Dell Technologies

Security Configuration Guide

Dell PowerEdge Server BIOS Security Configuration Guide

For 17G AMD-based PowerEdge servers

Abstract

This PowerEdge server BIOS Security Configuration Guide (SCG) describes the BIOS security features that you can use to manage and customize your PowerEdge servers with AMD processors. It also defines the fields used to configure these attributes and best practices for defining values in each field, where appropriate.

November 2024

Revisions

Date	Version	Author	Description
Nov 13, 2024	V1.0	Cecil Sheng and Ivy Yang	Updated Security Configuration guide for 17th generation PowerEdge servers with AMD processors.

Acknowledgments

Author:

Cecil Sheng—Firmware Senior Principal Engineer

Smith Cheng - Technical Staff, Firmware Engineering

Ivy Yang—Firmware Principal Engineer

Other:

Contents

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

For information about support, product, and licensing, visit the following websites:

- Product information and troubleshooting—For product and feature documentation or Release Notes, go to https://www.dell.com/support and locate the appropriate product support page.
- Technical support—For technical support and service requests, go to https://www.dell.com/support and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

1 Overview

The PowerEdge servers have provided robust security for several generations, including the innovation of using silicon-based data security. Starting from 15G, Dell introduced iDRAC Root-of-Trust (RoT) to authenticate BIOS at a higher security level. The Dell product team has considered several key requirements during the design of 17G PowerEdge servers in response to security threats faced by 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.

The PowerEdge servers conform to key industry standards on cryptography and security as elaborated throughout this technical white paper and perform on-going tracking and management of new vulnerabilities. The intended audience for this document includes system administrators, who are responsible to maintain and deploy servers and ensure that network and infrastructure security best practices are followed.

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 or 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 PowerEdge servers.

1.2 Threat and Dell server BIOS solution

Table 1 Dell server BIOS solution

Security Layer	Threat Vector	Dell Solution
Physical server	Server tampering	Physical deterrents

Firmware and software	Corrupted firmware, malware injection	• iDRAC Root-of-Trust • Silicon-based Root of Trust • AMD Secure Root-of-Trust Cryptographically signed and validated firmware.
Attestation trust features	Server identity spoofing	• TPM • PSB • Chain of trust • DRTM
Server Management	Rogue configuration and updates, unauthorized open-port attacks, data leak, and corruption	• iDRAC9

2 Protect a PowerEdge server using BIOS

2.1 Cryptographically verified Trusted Boot

2.1.1 iDRAC Root-of-Trust and Silicon-based Root-of-Trust

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

The BIOS boot process leverages 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 during manufacturing. A failure to verify results in a shutdown of the server, user notification in the Lifecycle Controller Log, and the BIOS recovery process can then be initiated by the user. If PSB validates successfully, the rest of the BIOS modules are validated by using a chain of trust procedure until control is handed off to the Operating System (OS) or hypervisor.

Starting from 15G, the 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

The PowerEdge servers also support industry standard Unified Extensible Firmware Interface (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 via the preferred iDRAC API to authenticate the customer’s specific OS boot loader.

The default configuration for Secure Boot is disabled. Do the following to enable the Secure Boot:

1. Power on the system.
2. When the company logo is displayed, press F2 to open the **System Setup** page.

3. On the **System Setup Main Menu** page, click **System BIOS → System Security**.
4. To enable the Secure Boot feature, click **Enable**.

Table 2 Options and Descriptions to enable the Secure Boot

Option	Description
Secure Boot	Enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is set to Disabled by default.
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, the BIOS uses the user-defined key and certificates. Secure Boot policy is set to Standard by default.
Secure Boot Mode	Configures how the BIOS uses the Secure Boot Policy Objects: • Platform Key (PK) • Key Exchange Key Database (KEK) • Authorized Signature Database (db) • Forbidden Signature Database (dbx) 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**. • **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.

