

# USB-LOCK-RP

By Advanced Systems International



## USB-LOCK-RP OPERATING MANUAL

Updated: April 26<sup>th</sup>, 2024

## Table of Contents:

1) Other Resources.....	3
2) Terminology Notes.....	4
3) Protection (Sectors) .....	5
4) Machines Security Status.....	6
5) Protecting sectors to Specific Machines .....	6
6) Authorizations (USB Whitelisting) .....	7
7) Authorizing specific devices on specific machines .....	7
8) Authorizations Panel (Per machine).....	8
9) Automatic Authorizations Mode (AA) .....	10
10) Automatic Authorizations Mode to specific Machines .....	11
11) Managing Groups.....	12
12) Other Group Actions .....	13
13) Automatic Authorizations Mode to Groups .....	14
14) Deploying Authorizations to Groups.....	15
15) Blocking behavior (Client-side).....	16
16) Alerts (Control-side).....	17
17) Master Password Functionality .....	19
18) Alert Screens (Client-side) .....	20
19) Files to USB Monitoring .....	22
20) Thumb drives Encryption.....	23
21) Protection against keystroke injection attacks.....	23
22) Discovery function .....	24
23) Reboot & Restart Function (Client-Computer).....	25
24) Reload & uninstall Functions (Client-service).....	25
25) Smartphones Charge-Only Allow/Deny function .....	25
26) Auto-Email Alerts function .....	26
27) Auto Reports (Reports scheduling) .....	27
28) CEF Logs (SIEM Interoperability) .....	27
29) Logs Short-date format configuration .....	28
30) Logged Clients & License Recovery .....	29
31) Change Control Password.....	29
32) Administrative management functions .....	30
33) Technical Support .....	34
34) Implementing USB security policy and whitelist. ....	35

## 1) Other Resources

### Product Page

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

### Video Tutorials page

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

### Datasheet

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

### Installation Instructions

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

### Client MSI Mass Deployment instructions (GPO)

- o [https://www.usb-lock-rp.com/usb-lock-rp\\_client-msi\\_deployment.pdf](https://www.usb-lock-rp.com/usb-lock-rp_client-msi_deployment.pdf)

### Operating Manual (This document, online)

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

### Licensing Cost (Published Price list)

- o [https://www.usb-lock-rp.com/usb\\_lock\\_pricing.pdf](https://www.usb-lock-rp.com/usb_lock_pricing.pdf)

### Latest version highlights

- o <https://www.usb-lock-rp.com/USB-Lock-RP-latest-version-highlights.pdf>

## 2) Terminology Notes

Within the scope of this document:

**Machines** = Physical or virtual machines in your network running Windows operating systems with client installed. **Client** = USB-Lock-RP service. = *ssrvc.exe (agent), (machine- side)*

Ssrvc.exe is a service running as system process at client stations. Its function is to communicate with the Control and enforce security set by the Control.

Ssrvc.exe is located at client stations: ProgramFiles(86) \ssrvc\ssrvc.exe

Ssrvc folder is a hidden system folder, to see it you would need to adjust Explorer folder options to show hidden system folders.

**Control** = USB-Lock-RP Control application = *usbblockrp.exe (server -side)*

### Group Status

Group Status Panel

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								

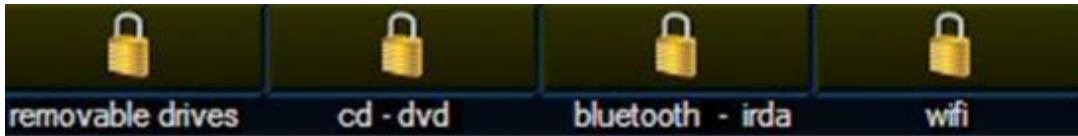
### Capabilities:

1. Groups Status at a Glance. (Main Interface)
2. Groups Enforce: Enforces Groups Settings. (One Pass, to all logged machines) (Main Interface)
3. Group Auto-Enforce Group 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.

### 3) Protection (Sectors)



Removable drives sector:



USB Mass storage | Media transfer protocol | badUSB-HID devices | Remote USB devices | e-SATA and Firewire drives | Card readers.

CD, DVD sector:



CD, DVD, Blu-Ray

Bluetooth –IrDA Sector:



File Transfers via Bluetooth & IrDA Transceivers

Wi-Fi Sector:



Wi-Fi Transceivers

## 4) Machines Security Status

Security status can be seen at a glance:

**The network list shows:**

(P) = Protected (Sector)

(U) =Unprotected. (Sector)

(Y) = ON (Monitoring)

(X) = OFF (Monitoring)

**The Selected machine panel shows:**

Sector Protected: 


Sector Unprotected: 


Monitoring

MONITORING — ON 

MONITORING — OFF 

**Automatic Authorizations Mode (ON/ OFF)**

 Automatic Authorizations (AA) OFF

 Automatic Authorizations (AA) ON  
Don't forget to turn off.

## 5) Protecting sectors to Specific Machines

1. Select a machine from the USB-Lock-RP network list.
2. Click on the desired sector lock. (Settings are apply to machines in real-time)



## 6) Authorizations (USB Whitelisting)

### DEVICE TYPE SCOPE:

USB Removable drives & USB Portable Devices

### GRANULARITY:

Specific Device ID Match (e.g. *USB\VID\_0718&PID\_070C\07072C1897488F87*)

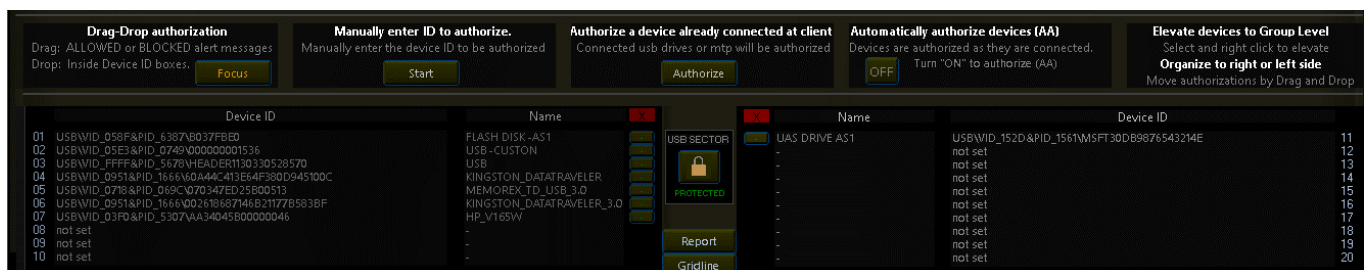
& Vendor/Model ID Match (e.g. *USB\VID\_0718&PID\_070C*)

### AUTHORIZATION SCOPE:

Specific machines & Groups of machines

## 7) Authorizing specific devices on specific machines (In Real-time)

USB-Lock-RP offers four easy ways to authorize USB removable drives and Portable devices such as smartphones.



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

## 8) Authorizations Panel (Per machine)

(Local authorizations Panel show below :)

**SURFACEPRO-1064 - LOCAL AUTHORIZATIONS PANEL**

Time	Event	Status	Action
2024-04-16 02:55:58 AM	AUTOMATIC AUTHORIZATIONS MODE	OFF	CONTROL*
2024-04-16 02:55:42 AM	USB\VID_03F0&PID_5307\AA34045800000046 HP_V165W	AUTHORIZED	CLIENT*
2024-04-16 02:55:38 AM	USB\VID_03F0&PID_5307\AA34045800000046 HP_V165W	AUTO SET(AA)	CLIENT*
2024-04-16 02:55:23 AM	USB\VID_0951&PID_1666\0026186871468211778583BF KINGSTON_DATATRAVELER_3.0	AUTHORIZED	CLIENT*
2024-04-16 02:55:12 AM	USB\VID_0951&PID_1666\0026186871468211778583BF KINGSTON_DATATRAVELER_3.0	AUTO SET(AA)	CLIENT*
2024-04-16 02:54:59 AM	USB\VID_0718&PID_069C\070347ED25800513 MEMOREX_TD_USB_3.0	AUTHORIZED	CLIENT*
2024-04-16 02:54:55 AM	USB\VID_0718&PID_069C\070347ED25800513 MEMOREX_TD_USB_3.0	AUTO SET(AA)	CLIENT*
2024-04-16 02:54:45 AM	USB\VID_0951&PID_1666\60A44C413E64F380D945100C KINGSTON_DATATRAVELER	AUTHORIZED	CLIENT*
2024-04-16 02:54:38 AM	USB\VID_0951&PID_1666\60A44C413E64F380D945100C 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\B037FBEO	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\070347ED25800513 USB	BLOCKED	CLIENT*
2024-04-16 02:48:49 AM	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\B037FBEO (EJECTED)	BLOCKED	CLIENT*
2024-04-16 02:48:48 AM	USB\VID_058F&PID_6387\B037FBEO GENERIC_FLASH_DISK	BLOCKED	CLIENT*
2024-04-16 02:44:08 AM	LOCAL AUTHORIZATION #11	REVOKED	CONTROL*
2024-04-16 02:44:05 AM	LOCAL AUTHORIZATION #1	REVOKED	CONTROL*
2024-04-16 02:44:03 AM	LOCAL AUTHORIZATION #11->:USBSTOR\DISK&VEN_HP&PROD_V165W&REV_8192\AA34045800000046	SET	CONTROL*
2024-04-16 02:43:58 AM	LOCAL AUTHORIZATION #1->:USB\VID_03F0&PID_5307\AA34045800000046	SET	CONTROL*
2024-04-16 02:43:50 AM	LOCAL AUTHORIZATION #1	REVOKED	CONTROL*
2024-04-15 05:00:51 PM	REMOVABLE STORAGE	PROTECTED	CONTROL*
2024-04-15 04:52:12 PM	LOCAL AUTHORIZATION #1->:USB\VID_346D&PID_5678\4824451206115613250	SET	CONTROL*
2024-04-15 04:43:15 PM	REMOVABLE STORAGE	UNPROTECTED	CONTROL*
2024-04-15 04:40:35 PM	LOCAL AUTHORIZATION #1	REVOKED	CONTROL*
2024-04-15 04:40:29 PM	LOCAL AUTHORIZATION #1->:USB\VID_03F0&PID_5307\AA34045800000046	SET	CONTROL*

