PSIClone™

User's Guide
Version 4.4

Law Enforcement & Government Addendum

DriveKey™

"Helping You Find What You're Looking For"

905 Industrial Blvd • LaBelle, FL 33935

www.cprtools.net • **info@cprtools.net**

Table of Contents

DriveKey™

The DriveKey™ feature is not available to the general public; this module is only made available to authorized Law Enforcement Organizations and Government agencies.

What is DriveKey™?

DriveKey™ represents a breakthrough in hard drive security manipulation. **On fully supported drives, DriveKey™ is able to retrieve the drive's security password, even if the drive was locked with the highest level of security supported by the ATA specification.**

For drives which are fully supported, DriveKey™ allows the retrieval of passwords which are in effect. For supported and unsupported drives, DriveKey™ acts as a user-friendly front-end to the locking and unlocking of drives at all security levels.

Launch DriveKey™ by clicking the Security button in the CPR Toolbox™ toolbar to reveal the DriveKey™ menu item. Click DriveKey™ to begin.

> **WARNING:**
> Use extreme caution when working with drives which are not fully supported. Locking a drive which is not fully supported can render the drive completely useless if the password is forgotten. **CPR Tools assumes no responsibility for drives locked and rendered unusable through misuse of DriveKey.**

> **NOTE:**
> Supported drives on either Side A or Side B of PSIClone™ may be locked or unlocked using DriveKey™.

User and Master Passwords

To understand the benefits of DriveKey™, a description of the workings of locking and unlocking drives using 'User' and 'Master' passwords is presented here.

DriveKey™ is a user interface which allows easy manipulation of the password security features implemented in the ATA specification.[1]

Security enabled ATA compliant hard drives use passwords to allow for security to be applied. These passwords, called 'User' and 'Master' may be used separately or together. The level of security depends entirely upon the choices made regarding which passwords are used.

Contrary to the naming conventions, the 'User' password is used to provide security. 'Master' passwords are used solely as an alternative method of unlocking a drive in certain instances.

> **DriveKey™ Key Feature:**
> Prior to DriveKey™, a drive locked with a User Password would be unusable without the User Password.
>
> With DriveKey™ support, this is no longer the case; fully supported, locked drives may simply be unlocked using DriveKey™.

To lock a drive, 'User' password must be used. The 'User' password has two possible levels of security:

1. High
   a. If a drive is locked with a user password in 'High' mode, either the Master password or User password may unlock the drive.
2. Max
   a. If a drive was locked with a user password in 'Max' mode, only the User password should be able to unlock the drive. The drive should be completely unusable without the correct 'User' password.

---

[1] The ATA specification is maintained by INCITS T-13 committee (http://www.t13.org)

DriveKey™'s feature set is best described through example. The first example will assume a fully supported drive so that all of DriveKey™'s features will be displayed.

Fully Supported Drives and DriveKey™

Assumptions for this example:

1. A fully supported drive is connected to PSIClone™ on Side B and is powered.
2. PSIClone™ has been attached to a USB 2.0 port on a host computer running CPR Toolbox™ version 4.0 or higher.
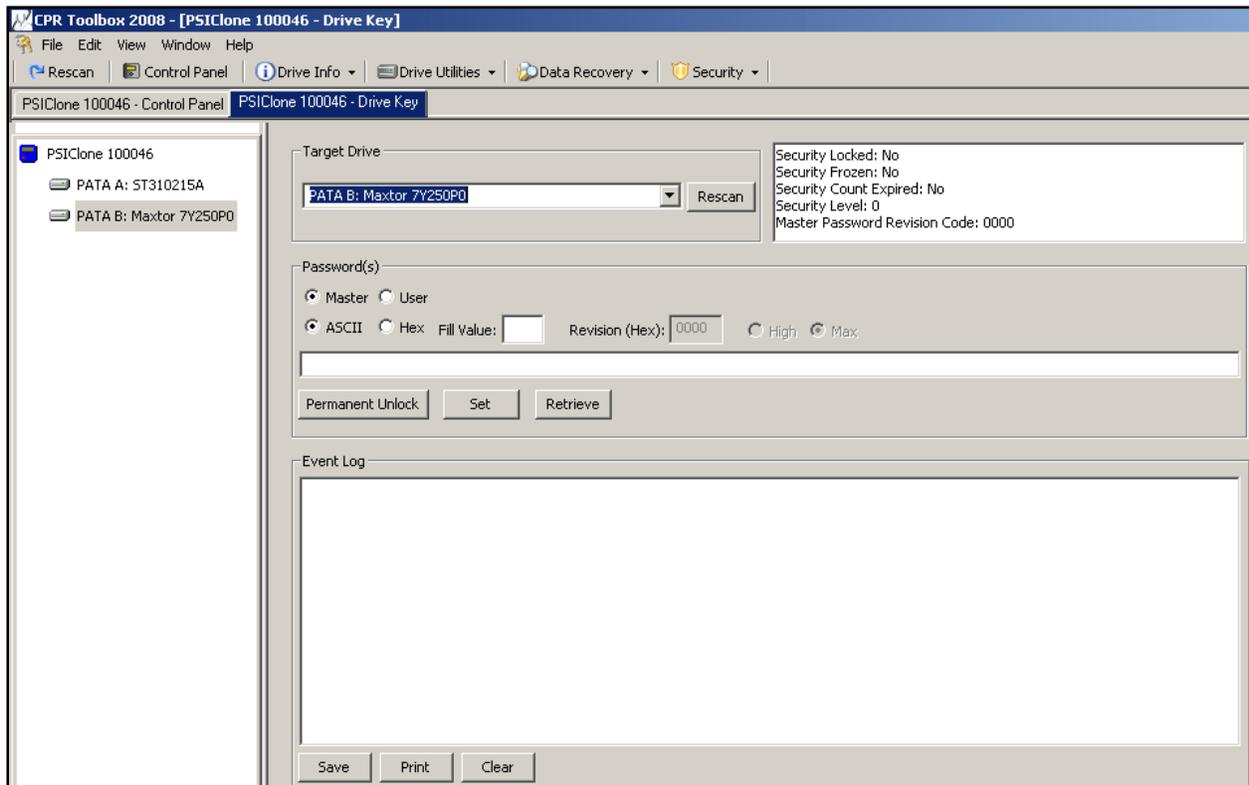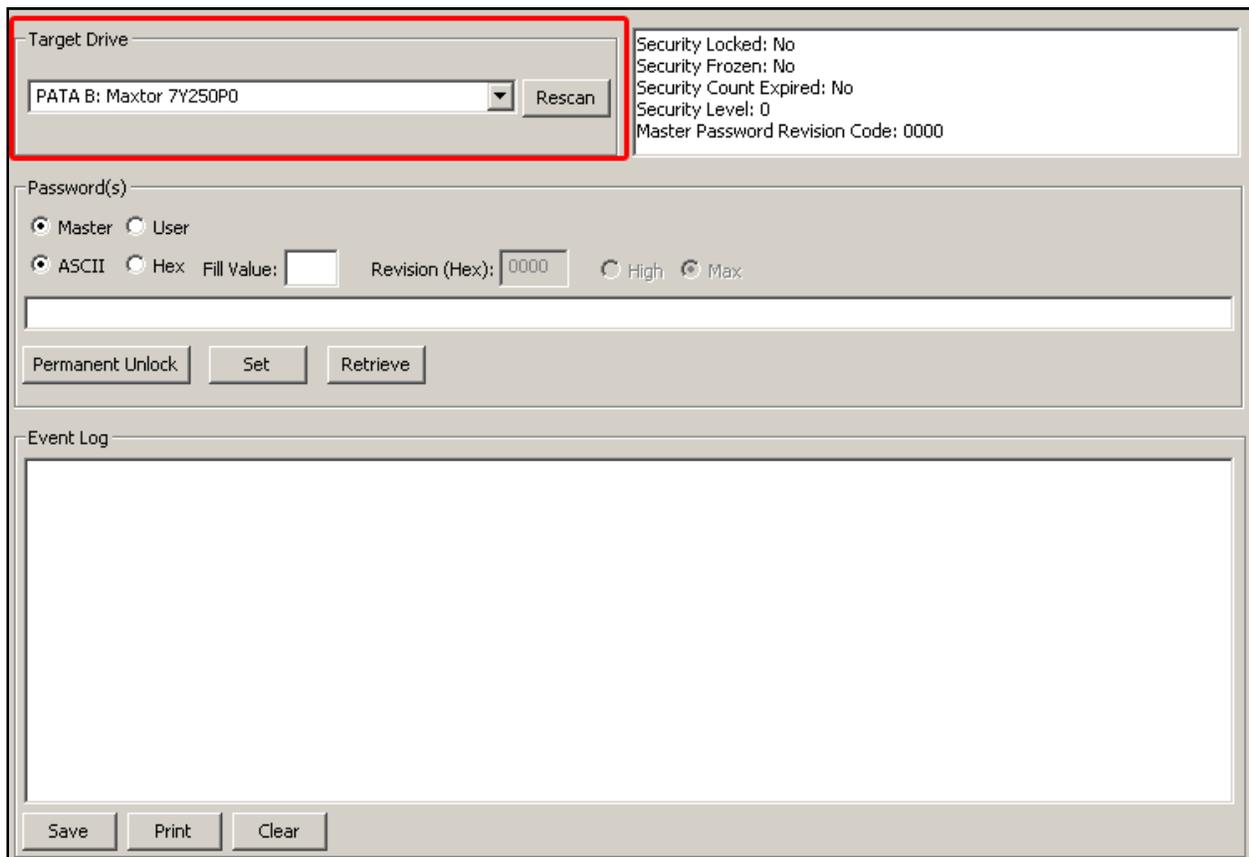3. PSIClone™ is using firmware which enables DriveKey™ support.

