WHITE PAPER

February 1998

Prepared By

Portable Software
Marketing

Compaq Computer
Corporation

CONTENTS

DriveLock Hard Drive Protection for the Armada 7800

DriveLock is a security feature that offers customers advanced protection against unauthorized access to valuable data on their internal notebook hard drives. The feature has been designed to meet expressed needs from customers who cannot afford to have their sensitive hard drive data fall into the wrong hands.

The purpose of this document is to explain the Compaq DriveLock security implementation. Particular focus will be given to the severe consequences that can arise from misuse. The document will also suggest strategies that corporate MIS managers can implement to make the most use of DriveLock and minimize the likelihood of adverse consequences.

The document has been written for internal Compaq personnel with a need to understand DriveLock and how to communicate its features, benefits and limitations to customers. For a concise overview of essential messages that need to be communicated to customers, refer to the section titled Key Customer Messages.

This document is intended external audiences with a need for information about DriveLock on the Armada 7800.

COMPAQ

NOTICE

The information in this publication is subject to change without notice.

THE COMPETITIVE INFORMATION CONTAINED IN THIS PUBLICATION IS BASED ON DATA AVAILABLE FROM PUBLIC SOURCES AT THE TIME OF PUBLICATION. COMPAQ COMPUTER CORPORATION SHALL NOT BE RESPONSIBLE FOR ANY INACCURACIES, ERRORS, OR OMISSIONS IN INFORMATION CONTAINED HEREIN, INCLUDING, BUT NOT LIMITED TO, INFORMATION OBTAINED FROM THIRD PARTY SOURCES, SUCH AS PUBLICATIONS OF OTHER COMPANIES, THE PRESS, OR COMPETITIVE DATA ORGANIZATIONS.

THIS PUBLICATION IS MADE AVAILABLE ON AN "AS IS" BASIS AND COMPAQ SPECIFICALLY DISCLAIMS ALL ASSOCIATED WARRANTIES, WHETHER EXPRESS OR IMPLIED. IN NO EVENT WILL COMPAQ BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF OR RELIANCE ON THE MATERIAL CONTAINED IN THIS PUBLICATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. COMPAQ RESERVES THE RIGHT TO MAKE IMPROVEMENTS OR CHANGES TO THIS PUBLICATION AND THE PRODUCTS AND SERVICES HEREIN DESCRIBED AT ANY TIME, WITHOUT NOTICE OR OBLIGATION.

This publication does not constitute an endorsement of the product or products that were tested. The configuration or configurations tested or described may or may not be the only available solution. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements. Compaq does not warrant products other than its own and then, only as strictly stated in Compaq product warranties.

DriveLock Hard Drive Protection for the Armada 7800

First Edition (October 1997)
Second Edition (February 1998)
0298/B

ATA-3 SPECIFICATION BACKGROUND

DriveLock is based on the industry standard ATA-3 specification. The standard uses a dual password structure featuring a *master* and *user* password. The *master* password has been designed to give the MIS manager supervisory control over DriveLock features. It allows for unlocking of protected hard drives as well as the ability to change the *user* password. The *user* password, as the name suggests, has been designed to give the user access to protected hard drives as well as the ability to change the *user* password.

ATA-3 also defines two security modes, *high* and *max*. Under *high* mode, the *master* password can be used to unlock a protected hard drive and reset the *user* password. By contrast, in *max* mode the *master* password can only be used to reformat the hard drive and reset security options for the newly formatted drive. In the *max* mode, the *master* password cannot be used to change the *user* password without first reformatting the hard drive. This protects against unauthorized access to hard drive by the owner of the *master* password. In both security modes, if both passwords are lost, the hard drive is rendered permanently unusable.

Compaq DriveLock is fully compatible with the ATA-3 specification, with the user model based on the *high* security mode. The decision to only implement the *high* mode was made to eliminate risk of data loss in the event only the *user* password is lost. The following table compares the key ATA-3 security specifications with the Compaq DriveLock implementation.

