Trusted Computing (Security Menu)
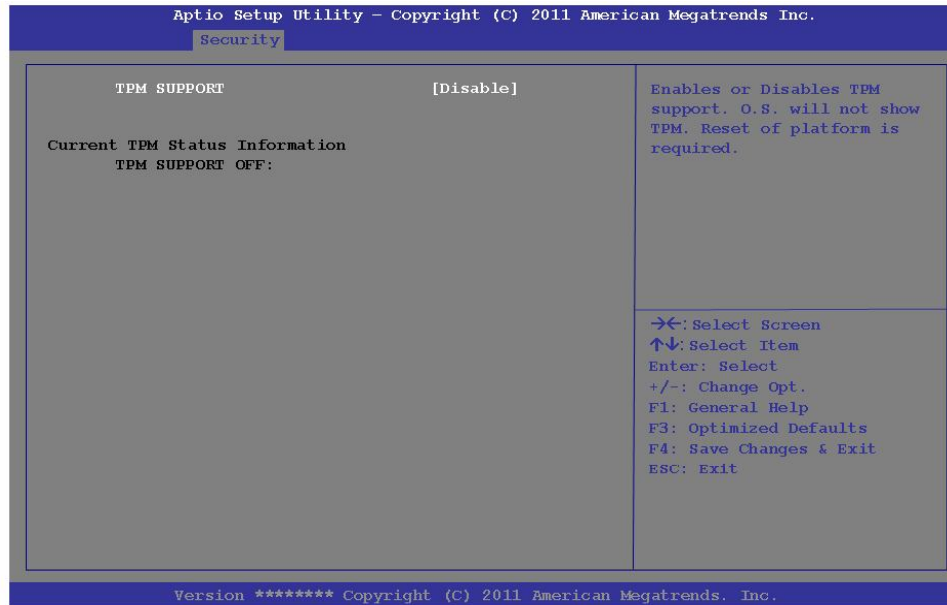
This sub-menu will allow you to enable/disable Trusted Platform Module (TPM) support, and to configure the TPM State. Select **Trusted Computing** and press Enter to access the sub-menu. Press Enter to access the **TPM Support** menu and select **Enable** to display the full TPM configuration menu (see *"Trusted Platform Module" on page 7 - 96* for details).

Figure 5 - 5
TPM Support

```
            Aptio Setup Utility - Copyright (C) 2011 American Megatrends Inc.
              Security

       TPM SUPPORT                      [Disable]          Enables or Disables TPM
                                                           support. O.S. will not show
                                                           TPM. Reset of platform is
   Current TPM Status Information                          required.
       TPM SUPPORT OFF:



                                                           →←:Select Screen
                                                           ↑↓:Select Item
                                                           Enter: Select
                                                           +/-: Change Opt.
                                                           F1: General Help
                                                           F3: Optimized Defaults
                                                           F4: Save Changes & Exit
                                                           ESC: Exit


            Version ******** Copyright (C) 2011 American Megatrends. Inc.
```

TPM State (Security Menu > TPM Support Enabled)
Select **TPM State**, press Enter and select **Enable** to change the TPM state to enabled. You will then need to press **F4** to save the changes and restart the computer.
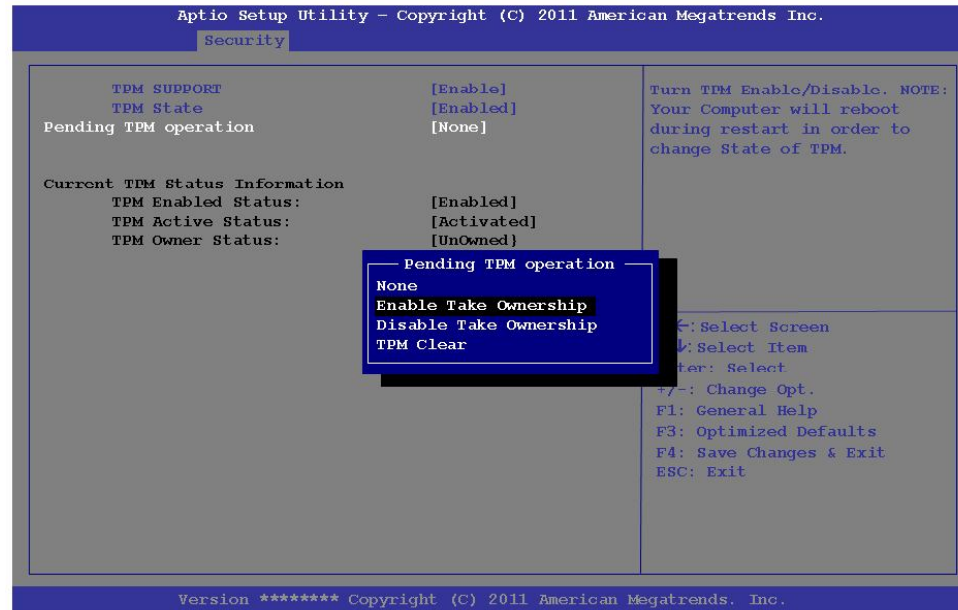
```
            Aptio Setup Utility - Copyright (C) 2011 American Megatrends Inc.
                 Security

      Configuration                                    Enables or Disables BIOS
          TPM SUPPORT              [Enable]            support for security device.
          TPM State               [Enabled]           O.S. will not show Security
      Pending operation           [None]              Device. TCG EFI protocol and
                                                       INT1A interface will not be
                                                       available.
      Current Status Information
          TPM Enabled Status:     [Enabled]
          TPM Active Status:      [Activated]
          TPM Owner Status:       [UnOwned]

                                                       →←: Select Screen
                                                       ↑↓: Select Item
                                                       Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F3: Optimized Defaults
                                                       F4: Save Changes & Exit
                                                       ESC: Exit



            Version ******** Copyright (C) 2011 American Megatrends. Inc.
```