Figure 1 – DriveKey™ initial screen

Using DriveKey™

Begin by selecting a supported drive from the drop-down list, labeled 'Target Drive'. Figure 2 depicts a Maxtor Drive, attached to Side B of PSIClone™ selected.


Figure 2 - DriveKey™ - Select Target Drive

DriveKey™ may display information regarding the security level of the selected drive. To ensure that the most current information about the selected drive is displayed, click the button labeled 'Rescan'. Drive security status is provided in the section to the right of the 'Rescan' button.

The 'Password(s)' section of the screen, depicted in Figure 3, provides an interface through which a drive may be locked or unlocked.
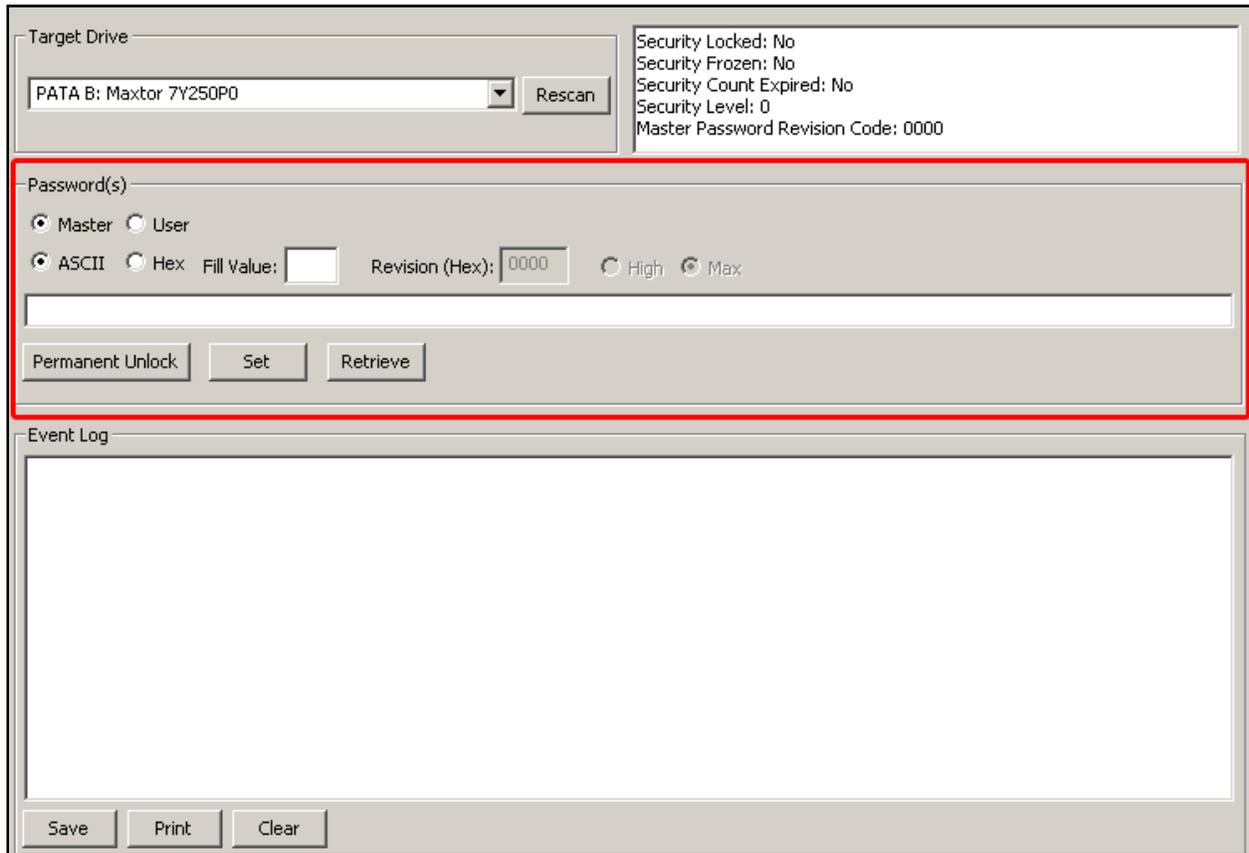

