Implementing an IT Security Policy (4e)

Fundamentals of Information Systems Security, Fourth Edition - Lab 07

Student:	Email:
Jamal Sherif	jamalsherif2@gmail.com

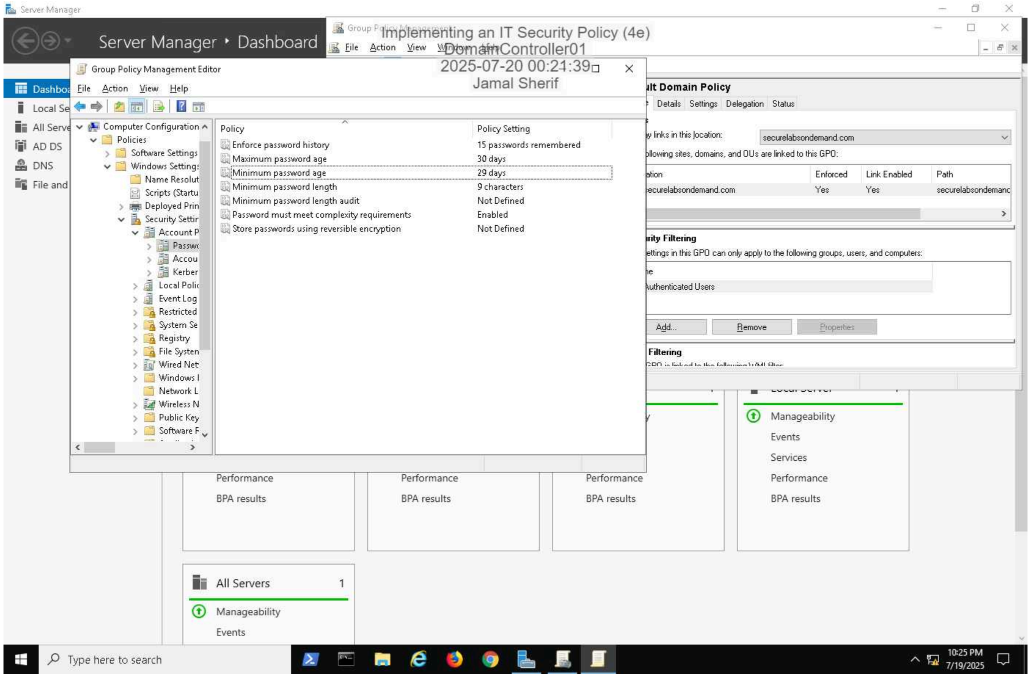
Time on Task:	Progress:
1 hour, 54 minutes	93%

Report Generated: Thursday, October 2, 2025 at 9:39 PM

Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

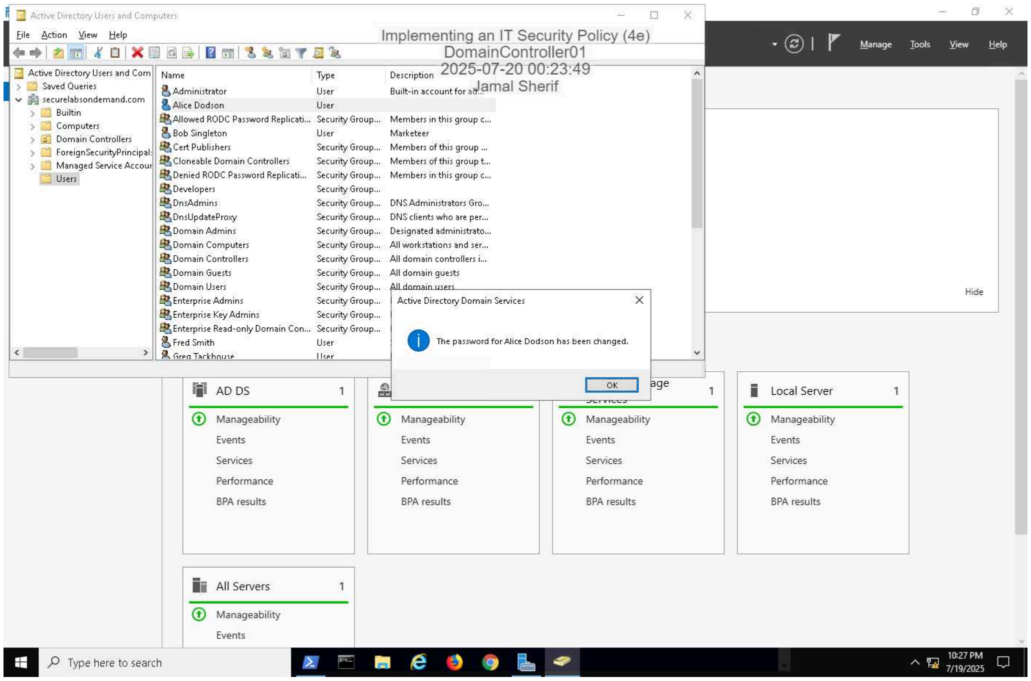
16. **Make a screen capture** showing the **newly configured Domain Password Policy settings**.



Implementing an IT Security Policy (4e)
DomainController01
2025-07-20 00:21:39
Jamal Sherif

Policy	Policy Setting
Enforce password history	15 passwords remembered
Maximum password age	30 days
Minimum password age	29 days
Minimum password length	9 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Not Defined

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



Implementing an IT Security Policy (4e)
DomainController01
2025-07-20 00:23:49
Jamal Sherif

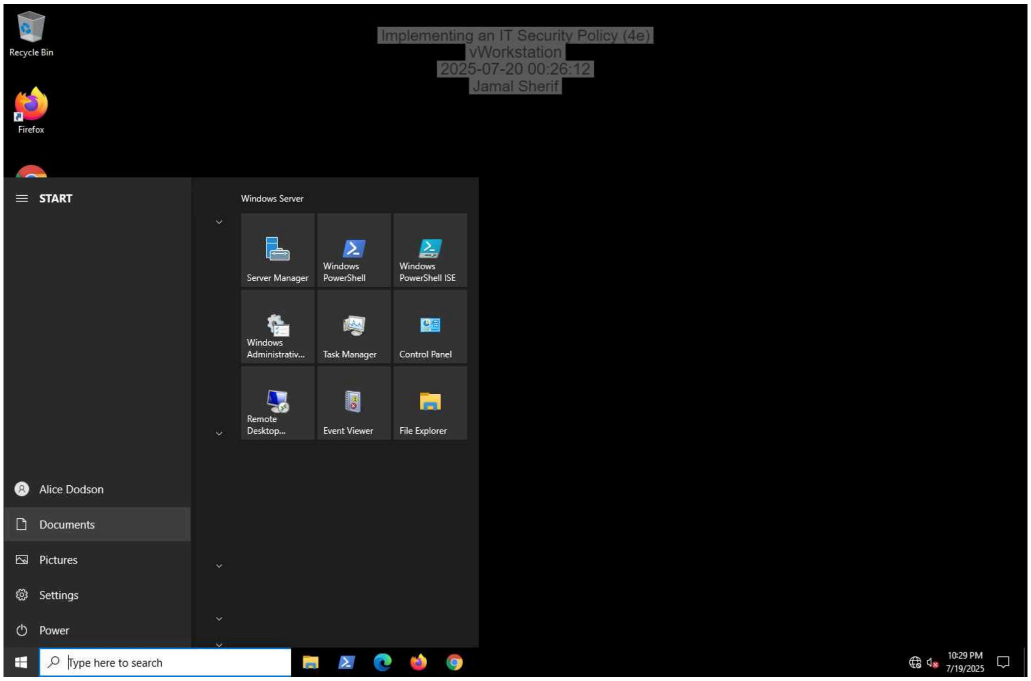
Active Directory Users and Computers

Name	Type	Description
Administrator	User	Built-in account for ad...
Alice Dodson	User	
Allowed RODC Password Replicati...	Security Group...	Members in this group c...
Bob Singleton	User	Marketeer
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replicati...	Security Group...	Members in this group c...
Developers	Security Group...	
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	
Enterprise Key Admins	Security Group...	
Enterprise Read-only Domain Con...	Security Group...	
Fred Smith	User	
Greg Tackhouse	User	

Active Directory Domain Services

The password for Alice Dodson has been changed.

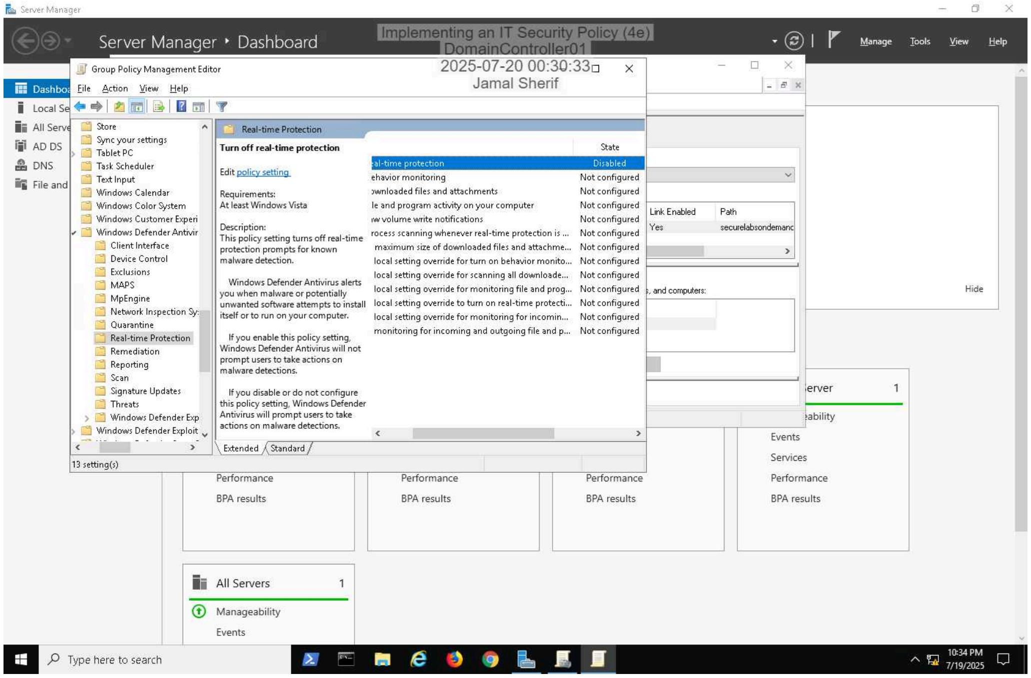
36. **Make a screen capture** showing the **logged on user account**.



