



Kon Boot Help Guide

Table of Content

1. Getting started

1.1	Introduction	page 2
1.2	Content	page 3
1.3	System requirements	page 4
1.4	Kon Boot Compatibility	page 5
1.5	How it works	page 6

2. Installing Kon Boot

2.1	How to make a Kon Boot USB flash drive	page 7
2.2	How to make a Kon Boot CD	page 8

3. Using Kon Boot

3.1	Inserting and enabling media	page 9
3.2	Kon Boot Logon	page 11
3.3	Privilege escalation	page 12
3.4	Using Kon Boot with VmWare	page 14
3.5	Resetting passwords and adding accounts	page 19

4.	Kon Boot FAQ	page 30
----	--------------------	---------

1.1 Introduction

Thank you for choosing Kon Boot. t

Kon Boot is an application which will bypass the authentication process of Windows based operating systems.

Kon Boot can work on a USB flash drive, CD, or floppy diskette.

Using Kon Boot is simple. First load it to your desired media (CD, USB drive, or floppy diskette) then insert it into the target computer, and start it up!

1.2 Content

Filename	Description
konFLOPPY.img	Floppy & USB image file of Kon Boot
konCD.iso	ISO image of Kon Boot
KonBootCDInstallGuide.pdf	Install guide for konCD.iso
KonBootUSBGuide.pdf	Install guide for konUSB
KonBootInstall.exe	Frontend for USB installation
menu.lst	Drive mapping instruction for Grub
grubinst.exe	Formats USB disk with grub MBR
grldr	GRUB for DOS universal boot loader
COPYING	GPL v3 License for grub files

1.3 System requirements

Recommended Minimum Hardware:

Intel Pentium III processor (or compatible) 128 MB RAM or greater

Operating Systems:

Microsoft Windows XP Home Edition (Service Pack 2+)

Microsoft Windows Vista Home Basic (32/64 bit)

Microsoft Windows Vista Home Premium (32/64 bit)

Microsoft Windows Vista Business (32/64 bit)

Microsoft Windows Vista Enterprise (32/64 bit)

Microsoft Windows 7 Home Premium (32/64 Bit)

Microsoft Windows 7 Professional (32/64 Bit)

Microsoft Windows 7 Ultimate (32/64 Bit)

Microsoft Windows Server 2003 Standard (32/64bit)

Microsoft Windows Server 2003 Datacenter (32/64bit)

Microsoft Windows Server 2003 Enterprise (32/64bit)

Microsoft Windows Server 2003 Web Edition (32/64bit)

Microsoft Windows Server 2008 Standard (32/64bit)

Microsoft Windows Server 2008 Datacenter (32/64bit)

Microsoft Windows Server 2008 Enterprise (32/64bit)

Technology Requires:

10MB free space on the hard drive. CD-ROM (for installation of the program from CD) or Floppy Drive or USB flash drive; computer mouse; keyboard; Internet connection (for product download);

1.4 Kon Boot Compatibility

Kon Boot will work with the following operating systems.

Microsoft Windows XP Home Edition (Service Pack 2+)
Microsoft Windows Vista Home Basic (32/64 bit)
Microsoft Windows Vista Home Premium (32/64 bit)
Microsoft Windows Vista Business (32/64 bit)
Microsoft Windows Vista Enterprise (32/64 bit)
Microsoft Windows 7 Home Premium (32/64 Bit)
Microsoft Windows 7 Professional (32/64 Bit)
Microsoft Windows 7 Ultimate (32/64 Bit)
Microsoft Windows Server 2003 Standard (32/64bit)
Microsoft Windows Server 2003 Datacenter (32/64bit)
Microsoft Windows Server 2003 Enterprise (32/64bit)
Microsoft Windows Server 2003 Web Edition (32/64bit)
Microsoft Windows Server 2008 Standard (32/64bit)
Microsoft Windows Server 2008 Datacenter (32/64bit)
Microsoft Windows Server 2008 Enterprise (32/64bit)

Hardware:

Intel Pentium III processor (or compatible) and greater

*Kon Boot may not work on all PC's due to different motherboard BIOS issues.

1.5 How it works

Kon Boot boots from external media such as floppy, CD, or USB removable drives. When a PC running Windows is started with Kon Boot, the BIOS of the PC will then be hooked by Kon Boot.

After hooking the BIOS, Kon Boot will modify the Windows kernel to allow a user to bypass the step of Windows authentication procedure during Windows Logon.

The changes made to the Windows kernel are temporary only. Rebooting the PC will restore the functionality of the Windows kernel and its corresponding authentication procedures.

2.1 How to make a Kon Boot USB flash drive

Locate KonBootInstall utility in the following directory:

KonBootv1.1\KONUSB\KonBootInstall.exe

- Insert a USB thumb or flash drive into your PC
- Run KonBootInstall.exe

Please note: On Windows Vista or newer, you will need to right click on the executable and “Run as Administrator”

- Installation is complete!

See KonBootUSBGuide.pdf for additional help.

2.2 How to make a Kon Boot CD

Locate konCD.iso in the following directory:

KonBootv1.1\KONCD\konCD.iso

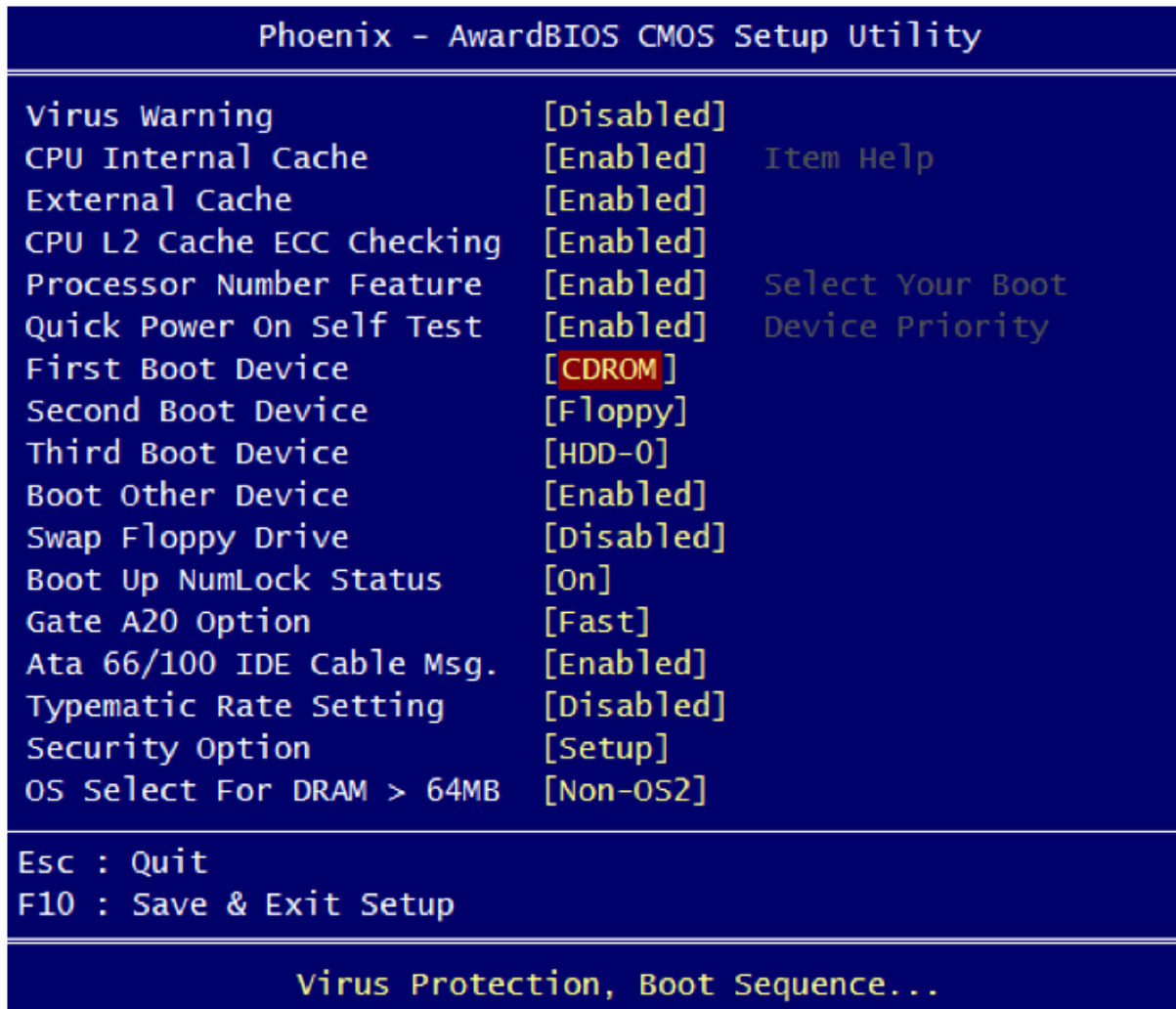
- Insert a blank recordable CD into your CD-RW/DVD-RW drive
- Launch your preferred CD Burning application
- Find and select burn image/iso option
- Installation is complete!

See KonBootUSBGuide.pdf for additional help.

3.1 Inserting and enabling media

- Power on the target PC to use Kon Boot on.
- Enter the BIOS of the PC. This procedure varies depending on the model of your computer. Common keys to enter the BIOS during startup are: F1, F2, DEL, F12. The BIOS generally will indicate the letter key needed to enter the BIOS during the initial seconds of powering on the PC.
- Set the first “Boot Device” or “Boot Priority” to CDROM if you are using Kon Boot CD. If you are using a USB removable drive (flash drive), set the “Boot Device” or “Boot Priority” to USB-HDD or the USB device if given. This procedure also varies depending on the model of the PC. Generally, the boot device priority can be found in Advanced Peripherals section of the BIOS.

Please note: If you are using a USB hub with multiple USB devices, ensure you have selected the corresponding device in the BIOS as well as the particular hub entry.



Example: BIOS of a PC

Consult your motherboard manual for specific instructions.

If the BIOS on your motherboard will not support the USB boot option, we suggest using Kon Boot CD or Floppy.

3.2 Kon Boot Logon

After Kon Boot screen has executed and Windows reaches the logon screen, simply select your desired username and login without any password present.

The password will be bypassed.

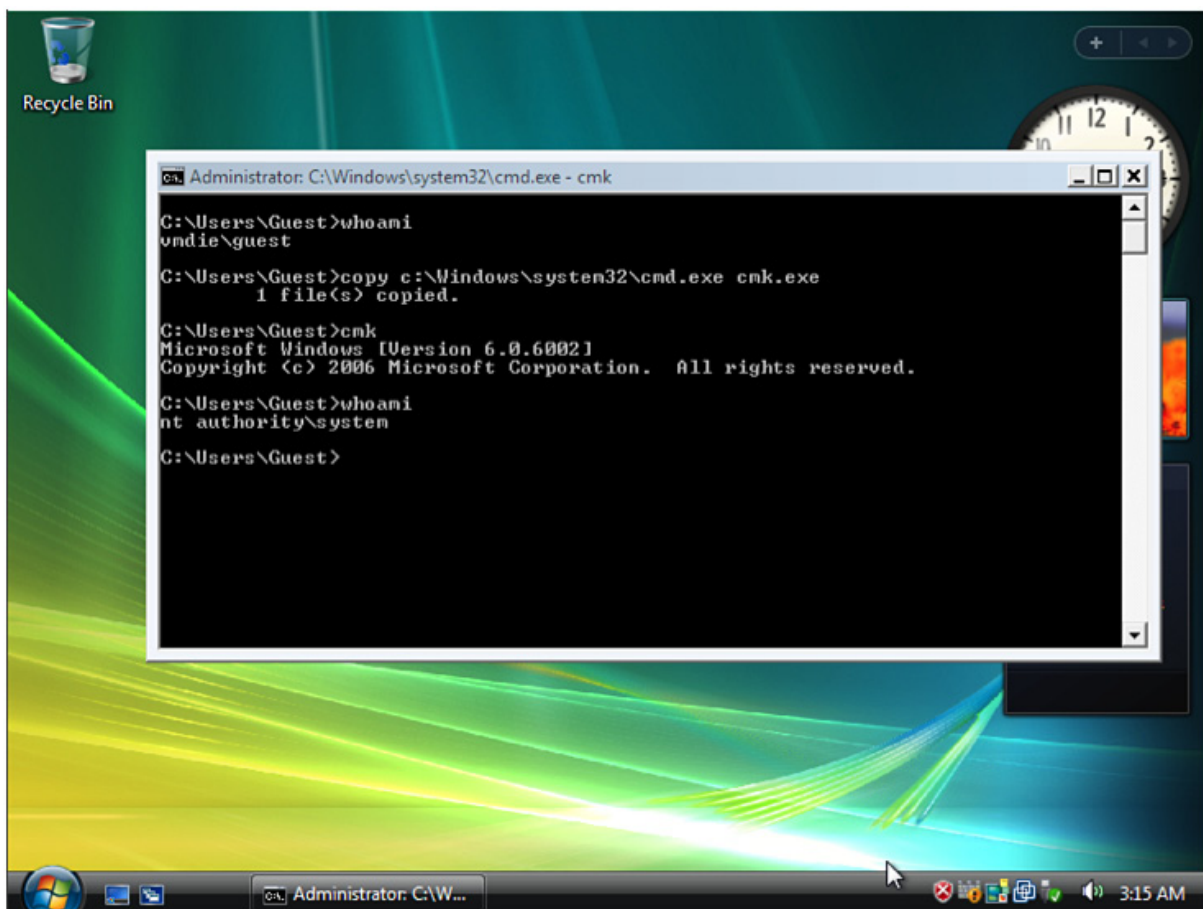
If the username field is blank, it must be typed in manually.
Typical default usernames are Guest and Administrator.

Please note:

Kon Boot will not work on network domains unless the username is cached locally.

3.3 Privilege escalation

- Log to any user account
- Run start → execute → cmd.exe
- In cmd.exe: copy c:\windows\system32\cmd.exe cmk.exe
- in cmd.exe: cmk
- in cmd.exe: whoami (you should have SYSTEM rights)



Example: cmd.exe with the commands above

To delete cmk.exe from the system

- Exit cmk by typing "Exit"
- Execute the command "del cmk.exe"
- cmk is now removed



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Guest>cmk
The system cannot find message text for message number 0x2350 in the message file for Application.

Copyright (c) 2009 Microsoft Corporation. All rights reserved.
The system cannot find message text for message number 0x8 in the message file for System.

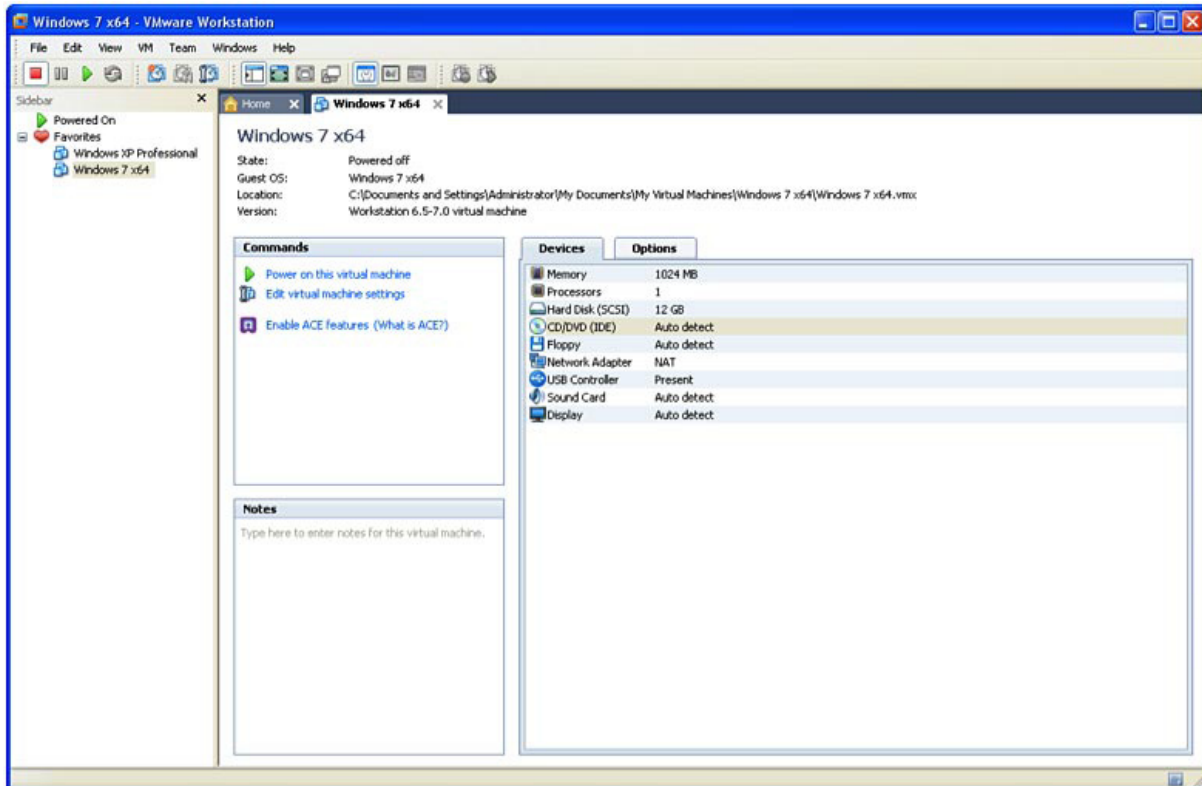
C:\Users\Guest>whoami
nt authority\system

C:\Users\Guest>exit

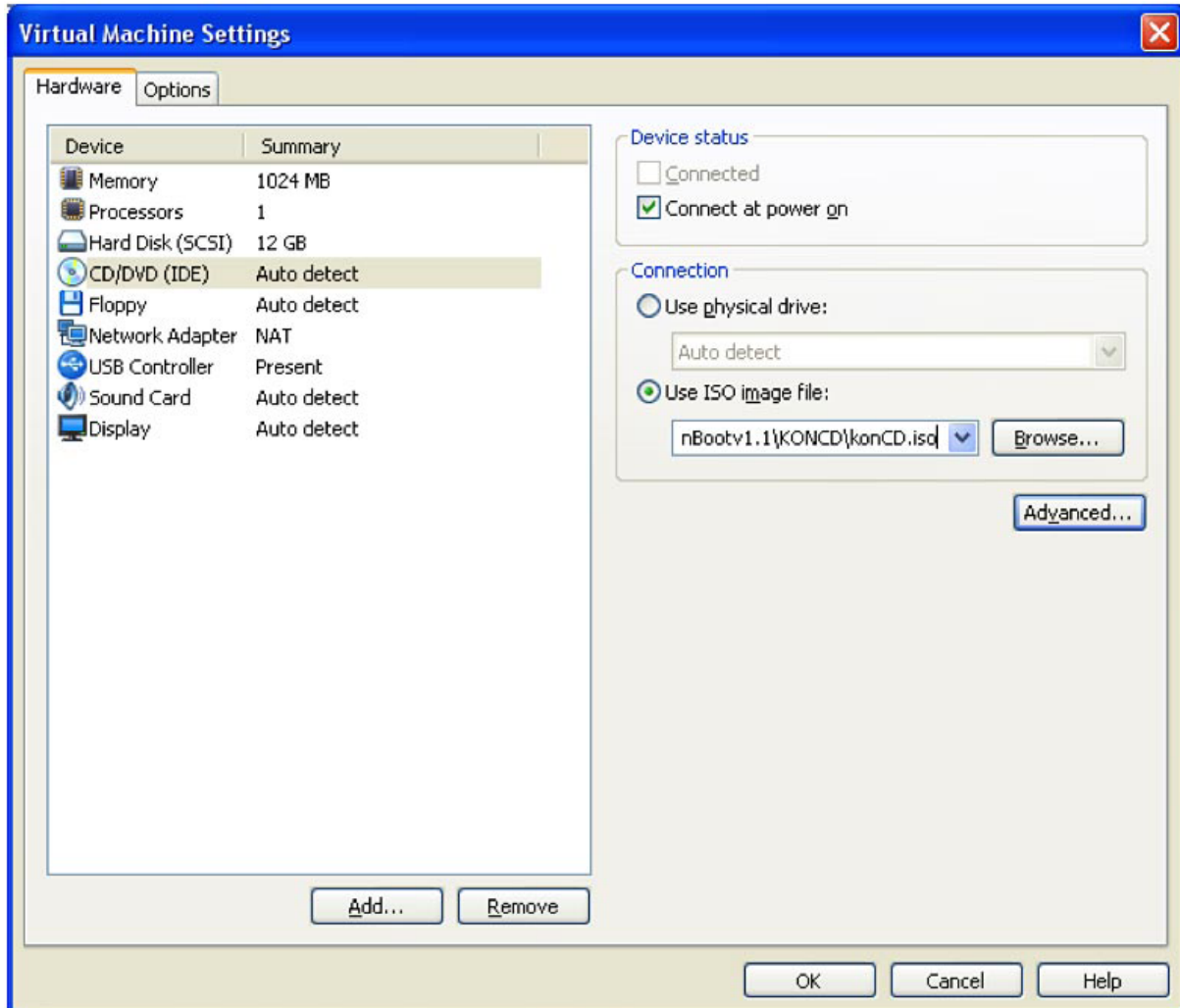
C:\Users\Guest>del cmk.exe

C:\Users\Guest>_
```

3.4 Using Kon Boot with VmWare



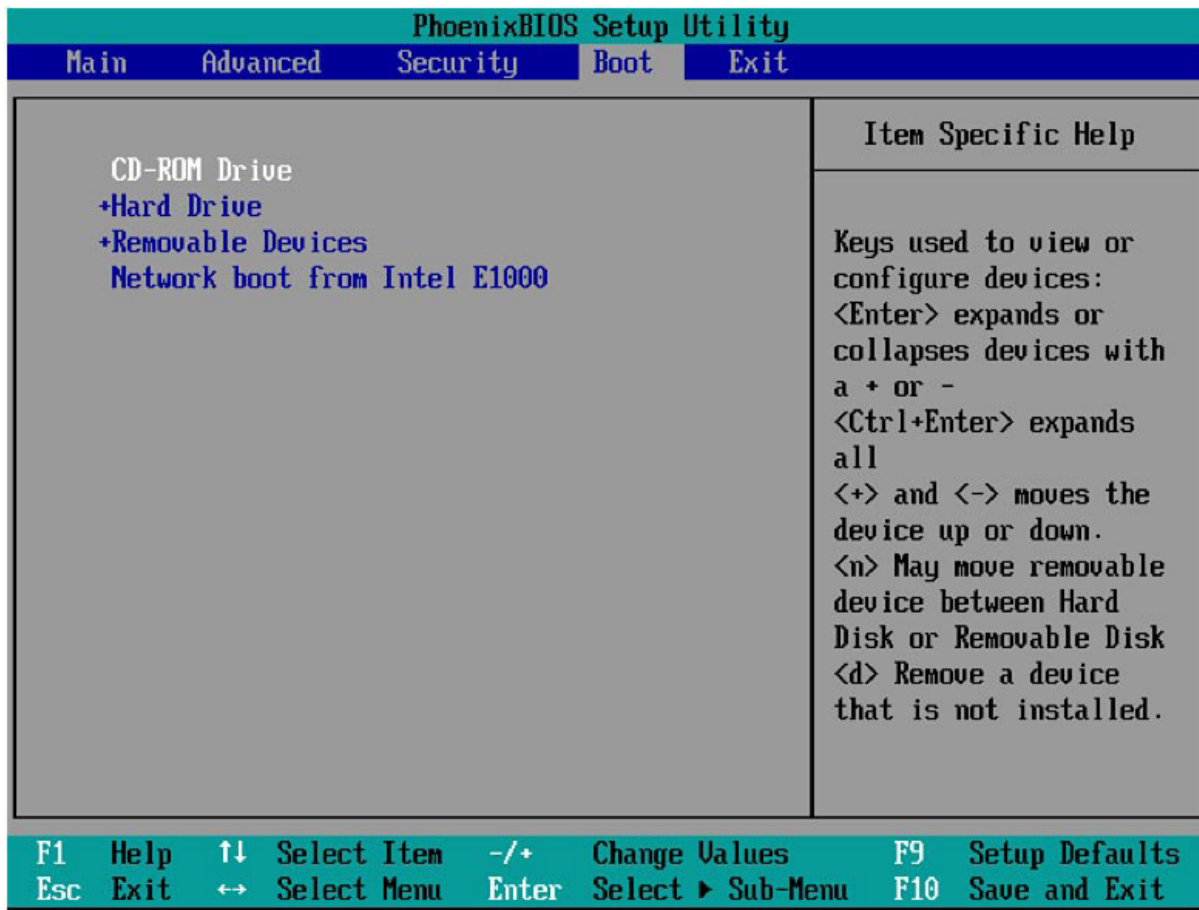
- Double click your CD/DVD (IDE) device.



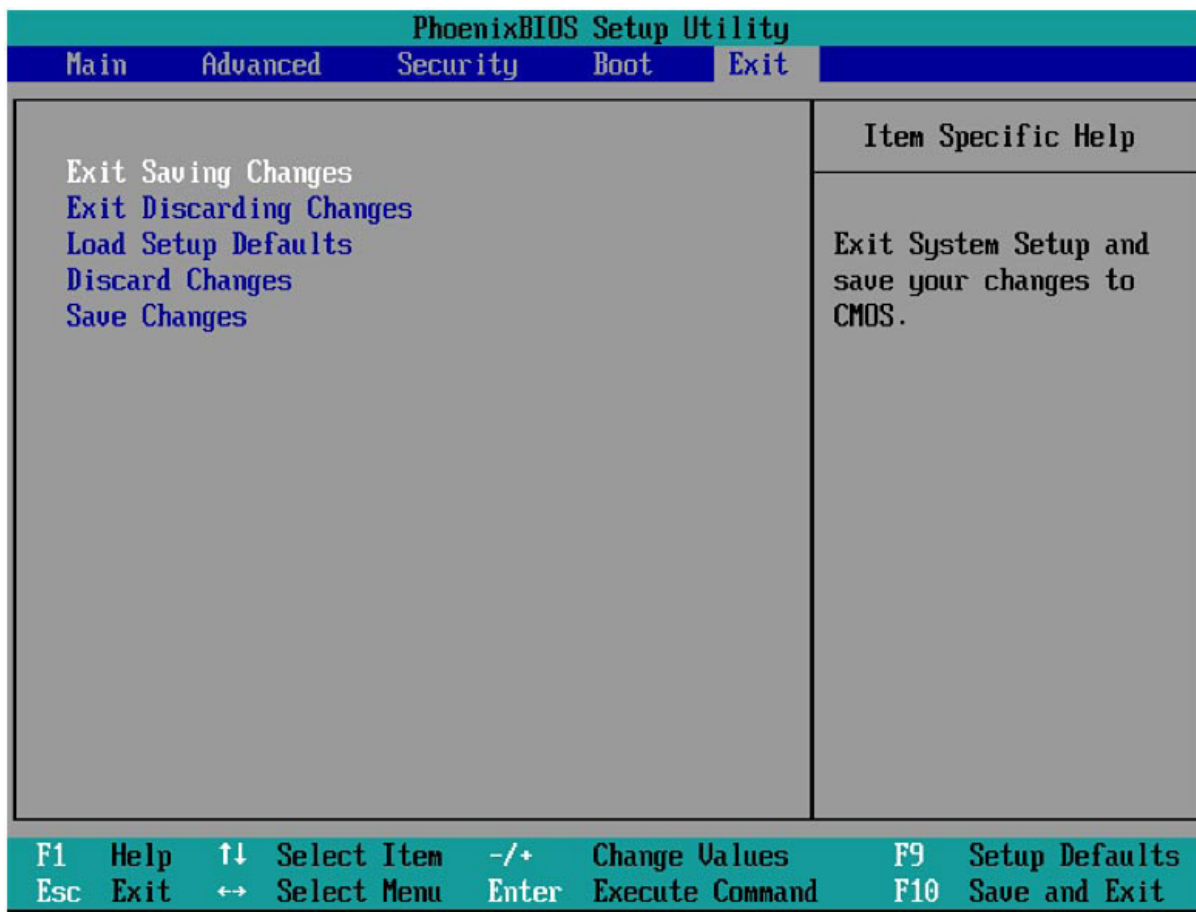
- Enable “Connect at power on” and browse the “Use ISO image file” option to konCD.iso
- Click OK.



- Press the F2 key during VMware BIOS screen



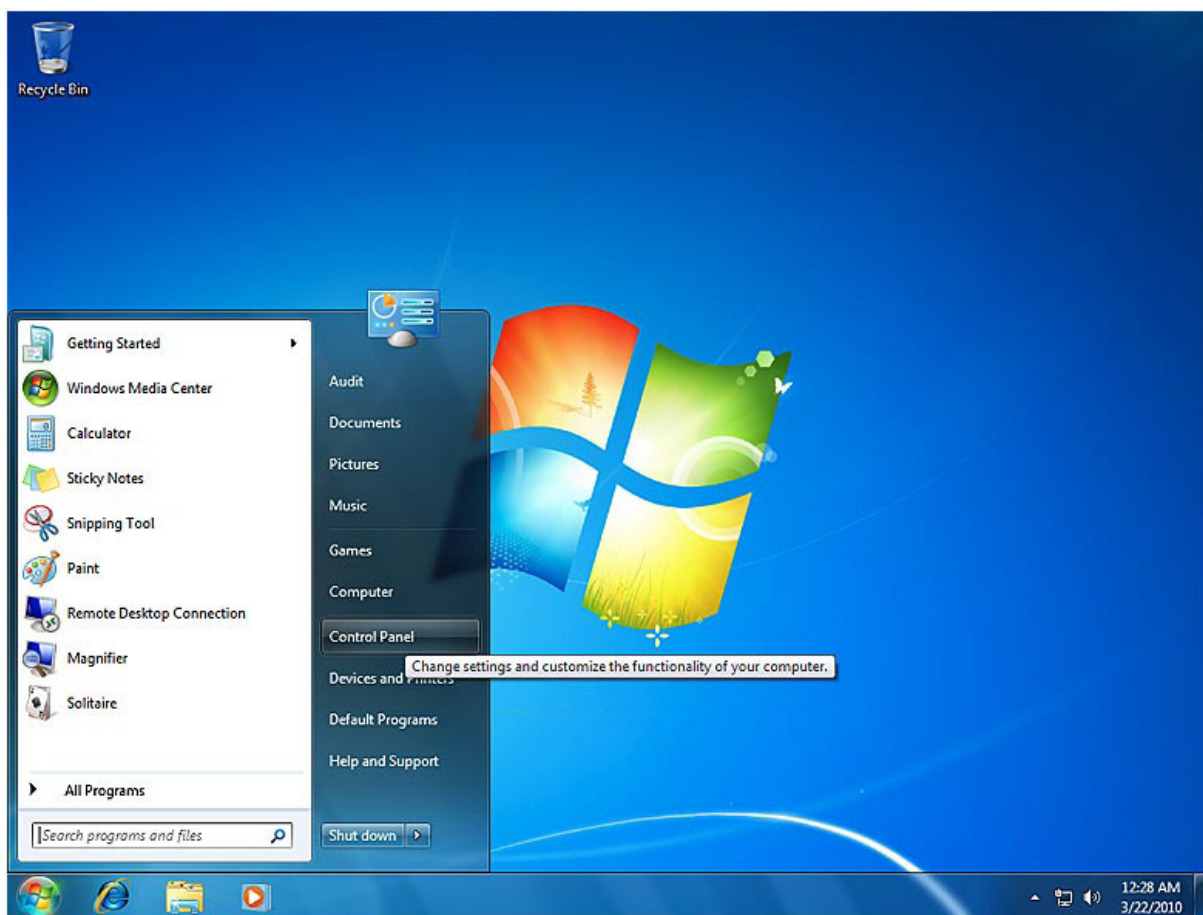
- Set the first drive to CD-ROM Drive.
- Exit and save your changes.



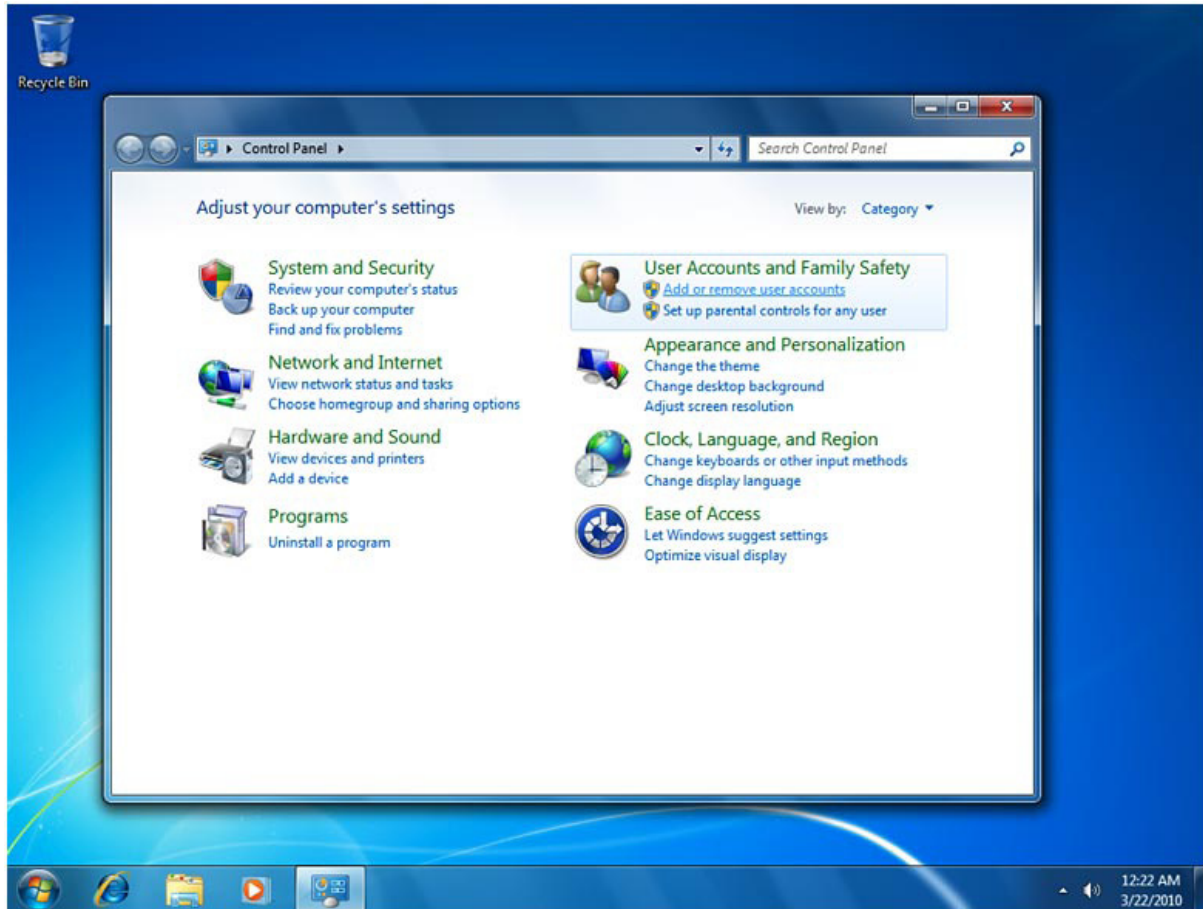
- KonBoot is now enabled for VMWare.

3.5 Resetting passwords and adding accounts

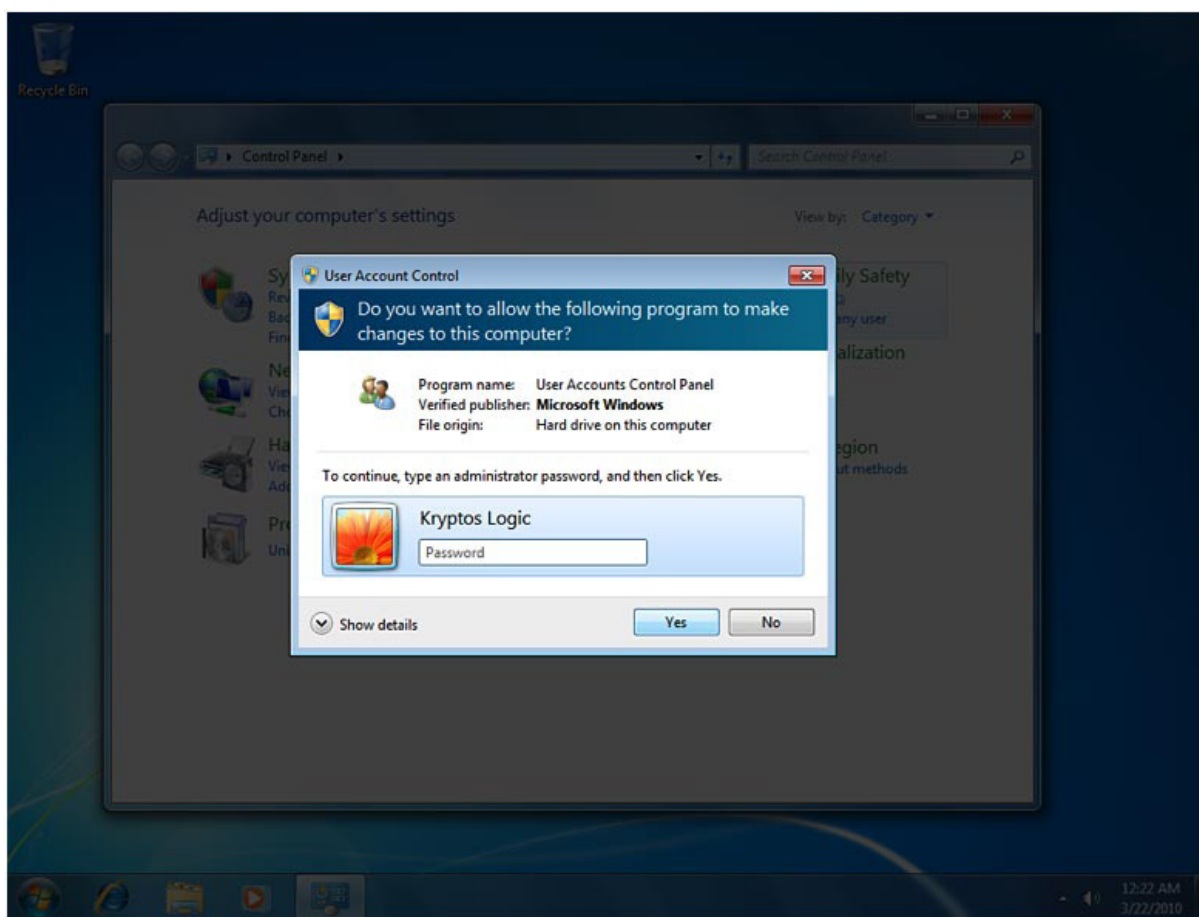
- Start computer with Kon Boot.
- Logon to Windows and choose any account. In this example, we use Guest.



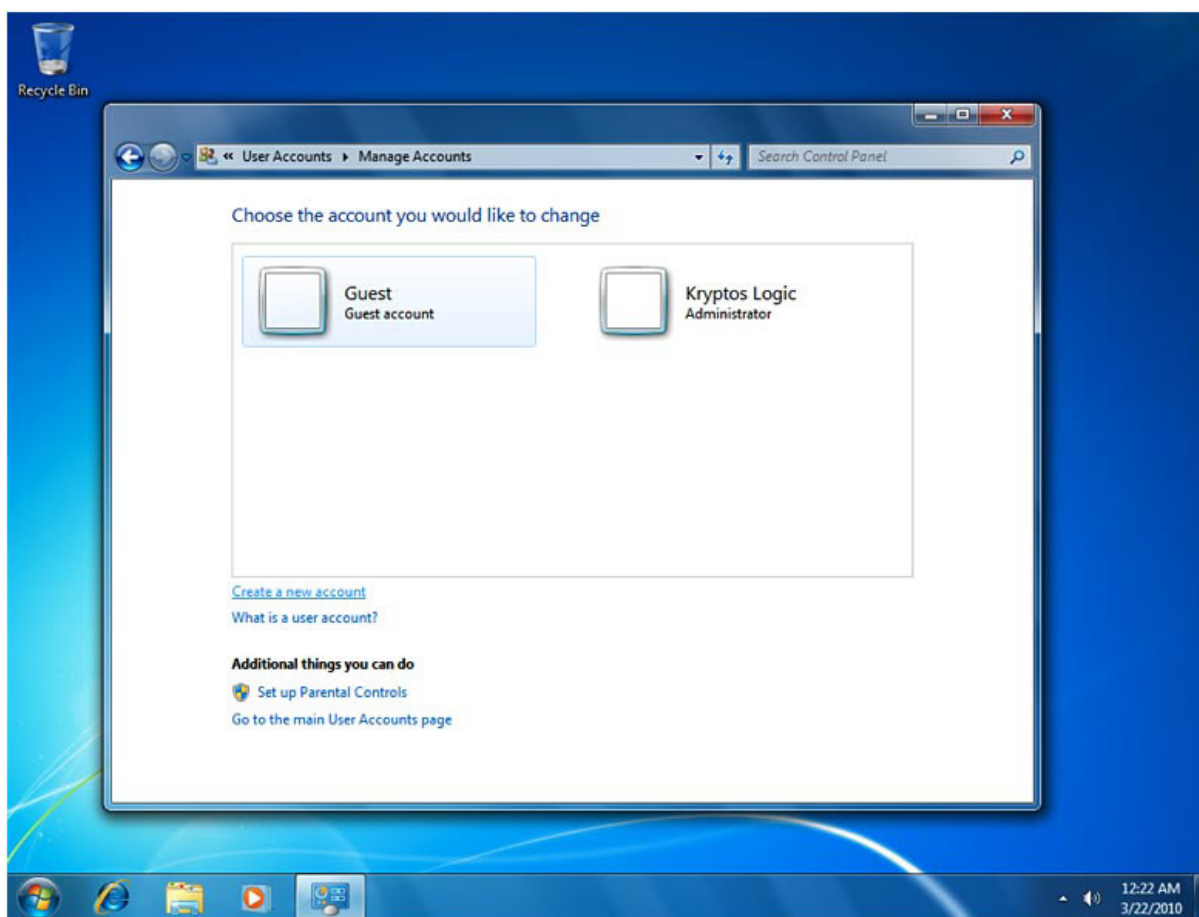
- Navigate the Start Menu to Control Panel



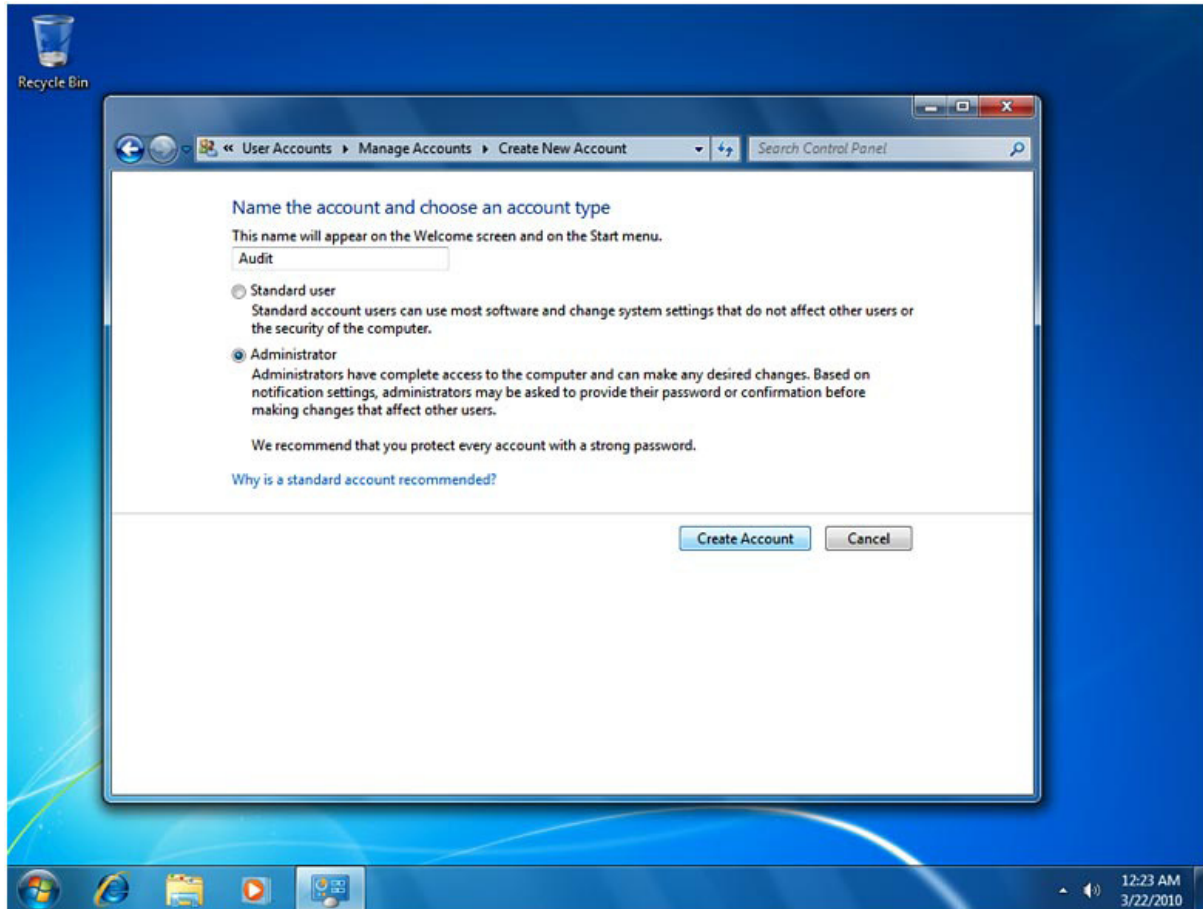
- Select “User Accounts and Family Safety”



- Click “Yes” and leave the password field empty



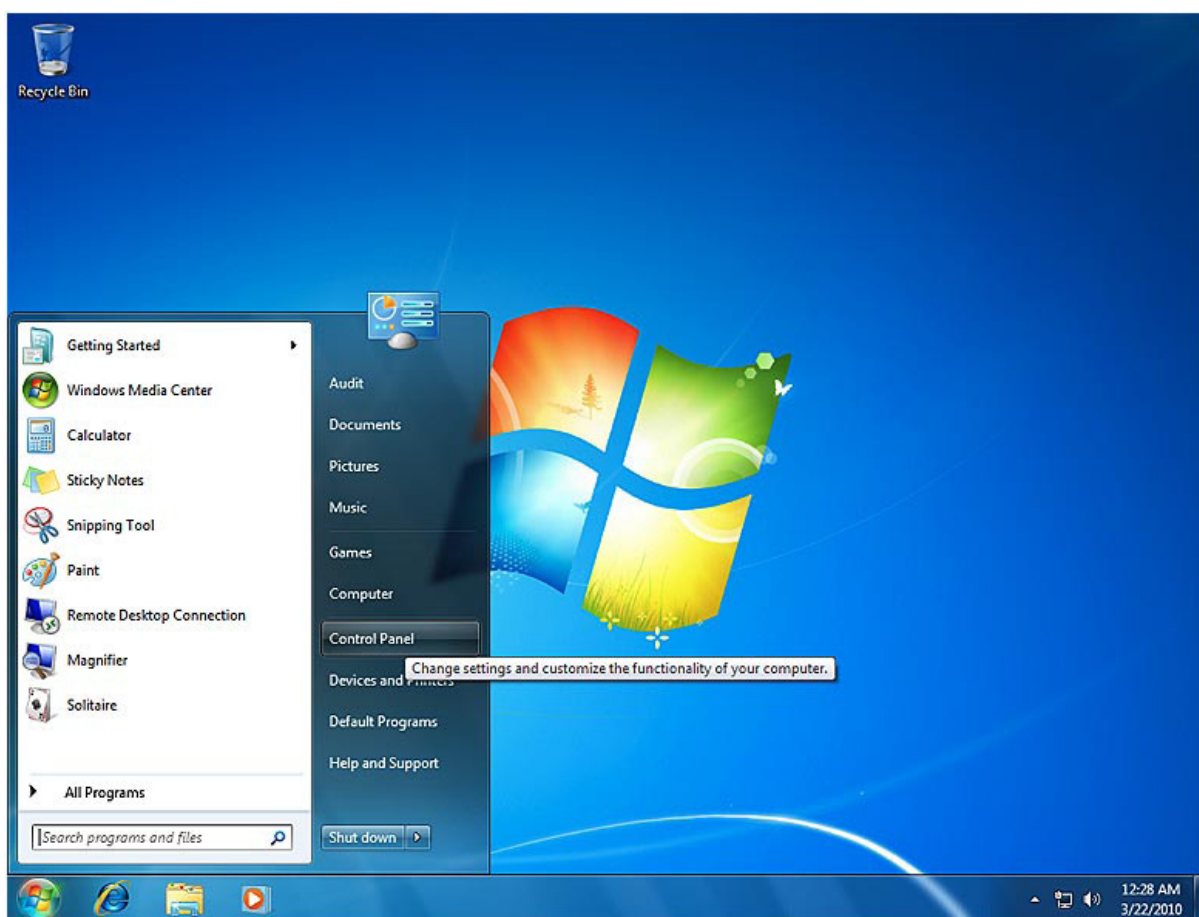
- Select "Create a new account"



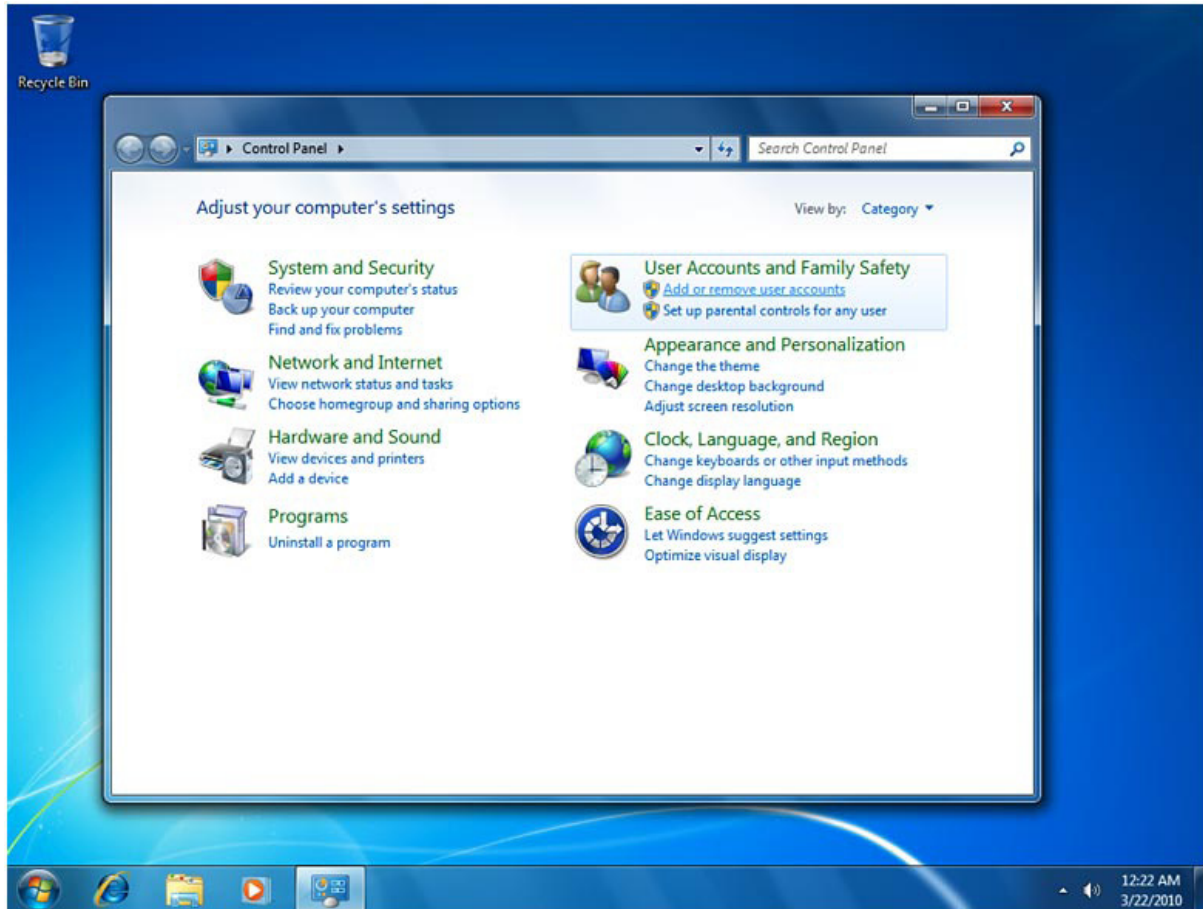
- Create the account and set the permissions.
- Disconnect Kon Boot and restart the computer to restore original Windows authentication functionality.



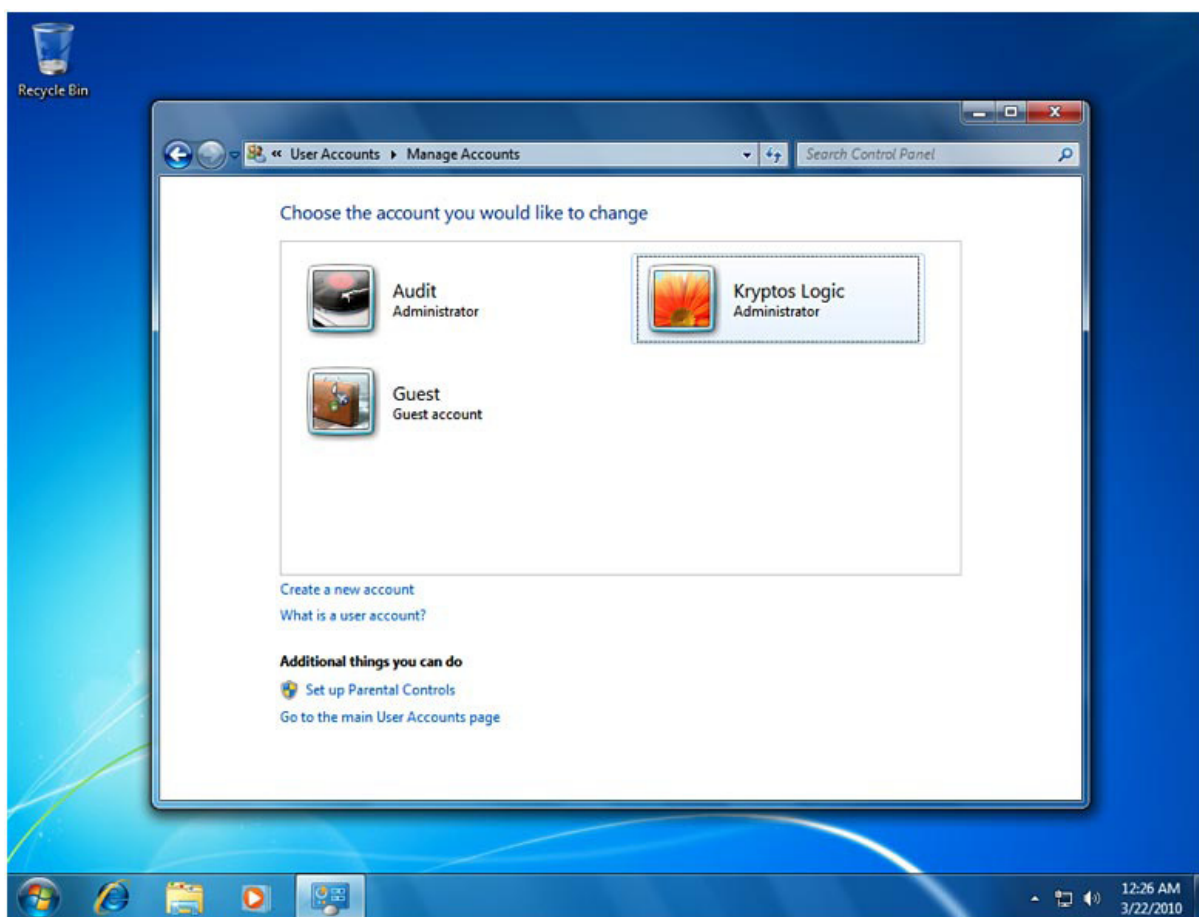
- Select your new User Account. In this example we choose “Audit”



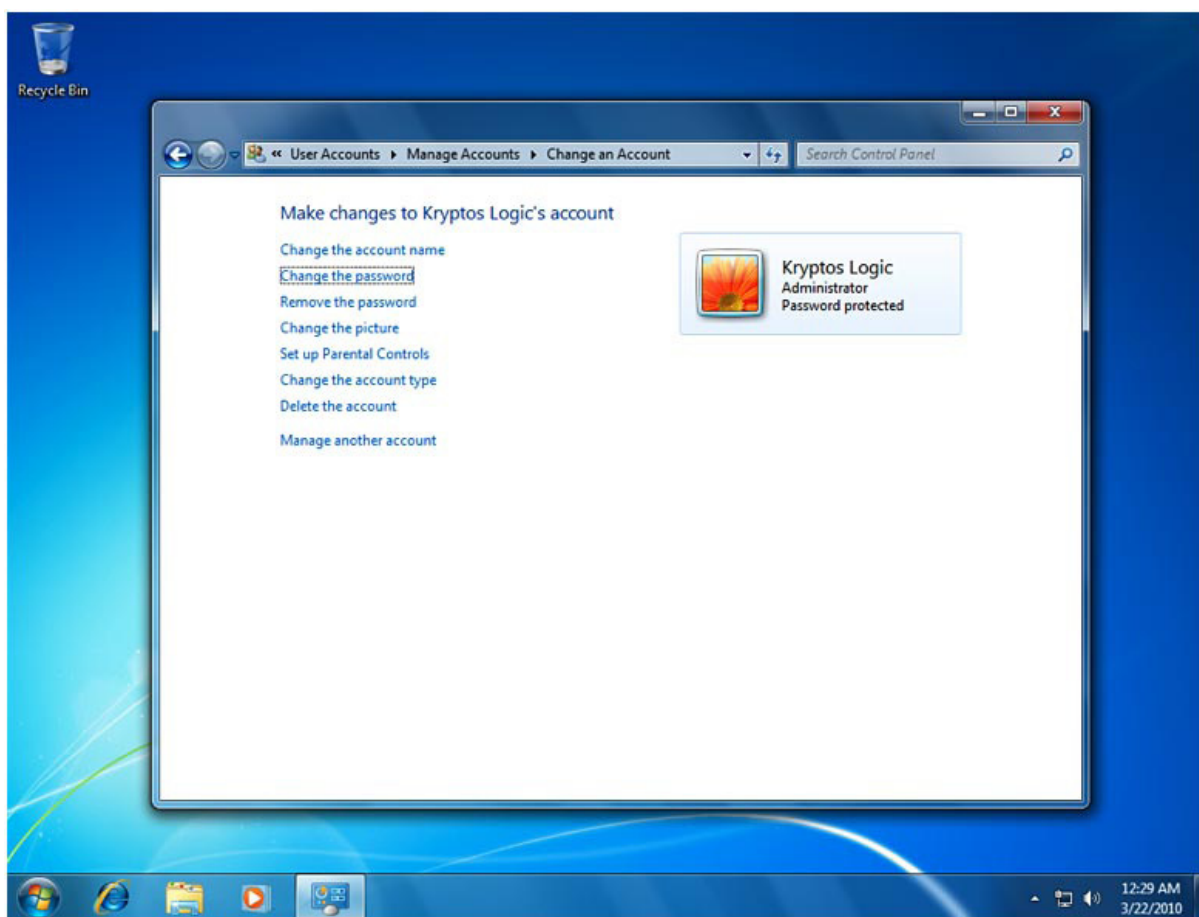
- Navigate the Start Menu to Control Panel



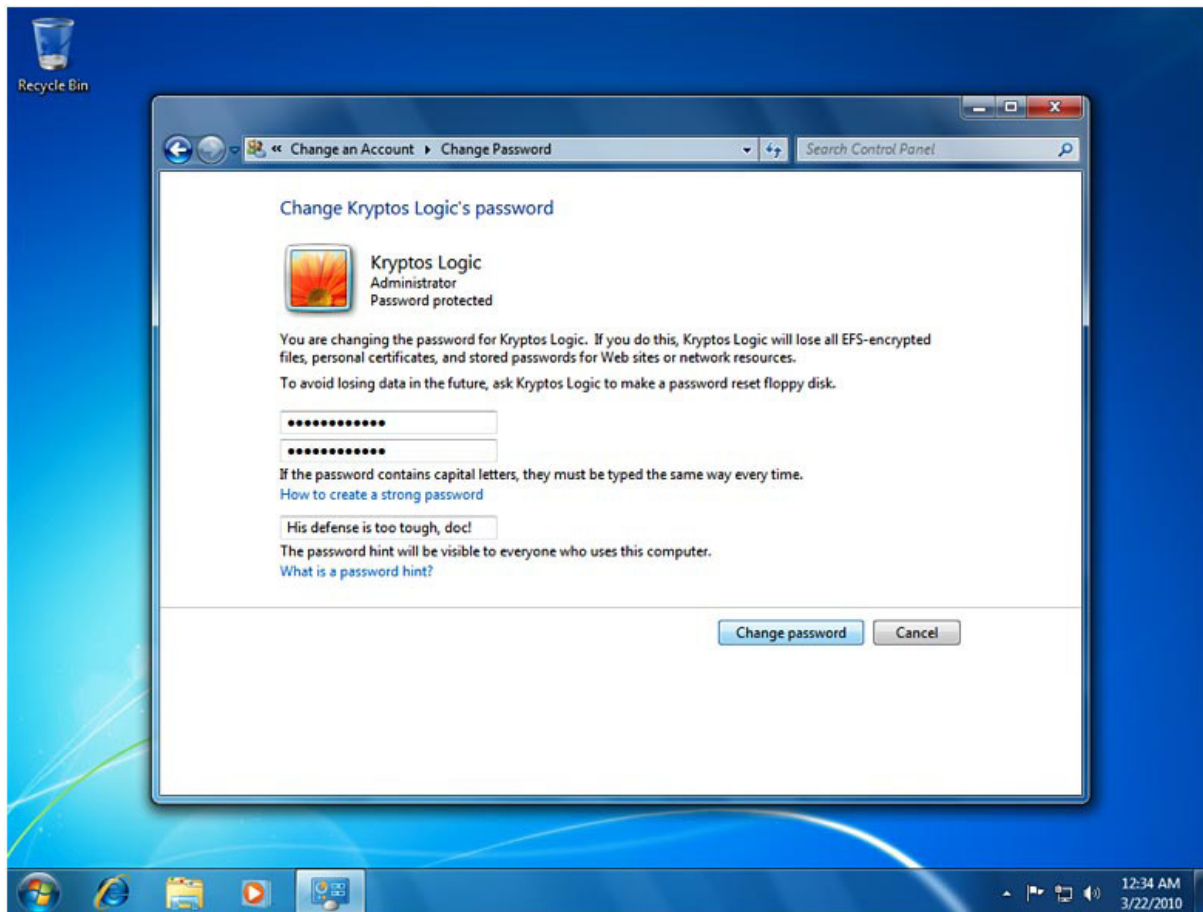
- Select “User Accounts and Family Safety”



- Select the target User Account



- Select "Change the password"



- Input the new information for the account and click “Change password”

4. Kon Boot FAQ

