Student:	Email:
Julie Clarke	clarke323@usf.edu

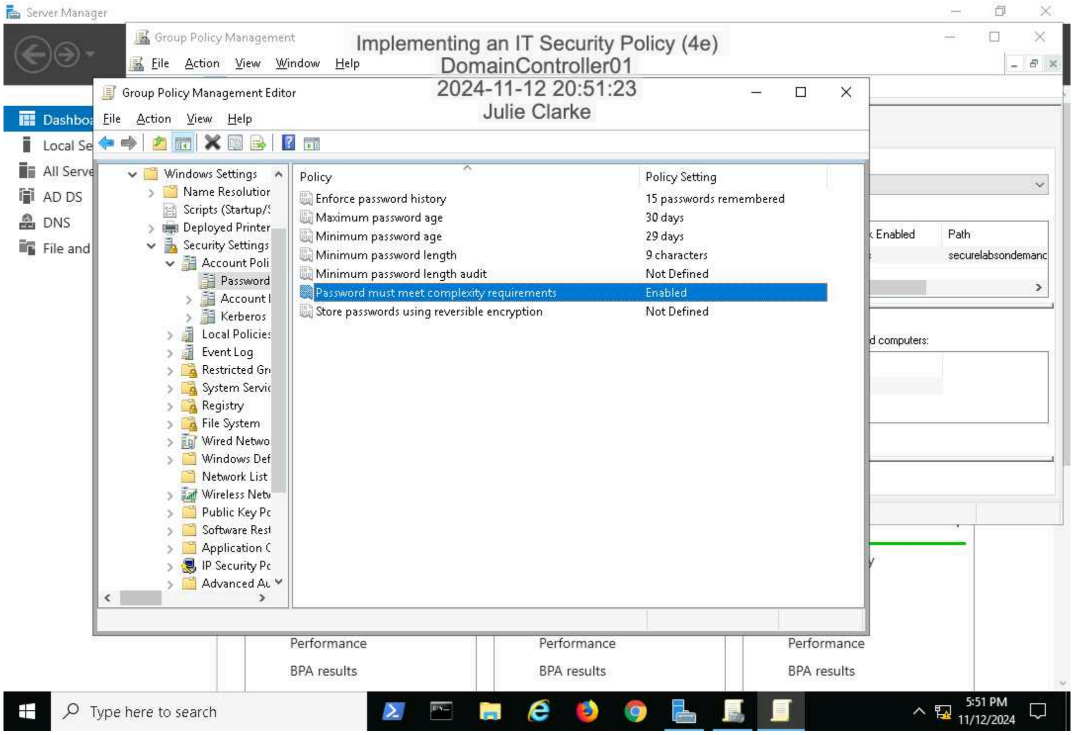
Time on Task:	Progress:
6 hours, 18 minutes	100%

Report Generated: Friday, November 15, 2024 at 12:02 AM

Section 1: Hands-On Demonstration

Part 1: Implement a Password Protection Policy

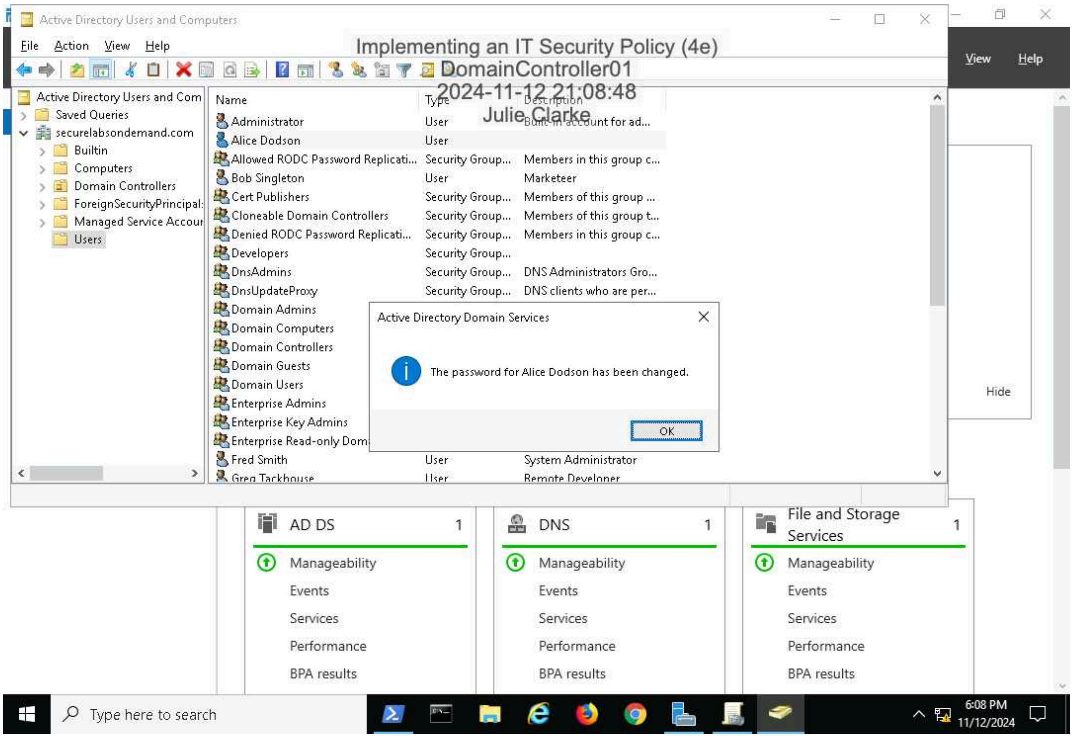
16. **Make a screen capture** showing the **newly configured Domain Password Policy settings**.



