

# DATALOCKER PORTBLOCKER

Solution de contrôle des ports USB des terminaux gérée par SafeConsole



## GARDEZ LE CONTRÔLE DE VOS PORTS USB

PortBlocker est une solution de prévention de perte de données (Data Loss Prevention, ou « DLP ») pour les dispositifs de stockage amovible, permettant de limiter les périphériques de stockage USB qui peuvent être utilisés sur les postes utilisateurs. Avec PortBlocker, les utilisateurs ne peuvent transférer des données qu'entre des dispositifs chiffrés, approuvés et sécurisés, ce qui empêche les violations de données via l'accès ou l'utilisation non autorisée. PortBlocker est intégré à SafeConsole, la solution leader de gestion centralisée pour le stockage chiffré et sécurisé. Toutes les activités des terminaux (telles que l'endroit et l'heure où un blocage a lieu) sont consignées dans les journaux d'audit de SafeConsole pour être soumises à l'examen des administrateurs.

## FONCTIONNALITÉS DE PORTBLOCKER

- **Contrôle des ports des terminaux** - Approbation et enregistrement sur liste blanche des périphériques de stockage USB selon l'ID de fournisseur (VID), l'ID de produit (PID) et le numéro de série via SafeConsole.
- **Mise en œuvre des stratégies selon les postes de travail** - Les stratégies sont appliquées en fonction de l'emplacement du poste de travail dans Active Directory. Si nécessaire, des stratégies individuelles peuvent être créées jusqu'au niveau du poste de travail.
- **Activation/désactivation rapide** - Les administrateurs peuvent « Autoriser tous » ou « Bloquer tous » les périphériques par l'intermédiaire de SafeConsole.
- **Audits d'activité** - Tous les événements (par ex. lorsqu'un périphérique est bloqué, lorsqu'un terminal est enregistré, ou lorsque des modifications sont apportées aux stratégies) sont signalés à SafeConsole dans les journaux d'audit.
- **Geofence** - Les dispositifs peuvent être bloqués automatiquement lorsqu'un poste de travail enfreint la stratégie de géolocalisation configurée par le biais de SafeConsole through SafeConsole.

## COMMENT FONCTIONNE PORTBLOCKER?

**Protection permanente.** Une fois installé par un administrateur, PortBlocker sera automatiquement exécuté en arrière-plan sur l'ordinateur de l'utilisateur. Il ne peut pas être désactivé ou désinstallé sans les privilèges d'administrateur.

**Application des stratégies.** Restriction des périphériques de stockage USB via la stratégie de liste blanche de SafeConsole (VID, PID et numéro de série). Les stratégies sont automatiquement mises à jour depuis SafeConsole.

**Rapports en temps réel.** La gestion centralisée de PortBlocker via SafeConsole permet de facilement vérifier qui, quoi, quand et où se produisent les menaces.

## CONFIGURATION MINIMALE

- Compte SafeConsole actif (v5.4.0+)
- Windows™ 7 ou 10 (compatibilité macOS disponible au 2ème trimestre 2019)
- 512 Mo de mémoire RAM
- 1 Go d'espace disque disponible
- Connexion au serveur SafeConsole pour l'enregistrement et les mises à jour des stratégies
- Connexion réseau 1 Mbits/s
- Processeur Intel Quad Core Atom, ou processeur x86 - x64 équivalent
- Utilise les paramètres proxy du système WinINET (Internet Explorer) de l'utilisateur. Les paramètres proxy peuvent être configurés manuellement ou via un script PAC.

Un compte SafeConsole est nécessaire pour utiliser et déployer PortBlocker. Pour les nouveaux comptes SafeConsole, un paiement unique est également requis. Une licence valide de PortBlocker est ensuite requise pour chaque poste de travail/ système sur lequel PortBlocker est déployé (les licences sont disponibles pour des périodes de 1 ou 3 ans).

🌐 [datalocker.com](http://datalocker.com)

✉ [sales@datalocker.com](mailto:sales@datalocker.com)

☎ +1 855 897 8755 ou +1 913 310 9088