Whitepaper

BIOS Security and Manageability – BIOS Configurations

Summary

- With attacks on PCs becoming more prevalent, it's more important than ever to harden the attack surface. Reducing the impact starts with secure BIOS access management.
- BIOS passwords can reduce risk, but current processes can make it challenging for IT admins to manage. This can lead to lax processes in setting and maintaining BIOS passwords.
- Dell recently introduced **Dell Command | Endpoint Configure for Microsoft Intune** which enables IT admins to configure BIOS settings and a unique per-device BIOS password on a fleet of Dell devices – securely, quickly, and natively in Microsoft Intune.
- However, some organizations prefer to bypass BIOS passwords altogether. For these customers, Dell's newest offering is **Dell Command | Secure BIOS Configuration (DCSBC).** With DCSBC, IT admins can securely configure and manage a fleet of Dell client systems' BIOS settings with certificate-based BIOS authentication – no BIOS passwords required.
- With these two recent introductions, Dell leads the commercial PC market with flexible BIOS configuration options that match the various needs of an organization's IT environment.

The need for BIOS security

The "BIOS" in a modern PC remains one of the most misunderstood components of the firmware and software stack. In simple terms, it is the lowest level of the PC stack that ensures successful 'boot up' of the device before it is passed on to the operating system. Because it is both misunderstood and unappreciated, the BIOS is not always discussed when talking about cybersecurity. But the reality in today's world is that attacks will target anywhere that an opportunity exists. And the BIOS most certainly can be attacked. A recent 2023 survey of global IT Decision Makers (ITDMs), conducted by the Futurum Group, reveals that 69% of organizations report a hardware or firmware level attack. That is up 1.5X since their previous study just 3 years prior. So, while discussions of high visibility cyberattacks will not often mention the BIOS, security and IT teams know that it can be a vulnerable target for an attack if not managed properly. When malware owns the BIOS, it owns the PC and access into the network. And since it can be done quite stealthily, a BIOS attack may not be noticed for quite some time since it is not as visible as other targets.

Having established that protecting the BIOS should be an important part of any organization's IT security strategy, what actions can an IT team take to keep the BIOS secure? One key area starts with the basics – managing access. Creating rules and policies to ensure secure management can help to address this potential vulnerability. And NIST has developed guidelines that IT teams can utilize. As a result, BIOS passwords have been a part of this strategy for some time as they inherently can reduce risk. But setting BIOS passwords can be a challenge for any IT team, especially in an era of devices that leave a building and can be anywhere on the globe. Passwords can be hard to manage; or they can be repeated or reused (thus adding inherent risk). In some of the most extreme situations, they may even be abandoned, leaving devices without the security level that a password can provide.

How can an organization successfully maximize the security of BIOS across their fleet of devices? This paper reviews the key challenges for IT admins pertaining to BIOS security and management and introduces two new Dell Command solutions that are designed to address these challenges and keep a fleet of devices' BIOS safe.

The challenges for IT administrators

With threats to the endpoint and the damage they can cause being ever present, the task for IT admins is to find a way to securely manage their fleet level BIOS settings in ways that reduce risk, follow Zero Trust policies, and use methods that are easily and efficiently managed. Dell's two recent product introductions address these challenges while acknowledging the different needs of our customers IT organizations.

The difficulties of setting and maintaining BIOS passwords present a clear need for easier ways to manage BIOS access. In the past, configuring BIOS settings for a fleet of devices was a complex and time-consuming task for IT admins.

Introducing Dell Command | Endpoint Configure for Microsoft Intune

Dell Command | Endpoint Configure for Microsoft Intune (DCEC for Microsoft Intune) addresses the challenge that IT admins face - the inability to have a way to easily configure BIOS settings for a fleet of Dell devices, natively & securely in a Unified Endpoint Management (UEM) console. DCEC enables this all within the Microsoft Intune environment, which is the market leader in UEM.

Dell and Microsoft have developed an Intune-based BIOS configuration solution that is the industry's first Binary Large Object (BLOB) package-based solution for securely configuring & managing endpoints natively in Microsoft Intune.

With DCEC, IT admins can manage Dell client device BIOS configuration as a native Intune function; deploy a unique-per-Dell-client device BIOS password; and report Dell client device BIOS configuration status in Intune.

How Dell Command | Endpoint Configure For Microsoft Intune works

1. The IT Admin deploys DCEC for Microsoft Intune connector service.
2. The admin configures the desired BIOS setting with Dell Command | Configure.
3. The admin then exports the configuration package with the desired BIOS settings.
4. The Microsoft Intune Connector Service receives the configuration package, verifies its integrity, and applies it to the endpoints.
5. The configuration package is then deployed via Microsoft Intune to the endpoints.
6. Last, the Admin imports the configuration package into their Microsoft Intune configuration profile and assigns it to the applicable device group.

With this streamlined, single-pane-of-glass solution, IT admins now have a simplified way of securely deploying BIOS configurations on their fleet of Dell devices.

The benefits of DCEC for Microsoft Intune include:

1. **Reduced Security Risks:** Ensures that secure settings are consistently applied. Minimize the chances for incorrect (or missing) BIOS settings that can expose devices to security vulnerabilities.
2. **Lower Risk of Noncompliance:** Maintains adherence to compliance regulations such as GDPR and HIPAA that mandate data protection as BIOS vulnerabilities can lead to unauthorized access or data breaches.
3. **Greater Compatibility:** BIOS settings must align with the operating system and hardware. Mismatched configurations can lead to compatibility issues thereby impacting productivity.
4. **Improved Management of Legacy Systems:** Managing the BIOS settings for older systems with outdated firmware can be cumbersome and time-consuming as these systems may lack modern management features. DCEC for Microsoft Intune enables fleet level BIOS settings management – including older devices.
5. **Enhanced BIOS Password Management:** For devices using a password, often a single BIOS password is applied to a fleet of devices, which can pose security threats. DCEC enables IT admins to set and maintain a unique password per Dell device.

Modern BIOS management: securing BIOS with a certificate

While BIOS passwords do enable a layer of security, and can be useful for older devices, IT admins still face multiple challenges:

1. **BIOS passwords are still stored:** The simple rule is, "if something is stored, it can be found." This implies that even the most secure BIOS passwords can still be intercepted by others. Because setting and managing passwords can be tedious, often devices have passwords that are weak, reused, or even missing.
2. **BIOS passwords can travel:** Since the SCE (Self Contained Executable) can reside on the device, your password security can be at risk of tampering from anywhere your devices travel.
3. **BIOS passwords can be vulnerable:** Though Dell DCEC enables a unique BIOS password per device, text-based passwords can still be susceptible to brute force attacks. The BIOS/UEFI provides a powerful realm of configuration, control, and access, below the OS, which is a primary target for adversaries.

As a result, some IT organizations are looking to move away from BIOS passwords altogether. Certificate-based authorization is a recent development as PC manufacturers look to move away from passwords and use certificates that address some of the above noted challenges with BIOS passwords.

Dell has recently introduced **Dell Command | Secure BIOS Configuration** (DCSBC) to address the needs of these customers. The following section summarizes DCSBC and provides details as to how it works.

Introducing Dell Command | Secure BIOS Configuration

With DCSBC, IT organizations can move away from BIOS passwords with certificate-based BIOS configurations. DCSBC allows IT admins to securely configure and manage a fleet of Dell client systems' BIOS settings with certificate-based BIOS authentication.

How Dell Command | Secure BIOS Configuration works

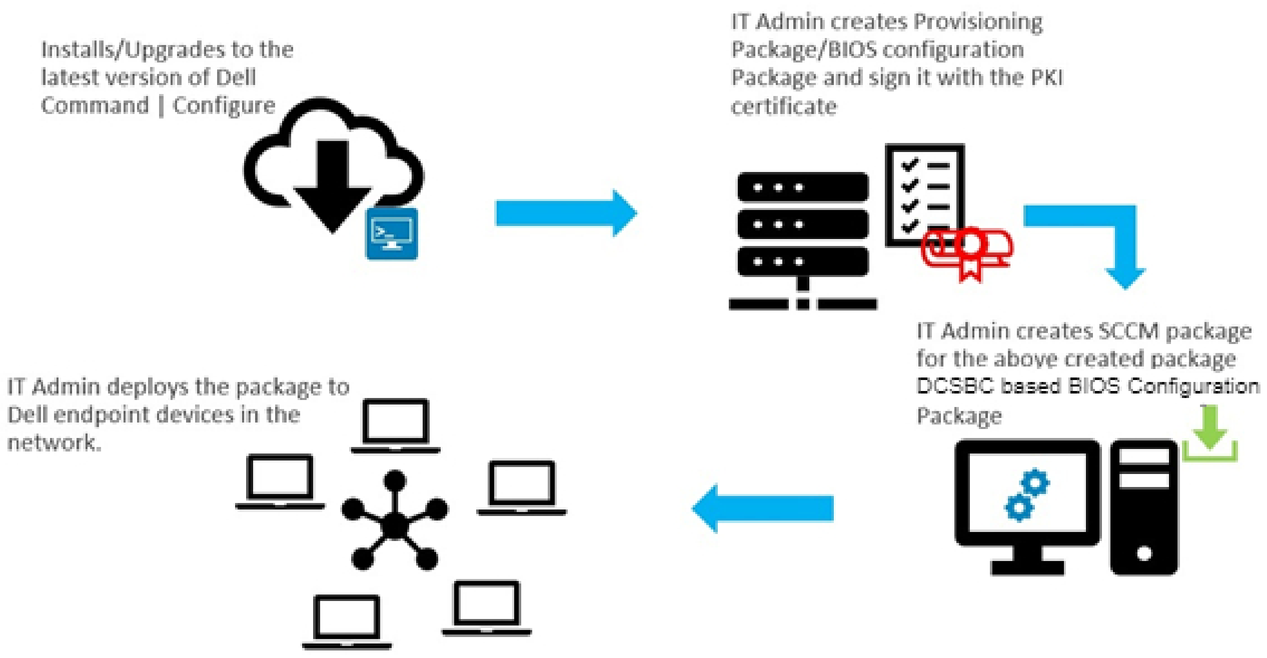
DCSBC is an approach to move away from authenticating Direct Access Controller Interface (DACI) commands with BIOS passwords. DCSBC provides a trusted communication by creating an interface that uses PKI (Public Key Infrastructure) authentication mechanisms and encrypted channels to pass messages between the platform and a client. This approach also provides both integrity and confidentiality to protect customer data.

