

USER MANUAL

SafeStick

----- Sep 2017 -----



Contents

About this User Guide

- 3 System Requirements
- 4 Recommendations

Setup

- 5 Setup- Windows
- 6 Setup- Mac
- 7 Device Initialization
- 10 Device Usage

About this User Guide

This quick start guide is for SafeStick®, a Forced Managed Secure USB device managed by SafeConsole®.

For more information on the central management service, visit safeconsole.com.

SYSTEM REQUIREMENTS

PC Platform

- 1-GHz Processor (or faster)
- 300MB free disk space
- USB 2.0/3.0
- Two available consecutive drive letters after the last physical drive

PC Operating System Support

- Windows 10
- Windows 8, 8.1 (non RT)
- Windows 7 (SP1)
- Windows Vista® (SP2)

Mac Platform

- 15MB free disk space
- USB 2.0/3.0

Mac Operating System Support

- Mac OS X 10.9.x - 10.12.x

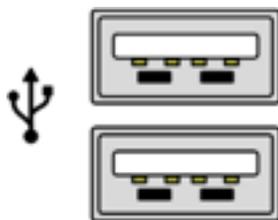


Figure 1.1 – USB 2.0/3.0 Ports, Type A



Figure 1.2 – SafeStick

RECOMMENDATIONS

To ensure there is ample power provided to the SafeStick device, insert it directly into a USB 2.0/3.0 port on your notebook or desktop, as seen in **Figure 1.3**. Avoid connecting it to any peripheral device(s) that may feature a USB port, such as a keyboard or USB-powered hub, as seen in **Figure 1.4**.



Figure 1.3 – Recommended Usage



Figure 1.4 – Not Recommended

SETUP (Windows Environment)

Step 1. Insert the SafeStick into an available USB port on your notebook or desktop and wait for Windows to detect it.

- Windows Vista/7/8/10 users will receive a device driver notification as seen in **Figure 2.1**.

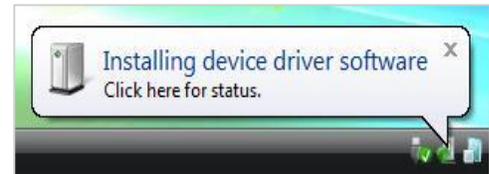


Figure 2.1 – Device Driver Installation

Once the new hardware detection is complete, Windows will prompt you to begin the initialization process.

- Windows Vista/7/8/10 users will see an AutoPlay window similar to the one in **Figure 2.2**.

Step 2. Select the option 'Unlocker.exe'

If Windows does not AutoPlay, you can browse to the CD-ROM partition (**Figure 2.3**) and manually execute the Unlocker program. This will also start the initialization process.

DVD RW Drive (D:) Login U...

Choose what to do with this disc.

Install or run program from your media

Run Unlocker.exe
Published by DataLocker Inc.

Other choices

Open folder to view files
File Explorer

Take no action

Figure 2.2 – AutoPlay Window

(Note: Menu options in the AutoPlay window may vary depending on what programs are currently installed on your computer. AutoRun will start the initialization process automatically.)

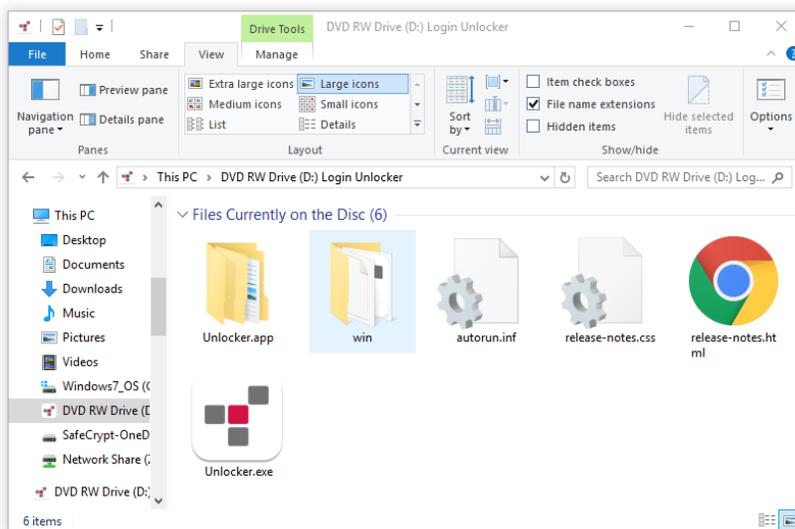


Figure 2.3 – SafeStick Contents

SETUP (Mac Environment)

Insert the SafeStick into an available USB port on your Mac notebook or desktop and wait for the operating system to detect it. If the 'Login' volume (**Figure 3.1**) does not appear on the desktop, open Finder  and locate the 'Login' volume (**Figure 3.2**) on the left side of the Finder window (listed under **DEVICES**.) Highlight the volume and double-click the 'Unlocker' application icon on the 'Finder' window. (**Figure 3.2**) This will start the initialization process.



