Executive Summary

Cyber Essentials is the UK government–backed certification that helps organizations of all sizes guard against the most common cyber threats and demonstrate their commitment to cybersecurity. Achieving this certification not only strengthens your security posture but also builds trust with customers, partners, and regulators.

This eBook, **UK Cyber Essentials with Microsoft 365**, is designed to bridge the gap between compliance requirements and real-world Microsoft 365 security controls. Many businesses already own the tools to meet Cyber Essentials standards but aren't using them to their full potential. By aligning the five Cyber Essentials technical control areas with Microsoft 365, we show you how to achieve compliance and elevate your security posture without unnecessary complexity or cost.

This eBook is based on Cyber Essentials: Requirements for IT Infrastructure v3.2

How the eBook is Structured:

For each of the five Cyber Essentials technical control areas: Firewalls, Secure Configuration, Security Update Management, User Access Control, and Malware Protection, we'll break down:

1. **Why It Matters**
    - The risks each control addresses.
    - How attackers exploit gaps in this area.
    - Why auditors look for evidence of control.
2. **Licensing Considerations**
    - Which protections are included in Microsoft 365 Business Premium, E3, and E5.
    - Where advanced licensing (e.g., Microsoft Defender for Endpoint, Entra ID P1/P2) unlocks more control.
    - How to maximize value from the licenses you already own.
3. **End-User Impact**
    - How each control affects day-to-day workflows (e.g., MFA prompts, restricted app installs, patch reboots).

- What staff will need to know.
- Communication strategies to reduce pushback and drive adoption.

4. **Implementation Steps**
    - Clear click-through guidance for configuring Microsoft 365 security and compliance features.
    - Baseline recommendations aligned to NCSC and Cyber Essentials requirements.
    - Audit-ready evidence collection tips for Cyber Essentials Plus.

1. **Firewalls**

Firewalls are critical in controlling the flow of traffic into and out of your devices and networks. Within a Microsoft 365 environment, firewall protections extend beyond the traditional office perimeter to include **endpoint firewalls and cloud access controls in Entra ID.**

At the device level, **Windows Defender Firewall** (centrally managed with Intune) enforces rules to block unauthorized inbound and outbound connections. At the identity and service edge, **Microsoft Entra Conditional Access** can restrict access based on network locations, ensuring that logins only occur from trusted IP ranges or geographies

On Devices:

Devices need to be enrolled into Intune where Firewall polices can be centrally managed and enforced on devices. If devices are not yet enrolled into Intune, do that first as a prerequisite step: Device enrollment guide for Microsoft Intune | Microsoft Learn

Licensing Considerations

- **Included in all Microsoft 365 tiers**: Windows Defender Firewall is built into Windows 10/11 Pro, Enterprise, and Education editions.
- **Intune (Endpoint Manager)** is required to centrally configure, enforce, and monitor firewall settings.

- **Microsoft Defender for Endpoint Plan 1 or 2 or Defender for Business** (included in M365 Business Premium and E5) adds visibility and reporting, surfacing firewall events in the security console.
- No additional license is required for basic firewall enforcement, but advanced detection and analytics rely on Defender for Endpoint.

End-User Impact

- Minimal day-to-day disruption when configured correctly.
- Some applications may initially be blocked if firewall rules are too strict, requiring IT to create allow exceptions. Overly restrictive rules may block line-of-business apps or custom software. These require exceptions.
- Users will not typically need to interact with the firewall — rules are silently applied in the background via Intune.
- Remote workers benefit from the same protections on home and public networks without needing to manage anything themselves.

Implementation Steps

Step 1: Configure Windows Firewall via Intune

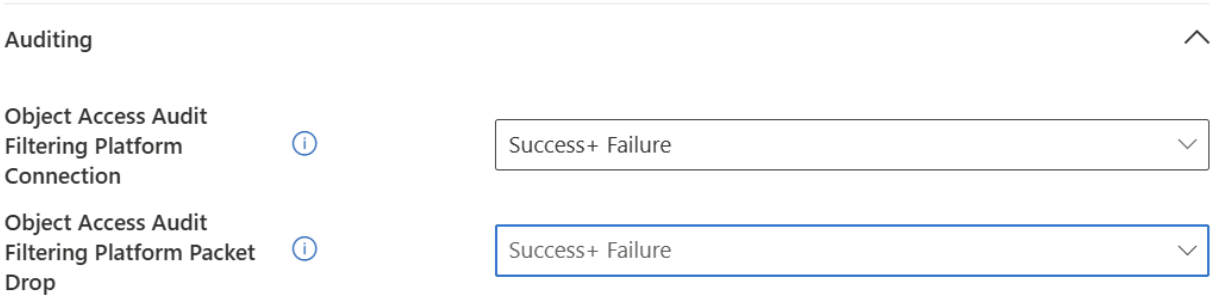
- Go to **Endpoint security → Firewall → Create Policy**.
- Platform: **Windows 10 and later**.
- Configure the following settings:

Certificate revocation list verification	Not configured
Disable Stateful Ftp	Not configured
Enable Packet Queue	Not Configured
IPsec Exceptions	Not Configured
Opportunistically Match Auth Set Per KM	Not configured
Preshared Key Encoding	Not configured
Security association idle time	Not Configured
Enable Domain Network Firewall	True (Default)
Allow Local Ipsec Policy Merge	True (Default)
Allow Local Policy Merge	True (Default)
Auth Apps Allow User Pref Merge	True (Default)
Default Inbound Action for Domain Profile	Block (Default)
Default Outbound Action	Allow (Default)
Disable Inbound Notifications	True
Disable Stealth Mode	False (Default)
Disable Stealth Mode Ipsec Secured Packet Exemption	True (Default)
Disable Unicast Responses To Multicast Broadcast	False (Default)
Enable Log Dropped Packets	Enable Logging Of Dropped Packets
Enable Log Ignored Rules	Disable Logging Of Ignored Rules (Default)

Enable Log Success Connections	Enable Logging Of Successful Connections
Global Ports Allow User Pref Merge	True (Default)
Shielded	False (Default)
	Configured
Log File Path	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
	Configured
Log Max File Size	16384

Enable Private Network Firewall	True (Default)
Allow Local Ipsec Policy Merge	True (Default)
Allow Local Policy Merge	True (Default)
Auth Apps Allow User Pref Merge	True (Default)
Default Inbound Action for Private Profile	Block (Default)
Default Outbound Action	Allow (Default)
Disable Inbound Notifications	True
Disable Stealth Mode	False (Default)
Disable Stealth Mode Ipsec Secured Packet Exemption	True (Default)
Disable Unicast Responses To Multicast Broadcast	False (Default)
Enable Log Dropped Packets	Enable Logging Of Dropped Packets
Enable Log Ignored Rules	Disable Logging Of Ignored Rules (Default)
Enable Log Success Connections	Enable Logging Of Successful Connections
Global Ports Allow User Pref Merge	True (Default)
Shielded	False (Default)
Log File Path	Configured %systemroot%\system32\LogFiles\Firewall\pfirewall.log
Log Max File Size	Configured 16384

Enable Public Network Firewall	True (Default)
Allow Local Ipsec Policy Merge	False
Allow Local Policy Merge	False
Auth Apps Allow User Pref Merge	True (Default)
Default Inbound Action for Public Profile	Block (Default)
Default Outbound Action	Allow (Default)
Disable Inbound Notifications	True
Disable Stealth Mode	False (Default)
Disable Stealth Mode Ipsec Secured Packet Exemption	True (Default)
Disable Unicast Responses To Multicast Broadcast	False (Default)
Enable Log Dropped Packets	Enable Logging Of Dropped Packets
Enable Log Ignored Rules	Disable Logging Of Ignored Rules (Default)
Enable Log Success Connections	Enable Logging Of Successful Connections
Global Ports Allow User Pref Merge	True (Default)
Shielded	False (Default)
Log File Path	Configured %systemroot%\system32\LogFiles\Firewall\pfirewall.log
Log Max File Size	Configured 16384



Step 2: Add Firewall Rules (optional)

- Firewall rules in Intune are optional — use them when you need to specifically allow or deny applications or ports.
- Example: A finance team uses a legacy accounting system that requires inbound TCP port 1433 for SQL traffic. A firewall rules profile can explicitly allow this connection while keeping all other inbound ports blocked.
- In most cases, leaving rules unconfigured and relying on the default block-inbound stance is sufficient.
- Sign in at https://endpoint.microsoft.com
- Navigate to Endpoint security → Firewall → Create Policy>Platform: Windows 10
- Profile: Windows Firewall Rules
- • Click + Add to create a new rule.
- • Fill out the details:
    - Name: A descriptive label (e.g., Allow SQL TCP 1433).
    - Direction: Inbound or Outbound.
    - Action: Allow or Block.
    - Enabled: Yes.
    - Protocol: Choose TCP, UDP, or Any.
    - Local port: Enter a specific port (e.g., 1433).
    - Remote port: Optional (can be set to Any).
    - Local address / Remote address: Optional, for scoping to specific IPs.
    - Application path: Optional, to target a specific app executable.

Conditional Access & Zero Trust in Microsoft 365

Traditional firewall models assumed that once a device or user was “inside the network,” they could be trusted. But in today’s world of remote work, hybrid offices, and cloud-first applications, there is no fixed perimeter. Employees access corporate data from coffee shops, home networks, or mobile devices, sometimes on unmanaged hardware.

This shift requires a Zero Trust approach: never trust by default, always verify, and enforce least privilege at every access point.

How Microsoft Implements This:

Microsoft 365 delivers Zero Trust through Entra ID Conditional Access:

- Context-aware controls: Policies evaluate who the user is, what device they’re using, where they’re connecting from, and the risk level of the sign-in.
- Adaptive access: Instead of simply “allow or block,” policies enforce conditions like require MFA when connecting from an unknown location or untrusted device.
- Granularity: Access can be scoped to specific applications (e.g., only allow Teams logins from compliant devices).
- Named Locations: Define trusted corporate networks vs. external IPs.
- Integration with Intune: Ensure only compliant, managed devices (encrypted, patched, AV-protected) can connect.

Defined Named Locations in Conditional Access

Attackers often attempt to compromise accounts from outside your normal operating region. If your business is UK-based but has no staff abroad, there is little reason for anyone to log in from other countries. By defining Named Locations in Entra ID, you can restrict access to your tenant, reducing risk from foreign-based attacks and credential stuffing.

At a minimum, businesses should define their home country (e.g., the United Kingdom) as an allowed Named Location, and block or challenge access from everywhere else. This simple step significantly reduces the number of malicious sign-in attempts that reach your environment.

Licensing Considerations

- Conditional Access requires Microsoft Entra ID P1 (included in Microsoft 365 Business Premium, E3, and above).
- Entra ID P2 (optional) adds risk-based policies (e.g., blocking based on risky sign-in behavior in addition to geography).
- No additional licensing is required for creating Named Locations themselves.

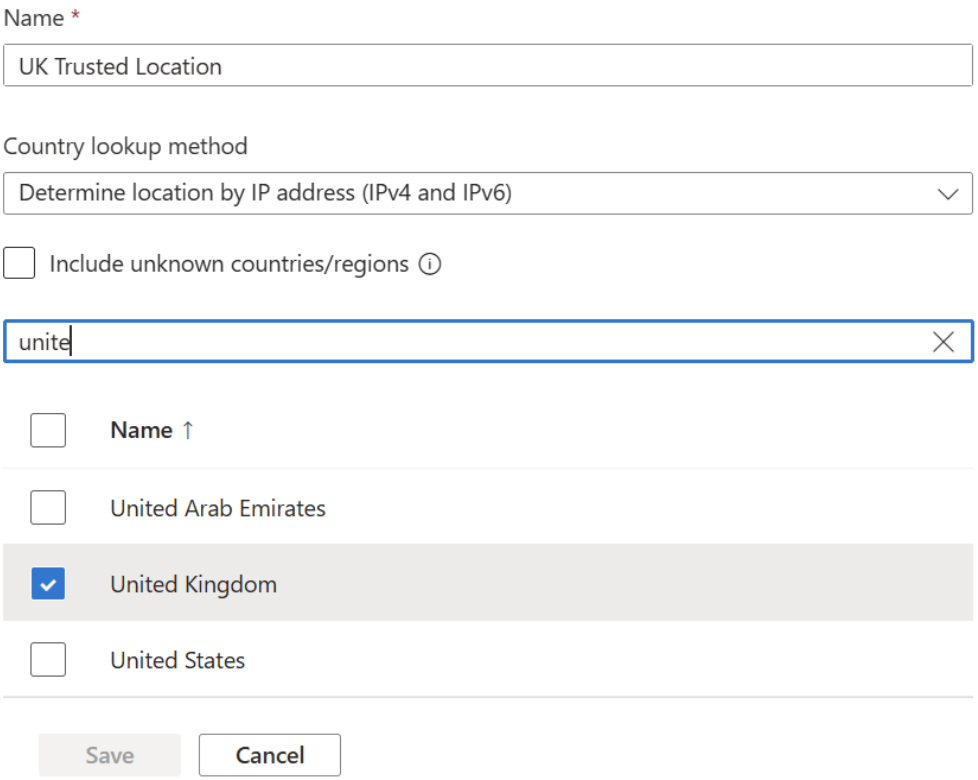
End-User Impact

- Expected behavior: Users in the UK log in normally with no additional friction.
- Blocked access: If a user attempts to sign in from outside the UK (whether malicious or legitimate), the login will be blocked.
- Travel exceptions: Staff who travel internationally will require policy exceptions or temporary exclusions. Without this, they may be locked out.