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

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

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

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

**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	Device ID	Name
01 USB\VID_058F&PID_6387\B037FBEO	FLASH DISK-A51	11 USB\VID_152D&PID_1561\MSFT30DB9876543214E	
02 USB\VID_05E3&PID_0749\000000001536	USB-CUSTOM	12 not set	
03 USB\VID_FFFF&PID_5678\HEADER1130330528570	USB	13 not set	
04 USB\VID_0951&PID_1666\60A44C413E64F380D945100C	KINGSTON_DATATRAVELER	14 not set	
05 USB\VID_0718&PID_069C\070347ED25800513	MEMOREX_TD_USB_3.0	15 not set	
06 USB\VID_0951&PID_1666\0026186871468211778583BF	KINGSTON_DATATRAVELER_3.0	16 not set	
07 USB\VID_03F0&PID_5307\AA34045800000046	HP_V165W	17 not set	
08 not set	-	18 not set	
09 not set	-	19 not set	
10 not set	-	20 not set	

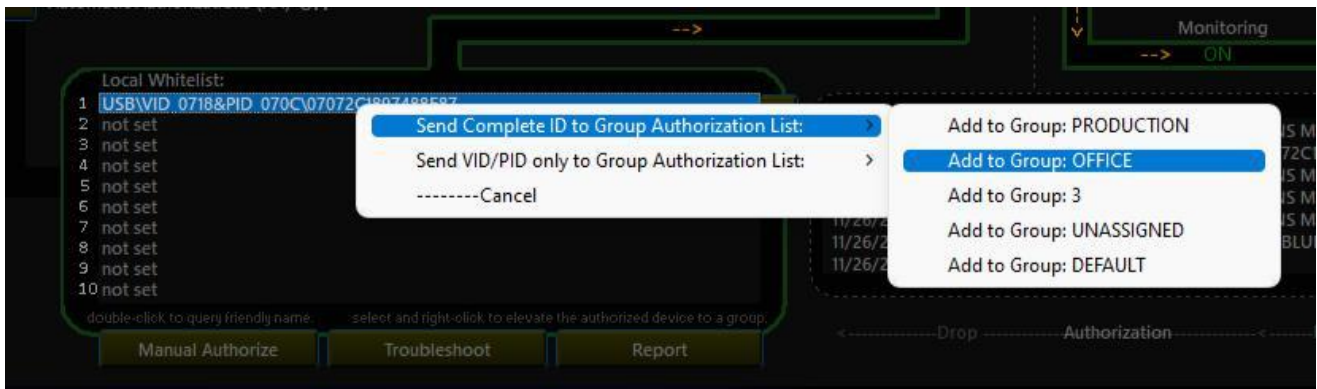
**Report** **Gridline**

### Characteristics:

- Panel Loads 200 most recent alert for any machine and updates in real-time. You may Drag blocked or allowed alerts (Highlighted in white) and Drop them inside the “Device ID” boxes of any of the 20 authorization spots available to any machine. Authorizations become effective at client machine in real-time. (Note: Authorizations can also be revoked (deleted) in real-time from this panel.



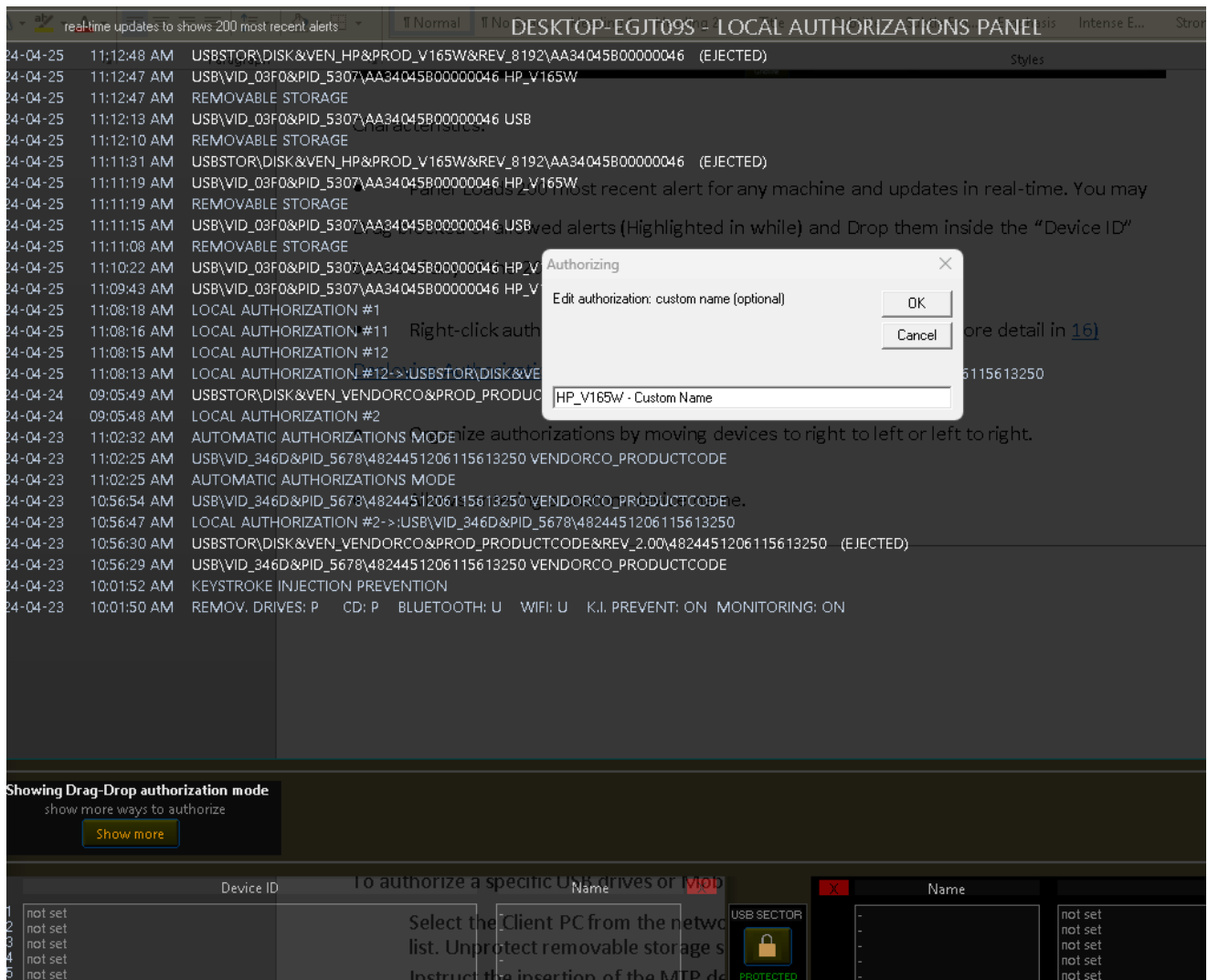
- Allows to easily elevate any authorized device to Groups level if needed so that all members of that group to be able to use the device. Right-click any authorized device IDs and select from the popup menu the option to elevate the complete ID or to elevate the Vendor Product part for a broader scope authorization based on Vendor Product match.



For more detail in [14\) Deploying Authorizations to Groups](#).

- Organize authorizations by moving devices to right to left or left to right.

This is useful to further organize device authorization.



- Allows entering a custom device name.

When Authorizing by Drag & Drop or by typing a device ID or by authorizing a connected device, the readable device name will be available, you may edit or enter a custom device name to further identify a device (Optional).

Note: You will be able to further enter notes if the device if the device is elevated to Group level from the Group authorizations panel.

## 9) Automatic Authorizations Mode (AA)

(Automatic USB drives and portable devices whitelisting)

**Scope:** Group wide & specific machine wide.

**Automatic authorization and control acquisition process.** (Advanced trademark feature of USB-Lock-RP)

Automatize devices authorization (whitelisting) process at any time authorizations need to be set to specific machines or Groups of machines automatically.

While AA Mode is active, removable drives and portable devices will be Automatically Authorized (Whitelisted) while they are normally used at Client side.

Authorizations are acquired and logged by the Control populating the machine Authorized Device ID List (See #8) in real-time and can be revoked or elevated further as needed at any time.