Implementing an IT Security Policy (4e)
vWorkstation
2025-07-20 00:26:12
Jamal Sherif

Part 2: Implement an Antivirus Policy

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



Implementing an IT Security Policy (4e)
DomainController01
2025-07-20 00:30:33
Jamal Sherif

Real-time Protection

Turn off real-time protection

Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting turns off real-time protection prompts for known malware detection.

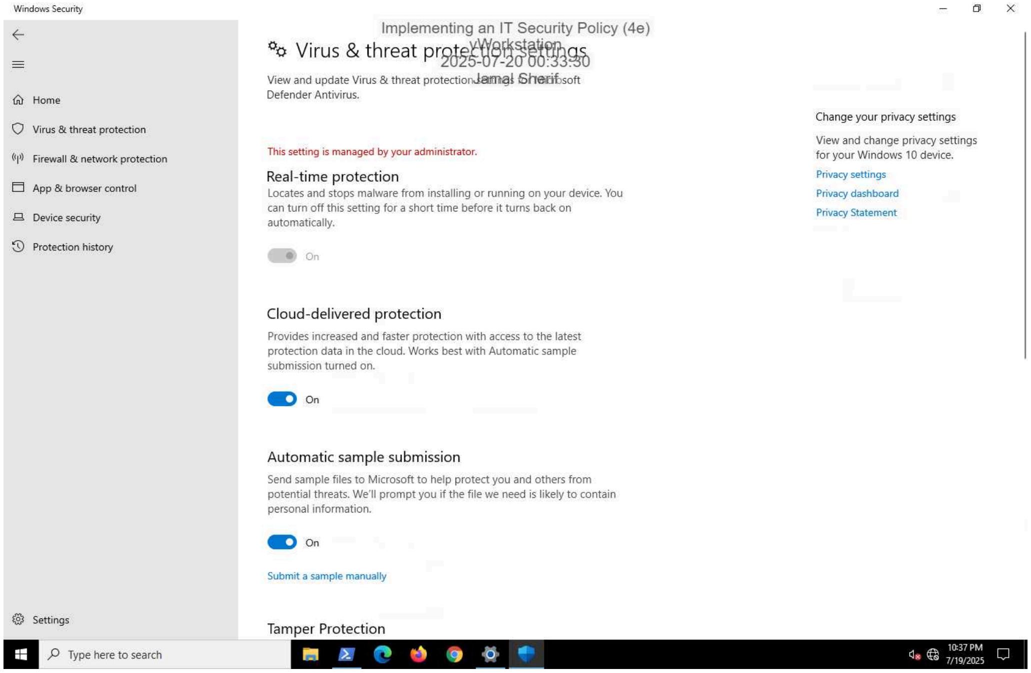
Windows Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer.

If you enable this policy setting, Windows Defender Antivirus will not prompt users to take actions on malware detections.

If you disable or do not configure this policy setting, Windows Defender Antivirus will prompt users to take actions on malware detections.

	State
eal-time protection	Disabled
ehavior monitoring	Not configured
ownloaded files and attachments	Not configured
le and program activity on your computer	Not configured
w volume write notifications	Not configured
rocess scanning whenever real-time protection is ...	Not configured
maximum size of downloaded files and attachme...	Not configured
local setting override for turn on behavior monito...	Not configured
local setting override for scanning all downloade...	Not configured
local setting override for monitoring file and prog...	Not configured
local setting override to turn on real-time protecti...	Not configured
local setting override for monitoring for incomin...	Not configured
monitoring for incoming and outgoing file and p...	Not configured

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



Implementing an IT Security Policy (4e)
vWorkstation
2025-07-20 00:33:30
Jamal Sherif

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

This setting is managed by your administrator.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

