USB LOCK RP
OPERATING MANUAL

I N DE X

WELCOME 03

VIDEOS LINKS 04

INSTALLATION INSTRUCTIONS 05

1. **Step 1**: Control Installation (Should be Installed First) 05
2. **Step 2**: Start the "Control" 05
3. **Step 3**: Clients Installation 06
   - Manual Client Installation 06
   - Clients Mass silent deployment Installation (MSI Pack) 06

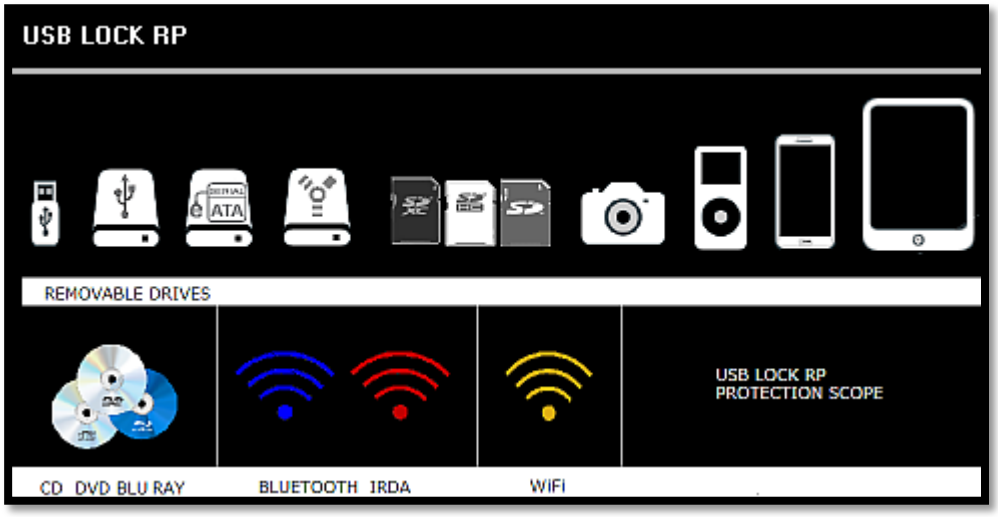
OPERATE ADMINISTRATIVE CONTROL 08

1. Start Administrative Control 08
2. Control Main Panel 09
3. Run Compact Mode 10
4. Full Screen Mode 11
5. Logged PCs 12
6. Fast PC Look-Up 12
7. Control Passwords 13
8. Alert Visor and Alerts Access Arrow 14
9. Network Status Panel and single control setups reporting 14
10. Real-time alerts reporting 16
11. Scalability and multiple control setups reporting 17
12. Protection Sectors 19
13. Auto-protect 20
14. Client Level USB Removable Drives Authorizations 21
15. Network Authorizations 23
16. Master Password Functionality 25
17. MTP or More USB Removable Drives Authorizations 26
18. E-SATA Authorization 26
19. Portable Protection 27
   a) Force Encryption 28
   b) Portable Protector 29
   c) Portable Protector Operation (Operates only within the authorized USB DRIVE) 29
   d) Drag and Drop Functionality 29
20. Files to USB monitoring 30
21. Administrative Command Tabs 31
   a) Clients Protection History: Button 31
   b) System Information Button 32
   c) Reboot Button 32
   d) Shutdown Button 32
   e) Uninstall Button 32
22. Security Alerts Screens 33
23. Personalization 34

WELCOME

WELCOME TO USB LOCK RP STRAIGHTFORWARD REAL - TIME NETWORK ENDPOINT SECURITY

- Receive devices connection alerts. (logs are automatically recorded, no action required)
- Authorize specific USB Drives, MTP protocol portable devices, and e-SATA super speed (up to 10 specific devices can be authorized per clients workstation + 60 local authorizations can be elevated to network level status allowing this devices to operate on any workstation in the network.
- Protect your organizations systems and data from the unauthorized use of USB removable drives-Portable flash memory devices – MTP protocol portable devices – Digital audio players including MP3, MP4 players and Ipods – External hard drives including e-SATA & Firewire Adapters bridging between standard flash memory cards and USB connection – Storage Capable Digital Cameras – Card readers: CF, SD, SDMicro, MMC, XD – PDA, Hand-held computers, smart phones – CDS, DVDS, BlueRay – IrDa and usb Bluetooth, Transceivers & WiFi. Protection changes are enforced in real-time (no need for restart for changes to take effect)
- Receive records of files transferred to usb removable drives (operation is automatic). Send alerts in real-time to an email account within your domain as a second level of control. (Automatic after easy setup)– (SSL TLS capable)
- Protect the information inside authorized usb drives (includes centralized password storage and auto encryption.



- **Supported Operating Systems:** Windows 10, Windows Server 2012 R2, Windows Server 2012, Embedded POSReady 2009, WES 7, WES 8, Windows 8.1, Windows 8, Windows 7, Windows 2000, Windows Server 2008 R2, Windows Vista, Windows Server 2003, Windows XP, and Windows 2K, VM Ware Ready. (32 or 64 bit). Endpoint data security for LAN, WAN or WLAN.
- Also capable of operating on workgroups or under dynamic IP configurations.
- Also capable of controlling clients outside your Local network.
- Effective even if clients are disconnected from the network or id the control is shutdown.
- Control machine does not need to be a server (any supported system will work fine)
- Scalable.

VIDEO LINKS

1. CEO INTRODUCTION

https://vimeo.com/networksecurity/usb_lock-rp_video1

2. ABOUT:
   ALERTS SHOWN AT CLIENTS

https://vimeo.com/networksecurity/usb_lock_rp_video2

3. ABOUT:
   NETWORK LIST – INCOMMING ALERTS VISOR – RECENT ALERTS PANEL - HISTORY PANEL – CENTRAL LOGGING – AUTOEMAIL ALERTS -

https://vimeo.com/networksecurity/usb_lock_rp_video3

4. ABOUT:
   LOCAL AND NETWORK WIDE AUTORIZATHIONS

https://vimeo.com/networksecurity/usb_lock_rp_video4

5. ABOUT:
   STATUS REPORT – CENTRAL LOGGING (RECAP) – DEVICES HARDWARD ID – MASTER PASSWORD – FILES USB MONITORING – GET SUPPORT - AUTOPROTECT

https://vimeo.com/networksecurity/usb_lock_rp_video5

INSTALLATION INSTRUCTIONS

"Control" Installation:

Install with administrative privileges on the PC or Server from where you will manage the security.

1. Execute the file "setup_control.exe"

2. Optional- Recommended: At prompt, Enter the port to use:

NOTE

If you leave blank then port 3100 is used.
If you leave blank at the control installation make sure you also leave blank when installing clients.
If you set a port number then use the same port when installing clients.

3. You may leave selected the option to create a quick launch icon on the windows quick start bar.

Start the "Control":

1. Click on: Windows Start Menu - Programs - USB Lock RP - Start USB Lock RP

2. Enter password and click OK.

NOTE

USB Lock RP Control is UAC aware and will require administrative privileges to be started.

You should have received your costume default password with your program delivery. (Password is case sensitive)

3. When starting for the first time the program will prompt to installed clients. The main interface will show the IP Number of the control. This IP should be used while installing clients.

Important:

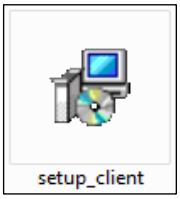
Write down the IP address as it will be required during client's installation. You could also use the Control Machine Name.

"Client's" Installation:

Manual Client Installation: Recommended for reviewing the program's functionality when you received it (prior to mass deployment), or for smalls networks installations, or for testing the demo posted on-line.

The Client Installer will require administrative privileges to be installer.
The Client Installer should only be installed on stations within your organization network.

1. Execute the file "setup_client.exe" on the client PCs.



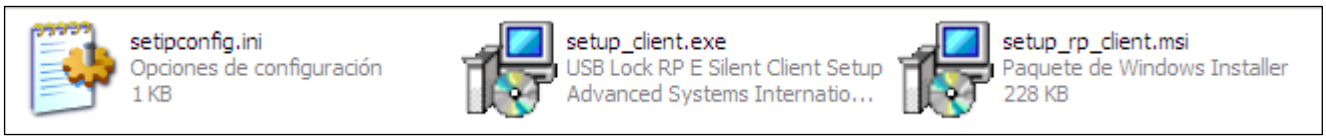
NOTE

- *You can store the file in a shared folder and run from each client.*
- *Or you could transfer the client installer on the USB.*
- *Or if during demo you could download the client on the test client stations.*

2. During the installation enter the "Control" IP address of the control machine noted during the control installation (Required).
3. Optional- Enter the port number you enter during control installation or also leave blank.
4. Continue to finalize the installation.

Important:
Once a client is installed it establishes connection with the control and will show on the control's network list.

Clients: Mass silent deployment installation (MSI Pack):



Instructions:

1. Required:
   Edit the file setipconfig.ini by entering the IP of the control server/PC right after the "=" sign.
   Example:
   IP=the server IP (or server machine name).

Optional: You may also edit the port if desired note. If you edit the port number then make sure you enter that port number when installing the control. (By default port 3100 will be used)

2. Save the edited file.

setipconfig.ini and setup_client.exe must be in the same shared location as setup_rp_client.msi .

Follow brief instructions using Group Policy Editor Deployment:

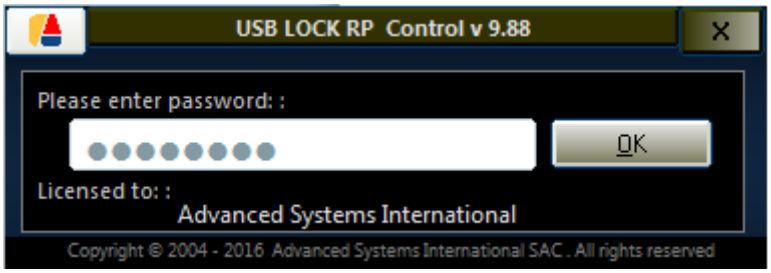
- The MSI file and the corresponding package must exist within a network share, and everyone must have read permissions for that share.
- To perform the deployment, open the Group Policy Editor.
- To assign the client navigate through the group policy console to Computer Configuration | Software Settings | Software Installation.
- Now, right click on the Software Installation container and select the New | Package commands from the shortcut menu.
- Select the provided client MSI file and click Open.
- You are now asked whether you want to publish or assign the application.
- Select assign and click OK.

