

# USB-LOCK-RP

By Advanced Systems International



## Manuel d'Exploitation

# USB-LOCK-RP

Mis à jour : 25 avril 2024

Copyright 2004 – 2024 Advanced Systems International SAC. Tous droits réservés.

## Table des Matières:

1) Autres Ressources .....	3
2) Notes de Terminologie .....	4
3) Protection (Secteurs) .....	5
4) Statut de Sécurité des Machines .....	6
5) Protéger des Secteurs sur des Machines Spécifiques .....	6
6) Autorisations (Liste Blanche USB).....	7
7) Autoriser des Périphériques sur des Machines Spécifiques .....	7
8) Panneau d'Autorisations (Par Machine) .....	8
9) Mode d'Autorisation Automatique (AA) .....	10
10) Mode d'Autorisation Automatique sur des Machines Spécifiques .....	11
11) Gérer les Groupes .....	12
12) Autres Actions de Groupe.....	13
13) Mode d'Autorisation Automatique pour les Groupes.....	14
14) Déploiement d'Autorisations pour les Groupes .....	15
15) Comportement de Blocage (Côté Client).....	16
16) Alertes (Côté Contrôle) .....	17
17) Fonctionnalité du Mot de Passe Principal.....	19
18) Écrans d'Alerte (Côté Client).....	20
19) Surveillance des Fichiers vers USB.....	22
20) Chiffrement des Clés USB .....	23
21) Protection contre les Attaques par Injection de Frappes .....	23
22) Fonction Informations Système.....	24
23) Fonction Redémarrer & Redémarrer (Ordinateur Client) .....	25
24) Fonctions Recharger & Désinstaller (Service Client) .....	25
25) Fonction Autoriser/Refuser Charge Seule des Smartphones.....	25
26) Fonction Alertes Automatiques par Email .....	26
27) Rapports Automatiques (Programmation des Rapports).....	27
28) Journaux CEF (Interopérabilité SIEM) .....	27
29) Configuration du Format de Date des Journaux.....	28
30) Clients Connectés & Récupération des Licences .....	29
31) Modification du Mot de Passe de Contrôle .....	29
32) Fonctions de Gestion Administrative .....	30
33) Support Technique .....	34
34) Mise en œuvre d'une Politique de Sécurité USB et Liste Blanche.....	35

## 1) Autres Ressources

### Page Produit

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

### Page des Tutoriels Vidéo

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

### Fiche Technique

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

### Instructions d'Installation

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

### Instructions de Déploiement en Masse (GPO)

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

### Manuel d'Exploitation (ce document, en ligne)

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

### Coûts de Licence (Liste de Prix Publiée)

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

### Faits saillants de la Dernière Version

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

## 2) Notes de Terminologie

Dans le cadre de ce document:

**Machines = Machines physiques ou virtuelles de votre réseau exécutant des systèmes Windows avec le client installé.**

**Client = Service USB-Lock-RP = ssrvc.exe (agent, côté machine).**

ssrvc.exe est un service s'exécutant comme un processus système sur les stations clientes. Sa fonction est de communiquer avec le Contrôle et d'appliquer les paramètres de sécurité définis par celui-ci.

Ssrvc.exe est situé sur les stations clientes : ProgramFiles(86)\ssrvc\ssrvc.exe.

Le dossier Ssrvc est un dossier système masqué. Pour le voir, vous devez ajuster les options de dossier dans l'Explorateur afin d'afficher les dossiers système masqués.

**Contrôle = Application de contrôle USB-Lock-RP = usblockrp.exe (côté serveur).**

### Statut des Groupes

#### Panneau de Statut des Groupes

GROUPS STATUS								
usb	cd	bt	wf	k. i.	mon	count	group name	
U	U	U	U	OFF	ON	2	Default	
P	P	P	U	ON	ON	197	Production	
P	P	P	U	ON	OFF	1	Office	
U	U	U	U	OFF	OFF	0	4	
U	U	U	U	OFF	OFF	0	5	

Buttons: Change, STOP, Enforce

130

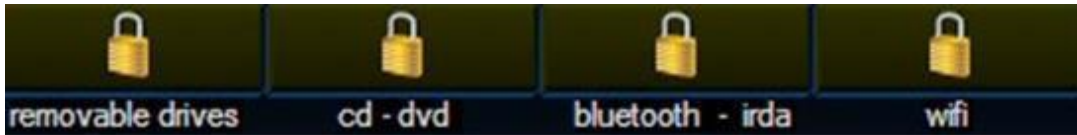
#### Fonctionnalités :

1. **Statut des Groupes en un coup d'œil.** (Interface principale)
2. **Application des Paramètres des Groupes :** Applique les paramètres des groupes. (Un passage pour toutes les machines connectées) (Interface principale)
3. **Auto-Application des Paramètres des Groupes :** Surveillance continue des paramètres des groupes (Interface principale).

**Remarque :** L'Auto-Application est le **nouveau mode recommandé d'opération.**

Lorsque les paramètres sont modifiés, les machines non connectées recevront automatiquement les nouveaux paramètres une fois qu'elles se reconnecteront.

### 3) Protection (Secteurs)



Secteur des lecteurs amovibles:



Stockage USB de masse | Protocole de transfert de médias | Appareils badUSB-HID | Périphériques USB distants | Lecteurs e-SATA et Firewire | Lecteurs de cartes.

Secteur CD, DVD:



CD, DVD, Blu-Ray

Secteur Bluetooth – IrDA:



Transferts de fichiers via émetteurs-récepteurs Bluetooth et IrDA

Secteur Wi-Fi :



Émetteurs-récepteurs Wi-Fi

#### 4) Statut de Sécurité des Machines

Le statut de sécurité peut être consulté en un coup d'œil :

##### La liste du réseau affiche :

(P) = Protégé (Secteur)

(U) = Non protégé (Secteur)

(Y) = Activé (Surveillance)

(X) = Désactivé (Surveillance)

##### Le panneau de la machine sélectionnée affiche :

Secteur Protégé : 


Secteur Non Protégé : 


Surveillance

MONITORING — ON 

MONITORING — OFF 

Mode d'Autorisation Automatique (ON/OFF)

 Automatic Authorizations (AA) OFF

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

#### 5) Protéger des Secteurs sur des Machines Spécifiques

1. Sélectionnez une machine dans la liste réseau de USB-Lock-RP.
2. Cliquez sur le verrou de secteur souhaité. (Les paramètres sont appliqués aux machines en temps réel)



## 6) Autorisations (Liste Blanche USB)

### PORTÉE DU TYPE DE PÉRIPHÉRIQUE :

Lecteurs USB amovibles et périphériques USB portables

### GRANULARITÉ :

Correspondance d'ID de Périphérique Spécifique (par ex. USB\VID\_0718&PID\_070C\07072C1897488F87)

& Correspondance d'ID Fournisseur/Modèle (par ex. USB\VID\_0718&PID\_070C)

### PORTÉE DE L'AUTORISATION :

Machines spécifiques et groupes de machines

## 7) Autoriser des Périphériques sur des Machines Spécifiques

(En temps réel)

USB-Lock-RP propose quatre moyens simples d'autoriser les lecteurs USB amovibles et les périphériques portables tels que les smartphones.



1. Glissez-déposez les alertes Bloquées ou Autorisées pour les autoriser.
2. Saisissez manuellement l'ID du périphérique à autoriser.
3. Autorisez un périphérique déjà connecté sur le client.
4. Autorisez les périphériques automatiquement dès qu'ils se connectent.

## 8) Panneau d'Autorisations (Par Machine) (Panneau des autorisations locales affiché ci-dessous :)

The screenshot shows the 'SURFACEPRO-1064 - LOCAL AUTHORIZATIONS PANEL' with the following data in the main table:

Time	Device ID	Name	Status	Control
2024-04-16 02:55:58 AM	AUTOMATIC AUTHORIZATIONS MODE		OFF	CONTROL*
2024-04-16 02:55:42 AM	USB\VID_03F0&PID_5307\AA34045800000046 HP_V165W		AUTHORIZED	CLIENT*
2024-04-16 02:55:38 AM	USB\VID_03F0&PID_5307\AA34045800000046 HP_V165W		AUTO SET(AA)	CLIENT*
2024-04-16 02:55:23 AM	USB\VID_0951&PID_1666\002618687146821177B583BF KINGSTON_DATATRAVELER_3.0		AUTHORIZED	CLIENT*
2024-04-16 02:55:12 AM	USB\VID_0951&PID_1666\002618687146821177B583BF KINGSTON_DATATRAVELER_3.0		AUTO SET(AA)	CLIENT*
2024-04-16 02:54:59 AM	USB\VID_0718&PID_069C\070347ED25B00513 MEMOREX_TD_USB_3.0		AUTHORIZED	CLIENT*
2024-04-16 02:54:55 AM	USB\VID_0718&PID_069C\070347ED25B00513 MEMOREX_TD_USB_3.0		AUTO SET(AA)	CLIENT*
2024-04-16 02:54:45 AM	USB\VID_0951&PID_1666\60A44C413E64F380D945100C KINGSTON_DATATRAVELER		AUTHORIZED	CLIENT*
2024-04-16 02:54:38 AM	USB\VID_0951&PID_1666\60A44C413E64F380D945100C KINGSTON_DATATRAVELER		AUTO SET(AA)	CLIENT*
2024-04-16 02:54:24 AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB		AUTHORIZED	CLIENT*
2024-04-16 02:54:19 AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB		AUTO SET(AA)	CLIENT*
2024-04-16 02:53:56 AM	AUTOMATIC AUTHORIZATIONS MODE		ON	CONTROL*
2024-04-16 02:53:38 AM	LOCAL AUTHORIZATION #2->:USB\VID_05E3&PID_0749\000000001536		SET	CONTROL*
2024-04-16 02:53:02 AM	LOCAL AUTHORIZATION #2		REVOKED	CONTROL*
2024-04-16 02:53:00 AM	LOCAL AUTHORIZATION #11->:USB\VID_152D&PID_1561\MSFT30DB9876543214E		SET	CONTROL*
2024-04-16 02:52:39 AM	LOCAL AUTHORIZATION #2->:USB\VID_152D&PID_1561\MSFT30DB9876543214E		SET	CONTROL*
2024-04-16 02:51:45 AM	LOCAL AUTHORIZATION #1->:USB\VID_058F&PID_6387\B037FBEO		SET	CONTROL*
2024-04-16 02:50:25 AM	USB\VID_152D&PID_1561\MSFT30DB9876543214E UAS		BLOCKED	CLIENT*
2024-04-16 02:50:02 AM	USBSTOR\DISK&VEN_GENERIC&PROD_MASSSTORAGECLASS&REV_1536\000000001536 (EJECTED)		BLOCKED	CLIENT*
2024-04-16 02:49:58 AM	USB\VID_05E3&PID_0749\000000001536 USB		BLOCKED	CLIENT*
2024-04-16 02:49:13 AM	USB\VID_FFFF&PID_5678\HEADER1130330528570 USB		BLOCKED	CLIENT*
2024-04-16 02:48:59 AM	USB\VID_0718&PID_069C\070347ED25B00513 USB		BLOCKED	CLIENT*
2024-04-16 02:48:49 AM	USBSTOR\DISK&VEN_GENERIC&PROD_FLASH_DISK&REV_8.07\B037FBEO (EJECTED)		BLOCKED	CLIENT*
2024-04-16 02:48:48 AM	USB\VID_058F&PID_6387\B037FBEO GENERIC_FLASH_DISK		BLOCKED	CLIENT*
2024-04-16 02:44:08 AM	LOCAL AUTHORIZATION #11		REVOKED	CONTROL*
2024-04-16 02:44:05 AM	LOCAL AUTHORIZATION #1		REVOKED	CONTROL*
2024-04-16 02:44:03 AM	LOCAL AUTHORIZATION #11->:USBSTOR\DISK&VEN_HP&PROD_V165W&REV_8192\AA34045800000046		SET	CONTROL*
2024-04-16 02:43:58 AM	LOCAL AUTHORIZATION #1->:USB\VID_03F0&PID_5307\AA34045800000046		SET	CONTROL*
2024-04-16 02:43:50 AM	LOCAL AUTHORIZATION #1		REVOKED	CONTROL*
2024-04-15 05:00:51 PM	REMOVABLE STORAGE		PROTECTED	CONTROL*
2024-04-15 04:52:12 PM	LOCAL AUTHORIZATION #1->:USB\VID_346D&PID_5678\4824451206115613250		SET	CONTROL*
2024-04-15 04:43:15 PM	REMOVABLE STORAGE		UNPROTECTED	CONTROL*
2024-04-15 04:40:35 PM	LOCAL AUTHORIZATION #1		REVOKED	CONTROL*
2024-04-15 04:40:29 PM	LOCAL AUTHORIZATION #1->:USB\VID_03F0&PID_5307\AA34045800000046		SET	CONTROL*

