Managing Group Policy within the Microsoft Windows Environment (3e)

Security Strategies in Windows Platforms and Applications, Third Edition - Lab 05

Student:	Email:
Bradley Adams	badams10@my.athens.edu

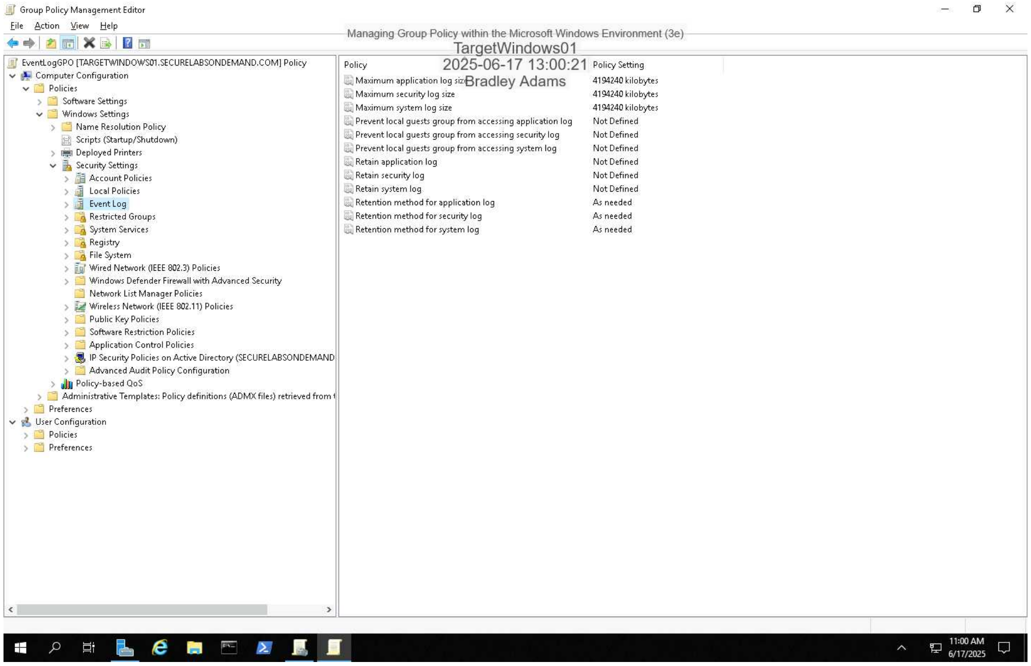
Time on Task:	Progress:
11 hours, 48 minutes	100%

Report Generated: Wednesday, June 18, 2025 at 9:42 AM

Section 1: Hands-On Demonstration

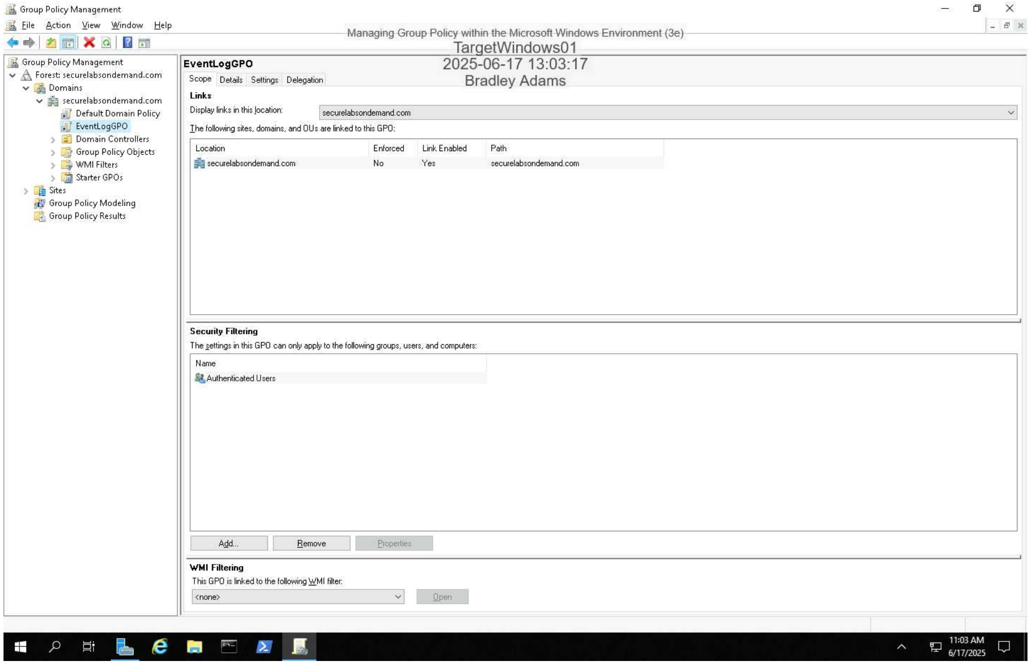
Part 1: Create and Link a New Domain-Level Group Policy Object

20. **Make a screen capture** showing the **updated policy settings for the new EventLogGPO**.


Group Policy Management Editor
File
Action
View
Help
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-17 13:00:21
Bradley Adams
EventLogGPO [TARGETWINDOWS01.SECURELABSONDEMAND.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (SECURELABSONDEMAND
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved from t
Preferences
User Configuration
Policies
Preferences
11:00 AM
6/17/2025

Policy	Policy Setting
Maximum application log size	4194240 kilobytes
Maximum security log size	4194240 kilobytes
Maximum system log size	4194240 kilobytes
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed

26. **Make a screen capture** showing the **linked EventLogGPO**.



Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-17 13:03:17
Bradley Adams

EventLogGPO

Links

Display links in this location: securelabsondemand.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
securelabsondemand.com	No	Yes	securelabsondemand.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

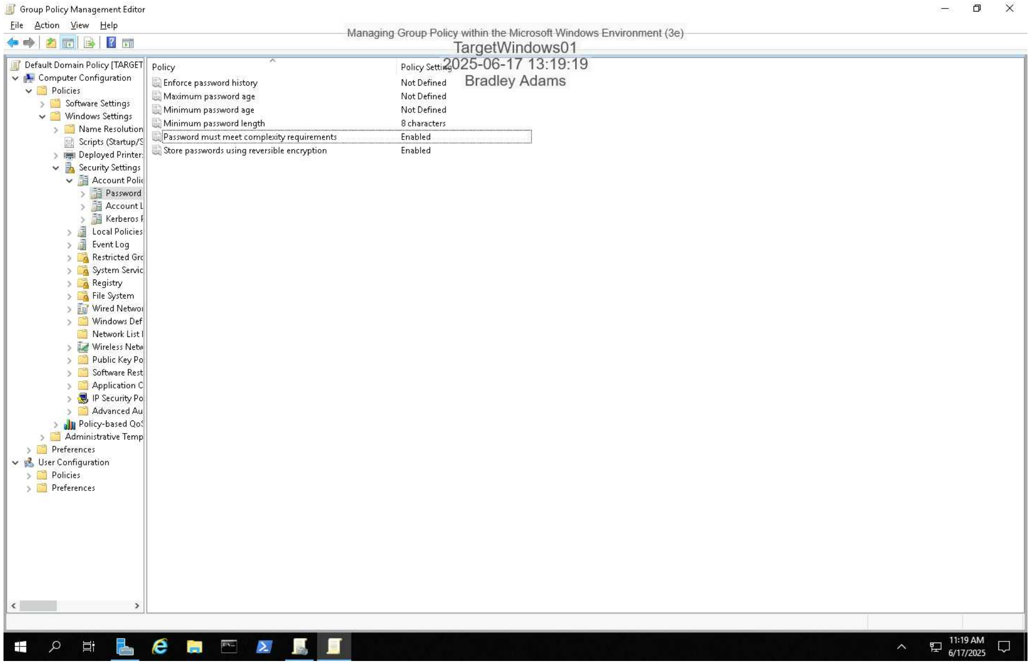
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter: <none>

Part 2: Edit the Default Domain Policy

9. **Make a screen capture** showing the **policy changes you made in the Group Policy Management Editor**.



Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-17 13:19:19
Bradley Adams

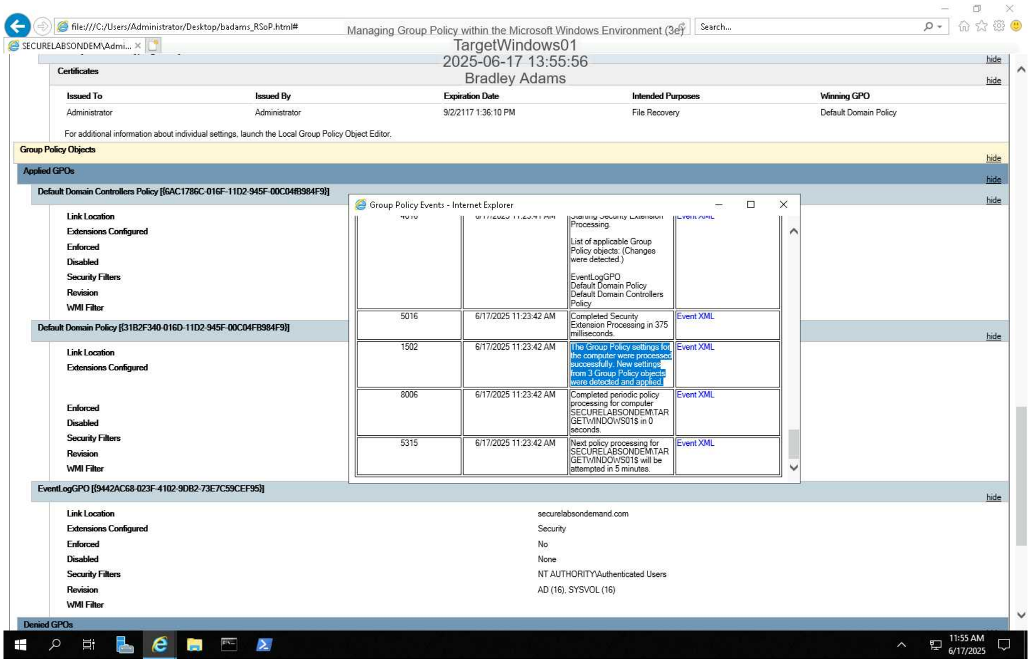
Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Enabled

10. **Explain** why you made the changes you made, **make note** of any suggested changes that you accepted, and **explain** why you believe the Group Policy Management Editor recommended those changes.

NIST best practices suggest a minimum password length of 8 characters and storing passwords using encryption. Password complexity may help, but users should also avoid creating guessable patterns. No suggested changes were given for these three settings. Suggested changes are often recommended to help administrators align with best practices, prevent misconfigurations, maintain compatibility, and Microsoft periodically updates recommendations based on known threats, trends, and updates to frameworks.

Part 3: Document and Audit Group Policy

10. **Make a screen capture** showing the **policy changes you made in the RSoP**.



file:///C:/Users/Administrator/Desktop/badams_RSoP.html#

SECURELABSONDEM\Admi...

Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-17 13:55:56
Bradley Adams

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Winning GPO
Administrator	Administrator	9/2/2117 1:36:10 PM	File Recovery	Default Domain Policy

For additional information about individual settings, launch the Local Group Policy Object Editor.

Group Policy Objects

Applied GPOs

Default Domain Controllers Policy [{6AC1786C-016F-11D2-945F-00C04fB984F9}]

Link Location
Extensions Configured
Enforced
Disabled
Security Filters
Revision
WMI Filter

Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}]

Link Location
Extensions Configured
Enforced
Disabled
Security Filters
Revision
WMI Filter

EventLogGPO [{9442AC68-023F-4102-9DB2-73E7C59CEF95}]

Link Location	securelabsondemand.com
Extensions Configured	Security
Enforced	No
Disabled	None
Security Filters	NT AUTHORITY\Authenticated Users
Revision	AD (16), SYSVOL (16)
WMI Filter	

Denied GPOs

Group Policy Events - Internet Explorer

		Processing. List of applicable Group Policy objects: (Changes were detected.) EventLogGPO Default Domain Policy Default Domain Controllers Policy	
5016	6/17/2025 11:23:42 AM	Completed Security Extension Processing in 375 milliseconds.	Event XML
1502	6/17/2025 11:23:42 AM	The Group Policy settings for the computer were processed successfully. New settings from 3 Group Policy objects were detected and applied.	Event XML
8006	6/17/2025 11:23:42 AM	Completed periodic policy processing for computer SECURELABSONDEM\TARGETWINDOWS01$ in 0 seconds.	Event XML
5315	6/17/2025 11:23:42 AM	Next policy processing for SECURELABSONDEM\TARGETWINDOWS01$ will be attempted in 5 minutes.	Event XML

