stickapps
Security & Productivity Apps for SafeStick™

SafeConsole Configuration & Initial Technical Requirements

This document is provided to guide you through the process of initially configuring SafeConsole (specifically the Publisher and Autostart features) in order to run one or more StickApps on your SafeSticks.

You only need follow this guide **ONCE**. If your SafeConsole is already configured, you may proceed to installing your chosen StickApp(s) following install guide specific to that app.

StickApp Anti-Virus, VPN Client and Password Manager have their own specific installation & configuration guides provided in PDF format with each download package - which you can follow to configure settings.

StickApp Free Tools have a README text file provided with each download package.

stickapp anti-virus
Powered by: avast!

stickapp password manager
Powered by: RoboForm Enterprise

stickapp vpn client
powered by portablevpn

stickapp free

Contents:

1. Overview - What are StickApps?

StickApps are a collection of tested and supported security and productivity applications, which can be used on SafeStick, or SafeStick Supersonic hardware encrypted USB memory drives.

Via SafeConsole, StickApps can be configured centrally, and distributed automatically to your SafeStick users without any user intervention. You can also update them and remove them from your users SafeSticks at any time.

Current free StickApps include;

- Skype
- Opera
- Firefox
- Google Chrome
- Sumatra PDF reader
- Pidgin IM Client
- Abiword – fully featured word processor
- Gnumeric – spreadsheet application
- *OpenOffice

Licenced StickApps include;

- On-access Anti-Virus client – which stops viruses and malware being copied to or from a SafeStick no matter if the host has anti-virus installed or not. Can also scan hosts for viruses and keyloggers.

- Password Manager – which automatically and securely stores user credentials and passwords. The application can then log them onto Websites AND Applications automatically, as well as being able to fill in web based forms – saving users considerable time. Strong Password Generator included.

- VPN Client (PPTP) – which could for example start a VPN connection to the office and automatically initiate an RDP session.

Datasheets, downloads and more information on all the features of the commercial StickApps are available on the website. http://www.StickApps.co.uk

StickApps have been configured and tested to run totally self-contained – i.e. they run completely from an unlocked SafeStick – no installation is necessary, and files are not installed on or left on the host computer.

***** Due to the potential size of OpenOffice >300Mb - depending on the apps in the suite you wish to deploy - it is not included in the StickApps package. It has been tested and works with SafeStick, and instructions for deployment and installation on SafeStick are available on request.

2. Licencing and Support Information

StickApp Anti-Virus, StickApp Password Manager and StickApp VPN Client are special OEM versions of certain commercial applications, and they require a licence to be purchased for use in all cases. All licenced applications are fully supported.

Other StickApps such as Abiword, Gnumeric, Firefox, Pidgin and Opera, are open source applications which are distributed free of charge under the GPL licence.

Some apps - such as Skype and Google Chrome - are distributed in original form without modification, and you must read and agree to the supplied EULA before use.

NOTE: Non-commercial free apps provided have been tested and have been shown to work perfectly with SafeStick – however these apps are <u>not officially supported</u> by StickApps.

3. Pre-Requisites

To install any StickApp application for use by your SafeStick users you will need the following as a minimum:

- Blockmaster SafeConsole "Enforce and Enable Edition" (E2) v4.x+ installed and configured.
- SafeSticks with Firmware at least v4.02 or higher. **STICKAPPS WILL NOT RUN unless at 4.02 minimum firmware.**
- A UNC share on your local network that is accessible to SafeConsole for hosting the StickApps.
- SafeStick's with sufficient free space to contain the StickApp(s) you choose to deploy.
- A downloaded copy of one or more StickApps you wish to deploy.

