Student:	Email:
Sadam Hashi	smhashi@asu.edu

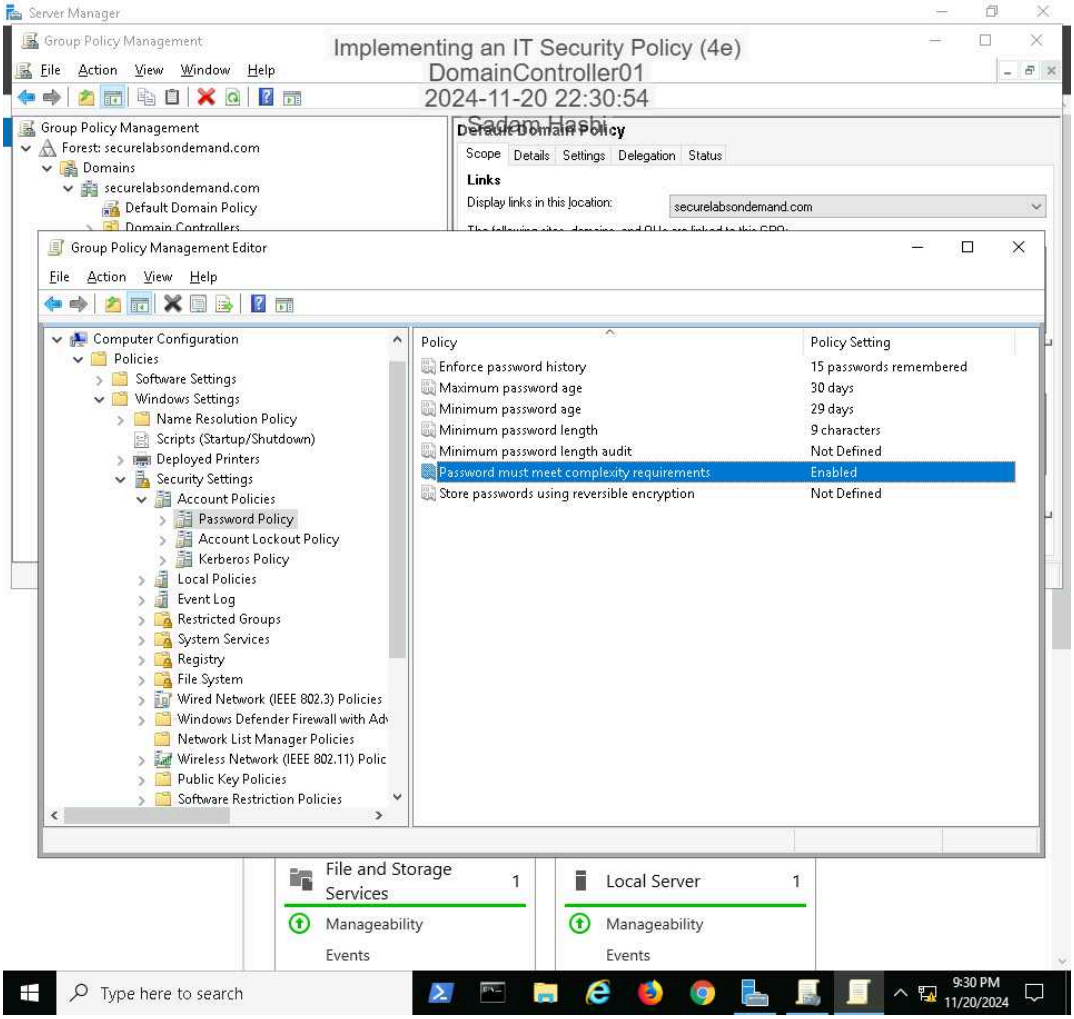
Time on Task:	Progress:
5 hours, 56 minutes	100%

