



## Sophos Anti-virus Basic Level Handout

Sophos Anti-Virus provides cross-platform protection against:

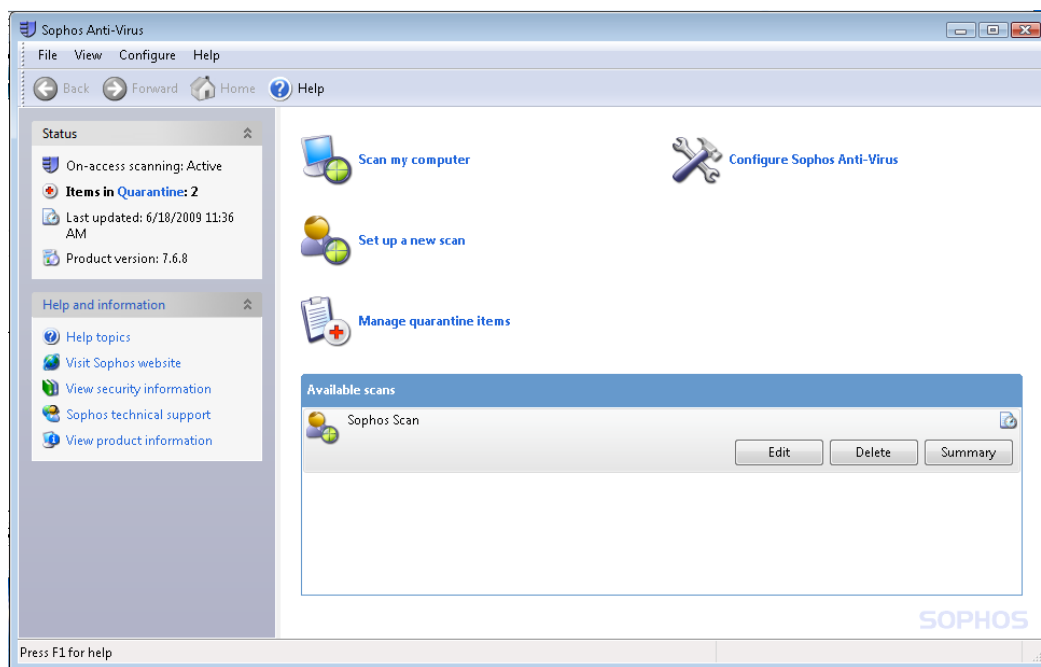
- **Computer viruses**
- **Potentially Unwanted Applications (PUA's)** such as spyware and adware
- **Host intrusions (HIPS)** such as suspicious files, behaviors and buffer overflow attacks

It provides on-access and on-demand scanning for most platforms.

### System requirements for Sophos Anti-Virus for Windows, version 7

Platforms supported	x86 32-bit	x86 64-bit	IA-64 (Itanium) 64-bit	Minimum disk space	Minimum memory
<b>Sophos Anti-Virus for Windows</b>					
Windows Server 2008	✓	✓	✓	120 MB	256 MB
Windows Vista	✓	✓			
Windows Server 2003	✓	✓	✓		
Windows XP Home SP1a+	✓	✓			
Windows XP Pro SP1a+	✓	✓			
Windows 2000 SP3	✓				
Windows 2000 Pro SP3+	✓				
WePOS SP2	✓				
VMWare ESX 3.0/3.5	✓				
VMWare Workstation 5.0	✓				
VMWare Server 1.0	✓				
<b>Sophos Client Firewall</b>					
Requires Pentium class 300 MHz processor					
Windows 2000 Pro SP3+	✓			100 MB	320 MB
Windows XP Home SP1a+	✓				
Windows XP Pro SP1a+	✓				
Windows Vista	✓				

The components of the Sophos Anti-Virus window are described below.



**Toolbar** – this contains buttons for getting help and navigating between the pages in the right-hand pane of the *Sophos Anti-Virus* window.

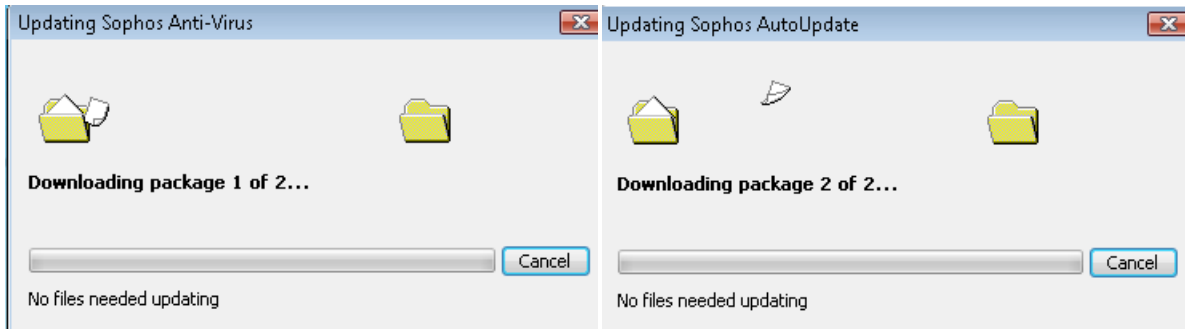
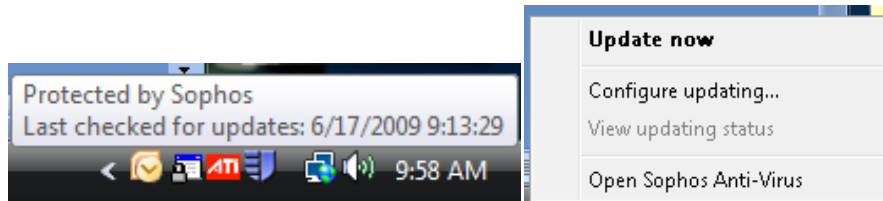
**Status** – this contains the status of on-access scanning, the number of items in Quarantine, the last time Sophos Anti-virus was updated and the product version number.

**Help and Information** – This enables you to contact Sophos technical support, and access help with Sophos Anti-virus and information on threats and controlled applications.

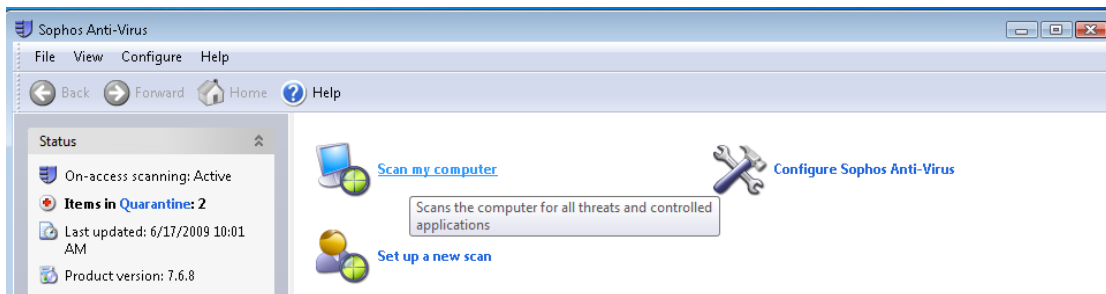
**Activity Summary** – this appears when you run a scan, and contains information about any items found.

**Home Page** - This is displayed in the right-hand pane when you open the Sophos Anti-Virus window. It includes the available task list and the available scans list. As you use the Sophos Anti-Virus window, the content of the right-hand pane may change. You can return to the home page by clicking on the **Home** button.

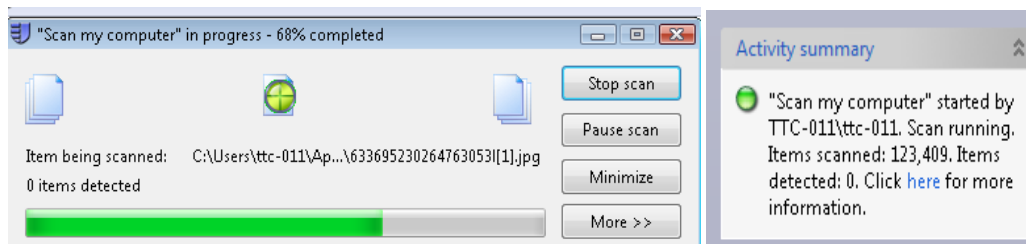
**How do I scan my computer using Sophos Anti-Virus program?** On the bottom of your Windows Taskbar, **Right-Click on the purple shield (Sophos Anti-Virus)**, then select **Update now** (this will download the anti-virus updates to your computer). See sample below.



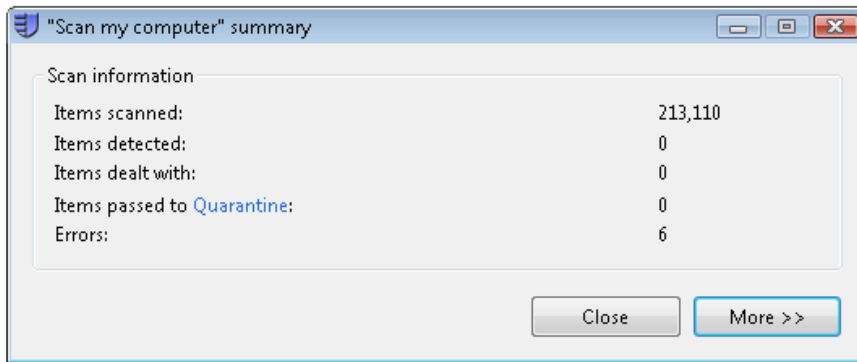
1. On the bottom of your Windows Taskbar, **Right-Click on the purple shield (Sophos Anti-Virus)**, then select **Open Sophos Anti-Virus**, then Click on **Scan my computer**.



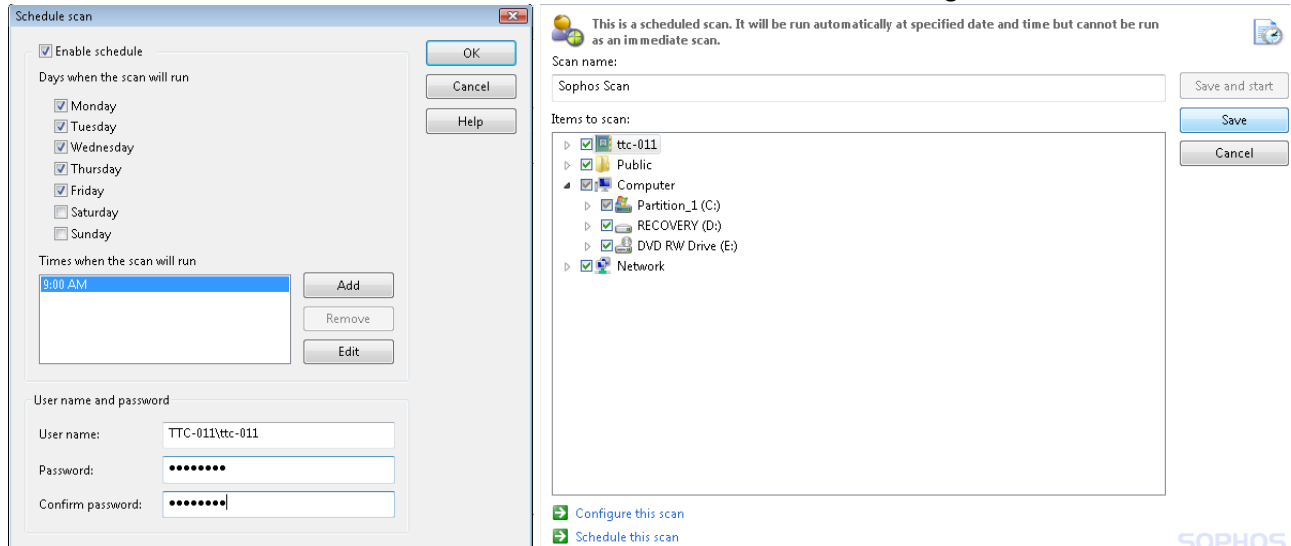
2. When Sophos is scanning for Anti-Viruses, you have the capability of **stopping scan, pause scanning, minimized dialog box**, or click **More** to find out a list of items scanned and detected. In the left hand side, you will be able to see the Activity Summary being scanned on your computer.









3. When the scan is completed, below is the message that you will receive.



4. **How do I schedule a Sophos scan on my computer?** In the right-hand pane of the **Sophos Anti-Virus** window, click **Set up a new scan**. In the **Items to scan (select the folders and drives that you want to scan)**, then type in a scan name: **Sophos Scan** (sample). Click on **Schedule this scan**, and then place a check mark on **Enable schedule**. Select the day(s) on which the scan should run. Add the time(s) by clicking **Add**. If necessary, remove or edit a time by selecting it and clicking **Remove** or **Edit**, respectively. Type a **user name** and **password**. Password cannot be blank. Click **ok**. The scheduled scan runs with the access rights of that user. Click **Save**.



5. **What does each Sophos Anti-Virus system tray icon represent? See Table Below for each labeled description.** The Sophos Anti-Virus systems tray icon is always displayed, even if the Sophos Anti-Virus windows is closed.

Icon Appearance	Explanation
	A <b>blue shield</b> means that on-access scanning is active. Sophos Anti-Virus updated successfully last time.
	If a <b>green stripe appears running over a blue shield</b> , this means that Sophos Anti-Virus is updating. On-access scanning is active.
	If a <b>red circle with a white cross</b> in it appears over a blue shield, this means that updating has failed. On-access scanning is active.
	A <b>gray shield</b> means that on-access scanning is inactive. Sophos Anti-Virus updated successfully last time.
	If a <b>green stripe appears running over a gray shield</b> , this means that Sophos Anti-Virus is updating. On-access scanning is inactive.
	If a <b>red circle with a white cross in it appears over a gray shield</b> , this means that updating has failed. On-access scanning is inactive.

6. **What is on-access scanning?** *On-access scanning* intercepts files as they are accessed, and grants access to only those that do not pose a threat to your computer or are authorized for use. The computer is protected by on-access scanning. When the on-access scanning is active, a blue shield is displayed in the system tray. However, when on-access scanning is active, a blue shield is displayed in the systems tray.
7. **What is an on-demand scan?** An *on-demand scan* is a scan of the computer, or parts of the computer, that you can run immediately or schedule to run at another time.
8. **What is a right-click scan?** A *right-click scan* is a scan of selected item(s) in Windows Explorer or on the desktop, that you can run by right-clicking the selection to display a menu, and selecting **Scan with Sophos Anti-Virus**
9. **What is runtime behavior analysis?** *Runtime behavior analysis* comprises suspicious behavior detection and buffer overflow detection. Suspicious behavior detection is the dynamic analysis of all programs running on the computer to detect and block activity that appears to be malicious.

10. **How do I scan a single item folder?** Open Windows Explorer. To do this, at the taskbar, click **Start | Programs | Accessories | Windows Explorer**. Select the file(s), folder(s) and/or disk drives you want to scan. Right-click the selection to display a menu, and select **Scan with Sophos Anti-Virus**. A progress dialog box is displayed. If any threats or controlled applications are found, click **More** and refer to *Managing quarantine items*. To stop scanning, click **Stop scan**.

11. **Representation of items to scan** In the **Items to scan** panel, different icons are displayed in the check box next to each item (drive or folder), depending on which items will be scanned. These icons are shown below with explanations. The item and all sub-items *are not* selected for scanning. The item and all sub-items *are* selected for scanning. The item is partially selected: the item is not selected, but some sub-items are selected for scanning. The item and all sub-items are excluded from this particular scan. The item is partially excluded: the item is selected, but some sub-items are excluded from this particular scan. The item and all sub-items are excluded from all on-demand scans, because of an on-demand exclusion that has been set up.

Icon	Explanation
<input type="checkbox"/>	The item and all sub-items <i>are not</i> selected for scanning.
<input checked="" type="checkbox"/>	The item and all sub-items <i>are</i> selected for scanning.
<input checked="" type="checkbox"/>	The item is partially selected: the item is not selected, but some sub-items are selected for scanning.
<input checked="" type="checkbox"/>	The item and all sub-items are excluded from this particular scan.
<input checked="" type="checkbox"/>	The item is partially excluded: the item is selected, but some sub-items are excluded from this particular scan.
<input checked="" type="checkbox"/>	The item and all sub-items are excluded from all on-demand scans, because of an on-demand exclusion that has been set up. For information, see <a href="#">Excluding items from scanning</a> on page 18.