NOTE: Installation of these pre-requisites are outside the scope of this document, however SafeConsole, SafeStick Firmware and full instructions can be obtained from http://www.safestick.co.uk/safestick

4. What is SafeConsole?

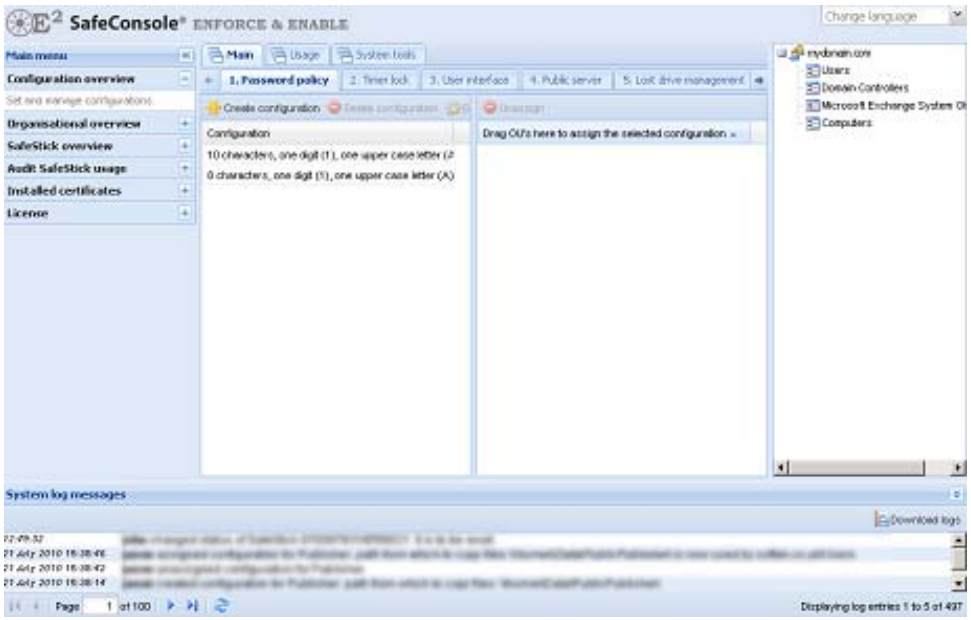
SafeConsole is a web based Enterprise Management Console for managing certain devices such as SafeStick hardware encrypted secure USB memory drives.

SafeConsole™ is a commercially licenced application by Blockmaster.

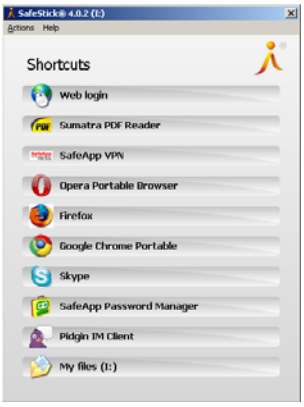
SafeConsole Enforce and Enable Edition (E^2) is required as StickApps utilises the Publisher feature, which is available as a licenced feature in this version of SafeConsole only.

The installation of, features and configuration of SafeConsole is outside the scope of this document.

More information on SafeConsole is available here: http://www.safestick.co.uk/safeconsole



5. What is Publisher?



Publisher is a feature of SafeConsole Enforce and Enable Edition (E²) which allows administrators to automatically push, deploy and maintain portable apps, data and files to remote SafeStick drives – whether the drive is inside or outside the local network.

Content and applications pushed to SafeSticks via the Publisher feature, will be accessible to the end user via shortcuts in the SafeStick "ShortCuts" menu, which appears once a SafeStick is successfully unlocked.

Many applications maintained by Publisher running from SafeConsole E² could also be auto started if required.

NOTE: Publisher is a feature of SafeConsole "Enforce and Enable Edition" only (also called SafeConsole E²). Publisher and Autostart are not available in SafeConsole Enforce (or E) Edition.

Contact your SafeConsole reseller if you need to upgrade to E² Edition.

6. Configuring Publisher

To be able to “push” one or more StickApps to your SafeSticks, it is necessary to configure the Publisher feature.

NOTE: If you are already using Publisher to publish files, and are familiar with this procedure then you can skip this step.

