



**SAFECONSOLE<sup>®</sup>**

# ZoneBuilder Overview

Version 1.0





## WHAT IS ZONEBUILDER ?

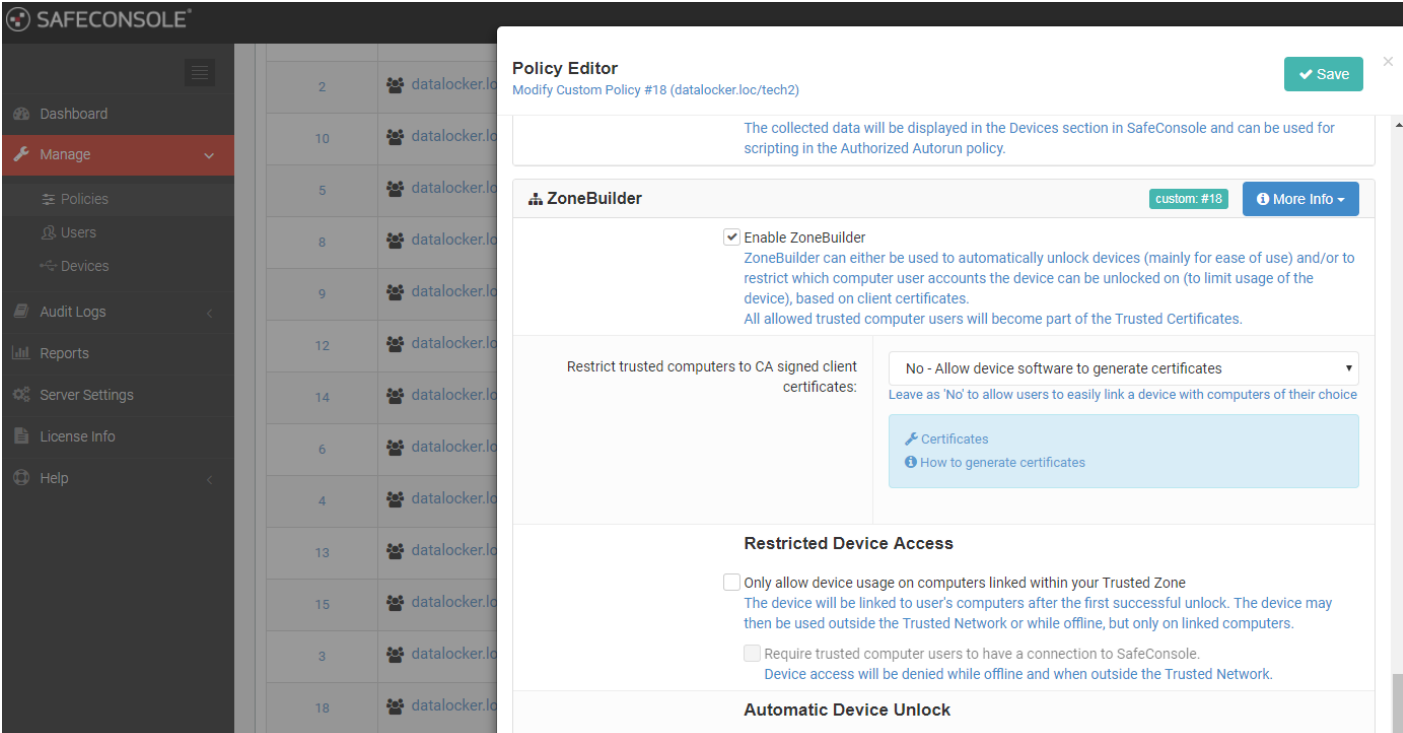
Zonebuilder is a tool to create a “trusted zone” of computers that makes using your SafeConsole managed devices even more Simply Secure.

## HOW TO CREATE A “TRUSTED ZONE”

- 1 White list the computer IP address in SafeConsole
- 2 Plug-in your SafeConsole Ready storage device and enter the device password.  
Your computer has been registered into your Trusted Zone!

## WITHIN YOUR “TRUSTED ZONE”, YOU CAN:

-  **RESTRICT** device access to computers inside your Trusted Zone.
-  **AUTO-UNLOCK** your storage device eliminating the need to enter your password. It makes sharing files within your Trusted Zone quick and easy. This feature uses RSA client certificates for authentication.



**SAFECONSOLE™**

Dashboard  
Manage  
Policies  
Users  
Devices  
Audit Logs  
Reports  
Server Settings  
License Info  
Help

**Policy Editor**  
Modify Custom Policy #18 (datalocker.loc/tech2) Save

The collected data will be displayed in the Devices section in SafeConsole and can be used for scripting in the Authorized Autorun policy.

**ZoneBuilder** custom: #18 More Info

**Enable ZoneBuilder**  
ZoneBuilder can either be used to automatically unlock devices (mainly for ease of use) and/or to restrict which computer user accounts the device can be unlocked on (to limit usage of the device), based on client certificates.  
All allowed trusted computer users will become part of the Trusted Certificates.

