



Application and Devices Control: Common Features

Feature	Function	Benefits
Whitelist	Assign permissions for authorized devices to user or user group, and by default those not authorized are not allowed	Eliminates unknown or unwanted devices in your network, reducing the risk of data leakage
Integrated Sanctuary Suite Console	Single management console for centralized configuration and management of application and device usage policies	Simplifies application and device management with extensive logging and reporting of connected devices, files and applications
Custom Access Denied Notifications	Customizable messages displayed to end user signaling access denied	Communicates organization-specific instructions, such as providing Help Desk contact information
Multi-Language Support	Supports 12 languages on Sanctuary client machines	Improves user experience in international organizations
Offline Permission Updates	Export of permissions to a file for import into offline computers	Enables updating of offline client systems with current Sanctuary permissions
Unified Log Management and Reporting	Sanctuary Device Control and Application Control logs are stored and displayed in a common format	Delivers more powerful forensic analysis by identifying the relationship between device, application usage and shadowed files
Flexible Log Queries	Enables administrator to search logs and sort results; Multiple entries can be stacked together to condense information	Provides powerful log analysis enabling quick drill down to a specific issue
Stored Log Query Templates	Pre-defined templates available; Configuration of any log query can be saved	Provides fast and easy review of logs on a regular basis
Log File Export	Displayed log entries can be saved in a CSV file format	Provides flexibility to review and analyze logs in any CSV compliant application
File Compression	Files are sent in a compressed format from the client to the server, from the server to the client and from the server to the console, and Shadowed files are compressed for storage	Optimizes network bandwidth and increases efficiency, taking less storage space, as well as providing faster file retrieval from remote servers
Disconnected/Remote Computer Protected	Enables constant protection by keeping a local copy of the last list of hashes and permissions on the disconnected machine	Secures computer regardless of network connection, ensuring that remote or disconnected users are also protected
Decentralized Files Storage	Shadow files, scans and log files are stored with each Sanctuary Application Server, maintaining central access from the management console	Reduces the bandwidth required to transmit and store files in large or complex enterprises
Active Directory and eDirectory Support	Leverages user and user group definitions in existing Active Directory and eDirectory	Reduces setup and maintenance of users and user groups
Highly Scalable Architecture	Multi-tier architecture with Database, one or more Application servers, and Client	Provides flexible and scalable deployment options in large and complex networks
Silent Unattended Installations	Install with any deployment tools which use MSI Setup (e.g. Microsoft Systems Management Server (SMS), Group Policies, WinInstall, etc).	Enables faster and easier deployment
Audit of Administrator Actions	Full auditing and reporting of all Administrator actions	Demonstrates regulatory compliance ensuring configuration remains intact and identify potential abuse or training needs
Differential Updates Sanctuary Application	Server sends smaller delta file updates to the clients for Sanctuary Application Control file signatures and all Sanctuary permissions	Optimizes performance on a highly decentralized network and/or working with a slower network connection
Automated Permission Updates	New permissions are updated at logon, every hour and upon network connection status change. Application file signatures updated at each logon	Automates policy updates requiring no user intervention, ensuring that users are working with latest policies
Push Changes to Permissions	Permission changes for applications or devices can be pushed to one or many users	Implements new policies regarding applications or devices immediately – no reliance on reboot or restart of network connection

Sanctuary Device Control

Feature	Function	Benefits
Access Control List Based Permissions	Assign permissions to a user/user group based on their Active Directory or eDirectory identity	Provides granular user permissions that remain with user login regardless of machine
Granular Device Control Permission Settings	Permission settings include read/write, scheduled access, temporary access, online/offline, I/O bus type, HDD/non-HDD devices and more	Eliminates risk of unauthorized devices connecting to the network while providing the flexibility users demand
Uniquely Identify and Authorize Specific Media	Authorize DVD/CD-ROM collections, grant access to users or user groups and encrypt removable media with unique ID's	Limits DVD/CD-ROM access to company standard discs, to avoid use of unauthorized content and/or encrypt removable media to prevent unauthorized viewing
Plug and Play Devices: Hot Plug Support	Detect Plug and Play Devices "on the fly"	Ensures user productivity is not disrupted by applying permissions for plug and play devices when detected
Bi-Directional Shadowing Option	Patented shadowing technology records filename or complete file that is read from and/or written to a removable device	Captures the flow of information into and out of your network, reducing risk and containing data leakage
Prevention of PS/2 and USB Hardware Keyloggers	Block PS/2 port, enforce USB keyboard usage and detect/block popular models of USB keyloggers	Reduces risk of attackers capturing passwords and other confidential information through keyloggers
Flexible Encryption Options for Removable Media	Administrators may centrally encrypt removable media or force users to encrypt media at time of use	Ensures that sensitive data is not inadvertently exposed to those without authorized access
File Type Filtering	Control the type of files that are moved to and from removable devices	Reduces risk of unwanted files from entering and

Sanctuary Application Control

Feature	Function	Benefits
SecureWave File Definitions	Classified, pre-loaded whitelist of all supported OS files	Speeds and simplifies whitelist definition
Automated Application Discovery	Process of identifying, categorizing and authorizing applications which produces a record of all executables on client computers, file servers and/or local directories	Provides flexible and fast options to create or update whitelists
Script / Macro Protection	Controls execution of VBScript, Microsoft Office VBA and JavaScript with central authorization or a prompt to local users	Extends application policy enforcement to include scripts/macros for greater protection
Path Protection	Optional file authorization based on location or path rules. Create a trusted owner, such as administrator, to reinforce security	Provides flexibility to support executable files for which hash definitions are not useful or applicable (i.e. auto-changing .exe files)
Non-Blocking Mode	Execute and log activity for administrator review	Enables Sanctuary to identify current state before defining and enforcing policy
Flexible File Authorization	Versatile File Processor (FileTool.exe) enables directory and subdirectory scans to discover new applications and packages while online or offline	Provides flexible and fast option to identify new and updated applications for review and ultimately to generate whitelists
Nested Executable File Groups	Hierarchical structure of organizing file groups	Provides fast administration of file groups and assignment of user permissions
Relaxed Logon	Executes logon scripts without authorization and automatically switches system into blocking mode after either a set of time or at the end of the script	Eliminates need to administer logon scripts in Sanctuary without compromising the security of the system
Local Authorization	Trusted users can authorize applications locally, while maintaining a log for administrator review	Delivers flexibility to the user, without giving up administrative control
Spread Check	Disables suspicious executables that are locally authorized on too many computers	Contains risk of malicious code spreading through network due to local authorization



Lumension Security - Luxembourg
 Atrium Business Park
 Z.A. Bourmicht
 23, rue du Puits Romain
 L-8070 Bertrange
 Luxembourg
 +350 265 364 11 / www.lumension.com



Sanctuary® - A Lumension Brand.

©2007 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.