Q. What does Kon Boot do?

A. Kon Boot will allow a user to bypass the authentication process on Windows based systems. The password is not overwritten or modified, it is bypassed.

Q. How does Kon Boot work?

A. Kon Boot will hook the BIOS during startup. Once Kon Boot has loaded itself to memory, it will modify the Windows OS kernel so that login authentication is not required.

Q. Are there any permanent changes to my computer when I use Kon Boot?

A. All changes made to the operating system are temporary and will be restored when the computer is rebooted. No permanent changes are made.

Q. My antivirus detects Kon Boot as a virus, does Kon Boot contain malicious code?

A. No. Due to the behavior of Kon Boot with the computers BIOS, Kon Boot may be incorrectly flagged as a boot virus. However, Kon Boot does not contain any malicious code or virus replication features, nor does it collect any information. The sole instruction of Kon Boot is to modify the Windows kernel so that it may bypass login authentication for the purpose of disaster recovery, auditing, forgotten passwords, or penetration testing. We do suggest disabling your antivirus when creating a Kon Boot CD, Floppy, or USB flash drive.

Q. Does Kon Boot work on domain controllers?

A. Kon Boot will not bypass authentication of domain controllers. There are instances where a client computer will locally cache a domain login, and Kon Boot may work.

Q. Can Kon Boot bypass hard drive encryption?

A. No. Kon Boot will only bypass authentication of Windows based local passwords.

Q. Can I read Windows EFS encrypted folders using Kon Boot?

