



V3.0 - JUNE 2019

Cyber Accelerator Alumni



in association with  
National Cyber  
Security Centre



# CYBER ESSENTIALS SMART SETUP

[www.cybersmart.co.uk](http://www.cybersmart.co.uk)

CyberSmart Ltd  
020 7993 6990  
[hello@cybersmart.co.uk](mailto:hello@cybersmart.co.uk)



# CONTENT

- 3 Getting Started
- 4 Deployment Methods
- 5 Securing Devices
- 6 Securing Mobile Devices
- 7 Questionnaire
- 8 Certification & More

## WELCOME TO CYBERSMART

We are delighted that you have decided to become a security champion for your organisation. Before we get started, please read this guide to make sure you get the best out of CyberSmart.

To achieve Cyber Essentials certification, you have to complete the “Questionnaire” stage.



## GETTING STARTED

Getting started with CyberSmart is simple and straightforward, you will be up and running in a few clicks.

1. Go to [app.cybersmart.co.uk/signup](https://app.cybersmart.co.uk/signup) and create an account.

2. Complete the onboarding stage by completing a few basic organisational questions, subscribing to the appropriate CyberSmart package, and enrolling your team members. When choosing a deployment method, please read the next page.

3. After this you will be directed to your dashboard where you will be able to start securing your organisation.

The screenshot shows the 'On Boarding' stage of the CyberSmart setup process. At the top, a progress bar indicates three steps: 1. Organisation (highlighted in dark blue), 2. Payment, and 3. Enrol. Below the progress bar, the title 'GETTING STARTED WITH CYBERSMART' is followed by the instruction 'Complete on boarding in less than 5 minutes'. The main section is titled 'Organisational Information' and contains three input fields: 'Our company is called', 'Our industry is', and 'Our company is'. Below these fields, there are radio button options for the number of staff: 'It's just me!' (selected), 'Up to 10 staff', 'Approx 11 - 25 staff', 'Approx 26 - 50 staff', 'Approx 50 - 250 staff', and 'More than 250 staff'. A 'Next' button is located at the bottom right of the form area. A small chat icon is visible in the bottom right corner of the page.



## DEPLOYMENT METHODS

CyberSmart is available on Windows, Mac as well as Android and IOS devices. The latter options require the apps to be downloaded from the iPhone App Store or Google Play, prior to completing the activation processes below.

There are two different ways to deploy the CyberSmart app. Individual enrolment and bulk deployment.

**Individual enrolment:** This involves each enrolled user installing the app via an automated email. This approach is primarily used for SMEs or organisations that do not use group policies for deployment. To enable this option, make sure bulk deployment is **not** selected.

Individual users are then enrolled via an automated email which deploys or configures the app on the device.

**GETTING STARTED WITH CYBERSMART**  
Complete on boarding in less than 5 minutes

1 Organisation 2 Payment 3 Enrol

**App deployment method**

☒ Individual Enrolment  
☐ Bulk Deployment [advanced]

This is the recommended way to get setup. Individual enrolment is designed for organisations with user-managed devices and without existing central management software. This method will send individualised emails to team members which they can install the app with.

**Start enrolment**

We'll send a custom email with the CyberSmart app download link to your enrolled users. As an increased security measure, please write a pre-shared message below to your team members which they will recognise to verify the email. Click the box for some suggestions!

Hello all, you are required to install this software as part of our compliance implementation. It doesn't take long, it's only a few clicks, I recommend you do this now. The secret word is [SECRET]

Please replace the word [SECRET] for your own word that you tell staff to look out for

**Bulk deployment:** This is the enterprise approach designed to 'silently' install the app across all devices on the network with a single push. This makes it quick and easy to secure multiple devices in one go.

**GETTING STARTED WITH CYBERSMART**  
Complete on boarding in less than 5 minutes

1 Organisation 2 Payment 3 Enrol

**App deployment method**

☐ Individual Enrolment  
☒ Bulk Deployment [advanced]

Bulk deployment is designed for organisations with centralised device management. This is usually via Group Policy Object (GPO), Mobile Device Management (MDM) or Remote Monitoring & Management (RMM). This method creates a single package for organisation wide deployment which can be deployed using existing systems.

**Mobile apps: approved domains**

Set your company email domain as users can enrol their mobile devices. This will ensure they are compliant and allow them to read policies on their mobile.

johnscompany.com

**Add any additional platform admins**

These users will have full access to the CyberSmart web dashboard with you.  
[Click here if you have no additional admins to add](#)



## SECURING DEVICES

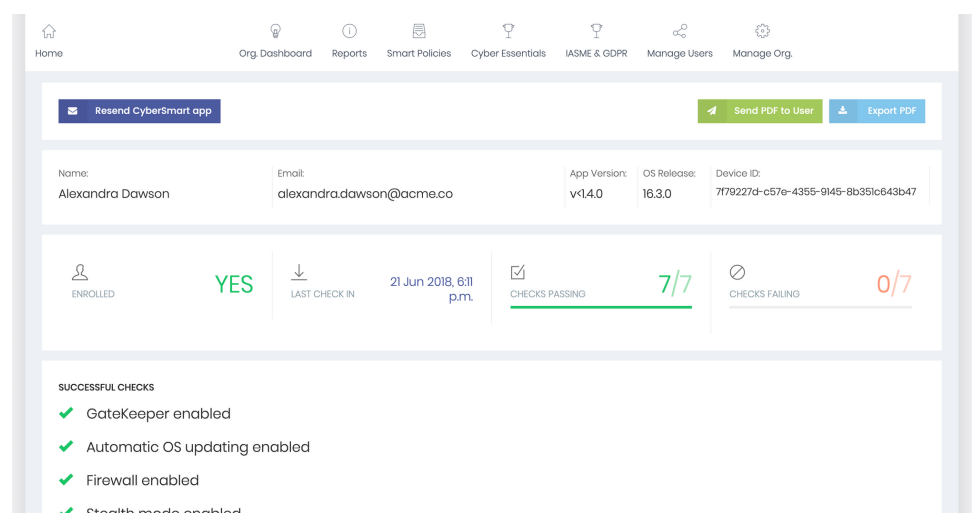
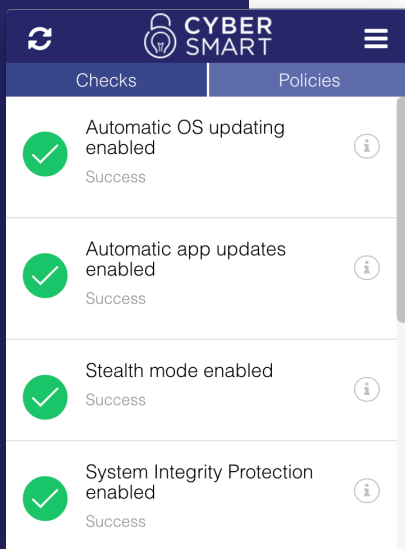
**Individual enrolment** users will receive an email from CyberSmart prompting them to install the app. By default, the app is in report only mode. In this mode it cannot modify anything on the device, it simply feeds back information about security configuration settings to the organisation's dashboard. A single email enables the user to install CyberSmart on their laptop and/or desktop. If you wish to secure portable devices you simply send an additional email to configure the deployed apps on all those devices.

**Bulk deployment** users will not receive any emails nor receive a notification from your CyberSmart dashboard to warn that the app has been installed.

The status of the various device checks can be viewed by clicking the "Hostname" of a user from your organisation's dashboard.

For users with non-compliant devices, CyberSmart automatically creates a personalised guide outlining the "steps to secure" which can be emailed to them. Alternatively you can download the guide and remediate the device centrally. Options to provide auto remediation are also available.

Once every device is secured, your organisation will conform with the Cyber Essentials standard.





