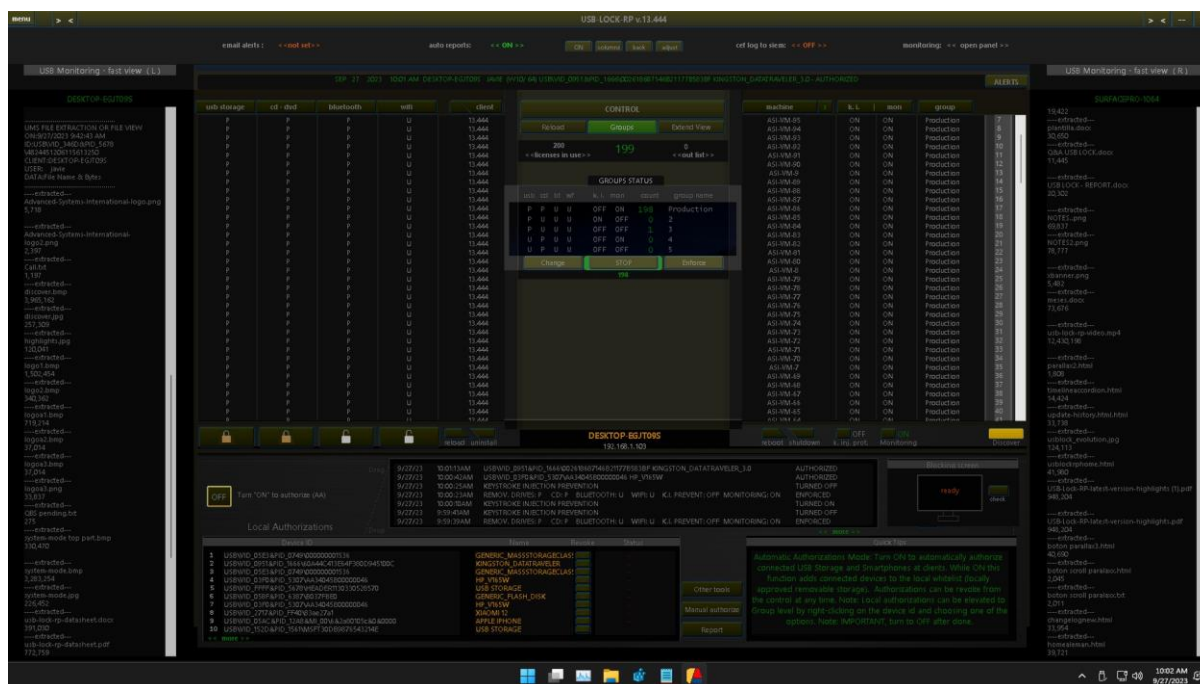




USB-LOCK-RP

Centralized USB Management & Lockdown Software for Enterprise.



USB-Lock-RP Control

Straightforward solution to centrally manage access of removable storage, mobile devices and wireless adapters to servers, workstations and laptops in a network.

Smart USB lockdown for enterprise designed to protect computers in Industrial processes as well as corporate offices. Includes functionality required and suggested by real world IT Infrastructure Architects, IT Managers and Network Systems Security Analysts of top-notch organizations.

Classified as USB Port Control for Enterprise, USB Lock RP Device Control Software is an administrative and enforcement tool specifically designed to control usb devices to protect windows operating systems, without concern to dependencies, at a very small memory/storage footprint. You will find serious capacity to allow securing your network without affecting its productivity, and no useless functionality wasting your systems resources.

Maximun Proven capacity: One USB Lock RP Control can centrally manage portable devices access up in up to 9000 computers.

In active development since 2004.

Latest version is 13.844 released on October 2nd, 2024.



CAPABILITIES:

