

Lumension® Device Control for Microsoft® System Center

Datasheet

Device / Port Control and Data Encryption for Microsoft System Center Configuration Manager (SCCM) Users

Data leakage caused by the accidental or sometimes malicious use of removable devices and/or media has reached alarming levels. In fact, over 85 percent of privacy and security professionals reported at least one breach and almost 64 percent reported multiple breaches that required notification.¹

Historically, in order to enjoy the security benefits of an advanced device / port control solution, System Center users had to deploy a secondary infrastructure (server, console, agents) as they implemented a solution from scratch. Now System Center users can easily enforce device / port control and data encryption policies without requiring new infrastructure and without adding new administration overhead.

Enhance Security Policy Enforcement and Reduce Implementation Costs

By centrally deploying, managing, enforcing and monitoring device / port access and file transfer / encryption policies via the already established SCCM environment, SCCM customers can significantly reduce implementation costs and quickly enhance their security policy enforcement.

With Lumension Device Control for Microsoft System Center, SCCM customers can:

- » Minimize data loss or theft by controlling removable storage device usage
- » Prevent unauthorized removable storage devices (e.g., USB flash drives) and media (e.g., CDs / DVDs) from connecting to organizational endpoints
- » Automatically encrypt and monitor critical information being moved to removable storage devices / media
- » Prevent introduction of malware via USB devices (one method used to spread the Conficker worm)

Lumension Device Control for Microsoft System Center integrates into the SCCM environment, eliminating the need for a separate server console and leveraging previously established system and user groups. This enables faster device / port control deployment, eliminating the acquisition and implementation costs related to “server sprawl,” and reducing the training costs and productivity hits associated with new software.

Key Features

- » Award-winning Device / Port Control and Data Encryption within SCCM
- » Installation on Existing SCCM Server
- » Compatible with SCCM and Leverages Entire SCCM Implementation
- » Create and Deploy Device Control Policies within SCCM
- » Administer Device Control Policies within SCCM Console
- » Prevent Data Loss and Malware Proliferation

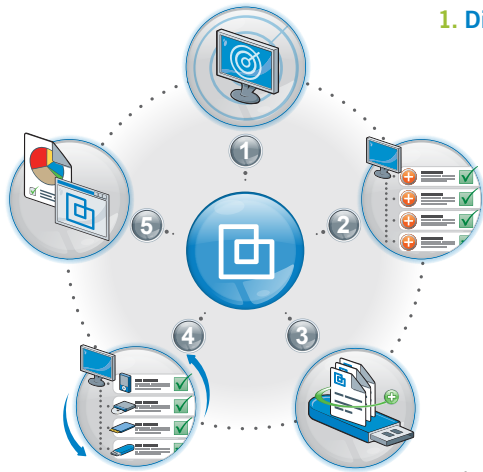
Key Benefits

- » Minimize data loss or theft by enforcing device / port usage policies
- » Prevent unauthorized storage devices from connecting to organizational endpoints
- » Automatically encrypt and monitor critical data being moved to removable devices (e.g., USB flash drives) and media (e.g., CDs / DVDs)
- » Prevent malware introduction via USB devices (one method used to spread the Conficker worm)



1. Deloitte & Touche, Enterprise@Risk: 2007 Privacy & Data Protection Survey, December 2007

How Lumension Device Control Works



- 1. Discover:** Identify all removable devices that are currently or have ever been connected to your endpoints.
- 2. Assess:** Categorize all “plug and play” devices by class, model and/or specific ID and define policy through a whitelist approach.
- 3. Implement:** Enforce file copy limitations, file type filtering and forced encryption policies for data moved onto removable devices.
- 4. Monitor:** Track all policy changes, administrator activities and file transfers to ensure continuous policy enforcement.
- 5. Report:** Provide visibility into device and data usage to demonstrate compliance with corporate and/or regulatory policies.

Lumension Device Control Features and Benefits

Whitelist / “Default Deny”: Assigns permissions for authorized removable devices and media to individual users or user groups; by default, devices / media and users not explicitly authorized are denied access.

Policy Enforced Encryption for Removable Storage: Centrally encrypts removable devices (such as USB flash drives) and media (such as DVDs/CDs), plus enforces encryption policies when copying to devices / media.

Data Copy Restriction: Restricts the daily amount of data copied to removable devices and media on a per-user basis; also, limits usage to specific time frames / days.

File Type Filtering: Controls file types that may be moved to and from removable devices (such as USB sticks) and media (such as DVDs/CDs) on per-user basis.

Centralized Management / Administrators’ Roles: Centrally defines and manages user, user groups, computer and computer groups access to authorized removable devices / media on the network; by default, those devices / media and users not explicitly authorized are denied access.

Temporary / Scheduled Access: Grants users temporary / scheduled access to removable devices/media; used to grant access “in the future” for a limited period.

Context-Sensitive Permissions: Applies different permissions when the endpoint is connected to the network, when it is not, and/or regardless of connection status.