Figure 3.1 – SafeStick

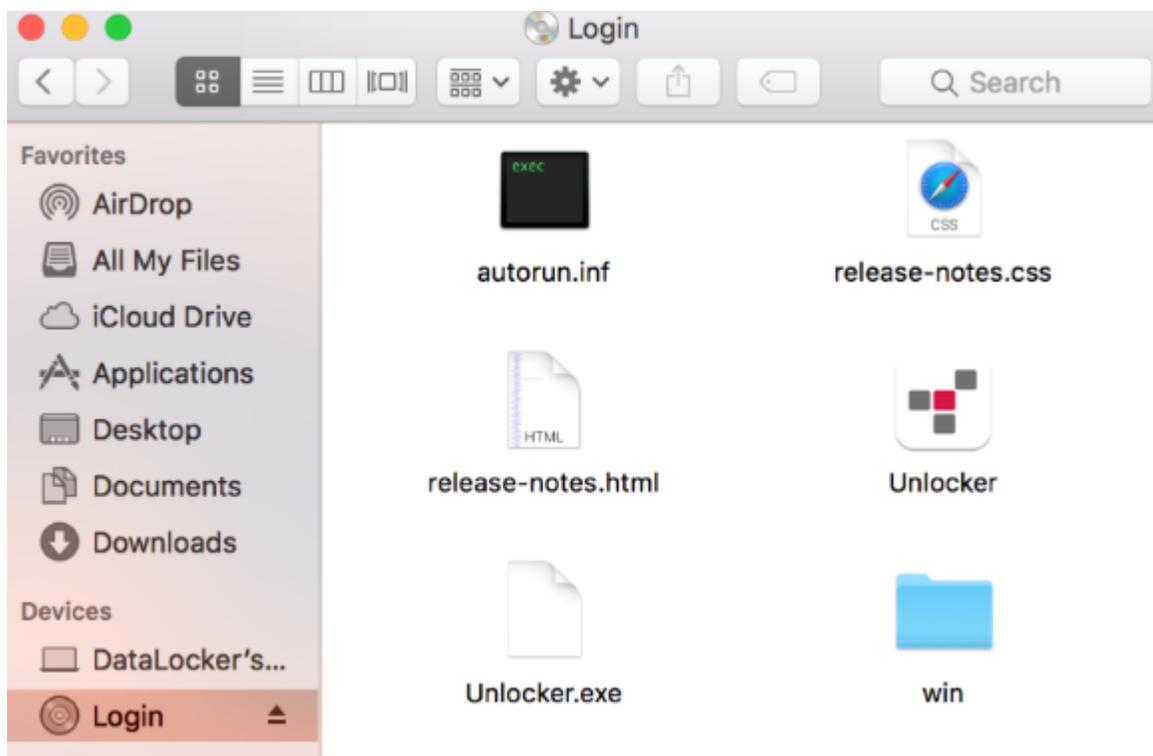


Figure 3.2 – Contents

DEVICE INITIALIZATION

Step 1. Enter a Connection Token. (**Figure 4.1**) A connection token is given by your SafeConsole administrator usually through email. After entering a valid connection token click **[Check token]**.



Figure 4.1 – Connection Token

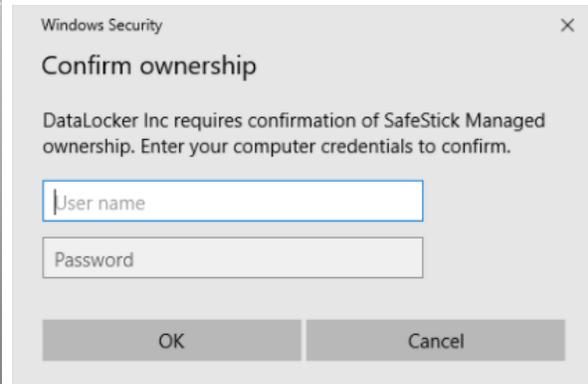


Figure 4.2 – Confirm Ownership

Step 2. Confirm the connection to the SafeConsole Server. Depending on the server settings configured by your SafeConsole Admin, you may be asked to enter any of the following:

- Confirm Ownership - SafeConsole uses your computer's credentials to assign the correct policy to the SafeStick. You will need to enter the username and password that you use to unlock the computer that the device is currently plugged into. (**Figure 4.2**)
- Unique Registration Token - (**Figure 4.3**) Along with a connection token, you may also receive a unique token. This token allows for a different deployment strategy. If you are prompted for a token that you do not know, please check your email then contact your SafeConsole Admin.

