

Microsoft Security Essentials User Guide

Compiled and written by

Le Roy Acres Web Services© 2010

Foreward

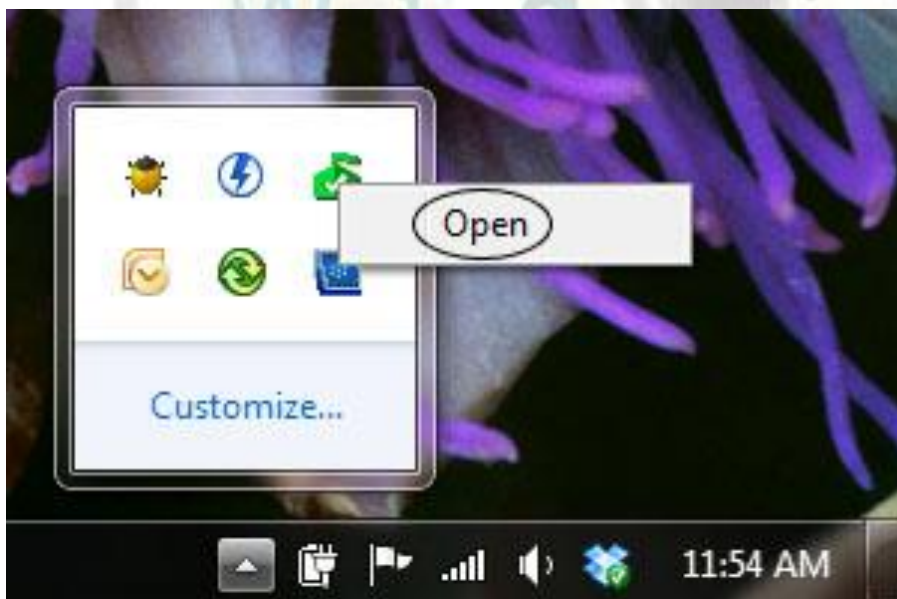
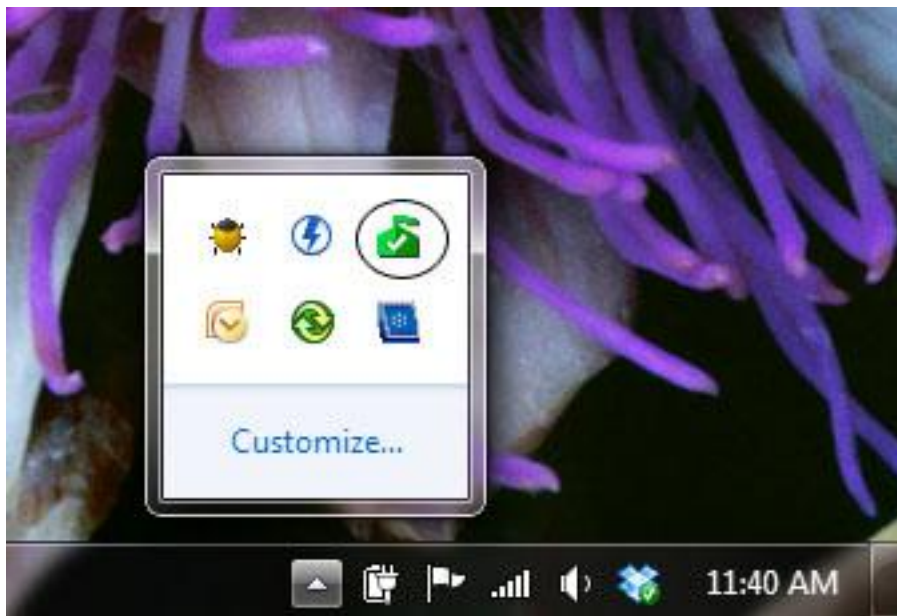
This is the first of numerous tutorials concerning some of the more basic maintenance routines that every personal computer owner should be acquainted with. Please follow along with the text and illustrations as we go along and for your own safety do not skip ahead until you are well familiarized with the routine methodology. The computer world is inhabited with malignant programs and routines that are commonly known as virus', Trojans, Root-kits, and other lesser known names. These programs can range from being mildly annoying all the way to being down rite destructive of your data and/or hardware (in some very rare cases). Because of these malignant programs it has become necessary for the average user to take precautionary steps to prevent infection of their systems by using programs such as Microsoft Security Essentials. In this tutorial we will attempt to teach you the very basic of steps necessary to help to ensure your data and your machine's safety in this ever more dangerous electronic world. Note: these are the most basic features, there are more advanced features that are beyond the scope of this document to inform you of at this time. Usage of the more advanced features are solely upon the user and may cause system disruption or may cause your system to become unstable or unresponsive.

This tutorial may be printed out from this PDF document. This material may be freely given without the consent of it's author as long as the copyright is maintained. You may not claim this work as your own nor may you charge any amount of funds for this document except for the amount of publishing or the amount of the media upon which it is distributed (e.g. – CD, DVD, 3.5" floppy disc).

Now on to the tutorial:

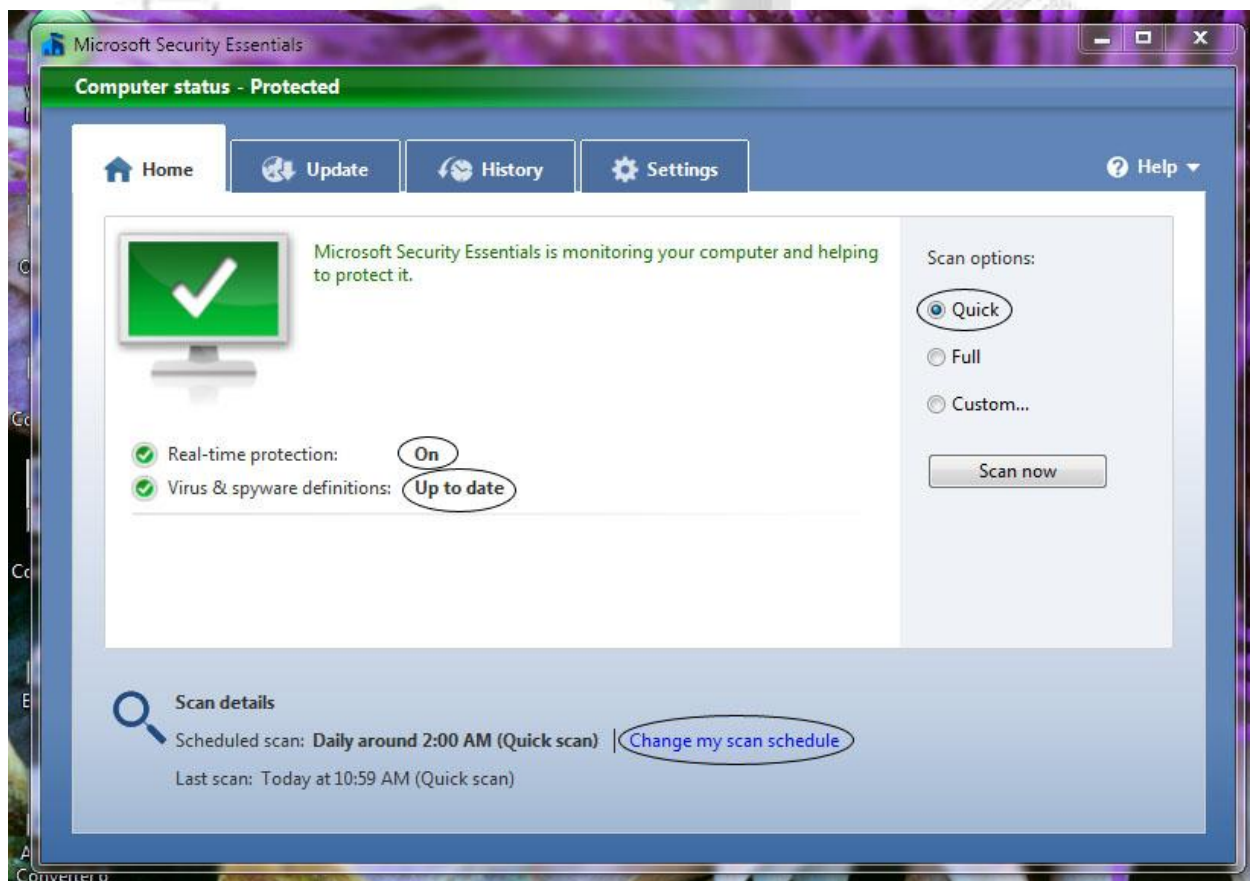
Step One:

Below is an image of the Microsoft Security Essentials (MSE) icon found on a Windows 7 machine in the lower right portion of the Toolbar. A similar image will be displayed on earlier versions of Windows Operating Systems. Please click on it and select Open.



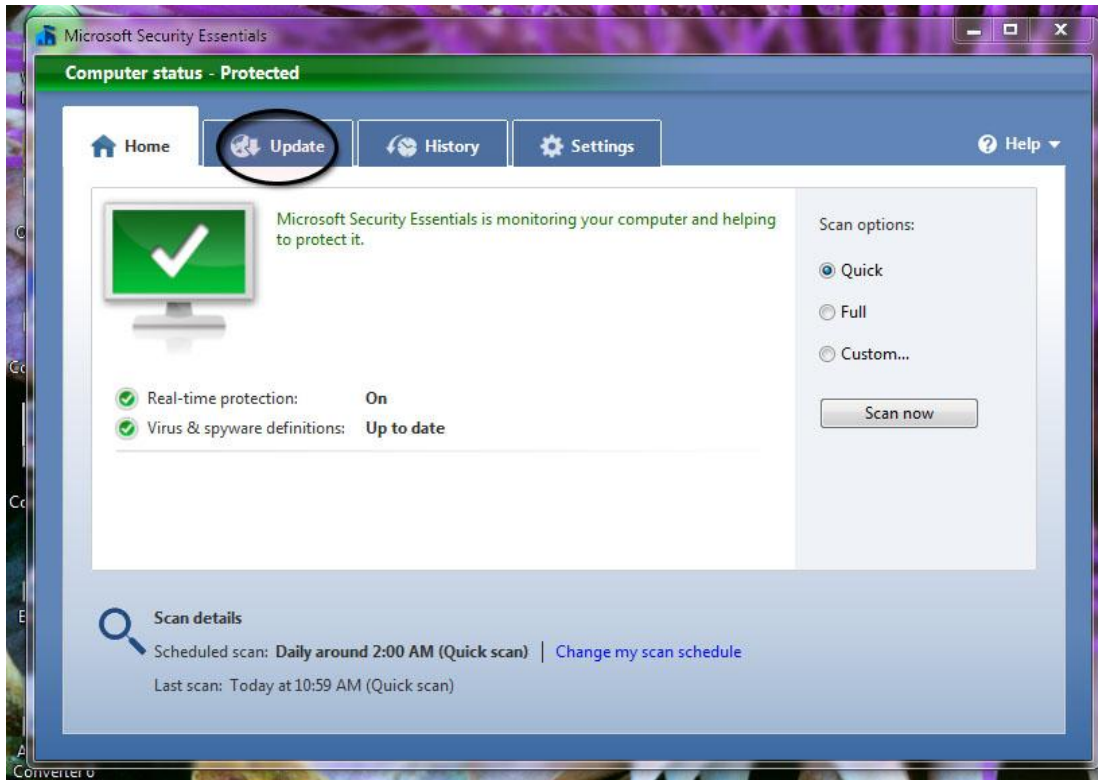
Step Two:

Below is an image showing the initial screen you will find upon opening MSE. You will note the areas circled and become familiar with them as they contain important information that determines what steps you need to take next. Let's take a quick moment to go over these features. The first item to look at is to see if the Real-time Protection is enabled (it should be). If this feature is not enabled you can enable it by going to the Settings tab at any time and enabling this feature. Now look at the Scan Options and ensure that the Quick feature is selected. You will also note the Change My Scan Schedule link at the bottom of the window. This feature will be used to setup your schedule for the program to automatically update your system definitions and run an automatic scan periodically. Now look at the Virus & spyware definitions line. If your system reports being up to date on the Virus & Spyware definitions you may skip to Step Five.



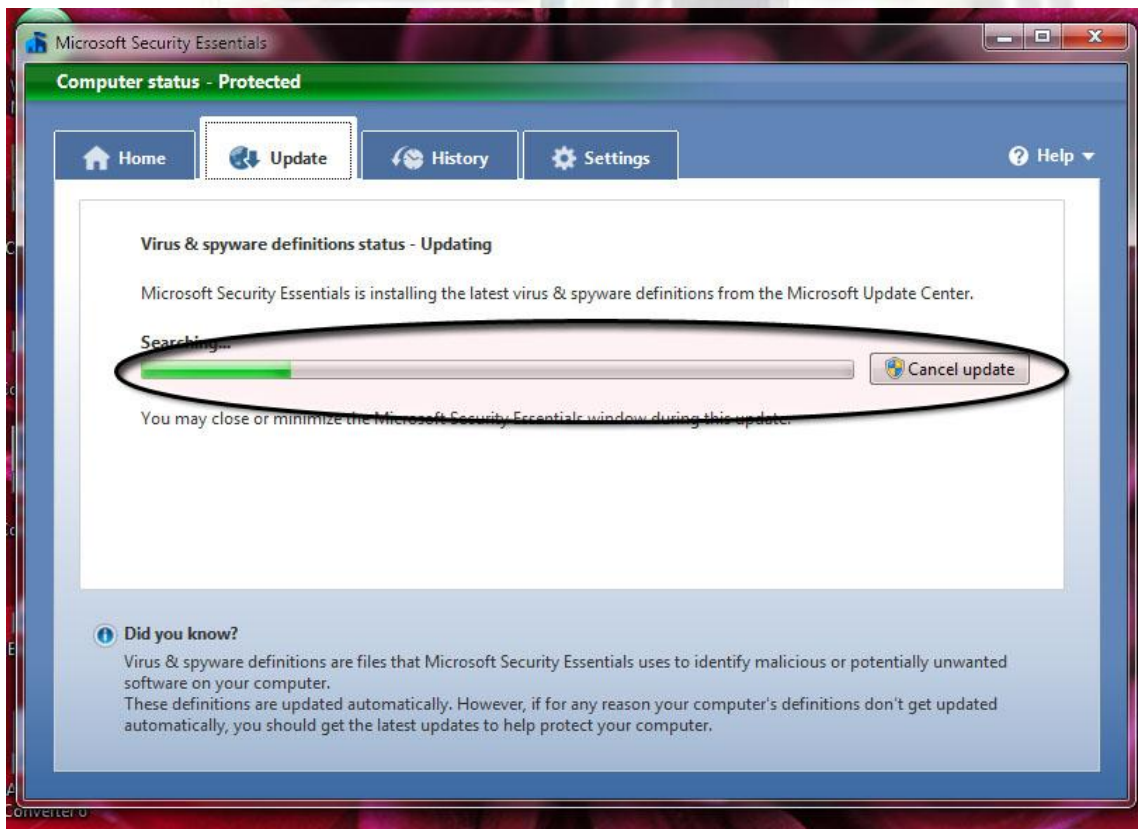
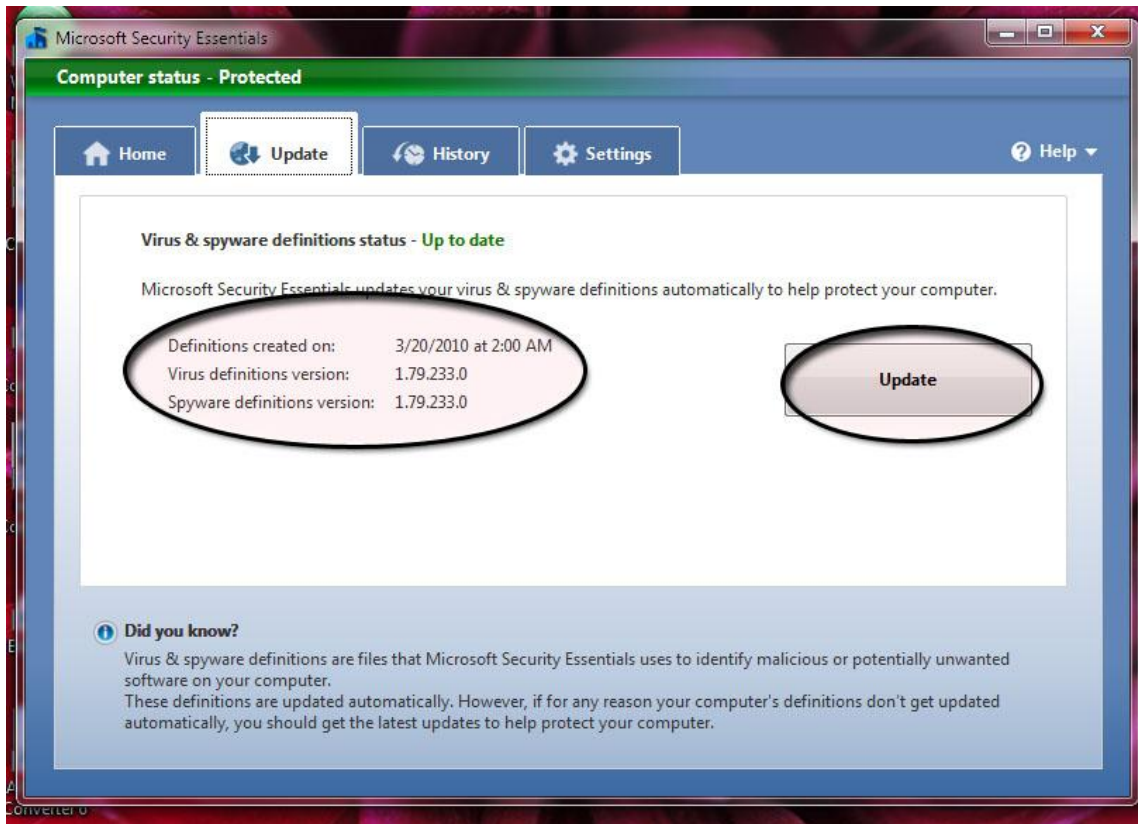
Step Three:

If your system reports that it is not up to date then you will need to click on the Update tab at the top of the window as shown here:



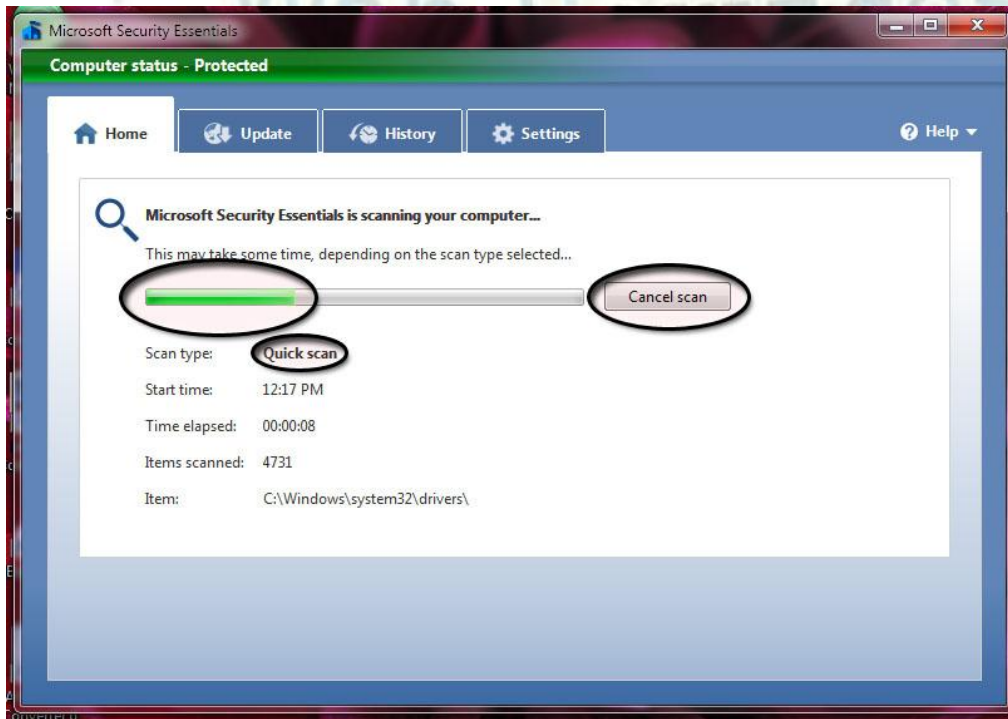
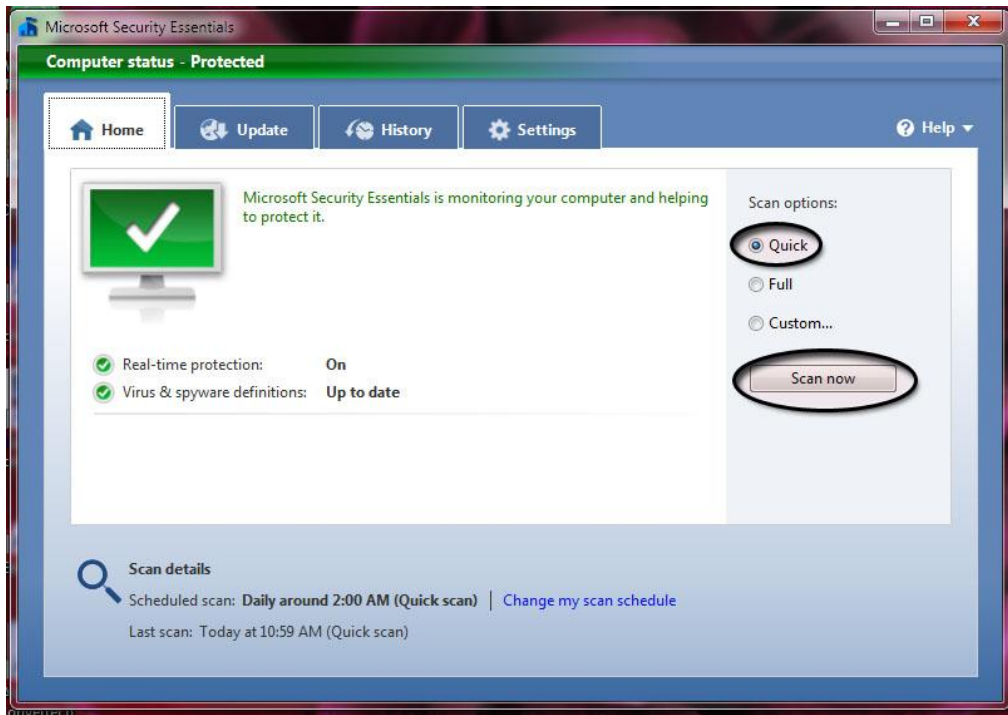
Step Four:

Once you have done this you will get the following window. This window will tell you information concerning the virus definitions and will provide you with a button to Update your definitions now. In order to update the definitions you MUST be connected to the Internet or have a virus definition file on some type of removable media (such as CD, DVD, Flashdrive, 3.5" floppy disk). If you are not currently connected to the Internet at this time please stop and do so. Also be advised that some definition files can be quite large so if you are not on a broadband connection (such as Cable, DSL, or Sattelite) the download time will be significantly longer. Please click on the Update button now and allow the update to be downloaded and installed. You may watch the process on the progress bar shown in the second image but personally I would go get a drink and occupy yourself otherwise until the process is complete.



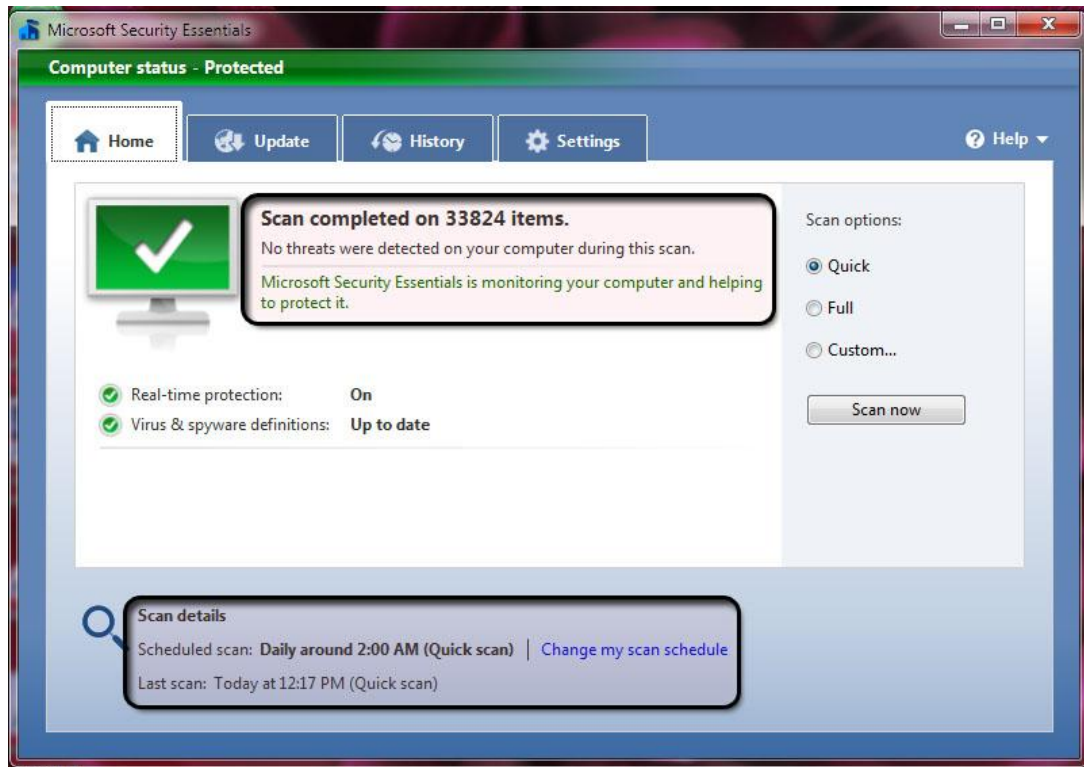
Step Five:

Once the update is complete you will return to the Home tab to begin the scanning process. Ensure that the Scan Option is set to Quick and then click on Scan Now. Go get another drink and please do not use your computer while the scan is being conducted.



Step Six:

Once the process is finished you will be able to see if your system has been infected or not. In the case of an infection, simply follow the advice of the program to get rid of the file(s) affected. The system may offer choices of quarantine, delete or ignore according to the severity of the risk. This program is quite intuitive and generally speaking it will choose the appropriate action for the type of infection detected. The final screen will be as below with information that you may find interesting to note.



You are welcome to explore the other options of this program but please do so with a moderate amount of caution. Usually nothing bad will happen to your system but you may forget what options you changed and may end up with some features you do not necessarily wish to have turned on. We hope you have found this tutorial helpful.