



# QUICK GUIDE

This guide will give you insight in how to configure your SafeConsole and get more acquainted with a selection of features.

If you walk through this guide and start using your drive you will quickly realize the power SafeConsole can bring to your secure USB flash drives.



# SafeConsole Overview

SAFECONSOLE QUICK GUIDE



Activate and configure SafeConsole features from these tabs

Navigate to different views

The screenshot shows the SafeConsole web interface. At the top, there is a 'Change language' dropdown. Below it, a navigation bar contains tabs for 'Security Configurations', 'Usage Configurations', and 'Device Administrator Tools'. Under 'Security Configurations', there are sub-tabs: '1. Device State Management', '2. Password Policy', '3. Inactivity Lock', '4. FileRestrictor', and '5. Authorized Autorun'. The 'Device State Management' sub-tab is active, showing a configuration table with columns for 'Configuration' and 'Unassign'. The table contains two rows with 'lost drive message' settings. To the right of the configuration table is a list of Organizational Units (OU's) for assignment: 'acme.com/Manufacturing/Americas', 'acme.com/Manufacturing/Asia/Japan', and 'acme.com/Research/Central lab'. On the far right, a tree view displays the organizational structure for 'acme.com', including 'Management', 'Sales', 'Research', 'Manufacturing', and 'Europe' with its sub-units.

Your organizational structure

# Setup & The Console

SAFECONSOLE QUICK GUIDE



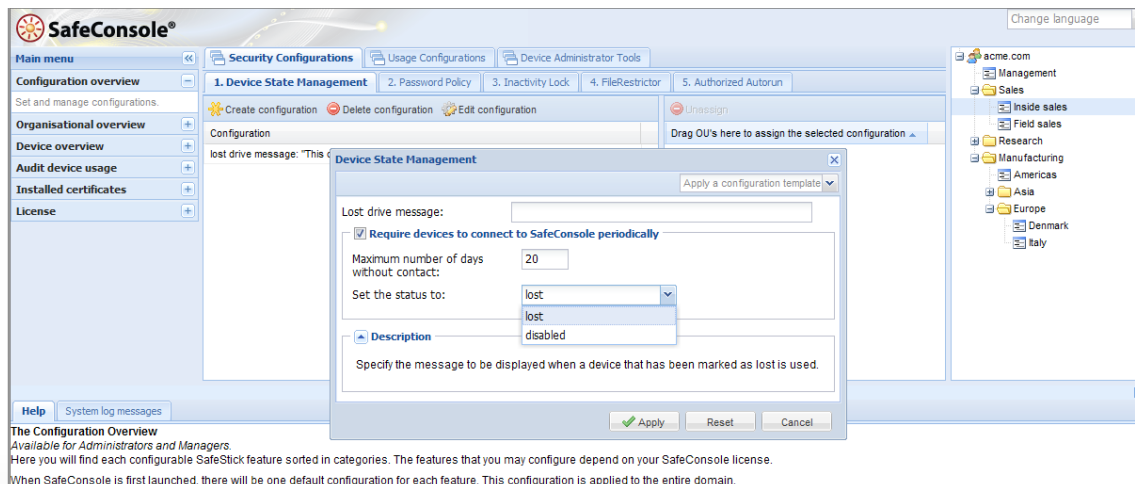
## SETUP

You can either get an online trial or download and install the standalone server. The setup procedure is explained in the Quick Start Guide PDF included in the SafeConsole Download Package.

## THE CONSOLE

### FIRST LOOK

The first screen you will see after logging in to SafeConsole is the Configuration Overview interface. The interface tabs, from which you can activate and configure any SafeConsole feature, are divided into three categories: Security Configurations, Usage Configurations and Device Administrator Tools.



On the right side of the interface is the organization structure pane. If you haven't synchronized SafeConsole with an active directory, the pane will contain only your organization name, but if you have, the pane will reflect all the organizational units of your organization. The bottom pane will display the help segment for your current view. The menu on the left can be used to navigate to other views.

# Setting Up Policies - Passwords

SAFECONSOLE QUICK GUIDE



## SETTING UP POLICIES

The first step is to set up your policies.

**Hint:** If you go to the 'Organisational overview' you can configure all features without navigating the tabs to find a certain feature. This is the quick and easy way to set up a default policy for your SafeConsole.

