



Kaspersky Embedded Systems Security

Kaspersky Embedded Systems Security

- ▶ designed for protection of ATMs and POS, as well as other devices running Microsoft Windows
- ▶ protects devices with a limited RAM size (256 MB and more) and limited free hard disk space (100 MB and more)
- ▶ will never require a reboot!*

* ESS will not require a reboot, but a reboot can be required from Windows Installer or previously installed AV solutions to release drivers

Kaspersky Embedded Systems Security

- ▶ can be managed by
 - Kaspersky Embedded Systems Security Console (local/remote)
 - Command-line
 - Kaspersky Security Center plugin

- ▶ requires no/limited network/internet connectivity
 - works with weak connection channels

Kaspersky Embedded Systems Security Features

► Features

- Real-time file protection
- On-demand anti-virus scan
- Kaspersky Security Network services integration
- Applications Launch Control
- Device Control

Supported Operating Systems

- ▶ Windows XP Embedded x86 SP3
- ▶ Windows Embedded POSReady 2009 x86
- ▶ Windows Embedded Standard/Enterprise 7 SP1 x86/x64
- ▶ Windows Embedded POSReady 7 x86/x64
- ▶ Windows Embedded 8.0 Standard x86/x64
- ▶ Windows Embedded 8.1 Industry Professional/Enterprise x86/x64
- ▶ Windows Embedded 8.1 Professional x86/x64
- ▶ Windows XP x86 SP2/SP3
- ▶ Windows 7 Professional/Enterprise SP1 x86/x64
- ▶ Windows 8 Professional/Enterprise x86/x64
- ▶ Windows 8.1 Professional/Enterprise x86/x64
- ▶ Windows 10 Professional/Enterprise x86/x64
- ▶ Windows 10 IoT Enterprise x86/x64

RAM Requirements

- ▶ 256 MB to install the Applications Launch Control component only on the computer under Microsoft® Windows® XP Embedded / Windows XP / Windows Embedded POSReady 2009
- ▶ 512 MB to perform full installation of all components on the computer under 32-bit Microsoft Windows XP Embedded / Windows XP / Windows Embedded POSReady 2009
- ▶ 1 GB to perform full installation of all components on the computer under other 32-bit Microsoft Windows OS
- ▶ 2 GB to perform full installation of all components on the computer under different types of the 64-bit Microsoft Windows OS



- Kaspersky Embedded Systems Security
 - Real-Time Protection
 - Real-Time File Protection
 - KSN Usage
 - Computer Control
 - Applications Launch Control
 - Rule Generator for Applications Launch Control
 - Device Control
 - Rule Generator for Device Control
 - On-Demand Scan
 - Scan at Operating System Startup
 - Critical Areas Scan
 - Quarantine Scan
 - Application Integrity Control
 - Update
 - Database Update
 - Software Modules Update
 - Copying Updates
 - Rollback of Application Database Update
 - Storages
 - Quarantine
 - Backup
 - Logs
 - System audit log
 - Task logs
 - Licensing

Kaspersky Embedded Systems Security 1.1.0.104



Protection

<u>Real-Time File Protection:</u>	Running
Detected:	0
<u>KSN Usage:</u>	Running
Untrusted conclusions:	0
<u>Critical Areas Scan</u>	
Last scan date:	5/30/2016 6:09:30 AM
<u>Quarantined objects:</u>	0
Space used:	0
<u>Backed up objects:</u>	0
Space used:	0

Control

<u>Applications Launch Control:</u>	Running
Operation mode:	Statistics Only
Applications launches denied:	6
Average processing time (ms):	124
<u>Device control:</u>	Running
Operation mode:	Statistics Only
Devices blocked:	1

Update

Database status:	Application database is up to date
Database release date:	5/30/2016 8:46:00 AM (UTC)
Number of database records:	7516100
Status of the latest completed Database Update task:	Completed
Number of module updates available:	0
Number of module updates installed:	0

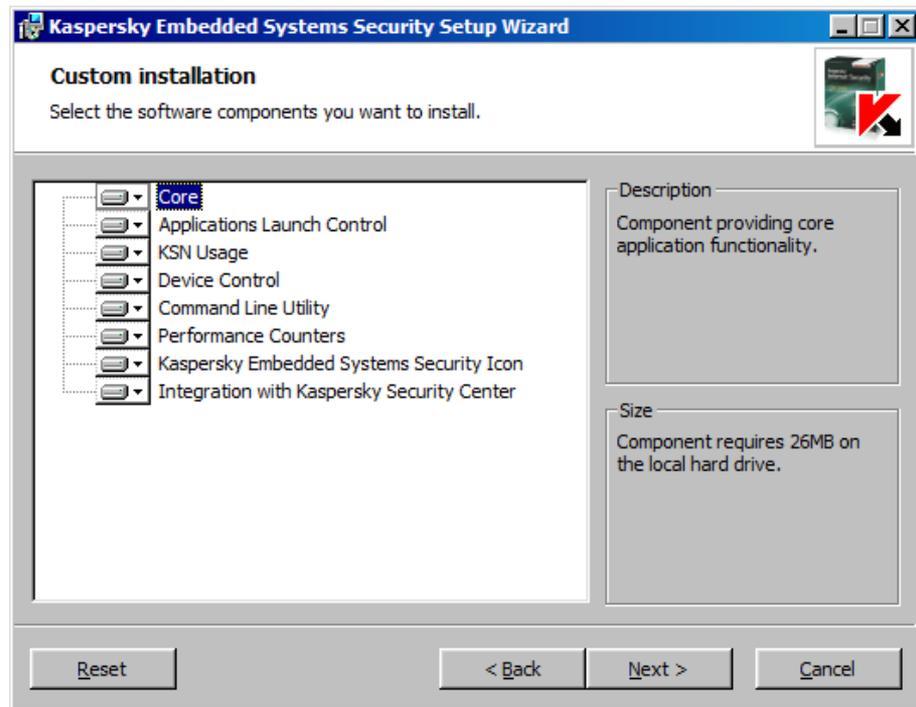
Expiration date: 4/25/2017

[Application properties](#)[Connect to another computer](#)

