Securing Operating Systems

Module 2

Simplifying Security.

Certified Secure Computer User

Module 2: Securing Operating Systems

Exam 112-12

Module Objective

As systems grow powerful, attacks on systems grow **more sophisticated**, and no amount of security measures may completely avert the attacks. But security measures do help in **mitigating the attacks**. Therefore, it is important that the system users secure the computer from threats. This module talks about securing a system from such threats.

This module will familiarize you with:

- System Security
- Threats to System Security
- How Does Malware Propagate?
- Guidelines for Windows Operating System Security
- Two-Way Firewall Protection in Windows
- Windows Encrypting File System (EFS)
- How to Hide Files and Folders?
- Windows Security Tools
- Guidelines for Securing Mac OS X
- Computer Security Resources on the Internet
- Operating System Security Checklists

Module Flow

System Security

Threats to System Security

Guidelines for Windows OS Security

Windows Encrypting File System (EFS)

Windows Security Tools

Guidelines for Securing Mac OS X

System Security

System security is a requirement for accessing various applications and downloads in enterprises. System security is a **major concern** to organizations and users as it may contain sensitive data. The system has various issues such as **malicious software**, hardware or software **failure**, **malicious user** or attacker, **user error**, **phishing**, and **theft** or **vandalism**.

Issues related to system security include:

- Every operating system and application is subject to **security flaws**, because every day, attackers are finding new attack codes to attack the operating systems.
- Software vendors usually develop patches to address these flaws, which are usually caused by the **uneven architecture** during the developing phase.
- The user has to obtain and **install the patches** and **configure the software**, which updates system protection and maintain an unaffected performance.

System compromise can be prevented by applying security patches in a timely manner.

Threats to System Security

Specific threats one should be aware of for system security include:

Virus

A virus is a program that **replicates** by copying itself to other programs, system boot sectors, or documents, and **alters** or **damages** the **computer files** and **applications**. A computer virus can do anything from popping up a short message to wiping key files so that your computer does not work. Some viruses may cause direct damage to your files by deleting or corrupting them. Viruses can also **use system resources**, and reduce computer speed by affecting the computer or network. Some viruses may display rude, political, or strange messages on the screen. Some viruses can allow other people to access and perhaps control your computer.

Worm

A worm is a **self-replicating** virus that does not alter files but **resides in computer memory** and replicates itself. A computer worm is similar to a computer virus. However, unlike a virus, it does not require user intervention to replicate, as it is a self-replicating computer program. A virus works by attaching itself to another executable program. A worm does not have to be part of another program to propagate itself and is designed to **exploit the file transfer activities** on target systems.

In addition to replication, a worm can cause further harm such as **deleting files** on the victim system or **sending documents** via email. A worm can wreak havoc with the network traffic generated by its reproduction. For example, the MyDoom worm caused a noticeable worldwide Internet slowdown at the peak of its spread.

Backdoor

Backdoor is an **unauthorized means** of accessing a system and bypassing the security mechanisms. An effective backdoor allows an attacker to **retain access** to an infected machine, even though the system administrator detects the intrusion.

Rootkit

Rootkit is a set of programs or utilities that allows a user to **maintain root-level access** to the system. The primary purpose of a rootkit is to allow an attacker repeated unregulated and **undetected access** to a compromised system. Typically, a rootkit may be a bundle of tools such as network sniffers or log-cleaning scripts or utilities. Rootkits can **crack the password** at the administrator level as well as exploit the system's vulnerability. Thus, the rootkit **compromises the existing security** of the affected system and violates its integrity.

Trojan

A Trojan is a program that seems to be legitimate but acts maliciously when executed. It appears to the user as an **apparently harmless program** or data in such a way that it can get control and execute its chosen form of damage. It can damage or erase information on the hard drive. It can also **open a discreet entry point for an attacker** to revisit and "own" the system. A Trojan can thus permit an attacker to **use the victim's system** for further attacks. Data can be stolen and manipulated. In contrast, the attacker may use the system's resources such as hard disk space to distribute illegal material over the net.

A Trojan can also:

- Spread other malware, such as viruses
- Set up networks of infected computers in order to attack others
- Retrieve data discreetly from the target computer
- Log keystrokes to steal information

Logic Bomb

A logic bomb is a code that is surreptitiously **inserted into an application** or operating system that causes it to perform a destructive or security-compromising activity **whenever specific conditions are met**.

Spyware

Spyware includes Trojans and other malicious software that **steals personal information** from a system without the users' knowledge. It can result in **undesired advertising** (pop-up ads in particular), the rerouting of page requests to illegally claim commercial site referral fees, and even the installation of **stealth phone dialers**. Some software providers bundle secondary programs to collect data or distribute advertisement content without explicitly informing the user about the real purpose of those programs. These secondary software programs can drastically impair or **degrade system performance**, and **consume**

network resources. They often have design features that make them difficult or impossible to uninstall from the system.

Insecure Windows-based computers, mainly those used by children or gullible adults, can swiftly accumulate many spyware components. Stealth dialers try to connect directly to a particular telephone number involving long-distance or overseas charges. A few spyware vendors, notably 180 Solutions, **redirect affiliate links** to major online merchants such as eBay and Dell, effectively hijacking the commissions that the affiliates would have expected to earn in the process. Examples of spyware include DirectRevenue, Bonzi Buddy, and Cydoor.

Keylogger

Keylogger is a hardware device or small software program that **monitors** and **records** each **keystroke** on a user's computer keyboard. It can be used by an attacker to **capture confidential information** for later use. This means a keylogger can be used to find out everything a person types into a computer, including personal letters, business correspondence, passwords, and credit card numbers.

Commercially available systems include devices that can be **attached** to the **keyboard cable** (and thus are instantly installable, but visible if the user makes a thorough inspection) as well as devices that can be installed in keyboards (and are thus invisible, but require some basic knowledge of soldering to install). Software keyloggers, like any computer program, can be distributed as a Trojan or as part of a virus or worm.

Password Cracking

Password cracking is the process of **identifying** or **recovering** an unknown or forgotten password. The malicious intent behind password cracking is to gain **unauthorized access** to a system. A **password cracker** is an application program that is used to identify an unknown or forgotten password to a computer or network resources.

Password Cracking

Password cracking techniques include:

Guessing

Password guessing is **trying different passwords** until one works. Password guessing may involve various **manual** and **automated** techniques to identify the correct password. Attackers may use the **brute-forcing**, **dictionary** attack, **shoulder surfing**, and **social engineering** techniques to guess the password.

Brute Forcing

Brute Forcing involves trying a combination of all the characters until the correct password is discovered. A brute-force attack tries every possible password. This is likely to

succeed when the password is small. Several **password-cracking programs** are available on the Internet. A strong password and frequent changes can help defend against password crackers.

Dictionary Attack

Dictionary attack uses a **pre-defined list** of words to recover the password. A dictionary attack also exploits the tendency of people to choose weak passwords, and is related to the previous attack. Password cracking programs usually come equipped with **dictionaries** or word lists, of several kinds. Examples include mythological names, music artists, places, and commonly used passwords.

Shoulder Surfing

Shoulder surfing involves **watching while someone types** the password. An intruder may be standing inconspicuously, but still near, a legitimate user, watching as the password is entered. The attacker simply looks at either the user's keyboard or screen while he or she is logging in, and watches to see if the user is staring at the desk for a password reminder or the actual password.

This type of attack can also occur in a grocery store checkout line when a potential victim is swiping a debit card and entering the required Personal Identification Numbers (PIN). Many of these PINs are only four digits long.

Social Engineering

Social Engineering is **tricking people** into **revealing their password** or other information that can be used to guess a password. An attacker can impersonate a user or system administrator in order to obtain the password from a user. It can be a simple telephone call from someone claiming to be the Internet Service Provider (ISP) asking for details to reset the account.

Many users, however, will blindly click any attachment they receive, thus allowing the attack to work. A contemporary example of a social engineering attack is the use of **email attachments** that contain **malicious payloads** (that, for instance, use the victim's machine to send massive quantities of spam). Internet and email users frequently receive messages that request password or credit card information in order to set up their account or reactivate settings, or are exposed to other forms of **phishing**.

Guidelines for Windows Operating System Security

Over the past several years, the number of computer security breaches has increased. Most of the operating systems (Windows and Mac OS) offer **peer-to-peer files sharing**, which may expose the computer to various **malware programs** or other threats. Guidelines are important and help a user to learn best security practices for securing a Windows operating system.

Follow these guidelines for Windows operating system security:

- Lock the system when not in use
- Create a strong user password
- Disable the guest account
- Lock out unwanted guests
- Rename the administrator account
- Disable startup menu
- Apply software security patches
- Use windows firewall
- Use NTFS
- Use Windows encrypting file system
- Enable BitLocker
- Disable unnecessary services
- Kill unnecessary processes
- Audit the attackers
- Hide files and folders
- Disable simple file sharing
- Use Windows user account control (UAC)
- Implement malware prevention

Lock the System When Not in Use

Lock the system when it is unattended. It helps to secure the workstation from an unauthorized user. It is a built-in feature found in the Windows operating system. Some ways to lock the system are:

Method 1

- Select the **Windows** and **L** buttons together on the keyboard to lock the system.

Method 2

- Click **Start** →  → **Lock.**

Method 3

- Right-click on desktop, select **Personalize,** click **Screensaver,** select the time**,** and check **On resume, display logon screen** for Windows 7.

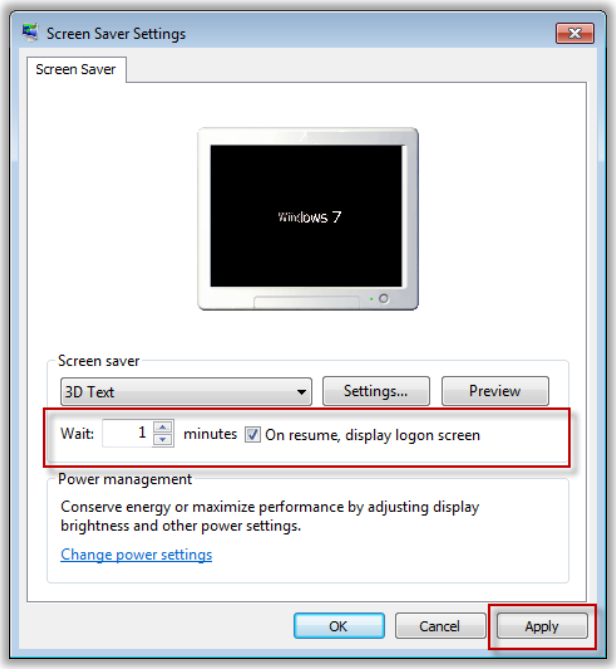


Figure 02-01: Automatic Locking for Windows 7, Screen Saver Settings

Create Strong User Password

A weak password does not offer an effective protection against unauthorized access to a resource. Always use strong passwords e.g. tEst@5#&*! for logging into the system. To create strong passwords in Windows OS:

- Go to **Start** → **Control Panel**.
- Choose the **User Accounts** option and click **Manage another account**.
- Choose the user for whom the password has to be created.
- Click **User name** and choose **Create a password** (if the password is already set, this option will be **Change the password**).
- In the **Create a password for user's account** window, type the password to be assigned to the selected user.
- Provide a password hint (optional).

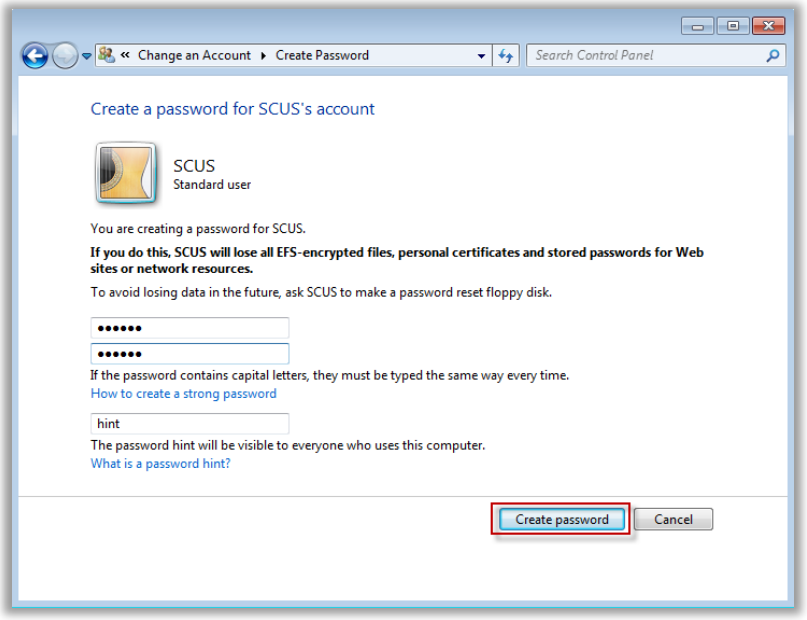


Figure 02-02: Creating or Changing Your Password in Windows 7

- If the password is already assigned to the user account and you are trying to change it, Windows 7 will ask you to verify the current password.
- Click the **Create/Change Password** button.

Disable the Guest Account: Windows 7

Unwanted guest accounts can be exploited by attackers to gain entry in to the system. Steps to disable the guest account include:

- Click the **Start** button, right-click **Computer** from the shortcut menu, and choose **Manage**.
- When the **Computer Management** window opens, go to **Local Users and Groups →Users**.
- Verify that the **Guest account** is disabled by looking for an icon  next to the name.

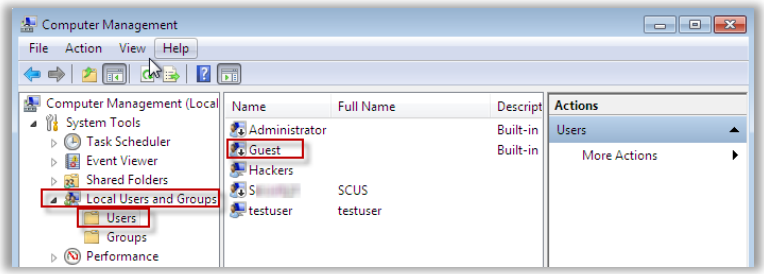


Figure 02-03: Computer Management in Windows 7

- If the account is not disabled, double-click the account name to open its **Properties** window.
- In the user's **Properties** window, check the box next to **Account is disabled** and click **OK**.

