Contrôle des périphériques

Différence entre "Drives" et "Devices"

Drives

DriveLock traite tout ce qui se voit attribuer une lettre de lecteur sous Windows comme un lecteur (*drive*). Un filtre sera posé pour les lecteurs, permettant un contrôle dynamique pour lequel généralement aucun redémarrage ou nouvelle connexion n'est nécessaire.

En principe, tous les types de lecteurs peuvent être contrôlés par DriveLock, pas seulement les supports amovibles ; même les lecteurs réseau et les disques durs locaux peuvent être contrôlés en option.

Drive type	Status	Tasks	Options
CD-ROM drives	Locked with exceptions	Properties... Set to 'Not Configured'	Audited
Encrypted volumes	Not configured (Not locked)	Properties...	
Via Firewire (1394) connected devices	Locked with exceptions	Properties... Set to 'Not Configured'	Audited
Fixed disks	Not configured (Not locked)	Properties...	
Floppy disk drives	Locked with exceptions	Properties... Set to 'Not Configured'	Audited
Network drives and shares	Not configured (Not locked)	Properties...	
Other removable drives	Locked with exceptions	Properties... Set to 'Not Configured'	Audited
SD bus-connected drives	Locked with exceptions	Properties... Set to 'Not Configured'	Audited
Drives connected via USB	Not locked	Properties... Set to 'Not Configured'	Filtered
WebDAV-based network drives	Not configured (Not locked)	Properties...	

Devices

DriveLock considère tout ce qui n'est pas directement connecté à une lettre de lecteur comme un appareil (*device*).

Le contrôle des appareils se fait par catégories, qui sont calquées sur celles du gestionnaire de Windows.

Device type	Status	Tasks
Bluetooth transmitters / radios	Not configured (Not locked)	Properties... Add whitelist rule...
Infrared interfaces	Not configured (Not locked)	Properties... Add whitelist rule...
Media player / Portable devices	Not configured (Not locked)	Properties... Add whitelist rule...
Modems	Not configured (Not locked)	Properties... Add whitelist rule...
Printers	Not configured (Not locked)	Properties... Add whitelist rule...
Scanners and cameras	Not configured (Not locked)	Properties... Add whitelist rule...
Smartcard readers	Not configured (Not locked)	Properties... Add whitelist rule...
Tape drives	Not configured (Not locked)	Properties... Add whitelist rule...
Smartphones		
Android	Whitelist rules active	Properties... Add whitelist rule... Set to 'Not Configured'
Apple	Locked with exceptions	Properties... Add whitelist rule... Set to 'Not Configured'
BlackBerry devices	Whitelist rules active	Properties... Add whitelist rule... Set to 'Not Configured'
Mobile phones	Whitelist rules active	Properties... Add whitelist rule... Set to 'Not Configured'
Palm OS devices	Whitelist rules active	Properties... Add whitelist rule... Set to 'Not Configured'
Windows Mobile devices	Whitelist rules active	Properties... Add whitelist rule... Set to 'Not Configured'

Règles de liste blanche

Après avoir activé le verrouillage pour une classe de périphériques, tout périphérique de cette classe sera bloqué. Pour définir une exception au blocage des périphériques, vous devez créer des règles de liste blanche. Cela signifie que vous devez définir une règle de liste blanche pour chaque périphérique (ou groupe de périphériques similaires) que vous devrez utiliser sur un ordinateur.

Si un périphérique n'est pas reconnu par l'agent DriveLock comme étant répertorié dans une règle de liste blanche, DriveLock bloquera le périphérique et il ne pourra pas être utilisé. Cela garantit que tous les nouveaux périphériques introduits sur votre réseau par les utilisateurs seront automatiquement bloqués jusqu'à ce que vous autorisiez explicitement leur utilisation.

Pour ajouter un périphérique en liste blanche, des informations peuvent être facilement lues en direct à partir d'un agent, ou en utilisant une précédente analyse de périphériques :

- ID du fabricant > Nom ou abréviation du fabricant du périphérique
- Identifiant de produit > Identifiant unique de produit émis par le fabricant
- Numéro de série > Caractéristique d'identification unique du périphérique

La combinaison ID du fabricant / de produit et numéro de série rend un périphérique unique.

