SafeConsole®

BLOCKMASTER®
SECURITY THROUGH INNOVATION

SafeConsole Server Software for Complete Visibility and Control of Your SafeConsoleReady Device Portfolio.

POWERFUL DEVICE SECURITY

Instantly gain complete and granular control over all of your secure USB drives. An automatic inventory is created, and administrators can quickly enforce organization-specific policies for passwords, usage and storage.

STRETCH THE POSSIBLE USES OF YOUR DEVICES

SafeConsole enables a host of productivity features for an organization's secure USB flash drives. Gain access to lots of productivity tools, including portable application delivery and file distribution.

MANAGE DEVICES ANYWHERE

Your devices connect to SafeConsole over the Internet or the local area network to receive policy updates and file packages, and to post audit logs. Administrators can remotely terminate, clone or deactivate a device or help a user reset a forgotten password.

QUICKLY TAILOR THE SOLUTION TO THE ORGANIZATIONAL REQUIREMENTS

Using the web-based interface in a standard browser, an administrator can create and assign a policy or feature setting to a specific organizational unit in the corporate directory. All features can be turned on or off and configured granularly for each organizational unit.

EASY AND RAPID DEPLOYMENT

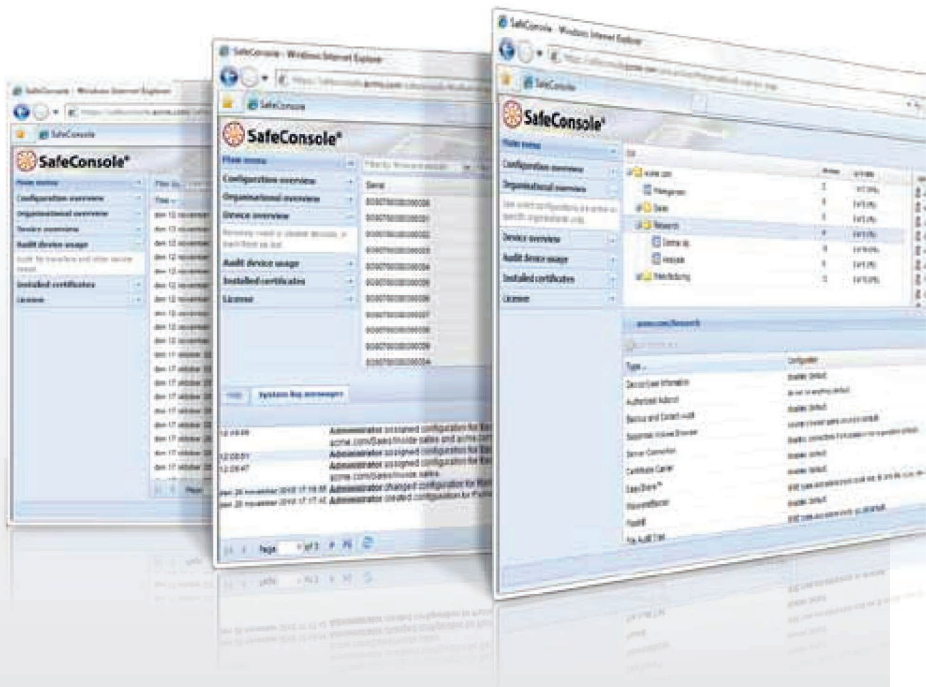
SafeConsole offers an easy and efficient roll-out scheme for larger organizations. Start with installing SafeConsole on your server and go on to deploying drives to users, and you will gain full management control from day one. Each unique device is registered to a specific user in SafeConsole and linked to the user in the corporate directory. The all-in-one installation has the power to serve large device deployments in the thousands. No extra licenses for databases or certificate management are needed, and the server requirements are low.

STAY AHEAD WITH BLOCKMASTER TECHNOLOGY

SafeConsole is continuously developed to stay ahead of emerging security threats and new business needs. BlockMaster developed SafeConsole to be not only a security product but also a product that enables new ways of working, with great usability and unique features. A current installation can normally be upgraded to a new feature edition at any point, without any interruption.

PROVIDED WITH PRECERTIFIED PORTABLE SOFTWARE

SafeConsoleReady Applications are an assortment of portable software that works well running off SafeConsoleReady Devices and that have been precertified to make deployment quick and easy.



TECH

SAFECONSOLE REQUIREMENTS

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.

Making Use of the Many Advantages of SafeConsole

REMOTE PASSWORD RESET

Reset passwords remotely over any channel. Administrators can get remote offline users back to work within minutes, without any loss of stored data.

PUBLISHER - CONTENT DISTRIBUTION

Recieve updates over the internet by allowing devices to call back to server. Publisher securely distributes a folder with files and applications to select devices in the field, enabling quick distribution of sensitive files and the ability to maintain portable software on the devices.

BACKUP AND CONTENT AUDIT

Automatically, incrementally and transparently back up device content. Make sure that lost devices can be cloned back, without data loss and without intervening in the user's everyday work.

DEVICE STATE MANAGEMENT

Mark devices automatically as lost or found, saving administrators both time and costs associated with handling lost devices.

PASSWORD POLICY

Ensure that all data is protected by strong, compliant passwords by enforcing password policies on the devices.

INACTIVITY LOCK

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

FILERESTRICTOR

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

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.

ZONEBUILDER

Allow users who have already securely authenticated their user accounts to have immediate access to their secure file storage on the device, with trusted automatic unlock and password reset self-service utilizing PKI.

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 AUDIT & FILE AUDIT TRAIL

Optionally activate device action audit logs; log actions such as unlock attempts on specific devices with the associated host computer. Audit device file actions showing what is and was stored on the device.

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.

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.