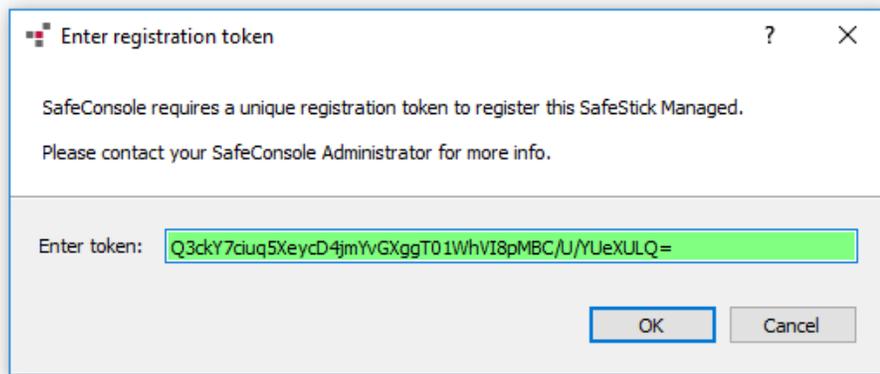


Figure 4.3 – Unique Token

- Your email address - SafeConsole Admins will need your email address to send password recovery codes. You will need to enter and confirm your email address if prompted (**Figure 4.4**).

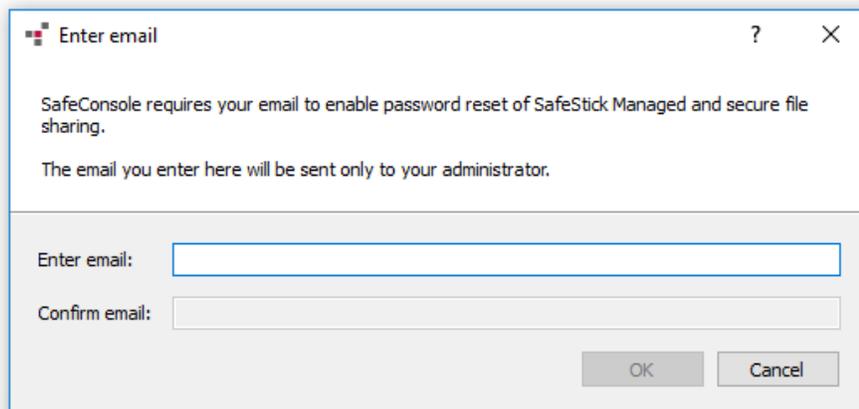


Figure 4.4 – Email Address

- Information about yourself - Extra information required by the SafeConsole Admins before device can be registered. Please see your SafeConsole Admin for any documentation on how these fields should be filled out if present. (**Figure 4.5**)

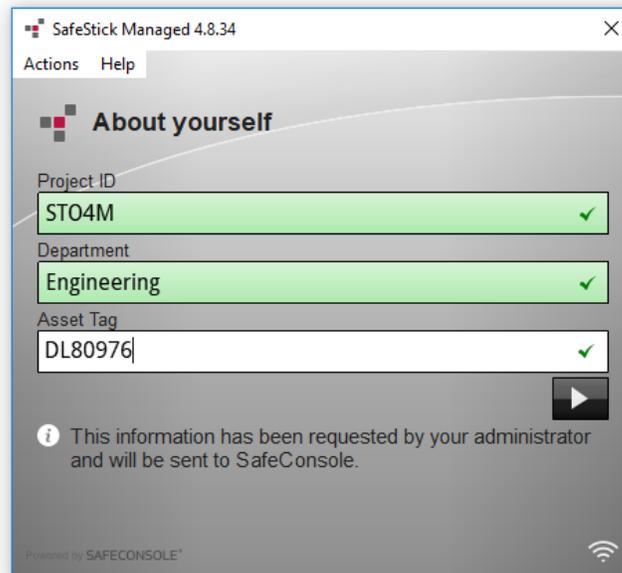


Figure 4.5 – About Yourself

Step 3. Create a Password.

Select a password that follows your company's password requirements which may be different from the one shown. (**Figure 4.6**)

Once a password has been selected (and it meets the specified criteria), you must enter it a second time in the 'Confirm Password' text box to ensure proper entry. Optionally, you may be allowed to create a password hint depending on your company's password policy. The warranty acknowledgement must be checked before you can click **[Confirm]**.

This will complete the initialization steps.

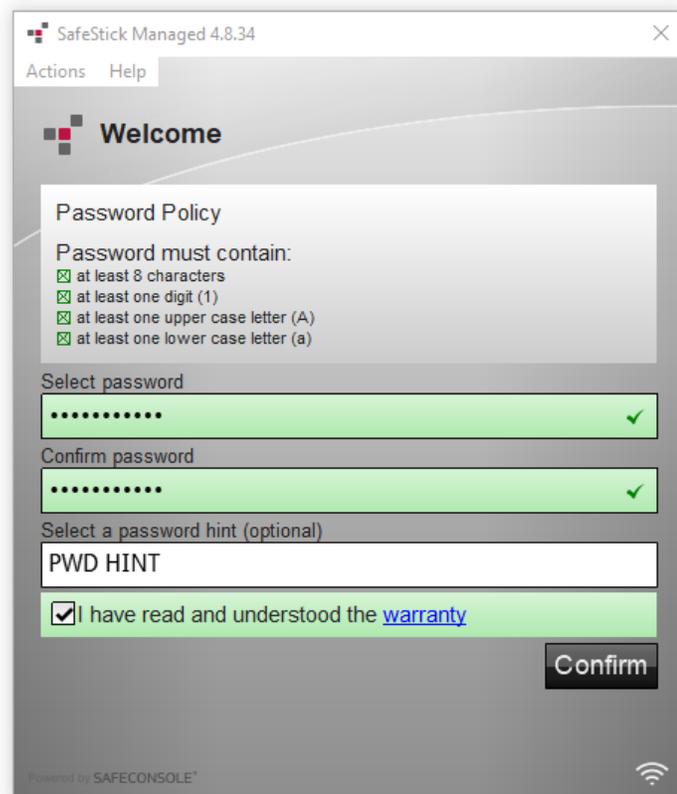


Figure 4.6 – Password Creation

DEVICE USAGE

With each insertion of the SafeStick, you will be prompted to enter the password created during the initialization process (**Figure 5.1**). During the login process, if an invalid password is entered (**Figure 5.2**), you will be given another opportunity to enter the correct password; note that there is a built-in security feature that tracks the number of invalid login attempts and if this number reaches the pre-configured value of 10 (maximum number of invalid logins), the SafeStick will lock the user out and require a password reset from a SafeConsole Administrator. **Figure 5.5**

(Note: Prior to locking the device with 10 invalid password attempts, the login counter will reset with a successful login.)