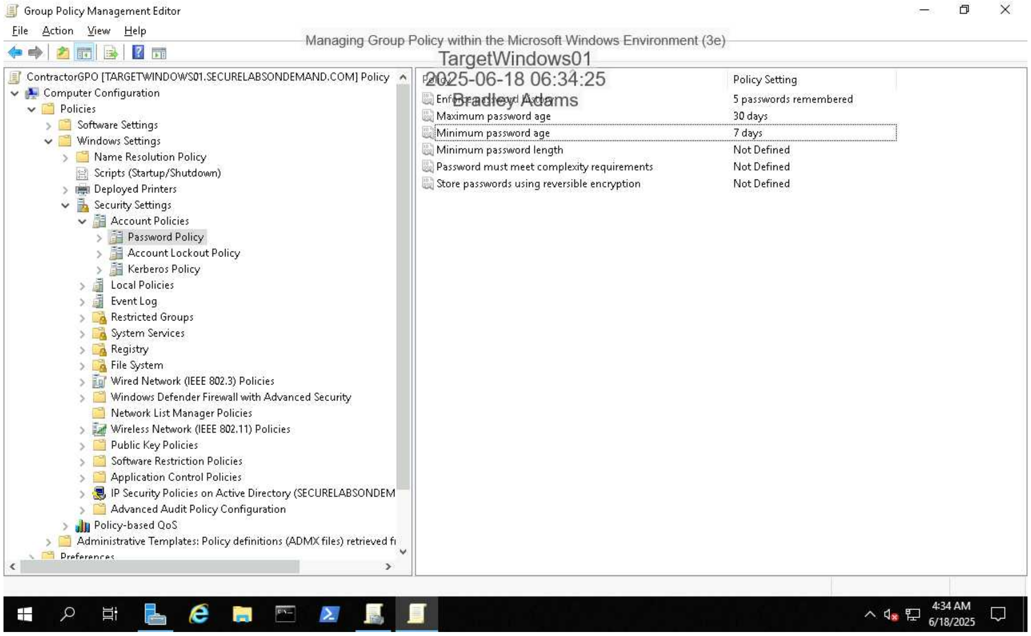
13. **Compare** the GPO Report and the RSoP Report.

The GPO report shows the configured settings within the group policy object. The GPO shows setting details about what has been defined such as enabled, disabled, or not configured. The RSoP report shows the actual settings applied to a user or computer. This report includes all GPOs and assists in troubleshooting conflicts.

Section 2: Applied Learning

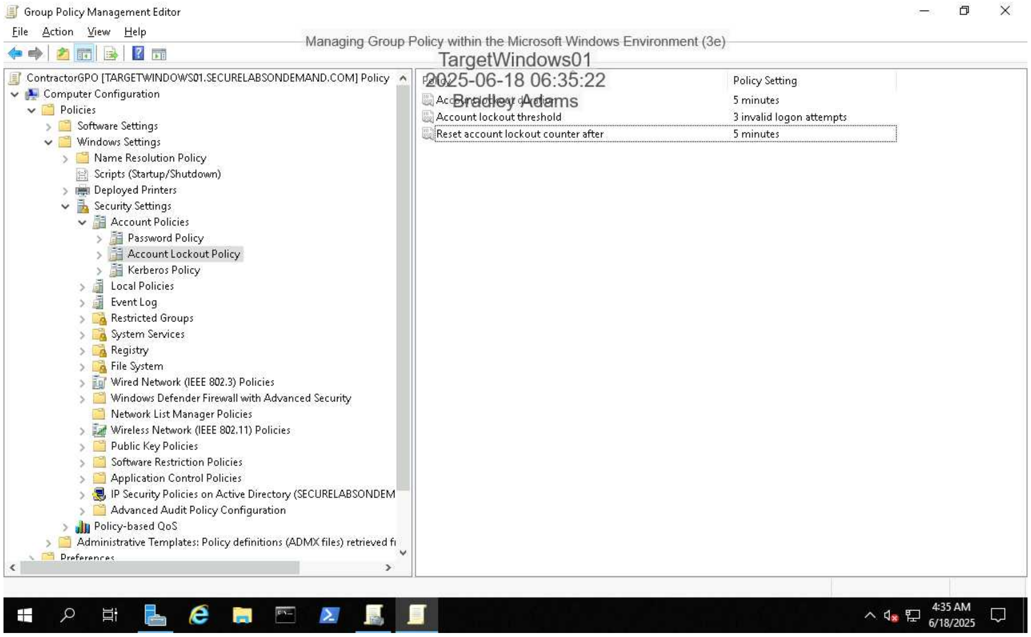
Part 1: Create and Link a New Domain-Level Group Policy Object

4. **Make a screen capture** showing the **new Password Policy for the ContractorsGPO**.


Group Policy Management Editor
File Action View Help
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 06:34:25
Bradley Adams
ContractorGPO [TARGETWINDOWS01.SECURELABSONDEMAND.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (SECURELABSONDEM
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved fr
Preferences
4:34 AM
6/18/2025

