



TECH

REQUIREMENTS

Requires SafeConsole (this is an add-on license, not a full installation).
2GB RAM on server. Windows or Linux. All other required software included.
Web browser to access the administrative interface. Internet Explorer 7+ , Firefox 1.5+ (PC, Mac), Safari 3+, Opera 9+ (PC, Mac).

SUPPORTED LANGUAGES

English, French, German, Spanish, Polish.

GROUP POLICIES

Optionally reflect an existing Active Directory or other directory service.
Assign configurations to Organizational Units by simple drag-and-drop.

SKU

Subscription license (yearly): SC-EP-SL
Perpetual license (lifetime): SC-EP-LL

SafeConsole Expansion Pack

Pack your secure USB device with those extra features that will take USB management to a whole new level! With SafeConsole Expansion Pack, you get access to tools that will assist you in taking further control over your devices, protect them from malicious malware, and increase productivity.

INCLUDED FEATURES:



WRITE PROTECTION

Protect your drives from malware by setting your drive in a read only mode when unlocking it on untrusted machines. With Write Protection, data can be published to drives without danger of modification, ideal for sensitive information that needs to stay intact after being sent to the target audience.



FILE RESTRICTOR

Protect your devices and network from malware by prohibiting storage of any malicious executables on managed devices.



DEVICE LOCKOUT

Ensure user adoption by disallowing usage of any other USB storage device on your network. A separate software service is installed on the machines in the network, disallowing anything but the trusted device for USB mass storage.



INACTIVITY LOCK

Make sure no device gets left behind, exposing sensitive data. Inactivity Lock locks down the device upon user inactivity.



AUTHORIZED AUTORUN

Start trusted applications upon unlock; allow scripts to tailor applications to your needs.



EASYSHARE

Share selected files protected with a temporary PIN without sharing the device password. EasyShare allows sharing of data even with untrusted machines and people.



WEB LOG-IN

Save time and add safety by enabling one-click log-in from the unlocked device to users' preset web mail or other web service.



CERTIFICATE CARRIER

Enable the user's trusted device to be used as a carrier of the user's digital certificates, which can be used for authentication.



DEVICE USER INFORMATION

Collects any chosen device's user information from the user at device setup. This provided user information can then be displayed under the "about" or "used" section in Authorized Autorun scripts. Optionally, choose to display information only within the local network or outside of it.



DEVICE USER SETTINGS

The administrator will preset and control device settings available to the user, thus speeding up deployment, saving costs and restricting user device options when needed.

