

# SafeConsole Product Paper

SafeConsole Server Software for Complete  
Visibility and Control of Your SafeStick Portfolio



## Enforce Control and Enable Features for SafeStick

SafeConsole enforces full, granular USB management control over an organization's SafeStick secure USB flash drives and enables a host of productivity features. The SafeStick/SafeConsole solution offers the most flexible and efficient rollout scheme for larger organizations.

### Licensing options

SafeConsole is available in three licensing levels: INTRO (I), ENFORCE (E) and ENFORCE & ENABLE (E2). SafeConsole INTRO enforces an organization's password policy, SafeConsole ENFORCE includes a full range of policy-enforcing features, and SafeConsole ENFORCE & ENABLE multiplies the benefits of SafeStick devices and SafeConsole through the addition of many productivity-boosting features.

 **SafeConsole® INTRO**

 **SafeConsole® ENFORCE**

 **SafeConsole® ENFORCE & ENABLE**

## SafeConsole Configuration

All SafeConsole features can be turned on and off and be configured granularly on specific user groups' SafeStick drives. By default, SafeStick devices include basic Authorized Autorun and Time Lockdown protection. Current installations can be upgraded to a new edition at any point, without interruption.

SafeStick Hardware Encrypted  
and Fully Password  
Protected USB Flash Drives  
Makes it Easy to be Secure.



## Editions Overview



## SafeConsole Central Management Console Strong Baseline of Features

Administrator audit (XML export)	X	X	X
Limit access to SafeConsole (IP filter, certificate)	X	X	X
Remote management of drive configurations	X	X	X
Optionally reflect any directory service (Active Directory)	X	X	X
Granular configuration	X	X	X
Self-service deployment	X	X	X
Multiple SafeConsole users and administrator roles	X	X	X
Optionally manage SafeConsole administrator groups in directory service	X	X	X
Multi-language administrator interface	X	X	X
English, Deutsch, Español, Français	X	X	X
Self-contained, all-in-one installation package	X	X	X
Locked to organization with certificate	X	X	X
Connect to server interface with web browser	X	X	X
Run in private or public (Internet) mode	X	X	X

## Policy and Device-Management Enforcing Features

Custom password policy	X	X	X
Remote password reset over phone or Internet (PKI)		X	X
<b>Status Management</b>			
Remote factory reset		X	X
Remote disable		X	X
Return-to-base countdown to activate status (lost, disabled, reset)		X	X
Self-service mark as "found"		X	X
Custom Return-To-Owner message		X	X
Search for SafeStick drives and users		X	X
FileBlocker Active Anti-malware		X	X
Timer Lockdown management		X	X
Full SafeStick usage audit (XML export)		X	X
Track and trace IP as part of audit		X	X
LockOut (restrict all other USB mass storage from computer)		X	X
<b>Publisher - Publish Files and Programs to Remote SafeStick Drives</b>			
Deploy antivirus*			X
Deploy two-factor token software (OTP)*			X
Deploy virtualization*			X
Deploy portable applications*			X
Publish files to drives over Internet			X
Certificate Carrier (portable x.509 certificates)			X
Authorized Autorun management with integration scripts			X
Gather and use user information in Authorized Autorun and "about" screen			X
Customized "about" screen (template in user information)			X
<b>Instant Web Login</b>			
Outlook Web Access with one-click login			X
Protected web page access with one-click login			X
EasyShare (protect select files with a temporary PIN)			X
ZoneBuilder			X
Local self-service password reset (PKI)			X
Backup SafeStick data to local network			X
Full File Shadowing			X

\*Brand of your choice



## SafeConsole Feature Overview

### SafeConsole® **INTRO**

#### CUSTOM PASSWORD POLICY

Administrators can configure multiple complex password policies within SafeConsole. They can also set a limited life span for passwords based on the number of unlocks or days passed since the last password change. Users receive alerts about unsuccessful unlock attempts, ensuring that social-engineered hacks will not succeed.

### SafeConsole® **ENFORCE**

#### REMOTE PASSWORD RESET – Remote Over Phone and Internet or With Local Self-Service

If a user forgets the password to his or her SafeStick device, a remote administrator can help the user retrieve the password in just a matter of minutes. The eight-character recovery codes are easily read over the phone (or sent over Internet) yet maintain the robust security of a 128-character code using a pre-buffer method. No data is lost with this recovery method, and the process is protected against social-engineered attacks directed at the help desk. Password reset is also important to recover data from devices that will be cleared and then issued to new users. Administrators have the option of activating local self-service password management as part of the ZoneBuilder feature.

#### STATUS MANAGEMENT – Kill, Disable or Mark as Lost

Using the SafeStick device overview in SafeConsole, an authorized administrator can “kill” rogue drives over the Internet. SafeStick devices can also be set to the statuses “disabled” and “lost.” Disabled devices can be recovered later with the password reset feature, while lost drives can be set to display a custom Return-To-Owner message. All such events are logged for audit purposes.

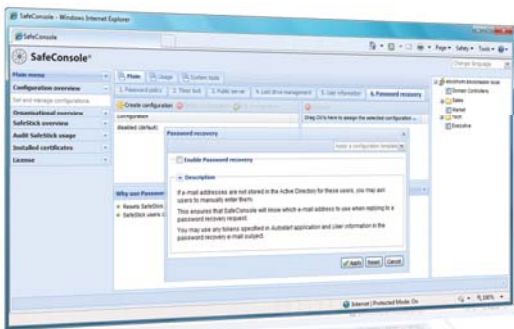
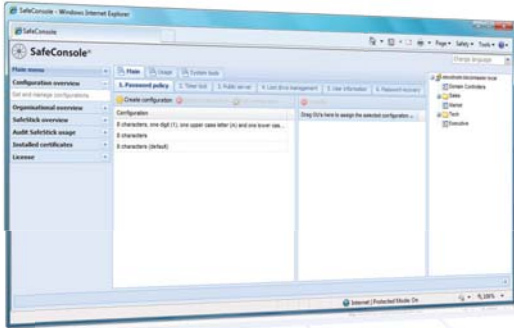
#### AUTOMATIC STATUS HANDLING

Automatic status handling requires that SafeStick drives connect to the SafeConsole server within a specific, configurable time period. SafeStick drives that have not returned are automatically regarded with a “lost” status. Lost drives are automatically marked as “found” if they are later inserted into the assigned user’s local machine. This feature effectively lowers support and administration costs.

#### FILEBLOCKER – Active Anti-malware

Use the SafeConsole **Authorized Autorun** and **FileBlocker** features to prevent Conficker autorun, malware infection, viruses and trojans from spreading via USB into your networks.

These unique technologies help users protect their SafeStick devices from becoming liabilities. FileBlocker defends SafeStick devices automatically, preventing rogue files from being copied onto SafeStick devices. FileBlocker takes a white-list approach to protecting SafeStick devices – and ultimately the corporate network – by allowing storage of only those file types and software that the administrator has approved and certified in SafeConsole. Authorized Autorun and FileBlocker can be complemented with a traditional antivirus of your choice, such as McAfee, Trend Micro and ClamAV, all of which are currently certified.





## TIMER LOCKDOWN MANAGEMENT

Administrators can preset the SafeStick Timer Lockdown feature to lock down devices after a specific number of minutes of inactivity. If a user leaves behind an unlocked SafeStick device in a computer, the device will automatically lock down in accordance with the set policy. This protective feature combats the risk of major data breach as a result of misplaced or forgotten drives.

## LOCKOUT – Enforce SafeStick Devices as Preferred USB Storage

LockOut from BlockMaster is an easy, straightforward solution to blocking unsecure USB storage from accessing your network. LockOut complements SafeStick devices by ensuring that no other USB storage devices will access their network. LockOut is the quickest and easiest way of closing the door on emerging threats, such as Conficker, by enforcing a policy mandating the use of SafeStick devices exclusively for USB storage on all selected endpoints in the network. Unlike more complex endpoint port control software, LockOut has a single mission: Allow only SafeStick devices for USB storage onto your network.

## SafeConsole® ENFORCE & ENABLE

### PUBLISHER – Publish Files and Programs to Remote SafeStick Drives

SafeConsole enables administrators to deploy software securely and publish files to SafeStick drives even when those drives are in the field. The SafeConsole Publisher feature is a cost-efficient way to deploy solutions to mobile workers, enabling them to make full use of the technology developments of remote-worker software such as portable VPN and virtualization software. All sensitive data is exchanged securely using two-way certificate-based SSL authentication, making Publisher an ideal way of distributing sensitive materials to a remote workforce. All files in transit are compressed to improve installation and transfer times, also minimizing bandwidth use. Together with Authorized Autorun management, Publisher can integrate with software easily, using powerful yet simple scripts. FileBlocker automatically whitelists published files.