Figure 3 - DriveKey™ - Password(s) section

Iin this section, the user will be able to read/display Master and User passwords. Additionally, the user may set a Master password and/or a User password in either High or Max modes. The passwords selected may be in either ASCII or Hex.

Setting a Master Password[2]

To set a Master password, ensure that the radio button labeled 'Master' is selected. Next, select either ASCII or Hex and enter a 'Fill Value', if desired, in the text box provided. The 'Fill Value' is used to pad the chosen password. If no Fill Value is

entered DriveKey™ will pad the password field, if needed with `0x00`.
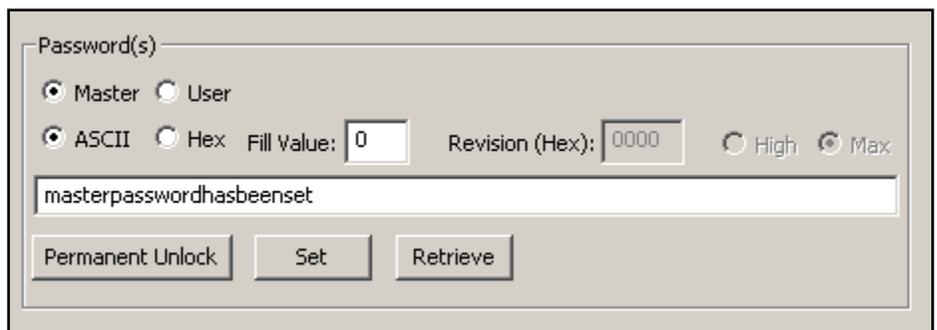
Key a password into the field shown.

---

[2] DriveKey is capable of setting Master passwords on both fully supported and minimally supported drives

According to the ATA specification, a Revision code may be set to specify information about the entity setting a security password. As not all vendors follow the specification, this field may be 'grayed out' as it is in the example shown. As specified in the ATA specification, valid hexadecimal values for Revision are 0001 through FFFE.
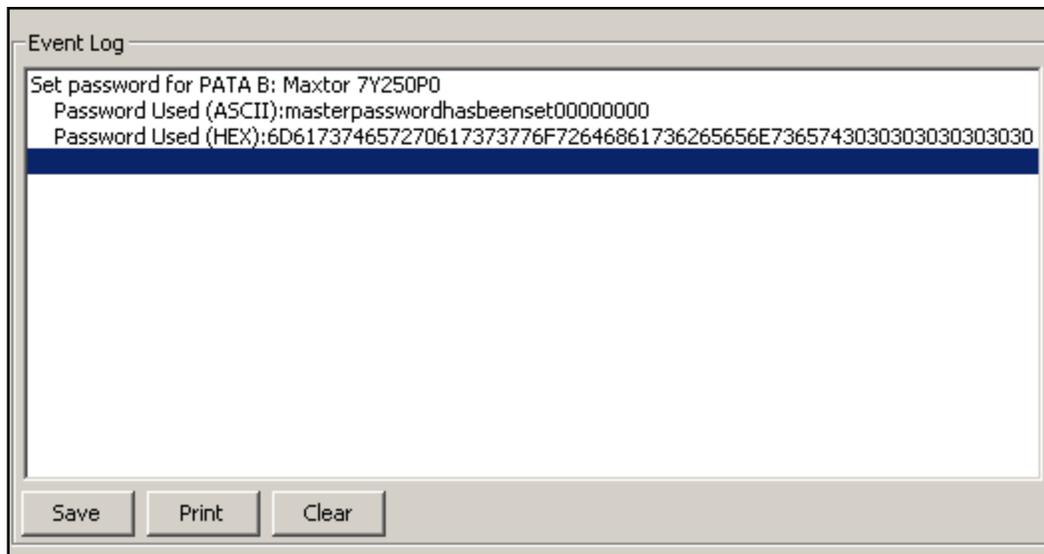
Click 'Set' to set the Master password.

