CIS-CAT Security Assessment and System Hardening Report

Assessment and Hardening of Windows 10 System Based on CIS Benchmark & Controls

Mansi Gharat
Internship: Real-Time Operating Systems Hardening
Course: Cyber Security
Internship Provider: NullClass

Date of Submission: May 1, 2025

CONTENTS

1. Executive Summary

This report documents the operating system hardening process during a cybersecurity internship with NullClass. The objective was to enhance the security posture of a Windows 10 system by assessing it against the CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0 and CIS Controls Assessment Module for Implementation Group 1 v1.0.3.

The project involved conducting a baseline security assessment using the CIS-CAT Assessor tool, identifying vulnerabilities based on severity, and mapping them to real-world threat scenarios. Subsequently, system hardening steps were implemented to remediate the critical, high, and medium-risk findings.

A post-hardening assessment was performed to measure the improvements achieved. The compliance score increased significantly, demonstrating successful system security and resilience enhancement. This report details the assessment methodology, vulnerabilities discovered, hardening procedures applied, results after implementation, and recommendations for further improvements.

2. Introduction

2.1 Overview of Operating System Hardening

Operating system (OS) hardening is securing a system by reducing its vulnerabilities, eliminating unnecessary services, applying security patches, and enforcing security configurations. The goal is to create a strong security baseline that minimizes the risk of unauthorized access, data breaches, and system compromise. In cybersecurity, OS hardening plays a crucial role in safeguarding sensitive information and ensuring the reliability of critical systems, especially in environments where real-time protection is essential.

2.2 Objective of the Internship

The objective of this internship project was to perform a complete security assessment and hardening of a Windows 10 operating system using the CIS-CAT Assessor tool. This involved running an initial baseline assessment based on CIS Benchmark and Controls, analyzing the findings, implementing recommended security measures to enhance compliance, and conducting a post-hardening reassessment. The target was to achieve at least a 40% improvement in compliance scores and maximize the security strength of the system, while documenting each step of the process systematically.

3. Initial Assessment

3.1 About CIS-CAT Tool

The **CIS-CAT (Centre for Internet Security Configuration Assessment Tool)** is a lightweight security auditing tool designed to automate the assessment of system configurations against recognized security benchmarks. Developed by the Centre for Internet Security (CIS), it compares the actual system settings against a baseline of best practices defined in CIS Benchmarks.

CIS-CAT Lite allows users to assess system compliance without making any changes to the system itself. It generates detailed reports highlighting areas of compliance and non-compliance, categorizing findings based on severity, such as Critical, High, Medium, and Low. It also provides actionable remediation steps for each finding, helping to quickly identify and correct security weaknesses.

For this project, **CIS-CAT Lite Assessor v4. x** was used to assess the system based on:

- **CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0**
- **CIS Controls Assessment Module - Implementation Group 1 for Windows 10 v1.0.3**

3.2 Baseline Assessment Methodology

The baseline security assessment followed a systematic methodology to ensure an accurate analysis of the system's security posture:

- **Step 1**: Downloaded and installed the latest version of the **CIS-CAT Lite Assessor** tool.
- **Step 2**: Configured the tool to assess compliance against the selected **CIS Benchmark** and **CIS Controls IG1** profiles.
- **Step 3**: Executed an initial scan of the Windows 10 Enterprise system **without** applying any pre-existing security policies or configurations.
- **Step 4**: Generated detailed reports in **HTML** and **TXT** formats documenting the compliance status of various system settings.

- **Step 5**: Classify the findings by severity levels (Critical, High, Medium, Low) for further prioritization during the hardening phase.
- **Step 6**: Captured important screenshots during tool execution and report generation for evidence.

This method provided a clear and comprehensive baseline understanding of the system's initial vulnerabilities.

3.3 Summary of Initial Findings

The initial CIS-CAT assessment revealed several vulnerabilities and misconfigurations that posed significant security risks to the system. Major areas needing improvement included:

- Lack of strong password policies (length and complexity requirements).
- Absence of proper account lockout mechanisms.
- Use of insecure services like SMBv1.
- Disabled Windows Defender Antivirus.
- Insufficient auditing and logging policies.
- Presence of unnecessary user accounts and administrative privileges.

Initial Compliance Results:

- **CIS Controls Assessment Module for IG1**: **60%** (26 out of 43 controls passed).
- **CIS Benchmark for Windows 10 Enterprise v3.0.0**: **38%** (5 out of 13 automated checks passed).

4. Vulnerability Analysis

4.1 Critical Findings

Policy/Control	Description	Risk	Severity (1–10)
Password Policy - Minimum Length	Passwords shorter than 14 characters were allowed.	High risk of brute-force attacks.	10
SMBv1 Protocol Enabled	An obsolete and insecure protocol is still active.	Vulnerable to ransomware attacks like WannaCry.	10
Windows Defender Antivirus Disabled	No active malware protection on the system.	Increased risk of malware infections.	9
Remote Desktop Protocol (RDP) - Not Restricted	RDP was enabled without security restrictions.	High risk of unauthorized remote access.	9

4.2 High, Medium, and Low Severity Findings

Policy/Control	Description	Risk	Severity (1–10)
User Account Control (UAC) Disabled	No administrative consent required for system changes.	Easier for malware to escalate privileges.	8
Firewall Profiles Disabled	Windows Firewall was inactive.	Exposed system to network attacks.	8
Lack of Account Lockout Policy	No limit on failed login attempts.	Easier for attackers to guess passwords.	7

Medium Severity Issues:

Policy/Control	Description	Risk	Severity (1–10)
Audit Log Settings Incomplete	Failure to audit login events and critical activities.	Reduced ability to detect breaches.	6
Insecure Screensaver Lockout Timing	Delay in automatic workstation locking.	Increased risk of unauthorized physical access.	5

Low Severity Issues:

Policy/Control	Description	Risk	Severity (1–10)
Banner Message Not Configured	No legal or warning message was displayed during login.	Legal risk, low direct security impact.	3
Unused Services Running	Running unnecessary services.	Slightly larger attack surface.	2

4.3 Mapping Vulnerabilities to Real-World Threats

Vulnerability	Possible Real-World Attack Scenario	Reference
Weak Password Policy	Credential stuffing or brute-force attack leading to system compromise.	NIST Special Publication 800-63B - Digital Identity Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html
SMBv1 Enabled	Ransomware spreads through SMBv1 vulnerabilities (e.g., WannaCry, EternalBlue).	Microsoft – Protect against ransomware (WannaCry): https://www.microsoft.com/en-us/security/blog/2017/05/12/wan

Vulnerability	Possible Real-World Attack Scenario	Reference
		nacrypt-ransomware-worm-targets-out-of-date-systems/
Disable Windows Defender	Malware infection through phishing or drive-by downloads.	Microsoft – Windows Security Overview: https://learn.microsoft.com/en-us/troubleshoot/windows-client/windows-security/windows-security-overview
RDP Misconfiguration	Unauthorized remote login and lateral network movement (e.g., BlueKeep vulnerability).	CISA – RDP Vulnerabilities and BlueKeep Advisory: https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-168a
Missing Audit Logs	Difficulty detecting and investigating breaches or insider activities.	NIST Special Publication 800-92 - Guide to Computer Security Log Management: https://csrc.nist.gov/pubs/sp/800/92/final

5. Hardening Implementation

5.1 Approach to System Hardening

The system hardening process followed a structured and standards-based approach guided by:

- **CIS Benchmarks (v3.0.0)** for Microsoft Windows 10 Enterprise
- **CIS Controls (v8)**, Implementation Group 1 (IG1)
- **CIS-CAT Pro Tool** for automated and manual compliance verification

The hardening plan was executed in stages:

- **Baseline Assessment**: Initial configuration reviewed using CIS-CAT Pro.
- **Gap Analysis**: Identified failed controls and non-compliant configurations.
- **Remediation**: Applied changes via Group Policy Objects (GPO), registry modifications, and local security settings.
- **Validation**: Re-ran CIS-CAT to verify compliance and document improvements.

5.2 Changes Made Based on CIS Benchmark

Key hardening actions included:

Control Area	Change Implemented
Password Policy	Enforced complexity, minimum length, and history requirements
Account Lockout	Configured thresholds to block brute force attempts
User Rights Assignment	Limited “Log on locally” and “Access this computer from network” permissions
Audit Policy	Enabled auditing for account logon events and object access
AutoRun Settings	Disable AutoRun for all drives
Windows Defender	Enabled real-time monitoring and cloud-delivered protection

Control Area	Change Implemented
Firewall	Ensured all profiles have the firewall enabled
Telemetry	Reduced diagnostic data to the minimum

5.3 Challenges Encountered and Solutions

Challenge	Description	Solution
Group Policy Conflicts	Existing GPOs conflicted with new CIS settings (e.g., password length)	Reviewed and reordered GPO links; documented all CIS overrides
User Disruption Risk	Changes like lockout policies risk locking out users	Applied changes during maintenance windows and monitored closely
Manual Configurations	Some CIS controls lacked automated enforcement (e.g., default passwords on software)	Used administrative scripts and manual verification via surveys
Time Constraints	Full hardening required several iterations to test and validate	Prioritized high-risk controls first (e.g., firewall, accounts)

6. Post-Hardening Assessment

After applying the recommended hardening measures on the Windows 10 Pro system, a post-hardening CIS-CAT assessment was conducted to evaluate improvements in compliance.

6.1 Re-running CIS-CAT Assessment

The CIS-CAT Assessor tool was re-run using the same benchmark profile (CIS Microsoft Windows 10 Benchmark - Level 1).
Both automated checks and user survey questions were reassessed to ensure consistent evaluation.

Procedure:

- Assessed the same environment without altering the benchmark version.
- Focused on improvements in system policies, security controls, and user account configurations.

6.2 Compliance Score Comparison

- **CIS Controls Assessment Module (IG1)**
    - **Before Hardening: 60% compliance**
    - **After Hardening: 88% compliance**
- **CIS Windows 10 Enterprise Benchmark**
    - **Before Hardening: 38% (automated checks)**
    - **After Hardening: 62% (automated checks)**

Notable Observations:

- Automated checks showed significant improvement.
- Manual or user survey responses were fully aligned with security standards after remediation.
- No critical failures or errors were reported post-hardening.

Important Note:

This CIS-CAT compliance testing was conducted on a Virtualized Windows 10 Pro environment. A full system backup was taken before hardening changes on the main operating system to ensure rollback capability.

7. Controls Assessment Summary

7.1 CIS Controls Implementation Highlights

Following the system hardening efforts based on the **CIS Controls Assessment Module - Implementation Group 1 (IG1)** for Windows 10 and the **CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0**, several critical controls were successfully implemented:

- **Audit Logging:** Activated and verified to ensure continuous security monitoring.
- **Password Management:** Default passwords were changed, and strong password policies were enforced.
- **Malware Protection:** Anti-malware software was updated, and real-time protection was confirmed.
- **AutoRun and AutoPlay Settings:** Disabled to prevent automatic execution of external media content.
- **Firewall Configuration:** Host-based firewall was enabled and properly configured to restrict inbound and outbound traffic.
- **Backup Strategy:** Although an automated system backup was initially missing, corrective actions were taken, and backups were secured.
- **Account Management:** Dormant accounts were disabled, and workstation locking after inactivity was enforced.
- **Encryption Standards:** Advanced Encryption Standard (AES) was applied for securing wireless communications.

Additionally, a **backup** of the operating system was taken before applying changes to ensure system recovery if needed.

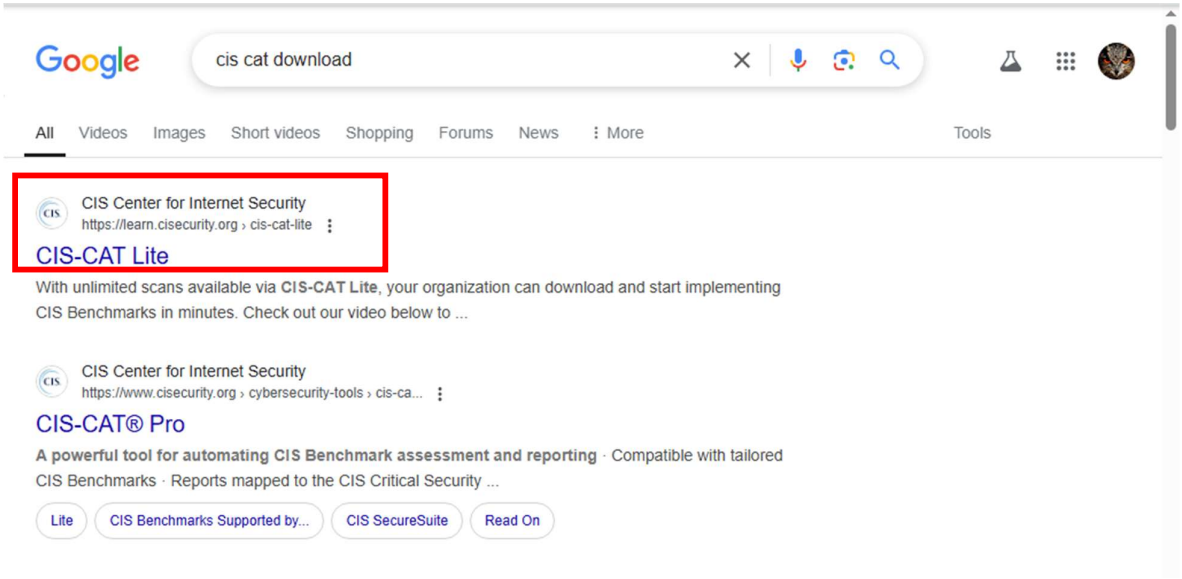
7.2 Compliance Improvement Achieved

Through the hardening process, substantial improvements were observed:

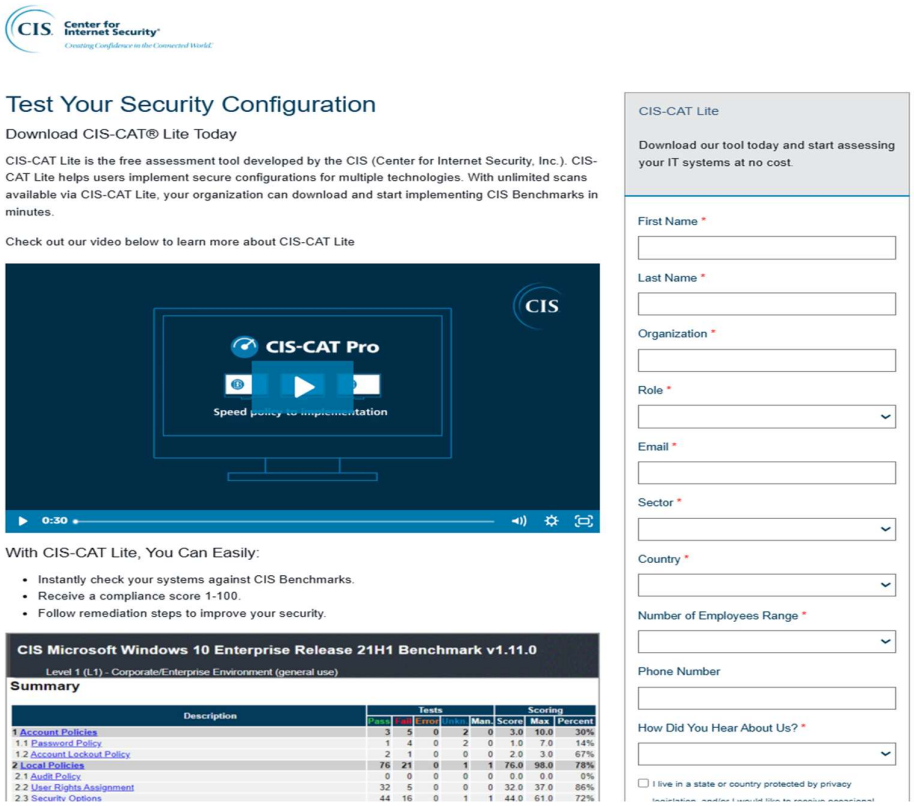
Benchmark	**Before Hardening**	**After Hardening**	**Compliance Improvement**
CIS Controls Assessment Module (IG1) v1.0.3	60% (26/43)	88% (38/43)	**+28%**
CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0	38% (5/13 Automated)	62% (8/13 Automated)	**+24%**

8. Screenshots

8.1 Installation of CIS-CAT



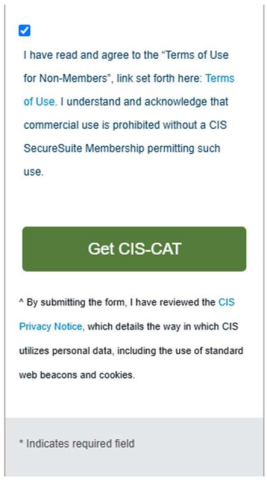
1. Visit this link mentioned above: https://learn.cisecurity.org/cis-cat-lite



2. Fill in the necessary details and get a download link in your email.

	Lite	Pro
CIS Benchmarks supported	Select*	80+
Requires a license key		✓
Graphical User and Command Line Interface (GUI and CLI) Options	✓	✓
CIS Controls Assessment Module	✓	✓
Measure assessment results on conformity scale of 0-100	✓	✓
Evidence-based reports in HTML format	✓	✓
Perform unlimited scans	✓	✓
Assess against other SCAP content (i.e. DISA STIGS)		✓
Remotely assess endpoints	✓	✓
Customize CIS Benchmark content via CIS WorkBench		✓
Access to CIS Benchmarks in XML/XCCDF/OVAL		✓
Assess multiple machines at one time via centralized workflows	✓	✓
Analyze assessment results in CIS-CAT Pro Dashboard		✓
Evidence-based reports in Text, Excel, and XML(ARF) formats		✓

*Windows 10, Ubuntu, and Google Chrome

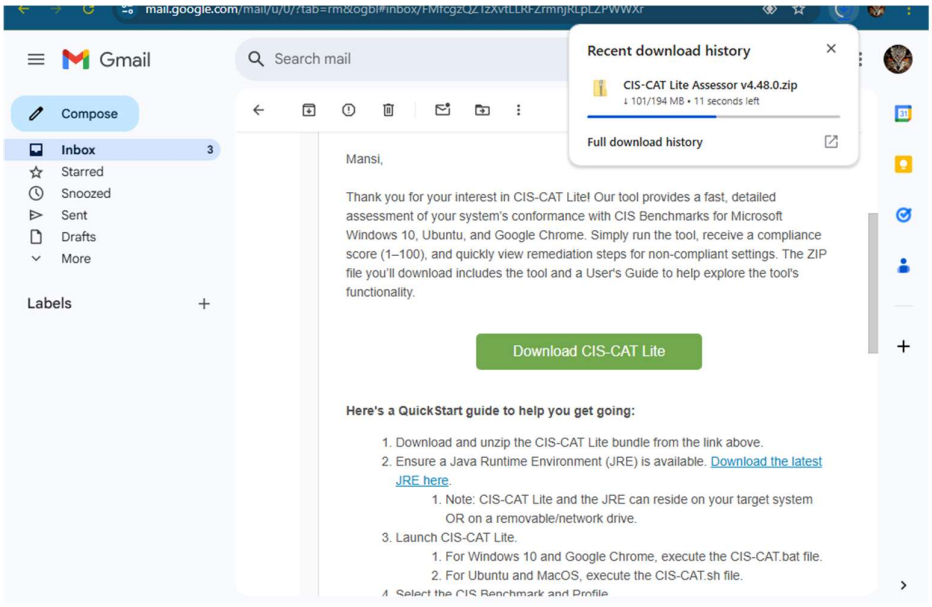


Check Your Email in a Few Minutes

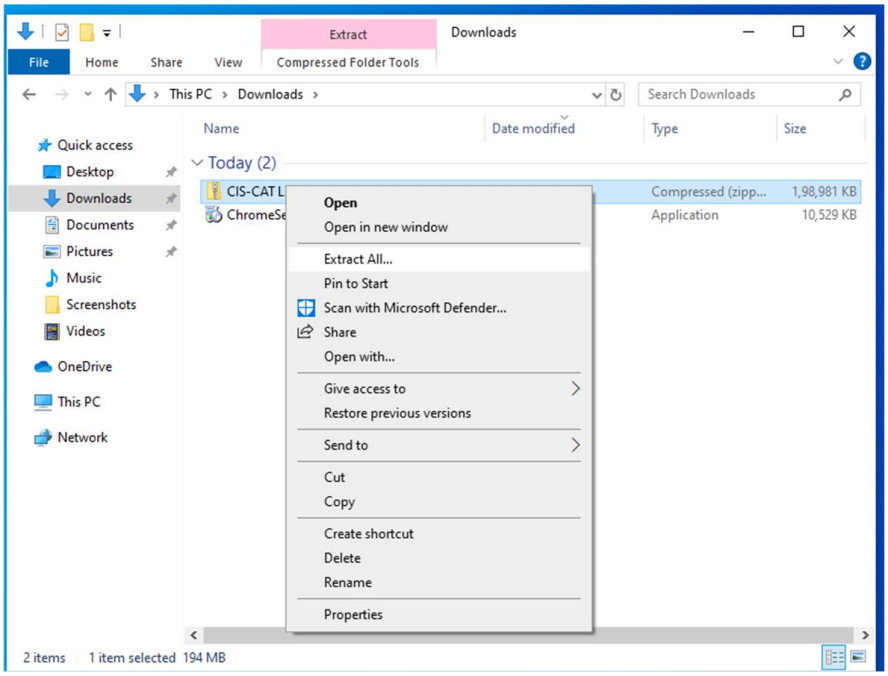
We have just sent you an email to the address you supplied on the form. The email will include a link to download CIS-CAT® Lite. Because it's an HTML email, your spam filter may have put it in your spam folder. Please check all folders.

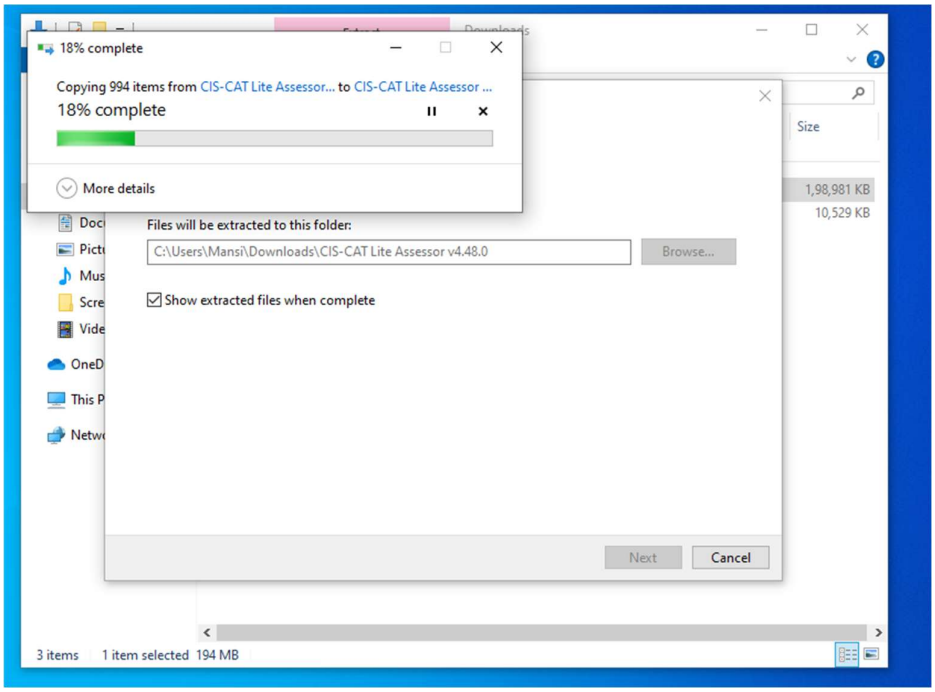
Used by more than 4,000 businesses and organizations around the world, *CIS SecureSuite® Membership* provides access to integrated benefits, tools, and resources that help you to streamline your implementation of security best practices from the Center for Internet Security® (CIS®).

Continue Exploring the CIS Website

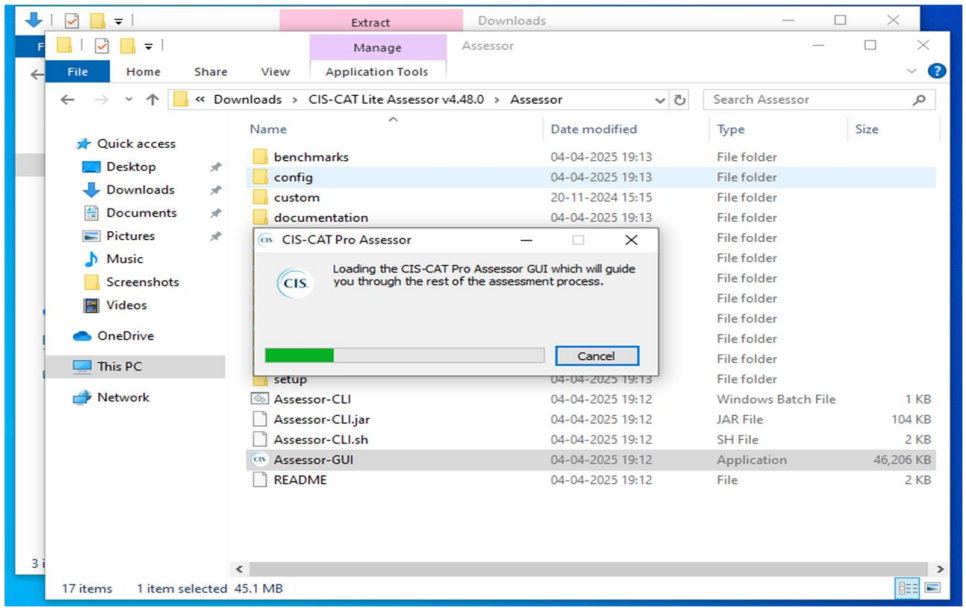


3. The above screenshots show the initial download process



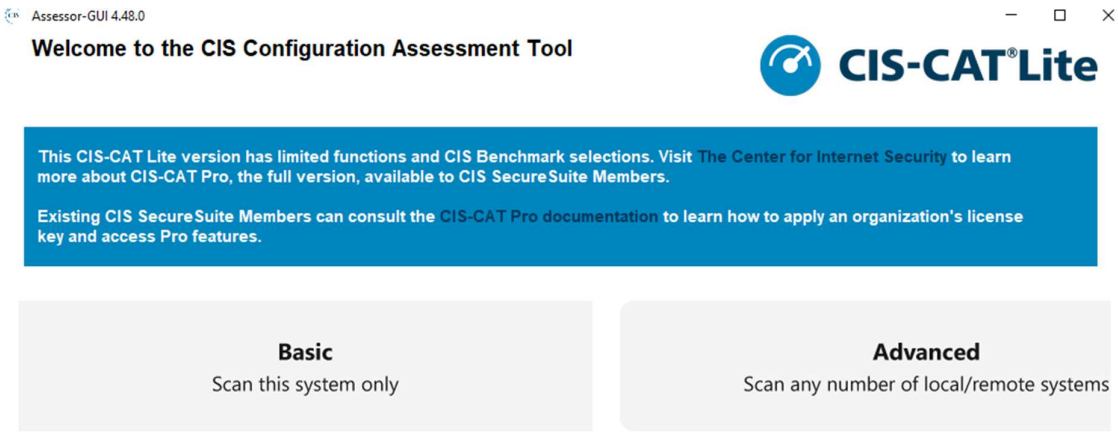


4. Extract downloaded software files



5. Click on Assessor-GUI to run

8.2 Initial Assessment Screenshots



CIS (Centre for Internet Security) CAT (Cybersecurity Assessment Tool) offers both **basic** and **advanced** assessment options. These tools are used for evaluating the cybersecurity posture of an organization based on a series of predefined best practices and standards. Here's a breakdown:

Basic CIS CAT Option:

The **basic** version is designed to be more straightforward and focuses on simple, high-level assessments. It provides:

- **Pre-configured Security Benchmarks:** The basic version assesses security based on CIS benchmarks. These benchmarks include security configuration guidelines for various operating systems, network devices, and cloud environments.
- **Ease of Use:** The basic tool is often more accessible, offering users an easy interface for quick assessments.
- **Manual Reporting:** It generates reports that give a snapshot of the organization's compliance with the CIS benchmarks.
- **Focus on Essential Security Controls:** It generally covers the most critical and fundamental controls that have the most significant impact on reducing risks.

Advanced CIS CAT Option:

The **advanced** version is more comprehensive and provides additional features for a deeper, more detailed security assessment. Key differences include:

- **In-depth Configuration Checks:** The advanced version may include additional checks and more specific configurations that align with different types of environments.
- **Customization:** Users can customize their assessments, such as focusing on certain benchmarks or control groups (like critical controls or specific platforms).
- **Detailed Reporting and Analytics:** It includes more granular reporting, often offering better insights into areas of vulnerability and compliance.
- **Advanced Features like Automation and Scheduling:** The advanced tool can integrate with systems for automated assessments, schedule regular scans, and provide more frequent updates.
- **Support for Complex Environments:** It can handle complex, heterogeneous IT environments, providing specific insights for each system or network configuration.

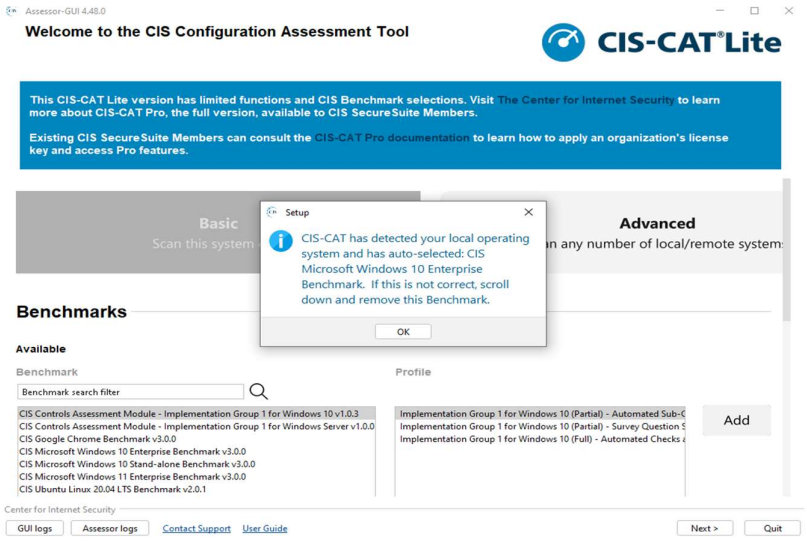
Summary of Key Differences:

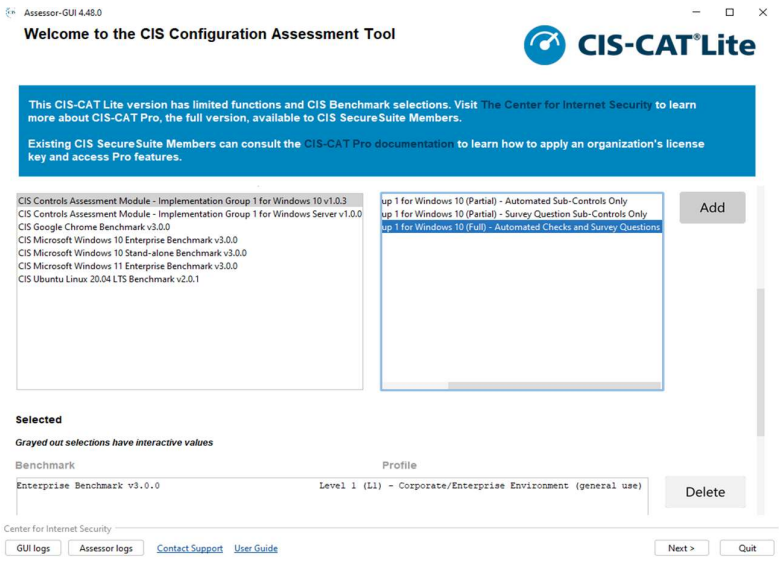
- **Basic:** Simpler, suitable for quick, high-level assessments and smaller environments.

- **Advanced:** More detailed, with deeper customization and integration capabilities, ideal for larger, more complex environments or ongoing security posture monitoring.

Both versions are designed to help organizations assess their cybersecurity practices, but the advanced version is more powerful and suited for those needing detailed, customized assessments.

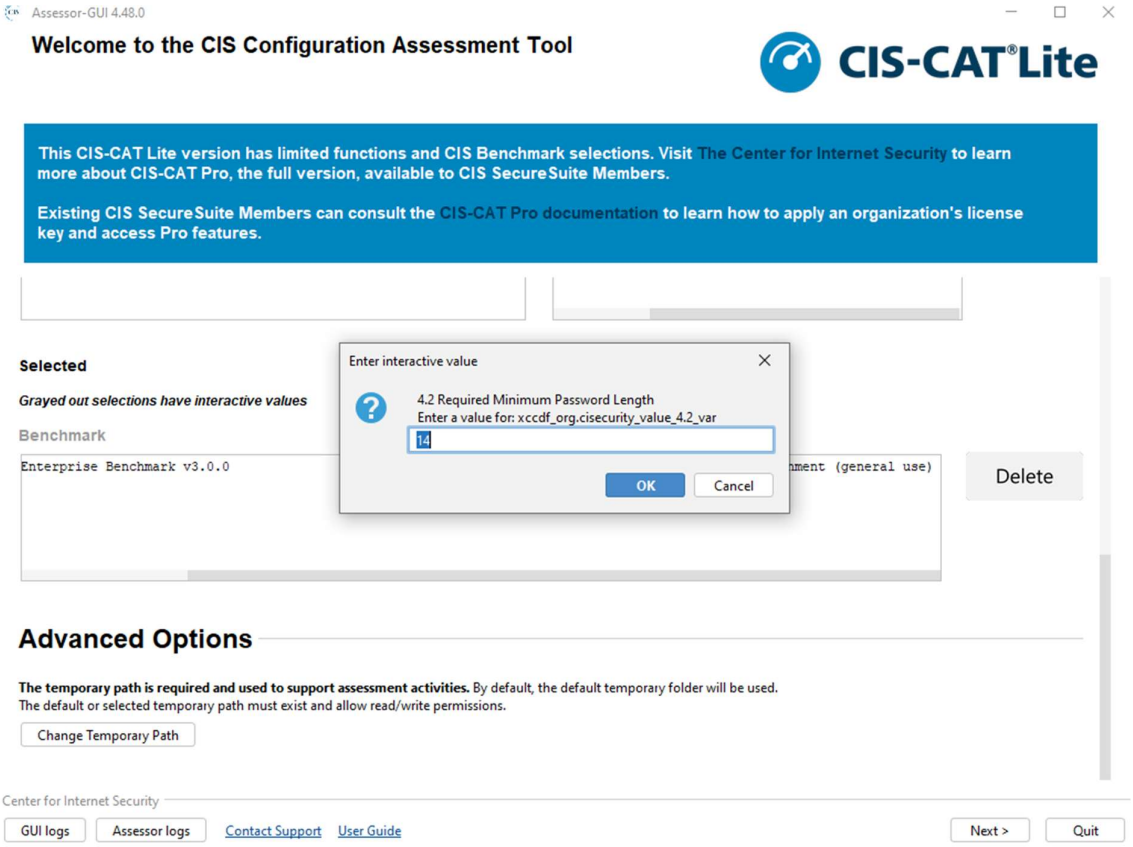
1. For testing purposes will run basic.





(Software will detect the system automatically.)

2. Answer the survey questions to get results for the assessment process



CIS CAT (Cybersecurity Assessment Tool) benchmarks are designed to assess an organization's security posture based on the Centre for Internet Security's best practices. The survey questions asked by the CIS CAT are generally focused on the specific security controls and configurations recommended by CIS for various platforms (such as operating systems, network devices, and cloud services).

Below are some typical types of survey questions asked by the **CIS CAT Benchmark**:

1. Operating System Configuration Questions:

- **System Configuration:** "Is the system configured to restrict access to sensitive files?"
- **User Permissions:** "Are user permissions restricted to the least privileged necessary for task completion?"
- **Account Lockout Policies:** "Is there a policy that locks user accounts after a specified number of failed login attempts?"

- **Password Management:** "Are password policies in place to enforce strong passwords (length, complexity, expiration)?"

2. Network Configuration Questions:

- **Firewall Settings:** "Is a firewall enabled and configured according to best practices?"
- **Remote Access:** "Are remote access methods secured with multi-factor authentication?"
- **Network Segmentation:** "Are internal networks segmented from critical systems to limit the impact of potential attacks?"
- **Open Ports and Services:** "Have unnecessary services been disabled or removed from the network?"

3. Patch Management:

- **Patch Updates:** "Are systems and applications regularly updated with the latest patches?"
- **Vulnerability Scanning:** "Does the organization conduct regular vulnerability assessments?"

4. Logging and Monitoring:

- **Audit Logging:** "Is audit logging enabled to capture key system and user activities?"
- **Log Retention:** "Are logs securely stored and retained for an appropriate period?"
- **Intrusion Detection Systems (IDS):** "Are IDS/IPS (Intrusion Detection and Prevention Systems) deployed and configured properly?"

5. System Hardening:

- **Unnecessary Software Removal:** "Are unused applications and services removed from the system?"
- **File Integrity Monitoring:** "Is file integrity monitoring in place to detect unauthorized changes to critical system files?"
- **Privilege Escalation Protection:** "Are there safeguards in place to detect and prevent privilege escalation?"

6. Cloud Environment (if applicable):

- **Cloud Security Configurations:** "Is the cloud environment configured to minimize access to sensitive data?"
- **Identity and Access Management (IAM):** "Are proper identity and access management policies configured in the cloud environment?"
- **Encryption of Data:** "Is sensitive data encrypted both in transit and at rest in the cloud?"

7. Security Awareness:

- **Employee Training:** "Do employees receive regular security training on phishing and other threats?"
- **Incident Response Plan:** "Is there a documented and tested incident response plan?"

8. Incident Response:

- **Incident Reporting:** "Are incidents reported and tracked according to a standard process?"
- **Backups and Recovery:** "Are regular backups performed and securely stored for critical data?"

Example Question Format:

- **Question:** "Is the system configured to restrict access to sensitive files?"
- **Answer Options:** Yes / No / Not Applicable
- **Explanation:** The tool will then analyze whether the answer is in line with CIS's recommended practices for securing sensitive data.

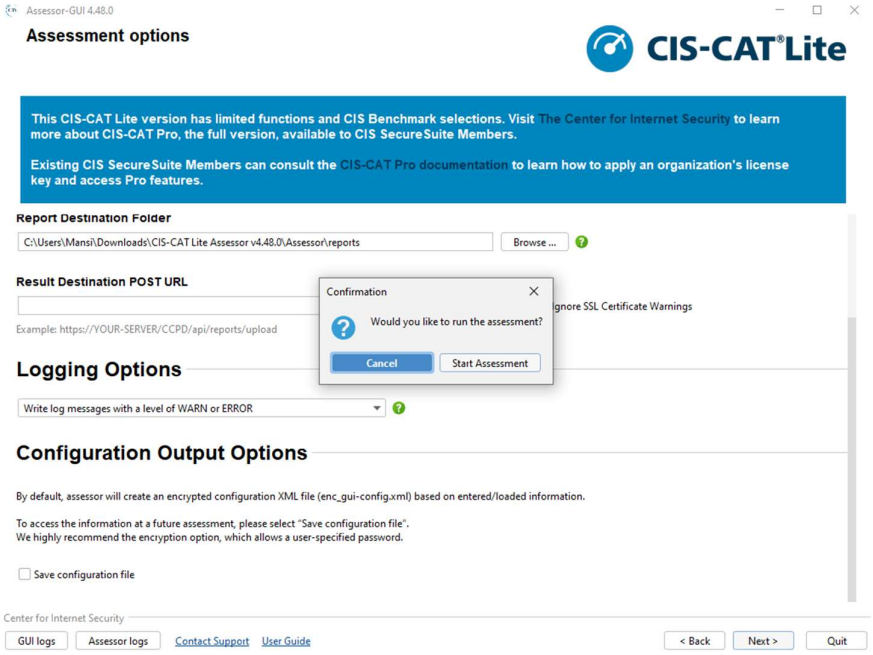
Summary:

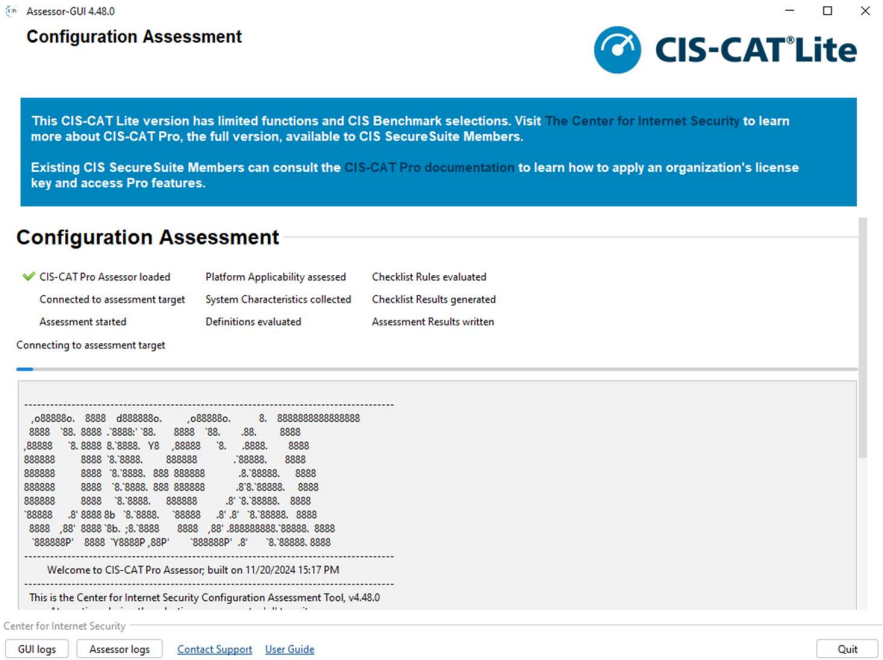
The CIS CAT tool focuses on evaluating configurations and practices related to **system hardening**, **network security**, **user access controls**, **patch management**, **logging and monitoring**, and more. The questions are often based on security best practices that reduce

vulnerabilities, and they require a simple yes/no (or sometimes a score) answer to determine whether a control is correctly implemented.

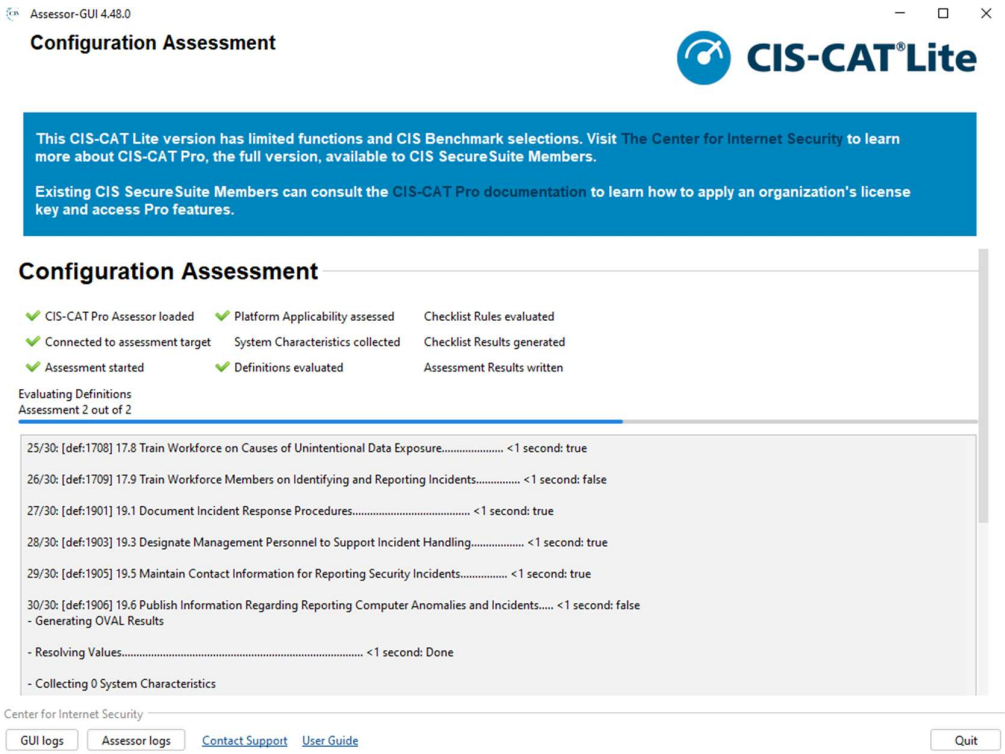
These questions are designed to guide users in assessing their current security configurations, identifying gaps, and providing actionable recommendations to improve security.

3. After that, start the assessment.

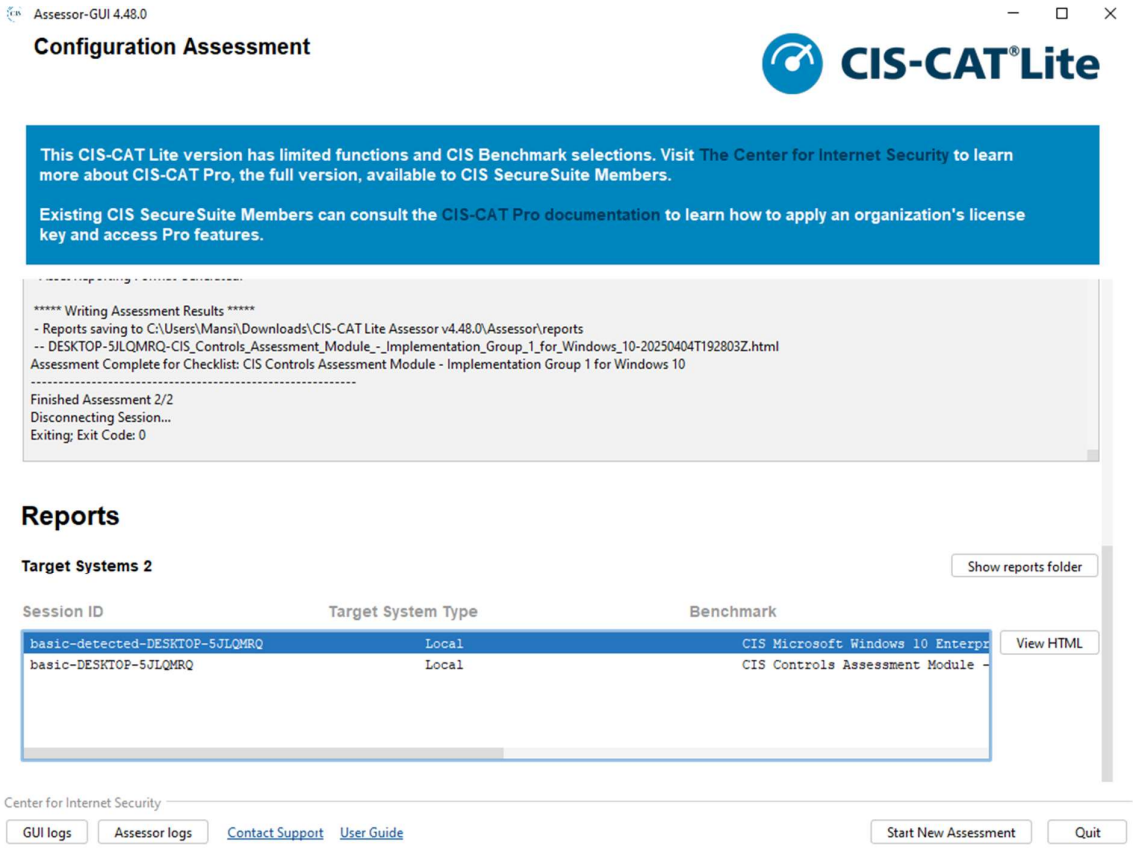




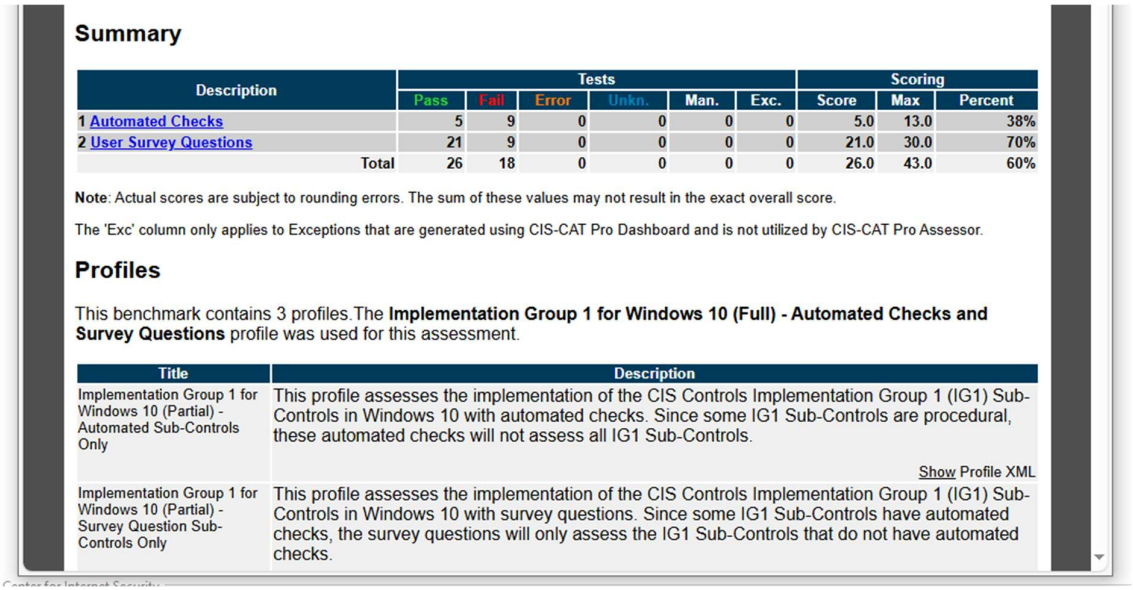
It will take a few minutes for this process. There would be 2 assessments taken.



4. Save the assessment results in HTML format.



5. Initial assessment results.



Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Automated Checks	5	9	0	0	0	0	5.0	13.0	38%
2 User Survey Questions	21	9	0	0	0	0	21.0	30.0	70%
Total	26	18	0	0	0	0	26.0	43.0	60%

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

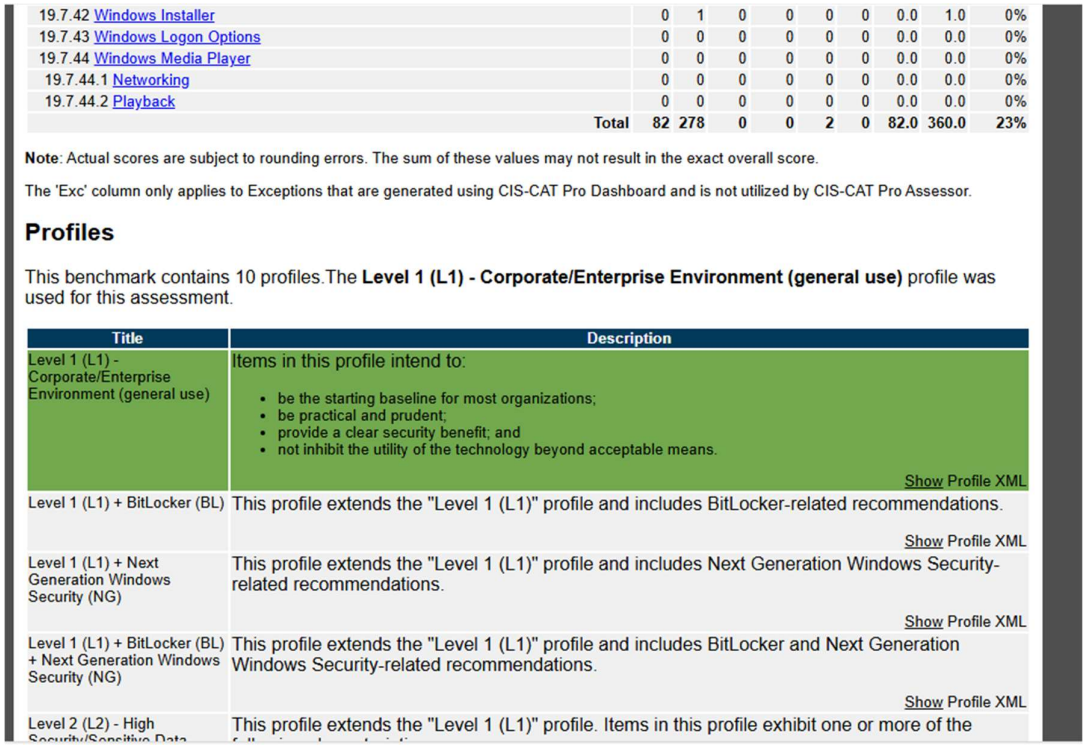
The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

Profiles

This benchmark contains 3 profiles.The **Implementation Group 1 for Windows 10 (Full) - Automated Checks and Survey Questions** profile was used for this assessment.

Title	Description
Implementation Group 1 for Windows 10 (Partial) - Automated Sub-Controls Only	This profile assesses the implementation of the CIS Controls Implementation Group 1 (IG1) Sub-Controls in Windows 10 with automated checks. Since some IG1 Sub-Controls are procedural, these automated checks will not assess all IG1 Sub-Controls. Show Profile XML
Implementation Group 1 for Windows 10 (Partial) - Survey Question Sub-Controls Only	This profile assesses the implementation of the CIS Controls Implementation Group 1 (IG1) Sub-Controls in Windows 10 with survey questions. Since some IG1 Sub-Controls have automated checks, the survey questions will only assess the IG1 Sub-Controls that do not have automated checks.

CIS Controls Assessment Module - Implementation Group 1 for Windows 10 v1.0.3



19.7.42 Windows Installer	0	1	0	0	0	0	0.0	1.0	0%
19.7.43 Windows Logon Options	0	0	0	0	0	0	0.0	0.0	0%
19.7.44 Windows Media Player	0	0	0	0	0	0	0.0	0.0	0%
19.7.44.1 Networking	0	0	0	0	0	0	0.0	0.0	0%
19.7.44.2 Playback	0	0	0	0	0	0	0.0	0.0	0%
Total	82	278	0	0	2	0	82.0	360.0	23%

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

Profiles

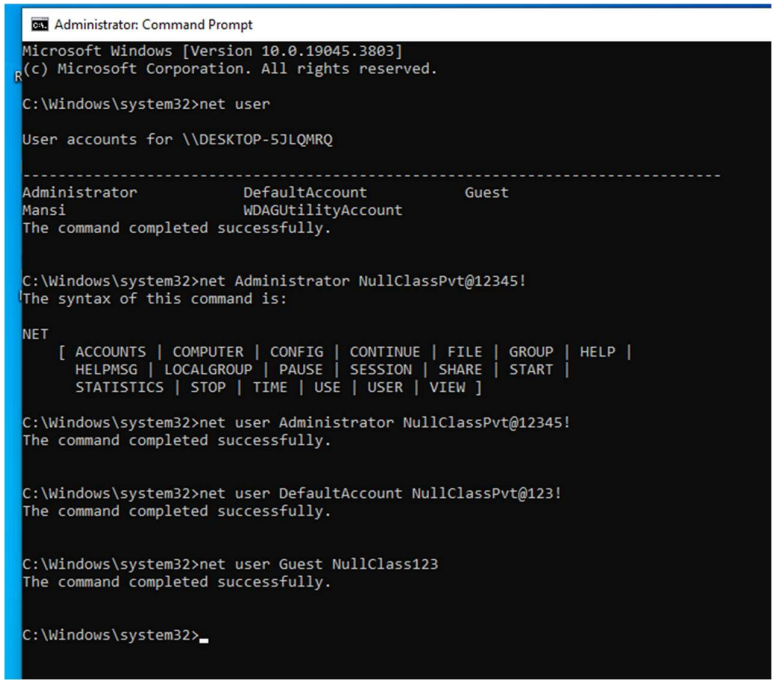
This benchmark contains 10 profiles.The **Level 1 (L1) - Corporate/Enterprise Environment (general use)** profile was used for this assessment.

Title	Description
Level 1 (L1) - Corporate/Enterprise Environment (general use)	Items in this profile intend to: • be the starting baseline for most organizations; • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. Show Profile XML
Level 1 (L1) + BitLocker (BL)	This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations. Show Profile XML
Level 1 (L1) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes Next Generation Windows Security-related recommendations. Show Profile XML
Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes BitLocker and Next Generation Windows Security-related recommendations. Show Profile XML
Level 2 (L2) - High	This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the

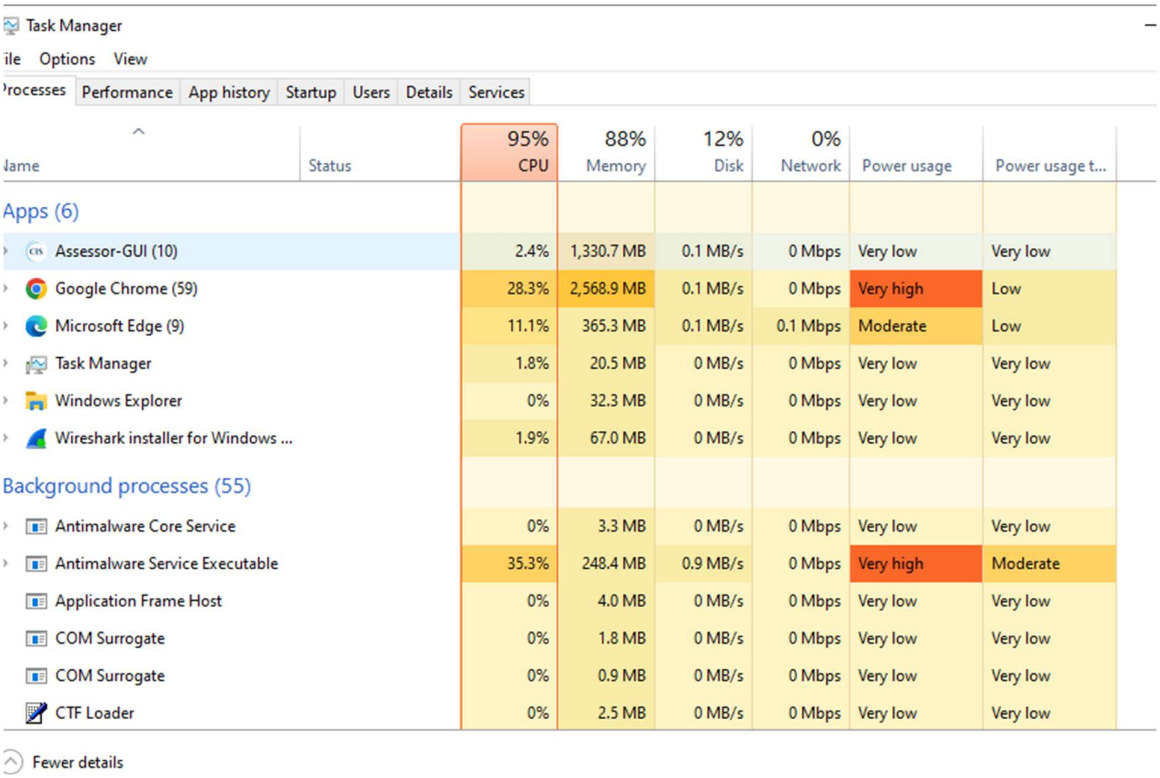
CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0

8.3 Hardening Process Evidence

1. Change the default administrator password



2. From Task Manager, stop the unnecessary processes that keep the CPU engaged a lot.



3. Change in Local Policies Setting.

1. Open Local Group Policy Editor (gpedit.msc)

You can use **gpedit.msc** to modify computer configuration policies.

- Press **Windows Key + R** to open the **Run** dialog box.
- Type gpedit.msc and press **Enter**.

This will open the **Local Group Policy Editor,** where you can navigate through different policy settings.

Common Settings in Local Group Policy Editor:

- **Computer Configuration:**
  - **Windows Settings → Security Settings** → Here, you can configure a variety of system-wide security policies (e.g., account lockout policies, audit policies, user rights assignments).
  - **Software Settings** → Configure software-related settings.
  - **Administrative Templates** → Configure system settings related to user interface, network, etc.
- **User Configuration:**
  - Similar to the computer settings, but applies to individual users rather than the whole system.
  -

2. Open Local Security Policy (secpol.msc)

If you're specifically looking to modify security policies (e.g., password policies, account lockout policies), you can use **secpol.msc**.

- Press **Windows Key + R** to open the **Run** dialog box.
- Type secpol.msc and press **Enter**.

This will open the **Local Security Policy** window.

Common Settings in Local Security Policy:

- **Account Policies:**
  - **Password Policy**: Set password length, complexity requirements, and expiration.
  - **Account Lockout Policy**: Set how many failed login attempts before an account is locked.
- **Local Policies:**
  - **Audit Policy**: Configure auditing for various events like login attempts, object access, etc.
  - **User Rights Assignment**: Control user permissions, such as who can log on locally or remotely.
- **Advanced Audit Policy Configuration**: Further fine-tuning of audit settings.

Steps to Modify Policies:

1. **Open the tool:**
   - For **gpedit.msc**, use Windows + R → type gpedit.msc → press **Enter**.
   - For **secpol.msc**, use Windows + R → type secpol.msc → press **Enter**.
2. **Navigate to the desired policy:**
   - In **gpedit.msc**, go to **Computer Configuration** or **User Configuration** depending on your target.
   - In **secpol.msc**, navigate to **Account Policies** for password/account lockout policies, or **Local Policies** for user rights and audit policies.
3. **Modify the policy:**
   - Double-click the policy you want to change.
   - Adjust the settings to meet your requirements. For example, to change the password policy, you can set the minimum password length or specify password complexity requirements.
4. **Apply the changes:**
   - After modifying the settings, click **Apply** and then **OK** to save the changes.
5. **Close the editor**: Once finished, close the **Local Group Policy Editor** or **Local Security Policy** window.

Example: Modifying Password Policy

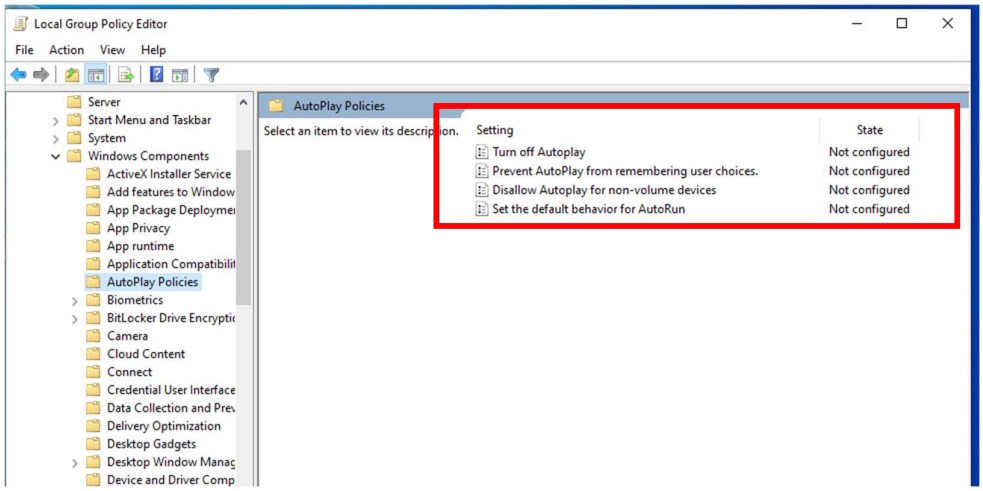
1. Open **secpol.msc** (Press **Windows + R**, type secpol.msc, press **Enter**).

2. In the **Local Security Policy** window, expand **Account Policies** and then select **Password Policy**.
3. Double-click **Minimum password length** and change the value (e.g., set it to 12 characters).
4. Click **Apply** and **OK**.

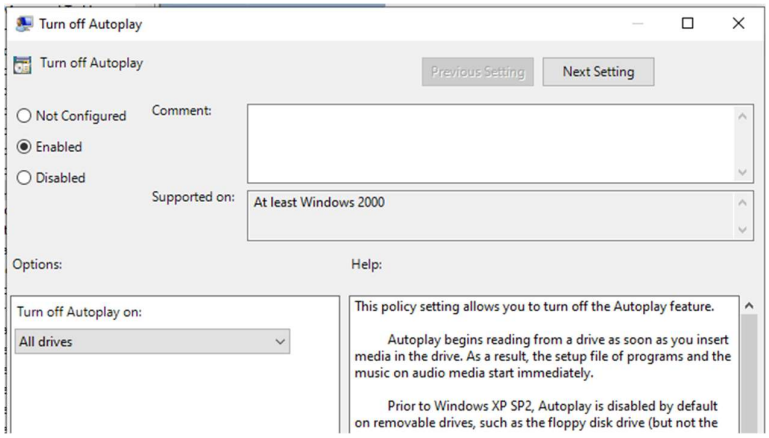
Example: Enabling Account Lockout Policy

1. Open **secpol.msc** (Press **Windows + R**, type secpol.msc, press **Enter**).
2. Under **Account Policies**, select **Account Lockout Policy**.
3. Modify the **Account lockout threshold** (e.g., set to 5 failed login attempts).
4. Click **Apply** and **OK**.

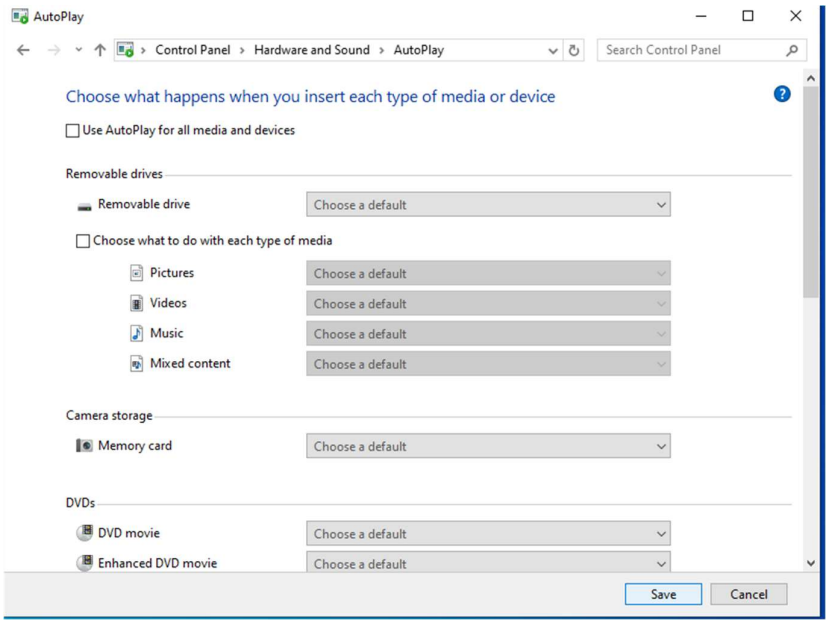
These changes will take effect immediately but may require a restart to fully propagate in some cases.

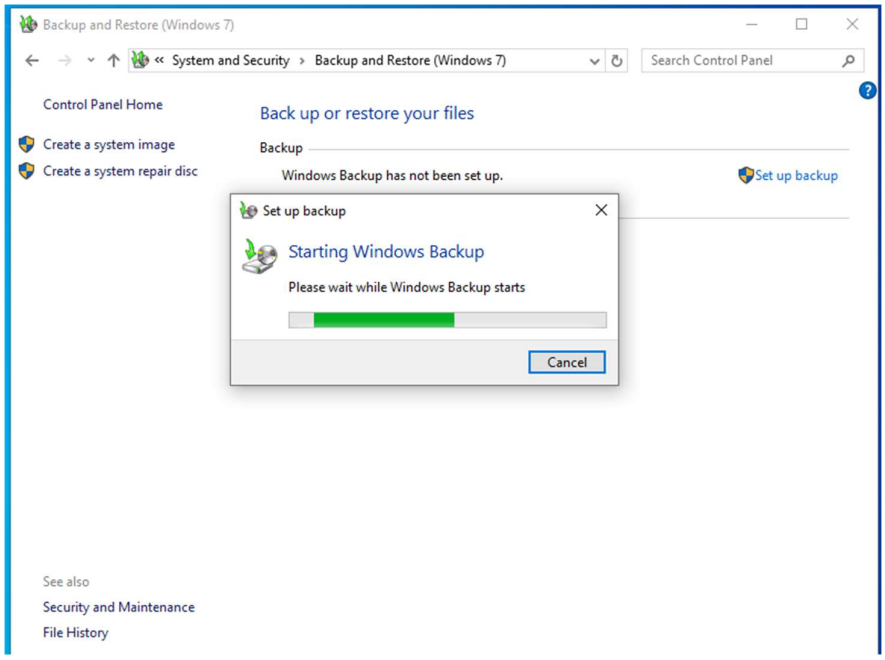


AutoPlay Policy Change



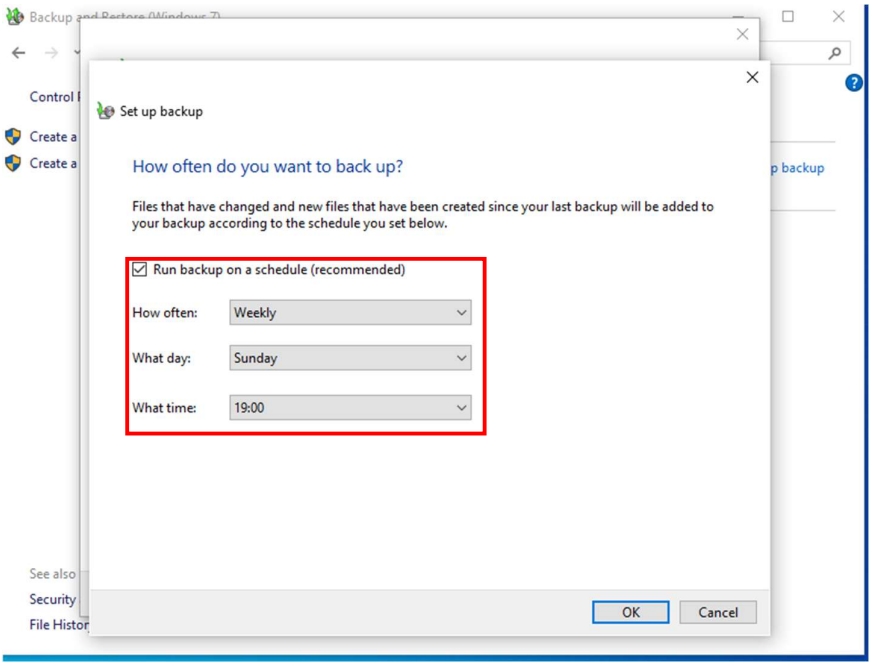
Turn off Autoplay → Enabled → All drives


AutoPlay
Control Panel › Hardware and Sound › AutoPlay
Search Control Panel
Choose what happens when you insert each type of media or device
Use AutoPlay for all media and devices
Removable drives
Removable drive
Choose a default
Choose what to do with each type of media
Pictures
Videos
Music
Mixed content
Camera storage
Memory card
DVDs
DVD movie
Enhanced DVD movie
Save
Cancel

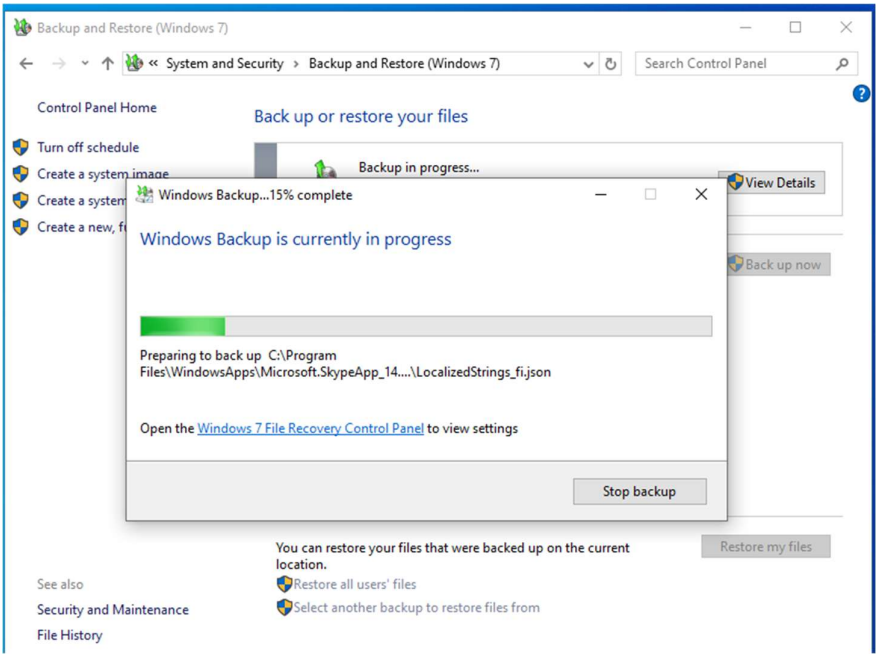

Backup and Restore (Windows 7)
System and Security › Backup and Restore (Windows 7)
Search Control Panel
Control Panel Home
Create a system image
Create a system repair disc
Back up or restore your files
Backup
Windows Backup has not been set up.
Set up backup
Set up backup
Starting Windows Backup
Please wait while Windows Backup starts
Cancel
See also
Security and Maintenance
File History

Perform System Backup

Control Panel→System & Security→Backup and Restore



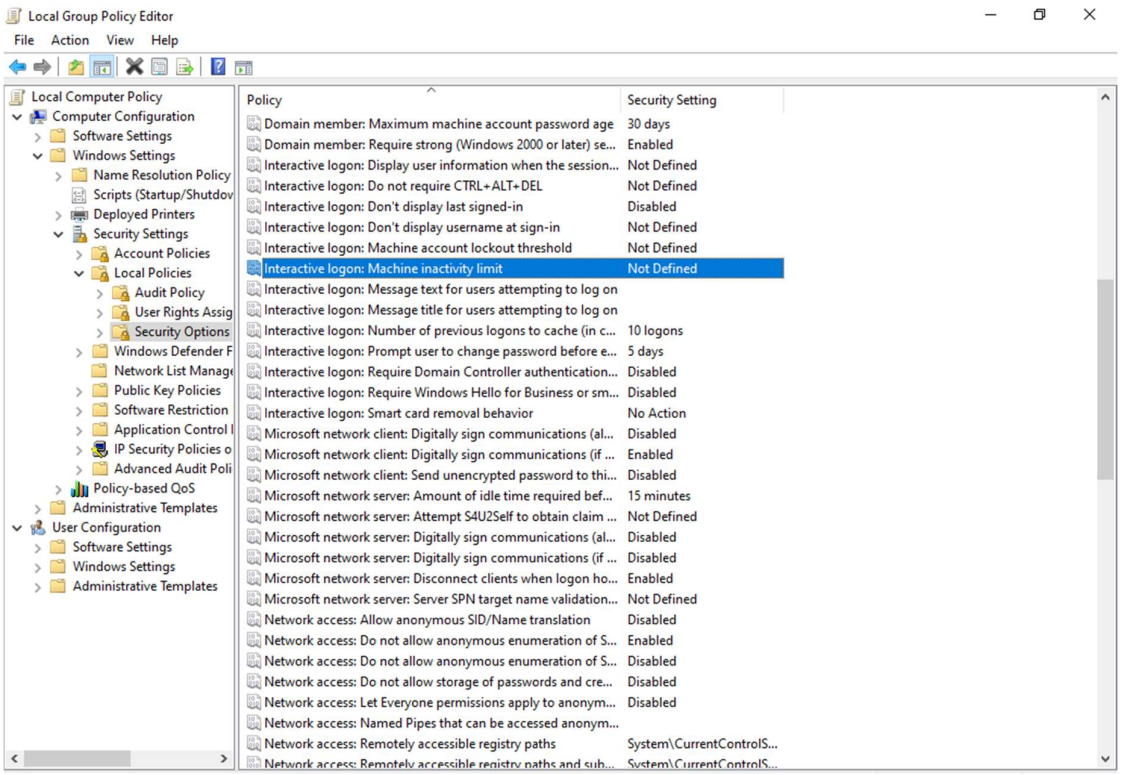
Automate the backup process by setting how often? What day? What time?

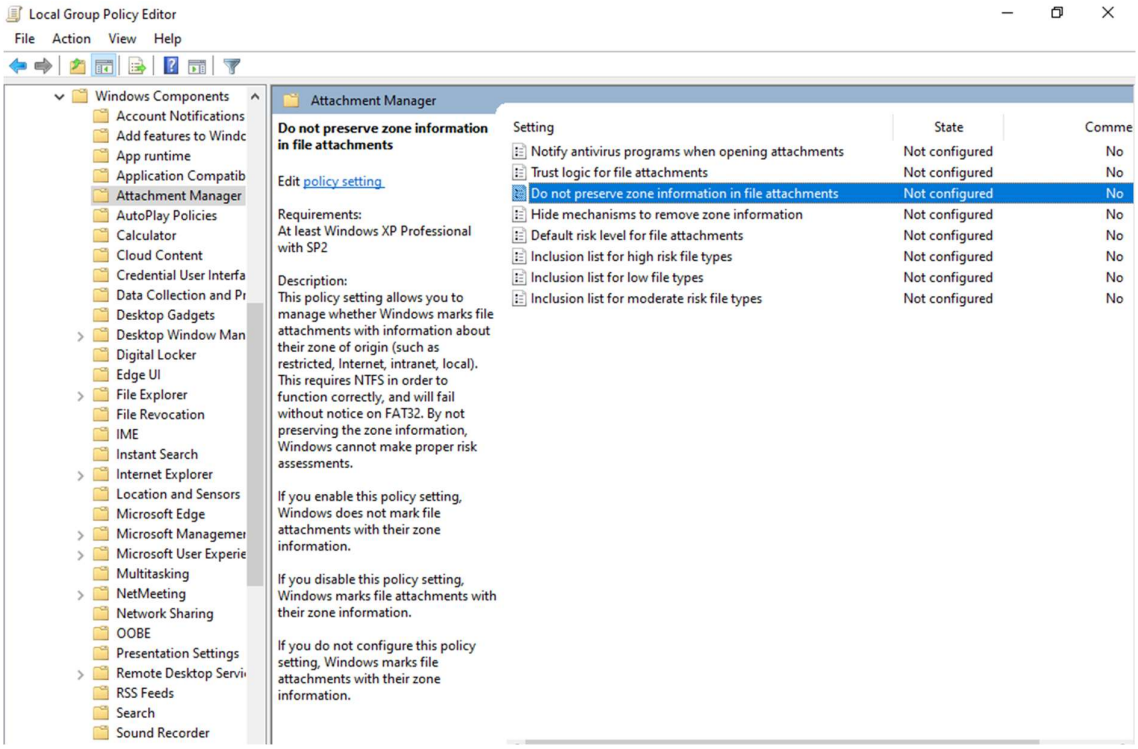


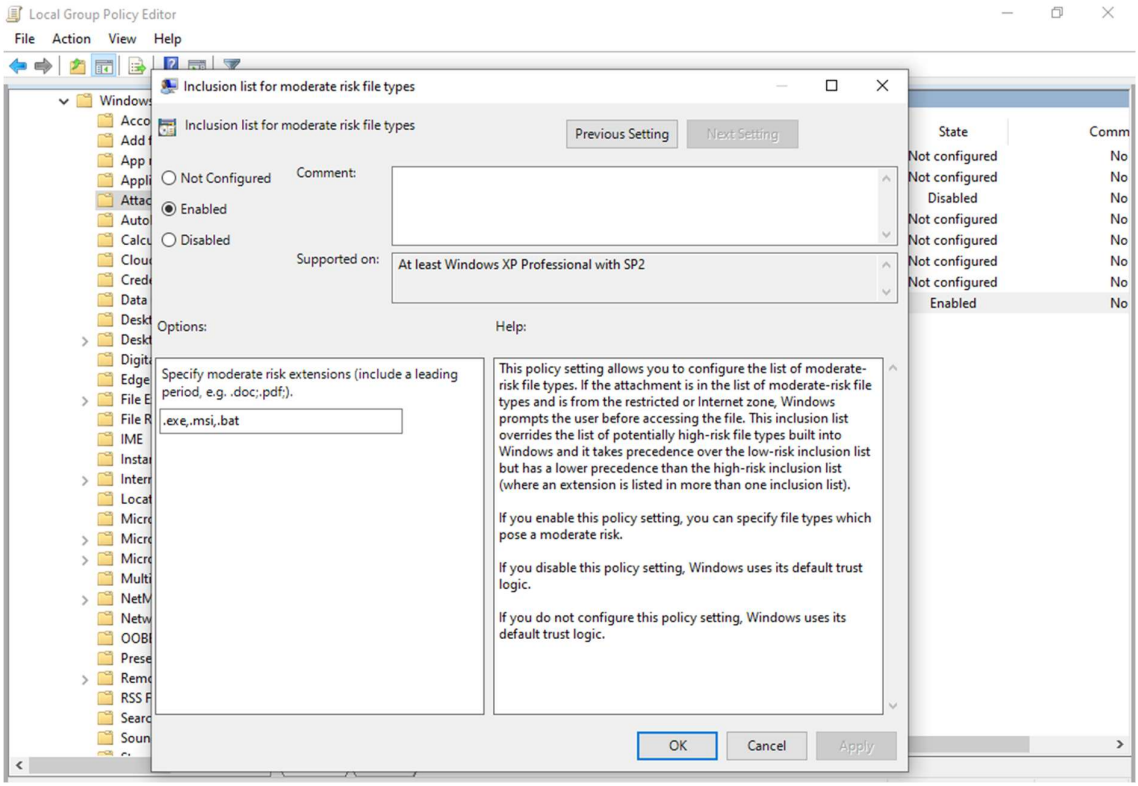
Important Note: *"I have not simulated backup on a virtual environment, but have a backup on a real OS."*

4. Follow the steps mentioned in the CIS-CAT report to edit more policies

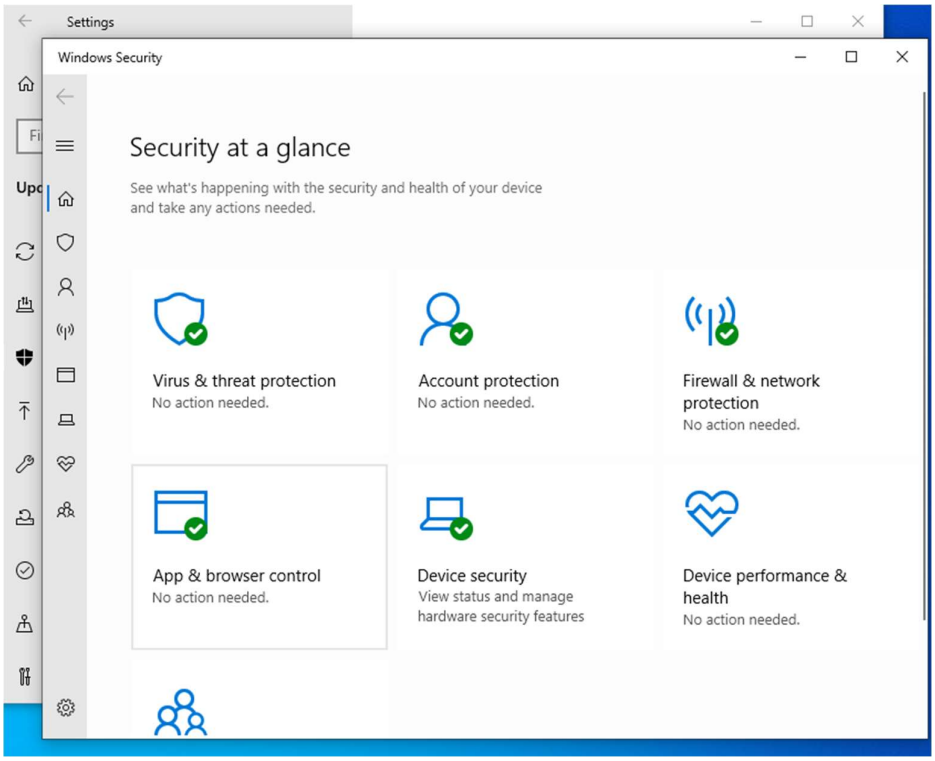
The Following screenshots show proofs of edits regarding policy change

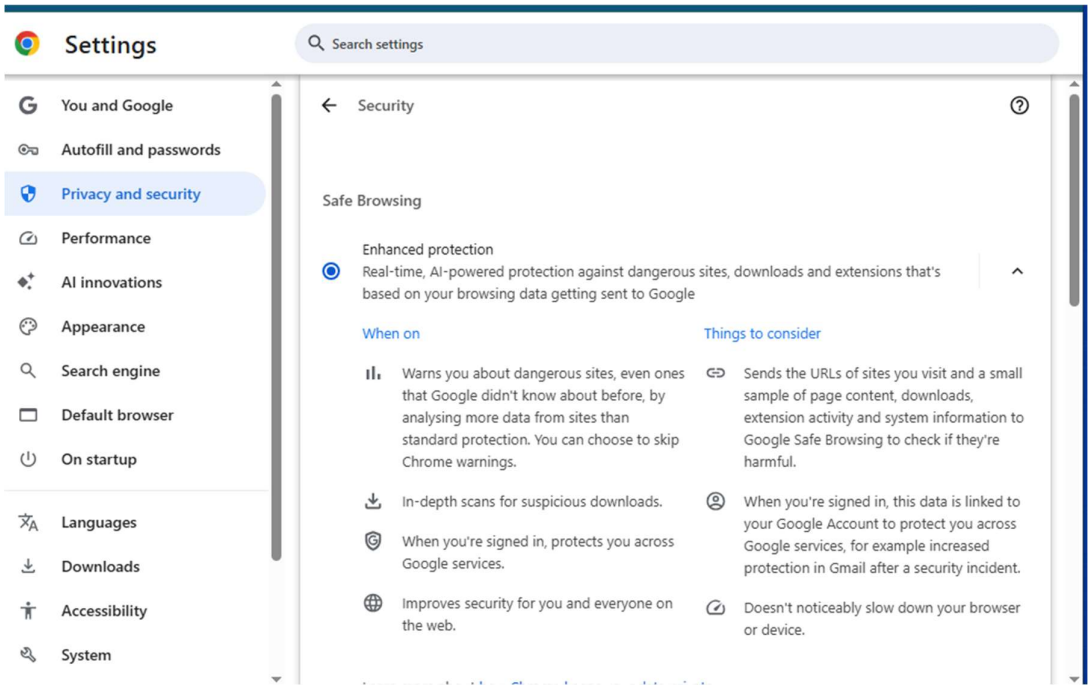




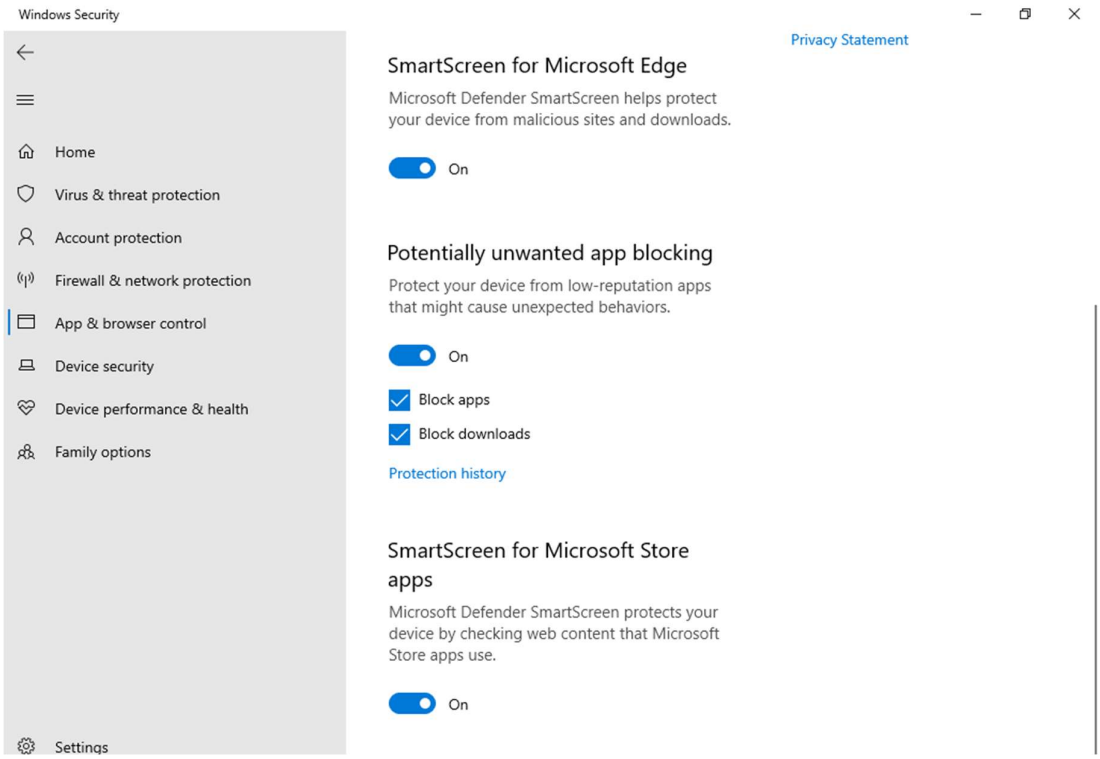


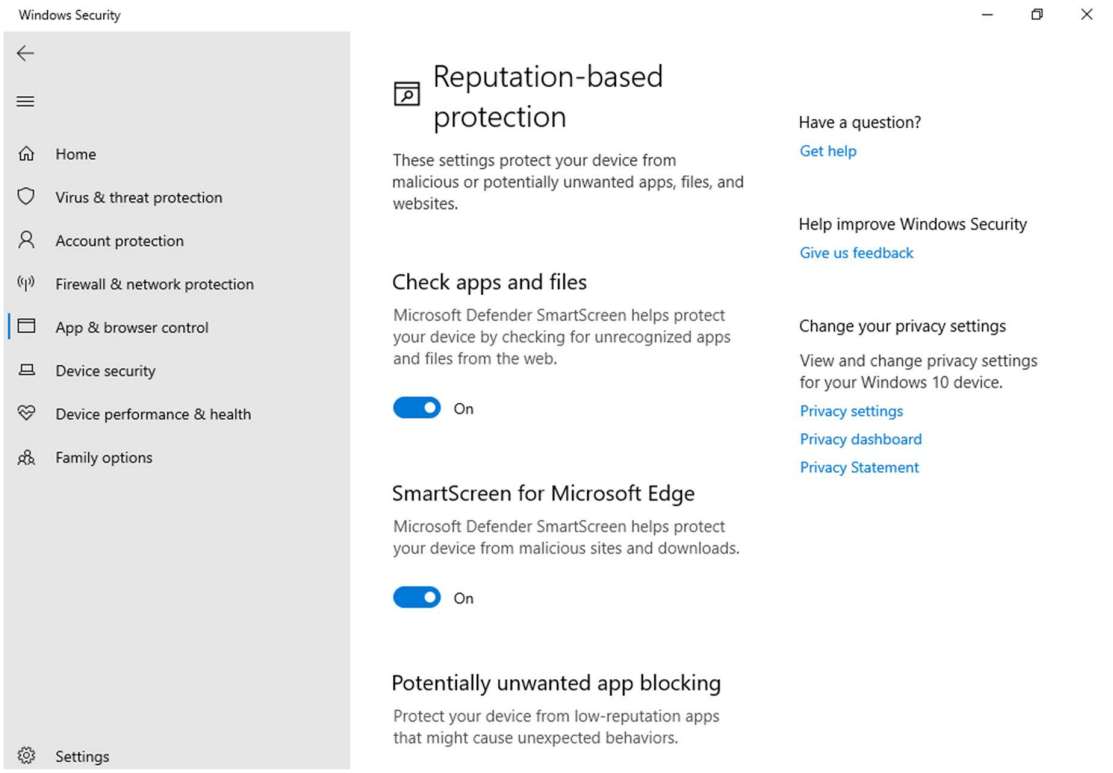
4.1 Windows Firewall Settings

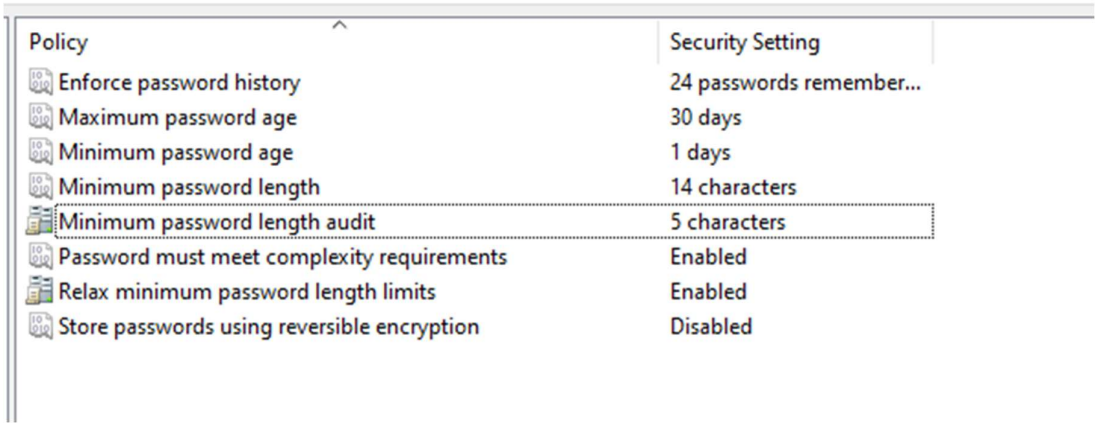




4.2 Google Chrome Browser Settings

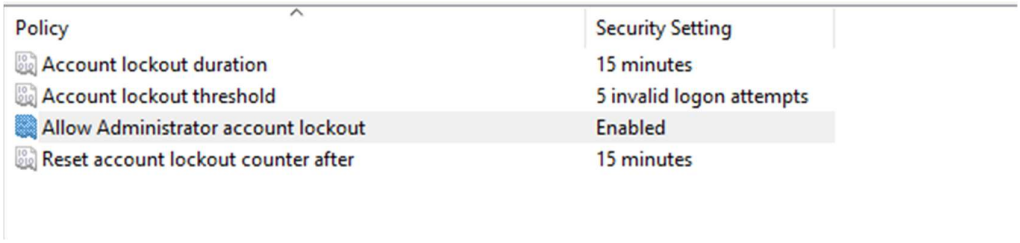

Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Privacy Statement
SmartScreen for Microsoft Edge
Microsoft Defender SmartScreen helps protect your device from malicious sites and downloads.
On
Potentially unwanted app blocking
Protect your device from low-reputation apps that might cause unexpected behaviors.
On
Block apps
Block downloads
Protection history
SmartScreen for Microsoft Store apps
Microsoft Defender SmartScreen protects your device by checking web content that Microsoft Store apps use.
On


Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Reputation-based protection
These settings protect your device from malicious or potentially unwanted apps, files, and websites.
Check apps and files
Microsoft Defender SmartScreen helps protect your device by checking for unrecognized apps and files from the web.
On
SmartScreen for Microsoft Edge
Microsoft Defender SmartScreen helps protect your device from malicious sites and downloads.
On
Potentially unwanted app blocking
Protect your device from low-reputation apps that might cause unexpected behaviors.
Have a question?
Get help
Help improve Windows Security
Give us feedback
Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement



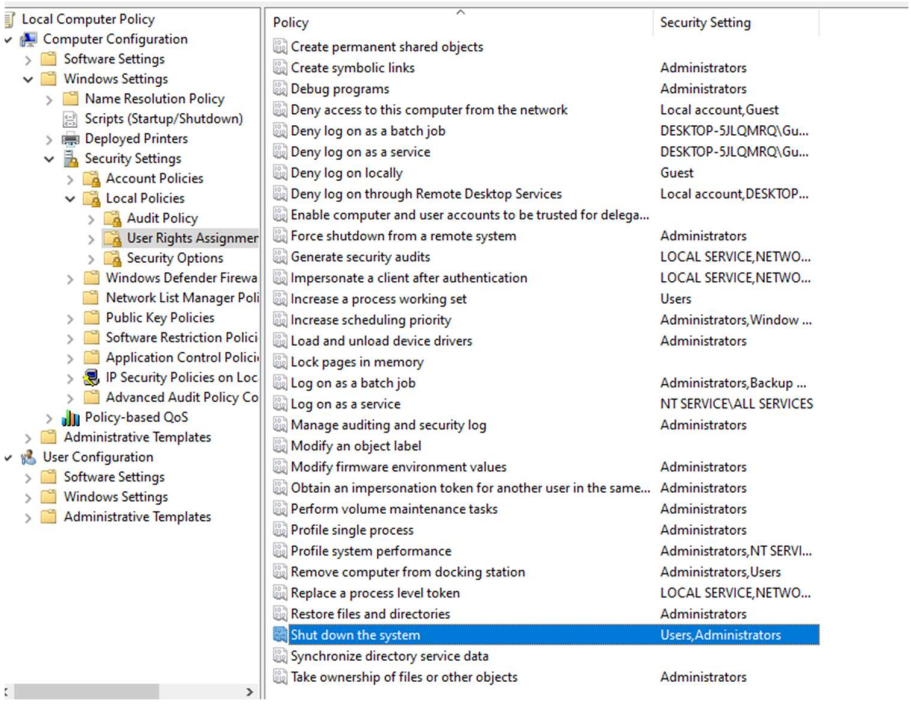
Policy	Security Setting
Enforce password history	24 passwords remember...
Maximum password age	30 days
Minimum password age	1 days
Minimum password length	14 characters
Minimum password length audit	5 characters
Password must meet complexity requirements	Enabled
Relax minimum password length limits	Enabled
Store passwords using reversible encryption	Disabled

4.3 Password Policy Change

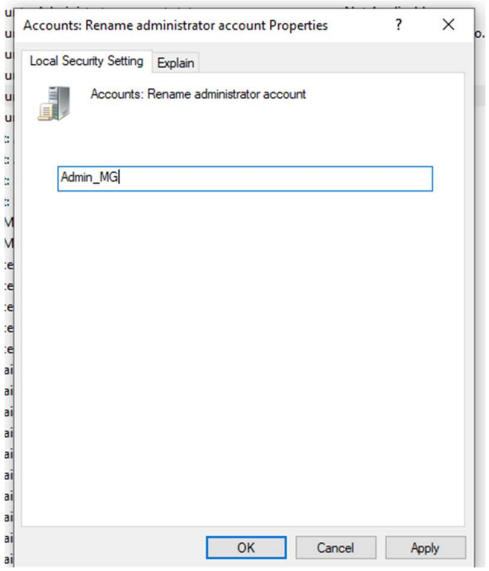


Policy	Security Setting
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	15 minutes