2.1.3 TPM support

PowerEdge servers support two versions of Trusted Platform Module (TPM):

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

TPM can perform public key cryptographic functions, computing hash functions, generating, managing and securely storing keys, and attestation. TPM can be used to enable the BitLocker™ hard drive encryption feature in Windows Server 2012 and later. TPM is compatible with the remote attestation HyTrust CloudControl solution Attestation and remote attestation systems can employ the TPM to take measurements of a server's hardware, hypervisor, BIOS, and OS during startup time and compare them to base measurements recorded in the TPM in a cryptographically secure way. If they are not the same, the server identity has been compromised, and system administrators can shut and disconnect the server 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, once 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 the data cannot simply be moved to another platform along with the TPM.

Do the following to enable the TPM:

1. Power on the server.
2. When the company logo is displayed, press F2 to open the **System Setup** page.
3. On the **System Setup Main Menu** page, click **System Setup Main Menu** → **System BIOS** → **System Security**.
4. Set the TPM Security status from Off to the required state.

Table 3 TPM 2.0 security information

Option	Description
TPM Security	**Note**—The TPM menu is available only when the TPM module is installed. 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 **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	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.

2.1.4 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 our firmware packages using SHA-384 hashing with 3072-bit RSAPSS encryption for the signature for BIOS. The iDRAC scans the 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 third-party devices which provide signature validation using their own Root-of-Trust mechanisms. This prevents the possible use of a compromised third-party update tool from being used to load malicious firmware. For example, a NIC or storage drive (and bypassing the use of signed Dell update packages). Many of the third 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 roll back many of the platform firmware images to a prior trusted version stored in iDRAC. As an example, keep two versions of device firmware on the server:

- The existing production version (N).
- A prior trusted version (N-1).

Also, an unsigned image file update from production level BIOS image file is not supported. To update the System BIOS, download DUP or EFI image files from Dell websites. To ensure the image file integrity, verify the checksum value of downloaded image files. The Checksum value is displayed on the Download page. For example, the checksum values of a BIOS DUP file are shown in the sample screen shot:

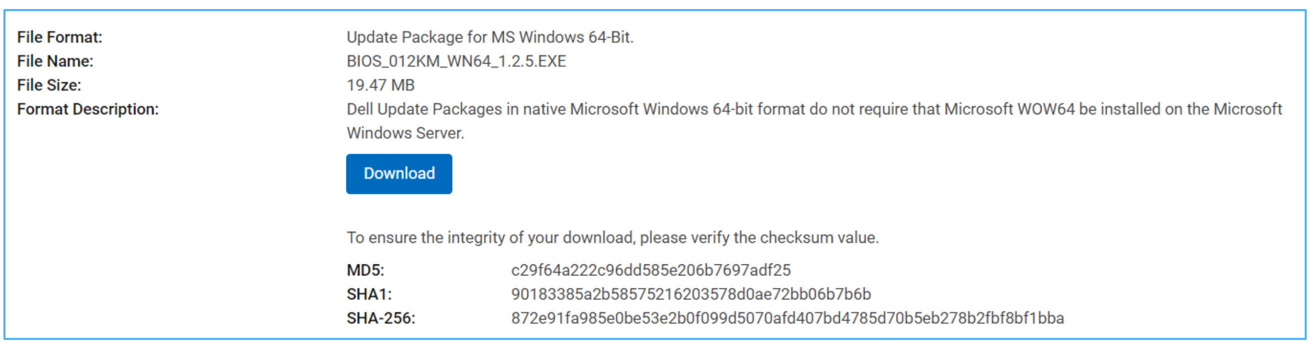

Figure 1 Example of a BIOS DUP files checksum

2.2 Disable USB ports

You can entirely disable USB ports for added protection. You can also disable only the USB ports on the front of the device. USB ports, for example, can be deactivated for production use and then temporarily enabled to allow debugging access to a crash cart. Following are the options to configure USB ports:

Table 4 Options to configure USB ports

Option	Description
User Accessible USB Ports	• 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. When user-accessible USB ports are set to **All Ports Off (Dynamic)**, the **Enable Front Ports Only** option is enabled. • **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	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. This option is set to **ON** by default.

