ManageEngine

The Cyber Essentials guide

www.manageengine.com

Table of **contents**

What is the Cyber Essentials scheme? 3

Purpose of the Cyber Essentials scheme 3

Levels of Cyber Essentials certification 4

Cyber Essentials 2023 updates 5

Cyber Essentials 2022 updates 7

How can my organization get a Cyber Essentials certification? 9

Security control 10

1. Firewalls 10
2. Secure configuration 11
3. Security update management 14
4. User access control 16
5. Malware protection 18

Other data privacy regulations that ManageEngine solutions help you comply with 21

Certifications that ManageEngine products comply with 22

About ManageEngine 25

What is **Cyber Essentials scheme?**

Cyber Essentials is a scheme formulated by the United Kingdom (UK) government to ensure that organizations are protected against common cyberattacks.

It is an industry-backed scheme essential for all companies that handle customer data and is mandatory for tendering any central government contracts in the UK. By adopting this scheme, organizations secure their compliance efforts and gain prospects' confidence.

Purpose of the **Cyber Essentials scheme**

It aims to:

» Identify and implement basic security controls that prevent 80% of common cyberattacks

» Set a minimum cybersecurity standard that organizations are expected to follow.

» Establish and promote basic cyber hygiene practices.

Levels of **Cyber Essentials certification**

Currently, there are two levels under which organizations can be certified:

Level 1

Cyber Essentials

Organizations are required to self-evaluate based on five basic security controls established by this scheme. This can be achieved by filling out and sending the free Cyber Essentials questionnaire to an authorized body. The questionnaire will be verified by the organization, and if the requirements are met, a certification will be awarded.

Level 2

Cyber Essentials Plus

A Level 1 Cyber Essentials certification is required to proceed to Level 2. Cyber Essentials Plus offers a higher level of assurance as it includes a thorough on-site audit by an authorized body. Compliance with the security controls is verified by the performance of vulnerability assessments through simulated attack scenarios.

Both certifications can be obtained from any authorized body found in the IASME Consortium listings.

Cyber Essentials 2023 updates

Clarifications on the technical requirements and other necessary guidance are listed below:

1. For all user devices except firewalls and routers, applicants are now only required to list the make and OS, as cited in the self-assessment question set.

2. The definition of software has been updated to cover only router and firewall firmware.

3. End-user devices that are loaned by the organization to third parties are now in scope for the assessment.

4. Where default settings are not configurable on certain devices, applicants are now allowed to use the vendor's default settings.

5. The malware protection mechanism should not be signature-based or sandboxed. Instruction on applying relevant antimalware measures has been documented.

6. Guidance is now available on asset management as a core security function and its impact on applicants in alignment with the five technical controls.

7. There is now guidance on the importance of the Zero Trust model in the evolving network architecture landscape.

8. The technical controls have been reordered with respect to changes in the layout of the self-assessment question set.

9. Revisions have been made to Cyber Essentials Plus' illustrative test specification considering amendments to malware protection mechanisms.

Here is further clarification on what is in and out of scope concerning third-party devices:

	Owned by your organisation	Owned by a third party	BYOD
Employee	✓	N/A	✓
Volunteer	✓	N/A	✓
Trustee	✓	N/A	✓
University research assistant	✓	N/A	✓
Student	✓	N/A	✗
MSP administrator	✓	✗	✗
Third party contractor	✓	✗	✗
Customer	✓	✗	✗

✓ In scope ✗ Out of scope

Source: Cyber Essentials: Requirements for IT infrastructure v3.1(NCSC)

User devices connected to the organization's data should be configured appropriately, even if they are out of the scope of the assessment.

The updated technical requirements and question set are effective from April 24, 2023. This means that applications received on or after the mentioned date must align with the revisions of 2022 and 2023.

Cyber Essentials 2022 updates

Here are the major changes brought into this scheme that will be considered for compliance from January 2023 on:

New additions to the scope (the areas that are considered for assessment under the Cyber Essentials certifications):

- Home working devices
- Cloud services (PaaS, IaaS, and SaaS)
- Thin clients
- End-user devices
- All servers
- Under BYOD: User-owned devices that access organizational data or services
- Subsets to be considered along with the whole of IT infrastructure used for business (subsets are a part of the organization with a separate network defined by a firewall or a VLAN)
- Wireless devices within the organization that use the internet to communicate with other devices and are vulnerable to direct internet attacks

The devices that remote workers use, both personal and company-owned, need to meet all the technical control requirements under Cyber Essentials.

Devices should be unlocked using a password, a PIN with a minimum of six characters, or biometric authentication. A process has also been established to change passwords in case of any suspicious activities.

MFA is extended to cloud services also due to the rising number of attacks in this segment. In cloud services, some of the technical controls need to be met both by the organization seeking certification as well as by the cloud provider.

Requirements	Applicant			Cloud provider		
	IaaS	PaaS	SaaS	IaaS	PaaS	SaaS
Firewalls	✓	✓	✗	✓	✓	✓
Secure configuration	✓	✓	✓	✓	✓	✓
User access control	✓	✓	✓	✗	✗	✗
Malware protection	✓	✓	✗	✓	✓	✓
Security update management	✓	✓	✗	✓	✓	✓

Separate accounts are needed for performing IT admin tasks to minimize risks to privileged accounts.

Cyber Essentials has adopted a tiered pricing structure based on the enterprise size determined by the employee count.

How can my organization get a Cyber Essentials certification?

The first step to becoming Cyber-Essentials-certified is to address the five security controls that apply to each of the two levels. This can be achieved by deploying the right combination of processes and IT tools.

The security control requirements for the certifications are specified under five broad themes discussed below:

- Firewalls
- Secure configuration
- Security update management
- User access control
- Malware protection

Security control 1: **Firewalls**

Applicable to boundary firewalls, laptops, desktops, routers, servers, and cloud services (IaaS, PaaS, and SaaS)

Have a firewall in place to secure all your internet-enabled devices. It controls and monitors the incoming and outgoing web traffic to prevent malicious content from entering your networks and devices. But how do you determine if your firewall is being used to its full potential, and if it delivers the expected protection to your networks and devices?

How can ManageEngine help?

Firewall Analyzer

This software analyzes the usage of firewall rules and fine-tunes them for maximum effectiveness. With this solution, you can view audit log information to track all the activities of the firewall users and receive notifications from its custom alert profile in case of anomalous activities in the network. The firewall security log reports help security admins analyze and visualize threat scenarios and strategize accordingly.

More features >>

Security control 2:
Secure configuration

Applicable to servers, desktops, laptops, tablets, thin clients, mobile phones, and cloud services (IaaS, PaaS, and SaaS)

Apply security settings that provide maximum protection for all your software and devices. When full network systems are deployed, default configurations are often set to enable ease of use, but these tend to provide minimal security and should be avoided. Using strong, unique passwords and MFA for your devices and applications is vital to fortifying your infrastructure. MFA is made mandatory for cloud services also in the Cyber Essentials 2022 revision.

Enabling device locking controls, like biometric tests, PINs, or passwords, is a new requirement in the updated scheme. These should be protected against brute-force attacks by either of the following methods:

- Permit no more than 10 device unlock attempts in five minutes.
- Do not permit another device unlock attempt after 10 failed attempts.

How can ManageEngine help?

Password Manager Pro

Store, access, and share passwords securely using the solution's centralized vault. Automate required periodic password resets while using critical systems and provide real-time alerts on password access. Password Manager Pro's role-based access control feature helps ensure that only authorized personnel can access the resources and passwords stored in its vault.

More features >>

PAM360

Enable MFA and access control workflows that leverage the solution's just-in-time privileged access. This ensures that only authorized users can remotely access sensitive data for a specific time period. Perform periodic password resets for cloud solutions. Centrally store IaaS infrastructure access keys and privileged user credentials, and log in to SaaS applications in a single click.

More features >>

Vulnerability Manager Plus

Scan and detect firewall misconfigurations, web server misconfigurations, and vulnerabilities in your local and remote office endpoints. Ensure that your network systems initially grant the least privileges, and utilize complex passwords and memory protection. The solution also helps you comply with the Security Technical Implementation Guide and the Center for Internet Security guidelines.

More features >>

Application Control Plus

Implement application allowlisting and application sandboxing to permit only authorized applications to run, thereby preventing malware intrusions, threats, and zero-day attacks.

More features >>

Device Control Plus

Prevent data leakage by ensuring only approved peripheral devices can access corporate data with the option of granting just-in-time access either permanently or temporarily. Monitor ports, data transfer, and everything in between to prevent unauthorized data access.

More features >>

Security control 3:
Security update management

Applicable to servers, desktops, laptops, mobile phones, tablets, firewalls, routers, and cloud services (IaaS, PaaS, and SaaS)

Ensure that your systems and applications are up to date by periodically patching them. The best way is to enable automated patching. Sometimes updates require systems to be restarted, and most of the time this is postponed due to inconvenience. This can leave your systems vulnerable to attacks. Having the right patch management tools can simplify such requirements and boost security.

How can ManageEngine help?

Patch Manager Plus

Secure your systems and applications by enabling automated patch deployment for OSs and third-party applications. Test patches before deployment to eliminate security risks. Gain visibility into the patch status of endpoints with real-time audits and reporting. The solution also helps patch remote endpoints in a work-from-home setup.

More features >>

Endpoint Central

Automate the entire patch testing and deployment process to shield your network from security threats. This unified endpoint management solution also detects vulnerabilities through periodic scans, instantly mitigates them using patches or alternative fixes, and is capable of much more.

More features >>

Backing up organizational data is not added as a technical requirement for now, but it is highly recommended under Cyber Essentials.

Vulnerability Manager Plus

Scan and detect firewall misconfigurations, web server misconfigurations, and vulnerabilities in your local and remote office endpoints. Ensure that your network systems initially grant the least privileges and utilize complex passwords and memory protection. The solution also helps you comply with the Security Technical Implementation Guide and the Center for Internet Security guidelines.

More features >>

Security control 4:
User access control

Applicable to servers, desktops, laptops, tablets, mobile phones, and cloud services (IaaS, PaaS, and SaaS)

Ensure that employees have access to only what is essential to fulfilling their roles. Confine administrative privileges to admin accounts only. If admin accounts are compromised, it will result in more damage. Restrict personal browsing and shopping on corporate devices and official accounts.

Guidance on password formation was added after the 2022 revision. Encourage users to maintain a password length of at least eight characters. Provide secure vaults through which passwords can be shared and accessed.

How can ManageEngine help?

Access Manager Plus

Regulate access to remote systems through secure channels from a unified console. Scrutinize access requests and approve them on a case-by-case basis by establishing a request-release workflow. Provide temporary role-based access to third parties, record privileged user sessions, shadow user sessions, and revoke access instantly upon detecting any anomalous activities.

More features >>

PAM360

Identify and automatically onboard privileged accounts separately into secure vaults to provide role-based access permissions, policy-based conditional access based on real-time risk assessment, Zero Trust protection, and encryption. Consolidate and securely store all passwords in the centralized password vault. Closely monitor privileged accounts to detect any unusual activities with the help of PAM360's AI- and ML-driven anomaly detection capabilities.

More features >>

Endpoint Central

Automate the entire patch testing and deployment process to shield your network from security threats. This unified endpoint management solution also detects vulnerabilities through periodic scans, instantly mitigates them using patches or alternative fixes, and is capable of much more.

More features >>

AD360

Receive detailed reports on the users who have access to privileged information. Manage the access permissions for critical file servers and clean up unused user accounts and empty security groups to avoid unauthorized access.

More features >>

Security control 5: **Malware protection**

Applicable to servers, desktops, laptops, tablets, mobile phones, and cloud services (IaaS, PaaS, and SaaS)

Implement the right practices and IT tools to protect your organization from malware, like viruses, Trojan horses, worms, and spyware. Here are some practices that can safeguard your organization from malware:

- Enable antimalware and keep it updated and aligned with vendor recommendations.
- Block access to malicious websites and malicious code executables.
- Implement application allowlisting.

Antimalware, whether built-in or purchased from a third party, should always be updated and configured in accordance with Cyber Essentials requirements.

Corporate and personal end-user devices used for remote working are also under scope now and need to be secured from cyberthreats.

How can ManageEngine help?

Endpoint Central

Automate the entire patch testing and deployment process to shield your network from security threats. This unified endpoint management solution also detects vulnerabilities through periodic scans, instantly mitigates them using patches or alternative fixes, and is capable of much more. With the next-gen antivirus feature, proactively detect, prevent, and mitigate malware threats.

More features >>

Browser Security Plus

Securely isolate and manage enterprise sites by creating a list of trusted sites and prevent malware threats from untrusted sites. Control access to specific sites, configure policies to guard browsers from security breaches, and restrict file downloads from unauthorized sites.

More features >>

Log360 Cloud

Instantly notify IT personnel upon detection of anomalous activities in the system using Log360 Cloud's predefined alert profiles. Block access to malicious websites and applications by performing regular web content filtering. Mitigate external threats by detecting known attack patterns, like denial-of-service, distributed denial-of-service, SQL injection, and ransomware attacks, with Log360 Cloud's real-time event log correlation engine.

More features >>

Application Control Plus

Implement application allowlisting and application sandboxing to permit only authorized applications to run, thereby preventing malware intrusions, threats, and zero-day attacks.

More features >>

Other data privacy regulations that ManageEngine solutions help you comply with

ManageEngine solutions help you comply with the following regulations and have also provided numerous organizations with the technological support to achieve GDPR and CCPA compliance.

GDPR

The GDPR is a Pan-European regulation that requires businesses to protect the personal data and privacy of European Union citizens for the processing of their personal data. Our cloud offerings have privacy features that comply with the GDPR, and our processing of customer data adheres to the GDPR's data protection principles. ManageEngine's GDPR compliance page helps you gain a comprehensive understanding of the requirements of this mandate.

CCPA

The CCPA is a state-wide data privacy regulation that aims to protect the personal information of California residents. This regulation stresses several actions that organizations need to take to prevent personally identifiable information (PII) from falling into the wrong hands. ManageEngine's CCPA compliance page provides an extensive look into the CCPA requisites and how organizations can comply with them.

LGPD

The LGPD is a Brazilian data protection law that requires businesses to handle the personal data of Brazilian citizens with care, or risk heavy fines. ManageEngine AD360 and Log360 help you meet the IT security requirements of this mandate. ManageEngine's LGPD compliance page helps you compare and contrast the LGPD and GDPR mandates.

Certifications that ManageEngine products comply with

ManageEngine solutions comply with a number of standards and certifications, including:

Cyber Essentials

Cyber Essentials is a UK government-backed scheme designed to help organizations protect themselves against common cyber threats. It outlines a set of basic cybersecurity controls that all organizations can implement to mitigate risks and demonstrate a commitment to cybersecurity.

ISO/IEC 27018

We follow guidelines for implementing measures to safeguard the PII that is processed in a public cloud.

ISO/IEC 27001

ManageEngine has earned certification for the most widely recognized independent international security standards, the ISO/IEC 27001:2013, for applications, systems, people, technology, and processes.

ISO/IEC 27017

ManageEngine is certified with the ISO/IEC 27017:2015 for IT, security techniques, and code of practice for information security controls based on the ISO/IEC 27002 for cloud services.

ISO/IEC 27701

ManageEngine and its solutions are fully compliant with the requirements of the ISO/IEC 27701. This certification enhances the existing information security management system and helps continually improve the privacy information management system, thereby enabling us to demonstrate compliance with various privacy regulations.

SOC 2 Type 2

The design and operating effectiveness of our controls meet the AICPA's Trust Services Criteria.

Take control of your IT.

Monitor, manage, and secure your digital enterprise with ManageEngine.

www.manageengine.com

About **ManageEngine**

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.

ManageEngine

For more information:

www.manageengine.com

sales@manageengine.com

ManageEngine