Ivanti Device Control

Your users need easy access to data, inside and outside the corporate network to make the everywhere workplace not only possible, but productive.

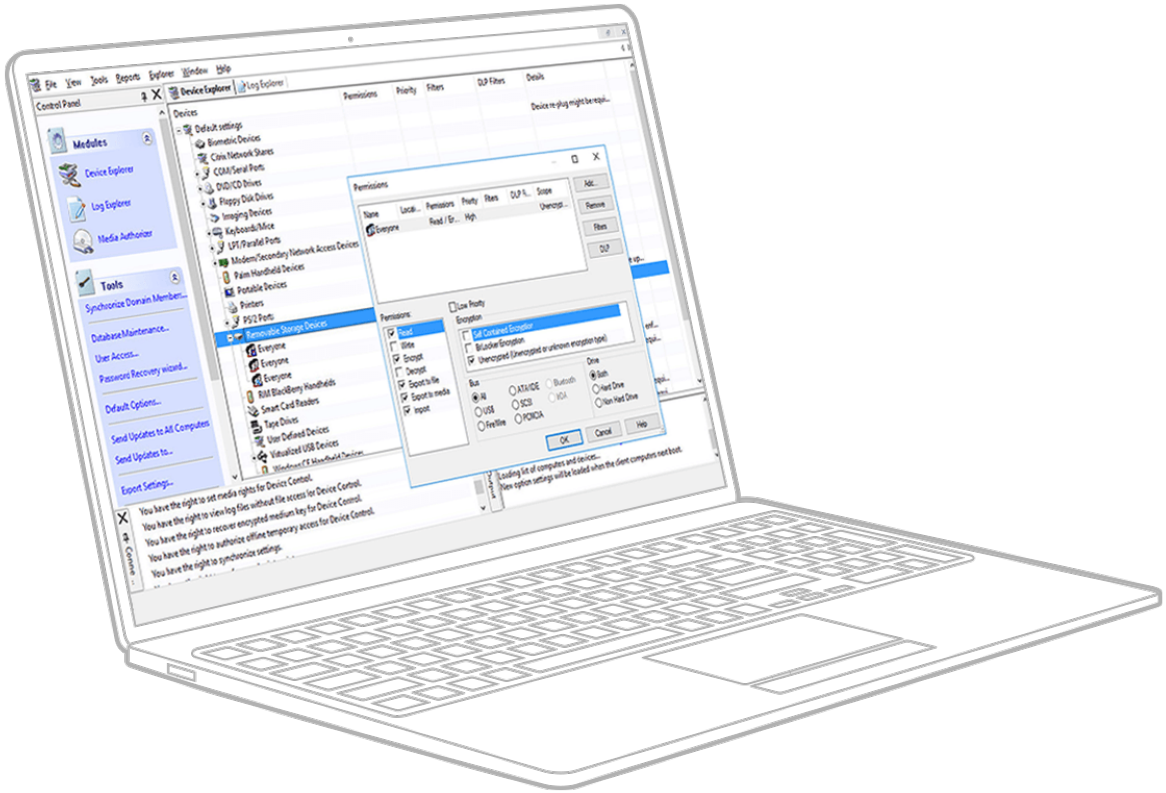
Enable them to use removable devices, cloud storage and media when needed, without leaving the door open to attack.

Protect Data from Loss or Theft While Keeping Employees Productive

With more employees working remotely, access is required from outside the network. But the potential impact of data loss, be it accidental or malicious, is a very real concern.

Today, removable media and devices are the most common routes for data leakage — no file-copy limits, no encryption, no audit trails, and no central management. Ivanti® Device Control enables the secure use of such productivity-enhancing tools while limiting the potential for data leakage and its impact.

Ivanti Device Control provides effective, scalable protection, ideal for (virtual) servers, fixed-function assets (e.g., POS, ATM and pay-at-the-pump systems), and thin clients or (virtual) endpoints. Reduce your attack surface by identifying and locking down endpoints to prevent unauthorized use of removable devices and cloud storage systems and prevent unknown apps from being installed or executed.



Key features on Ivanti Device Control include:

Centralized management

Centrally define and manage user, user group, workstation, and workstation group access to authorized devices, cloud storage systems as well as Microsoft Bitlocker System Drive encryption. Devices, media and users that are not explicitly authorized are denied access by default.

Centrally encrypt removable devices (such as USB flash drives) and media (such as DVDs and CDs) and enforce encryption policies when copying to devices or media.

