Student:	Email:
Matias Kun	rvh4zx@virginia.edu

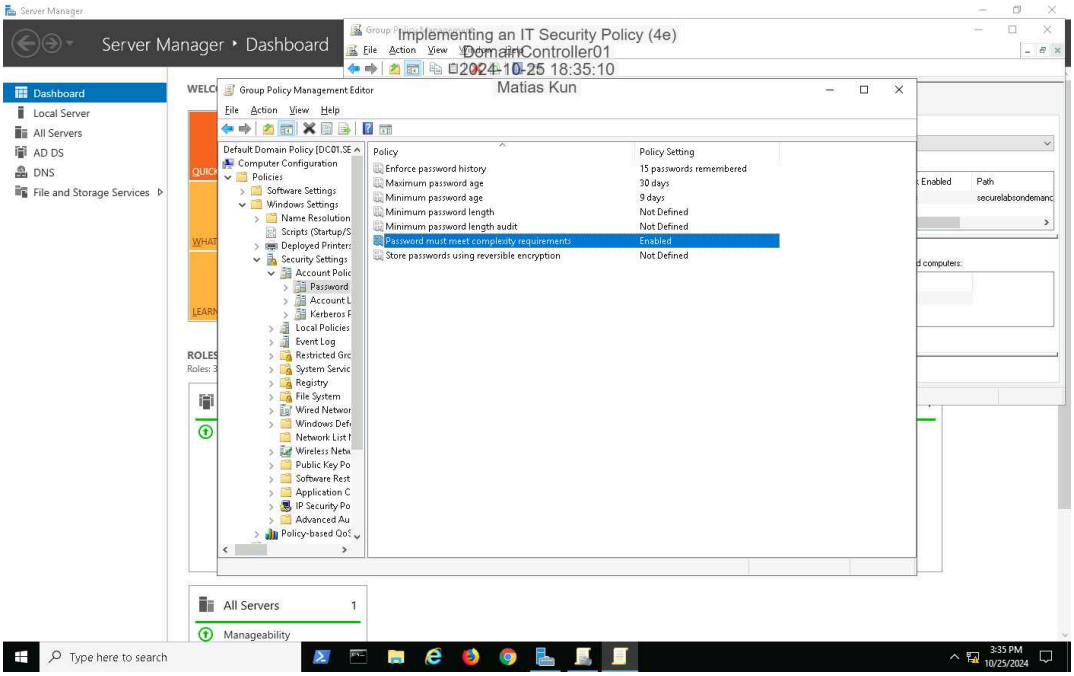
Time on Task:	Progress:
2 hours, 48 minutes	100%

Report Generated: Tuesday, October 29, 2024 at 12:16 PM

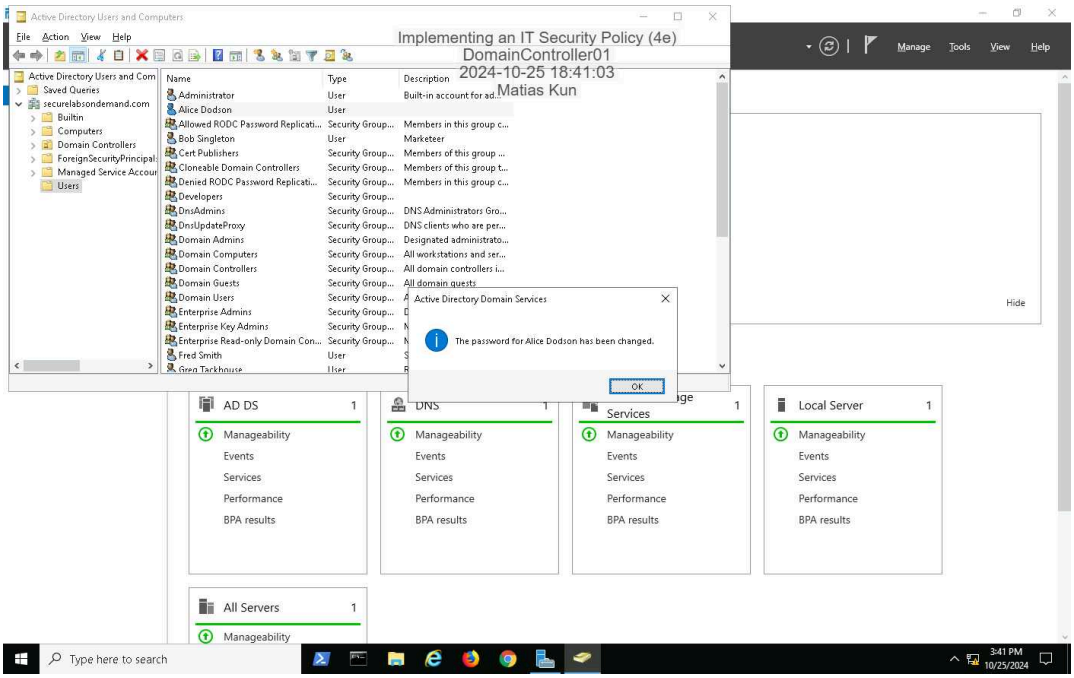
Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

