# Windows Vista: First Steps

With firewalls enabled by default, attacks haven&#039;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.

# Windows Vista: First Steps

## Table of Contents

## 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.

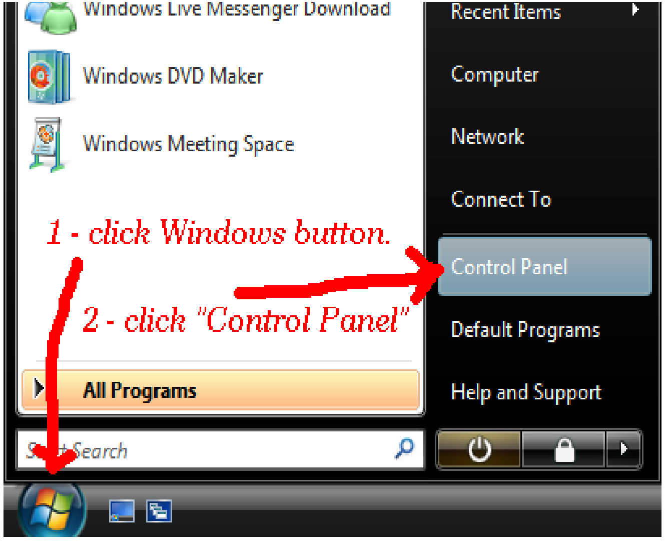
## How to Use this Guide

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*

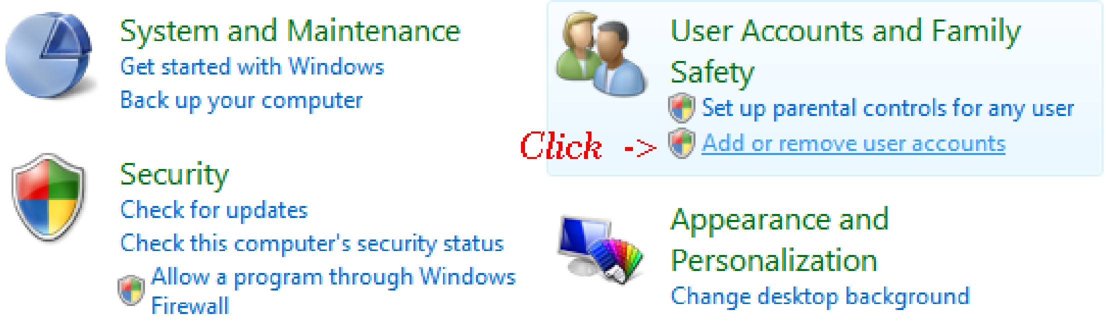


1 - click Windows button.

2 - click "Control Panel"

*Illustration 1: Start Menu*

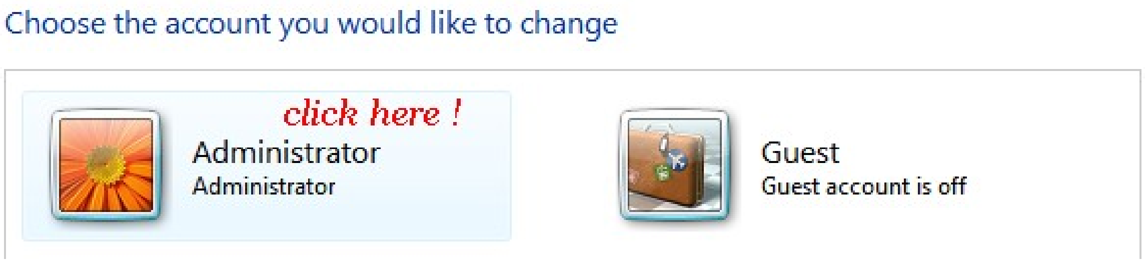
*2. Access the Control Panel (see Illustration 1)*


System and Maintenance
Get started with Windows
Back up your computer
Security
Check for updates
Check this computer's security status
Allow a program through Windows Firewall
User Accounts and Family Safety
Set up parental controls for any user
Add or remove user accounts
Appearance and Personalization
Change desktop background

Click ->

*Illustration 2: Control Panel*

3. `Click “Add or Remove User Accounts”`



click here !

*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”.`

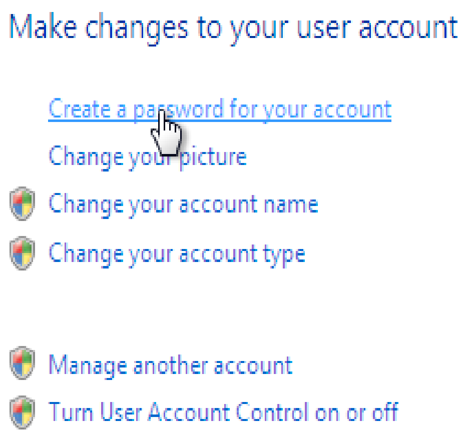
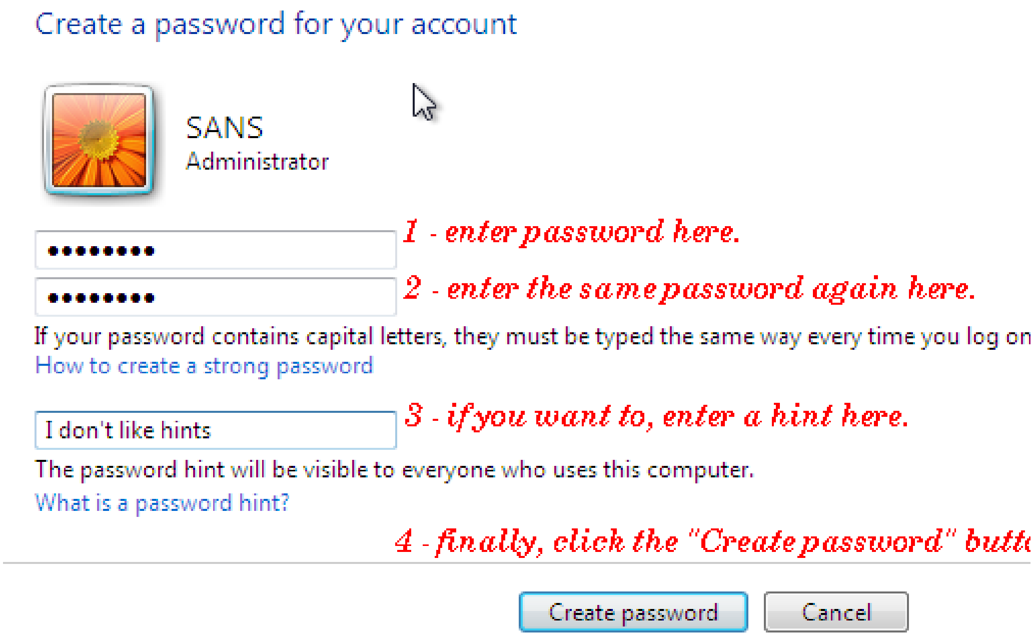

