Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Windows Vista: First Steps

With firewalls enabled by default, attacks haven't stopped. Unlike the Sasser and Blaster worms, modern malware frequently attacks the client. Windows Vista attempts to improve client security to help users defend against just these attacks. This guide will help you take full advantage of these new features.

Copyright SANS Institute
Author Retains Full Rights

AD

Windows Vista: First Steps

Table of Contents

1 Introduction....1
2 How to Use this Guide....2
3 Administrator Password....2
4 Automatic Updates....6
5 Malware Protection....8
6 Other Security Settings....8
7 Add a “regular User”....8
8 Run Software Update....10
9 Appendix: Firewall Settings....11
10 Appendix: Clean Installation....11
Administrator Account....11
Administrator Account....11
Automatic Updates....11
Automatic Updates....11
Network Settings (“Location”)....11
Network Settings (“Location”)....11
First Log In....12
First Log In....12

Introduction

This article is a follow on to our guide “Windows XP, Surviving the First Day”. This older guide was written based on Windows XP pre SP2. One of its main feature was step by step instructions on how to enable the Windows XP firewall. A lot has happened since then. Most notably, Windows XP SP2 enabled the firewall by default. This step has been a very significant improvement in particular for home users. However, even with firewalls enabled by default, attacks haven't stopped. Unlike the Sasser and Blaster worms, modern malware frequently attacks the client. Windows Vista attempts to improve client security to help users defend against just these attacks. This guide will help you take full advantage of these new features.

Our older guide stepped the user through the initial operating system install. This was important for Windows XP, as the firewall had to be enabled before the system was connected to the Internet the first time to download patches. With Vista, we are going a different route. Most users will receive Vista pre–installed. While these installations will differ from system to system, we will attempt to cover the most common issues one may encounter.

The target for this guide is a novice computer users / home user, not a seasoned system administrator.

How to Use this Guide

We added a lot of images to make it easy to follow the guide. All “actions”, tasks you should perform, use an *italics courier* font. Please first read a chapter to its end, then follow the step by step instructions.

Administrator Password

You should first configure an Administrator password. Likely, your system will come with no Administrator password, or a default password common to many systems. Before you go ahead, think about a good password. A good password is long and uses a diverse set of characters, numbers and special characters. One approach to a good password is a pass-pharse. A pass-phrase is a short, easy to remember sentence. Please don't forget to write down your Administrator password and store the note in a safe place (for example a safe, or store it in a sealed envelope with a friend or relative). It makes sense to keep one copy of the password in your safe, and another copy off site. Only after you wrote down the Administrator password, go through the following steps:

---

1. Log in as Administrator

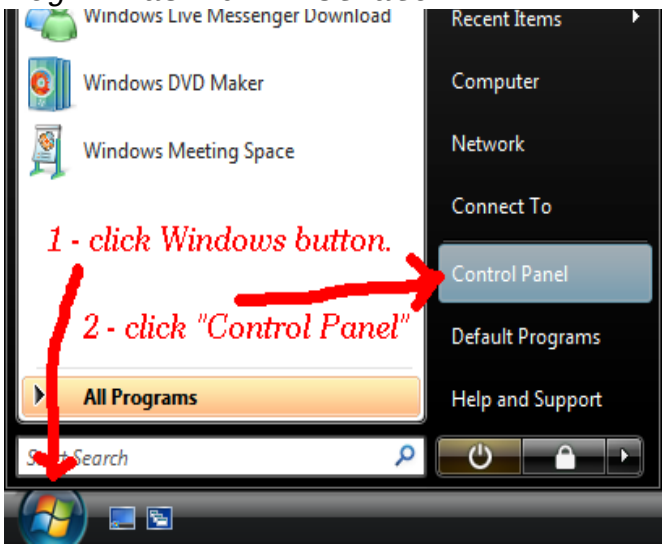


Illustration 1: Start Menu

2. Access the Control Panel (see Illustration 1)

Illustration 2: Control Panel

3. Click "Add or Remove User Accounts"

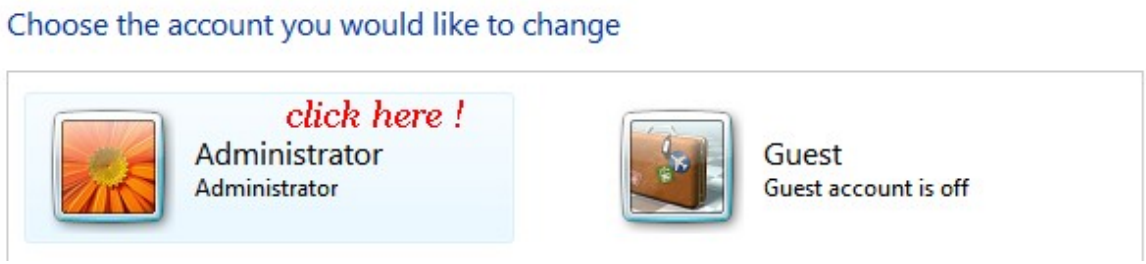


Illustration 3: Add or remove user account dialog.

4. Click on the "Administrator" icon. Your administrator account maybe named differently. But the second line should read "Administrator".

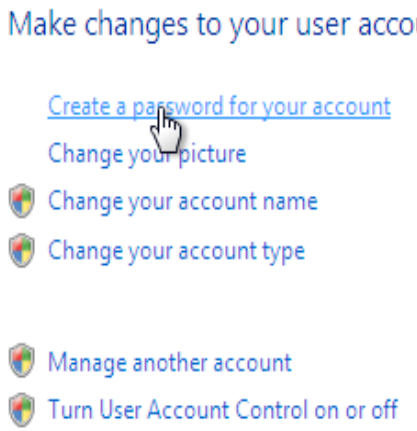


Illustration 4: Manage changes to your account.