NB : Veuillez noter qu'une même règle ne doit jamais être présente deux fois, car DriveLock n'utilisera que la première règle correspondante.

Quels points faut-il prendre en compte ?

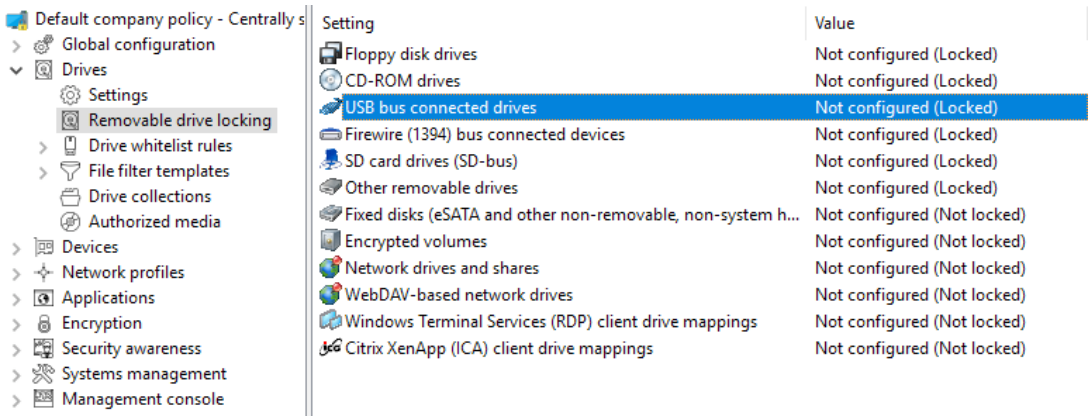
- Règles de politique de base <> règles de listes blanches individuelles
- Clés USB d'entreprise <> clés USB privées/existantes

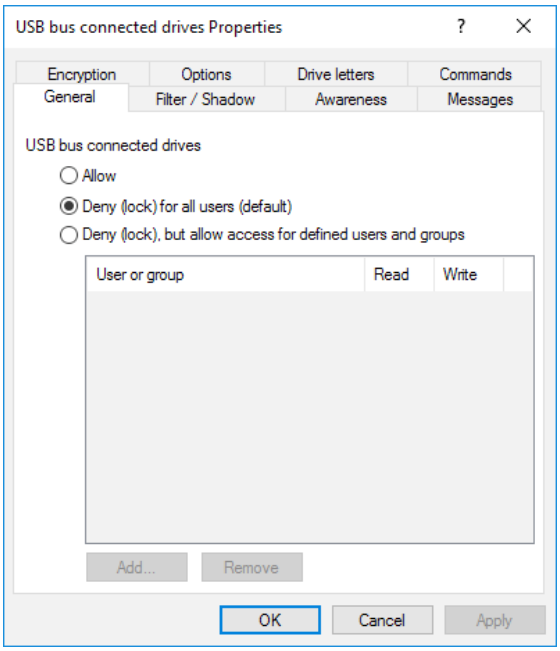
- Contrôle d'accès global uniquement <> autorisations utilisateur/ordinateur supplémentaires
- Contrôle supplémentaire grâce au filtrage par types de fichiers
- Considérations relatives à la journalisation des événements
- Chiffrement forcé (Encryption-2Go <> File & Folder Encryption <> BitLocker To Go)
- Politique d'utilisation <> Campagne de sensibilisation à la sécurité

Cas pratique : blocage des clés USB

Dans **Drives** > **Removable drive locking**, vérifiez que la catégorie "USB bus connected drives" est bloquée pour tout le monde (défini comme tel par défaut pour chaque nouvelle politique, même si des exceptions pour des utilisateurs ou des groupes peuvent être mises en place).