### PASSWORDS

#### PASSWORD POLICY

*Benefit: Ensures that your data is protected by strong compliant passwords.*

Let's start with a password policy. By double clicking on the configuration stating '8 characters, one digit (1)... etc' you will get a configuration window where you can set the complexity requirements for your drives. If you specify 6 characters and uncheck all the boxes you will be able to set a non complex password on your drive.

#### CREATE EXCEPTION POLICIES TO PARTS OF THE ORGANIZATION

If you have an active directory, try to create a new configuration as well with an alternate policy by clicking 'Create configuration'. Specify a more complex password policy by selecting all the tick boxes and then click 'apply'. You can now select the new complex configuration and then drag and drop a part of the organization to the empty pane on the right hand side of the window (visible in Illustration 1).

#### REMOTE PASSWORD RESET

*Benefit: Administrators can assist remote off-line users back to work within minutes without any loss of stored data.*

Go to the 'Usage configuration' tab and edit the configuration for 'Remote password reset'. Insert a support email address, a subject and check the box 'ask for user email address'. Click 'Apply'

You will now be able to recover passwords from a secure USB drive once the drive has been initialized with a password.

**Hint:** In the subject of remote password email, type: 'recover my {serial}'. This way it will be easier for you to find the drive if you evaluate multiple drives.

# ZoneBuilder & Publisher

SAFECONSOLE QUICK GUIDE



## ZONEBUILDER – TRUST USER ACCOUNTS

*Benefits: Offload work from helpdesk by having user's self-service their password resets. Allow users that have already securely authenticated to their user accounts to have immediate access to their secure file storage on the device – 'just as quick and simple as an old fashion USB drive, but secure'.*

To activate ZoneBuilder, check the box for "Enable ZoneBuilder" and then click "Apply."

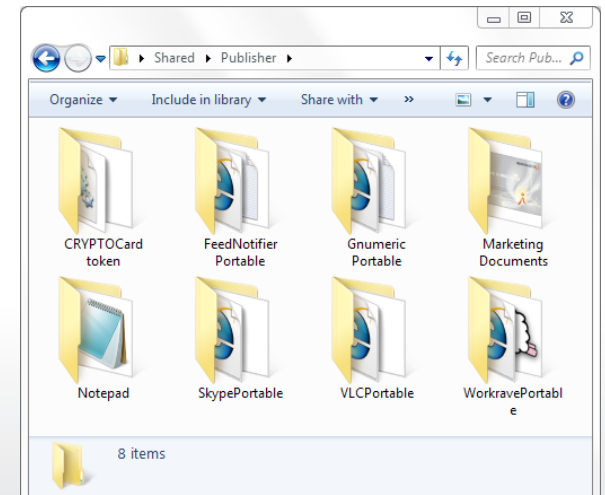
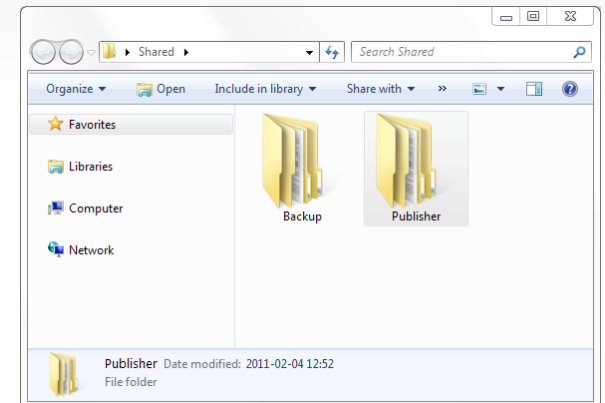
This will enable your drive to trust your account on your computer, so you won't have to enter a password to unlock your drive on that account.

## PUBLISHER – CONTENT DISTRIBUTION

*Benefit: Securely distribute a folder with files and applications to select devices in the field. This enables quick distribution of sensitive files and the ability to maintain portable software on the devices.*

**Note:** To do this you will need to have a network share folder available (see instructions on the following page). This network share can be a share on your own computer if you are running SafeConsole standalone but it can also be a shared folder in your network. You should now activate Publisher.