1) Start the SafeConsole interface in your web browser as normal for example;

https://safeconsole.mycompany.com

2) Navigate to “System Tools”, then “Publisher”

3) Click “Create Configuration”

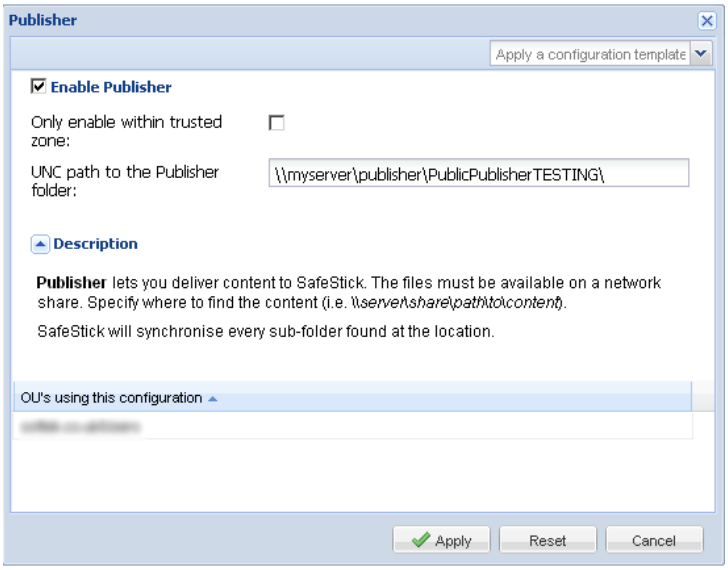
The configuration dialogue box contains just three fields.

- Enable (tick box)
- Only Enable within the Trusted Zone (tick box)
- UNC path

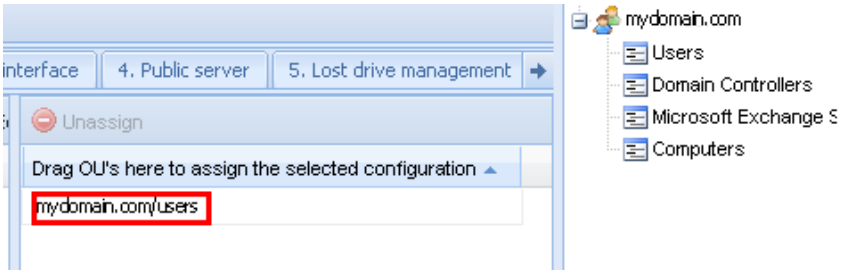
Publisher must be configured to use a local network share using a UNC name - which SafeConsole must have access to.

You will need to create this root folder on a Windows server (it could be the SafeConsole machine itself) for example;

\\myserver\publisher



Once you have created the Policy assign it to an OU group by dragging the group from the right hand window. **NOTE** you may wish to use a separate OU group for initial testing.



7. Publishing a StickApp - Example

NOTE: Please follow the installation & configuration guide relevant and supplied with each StickApp as the configuration procedure for each app is slightly different.

NOTE: The example below shows you how to publish a single App. To publish multiple apps just put them all in the root of the Published UNC folder. For example \\myserver\publisher\opera AND \\myserver\publisher\skype AND \\myserver\publisher\antivirus

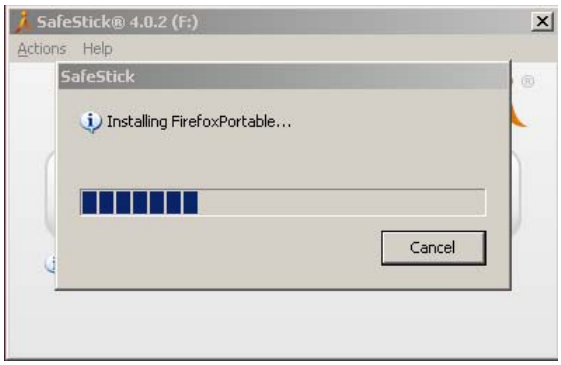
CRITICAL NOTE: Each StickApp has different requirements for the space it will occupy on a users SafeStick – from 3Mb to 100Mb or more. Therefore caution must be taken when Publishing a large package of apps. Also you should consider initially Publishing apps for users when SafeSticks are inside the LAN for performance reasons, as Publishing a large amount of files across the WAN could be very slow and bandwidth intensive.