2.3 Create a setup password in BIOS

When you receive a PowerEdge server, you must create a BIOS System Password and a BIOS Setup Password to protect the BIOS and the boot sequence.

Prerequisites

Ensure that the password jumper is enabled. The password jumper enables or disables the system password and setup password features. For how to use password jumper, see the **System board jumper settings** section in the **Installation and Service Manual** of the server.

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.

Do the following to create a system and setup password:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click **System BIOS → System Security**.
3. On the System Security screen, verify that Password Status is set to Unlocked.
4. In the **System Password** field, 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 message prompts you to reenter the system password.
5. Re-enter the system password and click **OK**.
6. In the **Setup Password** field, type your setup password and press Enter or Tab. A message prompts you to reenter the setup password.
7. Re-enter the setup password and click **OK**.
8. 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.

2.3.1 Secure system using system password

If you have assigned a setup password, the system accepts your setup password as an alternate system password.

Do the following to secure the system using password:

1. Power on the system.
2. Type the system password and press **Enter**.

When the **Password Status** is set to **Locked**, type the system password, and press **Enter** when prompted to reboot.

NOTE—If an incorrect system password is typed, the system displays a message and prompts you to re-enter your password. You have three attempts to type the correct password. After the third unsuccessful attempt, the system displays an error message that the system has stopped functioning and must be turned off. Even after you power off and restart the system, the error message is displayed until the correct password is entered.

2.3.2 Delete or change system and setup password

Prerequisites

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

To change or delete the server and setup password, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click **System BIOS → System Security**.
3. On the System Security screen, ensure that Password Status is set to **Unlocked**.
4. In the **System Password** box, alter or delete the existing system password, and then press Enter or Tab.
5. In the **Setup Password** field, alter or delete the existing setup password, and then press Enter or Tab.
6. If you change the system and setup password, a message prompts you to re-enter the new password. If you delete the system and setup password, a message prompts you to confirm the deletion.
7. Press Esc to return to the **System BIOS** screen. Press Esc again. A message prompts you to save the changes.
8. Select **Setup Password**, change or delete the existing setup password and press Enter or Tab.

NOTE—If you change the system password or setup password, a message prompts you to re-enter the new password. If you delete the system password or setup password, a message prompts you to confirm the deletion.

2.3.3 Operating with setup password enabled

If **Setup Password** is set to **Enabled**, type the correct setup password before modifying the system setup options. If you do not type 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 if you turn off and restart the system, the error message is displayed until the right password is entered. There are a few exceptions:

- If 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.

2.3.4 Password status

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 Option for the password status

Option	Description
Password status	**Unlocked**—the system password can be changed without entering the setup password. **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.

2.3.5 Strong password

The strong password support is an enhancement added in 17G PowerEdge servers. You can set a minimum acceptable length to the passwords. Also, if **Strong Password** is enabled, your password must include a combination of uppercase and lowercase letters, numbers, and special symbols.

Table 6 Option for a strong password

Option	Description
Strong password status	Enabled—verifies if the password is strong or not. Disabled—does not verify if the password is strong.
Strong password minimum length	The minimum length of the password. The value must be 8–32 characters.

2.4 UEFI variable access

UEFI variables are used for various system configurations and some variables are very critical and essential. Adding the access restriction (write-protected) is a feature to protect those UEFI variables and mitigate the vulnerability caused by unexpected system configuration.

A BIOS setup item **UEFI Variable Access** is provided to control the access restriction of UEFI variable:

- **Standard**—Default setting indicates the access is based on the definition of UEFI specification.
- **Controlled**—Indicates some specific UEFI variables are protected and cannot be modified in an OS environment.

The following UEFI variables are write-protected when BIOS attribute `UefiVariableAccess` is set to "**Controlled**" mode.

Table 7 List of UEFI variable names and variable GUID

UEFI Variable Name	UEFI 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—The setting `UefiVariableAcces` to **Controlled** may cause Linux DUP support to stop working. For example, if Linux DUP attempts to write to variables such as **BootNext**, those variables are now write-protected. This is expected behavior since the user opted-in to the extra protection.

To control UEFI Variable Access, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your 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 exit Setup. Restart the server to make the updated settings become effective.

2.5 SMM Security Mitigation

System Management Mode (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 indicates what specific mitigations are present. Firmware indicates these flags in an ACPI table called Windows SMM Security Mitigation Table (WSMT).

To enable to disable the SMM security mitigation, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the **System Setup Main Menu** screen, click **System BIOS** → **System Security**.
3. Enable or disable SMM security mitigation with **SMM Security Mitigation** setup option.

2.6 HTTPS boot

HTTPS boot enables you to use HTTP protocol to transfer the boot file over Transport Layer Security protocol to authenticate HTTPS server. To use HTTPS boot on Dell PowerEdge server, you need to setup DHCP server and HTTPS server. After generating the certificate on HTTPS server, you must import the certificate to the PowerEdge server so it can obtain boot file over HTTPS boot process.

Prerequisite

Setup DHCP server, DNS server and HTTPS server. You can setup based on your requirement. Also, get HTTPS server root certificate from HTTPS server so it can be later imported to HTTPS boot client.

To enable the HTTPS boot settings, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server. Ensure that this server receives boot image via HTTPS boot support.
2. On the **System Setup Main Menu** screen, click **System BIOS**.
3. Click **Network Settings**.
4. On the **Network Settings** page, enable HTTP Device 1 through 4 as necessary of your choice, and enter HTTP device settings.

