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).

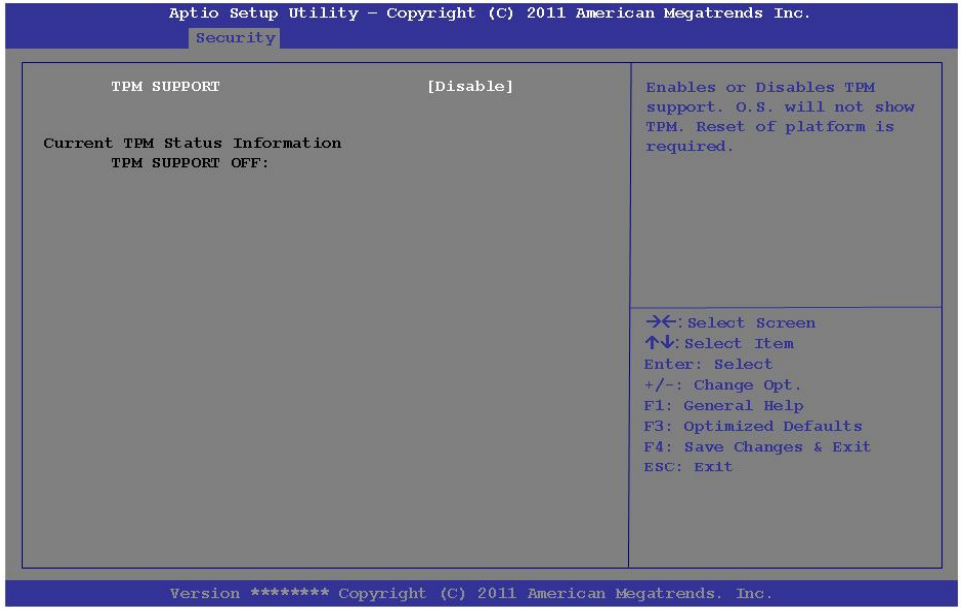


Figure 5 - 5
TPM Support

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.

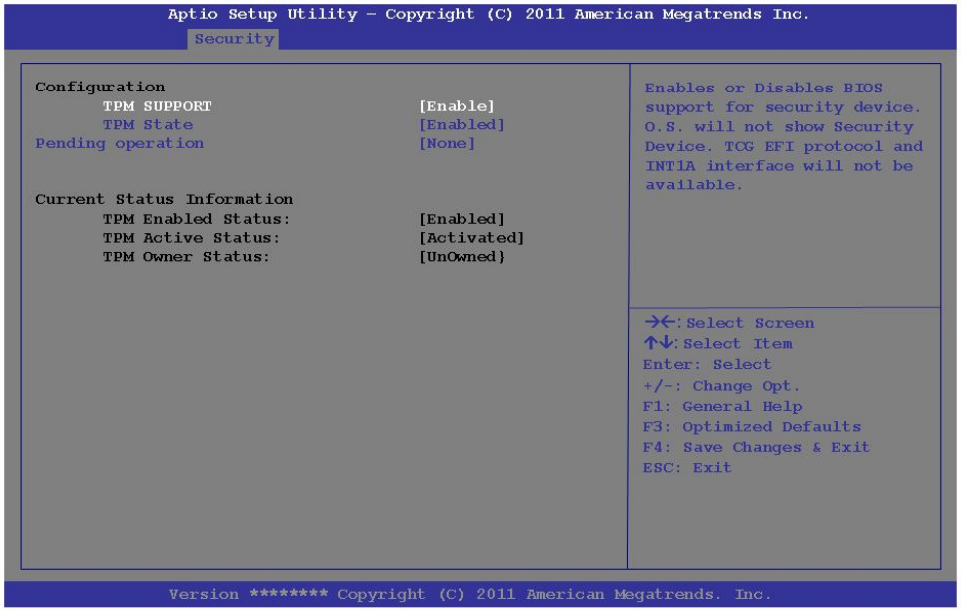


Figure 5 - 6
TPM State (Enabled)

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 - 78***) and then initialize the TPM.

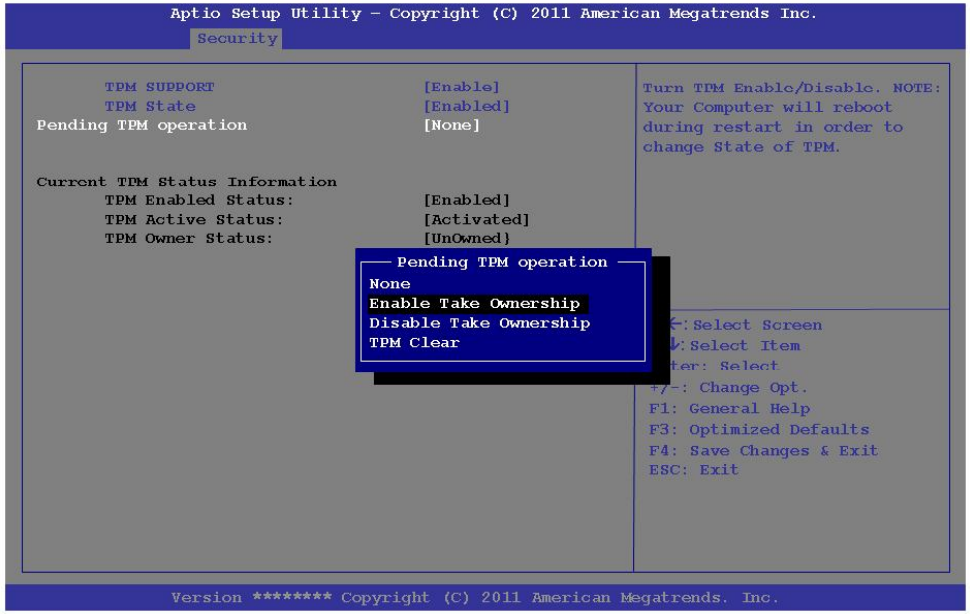


Figure 5 - 7
Pending TPM operation (Enable Take Ownership)

Trusted Platform Module (TPM) Driver Installation

1. Make sure you have enabled and activated the TPM in the BIOS before installing the driver (if you do not do see the note below).
2. Insert the ***Device Drivers & Utilities + User's Manual*** disc into the CD/DVD drive.
3. Click **Option Drivers** (button).
4. Click **5./4.Install TPM Driver > Yes**.
5. Click **Install > Next**.
6. Click the button to accept the license and click **Next**.
7. Click **Next > Next > Install**.
8. Click **Finish > Yes** to restart the computer.

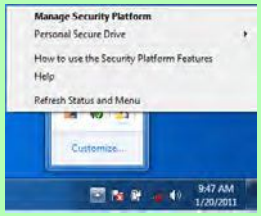
Initializing TPM

1. Run the application from the **Infineon Security Platform Solution > Manage Security Platform** item in the **Start > Programs** menu.
2. Click **User Settings** (tab) and click **Yes,** or right-click the icon in the notification area of the taskbar, and select **Security Platform Initialization** (or click the **Security Platform State** taskbar bubble).
3. The **Quick Initialization** method will automatically be selected for you (if you need to use advanced settings provided by your network administrator then select **Advanced Initialization**).
4. You will need to use a removable media (e.g. a USB Flash Drive) to store passwords and data (keep the media in a safe place until required).
5. Select the drive you want to use from the drop-down menu and click **Next**.

Figure 7 - 50
Security Platform Quick Initialization Wizard

Help

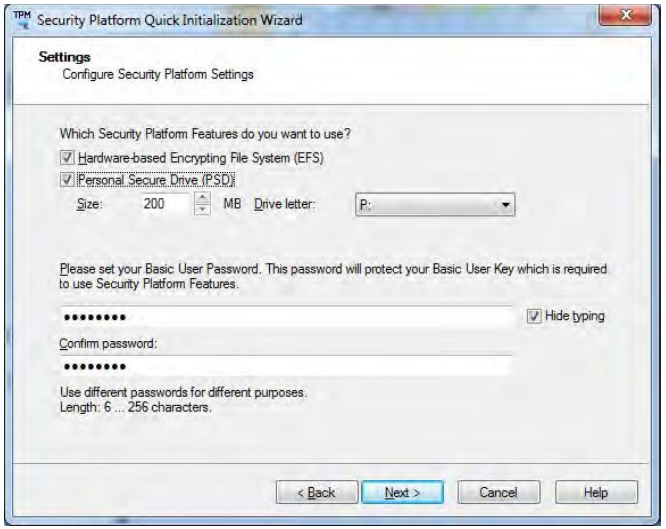
Right-click the icon in the notification area of the taskbar to bring up the menu to select ***Help*** or **How to use the Security Platform Features**.



You can also click the **Help** button in any of the Infineon Security Platform Settings Tool tabs to bring up specific help topics on each tab.

Figure 7 - 51
Settings

6. Choose the **Security Platform Features** you want to use by clicking the appropriate tickbox.
7. Enter a **Basic User Password** (and re-type to confirm it) and click **Next**.



