HP Business Notebook Password Localization Guidelines V1.0

November 2009

Table of Contents:

1. Introduction

HP has implemented the One Step Logon feature on its 2008 and newer commercial portable computers.

The HP ProtectTools Security Manager wizard enables various security levels to protect the computer system and the data. The security levels that can be set are:

- HP Credential Manager – Protects your Windows account
- Preboot Security – Protects your computer before booting to OS.
- HP Drive Encryption – Protects your computer data by encrypting the hard drive.

Along with security levels, the user can select the security login methods for authentication at each security level. The possible login methods are: Windows password, Fingerprint and HP Java Smartcard.

When the login method is set to Windows password and all security levels are enabled, the One Step Logon feature allows the user to enter her/his Windows password in the Preboot BIOS and drive encryption environment, which then logs the user all the way into the appropriate Windows account.

The complexity arises when Windows support hundreds of Input locales. A user can enter the Windows password using an input locale that's different than the physical keyboard. e.g. The user can select to type German using the International US keyboard layout etc.

However, at the Preboot Security level and the HP Drive Encryption level, the input localization support is limited. The purpose of this whitepaper is to help user understand the limitations and also to set the proper Windows password to avoid the lockout situation when the Preboot Security Level and/or the HP Drive Encryption level is enabled.

2. Supported Platforms

The HP_Tools partition feature described in this document is supported by 2008 and 2009 HP business notebooks.

3. Overview of Design

The goal of the HP ProtectTools implementation is to use password filters to reject passwords that might lock out a user at the Preboot BIOS level or Drive Encryption level. The ProtectTools Security Manager will be responsible to reject a user password at setup or password change time. A password can be acceptable for the Windows password, but if allowed may cause a lock out at Preboot BIOS or Drive Encryption level. These passwords will therefore be rejected by the HP ProtectTools password filter.

The BIOS Preboot and Drive Encryption each preloads tables of key mapping from Scan Code to Unicode based on the supported keyboard layout. (see table Figure -1 below). When the user enters the password before OS starts, the BIOS or the Drive Encryption software will convert the key strokes to the correct Unicode based on key mapping tables and then compare the password with the one stored. The ProtectTools Security Manager will pass the keyboard layout information to BIOS Preboot and Drive Encryption.

In addition, the BIOS Preboot and Drive Encryption may implement additional methods to assist password entering. E.g. In 2008 Business Notebook BIOS, a soft keyboard will be loaded to enter glyphs directly with the mouse instead of pressing a key on the keyboards if a user fails to type their password correctly. The Drive Encryption software allows the user to dynamically load the keyboard layouts.

4. Supported Keyboard Layouts in Preboot and Drive Encryption

The Preboot BIOS and Drive Encryption support a subset of Windows' keyboard layouts due to space and other limitations. Below is a list (Figure 1) of supported keyboards in Preboot and Drive Encryption. In some cases, the common name for a particular keyboard layout differs in Windows Vista from the HP designation. In order to clarify, we provide both names.

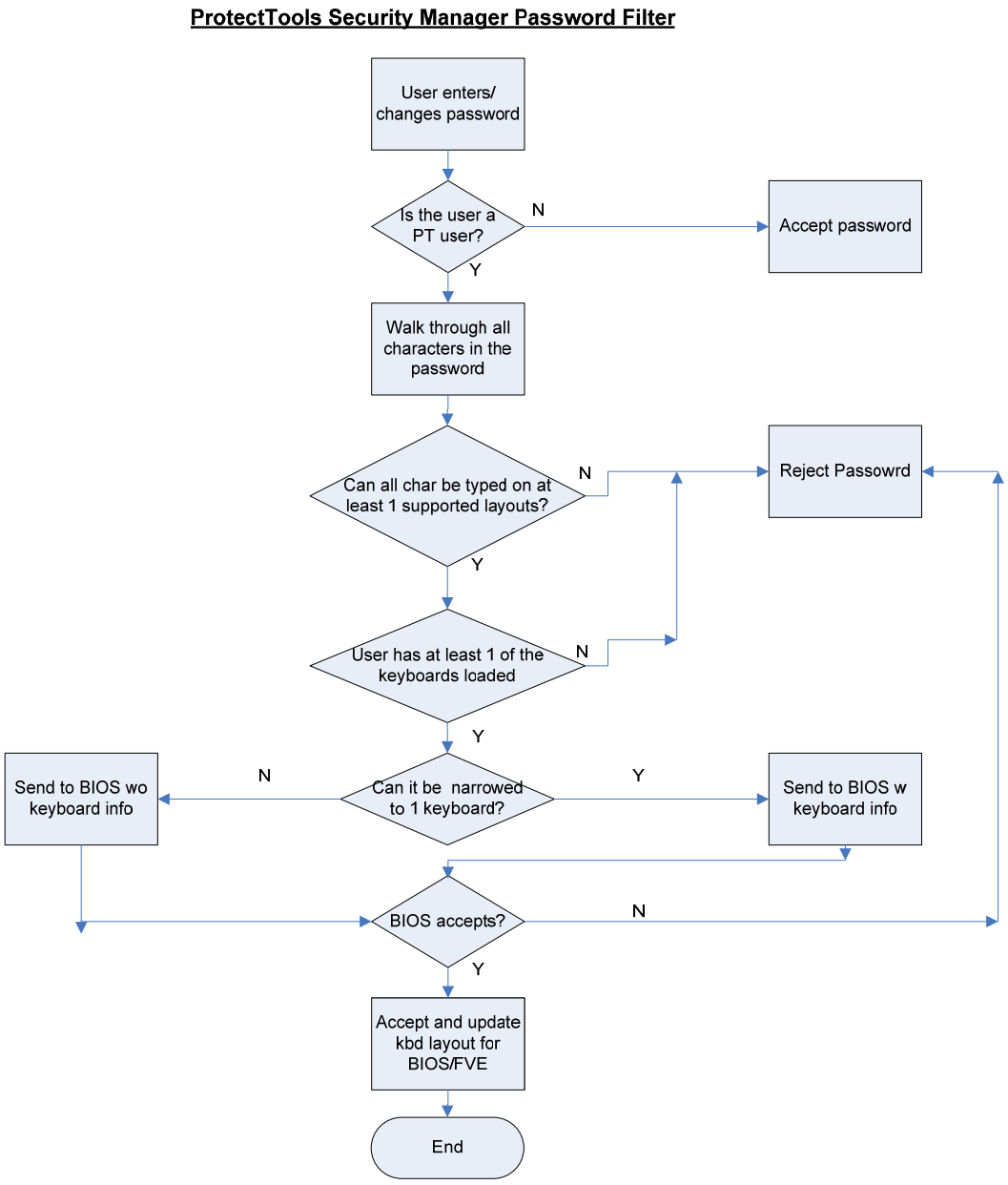
HP Keyboards	Common Name in Microsoft Windows Vista	Code (hex)
Arabic (101)	Arabic (101)	0401
Belgian (Comma)	Belgian (Comma)	1080c
Canadian French (Legacy)	Canadian French (Legacy)	0c0c
Canadian French	Canadian French	1009
Chinese Bopomofo	Chinese (Traditional) - US Keyboard	0404
Chinese ChaJei	Chinese (Simplified) - US Keyboard	0804
Czech	Czech	0405
Danish	Danish	0406
Dutch	Dutch	0413
Estonian	Estonian	0425
Finnish	Finnish	040b
French	French	040c
German	German	0407
Greek	Greek	0408
Hebrew	Hebrew	040d
Hungarian	Hungarian	040e
Icelandic	Icelandic	040f
Italian	Italian	0410
Japanese	Japanese	0411
Kazakh	Kazakh	043f
Korean	Korean	0412
Latin American	Latin American	080a

HP Keyboards	Common Name in Microsoft Windows Vista	Code (hex)
Norwegian	Norwegian	0414
Polish (Programmers)	Polish (Programmers)	0415
Polish (214)	Polish (214)	10415
Portuguese	Portuguese	0816
Portuguese (Brazilian)	Portuguese (Brazilian ABNT)	0416
Romanian	Romanian (Legacy)	0418
Slovakian	Slovak	041b
Slovenian	Slovenian	0424
Spanish	Spanish	0c0a
Spanish (International)	Spanish Variation	1040a
Swedish	Swedish	041d
Swiss	Swiss German	0807
Thai (Kedmanee)	Thai Kedmanee	041e
Turkish F	Turkish F	1041f
Turkish Q	Turkish Q	041f
UK	United Kingdom	0809
US	US	0409
US (International)	United States-International	20409

Figure -1

5. HP ProtectTools Security Manager Filter Logic

In order to prevent a lock out situation, the first level of defense is implemented by the HP ProtectTools Security Manager. It installs a password filter to reject those Windows passwords that may possibly cause a lock out in Preboot BIOS or Drive Encryption.



6. How Preboot BIOS Implements the Password Filter And Handles Dead Keys

The HP BIOS implements a second level password filter to further prevent the lock-out situation.

HP BIOS Preboot and HP Drive Encryption contain the keyboard mappings for all the supported keyboards listed above. When a user is setting up Preboot Security with the BIOS Preboot or Drive Encryption levels enabled, or when a user changes his/her password, the BIOS Preboot and Drive Encryption receives the Unicode password from the OS. The BIOS is responsible to guarantee that the keyboard being associated with that user is able to type the password. Otherwise, the BIOS will reject the password. However, there still may be an instance where the user changes the keyboard in Windows without the BIOS's knowledge or when the user is not aware of the keyboard layout currently in use. To compensate for the situation where the user may not be able to physically type their password due to these two situations, the BIOS will automatically provide the user the ability to "click" out her/his password after failing with the physical keyboard. This is done by showing every character on the screen that could be typed with the keyboard currently associated with the user, each of them as buttons and which can be clicked with the mouse to form the password. This method provides a way for the user to enter the password without the physical keyboard.

(Please note: When using the "On-Screen Keyboard" in the BIOS, there are many characters shown and some characters may look very similar to others on some keyboards. If experiencing trouble using this feature, so please look at all of the characters before clicking out your password to ensure you are entering the correct characters.)

In the BIOS, the use of Dead Keys has also been added to try to provide the user with as much keyboard functionality as possible. If for some reason a certain character is produced on the OS level that cannot be typed in the BIOS, this will cause the password change to be rejected. Unless rejected, the user should feel safe and confident in using Dead Keys for passwords associated with the Preboot Security feature.

This ability of the Preboot Security hinges on its ability to ensure that the Windows password can always be entered in the Preboot BIOS and Drive Encryption, and therefore all characters that require special typing methods that are not common to all keyboards, such as the use of the Kana key or the use of IME function of Windows, will result in the password change being rejected from the BIOS, as the BIOS does not contain these advanced typing features.

7. Exceptions

Windows IME is not supported at the Preboot Security Level and the HP Drive Encryption Level

In Windows, the user can choose an IME (Input Method Editor) to enter complex characters and symbols, such as Japanese or Chinese characters, by using a standard western keyboard.

The IME is not supported at Preboot and HP Drive Encryption level. Windows password entered with IME may not be entered at the Preboot or HP Drive Encryption level and may result in a lockout situation. In some cases, the Microsoft Windows doesn't display the IME when user enters password.

For example, for some Japanese installations of Windows XP, the default IME is called the "Microsoft IME Standard 2002" for Japanese[1], which actually translates as keyboard layout E0010411. However, this is an IME and not a keyboard layout (the keyboard layout coding scheme is simply preserved by Microsoft for IMEs, which themselves extend the concept of a keyboard layout). Since this is not a keyboard layout that can be represented in the typing environment for the BIOS Preboot password prompt or the Drive Encryption password prompt, *any* password typed with this IME is rejected by ProtectTools. The solution is to switch to a supported keyboard layout, such as Microsoft IME for Japanese or the Japanese keyboard layout itself, both of which translate to keyboard layout 00000411 (despite its "IME" designation in the former case). Another "IME" that actually translates to keyboard layout 00000411 is the "Office 2007 IME" for Japanese[2].

Warning
When HP ProtectTools is deployed, passwords entered with Windows IME will be rejected.

---

[1] It is worth observing that this name is also different from the "Common Name in Microsoft Windows Vista", shown in Figure 1. The reason for this is that Windows maps some IMEs to a keyboard layout. In such cases, the IME would be supported by HP ProtectTools, because the underlying keyboard layout definition, designated by the "Code (hex) column in Figure 1, is what matters.

[2] This is an important consideration. The mere fact that Microsoft or a third party uses the term, "IME" or "Input Method Editor" does *not* necessarily mean that the input method is an IME instead of a keyboard layout. This can make for confusion in some cases, but the software itself *always* looks at the hexadecimal code representation. Thus, if an "IME" really maps to a supported keyboard layout, then HP ProtectTools can support the configuration.

Password change on different keyboard layouts may have potential issues

If the password is initially set with one keyboard layout – e.g. US English (409) and then the user changes the password using a different but also supported keyboard layout – e.g. Latin American (080A), the password change will work in Drive Encryption but will fail in BIOS if the user uses characters which exist on the latter (say ē) but not on the former.

Note: this issue is worked by the dev team and maybe fixed in the later release.

A simple solution to this problem is to remove the user in question from HP ProtectTools by running the HP ProtectTools Manage Users application to remove the user from HP ProtectTools. Then, it is possible to run the Getting Started wizard again for the same user, ensuring that the desired keyboard layout is selected in the OS prior to running the wizard. This way, the BIOS stores the desired keyboard layout, and passwords that can be typed on this keyboard layout will be properly set in the BIOS.

Another potential issue is the use of different keyboard layouts that can all produce the same characters. For example, both the U.S. International keyboard layout (20409) and the Latin American keyboard layout (80A) can produce the character, é, though different keystroke sequences might be required. If a password is initially set with the Latin American keyboard layout, then the Latin American keyboard layout is set in the BIOS, even if the password is subsequently changed using the U.S. International keyboard layout.

Special Key Handling

- Chinese, Slovakian, Canadian French, Czech, Korean

When a user selects one of the above keyboard layouts and enters a password (e.g. abcdef), the same password has to be entered with a shift key for lower case and the shift key and cap key for upper case in Preboot BIOS and Drive Encryption.

Note: Some standard Asian keyboards don't allow numeric characters. In these cases if a user tries to enter a number for password, it will be rejected on the following keyboards.

· Chinese Bopomofo
· Japanese

Characters Not Supported

Arabic	Windows The ﹷ, ﹹ, ﹻ keys generate two characters	BIOS The ﹷ, ﹹ, ﹻ keys generate one character	Drive Encryption The ﹷ, ﹹ, ﹻ keys generate one character

French Canadian	Windows ç, è, à, é with cap locks are Ç, È, À, É in windows	BIOS ç, è, à, é with cap locks is ç, è, à, è in bios	Drive Encryption ç, è, à, é with cap locks is ç, è, à, è in FVE

Spanish	40a is not supported

US Int'l	Windows The ¡, ¤, ‘, ’, ¥, × keys are rejected on the top row The å, ®, þ keys are rejected on the second row The á, ð, ø keys are rejected on the third row The æ key is rejected on the bottom row

Czech	Windows The ğ key is rejected The į key is rejected The ų key is rejected The ė ı ż keys are rejected The ģ ķ ļ ņ ŗ keys are rejected

Slovakian	Windows	BIOS
	The ż key rejected	The š, ś, ş keys is rejected when typed, but accepted with the soft keyboard The ţ dead key is generating two characters

Hungarian	Windows	BIOS
	The ż key is rejected	The ţ key generates two keys

Slovenian	Windows *żŻ key rejected in windows and bios alt gr dead key*	BIOS *ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, and Š key rejected in bios* *Able to login with soft keyboard for all keys.*

8. What to do when a password is rejected

Passwords can be rejected for the following reasons:

1. User is using an IME keyboard which is not supported. This is a common issue with double-byte languages (Korean, Japanese, Chinese …). To resolve, when a password is rejected by the HP ProtectTools, please go to Windows -> Control Panel -> Regional and Language Options.

- Select the "Languages" tab
- Click on the "Details" button
- In the "Settings" tab, click on the "Add" button to add a supported keyboard (e.g. add US keyboards under Chinese Input Language).
- Set the supported keyboard for default input.
- Restart the HP ProtectTools and enter the password again.

2. User is using a character which is not supported. To resolve, the user needs to change the Windows password to include only supported characters. (Unsupported characters are listed above). Then the user can go through the HP ProtectTools Security Manager wizard again to enter the new Windows password.

[November 2009]