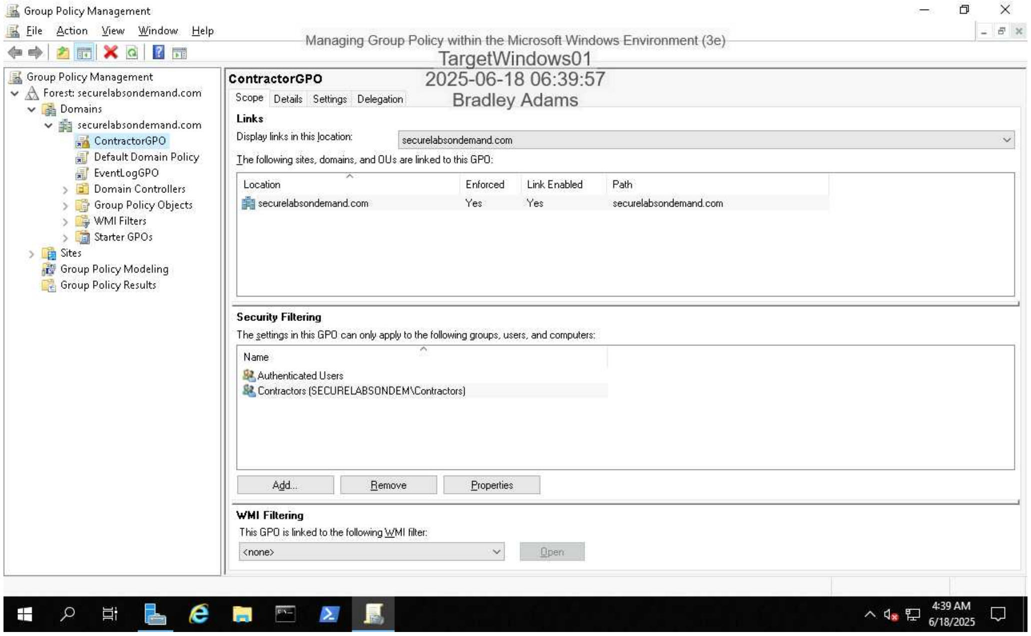
Policy	Policy Setting
Enforce password history	5 passwords remembered
Maximum password age	30 days
Minimum password age	7 days
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

6. **Make a screen capture** showing the **new Account Lockout Policy for the ContractorsGPO**.


Group Policy Management Editor
File Action View Help
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 06:35:22
Bradley Adams
ContractorGPO [TARGETWINDOWS01.SECURELABSONDEMAND.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (SECURELABSONDEM
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved fr
Preferences
4:35 AM
6/18/2025

Policy	Policy Setting
Account lockout duration	5 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	5 minutes

16. **Make a screen capture** showing the **Contractors group in the ContractorsGPO**.



Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 06:39:57
Bradley Adams

ContractorGPO

Links

Display links in this location: securelabsondemand.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
securelabsondemand.com	Yes	Yes	securelabsondemand.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users
Contractors (SECURELABSONDEM\Contractors)

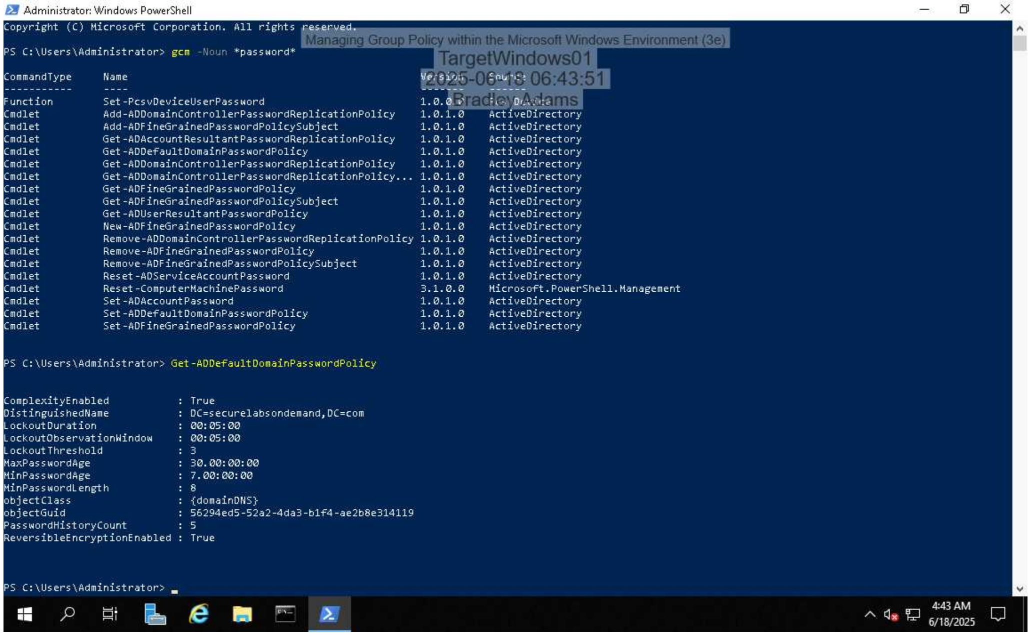
WMI Filtering

This GPO is linked to the following WMI filter:

<none>

Part 2: Edit the Default Domain Policy

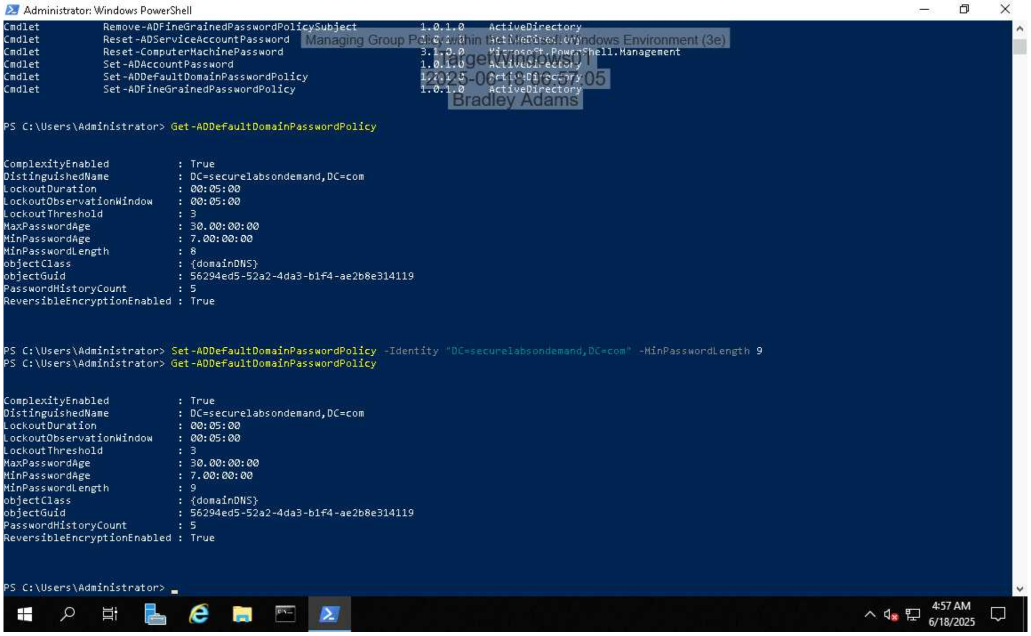
4. **Make a screen capture** showing the **current default domain password policy**.



Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 06:43:51
Bradley Adams

```
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gcm -Noun *password*

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Set-PcsvDeviceUserPassword                         1.0.0.0    PcsvDevice
Cmdlet          Add-ADDomainControllerPasswordReplicationPolicy    1.0.1.0    ActiveDirectory
Cmdlet          Add-ADFineGrainedPasswordPolicySubject             1.0.1.0    ActiveDirectory
Cmdlet          Get-ADAccountResultantPasswordReplicationPolicy    1.0.1.0    ActiveDirectory
Cmdlet          Get-ADDefaultDomainPasswordPolicy                  1.0.1.0    ActiveDirectory
Cmdlet          Get-ADDomainControllerPasswordReplicationPolicy    1.0.1.0    ActiveDirectory
Cmdlet          Get-ADDomainControllerPasswordReplicationPolicy... 1.0.1.0    ActiveDirectory
Cmdlet          Get-ADFineGrainedPasswordPolicy                    1.0.1.0    ActiveDirectory
Cmdlet          Get-ADFineGrainedPasswordPolicySubject             1.0.1.0    ActiveDirectory
Cmdlet          Get-ADUserResultantPasswordPolicy                  1.0.1.0    ActiveDirectory
Cmdlet          New-ADFineGrainedPasswordPolicy                    1.0.1.0    ActiveDirectory
Cmdlet          Remove-ADDomainControllerPasswordReplicationPolicy 1.0.1.0    ActiveDirectory
Cmdlet          Remove-ADFineGrainedPasswordPolicy                 1.0.1.0    ActiveDirectory
Cmdlet          Remove-ADFineGrainedPasswordPolicySubject          1.0.1.0    ActiveDirectory
Cmdlet          Reset-ADServiceAccountPassword                     1.0.1.0    ActiveDirectory
Cmdlet          Reset-ComputerMachinePassword                      3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Set-ADAccountPassword                              1.0.1.0    ActiveDirectory
Cmdlet          Set-ADDefaultDomainPasswordPolicy                  1.0.1.0    ActiveDirectory
Cmdlet          Set-ADFineGrainedPasswordPolicy                    1.0.1.0    ActiveDirectory


PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=securelabsondemand,DC=com
LockoutDuration             : 00:05:00
LockoutObservationWindow    : 00:05:00
LockoutThreshold            : 3
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 7.00:00:00
MinPasswordLength           : 8
objectClass                 : {domainDNS}
objectGuid                  : 56294ed5-52a2-4da3-b1f4-ae2b8e314119
PasswordHistoryCount        : 5
ReversibleEncryptionEnabled : True


PS C:\Users\Administrator> _
```

7. **Make a screen capture** showing the **modified default domain password policy**.

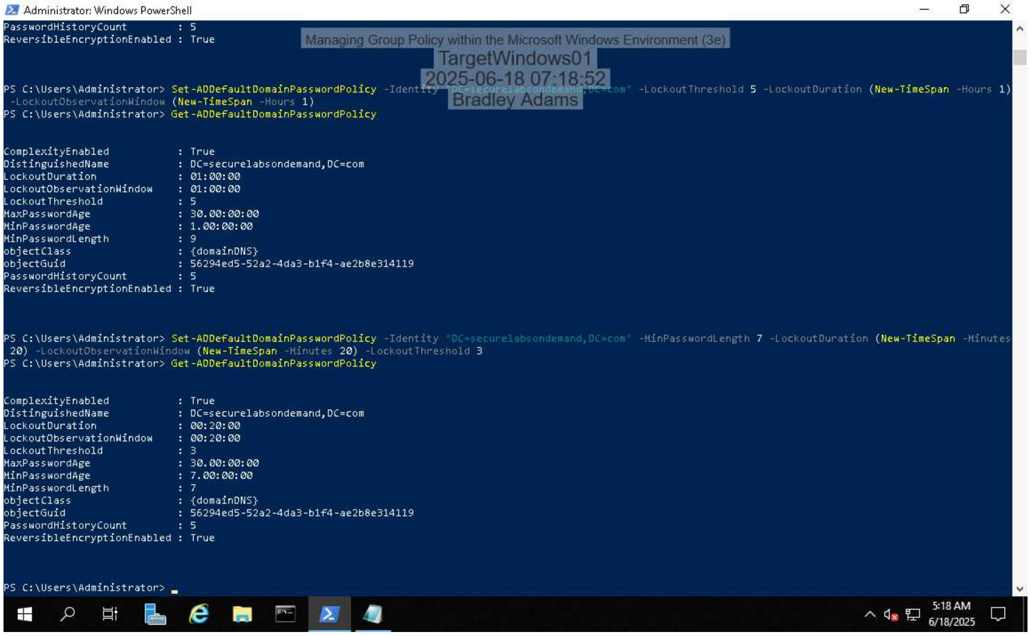

Administrator: Windows PowerShell
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 06:57:05
Bradley Adams
4:57 AM
6/18/2025

```
Cmdlet          Remove-ADFineGrainedPasswordPolicySubject          1.0.1.0    ActiveDirectory
Cmdlet          Reset-ADServiceAccountPassword                     1.0.1.0    ActiveDirectory
Cmdlet          Reset-ComputerMachinePassword                      3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Set-ADAccountPassword                              1.0.1.0    ActiveDirectory
Cmdlet          Set-ADDefaultDomainPasswordPolicy                  1.0.1.0    ActiveDirectory
Cmdlet          Set-ADFineGrainedPasswordPolicy                    1.0.1.0    ActiveDirectory


PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=securelabsondemand,DC=com
LockoutDuration             : 00:05:00
LockoutObservationWindow    : 00:05:00
LockoutThreshold            : 3
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 7.00:00:00
MinPasswordLength           : 8
objectClass                 : {domainDNS}
objectGuid                  : 56294ed5-52a2-4da3-b1f4-ae2b8e314119
PasswordHistoryCount        : 5
ReversibleEncryptionEnabled : True



PS C:\Users\Administrator> Set-ADDefaultDomainPasswordPolicy -Identity "DC=securelabsondemand,DC=com" -MinPasswordLength 9
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=securelabsondemand,DC=com
LockoutDuration             : 00:05:00
LockoutObservationWindow    : 00:05:00
LockoutThreshold            : 3
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 7.00:00:00
MinPasswordLength           : 9
objectClass                 : {domainDNS}
objectGuid                  : 56294ed5-52a2-4da3-b1f4-ae2b8e314119
PasswordHistoryCount        : 5
ReversibleEncryptionEnabled : True


PS C:\Users\Administrator> _
```

13. **Document** the **PowerShell command you used to make the changes**.