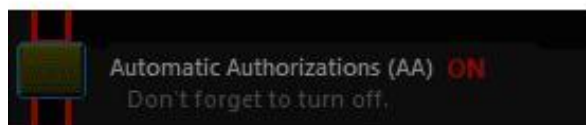
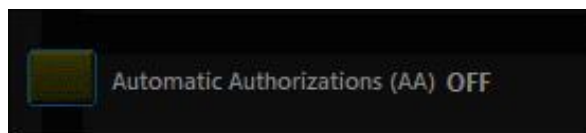
If a client system is disconnected from the Control while AA is active, AA deactivates automatically and protection becomes effective. When the client reconnects AA will re-activate automatically.

If the Control is closed AA deactivates in ALL clients and protection becomes effective.

**IMPORTANT:** Clients will NOT be effectively protected until AA is deactivated. If not deactivated earlier AA deactivates after 48 hours automatically.

## 10) Automatic Authorizations Mode to specific Machines

- 1) Select a machine from the list
- 2) Press the button (shown below)



## 11) Managing Groups

Group Status Panel

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							

### Capabilities:

Show all Groups Protection Status at a Glance. (Main Interface)

Groups Enforce: Enforces Groups Settings. (One Pass, to all logged machines) (Main Interface)

Group Auto-Enforce Group Settings: (Continuous watch over Group Settings) (Main Interface)

Note: Auto-Enforce set to ON is the Recommended Operation Mode.

When settings are changed, not logged machines will automatically receive setting once they log back.

### ○ Press Change to Set/Change Protection Settings:

GROUP ACTIONS PANEL

Rename Groups

Build Groups

Change Groups Settings

Auto Authorization Mode

Deploy Groups Authorizations

PRODUCTION

OFFICE

3

UNASSIGNED

DEFAULT

USB Removable Drives

Protect

Unprotect

CD/DVD

Protect

Unprotect

Bluetooth/IRDA

Protect

Unprotect

Wi-Fi

Protect

Unprotect

Keystroke

On

Off

Monitoring

On

Off

Save settings

Change Group Settings and Save (Once done use Enforce to apply or Auto-Enforce. (recommended))

- 1) Select a Group
- 2) Change settings
- 3) Press Save Settings
- 4) Press Enforce or Auto-Enforce to apply

## 12) Other Group Actions

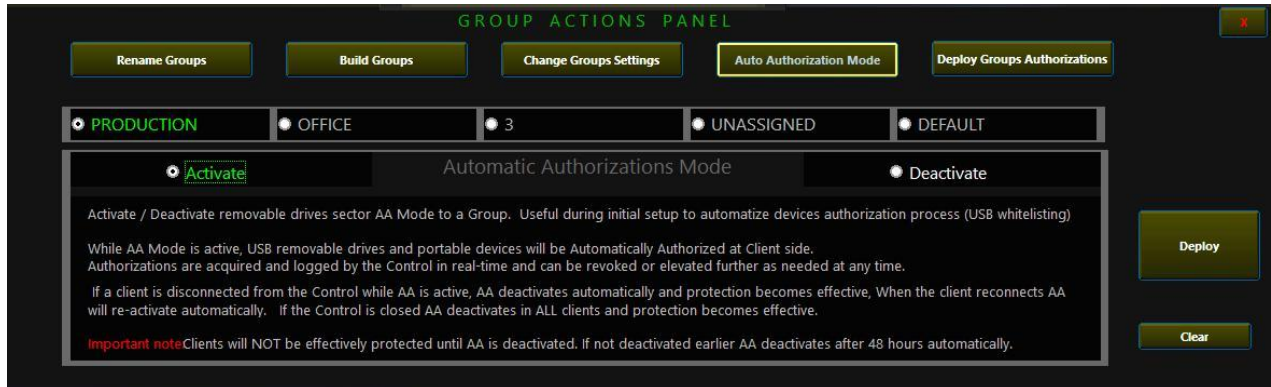
To access the Group Action panel press on the Green button.



Available Group Actions:

- **Build Groups:**  
The Group building functions allows moving Machines to Groups massively.
- **Rename Groups:**  
Five Groups are available by default (1, 2, 3, 4, and 5)  
You may change Group names at any time. (Naming groups is optional)
- **Set/Change Protection Settings: (Also accessible directly from the Group Status Panel)**  
Protects/Unprotects Sectors and sets ON/OFF Key Stroke injection prevention and Monitoring to the selected group. (Press Enforce or Auto-Enforce to apply)
- **Automatic Authorizations Mode. (Advanced Feature/Recommended)**  
Automatically whitelists removable drives and portable devices used at endpoint machines without upsetting normal operations. (Can be activated /deactivated at Group level or to specific machines)  
For more info: *Read #10.*
- **Deploy Authorizations to the selected group:**  
Specific devices (Complete ID) or by Vendor/Model (VID/PID) match.  
To populate the list see: (#12) *Elevating authorized IDs to Groups*

## 13) Automatic Authorizations Mode to Groups (Activate/Deactivate AA Mode at Group level)



- 1) Select a Group
- 2) Select Activate or Deactivate.
- 3) Press Deploy

## 14) Deploying Authorizations to Groups

**Note:** When a new device ID is elevated to the Group authorizations panel The **Group Actions** Button will be underlined in Orange Signaling a new device was added and needs to be deployed.



**Note:** You may continue to elevate devices to the list. 60 IDs can be elevated to each group.

**GROUP ACTIONS PANEL**

Build Groups | Rename Groups | Automatic Authorizations Mode | Deploy Protection Settings | **Deploy Authorizations**

Production | Office | 3 | 4 | 5

USBVID\_0951&PID\_1666/0026186871468211778583BF  
 USBVID\_03F0&PID\_5307/AA34045800000046  
 USBVID\_FFFF&PID\_5678/HEADER1130330526570  
 USBVID\_2717&PID\_FF40/dd49e51  
 USBVID\_03F0&PID\_5307  
 USBVID\_0718&PID\_069C/070347ED25800513  
 USBVID\_05E1&PID\_0749/000000001536  
 USBVID\_0718&PID\_070C/07072C1897488F87  
 USBVID\_FFFF&PID\_5678/HEADER1130330526570  
 USBVID\_0951&PID\_1666/0026186871468211778583BF

Expand  
Deploy

Press Expand To view details, revoke authorizations or set a master password | Press Deploy To apply

---

**PRODUCTION GROUP AUTHORIZATIONS**

Authorize a specific device (VID/PID/ID match): USBVID_0951&PID_1666/0026186871468211778583BF 7/31/2020 8:31:17 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_03F0&PID_5307/AA34045800000046 7/31/2020 8:31:20 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_FFFF&PID_5678/HEADER1130330526570 7/31/2020 8:31:23 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_2717&PID_FF40/dd49e51 7/31/2020 8:40:39 AM comments-> home: SURFACEPRO-1064	x	x	x
Authorize by VID/PID match: USBVID_03F0&PID_5307 7/31/2020 8:41:36 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_0718&PID_069C/070347ED25800513 7/31/2020 8:42:53 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_05E1&PID_0749/000000001536 7/31/2020 8:43:15 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_0718&PID_070C/07072C1897488F87 7/31/2020 8:44:29 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_FFFF&PID_5678/HEADER1130330526570 7/31/2020 8:46:04 AM comments-> home: ASI-NT 10-64-HP	x	x	x
Authorize a specific device (VID/PID/ID match): USBVID_0951&PID_1666/0026186871468211778583BF 7/31/2020 8:46:08 AM comments-> home: ASI-NT 10-64-HP	x	x	set x

