HP ProtectTools password guidelines

Table of contents

Introduction

The purpose of this paper is to describe how HP ProtectTools Security Manager for Microsoft Windows implements password filter logic and to explain the requirements for setting a proper Windows password when using HP ProtectTools. HP has implemented the One Step Logon feature through HP ProtectTools software on 2008 and newer commercial HP Notebook PCs. The HP ProtectTools Security Manager wizard enables various security levels to protect the computer system and data from unauthorized access. Three security levels can be set:

- HP Credential Manager—Consolidates user passwords and networks accounts into a single data unit called User Identity, which is protected by strong authentication and encryption methods
- Preboot Security—Protects your computer before it boots the operating system (OS)
- HP Drive Encryption—Protects data on your computer by encrypting the hard drive

In addition, you can select a single security login method for authentication at all security levels. The possible login methods include using a Windows® password or fingerprint sensor. When the Windows password is used as the login method, and all security levels are enabled, the One Step Logon feature requires you to enter the Windows password only in the Preboot Security environment or in the full volume encryption (FVE) preboot environment if BIOS isn't enabled. Then the One Step Login feature verifies your password at all subsequent security levels and logs you in to the appropriate Windows account. However, you can be locked out of the computer if you select a Windows password that is rejected at the Preboot Security or Drive Encryption levels. This can occur if you select or change your Windows password when the input locale setting of the computer is different from the physical keyboard being used.

Windows supports hundreds of input locales. Each locale is a set of information based on user preferences related to language, environment and/or cultural conventions. For example, a user may choose to type a password in German using the International US keyboard layout or by setting up a password combining words from different languages. This makes password verification more difficult because input language translation (localization) support is limited at the Preboot Security and HP Drive Encryption levels. In Windows it is possible to mix keyboard layouts within a single password, particularly by using the right-ALT key in conjunction with the numeric keypad to enter characters. Pre-boot environments do not support all keyboards or keyboard combinations that are possible within Windows. It is the role of HP ProtectTools Security Manager to prevent the user from being locked out due to password rejection at the Preboot Security and/or HP Drive Encryption levels.

Overview of HP ProtectTools Security Manager

With respect to typed authentication tokens such as passwords and HP Spare Key answers, the goal of HP ProtectTools Security Manager is to apply filters when the Windows password is set up or changed to ensure that the password can be typed at the Preboot Security level or Drive Encryption level. This filtering prevents the user from being inadvertently locked out of the computer by rejecting passwords that require a combination of keyboards or an unsupported keyboard layout. HP ProtectTools Security Manager achieves its goal by passing the keyboard layout information to the Preboot Security and Drive Encryption software. Preboot Security and Drive Encryption use preloaded tables of characters to map key strokes from scan code to Unicode based on the supported keyboard layout. When you enter a password before the OS starts, the Preboot Security and Drive Encryption software convert your key strokes to the correct Unicode characters based on the key mapping table. Each software component compares the entered password with the stored password.

Preboot Security and Drive Encryption may implement additional methods to assist you when entering your password. For example, in the 2008and newer HP Notebook PC BIOS, if you fail to type a password correctly, a soft keyboard is displayed on the screen so that you can click characters with the

mouse rather than pressing keys. The Drive Encryption software allows you to dynamically load the keyboard layouts if an incorrect keyboard is currently being used.

Supported keyboard layouts in Preboot Security and Drive Encryption

Table 1 contains a list of keyboards which HP supports in Preboot Security and Drive Encryption. The Preboot Security and Drive Encryption login screens support a portion of available Windows keyboard layouts due to space and other limitations particular to their operating environments. In some cases, the common name for a particular keyboard layout in Windows Vista® or Windows 7 differs from the HP designation; therefore, both names are listed in the table.