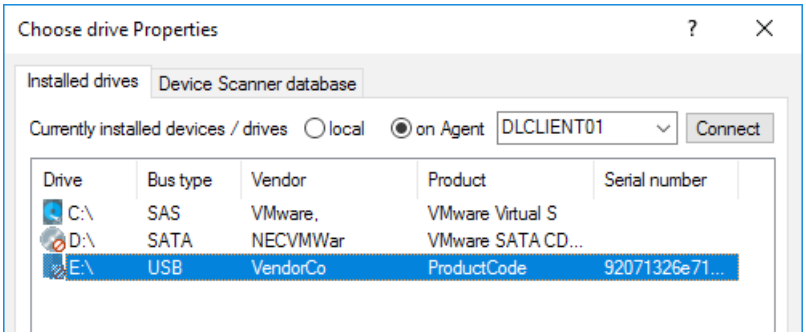
Enregistrez, publiez puis déployer la politique pour tester le comportement sur un poste client en essayant de connecter une clé USB.





Dans l'explorateur Windows, l'accès est refusé lorsque vous double-cliquez sur la clé USB pour essayer d'y accéder, avec un message d'avertissement qui s'affiche.

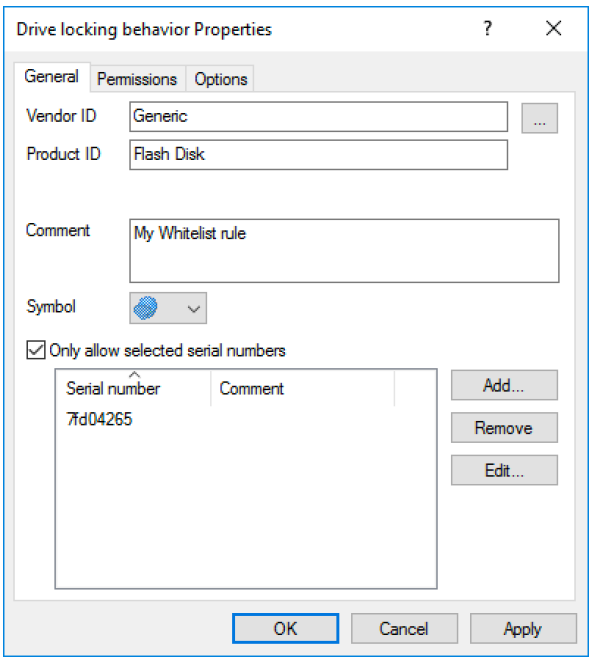
Pour ajouter un périphérique à la liste blanche, créez une règle dans **Drive whitelist rules**. Connectez-vous sur un poste sur lequel un agent DriveLock est installé afin de récupérer des informations sur ce périphérique.

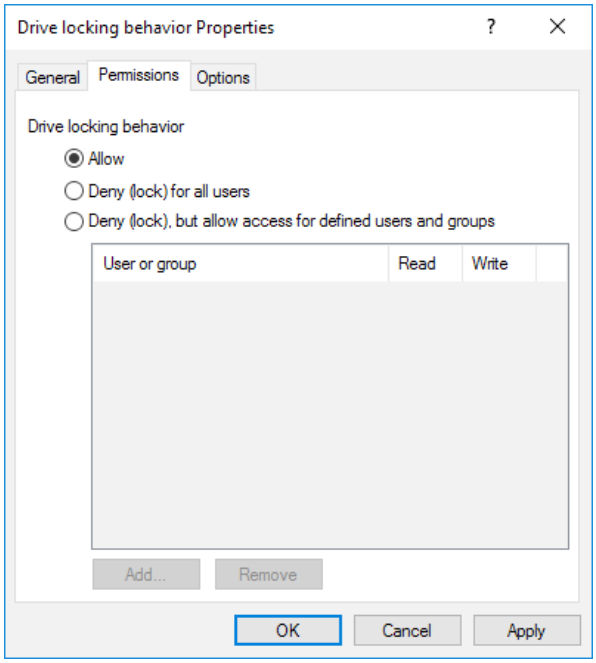


Il est même possible d'ajouter un ou plusieurs numéros de série pour affiner le filtrage.

Une fois les informations renseignées, validez l'autorisation dans l'onglet "Permissions".

Enregistrez, publiez puis déployer la politique pour tester le comportement sur un poste client en essayant de connecter une clé USB. Si elle ne correspond pas à celle indiquée dans la liste blanche, alors elle sera bloquée.