Kaspersky Embedded Systems Security

- ▶ Light install package
 - ~65MB
 - does not include Anti-Virus protection

 ess_light.kud	KUD File	5/17/2016 1:01 AM	10 KB
 ess_x64.msi	Windows Installer P...	5/17/2016 1:10 AM	31,944 KB
 ess_x86.msi	Windows Installer P...	5/17/2016 1:10 AM	29,640 KB
 klcfginst.exe	Application	5/17/2016 1:10 AM	4,152 KB
 license.txt	TXT File	2/24/2016 8:33 AM	24 KB
 setup.exe	Application	5/17/2016 1:10 AM	467 KB



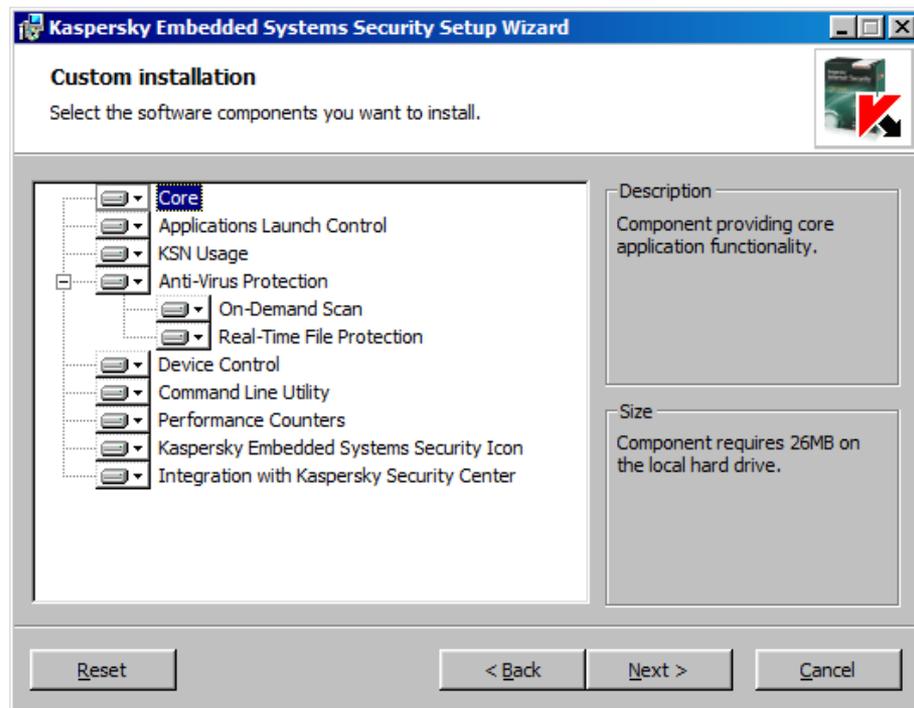
Kaspersky Embedded Systems Security Default Deny

- ▶ Default Deny only installation mode
 - low system requirements (\geq 256MB RAM)
 - low traffic consumption (no regular AV updates)
 - no internet connection required
 - Executable files, DLLs, drivers
 - Hash sum check, digital certificate check, destination check
 - Optional 2-layer check for black-/whitelisted applications with Kaspersky Security Network

Kaspersky Embedded Systems Security

- ▶ Full install package
 - ~155MB
 - includes all components
 - Most components are optional
 - Applications Launch Control not

 bases.cab	CAB File	5/17/2016 12:55 AM	95,120 KB
 ess.kud	KUD File	5/17/2016 1:01 AM	10 KB
 ess_x64.msi	Windows Installer P...	5/17/2016 1:09 AM	31,940 KB
 ess_x86.msi	Windows Installer P...	5/17/2016 1:09 AM	29,636 KB
 klcfginst.exe	Application	5/17/2016 1:10 AM	4,152 KB
 license.txt	TXT File	2/24/2016 8:33 AM	24 KB
 setup.exe	Application	5/17/2016 1:10 AM	466 KB



PCI DSS 3.1 mapping

- ▶ 5.1 Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).
- ▶ 5.1.1 Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software.
- ▶ 5.2 Ensure that all antivirus mechanisms are maintained as follows:
 - kept current
 - perform periodic scans
 - generate audit logs which are retained per PCI DSS Requirement 10.7.
- ▶ 5.3 Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

Real-time File Protection

- ▶ based on signature and heuristics
- ▶ scans files and NTFS streams. If a file is recognized to be infected the file will be processed according to the settings.

The screenshot shows the 'Real-Time File Protection' settings window in Kaspersky Embedded Systems Security. The window is divided into several sections: Management, Properties, and Statistics.

Management

Task status: **Running**
[Stop](#) [Pause](#)

Start time: 4/25/2016 5:00:18 AM
[Open task log](#)

Properties

Schedule: At application launch
Next start: At application launch

Objects protection mode: [On access and modification](#)
Use heuristic analyzer: [yes](#)
Heuristic analysis level: [Medium](#)
Apply Trusted Zone: [yes](#)
Use KSN services: [yes](#)
List hosts showing malicious activity as untrusted: [no](#)
Protection scope:
[My Computer](#), Security level: [recommended](#)