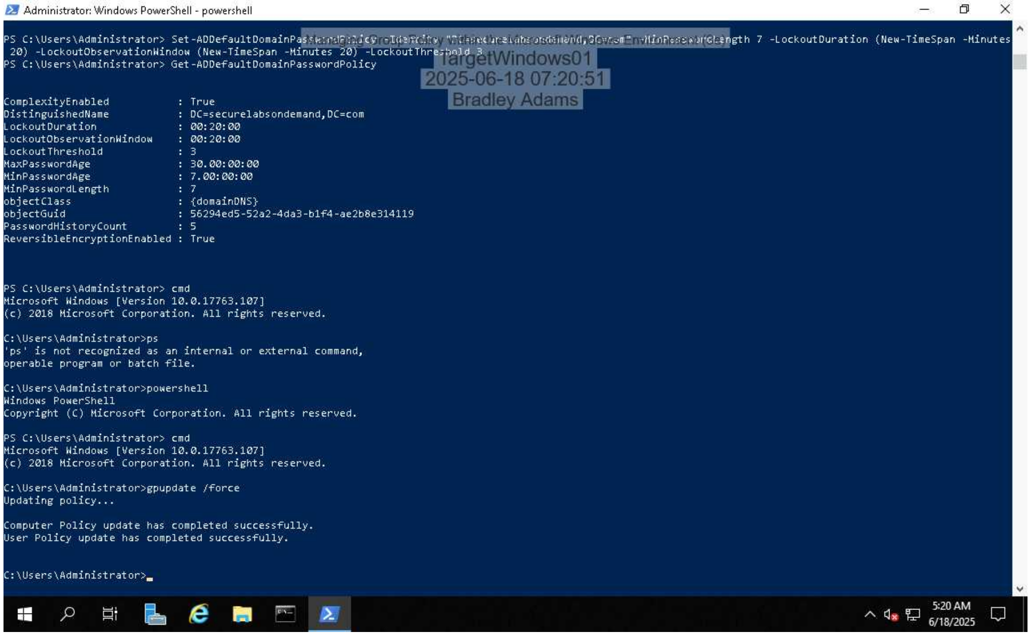
Set-ADDefaultDomainPasswordPolicy -Identity "DC=securelabsondemand,DC=com" -MinPasswordLength 7 -LockoutDuration (New-TimeSpan -Minutes 20) -LockoutObservationWindow (New-TimeSpan -Minutes 20) -LockoutThreshold 3

15. **Make a screen capture** showing the **final default domain password policy**.


Administrator: Windows PowerShell
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 07:18:52
Bradley Adams
5:18 AM
6/18/2025

```
PasswordHistoryCount        : 5
ReversibleEncryptionEnabled : True


PS C:\Users\Administrator> Set-ADDefaultDomainPasswordPolicy -Identity "DC=securelabsondemand,DC=com" -LockoutThreshold 5 -LockoutDuration (New-TimeSpan -Hours 1)
 -LockoutObservationWindow (New-TimeSpan -Hours 1)
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=securelabsondemand,DC=com
LockoutDuration             : 01:00:00
LockoutObservationWindow    : 01:00:00
LockoutThreshold            : 5
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 1.00:00:00
MinPasswordLength           : 9
objectClass                 : {domainDNS}
objectGuid                  : 56294ed5-52a2-4da3-b1f4-ae2b8e314119
PasswordHistoryCount        : 5
ReversibleEncryptionEnabled : True


PS C:\Users\Administrator> Set-ADDefaultDomainPasswordPolicy -Identity "DC=securelabsondemand,DC=com" -MinPasswordLength 7 -LockoutDuration (New-TimeSpan -Minutes
 20) -LockoutObservationWindow (New-TimeSpan -Minutes 20) -LockoutThreshold 3
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=securelabsondemand,DC=com
LockoutDuration             : 00:20:00
LockoutObservationWindow    : 00:20:00
LockoutThreshold            : 3
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 7.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 56294ed5-52a2-4da3-b1f4-ae2b8e314119
PasswordHistoryCount        : 5
ReversibleEncryptionEnabled : True


PS C:\Users\Administrator> _
```

18. **Make a screen capture** showing the **successful gpupdate command**.


Administrator: Windows PowerShell - powershell
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 07:20:51
Bradley Adams
5:20 AM
6/18/2025