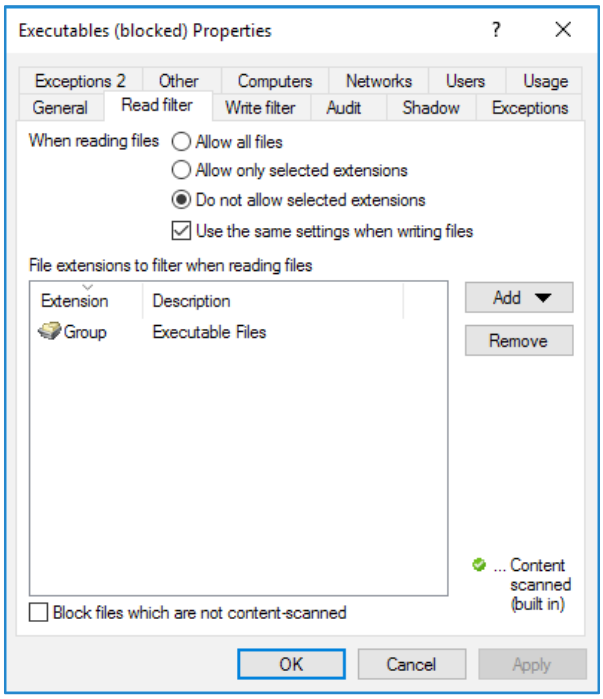


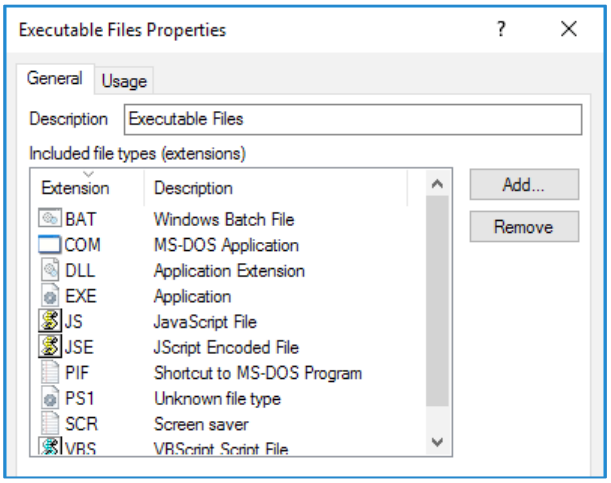


Filtrage par type de fichiers

En utilisant des types de fichiers (.docx, .jpg, etc.), des groupes (fichiers Office, images, etc.) ou encore des templates (n'autoriser que les fichiers Office, bloquer les exécutables, etc.) vous

pouvez configurer vos propres autorisations de lecture et/ou d'écriture pour les supports amovibles.



