



DELL PowerEdge Server BIOS Security Configuration for Intel Based PowerEdge Servers User Guide

[Home](#) » [Dell](#) » DELL PowerEdge Server BIOS Security Configuration for Intel Based PowerEdge Servers User Guide 



Technologies

Contents

- [1 PowerEdge Server BIOS Security Configuration for Intel Based PowerEdge Servers](#)
- [2 Prefaces](#)
- [3 Protect a PowerEdge server using BIOS](#)
- [4 Detect issues in server configuration and health status](#)
- [5 Recover server to a known state](#)
- [6 Summary](#)
- [7 Documents / Resources](#)
 - [7.1 References](#)
- [8 Related Posts](#)

PowerEdge Server BIOS Security Configuration for Intel Based PowerEdge Servers

Best Practices Guide (BPG)
Dell PowerEdge Server BIOS Security
Configuration Guide (SCG) for Intel based
PowerEdge servers
For 16G Intel-based PowerEdge servers

Abstract

This Dell PowerEdge Best Practices Guide (BPG) describes the BIOS security features that you can use to manage and customize your Dell PowerEdge servers. It also defines the fields used in configuring these attributes and best practices for defining values in each field, where appropriate. August 2023

Revisions

Date	Version	Author	Description
April 12, 2023	V0.1.0	Cecil Sheng	Initial draft based on 15G version.
April 20, 2023	V0.2.0	Cecil Sheng	Reorganized section level of chapter 2. Added section for secure OS/VM configurations.
August 21, 2023	V1.0.0	Cecil Sheng	First official version.

Authors

Cecil Sheng—Firmware Senior Principal Engineer

Ivy Yang—Firmware Senior Engineer

Support—Karthik Sarvi (Information Design and Development)

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [8/21/2023] [Best Practices Guide] [572] Dell PowerEdge Server BIOS Security Configuration Guide (SCG) for Intel based PowerEdge servers | 572

Security Development Lifecycle

Prefaces

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this SCG are not supported by all versions of the software or hardware currently in use. The product Release Notes provides the most up-to-date information about product features. Contact your service provider if a product does not function properly or does not function as described in this SCG.

Where to get help from?

Support, product, and licensing information are available in different sources such as:

- Product information—For product and feature documentation or release notes, go to the respective product documentation page on <https://www.dell.com/poweredgemanuals>.
- Troubleshooting—For information about products, software updates, licensing, and service, visit <https://www.dell.com/support> and locate the appropriate product support page.
- Technical support—For technical support and service requests, visit <https://www.dell.com/support> and go to the Service Requests page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for information about obtaining a valid support agreement or to answer any questions about your account.

Overview of 16G Dell server BIOS security configuration guide for Intel based platforms

Dell PowerEdge servers have featured robust security for several generations, including the innovation of using silicon-based data security. Starting from 15G, we introduced iDRAC Root-of-Trust to authenticate BIOS at higher security level. Dell product team considered several key requirements during the design of 16th generation of PowerEdge servers in response to security threats faced in modern IT environments:

- **Protect**—Protect server during every aspect of lifecycle, including BIOS, firmware, data, and physical hardware.
- **Detect**—Detect malicious cyberattacks and unapproved changes; engage IT administrators proactively.
- **Recover**—Recover BIOS, firmware, and OS to a known good state; securely retire or repurpose servers. Dell PowerEdge servers conform to key industry standards on cryptography and security as elaborated throughout this paper and perform on-going tracking and management of new vulnerabilities. The intended audience for this document includes system administrators who are responsible for maintaining and deploying servers and ensuring that network and infrastructure security best practices are followed.

Note—THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.

This SCG is a reference document. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk/guidance to your local installation and individual environment. It is recommended that you determine the applicability of this information to your individual environments and take appropriate actions. All aspects of this Security Configuration Guide (SCG) are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

1.1 Security Development Lifecycle

Dell has implemented the Security Development Lifecycle process with security as a key element in every aspect of development, procurement, manufacturing, shipping, and support resulting in a Cyber Resilient Architecture in 16G PowerEdge servers.

1.2 Today's threat and Dell server BIOS solution

table 1 :Threat vectors and relevant solutions in Dell PowerEdge servers

Server Platform Layers		
Security Layer	Threat Vector	Dell Solution
Physical server	Server tampering	Physical deterrents
Firmware and software	Firmware corruption, malware injection	<ul style="list-style-type: none"> •iDRAC Root-of-Trust •Silicon-based Root of Trust •Intel Boot Guard •Cryptographically signed and validated firmware
Attestation trust features	Server identity spoofing	<ul style="list-style-type: none"> •TPM •TXT •Chain of trust •THE •SGX
Server Management	Rogue configuration and updates, unauthorized open-port attacks, data leak, and corruption.	<ul style="list-style-type: none"> •iDRAC9 •Persistent memory passphrase

Protect a PowerEdge server using BIOS

2.1 Cryptographically verified Trusted Booting

2.1.1 iDRAC Root-of-Trust (RoT) and Silicon-based Root-of-Trust

Starting from 14G, PowerEdge servers use an immutable, silicon-based Root-of-Trust to cryptographically attest to the integrity of BIOS and iDRAC firmware. This Root-of-trust feature is based on one-time programmable, read-only, public keys that provide protection against malware tampering.

The BIOS boot process leverages the AMD Platform Secure Boot (PSB) technology which verifies that the digital signature of the cryptographic hash of the boot image matches the signature stored in silicon by Dell in factory. A failure to verify results server getting shut down, a user notification in the Lifecycle Controller Log, and the BIOS recovery process can then be initiated by the user. If Boot Guard validates successfully, the rest of the BIOS modules are validated by using a chain of trust procedure until control is handed off to the OS or hypervisor.