Make changes to your user account
Create a password for your account
Change your picture
Change your account name
Change your account type
Manage another account
Turn User Account Control on or off

*Illustration 4: Manage changes to your account.*

5. Click “Create a Password”.



1 - enter password here.

2 - enter the same password again here.

If your password contains capital letters, they must be typed the same way every time you log on

I don't like hints

3 - if you want to, enter a hint here.

The password hint will be visible to everyone who uses this computer.

4 - finally, click the "Create password" butt

*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.

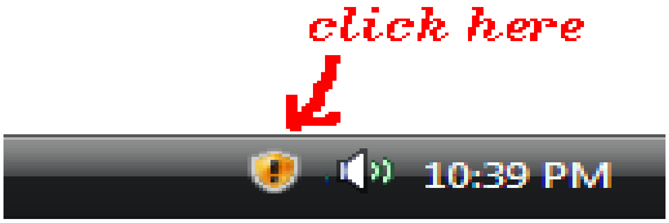
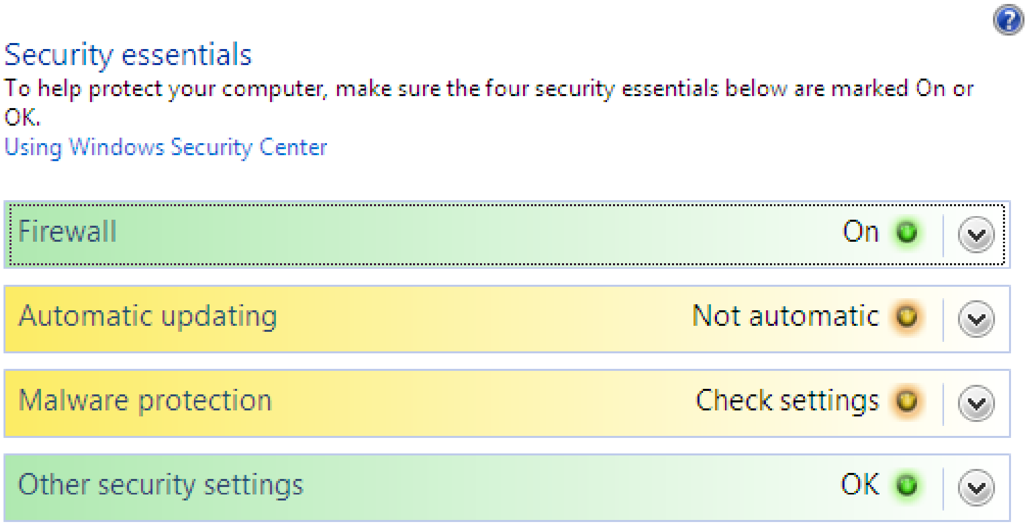


*Illustration 6: System Security Center Status Indicator*

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.



Security essentials

To help protect your computer, make sure the four security essentials below are marked On or OK.

Using Windows Security Center

Firewall On ●

Automatic updating Not automatic ●

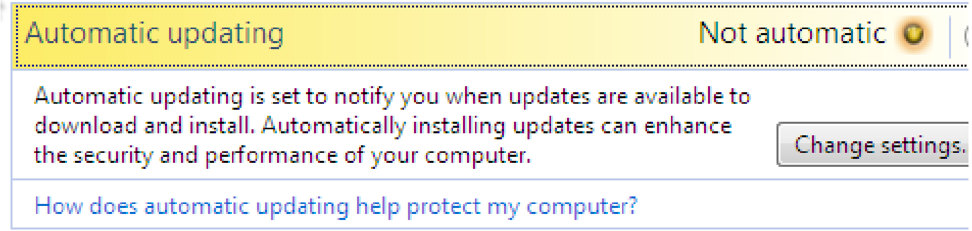
Malware protection Check settings ●

Other security settings OK ●

*Illustration 7: Security Center at Yellow*

To configure “Automatic Updating”:

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



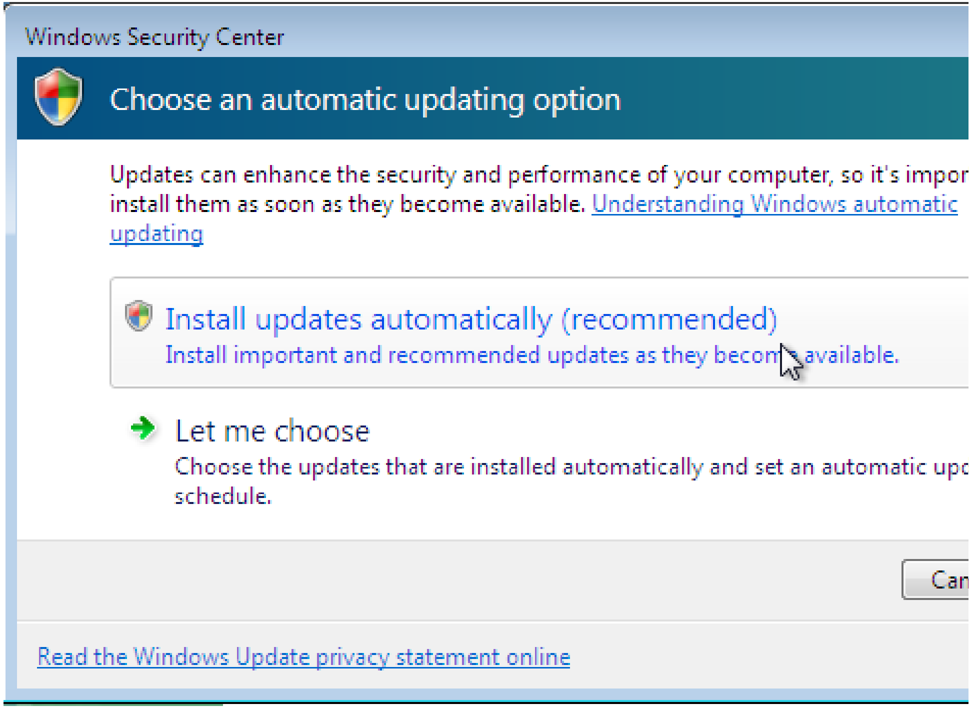
Automatic updating Not automatic

Automatic updating is set to notify you when updates are available to download and install. Automatically installing updates can enhance the security and performance of your computer.

How does automatic updating help protect my computer?

*Illustration 8: Security Center: Automatic Updating.*

2. Click "Change Settings".



Windows Security Center

Choose an automatic updating option

Updates can enhance the security and performance of your computer, so it's impor install them as soon as they become available. Understanding Windows automatic updating

Install updates automatically (recommended)
Install important and recommended updates as they become available.

Let me choose
Choose the updates that are installed automatically and set an automatic upc schedule.

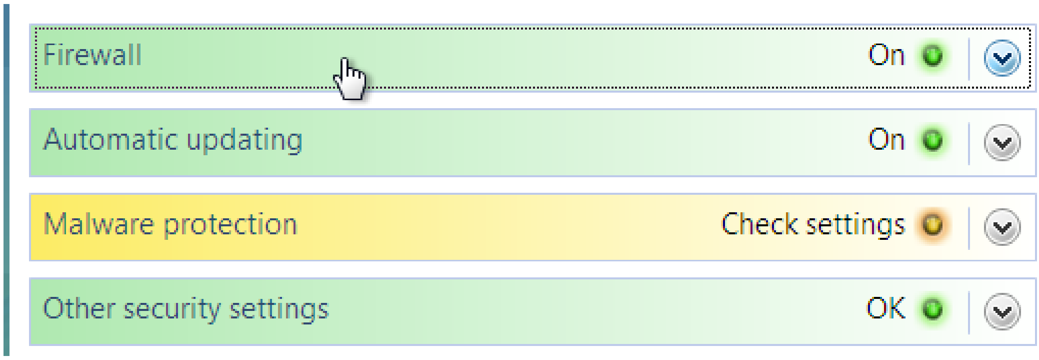
Read the Windows Update privacy statement online

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



Firewall On ●

Automatic updating On ●

Malware protection Check settings ●

Other security settings OK ●

*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.

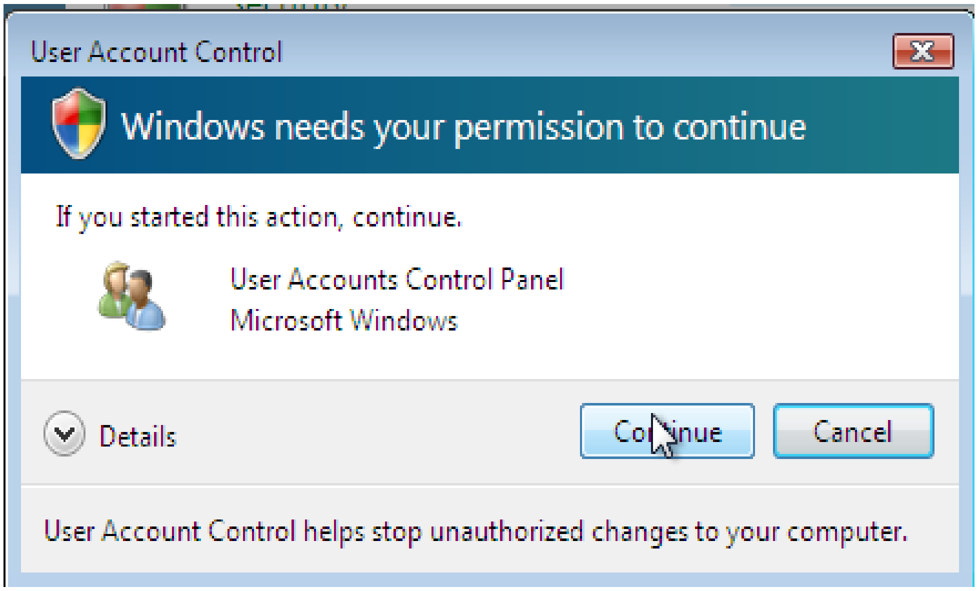
## Other Security Settings

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.



