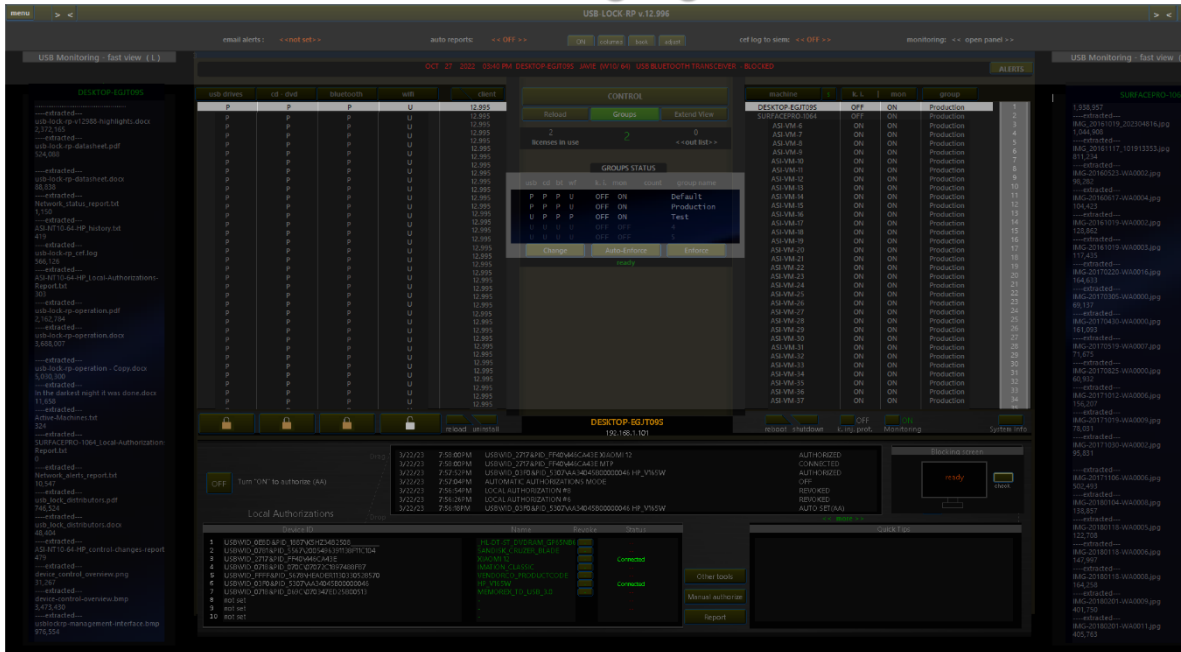


USB-Lock-RP Latest Version Highlights



V.13.838 – July 8th, 2024

New Features:

1. Disconnected Machines Enhanced Visibility:

- All settings, most recent alerts, and authorized devices for machines not logged into the system.
- This highly requested feature now provides administrators with the ability to monitor and manage disconnected machines efficiently.

2. Global Authorizations Panel and Reporting:

○ Enhanced Approved Devices Visibility:

- Displays and reports (CSV) all authorized devices divided by Groups, Per Machine, and Group-wide authorizations from one place.
- Centralized view simplifies the management of device authorizations across the network.



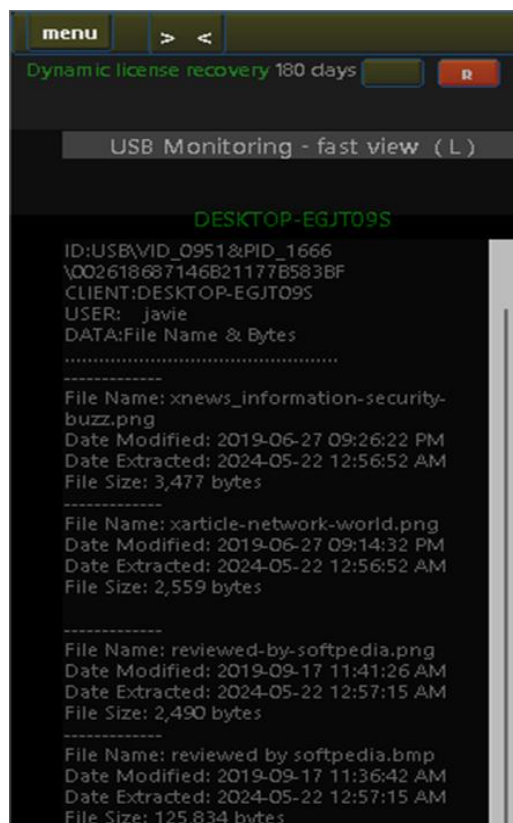
V.13.829 – May 22nd, 2024.