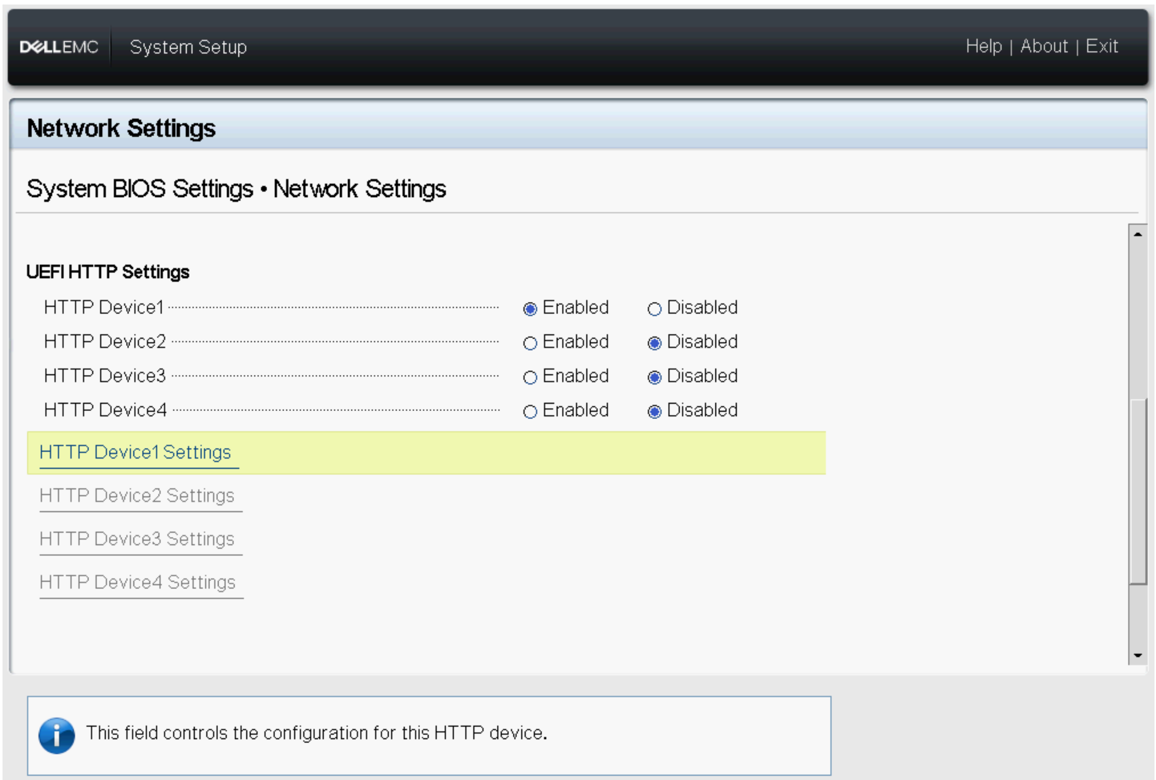

Figure 2 Dell UEFI HTTP settings

5. In **HTTP Device1/2/3/4 Settings**, setup HTTP boot based on network environment. For HTTPS boot, URI should start with `https://`. When the URI is obtained through DHCP server, enter the **TLS Authentication Configuration**.

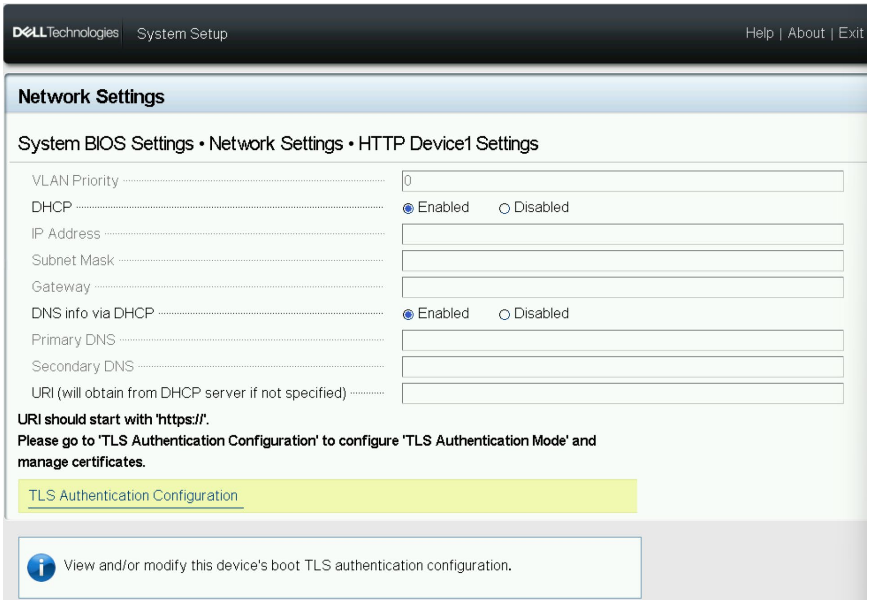

Figure 3 HTTP Device 1/2/3/4 Settings

6. For current design, TLS mode needs to be **One Way** for HTTPS boot. Enter the **Root Certificate Configuration** to manage certificate.