Control buttons at the bottom:

- Drag-Drop authorization: Focus
- Manually enter ID to authorize: Start
- Authorize a device already connected at client: Authorize
- Automatically authorize devices (AA): OFF
- Elevate devices to Group Level: Organize to right or left side

Table at the bottom:

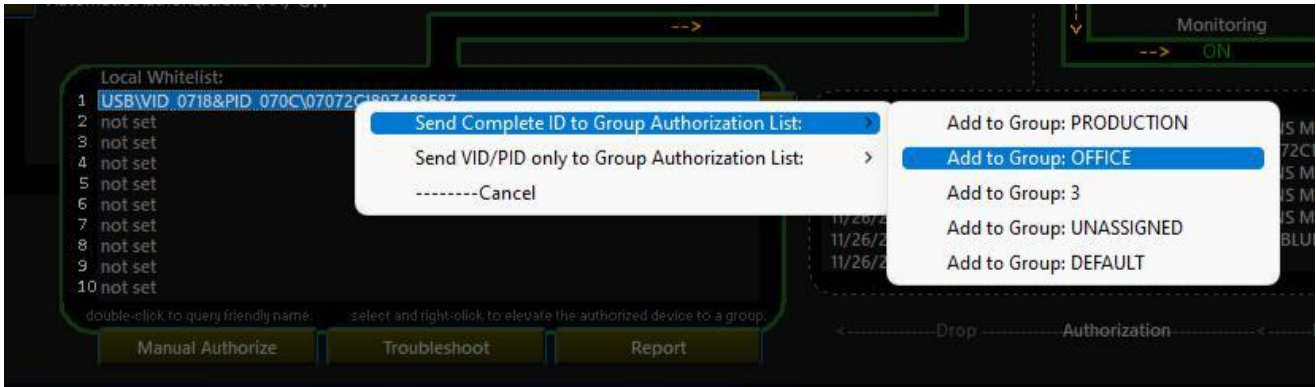
Device ID	Name	Status	Name	Device ID
01 USB\VID_058F&PID_6387\B037FBEO	FLASH_DISK_AS1	LOCKED	UAS DRIVE AS1	USB\VID_152D&PID_1561\MSFT30DB9876543214E
02 USB\VID_05E3&PID_0749\000000001536	USB-CUSTOM	LOCKED		not set
03 USB\VID_FFFF&PID_5678\HEADER1130330528570	USB	LOCKED		not set
04 USB\VID_0951&PID_1666\60A44C413E64F380D945100C	KINGSTON_DATATRAVELER	LOCKED		not set
05 USB\VID_0718&PID_069C\070347ED25B00513	MEMOREX_TD_USB_3.0	LOCKED		not set
06 USB\VID_0951&PID_1666\002618687146821177B583BF	KINGSTON_DATATRAVELER_3.0	LOCKED		not set
07 USB\VID_03F0&PID_5307\AA34045800000046	HP_V165W	LOCKED		not set
08 not set		LOCKED		not set
09 not set		LOCKED		not set
10 not set		LOCKED		not set

### Caractéristiques :

- Le panneau charge les 200 alertes les plus récentes pour n'importe quelle machine et se met à jour en temps réel. Vous pouvez glisser les alertes bloquées ou autorisées (surlignées en blanc) et les déposer dans les cases "ID de Périphérique" de l'un des 20 emplacements d'autorisation disponibles pour chaque machine. Les autorisations deviennent effectives sur la machine cliente en temps réel. (Remarque : Les autorisations peuvent également être révoquées (supprimées) en temps réel depuis ce panneau.)



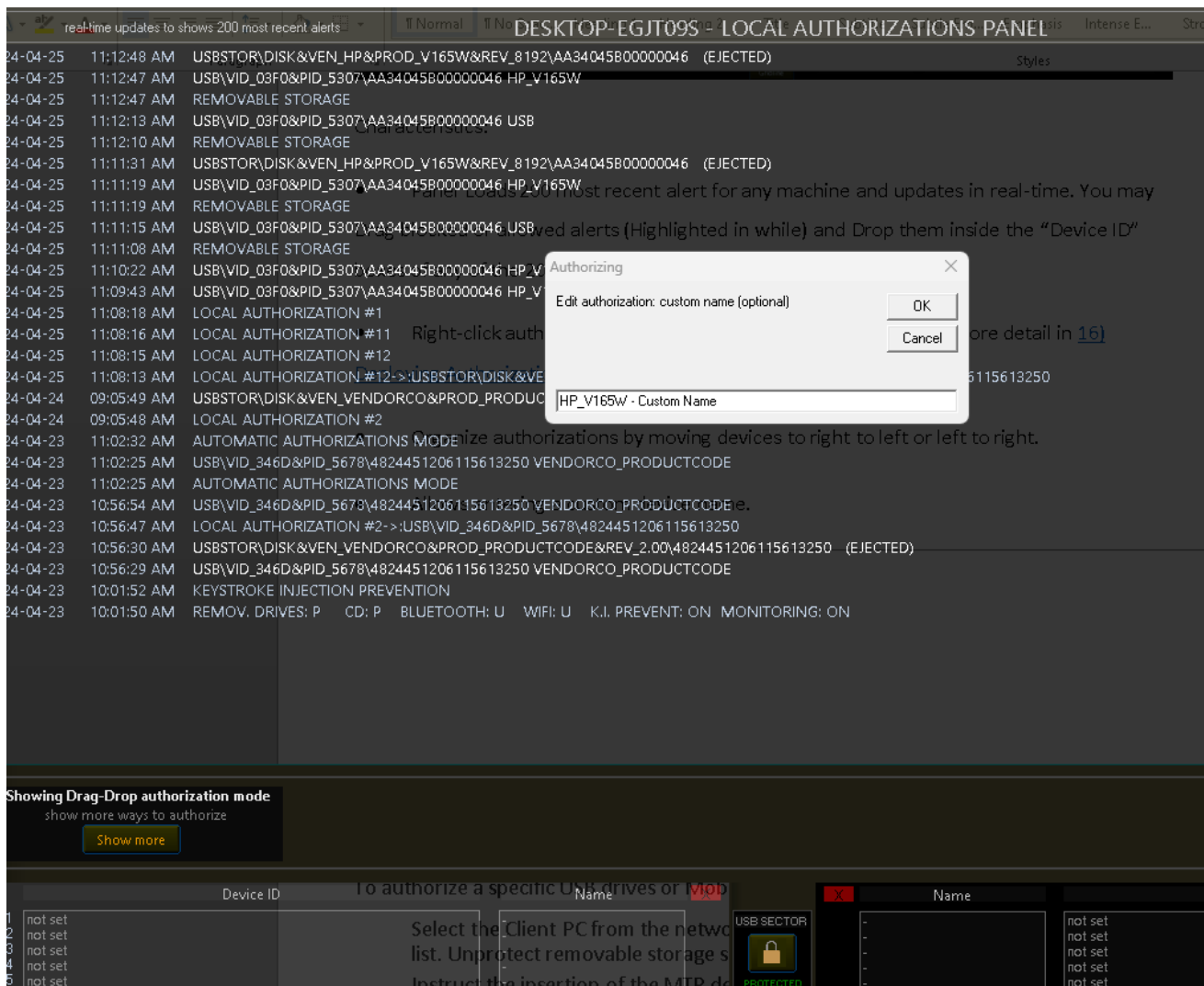
- Permet de facilement élever tout périphérique autorisé au niveau des Groupes si nécessaire, afin que tous les membres de ce groupe puissent utiliser le périphérique. Faites un clic droit sur n'importe quel ID de périphérique autorisé et sélectionnez dans le menu contextuel l'option pour élever l'ID complet ou pour élever la partie Fournisseur/Produit afin d'obtenir une autorisation de portée plus large basée sur la correspondance Fournisseur/Produit.