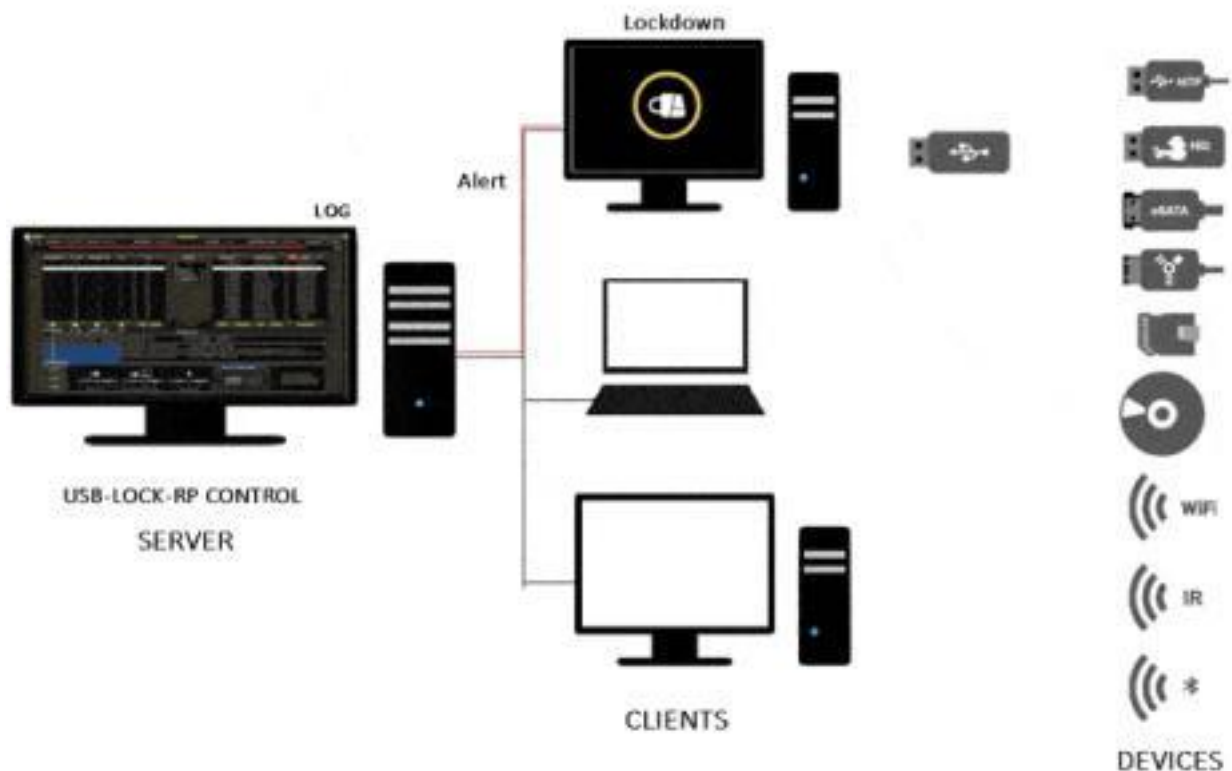
Group Master Password

View Details, Revoke Authorizations or set a Group Master Password

page 2 >>

Press expand to view detail, delete authorizations or set a group master password. When done: **Select a Group & Press Deploy**

## 15) Blocking behavior (Client-side)



USB Lockdown (blocking at client-side) is part of the software redundant measures applied to protect the system. This measures take place upon detection and included preventing drivers to load, stopping, dismounting, disabling, ejecting devices and also blocking access to the desktop.

Protection measures escalated depending on the device type and the device status but lockdown is normally included when blocking USB and other removable storage under the software protection scope.

Blocking & desktop Lockdown is simultaneous and present full-screen window alerts that extend to multiple monitors and remain until ANY of the following conditions is met:

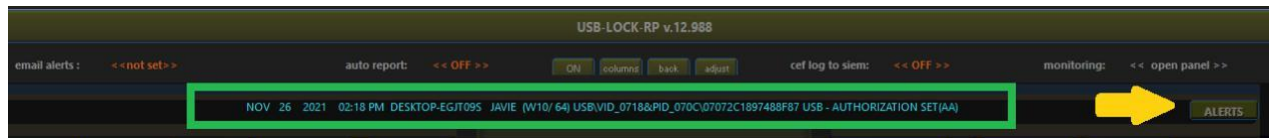
- The unauthorized device is removed. (Client-side)  
The master password is used. (Client-side.)  
The sector is unprotected. (Control-side.)  
The device is authorized. (Control-side.)



## 16) Alerts (Control-side)

The last received alert will show on the top visor. ALERTS Button to expand view and see alerts for all machine in the network.

Note: Automatically Logs: allowed, blocked or authorized insertion alerts in real-time.



Network Alerts Log: Shows alerts for all clients.

showing: 1539 records

Network Alerts Log:						
date	time	machine	user	os   bit	message	action
2024-04-03	10:26:39 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00_6&2A80105C&0&0000 APPLE IPHONE	AUTHORIZED
2024-04-03	10:26:21 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00_6&2A80105C&0&0000 APPLE IPHONE	AUTO SET(AA)
2024-04-03	10:22:35 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00_6&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:22:08 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00_6&2A80105C&0&0000 APPLE IPHONE	BLOCKED
2024-04-03	10:21:47 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00_6&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:19:58 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00_6&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:13:37 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_152D&PID_1561\MSFT30DB9876543214E 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_V16SW	AUTHORIZED
2024-04-03	10:11:18 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_03F0&PID_5307\AA34045B000000046 HP_V16SW	AUTO SET(AA)
2024-04-03	10:11:07 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USBSTOR\DISK&VEN_HP&PROD_V16SW&REV_8192\AA34045B000000046	EJECTED
2024-04-03	10:11:06 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_03F0&PID_5307\AA34045B000000046 HP_V16SW	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_V16SW&REV_8192\AA34045B000000046	EJECTED

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

- Blocked, Ejected, Uninstalled = RED
- Allowed, Authorized, Authorization Alerts Set = Green
- Charging, Connected = Gold
- Control Started, Control Closed = Grey

## Client History Log:

- Select a client PC from the network list.
- Click Double-click to open the machine history log.

menu < > USB-LOCK-RP v.12.988 < > -

email alerts: <<not set>> auto report: << OFF >> ON columns back adjust cef log to siem: << OFF >> monitoring: << open panel >>

DESKTOP-EGJT09S machine history log --> showing: 1483 records out of: 1483 X

11/25/21	2:10:59PM	USB\VID_03F0&PID_5307\AA34045800000046 USB	ALLOWED	CLIENT*
11/25/21	2:09:19PM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: ON	ENFORCED	CONTROL*
11/25/21	2:08:06PM	USB\VID_03F0&PID_5307\AA34045800000046 USB	ALLOWED	CLIENT*
11/25/21	2:03:02PM	KEYSTROKE INJECTION PREVENTION	TURNED OFF	CLIENT*
11/25/21	2:03:00PM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/25/21	2:01:43PM	REMOV. DRIVES: P CD: P BLUETOOTH: P WIF: U K.I. PREVENT: ON MONITORING: ON	ENFORCED	CONTROL*
11/25/21	2:00:38PM	KEYSTROKE INJECTION PREVENTION	TURNED ON	CLIENT*
11/25/21	2:00:36PM	REMOV. DRIVES: P CD: P BLUETOOTH: P WIF: U K.I. PREVENT: ON MONITORING: ON	ENFORCED	CONTROL*
11/24/21	9:15:55AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/24/21	8:52:22AM	REMOV. DRIVES: P CD: P BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/24/21	8:52:17AM	REMOV. DRIVES: U CD: P BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/24/21	8:52:12AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/24/21	1:13:15AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/24/21	1:13:14AM	CD DVD	PROTECTED	CONTROL*
11/24/21	1:13:12AM	CD DVD	UNPROTECTED	CONTROL*
11/24/21	1:13:08AM	CD DVD	PROTECTED	CONTROL*
11/24/21	12:57:42AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/24/21	12:57:41AM	CD DVD	PROTECTED	CONTROL*
11/24/21	12:48:44AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*

The machine history log includes all alert incoming from the machine and setting deployed from the control to the machine.

## 17) Master Password Functionality

SCOPE: Group Level (One password per Group)

BEHAVIOR: When a blocking alert screen remains more than 25 seconds at a client machine a password input box appears and can be used to enter the group master password to regain access to the client.

In case of USB MTP devices (e.g. smartphones) it will allow regaining access to the desktop and authorize the device usage for one time.

In case of USB Drives. It will only allow regaining access to the desktop.



Useful for:

Troubleshooting: Regaining access to the desktop if an internal device wrongfully reporting as removable is blocked & The Control is unreachable.

The program is delivered with a custom master password. Nevertheless it is recommended that you change this password and set one for each used group.

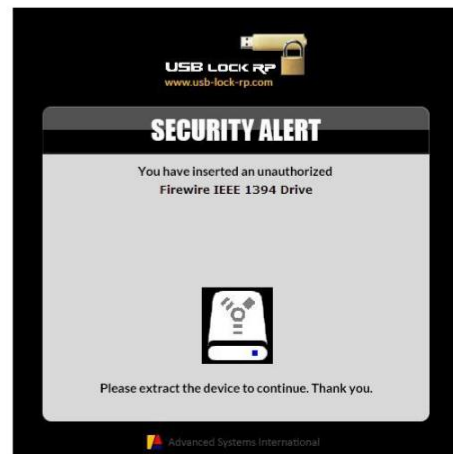
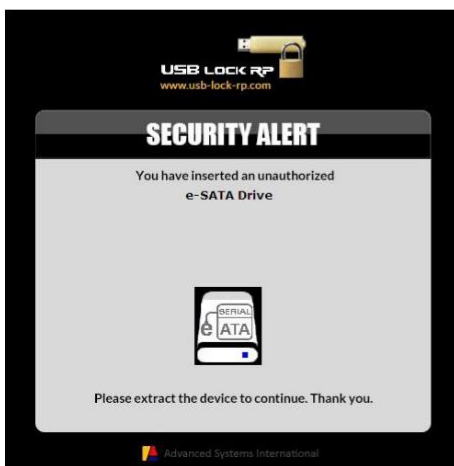
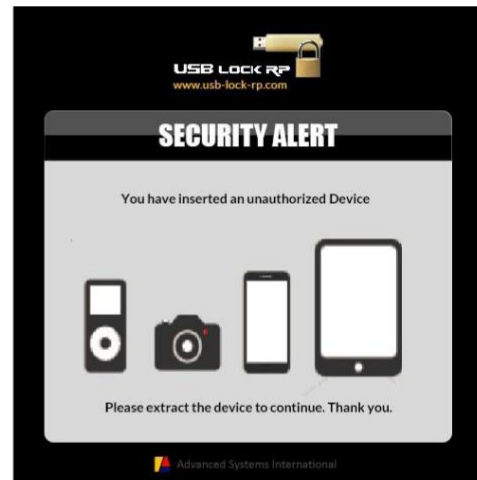
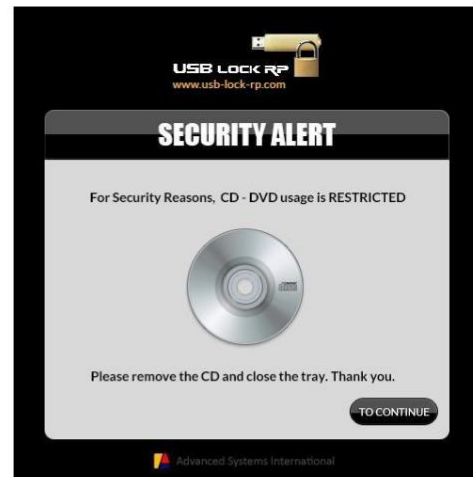
The Password as well as all critical program setting and IDs are stored encrypted (only readable within the Control interface)