ATA-3 SPECIFICATION

	ATA-3 Specification	Compaq Implementation
Defines a *user* password	✓	✓
Defines a *master* password	✓	✓
Defines a *high* security mode	✓	✓
Defines a *max* security mode	✓	✓
Under the *high* security model, the *master* password unlocks a protected hard drive	✓	✓
Under the *max* security model, the *master* password is only able to reformat a protected hard drive	✓	✗

Table 1 - ATA-3 Hard Drive Security versus DriveLock

COMPAQ DRIVELOCK IMPLEMENTATION

F10 Setup Passwords

DriveLock has been implemented as an extension to the F10 setup utility. Access to the F10 setup utility can be controlled by enabling an *admin* password[1]. If enabled, this password is required to make any modifications to the F10 settings including DriveLock. From a DriveLock perspective, the *admin* password is a key tool the MIS manager can use to maintain control over whether or not users are allowed to use the DriveLock feature. Given that a hard drive can be rendered permanently unusable, MIS managers may elect to restrict access to the feature to only those users who absolutely require it.

[1] The *admin* password is sometimes referred to as the *setup* password. This document consistently refers to the *admin* password as the password required to enter into F10 Setup at power-on.

DriveLock Setup

DriveLock will appear as one of the options available to the user in the F10 setup utility and presented as one of several tabs in the interface. Selecting the DriveLock tab will first bring up a warning screen to bring attention to the key considerations when choosing to enable DriveLock. Proceeding from this screen the user is presented with a second dialogue box displaying various fields that define how DriveLock is setup.

First time setup requires that the user press the *Set Button* in the DriveLock interface. Doing so then prompts the user for a *user* password. Once the *user* password has been set DriveLock will display a prompt to set the *master* password. It is important to keep in mind that first time setup is typically performed by an MIS administrator. The person responsible for maintaining the *master* password will not be the end user in most cases. Choosing a *master* password is the final step in protecting a hard drive and just before completing the step, a final warning message is displayed that requires the user to confirm that enabling DriveLock is something the user actually wants.

Changing passwords is accomplished through the same DriveLock tab in the F10 setup utility. Changing the *master* password requires the old *master* password to be entered first and therefore can only be changed by its owner. The *user* password can be changed only if the previous *user* password is known. In the event the *user* password is lost, under *high* security, the *master* password can be used to disable DriveLock protection and, therefore, erase the old *user* password. Once this is done, DriveLock can be re-enabled which will prompt for a new *master* and new *user* password for the hard drive.

Password Prompts

There are five distinct passwords that are involved in the DriveLock implementation. Each of these passwords and the role they play has been summarized in Table 2. The remainder of this section will focus on the password prompt logic.

DRIVELOCK RELATED PASSWORDS

	What is the password and how does it factor into DriveLock implementation?
Power-on Password	The power-on password controls access to the notebook computer itself. The user is prompted for this password when the unit is powered on. It can be set independent from DriveLock.
F10 Administrator Password	The administrator password controls access to the F10 setup utility. If this password is enabled end users are restricted from modifying DriveLock unless the owner of the admin password has enabled the feature.
QuickLock Password	The QuickLock password is the same as the power-on password. The QuickLock feature has been designed to prevent an unauthorized user from resuming the notebook from Standby. Through the F10 setup utility, users must enable the QuickLock on Standby Resume feature. On resume, the user will be prompted for the QuickLock password.
DriveLock *Master* Password	The MIS administrator typically owns the *master* password for each protected hard drive. The master password can be used to unlock a protected hard drive, reset the user password and remove DriveLock protection from a hard drive This second layer of password protection allows the MIS administrator to create and manage a consistent corporate policy for DriveLock usage.
DriveLock *User* Password	The end user is typically the owner of the *user* password. The user is prompted to set the *user* password when a hard drive is first protected. The password is then used to unlock the protected hard drive at power-on. Each protected hard drive has its own *user* password.

Table 2 - Password Summary

The first is the power-on password. This password can be set independently of DriveLock. When DriveLock is enabled, the user will always be prompted to enter the power-on password first assuming the user has enabled the *power-on password* feature.

Once the power-on password has been entered and validated the system will attempt to unlock any DriveLock protected hard drives that may be present at power-on. If the power-on password is different from the DriveLock *user* password the user will be prompted for a password for each protected hard drive. Protected hard drives will not be unlocked unless the correct password for the hard drive being unlocked is entered.