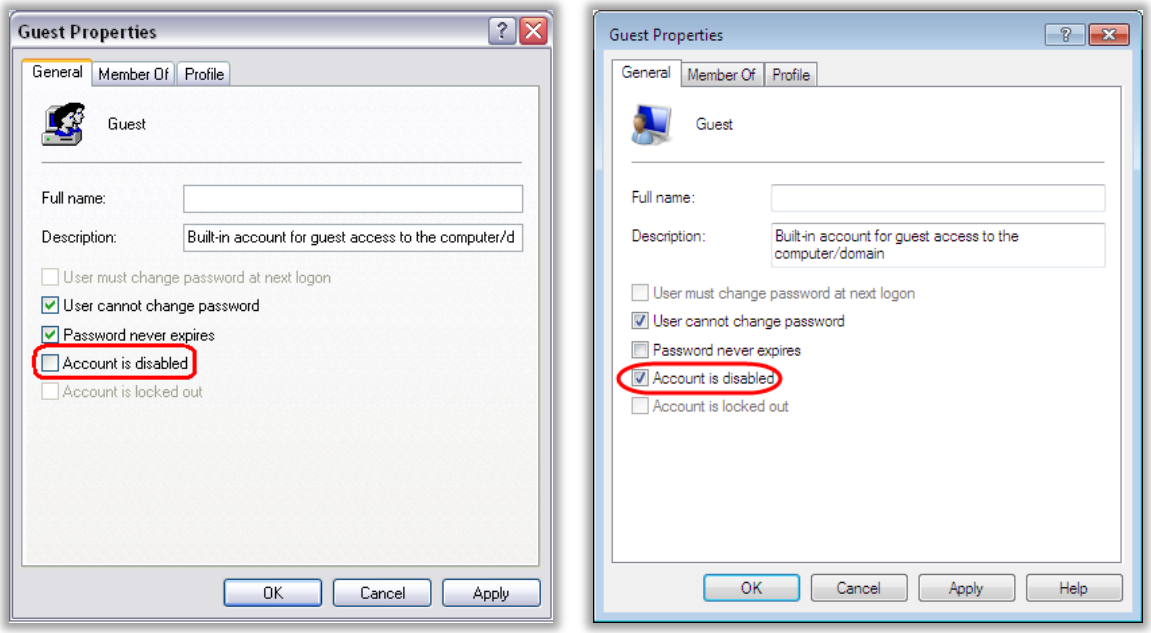


Figure 02-04: Disable the Guest Account Windows 7

Lock Out Unwanted Guests in Windows 7

Lock out unwanted guests by configuring the settings of the account lockout policy to limit the number of login attempts and prevent attacks by blocking the user account when incorrect login attempts exceed the limit. Steps to lock out unwanted guests include:

- Go to **Control Panel**, and click **Administrative Tools.**
- Double-click the **Local Security Policy**, click **Account Policies**, double-click the **Account Lockout Policy**, and double-click **Account Lockout Threshold**.
- At the prompt, enter the number of invalid logins (for example, 3).
- Click **OK** and close.

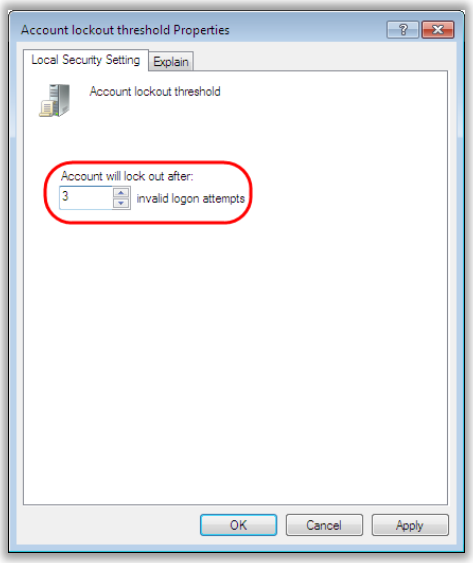


Figure 02-05: Lock Out Unwanted Guests in Windows 7

Rename the Administrator Account in Windows 7

The Administrator account exists on all computers running the Windows operating system (OS). Attackers may guess or crack the administrator password to get unauthorized access to system resources. Users should always rename the administrator account name to make password guessing difficult. Steps to rename the administrator account:

- Click the **Start** button, right-click **Computer**, and click **Manage**.
- In the **Computer Management** window, click **Local Users and Groups**, and select **Users**.
- Right-click on user **Admin** or **Administrator**, select **Rename**, type the new name for the account and click **OK**.

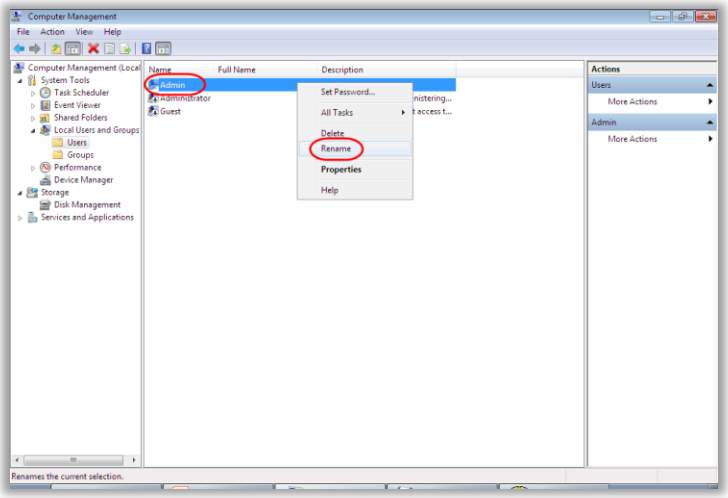


Figure 02-06: Rename the Administrator Account in Windows 7

Disable Start-Up Menu in Windows 7

The operating system keeps track of all the user's documents and programs, so it will start the programs at the start-up which may be useful for some users but not all users. Steps to disable the start-up menu include:

- Right-click on the **Taskbar**, select **Properties**, and click the **Start Menu** tab.
- Uncheck both **Store and display recently opened programs in the Start menu** and **Store and display recently opened programs items in the Start menu and the taskbar**. Click **OK**.

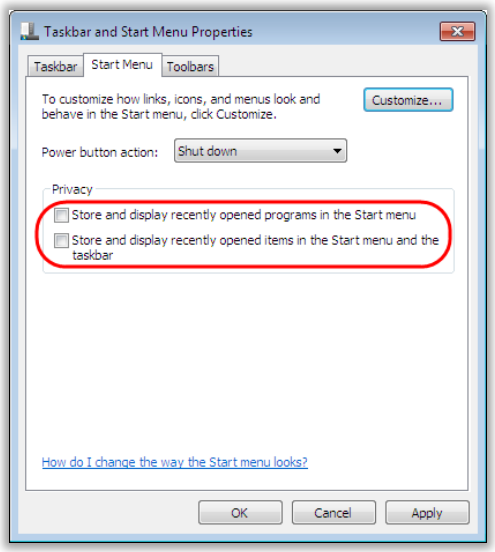


Figure 02-07: Disable Start-Up Menu

Windows Updates in Windows 7

For Windows operating systems, enable automatic updates to ensure that the OS is patched and up-to-date. Steps to configure update settings in Windows 7 include:

- Click **Start → Control Panel** and select **System and Security.**
- Select **Windows Update → Change Settings.**
- Choose how Windows should install updates.

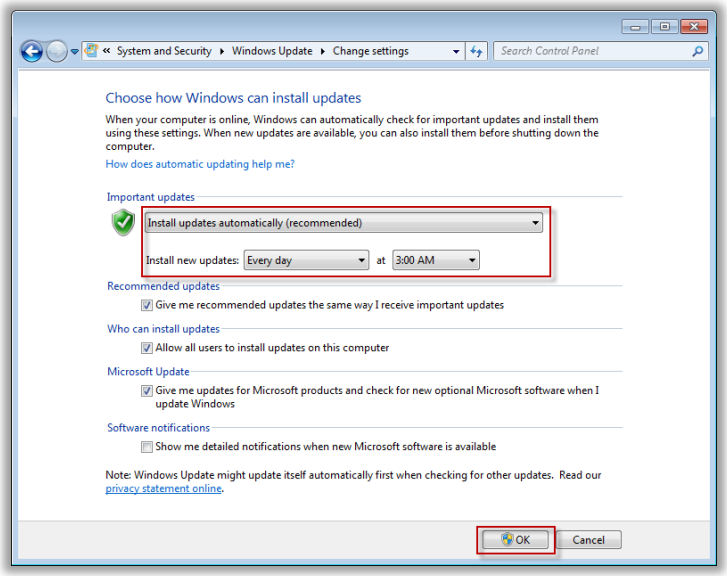


Figure 02-08: Windows Updates in Windows 7

Pointers for Updates

Getting the latest patches and the updates is the primary goal to keep the system protected. Steps for pointer updates include:

- Always patch the OS and applications to the **latest patch** levels.
- Ensure that patches are downloaded only from **authentic sources**—preferably, the vendor site.
- Use **patch management tools** for easier updating. Several free tools are available.
- Do not send patches through email.
- Do not open executable files from sources of questionable integrity.
- Choose to be notified by the vendor about **vulnerability announcements**

Apply Software Security Patches

A patch is a piece of **software** developed and released by software vendors **to fix problems** with or to update a computer program or its supporting data. This includes **fixing security vulnerabilities** and other bugs, and improving the usability or **performance**. Software security updates are used to keep the system OS and other software up to date.

Updates must be installed from the vendor's website. Downloading patches and updates from other sources may lead to downloading malicious software that may harm the system. Users should also avoid using applications that are no longer supported by vendors.

Updates can be installed automatically or manually. However, users should use **automatic updates** to avoid human error. Automatic updates can be installed on a **scheduled basis**. The update process in OS and other applications also can be configured to be hidden and can be restored when required.

Configuring Windows Firewall in Windows 7

A firewall is software that **guards** the system **from unwarranted traffic** when connected to a network. Hackers can try to take advantage of programs running on the system and try to execute malicious code. Hacking tools such as Trojan can send information from the victim's computer to the attacker's computer. A firewall can detect this attack and can allow the user to **block certain traffic** or programs that do not have to access network resources.

Windows Firewall is a built-in, **host-based firewall** that is included in Windows XP with Service Pack 2 and later, Windows Server 2003 with Service Pack 1 and later, Windows Vista, Windows Server 2008 and Windows 7. Windows Firewall drops incoming traffic that does not correspond to either traffic sent in response to a request from the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). It helps protect against malicious users and programs that rely on unsolicited incoming traffic to attack computers.

Steps to configure Windows Firewall include:

- Open Windows Firewall by clicking **Start → Control Panel**.
- In the search box, type ***Firewall*** and click **Windows Firewall**.
- In the left pane, click **Turn Windows Firewall ON or OFF**.

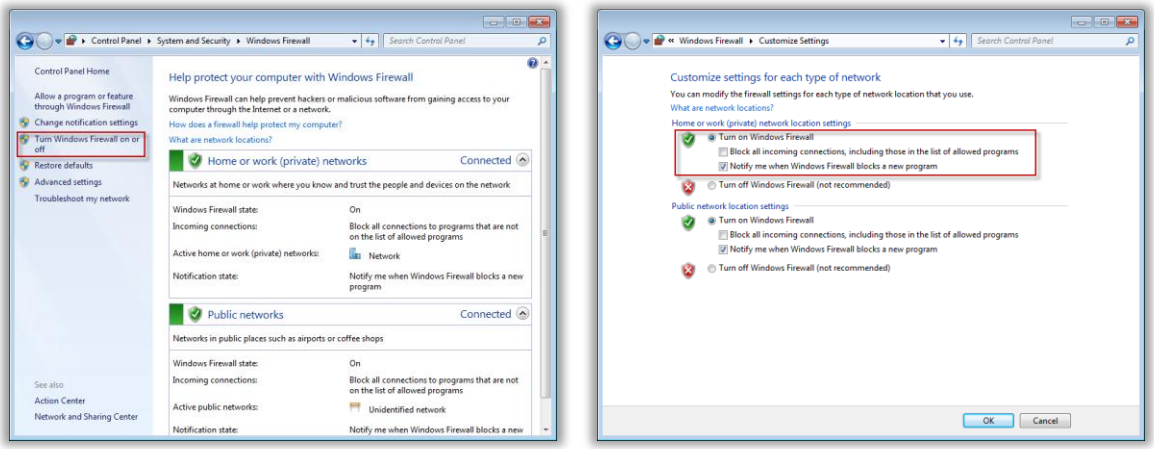


Figure 02-09: Configuring Windows Firewall Settings in Windows 7

Adding New Programs in Windows Firewall in Windows 7

Users can add a program to the list of allowed programs in a firewall to allow a particular program to send information to or from your computer through the firewall. Steps to add a new program in Windows firewall include:

- Click **Start → Control Panel**. Type **Firewall** in the search space and press **Enter**.
- Click **Allow a program or feature through Windows Firewall**.
- Click **Change Settings**.
- Click **Allow Another Program**.

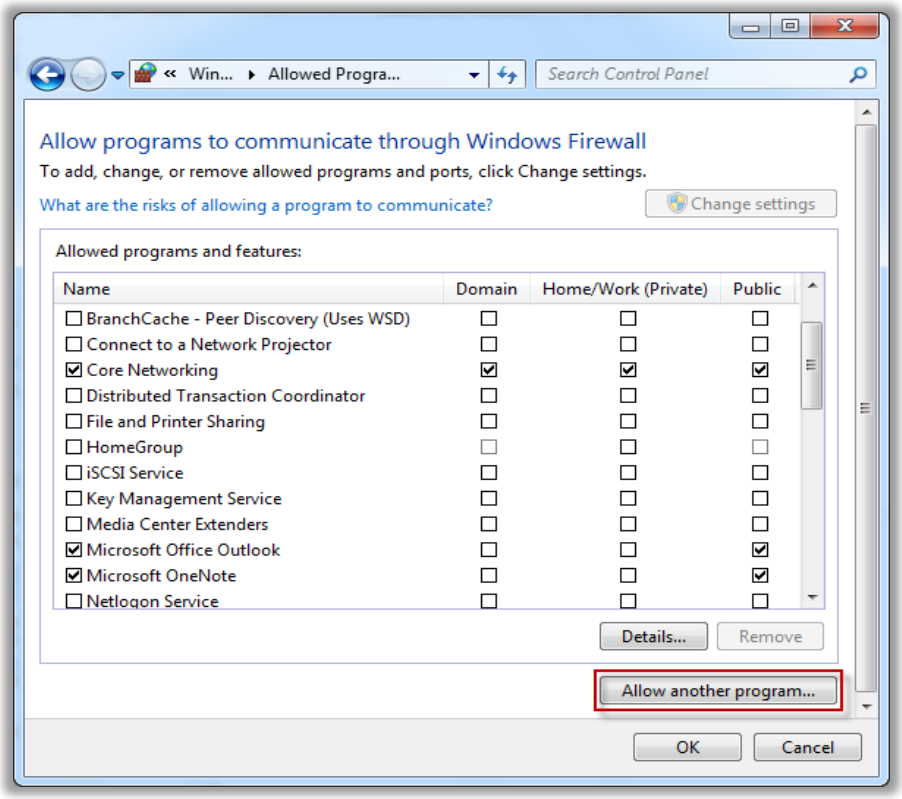


Figure 02-10: Allowing a Program to Communicate through Windows Firewall.