- Please open your shared folder (UNC path) and create a folder therein called 'publisher'. This will be your base publisher path.
- In the base path you can now create subfolders that will serve as packages to be published (Illustration 2). Please create a subfolder and name it 'files' for example.
- In the 'files' folder you can place your files to be published
- Create a portable application package and put an application in there (please see example below)
- In the SafeConsole, enter your path to the publisher folder (e.g \\computer\share\publisher) and click apply. The files will now be sent to your secure USB flash drives once they have been unlocked. You will also get a menu item for each package.



# Share Folders & Portable Applications

SAFECONSOLE QUICK GUIDE

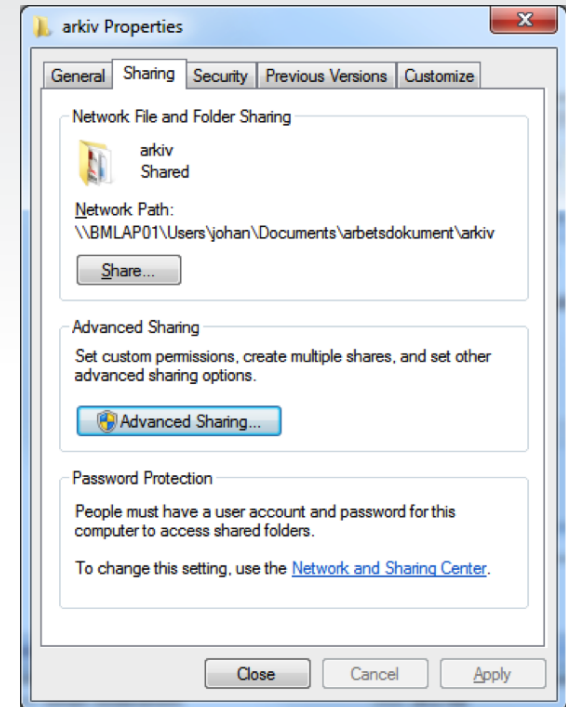


## SHARE FOLDERS

To share a folder on your PC, navigate to the folder you would like to share, right-click on it and choose 'Properties.' In the 'Share' tab you can see the path of the shared folder. To share the folder, click 'Advanced sharing' and then 'Share this folder.' Again, you will be able to see the UNC path in the 'Share' tab.

**Important!** This will now be your share path in which you must create a publisher folder. It is in the publisher folder you can place packages (as subfolders). Any files placed directly in the share folder or the publisher folder will not be published.

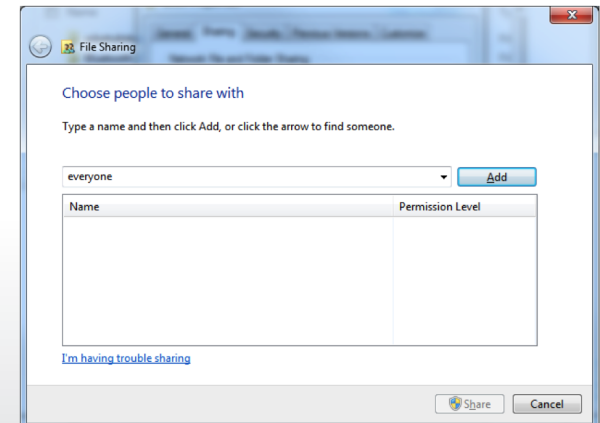
**Note:** In Windows XP you will not be able to see the resulting path of the share but you will be able to choose a name for the share. If you specify 'myshare' as the name, the resulting path will be: \\mycomputer\myshare – where 'mycomputer' is the name of your computer (visible by right clicking on 'My computer' in the start menu and then under the 'computer name' tab).



### INFO

## EXAMPLE OF A PORTABLE APPLICATION

Please download Skype portable installer from [http://portableapps.com/apps/internet/skype\\_portable](http://portableapps.com/apps/internet/skype_portable). Run the installer and choose your publisher base path as the install directory. A folder called SkypePortable will be created in your Publisher base path.



# EasyShare & File Audit Trail

SAFECONSOLE QUICK GUIDE



## EASYSHARE

*Benefits: Stops the bad habit of sharing and disclosing passwords to the secure devices and exposing all securely stored files. Allows sharing of data with untrusted machines and people.*

To activate EasyShare, navigate to the EasyShare configuration and click 'enable EasyShare'. You can leave the password length field with 4 characters.

