

Today's challenge

Employees of an organization often utilize portable storage devices to transport vital and sensitive data. Although these auxiliary devices offer convenience, they can also pose threats to information security if exploited or mishandled. As a best practice, the actions and whereabouts of these devices should be closely monitored and managed.

How Device Control Plus fits into your IT framework

Device Control Plus can be leveraged by IT administrators to gain comprehensive control over the numerous peripheral devices within their networks. This robust software solution includes a distinct set of features that enables the creation of flexible file access and transfer control policies. Therefore, by assigning the appropriate level of device permissions, all data transfers conducted via built-in and external devices can be meticulously tracked and regulated.

Device Control Plus is essential for averting data loss through USB and removable media, and is designed so that both preventative and restorative measures can be implemented effectively. This data leakage prevention tool features capabilities such as blacklisting and blocking data access, which are two of its many methods to deter file-based attacks. In the event of any emergency, out-of-box protocols like file tracing and file shadowing can also be adopted to ensure the diligent preservation of network integrity and retention of brand value.

Features



Device and Port Control

Effectively manage more than 17 types of peripheral devices from a singular console. Automatically discover the active ports within your network, as well as detect which devices are connected to your computers. You are empowered to take proactive actions to prevent malware injections and inadvertent data loss by disabling auto-run on all questionable devices.



File Access Control

Create and fine-tune file access control policies based on the specific departments and employee functions within your organization. Role-based access control protocol ensures that all users have sufficient access to corporate information pertaining to their roles, while other data irrelevant to their tasks is kept off-limits. Provisions such as granting read-only permissions also minimizes data loss as business-critical information can be restricted to select users.



File Shadowing

Automatically create mirror copies of the files transferred from a particular device. The copies are then safeguarded in a password protected share. In the event of an emergency, this precautionary measure helps identify the exact contents of transferred files and assists with the development of precise remediation strategies.

Highlights

- ◆ Auto-detection and management of more than 17 types of peripheral devices and continuous monitoring of network ports.
- ◆ Numerous granular settings for file protection policies.
- ◆ Meticulous tracing of file locations, users, and endpoints involved in data transfer operations.
- ◆ Temporary access provisions to encourage short-term collaboration with third-party users.
- ◆ Detailed reports and prompt alerts that enable enhanced visibility over devices and file actions.



File Transfer Control

Regulate the amount and type of data transferred through peripheral devices. By limiting the number of bytes, only information vital to the task at hand is transferred. By restricting the type of file extensions that are allowed to be copied, sensitive files, for example source code, or financial records that include .xml extensions and/or .xls extensions, can be blocked from unauthorized users.



Device Permissions

Enforce a zero-trust policy in your organization by having all devices blocked by default, with the exception of a few trusted devices that are routinely utilized by core personnel. For heightened security, the option to allow only BitLocker encrypted devices is also available. For each custom group or computer, policies solely for trusted devices can be created. This is advantageous as higher privileges can be assigned just for devices used only by key employees or for special tasks.



Temporary Access

On occasions where greylisted or blocked devices require access to computers for specific tasks, safely assign permissions so that the devices can obtain the necessary information without compromising cyber hygiene. As third-party users or lower-level employees are granted short-term access, ensure that sessions and file actions are closely monitored.

 Reports and Audits

Generate detailed reports, available at your fingertips, for all the device and file transfer operations. The audits can be closely analyzed to detect any unwanted intrusions or access policy discrepancies. The logs also offer insights into user and device patterns so that either existing policies can be modified or new policies can be created to further fortify the network.

Supported Devices


Biometric


Removable Storage Device


Imaging Devices
(Scanners, cameras)


Serial ports (COM)


Apple Devices


SmartCard Reader


Windows portable device


Printer


Modem


Mouse


Infrared


Floppy disks


Tape Drive


Wireless Network Adapters


Parallel Ports (LPT)


WCEUSBS


CDROM


Bluetooth

Hardware Requirements for Device Control Plus Servers

No of Computers		Processor Information	RAM Size	Hard Disk Space
1 to 250		Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache	2 GB	5 GB
251 to 500		Intel Core i3 (2 core/4 thread) 2.4 Ghz 3 MB cache	4 GB	10 GB
501 to 1000		Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MB cache	4 GB	20 GB
1001 to 3000		Intel Core i5 (4 core/4 thread) 2.3 GHz. 6 MB cache	8 GB	30 GB
3001 to 5000		Intel Core i7 (6 core/12 thread) 3.2 GHz. 12 MB cache	8 GB	40 GB
5001 to 10000		Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 20 MB cache	16 GB	60 GB
10001 to 20000		Intel Xeon E5 (8 core/16 thread) 2.6 GHz. 40 MB cache	32 GB	120 GB

Supported OS for Device Control Plus Servers

Windows 7	Windows 8	Windows 8.1	Windows 10
Windows 11	Windows Server 2003	Windows Server 2003 R2	Windows Server 2008*
Windows Server 2008 R2*	Windows Server 2012	Windows Server 2012 R2*	Windows Server 2016*
Windows Server 2019*	Windows Server 2022*		

* - recommended for managing 5000 or more endpoints.

Supported OS for Device Control Plus Agents

Windows OS		Windows Server OS	Supported macOS
Windows 11		Windows Server 2022	macOS 14 Sonoma
Windows 10		Windows Server 2019	macOS 13 Ventura
Windows 8.1		Windows server 2016	macOS 12 Monterey
Windows 8		Windows server 2012 R2	macOS 11 Big Sur
Windows 7		Windows server 2012	macOS 10.15 Catalina
		Windows server 2008 R2	macOS 10.14 Mojave
		Windows server 2003	macOS 10.13 High Sierra
			macOS 10.12 Sierra

Supported Browsers

You are required to install any of the following browsers on your computer to access the Device control Plus console:

- ◆ Microsoft Edge
- ◆ Microsoft Internet Explorer 11
- ◆ Mozilla Firefox 44 and later versions
- ◆ Google Chrome 47 and later versions

For more details:

- ◆ www.devicecontrolplus.com
- ◆ devicecontrolplus-support@manageengine.com
- ◆ Toll free: +1-888-720-9500

Pricing starts at:

- ◆ \$595/ year for 100 computers
- ◆ Device Control Plus Professional Edition