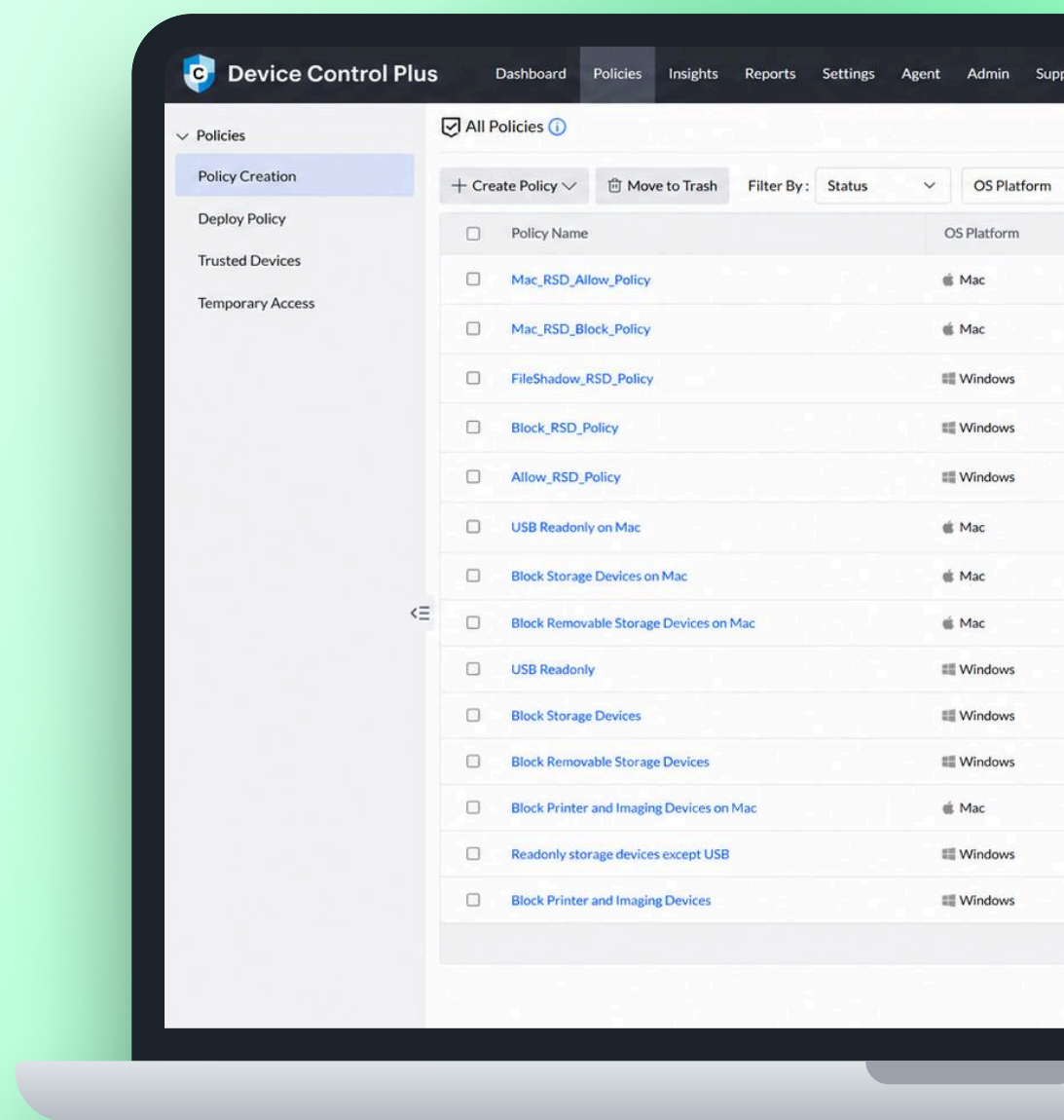




ManageEngine Device Control Plus

Control, block, and monitor unauthorized device access with Device Control Plus.

Device Control Plus is ManageEngine's USB & peripheral device control solution, built to manage, restrict, and audit every USB drive, bluetooth, and other peripheral devices connected to endpoints across your organization. By assigning the appropriate level of device permissions, all data transfers conducted via external devices can be meticulously tracked and regulated. With granular access policies, file tracing, and detailed audit reports, IT admins gain complete control over every peripheral device connected across the network.