For this example we will be deploying the "Opera" app.

- Download the "Opera" app or extract it from the app package.
- Extract the archive to a folder in your Publisher UNC shared folder – for example \\myserver\publisher\opera
- Close any currently open instances of Opera running on the local machine.
- From the installation folder run "operalauncher.exe"
- Opera Web Browser will now start.
- Configure any shortcuts, start page, proxy and anything else you would like as a Default for your users.
- Done !

The next time a SafeStick is unlocked by a user in the OU Group you have specified for Publisher, this app (and any others in the Published root) will be downloaded onto their SafeStick automatically, into a sub-folder of the <safestick drive letter>\Applications folder.

Opera (and any other Published apps) will also appear automatically in the users SafeStick ShortCut menu..



It is also possible to have this app Autostart automatically when a user unlocks their SafeStick if required. See further in this document for more information.

8. Publisher – Expected Behaviour

Assuming you have setup SafeConsole to be available on the Internet, Publisher works whether SafeSticks are inside the local network, or outside the network on a remote site with Internet access.

When a SafeStick is unlocked (either inside or outside the network) it first checks the UNC path to the published files as specified in the policy configuration, which it obtains from SafeConsole.

If SafeStick cannot access the UNC path directly (because the SafeStick is outside the network for example) it asks SafeConsole to obtain this list on its behalf, and it then compares this list with the files and folders already present on the SafeStick in <root>\Applications\

Any files or folders that are not present - or which are newer in the UNC share - are then downloaded from SafeConsole to the SafeStick, and are stored in a matching folder on the SafeStick – for example; <root>\Applications\<whatever app>

Any files which are newer on the SafeStick are **always** left untouched – unless the published folder is completely removed.

CRITICAL NOTE: If an entire Published folder (and subfolders) are removed (or renamed) from the UNC share, then the corresponding folder(s) on the SafeStick will be totally deleted – including any locally created files.

For example;

- We have published \\myserver\publisher\firefox (which includes several sub-folders).
- This folder has been previously published to users' SafeStick's.
- A user has created a folder on their SafeStick <root>\Applications\firefox\MYPICS.
- The entire "firefox" Published folder structure in the UNC share is then deleted.
- On next unlock, SafeSticks see that the folder has been deleted, and the entire folder structure <root>\Applications\firefox – including MYPICS - on the SafeStick is deleted.

NOTE: Therefore as the <root>\Applications folder is maintained by SafeConsole it is highly recommended that no critical user data is ever saved to this location.

Why is understanding this behaviour important?

Certain apps store personal user data and preferences in their install folder structure – for example Firefox stores user preference data in <root>\Applications\firefox\firefox\data

If the admin were to stop publishing the folder on the server, the folder name were to change, or this policy were to change (i.e. OU Group membership is changed), then not only would the application be deleted, but all user data and preferences stored in this folder or subfolder structure would be deleted also.

It is therefore important to fully consider this when upgrading applications, changing policy, or removing Published folders.

9. Configuring Autostart

As a security feature to protect from malware, viruses and other attacks (such as the Conficker worm), on successful unlock, SafeStick always overwrites its “standard” autorun.inf file with a certified, un-infected copy from its internal own encrypted storage volume.

Therefore you cannot modify the regular autorun.inf file to start programs.

However, by using SafeConsole E², you can issue and configure a trusted Autostart script to run instead.

In combination with Publisher, this can be used to automatically start various applications such as StickApp Anti-Virus or StickApp Password Manager.

