Lenovo BIOS Security Features for ThinkPad X250

Lenovo Product Security Office
1025 Think Place
Morrisville, NC
27560
November 9, 2015

Introduction

Computers have become an indispensible part of our lives. In our personal lives, we use computers to communicate with friends and relatives. We get news and information about the world. We use them to research topics and find information. And we use them to conduct our business and manage our finances.

Business processing has seen a similar revolution since the introduction of the personal computer. Gone are the days of paper processing and paper records. These have been replaced by computing systems and applications that exponentially increased the processing efficiency and records capability.

The goal of information security has always been to prevent unauthorized access to the information contained in the records archive. Prior to the advent of computer technology, this meant physical access security. The paper records were kept in a safe storage area with physical controls (perhaps even human guards) to prevent individuals who did not need access from obtaining the information. Today, security not only means physical access protection, but must also includes protection against virtual access by individuals who have managed to find a way to gain access to the networks that interconnect our computing systems.

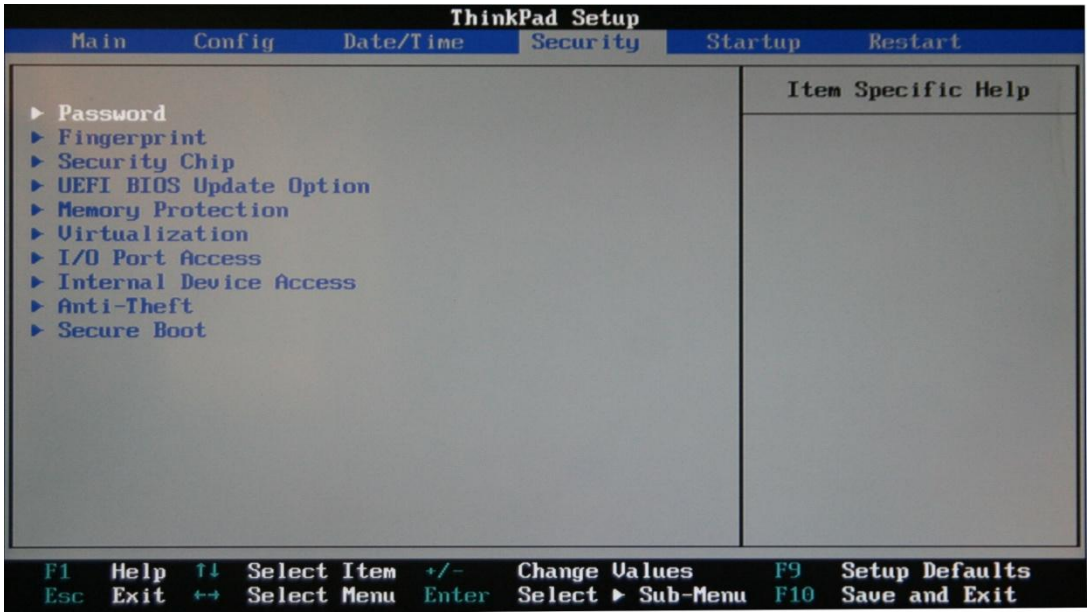
Protection of the information stored in the system begins with the firmware (BIOS). Lenovo system BIOS provides features that allow the user customize the level of protection provided by the system BIOS. The purpose for this document is describe those features and give some guidance about how they may be used to protect the unauthorized access to the system and the information stored on the system.

Illustrations in this document are based on a Lenovo ThinkPad x250 BIOS version. While not all features described here are implemented in all systems, other ThinkPads should be similar.

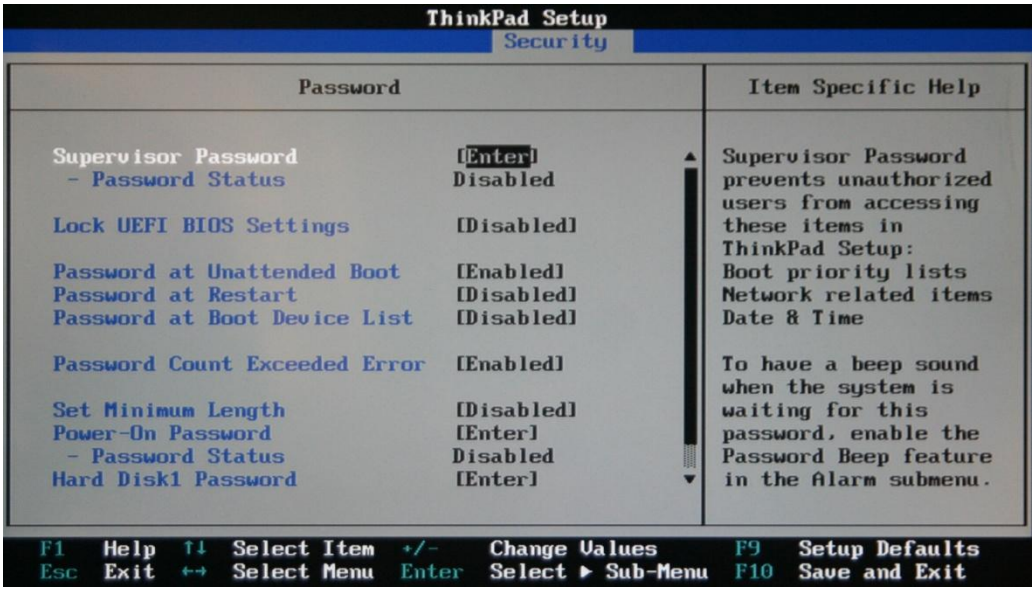
Lenovo ThinkPad BIOS Security Features

❖ BIOS Security Setup Screen

All ThinkPad BIOS security settings except the boot order settings are accessed from this screen. To access the BIOS security screen, users must press the F1 key while booting the system and then press the right arrow key until the “Security” tab is highlighted.



- **Password**



Bios passwords are the first line of defense in ensuring unauthorized access to a system does not occur.

Password generation rules should be established to reflect the sensitivity of the data stored on the system. Consider the following when establishing a BIOS password:

- Several characters in length (longer is stronger)
- Contain one or more spaces
- Contain numbers
- Do not use names, addresses, or other easily guessable words (i.e., password, secret, etc)
- Change passwords regularly

Lenovo ThinkPad BIOS allows the user to set two different passwords:

- Supervisor - This password is normally set and known only to those who have administrative rights for the system. This password allows configuration changes to be made in the BIOS settings that are not allowed under the Power On password.
- Power On – Power On passwords allow the user to boot the system, but limit the configuration changes that can be made. For instance, someone with knowledge of the user password may be able to change the user password, or may be able to add/change a HDD password, but would not be able to change the boot sequence.

The passwords may be independently set. In cases where a Power On Password has been set, but no Supervisor password has been set, the Power On Password functions as the Supervisor password. If there is a Supervisor Password, but no Power On Password, the Supervisor Password must be entered in order to change BIOS settings. However, in this case, the system will boot without the entry of any password. If both

passwords are set, the supervisor Password is always accepted in place of the Power On Password. As a minimum, a Power On Password should be used.

To reduce the possibility of guessing a password, BIOS will halt the boot and require a restart after the wrong password has been entered 3 times.

Passwords should be recorded and securely stored. There is no recovery for a lost BIOS password.

To provide additional security functionality, some ThinkPad systems have the following password related security functions:

- **Lock UEFI BIOS settings:** when enabled, the Supervisor password must be entered to change any BIOS settings. In cases where the user is not the system administrator and it is desirable to not allow the user to alter the system configuration, setting this option along with a Supervisor password that is known only to the administrator protects the system configuration from unauthorized alteration while allowing the user access to boot the system.
- **Password on Restart:** When enabled, BIOS will prompt for a password after a system restart (either user initiated or system crash). By setting this option, protection is provided against circumstances where an unauthorized user can force a reboot by some method (e.g., blue screen) and gain access by booting to an alternate boot device (i.e., bootable USB key).
- **Password on Unattended Boot:** When enabled, this option requires a password to boot if the system is powered on by an external trigger other than the power switch (for instance, a wake up packet received over the network or a real time clock wake event).
- **Password at Boot Device List:** BIOS provide an option to temporarily override the boot sequence and manually select an alternate boot device for this boot. Enabling this option requires the Supervisor Password to be entered to allow booting from the alternate device. Using this option prevents a user from booting to an unauthorized device, while allowing alternate devices to be included in the boot sequence (for instance, a USB key could be included in the boot sequence after the primary boot device to allow the administrator to boot to it for system update/service, but the user could not boot a USB device as long as the primary boot device is present and bootable).
- **Set Minimum Length:** The system administrator may choose to set a minimum password length. Longer passwords are stronger. Any length between 4 and 12 (inclusive) may be chosen for the minimum password length.

- **Password Count Exceeded Error:** Thinkpads implement an interface to allow the system administrator to modify certain BIOS settings from within the operating system (information about this interface can be found at https://support.lenovo.com/us/en/documents/ht100612). Changes made through this interface must be validated by either the Supervisor password (if it has been configured, or the Power On password (if no Supervisor password has been configured). After the password is entered incorrectly 3 times, the BIOS will lock the

capability to change BIOS settings from a utility until after the next reboot. If this option is enabled, BIOS will display an error and require the Supervisor password on the next reboot following a retry count exceeded error.

- **Disk Passwords**

  A drive password may be configured in BIOS on any drive that reports it allows passwords to be set (All modern ATA or SATA disk drives allow for passwords to be set.) Drive passwords are intended to protect the data on the drive, even if the drive is lost or stolen. The ATA standard allows for 2 passwords: user; and master. The user password is intended for use in normal booting of the system; the master password is intended for recovery if the user password is lost.

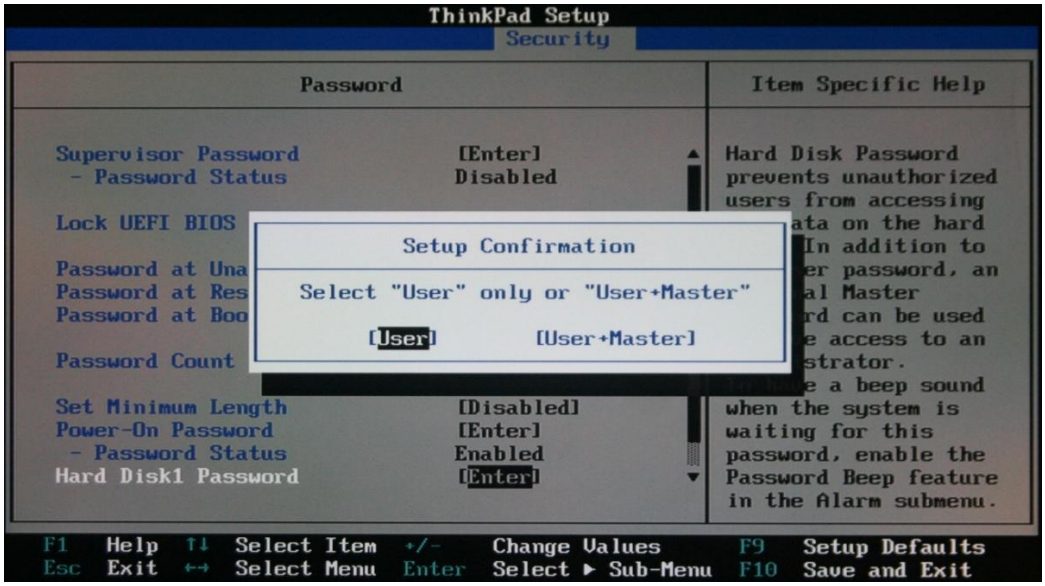
  To configure a drive password, boot the system into BIOS by pressing F1 when the system is booting and select the security screen, then select the password option, followed by the Hard Disk 1 Password option.

  Passwords for disk drives should conform to the same rules as the BIOS passwords. For the convenience of the user, BIOS allows the user to set the same password in the disk drives the same as the BIOS user password. In this case, BIOS will unlock the drive without prompting the user to enter a separate disk password. However, for maximum security, the same password should not used for both the disk drive and for BIOS.

  Verification of the disk password is performed by the drive, not by the system BIOS. Since it is the drive that verifies the password, BIOS only stores the password for use in unlocking the drive when exiting the Sleep (S3) states.

  Using a hard disk password can provide additional security for the data contained on the drive in case the drive is removed and installed in another system. Setting a drive password also enables S3 drive tamper detection. This means that if the system's data connection to the drive is disconnected while the system is in sleep state, the system will automatically reboot and require a password to start.

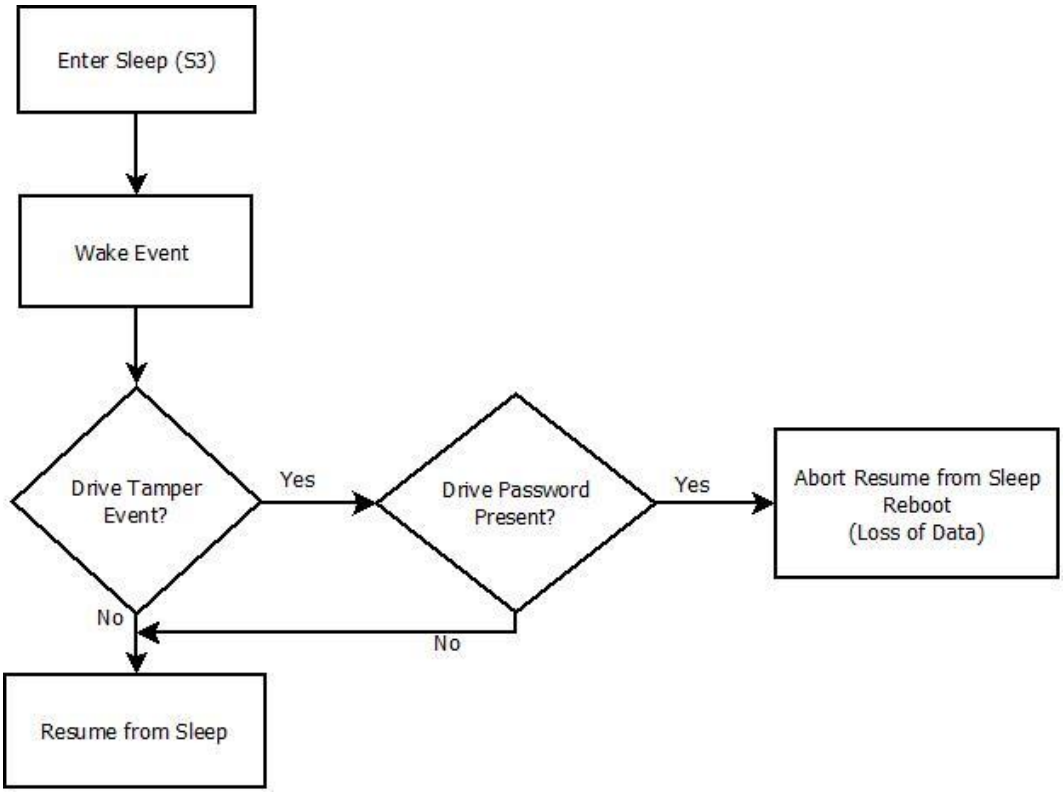
  A Master password may be set at the same time the drive's User password is set. The Master password allows the administrator to unlock the drive if the User password is lost.