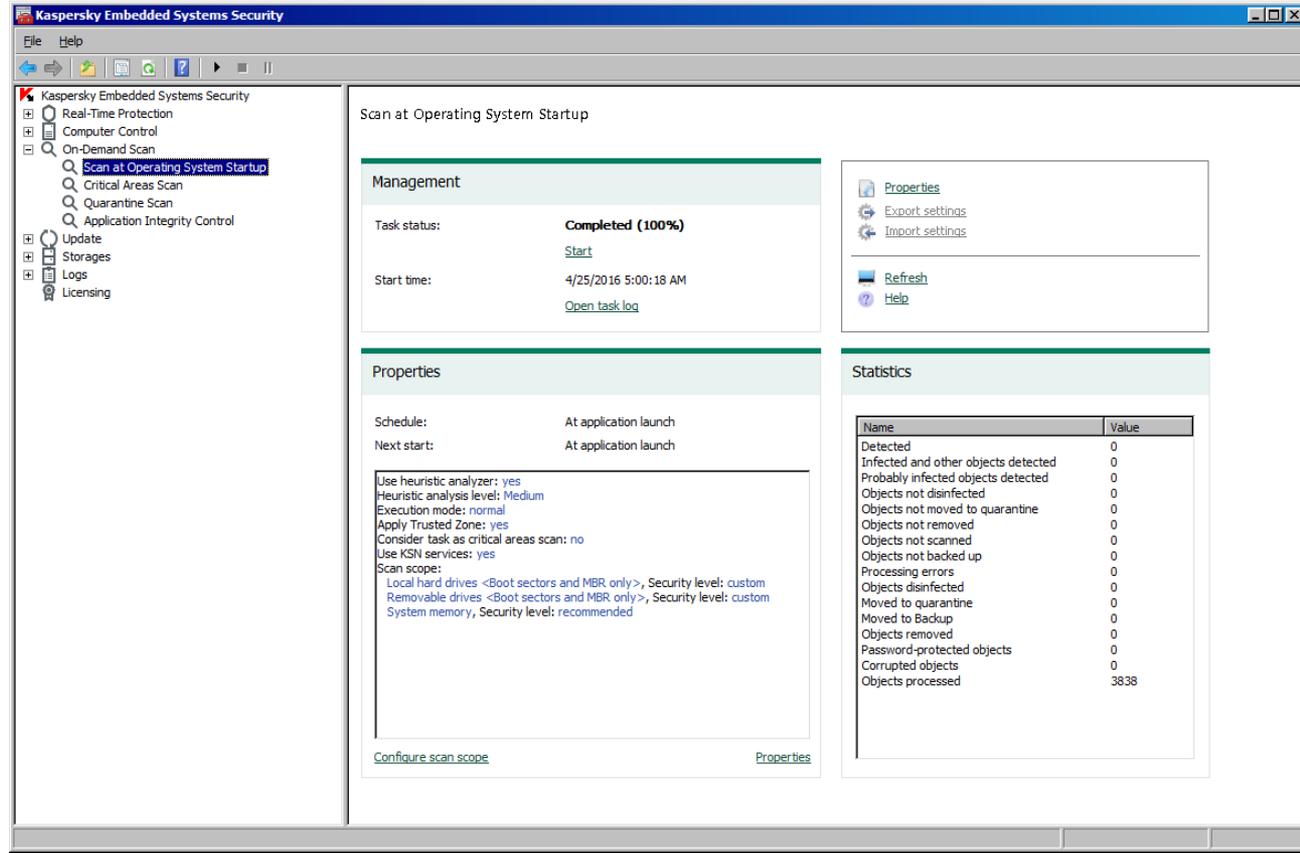
[Configure protection scope](#) [Properties](#)

Statistics

Name	Value
Detected	1
Infected and other objects detected	1
Probably infected objects detected	0
Objects not disinfected	1
Objects not moved to quarantine	0
Objects not removed	0
Objects not scanned	0
Objects not backed up	0
Processing errors	10
Objects disinfected	0
Moved to quarantine	0
Moved to Backup	1
Objects removed	1
Password-protected objects	0
Corrupted objects	0
Objects processed	2206

On-Demand Anti-Virus Scan

- ▶ scans specified areas for viruses and other computer security threats. The application scans files, the RAM of the protected device, and autorun objects.



The screenshot displays the Kaspersky Embedded Systems Security application window. The left sidebar shows a tree view with 'Scan at Operating System Startup' selected. The main area is titled 'Scan at Operating System Startup' and contains three panels: Management, Properties, and Statistics.

Management

Task status: **Completed (100%)**
[Start](#)

Start time: 4/25/2016 5:00:18 AM
[Open task log](#)

Properties

Schedule: At application launch
Next start: At application launch

Use heuristic analyzer: [yes](#)
Heuristic analysis level: [Medium](#)
Execution mode: [normal](#)
Apply Trusted Zone: [yes](#)
Consider task as critical areas scan: [no](#)
Use KSN services: [yes](#)
Scan scope:
Local hard drives <Boot sectors and MBR only>, Security level: custom
Removable drives <Boot sectors and MBR only>, Security level: custom
System memory, Security level: recommended

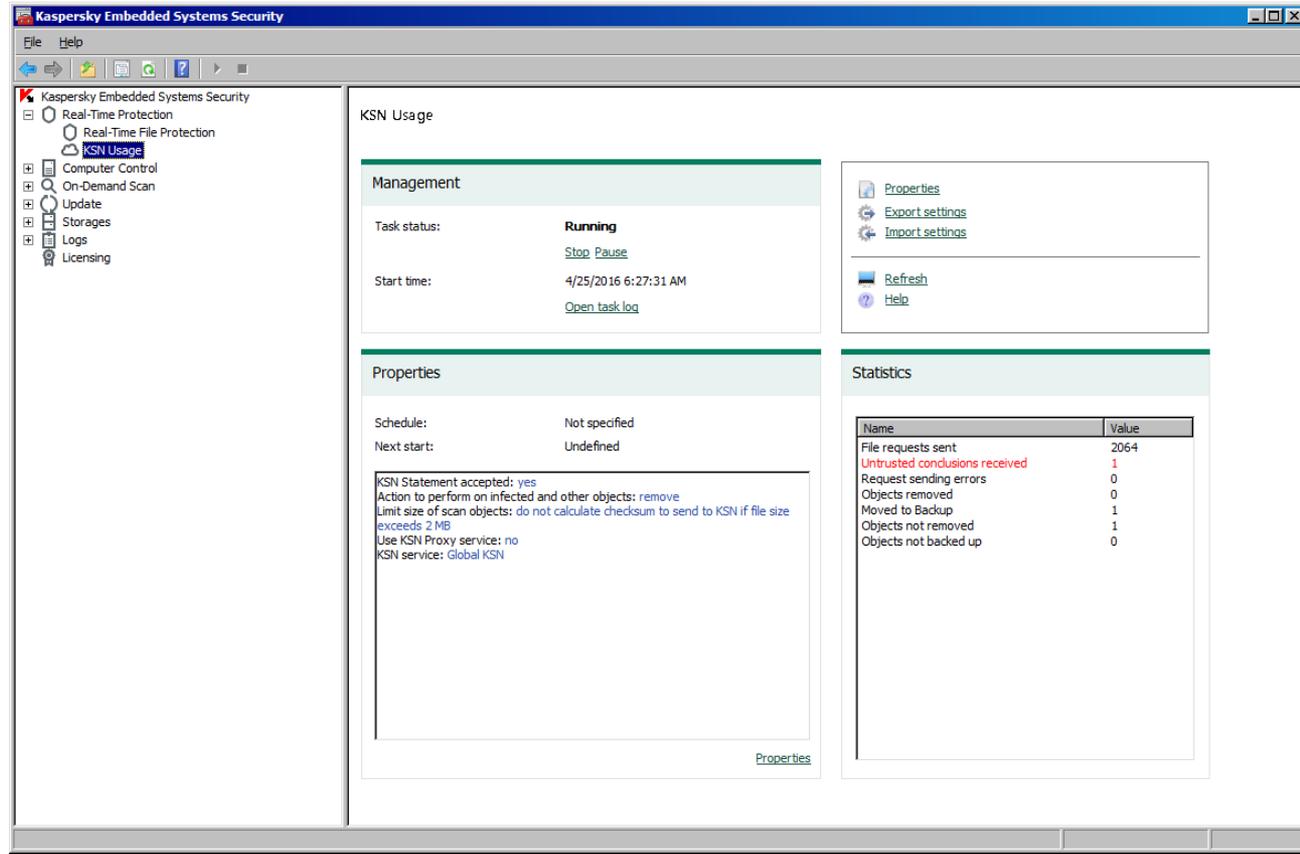
[Configure scan scope](#) [Properties](#)