New Monitoring & Email Alerts.

- Reports to Control upon transfer of files to authorized devices:
Machine name – User - Device ID and File Name -Date Modified - Date Extracted – File Size information per file.
- Email Alerts: Updated SMTP component capability automatic TLS/SSL Port 587 // TLS/SSL Port Based 465/578) (Supports TLS 1.2)
- Email USB Monitoring alerts can now be set to include approved USB thumb drives transfer data: Machine name – User - Device ID and File Name -Date Modified - Date Extracted – and File Size.

Upcoming News! Soon to be released: USB Alerts Action Center; (Add-on application)

Remotely receive alerts and take action to common tasks such as Authorizing devices.





USB-LOCK-RP v.13.824

Dynamic license recovery: OFF

email alerts: << not set >>

auto reports: << OFF >>

cef log to siem: << OFF >>

monitoring: << open panel >>

real-time updates to shows 200 most recent alerts

SURFACEPRO-1064 - LOCAL AUTHORIZATIONS PANEL

Time	Message	Action	Status
2024-04-16 02:55:58 AM	AUTOMATIC AUTHORIZATIONS MODE	OFF	CONTROL*
2024-04-16 02:55:42 AM	USB\VID_03F0&PID_5307\AA34045B00000046 HP_V165W	AUTHORIZED	CLIENT*
2024-04-16 02:55:38 AM	USB\VID_03F0&PID_5307\AA34045B00000046 HP_V165W	AUTO SET(AA)	CLIENT*
2024-04-16 02:55:23 AM	USB\VID_0951&PID_1666\00261868714682117785838F KINGSTON_DATATRAVELER_3.0	AUTHORIZED	CLIENT*
2024-04-16 02:55:12 AM	USB\VID_0951&PID_1666\00261868714682117785838F KINGSTON_DATATRAVELER_3.0	AUTO SET(AA)	CLIENT*
2024-04-16 02:54:59 AM	USB\VID_0718&PID_069C\070347ED25B00513 MEMOREX_TD_USB_3.0	AUTHORIZED	CLIENT*
2024-04-16 02:54:55 AM	USB\VID_0718&PID_069C\070347ED25B00513 MEMOREX_TD_USB_3.0	AUTO SET(AA)	CLIENT*
2024-04-16 02:54:45 AM	USB\VID_0951&PID_1666\60444C413E64F380D945100C KINGSTON_DATATRAVELER	AUTHORIZED	CLIENT*
2024-04-16 02:54:38 AM	USB\VID_0951&PID_1666\60444C413E64F380D945100C KINGSTON_DATATRAVELER	AUTO SET(AA)	CLIENT*
2024-04-16 02:54:24 AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB	AUTHORIZED	CLIENT*
2024-04-16 02:54:19 AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB	AUTO SET(AA)	CLIENT*
2024-04-16 02:53:56 AM	AUTOMATIC AUTHORIZATIONS MODE	ON	CONTROL*
2024-04-16 02:53:38 AM	LOCAL AUTHORIZATION #2->USB\VID_05E3&PID_0749\000000001536	SET	CONTROL*
2024-04-16 02:53:02 AM	LOCAL AUTHORIZATION #2	REVOKED	CONTROL*
2024-04-16 02:53:00 AM	LOCAL AUTHORIZATION #11->USB\VID_152D&PID_1561\MSFT30DB9876543214E	SET	CONTROL*
2024-04-16 02:52:39 AM	LOCAL AUTHORIZATION #2->USB\VID_152D&PID_1561\MSFT30DB9876543214E	SET	CONTROL*
2024-04-16 02:51:45 AM	LOCAL AUTHORIZATION #1->USB\VID_058F&PID_6387\B037FBE0	SET	CONTROL*
2024-04-16 02:50:25 AM	USB\VID_152D&PID_1561\MSFT30DB9876543214E UAS	BLOCKED	CLIENT*
2024-04-16 02:50:02 AM	USBSTOR\DISK\VEN_GENERIC&PROD_MASSSTORAGECLASS&REV_1536\000000001536 (EJECTED)	BLOCKED	CLIENT*
2024-04-16 02:49:58 AM	USB\VID_05E3&PID_0749\000000001536 USB	BLOCKED	CLIENT*
2024-04-16 02:49:13 AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB	BLOCKED	CLIENT*
2024-04-16 02:48:59 AM	USB\VID_0718&PID_069C\070347ED25B00513 USB	BLOCKED	CLIENT*
2024-04-16 02:48:49 AM	USBSTOR\DISK\VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\B037FBE0 (EJECTED)	BLOCKED	CLIENT*
2024-04-16 02:48:48 AM	USB\VID_058F&PID_6387\B037FBE0 GENERIC_FLASH_DISK	BLOCKED	CLIENT*
2024-04-16 02:44:08 AM	LOCAL AUTHORIZATION #11	REVOKED	CONTROL*
2024-04-16 02:44:03 AM	LOCAL AUTHORIZATION #1	REVOKED	CONTROL*
2024-04-16 02:43:58 AM	LOCAL AUTHORIZATION #11->USBSTOR\DISK\VEN_HP&PROD_V165W&REV_8192\AA34045B00000046	SET	CONTROL*
2024-04-16 02:43:50 AM	LOCAL AUTHORIZATION #1->USB\VID_03F0&PID_5307\AA34045B00000046	SET	CONTROL*
2024-04-15 05:00:51 PM	REMOVABLE STORAGE	REVOKED	CONTROL*
2024-04-15 04:52:12 PM	LOCAL AUTHORIZATION #1->USB\VID_346D&PID_5678\4824451206115613250	PROTECTED	CONTROL*
2024-04-15 04:43:15 PM	REMOVABLE STORAGE	SET	CONTROL*
2024-04-15 04:40:35 PM	LOCAL AUTHORIZATION #1	UNPROTECTED	CONTROL*
2024-04-15 04:40:29 PM	LOCAL AUTHORIZATION #1->USB\VID_03F0&PID_5307\AA34045B00000046	REVOKED	CONTROL*