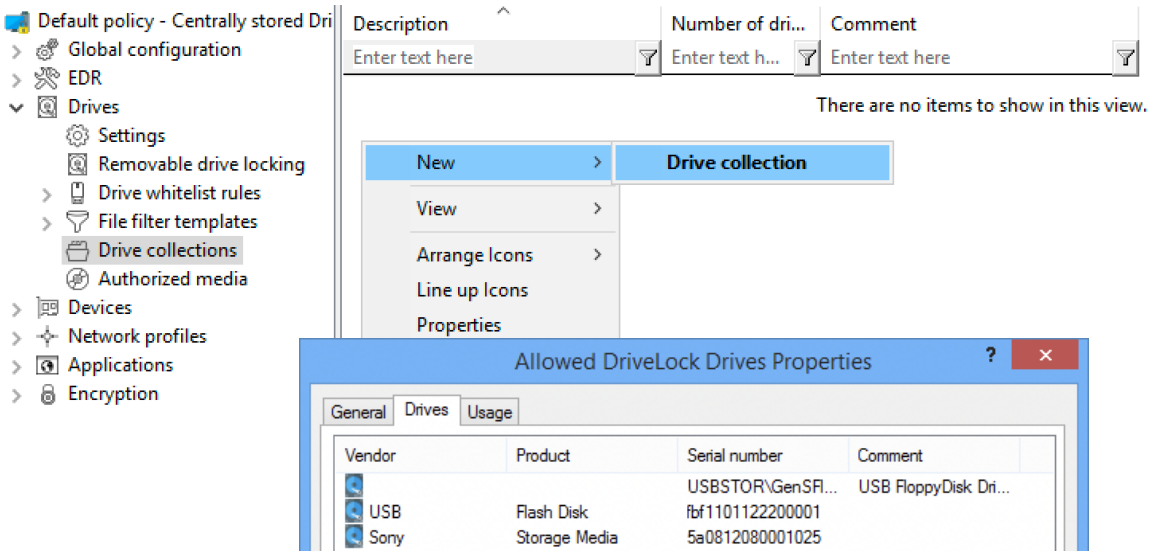


Collections

Pour simplifier la configuration des paramètres et des règles, vous avez la possibilité de regrouper vos lecteurs en créant une collection dans **Drives** > **Drive collections**.

Vous pouvez ajouter, supprimer, modifier, activer/désactiver et importer/exporter des lecteurs vers/depuis une collection.

Utilisez le bouton "Import" pour importer plusieurs lecteurs à partir d'un fichier au format CSV ou INI.



Il est également possible de constituer une collection pour les différentes classes d'appareils dans **Devices** > **Device collections**.

Classes de périphériques

Ce sont les informations données par Windows qui sont utilisées, et il arrive parfois que des périphériques soient reconnus dans une classe adéquate, par exemple une imprimante qui est reconnue comme périphérique Bluetooth.

NB : Les contrôleurs et les ports doivent être contrôlés avec soin, car vous risquez de tout bloquer.

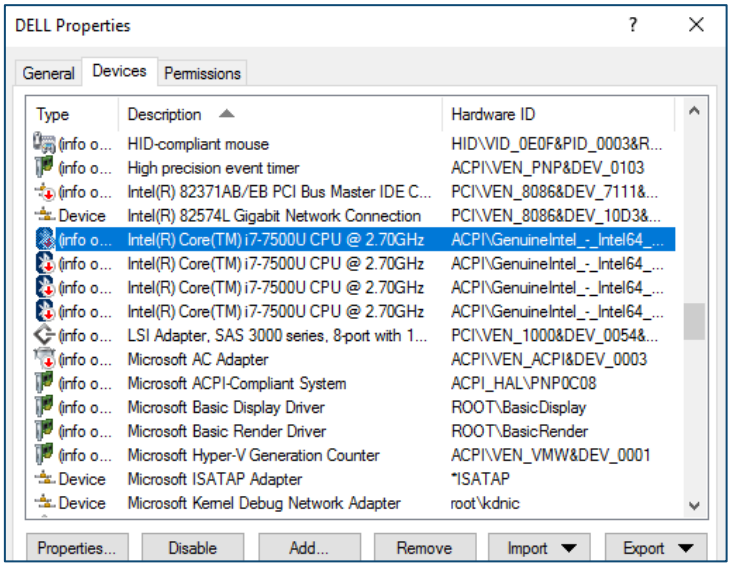
Un ID matériel, c'est-à-dire l'identifiant d'un périphérique, est composé des composants individuels suivants :

- Le bus via lequel le périphérique a été connecté, par exemple PCI ou USB.
- Le Vendor ID du fabricant, par exemple VEN_8086 ou Vid_0bb4 (VEN=Vendor, Vid=Vendor ID, 8086=ID d'Intel, 0bb4=ID de Canon)
- Le Product ID du type de produit, par exemple DEV_10F5 ou Pid_0a51 (DEV=Device, Pid=Product ID, 10F5=ID du 82567LM Gigabit, 0a51=ID du Powershot A80)
- Révision partielle du type de produit (Rev=Révision, 0001=Numéro de révision 1)

Exemples :
USB\Vid_0bb4&Pid_0a51&Rev_0001
PCI\VEN_8086&DEV_10F5

Computer templates

En analysant et en collectant tous les périphériques à partir d'un ordinateur local ou distant, il est possible d'autoriser l'ensemble du groupe plutôt que de constituer une liste blanche élément par élément.