From the Control: The master password can be deployed to Groups of machines from the Groups authorization panel. **See 14 (Deploying Authorizations to Groups)**

## 18) Alert Screens (Client-side)

Full screen alerts (Extend to all monitors)

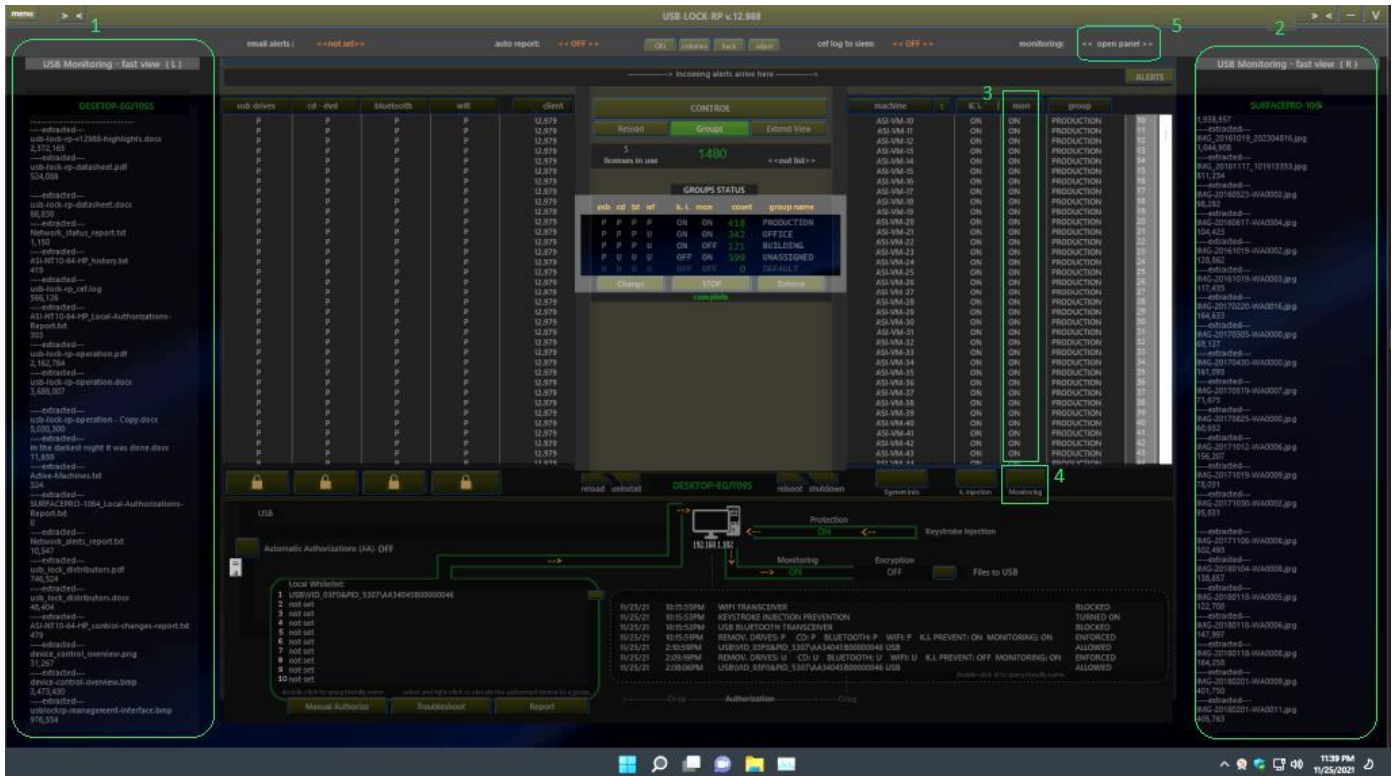
The following alerts show at clients depending on the blocked device type.



Wireless small alerts: (appear at right-low corner)



## 19) Files to USB Monitoring



- 1) Monitoring Left Fast view Panel
- 2) Monitoring Right Fast view Panel
- 3) Monitoring Status
- 4) Turn Monitoring ON or OFF
- 5) Open Main Monitoring Panel

Monitored data include the name and exact weight of transferred files from the client endpoint PC to flash drives, logged user, device hardware ID, source machine name, date/time when the event started.

Records are sent AES 256 encrypted and Hex masked from the endpoint computer to the control in near real-time and are organized at the control by endpoint machine name/date/time for review as needed.

At the Central control server data remains encrypted, same as all logged events only readable within the Device Control interface.

## 20) Thumb drives Encryption

Forcing automatic Encryption to authorized drives, this function can also be turned ON or OFF with just one click. (USB Monitoring needs to be activated for Encryption to be set). When USB Encryption is active all files transferred from the endpoint computer to authorized USB flash drives are automatically AES 256 encrypted. (All data not just the headers).

Stored files on encrypted USB Thumb drives can be opened within the endpoint originating client or within any other endpoint USB-Lock-RP client that has USB Encryption turned ON. On those systems Files are automatically decrypted when double-clicked. Alternatively files can be decrypted in those systems by transferring the files to the Folder named: decryptor

(Found at the client machine root directory).

This function ensures that information contained inside authorized devices is only accessible within determined computers in the network and none outside the network

## 21) Protection against keystroke injection attacks



Included in the removable drives sector is protection against badUSB device e.g. USB Rubber Ducky, this type of device is extremely dangerous as its firmware has been modified to impersonate Human interface devices (HID) such as keyboards and are capable of on the go inflicting keystroke injection attacks and introduce malicious payloads to harm the operating system and network infrastructure.

Blocking USB of this type is a standard function in USB Lock, the program makes a quick analysis when detects any change on keyboard/mouse enumeration will trigger an automatic assessment to neutralize the threat if present. This events as any other insertion attempt events at endpoint clients are reported to the Central Control in near real-time.

You may exclude the connected keyboards from analysis on the event that analysis is obtrusive. In cases laptops/tablets of detachable keyboards, smart pens or docking stations. But normally no action is required.

## 22) Discovery function



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.

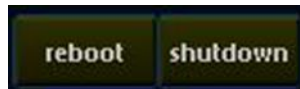
**SURFACEPRO-1064**

System Information	Removable Storage / Mobile phones	Printers / Printer queue	HID (Human interface device)
<p>4/26/2024 2:04:20 PM</p> <p>Machine name: SURFACEPRO-1064</p> <p>IP address: 192.168.1.105</p> <p>Logged user: JAVIE</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>OS: Windows 10 Enterprise 64 Bit.</p>	<p>Device Name: USB Drive (D:)</p> <p>Device Type: USB Drive</p> <p>Device Path: D:</p> <p>Id: \A4A4045B000000046</p> <p>Size: 7.60 GB</p> <p>Free: 7.38 GB</p> <p>File System: NTFS</p>	<p>Device Name: Canon E400 series Printer</p> <p>Status: Offline</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>Device Name: OneNote for Windows 10</p> <p>Status: Ready</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: 0x07</p> <p>MaxPower: 0x32 (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>
Installed Software	Running Processes	Network Adapters	
		<p>Wi-Fi</p> <p>Status: Disconnected</p> <p>Marvell AVASTAR Wireless-AC Network Controller</p> <p>Not connected</p> <p>MAC Address: B8-31-85-32-D6-92</p> <p>Ethernet</p> <p>Status: Connected</p> <p>Surface Ethernet Adapter</p> <p>IP Address: 192.168.1.106</p> <p>Subnet Mask: 255.255.255.0</p> <p>Assigned by DHCP</p> <p>IPv6 Enabled</p> <p>TP-LINK_9M424C</p> <p>MAC Address: BC-83-85-08-6D-CA</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: 0x22</p> <p>MaxPower: 0x32 (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>

Refresh Export



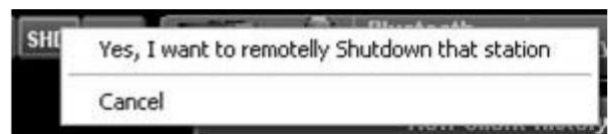
## 23) Reboot & Restart Function (Client-Computer)



Allows to reboot or shutdown the selected client computer remotely from the control.

Select a Client Machine from the network list.  
Press on the button Reboot or Shutdown.

When you press the corresponding button a popup will appear asking for confirmation to avoid accidentally executing the command.



When you execute either command a message will appear on the Clients screen advising the user has 20 seconds to save his/her work before the Reboot or Shutdown action takes place.