The recommendations for generating BIOS passwords, recording and protecting against loss apply to disk passwords as well. There is no recovery method available if the disk passwords are lost.

Self Encrypting Drives (SEDS) or Full Disk Encrypting Drives (FDE)

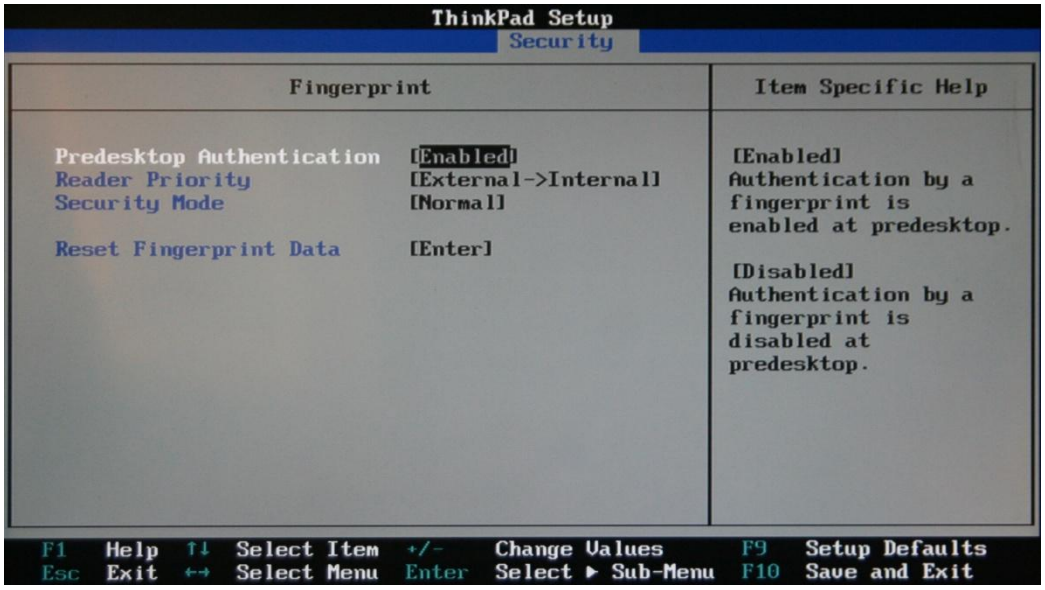
Self Encrypting Drives (SEDs) are a type of disk drive that automatically encrypts the data stored on the drive. The drive's "User password" is used as the key to encrypt the data encryption key; for other drives, the password/encryption key is provided using a protocol defined by the Trusted Computing Group (TCG) (see the discussion about TCG drives later in this section). Since the data is encrypted on the storage medium, these drives have the ability to protect the user's data even if the drive is disassembled to obtain direct access to the storage medium. To increase the data protection, ThinkPads have additional circuitry to detect if the disk drive has been removed during a Sleep state (S3). If the drive is removed and reinstalled during S3, and a disk password has been set via the ATA security feature set interface, BIOS will abort the resume from Sleep, and force a power boot that requires the user to enter the disk password. Note that in this case, any data that was not saved prior to entering the sleep state will be lost.



BIOS process flow for Lenovo ThinkPad S3 sleep state HDD tamper detection

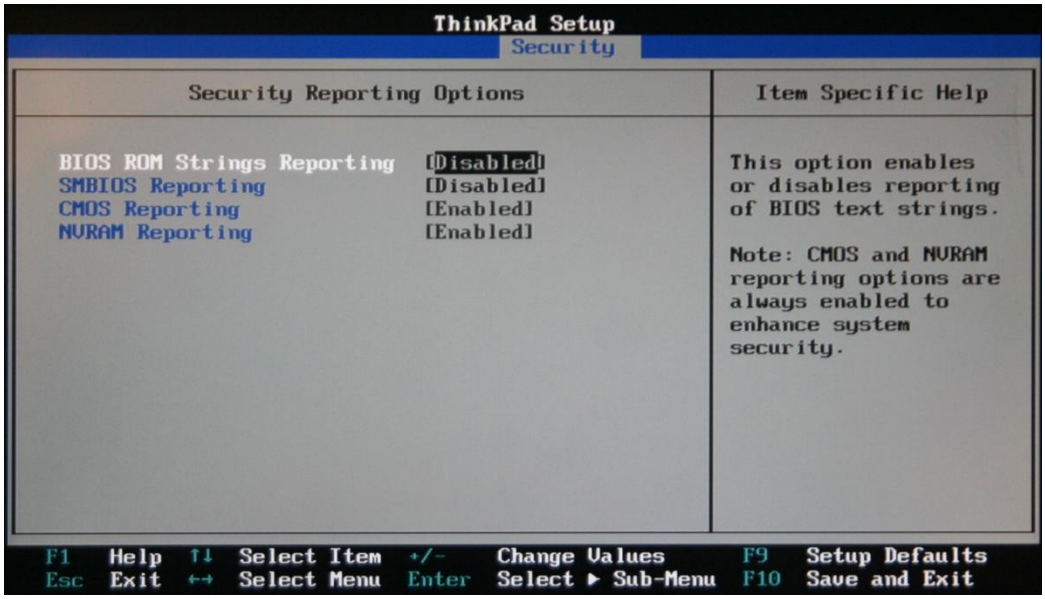
The TCG has established a standard for a class of self encrypting drives that are managed by the system software (these are referred to as OPAL drives). These drives do not report the presence of a password by the usual ATA security feature set interface; therefore BIOS does not manage the security of these drives and will not unlock them. Instead, they are unlocked by system software (e.g., Microsoft BitLocker, WinMagic, etc). Since BIOS does not recognize these drives have a password, BIOS will not detect tampering and will not abort the S3 resume in cases where the drive has been removed/replaced during sleep. Users who wish to ensure that an Opal drive is not tampered during S3 sleep should configure the OS to not allow entry into the S3 sleep state.

- FingerPrint



Some systems provide an integrated fingerprint reader. Fingerprint reader support allows the BIOS passwords, the disk passwords, or the system passwords to be associated with a fingerprint. During boot, the user will be asked to scan a finger over the sensor; after validation, the disk passwords associated with the fingerprint will be released to BIOS to unlock the disk drive. Once the operating system is booted, the fingerprint reader will also authenticate the user to system software, resulting in a single sign on process. To clear the previous owner's fingerprint data, select the Reset FingerPrint Data option.

- Security Chip



The “Security Chip selection” option can be used to enable the Trusted Platform Module (TPM). Lenovo supports the TPM/TCG per the current Trusted Computing Group (TCG) standards (TCG Standards are available at this website: http://www.trustedcomputinggroup.org). The system administrator may enable/disable the TPM function via BIOS setup options.

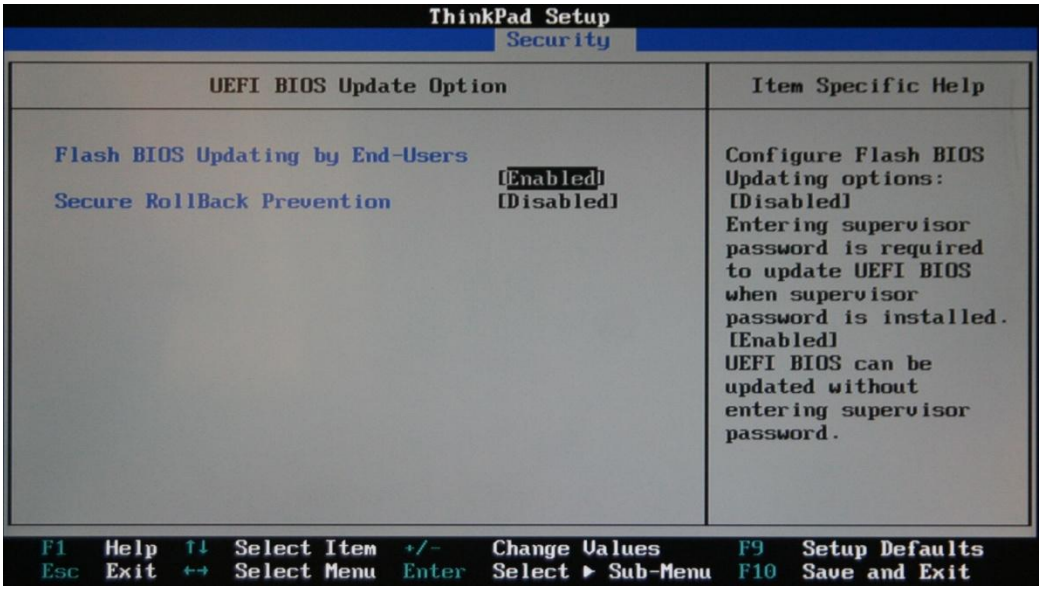
- **Security Chip Selection:** Allows the administrator to select either a TPM 2.0 or a TPM 1.2 security device. Which device should be selected depends on the requirements of the operating system and/or other system software.
- **Security Chip:** The administrator may choose for the security chip to be:
  - **Active:** Fully function and visible to the operating system and system software
  - **Inactive:** Visible to the OS and system software, but not fully functional. (Note this setting is not available if TPM 2.0 is selected.)

- **Disabled:** Not visible and not fully functional.

- **Security Reporting Options:** In addition to enabling or disabling the TPM function, the system administrator may configure optional items to be measured to PCR 1:
  - BIOS Rom Strings
  - SMBIOS
  - CMOS (Measures BIOS Options)
  - NVRAM (Measures BIOS Security Options)

  Enabling these options allows the system software (for example, Microsoft's BitLocker Application) to examine PCR 1 and determine if any changes have been made to system configuration. More information about Microsoft's Bitlocker Application can be found here: http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview. See this website for TCG information: http://www.trustedcomputinggroup.org.
- **Clear Security Chip:** allows administrator to clear any user/owner installed keys and reset the TPM to the default manufacturing state. This function can be used to clear the previous owner's keys to allow a system to be reused.
- **Intel TxT:** "Enabled" allows Intel's TxT technology to be used. See http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html for details about this technology. Intel VTd and TCG must both be "Enabled" before this technology can be Enabled.
- **Physical Presence for Provisioning:** "Disabled" allows the operating system to change the state of the TPM via the TCG defined Physical Presence Interface without operator approval. When "enabled", the user must approve each state change request.
- **Physical Presence for Clear:** "Disabled" allows the operating system to clear all keys and owner installed material from the TPM without operator approval. This function mimics the Clear Security Chip function describes above. "Enabled" requires the user to approve the clear request.

- UEFI BIOS Update Option

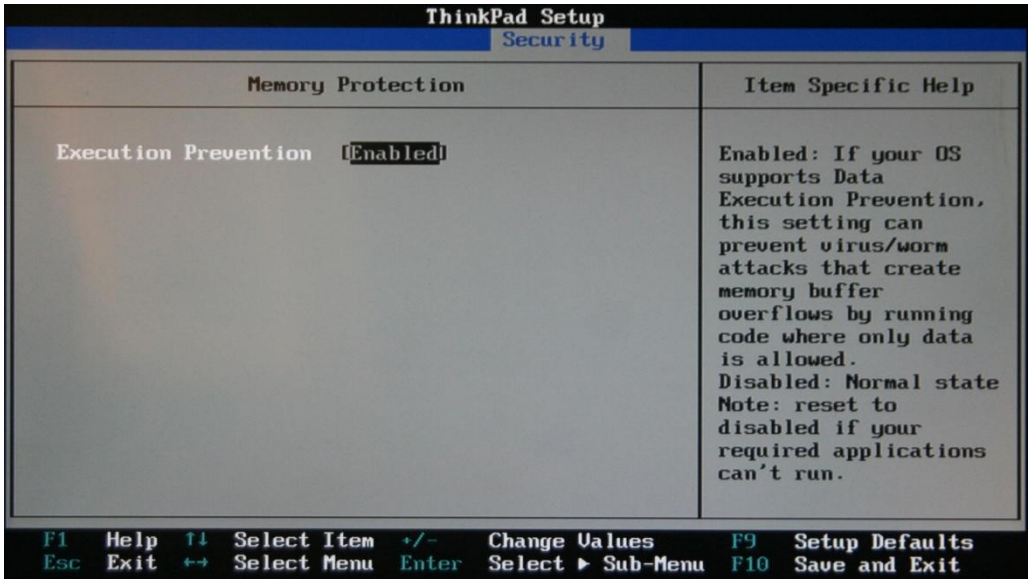


In compliance with the NIST 800-147 standard (http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf), Lenovo BIOS updates use a signed update process. When a BIOS update is requested, the update utility stores the new BIOS image in a UEFI capsule and initiates a special system reboot. On reboot, BIOS detects the pending update request and validates the new image via an RSA 2048 bit signature. After the image is validated, the BIOS in the flash is updated and the system reboots to use the new BIOS. If the validation fails, the update is aborted. In addition to a signed BIOS update, select systems implement Intel's "Boot Guard" technology (to determine if a particular system has "Boot Guard" technology, see the description for that system). This technology validates the part of the BIOS code that is executed first via a RSA 2048 bit signature.

BIOS setup provides several features designed to allow the user to manage the update process:

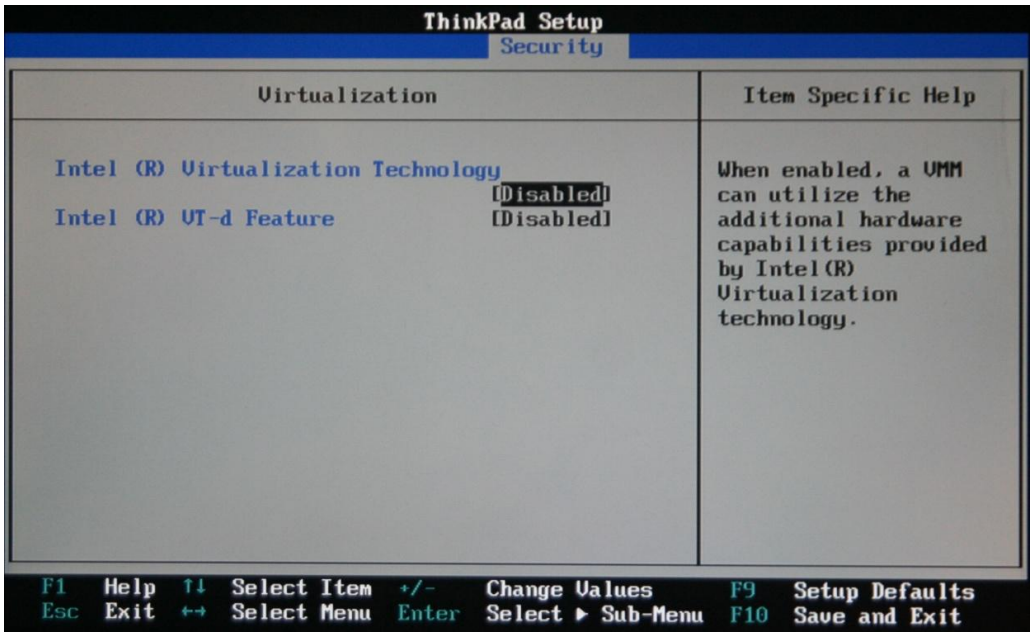
- **Flash BIOS Updating by End-Users:** When "Disabled," this setting BIOS setting requires Administrator/Supervisor password when BIOS update is requested. System administrators may use this setting to prevent user update of BIOS.
- **Secure Rollback Prevention:** When "Enabled," earlier versions of BIOS cannot be installed. NIST 800-147 requires that flashing to previous BIOS not be allowed. However, many organizations have standardized on a "gold" BIOS level that has been validated to meet their requirements. As later systems are added or failed planars are replaced, it is possible for these organizations to obtain a system with a newer BIOS than has been selected as the standard "gold" level. To allow an organization to flash back to the desired BIOS level, this option must be disabled. Once the desired BIOS level has been installed, this option can be re-enabled to prevent rollback to a previous level.

- **Memory Protection**



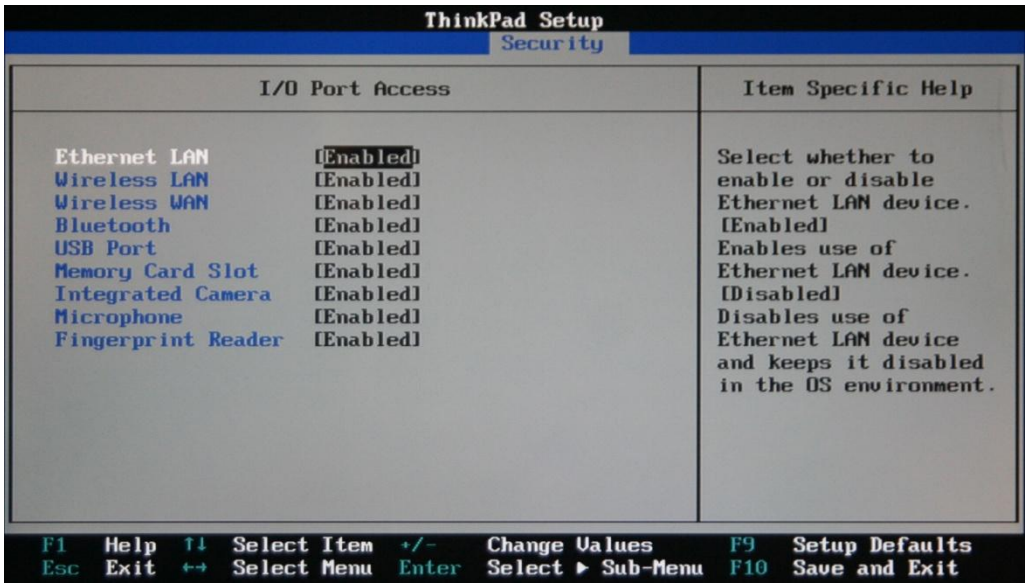
Some operating systems provide function to ensure that memory portions designated as data areas cannot be executed as code. Not allowing code execution from data areas help prevent memory buffer overflow attacks. To enable this protection, set the Execution Prevention setting to ”Enabled.”

- **Virtualization**



Settings on this screen are used to enable Intel's Virtualization Technology and Intel's Virtualization Technology for Directed I/O. See http://www.intel.com/content/www/us/en/virtualization/virtualization-technology/intel-virtualization-technology.html for more information.

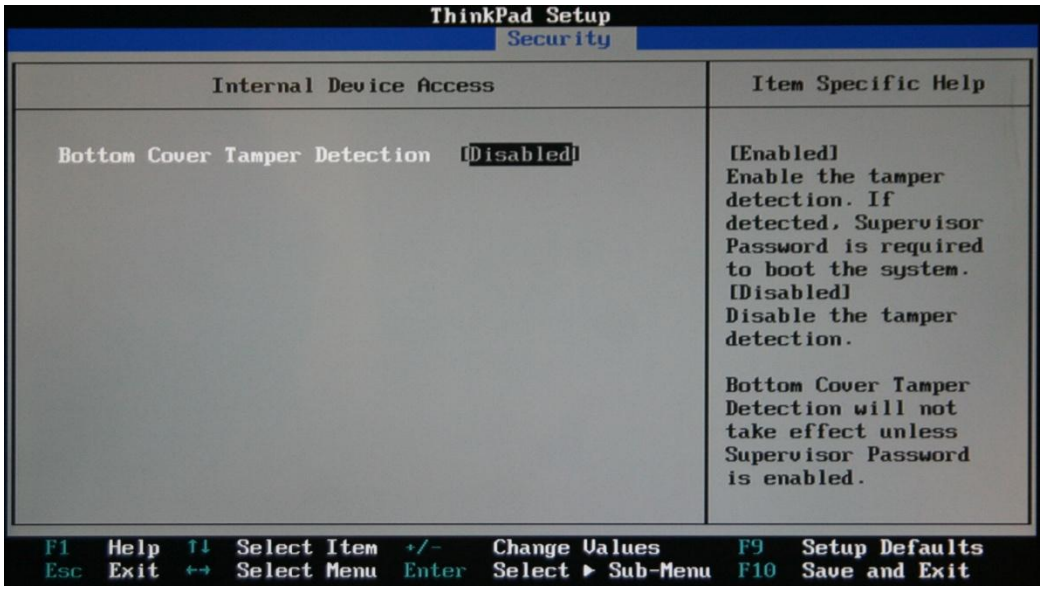
- **I/O Port Access**



Various devices and I/O ports can be enabled or disabled by BIOS settings. Some of the devices that can be controlled include:

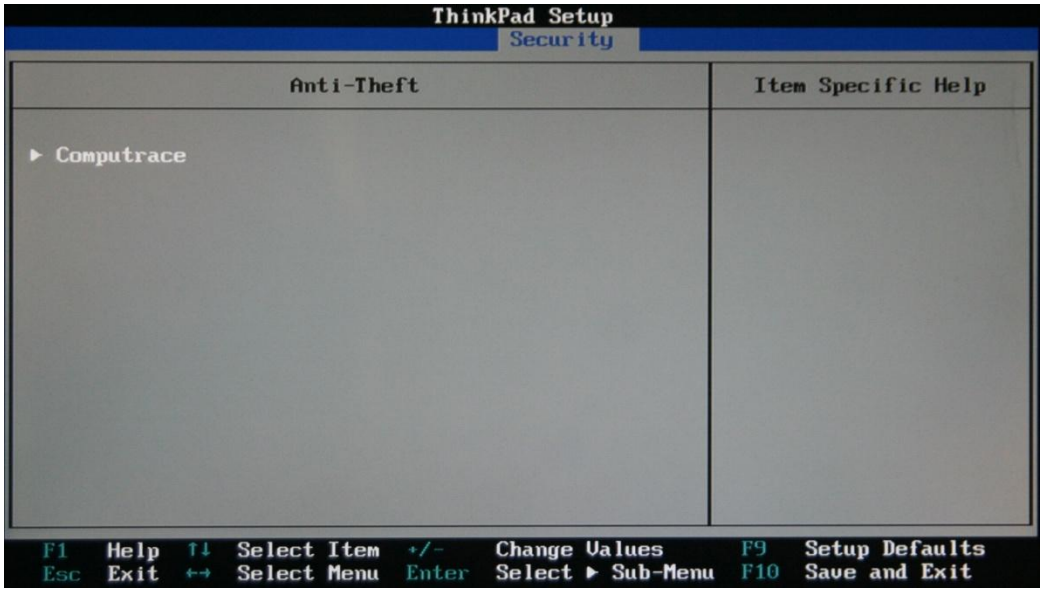
  - USB ports
  - Built in Network adapters
  - Memory card slots
  - Fingerprint reader
  - Microphone
  - Camera

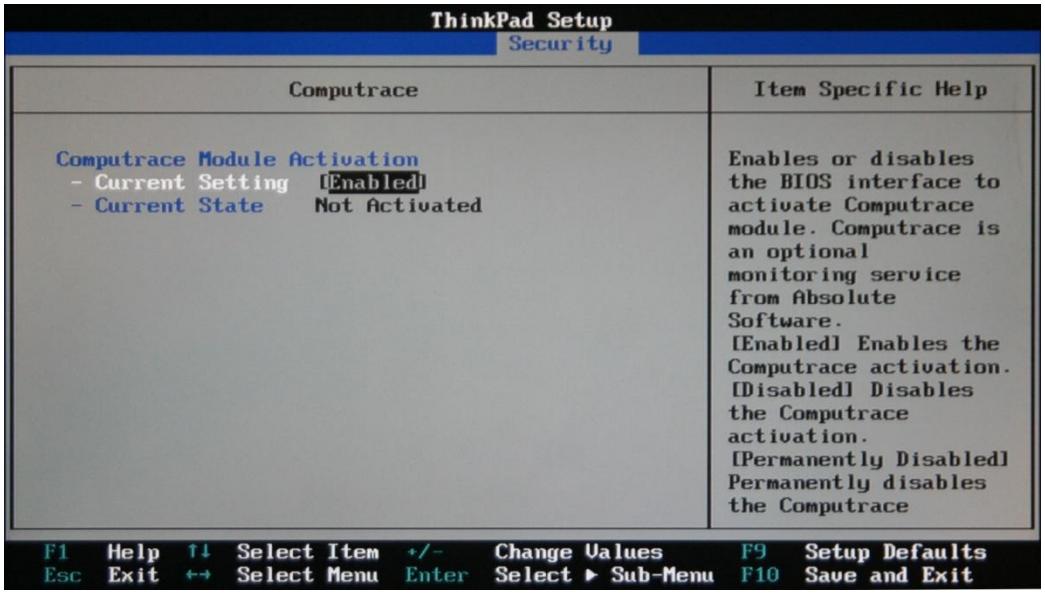
- **Internal Device Access**



Some Lenovo systems have the circuitry to detect when the cover has been removed. Set the Bottom Cover Tamper Detection setting to “Enabled” if tamper detection is desired. Once the reporting of the tamper has been enabled in BIOS setup, during system boot, BIOS will examine the status of the hardware and will report if the cover has been removed at any time since the last power cycle. To enable this feature, the administrator must enable the cover tamper reporting feature in BIOS and establish an administrator/supervisor password. To resume booting and clear this error, the administrator password must be entered at the BIOS password prompt during the boot process.

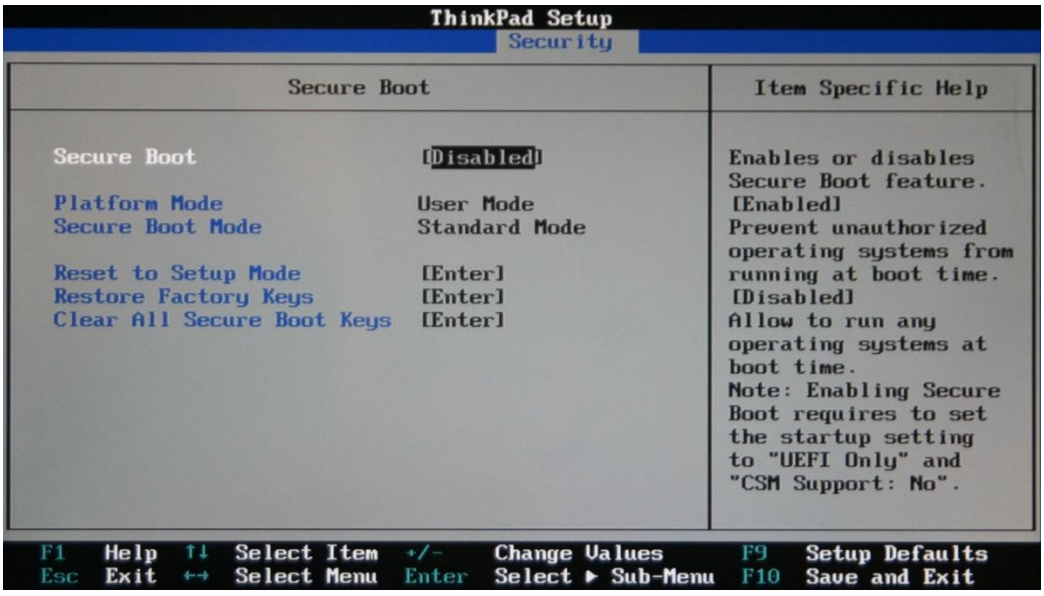
- **Anti-theft**





The settings on this screen enable/disable/permanently disable the Computrace (Absolute's device management service) function within ThinkPad BIOS. More information on the Computrace function may be found at this website: http://shop.lenovo.com/us/en/landing_pages/info/09/computrace

- **Secure Boot**



Lenovo BIOS supports the “UEFI secure boot process”. This means when a system is placed in the secure boot mode, all UEFI BIOS drivers not included in the BIOS image (for example, a UEFI driver loaded from a PCI card or other device installed by a user) and the OS loader are required to be signed with an RSA key that is known to BIOS. The BIOS image provided by Lenovo is preloaded with a set of keys that are appropriate for most situations. However, the system administrator may replace the Lenovo installed keys with other keys if necessary. See the UEFI Secure Boot Specification and the Windows 8.1 Secure Boot Key Creation and Management Guidance for details of installing custom boot keys. These documents may be found at the following websites:

- http://www.uefi.org/sites/default/files/resources/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf https://technet.microsoft.com/en-us/library/dn747883.aspx

System administrators may have to disable Secure Boot in the following conditions.

- If the OS loader is not signed by keys known to BIOS, the system will prevent loading such OS loader. So, if the system administrator must boot with Windows 7 or legacy operating systems, Secure Boot must be disabled in BIOS.
- When Secure Boot is enabled, Windows operating systems may prevent loading the kernel-mode drivers that are not certified by Microsoft. In order to allow using such Windows driver for some specific hardware, Secure Boot must be disabled in BIOS.

Lenovo systems are manufactured with the default Secure Boot signature database which allows running UEFI programs certified by Microsoft or by Lenovo. The program includes the following UEFI executable images.

