



# MANAGEMENT OF HARDWARE PASSWORDS IN THINK PCs.



Ideas from Lenovo®  
Notebooks and Desktops  
Workstations and Servers  
Software and Peripherals  
Service and Support

**lenovo**®

NEW WORLD. NEW THINKING.™

## INTRODUCTION

IBM® introduced hardware passwords in PCs in the late 1980's. These passwords were intended to accomplish two security goals: One, deny value of the PC as an asset to a thief. Two, protect confidentiality of sensitive information that is stored on the PC hard disk drive. These goals are clearly important to customers today, more than ever. Unfortunately, it is very difficult to manage hardware passwords in any fashion that is both secure and scalable. As a result, even though most customers are aware passwords exist, very few actually use them.

Up to 40% of help desk calls to companies are "I forgot my password"<sup>1</sup>. If the password is a hardware password and if there is no central management system for these passwords, then the company has lost the use of either a system motherboard or they have lost access to a hard disk drive (and all of the data on it). These are expensive consequences for a common problem.

Lenovo now offers a solution to the problem. The BIOS of select Think PCs now contain an infrastructure that makes it possible to centrally manage all four of the standard hardware passwords—these passwords are:

- The Power On Password (POP)
- The Supervisor Password (SVP)
- The Hard Drive Password (HDP)
- The Master Hard Drive Password (MHDP)



## WHAT ARE HARDWARE PASSWORDS?

Hardware passwords are divided based on who is supposed to use them. Two of them are intended for end-user use, the POP and HDP. Two of them are intended for administrative use, the SVP and MHDP. Another way to divide the passwords is based on what the passwords control access to. The POP and SVP are used to control access to the motherboard—whether the system will boot. The SVP can also be used to control who has the authority to modify BIOS configuration settings on that PC. The HDP and MHDP are used to control access to the hard disk drive—if they are set, the drive will not spin unless one of them is entered.

See notes at the end of this paper for a more complete description of each hardware password.

## WHY ARE HARDWARE PASSWORDS REQUIRED?

"Hardware passwords" are passwords associated with either the motherboard of the PC or with the disk drive in a PC. There were two objectives for these passwords. Firstly, they deter theft. The passwords disable the motherboard (making it impossible to boot) and the hard disk drive (if the hard disk drive password is set on a drive, it will not spin until the password is entered). In the case of internal theft, if the thief knows the passwords are set, it deters him from stealing the PC. Secondly, hardware passwords protect confidential data on the drive. Especially confidential data on a drive that is stolen as a target of opportunity by a thief who wants

to sell the hard disk drive and/or data for cash. The hard disk drive password can be defeated by sending the drive for forensic data recovery. In this case, the drive is disassembled and the data taken off the platters. The process costs over \$4,000 to perform, so a casual thief is very unlikely to do this.

These hardware passwords are very resistant to password crackers<sup>2</sup>. After three tries, you have to turn off the PC and turn it back on. For this and other reasons, there are no tools for cracking hardware passwords. It is still possible for the user to defeat the security of hardware passwords by writing the passwords on paper and taping them to the PC.



## WHY ARE HARDWARE PASSWORDS RARELY USED?

If these passwords are set, what happens if the user forgets them? The worst case is that the motherboard and hard disk drive must be replaced. In an organization of hundreds of users or more, there will be cases of forgotten hardware passwords every year. There is also the problem of recovering a PC if the user (who may be the only one who knows the passwords) is not available to divulge what those passwords are. In large enterprises, these problems occur almost every day.

Further, actually setting a hardware password for the first time requires physical presence at the keyboard. You have to turn on the PC, enter BIOS configuration and type in the passwords that you want. When the time to do this is multiplied by the number of PCs in deployment, it can result in large costs. In the future, if you want to change a hardware password, you have to go through the same process of manually starting the PC, entering BIOS configuration and making the change.

Based on this, most customers have decided that the cost of disabled hardware and lost data due to forgotten passwords far exceeds the security value of using hardware passwords. If these passwords could be managed, that would change how customers think.

For a solution to be viable in solving this problem, it must provide the following:

- Make it possible for a company to use hardware passwords to deter theft and improve system security
- Keep administrative costs for using passwords down by providing self-help capability and the opportunity to sync with the Windows Domain ID and password
- Control access to the PC through the definition and management of hardware accounts
- Protect the privacy of users by ensuring each user is the only person who knows his or her hardware account
- Protect accessibility to the system by ensuring that only I.T. Administration knows the real hardware passwords for all PCs in deployment

## LENOVO'S FIRST SOLUTION: CENTRAL MANAGEMENT OF BIOS SETTINGS USING WMI.

Lenovo made it possible for customers to centrally manage all BIOS settings beginning with the ThinkPad notebooks released in August, 2008. This solution is based on Microsoft's Windows Management Interface (WMI). It includes the ability to change hardware passwords if those passwords have been set and the administrator knows what they are.

WMI is a script-driven interface. It includes the ability to distribute scripts from a central console to the field of deployed PCs. Once the script arrives, it automatically executes. As a result, it fits well in many Active Directory management implementations.

In terms of the pros and cons for this solution to manage hardware passwords, we have:

### Pros:

- Built into the BIOS of PCs that support it and relies on a standard Microsoft technology—no additional charge
- Based on the same BIOS setting management model used across the PC industry
- Is not Active Directory (AD) based, but plays well with an AD management environment

### Cons:

- I.T. must manually set the initial passwords for each PC
- I.T. must know all of the passwords
- User can not set his own user passwords



## LENOVO'S HARDWARE PASSWORD MANAGER.

The problem is conceptually very simple to solve: Provide a solution for the central management of four passwords. The execution is rather more difficult. BIOS had to be made considerably smarter. It had to be provided with a network communications capability. It had to be provided with communications channels to the PC operating system and to an Active Directory back end. All of this new capability had to be created in a secure fashion. It also had to protect the privacy of users. Finally, a management console had to be created.

On the topic of user privacy, it is a privacy Best Practice to ensure that no one but the user himself knows what his password is (if he forgets it, it must be possible to reset it, not recover it). The problem of preserving user privacy is central to the design of the solution. ThinkPad and ThinkCentre® M Series BIOS contain storage containers, called "Vaults". A vault is used to contain a user ID and password for one user authorized to start and use that PC. When a user turns on the power to one of these PCs, he receives a prompt for authentication. He is expected to enter his vault user ID and password. At company discretion, the user's vault ID and password may be synchronized with his Windows® Domain ID and password. If that is done, the user will not see the Windows® logon prompt during system start; he will be taken to his desktop after authenticating to HPM. Either way, only the user knows his vault password. No one else, including the I.T. Security Administrator, can determine what that password is.

If the user enters a valid vault ID and password for that PC at power on, the vault will release the real hardware passwords to BIOS. BIOS will verify the passwords are correct and will allow the PC to start as normal. The real hardware passwords are known only to the system vault, to the PC hardware and to the Hardware Password Manager database, not the user.

It is possible to have up to 21 user IDs defined in the vault of a PC. Each user will have a unique user ID and password. Although the users do not know the real hardware passwords, they can start the PC. It is also possible for the administrator to define temporary user IDs on a PC. For example, he can define an ID to be used by a technician that might work for one day or one use.

Tools are provided to help users recover from "I forgot my password" scenarios. In one model, the user can authenticate to the HPM server to gain access to their computer and change their vault password. This is done from BIOS on the PC. In order to do this, the PC must have a wired Ethernet connection to a network with the HPM server. As an alternative, the company may create emergency IDs on each PC. The purpose of the ID is that the Help Desk can provide the ID and password to a user who is otherwise locked out of his PC. The Help Desk can post a password change order for the emergency user ID on that PC if they wish to prevent the user from using the emergency ID later.

The tool of last resort is for the help desk to provide a user with the real hardware passwords (it's possible to bypass Hardware Password Manager at system start and revert to the standard BIOS prompts for hardware passwords). These passwords can be unique to the PC. The help desk could also post a hardware password change order for the PC at the same time they provide the real passwords to the user. That means that the next time the user's PC communicates with the Hardware Password Manager console, the PC will receive new hardware passwords.

## THE FIRST-OF-ITS-KIND MANAGEMENT TOOL FOR ALL FULL DISK ENCRYPTING DRIVES.

In May 2007 Seagate released a hard disk drive with a new capability. The drive encrypts all data before writing it to the platters and unencrypts data read from the platters before sending it out of the drive. Hitachi and Fujitsu followed Seagate's lead. These drives are called Full Disk Encrypting drives – FDE drives. These drives are also called Self Encrypting Drives.

Customers have shown a great deal of interest in these drives. The primary concern is how to manage the keys used by the encrypting drives. A typical large enterprise I.T. shop encounters hard disk drive problems every day. If the data on these encrypting drives is lost forever because of the encryption technology used inside the drive, most corporations will not deploy until something more manageable is brought to market.

The drive manufacturers either do not allow access to the encryption key at all, or only through a proprietary interface. Which means, by design it is difficult or impossible to directly manage the encryption key on an encrypting drive.

There is another way to manage the hard disk drive encryption key. All drive manufacturers support the Hard Drive Password and Master Hard Drive Password architecture. FDE drives add a bit more to this. If the HDP is not set on an FDE drive, the drive will automatically begin decrypting data as soon as data is asked for by the PC. If the HDP is set, the drive will lock the encryption key to the HDP. This means that the HDP is required not only to make the platters spin, but also to release the encryption key<sup>4</sup>.

Hardware Password Manager makes it possible for a company to centrally manage Hard Drive Passwords. It does not make it possible to escrow FDE encryption keys or to directly access those keys. However, since the key is tied to the HDP, the ability to centrally control the HDP does give a company control over the keys in FDE drives.

## THE PAYBACK CAN BE SUBSTANTIAL FOR INTERESTED CUSTOMERS.

- FDE drives are built with a co-processor inside them that does all encryption. Which means, there's no performance impact from the use of encryption
- The cost of an FDE drive is higher than the cost of the same drive that does not perform encryption. However, this cost difference is substantially less than the cost of a software full drive encryption solution
- FDE drives always encrypt data. There is no way to prevent them from doing that. If the HDP is set, you either know the HDP can therefore access the data or you do not and you are locked out of the data
- Hardware Password Manager supports the use of a fingerprint for authentication. This raises the security profile on the PC by reducing the risk of the user selecting a weak password for his vault. The company might even enforce machine generated, very long and complex vault passwords. The users do not care, they just slide a finger, only hackers care. The passwords are not taped to the PC, they can't be socially engineered from the user ("I don't know my password, I just slide my finger") and Hardware Password Manager does not allow brute force attacks<sup>5</sup>

### HIGH-END DESIGN

At a high level, the design of Hardware Password Manager requires infrastructure code in the BIOS on the PC, a small client that lives in Windows on the PC and the setup of a management application in the back end.

### BIOS COMPONENT

The BIOS infrastructure must accomplish the following tasks:

- Create and maintain a "vault". The vault is stored in flash. It contains the user ID and password for the user who owns the vault (one vault per user per PC)
- Provide secured flash storage for copies of that PC's real hardware passwords
- Handle local logon at system power on
- Handle emergency logon to the Hardware Password Manager server in the event of the user having forgotten his vault password
- Handle the BIOS-based mailbox. The mailbox is a mechanism for transferring commands from Windows to BIOS for execution at the next system resume from standby or hibernation. It is one of the ways administrative tasks are communicated in Hardware Password Manager
- Handle registration—the process of creating a new vault for a user of the PC
- Handle vault restore and vault delete processing



### WINDOWS CLIENT

At the level of Windows, there are components that facilitate registration, single sign-on and communication between BIOS and the management server. The registration task is activated when the company deploys Hardware Password Manager to PCs already in the field. The Windows client prepares BIOS to execute user registration when someone presses the power-on switch to start the PC.

During regular use, the Windows client provides an XP GINA and a Vista® credential provider. They will take credentials from BIOS during system start and use them to log the user on to his desktop on the PC.

The Windows client also executes any remote requests generated by the I.T. administrator, such as reset hardware passwords or revoke user access to a specific PC.

### SERVER COMPONENT

The Hardware Password Manager server is an application that can stand alone or be launched from a Master Console, if one exists. It is responsible for the following tasks:

- Backup of all client vaults
- Generating and storing real hardware passwords. These passwords can be looked up any time they are needed.
- Providing an administrative console to manage clients, users, groups and passwords
- Serving as a conduit for user authentication with the corporate Active Directory or LDAP directory

### HIGH LEVEL USE CASES

At the level of Windows, there are components that facilitate registration, single sign-on and communication between BIOS and the management server. The registration task is activated when the company deploys Hardware Password Manager to PCs already in the field. The Windows client prepares BIOS to execute user registration when someone presses the power-on switch to start the PC.

During regular use, the Windows client provides an XP GINA.

In terms of normal use, users will interact with Hardware Password Manager every time they press the power switch to turn on their PC. This use case will require authentication early in BIOS execution. Administrative functions are much less common. Preparing a PC for deployment, retiring a PC and moving PCs between administrative groups are examples of normal use.

## NEW PC, IN PREPARATION WITHIN I.T.

In terms of unusual use, users will interact with Hardware Password Manager differently when they've forgotten their password. Resolution to this problem can be any of the following:

- If the PC has a wired connection to the company Intranet, the user can authenticate to the Hardware Password Manager server from BIOS. He will be expected to log on using his Intranet credentials. If Intranet authentication is successful, he can clear his vault on the PC and re-enroll. This means that his old vault is erased and a new one is created for him. A new password will be required for this process.
- If the company has provided an emergency account in the vault of that PC, the user can be given access to that account by someone at the Help Desk. This sort of emergency account is created when the administrator first adds the PC to his deployment of PCs using Hardware Password Manager. While he is at it, the administrator can create accounts for himself and for technicians who might need to access the PC.
- The Hardware Password Manager authentication prompt can be bypassed. If it is, the PC reverts to the standard interface for entry of the Power On Password and Hard Drive Password. The Help Desk can provide those passwords directly to the user. Since they are likely to be long and difficult, the user will have an incentive to stop using them. The Help Desk can place an order for the user's vault to be destroyed, for forcing the user to re-register on the PC. The Help Desk could also place an order for the real hardware passwords to be changed on that PC at the first opportunity after this call occurs. That would be the next time the PC establishes a VPN connection to the company network.

There are also use cases for technical support of the PC. This may be a desk side visit to respond to a problem. Because the user brings the PC to a technician with a problem. Whatever the cause, it shouldn't be necessary for the user to divulge his password to the technician. A company can solve this in the following ways:

- Build a permanent technical support vault ID for each PC. The vault ID has a standard password known to the tech support staff.
- Build a temporary technical support vault ID as and when needed. Provide the password to tech support prior to the service activity. In this model, only I.T. Administration knows the tech account passwords. When tech needs the password, he must ask for it. The password he gets may be one time or for a day's use only, then it is automatically changed.
- Provide the technician with the real hardware passwords for the PC. If company policy requires, follow up with a hardware password change order for the PC after the service event.

Companies have a couple of choices for deployment scenarios. To begin with, on initial release, Hardware Password Manager is supported on ThinkCentre M58 and later desktops and the following ThinkPad notebooks.

- T400, T500
- R400, R500
- X200, X300, X301
- W500, W700

The first step is applying a BIOS update, available through the normal channel for BIOS updates (provide URL and specify what BIOS update is required). This BIOS update fully implements the BIOS infrastructure required by Hardware Password Manager.

The HPM server is a stand alone server application. It is designed to operate in an Active Directory-based management environment. This server application can stand alone in the corporate infrastructure. It also fits under a master management console. A tool is available to launch the HPM server from a management master console if the customer wants to manage HPM in that way.

Once BIOS is updated, companies have the following options to implement Hardware Password Manager.

## PCs ALREADY IN THE FIELD

In this case, there are PCs in the field at the time the decision is made to deploy HPM.