Pour plus de détails, voir [14\) Déploiement des Autorisations aux Groupes.](#)

- Organisez les autorisations en déplaçant les périphériques de droite à gauche ou de gauche à droite.

Cela est utile pour mieux organiser les autorisations des périphériques.



- Permet de saisir un nom personnalisé pour le périphérique.

Lors de l'autorisation par glisser-déposer, en saisissant un ID de périphérique ou en autorisant un périphérique connecté, le nom lisible du périphérique sera disponible. Vous pouvez modifier ou saisir un nom personnalisé pour identifier davantage un périphérique (optionnel).

Remarque : Vous pourrez ajouter des notes supplémentaires si le périphérique est élevé au niveau du Groupe depuis le panneau d'autorisations des Groupes.

## 9) Mode d'Autorisation Automatique (AA)

(Mise en liste blanche automatique des lecteurs USB et des périphériques portables)

**Portée:** Au niveau du groupe et au niveau des machines spécifiques.

**Processus d'autorisation automatique et d'acquisition de contrôle.** (Fonction avancée brevetée de USB-Lock-RP)

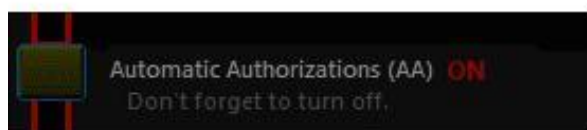
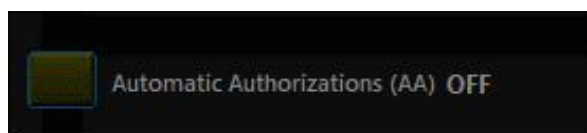
**Automatiquement autorisés (mis en liste blanche) lorsqu'ils sont utilisés normalement côté client.**

- Les autorisations sont acquises et enregistrées par le Contrôle, qui remplit en temps réel la liste des ID de périphériques autorisés de la machine (voir #8). Elles peuvent être révoquées ou élevées à tout moment si nécessaire.
- Si un système client est déconnecté du Contrôle pendant que le Mode AA est actif, AA se désactive automatiquement et la protection devient effective. Lorsque le client se reconnecte, le Mode AA se réactive automatiquement.
- Si le Contrôle est fermé, le Mode AA se désactive pour **tous les clients**, et la protection devient effective.

**IMPORTANT: Les clients ne seront pas efficacement protégés tant que le Mode AA n'est pas désactivé.** Si le Mode AA n'est pas désactivé manuellement, il se désactivera automatiquement après **48 heures**.

## 10) Mode d'Autorisation Automatique sur des Machines Spécifiques

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



## 11) Gérer les Groupes

### Panneau de Statut des Groupes

GROUPS STATUS							
usb	cd	bt	wf	k. i.	mon	count	group name
U	U	U	U	OFF	ON	2	Default
P	P	P	U	ON	ON	197	Production
P	P	P	U	ON	OFF	1	Office
U	U	U	U	OFF	OFF	0	4
U	U	U	U	OFF	OFF	0	5

Buttons: Change, STOP, Enforce

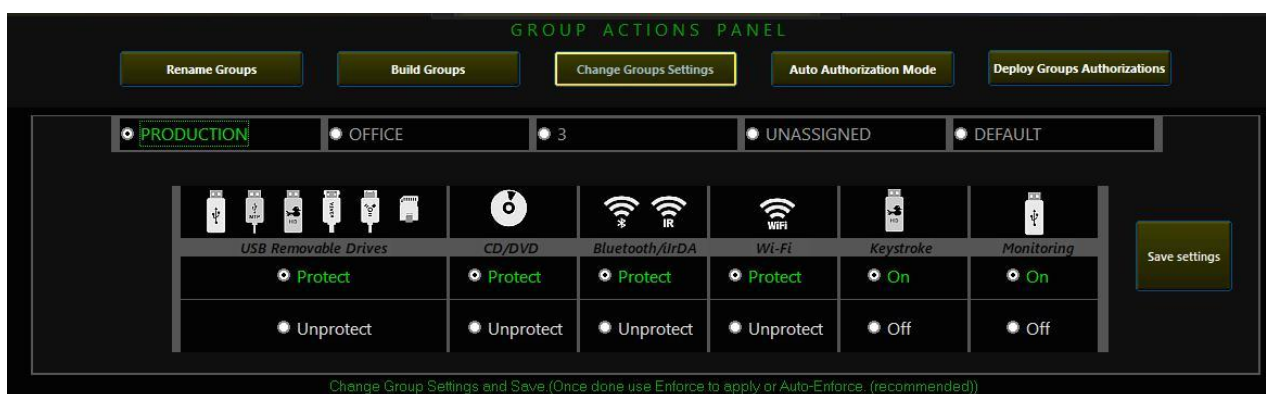
130

#### Fonctionnalités :

- **Afficher le statut de protection de tous les groupes en un coup d'œil.** (Interface principale)
- **Application des Groupes :** Applique les paramètres des groupes. (Un passage pour toutes les machines connectées) (Interface principale)
- **Auto-Application des Paramètres des Groupes :** Surveillance continue des paramètres des groupes. (Interface principale)

**Remarque :** L'**Auto-Application** réglée sur **ON** est le mode recommandé d'opération. Lorsque les paramètres sont modifiés, les machines non connectées recevront automatiquement les nouveaux paramètres une fois qu'elles se reconnecteront.

- Appuyez sur Modifier pour Configurer/Changer les Paramètres de Protection :



- 1) Sélectionnez un Groupe
- 2) Modifiez les paramètres
- 3) Appuyez sur Enregistrer les Paramètres
- 4) Appuyez sur Appliquer ou Auto-Appliquer pour valider

## 12) Autres Actions de Groupe

Pour accéder au panneau d'Actions de Groupe, appuyez sur le bouton vert.

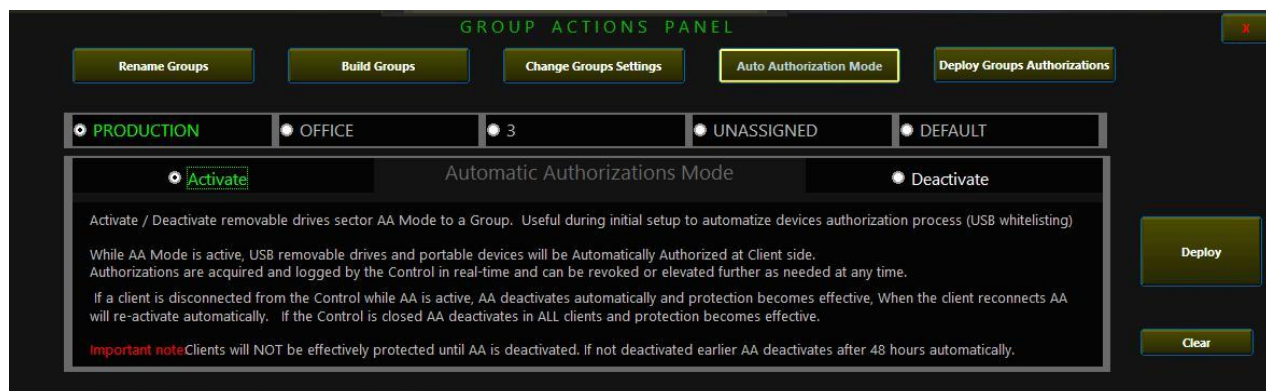


Actions de Groupe Disponibles:

- **Créer des Groupes :**  
La fonction de création de groupes permet de déplacer massivement des machines dans des groupes.
- **Renommer les Groupes :**  
Cinq groupes sont disponibles par défaut (1, 2, 3, 4 et 5).  
Vous pouvez changer les noms des groupes à tout moment. (Nommer les groupes est optionnel.)
- **Configurer/Changer les Paramètres de Protection : (Également accessible directement depuis le Panneau de Statut des Groupes)**  
Protège ou désactive la protection des secteurs et configure la prévention des injections de frappes clavier et la surveillance (ON/OFF) pour le groupe sélectionné. (Appuyez sur Appliquer ou Auto-Appliquer pour valider.)
- **Mode d'Autorisation Automatique : (Fonction avancée/recommandée)**  
Met automatiquement en liste blanche les lecteurs amovibles et les périphériques portables utilisés sur les machines finales sans perturber les opérations normales. (Peut être activé/désactivé au niveau du groupe ou des machines spécifiques).  
Pour plus d'informations, consultez : #10.
- **Déployer les Autorisations au Groupe sélectionné :**  
Specific devices (Complete ID) or by Vendor/Model (VID/PID) match. To populate the list see: (#12) *Elevating authorized IDs to Groups*.

## 13) Mode d'Autorisation Automatique pour les Groupes

(Activer/Désactiver le Mode AA au niveau du Groupe)



- 1) Sélectionnez un Groupe
- 2) Sélectionnez Activer ou Désactiver
- 3) Appuyez sur Déployer

## 14) Déploiement d'Autorisations pour les Groupes

**Remarque:** Lorsqu'un nouvel ID de périphérique est élevé au panneau d'autorisations du Groupe

Le Bouton **Actions de Groupe** sera souligné en orange, indiquant qu'un nouveau périphérique a été ajouté et doit être déployé.