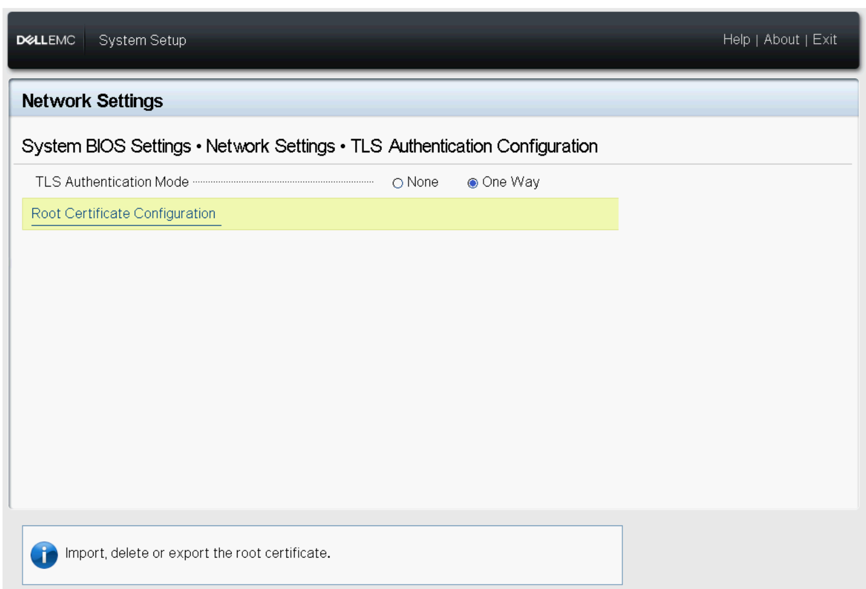

Figure 4 TLS Authentication Configuration

7. On the Root Certificate page, select Import Root Certificate.

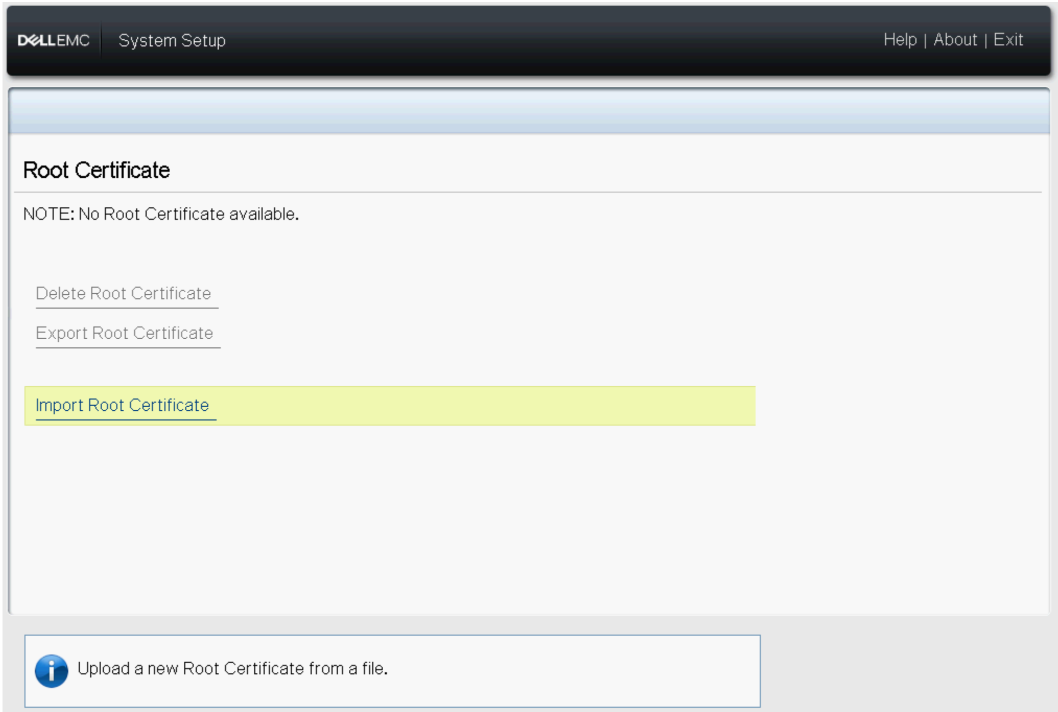

Figure 5 Import Root Certificate page

8. On the **Import Root Certificate** page, select the file system that contains the server root certificate.

Note—DER/PEM are the only supported certificate encoding formats.