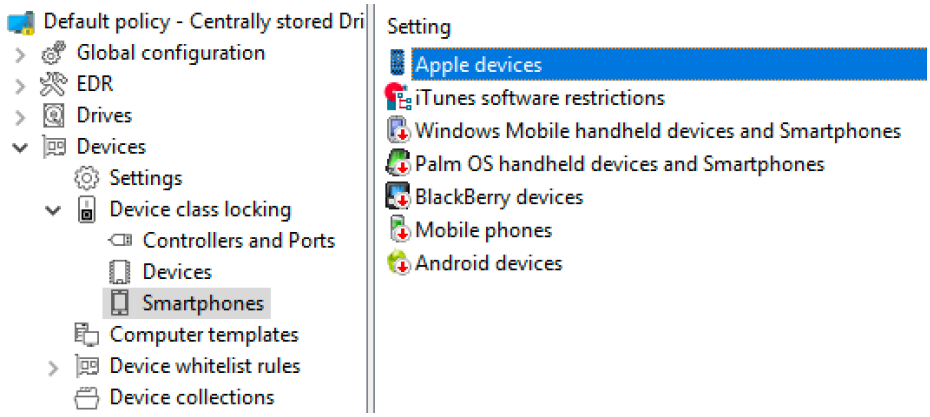
- Type de matériel (par exemple Dell Precision M5510)
- Regroupement logique (par exemple toutes les cartes réseau)

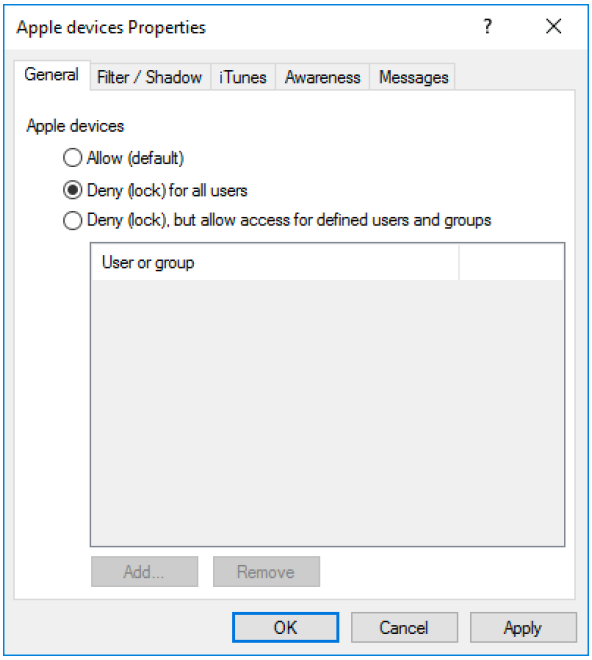
Cas pratique : blocage des smartphones Apple

Dans **Devices** > **Device class locking**, vérifiez que la catégorie "Apple devices" est bloquée pour tout le monde.

NB : Même si un smartphone est bloqué, le chargement électrique sera néanmoins toujours opérationnel.

Enregistrez, publiez puis déployer la politique pour tester le comportement sur un poste client en essayant de connecter un smartphone Apple.

