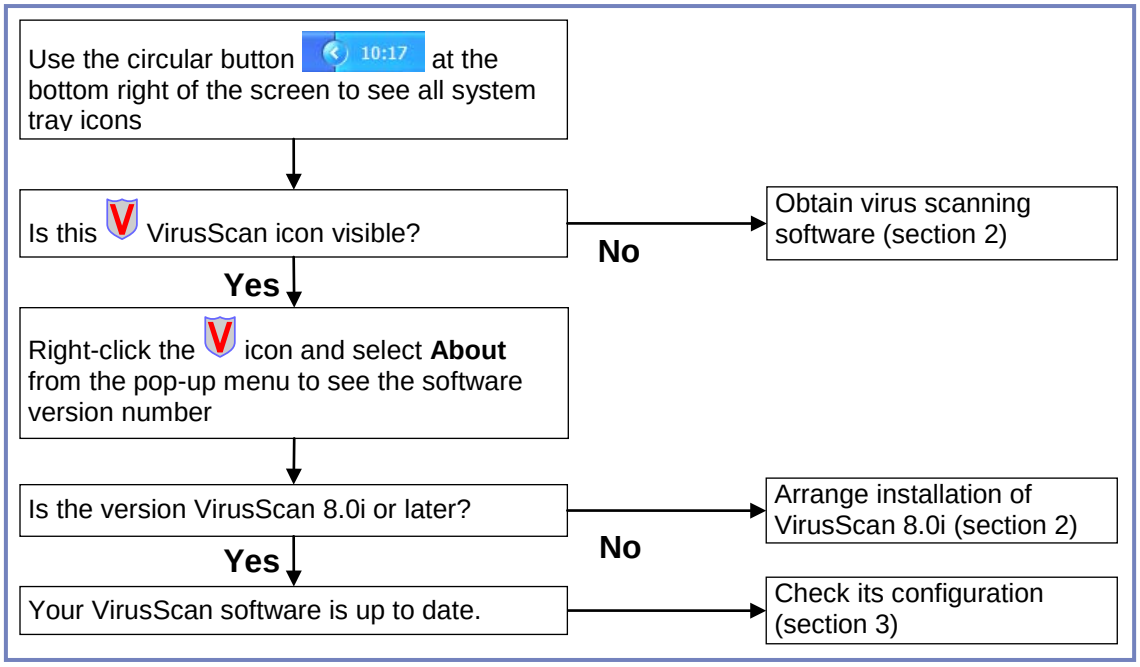
How to set up McAfee virus scanning software and become computer virus savvy

A virus infection of your workstation can seriously disrupt your learning, teaching, or research. You should arrange need virus protection on your computer at home if you regularly move files between there and the University. This guide suggests good virus protection practice.

1 Does your PC have up to date virus protection software?



2 How to obtain VirusScan Enterprise

- All PCs in The Libray Open Access areas already have installed virus scanning software.
- If you are a member of staff at this University, you should contact your local technical support staff who can install the McAfee virus scanning software on your office computer for you.
- If you are a student staying in University Residences and own a computer connected to the Residences Network, you will be entitled to use the virus scanning software under the University's licence. The Halls of Residence technical team can install the software for you, and to arrange this, you should contact ITS Service Desk by phone, email or web form — please visit www.its.salford.ac.uk/students/ for details.

3 How to configure VirusScan Enterprise

Most of the installed default settings for McAfee VirusScan will be satisfactory for your purpose but you may wish to set fine tune some settngs to suit your lifestyle. The following advice covers only those settings that you really need to change. If you reach a point where you are unsure which settings you have changed, section 3.3 offers a fresh start remedy!

3.1 General options

Start **VirusScan Console** from the **Start** → **Programs** menu, where you will find it under McAfee

- Select from the menus, **Task** → **On Access Scanner properties**.
- Select **All Processes** in the left panel of the window, then:
  - Under the **Detection** tab, in the *Scan Files* section, ensure that **When writing to disk** has a tick ☑ and that **When reading from disk** has no

tick ☐

- Under the **Advanced** tab, ensure that all 4 items have ticks: ☑

- Select **OK** and return to the VirusScan Console window.
- In the **Task** column of the VirusScan Console window, open **Auto Update**, select the **Schedule** button, then the **Schedule** tab. The settings here determine when VirusScan should update its database of virus signatures by checking your installation against McAfee's Web pages. Make these settings:
  - Schedule task: **daily**
  - Start time: **13:00**. Adjust this to suit your habits. Auto Update takes only a few minutes, and should be scheduled for a time when you know your PC will be switched on.
- Use the OK button to close the Schedule Settings window, and then the VirusScan Auto Update Properties window.
- Open **Unwanted programs policy** in the VirusScan Console window. Select the **Detection** tab and check the tickable list. ITS recommend that all the items should have ticks ☑, except **Remote administration tools**.

3.2 Settings for on-demand scanning

You should schedule VirusScan to check all files on the local fixed drives of your PC once per week. Usually, this will include just your C: drive — CD drive, pen drive and floppy drive are automatically excluded. Here is a general strategy for protection.

- ITS regularly scans networked drives, so there is no need to include your F: drive (etc) in your on-demand scan. If you decide to include your network drives in your on-demand scans, go to the VirusScan Console's **Detection** tab (as described in section 3.1) and ensure that the item **On network drives** is ticked: ☑
- Schedule a scan for a day and time when you know your PC will be switched on. For example, if you leave your PC switched on while attending a meeting every Thursday at 14:00, then this could be a suitable start time[1].
- Choose a time when you will not be using your workstation, since the scan may take an hour. In theory, you can work while it is taking place but the scan will absorb most of the PC's attention.
- If your PC is switched off at the scheduled time, VirusScan will skip it and wait until the next scheduled time.

To schedule the scan in this example, start VirusScan Console, and make these settings:

a) In the **Task** column, open the item **Scan all fixed disks.**

b) Use the **Schedule** button to see the Schedule Settings window.

c) Select the **Task** tab and ensure that there is a tick ☑ beside **Enable.**

d) Select the **Schedule** tab in the same window, and set its fields to your chosen values. For example:
   - Schedule task: **weekly**

- Start time: **13:00**, local time
- Every **1** week(s) on ☑ **Thu**

e) Close the Schedule Settings window with the OK button, close the VirusScan on-demand Properties window, and finally close VirusScan Console itself.

4 Virus-safe working

4.1 What they are, how they spread

A computer virus tries to insert itself into an existing system file or document on your PC. When Windows executes an infected file, or when you open an infected document, the virus becomes active and spreads by sending copies of itself to other workstations on the network. The term *Malware* (malicious software) includes other types of threat, but Virus and Malware are often used interchangeably.

Some creators of malware try to gain attention by causing widespread disruption and annoyance, such as preventing host workstations from starting up properly. Viruses may deliberately swamp an organisation's email servers and other services by sending huge numbers of requests from the infected workstations.

A *key logger* is an example of Malware that invades your privacy. For example, when you connect to a Web address that starts with https:// the information passing from your workstation to that web address is encrypted to secure it against snoopers. However, a key logger infecting your workstation will memorise the keys you press before the information is encrypted for sending. It notices when you are typing into a username and password box, gathers your keystrokes, and quietly sends this harvested information to a collecting site elsewhere on the Internet.

The Anti Virus software described here will protect you against viruses, worms, and other forms of Malware.

4.2 Scanning particular disc drives or files

If you set up McAfee VirusScan as described in section 3, it will automatically check all files as you save them from an application. The same applies if you are using a PC in an open access area with the standard ITS setup.

Check a pen drive (memory stick) that you use regularly, since the automatic on demand scanning set up in section 3.2 will not scan these drives:

- Plug in your pen drive, and open **My computer** on your PC desktop.
- You should see the pen drive listed.
- Right click on the pen drive, and select **Scan for viruses** from the context menu.

In the same way, you can browse in **My computer** until a particular filename is in view, and then right click it to scan just that file.

4.3 How to avoid viruses

- Install up to date virus scanning software, as in section 1. The scanning software should detect attempts to install viruses or malware and will protect your PC.

- Most viruses spread through email. ITS scans email coming to University of Salford addresses but you can still import a virus if you connect to an external email account (such as Yahoo or Hotmail) from a University PC. If you do this, be cautious about opening an email message (or an attachment) unless you trust the sender.
- Be cautious when downloading software from the Web and then installing it. When you download software from a reputable site, its installation program should make authenticity checks before continuing with installation.
- At regular intervals, make back up copies of data files that you keep on your PC's hard drive, and store these copies somewhere away from your computer. Files on your network drive are backed up regularly by ITS.
- Microsoft Office applications such as Word and Excel have a sophisticated macro capability that can be used by a virus. By merely opening an infected file, you can cause the virus to become active. As well as your virus scanning software, a good defence is to switch Word into high security mode for macros. Select from the menus **Tools**→ **Macro**→ **Security**, then select **high** as security level.

You can find background information at http://en.wikipedia.org/wiki/Malware and in the documentation from McAfee that you can obtain as explained in section 2