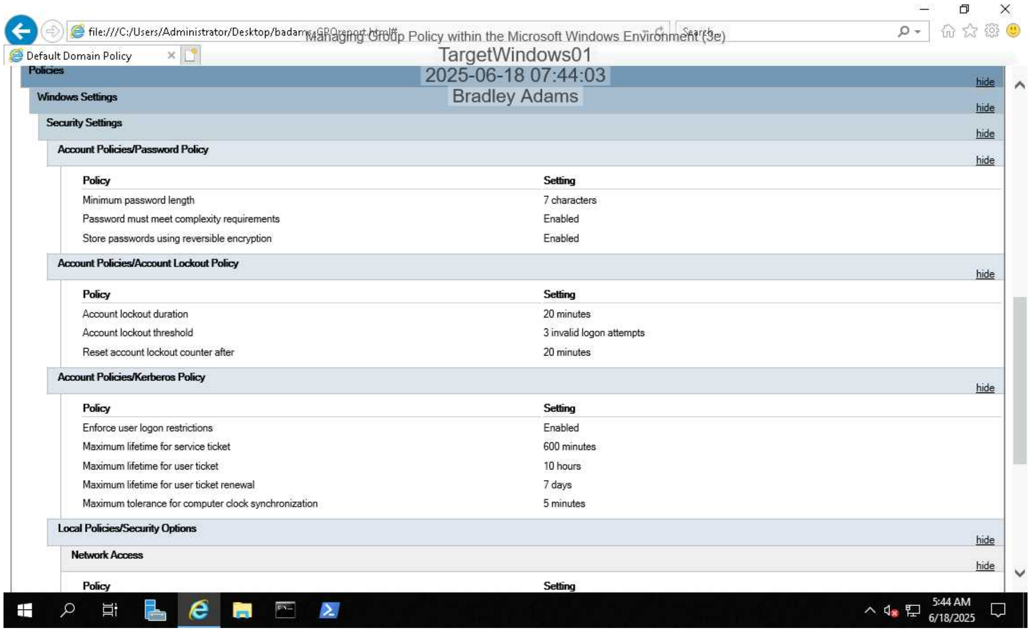
```
PS C:\Users\Administrator> Set-ADDefaultDomainPasswordPolicy -Identity "DC=securelabsondemand,DC=com" -MinPasswordLength 7 -LockoutDuration (New-TimeSpan -Minutes
 20) -LockoutObservationWindow (New-TimeSpan -Minutes 20) -LockoutThreshold 3
PS C:\Users\Administrator> Get-ADDefaultDomainPasswordPolicy


ComplexityEnabled           : True
DistinguishedName           : DC=securelabsondemand,DC=com
LockoutDuration             : 00:20:00
LockoutObservationWindow    : 00:20:00
LockoutThreshold            : 3
MaxPasswordAge              : 30.00:00:00
MinPasswordAge              : 7.00:00:00
MinPasswordLength           : 7
objectClass                 : {domainDNS}
objectGuid                  : 56294ed5-52a2-4da3-b1f4-ae2b8e314119
PasswordHistoryCount        : 5
ReversibleEncryptionEnabled : True



PS C:\Users\Administrator> cmd
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ps
'ps' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cmd
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator>_
```

Part 3: Document and Audit Group Policy

3. **Document** the **PowerShell command you used to generate the GPO report**.

```
Get-GPOReport -Name "Default Domain Policy" -ReportType Html -Path
"C:\Users\Administrator\Desktop\badams_GPOreport.html"
```

5. **Make a screen capture** showing the **final password policy changes**.


file:///C:/Users/Administrator/Desktop/badams_GPOreport.html
Search...
Default Domain Policy
hide

Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 07:44:03
Bradley Adams

Policies
Windows Settings
Security Settings
Account Policies/Password Policy

Policy	Setting
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Enabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	20 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	20 minutes

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Security Options
Network Access

Policy	Setting

5:44 AM
6/18/2025

Section 3: Challenge and Analysis

Part 1: Analysis and Discussion

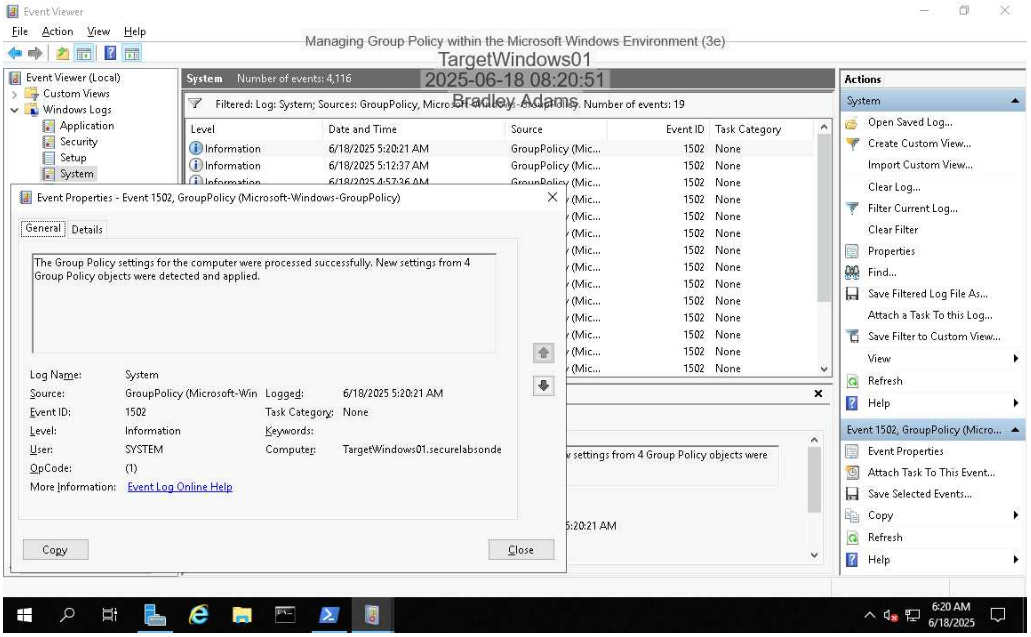
What are some of the benefits of using Group Policy in an enterprise environment? Use the Internet to research additional applications of Group Policy not discussed in this lab.

Group policy in an enterprise has several benefits, including Centralized Management, which allows administrators to configure and enforce settings across all domain workstations from a central location. It also improves security through password policies, software restrictions, and firewall rules. Group policy can deploy and update software packages, making software rollout centrally managed. Group policy can lock down critical settings and minimize user misconfiguration, which reduces help desk calls.

Sources:
https://www.demandtalk.com/insights/it-infra/why-group-policy-management-is-necessary-for-every-enterprise/
https://www.techtarget.com/searchwindowsserver/definition/Group-Policy-Object
https://www.ninjaone.com/blog/what-is-group-policy-in-active-directory/

Part 2: Tools and Commands

Make a screen capture showing the **filtered System Logs and the log entry associated with your changes**.



Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 08:20:51
Bradley Adams

System Number of events: 4,116

Filtered: Log: System; Sources: GroupPolicy, Microsoft-Windows-GroupPolicy. Number of events: 19

Level	Date and Time	Source	Event ID	Task Category
Information	6/18/2025 5:20:21 AM	GroupPolicy (Mic...	1502	None
Information	6/18/2025 5:12:37 AM	GroupPolicy (Mic...	1502	None
Information	6/18/2025 4:57:36 AM	GroupPolicy (Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None
		(Mic...	1502	None

Event Properties - Event 1502, GroupPolicy (Microsoft-Windows-GroupPolicy)

The Group Policy settings for the computer were processed successfully. New settings from 4 Group Policy objects were detected and applied.

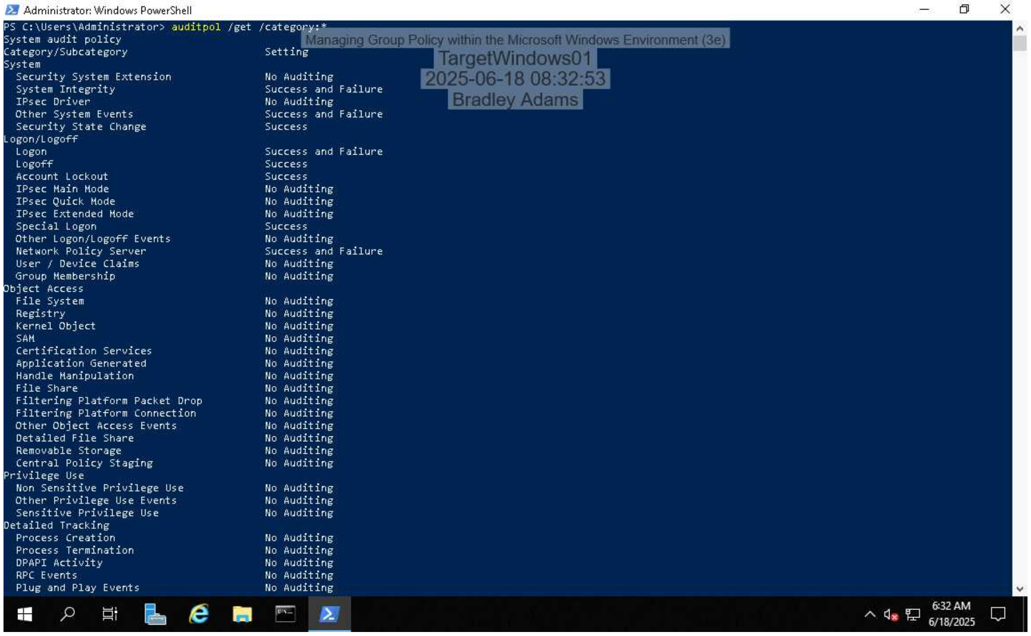
Log Name:	System		
Source:	GroupPolicy (Microsoft-Win	Logged:	6/18/2025 5:20:21 AM
Event ID:	1502	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	TargetWindows01.securelabsonde
OpCode:	(1)		
More Information:	Event Log Online Help		

w settings from 4 Group Policy objects were

5:20:21 AM

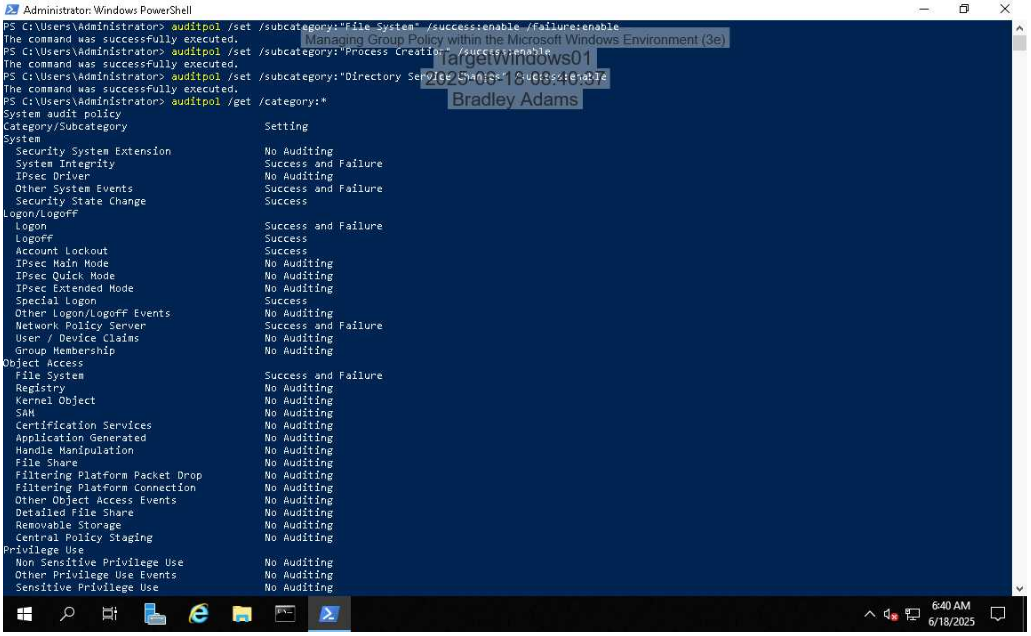
Part 3: Challenge Exercise

Make a screen capture showing the **current Audit Policy using either the Group Policy Management Editor or Windows PowerShell**.


Administrator: Windows PowerShell
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 08:32:53
Bradley Adams
6:32 AM
6/18/2025

```
PS C:\Users\Administrator> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
Detailed Tracking
  Process Creation                        No Auditing
  Process Termination                     No Auditing
  DPAPI Activity                          No Auditing
  RPC Events                              No Auditing
  Plug and Play Events                    No Auditing
```

Make a screen capture showing the **updated Audit Policy**.


Administrator: Windows PowerShell
Managing Group Policy within the Microsoft Windows Environment (3e)
TargetWindows01
2025-06-18 08:40:37
Bradley Adams
6:40 AM
6/18/2025

```
PS C:\Users\Administrator> auditpol /set /subcategory:"File System" /success:enable /failure:enable
The command was successfully executed.
PS C:\Users\Administrator> auditpol /set /subcategory:"Process Creation" /success:enable
The command was successfully executed.
PS C:\Users\Administrator> auditpol /set /subcategory:"Directory Service Changes" /success:enable
The command was successfully executed.
PS C:\Users\Administrator> auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        Success and Failure
  IPsec Driver                            No Auditing
  Other System Events                     Success and Failure
  Security State Change                   Success
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  Success
  Account Lockout                         Success
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           Success
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   Success and Failure
  User / Device Claims                    No Auditing
  Group Membership                        No Auditing
Object Access
  File System                             Success and Failure
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       No Auditing
  Central Policy Staging                  No Auditing
Privilege Use
  Non Sensitive Privilege Use             No Auditing
  Other Privilege Use Events              No Auditing
  Sensitive Privilege Use                 No Auditing
```