### SafeConsole Enables Antivirus to Run Off SafeStick Devices

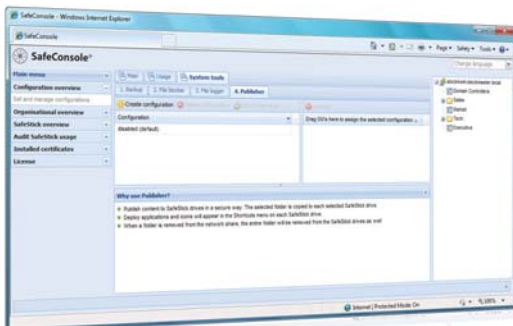
Portable antivirus software can be used together with the malware protection features FileBlocker and Authorized Autorun that are already onboard. Scans can be set to start upon unlocking the SafeStick device, and no files other than the select antivirus program can autostart. The antivirus protection can be combined with the day zero-attack protection of the FileBlocker feature.

## CERTIFICATE CARRIER

SafeStick drives may be used to carry certificates used for signing or encrypting documents, or access protected resources. These certificates will be available when SafeStick has been unlocked, and will be removed without a trace when SafeStick is locked or unplugged.

## AUTHORIZED AUTORUN MANAGEMENT

SafeStick always overwrites the autorun.inf file from the encrypted storage volume to protect against autorun viruses. You may specify a trusted command to run instead in the SafeConsole and there is also the possibility to use user information entered by the user. In combination with Publisher, this can be used to automatically start, for example, a portable antivirus program.





### INSTANT WEB LOGIN

Enable a shortcut to a web page for SafeStick users. The shortcut will be displayed as a button as soon as the users have unlocked SafeStick. There is out-of-the-box support for Outlook Web Access and additional services can be automatically configured by SafeConsole.

### EASYSHARE – Share Data, Not Your Password

When users share password-protected data, they are exposing their passwords. EasyShare is a social engineering–proof solution that enables users to share select files protected by a temporary PIN. One temporary shared EasyShare PIN keeps SafeStick device passwords private.

### ZONEBUILDER – Secure Automatic Unlock in Trusted Zones

Boost workforce productivity by allowing SafeStick device users to create and manage trusted zones with their user accounts and possibly their team members' user accounts. SafeStick devices automatically unlock when plugged into USB ports located in a trusted zone. ZoneBuilder can be configured to work as a trusted self-service for password resets.

### BACKUP – Transparent Central Backup of SafeStick Drives

In the event that a user loses or misplaces a SafeStick device, the administrator can easily re-create the drive by sending its backup information and settings to a new SafeStick device. Continuous incremental backups are transparent procedures that do not affect users' everyday work. The re-create procedure is handled remotely and does not involve any end-user actions other than plugging a SafeStick drive into the machine.

### FULL FILE SHADOWING AND AUDITING

With Full File Shadowing, SafeConsole administrators can re-create current SafeStick device content for auditing purposes. All administrator actions are logged in SafeConsole. Full File Shadowing gives administrators the ability to resolve a multitude of crisis situations. Administrators can search and export complete audit logs of SafeStick usage and file transfers. The IP number of the host machine is logged enabling track and trace with online IP tracking services. All actions taken by a SafeConsole administrator are logged and available for export.

## SafeConsole Technical Overview

SafeConsole is a Web-based application server software bundle that gives administrators management privileges over SafeStick drives. Administrators can use SafeConsole to manage and apply custom policies to all of an organization's SafeStick devices over the Internet.

### How Can SafeConsole Be Deployed?

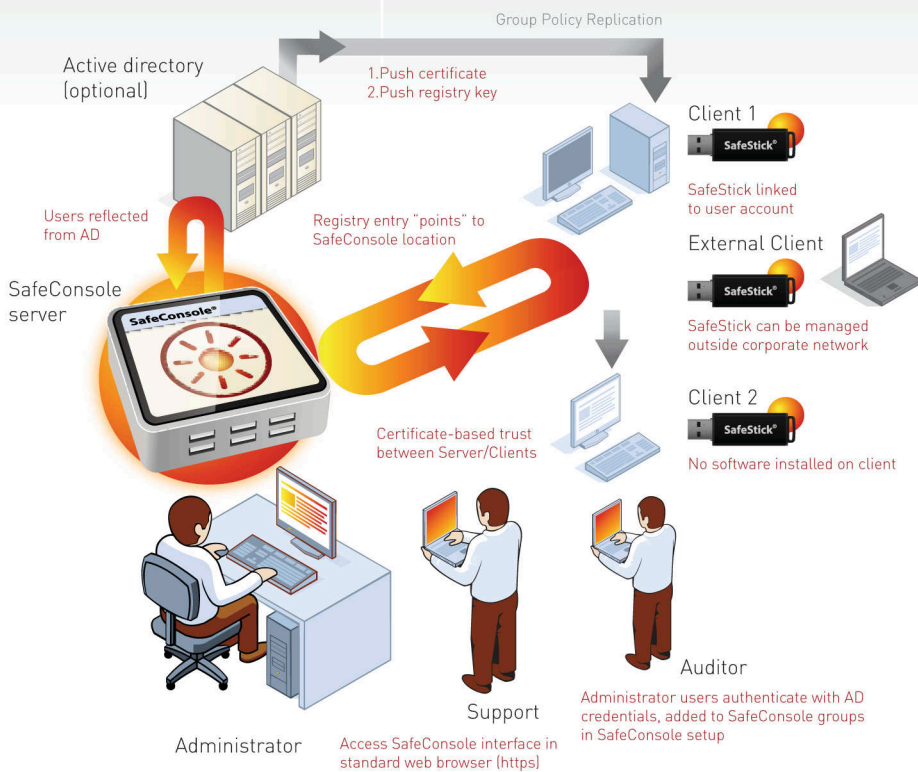
SafeStick devices and SafeConsole can be deployed flexibly. Start the rollout with a SafeStick device or SafeConsole: Either way, you gain complete control when the full solution is in place. The deployment process of the full SafeStick/SafeConsole solution is finished when each unique SafeStick drive is registered to a specific user on the SafeConsole server.





SafeConsole®

Complete visibility and control of your SafeStick portfolio



**1. User Accounts Authenticate to the SafeConsole Server**  
User accounts are connected to the SafeConsole server by setting a SafeStick drive-specific registry flag and deploying a certificate. This can be accomplished with a GPO in a larger organization.

### 2. Self-Service SafeStick Device Deployment

Each user claims ownership of his or her new SafeStick device by inserting the device into a computer, when the registry flag is first identified. This one-click procedure links the unique asset number embedded in each SafeStick drive to the specific user (in the reflected corporate directory, when available). No preregistration of devices or users is needed; the deployment is a fully automatic and compliant process.

### 3. SafeStick Devices Under Management Control – Ready to Use

The configurations set in SafeConsole for a specific user group are applied automatically to the group's SafeStick devices. Users who have expired or insufficient settings and passwords are made to align with the selected settings. The configurations can be continuously updated inside and outside the corporate network, and ownership can change during multiple device life cycles.

## Easy-to-Use Administrator Interface

Administrators use a web-based interface in a standard browser to create and assign SafeStick devices configurations. Functionality in SafeConsole is made available based on staff roles created in Active Directory or stored in an XML file.

## Secure Delivery and Installation

SafeConsole offers rapid deployment with an all-in-one installation process that can serve more than 100,000 SafeStick drives. No extra licenses for databases or certificate management are needed with SafeConsole, and server requirements are minimal (2GB RAM, Windows or Linux). Reflecting an existing directory service within SafeConsole is optional.

## SafeConsole Setup and Privacy

During the straightforward SafeConsole local server installation, the organization enters or generates its key (the private digital certificate). This unique key locks SafeConsole completely to the organization and enables authenticated management for administrators using trusted machines. This procedure guarantees safety for the organization and the managed SafeStick drives, as all communications are encrypted. The SafeConsole server software is available as a signed download to enable rapid deployments and even test installations. Setup instructions and a detailed manual are supplied with the installation files.

## More Information



UNITED KINGDOM

+44 (0)20 33 55 41 88

sales@blockmastersecurity.com

UNITED STATES

+1 - 888 - 432 - 4957

sales@blockmastersecurity.com

MAIN OFFICE (SWEDEN)

+46 (0)46 - 276 51 00

sales@blockmaster.se

© Copyright 2009 BlockMaster AB. All rights reserved. SafeStick and SafeConsole are registered trademarks of BlockMaster AB. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies.