

Securing Your Windows XP Computer

This document contains the following sections:

- [Step 1: Download & Install Symantec AntiVirus for Desktops](#)
- [Step 2: Run Microsoft Update](#)
- [Step 3: Configure Windows Firewall](#)
- [Step 4: Disable Simple File Sharing](#)
- [Step 5: Secure Your Accounts and Passwords](#)
- [Step 6: Enable a Screen Saver Password](#)
- [Step 7: Configure Windows Event Logs](#)
- [Step 8: Configure Local Security Auditing Policies](#)
- [Other Security Tips](#)
- [Advanced Steps](#)

For information related to this topic refer to:

- [Security Definitions](#)
(<http://www.cmu.edu/computing/doc/security/general/definitions.html>)
- [Security: General Practices](#)
(<http://www.cmu.edu/computing/doc/security/general/index.html>)
- [Symantec Anti-Virus](#)
(<http://www.cmu.edu/computing/doc/software/virus-windows/index.html>)
- [Encryption](#) (<http://www.cmu.edu/computing/doc/security/encrypt/index.html>)
- [Managing Your Andrew Password](#)
(<http://www.cmu.edu/computing/doc/accounts/passwords/index.html>)
- [System Restore](#) (<http://www.cmu.edu/computing/doc/security/restore/index.html>)
- [Information Security Office \(ISO\)](#) (<http://www.cmu.edu/iso/>)

Step 1: Download & Install Symantec Endpoint Protection for Desktops

Carnegie Mellon owns a volume license for Symantec Endpoint Protection which is our licensed, supported and recommended solution for virus protection. Beginning with version 10.0.1, Symantec also guards against Spyware.

When kept current, Symantec Endpoint Protection detects viruses, trojans, some worms and spyware as they appear on your hard drive and alerts you so that you are aware that your machine has been infected. You should always keep your antivirus software up-to-date to avoid any problems. Please note, anti-virus software does not protect you against break-ins. For more information on these terms, see the [Definitions](http://www.cmu.edu/computing/doc/security/general/definitions.html) (<http://www.cmu.edu/computing/doc/security/general/definitions.html>) section of the *Securing Your Computer: General Practices* (<http://www.cmu.edu/computing/doc/security/general/index.html>) document.

IMPORTANT: If you have a new machine, any anti-virus software that was included when you purchased it is most likely a trial package that is set to expire in three months. Once the software expires and you can no longer receive the continuous updates, the virus definition file quickly becomes outdated.

To ensure that your machine is protected you will want to download a copy of [Symantec Endpoint Protection](http://www.cmu.edu/computing/doc/software/virus-windows/index.html) (<http://www.cmu.edu/computing/doc/software/virus-windows/index.html>) software from Computing Services [Software](http://www.cmu.edu/computing/software/all/index.html) (<http://www.cmu.edu/computing/software/all/index.html>) page. For detailed instructions, read the [Download and Install](http://www.cmu.edu/computing/doc/software/virus-windows/install.html) (<http://www.cmu.edu/computing/doc/software/virus-windows/install.html>) section of the *Symantec Endpoint Protection* document.

Run Live Update

Virus definitions change daily. To fully protect your computer, you need to download the latest virus definition files by running **LiveUpdate**. The Carnegie Mellon installation of Symantec Endpoint Protection is pre-configured to run LiveUpdate daily. In addition, the software is configured with **File System Auto-Protect** enabled. Read the [Symantec LiveUpdate](http://www.cmu.edu/computing/doc/software/virus-windows/live-update/index.html) (<http://www.cmu.edu/computing/doc/software/virus-windows/live-update/index.html>) document for details.



Step 2: Run Microsoft Update

Last Updated: 8/17/09

Step 2: Run Microsoft Update

Load Service Packs

Windows users should be aware of which version of the operating system they are running and should update to the latest Service Pack. To determine which Service Pack is installed on your computer and to download the latest Service Pack, visit the ISO [Microsoft Windows Security Patches and Updates](http://www.cmu.edu/computing/security/ms-update.html) (<http://www.cmu.edu/computing/security/ms-update.html>) page.

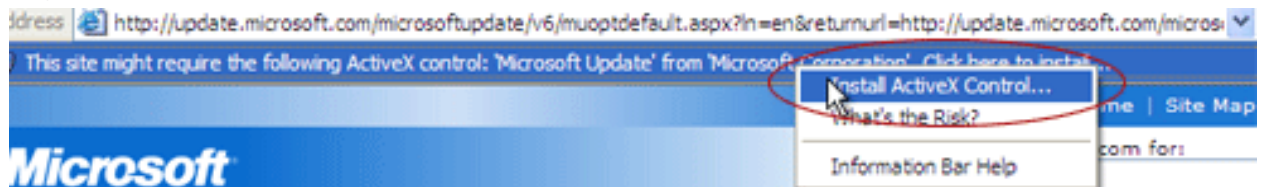
Upgrade to Microsoft Update

Microsoft developed Microsoft Update to install Windows and Office patches via the web making it easier to keep Microsoft products up-to-date.

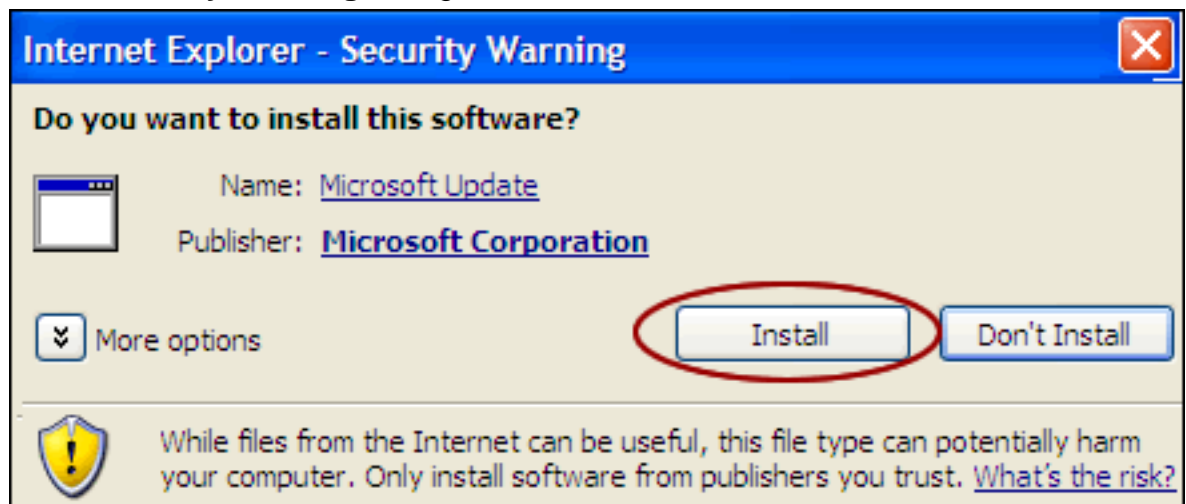
The following steps will upgrade Windows Update to Microsoft Update:

IMPORTANT: You MUST use Internet Explorer to use Microsoft Update.

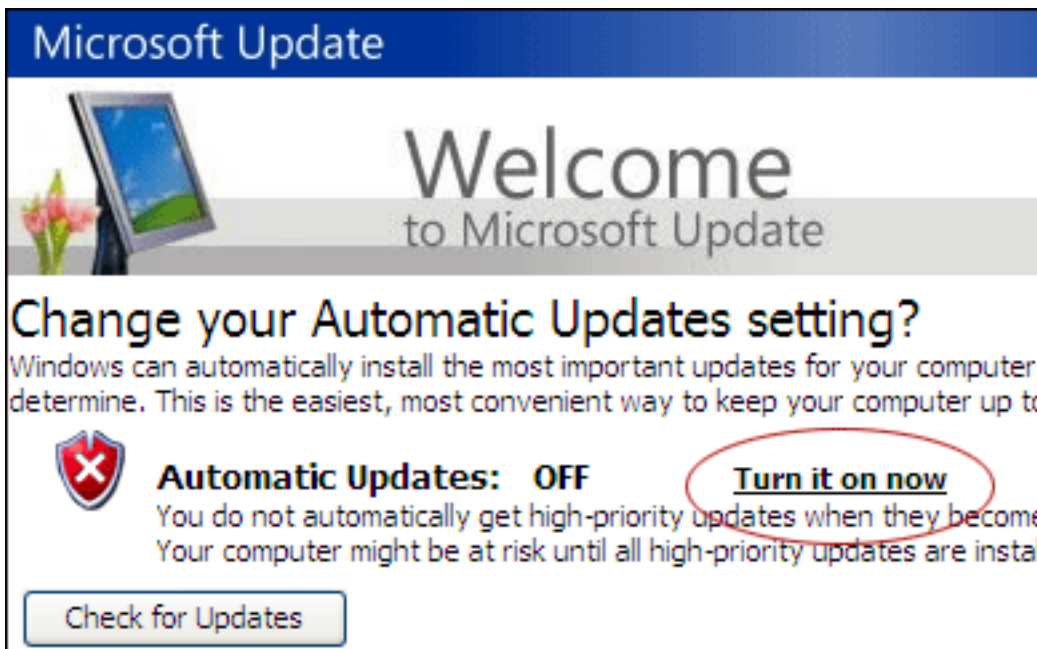
1. Open Internet Explorer.
2. In the **Address Bar** type <http://update.microsoft.com/microsoftupdate> (<http://update.microsoft.com/microsoftupdate>) (Microsoft Update web page).
3. If prompted, install the Microsoft Update ActiveX control.
 - Right-click the **Information Bar** (below the Address Bar).



- Select **Install ActiveX Control** from the pop-up menu.
- In the **Security Warning** dialog box, click **Install**.



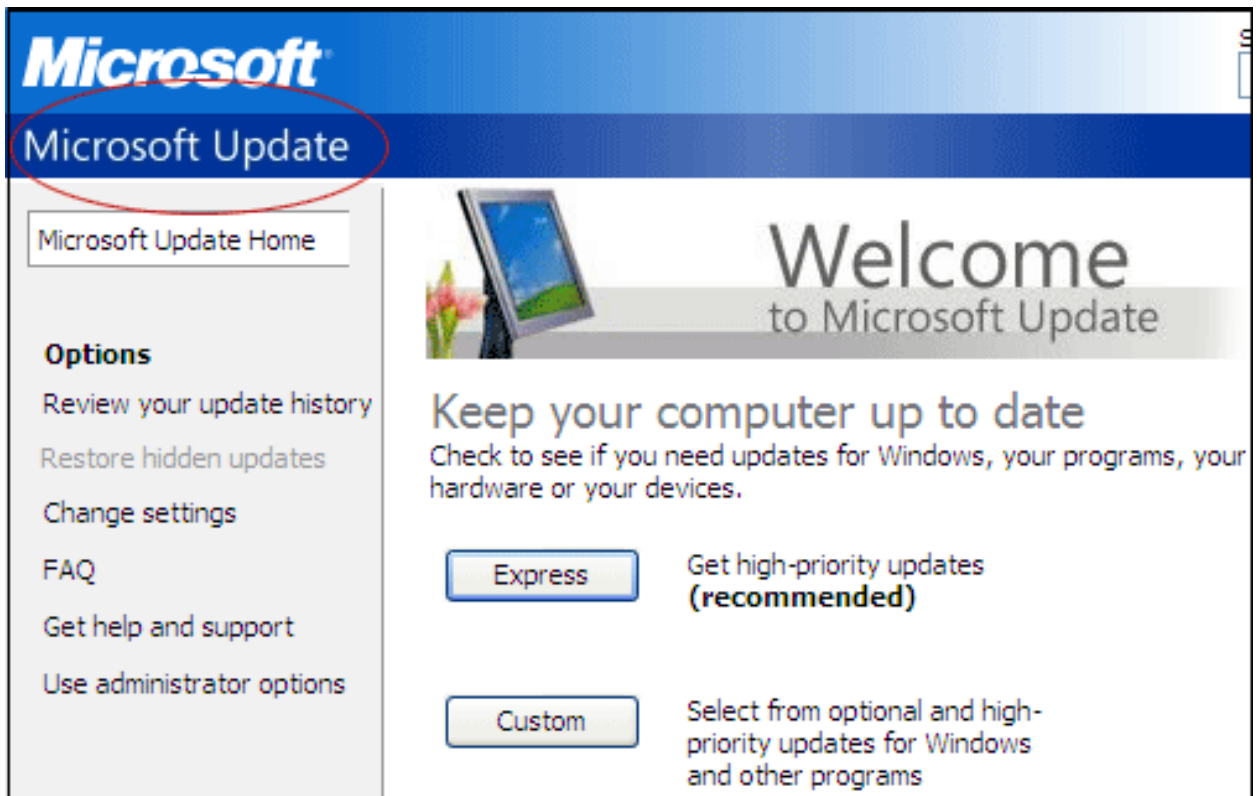
4. If you haven't already configured your computer for automatic updates, "Change your Automatic Updates setting" appears. Click **Turn it on now**.



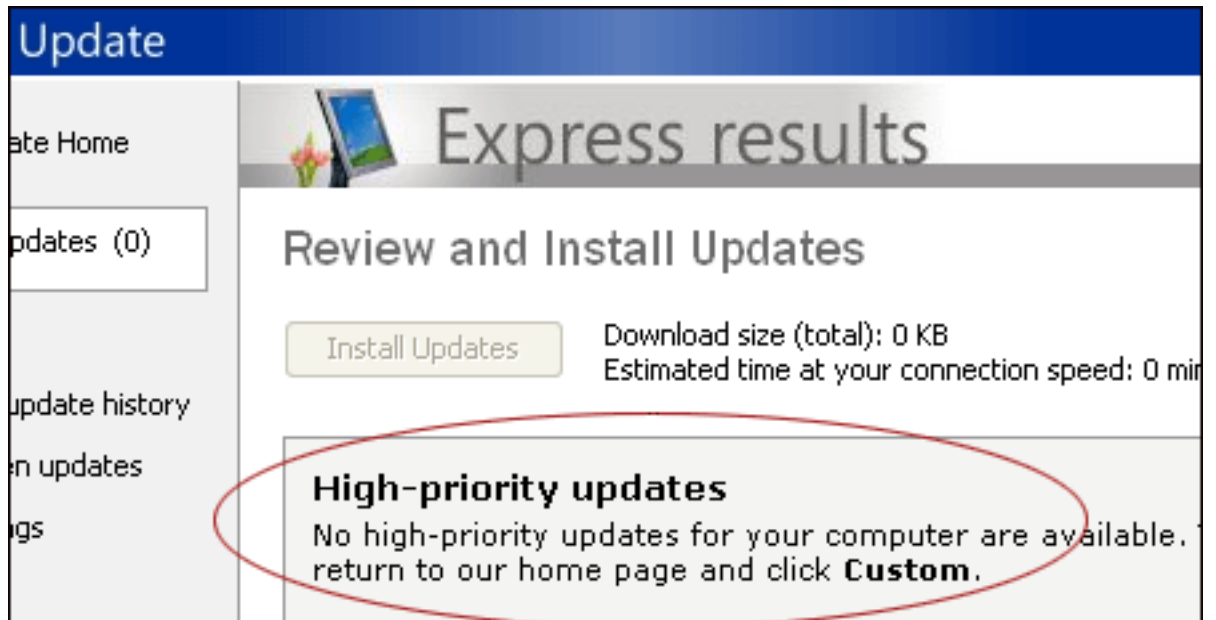
5. The Automatic Update window appears. Under Install new updates, select **Every day**. Be sure to select a time when your computer is turned ON and has Internet access.
6. The "Microsoft Update setup is complete" window appears. Click the **Check for Updates** button. Continue with the Run Microsoft Update steps below.

Run Microsoft Update

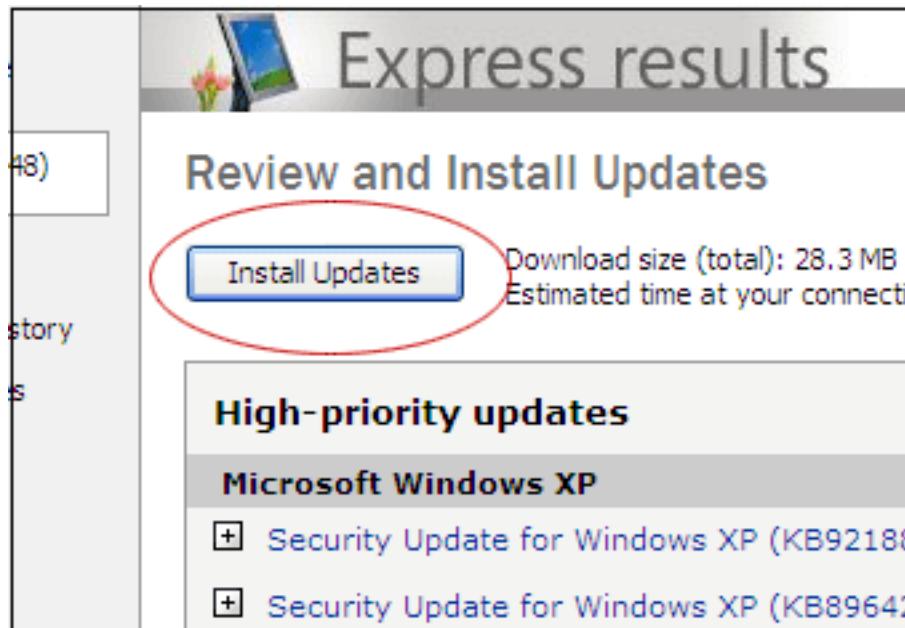
1. A **Microsoft Update** screen appears (similar to the following) select **Express** to update Microsoft Office AND the Microsoft operating system.



2. The program scans your system to determine which updates you need to install. Once the program finishes scanning, one of the following appears:
- A message that "No high-priority updates for your computer are available...". If this message appears, you're done! Your computer is up to date.



- A list of updates that you need to install. If this list appears, click **Install Updates**. The program will hang for a few moments as the updates are installed.



IMPORTANT NOTE: If you have a high number of priority updates to install, you may be prompted to reboot your system between updates. To assure that ALL AVAILABLE updates have been installed:

- o Relaunch Internet Explorer
- o Revisit the [Microsoft Update \(http://update.microsoft.com/microsoftupdate\)](http://update.microsoft.com/microsoftupdate) web page
- o Select **Express**. If the "No high-priority updates for your computer are available..." message appears. You're done. If the Install Updates

message appears again, click **Install Updates**. Repeat the process until there are no high-priority updates.



Step 3: Configure Windows Firewall

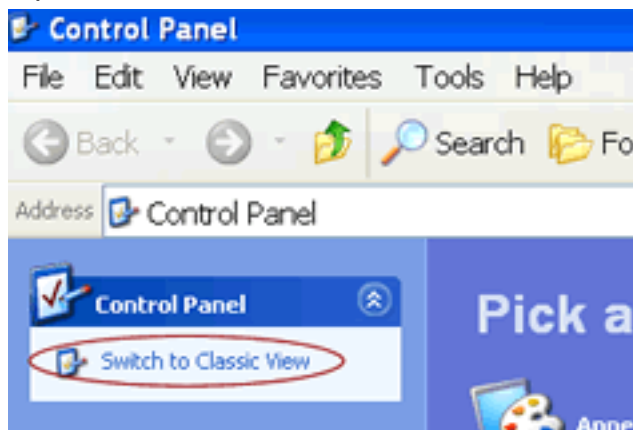
Last Updated: 4/1/09

Step 3: Configure Windows Firewall

A firewall is a system designed to reinforce the security of the data flowing between two networks, the internal network and the outside network, such as the Internet. It's important to note that enabling a firewall may break some applications that use non-standard or uncommon ports. For these applications, you can relax the firewall settings and enable exceptions. For more information on these terms, see [Securing Your Machine: Definitions \(http://www.cmu.edu/computing/doc/security/general/definitions.html\)](http://www.cmu.edu/computing/doc/security/general/definitions.html).

Follow these steps to configure the firewall:

1. Click **Start > Control Panel**.
 - If "Switch to Classic View" appears in the top-left of the window, select it to reveal the control panel.

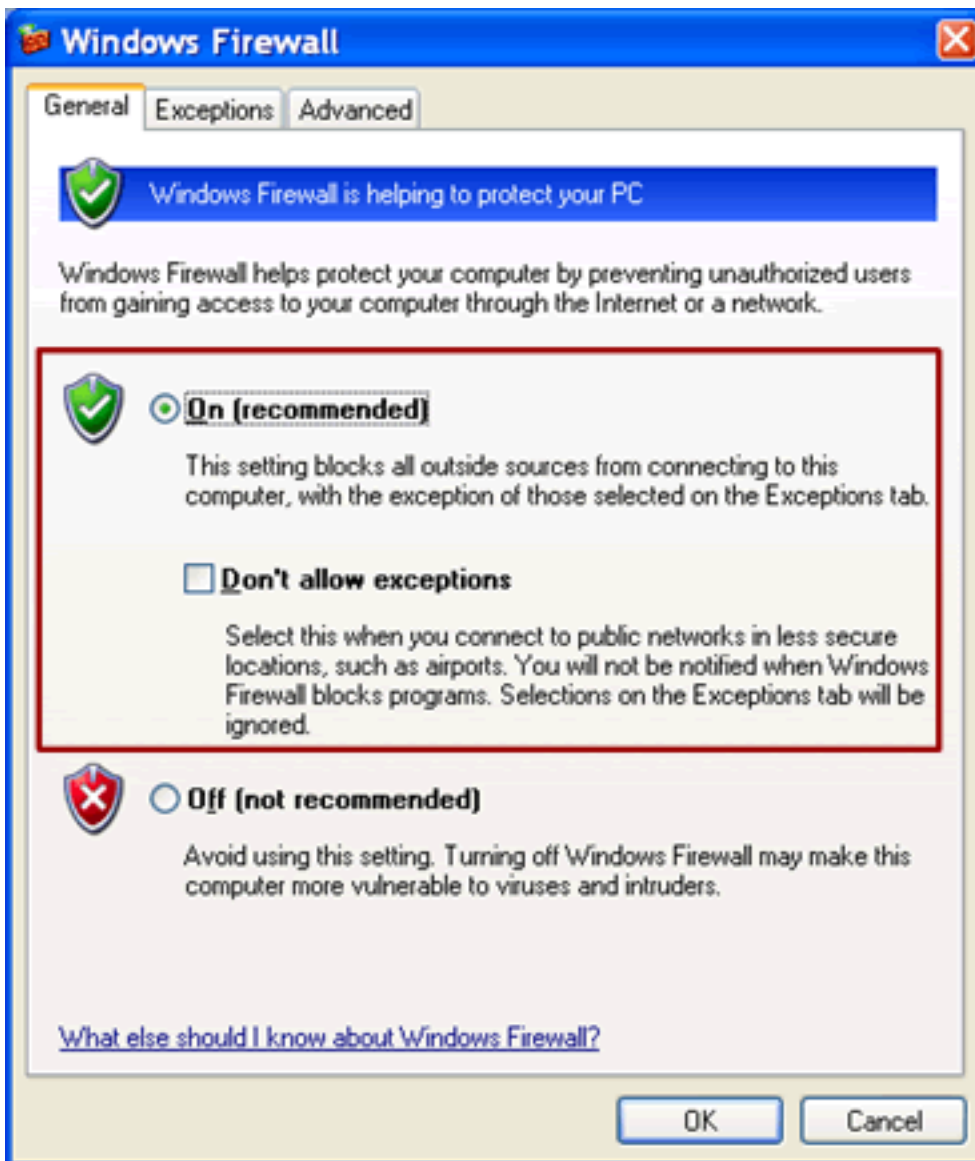


2.

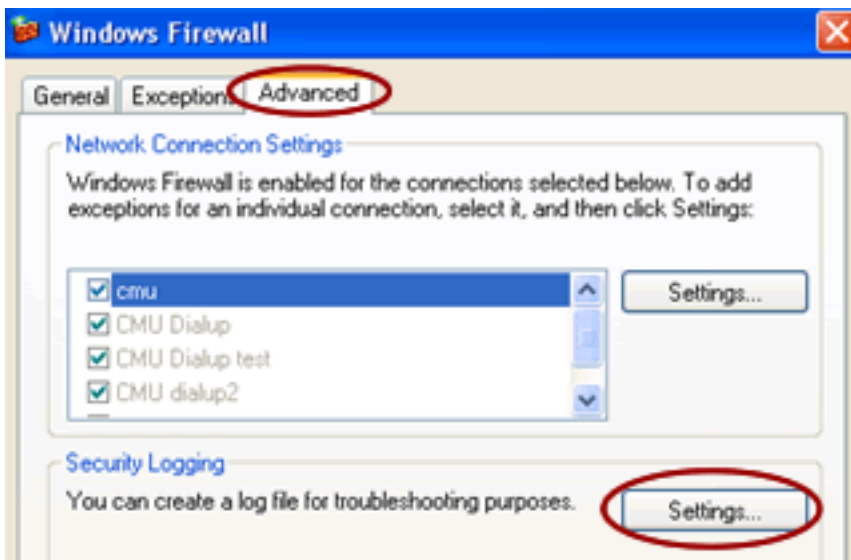


Double-click **Windows Firewall**. Windows Firewall
The Windows Firewall window appears.

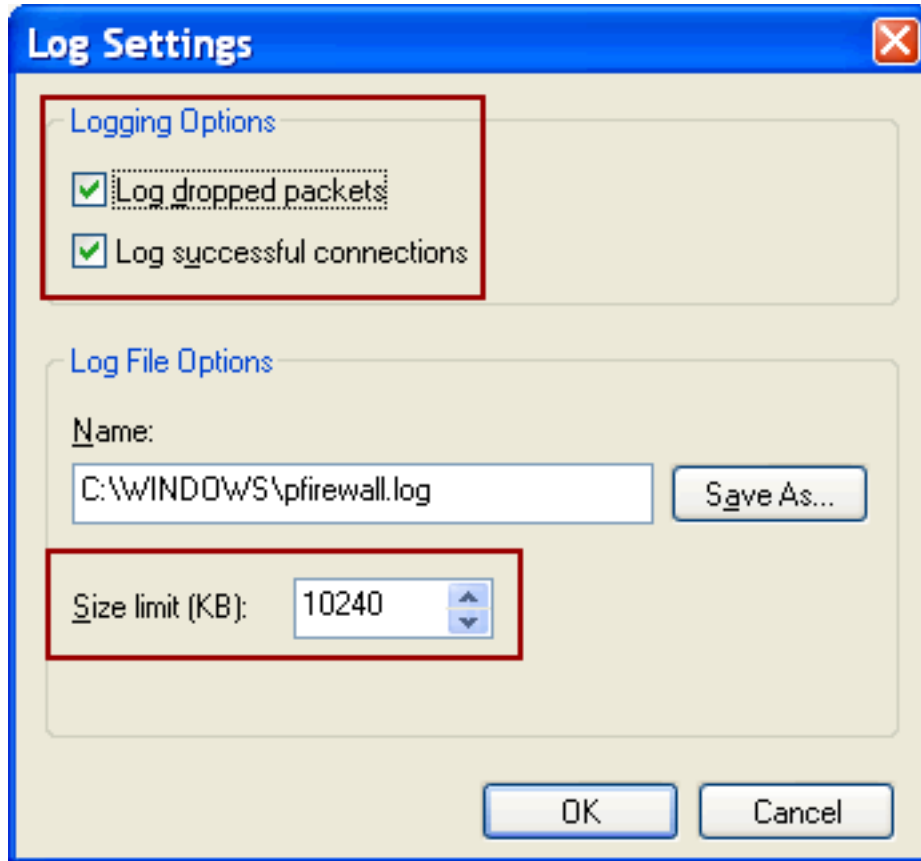
3. Uncheck **Don't allow exceptions** and select the **On** radio button.



4. Select the **Advanced** tab.
5. Under **Security Logging**, click the **Settings** button. The Log Settings window will appear.



6. In the Log Settings window
 - Check **Log dropped packets**
 - Check **Log successful connections**
 - Enter **10240** for **Size limit (KB)**:



7. Click **OK** to close the Log Settings window.
8. Select the **Exceptions** tab.

Note: See the [Definitions](http://www.cmu.edu/computing/doc/security/general/definitions.html) (<http://www.cmu.edu/computing/doc/security/general/definitions.html>) page for exception details.
9. Do the following:
 - Uncheck any program or service you **DO NOT** wish to accept incoming network connections.
 - Check any program or service you **DO** wish to accept incoming connections.
 - Check **Display a notification when Windows Firewall blocks a program**.

Note: Advanced users, if you need to make changes to a service or program, select the program or service and click the **Edit...** button. A list of common ports can be found in the [Definitions](http://www.cmu.edu/computing/doc/security/general/definitions.html) (<http://www.cmu.edu/computing/doc/security/general/definitions.html>) page.
10. Click **OK** to close the window and save all changes.



Step 4: Disable File Sharing

Last Updated: 01/12/07

Step 4: Disable Simple File Sharing

Simple File Sharing allows users to share folders without a password and may allow malicious attackers to read or write files from your shared folders.

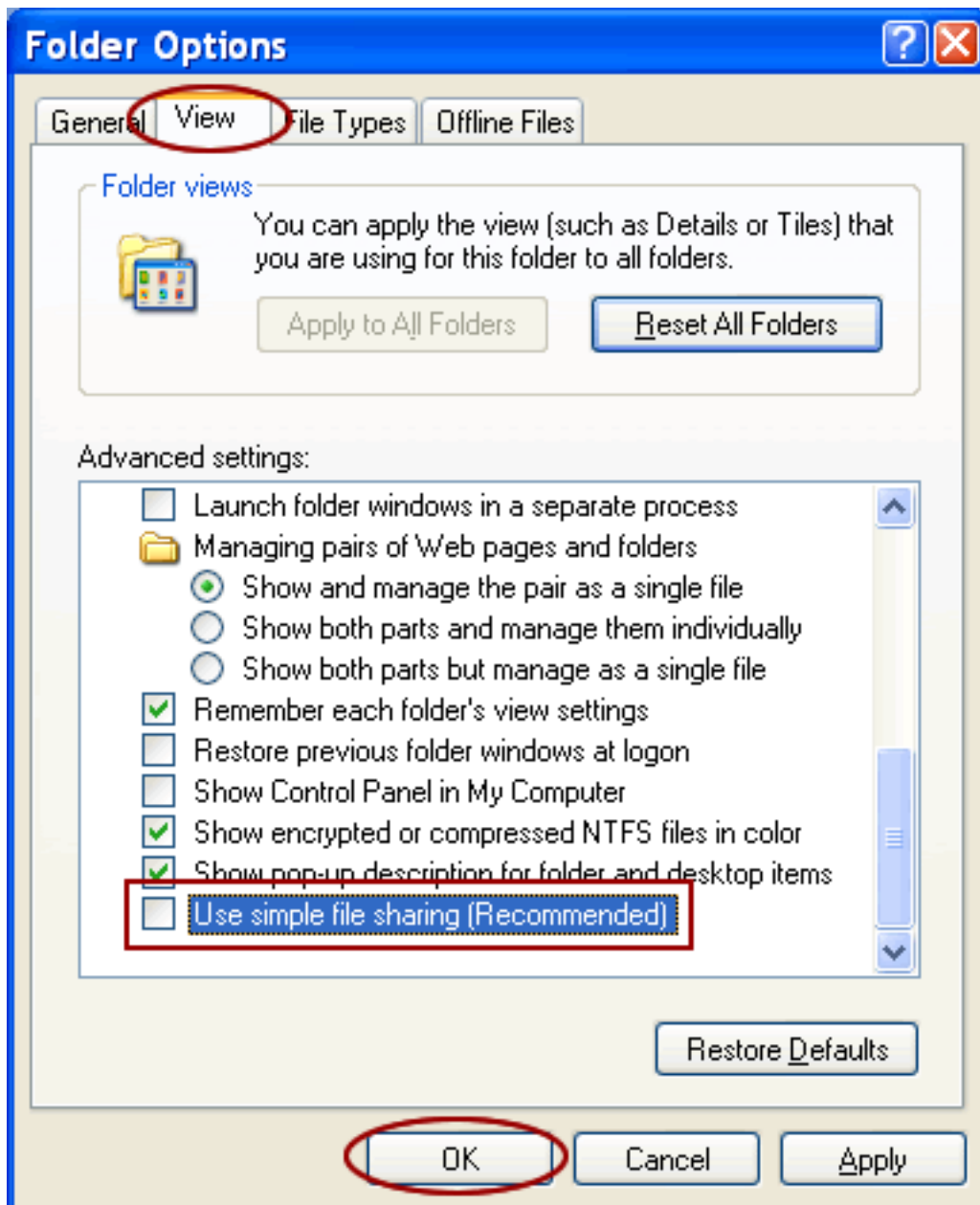
Windows XP Professional only allows you to disable Simple File Sharing and require a userid and password for shared folder access. To disable Simple File Sharing follow these steps:

1. Click **Start > Control Panel**.
- 2.



Double-click **Folder Options**. Folder Options

3. Select the **View** tab.
4. Scroll down in the list and uncheck **Use simple file sharing (Recommended)**.
5. Click **OK**.



Set a Password for File Sharing

If you are going to permit file sharing from your computer, you should always set permissions for the folder being shared. Before sharing a folder, keep these tips in mind:

- Sharing entire drives can be dangerous, especially if you are sharing the C: drive.
- Do not make a network share writable by others.
- It is never a good idea to give Full Control to your share.

For detailed information on sharing folders visit [Microsoft's Folder Permissions Support page](http://support.microsoft.com/default.aspx?scid=kb;en-us;308418&Product=winxp) (<http://support.microsoft.com/default.aspx?scid=kb;en-us;308418&Product=winxp>)



Step 5: Secure Your Accounts and Passwords

Last Updated: 01/12/07

Step 5: Secure Your Accounts and Passwords

You must establish effective passwords for all active accounts. Existing accounts with weak or nonexistent passwords are an invitation for malicious attackers to compromise your system. For tips on selecting an effective password, read *Managing Your Andrew Password* (<http://www.cmu.edu/computing/doc/accounts/passwords/index.html>).

To disable any unused accounts such as "Guest" and to verify that an effective password is set for the Administrator account, follow these steps:

1. Click **Start > Control Panel**.
- 2.



Double-click **User Accounts**. *User Accounts*

The User Accounts dialog box appears.

3. Select the **User Account** you want to set a password for (e.g., Administrator).
4. Click **Change the password** and enter your old and new password.
5. To disable a Guest account, select it in the dialog box and click **Turn off the guest account**.



Step 6: Enable a Screen Saver Password

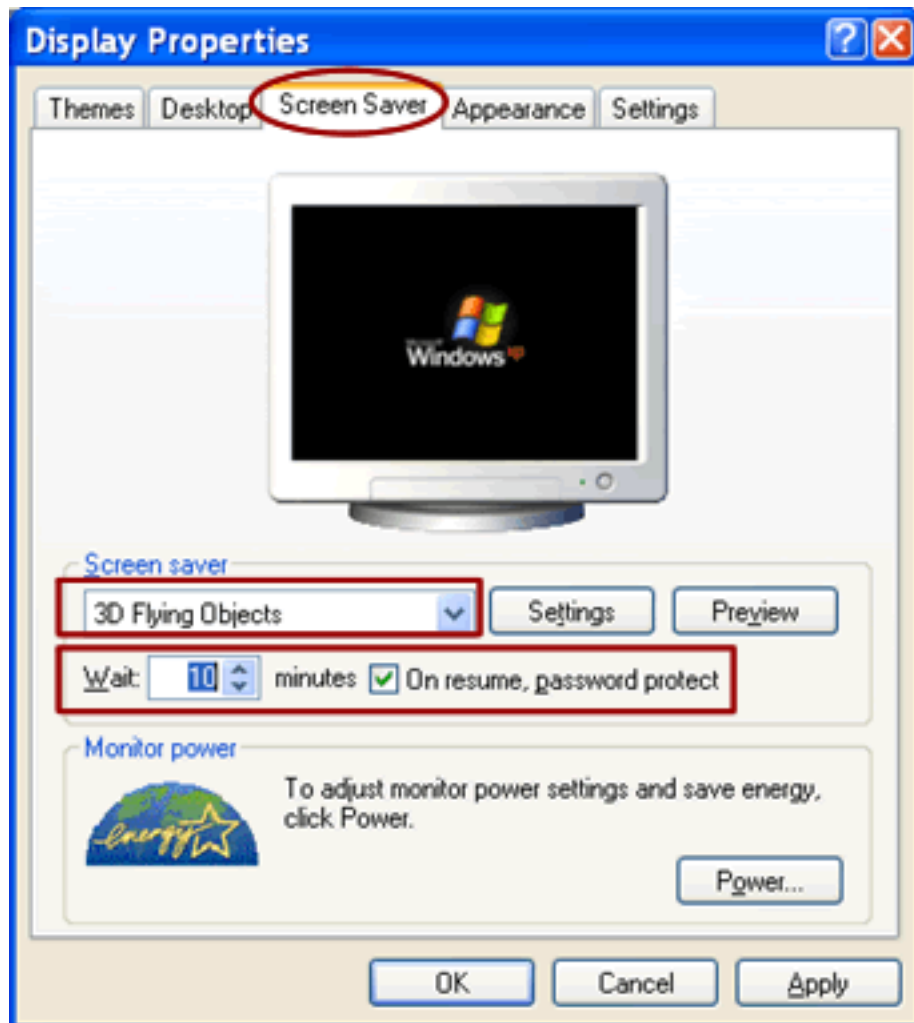
Last Updated: 01/12/07

Step 6: Enable a Screen Saver Password

To prevent someone from using your computer when you have stepped away, you should enable screen saver passwords. Your screen saver password will be your account login password.

Note: The settings for this option are specific to each user account so be sure to set it for each account.

1. Click **Start > Control Panel**.
2. Double-click **Display**.
The Display Properties window appears.
3. Select the **Screen Saver** tab and set the following properties:
 - Select a Screen saver from the drop down menu.
 - Set the **Wait** time to 10 minutes or less.
 - Select (check) **On resume, password protect**.



4. Click **OK**.



Step 7: Configure Windows Event Logs

Last Updated: 01/12/07

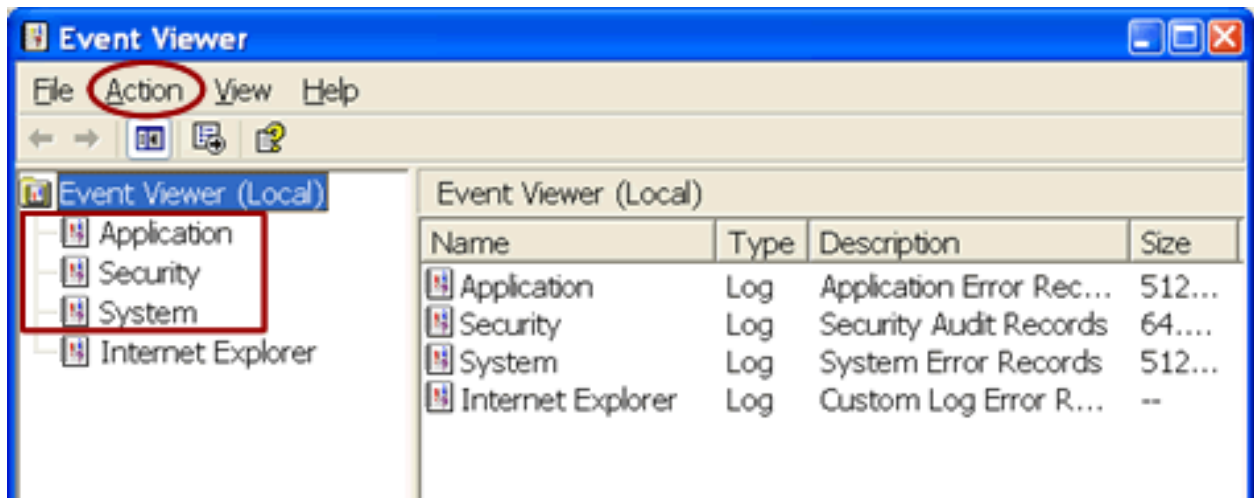
Step 7: Configure Windows Event Logs

Windows records system events, software changes, and some system setting change occurrences in the Windows Event Logs. By default these logs clear events older than 7 days because the log size is too small.

If your computer becomes compromised, keeping more logging information increases the chances that experts will be able to determine how and when the compromise occurred. This information is also useful in diagnosing other system and performance problems.

To increase the log size, follow these steps:

1. Click **Start > Control Panel**.
2. Double-click **Administrative Tools** and then **Event Viewer**.
3. In the left pane, select **Application**.
4. Choose **Action > Properties**.
5. Set the following:
 - **Maximum log size:** 10240KB
 - Select **Overwrite events as needed**
6. Click **OK** to save the settings.
7. Repeat Steps 3 through 7 for **Security** and **System**. Then, close the window.



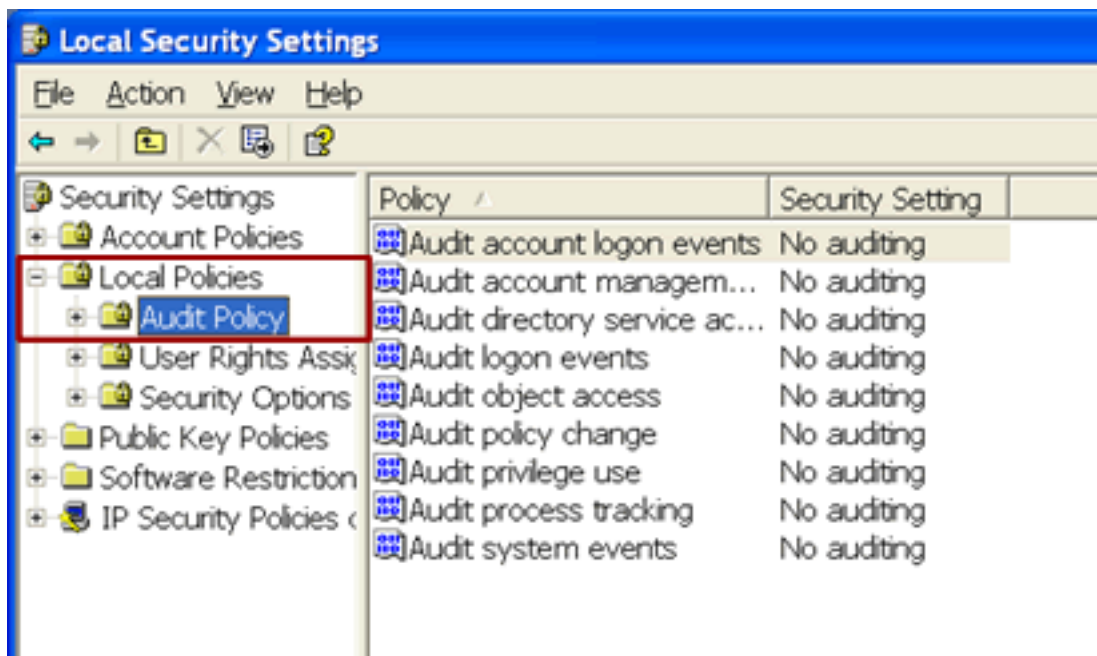
Step 8: Configure Local Security Auditing Policies

Last Updated: 01/12/07

Step 8: Configure Local Security Auditing Policies

Windows XP Professional has the ability to record more security events, but the settings are not enabled by default. Follow these steps to enable additional security event logging:

1. Click **Start > Control Panel**.
2. Double-click **Administrative Tools** and then **Local Security Policy**.
3. In the left pane, select **Local Policies > Audit Policy**.
4. Double-click **Audit account logon events** in the right pane.
5. Under Audit these attempts select (check) **Success** and **Failure**.
6. Click **OK** to save the settings.
7. Repeat Steps 4 through 6 for each **Audit** policy listed in the right pane. Then, close the window.



Note: These steps can not be performed on Windows XP Home Edition.

Once you complete the basic security steps, review the [Additional Security Tips](#) and [Advanced Steps](#) pages.



[Additional Security Tips](#)

Last Updated: 01/12/07

Additional Security Tips

- **Update Other Software**

Security vulnerabilities can exist in all software. Keep your software updated. You will find update information, for most software packages, from the Help menu.

- **Use Encrypted Authentication**

Clear-text transmission methods transfer your user ID and password WITHOUT converting them to an encrypted form. This makes your user ID and password readable by outsiders who may attempt to intercept and use the information. Carnegie Mellon servers DO NOT allow clear-text authentication. To ensure normal email and server access, follow the steps in the *Using Encrypted Authentication Methods* (<http://www.cmu.edu/computing/doc/security/encrypt/index.html>) document.

- **Backup Your Data Periodically**

You should perform regular backups on a weekly basis. At a minimum, backup your data before and after any system or data changes. Recovering from a system crash or a security compromise can be expedited if you maintain proper backups. Otherwise, you may be without your system for days or weeks and recreating lost work can be extremely difficult. For more information, read Microsoft's *Windows XP Backup Made Easy* (http://www.microsoft.com/windowsxp/using/setup/learnmore/bott_03july14.msp) article.

Important: Secure your backup media in a safe, locked place. It may contain sensitive information.



Advanced Security Steps

Last Updated: 01/12/07

Advanced Steps

We **strongly** recommend that you follow the advanced steps if you:

- Visit web sites you do not trust on a regular basis.
- Download software from servers you do not trust.
- Run a web server or semi-private file server.

If any or all of these usage patterns apply to you, please complete the following:

[Step 1: Create an Everyday User Account](#)

[Step 2: Disable Un-necessary Services](#)

[Step 3: Run and Update a Malware Removal Program](#)

Step 1: Create an Everyday User Account

By creating an everyday user account for daily work you limit the damage a virus or malicious attacker can inflict.

Follow these steps to create a normal user account.

1. Click **Start > Control Panel**.
- 2.



Double-click **User Accounts**. *User Accounts*
The User Accounts dialog box appears.

3. Select **Create a new account**.
4. Enter a name for the account. Click **Next**.
5. Select **Limited** for the account type. Choose **Create Account** .
6. Follow steps 2-3 in *Step 5: Secure Your Accounts and Passwords* page to create a password for this account.



Step 2: Disable Unnecessary Services

Last Updated: 01/12/07

Step 2: Disable Unnecessary Services

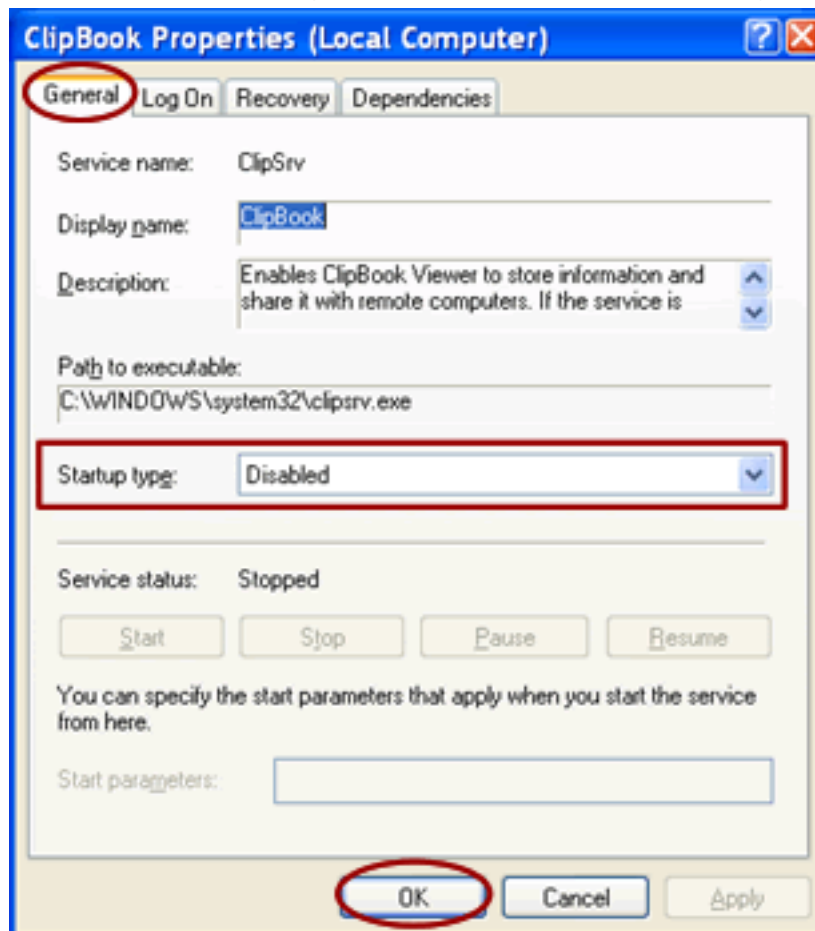
Any services which are not needed for your day-to-day use should be disabled. By disabling or removing these services, viruses have less avenues of attack and you have fewer services to maintain through patch updates.

Note: Be sure to work with your departmental computing administrator as you adjust or shut off services on your machine. Some of these services may be in use by departments for automatic patching or backups.

Note: Before you begin, see the [Definitions](http://www.cmu.edu/computing/doc/security/general/definitions.html) (<http://www.cmu.edu/computing/doc/security/general/definitions.html>) page for a list of services that can typically be turned off.

To view and disable the services that are running on your machine, follow these steps:

1. Click **Start > Control Panel**.
2. Double-click **Administrative Tools** and then **Services**. The Services window appears.
3. Double-click the service you wish to disable (e.g. Clipbook). The Properties window for that service appears.
4. From the **Startup type**: drop-down menu choose one of the following:
 - **Automatic:** This setting will start the service at boot time.
 - **Manual:** This setting allows Windows to start a service when needed.
 - **Disabled:** This setting will stop a service from starting, even if needed.



5. Repeat these steps for each service you want to disable.



Step 3: Run and Update a Spyware Removal Program

Last Updated: 01/12/07

Step 3: Run and Update a Malware Removal Program

Malware or more specifically, spyware is any technology-such as web site tracking or keystroke logging software-that aids in gathering information about a person without their knowledge. SpyWare is often installed along with popular programs such as KaZaA, GrokSter, iMesh and others. It is also installed by some web sites via pop-up ads and viruses. In some cases spyware can take over your web browser or generate pop-up ads even when your browser has been closed.

Before you can run a removal program, you need to download it. You can use any program of your choice, but we recommend Malwarebytes Anti-Malware Software. For help with downloading and running Malwarebytes, refer to the "[Download, Install and Run Malwarebytes' Anti-Malware](http://www.cmu.edu/computing/doc/security/clean-win/basic#malware.html)" (<http://www.cmu.edu/computing/doc/security/clean-win/basic#malware.html>) section of the *Clean Your Windows Computer* document.

Last Updated: 8/21/09