The QuickLock password is required to protect against unauthorized access to an unlocked hard drive while in standby mode.

Standby & Hibernation

Standby and hibernation modes on notebook computers present challenges to manufacturers implementing hard drive security. Under hibernation the current state of the user environment is saved to the hard drive. Once saved, the notebook completely powers down. Upon resume the user will be go through the normal password prompt sequence starting with the power-on password and *user* password for each protected hard drive. While in hibernation mode the hard drive is completely powered down which means that it is by definition locked if DriveLock is enabled. If a protected hard drive is removed while in hibernation, it will remain secure even if inserted into another notebook that does not have DriveLock enabled.

When in standby mode, the current user environment is saved to memory and the notebook enters a low power state. As with hibernation, if a protected hard drive is removed while in standby it will remain locked. This will prevent access by inserting the hard drive into another notebook that does not have DriveLock enabled.

When resuming from standby mode the user will not be presented with the same password prompt sequence as if resuming from hibernation. Immediately after unlocking a protected hard drive on power-on, the password is securely cached. When resuming from standby, this cached password is automatically used to unlock the protected hard drive. In order to prevent unauthorized access to a protected hard drive while in standby mode, it is essential that the user first enable the QuickLock on Standby Resume feature in the F10 setup utility. With this feature enabled, resuming from standby will require the user to enter the QuickLock password.

IMPORTANT CONSIDERATIONS

There are a number of DriveLock features that have the potential to render a protected hard drive permanently unusable. For this reason it is important that Compaq customers fully understand the responsibilities that are inherent in any decision to enable DriveLock.

First, it is important to understand the intent behind DriveLock. DriveLock has been designed for portable customers with a need to prevent unauthorized access to hard drive data. This particular profile of user regularly carries information on a notebook that could be potentially damaging if it were to fall into the wrong hands. The cost of the notebook itself is inconsequential when compared with the damage that could result from unauthorized access. Examples of the types of data in need of this level of protection include trade secrets, passwords to a corporate LAN/Intranet, replications of a sensitive corporate database, among others.

It is also important to note that users fitting this profile are not as concerned with actually losing the data as they are with unauthorized access. The data itself is often replicated on a corporate information system or is regularly backed up. If a notebook is stolen what is most important is for the customer to be able to rest assured that the thief will not be able to gain access to the hard drive.

The key consideration to keep in mind is that in the event both the *master* and *user* passwords are lost, the hard drive is rendered unusable. For any user who does not fit the previously defined profile, this can amount to a significant loss. For users who do fit the profile, it is a tolerable consequence given the nature of the data stored on the hard drive.

An obvious way to minimize the likelihood of losing both passwords is to make sure that one person is not responsible for both passwords. The most common scenario in which DriveLock is anticipated being used in is the corporate scenario where users are provided notebooks from a centralized MIS department. The MIS department would be responsible for setting up the notebook which would involve, among other things, setting the DriveLock *master* password. In the event the user loses the *user* password or the notebook is passed on to another employee, the *master* password can always be used to reset the *user* password and regain access to the hard drive.

Compaq recommends that corporate MIS departments who choose to enable DriveLock also establish a corporate policy for setting and maintaining *master* passwords. This should be done to prevent a situation where an employee knowingly or unknowingly sets both passwords before leaving the company. In such a scenario the hard drive would be rendered unusable and require replacement. As well, by not setting a *master* password, MIS managers may find themselves locked out of a hard drive and unable to perform routine checks for unauthorized software, other asset control functions and support. Clearly, enabling DriveLock and setting *master* passwords make sense from a management control perspective.

For users with less stringent security requirements, Compaq does not recommend enabling DriveLock. Users in this category include personal users or users who do not maintain sensitive data on their notebook as common practice. For these users, the potential loss of a hard drive resulting from losing both passwords is much greater than the value of the data DriveLock has been designed to protect. Access to the F10 setup utility and DriveLock can be restricted through the admin password. By setting this password and not giving it to end users, MIS administrators are able to restrict users from enabling DriveLock.

Careful consideration needs to be given to the potential consequences of enabling DriveLock before any decision to do so is made.

SERVICE & SUPPORT

Compaq supports DriveLock through normal support channels. For DriveLock users it is important to understand that responsibility for maintaining passwords rests with the user and the MIS administrator. In the event both passwords are lost, Compaq support is unable to recover the contents or otherwise make the hard drive usable again. DriveLock does not merely provide the illusion of security; it is a proven mechanism to secure hard drive data that cannot be circumvented without either the *master* or *user* password.

In the event both passwords have been lost the only option available to the user is to purchase a replacement hard drive. Should the user request support in such a case, Compaq is only able to provide the user with information on how to go about purchasing a replacement hard drive.

USER INTERFACE MESSAGES

In anticipation of DriveLock support requests from users, several design steps have been taken to educate the user on the consequences of misuse. Whenever the user attempts to enable or modify DriveLock an informational dialogue box appears with the following text:

> *Use EXTREME CAUTION when enabling DriveLock - DriveLock uses a powerful security technology to protect the contents of your hard drive from unauthorized access. DriveLock allows a USER password to be set for each protected hard drive and an overriding MASTER password. One of these*

> *passwords must be entered every time the computer is powered on in order to unlock and use a protected hard drive.*
>
> *In the event both passwords are lost or forgotten, the hard drive will be rendered permanently unusable. No one, including Compaq, will be able to access or recover the contents of protected hard drives. Hard drives rendered unusable under these circumstances are NOT covered under the Limited Warranty Statement. For these reasons Compaq recommends enabling DriveLock only if the potential cost of unauthorized access is greater than the cost of replacing a hard drive and rebuilding lost data. Consult your Compaq owner's manual for more information.*

The dialogue clearly explains that the onus is on the user to maintain passwords and the consequences of losing passwords. It further explains that Compaq support capabilities are limited in the event passwords have been lost and that the only course of action is to purchase a replacement hard drive.

Immediately prior to enabling DriveLock the following confirmation message is displayed:

> *CAUTION - You are about to protect a hard drive using DriveLock. Forgetting or losing both the USER and MASTER passwords will render the protected hard drive permanently unusable. Record your MASTER password and keep it in a secure location physically separate from your notebook computer. In the event you lose the USER password, the MASTER password can be used to unlock a protected hard drive and reset the USER password.*
>
> *Remember, with security comes responsibility. If you do not want to enable DriveLock, press the "Cancel" button or the "Esc" key. To proceed with enabling DriveLock you must type the word "DriveLock" and then press the "OK" button.*

In order to prevent accidental enabling of DriveLock, the confirmation procedure requires the user to type the word "DriveLock".

ADDITIONAL TABLES

KEY CUSTOMER MESSAGES

	What customers need to understand about DriveLock.
Warning	DriveLock will render a protected hard drive permanently unusable if both the *master* and *user* passwords have been lost. Customers should exercise extreme caution when enabling DriveLock.
Security	Hard drives protected with DriveLock are secure whenever they are in a power-off state. This ensures security when the notebook has been turned off, when in hibernation mode and in the event a protected hard drive is removed from a notebook while in Standby mode.
User Profile	DriveLock has been developed to protect highly sensitive user data that has the potential to be damaging should it fall into the wrong hands. The only customers who should consider enabling DriveLock are those who have a need to store sensitive information on their notebook and who replicate or regularly backup this data.
Support	In the event both the *master* and *user* passwords have been lost, Compaq is unable to restore or otherwise gain access to a protected hard drive. In such a situation, Compaq Support is only able to advise customers on how to go about purchasing a replacement hard drive.

Table 3 - Key customer messages

FEATURES & BENEFITS

Feature	Benefit
DriveLock is based on the industry standard ATA-3 hard drive controller specification	Ensures DriveLock compatibility and functionality with any ATA-3 compliant hard drive.
Dual password Security Model[2]	Corporate MIS administrators responsible for managing fleets of notebooks can give users secure storage without compromising their need to maintain administrative rights.
QuickLock password when resuming from standby mode	Since protected hard drives are automatically unlocked when resuming from Standby mode, requiring the QuickLock password revalidates the identity of the user before allowing access to an already unlocked hard drive. This feature is set independently from DriveLock.

Table 4 - DriveLock features & benefits summary

FREQUENTLY ASKED QUESTIONS

What level of support for DriveLock can I expect from Compaq?

DriveLock is fully supported by Compaq and endorsed as an effective solution to protect against unauthorized access to data stored on a notebook. Should users have questions or concerns about DriveLock they should consult the Compaq owner's manual for information on contacting customer support in their region. Compaq Customer Support will be able to address all general questions related to DriveLock functionality and troubleshoot any problems that may be experienced in enabling the feature or in its ongoing operation. It is important to note, however, that Compaq is unable to recover the contents of a protected hard drive if both the *master* and *user* passwords have been lost. In this case the hard drive will have been rendered unusable and it will need to be replaced at the customer's own expense.

Why do I need to set both a *master* and *user* password when only one is required to unlock a protected hard drive?

The dual password scheme has been designed to offer greater flexibility for customer organizations in managing security requirements. A central authority, typically the corporate MIS department, responsible for internal support for notebook users, should maintain *master* passwords for all notebooks. The *master* password gives an administrator the ability to reset the *user* password in the event it is lost or the notebook user leaves the company. Without this ability, employees could render their hard drives unusable by failing to leave their password when leaving the company.

I find having to enter a power-on password and a *user* password for each protected hard drive to be cumbersome. What can I do to simplify managing three separate password protection layers?

DriveLock intelligently attempts to match the power-on password with the *user* password for each protected hard drive. If it finds a match, the user will not be prompted for the *user* password. By setting the DriveLock *user* password or passwords the same as the power-on password, the user can eliminate the need to be prompted for multiple passwords.

[2] Refers to the fact that DriveLock allows the user to establish a *user* and *master* password.

I am concerned that my hard drives are unprotected while in Standby mode since I am not prompted for a password on resume. Is there any way to protect from unauthorized access while in Standby?

To prevent unauthorized access while in standby users must enable the QuickLock feature and chose the QuickLock on Standby Resume option in the F10 setup utility. Even though hard drives protected with DriveLock will be automatically unlocked on resume, the QuickLock feature will require the QuickLock password be entered before permitting access to the unlocked hard drives. QuickLock protection is not available if in docked mode with an external video controller.

Am I able to protect hard drives in my ArmadaStation 7000 with DriveLock?

No, DriveLock is unable to protect hard drives internal to the ArmadaStation 7000. Docking station hard drives are not mobile and therefore not prone to the same types of security threats DriveLock has been designed to protect against. Hard drives protected with DriveLock cannot be accessed if inserted into the ArmadaStation 7000. In order to unlock a protected hard drive, it must be inserted into one of the notebook bays.

Am I able to access an Armada 7800 hard drive protected with DriveLock in an Armada 7700 or 7300?

Although Armada 7800 hard drives are backward compatible, DriveLock protected hard drives cannot be unlocked in an Armada 7700 and 7300. To access an Armada 7800 hard drive in an Armada 7700 or 7300, it is necessary to first disable DriveLock protection.

Am I able to lock hard drive partitions separately?

No, DriveLock protection is provided at the hardware level and therefore cannot lock partitions separately, only physical hard drives. If you would like to organize your notebook such that there is a protected area and an unprotected area it is recommended that you use a removable hard drive in addition to the internal hard drive and only protect one of them (e.g. the boot drive). This would facilitate shared notebook scenarios where multiple users may need access to a common directory yet still have the ability store sensitive information related only to their personal activities. Although the notebook is shared in this case, each user would have a removable hard drive protected with DriveLock.

How is the Armada 7800 DriveLock implementation different from earlier implementations on LTE Elite notebook computers?

Earlier implementations of DriveLock were based on proprietary protection technologies that were limited to Compaq portable platforms using Connor hard drives. The Armada 7800 DriveLock implementation is based on the industry standard ATA-3 IDE controller specification making it compatible with any ATA-3 compliant hard drive.

Another important difference is the *master* password. On the LTE Elite, Compaq maintained *master* passwords that could be supplied to the customer in the event either the *master* or *user* password had been lost. The approach taken with the Armada 7800 DriveLock implementation is to give the user or corporate MIS manager complete control over their own security. The notebook owner is now responsible to maintain the integrity of the *master* password. This eliminates the potential for a breach in security that exists whenever a third party maintains control over passwords.

LIST OF TABLES