Anti-virus – SCEP and Windows Defender

The University of Aberdeen uses System Center Endpoint Protection software (SCEP) and Windows Defender to protect servers and networked Windows PCs against viruses, spyware and other malicious software.

Malicious software can try to install itself on your computer any time you connect to the Internet, or when you install a program using a CD, DVD, or other removable media. Once installed, it may not be immediately apparent as it can be programmed to run at unexpected times.

SCEP and Windows Defender prevent malicious software from infecting your computer via:

- **Real-time protection**
  By default, Endpoint Protection is configured to monitor your computer all the time and will alert you when a virus or other malicious software attempts to install or run on your computer.

- **Automatic scan**
  A full system scan is scheduled to run automatically every Wednesday lunchtime on all University computers.

- **Manual scan**
  You can also manually set Endpoint Protection to scan your whole PC or specific drives, files or folders for potential threats that might put your computer at risk.

Common symptoms of an infection

The presence of malware on your computer may not always be immediately obvious, so it’s important to run regular scans; however, some of the more common symptoms are listed below.

- New toolbars, links, or favourites that you did not intentionally add to your web browser.
- Your home page, mouse pointer, or search program changes unexpectedly.
- You type the address for a specific site, such as a search engine, but you are taken to a different website without notice.
- Files are automatically deleted from your computer.
- Your computer is used to attack other computers.
- You see pop-up ads, even if you are not on the Internet.
- Your computer suddenly starts running more slowly than usual.

  **Note:** Not all computer performance problems are caused by malicious software.

How to Open SCEP or Windows Defender

1. Click the Windows Start button.
2. In Windows 7, click All Programs then System Center Endpoint Protection.
3. In Windows 10, click All Apps then Windows System, Windows Defender.
Manual weekly scan

1. Open SCEP or Windows Defender.
2. Select Quick from the Scan options.
3. Click the Scan now button.

The scan will start immediately. You will see the filenames flashing momentarily on the screen as SCEP scans each of the files on your PC in turn.

A status bar indicates scan progress.

To abandon the scan, click Cancel scan. You will be returned to the home screen.

If a quick scan does not detect any problems but you still suspect that there is a virus infection on your PC, repeat the steps above but select Full from the Scan options at Step 2.

Scanning a USB pen or a CD

1. Open SCEP or Windows Defender.
2. Select Custom scan.
3. Click the Scan Now button.
4. In the Select the drives and folders you want to scan window, tick the drive corresponding to the device you want to scan.
5. Click OK. A scan will start – see Manual weekly scan (above) for details of the process.

Scanning a Specific File or Folder

1. From My Computer or Windows Explorer, browse to the location of the file or folder to be scanned.
2. Right click on the file or folder.
3. Select Scan with System Center Endpoint Protection or Windows Defender from the pop-up menu.
Completing a scan

Once a scan is complete, the Home screen will appear with a summary of the scan.

![Scan completed on 78658 items.](image)

Manually updating SCEP or Windows Defender

1. Open SCEP or Windows Defender.
2. Click the **Update** tab.
   The **Definitions last updated** date indicates when it was last successfully updated.
3. Click the **Update** button.
   A status bar will appear briefly as the latest update is downloaded.

What to do if a virus or other malicious software is detected

**Red notification message**

1. As soon as realtime protection detects a virus or other malicious software, a red notification message appears in the bottom right-hand corner of your computer screen.
2. Click **Clean Computer**.
3. SCEP or Windows Defender will automatically clean your computer and display a green notification message once the threat has been removed.

![Your computer was cleaned](image)

**Note:** If you connect a USB drive to University classroom or Lecture Theatre PCs, any virus-infected file on your USB drive that is identified by the University's anti-virus software as being high risk will be automatically deleted from your device.

**Red icon**

If the red notification message disappears from your screen before you have had time to take action, or if you notice that the status icon is now red instead of green, you will need to open SCEP or Windows Defender to initialise the cleaning process.

1. Open SCEP or Windows Defender.
2. The computer status bar will indicate that your PC is at risk.
3. Click **Clean Computer**.

![Computer status - at risk](image)

4. A popup window will appear indicating progress as the threat is removed.
   The status bar on this window will change to green once your PC has been cleaned. The status message will show that **Your actions were applied successfully**.

![Potential threat details](image)

5. Click **Close**.
6. Exit out of SCEP or Windows Defender.
7. The status icon will now have changed back to green.
**Status Icon**

The status icon is located at the right hand side of the Windows taskbar. It changes appearance according to the state of the software and whether it has detected any potential threats.

The icons below are for SCEP, but Windows Defender uses the same red, yellow and green warning system.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>SCEP is up to date. It is unlikely that harmful or unwanted software is present. This should be the normal working status of SCEP.</td>
</tr>
</tbody>
</table>
| ![Icon] | This occurs in one of the following circumstances:  
− A scan of the PC has not been run for a while. Follow the steps above to run a manual weekly scan to correct this problem.  
− SCEP is not up to date.  
− Malware with a low or medium severity rating has been detected. |
| ![Icon] | This indicates that SCEP has stopped working either due to:  
− An infection by malware with a high severity rating.  
− SCEP has not been updated for an extended period. |
| ![Icon] | SCEP is busy scanning your PC for malware or cleaning malware that it has found on your PC. |
| ![Icon] | SCEP is downloading updates. |

**Further information and help**

Use MyIT to log calls with the IT Service Desk: [https://myit.abdn.ac.uk](https://myit.abdn.ac.uk)