USB-LOCK-RP
By Advanced Systems International

USB-LOCK-RP
OPERATING MANUAL

Updated: September 27th, 2023

Table of Contents:

1) Other Resources

Product Page

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

Video Tutorials page

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

Datasheet

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

Installation Instructions

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

Client MSI Mass Deployment instructions (GPO)

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

Operating Manual (This document, online)

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

Licensing Cost (Published Price list)

- https://www.usb-lock-rp.com/usb_lock_pricing.pdf

Latest version highlights

- 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.

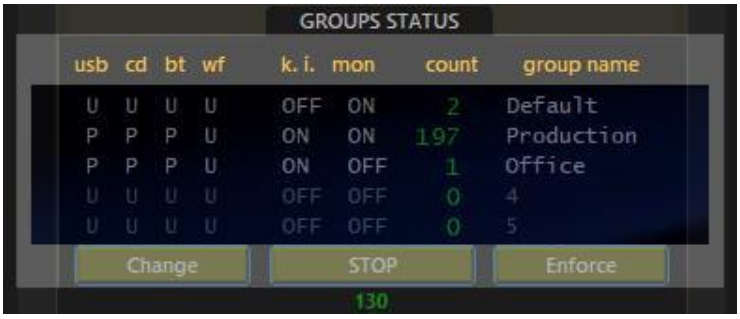
Ssrvc.exe is located at client stations: ProgramFiles(86) \ssrvc\ssrvc.exe

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 = *usblockrp.exe (server -side)*

Group Status

Group Status Panel



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)

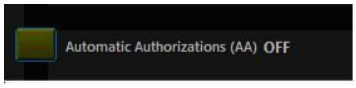
The Selected machine panel shows:

Sector Protected: 

Sector Unprotected: 

Monitoring 

Automatic Authorizations Mode (ON/ 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) Authorized Device ID Acquirement

(Getting ID from device to be authorized)

Manual-auto detection

Acquire from devices connected to specific machines

Note: Requires pressing authorize at Control-side.

Automatically (AA Mode) (recommended)

Acquired from devices connected to specific machines.(no Control-side action required)
Note: When AA is active on a machine, devices are authorized while normally used on the machine.

Acquire from devices connected to machines belonging to a Group. (no Control-side action required)

When AA is active on a Group, devices are authorized as they are normally used on machines belonging to the group.

8) Authorized Device IDs List (Per machine)

(Per machine authorized list shown below)

The machine authorized ID list populates:

Automatically when AA is Active

By pressing Authorize at Control-side while a device is connected at client. (Or at the server)

By typing a Device ID manually

By Dragging and dropping a most recent alert containing an ID to the List.

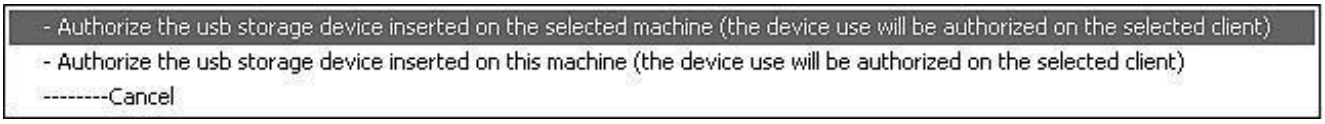
NOTE: A device ID showing in the list means that device is effectively authorized to be used on the machine. (No further action required)

9) Authorize Specific Devices (Per Machine)

To authorize a specific USB drives or Mobile phones on a specific machine:

Select the Client PC from the network list. Unprotect removable storage sector.

Instruct the insertion of the MTP device, or USB removable drive at client PC. Press Authorize.



Select the first option

Protect Removable drives sector to block unauthorized devices.

10) 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.

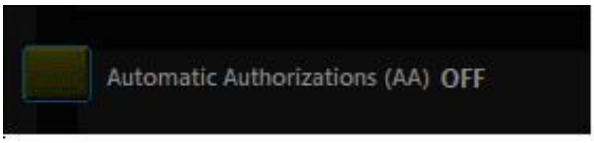
If a client system is disconnected from the Control while AA is active, AA deactivates automatically and protection becomes effective. When the client reconnects AA will re-activate automatically.

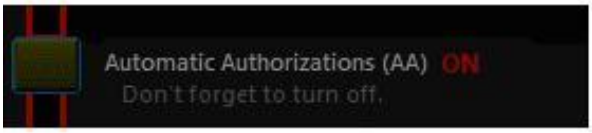
If the Control is closed AA deactivates in ALL clients and protection becomes effective.

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

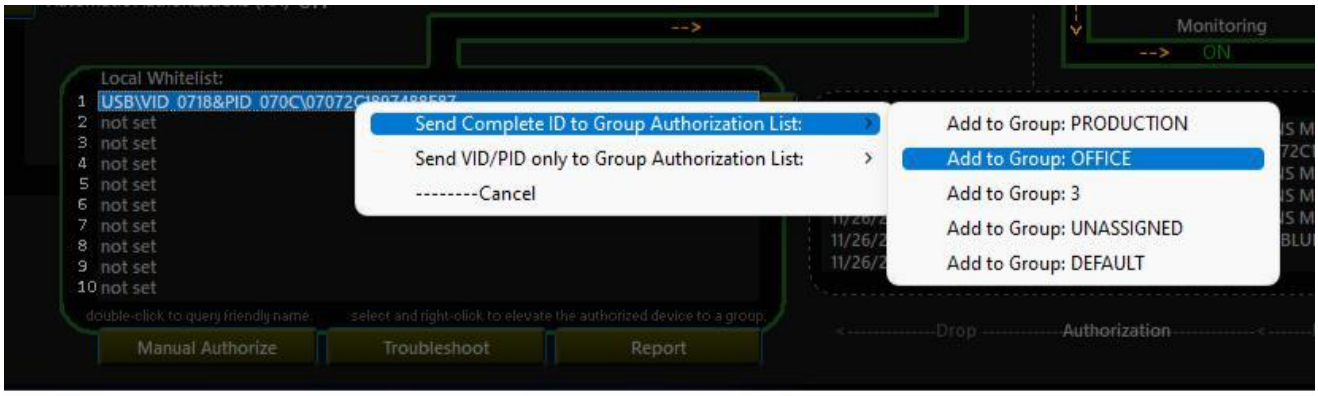
11) Automatic Authorizations Mode to specific Machines

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





12) Elevating authorized IDs to Groups

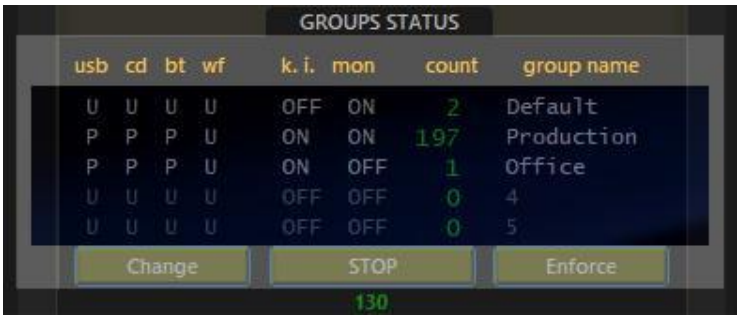


To elevate an ID to a group authorized ID list. Click on the id and select the Group from the popup menu.

Note: This is not required if using AA Mode at group level. (But is always available to complement whitelisting) Note: Once IDs are added to a Group Authorizations list they need to be deployed from Group Actions Panel.

13) Managing Groups

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:**

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

14) Other Group Actions

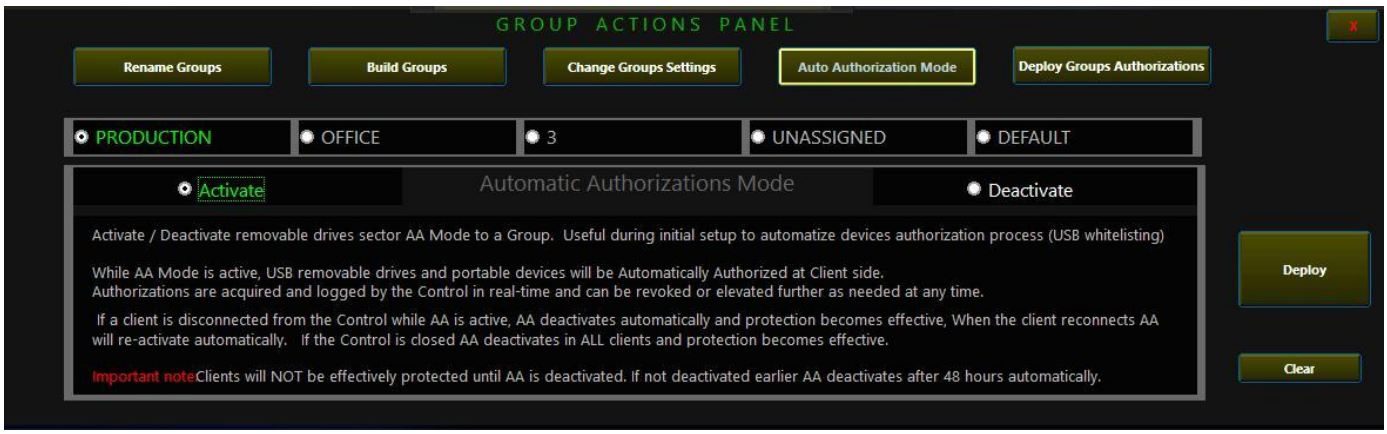
To access the Group Action panel press on the Green button.

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*

15) Automatic Authorizations Mode to Groups

(Activate/Deactivate AA Mode at Group level)

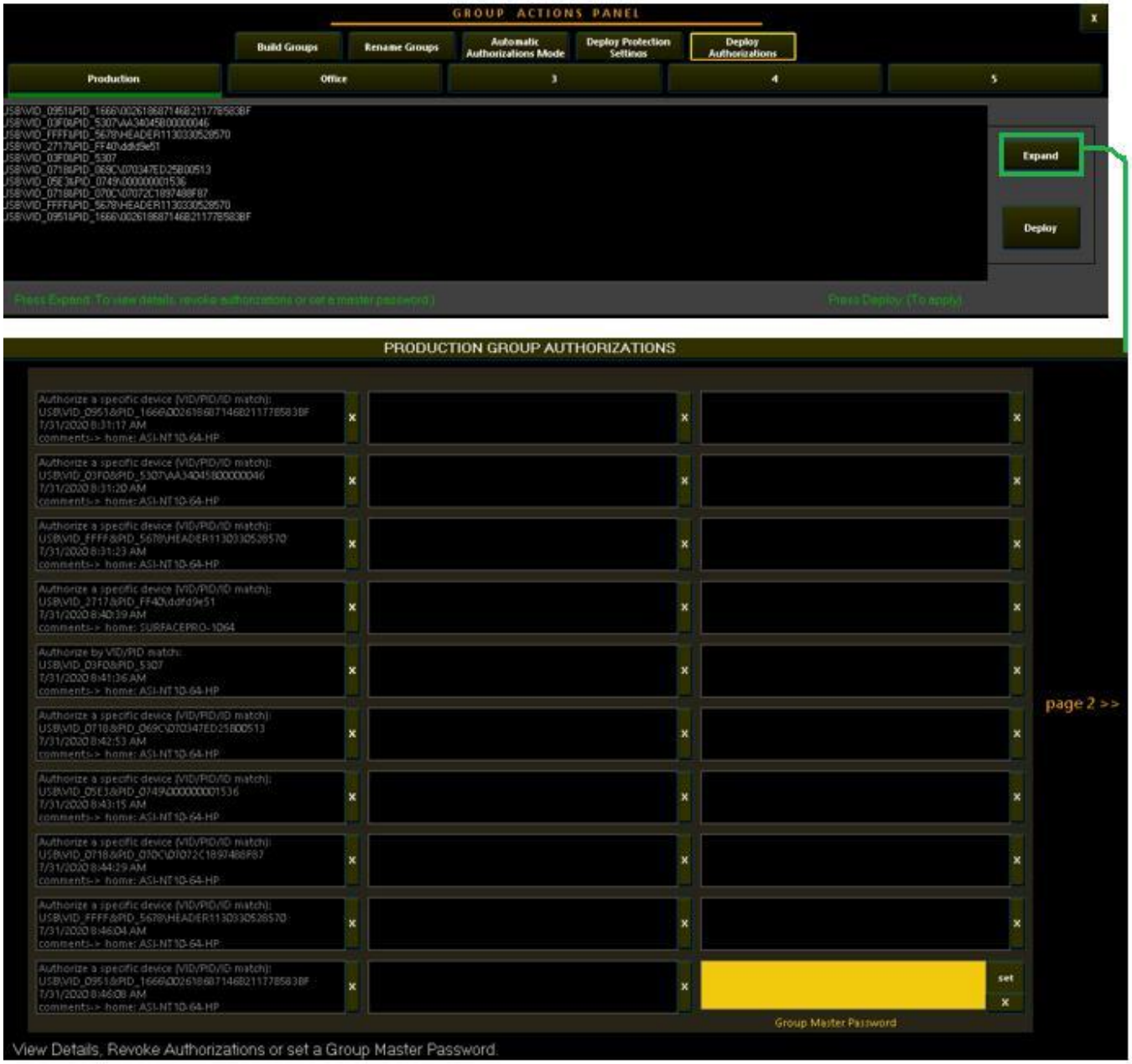


1) Select a Group
2) Select Activate or Deactivate.
3) Press Deploy

16) Deploying Authorizations to Groups

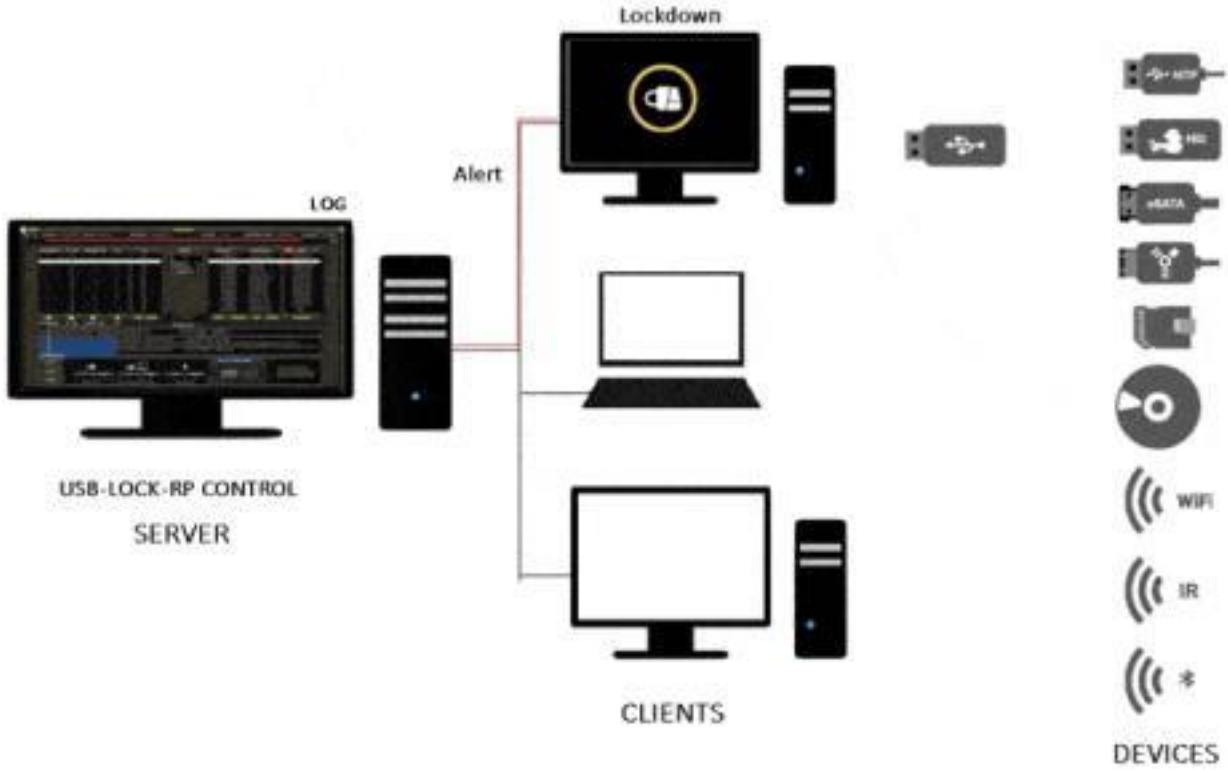
Note: When a new device ID is elevated to the Group authorizations panel The Group Actions Button will be underlined in Orange Signaling a new device was added and needs to be deployed.

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



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

17) 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:

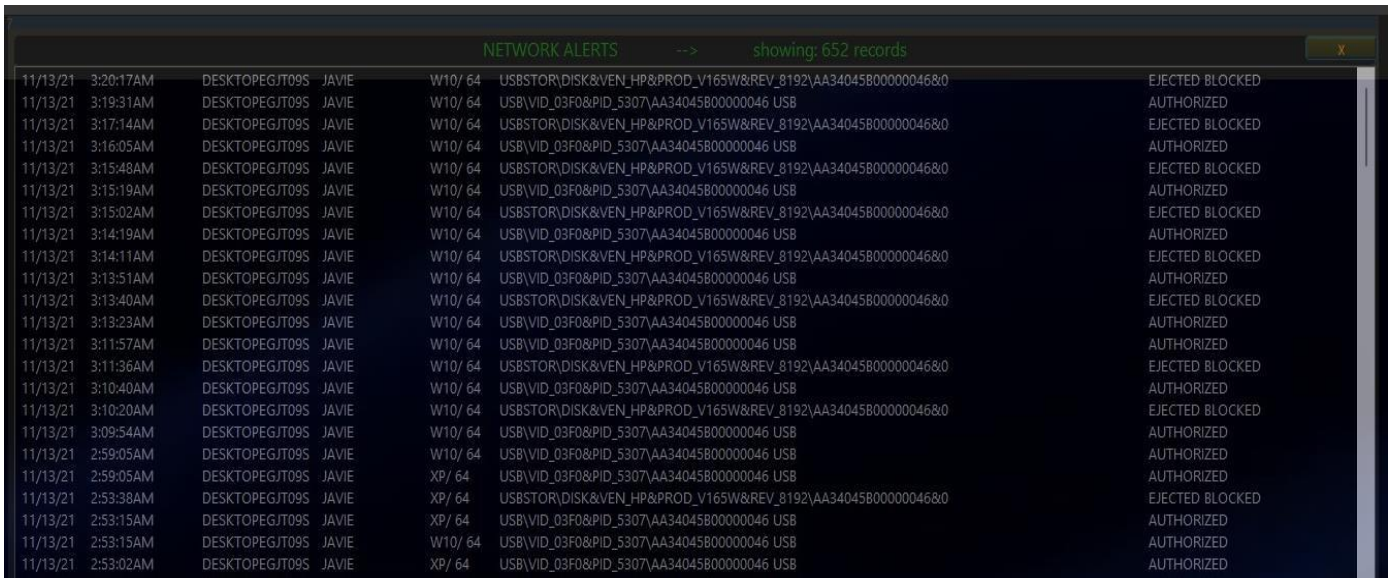
The unauthorized device is removed. (Client-side)
The master password is used. (Client-side.)
The sector is unprotected. (Control-side.)
The device is authorized. (Control-side.)

18) 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.

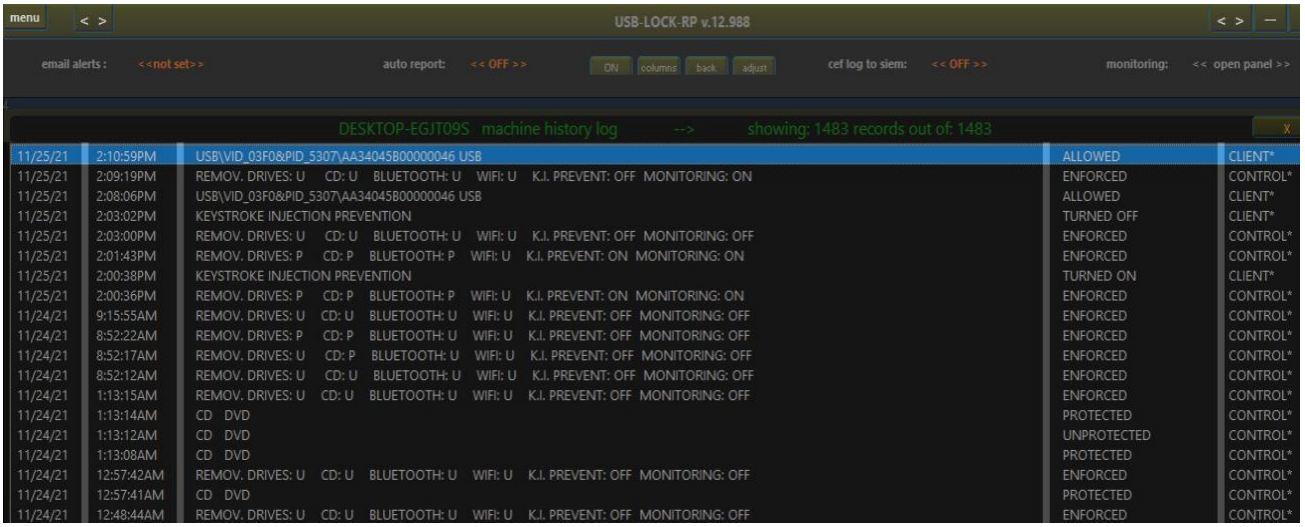
Note: Automatically Logs: allowed, blocked or authorized insertion alerts in real-time.

Network Alerts Log: Shows alerts for all clients.



Client History Log:

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



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

19) 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.

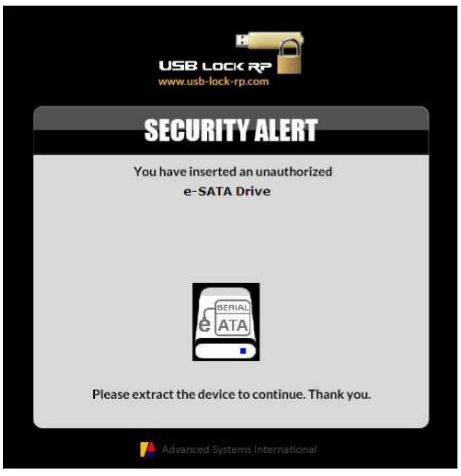
The Password as well as all critical program setting and IDs are stored encrypted (only readable within the Control interface)

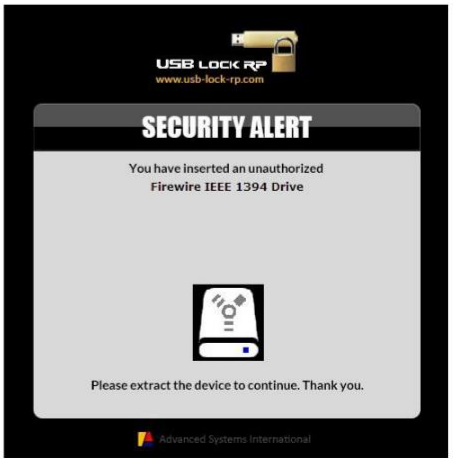
From the Control: The master password can be deployed to Groups of machines from the Groups authorization panel. ***See 16 (Deploying Authorizations to Groups)***

20) Alert Screens (Client-side)

Full screen alerts (Extend to all monitors)

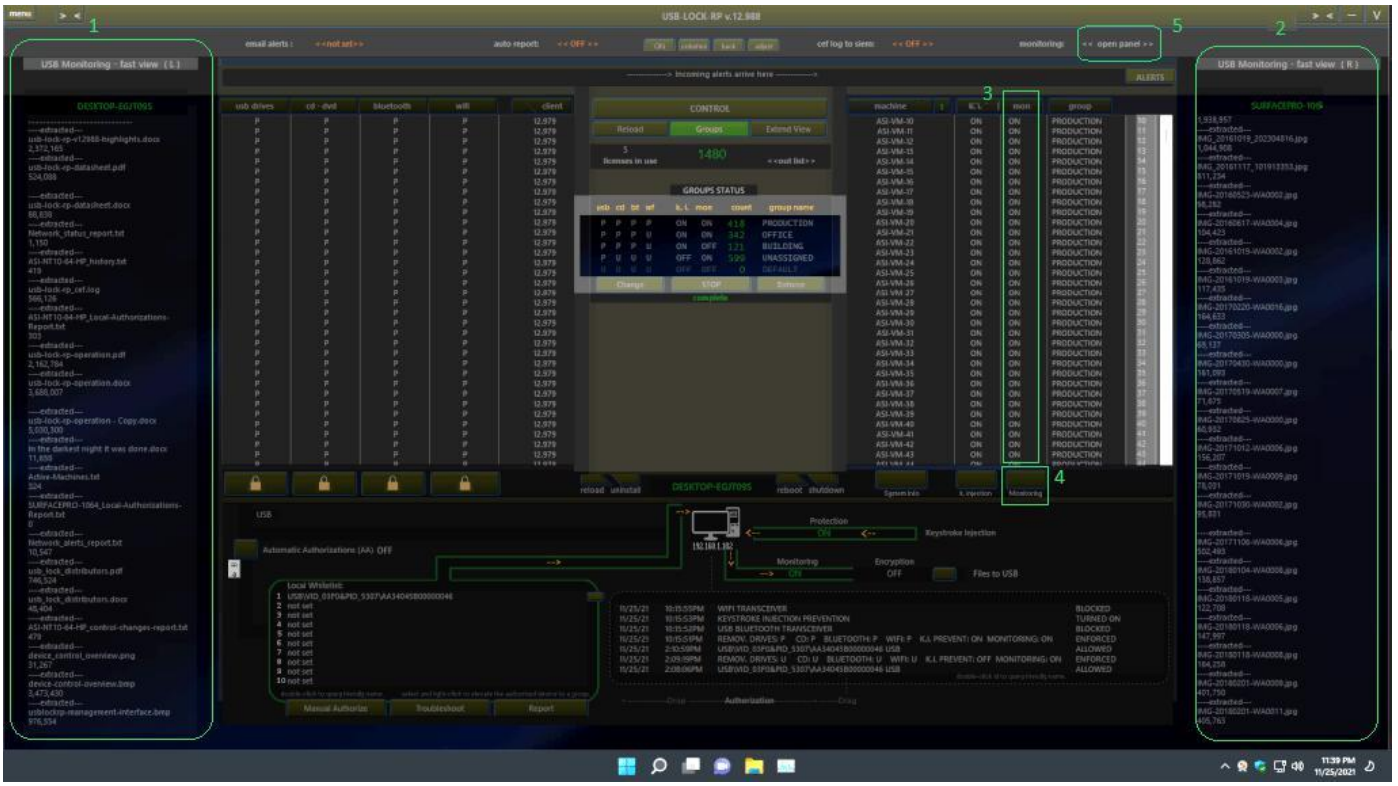
The following alerts show at clients depending on the blocked device type.





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

21) Files to USB Monitoring

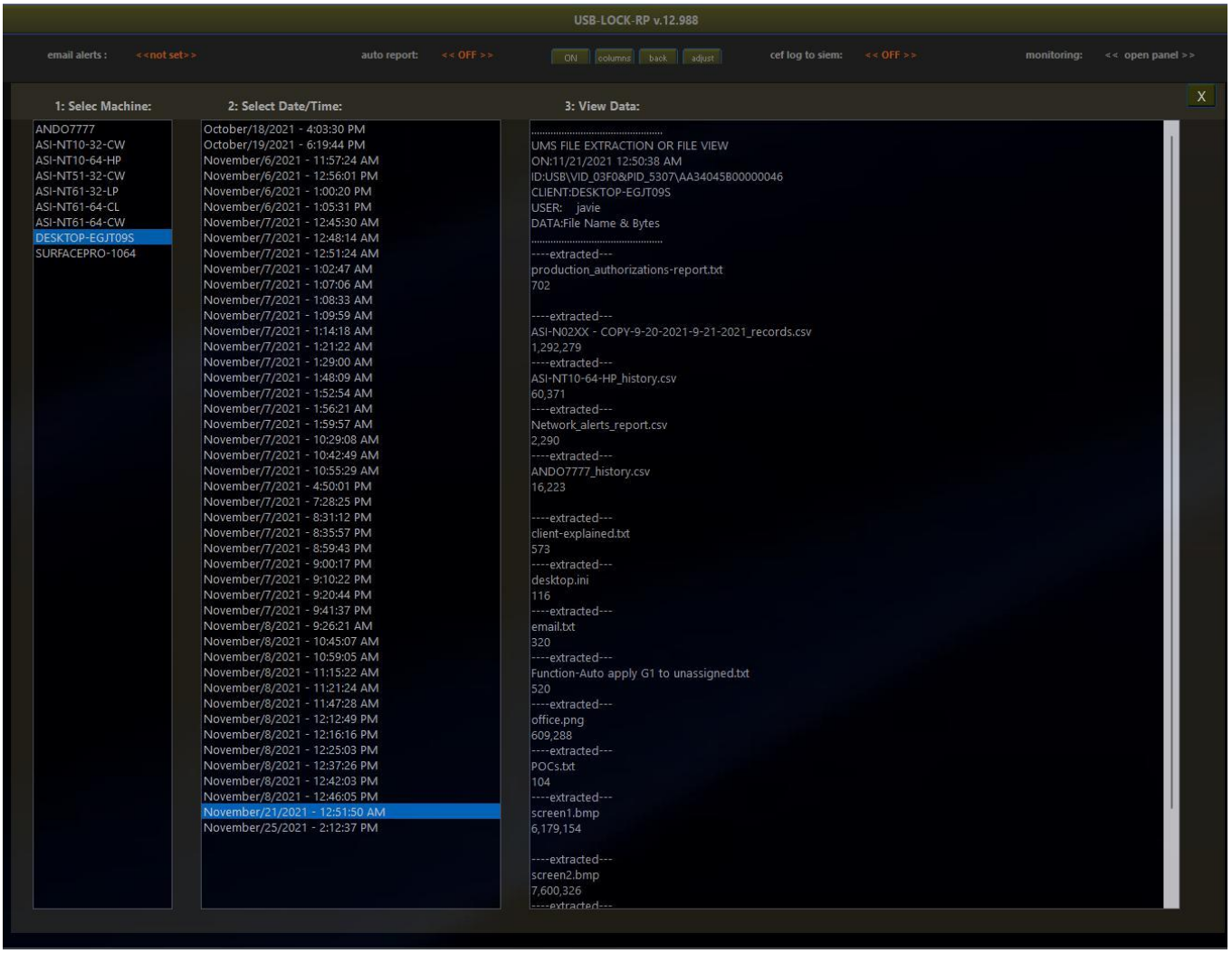


1) Monitoring Left Fast view Panel
2) Monitoring Right Fast view Panel
3) Monitoring Status
4) Turn Monitoring ON or OFF
5) Open Main Monitoring Panel

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.



22) Thumb drives Encryption

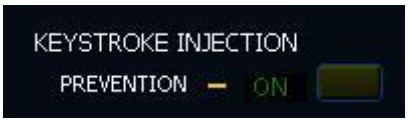
Forcing automatic Encryption to authorized drives, this function can also be turned ON or OFF with just one click. (USB Monitoring needs to be activated for Encryption to be set). When USB Encryption is active all files transferred from the endpoint computer to authorized USB flash drives are automatically 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.