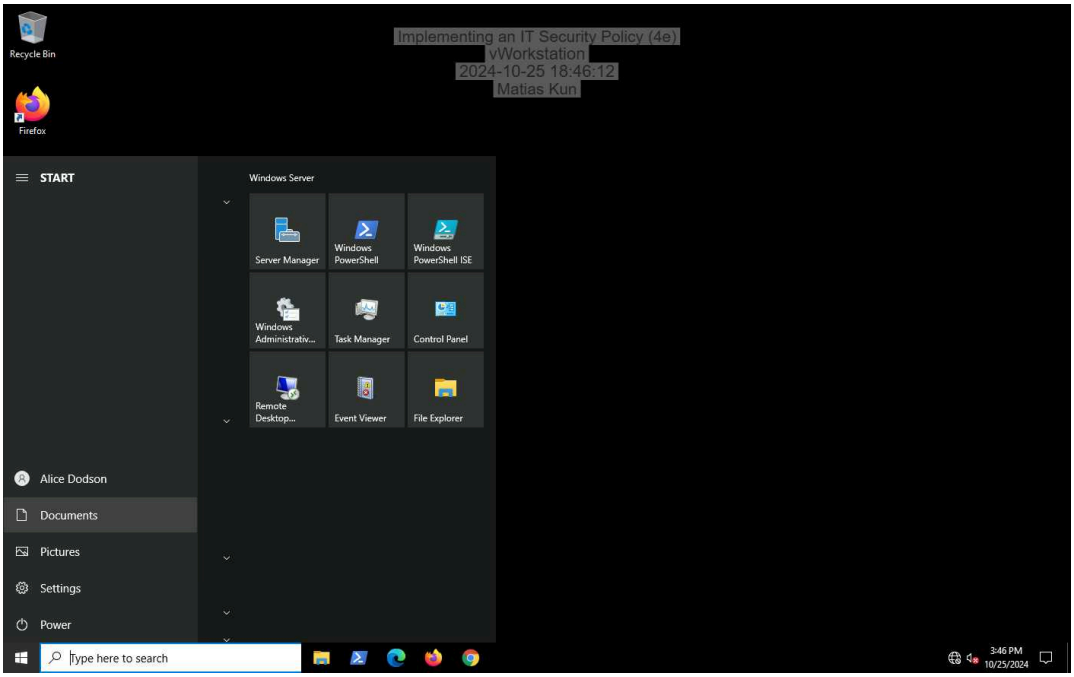
16. **Make a screen capture** showing the **newly configured Domain Password Policy settings**.



28. **Make a screen capture** showing the **successful password change message**.

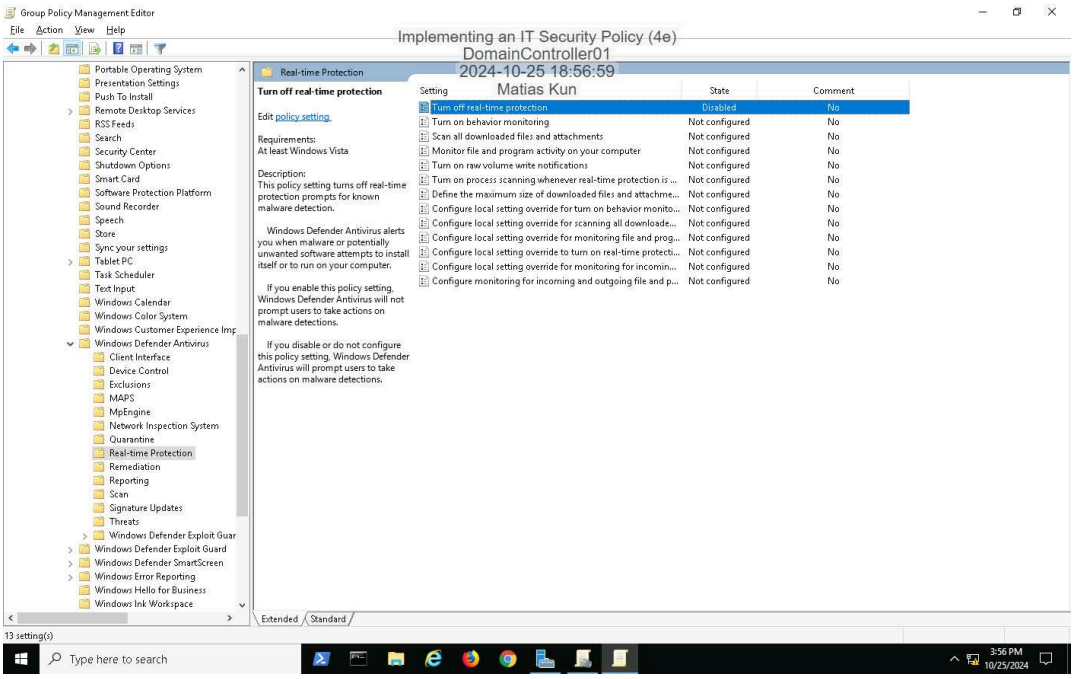


36. **Make a screen capture** showing the **logged on user account**.