On

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

On

Submit a sample manually

Tamper Protection

Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings

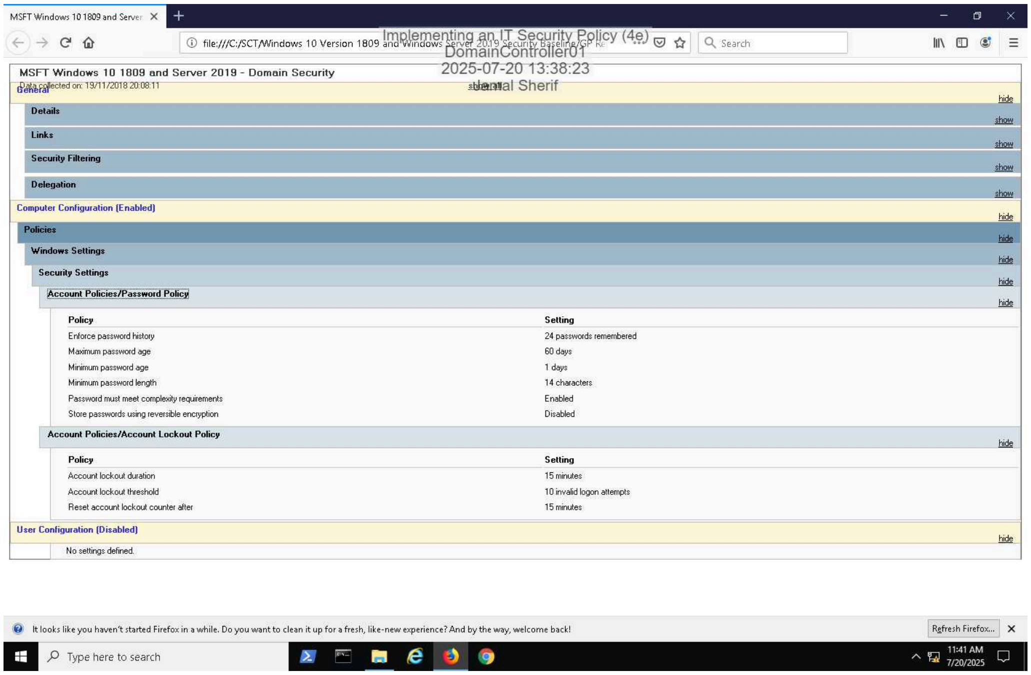
Privacy dashboard

Privacy Statement

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**.



Implementing an IT Security Policy (4e)
DomainController01
2025-07-20 13:38:23
Jamal Sherif

file:///C:/SCT/Windows 10 Version 1809 and Windows Server 2019 Security Baseline/GP Re

MSFT Windows 10 1809 and Server 2019 - Domain Security

Data collected on: 19/11/2018 20:08:11

General

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

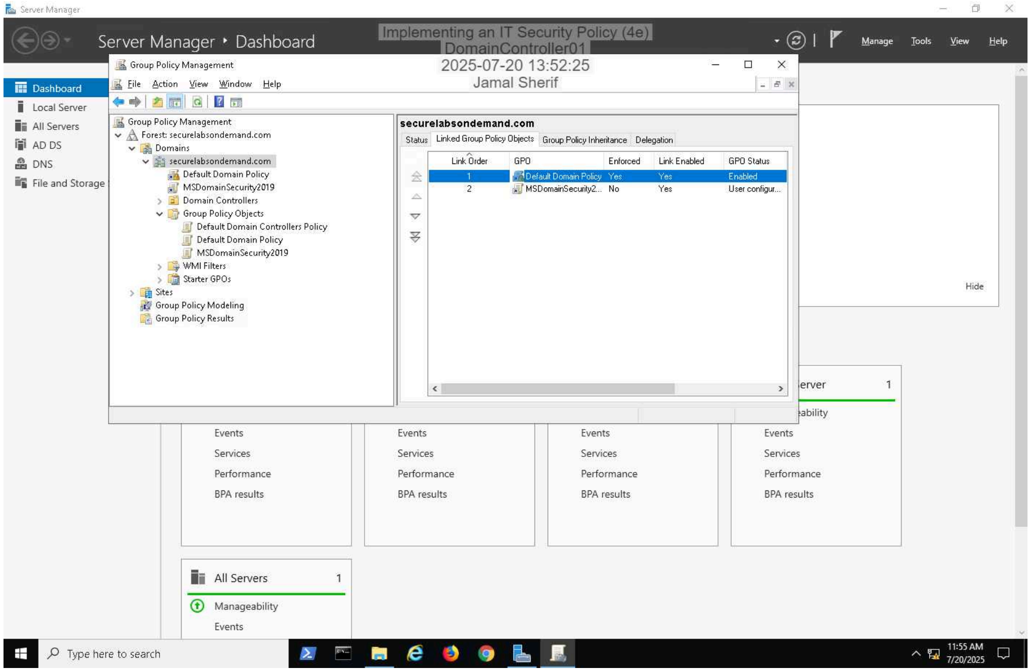
Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

User Configuration (Disabled)

No settings defined.