OPERATE ADMINISTRATIVE CONTROL

1. Start Administrative Control:

a. Click on windows start menu: Programs - USB Lock RP - Start USB Lock RP

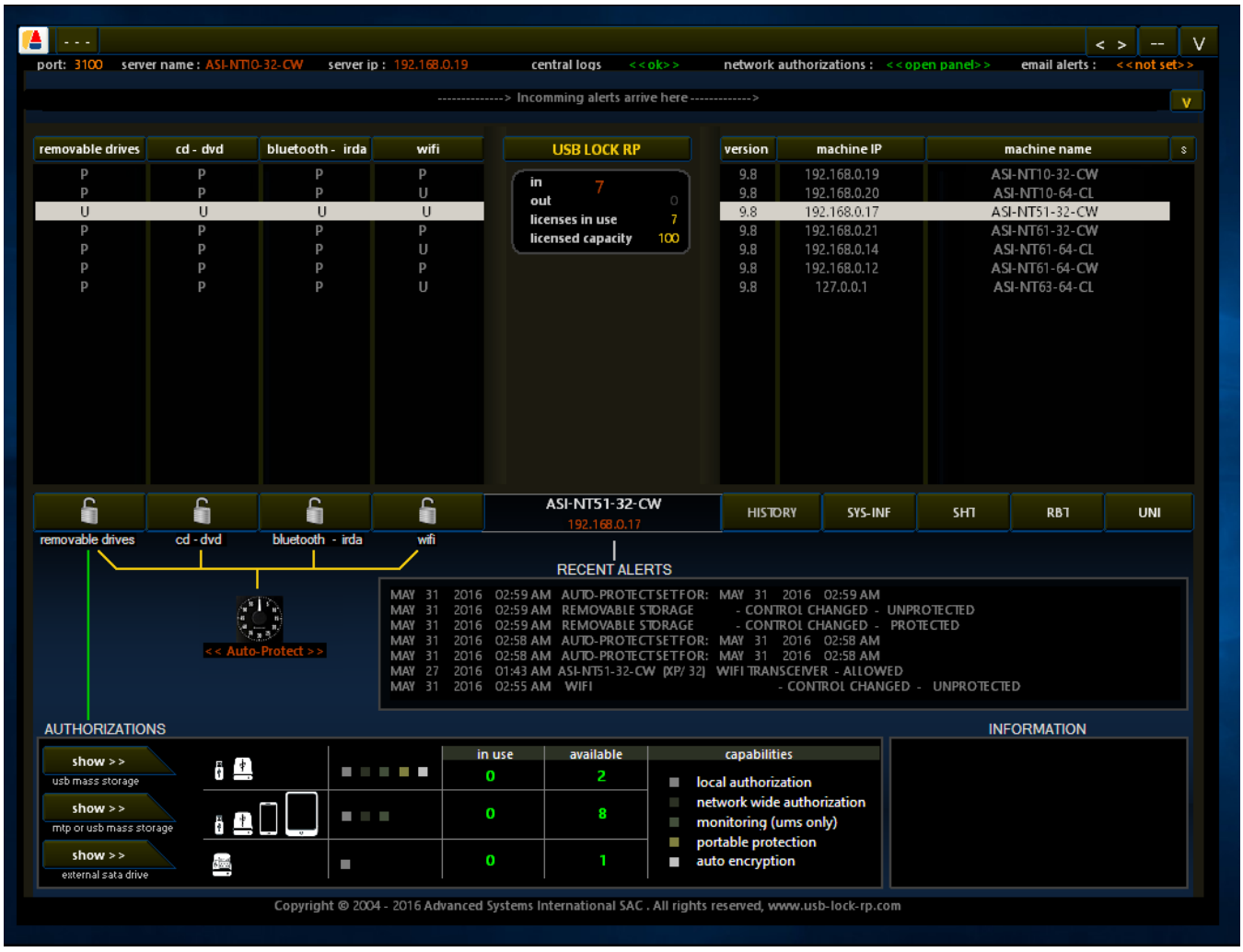
Note: USB Lock RP is UAC Aware (User Account Control Aware) and it will require administrative privileges to be started.



b. Enter the control password and click OK.

c. You will see the logged Client PCs showing their security status.

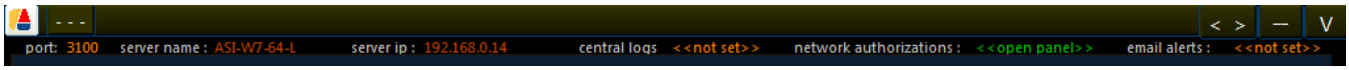
2. Control (Main Panel):



Control Main Menu

3. Run Compact mode:

Once you have set security you can run on compact mode **(pressing V at the right top corner)**



Compact Mode

- 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
- The A light: will show alert incoming. (Blocked is blue light and orange is approved or authorized.)
- The FT light: means File Transfer.
- The title bar: shows the machine name of the alert.

4. Full Screen Mode: (pressing < >)

Full Screen Mode

- The full Screen Mode: helps you focus on the interface if other applications are running.

5. Logged PCs:

Shows the number of logged Clients. **Out** shows a list of not logged Clients.
To remove unused Clients Pcs from the list you can drag the name from the list to the remove old Drop Zone.
Using these methods USB Lock RP allows recovering unused licenses.

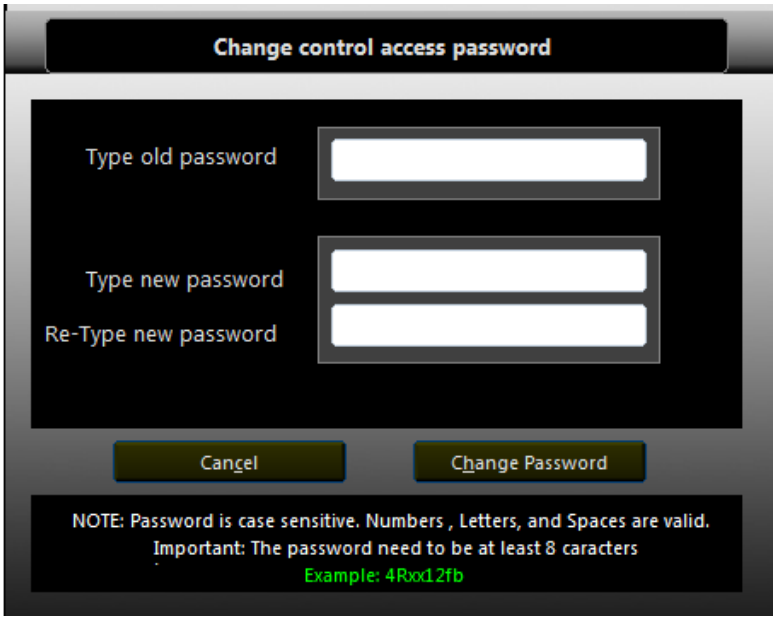
6. Fast PC Look-up:

For large Networks USB Lock RP Pc look up comes handy.
Press "S" at the right of the machine name to show Pc look up it will allow you to find Pcs by machine name.
Press columns headers to order alphabetic by machine IP, or machine name, or protection status on the list.

7. Control Password:

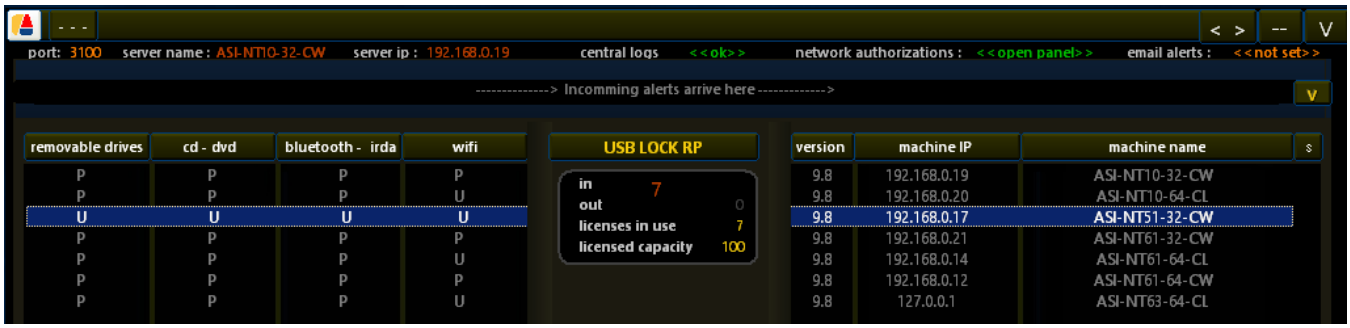
Use to change password to access the USB Lock RP Control.

- Enter the old password.
- Enter the new password.
- Re-Type the new password.



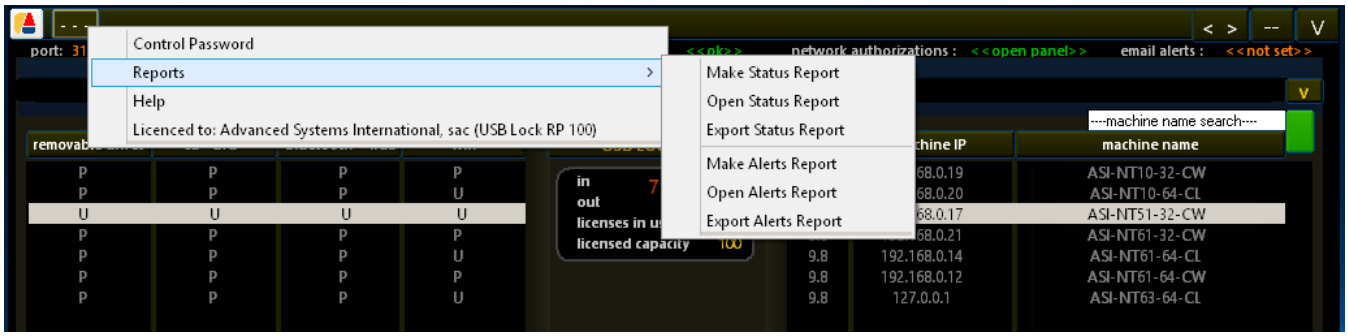
8. Alert visor and Alerts Access Arrow:

Last received alert will show on the visor. Click the arrow to expand view and see all alerts. Receive allowed, blocked or authorized insertion alerts in real-time.



