



Ohio Office of Information Technology

SafeBoot Seat License Overview

SafeBoot seat licenses are purchased under OIT Master License Agreement 0023 using federal GSA SmartBuy promotional pricing.

The bundle pricing is available until October 29, 2008. The SafeBoot OMB License Bundle includes the following as described below:

1. **Full Disk (Device) Encryption FDE**
2. **Content (File/Folder) Encryption (FFE)**
3. **Port Control**
4. **Connectors**
5. **Management Console**
6. **Database Backup**
7. **Scripting Tool**
8. **Web Help Desk**
9. **Web Recovery**
10. **Single User License covers up to 5 devices (in use by that user)**
11. **Home use of all licenses**
12. **Immediate temporary enterprise license for use during natural disasters, acts of war and/or terror**
13. **1st Year 7x24 Maintenance & Support**

1. Full Disk (Device) Encryption FDE

SafeBoot® Device Encryption™ for PCs, laptops, and tablet PCs uses strong access control, and pre-boot protection to authenticate users, and it supports Single Sign-On (SSO). It uses algorithms such as AES-256 to encrypt data on all storage drives. Encryption and decryption are transparent to the user and performed on the fly, with virtually no performance loss.

Operating Systems Supported include: Windows XP, Vista, Windows Mobile, Palm and Symbian. Additionally, the RIM OS is supported for key management, and the MAC OSX is under development.

2. Content (File/Folder) Encryption (FFE)

SafeBoot® Content Encryption™ transparently encrypts select files and folders automatically and on-the-fly before they move throughout your organization. It also ensures that files and folders are secure wherever they are saved, including on local hard disks, file servers, removable media, and more.

Scalable and easy to use, SafeBoot® Content Encryption™ enables administrators to easily specify the local or server-based files, file types, or folders that are to be encrypted. In accordance with your organization's security policies, administrators can also designate which users and groups will have the encryption key, allowing them to easily access and share specified files and folders across the network. Encrypted data stored on the network is safe even from all unauthorized personnel, even the administrator. Users cannot detect the encryption or decryption process, because there is no performance loss and no action is required on the part of the user.

3. Port Control

SafeBoot® Port Control™ uses strong access control to prevent unauthorized use of removable devices that connect to serial, parallel, USB, Bluetooth®, FireWire, IrDA®, and other ports on PCs, laptops, and tablet PCs. These devices include memory sticks, modems, removable hard disks, and more.

Port Control supports all port device classes and types and enables administrators to manage the kinds of devices that can and cannot be attached to the organization's machines. It also has tools that quickly identify newly attached devices. By centrally managing access to port devices at both the class- and manufacturer ID-level, SafeBoot Port Control enables administrators to restrict the use of all removable devices or those from particular manufacturers.

4. Connectors

For integrating and synchronizing SafeBoot solutions with market-leading technologies SafeBoot® Connectors™ are dedicated, customized modules designed to enable SafeBoot® solutions to integrate and synchronize with widely adopted and emerging technologies, including market-leading identity management and directory services. This ensures that more than two million SafeBoot International customers can employ the most comprehensive, feature-rich data and device security solutions available. It also helps provide administrators with a single, centralized point for the management of users, devices, and technologies enterprise-wide.

Public Key Infrastructure

Identity management systems supported by SafeBoot® Connectors™ include Public Key Infrastructure, or PKI—a transparent, standards-based solution for data encryption and strong user authentication that uses digital certificates. Among other things, PKI helps users securely exchange information, authenticate service providers, complete transactions, and prevent identity theft across applications and the Internet, intranets, and extranets. The technology helps safeguard IT infrastructure and securely extends business processes across networks to users, partners, and customers.

- **SafeBoot® Connector™ for Entrust Authority™**
- **SafeBoot® Connector™ for Microsoft® PKI**
- **SafeBoot® Connector™ for Windows NT®**

Directory Systems

As part of the core services offered by SafeBoot® Management Center™, SafeBoot® Connectors™ synchronize SafeBoot® Enterprise and Professional editions with third-party directory systems, including Microsoft® Active Directory®, Novell Directory Services (NDS®, now known as Novell eDirectory™), and the Lightweight Directory Access Protocol (LDAP).