Report Generated: Friday, November 22, 2024 at 3:09 AM

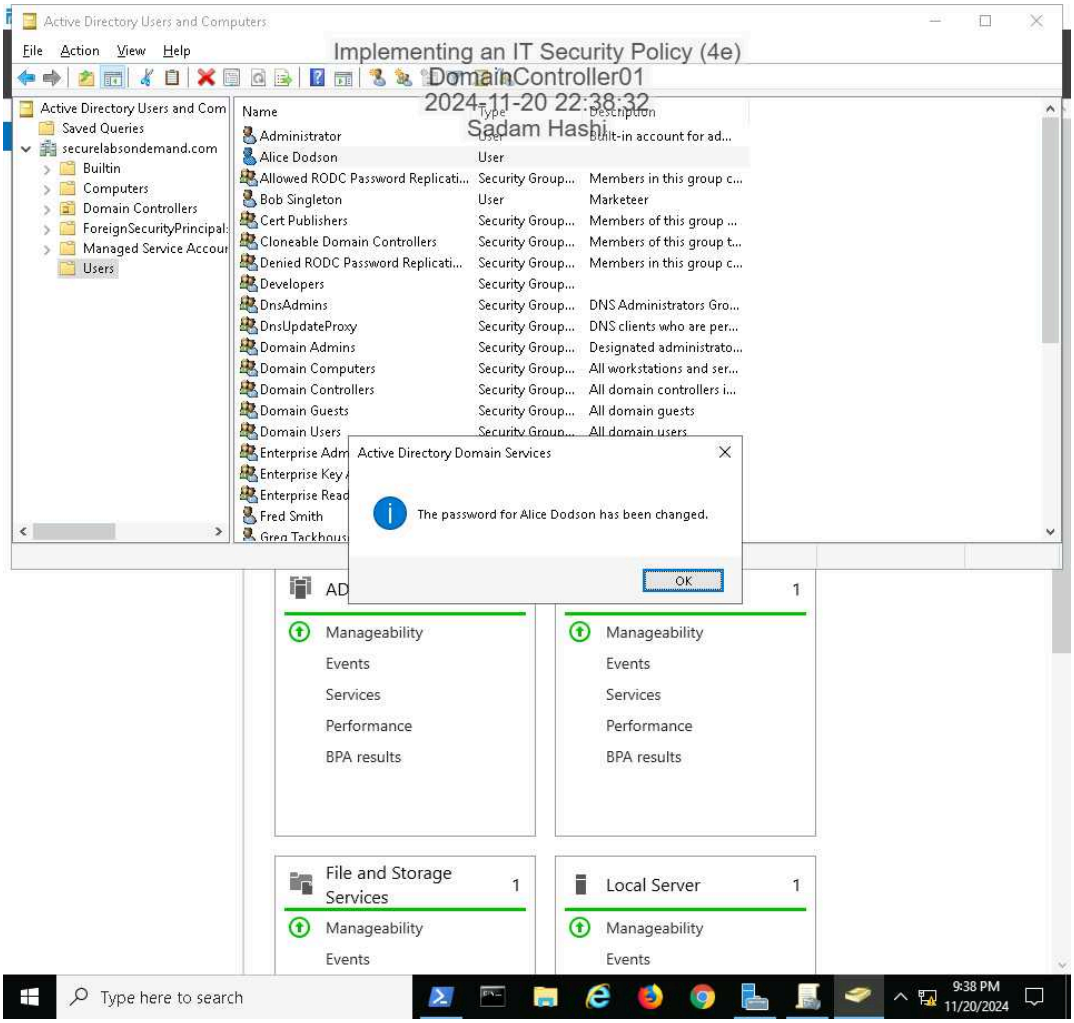
Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

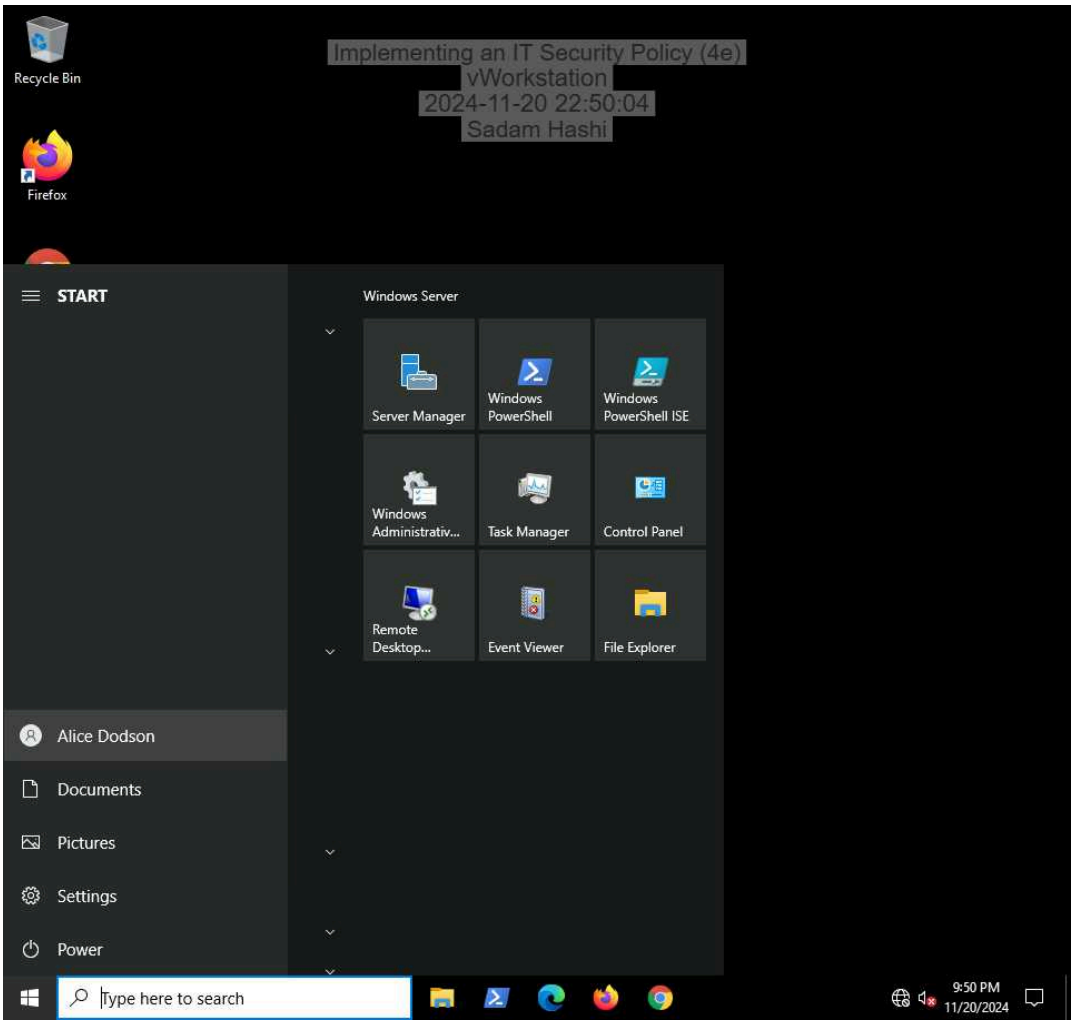
16. **Make a screen capture** showing the **newly configured Domain Password Policy settings**.