Statistics

Name	Value
Detected	0
Infected and other objects detected	0
Probably infected objects detected	0
Objects not disinfected	0
Objects not moved to quarantine	0
Objects not removed	0
Objects not scanned	0
Objects not backed up	0
Processing errors	0
Objects disinfected	0
Moved to quarantine	0
Moved to Backup	0
Objects removed	0
Password-protected objects	0
Corrupted objects	0
Objects processed	3838

Kaspersky Security Network Services Integration

- ▶ increases protection tasks efficacy by the means of Kaspersky Security Network cloud services, which conclusions regarding potential security dangers are based on Kaspersky Lab up-to-date data.



The screenshot displays the Kaspersky Embedded Systems Security interface. The left sidebar shows a tree view with 'KSN Usage' selected. The main window is titled 'KSN Usage' and contains three sections: Management, Properties, and Statistics.

Management

Task status: **Running**
[Stop](#) [Pause](#)

Start time: 4/25/2016 6:27:31 AM
[Open task log](#)

Properties

Schedule: Not specified
Next start: Undefined

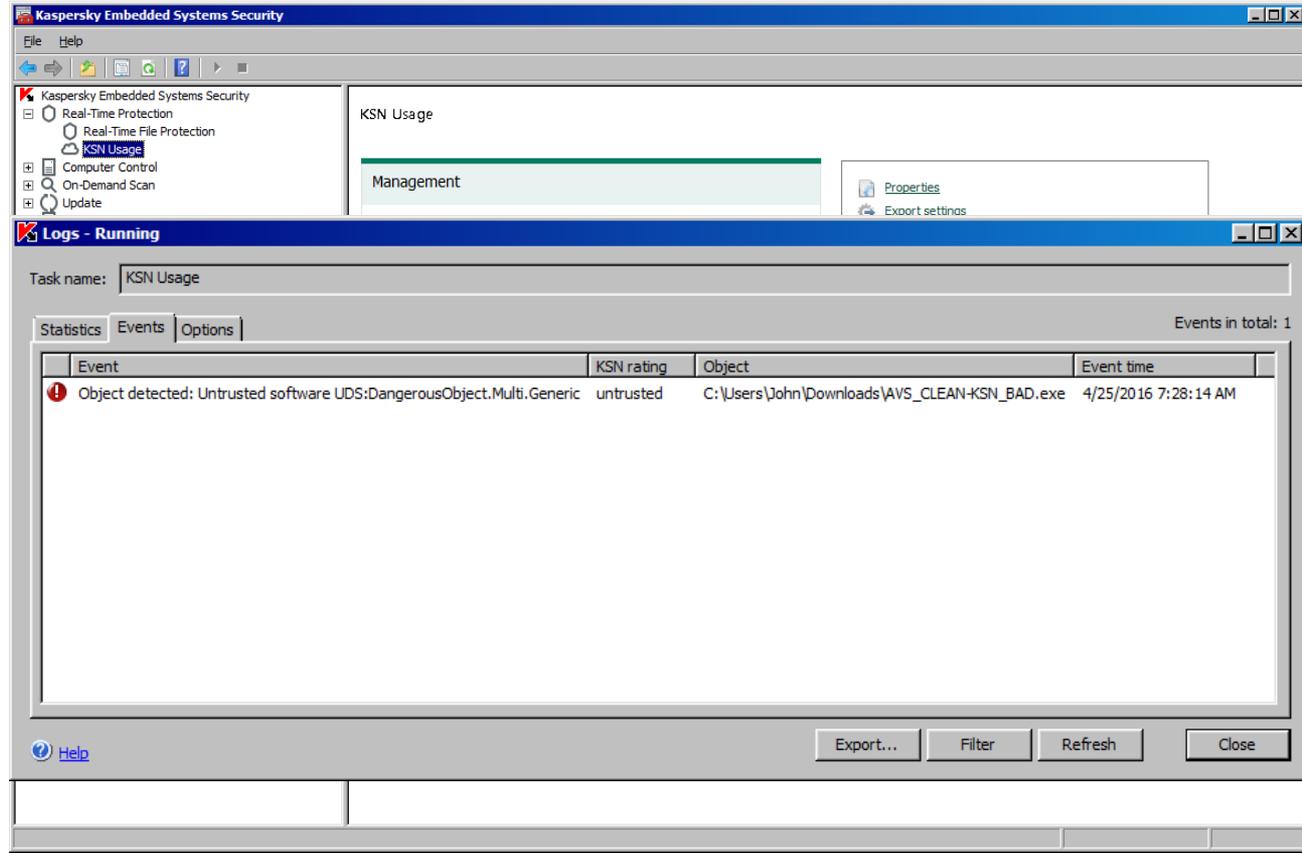
KSN Statement accepted: [yes](#)
Action to perform on infected and other objects: [remove](#)
Limit size of scan objects: [do not calculate checksum to send to KSN if file size exceeds 2 MB](#)
Use KSN Proxy service: [no](#)
KSN service: [Global KSN](#)

