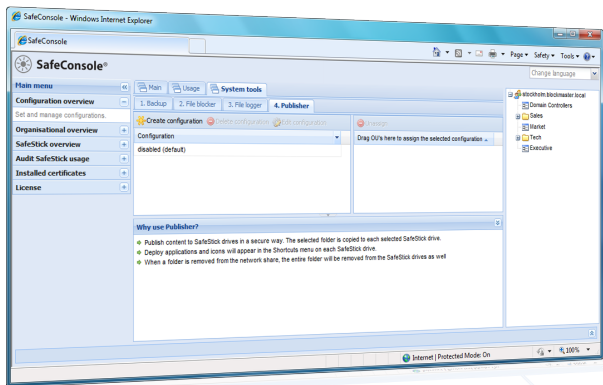


SafeConsole Extends the Possible Uses of SafeStick Drives and Enables Secure Workspace Virtualization



Distribute Files and Applications to Remote SafeStick Drives in a Matter of Seconds

SafeConsole® **Publisher** enables administrators to securely distribute software and files to SafeStick® drives even when they are in the field. The Publisher feature in SafeConsole presents organizations with a cost-efficient way to deploy solutions to mobile workers and enables them to make full use of the technology developments of remote worker software, such as portable VPN and virtualization software. Working from a SafeStick on an unknown host computer leaves zero footprint.



Better Economy and a Truly Portable Solution

Using laptops as portable workstations for your organization is no longer necessary. The SafeStick hardware failure rate of less than 0.1% compares favorably with the 15%-25% failure rate of many commonly used notebook brands. The low failure rates of SafeStick hardware mean that productivity will be maintained and support costs will be kept very low. For portability, nothing beats the nine-gram pocket-carried workstation loaded on a SafeStick.

A Secure Way to Send Files

All sensitive data is exchanged securely using two-way certificate-based SSL authentication, making Publisher the ideal way to distribute sensitive materials to a remote workforce. All files in transit are compressed to improve installation and transfer times, which also minimizes bandwidth usage. With Authorized Autorun, published software can easily be integrated with powerful yet simple scripts.

BlockMaster Works With CryptoCard to Provide a 2-in-1 solution

CryptoCard has integrated BlackShield ID tokens, deployed by the SafeConsole administrators, presenting SafeStick users with an elegant two-factor authentication feature. The administrator is able to centrally deploy any portable virtualization engine, portable antivirus software or file to the organization's SafeStick drives. SafeStick already works with FlashID from Deepnet Security, and soon RSA SecureID will be added to the list of supported software OTPs.



SafeConsole Makes It Possible to Truly Protect Your Network From Malware and Viruses

Stop the Threat of Malware From Portable Devices

In November 2008 a malicious worm spread across networks around the world. Data storage on portable units was quickly identified as a highway for the virus to spread as the worm copied itself to flash drives and other units. SafeStick Secure USB flash drives, with the SafeConsole features **Authorized Autorun** and **File Blocker**, already prevented Conficker autorun, malware infection, viruses and trojans from spreading over USB to your network.

SafeConsole Enables Antivirus to Run off SafeStick

By distributing portable antivirus software to SafeStick drives and specifying that it, with Authorized Autorun, autorun when the drive is unlocked, the SafeStick antivirus BlockMaster confirms support of McAfee and Trend Micro. Other antivirus software in a portable format can also be used and will be certified upon request. Scans can be set to start when the SafeStick is unlocked, and no files other than the selected antivirus engine can autostart. The antivirus protection can be combined with the day-zero attack protection of the FileBlocker feature.

Active Antimalware With FileBlocker

This unique technology aids the user in preventing the device from becoming a liability. Rogue files simply cannot be copied onto the SafeStick, as FileBlocker provides automatic defence. Choose between taking a white-list approach to protecting SafeStick – and ultimately the corporate network – only allowing storage of file types and software that have been certified by the administrator in SafeConsole, or creating a black-list, specifying which file types to deny.

Prevent Unapproved USB Devices From Accessing the Corporate Network

There is a straightforward solution to blocking unsecure USB storage from accessing your network. **LockOut** complements SafeStick by assuring the network administrator that no other USB storage devices will access the network. LockOut offers a quick and easy way of closing the door on the biggest emerging threats, such as Conficker, by enforcing the policy decision to use SafeStick exclusively for USB storage on all selected endpoints in the network. LockOut, in comparison with more complex endpoint port-control software, is a tool with a single mission: allow only SafeStick – as the sole USB storage device – onto your network.



SafeStick hardware-encrypted and fully password-protected USB flash drives make it easy to be secure.