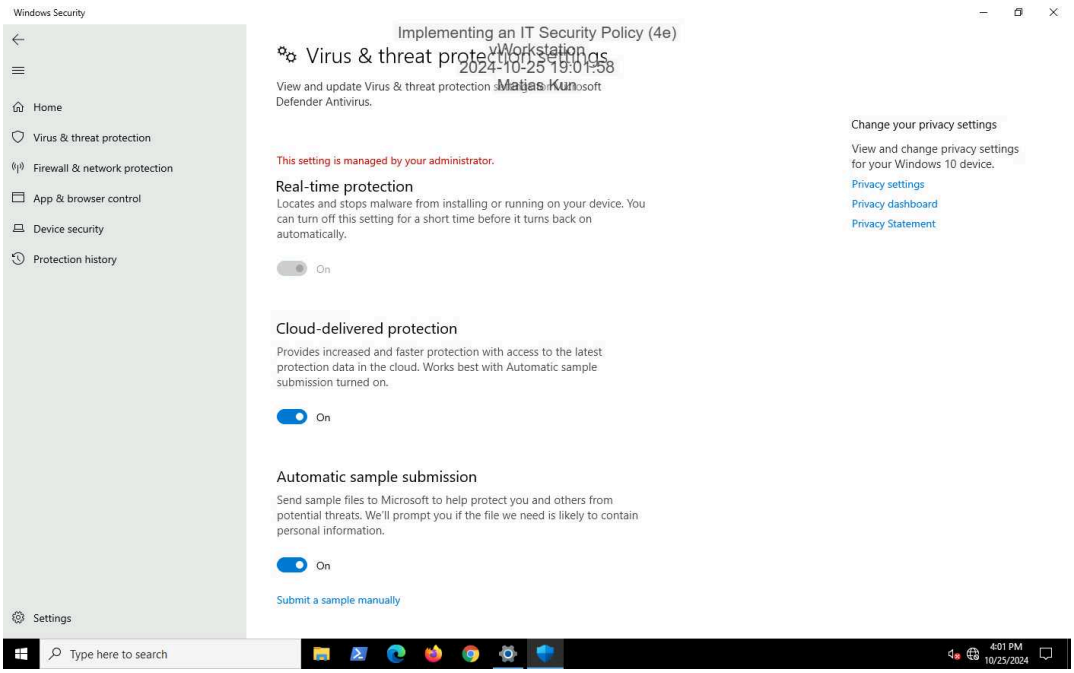


Part 2: Implement an Antivirus Policy

16. **Make a screen capture** showing the **newly configured Domain Real-time protection Policy settings.**



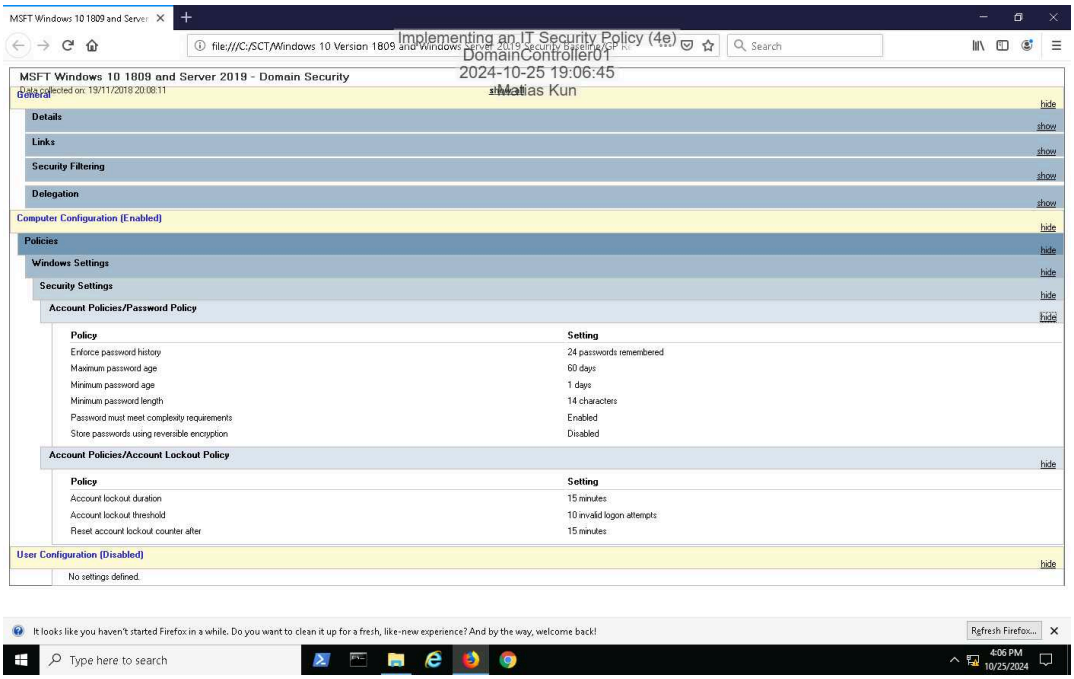
25. **Make a screen capture** showing the **grayed-out real-time threat protection settings**.



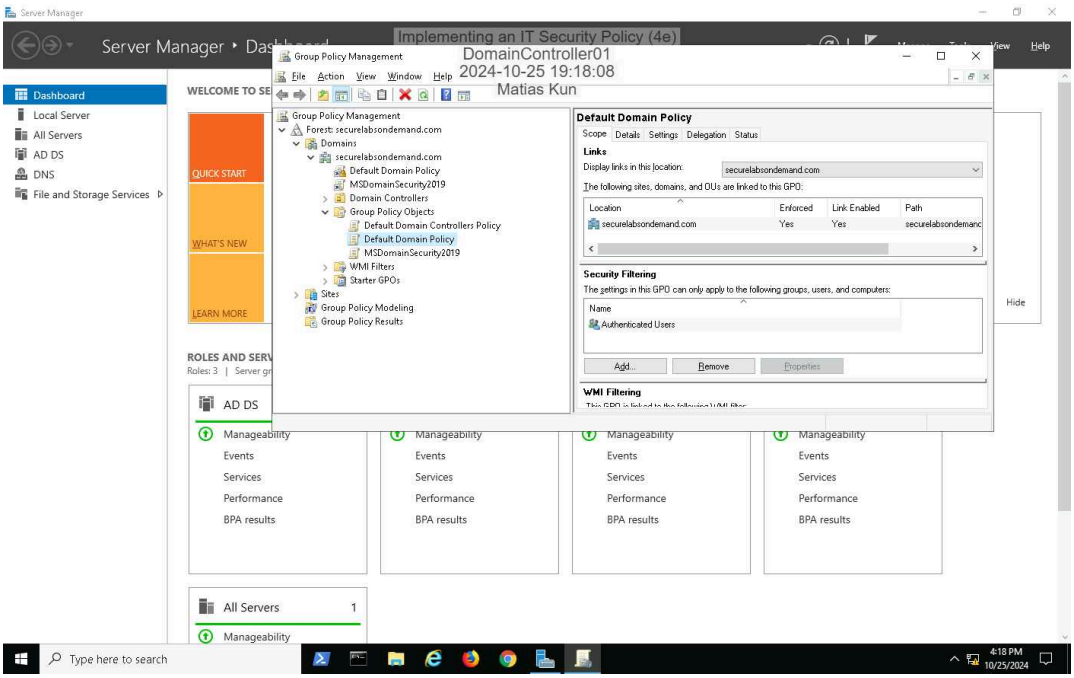
Section 2: Applied Learning

Part 1: Apply a Windows Security Baseline

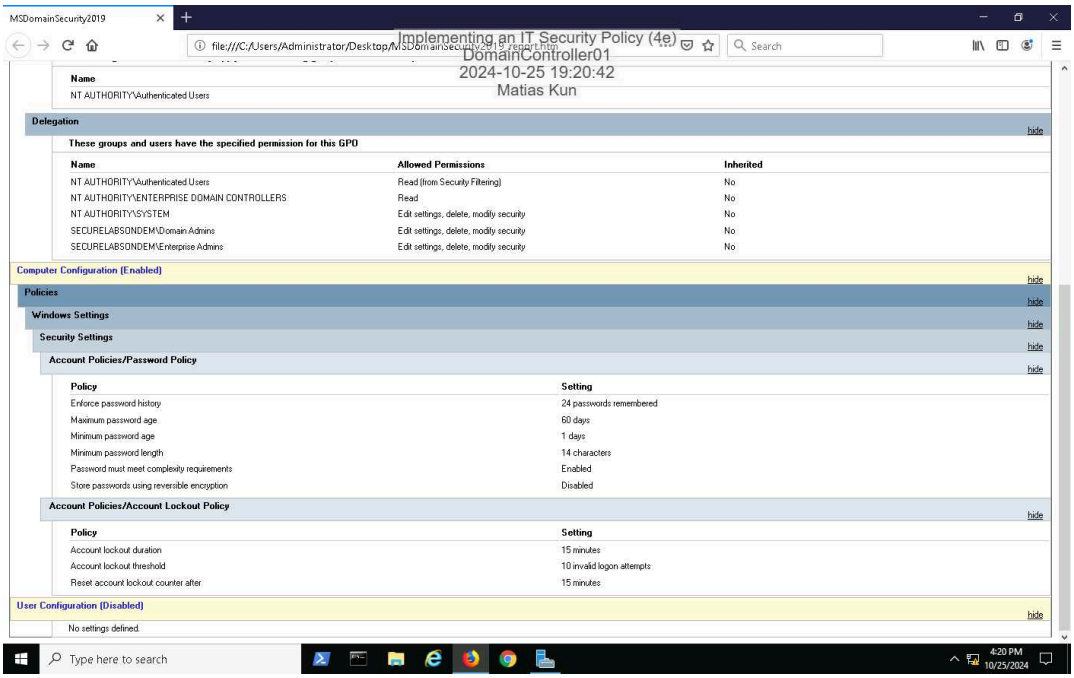
6. **Make a screen capture** showing **Microsoft's recommended Password and Account Lockout policy settings**.



19. **Make a screen capture** showing the **linked MSDomainSecurity2019 object**.

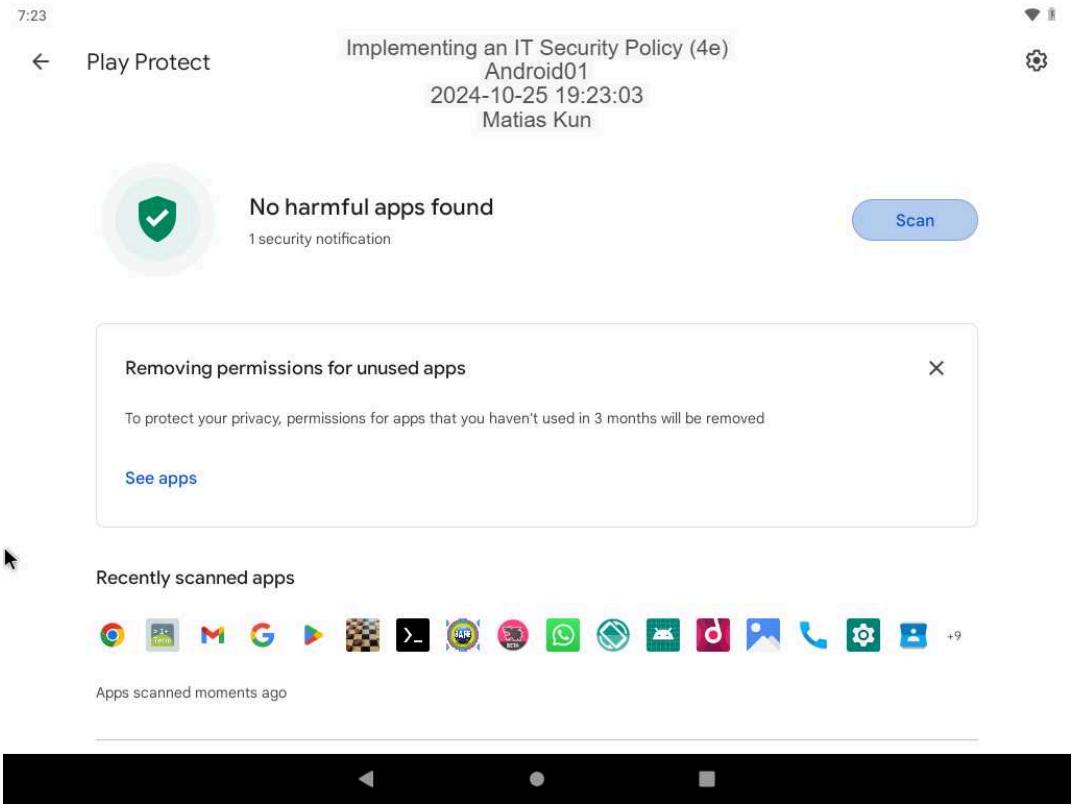


23. **Make a screen capture** showing the **Password and Account Lockout policy settings**.

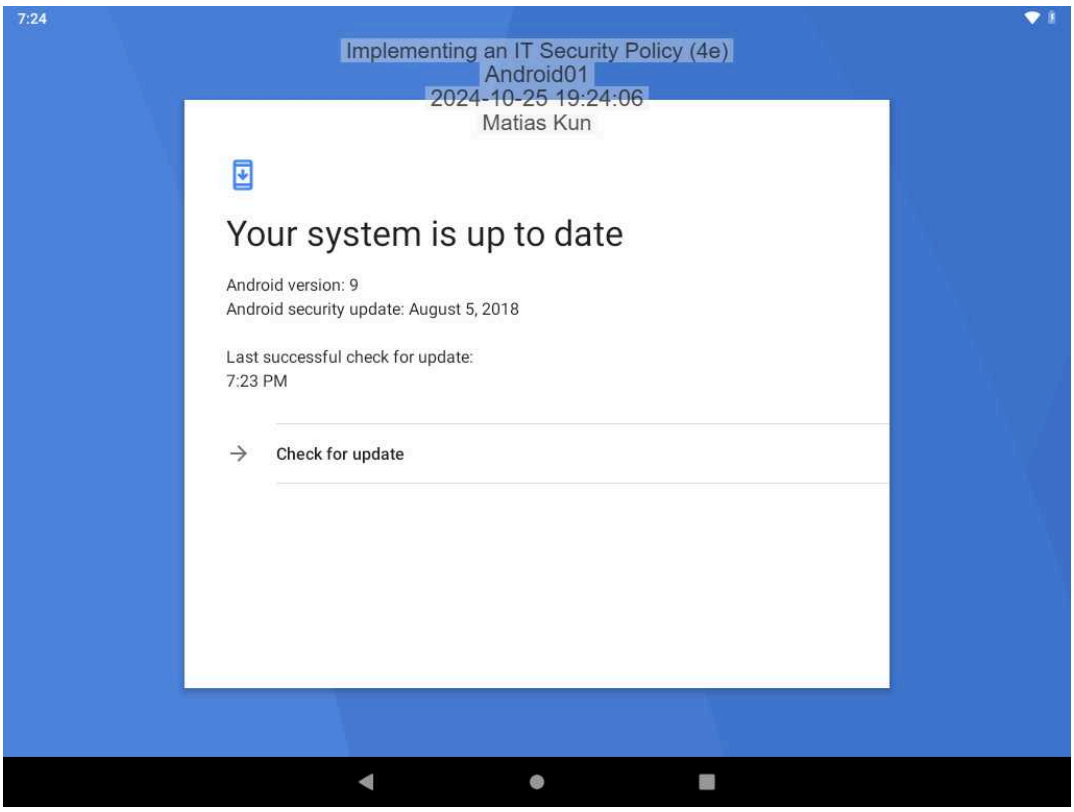


Part 2: Implement a Mobile Device Security Policy

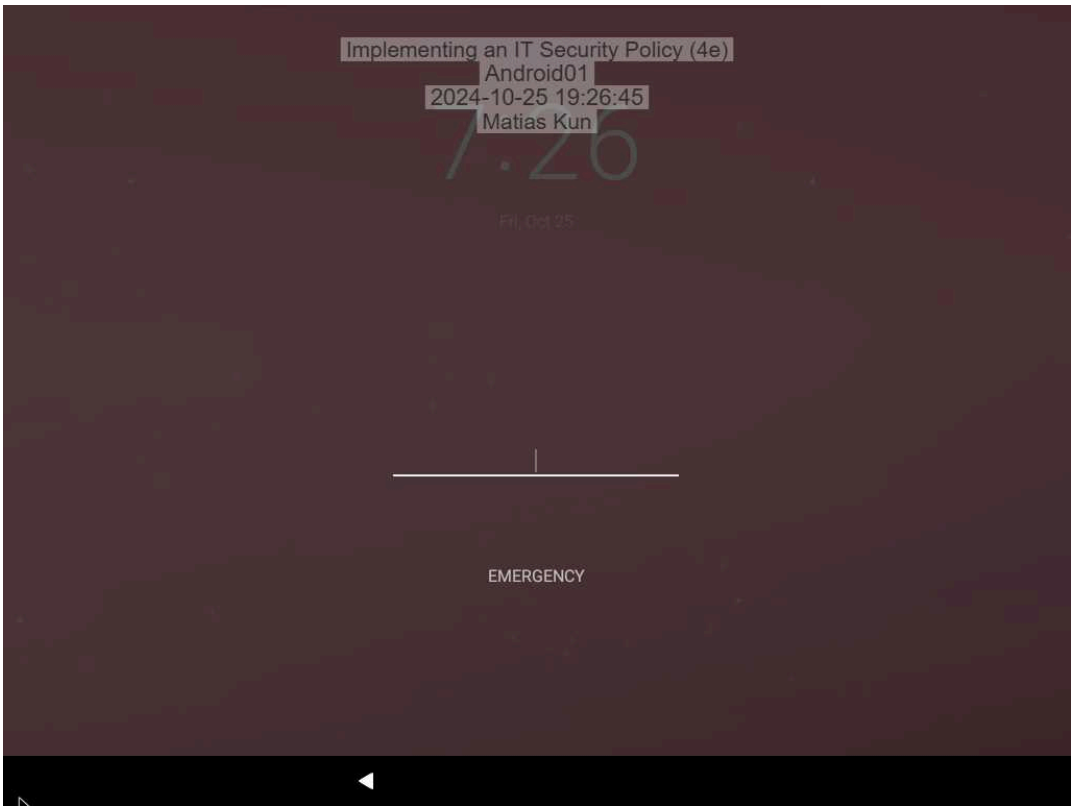
7. **Make a screen capture** showing the **results of the Google Play Protect scan**.



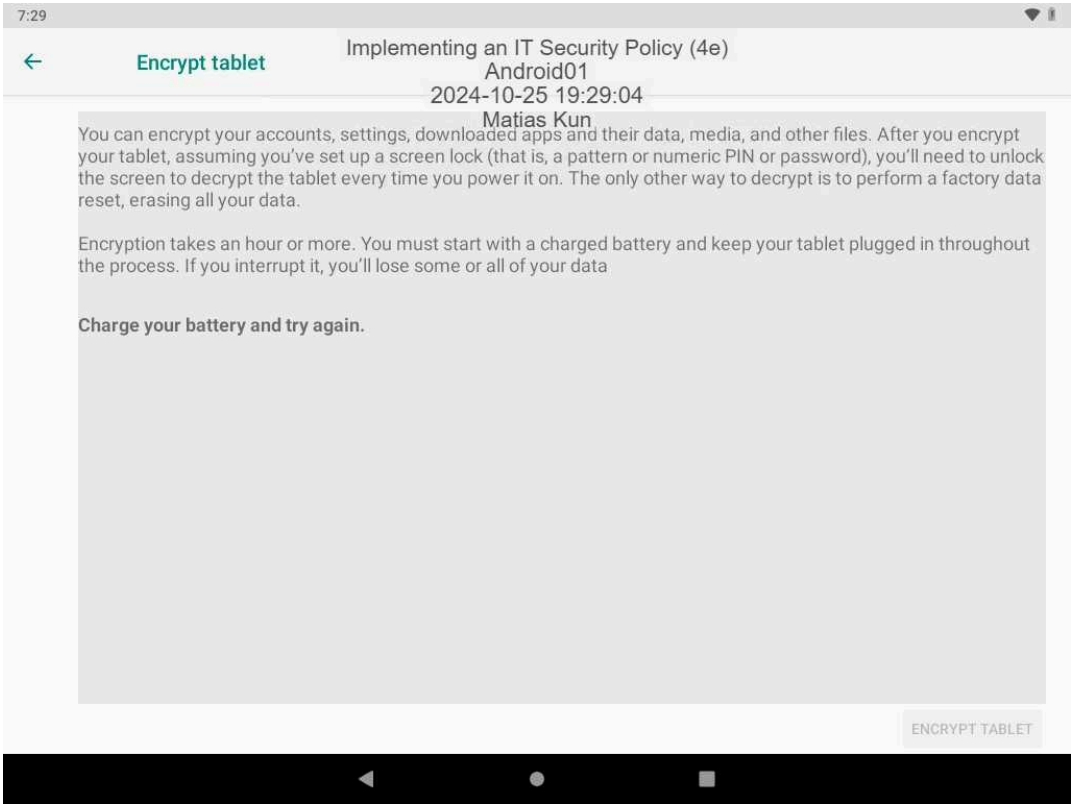
11. **Make a screen capture** showing the **updated "last successful check for update" timestamp**.



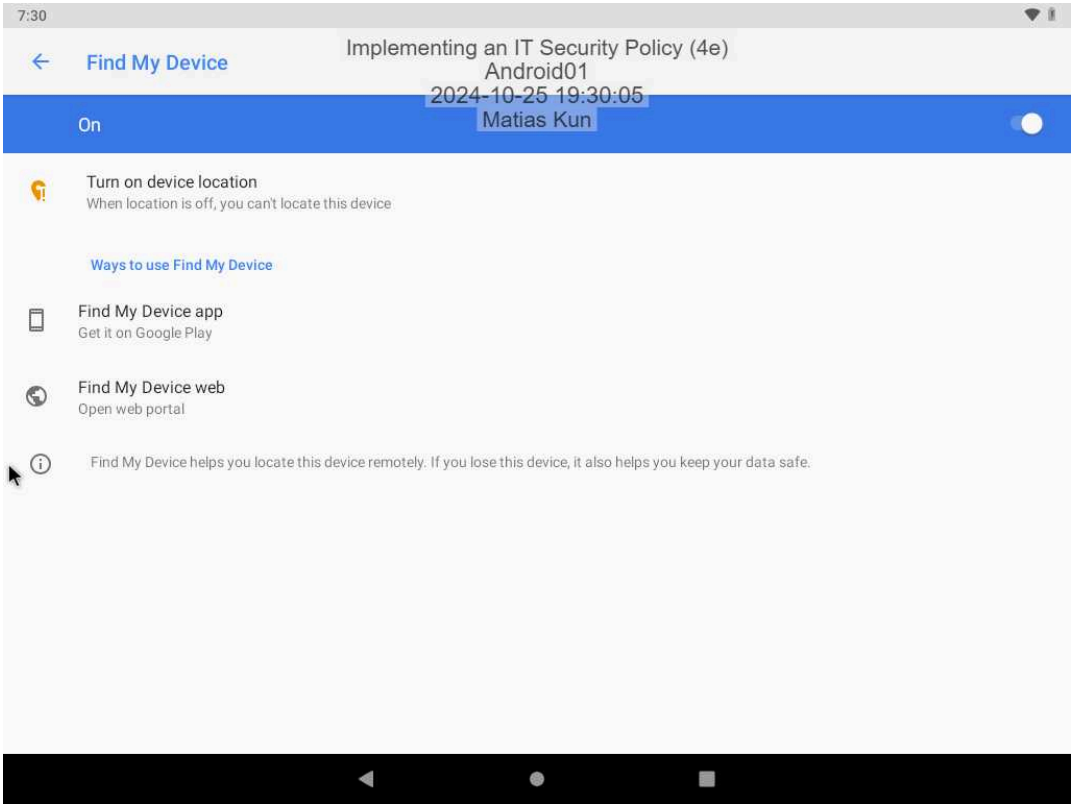
19. **Make a screen capture** showing the **Android lock screen**.



25. **Make a screen capture** showing the **encryption set-up explanation**.



27. **Make a screen capture** showing the **Find My Device settings**.



Section 3: Challenge and Analysis

Part 1: Research Acceptable Use Policies

Using the Internet, **research** Acceptable Use Policies, then **identify** at least five common policy statements and **explain** their significance. Be sure to cite your sources.

Prohibition of Illegal Activities: Most AUPs prohibit illegal actions, such as unethical hacking (black-hat-hacking) and unauthorized access. This is vital for maintaining the organization's integrity, reducing legal risks, and ensuring a secure working environment (University of Tennessee, 2023). Restricted Use of Company Resources: AUPs often require that company resources, such as networks and equipment, are used exclusively for work-related purposes. This reduces distractions, optimizes bandwidth, and keeps resources available for professional activities (University of Tennessee, 2023). Cybersecurity Practices: AUPs often include guidelines on password management, data encryption, and other security practices, and they will continually update resources as standards evolve. These requirements prevent data breaches and safeguard sensitive information, thereby reducing vulnerability to cyber threats (University of Tennessee, 2023). Remote Work and BYOD Policies: As remote work has become more common, AUPs often address device security and network access for remote work. This can include requirements for VPNs and specific security measures to prevent unauthorized access from non-secure networks (University of Tennessee, 2023). Consequences of Non-Compliance: Many AUPs outline specific consequences for violations, which could include disciplinary action up to termination. This reinforces the policy's importance and accountability standards, protecting both the organization and its employees (University of Tennessee, 2023). Reference: University of Tennessee. (2023). Understanding Acceptable Use Policies. Retrieved October 25, 2024, from https://oit.utk.edu/security/learning-library/article-archive/understandinig-aups/

Part 2: Research Privacy Policies

Using the Internet, **research** user Privacy Policies, then **identify** at least five common policy statements and **explain** their significance. Be sure to cite your sources.

Data Collection and Use: Privacy policies explain what data is collected and how it's used, such as for analytics or user experience improvements (quality assurance). This transparency helps build trust and ensures compliance with data protection laws (PrivacyPolicies, 2023). Consent for Data Processing: Policies frequently require user consent for data collection and processing, ensuring compliance with privacy laws like GDPR and respecting user control over personal data (PrivacyPolicies, 2023). Third-Party Data Sharing: Privacy policies often state whether user data is shared with third parties, such as advertising or service partners, so users are aware and can make informed decisions (PrivacyPolicies, 2023). Security Practices: Privacy policies outline the measures used to safeguard data, such as encryption or restricted access. This assurance supports user confidence in the company's data handling practices (PrivacyPolicies, 2023). User Data Rights: Many privacy policies inform users of their rights, including access, correction, or deletion of their data, which fosters transparency and supports regulatory compliance (PrivacyPolicies, 2023). Reference: PrivacyPolicies. (2023). What is a Privacy Policy? Retrieved October 25, 2024, from https://www.privacypolicies.com/blog/what-is-privacy-policy/