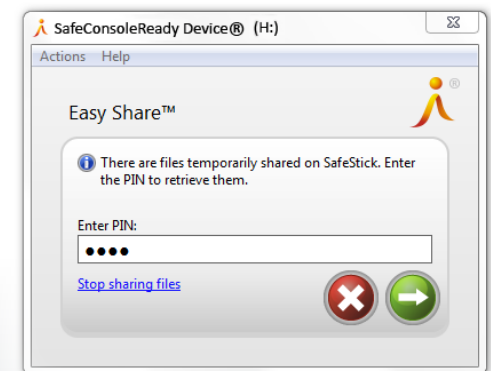
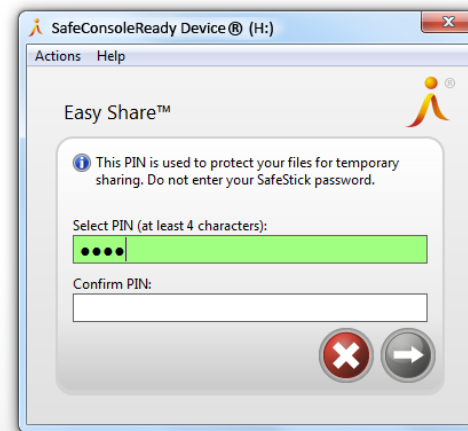
You will now be able to share a single set of files from the secure drives by activating 'EasyShare' from the USB drive login application.

## FILE AUDIT TRAIL

*Benefit: Allows organizations to achieve compliance.*

The last feature to activate in this guide is the File Audit Trail. Navigate to the configuration (under Device administration) and activate it with the 'enable' checkbox.

By clearing the text field with file types you will enable audit of all files. Clear the text field and click 'apply'.



# Using The Features

SAFECONSOLE QUICK GUIDE



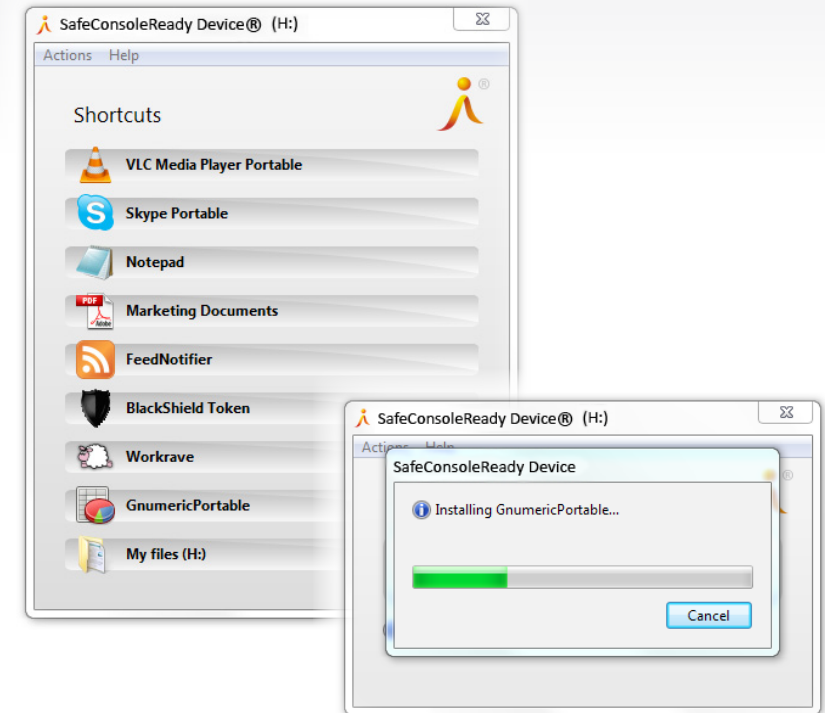
## USING THE FEATURES

Now the time has come to make use of the policies and features you have activated.

- Insert your drive and let it initialize (if you have autorun disabled you might have to start it from the login CD drive in 'my computer').
- When asked, confirm that you are the owner of the drive and that you want to connect to the SafeConsole (if you are not prompted for ownership you haven't deployed the server correctly, please see the manual or Quick start guide for troubleshooting).
- Note that your password complexity requirements will have been applied when you choose your password and click continue.
- You will now see a screen alerting you that your account has been trusted. This is thanks to ZoneBuilder.
- The next screen should prompt you for your name and email. This is to validate your identity during future password resets.
- Unlock the drive by typing your password once more, and your files from 'Publisher' will be installed on the drive. A menu will now be displayed which allows you to access your files or the published packages directly. Please note that Skype will be installed on the drive if you followed the example above.
- You can also access the other features from the 'Actions' menu .