Statistics

Name	Value
File requests sent	2064
Untrusted conclusions received	1
Request sending errors	0
Objects removed	0
Moved to Backup	1
Objects not removed	1
Objects not backed up	0

Kaspersky Security Network Services Integration

- ▶ used by Real-Time File protection, On-Demand Scan and Applications Launch Control



The screenshot displays the Kaspersky Embedded Systems Security interface. The top window shows the main menu with 'KSN Usage' selected. Below it, the 'Logs - Running' window is open, showing a task named 'KSN Usage'. The 'Events' tab is active, displaying a table with one event entry.

Event	KSN rating	Object	Event time
Object detected: Untrusted software UDS: DangerousObject.Multi.Generic	untrusted	C:\Users\John\Downloads\AVS_CLEAN-KSN_BAD.exe	4/25/2016 7:28:14 AM

Buttons at the bottom of the logs window include 'Help', 'Export...', 'Filter', 'Refresh', and 'Close'.

Applications Launch Control

- ▶ allows or denies the execution of executable files, scripts, MSI packages, driver loading and DLL modules loading via defined applications launch control rules.

The screenshot shows the 'Applications Launch Control' window in Kaspersky Embedded Systems Security. The interface is divided into several sections:

- Management:** Shows the task status as 'Running', with a 'Stop' button. The start time is '4/25/2016 6:42:21 AM' and there is an 'Open task log' button.
- Properties:** Shows the schedule as 'Not specified' and 'Next start' as 'Undefined'. A detailed list of task mode settings is provided, including: 'apply rules', 'Maintain previous start settings for applications launch control: yes', 'Apply rules to executable files: yes', 'Monitor DLL modules loading: no', 'Apply rules to scripts and MSI packages: yes', 'Deny applications untrusted by KSN: no', 'Allow applications trusted by KSN: no', 'Users and / or user groups allowed to run applications trusted by KSN: Everyone', 'Rules in total: 30', 'Rules for executable files: 23', and 'Rules for scripts and MSI packages: 7'. There are links for 'Applications Launch Control rules' and 'Properties' at the bottom.
- Statistics:** A table showing the following data:

Name	Value
Blocked	1
Allowed	4
Processing errors	0
Average file run processing time (ms)	37
- Navigation:** Includes buttons for 'Properties', 'Export settings', 'Import settings', 'Refresh', and 'Help'.

Applications Launch Control

- ▶ allows or denies the execution of executable files, scripts, MSI packages, driver loading and DLL modules loading via defined applications launch control rules.

The screenshot displays the Kaspersky Embedded Systems Security application interface. On the left, a tree view shows the 'Applications Launch Control' option selected under 'Computer Control'. The main window is the 'Task settings' dialog box, which is open to the 'General' tab. The 'Task mode' dropdown is set to 'Apply Rules'. The 'Maintain previous start settings for applications launch control' checkbox is checked. Under 'Rules usage scope', the checkboxes for 'Apply rules to executable files' and 'Apply rules to scripts and MSI packages' are checked, while 'Monitor loading of DLL modules' is unchecked. The 'KSN Usage' section has 'Deny applications untrusted by KSN' and 'Allow applications trusted by KSN' both unchecked. The 'Users and / or user groups allowed to run applications trusted by KSN:' field contains 'Everyone'. A warning icon and text at the bottom state: 'Monitoring the DLL modules loading may affect your operating system performance.' The 'OK' and 'Cancel' buttons are visible at the bottom right.

	Value
1	1
4	4
0	0
Processing time (ms)	37

Applications Launch Control

- ▶ allows creation of rules manually

The screenshot shows the 'Applications Launch Control rules' management window in Kaspersky Embedded Systems Security. The window title is 'Applications Launch Control rules' and it contains a search bar, 'Add...' and 'Remove Selected' buttons, and a 'Show rules for the file' button. Below these is a table listing 30 rules. The table has columns for Type, Rule name, Users, Triggering criterion, Exclusions, Scope, and Generation method. The rules are mostly 'Allowing' and apply to various system and application files.

Type	Rule name	Users	Triggering criter...	Exclusions	Scope	Generation met...
Allowing	EMBEDDEDSTD7:7z.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:7zFM.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:7zG.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:Microsoft(R) Connection Manager signed by O=MICROSOFT CORPORATION, L=REDM...	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7: signed by O=VMWARE, INC., L=PALO ALTO, S=CALIFORNIA, C=US	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:preinstallinf.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:softtehdcfg.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:Windows® Internet Explorer signed by O=MICROSOFT CORPORATION, L=REDMOND...	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:Kaspersky Embedded Systems Security signed by O=KASPERSKY LAB, L=MOSCOW, S=...	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:MSS CS signed by O=DEVGURU CO LTD, L=GEUMCHEON-GU, S=SEOUL, C=KR	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:SAMSUNG USB Drivers for Mobile Phones signed by O=SAMSUNG ELECTRONICS CO., L=...	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:rvmSetup.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:TPAutoConnect signed by O=CORTADO AG, L=BERLIN, S=BERLIN, C=DE	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:VGAAuthCLI.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:VGAAuthService.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:VMwareAliasImport.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:Microsoft® .NET Framework signed by O=MICROSOFT CORPORATION, L=REDMOND,...	Everyone	Digital certificate	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:dfsvc.ni.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7:PresentationFontCache.ni.exe	Everyone	SHA256 hash	No	Executable files	Generated auto...
Allowing	EMBEDDEDSTD7: signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Everyone	Digital certificate	No	Scripts and M...	Generated auto...
Allowing	EMBEDDEDSTD7: signed by O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Everyone	Digital certificate	No	Scripts and M...	Generated auto...
Allowing	EMBEDDEDSTD7: signed by O=KASPERSKY LAB, L=MOSCOW, S=MOSCOW CITY, C=RU	Everyone	Digital certificate	No	Scripts and M...	Generated auto...
Allowing	EMBEDDEDSTD7:54ehRb.msi	Everyone	SHA256 hash	No	Scripts and M...	Generated auto...