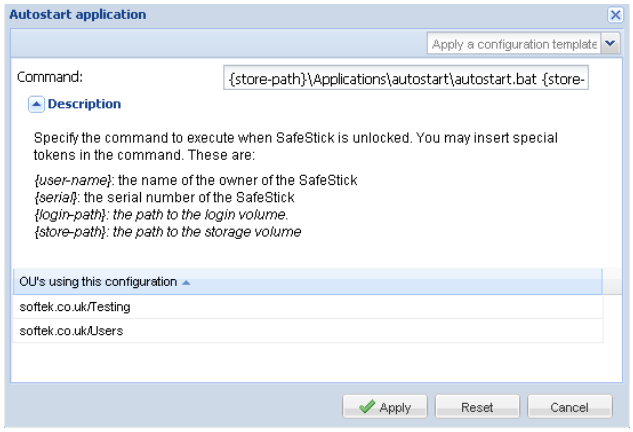
NOTE: It is probable that you will wish to start multiple applications, so while it is possible to simply call a single EXE directly, this is not advised. As detailed below, we strongly recommend that you create and call a script that can then handle multiple applications, and parse multiple switches and error conditions without too much additional modification;

1) Start the SafeConsole E² interface in your web browser as normal for example; https://safeconsole.mycompany.com

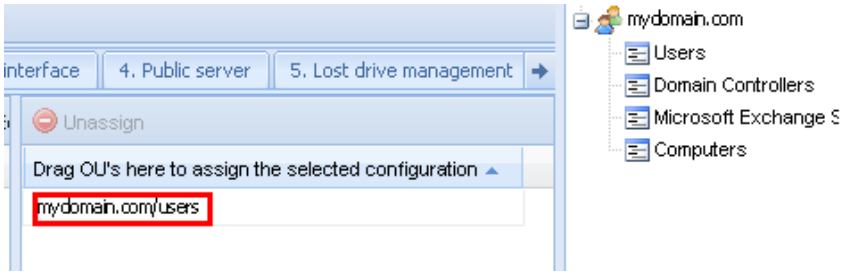
2) Navigate to “Usage”, then “Autostart Application”

3) Click “Create Configuration” and enter the following string in the “Command” box

   {store-path}\Applications\autostart\autostart.bat {store-path}



4) Once you have created the Policy assign it to an OU group by dragging the group from the right hand window. **NOTE** you may wish to use a separate OU group for initial testing.



5) In Windows Explorer, navigate to your Published UNC share - for example;

\\myserver\publisher

…and create a folder “autostart”.

6) Inside the autostart folder, create a simple text file called “safestick.ini” and insert the following lines (this will hide this script file / stop it appearing in the users shortcuts menu);

[starter]
hidden=yes

7) Create a new file “autostart.bat” text file and simply insert something the following

@ECHO OFF
%1Applications\opera\opera\opera.exe

NOTE: The “operalauncher.exe” file in the %1Applications\opera folder is used by the shortcuts menu and should not be called directly from Autostart.

8) Save the file – making sure it is just called “autostart.bat” and not “autostart.bat.TXT”

The next time a user in this OU group unlocks their SafeStick, this new autostart file will be pushed to their safestick and executed.

This will start Opera portable after the stick has been unlocked.

NOTE: You can add multiple entries into the autostart.bat script file to do any number of things – However not all apps will be able to be started like this – due to different programming and design issues.

Please consult other StickApp apps install guides, for specific documentation on additional switches, commands, sub-routines and other information which may be required to autostart them.

10. Un-Installing StickApps

StickApps are easily uninstalled – either individually or all installed StickApps completely - from users SafeSticks.

Option 1.

To remove ALL StickApps, start SafeConsole and disable the Publisher policy completely, or edit the Publisher policy from a selected OU as required.

The next time SafeSticks poll into SafeConsole to obtain policy, it will “know” that Publisher has been disabled and will delete all files from the <safestick driver letter>\Applications folder completely. Shortcuts will also be removed.

NOTE: Password Manager data will always be retained as it is stored in <safestick driver letter>\My Roboform Data

Option 2.

From your published share – for example \\myserver\publisher delete one or more StickApp folders as required.