Starting from 15G, PowerEdge servers provide even higher security level by introducing iDRAC Root-of-Trust. The iDRAC Root-of-Trust provides a critical trust anchor for authenticating the signatures of Dell firmware update packages (DUPs) including BIOS firmware update.

Let us look at the chain of trust in more detail. The iDRAC Root-of-Trust firstly authenticates specific regions of the BIOS image before it boots the system and start running code from the BIOS module. Each BIOS module contains a hash of the next module in the chain. The key modules in BIOS are the SEC (Security), PEI (Pre-EFI Initialization), DXE (Driver Execution Environment), and BDS (Boot Device Selection). AMD PSB authenticates the SEC module, then SEC validates the PEI module before handing control to it. The PEI module further validates the DXE+BDS modules. At this point, control is handed over to UEFI Secure Boot as explained in the next section.

2.1.2 UEFI Secure Boot Support

PowerEdge servers also support industry standard UEFI Secure Boot which checks the cryptographic signatures of UEFI drivers and other code loaded prior to the OS running. Secure Boot represents an industry-wide standard for security in the pre-boot environment. Computer system vendors, expansion card vendors, and operating system providers collaborate on this specification to promote interoperability. When enabled, UEFI Secure Boot prevents unsigned (that is, untrusted) UEFI device drivers from being loaded, displays an error message, and does not allow the device to function. You must disable Secure Boot to load unsigned device drivers.

In addition, PowerEdge servers offer customers the unique flexibility of using a customized boot loader certificate not signed by Microsoft. This is primarily a feature for administrators of Linux environments that want to sign their own OS boot loaders. Custom certificates can be uploaded using the preferred iDRAC API to authenticate the customer's specific OS boot loader.

The default configuration for Secure Boot is Disabled. To enable Secure Boot, power on the system, press F2, and click System Setup Main Menu → System BIOS → System Security. Set the Secure Boot feature to Enable.

Option	Description
Secure Boot	Enables Secure Boot, where the BIOS authenticates each pre-boot image file by using the certificates in the Secure Boot Policy. By default, Secure Boot is set to Disabled .
Secure Boot Policy	When Secure Boot policy is set to Standard , the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot policy is set to Custom , BIOS uses the user-defined key and certificates. By default, the Secure Boot policy is set to Standard .

Secure Boot Mode	<p>Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, or dbx).</p> <ul style="list-style-type: none"> If the current mode is set to Deployed Mode, the available options are User Mode and Deployed Mode. If the current mode is set to User Mode, the available options are User Mode, Audit Mode, and Deployed Mode. <p>Secure Boot Mode</p>		
		Options	Descriptions
		User Mode	In User Mode , PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes.
		Audit Mode	In Audit Mode , PK is not present. BIOS does not authenticate programmatic update to the policy objects and transitions between modes. The BIOS performs a signature verification on pre-boot images and logs the results in the image Execution Information Table but executes the images whether they pass or fail verification. Audit Mode is useful for programmatic determination of a working set of policy objects.
		Deployed Mode	Deployed Mode is the most secure mode. In Deployed Mode , PK must be installed, and the BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode restricts the programmatic mode transitions.
Secure Boot Policy Summary	Specifies the list of certificates and hashes that Secure Boot uses to authenticate images.		
Secure Boot Custom Policy Settings	Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to Custom .		
Option	Description		
Secure Boot	Enables Secure Boot, where the BIOS authenticates each pre-boot image file by using the certificates in the Secure Boot Policy. By default, Secure Boot is set to Disabled .		

Secure Boot Policy	<p>When Secure Boot policy is set to Standard, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When</p> <p>Secure Boot policy is set to Custom, BIOS uses the user-defined key and certificates. By default, the Secure Boot policy is set to Standard.</p>		
Secure Boot Mode	<p>Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, or dbx).</p> <ul style="list-style-type: none"> If the current mode is set to Deployed Mode, the available options are User Mode and Deployed Mode. If the current mode is set to User Mode, the available options are User Mode, Audit Mode, and Deployed Mode. <p>Secure Boot Mode</p>		
	Options	Descriptions	
	User Mode	In User Mode , PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes.	
	Audit Mode	<p>In Audit Mode, PK is not present. BIOS does not authenticate programmatic update to the policy objects and transitions between modes. The BIOS performs a signature verification on pre-boot images and logs the results in the image Execution Information Table but executes the images whether they pass or fail verification. Audit Mode is</p> <p>useful for programmatic determination of a working set of policy objects.</p>	
	Deployed Mode	Deployed Mode is the most secure mode. In Deployed Mode , PK must be installed, and the BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode restricts the programmatic mode transitions.	
Secure Boot Policy Summary	Specifies the list of certificates and hashes that Secure Boot uses to authenticate images.		
Secure Boot Custom Policy Settings	Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to Custom .		

2.1.3 TPM Support

PowerEdge servers support three versions of TPM:

- ✓ TPM 1.2 FIPS + Common Criteria+ TCG certified (Nuvoton)
- ✓ TPM 2.0 FIPS + Common Criteria+ TCG certified (Nuvoton)

TPM can be used to perform public key cryptographic functions, compute hash functions, generate, manage, & securely store keys, and do attestation. TPM can be used to enable the BitLocker™ hard drive encryption feature in Windows Server 2012 and later versions. TPM is compatible with the remote attestation HyTrust CloudControl solution. Attestation and remote attestation solutions can use the TPM to take measurements at boot time of a server's hardware, hypervisor, BIOS, and OS, and compare them in a cryptographically secure manner against base measurements stored in the TPM. If they are not identical, the server identity may have been compromised and system administrators can disable and disconnect the server either locally or remotely.

TPM is enabled through a BIOS option. It is offered as a Plug-In Module solution, the planar has a connector for this plug-in module. However, after the TPM module is enabled on any Dell PowerEdge 13G server (or later), that physical chip is now permanently tied to that specific server and cannot be moved to any other system. This physical and cryptographic binding ensures that the platform integrity cannot be breached or that the data cannot simply be moved to another platform along with the TPM.

To enable TPM:

1. Power on the system.
2. Press F2 and click System Setup Main Menu → System BIOS → System Security.
3. Set TPM Security from Off to the required state. For TPM 1.2, make sure TPM is activated.

Table 2 TPM 1.2 Setup option information

Option	Description
TPM Security	<p>Note: The TPM menu is available only when the TPM module is installed.</p> <p>Enables you to control the reporting mode of the TPM. The TPM Security option is set to Off by default. You can only modify the TPM Status, and TPM Activation if the TPM Status field is set to either On with Pre-boot Measurements or On without Pre-boot Measurements.</p> <p>When TPM 1.2 is installed, the TPM Security option is set to Off, On with Pre-boot Measurements, or On without Pre-boot Measurements.</p>
TPM Information	Changes the operational state of the TPM. This option is set to No Change by default.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Status	Specifies the TPM status.
TPM Command	<p>Controls the Trusted Platform Module (TPM). When set to None, no command is sent to the TPM. When set to Activate, the TPM is enabled and activated. When set to Deactivate, the TPM is disabled and deactivated. When set to Clear, all the contents of the TPM are cleared.</p> <p>This option is set to None by default.</p>

2.1.4 TPM 2.0 security information

Table 3 TPM 2.0 security information in PowerEdge servers

Option	Description
TPM Security	<p>Note—The TPM menu is available only when the TPM module is installed.</p> <ul style="list-style-type: none"> Enables you to control the reporting mode of the TPM. The TPM Security option is set to Off by default. You can modify only the TPM Status, and TPM Activation if the TPM Status field is set to On. When TPM 2.0 is installed, the TPM Security option is set to Off or On. This option is set to Off by default.
TPM Information	Changes the operational state of the TPM. This option is set to No Change by default.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Hierarchy	<ul style="list-style-type: none"> Enables, disables, or clears the storage and endorsement hierarchies. When set to Enabled, the storage and endorsement hierarchies can be used. When set to Disabled, the storage and endorsement hierarchies cannot be used. When set to Clear, the storage and endorsement hierarchies are cleared of any values, and then reset to Enabled.
TPM Advanced Settings	Specifies TPM Advanced Settings.

2.1.5 Intel TXT support

Intel TXT provides the hardware basis for platform to validate platform trustworthiness during boot. It allows integrity verifications on BIOS, operating system loader, and hypervisor.

Prerequisite

To enable the Intel TXT option, virtualization technology must be set to on. Also, TPM Security must be set to On with Pre-boot Measurements for TPM1.2 and TPM Security must be set to On for TPM2.0.

Steps to enable TXT

1. To enter System Setup, press F2 immediately after powering on or rebooting the server.
2. On the System Setup Main Menu screen, click System BIOS → System Security.
3. On the System Security screen, set the Intel TXT option to On.
4. Save settings and close Setup. Restart the server make the changes effective.

Option	Description
Intel(R) TXT	Enables you to set the Intel Trusted Execution Technology (TXT) option. To enable the Intel TXT option, virtualization technology and TPM Security must be enabled with Pre-boot measurements. This option is set to Off by default.

2.1.6 Signed firmware updates

PowerEdge servers have used digital signatures on firmware updates for several generations to assure that only authentic firmware is running on the server platform. We digitally sign all of our firmware packages using verified cryptography algorithms. The BIOS firmware is protected by SHA-256 hashing signed by a 3072-bit RSA private key. iDRAC will scan firmware updates and compare their signatures to what is expected using the silicon-based Root-of-Trust; any firmware package that fails validation is aborted and an error message is logged into the Lifecycle Log (LCL) to alert IT administrators.

Enhanced firmware authentication is embedded within many 3rd party devices which provide signature validation using their own Root-of-Trust mechanisms. This prevents the possible use of a compromised 3rd party update tool from being used to load malicious firmware into, for example, a NIC or storage drive (and bypassing the use of signed Dell update packages). Many of the 3rd party PCIe and storage devices shipped with PowerEdge servers use a hardware Root-of-Trust to validate their respective firmware updates.

If any firmware in any device is suspected of malicious tampering, IT administrators can rollback many of the platform firmware images to a prior trusted version stored in iDRAC. We keep 2 versions of device firmware on the server—the existing production version (“N”) and a prior trusted version (“N-1”). Furthermore, unsigned image update from production level BIOS image is not allowed.

To update System BIOS, you can download DUP or EFI image files from Dell websites. To ensure the image integrity, the user should check the checksum of downloaded images. Checksum can be found in download page. For example, checksums of a BIOS DUP file are listed as shown in the screen shot below.

File Format:	Update Package for MS Windows 64-Bit.
File Name:	BIOS_CTF4C_WN64_1.2.4_01.EXE
Download Type:	HTTP
File Size:	21.11 MB
Format Description:	Dell Update Packages in native Microsoft Windows 64-bit format do not require that Microsoft WOW64 be installed on the Microsoft Windows Server.

[Download](#)

To ensure the integrity of your download, please verify the checksum value.

MD5:	d408ee392b77cc62cb24283554ee4a53
SHA1:	4cd26e356cc01742e2d6d4205475b49a9bba7764
SHA-256:	f4fe76cf2b978122df9742248ec435d6354937232010bae496a76412579bb76c

2.2 Disable USB ports

The USB ports on a PowerEdge system can be completely disabled to further secure the system. The scope of the USB port disablement can be all ports or only the front ports. For example, setting USB ports to All Ports Off (Dynamic) can protect systems that run production tasks. The USB ports can be temporarily enabled for service purposes when needed.