- **SafeBoot® Connector™ for Active Directory®**
- **SafeBoot® Connector™ for Novell Directory Services (NDS®)**
- **SafeBoot® Connector™ for LDAP**

5. Management Console

For Managing Central Deployment, Policy Management, Hot Revocation, Audit Facilities, and Safe Central Recovery.

SafeBoot® Management Center™ is a feature-rich, cost-effective solution for setting and enforcing security policies enterprise-wide. It also vastly increases ROI. Because all SafeBoot® technologies are seamlessly integrated into this highly adaptive solution, SafeBoot® Management Center™ empowers the administrator -

rather than the users - with strong central management tools, modules, and technologies. Through SafeBoot® Management Center™ and the countless options it provides, security personnel can easily enforce policies and extensively manage identity, access, assets, communication, central deployment, remote upgrades, hot revocation, auditing, scripting, and much more.

Identity Management and Access Control

SafeBoot® Management Center™ tightly controls users' access to machines, encryption and recovery keys, files, ports, tokens, smartcards, and more, along with the policies attached to each user. Through SafeBoot® Management Center's identity management system, each SafeBoot® user has one identity that extends across all systems enterprise-wide. Thus, if a user is disabled in Active Directory® or PKI, for example, they are disabled everywhere. If the user changes his password, his password is changed everywhere.

Mandatory Security Policies

SafeBoot® Management Center™ supports hierarchal, branched, and flat-level administration structures, empowering administrators to set and enforce all mandatory security policies. Also, all policy changes are effected from one common policy database, and all SafeBoot® solutions can seamlessly connect to other access control databases and synchronize their identity attributes with the SafeBoot® database. Through various SafeBoot® Connectors (such as those for Active Directory® or PKI), user identities can be easily integrated.

Asset and Communication Management

SafeBoot® Management Center™ simplifies the installation of all SafeBoot® solutions, making it transparent to the user. An implementation of more than 1,000 users can be completed in just one day, and the number of users an administrator can manage from a single, central point is virtually unlimited. Further, SafeBoot® Management Center™ enables administrators to determine the devices on which users are allowed to work, including PCs, laptops, mobile phones, etc. Security personnel can prevent users from loading and running unauthorized software or code, and the solution's trusted application tool can restrict users' access to specific applications and limit their use. Also, through TCP/IP, SafeBoot® Management Center™ allows encrypted communication via LAN and Internet, and it manages load-balancing across multiple servers. Finally, SafeBoot® Management Center™ provides one helpdesk to enable central, fail-safe recovery.

Other Features

SafeBoot® Management Center™ also provides the following features:

- **Remote Deployment of Upgrades and Updates:** SafeBoot® files and others can be transparently pushed to clients using the intelligent update system.
- **Hot Revocation:** Administrators can remotely enable and disable users and machines with one push.
- **Rapid Restore:** The entire hard disk is encrypted, and a unique disk cryptography driver is embedded in the IBM environment, allowing IBM's Rescue and Recovery™ with rapid Restore™ to access the encrypted disk and restore damaged files and folders.
- **Auditing Facilities:** Records all logon information and provides a comprehensive, central audit trail, increasing the level of accountability for end-users and administrators. All SafeBoot® technologies audit user action and enable administrators to extensively report on statistics.
- **Scripting Tool:** A command line interface with the administration system and object directory that enables administrators to automate various commonly performed tasks.

6. Database Backup

SafeBoot® Database Backup™ is an add-on to the SafeBoot® Management Center™. It provides current a current backup of all pertinent SafeBoot® security information. To ensure efficiency in maintaining and deploying security policies enforced with SafeBoot®, it is important to have a current back up of the

SafeBoot® Object Directory™. While typical server backup tools are known to significantly reduce the performance of a server, Database Backup will efficiently provide a backup of vital information needed by the SafeBoot® Management Center™.

SafeBoot's® proprietary backup tool monitors the change logs and locking information stored in the Object Directory, so it does not have to search for changes. This makes it far more efficient and effective in making reliable hot-backups.

Smart Service Scheduling Using Microsoft's® schedule service, administrators find a familiar and intuitive scheduling interface. SafeBoot® Database Backup™ supports multiple jobs (at high and low frequencies), one-off, and repeated events.

Service-Based

Running as a background service ensures that the Directory Backup utility does not cause headaches for system administrators. Backup schedules resume transparently in the event of power outages and server restarts.

