

Secure Your Windows Vista Computer

This document contains the following sections:

- [Step 1: Download and Install Symantec Endpoint Protection for Desktops](#)
- [Step 2: Turn on Windows Automatic Updating](#)
- [Step 3: Ensure Windows Firewall is Turned On](#)
- [Step 4: Ensure File Sharing is Off](#)
- [Step 5: Secure Your Accounts](#)
- [Step 6: Enable a Screen Saver Password](#)
- [Step 7: Configure Local Security Auditing Policies](#)
- [Additional 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 Endpoint Protection](#)
(<http://www.cmu.edu/computing/doc/software/virus-windows/index.html>)
- [Using Encrypted Authentication Methods](#)
(<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](#) (<http://www.cmu.edu/iso/>) _ (<http://www.cmu.edu/iso/>)
(ISO) (<http://www.cmu.edu/iso/>)

Important: If your machine is managed by a Carnegie Mellon departmental administrator, please check with that person before proceeding. Also, make sure you have admin access to the machine you want to secure and login using the admin account for all actions unless otherwise noted.

Last Updated: 08/18/09

Step 1: Download and Install Symantec Endpoint Protection for Desktops

Carnegie Mellon owns a volume license for [Symantec Endpoint Protection](http://www.cmu.edu/computing/software/all/symantec/index.html) (<http://www.cmu.edu/computing/software/all/symantec/index.html>) 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. For more information, see [Definitions](http://www.cmu.edu/computing/doc/security/general/definitions.html) (<http://www.cmu.edu/computing/doc/security/general/definitions.html>). 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.

Important Note: 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 files quickly becomes outdated.

To ensure that your machine is protected you will want to download a copy of Symantec Endpoint Protection software from the Computing Services [Software](http://www.cmu.edu/computing/software/all/index.html) (<http://www.cmu.edu/computing/software/all/index.html>) page and follow the installation instructions. For more information on configuring Symantec read the [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>) web page.

Run Live Update

Virus definitions change daily. To fully protect your computer, you need to download the latest virus definition files by running Live Update. 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 *Live Update* section of the [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>) page for details.



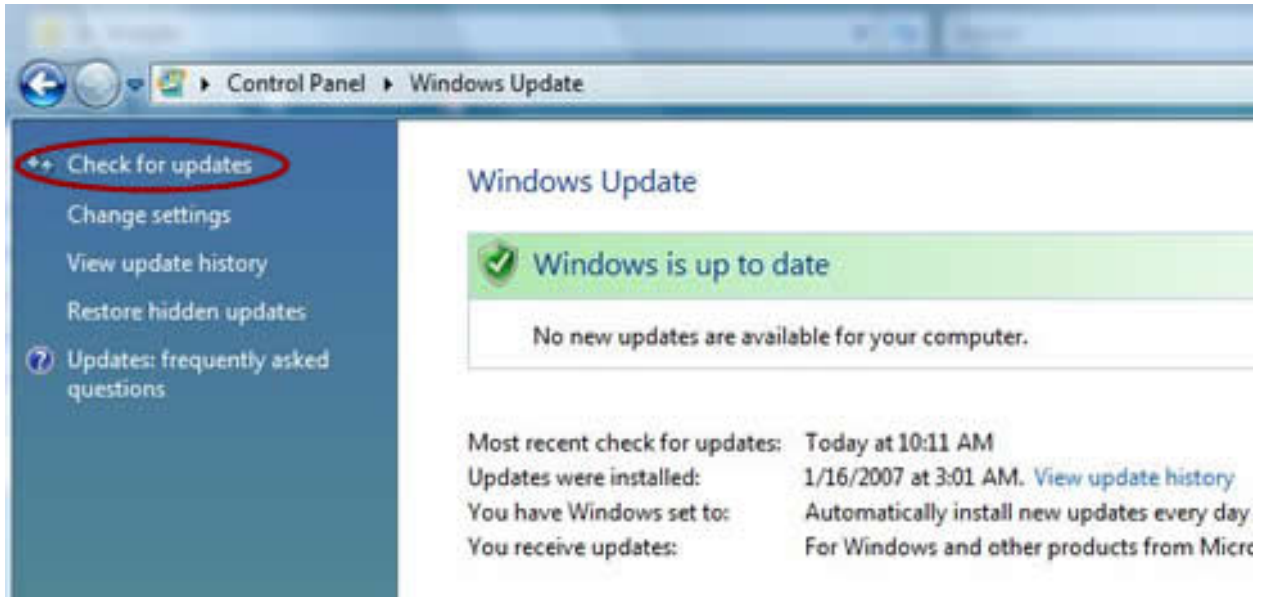
Step 2: Turn on Windows Automatic Updating

Last Updated: 8/17/09

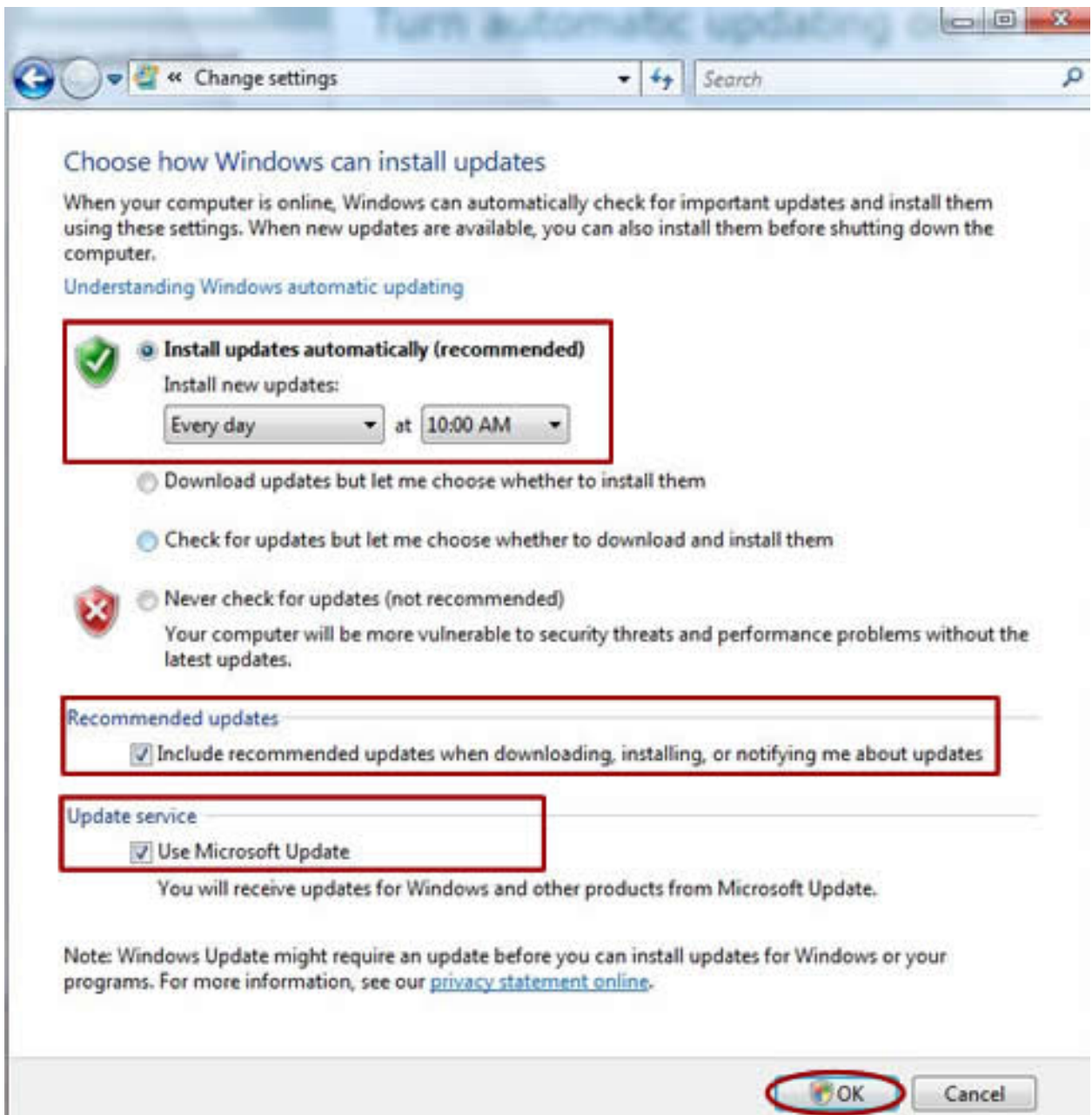
Step 2: Turn on Windows Automatic Updating

Security updates can help protect your computer against new and ongoing threats. Follow these steps to have Windows install important updates automatically:

1. Select **Start > All Programs > Windows Update**.
2. In the left pane, click **Change settings**.



3. In the **Change settings** window, select the following options:
 - **Install updates automatically (recommended).**
 - Install new updates: **Everyday.**
 - at: **choose a time** when your machine will be turned on.
 - Recommended updates: select (check) **Include recommended updates when downloading, installing, or notifying me about updates.**
 - Update service: select **Use Microsoft Update.**
4. Click **OK** to save changes.



Step 3: Ensure Windows Firewall is Turned

On

Last Updated: 02/02/07

Step 3: Ensure Windows Firewall is Turned On

A firewall can help prevent malicious attackers from gaining access to your computer through a network or the Internet. By default, Windows (Vista) Firewall is turned on. When the firewall is on, most programs are blocked from communicating through the firewall. If you want to unblock a program, add it to the list of exceptions. For more information about firewalls, see [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 Windows Firewall and ensure it is turned on:

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **Windows Firewall**.
4. In the **Windows Firewall** window, ensure **Windows Firewall is on**. If the firewall is off or you want to unblock a program, click **Change settings**.



If the **User Account Control** window appears, click **Continue**.

5. In the **Firewall Settings** window, select the **General** tab.
6. Select **On (recommended)**.
 - If you are making no further changes, click **OK**.
 - To allow a program to communicate through the firewall, continue with the steps below:
 - a. Select the **Exceptions** tab.
 - b. Do the following:
 - o Uncheck any program or service you **DO NOT** wish to accept incoming network connections.
 - o Check any program or service you **DO** wish to accept incoming connections.
 - o Check **Notify me when Windows Firewall blocks a new program**.
Note: If a program you want to allow does not appear in the list, click the **Add program...** button and **Browse** for the program.
 - c. Click **OK** to save your changes.



