



# Essential Eight Configuration & Validation Report

Date: 06 Sep 2025

User ID/Session ID: Heyhey-Application-  
Control-Screenshot3-AC-01-01

## 1. Executive Summary

This EC&V scan analyses the evidence uploaded against the Essential 8 mitigation strategies.

It provides a maturity level estimate per detected strategy, recommendations for improvement, and an appendix of the original evidence for transparency.

Note: This is not a full audit. Results are based only on the uploaded evidence and may not reflect your complete security posture.

## 2. Definitions

### Maturity Levels:

- ✓ **Level 0 (Initial):** No or ad-hoc implementation
- ✓ **Level 1 (Baseline):** All baseline criteria fully met
- ✓ **Level 2 (Maturity):** Baseline + advanced criteria fully met
- ✓ **Level 3 (Target):** Level 2 + continuous validation and automated enforcement

## 3. Detailed Findings & Recommendations

### Summary Table:

Strategy	Test ID	Sub-Strategy	Detected Level	Target Level	Pass/Fail	Priority
Application Control	ML1-AC-01	Executables Files must be blocked	Level 1	Level 3	Pass	High

**Strategy:** Application Control // **Test ID:** {Test\_id} // **Sub-Strategy:** Executables Files must be blocked

- **Description:**
- **Detected Maturity Level:** 1
- **Evidence Extract:**  
“executable files; re:\bblock(?:ed|ing)?\b”
- **Recommendations:**  
  
(1) Ensure executable files (EXE and COM files) cannot be run from user or temp folders by standard users (2) Use AppLocker or Windows Defender Application Control rules

## 4. Confidence & Limitations

### OCR Match Confidence:

- Executables Files must be blocked – %

### Limitations:

- Evidence may be incomplete
- Some configurations require manual verification

## 5. Appendix – Uploaded Evidence

File: Screenshot3 AC-01.jpeg

[Home](#) > [Endpoint security](#) | [Attack surface reduction](#) >

### Create profile ...

Attack Surface Reduction Rules

✓ Basics   **2 Configuration settings**   ③ Scope tags   ④ Assignments   ⑤ Review + create

#### ^ Defender

Block execution of potentially obfuscated scripts ①

Block ▾

ASR Only Per Rule Exclusions ①

☒ Not configured

Block Win32 API calls from Office macros ①

Block ▾

ASR Only Per Rule Exclusions ①

☒ Not configured

Block executable files from running unless they meet a prevalence, age, or trusted list criterion ①

Block ▾

ASR Only Per Rule Exclusions ①

☒ Not configured

Block Office communication application from creating child processes ①

Block ▾