Upon successful setting of the Master password, CPR Toolbox™ will display a confirmation message, shown in Figure 4.

Figure 4 - Master password has been successfully set

In addition to the success message, CPR Toolbox™ displays the output of the command in the Event Log section of the module, as shown in Figure 5.

Figure 5 - Output resulting from successful setting of Master password

The password is displayed in both ASCII and Hex. Note that as the password phrase entered did not fill the requisite 32 bytes, the 'Fill Value' was appended to the phrase to pad it to the full length of the password field.

The output in the Event Log may be saved to a file by clicking the 'Save' button. Alternately, this data may be easily printed by clicking 'Print'. The Event Log display may be cleared by clicking 'Clear'.

Setting a User Password[3]

The process for setting a 'User' password closely resembles those for setting a Master password as described above. One significant difference is the ability to choose a security level for the User password.

Figure 6 depicts the DriveKey™ screen as we prepare to set a User password in 'Max' mode.

Figure 6 - Preparing to set a User password in 'Max' mode

As with the setting of the Master password, the user must select ASCII or Hex, 'Fill Value', if desired, in the text box provided. The 'Fill Value' is used to pad the chosen password. If no Fill Value is entered DriveKey™ will pad the password field, if needed with $0x00$.

The 'User' password has two possible levels of security:

1. High
   a. If a drive is locked with a user password in 'High' mode, either the Master password or User password may unlock the drive.
2. Max
   a. If a drive was locked with a user password in 'Max' mode, only the User password should be able to unlock the drive. The drive should be completely unusable without the correct 'User' password.

> **DriveKey™ Key Feature:**
> Prior to DriveKey™, a drive locked with a User password would be unusable without the User password.
>
> With DriveKey™ support, this is no longer the case; fully supported, locked drives may simply be unlocked using DriveKey™.

---

[3] DriveKey is capable of setting User passwords on both fully supported and minimally supported drives

To set a User password, ensure that the radio button labeled 'User' is selected. Next, select either ASCII or Hex and enter a 'Fill Value' in the text box provided.

The 'Fill Value' is used to pad the chosen password. Select 'High' or 'Max'.
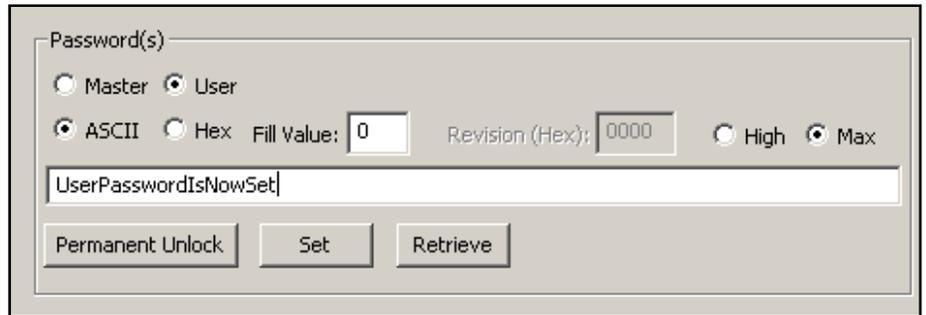
Key a password into the field shown.