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

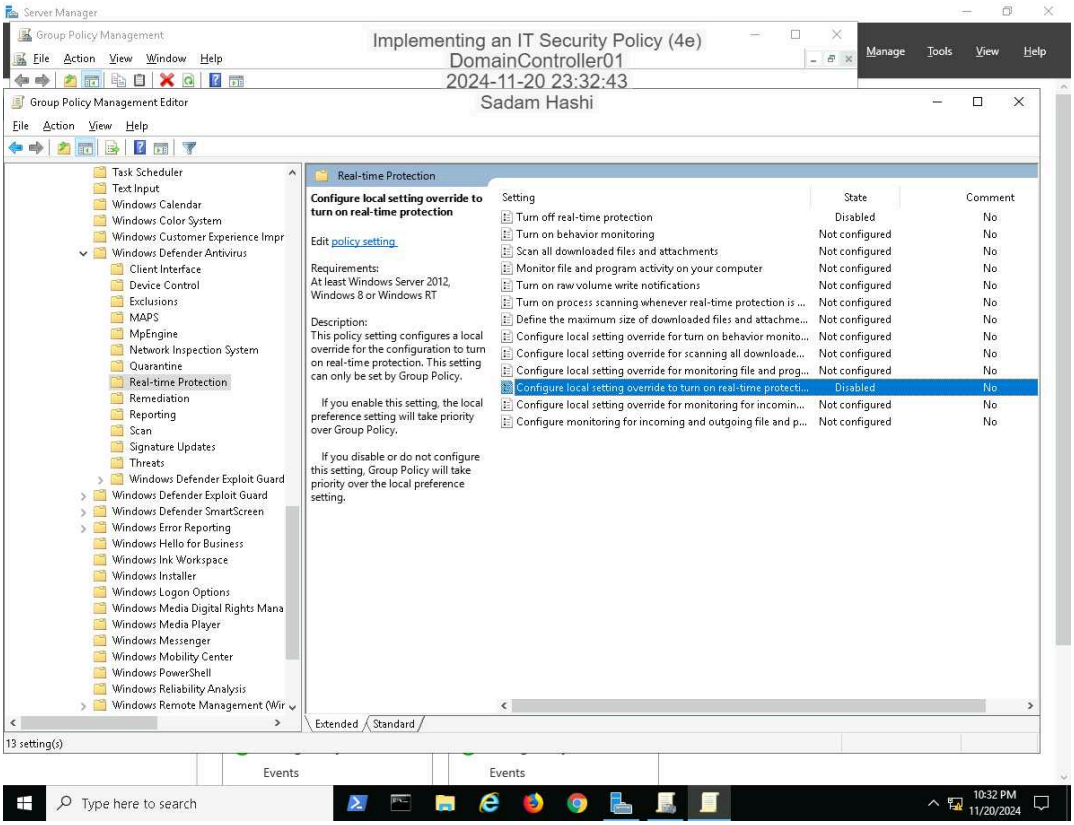


36. **Make a screen capture** showing the **logged on user account**.

