



WINMAGIC | Leading the Way to the Next Generation of Full Disk Encryption!

Reduce your IT total cost of ownership, enhance system security and create a better user experience!

As regulatory requirements continue to burden IT organizations, IT managers struggle to contain costs and complexity while protecting users and maintaining compliance. WinMagic's new Pre-Boot Networking dramatically improves control, security, and visibility while reducing the complexity of encryption for end users.

The introduction of local area networks to personal computing in the 1980's created a revolutionary new approach to how systems were managed within organizations. WinMagic's revolutionary Pre-Boot Networking (PBN) brings a similar paradigm shift to administering laptops and other mobile devices.

Pre-Boot Networking utilizes network based resources to authenticate users, enforce access controls, and manage end point devices before the operating system even loads. This unique and ground-breaking approach to Full Disk Encryption (FDE) management results in significant cost savings for organizations by streamlining both IT management and end user functionality.

Previously IT Managers and Administrators were faced with two problematic options when using pre-boot authentication for encrypted computers:

- Enable pre-boot authentication for all devices thereby creating complexity in user provisioning, password management, policy changes, software updates and general administrative functionality.
- Bypass pre-boot authentication altogether with "autoboot"; creating possible exposures to privacy issues, data breaches and compliance infractions.

PBN enables users to get the convenience of autoboot with the security of pre-boot authentication. WinMagic is the first FDE vendor to integrate secure network support into the pre-boot environment.

PBN authenticates users against Active Directory (AD) and authorizes them against the SecureDoc Enterprise Server (SES) via the network before the encrypted data is read off of the drive. By taking advantage of the connection to the SecureDoc Enterprise Server the burden of encryption administration is alleviated by allowing the Active Directory administrator to control user access to encrypted machines anywhere at any time. This approach removes redundant and inefficient network management steps and streamlines end user productivity resulting in a minimum of fifteen percent reduction in FDE total cost of ownership*

Reduce IT Cost of Ownership

Ease of Provisioning: Temporary, remote and multi-workstation users can quickly and efficiently be granted or denied access by adjusting the group membership in Active Directory (AD). Now users can be supported on shared devices without having to manually provision them if they are already assigned in AD to a specific group. Users can be granted access to specified machines by the Active Directory administrator avoiding redundant work on the FDE management console altogether.

Remote Management: Administrators can remotely manage encrypted laptops with real time user revocation. This also provides the capability to execute pre-boot authentication for remote computers, thus enabling secure unattended software updates overnight.

*Based on average calculations of standard networking structure.

Improve the User Experience

Access Any (Approved) System with One Password: Using PBN with AD, users have a single account for any machine using their existing windows password; There's no need to push credentials to encrypted machines; users can now use them the same as any other computer on the network.

Improved Control and Password Resets: Encrypted laptops can now be supported as easily as unencrypted laptops when pre-boot networking is in use. PBN eliminates expensive and time-consuming calls to FDE administrators to re-establish password credentials. By synchronizing encryption passwords with Active Directory, a user or administrator can immediately update their password and login to a specified device. By working directly with Active Directory, lengthy and costly delays are eliminated for password lockouts, resets and more.

Increase Security

Enhanced Security: With autoboot, protection is reduced to what is provided by basic Windows security. At this point the data encryption key has already been exposed in the computer's memory and is therefore vulnerable to attacks such as the famous Princeton Cooled Ram exploit**. PBN avoids these issues by authenticating the computer to Active Directory before the OS is booted and before the encryption key is vulnerable.

Policy Protection: PBN provides the ability to setup IT governance guidelines surrounding data protection right in the pre-boot environment streamlining policy management. System updates and policies can be installed without compromising security due to requirements to skip authentication on reboots.