Click 'Set' to set the User password. CPR Toolbox™ displays a confirmation message to acknowledge the setting of the User password, as shown in Figure 7.
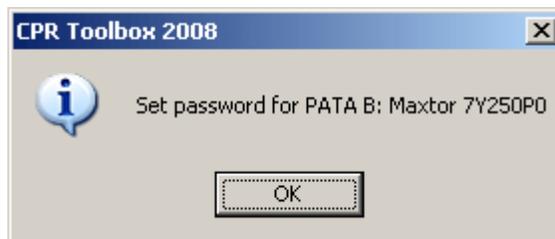
Figure 7 - User password has been set

Retrieve

For fully supported drives, any passwords which exist may be shown within the DriveKey™ module by clicking 'Retrieve'. If 'Retrieve' is used on drives which are not fully supported, CPR Toolbox™ displays a message stating that the selected drive is not yet supported.

Figure 8 - CPR Toolbox has identified a drive which is not fully supported by DriveKey™

If 'Retrieve' is successful, CPR Toolbox displays a confirmation that the retrieval was successful.
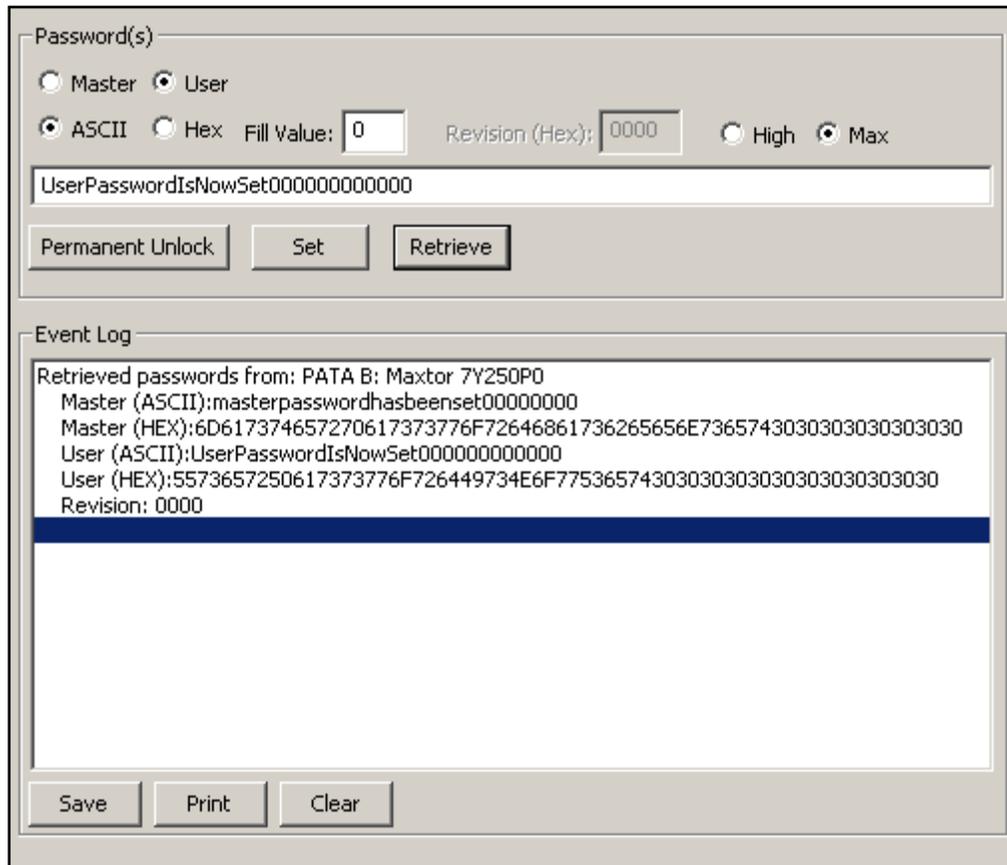
Click 'OK'. All known password information about the drive is displayed in the Event Log window. A successful 'Retrieve' operation is shown in Figure 9.