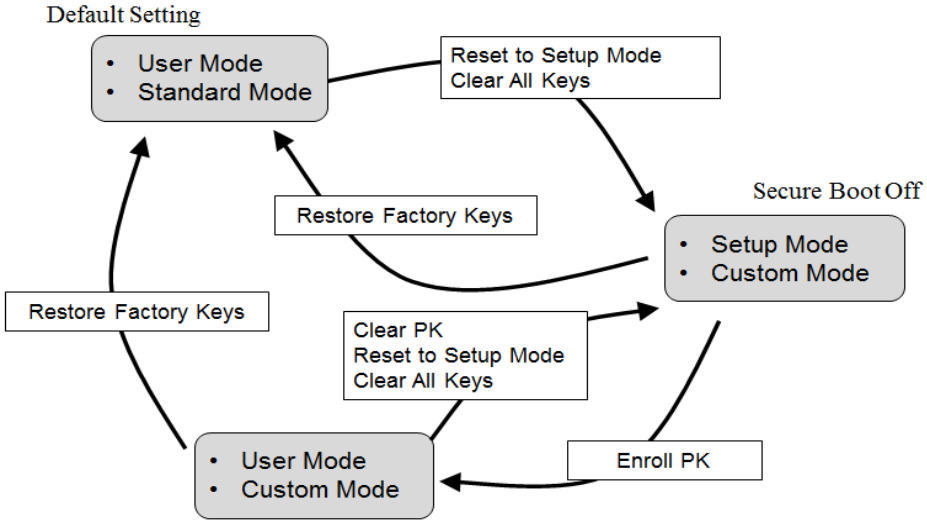
- Windows OS loader
- BIOS update utility
- Lenovo hardware maintenance utility
- Lenovo drive erase utility
- Lenovo hardware diagnostic utility
- Firmware update utility for optical drive

The system administrator may modify this default Secure Boot database to load own UEFI programs or UEFI drivers that are signed by custom key. So, Lenovo BIOS provides some options to change the Secure Boot database for such purpose.

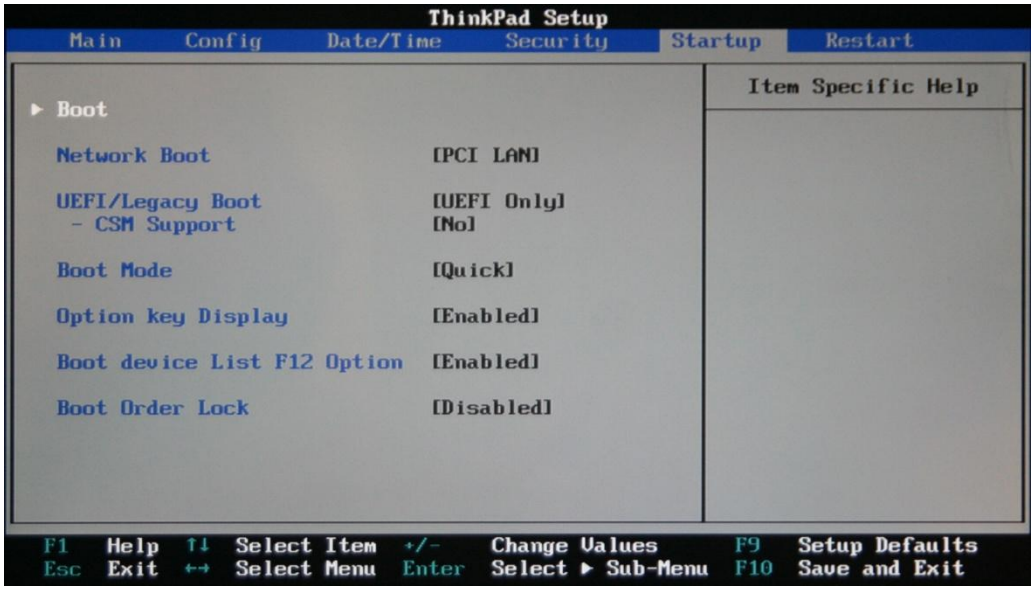
The system administrator can manage the Secure Boot configuration via following BIOS setup options.

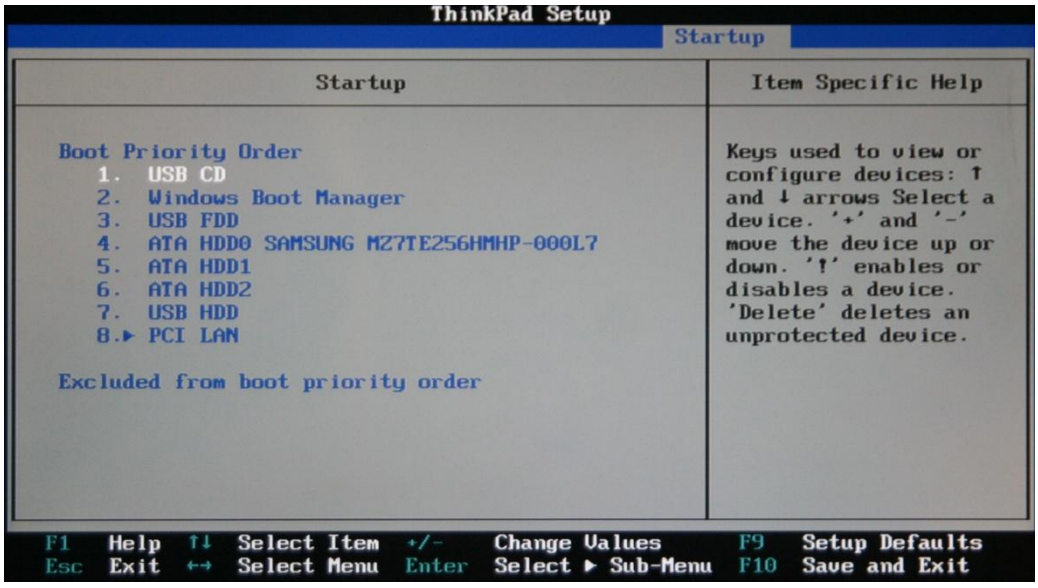
- **Secure Boot:** The system administrator can enable or disable Secure Boot depending on the operating system type. Secure Boot option is enabled by default on the systems that were manufactured with Windows 8 or later Windows. If the system was manufactured with Windows 7 and it was upgraded to Windows 8 or later Windows, Secure Boot can be enabled with this option. Since Secure Boot works with UEFI boot, BIOS boot mode is always set to "UEFI Only" mode with Secure Boot enabled. So, Secure Boot must be disabled in order to select the "Legacy Boot" mode in BIOS setup option.
- **Platform Mode:** This option indicates the current Platform Mode. When Platform Mode is "User Mode", PK (Platform Key) is enrolled in the Secure Boot database. When in "Setup Mode", the PK is not enrolled and so the Secure Boot database is accessible to replace keys. BIOS does not attempt Secure Boot if Platform Mode is set to "Setup Mode".
- **Secure Boot Mode:** This option indicates the current condition of Secure Boot database. When Secure Boot Mode is "Standard Mode", the Secure Boot database is factory default setting. When "Custom Mode", the Secure Boot database is modified from default setting in order to allow loading the UEFI images that are signed by custom keys.
- **Reset to Setup Mode:** This option is used to clear the current PK and put the system into setup mode. The system administrator can install own PK in the Secure Boot database after selecting this option.
- **Restore Factory Keys:** This option is used to restore all keys in the Secure Boot database to factory defaults. Any customized Secure Boot settings will be erased, and the default PK will be re-established along with the original keys provided by Microsoft/Lenovo.
- **Clear All Secure Boot Keys:** This option is used to clear all keys in the Secure Boot database. The system administrator can install own keys in the Secure Boot database after selecting this option.

The following figure illustrates the Secure Boot mode transition.



