SAFECONSOLE®

WHITE PAPER

Best Practices for Password Management of Encrypted USB Flash Drives

If you have a need for mandatory password protected portable data storage you must consider best practices for the management of passwords for these devices. Security industry organizations such as the SANS Institute and (ISC)² put strong emphasis on the handling of passwords in access controls. These best practices offer technical decision guidance and highlight important focus areas when electing a solution. It is important to recognize from a business decision perspective that password management highly affects the overall costs

INTRODUCTION

When selecting a secure storage solution the need for solid password management is a must have. The way passwords are managed i.e. their change and reset processes are pivotal to the security of the password protected USB drive. It is critical that the password management follows security industry best practices to motivate the investment into hardware encryption. You may have heard “a chain is only as strong as its weakest link”, therefore, weak password management will lead to weak security no matter the level of encryption. As stated in information system security best practice from (ISC)2 for CISSP® CBK® [1] it is clear that the security of a device that relies on a password for its access control, is completely reliant on the management of that password to uphold the security of the protected stored data.

Password management is often one feature of many, in a broader device management solution but it is the most critical feature given the nature of the design of these solutions.

These best practices focus on achieving a full password management solution, this can only be attained

ADVISED BEST PRACTICES

It is advised to adhere to the following best practices in the management of passwords of secure storage devices.

- Ensure the solution does not allow the user to enter the password in any free text field on the device such as a hint field. This will lead to unsecure and unwanted user behavior.
- Offer the option of a password hint but ensure that it cannot contain the password. If your policy decision is to disallow hints, confirm that it can be deactivated.
- The user’s data must be intact after the password reset has been completed.
- The solution must prompt a mandatory password change upon each password reset request. This avoids the risk of someone breaching the password reset process and then making use of both old and new passwords without the end-user being aware of the passwords being exposed.
- The password reset must never expose the old forgotten password to administrators as this is not required information and could cause a data breach situation. Users are known to share passwords between services and a flawed password handling process can expose a password that is used in a system that has a higher classification than the drive itself. The SANS Institute Password Policy template which refers to this as: one user [must be able to] take over the functions of another without having to know the other’s password.
- The password reset policies should be controlled by the administrator not the end user. If it is left to the end user to periodically change their password, it has been found that users most often do not do so until they have forgotten their password and it is too late to

activate the password reset process. Refusal by users to adopt new software systems is a highly recognized problem; any measures that can be taken to avoid end-user frustration during enrollment should be considered, as the cost of non-adoption is unacceptable.

- Offer a secure self-service password reset option which works locally on the trusted user account. This avoids unnecessary helpdesk calls.
- Offer an out-of-band method for resetting a password using voice or text messages utilizing a challenge response scheme. This allows for trusted password resets where there is no Internet available and ensures the availability of information at all times for authenticated users even when they have forgotten their device passwords.
- Avoid schemes that offer password backups. Storing an unencrypted, or even an obscured, list of passwords at a central location is a flawed security practice according to the SANS Institute: do not store passwords in clear text or in any easily reversible form.[2] It creates an unnecessary aggregated information asset that will require additional steps to be protected.
- Never accept the usage of master passwords as a substitute for a real password management scheme. The reasons for avoiding one password for all devices are numerous. One is the risk for a 'keys to the kingdom' attack. If the master password is known by a group of people in plain text, it risks exposing all drives if one individual becomes an insider threat. It also exposes the organization to the risk of administrators performing unaudited checks on users' devices. Further, it divides responsibility of the drives since numerous individuals could have access to the device. The biggest pitfall of having a master password is the maintenance it requires -- having one password to rule them all is a completely unmanageable approach because when the master password is exposed it needs to be changed immediately on all devices.
- To increase user adoption of the secure USB drives it may be advisable to allow a secure automatic unlock (Single Sign On, SSO) if the users have already authenticated themselves. This approach saves time and maintains the security since the drives will ask for the password when used on any other system but the registered users' own trusted system.

[1] *Official (ISC)2 Guide to the CISSP CBK, Second Edition, 2009*

[2] *http://www.sans.org/security-resources/policies/Password_Policy.pdf*

SAFECONSOLE.COM

To find your local SafeConsole Reseller
please visit datalocker.com for more information.