NCSC Cyber Essentials Guide

Cyber Essentials (CE), from the National Cyber Security Centre (NCSC), is a scheme designed to help organisations protect against a range of the most common cyberattacks. This guide from Jamf — the standard in Apple Enterprise Management — will show you how to implement these recommendations.

What are Cyber Essentials (CE) and Cyber Essentials Plus (CE+) certifications?

- Cyber Essentials is a foundation-level certification designed to provide a statement of the basic controls your organisation should have in place to mitigate the risk from common cyber threats.
- Cyber Essentials Plus is the highest level of certification offered under the Cyber Essentials scheme. It is a more rigorous test of your organisation's cyber security systems: an external auditor assesses your security controls to ensure that your organisation is protected against basic hacking and phishing attacks.

To see more about Jamf Pro's security features and recommendations, visit:
www.jamf.com/security

Why should my organisation follow these recommendations?

The vast majority of cyberattacks are the equivalent of a thief simply trying your front door to see if it's open, and the recommended plan from Cyber Essentials helps to mitigate this risk. Adopting these policies can:

- Reassure clients and customers that your organisation is working to secure their technology infrastructure and their data against cyber attack
- Attract new business who value organisations that take cyber security seriously
- Allow you to seek government contracts requiring Cyber Essentials certification
- Build a relationship with a trusted IT supplier

What attacks can we prevent by following the Cyber Essentials scheme?

The Cyber Essentials scheme addresses the most common Internet-based threats to cyber security: particularly attacks that use widely available tools and demand little skill. The scheme was created to thwart:

Hacking: exploiting known vulnerabilities in internet-connected devices, using widely available tools and techniques

Phishing: attempting to trick users into installing or executing a malicious application through email or other means

Password-guessing: manual or automated attempts to log onto a system from the internet by cracking passwords

How can we implement this plan?

There are multiple ways to engage with the Cyber Essentials scheme, and Jamf can help with many of them. By mapping the capabilities of the Jamf platform to your Cyber Essentials requirements, you will be well on your way to achieving certification.

For information on obtaining either certification, please visit https://www.ncsc.gov.uk/cyberessentials/overview/.

How can Jamf help?

Whatever your level of participation in these best practice guidelines for security, Jamf can help. Jamf Pro, Jamf Protect and Jamf Connect have existing built-in functionality that will achieve most, if not all, of these guidelines.

Cyber Essentials Requirements

REQUIREMENT #1: Firewalls

Cyber Essentials requires that organisations ensure that only safe and necessary network services can be accessed from the Internet.

Organisations should routinely:

- Change passwords to difficult-to-guess, complex passwords
- Prevent access to the administrative interface from the internet, unless the interface is protected by one of the following controls:
  - A second authentication factor, such as a one-time token
  - An IP allow list that limits access to a small range of trusted addresses
- Block unauthenticated inbound connections by default
- Ensure inbound firewall rules are approved and documented by an authorised individual
- Remove or disable permissive firewall rules quickly
- Use a host-based firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

Meet firewall requirements with Jamf

We've got you covered! Jamf Pro offers settings that accomplish these requirements in the security and privacy payload of a Jamf Pro configuration profile, which is pushed out to all managed Macs:

- Enable Firewall
- Block all incoming connections such as file sharing, screen sharing, Messages Bonjour and iTunes music sharing
- Control incoming connections through the Connection Setting dropdown for specific apps — requiring app name, bundle ID and connection setting before allowing the app
- Enable stealth mode: ignore attempts to access the computer from the network by test applications using ICMP, such as Ping
- Configure managed devices to automatically connect to a VPN when conditions are met, offering more secure network access

jamf | PROTECT

Jamf Protect can aid in meeting these requirements, as well, with its Protect Insights feature providing visibility into the configuration of many of these settings, such as the macOS Firewall settings.

More details about Jamf Protect

jamf | CONNECT

Jamf Connect offers simple provisioning of users from a cloud identity service during an Apple provisioning workflow, complete with multi-factor authentication.

More details on Jamf Connect

For a deeper, more technical dive into information on the application firewall and configuring it with Jamf Pro, please take a look at these developer resources:

Apple's Developer Configuration Profile Reference, Firewall Payload

Apple KB - OS X: About the application firewall

Jamf Pro Administrator's Guide, Computer Configuration Profiles

REQUIREMENT #2: Secure Configuration

Cyber Essentials requires that organisations ensure that only safe and necessary network services can be accessed from the internet.

