Datasheet

Dell Command | Secure BIOS Configuration

Move away from BIOS passwords with certificate-based BIOS configurations

Highlights

- **Secure:** With Dell Command | Secure BIOS Configuration, IT admins can securely configure and manage a fleet of Dell client systems' BIOS settings with certificate-based BIOS configurations.
- **Scalable:** 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.
- **Streamlined:** Agent-free and signed-payload BIOS configuration deployment to endpoints – no endpoint software required. Admins can save time by moving away from fleet-level password management processes.

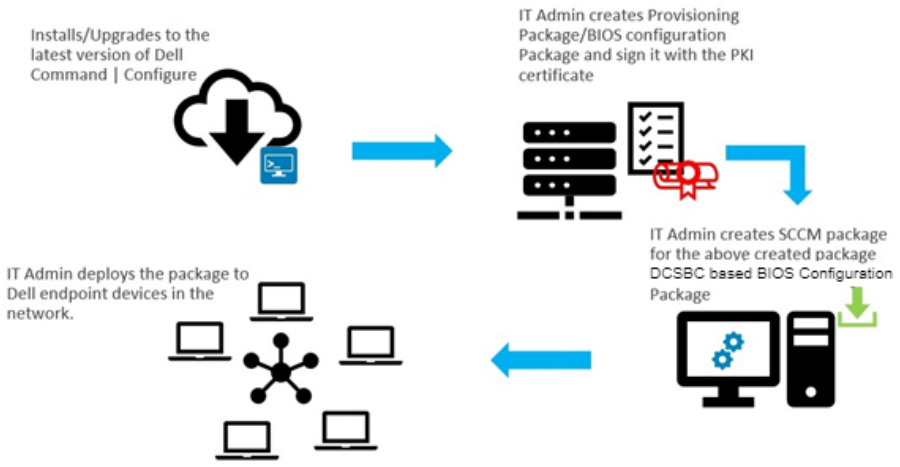
The challenges with BIOS passwords

While setting passwords does offer an added layer of security, they can still be a challenge for several reasons. Text-based passwords can be susceptible to brute force attacks. BIOS passwords are stored, which implies they can be intercepted by others. And they can be tedious, as it can sap an IT admin's time to manage a fleet of BIOS passwords. The results can often lead to weak, repetitive password settings, if passwords are set at all. How can an IT admin reduce the risk of their fleet's BIOS security in an efficient manner?

Introducing Dell Command | Secure BIOS Configuration

Dell Command | Secure BIOS Configuration (DCSBC) is an approach to move away from authenticating Direct Access Controller Interface (DACI) commands with BIOS passwords. DCSBC provides 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.

How DCSBC works



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. A SCE is a type of application that includes all necessary components within the executable itself. Users can run an 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.

DCSBC offers six layers of security to reduce the risk of attacks

Dual Key Signing Model	Whatever configuration that is being made must be signed by a private key that the BIOS will verify through a public key. 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 each is targeted specifically for a unique 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 Dell Command | Secure BIOS Configuration establishes a session, the BIOS also provides a unique session that is utilized to encrypt the payload.
Text/Encrypted Text Configuration Moves Away from the Endpoint	Adhering to Zero Trust principles, the only trusted entities are the server or the BIOS. Configuration 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 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.

Contact your Dell Sales Representative for more information or visit www.dell.com/endpoint-management

Related Dell Manageability Solutions

- **Dell Management Portal** helps manage Dell PCs, over the cloud, in conjunction with Microsoft Intune
- **Dell Command | Configure** provides configuration capability to business client platforms
- **Dell Command | Endpoint Configure for Microsoft Intune** configures BIOS settings on a fleet of Dell devices securely, quickly, and natively in Microsoft Intune
- **Dell Trusted Update Experience** - the latest BIOS, driver, and firmware updates – validated against all your device models and delivered seamlessly, on an industry-standard release cadence

Learn more about Dell Manageability Solutions

Contact a Dell Technologies Expert

View more resources

Join the conversation