Table 4 Options to configure USB ports

Option	Description
User Accessible USB Ports	<ul style="list-style-type: none"> Configures the user-accessible USB ports. Selecting Only Back Ports On disables the front USB ports. Selecting All Ports Off disables all front and back USB ports. Selecting All Ports Off (Dynamic) disables all front and back USB ports during POST and front ports can be enabled or disabled dynamically by authorized user without resetting the system. This option is set to All Ports On by default.
	<ul style="list-style-type: none"> When user-accessible USB ports are set to All Ports Off (Dynamic), the Enable Front Ports Only option is enabled.
	<ul style="list-style-type: none"> Enable Front Ports Only: Enables or disables the front USB ports during the OS runtime.
	The USB keyboard and mouse still function in certain USB ports during the boot process, depending on the selection. After the boot process is complete, the USB ports will be enabled or disabled as per the setting.
iDRAC Direct USB Port	<ul style="list-style-type: none"> The iDRAC Direct USB port is managed by iDRAC exclusively with no host visibility. This option is set to ON or OFF. When set to OFF, iDRAC does not detect any USB devices installed in this managed port. By default, this option is set to ON.

2.3 Create a setup password using BIOS

After you receive a PowerEdge server the first thing you must do is to create a BIOS setup password to safeguard the BIOS configurations. To create a password, do the following:

Prerequisites

The password jumper enables or disables the system password and setup password features. It is enabled by default. Ensure that the password jumper is enabled so that the password is effective. For more information about how to use the password jumper on your system, see the “System board jumper settings” section in one of the Installation and Service Manual listed in AppendixC.

NOTE—If the password jumper is set to disabled, the existing system password and setup password are deleted, and you need not provide the system password to boot the system. The server case must be opened to access the password jumper, which will be logged as an intrusion event.

- View the System Setup page by pressing F2 during POST after powering on or restarting the server.
- On the System Setup Main Menu screen, click System BIOS → System Security.
- On the System Security screen, ensure that the password status is set to Unlocked.
- In the Setup Password box, type your system password, and press Enter or Tab. Use the following

guidelines to assign the system password:

- A password can have up to 32 characters.
- A password can be a combination of alphabets, numbers, and symbols.

A message prompts you to reenter the system password.

9. Reenter the setup password and click OK.

10. Press Esc to return to the System BIOS screen. Press Esc again.

A message prompts you to save the changes.

NOTE—The Password protection feature will not be effective until the server is restarted.

2.4 Operating with setup password enabled

If the setup password is set to Enabled, enter the correct setup password before modifying the System Setup options. If you do not enter the correct password in three attempts, the system displays the following message:

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

Even after you power off and restart the server, the message is displayed until the correct password is entered. The following options are exceptions:

- If the system password is not set to Enabled and is not locked through the Password Status option, you can assign a system password.
- You cannot disable or change an existing system password.

NOTE—You can use the password status option with the setup password option to protect the system password from unauthorized changes.

2.5 Using your system password to secure your system

If a system password is assigned, during every boot it must be entered to continue booting. The system accepts your setup password as an alternate system password. To configure a system password, do the following.

Steps

1. Power on or restart the server.
2. Enter the server password and press Enter.

Next steps

When the password status is set to Locked, enter the server password and press Enter when prompted during restarting.

Note—If an incorrect system password is entered, the system displays a message and prompts you to reenter your password. You will have three attempts to type the correct password. After the third unsuccessful attempt, the server displays a message that the server has stopped functioning and must be powered off.

During the next restart operation, the correct password is still required to continue the boot process.

2.6 Delete or change system and setup password

NOTE—You cannot delete or change an existing system or setup password if the password status is set to Locked.

1. Press F2 during the POST after powering on or restarting server.
2. On the System Setup page, on the System Setup Main Menu screen, click System BIOS → System Security.
3. On the System Security screen, ensure that the password status is set to Unlocked.
4. Select the password you want to change or disable, then press Enter. To delete a password, leave the box empty.
 - If you change a password, a message prompts you to reenter the new password.

- If you delete a password, a message prompts you to confirm the deletion.
5. Press Esc to return to the System BIOS screen.
 6. Press Esc again, and a message prompts you to save the changes.

2.6.1 Lock or unlock a server setup password

Password status allows an administrator to maintain a setup password to protect against unauthorized BIOS Setup changes, while a user can freely change the system password.

Table 5 Lock or unlock the server setup password

Option	Description
Password status	When set to Unlocked , the system password can be changed without entering the setup password.
	When set to Locked , the setup password must be entered to change the system password. To prevent the system password
	from being modified without providing the setup password, set this option to Locked and enable the setup password.

2.7 Persistent memory passphrase

The purpose of AEP security is to protect data located in the persistent memory region of an AEP DIMM. The data is secured (no read or write access) if the passphrase in the DIMM is set by the user/administrator. The passphrase is stored encrypted. After a system reset, the data is inaccessible until or unless the Dell AEP Security driver unlocks the DIMM with the correct passphrase. Note that the user does not need re-enter the passphrase at this point. The DIMMs are unlocked automatically by BIOS if passphrase is correct. The threat model that the AEP passphrase protects against is physically removing AEP DIMMs from a target system, installing those DIMMs into another system, and accessing the persistent memory data.

Note that the persistent memory passphrase must be safeguarded, and all data stored in the persistent memory DIMMs be backed up. If persistent memory DIMMs are moved from one system board to another, then the user must re-enter the persistent memory passphrase in BIOS Setup. Else, all persistent memory DIMMs' contents will be lost.