8. Click **Next** to confirm the settings.
9. The computer will then initialize the settings.
10. Click **Finish**.
11. Click the tabs and control panels to adjust the settings.
12. Double-click the icon in the taskbar notification area to access the **Infineon Security Platform Settings Tool**, or right-click the icon and select a menu item.

Infineon Security Platform Settings Tool

The Infineon Security Platform Settings Tool allows you to manage and check the TPM state, manage your password information, and to backup and restore the TPM data. As TPM is usually administered within large enterprises and organizations, your system administrator will need to assist you in managing the information here.

Figure 7 - 52
Infineon Security Platform Settings Tool

Menus

Note that not all the menus pictured here will be available for access. The menu items that appear will be dependent on your configuration settings etc. (see the **Help** file for full details).

User Settings

This page allows the settings to be configured for the currently logged in Infineon Security Platform user including the ability to change the password, configure secure e-mail, file and folder encryption and Enhanced Authentication. You can also import or delete certificates protected by the security platform.

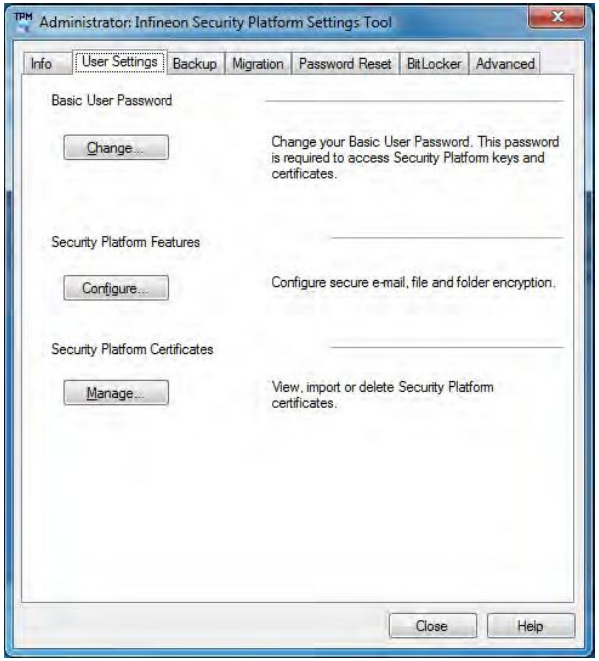


Figure 7 - 53
Infineon Security Platform Settings Tool (User Settings)

Backup

Here you can configure backup and restore operations. Backup files contain the computer identification and user identification information which is used to match the machine name and user name with the current machine and user during restoration.

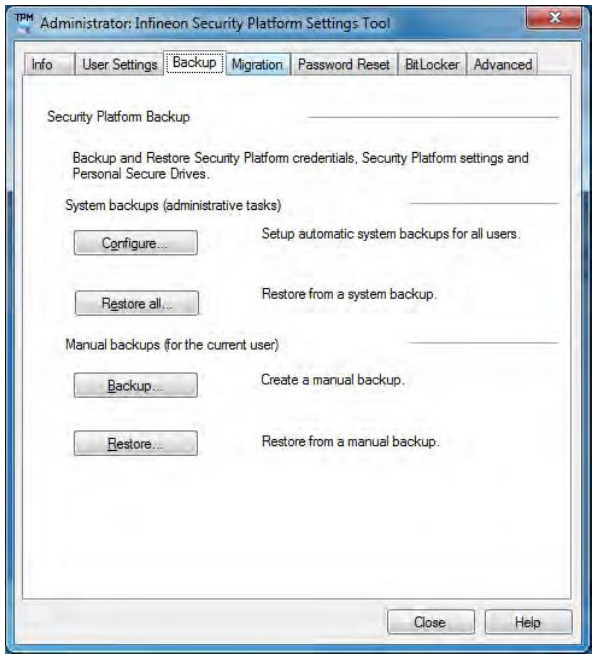


Figure 7 - 54
Infineon Security Platform Settings Tool (Backup)

Migration

The Migration tab is used to help securely transfer keys and certificates from one platform to another.