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

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



Implementing an IT Security Policy (4e)
DomainController01
2025-07-20 13:52:25
Jamal Sherif

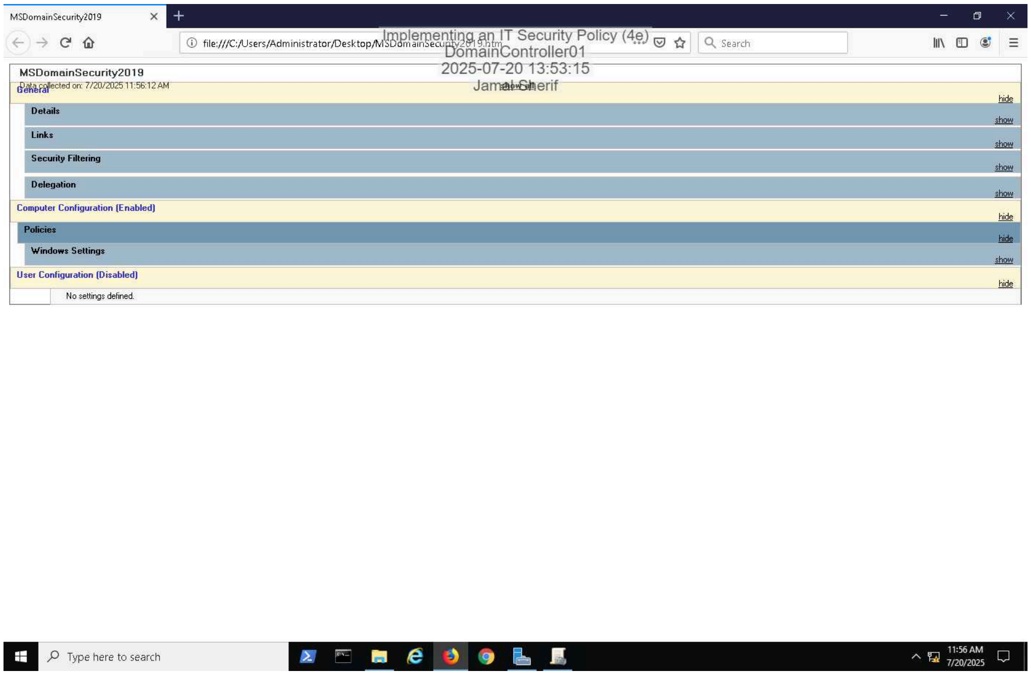
Group Policy Management
- Group Policy Management
  - Forest: securelabsondemand.com
    - Domains
      - securelabsondemand.com
        - Default Domain Policy
        - MSDomainSecurity2019
        - Domain Controllers
        - Group Policy Objects
          - Default Domain Controllers Policy
          - Default Domain Policy
          - MSDomainSecurity2019
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

securelabsondemand.com

Status | Linked Group Policy Objects | Group Policy Inheritance | Delegation

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Default Domain Policy	Yes	Yes	Enabled
2	MSDomainSecurity2...	No	Yes	User configur...

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



MSDomainSecurity2019

file:///C:/Users/Administrator/Desktop/MSDomainSecurity2019.htm

Implementing an IT Security Policy (4e)
DomainController01
2025-07-20 13:53:15
Jamal Sherif

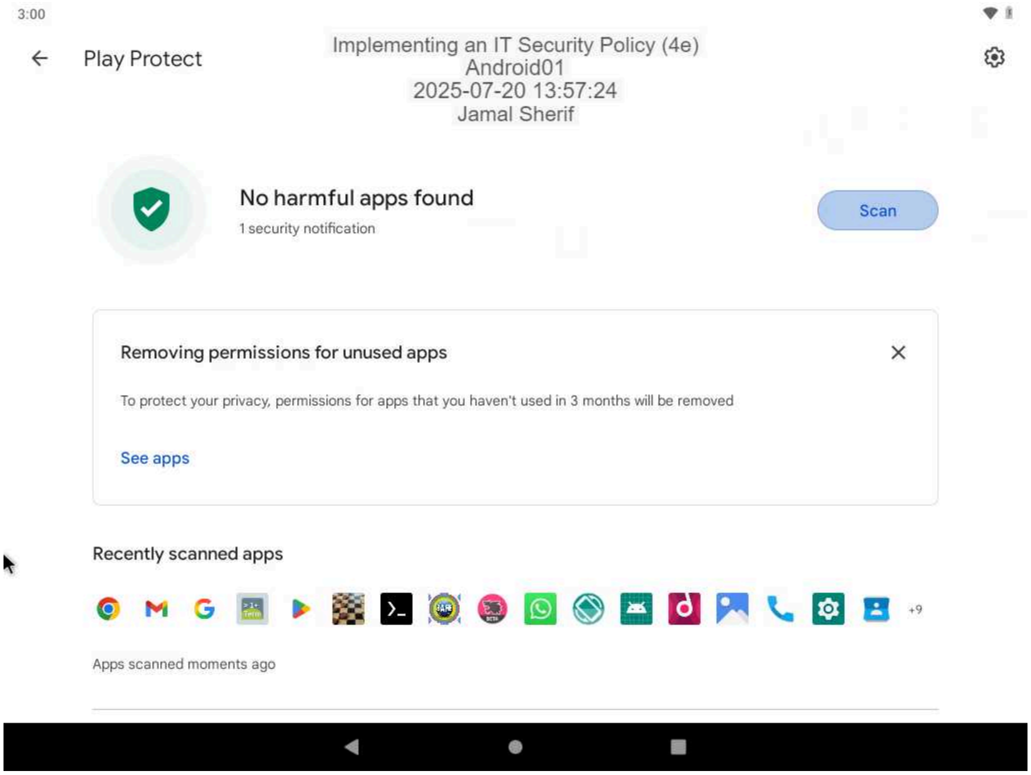
MSDomainSecurity2019
Data collected on: 7/20/2025 11:56:12 AM

show all

General	hide
Details	show
Links	show
Security Filtering	show
Delegation	show
Computer Configuration (Enabled)	hide
Policies	hide
Windows Settings	show
User Configuration (Disabled)	hide
No settings defined.	

Part 2: Implement a Mobile Device Security Policy

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



Implementing an IT Security Policy (4e)
Android01
2025-07-20 13:57:24
Jamal Sherif

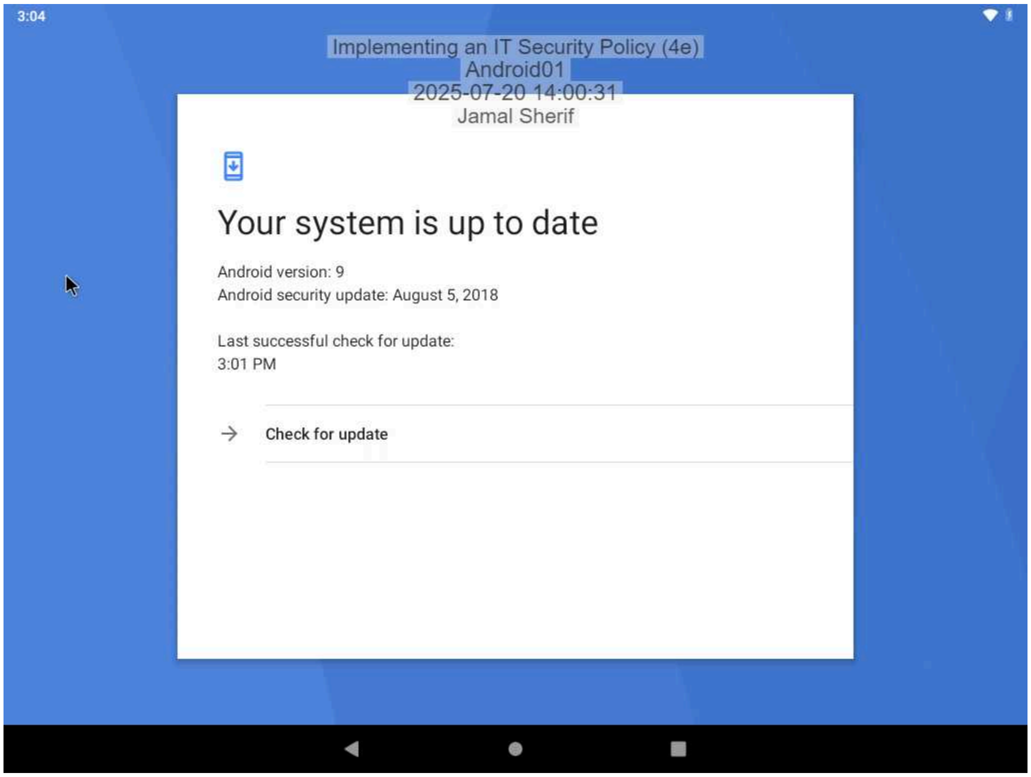
No harmful apps found
1 security notification

Removing permissions for unused apps
To protect your privacy, permissions for apps that you haven't used in 3 months will be removed
See apps

Recently scanned apps

Apps scanned moments ago

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



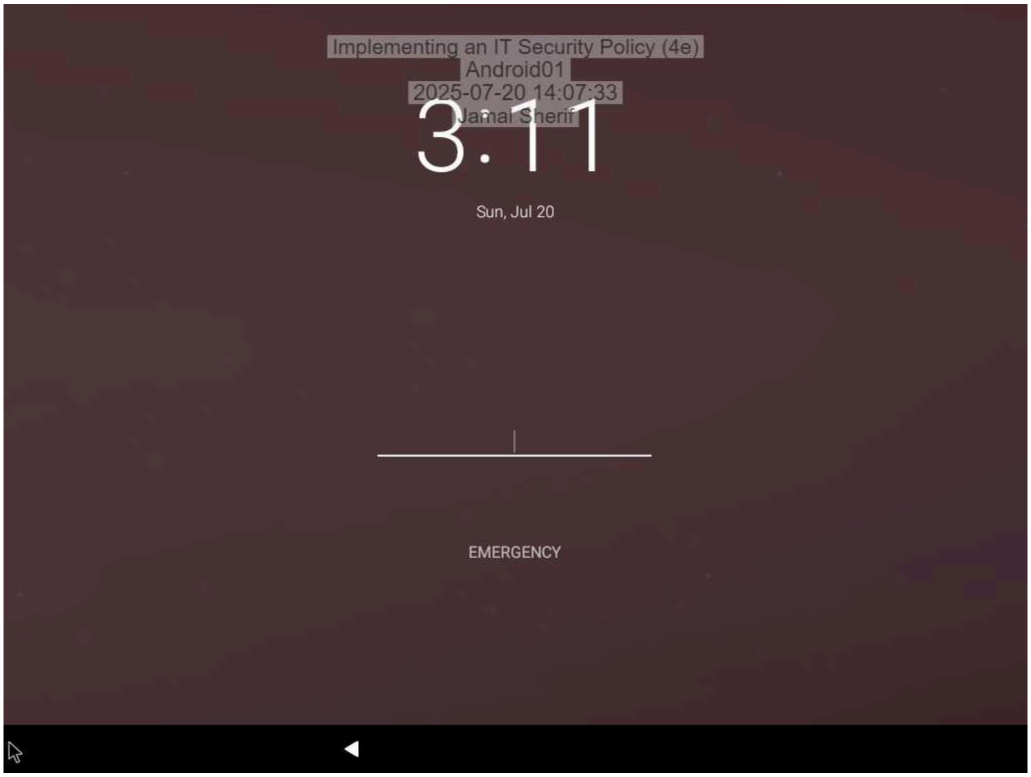
Implementing an IT Security Policy (4e)
Android01
2025-07-20 14:00:31
Jamal Sherif

Your system is up to date

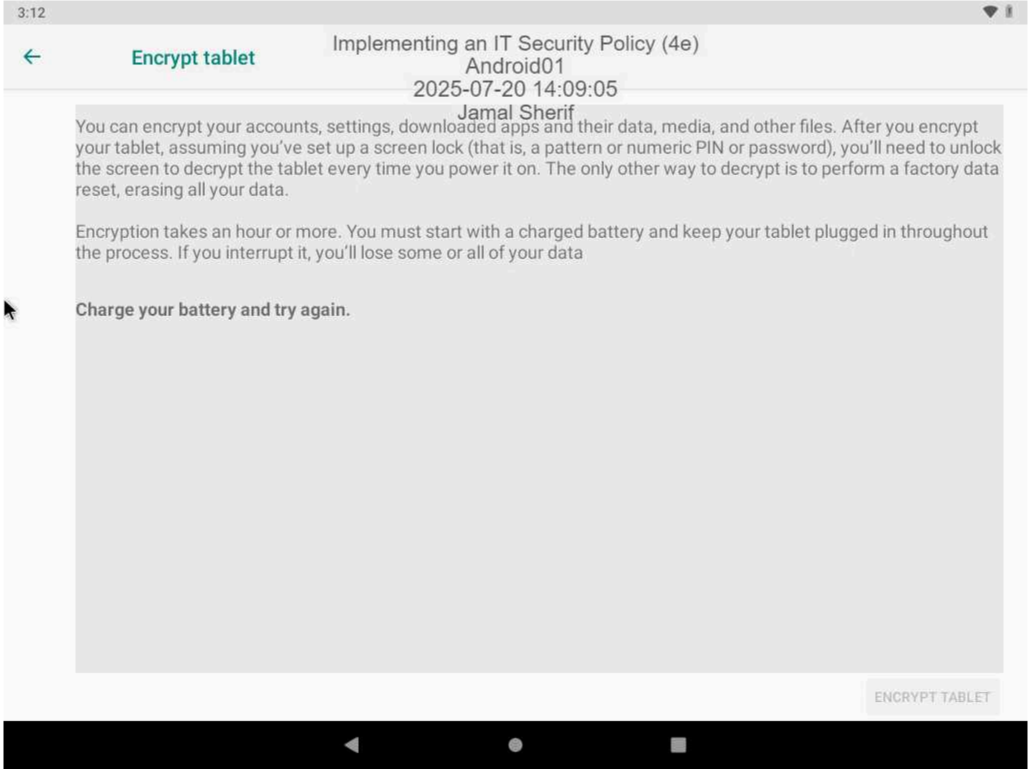
Android version: 9
Android security update: August 5, 2018