Figure 5 - 6
TPM State (Enabled)

As the computer restarts press **F2** to enter the BIOS again and go to the **TPM Configuration menu**.

Pending TPM operation (Security Menu > TPM Support & TPM State Enabled)
Select **Pending TPM operation**, press Enter and select the option you require (if
you are initializing TPM you should select **Enable Take Ownership**). You will then
need to press **F4** to save the changes and restart the computer. You can now install
the TPM driver (see *"Trusted Platform Module (TPM) Driver Installation" on
page 7 - 57*) and then initialize the TPM.

Figure 5 - 7
**Pending TPM
operation
(Enable Take
Ownership)**

```
              Aptio Setup Utility - Copyright (C) 2011 American Megatrends Inc.
              Security

         TPM SUPPORT                      [Enable]            Turn TPM Enable/Disable. NOTE:
         TPM State                        [Enabled]           Your Computer will reboot
     Pending TPM operation                [None]              during restart in order to
                                                              change State of TPM.

     Current TPM Status Information
         TPM Enabled Status:              [Enabled]
         TPM Active Status:               [Activated]
         TPM Owner Status:                [UnOwned]
                            ┌─── Pending TPM operation ───┐
                            │ None                        │
                            │ Enable Take Ownership       │
                            │ Disable Take Ownership      │
                            │ TPM Clear                   │     ←:Select Screen
                            └─────────────────────────────┘     ↓:Select Item
                                                              ter: Select
                                                              +/-: Change Opt.
                                                              F1: General Help
                                                              F3: Optimized Defaults
                                                              F4: Save Changes & Exit
                                                              ESC: Exit

              Version ******** Copyright (C) 2011 American Megatrends. Inc.
```

7

⚠

Password Warning

If you set passwords for any of the security modules, **NEVER** forget your password.

The consequences of this could be serious. If you cannot remember your boot password you must contact your vendor and you may lose all of the information on your hard disk.

Security Modules (Fingerprint & TPM)

The encrypted channel between the **Trusted Platform Module security chip** (see *"Trusted Platform Module" on page 7 - 54*) and the **fingerprint reader** with **AuthenTec TrueSuite** software (see *"Fingerprint Reader Module" on page 7 - 35*) provides a high level of security for your computer. A further level of security and control is provided in the BIOS (see *"Security Menu" on page 5 - 10*).

The **fingerprint reader** and **AuthenTec TrueSuite** software allow you to:

- Access or Lock your computer
- Protect sensitive files
- Access frequently used websites using your fingerprint
- Fill in frequently log on information

Fingerprint Reader Module

The fingerprint reader module provides a high level of security for your computer. Make sure you have administrator's rights to your computer, and have a *Windows* password enabled for full security protection.

Fingerprint Reader Driver Installation

1. Insert the *Device Drivers & Utilities + User's Manual* disc into the CD/ DVD drive.
2. Click **Option Drivers**.
3. Click **3.Install FingerPrint Driver > Yes**.
4. Click **Next**.
5. Click the button to accept the license and click **Next**.
6. Click **Next > Install**.
7. Click **Finish > Yes** to restart the computer.
8. Click **Start > All Programs > AuthenTec TrueSuite**.

7

<div style="border: 2px solid red; background: red; color: white;">

🔔

Fingerprint Enrollment

Note that it is strongly recommended that you **enroll more than one finger in case of injury etc.**

</div>

AuthenTec TrueSuite Application

The **AuthenTec TrueSuite** application is used in conjunction with your fingerprint reader to enroll fingerprints and manage settings etc.

User Enrollment

1. Click **Start > All Programs > AuthenTec TrueSuite**.
2. Click **Yes** when you have identified your **fingerprint sensor** (**11** Fingerprint Reader Module in *Figure 1 - 2 on page 1 - 6*).
3. Click **Yes** when you are ready to enroll your fingerprints.
4. Click on the fingerprint diagram to select any finger to enroll.
5. You will be required to enter your *Windows* password (you will be prompted to create a password if you have not already done so) at this point (click **OK** to confirm the password entry).
6. Swipe the finger until the progress bar reaches **100%** to enroll that finger.
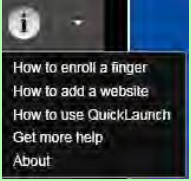
Figure 7 - 16
Fingerprint Enrollment

7. You will be prompted to select another finger for enrollment (it is recommended that you enroll a number of fingers - see sidebar).
8. Click the button to continue once you have enrolled a number of fingerprints.
9. Enter the required information and click the button to register your software, or click to register later.
10. Your fingerprints will now be enrolled (you may enroll any additional fingerprints at any time).

Figure 7 - 17
AuthenTec
TrueSuite

Help

Click the **Help** ⓘ icon and select a help topic from the drop-down menu. **Get more help** will provide a more comprehensive list of help topics.

Settings

Click the **Settings** 🍴 button on the menu bar to access the personalization settings for **AuthenTec TrueSuite**. Here you can choose to enable/disable Website Log On, QuickLaunch, Fast User Switching and the desktop icon. You can also select the Theme and export/import identities. Click the **Save** button to save any changes made.

Figure 7 - 18
**AuthenTec
TrueSuite - Settings**

Windows Log On

Windows log on allows you to gain access to your computer by swiping your finger across the fingerprint reader sensor. Use the **Biometric Devices** control panel (in the **Hardware & Sound** category) in *Windows* to turn **Biometrics on/off** when required. Access the **Biometric Devices** control panel and select **Change biometric settings** to turn the biometrics on or off, or to allow users to log on to *Windows* using fingerprints.
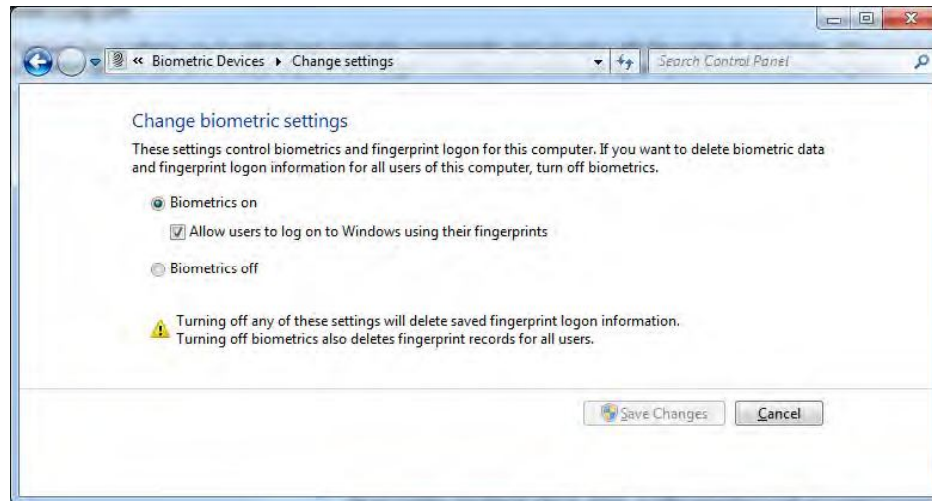
Figure 7 - 19
Biometric Devices Control Panel (Windows Hardware & Sound)

7

When Biometrics is on, and "*Allow users to log on to Windows using their finger-prints*" is enabled, simple swipe you finger across the reader to log on to *Windows*.

AuthenTec KeepSafe

The **KeepSafe folder** is an encrypted area assigned on your hard drive that allows you to store files and folders to be protected by fingerprint protection. The folder will appear on your desktop (if selected in the **Personalization Settings**) and in My Computer, but will not be visible to other users of your computer.

To **lock/unlock** the **KeepSafe** folder right-click it to display the context menu and select **Unlock/Lock**. You will be required to authenticate when unlocking the folder using either a fingerprint swipe or *Windows* password.

To add files to **KeepSafe** folder just open the folder and drag and drop files into the folder. You may also right-click any file to bring up the context menu and select **Add to KeepSafe** (you can select whether or not to keep or delete the original file).

7