**Reference the Princeton Cooled RAM attack -Feb 26, 2008

How It Works

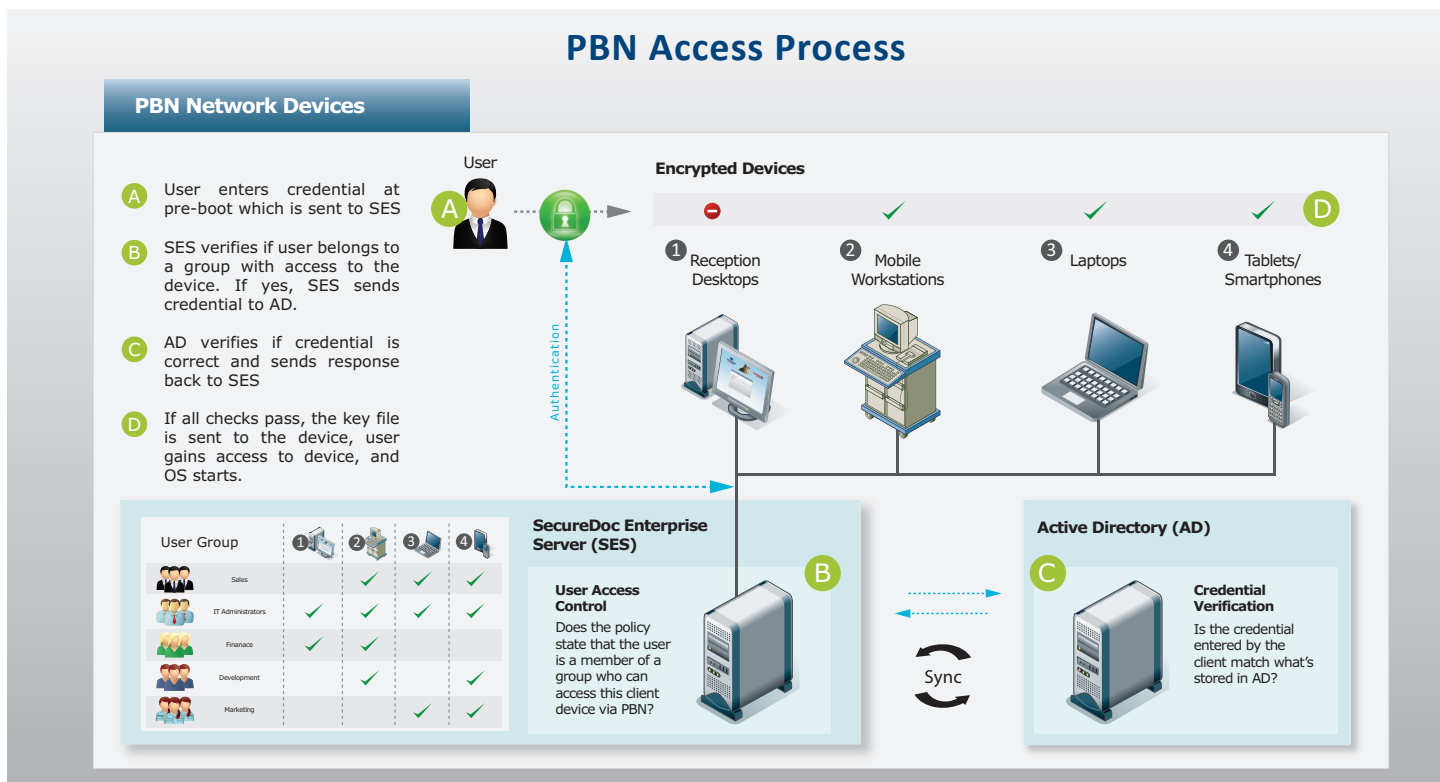


Figure 1

As seen in figure 1 within a given organization, PBN enables a defined group of staff to be enabled for secure access to workstations, laptops and mobile machines from a powered-off state – while ensuring users who do not belong to the defined group cannot access these devices.

If devices are taken off the network while the data is at rest, with PBN authentication they can't be accessed at all – ensuring total protection of any information and denying access to Windows or down-stream server applications.

Staff can have secure shared workstation access via groups in Active Directory with single sign-on using the Windows password thus ensuring full confidence that no one else can access their Windows session and ensuring confidentiality remains intact.

In short pre-boot networking addresses the long-standing issue of network administrators not being able to access and administer encrypted endpoint devices in a simple and efficient fashion. PBN decreases the total cost of managing encrypted devices enhances overall security and provides a user experience where the protection of FDE is truly transparent. What could be better than that?

WinMagic – Bringing You The Next Generation in Data Encryption.