Last successful check for update:
3:01 PM

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



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

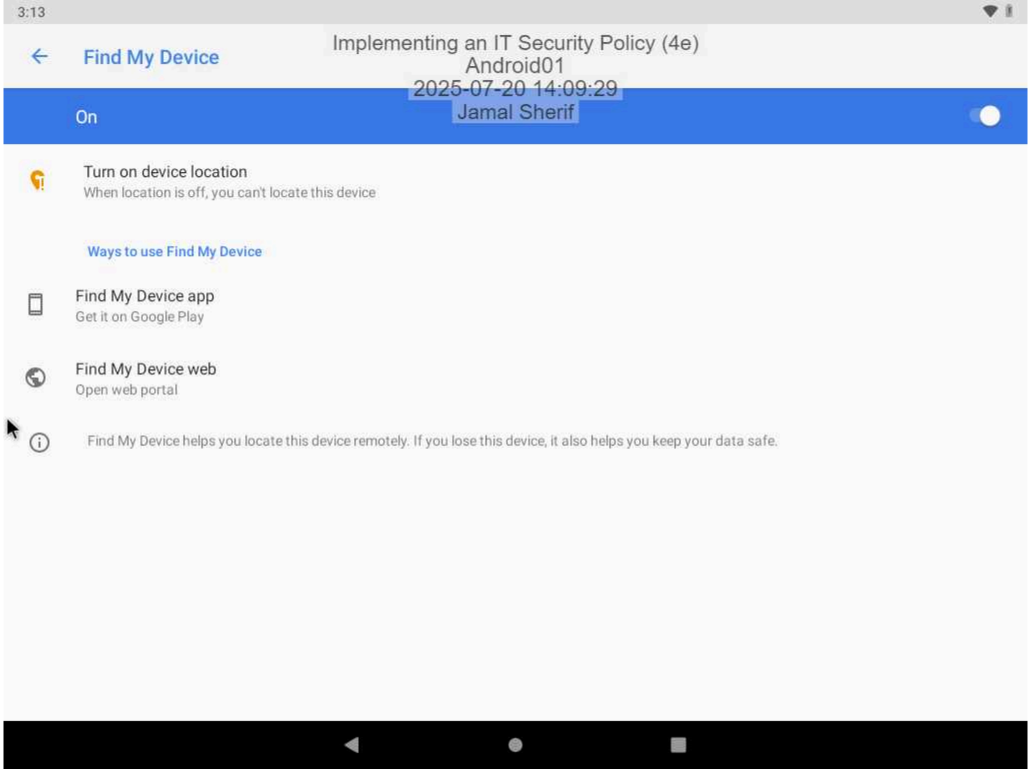


You can encrypt your accounts, settings, downloaded apps and their data, media, and other files. After you encrypt your tablet, assuming you've set up a screen lock (that is, a pattern or numeric PIN or password), you'll need to unlock the screen to decrypt the tablet every time you power it on. The only other way to decrypt is to perform a factory data reset, erasing all your data.

Encryption takes an hour or more. You must start with a charged battery and keep your tablet plugged in throughout the process. If you interrupt it, you'll lose some or all of your data

Charge your battery and try again.

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



3:13

Find My Device

Implementing an IT Security Policy (4e)
Android01
2025-07-20 14:09:29
Jamal Sherif

On

Turn on device location
When location is off, you can't locate this device

Ways to use Find My Device

Find My Device app
Get it on Google Play

Find My Device web
Open web portal

Find My Device helps you locate this device remotely. If you lose this device, it also helps you keep your data safe.

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.

confidentiality: “Malware can disclose an organization’s private information or the private information of personnel” This shows show bad data breaches can be through careless behavior. Having confidentiality protects personal identities and company secrets.
Authentication and Authorization: “Authentication—The proving of that assertion” “Authorization—The permissions a legitimate user or process has on the system”This practice helps to limit access to the sensitive systems. without this data can be stolen or tampered with.
Use of Security Controls: “Security controls are the safeguards or countermeasures that an organization uses to avoid, counteract, or minimize loss or system unavailability” The user cannot mess with the encryption or network protection.
Prohibited Uses and System Misuse: “Administrative controls develop and ensure compliance with policy and procedures. They tend to be things that employees might do, are supposed to do, or are not supposed to do” misuse of the systems can make malware bypass.
Kim, D., & Solomon, M. G. (2021). Fundamentals of Information Systems Security. Jones & Bartlett Learning.

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.

Incomplete