Implementing an IT Security Policy (4e)
DomainController01
2024-11-12 20:51:23
Julie Clarke

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**.



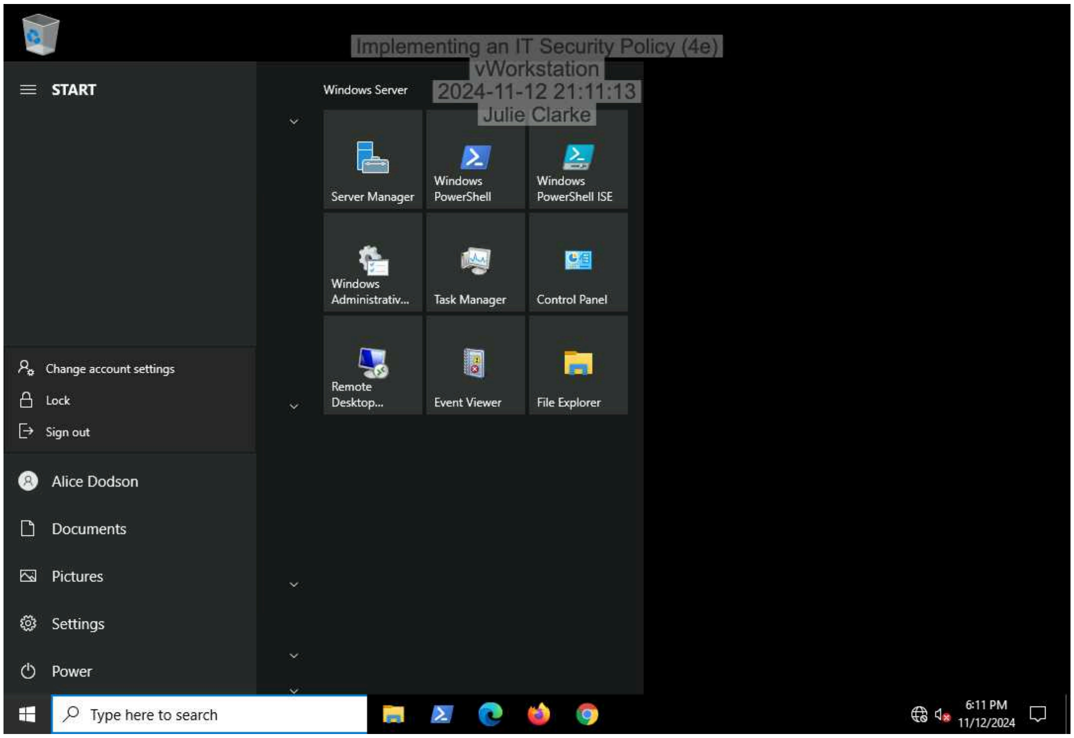
Name	Type	Description
Administrator	User	Built-in account for ad...
Alice Dodson	User	
Allowed RODC Password Replicati...	Security Group...	Members in this group c...
Bob Singleton	User	Marketeer
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	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		
Domain Computers		
Domain Controllers		
Domain Guests		
Domain Users		
Enterprise Admins		
Enterprise Key Admins		
Enterprise Read-only Dom		
Fred Smith	User	System Administrator
Greg Tackhouse	User	Remote Developer

Active Directory Domain Services

The password for Alice Dodson has been changed.