Step 4: Ensure File Sharing is Off

Last Updated: 02/02/07

Step 4: Ensure File Sharing is Off

File sharing allows users to share folders and may allow malicious attackers to read or write files from your shared folders. By default, file sharing is turned off. If you decide to share a folder, make sure password protected sharing is turned on.

To ensure file sharing is turned off, follow these steps:

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **Network and Sharing Center**.
4. Under **Sharing and Discovery** ensure **File sharing** is **Off**.



- To turn file sharing off or on, click the **File sharing arrow** button.
Note: For more information on file sharing, refer to the *File sharing essentials* article found in Help and Support. Click **Start > Help and Support** and search **file sharing**.
- To enable password protected sharing, click the **Password protected sharing arrow** button and click **Turn on password protected sharing**.



Step 5: Secure Your Accounts

Last Updated: 02/02/07

Step 5: Secure Your Accounts

To prevent someone from gaining access to your computer, physically or through the network, each user account **MUST** have a strong password. Accounts with weak or nonexistent passwords are an invitation for malicious attackers to compromise your system.

Set Passwords for User Accounts

To prevent someone from gaining access to your computer, physically or through the network, each user account **MUST** have a strong password.

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **User Accounts**.
4. In the **User Accounts** window, click **Manage another account**. If the **User Account Control** window appears, click **Continue**.
5. A password protected account will have **Password protected** listed under account type.



Add a password to accounts that need one by double-clicking the account.

6. Select **Create a password**.
7. In the **Create Password** window:
 - In the **New password** field enter a password.
 - Retype the password in the **Confirm new password** field.

Note: For tips on selecting a strong password, read *Managing Your Andrew Password* (<http://www.cmu.edu/computing/doc/accounts/passwords/index.html>).
8. Click **Create password** to save your changes.

Delete Unused Accounts

To delete any unused accounts, follow these steps:

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **User Accounts**.
4. In the **User Accounts** window, click **Manage another account**.



If the **User Account Control** window appears, click **Continue**. A list of user accounts will appear.

5. Double-click the account you want to remove and choose **Delete the account**.

Create a Strong Administrator Password

To verify that a strong password is set for the Administrator account, follow these steps:

1. Login to the computer using the Administrator userid and password.
2. Select **Start > Control Panel**.
3. In the left panel, click **Classic View**.
4. In the **Control Panel** window, double-click **User Accounts**.
5. In the **User Accounts** window, click **Change your password**.
6. In the **Change your password** window, enter your current password and a new password.

Note: For tips on selecting a strong password, read *Managing Your Andrew Password* (<http://www.cmu.edu/computing/doc/accounts/passwords/index.html>).

7. Click the **Change password** to save your changes.



Step 6: Enable a Screen Saver Password

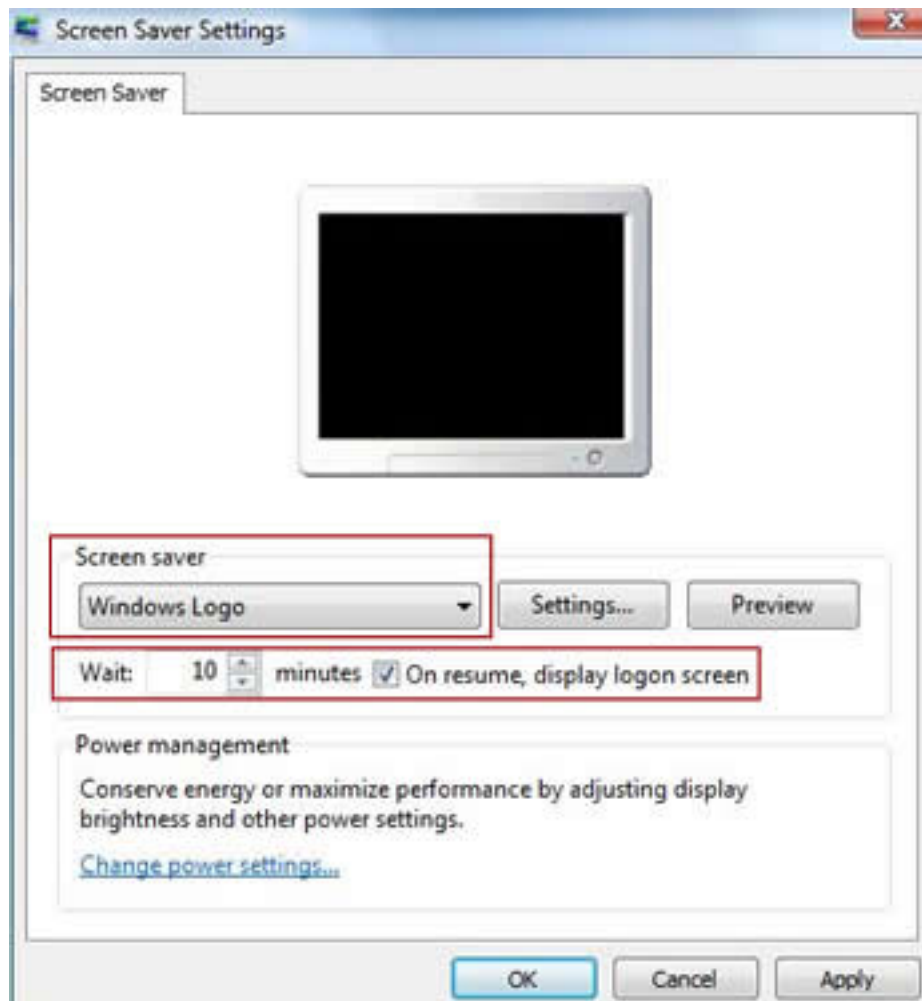
Last Updated: 02/02/07

Step 6: Enable a Screen Saver Password

To prevent someone from using your computer when you have stepped away, you should enable a screen saver password. 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. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **Personalization**. A list of options appears.
4. Select **Screen Saver**.
5. Set the following:
 - Select a Screen saver from the drop down menu.
 - Set the **Wait** time to 10 minutes or less.
 - Select (check) **On resume, display logon screen**.



6. Click **OK**.



Step 7: Configure Local Security Auditing Policies

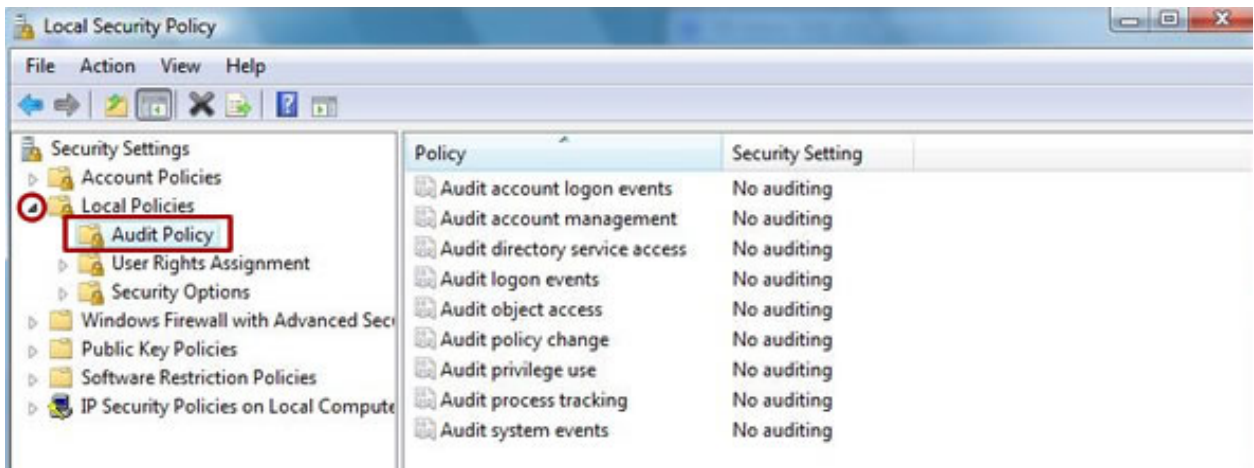
Last Updated: 02/02/07

Step 7: Configure Local Security Auditing Policies

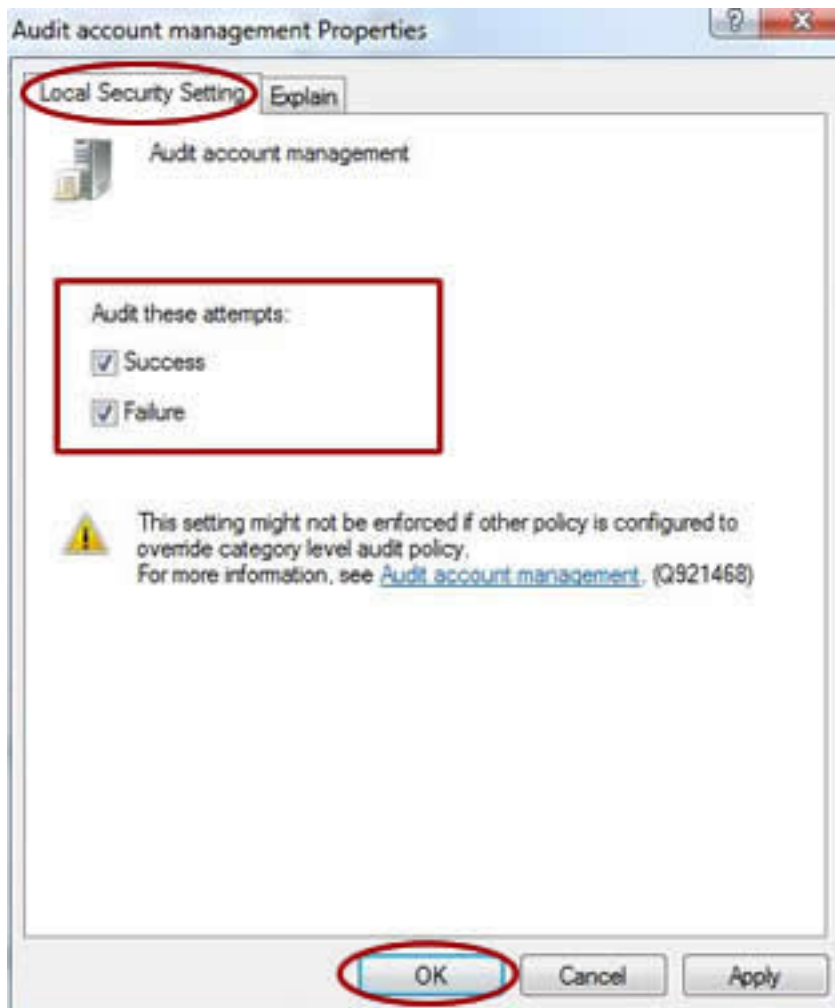
Windows Vista has the ability to record more security events, but the settings are not enabled by default. If your computer becomes compromised, keeping more logging information increases the chances that experts will be able to determine how and when the compromise occurred.

Follow these steps to enable additional security event logging:

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **Administrative Tools** and then **Local Security Policy**.
4. If the **User Account Control** window appears, click **Continue**.
5. In the left pane, click the small arrow next to **Local Policies** and then select **Audit Policy**.
6. Double-click **Audit account logon events** in the right pane.



7. In the **Properties** window, select the **Local Security Settings** tab.
8. Under **Audit these attempts** select (check) **Success** and **Failure**.



9. Click **OK** to save the settings.
10. Repeat Steps 6 through 9 for each **Audit** policy listed in the right pane.



Additional Security Tips

Last Updated: 02/02/07

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 \(http://www.cmu.edu/computing/doc/security/encrypt/index.html\)](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.

To backup your files and folders to a CD, follow these steps:

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **Backup and Restore Center**.
4. To create a backup, do one of the following:
 - Click **Back up files** to backup files and folders in your Documents folder.
 - Click **Back up computer** to create a restore image. Microsoft recommends doing this every six months.
5. If the **User Account Control** window appears, click **Continue** and follow the onscreen instructions.

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



Advanced Security Steps

Last Updated: 02/02/07

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 Unnecessary Services](#)

[Step 3: Use BitLocker Drive Encryption](#)

Last Updated: 02/02/07

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.

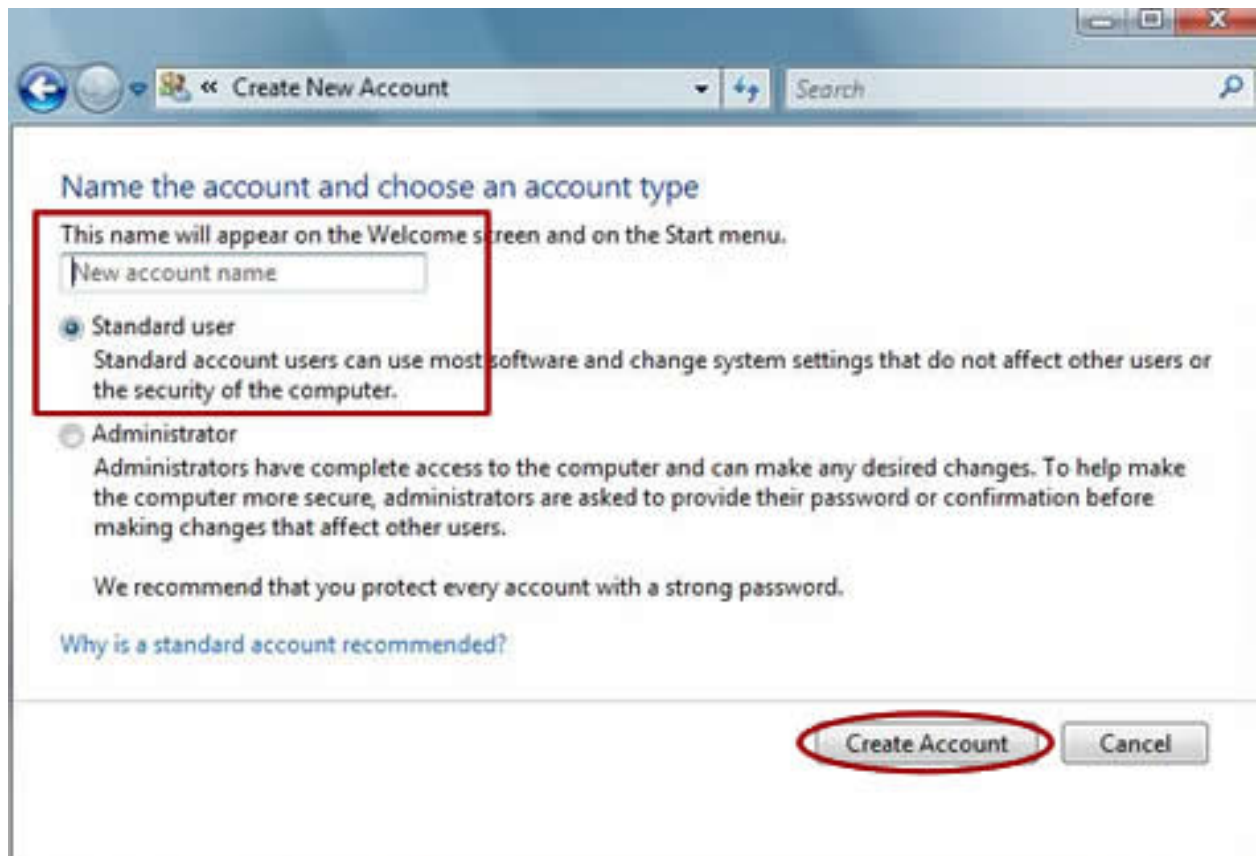
Follow these steps to create a everyday user account.

