



# SafeBoot® Management Center™

## Security Solutions for Centrally Managing Mobile Data Security

TODAY, ORGANIZATIONS REQUIRE MAXIMUM SECURITY, BUT THEY STILL LOOK FOR THE HIGHEST POSSIBLE RETURN ON INVESTMENT (ROI). TO ACHIEVE THIS SAFEBOOT® MANAGEMENT CENTER™ PROVIDES UNIQUE, POWERFUL CENTRAL MANAGEMENT TOOLS, INCLUDING CENTRAL DEPLOYMENT, USER MANAGEMENT, POLICY MANAGEMENT, RECOVERY, AUDITS, AND SEAMLESS INTEGRATION WITH THIRD-PARTY ENTERPRISE SYSTEMS AND PKI.

### REAL CENTRAL USER MANAGEMENT

Using the administration module, administrators can centrally create and assign user accounts to one or more machines and specify access rights for groups of users or individuals, according to the organization's security policies. User tokens can also be configured. Unlike other solutions, SafeBoot® Management Center™ (SafeBootMC) offers true multi-user capability. For example, an implementation of more than 1,000 users can be completed in just one day with central deployment, and the number of users managed from the central administration point is virtually unlimited. For large corporations, the convenience of these tools offers higher ROI compared to other products that lack high-level central management capabilities.

### SECURE CENTRAL USER RECOVERY

SafeBootMC offers several core tools and services such as SafeBoot® webRecovery™, which allows users reset or recover passwords from any Internet- or intranet-enabled Web browser after passing several pre-registered questions to prove their identity. It integrates with and uses the same SSL server as the SafeBootMC webHelpdesk™. Password recovery and resets can also be performed with the help of the SafeBoot administrator or helpdesk personnel. These options enable users to reset



their passwords safely from anywhere in the world at anytime, enhancing business continuity and helping to reduce total cost of ownership dramatically.

### MANAGEMENT OF ALL SAFEBOOT CLIENTS

SafeBoot provides the only security solutions on the market designed from the ground up with central administration. SafeBoot's architecture enables remote, centralized management of all SafeBoot client applications over TCP/IP. SafeBootMC supports hierarchal, branched, and flat-level administration structures. It simplifies the installation of SafeBoot solutions, which integrate perfectly with existing IT environments. A single file is all that is needed to install SafeBoot solutions on any Windows® platform, and installation is transparent to the

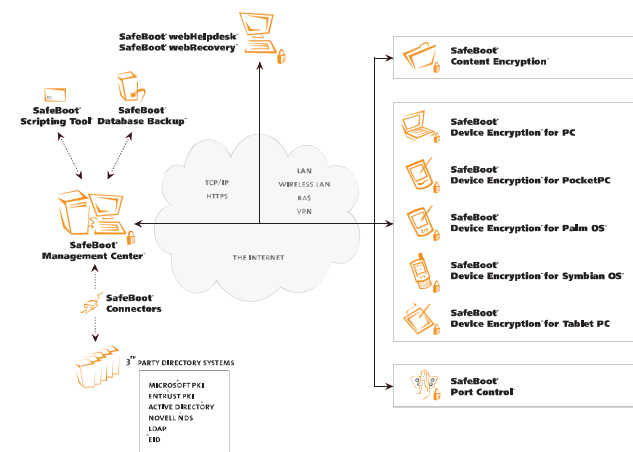


user, with no special training required. Deployment solutions such as Microsoft® SMS and Novell® ZENworks® can be also used, eliminating the need for administrators to configure each and every PC within an organization. The installation process is even failsafe in the event of power failures or machine reboots.

## MANDATORY SECURITY POLICIES & ACTIVE DIRECTORY INTEGRATION

SafeBoot solutions implement a “headless client” architecture that is PKI-aware, and all policy changes are effected from one common policy database. Encryption keys, recovery keys, encryption privileges, and security policies are also created through SafeBootMC and assigned to users and groups.

SafeBoot solutions integrate with other access control databases – including X.500 directories, Active Directory®, Windows NT® Domain, Novell NDS®, and other LDAP-based directories – and synchronize the identity attributes with the SafeBoot database. Changes in connected systems are automatically reflected in SafeBoot. Again, this single point of administration helps achieve the lowest possible TCO.



© Control Break Beheer N.V. All Trademarks are recognized as the property of their respective owners.

## PKI INTEGRATION

SafeBootMC's core tools and services also support identity management systems through various SafeBoot® Connectors™. SafeBoot® Connector™ for Entrust Authority™ and SafeBoot® Connector™ for Microsoft® PKI enable authorized users to log on to SafeBoot applications from designated machines that utilize Entrust and Microsoft PKI digital certificates, which can be stored on tokens such as USB keys and smart cards. Because SafeBoot solutions are PKI-aware, administrators do not need to reconfigure tokens to ensure compatibility. SafeBoot Connectors, PKI technology can consistently and transparently be applied to all SafeBoot® solutions, ensuring additional encryption, digital signature, and authentication capabilities.

## CENTRAL AUDITS

SafeBoot Management Center's auditing facilities records all logon information, including unsuccessful logon attempts and any changes to security configurations. They provide a comprehensive audit trail that increases the level of accountability for end-users and administrators. Audits can be interrogated directly through the administration console or saved to a separate log file for detailed analysis.

## CERTIFIED, AWARD-WINNING TECHNOLOGY

With more than two million users, SafeBoot solutions have the largest installed base of any mobile data and device security solution. CBI has achieved twelve consecutive 4- or 5-star ratings from SC Magazine, as well as the SC Magazine 2004 Reader Trust Award for Best Encryption Product. SafeBoot solutions are FIPS 140-2- and Common Criteria EAL4-certified, ensuring that they employ true strong encryption and secure key management. SafeBoot is widely used by organizations worldwide that require robust, end-to-end protection of mission-critical data, devices, and networks, including banks, insurance companies, consultancy firms, governmental bodies, and health care organizations.



MORE INFORMATION ON SAFEBOOT SPECIFICATIONS AND RESELLERS:

▶ [INFO@SAFEBOOT.COM](mailto:INFO@SAFEBOOT.COM) ▶ [WWW.SAFEBOOT.COM](http://WWW.SAFEBOOT.COM)

SAFEBOOT IS DEVELOPED BY CONTROL BREAK INTERNATIONAL