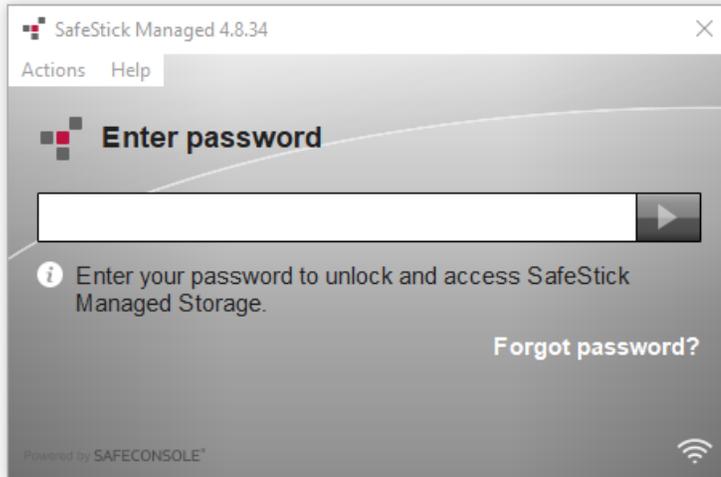


Figure 5.1 – Enter Password

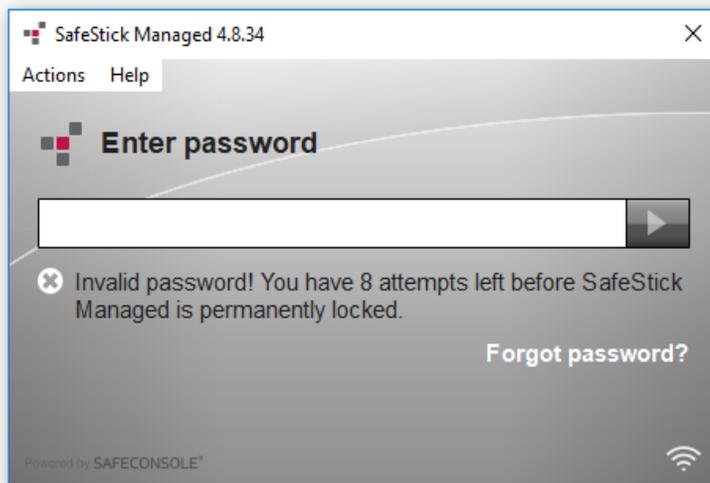


Figure 5.2 – Login Failure

DEVICE USAGE

Once the device is unlocked with the correct password, your files are ready to be stored on the Private USB partition. This private USB partition will show up to the operating system like a normal USB storage device allowing files to be transferred with the system's file manager or any application that allows saving to an external location.

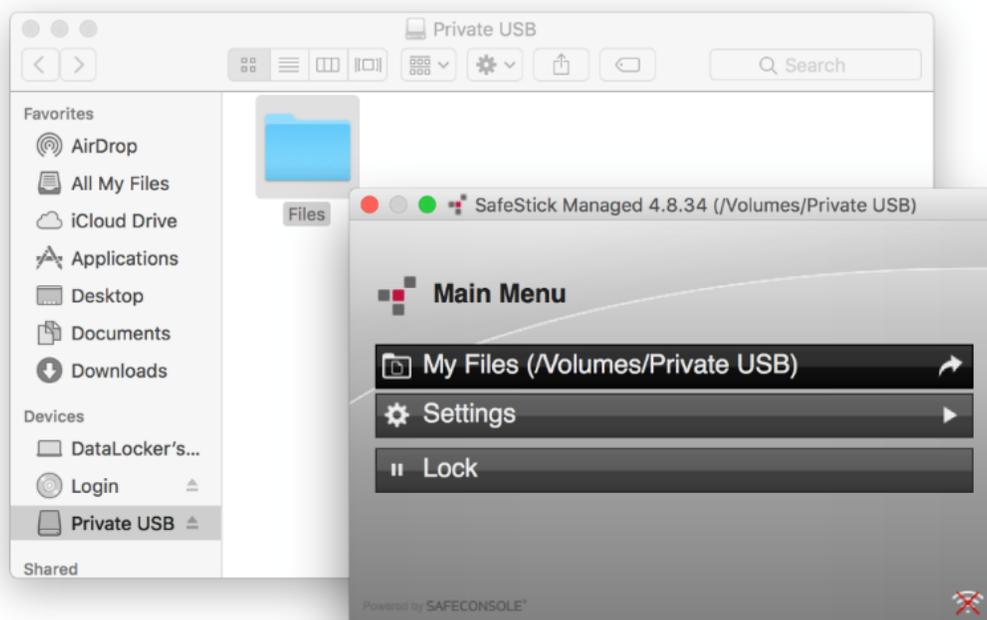
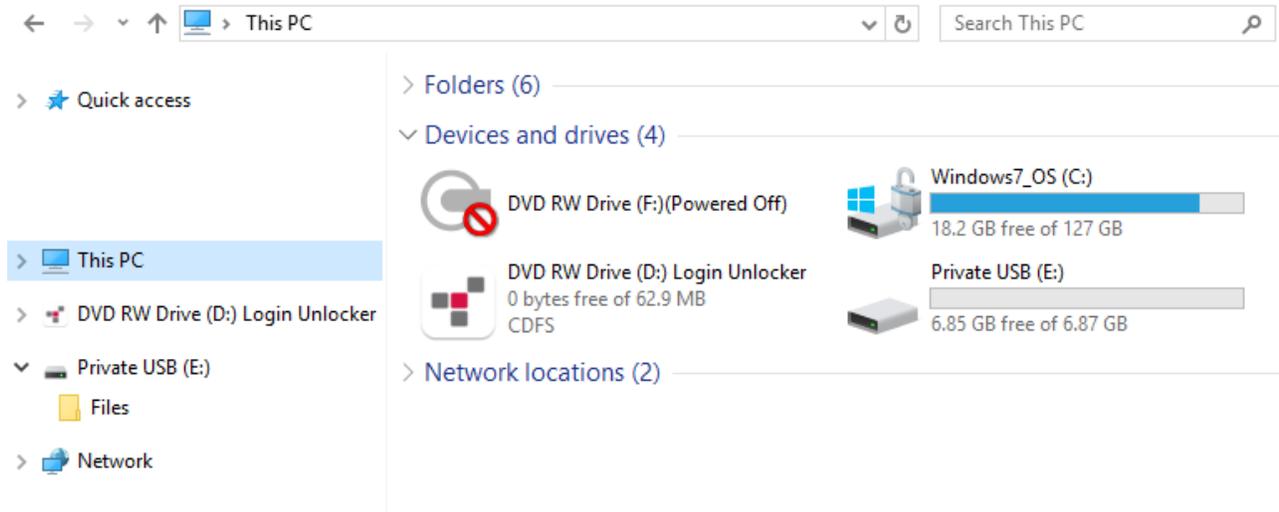


Figure 5.4 – Unlocked, Mac

DEVICE USAGE (Password Reset)

If enabled by your SafeConsole Administrator, a password reset can be done at anytime by clicking **[Forgot Password?]** on the login screen (**Figure 5.1**).

When at the Password Reset Screen (**Figure 5.5**), the SafeStick Client will present your password ID.

You will need to contact your SafeConsole Administrator using either the email link or phone number provided. Your administrator may require additional information to verify your identity.

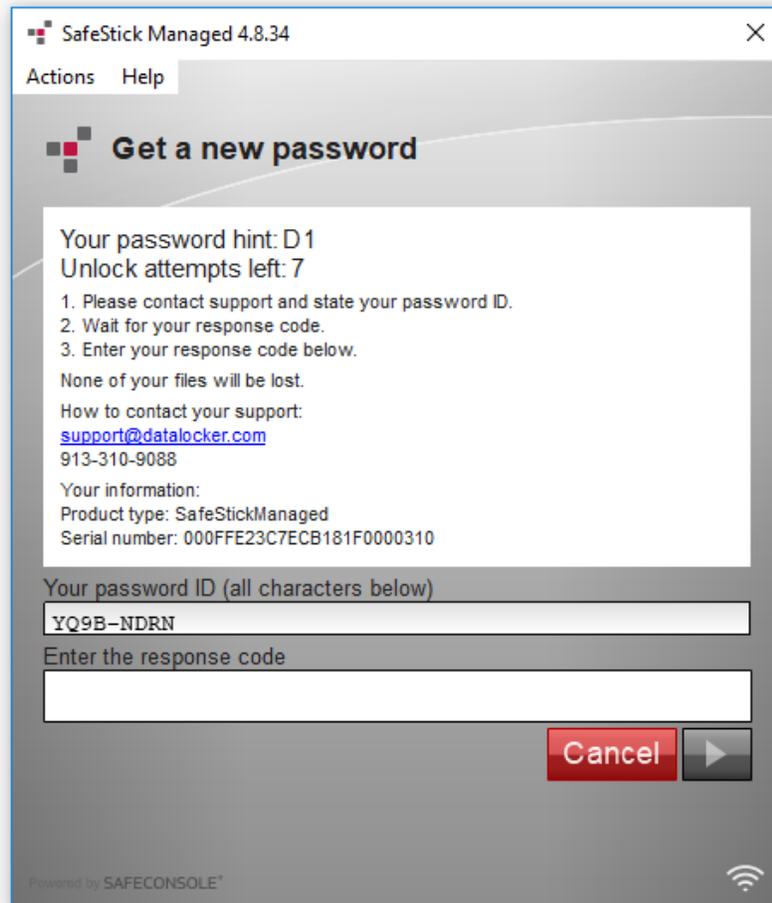


Figure 5.5 – Password Reset

After verification, you should receive a response code from your SafeConsole Administrator. Entering this response code and clicking the green arrow will allow you to change your password. (**Figure 5.3**) You will likely receive the response code via email. However, if needed, the response code can be given orally over the phone in situations where no network access is available. In these situations it is important that the response code is entered correctly, as an invalid response code can trigger the brute force protection and cause the data on the device to be wiped.

*Actual Device Usage may depend on the configuration of your SafeConsole Server.