## 24) Reload & uninstall Functions (Client-service)



Select a Client Machine from the network list.  
Press on the button Reload or uninstall.

Reload: reestablishes the selected client connection.

Uninstall: uninstalls the usb-lock-rp service installed on the client machine.

Note: This action also unprotects all sectors.

## 25) Smartphones Charge-Only Allow/Deny function



New MTP blocking behavior:

Allows unauthorized Smartphones to be connected for-charging-only without blocking. (When set to deny, smartphones require to be authorized even if to be connected for charge only.)

## 26) Auto-Email Alerts function

Automatically send **ALL** incoming alerts arriving to the Control to an email address of your choice within your domain (to be used as centralized alternative logs repository)

Automatic after easy setup

Allows SSL / TLS

All incoming alerts logged to the Control are sent.

USB Lock RP (Auto email alerts setup)

**auto e-mail alerts (smtp)**

1 Enter from email account:   
This is the email address originating the alert

2 Enter destination email account   
This is the email address were alerts will arrive.

3 Enter mail server   
example: mail.yourcompanydomain.com or ip number

Server requires authentication ☐

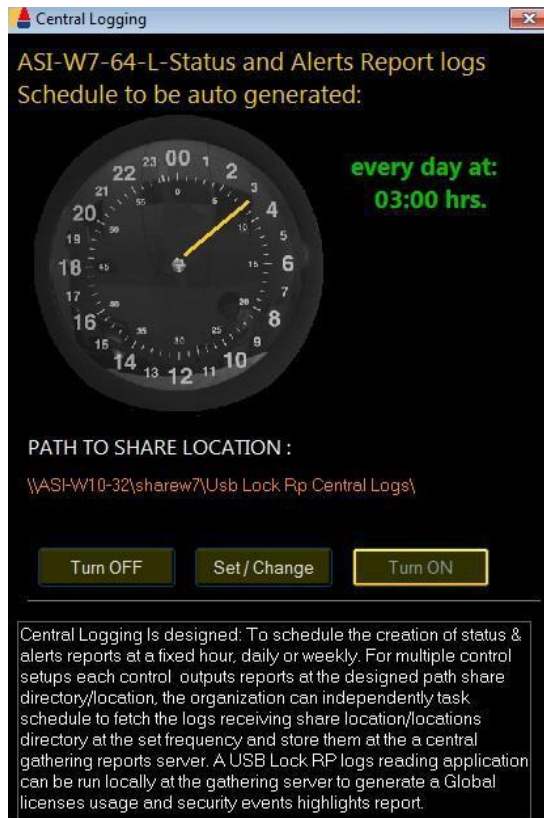
SMTP port 25 ☐  
SMTP port 587 ☐  
SMTP port 465 ☐

TLS ☐  
SSL ☐

Set / Change / Turn ON Close

## 27) Auto Reports (Reports scheduling)

To schedule the automatic creation of status & alerts report at a fixed hour, daily or weekly to a set shared path.



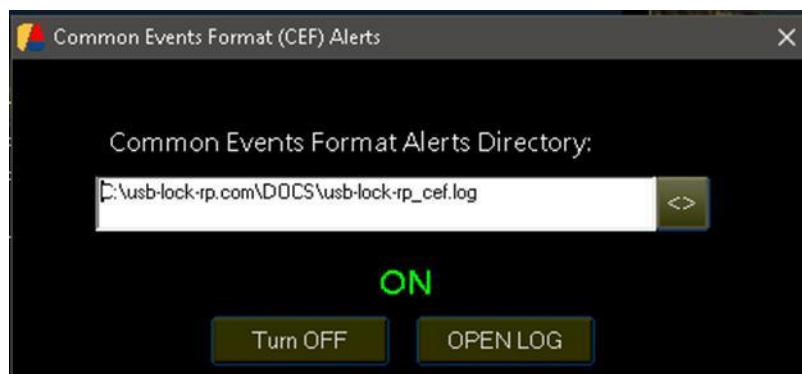
## 28) CEF Logs (SIEM Interoperability)

(Set Common Events Format logs for integration with SIEM)

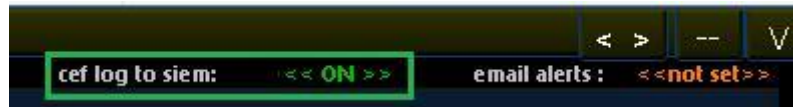
- 1) Click on << OFF >> label



- 2) Set Path



3) Turn ON to log events in Common Events format.



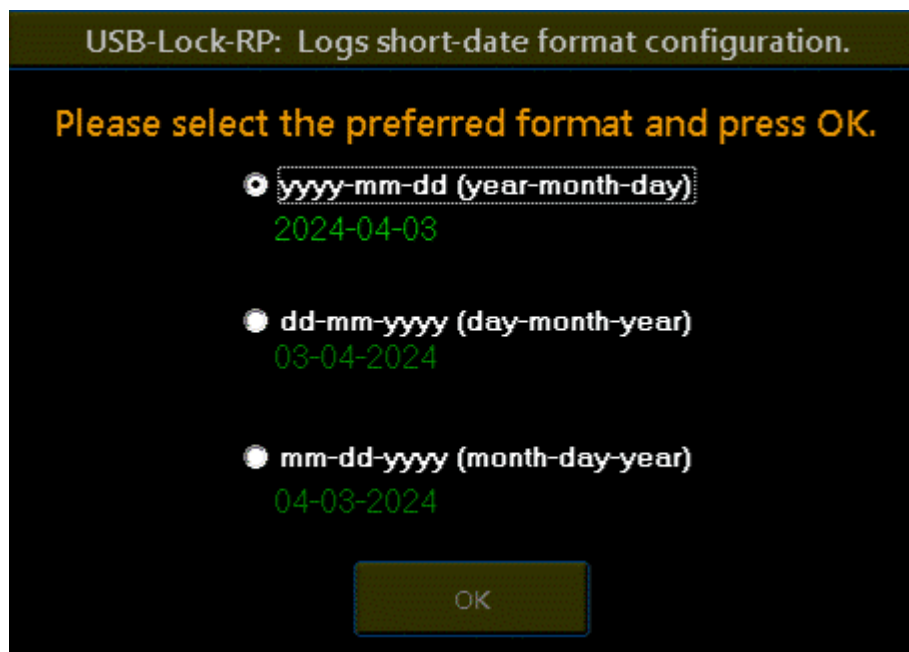
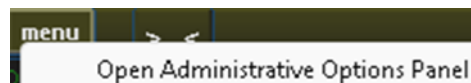
Log format example: (Copy/past to view detail)

```
Jul 02 11:15:54 ASI-NT10-64-HP CEF:0|Advanced Systems|USB-LOCK-RP|12.8|104|authorized device connection|7|src=192.168.0.13 msg=ASI-NT10-64-HP JAVIE (W10/ 64) USB\\VID_03F0&PID_5307\\AA34045B000000046 USB - AUTHORIZED
Jul 02 14:10:34 ASI-NT10-64-HP CEF:0|Advanced Systems|USB-LOCK-RP|12.8|103|unauthorized device connection blocked|9|src=192.168.0.13 msg=ASI-NT10-64-HP JAVIE (W10/ 64) USB\\VID_03F0&PID_5307\\AA34045B000000046 USB - BLOCKED
```

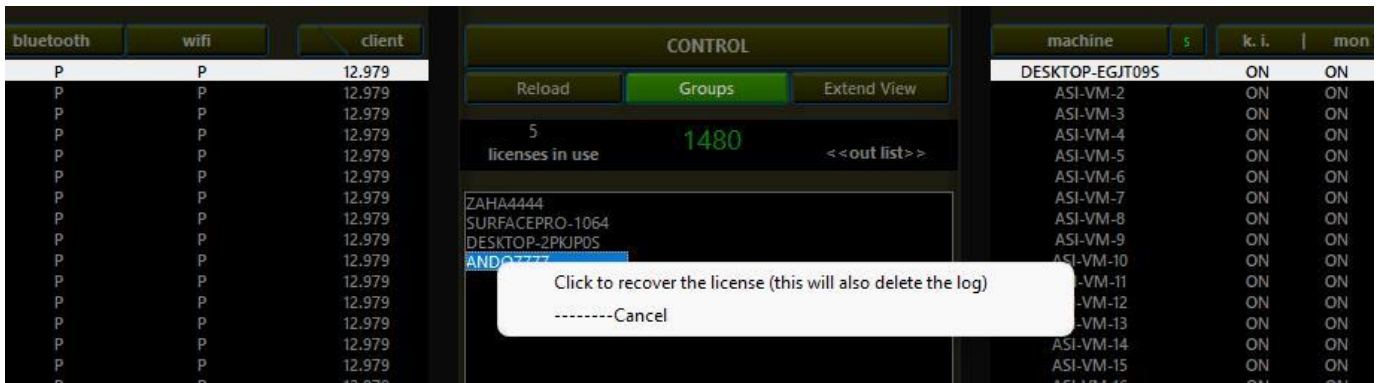
## 29) Logs Short-date format configuration

**The Logs Short-date format configuration Panel will appear automatically the first time the Control is started.**

Note: It can also be accessed thru the: Main Menu / Administrative Options Panel /Short date format function



## 30) Logged Clients & License Recovery



Shows the number of logged Clients. (1)

<<Out list>> shows a list of not logged Clients. (2)

To remove unused Clients Pcs to recover licenses. (3)

1. Click on <<out list>>
2. Select a Machine from the outlist
3. Click recover license.

Using these methods USB Lock RP allows recovering unused licenses.