Showing Drag-Drop authorization mode
show more ways to authorize

Elevate devices to Group Level
Select and right click to elevate
Organize to right or left side
Move authorizations by Drag and Drop

Device ID	Name	USB SECTOR	Name	Device ID
01 USB\VID_058F&PID_6387\B037FBE0	FLASH_DISK_A51	USB SECTOR	UAS DRIVE A51	11
02 USB\VID_05E3&PID_0749\000000001536	USB-CUSTOM			12
03 USB\VID_FFFF&PID_5678\HEADER1130330528570	USB			13
04 USB\VID_0951&PID_1666\60444C413E64F380D945100C	KINGSTON_DATATRAVELER			14
05 USB\VID_0718&PID_069C\070347ED25B00513	MEMOREX_TD_USB_3.0			15
06 USB\VID_0951&PID_1666\00261868714682117785838F	KINGSTON_DATATRAVELER_3.0			16
07 USB\VID_03F0&PID_5307\AA34045B00000046	HP_V165W			17
08 not set				18
09 not set				19
10 not set				20

New Local Authorization Panel: Offers 4 easy ways to authorize devices.

Drag-Drop authorization
Drag: ALLOWED or BLOCKED alert messages
Drop: Inside Device ID boxes

Manually enter ID to authorize.
Manually enter the device ID to be authorized

Authorize a device already connected at client
Connected usb drives or mtp will be authorized

Automatically authorize devices (AA)
Devices are authorized as they are connected.
Turn "ON" to authorize (AA)

Elevate devices to Group Level
Select and right click to elevate
Organize to right or left side
Move authorizations by Drag and Drop

Device ID	Name	USB SECTOR	Name	Device ID
01 USB\VID_058F&PID_6387\B037FBE0	FLASH_DISK_A51	USB SECTOR	UAS DRIVE A51	11
02 USB\VID_05E3&PID_0749\000000001536	USB-CUSTOM			12
03 USB\VID_FFFF&PID_5678\HEADER1130330528570	USB			13
04 USB\VID_0951&PID_1666\60444C413E64F380D945100C	KINGSTON_DATATRAVELER			14
05 USB\VID_0718&PID_069C\070347ED25B00513	MEMOREX_TD_USB_3.0			15
06 USB\VID_0951&PID_1666\00261868714682117785838F	KINGSTON_DATATRAVELER_3.0			16
07 USB\VID_03F0&PID_5307\AA34045B00000046	HP_V165W			17
08 not set				18
09 not set				19
10 not set				20

- Drag and Drop Blocked or Allowed alerts to authorize.
- Manually enter the device ID to be authorized.
- Authorize a device already connected at client.
- Authorize devices automatically as they connect.



Other Characteristics:

- New Panel Loads 200 most recent alert for any machine in real-time.
- Right-click locally authorized devices to elevate to groups.
- Organize authorizations by moving devices to right to left or left to right.
- Allows entering a custom device name.

V.13.531 – April 3rd, 2024.

- Color coded Network alerts view to ease alerts identification at a glance.

showing: 1539 records

Network Alerts Log:						
date	time	machine	user	os bit	message	action
2024-04-03	10:26:39 AM	DESKTOP-EGJTO9S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MID_006&2A80105C&0&0000 APPLE IPHONE	AUTHORIZED
2024-04-03	10:26:21 AM	DESKTOP-EGJTO9S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MID_006&2A80105C&0&0000 APPLE IPHONE	AUTO SET(AA)
2024-04-03	10:22:35 AM	DESKTOP-EGJTO9S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MID_006&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:22:08 AM	DESKTOP-EGJTO9S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MID_006&2A80105C&0&0000 APPLE IPHONE	BLOCKED
2024-04-03	10:21:47 AM	DESKTOP-EGJTO9S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MID_006&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:19:58 AM	DESKTOP-EGJTO9S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MID_006&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:13:37 AM	DESKTOP-EGJTO9S	JAVIE	W10/ 64	USB\VID_152D&PID_1561\MSFT30D89876543214E UASP	AUTHORIZED
2024-04-03	10:12:12 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB BLUETOOTH TRANSCEIVER	BLOCKED
2024-04-03	10:11:36 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_03F0&PID_5307\AA34045B000000046 HP_V165W	AUTHORIZED
2024-04-03	10:11:18 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_03F0&PID_5307\AA34045B000000046 HP_V165W	AUTO SET(AA)
2024-04-03	10:11:07 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USBSTOR\DISK&VEN_HP&PROD_V165W&REV_8192\AA34045B000000046	EJECTED
2024-04-03	10:11:06 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_03F0&PID_5307\AA34045B000000046 HP_V165W	BLOCKED
2024-04-03	10:10:55 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_346D&PID_5678\4824451206115613250 VENDORCO_PRODUCTCODE	AUTHORIZED
2024-04-03	10:10:26 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_346D&PID_5678\4824451206115613250 VENDORCO_PRODUCTCODE	AUTO SET(AA)
2024-04-03	10:09:59 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_346D&PID_5678\4824451206115613250 VENDORCO_PRODUCTCODE	BLOCKED
2024-04-03	09:38:43 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USBSTOR\DISK&VEN_HP&PROD_V165W&REV_8192\AA34045B000000046	EJECTED

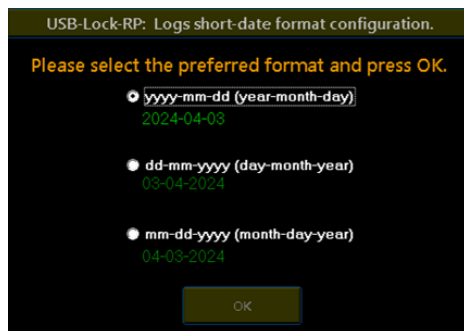
- Column headers in Alerts logs view and Per Machine logs.

yyyy-mm-dd SURFACEPRO-1064 machine history log → showing: 100 records out of 100

date	time	message	action	source
2024-04-01	10:58:52AM	AUTOMATIC AUTHORIZATIONS MODE	Off	CONTROL*
2024-04-01	10:58:48AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB	AUTO SET(AA)	CLIENT*
2024-04-01	10:58:45AM	AUTOMATIC AUTHORIZATIONS MODE	ON	CONTROL*
2024-04-01	10:58:31AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB	BLOCKED	CLIENT*
2024-04-01	03:45:00AM	REMOV. DRIVES: P CD: P BLUETOOTH: U WIFI: U K.I. PREVENT: ON MONITORING: OFF	ENFORCED	CONTROL*
2024-04-01	03:44:50AM	REMOVABLE STORAGE	UNPROTECTED	CONTROL*
2024-04-01	03:44:49AM	CD DVD	UNPROTECTED	CONTROL*
2024-03-31	07:38:26PM	USBSTOR\DISK&VEN_HP&PROD_V165W&REV_8192\AA34045B000000046 (EJECTED)	BLOCKED	CLIENT*
2024-03-31	07:38:25PM	USB\VID_03F0&PID_5307\AA34045B000000046 HP_V165W	BLOCKED	CLIENT*
2024-03-31	04:34:40PM	REMOV. DRIVES: P CD: P BLUETOOTH: U WIFI: U K.I. PREVENT: ON MONITORING: OFF	ENFORCED	CONTROL*
2024-03-31	04:34:39PM	REMOVABLE STORAGE	UNPROTECTED	CONTROL*



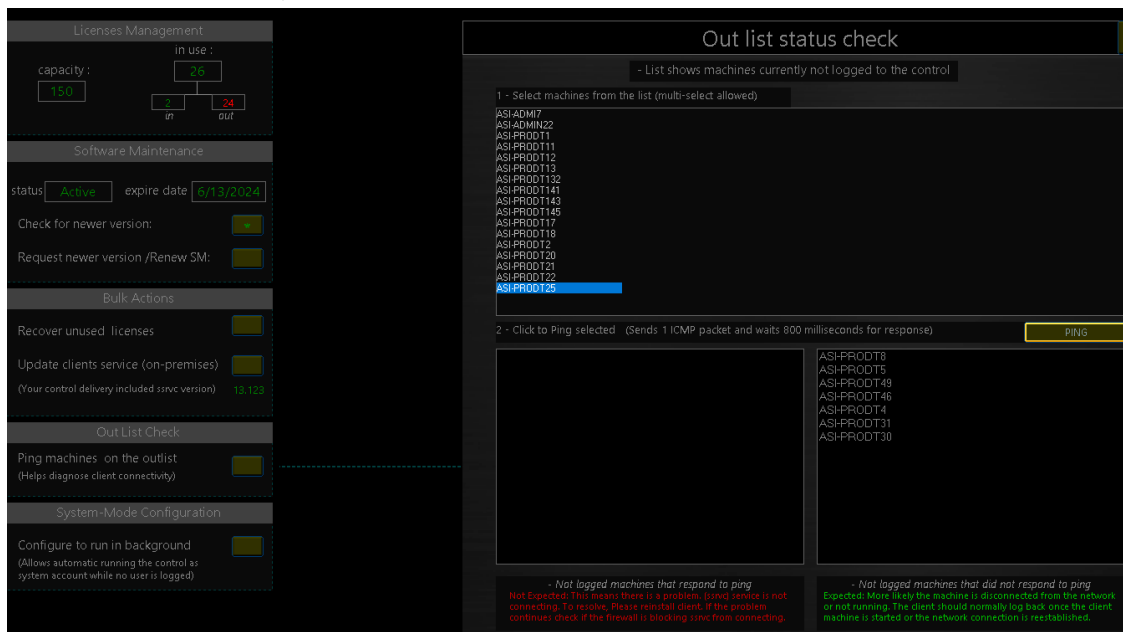
- Logs Short-date configuration function:



V.13.522 - December 21st, 2023

- New management functions panel: Large network ready!
- Improved Control load time: Tested on 7000 machines load.
- Improved performance on all functions involving not-logged Machines.
- New bulk recover licenses: Shows last seen by control date column.
- New Dynamic licenses recovery: Recover licenses by last seen by the control date.
(Auto recover by Last seen older than: 60 days, 90 days, 180 days, 1 year)
- New IN and OUT Machines list (csv) report.

V. 13.449 – October 19th, 2023





- Out list Diagnostic function: Allows to send an ICMP packet (ping) to not logged machines to diagnose client/machine availability to help identify client connectivity issues.

V. 13.444 – September 26th, 2023

Device ID	Name	Revoke
11 USB\VID_05E3&PID_0749\000000001536	GENERIC_MASSSTORAGECLAS	<input type="button" value="X"/>
12 USB\VID_0951&PID_1666\60A44C413E64F380D945100C	KINGSTON_DATATRAVELER	<input type="button" value="X"/>
13 USB\VID_0781&PID_557D\AC530000130605112493	SANDISK_CRUZER_FORCE	<input type="button" value="X"/>
14 USB\VID_346D&PID_5678\4824451206115613250	VENDORCO_PRODUCTCODE	<input type="button" value="X"/>
15 USB\VID_FFFF&PID_5678\HEADER1130330528570	USB STORAGE	<input type="button" value="X"/>
16 USB\VID_058F&PID_6387\B037FBE0	GENERIC_FLASH_DISK	<input type="button" value="X"/>
17 USB\VID_03F0&PID_5307\AA34045B00000046	HP_V165W	<input type="button" value="X"/>
18 USB\VID_2717&PID_FF40\83ae27a1	XIAOMI 12	<input type="button" value="X"/>
19 USB\VID_05AC&PID_12A8\MI_00\6&2a80105c&0&0000	APPLE IPHONE	<input type="button" value="X"/>
20 not set	-	<input type="button" value="X"/>

Select and right-click to elevate the authorized device to a group.

New Total 20 per machine local authorization. (10 additional per machine)