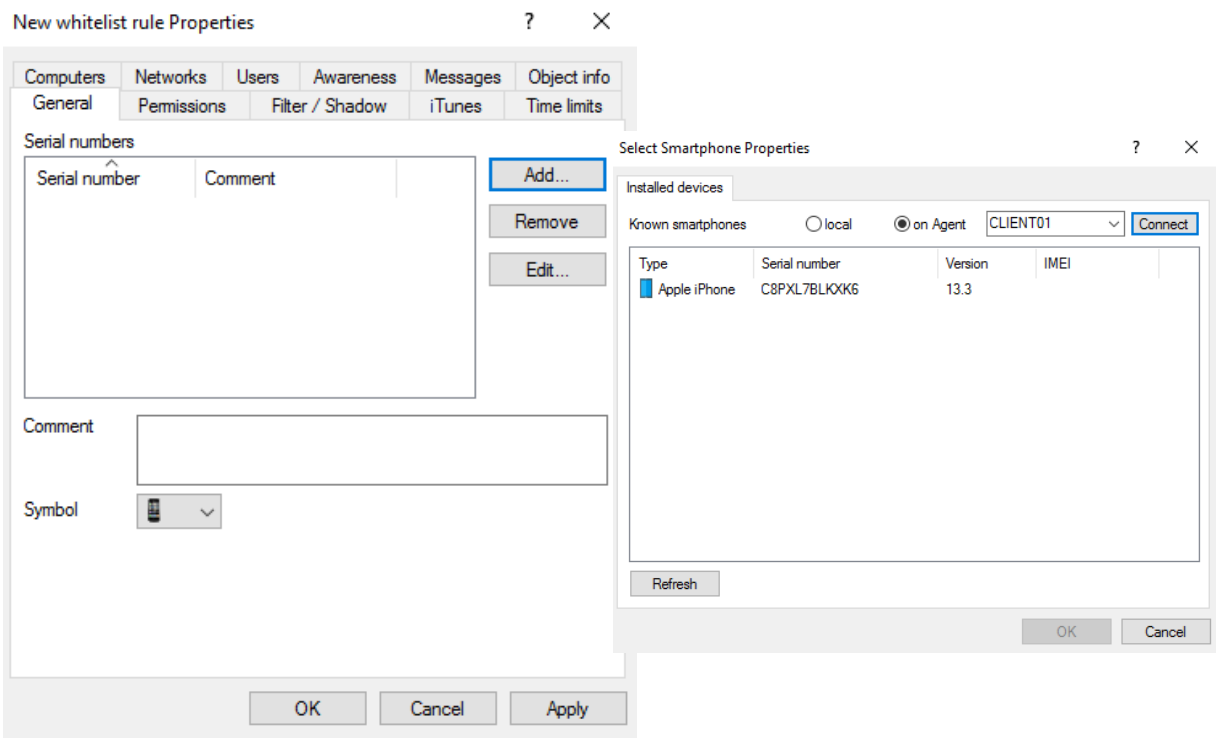


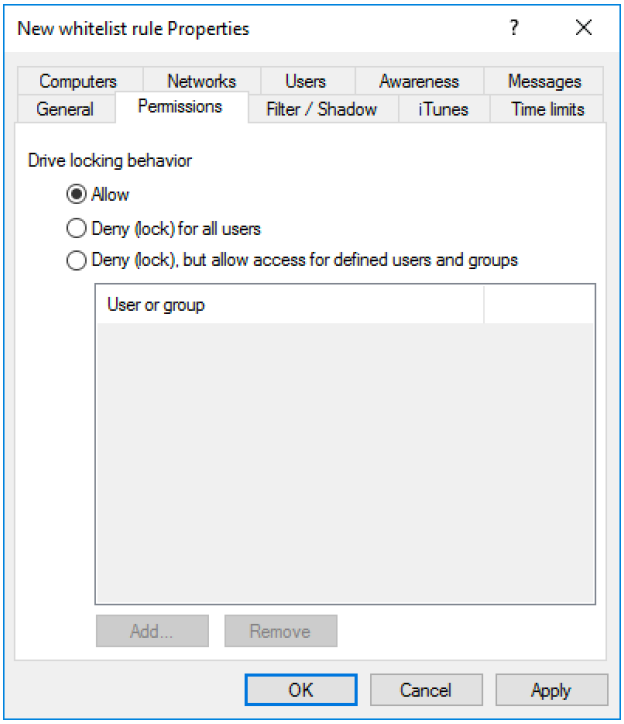


Pour ajouter un smartphone à la liste blanche, créez une règle dans **Device whitelist rules**. Connectez-vous sur un poste sur lequel un agent DriveLock est installé afin de récupérer des informations sur ce smartphone.

Une fois les informations renseignées, validez l'autorisation dans l'onglet "Permissions".

Enregistrez, publiez puis déployer la politique pour tester le comportement sur un poste client en essayant de connecter un smartphone Apple. S'il ne correspond pas à celui indiqué dans la liste blanche, alors il sera bloqué.





Pour informer les utilisateurs

Lorsqu'un blocage ou un filtrage est effectué sur un poste, l'utilisateur concerné peut être informé de différentes façons, via un message personnalisé dans la zone de notification de Windows ou une fenêtre avec une demande de validation.