Support for Multiple Backups of Multiple Object Directories

Database Backup creates multiple backups of the same ODB (i.e. a daily full backup on an archive server; an hourly incremental backup at a disaster recovery site; or, a change-by-change, minute-by-minute backup on a hot-standby server). With Database Backup, administrators may use one scheduled backup machine to create duplicates of multiple SafeBoot® directories.

6. Scripting Tool

The SafeBoot® Scripting Tool™, a command line interface to the SafeBoot® administration system and object directory, enables the administrator to automate more than 35 common tasks and management functions. It can create users, assign them to machines, import offline install sets, dump audit logs, perform database integrity checks, and much more. This automation tool further lowers TCO by reducing administration time and preventing typographical errors.

SafeBoot® Scripting Tool™ is a command line (shell) tool. Used in conjunction with SafeBoot® Device Encryption™ and SafeBoot® Management Center™, it can be automated through batch files and common scripting technologies, and it is used by SafeBoot® customers primarily to aid automatic personalization of systems in "Gold Build" environments.

Other tasks and management functions that SafeBoot® Scripting Tool™ automates include: setting or updating selected aspects of user or machine configuration; creating, renaming, or deleting users and machines; and moving users and machines between groups. For machines, it also sets file groups, forces synchronization, dumps user lists and machine descriptions, and get or set a machine's encryption state. Finally, for databases, SafeBoot® Scripting Tool™ can get user and machine counts, validate machine and user groups, and search for orphan machines and users.

8. Web Help Desk

Integrating with the SafeBoot® Management Center's webHelpdesk™, SafeBoot® webRecovery™ enables users to recover or reset their own passwords should they forget them or lose their tokens. Previously, a password recovery or reset could be performed only with the help of the SafeBoot® administrator or helpdesk personnel. With SafeBoot® webRecovery™, users can reset their own password from any Internet- or intranet-enabled browser by passing several pre-registered questions to prove their identity.

SafeBoot® webRecovery™ enables users to reset their passwords safely from anywhere in the world at anytime. It uses the same SSL server as the SafeBoot® webHelpdesk™, and together they enhance business continuity and help reduce total cost of ownership dramatically.

9. Web Recovery

Integrating with the SafeBoot® Management Center's webHelpdesk™, SafeBoot® webRecovery™ enables users to recover or reset their own passwords should they forget them or lose their tokens. Previously, a password recovery or reset could be performed only with the help of the SafeBoot® administrator or helpdesk personnel. With SafeBoot® webRecovery™, users can reset their own password from any Internet- or intranet-enabled browser by passing several pre-registered questions to prove their identity.

SafeBoot® webRecovery™ enables users to reset their passwords safely from anywhere in the world at anytime. It uses the same SSL server as the SafeBoot® webHelpdesk™, and together they enhance business continuity and help reduce total cost of ownership dramatically.

10. Single User License covers up to 5 devices (in use by that user)

The SafeBoot single user license includes all of the functions described above, including full disk and / or content encryption for up to five devices per end-user. This includes desktop and portable computers, personal digital assistants and smart phones.

11. Home use of all licenses

The SafeBoot single user license covers end-user computing devices used by an employee in the home. Of course, installation of such protection on an employee's computing devices is completely at the option of the customer.

12. Immediate temporary enterprise license for use during natural disasters, acts of war and/or terror

The SafeBoot license agreement allows for the immediate temporary concurrent use during natural disasters acts of war and / or terror. After such events, replacement licenses will be available from SafeBoot for licensed end-users.

13. 1st Year 7x24 Maintenance & Support

Licenses purchased under OIT's Master License Agreement will receive 7x24 Maintenance and Support as defined by Service Level Terms and Conditions. Standard Technical Support Hotline hours are from Monday through Friday, 8:00 am to 8:00 pm, Eastern Standard Time, with access to a Technical Support Hotline during non-standard support hours. After the first year, support availability will convert to standard operating hours.

14. 2nd Year Maintenance & Support

While not part of the license bundle, in addition to the first year's maintenance and support, for state agencies participating in the program, the second year's support at standard operating hours of 8:00 am to 8:00 pm, Monday through Friday, Eastern Standard Time will be provided by OIT. Please note that for all other eligible entities purchasing from the Master License Agreement that the second year's support (\$2.89 per license) *is not* included in the bundle and consequently is the obligation of the purchasing entity.