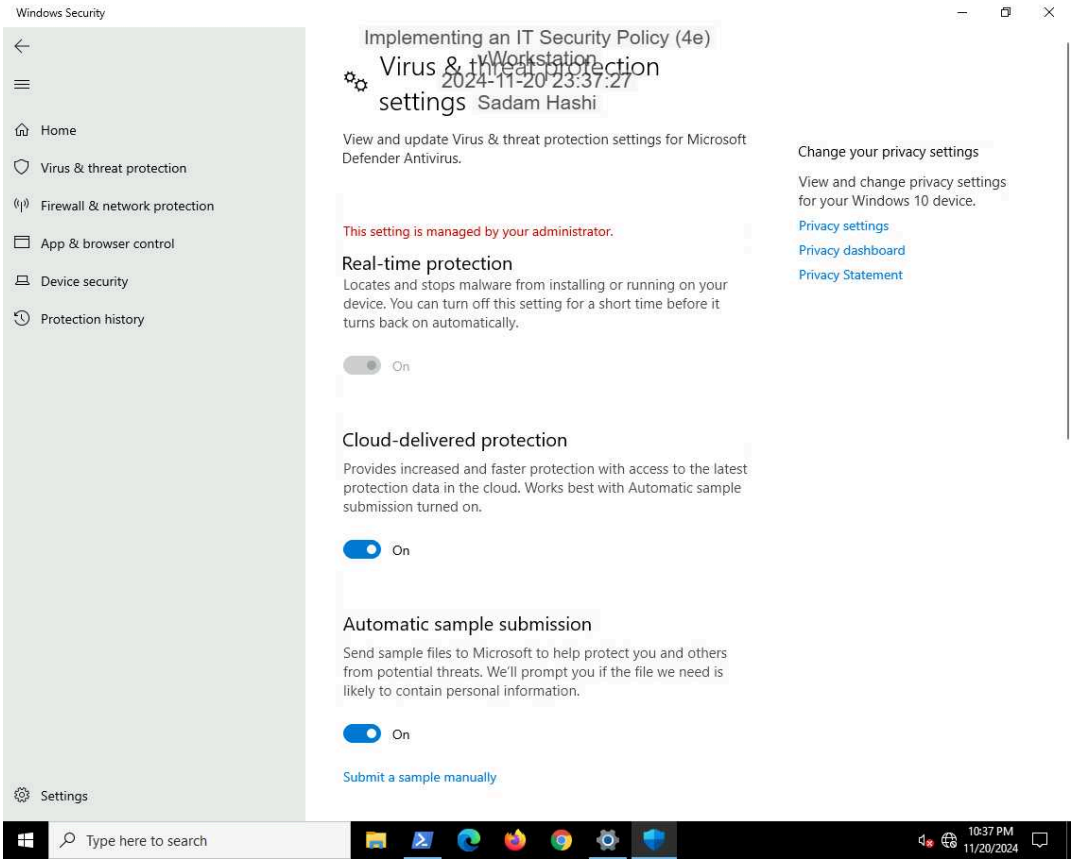


Part 2: Implement an Antivirus Policy

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



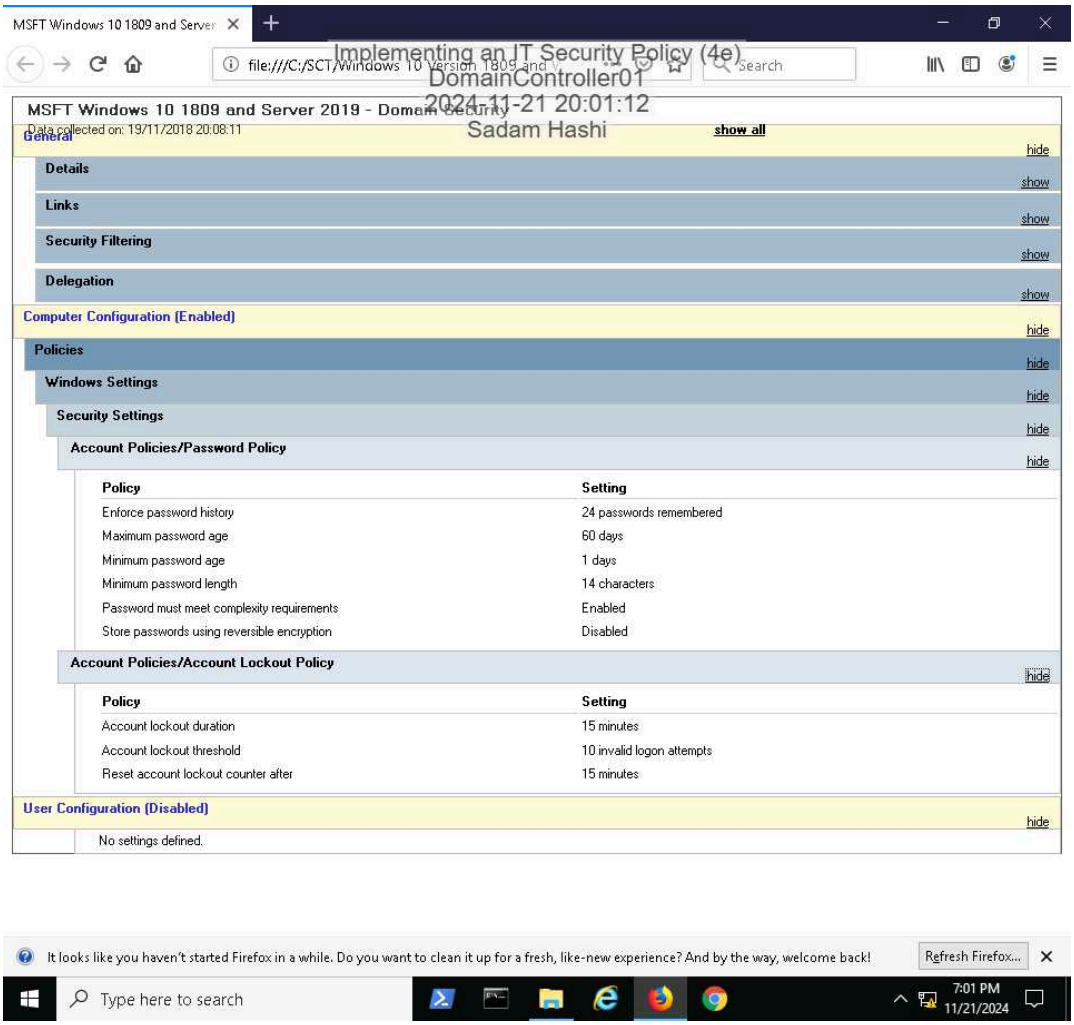
25. **Make a screen capture** showing the **grayed-out real-time threat protection settings**.



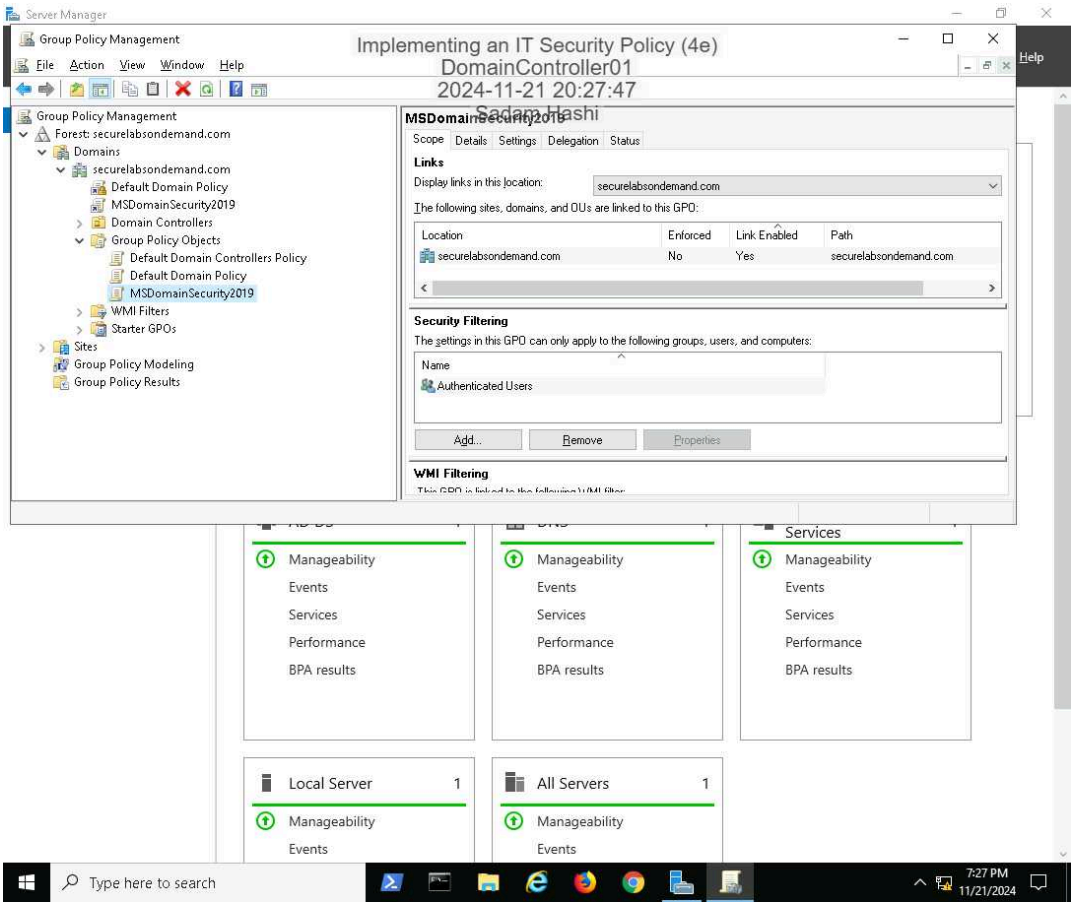
Section 2: Applied Learning

Part 1: Apply a Windows Security Baseline

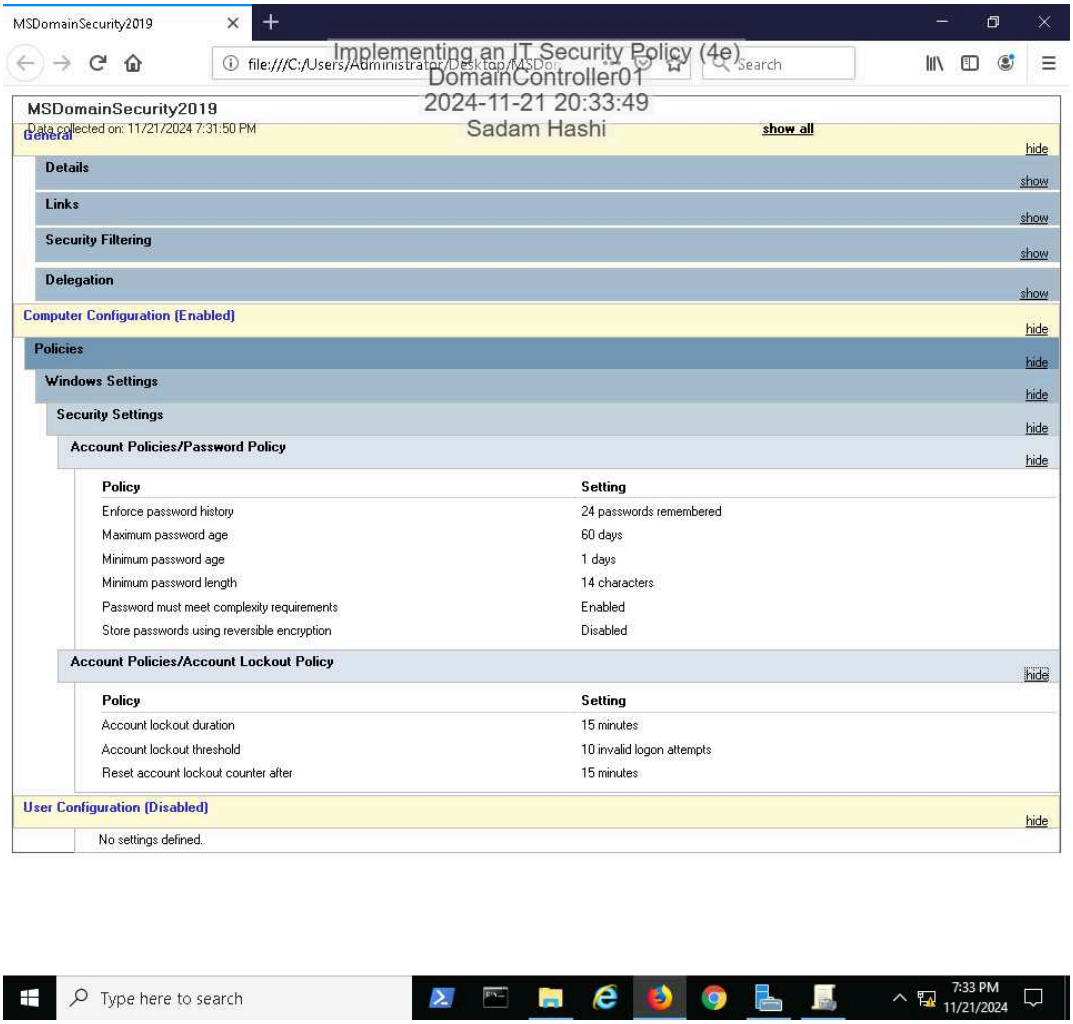
6. **Make a screen capture** showing **Microsoft's recommended Password and Account Lockout policy settings**.



