



# USB-LOCK-RP OPERATING MANUAL

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

Copyright 2004 – 2024 Advanced Systems International SAC. All rights reserved

# 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 <a href="https://www.usb-lock-rp.com/">https://www.usb-lock-rp.com/</a>

### Video Tutorials page

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

### Datasheet

o <a href="https://www.usb-lock-rp.com/usb-lock-rp-datasheet.pdf">https://www.usb-lock-rp.com/usb-lock-rp-datasheet.pdf</a>

### Installation Instructions

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

### Client MSI Mass Deployment instructions (GPO)

o https://www.usb-lock-rp.com/usb-lock-rp\_client-msi\_deployment.pdf

### Operating Manual (This document, online)

o <a href="https://www.usb-lock-rp.com/usb-lock-rp-operation.pdf">https://www.usb-lock-rp.com/usb-lock-rp-operation.pdf</a>

### Licensing Cost (Published Price list)

o <u>https://www.usb-lock-rp.com/usb\_lock\_pricing.pdf</u>

### Latest version highlights

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

# 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 = *usblockrp.exe* (*server -side*)

#### **Group Status**

#### **Group Status Panel**

				GR	OUPS S	TATUS	
usb	cd	bt	wf	k. i.	mon	count	group name
U	U	U.	U	OFF	ON	2	Default
				ON	ON		Production
		Ρ		ON	OFF		Office
	Ch	ange	-		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)

9			9
removable drives	cd - dvd	bluetooth - irda	wifi

### 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)

matic Authorizations (AA)

#### The Selected machine panel shows:



# 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.

Drag-Drop authorization Drag: ALLOWED or BLOCKED alert messages Drop: Inside Device ID boxes.	Manually enter ID to au Manually enter the device ID to Start				nected at client vill be authorized	Devices are au	r <b>authorize devices (AA)</b> thorized as they are connected. rn "ON" to authorize (AA)	Elevate devices to Select and right cli Organize to right Move authorizations	ick to elevate or left side
Device ID		Name	X		X	Name		Device ID	
01 USBWID_055F&PID_6387/B037FBD 22 USBWID_05E5&PID_742400000001536 03 USBWID_95E5&PID_7424000000001536 04 USBWID_951&PID_1666400.444473854F38009 05 USBWID_0351&PID_16664002478567746821777B 07 USBWID_03F0&PID_53074A34045800000046 08 notset 10 notset	70 45100C 583BF	FLASH DISK -AS1 USB -CUSTON USB KINGSTON_DATATRAVELER MEMOREX_TD_USB_30 KINGSTON_DATATRAVELER HP_V165W - -		Report Gridline			USBWID_IS2D&PID_IS61WISFI not set not set not set not set not set not set not set not set not set	T30D89876543214E	11 12 13 14 15 16 17 17 18 19 20

- 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 :)

1U <		USB-LOCK-RP v.13.824		
mic license email ale		>> auto reports: << OFF >> ON columns back adjust cef log to siem: << OFF >>	monitoring: <	< open panel >>
	eal-time updates to sh	ws 200 most recent alerts SURFACEPRO-1064 - LOCAL AUTHORIZATIONS PANEL		
4-04-16			OFF	CONTROL
4-04-16		JSB\vID_03F0&PID_5307\AA34045B00000046 HP_V165W	AUTHORIZED	CLIENT*
-04-16		JS8\vID_03F0&PID_5307\AA34045800000046 HP_V165W	AUTO SET(AA)	CLIENT*
-04-16		JS8\vID_0951&PID_1666\00261868714682117785838F KINGSTON_DATATRAVELER_3.0	AUTHORIZED	CLIENT*
-04-16	02:55:12 AM	JSB\VID_0951&PID_1666\00261868714682117785838F KINGSTON_DATATRAVELER_3.0	AUTO SET(AA)	CLIENT*
	02:54:59 AM	JS8\VID_0718&PID_069C\070347ED25800513 MEMOREX_TD_US8_3.0	AUTHORIZED	
-04-16	02:54:55 AM	JSB\VID_0718&PID_069C\070347ED25B00513 MEMOREX_TD_USB_3.0	AUTO SET(AA)	CLIENT*
-04-16		JSB\VID_0951&PID_1666\60A44C413E64F380D945100C KINGSTON_DATATRAVELER	AUTHORIZED	
		JSB\VID_0951&PID_1666\60A44C413E64F380D945100C KINGSTON_DATATRAVELER	AUTO SET(AA)	CLIENT*
-04-16		JSB\vID_FFF&PiD_5678\HEADER1130330528570 USB	AUTHORIZED	CLIENT*
-04-16		JSB\VID_FFFF&PID_5678\HEADER1130330528570 USB	AUTO SET(AA)	CLIENT*
-04-16		AUTOMATIC AUTHORIZATIONS MODE	ON	CONTRO
-04-16		.0CAL AUTHORIZATION #2->:USB\VID_05E3&PID_0749\000000001536	SET	CONTROL
-04-16			REVOKED	CONTROL
-04-16		OCAL AUTHORIZATION #11->:USB/UD_1520&PID_1561;MSFT300B9876543214E	SET	CONTROL
-04-16 -04-16		.OCAL AUTHORIZATION #2->:USB\VID_152D&PID_1561\MSFT30DB9876543214E	SET	CONTRO
-04-16		.OCAL AUTHORIZATION #1->:USB\VID_058F&PID_6387\B037FBE0 JSB\VID_152D&PID_1561\MSFT30DB9876543214E_UAS		CUNTRO CLIENT*
-04-16		JSBSTOR\DISK&VEN_GENERIC&PROD_MASSSTORAGECLASS&REV_1536\00000001536 (EJECTED)		CLIENT*
-04-16		JSB/VID_05E3&PID_0749\00000001536 USB		CLIENT*
-04-16		JSUVID FFFAPID 5676/HEADER 1130330528570 USB		CLIENT*
-04-16		35(VID.0718&PID.069(V70347ED25800513 USB		CLIENT*
-04-16		USBYTORYDISKAVEN GENERIC&PROD FLASH DISK&REV 8.07\B037FBE0 (EJECTED)		CLIENT*
-04-16		JSB\vID 058F&PID 6387\B037FBE0 GENERIC FLASH DISK		CLIENT*
-04-16		OCAL AUTHORIZATION #11	REVOKED	CONTROL
-04-16	02:44:05 AM	.OCAL AUTHORIZATION #1	REVOKED	CONTROL
-04-16	02:44:03 AM	.OCAL AUTHORIZATION #11->:USBSTOR\DISK&VEN_HP&PROD_V165W&REV_8192\AA34045B00000046		CONTROL
	02:43:58 AM	.OCAL AUTHORIZATION #1->:USB\VID_03F0&PID_5307\AA34045B00000046		CONTRO
	02:43:50 AM	.ocal authorization #1	REVOKED	CONTRO
-04-15	05:00:51 PM	REMOVABLE STORAGE	PROTECTED	CONTRO
		.OCAL AUTHORIZATION #1->:USB\VID_346D&PID_5678\4824451206115613250		CONTRO
-04-15		REMOVABLE STORAGE	UNPROTECTED	CONTRO
		OCAL AUTHORIZATION #1	REVOKED	CONTRO
	04-40-29 PM	∩CAL_ALITHORIZATION #1->+ISB\VID_03F0%PID_5307\AA34045R00000046		CONTRO
	rag-Drop authoriz		Elevate devices	
	WED or BLOCKED a Device ID boxes. (	Turn "ON" to authorize (84)	d. Select and righ Organize to ric	t click to elevate I <b>ht or left side</b>
		Focus Start Authorize OFF	Move authorizatio	
		Device ID Name 🔀 Name	Device ID	
	058F&PID_6387\B	37F660 FLASH DISK-AS1 USB SECTOR UAS DRIVE AS1 USB SHOLD 152D APID 1561V		
USB\VID	05E3&PID_0749\0	D00001536 USB-CUSTON		
	0951&PID_1666\60	ADER1130330520570 USB not set 44C413E54F380D945100C KINGSTON_DATATRAVELER IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		
	0718&PID_069C\07			
USB/VID	)_0951&PID_1666\00 )_03F0&PID_5307\A	- not set 3404580000046 - HP_V165W - not set		
not set not set		- not set		
		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.