- The **Add a Program** window opens, which lists pre-installed programs. Click **Browse** to add a program (if required).

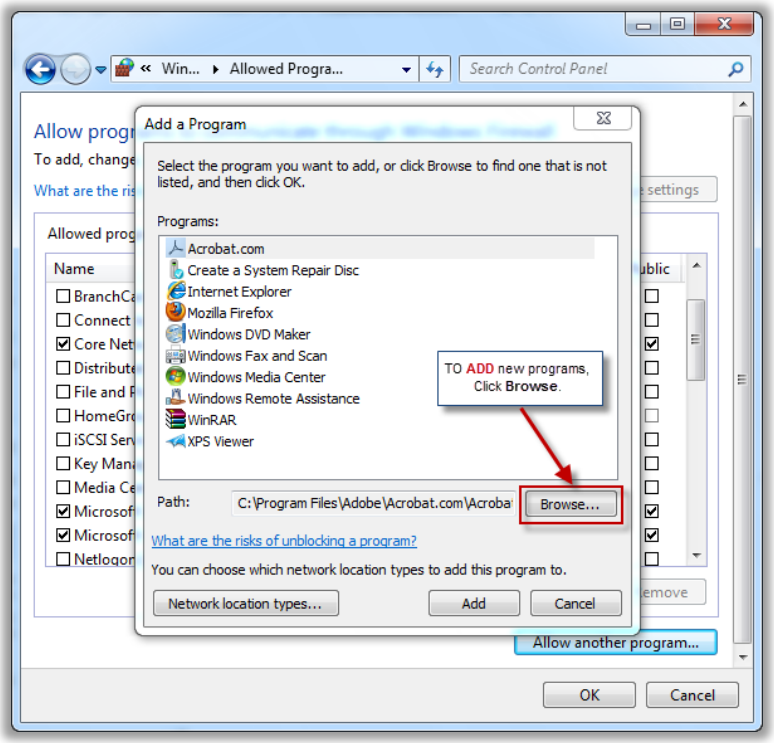


Figure 02-11: Browsing to Add Program

- Find the location of the program, select its executable file, and click **Open.**
- Click **Add** → **OK** to exit the Windows Firewall.

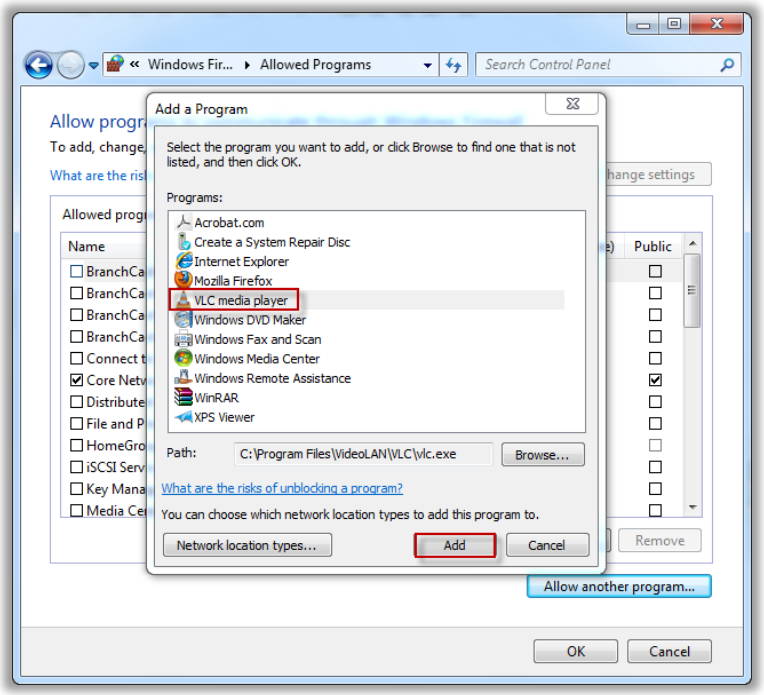


Figure 02-12: Adding New Programs in Windows Firewall in Windows 7

Removing/Disabling Programs Rules from the Windows Firewall in Windows 7

Steps to remove or disable programs from the Windows Firewall in Windows 7 include:

- Click **Start → Control Panel**. Search for **Windows Firewall** and go to **Allow a program or feature through Windows Firewall**. Click **Change Settings.**
- Select the rule you want to **Remove/Disable.**
- To **Disable** any rule for any specific network location, uncheck its respective checkbox and click **OK.**
- To remove any program completely from the allowed program list, click **Remove → YES → OK.**

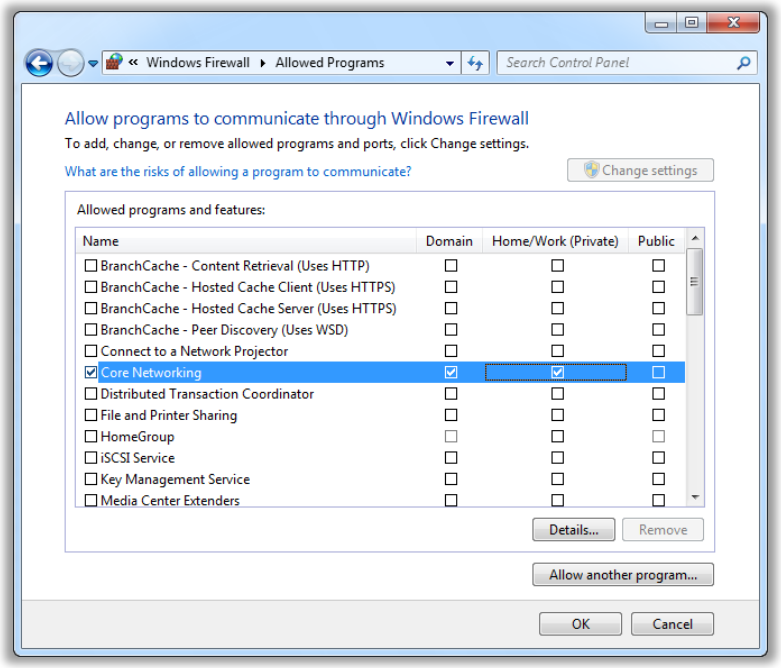


Figure 02-13: Removing/Disabling Programs Rules from the Windows Firewall in Windows 7

Creating a New Windows Firewall Rule in Windows 7

Windows Firewall with Advance Security allows a user to create custom rules. Steps to create a new Windows Firewall Rule in Windows 7 include:

- Click **Start → Control Panel.** Search for **Windows Firewall** and click **Check Firewall Status →** On the left pane click **Advanced Settings.**
- In the **Windows Firewall with Advanced Security** window, click **Inbound Rules → New Rule.**

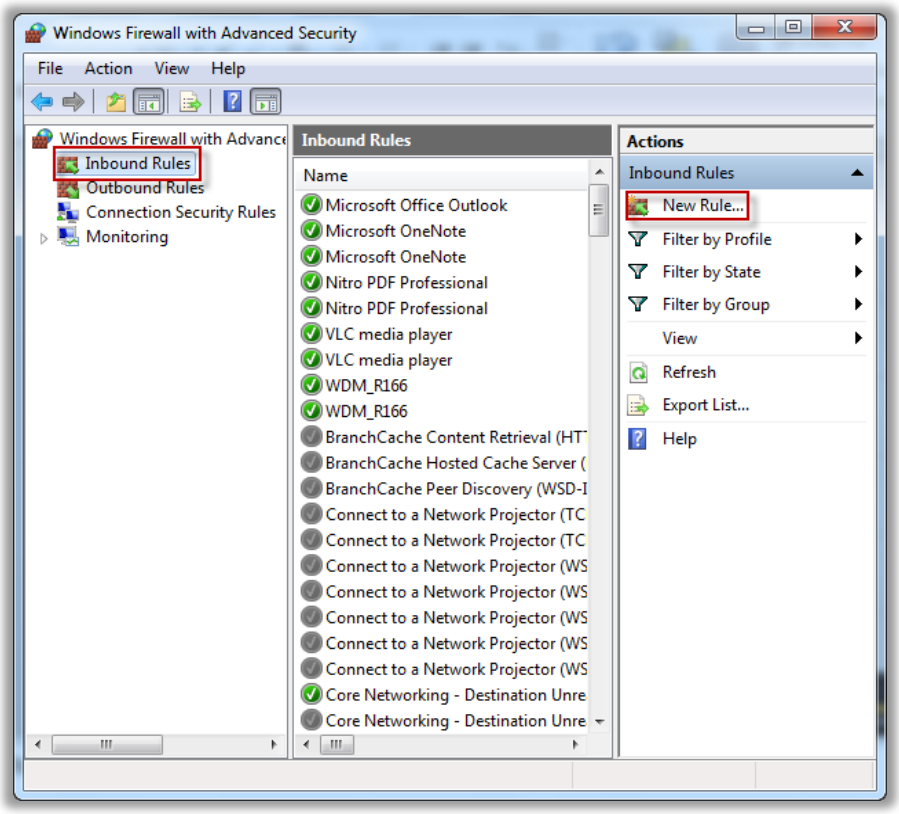


Figure 02-14: Windows Firewall with Advanced Security

- The **New Inbound Rule Wizard** opens. Select (any) the **Rule Type** (Program, Port, Predefined, and Custom rules) you would like to create. Select **Rule Type** as **Port** for this example. Click **Next.**
- Select the type of protocol (**TCP**/**UDP**) and provide the ports numbers or select the option **All Local Ports** for the rule you want to be applied. Click **Next.**

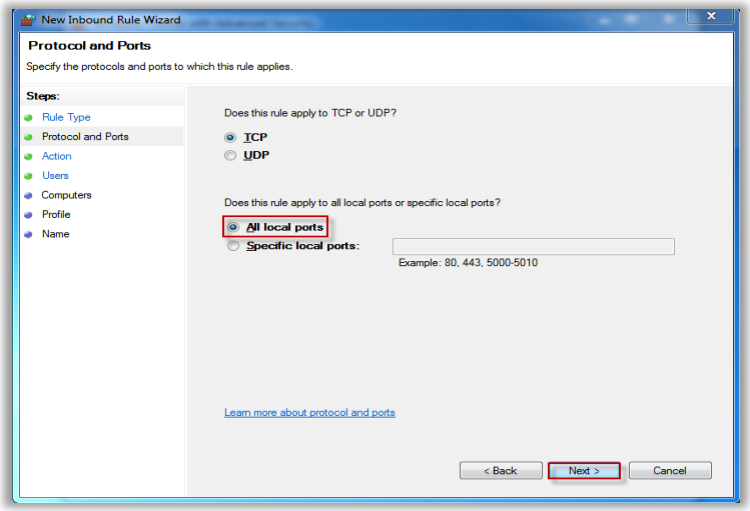


Figure 02-15: Selecting protocol and port number

- Decide the **Action** to take when a connection matches the specified condition (here, **Allow the Connection**). Click **Next.**

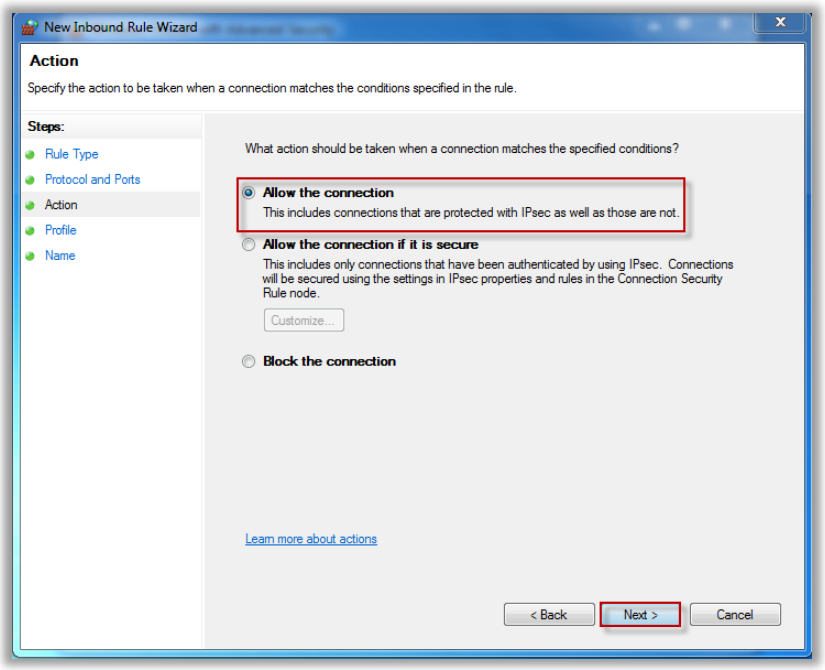


Figure 02-16: Allowing the Connection

- Select the **Network Location** for which the rule has to be applied. Click **Next.**

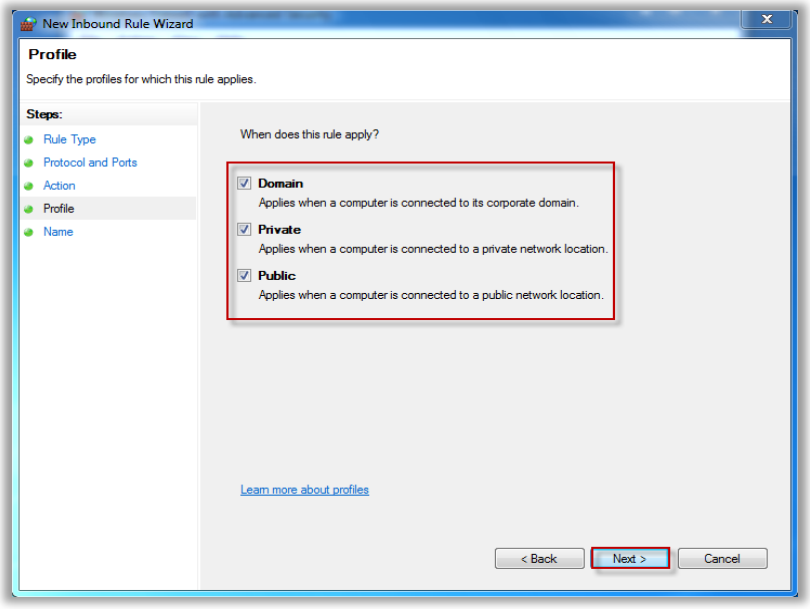


Figure 02-17: Selecting Network Location

- Give a **name** to the newly created rule and description (optional). Click **Finish.**

The rule is created and allows **TCP Inbound Traffic** to all the ports.