❖ Startup screen



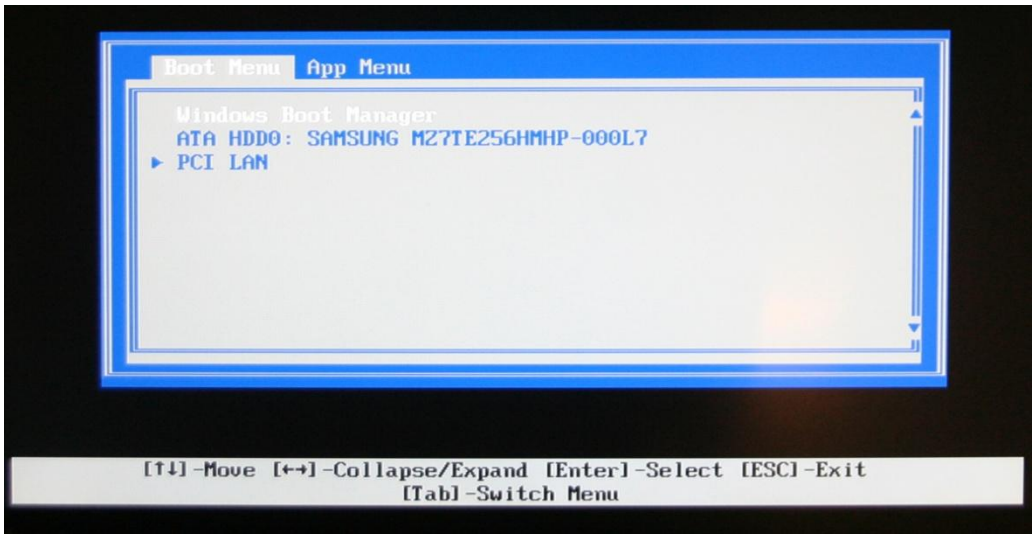


- **Boot**

  Boot sequences within the system BIOS allow the system administrator to be able to limit the sources from which a system can boot with Boot Order Lock. The following example illustrates how this feature can be used to prevent unauthorized access. Without limiting the boot sequence, it is possible to gain unauthorized access by inserting a bootable USB key in a USB slot and forcing a system reboot. Upon reboot, the attacker can select to boot to the key that was just inserted. Once the system has booted, the attacker can read the data from the system's drive.

- **Boot Device List F12**

This option enables/disables the Boot override popup selection. When “Enabled,” pressing F12 during POST will cause a pop up with the devices in the boot list to be displayed. From the popup, the user can select any device from the boot order to be boot instead of the normal device.



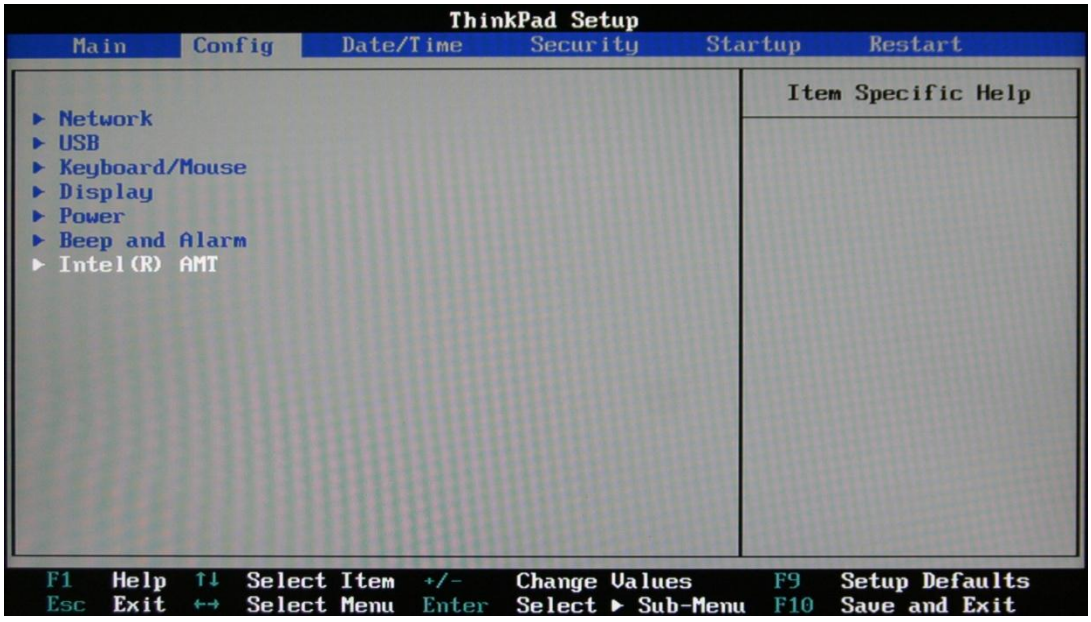
When disabled, the popup menu is disabled, preventing the selection of an alternate boot device.

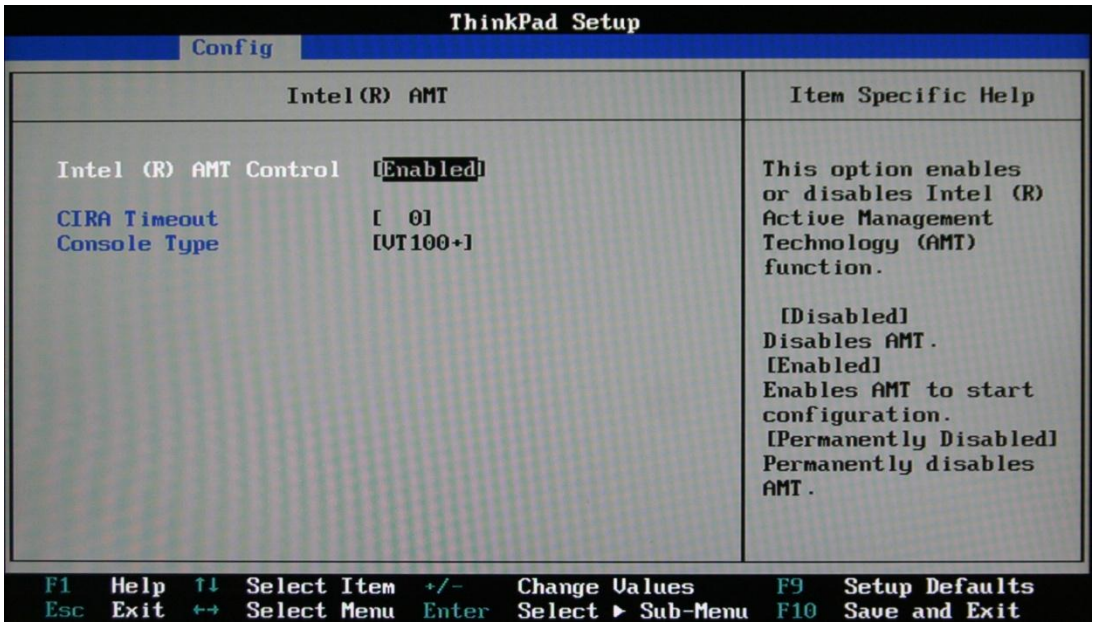
- **Boot Order Lock**

Some administrator may want to limit the sources from which a system can boot. Set this item to “Enabled” to protect the write access to UEFI variables of BootOrder and Boot Options.

.

❖ AMT





Use this screen to “Enable” or “Disable” Intel’s AMT. For users who have systems with the option of using AMT, but do not desire to use AMT, the following is recommended:

- Remote Provisioning of Intel AMT computer systems into Admin Control Mode. Refer to Intel Setup and Configuration User Guide for instructions (http://www.intel.com/content/dam/www/public/us/en/documents/guides/vpro-setup-and-configuration-guide-for-intel-vpro-technology-based-pcs-guide.pdf).
- Local MEBX password change using a USB memory stick. Refer to Intel Setup and Configuration User Guide for instructions

(http://www.intel.com/content/dam/www/public/us/en/documents/guides/vpro-setup-and-configuration-guide-for-intel-vpro-technology-based-pcs-guide.pdf .

- Local MEBX password change using the Management Engine BIOS Extension (MEBX). Refer to Intel Setup and Configuration User's Guide for instructions http://www.intel.com/content/dam/www/public/us/en/documents/guides/vpro-setup-and-configuration-guide-for-intel-vpro-technology-based-pcs-guide.pdf).