#### USB-LOCK-RP Operating Manual

• 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 f or a broader scope authorization based on Vendor Product match.



For more detail in <u>14</u>) 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.

#### USB-LOCK-RP Operating Manual

) - 🌌	real-time updates to	shows 200 most recent alerts	¶ Normal	TNº DES	KTOP-EGJT09S - LO	CAL AUTHC	RIZATIONS PANE	nasis Intense E St
24-04-2	5 11:12:48 AM	USBSTOR\DISK&VEN_HP8	PROD_V165W8	&REV_8192\	AA34045800000046 (EJECT	TED)		les
24-04-2	5 11:12:47 AM	USB\VID_03F0&PID_5307\	AA34045B00000	0046 HP_V1	65W	GISINE		
24-04-2	5 11:12:47 AM	REMOVABLE STORAGE						
24-04-2	5 11:12:13 AM	USB\VID_03F0&PID_5307\	4A34045B00000	0046 USB				
24-04-2	5 11:12:10 AM	REMOVABLE STORAGE						
24-04-2					\AA34045B00000046 (EJECT			
24-04-2		USB\VID_03F0&PID_5307\.	AA34045B00000	0046 HP_V1	65Wst recent alert for a	anv machine a	and updates in real-t	ime. You may
24-04-2		REIVIOVABLE STORAGE						
24-04-2		USB\VID_03F0&PID_5307\	A34045800000	0046 USB <sub>V C</sub>	ed alerts (Highlighted in	n while) and D	rop them inside the	"Device ID"
24-04-2								
24-04-2				24-10 LU 24	Authorizing		$\times$	
24-04-2				0046 HP_V1	Edit authorization: custom name (o	optional)	ок	
24-04-2								
24-04-2			<u> </u>	líck auth			Cancel ore deta	ail in <u>16)</u>
24-04-2		LOCAL AUTHORIZATION #						
24-04-2							511561325	50
24-04-24				D_PRODUC	HP_V165W - Custom Name			
24-04-24		LOCAL AUTHORIZATION #	#2	ra outhor	izationa hu navina dau	iooo to right t	o laft or laft to right	
24-04-2					izations by moving dev	aces to right t	o leit on ert to right.	
24-04-2				5613250 VE	NDORCO_PRODUCTCODE			
24-04-2								
24-04-2				-	NDORCO_PRODUCTCODELE.	•		
24-04-2					678\4824451206115613250			
24-04-2		` =			CODE&REV_2.00\482445120	ю115613250 (EJ	ECTED)	
24-04-2				50 1325U VE	NDORCO_PRODUCTCODE			
24-04-2) 24-04-2)		KEYSTROKE INJECTION P						
24-04-2.	3 10:01:50 AM	REMOV. DRIVES: P CD:	P BLUETOUT	H:U WIFI	I: U K.I. PREVENT: ON MO	INITORING: UN		
Showing	g Drag-Drop auth	prization mode						
sh	iow more ways to a	uthorize						
	Show more							
		Device ID	o authorize	a specific	CUNEMPTIVES OF I <mark>VIO</mark> D	X	Name	
1 not se			Salasta	the Client	t PC from the netwo	SB SECTOR		not set
2 notse 3 notse								not set not set
4 not se					removable stora <mark>ge s</mark>			not set
5 not se			Instruc	t the ince	ertion of the MTP de			not set

• 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 reactivate 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

				GR	OUPS S	TATUS	
ısb	cd	bt	wf	<b>k</b> . i.	mon	count	group name
U	U	U.	U	OFF	ON	2	Default
				ON	ON		Production
	Ρ			ON	OFF		Office
	Ch	ange	-		STOP		Enforce
					130		

#### **Group Status Panel**

#### 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:

Rename	Groups Build	l Groups	Change Groups Setting	s Auto Aut	horization Mode	Deploy Groups Aut	norizations
• PRODUC		• 3		O UNASSIGI	NED	O DEFAULT	
	the state of the		*ı)) ((r≖	((t)	<b>×</b> 10	ų	
	USB Removable Drives	CD/DVD	Bluetooth/iIrDA	Wi-Fi	Keystroke	Monitoring	Save setti
	Protect	Protect	Protect	Protect	• On	• On	Save setti
		Unprotect	Unprotect	Unprotect	Off	• Off	

- 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.*

### $\circ~$ 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 de elevated to each group.

	- 14 K		GROUP ACTION	IS PANEL				x
	Build Groups	Rename Groups	Automatic Authorizations Mode	Deploy Protection Settings	Deploy Authorizations			
Production	Office				4			
09514/HD_16660.002613687146821177556 03704/HD_50744.3644500000046 FFFH4/HD_5574/H2426110330525970 02704/HD_55307 07164/HD_655.00703476.025800513 06534/HD_0744000000061558 07164/HD_07054072321937488687 FFFH4/HD_9574/H2426113303052870 09514/HD_1666-002618687146821177558								epand veploy
Explorit To view defails, revoke au	thencesonia or cot exten	nan peseyara)				France Deploy (	lo espiri	27
		PRODUC	TION GROUP AUT	THORIZATIONS				
withorize a specific device (VID/PID/ID ISBV/ID_035536/HD_1664/00261560714 /31/20203031173AM omments> trame: ASI-NT1D-64-HP		c			×		×	
whonze a specific device (VID/PID/ID SB/VID_03P06/PD_5307-VA3-40458000 /31/2020 8-3 1:20 AM omments-> home: ASI-NT 10-64-HP	match): 00046	•			×		×	
uthorize a specific device (MD/PD//D SB/v1D_FFFF&PD_5678/HEADER1130 /31/3008631:23 AM omments-> home: ASI-NT1D-68-HP	match): 330538570	•			×		×	
wthorate a specific device twit/PiD/I0 SB(vID_2717&PID_FF40\ddfd9y51 /31/2020 834039 AM amments-> home: SURFACEPRO-1064		•			×		×	
wthorge by VID/PID eatch: ISB/VID_03F06/PID_5307 /31/2020 8xH136 AM omments-> home: ASI-NT10-64-HP		•			×		×	page 2
wthoraze a specific dewice (VID/PID/ID ISB/VID_0118.8PID_0690;070347ED25E /31/2020 Bx82(53.AM simments-> hame: ASI-NT10-64-HP	10/06/11	•			×		×	hold - r
uthorize a specific device (VID/PD/ID ISB/VID_05E3.aRID_074940000000153 /31/2000 8:43:15 AM primenta-> home: ASI-NE10-64-HP					*		×	
withorize a specific device (MD/PiD/RD (SB/VID_0718-049D_070C/07072C18974 (31/2020 8:44:29 AM unitients > frome: ASI-NT10-64 HP	Matchil 66F67	<			×		×	
withorize a specific device (MD/PD//D SB/VID_FFFF&PID_5678/HEADER1130 /31/2000 8:46:04 AM omments = home: ASENT 10-64-HP	match] 330526570	•			×		×	
whorize a specific device [VID/PID/IG	mətch): 682117785838F						set	

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.

	USB-LOCK-RP v.12.988	
email alerts :	auto report: << OFF >> ON columns back adjust cef log to siem: << OFF >>	monitoring: << open panel >>
	NOV 26 2021 02-18 PM DESKTOP-EG/T095 JAVIE (M10/ 64) USB\VID_0718&PD_070C\07072C1897488F87 USB - AUTHORIZATION SET(AA)	ALERTS

Network Alerts Log: Shows alerts for all clients.

showing: 153	39 records				Network Alerts Log:	X
date	time	machine	user	os   bit	message	action
2024-04-03	10:26:39 AM	DESKTOP-EGJT09S	JAVIE	W10/64	US8\VID_05AC&PID_12A8&MI_00\6&2A80105C&0&0000 APPLE IPHONE	AUTHORIZED
2024-04-03	10:26:21 AM	DESKTOP-EGJT09S		W10/64	USB\VID_05AC&PID_12A8&MI_00\6&2A80105C&0&0000 APPLE IPHOINE	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	US8\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	US8\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\AA34045B00000046 HP_V165W	AUTHORIZED
2024-04-03	10:11:18 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/64	USB\VID_03F0&PID_5307\AA34045B00000046 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\AA34045B00000046	EJECTED
2024-04-03	10:11:06 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/64	USB\VID_03F0&PID_5307\AA34045B00000046 HP_V165W	BLOCKED
2024-04-03	10:10:55 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/64	US8\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\AA34045B00000046	EJECTED

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

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

### Client History Log:

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

menu	< >	USB-LOCK-RP v.12.988		< > -
11/25/21	2:10:59PM	US8/VID_03F0&PID_5307\AA34045800000046 US8	ALLOWED	CLIENT*
11/25/21	2:09:19PM	REMOV, DRIVES: U CD: U BLUETOOTH: U WIFI: U K.I. PREVENT: OFF MONITORING: ON	ENFORCED	CONTROL*
	2:08:06PM	USB\VID_03F0&PID_5307\AA34045B00000046 USB	ALLOWED	CLIENT*
	2:03:02PM	KEYSTROKE INJECTION PREVENTION	TURNED OFF	CLIENT*
	2:03:00PM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIFI: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
	2:01:43PM	REMOV. DRIVES: P CD: P BLUETOOTH: P WIFI: U K.I. PREVENT: ON MONITORING: ON	ENFORCED	CONTROL*
	2:00:38PM	KEYSTROKE INJECTION PREVENTION	TURNED ON	CLIENT*
	2:00:36PM	REMOV. DRIVES: P CD: P BLUETOOTH: P WIFI: U K.I. PREVENT: ON MONITORING: ON	ENFORCED	CONTROL*
	9:15:55AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIFI: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
	8:52:22AM	REMOV. DRIVES: P CD: P BLUETOOTH: U WIFI: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
11/24/21	8:52:17AM	REMOV. DRIVES: U CD: P BLUETOOTH: U WIFI: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
	8:52:12AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIFI: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
	1:13:15AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIFI: 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*
	1:13:08AM	CD DVD	PROTECTED	CONTROL*
	12:57:42AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIFI: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED	CONTROL*
	12:57:41AM	CD_DVD	PROTECTED	CONTROL*
11/24/21	12:48:44AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIFI: 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

