CIS Benchmark Implementation Report

1. Overview of CIS benchmark

The Center for Internet Security (CIS) Benchmark is a set of best practices and recommendations designed to secure IT systems, networks, and devices. For Windows Server 2022, the CIS Benchmark focuses on hardening the server environment by securing system configurations, reducing vulnerabilities, and ensuring compliance with industry standards. By aligning with these benchmarks, organizations can mitigate security risks and ensure system integrity, protecting sensitive data from external and internal threats.

Importance of CIS

• Security Best Practices: CIS provides globally recognized guidelines to secure IT systems, reducing vulnerabilities.

• Configuration Hardening: Helps organizations strengthen default system configurations to minimize attack surfaces.

• Compliance: Supports alignment with industry standards and regulatory requirements, ensuring organizations meet cybersecurity audits.

• Risk Mitigation: Reduces exposure to common threats, improving overall security posture.

• Operational Efficiency: Provides a clear framework for managing and maintaining secure environments.

• Cyber Resilience: Enhances protection against evolving cyber threats, improving data security and system integrity.

• Community-driven: Developed through collaboration with security experts and professionals worldwide.

2. Comparison of Existing System's Account Policies vs. CIS Benchmark Recommendations

Account Policy Areas Covered:

• Password Policies: Complexity, length, expiration, and history.
• Account Lockout Policies

Password Policy

Policy area	Before changes	After changes (CIS recommendation)
1. Enforce Password History	0 passwords remembered	24 passwords remembered
2. Maximum Password Age	42 days	60 days
3. Minimum Password Age	0 days	1 days
4. Minimum Password Length	0 characters	14 characters
5. Minimum Password Length (Audit)	Not defined	Not defined
6. Password Must Meet Complexity Requirements	Disabled	Enabled
7. Relax minimum password length limits	Not defined	Not defined
8. Store Passwords Using Reversible Encryption	Disabled	Disabled

Account Lockout Policy

Policy Area	Before changes	After changes (CIS recommendation)
1.Account lockout duration	10 minutes	15 minutes
2.Account lockout Threshold	10 invalid logon attempts	5 invalid logon attempts
3.Reset Account Lockout Counter After	10 minutes	15 minutes

3. Changes Made to Align with CIS Benchmark

The following specific changes were made to align the system with the CIS Benchmark:

- Password Policy Changes:

    a. Increased the minimum password length to 14 characters.
    b. Set password expiration to 60 days.
    c. Enabled password complexity requirements.
    d. Set minimum password age to 1 day.

- Account Lockout Policy:

    a. Configured account lockout threshold to 5 failed login attempts.
    b. Set lockout duration to 15 minutes after threshold is reached.
    c. set Reset Account Lockout Counter After to 15 minutes

4. Challenges Encountered

1. Policy Conflicts:

Some existing policies were set according to organizational needs, and modifying them to match CIS recommendations caused initial conflicts with other security software, particularly around password expiry.

2. User Experience Impact:

Increasing password complexity and reducing password expiry durations led to complaints from users regarding the frequency of required password changes.

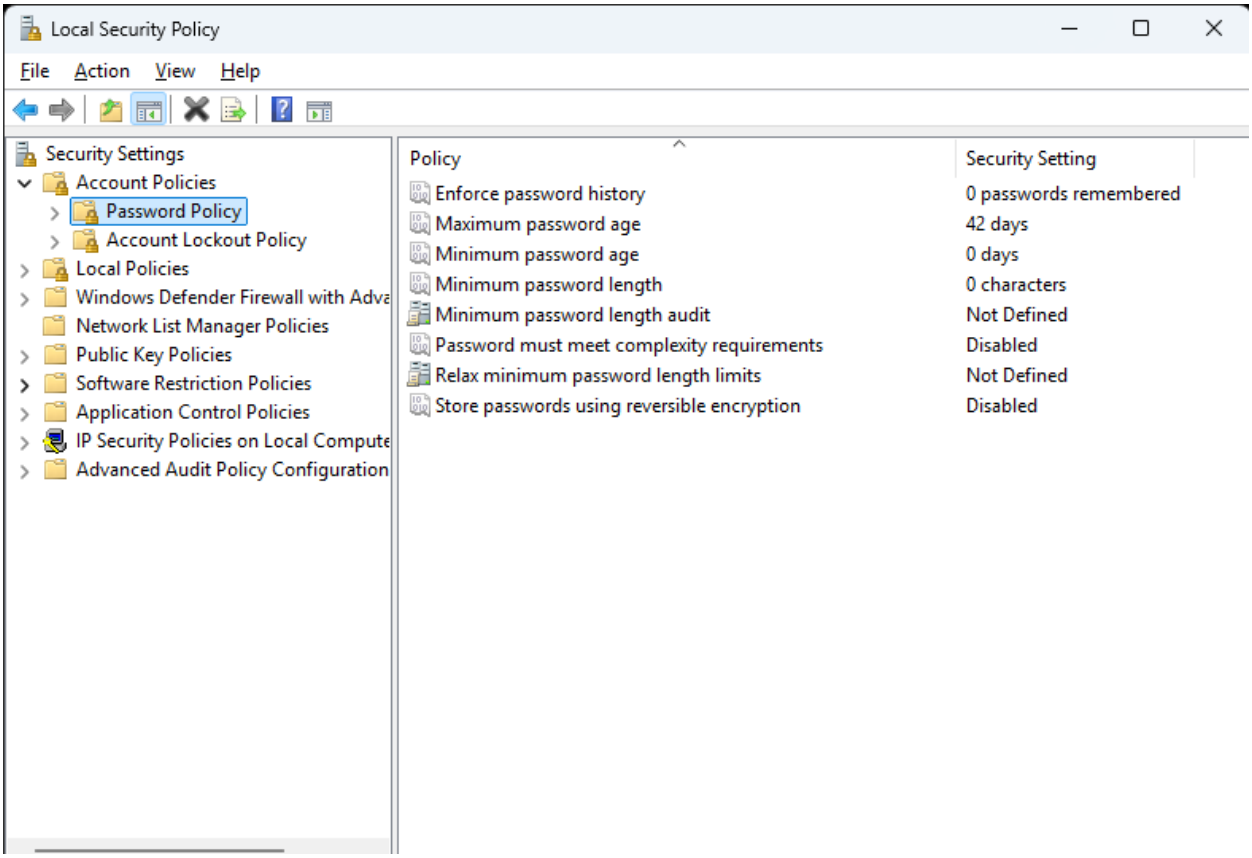
3. Tool Compatibility:

Some third-party applications initially faced issues due to tighter lockout thresholds, requiring policy adjustments to allow certain services or accounts to function properly.

5. Evidence of Policy Changes

Before changes:

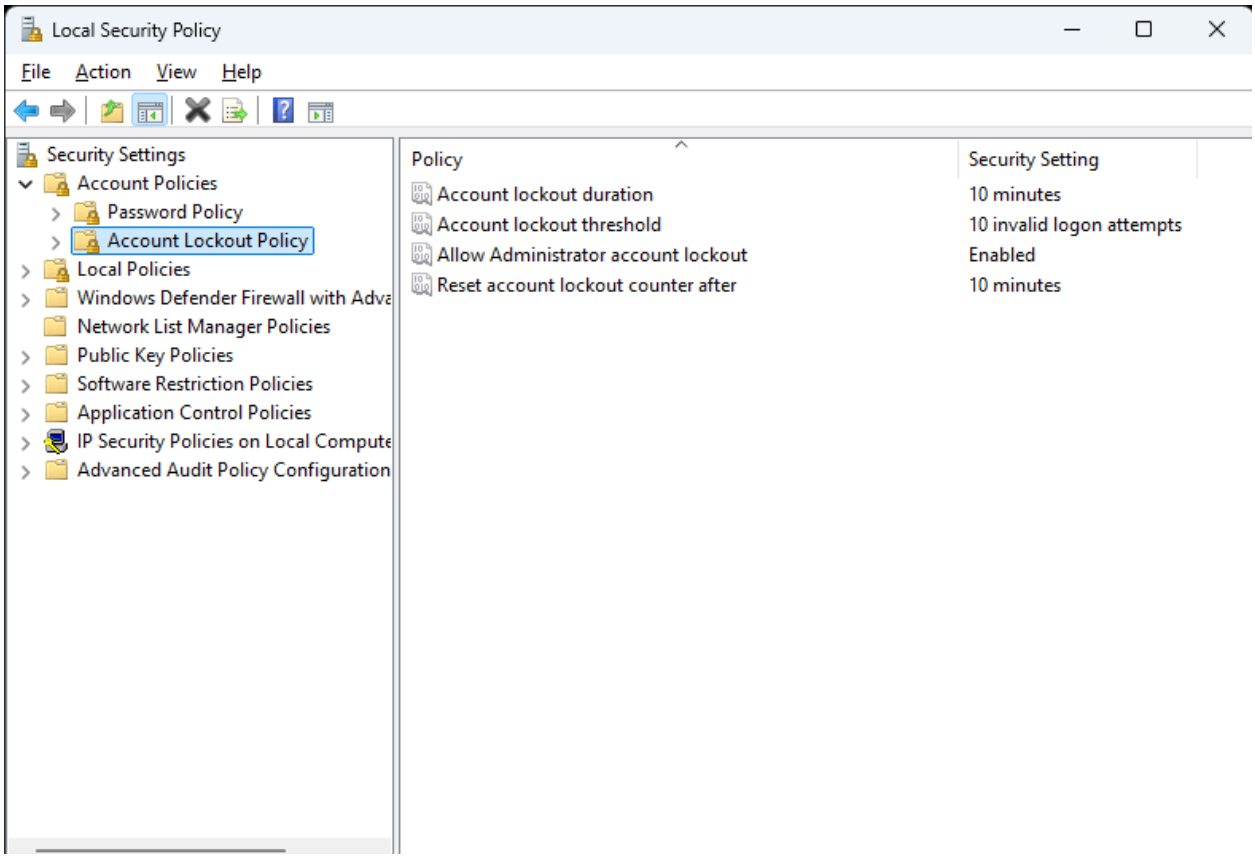
- Password policy
  a. Password History: 0 passwords remembered
  b. Minimum password age:0 days
  c. Maximum password age:42 days
  d. Minimum Password Length: 0 characters
  e. Password Must Meet Complexity Requirements: disabled



• Account Lockout Policy:

  a. Account lockout duration: 10 minutes

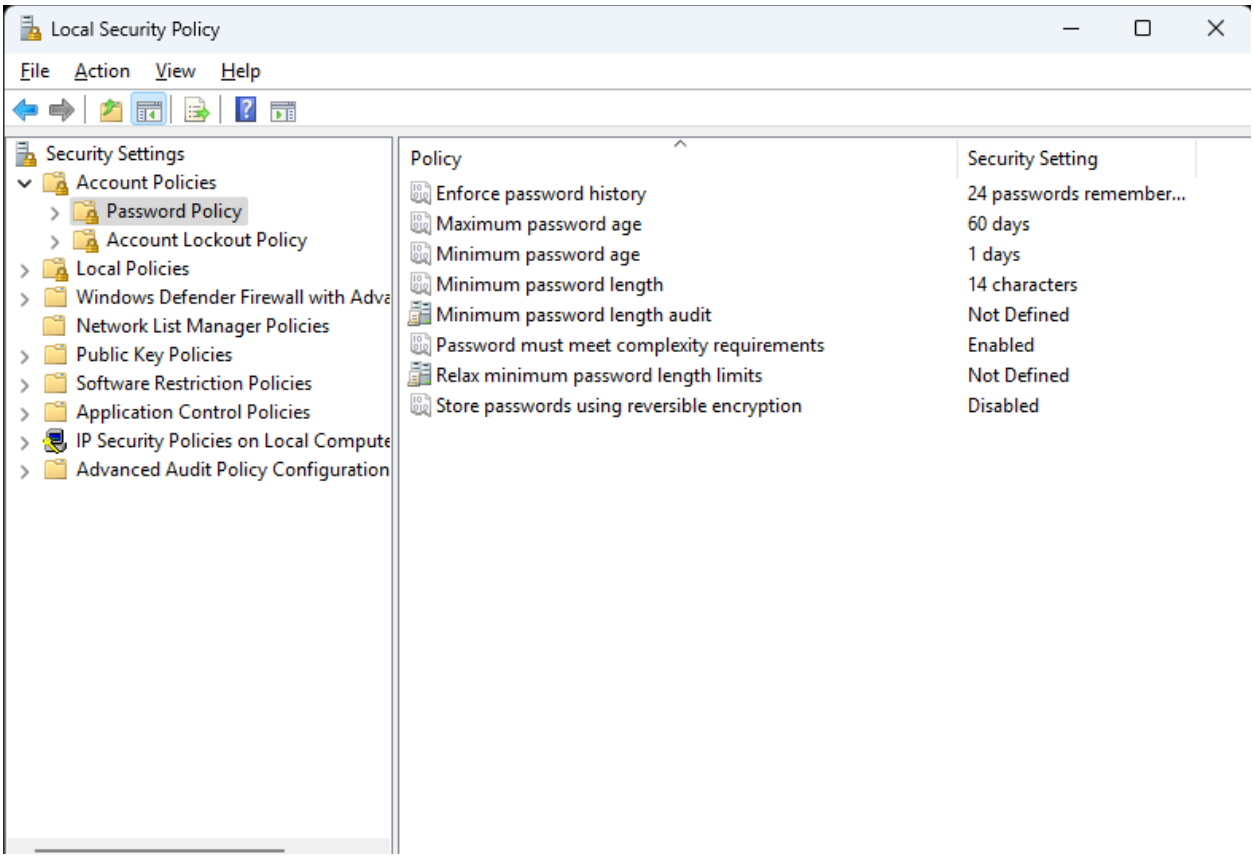
b. Account lockout Threshold: 10 invalid logon attempts
c. Reset Account Lockout Counter After: 10 minutes



After changes:

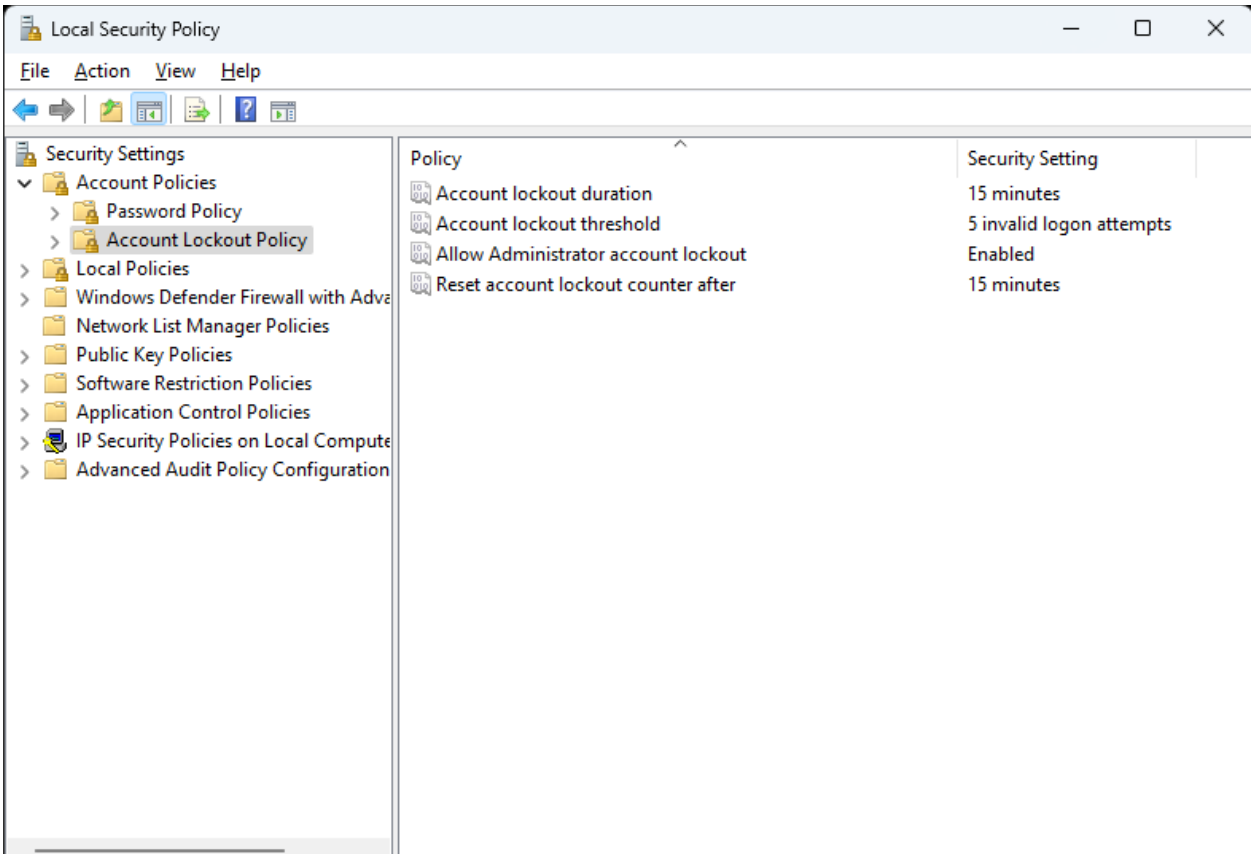
- Password policy

a. Password History: 24 passwords remembered
b. Minimum password age:1 days
c. Maximum password age:60 days
d. Minimum Password Length: 14 characters
e. Password Must Meet Complexity Requirements: enabled



- Account lockout policy

    a. Account lockout duration: 15 minutes
    b. Account lockout Threshold: 5 invalid logon attempts
    c. Reset Account Lockout Counter After: 15 minutes



6. Conclusion

Aligning the account policies with the CIS Benchmark recommendations significantly improved the security posture of the Windows Server 2022 environment. While there were challenges, particularly around user experience and log management, the result is a more secure server configuration that meets industry best practices for vulnerability management.