

# Sanctuary<sup>®</sup> Device Control Modules



To accommodate organizations' different endpoint policy, auditing and enforcement requirements, Sanctuary Device Control is available in a modular way:

## SANCTUARY DEVICE CONTROL - AUDIT ONLY

Focusing on audit and reporting requirements to comply with regulatory requirements or internal policies, Sanctuary Device Control – Audit Only provides extensive auditing & reporting features:

- ▣ **Logging of user actions** - Keeps track of access denied (read/write), new device entered, by whom, when, on what host, etc.
- ▣ **Patented Bi-Directional Shadowing of all copied data** - Tracks all data read from and/or copied to removable devices. First level provides file name, type, size, by whom, when, etc. while second level captures and retains a full copy of all data written to / from removable devices for audit needs by administrators.
- ▣ **Reporting to third party systems** - Allows the export of CSV files to any compliant third party reporting system for further processing (e.g. statistics on device usage, denied access, etc.). A flexible and intuitive query builder generates the export files to be re-imported to MS Excel, Crystal Reports, Intellitactics and others.
- ▣ **Use of Sanctuary Device Scanner** in order to create an inventory of all devices that have ever been plugged into the hosts connected to the corporate network.

## SANCTUARY DEVICE CONTROL – BASE

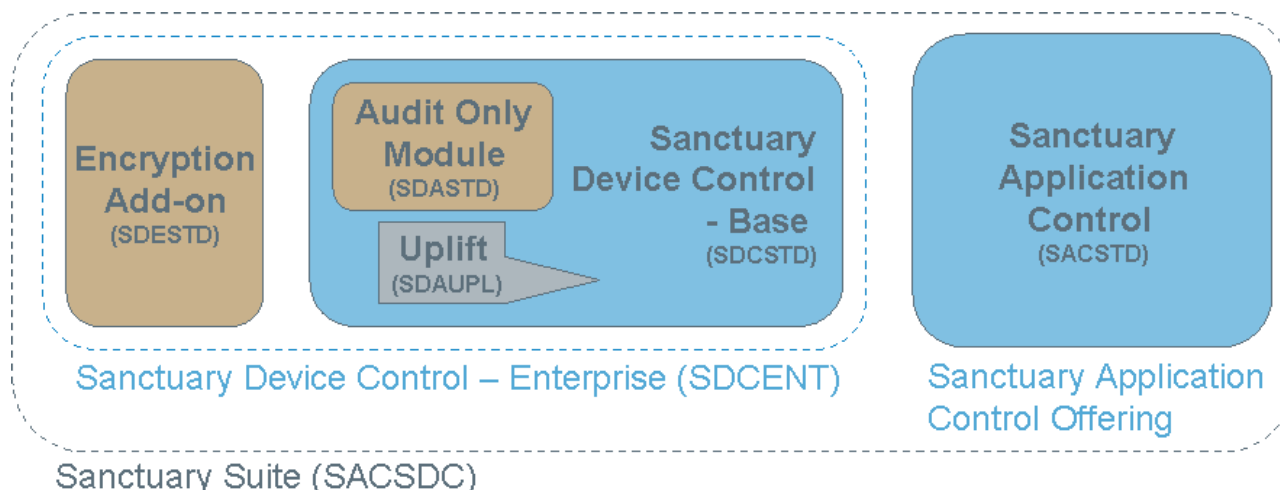
Sanctuary Device Control – Base includes the audit and reporting features of Sanctuary Device Control – Audit Only and adds on top of these all enforcement features of our award-winning policy enforcement product, including access attributes; device management; enforcement by class, sub class, device level, etc.; administrative roles, etc. Note that this module does not include removable media encryption features.

## SANCTUARY DEVICE CONTROL – ENCRYPTION ADD-ON

This is an add-on module to Sanctuary Device Control – Base (which is therefore a prerequisite to this add-on). Management of unique and encrypted devices offers the possibility to encrypt memory keys (AES-256) and thereby to uniquely identify them. The media authorizer module provides the capability to authorize a specific removable device to a particular user. The module specifically allows the encryption and protection of data stored on removable media.

## SANCTUARY DEVICE CONTROL – ENTERPRISE

For organizations that need the entire set of the above mentioned modules, Sanctuary Device Control – Enterprise provides within a unique bundle the full feature set enabling auditing, reporting, enforcement and encryption features of our product.



Feature	Function	Benefits	SDA STD	SDC STD	SDE STD	SDC ENT
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	x	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
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	x	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
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	x	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
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	x	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
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	✓	✓	N/A	✓
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	✓	✓	N/A	✓
Restrict the Amount of Data Copied	Restrict the daily amount of data copied from an endpoint to a device on a per-user basis	Removes risk of large pieces of confidential information leaving the network	x	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
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	✓ <sup>3</sup>	✓	N/A	✓
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	x	x	✓	✓
File Type Filtering	Control the type of files that are moved to and from removable devices	Reduces risk of unwanted files from entering and sensitive files from leaving the network	x	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
Disconnected/ Remote Computer Protected	Enables constant protection by keeping a local copy of the last list of permissions on the disconnected machine	Secures computer regardless of network connection, ensuring that remote or disconnected users are also protected	x <sup>4</sup>	✓	N/A	✓
Highly Scalable Architecture	Three tier architecture with Database, one or more Application servers, and Client	Provides flexible and scalable deployment options in large and complex networks	✓	✓	N/A	✓
Powerful Log Analysis and Reporting	Detailed log analysis with flexible filter, sort and display options and stored query templates as well as central reporting	Demonstrates policy compliance and drills down on suspicious behavior for legal or management follow up	✓	✓	N/A	✓
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	✓	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
Multi-Language Support	Supports 12 languages on Sanctuary client machines	Improves user experience in international organizations	✓	✓	N/A	✓
Custom Reports	Custom query templates can be scheduled to automatically generate reports in HTML, XML or CSV formats and delivered via email or network file share	Produces data required for compliance audit purposes and management reporting in a report format or data format for easy integration into a 3rd party system	✓	✓	N/A	✓
Password Lockout and Recovery	Lockout users after three failed attempts; recover access to devices when passwords are forgotten	Reduces risk of hackers breaking into devices; enables recovery of encrypted data on devices	x	x	✓	✓
Offline Temporary Permissions	Challenge/response system generates new permissions on disconnected machines, allowing for temporary permissions to users on demand, even when a user is not connected to the network	Enables provision of temporary permissions to users on demand, even when not connected	x	✓ <sup>1</sup>	✓ <sup>2</sup>	✓
Device Scanner Tool	Enumerate each device in the corporate network and allows the generation of html and XML reports.	Independent from the agent installation of Sanctuary, this tool can be used as a first phase approach to Sanctuary deployment to identify all I/O devices that have ever been connected to any corporate network hosts.	✓	✓	N/A	✓

1 - Except Sanctuary encryption related features – permissions to devices not encrypted by Sanctuary are possible

2 - Includes Sanctuary encryption related features

3 - Except PS2 port blocking.

4 - Permissions stored locally – however, no enforcement is allowed with SDA, thus not a meaningful feature for SDA.



**Lumension Security - Luxembourg**

Atrium Business Park  
 Z.A. Bourmicht  
 23, rue du Puits Romain  
 L-8070 Bertrange  
 Luxembourg  
 +352 265 364 11 / [www.lumension.com](http://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.