V. 13.246 – June 5th, 2023

SURFACEPRO-1064

System Information	Removable Storage / Mobile phones	Printers / Printer queue	HID (Human interface device)
<p>None/6/5/2023 10:16:34 AM</p> <p>Machine name: SURFACEPRO-1064</p> <p>IP address: 192.168.1.103</p> <p>Logged user: ANDREA</p> <p>Manufacturer: Microsoft Corporation</p> <p>Model: Surface Pro 4</p> <p>Processor</p> <p>Processors Type: GenuineIntel</p> <p>Number of Processors: 4</p> <p>Processors Name: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz</p> <p>Processors ID: Intel64 Family 6 Model 78 Stepping 3</p> <p>Processors Speed: 2496MHz</p> <p>Memory RAM: 4017 Mb</p>	<p>None</p> <p>Device Name: HP V165W (G)</p> <p>Device Type: USB Drive</p> <p>Device Path G:</p> <p>ID: VAA34045B00000046</p> <p>Size: 7.60 GB</p> <p>Free: 7.21 GB</p> <p>File System: NTFS</p>	<p>None</p> <p>Device Name: Canon E400 series Printer</p> <p>Status: Online</p> <p>Device Name: Fax</p> <p>Status: Ready</p> <p>Device Name: Microsoft Print to PDF</p> <p>Status: Ready</p> <p>Device Name: Microsoft XPS Document Writer</p> <p>Status: Ready</p> <p>Device Name: Send To OneNote 2013</p> <p>Status: Ready</p>	<p>None</p> <p>Surface Dock Extender</p> <p>Microsoft</p> <p>VID: 0x045E, PID: 0x0904</p> <p>SerialNumber: None</p> <p>bNumConfigurations: 0x01</p> <p>Device Bus Speed: Full</p> <p>Device Address: 0x15</p> <p>MaxPower: 0x02 (100 mA)</p> <p>Total Open Pipes: 2</p> <p>Pipe 1: Interface:</p> <p>Interface number: 0</p> <p>InterfaceClass: 0x03 (HID)</p> <p>InterfaceProtocol: 0x00 (Unknown)</p> <p>Pipe 1: Endpoint:</p> <p>bEndpointAddress: 0x81 IN</p> <p>Transfer Type: 3 (Interrupt)</p> <p>wMaxPacketSize: 0x0040 (64)</p> <p>bInterval: 0x01</p> <p>Pipe 2: Endpoint:</p> <p>bEndpointAddress: 0x02 OUT</p> <p>Transfer Type: 3 (Interrupt)</p> <p>wMaxPacketSize: 0x0040 (64)</p> <p>bInterval: 0x01</p>
<p>Installed Software</p> <p>NoneGoogle Chrome</p> <p>Microsoft Edge</p> <p>Microsoft Edge Update</p> <p>Microsoft Edge WebView2 Runtime</p> <p>MS Studio</p> <p>Slype version 8.67</p> <p>USB-Lock-RP Control 12.9.9.6</p> <p>Windows 11 Installation Assistant</p> <p>Wondershare Helper Compact 2.6.0</p> <p>PowerREC V15.0.19</p> <p>Office 15 Click-to-Run Extensibility Component</p> <p>Office 15 Click-to-Run Localization Component</p> <p>USB-Lock-RP demo client.msi</p> <p>Windows 10 Update Assistant</p>	<p>Running Processes</p> <p>(system process)</p> <p>system</p> <p>registry</p> <p>smss.exe</p> <p>csrss.exe</p> <p>wininit.exe</p> <p>services.exe</p> <p>lsass.exe</p> <p>fontdrvhost.exe</p> <p>wudhost.exe</p> <p>wudhost.exe</p> <p>memory compression</p> <p>spoolsv.exe</p> <p>dashost.exe</p> <p>officeclktorun.exe</p> <p>intelchdpsvc.exe</p> <p>intelphcsvc.exe</p> <p>surfacebroker.exe</p> <p>googlecrashhandler.exe</p> <p>googlecrashhandler4.exe</p>	<p>Network Adapters</p> <p>None</p> <p>Wi-Fi</p> <p>Status: Disconnected</p> <p>Marvell Avastar Wireless-AC Network Controller</p> <p>Not connected</p> <p>MAC Address: 88-31-85-32-D6-92</p> <p>Ethernet</p> <p>Status: Connected</p> <p>Surface Ethernet Adapter</p> <p>IP Address: 192.168.1.103</p> <p>Subnet Mask: 255.255.255.0</p> <p>Assigned by DHCP</p> <p>IPv6 Enabled</p> <p>TP-LINK_TL-WA824C</p> <p>MAC Address: BC-63-65-08-60-C8</p>	<p>Surface Type Cover</p> <p>Microsoft</p> <p>VID: 0x045E, PID: 0x07E8</p> <p>SerialNumber: None</p> <p>bNumConfigurations: 0x01</p> <p>Device Bus Speed: Full</p> <p>Device Address: 0x04</p> <p>MaxPower: 0x02 (100 mA)</p> <p>Total Open Pipes: 2</p> <p>Pipe 1: Interface:</p> <p>Interface number: 0</p> <p>InterfaceClass: 0x03 (HID)</p> <p>InterfaceProtocol: 0x00 (Unknown)</p> <p>Pipe 1: Endpoint:</p>