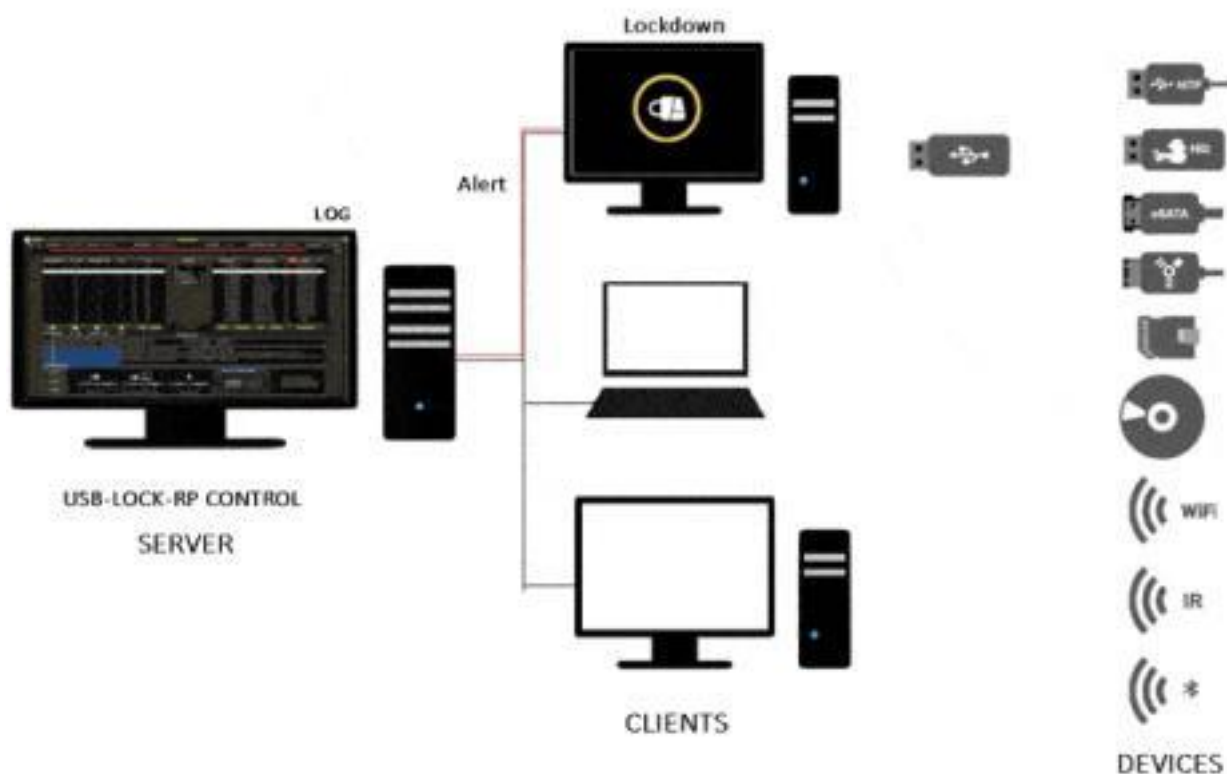


**Remarque:** Vous pouvez continuer à élever des périphériques dans la liste. 60 ID peuvent être élevés pour chaque groupe.



Appuyez sur Développer pour afficher les détails, supprimer des autorisations ou définir un mot de passe maître pour le groupe. Une fois terminé : **Sélectionnez un Groupe et appuyez sur Déployer.**

## 15) Comportement de Blocage (Côté Client)



Le verrouillage USB (blocage côté client) fait partie des mesures redondantes du logiciel appliquées pour protéger le système. Ces mesures sont activées lors de la détection et incluent la prévention du chargement des pilotes, l'arrêt, le démontage, la désactivation, l'éjection des périphériques ainsi que le blocage de l'accès au bureau.

Les mesures de protection s'intensifient en fonction du type et du statut du périphérique, mais le verrouillage est normalement inclus lors du blocage des périphériques USB et autres supports amovibles dans le cadre de la protection logicielle.

Le blocage et le verrouillage du bureau sont simultanés et présentent des alertes en plein écran qui s'étendent sur plusieurs écrans et restent visibles jusqu'à ce que l'une des conditions suivantes soit remplie :

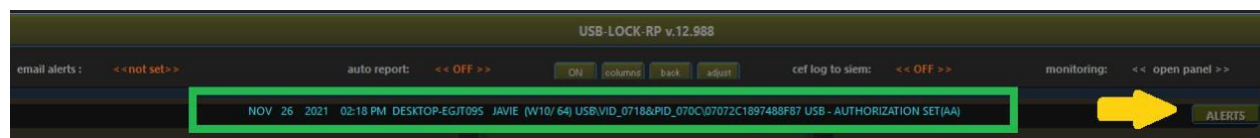
- Le périphérique non autorisé est retiré. (Côté client)
- Le mot de passe maître est utilisé. (Côté client)
- Le secteur est désactivé. (Côté contrôle)
- Le périphérique est autorisé. (Côté contrôle)



## 16) Alertes (Côté Contrôle)

La dernière alerte reçue s'affichera sur le haut de l'écran. Appuyez sur le bouton ALERTES pour développer la vue et consulter les alertes pour toutes les machines du réseau.

**Remarque:** Enregistre automatiquement en temps réel les alertes d'insertion autorisées, bloquées ou approuvées.



Journal des Alertes Réseau:  
Affiche les alertes pour tous  
les clients.

showing 1539 records

Network Alerts Log:						
date	time	machine	user	os   bit	message	action
2024-04-03	10:26:39 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00,6&2A80105C&0&0000 APPLE IPHONE	AUTHORIZED
2024-04-03	10:26:21 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00,6&2A80105C&0&0000 APPLE IPHONE	AUTO_SET(AA)
2024-04-03	10:22:35 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00,6&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:22:08 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00,6&2A80105C&0&0000 APPLE IPHONE	BLOCKED
2024-04-03	10:21:47 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00,6&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:19:58 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_05AC&PID_12A8&MI_00,6&2A80105C&0&0000 APPLE IPHONE	CONNECTED
2024-04-03	10:13:37 AM	DESKTOP-EGJT09S	JAVIE	W10/ 64	USB\VID_152D&PID_1561\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\AA34045800000046 HP_V165W	AUTHORIZED
2024-04-03	10:11:18 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_03F0&PID_5307\AA34045800000046 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\AA34045800000046	EJECTED
2024-04-03	10:11:06 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_03F0&PID_5307\AA34045800000046 HP_V165W	BLOCKED
2024-04-03	10:10:55 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_346D&PID_5678\4824451206115613250 VENDORCO_PRODUCTCODE	AUTHORIZED
2024-04-03	10:10:26 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_346D&PID_5678\4824451206115613250 VENDORCO_PRODUCTCODE	AUTO_SET(AA)
2024-04-03	10:09:59 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USB\VID_346D&PID_5678\4824451206115613250 VENDORCO_PRODUCTCODE	BLOCKED
2024-04-03	09:38:43 AM	SURFACEPRO-1064	ANDREA JAVIE	W10/ 64	USBSTOR\DISK&VEN_HP&PROD_V165W&REV_8192\AA34045800000046	EJECTED

Vue des alertes réseau avec code couleur pour faciliter l'identification des alertes en un coup d'œil:

- Bloqué, Éjecté, Désinstallé = ROUGE
- Autorisé, Approuvé, Autorisation Appliquée = VERT
- En Charge, Connecté = OR
- Contrôle Démarré, Contrôle Fermé = GRIS

**Journal Historique du Client :**

- Sélectionnez un PC client dans la liste réseau.
- Double-cliquez pour ouvrir le journal historique de la machine.

DESKTOP-EGJT09S machine history log		showing: 1483 records out of: 1483	
11/25/21	2:10:59PM	USB\VID_03F0&PID_5307\AA34045800000046 USB	ALLOWED CLIENT*
11/25/21	2:09:19PM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: ON	ENFORCED CONTROL*
11/25/21	2:08:06PM	USB\VID_03F0&PID_5307\AA34045800000046 USB	ALLOWED CLIENT*
11/25/21	2:03:02PM	KEYSTROKE INJECTION PREVENTION	TURNED OFF CLIENT*
11/25/21	2:03:00PM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*
11/25/21	2:01:43PM	REMOV. DRIVES: P CD: P BLUETOOTH: P WIF: U K.I. PREVENT: ON MONITORING: ON	ENFORCED CONTROL*
11/25/21	2:00:38PM	KEYSTROKE INJECTION PREVENTION	TURNED ON CLIENT*
11/25/21	2:00:36PM	REMOV. DRIVES: P CD: P BLUETOOTH: P WIF: U K.I. PREVENT: ON MONITORING: ON	ENFORCED CONTROL*
11/24/21	9:15:55AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*
11/24/21	8:52:22AM	REMOV. DRIVES: P CD: P BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*
11/24/21	8:52:17AM	REMOV. DRIVES: U CD: P BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*
11/24/21	8:52:12AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*
11/24/21	1:13:15AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*
11/24/21	1:13:14AM	CD DVD	PROTECTED CONTROL*
11/24/21	1:13:12AM	CD DVD	UNPROTECTED CONTROL*
11/24/21	1:13:08AM	CD DVD	PROTECTED CONTROL*
11/24/21	12:57:42AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*
11/24/21	12:57:41AM	CD DVD	PROTECTED CONTROL*
11/24/21	12:48:44AM	REMOV. DRIVES: U CD: U BLUETOOTH: U WIF: U K.I. PREVENT: OFF MONITORING: OFF	ENFORCED CONTROL*

Le journal historique de la machine inclut toutes les alertes reçues provenant de la machine ainsi que les paramètres déployés depuis le contrôle vers la machine.

## 17) Fonctionnalité du Mot de Passe Principal

PORTÉE : Niveau du Groupe (Un mot de passe par groupe)

**COMPORTEMENT** : Lorsqu'un écran d'alerte de blocage reste affiché plus de 25 secondes sur une machine cliente, une boîte de saisie de mot de passe apparaît et peut être utilisée pour entrer le mot de passe maître du groupe afin de reprendre l'accès à la machine cliente.

- **Dans le cas des périphériques USB MTP** (par ex. smartphones), cela permettra de reprendre l'accès au bureau et d'autoriser l'utilisation du périphérique pour une seule fois.
- **Dans le cas des lecteurs USB**, cela permettra uniquement de reprendre l'accès au bureau.



Utile pour:

- Dépannage : Reprendre l'accès au bureau si un périphérique interne, à tort signalé comme amovible, est bloqué et que le Contrôle est inaccessible.

Le programme est livré avec un mot de passe maître personnalisé. Cependant, il est recommandé de changer ce mot de passe et d'en définir un pour chaque groupe utilisé.

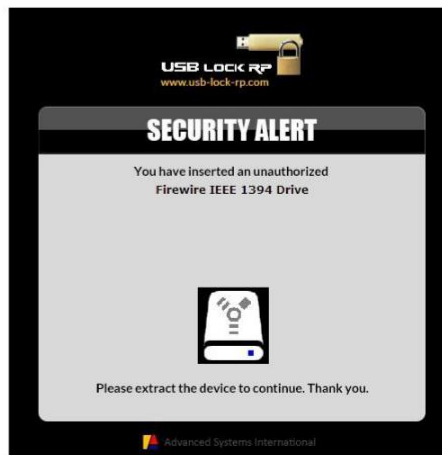
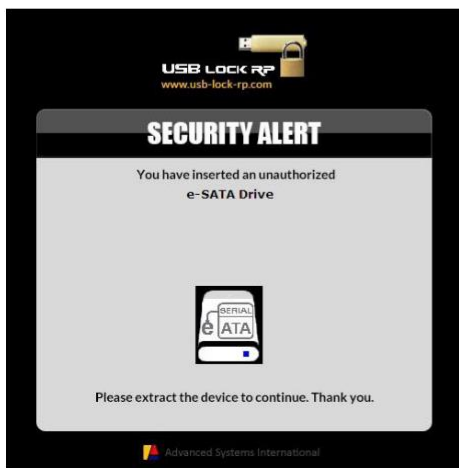
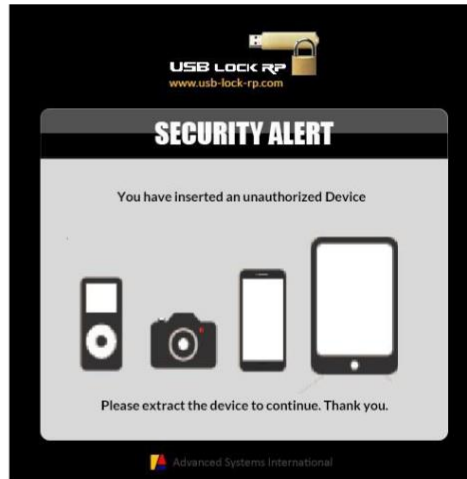
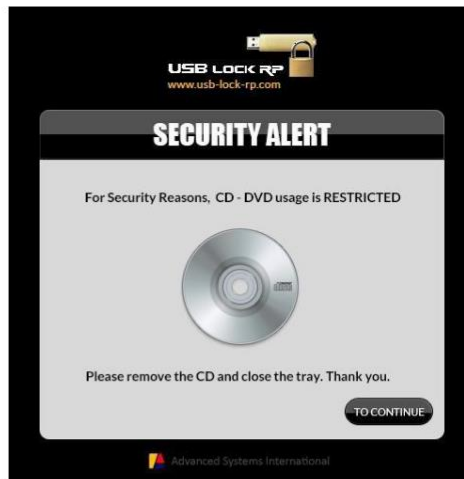
Le mot de passe, ainsi que tous les paramètres critiques du programme et les ID, sont stockés de manière cryptée (uniquement lisibles depuis l'interface du Contrôle).

Depuis le Contrôle : Le mot de passe maître peut être déployé sur des groupes de machines depuis le panneau d'autorisations des groupes. **Consultez la section 14 (Déploiement des Autorisations aux Groupes)**

## 18) Écrans d'Alerte (Côté Client)

Alertes en plein écran (S'étendent à tous les moniteurs)

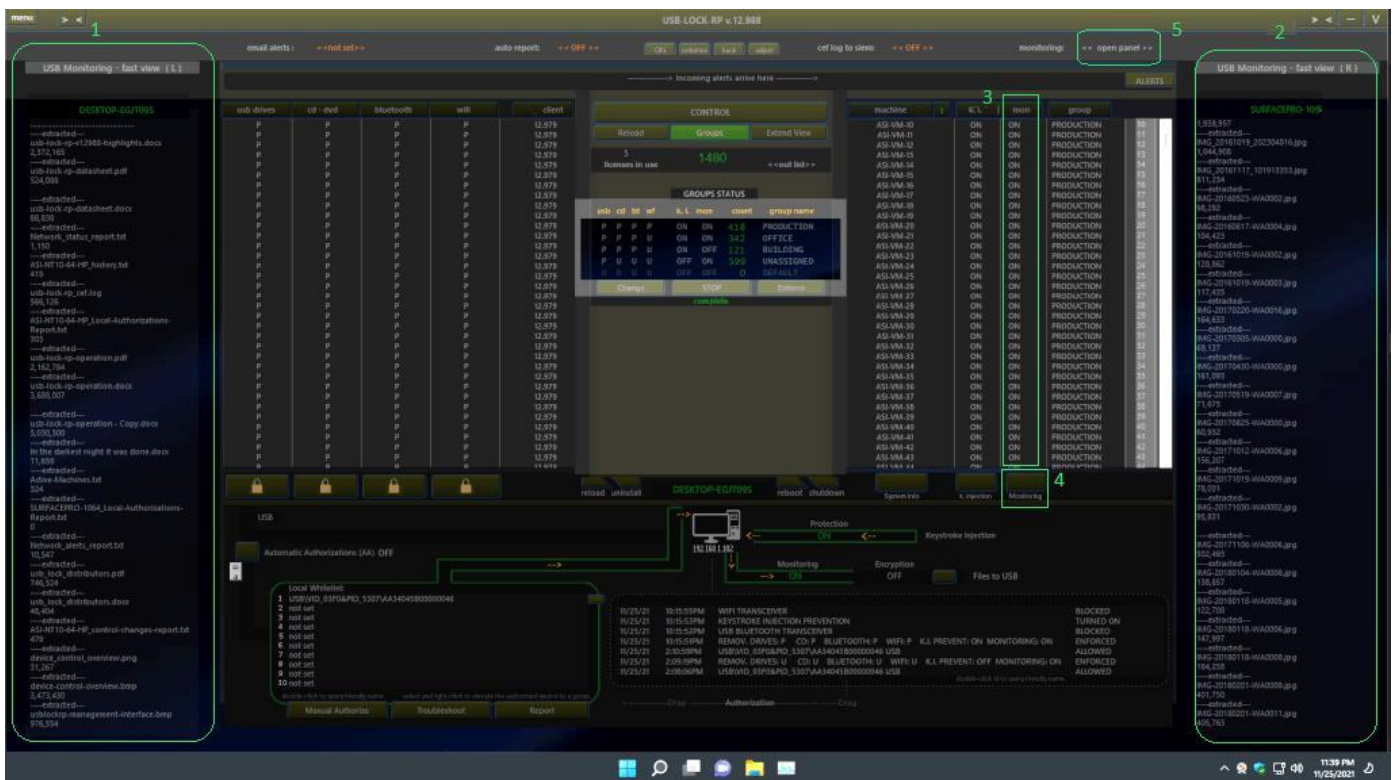
Les alertes suivantes s'affichent sur les clients en fonction du type de périphérique bloqué.



Petites alertes sans fil : (apparaissent dans le coin inférieur droit)



## 19) Surveillance des Fichiers vers USB



1. Panneau de Vue Rapide de Surveillance à Gauche
2. Panneau de Vue Rapide de Surveillance à Droite
3. Statut de la Surveillance
4. Activer ou Désactiver la Surveillance
5. Ouvrir le Panneau Principal de Surveillance

Les données surveillées incluent le nom et le poids exact des fichiers transférés depuis le PC client vers les lecteurs flash, l'utilisateur connecté, l'ID matériel du périphérique, le nom de la machine source, ainsi que la date/heure de début de l'événement.

Les enregistrements sont envoyés chiffrés en AES 256 et masqués en Hex depuis l'ordinateur client vers le contrôleur en quasi-temps réel. Ils sont organisés au niveau du contrôleur par nom de machine client/date/heure pour une consultation au besoin.

Sur le serveur central de contrôle, les données restent chiffrées, comme tous les événements enregistrés, et ne sont lisibles qu'au sein de l'interface de Contrôle des Périphériques.

## 20) Chiffrement des Clés USB

Forcer le chiffrement automatique des lecteurs autorisés : Cette fonction peut également être activée ou désactivée en un seul clic. (La surveillance USB doit être activée pour que le chiffrement puisse être configuré). Lorsque le chiffrement USB est actif, tous les fichiers transférés depuis l'ordinateur client vers les clés USB autorisées sont automatiquement chiffrés en AES 256. (Toutes les données, pas seulement les en-têtes).

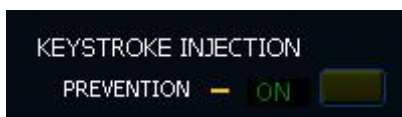
Les fichiers stockés sur des clés USB chiffrées peuvent être ouverts sur le client d'origine ou sur tout autre client USB-Lock-RP ayant le chiffrement USB activé. Sur ces systèmes, les fichiers sont automatiquement déchiffrés lorsqu'ils sont double-cliqués.

Alternativement, les fichiers peuvent être déchiffrés sur ces systèmes en les transférant dans le dossier nommé : decryptor.

(Situé à la racine du répertoire de la machine cliente).

Cette fonction garantit que les informations contenues dans les périphériques autorisés ne sont accessibles que sur des ordinateurs déterminés au sein du réseau, et sur aucun en dehors du réseau.

## 21) Protection contre les Attaques par Injection de Frappes



Le secteur des lecteurs amovibles inclut une protection contre les périphériques badUSB, tels que le USB Rubber Ducky. Ce type de périphérique est extrêmement dangereux car son firmware a été modifié pour imiter des périphériques d'interface humaine (HID), tels que les claviers, et est capable d'effectuer des attaques par injection de frappes et d'introduire des charges malveillantes pour endommager le système d'exploitation et l'infrastructure réseau.

Le blocage de ce type de périphérique est une fonction standard de USB-Lock. Le programme effectue une analyse rapide lorsqu'il détecte un changement dans l'énumération du clavier/souris, ce qui déclenche une évaluation automatique pour neutraliser la menace si elle est présente. Ces événements, comme toutes les tentatives d'insertion au niveau des clients, sont signalés au Contrôle Central en quasi-temps réel.

Vous pouvez exclure les claviers connectés de l'analyse dans le cas où celle-ci serait intrusive, notamment pour les claviers détachables des ordinateurs portables/tablettes, les stylos intelligents ou les stations d'accueil. Mais en règle générale, aucune action n'est nécessaire.