## 31) Change Control Password

(Use to change the password used to access the USB Lock RP Control)

The program is delivered with a custom default Control password:



Enter the old password. Enter the new password.

Re-Type the new password.



**Change control access password**

Type old password

Type new password

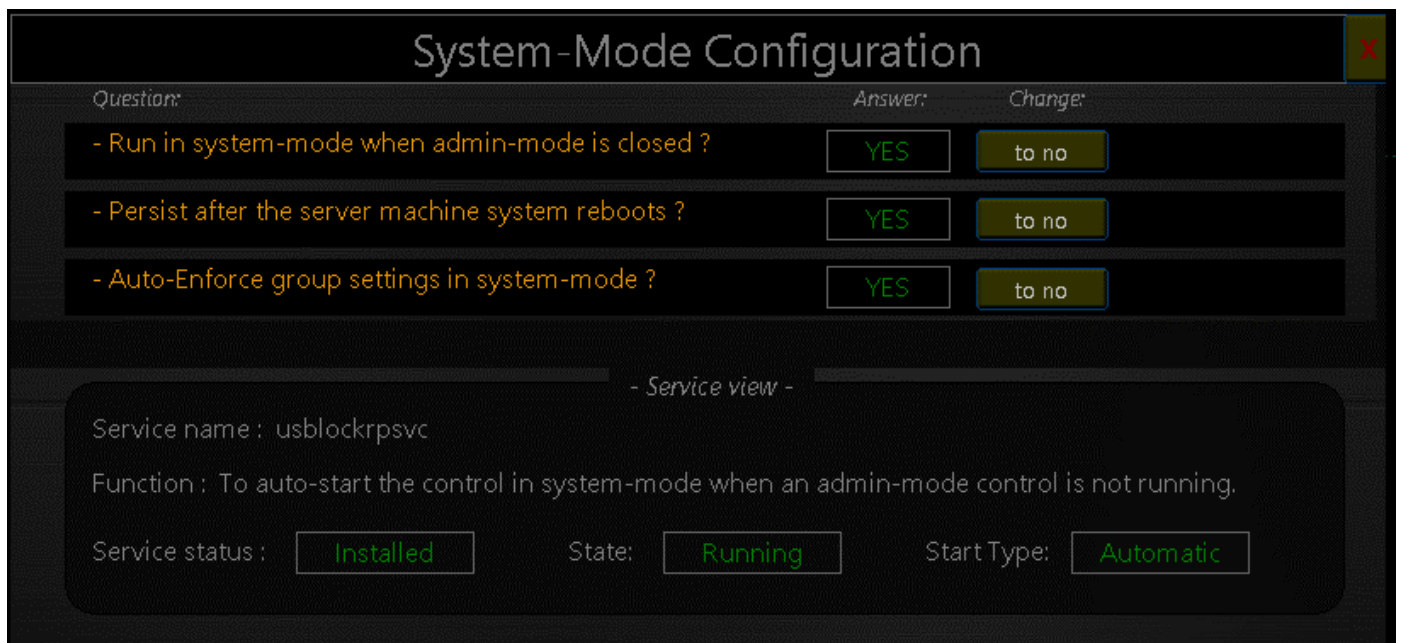
Re-Type new password

NOTE: Password is case sensitive. Numbers , Letters, and Spaces are valid.  
Important: The password need to be at least 8 characters  
Example: 4Rxd12fb

## 32) Administrative management functions

### Control System-Mode operation:

System-mode control operation. Allows 24x7 real-time USB security management, alerting and enforcement. This function automatically starts the control in system-mode while an admin-mode control is not running.



**System-Mode Configuration**

Question:	Answer:	Change:
- Run in system-mode when admin-mode is closed ?	<input type="button" value="YES"/>	<input type="button" value="to no"/>
- Persist after the server machine system reboots ?	<input type="button" value="YES"/>	<input type="button" value="to no"/>
- Auto-Enforce group settings in system-mode ?	<input type="button" value="YES"/>	<input type="button" value="to no"/>

- Service view -

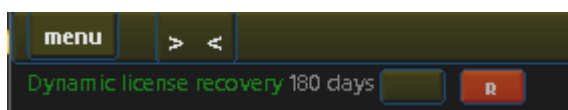
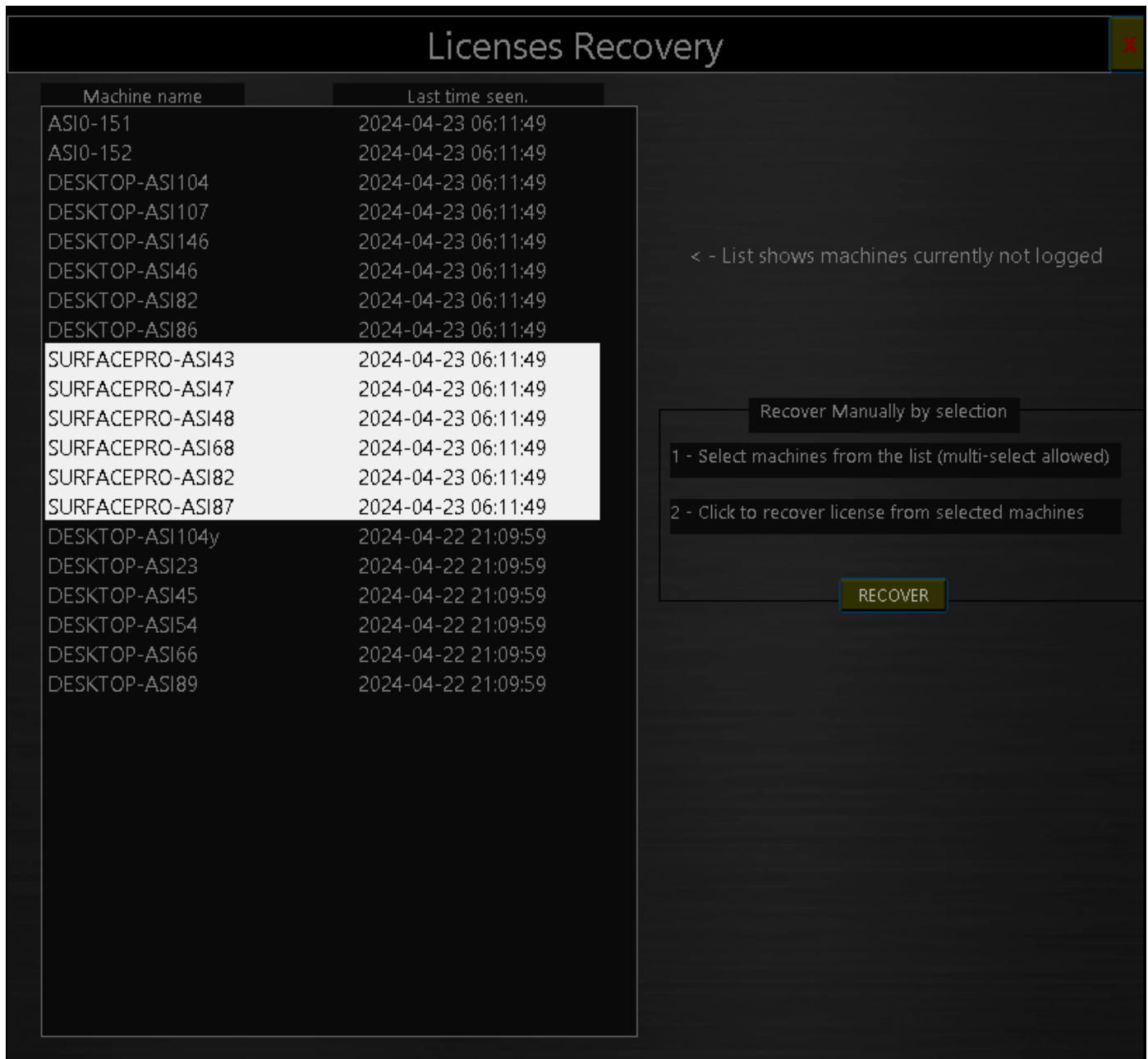
Service name : usblockrpsvc

Function : To auto-start the control in system-mode when an admin-mode control is not running.