8 Monitoring - fast view (1.)	email alerts													2 **
5 Monitorion - fast view (11)													1 panel ++ 5	
							-> incoming elects with							USB Monitoring - fast view i
												1		
	usb drives	cd-dvd.	bluetootti	in the second	elent.				machine	1	1 main	01000	the second second	SUNACLINO-105
	1				12.975				ASI-VM-90 ASI-VM-IT	ON	ON	PRODUCTION PRODUCTION		extracted
	ji ji										ON	ERODUCTION	100	MG_20161019_202304816.jpg 1.044.908
22- 1 (1 g (1	5				12.979 12.979	5. Termines in une		second lists a	ASI-VM-15 ASI-VM-54		ON	PRODUCTION PRODUCTION		estracted
	÷				12.979	incenties on the		S Spin Dires	ASI-VM-15	ON	ON	PRODUCTION		84G_20161117_101913353.jpg 811.724
	i e										ON	PRODUCTION	823	all, 224
	- E				12.971		GROUPS STATUS	_	ASI-WM-17 ASI-WM-18	ON: ON	ON	PRODUCTION	1141	MG-20160523-WA0002.prg
	5				12.975				ASI-VM-39	014	ON	PRODUCTION		56,212 estraited
	<b>P</b>				12.875	PPPB	ON ON 415	PRODUCTION	ASI/W-20		ON	PRODUCTION	100	IMG-20160617-WA0004.grg
	10 M				12.979				ASI-MM-21		ON	PRODUCTION	123	104,423
	<u>5</u>				12.979 12.979				451-VW-22 451-VM-23		ON ON	PRODUCTION PRODUCTION		extracted MIG-20161019-WA0002.apg
64-PF history.txt	÷				12,375				ASI-VM-23 ASI-VM-24	ON ON	- ON	PRODUCTION		128,862
	i i				12.975	1 1 1 1	OFF DEFF 0	DEFAULT	A51-VM-25		ON	PRODUCTION	1023	extracted IMG-20161019-WA00003app
td⊷ p_cefilog	<u>8</u>				12,979				A\$1-VM-25	ON: ON:	ON	PRODUCTION PRODUCTION	8.1	117.435
	5				12.979	-	Complete.	1	ASI-VM-25 ASI-VM-28	ON ON	ON: ON	PRODUCTION	100	
d A-MP_Local-Authorizations-	10 A								ASI-VM-20		ON	PRODUCTION	811	M4G-20170220-W40016.jpg 164,633
	. B										ON	PRODUCTION		estracted
	1 S				12.979 12.979				ASI-VM-31 ASI-VM-12	ON: ON:	ON ON	PRODUCTION PRODUCTION		MAG-20170305-WA0000.jpg
rd p-operation.pdf	i i				12,979				ASI-VM-33	ON .	ON	FRODUCTION	841	93,13
	P .										ON	PRODUCTION		MG-20170430-WA0000.jpg
	1 C				12.979				A\$1-VM-35	ON	ON	PRODUCTION		361,093
	5				12.979				A51-VM-36 A51-VM-37	ON	ON	PRODUCTION	1012	ING-20170519-WA0007.arg
	a a				12.979				A\$1/VM-38		ON	PRODUCTION		71,475
ed p-operation Copy.door	15 E										ON	PRODUCTION	841	
	5				12,979				ASI-944-40 ASE-944-41		ON	PRODUCTION PRODUCTION	1063 I	65,932
a diama di seconda di s	÷				12.979				451-194-42		ON	PRODUCTION		
					12.979						ON	PRODUCTION	1651	156,207
	- X										-	A	No. of Concession, name	
	<b>A</b>	8		<u> </u>								4		IMS-20171019-WA0009.jpg 71,001
					п	load uninted		reboot shutdows			n Al-limit			extracted
PRD-1064_Local-Authenzations-	a second						and a second sec							#4G-20171030-WA0052.jpg 95.631
	USB.													50.00
							والاستعداد		<b>(</b> **					estratted
	Autom		(AA) OFF				192100.1.982							BMG-20171106-WA0036.jpg 502-493
	and the second sec													
	1 - A													#MG-20180104-WA0308.grg 136.857
		Local Whitelet:												estracted
		USEVID_03104210					INTERSTERN WITH THE							M4G-20180118-WA0005.jpg 122.708
	9	rest pert -				11/23/21		NSCEIVER KE IWECTION PREVENTIK				BLOCKED TURNED 0		122,708 estraited
H-HF_control-changes-report.tat		not set				10/15/21		TOOTH TRANSCEIVER				BLOCKED		MG-20100118-WA0006.jpg
		nat set nat set												147,997
td rtrol_overview.ong	7					11/25/21		SSPORPED SSSTWAS404			E ANDALIZOUR	ALLOWED		84G-20180118-WA0008.pg
		ootset. ootset				10/25/21 15/25/21		DRIVES U CDI U BEU DIPOLIPID SIDTVA34041	JETOOTHEU WIFEU II ISB00000946 USB		- MUMILORIZ	4GLON ENFORCED ALLOWED		164,250
ed nbiol-aveniew.baip	10	notset.												#MG-20180201-WA0000.316
														401,750
														MG-20180201-WA0011.grg
														405,763