CPR Toolbox 2008

Retrieved passwords from: PATA B: Maxtor 7Y250P0

OK

Password(s)

○ Master ⦿ User

⦿ ASCII ○ Hex Fill Value: 0   Revision (Hex): 0000   ○ High ⦿ Max

UserPasswordIsNowSet000000000000

Permanent Unlock   Set   Retrieve

Event Log

Retrieved passwords from: PATA B: Maxtor 7Y250P0
   Master (ASCII):masterpasswordhasbeenset00000000
   Master (HEX):6D6173746572270617373776F72646861736265656E73657430303030303030
   User (ASCII):UserPasswordIsNowSet000000000000
   User (HEX):5573657250617373776F726449734E6F7753657430303030303030303030303030
   Revision: 0000

Save   Print   Clear

Figure 9 - Successfully retrieved password information is displayed

The output in the Event Log may be saved to a file by clicking the 'Save' button. Alternately, this data may be easily printed by clicking 'Print'. The Event Log display may be cleared by clicking 'Clear'.

Permanent Unlock

The button marked Permanent Unlock may be used to unlock a drive in such a way as to have the 'unlocked' status survive a power cycle of the drive. This feature is available to fully supported drives under most conditions. For drives which are not fully supported, this feature will only succeed if the password(s), if any, for the drive are known.

CPR TOOLS
Media Research & Recovery

To use the 'Permanent Unlock' feature for fully supported drives, first click 'Retrieve' to populate the password field. Once the password field is populated, clicking the 'Permanent Unlock' button will unlock the drive. CPR Toolbox™ will display a confirmation message upon success.

Figure 10 – A drive has been successfully unlocked

The Event Log will show an entry upon successful unlocking of a drive, as shown in Figure 11.
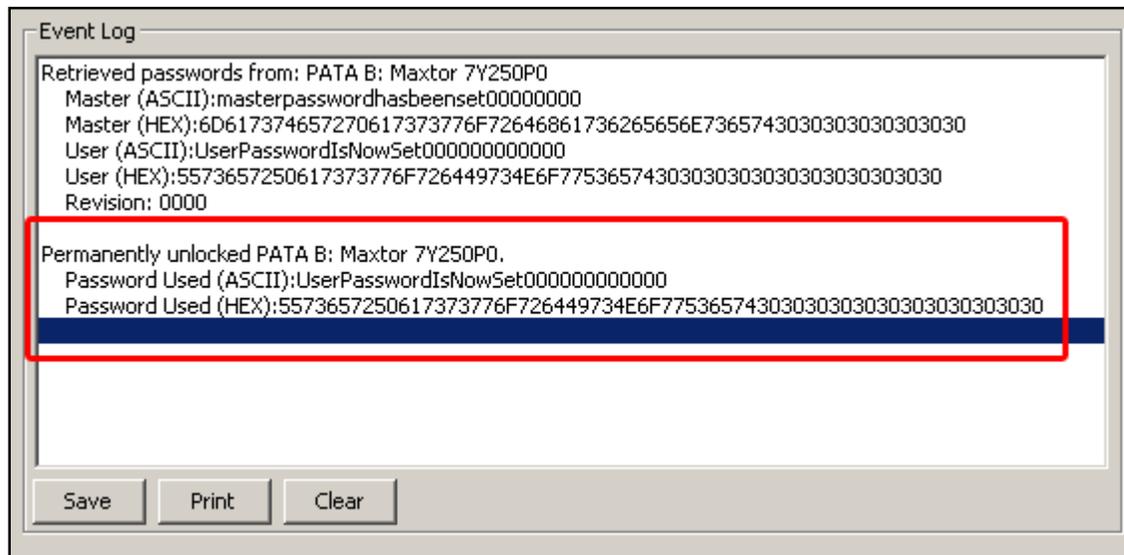
Figure 11 - Event Log provides a summary of the unlocking process

The output in the Event Log may be saved to a file by clicking the 'Save' button. Alternately, this data may be easily printed by clicking 'Print'. The Event Log display may be cleared by clicking 'Clear'.

Unsupported Drives and DriveKey™

DriveKey™ serves as a front-end for manipulation of security passwords on both fully supported and unsupported drives.

To set User and/or Master passwords for unsupported drives follow the same steps as listed in the 'fully supported drives' section of this guide.

When working with unsupported drives, DriveKey™ will be unable to retrieve a pre-existing password but will allow setting of User and Master passwords.

WARNING:
Use extreme caution when working with drives which are not fully supported. Locking a drive which is not fully supported can render the drive completely useless if the password is forgotten. **CPR Tools assumes no responsibility for drives locked and rendered unusable through misuse of DriveKey™.**