Service status :  State:  Start Type:

Licenses recovery:

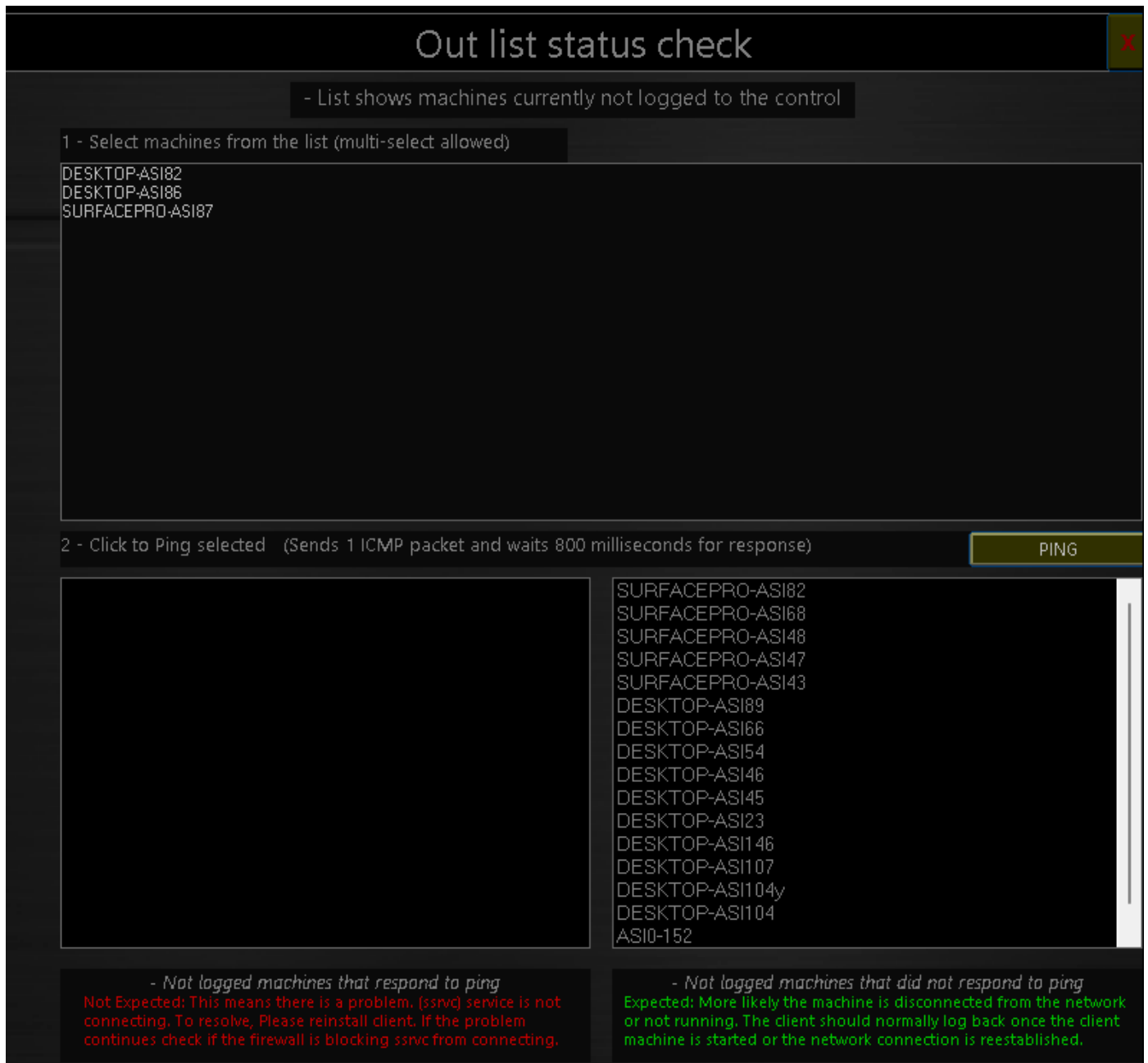
The license recovery function allow recovering licenses from the not logged machines list, allows you to recover unused machines licenses.



You can also recover licenses dynamically based on the last time a client logged to the control. The image shows setting to recover licenses from machines not seen by the control for a time older than 6 months. (You can also choose to recover after 2 months, 3 months 1 year.)

Connection troubleshooting:

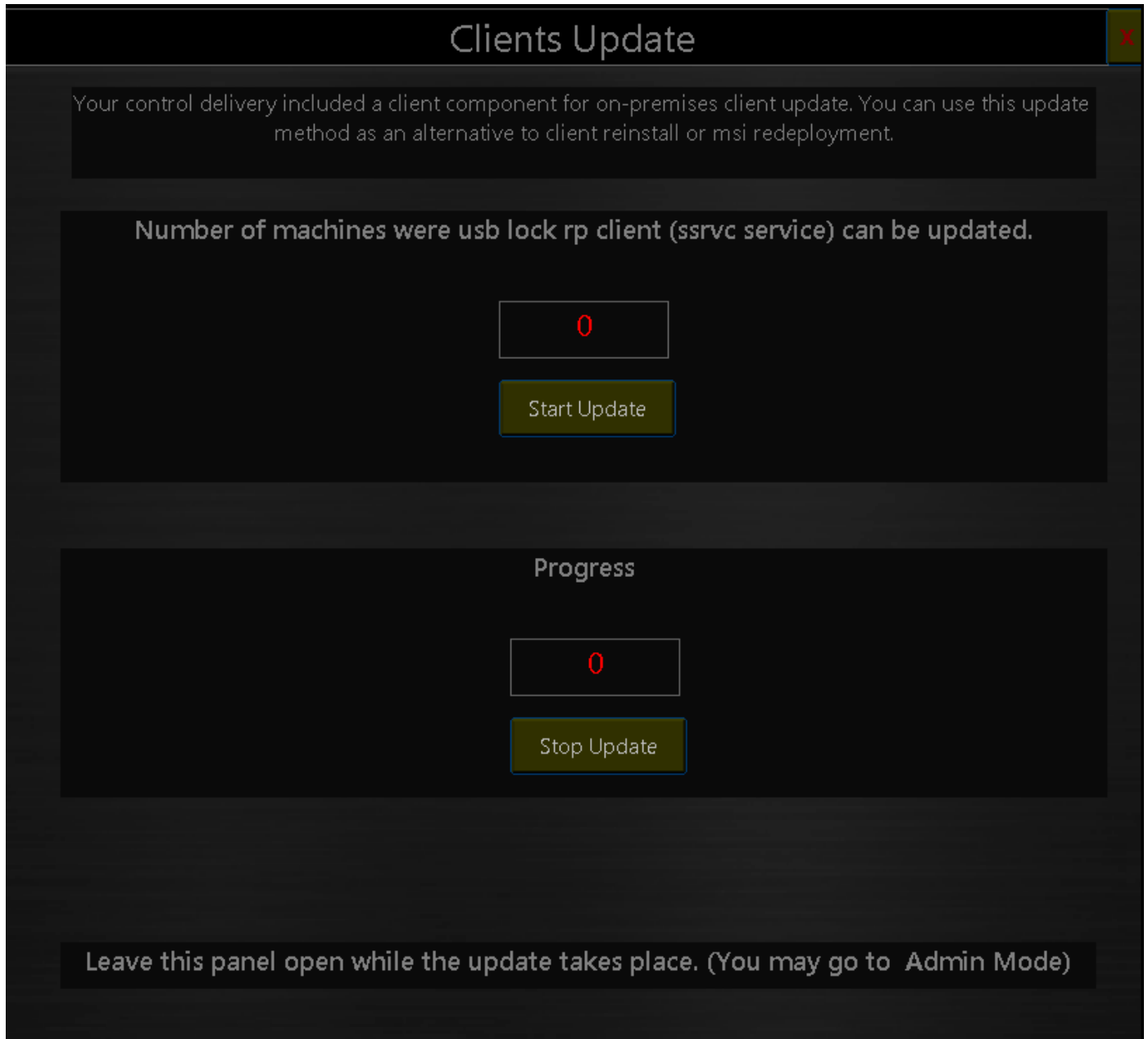
Out list Diagnostic function: Allows to send an ICMP packet (ping) to not-logged machines to diagnose client/machine availability to help identify client connectivity issues.





On-premises Clients Update function:

Clients Update function panel: Allows to massively update client's version from control-side. Your Control update is always delivered with a latest version client component you can update clients internally from the control. (on-premises) no connection outside your network required.



## 33) Technical Support

**USB-LOCK-RP**  
By Advanced Systems International



info@usb-lock-rp.com

www.usb-lock-rp.com

Phone:

**+1 (972) 890 9488**

**+44 020 3286 0406**

USB LOCK RP ©: Developer & Licensor & Backbone Support

We stand by.

## 34) Implementing USB security policy and whitelist.

The following applies to Large or small networks and assume usb-lock-rp client has already been deployed to machines in the network.

### **Setting and enforcing removable media policy.**

1. Go to group actions panel.
2. Rename and Build Groups.
3. Set settings to groups
4. Press auto-enforce.

### **Automatic Whitelisting.**

**(The following won't be suitable for all type networks, nevertheless is the most automatic whitelist implementation)**

5. Build a group conformed by machines that need to have devices authorized. (Whitelisted)
6. Click Automatic Authorizations Mode Button.
7. Activate Automatic Authorizations to "that group". (Instead of blocking the program will authorized connected devices automatically)

Client-side users on "that group" operate normally connecting the devices they normally use.

Note: You may harden on restricting external physical access to premises during this process.

Connected removable storage and portable devices will be automatically added to the local authorized ID list at the control.

8. De-activate Automatic Authorizations to that group. (After a few hours)

**AA Deactivates and security becomes effective and unauthorized removable drive or smartphone will be blocked**

**&**

**While authorized (whitelisted) devices can be connected and used normally.**

You can now revoke any authorizations you don't like in real-time or elevate them further to groups.

You may set your SIEM Interoperability, Schedule automatic reports, email alerts, monitor transfers to authorized USBs...