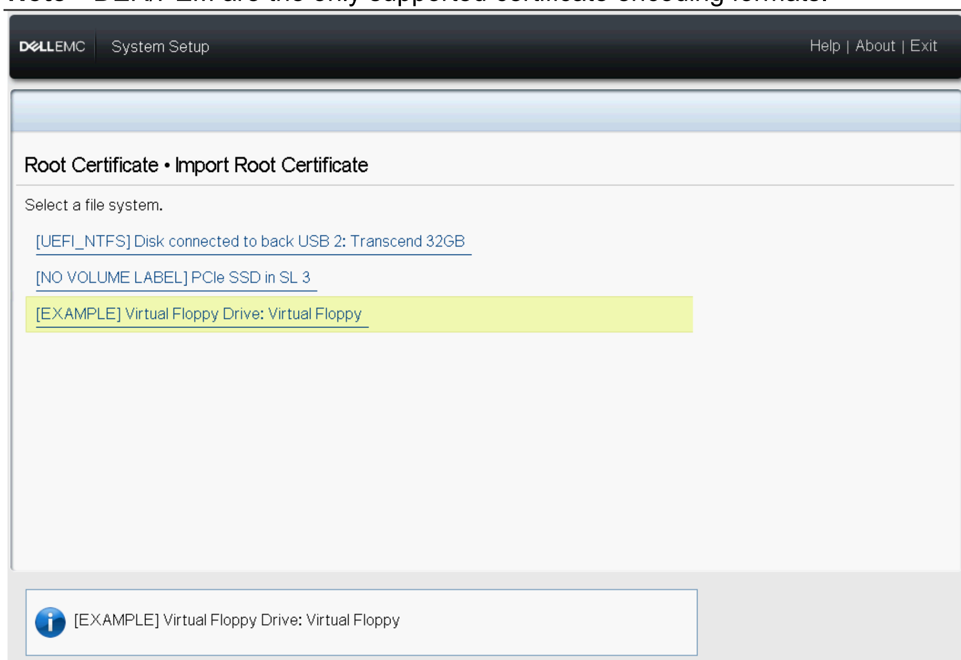

Figure 6 Import Root Certificate

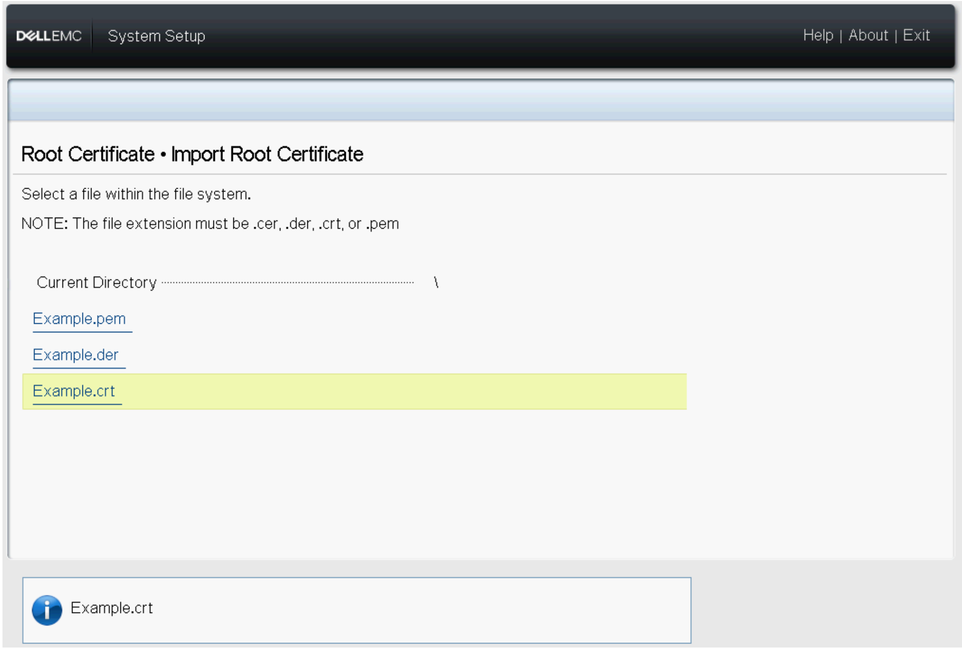

Figure 7 Select cert file in Import Root Certificate

9. Select the certificate of your choice. For example, select **Example.crt** and click **Import**.

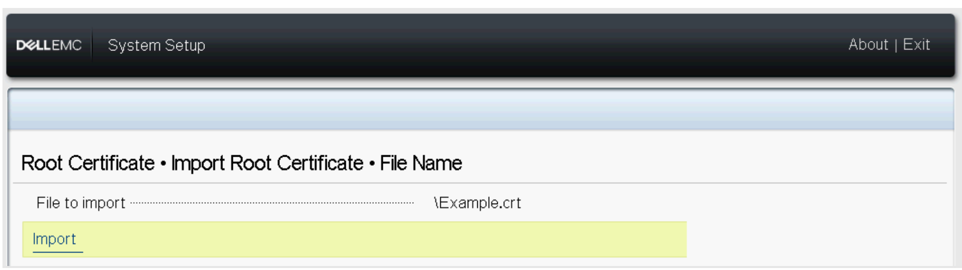

Figure 8 Importing a certificate

After the certificate is imported successfully, system displays the message: `The Root Certificate was imported successfully.`