Computers and network devices requirements

Companies must routinely:

- Remove and disable unnecessary user accounts
- Change any default or guessable account passwords
- Remove or disable unnecessary software
- Disable any auto-run feature which allows file execution without user authorisation
- Authenticate users before allowing internet-based access to sensitive data

Meet computer and network requirements with Jamf

Jamf Pro can help administrators meet these requirements through configuration profiles, policies and scripts to disable, report or quickly remediate. For example:

- To ensure the guest user account is disabled permanently, a Jamf administrator may deploy a configuration profile with the login window payload to all managed devices.
- Using Smart Groups, administrators can disallow certain types of users with a scripted payload. Jamf Nation, the largest online community of Apple-focused admins and Jamf users, contains a wealth of information, sample scripts and user-led troubleshooting.
- Automated reports provide administrators information on local user accounts, if needed, and user-initiated enrolment settings can be set in Global Management or retroactively using the management accounts payload.
- Administrators may disable Bluetooth and restrict or disallow apps.
- When configuring enrolment settings, a Jamf administrator may enable randomised passwords or enforcement of complex passwords through the user-initiated enrolment option.

For more detailed information on administering account passwords with Jamf Pro, please see these technical resources:

Jamf Pro Administrator's Guide, Administering the Management Account

Jamf Pro Administrator's Guide, User-Initiated Enrolment Settings

Password-based authentication requirements

This requirement is meant to protect against brute-force password guessing by using at least one of the following methods:

- Lock accounts after too many attempts
- Limit the number of guesses allowed within a certain time frame
- Set requirements for password length and complexity
- Have a password policy that clearly explains to users strong and secure password practices

Meet password-based authentication requirements with Jamf

Jamf Pro offers the ability to set all of these preferences in a configuration profile. Jamf Pro administrators can also create password blocklists for common, easily-guessed guessed passwords. With Jamf Connect and Jamf Pro, users can take advantage of single sign-on and multi-factor authentication for even stronger password protections.

Local accounts with NoMAD or mobile accounts with Active Directory are also in luck: Jamf Connect works smoothly with NoMAD for an even more secure experience.

For information on how they work together, please see this infographic that lays it all out: **https://www.jamf.com/resources/infographics/understanding-macos-catalina-and-jamf-connect/**

REQUIREMENT #3: Secure Configuration

This requires organisations to ensure that user accounts are assigned to authorised individuals only, and that applications, computers, and networkers are only accessible to users who actually need them.

This means organisations must:

- Have a user account creation and approval process
- Authenticate users before granting access to applications or devices
- Remove or disable user accounts when no longer required
- Use administrative accounts to perform administrative activities only
- Remove or disable special access privileges when no longer required

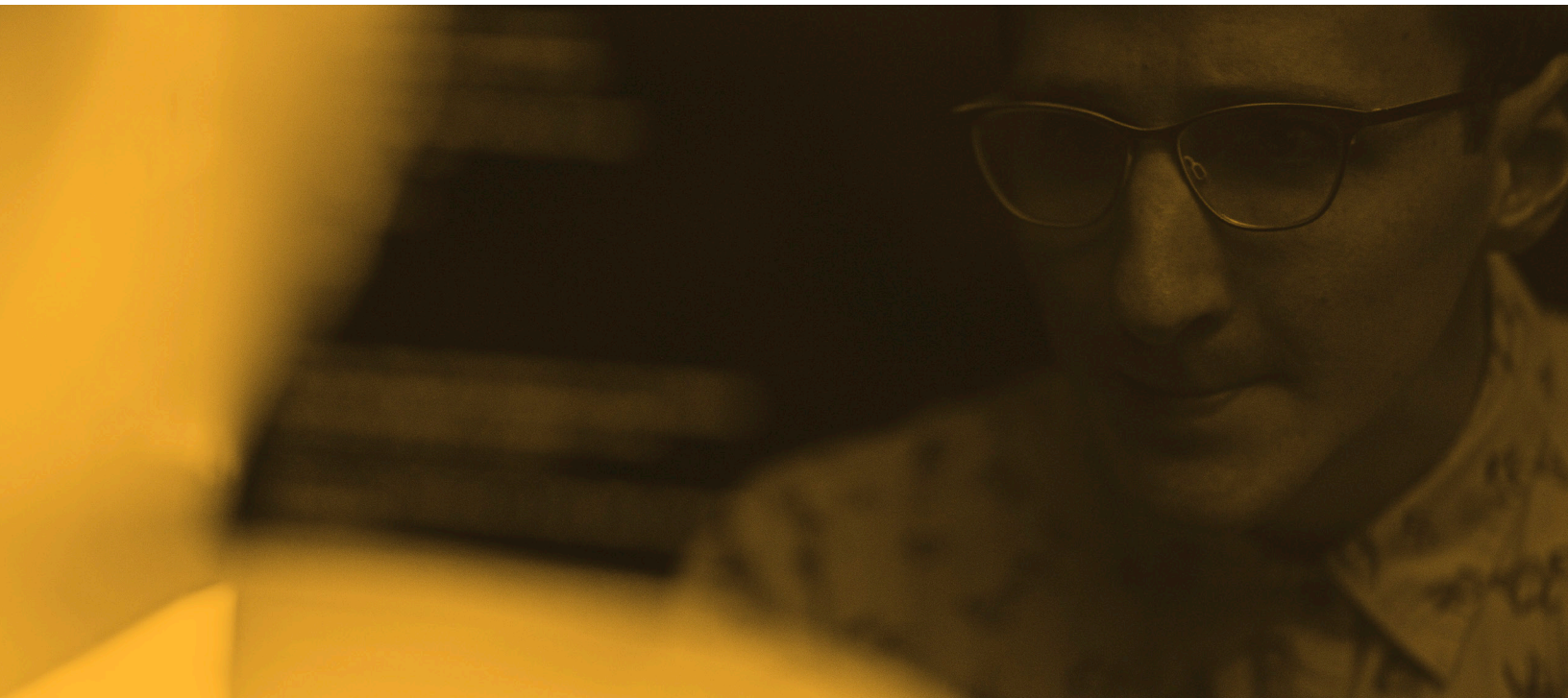
Meet access control requirements with Jamf

Jamf's available restrictions to the System Preferences through the configuration profile, restrictions payload or simple removal of administrative access when no longer needed will cover these issues, and the well-managed **Self Service** option ensures that no one has access to areas or apps that they don't need.

To remove users and accounts, administrators deploy a simple policy removing these accesses, accounts or users.

Endpoint compliance assessment

Get quick insight into the security posture and endpoint configuration of all managed macOS endpoints with Jamf Protect, which provides visibility on user account creation, authentication and more. Custom analytics and unified log filtering report on the creation and deletion of user accounts, when privileges are escalated or demoted and even login activity (such as for guest users).



REQUIREMENT #4: Malware protection

This requires that organisations restrict execution of known malware and untrusted software to prevent harmful code from causing damage or accessing sensitive data.

Malware protection requirements

- Anti-virus and other security software must be kept up to date — automatically or in an established workflow at least daily
- The software must be configured to scan files and web pages automatically upon access
- The software must prevent connections to malicious websites on the internet
- Only approved applications are allowed on devices
- Gatekeeper, a security feature native to the macOS operating system, enforces code signing and verifies downloaded applications before allowing them to run, which reduces the chance that malware will be able to execute commands. Gatekeeper can then notify Jamf Protect, which can offer up reports to administrators.

Meeting malware requirements with Jamf Protect and Jamf Pro

- Jamf Protect, which includes malware protection, automatically updates
- Jamf Pro's Smart Groups allow for focused deployment of updates and patches
- To protect the seamless Apple user experience, Jamf Protect scans all executables as they attempt to run. Its behavioral-based analytics alert administrators to malware-like behavior, as well as invoking a Jamf Pro response to the issue
- Jamf Pro's Self Service feature means that all applications available to users must be pre-approved before its even an option to download them
- Jamf Pro offers software deployment through the App Store, which provides code signing and verification benefits from Apple
- Jamf Protect also offers unprecedented Apple security visibility with data monitoring and control as well as organisational visibility of built-in prevention activity by XProtect, Gatekeeper and MRT

Jamf's security features are built in. With software deployment via a policy and automatic updates of all software, you can rest assured that all anti-viral and other security software is always up to date. Additionally, with Jamf Pro's configuration profiles, administrators may set security and privacy payloads through Gatekeeper settings, deploy certificate transparency payloads, restrict apps to a specific allow list and more.

The beauty of Jamf Protect is that, rather than being a simple malware toolset it is much, much more. While malware programs catch known malware code, the behavioral-based security of Jamf Protect — mapped to the MITRE ATT&CK framework —looks for unusual patterns, virus-like behavior, and other suspicious activity. Its signature detections can sandbox known malware, remove the device that showed malicious activity from the network and present its findings and built-in analysis.

In addition, Jamf Protect allows for astoundingly detailed and sortable data from the unified log in macOS for off-device analysis.

REQUIREMENT #5:
Patch Management

This requirement ensures that devices and software are not vulnerable to known security issues for which fixes are available.

Software must be:

- Kept up to date
- Licensed and supported
- Removed from devices when no longer supported
- Patched within 14 days of an update being released

Administrators can use Jamf Pro's Patch Management feature to monitor, track and patch software on managed devices: Patch Management automatically patches software on managed devices after an administrator uploads a package, associates it with a patch version and creates a patch policy. Administrators can also easily use Jamf Protect to alert on installation of new software to specific directories, such as /Applications, with a custom analytic.

Recent improvements to Jamf Pro after the purchase of Mondada's patch management solution, Kinobi, allow organisations to extend Jamf Pro's built-in patch management functionality to include all Mac applications within an environment. This helps them stay secure while taking away the headache of manually monitoring patch updates.

Jamf's patch server may provide software titles, or customers may wish to integrate an external patch source managed by themselves or a third party. Software title information includes supported OS versions.

Software can be easily uninstalled with a policy configured for uninstall or by removing the device from the scope of the Mac app store record.

Conclusion

Jamf Pro and Jamf Protect make it easy to implement and follow the National Cyber Security Centre's Cyber Essentials recommendations.

For a full and more detailed list of requirements, visit:
https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure

To put these security features to the test, request a **Free Product Trial**.