Table 1. HP keyboards supported in Preboot Security and Drive Encryption

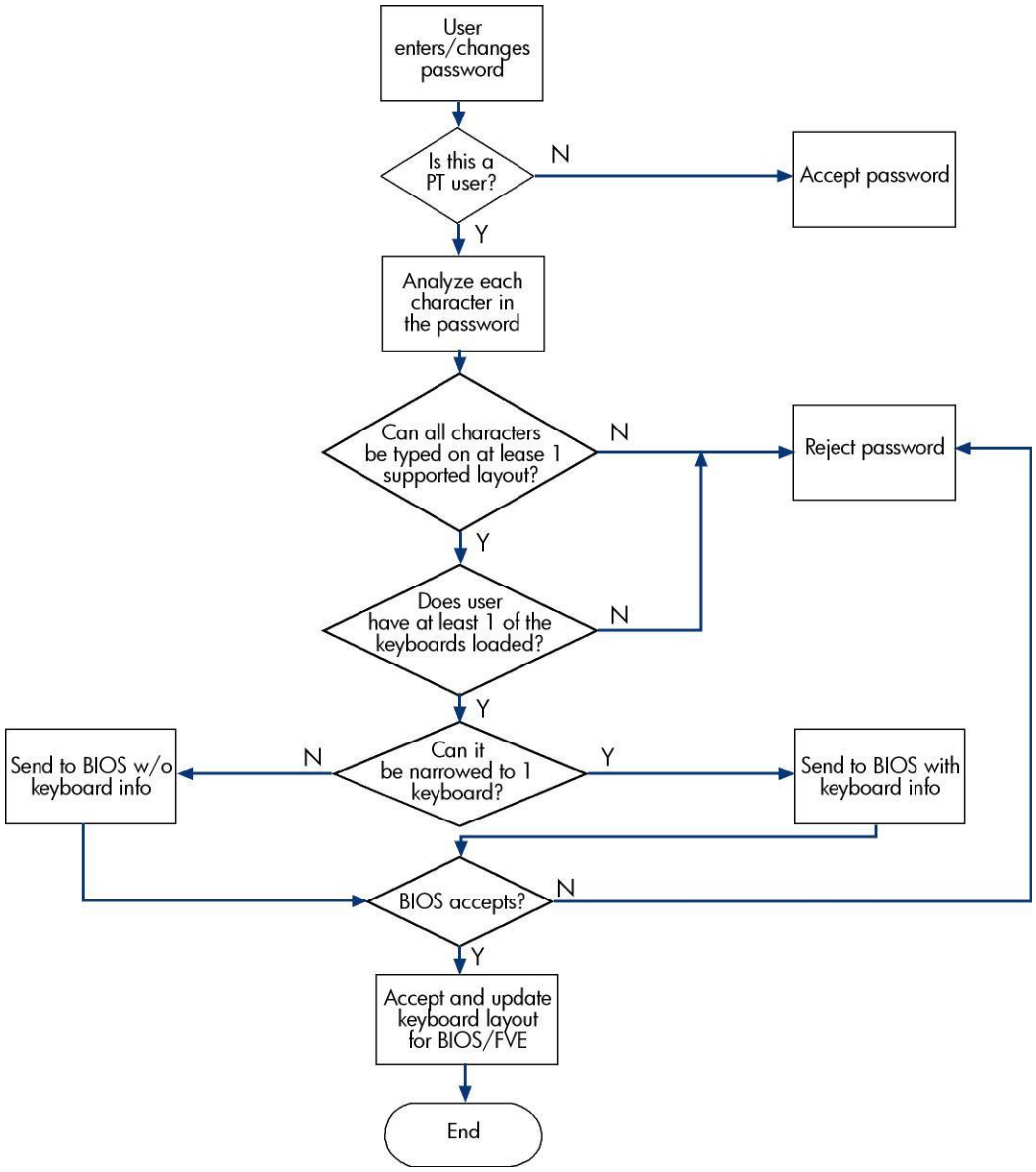
HP keyboards supported	Common name in Windows Vista or Windows 7	Code (hex)
Arabic (101)	Arabic (101)	0401
Belgian (Comma)	Belgian (Comma)	1080c
Canadian French (Legacy)	Canadian French (Legacy)	0c0c
Canadian French	Canadian French	1009
Chinese Bopomofo	Chinese (Traditional) - US Keyboard	0404
Chinese 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
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

HP keyboards supported	Common name in Windows Vista or Windows 7	Code (hex)
US	US	0409
US (International)	United States-International	20409

HP ProtectTools Security Manager filter logic

To prevent the user from being locked out by the Preboot Security or Drive Encryption logins, HP ProtectTools Security Manager uses a password filter to reject Windows passwords that may be unacceptable. The logic behind the password filter is shown in Figure 1. After a ProtectTools user enters or changes a password, Security Manager verifies that each character entered can be typed by the keyboard layout loaded into the current user's profile. If a character is not supported, the password is rejected.