Applications Launch Control

- ▶ allows creation of rules manually or automatically by meaning of Rule Generator task.

The screenshot displays the Kaspersky Embedded Systems Security application window. The left sidebar shows a tree view with 'Rule Generator for Applications Launch Control' selected. The main window is titled 'Rule Generator for Applications Launch Control' and is divided into three sections: Management, Properties, and Statistics.

Management

Task status: **Completed (100%)**
[Start](#)

Start time: 4/25/2016 6:41:02 AM
[Open task log](#)

Properties

Schedule: Not specified
Next start: Undefined

Prefix for rule names: EMBEDDEDSTD7:
Generate rules for running applications: yes
Process files from the following folders:
c:\Program Files
Files: executables
C:\Windows
Files: executables, MSI packages, scripts
Generate rule based on settings: digital certificate
Require strict compliance with digital certificate: yes
If those settings are missing, use: SHA256 hash
Generate rules for user or group: Everyone
Upon task completion, add rules to the Applications Launch Control rules list: yes
Principle of adding: merge with existing rules

[Properties](#)

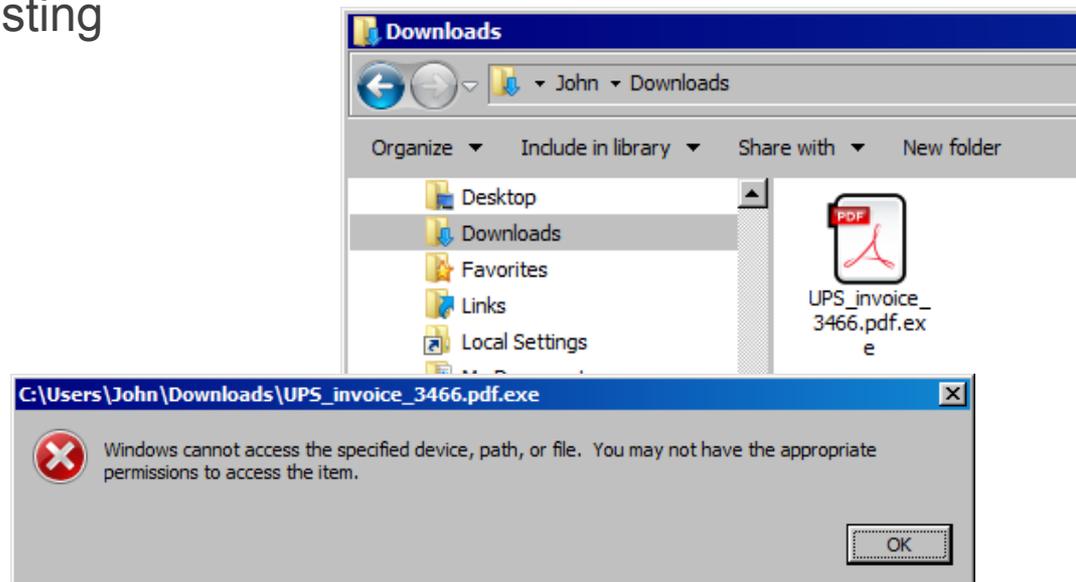
Statistics

Name	Value
Files processed	819
Rules based on digital certificate	16
Rules based on SHA256 hash	14
Rules based on path to a file	0
Rule generation errors	0

[Properties](#) [Export settings](#) [Import settings](#)
[Refresh](#) [Help](#)

Applications Launch Control

- ▶ denies application execution if not allowed explicitly, so called whitelisting



Device Control

- ▶ allows or denies usage of mass storages connected to protected computer via USB. External devices control is based on the allowing rules and Default Deny technology.

The screenshot shows the Kaspersky Embedded Systems Security interface. The left sidebar contains a tree view with the following items: Kaspersky Embedded Systems Security, Real-Time Protection, Computer Control, Applications Launch Control, Rule Generator for Applications Launch Control, **Device Control** (highlighted), Rule Generator for Device Control, On-Demand Scan, Update, Storages, Logs, and Licensing. The main window is titled 'Device Control' and is divided into three panels: Management, Properties, and Statistics.

Management

Task status: **Running**
[Stop](#)

Start time: 4/25/2016 7:44:15 AM
[Open task log](#)

Properties

Schedule: At application launch
Next start: At application launch

Task mode: [apply default deny](#)
Allow using all mass storages when the Device Control task is not running: [no](#)
Allowing rules: 1

[Device Control rules](#) [Properties](#)