The Device Control Plus lifecycle

Discover

Identify peripheral devices

- Automatically scan and detect all peripheral devices connected across managed endpoints
- Log device type, vendor ID, model, and serial number.

1



Authorize

Provide secure and exclusive access

- Create role-based policies per user, department, or job function.
- Assign read-only, read-write, or block access per device type.
- Allowlist trusted devices; block all others by default for strict governance.
- Grant temporary access to devices not on the trusted list, upon request

2



Monitor

Analyze device and user behaviour

- Track all device, user, and file activities from one console.
- Trace file names, locations, users, and timestamps.
- Shadow copy files transferred via removable media.
- Schedule reports and get instant alerts on policy violations.

4



Protect

Proactively prevent data loss

- Restrict file transfers to connected peripherals by size, type, and extension.
- Disable auto-run on all connected peripheral devices.
- Enforce BitLocker encryption for USB data transfers.
- Ensure policies are enforced automatically, even when endpoints are offline.

3

Manage 17+ peripheral device types from a single console.



USB storage



CD / DVD



Bluetooth



Printers



Scanners



Webcams



Smartphones



Wi-Fi adapters



Card readers

+8

more types



Device Control Plus

Core Capabilities

1. Device access control and management

- Manage 17+ peripheral device types from a single console.
- Block unauthorized devices or set read, write, or read-only access per policy.
- Disable auto-run when a removable storage device is connected.
- Policies apply inside and outside the network, even offline.

3. File access control

- Classify users by role, department, or job function.
- Grant read-only or read-write access based on the role.
- Apply policies to entire departments via custom computer groups.
- Restrict data access to only what is relevant to each role.

5. USB encryption

- Permit only BitLocker-encrypted USB devices to access the network.
- Set read-only permission for unencrypted devices or block them entirely.
- Prompt users to encrypt unencrypted devices when they attempt to transfer files.
- Secure data on USB drives with 128-bit or 256-bit AES encryption.

7. File shadowing and file tracing

- Auto-create mirror copies of all files transferred to USB.
- Store shadow copies securely in a designated network shared folder.
- Trace file names, locations, users, and timestamps per transfer.
- Track files skipped by shadowing based on size limits or file extension.

2. Trusted device lists

- Allowlist devices by device instance path or serial number.
- Use wildcard patterns to allowlist a group of company-owned devices at once
- Import trusted devices via CSV for large-scale deployments.
- Ensure no device connects unless explicitly authorized by the admin.

4. File transfer control

- Set maximum file size limits for transfers via removable devices.
- Restrict transfers by file type and extensions such as .xml, .exe, etc.
- Block copying of business-sensitive files to, and malicious files from, removable devices.
- Notify users instantly when a transfer is denied.

6. Temporary access

- Grant time-bound access to third-party, vendor, or employee devices not on the trusted list, upon request.
- Enforce explicit admin approval for every device access request.
- Generate offline access codes for out-of-network users.
- Set exact start and end time windows per access request.

8. Reports and audits

- View intuitive dashboards on device, user, and file actions. Export audit reports in PDF, XLSX, or CSV with option to hide personal information.
- Schedule reports daily, weekly, or monthly via email to admin and stakeholder inboxes.
- Retain and archive audit logs for an admin-specified retention period for compliance requirements.

Key Benefits

- **Zero data loss** from USB
- **Zero Trust** device security model
- **Always on**, even offline
- **Template policies**, faster deployment
- **Audit-ready compliance**, always.
- **Full device accountability**

- **5M+**
Endpoints secured
- **5+ Years**
in the industry
- **100+**
countries served
- **5000+**
organizations worldwide

Trusted by

- SanDisk
- KM
- unisys
- Panasonic

More Resources

-  User guide
-  System requirements
-  Support Email:
devicecontrolplus-support@manageengine.com

Free up to 25 machines

Professional Edition
\$5.95 per endpoint/year.

- 30-DAY FREE TRIAL
- REQUEST A PRICE QUOTE