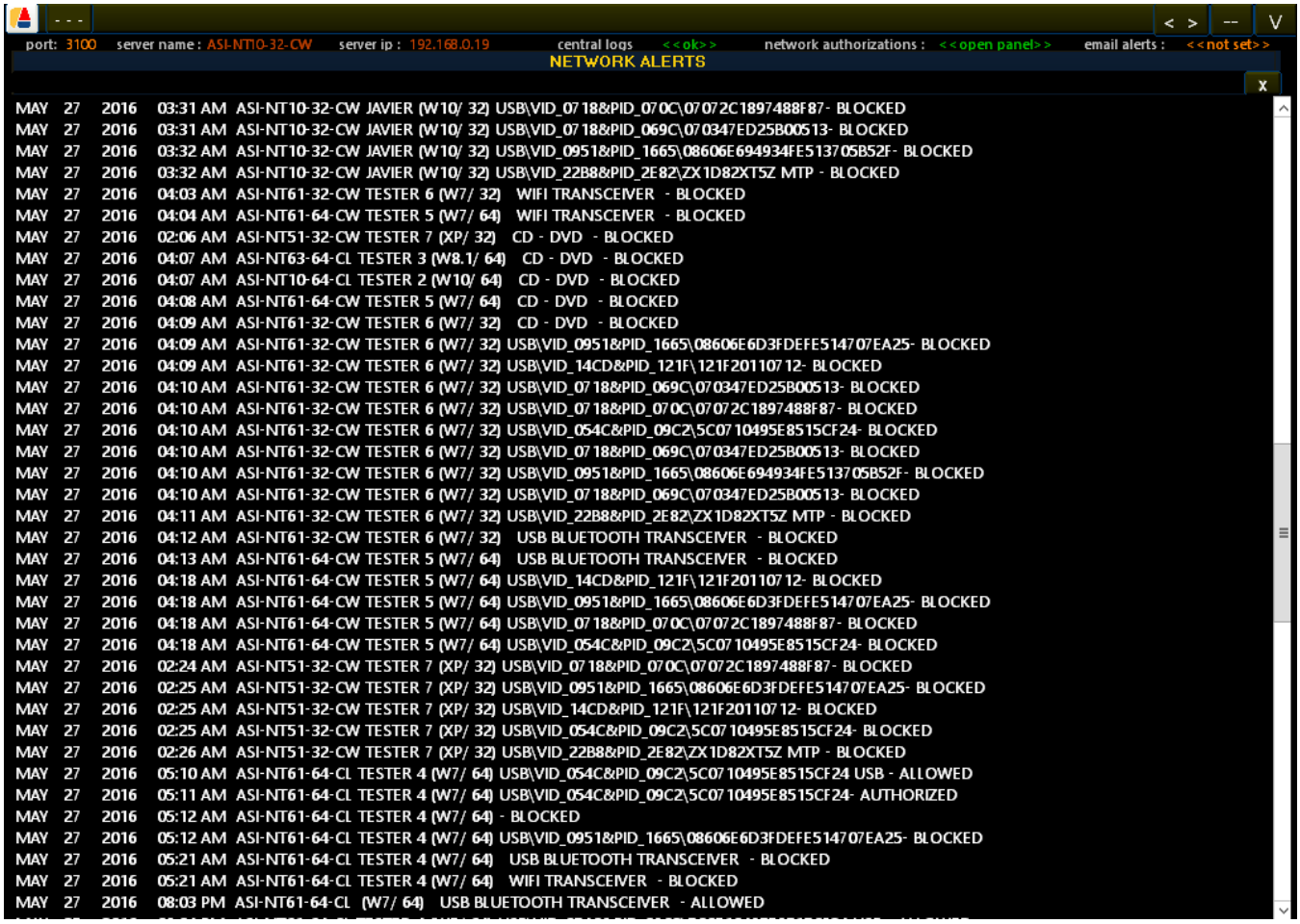
9. Network Status Panel and single control setups reporting

Networks Reports: Generate global security status or alerts reports.



Network Status List

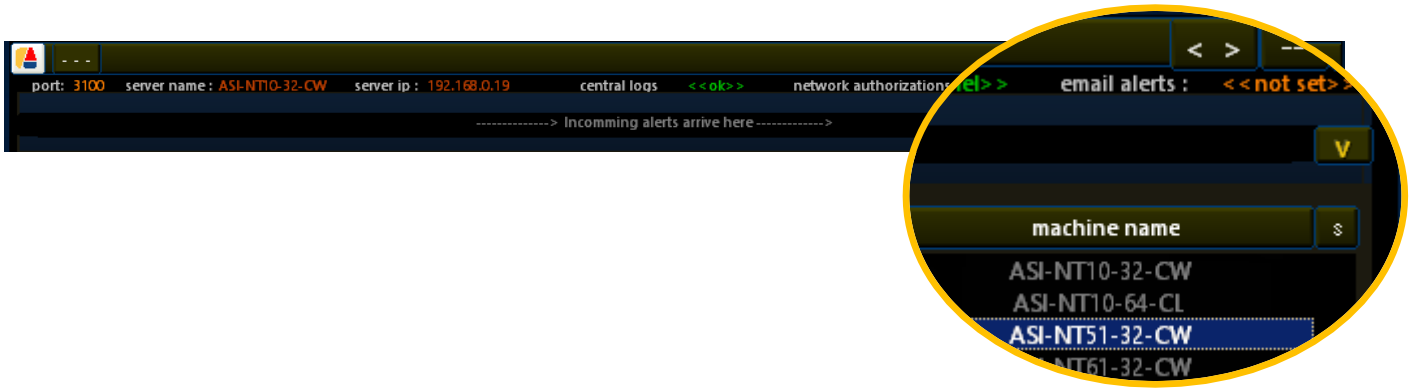
Network Alerts List

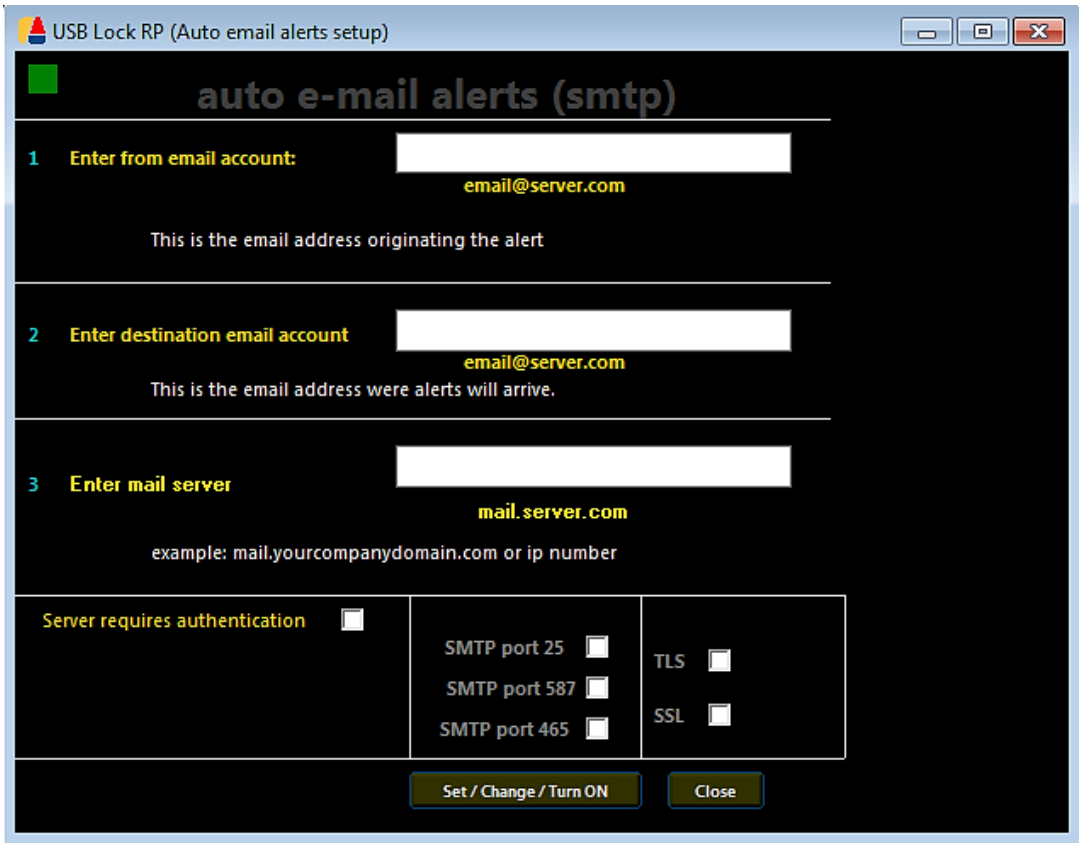


10. Real-time alerts reporting:

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)

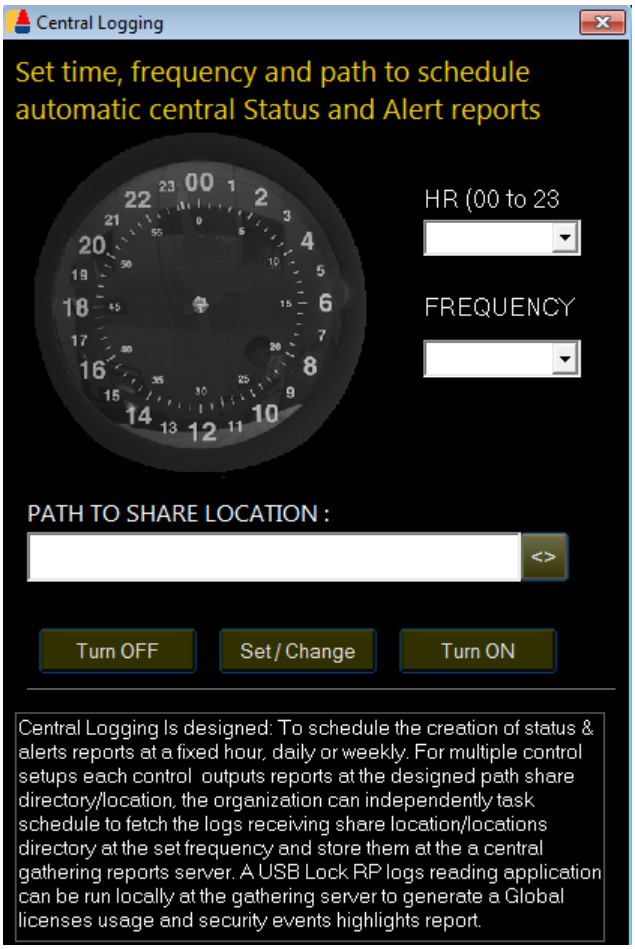
1. Automatic after easy setup
2. Allows SSL / TLS
3. All incoming alerts logged to the Control are sent.