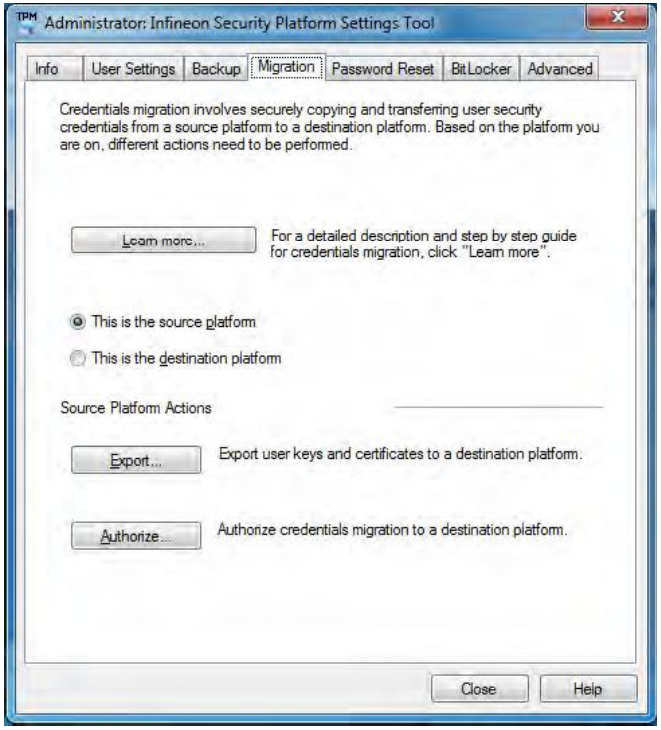


Figure 7 - 55
Infineon Security Platform Settings Tool (Migration)

Password Reset

Use Password Reset to reset basic user passwords when required.

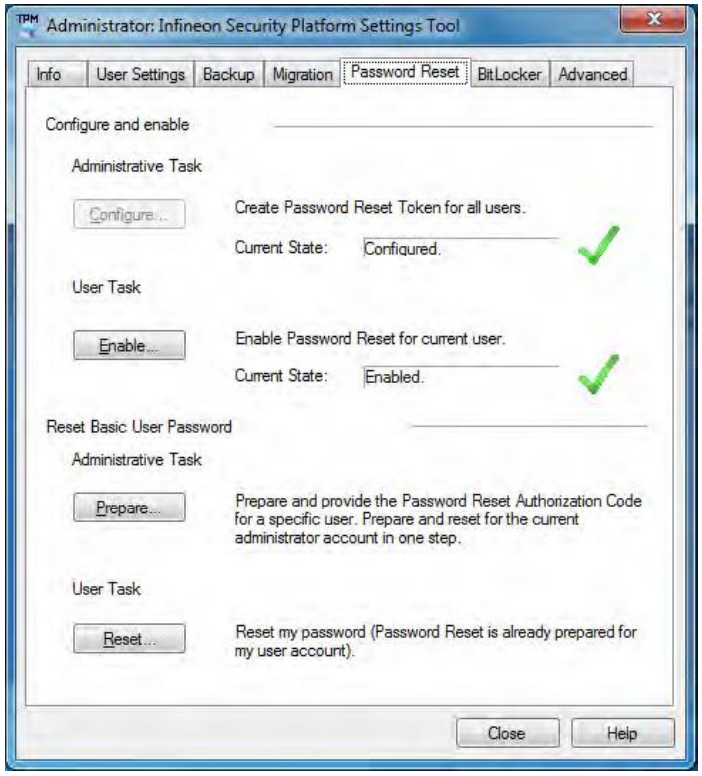


Figure 7 - 56
Infineon Security Platform Settings Tool (Password Reset)

BitLocker

BitLocker Drive Encryption can be used in conjunction with the TPM to encrypt data on the disk and is done via the **Microsoft BitLocker Control Panel Applet**. Click **Configure** and select a drive to be encrypted and then follow the Wizard to begin the encryption process.

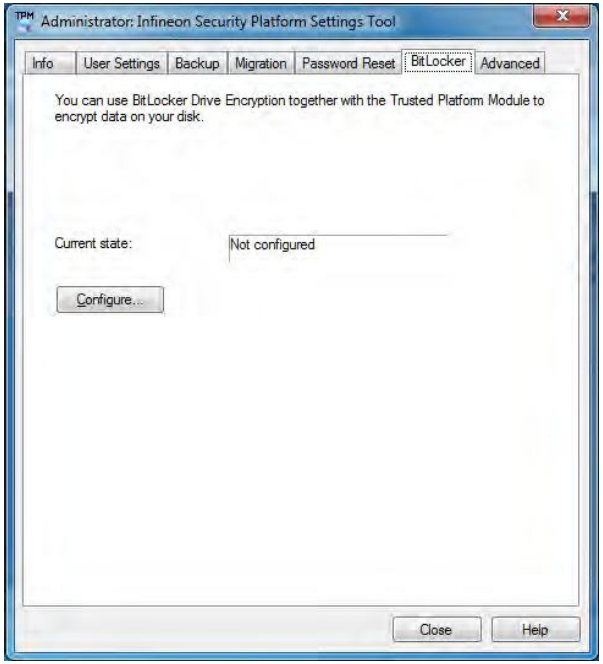


Figure 7 - 57
Infineon Security Platform Settings Tool (BitLocker)

Access the Microsoft **BitLocker Drive Encryption** control panel applet from the ***Windows*** control panel (**System and Security**).

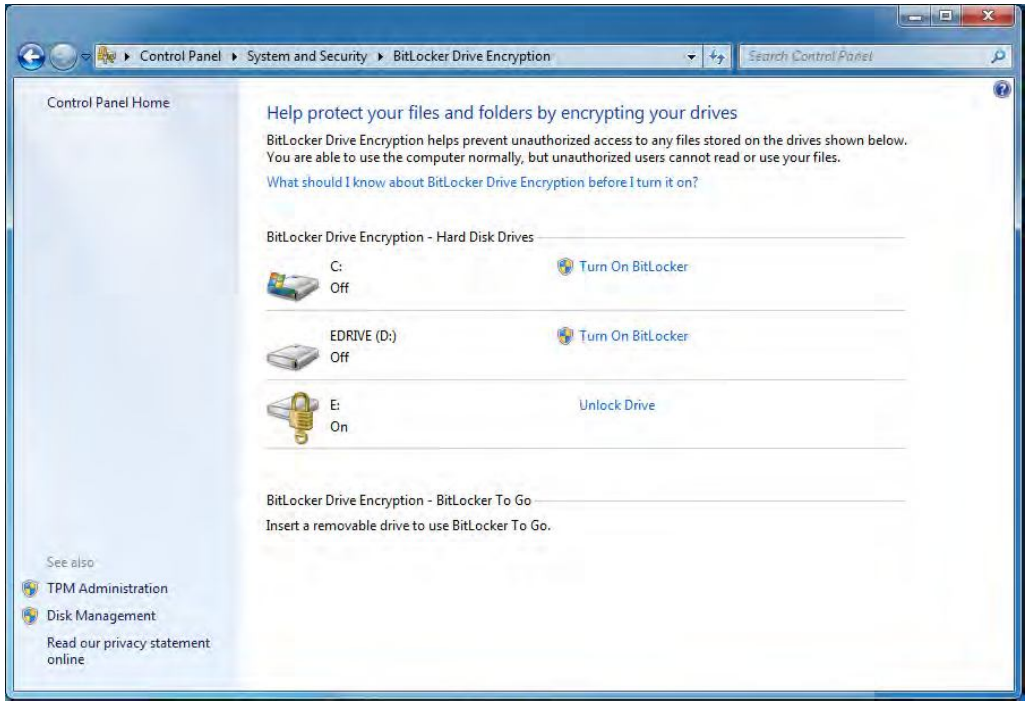


Figure 7 - 58
BitLocker Drive Encryption

Advanced

Configure all the Security Platform owner and policy settings from the Advanced tab. The settings that can be changed are for the local computer only.

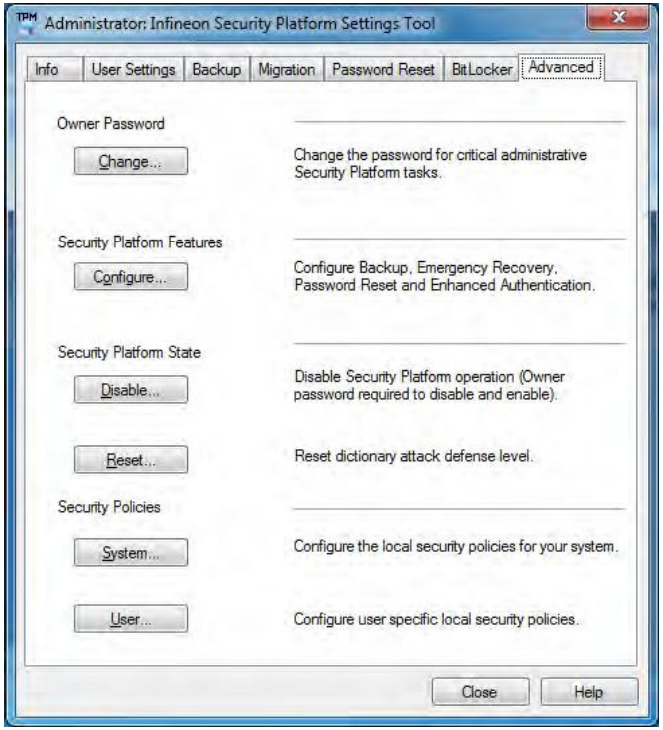


Figure 7 - 59
Infineon Security Platform Settings Tool (Advanced)