23) Protection against keystroke injection attacks

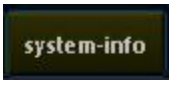


Included in the removable drives sector is protection against badUSB device e.g. USB Rubber Ducky, this type of device is extremely dangerous as its firmware has been modified to impersonate Human interface devices (HID) such as keyboards and are capable of on the go inflicting keystroke injection attacks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

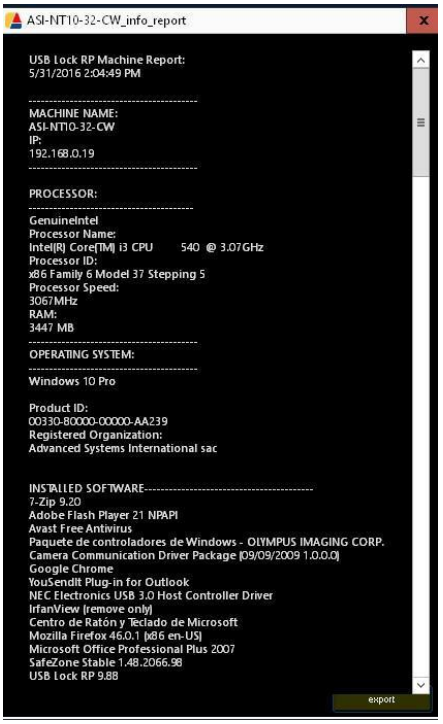
You may exclude the connected keyboards from analysis on the event that analysis is obtrusive. In cases laptops/tablets of detachable keyboards, smart pens or docking stations. But normally no action is required.

24) System Information function (Client-machine)



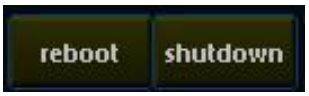
Queries in real time valuable information on any client machine:

- Processor and memory.
- Operating system
- Installed software
- Windows updates and patches
- Running processes



Select the Client PC from the network list.
Press on the system-info button.

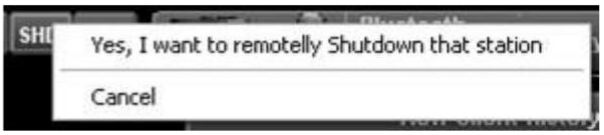
25) Reboot & Restart Function (Client-Computer)



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.

26) 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.

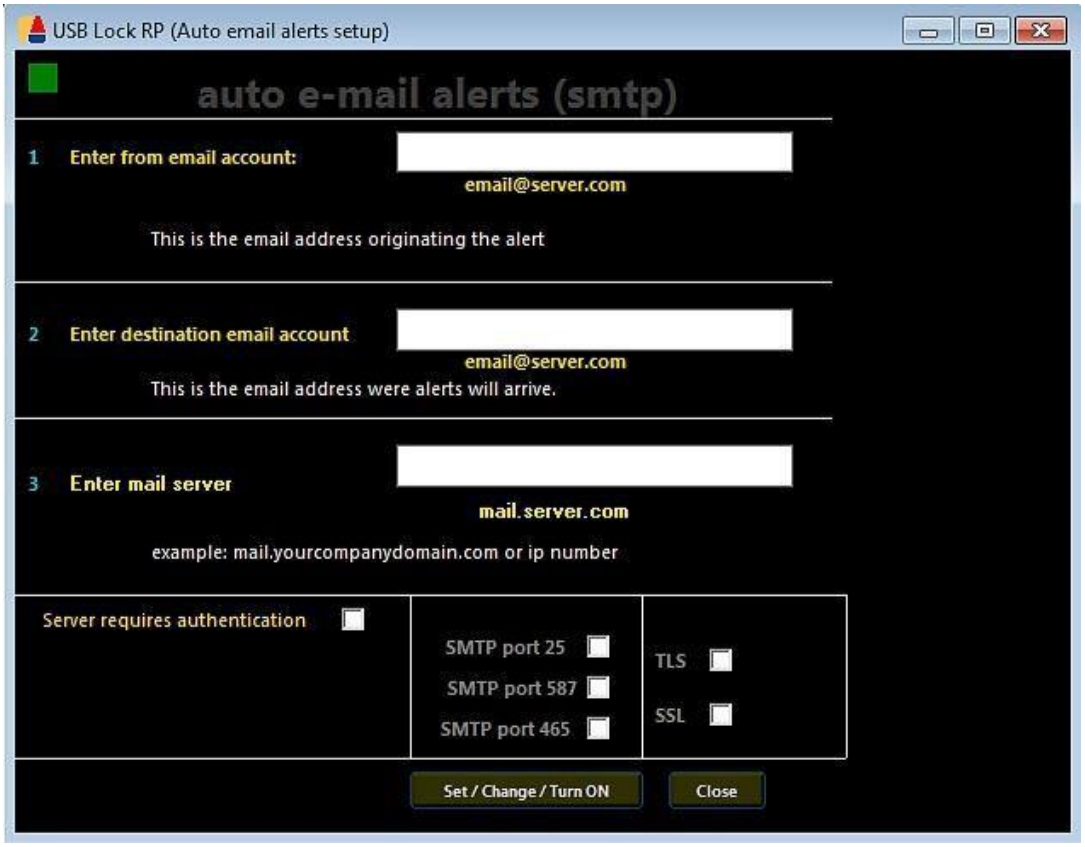
27) Auto-protect Function

(No longer available, Replaced by auto-enforced function)

28) Auto-Email Alerts function

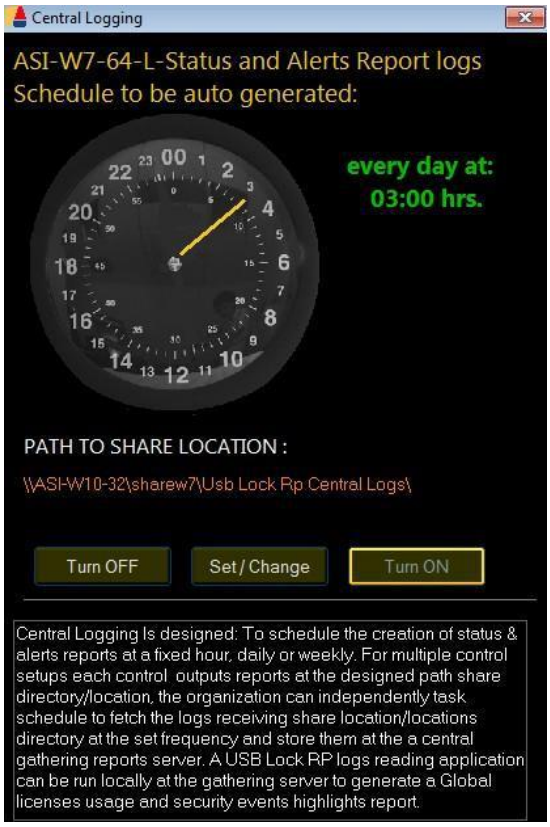
Automatically send **ALL** incoming alerts arriving to the Control to an email address of your choice within your domain (to be used as centralized alternative logs repository)

Automatic after easy setup
Allows SSL / TLS
All incoming alerts logged to the Control are sent.



29) 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.

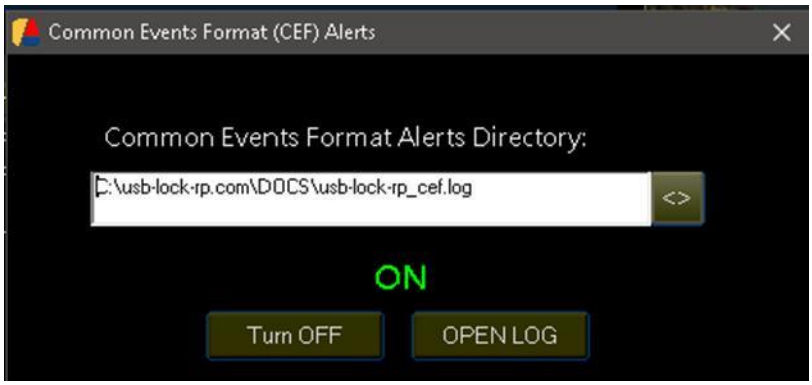


30) CEF Logs (SIEM Interoperability)

(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\\AA34045B00000046 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\\AA34045B00000046 USB - BLOCKED

31) Compact Mode

To enter compact mode press V at the right top corner

The control recommended operation is always ON (Normal mode or Compact mode). If you wish to close the program then you will press the right-top "X" Button at the password window.

To access the Control back from Compact Mode you will need to re-enter the password.

> Note: The password is remembered for 5 minutes after entering Compact Mode so you don't have to re-enter the password if you are just switching modes).

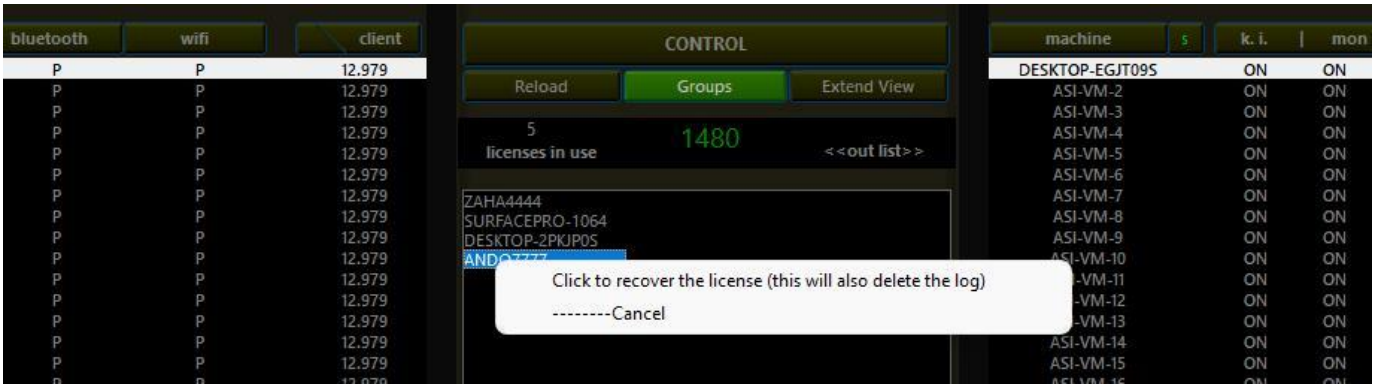
In: reports log in clients

Out: reports not logged clients

A: will show alert incoming. (Blocked is blue light and orange is approved or authorized.)

FT: Means File transfer taking place. (monitoring)

32) 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.

33) 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.

34) Closing USB-Lock-RP Control

To close USB-Lock-RP Control Press the X on the top Right corner of the password window.

Note:

To access the password window go to Compact mode and click the compact mode window.

The recommended Control operation is always ON.

35) 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.

36) 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...