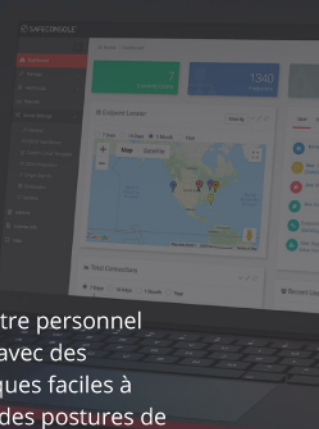


# DATALOCKER GESTION CENTRALISÉE SAFECONSOLE



La plateforme de DataLocker est un moyen puissant de gérer des centaines de milliers de périphériques et points d'accès. Elle vous permet de provisionner, sécuriser, gérer et auditer facilement des clés USB chiffrées, des ports USB et des disques virtuels chiffrés à distance. SafeConsole se déploie sur site ou est accessible dans le cloud (SaaS). Il propose également en option une prise en charge Premium et d'autres fonctionnalités, notamment SSO et bien plus encore.



Améliorez la sécurité des clés USB ainsi que des ports USB des postes de travail



Réduisez le temps consacré au déploiement et à la gestion des clés USB sécurisées



Simplifiez le suivi et la conformité des clés USB sécurisées grâce à des outils d'audit et de création de rapports sophistiqués



Gardez votre personnel productif avec des périphériques faciles à utiliser et des postures de sécurité dynamiques

## DÉPLOYER EN TANT QUE CLOUD (SAAS) OU SUR SITE\*



Provisionnez, configurez, gérez et auditez à distance votre parc de périphériques USB chiffrés, tout en déverrouillant de puissantes fonctionnalités de sécurité pour les périphériques DataLocker.



L'anti-malware McAfee® intégré est toujours activé pour analyser les fichiers sur les clés USB sécurisées, supprimer ou mettre en quarantaine les menaces de malware et remonter ces informations à SafeConsole.



Stocker et sécurisez les données locales ou cloud dans un lecteur virtuel chiffré.



Assurez-vous que votre personnel utilise uniquement des périphériques USB approuvés pour empêcher l'intrusion de logiciels malveillants ou la perte accidentelle de fichiers.

\* Utilisez Windows Installer, qui peut fonctionner à partir d'un matériel vierge, d'images virtuelles ou de n'importe quel cloud, y compris des clouds privés.



[www.query-informatique.com](http://www.query-informatique.com)

# SAFECONSOLE CLOUD / SUR SITE FONCTIONNANT AVEC WINDOWS ET MACOS

GESTION ET CONTRÔLE CENTRALISÉS COMPLETS POUR LES ADMINISTRATEURS

## CONTRÔLE DE PÉRIPHÉRIQUE POUR SÉCURISER LES USB

- Configuration de la politique de mot de passe
- Répertoire d'inventaire automatique de tous les utilisateurs et périphériques
- Audit des actions du périphérique et des mouvements de fichiers pour la conformité
- Réinitialisation du mot de passe à distance
- Connexions autonomes gérées sur Linux ou n'importe quelle machine
- Détruire définitivement un périphérique à distance
- Réinitialisation d'usine à distance/désactiver/refuser l'accès/définir comme perdu
- Passer en mode audit (restreindre l'accès et désactiver les modifications)
- Réattribuer à distance le périphérique à un nouvel utilisateur
- Verrou d'inactivité
- Protection en écriture (mode lecture seule)
- Restrictions de fichiers (interdire/autoriser les extensions de fichiers)
- Géolocalisation (basée sur l'adresse IP de l'hôte)
- Message d'écran de déverrouillage personnalisé
- Windows ou Mac
- Options de déploiement sur site ou dans le cloud

## ANTI-MALWARE POUR USB SÉCURISÉ

- Dispositif McAfee® anti-malware intégré
- Éliminer ou supprimer automatiquement les logiciels malveillants sur le périphérique
- Rapports en temps réel des fichiers et périphériques infectés

## PORTBLOCKER POUR LES PORTS USB DU RÉSEAU

- Assurez-vous que seuls les périphériques USB approuvés sont utilisés
- Ports USB entièrement verrouillés au niveau de la couche matérielle
- Signaler les tentatives de périphériques non approuvés
- Accès temporaire au périphérique USB

## SAFECRYPT POUR FICHIERS ET DOSSIERS

- Lecteur virtuel chiffré pour Windows ou macOS
- Lecteur chiffré virtuel géré de manière centralisée sur le bureau qui permet le stockage sécurisé et la séparation des fichiers et dossiers de travail
- Configuration en tant que lecteur réseau distant partagé ; chiffrez et synchronisez localement en toute sécurité avec le réseau (NAS), OneDrive, Google Drive et plus encore
- Gardez les lecteurs verrouillés séparés du système d'exploitation hôte

## AJOUTER DES FONCTIONNALITÉS DU PLAN PRO

Ajoutez à votre déploiement de SafeConsole.

### FONCTIONNALITÉS PLAN PRO

- Niveau de support Premium (temps de réponse maximum de 2 heures)
- Une équipe dédiée de responsables de support
- File d'attente d'assistance prioritaire
- Remplacement matériel avancé avec SAV
- ZoneBuilder : connexion automatique sécurisée et restriction des périphériques

## AJOUTER DES FONCTIONNALITÉS DU PLAN ENTERPRISE

Comprend tout le plan Pro, plus les éléments suivants pour votre déploiement de SafeConsole.

### FONCTIONNALITÉS PLAN ENTERPRISE

- Accès à REST API
- Authentification unique pour les administrateurs (SSO, SAML v2)
- Intégration SSO/SIEM
- Journalisation externe SIEM
- Prise en charge du serveur SMTP Kerberos
- Synchronisation des utilisateurs Active Directory et synchronisation sécurisée des utilisateurs Active Directory (LDAPS)
- Adresses IP du serveur dédié (permet la mise sur liste blanche du pare-feu pour le trafic sortant)
- Emplacement géographique personnalisé du serveur (répond aux exigences de conformité)
- Journaux d'audit utilisateur illimités

## Prêt à commencer ?

Demandez votre Starter Pack pour déployer correctement SafeConsole. Le pack de démarrage contient 20 licences qui peuvent être utilisées pour n'importe quel produit. Des licences supplémentaires peuvent être achetées séparément.

## Références du Starter Pack

CLOUD

1 AN  
START-SCC-1  
3 ANS  
START-SCC-3

SUR SITE

1 AN  
START-SCOP-1  
3 ANS  
START-SCOP-3



[www.query-informatique.com](http://www.query-informatique.com)



Immeuble Le Noblet - Hall A  
1 bd Charles de Gaulle  
92700 Colombes - FRANCE  
Tél. : +33 (0)1 499 733 00