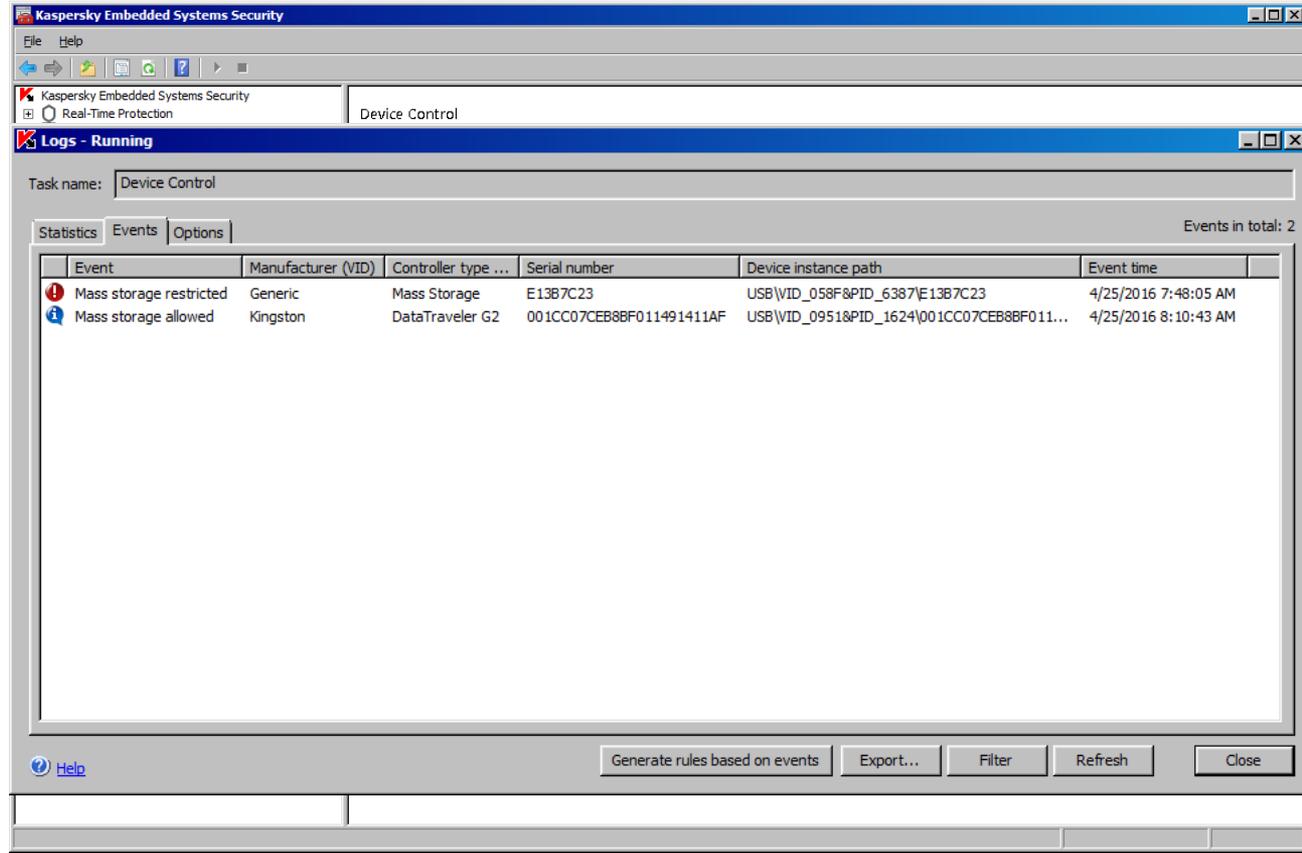
Statistics

Name	Value
Mass storages denied	1
Mass storages allowed	0

Buttons: [Properties](#), [Export settings](#), [Import settings](#), [Refresh](#), [Help](#)

Device Control

- ▶ allows or denies usage of mass storages connected to protected computer via USB. External devices control is based on the allowing rules and Default Deny technology.



The screenshot shows the 'Kaspersky Embedded Systems Security' interface. The 'Logs - Running' window is open, displaying a table of events for the 'Device Control' task. The table has columns for Event, Manufacturer (VID), Controller type, Serial number, Device instance path, and Event time. Two events are listed: 'Mass storage restricted' for a Generic Mass Storage device and 'Mass storage allowed' for a Kingston DataTraveler G2 device.

Event	Manufacturer (VID)	Controller type ...	Serial number	Device instance path	Event time
Mass storage restricted	Generic	Mass Storage	E1387C23	USB\VID_058F&PID_6387\{E1387C23}	4/25/2016 7:48:05 AM
Mass storage allowed	Kingston	DataTraveler G2	001CC07CEB8BF011491411AF	USB\VID_0951&PID_1624\{001CC07CEB8BF011...}	4/25/2016 8:10:43 AM

Device Control

- ▶ controls the following USB mass storages connections:
 - ▶ Flash drives
 - ▶ CD ROM drives
 - ▶ Floppy drives
 - ▶ MTP devices*

- ▶ Identifies trusted devices by
 - exact match of InstanceID
 - Use of masks by VID\PID

* Device Control task scope includes MTP-connected mass storages, if a protected computer works under OS Microsoft Windows 7 or higher. Kaspersky Embedded Systems Security controls MTP-connected mass storages on a protected computer under OS Microsoft Windows XP, if the driver setups class GUID value for external devices that is identical to a standart Windows driver GUID value

Device Control

- ▶ allows generating allowing rules by meaning of Rule Generator task.

The screenshot displays the Kaspersky Embedded Systems Security interface. The left sidebar shows a tree view with 'Rule Generator for Device Control' selected. The main window is titled 'Rule Generator for Device Control' and contains three panels: Management, Properties, and Statistics.

Management

Task status: **Completed (100%)**
[Start](#)

Start time: 4/25/2016 10:14:50 AM
[Open task log](#)

Properties

Schedule: Not specified
Next start: Undefined

Add allowing rules to the Device Control rules list: [yes](#)
Principle of adding: [merge with existing rules](#)

[Properties](#)