The Dell AEP Security BIOS feature provides the following functionality:

- A Setup option "Persistent Memory Passphrase" to set/change/remove the AEP
- Freeze all AEP DIMMs before booting the OS

The following section explains how to use persistent memory passphrase.

The Setup option allows the user to set, change, or delete the AEP Passphrase. The user enters an AEP Passphrase string (a maximum of 32 characters). Note that all Persistent Memory DIMMs with and without a persistent memory region are affected if the passphrase is modified. Entering an empty passphrase will delete the passphrase and disable security in the AEP DIMMs.

Prerequisite

The setup option "Persistent Memory Passphrase" field is available only if at least one AEP DIMM is present in the ACPI NFIT.

Steps

1. To enter System Setup, press F2 immediately after powering on or restarting the server.
2. On the System Setup Main Menu screen, click System BIOS > Memory Settings > Persistent Memory > Intel Persistent Memory.

3. In Persistent Memory Passphrase option, set, change, or remove the AEP passphrase. A passphrase can have up to 32 characters. A passphrase can be a combination of alphabets, numbers, and symbols.
4. Save settings and exit Setup. Restart the server to the changes become effective.

If a secured AEP DIMM fails to unlock, BIOS displays an error message, saves it in the log data, and pauses the operation at the F1 or F2 prompt. The following message and recommended response action is displayed:

Message

The data in the Persistent Memory DIMM located in memory slot <slot label> is not accessible because the DIMM is locked, and the passphrase is incorrect.

Recommended Response Action

Update the Persistent Memory Passphrase to the correct passphrase or perform a Secure Erase operation on the Dual in-line Memory Module (DIMM). Secure erase will erase all persistent data.

2.8 UEFI Variable Access

UEFI variables are where various system configurations stored. Some variables are essential and critical to the system security. Limiting the access (write-protected) is a PowerEdge feature that protects those UEFI variables from malicious changes.

The BIOS setup item “UEFI Variable Access” controls the access of essential UEFI variables:

- “Standard” is the default setting. All access to UEFI variables follows the official UEFI specification.
- “Controlled” enables the write protection. UEFI variables listed below cannot be modified in the OS.

Note—The following EFI variables will be write-protected when the BIOS attribute UefiVariableAccess is set to the Controlled mode.

Table 6 Protect UEFI variables

EFI Variable Name	EFI Variable GUID
L"BootNext"	EFI_GLOBAL_VARIABLE
L"DriverOrder"	EFI_GLOBAL_VARIABLE
L"ConIn"	EFI_GLOBAL_VARIABLE
L"ConOut"	EFI_GLOBAL_VARIABLE
L"BootState"	EFI_GLOBAL_VARIABLE
L"ReserveMemFlag"	EFI_GLOBAL_VARIABLE
L"UefiOptimizedBoot"	{0x356471b1, 0xb483, 0x42ae, 0xb6, 0xe7, 0x3b, 0x2e, 0xba, 0xb1, 0x4e, 0x15}

Note—Setting UEFI Variable Access to “Controlled” may break Linux DUP. If a Linux DUP attempts to write to variables such as “BootNext”, it will not work. This is an expected behavior because the you opted for the extra protection. You can still upload the Linux DUP to iDRAC to update a firmware.

2.9 Enable UEFI Variable Access control

1. Press F2 during the POST after powering on or restarting the server.
2. On the System Setup Main Menu screen, click System BIOS → System Security.
3. Enable UEFI Variable Access by setting it to Controlled.
4. Save settings and close the BIOS Setup page. Ensure that you restart the server so the changes become

effective.

2.10 Intel Total Memory Encryption and Multi-Tenant

Intel Total memory encryption (TME) enables memory pages across system to be encrypted. When used with a single key, no software code modification is required. It uses the NIST standard AES-XTS algorithm with 128-bit keys, or 256-bit keys depends on availability and selection of algorithm. The key for encrypting the entire memory physical memory of the system comes from hardware random number generator in Intel SoC. It is also ensured that the key is not accessible to software or using external interfaces to Intel SoC. TME-MT uses the same hardware architecture with TME. The difference is that it allows multiple keys to be used.

Prerequisite

Platform must meet certain requirements before Total Memory Encryption can be enabled:

- Processor must be Total Memory Encryption capable.

Steps for enabling Memory Encryption

1. To enter System Setup, press F2 immediately after powering on or restarting the server.
2. On the System Setup Main Menu screen, click System BIOS > System Security.
3. Enable “Memory Encryption” by setting it to either “Single Key” or “Multiple Key”.
4. Save settings and exit Setup. Restart the server to make the changes effective.

Table 7 Memory Encryption setup options

Option	Description
Intel® Memory Encryption	<p>Enables or disables the Intel Total Memory Encryption (TME and TME-MT). When option is set to Disabled, BIOS disables both TME and TME-MT technology. When option is set to Single Key, BIOS enables the TME technology. When set to Multiple Keys, BIOS enables the TME-MT technology.</p> <p>This option is set to Disabled by default.</p>

2.10.1 Intel Software Guard Extensions

Dell PowerEdge servers support Intel® Software Guard Extensions (Intel® SGX) CPU instructions and platform enhancements. It allows software to protect its sensitive information by creating secure enclave.

With significantly smaller trusted computing base, software sensitive information is protected from hardware or software attacks even if OS ring0 and BIOS/SMM are compromised. It also helps prevent memory snooping by keeping the secure perimeter to CPU package boundary. In other words, code and data are encrypted outside of CPU package so external memory read only sees encrypted code and data. During the Initial Platform Establishment boot flow, the BIOS checks the key blobs for each CPU package to

verify that they are all consistent with each other and the platform. Microcode sees that there are no key blobs provided and generates new platform keys. The new platform keys are randomly generated for this platform instance. Each CPU package uses its HW key to encrypt the shared platform keys and generate a key blob.

BIOS stores the key blobs in flash for future boots. Microcode also generates a new platform manifest for the new platform instance. BIOS provides the new platform manifest to software via the SGXRegistrationServerRequest UEFI variable and indicates that a registration flow is required using the SGXRegistrationStatus UEFI variable. The registration authority service must evaluate the new platform manifest before it can generate any PCK Certificates for the new platform.

Prerequisite

Platform must meet certain requirements before SGX can be enabled:

- Processor must be SGX capable.
- Memory population must be compatible. Minimum configuration is 8 identical DIMMs per CPU socket (DIMM1

to DIMM8). See the following table.

- Memory operating mode must be set to the Optimizer mode.
- Memory encryption must be enabled.
- Node interleaving must be disabled.

DDR4	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1
8	DDR4		DDR4		DDR4		DDR4		DDR4		DDR4		DDR4		DDR4	
12	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	
16	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4

Note: This diagram is for platforms that have two DIMMs per channel. Some platforms might have only one DIMM per channel. In that case, SGX supported configuration will be fully populated.
 Steps for enabling SGX

1. To enter System Setup, press F2 immediately after powering on or restarting the server.
2. On the System Setup Main Menu screen, click System BIOS > System Security.
3. Enable “Intel SGX” by setting it to “On”.
4. Set “PRMRR size” to desired size. After the next boot operation, BIOS will try to allocate one PRMRR with selected “PRMRR size” per NUMA/Sub NUMA domain.
5. Save settings and exit Setup. Restart the server to make the changes effective.

Table 8 SGX setup options

Option	Description
Intel® SGX	Enables you to set the Intel Software Guard Extension (SGX) option. This option is set to Off by default. When this option is to Off , BIOS disables the SGX technology. When this option is to On , BIOS enables the SGX technology.

SGX Package Info In- Band Access	<p>Enables you to access the Intel Software Guard Extension (SGX) package info in-band option. This option is set to Off by default.</p> <p>Each CPU package on the platform has a key blob when SGX is enabled on a multi-package platform.</p> <p>BIOS provides a mechanism for retrieving the key blobs. Platform owners may want to maintain a copy of the key blobs in case they need to be restored after they are deleted from BIOS persistent store (e.g. the FLASH was erased or SGX was reset). The <i>SgrRegistrationPackageInfo</i> UEFI variable provides the key blobs.</p> <p>By default, BIOS does not present the key blobs to the software. The platform owner needs to 'opt-in' by enabling this option before BIOS provides the key blobs.</p>
PPMRR Size	<p>Sets the PPMRR size.</p> <p>PPMRR stands for Processor Reserved Memory Region Registers. It defines the Enclave Page Cache size for SGX application execution. System BIOS would try to allocate the PPMRR. The allocation is based on current memory map, memory DIMM population, and PPMRR allocation rules. In some configurations, BIOS may not be able to allocate PPMRR or PPMRR may be less than expected.</p>
SGX QoS	<p>Enables or disables the SGX quality of service.</p> <p>When Intel® SGX QoS is enabled, the processor reserves LLC cache for EPC to increase secure enclave performance at the cost of other workload performance.</p>
Select Owner EPOCH input type	<p>Enables you to select Change to New random Owner EPOCHs or Manual User Defined Owner EPOCHs. Each EPOCH is 64-bit. After generating new EPOCH by selecting Change to New random Owner EPOCHs, the selection reverts to Manual User Defined Owner EPOCHs.</p> <p>Software Guard Extensions Epoch n: Sets the Software Guard Extensions Epoch values.</p>
Enable writes to SGXLEPUBLICKEYHASH[3:0] from OS/SW	<p>Enables or disables the Enable writes to SGXLEPUBLICKEYHASH[3:0] from OS/SW.</p> <p>SGX LE Public Key Hash0: Sets the bytes from 0-7 for SGX Launch Enclave Public Key Hash.</p> <p>SGX LE Public Key Hash1: Sets the bytes from 8-15 for SGX Launch Enclave Public Key Hash.</p>

	SGX LE Public Key Hash2 : Sets the bytes from 16-23 for SGX Launch Enclave Public Key Hash.
	SGX LE Public Key Hash3 : Sets the bytes from 24-31 for SGX Launch Enclave Public Key Hash.
Enable/Disable SGX Auto MP Registration Agent	Enables or disables the SGX Auto MP Registration . The MP registration agent (MPA) is responsible to register the platform. This option allows the user to enable/disable the MPA from running automatically at OS boot. By default, the MPA does not automatically run at boot.
SGX Factory Reset	When enables, set SGX setup options (except Intel SGX option) back to default. All the key blobs for that platform will be deleted and system will be
	forced to run a new Initial Platform Establishment flow. This option is reset back to Off after factory reset operations are done after reboot. This option is set to Off by default.

2.11 System Management Mode (SMM) SMM Security Mitigation

SMM operations are transparent to operating systems. Over the years, SMM has become a significant attack surface. Numerous SMM security mitigations are therefore introduced to protect from threats. SMM Security Mitigation provides a way for firmware to indicate what specific mitigations are present. Firmware reports these flags to the OS using the Windows SMM Security Mitigation Table (WSMT) defined in the ACPI specification. To enable or disable the SMM, do the following:

1. Press F2 during the POST after powering on or rebooting your system and enter System Setup.
2. On the System Setup Main Menu screen, click System BIOS > System Security.
3. Enable or disable SMM security mitigation with the SMM Security Mitigation setup option.

2.12 HTTPS boot

HTTPS boot is a Dell PowerEdge feature that loads a boot image over the network via HTTPS. The HTTPS server which provides the boot image should be provided by the customer. To set up trusted HTTPS connection, the certificate of the HTTPS server must be imported to the BIOS. During the boot process, the BIOS verifies the certificate against the target HTTPS server. The BIOS only loads the specified boot image when the certificate verification passes.

Prerequisite

A DHCP server, a DNS server, and a HTTPS server are required. The services can all run on the same system depending on your network architecture. Here we don't go into details on the setup and configuration of these servers. The important thing here is to get the root certificate from the HTTPS server so it can be later imported to the PowerEdge server BIOS.

1. Press F2 during the POST after powering on or resarting the server.
2. On the System Setup Main Menu screen, click System BIOS.
3. In System BIOS, click Network Settings.
4. In Network Settings, enable HTTP Device 1/2/3/4 of choice and enter HTTP device settings.
5. In HTTP Device1/2/3/4 Settings, set up HTTP boot based on network environment. Note that for HTTPS boot, the URL must start with "https://". This is also true when URI is obtained through a DHCP server.
6. Click TLS Authentication Configuration.
7. In the current design, TLS mode must be "One Way" for HTTPS.
8. To manage a certificate, click Root Certificate Configuration.
9. On the Root Certificate page, click Import Root Certificate.

10. Select the file system that contains the server root certificate. Currently, Dell supports certificates stored only in an unencrypted DER or PEM format.
11. Select the certificate file to load. For example, click Example.crt.
12. Click Import. A message is displayed indicating that the root certificate is successfully imported.
13. Click OK. The Root Certificate page is displayed.

Detect issues in server configuration and health status

It is critical to be able to detect any abnormality among the configuration, health status, and change events on a server system. It is also important to detect malicious changes to BIOS, firmware, and Option ROMs within the boot and OS runtime process. Proactive polling must be coupled with the ability to send alerts for all events within the system. Logs must provide complete information about access and changes to the server. Most importantly, the server must extend these capabilities to all components.

3.1 Comprehensive monitoring using iDRAC

Rather than depending on OS agents to communicate with managed resources in a server, iDRAC uses a direct side-band path to each device. Dell has leveraged industry standard protocols such as MCTP, NC-SI, and NVMe-MI to communicate to peripheral devices such as PERC RAID controllers, Ethernet NICs, Fibre Channel HBAs, SAS HBAs, and NVMe drives. This architecture is the result of lengthy, multi-year partnerships with industry-leading vendors to provide agent-free device management in our PowerEdge servers. Configuration and firmware update operations also leverage the powerful UEFI and HII features that Dell and our partner's support.

With this capability, iDRAC can monitor the system for configuration events, intrusion events (such as chassis intrusion detection mentioned earlier in this SCG), and health changes. Configuration events are tied directly to the identity of the user that initiated the change, whether it is from a GUI user, API user, or console user.

3.1.1 Lifecycle Log

Lifecycle log is a collection of events that occur in a server over a period. Lifecycle log provides a description of events with timestamps, severity, user ID or source, recommended actions, and other technical information that could come very handy for tracking or alert purposes.

BIOS configuration change is among the various types of information recorded in the Lifecycle Log (LCL):

- Configuration Changes on the system hardware components
- iDRAC, BIOS, NIC, and RAID configuration changes
- Logs of all the remote operations
- Firmware update history based on device, version, and date
- Information about replaced parts
- Information about failed parts
- Event and error message IDs
- Host power-related events
- POST errors
- User login events
- Sensor state change events

Recover server to a known state

Server solutions must support recovery to a known, consistent state as a response to a variety of events:

- Newly discovered vulnerabilities
- Malicious attacks and data tampering
- Corruption of firmware due to memory failures or improper update procedures
- Replacement of server components

- Retiring or repurposing a server

The following sections describe how we respond to new vulnerabilities and corruption issues, and how we recover the server to its original state if necessary.

4.1 Rapid response to new vulnerabilities

Common Vulnerabilities and Exposures (CVEs) are entries for discovered attack vectors that compromise software and hardware products. Timely responses to newly discovered CVEs are critical to Dell Technologies so that we can swiftly assess the exposure and take appropriate action to protect our customers.

When a new security vulnerability is discovered and reported, a new CVE is issued in response. A typical CVE may come from:

- Open-source components such as OpenSSL
- Web browsers and other Internet access software
- A Hardware or firmware component
- Operating systems and hypervisors

Dell Technologies works aggressively to quickly respond to new CVEs in our PowerEdge servers and provide customers timely information including the following:

- Which products are affected
- What remediation steps may be taken
- If needed when updates will be available to address the CVE

4.2 Recover the BIOS state

The BIOS Recovery feature of the PowerEdge servers provides enables rapid recovery when the BIOS image file is corrupted. A special storage area is hidden from run-time software (BIOS, OS, and device firmware).

These storage areas contain pristine and verified images that can be used to recover system functionality.

In rare cases, the BIOS image may be corrupted. It is important to be able to recover BIOS to a working state.

A backup BIOS image is stored in the iDRAC so it can be used to recover the BIOS image if needed. iDRAC orchestrates the entire end-to-end recovery process.

- Automatic BIOS recovery is initiated by iDRAC Root-of-Trust protection.
- On-demand BIOS recovery can be initiated by you using the RACADM or other management tools.