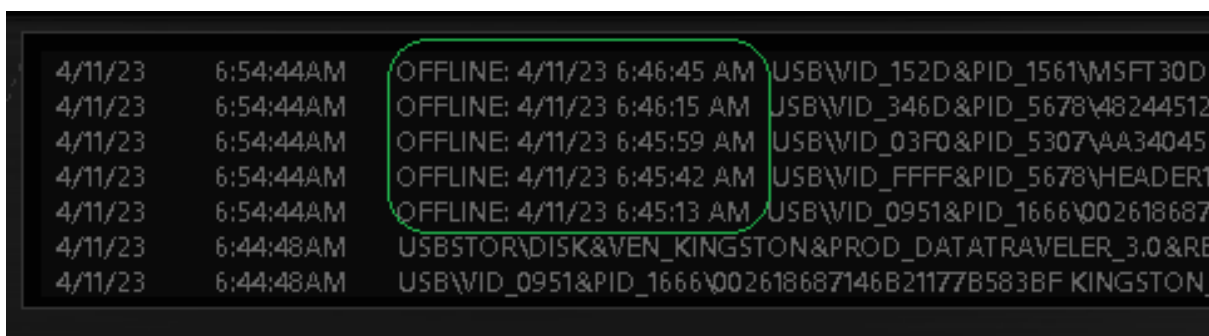
Refresh Export



- New Discovery function: Reports real-time client-side information on: -Connected removable storage (including smartphones), -Network adapters (Including MAC Address), -Printers (Includes printer queues), -HID devices (Low Level descriptors), - Machine data, - Logged user, -Installed software, -Running processes.

V. 13.126 – April 11th, 2023

- Offline alert logs: Blocked and authorized alert events happening while a client is disconnected from the control for any reason are automatically retrieved when the client reconnects to the control.



Note: OFFLINE alerts can be found normally on the machine alerts log and the most recent alerts. (Same as other per machine alert logs). Offline alerts are marked as OFFLINE.

V. 13.121 – March 23rd, 2023



- Show in real-time when any locally authorized removable storage device is in use (connected/disconnected)
- Function to query if a client is blocked at any time.



- New interface layout includes Quick tips visor that informs about the functionality of all elements on mouse over.

V. 12.998 – December 1st, 2022

- Per machine right-click on main network list to move machines and apply:
- Group Settings, Group authorized devices and Group master password. (In one action)

Add to Group: Default: Apply Group (settings, authorized devices and master password)

Add to Group: Production: Apply Group (settings, authorized devices and master password)

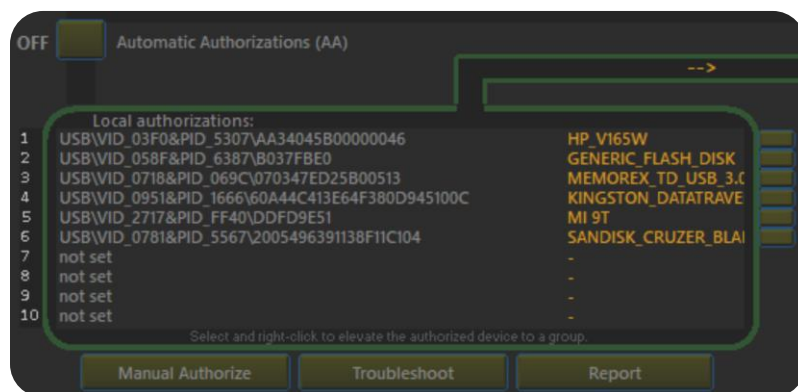
Add to Group: 3: Apply Group (settings, authorized devices and master password)

Add to Group: 4: Apply Group (settings, authorized devices and master password)

Add to Group: 5: Apply Group (settings, authorized devices and master password)

V. 12.996 - October 27th, 2022

- Removable storage and smartphones friendly name column. (Local authorizations)





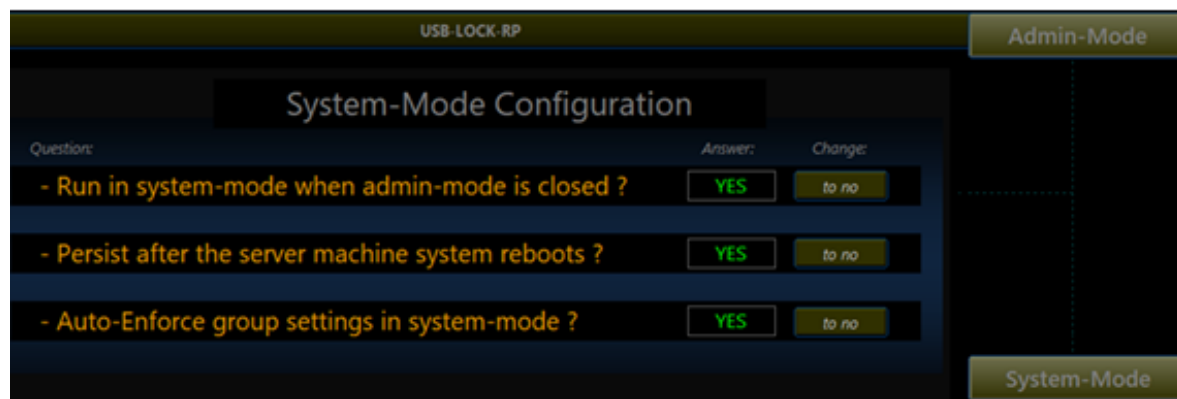
- Devices friendly name also included on alert logs and reports.
- Color coded alerts arrival: Allows to easily call the attention on events at a glance.