Restrict trusted computers to CA signed client certificates:  
No - Allow device software to generate certificates  
Leave as 'No' to allow users to easily link a device with computers of their choice

[Certificates](#)  
[How to generate certificates](#)

**Restricted Device Access**

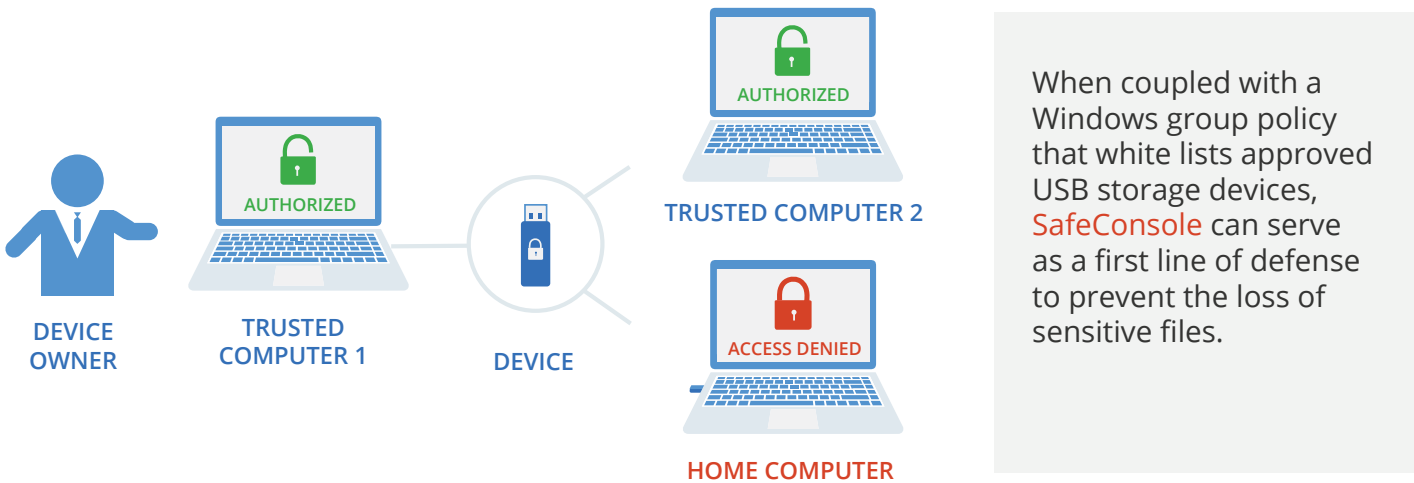
Only allow device usage on computers linked within your Trusted Zone  
The device will be linked to user's computers after the first successful unlock. The device may then be used outside the Trusted Network or while offline, but only on linked computers.

Require trusted computer users to have a connection to SafeConsole.  
Device access will be denied while offline and when outside the Trusted Network.

**Automatic Device Unlock**

## USE CASE: DLP SOLUTION

Prevent your team from copying sensitive data from your Trusted Zone to an unknown computer.

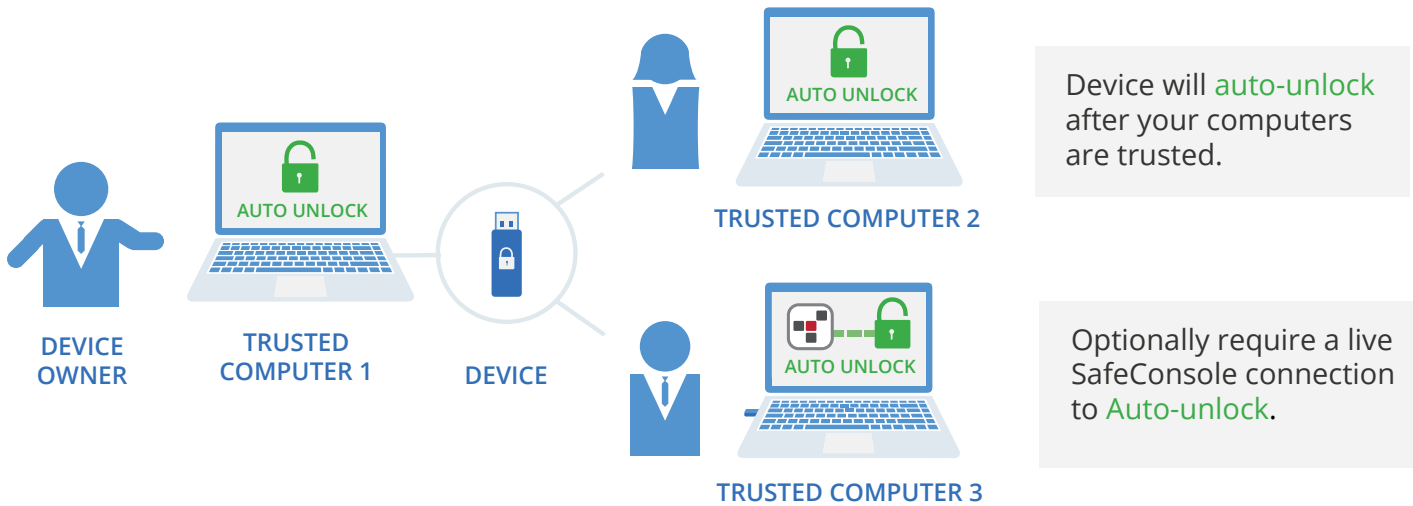


### BENEFIT

Only approved SafeConsole USB storage devices can be used within your Trusted Zone and those devices cannot be used outside the Zone.

# USE CASE: SECURE FILE SHARING

Sharing your encrypted device with the team using 'Auto-unlock' mode.



## BENEFIT

The device owner does not have to share the device password when sharing files with other members within the trusted zone.