- The first step is to deploy and install BIOS flash updates using standard BIOS update procedures
- Once the BIOS is ready, the HPM install package can be distributed for silent installation on the deployment of PCs Any method of software distribution will work for this task. In this model, the real passwords, Administrative ID, emergency ID and the first user ID are all created together, at the same time and during this step
- Once the package is installed, the PC is ready for registration and enrollment
- The next time the user logs on to Windows, he will see a prompt to enroll in HPM

As stated in the previous case, the registration process requires an Ethernet connection between the registering PC and the HPM server. This can be over a VPN.



## SUMMARY

PC hardware passwords were created to provide another layer of protection for the PC and the data on the hard disk drive. These passwords have never been widely used because there is no management capability and no ability to recover from the “I forgot my password” problem. In the case of hardware passwords, forgetting the POP means replacing the PC motherboard. Forgetting the HDP means replacing the hard disk drive and loss of all data on the old drive.

There are now hard disk drives on the market that feature a native ability to encrypt all data written to the drive platters. This is automatic. The drives depend on the Hard Drive Password as the mechanism for authenticating to the drive. We’ve already established that the HDP will not be widely used until it can be managed.

Lenovo now offers two solutions to the problem of managing hardware passwords. The first solution is based on the use of Microsoft’s WMI technology as the delivery and execution method for facilitating central management of BIOS settings, including hardware passwords. In order to manage hardware passwords, the passwords must first be manually set so the user is unable to change the passwords to something he prefers.

The second solution is Lenovo Hardware Password Manager. This client-server application fits into an existing Active Directory or LDAP infrastructure. It can also stand alone. It gives Company I.T. full control over the hardware passwords for all PCs under the control of HPM. Further, it creates the notion of a BIOS-level user ID and password for the end user to use as a single sign-on proxy. This user ID and password can be synchronized with the Windows ID and password for the user. The user also has the option to authenticate himself to BIOS using his fingerprint. With the system power on, the user is asked for these credentials. If he can provide them, the system will boot to his desktop. This mechanism preserves the user’s privacy and makes it possible for him to use the system, even though he does not know what the actual hardware passwords are.

These solutions create new opportunities for a company to control access to their PCs and most importantly, to the confidential data stored on those PCs.



## APPENDIX HARDWARE PASSWORD STRUCTURE.

The Power On Password (POP) is intended for the user responsible for the PC. The user is prompted to enter the Power On Password early in the BIOS execution process. Failure to enter either the POP or the SVP at the time will cause BIOS to halt execution. If a halt occurs, the only way to re-start it is to turn the PC off and then back on. The POP can be a combination of characters with a maximum length of 32 characters.

The Supervisor Password is an administrative password for the control of BIOS. It is also called the Privileged Access Password (PAP). PC behavior can be influenced by how BIOS settings are configured on a PC. If the SVP is set on a PC, BIOS settings cannot be changed unless the SVP is known and entered during PC start-up. If the SVP is set, the only way to set or change the POP is by entering the SVP when prompted or when the password is being changed.

The Hard Drive Password is also intended for the user responsible for the PC. The user is prompted to enter the HDP immediately following entry of the POP. If the HDP is set and is not entered when requested, the hard disk drive will not unlock and the platters will not spin. If the HDP is not entered or entered incorrectly too many times (three times), then the user will have to turn the PC off and then try again. The HDP can be up to 32 characters in length.

The Master Hard Drive Password is an administrative password used to control the setting of the HDP. If the MHDP is set, it must be entered in order to change the HDP. If the MHDP is not set, then the user must know the current HDP to change the HDP.

1 <http://www.networkworld.com/columnists/2008/051908-single-sign-on-password.html>

2 Password Cracker—a program that serially tries all possible passwords, looking for the right one.

3 Active Directory is a Microsoft technology that serves as the basis for managing a deployment of PCs within an organization. The server or servers that the Active Directory based management infrastructures are installed on is often referred to as the “Active Directory back end” management system.

4 If the HDP is subsequently changed, the drive will unlock the key from the old password and lock the same key with the new password—no need to worry that the current key might be lost by a password change.

5 Brute force attack—sequentially trying every single possible password in the expectation that you will eventually find the correct password. There are two kinds of defense against this attack.