- 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

KEYSTROKE INJECTION PREVENTION - ON

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 X									
			HID (Human interface device)						
4/26/2024 2:04:20 PM Machine name: SUBPACEPRO-1064 Parkness: 192: 2016 105 Logged uker: JAVIE Manufacturer: Microsoft Corporation Models Surface Pro 4 Processors: Processors: Processors: Processors: Ame: Intel@(©.core(TM) 5-63000 CPU @ 2:40GHz Processors: Sumes: Intel@(O.core(TM) 5-6400 CPU @ 2:40GHz	Privite Name: USB Drive (D.) Device Type: USB Drive Device Patho Ud: VAAAMABOOOOOA6 Soor: 760 (G Free: 7.8) 68 Frie System: NTTS	Device Name: Chaon E400 series Printer Status: Offine Point Name: Fixe Status: Ready Status: Ready Device Name: Microsoft Print to PDF Status: Ready Device Name: Microsoft XPS Document Writer Status: Ready Device Name: Microsoft XPS Document Writer Status: Ready Device Name: OneNote 2013 Status: Ready Device Name: OneNote Tor Windows: 10 Status: Ready	Surface Dock Extender Microsoft Witchards Dock Extender Microsoft Witchards Pills: CooPOA Servision Status Servision Device Bus Speech full Device Bus Speech f						
Installed Software	Running Processes	Network Adapters	Surface Type Cover Microsoft VID: DoXSE FID: 0x07E8						
		<ul> <li>Wi-fi Status: Disconnected Mureill AVASTR Wireless-AC Network Controller Not connected MAC Address: 88 31 65 32:06-92 Effentel Bonnet Disconnected Surface Ethernet Adoptor Pr Address 102:168,106 Submet Music 255:352:50 Assigned by Dic/Pi Inv6 Enabled Th-LINE, SAA2AC MAC Address: 80:68:68:68:60:6A</li> </ul>	<pre>Wardward with wardward wardwardwardwardwardwardwardwardwardward</pre>						

# 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.

DBE	Bluetooth
IX	Yes, I want to remotelly Restart that station
	Cancel



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.

uninstall

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

reload

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-m	ail alerts (sm	tp)	
1 Enter from email account:	email@server.com		
This is the email address o	riginating the alert		
2 Enter destination email account This is the email address w	email@server.com vere alerts will arrive.		
3 Enter mail server example: mail.yourcompar	<b>mail.server.com</b> nydomain.com or ip number		
Server requires authentication	SMTP port 25 SMTP port 587 SMTP port 465	TLS	
	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



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\/AA34045B00000046 USB - AUTHORIZED Jul 02 14:10:34 ASI-NT10-64-HP JAVIE (W10/ 64) USB\/VID\_03F0&PID\_5307\/AA34045B00000046 USB - BUCKED

# 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

bluetooth	wifi	client		CONTROL		machine s	k. i.	mon
Р	Р	12.979				DESKTOP-EGJT095	ON	ON
P	P	12.979	Reload	Groups	Extend View	ASI-VM-2	ON	ON
		12.979				ASI-VM-3	ON	ON
		12.979		1480		ASI-VM-4	ON	ON
		12,979	licenses in use		< <out list="">&gt;</out>	ASI-VM-5	ON	ON
		12.979				ASI-VM-6	ON	ON
		12.979	ZAHA4444			ASI-VM-7	ON	ON
		12,979	SURFACEPRO-1064			ASI-VM-8	ON	ON
		12,979	DESKTOP-2PKJP0S			ASI-VM-9	ON	ON
		12.979	ANDO7777			ASI-VM-10	ON	ON
		12.979	Click to red	cover the license (t	his will also delete the log)	I-VM-11	ON	ON
		12,979				-VM-12	ON	ON
		12,979	Ca	ncel		-VM-13	ON	ON
		12.979				ASI-VM-14	ON	ON
		12.979				ASI-VM-15	ON	ON
		10.000				A 177 A 179 A 171		

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:

