HP Commercial Notebook BIOS Password Setup

Table of Contents:

Introduction

The purpose of this document is to provide user guidance in the creation and setup of BIOS passwords for HP Business Notebooks. This paper addresses both single and multi-user password environments as well as integration with HP DriveLock and recovery of lost password via HP SpareKey.

Preboot Passwords

Multiple User Architecture in BIOS

Multi-user support has been implemented on the notebook BIOS since 2008.

- Multi-user support is necessary to solve boot password sharing issues
- Required for the HP ProtectTools One-Step Logon feature
- Multi-user architecture enables access control to BIOS policies and settings

User Groups in BIOS

In the multi-user architecture, there are different role based user groups. The BIOS has the capability for separation of function and access among these different user groups. The separation promotes higher security in situations where:

- Users will not have to share passwords
- BIOS administrator will not have to share setup passwords with users
- BIOS administrator will be able to assign granular control of setup features to users

Currently there are three types of BIOS users defined:

BIOS Administrator

The BIOS administrator user is created in F10 or remotely via the WMI tools.

BIOS administrator privilege includes:

- Management of other BIOS users
- Full access to F10 BIOS policy and settings
- Control F10 access of other users
- Unlocking the system when other BIOS users fail preboot authentication (BIOS administrator is one of the recovery options when the user authentication fails)

BIOS User

BIOS users are created by BIOS administrator in F10 or remotely via the WMI tools. BIOS users are OS independent.

BIOS user privilege includes:

- Use his/her BIOS password to authenticate and boot the BIOS
- Use his/her BIOS password to access F10 based upon permissions setup by the BIOS administrator

ProtectTools Users

ProtectTools users are created by HP ProtectTools within Windows. One-Step Logon requires the BIOS ProtectTools user, Drive Encryption user, and the Windows user to be one in the same. These users are registered in Windows with supporting user information dispatched down to FVE and BIOS domain. The user information includes user name, domain, SID, password/credentials. The resulting authentication is OS independent. This group of uses cannot change their password in F10.

ProtectTools user privileges include:

- Use his/her Windows password and other security tokens to authenticate and boot the BIOS and if enabled, can log all the way into Windows.
- Use his/her Windows password to access F10 based upon permissions setup by the BIOS administrator. ProtectTools users have the same privilege as the BIOS users when accessing F10.

Preboot Password Setup

Setting up BIOS preboot authentication without HP ProtectTools

Note: This procedure is equivalent to the earlier Power-On Password.

2008 and newer Business Notebook BIOS support multi-user authentication. To enable BIOS preboot authentication:

- First setup the BIOS administrator password via F10 setup -> Security. This establishes a BIOS administrator
- Next log into F10 as the BIOS administrator and add BIOS user(s) to BIOS via F10 setup -> Security -> User Management

At this point the BIOS will prompt for a BIOS user password during boot.

Setting up BIOS preboot authentication with HP ProtectTools

An alternative way to enable BIOS preboot authentication is to use the HP ProtectTools Security Manager within Windows. This process requires the user to go through the HP ProtectTools wizard to setup as a ProtectTools user, select and register security tokens such as a smart card or fingerprints and enable preboot security. The BIOS will then prompt for the PT user to authenticate themselves by using a Windows password, smart card or fingerprint during boot.

If there are both BIOS users and ProtectTools users within BIOS and preboot security is enabled within ProtectTools, the BIOS will prompt with a list of all current BIOS users and ProtectTools users.

If a BIOS user is selected from the list, the BIOS will authenticate the BIOS user with the appropriate BIOS user password, afterwards the user must log in again to Windows.

However, if a ProtectTools user is selected from the list, the BIOS will authenticate the user according to the policy set within ProtectTools, enabling the user to log in all the way to Windows.

Password Change

For BIOS users and BIOS administrator, go to F10 or use remote WMI tool to change the password if the old password is known.

For ProtectTools users, boot to Windows and then change the Windows password. The change will be automatically reflected in BIOS.