Figure 1. Operational logic of the ProtectTools Security Manager password filter



HP BIOS implements a second level password filter to ensure that the user is not locked out of the computer. Preboot Security and Drive Encryption contain the keyboard mappings for all the supported keyboards. When a user sets up or changes a password while the Preboot Security or Drive Encryption levels are enabled, Preboot Security and Drive Encryption receive the Unicode password hash from the OS. Password filtering logic verifies that the keyboard layout associated with the user is able to type the password. Otherwise, the password filter will reject the password.

Changing the keyboard in Windows without verification by the password filter or choosing a password while unaware that an unintended keyboard layout is selected may prevent you from physically typing your password. After three unsuccessful login attempts, Preboot Security login will automatically display an on-screen keyboard with all possible characters from the associated keyboard layout and allow you to "click" each character in the password.

Note
The on-screen keyboard in the Preboot Security login displays many characters, some of which look very similar to characters on other keyboards. To enter the correct characters, you should look at all available characters before attempting to enter the password.

How Preboot Security handles dead keys

A dead key is a keyboard key that modifies the next key that is typed. For example, in Windows, some keyboards allow you to type combinations like the following: pressing the dead key **'** and then "**e**" produces "**é**." In other cases, applications themselves allow for dead keys. Many Windows applications allow you to press the dead key **Ctrl - '** and then "**e**" to produce "**é**", independent of the keyboard layout being used. At the Preboot Security login, the use of dead keys has been added to provide you with as much keyboard functionality as possible. If a character can be produced in Windows and cannot be typed at the Preboot Security login, the password will be rejected. If the dead key is not rejected when changing the password of a ProtectTools user within Windows, the user can also use the dead key when logging in at the Preboot Security login screen. Typically, Preboot Security supports dead keys that are supported by a keyboard and does **not** support dead keys that are supported by particular applications. Thus, the Spanish keyboard layout in Preboot allows for the **'** and then "**e**" combination to produce "**é**"; it does **not** support the **Ctrl - '** and then "**e**" combination to produce "**é.**"

Preboot Security ensures that the Windows password chosen can always be typed at the Preboot Security and Drive Encryption login screens, as neither of these two operating environments supports all the advanced typing features available in Windows. Therefore, all characters that require special typing methods that are not common to all keyboards, such as the use of the Kana key (Japanese) or the Input Method Editor (IME) function of Windows, will result in password rejection by the password filtering logic.

Exceptions

Windows Input Method Editor (IME) is not supported

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

Windows features an IME that allows a user to compose thousands of complex characters and symbols, such as the many Japanese or Chinese characters, using a standard keyboard. IME is an OS component that extends the capability of the keyboard, but it is not a supported keyboard layout that can be used to enter a password at the Preboot Security or Drive Encryption login screens. Therefore, *any* password typed with an IME is rejected by the ProtectTools password filtering logic.

For example, in some Japanese installations of Windows XP, the default IME is called "Microsoft IME Standard 2002."[1] Because this IME is not a keyboard layout that can be used during the password prompt at the Preboot Security or Drive Encryption login screens, the password typed with this IME in Windows is rejected by ProtectTools. The solution is to switch to a supported keyboard layout, such as Microsoft® IME for Japanese (despite its IME designation) or the Japanese keyboard layout itself, both of which translate to keyboard layout 00000411. Another IME that actually translates to keyboard layout 00000411 is the "Office 2007 IME" for Japanese[2].

Password changes using different keyboard layouts

There are potential issues if a user initially sets up a password using one keyboard layout and then changes the password using a different keyboard layout. In general, the password filtering logic attempts to determine the user's current keyboard layout and uses this keyboard layout to update the password token information in both the Preboot Security and Drive Encryption authentication domains. If the user enters a character that exists on the latter keyboard but not on the former, the password change will be accepted in Drive Encryption but it will be rejected in the BIOS.

A simple solution to this problem is to remove the user in question from HP ProtectTools by running the HP ProtectTools Administrative Console. After ensuring that the desired keyboard layout is selected in the OS, add the user again through the Administrative Console. This allows the Preboot Security and Drive Encryption authentication domains to store the desired keyboard layout, and allows passwords that are typed on the stored keyboard layout to be properly typed at the login screens for either domain.

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

---

[1] This name is different from the "Common Name in Microsoft Windows Vista" shown in Table 1 because Windows maps some IMEs to a keyboard layout. In such cases, the IME is supported by HP ProtectTools because the underlying keyboard layout is defined, as designated by the Code (hex) column in Table 1.

[2] The use of the terms "IME" and "Input Method Editor" by Microsoft or a third party can be confusing because the input method could be a keyboard layout instead of an IME. However, the software *always* looks at the hexadecimal code representation to determine if an IME maps to a supported keyboard layout. Thus, if an IME maps to a supported keyboard layout, HP ProtectTools can support the configuration.

Some Asian Keyboards don't support numeric characters

Some standard Asian keyboards don't allow numeric characters. If a user tries to enter a number for password, it will be rejected on these keyboards.

- Chinese Bopomofo
- Japanese

What to do when a password is rejected

If a password is rejected by HP ProtectTools for one of the reasons listed below, follow the appropriate procedure.

- The password was typed using an unsupported IME keyboard. This is a common issue with double-byte languages, such as Korean, Japanese, and Chinese. To avoid password rejection by ProtectTools:
  1. Select **Windows > Control Panel > Regional and Language Options**.
  2. Select the **Languages** tab
  3. Click the **Details** button
  4. In the Settings tab, click the **Add** button to add a supported keyboard. For example, add US keyboards under Chinese Input Language.
  5. Set the supported keyboard as the default input. Close ProtectTools.
  6. Open ProtectTools. Enter the password again.

- One or more characters in the password is not supported (see Characters not supported). To resolve this problem, select a Windows password that includes only supported characters. Then open the HP ProtectTools Security Manager wizard again to enter the new Windows password.

Special key handling

Chinese, Slovakian, Canadian French, Czech, and Korean

When a user selects one of the supported 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 CAPS LOCK key for upper case in Preboot Security and Drive Encryption. With the Korean keyboard layout, it is not the SHIFT key that is used to produce English characters but rather the ALT key. Depressing ALT will allow the Preboot Security or Drive Encryption login screens to type English lowercase characters. Depressing ALT and CAPS LOCK will produce English uppercase characters.

Characters not supported

Table 2. Characters not supported

Keyboard Layout	Windows	BIOS	Drive Encryption
Arabic	The ﻷ, ﻹ, ﻵ keys generate two characters.	The ﻷ, ﻹ, ﻵ keys generate one character.	The ﻷ, ﻹ, ﻵ keys generate one character.
French Canadian	ç, è, à, é with cap locks are Ç, È, À, É	ç, è, à, é with cap locks is ç, è, à, è in bios.	ç, è, à, é with cap locks is ç, è, à, è in FVE.
Spanish	40a is not supported.		
US International	On the top row, the ¡, ¤, ‘, ’, ¥,		

Keyboard Layout	Windows	BIOS	Drive Encryption
	× keys are rejected. On the second row, the å, ®, þ keys are rejected. On the third row, the á, ð, ø keys are rejected. On the bottom row, the æ key is rejected.		
Czech	The ǧ 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	The ż key is rejected	The š, ś, ș keys are rejected when typed, but accepted with the soft keyboard. The ț dead key generates two characters.	
Hungarian	The ż key is rejected	The ț key generates two characters.	
Slovenian	żŻ key is rejected in Windows and BIOS alt gr dead key	ú, Ú, ů, Ů, ș, Ș, ś, Ś, š, and Š keys are rejected in BIOS. Login is possible with soft keyboard for all keys.	

For more information

To learn more about HP business notebooks, contact your local HP sales representative or visit www.hp.com/go/notebooks.

664183-001, Created May 2011