## 22) Fonction Informations Système



Fonction de Découverte : Fournit en temps réel des informations côté client sur :

- Stockage amovible connecté (y compris les smartphones)
- Adaptateurs réseau (y compris l'adresse MAC)
- Imprimantes (y compris les files d'attente d'impression)
- Périphériques HID (descripteurs de bas niveau)
- Données de la machine
- Utilisateur connecté
- Logiciels installés
- Processus en cours d'exécution

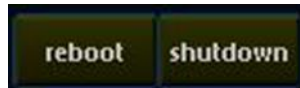
The screenshot displays the 'SURFACEPRO-1064' system information tool with the following sections:

- System Information:**
  - Date/Time: 4/26/2024 2:04:20 PM
  - Machine name: SURFACEPRO-1064
  - IP address: 192.168.1.105
  - Logged user: JAVIE
  - Manufacturer: Microsoft Corporation
  - Model: Surface Pro 4
  - Processor: Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz
  - Processors: 4
  - Processors Speed: 2496Mhz
  - Memory RAM: 4017 MB
  - OS: Windows 10 Enterprise 64 Bit
- Removable Storage / Mobile phones:**
  - Device Name: USB Drive (D:)
  - Device Type: USB Drive
  - Device Path: D:\
  - Id: 5A834045B00000046
  - Size: 7.00 GB
  - Free: 7.38 GB
  - File System: NTFS
- Printers / Printer queue:**
  - Device Name: Canon E400 series Printer
  - Status: Offline
  - Device Name: Fax
  - Status: Ready
  - Device Name: Microsoft Print to PDF
  - Status: Ready
  - Device Name: Microsoft XPS Document Writer
  - Status: Ready
  - Device Name: Send To OneNote 2013
  - Status: Ready
  - Device Name: OneNote for Windows 10
  - Status: Ready
- HID (Human interface device):**
  - Surface Dock Extender
  - Microsoft
  - VID: 0x045E, PID: 0x0904
  - SerialNumber: None
  - NumConfigurations: 0x01
  - Device Bus Speed: Full
  - Device Address: 0x07
  - MaxPower: 0x2 (100 mA)
  - Total Open Pipes: 2
  - Pipe 1: Interface: 0, Interface number: 0, bInterfaceClass: 0x03 (HID), bInterfaceProtocol: 0x00 (Undefined)
  - Pipe 1: Endpoint: bEndpointAddress: 0x81 IN, Transfer Type: 3 (Interrupt), wMaxPacketSize: 0x0040 (64), bInterval: 0x01
  - Pipe 2: Endpoint: bEndpointAddress: 0x02 OUT, Transfer Type: 3 (Interrupt), wMaxPacketSize: 0x0040 (64), bInterval: 0x01
- Installed Software:** (Empty)
- Running Processes:** (Empty)
- Network Adapters:**
  - Surface Type Cover
  - Microsoft
  - VID: 0x045E, PID: 0x07E8
  - SerialNumber: None
  - NumConfigurations: 0x01
  - Device Bus Speed: Full
  - Device Address: 0x22
  - MaxPower: 0x2 (100 mA)
  - Total Open Pipes: 2
  - Pipe 1: Interface: 0, Interface number: 0, bInterfaceClass: 0x03 (HID), bInterfaceProtocol: 0x00 (Undefined)
  - Pipe 1: Endpoint: bEndpointAddress: 0x81 IN, Transfer Type: 3 (Interrupt), wMaxPacketSize: 0x0040 (64), bInterval: 0x01
  - Pipe 2: Endpoint: bEndpointAddress: 0x02 OUT, Transfer Type: 3 (Interrupt), wMaxPacketSize: 0x0040 (64), bInterval: 0x01

Buttons: Refresh, Export



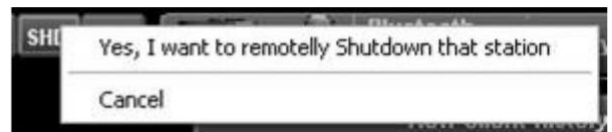
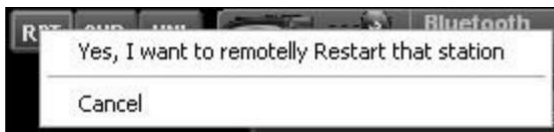
## 23) Fonction Redémarrer & Redémarrer (Ordinateur Client)



Permet de redémarrer ou d'éteindre l'ordinateur client sélectionné à distance depuis le contrôle.

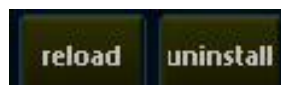
- Sélectionnez une machine cliente dans la liste réseau.
- Appuyez sur le bouton **Redémarrer** ou **Éteindre**.

Lorsque vous appuyez sur le bouton correspondant, une fenêtre contextuelle s'affiche pour demander une confirmation afin d'éviter l'exécution accidentelle de la commande.



Lorsque vous exécutez l'une des commandes, un message s'affiche à l'écran du client, informant l'utilisateur qu'il dispose de 10 secondes pour sauvegarder son travail avant que l'action de redémarrage ou d'arrêt ne soit effectuée.

## 24) Fonctions Recharger & Désinstaller (Service Client)



Sélectionnez une machine cliente dans la liste réseau. Appuyez sur le bouton Recharger ou Désinstaller.

- Recharger : Réétablit la connexion du client sélectionné.
- Désinstaller : Désinstalle le service USB-Lock-RP installé sur la machine cliente.

Remarque : Cette action désactive également la protection de tous les secteurs.

## 25) Fonction Autoriser/Refuser Charge Seule des Smartphones

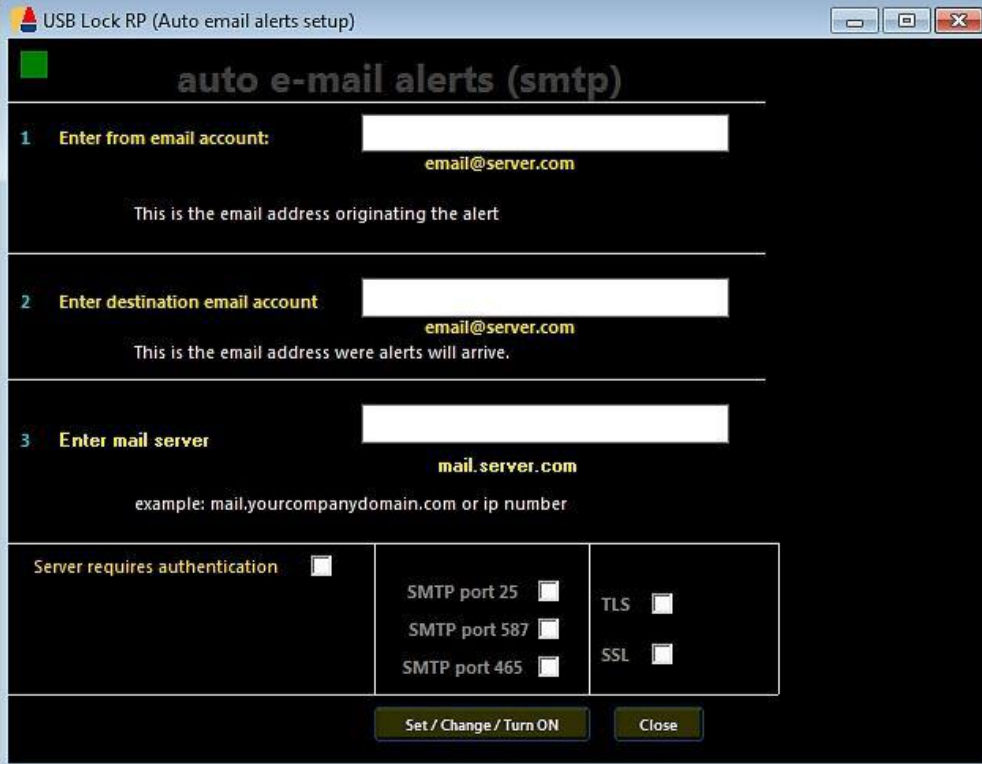


**Nouveau comportement de blocage MTP:** Permet aux smartphones non autorisés d'être connectés uniquement pour la charge sans être bloqués. (Lorsque le paramètre est défini sur Refuser, les smartphones doivent être autorisés, même pour une connexion uniquement pour la charge.)

## 26) Fonction Alertes Automatiques par Email

Envoyez automatiquement TOUTES les alertes entrantes reçues par le Contrôle à une adresse email de votre choix au sein de votre domaine (à utiliser comme un référentiel centralisé alternatif de journaux).

- Automatique après une configuration simple: Permet SSL / TLS.
  - Vous pouvez sélectionner le type d'alertes à envoyer (y compris les alertes de transfert de fichiers avec les détails du transfert).



The screenshot shows a window titled "USB Lock RP (Auto email alerts setup)" with a dark background and white text. The window is titled "auto e-mail alerts (smtp)". It contains three main sections for configuration:

- 1 Enter from email account:** A text input field containing "email@server.com". Below it, a note states: "This is the email address originating the alert".
- 2 Enter destination email account:** A text input field containing "email@server.com". Below it, a note states: "This is the email address were alerts will arrive."
- 3 Enter mail server:** A text input field containing "mail.server.com". Below it, an example is provided: "example: mail.yourcompanydomain.com or ip number".

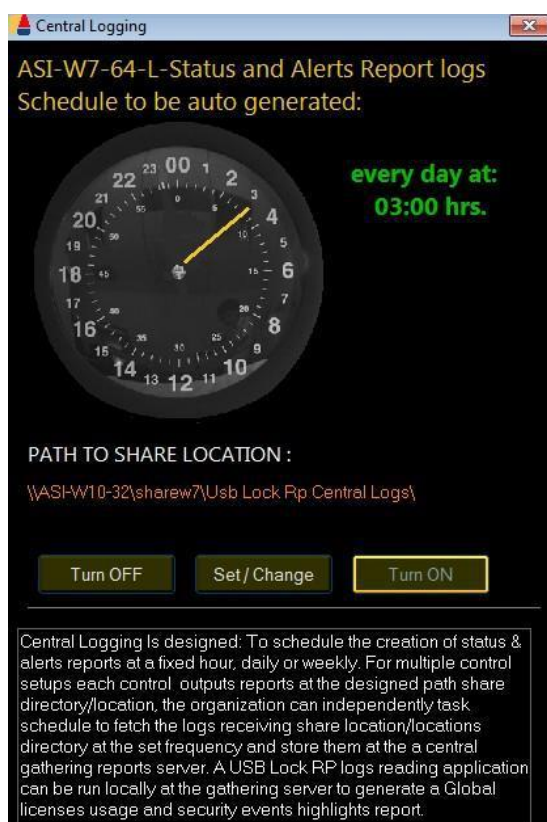
At the bottom, there are several checkboxes for server settings:

- Server requires authentication
- SMTP port 25
- SMTP port 587
- SMTP port 465
- TLS
- SSL

At the very bottom, there are two buttons: "Set / Change / Turn ON" and "Close".

## 27) Rapports Automatiques (Programmation des Rapports)

Planifiez la création automatique de rapports de statut et d'alertes à une heure fixe, quotidiennement ou hebdomadairement, vers un chemin partagé défini.



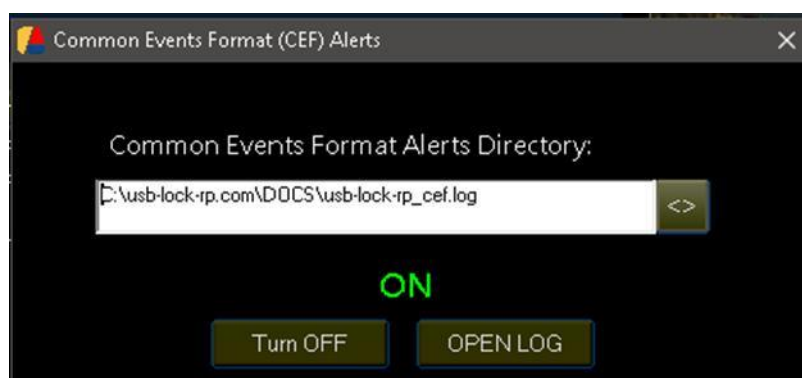
## 28) Journaux CEF (Interopérabilité SIEM)

(Configurer les journaux au format Common Events Format pour l'intégration avec un SIEM)

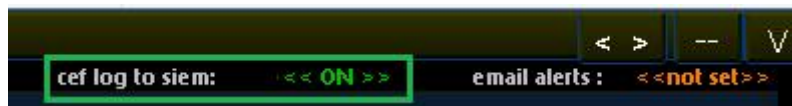
1. Cliquez sur l'étiquette << OFF >>



2. Définir le Chemin



3) Activez (ON) pour enregistrer les événements au format Common Events..



Exemple de format de journal: (Copiez/collez pour afficher les détails)

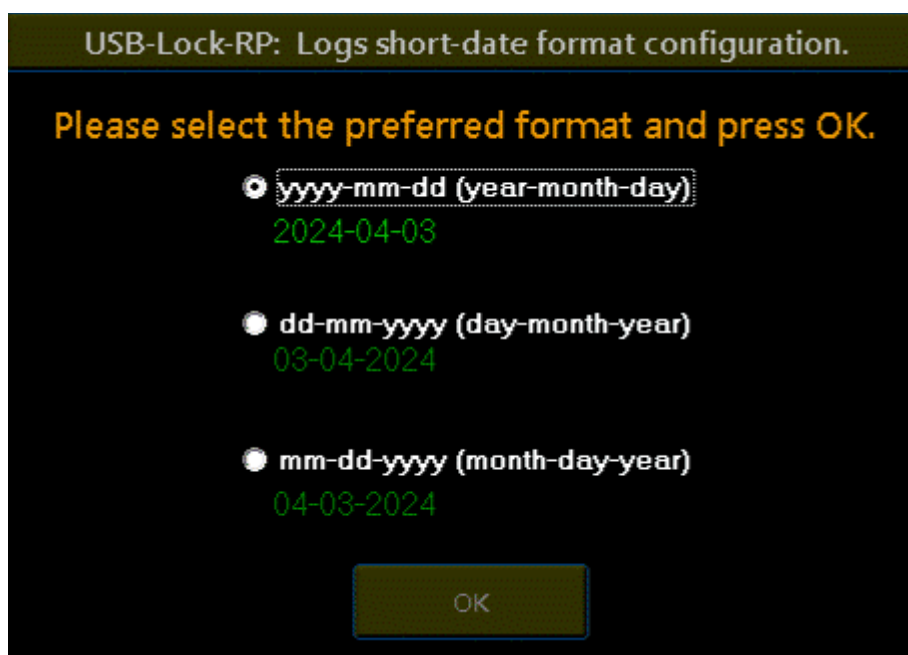
02 juillet 11:15:54 ASI-NT10-64-HP CEF:0|Advanced Systems|USB-LOCK-RP|12.8|104|connexion de périphérique autorisée|7|src=192.168.0.13 msg=ASI-NT10-64-HP JAVIE (W10/ 64) USB\VID\_03F0&PID\_5307\AA34045B00000046 USB - AUTORISÉ

02 juillet 14:10:34 ASI-NT10-64-HP CEF:0|Advanced Systems|USB-LOCK-RP|12.8|103|connexion de périphérique non autorisée bloquée|9|src=192.168.0.13 msg=ASI-NT10-64-HP JAVIE (W10/ 64) USB\VID\_03F0&PID\_5307\AA34045B00000046 USB - BLOQUÉ

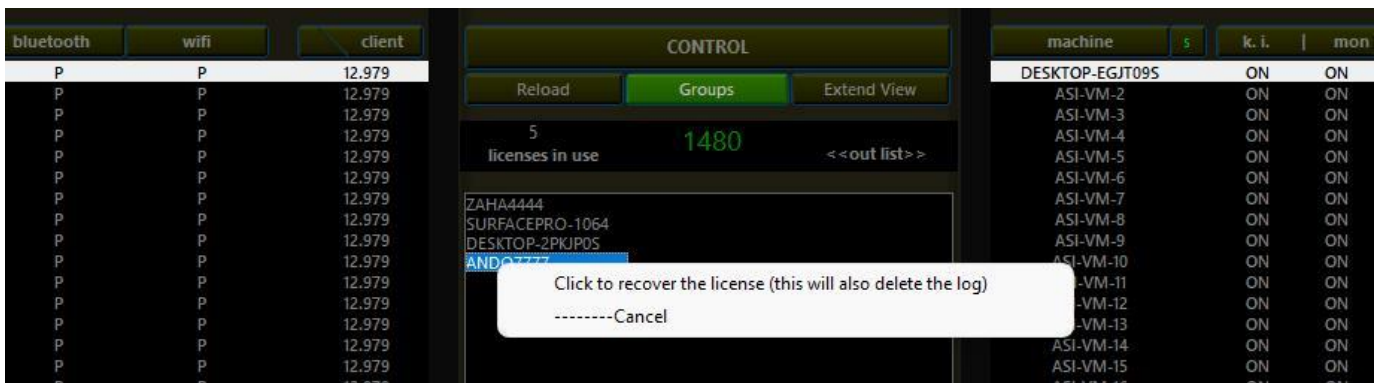
## 29) Configuration du Format de Date des Journaux

Le Panneau de Configuration du Format de Date Court des Journaux apparaîtra automatiquement lors du premier démarrage du Contrôle.

**Remarque:** Il peut également être accessible via: Menu Principal / Panneau des Options Administratives / Fonction de Format de Date Court.



### 30) Clients Connectés & Récupération des Licences



Affiche le nombre de Clients connectés. (1)

<<Liste hors ligne>> affiche une liste des Clients non connectés. (2)

Pour supprimer les PC Clients inutilisés et récupérer des licences. (3)

1. Cliquez sur <<Liste hors ligne>>
2. Sélectionnez une machine dans la liste hors ligne
3. Cliquez sur Récupérer la licence.

Grâce à ces méthodes, USB-Lock-RP permet de récupérer les licences inutilisées.

### 31) Modification du Mot de Passe de Contrôle

**(Utilisé pour changer le mot de passe permettant d'accéder au Contrôle USB-Lock-RP).**

Le programme est livré avec un mot de passe par défaut personnalisé pour le Contrôle :



1. Saisissez l'ancien mot de passe.
2. Saisissez le nouveau mot de passe.
3. Re-saisissez le nouveau mot de passe.

**Change control access password**

Type old password

Type new password

Re-Type new password

NOTE: Password is case sensitive. Numbers, Letters, and Spaces are valid.  
Important: The password need to be at least 8 characters  
Example: 4Rxx12fb

### 32) Fonctions de Gestion Administrative

#### Mode de Fonctionnement du Système de Contrôle:

Permet la gestion en temps réel 24h/24 et 7j/7 de la sécurité USB, l'alerte et l'application des règles. Cette fonction démarre automatiquement le contrôle en mode système lorsqu'un contrôle en mode administrateur n'est pas en cours d'exécution.