5. Click "Create a Password".

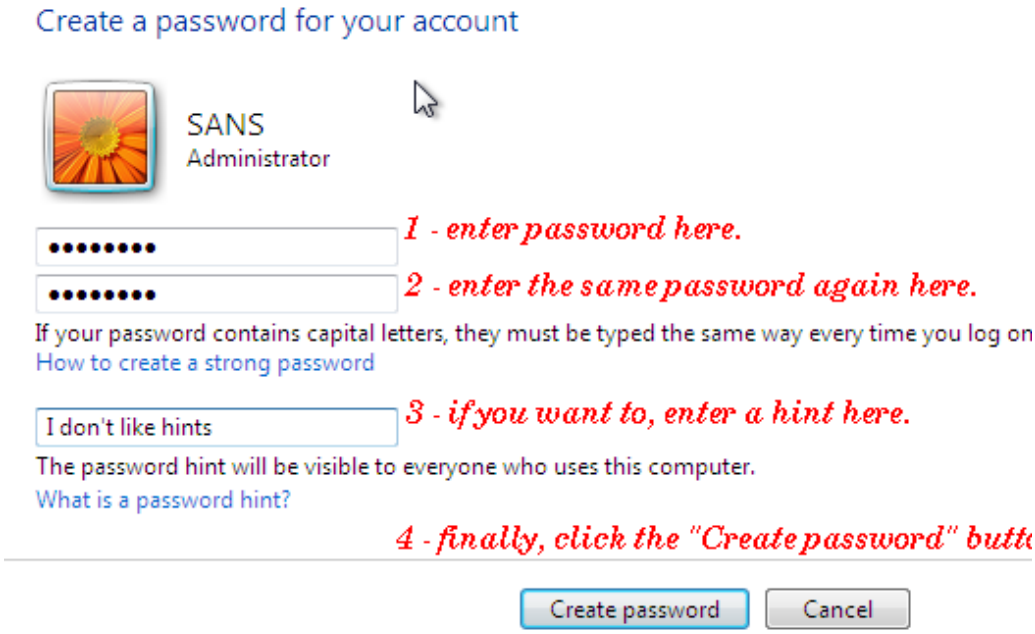


Illustration 5: Create a password dialog.

6. You will have to enter the password twice.
7. Think about if you want a password hint or not. In particular for the Administrator account, you should probably not enter a password hint.
8. Click "Create Password"

That's it! Now try it out. Log off and log in again using your new password. To Log off, select "Log off" in your "Start Menu".

To Log in. click the "Administrator" icon and enter the password. Type the password by reading it from your note, so you will make sure that you got it written down right.

Automatic Updates

Next, lets click on the shield in the lower right hand corner of the screen. Likely, the shield is “Yellow”, indicating that your system has not been secured yet.

Illustration 6: System Security Center Status Indicator

You will see four items (see Illustration 7):

1. Firewall Settings: This setting should be “green”, indicating that the firewall is on. Please jump to the Appendix “Firewall Settings” if it is not green.
2. Automatic Updating: This setting is likely “Yellow” if you have not yet configured automatic updates.
3. Malware protection: Again, this setting is yellow if you have not yet installed any anti–malware products like virus scanners.
4. Other Security Settings. More about this later.

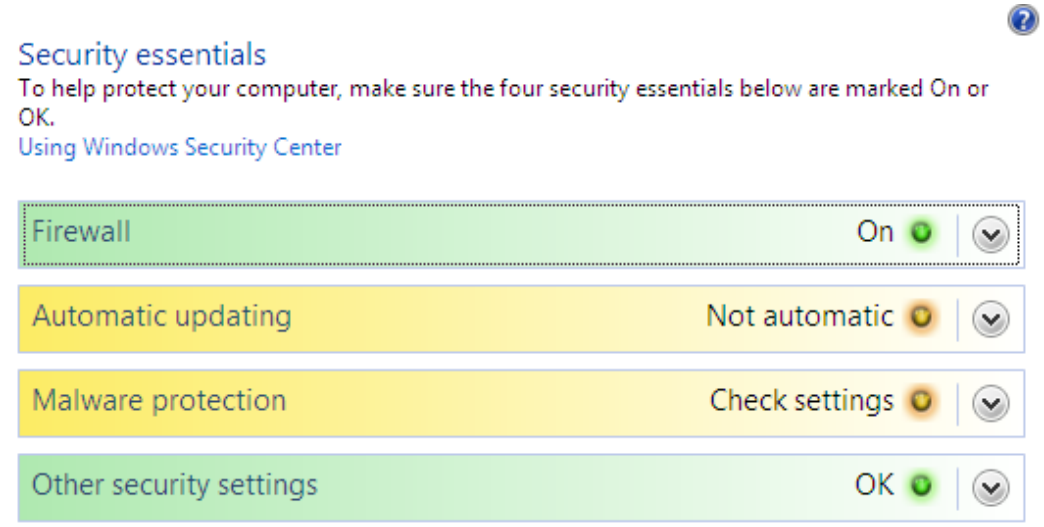


Illustration 7: Security Center at Yellow

To configure “Automatic Updating”:

1. Click on the (yellow) "Automatic Updating" line.

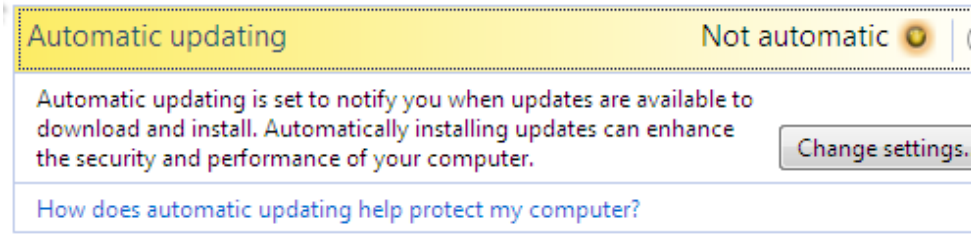
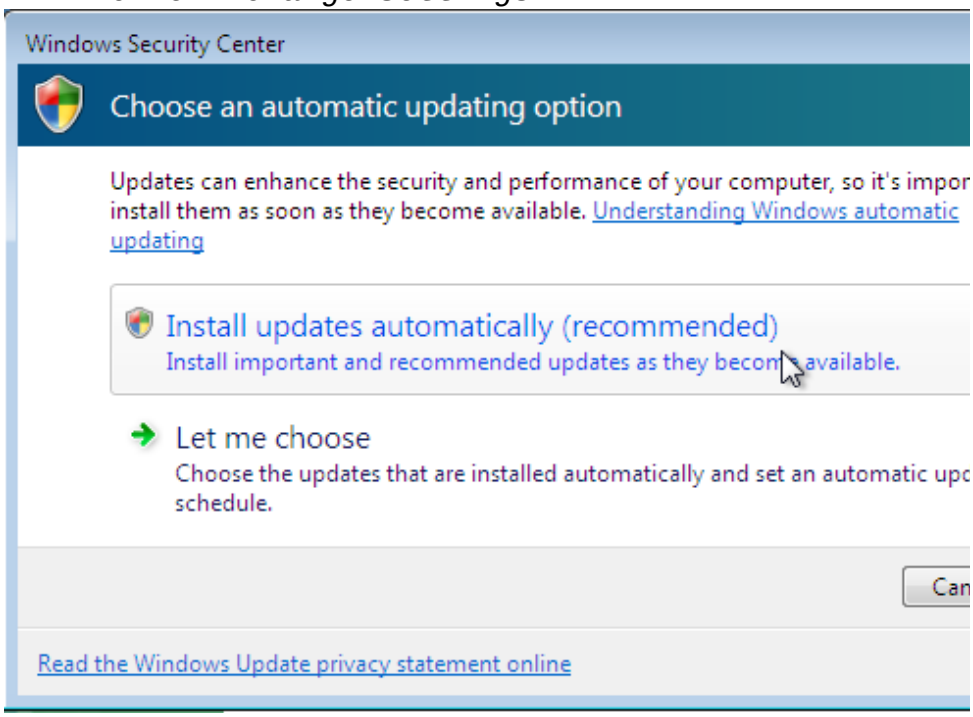


Illustration 8: Security Center: Automatic Updating.

2. Click "Change Settings".



3. Next, select "Install updates automatically".

In particular for a home system, this is a safe choice. If you are using a lot of odd/custom software, or if your system is supported by a corporate IT department, you should likely select "*Let me choose*". But in this case, you will have to pick and choose which updates you would like to install. The process of picking and choosing updates is nothing a novice computer user typically would like to do.

If you selected "*Install updates automatically*", your "*Automatic Updating*" line will now be green (Illustration 10).

Malware Protection

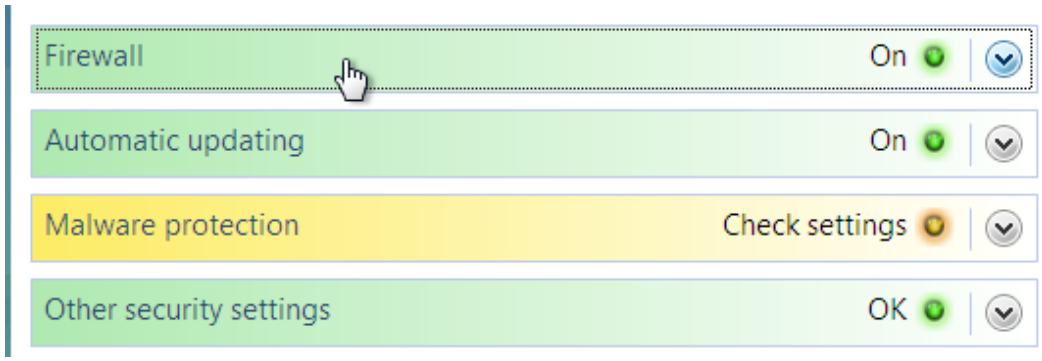


Illustration 10: Security Center after enabling automatic updates.

It is strongly recommended to install an anti virus scanner. However, not all anti virus scanners will be recognized by Vista, even if they are perfectly fine and functioning properly. The "*Malware Protection*" line will turn green on its own if your anti-virus scanner is installed and recognized by Vista. Most anti-virus programs will require a reboot after installation. Please refer to the installation instructions for your anti-malware of choice for details.

Other Security Settings

There are two options in this section. The first option will indicate if Internet Explorer is running at its recommended security level. The second option indicates if "User Access Control" is turned on. Both are enabled by default and nothing needs to be changed. Each one of this options includes links to extensive help pages.

Add a "regular User"

The default install will only configure an administrator user. In prior versions of Windows, most users ran as "Administrator", or added themselves to the "Administrator" group to obtain the privileges to install software and change configurations without having to log in as Administrator each time.

Windows Vista added a new feature, "User Account Control" (UAC). See Section 6 for details on how to enable UAC. This feature will allow you to become an Administrator for specific tasks, just by entering the Administrator password. As a result, it is much easier, and highly recommended, to use a non-Administrator user for day to day work.

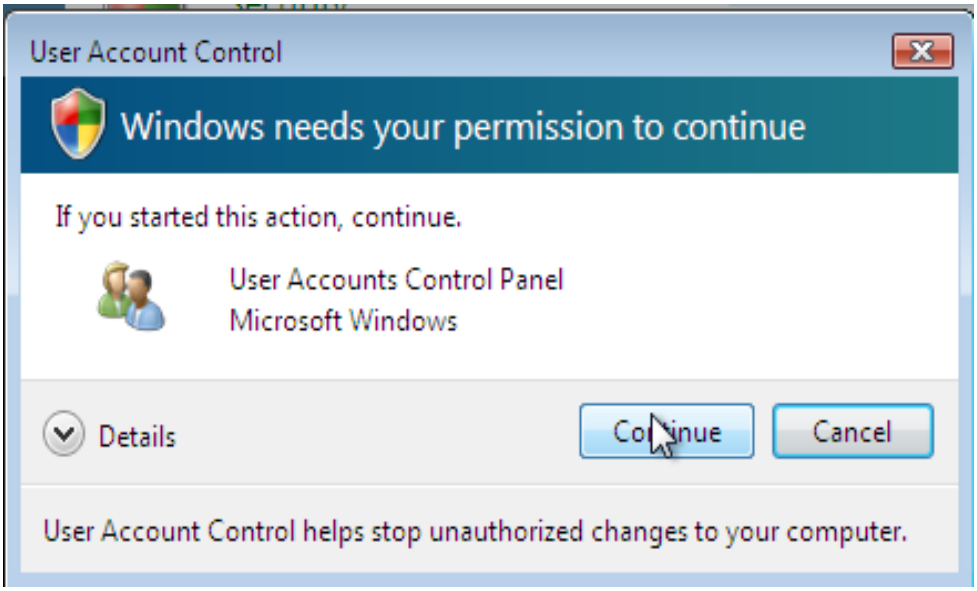


Illustration 11: User Account Control popup dialog.

The big advantage of running as a non-Administrator user is that any damage caused by malware will be limited to this account. This will make it much harder for malware to remain undetected by installing root kits and other defenses.

To add a regular user:

```
1. Open the control panel
2. Click on "Add or remove user accounts"
```

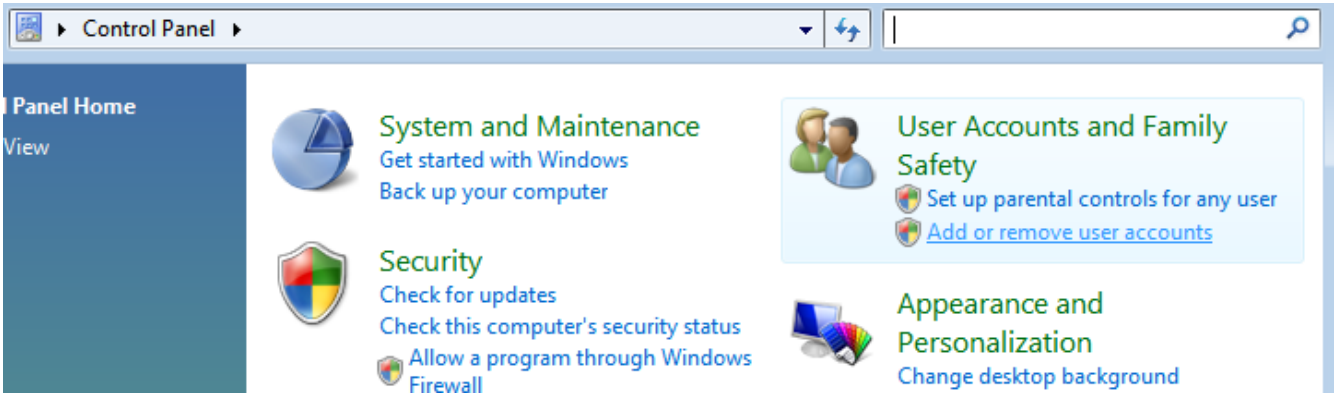


Illustration 12: Control Panel: Add and remove user accounts.

```
3. Click on "Create a new account"
```

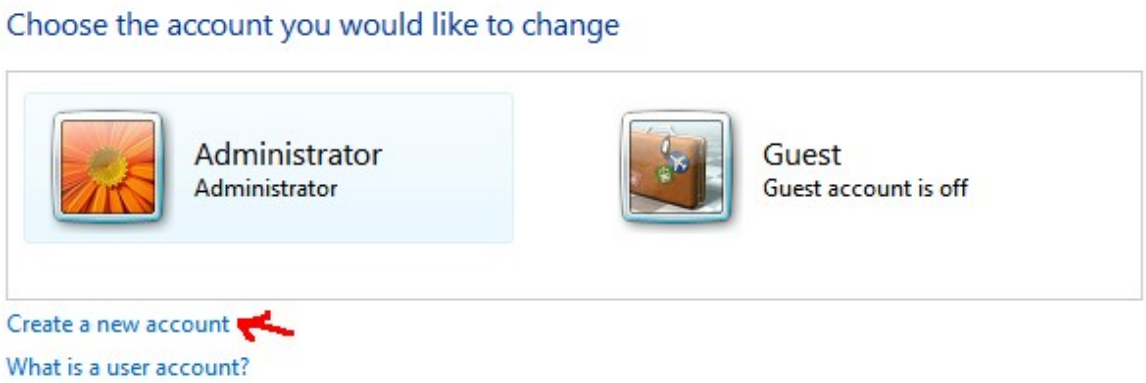


Illustration 13: Control Panel, Manage Accounts Screen.

4. Enter user name and make sure you select the "Standard user" radio button.

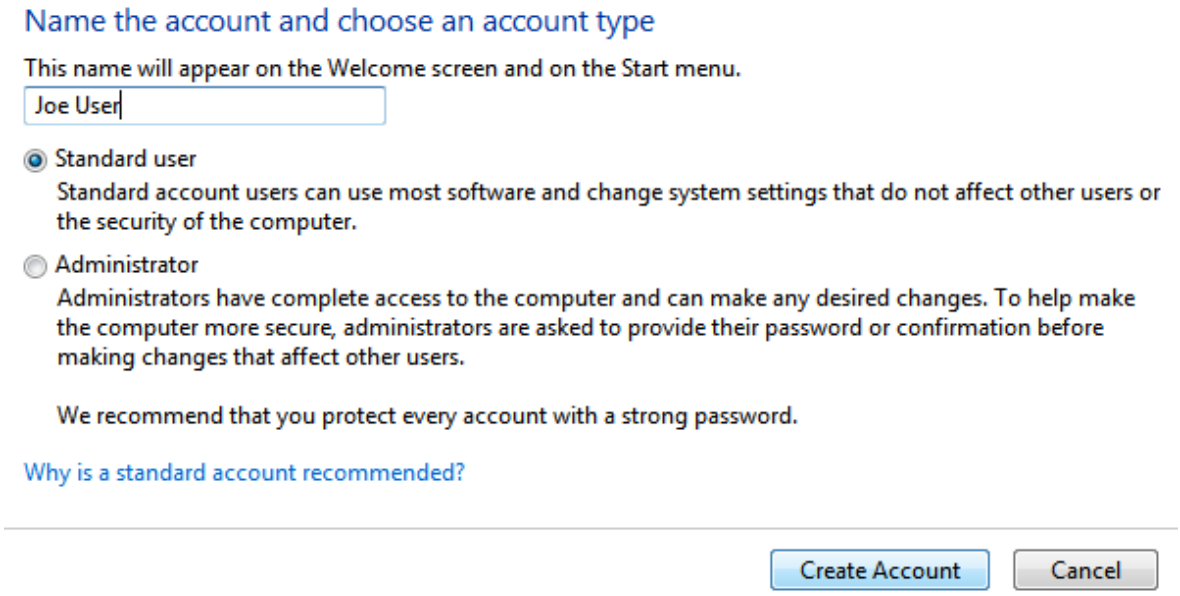


Illustration 14: Create New Account dialog.

By default, the user will not be asked for a password. However, this will limit the user to log in locally only. You should ask the user to setup a password, or you may do so for the user by following the same steps we used above for the administrator.

Run Software Update

For none of the steps listed so far did you require Internet access. This is one reason why we saved this step for last. Now connect your system to your network. You may want to reboot in order to have the network configuration applied correctly.

To check for updates manually:

- *Close all programs and safe your work.*
- *open the control panel.*
- *Select "Check for updates".*

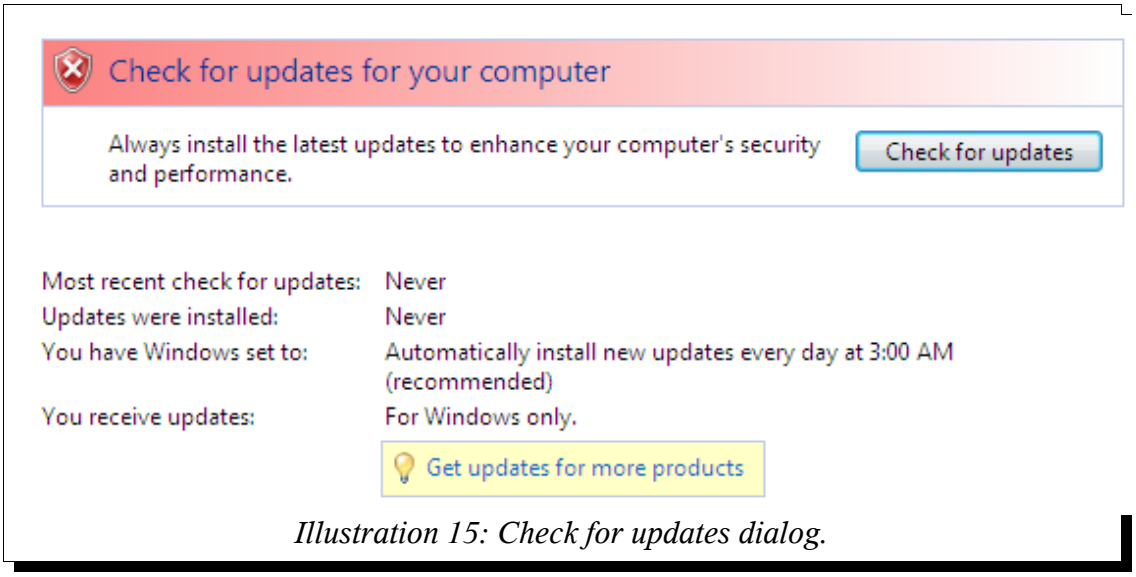


Illustration 15: Check for updates dialog.

- *If there are any updates, Vista will tell you. Click "Install updates" in the next dialog.*

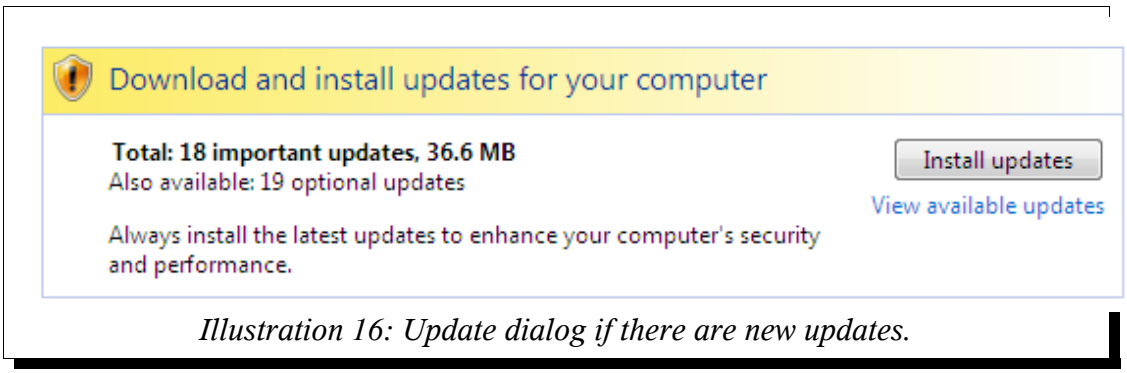


Illustration 16: Update dialog if there are new updates.

- *now wait while the updates are downloaded. The time it takes to download the updates will vary based on the number of updates and your network connection.*

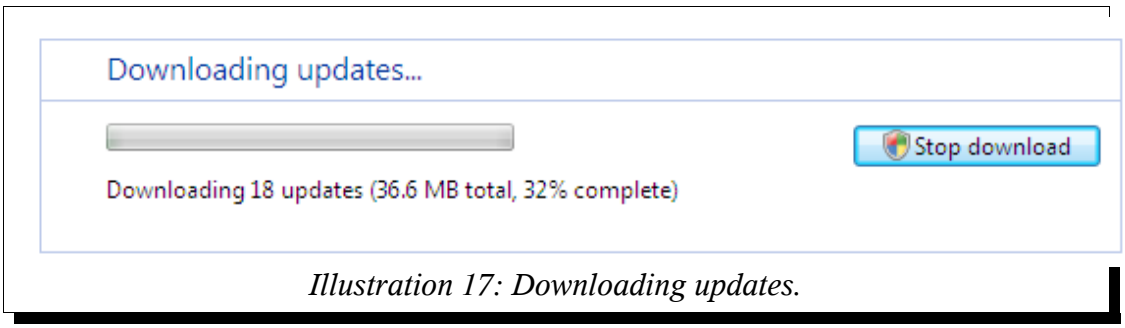


Illustration 17: Downloading updates.

- *After the patches are installed, you will likely have to reboot your system.*

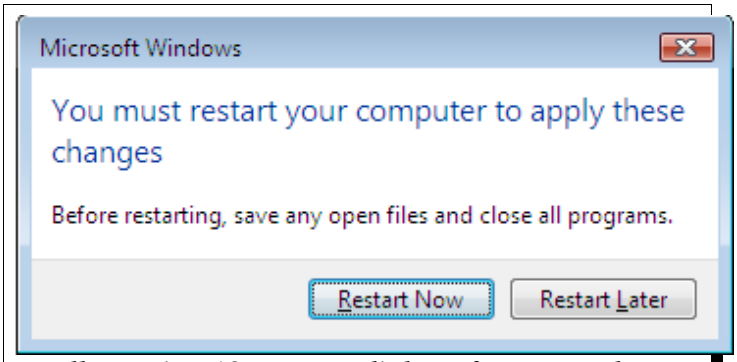


Illustration 18: Restart dialog after a complete update.

•

Appendix: Clean Installation

If you are upgrading a Windows XP system, or if you install Vista on a new system yourself, you will have to slightly modify the instructions above. First of all, there are a few security related choices during the installation process:

Administrator Account

Vista will ask for the user name and password for your Administrator user (see Illustration 18). Pick a “generic” username. Later, you will be asked to add a regular user, and you will probably use your own name for this regular user. The administrator will only be used for selected tasks like adding additional users.

Automatic Updates

You have three options to configure automatic updates while installing Vista (see Illustration 17). The recommended settings will install all important and recommended updates automatically. The second option, “Install important updates only” is acceptable as well. You should not select the “Ask me later” option unless you are asked to by your corporate IT department or you feel qualified to make the decision to patch.

Network Settings (“Location”)

During the install, Vista will ask you what category of system you are installing. You will have 3 options (see Illustration 15). This is probably the most important setting during your setup procedure, so choose wisely. The most secure option is “Public Location”. This setting will consider the network you connect your system to as “hostile”. It will not be possible to share files or to access network printers. If this is your only system, and if your printer is attached via USB, then by all means choose “Public Location”. The other two options, “Home” and “Work” are very similar to each other. They assume that your system is connected to a local area

network (LAN), and a device like a router or a firewall is protecting the LAN from unauthorized access.

You will be able to make changes to this later. I strongly recommend you select “Public Location” and keep it that way until you went through this document and fully patched your system.

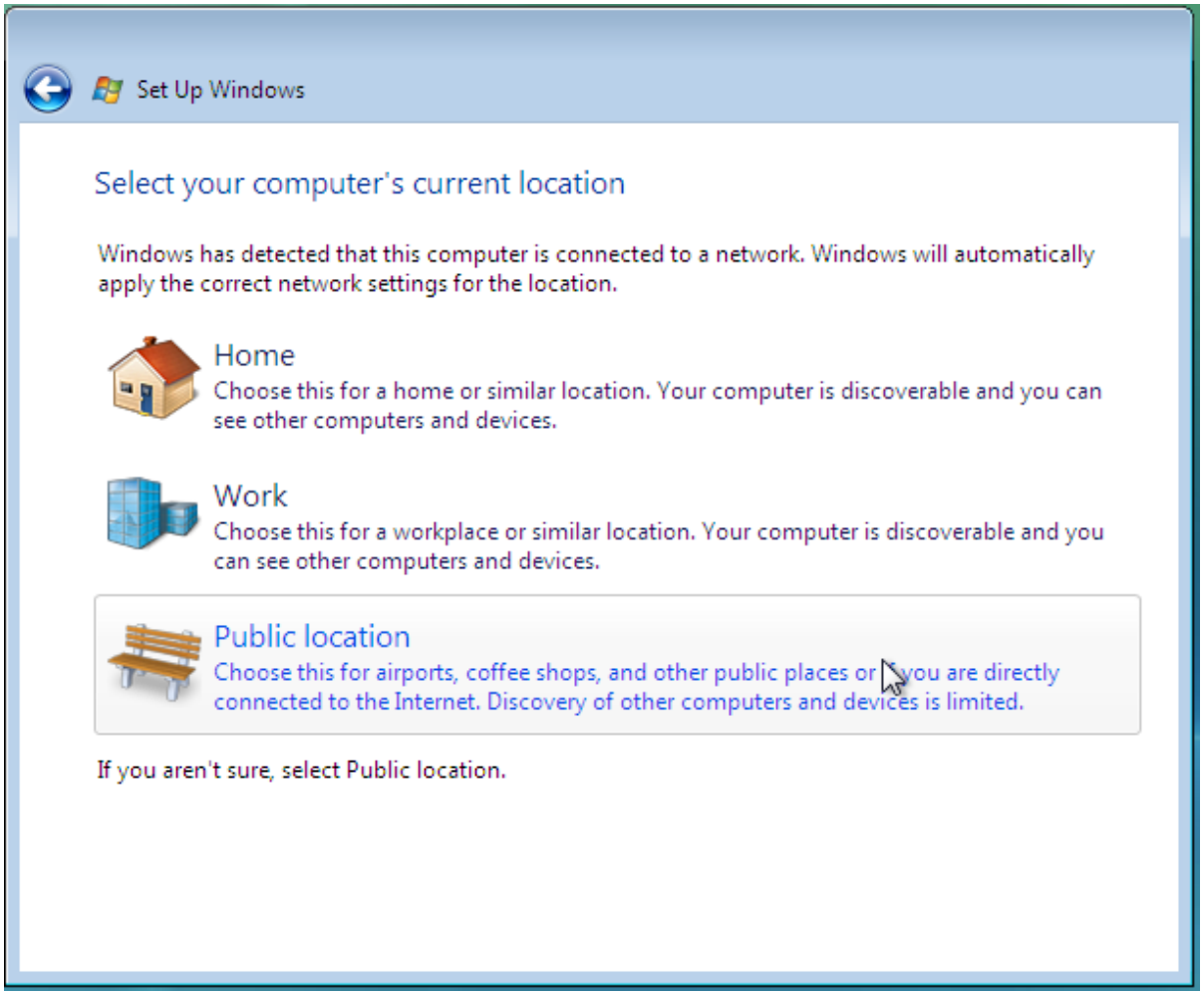


Illustration 19: Selecting your computer's location dialog.

First Log In

The first time you log in to Vista, it will open the “*Welcome Center*” for you. You should now be able to follow the instructions above. Start at “*Malware Protection*”, or “*Adding a New User*”.

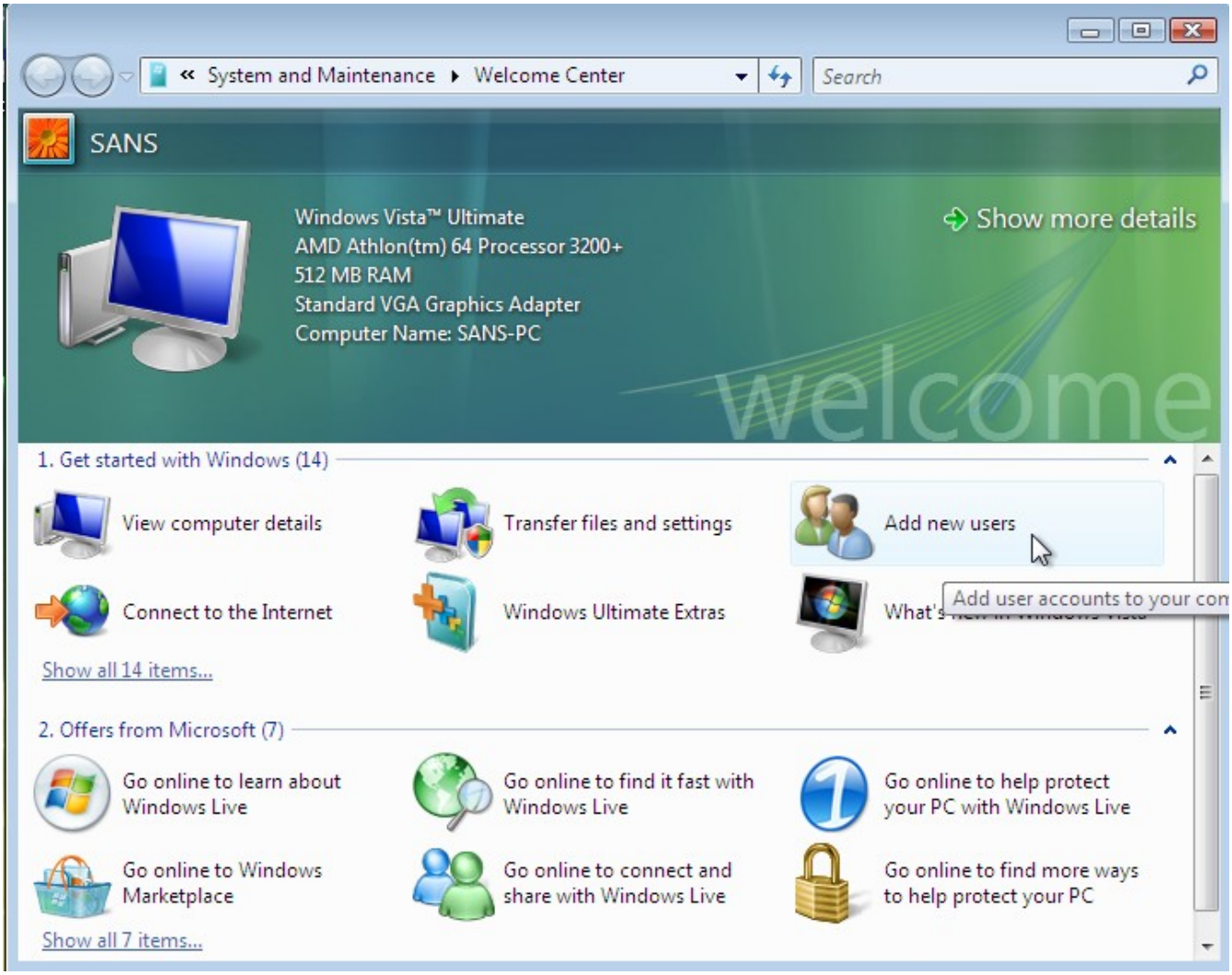


Illustration 20: Control Panel after first login.

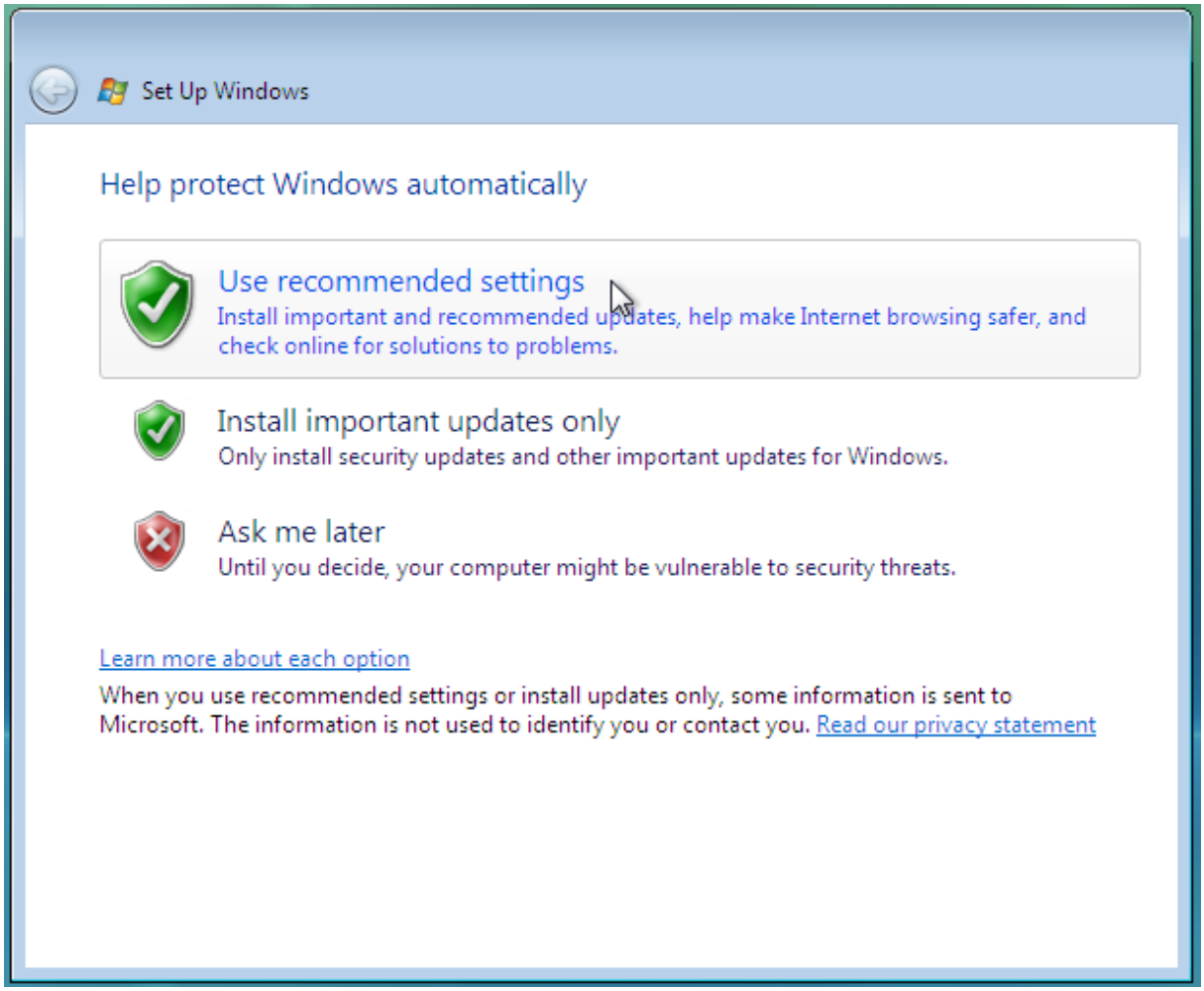


Illustration 21: Automatic Update Settings during Installation.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**