

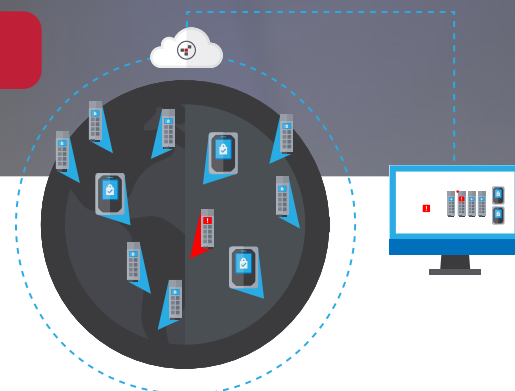
# SAFECONSOLE

## ADMINISTRACIÓN DE DISPOSITIVOS USB

Control centralizado, seguridad y gobernanza para dispositivos USB cifrados

SafeConsole USB Device Management proporciona administración, seguridad y monitoreo centralizados para unidades USB con cifrado por hardware. Mediante una sólida aplicación de políticas, visibilidad en tiempo real e integración perfecta con la plataforma SafeConsole, las organizaciones mantienen un control total sobre todos los dispositivos SafeConsoleReady™ mientras protegen los datos confidenciales, previenen pérdidas y fortalecen la seguridad operativa.

SafeConsole USB Device Management permite a las organizaciones proteger los datos portátiles sin sacrificar la productividad, combinando automatización, visibilidad y control basado en políticas en una única plataforma unificada de administración.



Gestionado por

 **SAFECONSOLE**<sup>®</sup>

### Administración segura de contraseñas

Restablezca de forma remota contraseñas sin pérdida de datos mediante códigos de recuperación y validación criptográfica. Los procesos seguros evitan los riesgos de ingeniería social, al tiempo que permiten una verificación flexible de la identidad y canales alternativos de comunicación.

### Cumplimiento normativo y auditoría detallada

Mantenga un inventario de dispositivos en tiempo real con una auditoría integral de archivos. Realice un seguimiento de los archivos copiados, eliminados o renombrados en unidades USB cifradas para respaldar la gobernanza, las investigaciones y los requisitos regulatorios.

### Administración del estado del dispositivo

Deshabilite, bloquee, elimine o recupere de forma remota unidades comprometidas. Proteja al instante los datos confidenciales deshabilitando el acceso o borrando dispositivos perdidos o robados.

### Restricciones de tipos de archivo y protección contra escritura

Restrinja qué tipos de archivos pueden guardarse en unidades USB cifradas para evitar el almacenamiento de contenido no autorizado como archivos ejecutables. Active la protección contra escritura para bloquear los dispositivos en modo de solo lectura cuando se utilicen en sistemas no confiables.

### Geolocalización y geocercas

Realice el seguimiento de la ubicación de los dispositivos y restrinja el acceso según la ubicación geográfica. Aplique políticas de geocercas para garantizar que las unidades solo funcionen dentro de regiones o zonas autorizadas.

### Seguridad y cifrado integrales

SafeConsole aplica un sólido cifrado, autenticación y controles de políticas en todos los dispositivos USB administrados.

- Cifrado AES de 256 bits para unidades USB y aplicación de políticas
- Reglas de contraseñas y políticas de seguridad del dispositivo
- Restricciones de tipos de archivos, control de escritura y geolocalización
- Recuperación segura de contraseñas mediante criptografía
- Autenticación basada en políticas (certificados, MFA)
- Responsabilidad completa de administradores y usuarios



### LICENCIAMIENTO

Se requiere una cuenta válida de SafeConsole. Se requiere una licencia de USB Device Management por dispositivo, disponible con vigencia de 1 o 3 años.



### Implementación eficiente y control de dispositivos

SafeConsole simplifica la implementación segura de dispositivos USB y las operaciones empresariales de administración de dispositivos.

- Aprovisionamiento por lotes con DeviceDeployer
- Configuración y aplicación remotas
- Borrado remoto y recuperación de dispositivos
- Administración de actualizaciones de software y firmware
- Activación del modo de solo lectura
- Monitoreo e informes en tiempo real



### Implementación y compatibilidad con la plataforma

- Administración centralizada mediante SafeConsole
- Arquitectura empresarial escalable
- Distribución segura de actualizaciones administrativas
- Compatibilidad multiplataforma
- Modelos de implementación en la nube (SaaS) y local (On-Prem)
- Integración con SIEM\*

### ADMINISTRACIÓN DE DISPOSITIVOS USB

- ✓ Administración centralizada de flotas de dispositivos USB cifrados
- ✓ Compatibilidad con dispositivos SafeConsoleReady™
- ✓ Aplicación del cifrado por hardware AES de 256 bits
- ✓ Restablecimiento remoto de contraseñas con recuperación criptográfica
- ✓ Flujos de trabajo seguros para la verificación de identidad
- ✓ Inventario de dispositivos y administración de activos
- ✓ Auditoría detallada a nivel de archivos
- ✓ Monitoreo de actividad en tiempo real
- ✓ Funciones remotas para deshabilitar, inutilizar, bloquear y borrar dispositivos
- ✓ Controles de respuesta para dispositivos perdidos o robados
- ✓ Restricciones de tipos de archivos
- ✓ Protección contra escritura y modos de solo lectura
- ✓ Seguimiento de geolocalización
- ✓ Aplicación de políticas de geocercas
- ✓ Autenticación basada en políticas (certificados, MFA)
- ✓ Aplicación remota de políticas
- ✓ Administración de actualizaciones de software y firmware
- ✓ Integración con SIEM\*
- ✓ Informes centralizados
- ✓ Registros de auditoría preparados para el cumplimiento normativo
- ✓ Compatibilidad multiplataforma
- ✓ Opciones de implementación en la nube (SaaS) y local (On-Prem)

\*Disponible en la versión SafeConsole Enterprise



#### Borrado certificado de datos USB

Borrado criptográfico certificado con generación automática de comprobantes de borrado, certificados a prueba de manipulaciones e informes de cumplimiento conforme a NIST SP 800-88.



#### Antimalware para dispositivos USB seguros

Proteja sus unidades USB con un sistema antimalware integrado que analiza y reporta amenazas de malware directamente a SafeConsole.



#### PortBlocker USB DLP Endpoint Protection

Evite que dispositivos USB no autorizados accedan a su red mediante la sólida protección de endpoints.



Solicita una demostración personalizada

[datalocker.com](https://datalocker.com) [sales@datalocker.com](mailto:sales@datalocker.com)