

If you need to secure your endpoint computers You need Device Protector to help you keep it that way

Device Protector is Data Loss Prevention (DLP) and device control endpoint security software that enforce endpoint devices protection policies on organization computers. The software helps to secure IT environments from un-trusted endpoint devices that can be used by potential intruders to access sensitive organization data and prevent data leakage and information theft.

Real-time protection

Device Protector is acting as a server to all protected computers and can be deployed through the software management console or through any 3rd party deployment system by using the software MSI package deployment option. The software powerful engine can control and secure any number of computers by installing a remote service on the protected computers. It is supporting devices online and offline protection including read-only, read-write, working hours, exclude users and exclude media serial numbers capabilities.

tan Seave Device Protector + 33 ♦ Home → Sam ④ Reports ③ Tools ④ •					-Secure e Protector
To set or chang		options, go to Settings option	228-	Search	
Computer Name	IP Address 192.168.0.1	Last Version	Last Update 24/06/13 10:36:25	Last Status Protected Successfully	
Ø WIN-8	10.0.10	13	20/06/13 18 21:00	Protected Successfully	
	Add Computers	Deploy Computers	Set Protection	Delete Computers	Refresh List
		Your license will be	expired in 30 days		

Real-time reports

Device Protector is collecting activity logging events of the protected computers and generates real-time reports. The reports provide logging information about the protected devices activity including optional actions like command executions, e-mail messages, Syslog notification and exporting capabilities.



Real-time options

Device Protector provides optional software settings that include automatic software startup options, automatic events removal, unstoppable client service, client notification message, auto discovery and multiple redundant servers.

A Lan-Secure Device Protector - 1.3							
🛟 Home 🏓 Scan 🥹 Repo	Lan-Secure Device Protector						
Options	<u>^</u>						
Events removal							
Choose automatic events removal o	ptions from the list below						
Protected events removal after:	10 🕂 Daws 🔹						
Failed events removal after:	10 💠 Days 👻						
System events removal after:	10 🔄 Days 💌						
Clients service		user control					
Clients release							
Choose how to release DHCP address of protected wireless devices							
Protect wireless devices without DHCP release							
Release DHCP address before wireless devices being protected							
		Save Cancel					
	Your license will be expire	nd in 30 days					

Device Protector Key Features

- Real-time Data Loss Prevention (DLP) device control endpoint security.
- Support Bluetooth, DVD/CD-ROM, Firewire, Floppy, Imaging, Infrared, Microphones, Modems, Portable Mobile Phones, Ports, Printers, Removable Disks, SD Cards, Sound, Tape Drives and Wireless devices.
- Support online and offline endpoint security including read-write, read-only and working hours protection options.
- Support device control exclude options of users and DVD/CD, Flash drives media serial numbers.
- Optional settings like unstoppable protection service, events removal and client's notification.
- Optional automatic computers discovery and scanning.
- Optional actions and exporting capabilities on protected devices.

Device Protector System requirements

- A 800 MHz or faster processor with at least 256 MB of RAM
- Microsoft Windows XP, Windows 7/Vista™ or 2003/2008 Server
- At least 10 MB of available free space on your hard disk