### EASYSHARE

- Select EasyShare and then choose one or more files from your drive to share
- Choose a temporary password for your shared files
- Lock the drive from the actions menu.
- If you choose EasyShare again, you will be prompted for a password and you can then save the files to where you see fit.



**Hint:** You can also use EasyShare to get files from someone else without giving out your password. Simply hand this someone the drive and tell them to activate EasyShare and they can import files to it without unlocking your drive.

# Using The Features

## SAFECONSOLE QUICK GUIDE



### PASSWORD RESET

- Select 'Forgot password' from the 'Actions' menu. You will see a screen with an 8 character code. Copy this code and go back to your SafeConsole. (Hint, you can also click the email address in the window and an email will be generated with the recovery code)
- In the SafeConsole, navigate to the 'Device overview' and search for your USB flash drive by entering the name you used when connecting to the SafeConsole the first time and then click 'search'. You will see a list of drives with information on ownership, date used and software version.
- Select your drive and click 'Recover password'. You can now paste your 8 character code in the field and then click 'I have verified the user identity'. A new, 20 character code will be shown below along with your email address.
- Click your email address or copy the new code
- Feed the 20 character code into the 'Forgot password' screen on the USB flash drive login application and click next
- You can now choose a new password.



**Note:** Neither you or your administrator can see or derive the real password at any time. This is an important security aspect.

**Q:** Do I have to be online to perform a password reset?

**A:** No, you can perform a password reset on an offline computer thanks to the challenge response system, which can be used via email or phone.

The screenshot shows the SafeConsole web interface. The 'Device overview' table lists several devices with columns for Serial, Owner, Firmware version, Status, Updated, and Last used. A modal dialog titled 'Enter the Password ID code supplied by Lewis Weaver' is open, showing a checked checkbox 'I have verified the identity of Lewis Weaver' and a text input field. Below the input field, there is a section for 'Send the PUK code to the user'.

Serial	Owner	Firmware version	Status	Updated	Last used
0000700000000000	acme.com/Manufacturing/Ryan Morin	4.0.2	in use	No	
0000700000000001	acme.com/Manufacturing/Americas/Cory Pena	4.0.2	in use	No	
0000700000000002	acme.com/Manufacturing/Asia/Cono, Elmas...	4.0.2	in use	No	
0000700000000003			in use	No	
0000700000000004			in use	No	
0000700000000005			in use	No	
0000700000000006			in use	No	
0000700000000007			in use	No	
0000700000000008			in use	No	
0000700000000009			in use	No	
000070000000000A			in use	No	
000070000000000B			in use	No	
000070000000000C			in use	No	
000070000000000D			in use	No	
000070000000000E			in use	No	
000070000000000F			in use	No	

# Using The Features

SAFECONSOLE QUICK GUIDE



## ZONEBUILDER

- Choose lock and exit and then pull out your drive and reinsert it
- Notice how the drive unlocks automatically. You can now use your Secure USB flash drive as quick and easy as you could with a standard flash drive. Note. You are still secure, when you insert your drive into another computer or logged in as another user you will be prompted for the password.

**Extra 1:** You can trust more computers or user accounts by inserting your drive in that computer and then choosing "Trust this user account" from the "Actions" menu.

**Extra 2:** If you lock the drive and then enter the wrong password three times, you will be prompted to reset your password the next time you insert the drive in a trusted computer.

**Extra 3:** You can easily remove accounts from on the list on the "Show trusted user accounts" page.

File Audit Trail

## FILE AUDIT TRAIL

- Open the browser with SafeConsole again
- Navigate to the 'Device audit overview'
- Click search and see all your actions and files being shown in the log window. This window will also display; the time of each event, the logged in user and the computer name

## REMOTE KILL

- To finish the tour, you can optionally reset the drive from the SafeConsole. Navigate to the 'Device overview' page again
- Find your drive and choose 'Factory reset' (and then click yes)
- Pull out your drive once more and then reinsert it
- Wait for the reset progress to finish.



Thanks for reviewing these features of SafeConsole. The full SafeConsole Manual (available from the "Start" menu) contains instructions for all the other features of SafeConsole.