.

**NOTA:** De manera predeterminada, esta opción está deshabilitada en la configuración del BIOS. Una vez habilitada, esta opción no se puede deshabilitadar y no se permite actualizar a una versión anterior del BIOS que no esté de conformidad con el NIST.

12/2012

La Tabla 1 muestra la versión del BIOS mínima que admite la función de actualización del BIOS firmado en los respectivos sistemas PowerEdge.

**Tabla 1. Versiones del BIOS que admiten la función de actualización del BIOS firmado**

| Sistema PowerEdge | Versión del BIOS |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# Actualización de las opciones de configuración del sistema

La Tabla 2 muestra la nueva función de la configuración del BIOS bajo la pantalla de **System Security** (Sistema de Seguridad).

**Tabla 2. Opción de la pantalla del Sistema de Seguridad**

| Opción | Descripción |
|---|---|
| Actualización del BIOS firmado | Permite habilitar la función de actualización del BIOS firmado en el sistema. De manera predeterminada, la opción está deshabilitada.<br>**NOTA:** Actualmente, esta función es compatible exclusivamente con los sistemas PowerEdge R910, R210 II y T110 II 11G. |

# Habilitación de la función de actualización del BIOS firmado

Puede habilitar la actualización del BIOS firmado en su sistema durante la configuración del BIOS o utilizando Unified Server Configurator (USC).

## Habilitación de la actualización del BIOS firmado desde la configuración del BIOS

1. Presione <F2> para entrar en la configuración del BIOS del sistema.
2. Desplácese a la opción **System Security** (Sistema de seguridad).

**NOTA:** De manera predeterminada, el campo de la **Signed BIOS Update** (Actualización del BIOS firmado) está **Disabled** (Deshabilitado).

3 Seleccione la opción **Signed BIOS Update** (Actualización del BIOS firmado) y presione la tecla de dirección derecha para seleccionar **Enabled** (Habilitado).

Aparece un mensaje de aviso. Presione cualquier tecla para cerrar el mensaje.

4 Presione la tecla de dirección derecha otra vez para seleccionar **Enabled** (Habilitado) y presione <Intro>.

La función de **Signed BIOS Update** (Actualización del BIOS firmado) está habilitada.

## Habilitación de la actualización del BIOS firmado mediante USC

Para habilitar la **Signed BIOS Update** (Actualización del BIOS firmado) en su sistema mediante Dell USC-LCE:

1 Desplácese a la página de la **System BIOS Settings** (Configuración de BIOS del sistema).

**NOTA:** De manera predeterminada,el campo de **Signed BIOS Update** (Actualización del BIOS firmado) está **Disabled** (Deshabilitado).

2 Bajo **System Security** (Sistema de Seguridad), seleccione **Enabled** (Habilitado) en el menú despegable de la **Signed BIOS Update** (Actualización del BIOS firmado).

La función de **Signed BIOS Update** (Actualización del BIOS firmado) está habilitada.

# İmzalı BIOS Ürün Yazılımı Güncellemesi

## Önemli Bilgiler

Bu belge aşağıdaki Dell PowerEdge sistemlerde desteklenen İmzalı BIOS güncelleme özelliği hakkında bilgi içerir:

- R910
- R210 II
- T110 II

**NOT:** Varsayılan olarak, İmzalı BIOS güncelleme özelliği 12. nesil PowerEdge sistemlerde etkindir.

## İmzalı BIOS Güncelleme Ürün Yazılımı Özelliği

İmzalı BIOS güncelleme, bir ortak anahtar tarafından kimlik doğrulaması yapılmış dijital imzaya sahip bir özelliktir ve yetkisiz BIOS değişikliklerini önlemek üzere yerleşik bir özelliği sahiptir. Bu BIOS'lar, *Özel Yayın 800-147* olarak bilinen BIOS Koruma Esasları altında Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) özetlediği şekilde tasarlanmış ve uygulanmıştır.

İmzalı BIOS güncellemesi; kimlik doğrulama güncellemesi, ürün yazılımı kilitlemesi ve geçilmezlik gibi gelişmiş koruma özellikleri sağlar.

**NOT:** Varsayılan olarak, bu seçenek BIOS ayarlarında devre dışı bırakılmıştır. Bu özellik, etkinleştirildikten sonra devre dışı bırakılamaz ve NIST uyumlu olmayan ve izin verilmeyen BIOS sürümünee geri döndürülemez.

Tablo 1, ilgili PowerEdge sistemlerdeki İmzalı BIOS güncelleme özelliğini destekleyen minimum BIOS sürümünü listeler.

**Tablo 1. İmzalı BIOS Güncellemesi Özelliğini Destekleyen BIOS Sürümleri**

| PowerEdge Sistem | BIOS Version (BIOS Sürümü) |
|---|---|
| R910 | 2.8.2 |
| R210 II | 2.2.3 |
| T110 II | 2.2.3 |

# Sistem Kurulum Seçenekleri Güncellemesi

Tablo 2, **Sistem Güvenliği** ekranı altında, BIOS ayarlarının yeni özelliklerini listeler.

**Tablo 2. Sistem Güvenliği Ekranı Seçenekleri**

| Seçenek | Açıklama |
|---|---|
| İmzalı BIOS Güncellemesi | Sistemde İmzalı BIOS güncellemesi özelliğini etkinleştirmenizi sağlar. Bu seçenek varsayılan olarak devre dışıdır.<br>**NOT:** Bu özellik şu anda yalnızda PowerEdge R910, R210 II ve T110 II 11G sistemlerde desteklenmektedir. |

# İmzalı BIOS Güncelleme Özelliğini Etkinleştirme

Sisteminizdeki İmzalı BIOS güncellemesini BIOS kurulumu sırasında veya Birleştirilmiş Sunucu Yapılandırıcısı'nı (USC) kullanarak etkinleştirebilirsiniz.

## İmzalı BIOS Güncellemesini BIOS Kurulumu'ndan Etkinleştirme

1. Sistem BIOS Kurulumu'na girmek için <F2> tuşuna basın.
2. **Sistem Güvenliği** seçeneğine **gidin**.

**NOT: İmzalı BIOS Güncellemesi** alanı varsayılan olarak **Devre dışıdır**.

3. **İmzalı BIOS Güncellemesi** öğesini seçin ve **Etkin** öğesini seçmek için sağ ok tuşuna basın.

   Bir uyarı iletisi görüntülenir. İletiyi kapatmak için herhangi bir tuşa basın.

4. **Etkin** öğesini seçmek için tekrar sağ ok tuşuna ve ardından <Enter> tuşuna basın.

   **İmzalı BIOS Güncellemesi** özelliği etkinleştirimiştir.

## İmzalı BIOS Güncellemesini USC Kullanarak Etkinleştirme

Sisteminizdeki **İmzalı BIOS Güncellemesini** Dell USC-LCE kullanarak etkinleştirmek için:

1. **Sistem BIOS Ayarları** sayfasına gidin.

**NOT: İmzalı BIOS Güncellemesi** alanı varsayılan olarak **Devre dışıdır**.

2 **Sistem Güvenliği** altındaki **İmzalı BIOS Güncellemesi** açılır menüsünden **Etkin**'i seçin.

**İmzalı BIOS Güncellemesi** özelliği etkinleştirimiştir.