V. 12.995 - October 7th, 2022

- New Bulk license recovery function panel:
Allows to massively recover licenses from unused machines.
- New Clients Update function panel:
Allows to massively update client's version from control-side.
- New MTP blocking behavior:
Allows unauthorized Smartphones to be connected for-charging-only without blocking.

V. 12.994 - September 7th, 2022

- 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.



- Includes system-mode and admin-mode start stop log.
- Includes capacity to configure the service from admin-mode.
- Includes capability to set auto-enforce group setting while on system-mode.



V. 12.992 - July 5th, 2022

USB Device tracking alert function alerts the Control administrator in real-time upon the connection of any specific USB ID to any client in the networks. This function can be used for intrusion detection or to test behavior of employees regarding policy in reference the connection of unknown devices to company computer peripheral ports. *(Control-side update available)*

V. 12.990 - January 25th, 2022

Specific Read-Only Function: Write-Protects Specific USB Drives while other authorized USB drives can be full access on the same machine. (While unauthorized drives continue to be blocked)



Characteristics:

- Files transfer to write-protected USB drives are interrupted at Operating System level.
- Other USB drives authorized as full access can be used simultaneously.
- Read-only Policy is informed to the user upon device insertion.
- Read-only Policy violation attempts are reported to the Control in real-time.
- Any of the 10 local authorizations can be made Read-Only.



- Selective Read-Only behavior can be turned ON/OFF in real-time without requiring the disconnection of the device or the device to be connected.

While Read-Only is ON, Files cannot be transferred, modified or deleted and the USB Drive cannot be formatted.

V. 12.988 - November 22nd, 2021

GROUPS STATUS							
usb	cd	bt	wf	k. i.	mon	count	group name
U	U	U	U	OFF	ON	2	Default
P	P	P	U	ON	ON	197	Production
P	P	P	U	ON	OFF	1	Office
U	U	U	U	OFF	OFF	0	4
U	U	U	U	OFF	OFF	0	5
Change				STOP		Enforce	
130							

1. Groups Status at a Glance. (Main Interface)
2. Groups Enforce: Enforces Settings. (One Pass, to all logged machines) (Main Interface)
3. Groups Auto-Enforce Settings: (Continuous watch over Group Settings) (Main Interface)
 - Note: Auto-enforce is the New Recommended Operation Mode.
 - When settings are changed, not logged machines will automatically receive setting once they are back.
4. New Network status report includes Groups Protection Status and Auto Enforce Status. (Menu)
5. Machine history by double click. (Double click on any machine on the main network list to view its history)
6. Friendly Name Query:
 - Double click device IDs on local Authorizations list to view Device friendly name.



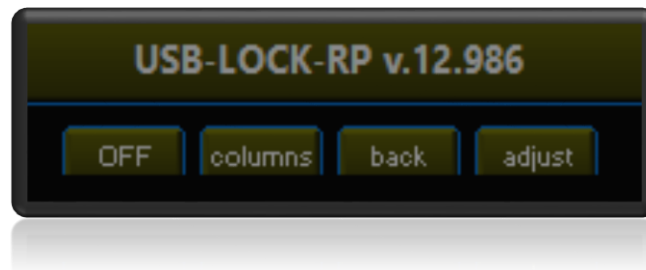
- Double click device IDs on most recent Alerts list to view Device friendly name.
(alerts containing USB IDs)

- Double click device IDs on any machine history list to view Device friendly name.
(alerts containing USB IDs)

7. Keystroke Prevention and Monitoring columns on main interface network list.
8. Remote desktop compatibility, auto adjusts to accommodate different screen resolutions.
9. Left and right side panels for USB Monitoring at a glance.

V. 12.986 - November 11th, 2021

Viewing options: allow to change background, show columns, and adjust transparency.



- More info at: <https://www.usb-lock-rp.com/>
- Demo available for download at: <https://www.usb-lock-rp.com/download.html>