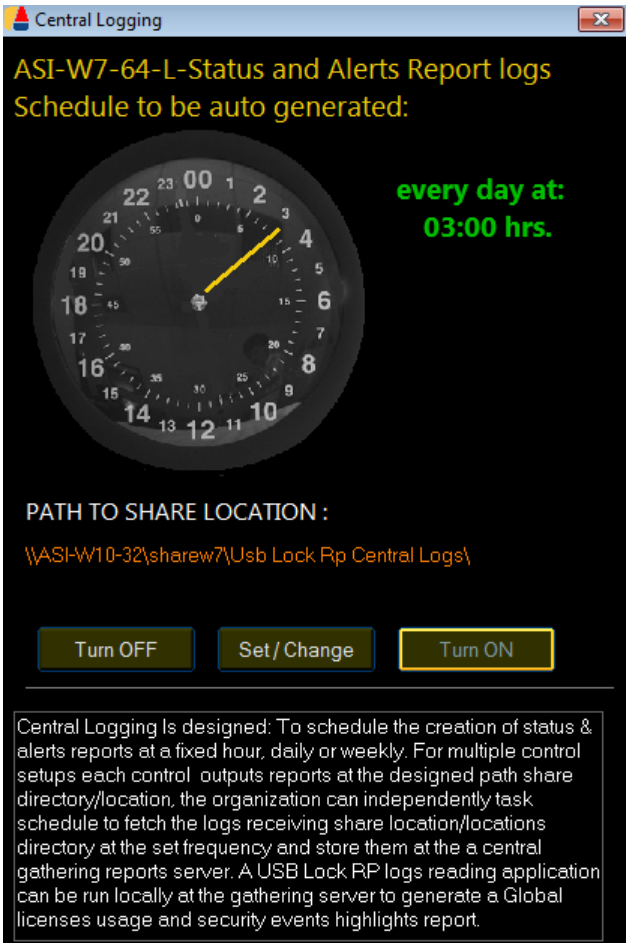




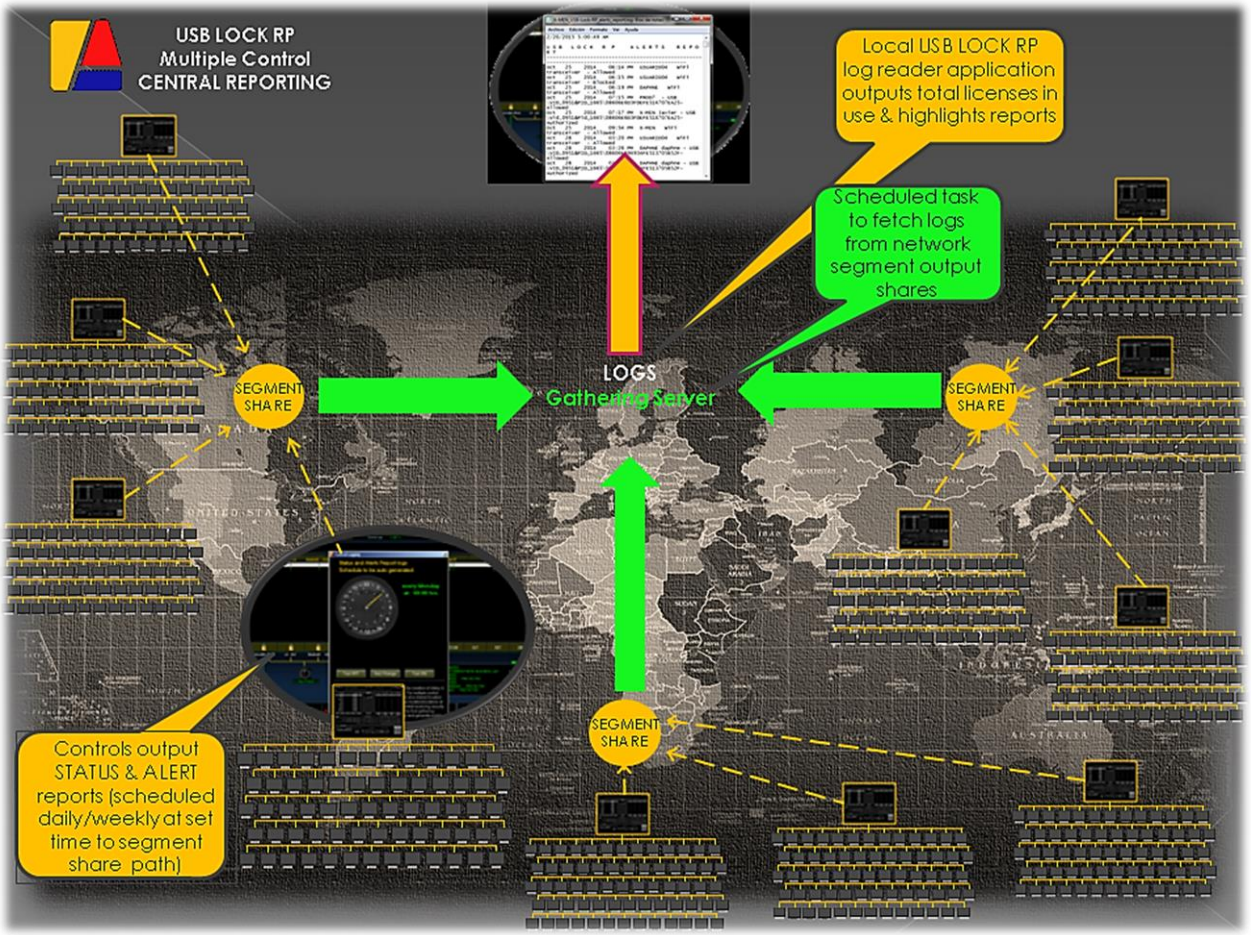
11. Scalability and Multiple Control Setups Reporting

Central Logging function:





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

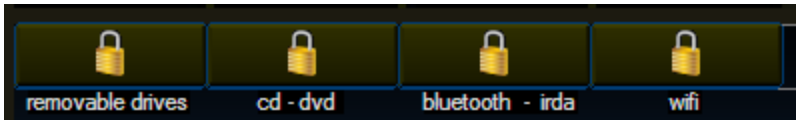


(MULTIPLE CONTROL CENTRAL REPORTING)

For multiple control setups each control outputs its reports at the set frequency to the shared location, then the organization can internally task schedule fetch this logs location/locations and gather them at the central receiving security server. An Usb Lock RP logs reader application is used to read the logs and output a total licenses usage status count and a global highlights security report.

12. Protection Sectors:

Select PC on status panel press to protect or unprotect accordingly



- A closed golden padlock indicates: **Protected**
- An open gray padlock indicates: **Unprotected**

REMOVABLE DRIVES Sector Lock:

Blocks USB removable drives-Portable flash memory devices – MTP protocol portable devices – Digital audio players including MP3, MP4 players and Ipods – External hard drives including e-SATA & Firewire Adapters bridging between standard flash memory cards and USB connection – Storage Capable Digital Cameras – Card readers: CF, SD, SDMicro, MMC, XD – PDA, Hand-held computers, smart phones.

NOTE

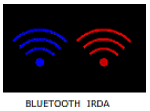
Specific USB removable drives specific MTP; specify e-sata can be authorized

CDS, DVD, Blu Ray Sector Lock:

blocks Cds, dvds, and blu-ray.

Bluetooth, IrDa Sector Lock:

blocks IrDa and Bluetooth Transceivers.



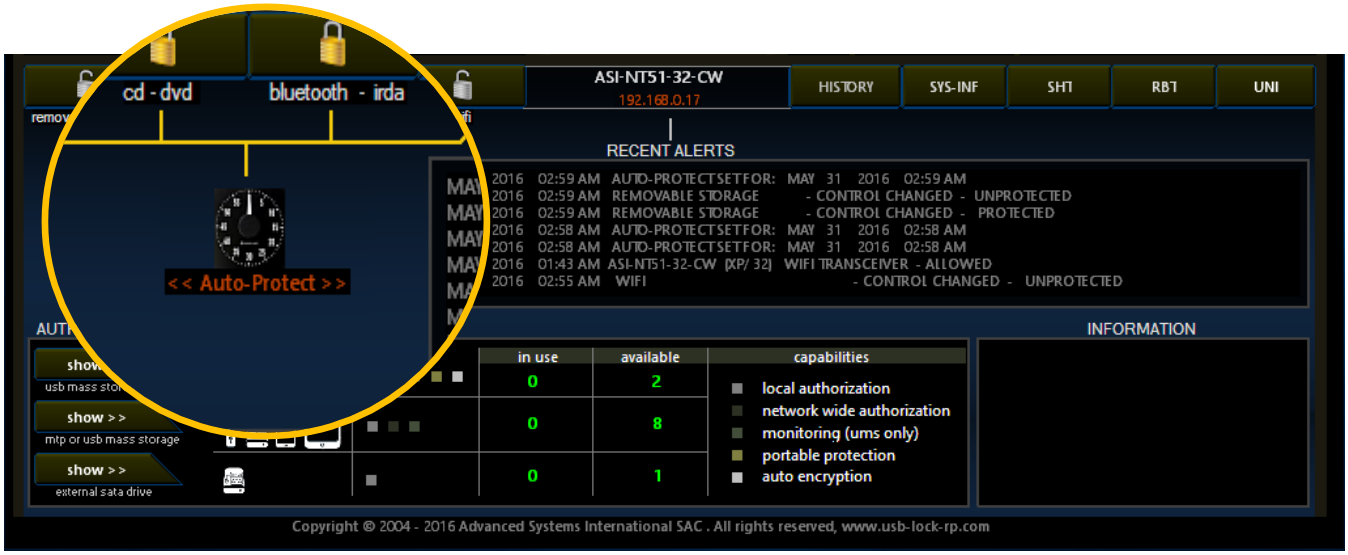
WiFi Sector Lock:

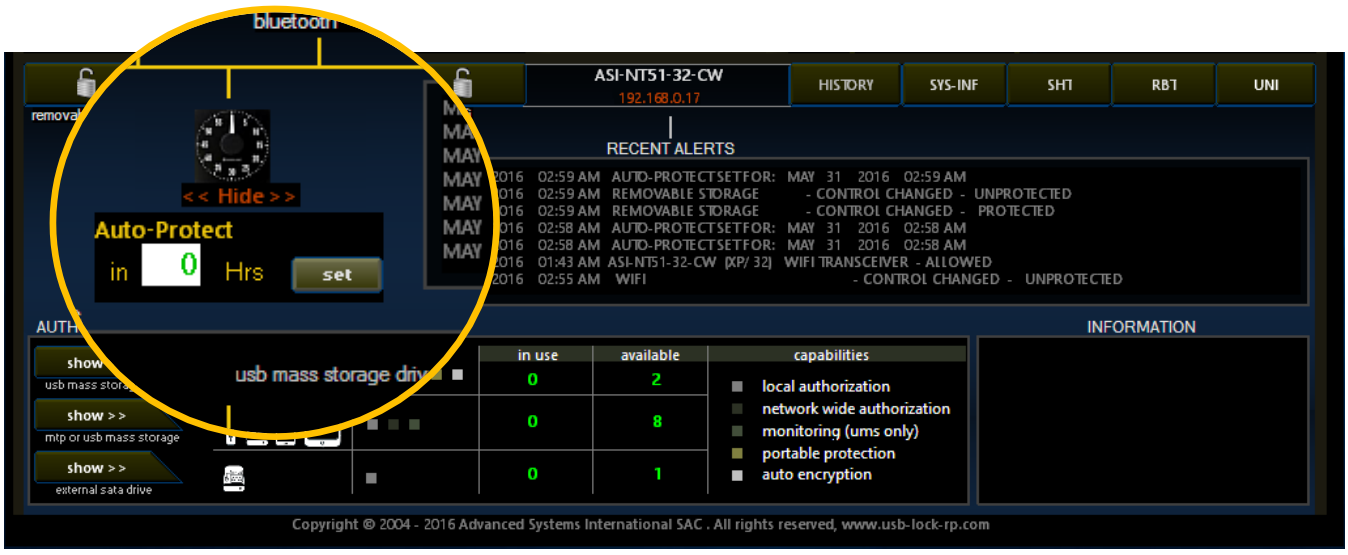
blocks wifi.

Protection changes are enforced in real-time (no need for restart for changes to take effect)

13. Auto-protect:

Auto Protect this will allow to protect all sectors on a client after a select period of time. This is specially designed for situation if for example engineers arrive to work on the systems for a couple day or hours and require full access (in those cases authorizing their specific USBS might not be sufficient to let them do their job). So in real scenario what the control manager could do is unprotect all sectors and let them work. Auto-protect ensure the control manager doesn't forget to re-protect the system when engineers leave.



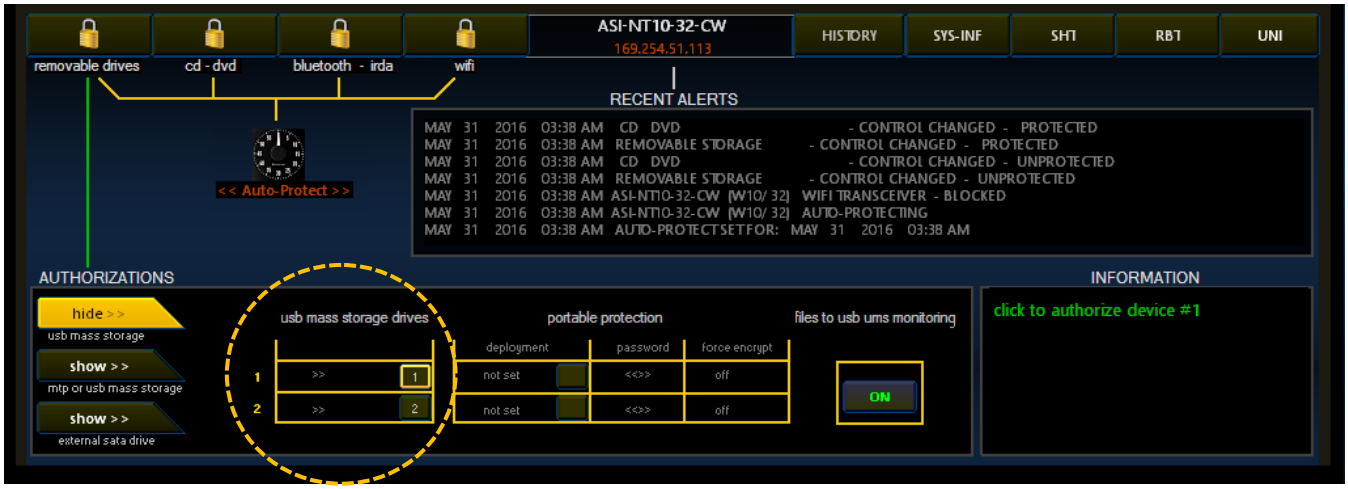


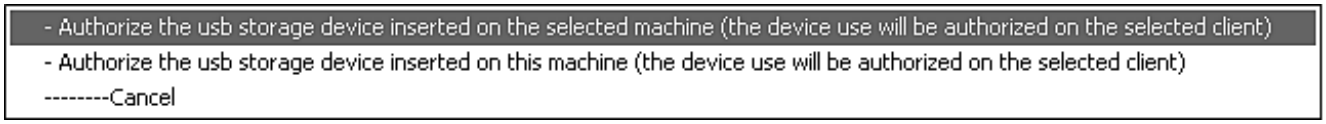
14. Client Level USB Removable Drives Authorizations:

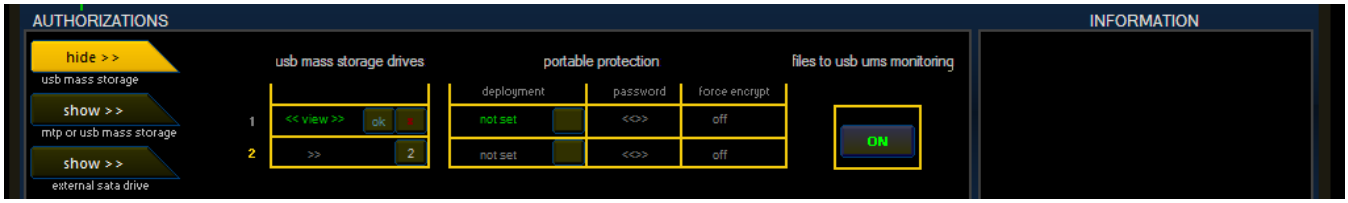
- Ten (10) specific usb removable drives or MTP protocol devices can be authorized on any client PC.
- Two (02) specific authorized usb removable drives have extended portable protection capabilities.
- One (01) specific e sata (external sata) drive can be authorized on any client PC.

To authorize USB REMOVABLE DRIVES
First Option:
(To authorize the device actually inserted on a client to function)

- Select the Client PC from the network list.
- Unprotect removable storage sector.
- Instruct the insertion of the USB drive at client PC
- Press on the button 1 and select the first option







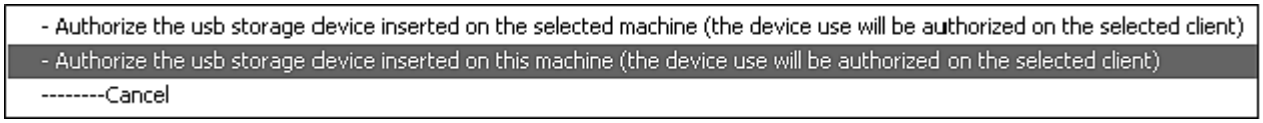
- Automatically the status of USB storage device will change to protect and the label will indicate “view”.

Second Option:

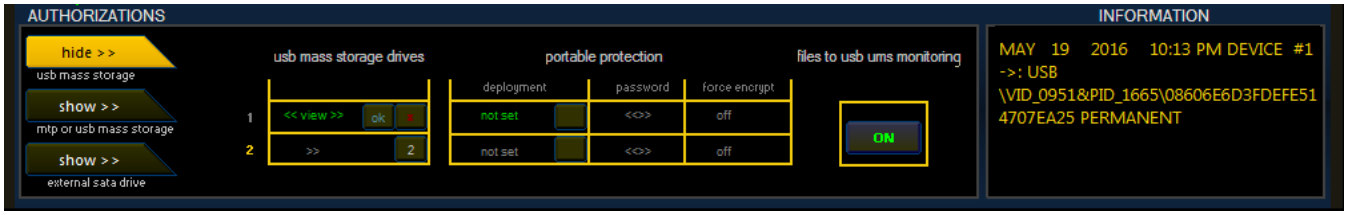
(To authorize the device inserted on the control to function on a client)

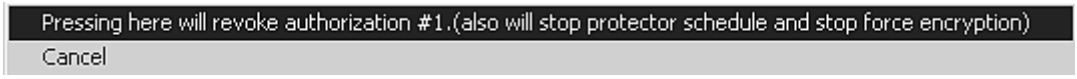
- Select the Client PC from the network list.

- Unprotect the USB removable storage device.
- Insert the USB removable storage device to be authorized on the control machine.
- Press on the button and select the second option



- Authorizations are permanent but you can revoke the authorizations at any time.

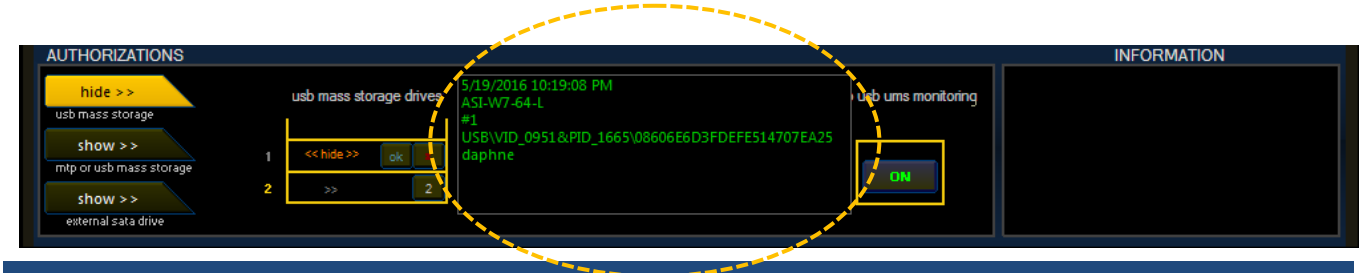




- The status of USB storage device will change to protect and the label will indicate “view”.