	Control Password Reports Help Licenced to: Advan	ced Systems Internatio	nal cac (USB I	< <ok>&gt; ts arrive here ack RP 100)</ok>		uthorizations : << op		> V < <not set="">&gt; V</not>
remova				K RP	version	machine IP	machine name	
P	P	P	P U	in 7	9.8 9.8	192.168.0.19 192.168.0.20	ASI-NT10-32-CW ASI-NT10-64-CL	
U	U	U	U	out	9.8	192.168.0.17	ASI-NT51-32-CW	
P	p	P	P	licenses in use 7	9.8	192,168.0,21	ASI-NT61-32-CW	-
				licensed capacity 100	9.8	192.168.0.14	ASI-NT61-64-CL	
					9.8	192.168.0.12	ASI-NT61-64-CW	
					9.8	127.0.0.1	ASI-NT63-64-CL	
removable driv	es cd - dvd	bluetooth - irda	wfi	ASI-NT51-32-CW 192.168.0.17	HISTOR	RY SYS-INF	SHT RB1	UNI

Enter the old password. Enter the new password.

Re-Type the new password.

Type old password		
Type new password Re-Type new password		
Can <u>c</u> el	C <u>h</u> ange Passw	ord

## 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 Conf	iguration ×
Question:	Answer: Change:
- Run in system-mode when admin-mode is closed ?	YES to no
- Persist after the server machine system reboots ?	YES to no
- Auto-Enforce group settings in system-mode ?	YES to no
- Service view - Service name : usblockrpsvc Function : To auto-start the control in system-mode when ar Service status : Installed State: Running	

#### Licenses recovery:

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

Machine name         Last time seen.           ASI0-151         2024-04-23 06:11:49           ASI0-152         2024-04-23 06:11:49           DESKTOP-ASI104         2024-04-23 06:11:49           DESKTOP-ASI107         2024-04-23 06:11:49           DESKTOP-ASI146         2024-04-23 06:11:49           DESKTOP-ASI82         2024-04-23 06:11:49           DESKTOP-ASI82         2024-04-23 06:11:49           DESKTOP-ASI86         2024-04-23 06:11:49           SURFACEPRO-ASI43         2024-04-23 06:11:49           SURFACEPRO-ASI43         2024-04-23 06:11:49           SURFACEPRO-ASI82         2024-04-22 06:11:49           SURFACEPRO-ASI82         2024-04-22 10:09:59           DESKTOP-ASI23         2024-04-22 21:09:59           DESKTOP-ASI54         2024-04-22 21:09:59           DESKTOP-ASI86         2024-04-22 21:09:59           DESKTOP-ASI89         2024-04-22 21:09:59           DESKTOP-ASI89         2024-04-22 21:09:59           DESKTOP-ASI89         2024-04-22 21:09:59



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.

- List shows machines current	
	ly not logged to the control
- Select machines from the list (multi-select allowed)	
DESKTOP-ASI82 DESKTOP-ASI86 SURFACEPRO-ASI87	
2 - Click to Ping selected (Sends 1 ICMP packet and waits 800	) milliseconds for response) PING
	SURFACEPRO-ASI82 SURFACEPRO-ASI68 SURFACEPRO-ASI48 SURFACEPRO-ASI47
	SURFACEPRO-ASI43 DESKTOP-ASI89 DESKTOP-ASI66 DESKTOP-ASI54 DESKTOP-ASI46 DESKTOP-ASI45 DESKTOP-ASI23 DESKTOP-ASI146 DESKTOP-ASI107 DESKTOP-ASI104 ASI0-152

### On-premises Clients Update function:

Clients Update function panel: Allows to massively update client's version from controlside. 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.

Clients Update	X
Your control delivery included a client component for on-premises client update. You can use this update method as an alternative to client reinstall or msi redeployment.	
Number of machines were usb lock rp client (ssrvc service) can be updated. 0 Start Update	
Progress O Stop Update	
Leave this panel open while the update takes place. (You may go to Admin Mode)	

# 33) Technical Support



### 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...