Role Based Access Control: Assigns permissions to individual users or user groups based on their Windows Active Directory or Novell eDirectory identity, both of which are fully supported.

Tamper-proof Agent: Installs agents on every endpoint on the network; agents are protected against unauthorized removal – even by users with administrative permissions.. Only Device Control Administrators may deactivate this protection.

Flexible / Scalable Architecture: Provides organization-wide control and enforcement using scalable client-server architecture with a central database that is optimized for performance. Supports virtualized server configurations.

System Requirements

- » **Supported Microsoft® System Center Configuration Manager (SCCM) Environments:**
 - SCCM 2007, SCCM 2007 SP1, and SCCM 2007 R2
- » **Database:**
 - Microsoft SQL Server 2005 or SQL Server 2008, Standard or Enterprise Editions

[Complete Requirements](#)

Feature	Benefit
<p>Award-Winning Device / Port Control and Data Encryption within SCCM Infrastructure: Lumension® Device Control capabilities including granular policies for enforcing removable device usage, data encryption and malware prevention are integrated into the existing SCCM infrastructure.</p>	<p>Rapidly Deploy Device Control Capabilities</p> <ul style="list-style-type: none"> • Advanced, granular control of USB storage devices and other endpoint media devices / ports in a solution that can be immediately deployed. • Quickly deploy Lumension Device Control clients to all managed endpoints by utilizing your existing SCCM infrastructure. • Easily create device / port control policies from within the familiar SCCM console and deployed via the SCCM infrastructure. • Realize the device / port control, data encryption and malware prevention benefits of Lumension Device Control more quickly via existing SCCM infrastructure.
<p>Installation of Lumension Device Control for System Center on Existing SCCM Server: Leverages current SCCM infrastructure, thus eliminating the need for a separate server / database.</p>	<p>Reduce IT and Security TCO</p> <ul style="list-style-type: none"> • Reduce the infrastructure acquisition and provisioning costs of a device / port control solution. • Reduce the maintenance and power consumption costs associated with “server sprawl.”
<p>Compatible with SCCM and Leverages Entire SCCM Implementation: Lumension Device Control for System Center is an SCCM Module, created using the SCCM Software Developers Kit. Because it follows the Microsoft integration guidelines completely, it is fully compatible with SCCM and leverages all aspects of an SCCM implementation. Granular policy enforcement controls within Lumension Device Control are made available via Lumension Device Control for System Center.</p>	<p>Improve Return on Your SCCM Investment (ROI)</p> <ul style="list-style-type: none"> • Extend SCCM implementation to include advanced, granular device / port control capabilities of Lumension Device Control. • Increase return on SCCM investment by leveraging it as a platform for advanced device / port control, data encryption and malware containment.
<p>Create and Deploy Device Control Policies within SCCM:</p> <ul style="list-style-type: none"> • Implements as fully functional and standardized SCCM policies. • Applies policies and enforces immediately according your unique system and user groups. • Deploys policies via the existing functional and tested SCCM infrastructure. 	<p>Save IT Time and Resources</p> <ul style="list-style-type: none"> • Reuse the system and user groups already established in the SCCM environment. • Leverage the significant time and effort made in configuring the SCCM environment to mirror the structure and manage the complexity of an organization across new applications. • Avoid the costs and impact on productivity required to duplicate this effort for every new application.
<p>Administer Device Control Policies within SCCM Console: Lumension Device Control for System Center brings device / port control policy management to the familiar SCCM console.</p>	<p>Reduce IT Management + Administration Time</p> <ul style="list-style-type: none"> • By strictly adhering to established SCCM UI standards, Lumension Device Control for System Center administrators can get up-to-speed quickly. • Leveraging the familiar SCCM UI, Lumension Device Control for System Center reduces costs and productivity hits that are common as administrators are trained on, learn, and implement new software. • Integrated help feature provides easy access to contextual information that aids in completing the task at hand.
<p>Prevent Data Loss & Malware Proliferation: Lumension Device Control for System Center enables the use of SCCM policy and enforcement capabilities for device / port control, data encryption and malware containment.</p>	<p>Enhance Your Security Posture</p> <ul style="list-style-type: none"> • Leverage established processes / procedures for enforcing SCCM configuration policy to create / enforce device / port control policies. • Eliminate complexity and costs associated with duplicating policy processes for different applications. • Reduce costs and increase speed of policy implementation. • Create and enforce powerful and granular device / port control policies in the same way as normal SCCM configuration policies.

Contact Lumension

- » Global Headquarters
15880 N. Greenway Hayden
Suite 100
Scottsdale, AZ 85260
+1.480.970.1025
sales@lumension.com
- » United Kingdom
+44.0.1908.357.897
sales.uk@lumension.com
- » Europe
+352.265.364.11
sales-emea@lumension.com
- » Asia & Pacific
+65.6725.6415
sales-apac@lumension.com