4.3 Roll back a server BIOS firmware

It is recommended to use the latest firmware to ensure the system is running with the up-to-date security fixes. However, there are cases when a rollback to an earlier version is required. In general, you can roll back the BIOS firmware version from only an existing production version “N” to a previous version “N-1”. You can roll back the firmware to the previously installed version (“N-1”) using any of the following methods:

- iDRAC web interface
- Chassis Management Controller (CMC) web interface
- RACADM Command Line Interface (CLI)—iDRAC and CMC
- Lifecycle Controller User Interface (UI)
- Lifecycle Controller-Remote Services

You can roll back the firmware even if the upgrade was previously performed using another interface. For example, if the firmware was upgraded using the Lifecycle Controller UI, you can roll back the firmware using an iDRAC web interface. You can perform firmware rollback for multiple devices with one system reboot.

4.4 Restore a server configuration after hardware servicing

Remediating service events is a critical part of any IT operation. The ability to meet recovery time objectives and recovery point objectives has direct implications on the security of the solution. Restoring server configuration and firmware assures that security policies for server operation are automatically met.

PowerEdge servers provide functionality that quickly restores server configuration in the following situations:

- Individual part replacement
- Motherboard replacement (full server profile backup and restore)
- Motherboard replacement (Easy Restore)

4.4.1 Easy Restore (for Motherboard Replacement)

Motherboard replacements can be time-consuming and affect productivity. iDRAC offers the ability to backup and restore a PowerEdge server's configuration and firmware to minimize the effort needed to replace a failed motherboard. You can back up and restore. There are two methods the PowerEdge server can backup and restore:

- PowerEdge servers automatically backup system configuration settings (BIOS, iDRAC, or NIC), Service Tag, UEFI diagnostics app, and other licensed data to the flash memory. After you replace the motherboard on your server, the Easy Restore feature prompts you to automatically restore this data.
- For a comprehensive backup, you can back up the server configuration, including the installed firmware image files, on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller, and Network Daughter Cards (NDCs), and the configuration settings of those components. The backup operation also includes the hard drive configuration data, motherboard, and replaced parts. The backup operation creates a single file that you can save to a vFlash SD card or network share (CIFS, NFS, HTTP, or HTTPS). This profile backup can be restored anytime by you. Dell recommends that you perform the backup operation for every system profile you think you might want to restore at some point.

4.5 System Erase

At the end of a system's lifecycle, it must be either retired or repurposed. The goal of the System Erase feature is to erase sensitive data and settings so no confidential information is unintentionally compromised. It is a utility in Lifecycle Controller that is designed to erase logs, configuration data, storage data, cache, and any embedded apps. The following devices, configuration settings, and applications can be erased by using the System Erase feature:

- iDRAC is reset to default
- Lifecycle Controller (LC) data
- BIOS
- Embedded diagnostics and OS driver packs
- iSM
- SupportAssist Collection reports
- Additionally, the following components can also be erased:
 - Hardware Cache (clear PERC NVCache)
 - vFlash SD Card (initialize card)
- Data on the following components are cryptographically disposed of by System Erase as described below:
 - SED (Self Encrypting Drives)
 - ISE-only drives (Instant Secure Erase drives)
 - NVM devices (Apache Pass, NVDIMMs) – Available later in 2018
- Also, non-ISE SATA hard drives can be erased using the data overwrite feature.

4.6 Full Power-Cycle

By using the Full Power Cycle feature, the server and all its components are restarted. It drains main and auxiliary power from the server and all components. All data in volatile memory is also erased. A physical Full Power Cycle requires taking out the AC power cable, waiting for 30 seconds, and then putting the cable back. This poses a challenge when working with a remote system. This feature allows you to do an effective Full Power Cycle from iSM, iDRAC GUI, BIOS, or a script. Full Power Cycle takes effect at the next power cycle. The Full Power Cycle feature eliminates the necessity for anyone to be physically present in the data center, thus reducing time to troubleshoot. It can eliminate, for example, any malware that is still memory-resident.

Summary

Data center security is crucial to business success and the security of the underlying server infrastructure is critical. Cyberattacks have the potential for extended system and business downtime, lost revenue and customers, legal damages, and tarnished corporate reputation. To protect, detect, and recover from hardware-targeted cyberattacks, security needs to be built into server hardware design, not added on after the fact.

Dell has been a leader in leveraging silicon-based security to secure firmware and protect sensitive user data in PowerEdge servers for the past two generations. Starting from 15G, the PowerEdge product line features an enhanced Cyber Resilient Architecture that uses iDRAC Root-of-Trust to further harden server security. Furthermore, Dell PowerEdge BIOS also introduced the following new security features to provide users even higher security level:

- Protect production level BIOS image from unsigned image update.
- SMM Security Mitigation feature

In conclusion, the 16G PowerEdge servers, with their industry leading security, form the trusted bedrock of the modern data center upon which customers will securely run their IT operations and workloads.

A Technical support and resources

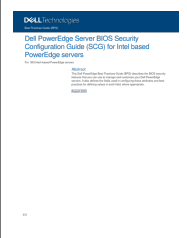
[Dell.com/support](https://dell.com/support) is focused on meeting your requirements with proven services and support.

A.1 Related resources

- Dell PowerEdge R760 Installation and Service Manual: <https://dl.dell.com/content/manual32513608-dellpoweredge-r760-installation-and-service-manual.pdf>

Dell PowerEdge Server BIOS Security Configuration Guide (SCG) for Intel based PowerEdge servers

Documents / Resources

	<p>DELL PowerEdge Server BIOS Security Configuration for Intel Based PowerEdge Servers [pdf] User Guide</p> <p>R760, 16G, PowerEdge Server BIOS Security Configuration for Intel Based PowerEdge Servers, PowerEdge Server BIOS Security Configuration, Intel Based PowerEdge Servers</p>
---	--

References

-  [Support | Dell US](#)
-  [Support | Dell US](#)
-  [Support | Dell US](#)
-  [Computers, Monitors & Technology Solutions | Dell USA](#)