- Secure Groups of Computers or Specific Computers from USB threat in real-time. Whitelists USB Devices by Hardware ID and Block others.
- Automatically apply default protection settings to unassigned clients.
- Automatic Authorizations Mode, Whitelist USB devices across the network automatically. Receives alerts & logs USB device connections in the network.
- Export Status and Alerts Reports to csv format (Comma-separated value)
- Presents Full Screen Locking upon Blocking Devices (includes your company logo).
- Easy Client Deployment through Group Policy (Windows Installer MSI).
- Event logs in CEF (Common events format) for integration with SIEM.
- Automatically receive and log the insertion of allowed or blocked devices at any clients in real-time.
- Generate per client detailed historic reports and global security status, and global alerts reports.
- Audit from any client at anytime: system information, installed software, windows updates- security patches, running processes on any client in real-time.
- Monitors File Transfers from Endpoints to Authorized USB drives (ON/OFF).
Automatically monitors and registers:
 - The name and exact size of files transferred.
 - Device insertion date / time and the specific device hardware identifier (ID).
 - The name of the PC machine and user/users logged at insertion time.
- Auto email alerts & authorized usb file extractions fully compatible with exchange mail servers and allows authentication.
- Get all insertion incoming alerts also sent to an email address at your organizations domain.
- Get all details on files extracted on authorized devices also sent to an email address at your organizations domain
- Keep data transferred to Thumb drives protected: Encrypts File Transfers from Endpoints to Authorized USB drives (ON/OFF).
- When encryption is set to ON, files transferred to Thumb drives are automatically Encrypted.
Note: Encrypted Data is accessible only within clients that have encryption capability set to ON.
- Central Logging: Schedules the automatic output of status & alerts report at a fixed hour, daily or weekly. To a set share path.
- New "system-mode" 24/7 real-time management and enforcement capability. Function: To auto-start the control in system-mode while an admin-mode control is not running.
- Groups Auto-Enforce Settings: (Continuous watch over Group Settings) (Main Interface)
 - Auto-enforce is the New Recommended Operation Mode.
 - Enforces setting to not-logged machines automatically upon logging back.



SUPPORTED OPERATING SYSTEMS:

Windows-Server 2022 - Windows 11 - Windows-Server 2019 - Windows 10 - Windows-Server 2016 - Windows 8.1 - Windows-Server 2012 R2 - Windows 8 - Windows-Server 2012 - Windows 7 - Windows Server 2008 R2 - Windows-Server 2008 - Windows Vista - Windows-Server 2003 R2 - Windows-Server 2003 - Windows XP - Windows Embedded OS with Minimal Components - Virtual Machines and Thin Clients.(32/64 bits).

PROTECTION SCOPE:

- USB mass storage devices
- USB MTP protocol (extensively used in Smartphone's and new generation devices)
- BadUSB HID impostor devices, (Such as USB Rubber Ducky) Remote USB devices.
- Portable flash memory devices external sata, Firewire drives.
- Digital audio players including MP3 players and iPod External magnetic hard drives
- External optical drives, including CD and DVD reader and writer drives, Blue ray adapters bridging between standard flash memory cards and a USB connection Digital cameras (Storage, mtp, Twain).
- Card readers including CF, SD, SDMicro, MMC, XD.
- PDA, and handheld computers, mobile phones, smartphone, tablets.
- Internal optical drives, including CD, DVD, Burners, Combos, Floppy drives
- Wireless Transceivers.
- IrDA, USB Bluetooth, file transfer capability.

ADVANTAGES:

- Protects even if clients are disconnected from the network.
- Doesn't restrict the normal use of non-storage capable peripherals, (printers, mouse, Webcams).
Note: Keyboard changes are automatically analyzed to prevent keystroke injection attacks. (Once keyboards are analyzed there are automatically excluded from analysis).
- Easy authorize specific devices or by brand and model on specific machines or groups.
- Light on system resources.
- Personalized Alert screens presented at clients include licensed organization logo, automatically at no extra charge.
- Recent Alerts: Eight most recent alerts per client visible at a glance.
- Network-wide PID match authorization excellent to authorize large number of organization provided custom devices.
- Protects logs storage AES256 CBC MODE variable key, variable initiation vector.
- Local-client and/or network-wide specific device authorizations. (Granular protection).
- Client silent initial deployment easy with MSI Windows Installer (included for all size orders) Scalable, Windows multiplatform.
- Allows for sub network management, also Ideal for controlling port security on startups, or field operation, remote locations.
- Automatically receive and record devices insertion alerts in real-time.
- Capable of automatically email you all insertion alerts blocked and extraction records as they happen.
- Allows its implementation without disrupting operations.
- Elevate to network authorizations MTP and USB (drag & drop).
- Real time show not logged Pcs.



- Bulk license recovery function: Allows to recover unused licenses to be installed on new systems.
- Bulk client update: Allows to update clients from the Admin Control.

SOFTWARE TYPE:

Windows multiplatform two components server/client type application.

HARDWARE REQUIREMENTS:

Network (Fixed or dynamic IP configuration) (LAN, Workgroup, WAN) (Wired or wireless).

RESOURCES REQUIREMENTS:

Minimum: Low demand: Not significantly higher than the originally recommended to run the installed Operating System.

LICENSING:

Licenses are End-user Organization Perpetual use Licenses and include 2 years updates, after 2 years updates are optional at 20% of licensing cost.

MORE INFORMATION:

Main product page:

<https://www.usb-lock-rp.com/>

Installation instructions:

<https://www.usb-lock-rp.com/usb-lock-rp-installation-en.pdf>

Client MSI deployment:

https://www.usb-lock-rp.com/usb-lock-rp_client-msi_deployment.pdf

Operating Manual:

<https://www.usb-lock-rp.com/usb-lock-rp-operation.pdf>