Vynamic™ View BIOS Manager

Avoid compromising security with proper BIOS governance

BIOS Management

In the retail banking industry, overall ATM security continues to grow as the threat of both external and internal fraud increases. Yet many financial institutions trust the out-of-the box settings which can leave their self-service fleet vulnerable. In fact, it has become customary for many to keep the default passwords or share passwords with the technical teams so that they have access when required. These practices can lead to issues with PCI compliance; or intentional or accidental fraud, which can be even worse. The only way to ensure your devices are properly secured is to combat them with proven tools and governance.

Vynamic View BIOS (Basic Input/Output System) Manager is a vendor-agnostic system that enables single or multi-device remote changes of the BIOS password. With proper password management, the authentication information required to log into the ATM's BIOS remains secure and trustworthy.

Additionally, Vynamic View BIOS Manager solves another challenge, remote BIOS configuration. Traditional remote tools are based on OS (Windows) level, not BIOS level. Therefore, for any configuration change in BIOS, it would require a field engineer to be dispatched to the terminal, incurring considerable cost. Vynamic View BIOS Manager enables remote power on/off/reset to the PC, even if the PC is shut down or the OS is not responding. Additionally changes to the BIOS setting can be made remotely for a single device, or a unified BIOS settings can be set for the entire terminal network.

FEATURES & BENEFITS

- Not limited to just ATMs, can be utilized on all PC–based devices with Intel® Active Management Technology (AMT) BIOS management, such as POS and self-check-out devices
- Multi-vendor compatible
- Changes partial or whole fleet
- Support UEFI: Not limited to traditional BIOS, but also support new cutting-edge technology of UEFI (Unified Extensible Firmware Interface)

SECURE, REGULAR PASSWORD MANAGEMENT

In order to enhance the security of your terminals, setting and regularly updating the BIOS passwords keeps the integrity of the boot process and ensures that nobody can boot from removable devices or change BIOS or UEFI settings without being authorized. Vynamic View BIOS Manager:

- Enables initial BIOS Password set up and configuration to follow PCI DSS requirements
- Can schedule all or partial device network for regular BIOS password updates (example every three month)
- Utilizes Intel Active Management Technology or DN EPC BIOS tool to change BIOS passwords remotely
- Automatically generates a certificate from a root certificate and uses that certificate to establish the TLS connection
- Password changes on demand or on a re-occurring schedule
- Secure generation of random and encrypted passwords
- Automatic password reset after field engineer visit (when Vynamic View Availability Manager is enabled)

REMOTE BIOS CONFIGURATION MANAGEMENT (ONLY FOR AMT PROCESSORS)

With KVM (Keyboard, Video, Mouse) Remote Desktop function, you can remotely login to BIOS screens to view/manipulate BIOS settings. With Vynamic View BIOS Manager, the system administrator can update all enabled devices in the network.

- Reboot or reset a terminal that is hangs due to software problems
- Eliminates sending a field engineer to check all ATMs and change each one by one
- Remote power management via out-of-band communication
- Change BIOS boot order
- Standardize BIOS settings for your entire terminal network
- Secure connection with TLS and automatic certificate provisioning

CREATE TEMPORARY PASSWORDS

During troubleshooting and maintenance, access to the BIOS is sometimes required by the field engineer. With Vynamic View BIOS Manager, a temporary password can be created and activated for those terminals that require access.

- A temporary password can be generated on demand and sent to field engineer by an authorized user
- Can only be used once and it is immediately changed once work is complete
- Passwords are randomly created and encrypted for increased security

COMPLEMENTS OTHER VYNAMIC VIEW MANAGERS

As part of the larger Vynamic View suite, BIOS Manager can be enhanced to offer increased functionality and security.

- With Availability Manager, events can be configured to recognize once repair work is complete, and can trigger a pre-defined business rule to automatically reset the password. Alternatively a maximum time period after one-time password has been sent can be defined in which a reset has to occur.
- With Security Manager and Vynamic Security Intrusion Protection, security level decreases can be scheduled to allow for the change of BIOS passwords.

WHAT IS DN VYNAMIC?

DN Vynamic is the first end-to-end connected commerce software portfolio in the marketplace. Traversing mobile, ATM, POS, branch, kiosk, and online, DN Vynamic is a system of consumer engagement powered by data and analytics and is cloud/SAAS ready when you are. Built to enable the connectivity businesses of the future require, DN Vynamic extends beyond omnichannel to enable banks and retailers to create seamless, secure, personal connections across the digital and physical channels of today and tomorrow.

Ensure proper BIOS governance across your entire network: Harness the power of the Vynamic View Software Suite. **Talk to your Diebold Nixdorf Representative today.**

Diebold Nixdorf

To learn more, **visit DieboldNixdorf.com.**