

## ControlGuard Device Control

ControlGuard Device Control provides the endpoint protection to round out IT security by allowing the monitoring, detection, logging, alerts, blocking, responses and reports on removable devices and endpoints on laptops, PCs and servers across the network.

ControlGuard Device Control is a policy-based security software that provides an administrative Management Console for configuring security policies related to endpoints, portable devices, and the type and volume of data that

is permitted to be transferred. ControlGuard Device Control allows defining policies that require all files copied to removable storage must be encrypted first.

Configurations can be made for layered positive and negative security policies.

Granularity of configurations can be defined at each user group, user, computer, endpoint and device on the network.

### Benefits

- Detects intrusion of unauthorized devices or use of unauthorized ports and peripherals
- Real-time monitoring of endpoints and usage that provides alerts and logging including customizable user prompts, SMTP traps and email
- Blocks authenticates user groups, users, computers and endpoints devices by unique ID as well as limits copy volumes
- Works as a measure against malware, pod-slurping, and thumb-sucking attacks (cannot exploit the autorun vulnerability)
- Security on client includes an advanced anti-tampering mechanism that detects and prevents disabling
- Client agent maintains security policies and logging even while the network or servers are unavailable (online or offline)
- Layered policy based protection includes positive and negative security policies
- Intelligent distribution of client agents
  - Security policy application for hot-plugging of plug-&-play devices
- Dynamic policy swap (automatically applies online and offline)
- Remote batch deployment and live update mechanisms
- Directory integration with enterprise directory infrastructure such as Microsoft Active Directory and Novell eDirectory
- Comprehensive query and reports on events and activities
- Real-time logging, notifications, actions and auditing

# ControlGuard Device Control

## Devices and Endpoints Supported:

### Removable Storage:

- iPods
- MP3s Players
- MP4s Players
- SD Cards
- Flash Memory Cards
- SDHC Cards
- Micro SD Cards
- Compact Flash
- Memory Sticks
- Mini SD Cards
- Mini DV Tape
- Iomega Zip Disk
- Magneto Optical Disk
- DLT Tape Cartridge
- LTO Tape Cartridge

### CDs Media:

- CD-R
- CD-RW
- DVD-R
- DVD+R
- DVD-RW/+RW
- HD DVD
- Mini DVD-R
- Blu-ray Disk
- Dual Layer DVD-R

### Modems:

- Internal Modems
- External Modems
- Datacard Modems
- ADSL Modems
- UMTS Modems
- GPRS Modems
- Cable Modems

### Ports:

- USB
- FireWire
- Infrared
- Parallel
- Serial
- PCMCIA
- PS/2
- IDE
- PCI
- SD Port

### WiFi Adapters:

- Internal Wireless
- External Wireless

### RIM Devices & Phones:

- Blackberries
- Smartphones
- Wireless Handheld Devices
- iPhones

### PDA / XDA Devices:

- Windows CE Devices
- Windows Mobile Devices
- Palm devices

### Imaging:

- Still Cameras
- Webcams
- Camcorders
- Scanners

### Tape Devices:

- DV Tape
- Iomega Zip Tape
- Magneto Optical Tape

### Encrypted Devices:

- U3 Devices
- Secure USB Devices

### Printers:

- Local printers
- Network Printers
- Virtual Printers

### Other:

- Floppies
- Smart Card Readers
- Keyloggers
- Print Screen

## System Requirements:

### Server Hardware and Software Requirements

**CPU:** Intel Pentium 4-class or higher, 450 MHz minimum 2.8 GHz

**Disk space:** 2GB free

**RAM:** 1 GB RAM minimum, 2 GB recommended

**Server:** Microsoft IIS with ASP.NET 2.0

**OS:** MS Windows® 2003 Std. or Ent. SP 0-2 and R2

**Browser:** Microsoft Internet Explorer® 5.5 or greater

### Database

**Database Applications:** MSDE 2000 (included default), Microsoft Express® 2005, Microsoft SQL® 2000 SP 3 and above, or Microsoft SQL® 2005

### EAM Agent - desktop/laptop clients

**CPU:** Pentium III 1 GHz or greater

**Network Connection:** TCP/IP for remote access

**RAM:** 512 MB

**Disk Space:** 200 MB minimum

**OS:** MS Windows 2000 Pro. SP 4, 2000 Server SP 4, 2000 Advanced Server SP 4, MS Windows 2003 Std. or Ent. SP 0-2 and R2, XP Professional SP 0-3, XP Tablet PC Edition SP 0-3, Vista® Ent.\Ultimate\Business SP 0-1, MSI Ver. 2 or higher

( www.controlguard.com )



ZMA - ESET Argentina  
 Larrea 1011 piso 8° C1117ABE, Ciudad de Buenos Aires - ARG  
 Tel: 011 4825 1602 - Fax: 011 4825 7692  
 www.zma.com.ar / info@zma.com.ar