A. Kon Boot will not allow encrypted folder access. In no case should you reset or change your password with a Windows EFS based login using Kon Boot (or any other tool). The password and the encryption key are binded, and changing the password of a Windows EFS login will require the original password to be reset before EFS folders can be accessed again via login.

Q. Kon Boot gives an error related to BIOS. What's wrong?

A. It is likely that the BIOS memory is too small for Kon Boot to run, and therefore Kon Boot is not compatible with this particular computer.

Q. How do I protect my computer so Kon Boot does not work on it?

A. We recommend hard drive encryption using tools such as TrueCrypt or PGP. Disabling CDROM and USB boot while password protecting your BIOS is also helpful. Kryptos Logic will also release a BIOS protector, which will prevent any tool, including Kon Boot, from booting.

Q. Kon Boot USB does not work for me?

A. Various BIOS and computer configurations may be incompatible with certain USB flash drives. Additionally, certain BIOS configurations and Kon Boot are incompatible. If you have an instance which Kon Boot will not run, please submit the BIOS version and computer model to Kryptos Logic. We will try to fix it for our next release!

Q. Can I make any suggestions or comments about Kon Boot?

A. Absolutely. Please send your thoughts to contact@kryptoslogic.com

Q. Are copies of Kon Boot on P2P and sites other than KryptosLogic.com safe?

A. Do not use unauthorized copies of Kon Boot. Kon Boot should be purchased only from verified sources, such as KryptosLogic.com. Versions obtained outside of our distribution channels may contain virus infections, malware, or simply be damaged. These versions are not trusted, safe, or supported. Furthermore, we do not support unauthorized versions of Kon Boot.