## SECURING MOBILE DEVICES

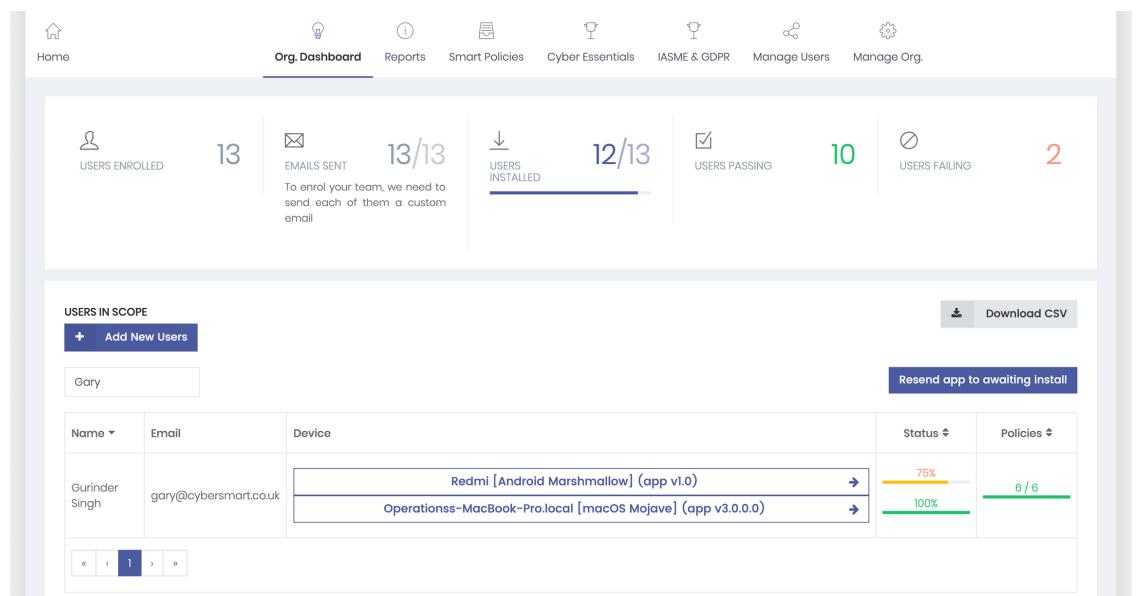
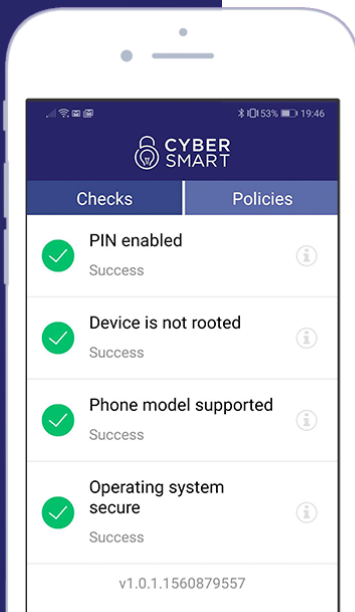
The process is the same to secure mobile devices and tablets.

First, your users should download the appropriate app from the iPhone App Store or Google Play.

When you have sent the activation email from the dashboard, the user will need to click the button at the bottom of the email to configure the app. Once the app is activated, it will continue to protect in the background.

Alternatively, users can send themselves a 'magic' link by SMS from their own laptop / desktop to activate the app.

User information is aggregated in the dashboard, as shown below.





## QUESTIONNAIRE

At this point all devices will be secured and compliant with the Cyber Essentials standard. Now it is time to fill out the self-assessed questionnaire reflecting your current organisation's security controls.

The questionnaire is part-completed with automated reporting to speed up the process. It pre-fills answers with information gathered from the apps. We have also provided suggested answers collected from any previous certifications and compiled them into an easy, tick-box style format.

The questionnaire has no time limit and all the answers can be saved and continued later.

Submitting the questionnaire with CyberSmart has a **100% pass rate**. You cannot submit the questionnaire if your organisation will not pass the criteria. Incorrect answers will be flagged up and made clear which areas need amending in order to successfully submit your responses.

The screenshot shows the Cyber Essentials questionnaire interface. At the top, there is a navigation bar with icons for Home, Org. Dashboard, Reports, Smart Policies, Cyber Essentials (active), IASME & GDPR, Manage Users, and Manage Org. Below the navigation bar, the 'Cyber Essentials' section is displayed. A progress bar indicates 54% completion. The questionnaire is divided into sections: Organisation, Assessment Scope, Office Firewalls, Secure Configuration (active), Patches & Updates, User Accounts, Admin Accounts, Anti-Malware, and Insurance. The 'Secure Configuration' section contains two questions with 'No' radio buttons selected. Question 28 asks about removing unnecessary software, and Question 29 asks about necessary user accounts. Guidance text is provided for both questions.

Home Org. Dashboard Reports Smart Policies **Cyber Essentials** IASME & GDPR Manage Users Manage Org.

**Cyber Essentials**

PROGRESS 54%

Organisation Assessment Scope Office Firewalls **Secure Configuration** Patches & Updates User Accounts Admin Accounts Anti-Malware Insurance

Computers are often not secure upon default installation. An 'out-of-the-box' set-up can often include an administrative account with a standard, publicly known default password, one or more unnecessary user accounts enabled (sometimes with special access privileges) and pre-installed but unnecessary applications or services. All of these present security risks.

Questions in this section apply to: Servers, Computers, Laptops, Tablets and Mobile Phones

28. Where you are able to do so, have you removed or disabled all the software that you do not use on your **laptops, computers, servers, tablets and mobile phones**? Describe how you achieve this.

☐ No

Guidance: It is acceptable to use a 'standard build' (where the organisation has decided which applications will be installed on all computers) to comply with this question.

Some pre-installed applications on Android smartphones and tablets cannot be uninstalled - this is acceptable for this question.

29. Have you ensured that all your **laptops, computers, servers, tablets and mobile devices** only contain necessary user accounts that are regularly used in the course of your business?

☐ No

Guidance: You must remove or disable any user accounts that are no needed in day-to-day use on all devices.



## CERTIFICATION & MORE

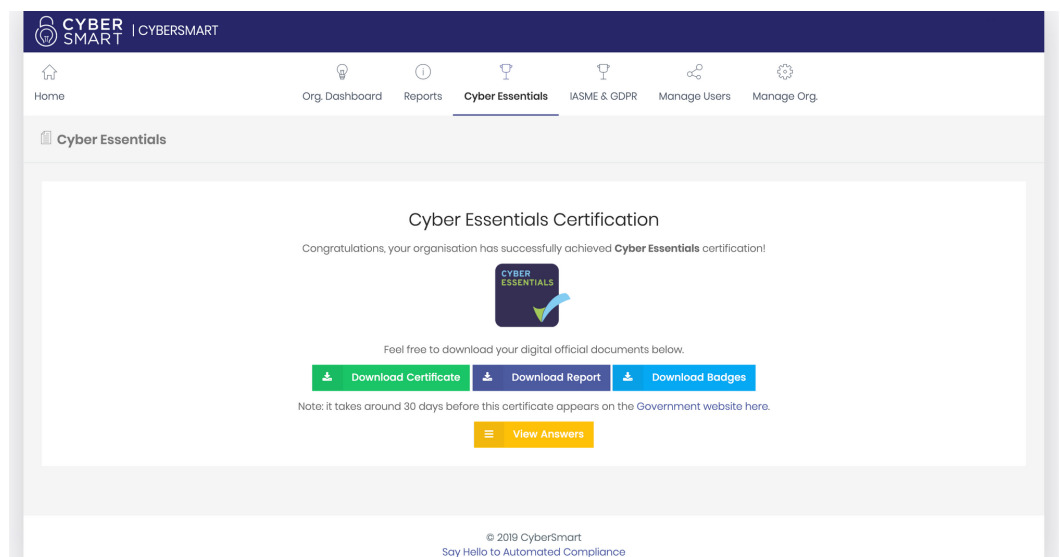
The hard work is over. The moment the questionnaire is submitted we will be notified and start reviewing the submission. We will then issue the official certificate within 24 hours. You will receive an email with the certification and a path to your report for your records. At this point, the certificate, full report and eligible badges will be available to freely download in the “Questionnaire” tab.

Once you have been successfully certified for Cyber Essentials, you can use the platform to maintain your compliance state, secure new users, get an overview of the status of individual devices and receive continuous support from CyberSmart.

As Cyber Essentials is an annual certification, we will get in touch with you near the time of your certificates expiry to ensure you maintain continuous compliance.

If you have any questions, feedback or comments, you can contact us by email, phone or live chat readily available within the dashboard.

**Thank you for choosing CyberSmart!**







“

*CyberSmart really helped us on our journey to achieving Cyber Essentials certification. The device compliance is a real help and their support team were always on hand to offer advice relating to both the product and the CE scheme. Once we submitted the completed application we were certified within a few hours - having this all in one place was useful.*

”

### Get in touch

145 City Road  
7th Floor London  
EC1V 1AW

020 7993 6990  
[hello@cybersmart.co.uk](mailto:hello@cybersmart.co.uk)

★ Trustpilot



[www.cybersmart.co.uk](http://www.cybersmart.co.uk)