Implementation Steps

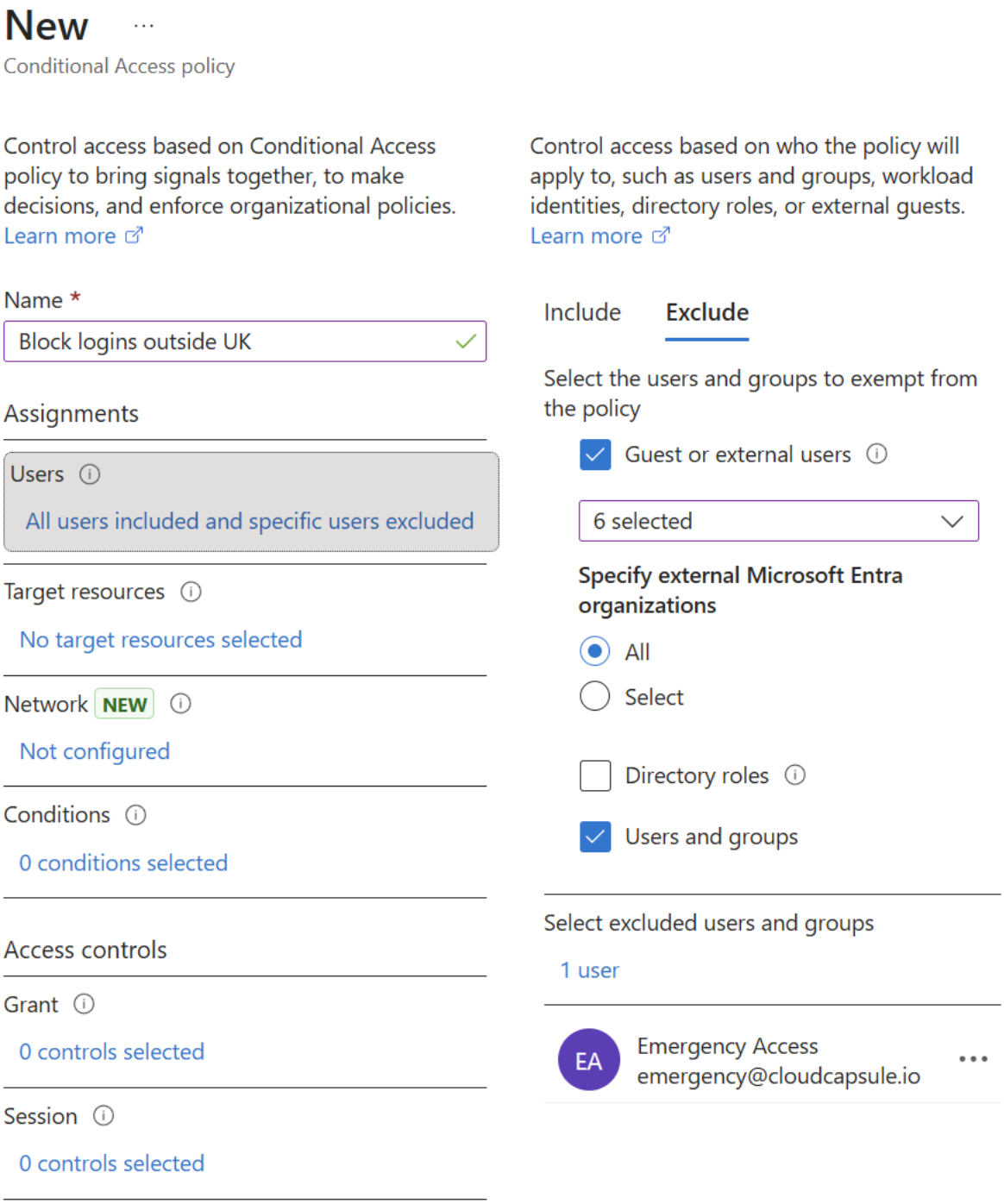
Step 1: Define Named Location

1. In the Entra admin center, go to Protection → Conditional Access → Named locations.
2. Select Countries/Regions location.
3. Choose United Kingdom (or your business's primary country).
4. Save this location as *"UK Trusted Location"*.

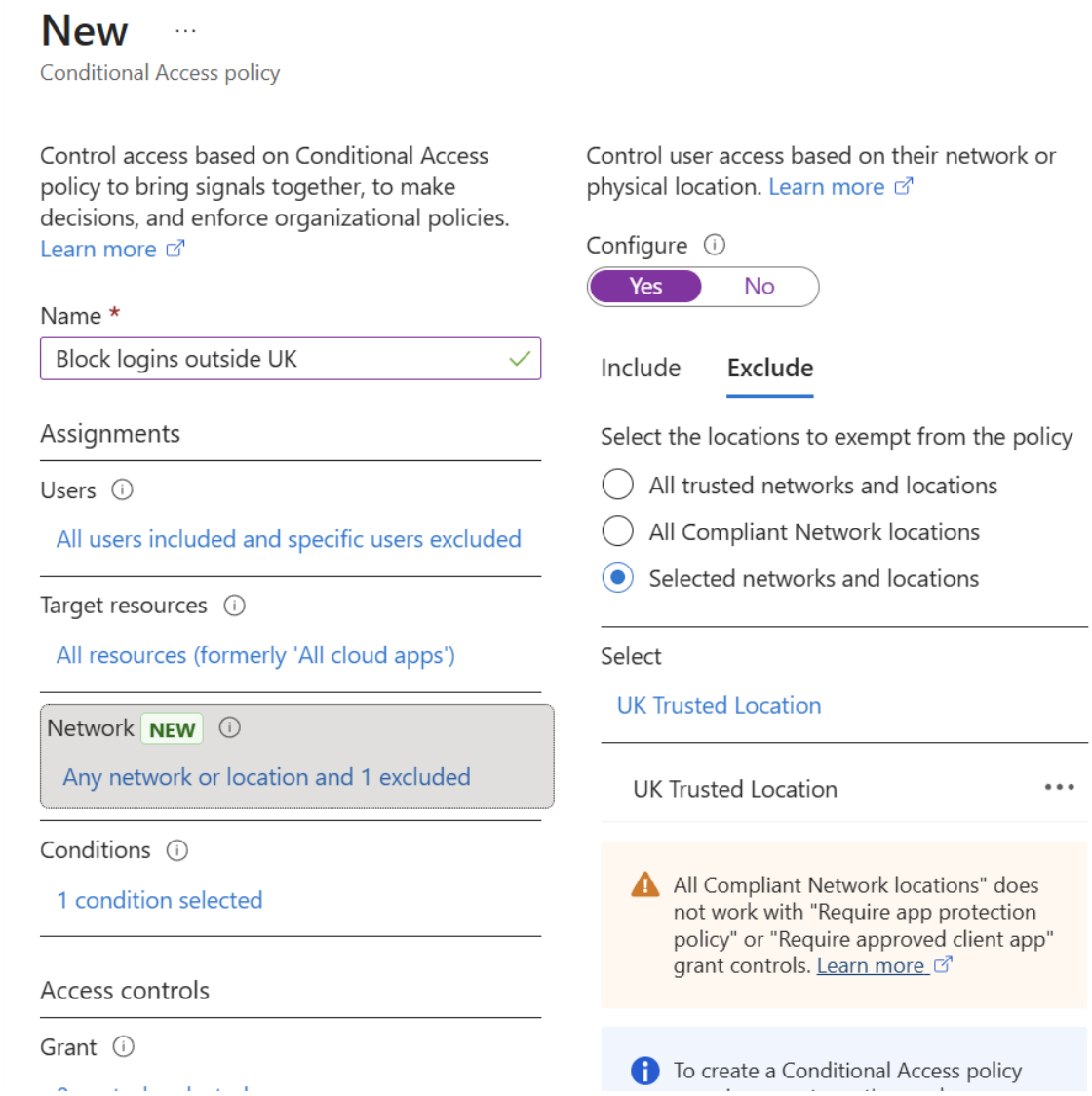


Step 2: Create Conditional Access Policy

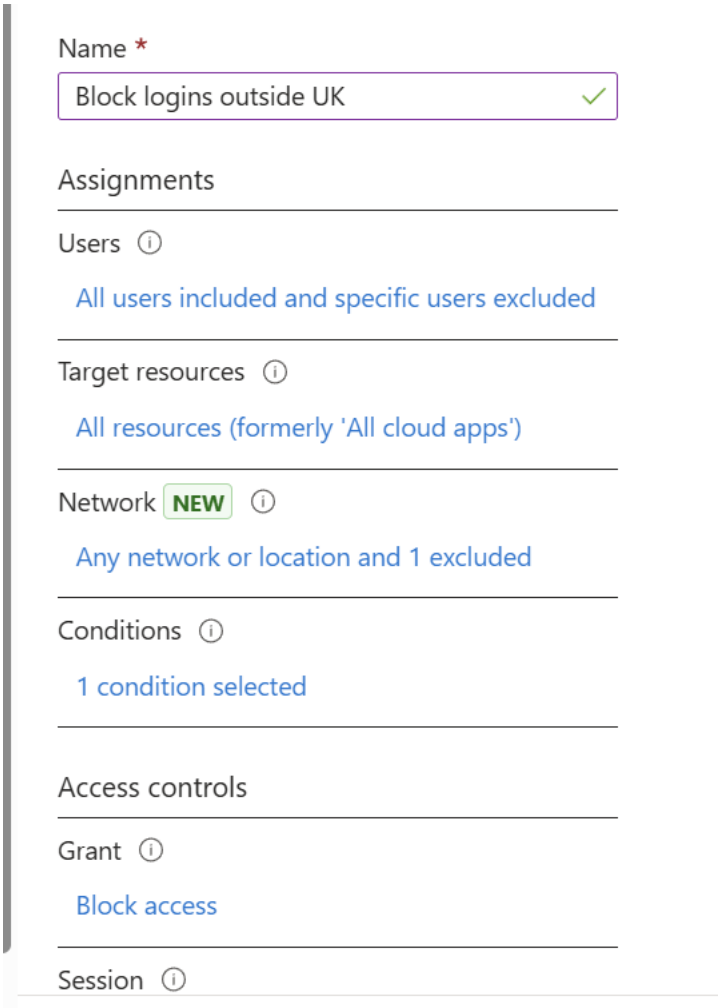
1. Navigate to **Protection → Conditional Access → Policies → New Policy**.
2. Name: *"Block logins outside UK"*.
3. **Assignments**:
    - Users: *All users* (or all except break-glass admin accounts).
        1. Exclude a break-glass admin account and guest users
    - Cloud apps: *All cloud apps*.



4. **Conditions → Locations**:
    - Include: *Any location*.
    - Exclude: *UK Trusted Location*.



5. **Access controls → Grant**:
    - Block access.



6. Enable policy in **Report-only mode** first → review logs → then enforce.

Step 3: Test and Document

- Verify in the **Sign-in logs** that attempts outside the UK are blocked.
- Document the Named Location and Conditional Access settings for your Cyber Essentials evidence.

2. Secure Configuration

Cyber Essentials Definition: 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 unauthorized access to your organization's sensitive information. But by applying some simple technical controls when installing computers and network devices, you can minimize vulnerabilities and protect against common types of attack.

Managed Devices

One of the most effective ways to maintain a secure configuration is by ensuring that devices accessing corporate resources are managed. With unmanaged or personal (BYOD) devices, IT has little to no visibility or control over:

- Whether the OS is patched,
- If antivirus is running,
- Whether encryption (BitLocker/File Vault) is enabled,
- Or if risky software is installed.

Attackers love BYOD because it's often the weakest link — a personal laptop with outdated software connecting directly to business-critical services. Cyber Essentials emphasizes reducing unnecessary risk; allowing unmanaged devices contradicts this principle.

Managed Devices in Microsoft Entra & Intune

- Entra ID Join: Corporate-owned devices are joined directly to Entra ID, enabling central policy enforcement.
- Hybrid Join: Devices joined to both on-prem AD and Entra ID (common in staged migrations).
- Intune Enrollment: Provides full management of configuration, patching, AV, and compliance enforcement.

With these in place, you can enforce Conditional Access policies that require devices to be:

- Enrolled Entra Joined or Hybrid Joined
- Be enrolled in Intune and Marked as compliant (e.g., encrypted, patched, no malware detected),
- Before they are granted access to Microsoft 365 apps and data.

Note: The policy coverage listed below is explicitly for Windows Devices.

Policies:

1. Devices are Joined or Hybrid Joined to Entra ID

For a device to be securely configured and consistently managed, it must first be joined into the organization's identity system. In Microsoft 365, that means joining devices into Microsoft Entra ID.

When devices are Entra-joined (cloud-native) or Hybrid-joined (on-prem + Entra), IT gains:

- Centralized policy enforcement (password, lockout, MFA).
- Visibility into device compliance and status.
- The ability to apply conditional access based on device trust.

Licensing Considerations

Any License type in Microsoft 365 supports joining devices into Entra ID.

Implementation Steps

Step 1: Enable Entra Join

1. In the **Entra admin center → Devices → Device settings**, set:
    - *Users may join devices to Azure AD*: Choose the right scope (e.g., All or specific groups).

Step 2: Join a Device

- During Windows setup (OOBE), choose **Join this device to Microsoft Entra ID**.
- Or, on existing devices:
    - Go to **Settings → Accounts → Access work or school → Connect**.
    - Sign in with corporate credentials → device is joined to Entra and automatically enrolled into Intune.
- For Hybrid: Configure Microsoft Entra hybrid join - Microsoft Entra ID | Microsoft Learn

Step 3: Validate in Entra & Intune

- In **Entra admin center → Devices**, verify the device shows as *Microsoft Entra joined*.

2. Devices are enrolled into Intune for MDM

Joining a device to Entra ID establishes identity trust, but Intune enrollment brings device management. With Intune, IT can:

- Push secure configuration profiles (firewall, encryption, password rules).
- Deploy security baselines aligned to Cyber Essentials.
- Enforce compliance (e.g., block outdated OS versions, require BitLocker).
- Remotely wipe or retire lost/stolen devices.

Without Intune enrollment, you have no assurance that endpoints meet the security standards required for Cyber Essentials. Users could connect with unpatched or misconfigured devices, bypassing the secure configuration principle.

Licensing Considerations

- Included in Microsoft 365 Business Premium, E3, and E5.
- No separate Intune license required for these suites.

Implementation Steps

Step 1: Configure Automatic Enrollment

1. In the **Intune admin center → Devices → Enroll devices → Automatic enrollment**, link Entra ID with Intune.
2. Select **MDM user scope** → *All users* (or specific groups).

Step 2: Enroll Windows Devices

- During OOBE: choose **Join this device to Microsoft Entra ID** → enrollment is automatic.
- On existing devices:
    - Go to **Settings → Accounts → Access work or school → Connect**.
    - Sign in with corporate credentials → device is auto-enrolled.

Step 3: Validate Enrollment

- In **Intune → Devices**, confirm the device shows as *MDM Enrolled*.

3. App Protection Policies are applied for Mobile Access

Not every mobile device that accesses company data will be corporate-owned or fully managed with Intune MDM. Staff often use their own phones and tablets for email, Teams, and document access. Without safeguards, sensitive data could be stored unprotected on personal devices or transferred to unmanaged apps.

App Protection Policies (APP) solve this problem by applying security directly to the corporate apps and data, not the entire device. They enforce rules such as:

- Requiring a PIN or biometric to open corporate apps.
- Encrypting data at rest within apps like Outlook and Teams.
- Preventing copy/paste or “Save As” into personal apps.
- Selectively wiping company data from a device without touching personal data.

This allows businesses to support BYOD for mobile access while still maintaining the secure configuration principle of Cyber Essentials.

Licensing Considerations

- Requires Microsoft Intune
- Included in Microsoft 365 Business Premium, E3, and E5.

End-User Impact

- Users can continue using their personal devices without full corporate control.
- They may notice:
    - PIN or biometric prompt when opening Outlook, Teams, or OneDrive.
    - Restrictions on copy/paste, saving, or sharing files outside approved apps.
    - Company data disappearing if they leave the business or the device is unenrolled (selective wipe).
- Minimal impact on personal use — personal apps and data remain untouched.

Implementation Steps

Step 1: Create an App Protection Policy

1. In **Intune admin center → Apps → App protection policies → Create policy**.
2. Choose platform: *iOS/iPadOS* or *Android*.
3. Configure settings:
    - Require PIN or biometric to access corporate apps.
    - Encrypt data within managed apps.
    - Restrict cut/copy/paste between apps (e.g., only allowed between Outlook and Teams).
    - Prevent "Save As" to unmanaged storage.

Step 2: Assign to Users

- Target the policy to **users or groups** who access company apps on mobile devices.
- Common assignment: *All users* for email/Teams access.

Step 3: Enforce Access via Conditional Access

- Create a **Conditional Access policy** that requires apps to be protected by APP before accessing Microsoft 365.
- Example: *"Require approved client app + App Protection Policy"*.

Step 4: Validate

- Test on a personal iOS/Android device by signing into Outlook or Teams.
- Confirm PIN prompt, encryption, and sharing restrictions are applied.

4. **Device Platform Restrictions are set in Intune**

Cyber Essentials requires organizations to ensure that only **trusted and supported devices** can access business resources. Allowing any device — including personally owned laptops or outdated platforms — increases the risk of unmanaged, insecure endpoints accessing sensitive data.

In Microsoft Intune, **Device Enrollment Restrictions** provide granular control over:

- Which **platforms** (Windows, iOS/iPadOS, macOS, Android) are allowed to enroll.
- Whether **personally owned devices** are permitted to register or join.

By default, all platforms and ownership types are often set to **Allow**. For Cyber Essentials compliance, you should review and restrict these settings to **block personal devices** unless explicitly needed, and ensure only supported OS platforms can be used.

Licensing Considerations

- **Microsoft Intune** (included with Microsoft 365 Business Premium, E3, and E5) is required.
- No additional licensing is needed to configure platform or ownership restrict

End-User Impact

- Users attempting to enroll a **personal device** (e.g., home Windows PC or personal iPhone) will be blocked.
- This prevents “shadow IT” scenarios where corporate data is accessed from unmanaged hardware.
- Corporate-issued and Intune-managed devices continue to enroll normally.

Implementation Steps

Step 1: Open Enrollment Restrictions

1. In the **Intune admin center → Devices → Enrollment → Enrollment restrictions**.
2. You'll see two types of restrictions:
    - **Device type restrictions** → Control which platforms are allowed.
    - **Device limit restrictions** → Limit how many devices a user can enroll.

Step 2: Modify Default Device Type Restriction

1. Edit the **All Users** restriction (or create a new custom one).
2. Under **Platform settings**, allow only supported platforms (e.g., Windows 10/11, iOS 16+, Android Enterprise).
3. Block outdated or unsupported platforms (e.g., Android device administrator, legacy Windows versions).

Step 3: Block Personally Owned Devices

- For each allowed platform, set **Personally owned** = **Block**.
- This ensures only **corporate-issued, Intune-enrolled devices** can access company resources.

Step 4: Assign to All Users

- Apply the restriction to all users or to security groups that should be limited to corporate devices only.

Step 5: Validate

- Attempt to register a personal device → enrollment should fail.
- Monitor **Enrollment failures** under Intune → Devices → Monitor.

5. Managed Devices are required for Sign-In

Cyber Essentials requires organizations to ensure that only **trusted, secure devices** can access company resources. Allowing unmanaged or personal devices to sign in introduces risk — attackers could use stolen credentials from any machine, bypassing all endpoint protections.

With **Microsoft Entra Conditional Access**, you can enforce that only **Hybrid-joined (on-prem AD + Entra)** or **Entra-joined (cloud-native)** devices are allowed to sign in. This guarantees that devices are enrolled, managed, and subject to your Intune compliance policies.

By blocking access from unmanaged endpoints, businesses prevent data leakage and align directly with Cyber Essentials' goal of reducing the attack surface.

Licensing Considerations

- Requires **Microsoft Entra ID P1** (included in Microsoft 365 Business Premium, E3, and E5).
- Intune is required to apply compliance and secure configuration settings to managed devices.
- No additional license needed for the core Conditional Access policy.

End-User Impact

- Users signing in from **managed devices** (Hybrid or Entra-joined) → normal access.
- Users on **personal or unmanaged devices** → blocked or restricted depending on policy.
- Guest accounts may be excluded if business workflows require external collaboration.
- Short-term disruption possible if users previously accessed services from BYOD devices.

Implementation Steps

Variation 1: Hybrid-Joined Devices

1. In **Entra admin center → Protection → Conditional Access → Policies → New policy**.
2. Assignments:
    - Users: *All users* (exclude break-glass admin and guest accounts).
    - Cloud apps: *All cloud apps*.
3. Conditions:
    - **Device platforms**: Windows
4. Access controls:
    - **Grant → Require device to be Hybrid Azure AD joined**.
5. Save and enable.

Variation 2: Entra-Joined Devices

1. In **Entra admin center → Conditional Access → Policies → New policy**.
2. Assignments:
    - Users: *All users* (exclude break-glass admin and guest accounts).
    - Cloud apps: *All cloud apps*.
3. Conditions:
    - Go to **Conditions → Devices → Filter for devices**.
    - Add filter: *device.trustType -eq "AzureAD"*.
    - This ensures only **Entra-joined devices** are trusted.
4. Access controls:
    - **Grant Controls → Block**
5. Save and enable.

Password & Lockout Requirements

Strong authentication is one of the most effective ways to reduce account compromise. Cyber Essentials requires organizations to enforce **minimum password standards** (length and complexity) and **lockout rules** to block brute force attempts. In Microsoft 365, how this is managed depends on whether devices are **cloud-joined, hybrid-joined, or Intune-only enrolled**.

Password Management in Entra vs. AD

- **Entra-joined devices**: Passwords are managed centrally in **Entra ID**. Policies for complexity, length, and lockout thresholds are applied consistently across cloud resources and device sign-ins.
- **Hybrid-joined devices**: Passwords are governed by **Active Directory Group Policy (GPOs)**. Intune can layer on compliance checks, but the baseline comes from on-prem AD.
- **Non-joined devices enrolled in Intune (MDM only)**: Password requirements (e.g., minimum length, complexity) can be pushed directly via **Intune device restriction policies**.'

Lockout & Screen Requirements with Intune

Beyond password policies, Intune enforces **local device protections**:

- **Auto-lock timers**: Require devices to lock after inactivity (e.g., 15 minutes).
- **Password or PIN on wake**: Users must re-authenticate when resuming from lock.
- **Failed attempt lockout**: Configure thresholds (e.g., 10 failed attempts → lockout for 15 minutes).
- **Biometric integration**: Support Windows Hello for Business with PIN/biometric as an alternative.

Policies

1. **Custom Lockout Requirements in Entra ID**

Cyber Essentials requires that accounts are locked out after a certain number of failed sign-in attempts to defend against brute-force and credential stuffing attacks. Without this, attackers can attempt unlimited password guesses until they succeed.

In Microsoft 365, these protections are configured in **Microsoft Entra ID Password Protection**. With custom smart lockout, administrators define the **threshold** (number of failed attempts) and the **lockout duration**, balancing security with user convenience.

Licensing Considerations

- **Available in all Microsoft Entra ID tiers**, including the free version.
- No additional license is needed for configuring smart lockout or password protection.
- For hybrid environments, password protection can also extend to **on-prem Active Directory**, but requires Entra Connect integration.

End-User Impact

- Users who repeatedly mistype their password may be temporarily locked out (e.g., 10 attempts → 1 minute lockout).
- Helps prevent account compromise but can be disruptive if thresholds are set too aggressively.
- Self-service password reset (SSPR) or MFA helps users recover quickly if legitimately locked out.

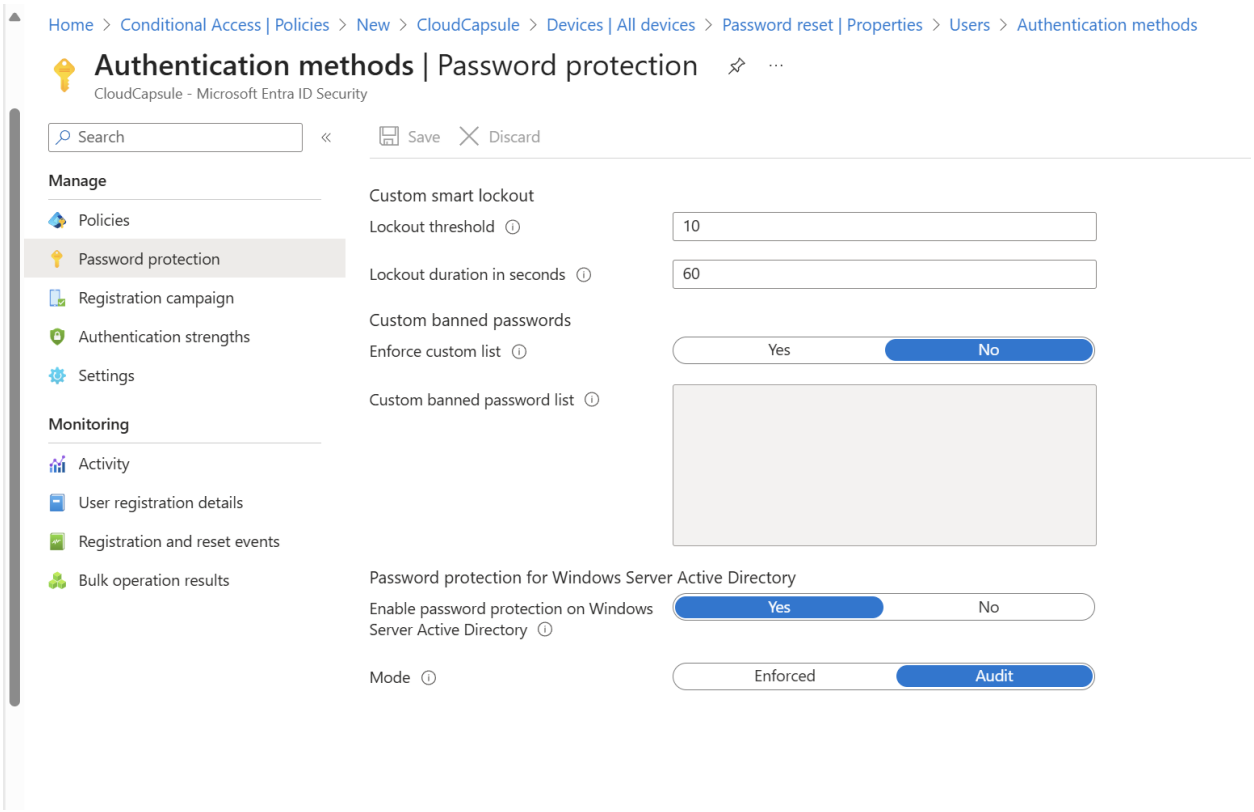
Implementation Steps

Step 1: Navigate to Password Protection

1. Go to **Entra admin center → Protection → Authentication methods → Password protection**.

Step 2: Configure Custom Smart Lockout

- **Lockout threshold**: Recommended = *10 failed attempts*.
- **Lockout duration**: Recommended = *60 seconds (1 min)*.
- This provides security against brute force without overly disrupting legitimate users.



2. **Configuration Profiles are configured for Device Locking**

Cyber Essentials requires that devices automatically lock after a period of inactivity to reduce the risk of unauthorized access. If a laptop or mobile device is left unattended, an attacker could easily access sensitive data unless the screen locks and requires reauthentication.

With Intune Configuration Profiles, organizations can centrally enforce idle lock timers and require reauthentication when devices wake. This ensures a consistent baseline across all managed devices — whether in the office, remote, or hybrid.

Licensing Considerations

- **Microsoft Intune** is required to configure and deploy device restriction profiles.
- Intune is included with **Microsoft 365 Business Premium, E3, and E5**.
- No additional Defender licensing is needed for this control.

End-User Impact

- Users will notice devices locking automatically after a set idle period (e.g., 15 minutes).
- They must re-enter their password, PIN, or biometric to resume work.
- While this may feel like a minor inconvenience, it's essential for compliance and security — especially in shared or open workspaces.

Implementation Steps

Step 1: Create a Configuration Profile

1. Go to **Intune admin center → Devices → Configuration profiles → Create new policy**.
2. Platform: *Windows 10 and later*.
3. Profile type: *Templates>Device Restrictions*

Step 2: Configure Device Lock Settings

- Under Password:
- Configure the following options:
    - **Require password**: *Yes*.
    - **Minimum password length**: *14 characters*
    - **Block simple passwords**: *Yes*.
    - **Password expiration (days)**: Leave unset unless specifically required (NCSC recommends not forcing expiry).
    - **Prevent reuse of previous passwords**: *24*
    - **Maximum minutes of inactivity until screen locks**: *15 minutes max*.
    - **Windows Hello device authentication**: *Allow*

Step 3: Assign the Profile

- Target to device groups (e.g., *All Windows laptops*).

Step 4: Validate on Endpoints

- After assignment, test on a Windows device.
- Leave idle for 15 minutes → confirm lock screen triggers and requires reauthentication.

Step 5: Document for Audit

- Provide screenshots of Intune policy configuration.
- Demonstrate test results with device lockout behavior.

3**. Minimum Password Requirements are set in Intune**

Passwords are still a critical layer of defense in Microsoft 365 environments. Weak or short passwords are one of the most common ways attackers gain access, often through credential stuffing or brute-force attempts. Cyber Essentials requires organizations to enforce **minimum standards** for password length, complexity, and reuse to reduce this risk. This section is specifically for non-joined devices that are authenticating to managed workstations.

With **Intune Device Compliance Policies** and **Configuration Profiles**, administrators can centrally define minimum password requirements for managed devices — ensuring a consistent baseline across Windows laptops, desktops, and mobile devices.

Licensing Considerations

- **Microsoft Intune** is required to configure and enforce password policies on devices.
- Intune is included with **Microsoft 365 Business Premium, E3, and E5**.
- No additional licensing is needed beyond baseline Intune.

End-User Impact

- Users may need to change their password if their current one doesn't meet requirements.
- They'll be required to create stronger passwords or PINs going forward.
- Some users may initially resist stricter rules, but it significantly reduces risk of compromise.

- With **Windows Hello for Business**, users can substitute strong passwords with PINs and biometrics, making the experience smoother.

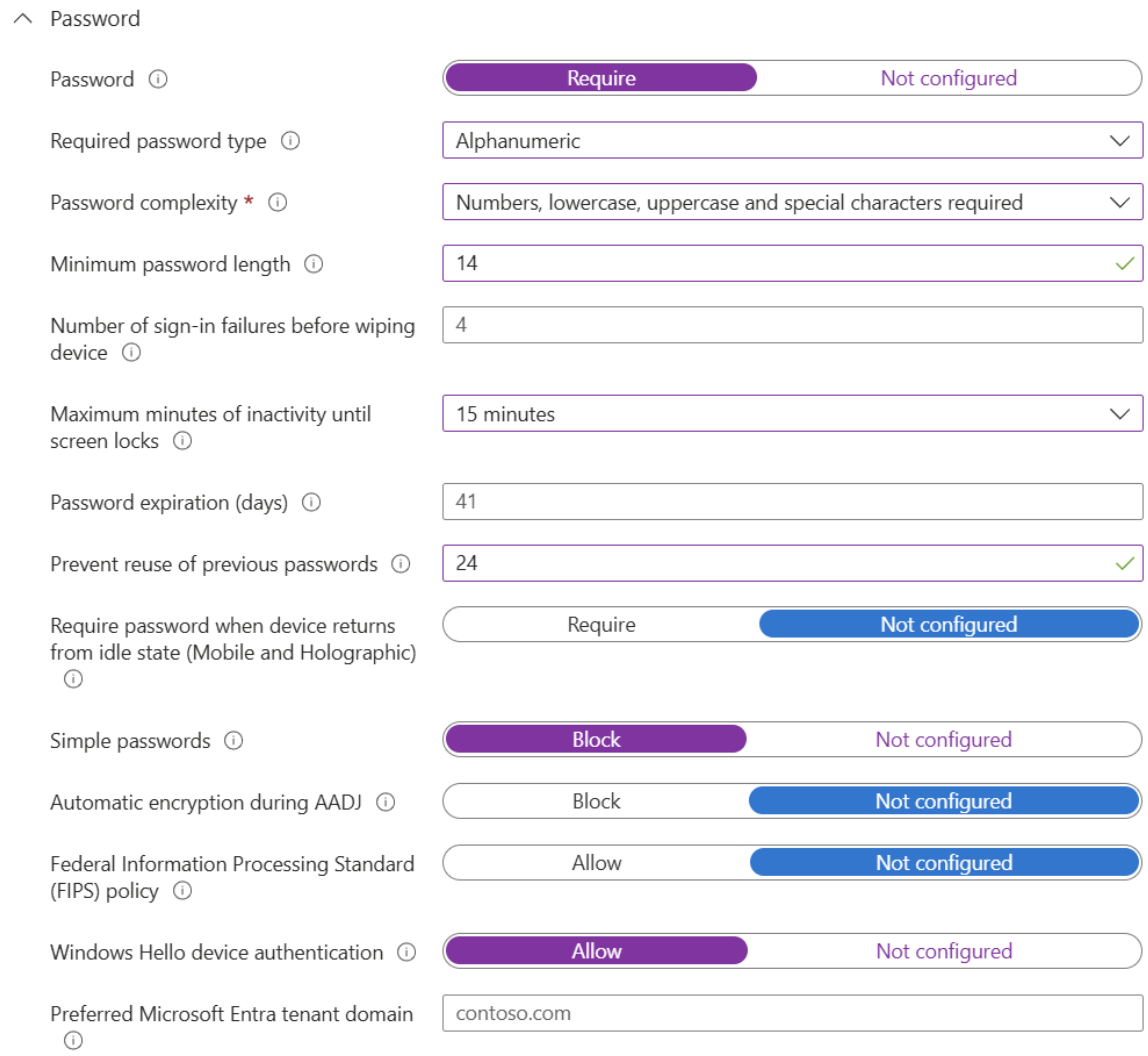
Implementation Steps

Step 1: Create a Configuration Profile

1. In the **Intune admin center → Devices → Configuration profiles → Create profile**.
2. Platform: *Windows 10 and later*.
3. Profile type: *Settings catalog*.
4. Name the profile (e.g., *"Windows – Minimum Password Policy"*).

Step 2: Configure Password Settings

1. Under **Configuration settings**, search for *Password*.
2. Configure the following options:
    - **Require password**: *Yes*.
    - **Minimum password length**: *14 characters* (
    - **Block simple passwords**: *Yes*.
    - **Password expiration (days)**: Leave unset unless specifically required (NCSC recommends not forcing expiry).
    - **Password history**: *Remember last 24 passwords*.
    - **Device lock after inactivity**: *15 minutes max*.
    - **Require password on wake**: *Enabled*.



Step 3: Assign the Profile

- Under **Assignments**, select the device groups you want to target (e.g., *All laptops*).

Step 4: Review & Create

- Confirm settings → click **Create**.

Step 5: Validate & Monitor

- On a test device, attempt to set a short or simple password (e.g., “1234” or “password”).
- Confirm that it’s rejected.
- Use **Intune → Reports → Device configuration** to monitor compliance and catch any failures.

4. **Windows Hello For Business is leveraged for Device sign in**

Passwords are one of the weakest links in cybersecurity. They can be guessed, reused, or stolen in phishing and credential stuffing attacks. Cyber Essentials requires organizations to enforce strong authentication and protect accounts from brute-force compromise.

Windows Hello for Business (WHfB) replaces traditional passwords with **multi-factor authentication tied to the device itself**. Users sign in with something they **know** (a PIN) and something they **have** (the enrolled device) — often combined with something they **are** (biometric, like fingerprint or facial recognition).

Because the PIN is unique to the device and never transmitted to a server, even if stolen, it cannot be used elsewhere. This dramatically reduces the risk of password-based attacks.

Licensing Considerations

- **Included in Microsoft 365 Business Premium, E3, and E5**.
- Requires devices to be **Entra-joined or Hybrid-joined** and **Intune-managed**.
- Works best when combined with **MFA/Conditional Access** for cloud apps.

End-User Impact

- Users sign in with a short PIN, fingerprint, or facial recognition instead of a long, complex password.
- Faster and more convenient daily login experience.
- If biometric fails, the device still requires the PIN (cannot fall back to just a password).
- Some users may need training to understand the difference between their Microsoft account password and their WHfB PIN.

Implementation Steps

Step 1: Enable Windows Hello for Business in Intune

1. Go to **Intune admin center → Devices → Windows → Windows enrollment → Windows Hello for Business**.
2. Configure as follows:

- **State**: Enabled.
- **Configure Windows Hello for Business**: Enabled.
- **PIN complexity**: Require 6+ digits, block simple patterns (e.g., 111111).
- **Biometrics**: Enabled if hardware supports it (Face/Fingerprint).
- **Use enhanced anti-spoofing**: Enabled.

Step 2: Create an Intune Device Configuration Profile

1. Go to **Configuration profiles → Create profile**.
2. Platform: *Windows 10 and later*.
3. Profile type: *Identity protection*.
4. Configure:
   - Minimum PIN length = 6+ digits.
   - Special characters = Optional, based on policy.
   - Expiration = None (PINs are device-tied, not reused like passwords).

Step 3: Assign to Users or Devices

- Assign policy to device/user groups (e.g., *All Windows 10/11 Devices*).

Step 4: Educate Users

- Communicate that WHfB replaces their device password with a device-specific PIN/biometric.
- Reinforce that this improves both **security and convenience**.

Local User and Administrator Accounts

Cyber Essentials requires that devices are configured securely, which includes removing or restricting unnecessary accounts and minimizing administrative privileges. Local accounts — especially those with admin rights — are a common target for attackers, as they can be used to escalate privileges, disable security tools, or move laterally between systems.

In Microsoft 365 environments, Entra ID and Intune provide centralized controls to manage how local accounts are created, secured, and monitored. By configuring **local administrator settings, leveraging Windows Autopilot, enforcing unique admin passwords with LAPS, and blocking personal accounts from gaining admin access**, organizations ensure only the right people, with the right permissions, can perform sensitive actions on devices.

This subsection covers the key controls to harden local user and administrator accounts so that devices meet Cyber Essentials' secure configuration requirements while reducing the risk of privilege misuse.

Policies

1. Configure Local Administrator Settings for Device Joins

By default, when a Windows device is joined to Microsoft Entra ID, the **user performing the join** may be added as a local administrator. Similarly, global administrators can also end up with unnecessary local admin rights on endpoints.

From a Cyber Essentials perspective, uncontrolled local admin rights represent a major security risk:

- Attackers who compromise a local admin account gain **full control of the device**.
- Local admin rights can be used to **disable security controls**, install malicious software, or extract credentials.
- Cyber Essentials explicitly requires that **unnecessary accounts and privileges are removed** as part of secure configuration.

Properly configuring local administrator settings ensures only a **small, controlled set of IT accounts** have local admin access, reducing the risk of privilege abuse.

Licensing Considerations

- **Microsoft Entra ID (all tiers)** allows configuration of local admin settings during device joins.

End-User Impact

- Standard users will not have local admin rights on their corporate devices.
- This may prevent them from installing applications or making system changes without IT approval.
- While it may feel restrictive, it prevents malware or phishing attempts from elevating privileges silently.

Implementation Steps

Step 1: Configure Device Join Settings in Entra

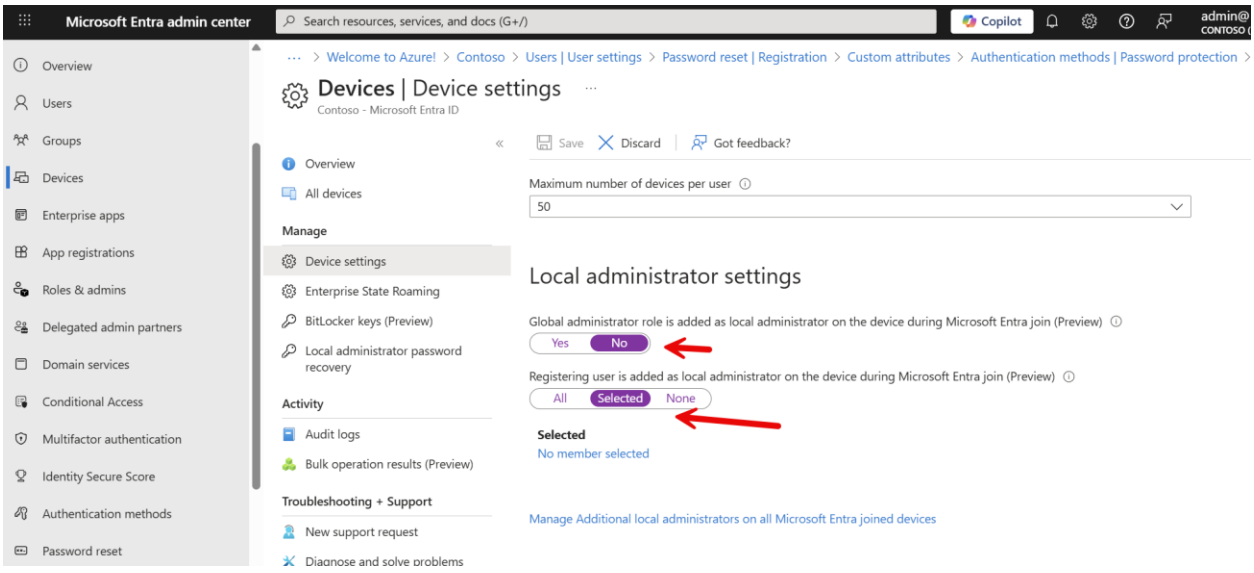
1. In the **Entra admin center → Devices → Device settings**.
2. Under **Local administrator settings**:
    - **Global administrator role is added as local administrator** → Set to **No**.
    - **Registering user is added as local administrator** → Set to **None** or **Selected** (limit to specific IT groups).

Step 2: Define Additional Local Admins

- Use the link **Manage Additional local administrators on all Microsoft Entra joined devices**.
- Add only **dedicated IT admin accounts or groups**.

Step 3: Validate and Monitor

- Test by enrolling a new device → confirm end-users are standard users only.
- Periodically audit local admin membership using Intune or Defender for Endpoint reports.



2. Windows Autopilot Profiles for Local Account Control

When new Windows devices are provisioned, the first account created during setup typically becomes a **local administrator**. If unmanaged, this default behavior introduces risk, as every user who sets up a device could unknowingly grant themselves admin rights.

Windows Autopilot solves this problem by automating the provisioning process and ensuring consistent, secure settings. Autopilot profiles can be configured to **create the initial local account as a standard user** instead of an administrator. This aligns directly with Cyber Essentials' requirement to **minimize unnecessary accounts and privileges**.

With Autopilot, devices are shipped straight from the vendor to the end-user, but when powered on and connected to the internet, they:

1. Automatically join Microsoft Entra ID.
2. Enroll into Intune.
3. Apply the assigned Autopilot profile.
4. Create the local user account with the role specified in the profile (Standard or Administrator).

Licensing Considerations

- **Windows Autopilot** is available with **Microsoft Intune** (included in Microsoft 365 Business Premium, E3, and E5)

End-User Impact

- Users receive devices preconfigured and ready to use without needing IT to manually image or configure them.
- If the Autopilot profile is set to **Standard user**, end-users will not have local admin rights.
- Reduces variability in device setup while still offering a smooth out-of-box experience.

Implementation Steps

Step 1: Import Devices into Autopilot

1. In the **Intune admin center → Devices → Windows → Windows enrollment → Devices**, import hardware IDs provided by OEM or captured manually.

Step 2: Create an Autopilot Profile

1. Go to **Intune → Devices → Windows → Windows enrollment → Deployment profiles**.
2. Click **+ Create profile → Windows PC**.
3. Configure profile settings:
    - **Convert all targeted devices to Autopilot**: Yes.
    - **Join to Microsoft Entra ID**: Yes.
    - **User account type**: Select *Standard user* (preferred for Cyber Essentials).
    - **Skip privacy and setup pages**: Enabled for consistency.

Step 3: Assign Profile

- Assign the profile to the device group that contains your Autopilot-registered devices.

Step 4: Test and Validate

- Power on a new device → it should auto-join Entra ID, enroll in Intune, and create the local account as a **Standard user**.

3. Enable Microsoft Entra Local Administrator Password Solution (LAPS)

Even if local administrator accounts are restricted, many organizations still need at least one local admin account on Windows devices for support and recovery. If this account has a **shared or static password** across multiple devices, it becomes a massive risk:

- If an attacker compromises one device, they can use the local admin password to move laterally across the environment.
- Static passwords are often weak or reused, making them easier to crack.

The **Local Administrator Password Solution (LAPS)** mitigates this risk by automatically generating **unique, complex passwords** for local admin accounts on each device. These passwords are stored securely in Microsoft Entra ID (cloud-native) or Active Directory (on-prem), and IT admins can retrieve them when needed.

This aligns directly with Cyber Essentials' requirement to **remove unnecessary accounts** and **securely configure required accounts**.

Licensing Considerations

- **Windows LAPS (cloud-native)** is included in **Windows 10/11 Pro, Enterprise, and Education editions (April 2023 update or later)**.
- Management and policy deployment are available through **Intune** (included in Microsoft 365 Business Premium, E3, and E5).

End-User Impact

- End-users are **not impacted** — they continue logging in with their Entra ID accounts.
- IT admins may need to adjust workflows to retrieve local admin passwords via Entra ID/Intune rather than relying on a shared static credential.

Implementation Steps

Step 1: Enable LAPS in Entra

1. Go to the **Entra admin center → Devices → Device settings**.
2. Enable **Local administrator password solution (Preview)**.

Step 2: Create and Assign LAPS Policy in Intune

1. In the **Intune admin center → Endpoint Security → Account protection → Create policy**.
2. Platform: *Windows 10 and later*.
3. Configure settings:
    - **Backup directory**: *Microsoft Entra ID*.
    - **Administrator account name**: Specify or use default built-in admin.
    - **Password complexity**: *Large letters, small letters, numbers, special characters*.
    - **Password length**: At least *14 characters*.
    - **Password age (days)**: Rotate every *30 days*.

Step 3: Retrieve Passwords (IT Admin Use Only)

- In **Entra admin center → Devices → Local administrator password**, admins can view or reset passwords when needed.
- Access is restricted to accounts with appropriate RBAC roles (e.g., Privileged Authentication Administrator).

Step 4: Validate and Document

- Confirm each managed device has a unique local admin password.
- Test retrieval of a password in Entra to ensure backup is working.
- Capture screenshots/policy exports as evidence for Cyber Essentials Plus audit.

Local Protections

Cyber Essentials requires that devices are configured to minimize the risk of malware infection and unauthorized access. Local protections harden endpoints directly by applying system-level security settings, restricting risky behavior, and ensuring sensitive data is encrypted. In Microsoft 365 environments, these controls are typically applied via Intune configuration profiles, Attack Surface Reduction (ASR) rules, and BitLocker encryption policies.

The following controls ensure consistent, baseline protections across all managed devices.

1. Set Default Behavior for AutoRun

AutoRun is a legacy Windows feature that automatically executes commands from removable media (USB drives, CDs, DVDs) when inserted. Attackers often use malicious USBs or media to exploit this functionality, allowing malware to run without user consent.

Disabling AutoRun closes this attack vector, preventing opportunistic infections and aligning with Cyber Essentials' requirement to disable unnecessary features that expand the attack surface.

Licensing Considerations

- **Intune** is required to deploy the configuration at scale.
- Intune is included in **Microsoft 365 Business Premium, E3, and E5**.
- No additional Defender licensing is required for this control.

End-User Impact

- Users will no longer see software auto-launch when inserting USB drives, CDs, or DVDs.
- They will still be able to manually open files (e.g., Word docs, PDFs) from removable media.
- Minimal disruption to daily workflows — but users should be made aware of the change to reduce confusion.

Implementation Steps

Step 1: Create a Configuration Profile

1. Go to **Intune admin center → Devices → Configuration profiles → Create profile**.
2. Platform: *Windows 10 and later*.
3. Profile type: *Settings catalog*.

Step 2: Configure AutoRun Settings
In the settings catalog, search for *AutoPlay/AutoRun* and configure:

- **Turn off AutoPlay**: *Enabled → All drives*.
- **Set the default behavior for AutoRun**: *Enabled → Do not execute any AutoRun commands*.
- **Turn off Autoplay for non-volume devices**: *Enabled*.

Step 3: Assign and Deploy

- Assign the profile to all managed Windows devices.

Step 4: Validate

- Insert a USB or DVD → confirm that nothing executes automatically.
- Review Intune device configuration reports for successful policy application.

2. Bitlocker encryption is applied on all devices

Cyber Essentials requires that data stored on devices is protected, even if a laptop or PC is lost or stolen. Without encryption, attackers can bypass sign-in controls by directly accessing the disk.

BitLocker (on Windows) and **FileVault** (on macOS) provide full-disk encryption, ensuring that data at rest is only accessible to authorized users. Even if an attacker removes the drive, the data remains unreadable without the decryption key.

For Microsoft 365 environments, enforcing encryption through Intune guarantees that **all managed devices** meet this baseline consistently.

Licensing Considerations

- **BitLocker** is available in Windows 10/11 Pro, Enterprise, and Education.
- Management and enforcement require **Intune** (included in Microsoft 365 Business Premium, E3, and E5).
- **Key escrow in Entra ID** is supported for cloud-joined and hybrid devices.
- macOS encryption (FileVault) can also be enforced via Intune, using the same compliance policies.

End-User Impact

- Encryption happens in the background after policy deployment — minimal disruption.
- A restart may be required for initial enablement.
- Users may see prompts to back up their BitLocker recovery key (if not automatically escrowed to Entra/Intune).
- Device performance impact is negligible on modern hardware.

Implementation Steps

Step 1: Create a BitLocker Policy

1. In **Intune admin center → Endpoint Security → Disk encryption → Create Policy**.
2. Platform: *Windows 10 and later*.
3. Profile type: *BitLocker*.

Step 2: Configure Policy Settings

- **Require BitLocker**: Enabled.
- **Encryption method**: XTS-AES 256 (preferred).
- **Fixed and removable drives**: Encrypt OS drives, fixed drives, and optionally removable drives.
- **Recovery key backup**: Require backup to **Microsoft Entra ID** (cloud escrow).

- **User interaction**: Hide or minimize prompts where possible to avoid user confusion.

Step 3: Assign the Policy

- Apply to device groups (e.g., *All Windows laptops*).

Step 4: Monitor Compliance

- Go to **Intune → Endpoint Security → Disk encryption → Monitor**.
- Verify encryption status and recovery key backup for all devices.

Step 5: macOS Devices (FileVault)

- In **Intune → Endpoint Security → Disk encryption**, create a FileVault policy for macOS.
- Require FileVault and escrow recovery keys to Intune.

Monitoring and Compliance

Cyber Essentials isn't just about setting policies — it's about proving they're consistently applied. Devices must be monitored to ensure they remain compliant with baseline security requirements. Microsoft Intune provides Compliance Policies, which evaluate devices against your organization's security standards and mark them as compliant or noncompliant. These results can then feed into Conditional Access to block or restrict risky devices.

Policies

1. Device Compliance Policies are Configured

A policy is only effective if you know it's being followed. Compliance policies in Intune enforce continuous monitoring across your fleet, ensuring every device meets minimum security standards.

From a Cyber Essentials perspective, this provides the **audit evidence** that controls like encryption, password requirements, and malware protection are not just configured but actually **active and enforced**. Noncompliant devices are flagged and can be blocked from accessing Microsoft 365 apps until remediated.

Licensing Considerations

- **Intune** (included in Microsoft 365 Business Premium, E3, and E5) is required to create and enforce compliance policies.

End-User Impact

- Users may receive warnings or prompts if their device doesn't meet requirements (e.g., encryption not enabled, password too short, OS outdated).
- In some cases, access to company apps may be restricted until compliance is restored (though the enforcement mechanism is covered in Conditional Access separately).
- With proper communication, this improves user accountability and keeps endpoints secure.

Implementation Steps

Step 1: Create a Compliance Policy

1. In the **Intune admin center → Devices → Compliance policies → Create policy**.
2. Platform: *Windows 10 and later*.
3. Name the policy (e.g., *Windows – Cyber Essentials Compliance*).

Step 2: Configure Compliance Settings
Cyber Essentials–aligned examples:

- **Require BitLocker encryption**: Enabled.
- **Require a password to unlock device**: Enabled (min length 8–12).
- **Block simple passwords**: Yes.
- **Mark jailbroken/rooted devices as noncompliant**: Enabled.
- **Minimum OS version**: Current supported Windows build.
- **Require Secure Boot and TPM**: Where supported.

Step 3: Assign Policy

- Assign to all managed device groups (e.g., *All Windows 10/11 Devices*).

Step 4: Monitor Compliance

- Go to **Intune → Reports → Device compliance**.
- Review compliant vs noncompliant devices.

2. Conditional Access Policy Blocks Sign-In for Noncompliant Devices

Cyber Essentials requires not only that compliance is monitored but that **noncompliant devices cannot access company data** until they are remediated. Without enforcement, users could continue working from devices that are missing patches, lack encryption, or fail password requirements.

Microsoft Entra Conditional Access provides this enforcement by linking Intune device compliance status to authentication. If a device is marked *noncompliant* by Intune, Conditional Access policies can **block sign-in** or restrict access until the device is brought back into compliance.

This ensures only **secure, managed devices** can connect to Microsoft 365 services — aligning with Cyber Essentials' principle of preventing insecure endpoints from introducing risk.

Licensing Considerations

- Requires **Microsoft Entra ID P1** or higher (included in Microsoft 365 Business Premium, E3, and E5).
- Intune compliance integration works with all device platforms managed through Intune.
- No Defender for Endpoint license is required for this baseline control (though it enhances compliance signals).

End-User Impact

- Users on compliant devices → normal access.
- Users on noncompliant devices → blocked from signing into Microsoft 365 until they fix the issue (e.g., enable BitLocker, update OS, set stronger password).
- This may cause short-term disruption, but drives accountability and keeps all endpoints within policy.

Implementation Steps

Step 1: Create Conditional Access Policy

1. In **Entra admin center → Protection → Conditional Access → Policies → New Policy**.
2. Name: *Block Noncompliant Devices*.
3. Assignments:
    - Users: *All users* (exclude break-glass accounts).
    - Cloud apps: *All cloud apps*.

Step 2: Define Conditions

- Under **Conditions → Device state**, include *All devices*.

Step 3: Configure Access Controls

- Under **Grant**, select:
    - **Require device to be marked as compliant**.
- Save and enable the policy.

Step 4: Test and Validate

- Test with a device missing BitLocker encryption (noncompliant in Intune).
- Attempt login → should be blocked.
- Monitor results under **Sign-in logs → Conditional Access** in Entra.

Step 5: Document for Cyber Essentials

- Provide screenshots of the policy.
- Show audit logs confirming noncompliant devices are denied access

3. Security Update Management

Cyber Essentials Definition: Any device that runs software can contain security flaws, known as vulnerabilities. Vulnerabilities are regularly discovered in all sorts of software. Once discovered, malicious individuals or groups move quickly to misuse (or 'exploit') vulnerabilities to attack computers and networks. Product vendors provide fixes for vulnerabilities identified in products that they still support, in the form of patches, security updates, registry fixes, scripts, configuration changes or any other mechanism prescribed by the vendor to fix a known vulnerability. These may be made available to customers immediately or on a regular release schedule (perhaps monthly).

Cyber Essentials requires organizations to ensure that all systems are updated quickly with the latest security patches. Attackers routinely exploit unpatched vulnerabilities — sometimes within hours of disclosure — making timely patching one of the most effective defenses.

In a Microsoft 365 environment, this is delivered through two complementary layers:

---

1. Intune & Windows Update for Business (WUfB)

- Centrally enforces Windows security updates and feature updates across all managed devices.
- Uses update rings to define how quickly devices receive patches (e.g., immediate for pilot users, staged rollout for wider fleet).
- Ensures Office/Microsoft 365 Apps are kept current with monthly security updates.
- Compliance policies in Intune can flag or block devices that are behind on updates.

---

2. Threat & Vulnerability Management (TVM) in Microsoft Defender

- Included in Microsoft Defender for Business (part of Microsoft 365 Business Premium) and Defender for Endpoint Plan 2.
- Continuously scans devices for missing security updates, misconfigurations, and vulnerable applications.

- Provides real-time exposure score and prioritized remediation actions, so IT knows which vulnerabilities are most urgent.
- Integrates directly with Intune to trigger remediation tasks (e.g., install missing patches, update outdated software).
- Goes beyond Windows — can detect risks in third-party applications and misconfigurations.

Policies

1. **Windows Update Rings Configured for Windows Devices**

Cyber Essentials requires that devices are kept up to date with the latest security patches. In Microsoft 365 environments, **Windows Update for Business (WUfB)**, managed through **Intune Update Rings**, is the primary way to enforce this.

Update Rings let you define **when and how updates are applied**:

- **Quality updates** (monthly security patches).
- **Feature updates** (new Windows versions).
- **Driver and Microsoft product updates**.

By enforcing Update Rings, you ensure every Windows device receives security patches automatically and on schedule — closing one of the biggest attack vectors (unpatched vulnerabilities).

Licensing Considerations

- Requires **Intune**, included in Microsoft 365 Business Premium, E3, and E5.
- Windows 10/11 Pro, Enterprise, and Education editions are supported.
- No additional licensing required for baseline update management.

End-User Impact

- Users may experience required restarts after updates are installed.
- You can configure **grace periods** and **active hours** to minimize disruption.

- Updates are installed automatically in the background, reducing user responsibility for patching.

Implementation Steps

Step 1: Create Update Ring Policy

1. In **Intune admin center → Devices → Update rings for Windows 10 and later → Create profile**.
2. Name the ring (e.g., *Windows – Monthly Security Updates*).

Step 2: Configure Update Settings

- **Servicing channel**: Semi-Annual Enterprise Channel (recommended for most).
- **Microsoft product updates**: Allow.
- **Driver updates**: Optional, depending on org policy.
- **Quality update deferral**: 0–7 days (recommended = 0 for fast security patching).
- **Feature update deferral**: 30–90 days (gives time to validate new versions).
- **Restart checks**:
    - Set active hours (e.g., 8 AM – 6 PM).
    - Grace period: 2–7 days for users to restart before forced reboot.

Step 3: Assign to Device Groups

- Assign the update ring policy to all managed Windows device groups.

Step 4: Monitor Update Status

- In Intune, go to **Reports → Windows update (preview)** to track compliance.
- Confirm devices are receiving and installing updates within your set timelines.

2. **Office/Microsoft 365 Apps** are kept current with monthly security updates

Cyber Essentials requires that all software in use is supported and patched with the latest security updates. Microsoft 365 Apps (Word, Excel, Outlook, Teams, etc.) are some of the most widely targeted applications for attacks, especially via malicious attachments and macros.

By keeping Microsoft 365 Apps updated on the **Monthly Enterprise Channel**, organizations ensure that the latest **security patches and feature hardening** are applied quickly. Running outdated Office builds leaves users exposed to exploits that are often weaponized within days of disclosure.

Licensing Considerations

- **Microsoft 365 Apps for Business** (included in Microsoft 365 Business Premium) and **Microsoft 365 Apps for Enterprise** (E3/E5) both support managed update channels.
- Intune can centrally manage update channels and versions for compliance.

End-User Impact

- Updates install automatically in the background with minimal disruption.
- Users may occasionally need to restart Office apps for updates to apply.
- Using the Monthly Enterprise Channel ensures predictable patching cadence (once per month, on Patch Tuesday).

Implementation Steps

Step 1: Configure Microsoft 365 Apps Update Policy in Intune

Use the steps outlined here for deploying the Microsoft 365 Apps as a Win32 app in Intune: How to Deploy Microsoft 365 Apps With Intune – Our Cloud Network

3. Devices shall be enrolled for Defender for Business or Defender for Endpoint

Cyber Essentials requires organizations to keep systems secure by applying updates and protecting against malware. But updates alone aren't enough — you also need **visibility into vulnerabilities** and assurance that patches are applied where needed.

Microsoft Defender for Business (included in Microsoft 365 Business Premium) and **Defender for Endpoint Plan 2 (E5)** include **Threat & Vulnerability Management (TVM)**, which continuously scans devices for:

- Missing security patches,
- Vulnerable applications,
- Misconfigurations that weaken security.

TVM integrates directly with Intune, allowing you to **remediate issues automatically** through configuration and update policies. This creates a feedback loop: detect → prioritize → fix → verify, which aligns directly with Cyber Essentials' requirement for ongoing patch and vulnerability management.

Licensing Considerations

- **Defender for Business** → included in Microsoft 365 Business Premium (up to 300 seats).
- **Defender for Endpoint Plan 2 (E5)** → includes full TVM capabilities.
- **Defender for Endpoint Plan 1 (E3)** → provides core AV/EDR but **does not include TVM**.

End-User Impact

- Transparent to end-users — Defender runs silently in the background.
- Users may occasionally see alerts if threats or exploits are blocked.
- Some legacy apps may be flagged as vulnerable, requiring IT review or exceptions.

Implementation Steps

Prerequisite: Devices Must Be Intune-Enrolled

- Devices need to be **managed by Intune** (Entra-joined, Hybrid-joined, or MDM-enrolled).

Step 1: Connect Intune to Defender

1. In **Intune admin center → Endpoint security → Microsoft Defender for Endpoint**, enable the connection.
2. Ensure "Connect Windows, macOS, iOS, and Android devices" = *Yes*.

Step 2: Deploy Defender Configuration Profile

1. Go to **Intune admin center → Endpoint security → Endpoint Detection and Response → Create policy**.

2. Platform: *Windows 10 and later*.
3. Profile: Endpoint Detection and Response
4. Configure:
    - Microsoft Defender for Endpoint client configuration package type: *Auto From Connector*
5. *Assign: All Devices (or scope for pilot to begin)*

Step 3: Verify Onboarding

- Devices should appear in the **Microsoft 365 Security Admin Center → Assets → Devices**
- Exposure score and TVM dashboards will start populating (Defender for Business or E5 only). (In the Security Admin Center>Endpoints>Vulnerability Management>Dashboard)

4. Applications Are Patched Within 14 Days of Critical or High-Risk Updates

Cyber Essentials (v3.2, April 2025) mandates that **security updates must be applied within 14 days** of release if they address vulnerabilities that:

- Are described by the vendor as **'critical'** or **'high risk'**.
- Have a **CVSS v3 base score of 7.0 or above**.
- Do not provide clear vulnerability details — in which case they must be treated as **high risk by default**.

This standard ensures that exploitable vulnerabilities cannot remain unpatched beyond a short window, reducing the risk of ransomware, malware, and privilege escalation attacks.

Licensing Considerations

- **Microsoft Intune** (included in Microsoft 365 Business Premium, E3, E5) enforces update policies for Windows and Microsoft 365 Apps.
- **Defender for Business** (Business Premium) and **Defender for Endpoint Plan 2 (E5)** provide **Threat & Vulnerability Management (TVM)** to surface CVSS severity ratings and prioritize remediation.

- Third-party apps not covered by Microsoft require either **Win32 app packaging** in Intune or a third-party patching solution.

End-User Impact

- Security updates are installed silently in the background.
- Users may occasionally need to restart apps or devices (e.g., Office or Windows reboots).
- Some line-of-business apps may be disrupted if updates are not tested quickly — but Cyber Essentials requires that **security patches take priority** over compatibility concerns.

Implementation Steps

Step 1: Detect Critical & High-Risk Updates

- In **Defender for Business / Endpoint TVM**, review vulnerability dashboards.
- TVM highlights updates with CVSS ≥ 7 and vendor-labeled "critical/high" patches.
- Treat all updates without disclosed severity as **high risk by default**.

Step 2: Remediate Within 14 Days

- Use Intune to deploy missing updates.
- Assign remediation tasks from Defender TVM directly to Intune for automatic enforcement.
- For third-party apps, package updates as Win32 apps or integrate with a patching vendor.

Step 3: Monitor Compliance

- Track update deployment via **Intune Update reports**.
- Monitor exposure score and unpatched vulnerability count in Defender TVM.
- Generate reports for audit evidence showing no critical/high-risk patches older than 14 days.

4. User Access Control

Cyber Essentials Definition: Every active user account in your organization facilitates access to devices and applications, and to sensitive business information. By making sure that only authorized 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 unauthorized access to other devices in the organization

Cyber Essentials requires that organizations carefully manage **who has access to systems, accounts, and data**. The principle is simple: users should only have the access they need to perform their job, and nothing more. This reduces the risk of accidental or malicious misuse of privileged accounts.

In Microsoft 365, **User Access Control** is enforced through:

- **Microsoft Entra ID** for centralized identity and role-based access.
- **Conditional Access policies** to limit sign-in contexts (location, device compliance, risk).
- **RBAC and Privileged Identity Management (PIM)** to control and audit administrator access.
- **MFA enforcement** to prevent unauthorized logins.

Policies

1. A user onboarding process is defined

Cyber Essentials requires organizations to demonstrate that **user accounts are created in a controlled and consistent manner**. Ad hoc account creation risks:

- Granting unnecessary access (violating least privilege).
- Skipping security measures like MFA, group assignment, or licensing.
- Leaving accounts without proper tracking, making later audits difficult.

A well-defined **onboarding process** ensures that each new user receives only the access they need, with the correct security controls applied from day one.

Licensing Considerations

- **Microsoft Entra ID** (all plans) provides identity lifecycle management, group-based access, and audit logs.
- **Microsoft Entra ID P1** (included in Microsoft 365 Business Premium, E3, E5) adds Conditional Access and dynamic groups for automation.
- **Intune** is used to automatically apply device and app protection policies during onboarding.

End-User Impact

- Users receive a consistent onboarding experience with the right apps, licenses, and access pre-configured.
- MFA enrollment is required at first sign-in, ensuring security is enabled immediately.
- Reduces friction compared to manually assigning permissions later.

Implementation Steps

Step 1: Define the Onboarding Workflow

- HR or IT request → IT creates account in **Entra ID**.
- Assign appropriate **Microsoft 365 license** (e.g., Business Premium, E3, E5).
- Place user in correct **security groups** (department, role, or least privilege).

Step 2: Automate with Group-Based Licensing & Policies

- Create **dynamic Entra groups** based on role, department, or attributes (e.g., "All Finance Users").
- Assign licenses and **Intune device compliance/app protection policies** automatically via group membership.

Step 3: Enforce MFA at First Sign-In

- Require MFA registration (Authenticator app) as part of onboarding.
- Document this as part of your Cyber Essentials evidence.

Step 4: Provision Devices & Apps

- Autopilot profiles applied for corporate devices.

- Office/Microsoft 365 apps automatically installed via Intune.
- Default Conditional Access policies applied (block legacy auth, require compliant device).

Step 5: Document the Process

- Maintain written onboarding steps in IT policy docs.
- Ensure HR and IT roles are clearly defined (who requests, who approves, who creates accounts).

2. A user offboarding process is defined

Cyber Essentials requires organizations to ensure that **access is revoked promptly when a user no longer needs it** — for example, when they leave the company, change roles, or no longer require certain systems.

Failing to offboard properly creates **orphaned accounts** that attackers can exploit, or that disgruntled former employees could use to access sensitive data. A consistent offboarding process ensures accounts are closed, access to devices and apps is removed, and company data is protected.

Licensing Considerations

- **Microsoft Entra ID** provides tools for account disablement, license removal, and access revocation.
- **Intune** enables remote device wipe or selective wipe for mobile devices.

End-User Impact

- Once offboarded, the user loses access to Microsoft 365 apps, email, and company resources.
- Devices may be remotely wiped or reset.
- Mailbox access can be reassigned to managers or archived for compliance.

Implementation Steps

Step 1: HR Notification

- HR triggers an offboarding request when an employee leaves.
- IT receives formal approval to disable access.

Step 2: Disable Account in Entra ID

- In the **Entra admin center → Users → Disable sign-in**.
- Revoke all sessions
- Remove account from all security groups and Conditional Access policies.

Step 3: Reclaim Licenses and Data

- Remove Microsoft 365 licenses to free up for reuse.
- Convert the user to a shared mailbox and provide delegated access as needed
- Archive or export OneDrive/SharePoint data before deletion.

Step 4: Secure Devices

- Use Intune to **retire** or **wipe** company-owned devices.
- For BYOD with app protection, perform a **selective wipe** to remove company data while preserving personal apps.

Step 5: Document and Audit

- Keep records of account disablement, device wipe, and data handover.
- Review Entra ID audit logs for evidence that access was revoked.

3. Dormant accounts are disabled after 45 days

Cyber Essentials requires that **unused accounts are removed or disabled** to prevent them from being exploited. Dormant accounts are particularly dangerous because:

- They often remain unnoticed by IT and unmonitored by users.
- Attackers target them for stealthy access since no one expects activity.
- They may still hold licenses, permissions, or sensitive data access.

By disabling accounts that have been inactive for 45 days, organizations reduce the attack surface and comply with Cyber Essentials' mandate to remove unnecessary access.

Licensing Considerations

- **Microsoft Entra ID** (all tiers) supports monitoring last sign-in dates and disabling accounts.
- **Entra ID P1/P2** (included in Microsoft 365 Business Premium, E3, and E5) allows automation with Conditional Access and Identity Protection.
- **Intune** integrates with Entra to remove app and device access when accounts are disabled.

End-User Impact

- Users who legitimately haven't logged in for 45+ days will be blocked until IT re-enables their account.
- This may affect seasonal workers, contractors, or employees on extended leave — IT should have an exception process.

Implementation Steps

1. **Monitor Account Activity with Azure AD Sign-In Logs:**
    - **Go to the Entra admin center (Entra Admin Center).**
    - **Navigate to Sign-ins under Monitoring to identify accounts with no recent activity over the last 45 days.**
2. **Create Automation to Disable Dormant Accounts:**
    - **Review dormant users**
        - **Run this first to verify you're targeting the correct accounts:**
        - **$threshold = (Get-Date).AddDays(-45)**

          Get-MgUser -All -Property "Id,AccountEnabled,SignInActivity,DisplayName,UserPrincipalName"
          | Where-Object {
          $_.AccountEnabled -eq $true -and
          $_.SignInActivity.LastSignInDateTime -and

[DateTime]$_.SignInActivity.LastSignInDateTime -lt $threshold
}
| Select-Object
DisplayName,UserPrincipalName,@{Name='LastSignIn';Expressi
on={$_.SignInActivity.LastSignInDateTime}}

2. Disable dormant users

- **Open PowerShell as an administrator, then run:**
- **$threshold = (Get-Date).AddDays(-45)**

Get-MgUser -All -Property "Id,AccountEnabled,SignInActivity"
| Where-Object {
$_.AccountEnabled -eq $true -and
$_.SignInActivity.LastSignInDateTime -and
[DateTime]$_.SignInActivity.LastSignInDateTime -lt $threshold
}
| ForEach-Object {
Update-MgUser -UserId $_.Id -AccountEnabled:$false
}

4. Users are authenticated with unique credentials

Cyber Essentials requires that **all users are authenticated with unique credentials**. Shared accounts are a major risk because:

- They make it impossible to trace actions back to an individual user.
- Credentials are often written down or passed around insecurely.
- They bypass accountability and auditability, which are critical for security investigations.

Using **unique accounts with strong authentication** ensures that each user can be identified, their activity can be logged, and access can be revoked promptly if needed. If accounts are cloud-only, password complexity requirements are set by Entra ID.

Licensing Considerations

- **Microsoft Entra ID** (all tiers) supports unique user identities and centralized password policy enforcement.

- Hybrid environments with on-prem Active Directory require Group Policy / AD password policies unless Entra is the source of authority.

End-User Impact

- Each user must log in with their own Microsoft 365 account credentials.
- Shared logins (e.g., “info@company.com” used by multiple staff) should be replaced with **shared mailboxes** or **delegated access** while still using unique user identities.
- Users will be required to follow defined password complexity rules or, ideally, enroll in passwordless authentication methods (e.g., Windows Hello for Business, FIDO2 keys).

Implementation Steps

Step 1: Eliminate Shared Accounts

- Replace any shared credentials with **individual Entra ID accounts**.
- If multiple staff need access to the same mailbox or resource, use:
    - **Shared mailbox with delegated access** (Exchange Online).

Step 2: Enforce Password Complexity in Entra ID

- In a cloud-only environment:
    - You are not able to change the password complexity if cloud-only: Self-service password reset policies - Microsoft Entra ID | Microsoft Learn
- In a **hybrid environment**, enforce password policies via **Active Directory Group Policy Objects (GPOs)**.

Step 3: Monitor & Audit

- Use **Entra sign-in logs** to confirm that each login maps to a unique account.
- Regularly review to ensure no generic or shared accounts exist.

5. Passwords are set to not expire

Historically, many organizations enforced **regular password expiry** (e.g., every 60 or 90 days). However, this often led to weaker security because users chose simple, predictable passwords or wrote them down.

By disabling arbitrary password expiry, organizations reduce user frustration while **improving real security**.

Licensing Considerations

- **Microsoft Entra ID** (all tiers) supports disabling password expiration policies.

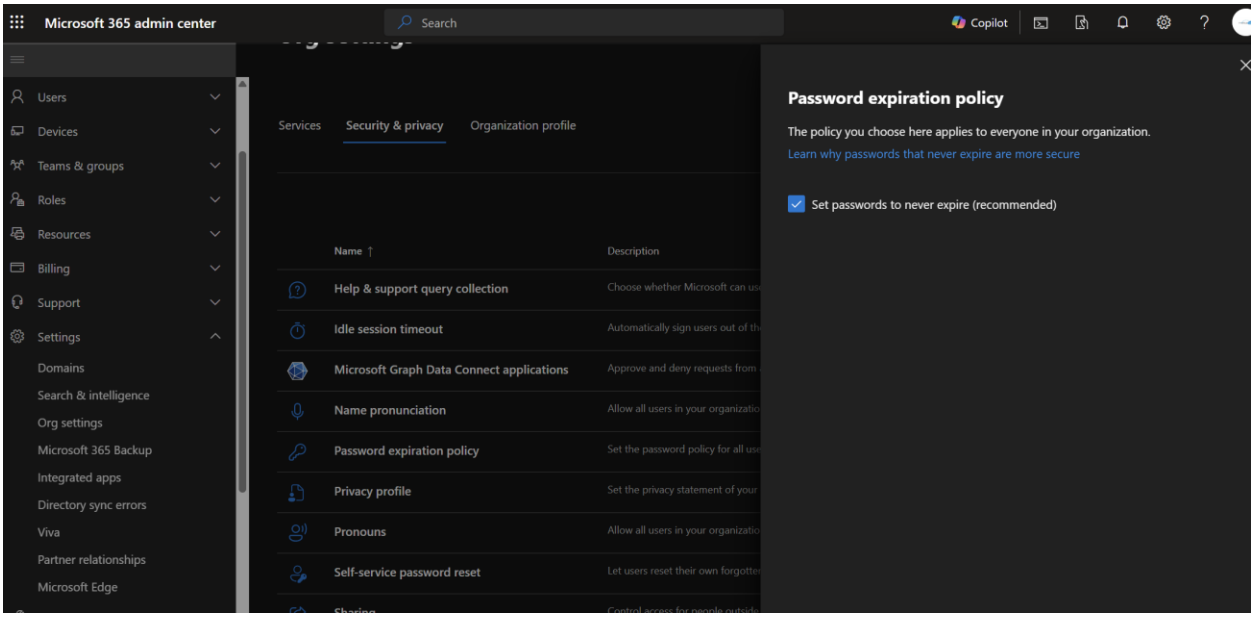
End-User Impact

- Users are no longer forced to change passwords every few months.
- Instead, they must create **stronger, longer, unique passwords** at account creation.
- Password resets occur only if there is evidence of compromise, reducing disruption.

Implementation Steps

Step 1: Configure Entra Password Expiry Policy

1. In **Microsoft Admin center → Settings → Org Settings → Security & Privacy -> Password Expiration Policy**
2. Set:
    - **Password expiration policy** = *Never expire*.



6. Custom Lockout Requirements are set in Entra ID (duplicate of Secure Configuration recommendation)

Cyber Essentials requires that accounts are locked out after a certain number of failed sign-in attempts to defend against brute-force and credential stuffing attacks. Without this, attackers can attempt unlimited password guesses until they succeed.

In Microsoft 365, these protections are configured in **Microsoft Entra ID Password Protection**. With custom smart lockout, administrators define the **threshold** (number of failed attempts) and the **lockout duration**, balancing security with user convenience.

Licensing Considerations

- **Available in all Microsoft Entra ID tiers**, including the free version.
- No additional license is needed for configuring smart lockout or password protection.
- For hybrid environments, password protection can also extend to **on-prem Active Directory**, but requires Entra Connect integration.

End-User Impact

- Users who repeatedly mistype their password may be temporarily locked out (e.g., 10 attempts → 1 minute lockout).

- Helps prevent account compromise but can be disruptive if thresholds are set too aggressively.
- Self-service password reset (SSPR) or MFA helps users recover quickly if legitimately locked out.

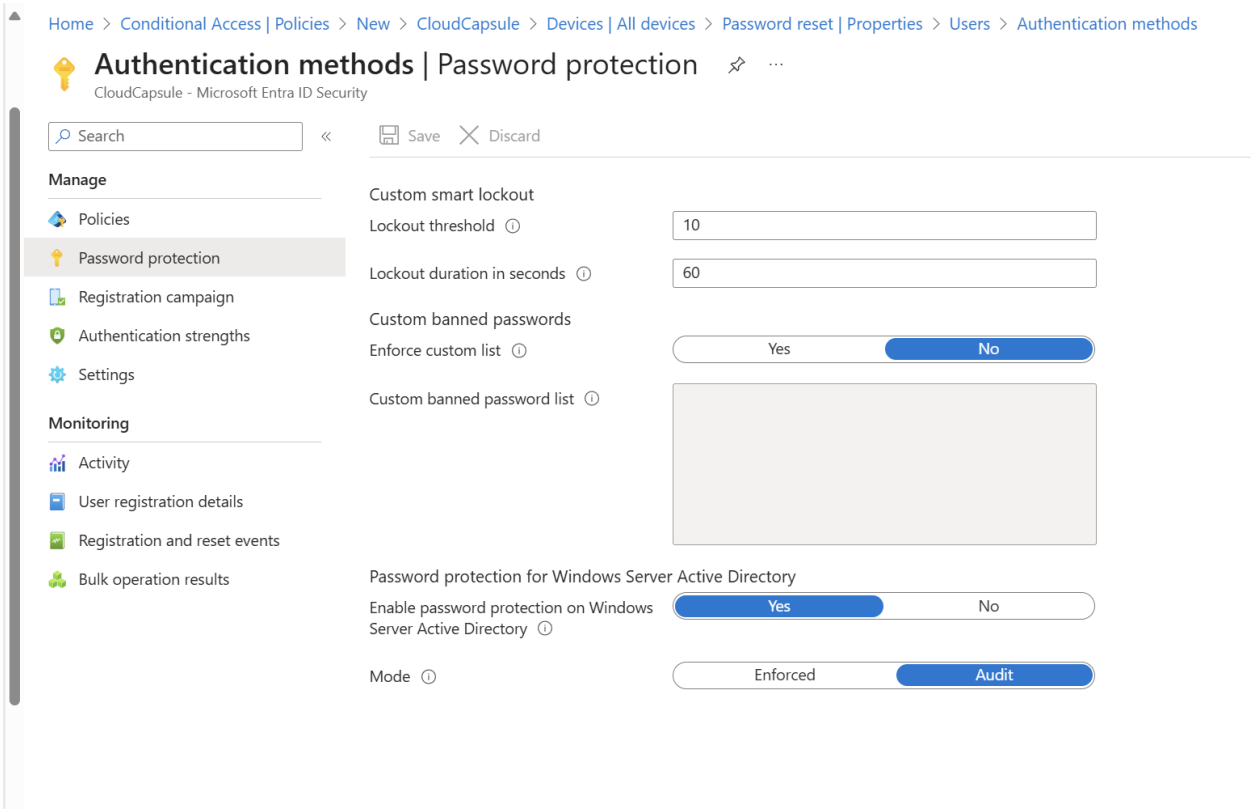
Implementation Steps

Step 1: Navigate to Password Protection

3. Go to **Entra admin center → Protection → Authentication methods → Password protection**.

Step 2: Configure Custom Smart Lockout

- **Lockout threshold**: Recommended = *10 failed attempts*.
- **Lockout duration**: Recommended = *60 seconds (1 min)*.
- This provides security against brute force without overly disrupting legitimate users.



7. The custom banned password list is leveraged

Cyber Essentials requires organizations to prevent the use of weak or easily guessable passwords. Attackers rely on password spraying (using common passwords like Password123 or Welcome1) and credential stuffing attacks with leaked credentials.

Microsoft Entra ID includes a **banned password list** feature that blocks the use of common, compromised, or predictable passwords. By extending this with a **custom banned password list**, organizations can also block business-specific terms (e.g., company name, product names, local sports teams) that users might otherwise choose.

This enforces **unique, strong, and resilient credentials**, reducing the risk of account compromise.

Licensing Considerations

- **Custom banned password lists** require **Microsoft Entra ID Premium P1 or P2** (included in Microsoft 365 Business Premium, E3, and E5).
- The **default banned password list** (maintained by Microsoft) is included in all Entra ID editions.

End-User Impact

- Users attempting to set weak or company-themed passwords will be prevented from doing so.
- They will need to create more secure passwords at first setup or when changing a password.
- Some frustration may occur, but this ensures compliance with Cyber Essentials' password strength requirements.

Implementation Steps

Step 1: Enable Password Protection in Entra

1. In **Entra admin center → Security → Authentication methods → Password protection**.
2. Ensure **Password protection** is *Enabled*.

3. Confirm that the **global banned password list** is enforced.

Step 2: Configure Custom Banned Passwords

- Add up to **1,000 custom banned words** relevant to your organization.
- Examples to include:
    - Company name(s) and variations.
    - Location-specific terms (e.g., “London123”).
    - Common product/service names.
    - Seasonal words like “Summer2025” or “Christmas1”.

Step 3: Apply Policy to Users

- Under **Mode**, select *Enforced*.
- Assign policy to *All users* for consistent enforcement.

Step 4: Test and Monitor

- Attempt to reset a password using a blocked word (e.g., companyname2025).
- Verify that Entra ID prevents its use.
- Audit logs in Entra will show blocked password attempts.

8. MFA is enforced for all users

Passwords alone are no longer enough to protect accounts. Cyber Essentials requires strong authentication for all users, and **Multi-Factor Authentication (MFA)** is one of the most effective defenses against account compromise.

MFA ensures that even if a password is guessed, stolen, or reused from a breach, attackers cannot gain access without a second factor. In Microsoft 365, MFA should be enforced across **all accounts** — standard users, administrators, and guests.

Licensing Considerations

- **All Entra ID tiers** (including free) support MFA via **Per-User settings** or **Security Defaults**.

- **Microsoft Entra ID P1/P2** (included in Microsoft 365 Business Premium, E3, and E5) enables **Conditional Access policies** for granular MFA enforcement.

End-User Impact

- Users must register for MFA during onboarding (typically via Microsoft Authenticator app).
- MFA prompts appear during new or risky sign-ins, or as enforced by policy.
- Some user training may be required for mobile authenticator apps, hardware tokens, or security keys.

Implementation Options

Option 1: Per-User MFA (Basic, Legacy Method)

1. Go to **Entra admin center → Users → Per-user MFA**.
2. Select individual users or groups → set to *Enforced*.
3. Users will be prompted to register and use MFA on next sign-in.

Option 2: Security Defaults (Baseline MFA)

1. In **Entra admin center → Properties → Manage Security defaults**.
2. Enable Security Defaults.
3. MFA is required for all users, and legacy authentication is blocked.

Option 3: Conditional Access (Granular MFA – Recommended)

1. In **Entra admin center → Security → Conditional Access → New policy**.
2. Assignments:
    - Users: *All users* (exclude **break-glass admin accounts**).
    - Cloud apps: *All cloud apps*.
3. Controls:

    - Under **Grant**, select *Require multi-factor authentication*.
4. Enable policy

9. Legacy Authentication is Blocked

Legacy authentication (basic auth protocols such as POP, IMAP, SMTP AUTH, and older Office client connections) does **not support MFA** and is one of the most common attack vectors for account compromise. Attackers routinely use password spraying and brute force attacks against these endpoints.

Cyber Essentials requires that organizations enforce **strong authentication methods** and remove insecure ones. Blocking legacy authentication ensures that all sign-ins use modern protocols that support MFA and Conditional Access.

Licensing Considerations

- **Microsoft Entra ID** (all tiers) allows legacy authentication blocking.
- **Microsoft Entra ID P1/P2** (Business Premium, E3, E5) adds Conditional Access for targeted enforcement and reporting.

End-User Impact

- Users relying on legacy clients (older versions of Outlook, or mobile mail apps not using modern auth) will no longer be able to connect.
- Some third-party apps and devices (e.g., multifunction printers, old SMTP relay setups) may require reconfiguration to use modern authentication or an app password (not recommended for CE compliance).
- Modern versions of Outlook, Teams, and the native iOS/Android mail apps all support modern authentication.

Implementation Steps

Step 1: Audit Legacy Authentication Usage

- In **Entra admin center → Sign-in logs**, filter for "Client app = Legacy Authentication."

- Review which accounts are still using legacy protocols.

Step 2: Block Legacy Authentication via Conditional Access (Recommended)

1. In **Entra admin center → Security → Conditional Access → New policy**.
2. Assignments:
    - Users: *All users* (exclude **break-glass accounts**).
    - Cloud apps: *All cloud apps*.
    - Conditions → Client apps: *Select only legacy authentication clients*.
3. Access controls:
    - **Block access**.
4. Enable policy.

Step 3: Disable Protocols in Exchange Online

- Go to **Exchange admin center → Settings → Authentication**.
- Disable protocols like **POP3, IMAP4, SMTP AUTH** unless absolutely required.

10. Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.

Cyber Essentials requires that administrator accounts are used **only for administrative tasks**. Privileged accounts are high-value targets — if compromised, they can give attackers full control over systems and data.

Using a single account for both everyday work (email, Teams, web browsing) and privileged tasks dramatically increases risk. A phishing email opened in Outlook, for example, could compromise domain admin rights if that same account has elevated privileges.

By assigning **dedicated privileged user accounts** (separate from standard user accounts), organizations:

- Contain exposure to everyday risks like phishing or malware.
- Ensure admin activity is logged and auditable.
- Reduce the attack surface by limiting when and how elevated accounts are used.

Licensing Considerations

- **Microsoft Entra ID** (all tiers) supports role-based access control (RBAC) to assign admin roles.

End-User Impact

- Admins must use **two accounts**:
    - A **standard user account** for day-to-day activities (email, Teams, SharePoint).
    - A **privileged admin account** for administrative duties only.
- Inconvenience may occur when switching between accounts, but this separation greatly reduces compromise risk.

Implementation Steps

Step 1: Create Dedicated Admin Accounts

- In **Entra admin center → Users → New user**, create accounts named consistently (e.g., admin.firstname.lastname@company.com).
- Do not assign email or Teams licenses to admin accounts (to prevent everyday use).

Step 2: Assign Admin Roles via Entra RBAC

- Navigate to **Entra admin center → Roles & administrators**.
- Assign roles such as *Global Administrator, Security Administrator, Exchange Administrator* to the admin accounts — not personal accounts.
- Follow the principle of least privilege (assign only the rights needed).

Step 3: Monitor and Audit Admin Activity

- Use **Entra sign-in logs** to monitor privileged account logins.
- Configure alerts for suspicious or high-risk admin activity.

Step 5: Document Admin Account Policy

- In your IT security policy, clearly state:

- Admin accounts must not be used for email or day-to-day tasks.
- Admin accounts are for privileged actions only.

16. Passwordless authentication is leveraged

Cyber Essentials requires organizations to strengthen user authentication beyond passwords. Even with MFA, passwords remain a weak link — they can be phished, guessed, or reused from breaches.

Passwordless authentication removes this dependency, replacing passwords with secure methods based on **something you have (device, token, passkey)** or **something you are (biometric)**.

In Microsoft 365, passwordless can be implemented using:

- **Windows Hello for Business** → PIN or biometric tied to the device's TPM.
- **FIDO2 security keys** → physical hardware keys for phishing-resistant sign-in.
- **Microsoft Authenticator app passwordless sign-in** → app-based approval with number matching.
- **Passkeys** → cross-platform, phishing-resistant credentials based on the FIDO2 standard, allowing users to authenticate with built-in device biometrics (like Face ID, Touch ID, or Windows Hello) across supported browsers and devices.

Passkeys are particularly powerful as they:

- Work across devices and ecosystems (Windows, iOS, Android).
- Are resistant to phishing since the private key never leaves the device.
- Provide a user-friendly login experience without requiring users to remember complex credentials.

Licensing Considerations

- **Microsoft Entra ID Free** supports passwordless via Microsoft Authenticator app and passkeys.
- **Microsoft Entra ID P1/P2** (Business Premium, E3, E5) adds Conditional Access enforcement and advanced policy controls.

- **Windows Hello for Business** is included with Windows 10/11 Pro and Enterprise, managed through Intune.
- **Passkeys** require modern browsers and OS support but do not need extra licensing.

End-User Impact

- Users log in with biometrics, device PINs, or a passkey instead of remembering a password.
- Authentication becomes faster, simpler, and more secure.
- Initial setup requires enrollment in Microsoft Authenticator, Windows Hello, FIDO2 key, or passkey registration.

Implementation Steps

Step 1: Enable Passwordless Authentication in Entra ID

1. In **Entra admin center → Security → Authentication methods → Policies**.
2. Enable and assign:
    - **Microsoft Authenticator app** (for passwordless sign-in).
    - **Windows Hello for Business**.
    - **FIDO2 security keys**.
    - **Passkeys** (Entra now supports passkey-based sign-in for supported devices).

Step 2: Configure Intune for Windows Hello for Business

- In **Intune → Devices → Configuration profiles**, create a profile:
    - Platform: *Windows 10/11*.
    - Profile type: *Identity Protection*.
    - Enforce Hello for Business with PIN and biometric requirements.

Step 3: Register and Distribute Methods

- Encourage users to register passkeys on personal devices with biometric support.

- Provide FIDO2 keys for privileged users or environments requiring phishing-resistant hardware-based sign-in.
- Train users on using Microsoft Authenticator as a backup option.

Step 4: Enforce with Conditional Access

- In **Conditional Access → Grant controls**, require strong authentication methods (Authenticator, passkeys, FIDO2, Windows Hello).
- Block legacy password-only login flows.

Step 5: Monitor and Audit Adoption

- Use **Entra → Authentication methods activity** to track passwordless adoption.
- Report passkey registrations and usage as Cyber Essentials evidence.

5. Malware Protection

Cyber Essentials requires organizations to **minimize the risk of malware execution** and prevent unauthorized applications from running without user approval. Attackers often abuse common apps like Office, email clients, and web browsers to launch malicious code.

1. Microsoft Defender Attack Surface Reduction (ASR) rules

Microsoft Defender Attack Surface Reduction (ASR) rules directly address this by blocking or restricting high-risk behaviors at the endpoint level. For example:

- Preventing Office apps from launching child processes (e.g., Word starting PowerShell).
- Blocking executable content from email and webmail.
- Using SmartScreen to block untrusted downloads.

This aligns with the Cyber Essentials requirement to **disable auto-run features** and to stop files from executing without explicit user authorization.

Licensing Considerations

- ASR rules require **Microsoft Defender Antivirus** (built into Windows 10/11).
- Centralized management and reporting require **Microsoft Intune**.
- Visibility and advanced reporting are available with **Defender for Endpoint Plan 1 or 2** (included in Microsoft 365 Business Premium and E5).

End-User Impact

- End-users may see some actions blocked, such as:
    - Macros attempting to run hidden scripts.
    - Files downloaded via Outlook or Edge being blocked.
- Some legitimate workflows (e.g., certain Excel macros or line-of-business apps) may require exclusions.
- Generally low friction if deployed first in **Audit Mode** before enforcement.

Implementation Steps

Step 1: Create an ASR Policy

1. In **Intune admin center → Endpoint security → Attack surface reduction → Create policy**.
2. Platform: *Windows 10 and later*.
3. Profile type: *Attack surface reduction rules*.

Step 2: Configure Core Rules (Recommended for Cyber Essentials)
Enable these high-value rules:

- Block executable content from email and webmail.
- Block Office applications from creating child processes.
- Block credential stealing from LSASS.
- Block persistence through WMI event subscription.
- Use advanced protection against ransomware (Controlled Folder Access).
- Use Microsoft Defender SmartScreen to block unverified downloads.

Step 3: Start in Audit Mode

- Set rules to **Audit only** initially.
- Review logs in **Defender Security Center** or Intune reports.
- Identify false positives before moving to enforcement.

Step 4: Switch to Enforce Mode

- After validation, change rules to **Block** mode for production rollout.

2. Application Control for Business

Why It Matters

Cyber Essentials requires organizations to ensure that **only approved, trusted applications can run on devices**. One of the most common ways malware spreads is by tricking users into downloading and running unapproved or malicious executables.

Microsoft App Control for Business (formerly WDAC — Windows Defender Application Control) enforces **application allowlisting** at the OS level. Instead of trying to block known bad apps, it ensures only **signed, approved, and trusted code** can execute.

This provides protection against:

- Malware and ransomware payloads delivered via phishing or downloads.
- Unsanctioned software that could introduce vulnerabilities.
- Zero-day threats, since unrecognized code is simply not allowed to run.

Licensing Considerations

- **Windows 10/11 Enterprise** includes the full App Control for Business feature set.
- **Windows 10/11 Pro** supports a limited subset.
- Management and deployment are handled through **Microsoft Intune** or **Group Policy**.
- Included in **Microsoft 365 Business Premium, E3, and E5** via Intune integration.

End-User Impact

- Users can only run applications that are trusted by the organization (signed by Microsoft, OEMs, or explicitly allowed by policy).
- Attempting to install unapproved apps will be blocked.
- IT must maintain an approved list of applications — false positives are possible if legitimate apps are not added to the allowlist.

Implementation Steps

Step 1: Plan Your Allowlisting Policy

- Decide whether to start with a **default Microsoft-recommended block policy** or a **custom allowlist**.
- Consider piloting in audit mode first to identify apps in use.

Step 2: Create App Control Policy in Intune

1. In **Intune admin center → Endpoint security → App control for Business → Create policy**.
2. Platform: *Windows 10 and later*.
3. Profile type: *Application control*.
4. Configure:
    - Allow only apps signed by Microsoft and the OEM.
    - Optionally add line-of-business apps or trusted third-party vendors.

Step 3: Deploy in Audit Mode (Optional)

- First roll out in **Audit mode** to log violations without blocking.
- Use Intune reporting to review which apps are in use and refine the allowlist.

Step 4: Enforce the Policy

- Switch policy to **Enforce mode**.
- Block unsigned, unknown, or unapproved apps from running.

Step 5: Monitor and Maintain

- Regularly review logs in **Microsoft Defender Security Center** and Intune reports.
- Update allowlists when deploying new approved apps.