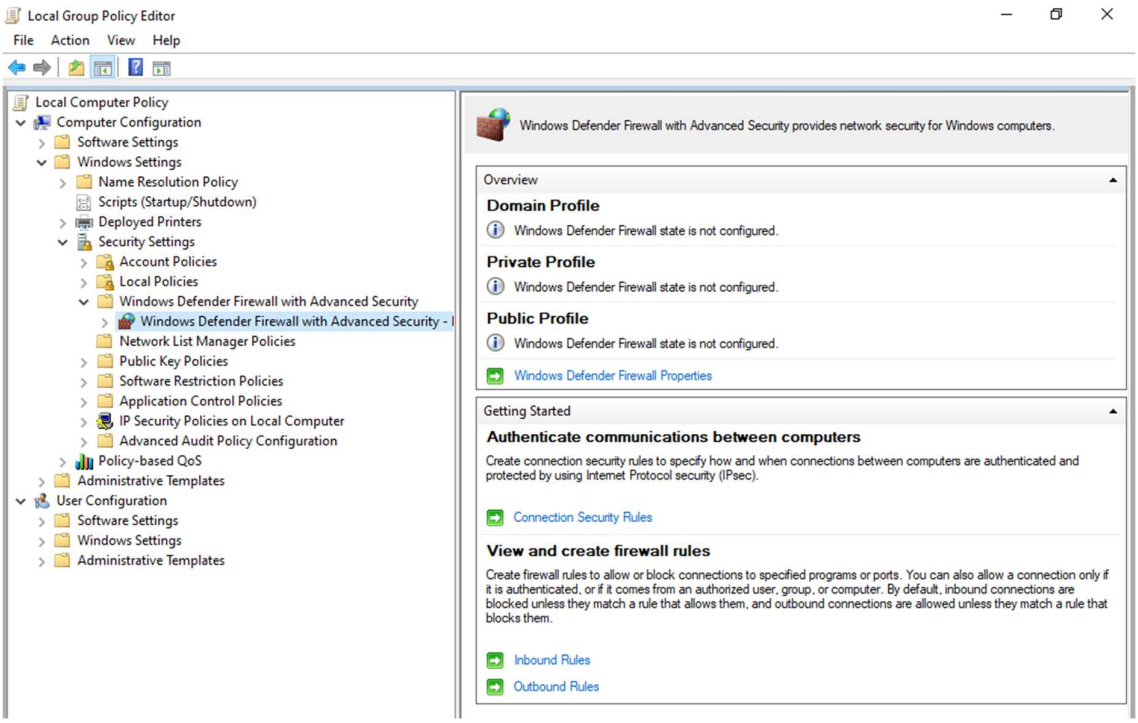
4.4 Account lockout setting



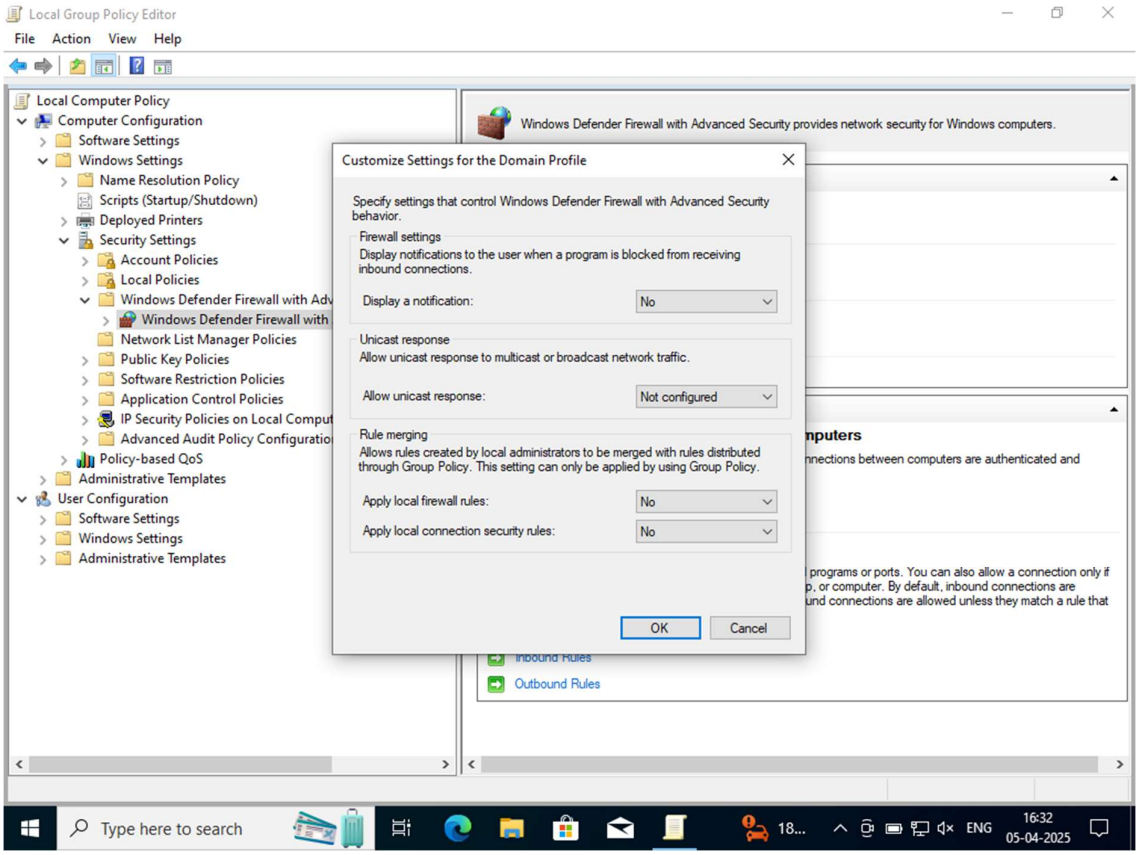
4.5 User Rights Assignments



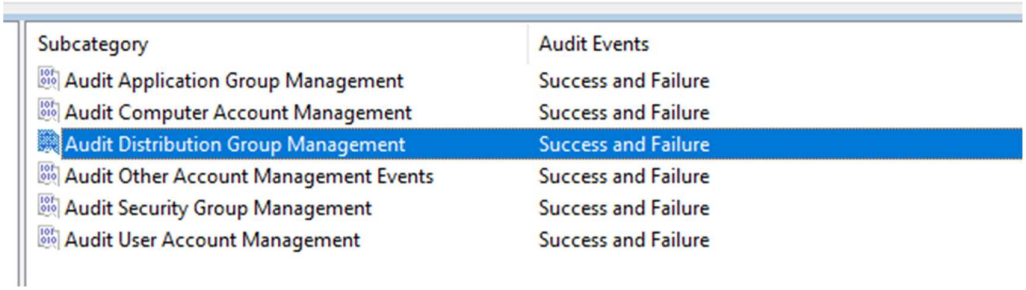
4.6 Rename the administrator account to avoid common names



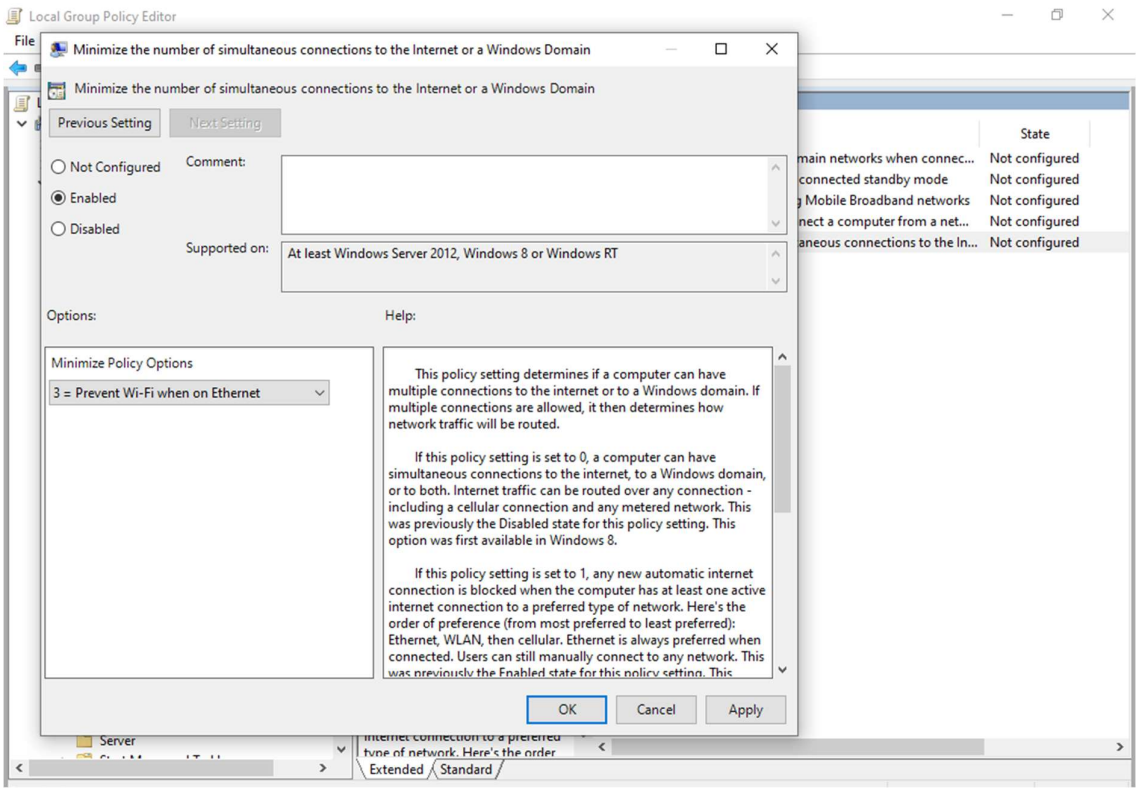
4.7 Windows Defender Firewall



4.8 Edit Firewall Rules According to Assessment Results



4.9 Advanced Audit Policy Configuration under Windows Settings



4.10 Limit simultaneous connections to the Internet Windows Domain

8.4 Post-Hardening Assessment Screenshots

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn.	Man.	Exc.	Score	Max	Percent
1 Automated Checks	9	5	0	0	0	0	8.0	13.0	62%
2 User Survey Questions	30	0	0	0	0	0	30.0	30.0	100%
Total	39	5	0	0	0	0	38.0	43.0	88%

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

Profiles

This benchmark contains 3 profiles.The **Implementation Group 1 for Windows 10 (Full) - Automated Checks and Survey Questions** profile was used for this assessment.

19.7.42 Windows Installer	1	0	0	0	0	0	1.0	1.0	100%
19.7.43 Windows Logon Options	0	0	0	0	0	0	0.0	0.0	0%
19.7.44 Windows Media Player	0	0	0	0	0	0	0.0	0.0	0%
19.7.44.1 Networking	0	0	0	0	0	0	0.0	0.0	0%
19.7.44.2 Playback	0	0	0	0	0	0	0.0	0.0	0%
Total	**289**	**71**	**0**	**0**	**2**	**0**	**289.0**	**360.0**	**80%**

Note: Actual scores are subject to rounding errors. The sum of these values may not result in the exact overall score.

The 'Exc' column only applies to Exceptions that are generated using CIS-CAT Pro Dashboard and is not utilized by CIS-CAT Pro Assessor.

Profiles

This benchmark contains 10 profiles.The **Level 1 (L1) - Corporate/Enterprise Environment (general use)** profile was used for this assessment.

Title	Description
Level 1 (L1) - Corporate/Enterprise Environment (general use)	Items in this profile intend to: • be the starting baseline for most organizations; • be practical and prudent; • provide a clear security benefit; and • not inhibit the utility of the technology beyond acceptable means. Show Profile XML
Level 1 (L1) + BitLocker (BL)	This profile extends the "Level 1 (L1)" profile and includes BitLocker-related recommendations. Show Profile XML
Level 1 (L1) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes Next Generation Windows Security-related recommendations. Show Profile XML
Level 1 (L1) + BitLocker (BL) + Next Generation Windows Security (NG)	This profile extends the "Level 1 (L1)" profile and includes BitLocker and Next Generation Windows Security-related recommendations. Show Profile XML
Level 2 (L2) - High Security/Sensitive Data	This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics:

9. Conclusion

9.1 Summary of Hardening Achievements

The operating system hardening process undertaken during this internship successfully improved the security posture of the Windows 10 machine based on CIS industry standards. Through systematic assessment, vulnerability identification, and remediation based on the **CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0** and the **CIS Controls Assessment Module - Implementation Group 1 (IG1) v1.0.3**, notable compliance improvements were achieved.

Key Achievements:

- **CIS Controls Assessment Module (IG1) Compliance** increased from **60%** (26/43 controls passed) to **88%** (38/43 controls passed), showing an improvement of **+28%**.
- **CIS Microsoft Windows 10 Enterprise Benchmark Compliance** increased from **38%** (5/13 automated checks passed) to **62%** (8/13 automated checks passed), showing an improvement of **+24%**.
- **Critical vulnerabilities**, such as weak password policies, insecure remote desktop configurations, and outdated services like SMBv1, were successfully mitigated.
- **High and Medium severity issues**, including lack of account lockout, disabled firewalls, missing audit policies, and insecure access control configurations, were addressed.

The hardening efforts resulted in a significantly more resilient and secure system, reducing the likelihood of successful ransomware attacks, unauthorized access, malware infections, and insider threats.

9.2 Recommendations for Future Improvements

While substantial progress was made during this project, cybersecurity is a continuous process that requires ongoing vigilance. The following future improvements are recommended to maintain and enhance system security:

- **Implement Multi-Factor Authentication (MFA)** for all administrative and remote access accounts to strengthen authentication mechanisms.
- **Expand hardening** to additional benchmarks beyond IG1, such as **CIS Controls Implementation Group 2 (IG2)** for intermediate cybersecurity maturity.
- **Regularly perform vulnerability assessments** and patch management cycles to address emerging threats promptly.
- **Deploy advanced endpoint protection solutions** for enhanced malware detection and response capabilities.
- **Establish regular backup and disaster recovery testing** to ensure data resilience in case of system failure or ransomware attacks.
- **Enhance user awareness** through security training programs to minimize risks from phishing and social engineering attacks.
- **Schedule quarterly CIS-CAT reassessments** to ensure continued compliance and adapt security configurations as per evolving threats.

By following these recommendations, the system's cybersecurity defenses will be maintained at a high standard, and it will remain resilient against both current and future attack vectors.

Lessons Learned:

Performing the CIS-CAT assessment and system hardening process taught me the significance of baseline security standards in safeguarding an operating system. I understood how each hardening step, from enforcing password policies to configuring firewalls and audit policies, collectively strengthens system security. This experience emphasized the need for continuous security assessments, timely patch management, and adherence to best practices to maintain a strong cybersecurity posture.

10. References

1. Centre for Internet Security (CIS) Benchmarks –
   CIS Microsoft Windows 10 Enterprise Benchmark v3.0.0
   https://www.cisecurity.org/insights/blog/cis-benchmarks-march-2024-update
2. Centre for Internet Security (CIS) Controls –
   CIS Controls Implementation Group 1 for Windows 10 v1.0.3
   https://www.cisecurity.org/controls
3. CIS-CAT Lite Assessor Tool –
   Official CIS-CAT Lite Tool Documentation
   https://learn.cisecurity.org/cis-cat-lite
4. Microsoft Documentation –
   Windows 10 Security Best Practices
   https://learn.microsoft.com/en-us/windows/security/
5. National Institute of Standards and Technology (NIST) –
   Framework for Improving Critical Infrastructure Cybersecurity
   https://www.nist.gov/cyberframework
6. NIST Special Publication 800-63B –
   Digital Identity Guidelines
   https://pages.nist.gov/800-63-3/sp800-63b.html
7. Microsoft Security Advisories –
   Protect against ransomware (WannaCry)
   https://www.microsoft.com/en-us/industry/blog/healthcare/2017/06/06/wannacry-ransomware-attack-lessons-learned/
8. CISA –
   Remote Desktop Vulnerability (BlueKeep) Advisory
   https://www.cisa.gov/news-events/cybersecurity-advisories/aa19-168a
9. NIST Special Publication 800-92 –
   Guide to Computer Security Log Management
   https://csrc.nist.gov/publications/detail/sp/800-92/final

11. Appendix A: CIS-CAT Full Assessment Reports

CIS-CAT Full Assessment Reports Archive

This archive contains:

- Initial CIS-CAT Assessment Report (before hardening)
- Post-Hardening CIS-CAT Assessment Report (after implementing mitigations)
- Raw .html and .xml files generated by CIS-CAT
- Additional screenshots and evidence

🔗 **Download Link:** CIS-CAT-Assessment-Reports.zip

https://drive.google.com/file/d/1-Mn8Sh5zesEOLM3AhaqYyb_3H0RTOCkJ/view?usp=sharing