Forgotten Passwords

BIOS Users

There are three possible scenarios which apply regarding forgotten passwords:

- If a BIOS user forgets his/her password and has setup HP SpareKey, he/she can use the assistance offered by HP SpareKey to boot up the system. The BIOS will take the user to BIOS recovery screen upon his/her failure to enter the correct password, where the user can then use HP SpareKey to re-gain access to the system.
- If the BIOS user forgets their password and there is a BIOS administrator, the BIOS administrator can go to F10 to remove and add the BIOS user again, effectively supplying the user with a new password.
- If the PT user forgets the PT user password and has no HP SpareKey and there is NO BIOS administrator, the PT user can enter F10 as Guest User and then define a BIOS administrator and remove the PT user. Or, as an alternative, request HP Services to use a secured HP service tool to reset the system to factory default.

BIOS Administrator

If the BIOS administrator forgets the BIOS administrator password and has setup HP SpareKey, he/she can use the HP SpareKey to enter F10.

Otherwise, for 2009 and newer commercial notebook platforms, it would require HP Services to use a secured HP service tool to reset the system to factory default.

ProtectTools Users

If the ProtectTools user forgets his/her Windows password and has setup HP SpareKey, he/she can use the HP SpareKey to boot up the system.

- If Preboot Security is enabled and the user fails to enter the correct password the BIOS will take the user to a BIOS recovery screen where the user can use HP SpareKey to re-gain access to the system.
- If Preboot Security is not enabled, the user can press F7 to go to the BIOS recovery screen and use HP SpareKey to re-gain access to the system.

If a ProtectTools user forgets his/her password and there is a BIOS administrator, the BIOS administrator can use the BIOS administrator password at the BIOS authentication screen. However, the user will have to be authenticated again at the next domain: Drive Encryption or Windows.

HP DriveLock Passwords

Setup HP DriveLock Passwords

The BIOS options for managing DriveLock are:

Automatic DriveLock	– Enable/Disable	-Default: Disable
DriveLock	– Enable/Disable	-Default: Disable

Key points of distinction for DriveLock:

- DriveLock is a legacy single user approach
- Automatic DriveLock allows multiple user support for DriveLock.
- Legacy DriveLock and Automatic DriveLock settings are mutually exclusive.

Auto-DriveLock

When Automatic DriveLock is enabled, the BIOS will automatically generate a user DriveLock password, and the BIOS admin password is used as the master DriveLock password. This Automatic DriveLock feature is tied to the BIOS preboot authentication scheme. On boot the BIOS will first authenticate the user. This could consist of TPM (Trusted Platform Module) pre-boot authentication, a BIOS

user password, or a ProtectTools user with their Windows password or other token type such as a fingerprint or smartcard. Once this is done, the BIOS will automatically decrypt the DriveLock user password and unlock the drive.

How to recover when Automatic DriveLock fails

In the case where the user password fails to unlock the drive, the BIOS will display the message saying "Automatic DriveLock was previously enabled on this drive. Please enter the BIOS admin password from when this drive was present." If the BIOS admin password is correctly presented the user will be able to successfully boot and access the drive, otherwise the drive will be locked and a Non-system disk error will be displayed.

Manual DriveLock

The manual DriveLock feature allows a user to type in his/her own passwords. However, this feature only supports one password and in the case where more than one user is sharing the system, they will also have to share the DriveLock password.

How to recovery when DriveLock password is forgotten

If a user forgets the DriveLock password, the BIOS will allow the user to enter the BIOS administrator password to unlock the drive. Successfully entering the BIOS admin password will permit booting and access to the drive, otherwise the drive will be locked and a Non-system disk error will be displayed.

Note: In case where both the DriveLock password and the BIOS administrator password are not available, the drive cannot be recovered.

For more information

HP Business PC Security Solutions -
http://h20331.www2.hp.com/hpsub/cache/281822-0-0-225-121.html

2008 HP Business Notebook PC F10 Setup Overview
http://bizsupport1.austin.hp.com/bc/docs/support/SupportManual/c01607517/c01607517.pdf