User Account Control

Windows needs your permission to continue

If you started this action, continue.

User Accounts Control Panel
Microsoft Windows

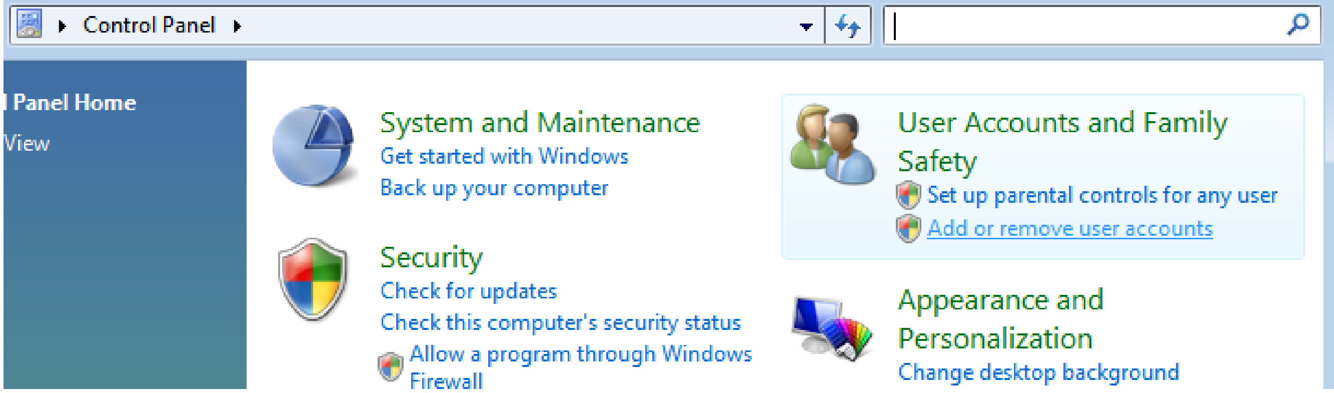
User Account Control helps stop unauthorized changes to your computer.

*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:

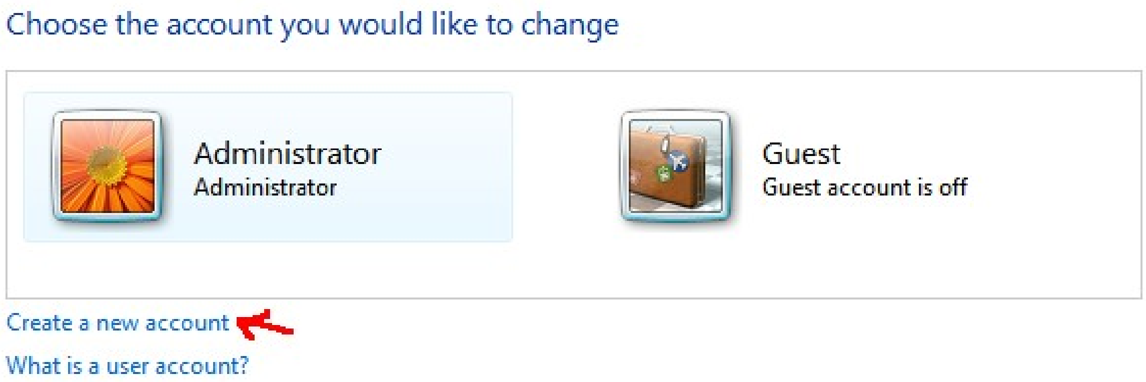
1. Open the control panel
2. Click on “Add or remove user accounts”



Control Panel
l Panel Home
View
System and Maintenance
Get started with Windows
Back up your computer
Security
Check for updates
Check this computer's security status
Allow a program through Windows Firewall
User Accounts and Family Safety
Set up parental controls for any user
Add or remove user accounts
Appearance and Personalization
Change desktop background

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

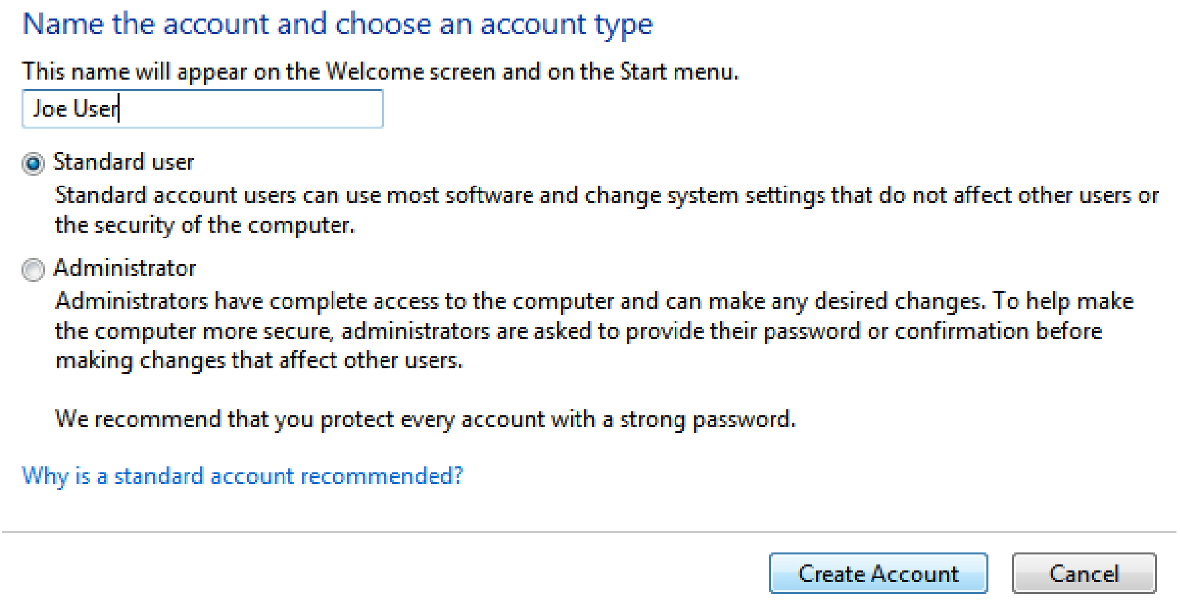
3. Click on “Create a new account”