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

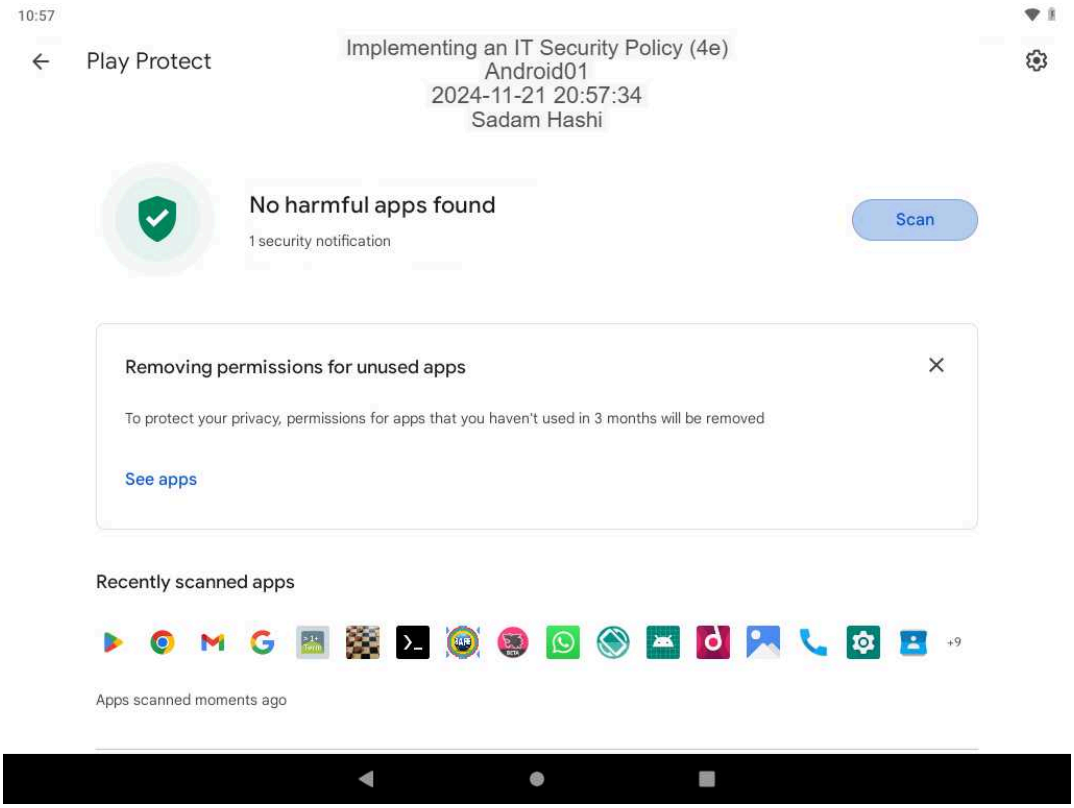


23. **Make a screen capture** showing the **Password and Account Lockout policy settings**.

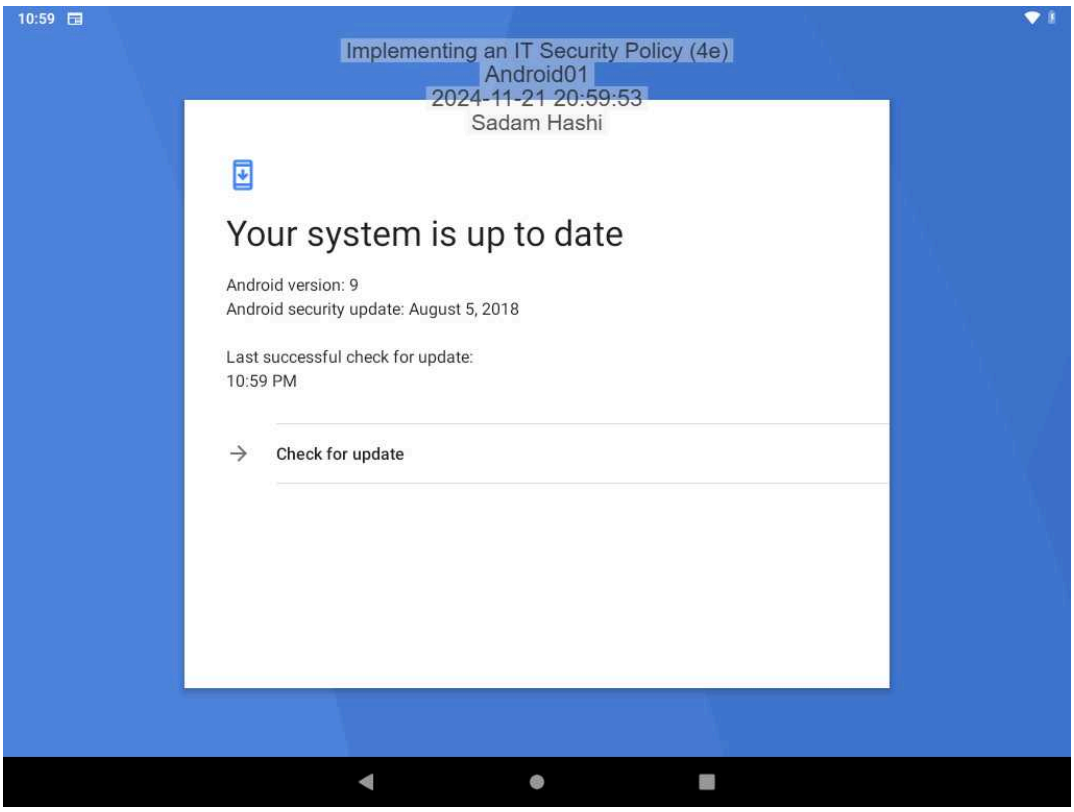


Part 2: Implement a Mobile Device Security Policy

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

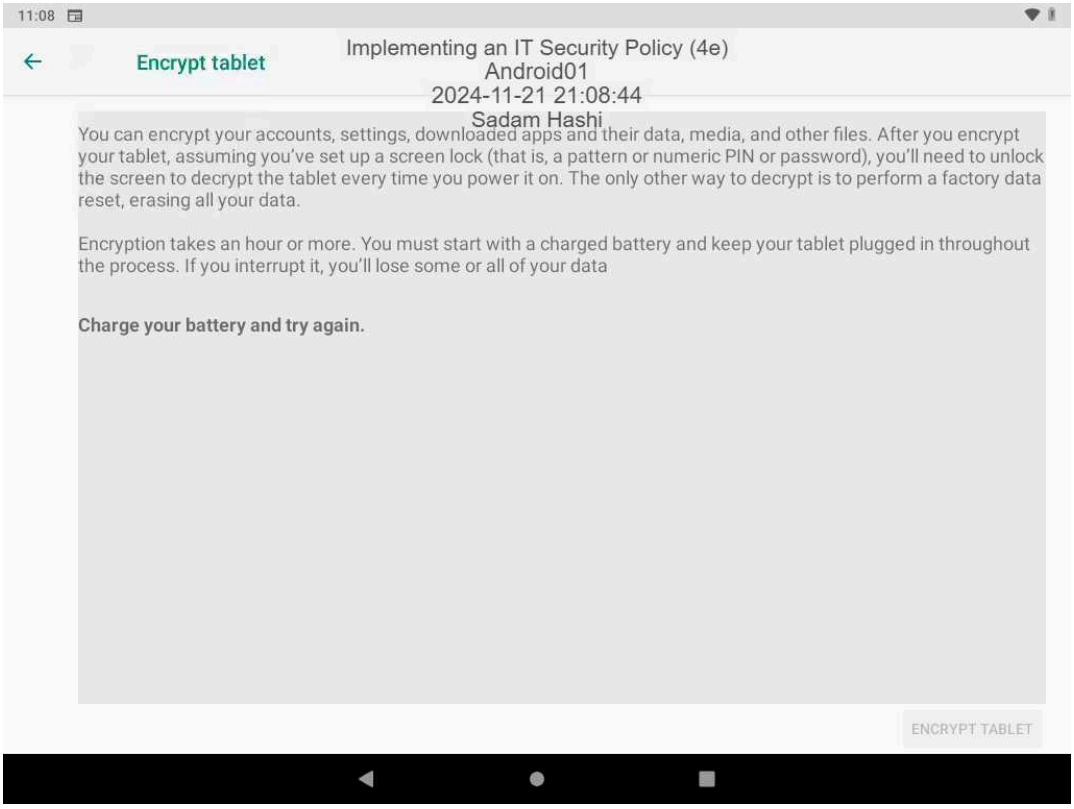


11. **Make a screen capture** showing the **updated "last successful check for update" timestamp**.

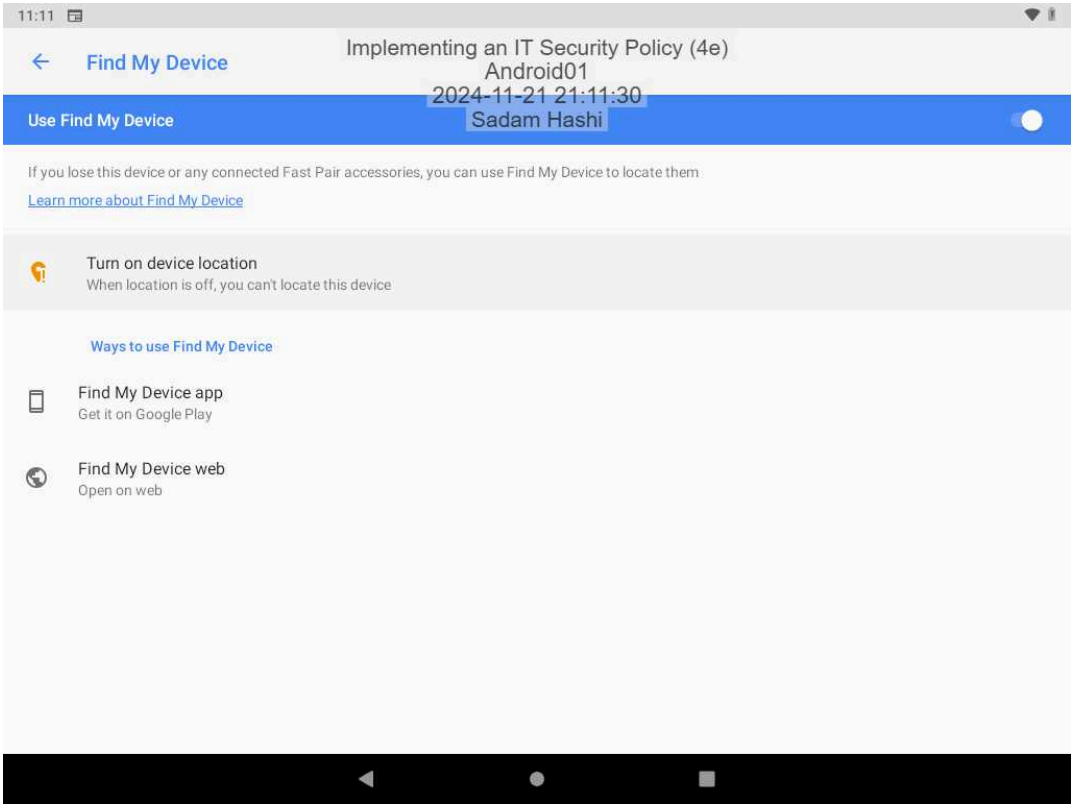


19. **Make a screen capture** showing the **Android lock screen**.

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.

1. Data Protection and Privacy Compliance - This refers to best practices and policies companies need to follow due to legal regulations. The companies need to comply with protections laws set by GDPR, HIPPA, etc.
2. Consequences for Policy Violations - This underlines the consequences of violating AUP, which include disciplinary actions such as termination of employment, suspension or even legal action. This deters users of the resources to break the law.
3. Bring Your Own Device(BYOD) - This rule entails the user the security measure to follow when their personal device is brought to working environment. This often requires the usage of VPNs for data protection.
4. Software Usage - This restricts employees or users from installing unauthorized software in the a company's software. This includes users using the software for personal gains, and this protects a company from threats.
5. Email and Communication - This rule requires a company's email system to be under strict guidelines. This prevents the sending of spam, or inappropriate content to minimize legal retaliations from any affected third-party group.

Sources:

Aware. “Acceptable Use Policy: What It Is and Why You Need It.” Www.awarehq.com, www.awarehq.com/blog/acceptable-use-policy.
“Crafting an Effective Acceptable Use Policy: Best Practices for Businesses.” TrustCommunity, 19 Aug. 2024, community.trustcloud.ai/docs/grc-launchpad/grc-101/governance/crafting-an-effective-acceptable-use-policy-best-practices-for-businesses/.

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.

1. User Rights - This often highlights a user's rights such as engaging to delete certain data or opting out if it. This is heavily regulated by government agencies such as GDPR, and it helps empower a user and be confident in using an organization's technology.
2. Data Collection - This explains the collected data, whether that is a user's name or IP address. By providing this, their is transparency which helps understand how what of their personal data is collected.
3. Data Storage and Protection - This ensures a user's data is protected from theft and that their are safeguards in place to achieve this. An authorized access or breaches are protected from the user, which in return helps the user feel reassured.
4. Updates To The Policy - If a the current privacy policy is updated, the users will be informed about such changes. This statement maintains the users trust and also helps organization comply with existing laws.
5. Data Sharing And Third Parties - An organization must specify if the collected data of the users are shared with any third parties. This information must be disclosed to the user including what type of collected data is being shared. An organization can assure users to not share any of their data in the established policy.

Sources:

Lane, Amanda. “How to Lock Your Digital Door: Data Privacy Best Practices in 2024.” Salesforce, 7 Feb. 2024, www.salesforce.com/blog/data-privacy-best-practices/.
“9 Things to Include in a Privacy Policy.” Www.contractscounsel.com, www.contractscounsel.com/b/9-things-to-include-in-a-privacy-policy.