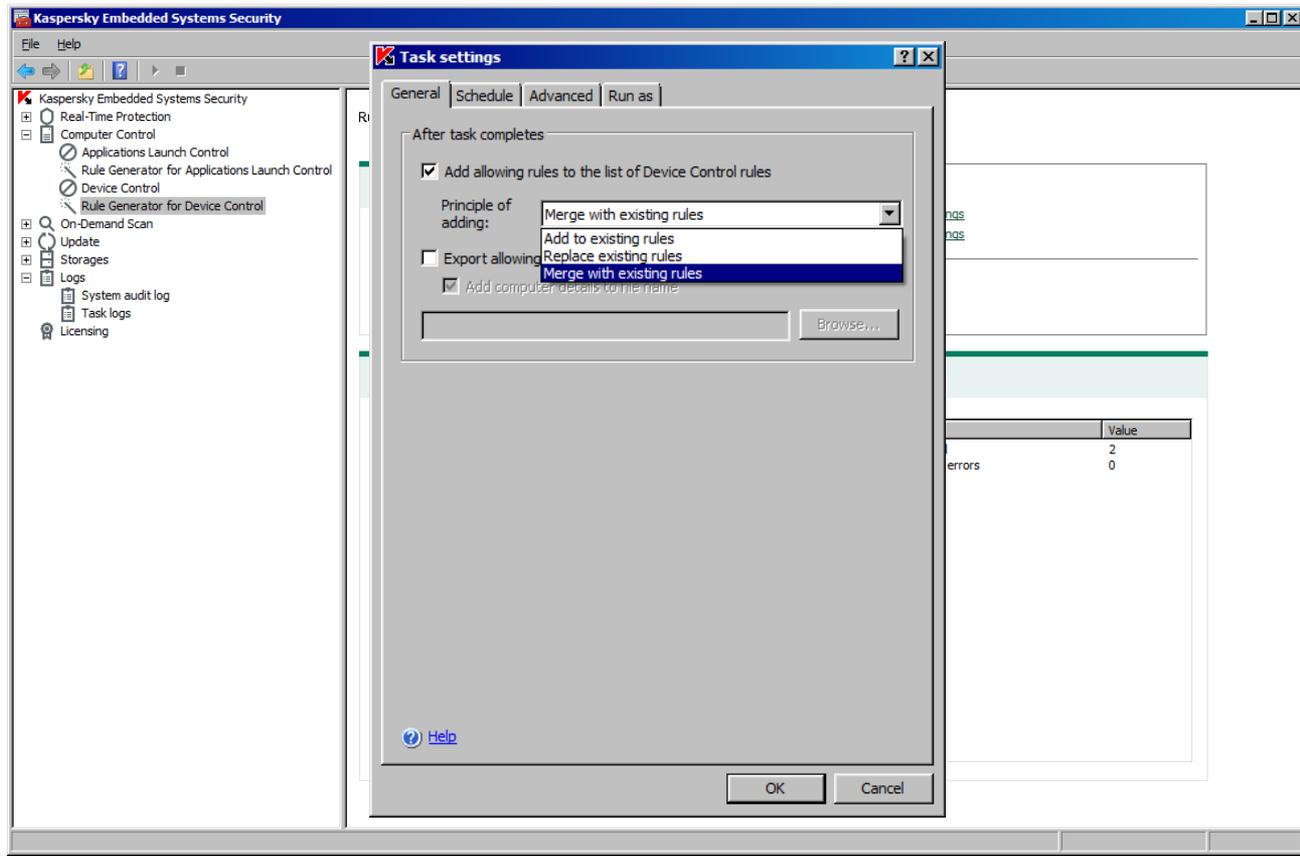
Statistics

Name	Value
Rules generated	2
Rule generation errors	0

[Properties](#) [Export settings](#) [Import settings](#)
[Refresh](#) [Help](#)

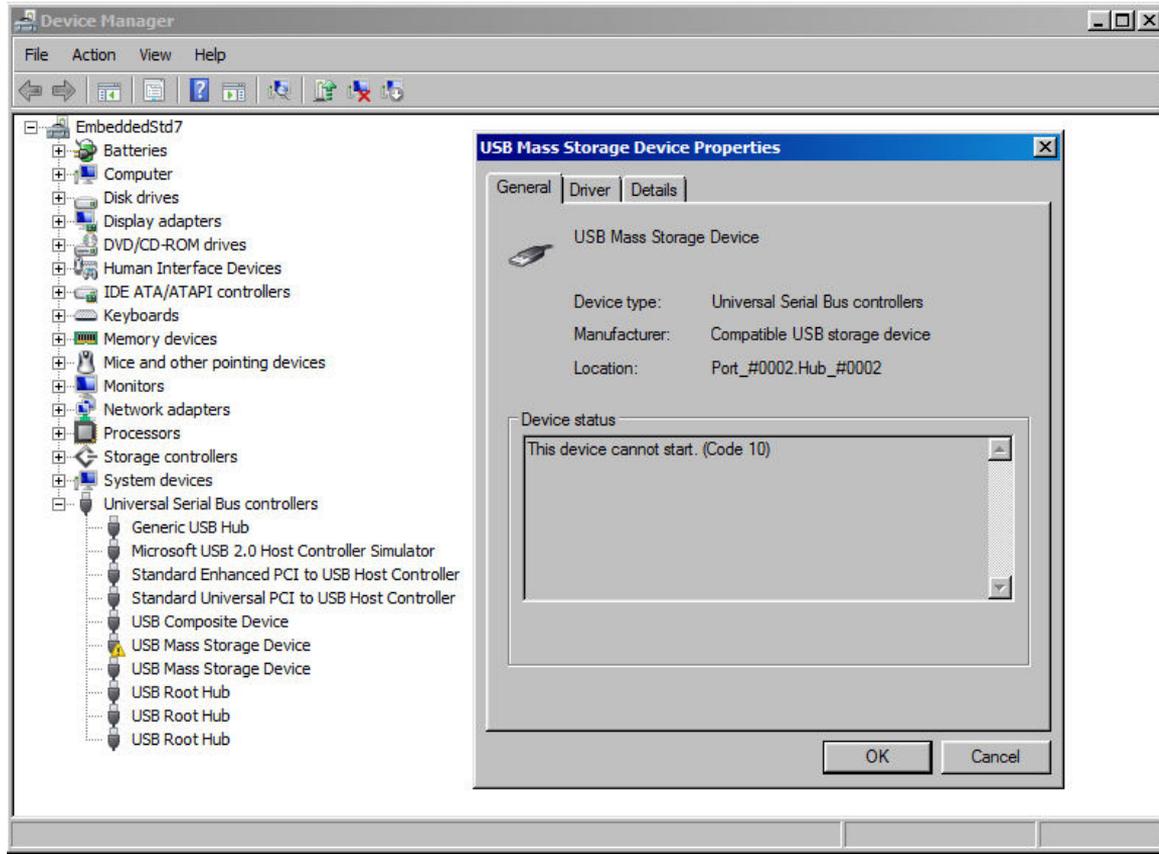
Device Control

- ▶ allows generating allowing rules by meaning of Rule Generator task.
- ▶ Allowing rules can be added/replaced and merged



Device Control

- ▶ prohibits Windows to assign a drive letter to a device if it's not allowed.



Thank you.