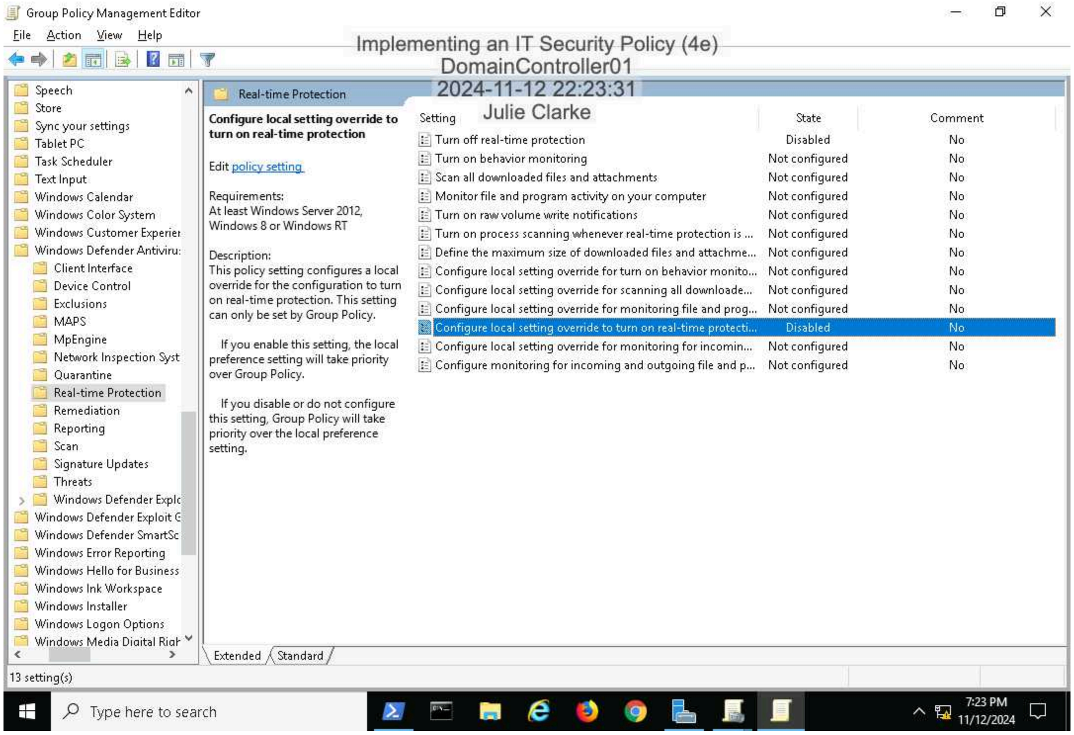
OK

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.**



Implementing an IT Security Policy (4e)
DomainController01
2024-11-12 22:23:31
Julie Clarke

Configure local setting override to turn on real-time protection

Edit policy setting

Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:
This policy setting configures a local override for the configuration to turn on real-time protection. This setting can only be set by Group Policy.

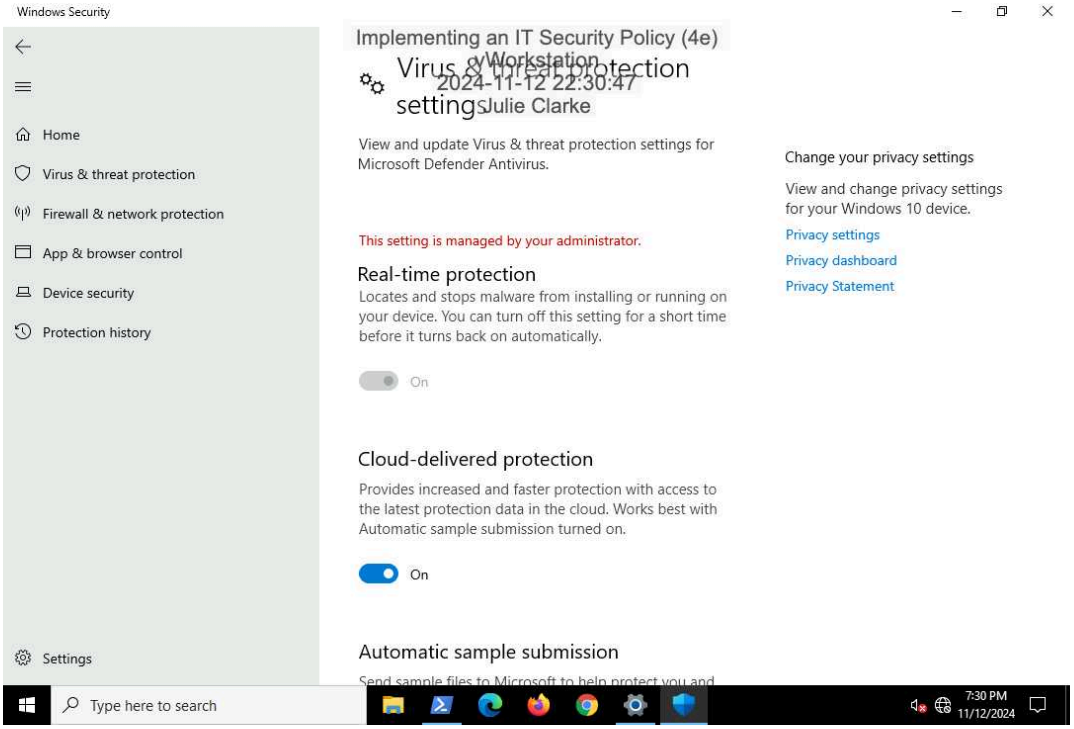
If you enable this setting, the local preference setting will take priority over Group Policy.

If you disable or do not configure this setting, Group Policy will take priority over the local preference setting.

Setting	State	Comment
Turn off real-time protection	Disabled	No
Turn on behavior monitoring	Not configured	No
Scan all downloaded files and attachments	Not configured	No
Monitor file and program activity on your computer	Not configured	No
Turn on raw volume write notifications	Not configured	No
Turn on process scanning whenever real-time protection is ...	Not configured	No
Define the maximum size of downloaded files and attachme...	Not configured	No
Configure local setting override for turn on behavior monito...	Not configured	No
Configure local setting override for scanning all downloade...	Not configured	No
Configure local setting override for monitoring file and prog...	Not configured	No
Configure local setting override to turn on real-time protecti...	Disabled	No
Configure local setting override for monitoring for incomin...	Not configured	No
Configure monitoring for incoming and outgoing file and p...	Not configured	No

13 setting(s)

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



Implementing an IT Security Policy (4e)
vWorkstation
2024-11-12 22:30:47
Julie Clarke