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **User Accounts**.
4. In the **User Accounts** window, click **Manage another account**.



If the **User Account Control** window appears, click **Continue**.

5. Below the list of user accounts, click **Create a new account**.
6. In the **Create New Account** window:
 - Enter a name in the **New account name** field.
 - Select **Standard user**.
 - Click **Create Account**.



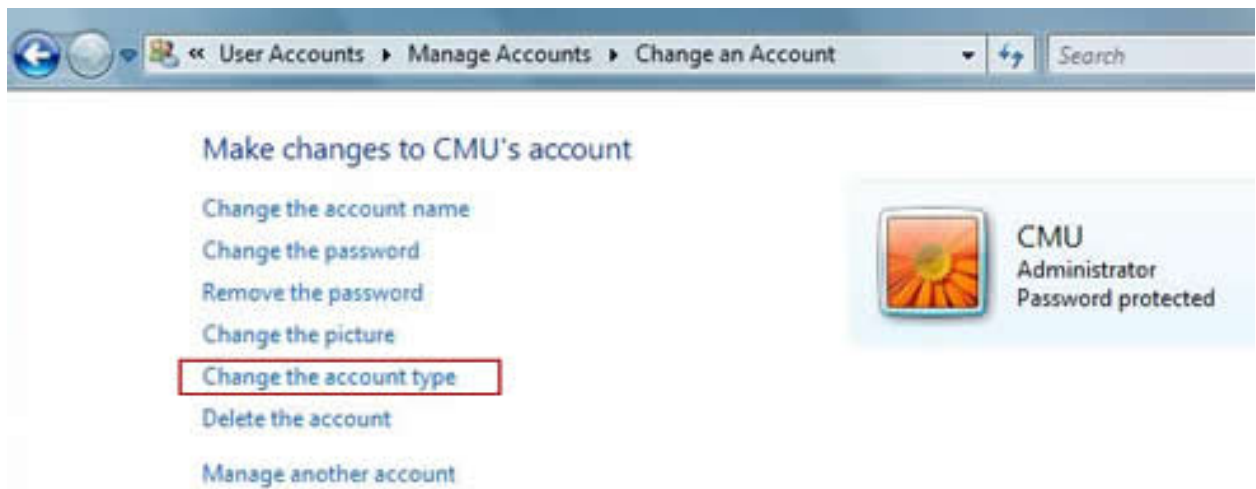
IMPORTANT NOTE: Make sure you set a password for the everyday account you created by following the steps in the *Set Passwords for User Accounts* section of the [Step 5: Secure Your Accounts](#) page.

Remove Administrator Access from Everyday Accounts

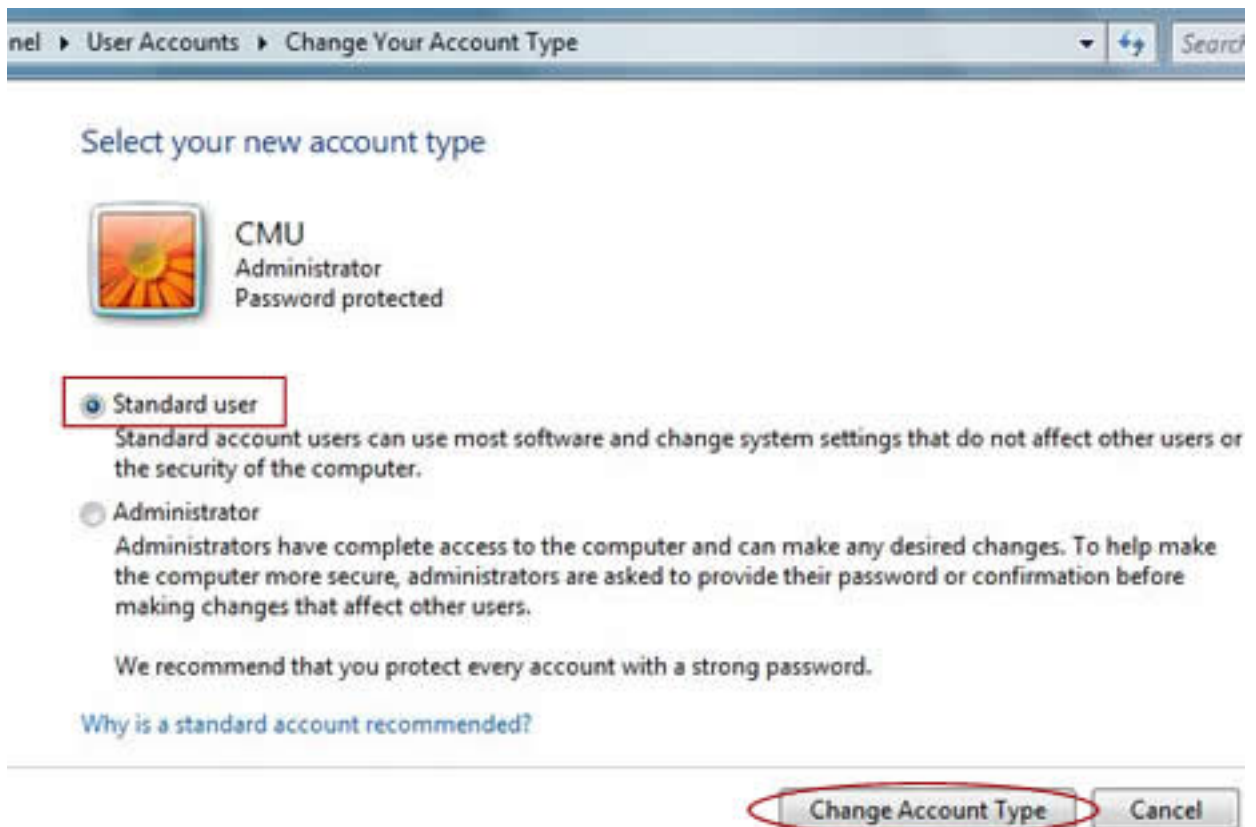
Use the following steps to remove Administrator access from other accounts:

IMPORTANT NOTE: Make sure you have one account with Administrator access.

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **User Accounts**.
4. In the **User Accounts** window, click **Manage another account**. If the **User Account Control** window appears, click **Continue**.
5. Select the user account you want to change.
6. In the **Change an Account** window, select **Change the account type**.



7. Select **Standard user** and click **Change Account Type**.



Turn User Account Control On

User Account Control (UAC) can help prevent unauthorized changes to your computer. It is recommended that you leave UAC turned on.

To ensure UAC is turned on, follow these steps:

1. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **User Accounts**.
4. In the **User Accounts** window, click **Turn User Account Control on or off**. If the **User Account Control** window appears, click **Continue**.

5. Select (check) **Use User Account Control (UAC) to help protect your computer.**
6. Click **OK.**



Step 2: Disable Unnecessary Services

Last Updated: 02/02/07

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.

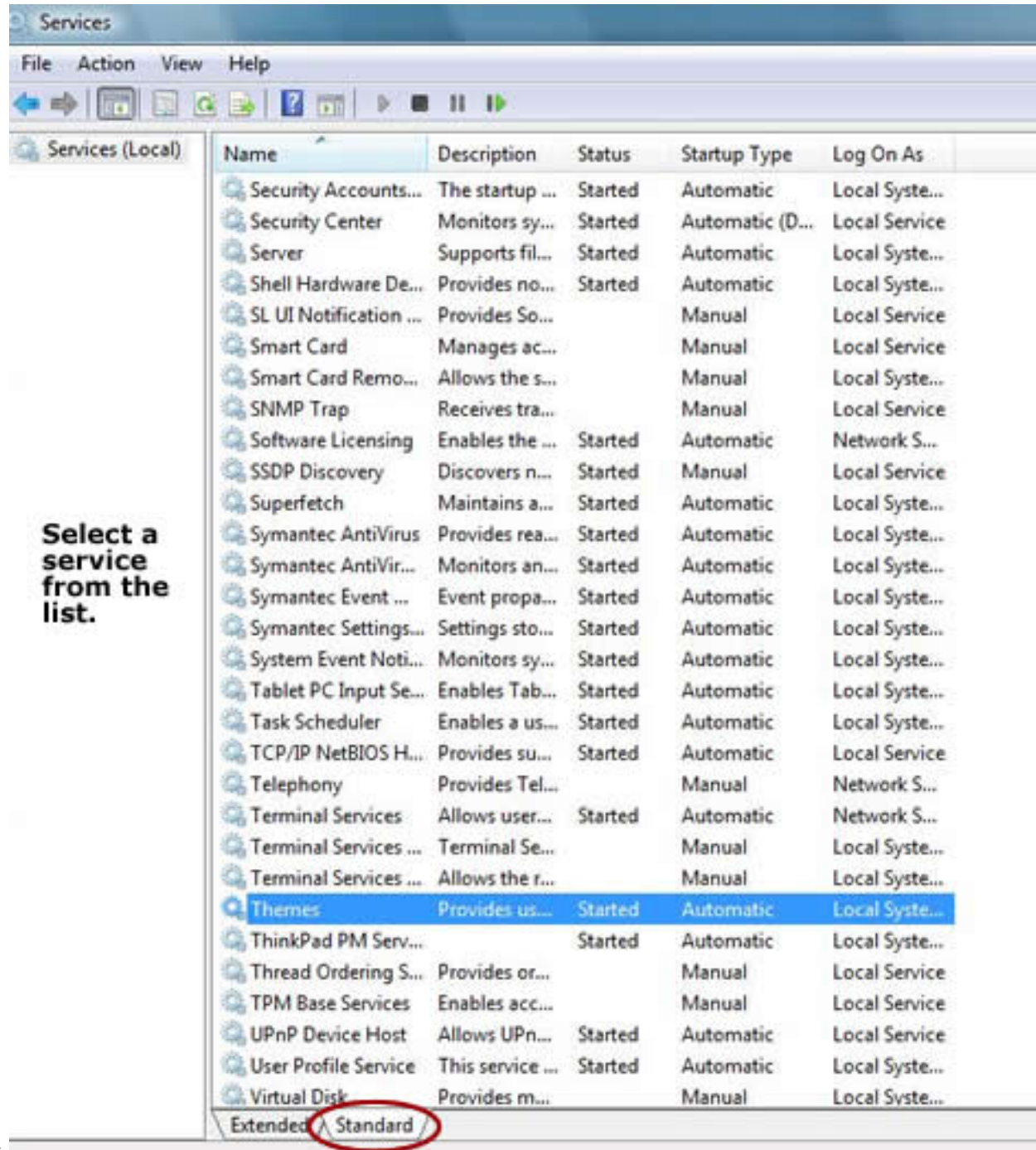
Note: Be sure to work with your departmental computing administrator as you adjust or shut off services on your machine. Some of these services may be in use by departments for automatic patching or backups.

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>) document 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. Select **Start > Control Panel**.
2. In the left panel, click **Classic View**.
3. In the **Control Panel** window, double-click **Administrative Tools** and then **Services**.
4. If the **User Account Control** window appears, click **Continue**.
5. Select the **Standard** tab and double-click the service you wish to disable (e.g. Themes). The **Properties**

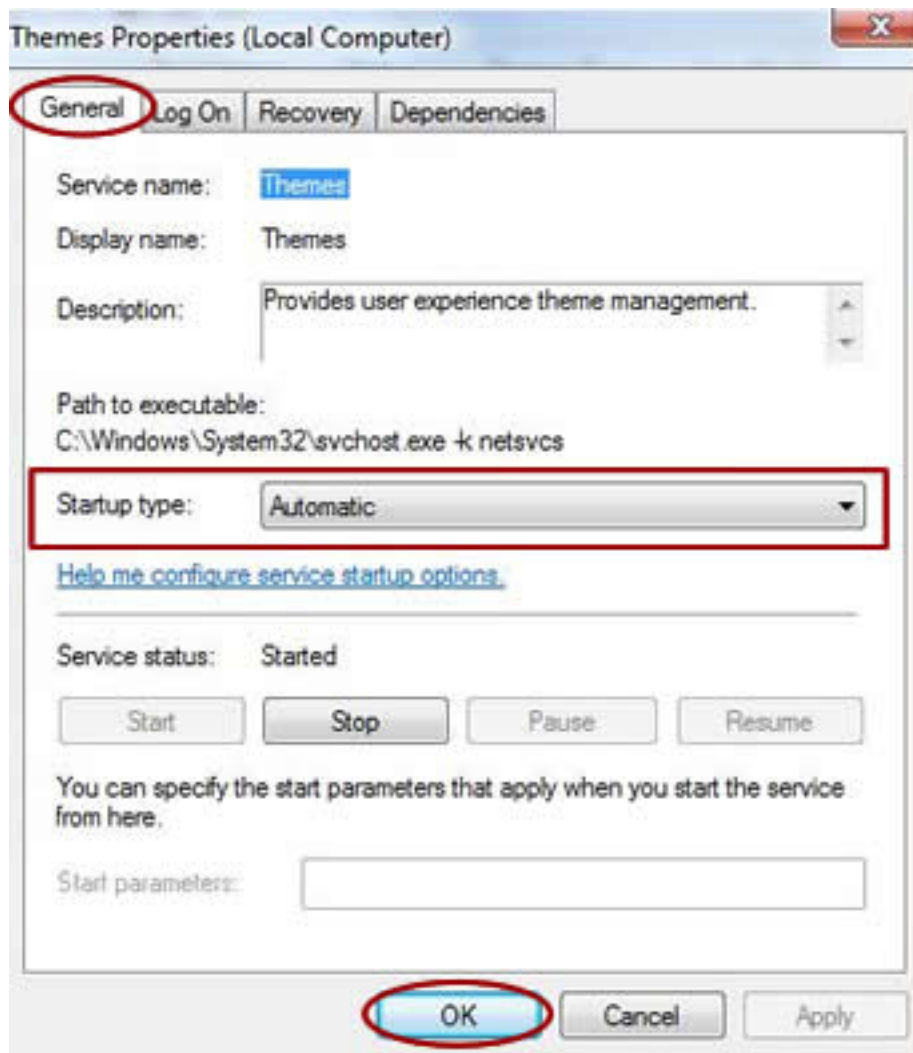
window for that service



Select a service from the list.

appears.

6. Choose the **General** tab.
7. 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.
8. Click **OK**.



9. Repeat steps 5-8 for each service you want to disable.



Step 3: Use BitLocker Drive Encryption

Last Updated: 02/02/07

Step 3: Use BitLocker Drive Encryption

BitLocker Drive Encryption is a new security feature in Windows Vista. BitLocker protects your operating system and data from a physical or offline attack. For more information on BitLocker, read Microsoft's [Windows BitLocker Drive Encryption Step-by-Step Guide \(http://go.microsoft.com/fwlink/?LinkId=53779\)](http://go.microsoft.com/fwlink/?LinkId=53779).

Note: The step-by-step guide is intended for IT analysts and Security architects.

Last Updated: 02/02/07