UYOD VDI Solution – Installing the OPSWAT Security Application

These instructions are for installing the OPSWAT security application which, once installed on to a connecting device (UYOD PC or Laptop), will check to ensure the device is updated and adequately protected by an Anti-Virus product. If OPSWAT finds vulnerabilities it will display a report with instructions to take remedial action – e.g. run "Windows Update", update anti-virus software, etc.

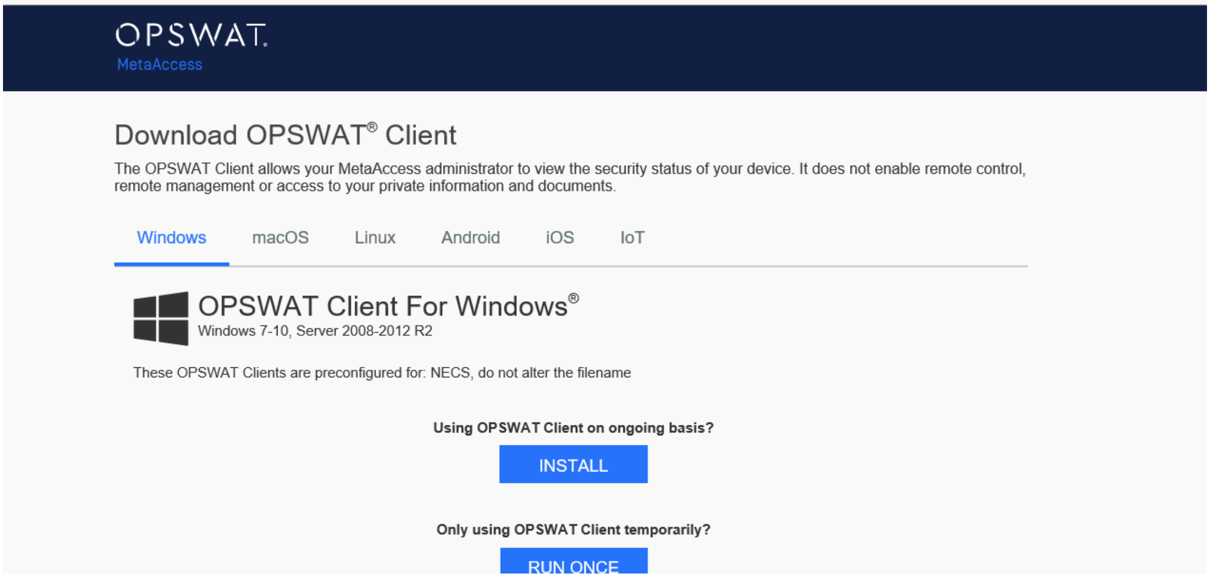
If your device does not pass the necessary tests then your device will be prevented from accessing the UYOD VDI until the issues are remedied.

These checks will include a comprehensive examination of your device's software and hardware configurations. It will not access any data, personal data or internet browsing history etc. These checks are important to ensure the integrity of the solution and protect against cyber threats as the solution connects to the NECS network and accesses clinical platforms.

If OPSWAT finds vulnerabilities it will display a report with instructions to take remedial action – e.g. run "Windows Update", update anti-virus software, etc.

Use the browser on your own device (not a NECS provided computer) to access:

https://gears-eu.opswat.com/console/download/af0bd64e6079ed949be1a28b799f5be2/



Download OPSWAT® Client

The OPSWAT Client allows your MetaAccess administrator to view the security status of your device. It does not enable remote control, remote management or access to your private information and documents.

OPSWAT Client For Windows®

Windows 7-10, Server 2008-2012 R2

These OPSWAT Clients are preconfigured for: NECS, do not alter the filename

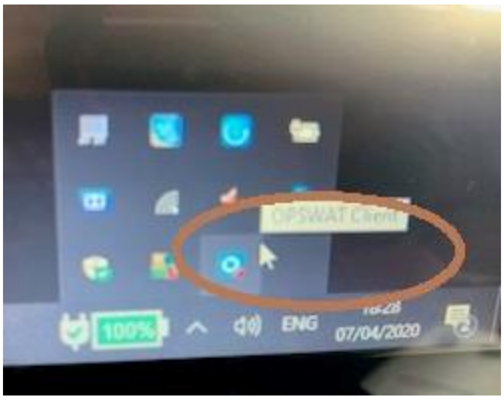
Using OPSWAT Client on ongoing basis?

Only using OPSWAT Client temporarily?

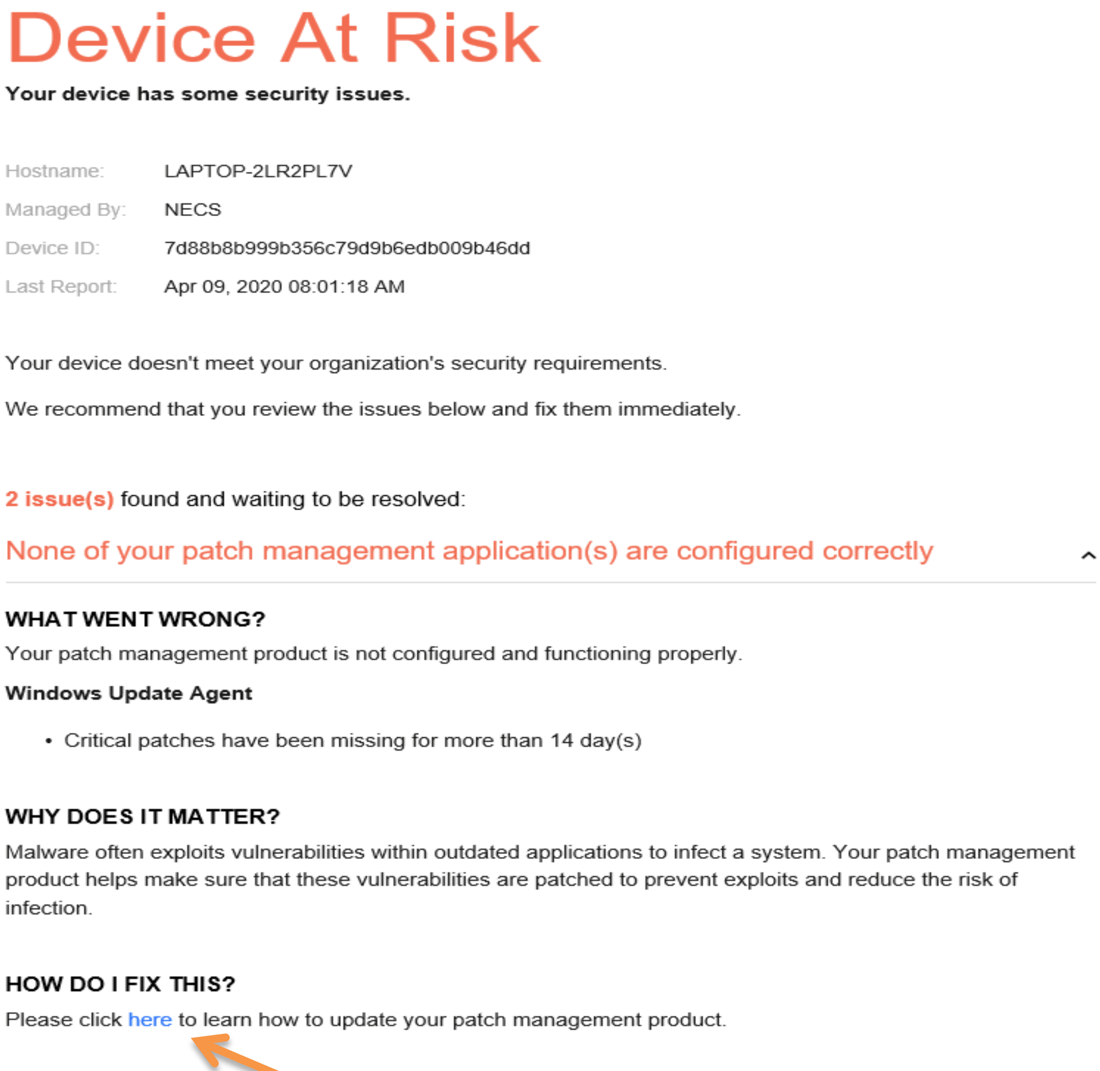
Press the INSTALL button under the "Using OPSWAT Client on ongoing basis".

Only connecting devices which have OPSWAT installed (and are appropriately patched) will be able to access the VDI solution.

Once installed there will be a new icon (see below) in the Window 10 task tray (bottom right hand corner for your screen).



If the icon's bottom right-hand corner is **red**, then vulnerabilities have been discovered. Double click the OPSWAT icon to open the report (see below example)



Device At Risk

Your device has some security issues.

Hostname:	LAPTOP-2LR2PL7V
Managed By:	NECS
Device ID:	7d88b8b999b356c79d9b6edb009b46dd
Last Report:	Apr 09, 2020 08:01:18 AM

Your device doesn't meet your organization's security requirements.

We recommend that you review the issues below and fix them immediately.

2 issue(s) found and waiting to be resolved:

None of your patch management application(s) are configured correctly

WHAT WENT WRONG?

Your patch management product is not configured and functioning properly.

Windows Update Agent

- Critical patches have been missing for more than 14 day(s)

WHY DOES IT MATTER?

Malware often exploits vulnerabilities within outdated applications to infect a system. Your patch management product helps make sure that these vulnerabilities are patched to prevent exploits and reduce the risk of infection.

HOW DO I FIX THIS?

Please click here to learn how to update your patch management product.

Click on the hyperlink under the **How Do I Fix This heading**, this will link you to a knowledge base article relating to the issue that OPSWAT is reporting. This will allow you to attempt to remediate your issue.

If you encounter difficulties accessing the VDI client after the OPSWAT installation or have issues remediating the issues, please contact the NECS Service Desk on 0300 555 0340