CyberQP

CyberQP Product Mapping:

Cyber Essentials Requirements for IT infrastructure v3.1

Cyber Essentials:

Requirements for IT infrastructure v3.1/CyberQP Product Mapping

This guide outlines how CyberQP products can help you achieve Cyber Essentials compliance to help secure you and your customers.

Cyber Essentials is a cybersecurity certification scheme in the UK. It offers a set of basic cybersecurity controls that organizations can implement to protect against common cyber threats. The initiative aims to help organizations demonstrate their commitment to cybersecurity best practices. Organizations can enhance their cybersecurity posture by achieving certification and gain new business opportunities. Cyber Essentials is designed to be accessible and affordable for organizations of all sizes.

Cyber Essentials is organized under five technical control groups:

Firewalls	Secure configuration	Malware protection	User access control	Security update management

CyberQP products help achieve compliance in two control groups, Secure Configuration, and User Access Control:

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

Secure Configuration:

Introduction

Default configurations often have security vulnerabilities, including weak passwords and commonly used user accounts. Attackers can exploit these defaults to gain unauthorized access to sensitive information. CyberQP can help by applying technical controls, such as strong passwords, unique passwords, and removing unnecessary accounts. These controls help minimize vulnerabilities and protect against common attacks. Effective identity and access management is crucial for enhancing cybersecurity.

Cyber Essentials: Requirements for IT infrastructure v3.1: Secure Configuration Introduction:

"The default configurations of computers and network devices aren't always secure. Standard out-of-the-box configurations often include one or more weak points, such as:

- An administrative account with a pre-set, publicly known default password or without multi-factor authentication enabled
- Pre-enabled but unnecessary user accounts (sometimes with special access privileges)
- Pre-installed but unnecessary applications or services

These default installations can allow attackers to gain unauthorised access to your organisation's sensitive information. But by applying some simple technical controls when installing computers and network devices, you can minimise vulnerabilities and protect against common types of attack."

Requriements

CyberQP can help you meet the Cyber Essentials Secure Configuration requirements related to managing accounts on your local computers, Active Directory, and Azure Active Directory.

Cyber Essentials Requirements:	CyberQP Solution:
Remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)	CyberQP QGuard Just-in-Time Account Creation
Change any default or guessable account passwords (see password-based authentication)	CyberQP QGuard Privileged Identity Management

User Access Control:

Introduction

Proper management of user accounts reduces the risk of unauthorized access and protects IT systems. Privileged accounts pose a higher risk if compromised, allowing attackers to manipulate data, disrupt processes, or gain unauthorized entry. CyberQP's QGuard is purpose built to help MSPs manage the risks associated with administrative accounts.

Cyber Essentials: Requirements for IT infrastructure v3.1: User Access Control Introduction:

"Every active user account in your organisation facilitates access to devices and applications, and to sensitive business information. By making sure that only authorised individuals have user accounts, and that they're only granted as much access as they need to carry out their role, you reduce the risk of information being stolen or damaged.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information. If these accounts are compromised, an attacker could take advantage of their greater accesses to corrupt information on a large scale, disrupt business processes or gain unauthorised access to other devices in the organisation. Administrative accounts are especially highly privileged, for example. These accounts typically allow the user to:

- An administrative account with a pre-set, publicly known default password or without multi-factor authentication enabled
- Pre-enabled but unnecessary user accounts (sometimes with special access privileges)
- Pre-installed but unnecessary applications or services

These default installations can allow attackers to gain unauthorised access to your organisation's sensitive information. But by applying some simple technical controls when installing computers and network devices, you can minimise vulnerabilities and protect against common types of attack."

All types of administrators will have this kind of account, including domain administrators and local administrators.

This is important because if a user opens a malicious URL or email attachment, the malware would typically be executed with the same privilege level of the user's account. This is why it's important to take special care allocating and using privileged accounts."

Requriements

Cyber Security Essentials requires that your organization be in control of your user accounts and the access privileges that allow access. Accounts used by third-party support services are specifically highlighted in the requirements.

Cyber Essentials Requirements:	CyberQP Solution:
Have in place a process to create and approve user accounts	CyberQP QGuard Just-in-Time Account Creation
Authenticate users with unique credentials before granting access to applications or devices (see password-based authentication)	CyberQP QGuard Privileged Identity Management
Remove or disable user accounts when they're no longer required (for example, when a user leaves the organisation or after a defined period of account inactivity)	CyberQP QGuard Just-in-Time Account Creation
Use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
Remove or disable special access privileges when no longer required (when a member of staff changes role, for example)	CyberQP QGuard Just-in-Time Account Creation

Password-based authentication

Cyber Security Essentials states that all user accounts must require the user to authenticate. CyberQP can help you adhere to the Cyber Security Essentials password requirements.

Requriements

Cyber Security Essentials requires that your organization be in control of your user accounts and the access privileges that allow access. Accounts used by third-party support services are specifically highlighted in the requirements.

Cyber Essentials Requirements:	CyberQP Solution:
Passwords are protected against brute-force password guessing by implementing at least one of:	
• multi-factor authentication	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
Use technical controls to manage the quality of passwords. This will include one of the following:	
• Using multi-factor authentication (see below)	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
• A minimum password length of at least 12 characters, with no maximum length restrictions	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management

Cyber Essentials Requirements:	CyberQP Solution:
Use technical controls to manage the quality of passwords. This will include one of the following:	
• Using multi-factor authentication (see below)	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
• A minimum password length of at least 12 characters, with no maximum length restrictions	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
• A minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
Support users to choose unique passwords for their work accounts by:	
• Educating people about avoiding common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers.	CyberQP Password Manager
• Encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using three random words)	CyberQP QGuard Privileged Identity Management CyberQP QGuard Just-in-Time Account Creation CyberQP Password Manager
• Providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used.	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management
You should also make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised.	CyberQP QGuard Just-in-Time Account Creation CyberQP QGuard Privileged Identity Management