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

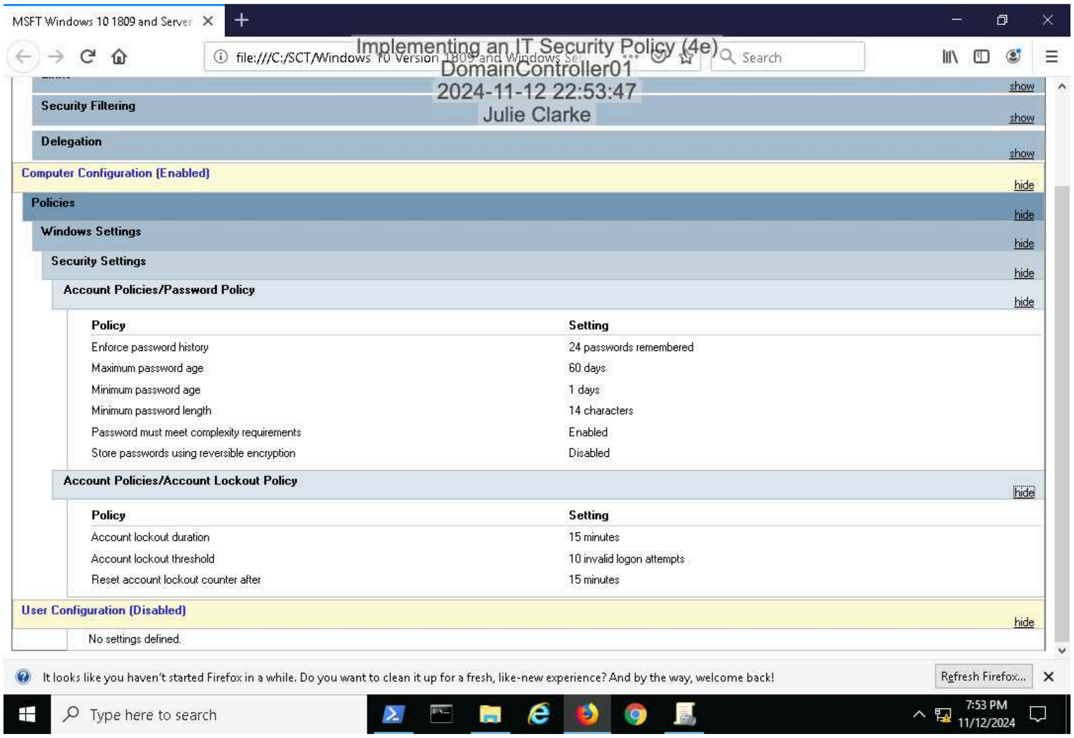
Automatic sample submission
Send sample files to Microsoft to help protect you and

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**.


MSFT Windows 10 1809 and Server
file:///C:/SCT/Windows 10 Version 1809 and Windows Se
Search
Implementing an IT Security Policy (4e)
DomainController01
2024-11-12 22:53:47
Julie Clarke
Type here to search
7:53 PM
11/12/2024

Security Filtering show

Delegation show

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

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 hide

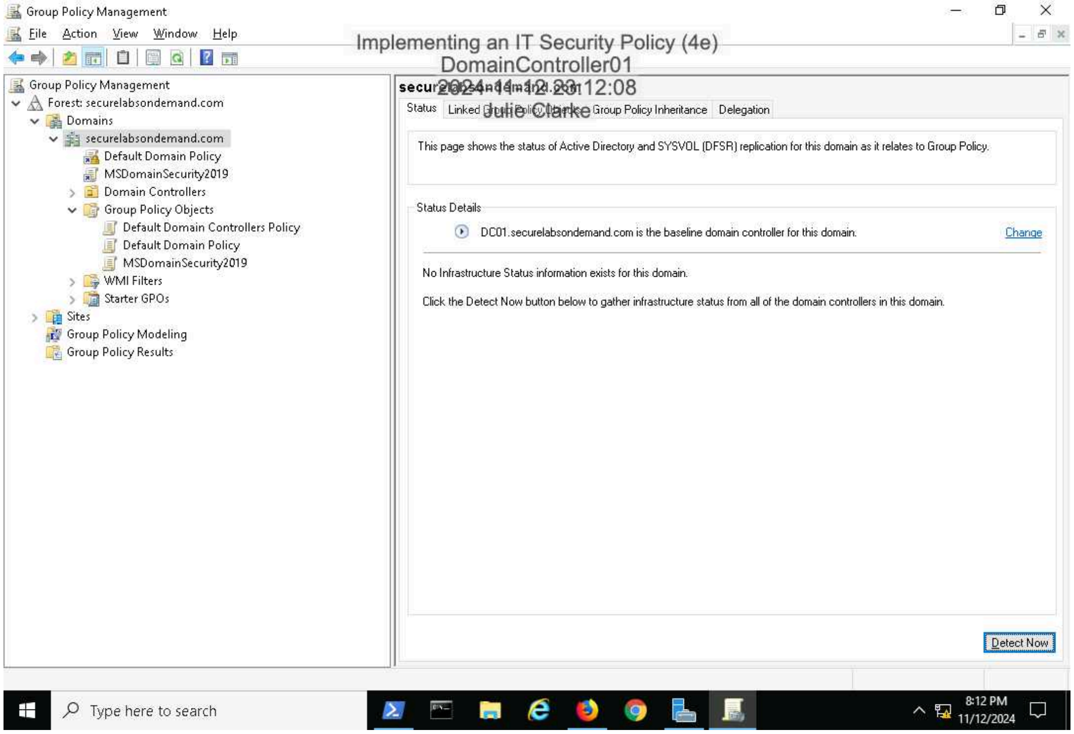
Policy	Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

User Configuration (Disabled) hide

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! Refresh Firefox...

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



- 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

This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.

Status Details

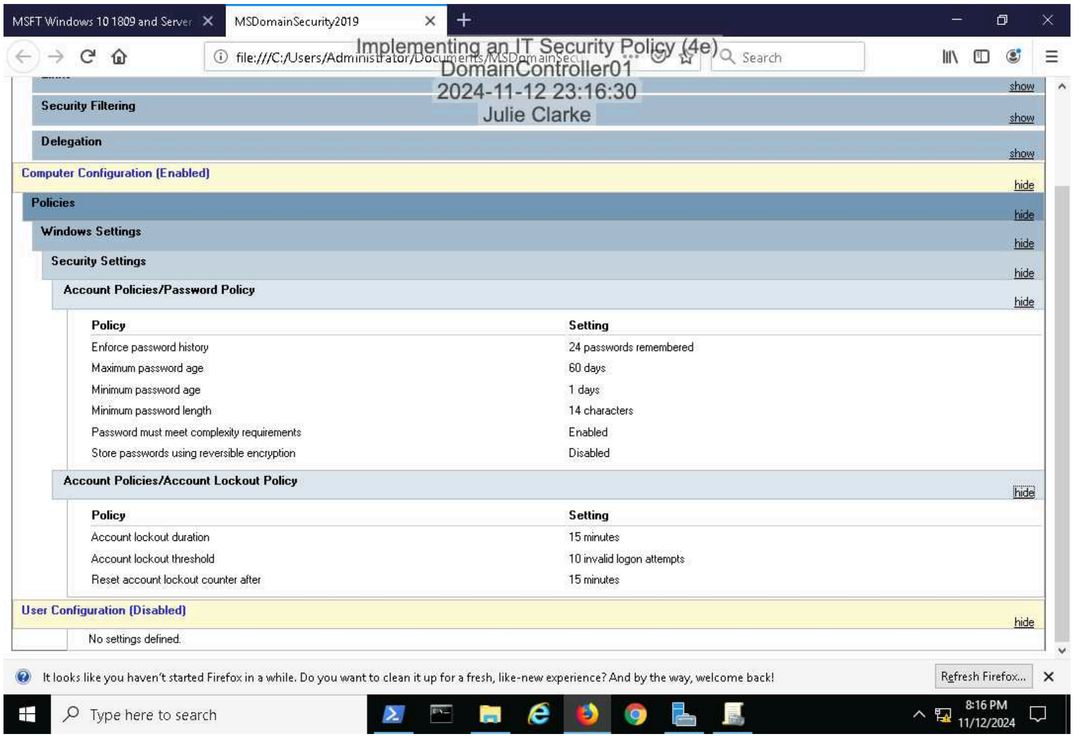
DC01.securelabsondemand.com is the baseline domain controller for this domain. Change

No Infrastructure Status information exists for this domain.

Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

Detect Now

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


MSFT Windows 10 1809 and Server
MSDomainSecurity2019
file:///C:/Users/Administrator/Documents/MSDomainSec...
Search
Implementing an IT Security Policy (4e)
DomainController01
2024-11-12 23:16:30
Julie Clarke
Type here to search
8:16 PM
11/12/2024

Security Filtering show

Delegation show

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

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 hide

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

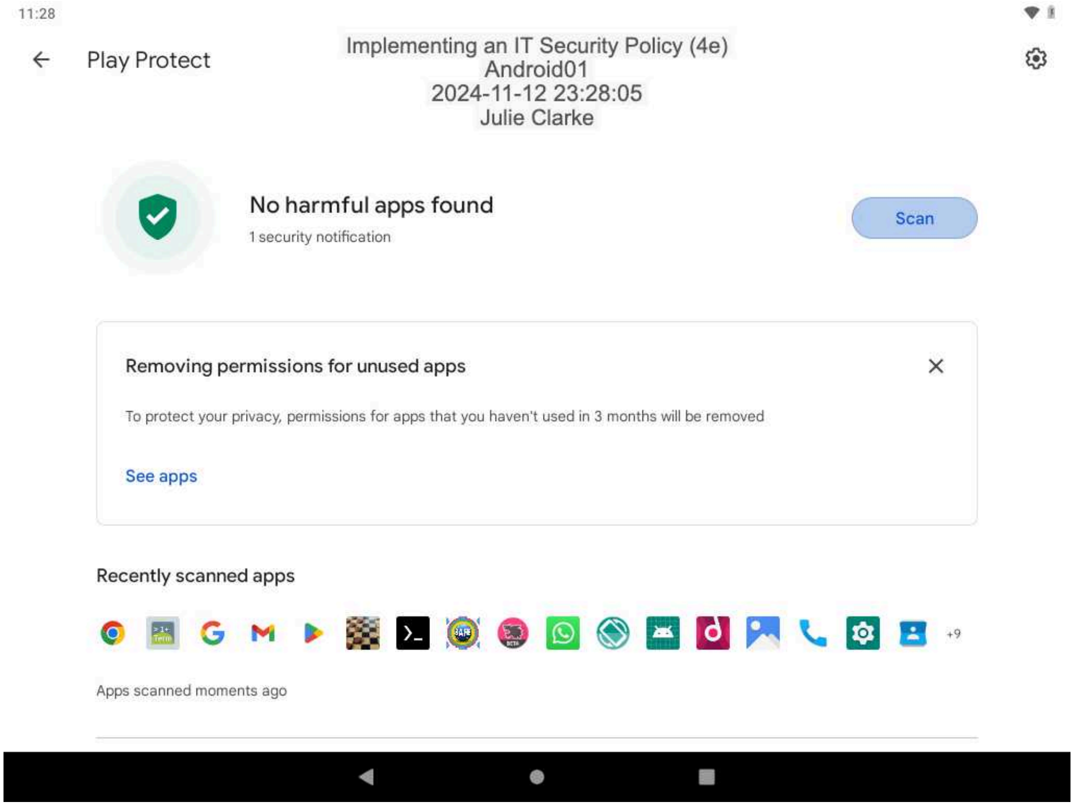
User Configuration (Disabled) hide

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! Refresh Firefox...

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
2024-11-12 23:28:05
Julie Clarke

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

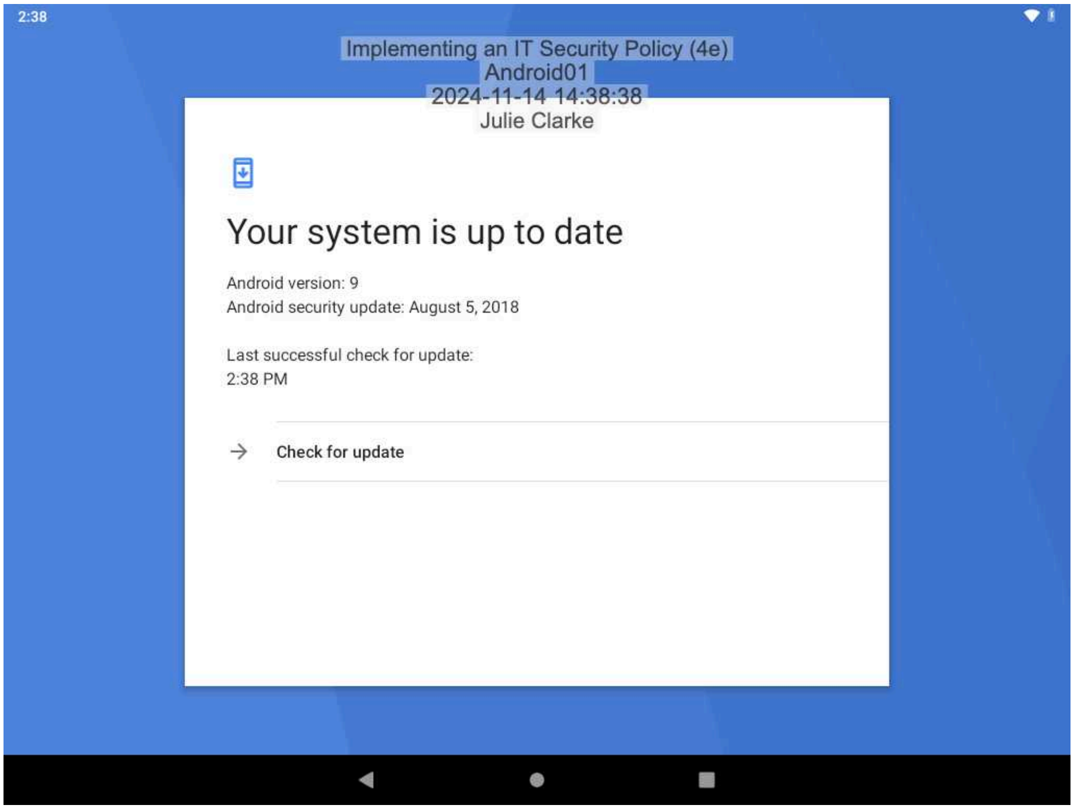
See apps

Recently scanned apps

+9

Apps scanned moments ago

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



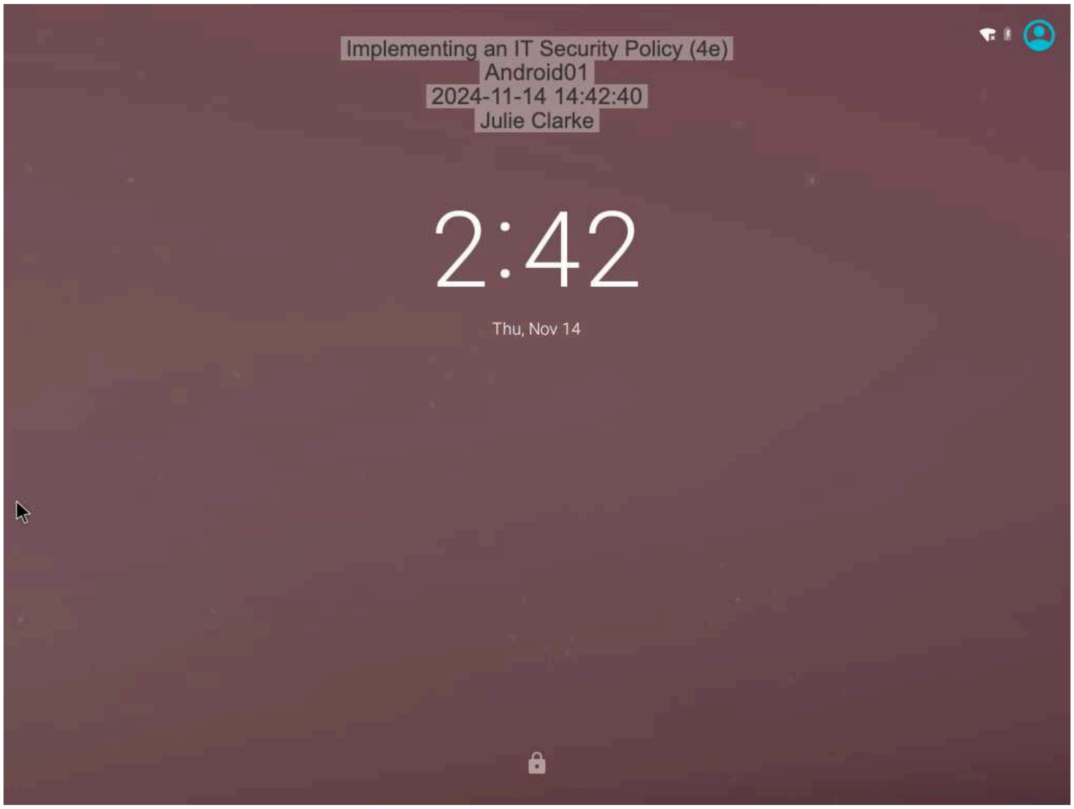
Implementing an IT Security Policy (4e)
Android01
2024-11-14 14:38:38
Julie Clarke

Your system is up to date

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

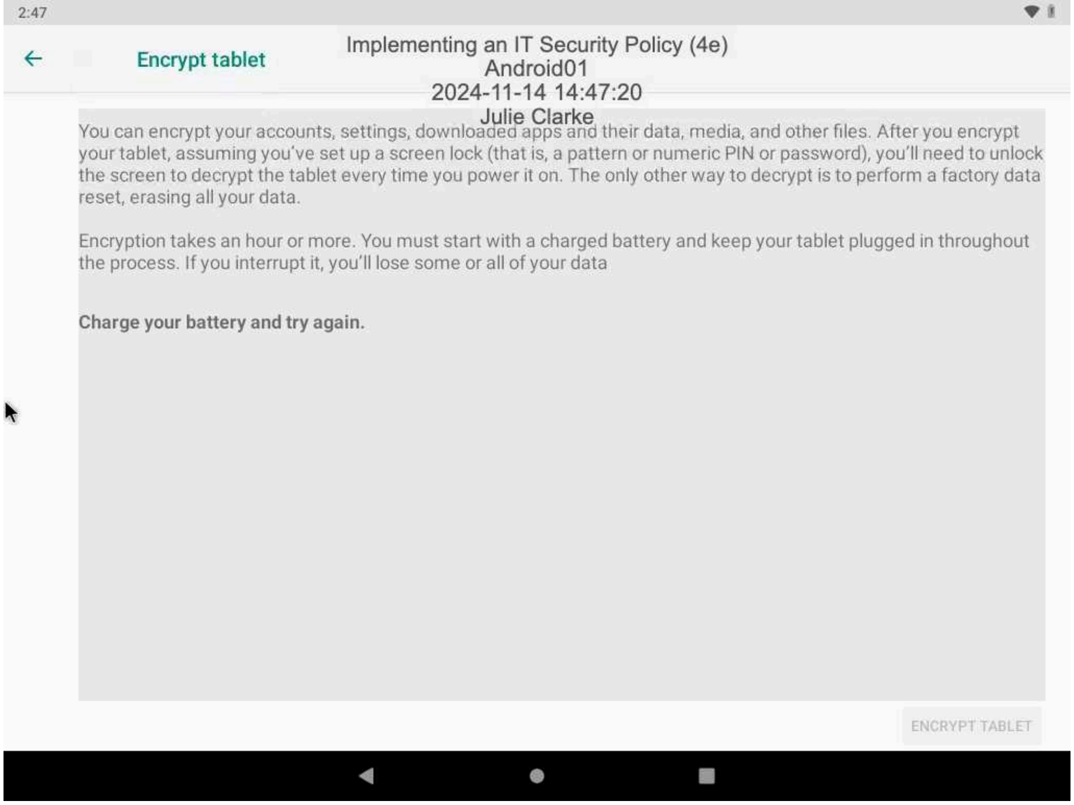
Last successful check for update:
2:38 PM

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



Implementing an IT Security Policy (4e)
Android01
2024-11-14 14:42:40
Julie Clarke

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



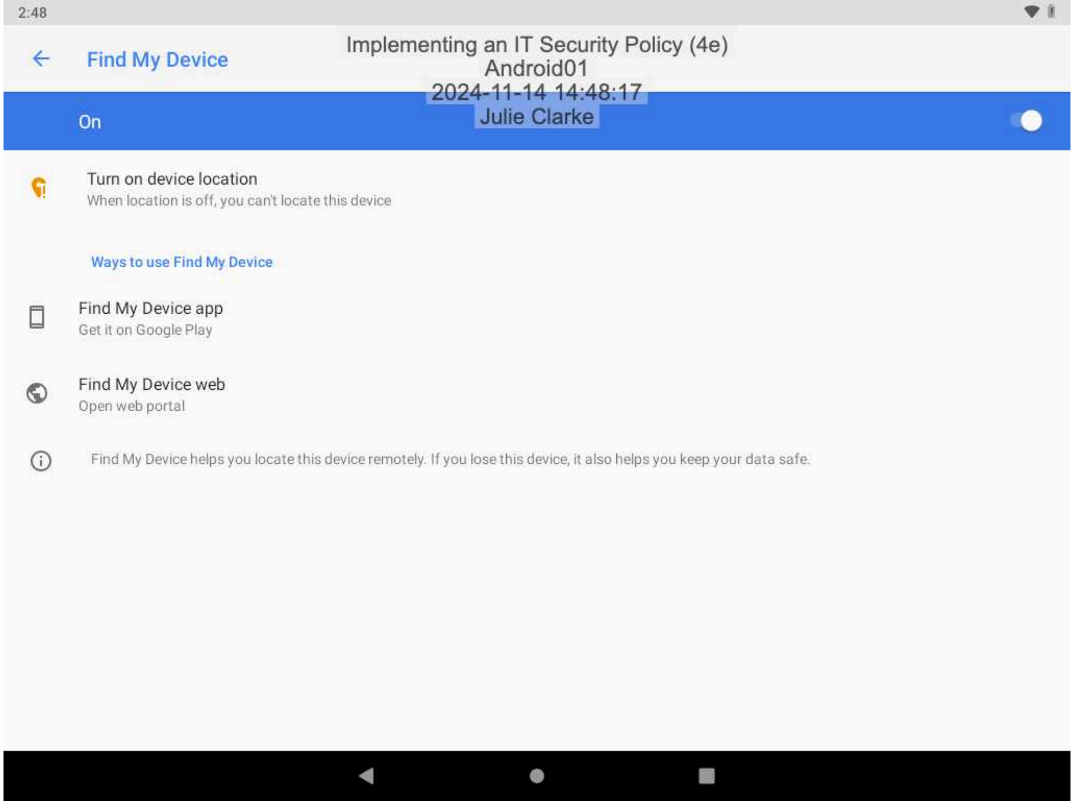
Implementing an IT Security Policy (4e)
Android01
2024-11-14 14:47:20
Julie Clarke

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**.



Implementing an IT Security Policy (4e)
Android01
2024-11-14 14:48:18
Julie Clarke

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.

1. Device and Network Security: Policies usually require that only approved devices and software connect to the company's network. This is to protect the company from malware and hackers. By sticking to approved devices, the whole network stays more secure and reliable.
2. Internet and Email Usage: Most AUPs will set rules for using the internet and email at work, like not visiting inappropriate sites or sharing sensitive info through unencrypted emails. This isn’t just about professionalism; it also helps protect against phishing scams and data leaks, which can harm both the company and employees.
3. Compliance with Laws: AUPs often require that users follow laws around data privacy and intellectual property (like not sharing copyrighted content). This not only keeps the company out of legal trouble but also keeps things fair and respectful of privacy laws.
4. Monitoring and Privacy: Companies often monitor network traffic to make sure the policy is being followed, but a good AUP will explain this up front. Transparency is important—it lets employees know what’s being tracked so there aren’t surprises if a violation gets flagged.
5. Consequences for Violations: Finally, AUPs lay out what will happen if someone breaks the rules, like warnings or disciplinary action. Knowing there are consequences helps encourage everyone to follow the policy and keeps the work environment fair.

Sources:https://www.business.com/articles/acceptable-use-policy/
https://www.awarehq.com/blog/acceptable-use-policy
https://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. Transparency with Data Collection: Companies need to be upfront about what data they're collecting, like your name, email, or browsing history, and why they're doing it. A good policy explains this in plain language instead of legal jargon, so users really get what's happening with their data. This kind of transparency is crucial for building trust since it reassures users that nothing shady is happening behind the scenes. Plus, it gives people the info they need to make informed choices about what data they're okay with sharing.
2. Getting Consent and Explaining Rights: Privacy Policies should make it clear how users can give (or take back) permission for the company to collect and use their info. It should also explain users' rights, like being able to view, correct, or delete their data. Some companies even have privacy settings that let users control this stuff easily. This part is not just about giving people control—it's also a big part of staying compliant with privacy laws like GDPR and CCPA. Companies that make it simple for users to manage these settings show they care about user choices, which helps boost trust and keep the company out of legal trouble.3. Only Collect What's Necessary: The principle of data minimization is all about only gathering data that's actually useful for the company. For example, if an app just needs your email to send you updates, it shouldn't be asking for your location data too. Collecting only what's essential means there's less sensitive info stored, which reduces the risk in case of a data breach. This approach isn't just good for security; it also helps users feel better about sharing their info because they know it's only being used in ways that make sense.
4. Security Measures: Letting users know that their data is being protected with tools like encryption, firewalls, and regular security checks is a must in a good Privacy Policy. Explaining these security measures shows that the company takes its responsibility seriously and is actively working to prevent data leaks or breaches. This kind of transparency about security can be a big trust-builder since users can see the company has specific systems to keep their info safe.
5. Sharing with Third Parties: If the company works with other businesses (like for ads, analytics, or payment processing), a good Privacy Policy will be clear about what data is shared and why. It's also helpful if the policy mentions how these third parties are vetted to ensure they meet privacy standards. This part helps users feel more in control of where their data goes and builds trust, especially if the company is open about which partners they're working with and how these partners handle data security too.

Sources:
https://www.digitalguardian.com/blog/data-privacy-best-practices-ensure-compliance-security
https://www.pandadoc.com/blog/how-to-write-a-privacy-policy/
https://ironcladapp.com/journal/contracts/how-to-create-the-best-privacy-policy-for-your-business/