Two-Way Firewall Protection in Windows

Threats travel through the web looking for suitable systems with low security levels and outdated or unpatched software. They enter these systems quietly without the knowledge of the user. Installing a better firewall solution could solve the problem. Steps to avail two-way firewall protection include:

- Click **Start,** type **wf.msc** or ***Firewall*** in the search space, and press **Enter.**
- Click the **Windows Firewall** with **Advanced Security** icon.
- This management interface displays the inbound and outbound rules.
- Click **Windows Firewall Properties.**
- A dialog box with several tabs will appear.
- For each profile—Domain, Private, and Public—change the setting to **Block**, and then click **OK.**

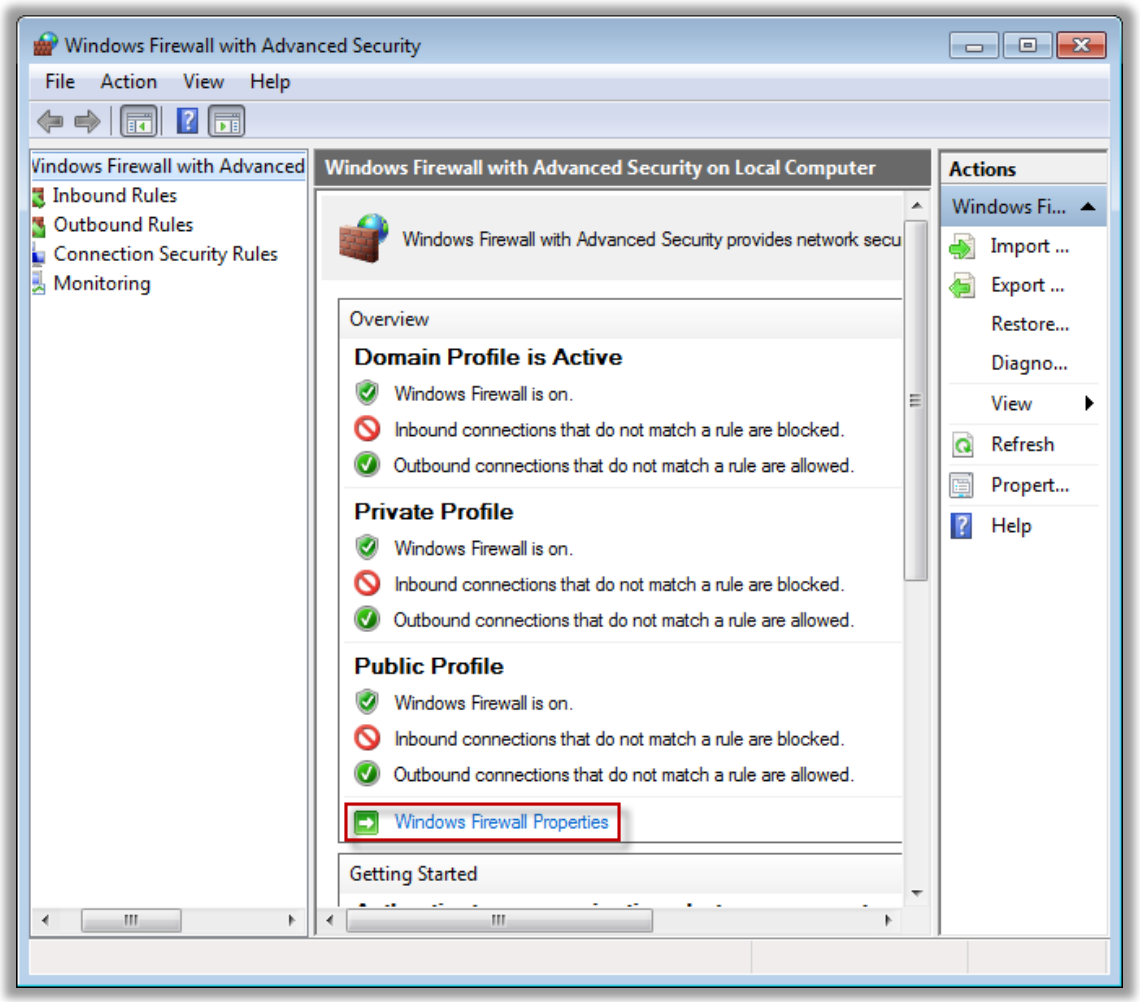


Figure 02-18: Windows Firewall with Advanced Security

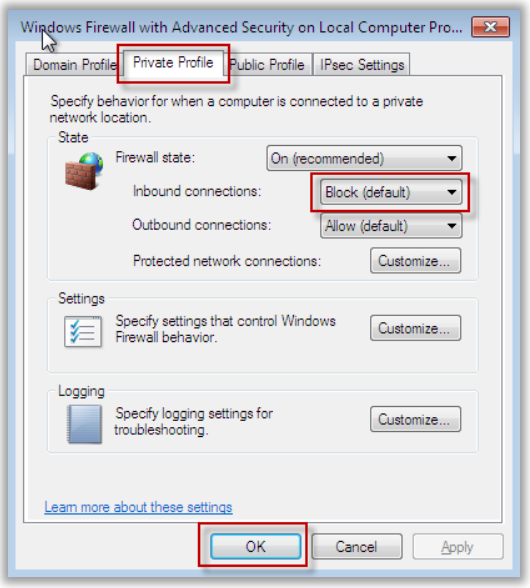


Figure 02-19: Two-Way Firewall Protection in Windows

Always use NTFS

The NTFS file system provides better performance and security for data on hard disks and partitions than the FAT file system. If the Windows system is running with **FAT** or **FAT32**, ensure that the **non-NTFS** partitions are converted to NTFS. You can convert partitions that use the earlier FAT16 or FAT32 file system to NTFS by using the **`convert`** command

- Click **Start** → **All Programs** → **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**. Type the password or provide confirmation if prompted.
- In the **Command Prompt**, type convert ***`drive_letter`*****`: /fs:ntfs`**, where *drive_letter* is the letter of the drive to be converted to NTFS, and then press **ENTER.**
- Type the name of the volume you want to convert, and then press **ENTER**
- When the conversion is complete, exit the command prompt by typing **EXIT.**

Note: Converting a partition from FAT to NTFS does not affect the data on it. You need to restart the computer for the NTFS conversion if the partition contains system files

Windows EFS

Windows Encrypting File System (EFS) allows Windows 7 system users to encrypt files and folder in an NTFS formatted disk drive. EFS does not allow encryption on compressed or zipped files and system files. Steps to encrypt files and folders in Windows 7 include:

- Right-click the file or folder to be encrypted, select **Properties** on the **General** tab, and click the **Advanced** button. The **Advanced Attributes** dialog box appears.

- There are two options under **Compress or Encrypt attributes—Compress contents to save disk space** and **Encrypt contents to secure data**.
- Select **Encrypt contents to secure data**. Click **OK** to close the **Compress or Encrypt attributes** dialog box and click **Apply**.

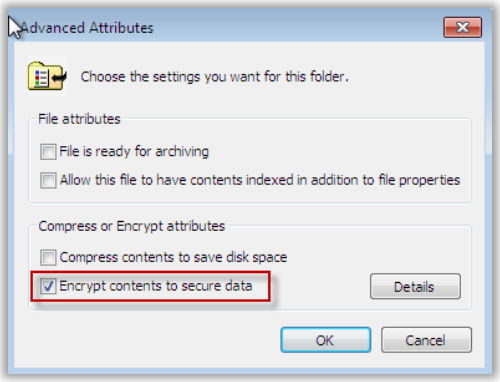


Figure 02-20: Compress or Encrypt Attributes

- The encryption warning dialog box appears. Check either of the two options (not every time): **Encrypt the file and its parent folder** and **Encrypt the file only**. Click **OK**.

How to Decrypt a File using EFS in Windows

- Right-click the file to be decrypted and select **Properties**.
- On the **General** tab, click the **Advanced** button. The **Advanced Attributes** dialog box appears.
- There are two options under **Compress or Encrypt Attributes—Compress contents to save disk space** and **Encrypt contents to secure data**.
- Uncheck **Encrypt contents to secure data**, click **OK** to close the **Compress/Encrypt Attributes** dialog box, apply the settings, and click **OK**.

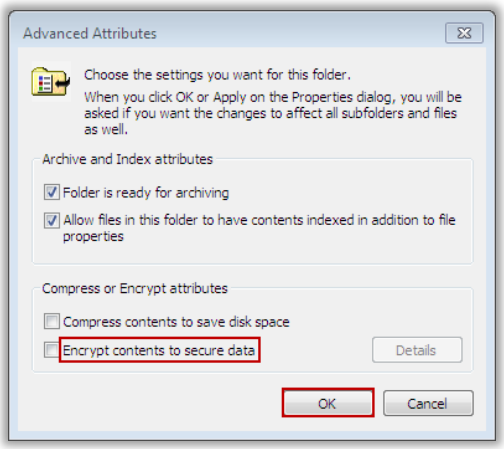


Figure 02-21: Decrypting Files Using Windows EFS

Using Windows Defender

Windows Defender is an **anti-spyware** software that offers real-time protection against spyware and other potentially malicious programs.

- To turn Windows Defender **ON** or **OFF.** open **Windows Defender** by clicking the **Start** button → **All Programs** → **Windows Defender** or type ***Windows Defender*** in the search space.
- Click **Tools** → **Options** → **Administrator.** Check or uncheck the **Use this program** check box. Click **Save.**

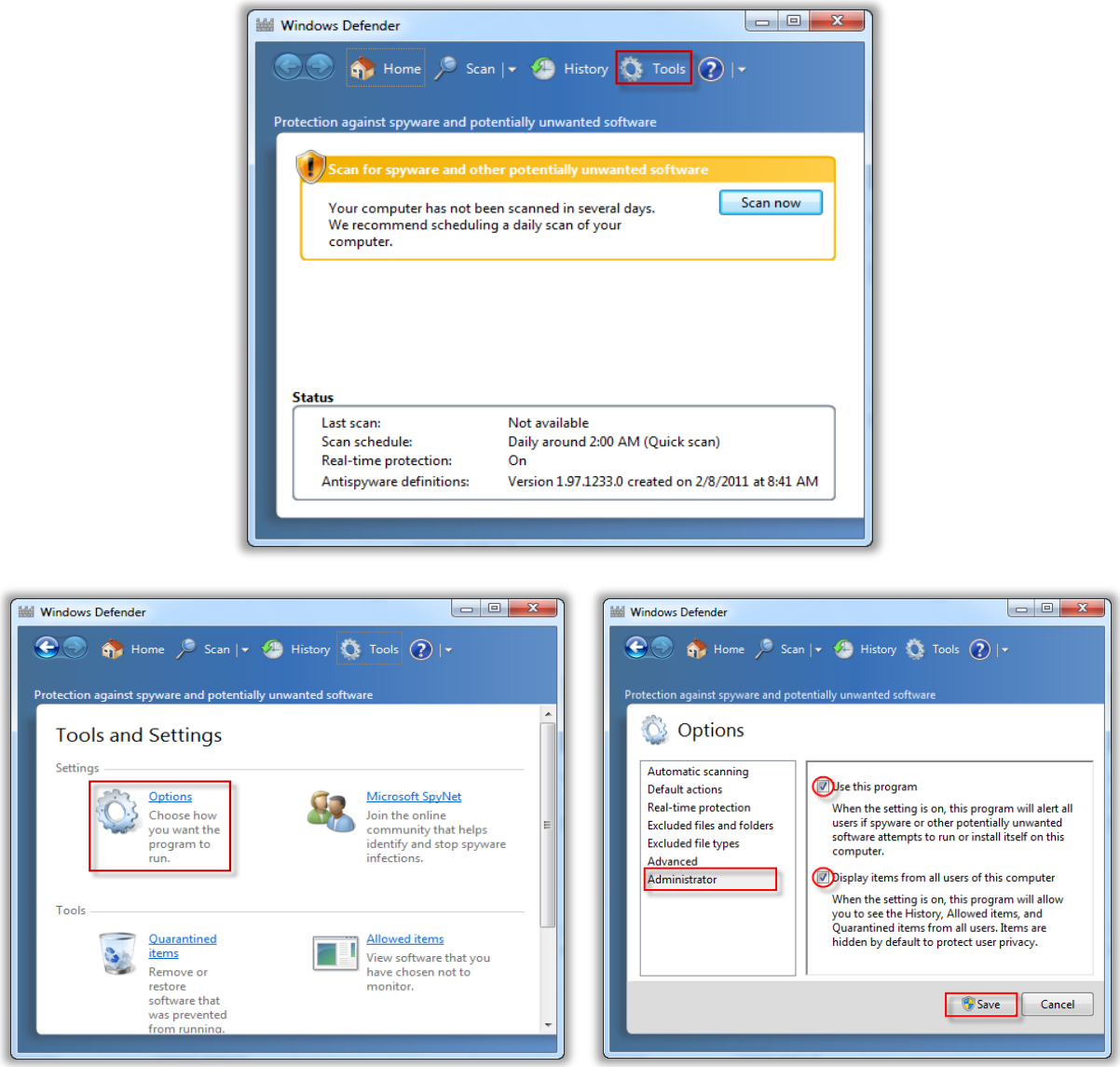


Figure 02-22: Antispyware Software—Windows Defender

Enable BitLocker in Windows 7

BitLocker Drive Encryption allows the entire volume of the system to be secured. Using BitLocker, the hard drive and any removable media on the computer can be encrypted. Encrypted removable media can be decrypted and re-encrypted on any Windows 7 computer. BitLocker in Windows 7 allows:

- The entire volume of the system to be secured
- Encryption of the hard drive and any removable media on the computer
- Decryption and re-encryption of encrypted removable media on any Windows 7 computer
- To enable BitLocker, click **Start → Computer.** Right-click on any of the available drives and select the option **Turn on BitLocker…**

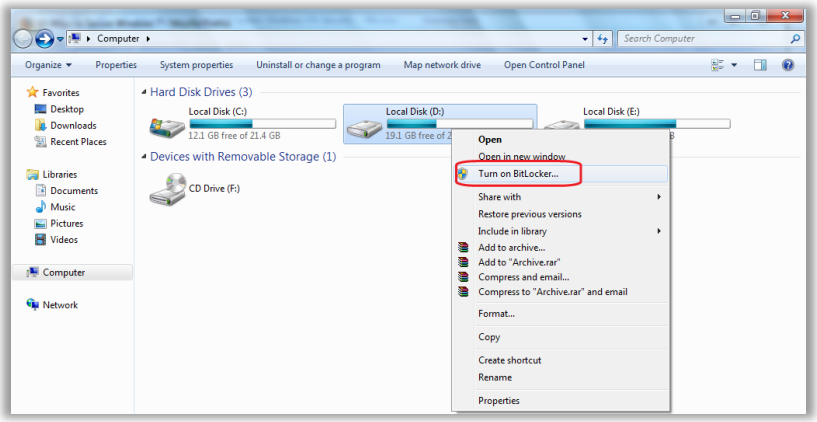


Figure 02-23: Enabling BitLocker in Windows 7

Launching Event Viewer in Windows 7

Event Viewer is a built-in Windows utility that allows users to view and manage the event logs, gather information about hardware and software problems, and monitor Windows security events. It stores logs of application, security, and system events. It may be helpful in detecting any security breach and troubleshooting problems and errors with Windows and other programs. The user can view events that have taken place on the machine by choosing an appropriate log in the tree on the scope pane. It provides an interface to the user that makes it easier to filter and sort events as well as control the types of event logs. The user can gather information about the software and hardware in the system, and can manage those events with Event Viewer. Event Viewer displays detailed information about significant events in the system.

- To start Event Viewer in Windows 7, click **Start → Control Panel → System and Security → Administrative Tools → Event Viewer**.

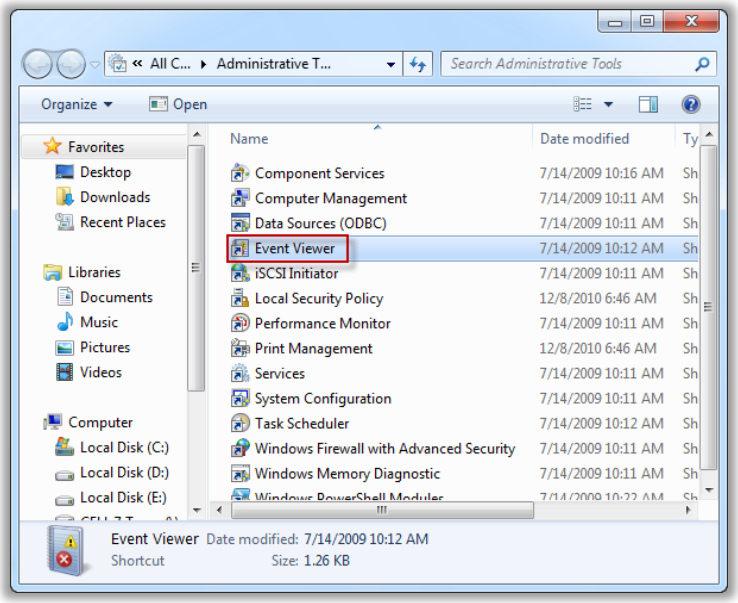
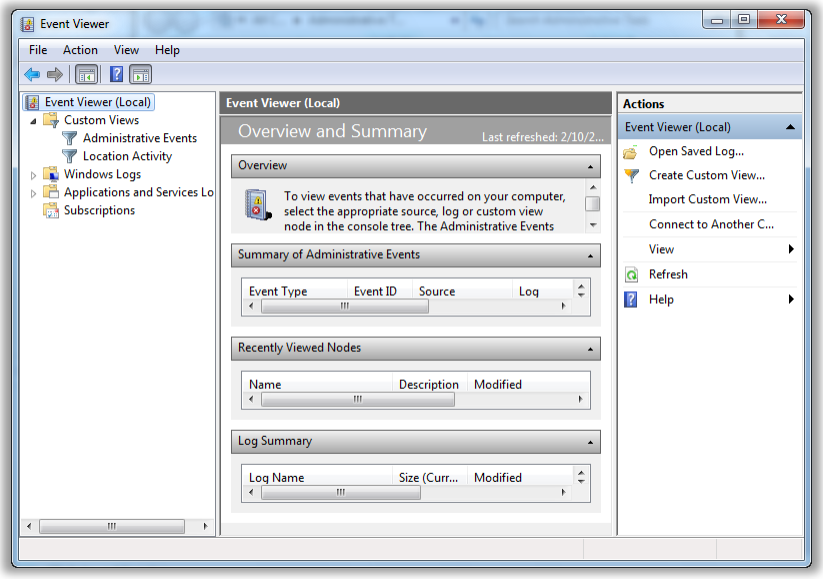


Figure 02-24: Launching Event Viewer in Windows 7

Event Viewer: Events and How to Read Logs on the System

The user must know the logs in his system. By knowing the logs, he or she can detect unauthorized log events. Event Viewer categorizes events into five types: **Error**, **Warning**, **Information**, **Audit Success**, and **Audit Failure**.

Each event log is differentiated by its level and contains header information and a description of the event. Each event header contains a detailed description of the level, date, time, source, event ID, and task category.



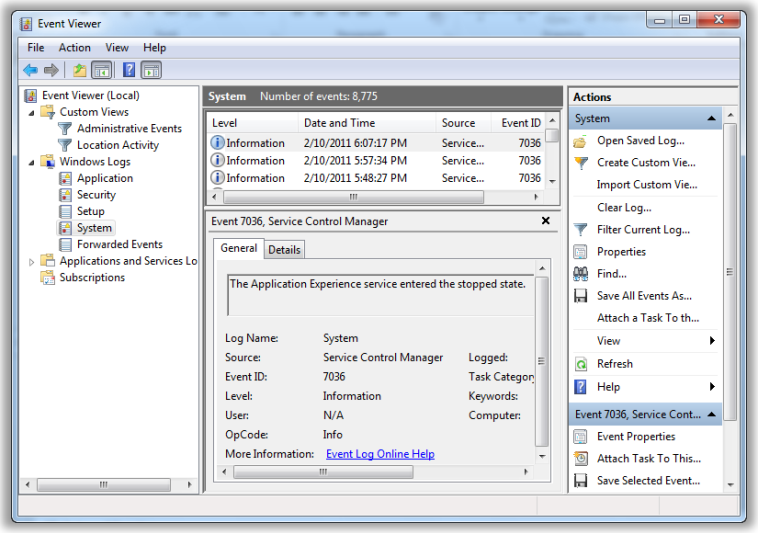


Figure 02-25: Event Viewer Screenshots

Disabling Unnecessary Services in Windows 7

A service does not require the user's intervention. It is a long-running executable that is intended to perform specific functions. Services normally start up when the system boots up. Some services load automatically, whereas others are called when a program is used. To disable unnecessary services:

- Click **Start → Control Panel → Administrative Tools → Services.**
- Alternatively, select **Start** and type ***services.msc*** in search bar and press ***Enter*** to open the **Services** window.
- Once the **Services** window is loaded, the user can turn off any unneeded services.

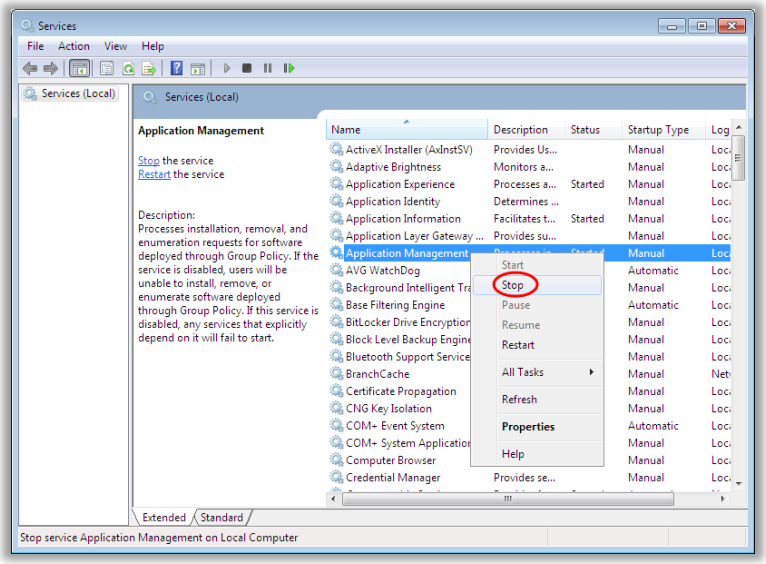


Figure 02-26: Disabling Unnecessary Services in Windows 7

Killing Unwanted Processes

The user can run or kill the processes in the system using two methods. To kill a particular process, perform any one of the following actions:

- Open **Task Manager** by pressing **[Ctrl] + [Alt] + [Del].**
- In **Task Manager** on the **Processes** tab, select the **Process,** and click **End Process.**
- Alternatively, Select the process**,** right-click, and select **End Process.**

Steps to **RUN** a particular process:

- In **Task Manager,** click **File** → **New Task (Run)** and enter the **Process** to run.

Steps to **KILL** a particular process tree:

- Run the **Task Manager,** select the the process, right-click and select **End Process Tree.**

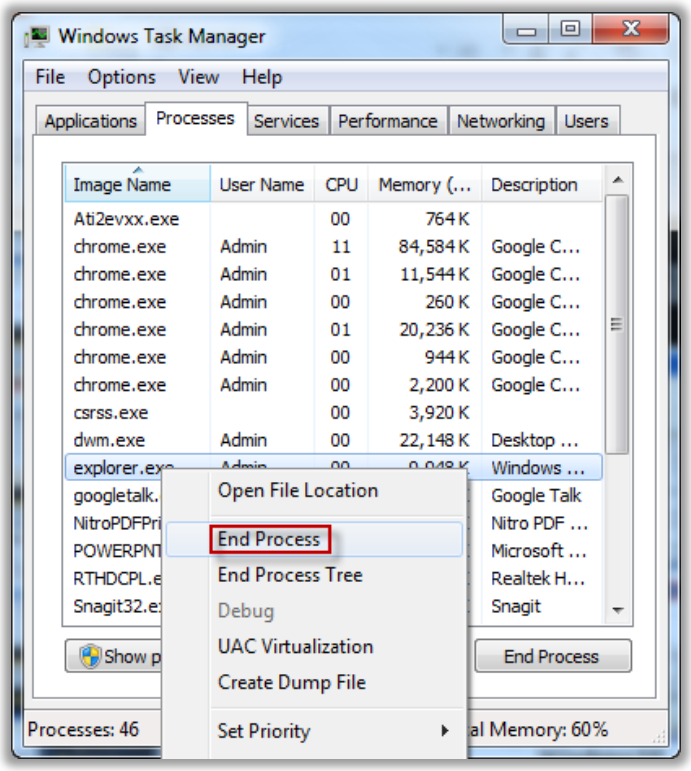


Figure 02-27: Killing Process Trees in Windows 7

Finding Open Ports Using Netstat Tool

Knowing open ports as well as the services and applications associated with these ports helps in detecting the presence of malware such as virus, worms, Trojans, and so on in the system. Malware generally open ports to receive or send data packets from attackers.

Netstat, a Windows inbuilt utility, can be used to determine open ports in the system and associated applications.

- Click **Start → All Programs → Accessories**, right-click **Command Prompt**, and click **Run as administrator**. Type the password or provide confirmation if prompted.
- Type **`netstat -b`** in the command prompt window to see the open ports and associated applications.

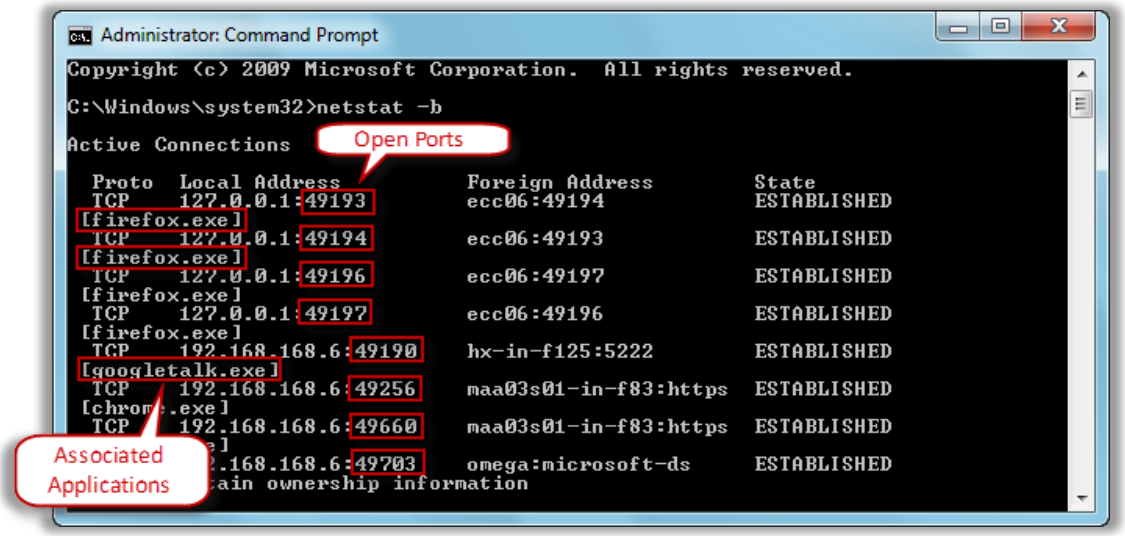


Figure 02-28: Finding Open Ports Using Netstat Tool

Configuring Audit Policy

Audit policies should be configured to identify attempted or successful attacks on a system or network.

1. Click **Start**, type ***secpol.msc*** in search bar, and press **Enter.**
2. Click **Local Policies**, select **Audit Policy,** double-click the **Audit account logon events** policy**,** check the **Success** and **Failure** boxes, click **Apply**, and click **OK.**
3. Similarly, change the security setting for all policies listed in the right-hand pane of the **Local Security Policy** window.
4. Close the **Local Security Policy** window.

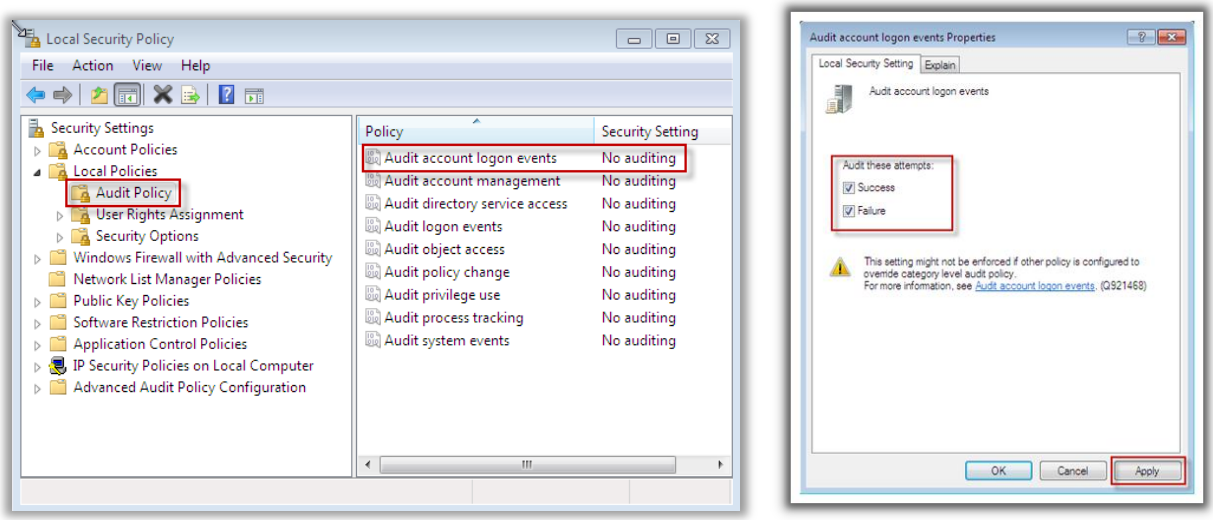


Figure 02-29: Audit Account Logon Events Properties Wizard

How to Hide Files and Folders?

A user can hide the files and folders in the system to avoid attacks from guest or unauthorized users. To hide files and folders:

- Right-click the file or folder to be hidden and select **Properties.**
- Under **Attributes**, check **Hidden**, click **Apply**, and then click **OK.**
- In the Windows Explorer, click Organize → select Folder and search options. In the **Folder Options** window, click **View** tab**.**
- On the **View** tab, there is a list of options.
- Select the **Do not show hidden files and folders** option.

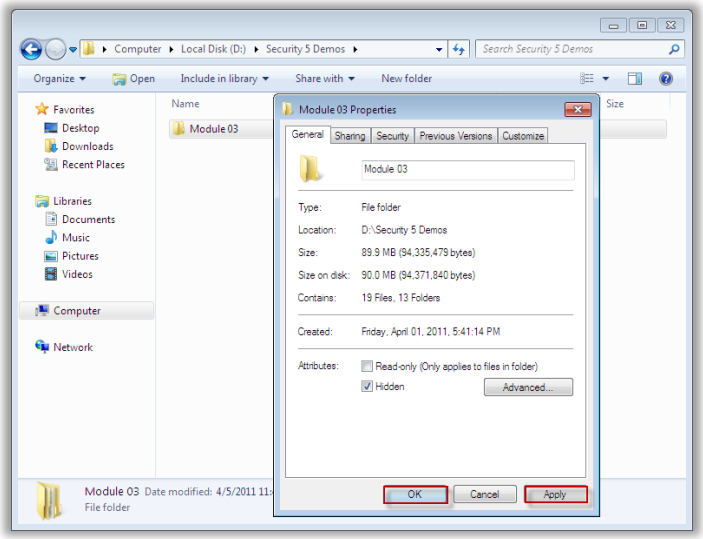


Figure 02-30: File Properties Wizard

Disable Simple File Sharing in Windows 7

File sharing feature in Windows OS enables users to access and share files with other users in the network. It presents potential security risk. Attackers can access all the shared files in a network if they are able to access a system in the network. File sharing feature in Windows should be disabled (if it is not required) to increase system security. To disable simple file sharing:

- Go to **Start → Control Panel → Folder Options.**
- From the **Folder Options** window, choose the **View** tab.
- Scroll to the bottom of the **Advanced Settings** portion of the window.
- Uncheck the box for **Using sharing wizard** and **OK.**

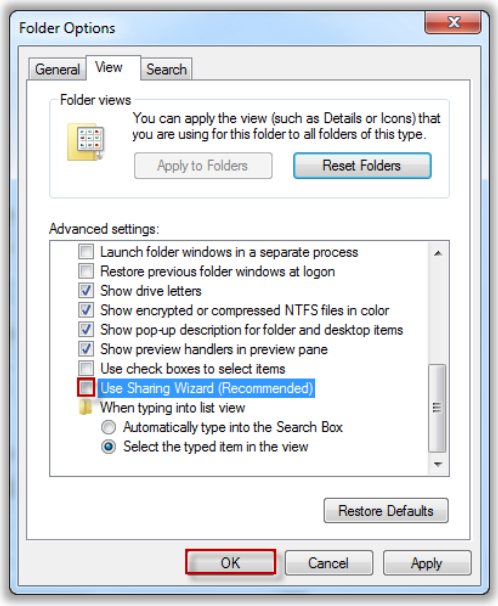


Figure 02-31: Disable Simple File Sharing in Windows 7

Raise the UAC Slider Bar in Windows 7

User Account Control (UAC) helps defend your PC against hackers and malicious software. Any time a program wants to make a major change to your computer, UAC lets you know and asks for permission. User Account Control (UAC) helps the user to make critical decisions in and when installing software.

- Click **Start → Control Panel → Action Center → Change User Account Control Settings** and raise/adjust the UAC slider bar to **Always Notify**.

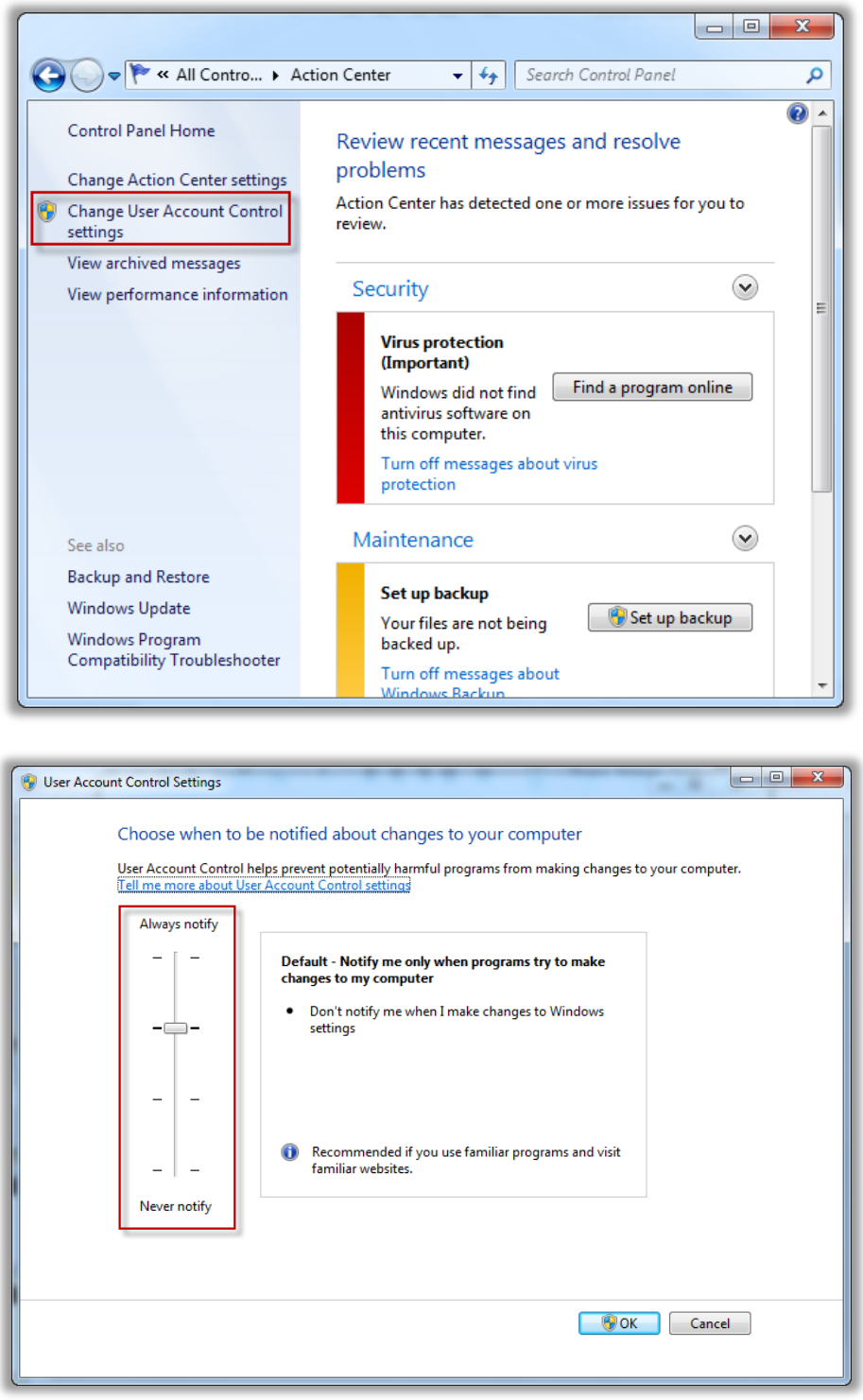


Figure 02-32: UAC Slider Bar: Windows 7

Windows Security Tools: Microsoft Security Essentials

Source: http://www.microsoft.com

Microsoft Security Essentials provides **real-time protection** for your home or small business PC that guards against viruses, spyware, and other malicious software. Security essentials cover the complete protection of a system and guards against attacks.

Microsoft Security Essentials is backed by the **Microsoft Malware Protection Center** (MMPC), which provides world-class antimalware research and response capabilities to support all Microsoft security products and services.

Key features include:

- Comprehensive **malware protection**
- Simple, free download
- Automatic updates
- Easy to use

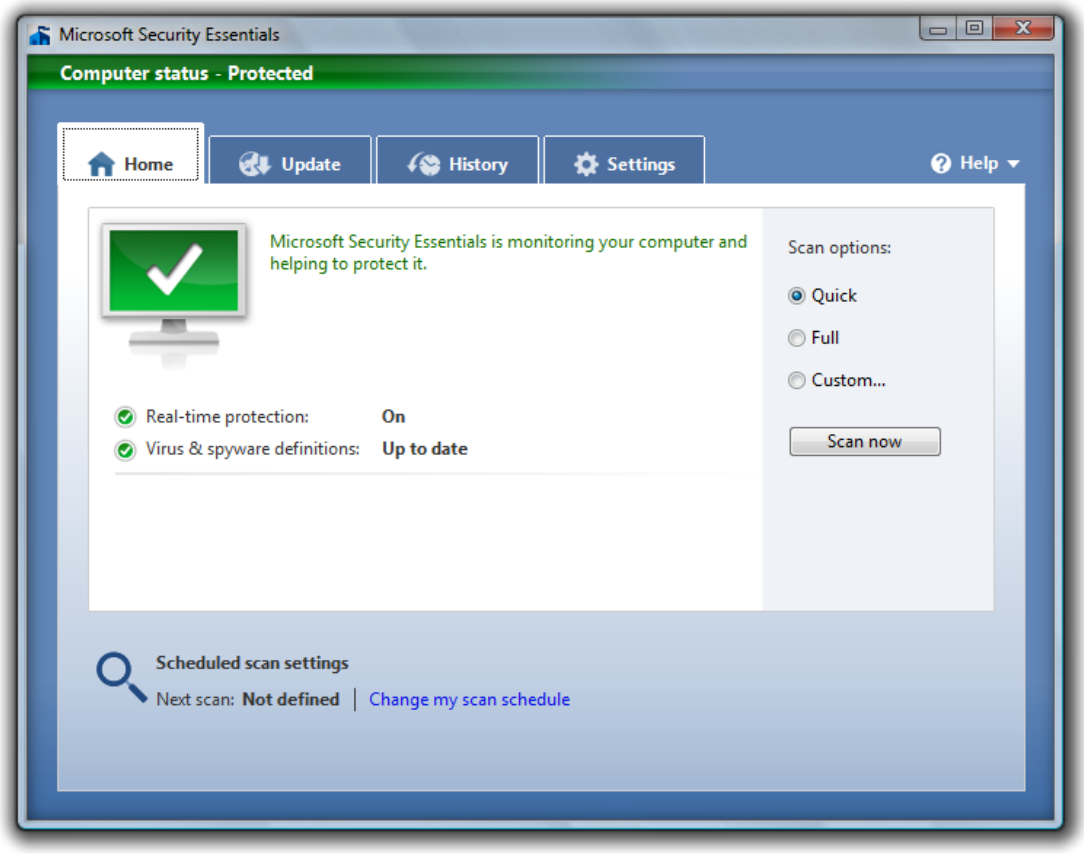


Figure 02-33: Microsoft Security Essentials

Windows Security Tools: Keepass Password Safe Portable

Source: http://www.portableapps.com

KeePass is a free open source **password manager**, which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one **master key** or a key file. So you only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known **AES** and **Twofish**. The main features of the tool include:

- It allows the user to securely carry email, Internet, and other passwords with him or her.
- A user can put all **passwords in one database**, which is locked with a master key or key disk.
- A user can place this application on a USB flash drive, iPod, portable hard drive, or CD.

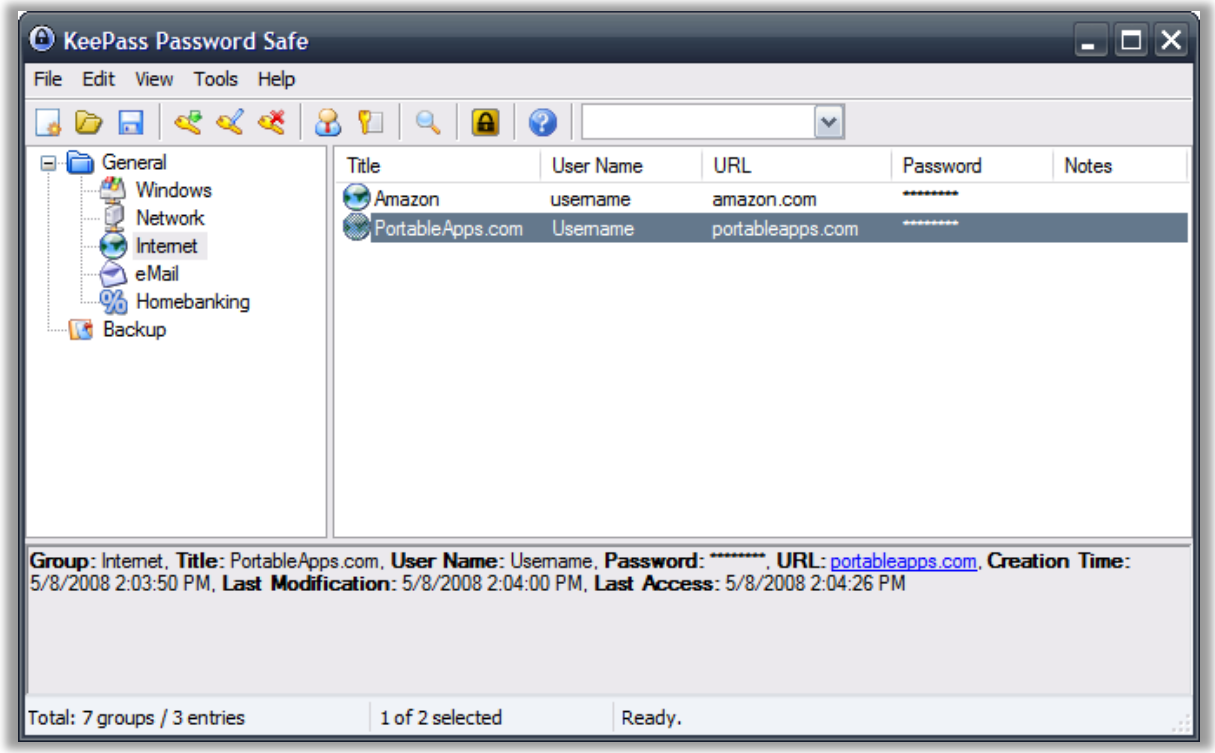


Figure 02-34: Keepass Password Safe Portable Tool Screenshot

Windows Security Tools: Registry Mechanic

Source: http://www.pctools.com

Registry Mechanic offers easy-to-use optimization tools to speed up and improve the stability of your Windows system. Regardless of your level of expertise, Registry Mechanic safely cleans, repairs, and optimizes the registry and automatically backs up changes for future recovery. It now includes essential tools to **fix Windows security loopholes**. Permanently erase your Internet activity, personal files, and free space to keep your information away from prying eyes.

Main features of Registry Mechanic include:

- **Increased speed** for your PC and improvement in your Windows® 7 Windows Vista®, and Windows XP experience
- **Optimized performance** by scanning and repairing invalid registry entries to fix freezes, crashes, and slowdowns
- Removal of orphaned registry references to **improve performance** and **stability**.
- Options to boost system speed provided by Performance Monitor
- Organized and compact registry to increase system efficiency.
- An assessment by the System Monitor of your PC's start up and shut down times, **highlighting potential issues**
- Tune up services that optimize your PC performance and provide better start-up times by turning off non-essential Windows services.
- Customizable ignore lists, which allow you to prevent specific items from being detected and repaired

Figure 02-35: Registry Mechanic Tool Screenshot

Guidelines for Securing Mac OS X

Step 1: Enabling and locking down the Login Window

Steps to enable and lock down the login window include:

- Click **Apple** menu → **System Preferences** → **Accounts** → **Login Options** → **Display Login Windows as** → **Name and Password**
- Uncheck **Automatically login** and:
  - Check **Hide the Sleep**, **Restart** and **Shut Down** buttons
  - Uncheck **Enable fast users switching** if not used

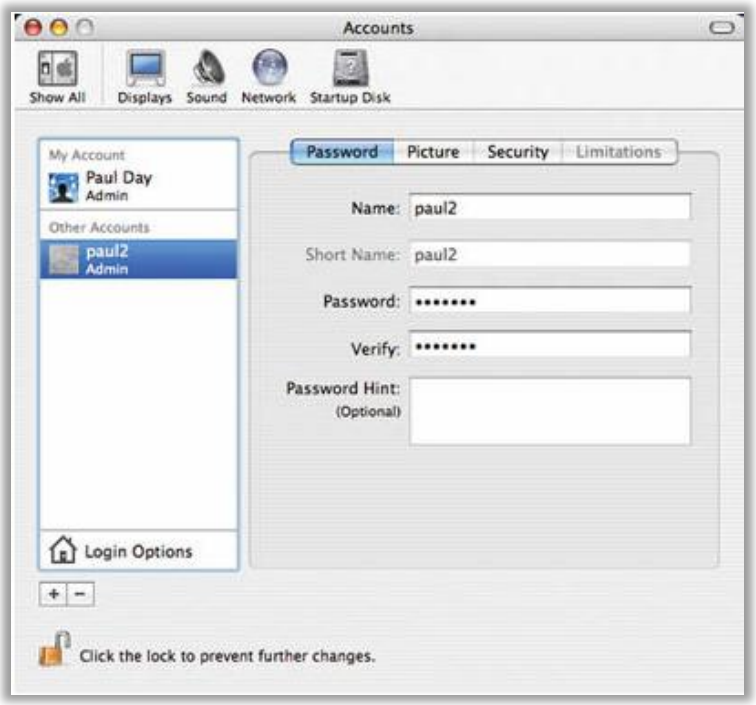


Figure 02-36: Enabling and Locking Down the Login Window

Step 2: Configure Accounts Preferences

Steps for configuring Accounts preferences include:

- From the **Apple** menu, choose **System Preferences.** From the **View** menu, choose **Accounts** and select the **user name** whose password you want to change.
- Click **Reset Password** (Mac OS X v10.3 and v10.4) or **Change Password** (Mac OS X v10.5 or later).

- Enter a new password in both the **Password** and **Verify** fields. Click **Reset Password** (Mac OS X v10.3 and v10.4) or **Change Password** (Mac OS X v10.5 or later).
- If a dialog box appears with the message **Your Keychain password will be changed to your new account password**, click **OK.**

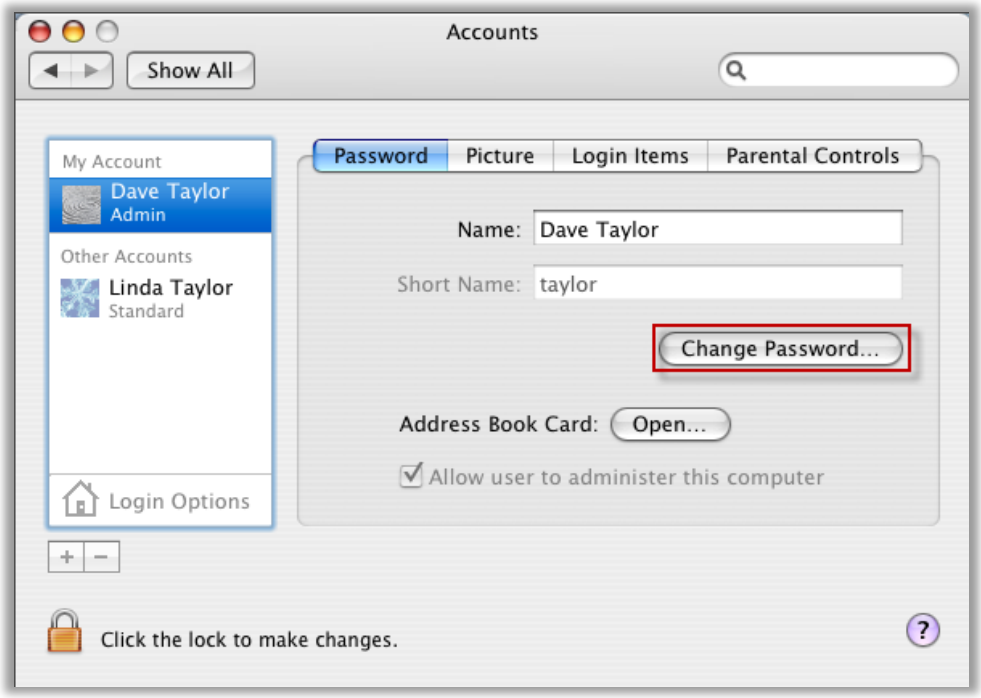


Figure 02-37: Configuring Account Preferences

Step 3: Guidelines for Creating Accounts

Guidelines for creating accounts include:

- Never create accounts that are shared by several users.
- Each user should have his or her standard or managed account.
- Individual accounts are necessary to maintain accountability.
- Administrator users should only use their **administrator accounts** for administrator purposes.

Step 4: Securing the Guest Account

To secure a guest account:

- The guest account must be used for temporary access to the system.

- The guest account should be **disabled by default** as it does not require a password to login on the computer.
- If the guest account is enabled, enable **parental controls** to limit what the user can do.
- If the user permits the guest account to **access shared folders**, then an attacker can easily attempt to access shared folders without a password.

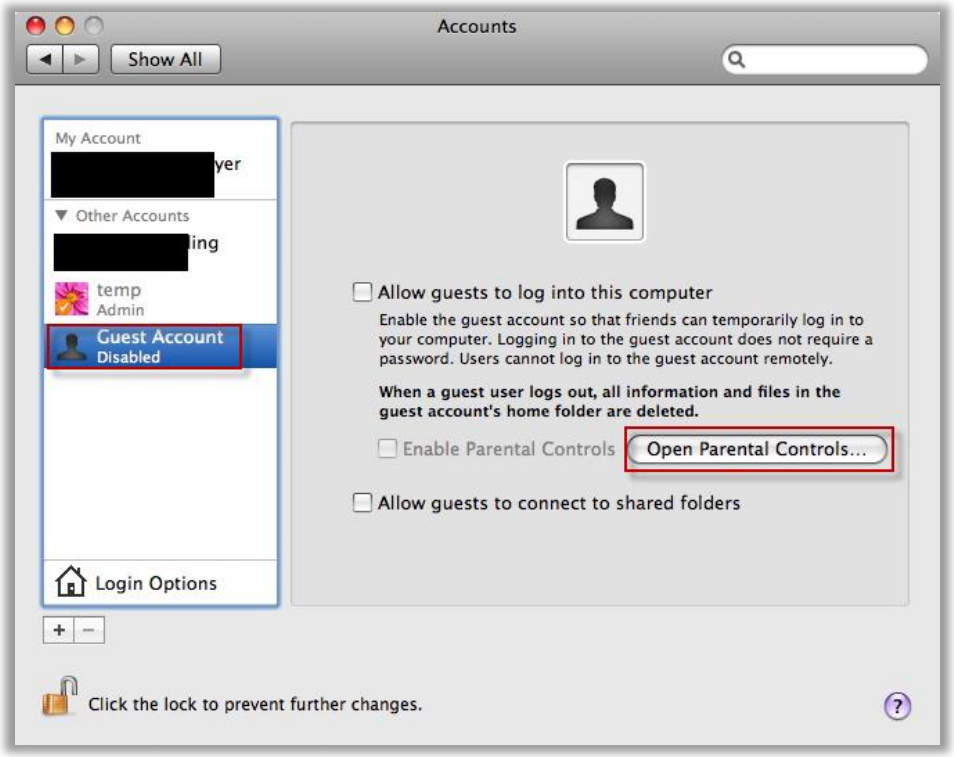


Figure 02-38: Securing the Guest Account

Step 5: Controlling Local Accounts with Parental Controls

For a user to control local accounts and parental controls:

- Open the **System Preferences** and click **Accounts.**
- If the lock icon is locked, click the lock icon and enter the **Administrator** name and **Password.**
- Select the user account to be managed with parental controls and check the **Enable Parental Controls** box.
- Click **Open Parental Controls…**, click **System**, **Content**, **Mails & other messages**, **Time Limits**, and the number of logs.

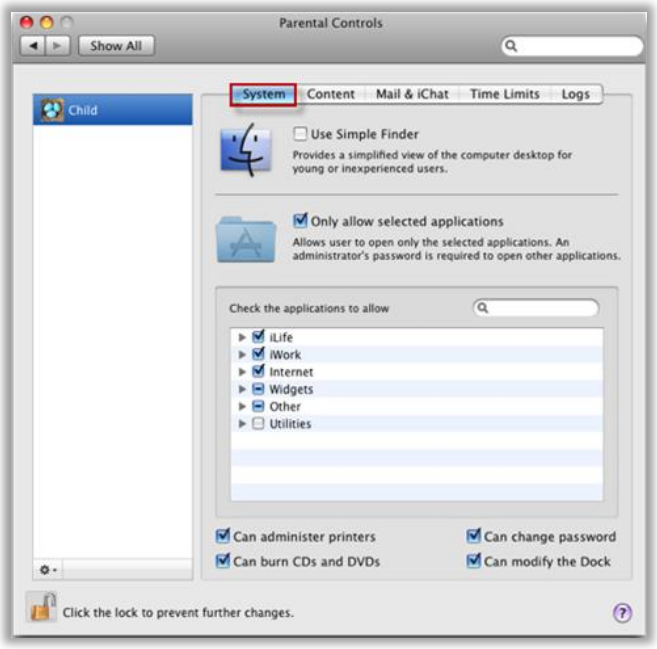


Figure 02-39: Controlling Local Accounts with Parental Controls

Step 6: Use Keychain Settings

Steps to configure Keychain settings include:

- A keychain stores passwords on a disk in an encrypted form and it is difficult for a non-root user to sniff a password between applications.
- Click **Applications → Utilities → Keychain Access → Edit → Change settings** for keychain "login."
- Check **Lock after**, change **minutes of inactivity** to desired minutes, check **Lock when sleeping**, and click **Save**.

Figure 02-40: Change Keychain Settings

Step 7: Use Apple Software Update

Mac OS X includes an automatic software update tool to patch the majority of Apple applications. Software update often includes important security updates, which should be applied to the user's machine. To navigate the software update:

- Open **Software Update** preferences and click the **Scheduled Check** pane.
- Check **Download important updates automatically** and **Check for updates**.

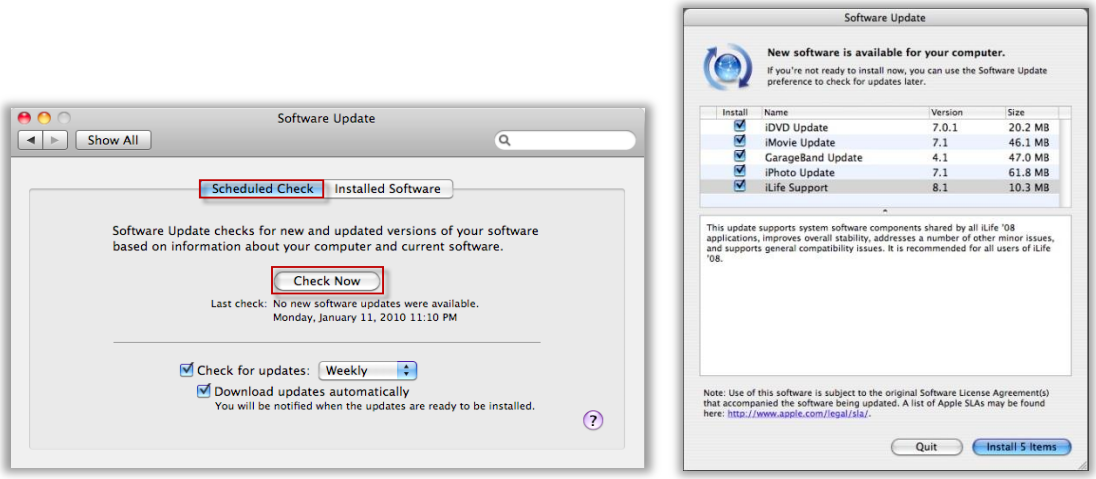


Figure 02-41: Apple Software Update

Step 8: Securing Date & Time Preferences

A user can secure the date and time as follows:

- Open **Date & Time preferences.** In the **Date & Time** pane, enter a secure and trusted NTP server in the **Set date & time automatically** field.
- Click the **Time Zone** button → Choose a **Time Zone**

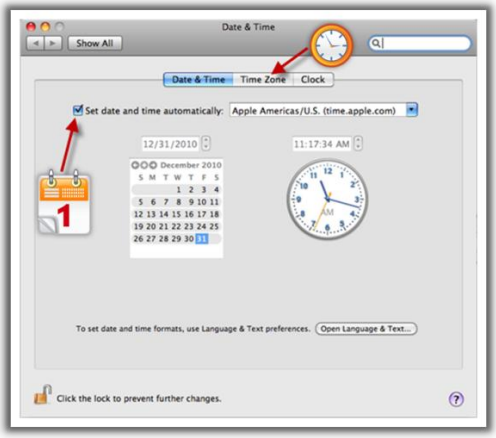


Figure 02-42: Securing Date & Time Preferences

Step 9: Securing Network Preferences

Securing the Network preferences prevents intrusions or attacks.

- It is recommended to disable unused hardware devices listed in Network preferences.
- Open **Network preferences**. From the list of hardware devices, select the hardware device that connects the network.
- From the **Configure** pop-up menu, choose **Manually**.
- Enter the user's static IP address, subnet mask, router, DNS server, and search domain configuration settings.
- Click **Advanced**. In the Configure **IPv6** pop-up menu, choose **Off** and then click **OK**.

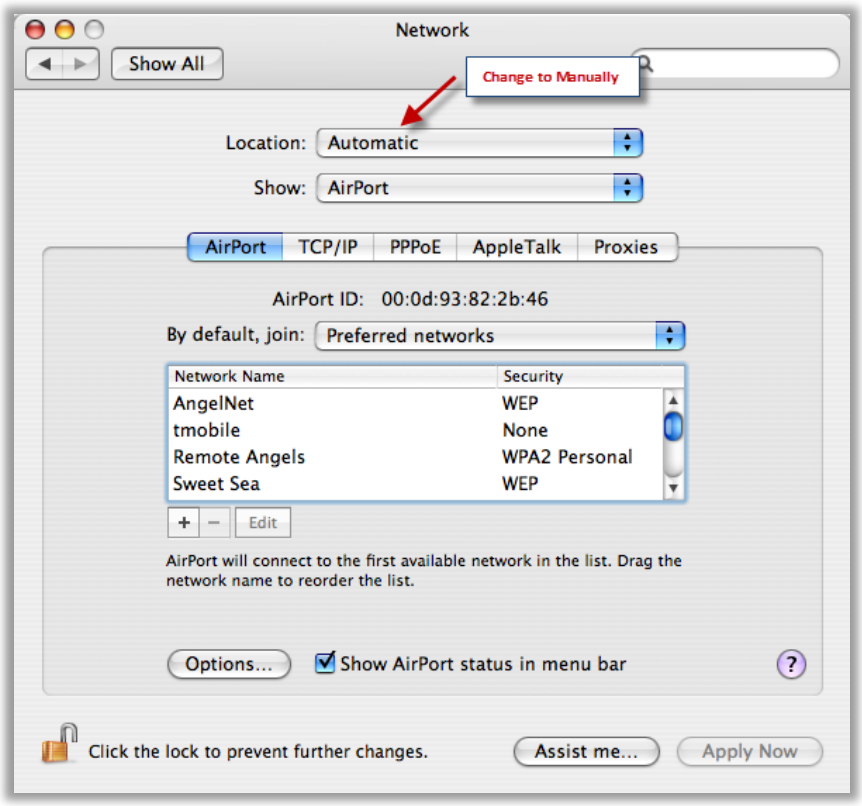


Figure 02-43: Securing Date & Time Preferences

Step 10: Enable Screen Saver Password

To prevent unauthorized access to a system, enable a screen saver password.

- From the **Apple** menu, select **System Preferences**, click **Security**, and click the **Lock** icon to make changes.
- If prompted, type the **admin user name** and **password**.

- In the **Security** window, click the **General** tab and check **Require password to wake this computer from sleep or screen saver** (Leopard) or **Require password immediately after sleep or screen saver begins** (Snow Leopard).
- In addition to the screen saver password, also secure the system by selecting:
  - **Disable** automatic login
  - Require password to **unlock** each System Preference
  - Use secure virtual memory
  - Click the lock icon to prevent further changes
  - Close the **Security** window and restart your machine

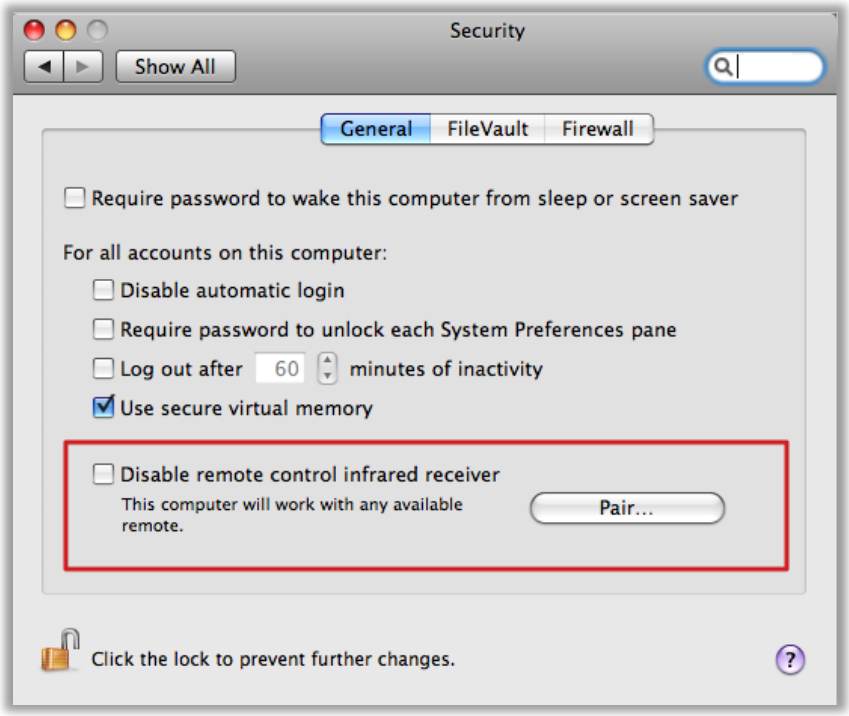


Figure 02-44: Enabling Screen Saver Password

Step 11: Set Up FileVault to Keep Home Folder Secure

Steps to set up FileVault include:

- Click **System Preferences → Security → FileVault → Set Master Password**.
- Create the master password for the computer, but ensure that this password is different from the user account password.
- Verify the password and click **OK.**

Figure 02-45: Set Up FileVault to Keep Home Folder Secure

Step 12: Firewall Security

Firewall should be used to block unauthorized programs from accepting new network connections. To improve the firewall security:

- Click **System Preferences → Security → Firewall.**
- Click the l**ock** icon to make changes.
- If prompted, type the **admin user name** and **password.**
- By default, the firewall **allows all incoming connections,** change the option by clicking the second (**Allow only essential services**) or third option (**Set access for specific services and applications**).
- Now choose which application(s) you want the firewall to allow and which to block block.
- Click the lock icon to prevent further changes and close the **Security** window.

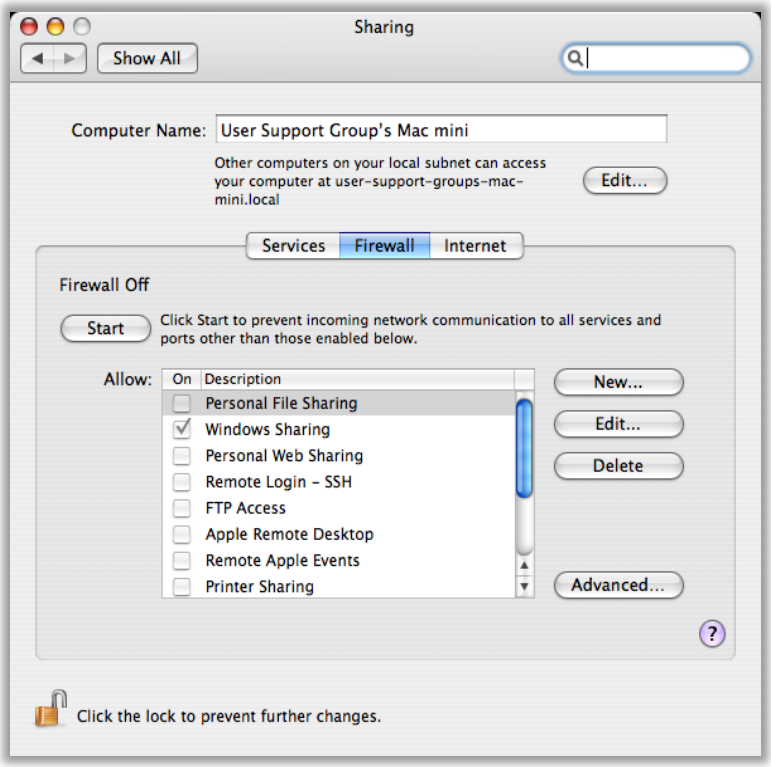


Figure 02-46: Firewall Security

Module Summary

Attackers discover new vulnerabilities and bugs to exploit in computer software.

Software vendors usually develop patches to address the problems.

Encryption is the process of converting data into a secret code.

Regularly update the operating system and other applications.

Windows System Restore is used to return a computer to an earlier state in case of a system failure or another major problem with the system.

Microsoft Security Essentials provides real-time protection for the PC that guard against viruses, spyware, and other malicious software.

Windows Defender helps to protect the system against pop-ups, slow performance, and security threats.

Operating Systems Security Checklist

Operating system security checklist includes:

- ☐ Regularly update the operating system and other applications.
- ☐ Install antivirus software and scan the system regularly.
- ☐ Do not open any emails that are sent by unknown individuals.
- ☐ Perform an antivirus scan while downloading.
- ☐ Lock the system when not in use.
- ☐ Physically secure the system from unauthorized access.
- ☐ Enable firewall protection and configure all computer settings for high security.
- ☐ Use strong passwords, at least eight characters long containing both letters and numbers.

Operating Systems Security Checklist

Operating system security checklist includes:

- ☐ Configure antivirus to check all mediums (floppy disk, CD-ROMs, email, websites, downloaded files, etc.) for viruses.
- ☐ Delete the Internet history files, logs, and personal files and use encryption to enhance privacy.
- ☐ Make backups of important data and store them safely.
- ☐ Limit the number of unnecessary accounts.
- ☐ Keep up to date with hot fixes and service packs.
- ☐ Disable **AutoRun** for the DVD/CD-ROM.
- ☐ Secure the wireless network.

Security Checklist for Windows 7

Windows 7 operating system security checklist includes:

- ☐ Use Windows Defender to help prevent spyware and other potentially unwanted software from being installed on the computer automatically.
- ☐ User Account Control asks for permission before installing software or opening certain kinds of programs that could potentially harm your computer or make it vulnerable to security threats.
- ☐ Back up your files and settings regularly so that, if you get a virus or have any kind of hardware failure, you can recover your files.
- ☐ Set Windows Update to download and install the latest updates for the computer automatically.
- ☐ Windows Firewall can help prevent hackers and malicious software, such as viruses, from gaining access to your computer through the Internet.
- ☐ Use Action Center to ensure that the firewall is *on*, antivirus software is up to date, and the computer is set to install updates automatically.

MAC OS Security Checklist

Here is a checklist for securing a system that runs on MAC OS:

- ☐ Securely erase the Mac OS X partition before installation.
- ☐ Set parental controls for managed accounts.
- ☐ Use Password Assistant to generate complex passwords.
- ☐ Securely configure Accounts preferences.
- ☐ Install Mac OS X using Mac OS Extended disk formatting.
- ☐ Securely configure Date & Time preferences.
- ☐ Create an administrator account and a standard account for each administrator.
- ☐ Create a standard or managed account for each non administrator.
- ☐ Create Keychains for specialized purposes.
- ☐ Securely configure Security preferences.

This page is intentionally left blank.