Choose the account you would like to change

*Illustration 13: Control Panel, Manage Accounts Screen.*

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



Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

Joe User

● Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

○ Administrator

Administrators have complete access to the computer and can make any desired changes. To help make the computer more secure, administrators are asked to provide their password or confirmation before making changes that affect other users.

We recommend that you protect every account with a strong password.

*Illustration 14: Create New Account dialog.*

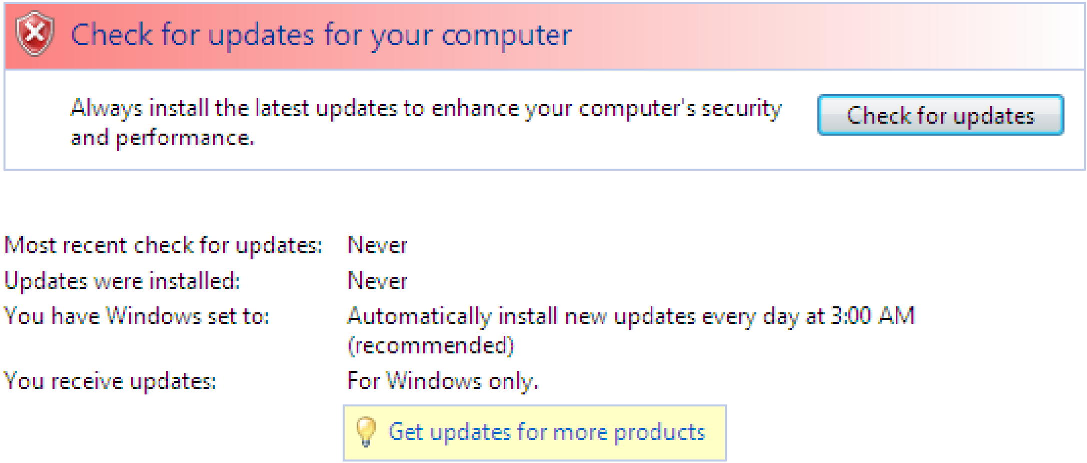
By default, the user will not be asked for a password. However, this will limit the user to log in locally only. You should ask the user to setup a password, or you may do so for the user by following the same steps we used above for the administrator.

## 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".*



Check for updates for your computer

Always install the latest updates to enhance your computer's security and performance.

Most recent check for updates: Never

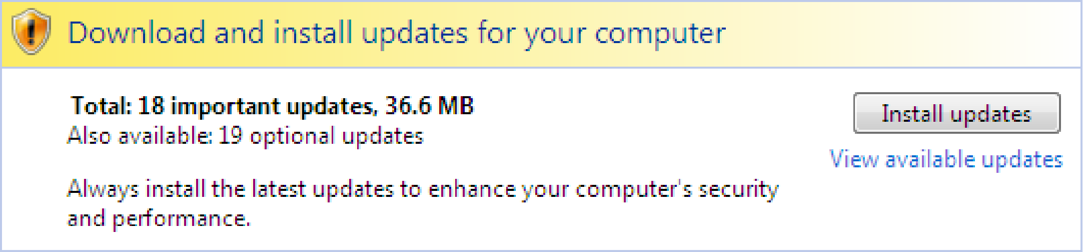
Updates were installed: Never

You have Windows set to: Automatically install new updates every day at 3:00 AM (recommended)

You receive updates: For Windows only.

*Illustration 15: Check for updates dialog.*

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



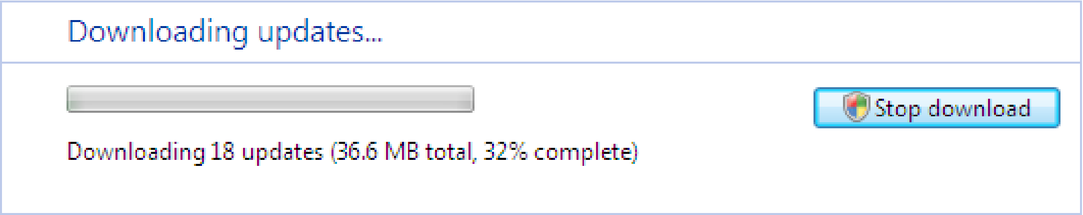
Download and install updates for your computer

**Total: 18 important updates, 36.6 MB**
Also available: 19 optional updates

Always install the latest updates to enhance your computer's security and performance.

*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.*

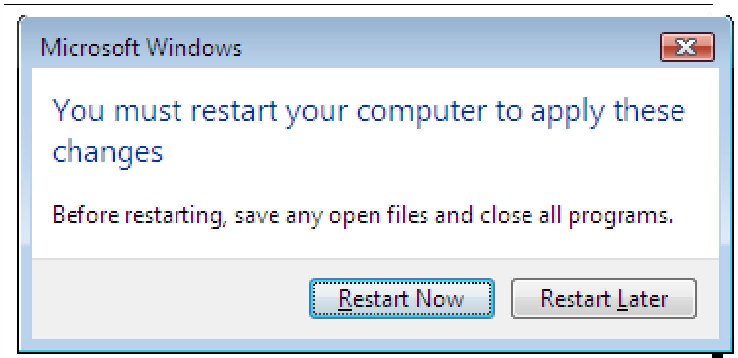


Downloading updates...

Downloading 18 updates (36.6 MB total, 32% complete)

*Illustration 17: Downloading updates.*

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



You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

*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.

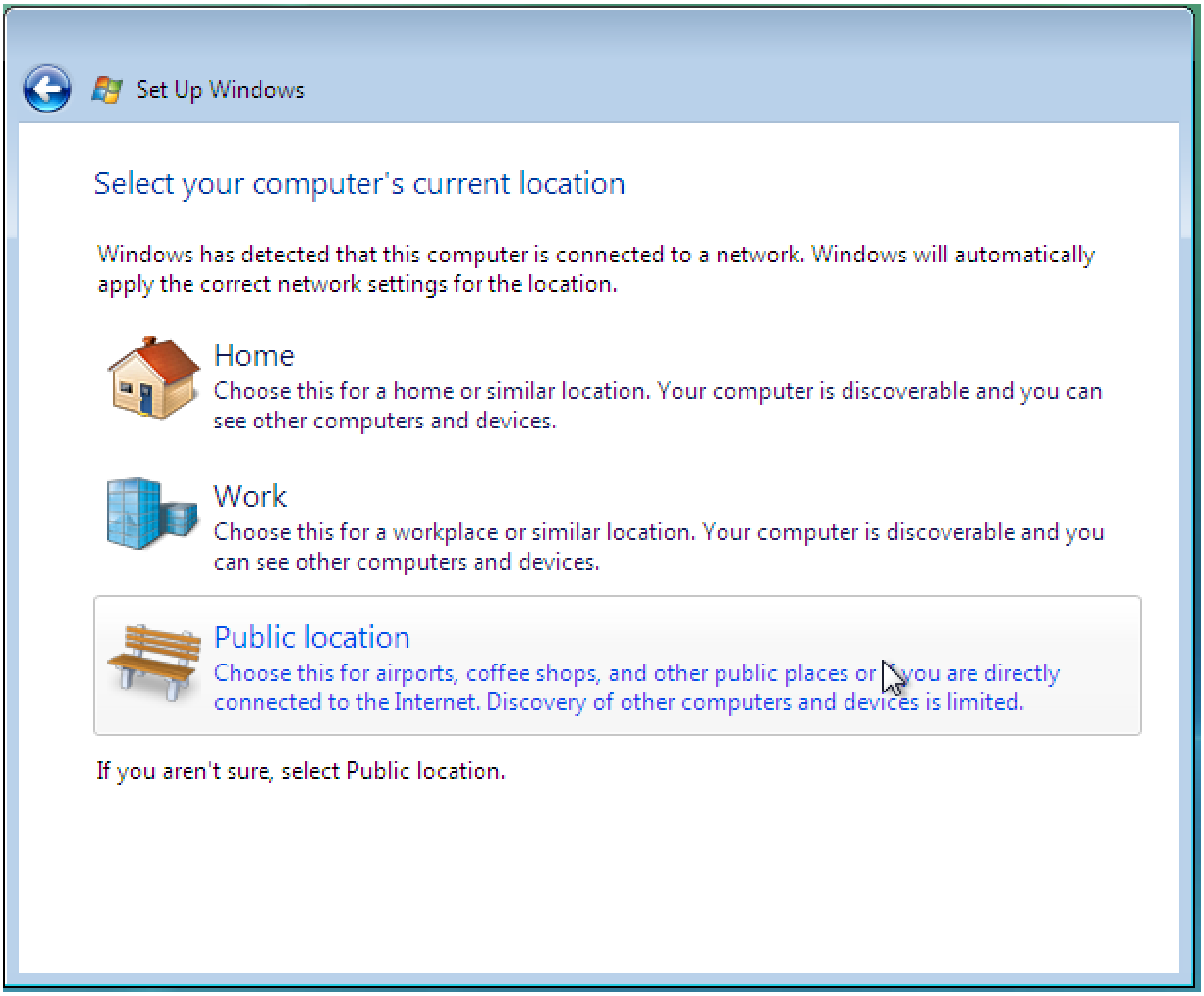
### *Automatic Updates*

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.



Select your computer's current location

Windows has detected that this computer is connected to a network. Windows will automatically apply the correct network settings for the location.

Home
Choose this for a home or similar location. Your computer is discoverable and you can see other computers and devices.

Work
Choose this for a workplace or similar location. Your computer is discoverable and you can see other computers and devices.

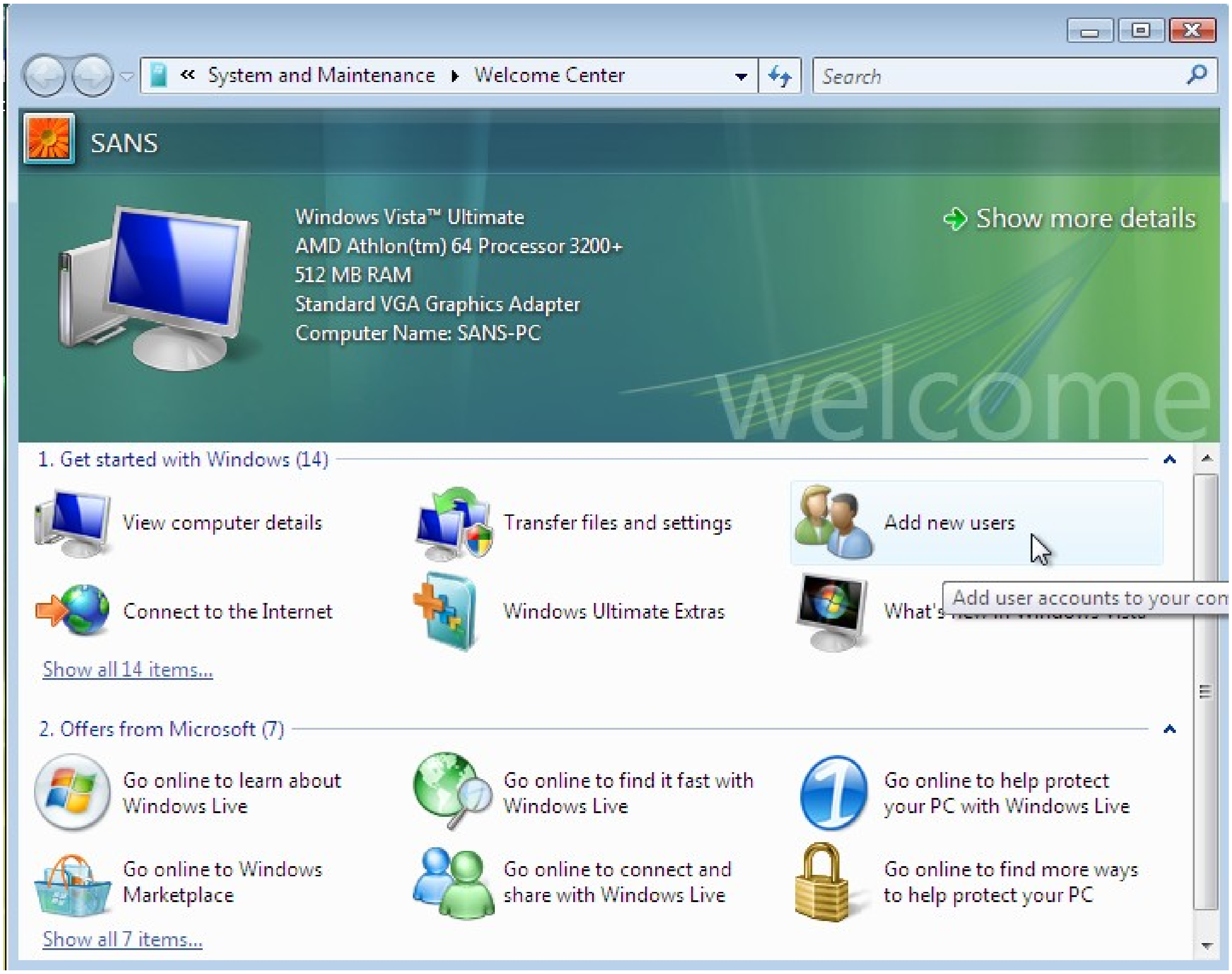
Public location
Choose this for airports, coffee shops, and other public places or if you are directly connected to the Internet. Discovery of other computers and devices is limited.

If you aren't sure, select Public location.

*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*".

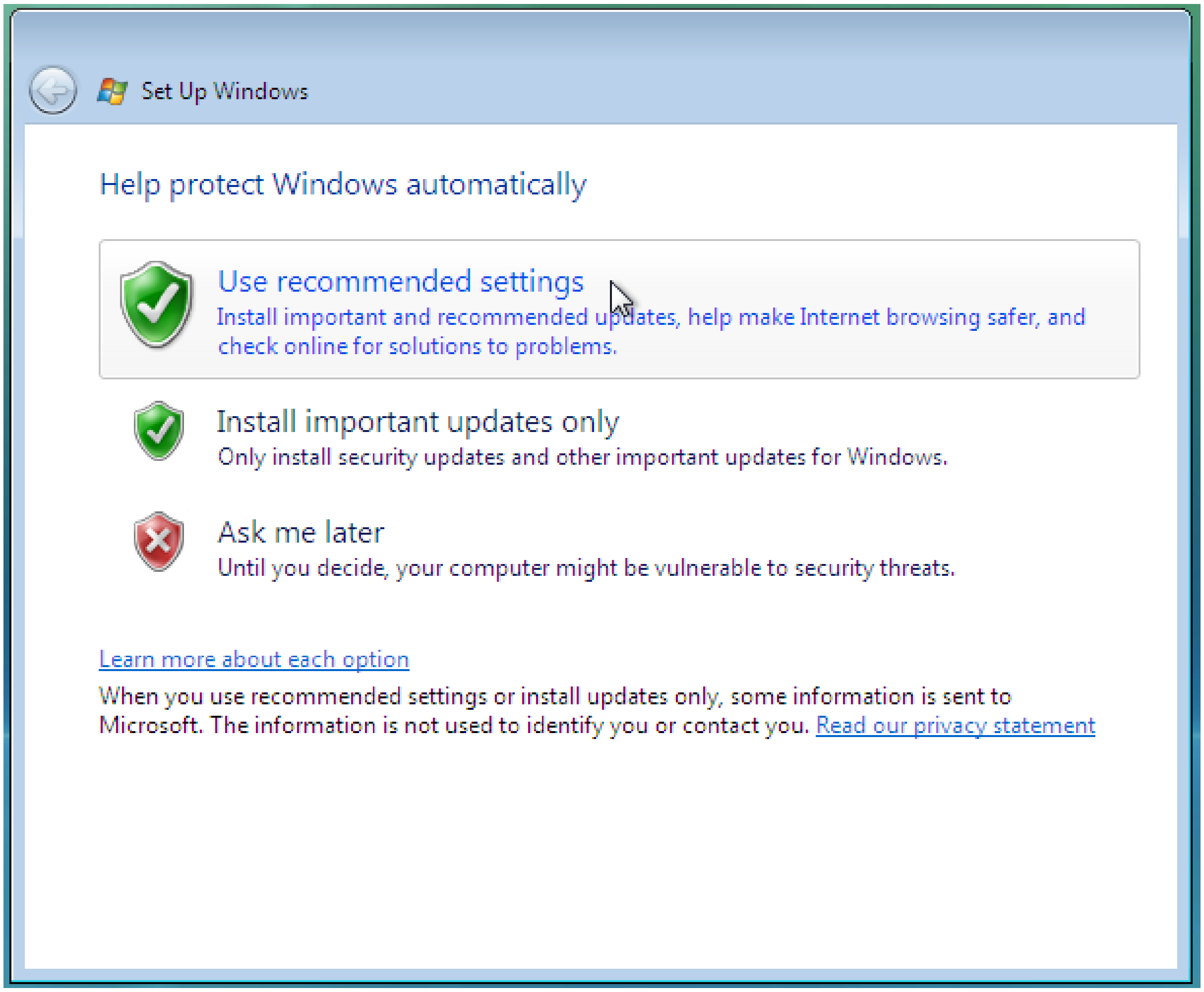


« System and Maintenance ▸ Welcome Center
Search
SANS
Show more details
welcome

Windows Vista™ Ultimate
AMD Athlon(tm) 64 Processor 3200+
512 MB RAM
Standard VGA Graphics Adapter
Computer Name: SANS-PC

1. Get started with Windows (14)
View computer details
Transfer files and settings
Add new users
Connect to the Internet
Windows Ultimate Extras
What's new in Windows Vista
Add user accounts to your com
Show all 14 items...
2. Offers from Microsoft (7)
Go online to learn about Windows Live
Go online to find it fast with Windows Live
Go online to help protect your PC with Windows Live
Go online to Windows Marketplace
Go online to connect and share with Windows Live
Go online to find more ways to help protect your PC
Show all 7 items...

*Illustration 20: Control Panel after first login.*



Help protect Windows automatically

Use recommended settings
Install important and recommended updates, help make Internet browsing safer, and check online for solutions to problems.

Install important updates only
Only install security updates and other important updates for Windows.

Ask me later
Until you decide, your computer might be vulnerable to security threats.

Learn more about each option

When you use recommended settings or install updates only, some information is sent to Microsoft. The information is not used to identify you or contact you. Read our privacy statement

*Illustration 21: Automatic Update Settings during Installation.*

Last Updated: September 11th, 2012

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| **SANS Forensics Prague 2012** | **Prague, CZ** | **Oct 07, 2012 - Oct 13, 2012** | **Live Event** |
| **SEC 579: Virtualization and Private Cloud Security @ Bangalore** | **Bangalore, IN** | **Oct 08, 2012 - Oct 13, 2012** | **Live Event** |
| **SANS CyberCon 2012** | **Online, VAUS** | **Oct 08, 2012 - Oct 13, 2012** | **Live Event** |
| **SOS: SANS October Singapore 2012** | **Singapore, SG** | **Oct 08, 2012 - Oct 20, 2012** | **Live Event** |
| **SANS Gulf Region 2012** | **Dubai, AE** | **Oct 13, 2012 - Oct 25, 2012** | **Live Event** |
| **SANS Seattle 2012** | **Seattle, WAUS** | **Oct 14, 2012 - Oct 19, 2012** | **Live Event** |
| **SANS Baltimore 2012** | **Baltimore, MDUS** | **Oct 15, 2012 - Oct 20, 2012** | **Live Event** |
| **SANS@ Grid Security Conference 2012** | **San Diego, CAUS** | **Oct 16, 2012 - Oct 16, 2012** | **Live Event** |
| **SANS South Africa 2012 - Cape Town** | **Cape Town, ZA** | **Oct 26, 2012 - Oct 27, 2012** | **Live Event** |
| **SANS Chicago 2012** | **Chicago, ILUS** | **Oct 27, 2012 - Nov 05, 2012** | **Live Event** |
| **SANS South Africa 2012** | **Johannesburg, ZA** | **Oct 29, 2012 - Nov 03, 2012** | **Live Event** |
| **SANS Bangalore 2012** | **Bangalore, IN** | **Oct 29, 2012 - Nov 03, 2012** | **Live Event** |
| **SANS Korea 2012** | **Seoul, KR** | **Nov 05, 2012 - Nov 13, 2012** | **Live Event** |
| **SANS Tokyo Autumn 2012** | **Tokyo, JP** | **Nov 05, 2012 - Nov 10, 2012** | **Live Event** |
| **FOR526 Beta** | **Denver, COUS** | **Nov 05, 2012 - Nov 09, 2012** | **Live Event** |
| **SANS Sydney 2012** | **Sydney, AU** | **Nov 12, 2012 - Nov 20, 2012** | **Live Event** |
| **SANS San Diego 2012** | **San Diego, CAUS** | **Nov 12, 2012 - Nov 17, 2012** | **Live Event** |
| **SANS London 2012** | **London, GB** | **Nov 26, 2012 - Dec 03, 2012** | **Live Event** |
| **SANS San Antonio 2012** | **San Antonio, TXUS** | **Nov 27, 2012 - Dec 02, 2012** | **Live Event** |
| **European SCADA and Process Control System Security Summit 2012** | **Barcelona, ES** | **Dec 05, 2012 - Dec 11, 2012** | **Live Event** |
| **SANS Cyber Defense Initiative 2012** | **Washington, DCUS** | **Dec 07, 2012 - Dec 16, 2012** | **Live Event** |
| **SANS Network Security 2012** | **OnlineNVUS** | **Sep 16, 2012 - Sep 24, 2012** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |