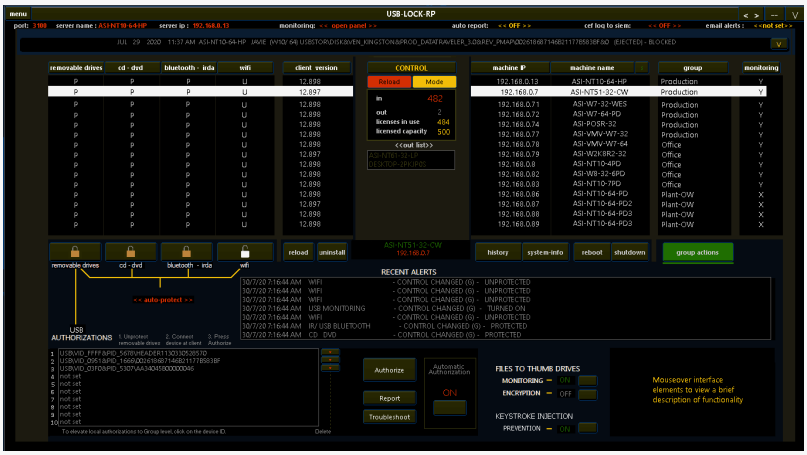
USB-Lock-RP v 12.898 Device Control, Featuring Automatic USB Whitelisting & Lockdown for Enterprise.

DALLAS, TEXAS, USA, August 4, 2020 /EINPresswire.com/ -- Advanced Systems International, CEO Javier Arrospide, officially announced the release of USB-Lock-RP v 12.898 USB Management for Enterprise software.



Centralized USB Control & Whitelisting for enterprise

Featuring: Automatic Authorization Mode, Fully Automatic USB Whitelisting.

Arrospide, is calling the new capability Unseen USB management, result of 15 years of commitment to its flagship endpoint security software USB-Lock-RP and organizations security requirements. “You won’t find this capability elsewhere”, it’s a major breakthrough in cybersecurity”

The function allows to automatically whitelist USB Removable drives and portable device as they are naturally used within the enterprise endpoints across the network. Once AA is deactivated USB-Lock-RP blocks all unauthorized devices automatically.

When asked if this was available for testing, responded “USB-Lock-RP is published as a fully functional demo so organizations can review the new capability”

Briefly explained:
The New Automatic Authorizations Mode Is useful during initial setup to automatize devices authorization process in busy offices or large networks.

While AA Mode is active, removable drives and portable devices will be Automatically Authorized (Whitelisted) at Client side. Authorizations are acquired and logged by the Control in real-time and can be revoked or elevated further as needed at any time.

When asked about the purpose of the software described it functionality as follows:

USB-Lock-RP is the strongest solution to centrally manage access to USB ports, removable storage, mobile devices and wireless adapters to servers, workstations and laptops in a network. Presents Smart USB lockdown designed to protect computers in Industrial processes as well as corporate offices:

OT Industrial Networks DCS and SCADA (Critical Infrastructure)

IT Small-Mid-Large Business/Enterprise Networks.

Classified as USB Port Control for Enterprise, USB Lock RP Device Control Software is an administrative and enforcement tool specifically designed to control usb devices to protect windows operating systems, without concern to dependencies, at a very small memory/storage footprint.

USB-Lock-RP v 12.898 at a Glance:
Automatic Authorizations mode: The perfect solution to automatize implementation.
No need to re-plug authorized devices to use them.

Can use as many authorized devices as needed simultaneously.
Flawless, 100% reliable and consistent client side behavior.
Immediate alerts, 100% reliable

Groups Management:
Groups building. (Massively moves machines to Groups)
Group level, Real-time Set and deploy security policy of all sectors simultaneously.
Group level, Real-time Set and deploy authorized devices. (Capacity: 60 spots per group (Complete ID or VID/PID only)

Group level master password.
SIEM Interoperability.
Automatic report scheduling.

Finally Advanced System International CEO made the following recommendations as part of what he called “the Friendly Mode” implementation of USB Control for organizations:

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

This method won’t be suitable to secure all type of organizations, but it’s the most straightforward, automatic and less obtrusive. By design “The Friendly Mode”

1. Start and log in to USB-Lock-RP Control
Note: Machines will populate the Network list showing their security status.

2. Go to group actions panel.
Note: At this point all clients belong to Group 1.
3. Click the Build Groups Button
4. Select Group 2 (On Build Groups Panel)
5. Check select all. (On Build Groups Panel)
Note: All machines will populate the Build Groups list.
6. Press move. (This will move all logged-in machines to Group 2)
Why? This way any newly installed or logged-out clients can be easily identified as not having pass the
Following steps.
7. Click Automatic Authorizations Mode Button.
8. Activate Automatic Authorizations to Group 2.

Let users operate normally. They'll be connecting the devices they normally use.

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

Removable storage and portable devices will be automatically added to Machines authorized ID list at the control.

Note: AA deactivates after 48 hour automatically. (Or you could deactivate it earlier depending on you network characteristics)

AA Deactivates and security becomes effective automatically & Any unauthorized removable drive or smartphone will be blocked

You can now revoke any authorizations you don't like in real-time or elevate them further to groups, build, rename, set specific setting to groups, From macro to the micromanagement at a glance and in real-time.
You may set your SIEM Interoperability, Schedule automatic reports, email alerts, monitor transfers to authorized USB devices.
More information at: www.usb-lock-rp.com

Javier Arrospide
Advanced Systems International
+ 1 972 890 9488
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.