DCSBC follows a layered security approach for performing BIOS configurations. This includes:

1. PKI Infrastructure for BIOS authentication. Any DACI call can be successfully processed by the BIOS only when it contains a valid signature.
2. Session based model to perform BIOS configuration; each session payload is unique for each client.
3. Encryption of BIOS configuration payloads.
4. Replay protection through single use random numbers (nonce).
5. Zero Trust on client – Trust boundaries only exist between the client BIOS and DCC Server.

The graphic below summarizes the workflow:

1. **Installation/Upgrades to the latest version of Dell Command | Configure (DCC).** This includes installing and setting up the DCSBC server with DCC.
2. **Configuring the DCSBC Server** with HTTPS, which allows for greater security.
3. **Creating Self Contained Executables** (SCEs) for DCSBC Workflows on the DCSBC Server using Dell Command | Configure. An SCE is a type of application that includes all necessary components within the executable itself. Users can run a SCE without having to install additional software on their system. The SCEs created in this case include those for performing provisioning for DCSBC Certificates as well as BIOS configuration packages for signing payloads using PKI (Public Key Infrastructure) certificates.
4. From here, the IT admin **deploys the package** to Dell endpoint devices in the network.


Installs/Upgrades to the latest version of Dell Command | Configure
IT Admin creates Provisioning Package/BIOS configuration Package and sign it with the PKI certificate
IT Admin creates SCCM package for the above created package DCSBC based BIOS Configuration Package
IT Admin deploys the package to Dell endpoint devices in the network.

Benefits of Dell Command | Secure BIOS Configuration

- **Security:** Admins can securely configure and manage a fleet of Dell client systems' BIOS settings with certificate-based BIOS authentication, removing passwords from the process. Admins can also reduce the security risk of unauthorized BIOS configuration changes by moving away from traditional password solutions.
- **Scalability:** In addition, DCSBC's vendor-agnostic Hardware Security Model (HSM) enables secure certificates for fleet-wide BIOS configuration. Admins will appreciate the expanded manageability and flexibility of improved fleet configuration deployment options, which can be utilized for larger device fleets.
- **Streamlined for Greater Efficiency:** DCSBC requires no endpoint software. The solution is agent-free and provides signed-payload BIOS configuration deployment to endpoints. Admins can save time by moving away from fleet-level password management processes.

Dell Command | Secure BIOS Congiruation offers six layers of security

DCSBC offers six layers of security at the BIOS level to reduce the risk of attacks:

- **Dual Key Signing Model:** Whatever configuration that is made must be signed by a private key that the BIOS will verify through a PKI (Public Key Infrastructure). This dual key signing model inherently reduces security risk.
- **Session-based Authorization:** Session-based authorization means that no configuration can be sent to the BIOS until the session has been established, and only via the authorized application. Configuration is only possible once the sessions are established with the BIOS.
- **Platform-Specific Payloads:** Payloads are specifically made on the server. No generic payloads are used, and it is targeted specifically for each individual endpoint. Command payload generation is the foundation for secure BIOS configuration commands leveraging PKI technology and Certificate Authorities.

- **Encrypted Payloads Using Session Key:** Once DCSBC establishes a session, the BIOS also provides a unique session key that is utilized to encrypt the BIOS configuration payloads.
- **Text/Encrypted Text Configuration Moves Away from the Endpoint:** Adhering to Zero Trust principles, the only trusted entities are the server or the BIOS. DCSBC moves away from previous models of text or even encrypted text. All the configurations are stored in a server, and when the SCE is being applied, the endpoint communicates with the server and asks for the specific payload.
- **Replay Protection:** Any payload that is created as part of the configuration contains random numbers that are verified from the server side, as well as the BIOS side. The random number expires as soon as any payload reaches the BIOS. So not only are payloads unique, but they also cannot be replayed again, which ensures that previous information is not reused for possible hacking.

Summary

Dell provides different BIOS configuration management options to fit the needs of our customers. Whether it is secure unique-per-device BIOS password management within the Intune environment or moving away from passwords entirely with Dell Command | Secure BIOS Configuration, Dell has a solution that will help IT admins address their BIOS security needs in an efficient and productive manner.

Resources

- Datasheet : Dell Command | Secure BIOS Configuration
- Blog : Dell Command | Endpoint Configure for Microsoft Intune

Learn more about Dell solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation