



Secure Configuration // What are the Cyber Essentials controls?



- Remove unrequired software and accounts
- Set an access pin or password to unlock devices
- Disable autoplay/autorun

[www.ncsc.gov.uk/cyberessentials](http://www.ncsc.gov.uk/cyberessentials) 

**Set up your computer securely to minimise the ways a cyber criminal can find a way in.**

## Remove or disable unused software

Software is made up of thousands of lines of code which instruct the device what to do. It is common that within the many lines of code, there will be errors or vulnerabilities. Criminals exploit these vulnerabilities to hack into your systems; it is like a burglar finding an open window. Many devices and software come from the manufacturer with extra features enabled that you do not use. Vulnerabilities that lie within the code in each 'extra' feature can potentially offer additional openings or access points for cyber criminals. For Cyber Essentials, any services, software or applications that you are not using must be uninstalled. This includes features that came with your device/operating system that you do not want or require.

## Remove or disable unrequired accounts

For the same reason, any accounts on your devices and cloud services that are not used for day-to-day business must be removed or disabled.

## Device locking

For mobile devices there needs to be a locking mechanism in place on each device to access the software and services installed.

By setting a unique 6 character or more password or pin number, or a **biometric** method to unlock your devices, you can stop unauthorised people accessing your information if the device is lost, stolen or left unattended.

## Disable autoplay and autorun

Autorun or autoplay is a feature that allows software to automatically open by itself when a USB or DVD is plugged into your device.

It is important to disable autorun or autoplay on all operating systems and web browsers in order to avoid automatic installations of unauthorised software. When autorun or autoplay is disabled, the user is prompted to give permission every time before software is allowed to run or play.

## Opening ports - a security risk

### What is a port?

Computer hardware is the physical part of a computing system such as a laptop, monitor, keyboard, cables etc. **A port in the hardware** is the jack or receptacle for an external device to plug into. These are standardised for each purpose. Some common ports are Universal Serial Bus ports, USB-C ports, Ethernet ports or DisplayPorts. Examples of external devices attached via ports are the mouse, keyboard, monitor, microphone and speakers.

Vastly different types of data flow to and from a computer over the same network connection, **software-based ports** are used by programs and services to exchange information and help computers understand what to do with the data they receive. Ports are standardised across all network-connected devices, with each port assigned a number. Most ports are reserved for certain roles or 'protocols' — for example, all Hypertext Transfer Protocol (HTTP) messages go to port 80. This is the way internet communications platforms such as web browsers ask for the information they need to load a website.

An **IP address** is a numeric address (e.g. 216.239.32.0) or an identifier for every connected computer or device. An IP address and a port number work together to exchange data on a network. Whereas the IP address is used to determine the geographical location of that server, the port number determines which service or program on that server it wants to use. Port numbers allow targeting of specific services or applications within those devices, for example, a computer can simultaneously load HTTP webpages using port 80, transfer an MP3 recording using port 21 (the File Transfer Protocol FTP) and send email from an email server using the SMTP Port 25.

## Correctly configure your open ports

There are two areas where you would open and configure software or 'logical' ports to allow your organisation's devices and services to connect to the outside, wider internet.

The first one, covered in the first control is the firewall. This is your boundary and your first line of defence and may be configured to open a hole and allow a system on the inside of your network to become accessible from the wider internet. The second is covered in secure configuration and covers ports that are used for external services. An example might be an in-house email server or an Infrastructure as a service (IaaS) cloud service such as Azure or AWS. IaaS is a service with the servers in the cloud (located elsewhere) where the user organisation is responsible for configuring the ports.

If you have a software system that is only used internally, it is far more secure because it is not exposed to the internet and the external ports are closed. However, if your organisation hosts something internally such as an email service that you are exposing to the internet because you allow people outside your network to access it, it is vital that you correctly configure those services. It is important that you understand the services that you have opened up and made available externally to your users/ members of the public. It is not secure to simply turn on an external service and open up everything to the internet.

When you configure an email service on the server, the default instructions will be to open several ports. It's worth noting that there is different functionality for the email server, and you may not actually need to be running all those services on your email, which means you may not need all those ports open. The simple message is, if you've got ports open that don't need to be open, close them. The ports that you have open, need to be understood and documented. An important element of Cyber Essentials is helping organisations look at their IT systems and realise what they've got exposed to the internet.

# Remote Desktop Protocol-port 3389

Port 3389 is the port for Remote Desktop Protocol (RDP). Remote Desktop Protocol enables a user of a computer in one location to access a computer or server somewhere else. This is often used by technicians to support users and to carry out maintenance tasks.

Remote Desktop Protocol is a common attack route for ransomware and should only be used on internal networks. There is no good business reason to have this port open for external use as it is extremely hard to make secure. Some security experts compare an open port 3389 to a front door jammed open. If a cyber criminal running a port scan on the internet saw that port 3389 was open, it would be like hitting the jack pot for easy access to that network.

Close or block the RDP port (3389) at the firewall so that it is not open for use across the internet.

Where possible, rather than using remote connections, utilise cloud services such as OneDrive or Google Drive.

## The five controls of Cyber Essentials are:

- User Access Control
- Security Updates
- **Secure Configuration**
- Malware Protection
- Firewall and Routers

## Help and support

There are over 300 specially trained cyber security companies around the UK who are licensed to certify against the Government's Cyber Essentials Scheme. They can offer help and support in preparation for the assessment. [Find one near you.](#)

For questions and feedback about the Cyber Essentials scheme, contact IASME at [info@iasme.co.uk](mailto:info@iasme.co.uk) or Tel: 03300 882 752