Authorization Info:

- Select the Client PC from PC Protection Status View.
- Press on the label of the authorization corresponding number.
- Shows the authorization information.



15. Network Authorizations:

Elevate the device ID to the network authorization list.

- Select the Client PC from the network list.
- Press on the button (+) of the authorization corresponding number. The button will indicate "ok"
- See the network authorizations list. At this point the authorization has been elevated to the network list. (Once you are done elevating to the network list you may click **<<deploy>>** button to access the network authorization panel.

- You may start the list deployment sequence to all clients. Click on the button "Start deployment sequence"
- Once deployment sequence is started the list is sent to all clients.

NOTE

Deploying the network authorization list replaces previously deployed list

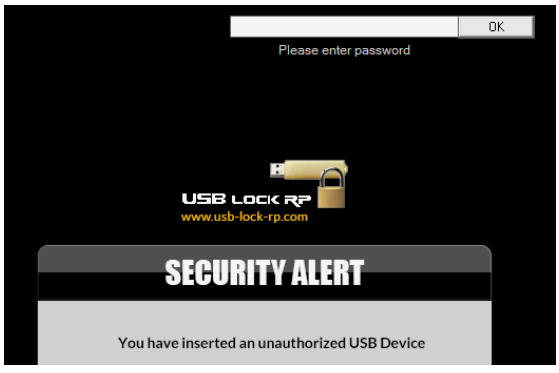
16. Master Password Functionality:

Alternative method to authorized USB drives while a client is outside the network or when the control is turn off for any reason or when there is no communication between the client and the control. For example: server failure, network failure, client outside the network. (Also useful for laptops travelling outside the network requiring authorization of USB drives while they are away).

When two conditions are true the blocking alert allows for password to be entered authorizing device use:

Condition 1: Master password is set from the control (this can be set and deployed from the Network wide authorization panel)

Condition 2: There is no connection with the control, (this can be tested by just shutting down the control to simulate the client disconnected from the network).



If the master password is deployed and client is not on the usb lock network the USB Lock RP Control Administrator could disclosed the master password to the client user so he/she can enter the master password on blocking screen input box to temporary authorized and use the USB drive (input box is only visible if the 2 conditions are true).

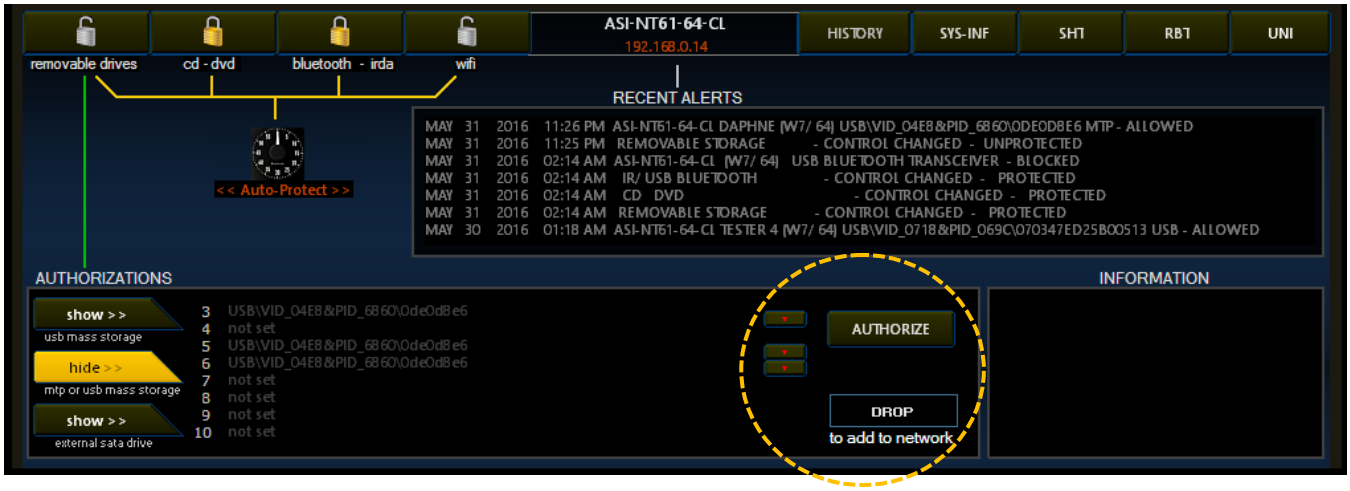
NOTE

The Usb Lock RP Control Administrator can reset the password at any time and deploy to all clients by just pressing start deployment sequence.

IT IS ALWAYS RECOMMENDED THAT A MASTER PASSWORD IS SET AND DEPLOYED SO IF THE SITUATION WERE ITS NEEDED ARISES IT CAN BE USED.

17. MTP or More USB Removable Drives Authorizations:

- 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 on the large button (in golden below) and select authorize.
- Repeat the procedure for more devices.

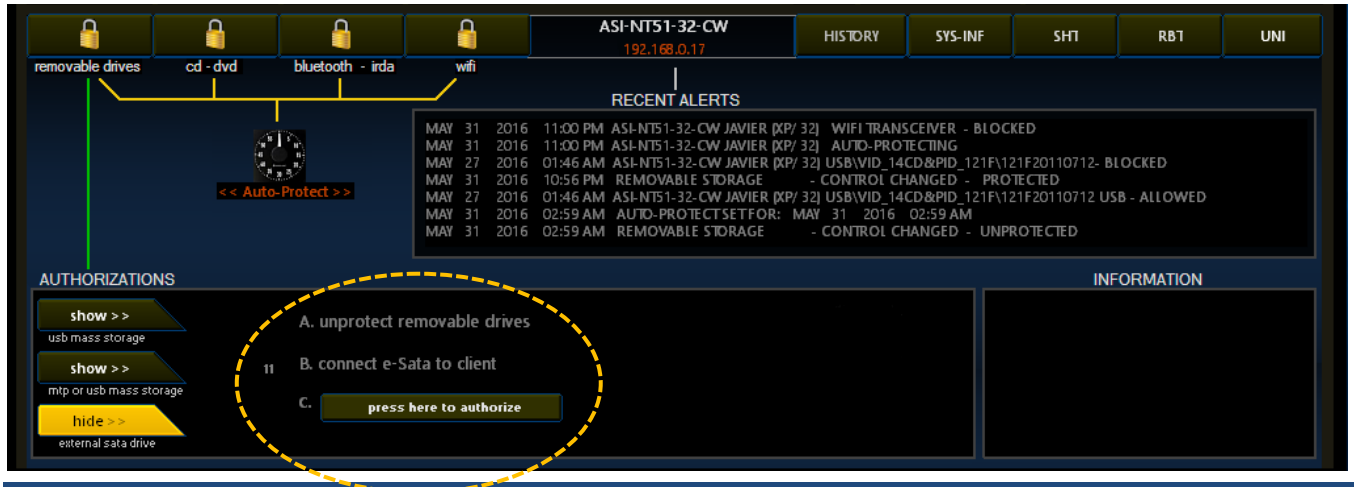


Drop Zone:

You may elevate these type of authorizations by dragging a hardware Id to the drop zone once you are done elevating authorizations to network level list you can start deployment as explain in Index 12.

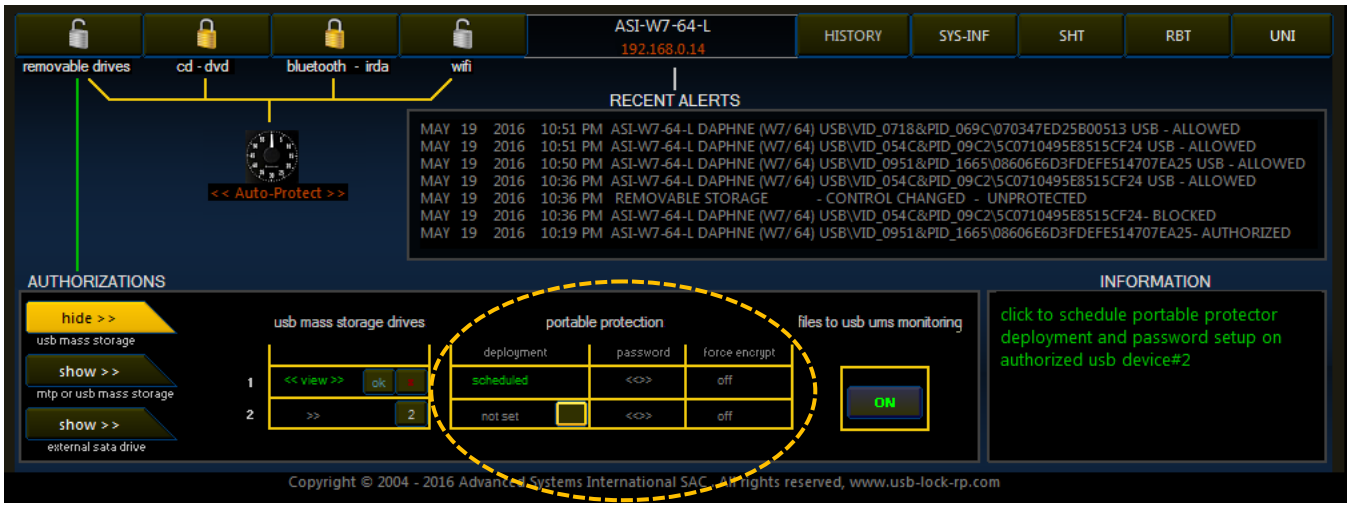
18. E-SATA Authorization:

- Select the Client PC from the network list.
- Unprotect removable storage sector.
- Instruct the insertion of the e-sata at client PC.
- Press on the button number 3. (See picture below).
- Removable Sector will be automatically protected.



19. Portable Protection:

Two (02) specific authorized usb removable drives have extended portable protection capabilities. Once you have already followed the steps (Index 11) You made protect the information inside authorized usb drives while used to transport or store information:
Remote portable protection assignment and distribution for the 2 main usb storage authorizations at any time any client.



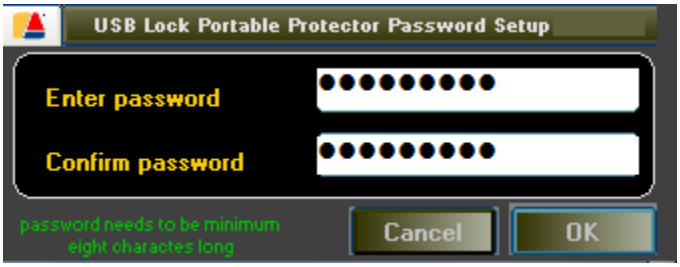
To schedule deployment of a portable protector to an authorized usb storage device:

At Control: (set)

Press the button below portable protector **deployment** insert to the desired authorized device 1 or 2.

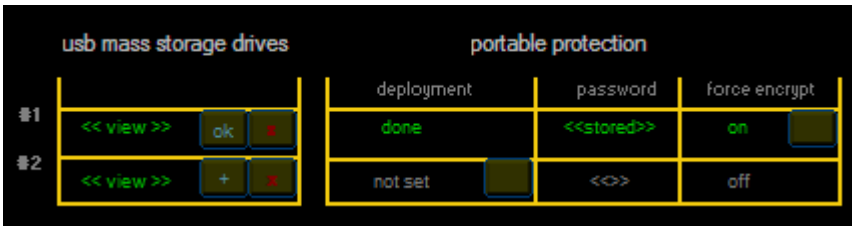
At Client: (set-test)

Once the device is connected the user will be prompted to set the protector password and protector.exe will be created on the usb drive automatically. After settings deployment you don't have to worry as once the user set the password. The password will automatically arrive to the control.

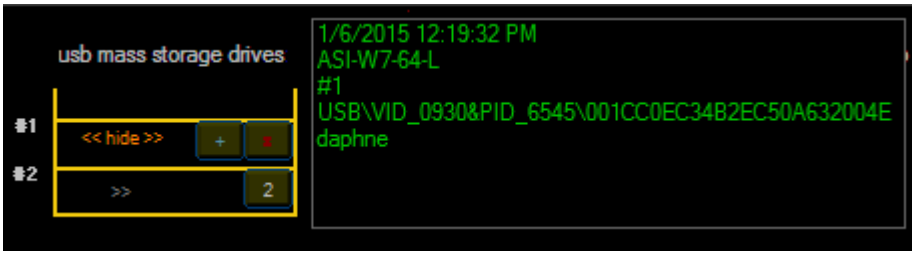


At control (test)

Once the portable protector is created the password user, pid, and machine relation can be seen at the control pressing **<<stored>>** below password. (So the information is always accessible to the organization and lost password issues can be resolved with no problem)



Centralized password storage: Allowing to internally troubleshooting any "lost password issues"

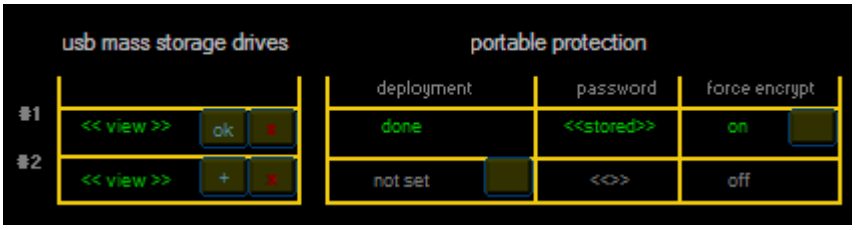


NOTE

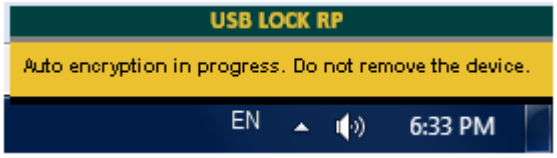
Automatically logs the relation: Device User-Device Id Device Home Device Portable Protector Password

a) Force Encryption:

Smart auto encryption: When force encryption is set to ON, files transferred to the two main authorized devices are automatically encrypted.



And the user at client PC is noted of the encryption progress by a small unobtrusive message and distinctive pitch beep. Forcing auto encryption is recommended to ensure the portable protector is used

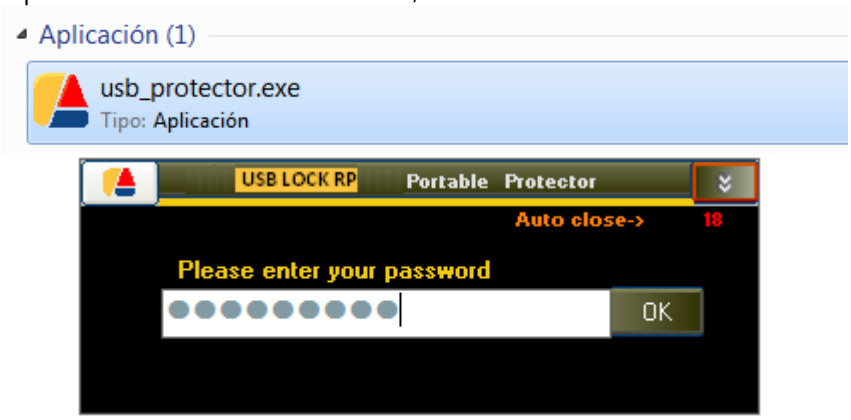


b) Portable protector

- Drag & Drop functionality
- Auto destroys protected files after 4 wrong password entries (optional).
- 128 bit hash key to cipher all data content.
- The license to use two portable protectors is included per USB LOCK RP licensed client. For example USB LOCK RP 100 grants license to 200 portable protectors.
- Runs within usb drive (operates in other PC outside the network). Always required password to encrypt or decrypt.

c) Portable protector Operation (Operates only within the authorized USB DRIVE)

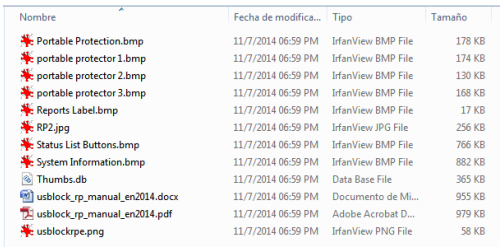
To start the portable protector click on the advice icon, inside the USB drive

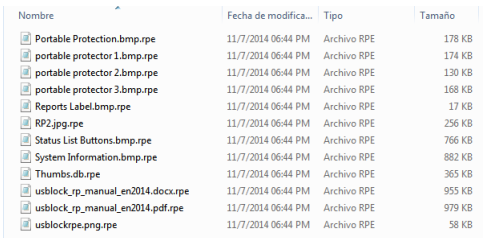


(Enter the password you have set for the protector when it was created)

d) Drag and Drop functionality

(Drag files folders or the entire usb to encrypt or decrypt)

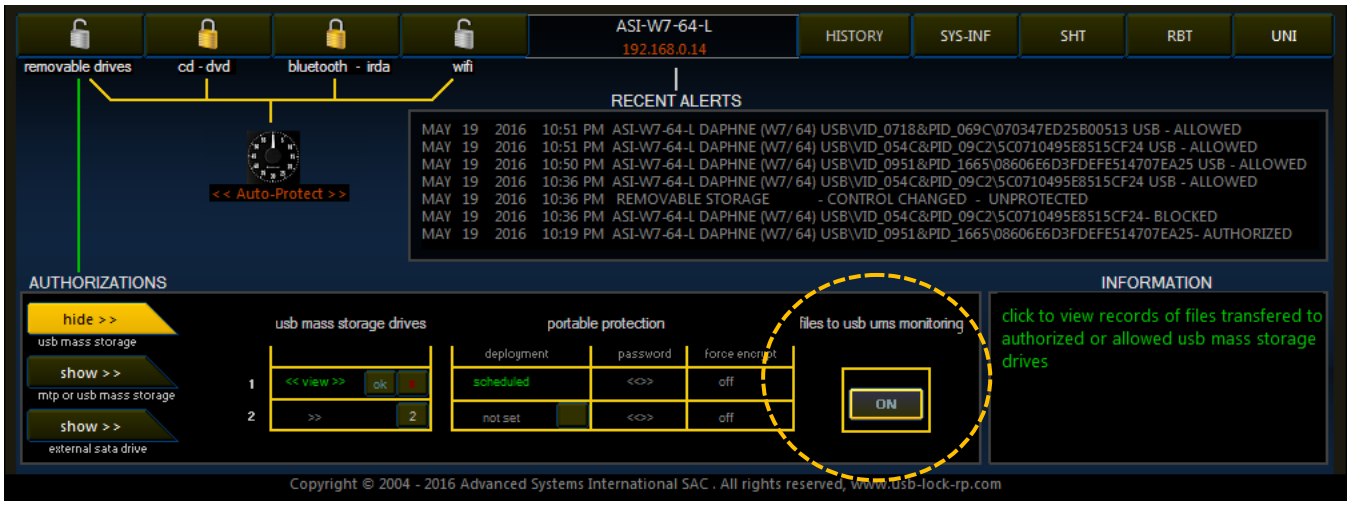




20. Files to USB monitoring:

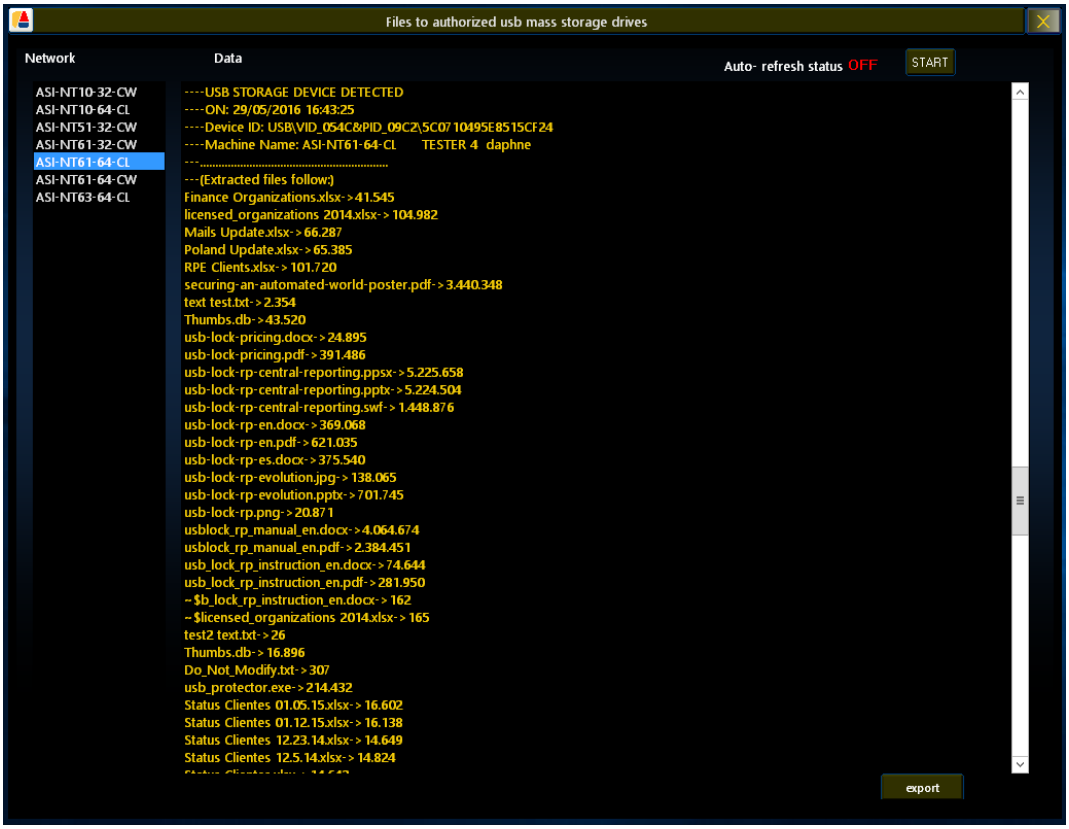
Provides report of files transferred from Client PC's to USB removable storage (optional).

- Select the Client PC from PC Protection Status View.
- Click on the "on" label.

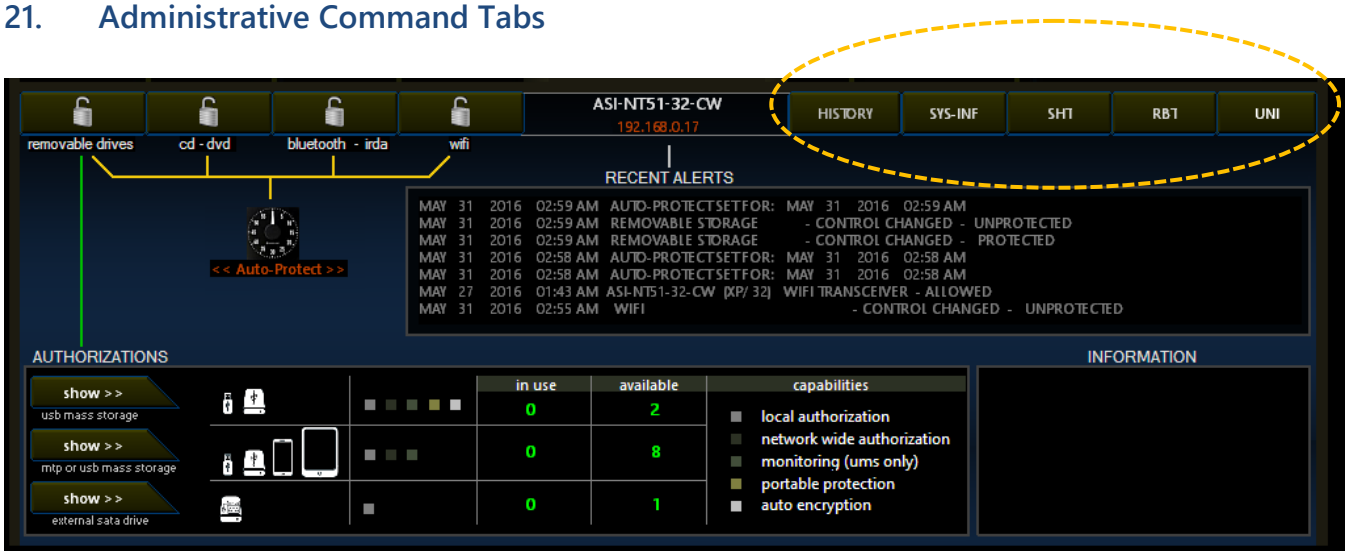


The following information is recorded:

- Date and time of device insertion.
- ID of the device used on the extraction
- Client machine name.
- Name of user or users logged while the device was connected.
- Exact size of the file.



21. Administrative Command Tabs



a) Clients Protection History: Button:

Shows selected machine protection and read RECENT ALERTS.

This panel will allow you to have a record of USB storage devices that have been blocked, authorized or allowed at the client's machine, also a record of the security setting changes that have been made and show the authorizations history per client machine. History records are available for each Client. You can generate a report of this file by pressing export.

b) System Information Button: Requires in real time valuable information on any client.

- Select the Client PC from the network list.
- Press on the button SYSTEM STATUS.
- You will be able to obtain the following information:
  - ✓ Processor and memory.
  - ✓ Operating system
  - ✓ Installed software
  - ✓ Windows updates and patches
  - ✓ Running processes
  - ✓ Authorizations

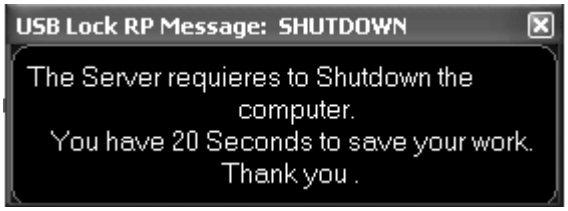
c) Reboot Button:

d) Shutdown Button:

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

- Select the Client PC from PC Protection Status View.
- 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 him he has 20 seconds to save his work before the action takes place



e) Uninstall Button:

Remotely uninstall the selected client PC.

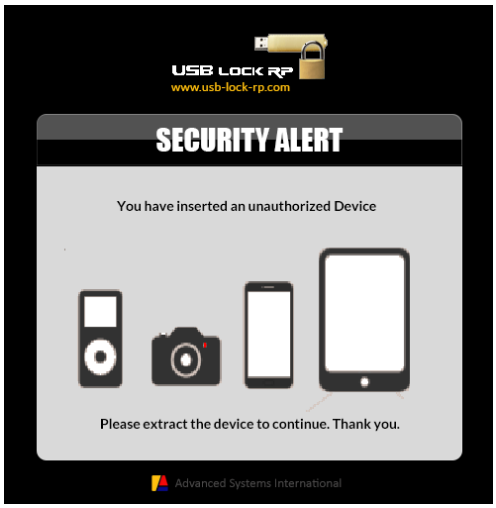
22. Security Alerts Screens:

The following Security alerts will visible at clients depending on the unauthorized device connected.

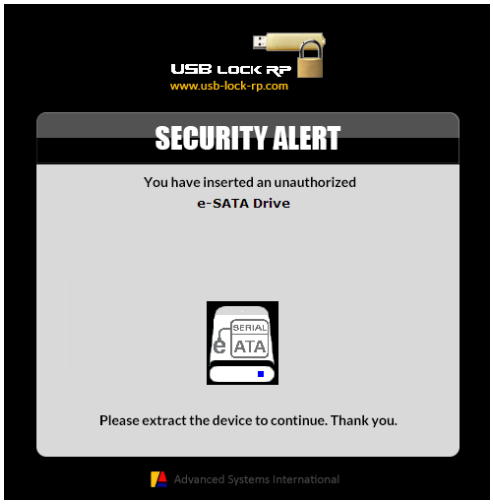
USB DEVICE

CD-DVD-Blue Ray

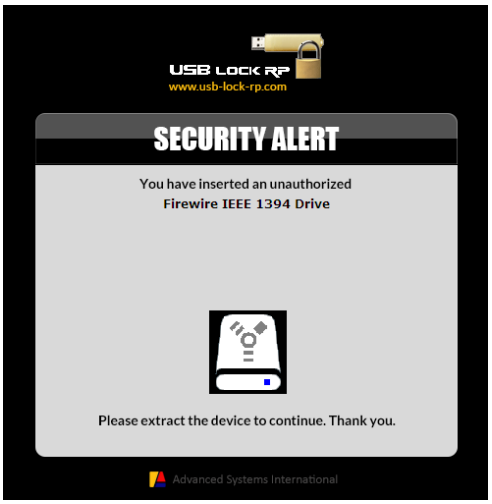
SD Card



MTP Device

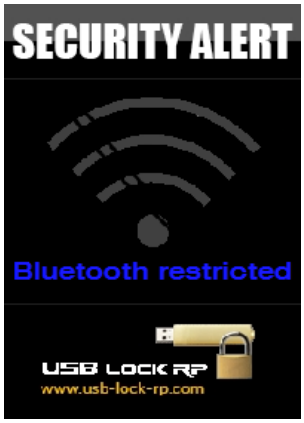


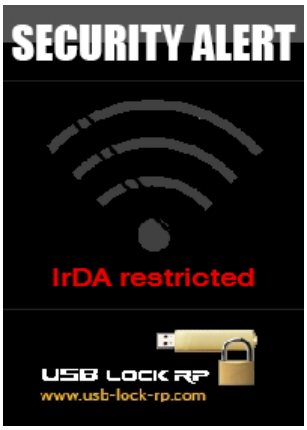
E SATA

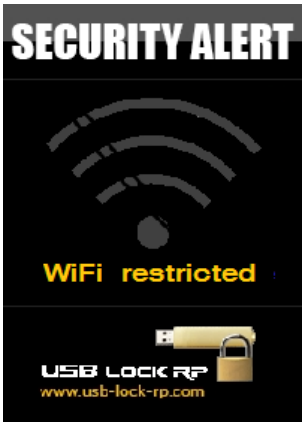


Fire Wire

Wireless Alerts:







23. Personalization:

a) Organization Logo Inclusion:

The inclusion of the End User Organization Logo is required. (We take care of that automatically when we build your digitally signed installers)(at no extra charge)

b) Optional Message:

If your IT Security Department wishes to include a custom message, you can let us know during ordering time so it is included when the order is attended. If your IT Security Department decides to include a custom message after the order has been attended then let us know and it will be included on your next update or license expansion. The custom message should be provided to us in image BMP format. (Size considering orange area picture)