Enterprise file-type filtering, file encryption and data restrictions

On a per-user basis, manage file types that are denied or allowed to be moved to and from removable devices and media and restrict the daily amount of data copied to removable devices and media. Add forced encryption and prohibit downloading of executables from removable devices for an added layer of malware protection.

Shadowing Capabilities

Enable file name shadowing or full file shadowing to capture and store all copied data in a centralized place to be able to monitor what has been copied as well as restore entire files in case of theft or hardware failure.

Role-based access control

Assign permissions to individual users or user groups based on their Windows Active Directory.

Context-based permissions

Assess and apply policies to all plug-and-play devices by class, group, model and specific ID.

Access and usage policies remain enforced regardless of connection status and can be tailored whether the endpoint is connected to the network or offline.

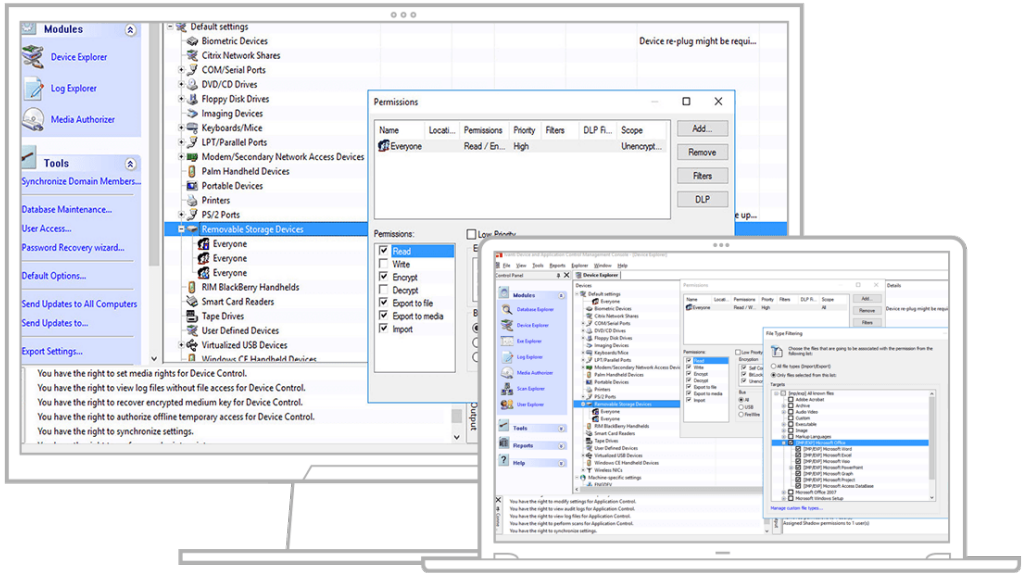
Grant users temporary or scheduled access to removable devices or media so they can access what they need, when they need it.

Secure, flexible and scalable architecture

Our solution grows with your business. Provide organization-wide control and enforcement using scalable client-server architecture with a central database, supporting Windows, macOS as well as Microsoft Surface devices (ARM64). Ivanti Device Control agents are protected against unauthorized removal — even by users with administrative permission.

Actionable insights

Unify your IT data without scripting. All network events related to your security policy are logged automatically. Provide visibility into policy compliance and violations via customizable reports and email.



ivanti

> “Device Control fully meets our expectations. We can control the most vulnerable parts of our infrastructure, proactively address any threats and adhere to our security standards.”

Grigory Kashin
Head of Software Sector, IT Department
NTEK

How Ivanti Device Control Works

1. Discover in audit / non-blocking mode to get a concise inventory of all devices connected to your endpoints and their usage.

2. Assess all “plug and play” devices by class, group, model and/or specific ID and define policy through a allow-list approach.

3. Implement file-copy limitations, file-type filtering and forced encryption policies for data moved onto removable devices.

4. Monitor all policy changes, administrator activities and file transfers to ensure continuous policy enforcement.

5. Report on device and data usage to document compliance with corporate and/or regulatory policies.

Benefits of Ivanti Device Control

- Protect data from loss and theft
- Safeguard endpoints from malware
- Enable secure use of productivity tools
- Enhance security policy enforcement
- Deliver precise control with access limits
- Document corporate or regulatory compliance

Monitor and control Cloud Drive usage

Become more proactive with data access and device control without putting user productivity on hold.

ivanti

ivanti.com/contact
1 800 982 2130
epg@ivanti.com