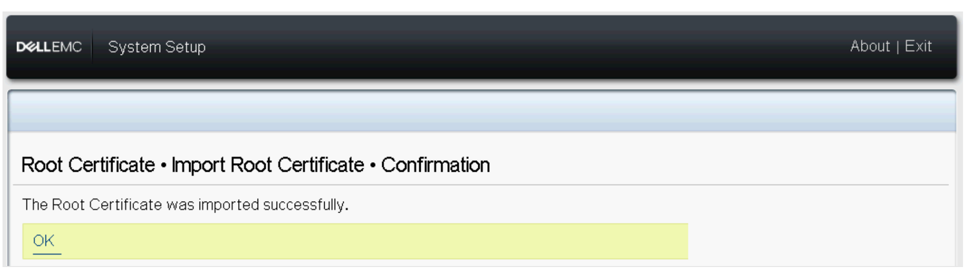

Figure 9 System message to indicate certificate import status

10. Click **OK** to complete the operation and return to the **Root Certificate** page.

3 Detect issues in server configuration and health status

It is critical to detect any issues 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 via iDRAC

Rather than depending upon OS agents to communicate with managed resources in a server, iDRAC employs 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 paper), and health changes. Configuration events are linked directly to the identity of the user who initiates the change, for example, GUI user, API user, or console user.

3.1.1 Lifecycle log

The lifecycle log is a collection of events that occur in the server over a period of time. 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

4 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 to respond to new vulnerabilities and corruption issues, and how to 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 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 enables the 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 image files that can be used to recover system functionality.

In some cases, the BIOS image file may be corrupted. It is important to recover the BIOS to a working state. A backup BIOS image file 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 firmware

It is recommended to use the latest firmware to ensure that 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 server configuration after hardware servicing

To remediate the 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 configuration and firmware to minimize the effort needed to replace a failed motherboard.

There are two ways the PowerEdge server can backup and restore server configurations:

- PowerEdge servers automatically backup system configuration settings (BIOS, iDRAC, NIC), Service Tag, UEFI diagnostics app, and other licensed data to the flash memory. After you replace the motherboard on your server, **Easy Restore** prompts you to automatically restore this data.
- For a more comprehensive backup, you can back up the system 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 disk configuration data, motherboard, and replaced parts. The backup creates a single file that you can save to a vFlash SD card or network share (CIFS, NFS, HTTP or HTTPS).

You can restore this profile backup anytime. 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 lifecycle, it must be either retired or repurposed. The goal of the System Erase feature is to erase sensitive data and settings so that no confidential information is unintentionally compromised. It is a utility in Lifecycle Controller that is designed to erase the 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 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 by System Erase:

- Self-Encrypting Drives (SED)
- Instant Secure Erase drives (ISE)
- NVM devices (Apache Pass, NVDIMMs) – Available later in 2018
- Additionally, non-ISE SATA hard drives can be erased using data overwrite.

4.6 Full Power Cycle

In a Full Power Cycle, the server and its components are rebooted. It drains main and auxiliary power from the server and all components. The data in volatile memory is also erased.

A physical Full Power Cycle requires removing the AC power cable, wait for 30 seconds, and then insert 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.

Full Power Cycle feature eliminates the need 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.

5 Summary

The data center security is crucial to the business success and the security of the underlying server infrastructure. 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 17G PowerEdge servers, with their industry leading security, form the trusted bedrock of the modern data center upon which customers can securely run their IT operations and workloads.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.