**System-Mode Configuration**

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

- Service view -

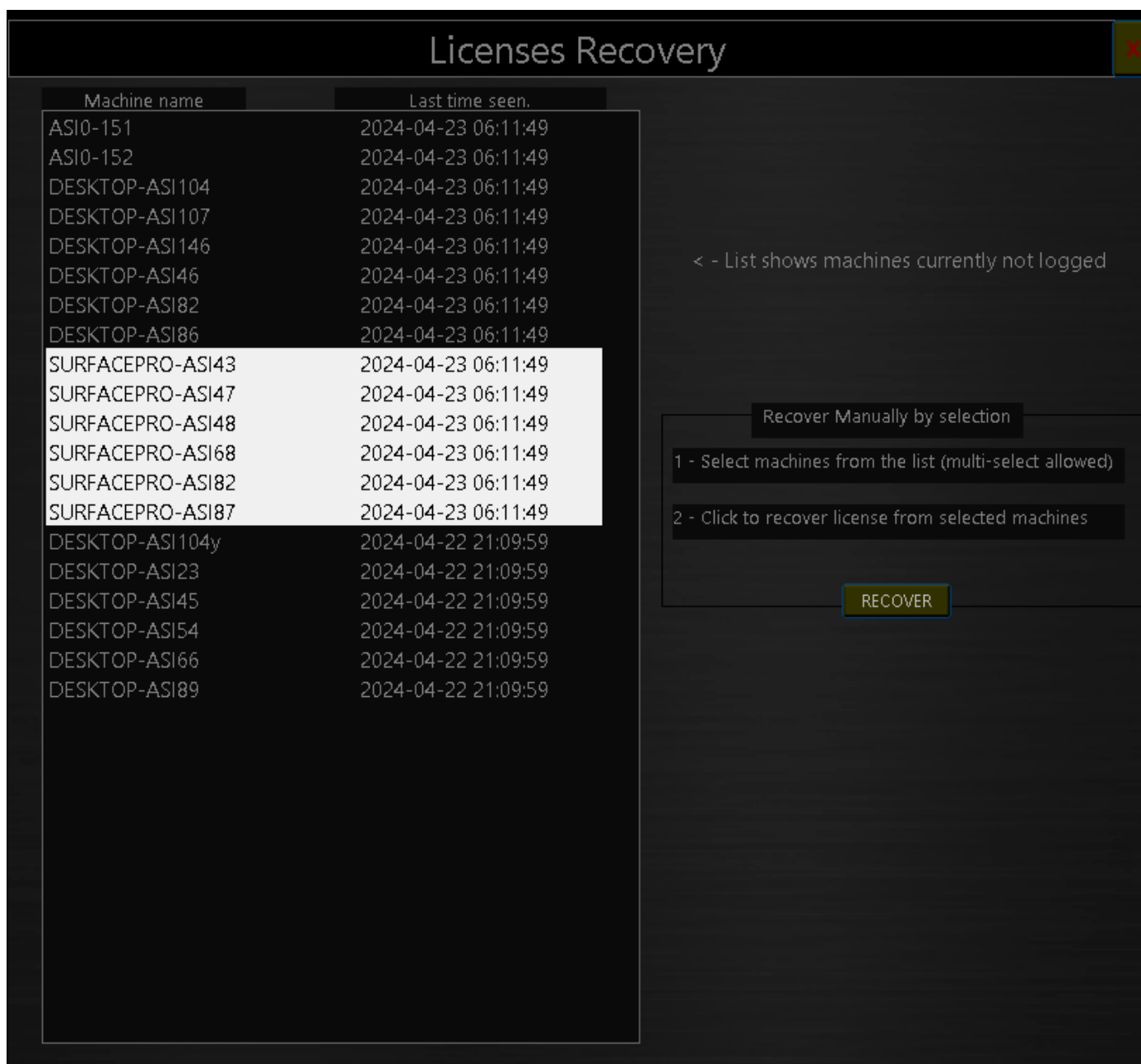
Service name : usblockrpsvc

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

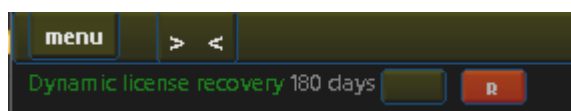
Service status :  State:  Start Type:

## Récupération de Licences:

La fonction de récupération de licences permet de récupérer les licences des machines figurant dans la



liste des machines non connectées, ce qui vous permet de récupérer les licences des machines inutilisées.



Vous pouvez également récupérer des licences de manière dynamique en fonction de la dernière connexion d'un client au contrôle.

L'image montre un paramètre permettant de récupérer les licences des machines qui n'ont pas été vues par le contrôle depuis plus de 6 mois. (Vous pouvez également choisir de récupérer après 2 mois, 3 mois ou 1 an.)

## Out list status check

- List shows machines currently not logged to the control

1 - 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-ASI104y
DESKTOP-ASI104
ASI0-152
```

- Not logged machines that respond to ping  
 Not Expected: This means there is a problem. [ssrv] service is not connecting. To resolve, Please reinstall client. If the problem continues check if the firewall is blocking ssrv from connecting.

- Not logged machines that did not respond to ping  
 Expected: More likely the machine is disconnected from the network or not running. The client should normally log back once the client machine is started or the network connection is reestablished.

### Dépannage de la Connexion :

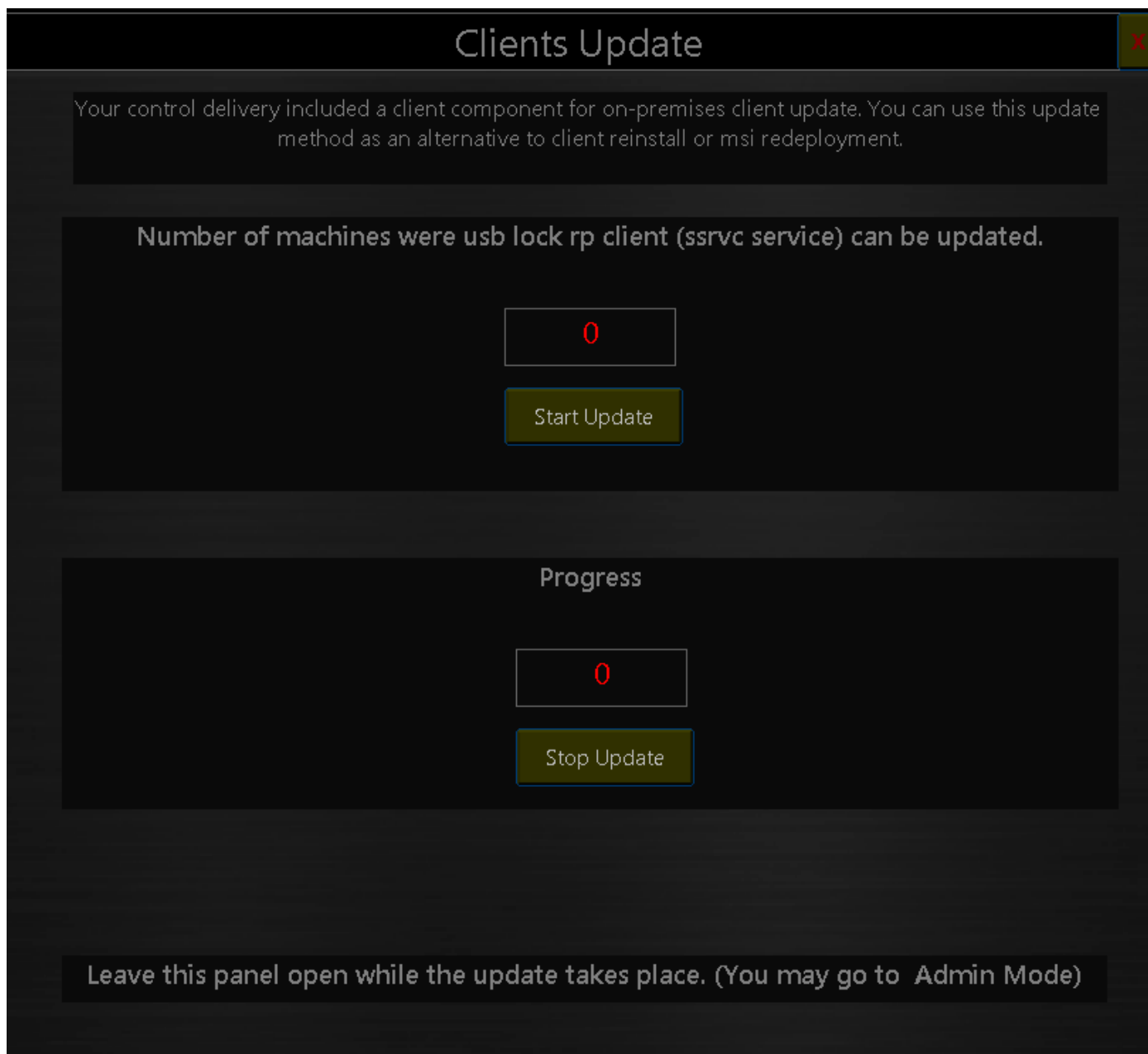
La fonction de diagnostic de la liste hors ligne permet d'envoyer un paquet ICMP (ping) aux machines non connectées pour diagnostiquer leur disponibilité et aider à identifier les problèmes de connectivité des clients.



### Fonction de Mise à Jour des Clients On-Premises :

Le panneau de fonction de mise à jour des clients permet de mettre à jour massivement la version des clients depuis le côté contrôle.

Votre mise à jour du contrôle est toujours livrée avec la dernière version du composant client, vous pouvez ainsi mettre à jour les clients en interne depuis le contrôle. (On-Premises) Aucune connexion en dehors de



The screenshot shows a control panel titled "Clients Update" with a close button (X) in the top right corner. The panel contains the following text and controls:

- Introductory text: "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."
- Section header: "Number of machines were usb lock rp client (ssrvc service) can be updated."
- Count display: A box showing the number "0".
- Action button: A green button labeled "Start Update".
- Section header: "Progress".
- Count display: A box showing the number "0".
- Action button: A green button labeled "Stop Update".
- Footer text: "Leave this panel open while the update takes place. (You may go to Admin Mode)"

votre réseau n'est requise.

### 33) Support Technique

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



[info@usb-lock-rp.com](mailto:info@usb-lock-rp.com)

[www.usb-lock-rp.com](http://www.usb-lock-rp.com)

Telephone:

**+1 (972) 890 9488**

**+44 020 3286 0406**

USB LOCK RP ©: Développeur & Concédant & Support Fondamental

Nous restons à votre disposition.

### 34) Mise en œuvre d'une Politique de Sécurité USB et Liste Blanche

Les points suivants s'appliquent aux réseaux de grande ou petite taille et supposent que le client USB-Lock-RP a déjà été déployé sur les machines du réseau.

Configurer et appliquer une politique de médias amovibles:

1. Allez au panneau des actions de groupe.
2. Renommez et créez des groupes.
3. Définissez les paramètres pour les groupes.
4. Appuyez sur Auto-Appliquer.

#### Mise en Liste Blanche Automatique.

**(Ce qui suit ne conviendra pas à tous les types de réseaux, mais reste la méthode de mise en liste blanche la plus automatique.)**

5. Créez un groupe composé de machines nécessitant l'autorisation (mise en liste blanche) de périphériques.
  6. Cliquez sur le bouton Mode d'Autorisation Automatique.
  7. Activez les Autorisations Automatiques pour "ce groupe".  
(Inversement au blocage, le programme autorisera automatiquement les périphériques connectés.)  
Les utilisateurs côté client du "groupe" fonctionnent normalement en connectant les périphériques qu'ils utilisent habituellement.  
Remarque : Vous pouvez renforcer les restrictions d'accès physique externe aux locaux pendant ce processus.
- Les périphériques de stockage amovible et portables connectés seront automatiquement ajoutés à la liste locale des ID autorisés au niveau du contrôle.
8. Désactivez les Autorisations Automatiques pour ce groupe. (Après quelques heures)  
AA se désactive et la sécurité devient effective. Les lecteurs amovibles ou smartphones non autorisés seront bloqués.

**Les périphériques autorisés (mis en liste blanche) peuvent être connectés et utilisés normalement.**

Vous pouvez maintenant révoquer en temps réel toutes les autorisations indésirables ou les élever davantage au niveau des groupes.

Vous pouvez également configurer l'interopérabilité SIEM, programmer des rapports automatiques, recevoir des alertes par email, surveiller les transferts vers les USB autorisés...